





Join a community dedicated to learning open source

The Red Hat® Learning Community is a collaborative platform for users to accelerate open source skill adoption while working with Red Hat products and experts.



Network with tens of thousands of community members



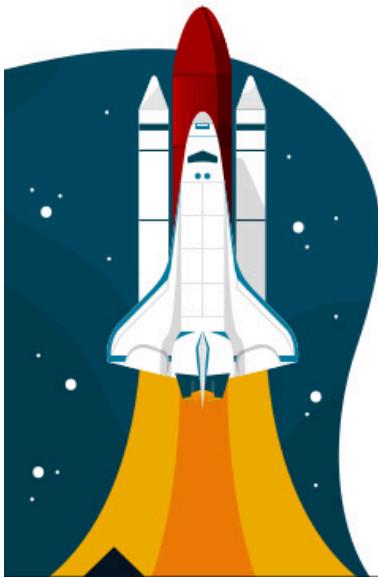
Engage in thousands of active conversations and posts



Join and interact with hundreds of certified training instructors



Unlock badges as you participate and accomplish new goals



This knowledge-sharing platform creates a space where learners can connect, ask questions, and collaborate with other open source practitioners.

Access free Red Hat training videos

Discover the latest Red Hat Training and Certification news

Connect with your instructor - and your classmates - before, after, and during your training course.

Join peers as you explore Red Hat products

Join the conversation learn.redhat.com



Copyright © 2020 Red Hat, Inc. Red Hat, Red Hat Enterprise Linux, the Red Hat logo, and Ansible are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Red Hat OpenShift I: Containers & Kubernetes



OCP 4.10 DO180
Red Hat OpenShift I: Containers & Kubernetes
Edition 3 20220819
Publication date 20220819

Authors: Zach Guterman, Dan Kolepp, Eduardo Ramirez Ronco, Jordi Sola Alaball, Richard Allred, Michael Jarrett, Harpal Singh, Federico Capitalle, Maria Fernanda Ordonez Casado, Aykut Bulgu, Shatakshi Jain, Sourabh Mishra, Andres Hernandez, Ivan Chavero
Editors: Seth Kenlon, Dave Sacco, Connie Petlitzer, Nicole Muller, Sam Ffrench

Copyright © 2021 Red Hat, Inc.

The contents of this course and all its modules and related materials, including handouts to audience members, are Copyright © 2021 Red Hat, Inc.

No part of this publication may be stored in a retrieval system, transmitted or reproduced in any way, including, but not limited to, photocopy, photograph, magnetic, electronic or other record, without the prior written permission of Red Hat, Inc.

This instructional program, including all material provided herein, is supplied without any guarantees from Red Hat, Inc. Red Hat, Inc. assumes no liability for damages or legal action arising from the use or misuse of contents or details contained herein.

If you believe Red Hat training materials are being used, copied, or otherwise improperly distributed, please send email to training@redhat.com or phone toll-free (USA) +1 (866) 626-2994 or +1 (919) 754-3700.

Red Hat, Red Hat Enterprise Linux, the Red Hat logo, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph, and Gluster are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries 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 American, Inc. and/or its affiliates.

XFS® is a registered trademark of Hewlett Packard Enterprise Development LP 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 a 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 the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. Red Hat, Inc. is not affiliated with, endorsed by, or sponsored by the OpenStack Foundation or the OpenStack community.

All other trademarks are the property of their respective owners.

Contributors: Forrest Taylor, Manuel Aude Morales, James Mighion, Michael Phillips, and Fiona Allen

Document Conventions	ix
	ix
Introduction	xi
DO180: Red Hat OpenShift I: Containers & Kubernetes	xi
Internationalization	xii
Orientation to the Classroom Environment	xvii
Performing Lab Exercises	xxi
1. Introducing Container Technology	1
Overview of Container Technology	2
Quiz: Overview of Container Technology	5
Overview of Container Architecture	9
Quiz: Overview of Container Architecture	12
Overview of Kubernetes and OpenShift	14
Quiz: Describing Kubernetes and OpenShift	17
Guided Exercise: Configuring the Classroom Environment	19
Summary	27
2. Creating Containerized Services	29
Provisioning Containerized Services	30
Guided Exercise: Creating a MySQL Database Instance	36
Using Rootless Containers	39
Guided Exercise: Exploring Root and Rootless Containers	41
Lab: Creating Containerized Services	43
Summary	46
3. Managing Containers	47
Managing the Lifecycle of Containers	48
Guided Exercise: Managing a MySQL Container	56
Attaching Persistent Storage to Containers	59
Guided Exercise: Create MySQL Container with Persistent Database	63
Accessing Containers	66
Guided Exercise: Loading the Database	68
Lab: Managing Containers	71
Summary	80
4. Managing Container Images	81
Accessing Registries	82
Quiz: Working with Registries	88
Manipulating Container Images	92
Guided Exercise: Creating a Custom Apache Container Image	98
Lab: Managing Images	103
Summary	112
5. Creating Custom Container Images	113
Designing Custom Container Images	114
Quiz: Approaches to Container Image Design	118
Building Custom Container Images with Containerfiles	120
Guided Exercise: Creating a Basic Apache Container Image	126
Lab: Creating Custom Container Images	130
Summary	137
6. Deploying Containerized Applications on OpenShift	139
Describing Kubernetes and OpenShift Architecture	140
Quiz: Describing Kubernetes and OpenShift	147
Creating Kubernetes Resources	151
Guided Exercise: Deploying a Database Server on OpenShift	163

Creating Routes	168
Guided Exercise: Exposing a Service as a Route	172
Creating Applications with Source-to-Image	177
Guided Exercise: Creating a Containerized Application with Source-to-Image	187
Creating Applications with the OpenShift Web Console	193
Guided Exercise: Creating an Application with the Web Console	198
Lab: Deploying Containerized Applications on OpenShift	210
Summary	214
7. Deploying Multi-Container Applications	215
Considerations for Multi-Container Applications	216
Guided Exercise: Deploying the Web Application and MySQL on Linux Containers	221
Deploying a Multi-Container Application on OpenShift	226
Guided Exercise: Creating an Application on OpenShift	228
Deploying a Multi-container Application on OpenShift Using a Template	232
Guided Exercise: Creating an Application with a Template	238
Lab: Deploying Multi-Container Applications	242
Summary	249
8. Troubleshooting Containerized Applications	251
Troubleshooting S2I Builds and Deployments	252
Guided Exercise: Troubleshooting an OpenShift Build	258
Troubleshooting Containerized Applications	266
Guided Exercise: Configuring Apache Container Logs for Debugging	272
Lab: Troubleshooting Containerized Applications	275
Summary	286
9. Comprehensive Review	287
Comprehensive Review	288
Lab: Containerizing and Deploying a Software Application	290
A. Implementing Microservices Architecture	301
Implementing Microservices Architectures	302
Guided Exercise: Refactoring the To Do List Application	307
Summary	312
B. Creating a GitHub Account	313
Creating a GitHub Account	314
C. Creating a Quay Account	317
Creating a Quay Account	318
Repository Visibility	320
D. Creating a Red Hat Account	323
Creating a Red Hat Account	324
E. Useful Git Commands	327
Git Commands	328

Document Conventions

This section describes various conventions and practices that are used throughout all Red Hat Training courses.

Admonitions

Red Hat Training courses use the following admonitions:



References

References describe where to find external documentation that is relevant to a subject.



Note

Notes are tips, shortcuts, or alternative approaches to the task at hand. Ignoring a note should have no negative consequences, but you might miss out on something that makes your life easier.



Important

They provide details of information that is easily missed: configuration changes that apply only to the current session, or services that need restarting before an update applies. Ignoring these admonitions will not cause data loss, but might cause irritation and frustration.



Warning

Warnings should not be ignored. Ignoring these admonitions will most likely cause data loss.

Inclusive Language

Red Hat Training is currently reviewing its use of language in various areas to help remove any potentially offensive terms. This is an ongoing process and requires alignment with the products and services that are covered in Red Hat Training courses. Red Hat appreciates your patience during this process.

Introduction

DO180: Red Hat OpenShift I: Containers & Kubernetes

DO180: Red Hat OpenShift I: Containers & Kubernetes is a hands-on course that teaches students how to create, deploy, and manage containers using Podman, Kubernetes, and the Red Hat OpenShift Container Platform.

One of the key tenants of the DevOps movement is continuous integration and continuous deployment. Containers have become a key technology for the configuration and deployment of applications and microservices. Red Hat OpenShift Container Platform is an implementation of Kubernetes, a container orchestration system.

Course Objectives

- Demonstrate knowledge of the container ecosystem.
- Manage Linux containers using Podman.
- Deploy containers on a Kubernetes cluster using the OpenShift Container Platform.
- Demonstrate basic container design and the ability to build container images.
- Implement a container-based architecture using knowledge of containers, Kubernetes, and OpenShift.

Audience

- System Administrators
- Developers
- IT Leaders and Infrastructure Architects

Prerequisites

Students should meet one or more of the following prerequisites:

- Be able to use a Linux terminal session and issue operating system commands. An RHCSA certification is recommended but not required.
- Have experience with web application architectures and their corresponding technologies.

Internationalization

Per-user Language Selection

Your users might prefer to use a different language for their desktop environment than the system-wide default. They might also want to use a different keyboard layout or input method for their account.

Language Settings

In the GNOME desktop environment, the user might be prompted to set their preferred language and input method on first login. If not, then the easiest way for an individual user to adjust their preferred language and input method settings is to use the **Region & Language** application.

You can start this application in two ways. You can run the `gnome-control-center region` command from a terminal window, or on the top bar, from the system menu in the right corner, select the settings button (which has a crossed screwdriver and wrench for an icon) from the bottom left of the menu.

In the window that opens, select **Region & Language**. Click the **Language** box and select the preferred language from the list that appears. This also updates the **Formats** setting to the default for that language. The next time you log in, these changes will take full effect.

These settings affect the GNOME desktop environment and any applications such as `gnome-terminal` that are started inside it. However, by default they do not apply to that account if accessed through an `ssh` login from a remote system or a text-based login on a virtual console (such as `tty5`).

Individual commands can be made to use another language by setting the `LANG` environment variable.

```
[user@host ~]$ LANG=fr_FR.utf8 date  
mar. mai 24 12:16:51 CDT 2022
```

Subsequent commands will revert to using the system's default language for output. The `locale` command can be used to determine the current value of `LANG` and other related environment variables.

Input Method Settings

GNOME 3 in Red Hat Enterprise Linux 7 or later automatically uses the `IBus` input method selection system, which makes it easy to change keyboard layouts and input methods quickly.

The **Region & Language** application can also be used to enable alternative input methods. In the **Region & Language** application window, the **Input Sources** box shows what input methods are currently available. By default, English (US) may be the only available method. Highlight English (US) and click the **Keyboard** icon to see the current keyboard layout.

To add another input method, click the **+** button at the bottom left of the **Input Sources** window. An **Add an Input Source** window will open. Select your language, and then your preferred input method or keyboard layout.

Introduction

When more than one input method is configured, the user can switch between them quickly by typing Super+Space (sometimes called Windows+Space). A status indicator will also appear in the GNOME top bar, which has two functions: It indicates which input method is active, and acts as a menu that can be used to switch between input methods or select advanced features of more complex input methods.

Some of the methods are marked with gears, which indicate that those methods have advanced configuration options and capabilities. For example, the Japanese Japanese (Kana Kanji) input method allows the user to pre-edit text in Latin and use Up Arrow and Down Arrow keys to select the correct characters to use.

US English speakers may also find this useful. For example, under English (United States) is the keyboard layout English (international AltGr dead keys), which treats AltGr (or the right Alt) on a PC 104/105-key keyboard as a "secondary shift" modifier key and dead key activation key for typing additional characters. There are also Dvorak and other alternative layouts available.



Note

Any Unicode character can be entered in the GNOME desktop environment if you know the character's Unicode code point. Type Ctrl+Shift+U, followed by the code point. After Ctrl+Shift+U has been typed, an underlined u will be displayed to indicate that the system is waiting for Unicode code point entry.

For example, the lowercase Greek letter lambda has the code point U+03BB, and can be entered by typing Ctrl+Shift+U, then 03BB, then Enter.

System-wide Default Language Settings

The system's default language is set to US English, using the UTF-8 encoding of Unicode as its character set (`en_US.utf8`), but this can be changed during or after installation.

From the command line, the `root` user can change the system-wide locale settings with the `localectl` command. If you run `localectl` with no arguments, it displays the current system-wide locale settings.

To set the system-wide default language, run the `localectl set-locale LANG=locale` command, where `locale` is the appropriate value for the `LANG` environment variable from the "Language Codes Reference" table in this chapter. The change will take effect for users on their next login, and is stored in `/etc/locale.conf`.

```
[root@host ~]# localectl set-locale LANG=fr_FR.utf8
```

In GNOME, an administrative user can change this setting from Region & Language by clicking the Login Screen button at the upper-right corner of the window. Changing the language of the graphical login screen will also adjust the system-wide default language setting stored in the `/etc/locale.conf` configuration file.

**Important**

Text-based virtual consoles such as `tty4` are more limited in the fonts they can display than terminals in a virtual console running a graphical environment, or pseudoterminals for `ssh` sessions. For example, Japanese, Korean, and Chinese characters may not display as expected on a text-based virtual console.

For this reason, you should consider using English or another language with a Latin character set for the system-wide default. Likewise, text-based virtual consoles are more limited in the input methods they support, and this is managed separately from the graphical desktop environment.

The available global input settings can be configured through `localectl` for both text-based virtual consoles and the graphical environment. See the `localectl(1)` and `vconsole.conf(5)` man pages for more information.

Language Packs

Special RPM packages called langpacks install language packages that add support for specific languages. These language packs use dependencies to automatically install additional RPM packages containing localizations, dictionaries, and translations for other software packages on your system.

To list the langpacks that are installed and that may be installed, use the following command.

```
[root@host ~]# yum list langpacks-*
Updating Subscription Management repositories.
Updating Subscription Management repositories.
Installed Packages
langpacks-en.noarch      1.0-12.el8      @AppStream
Available Packages
langpacks-af.noarch      1.0-12.el8      rhel-8-for-x86_64-appstream-rpms
langpacks-am.noarch      1.0-12.el8      rhel-8-for-x86_64-appstream-rpms
langpacks-ar.noarch      1.0-12.el8      rhel-8-for-x86_64-appstream-rpms
langpacks-as.noarch      1.0-12.el8      rhel-8-for-x86_64-appstream-rpms
langpacks-ast.noarch     1.0-12.el8      rhel-8-for-x86_64-appstream-rpms
...output omitted...
```

To add language support, install the appropriate language packs package. For example, the following command adds support for French.

```
[root@host ~]# yum install langpacks-fr
```

Use `yum repoquery --whatsonplements` to determine what RPM packages might be installed by a language pack.

```
[root@host ~]# yum repoquery --whatsonplements langpacks-fr
Updating Subscription Management repositories.
Updating Subscription Management repositories.
Last metadata expiration check: 0:01:33 ago on Wed 06 Feb 2019 10:47:24 AM CST.
glibc-langpack-fr-0:2.28-18.el8.x86_64
gnome-getting-started-docs-fr-0:3.28.2-1.el8.noarch
hunspell-fr-0:6.2-1.el8.noarch
```

Introduction

```
hyphen-fr-0:3.0-1.el8.noarch
libreoffice-langpack-fr-1:6.0.6.1-9.el8.x86_64
man-pages-fr-0:3.70-16.el8.noarch
mythes-fr-0:2.3-10.el8.noarch
```

**Important**

Langpacks packages use RPM weak dependencies in order to install supplementary packages only when the core package that needs it is also installed.

For example, when installing `langpacks-fr` as shown in the preceding examples, the `mythes-fr` package will only be installed if the `mythes` thesaurus is also installed on the system.

If `mythes` is subsequently installed on that system, the `mythes-fr` package will also automatically be installed due to the weak dependency from the already installed `langpacks-fr` package.

**Note**

This table might not reflect all the language packs available on your system. Use `yum info langpacks-SUFFIX` to get more information about any particular langpacks package.

Language Codes Reference

**Note**

This table might not reflect all the language packs available on your system. Use `yum info langpacks-SUFFIX` to get more information about any particular langpacks package.

Language Codes

Language	Langpacks Suffix	\$LANG value
English (US)	en	en_US.utf8
Assamese	as	as_IN.utf8
Bengali	bn	bn_IN.utf8
Chinese (Simplified)	zh_CN	zh_CN.utf8
Chinese (Traditional)	zh_TW	zh_TW.utf8
French	fr	fr_FR.utf8
German	de	de_DE.utf8
Gujarati	gu	gu_IN.utf8

Language	Langpacks Suffix	\$LANG value
Hindi	hi	hi_IN.utf8
Italian	it	it_IT.utf8
Japanese	ja	ja_JP.utf8
Kannada	kn	kn_IN.utf8
Korean	ko	ko_KR.utf8
Malayalam	ml	ml_IN.utf8
Marathi	mr	mr_IN.utf8
Odia	or	or_IN.utf8
Portuguese (Brazilian)	pt_BR	pt_BR.utf8
Punjabi	pa	pa_IN.utf8
Russian	ru	ru_RU.utf8
Spanish	es	es_ES.utf8
Tamil	ta	ta_IN.utf8
Telugu	te	te_IN.utf8

Orientation to the Classroom Environment

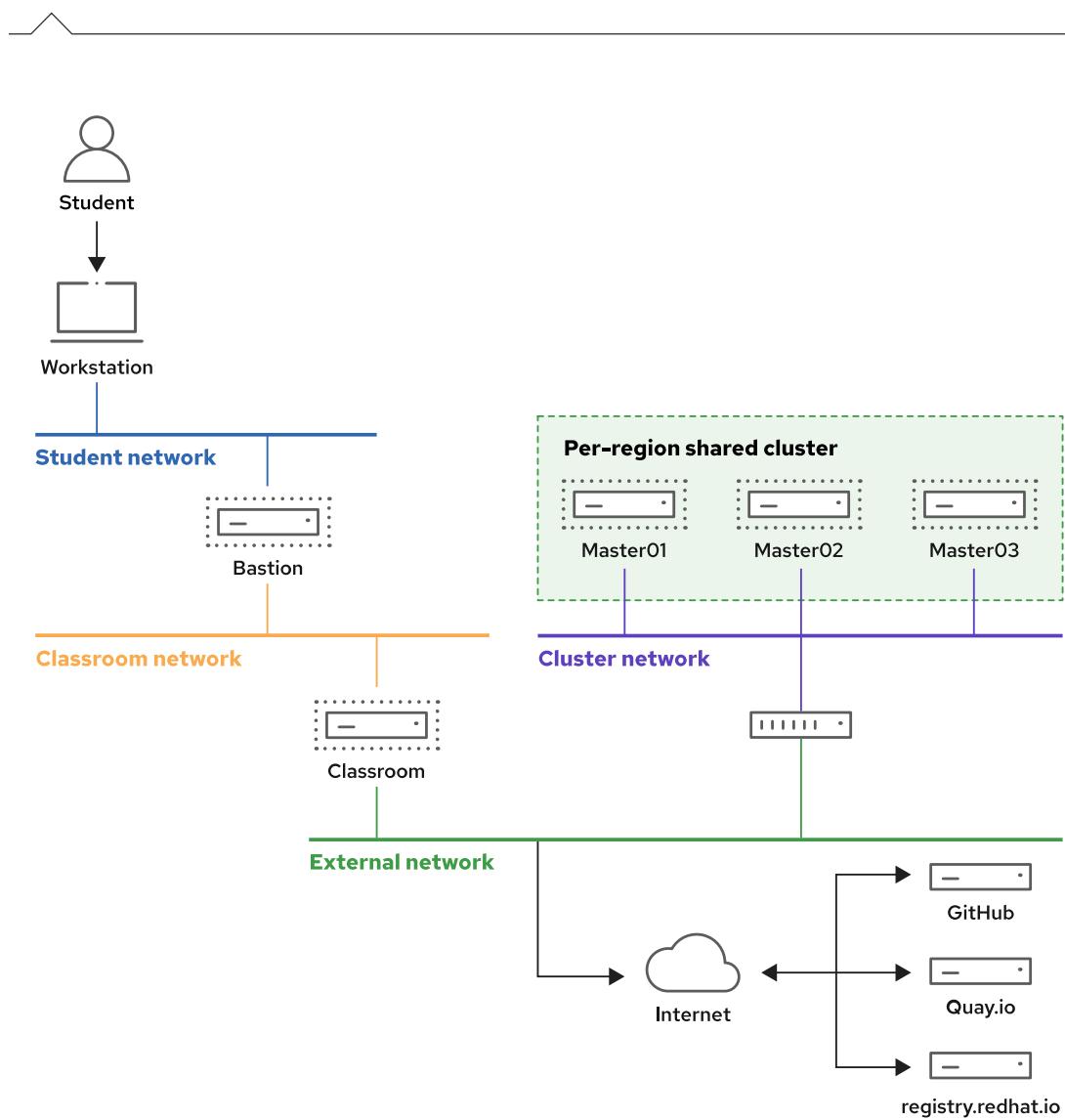


Figure 0.1: Classroom environment

In this course, the main computer system used for hands-on learning activities is **workstation**. This is a virtual machine (VM) named `workstation.lab.example.com`.

All student computer systems have a standard user account, **student**, which has the password **student**. The **root** password on all student systems is **redhat**.

Classroom Machines

Machine name	IP addresses	Role
workstation.lab.example.com	172.25.250.9	Graphical workstation used for system administration.
classroom.example.com	172.25.254.254	Router linking the Classroom Network to the Internet.
bastion.lab.example.com	172.25.252.1	Router linking the Student Network to the Classroom Network.

Several systems in the classroom provide supporting services. Two servers, `content.example.com` and `materials.example.com`, are sources for software and lab materials used in hands-on activities. Information on how to use these servers is provided in the instructions for those activities.

Students use the `workstation` machine to access a shared OpenShift cluster hosted externally. Students do not have cluster administrator privileges on the cluster, but that is not necessary to complete the DO180 content.

Students are provisioned an account on a shared OpenShift 4 cluster when they provision their environments in the Red Hat Online Learning interface. Cluster information such as the API endpoint, and cluster-ID, as well as their username and password are presented to them when they provision their environment.

Students also have access to a MySQL and a Nexus server hosted by either the OpenShift cluster or an external provider. Hands-on activities in this course provide instructions to access these servers when required.

Hands-on activities in DO180 also require that students have personal accounts on two public, free internet services: GitHub and Quay.io. Students need to create these accounts if they do not already have them (see Appendix) and verify their access by signing in to these services before starting the class.

Students are assigned remote computers in a Red Hat Online Learning classroom. They are accessed through a web application hosted at `rol.redhat.com` [<http://rol.redhat.com>]. Students should log in to this site using their Red Hat Customer Portal user credentials.

Controlling Your Systems

You are assigned remote computers in a Red Hat Online Learning (ROLE) classroom. Self-paced courses are accessed through a web application hosted at `rol.redhat.com` [<https://rol.redhat.com>]. If your course is an instructor-led virtual training, you will be provided with your course location URL. Log in to this site using your Red Hat Customer Portal user credentials.

Controlling the Virtual Machines

The virtual machines in your classroom environment are controlled through web page interface controls. The state of each classroom virtual machine is displayed on the **Lab Environment** tab.

The screenshot shows the Red Hat OpenShift Container Platform Lab Environment interface. At the top, there are navigation links for 'Table of Contents', 'Course', 'Lab Environment', and icons for a star and help. Below this is a section titled 'Lab Controls' with instructions: 'Click CREATE to build all of the virtual machines needed for the classroom lab environment. This may take several minutes to complete. Once created the environment can then be stopped and restarted to pause your experience.' It also notes that deleting the lab will remove all virtual machines and lose progress. Below these instructions are three buttons: 'DELETE' (red), 'STOP' (teal), and an info icon ('i'). A table lists five virtual machines with their current state, actions, and console access:

Machine Name	State	Action	Open Console
bastion	active	ACTION -	OPEN CONSOLE
classroom	active	ACTION -	OPEN CONSOLE
servera	building	ACTION -	OPEN CONSOLE
serverb	building	ACTION -	OPEN CONSOLE
workstation	active	ACTION -	OPEN CONSOLE

Machine States

Virtual Machine State	Description
BUILDING	The initial creation of the virtual machine is being performed.
ACTIVE	The virtual machine is running and available. If just started, it may still be starting services.
STOPPED	The virtual machine is completely shut down. Upon starting, the virtual machine boots into the same state as it was before it was shut down. The disk state is preserved.

Depending on the state of a machine, a selection of the following actions is available.

Classroom Actions

Button or Action	Description
CREATE	Create the ROLE classroom. Creates and starts all of the virtual machines needed for this classroom.
CREATING	The ROLE classroom virtual machines are being created. Creates and starts all of the virtual machines needed for this classroom. This action can take several minutes to complete.
DELETE	Delete the ROLE classroom. Destroys all virtual machines in the classroom. All work saved on that system's disks is lost.
START	Start all virtual machines in the classroom.
STARTING	All virtual machines in the classroom are starting.
STOP	Stop all virtual machines in the classroom.

Machine Actions

Button or Action	Description
OPEN CONSOLE	Connect to the system console of the virtual machine in a new browser tab. You can log in directly to the virtual machine and run commands, when required. Normally, log in to the workstation virtual machine only, and from there, use ssh to connect to the other virtual machines.
ACTION > Start	Start (power on) the virtual machine.
ACTION > Shutdown	Gracefully shut down the virtual machine, preserving disk contents.
ACTION > Power Off	Forcefully shut down the virtual machine, while still preserving disk contents. This is equivalent to removing the power from a physical machine.
ACTION > Reset	Forcefully shut down the virtual machine and reset the disk to its initial state. All work saved on that system's disks is lost.

At the start of an exercise, if instructed to reset **a single virtual machine node**, click ACTION > Reset for only the specific virtual machine.

At the start of an exercise, if instructed to reset **all virtual machines**, click ACTION > Reset on every virtual machine in the list.

If you want to return the classroom environment to its original state at the start of the course, you can click **DELETE** to remove the entire classroom environment. After the lab has been deleted, you can click **CREATE** to provision a new set of classroom systems.



Warning

The **DELETE** operation cannot be undone. **All work you have completed in the classroom environment will be lost.**

The Autostop Timer

The Red Hat Online Learning enrollment entitles you to a set allotment of computer time. To help conserve your allotted time, the ROLE classroom uses timers, which shut down or delete the classroom when the appropriate timer expires.

To adjust the timers, locate the two + buttons at the bottom of the course management page. Click the auto-stop + button to add another hour to the auto-stop timer. Click the auto-destroy + button to add another day to the auto-destroy timer. There is a maximum for auto-stop at 12 hours, and a maximum auto-destroy at 14 days. Be careful to keep the timers set while you are working, so as to not have your environment unexpectedly shut down. Be careful not to set the timers unnecessarily high, which could waste your subscription time allotment.

Performing Lab Exercises

Run the `lab` command from the `workstation` machine to prepare your environment before each hands-on exercise, and again to clean up after an exercise. Each hands-on exercise has a unique name within a course. The exercise is prepended with `lab-` as its file name in `/usr/local/lib`. For example, the `instances-cli` exercise has the file name `/usr/local/lib/lab-instances-cli`. To list the available exercises, use tab completion in the `lab` command. Note that the word "Tab" in the following command refers to pressing the Tab key on your keyboard:

```
[student@workstation ~]$ lab Tab Tab
administer-users  deploy-overcloud-lab  prep-deploy-ips      stacks-autoscale
analyze-metrics   instances-cli        prep-deploy-router  stacks-deploy
assign-roles       manage-interfaces  public-instance-deploy verify-overcloud
```

There are two types of exercises. The first type, a guided exercise, is a practice exercise that follows a course narrative. If a narrative is followed by a quiz, this usually indicates that the topic did not have an achievable practice exercise. The second type, an end-of-chapter lab, is a gradable exercise to help verify your learning. When a course includes a comprehensive review, the review exercises are structured as gradable labs. The syntax for running an exercise script is:

```
[student@workstation ~]$ lab exercise action
```

The `action` is a choice of `start`, `grade`, or `finish`. All exercises support `start` and `finish`. Only end-of-chapter labs and comprehensive review labs support `grade`. Older courses might still use `setup` and `cleanup` instead of the current `start` and `finish` actions.

start

Formerly `setup`. The start logic of the script verifies the resources required to begin an exercise. This might include configuring settings, creating resources, checking prerequisite services, and verifying necessary outcomes from previous exercises.

grade

End-of-chapter labs help verify what you have learned, after practicing with earlier guided exercises. The `grade` action directs the `lab` command to display a list of grading criteria, with a `PASS` or `FAIL` status for each. To achieve a `PASS` status for all criteria, fix the failures and re-run the `grade` action.

finish

Formerly `cleanup`. The finish logic of the script deletes exercise resources that are no longer necessary.

Troubleshooting Lab Scripts

Exercise scripts do not exist on the `workstation` machine until each is first run. When you run the `lab` command with a valid exercise and action, the script named `lab-exercise` is downloaded from the `classroom` server content share to `/usr/local/lib` on the `workstation` machine. The `lab` command creates two log files in `/var/tmp/labs`, plus the directory if it does not exist. One file, named `exercise`, captures standard output messages that normally display on your terminal. The other file, named `exercise.err`, captures error messages.

```
[student@workstation ~]$ ls -l /usr/local/lib
-rwxr-xr-x. 1 root root 4131 May  9 23:38 lab-instances-cli
-rwxr-xr-x. 1 root root 93461 May  9 23:38 labtool.cl110.shlib
-rwxr-xr-x. 1 root root 10372 May  9 23:38 labtool.shlib

[student@workstation ~]$ ls -l /var/tmp/labs
-rw-r--r--. 1 root root 113 May  9 23:38 instances-cli
-rw-r--r--. 1 root root 113 May  9 23:38 instances-cli.err
```

**Note**

Scripts download from the `http://content.example.com/courses/COURSE/RELEASE/grading-scripts` share, but only if the script does not yet exist on the `workstation` machine.

If you must download a script again, such as when a script on the share is modified, manually delete the current exercise script from `/usr/local/lib` on the `workstation` machine, then run the `lab` command for the exercise again. The newer exercise script then downloads from the `grading-scripts` share.

To delete all current exercise scripts on the `workstation` machine, use the `lab` command with the `--refresh` option. A refresh deletes all scripts in `/usr/local/lib` but does not delete the log files.

```
[student@workstation ~]$ lab --refresh
[student@workstation ~]$ ls -l /usr/local/lib

[student@workstation ~]$ ls -l /var/tmp/labs
-rw-r--r--. 1 root root 113 May  9 23:38 instances-cli
-rw-r--r--. 1 root root 113 May  9 23:38 instances-cli.err
```

Interpreting the Exercise Log Files

Exercise scripts send output to log files, even when the scripts are successful. Step header text is added between steps and additional date and time headers are added at the start of each script run. The exercise log normally contains messages that indicate successful completion of command steps. Therefore, the exercise output log is useful for observing messages that are expected if no problems occur, but offers no additional help when failures occur.

Instead, the exercise error log is more useful for troubleshooting. Even when the scripts succeed, messages are still sent to the exercise error log. For example, a script that verifies that an object already exists before attempting to create it should cause an *object not found* message when the object does not exist yet. In this scenario, that message is expected and does not indicate a failure. Actual failure messages are typically more verbose, and experienced system administrators should recognize common log message entries.

Although exercise scripts are always run from the `workstation` machine, they perform tasks on other systems in the course environment. Many course environments, including OpenStack and OpenShift, use a command-line interface (CLI) invoked from the `workstation` machine to communicate with server systems using API calls. Because script actions typically distribute tasks to multiple systems, additional troubleshooting is necessary to determine where a failed task occurred. Log in to those other systems and use Linux diagnostic skills to read local system log files and determine the root cause of the lab script failure.

Using Chromium as an Alternative to Firefox

The **workstation** machine runs Red Hat Enterprise Linux 8 (RHEL 8). If you have issues with rendering any web pages, the EPEL repository is enabled on the **workstation** machine, so you can install the Chromium web browser. If necessary, execute the `sudo yum install chromium` command to install Chromium.

Chapter 1

Introducing Container Technology

Goal

Describe how applications run in containers orchestrated by Red Hat OpenShift Container Platform.

Objectives

- Describe the difference between container applications and traditional deployments.
- Describe the basics of container architecture.
- Describe the benefits of orchestrating applications and OpenShift Container Platform.

Sections

- Overview of Container Technology (and Quiz)
- Overview of Container Architecture (and Quiz)
- Overview of Kubernetes and OpenShift (and Quiz)

Overview of Container Technology

Objectives

After completing this section, students should be able to describe the difference between containerized applications and traditional deployments.

Containerized Applications

Software applications typically depend on other libraries, configuration files, or services that are provided by the runtime environment. The traditional runtime environment for a software application is a physical host or virtual machine, and application dependencies are installed as part of the host.

For example, consider a Python application that requires access to a common shared library that implements the TLS protocol. Traditionally, a system administrator installs the required package that provides the shared library before installing the Python application.

The major drawback to a traditionally deployed software application is that the application's dependencies are closely related to the runtime environment.

An application may break when any updates or patches are applied to the base operating system (OS).

For example, an OS update to the TLS shared library removes TLS 1.0 as a supported protocol. This breaks the deployed Python application because it is written to use the TLS 1.0 protocol for network requests. This forces the system administrator to roll back the OS update to keep the application running, preventing other applications from using the benefits of the updated package.

Therefore, a company developing traditional software applications may require a full set of tests to guarantee that an OS update does not affect applications running on the host.

Furthermore, a traditionally deployed application must be stopped before updating the associated dependencies. To minimize application downtime, organizations design and implement complex systems to provide high availability of their applications. Maintaining multiple applications on a single host often becomes cumbersome, and any deployment or update has the potential to break one of the organization's applications.

Figure 1.1 describes the difference between applications running as containers and applications running on the host operating system.

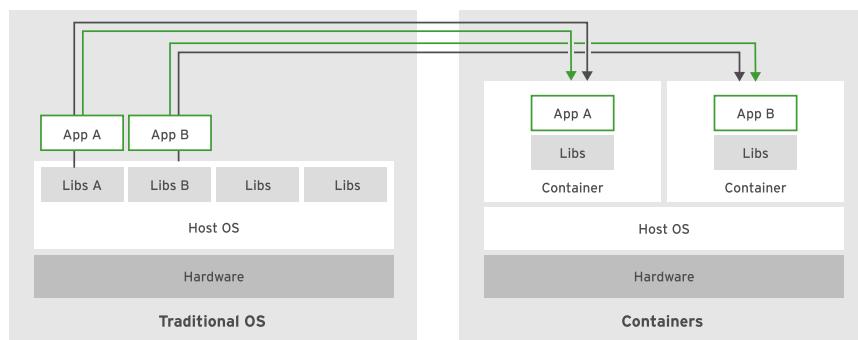


Figure 1.1: Container versus operating system differences

Alternatively, a software application can be deployed using a container.

A container is a set of one or more processes that are isolated from the rest of the system.

Containers provide many of the same benefits as virtual machines, such as security, storage, and network isolation. Containers require far fewer hardware resources and are quick to start and terminate. They also isolate the libraries and the runtime resources (such as CPU and storage) for an application to minimize the impact of any OS update to the host OS, as described in *Figure 1.1*.

The use of containers not only helps with the efficiency, elasticity, and reusability of the hosted applications, but also with application portability. The Open Container Initiative (OCI) provides a set of industry standards that define a container runtime specification and a container image specification. The image specification defines the format for the bundle of files and metadata that form a container image. When you build an application as a container image, which complies with the OCI standard, you can use any OCI-compliant container engine to execute the application.

There are many container engines available to manage and execute individual containers, including Rocket, Drawbridge, LXC, Docker, and Podman. Podman is available in Red Hat Enterprise Linux 7.6 and later, and is used in this course to start, manage, and terminate individual containers.

The following are other major advantages to using containers:

Low hardware footprint

Containers use OS internal features to create an isolated environment where resources are managed using OS facilities such as namespaces and cgroups (control groups). This approach minimizes the amount of CPU and memory overhead compared to a virtual machine hypervisor. Running an application in a VM is a way to create isolation from the running environment, but it requires a heavy layer of services to support the same low hardware footprint isolation provided by containers.

Environment isolation

Containers work in a closed environment where changes made to the host OS or other applications do not affect the container. Because the libraries needed by a container are self-contained, the application can run without disruption. For example, each application can exist in its own container with its own set of libraries. An update made to one container does not affect other containers.

Quick deployment

Containers deploy quickly because there is no need to install the entire underlying operating system. Normally, to support the isolation, a new OS installation is required on a physical host or VM, and any simple update might require a full OS restart. A container restart does not require stopping any services on the host OS.

Multiple environment deployment

In a traditional deployment scenario using a single host, any environment differences could break the application. Using containers, however, all application dependencies and environment settings are encapsulated in the container image.

Reusability

The same container can be reused without the need to set up a full OS. For example, the same database container that provides a production database service can be used by each developer to create a development database during application development. Using containers, there is no longer a need to maintain separate production and development database servers. A single container image is used to create instances of the database service.

Often, a software application with all of its dependent services (databases, messaging, file systems) are made to run in a single container. This can lead to the same problems associated with traditional software deployments to virtual machines or physical hosts. In these instances, a multicontainer deployment may be more suitable.

Furthermore, containers are an ideal approach when using microservices for application development. Each service is encapsulated in a lightweight and reliable container environment that can be deployed to a production or development environment. The collection of containerized services required by an application can be hosted on a single machine, removing the need to manage a machine for each service.

In contrast, many applications are not well suited for a containerized environment. For example, applications accessing low-level hardware information, such as memory, file systems, and devices might be unreliable due to container limitations.



References

Home - Open Containers Initiative

<https://www.opencontainers.org/>

► Quiz

Overview of Container Technology

Choose the correct answers to the following questions:

- ▶ 1. **Which two options are examples of software applications that might run in a container? (Choose two.)**
 - a. A database-driven Python application accessing services such as a MySQL database, a file transfer protocol (FTP) server, and a web server on a single physical host.
 - b. A Java Enterprise Edition application with an Oracle database, and a message broker running on a single VM.
 - c. An I/O monitoring tool responsible for analyzing the traffic and block data transfer.
 - d. A memory dump application tool capable of taking snapshots from all the memory CPU caches for debugging purposes.
- ▶ 2. **Which two of the following use cases are best suited for containers? (Choose two.)**
 - a. A software provider needs to distribute software that can be reused by other companies in a fast and error-free way.
 - b. A company is deploying applications on a physical host and would like to improve its performance by using containers.
 - c. Developers at a company need a disposable environment that mimics the production environment so that they can quickly test the code they develop.
 - d. A financial company is implementing a CPU-intensive risk analysis tool on their own containers to minimize the number of processors needed.
- ▶ 3. **A company is migrating their PHP and Python applications running on the same host to a new architecture. Due to internal policies, both are using a set of custom made shared libraries from the OS, but the latest update applied to them as a result of a Python development team request broke the PHP application. Which two architectures would provide the best support for both applications? (Choose two.)**
 - a. Deploy each application to different VMs and apply the custom-made shared libraries individually to each VM host.
 - b. Deploy each application to different containers and apply the custom-made shared libraries individually to each container.
 - c. Deploy each application to different VMs and apply the custom-made shared libraries to all VM hosts.
 - d. Deploy each application to different containers and apply the custom-made shared libraries to all containers.

► 4. Which three kinds of applications can be packaged as containers for immediate consumption? (Choose three.)

- a. A virtual machine hypervisor
- b. A blog software, such as WordPress
- c. A database
- d. A local file system recovery tool
- e. A web server

► Solution

Overview of Container Technology

Choose the correct answers to the following questions:

- ▶ 1. **Which two options are examples of software applications that might run in a container? (Choose two.)**
 - a. A database-driven Python application accessing services such as a MySQL database, a file transfer protocol (FTP) server, and a web server on a single physical host.
 - b. A Java Enterprise Edition application with an Oracle database, and a message broker running on a single VM.
 - c. An I/O monitoring tool responsible for analyzing the traffic and block data transfer.
 - d. A memory dump application tool capable of taking snapshots from all the memory CPU caches for debugging purposes.
- ▶ 2. **Which two of the following use cases are best suited for containers? (Choose two.)**
 - a. A software provider needs to distribute software that can be reused by other companies in a fast and error-free way.
 - b. A company is deploying applications on a physical host and would like to improve its performance by using containers.
 - c. Developers at a company need a disposable environment that mimics the production environment so that they can quickly test the code they develop.
 - d. A financial company is implementing a CPU-intensive risk analysis tool on their own containers to minimize the number of processors needed.
- ▶ 3. **A company is migrating their PHP and Python applications running on the same host to a new architecture. Due to internal policies, both are using a set of custom made shared libraries from the OS, but the latest update applied to them as a result of a Python development team request broke the PHP application. Which two architectures would provide the best support for both applications? (Choose two.)**
 - a. Deploy each application to different VMs and apply the custom-made shared libraries individually to each VM host.
 - b. Deploy each application to different containers and apply the custom-made shared libraries individually to each container.
 - c. Deploy each application to different VMs and apply the custom-made shared libraries to all VM hosts.
 - d. Deploy each application to different containers and apply the custom-made shared libraries to all containers.

► 4. Which three kinds of applications can be packaged as containers for immediate consumption? (Choose three.)

- a. A virtual machine hypervisor
- b. A blog software, such as WordPress
- c. A database
- d. A local file system recovery tool
- e. A web server

Overview of Container Architecture

Objectives

After completing this section, you should be able to:

- Describe the architecture of Linux containers.
- Describe the podman tool for the managing of containers.

Introducing Container History

Containers have quickly gained popularity in recent years. However, the technology behind containers has been around for a relatively long time. In 2001, Linux introduced a project named VServer. VServer was the first attempt at running complete sets of processes inside a single server with a high degree of isolation.

From VServer, the idea of isolated processes further evolved and became formalized around the following features of the Linux kernel:

Namespaces

A namespace isolates specific system resources usually visible to all processes. Inside a namespace, only processes that are members of that namespace can see those resources. Namespaces can include resources like network interfaces, the process ID list, mount points, IPC resources, and the system's host name information.

Control groups (cgroups)

Control groups partition sets of processes and their children into groups to manage and limit the resources they consume. Control groups place restrictions on the amount of system resources processes might use. Those restrictions keep one process from using too many resources on the host.

Seccomp

Developed in 2005 and introduced to containers circa 2014, Seccomp limits how processes could use system calls. Seccomp defines a security profile for processes that lists the system calls, parameters and file descriptors they are allowed to use.

SELinux

Security-Enhanced Linux (SELinux) is a mandatory access control system for processes. Linux kernel uses SELinux to protect processes from each other and to protect the host system from its running processes. Processes run as a confined SELinux type that has limited access to host system resources.

All of these innovations and features focus on a basic concept: enabling processes to run isolated while still accessing system resources. This concept is the foundation of container technology and the basis for all container implementations. Nowadays, containers are processes in the Linux kernel making use of those security features to create an isolated environment. This environment forbids isolated processes from misusing system or other container resources.

A common use case of containers is having several replicas of the same service (for example, a database server) in the same host. Each replica has isolated resources (file system, ports, memory), so there is no need for the service to handle resource sharing. Isolation guarantees that

a malfunctioning or harmful service does not impact other services or containers in the same host, nor in the underlying system.

Describing Linux Container Architecture

From the Linux kernel perspective, a container is a process with restrictions. However, instead of running a single binary file, a container runs an image. An image is a file-system bundle that contains all dependencies required to execute a process: files in the file system, installed packages, available resources, running processes, and kernel modules.

Like executable files are the foundation for running processes, images are the foundation for running containers. Running containers use an immutable view of the image, allowing multiple containers to reuse the same image simultaneously. As images are files, they can be managed by versioning systems, improving automation on container and image provisioning.

Container images need to be locally available for the container runtime to execute them, but the images are usually stored and maintained in an image repository. An image repository is just a service - public or private - where images can be stored, searched, and retrieved. Other features provided by image repositories are remote access, image metadata, authorization, or image version control.

There are many different image repositories available, each one offering different features:

- Red Hat Container Catalog [<https://registry.redhat.io/>]
- Red Hat Quay [<https://quay.io/>]
- Docker Hub [<https://hub.docker.com/>]
- Google Container Registry [<https://cloud.google.com/container-registry/>]
- Amazon Elastic Container Registry [<https://aws.amazon.com/ecr/>]



Note

This course uses the public image registry Quay, so students can operate with images without worrying about interfering with each other.

Managing Containers with Podman

Containers, images, and image registries need to be able to interact with each other. For example, you need to be able to build images and put them into image registries. You also need to be able to retrieve an image from the image registry and build a container from that image.

Podman is an open source tool for managing containers, container images and interacting with image registries. It offers the following key features:

- It uses image format specified by the Open Container Initiative [<https://www.opencontainers.org/>] (OCI). Those specifications define a standard, community-driven, non-proprietary image format.
- Podman stores local images in local file-system. Doing so avoids unnecessary client/server architecture or having daemons running on local machine.
- Podman follows the same command patterns as the Docker CLI, so there is no need to learn a new toolset.
- Podman is compatible with Kubernetes. Kubernetes can use Podman to manage its containers.



References

Red Hat Quay Container Registry

<https://quay.io/>

Podman site

<https://podman.io/>

Open Container Initiative

<https://www.opencontainers.org/>

► Quiz

Overview of Container Architecture

Choose the correct answers to the following questions:

- ▶ 1. **Which three of the following Linux features are used for running containers? (Choose three.)**
 - a. Namespaces
 - b. Integrity Management
 - c. Security-Enhanced Linux
 - d. Control Groups

- ▶ 2. **Which of the following best describes a container image?**
 - a. A virtual machine image from which a container is created.
 - b. A file-system bundle that contains all dependencies required to execute the process inside the container.
 - c. A runtime environment where an application will run.
 - d. The container's index file used by a registry.

- ▶ 3. **Which three of the following components are common across container architecture implementations? (Choose three.)**
 - a. Container runtime
 - b. Container permissions
 - c. Container images
 - d. Container registries

- ▶ 4. **What is a container in relation to the Linux kernel?**
 - a. A virtual machine.
 - b. An isolated process with regulated resource access.
 - c. A set of file-system layers exposed by UnionFS.
 - d. An external service providing container images.

- ▶ 5. **Which of the following are Podman features (Choose two.)**
 - a. Manage operating system configuration and permissions to execute virtual machines.
 - b. Manage containers, container images and interact with registries.
 - c. Execute a daemon on the local machine to run containers.
 - d. Podman uses the same command patterns as Docker.

► Solution

Overview of Container Architecture

Choose the correct answers to the following questions:

- ▶ 1. **Which three of the following Linux features are used for running containers? (Choose three.)**
 - a. Namespaces
 - b. Integrity Management
 - c. Security-Enhanced Linux
 - d. Control Groups
- ▶ 2. **Which of the following best describes a container image?**
 - a. A virtual machine image from which a container is created.
 - b. A file-system bundle that contains all dependencies required to execute the process inside the container.
 - c. A runtime environment where an application will run.
 - d. The container's index file used by a registry.
- ▶ 3. **Which three of the following components are common across container architecture implementations? (Choose three.)**
 - a. Container runtime
 - b. Container permissions
 - c. Container images
 - d. Container registries
- ▶ 4. **What is a container in relation to the Linux kernel?**
 - a. A virtual machine.
 - b. An isolated process with regulated resource access.
 - c. A set of file-system layers exposed by UnionFS.
 - d. An external service providing container images.
- ▶ 5. **Which of the following are Podman features (Choose two.)**
 - a. Manage operating system configuration and permissions to execute virtual machines.
 - b. Manage containers, container images and interact with registries.
 - c. Execute a daemon on the local machine to run containers.
 - d. Podman uses the same command patterns as Docker.

Overview of Kubernetes and OpenShift

Objectives

After completing this section, students should be able to:

- Identify the limitations of Linux containers and the need for container orchestration.
- Describe the Kubernetes container orchestration tool.
- Describe Red Hat OpenShift Container Platform (RHOC).

Limitations of Containers

Containers provide an easy way to package and run services. As the number of containers managed by an organization grows, the work of manually starting them rises exponentially along with the need to quickly respond to external demands.

When using containers in a production environment, enterprises often require:

- Easy communication between a large number of services.
- Resource limits on applications regardless of the number of containers running them.
- Responses to application usage spikes to increase or decrease running containers.
- Reaction to service deterioration.
- Gradual roll-out of new release to a set of users.

Enterprises often require a container orchestration technology because container runtimes (such as Podman) do not adequately address the above requirements.

Kubernetes Overview

Kubernetes is an orchestration service that simplifies the deployment, management, and scaling of containerized applications.

The smallest unit manageable in Kubernetes is a pod. A pod consists of one or more containers with their storage resources and IP address that represent a single application. Kubernetes also uses pods to orchestrate the containers inside it and to limit its resources as a single unit.

Kubernetes Features

Kubernetes offers the following features on top of a container infrastructure:

Service discovery and load balancing

Kubernetes enables inter-service communication by assigning a single DNS entry to each set of containers. This way, the requesting service only needs to know the target's DNS name, allowing the cluster to change the container's location and IP address, leaving the service unaffected. This permits load-balancing the request across the pool of containers providing the service. For example, Kubernetes can evenly split incoming requests to a MySQL service taking into account the availability of the pods.

Horizontal scaling

Applications can scale up and down manually or automatically with a configuration set, with either the Kubernetes command-line interface or the web UI.

Self-healing

Kubernetes can use user-defined health checks to monitor pods to restart and reschedule them in case of failure.

Automated rollout

Kubernetes can gradually roll updates out to your application's containers while checking their status. If something goes wrong during the rollout, Kubernetes can roll back to the previous iteration of the deployment.

Secrets and configuration management

You can manage the configuration settings and secrets of your applications without rebuilding containers. Application secrets can be user names, passwords, and service endpoints, or any configuration setting that must be kept private.

Operators

Operators are packaged Kubernetes applications that also bring the knowledge of the application's lifecycle into the Kubernetes cluster. Applications packaged as Operators use the Kubernetes API to update the cluster's state reacting to changes in the application state.

OpenShift Overview

Red Hat OpenShift Container Platform (RHOCP) is a set of modular components and services built on top of a Kubernetes container infrastructure. RHOCP adds the capabilities to provide a production PaaS platform such as remote management, multitenancy, increased security, monitoring and auditing, application life-cycle management, and self-service interfaces for developers.

Beginning with Red Hat OpenShift v4, hosts in an OpenShift cluster all use Red Hat Enterprise Linux CoreOS as the underlying operating system.

**Note**

Throughout this course, the terms RHOCP and OpenShift are used to refer to the Red Hat OpenShift Container Platform.

OpenShift Features

OpenShift adds the following features to a Kubernetes cluster:

Integrated developer workflow

RHOCP integrates a built-in container registry, CI/CD pipelines, and S2I, a tool to build artifacts from source repositories to container images.

Routes

Easily expose services to the outside world.

Metrics and logging

Include built-in and self-analyzing metrics service and aggregated logging.

Unified UI

OpenShift brings unified tools and a UI to manage all the different capabilities.



References

Production-Grade Container Orchestration - Kubernetes

<https://kubernetes.io/>

OpenShift: Container Application Platform by Red Hat, Built on Containers and Kubernetes

<https://www.openshift.com/>

► Quiz

Describing Kubernetes and OpenShift

Choose the correct answers to the following questions:

- ▶ 1. **Which three of the following statements are correct regarding container limitations? (Choose three.)**
 - a. Containers are easily orchestrated in large numbers.
 - b. Lack of automation increases response time to problems.
 - c. Containers do not manage internal application failures.
 - d. Containers are not load-balanced.
 - e. Containers are heavily-isolated, packaged applications.
- ▶ 2. **Which two of the following statements are correct regarding Kubernetes? (Choose two.)**
 - a. Kubernetes is a container.
 - b. Kubernetes can only use Docker containers.
 - c. Kubernetes is a container orchestration system.
 - d. Kubernetes simplifies management, deployment, and scaling of containerized applications.
 - e. Applications managed in a Kubernetes cluster are harder to maintain.
- ▶ 3. **Which three of the following statements are true regarding Red Hat OpenShift v4? (Choose three.)**
 - a. OpenShift provides additional features to a Kubernetes infrastructure.
 - b. Kubernetes and OpenShift are mutually exclusive.
 - c. OpenShift hosts use Red Hat Enterprise Linux as the base operating system.
 - d. OpenShift simplifies development incorporating a Source-to-Image technology and CI/CD pipelines.
 - e. OpenShift simplifies routing and load balancing.
- ▶ 4. **What features does OpenShift offer that extend Kubernetes capabilities? (Choose two.)**
 - a. Operators and the Operator Framework.
 - b. Routes to expose services to the outside world.
 - c. An integrated development workflow.
 - d. Self-healing and health checks.

► Solution

Describing Kubernetes and OpenShift

Choose the correct answers to the following questions:

- ▶ 1. **Which three of the following statements are correct regarding container limitations? (Choose three.)**
 - a. Containers are easily orchestrated in large numbers.
 - b. Lack of automation increases response time to problems.
 - c. Containers do not manage internal application failures.
 - d. Containers are not load-balanced.
 - e. Containers are heavily-isolated, packaged applications.
- ▶ 2. **Which two of the following statements are correct regarding Kubernetes? (Choose two.)**
 - a. Kubernetes is a container.
 - b. Kubernetes can only use Docker containers.
 - c. Kubernetes is a container orchestration system.
 - d. Kubernetes simplifies management, deployment, and scaling of containerized applications.
 - e. Applications managed in a Kubernetes cluster are harder to maintain.
- ▶ 3. **Which three of the following statements are true regarding Red Hat OpenShift v4? (Choose three.)**
 - a. OpenShift provides additional features to a Kubernetes infrastructure.
 - b. Kubernetes and OpenShift are mutually exclusive.
 - c. OpenShift hosts use Red Hat Enterprise Linux as the base operating system.
 - d. OpenShift simplifies development incorporating a Source-to-Image technology and CI/CD pipelines.
 - e. OpenShift simplifies routing and load balancing.
- ▶ 4. **What features does OpenShift offer that extend Kubernetes capabilities? (Choose two.)**
 - a. Operators and the Operator Framework.
 - b. Routes to expose services to the outside world.
 - c. An integrated development workflow.
 - d. Self-healing and health checks.

► Guided Exercise

Configuring the Classroom Environment

In this exercise, you will configure the workstation to access all infrastructure used by this course.

Outcomes

You should be able to:

- Configure the workstation machine to access an OpenShift cluster, a container image registry, and a Git repository used throughout the course.
- Fork this course's sample applications repository to your personal GitHub account.
- Clone this course's sample applications repository from your personal GitHub account to the workstation machine.

Before You Begin

To perform this exercise, ensure you have:

- Access to the DO180 course in the Red Hat Training's Online Learning Environment.
- The connection parameters and a developer user account to access the OpenShift cluster provided in your classroom environment.
- A personal, free GitHub account. If you need to register to GitHub, see the instructions in *Appendix B, Creating a GitHub Account*.
- A personal, free Quay.io account. If you need to register to Quay.io, see the instructions in *Appendix C, Creating a Quay Account*.
- A personal, GitHub access token.

Instructions

Before starting any exercise, ensure you have:

► 1. Prepare your GitHub access token.

- 1.1. Navigate to <https://github.com> using a web browser and authenticate.
- 1.2. On the top of the page, click your profile icon, select the **Settings** menu

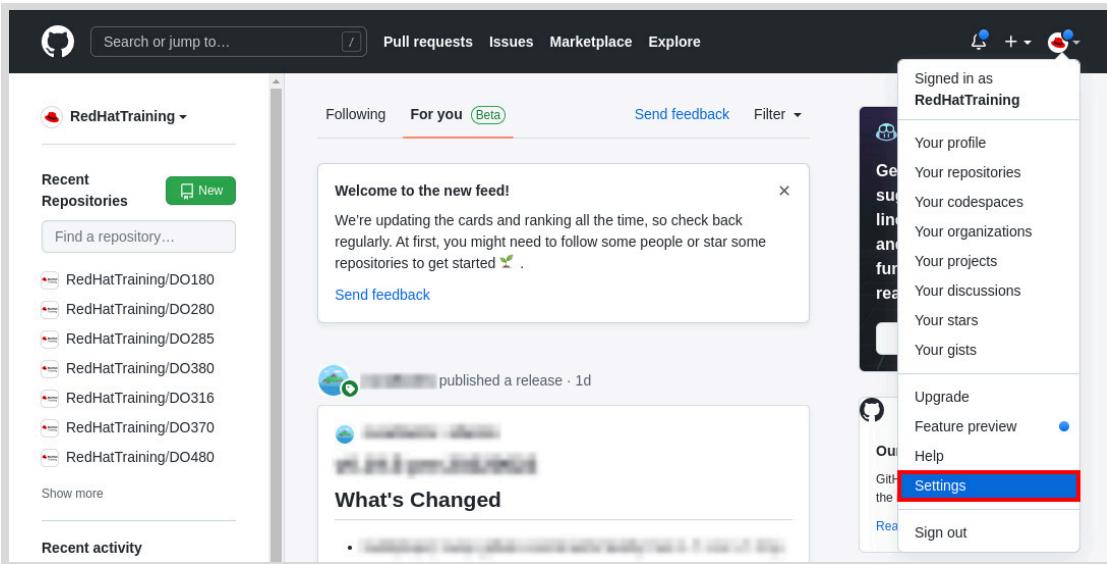


Figure 1.2: User menu

Select **Developer settings** in the left pane of the page.

A screenshot of the GitHub developer settings page. The left sidebar lists various settings categories: Profile, Account, Appearance (with a 'New' badge), Account security, Billing & plans, Security log, Security & analysis, Emails, Notifications, SSH and GPG keys, Repositories, Packages, Organizations, Saved replies, Applications, and Developer settings. The 'Developer settings' option is highlighted with a red box. The main right pane contains fields for Name, Public email, Bio, URL, Twitter username, and Company, each with descriptive placeholder text.

Figure 1.3: Developer settings

- 1.3. Select the Personal access token section on the left pane. On the next page, create your new token by clicking **Generate new token**, you are then prompted to enter your password.

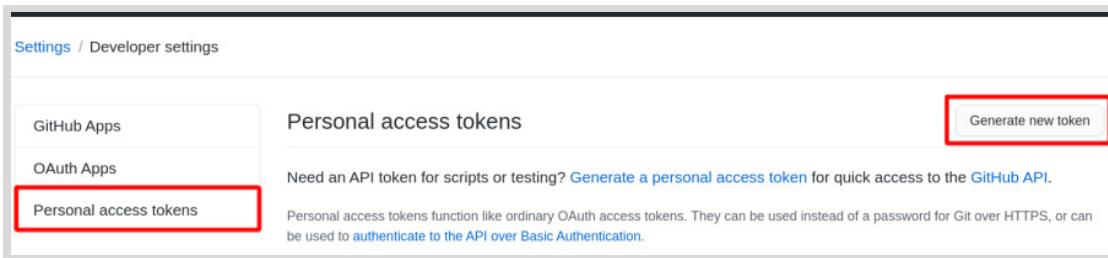


Figure 1.4: Personal access token pane

- 1.4. Write a short description of your new access token on the **Note** field.
- 1.5. Select the **public_repo** option and leave the other options unchecked. Create your new access token by clicking **Generate token**.

The screenshot shows the 'New personal access token' configuration page. It includes a note about the function of personal access tokens, a 'Note' field containing 'Course DO180', and a 'Select scopes' section. In the 'Select scopes' section, the 'public_repo' checkbox is checked and highlighted with a red box.

Scope	Description
<input type="checkbox"/> repo	Full control of private repositories
<input type="checkbox"/> repo:status	Access commit status
<input type="checkbox"/> repo_deployment	Access deployment status
<input checked="" type="checkbox"/> public_repo	Access public repositories
<input type="checkbox"/> repo:invite	Access repository invitations
<input type="checkbox"/> security_events	Read and write security events

Figure 1.5: Personal access token configuration

- 1.6. Your new personal access token is displayed in the output. Using your preferred text editor, create a new file in student's home directory named `token` and ensure you paste in your generated personal access token. The personal access token can not be displayed again in GitHub.

The screenshot shows the GitHub 'Personal access tokens' page. At the top, there are buttons for 'Generate new token' and 'Revoke all'. Below that, a message says 'Tokens you have generated that can be used to access the [GitHub API](#)'. A note below says 'Make sure to copy your new personal access token now. You won't be able to see it again!'. A red box highlights a generated token: '✓ ghp_kgYGzWcGE1CrdovkzuzeLTWvYY6eBX2l0vCK' with a copy icon. To the right is a 'Delete' button. At the bottom, a note states: 'Personal access tokens function like ordinary OAuth access tokens. They can be used instead of a password for Git over HTTPS, or can be used to [authenticate to the API](#) over Basic Authentication'.

Figure 1.6: Generated access token

- 1.7. On workstation execute the `git config` command with the `credential.helper cache` parameters to store in cache memory your credentials for future use. The `--global` parameter applies the configuration to all of your repositories.

```
[student@workstation ~]$ git config --global credential.helper cache
```

**Note**

The default timeout is 900 seconds, you can specify a different timeout if needed.

```
[student@workstation ~]$ git config --global credential.helper \
  'cache --timeout=3600'
```

**Important**

During this course, if you are prompted for a password while using Git operations on the command line, use your access token as the password.

- 2. Prepare your Quay.io password.

- 2.1. Configure a password for your Quay.io account. On the *Account Settings* page, click the *Change password* link. See *Appendix C, Creating a Quay Account* for further details.

- 3. Configure the **workstation** machine.

Open a terminal on the **workstation** machine and execute the following command.

```
[student@workstation ~]$ lab-configure
```

Answer the interactive prompts before starting any other exercise in this course.

**Note**

If you make a mistake, you can interrupt the command at any time using **Ctrl+C** and start over adding the **-d** option.

```
[student@workstation ~]$ lab-configure -d
```

- 3.1. The **lab-configure** command starts by displaying a series of interactive prompts and uses sensible defaults when they are available.

```
[student@workstation ~]$ lab-configure
```

- Enter the GitHub account name: **yourgituser** ①
Verifying GitHub account name: **yourgituser**
 - Enter the Quay.io account name: **yourquayuser** ②
Verifying Quay.io account name: **yourquayuser**
- ...output omitted...

① ② Your personal GitHub and Quay.io account names. You need valid, free accounts on these online services to perform this course's exercises. If you have never used any of these online services, refer to *Appendix B, Creating a GitHub Account* and *Appendix C, Creating a Quay Account* for instructions about how to register.

- 3.2. If **lab-configure** finds any issues, it displays an error message and exits. You must verify your information and run the **lab-configure -d** command again. The following listing shows an example of a verification error.

- Enter the Quay.io account name: **notexists**
Verifying Quay.io account name: **notexists**
ERROR: Cannot find Quay.io account user 'notexists'
- To reconfigure, run: **lab-configure -d**

- 3.3. Finally, the **lab-configure** command verifies that the **developer** user can log in to your OpenShift cluster.

...output omitted...

- . Ensuring user 'developer' can log in to the OpenShift cluster.
- ...output omitted...

- 3.4. If all checks pass, the **lab-configure** command saves your configuration:

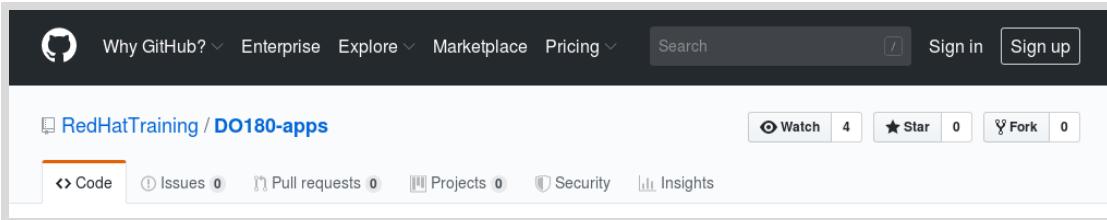
- 3.5. If there are no errors saving your configuration, you are almost ready to start any of this course's exercises. If there were any errors, do not try to start any exercise until you can execute the **lab-configure** command successfully.

- 4. Fork this course's sample applications into your personal GitHub account. Perform the following steps:

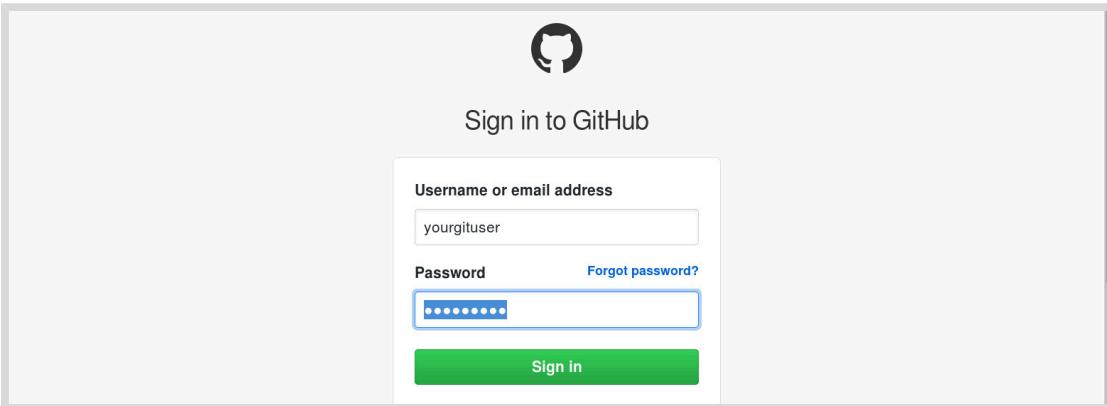
- 4.1. Open a web browser and navigate to the DO180-apps GitHub repository.

- <https://github.com/RedHatTraining/DO180-apps>

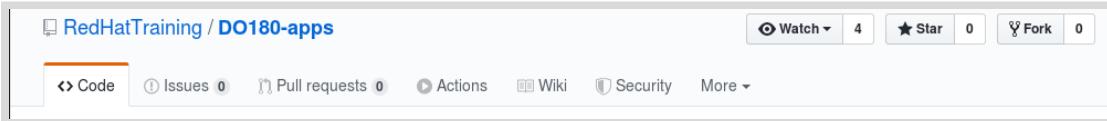
If you are not logged in to GitHub, click **Sign in** in the upper-right corner.



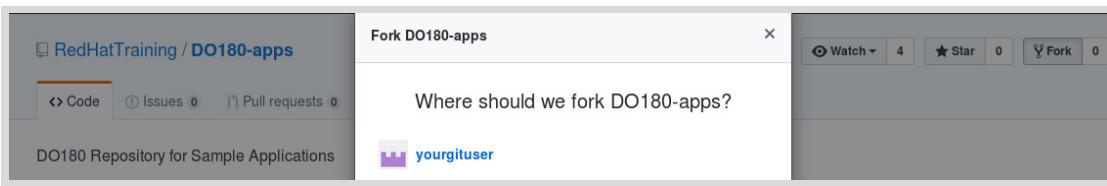
- 4.2. Log in to GitHub using your personal user name and password.



- 4.3. Navigate to the RedHatTraining/D0180-apps repository and click **Fork** in the top right corner.



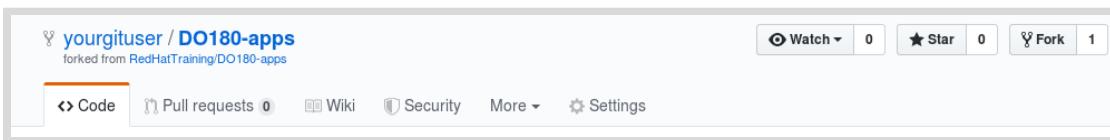
- 4.4. In the **Fork D0180-apps** window, click **yourgituser** to select your personal GitHub project.



Important

While it is possible to rename your personal fork of the <https://github.com/RedHatTraining/DO180-apps> repository, grading scripts, helper scripts, and the example output in this course assume that you retain the name **D0180-apps** when your fork the repository.

- 4.5. After a few minutes, the GitHub web interface displays your new repository `yourgituser/DO180-apps`.



- ▶ 5. Clone this course's sample applications from your personal GitHub account to your workstation machine. Perform the following steps:

- 5.1. Run the following command to clone this course's sample applications repository. Replace `yourgituser` with the name of your personal GitHub account.

```
[student@workstation ~]$ git clone https://github.com/yourgituser/DO180-apps
Cloning into 'DO180-apps'...
...output omitted...
```

- 5.2. Verify that `/home/student/DO180-apps` is a Git repository.

```
[student@workstation ~]$ cd DO180-apps
[student@workstation DO180-apps]$ git status
# On branch master
nothing to commit, working directory clean
```

- 5.3. Create a new branch to test your new personal access token.

```
[student@workstation DO180-apps]$ git checkout -b testbranch
Switched to a new branch testbranch
```

- 5.4. Make a change to the TEST file and then commit it to Git.

```
[student@workstation DO180-apps]$ echo "DO180" > TEST
[student@workstation DO180-apps]$ git add .
[student@workstation DO180-apps]$ git commit -m "DO180"
...output omitted...
```

- 5.5. Push the changes to your recently created testing branch.

```
[student@workstation DO180-apps]$ git push --set-upstream origin testbranch
Username for https://github.com: ①
Password for https://yourgituser@github.com: ②
...output omitted...
```

- ① Enter your GitHub username,
- ② Enter your personal access token.

- 5.6. Make other change to a text file, commit it and push it. You will notice you are no longer asked to put your user and password. This is because the `git config` command you ran in step 1.7.

```
[student@workstation D0180-apps]$ echo "OCP4" > TEST  
[student@workstation D0180-apps]$ git add .  
[student@workstation D0180-apps]$ git commit -m "OCP4"  
[student@workstation D0180-apps]$ git push  
...output omitted...
```

- 5.7. Verify that /home/student/D0180-apps contains this course's sample applications, and change back to the user's home folder.

```
[student@workstation D0180-apps]$ head README.md  
# D0180-apps  
...output omitted...  
  
[student@workstation D0180-apps]$ cd ~  
[student@workstation ~]$
```

Finish

Now that you have a local clone of the D0180-apps repository on the workstation machine, and you have executed the `lab-configure` command successfully, you are ready to start this course's exercises.

During this course, all exercises that build applications from source start from the `master` branch of the D0180-apps Git repository. Exercises that make changes to source code require you to create new branches to host your changes so that the `master` branch always contains a known good starting point. If for some reason you need to pause or restart an exercise and need to either save or discard changes you make into your Git branches, refer to *Appendix E, Useful Git Commands*.

This concludes the guided exercise.

Summary

In this chapter, you learned:

- Containers are isolated application runtimes, created with very little overhead.
- A container image packages an application with all of its dependencies, making it easier to run the application in different environments.
- Applications such as Podman create containers using features of the standard Linux kernel.
- Container image registries are the preferred mechanism for distributing container images to multiple users and hosts.
- OpenShift orchestrates applications composed of multiple containers using Kubernetes.
- Kubernetes manages load balancing, high availability, and persistent storage for containerized applications.
- OpenShift adds to Kubernetes multitenancy, security, ease of use, and continuous integration and continuous development features.
- OpenShift routes enable external access to containerized applications in a manageable way.

Chapter 2

Creating Containerized Services

Goal

Provision a service using container technology.

Objectives

- Create a database server from a container image.

Sections

- Provisioning a Containerized Database Server (and Guided Exercise)
- Using Rootless Containers (and Guided Exercise)

Lab

- Creating Containerized Services

Provisioning Containerized Services

Objectives

After completing this section, students should be able to:

- Search for and fetch container images with Podman.
- Run and configure containers locally.
- Use the Red Hat Container Catalog.

Fetching Container Images with Podman

Applications can run inside containers, providing an isolated and controlled execution environment. Running a containerized application, that is, running an application inside a container, requires a container image and a file system bundle that provides all the application files, libraries, and dependencies that the application needs to run. Container images are available from image registries that allow users to search and retrieve container images. Podman users can use the `search` subcommand to find available images from remote or local registries.

```
[user@demo ~]$ podman search rhel
INDEX      NAME          DESCRIPTION STARS OFFICIAL AUTOMATED
redhat.com registry.access.redhat.com/rhel This plat... 0
...output omitted...
```

After finding an image, you can use Podman to download it. Use the `pull` subcommand to direct Podman to fetch the image and save it locally for future use.

```
[user@demo ~]$ podman pull rhel
Trying to pull registry.access.redhat.com/rhel...
Getting image source signatures
Copying blob sha256: ...output omitted...
  72.25 MB / 72.25 MB [=====] 8s
Copying blob sha256: ...output omitted...
  1.20 KB / 1.20 KB [=====] 0s
Copying config sha256: ...output omitted...
  6.30 KB / 6.30 KB [=====] 0s
Writing manifest to image destination
Storing signatures
699d44bc6ea2b9fb23e7899bd4023d3c83894d3be64b12e65a3fe63e2c70f0ef
```

Container images are named based on the following syntax:

```
registry-name/user-name/image-name:tag
```

Registry Naming syntax:

- The `registry-name` is the name of the registry storing the image. It is usually the FQDN of the registry.

- The `user-name` is the name of the user or organization to which the image belongs.
- The `image-name` must be unique in user namespace.
- The `tag` identifies the image version. If the image name includes no image tag, `latest` is assumed.



Note

This classroom's Podman installation uses several publicly available registries, like Quay.io and Red Hat Container Catalog.

After retrieval, Podman stores images locally and you can list them with the `images` subcommand:

```
[user@demo ~]$ podman images
REPOSITORY                      TAG      IMAGE ID      CREATED        SIZE
registry.access.redhat.com/rhel   latest   699d44bc6ea2  4 days ago   214MB
...output omitted...
```

Running Containers

The `podman run` command runs a container locally based on an image. At a minimum, the command requires the name of the image to execute in the container.

The container image specifies a process that starts inside the container known as the entry point. The `podman run` command uses all parameters after the image name as the entry point command for the container. The following example starts a container from a Red Hat Universal Base Image. It sets the entry point for this container to the `echo "Hello world"` command:

```
[user@demo ~]$ podman run ubi8/ubi:8.3 echo 'Hello world!'
Hello world!
```

To start a container image as a background process, pass the `-d` option to the `podman run` command:

```
[user@demo ~]$ podman run -d -p 8080 registry.redhat.io/rhel8/httpd-24
ff4ec6d74e9b2a7b55c49f138e56f8bc46fe2a09c23093664fea7febcb3dfa1b2
[user@demo ~]$ podman port -l
8080/tcp -> 0.0.0.0:44389
[user@demo ~]$ curl http://0.0.0.0:44389
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
...output omitted...
```

This example runs a containerized Apache HTTP server in the background. It uses the `-p 8080` option to bind HTTP server's port to a local port. Then, it uses the `podman port` command to retrieve the local port on which the container listens. Finally, it uses this port to create the target URL and fetch the root page from the Apache HTTP server. This response proves the container is still up and running after the `podman run` command.

**Note**

Most Podman subcommands accept the `-l` flag (`l` for latest) as a replacement for the container id. This flag applies the command to the latest used container in any Podman command.

**Note**

If the image to be executed is not available locally when using the `podman run` command, Podman automatically uses `pull` to download the image.

When referencing the container, Podman recognizes a container either with the container name or the generated container id. Use the `--name` option to set the container name when running the container with Podman. Container names must be unique. If the `podman run` command includes no container name, Podman generates a unique random one for you.

If the images require that the user interact with the console, then Podman can redirect container input and output streams to the console. The `run` subcommand requires the `-t` and `-i` flags (or the `-it` flag) to enable interactivity.

**Note**

Many Podman flags also have an alternative long form; some of these are explained below:

- `-t` is equivalent to `--tty`, meaning a `pseudo-tty` (pseudo-terminal) is to be allocated for the container.
- `-i` is the same as `--interactive`. When used, standard input is kept open into the container.
- `-d`, or its long form `--detach`, means the container runs in the background (detached). Podman then prints the container id.

See the Podman documentation for the complete list of flags.

The following example starts a Bash terminal *inside* the container, and interactively runs some commands in it:

```
[user@demo ~]$ podman run -it ubi8/ubi:8.3 /bin/bash
bash-4.2# ls
...output omitted...
bash-4.2# whoami
root
bash-4.2# exit
exit
[user@demo ~]$
```

Some containers need or can use external parameters provided at startup. The most common approach for providing and consuming those parameters is through environment variables. Podman can inject environment variables into containers at startup by adding the `-e` flag to the `run` subcommand.

```
[user@demo ~]$ podman run -e GREET=Hello -e NAME=RedHat \
> ubi8/ubi:8.3 printenv GREET NAME
Hello
RedHat
[user@demo ~]$
```

The previous example starts a UBI image container that prints the two environment variables provided as parameters.

Another use case for environment variables is setting up credentials into a MySQL database server.

```
[user@demo ~]$ podman run --name mysql-custom \
> -e MYSQL_USER=redhat -e MYSQL_PASSWORD=r3dh4t \
> -e MYSQL_ROOT_PASSWORD=r3dh4t \
> -d registry.redhat.io/rhel8/mysql-80
```

Using the Red Hat Container Catalog

Red Hat maintains its repository of finely-tuned container images. Using this repository provides customers with a layer of protection and reliability against known vulnerabilities that could potentially be caused by untested images. The standard `podman` command is compatible with the Red Hat Container Catalog. The Red Hat Container Catalog provides a user-friendly interface for searching and exploring container images from the Red Hat repository.

The Container Catalog also serves as a single interface, providing access to different aspects of all the available container images in the repository. It is useful in determining the best image among multiple versions of container images using health index grades. The health index grade indicates how current an image is, and whether it contains the latest security updates.

The Container Catalog also gives access to the errata documentation for an image. It describes the latest bug fixes and enhancements in each update. It also suggests the best technique for pulling an image on each operating system.

The following images highlight some of the features of the Red Hat Container Catalog:

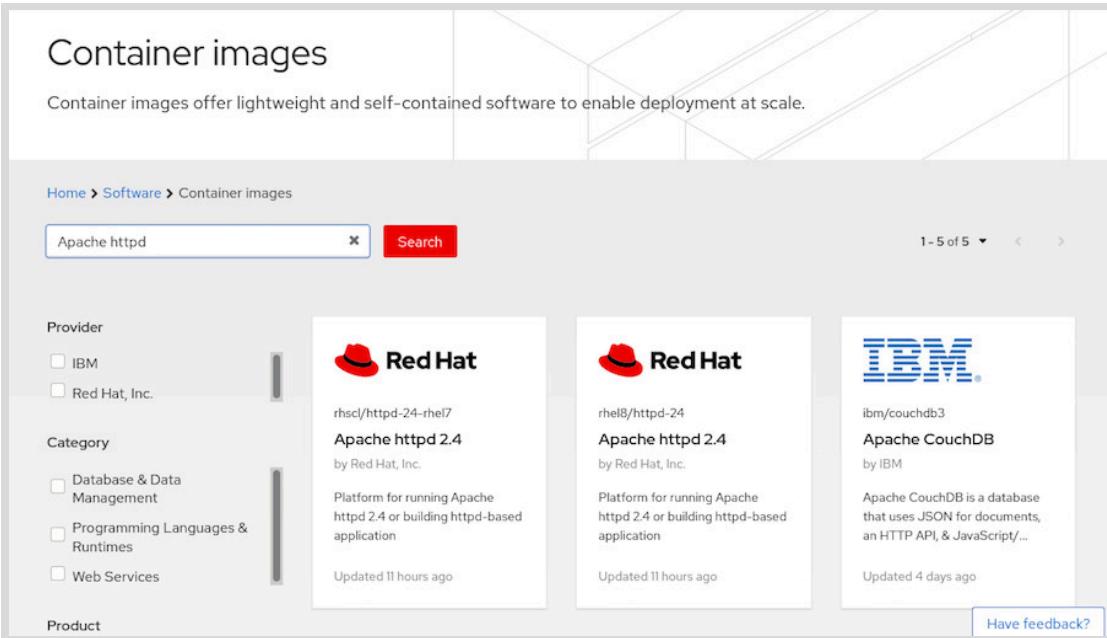


Figure 2.1: Red Hat Container Catalog search page

As displayed in the preceding image, searching for Apache `httpd` in the search box of the Container Catalog displays a suggested list of products and image repositories matching the search pattern. To access the Apache `httpd 2.4` image page, select `rhel8/httpd-24` from the suggested list.

After selecting the desired image, the subsequent page provides additional information about the image:

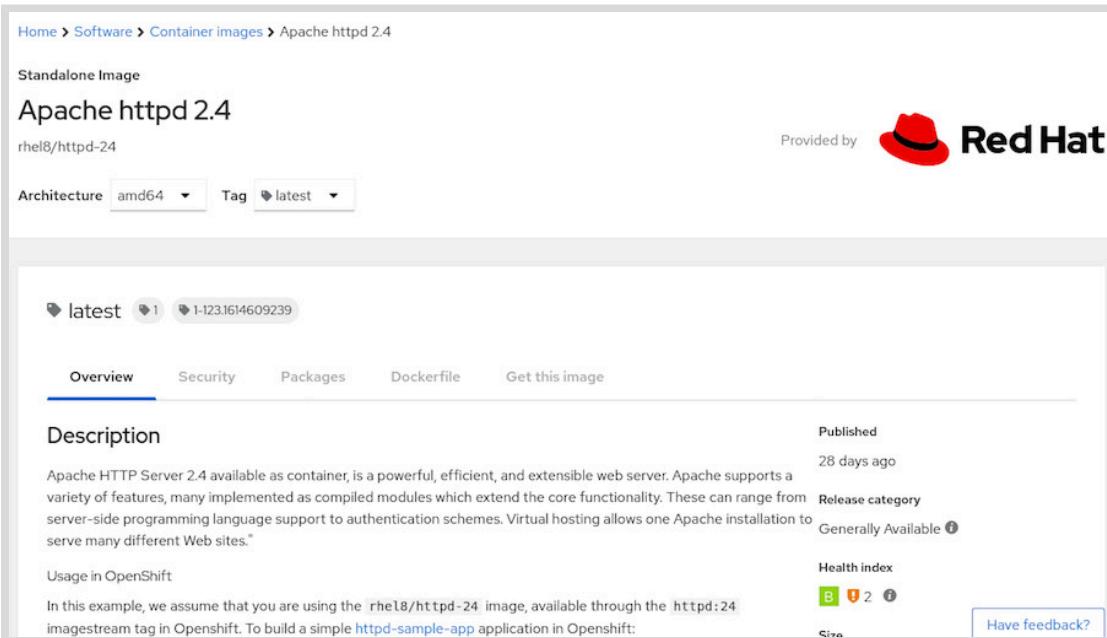


Figure 2.2: Apache httpd 2.4 (rhel8/httpd-24) overview image page

The *Apache httpd 2.4* panel displays image details and several tabs. This page states that Red Hat maintains the image repository.

Under the *Overview* tab, there are other details:

- *Description*: A summary of the image's capabilities.
- *Documentation*: References to container's author documentation.
- *Products using this container*: It indicates that Red Hat Enterprise Linux uses this image repository.

On the right side, it shows information about when the image received its latest update, the latest tag applied to the image, its health, size, and more.

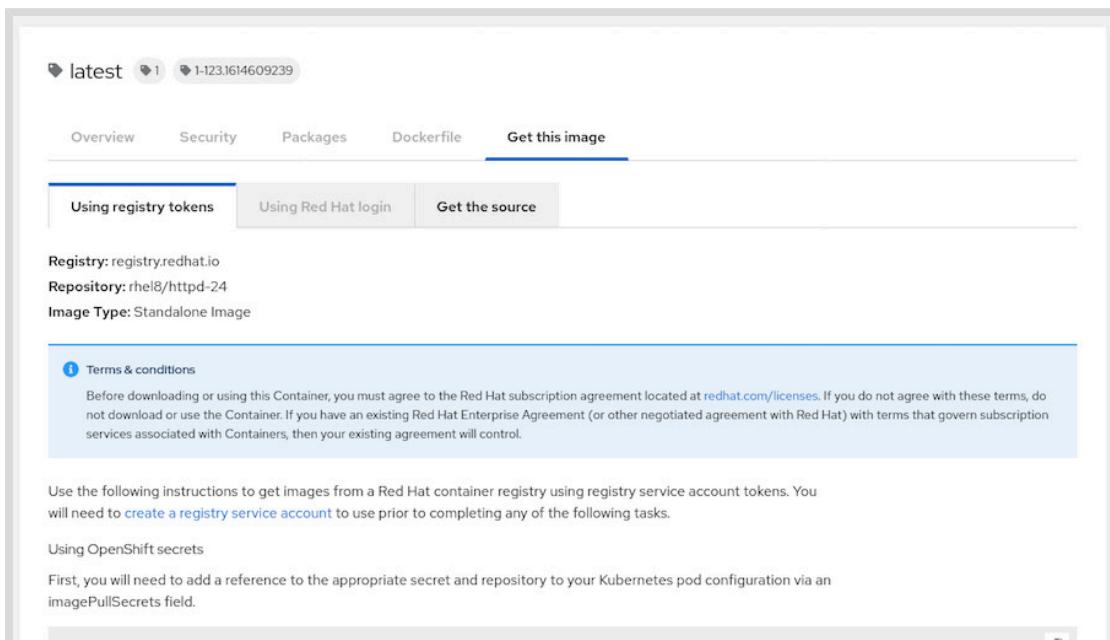


Figure 2.3: Apache httpd 2.4 (rhel8/httpd-24) latest image page

The *Get this image* tab provides the procedure to get the most current version of the image. The page provides different options to retrieve the image. Choose your preferred procedure in the tabs, and the page provides the appropriate instructions to retrieve the image.

█

References

Red Hat Container Catalog
<https://registry.redhat.io>

Quay.io website
<https://quay.io>

► Guided Exercise

Creating a MySQL Database Instance

In this exercise, you will start a MySQL database inside a container and then create and populate a database.

Outcomes

You should be able to start a database from a container image and store information inside the database.

Before You Begin

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab container-create start
```

Instructions

- 1. Create a MySQL container instance.

- 1.1. Log in to the Red Hat Container Catalog with your Red Hat account. If you need to register with Red Hat, see the instructions in *Appendix D, Creating a Red Hat Account*.

```
[student@workstation ~]$ podman login registry.redhat.io
Username: your_username
Password: your_password
Login Succeeded!
```

- 1.2. Start a container from the Red Hat Container Catalog MySQL image.

```
[student@workstation ~]$ podman run --name mysql-basic \
> -e MYSQL_USER=user1 -e MYSQL_PASSWORD=mypa55 \
> -e MYSQL_DATABASE=items -e MYSQL_ROOT_PASSWORD=r00tpa55 \
> -d registry.redhat.io/rhel8/mysql-80:1
Trying to pull ...output omitted...
Copying blob ...output omitted...
Writing manifest to image destination
Storing signatures
2d37682eb33a70330259d6798bdfdc37921367f56b9c2a97339d84faa3446a03
```

This command downloads the MySQL 8.0 container image with the `1` tag, and then starts a container based on that image. It creates a database named `items`, owned by a user named `user1` with `mypa55` as the password. The database administrator password is set to `r00tpa55` and the container runs in the background.

- 1.3. Verify that the container started without errors.

```
[student@workstation ~]$ podman ps --format "{{.ID}} {{.Image}} {{.Names}}"
2d37682eb33a registry.redhat.io/rhel8/mysql-80:1 mysql-basic
```

- 2. Access the container sandbox by running the following command:

```
[student@workstation ~]$ podman exec -it mysql-basic /bin/bash
bash-4.4$
```

This command starts a Bash shell, running as the `mysql` user inside the MySQL container.

- 3. Add data to the database.

- 3.1. Connect to MySQL as the database administrator user (root).

Run the following command from the container terminal to connect to the database:

```
bash-4.4$ mysql -uroot
Welcome to the MySQL monitor. Commands end with ; or \g.
...output omitted...
mysql>
```

The `mysql` command opens the MySQL database interactive prompt. Run the following command to determine the database availability:

```
mysql> SHOW DATABASES;
+-----+
| Database      |
+-----+
| information_schema |
| items          |
| mysql          |
| performance_schema |
| sys            |
+-----+
5 rows in set (0.01 sec)
```

- 3.2. Create a new table in the `items` database. Run the following command to access the database.

```
mysql> USE items;
Database changed
```

- 3.3. Create a table called `Projects` in the `items` database.

```
mysql> CREATE TABLE Projects (id int NOT NULL,
-> name varchar(255) DEFAULT NULL,
-> code varchar(255) DEFAULT NULL,
-> PRIMARY KEY (id));
Query OK, 0 rows affected (0.01 sec)
```

You can optionally use the ~/D0180/solutions/container-create/create_table.txt file to copy and paste the CREATE TABLE MySQL statement provided.

- 3.4. Use the show tables command to verify that the table was created.

```
mysql> SHOW TABLES;
+-----+
| Tables_in_items      |
+-----+
| Projects            |
+-----+
1 row in set (0.00 sec)
```

- 3.5. Use the insert command to insert a row into the table.

```
mysql> INSERT INTO Projects (id, name, code) VALUES (1, 'DevOps', 'D0180');
Query OK, 1 row affected (0.02 sec)
```

- 3.6. Use the select command to verify that the project information was added to the table.

```
mysql> SELECT * FROM Projects;
+----+-----+----+
| id | name      | code   |
+----+-----+----+
| 1  | DevOps    | D0180 |
+----+-----+----+
1 row in set (0.00 sec)
```

- 3.7. Exit from the MySQL prompt and the MySQL container.

```
mysql> exit
Bye
bash-4.4$ exit
exit
```

Finish

On workstation, run the lab container-create finish script to complete this lab.

```
[student@workstation ~]$ lab container-create finish
```

This concludes the exercise.

Using Rootless Containers

Objectives

After completing this section, you should be able to:

- Explain the differences between running root and rootless containers.
- Describe the advantages and disadvantages of each case.
- Run as root and rootless containers with Podman.

Evolution of Container Usage

If you have been running containers for some time, chances are that you are running them as a privileged user. Historically, tools for container creation required that runtime engines run as root, and privileged access was necessary to create resources, such as network interfaces.

From a security perspective, providing this level of access is a bad practice. You should always run software with privileges that are as limited as possible. When a security bug is exploited, either on the runtime engine or the application itself, the impact is minimized.

A better practice is to containerize applications in such a way that they do not require a privileged user to run. These applications should use a well-known user instead.

Many community container images, such as those available at docker.io, still require root to run.

Some tools, such as Podman and Red Hat OpenShift, run rootless containers by default. Docker announced that rootless mode is generally available in version 20.10.

Advantages of Rootless Containers

Rootless containers are a new concept of containers that do not require root privileges to run. Rootless containers are advantageous from a security perspective for several reasons, including:

- Allows code to run inside a rootless container with root privileges, without having to run as the host's root user.
- Adds a new security layer; if the container engine is compromised, then the attacker will not gain root privileges on the host.
- Allows multiple unprivileged users to run containers on the same machine.
- Allows isolation inside nested containers.

Despite all of these advantages, running rootless containers has several limitations, including:

- Dropped capabilities
- Binding to ports less than 1024
- Volume mounting other content

There is a detailed list of rootless shortcomings in <https://github.com/containers/podman/blob/master/rootless.md>.

Understanding Rootless Containers

To understand how rootless containers work, consider the following concepts.

User Namespaces

Containers use Linux namespaces to isolate themselves from the host on which they run. In particular, the User namespace is used to make containers rootless. This namespace maps user and group IDs so that a process inside the namespace might appear to be running under a different ID.

Rootless containers use the User namespace to make application code appear to be running as root. However, from the host's perspective, permissions are limited to those of a regular user. If an attacker manages to escape the user namespace onto the host, then it will have only the capabilities of a regular, unprivileged user.

Networking

To allow proper networking inside a container, a Virtual Ethernet device is created. This poses a problem for rootless containers because only a real root user has the privileges to create this and similar devices.

On a rootless container, networking is usually managed by Slirp. It works by forking into the container's user and network namespaces and creating a tap device that becomes the default route. Then, it passes the device's file descriptor to the parent, who runs in the default network namespace and can now communicate with both the container and the internet.

Storage

By default, container engines use a special driver called Overlay2 (or Overlay) to create a layered file system that is efficient in both capacity and performance. This cannot be done with rootless containers, because most Linux distributions do not allow mounting overlay file systems in user namespaces.

For rootless containers, the solution is to create a new storage driver. The FUSE-OverlayFS is a user-space implementation of Overlay, which is more efficient than the VFS storage driver used before and can run inside user namespaces.



References

[user_namespaces\(7\) man page](#)

https://man7.org/linux/man-pages/man7/user_namespaces.7.html

[Use of Podman in a Rootless environment](#)

https://github.com/containers/podman/blob/master/docs/tutorials/rootless_tutorial.md

► Guided Exercise

Exploring Root and Rootless Containers

In this exercise, you will understand the differences between running containers as root and running them rootless.

Outcomes

You should be able to see the UIDs for processes running inside containers.

Before You Begin

As the student user on the workstation machine, use the `lab` command to prepare your system for this exercise.

This command ensures that you have available the tools needed to perform this exercise.

```
[student@workstation ~]$ lab container-rootless start
```

Instructions

- 1. Run a container as the root user and check the UID of a running process inside it.

- 1.1. Start a container with sudo from the Red Hat UBI 8 image.

```
[student@workstation ~]$ sudo podman run --rm --name asroot -it \
> registry.access.redhat.com/ubi8:latest /bin/bash
Trying to pull registry.access.redhat.com/ubi8:latest...
Getting image source signatures
...output omitted...
[root@f95d16108991 /]# whoami
root
[root@f95d16108991 /]# id
uid=0(root) gid=0(root) groups=0(root)
```

- 1.2. Start a `sleep` process inside the container.

```
[root@f95d16108991 /]# sleep 1000
```

- 1.3. On a new terminal, run `ps` to search for the process.

```
[student@workstation ~]$ sudo ps -ef | grep "sleep 1000"
root      3137      3117  0 10:18 pts/0    00:00:00 /usr/bin/coreutils --
coreutils-prog-shebang=sleep /usr/bin/sleep 1000
```

- 1.4. Exit the container.

```
[root@f95d16108991 /]# sleep 1000
^C
[root@f95d16108991 /]# exit
exit
[student@workstation ~]$
```

- 2. Run a container as a regular user and check the UID of a running process inside it.

2.1. Start another container from the Red Hat UBI 8 as a regular user.

```
[student@workstation ~]$ podman run --rm --name asuser -it \
> registry.access.redhat.com/ubi8:latest /bin/bash
Trying to pull registry.access.redhat.com/ubi8:latest...
Getting image source signatures
...output omitted...
[root@d289dccd5285 /]# whoami
root
[root@d289dccd5285 /]# id
uid=0(root) gid=0(root) groups=0(root)
```

2.2. Start a `sleep` process inside the container.

```
[root@d289dccd5285 /]# sleep 2000
```

2.3. On a new terminal, run `ps` to search for the process.

```
[student@workstation ~]$ sudo ps -ef | grep "sleep 2000" | grep -v grep
student      3345      3325  0 10:24 pts/0    00:00:00 /usr/bin/coreutils --
coreutils-prog-shebang=sleep /usr/bin/sleep 2000
```

2.4. Exit the container.

```
[root@d289dccd5285 /]# sleep 2000
^C
[root@d289dccd5285 /]# exit
exit
[student@workstation ~]$
```

Finish

On the `workstation` machine, use the `lab` command to complete this exercise. This is important to ensure that resources from previous exercises do not impact upcoming exercises.

```
[student@workstation ~]$ lab container-rootless finish
```

This concludes the section.

► Lab

Creating Containerized Services

Outcomes

You should be able to start and customize a container using a container image.

Before You Begin

Open a terminal on the `workstation` machine as the `student` user and run the following command:

```
[student@workstation ~]$ lab container-review start
```

Instructions

1. Use the `quay.io/redhattraining/httpd-parent` image with the `2.4` tag to start a new container named `httpd-basic` in the background. Forward port `8080` on the host to port `80` in the container. Use the `-p` option of the `podman` command, and set the option value to `8080:80`.
2. Test that Apache HTTP server is running inside the `httpd-basic` container.
3. Customize the `httpd-basic` container to display `Hello World` as the message. The container's message is stored in the file `/var/www/html/index.html`.

Evaluation

Grade your work by running the `lab container-review grade` command on your `workstation` machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab container-review grade
```

Finish

On the `workstation` machine, run the `lab container-review finish` script to complete this lab.

```
[student@workstation ~]$ lab container-review finish
```

This concludes the lab.

► Solution

Creating Containerized Services

Outcomes

You should be able to start and customize a container using a container image.

Before You Begin

Open a terminal on the **workstation** machine as the **student** user and run the following command:

```
[student@workstation ~]$ lab container-review start
```

Instructions

1. Use the `quay.io/redhattraining/httpd-parent` image with the `2.4` tag to start a new container named `httpd-basic` in the background. Forward port `8080` on the host to port `80` in the container. Use the `-p` option of the `podman` command, and set the option value to `8080:80`.
 - 1.1. Use the `podman run` command to start a container. Add the `-d` option to start it in the background, and add the `-p` option to map port `8080` on the host to port `80` in the container.

```
[student@workstation ~]$ podman run -d -p 8080:80 --name httpd-basic \
> quay.io/redhattraining/httpd-parent:2.4
...output omitted...
Copying blob a3ed95caeb02 done
...output omitted...
Writing manifest to image destination
Storing signatures
b51444e3b1d7aaaf94b3a4a54485d76a0a094cbfac89c287d360890a3d2779a5a
```

This command starts the Apache HTTP server in the background and returns you to the Bash prompt.

2. Test that Apache HTTP server is running inside the `httpd-basic` container.
 - 2.1. From the **workstation** machine, attempt to access `http://localhost:8080` using any web browser.
A `Hello from the httpd-parent container!` message is displayed. This message is located on the `index.html` page from the Apache HTTP server container running on the **workstation** machine.

```
[student@workstation ~]$ curl http://localhost:8080
Hello from the httpd-parent container!
```

3. Customize the `httpd-basic` container to display Hello World as the message. The container's message is stored in the file `/var/www/html/index.html`.
- 3.1. Start a Bash session inside the container.

Run the following command:

```
[student@workstation ~]$ podman exec -it httpd-basic /bin/bash  
bash-4.4#
```

- 3.2. From the Bash session, verify the `index.html` file under `/var/www/html` directory using the `ls -la` command.

```
bash-4.4# ls -la /var/www/html  
total 4  
drwxr-xr-x. 2 root root 24 Jun 12 11:58 .  
drwxr-xr-x. 4 root root 33 Jun 12 11:58 ..  
-rw-r--r--. 1 root root 39 Jun 12 11:58 index.html
```

- 3.3. Change the `index.html` file to contain the text Hello World, replacing all of the existing content.

From the Bash session in the container, run the following command:

```
bash-4.4# echo "Hello World" > /var/www/html/index.html
```

- 3.4. Attempt to access `http://localhost:8080` again, and verify that the web page has been updated.

```
bash-4.4# exit  
exit  
[student@workstation ~]$ curl http://localhost:8080  
Hello World
```

Evaluation

Grade your work by running the `lab container-review grade` command on your workstation machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab container-review grade
```

Finish

On the workstation machine, run the `lab container-review finish` script to complete this lab.

```
[student@workstation ~]$ lab container-review finish
```

This concludes the lab.

Summary

In this chapter, you learned:

- Podman allows users to search for and download images from local or remote registries.
- The `podman run` command creates and starts a container from a container image.
- Containers are executed in the background by using the `-d` flag, or interactively by using the `-it` flag.
- Some container images require environment variables that are set using the `-e` option with the `podman run` command.
- Red Hat Container Catalog assists in searching, exploring, and analyzing container images from Red Hat's official container image repository.

Chapter 3

Managing Containers

Goal

Make use of prebuilt container images to create and manage containerized services.

Objectives

- Manage a container's lifecycle from creation to deletion.
- Save container application data with persistent storage.
- Describe how to use port forwarding to access a container.

Sections

- Managing the Lifecycle of Containers (and Guided Exercise)
- Attaching Persistent Storage to Containers (and Guided Exercise)
- Accessing Containers (and Guided Exercise)

Lab

- Managing Containers

Managing the Lifecycle of Containers

Objectives

After completing this section, students should be able to manage the lifecycle of a container from creation to deletion.

Container Lifecycle Management with Podman

In previous chapters, you learned how to use Podman to create a containerized service. Now you will dive deeper into commands and strategies that you can use to manage a container's lifecycle. Podman allows you not only to run containers, but also to make them run in the background, execute new processes inside them, and provide them with resources, such as file system volumes or a network.

Podman, implemented by the `podman` command, provides a set of subcommands to create and manage containers. Developers use those subcommands to manage the container and container image lifecycle. The following figure shows a summary of the most commonly used subcommands that change the container and image state:

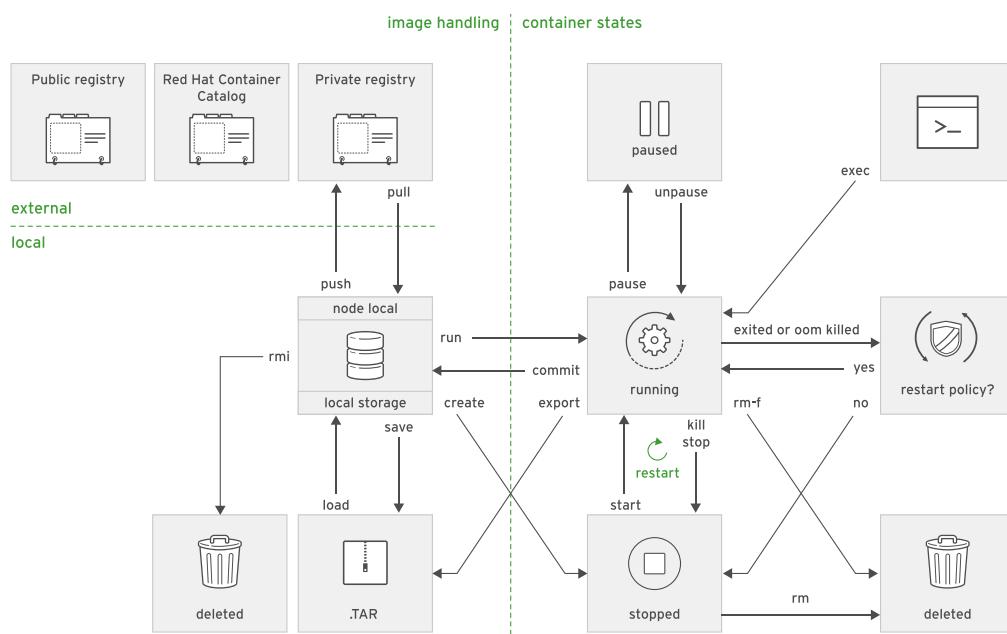


Figure 3.1: Podman managing subcommands

Podman also provides a set of useful subcommands to obtain information about running and stopped containers.

You can use these subcommands to extract information from containers and images for debugging, updating, or reporting purposes. The following figure shows a summary of the most commonly used subcommands that query information from containers and images:

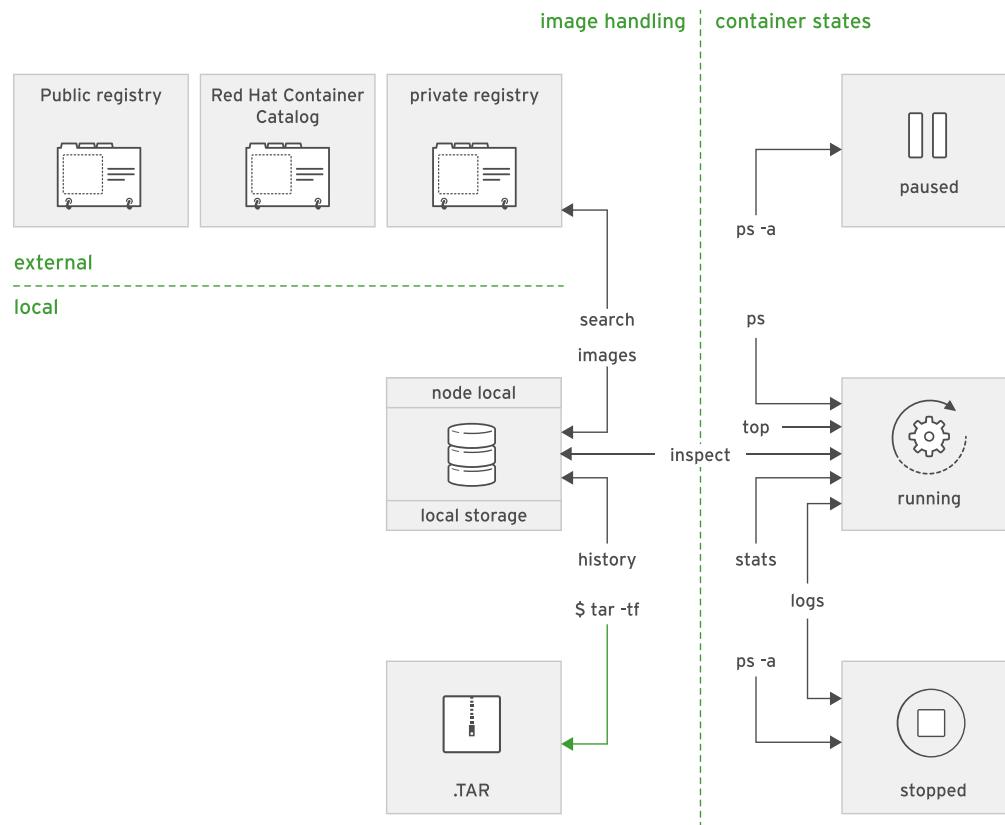


Figure 3.2: Podman query subcommands

Use these two figures as a reference while you learn about Podman subcommands in this course.

Creating Containers

The `podman run` command creates a new container from an image and starts a process inside the new container. If the container image is not available locally, this command attempts to download the image using the configured image repository:

```
[user@host ~]$ podman run registry.redhat.io/rhel8/httpd-24
Trying to pull registry.redhat.io/rhel8/httpd-24...
Getting image source signatures
Copying blob sha256:23113...b0be82
72.21 MB / 72.21 MB [=====] 7s
...output omitted... AH00094: Command line: 'httpd -D FOREGROUND'
^C
```

In this output sample, the container was started with a non-interactive process (without the `-it` option) and is running in the foreground because it was not started with the `-d` option. Stopping the resulting process with `Ctrl+C` (`SIGINT`) stops both the container process as well as the container itself.

Podman identifies containers by a unique container ID or container name. The `podman ps` command displays the container ID and names for all actively running containers:

```
[user@host ~]$ podman ps
CONTAINER ID IMAGE COMMAND ... NAMES
47c9aad6049①
registry.redhat.io/rhel8/httpd-24 "/usr/bin/run-http..." ... focused_fermat②
```

- ① The container ID is unique and generated automatically.
- ② The container name can be manually specified, otherwise it is generated automatically. This name must be unique or the `run` command fails.

The `podman run` command automatically generates a unique, random ID. It also generates a random container name. To define the container name explicitly, use the `--name` option when running a container:

```
[user@host ~]$ podman run --name my-httpd-container \
> registry.redhat.io/rhel8/httpd-24
...output omitted... AH00094: Command line: 'httpd -D FOREGROUND'
```



Note

The name must be unique. Podman throws an error if the name is already in use by any container, including stopped containers.

Another important feature is the ability to run the container as a daemon process in the background. The `-d` option is responsible for running in detached mode. When using this option, Podman returns the container ID on the screen, allowing you to continue to run commands in the same terminal while the container runs in the background:

```
[user@host ~]$ podman run --name my-httpd-container \
> -d registry.redhat.io/rhel8/httpd-24
77d4b7b8ed1fd57449163bcb0b78d205e70d2314273263ab941c0c371ad56412
```

The container image specifies the command to run to start the containerized process, known as the entry point. The `podman run` command can override this entry point by including the command after the container image:

```
[user@host ~]$ podman run registry.redhat.io/rhel8/httpd-24 ls /tmp
ks-script-1j4CXN
```

The specified command must be executable inside the container image.



Note

Because a specified command appears in the example, the container skips the entry point for the `httpd` image. Hence, the `httpd` service does not start.

Some containers need to run as an interactive shell or process. This includes containers running processes that need user input (such as entering commands), and processes that generate output through standard output. The following example starts an interactive bash shell in a `registry.redhat.io/rhel8/httpd-24` container:

```
[user@host ~]$ podman run -it registry.redhat.io/rhel8/httpd-24 /bin/bash
bash-4.4#
```

- The `-t` and `-i` options enable terminal redirection for interactive text-based programs.
- The `-t` option allocates a pseudo-tty (a terminal) and attaches it to the standard input of the container.
- The `-i` option keeps the container's standard input open, even if it was detached, so the main process can continue waiting for input.

Running Commands in a Container

When a container starts, it executes the entry point command. However, it may be necessary to execute other commands to manage the running container.

Some typical use case are shown below:

- Executing an interactive shell in an already running container.
- Running processes that update or display the container's files.
- Starting new background processes inside the container.

The `podman exec` command starts an additional process inside an already running container:

```
[user@host ~]$ podman exec 7ed6e671a600 cat /etc/hostname
7ed6e671a600
```

In this example, the container ID is used to execute a command in an existing container.

Podman remembers the last container created. Developers can skip writing this container's ID or name in later Podman commands by replacing the container id by the `-l` (or `--latest`) option:

```
[user@host ~]$ podman exec my-httdp-container cat /etc/hostname
7ed6e671a600

[user@host ~]$ podman exec -l cat /etc/hostname
7ed6e671a600
```

Managing Containers

Creating and starting a container is just the first step of the container's lifecycle. This lifecycle also includes stopping, restarting, or removing the container. Users can also examine the container status and metadata for debugging, updating, or reporting purposes.

Podman provides the following commands for managing containers:

`podman ps`

This command lists running containers:

```
[user@host ~]$ podman ps
CONTAINER ID  IMAGE          COMMAND      CREATED     STATUS      PORTS      NAMES
77d4b7b8ed1f  registry.redhat.io/rhel8/httpd-24  /usr/bin/run-httpd... ...ago
Up...  my-htt... ●
```

Chapter 3 | Managing Containers

- 1 Each row describes information about the container.

CONTAINER ID

Each container, when created, gets a **container ID**, which is a hexadecimal number. This ID looks like an image ID but is unrelated.

IMAGE

The **IMAGE** field indicates container image that was used to start the container.

COMMAND

The **COMMAND** field indicates command executed when the container started.

CREATED

The **CREATED** field indicates date and time the container was started.

STATUS

The **STATUS** field indicates total container uptime, if still running, or time since terminated.

PORTS

The **PORTS** field indicates ports that were exposed by the container or any port forwarding that might be configured.

NAMES

The **NAMES** field indicates the container name.

Podman does not discard stopped containers immediately. Podman preserves their local file systems and other states for facilitating *postmortem* analysis. Option `-a` lists all containers, including stopped ones:

```
[user@host ~]$ podman ps -a
CONTAINER ID  IMAGE          COMMAND       CREATED      STATUS        PORTS     NAMES
4829d82fbbff  registry.redhat.io/rhel8/httpd-24  /usr/bin/run-httpd...  ...ago
             Exited (0)...  my-httpd...
```



Note

While creating containers, Podman aborts if the container name is already in use, even if the container is in a stopped status. This option helps to avoid duplicated container names.

podman stop

This command stops a running container gracefully:

```
[user@host ~]$ podman stop my-httpd-container
77d4b7b8ed1fd57449163bcb0b78d205e70d2314273263ab941c0c371ad56412
```

Using `podman stop` is easier than finding the container start process on the host OS and killing it.

podman kill

This command sends Unix signals to the main process in the container. If no signal is specified, it sends the `SIGKILL` signal, terminating the main process and the container.

```
[user@host ~]$ podman kill my-httdp-container
77d4b7b8ed1fd57449163bcb0b78d205e70d2314273263ab941c0c371ad56412
```

You can specify the signal with the `-s` option:

```
[user@host ~]$ podman kill -s SIGKILL my-httdp-container
77d4b7b8ed1fd57449163bcb0b78d205e70d2314273263ab941c0c371ad56412
```

Any Unix signal can be sent to the main process. Podman accepts either the signal name or number.

The following table shows several useful signals:

Signal	Value	Default Action	Comment
SIGHUP	1	Term	Hangup detected on controlling terminal or death of controlling process
SIGINT	2	Term	Interrupt from keyboard
SIGQUIT	3	Core	Quit from keyboard
SIGILL	4	Core	Illegal Instruction
SIGABRT	6	Core	Abort signal from <code>abort(3)</code>
SIGFPE	8	Core	Floating point exception
SIGKILL	9	Term	Kill signal
SIGSEGV	11	Core	Invalid memory reference
SIGPIPE	13	Term	Broken pipe: write to pipe with no readers
SIGALRM	14	Term	Timer signal from <code>alarm(2)</code>
SIGTERM	15	Term	Termination signal
SIGUSR1	30,10,16	Term	User-defined signal 1
SIGUSR2	31,12,17	Term	User-defined signal 2
SIGCHLD	20,17,18	Ign	Child stopped or terminated
SIGCONT	19,18,25	Cont	Continue if stopped
SIGSTOP	17,19,23	Stop	Stop process
SIGTSTP	18,20,24	Stop	Stop typed at tty
SIGTTIN	21,21,26	Stop	tty input for background process
SIGTTOU	22,22,27	Stop	tty output for background process

The default action for each signal is specified as follows:

Default Action	Description
Term	Terminate the process.
Core	Terminate the process and generate a core dump.
Ign	Signal is ignored.
Stop	Stop the process.

Additional useful podman commands include the following:

podman restart

This command restarts a stopped container:

```
[user@host ~]$ podman restart my-httppd-container
77d4b7b8ed1fd57449163bcb0b78d205e70d2314273263ab941c0c371ad56412
```

The `podman restart` command creates a new container with the same container ID, reusing the stopped container state and file system.

podman rm

This command deletes a container and discards its state and file system.

```
[user@host ~]$ podman rm my-httppd-container
77d4b7b8ed1fd57449163bcb0b78d205e70d2314273263ab941c0c371ad56412
```

The `-f` option of the `rm` subcommand instructs Podman to remove the container even if it is not stopped. This option terminates the container forcefully and then removes it. Using the `-f` option is equivalent to the `podman kill` and `podman rm` commands together.

You can delete all containers at the same time. Many `podman` subcommands accept the `-a` option. This option indicates using the subcommand on all available containers or images. The following example removes all containers:

```
[user@host ~]$ podman rm -a
5fd8e98ec7eab567eabe84943fe82e99fdfc91d12c65d99ec760d5a55b8470d6
716fd687f65b0957edad73b84b3253760e915166d3bc620c4aec8e5f4eadfe8e
86162c906b44f4cb63ba2e3386554030dc6abedbce9e9fcad60aa9f8b2d5d4
```

Before deleting all containers, all running containers must be in a stopped status. You can use the following command to stop all containers:

```
[user@host ~]$ podman stop -a
5fd8e98ec7eab567eabe84943fe82e99fdfc91d12c65d99ec760d5a55b8470d6
716fd687f65b0957edad73b84b3253760e915166d3bc620c4aec8e5f4eadfe8e
86162c906b44f4cb63ba2e3386554030dc6abedbce9e9fcad60aa9f8b2d5d4
```



Note

The `inspect`, `stop`, `kill`, `restart`, and `rm` subcommands can use the container ID instead of the container name.



References

Unix Posix Signals man page

<http://man7.org/linux/man-pages/man7/signal.7.html>

► Guided Exercise

Managing a MySQL Container

In this exercise, you will create and manage a MySQL® database container.

Outcomes

You should be able to create and manage a MySQL database container.

Before You Begin

Make sure that the `workstation` machine has the `podman` command available and is correctly set up by running the following command from a terminal window:

```
[student@workstation ~]$ lab manage-lifecycle start
```

Instructions

- 1. Download the MySQL database container image and attempt to start it. The container does not start because several environment variables must be provided to the image.
 - 1.1. Log in to the Red Hat Container Catalog with your Red Hat account. If you need to register with Red Hat, see the instructions in *Appendix D, Creating a Red Hat Account*.

```
[student@workstation ~]$ podman login registry.redhat.io
Username: your-username
Password: your-password
Login Succeeded!
```

- 1.2. Download the MySQL database container image and attempt to start it.

```
[student@workstation ~]$ podman run --name mysql-db \
> registry.redhat.io/rhel8/mysql-80:1
Trying to pull ...output omitted...
...output omitted...
Writing manifest to image destination
Storing signatures
You must either specify the following environment variables:
  MYSQL_USER      (regex: ...)
  MYSQL_PASSWORD  (regex: ...)
  MYSQL_DATABASE  (regex: ...)
Or the following environment variable:
  MYSQL_ROOT_PASSWORD (regex: ...)
Or both.
Optional Settings:
...output omitted...
```

**Note**

If you try to run the container as a daemon (-d), then the error message about the required variables is not displayed. However, this message is included as part of the container logs, which can be viewed using the following command:

```
[student@workstation ~]$ podman logs mysql-db
```

- ▶ 2. Create a new container named `mysql`, and then specify each required variable using the `-e` parameter.

**Note**

Make sure you start the new container with the correct name.

```
[student@workstation ~]$ podman run --name mysql \
> -d -e MYSQL_USER=user1 -e MYSQL_PASSWORD=mypa55 \
> -e MYSQL_DATABASE=items -e MYSQL_ROOT_PASSWORD=r0otpa55 \
> registry.redhat.io/rhel8/mysql-80:1
```

The command displays the container ID for the `mysql` container. Below is an example of the output.

```
a8a6090a0a632b5876001725b581fdd331c9ab8b9eda21cc2a2899c23f078509
```

- ▶ 3. Verify that the `mysql` container started correctly. Run the following command:

```
[student@workstation ~]$ podman ps
CONTAINER ID  ... STATUS          ... NAMES
a8a6090a0a63  ... Up 13 seconds ... mysql
```

The command only shows the first 12 characters of the container ID displayed in the previous command.

- ▶ 4. Populate the `items` database with the `Projects` table:

- 4.1. Run `podman cp` command to copy database file to `mysql` container.

```
[student@workstation ~]$ podman cp ~/DO180/labs/manage-lifecycle/db.sql mysql:/
```

- 4.2. Populate the `items` database with the `Projects` table.

```
[student@workstation ~]$ podman exec mysql /bin/bash -c \
> 'mysql -uuser1 -pmypa55 items < /db.sql'
mysql: [Warning] Using a password on the command line interface can be insecure.
```

- 5. Create another container using the same container image as the previous container. Interactively enter the /bin/bash shell instead of using the default command for the container image.

```
[student@workstation ~]$ podman run --name mysql-2 -it \
> registry.redhat.io/rhel8/mysql-80:1 /bin/bash
bash-4.4$
```

- 6. Try to connect to the MySQL database in the new container:

```
bash-4.4$ mysql -uroot
```

The following error displays:

```
ERROR 2002 (HY000): Can't connect to local MySQL ...output omitted...
```

The MySQL database server is not running because the container executed the /bin/bash command rather than starting the MySQL server.

- 7. Exit the container.

```
bash-4.4$ exit
```

- 8. Verify that the mysql-2 container is not running.

```
[student@workstation ~]$ podman ps -a
CONTAINER ID  ... STATUS          ... NAMES
27b4b00b7f5c  ... Exited (1) 4 minutes ago ... mysql-db
a8a6090a0a63  ... Up 4 minutes ago   ... mysql
bd517765c217  ... Exited (0) 8 seconds ago ... mysql-2
```

- 9. Query the mysql container to list all rows in the Projects table. The command instructs the bash shell to query the items database using a mysql command.

```
[student@workstation ~]$ podman exec mysql /bin/bash -c \
> 'mysql -uuser1 -pmypa55 -e "select * from items.Projects;"'
mysql: [Warning] Using a password on the command-line interface can be insecure.
+----+-----+-----+
| id | name | code |
+----+-----+-----+
| 1  | DevOps | D0180 |
```

Finish

On workstation, run the following script to complete this exercise.

```
[student@workstation ~]$ lab manage-lifecycle finish
```

This concludes the exercise.

Attaching Persistent Storage to Containers

Objectives

After completing this section, students should be able to:

- Save application data across container removals through the use of persistent storage.
- Configure host directories to use as container volumes.
- Mount a volume inside the container.

Preparing Permanent Storage Locations

Container storage is said to be *ephemeral*, meaning its contents are not preserved after the container is removed. Containerized applications work on the assumption that they always start with empty storage, and this makes creating and destroying containers relatively inexpensive operations.

Previously in this course, container images were characterized as *immutable* and *layered*, meaning that they are never changed, but rather composed of layers that add or override the contents of layers below.

A running container gets a new layer over its base container image, and this layer is the *container storage*. At first, this layer is the only read/write storage available for the container, and it is used to create working files, temporary files, and log files. Those files are considered volatile. An application does not stop working if they are lost. The container storage layer is exclusive to the running container, so if another container is created from the same base image, it gets another read/write layer. This ensures the each container's resources are isolated from other similar containers.

Ephemeral container storage is *not* sufficient for applications that need to keep data beyond the life of the container, such as databases. To support such applications, the administrator must provide a container with persistent storage.

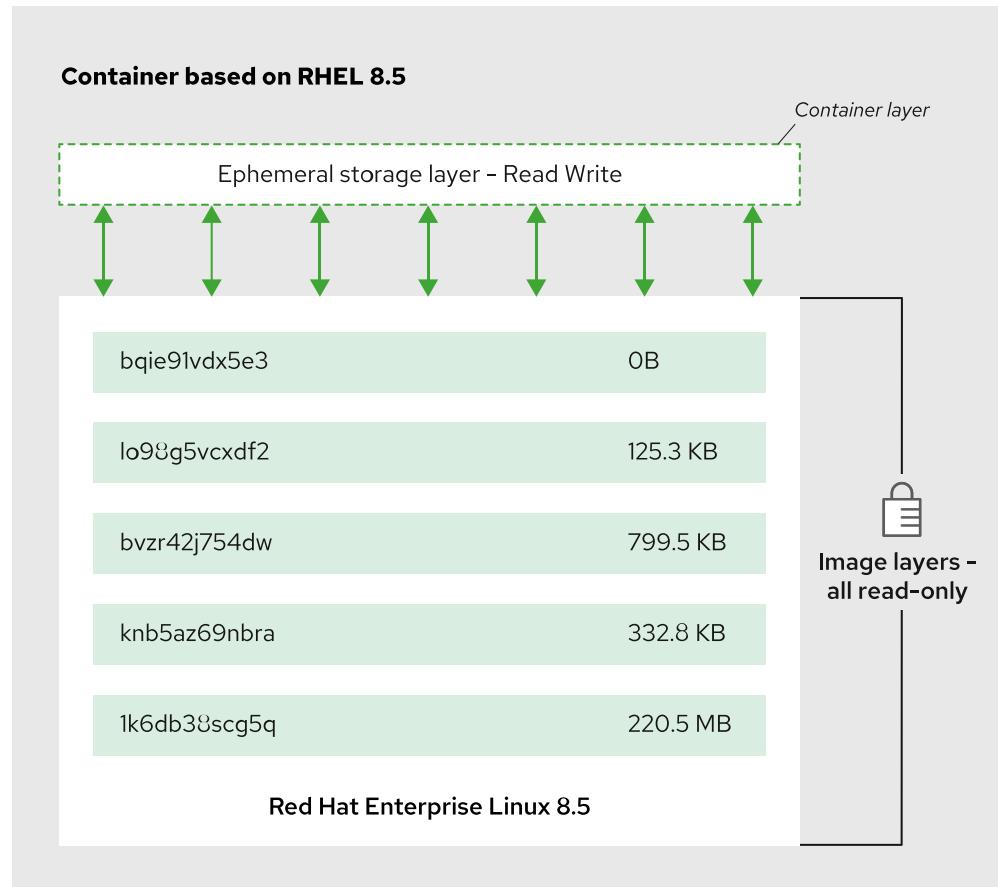


Figure 3.3: Container layers

Containerized applications should not try to use the container storage to store persistent data, because they cannot control how long its contents will be preserved.

Even if it were possible to keep container storage indefinitely, the layered file system does not perform well for intensive I/O workloads and would not be adequate for most applications requiring persistent storage.

Reclaiming Storage

Podman keeps old stopped container storage available to be used by troubleshooting operations, such as reviewing failed container logs for error messages.

If the administrator needs to reclaim old container storage, then the container can then be deleted using `podman rm container_id`. This command also deletes the container storage. You can find the stopped container IDs using `podman ps -a` command.

Preparing the Host Directory

Podman can mount host directories inside a running container. The containerized application sees these host directories as part of the container storage, much like regular applications see a remote network volume as if it were part of the host file system. But these host directories' contents are not reclaimed after the container is stopped, so they can be mounted to new containers whenever needed.

For example, a database container can use a host directory to store database files. If this database container fails, Podman can create a new container using the same host directory, keeping the

database data available to client applications. To the database container, it does not matter where this host directory is stored from the host point of view; it could be anywhere from a local hard disk partition to a remote networked file system.

A container runs as a host operating system process, under a host operating system user and group ID, so the host directory must be configured with ownership and permissions allowing access to the container. In RHEL, the host directory also needs to be configured with the appropriate SELinux context, which is `container_file_t`. Podman uses the `container_file_t` SELinux context to restrict which files on the host system the container is allowed to access. This avoids information leakage between the host system and the applications running inside containers.

One way to set up the host directory is described below:

1. Create a directory:

```
[user@host ~]$ mkdir /home/student/dbfiles
```

2. The user running processes in the container must be capable of writing files to the directory. The permission should be defined with the numeric user ID (UID) from the container. For the MySQL service provided by Red Hat, the UID is 27. The `podman unshare` command provides a session to execute commands within the same user namespace as the process running inside the container.

```
[user@host ~]$ podman unshare chown -R 27:27 /home/student/dbfiles
```

3. Apply the `container_file_t` context to the directory (and all subdirectories) to allow containers access to all of its contents.

```
[user@host ~]$ sudo semanage fcontext -a -t container_file_t \
'/home/student/dbfiles(/.*)?'
```

4. Apply the SELinux container policy that you set up in the first step to the newly created directory:

```
[user@host ~]$ sudo restorecon -Rv /home/student/dbfiles
```

The host directory must be configured *before* starting the container that uses the directory.

Mounting a Volume

After creating and configuring the host directory, the next step is to mount this directory to a container. To bind mount a host directory to a container, add the `-v` option to the `podman run` command, specifying the host directory path and the container storage path, separated by a colon (`:`).

For example, to use the `/home/student/dbfiles` host directory for MySQL server database files, which are expected to be under `/var/lib/mysql` inside a MySQL container image named `mysql`, use the following command:

```
[user@host ~]$ podman run -v /home/student/dbfiles:/var/lib/mysql rhmap47/mysql
```

In this command, if the `/var/lib/mysql` already exists inside the `mysql` container image, the `/home/student/dbfiles` mount overlays, but does not remove, the content from the container image. If the mount is removed, the original content is accessible again.



References

Dealing with user namespaces and SELinux on rootless containers

<https://www.redhat.com/sysadmin/user-namespaces-selinux-rootless-containers>

Understanding SELinux labels for container runtimes

<https://opensource.com/article/18/2/selinux-labels-container-runtimes>

► Guided Exercise

Create MySQL Container with Persistent Database

In this exercise, you will create a container that stores the MySQL database data into a host directory.

Outcomes

You should be able to deploy a container with a persistent database.

Before You Begin

The workstation should not have any container images running.

Run the following command on workstation:

```
[student@workstation ~]$ lab manage-storage start
```

Instructions

- ▶ 1. Create the /home/student/local/mysql directory with the correct SELinux context and permissions.
 - 1.1. Create the /home/student/local/mysql directory.

```
[student@workstation ~]$ mkdir -vp /home/student/local/mysql
mkdir: created directory /home/student/local
mkdir: created directory /home/student/local/mysql
```

- 1.2. Add the appropriate SELinux context for the /home/student/local/mysql directory and its contents.

```
[student@workstation ~]$ sudo semanage fcontext -a \
> -t container_file_t '/home/student/local/mysql(/.*)?'
```

- 1.3. Apply the SELinux policy to the newly created directory.

```
[student@workstation ~]$ sudo restorecon -R /home/student/local/mysql
```

- 1.4. Verify that the SELinux context type for the /home/student/local/mysql directory is container_file_t.

```
[student@workstation ~]$ ls -ldZ /home/student/local/mysql
drwxrwxr-x. 2 student student unconfined_u:object_r:container_file_t:s0 6 May 26
14:33 /home/student/local/mysql
```

15. Change the owner of the /home/student/local/mysql directory to the mysql user and mysql group:

```
[student@workstation ~]$ podman unshare chown 27:27 /home/student/local/mysql
```

**Note**

The user running processes in the container must be capable of writing files to the directory.

The permission should be defined with the numeric user ID (UID) from the container. For the MySQL service provided by Red Hat, the UID is 27. The `podman unshare` command provides a session to execute commands within the same user namespace as the process running inside the container.

- ▶ 2. Create a MySQL container instance with persistent storage.

- 2.1. Log in to the Red Hat Container Catalog with your Red Hat account. If you need to register with Red Hat, see the instructions in *Appendix D, Creating a Red Hat Account*.

```
[student@workstation ~]$ podman login registry.redhat.io
Username: your-username
Password: your-password
Login Succeeded!
```

- 2.2. Pull the MySQL container image.

```
[student@workstation ~]$ podman pull registry.redhat.io/rhel8/mysql-80:1
Trying to pull registry.redhat.io/rhel8/mysql-80:1...
Getting image source signatures
Checking if image destination supports signatures
Copying blob 028bdc977650 done
...output omitted...
Writing manifest to image destination
Storing signatures
4ae3a3f4f409a8912cab9fbf71d3564d011ed2e68f926d50f88f2a3a72c809c5
```

- 2.3. Create a new container specifying the mount point to store the MySQL database data:

```
[student@workstation ~]$ podman run --name persist-db \
> -d -v /home/student/local/mysql:/var/lib/mysql/data \
> -e MYSQL_USER=user1 -e MYSQL_PASSWORD=mypa55 \
> -e MYSQL_DATABASE=items -e MYSQL_ROOT_PASSWORD=r00tpa55 \
> registry.redhat.io/rhel8/mysql-80:1
6e0ef134315b510042ca757faf869f2ba19df27790c601f95ec2fd9d3c44b95d
```

This command mounts the /home/student/local/mysql directory from the host to the /var/lib/mysql/data directory in the container. By default, the MySQL database stores data in the /var/lib/mysql/data directory.

- 2.4. Verify that the container started correctly.

```
[student@workstation ~]$ podman ps --format="{{.ID}} {{.Names}} {{.Status}}"
6e0ef134315b  persist-db  Up 3 minutes ago
```

- 3. Verify that the /home/student/local/mysql directory contains the items directory.

```
[student@workstation ~]$ ls -ld /home/student/local/mysql/items
drwxr-x---. 2 100026 100026 6 Apr 8 07:31 /home/student/local/mysql/items
```

The items directory stores data related to the items database that was created by this container. If the items directory does not exist, then the mount point was not defined correctly during container creation.



Note

Alternatively you can run the same command with podman unshare to check numeric user ID (UID) from the container.

```
[student@workstation ~]$ podman unshare ls -ld /home/student/local/mysql/items
drwxr-x---. 2 27 27 6 Apr 8 07:31 /home/student/local/mysql/items
```

Finish

On workstation, run the lab manage-storage finish script to complete this lab.

```
[student@workstation ~]$ lab manage-storage finish
```

This concludes the exercise.

Accessing Containers

Objectives

After completing this section, students should be able to:

- Describe the basics of networking with containers.
- Remotely connect to services within a container.

Mapping Network Ports

Accessing a rootless container from the host network can be challenging because no IP address is available for a rootless container.

To solve these problems, define port forwarding rules to allow external access to a container service. Use the `-p [<IP address>:]<host port>:<container port>` option with the `podman run` command to create an externally accessible container.

Consider the following example:

```
[user@host ~]$ podman run -d --name apache1 -p 8080:8080 \
> registry.redhat.io/rhel8/httpd-24
```

This example creates an externally accessible container. The value 8080 colon 8080 specifies that any requests to port 8080 on the host are forwarded to port 8080 within the container.

You can also use the `-p` option to bind the port to the specified IP address.

```
[user@host ~]$ podman run -d --name apache2 \
> -p 127.0.0.1:8081:8080 registry.redhat.io/rhel8/httpd-24
```

This example limits external access to the `apache2` container to requests from `localhost` to host port 8081. These requests are forwarded to port 8080 in the `apache2` container.

If a port is not specified for the host port, Podman assigns a random available host port for the container:

```
[user@host ~]$ podman run -d --name apache3 -p 127.0.0.1::8080 \
> registry.redhat.io/rhel8/httpd-24
```

To see the port assigned by Podman, use the `podman port <container name>` command:

```
[user@host ~]$ podman port apache3
8080/tcp -> 127.0.0.1:35134

[user@host ~]$ curl -s 127.0.0.1:35134 | egrep '</?title>' 
<title>Test Page for the HTTP Server on Red Hat Enterprise Linux</title>
```

If only a container port is specified with the `-p` option, then a random available host port is assigned to the container. Requests to this assigned host port from any IP address are forwarded to the container port.

```
[user@host ~]$ podman run -d --name apache4 \
> -p 8080 registry.redhat.io/rhel8/httpd-24

[user@host ~]$ podman port apache4
8080/tcp -> 0.0.0.0:37068
```

In this example, any routable request to host port 37068 is forwarded to port 8080 in the container.



References

Container Network Interface - networking for Linux containers

<https://github.com/containernetworking/cni>

Cloud Native Computing Foundation

<https://www.cncf.io/>

► Guided Exercise

Loading the Database

In this exercise, you will create a MySQL database container with port forwarding enabled. After populating a database with a SQL script, you verify the database content using three different methods.

Outcomes

You should be able to deploy a database container and load a SQL script.

Before You Begin

Open a terminal on the workstation machine as the student user and run the following command:

```
[student@workstation ~]$ lab manage-networking start
```

This ensures the /home/student/local/mysql directory exists and is configured with the correct permissions to enable persistent storage for the MySQL container.

Instructions

- 1. Create a MySQL container instance with persistent storage and port forwarding.
 - 1.1. Log in to the Red Hat Container Catalog with your Red Hat account. If you need to register with Red Hat, see the instructions in *Appendix D, Creating a Red Hat Account*.
- ```
[student@workstation ~]$ podman login registry.redhat.io
Username: your-username
Password: your-password
Login Succeeded!
```
- 1.2. Download the MySQL database container image and then create a MySQL container instance with persistent storage and port forwarding.

```
[student@workstation ~]$ podman run --name mysqldb-port \
> -d -v /home/student/local/mysql:/var/lib/mysql/data -p 13306:3306 \
> -e MYSQL_USER=user1 -e MYSQL_PASSWORD=mypa55 \
> -e MYSQL_DATABASE=items -e MYSQL_ROOT_PASSWORD=r00tpa55 \
> registry.redhat.io/rhel8/mysql-80:1
Trying to pull registry.redhat.io/rhel8/mysql-80:1...
Getting image source signatures
Checking if image destination supports signatures
Copying blob 0c673eb68f88 done
...output omitted...
Writing manifest to image destination
Storing signatures
066630d45cb902ab533d503c83b834aa6a9f9cf88755cb68eedb8a3e8edbc5aa
```

The last line of your output and the time needed to download each image layer will differ. The `-p` option configures port forwarding so that port 13306 on the local host forwards to container port 3306.



### Note

The start script creates the `/home/student/local/mysql` directory with the appropriate ownership and SELinux context required by the containerized database.

- ▶ 2. Verify that the `mysqldb-port` container started successfully and enables port forwarding.

```
[student@workstation ~]$ podman ps --format="{{.ID}} {{.Names}} {{.Ports}}"
9941da2936a5 mysqldb-port 0.0.0.0:13306->3306/tcp
```

- ▶ 3. Populate the database using the provided file. If there are no errors, then the command does not return any output.

```
[student@workstation ~]$ mysql -uuser1 -h 127.0.0.1 -pmypa55 -P13306 \
> items < /home/student/D0180/labs/manage-networking/db.sql
mysql: [Warning] Using a password on the command line interface can be insecure.
```

There are multiple ways to verify that the database loaded successfully. The next steps show three different methods. You only need to use one of the methods.

- ▶ 4. Verify that the database loaded successfully by executing a non-interactive command inside the container.

```
[student@workstation ~]$ podman exec -it mysqldb-port \
> mysql -uroot items -e "SELECT * FROM Item"
+-----+-----+
| id | description | done |
+-----+-----+
| 1 | Pick up newspaper | 0 |
| 2 | Buy groceries | 1 |
+-----+-----+
```

- ▶ 5. Verify that the database loaded successfully by using port forwarding from the local host. This alternate method is optional.

```
[student@workstation ~]$ mysql -uuser1 -h 127.0.0.1 -pmypa55 -P13306 \
> items -e "SELECT * FROM Item"
+-----+-----+
| id | description | done |
+-----+-----+
| 1 | Pick up newspaper | 0 |
| 2 | Buy groceries | 1 |
+-----+-----+
```

- ▶ 6. Verify that the database loaded successfully by opening an interactive terminal session inside the container. This alternate method is optional.

- 6.1. Open a Bash shell inside the container.

```
[student@workstation ~]$ podman exec -it mysql ldb-port /bin/bash
bash-4.4$
```

- 6.2. Verify that the database contains data:

```
bash-4.4$ mysql -uroot items -e "SELECT * FROM Item"
+----+-----+----+
| id | description | done |
+----+-----+----+
| 1 | Pick up newspaper | 0 |
| 2 | Buy groceries | 1 |
+----+-----+----+
```

- 6.3. Exit from the container:

```
bash-4.4$ exit
exit
[student@workstation ~]$
```

## Finish

On workstation, run the `lab manage-networking finish` script to complete this lab.

```
[student@workstation ~]$ lab manage-networking finish
```

This concludes the exercise.

## ► Lab

# Managing Containers

## Outcomes

You should be able to deploy and manage a persistent database using a shared volume. You should also be able to start a second database using the same shared volume and observe that the data is consistent between the two containers because they are using the same directory on the host to store the MySQL data.

## Before You Begin

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab manage-review start
```

## Instructions

1. Create the `/home/student/local/mysql` directory with the correct SELinux context and permissions.
2. Deploy a MySQL container instance using the following specification:

| Property        | Description                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| Name            | <code>mysql-1</code>                                                                                                 |
| Run as daemon   | <code>yes</code>                                                                                                     |
| Volume          | Bind the <code>/home/student/local/mysql</code> host folder to the <code>/var/lib/mysql/data</code> container folder |
| Container image | <code>registry.redhat.io/rhel8/mysql-80:1</code>                                                                     |
| Port forward    | <code>yes</code> , Bind host port 13306 to container port 3306                                                       |

Use the following environment variables for the container:

| Environment Variable             | Value                 |
|----------------------------------|-----------------------|
| <code>MYSQL_USER</code>          | <code>user1</code>    |
| <code>MYSQL_PASSWORD</code>      | <code>mypa55</code>   |
| <code>MYSQL_DATABASE</code>      | <code>items</code>    |
| <code>MYSQL_ROOT_PASSWORD</code> | <code>r00tpa55</code> |

3. Load the `items` database using the `/home/student/D0180/labs/manage-review/db.sql` script.

4. Stop the container gracefully.



### Important

This step is very important because a new container will be created sharing the same volume for database data. Having two containers using the same volume can corrupt the database. Do not restart the `mysql-1` container.

5. Create a new container with the following specification:

| Property        | Description                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| Name            | <code>mysql-2</code>                                                                                                 |
| Run as daemon   | yes                                                                                                                  |
| Volume          | Bind the <code>/home/student/local/mysql</code> host folder to the <code>/var/lib/mysql/data</code> container folder |
| Container image | <code>registry.redhat.io/rhel8/mysql-80:1</code>                                                                     |
| Port forward    | yes, Bind host port 13306 to container port 3306                                                                     |

Use the following environment variables for the container:

| Environment Variable             | Value                 |
|----------------------------------|-----------------------|
| <code>MYSQL_USER</code>          | <code>user1</code>    |
| <code>MYSQL_PASSWORD</code>      | <code>mypa55</code>   |
| <code>MYSQL_DATABASE</code>      | <code>items</code>    |
| <code>MYSQL_ROOT_PASSWORD</code> | <code>r00tpa55</code> |

- Save the list of all containers (including stopped ones) to the `/tmp/my-containers` file.
- Access the Bash shell inside the container and verify that the `items` database and the `Item` table are still available. Confirm also that the table contains data.
- Using port forwarding, insert a new row into the `Item` table. The row should have a `description` value of `Finished lab`, and a `done` value of `1`.
- Because the first container is not required any more, remove it to release resources.

## Evaluation

Grade your work by running the `lab manage-review grade` command from your `workstation` machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab manage-review grade
```

## Finish

On `workstation`, run the `lab manage-review finish` command to complete this lab.

```
[student@workstation ~]$ lab manage-review finish
```

This concludes the lab.

## ► Solution

---

# Managing Containers

### Outcomes

You should be able to deploy and manage a persistent database using a shared volume. You should also be able to start a second database using the same shared volume and observe that the data is consistent between the two containers because they are using the same directory on the host to store the MySQL data.

### Before You Begin

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab manage-review start
```

### Instructions

1. Create the `/home/student/local/mysql` directory with the correct SELinux context and permissions.

- 1.1. Create the `/home/student/local/mysql` directory.

```
[student@workstation ~]$ mkdir -vp /home/student/local/mysql
mkdir: created directory '/home/student/local/mysql'
```

- 1.2. Add the appropriate SELinux context for the `/home/student/local/mysql` directory and its contents. With the correct context, you can mount this directory in a running container.

```
[student@workstation ~]$ sudo semanage fcontext -a -t container_file_t \
> '/home/student/local/mysql(/.*)?'
```

- 1.3. Apply the SELinux policy to the newly created directory.

```
[student@workstation ~]$ sudo restorecon -R /home/student/local/mysql
```

- 1.4. Change the owner of the `/home/student/local/mysql` directory to match the `mysql` user and `mysql` group for the `registry.redhat.io/rhel8/mysql-80:1` container image:

```
[student@workstation ~]$ podman unshare chown -Rv 27:27 /home/student/local/mysql
changed ownership of '/home/student/local/mysql' from root:root to 27:27
```

2. Deploy a MySQL container instance using the following specification:

| Property        | Description                                                                                |
|-----------------|--------------------------------------------------------------------------------------------|
| Name            | mysql-1                                                                                    |
| Run as daemon   | yes                                                                                        |
| Volume          | Bind the /home/student/local/mysql host folder to the /var/lib/mysql/data container folder |
| Container image | registry.redhat.io/rhel8/mysql-80:1                                                        |
| Port forward    | yes, Bind host port 13306 to container port 3306                                           |

Use the following environment variables for the container:

| Environment Variable | Value    |
|----------------------|----------|
| MYSQL_USER           | user1    |
| MYSQL_PASSWORD       | mypa55   |
| MYSQL_DATABASE       | items    |
| MYSQL_ROOT_PASSWORD  | r00tpa55 |

2.1. Log in to the Red Hat Container Catalog with your Red Hat account.

```
[student@workstation ~]$ podman login registry.redhat.io
Username: your-username
Password: your-password
Login Succeeded!
```

2.2. Create and start the container.

```
[student@workstation ~]$ podman run --name mysql-1 -p 13306:3306 \
> -d -v /home/student/local/mysql:/var/lib/mysql/data \
> -e MYSQL_USER=user1 -e MYSQL_PASSWORD=mypa55 \
> -e MYSQL_DATABASE=items -e MYSQL_ROOT_PASSWORD=r00tpa55 \
> registry.redhat.io/rhel8/mysql-80:1
Trying to pull registry.redhat.io/rhel8/mysql-80:1...
Getting image source signatures
Checking if image destination supports signatures
Copying blob 0c673eb68f88 done
...output omitted...
Writing manifest to image destination
Storing signatures
616azfaa55x866e7eb18b1fd0423a5461d8f24c147b1ad8668b76e6167587cdd
```

2.3. Verify that the container was started correctly.

```
[student@workstation ~]$ podman ps --format="{{.ID}} {{.Names}}"
616azfaa55x8 mysql-1
```

3. Load the `items` database using the `/home/student/D0180/labs/manage-review/db.sql` script.
- 3.1. Load the database using the SQL commands in `/home/student/D0180/labs/manage-review/db.sql`.

```
[student@workstation ~]$ mysql -uuser1 -h 127.0.0.1 -pmypa55 -P13306 \
> items < /home/student/D0180/labs/manage-review/db.sql
mysql: [Warning] Using a password on the command-line interface can be insecure.
```

- 3.2. Use an SQL SELECT statement to output all rows of the Item table to verify that the Items database is loaded.



**Note**

You can add the `-e SQL` parameter to the `mysql` command to execute an SQL instruction.

```
[student@workstation ~]$ mysql -uuser1 -h 127.0.0.1 -pmypa55 -P13306 \
> items -e "SELECT * FROM Item"
+----+-----+----+
| id | description | done |
+----+-----+----+
| 1 | Pick up newspaper | 0 |
| 2 | Buy groceries | 1 |
+----+-----+----+
```

4. Stop the container gracefully.



**Important**

This step is very important because a new container will be created sharing the same volume for database data. Having two containers using the same volume can corrupt the database. Do not restart the `mysql-1` container.

- 4.1. Use the `podman` command to stop the container.

```
[student@workstation ~]$ podman stop mysql-1
mysql-1
```

5. Create a new container with the following specification:

| Property        | Description                                                                                |
|-----------------|--------------------------------------------------------------------------------------------|
| Name            | mysql-2                                                                                    |
| Run as daemon   | yes                                                                                        |
| Volume          | Bind the /home/student/local/mysql host folder to the /var/lib/mysql/data container folder |
| Container image | registry.redhat.io/rhel8/mysql-80:1                                                        |
| Port forward    | yes, Bind host port 13306 to container port 3306                                           |

Use the following environment variables for the container:

| Environment Variable | Value    |
|----------------------|----------|
| MYSQL_USER           | user1    |
| MYSQL_PASSWORD       | mypa55   |
| MYSQL_DATABASE       | items    |
| MYSQL_ROOT_PASSWORD  | r00tpa55 |

5.1. Create and start the container.

```
[student@workstation ~]$ podman run --name mysql-2 -p 13306:3306 \
> -d -v /home/student/local/mysql:/var/lib/mysql/data \
> -e MYSQL_USER=user1 -e MYSQL_PASSWORD=mypa55 \
> -e MYSQL_DATABASE=items -e MYSQL_ROOT_PASSWORD=r00tpa55 \
> registry.redhat.io/rhel8/mysql-80:1
281c0e2790e54cd5a0b8e2a8cb6e3969981b85cde8ac611bf7ea98ff78bdffb
```

5.2. Verify that the container was started correctly.

```
[student@workstation ~]$ podman ps --format="{{.ID}} {{.Names}}"
281c0e2790e5 mysql-2
```

6. Save the list of all containers (including stopped ones) to the /tmp/my-containers file.

6.1. Use the podman command to save the information in /tmp/my-containers.

```
[student@workstation ~]$ podman ps -a > /tmp/my-containers
```

7. Access the Bash shell inside the container and verify that the items database and the Item table are still available. Confirm also that the table contains data.

7.1. Access the Bash shell inside the container.

```
[student@workstation ~]$ podman exec -it mysql-2 /bin/bash
```

7.2. Connect to the MySQL server.

```
bash-4.4$ mysql -uroot
Welcome to the MySQL monitor. Commands end with ; or \g.

...output omitted...

mysql>
```

7.3. List all databases and confirm that the `items` database is available.

```
mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| items |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.03 sec)
```

7.4. List all tables from the `items` database and verify that the `Item` table is available.

```
mysql> USE items;
Database changed

mysql> SHOW TABLES;
+-----+
| Tables_in_items |
+-----+
| Item |
+-----+
1 row in set (0.01 sec)
```

7.5. View the data from the table.

```
mysql> SELECT * FROM Item;
+---+-----+---+
| id | description | done |
+---+-----+---+
| 1 | Pick up newspaper | 0 |
| 2 | Buy groceries | 1 |
+---+-----+---+
```

7.6. Exit from the MySQL client and from the container shell.

```
mysql> exit
Bye
bash-4.4$ exit
exit
[student@workstation ~]$
```

8. Using port forwarding, insert a new row into the `Item` table. The row should have a `description` value of `Finished lab`, and a `done` value of 1.

8.1. Connect to the MySQL database.

```
[student@workstation ~]$ mysql -uuser1 -h workstation.lab.example.com \
> -pmypa55 -P13306 items
...output omitted...

Welcome to the MySQL monitor. Commands end with ; or \g.
...output omitted...

mysql>
```

8.2. Insert the new row.

```
mysql> INSERT INTO Item (description, done) VALUES ('Finished lab', 1);
Query OK, 1 row affected (0.00 sec)
```

8.3. Exit from the MySQL client.

```
mysql> exit
Bye
[student@workstation ~]$
```

9. Because the first container is not required any more, remove it to release resources.

9.1. Use the following command to remove the container:

```
[student@workstation ~]$ podman rm mysql-1
616azfaa55x866e7eb18b1fd0423a5461d8f24c147b1ad8668b76e6167587cdd
```

## Evaluation

Grade your work by running the `lab manage-review grade` command from your `workstation` machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab manage-review grade
```

## Finish

On `workstation`, run the `lab manage-review finish` command to complete this lab.

```
[student@workstation ~]$ lab manage-review finish
```

This concludes the lab.

# Summary

---

In this chapter, you learned:

- Podman has subcommands to: create a new container (`run`), delete a container (`rm`), list containers (`ps`), stop a container (`stop`), and start a process in a container (`exec`).
- Default container storage is ephemeral, meaning its contents are not present after the container is removed.
- Containers can use a folder from the host file system to work with persistent data.
- Podman mounts volumes in a container with the `-v` option in the `podman run` command.
- The `podman exec` command starts an additional process inside a running container.
- Podman maps local ports to container ports by using the `-p` option in the `run` subcommand.

## Chapter 4

# Managing Container Images

### Goal

Manage the lifecycle of a container image from creation to deletion.

### Objectives

- Search for and pull images from remote registries.
- Export, import, and manage container images locally and in a registry.

### Sections

- Accessing Registries (and Quiz)
- Manipulating Container Images (and Guided Exercise)

### Lab

- Managing Container Images

# Accessing Registries

---

## Objectives

After completing this section, students should be able to:

- Search for and pull images from remote registries using Podman commands and the registry REST API.
- List the advantages of using a certified public registry to download secure images.
- Customize the configuration of Podman to access alternative container image registries.
- List images downloaded from a registry to the local file system.
- Manage tags to pull tagged images.

## Public Registries

Image registries are services offering container images to download. They allow image creators and maintainers to store and distribute container images to public or private audiences.

Podman searches for and downloads container images from public and private registries. Red Hat Container Catalog is the public image registry managed by Red Hat. It hosts a large set of container images, including those provided by major open source projects, such as Apache, MySQL, and Jenkins. All images in the Container Catalog are vetted by the Red Hat internal security team and all components have been rebuilt by Red Hat to avoid known security vulnerabilities.

Red Hat container images provide the following benefits:

- *Trusted source*: All container images comprise sources known and trusted by Red Hat.
- *Original dependencies*: None of the container packages have been tampered with, and only include known libraries.
- *Vulnerability-free*: Container images are free of known vulnerabilities in the platform components or layers.
- *Runtime protection*: All applications in container images run as non-root users, minimizing the exposure surface to malicious or faulty applications.
- *Red Hat Enterprise Linux (RHEL) compatible*: Container images are compatible with all RHEL platforms, from bare metal to cloud.
- *Red Hat support*: Red Hat commercially supports the complete stack.

Quay.io is another public image repository sponsored by Red Hat. Quay.io introduces several exciting features, such as server-side image building, fine-grained access controls, and automatic scanning of images for known vulnerabilities.

While Red Hat Container Catalog images are trusted and verified, Quay.io offers live images regularly updated by creators. Quay.io users can create their namespaces, with fine-grained access control, and publish the images they create to that namespace. Container Catalog users rarely or never push new images, but consume trusted images generated by the Red Hat team.

## Private Registries

Image creators or maintainers want to make their images publicly available. However, there are other image creators who prefer to keep their images private due to:

- Company privacy and secret protection.
- Legal restrictions and laws.
- Avoidance of publishing images in development.

In some cases, private images are preferred. Private registries give image creators the control over their images placement, distribution and usage.

## Configuring Registries in Podman



### Note

The following content uses the version 1 format for registry configuration. The version 1 format is deprecated in recent versions of Podman and does not support using registry mirrors, longest-prefix matches, or location rewriting.

Refer to the `containers-registries.conf(5)` man page for further details on the supported registry configuration format and capabilities.

To configure registries for the `podman` command, you need to update the `/etc/containers/registries.conf` file. Edit the `registries` entry in the `[registries.search]` section, adding an entry to the values list:

```
[registries.search]
registries = ["registry.access.redhat.com", "quay.io"]
```



### Note

Use an FQDN and port number to identify a registry. A registry that does not include a port number has a default port number of 5000. If the registry uses a different port, it must be specified. Indicate port numbers by appending a colon (:) and the port number after the FQDN.

Secure connections to a registry require a trusted certificate. To support insecure connections, add the registry name to the `registries` entry in `[registries.insecure]` section of `/etc/containers/registries.conf` file:

```
[registries.insecure]
registries = ['localhost:5000']
```

## Accessing Registries

Podman provides commands that enable you to search for images. Images registries can also be accessed via an API. The following discusses both approaches.

## Searching for Images in Registries

The podman search command finds images by image name, user name, or description from all the registries listed in the /etc/containers/registries.conf configuration file. The syntax for the podman search command is shown below:

```
[user@host ~]$ podman search [OPTIONS] <term>
```

The following table displays useful options available for the search subcommand:

| Option                    | Description                                                                                                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --limit <number>          | Limits the number of listed images per registry.                                                                                                                                                                                                                         |
| --filter <filter=value>   | Filter output based on conditions provided. Supported filters are: stars=<number>: Show only images with at least this number of stars. is-automated=<true false>: Show only images automatically built. is-official=<true false>: Show only images flagged as official. |
| --tls-verify <true false> | Enables or disables HTTPS certificate validation for all used registries.                                                                                                                                                                                                |
| --list-tags               | List the available tags in the repository for the specified image.                                                                                                                                                                                                       |

## Registry HTTP API

A remote registry exposes web services that provide an application programming interface (API) to the registry. Podman uses these interfaces to access and interact with remote repositories. Many registries conform to the Docker Registry HTTP API v2 specification, which exposes a standardized REST interface for registry interaction. You can use this REST interface to directly interact with a registry, instead of using Podman.

Examples for using this API with curl commands are shown below:

To list all repositories available in a registry, use the /v2/\_catalog endpoint. The n parameter is used to limit the number of repositories to return:

```
[user@host ~]$ curl -Ls https://myserver/v2/_catalog?n=3
{"repositories":["centos/httpd","do180/custom-httdp","hello-openshift"]}
```

**Note**

If Python is available, use it to format the JSON response:

```
[user@host ~]$ curl -Ls https://myserver/v2/_catalog?n=3 \
> | python -m json.tool
{
 "repositories": [
 "centos/httpd",
 "do180/custom-httpd",
 "hello-openshift"
]
}
```

The /v2/<name>/tags/list endpoint provides the list of tags available for a single image:

```
[user@host ~]$ curl -Ls \
> https://quay.io/v2/redhattraining/httpd-parent/tags/list \
> | python -m json.tool
{
 "name": "redhattraining/httpd-parent",
 "tags": [
 "latest",
 "2.4"
]
}
```

**Note**

Quay.io offers a dedicated API to interact with repositories beyond what is specified in Docker Repository API. See <https://docs.quay.io/api/> for details.

## Registry Authentication

Some container image registries require access authorization. The `podman login` command allows username and password authentication to a registry:

```
[user@host ~]$ podman login -u username \
> -p password registry.access.redhat.com
Login Succeeded!
```

The registry HTTP API requires authentication credentials. First, use the Red Hat Single Sign On (SSO) service to obtain an access token:

```
[user@host ~]$ curl -u username:password -Ls \
> "https://sso.redhat.com/auth/realms/rhcc/protocol/redhat-docker-v2/auth?
service=docker-registry"
{"token":"eyJ...o5G8",
"access_token":"eyJh...mgL4",
"expires_in":...output omitted...}[user@host ~]$
```

Then, include this token in a `Bearer` authorization header in subsequent requests:

```
[user@host ~]$ curl -H "Authorization: Bearer eyJh...mgL4" \
> -Ls https://registry.redhat.io/v2/rhel8/mysql-80/tags/list \
> | python -mjson.tool
{
 "name": "rhel8/mysql-80",
 "tags": [
 "1.0",
 "1.2",
 ...output omitted...
```



### Note

Other registries may require different steps to provide credentials. If a registry adheres to the Docker Registry HTTP v2 API, authentication conforms to the RFC7235 scheme.

## Pulling Images

To pull container images from a registry, use the `podman pull` command:

```
[user@host ~]$ podman pull [OPTIONS] [REGISTRY[:PORT]/]NAME[:TAG]
```

The `podman pull` command uses the image name obtained from the search subcommand to pull an image from a registry. The `pull` subcommand allows adding the registry name to the image. This variant supports having the same image in multiple registries.

For example, to pull an NGINX container from the quay.io registry, use the following command:

```
[user@host ~]$ podman pull quay.io/bitnami/nginx
```



### Note

If the image name does not include a registry name, Podman searches for a matching container image using the registries listed in the `/etc/containers/registries.conf` configuration file. Podman searches for images in registries in the same order they appear in the configuration file.

Red Hat recommends always including the registry name to prevent accidental use of unexpected images.

Malicious actors can upload images to registries. If these registries appear first in your configuration, then you use the image uploaded by a malicious actor instead of the image you intend to use.

## Listing Local Copies of Images

Any container image downloaded from a registry is stored locally on the same host where the `podman` command is executed. This behavior avoids repeating image downloads and minimizes the deployment time for a container. Podman also stores any custom container images you build in the same local storage.

**Note**

By default, Podman stores container images in the `/var/lib/containers/storage/overlay-images` directory.

Podman provides an `images` subcommand to list all the container images stored locally:

```
[user@host ~]$ podman images
REPOSITORY TAG IMAGE ID CREATED SIZE
registry.redhat.io/rhel8/mysql-80 latest ad5a0e6d030f 3 weeks ago 588 MB
```

## Image Tags

An image tag is a mechanism to support multiple releases of the same image. This feature is useful when multiple versions of the same software are provided, such as a production-ready container or the latest updates of the same software developed for community evaluation. Any Podman subcommand that requires a container image name accepts a tag parameter to differentiate between multiple tags. If an image name does not contain a tag, then the tag value defaults to `latest`. For example, to pull an image with the tag `1` from `rhe18/mysql-80`, use the following command:

```
[user@host ~]$ podman pull registry.redhat.io/rhel8/mysql-80:1
```

To start a new container based on the `rhe18/mysql-80:1` image, use the following command:

```
[user@host ~]$ podman run registry.redhat.io/rhel8/mysql-80:1
```

**References****Red Hat Container Catalog**

<https://registry.redhat.io>

**Quay.io**

<https://quay.io>

**Docker Registry HTTP API V2**

<https://github.com/docker/distribution/blob/master/docs/spec/api.md>

**RFC7235 - HTTP/1.1: Authentication**

<https://tools.ietf.org/html/rfc7235>

## ► Quiz

# Working with Registries



### Note

The following quiz uses the version 1 format for registry configuration. The version 1 format is deprecated in recent versions of Podman and does not support using registry mirrors, longest-prefix matches, or location rewriting.

Refer to the `containers-registries.conf(5)` man page for further details on the supported registry configuration format and capabilities.

Choose the correct answers to the following questions, based on the following information:

Podman is available on a RHEL host with the following entry in `/etc/containers/registries.conf` file:

```
[registries.search]
registries = ["registry.redhat.io", "quay.io"]
```

The `registry.redhat.io` and `quay.io` hosts have a registry running, both have valid certificates, and use the version 1 registry. The following images are available for each host:

#### Image names/tags per registry

| Registry                        | Image                                                                                                                                            |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>registry.redhat.io</code> | <ul style="list-style-type: none"> <li>• <code>nginx:1.1.6</code></li> <li>• <code>mysql:8.0</code></li> <li>• <code>httpd:2.4</code></li> </ul> |
| <code>quay.io</code>            | <ul style="list-style-type: none"> <li>• <code>mysql:5.7</code></li> <li>• <code>httpd:2.4</code></li> </ul>                                     |

No images are locally available.

- 1. Which two commands display `mysql` images available for download from `registry.redhat.io`? (Choose two.)
- `podman search registry.redhat.io/mysql`
  - `podman images`
  - `podman pull mysql`
  - `podman search mysql`

► 2. Which command is used to list all available image tags for the httpd container image?

- a. podman search --list-tags httpd
- b. podman images httpd
- c. podman pull --all-tags=true httpd
- d. There is no podman command available to search for tags.

► 3. Which two commands pull the httpd image with the 2.4 tag? (Choose two.)

- a. podman pull httpd:2.4
- b. podman pull httpd:latest
- c. podman pull quay.io/httpd
- d. podman pull registry.redhat.io/httpd:2.4

► 4. When running the following commands, what container images will be downloaded?

```
[user@host ~]$ podman pull registry.redhat.io/httpd:2.4
[user@host ~]$ podman pull quay.io/mysql:8.0
```

- a. quay.io/httpd:2.4, and `registry.redhat.io/mysql:8.0
- b. registry.redhat.io/httpd:2.4, and registry.redhat.io/mysql:8.0
- c. registry.redhat.io/httpd:2.4, no image will be downloaded for mysql.
- d. quay.io/httpd:2.4, no image will be downloaded for mysql.

## ► Solution

# Working with Registries



### Note

The following quiz uses the version 1 format for registry configuration. The version 1 format is deprecated in recent versions of Podman and does not support using registry mirrors, longest-prefix matches, or location rewriting.

Refer to the `containers-registries.conf(5)` man page for further details on the supported registry configuration format and capabilities.

Choose the correct answers to the following questions, based on the following information:

Podman is available on a RHEL host with the following entry in `/etc/containers/registries.conf` file:

```
[registries.search]
registries = ["registry.redhat.io", "quay.io"]
```

The `registry.redhat.io` and `quay.io` hosts have a registry running, both have valid certificates, and use the version 1 registry. The following images are available for each host:

#### Image names/tags per registry

| Registry                        | Image                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <code>registry.redhat.io</code> | <ul style="list-style-type: none"> <li><code>nginx:1.1.6</code></li> <li><code>mysql:8.0</code></li> <li><code>httpd:2.4</code></li> </ul> |
| <code>quay.io</code>            | <ul style="list-style-type: none"> <li><code>mysql:5.7</code></li> <li><code>httpd:2.4</code></li> </ul>                                   |

No images are locally available.

- 1. Which two commands display `mysql` images available for download from `registry.redhat.io`? (Choose two.)
- `podman search registry.redhat.io/mysql`
  - `podman images`
  - `podman pull mysql`
  - `podman search mysql`

► 2. Which command is used to list all available image tags for the httpd container image?

- a. podman search --list-tags httpd
- b. podman images httpd
- c. podman pull --all-tags=true httpd
- d. There is no podman command available to search for tags.

► 3. Which two commands pull the httpd image with the 2.4 tag? (Choose two.)

- a. podman pull httpd:2.4
- b. podman pull httpd:latest
- c. podman pull quay.io/httpd
- d. podman pull registry.redhat.io/httpd:2.4

► 4. When running the following commands, what container images will be downloaded?

```
[user@host ~]$ podman pull registry.redhat.io/httpd:2.4
[user@host ~]$ podman pull quay.io/mysql:8.0
```

- a. quay.io/httpd:2.4, and `registry.redhat.io/mysql:8.0
- b. registry.redhat.io/httpd:2.4, and registry.redhat.io/mysql:8.0
- c. registry.redhat.io/httpd:2.4, no image will be downloaded for mysql.
- d. quay.io/httpd:2.4, no image will be downloaded for mysql.

# Manipulating Container Images

## Objectives

After completing this section, students should be able to:

- Save and load container images to local files.
- Delete images from the local storage.
- Create new container images from containers and update image metadata.
- Manage image tags for distribution purposes.

## Introduction

There are various ways to manage image containers while adhering to DevOps principles. For example, a developer finishes testing a custom container in a machine and needs to transfer this container image to another host for another developer, or to a production server. There are two ways to do this:

1. Save the container image to a .tar file.
2. Publish (*push*) the container image to an image registry.



### Note

One of the ways a developer could have created this custom container is discussed later in this chapter (`podman commit`). However, in the following chapters we discuss the recommended way to do so using `Containerfiles`.

## Saving and Loading Images

Existing images from the Podman local storage can be saved to a .tar file using the `podman save` command. The generated file is not a regular TAR archive; it contains image metadata and preserves the original image layers. Using this file, Podman can recreate the original image.

The general syntax of the `save` subcommand is as follows:

```
[user@host ~]$ podman save [-o FILE_NAME] IMAGE_NAME[:TAG]
```

Podman sends the generated image to the standard output as binary data. To avoid that, use the `-o` option.

The following example saves the previously downloaded MySQL container image from the Red Hat Container Catalog to the `mysql.tar` file:

```
[user@host ~]$ podman save \
> -o mysql.tar registry.redhat.io/rhel8/mysql-80
```

## Chapter 4 | Managing Container Images

Note the use of the `-o` option in this example.

Use the `.tar` files generated by the `save` subcommand for backup purposes. To restore the container image, use the `podman load` command. The general syntax of the command is as follows:

```
[user@host ~]$ podman load [-i FILE_NAME]
```

The `load` command is the opposite of the `save` command.

For example, this command would load an image saved in a file named `mysql.tar`:

```
[user@host ~]$ podman load -i mysql.tar
```

If the `.tar` file given as an argument is not a container image with metadata, the `podman load` command fails.



### Note

To save disk space, compress the file generated by the `save` subcommand with Gzip using the `--compress` parameter. The `load` subcommand uses the `gunzip` command before importing the file to the local storage.

## Deleting Images

Podman keeps any image downloaded in its local storage, even the ones currently unused by any container. However, images can become outdated, and should be subsequently replaced.



### Note

Any updates to images in a registry are not automatically updated. The image must be removed and then pulled again to guarantee that the local storage has the latest version of an image.

To delete an image from the local storage, run the `podman rmi` command.

```
[user@host ~]$ podman rmi [OPTIONS] IMAGE [IMAGE...]
```

An image can be referenced using the name or the ID for removal purposes. Podman cannot delete images while containers are using that image. You must stop and remove all containers using that image before deleting it.

To avoid this, the `rmi` subcommand has the `--force` option. This option forces the removal of an image even if that the image is used by several containers or these containers are running. Podman stops and removes all containers using the forcefully removed image before removing it.

## Deleting All Images

To delete all images that are not used by any container, use the following command:

```
[user@host ~]$ podman rmi -a
```

The command returns all the image IDs available in the local storage and passes them as parameters to the `podman rmi` command for removal. Images that are in use are not deleted. However, this does not prevent any unused images from being removed.

## Modifying Images

Ideally, all container images should be built using a `Containerfile`, in order to create a clean, lightweight set of image layers without log files, temporary files, or other artifacts created by the container customization. However, some users may provide container images as they are, without a `Containerfile`. As an alternative approach to creating new images, change a running container in place and save its layers to create a new container image. The `podman commit` command provides this feature.



### Warning

Even though the `podman commit` command is the most straightforward approach to creating new images, it is not recommended because of the image size (`commit` keeps logs and process ID files in the captured layers), and the lack of change traceability. A `Containerfile` provides a robust mechanism to customize and implement changes to a container using a human-readable set of commands, without the set of files that are generated by the operating system.

The syntax for the `podman commit` command is as follows:

```
[user@host ~]$ podman commit [OPTIONS] CONTAINER \
> [REPOSITORY[:PORT]/]IMAGE_NAME[:TAG]
```

The following table shows the most important options available for the `podman commit` command:

| Option                    | Description                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------------------|
| <code>--author ""</code>  | Identifies who created the container image.                                                   |
| <code>--message ""</code> | Includes a commit message to the registry.                                                    |
| <code>--format</code>     | Selects the format of the image. Valid options are <code>oci</code> and <code>docker</code> . |



### Note

The `--message` option is not available in the default OCI container format.

To find the ID of a running container in Podman, run the `podman ps` command:

```
[user@host ~]$ podman ps
CONTAINER ID IMAGE ...
87bdfcc7c656 mysql ...output omitted... mysql-basic
```

Eventually, administrators might customize the image and set the container to the desired state. To identify which files were changed, created, or deleted since the container was started, use the `diff` subcommand. This subcommand only requires the container name or container ID:

```
[user@host ~]$ podman diff mysql-basic
C /run
C /run/mysql
A /run/mysql/mysql.pid
A /run/mysql/mysql.sock
A /run/mysql/mysql.sock.lock
A /run/secrets
```

The `diff` subcommand tags any added file with an A, any changed ones with a C, and any deleted file with a D.



### Note

The `diff` command only reports added, changed, or deleted files to the container file system. Files that are mounted to a running container are not considered part of the container file system. To retrieve the list of mounted files and directories for a running container, use the `podman inspect` command:

```
[user@host ~]$ podman inspect \
> -f "{{range .Mounts}}{{println .Destination}}{{end}}" CONTAINER_NAME/ID
```

Any file in this list, or file under a directory in this list, is not shown in the output of the `podman diff` command.

To commit the changes to another image, run the following command:

```
[user@host ~]$ podman commit mysql-basic mysql-custom
```

The previous example creates a new image named `mysql-custom`.

## Tagging Images

A project with multiple images based on the same software could be distributed, creating individual projects for each image, but this approach requires more maintenance for managing and deploying the images to the correct locations.

Container image registries support tags to distinguish multiple releases of the same project. For example, a customer might use a container image to run with a MySQL or PostgreSQL database, using a tag as a way to differentiate which database is to be used by a container image.



### Note

Usually, the tags are used by container developers to distinguish between multiple versions of the same software. Multiple tags are provided to identify a release easily. The official MySQL container image website uses the version as the tag's name (8.0). Also, the same image might have a second tag with the minor version to minimize the need to get the latest release for a specific version.

To tag an image, use the `podman tag` command:

```
[user@host ~]$ podman tag [OPTIONS] IMAGE[:TAG] \
> [REGISTRYHOST/]USERNAME/]NAME[:TAG]
```

The `IMAGE` argument is the image name with an optional tag, which is managed by Podman. The following argument refers to the new alternative name for the image. Podman assumes the latest version, as indicated by the `latest` tag, if the tag value is absent. For example, to tag an image, use the following command:

```
[user@host ~]$ podman tag mysql-custom devops/mysql
```

The `mysql-custom` option corresponds to the image name in the container registry.

To use a different tag name, use the following command instead:

```
[user@host ~]$ podman tag mysql-custom devops/mysql:snapshot
```

## Removing Tags from Images

A single image can have multiple tags assigned using the `podman tag` command. To remove them, use the `podman rmi` command, as mentioned earlier:

```
[user@host ~]$ podman rmi devops/mysql:snapshot
```



### Note

Because multiple tags can point to the same image, to remove an image referred to by multiple tags, first remove each tag individually.

## Best Practices for Tagging Images

Podman automatically adds the `latest` tag if you do not specify any tag, because Podman considers the image to be the latest build. However, this may not be true depending on how each project uses tags. For example, many open source projects consider the `latest` tag to match the most recent release, but not the latest build.

Moreover, multiple tags are provided to minimize the need to remember the latest release of a particular version of a project. Thus, if there is a project version release, for example, `2.1.10`, another tag named `2.1` can be created pointing to the same image from the `2.1.10` release. This simplifies pulling images from the registry.

## Publishing Images to a Registry

To publish an image to a registry, it must reside in the Podman local storage and be tagged for identification purposes. To push the image to the registry, use the `push` subcommand:

```
[user@host ~]$ podman push [OPTIONS] IMAGE [DESTINATION]
```

For example, to push the `bitnami/nginx` image to its repository, use the following command:

```
[user@host ~]$ podman push quay.io/bitnami/nginx
```

The previous example pushes the image to Quay.io.



### References

#### Podman site

<https://podman.io/>

## ► Guided Exercise

# Creating a Custom Apache Container Image

In this guided exercise, you will create a custom Apache container image using the `podman commit` command.

## Outcomes

You should be able to create a custom container image.

## Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from Chapter 1 before executing any command of this practice.

Open a terminal on the `workstation` machine as the `student` user and run the following command:

```
[student@workstation ~]$ lab image-operations start
```

## Instructions

- 1. Log in to your Quay.io account and start a container by using the image available at `quay.io/redhattraining/httpd-parent`. The `-p` option allows you to specify a redirect port. In this case, Podman forwards incoming requests on TCP port 8180 of the host to TCP port 80 of the container.

```
[student@workstation ~]$ podman login quay.io
Username: your_quay_username
Password: your_quay_password
Login Succeeded!

[student@workstation ~]$ podman run -d --name official-httpd \
> -p 8180:80 quay.io/redhattraining/httpd-parent
Trying to pull quay.io/redhattraining/httpd-parent:latest...
Getting image source signatures
Copying blob a3ed95caeb02 done
...output omitted...
Writing manifest to image destination
Storing signatures
3a6baecaff2b4e8c53b026e04847dda5976b773ade1a3a712b1431d60ac5915d
```

Your last line of output is different from the last line shown above. Note the first twelve characters.

- 2. Create an HTML page on the `official-httpd` container.

- 2.1. Access the shell of the container by using the `podman exec` command and create an HTML page.

```
[student@workstation ~]$ podman exec -it official-httdp /bin/bash
bash-4.4# echo "DO180 Page" > /var/www/html/do180.html
```

- 2.2. Exit from the container.

```
bash-4.4# exit
exit
```

- 2.3. Ensure that the HTML file is reachable from the workstation machine by using the `curl` command.

```
[student@workstation ~]$ curl 127.0.0.1:8180/do180.html
```

The expected output is similar to the following:

```
DO180 Page
```

- 3. Use the `podman diff` command to examine the differences in the container between the image and the new layer created by the container.

```
[student@workstation ~]$ podman diff official-httdp
C /etc
C /root
A /root/.bash_history
...output omitted...
C /tmp
C /var
C /var/log
C /var/log/httpd
A /var/log/httpd/access_log
A /var/log/httpd/error_log
C /var/www
C /var/www/html
A /var/www/html/do180.html
```



### Note

Often, web server container images label the `/var/www/html` directory as a volume. In these cases, any files added to this directory are not considered part of the container file system, and would not show in the output of the `podman diff` command.

The `quay.io/redhattraining/httpd-parent` container image does not label the `/var/www/html` directory as a volume. As a result, the change to the `/var/www/html/do180.html` file is considered a change to the underlying container file system.

- 4. Create a new image with the changes created by the running container.

- 4.1. Stop the `official-httdp` container.

```
[student@workstation ~]$ podman stop official-httdp
official-httdp
```

- 4.2. Commit the changes to a new container image with a new name. Use your name as the author of the changes.

```
[student@workstation ~]$ podman commit -a 'Your Name' \
> official-httdp do180-custom-httdp
Getting image source signatures
...output omitted...
Copying blob 7f9108fde4a1 skipped: already exists
Copying blob 4c0f28c7efd0 done
Copying config 5c2bb39b76 done
Writing manifest to image destination
Storing signatures
31c3ac78e9d4137c928da23762e7d32b00c428eb1036cab1caeeb399befef2a23
```

- 4.3. List the available container images.

```
[student@workstation ~]$ podman images
```

The expected output is similar to the following:

| REPOSITORY                          | TAG    | IMAGE ID            | CREATED | SIZE |
|-------------------------------------|--------|---------------------|---------|------|
| localhost/do180-custom-httdp        | latest | <b>31c3ac78e9d4</b> | ...     | ...  |
| quay.io/redhattraining/httdp-parent | latest | 2cc07fbb5000        | ...     | ...  |

The image ID matches the first 12 characters of the hash. The most recent images are listed at the top.

- 5. Publish the saved container image to the container registry.

- 5.1. Load your classroom environment configuration.

Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```

- 5.2. To tag the image with the registry host name and tag, run the following command.

```
[student@workstation ~]$ podman tag do180-custom-httdp \
> quay.io/${RHT_OCP4_QUAY_USER}/do180-custom-httdp:v1.0
```

- 5.3. Run the `podman images` command to ensure that the new name has been added to the cache.

```
[student@workstation ~]$ podman images
REPOSITORY TAG IMAGE ID
localhost/do180-custom-httdp latest 31c3ac78e9d4 ...
quay.io/${RHT_OCP4_QUAY_USER}/do180-custom-httdp v1.0 31c3ac78e9d4 ...
quay.io/redhattraining/httpd-parent latest 2cc07fbb5000 ...
```

- 5.4. Publish the image to your Quay.io registry.

```
[student@workstation ~]$ podman push \
> quay.io/${RHT_OCP4_QUAY_USER}/do180-custom-httdp:v1.0
Getting image source signatures
...output omitted...
Copying blob 24d85c895b6b skipped: already exists
Copying config 5c2bb39b76 done
Writing manifest to image destination
Storing signatures
```



### Note

Pushing the `do180-custom-httdp` image creates a private repository in your Quay.io account. Currently, private repositories are disallowed by Quay.io free plans. You can either create the public repository prior to pushing the image, or change the repository to public afterwards.

- 5.5. Verify that the image is available from Quay.io. The `podman search` command requires the image to be indexed by Quay.io. That may take some hours to occur, so use the `podman pull` command to fetch the image. This proves that the image is available.

```
[student@workstation ~]$ podman pull \
> -q quay.io/${RHT_OCP4_QUAY_USER}/do180-custom-httdp:v1.0
31c3ac78e9d4137c928da23762e7d32b00c428eb1036cab1caeeb3
```

6. Create a container from the newly published image.

Use the `podman run` command to start a new container. Use `your_quay_username/do180-custom-httdp:v1.0` as the base image.

```
[student@workstation ~]$ podman run -d --name test-httdp -p 8280:80 \
> ${RHT_OCP4_QUAY_USER}/do180-custom-httdp:v1.0
c0f04e906bb12bd0e514cbd0e581d2746e04e44a468dfbc85bc29ffcc5acd16c
```

7. Use the `curl` command to access the HTML page. Make sure you use port 8280.

This should display the HTML page created in the previous step.

```
[student@workstation ~]$ curl http://localhost:8280/do180.html
DO180 Page
```

## Finish

On workstation, run the `lab image-operations finish` script to complete this lab.

```
[student@workstation ~]$ lab image-operations finish
```

This concludes the guided exercise.

## ▶ Lab

# Managing Images

## Outcomes

You should be able to create a custom container image and manage container images.

## Before You Begin

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab image-review start
```

## Instructions

1. Use the `podman pull` command to download the `quay.io/redhattraining/nginx:1.17` container image. This image is a copy of the official container image available at `docker.io/library/nginx:1.17`.  
Ensure that you successfully downloaded the image.
2. Start a new container using the Nginx image, according to the specifications listed in the following list.

| Property        | Description                                                  |
|-----------------|--------------------------------------------------------------|
| Name            | <code>official-nginx</code>                                  |
| Run as daemon   | <code>yes</code>                                             |
| Container image | <code>quay.io/redhattraining/nginx:1.17</code>               |
| Port forward    | <code>yes</code> , from host port 8080 to container port 80. |

3. Log in to the container using the `podman exec` command. Replace the contents of the `index.html` file with `D0180`. The web server directory is located at `/usr/share/nginx/html`.  
After the file has been updated, exit the container and use the `curl` command to access the web page.
4. Stop the running container and commit your changes to create a new container image. Give the new image a name of `do180/mynginx` and a tag of `v1.0-SNAPSHOT`. Use the following specifications:

| Property    | Description                |
|-------------|----------------------------|
| Image name  | <code>do180/mynginx</code> |
| Image tag   | <code>v1.0-SNAPSHOT</code> |
| Author name | <code>your name</code>     |

5. Start a new container using the updated Nginx image, according to the specifications listed in the following list.

| Property        | Description                                    |
|-----------------|------------------------------------------------|
| Name            | official-nginx-dev                             |
| Run as daemon   | yes                                            |
| Container image | do180/mynginx:v1.0-SNAPSHOT                    |
| Port forward    | yes, from host port 8080 to container port 80. |

6. Log in to the container using the `podman exec` command, and introduce a final change. Replace the contents of the file `/usr/share/nginx/html/index.html` file with D0180 Page.  
After the file has been updated, exit the container and use the `curl` command to verify the changes.
7. Stop the running container and commit your changes to create the final container image. Give the new image a name of `do180/mynginx` and a tag of `v1.0`. Use the following specifications:

| Property    | Description      |
|-------------|------------------|
| Image name  | do180/mynginx    |
| Image tag   | v1.0             |
| Author name | <i>your name</i> |

8. Remove the development image `do180/mynginx:v1.0-SNAPSHOT` from local image storage.
9. Use the image tagged `do180/mynginx:v1.0` to create a new container with the following specifications:

| Property        | Description                                   |
|-----------------|-----------------------------------------------|
| Name            | my-nginx                                      |
| Run as daemon   | yes                                           |
| Container image | do180/mynginx:v1.0                            |
| Port forward    | yes, from host port 8280 to container port 80 |

On workstation, use the `curl` command to access the web server, accessible from the port 8280.

## Evaluation

Grade your work by running the `lab image-review grade` command on your workstation machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab image-review grade
```

## Finish

On workstation, run the `lab image-review finish` command to complete this lab.

```
[student@workstation ~]$ lab image-review finish
```

This concludes the lab.

## ► Solution

# Managing Images

### Outcomes

You should be able to create a custom container image and manage container images.

### Before You Begin

Open a terminal on workstation as the `student` user and run the following command:

```
[student@workstation ~]$ lab image-review start
```

### Instructions

1. Use the `podman pull` command to download the `quay.io/redhattraining/nginx:1.17` container image. This image is a copy of the official container image available at [docker.io/library/nginx:1.17](https://docker.io/library/nginx:1.17).  
Ensure that you successfully downloaded the image.

- 1.1. Use the `podman pull` command to pull the Nginx container image.

```
[student@workstation ~]$ podman pull quay.io/redhattraining/nginx:1.17
Trying to pull quay.io/redhattraining/nginx:1.17...
...output omitted...
Storing signatures
9beeba249f3ee158d3e495a6ac25c5667ae2de8a43ac2a8bfd2bf687a58c06c9
```

- 1.2. Ensure that the container image exists on the local system by running the `podman images` command.

```
[student@workstation ~]$ podman images
```

This command produces output similar to the following:

| REPOSITORY                   | TAG  | IMAGE ID     | CREATED      | SIZE  |
|------------------------------|------|--------------|--------------|-------|
| quay.io/redhattraining/nginx | 1.17 | 9beeba249f3e | 6 months ago | 428MB |

2. Start a new container using the Nginx image, according to the specifications listed in the following list.

| Property        | Description                                    |
|-----------------|------------------------------------------------|
| Name            | official-nginx                                 |
| Run as daemon   | yes                                            |
| Container image | quay.io/redhattraining/nginx:1.17              |
| Port forward    | yes, from host port 8080 to container port 80. |

- 2.1. On workstation, use the podman run command to create a container named official-nginx.

```
[student@workstation ~]$ podman run --name official-nginx \
> -d -p 8080:80 quay.io/redhattraining/nginx:1.17
b9d5739af239914b371025c38340352ac1657358561e7ebbd5472dfd5ff97788
```

3. Log in to the container using the podman exec command. Replace the contents of the index.html file with D0180. The web server directory is located at /usr/share/nginx/html.

After the file has been updated, exit the container and use the curl command to access the web page.

- 3.1. Log in to the container by using the podman exec command.

```
[student@workstation ~]$ podman exec -it official-nginx /bin/bash
root@b9d5739af239:/#
```

- 3.2. Update the index.html file located at /usr/share/nginx/html. The file should read D0180.

```
root@b9d5739af239:/# echo 'D0180' > /usr/share/nginx/html/index.html
```

- 3.3. Exit the container.

```
root@b9d5739af239:/# exit
exit
```

- 3.4. Use the curl command to ensure that the index.html file is updated.

```
[student@workstation ~]$ curl 127.0.0.1:8080
D0180
```

4. Stop the running container and commit your changes to create a new container image. Give the new image a name of do180/mynginx and a tag of v1.0-SNAPSHOT. Use the following specifications:

| Property    | Description      |
|-------------|------------------|
| Image name  | do180/mynginx    |
| Image tag   | v1.0-SNAPSHOT    |
| Author name | <i>your name</i> |

- 4.1. Use the `podman stop` command to stop the `official-nginx` container.

```
[student@workstation ~]$ podman stop official-nginx
official-nginx
```

- 4.2. Commit your changes to a new container image. Use your name as the author of the changes.

```
[student@workstation ~]$ podman commit -a 'Your Name' \
> official-nginx do180/mynginx:v1.0-SNAPSHOT
Getting image source signatures
...output omitted...
Copying blob 1e69eb596a89 done
Copying config e8c32f0b53 done
Writing manifest to image destination
Storing signatures
d6d10f52e258e4e88c181a56c51637789424e9261b208338404e82a26c960751
```

- 4.3. List the available container images to locate your newly created image.

```
[student@workstation ~]$ podman images
REPOSITORY TAG IMAGE ID CREATED ...
localhost/do180/mynginx v1.0-SNAPSHOT d6d10f52e258 30 seconds ago ...
quay.io/redhattraining/nginx 1.17 9beeba249f3e 6 months ago ...
```

5. Start a new container using the updated Nginx image, according to the specifications listed in the following list.

| Property        | Description                                    |
|-----------------|------------------------------------------------|
| Name            | <code>official-nginx-dev</code>                |
| Run as daemon   | yes                                            |
| Container image | <code>do180/mynginx:v1.0-SNAPSHOT</code>       |
| Port forward    | yes, from host port 8080 to container port 80. |

- 5.1. On workstation, use the `podman run` command to create a container named `official-nginx-dev`.

```
[student@workstation ~]$ podman run --name official-nginx-dev \
> -d -p 8080:80 do180/mynginx:v1.0-SNAPSHOT
cfa21f02a77d0e46e438c255f83dea2dfb89bb5aa72413a28866156671f0bbbb
```

6. Log in to the container using the `podman exec` command, and introduce a final change. Replace the contents of the file `/usr/share/nginx/html/index.html` file with `D0180 Page`.

After the file has been updated, exit the container and use the `curl` command to verify the changes.

- 6.1. Log in to the container by using the `podman exec` command.

```
[student@workstation ~]$ podman exec -it official-nginx-dev /bin/bash
root@cfa21f02a77d:/#
```

- 6.2. Update the `index.html` file located at `/usr/share/nginx/html`. The file should read `D0180 Page`.

```
root@cfa21f02a77d:/# echo 'D0180 Page' > /usr/share/nginx/html/index.html
```

- 6.3. Exit the container.

```
root@cfa21f02a77d:/# exit
exit
```

- 6.4. Use the `curl` command to ensure that the `index.html` file is updated.

```
[student@workstation ~]$ curl 127.0.0.1:8080
D0180 Page
```

7. Stop the running container and commit your changes to create the final container image. Give the new image a name of `do180/mynginx` and a tag of `v1.0`. Use the following specifications:

| Property    | Description                |
|-------------|----------------------------|
| Image name  | <code>do180/mynginx</code> |
| Image tag   | <code>v1.0</code>          |
| Author name | <code>your name</code>     |

- 7.1. Use the ` `podman stop`` command to stop the `official-nginx-dev` container.

```
[student@workstation ~]$ podman stop official-nginx-dev
official-nginx-dev
```

- 7.2. Commit your changes to a new container image. Use your name as the author of the changes.

```
[student@workstation ~]$ podman commit -a 'Your Name' \
> official-nginx-dev do180/mynginx:v1.0
Getting image source signatures
...output omitted...
Copying blob 26d691d5f9e8 done
Copying config 60332a1074 done
Writing manifest to image destination
Storing signatures
90915976c33de534e06778a74d2a8969c25ef5f8f58c0c1ab7aeaac19abd18af
```

- 7.3. List the available container images in order to locate your newly created image.

```
[student@workstation ~]$ podman images
REPOSITORY TAG IMAGE ID CREATED ...
localhost/do180/mynginx v1.0 90915976c33d 6 seconds ago ...
localhost/do180/mynginx v1.0-SNAPSHOT d6d10f52e258 8 minutes ago ...
quay.io/redhattraining/nginx 1.17 9beeba249f3e 6 months ago ...
```

8. Remove the development image do180/mynginx:v1.0-SNAPSHOT from local image storage.
- 8.1. Despite being stopped, the official-nginx-dev is still present. Display the container with the podman ps command with the -a flag.

```
[student@workstation ~]$ podman ps -a --format="{{.ID}} {{.Names}} {{.Status}}"
cfa21f02a77d official-nginx-dev Exited (0) 9 minutes ago
b9d5739af239 official-nginx Exited (0) 12 minutes ago
```

- 8.2. Remove the container with the podman rm command.

```
[student@workstation ~]$ podman rm official-nginx-dev
cfa21f02a77d0e46e438c255f83dea2dfb89bb5aa72413a28866156671f0bbbb
```

- 8.3. Verify that the container is deleted by resubmitting the same podman ps command.

```
[student@workstation ~]$ podman ps -a --format="{{.ID}} {{.Names}} {{.Status}}"
b9d5739af239 official-nginx Exited (0) 12 minutes ago
```

- 8.4. Use the `podman rmi` command to remove the do180/mynginx:v1.0-SNAPSHOT image.

```
[student@workstation ~]$ podman rmi do180/mynginx:v1.0-SNAPSHOT
Untagged: localhost/do180/mynginx:v1.0-SNAPSHOT
```

- 8.5. Verify that the image is no longer present by listing all images using the podman images command.

```
[student@workstation ~]$ podman images
REPOSITORY TAG IMAGE ID CREATED SIZE
localhost/do180/mynginx v1.0 90915976c33d 5 minutes ago 131MB
quay.io/redhattraining/nginx 1.17 9beeba249f3e 6 months ago 131MB
```

9. Use the image tagged do180/mynginx:v1.0 to create a new container with the following specifications:

| Property        | Description                                   |
|-----------------|-----------------------------------------------|
| Name            | my-nginx                                      |
| Run as daemon   | yes                                           |
| Container image | do180/mynginx:v1.0                            |
| Port forward    | yes, from host port 8280 to container port 80 |

On workstation, use the curl command to access the web server, accessible from the port 8280.

- 9.1. Use the `podman run` command to create the my-nginx container, according to the specifications.

```
[student@workstation ~]$ podman run -d --name my-nginx \
> -p 8280:80 do180/mynginx:v1.0
51958c8ec8d2613bd26f85194c66ca96c95d23b82c43b23b0f0fb9fded74da20
```

- 9.2. Use the curl command to ensure that the index.html page is available and returns the custom content.

```
[student@workstation ~]$ curl 127.0.0.1:8280
DO180 Page
```

## Evaluation

Grade your work by running the lab image-review grade command on your workstation machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab image-review grade
```

## Finish

On workstation, run the lab image-review finish command to complete this lab.

```
[student@workstation ~]$ lab image-review finish
```

This concludes the lab.

# Summary

---

In this chapter, you learned:

- The Red Hat Container Catalog provides tested and certified images at [registry.redhat.io](https://registry.redhat.io).
- Podman can interact with remote container registries to search, pull, and push container images.
- Image tags are a mechanism to support multiple releases of a container image.
- Podman provides commands to manage container images both in local storage and as compressed files.
- Use the `podman commit` command to create an image from a container.

## Chapter 5

# Creating Custom Container Images

### Goal

Design and code a Containerfile to build a custom container image.

### Objectives

- Describe the approaches for creating custom container images.
- Create a container image using common Containerfile commands.

### Sections

- Designing Custom Container Images (and Quiz)
- Building Custom Container Images with Containerfiles (and Guided Exercise)

### Lab

- Creating Custom Container Images

# Designing Custom Container Images

## Objectives

After completing this section, students should be able to:

- Describe the approaches for creating custom container images.
- Find existing Containerfiles to use as a starting point for creating a custom container image.
- Define the role played by the Red Hat Software Collections Library (RHSCl) in designing container images from the Red Hat registry.
- Describe the Source-to-Image (S2I) alternative to Containerfiles.

## Reusing Existing Containerfiles

One method of creating container images previously discussed requires that you create a container, modify it to meet the requirements of the application to run in it, and then commit the changes to an image. This option, although straightforward, is only suitable for using or testing very specific changes. It does not follow best software practices, like maintainability, automation of building, and repeatability.

Containerfiles are another option for creating container images that addresses these limitations. Containerfiles are easy to share, version control, reuse, and extend.

Containerfiles also make it easy to extend one image, called a child image, from another image, called a parent image. A child image incorporates everything in the parent image and all changes and additions made to create it.



### Note

For this remainder of this course, a file referred to as a Containerfile can be a file named either *Containerfile* or *Dockerfile*. Both share the same syntax. *Containerfile* is the default name used by OCI compliant tools.

To share and reuse images, many popular applications, languages, and frameworks are already available in public image registries, such as Quay.io [<https://quay.io>]. It is not trivial to customize an application configuration to follow recommended practices for containers, and so starting from a proven parent image usually saves a lot of work.

Using a high-quality parent image enhances maintainability, especially if the parent image is kept updated by its author to account for bug fixes and security issues.

Creating a Containerfile for building a child image from an existing container image is often used in the following typical scenarios:

- Add new runtime libraries, such as database connectors.
- Include organization-wide customization such as SSL certificates and authentication providers.
- Add internal libraries to be shared as a single image layer by multiple container images for different applications.

Changing an existing Containerfile to create a new image can be a sensible approach in other scenarios. For example:

- Trim the container image by removing unused material (such as man pages, or documentation found in /usr/share/doc).
- Lock either the parent image or some included software package to a specific release to lower risk related to future software updates.

Two sources of container images to use, either as parent images or for modification of the Containerfiles, are Docker Hub and the Red Hat Software Collections Library (RHSCl).

## Working with the Red Hat Software Collections Library

Red Hat Software Collections Library (RHSCl), or simply Software Collections, is Red Hat's solution for developers who require the latest development tools that usually do not fit the standard RHEL release schedule.

Red Hat Enterprise Linux (RHEL) provides a stable environment for enterprise applications. This requires RHEL to keep the major releases of upstream packages at the same level to prevent API and configuration file format changes. Security and performance fixes are backported from later upstream releases, but new features that would break backwards compatibility are not backported.

RHSCl allows software developers to use the latest version without impacting RHEL, because RHSCl packages do not replace or conflict with default RHEL packages. Default RHEL packages and RHSCl packages are installed side by side.



### Note

All RHEL subscribers have access to the RHSCl. To enable a particular software collection for a specific user or application environment (for example, MySQL 5.7, which is named rh-mysql57), enable the RHSCl software Yum repositories and follow a few simple steps.

## Finding Containerfiles from the Red Hat Software Collections Library

RHSCl is the source of most container images provided by the Red Hat image registry for use by RHEL Atomic Host and OpenShift Container Platform customers.

Red Hat provides RHSCl Containerfiles and related sources in the `rhscl-dockerfiles` package available from the RHSCl repository. Community users can get Containerfiles for CentOS-based equivalent container images from GitHub's repository at <https://github.com/sclorg?q=-container>.



### Note

Many RHSCl container images include support for Source-to-Image (S2I), best known as an OpenShift Container Platform feature. Having support for S2I does not affect the use of these container images with Docker.

## Container Images in Red Hat Container Catalog (RHCC)

Critical applications require trusted containers. The Red Hat Container Catalog is a repository of reliable, tested, certified, and curated collection of container images built on versions of Red Hat Enterprise Linux (RHEL) and related systems. Container images available through RHCC have undergone a quality-assurance process. All components have been rebuilt by Red Hat to avoid known security vulnerabilities. They are upgraded on a regular basis so that they contain the required version of software even when a new image is not yet available. Using RHCC, you can browse and search for images, and you can access information about each image, such as its version, contents, and usage.

### Searching for Images Using Quay.io

Quay.io is an advanced container repository from CoreOS optimized for team collaboration. You can search for container images using <https://quay.io/search>.

Clicking on an image's name provides access to the image information page, including access to all existing tags for the image and the command to pull the image.

### Finding Containerfiles on Docker Hub

Be careful with images from Docker Hub. Anyone can create a Docker Hub account and publish container images there. There are no general assurances about quality and security; images on Docker Hub range from professionally supported to one-time experiments. Each image has to be evaluated individually.

After searching for an image, the documentation page might provide a link to its Containerfile. For example, the first result when searching for `mysql` is the documentation page for the MySQL official image at [https://hub.docker.com/\\_/mysql](https://hub.docker.com/_/mysql).

On that page, under the `Supported tags and respective Dockerfile links` section, each of the tags points to the `docker-library` GitHub project, which hosts Containerfiles for images built by the Docker community automatic build system.

The direct URL for the Docker Hub MySQL 8.0 Containerfile tree is <https://github.com/docker-library/mysql/blob/master/8.0>.

### Describing How to Use the OpenShift Source-to-Image Tool

Source-to-Image (S2I) provides an alternative to using Containerfiles to create new container images that can be used either as a feature from OpenShift or as the standalone `s2i` utility. S2I allows developers to work using their usual tools, instead of learning Containerfile syntax and using operating system commands such as `yum`. The `S2I` utility usually creates slimmer images with fewer layers.

S2I uses the following process to build a custom container image for an application:

1. Start a container from a base container image called the builder image. This image includes a programming language runtime and essential development tools, such as compilers and package managers.
2. Fetch the application source code, usually from a Git server, and send it to the container.
3. Build the application binary files inside the container.

4. Save the container, after some clean up, as a new container image, which includes the programming language runtime and the application binaries.

The builder image is a regular container image following a standard directory structure and providing scripts that are called during the S2I process. Most of these builder images can also be used as base images for Containerfiles, outside of the S2I process.

The `s2i` command is used to run the S2I process outside of OpenShift, in a Docker-only environment. It can be installed on a RHEL system from the `source-to-image` RPM package, and on other platforms, including Windows and Mac OS, from the installers available in the S2I project on GitHub.



## References

### **Red Hat Software Collections Library (RHSCl)**

<https://access.redhat.com/documentation/en/red-hat-software-collections/>

### **Red Hat Container Catalog (RHCC)**

<https://access.redhat.com/containers/>

### **RHSCl Dockerfiles on GitHub**

<https://github.com/sclorg?q=-container>

### **Using Red Hat Software Collections Container Images**

<https://access.redhat.com/articles/1752723>

### **Quay.io**

<https://quay.io/search>

### **Docker Hub**

<https://hub.docker.com/>

### **Docker Library GitHub project**

<https://github.com/docker-library>

### **The S2I GitHub project**

[https://github.com/openshift/source-to-image/](https://github.com/openshift/source-to-image)

## ► Quiz

---

# Approaches to Container Image Design

Choose the correct answers to the following questions:

- ▶ 1. **Which method for creating container images is recommended by the containers community?**
  - a. Run commands inside a basic OS container, commit the container, and then save or export it as a new container image.
  - b. Run commands from a Containerfile and push the generated container image to an image registry.
  - c. Create the container image layers manually from tar files.
  - d. Run the `podman build` command to process a container image description in YAML format.
  
- ▶ 2. **Which of the following options is an advantage of using the stand-alone S2I process as an alternative to Containerfiles?**
  - a. Requires no additional tools apart from a basic Podman setup.
  - b. Creates smaller container images with fewer layers.
  - c. Reuses high-quality builder images.
  - d. Automatically updates the child image as the parent image changes (for example, with security fixes).
  - e. Creates images compatible with OpenShift, unlike container images created from Docker tools.
  
- ▶ 3. **What are two typical scenarios for creating a Containerfile to build a child image from an existing image? (Choose two.)**
  - a. Adding new runtime libraries.
  - b. Setting constraints on a container's access to the host machine's CPU.
  - c. Adding internal libraries to be shared as a single image layer by multiple container images for different applications.

## ► Solution

---

# Approaches to Container Image Design

Choose the correct answers to the following questions:

- ▶ 1. **Which method for creating container images is recommended by the containers community?**
  - a. Run commands inside a basic OS container, commit the container, and then save or export it as a new container image.
  - b. Run commands from a Containerfile and push the generated container image to an image registry.
  - c. Create the container image layers manually from tar files.
  - d. Run the podman build command to process a container image description in YAML format.
  
- ▶ 2. **Which of the following options is an advantage of using the stand-alone S2I process as an alternative to Containerfiles?**
  - a. Requires no additional tools apart from a basic Podman setup.
  - b. Creates smaller container images with fewer layers.
  - c. Reuses high-quality builder images.
  - d. Automatically updates the child image as the parent image changes (for example, with security fixes).
  - e. Creates images compatible with OpenShift, unlike container images created from Docker tools.
  
- ▶ 3. **What are two typical scenarios for creating a Containerfile to build a child image from an existing image? (Choose two.)**
  - a. Adding new runtime libraries.
  - b. Setting constraints on a container's access to the host machine's CPU.
  - c. Adding internal libraries to be shared as a single image layer by multiple container images for different applications.

# Building Custom Container Images with Containerfiles

---

## Objectives

After completing this section, students should be able to create a container image using common Containerfile commands.

## Building Base Containers

A Containerfile is a mechanism to automate the building of container images. Building an image from a Containerfile is a three-step process.

1. Create a working directory
2. Write the Containerfile
3. Build the image with Podman

### Create a Working Directory

The working directory is the directory containing all files needed to build the image. Creating an empty working directory is good practice to avoid incorporating unnecessary files into the image. For security reasons, the root directory, /, should never be used as a working directory for image builds.

### Write the Containerfile Specification

A Containerfile is a text file named either *Containerfile* or *Dockerfile* that contains the instructions needed to build the image. The basic syntax of a Containerfile follows:

```
Comment
INSTRUCTION arguments
```

Lines that begin with a hash, or pound, symbol (#) are comments. *INSTRUCTION* states for any Containerfile instruction keyword. Instructions are not case-sensitive, but the convention is to make instructions all uppercase to improve visibility.

The first non-comment instruction must be a FROM instruction to specify the base image. Containerfile instructions are executed into a new container using this image and then committed to a new image. The next instruction (if any) executes into that new image. The execution order of instructions is the same as the order of their appearance in the Containerfile.



#### Note

The ARG instruction can appear before the FROM instruction, but ARG instructions are outside the objectives for this section.

Each Containerfile instruction runs in an independent container using an intermediate image built from every previous command. This means each instruction is independent from other instructions

in the Containerfile. The following is an example Containerfile for building a simple Apache web server container:

```
This is a comment line ①
FROM ubi8/ubi:8.5 ②
LABEL description="This is a custom httpd container image" ③
MAINTAINER John Doe <jdoe@xyz.com> ④
RUN yum install -y httpd ⑤
EXPOSE 80 ⑥
ENV LogLevel "info" ⑦
ADD http://someserver.com/filename.pdf /var/www/html ⑧
COPY ./src/ /var/www/html/ ⑨
USER apache ⑩
ENTRYPOINT ["/usr/sbin/httpd"] ⑪
CMD ["-D", "FOREGROUND"] ⑫
```

- ① Lines that begin with a hash, or pound, sign (#) are comments.
- ② The **FROM** instruction declares that the new container image extends `ubi8/ubi:8.5` container base image. Containerfiles can use any other container image as a base image, not only images from operating system distributions. Red Hat provides a set of container images that are certified and tested and highly recommends using these container images as a base.
- ③ The **LABEL** is responsible for adding generic metadata to an image. A **LABEL** is a simple key-value pair.
- ④ **MAINTAINER** indicates the **Author** field of the generated container image's metadata. You can use the `podman inspect` command to view image metadata.
- ⑤ **RUN** executes commands in a new layer on top of the current image. The shell that is used to execute commands is `/bin/sh`.
- ⑥ **EXPOSE** indicates that the container listens on the specified network port at runtime. The **EXPOSE** instruction defines metadata only; it does not make ports accessible from the host. The `-p` option in the `podman run` command exposes container ports from the host.
- ⑦ **ENV** is responsible for defining environment variables that are available in the container. You can declare multiple **ENV** instructions within the Containerfile. You can use the `env` command inside the container to view each of the environment variables.
- ⑧ **ADD** instruction copies files or folders from a local or remote source and adds them to the container's file system. If used to copy local files, those must be in the working directory. **ADD** instruction unpacks local `.tar` files to the destination image directory.
- ⑨ **COPY** copies files from the working directory and adds them to the container's file system. It is not possible to copy a remote file using its URL with this Containerfile instruction.
- ⑩ **USER** specifies the username or the UID to use when running the container image for the **RUN**, **CMD**, and **ENTRYPOINT** instructions. It is a good practice to define a different user other than `root` for security reasons.
- ⑪ **ENTRYPOINT** specifies the default command to execute when the image runs in a container. If omitted, the default **ENTRYPOINT** is `/bin/sh -c`.

- ⑫ CMD provides the default arguments for the ENTRYPPOINT instruction. If the default ENTRYPPOINT applies (`/bin/sh -c`), then CMD forms an executable command and parameters that run at container start.

## CMD and ENTRYPPOINT

ENTRYPPOINT and CMD instructions have two formats:

### Exec form

This form uses a JSON array:

```
ENTRYPPOINT ["command", "param1", "param2"]
CMD ["param1", "param2"]
```

### Shell form

```
ENTRYPPOINT command param1 param2
CMD param1 param2
```

Exec form is the preferred form. Shell form wraps the commands in a `/bin/sh -c` shell, creating a sometimes unnecessary shell process. Also, some combinations are not allowed or may not work as expected. For example, if ENTRYPPOINT is `["ping"]` (exec form) and CMD is `localhost` (shell form), then the expected executed command is `ping localhost`, but the container tries `ping /bin/sh -c localhost`, which is a malformed command.

The Containerfile should contain at most one ENTRYPPOINT and one CMD instruction. If more than one of each is present, then only the last instruction takes effect. CMD can be present without specifying an ENTRYPPOINT. In this case, the base image's ENTRYPPOINT applies, or the default ENTRYPPOINT if none is defined.

Podman can override the CMD instruction when starting a container. If present, all parameters for the `podman run` command after the image name form the CMD instruction. For example, the following instruction causes the running container to display the current time.

```
ENTRYPPOINT ["/bin/date", "+%H:%M"]
```

The ENTRYPPOINT defines both the command to be executed and the parameters. So the CMD instruction cannot be used. The following example provides the same functionality as the preceding one, with the added benefit of the CMD instruction being overwritable when a container starts.

```
ENTRYPPOINT ["/bin/date"]
CMD ["+%H:%M"]
```

In both cases, when a container starts without providing a parameter, the current time is displayed:

```
[student@workstation ~]$ sudo podman run -it do180/rhel
11:41
```

In the second case, if a parameter appears after the image name in the `podman run` command, it overwrites the `CMD` instruction. The following command displays the current day of the week instead of the time:

```
[student@workstation demo-basic]$ sudo podman run -it do180/rhel +%A
Tuesday
```

Another approach is using the default `ENTRYPOINT` and the `CMD` instruction to define the initial command. The following instruction displays the current time, with the added benefit of being able to be overridden at run time.

```
CMD ["date", "+%H:%M"]
```

## ADD and COPY

The ADD and COPY instructions have two forms:

### Shell form

```
ADD source ... destination
COPY source ... destination
```

### Exec form:

```
ADD ["source", ... "destination"]
COPY ["source", ... "destination"]
```

If the `source` is a file system path, it must be inside the working directory.

The ADD instruction also allows you to specify a resource using a URL.

```
ADD http://someserver.com/filename.pdf /var/www/html
```

If the `source` is a local tar archive in a recognized compression format (`identity`, `gzip`, `bzip2` or `xz`), then the ADD instruction unpacks the archive as a directory to the `destination` folder. The COPY instruction does not have this functionality.



### Important

Both the ADD and COPY instructions copy normal files, with `root` as the owner. The ADD instruction retrieves the contents of the URL and the file is copied with `root` as the owner. The ADD instruction extracts the tar archive and preserve the owner and permissions.

You can use the `--chown=<user>:<group>` option with the COPY or ADD command to set the desired owner or use a RUN instruction after the copy to set the owner and permissions.

## Layering Image

Each instruction in a Containerfile creates a new image layer. Having too many instructions in a Containerfile causes too many layers, resulting in large images. For example, consider the following RUN instructions in a Containerfile:

```
RUN yum --disablerepo=* --enablerepo="rhel-7-server-rpms"
RUN yum update -y
RUN yum install -y httpd
```

This example shows the creation of a container image having three layers (one for each RUN instruction). Red Hat recommends minimizing the number of layers. You can achieve the same objective by creating a single layer image using the `&&` conjunction in the RUN instruction.

```
RUN yum --disablerepo=* --enablerepo="rhel-7-server-rpms" && yum update -y && yum
install -y httpd
```

The problem with this approach is that the readability of the Containerfile decays. Use the `\` escape code to insert line breaks and improve readability. You can also indent lines to align the commands:

```
RUN yum --disablerepo=* --enablerepo="rhel-7-server-rpms" && \
 yum update -y && \
 yum install -y httpd
```

This example creates only one layer and the readability improves. RUN, COPY, and ADD instructions create new image layers, but RUN can be improved this way.

Red Hat recommends applying similar formatting rules to other instructions accepting multiple parameters, such as LABEL and ENV:

```
LABEL version="2.0" \
 description="This is an example container image" \
 creationDate="01-09-2017"
```

```
ENV MYSQL_ROOT_PASSWORD="my_password" \
 MYSQL_DATABASE="my_database"
```

## Building Images with Podman

The `podman build` command processes the Containerfile and builds a new image based on the instructions it contains. The syntax for this command is as follows:

```
[user@host ~]$ podman build -t NAME:TAG DIR
```

`DIR` is the path to the working directory. It can be the current directory as designated by a dot (`.`) if the working directory is the current directory. `NAME:TAG` is a name with a tag given to the new image. If `TAG` is not specified, then the image is automatically tagged as `latest`.



### Note

The current working directory is by default the path for the Containerfile, but you can specify a different directory using the `-f` flag. For more information you can check the Best practices for writing Dockerfiles [[https://docs.docker.com/develop/develop-images/dockerfile\\_best-practices/](https://docs.docker.com/develop/develop-images/dockerfile_best-practices/)].



### References

#### Dockerfile Reference Guide

<https://docs.docker.com/engine/reference/builder/>

#### Creating base images

<https://docs.docker.com/engine/userguide/eng-image/baseimages/>

## ► Guided Exercise

# Creating a Basic Apache Container Image

In this exercise, you will create a basic Apache container image.

### Outcomes

You should be able to create a custom Apache container image built on a Red Hat Universal Base Image 8 image.

### Before You Begin

Run the following command to download the relevant lab files and to verify that Docker is running:

```
[student@workstation ~]$ lab dockerfile-create start
```

### Instructions

► 1. Create the Apache Containerfile.

- 1.1. Open a terminal on `workstation`. Using your preferred editor, create a new Containerfile.

```
[student@workstation ~]$ vim ~/DO180/labs/dockerfile-create/Containerfile
```

- 1.2. Use UBI 8.5 as a base image by adding the following `FROM` instruction at the top of the new Containerfile:

```
FROM ubi8/ubi:8.5
```

- 1.3. Beneath the `FROM` instruction, include the `MAINTAINER` instruction to set the `Author` field in the new image. Replace the values to include your name and email address.

```
MAINTAINER Your Name <youremail>
```

- 1.4. Below the `MAINTAINER` instruction, add the following `LABEL` instruction to add description metadata to the new image:

```
LABEL description="A custom Apache container based on UBI 8"
```

- 1.5. Add a `RUN` instruction with a `yum install` command to install Apache on the new container.

```
RUN yum install -y httpd && \
 yum clean all
```

- 1.6. Add a RUN instruction to replace contents of the default HTTPD home page.

```
RUN echo "Hello from Containerfile" > /var/www/html/index.html
```

- 1.7. Use the EXPOSE instruction beneath the RUN instruction to document the port that the container listens to at runtime. In this instance, set the port to 80, because it is the default for an Apache server.

```
EXPOSE 80
```



### Note

The EXPOSE instruction does not actually make the specified port available to the host; rather, the instruction serves as metadata about the ports on which the container is listening.

- 1.8. At the end of the file, use the following CMD instruction to set `httpd` as the default entry point:

```
CMD ["httpd", "-D", "FOREGROUND"]
```

- 1.9. Verify that your Containerfile matches the following before saving and proceeding with the next steps:

```
FROM ubi8/ubi:8.5

MAINTAINER Your Name <youremail>

LABEL description="A custom Apache container based on UBI 8"

RUN yum install -y httpd && \
 yum clean all

RUN echo "Hello from Containerfile" > /var/www/html/index.html

EXPOSE 80

CMD ["httpd", "-D", "FOREGROUND"]
```

- 2. Build and verify the Apache container image.

- 2.1. Use the following commands to create a basic Apache container image using the newly created Containerfile:

```
[student@workstation ~]$ cd ~/DO180/labs/dockerfile-create

[student@workstation dockerfile-create]$ podman build --layers=false \
> -t do180/apache .
STEP 1/7: FROM ubi8/ubi:8.5
...output omitted...
Trying to pull registry.access.redhat.com/ubi8/ubi:8.5... 1
```

```
...output omitted...
STEP 2/7: MAINTAINER Your Name <youremail>
STEP 3/7: LABEL description="A custom Apache container based on UBI 8"
STEP 4/7: RUN yum install -y httpd && yum clean all
Updating Subscription Management repositories.
Unable to read consumer identity
Subscription Manager is operating in container mode.
...output omitted...
STEP 5/7: RUN echo "Hello from Containerfile" > /var/www/html/index.html
STEP 6/7: EXPOSE 80
STEP 7/7: CMD ["httpd", "-D", "FOREGROUND"]
COMMIT do180/apache
Getting image source signatures
...output omitted...
Writing manifest to image destination
Storing signatures
--> 16c8493a19a
Successfully tagged localhost/do180/apache:latest
16c8493a19ad5162031cf17c6b2e338171f4619b6358cb367608c80791aa7718
```

- ➊ The container image listed in the FROM instruction is only downloaded if it is not already present in local storage.



### Note

Podman creates many anonymous intermediate images during the build process. They are not be listed unless -a is used. Use the --layers=false option of the build subcommand to instruct Podman to delete intermediate images.

- 2.2. After the build process has finished, run podman images to see the new image in the image repository.

```
[student@workstation dockerfile-create]$ podman images
REPOSITORY TAG IMAGE ID CREATED SIZE
localhost/do180/apache latest 16c8493a19ad 45 seconds ago 257 MB
registry.access.redhat.com/ubi8/ubi 8.5 202c1768b1f7 2 months ago 235 MB
```

- ▶ 3. Run the Apache container.

- 3.1. Use the following command to run a container using the Apache image:

```
[student@workstation dockerfile-create]$ podman run --name lab-apache \
> -d -p 10080:80 do180/apache
fa1d1c450e8892ae085dd8bbf763edac92c41e6ffaa7ad6ec6388466809bb391
```

- 3.2. Run the podman ps command to see the running container.

```
[student@workstation dockerfile-create]$ podman ps
CONTAINER ID IMAGE COMMAND CREATED
STATUS PORTS NAMES
fa1d1c450e88 localhost/do180/apache:latest httpd -D ... 10 seconds ago
Up 9 seconds ago 0.0.0.0:10080->80/tcp lab-apache
```

- 3.3. Use the `curl` command to verify that the server is running.

```
[student@workstation dockerfile-create]$ curl -s 127.0.0.1:10080
Hello from Containerfile
```

## Finish

On `workstation`, run the `lab dockerfile-create finish` script to complete this lab.

```
[student@workstation ~]$ lab dockerfile-create finish
```

This concludes the guided exercise.

## ► Lab

# Creating Custom Container Images

In this lab, you will create a Containerfile to build a custom Apache Web Server container image. The custom image will be based on a RHEL 8.5 UBI image and serve a custom `index.html` page.

## Outcomes

You should be able to create a custom Apache Web Server container that hosts static HTML files.

## Before You Begin

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab dockerfile-review start
```

## Instructions

1. Review the provided Containerfile stub in the `~/DO180/labs/dockerfile-review` folder. Edit the `Containerfile` and ensure that it meets the following specifications:
  - The base image is `ubi8/ubi:8.5`
  - Sets the desired author name and email ID with the `MAINTAINER` instruction
  - Sets the environment variable `PORT` to `8080`
  - Install Apache (`httpd` package).
  - Change the Apache configuration file `/etc/httpd/conf/httpd.conf` to listen to port `8080` instead of the default port `80`.
  - Change ownership of the `/etc/httpd/logs` and `/run/httpd` folders to user and group `apache` (UID and GID are `48`).
  - Expose the value set in the `PORT` environment variable so that container users know how to access the Apache Web Server.
  - Copy the contents of the `src/` folder in the lab directory to the Apache DocumentRoot file (`/var/www/html/`) inside the container.

The `src` folder contains a single `index.html` file that prints a `Hello World!` message.

- Start the Apache `httpd` daemon in the foreground using the `CMD` instruction and the following command:

```
httpd -D FOREGROUND
```

2. Build the custom Apache image with the name `do180/custom-apache`.

3. Create a new container in detached mode with the following characteristics:

- Name: `containerfile`
- Container image: `do180/custom-apache`
- Port forward: from host port 20080 to container port 8080
- Run as a daemon: yes

Verify that the container is ready and running.

4. Verify that the server returns the HTML page.

## Evaluation

Grade your work by running the `lab dockerfile-review grade` command from your workstation machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab dockerfile-review grade
```

## Finish

From workstation, run the `lab dockerfile-review finish` command to complete this lab.

```
[student@workstation ~]$ lab dockerfile-review finish
```

This concludes the lab.

## ► Solution

# Creating Custom Container Images

In this lab, you will create a Containerfile to build a custom Apache Web Server container image. The custom image will be based on a RHEL 8.5 UBI image and serve a custom `index.html` page.

## Outcomes

You should be able to create a custom Apache Web Server container that hosts static HTML files.

## Before You Begin

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab dockerfile-review start
```

## Instructions

1. Review the provided Containerfile stub in the `~/D0180/labs/dockerfile-review` folder. Edit the `Containerfile` and ensure that it meets the following specifications:
  - The base image is `ubi8/ubi:8.5`
  - Sets the desired author name and email ID with the `MAINTAINER` instruction
  - Sets the environment variable `PORT` to `8080`
  - Install Apache (`httpd` package).
  - Change the Apache configuration file `/etc/httpd/conf/httpd.conf` to listen to port `8080` instead of the default port `80`.
  - Change ownership of the `/etc/httpd/logs` and `/run/httpd` folders to user and group `apache` (UID and GID are `48`).
  - Expose the value set in the `PORT` environment variable so that container users know how to access the Apache Web Server.
  - Copy the contents of the `src/` folder in the lab directory to the Apache DocumentRoot file (`/var/www/html/`) inside the container.

The `src` folder contains a single `index.html` file that prints a `Hello World!` message.

- Start the Apache `httpd` daemon in the foreground using the `CMD` instruction and the following command:

```
httpd -D FOREGROUND
```

**Chapter 5 |** Creating Custom Container Images

- 1.1. Use your preferred editor to modify the Containerfile located in the ~/DO180/labs/dockerfile-review folder.

```
[student@workstation ~]$ cd ~/DO180/labs/dockerfile-review
[student@workstation dockerfile-review]$ vim Containerfile
```

- 1.2. Set the base image for the Containerfile to ubi8/ubi:8.5.

```
FROM ubi8/ubi:8.5
```

- 1.3. Set your name and email with a MAINTAINER instruction.

```
MAINTAINER Your Name <youremail>
```

- 1.4. Create an environment variable called PORT and set it to 8080.

```
ENV PORT 8080
```

- 1.5. Install the Apache httpd server.

```
RUN yum install -y httpd && \
 yum clean all
```

- 1.6. Change the Apache HTTP Server configuration file to listen on port 8080 and change ownership of the server working folders with a single RUN instruction.

```
RUN sed -ri -e "/^Listen 80/c\Listen ${PORT}" /etc/httpd/conf/httpd.conf && \
 chown -R apache:apache /etc/httpd/logs/ && \
 chown -R apache:apache /run/httpd/
```

- 1.7. Use the USER instruction to run the container as the apache user. Use the EXPOSE instruction to document the port that the container listens to at runtime. In this instance, set the port to the PORT environment variable, which is the default for an Apache server.

```
USER apache

Expose the custom port that you provided in the ENV var
EXPOSE ${PORT}
```

- 1.8. Copy all the files from the src folder to the Apache DocumentRoot path at /var/www/html.

```
Copy all files under src/ folder to Apache DocumentRoot (/var/www/html)
COPY ./src/ /var/www/html/
```

- 1.9. Finally, insert a CMD instruction to run httpd in the foreground, and then save the Containerfile.

```
Start Apache in the foreground
CMD ["httpd", "-D", "FOREGROUND"]
```

**2.** Build the custom Apache image with the name do180/custom-apache.

- 2.1. Verify the Containerfile for the custom Apache image. The Containerfile for the custom Apache image should look similar to the following:

```
FROM ubi8/ubi:8.5

MAINTAINER Your Name <youremail>

ENV PORT 8080

RUN yum install -y httpd && \
 yum clean all

RUN sed -ri -e "/^Listen 80/c\Listen ${PORT}" /etc/httpd/conf/httpd.conf && \
 chown -R apache:apache /etc/httpd/logs/ && \
 chown -R apache:apache /run/httpd/

USER apache

Expose the custom port that you provided in the ENV var
EXPOSE ${PORT}

Copy all files under src/ folder to Apache DocumentRoot (/var/www/html)
COPY ./src/ /var/www/html/

Start Apache in the foreground
CMD ["httpd", "-D", "FOREGROUND"]
```

- 2.2. Run a podman build command to build the custom Apache image and name it do180/custom-apache.

```
[student@workstation dockerfile-review]$ podman build --layers=false \
> -t do180/custom-apache .
STEP 1/9: FROM ubi8/ubi:8.5
Trying to pull registry.access.redhat.com/ubi8/ubi:8.5...
...output omitted...
STEP 2/9: MAINTAINER username <username@example.com>
STEP 3/9: ENV PORT 8080
STEP 4/9: RUN yum install -y httpd && yum clean all
Updating Subscription Management repositories.
Unable to read consumer identity
Subscription Manager is operating in container mode.
...output omitted...
STEP 5/9: RUN sed -ri -e "/^Listen 80/c\Listen ${PORT}" /etc/httpd/conf/httpd.conf \
&& chown -R apache:apache /etc/httpd/logs/ && chown -R apache:apache /run/httpd/
STEP 6/9: USER apache
STEP 7/9: EXPOSE ${PORT}
STEP 8/9: COPY ./src/ /var/www/html/
STEP 9/9: CMD ["httpd", "-D", "FOREGROUND"]
```

```
COMMIT do180/custom-apache
Getting image source signatures
...output omitted...
Writing manifest to image destination
Storing signatures
--> 06f94fef73b
Successfully tagged localhost/do180/custom-apache:latest
06f94fef73b0b617f6e51b34856ada9d499a45efbd738e9d0cd9586f8786e181
```

- 2.3. Run the `podman images` command to verify that the custom image is built successfully.

```
[student@workstation dockerfile-review]$ podman images
REPOSITORY TAG IMAGE ID CREATED SIZE
localhost/do180/custom-apache latest 06f94fef73b0 2 minutes ago 257 MB
registry.access.redhat.com/ubi8/ubi 8.5 202c1768b1f7 2 months ago 235 MB
```

3. Create a new container in detached mode with the following characteristics:

- Name: `containerfile`
- Container image: `do180/custom-apache`
- Port forward: from host port 20080 to container port 8080
- Run as a daemon: yes

Verify that the container is ready and running.

- 3.1. Create and run the container.

```
[student@workstation dockerfile-review]$ podman run -d \
> --name containerfile -p 20080:8080 do180/custom-apache
4a64836e7105c16a1ea4206dd1941a38f587957d7dc5fd0be5f87d11854d3146
```

- 3.2. Verify that the container is ready and running.

```
[student@workstation dockerfile-review]$ podman ps
CONTAINER ID IMAGE COMMAND CREATED
STATUS PORTS NAMES
4a64836e7105 localhost/do180/custom-apache:latest httpd -D ... 5 seconds ago
Up 5 seconds ago 0.0.0.0:20080->8080/tcp containerfile
```

4. Verify that the server returns the HTML page.

- 4.1. Run a `curl` command on `127.0.0.1:20080`.

```
[student@workstation dockerfile-review]$ curl -s 127.0.0.1:20080
```

The output should be as follows:

```
<html>
<header><title>DO180 Hello!</title></header>
<body>
 Hello World! The containerfile-review lab works!
</body>
</html>
```

## Evaluation

Grade your work by running the `lab dockerfile-review grade` command from your `workstation` machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab dockerfile-review grade
```

## Finish

From `workstation`, run the `lab dockerfile-review finish` command to complete this lab.

```
[student@workstation ~]$ lab dockerfile-review finish
```

This concludes the lab.

# Summary

---

In this chapter, you learned:

- A `Containerfile` contains instructions that specify how to construct a container image.
- Container images provided by Red Hat Container Catalog or Quay.io are a good starting point for creating custom images for a specific language or technology.
- The Source-to-Image (S2I) process provides an alternative to Containerfiles. S2I implements a standardized container image build process for common technologies from application source code. This allows developers to focus on application development and not Containerfile development.



## Chapter 6

# Deploying Containerized Applications on OpenShift

### Goal

Deploy single container applications on OpenShift Container Platform.

### Objectives

- Describe the architecture of Kubernetes and Red Hat OpenShift Container Platform.
- Create standard Kubernetes resources.
- Create a route to a service.
- Build an application using the Source-to-Image facility of OpenShift Container Platform.
- Create an application using the OpenShift web console.

### Sections

- Describing Kubernetes and OpenShift Architecture (and Quiz)
- Creating Kubernetes Resources (and Guided Exercise)
- Creating Routes (and Guided Exercise)
- Creating Applications with the Source-to-Image Facility (and Guided Exercise)
- Creating Applications with the OpenShift Web Console (and Guided Exercise)

### Lab

- Deploying Containerized Applications on OpenShift

# Describing Kubernetes and OpenShift Architecture

---

## Objectives

After completing this section, students should be able to:

- Describe the architecture of a Kubernetes cluster running on the Red Hat OpenShift Container Platform (RHOC).
- List the main resource types provided by Kubernetes and RHOC.
- Identify the network characteristics of containers, Kubernetes, and RHOC.
- List mechanisms to make a pod externally available.

## Kubernetes and OpenShift

In previous chapters we saw that Kubernetes is an orchestration service that simplifies the deployment, management, and scaling of containerized applications. One of the main advantages of using Kubernetes is that it uses several nodes to ensure the resiliency and scalability of its managed applications. Kubernetes forms a cluster of node servers that run containers and are centrally managed by a set of control plane servers. A server can act as both a control plane node and a compute node, but those roles are usually separated for increased stability.

### Kubernetes Terminology

Term	Definition
Node	A server that hosts applications in a Kubernetes cluster.
Control Plane	Provides basic cluster services such as APIs or controllers.
Compute Node	This node executes workloads for the cluster. Application pods are scheduled onto compute nodes.
Resource	Resources are any kind of component definition managed by Kubernetes. Resources contain the configuration of the managed component (for example, the role assigned to a node), and the current state of the component (for example, if the node is available).
Controller	A controller is a Kubernetes process that watches resources and makes changes attempting to move the current state towards the desired state.
Label	A key-value pair that can be assigned to any Kubernetes resource. Selectors use labels to filter eligible resources for scheduling and other operations.
Namespace	A scope for Kubernetes resources and processes, so that resources with the same name can be used in different boundaries.

**Note**

The latest Kubernetes versions implement many controllers as Operators. Operators are Kubernetes plug-in components that can react to cluster events and control the state of resources. Operators and CoreOS Operator Framework are outside the scope of this document.

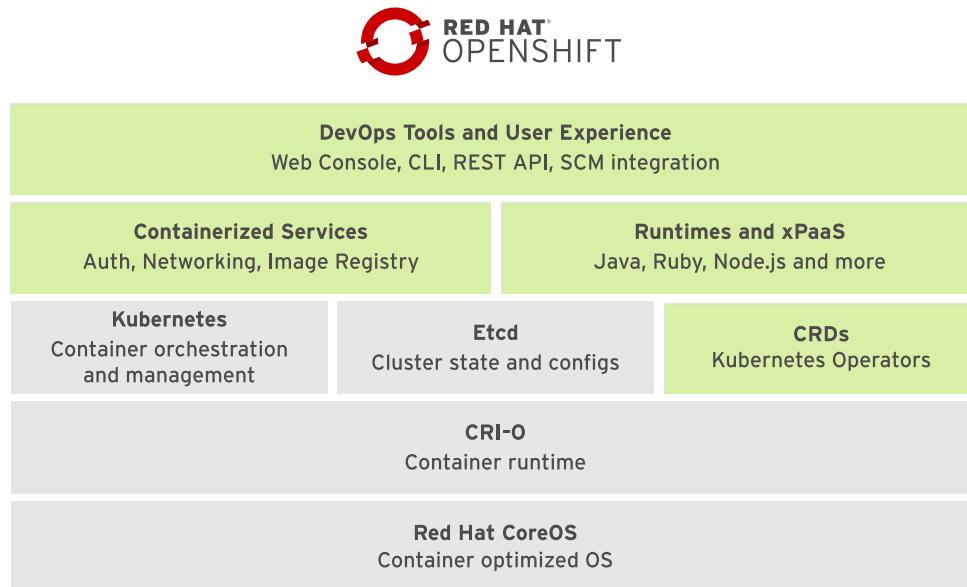
Red Hat OpenShift Container Platform is a set of modular components and services built on top of Red Hat CoreOS and Kubernetes. RHOCP adds PaaS capabilities such as remote management, increased security, monitoring and auditing, application lifecycle management, and self-service interfaces for developers.

An OpenShift cluster is a Kubernetes cluster that can be managed the same way, but using the management tools provided by OpenShift, such as the command-line interface or the web console. This allows for more productive workflows and makes common tasks much easier.

### OpenShift Terminology

Term	Definition
Infra Node	A node server containing infrastructure services like monitoring, logging, or external routing.
Console	A web UI provided by the RHOCP cluster that allows developers and administrators to interact with cluster resources.
Project	OpenShift extension of Kubernetes' namespaces. Allows the definition of user access control (UAC) to resources.

The following schema illustrates the OpenShift Container Platform stack:



**Figure 6.1: OpenShift component stack**

From bottom to top, and from left to right, this shows the basic container infrastructure, integrated and enhanced by Red Hat:

- The base OS is Red Hat CoreOS. Red Hat CoreOS is a Linux distribution focused on providing an immutable operating system for container execution.
- CRI-O is an implementation of the Kubernetes Container Runtime Interface (CRI) to enable using Open Container Initiative (OCI) compatible runtimes. CRI-O can use any container runtime that satisfies CRI: `runc` (used by the Docker service), `libpod` (used by Podman) or `rkt` (from CoreOS).
- Kubernetes manages a cluster of hosts, physical or virtual, that run containers. It uses resources that describe multicontainer applications composed of multiple resources, and how they interconnect.
- Etcd is a distributed key-value store, used by Kubernetes to store configuration and state information about the containers and other resources inside the Kubernetes cluster.
- Custom Resource Definitions (CRDs) are resource types stored in Etcd and managed by Kubernetes. These resource types form the state and configuration of all resources managed by OpenShift.
- Containerized services fulfill many PaaS infrastructure functions, such as networking and authorization. RHOCP uses the basic container infrastructure from Kubernetes and the underlying container runtime for most internal functions. That is, most RHOCP internal services run as containers orchestrated by Kubernetes.
- Runtimes and xPaaS are base container images ready for use by developers, each preconfigured with a particular runtime language or database. The xPaaS offering is a set of base images for Red Hat middleware products such as JBoss EAP and ActiveMQ. Red Hat OpenShift Application Runtimes (RHOAR) are a set runtimes optimized for cloud native applications in OpenShift. The application runtimes available are Red Hat JBoss EAP, OpenJDK, Thorntail, Eclipse Vert.x, Spring Boot, and Node.js.
- RHOCP provides web UI and CLI management tools for managing user applications and RHOCP services. The OpenShift web UI and CLI tools are built from REST APIs which can be used by external tools such as IDEs and CI platforms.

This OpenShift and Kubernetes architecture illustration gives further insight into how the infrastructure components work together.

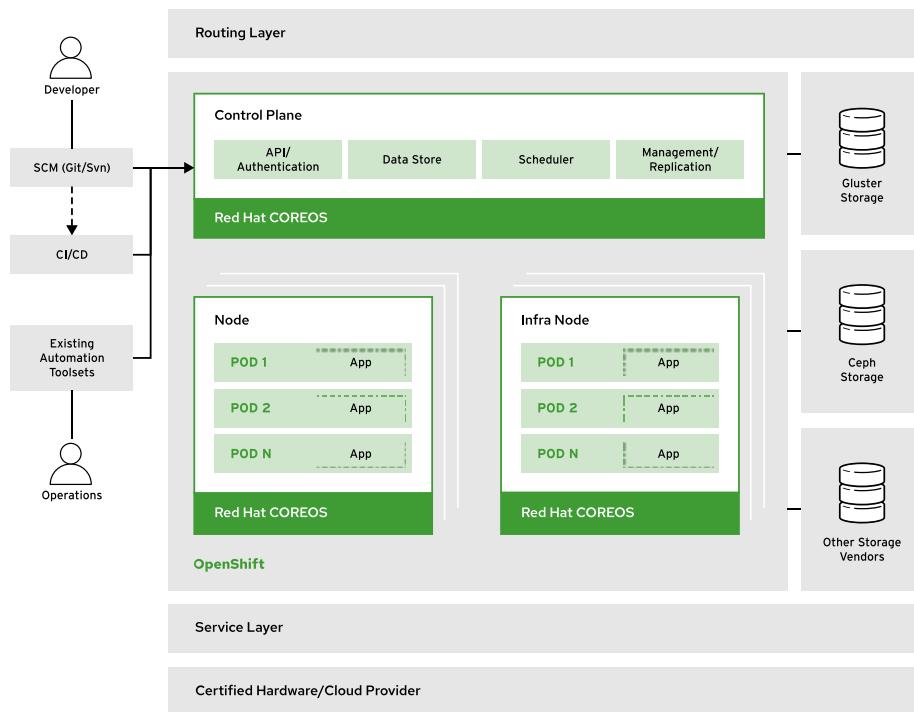


Figure 6.2: OpenShift and Kubernetes architecture

## New Features in RHOC 4

RHOC 4 is a massive change from previous versions. As well as keeping backwards compatibility with previous releases, it includes new features, such as:

- CoreOS as the mandatory operating system for all nodes, offering an immutable infrastructure optimized for containers.
- A brand new cluster installer which guides the process of installation and update.
- A self-managing platform, able to automatically apply cluster updates and recoveries without disruption.
- A redesigned application lifecycle management.
- An Operator SDK to build, test, and package Operators.

## Describing Kubernetes Resource Types

Kubernetes has six main resource types that can be created and configured using a YAML or a JSON file, or using OpenShift management tools:

### **Pods (pod)**

Represent a collection of containers that share resources, such as IP addresses and persistent storage volumes. It is the basic unit of work for Kubernetes.

### **Services (svc)**

Define a single IP/port combination that provides access to a pool of pods. By default, services connect clients to pods in a round-robin fashion.

**Replication Controllers (rc)**

A Kubernetes resource that defines how pods are replicated (horizontally scaled) into different nodes. Replication controllers are a basic Kubernetes service to provide high availability for pods and containers.

**Persistent Volumes (pv)**

Define storage areas to be used by Kubernetes pods.

**Persistent Volume Claims (pvc)**

Represent a request for storage by a pod. PVCs links a PV to a pod so its containers can make use of it, usually by mounting the storage into the container's file system.

**ConfigMaps (cm) and Secrets**

Contains a set of keys and values that can be used by other resources. ConfigMaps and Secrets are usually used to centralize configuration values used by several resources. Secrets differ from ConfigMaps maps in that Secrets' values are always encoded (not encrypted) and their access is restricted to fewer authorized users.

**Note**

Although Kubernetes pods can be created standalone, they are usually created by high-level resources such as replication controllers.

## OpenShift Resource Types

The main resource types added by OpenShift Container Platform to Kubernetes are as follows:

**Deployment and Deployment config (dc)**

OpenShift 4.5 introduced the Deployment resource concept to replace the DeploymentConfig as the default configuration for pods. Both are the representation of a set of containers included in a pod, and the deployment strategies to be used. It contains the configuration to be applied to all containers of each pod replica, such as the base image, tags, storage definitions and the commands to be executed when the containers start.

The Deployment object serves as the improved version of the DeploymentConfig object. Some replacements of functionalities between both objects are the following:

- Automatic rollback is no longer supported by deployment objects.
- Every change in the pod template used by deployment objects triggers a new rollout automatically.
- Lifecycle hooks are no longer supported by deployment objects.
- The deployment process of a deployment object can be paused at any time without affecting the deployer process.
- A deployment object can have as many active replica sets as the user wants, scaling down old replicas after a while. In contrast, the deploymentconfig object can only have two replication sets active at the same time.

Even if Deployment objects are meant to act as the default replacement of DeploymentConfig objects, in OpenShift 4.10 users can still make use of them if they need a specific feature provided by these objects. In this case, it is necessary to specify the type of object when creating a new application by specifying the `--as=deployment-config` flag.

### Build config (bc)

Defines a process to be executed in the OpenShift project. Used by the OpenShift Source-to-Image (S2I) feature to build a container image from application source code stored in a Git repository. A bc works together with a dc to provide a basic but extensible continuous integration and continuous delivery workflows.

### Routes

Represent a DNS host name recognized by the OpenShift router as an ingress point for applications and microservices.



#### Note

To obtain a list of all the resources available in a RHOCP cluster and their abbreviations, use the `oc api-resources` or `kubectl api-resources` commands.

Although Kubernetes replication controllers can be created standalone in OpenShift, they are usually created by higher-level resources such as deployment controllers.

## Networking

Each container deployed in a Kubernetes cluster has an IP address assigned from an internal network that is accessible only from the node running the container. Because of the container's ephemeral nature, IP addresses are constantly assigned and released.

Kubernetes provides a software-defined network (SDN) that spawns the internal container networks from multiple nodes and allows containers from any pod, inside any host, to access pods from other hosts. Access to the SDN only works from inside the same Kubernetes cluster.

Containers inside Kubernetes pods should not connect to each other's dynamic IP address directly. Services resolves this problem by linking more stable IP addresses from the SDN to the pods. If pods are restarted, replicated, or rescheduled to different nodes, services are updated, providing scalability and fault tolerance.

External access to containers is more complicated. Kubernetes services can be set as a `NodePort` service type. With this type of service, Kubernetes allocates a network port from a predefined range in each of the cluster nodes and proxies it into your service. Unfortunately, this approach does not scale well.

OpenShift makes external access to containers both scalable and simpler by defining route resources. A route defines external-facing DNS names and ports for a service. A router (ingress controller) forwards HTTP and TLS requests to the service addresses inside the Kubernetes SDN. The only requirement is that the desired DNS names are mapped to the IP addresses of the RHOCP router nodes.



## References

### Kubernetes documentation website

<https://kubernetes.io/docs/>

### OpenShift documentation website

<https://docs.openshift.com/>

### Understanding Operators

<https://docs.openshift.com/container-platform/4.10/operators/understanding/olm-what-operators-are.html>

## ► Quiz

# Describing Kubernetes and OpenShift

Choose the correct answers to the following questions:

- ▶ **1. Which two sentences are correct regarding Kubernetes architecture? (Choose two.)**
  - a. Kubernetes nodes can be managed without a control plane.
  - b. Kubernetes control planes manage pod scaling.
  - c. Kubernetes control planes schedule pods to specific nodes.
  - d. Kubernetes tools cannot be used to manage resources in an OpenShift cluster.
  - e. Containers created from Kubernetes pods cannot be managed using standalone tools such as Podman.
- ▶ **2. Which two sentences are correct regarding Kubernetes and OpenShift resource types? (Choose two.)**
  - a. A pod is responsible for provisioning its own persistent storage.
  - b. All pods generated from the same replication controller have to run in the same node.
  - c. A persistent volume define storage areas available to pods through a persistent volume claim.
  - d. A replication controller is responsible for monitoring and maintaining the number of pods for a particular application.
- ▶ **3. Which two statements are true regarding Kubernetes and OpenShift networking? (Choose two.)**
  - a. A Kubernetes service can provide an IP address to access a set of pods.
  - b. Kubernetes is responsible for providing a fully qualified domain name for a pod.
  - c. A replication controller is responsible for routing external requests to the pods.
  - d. A route is responsible for providing DNS names for external access.
- ▶ **4. Which statement is correct regarding persistent storage in OpenShift and Kubernetes?**
  - a. A PVC represents a storage area that a pod can use to store data and is provisioned by the application developer.
  - b. A PVC represents a storage area that can be requested by a pod to store data but is provisioned by the cluster administrator.
  - c. A PVC represents the amount of memory that can be allocated to a node, so that a developer can state how much memory he requires for his application to run.
  - d. A PVC represents the number of CPU processing units that can be allocated to an application pod, subject to a limit managed by the cluster administrator.

► **5. Which statement is correct regarding OpenShift additions to Kubernetes?**

- a. OpenShift adds features to simplify Kubernetes configuration of many real-world use cases.
- b. Container images created for OpenShift cannot be used with plain Kubernetes.
- c. Red Hat maintains forked versions of Kubernetes internal to the RHOCP product.
- d. Doing continuous integration and continuous deployment with RHOCP requires external tools.

## ► Solution

# Describing Kubernetes and OpenShift

Choose the correct answers to the following questions:

► 1. **Which two sentences are correct regarding Kubernetes architecture? (Choose two.)**

- a. Kubernetes nodes can be managed without a control plane.
- b. Kubernetes control planes manage pod scaling.
- c. Kubernetes control planes schedule pods to specific nodes.
- d. Kubernetes tools cannot be used to manage resources in an OpenShift cluster.
- e. Containers created from Kubernetes pods cannot be managed using standalone tools such as Podman.

► 2. **Which two sentences are correct regarding Kubernetes and OpenShift resource types? (Choose two.)**

- a. A pod is responsible for provisioning its own persistent storage.
- b. All pods generated from the same replication controller have to run in the same node.
- c. A persistent volume define storage areas available to pods through a persistent volume claim.
- d. A replication controller is responsible for monitoring and maintaining the number of pods for a particular application.

► 3. **Which two statements are true regarding Kubernetes and OpenShift networking? (Choose two.)**

- a. A Kubernetes service can provide an IP address to access a set of pods.
- b. Kubernetes is responsible for providing a fully qualified domain name for a pod.
- c. A replication controller is responsible for routing external requests to the pods.
- d. A route is responsible for providing DNS names for external access.

► 4. **Which statement is correct regarding persistent storage in OpenShift and Kubernetes?**

- a. A PVC represents a storage area that a pod can use to store data and is provisioned by the application developer.
- b. A PVC represents a storage area that can be requested by a pod to store data but is provisioned by the cluster administrator.
- c. A PVC represents the amount of memory that can be allocated to a node, so that a developer can state how much memory he requires for his application to run.
- d. A PVC represents the number of CPU processing units that can be allocated to an application pod, subject to a limit managed by the cluster administrator.

► **5. Which statement is correct regarding OpenShift additions to Kubernetes?**

- a. OpenShift adds features to simplify Kubernetes configuration of many real-world use cases.
- b. Container images created for OpenShift cannot be used with plain Kubernetes.
- c. Red Hat maintains forked versions of Kubernetes internal to the RHOCP product.
- d. Doing continuous integration and continuous deployment with RHOCP requires external tools.

# Creating Kubernetes Resources

## Objectives

After completing this section, students should be able to create standard Kubernetes resources.

## The Red Hat OpenShift Container Platform (RHOCP) Command-line Tool

The main method of interacting with an RHOCP cluster is using the `oc` command. The basic usage of the command is through its subcommands in the following syntax:

```
[user@host ~]$ oc <command>
```

Before interacting with a cluster, most operations require the user to log in. The syntax to log in is shown below:

```
[user@host ~]$ oc login <cluster-url>
```

## Describing Pod Resource Definition Syntax

RHOCP runs containers inside Kubernetes pods, and to create a pod from a container image, OpenShift needs a *pod resource definition*. This can be provided either as a JSON or YAML text file, or can be generated from defaults by the `oc new-app` command or the OpenShift web console.

A pod is a collection of containers and other resources. An example of a WildFly application server pod definition in YAML format is shown below:

```
apiVersion: v1
kind: Pod 1
metadata:
 name: wildfly 2
 labels:
 name: wildfly 3
spec:
 containers:
 - resources:
 limits:
 cpu: 0.5
 image: do276/todojee 4
 name: wildfly
 ports:
 - containerPort: 8080 5
 name: wildfly
 env: 6
 - name: MYSQL_ENV_MYSQL_DATABASE
 value: items
```

```

- name: MYSQL_ENV_MYSQL_USER
 value: user1
- name: MYSQL_ENV_MYSQL_PASSWORD
 value: mypa55

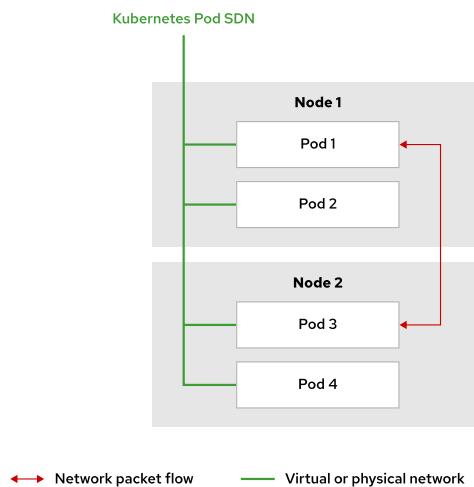
```

- ➊ Declares a Kubernetes pod resource type.
- ➋ A unique name for a pod in Kubernetes that allows administrators to run commands on it.
- ➌ Creates a label with a key named name that other resources in Kubernetes, usually as service, can use to find it.
- ➍ Defines the container image name.
- ➎ A container-dependent attribute identifying which port on the container is exposed.
- ➏ Defines a collection of environment variables.

Some pods may require environment variables that can be read by a container. Kubernetes transforms all the name and value pairs to environment variables. For instance, the MYSQL\_ENV\_MYSQL\_USER variable is declared internally by the Kubernetes runtime with a value of user1, and is forwarded to the container image definition. Because the container uses the same variable name to get the user's login, the value is used by the WildFly container instance to set the username that accesses a MySQL database instance.

## Describing Service Resource Definition Syntax

Kubernetes provides a virtual network that allows pods from different compute nodes to connect. But, Kubernetes provides no easy way for a pod to discover the IP addresses of other pods:

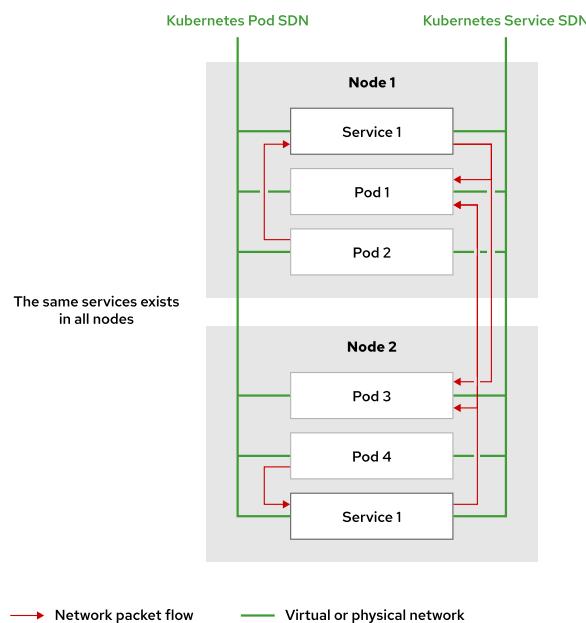


**Figure 6.3: Basic Kubernetes networking**

If Pod 3 fails and is restarted, it could return with a different IP address. This would cause Pod 1 to fail when attempting to communicate with Pod 3. A service layer provides the abstraction required to solve this problem.

Services are essential resources to any OpenShift application. They allow containers in one pod to open network connections to containers in another pod. A pod can be restarted for many reasons, and it gets a different internal IP address each time. Instead of a pod having to discover the IP

address of another pod after each restart, a service provides a stable IP address for other pods to use, no matter what compute node runs the pod after each restart:



**Figure 6.4: Kubernetes services networking**

Most real-world applications do not run as a single pod. They need to scale horizontally, so many pods run the same containers from the same pod resource definition to meet growing user demand. A service is tied to a set of pods, providing a single IP address for the whole set, and a load-balancing client request among member pods.

The set of pods running behind a service is managed by a Deployment resource. A Deployment resource embeds a ReplicationController that manages how many pod copies (replicas) have to be created, and creates new ones if any of them fail. Deployment and ReplicationController resources are explained later in this chapter.

The following example shows a minimal service definition in JSON syntax:

```
{
 "kind": "Service", ①
 "apiVersion": "v1",
 "metadata": {
 "name": "quotedb" ②
 },
 "spec": {
 "ports": [③
 {
 "port": 3306,
 "targetPort": 3306
 }
],
 "selector": {
 "name": "mysql ldb" ④
 }
 }
}
```

}

- ❶ The kind of Kubernetes resource. In this case, a Service.
  - ❷ A unique name for the service.
  - ❸ `ports` is an array of objects that describes network ports exposed by the service. The `targetPort` attribute has to match a `containerPort` from a pod container definition, and the `port` attribute is the port that is exposed by the service. Clients connect to the service port and the service forwards packets to the pod `targetPort`.
  - ❹ `selector` is how the service finds pods to forward packets to. The target pods need to have matching labels in their metadata attributes. If the service finds multiple pods with matching labels, it load balances network connections between them.

Each service is assigned a unique IP address for clients to connect to. This IP address comes from another internal OpenShift SDN, distinct from the pods' internal network, but visible only to pods. Each pod matching the `selector` is added to the service resource as an endpoint.

# Discovering Services

An application typically finds a service IP address and port by using environment variables. For each service inside an OpenShift project, the following environment variables are automatically defined and injected into containers for all pods inside the same project:

- `SVC_NAME_SERVICE_HOST` is the service IP address.
  - `SVC_NAME_SERVICE_PORT` is the service TCP port.



## Note

The *SVC\_NAME* part of the variable is changed to comply with DNS naming restrictions: letters are capitalized and underscores (\_) are replaced by dashes (-).

Another way to discover a service from a pod is by using the OpenShift internal DNS server, which is visible only to pods. Each service is dynamically assigned an SRV record with an FQDN of the form:

**SVC\_NAME.PROJECT\_NAME.svc.cluster.local**

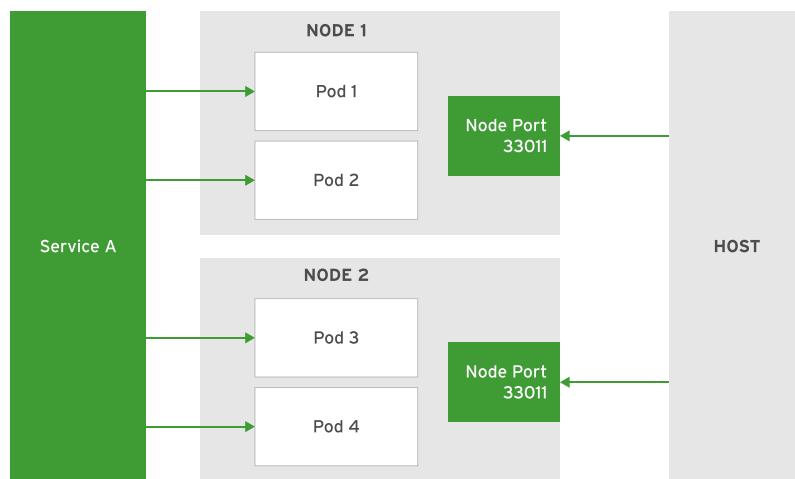
When discovering services using environment variables, a pod has to be created and started only after the service is created. If the application was written to discover services using DNS queries, however, it can find services created after the pod was started.

There are two ways for an application to access the service from outside an OpenShift cluster:

1. **NodePort** type: This is an older Kubernetes-based approach, where the service is exposed to external clients by binding to available ports on the compute node host, which then proxies connections to the service IP address. Use the `oc edit svc` command to edit service attributes and specify `NodePort` as the value for `type`, and provide a port value for the `nodePort` attribute. OpenShift then proxies connections to the service via the public IP address of the compute node host and the port value set in `NodePort`.

2. OpenShift Routes: This is the preferred approach in OpenShift to expose services using a unique URL. Use the `oc expose` command to expose a service for external access or expose a service from the OpenShift web console.

*Figure 6.5 illustrates how NodePort services allow external access to Kubernetes services. OpenShift routes are covered in more detail later in this course.*



**Figure 6.5: Alternative method for external access to a Kubernetes service**

OpenShift provides the `oc port-forward` command for forwarding a local port to a pod port. This is different from having access to a pod through a service resource:

- The port-forwarding mapping exists only on the workstation where the `oc` client runs, while a service maps a port for all network users.
- A service load balances connections to potentially multiple pods, whereas a port-forwarding mapping forwards connections to a single pod.



### Note

Red Hat discourages the use of the NodePort approach to avoid exposing the service to direct connections. Mapping via port-forwarding in OpenShift is considered a more secure alternative.

The following example demonstrates the use of the `oc port-forward` command:

```
[user@host ~]$ oc port-forward mysql-openshift-1-glqrp 3306:3306
```

The command forwards port 3306 from the developer machine to port 3306 on the db pod, where a MySQL server (inside a container) accepts network connections.



### Note

When running this command, make sure you leave the terminal window running. Closing the window or canceling the process stops the port mapping.

## Creating Applications

Simple applications, complex multitier applications, and microservice applications can be described by a single resource definition file. This single file would contain many pod definitions, service definitions to connect the pods, replication controllers or Deployment to horizontally scale the application pods, PersistentVolumeClaims to persist application data, and anything else needed that can be managed by OpenShift.

The `oc new-app` command can be used with the `-o json` or `-o yaml` option to create a skeleton resource definition file in JSON or YAML format, respectively. This file can be customized and used to create an application using the `oc create -f <filename>` command, or merged with other resource definition files to create a composite application.

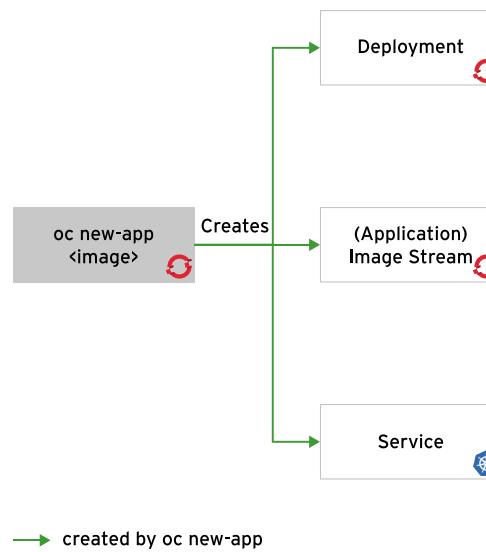
The `oc new-app` command can create application pods to run on OpenShift in many different ways. It can create pods from existing docker images, from Dockerfiles, and from raw source code using the Source-to-Image (S2I) process.

Run the `oc new-app -h` command to understand all the different options available for creating new applications on OpenShift.

The following command creates an application based on an image, `mysql`, from Docker Hub, with the label set to `db=mysql`:

```
[user@host ~]$ oc new-app mysql MYSQL_USER=user MYSQL_PASSWORD=pass \
> MYSQL_DATABASE=testdb -l db=mysql
```

The following figure shows the Kubernetes and OpenShift resources created by the `oc new-app` command when the argument is a container image:



**Figure 6.6: Resources created for a new application**

The following command creates an application based on an image from a private Docker image registry:

```
[user@host ~]$ oc new-app --image=myregistry.com/mycompany/myapp --name=myapp
```

The following command creates an application based on source code stored in a Git repository:

```
[user@host ~]$ oc new-app https://github.com/openshift/ruby-hello-world \
> --name=ruby-hello
```

You will learn more about the Source-to-Image (S2I) process, its associated concepts, and more advanced ways to use `oc new-app` to build applications for OpenShift in the next section.

The following command creates an application based on an existing template:

```
[user@host ~]$ oc new-app \
> --template=mysql-persistent \
> -p MYSQL_USER=user1 -p MYSQL_PASSWORD=mypa55 -p MYSQL_DATABASE=testdb \
> -p MYSQL_ROOT_PASSWORD=r0otpa55 -p VOLUME_CAPACITY=10Gi
...output omitted...
```



### Note

You will learn more about templates on the next chapter.

## Managing Persistent Storage

In addition to the specification of custom images, you can create persistent storage and attach it to your application. In this way you can make sure your data is not lost when deleting your pods. To list the `PersistentVolume` objects in a cluster, use the `oc get pv` command:

```
[admin@host ~]$ oc get pv
NAME CAPACITY ACCESS MODES RECLAIM POLICY STATUS CLAIM ...
pv0001 1Mi RWO Retain Available ...
pv0002 10Mi RWX Recycle Available ...
...output omitted...
```

To see the YAML definition for a given `PersistentVolume`, use the `oc get` command with the `-o yaml` option:

```
[admin@host ~]$ oc get pv pv0001 -o yaml
apiVersion: v1
kind: PersistentVolume
metadata:
 creationTimestamp: ...value omitted...
 finalizers:
 - kubernetes.io/pv-protection
 labels:
 type: local
 name: pv0001
 resourceVersion: ...value omitted...
 selfLink: /api/v1/persistentvolumes/pv0001
 uid: ...value omitted...
```

```
spec:
 accessModes:
 - ReadWriteOnce
 capacity:
 storage: 1Mi
 hostPath:
 path: /data/pv0001
 type: ""
 persistentVolumeReclaimPolicy: Retain
status:
 phase: Available
```

To add more `PersistentVolume` objects to a cluster, use the `oc create` command:

```
[admin@host ~]$ oc create -f pv1001.yaml
```



### Note

The above `pv1001.yaml` file must contain a persistent volume definition, similar in structure to the output of the `oc get pv pv-name -o yaml` command.

## Requesting Persistent Volumes

When an application requires storage, you create a `PersistentVolumeClaim` (PVC) object to request a dedicated storage resource from the cluster pool. The following content from a file named `pvc.yaml` is an example definition for a PVC:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: myapp
spec:
 accessModes:
 - ReadWriteOnce
 resources:
 requests:
 storage: 1Gi
```

The PVC defines storage requirements for the application, such as capacity or throughput. To create the PVC, use the `oc create` command:

```
[admin@host ~]$ oc create -f pvc.yaml
```

After you create a PVC, OpenShift attempts to find an available `PersistentVolume` resource that satisfies the PVC's requirements. If OpenShift finds a match, it binds the `PersistentVolume` object to the `PersistentVolumeClaim` object. To list the PVCs in a project, use the `oc get pvc` command:

[admin@host ~]\$ oc get pvc						
NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
myapp	Bound	pv0001	1Gi	RWO		6s

## Chapter 6 | Deploying Containerized Applications on OpenShift

The output indicates whether a persistent volume is bound to the PVC, along with attributes of the PVC (such as capacity).

To use the persistent volume in an application pod, define a volume mount for a container that references the `PersistentVolumeClaim` object. The application pod definition below references a `PersistentVolumeClaim` object to define a volume mount for the application:

```
apiVersion: "v1"
kind: "Pod"
metadata:
 name: "myapp"
 labels:
 name: "myapp"
spec:
 containers:
 - name: "myapp"
 image: openshift/myapp
 ports:
 - containerPort: 80
 name: "http-server"
 volumeMounts:
 - mountPath: "/var/www/html"
 name: "pvol" ①
 volumes:
 - name: "pvol" ②
 persistentVolumeClaim:
 claimName: "myapp" ③
```

- ① This section declares that the `pvol` volume mounts at `/var/www/html` in the container file system.
- ② This section defines the `pvol` volume.
- ③ The `pvol` volume references the `myapp` PVC. If OpenShift associates an available persistent volume to the `myapp` PVC, then the `pvol` volume refers to this associated volume.

## Managing OpenShift Resources at the Command Line

There are several essential commands used to manage OpenShift resources as described below.

Use the `oc get` command to retrieve information about resources in the cluster. Generally, this command outputs only the most important characteristics of the resources and omits more detailed information.

The `oc get RESOURCE_TYPE` command displays a summary of all resources of the specified type. The following illustrates example output of the `oc get pods` command.

NAME	READY	STATUS	RESTARTS	AGE
nginx-1-5r583	1/1	Running	0	1h
myapp-1-l44m7	1/1	Running	0	1h

### oc get all

Use the `oc get all` command to retrieve a summary of the most important components of a cluster. This command iterates through the major resource types for the current project and prints out a summary of their information:

NAME	DOCKER_REPO	TAGS	UPDATED	
is/nginx	172.30.1.1:5000/basic-kubernetes/nginx	latest	About an hour ago	
NAME	REVISION	DESIRED	CURRENT	TRIGGERED_BY
dc/nginx	1	1	1	config,image(nginx:latest)
NAME	DESIRED	CURRENT	READY	AGE
rc/nginx-1	1	1	1	1h
NAME	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
svc/nginx	172.30.72.75	<none>	80/TCP, 443/TCP	1h
NAME	READY	STATUS	RESTARTS	AGE
po/nginx-1-ypp8t	1/1	Running	0	1h

### oc describe

If the summaries provided by `oc get` are insufficient, use the `oc describe RESOURCE_TYPE RESOURCE_NAME` command to retrieve additional information. Unlike the `oc get` command, there is no way to iterate through all the different resources by type. Although most major resources can be described, this functionality is not available across all resources. The following is an example output from describing a pod resource:

```
Name: mysql-openshift-1-glqrp
Namespace: mysql-openshift
Priority: 0
Node: cluster-worker-1/172.25.250.52
Start Time: Fri, 15 Feb 2019 02:14:34 +0000
Labels: app=mysql-openshift
 deployment=mysql-openshift-1
...output omitted...
Status: Running
IP: 10.129.0.85
```

### oc get

The `oc get RESOURCE_TYPE RESOURCE_NAME` command can be used to export a resource definition. Typical use cases include creating a backup, or to aid in the modification of a definition. The `-o yaml` option prints out the object representation in YAML format, but this can be changed to JSON format by providing a `-o json` option.

### oc create

This command creates resources from a resource definition. Typically, this is paired with the `oc get RESOURCE_TYPE RESOURCE_NAME -o yaml` command for editing definitions.

### oc edit

This command allows the user to edit resources of a resource definition. By default, this command opens a `vi` buffer for editing the resource definition.

### oc delete

The `oc delete RESOURCE_TYPE name` command removes a resource from an OpenShift cluster. Note that a fundamental understanding of the OpenShift architecture is needed here, because deleting managed resources such as pods results in new instances of those resources being automatically created. When a project is deleted, it deletes all of the resources and applications contained within it.

**oc exec**

The `oc exec CONTAINER_ID options` command executes commands inside a container. You can use this command to run interactive and noninteractive batch commands as part of a script.

## Labelling Resources

When working with many resources in the same project, it is often useful to group those resources by application, environment, or some other criteria. To establish these groups, you define labels for the resources in your project. Labels are part of the `metadata` section of a resource, and are defined as key/value pairs, as shown in the following example:

```
apiVersion: v1
kind: Service
metadata:
 ...contents omitted...
 labels: app: nexus template: nexus-persistent-template
 name: nexus
 ...contents omitted...
```

Many `oc` subcommands support a `-l` option to process resources from a label specification. For the `oc get` command, the `-l` option acts as a selector to only retrieve objects that have a matching label:

```
[user@host ~]$ oc get svc,deployments -l app=nexus
NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
service/nexus ClusterIP 172.30.29.218 <none> 8081/TCP 4h

NAME REVISION DESIRED CURRENT ...
deployment.apps.openshift.io/nexus 1 1 1 ...
```

**Note**

Although any label can appear in resources, both the `app` and `template` keys are common for labels. By convention, the `app` key indicates the application related to this resource. The `template` key labels all resources generated by the same template with the template's name.

When using templates to generate resources, labels are especially useful. A template resource has a `labels` section separated from the `metadata.labels` section. Labels defined in the `labels` section do not apply to the template itself, but are added to every resource generated by the template:

```
apiVersion: template.openshift.io/v1
kind: Template
labels: app: nexus template: nexus-persistent-template
metadata:
 ...contents omitted...
 labels: maintainer: redhat
 name: nexus-persistent
 ...contents omitted...
objects:
```

```
- apiVersion: v1
 kind: Service
 metadata:
 name: nexus
 labels: version: 1
...contents omitted...
```

The previous example defines a template resource with a single label: `maintainer: redhat`. The template generates a service resource with three labels: `app: nexus`, `template: nexus-persistent-template`, and `version: 1`.



## References

Additional information about pods and services is available in the *Pods and Services* section of the OpenShift Container Platform documentation:

### Architecture

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.10/html-single/architecture/index](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.10/html-single/architecture/index)

Additional information about creating images is available in the OpenShift Container Platform documentation:

### Creating Images

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.10/html-single/images/index](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.10/html-single/images/index)

Labels and label selectors details are available in *Working with Kubernetes Objects* section for the Kubernetes documentation:

### Labels and Selectors

<https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/>

## ► Guided Exercise

# Deploying a Database Server on OpenShift

In this exercise, you will create and deploy a MySQL database pod on OpenShift using the `oc new-app` command.

### Outcomes

You should be able to create and deploy a MySQL database pod on OpenShift.

### Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from Chapter 1 before executing any command of this practice.

On `workstation`, run the following command to set up the environment:

```
[student@workstation ~]$ lab openshift-resources start
```

## Instructions

- 1. Prepare the lab environment.

- 1.1. Load your classroom environment configuration.

Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```

- 1.2. Log in to the OpenShift cluster.

```
[student@workstation ~]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
Login successful
...output omitted...
```

- 1.3. Create a new project that contains your RHOCP developer username for the resources you create during this exercise:

```
[student@workstation ~]$ oc new-project ${RHT_OCP4_DEV_USER}-mysql-openshift
Now using project ...output omitted...
```

- 2. Create a new application from the `mysql-persistent` template using the `oc new-app` command.

This image requires that you use the `-p` option to set the `MYSQL_USER`, `MYSQL_PASSWORD`, `MYSQL_DATABASE`, `MYSQL_ROOT_PASSWORD` and `VOLUME_CAPACITY` environment variables.

Use the `--template` option with the `oc new-app` command to specify a template with persistent storage so that OpenShift does not pull the image from the internet:

```
[student@workstation ~]$ oc new-app \
> --template=mysql-persistent \
> -p MYSQL_USER=user1 -p MYSQL_PASSWORD=mypa55 -p MYSQL_DATABASE=testdb \
> -p MYSQL_ROOT_PASSWORD=r00tpa55 -p VOLUME_CAPACITY=10Gi
--> Deploying template "openshift/mysql-persistent" to project
${RHT_OCP4_DEV_USER}-mysql-openshift
...output omitted...
--> Creating resources ...
 secret "mysql" created
 service "mysql" created
 persistentvolumeclaim "mysql" created
 deploymentconfig.apps.openshift.io "mysql" created
--> Success
 Application is not exposed. You can expose services to the outside world by
executing one or more of the commands below:
 'oc expose service/mysql'
 Run 'oc status' to view your app.
```

- 3. Verify that the MySQL pod was created successfully and view the details about the pod and its service.
- 3.1. Run the `oc status` command to view the status of the new application and verify that the deployment of the MySQL image was successful:

```
[student@workstation ~]$ oc status
In project ${RHT_OCP4_DEV_USER}-mysql-openshift on server ...

svc/mysql - 172.30.151.91:3306
...output omitted...
deployment #1 deployed 6 minutes ago - 1 pod
```

- 3.2. List the pods in this project to verify that the MySQL pod is ready and running:

```
[student@workstation ~]$ oc get pods
NAME READY STATUS RESTARTS AGE
mysql-1-deploy 0/1 Completed 0 120s
mysql-1-5vfn4 1/1 Running 0 100s
```

**Note**

Notice the name of the running pod. You need this information to be able to log in to the MySQL database server later.

- 3.3. Use the `oc describe` command to view more details about the pod:

```
[student@workstation ~]$ oc describe pod mysql-1-5vfn4
Name: mysql-1-5vfn4
Namespace: ${RHT_OCP4_DEV_USER}-mysql-openshift
Priority: 0
Node: master01/192.168.50.10
Start Time: Mon, 29 Mar 2021 16:42:13 -0400
Labels: deployment=mysql-1
...output omitted...
Status: Running
IP: 10.10.0.34
...output omitted...
```

The output from the `oc describe` command might contain errors related to the readiness probe. You can ignore these errors.

- 3.4. List the services in this project and verify that the service to access the MySQL pod was created:

```
[student@workstation ~]$ oc get svc
NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
mysql ClusterIP 172.30.151.91 <none> 3306/TCP 10m
```

- 3.5. Retrieve the details of the `mysql` service using the `oc describe` command and note that the service type is `ClusterIP` by default:

```
[student@workstation ~]$ oc describe service mysql
Name: mysql
Namespace: ${RHT_OCP4_DEV_USER}-mysql-openshift
Labels: app=mysql-persistent
 app.kubernetes.io/component=mysql-persistent
 app.kubernetes.io/instance=mysql-persistent
 template=mysql-persistent-template
Annotations: openshift.io/generated-by: OpenShiftNewApp
...output omitted...
Selector: name=mysql
Type: ClusterIP
IP Family Policy: SingleStack
IP Families: IPv4
IP: 172.30.151.91
IPs: 172.30.151.91
Port: mysql 3306/TCP
TargetPort: 3306/TCP
Endpoints: 10.10.0.34:3306
Session Affinity: None
Events: <none>
```

- 3.6. List the persistent storage claims in this project:

```
[student@workstation ~]$ oc get pvc
NAME STATUS VOLUME CAPACITY ...
mysql Bound pvc-e9bf0b1f-47df-4500-afb6-77e826f76c15 10Gi ...
 standard
```

3.7. Retrieve the details of the mysql pvc using the oc describe command:

```
[student@workstation ~]$ oc describe pvc/mysql
Name: mysql
Namespace: ${RHT_OCP4_DEV_USER}-mysql-openshift
StorageClass: standard
Status: Bound
Volume: pvc-e9bf0b1f-47df-4500-afb6-77e826f76c15
Labels: app=mysql-persistent
 app.kubernetes.io/component=mysql-persistent
 app.kubernetes.io/instance=mysql-persistent
 template=mysql-persistent-template
Annotations: openshift.io/generated-by: OpenShiftNewApp
...output omitted...
Capacity: 10Gi
Access Modes: RWO
VolumeMode: Filesystem
Used By: mysql-1-5vfn4
...output omitted...
```

- ▶ 4. Connect to the MySQL database server and verify that the database was created successfully.

- 4.1. From the workstation machine, configure port forwarding between workstation and the database pod running on OpenShift using port 3306. The terminal will hang after executing the command.

```
[student@workstation ~]$ oc port-forward mysql-1-5vfn4 3306:3306
Forwarding from 127.0.0.1:3306 -> 3306
Forwarding from [::1]:3306 -> 3306
```

- 4.2. From the workstation machine open another terminal and connect to the MySQL server using the MySQL client.

```
[student@workstation ~]$ mysql -uuser1 -pmypa55 --protocol tcp -h localhost
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 13
Server version: 8.0.26 Source distribution

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql>
```

4.3. Verify the creation of the testdb database.

```
mysql> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| testdb |
+-----+
2 rows in set (0.00 sec)
```

4.4. Exit from the MySQL prompt:

```
mysql> exit
Bye
```

Close the terminal and return to the previous one. Finish the port forwarding process by pressing **Ctrl+C**.

```
Forwarding from 127.0.0.1:3306 -> 3306
Forwarding from [::1]:3306 -> 3306
Handling connection for 3306
^C
```

► 5. Delete the project to remove all the resources within the project:

```
[student@workstation ~]$ oc delete project ${RHT_OCP4_DEV_USER}-mysql-openshift
```

## Finish

On workstation, run the `lab openshift-resources finish` script to complete this lab.

```
[student@workstation ~]$ lab openshift-resources finish
```

This concludes the exercise.

# Creating Routes

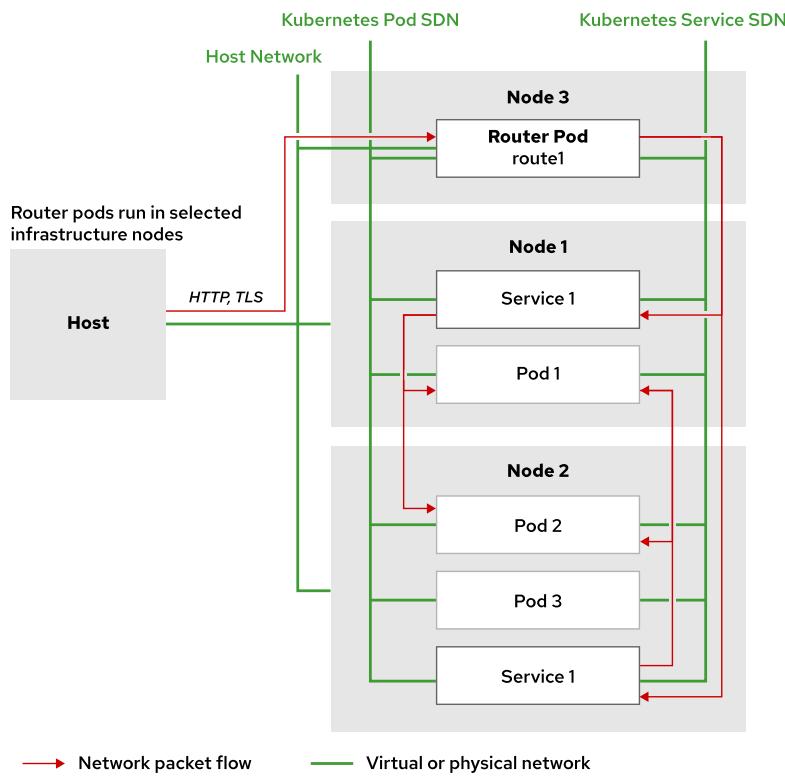
---

## Objectives

After completing this section, students should be able to expose services using OpenShift routes.

## Working with Routes

Services allow for network access between pods inside an OpenShift instance, and routes allow for network access to pods from users and applications outside the OpenShift instance.



**Figure 6.7: OpenShift routes and Kubernetes services**

A route connects a public-facing IP address and DNS host name to an internal-facing service IP. It uses the service resource to find the endpoints; that is, the ports exposed by the service.

OpenShift routes are implemented by a cluster-wide router service, which runs as a containerized application in the OpenShift cluster. OpenShift scales and replicates router pods like any other OpenShift application.

**Note**

In practice, to improve performance and reduce latency, the OpenShift router connects directly to the pods using the internal pod software-defined network (SDN).

The router service uses *HAProxy* as the default implementation.

An important consideration for OpenShift administrators is that the public DNS host names configured for routes need to point to the public-facing IP addresses of the nodes running the router. Router pods, unlike regular application pods, bind to their nodes' public IP addresses instead of to the internal pod SDN.

The following example shows a minimal route defined using JSON syntax:

```
{
 "apiVersion": "v1",
 "kind": "Route",
 "metadata": {
 "name": "quoteapp"
 },
 "spec": {
 "host": "quoteapp.apps.example.com",
 "to": {
 "kind": "Service",
 "name": "quoteapp"
 }
 }
}
```

The `apiVersion`, `kind`, and `metadata` attributes follow standard Kubernetes resource definition rules. The `Route` value for `kind` shows that this is a route resource, and the `metadata.name` attribute gives this particular route the identifier `quoteapp`.

As with pods and services, the main part is the `spec` attribute, which is an object containing the following attributes:

- `host` is a string containing the FQDN associated with the route. DNS must resolve this FQDN to the IP address of the OpenShift router. The details to modify DNS configuration are outside the scope of this course.
- `to` is an object stating the resource this route points to. In this case, the route points to an OpenShift Service with the name set to `quoteapp`.

**Note**

Names of different resource types do not collide. It is perfectly legal to have a route named `quoteapp` that points to a service also named `quoteapp`.

**Important**

Unlike services, which use selectors to link to pod resources containing specific labels, a route links directly to the service resource name.

## Creating Routes

Use the `oc create` command to create route resources, just like any other OpenShift resource. You must provide a JSON or YAML resource definition file, which defines the route, to the `oc create` command.

The `oc new-app` command does not create a route resource when building a pod from container images, Containerfiles, or application source code. After all, `oc new-app` does not know if the pod is intended to be accessible from outside the OpenShift instance or not.

Another way to create a route is to use the `oc expose service` command, passing a service resource name as the input. The `--name` option can be used to control the name of the route resource. For example:

```
[user@host ~]$ oc expose service quotedb --name quote
```

By default, routes created by `oc expose` generate DNS names of the form:

```
route-name-project-name.default-domain
```

Where:

- route-name* is the name assigned to the route. If no explicit name is set, OpenShift assigns the route the same name as the originating resource (for example, the service name).
- project-name* is the name of the project containing the resource.
- default-domain* is configured on the OpenShift Control Plane and corresponds to the wildcard DNS domain listed as a prerequisite for installing OpenShift.

For example, creating a route named `quote` in project named `test` from an OpenShift instance where the wildcard domain is `cloudapps.example.com` results in the FQDN `quote-test.cloudapps.example.com`.



### Note

The DNS server that hosts the wildcard domain knows nothing about route host names. It merely resolves any name to the configured IP addresses. Only the OpenShift router knows about route host names, treating each one as an HTTP virtual host. The OpenShift router blocks invalid wildcard domain host names that do not correspond to any route and returns an HTTP 404 error.

## Leveraging the Default Routing Service

The default routing service is implemented as an HAProxy pod. Router pods, containers, and their configuration can be inspected just like any other resource in an OpenShift cluster:

```
[user@host ~]$ oc get pod --all-namespaces | grep router
openshift-ingress router-default-746b5cfb65-f6sdm 1/1 Running 1 4d
```

Note that you can query information on the default router using the associated label as shown here.

By default, router is deployed in openshift-ingress project. Use `oc describe pod` command to get the routing configuration details:

```
[user@host ~]$ oc describe pod router-default-746b5cfb65-f6sdm
Name: router-default-746b5cfb65-f6sdm
Namespace: openshift-ingress
...output omitted...
Containers:
 router:
 ...output omitted...
 Environment:
 STATS_PORT: 1936
 ROUTER_SERVICE_NAMESPACE: openshift-ingress
 DEFAULT_CERTIFICATE_DIR: /etc/pki/tls/private
 ROUTER_SERVICE_NAME: default
 ROUTER_CANONICAL_HOSTNAME: apps.cluster.lab.example.com
 ...output omitted...
```

The subdomain, or default domain to be used in all default routes, takes its value from the `ROUTER_CANONICAL_HOSTNAME` entry.



## References

Additional information about the architecture of routes in OpenShift is available in the *Architecture* and *Developer Guide* sections of the

**OpenShift Container Platform documentation.**

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.10/](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.10/)

## ► Guided Exercise

# Exposing a Service as a Route

In this exercise, you will create, build, and deploy an application on an OpenShift cluster and expose its service as a route.

## Outcomes

You should be able to expose a service as a route for a deployed OpenShift application.

## Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab openshift-routes start
```

## Instructions

► 1. Prepare the lab environment.

- 1.1. Load your classroom environment configuration.

Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```

- 1.2. Log in to the OpenShift cluster.

```
[student@workstation ~]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
```

```
Login successful
```

```
...output omitted...
```

- 1.3. Create a new project that contains your RHOCUP developer username for the resources you create during this exercise.

```
[student@workstation ~]$ oc new-project ${RHT_OCP4_DEV_USER}-route
```

► 2. Create a new PHP application using the `quay.io/redhattraining/php-hello-dockerfile` image.

- 2.1. Use the `oc new-app` command to create the PHP application.

**Important**

The following example uses a backslash (\) to indicate that the second line is a continuation of the first line. If you wish to ignore the backslash, you can type the entire command in one line.

```
[student@workstation ~]$ oc new-app \
> --image=quay.io/redhattraining/php-hello-dockerfile \
> --name php-helloworld
--> Found container image 4b696cc (2 years old) from quay.io for "quay.io/
redhattraining/php-hello-dockerfile"
...output omitted...
--> Creating resources ...
...output omitted...
--> Success
Application is not exposed. You can expose services to the outside world by
executing one or more of the commands below:
'oc expose service/php-helloworld'
Run 'oc status' to view your app.
```

- 2.2. Wait until the application finishes deploying by monitoring the progress with the `oc get pods -w` command:

```
[student@workstation ~]$ oc get pods -w
NAME READY STATUS RESTARTS AGE
php-helloworld-74bb86f6cb-zt6wl 1/1 Running 0 5s
^C
```

Your exact output may differ in names, status, timing, and order. The container in `Running` status with a random suffix (`74bb86f6cb-zt6wl` in the example) contains the application and shows it is up and running.

Alternatively, monitor the deployment logs with the `oc logs -f php-helloworld-74bb86f6cb-zt6wl` command. Press Ctrl + C to exit the command if necessary.

```
[student@workstation ~]$ oc logs -f php-helloworld-74bb86f6cb-zt6wl
AH00558: httpd: Could not reliably determine the server's fully qualified domain
name, using 10.129.5.124. Set the 'ServerName' directive globally to suppress
this message
[09-Aug-2021 22:09:45] NOTICE: [pool www] 'user' directive is ignored when FPM is
not running as root
[09-Aug-2021 22:09:45] NOTICE: [pool www] 'group' directive is ignored when FPM is
not running as root
^C
```

Your exact output may differ.

- 2.3. Review the service for this application using the `oc describe` command:

```
[student@workstation ~]$ oc describe svc/php-helloworld
Name: php-helloworld
Namespace: user-route
Labels: app=php-helloworld
 app.kubernetes.io/component=php-helloworld
 app.kubernetes.io/instance=php-helloworld
Annotations: openshift.io/generated-by: OpenShiftNewApp
Selector: deployment=php-helloworld
Type: ClusterIP
IP: 172.30.100.236
Port: 8080-tcp 8080/TCP
TargetPort: 8080/TCP
Endpoints: 10.129.5.124:8080
Session Affinity: None
Events: <none>
```

The IP address and namespace displayed in the output of the command may differ.

- ▶ 3. Expose the service, which creates a route. Use the default name and fully qualified domain name (FQDN) for the route:

```
[student@workstation ~]$ oc expose svc/php-helloworld
route.route.openshift.io/php-helloworld exposed

[student@workstation ~]$ oc describe route
Name: php-helloworld
Namespace: user-route
Created: 16 seconds ago
Labels: app=php-helloworld
 app.kubernetes.io/component=php-helloworld
 app.kubernetes.io/instance=php-helloworld
Annotations: openshift.io/host.generated=true
Requested Host: php-helloworld-user-route.apps.na46-stage2.dev.nextcle.com
 exposed on router default
 (host apps.na46-stage2.dev.nextcle.com) 16 seconds ago
Path: <none>
TLS Termination: <none>
Insecure Policy: <none>
Endpoint Port: 8080-tcp

Service: php-helloworld
Weight: 100 (100%)
Endpoints: 10.129.5.124:8080
```

- ▶ 4. Access the service from a host external to the cluster to verify that the service and route are working.

```
[student@workstation ~]$ curl \
> php-helloworld-${RHT_OCP4_DEV_USER}-route.${RHT_OCP4_WILDCARD_DOMAIN}
Hello, World! PHP version is 7.2.11
```

**Note**

The output of the PHP application depends on the actual image version. It may be different from yours.

Notice the FQDN is comprised of the application name and project name by default. The remainder of the FQDN, the subdomain, is defined when OpenShift is installed.

- ▶ 5. Replace this route with a route named xyz.

5.1. Delete the current route:

```
[student@workstation ~]$ oc delete route/php-helloworld
route.route.openshift.io "php-helloworld" deleted
```

**Note**

Deleting the route is optional. You can have multiple routes for the same service, provided they have different names.

5.2. Create a route for the service with a name of \${RHT\_OCP4\_DEV\_USER}-xyz.

```
[student@workstation ~]$ oc expose svc/php-helloworld \
> --name=${RHT_OCP4_DEV_USER}-xyz
route.route.openshift.io/${RHT_OCP4_DEV_USER}-xyz exposed

[student@workstation ~]$ oc describe route
Name: user-xyz
Namespace: user-route
Created: 23 seconds ago
Labels: app=php-helloworld
 app.kubernetes.io/component=php-helloworld
 app.kubernetes.io/instance=php-helloworld
Annotations: openshift.io/host.generated=true
Requested Host: user-xyz-user-route.apps.na46-stage2.dev.nextcle.com
 exposed on router default
 (host apps.na46-stage2.dev.nextcle.com) 22 seconds ago
Path: <none>
TLS Termination: <none>
Insecure Policy: <none>
Endpoint Port: 8080-tcp
```

```
Service: php-helloworld
Weight: 100 (100%)
Endpoints: 10.129.5.124:8080
```

Your exact output may differ. Note the new FQDN that was generated based on the new route name. Both the route name and the project name contain your user name, hence it appears twice in the route FQDN.

- 5.3. Make an HTTP request using the FQDN on port 80:

```
[student@workstation ~]$ curl \
> ${RHT_OCP4_DEV_USER}-xyz-${RHT_OCP4_DEV_USER}-route.${RHT_OCP4_WILDCARD_DOMAIN}
Hello, World! PHP version is 7.2.11
```

## Finish

On workstation, run the `lab openshift-routes finish` script to complete this exercise.

```
[student@workstation ~]$ lab openshift-routes finish
```

This concludes the guided exercise.

# Creating Applications with Source-to-Image

---

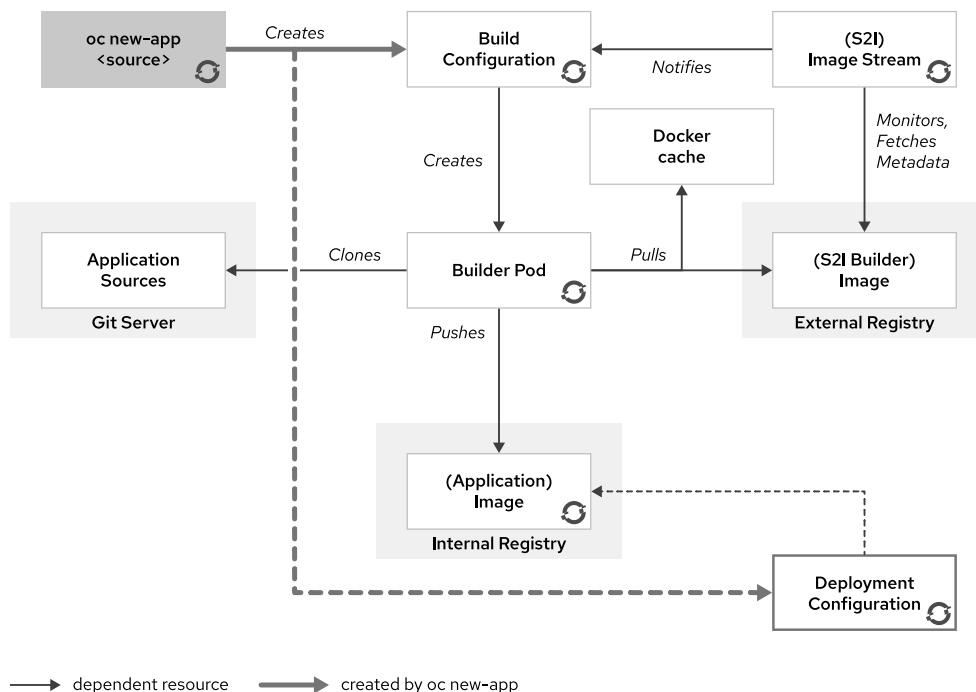
## Objectives

After completing this section, students should be able to deploy an application using the Source-to-Image (S2I) facility of OpenShift Container Platform.

## The Source-to-Image (S2I) Process

Source-to-Image (S2I) is a tool that makes it easy to build container images from application source code. This tool takes an application's source code from a Git repository, injects the source code into a base container based on the language and framework desired, and produces a new container image that runs the assembled application.

This figure shows the resources created by the `oc new-app <source>` command when the argument is an application source code repository. Notice that S2I also creates a Deployment and all its dependent resources:



**Figure 6.8: Deployment and dependent resources**

S2I is the primary strategy used for building applications in OpenShift Container Platform. The main reasons for using source builds are:

- User efficiency: Developers do not need to understand Dockerfiles and operating system commands such as `yum install`. They work using their standard programming language tools.

- Patching: S2I allows for rebuilding all the applications consistently if a base image needs a patch due to a security issue. For example, if a security issue is found in a PHP base image, then updating this image with security patches updates all applications that use this image as a base.
- Speed: With S2I, the assembly process can perform a large number of complex operations without creating a new layer at each step, resulting in faster builds.
- Ecosystem: S2I encourages a shared ecosystem of images where base images and scripts can be customized and reused across multiple types of applications.

## Describing Image Streams

OpenShift deploys new versions of user applications into pods quickly. To create a new application, in addition to the application source code, a base image (the S2I builder image) is required. If either of these two components gets updated, OpenShift creates a new container image. Pods created using the older container image are replaced by pods using the new image.

Even though it is evident that the container image needs to be updated when application code changes, it may not be evident that the deployed pods also need to be updated should the builder image change.

The image stream resource is a configuration that names specific container images associated with image stream tags, an alias for these container images. OpenShift builds applications against an image stream. The OpenShift installer populates several image streams by default during installation. To determine available image streams, use the `oc get` command, as follows:

```
[user@host ~]$ oc get is -n openshift
NAME IMAGE REPOSITORY TAGS
cli ...svc:5000/openshift/cli latest
dotnet ...svc:5000/openshift/dotnet 2.1,...,3.1-el7,latest
dotnet-runtime ...svc:5000/openshift/dotnet-runtime 2.1,...,3.1-el7,latest
httpd ...svc:5000/openshift/httpd 2.4,2.4-el7,2.4-el8,latest
jenkins ...svc:5000/openshift/jenkins 2,latest
mariadb ...svc:5000/openshift/mariadb 10.3,10.3-el7,10.3-el8,latest
mongodb ...svc:5000/openshift/mongodb 3.6,latest
mysql ...svc:5000/openshift/mysql 8.0,8.0-el7,8.0-el8,latest
nginx ...svc:5000/openshift/nginx 1.10,1.12,1.8,latest
nodejs ...svc:5000/openshift/nodejs 10,...,12-ubi7,12-ubi8
perl ...svc:5000/openshift/perl 5.26,...,5.30,5.30-el7
php ...svc:5000/openshift/php 7.2-ubi8,...,7.3-ubi8,latest
postgresql ...svc:5000/openshift/postgresql 10,10-el7,...,12-el7,12-el8
python ...svc:5000/openshift/python 2.7,2.7-ubi7,...,3.6-ubi8,3.8
redis ...svc:5000/openshift/redis 5,5-el7,5-el8,latest
ruby ...svc:5000/openshift/ruby 2.5,2.5-ubi7,...,2.6,2.6-ubi7
...
```



### Note

Your OpenShift instance may have more or fewer image streams depending on local additions and OpenShift point releases.

OpenShift detects when an image stream changes and takes action based on that change. If a security issue arises in the `rhe18/nodejs-10` image, it can be updated in the image repository, and OpenShift can automatically trigger a new build of the application code.

It is likely that an organization chooses several supported base S2I images from Red Hat, but may also create their own base images.

## Building an Application with S2I and the CLI

Building an application with S2I can be accomplished using the OpenShift CLI.

An application can be created using the S2I process with the `oc new-app` command from the CLI:

```
[user@host ~]$ oc new-app php~http://my.git.server.com/my-app \ ①②
> --name=myapp ③
```

- ① The image stream used in the process appears to the left of the tilde (~).
- ② The URL after the tilde indicates the location of the source code's Git repository.
- ③ Sets the application name.



### Note

Instead of using the tilde, you can set the image stream by using the `-i` option or `--image-stream` for the full version.

```
[user@host ~]$ oc new-app -i php http://services.lab.example.com/app \
> --name=myapp
```

The `oc new-app` command allows creating applications using source code from a local or remote Git repository. If only a source repository is specified, `oc new-app` tries to identify the correct image stream to use for building the application. In addition to application code, S2I can also identify and process Dockerfiles to create a new image.

The following example creates an application using the Git repository in the current directory:

```
[user@host ~]$ oc new-app .
```



### Important

When using a local Git repository, the repository must have a remote origin that points to a URL accessible by the OpenShift instance.

It is also possible to create an application using a remote Git repository and a context subdirectory:

```
[user@host ~]$ oc new-app https://github.com/openshift/sti-ruby.git \
> --context-dir=2.0/test/puma-test-app
```

Finally, it is possible to create an application using a remote Git repository with a specific branch reference:

```
[user@host ~]$ oc new-app https://github.com/openshift/ruby-hello-world.git#beta4
```

If an image stream is not specified in the command, new-app attempts to determine which language builder to use based on the presence of certain files in the root of the repository:

Language	Files
Ruby	Rakefile, Gemfile, config.ru
Java EE	pom.xml
Node.js	app.json, package.json
PHP	index.php, composer.json
Python	requirements.txt, config.py
Perl	index.pl, cpanfile

After a language is detected, the new-app command searches for image stream tags that have support for the detected language, or an image stream that matches the name of the detected language.

Create a JSON resource definition file by using the `-o json` parameter and output redirection:

```
[user@host ~]$ oc -o json new-app php-http://services.lab.example.com/app \
> --name=myapp > s2i.json
```

This JSON definition file creates a list of resources. The first resource is the image stream:

```
...output omitted...
{
 "kind": "ImageStream", ①
 "apiVersion": "image.openshift.io/v1",
 "metadata": {
 "name": "myapp", ②
 "creationTimestamp": null
 "labels": {
 "app": "myapp"
 },
 "annotations": {
 "openshift.io/generated-by": "OpenShiftNewApp"
 }
 },
 "spec": {
 "lookupPolicy": {
 "local": false
 }
 },
 "status": {
 "dockerImageRepository": ""
 }
}
```

```

 },
},
...output omitted...

```

- ➊ Define a resource type of image stream.
- ➋ Name the image stream myapp.

The build configuration (bc) is responsible for defining input parameters and triggers that are executed to transform the source code into a runnable image. The **BuildConfig** (BC) is the second resource, and the following example provides an overview of the parameters used by OpenShift to create a runnable image.

```

...output omitted...
{
 "kind": "BuildConfig", ➊
 "apiVersion": "build.openshift.io/v1",
 "metadata": {
 "name": "myapp", ➋
 "creationTimestamp": null,
 "labels": {
 "app": "myapp"
 },
 "annotations": {
 "openshift.io/generated-by": "OpenShiftNewApp"
 }
 },
 "spec": {
 "triggers": [
 {
 "type": "GitHub",
 "github": {
 "secret": "S5_4BZpPabM6KrIuPBvI"
 }
 },
 {
 "type": "Generic",
 "generic": {
 "secret": "3q8K8JNDoRzhjoz1KgMz"
 }
 },
 {
 "type": "ConfigChange"
 },
 {
 "type": "ImageChange",
 "imageChange": {}
 }
],
 "source": {
 "type": "Git",
 "git": {
 "uri": "http://services.lab.example.com/app" ➌
 }
 }
 }
}

```

```

},
"strategy": {
 "type": "Source", ④
 "sourceStrategy": {
 "from": {
 "kind": "ImageStreamTag",
 "namespace": "openshift",
 "name": "php:7.3" ⑤
 }
 }
},
"output": {
 "to": {
 "kind": "ImageStreamTag",
 "name": "myapp:latest" ⑥
 }
},
"resources": {},
"postCommit": {},
"nodeSelector": null
},
"status": {
 "lastVersion": 0
}
},
...output omitted...

```

- ①** Define a resource type of `BuildConfig`.
- ②** Name the `BuildConfig` `myapp`.
- ③** Define the address to the source code Git repository.
- ④** Define the strategy to use S2I.
- ⑤** Define the builder image as the `php:7.3` image stream.
- ⑥** Name the output image stream `myapp:latest`.

The third resource is the deployment object that is responsible for customizing the deployment process in OpenShift. It may include parameters and triggers that are necessary to create new container instances, and are translated into a replication controller from Kubernetes. Some of the features provided by `Deployment` objects are:

- User customizable strategies to transition from the existing deployments to new deployments.
- Have as many active replica set as wanted and possible.
- Replication scaling depends of the sizes of old and new replica sets.

```

...output omitted...
{
 "kind": "Deployment", ①
 "apiVersion": "apps/v1",
 "metadata": {
 "name": "myapp", ②
 }
}

```

```

 "creationTimestamp": null,
 "labels": {
 "app": "myapp",
 "app.kubernetes.io/component": "myapp",
 "app.kubernetes.io/instance": "myapp"
 },
 "annotations": {
 "image.openshift.io/triggers": "[{"from": {"kind": "ImageStreamTag", "name": "myapp:latest"}, "path": "spec.template.spec.containers[?(@.name==\"myapp\")].image"}]", ❸
 "openshift.io/generated-by": "OpenShiftNewApp"
 }
},
"spec": {
 "replicas": 1,
 "selector": {
 "matchLabels": {
 "deployment": "myapp"
 }
 },
 "template": {
 "metadata": {
 "creationTimestamp": null,
 "labels": {
 "deployment": "myapp" ❹
 },
 "annotations": {
 "openshift.io/generated-by": "OpenShiftNewApp"
 }
 },
 "spec": {
 "containers": [
 {
 "name": "myapp", ❺
 "image": " ", ❻
 "ports": [
 {
 "containerPort": 8080,
 "protocol": "TCP"
 },
 {
 "containerPort": 8443,
 "protocol": "TCP"
 }
],
 "resources": {}
 }
]
 },
 "strategy": {}
 },
}

```

```

 "status": {}
 },
...output omitted...

```

- ① Define a resource type of Deployment.
- ② Name the Deployment myapp.
- ③ An image change trigger causes the creation of a new deployment each time a new version of the myapp:latest image is available in the repository.
- ④ A configuration change trigger causes a new deployment to be created any time the replication controller template changes.
- ⑤ Defines the container image to deploy: myapp:latest.
- ⑥ Specifies the container ports. A configuration change trigger causes a new deployment to be created any time the replication controller template changes.

The last item is the service, already covered in previous chapters:

```

...output omitted...
{
 "kind": "Service",
 "apiVersion": "v1",
 "metadata": {
 "name": "myapp",
 "creationTimestamp": null,
 "labels": {
 "app": "myapp"
 "app.kubernetes.io/component": "myapp",
 "app.kubernetes.io/instance": "myapp"
 },
 "annotations": {
 "openshift.io/generated-by": "OpenShiftNewApp"
 }
 },
 "spec": {
 "ports": [
 {
 "name": "8080-tcp",
 "protocol": "TCP",
 "port": 8080,
 "targetPort": 8080
 },
 {
 "name": "8443-tcp",
 "protocol": "TCP",
 "port": 8443,
 "targetPort": 8443
 }
],
 "selector": {
 "deployment": "myapp"
 }
 }
}

```

```

},
"status": {
 "loadBalancer": {}
}
}

```

**Note**

By default, the `oc new-app` command does not create a route. You can create a route after creating the application. However, a route is automatically created when using the web console because it uses a template.

After creating a new application, the build process starts. Use the `oc get builds` command to see a list of application builds:

```
[user@host ~]$ oc get builds
NAME TYPE FROM STATUS STARTED DURATION
php-helloworld-1 Source Git@9e17db8 Running 13 seconds ago
```

OpenShift allows viewing the build logs. The following command shows the last few lines of the build log:

```
[user@host ~]$ oc logs build/myapp-1
```

**Important**

If the build is not Running yet, or OpenShift has not deployed the `s2i-build` pod yet, the above command throws an error. Just wait a few moments and retry it.

Trigger a new build with the `oc start-build build-config-name` command:

```
[user@host ~]$ oc get buildconfig
NAME TYPE FROM LATEST
myapp Source Git 1
```

```
[user@host ~]$ oc start-build myapp
build "myapp-2" started
```

## Relationship Between Build and Deployment

The `BuildConfig` pod is responsible for creating the images in OpenShift and pushing them to the internal container registry. Any source code or content update typically requires a new build to guarantee the image is updated.

The `Deployment` pod is responsible for deploying pods to OpenShift. The outcome of a `Deployment` pod execution is the creation of pods with the images deployed in the internal container registry. Any existing running pod may be destroyed, depending on how the `Deployment` resource is set.

The **BuildConfig** and **Deployment** resources do not interact directly. The **BuildConfig** resource creates or updates a container image. The **Deployment** reacts to this new image or updated image event and creates pods from the container image.



## References

### Source-to-Image (S2I) Build

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.10/html-single/cicd/builds#builds-strategy-s2i-build\\_understanding-image-builds](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.10/html-single/cicd/builds#builds-strategy-s2i-build_understanding-image-builds)

### S2I GitHub repository

<https://github.com/openshift/source-to-image>

## ► Guided Exercise

# Creating a Containerized Application with Source-to-Image

In this exercise, you will build an application from source code and deploy the application to an OpenShift cluster.

## Outcomes

You should be able to:

- Build an application from source code using the OpenShift command-line interface.
- Verify the successful deployment of the application using the OpenShift command-line interface.

## Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Run the following command to download the relevant lab files and configure the environment:

```
[student@workstation ~]$ lab openshift-s2i start
```

## Instructions

- 1. Inspect the PHP source code for the sample application and create and push a new branch named `s2i` to use during this exercise.
- 1.1. Enter your local clone of the `D0180-apps` Git repository and checkout the `master` branch of the course's repository to ensure you start this exercise from a known good state:

```
[student@workstation ~]$ cd ~/D0180-apps
[student@workstation D0180-apps]$ git checkout master
...output omitted...
```

- 1.2. Create a new branch to save any changes you make during this exercise:

```
[student@workstation D0180-apps]$ git checkout -b s2i
Switched to a new branch 's2i'

[student@workstation D0180-apps]$ git push -u origin s2i
...output omitted...
* [new branch] s2i -> s2i
Branch 's2i' set up to track remote branch 's2i' from 'origin'.
```

13. Review the PHP source code of the application, inside the the `php-helloworld` folder.

Open the `index.php` file in the `~/D0180-apps/php-helloworld` folder:

```
<?php
print "Hello, World! php version is " . PHP_VERSION . "\n";
?>
```

The application implements a simple response which returns the PHP version it is running.

► **2.** Prepare the lab environment.

- 2.1. Load your classroom environment configuration.

Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation D0180-apps]$ source /usr/local/etc/ocp4.config
```

- 2.2. Log in to the OpenShift cluster.

```
[student@workstation D0180-apps]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
Login successful
...output omitted...
```

- 2.3. Create a new project that contains your RHOCP developer username for the resources you create during this exercise:

```
[student@workstation D0180-apps]$ oc new-project ${RHT_OCP4_DEV_USER}-s2i
```

► **3.** Create a new PHP application using Source-to-Image from the `php-helloworld` directory using the `s2i` branch you created in the previous step in your fork of the DO180-apps Git repository.

- 3.1. Use the `oc new-app` command to create the PHP application.



**Important**

The following example uses the number sign (#) to select a specific branch from the git repository, in this case the `s2i` branch created in the previous step.

```
[student@workstation D0180-apps]$ oc new-app php:7.3 --name=php-helloworld \
> https://github.com/${RHT_OCP4_GITHUB_USER}/D0180-apps#s2i \
> --context-dir php-helloworld
```

- 3.2. Wait for the build to complete and the application to deploy. Verify that the build process starts with the `oc get pods` command.

```
[student@workstation openshift-s2i]$ oc get pods
NAME READY STATUS RESTARTS AGE
php-helloworld-1-build 1/1 Running 0 5s
```

- 3.3. Examine the logs for this build. Use the build pod name for this build, `php-helloworld-1-build`.

```
[student@workstation D0180-apps]$ oc logs --all-containers \
> -f php-helloworld-1-build
...output omitted...

Writing manifest to image destination
Storing signatures
Generating dockerfile with builder image image-registry.openshift-image-...
php@sha256:3206...37b4
Adding transient rw bind mount for /run/secrets/rhsm
STEP 1: FROM image-registry.openshift-image-registry.svc:5000...
...output omitted...

STEP 8: RUN /usr/libexec/s2i/assemble
...output omitted...

Pushing image .../php-helloworld:latest ...
Getting image source signatures
...output omitted...

Writing manifest to image destination
Storing signatures
Successfully pushed .../php-
helloworld@sha256:3f1cdb278548c7f24429e2469c51ae35482d54e2616d596ab6fb59d6b432c454
Push successful
Cloning "https://github.com/${RHT_OCP4_GITHUB_USER}/D0180-apps" ...
Commit: 9a042f7e3650ef38ad07af83b74f57c7a7d1820c (Added start up script)
...output omitted...
```

Notice that the clone of the Git repository is the first step of the build. Next, the Source-to-Image process built a new image called  `${RHT_OCP4_DEV_USER} -s2i /php-helloworld:latest`. The last step in the build process is to push this image to the OpenShift private registry.

- 3.4. Review the Deployment for this application:

```
[student@workstation D0180-apps]$ oc describe deployment/php-helloworld
Name: php-helloworld
Namespace: ${RHT_OCP4_DEV_USER}-s2i
CreationTimestamp: Tue, 30 Mar 2021 12:54:59 -0400
Labels: app=php-helloworld
 app.kubernetes.io/component=php-helloworld
 app.kubernetes.io/instance=php-helloworld
```

```

Annotations: deployment.kubernetes.io/revision: 2
 image.openshift.io/triggers:
 [{"from": {"kind": "ImageStreamTag", "name": "php-
helloworld:latest"}, "fieldPath": "spec.template.spec.containers[?(@.name==\"php-
helloworld\")...]
 openshift.io/generated-by: OpenShiftNewApp
Selector: deployment=php-helloworld
Replicas: 1 desired | 1 updated | 1 total | 1 available | 0
 unavailable
StrategyType: RollingUpdate
MinReadySeconds: 0
RollingUpdateStrategy: 25% max unavailable, 25% max surge
Pod Template:
 Labels: deployment=php-helloworld
 Annotations: openshift.io/generated-by: OpenShiftNewApp
 Containers:
 php-helloworld:
 Ports: 8080/TCP, 8443/TCP
 Host Ports: 0/TCP, 0/TCP
 Environment: <none>
 Mounts: <none>
 Volumes: <none>
 Conditions:
 Type Status Reason
 ---- -----
 Available True MinimumReplicasAvailable
 Progressing True NewReplicaSetAvailable
 OldReplicaSets: <none>
 NewReplicaSet: php-helloworld-6f5d4c47ff (1/1 replicas created)
...output omitted...

```

3.5. Add a route to test the application:

```
[student@workstation D0180-apps]$ oc expose service php-helloworld \
> --name ${RHT_OCP4_DEV_USER}-helloworld
route.route.openshift.io/${RHT_OCP4_DEV_USER}-helloworld exposed
```

3.6. Find the URL associated with the new route:

```
[student@workstation D0180-apps]$ oc get route -o jsonpath='{..spec.host}{"\n"}'
${RHT_OCP4_DEV_USER}-helloworld-${RHT_OCP4_DEV_USER}-s2i.
${RHT_OCP4_WILDCARD_DOMAIN}
```



### Note

The URL is displayed in a single line.

3.7. Test the application by sending an HTTP GET request to the URL you obtained in the previous step. Type the URL in a single line.

```
[student@workstation D0180-apps]$ curl -s \
> ${RHT_OCP4_DEV_USER}-helloworld-${RHT_OCP4_DEV_USER}-s2i.\
> ${RHT_OCP4_WILDCARD_DOMAIN}
Hello, World! php version is 7.3.29
```

The php:7.3 image stream might contain a more recent version of PHP 7.3.

- ▶ 4. Explore starting application builds by changing the application in its Git repository and executing the proper commands to start a new Source-to-Image build.

- 4.1. Enter the source code directory.

```
[student@workstation D0180-apps]$ cd ~/D0180-apps/php-helloworld
```

- 4.2. Edit the index.php file as shown below:

```
<?php
print "Hello, World! php version is " . PHP_VERSION . "\n";
print "A change is a coming!\n";
?>
```

Save the file.

- 4.3. Commit the changes and push the code back to the remote Git repository:

```
[student@workstation php-helloworld]$ git add .
[student@workstation php-helloworld]$ git commit -m 'Changed index page contents.'
[s2i b1324aa] changed index page contents
 1 file changed, 1 insertion(+)
[student@workstation php-helloworld]$ git push origin s2i
...output omitted...
Counting objects: 7, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (3/3), done.
Writing objects: 100% (4/4), 417 bytes | 0 bytes/s, done.
Total 4 (delta 1), reused 0 (delta 0)
remote: Resolving deltas: 100% (1/1), completed with 1 local object.
To https://github.com/${RHT_OCP4_GITHUB_USER}/D0180-apps
 f7cd896..b1324aa s2i -> s2i
```

- 4.4. Start a new Source-to-Image build process and wait for it to build and deploy:

```
[student@workstation php-helloworld]$ oc start-build php-helloworld
build.build.openshift.io/php-helloworld-2 started

[student@workstation php-helloworld]$ oc get pods
NAME READY STATUS RESTARTS AGE
php-helloworld-1-build 0/1 Completed 0 5m7s
php-helloworld-2-build 0/1 Completed 0 43s
...output omitted...

[student@workstation php-helloworld]$ oc logs php-helloworld-2-build -f
```

*...output omitted...*

```
Successfully pushedphp-helloworld:latest@sha256:74e757a4c0edaeda497dab7...
Push successful
```

**Note**

Logs may take some seconds to be available after the build starts. If the previous command fails, wait a bit and try again.

- 4.5. After the second build has completed use the `oc get pods` command to verify that the new version of the application is running.

```
[student@workstation php-helloworld]$ oc get pods
NAME READY STATUS RESTARTS AGE
php-helloworld-1-build 0/1 Completed 0 11m
php-helloworld-1-deploy 0/1 Completed 0 10m
php-helloworld-2-build 0/1 Completed 0 45s
php-helloworld-2-deploy 0/1 Completed 0 16s
php-helloworld-2-wq9wz 1/1 Running 0 13s
```

- 4.6. Test that the application serves the new content. Type the URL in a single line.

```
[student@workstation php-helloworld]$ curl -s \
> ${RHT_OCP4_DEV_USER}-helloworld-${RHT_OCP4_DEV_USER}-s2i.\
> ${RHT_OCP4_WILDCARD_DOMAIN}
Hello, World! php version is 7.3.29
A change is a coming!
```

**Finish**

On workstation, run the `lab openshift-s2i finish` script to complete this lab.

```
[student@workstation php-helloworld]$ lab openshift-s2i finish
```

This concludes the guided exercise.

# Creating Applications with the OpenShift Web Console

---

## Objectives

After completing this section, students should be able to:

- Create an application with the OpenShift web console.
- Manage and monitor the build cycle of an application.
- Examine resources for an application.

## Accessing the OpenShift Web Console

The OpenShift web console allows users to execute many of the same tasks as the OpenShift command-line client. You can create projects, add applications to projects, view application resources, and manipulate application configurations as needed. The OpenShift web console runs as one or more pods, each pod running on a Control Plane.

Although the command-line client is more versatile than the web-console, you may find that the visual representation of the concepts in OpenShift will be helpful learning.

The web console runs in a web browser.

The default URL is of the format `https://console-openshift-console.${RHT_OCP4_WILDCARD_DOMAIN}`. By default, OpenShift generates a self-signed certificate for the web console. You must trust this certificate in order to gain access.

The web console uses a REST API to communicate with the OpenShift cluster. By default, the REST API endpoint is accessed with a different DNS name and self-signed certificate. You must also trust this certificate for the REST API endpoint.

After you have trusted the two OpenShift certificates, the console requires authentication to proceed.

## Managing Projects

Upon successful login, the Home > Projects page displays a list of projects you can access. From this page you can create, edit, or delete a project.

If you have permission to view cluster metrics, then you are instead redirected to the Home > Overview page. This page shows general information and metrics about the cluster. The Home > Overview menu item is hidden from users without authority to view cluster metrics.

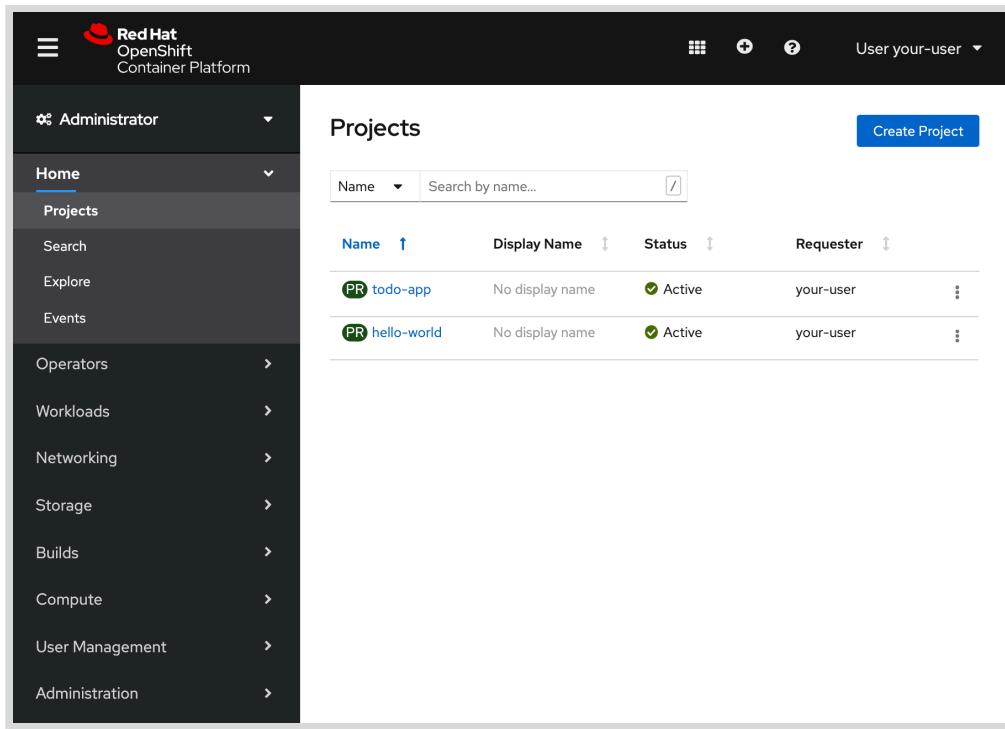


Figure 6.9: OpenShift web console home page

The ellipsis icon at the end of each row provides a menu with project actions. Select the appropriate entry to edit or delete the project.

If you click a project link in this view, you are redirected to the **Project Status** page which shows all of the applications created within that project space.

## Navigating the Web Console

A navigation menu is located on the left side of the web console. The menu includes two perspectives: **Administrator** and **Developer**. Each item in the menu expands to provide access to a set of related management functions. When the **Administrator** perspective is selected, these items are as follows:

### Home

The home menu allows users to quickly access projects and resources. From this menu, you can browse and manage projects, search or explore cluster resources, and inspect cluster events.

### Operators

The **OperatorHub** is a catalog that allows you to discover, search and install operators in the cluster. After installing an operator, you can use the **Installed Operators** option to manage the operator or search for other installed operators.



#### Note

The latest Kubernetes versions implement many controllers as Operators. Operators are Kubernetes plug-in components that can react to cluster events and control the state of resources. Operators and the CoreOS Operator Framework are outside the scope of this document.

## Workloads

These options enable management of several types of Kubernetes and OpenShift resources, such as pods and deployments. Other advanced deployment options that are accessible from this menu, such as configuration maps, secrets, and cron jobs, are beyond the scope of the course.

## Networking

This menu contains options to manage OpenShift resources that affect application access, such as services and routes, for a project. Other options for configuring an OpenShift Network Policy or Ingress are available, but these topics are outside the scope of this course.

## Storage

This menu contains options to configure persistent storage for project applications. In particular, persistent volumes and persistent volume claims for a project are managed from the **Storage** menu.

## Builds

The **Build Configs** option displays a list of project build configurations. Click a build configuration link in this view to access an overview page for the specified build configuration. From this page, you can view and edit the application's build configuration.

The **Builds** option provides a list of recent build processes for application container images in the project. Click the link for a particular build to access the build logs for that particular build process.

The **Image Streams** option provides a list of image streams defined in the project. Click an image stream entry in this list to access an overview page to view and manage that image stream.

## Compute

Provides options to access and manage the compute nodes of the OpenShift cluster. From this page, you can also configure node health checks and autoscaling.

## User management

From this option, you can configure authentication and authorization using users, groups, roles, role bindings and service accounts.

## Administration

Provides options to manage cluster and project settings, such as resource quotas and role-based access controls. Functions in the **Administration** section are outside the scope of this course.

# Creating New Applications

From the **Developer** perspective, use **+Add** to select a way to create a new application in an OpenShift project. You can add an application from the **Developer Catalog**, by using the **All services** option, which offers a selection of Source-to-Image (S2I) templates, builder images and Helm charts to create technology-specific applications. Select a desired template, and provide the necessary information to deploy the new application.

You are not limited to deploying an application from the catalog. You can also deploy an application using:

- A container image hosted on a remote container registry.
- A YAML file that specifies the Kubernetes and OpenShift resources to create.
- A builder image using the source code or a Containerfile from your own git repository.

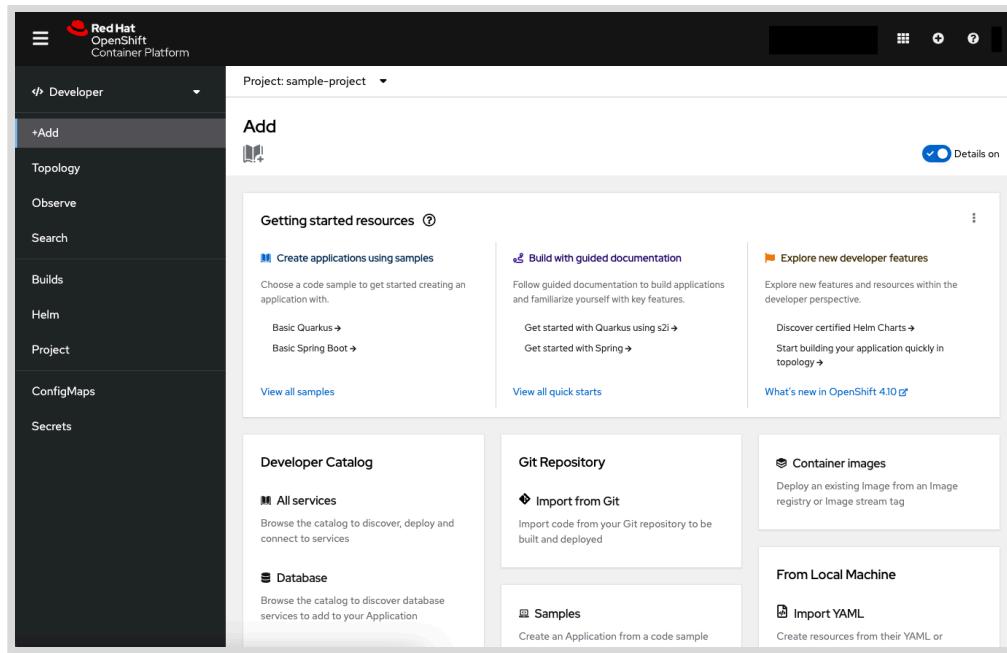


Figure 6.10: OpenShift Developer Catalog page

To create an application with one of these methods, select the appropriate option in the **Add** page. Use the **Container images** option to deploy an existing container image. Use the **Import YAML** option to create the resources specified in a YAML file. Use the **Import from Git** option to deploy your source code using a builder image or your Containerfile. The **Database**, **Operator Backed** and **Helm Chart** options are shortcuts to the catalog.

## Managing Application Builds

From the **Administrator** perspective, click the **Build Configs** option of the **Builds** menu after you add a Source-to-Image application to a project. The new build configuration is accessible from this view:

Name	Namespace	Labels	Created
BC todoapp	NS test	app=todoapp	Aug 3, 1:42 pm

Figure 6.11: OpenShift build configurations page

Click a build configuration in the list to view an overview page for the selected build configuration. From the overview page, you can:

- View the build configuration parameters, such as the URL for the source code's Git repository.
- View and edit the environment variables that are set in the builder container, during an application build process.
- View a list of recent application builds, and click a selected build to access logs from the build process.

## Managing Deployed Applications

The Workloads menu provides access to deployments in the project:

The screenshot shows the Red Hat OpenShift Container Platform web interface. The top navigation bar includes the Red Hat logo, 'Red Hat OpenShift Container Platform', and a search bar with the text 'test'. On the far right is the 'OpenShift Administrator' dropdown. The left sidebar has a dark theme with a light gray header. It features a user icon and the text 'Administrator'. Below this are several menu items: 'Home', 'Operators', 'Workloads' (which is expanded to show 'Pods', 'Deployments', 'Deployment Configs', 'Stateful Sets', 'Secrets', and 'Config Maps'), and a 'Create Deployment Config' button. The 'Deployment Configs' section is currently active, displaying a table with one row. The table columns are 'Name' (sorted by name), 'Namespace' (sorted by namespace), 'Status' (sorted by status), 'Labels' (sorted by labels), and 'Pod Selector' (sorted by pod selector). The single entry in the table is 'todoapp' in the 'test' namespace, with a status of '1 of 1 pods', labels 'app=todoapp', and a pod selector 'app=todoapp, deploymentconfig=todoapp'. There is also a three-dot menu icon at the end of the table row.

Figure 6.12: OpenShift Workloads menu

Under workloads, you will find many of the constructs discussed in the course including pods, Deployments, and Config Maps.

Click a deployments entry in the list to view an overview page for the selection. From the overview page, you can:

- View the deployments parameters, such as the specifications of an application container image.
- Change the desired number of application pods to manually scale the application.
- View and edit the environment variables that are set in the deployed application container.
- View a list of application pods, and click a selected pod to access logs for that pod.

## Other Web Console Features

The web console allows you to:

- Manage resources, such as project quotas, user membership, secrets, and other advanced resources.
- Create persistent volume claims.
- Monitor builds, deployments, pods, and system events.
- Create continuous integration and deployment pipelines.

Detailed usage for the above features is outside the scope of this course.

## ► Guided Exercise

# Creating an Application with the Web Console

In this exercise, you will create, build, and deploy an application to an OpenShift cluster using the OpenShift web console.

## Outcomes

You should be able to create, build, and deploy an application to an OpenShift cluster using the web console.

## Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Get the lab files by executing the lab script:

```
[student@workstation ~]$ lab openshift-webconsole start
```

The lab script verifies that the OpenShift cluster is running.

## Instructions

- 1. Inspect the PHP source code for the sample application and create and push a new branch named `console` to use during this exercise.
  - 1.1. Enter your local clone of the `D0180-apps` Git repository and checkout the `master` branch of the course's repository to ensure you start this exercise from a known good state:

```
[student@workstation ~]$ cd ~/D0180-apps
[student@workstation D0180-apps]$ git checkout master
...output omitted...
```

- 1.2. Create a new branch to save any changes you make during this exercise:

```
[student@workstation D0180-apps]$ git checkout -b console
Switched to a new branch 'console'

[student@workstation D0180-apps]$ git push -u origin console
...output omitted...
 * [new branch] console -> console
Branch 'console' set up to track remote branch 'console' from 'origin'.
```

- 1.3. Review the PHP source code of the application, inside the the `php-helloworld` folder.

Open the index.php file in the ~/D0180-apps/php-helloworld folder:

```
<?php
print "Hello, World! php version is " . PHP_VERSION . "\n";
?>
```

The application implements a simple response which returns the PHP version it is running.

- ▶ 2. Open a web browser and navigate to [https://console-openshift-console.\\${RHT\\_OCP4\\_WILDCARD\\_DOMAIN}](https://console-openshift-console.${RHT_OCP4_WILDCARD_DOMAIN}) to access the OpenShift web console. Log in and create a new project named *youruser-console*.

- 2.1. Load your classroom environment configuration.

Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```

- 2.2. Retrieve the value of the wildcard domain specific to your cluster, using the \${RHT\_OCP4\_WILDCARD\_DOMAIN}

```
[student@workstation ~]$ echo ${RHT_OCP4_WILDCARD_DOMAIN}
apps.cluster.lab.example.com
```

- 2.3. Open the Firefox browser and navigate to [https://console-openshift-console.\\${RHT\\_OCP4\\_WILDCARD\\_DOMAIN}](https://console-openshift-console.${RHT_OCP4_WILDCARD_DOMAIN}) to access the OpenShift web console. Click **RedHatTraining**, and then log in to the OpenShift console using your credentials.

- 2.4. Select the **Administrator** perspective from the list at the top of the left menu.

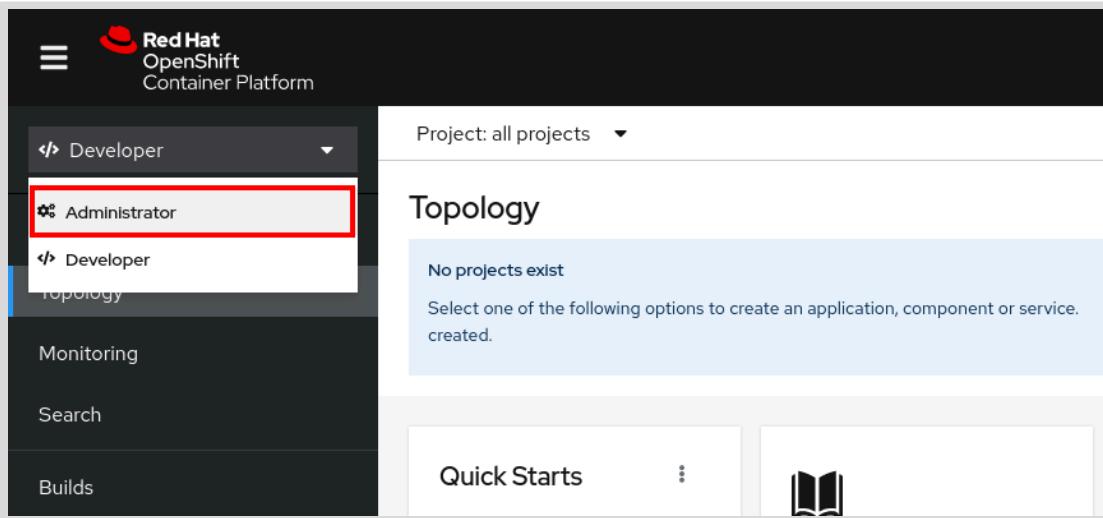


Figure 6.13: Administrator perspective drop-down

- 2.5. Create a new project named *youruser-console*. You can type any values you prefer in the other fields.

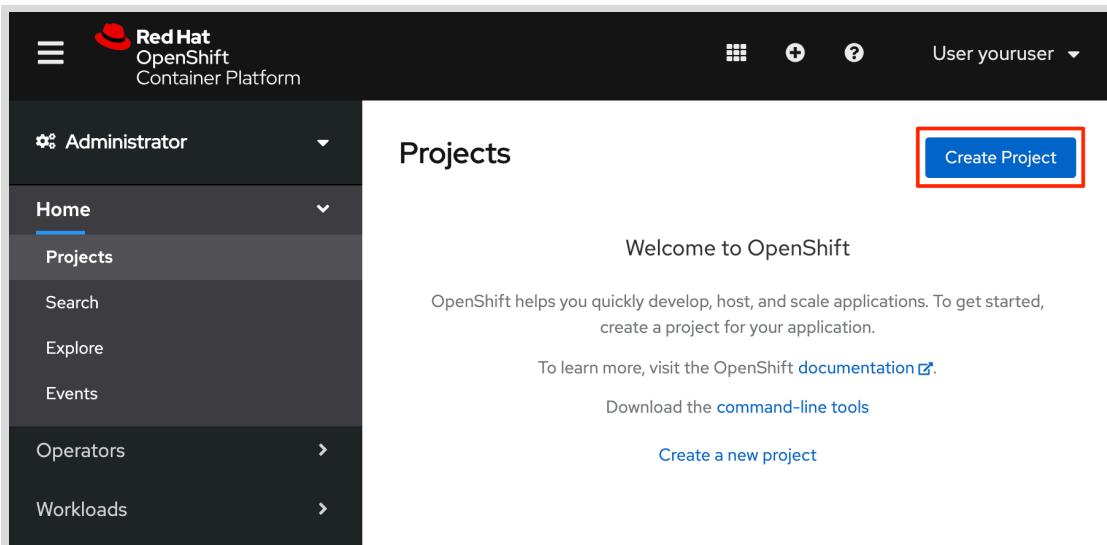


Figure 6.14: Create a new project

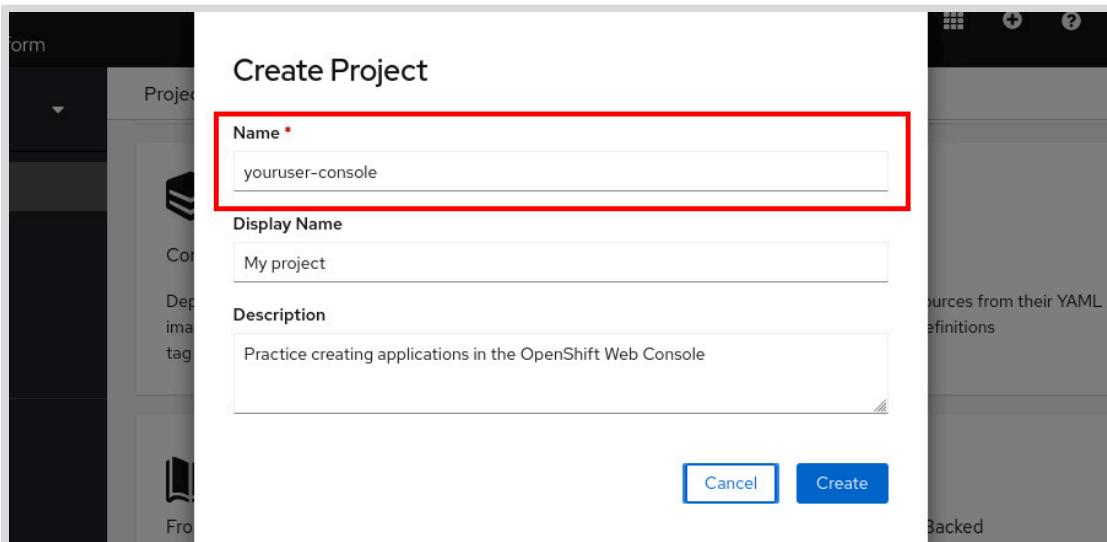


Figure 6.15: Create a new project

- 2.6. After you have completed the required fields, click **Create** in the **Create Project** dialog box to go to the **Project Status** page for the *youruser-console* project:

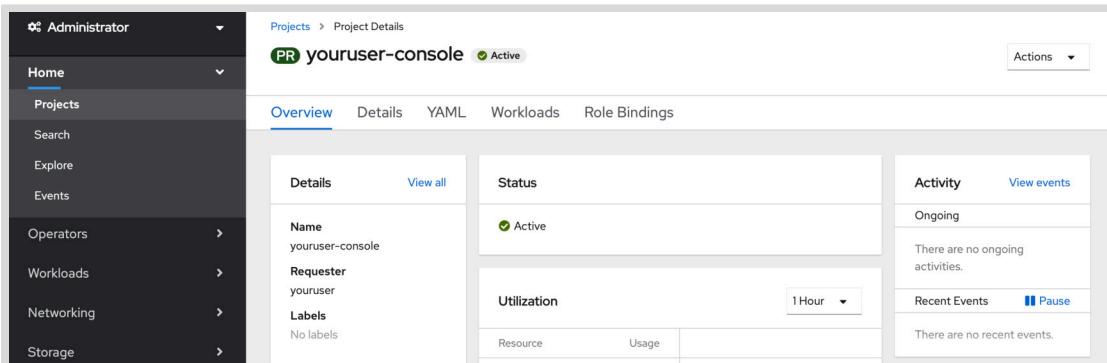


Figure 6.16: Project Status page

- 3. Create the new php-helloworld application with a PHP template.

- 3.1. Select the Developer perspective from the list at the top of the left menu.

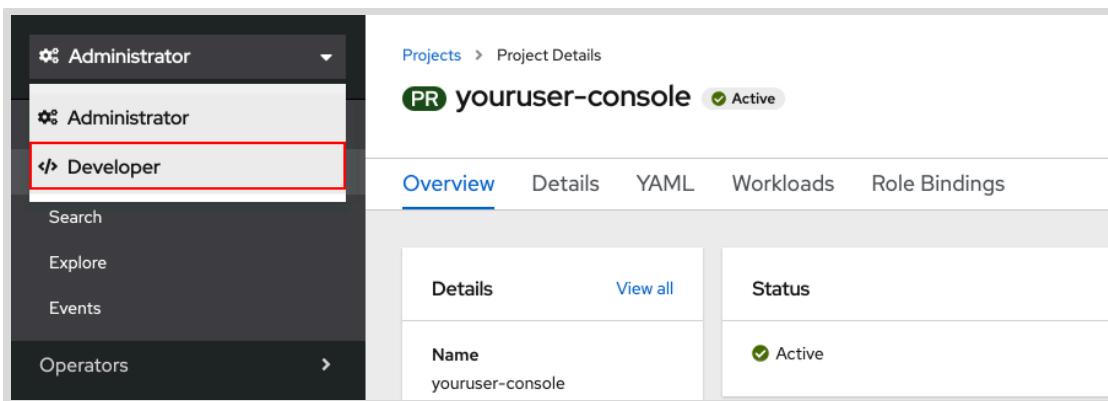


Figure 6.17: Developer perspective drop-down

- 3.2. Click +Add on the left menu. Scroll on the opened page, click From Catalog, to open the Developer Catalog section.

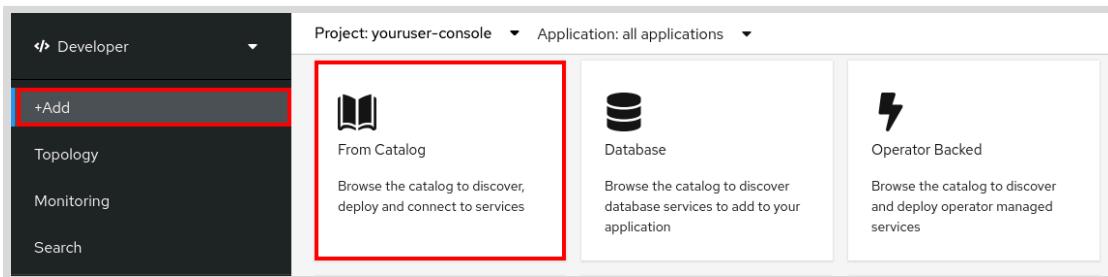


Figure 6.18: Developer Catalog page

- 3.3. Enter php in the Filter by keyword field.

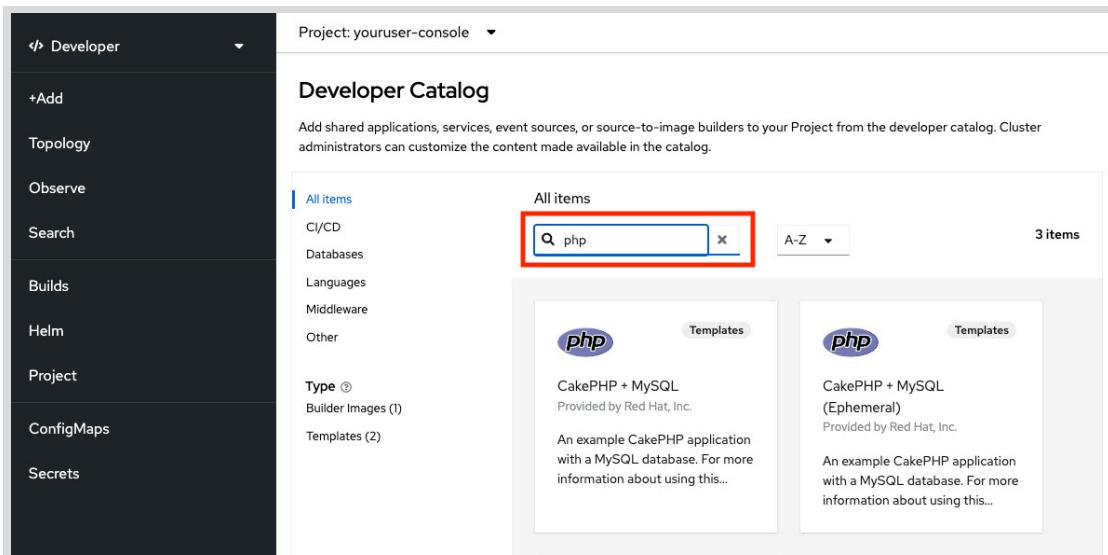


Figure 6.19: Finding PHP-related templates

- 3.4. After filtering, click the **PHP builder image** to display the PHP dialog box. Click **Create Application** to display the Create Source-to-Image Application page.

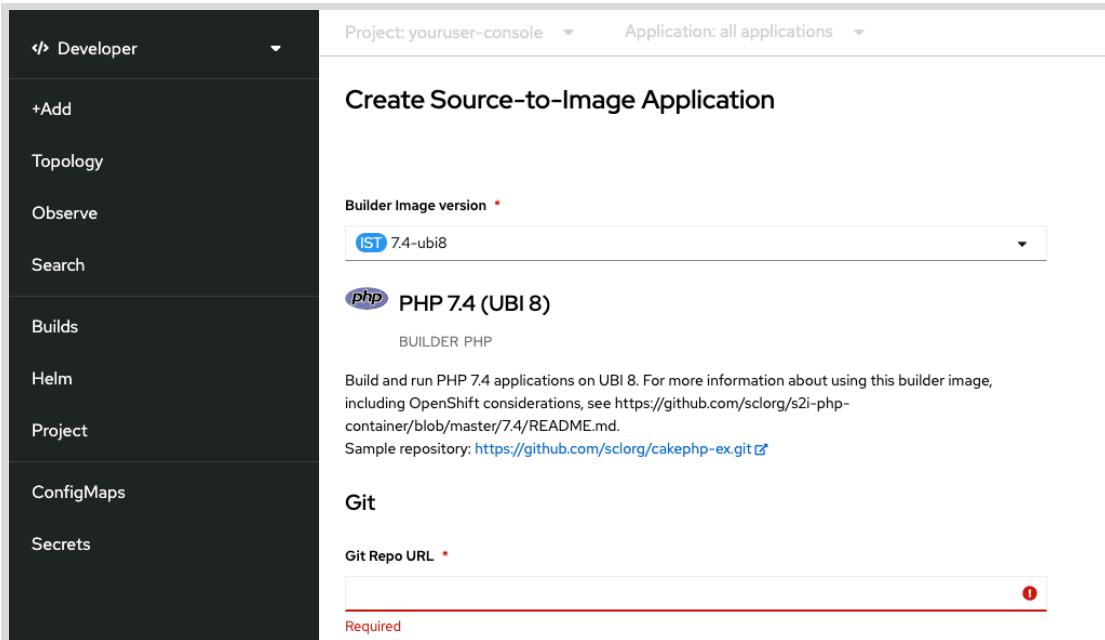


Figure 6.20: Configuring Source-to-Image for a PHP application

3.5. Change the Builder Image Version to PHP version 7.4 (UBI 8).

Specify the location of the source code git repository: <https://github.com/yourgituser/D0180-apps>

Use the Advanced Git Options to set the context directory to `php-helloworld` and branch `console` for this exercise

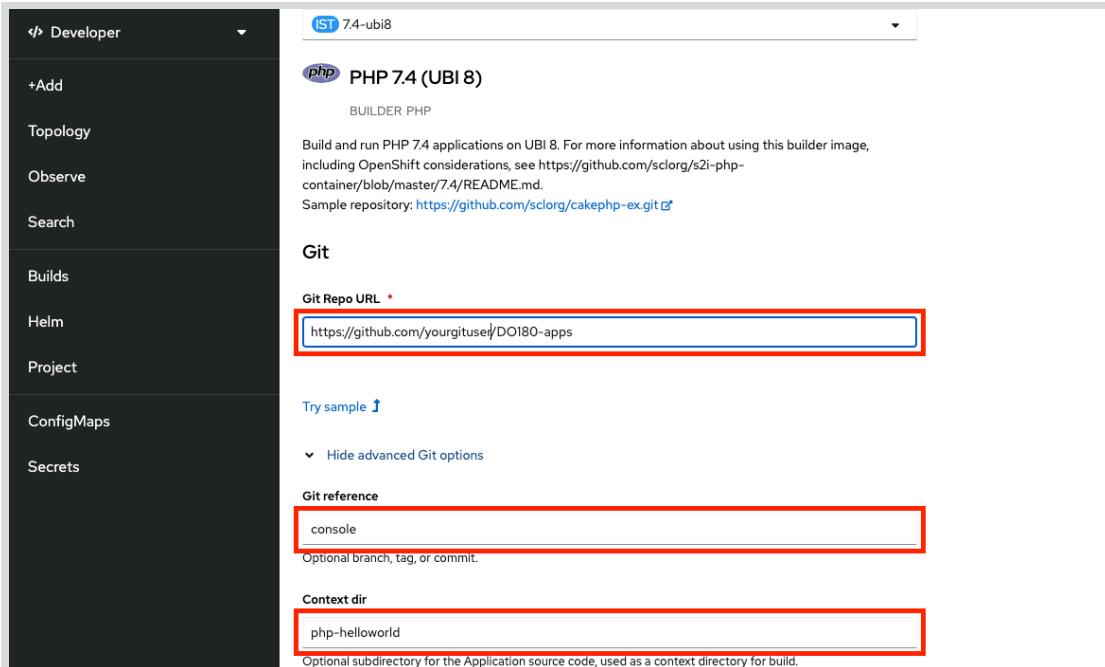


Figure 6.21: Setting Advanced Git Options for the application

Enter `php-helloworld` for both the application name and the name used for associated resources. Select **Deployment** as the resource type.

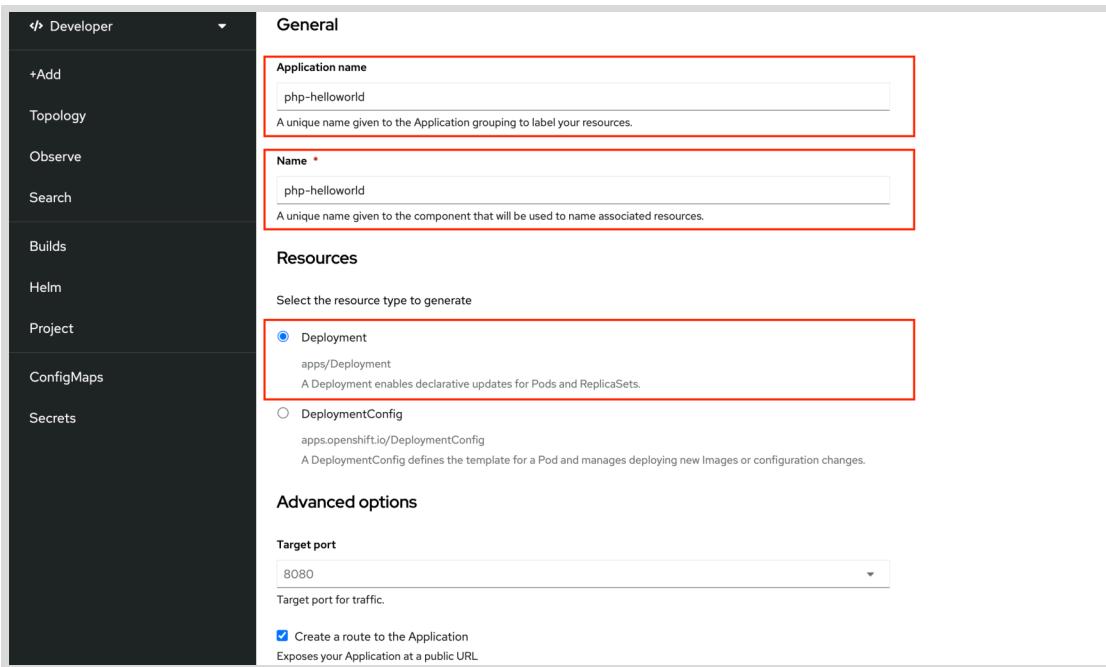


Figure 6.22: Setting application options

Scroll to the bottom of the page, and select **Create a route to the application**. Click **Create** to create the required OpenShift and Kubernetes resources for the application.

You are redirected to the **Topology** page:

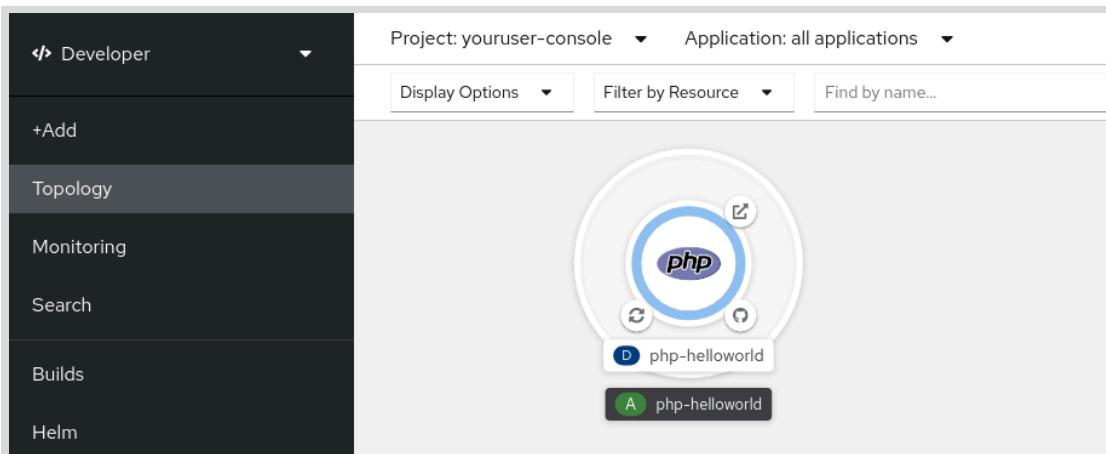


Figure 6.23: Topology page

This page indicates that the **php-helloworld** application is created. The **D** annotation to the left of the **php-helloworld** link is an acronym for Deployment. This link redirects to a page containing information about the application's deployment.

- 3.6. Switch back to the **Administrator** perspective for the remainder of the exercise:

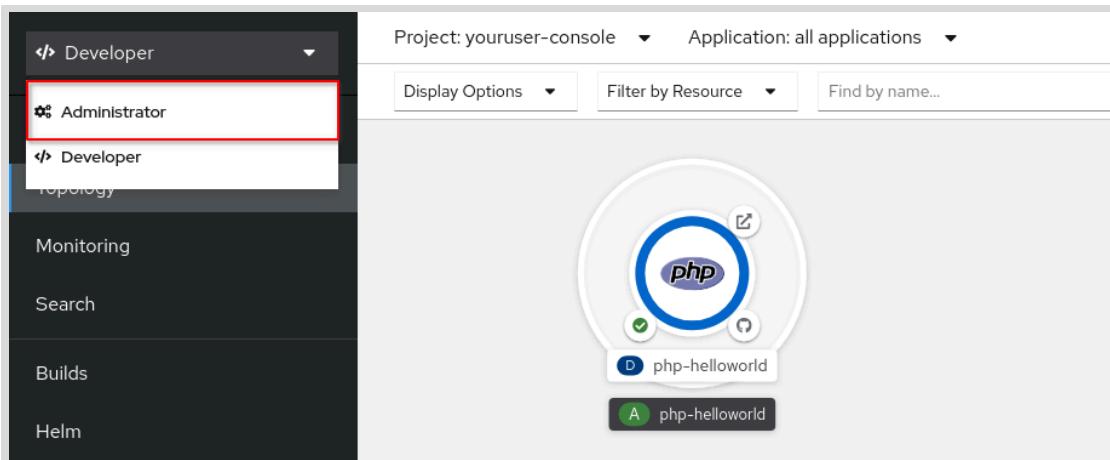


Figure 6.24: Administrator perspective drop-down

- 4. Use the navigation bar on the left side of the OpenShift web console to locate information for the application's OpenShift and Kubernetes resources:
- Deployments
  - BuildConfig
  - Build Logs
  - Service
  - Route
- 4.1. Examine the deployment. In the navigation bar, click **Workloads > Deployments** to display a list of deployments for the **youruser-console** project. Click the **php-helloworld** link to display deployment details.

The screenshot shows the 'Deployment details' page for the 'php-helloworld' deployment. The left sidebar shows the 'Workloads' category selected, with 'Deployments' highlighted. The main content area shows the deployment details for 'php-helloworld'. It includes a summary section with a blue circle containing the number '1 Pod'. Below this, there are sections for 'Name' (php-helloworld), 'Namespace' (jmzzjv-console), 'Labels' (app=php-helloworld, app.kubernetes.io/component=php-helloworld, app.kubernetes.io/instance=php-helloworld, app.kubernetes.io/name=php-helloworld), and 'Update strategy' (RollingUpdate). Other settings shown include 'Max unavailable' (25% of 1 pod) and 'Max surge' (25% greater than 1 pod). A 'Progress deadline seconds' setting is also listed as 600 seconds.

Figure 6.25: Application deployment details page

Explore the available information from the **Details** tab. The build may still be running when you reach this page, so the Deployment might not have a value of 1 pod, yet.

If you click the up and down arrow icons next to the doughnut chart that indicates the number of pods, you can scale the application up and down horizontally.

- 4.2. Examine the build configuration. In the navigation bar, click **Builds > Build Configs** to display a list of build configurations for the *youruser-console* project. Click the **php-helloworld** link to display the build configuration for the application.

The screenshot shows the 'BuildConfig details' page for the 'php-helloworld' build in the 'youruser-console' project. The left sidebar shows various Kubernetes resources like Jobs, DaemonSets, ReplicaSets, etc. The main content area shows the build configuration details:

- Name:** php-helloworld
- Type:** Source
- Namespace:** youruser-console
- Labels:** app=php-helloworld, app.kubernetes.io/component=php-helloworld, app.kubernetes.io/instance=php-helloworld, app.kubernetes.io/name=php-helloworld, app.kubernetes.io/part-of=php-helloworld, app.openshift.io/runtime=php, app.openshift.io/runtime-version=74-ubi8
- Annotations:** 3 annotations
- Git repository:** https://github.com/yourgithubuser/DO180-apps
- Git ref:** console
- Context dir:** php-helloworld
- Build from:** IS php7.4-ubi8
- Output to:** IS php-helloworld:latest

Figure 6.26: Application build configuration details page

Explore the available information from the **Details** tab. The **YAML** tab allows you to view and edit the build configuration as a YAML file. The **Builds** tab provides an historical list of builds, along with a link to more information for each build.

The **Environment** tab allows you to view and edit environment variables for the application's build environment. The **Events** tab displays a list of build related events and metadata.

- 4.3. Examine the logs for the Source-to-Image build of the application. In the **Builds** menu, click **Builds** to display a list of recent builds for the *youruser-console* project.

Click the **php-helloworld-1** link to access information for the first build of the **php-helloworld** application:

The screenshot shows the 'Build details' page for the 'php-helloworld-1' build in the 'youruser-console' project. The left sidebar shows various Kubernetes resources like Deployments, DeploymentConfigs, StatefulSets, etc. The main content area shows the build details:

- Name:** php-helloworld-1
- Status:** Complete
- Namespace:** youruser-console
- Type:** Source
- Labels:** app=php-helloworld, app.kubernetes.io/part-of=php-helloworld
- Git repository:** https://github.com/yourgithubuser/DO180-apps

Figure 6.27: An application build details page

Explore the available information from the **Details** tab. Next, click the **Logs** tab. A scrollable text box contains output from the build process:

```

43 Copying blob sha256:7f1fd656af6e7b6af2b3523a01c717b13d94bd9dede6c1f0061ed9e70b22d65
44 Copying config sha256:98a358743a0541f78e13a5a14a9add4fd4acd3505ab5d057fc274581887212
45 Writing manifest to image destination
46 Storing signatures
47 --> 98a358743a0
48 Successfully tagged temp.builder.openshift.io/jmzzjv-console/php-helloworld-1:3454a6ca
98a358743a0541f78e13a5a14a9add4fd4acd3505ab5d057fc274581887212
49
50
51 Pushing image image-registry.openshift-image-registry.svc:5000/jmzzjv-console/php-helloworld:latest ...
52 Getting image source signatures
53 Copying blob sha256:7f1fd656af6e7b6af2b3523a01c717b13d94bd9dede6c1f0061ed9e70b22d65
54 Copying blob sha256:5dc0e60e6b60326f98eb49d6ebcb777df4b78c6297df2d7dede6692df6e
55 Copying blob sha256:79a56ba04a301eb949644bc29f18b1879b6f305091ef1eb8068a0f5828db863
56 Copying blob sha256:8671113e1c57d3106acaeff2383f9bfe1c45a2eacbf03ec82786a494e15956c3
57 Copying blob sha256:12bb8b1afe30f16fe8a264840ad3f250b82b335b9ebdc9a922db57b48836ce0c8c
58 Copying blob sha256:aad543859364662db264ad5752fd9449d47410b9ef0a0278463c09c578b79c6
59 Copying config sha256:98a358743a0541f78e13a5a14a9add4fd4acd3505ab5d057fc274581887212
60 Writing manifest to image destination
61 Storing signatures

```

**Figure 6.28: Logs for an application build**

When Podman builds a container image, similar output is observed compared with the output shown in the browser.

- Locate information for the **php-helloworld** application's service. In the navigation bar, click **Networking > Services** to display a list of services for the *youruser-console* project. Click the **php-helloworld** link to display the information associated with the application's service:

Name	php-helloworld
Namespace	youruser-console
Labels	app=php-helloworld app.kubernetes.io/component=php-helloworld app.kubernetes.io/instance=php-helloworld app.kubernetes.io/name=php-helloworld app.kubernetes.io/part-of=php-helloworld app.openshift.io/runtime=php app.openshift.io/runtime-version=7.4-ubi8
Service address	Type: Cluster IP Location: 172.30.215.25 Accessible within the cluster only
Service port mapping	Name Port Protocol Pod port or name

**Figure 6.29: Service details page**

Explore the available information from the **Details** tab. The **YAML** tab allows you to view and edit the service configuration, as a YAML file. The **Pods** tab displays the current list of pods that provide the application service.

- Locate external route information for the application. On the navigation bar, click **Networking > Routes** to display a list of configured routes for the *youruser-*

console project. Click the php-helloworld link to display information associated with the application's route:

Figure 6.30: Route details page

Explore the available information from the Details tab. The Location field provides a link to the external route for the application; `https://php-helloworld- ${RHT_OCP4_DEV_USER} -console.${RHT_OCP4_WILDCARD_DOMAIN}`. Click the link to access the application in a new tab:

Figure 6.31: Initial PHP application results

- ▶ 5. Modify the application code, commit the change, push the code to the remote Git repository, and trigger a new application build.

- 5.1. Enter the source code directory:

```
[student@workstation D0180-apps]$ cd ~/D0180-apps/php-helloworld
```

- 5.2. Add the second print line statement in the `index.php` page to read "A change is in the air!" and save the file. Add the change to the Git index, commit the change, and push the changes to the remote Git repository.

```
[student@workstation php-helloworld]$ vim index.php
[student@workstation php-helloworld]$ cat index.php
<?php
print "Hello, World! php version is " . PHP_VERSION . "\n";
print "A change is in the air!\n";
?>
[student@workstation php-helloworld]$ git add index.php
```

```
[student@workstation php-helloworld]$ git commit -m 'updated app'
[console d198fb5] updated app
...output omitted...
1 file changed, 1 insertion(+), 1 deletion(-)
[student@workstation php-helloworld]$ git push origin console
Counting objects: 7, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (3/3), done.
Writing objects: 100% (4/4), 409 bytes | 0 bytes/s, done.
Total 4 (delta 1), reused 0 (delta 0)
...output omitted...
```

5.3. Trigger an application build manually from the web console.

On the navigation bar, click **Builds** > **Build Configs** and then click the **php-helloworld** link to access the **Build Config Details** page. From the **Actions** menu in the upper right of the screen, click **Start Build**:

The screenshot shows the OpenShift web interface. On the left is a navigation sidebar with options like Home, Operators, Workloads, Networking, Services, Routes, and Ingresses. The main area shows a project named 'youruser-console'. Under 'BuildConfigs', there is a link to 'BuildConfig details' for 'BC php-helloworld'. Below this, there are tabs for Details, YAML, Builds, Environment, and Events. The 'Details' tab is selected. It shows the 'Name' as 'php-helloworld', 'Type' as 'Source', and 'Namespace' as 'NS youruser-console'. A 'Git repository' field contains the URL 'https://github.com/yourgithubuser/DO180-apps'. To the right of the main content is an 'Actions' dropdown menu with options: Start build (which is highlighted with a red box), Edit labels, Edit annotations, Edit BuildConfig, and Delete BuildConfig.

Figure 6.32: Start an application build

You are redirected to a Build Details page for the new build. Click the **Logs** tab to monitor progress of the build. The last line of a successful build contains **Push successful**.

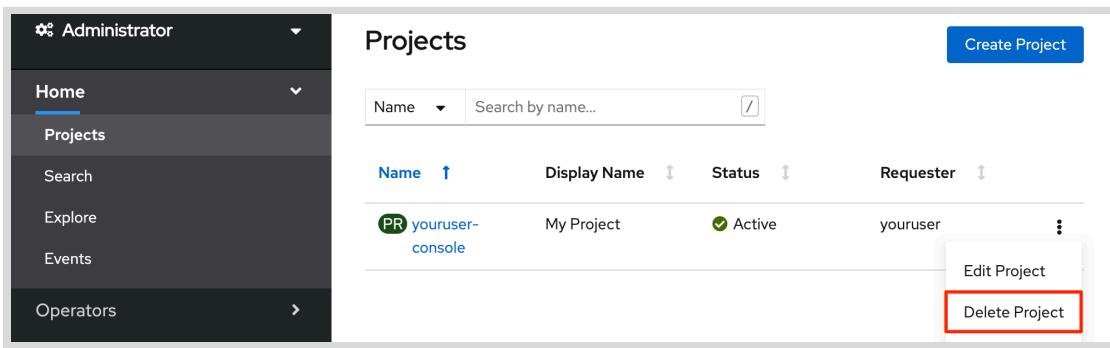
When the build completes, the deploy starts. Go to the **Workloads** > **Pods** section, and wait for the new pod is deployed and running.

5.4. Reload the `http://php-helloworld-${RHT_OCP4_DEV_USER}-console.${RHT_OCP4_WILDCARD_DOMAIN}` URL in the browser. The application response corresponds to the updated source code:

The screenshot shows a Mozilla Firefox browser window. The address bar shows the URL 'php-helloworld-console.apps.cluster.lab.example.com'. The main content area of the browser displays the text 'Hello, World! php version is 7.4.19 A change is in the air!'.

Figure 6.33: Updated web application output

- 6. Delete the project. On the navigation bar, click **Home** > **Projects**. Click the icon at the right side of the row containing an entry for the **youruser-console** project. Click **Delete Project** from the menu that appears.



The screenshot shows the OpenShift web console's 'Projects' page. On the left is a sidebar with 'Administrator' at the top, followed by 'Home' (which is underlined in blue), 'Projects', 'Search', 'Explore', 'Events', and 'Operators'. The main area is titled 'Projects' with a 'Create Project' button. Below is a search bar with 'Name' and 'Search by name...' placeholder. A table lists projects: 'PR youruser-console' (Display Name: 'My Project', Status: 'Active', Requester: 'youruser'). A context menu is open over the 'youruser-console' project, with options 'Edit Project' and 'Delete Project' visible. The 'Delete Project' option is highlighted with a red box.

**Figure 6.34: Delete a project**

Enter `youruser-console` in the confirmation dialog box, and click **Delete**.

## Finish

On `workstation`, run the following script to complete this lab.

```
[student@workstation php-helloworld]$ lab openshift-webconsole finish
```

This concludes the guided exercise.

## ► Lab

# Deploying Containerized Applications on OpenShift

### Outcomes

You should be able to create an OpenShift application and access it through a web browser.

### Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Open a terminal on `workstation` as the `student` user and run the following command:

```
[student@workstation ~]$ lab openshift-review start
```

### Instructions

1. Load the configuration of your classroom environment. Log in to OpenShift cluster and create a new project for this exercise. Name the project as  `${RHT_OCP4_DEV_USER} -ocp`.
2. Create a temperature converter application named `temps` written in PHP using the `php:7.3` image stream tag.  
The source code is in the Git repository at <https://github.com/RedHatTraining/DO180-apps/> in the `temps` directory. You may use the OpenShift command-line interface or the web console to create the application.
3. Verify that you can access the application URL in a web browser.
  - `http://temps- ${RHT_OCP4_DEV_USER} -ocp. ${RHT_OCP4_WILDCARD_DOMAIN}`

### Evaluation

On `workstation`, run the `lab openshift-review grade` command to grade your work. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab openshift-review grade
```

### Finish

On `workstation`, run the `lab openshift-review finish` command to complete this lab.

```
[student@workstation ~]$ lab openshift-review finish
```

This concludes the lab.

## ► Solution

# Deploying Containerized Applications on OpenShift

### Outcomes

You should be able to create an OpenShift application and access it through a web browser.

### Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Open a terminal on **workstation** as the student user and run the following command:

```
[student@workstation ~]$ lab openshift-review start
```

### Instructions

1. Load the configuration of your classroom environment. Log in to OpenShift cluster and create a new project for this exercise. Name the project as \${RHT\_OCP4\_DEV\_USER}-ocp.
  - 1.1. Load your classroom environment configuration.  
Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```

- 1.2. Log in to the OpenShift cluster.

```
[student@workstation ~]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
Login successful
...output omitted...
```

- 1.3. Create a new project named \${RHT\_OCP4\_DEV\_USER}-ocp for the resources you create during this exercise:

```
[student@workstation ~]$ oc new-project ${RHT_OCP4_DEV_USER}-ocp
```

2. Create a temperature converter application named temps written in PHP using the php:7.3 image stream tag.

The source code is in the Git repository at <https://github.com/RedHatTraining/D0180-apps/> in the temps directory. You may use the OpenShift command-line interface or the web console to create the application.

- 2.1. If using the command-line interface, run the following commands:

```
[student@workstation ~]$ oc new-app \
> php:7.3~https://github.com/RedHatTraining/D0180-apps \
> --context-dir temps --name temps
--> Found image 688c0bd (2 months old) in image stream "openshift/php" under tag
"7.3" for "php:7.3"

Apache 2.4 with PHP 7.3

PHP 7.3 available as container is a base platform ...output omitted...
...output omitted...

--> Creating resources ...
imagestream.image.openshift.io "temps" created
buildconfig.build.openshift.io "temps" created
deployment.apps "temps" created
service "temps" created
--> Success
Build scheduled, use "oc logs -f bc/temps" to track its progress.
Application is not exposed. You can expose services to the outside world by
executing one or more of the commands below:
"oc expose svc/temps"
Run 'oc status' to view your app.
```

2.2. Monitor progress of the build.

```
[student@workstation ~]$ oc logs -f bc/temps
Cloning "https://github.com/RedHatTraining/D0180-apps" ...
Commit: f7cd8963ef353d9173c3a21dccc402f3616840b (Initial commit, including all
apps previously in course)
...output omitted...
Successfully pushed image-registry.openshift-image-registry.svc:5000/
${RHT_OCP4_DEV_USER}-temps
Push successful
```

2.3. Verify that the application is deployed.

```
[student@workstation ~]$ oc get pods -w
NAME READY STATUS RESTARTS AGE
temps-1-build 0/1 Completed 0 91s
temps-57d678bbdd-dlz9c 1/1 Running 0 58s
```

Press Ctrl+C to exit the `oc get pods -w` command.

2.4. Expose the `temps` service to create an external route for the application.

```
[student@workstation ~]$ oc expose svc/temps
route.route.openshift.io/temps exposed
```

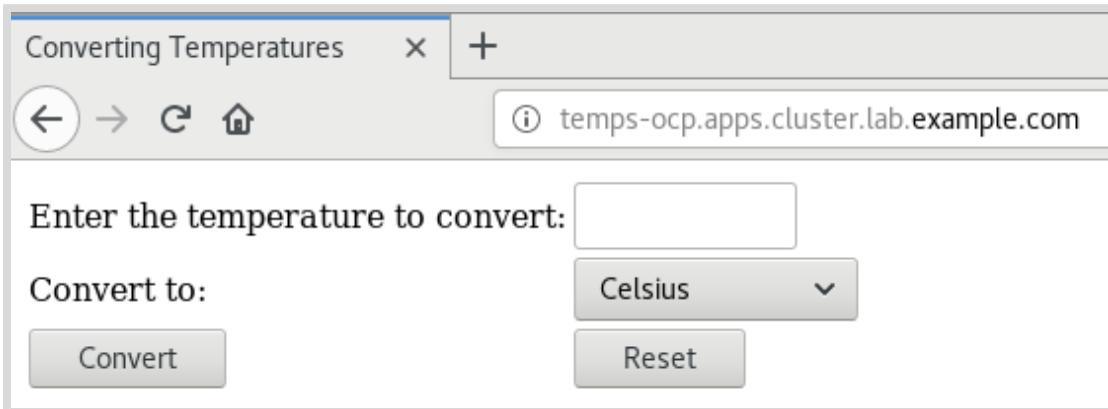
3. Verify that you can access the application URL in a web browser.

- `http://temps-${RHT_OCP4_DEV_USER}-ocp.${RHT_OCP4_WILDCARD_DOMAIN}`

- 3.1. Determine the URL for the route.

```
[student@workstation ~]$ oc get route/temps
NAME HOST/PORT
temps temps-${RHT_OCP4_DEV_USER}-ocp.${RHT_OCP4_WILDCARD_DOMAIN} ...
```

- 3.2. Verify that the temperature converter application works by opening a web browser and navigating to the URL displayed in the previous step.



## Evaluation

On workstation, run the `lab openshift-review grade` command to grade your work. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab openshift-review grade
```

## Finish

On workstation, run the `lab openshift-review finish` command to complete this lab.

```
[student@workstation ~]$ lab openshift-review finish
```

This concludes the lab.

# Summary

---

In this chapter, you learned:

- OpenShift Container Platform stores definitions of each OpenShift or Kubernetes resource instance as an object in the cluster's distributed database service, etcd. Common resource types are: Pod, Persistent Volume (PV), Persistent Volume Claim (PVC), Service (SVC), Route, Deployment, DeploymentConfig and Build Configuration (BC).
- Use the OpenShift command-line client oc to:
  - Create, change, and delete projects.
  - Create application resources inside a project.
  - Delete, inspect, edit, and export resources inside a project.
  - Check logs from application pods, deployments, and build operations.
- The oc new-app command can create application pods in many different ways: from an existing container image hosted on an image registry, from Containerfiles, and from source code using the Source-to-Image (S2I) process.
- Source-to-Image (S2I) is a tool that makes it easy to build a container image from application source code. This tool retrieves source code from a Git repository, injects the source code into a selected container image based on a specific language or technology, and produces a new container image that runs the assembled application.
- A Route connects a public-facing IP address and DNS host name to an internal-facing service IP. While services allow for network access between pods inside an OpenShift instance, routes allow for network access to pods from users and applications outside the OpenShift instance.
- You can create, build, deploy, and monitor applications using the OpenShift web console.

## Chapter 7

# Deploying Multi-Container Applications

### Goal

Deploy applications that are containerized using multiple container images.

### Objectives

- Describe considerations for containerizing applications with multiple container images.
- Deploy a multi-container application on OpenShift Platform.
- Deploy an Application on OpenShift using a template.

### Sections

- Considerations for Multi-Container Applications (and Guided Exercise)
- Deploying a Multi-Container Application on OpenShift (and Guided Exercise)
- Deploying a Multi-container Application on OpenShift Using a Template (and Guided Exercise)

### Lab

- Deploying Multi-Container Applications

# Considerations for Multi-Container Applications

## Objectives

After completing this section, students should be able to:

- Describe considerations for containerizing applications with multiple container images.
- Leverage networking concepts in containers.
- Create a multi-container application with Podman.
- Describe the architecture of the To Do List application.

## Leveraging Multi-Container Applications

The examples shown so far throughout this course have worked fine with a single container. A more complex application, however, can get the benefits of deploying different components into different containers. Consider an application composed of a front-end web application, a REST back end, and a database server. Those components may have different dependencies, requirements, and lifecycles.

Although it is possible to orchestrate multi-container applications' containers manually, Kubernetes and OpenShift provide tools to facilitate orchestration. Attempting to manually manage dozens or hundreds of containers quickly becomes complicated. In this section, we are going to return to using Podman to create a simple multi-container application to demonstrate the underlying manual steps for container orchestration. In later sections, you will use Kubernetes and OpenShift to orchestrate these same application containers.

## Discovering Services in a Multi-Container Application

### Rootfull containers

Podman uses Container Network Interface (CNI) to create a software-defined network (SDN) between all containers in the host. Unless stated otherwise, CNI assigns a new IP address to a container when it starts.

Each container exposes all ports to other containers in the same SDN. As such, services are readily accessible within the same network. The containers expose ports to external networks only by explicit configuration.

Due to the dynamic nature of container IP addresses, applications cannot rely on either fixed IP addresses or fixed DNS host names to communicate with middleware services and other application services. Containers with dynamic IP addresses can become a problem when working with multi-container applications because each container must be able to communicate with others to use services upon which it depends.

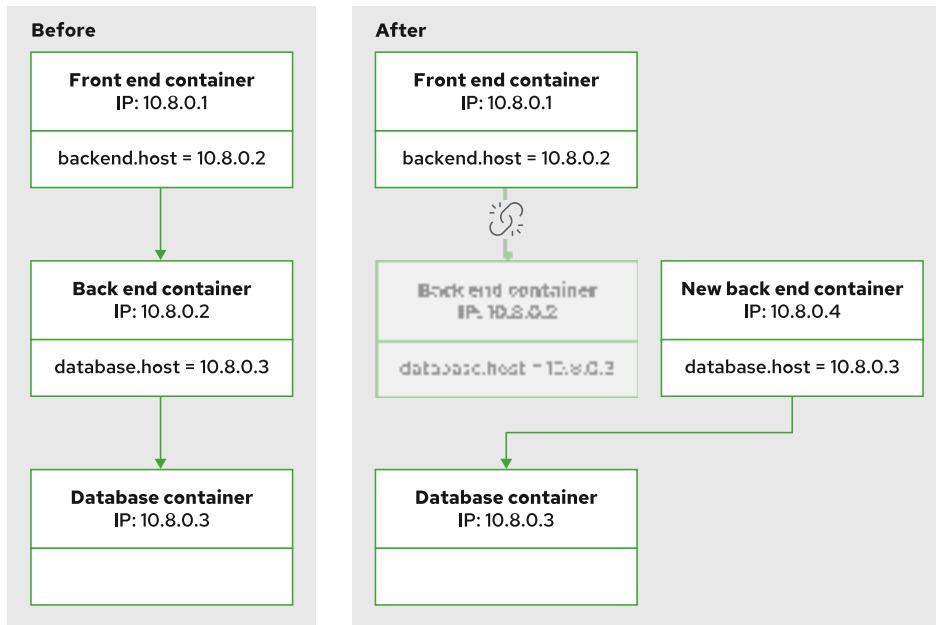


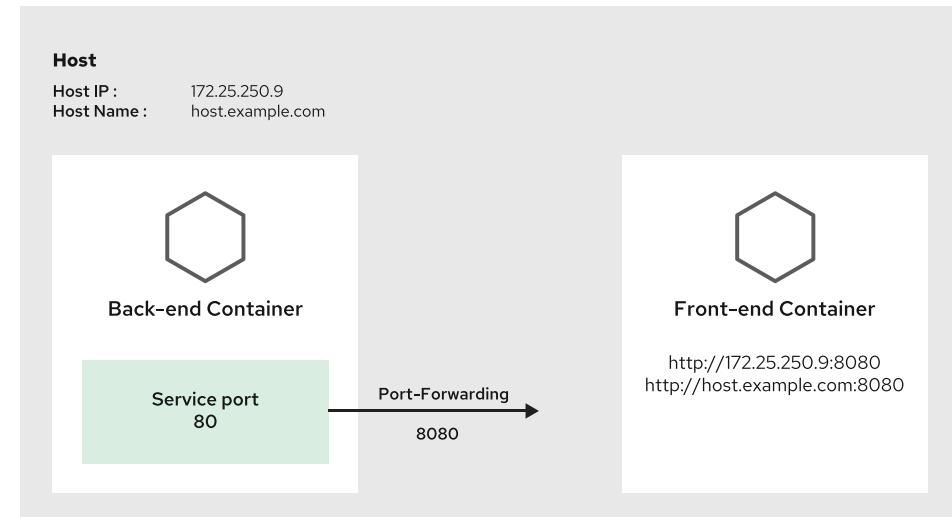
Figure 7.1: A restart breaks three-tiered application links

For example, consider an application composed of a front-end container, a back-end container, and a database. The front-end container needs to retrieve the IP address of the back-end container. Similarly, the back-end container needs to retrieve the IP address of the database container. Additionally, the IP address could change if a container restarts, so a process is needed to ensure any change in IP triggers an update to existing containers.

Both Kubernetes and OpenShift provide potential solutions to the issue of service discoverability and the dynamic nature of container networking. Some of these solutions are covered later in the chapter.

## Rootless containers

Rootless containers do not support software-defined network (SDN). Therefore, the container's IP address is not available to communicate with other containers on the host. We can achieve networking between rootless containers by using port-forwarding. Port-forwarding allows external access to a container service from the host. Port-forwarding has been discussed in *Chapter 3, Managing Containers*.

**Figure 7.2: Multi-Container Applications for rootless containers**

For example, consider an application that has both a front-end container and a back-end container. The back-end container has a service running on specific port 80. This service/port is not accessible from outside of the container. The front-end container needs to access the service/port from the back-end container. The first step is to use *port-forwarding* for the required service. In this example, we have forwarded service port 80 to 8080. Now the front-end container can access the service/port of the back-end container by using the host IP address and forwarded port.

## Describing the To Do List Application

Many labs from this course make use of a To Do List application. This application is divided into three tiers, as illustrated by the following figure:

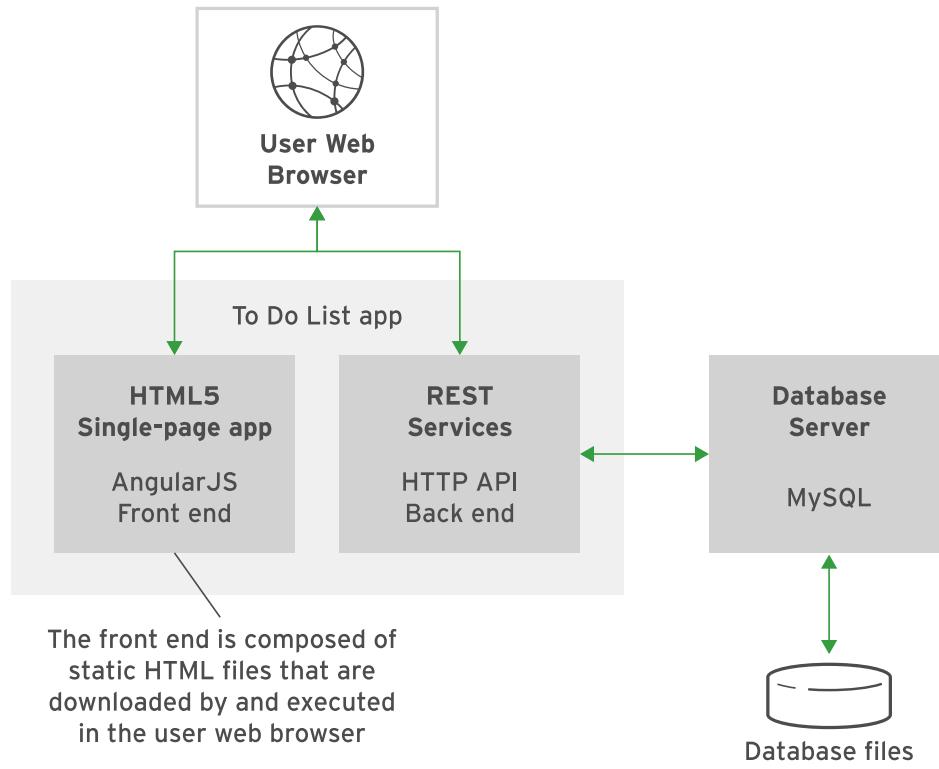


Figure 7.3: To Do List application logical architecture

- The presentation tier is built as a single-page HTML5 front-end using AngularJS.
- The business tier is composed by an HTTP API back-end, with Node.js.
- The persistence tier based on a MySQL database server.

The following figure is a screen capture of the application web interface:

ID	Description	Done	
1	Pick up new...	false	X
2	Buy groceries	true	X

Figure 7.4: The To Do List application

On the left is a table with items to complete, and on the right is a form to add a new item.

The classroom private registry server, `services.lab.example.com`, provides the application in two versions:

**nodejs**

Represents the way a typical developer would create the application as a single unit, without caring to break it into tiers or services.

**nodejs\_api**

Shows the changes needed to break the application into presentation and business tiers. Each tier corresponds to an isolated container image

The sources of both of these application versions are available from the `todoapp/nodejs` folder in the Git repository at: <https://github.com/RedHatTraining/DO180-apps.git>.

## ► Guided Exercise

# Deploying the Web Application and MySQL on Linux Containers

In this lab, you will create a script that runs and networks a Node.js application container and the MySQL container.

### Outcomes

You should be able to network containers to create a multi-tiered application.

### Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from Chapter 1 before executing any command of this practice.

You must have the To Do List application source code and lab files on workstation. To set up the environment for the exercise, run the following command:

```
[student@workstation ~]$ lab multicontainer-design start
```

## Instructions

- ▶ 1. Log in to the Red Hat Container Catalog with your Red Hat account. If you need to register to Red Hat, see the instructions in *Appendix D, Creating a Red Hat Account*.

```
[student@workstation ~]$ podman login registry.redhat.io
Username: your_username
Password: your_password
Login Succeeded!
```

- ▶ 2. Review the Containerfile.

Using your preferred editor, open and examine the completed Containerfile located at ~/D0180/labs/multicontainer-design/deploy/nodejs/Containerfile.

- ▶ 3. Run ip addr command to grep host IP address.

```
[student@workstation ~]$ ip -br addr list eth0
eth0 UP 172.25.250.9/24 fe80::d1cf:b1dc:ddc8:b79b/64
```

- ▶ 4. Explore the Environment Variables.

Inspect the environment variables that allow the Node.js REST API container to communicate with the MySQL container.

- 4.1. View the file ~/D0180/labs/multicontainer-design/deploy/nodejs/nodejs-source/models/db.js, containing the database configuration provided below:

```
module.exports.params = {
 dbname: process.env.MYSQL_DATABASE,
 username: process.env.MYSQL_USER,
 password: process.env.MYSQL_PASSWORD,
 params: {
 host: '172.25.250.9',
 port: '30306',
 dialect: 'mysql'
 }
};
```

- 4.2. Notice the environment variables used by the REST API. These variables are exposed to the container using -e options with the `podman run` command in this guided exercise. Those environment variables are described below.

#### **MYSQL\_DATABASE**

The name of the MySQL database in the `mysql` container.

#### **MYSQL\_USER**

The name of the database user used by the `todoapi` container to run MySQL commands.

#### **MYSQL\_PASSWORD**

The password of the database user that the `todoapi` container uses to authenticate to the `mysql` container.



#### **Note**

The host and port details of the MySQL container are embedded with the REST API application. The host, as shown above in the `db.js` file, is the IP address of host, which we have grep in previous step.

- 5. Build the To Do List application child image using the provided Containerfile.

- 5.1. Build the child image.

Examine the `~/DO180/labs/multicontainer-design/deploy/nodejs/build.sh` script to see how the image is built. Run the following commands to build the child image.

```
[student@workstation nodejs]$ cd ~/DO180/labs/multicontainer-design/deploy/nodejs
[student@workstation nodejs]$./build.sh
Preparing build folder
Preparing build folder
STEP 1: FROM registry.redhat.io/rhel8/nodejs-12
Getting image source signatures
Copying blob 666be21779ed done
...output omitted...
Writing manifest to image destination
Storing signatures
STEP 2: ARG NEXUS_BASE_URL
STEP 3: MAINTAINER username <username@example.com>
STEP 4: COPY run.sh build ${HOME}/
STEP 5: RUN npm install --registry=http://$NEXUS_BASE_URL/repository/nodejs/
```

```
...output omitted...
Writing manifest to image destination
Storing signatures
e4901...d37eb
```

**Note**

The `build.sh` script lowers restrictions for write access to the build directory, allowing non-root users to install dependencies.

Sometimes network instability causes an ERR! with the build script. To resolve this issue, re-run the build script.

- 5.2. Wait for the build to complete and then run the following command to verify that the image has been built successfully:

```
[student@workstation nodejs]$ podman images \
> --format "table {{.ID}} {{.Repository}} {{.Tag}}"
IMAGE ID REPOSITORY TAG
e4901b30413b localhost/do180/todonodejs latest
6b949cc5e908 registry.redhat.io/rhel8/nodejs-12 1
```

- ▶ 6. Modify the existing script to create containers with the appropriate ports, as defined in the previous step. In this script, the order of commands is given such that it starts the mysql container and then starts the todoapi container before connecting it to the mysql container. After invoking every container, there is a wait time of 9 seconds, so each container has time to start.
  - 6.1. Edit the `run.sh` file located at `~/D0180/labs/multicontainer-design/deploy/nodejs/networked` to insert the `podman run` command at the appropriate line for invoking mysql container. The following screen shows the exact `podman` command to insert into the file.

```
podman run -d --name mysql -e MYSQL_DATABASE=items -e MYSQL_USER=user1 \
-e MYSQL_PASSWORD=mypa55 -e MYSQL_ROOT_PASSWORD=r00tpa55 \
-v $PWD/work/data:/var/lib/mysql/data \
-p 30306:3306 \
registry.redhat.io/rhel8/mysql-80:1
```

In the previous command, the `MYSQL_DATABASE`, `MYSQL_USER`, and `MYSQL_PASSWORD` are populated with the credentials to access the MySQL database. These environment variables are required for the `mysql` container to run. Also, the `$PWD/work/data` local folder are mounted as volume into the container's file system.

- 6.2. In the same `run.sh` file, insert another `podman run` command at the appropriate line to run the `todoapi` container. The following screen shows the `podman` command to insert into the file.

```
podman run -d --name todoapi -e MYSQL_DATABASE=items -e MYSQL_USER=user1 \
-e MYSQL_PASSWORD=mypa55 \
-p 30080:30080 \
do180/todonodejs
```

**Note**

After each `podman run` command inserted into the `run.sh` script, ensure that there is also a `sleep 9` command. If you need to repeat this step, the `work` directory and its contents must be deleted before re-running the `run.sh` script.

- 6.3. Verify that your `run.sh` script matches the solution script located at `~/D0180/solutions/multicontainer-design/deploy/nodejs/networked/run.sh`.

- 6.4. Save the file and exit the editor.

▶ **7.** Run the containers.

- 7.1. Use the following command to execute the script that you updated to run the `mysql` and `todoapi` containers.

```
[student@workstation nodejs]$ cd \
> ~/D0180/labs/multicontainer-design/deploy/nodejs/networked
[student@workstation networked]$./run.sh
```

- 7.2. Verify that the containers started successfully.

```
[student@workstation networked]$ podman ps \
> --format="table {{.ID}} {{.Names}} {{.Image}} {{.Status}}"
ID Names Image Status
c74b4709e3ae todoapi localhost/do180/todonodejs:latest Up 3 minutes ago
3bc19f74254c mysql registry.redhat.io/rhel8/mysql-80:1 Up 3 minutes ago
```

▶ **8.** Populate the items database with the Projects table.

```
[student@workstation networked]$ mysql -uuser1 -h 172.25.250.9 \
> -pmypa55 -P30306 items < \
> ~/D0180/labs/multicontainer-design/deploy/nodejs/networked/db.sql
mysql: [Warning] Using a password on the command line interface can be insecure.
```

▶ **9.** Examine the environment variables of the API container.

Run the following command to explore the environment variables exposed in the API container.

```
[student@workstation networked]$ podman exec -it todoapi env
...output ommitted...
HOME=/opt/app-root/src
MYSQL_DATABASE=items
MYSQL_USER=user1
MYSQL_PASSWORD=mypa55
APP_ROOT=/opt/app-root
```

▶ **10.** Test the application.

- 10.1. Run a `curl` command to test the REST API for the To Do List application.

```
[student@workstation networked]$ curl -w "\n" \
> http://127.0.0.1:30080/todo/api/items/1
>{"id":1,"description":"Pick up newspaper","done":false}
```

The `-w "\n"` option with `curl` command lets the shell prompt appear at the next line rather than merging with the output in the same line.

- 10.2. Open Firefox on `workstation` and point your browser to `http://127.0.0.1:30080/todo/`. You should see the `To Do List` application.



### Note

Make sure to append the trailing slash (/).

- 10.3. Change to the `/home/student` directory.

```
[student@workstation networked]$ cd ~
[student@workstation ~]$
```

## Finish

On `workstation`, run the `lab multicontainer-design finish` script to complete this exercise.

```
[student@workstation ~]$ lab multicontainer-design finish
```

This concludes the guided exercise.

# Deploying a Multi-Container Application on OpenShift

---

## Objectives

After completing this section, students should be able to:

- Describe differences between Podman and Kubernetes
- Deploy a multicontainer application on OpenShift.

## Comparing Podman and Kubernetes

Using environment variables allows you to share information between containers with Podman. However, there are still some limitations and some manual work involved in ensuring that all environment variables stay in sync, especially when working with many containers. Kubernetes provides an approach to solve this problem by creating services for your containers, as covered in previous chapters.

## Services in Kubernetes

Pods are attached to a Kubernetes namespace, which OpenShift calls a *project*. When a pod starts, Kubernetes automatically adds a set of environment variables for each service defined on the same namespace.

Any service defined on Kubernetes generates environment variables for the IP address and port number where the service is available. Kubernetes automatically injects these environment variables into the containers from pods in the same namespace. These environment variables usually follow a convention:

### Uppercase

All environment variables are set using uppercase names.

### Snakecase

Any environment variable created by a service is usually composed of multiple words separated with an underscore (\_).

### Service name first

The first word for an environment variable created by a service is the service name.

### Protocol type

Most network environment variables include the protocol type (TCP or UDP).

These are the environment variables generated by Kubernetes for a service.

<SERVICE\_NAME>\_SERVICE\_HOST

Represents the IP address enabled by a service to access a pod.

<SERVICE\_NAME>\_SERVICE\_PORT

Represents the port where the server port is listed.

<SERVICE\_NAME>\_PORT

Represents the address, port, and protocol provided by the service for external access.

<SERVICE\_NAME>\_PORT\_<PORT\_NUMBER>\_<PROTOCOL>  
 Defines an alias for the <SERVICE\_NAME>\_PORT.

<SERVICE\_NAME>\_PORT\_<PORT\_NUMBER>\_<PROTOCOL>\_PROTO  
 Identifies the protocol type (TCP or UDP).

<SERVICE\_NAME>\_PORT\_<PORT\_NUMBER>\_<PROTOCOL>\_PORT  
 Defines an alias for <SERVICE\_NAME>\_SERVICE\_PORT.

<SERVICE\_NAME>\_PORT\_<PORT\_NUMBER>\_<PROTOCOL>\_ADDR  
 Defines an alias for <SERVICE\_NAME>\_SERVICE\_HOST.

For instance, given the following service:

```
apiVersion: v1
kind: Service
metadata:
 labels:
 name: mysql
 name: mysql
spec:
 ports:
 - protocol: TCP
 port: 3306
 selector:
 name: mysql
```

The following environment variables are available for each pod created after the service, on the same namespace:

```
MYSQL_SERVICE_HOST=10.0.0.11
MYSQL_SERVICE_PORT=3306
MYSQL_PORT=tcp://10.0.0.11:3306
MYSQL_PORT_3306_TCP=tcp://10.0.0.11:3306
MYSQL_PORT_3306_TCP_PROTO=tcp
MYSQL_PORT_3306_TCP_PORT=3306
MYSQL_PORT_3306_TCP_ADDR=10.0.0.11
```



### Note

Other relevant <SERVICE\_NAME>\_PORT\_\* environment variable names are set on the basis of the protocol. IP address and port number are set in the <SERVICE\_NAME>\_PORT environment variable.

For example, MYSQL\_PORT=tcp://10.0.0.11:3306 entry leads to the creation of environment variables with names such as MYSQL\_PORT\_3306\_TCP, MYSQL\_PORT\_3306\_TCP\_PROTO, MYSQL\_PORT\_3306\_TCP\_PORT, and MYSQL\_PORT\_3306\_TCP\_ADDR. If the protocol component of an environment variable is undefined, Kubernetes uses the TCP protocol and assigns the variable names accordingly.

## ► Guided Exercise

# Creating an Application on OpenShift

In this exercise, you will deploy the To Do List application in OpenShift Container Platform.

### Outcomes

You should be able to build and deploy an application in OpenShift Container Platform.

### Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

You must have the To Do List application source code and lab files on workstation. To download the lab files and verify the status of the OpenShift cluster, run the following command in a new terminal window.

```
[student@workstation ~]$ lab multicontainer-application start
```

### Instructions

- 1. Create the To Do List application from the provided YAML file.

- 1.1. Log in to OpenShift Container Platform.

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config

[student@workstation ~]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
Login successful.

...output omitted...

Using project "default".
```



#### Note

If the `oc login` command prompts about using insecure connections, answer `y` (yes).

- 1.2. Create a new project *application* in OpenShift to use for this exercise. Run the following command to create the application project.

```
[student@workstation ~]$ oc new-project ${RHT_OCP4_DEV_USER}-application
Now using project ...output omitted...
```

- 1.3. Review the YAML file.

**Chapter 7 |** Deploying Multi-Container Applications

Using your preferred editor, open and examine the app file located at `~/DO180/labs/multicontainer-application/todo-app.yml`. Notice the following resources defined in the `todo-app.yml` and review their configurations.

- The `todoapi` pod definition defines the Node.js application.
- The `mysql` pod definition defines the MySQL database.
- The `todoapi` service provides connectivity to the Node.js application pod.
- The `mysql` service provides connectivity to the MySQL database pod.
- The `dbclaim` persistent volume claim definition defines the MySQL `/var/lib/mysql/data` volume.

1.4. Create application resources with given yaml file.

Use the `oc create` command to create the application resources. Run the following command in the terminal window:

```
[student@workstation ~]$ cd ~/DO180/labs/multicontainer-application
[student@workstation multicontainer-application]$ oc create -f todo-app.yml
pod/mysql created
pod/todoapi created
service/todoapi created
service/mysql created
persistentvolumeclaim/dbclaim created
```

1.5. Review the status of the deployment using the `oc get pods` command with the `-w` option to continue to monitor the pod status. Wait until both the containers are running. It may take some time for both pods to start.

```
[student@workstation multicontainer-application]$ oc get pods -w
NAME READY STATUS RESTARTS AGE
todoapi 1/1 Running 0 27s
mysql 1/1 Running 0 27s
```

Press `Ctrl+C` to exit the command.

► 2. Connect to the MySQL database server and populate the data to the `item` database.

2.1. From the workstation machine, configure port forwarding between workstation and the database pod running on OpenShift using port 3306. The terminal will hang after executing the command.

```
[student@workstation multicontainer-application]$ oc port-forward mysql 3306:3306
Forwarding from 127.0.0.1:3306 -> 3306
Forwarding from [::1]:3306 -> 3306
```

2.2. From the workstation machine open another terminal and populate the data to the MySQL server using the MySQL client.

```
[student@workstation ~]$ cd ~/DO180/labs/multicontainer-application
[student@workstation multicontainer-application]$ mysql -uuser1 \
> -h 127.0.0.1 -pmypa55 -P3306 items < db.sql
mysql: [Warning] Using a password on the command line interface can be insecure.
```

- 2.3. Close the terminal and return to the previous one. Finish the port forwarding process by pressing **Ctrl+C**.

```
Forwarding from 127.0.0.1:3306 -> 3306
Forwarding from [::1]:3306 -> 3306
Handling connection for 3306
^C
```

► 3. Expose the Service.

To allow the To Do List application to be accessible through the OpenShift router and to be available as a public FQDN, use the `oc expose` command to expose the `todoapi` service.

Run the following command in the terminal window.

```
[student@workstation multicontainer-application]$ oc expose service todoapi
route.route.openshift.io/todoapi exposed
```

► 4. Test the application.

- 4.1. Find the FQDN of the application by running the `oc status` command and note the FQDN for the app.

Run the following command in the terminal window.

```
[student@workstation multicontainer-application]$ oc status | grep -o "http:.*com"
http://todoapi-${RHT_OCP4_DEV_USER}-application.${RHT_OCP4_WILDCARD_DOMAIN}
```

- 4.2. Use `curl` to test the REST API for the To Do List application.

```
[student@workstation multicontainer-application]$ curl -w "\n" \
> $(oc status | grep -o "http:.*com")/todo/api/items/1
{"id":1,"description":"Pick up newspaper","done":false}
```



**Note**

The `-w "\n"` option with `curl` command lets the shell prompt appear at the next line rather than merging with the output in the same line.

- 4.3. Change to the `/home/student` directory.

```
[student@workstation multicontainer-application]$ cd ~
[student@workstation ~]$
```

- 4.4. Open Firefox on workstation and point your browser to the To Do List application URL.

- `http://todoapi-${RHT_OCP4_DEV_USER}-application.${RHT_OCP4_WILDCARD_DOMAIN}/todo/`

**Important**

The trailing slash in the URL mentioned above is necessary. If you do not include that in the URL, you may encounter issues with the application.

Id	Description	Done	
1	Pick up new...	false	X
2	Buy groceries	true	X

First Previous 1 Next Last

Add Task

Description:  Add Description.

Completed:

Clear Save

Figure 7.5: To Do List application

## Finish

On workstation, run the `lab multicontainer-application finish` script to complete this lab.

```
[student@workstation ~]$ lab multicontainer-application finish
```

This concludes the guided exercise.

# Deploying a Multi-container Application on OpenShift Using a Template

---

## Objectives

After completing this section, students should be able to deploy a multi-container application on OpenShift using a template.

## Examining the Skeleton of a Template

Deploying an application on OpenShift Container Platform often requires creating several related resources within a Project. For example, a web application may require a `BuildConfig`, `Deployment`, `Service`, and `Route` resource to run in an OpenShift project. Often the attributes of these resources have the same value, such as a resource's name attribute.

OpenShift templates provide a way to simplify the creation of resources that an application requires. A template defines a set of related resources to be created together, as well as a set of application parameters. The attributes of template resources are typically defined in terms of the template parameters, such as a resource's name attribute.

For example, an application might consist of a front-end web application and a database server. Each consists of a service resource and a deployment resource. They share a set of credentials (parameters) for the front end to authenticate to the back end. The template can be processed by specifying parameters or by allowing them to be automatically generated (for example, for a unique database password) in order to instantiate the list of resources in the template as a cohesive application.

The OpenShift installer creates several templates by default in the `openshift` namespace. Run the `oc get templates` command with the `-n openshift` option to list these preinstalled templates:

```
[user@host ~]$ oc get templates -n openshift
NAME DESCRIPTION
cakephp-mysql-example An example CakePHP application ...
cakephp-mysql-persistent An example CakePHP application ...
dancer-mysql-example An example Dancer application with a MySQL ...
dancer-mysql-persistent An example Dancer application with a MySQL ...
django-psql-example An example Django application with a PostgreSQL ...
...output omitted...
rails-psql-persistent An example Rails application with a PostgreSQL ...
rails-postgresql-example An example Rails application with a PostgreSQL ...
redis-ephemeral Redis in-memory data structure store, ...
redis-persistent Redis in-memory data structure store, ...
```

The YAML definition of a template can be modified to suit the needs of your applications. You will do this in an upcoming lab.

The following shows a YAML template definition:

```
[user@host ~]$ oc get template mysql-persistent -n openshift -o yaml
apiVersion: template.openshift.io/v1
kind: Template
labels: ...value omitted...
message: ...message omitted ...
metadata:
 annotations:
 description: ...description omitted...
 iconClass: icon-mysql-database
 openshift.io/display-name: MySQL
 openshift.io/documentation-url: ...value omitted...
 openshift.io/long-description: ...value omitted...
 openshift.io/provider-display-name: Red Hat, Inc.
 openshift.io/support-url: https://access.redhat.com
 tags: database,mysql ①
 labels: ...value omitted...
 name: mysql-persistent ②
objects: ③
- apiVersion: v1
 kind: Secret
 metadata:
 annotations: ...annotations omitted...
 name: ${DATABASE_SERVICE_NAME} ④
 stringData: ...stringData omitted...
- apiVersion: v1
 kind: Service
 metadata:
 annotations: ...annotations omitted...
 name: ${DATABASE_SERVICE_NAME}
 spec: ...spec omitted...
- apiVersion: v1
 kind: PersistentVolumeClaim
 metadata:
 name: ${DATABASE_SERVICE_NAME}
 spec: ...spec omitted...
- apiVersion: v1
 kind: Deployment
 metadata:
 annotations: ...output omitted...
 name: ${DATABASE_SERVICE_NAME}
 spec: ...output omitted...
parameters: ⑤
- ...MEMORY_LIMIT parameter omitted...
- ...NAMESPACE parameter omitted...
- description: The name of the OpenShift Service exposed for the database.
 displayName: Database Service Name
 name: DATABASE_SERVICE_NAME ⑥
 required: true
 value: mysql
- ...MYSQL_USER parameter omitted...
- description: Password for the MySQL connection user.
 displayName: MySQL Connection Password
 from: '[a-zA-Z0-9]{16}' ⑦
 generate: expression
```

```
name: MYSQL_PASSWORD
required: true
- ...MYSQL_ROOT_PASSWORD parameter omitted...
- ...MYSQL_DATABASE parameter omitted...
- ...VOLUME_CAPACITY parameter omitted...
- ...MYSQL_VERSION parameter omitted...
```

- ➊ Defines a list of arbitrary tags to associate with this template. Enter any of these tags in the UI to find this template.
- ➋ Defines the template name.
- ➌ The **objects** section defines the list of OpenShift resources for this template. This template creates four resources: a **Secret**, a **Service**, a **PersistentVolumeClaim**, and a **Deployment**.
- ➍ All four resource objects have their names set to the value of the **DATABASE\_SERVICE\_NAME** parameter.
- ➎ The **parameters** section contains a list of nine parameters.
- ➏ Template resources often define their attributes using the values of these parameters, as demonstrated with the **DATABASE\_SERVICE\_NAME** parameter.
- ➐ If you do not specify a value for the **MYSQL\_PASSWORD** parameter when you create an application with this template, OpenShift generates a password that matches this regular expression.

You can publish a new template to the OpenShift cluster so that other developers can build an application from the template.

Assume you have an task list application named `todo` that requires an OpenShift **Deployment**, **Service**, and **Route** object for deployment. You create a YAML template definition file that defines attributes for these OpenShift resources, along with definitions for any required parameters. Assuming the template is defined in the `todo-template.yaml` file, use the `oc create` command to publish the application template:

```
[user@host deploy-multicontainer]$ oc create -f todo-template.yaml
template.template.openshift.io/todonodejs-persistent created
```

By default, the template is created under the current project unless you specify a different one using the `-n` option, as shown in the following example:

```
[user@host deploy-multicontainer]$ oc create -f todo-template.yaml \
> -n openshift
```



### Important

Any template created under the `openshift` namespace (OpenShift project) is available in the web console under the **Developer Catalog** of the **Developer** perspective. Moreover, any template created under the current project is accessible from that project.

## Parameters

Templates define a set of parameters, which are assigned values. OpenShift resources defined in the template can get their configuration values by referencing *named parameters*. Parameters in a template can have default values, but they are optional. Any default value can be replaced when processing the template.

Each parameter value can be set either explicitly by using the `oc process` command, or generated by OpenShift according to the parameter configuration.

There are two ways to list available parameters from a template. The first one is using the `oc describe` command:

```
[user@host ~]$ oc describe template mysql-persistent -n openshift
Name: mysql-persistent
Namespace: openshift
Created: 12 days ago
Labels: samplesoperator.config.openshift.io/managed=true
Description: MySQL database service, with ...description omitted...
Annotations: iconClass=icon-mysql-database
 openshift.io/display-name=MySQL
 ...output omitted...
tags=database,mysql

Parameters:
 Name: MEMORY_LIMIT
 Display Name: Memory Limit
 Description: Maximum amount of memory the container can use.
 Required: true
 Value: 512Mi

 Name: NAMESPACE
 Display Name: Namespace
 Description: The OpenShift Namespace where the ImageStream resides.
 Required: false
 Value: openshift

 ...output omitted...

 Name: MYSQL_VERSION
 Display Name: Version of MySQL Image
 Description: Version of MySQL image to be used (8.0, or latest).
 Required: true
 Value: 8.0

Object Labels: template=mysql-persistent-template

Message: ...output omitted... in your project: ${DATABASE_SERVICE_NAME}.

 Username: ${MYSQL_USER}
 Password: ${MYSQL_PASSWORD}
 Database Name: ${MYSQL_DATABASE}
 Connection URL: mysql://${DATABASE_SERVICE_NAME}:3306/
```

```
For more information about using this template, ...output omitted...
```

Objects:

```
Secret ${DATABASE_SERVICE_NAME}
Service ${DATABASE_SERVICE_NAME}
PersistentVolumeClaim ${DATABASE_SERVICE_NAME}
Deployment ${DATABASE_SERVICE_NAME}
```

The second way is by using the `oc process` with the `--parameters` option:

```
[user@host ~]$ oc process --parameters mysql-persistent -n openshift
NAME DESCRIPTION GENERATOR VALUE
MEMORY_LIMIT Maximum a... expression 512Mi
NAMESPACE The OpenS... expression openshift
DATABASE_SERVICE_NAME The name ... expression mysql
MYSQL_USER Username ... expression user[A-Z0-9]{3}
MYSQL_PASSWORD Password ... expression [a-zA-Z0-9]{16}
MYSQL_ROOT_PASSWORD Password ... expression [a-zA-Z0-9]{16}
MYSQL_DATABASE Name of t... expression sampledb
VOLUME_CAPACITY Volume sp... expression 1Gi
MYSQL_VERSION Version o... expression 8.0
```

## Processing a Template Using the CLI

When you process a template, you generate a list of resources to create a new application. To process a template, use the `oc process` command:

```
[user@host ~]$ oc process -f <filename>
```

The previous command processes a template file, in either JSON or YAML format, and returns the list of resources to standard output. The format of the output resource list is JSON. To output the resource list in YAML format, use the `-o yaml` with the `oc process` command:

```
[user@host ~]$ oc process -o yaml -f <filename>
```

Another option is to process a template from the current project or the `openshift` project:

```
[user@host ~]$ oc process <uploaded-template-name>
```



### Note

The `oc process` command returns a list of resources to standard output. This output can be redirected to a file:

```
[user@host ~]$ oc process -o yaml -f filename > myapp.yaml
```

Templates often generate resources with configurable attributes that are based on the template parameters. To override a parameter, use the `-p` option followed by a `<name>=<value>` pair.

```
[user@host ~]$ oc process -o yaml -f mysql.yaml \
> -p MYSQL_USER=dev -p MYSQL_PASSWORD=$P4SSD -p MYSQL_DATABASE=bank \
> -p VOLUME_CAPACITY=10Gi > mysqlProcessed.yaml
```

To create the application, use the generated YAML resource definition file:

```
[user@host ~]$ oc create -f mysqlProcessed.yaml
```

Alternatively, it is possible to process the template and create the application without saving a resource definition file by using a UNIX pipe:

```
[user@host ~]$ oc process -f mysql.yaml -p MYSQL_USER=dev \
> -p MYSQL_PASSWORD=$P4SSD -p MYSQL_DATABASE=bank \
> -p VOLUME_CAPACITY=10Gi | oc create -f -
```

To use a template in the openshift project to create an application in your project, first export the template:

```
[user@host ~]$ oc get template mysql-persistent -o yaml \
> -n openshift > mysql-persistent-template.yaml
```

Next, identify appropriate values for the template parameters and process the template:

```
[user@host ~]$ oc process -f mysql-persistent-template.yaml \
> -p MYSQL_USER=dev -p MYSQL_PASSWORD=$P4SSD -p MYSQL_DATABASE=bank \
> -p VOLUME_CAPACITY=10Gi | oc create -f -
```

You can also use two slashes (//) to provide the namespace as part of the template name:

```
[user@host ~]$ oc process openshift//mysql-persistent \
> -p MYSQL_USER=dev -p MYSQL_PASSWORD=$P4SSD -p MYSQL_DATABASE=bank \
> -p VOLUME_CAPACITY=10Gi | oc create -f -
```

Alternatively, it is possible to create an application using the `oc new-app` command passing the template name as the `--template` option argument:

```
[user@host ~]$ oc new-app --template=mysql-persistent \
> -p MYSQL_USER=dev -p MYSQL_PASSWORD=$P4SSD -p MYSQL_DATABASE=bank \
> -p VOLUME_CAPACITY=10Gi
```



## References

Developer information about templates can be found in the *Using Templates* section of the OpenShift Container Platform documentation:

### Developer Guide

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.10/html-single/images/index#using-templates](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.10/html-single/images/index#using-templates)

## ► Guided Exercise

# Creating an Application with a Template

In this exercise, you will deploy the `To Do List` application in OpenShift Container Platform using a template to define resources your application needs to run.

## Outcomes

You should be able to build and deploy an application in OpenShift Container Platform using a provided JSON template.

## Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

You must have the `To Do List` application source code and lab files on `workstation`. To download the lab files and verify the status of the OpenShift cluster, run the following command in a new terminal window.

```
[student@workstation ~]$ lab multicontainer-openshift start
```

## Instructions

- ▶ 1. Create the `To Do List` application from the provided JSON template.
  - 1.1. Load your classroom environment configuration. Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```
  - 1.2. Log in to OpenShift Container Platform. If the `oc login` command prompts about using insecure connections, answer `y` (yes).

```
[student@workstation ~]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
Login successful.

...output omitted...

Using project "default".
```

- 1.3. Create a new project *template* in OpenShift to use for this exercise. Run the following command to create the `template` project.

```
[student@workstation ~]$ oc new-project ${RHT_OCP4_DEV_USER}-template
Now using project ...output omitted...
```

1.4. Review the template.

Using your preferred editor, open and examine the template located at `~/D0180/labs/multicontainer-openshift/todo-template.json`. Notice the following resources defined in the template and review their configurations.

- The `todoapi` pod definition defines the Node.js application.
- The `mysql` pod definition defines the MySQL database.
- The `todoapi` service provides connectivity to the Node.js application pod.
- The `mysql` service provides connectivity to the MySQL database pod.
- The `dbclaim` persistent volume claim definition defines the MySQL `/var/lib/mysql/data` volume.

1.5. Process the template and create the application resources.

Use the `oc process` command to process the template file. This template requires the Quay.io namespace to retrieve the container images. Use the pipe command to send the result to the `oc create` command.

Run the following command in the terminal window:

```
[student@workstation ~]$ cd ~/D0180/labs/multicontainer-openshift
[student@workstation multicontainer-openshift]$ oc process \
> -f todo-template.json | oc create -f -
pod/mysql created
pod/todoapi created
service/todoapi created
service/mysql created
persistentvolumeclaim/dbclaim created
```

1.6. Review the status of the deployment using the `oc get pods` command with the `-w` option to continue to monitor the pod status. Wait until both the containers are running. It may take some time for both pods to start.

```
[student@workstation multicontainer-openshift]$ oc get pods -w
NAME READY STATUS RESTARTS AGE
todoapi 1/1 Running 0 27s
mysql 1/1 Running 0 27s
```

Press `Ctrl+C` to exit the command.

► 2. Connect to the MySQL database server and populate the data to the `item` database.

2.1. From the workstation machine, configure port forwarding between workstation and the database pod running on OpenShift using port 3306. The terminal will hang after executing the command.

```
[student@workstation multicontainer-openshift]$ oc port-forward mysql 3306:3306
Forwarding from 127.0.0.1:3306 -> 3306
Forwarding from [::1]:3306 -> 3306
```

2.2. From the workstation machine open another terminal and populate the data to the MySQL server using the MySQL client.

```
[student@workstation ~]$ cd ~/DO180/labs/multicontainer-openshift
[student@workstation multicontainer-openshift]$ mysql -uuser1 \
> -h 127.0.0.1 -pmypa55 -P3306 items < db.sql
mysql: [Warning] Using a password on the command line interface can be insecure.
```

- 2.3. Close the terminal and return to the previous one. Finish the port forwarding process by pressing **Ctrl+C**.

```
Forwarding from 127.0.0.1:3306 -> 3306
Forwarding from [::1]:3306 -> 3306
Handling connection for 3306
^C
```

► 3. Expose the Service.

To allow the `To Do List` application to be accessible through the OpenShift router and to be available as a public FQDN, use the `oc expose` command to expose the `todoapi` service.

Run the following command in the terminal window.

```
[student@workstation multicontainer-openshift]$ oc expose service todoapi
route.route.openshift.io/todoapi exposed
```

► 4. Test the application.

- 4.1. Find the FQDN of the application by running the `oc status` command and note the FQDN for the app.

Run the following command in the terminal window.

```
[student@workstation multicontainer-openshift]$ oc status | grep -o "http:.*com"
http://todoapi-${{RHT_OCP4_DEV_USER}}-template.${{RHT_OCP4_WILDCARD_DOMAIN}}
```

- 4.2. Use `curl` to test the REST API for the `To Do List` application.

```
[student@workstation multicontainer-openshift]$ curl -w "\n" \
> $(oc status | grep -o "http:.*com")/todo/api/items/1
{"id":1,"description":"Pick up newspaper","done":false}
```



**Note**

The `-w "\n"` option with `curl` command lets the shell prompt appear at the next line rather than merging with the output in the same line.

- 4.3. Change to the `/home/student` directory.

```
[student@workstation multicontainer-openshift]$ cd ~
[student@workstation ~]$
```

- 4.4. Open Firefox on `workstation` and point your browser to the application URL and you should see the `To Do List` application.

- `http://todoapi-$\{RHT_OCP4_DEV_USER\}-template.\$\{RHT_OCP4_WILDCARD_DOMAIN\}/todo/`

**Important**

The trailing slash in the URL mentioned above is necessary. If you do not include that in the URL, you may encounter issues with the application.

## To Do List Application

### To Do List

Id	Description	Done	
1	Pick up new...	false	X
2	Buy groceries	true	X

FirstPrevious1NextLast

### Add Task

Description:

Add Description.

Completed:

Clear Save

Figure 7.6: To Do List application

## Finish

On `workstation`, run the following script to complete this lab.

```
[student@workstation ~]$ lab multicontainer-openshift finish
```

This concludes the guided exercise.

## ▶ Lab

# Deploying Multi-Container Applications

### Outcomes

You should be able to create an OpenShift application comprised of multiple containers and access it through a web browser.

### Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Open a terminal on `workstation` as the `student` user and run the following commands:

```
[student@workstation ~]$ lab multicontainer-review start
[student@workstation ~]$ cd ~/D0180/labs/multicontainer-review
```

### Instructions

1. Log in to OpenShift cluster and create a new project for this exercise. Name the project as  `${RHT_OCP4_DEV_USER} -deploy`.
2. Build the Database container image located in the `images/mysql` directory, tag it with `do180-mysql-80-rhel8` and publish it to your `quay.io` repository.
3. Build the PHP container image located in the `images/quote-php`, tag it with `do180-quote-php` and publish it to your `quay.io` repository.



#### Warning

Make sure both repositories are public in `quay.io` so OpenShift can get the images from it. Refer to the **Repositories Visibility** section of the *Quay appendix* to read details about how change repository visibility.

4. Go to the `~/D0180/labs/multicontainer-review` directory and review the provided template `quote-php-template.json` file.
5. Upload the PHP application template so that any developer with access to your project can use it.
6. Process the uploaded template, create the application resources and verify their status.
7. Expose the service `quote-php`.  
Allow the `PHP Quote` application to be accessible through the OpenShift router and reachable from an external network.
8. Test the application with `curl` and verify that it outputs an inspiring message.

### Evaluation

Grade your work by running the `lab multicontainer-review grade` command from your `workstation` machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab multicontainer-review grade
```

## Finish

To complete this lab, run the `lab multicontainer-review finish` command on `workstation`.

```
[student@workstation ~]$ lab multicontainer-review finish
```

This concludes the lab.

## ► Solution

# Deploying Multi-Container Applications

### Outcomes

You should be able to create an OpenShift application comprised of multiple containers and access it through a web browser.

### Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Open a terminal on **workstation** as the **student** user and run the following commands:

```
[student@workstation ~]$ lab multicontainer-review start
[student@workstation ~]$ cd ~/DO180/labs/multicontainer-review
```

### Instructions

1. Log in to OpenShift cluster and create a new project for this exercise. Name the project as  `${RHT_OCP4_DEV_USER}-deploy`.
  - 1.1. From the **workstation** machine, log in as the user provided at the first exercise.

```
[student@workstation multicontainer-review]$ source /usr/local/etc/ocp4.config
[student@workstation multicontainer-review]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
Login successful.
```

You don't have any projects.  
You can try to create a new project, by running

```
oc new-project <projectname>
```



#### Note

If the `oc login` command prompts about using insecure connections, answer **y** (yes).

- 1.2. Create a new project in OpenShift named `deploy` and prefixed by your OpenShift username:

```
[student@workstation multicontainer-review]$ oc new-project \
> ${RHT_OCP4_DEV_USER}-deploy
Now using project ...output omitted...
```

2. Build the Database container image located in the `images/mysql` directory, tag it with `do180-mysql-80-rhel8` and publish it to your `quay.io` repository.

2.1. Log in to the Red Hat Container Catalog with your Red Hat account.

```
[student@workstation ~]$ podman login registry.redhat.io
Username: your-username
Password: your-password
Login Succeeded!
```

- 2.2. Build the MySQL Database image using the provided `Containerfile` in the `images/mysql` directory.

```
[student@workstation multicontainer-review]$ cd images/mysql

[student@workstation mysql]$ podman build -t do180-mysql-80-rhel8 .
STEP 1: FROM registry.redhat.io/rhel8/mysql-80:1
...output omitted...
STEP 4: COMMIT do180-mysql-80-rhel8
397a...5cfb
```

- 2.3. Push the MySQL image to the your Quay.io repository.

In order to make the image available for OpenShift to use in the template, give it the tag `quay.io/${RHT_OCP4_QUAY_USER}/do180-mysql-80-rhel8` and push it to the `quay.io` registry. In order to push images to `quay.io` you first need to log in with your own credentials.

```
[student@workstation mysql]$ podman login quay.io -u ${RHT_OCP4_QUAY_USER}
Password: your-quay-password
Login Succeeded!
```

To tag and push the image run the following commands in the terminal window.

```
[student@workstation mysql]$ podman tag do180-mysql-80-rhel8 \
> quay.io/${RHT_OCP4_QUAY_USER}/do180-mysql-80-rhel8

[student@workstation mysql]$ podman push \
> quay.io/${RHT_OCP4_QUAY_USER}/do180-mysql-80-rhel8
Getting image source signatures
...output omitted...
Writing manifest to image destination
Storing signatures
```

Return to the previous directory.

```
[student@workstation mysql]$ cd ~/D0180/labs/multicontainer-review
```

3. Build the PHP container image located in the `images/quote-php`, tag it with `do180-quote-php` and publish it to your `quay.io` repository.

**Warning**

Make sure both repositories are public in quay.io so OpenShift can get the images from it. Refer to the **Repositories Visibility** section of the Quay appendix to read details about how change repository visibility.

- 3.1. Build the PHP image using the provided Containerfile in the images/quote-php directory.

```
[student@workstation multicontainer-review]$ cd images/quote-php

[student@workstation quote-php]$ podman build -t do180-quote-php .
STEP 1: FROM registry.access.redhat.com/ubi8/ubi
...output omitted...
STEP 8: COMMIT do180-quote-php
271f...525d
```

- 3.2. Tag and push the PHP image to your Quay.io registry.

In order to make the image available for OpenShift to use in the template, give it the tag of quay.io/\${RHT\_OCP4\_QUAY\_USER}/do180-quote-php and push it to Quay.io.

```
[student@workstation quote-php]$ podman tag do180-quote-php \
> quay.io/${RHT_OCP4_QUAY_USER}/do180-quote-php

[student@workstation quote-php]$ podman push \
> quay.io/${RHT_OCP4_QUAY_USER}/do180-quote-php
Getting image source signatures
...output omitted...
Writing manifest to image destination
Storing signatures
```

4. Go to the ~/D0180/labs/multicontainer-review directory and review the provided template quote-php-template.json file.

- 4.1. Note the definitions and configuration of the pods, services, and persistent volume claims defined in the template.

```
[student@workstation quote-php]$ cd ~/D0180/labs/multicontainer-review
```

5. Upload the PHP application template so that any developer with access to your project can use it.

- 5.1. Use the oc create -f command to upload the template file to the project.

```
[student@workstation multicontainer-review]$ oc create -f quote-php-template.json
template.template.openshift.io/quote-php-persistent created
```

6. Process the uploaded template, create the application resources and verify their status.

- 6.1. Use the oc process command to process the template file. Make sure providing the RHT\_OCP4\_QUAY\_USER parameter with the quay.io namespace where images are

located. Use the pipe command to send the result to the `oc create` command to create an application from the template.

```
[student@workstation multicontainer-review]$ oc process quote-php-persistent \
> -p RHT_OCP4_QUAY_USER=${RHT_OCP4_QUAY_USER} | oc create -f -
pod/mysql created
pod/quote-php created
service/quote-php created
service/mysql created
persistentvolumeclaim/dbinit created
persistentvolumeclaim/dbclaim created
```

- 6.2. Verify the status of the deployment using the `oc get pods` command with the `-w` option to monitor the deployment status. Wait until both pods are running. It may take some time for both pods to start up.

```
[student@workstation multicontainer-review]$ oc get pods -w
NAME READY STATUS RESTARTS AGE
mysql 0/1 ContainerCreating 0 21s
quote-php 0/1 ContainerCreating 0 20s
quote-php 1/1 Running 0 35s
mysql 1/1 Running 0 49s
^C
```

Press `Ctrl+C` to exit the command.

7. Expose the service `quote-php`.

Allow the PHP Quote application to be accessible through the OpenShift router and reachable from an external network.

- 7.1. Use the `oc expose` command to expose the `quote-php` service.

```
[student@workstation multicontainer-review]$ oc expose svc quote-php
route.route.openshift.io/quote-php exposed
```

8. Test the application with `curl` and verify that it outputs an inspiring message.

- 8.1. Use the `oc get route` command to find the FQDN where the application is available. Note the FQDN for the app.

Run the following command in the terminal window.

```
[student@workstation multicontainer-review]$ oc get route
NAME HOST/PORT PATH SERVICES ...
quote-php quote-php-your_dev_user-deploy.wildcard_domain quote-php ...
```

- 8.2. Change to the `/home/student` directory.

```
[student@workstation multicontainer-review]$ cd ~
[student@workstation ~]$
```

- 8.3. Use the `curl` command to test the REST API for the PHP Quote application.

```
[student@workstation ~]$ curl -w "\n" \
> http://quote-php-${RHT_OCP4_DEV_USER}-deploy.${RHT_OCP4_WILDCARD_DOMAIN}
Always remember that you are absolutely unique.
Just like everyone else.
```



### Note

The text displayed in the output above may differ, but the `curl` command should run successfully.

## Evaluation

Grade your work by running the `lab multicontainer-review grade` command from your `workstation` machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab multicontainer-review grade
```

## Finish

To complete this lab, run the `lab multicontainer-review finish` command on `workstation`.

```
[student@workstation ~]$ lab multicontainer-review finish
```

This concludes the lab.

# Summary

---

In this chapter, you learned:

- Software-defined networks enable communication between containers. Containers must be attached to the same software-defined network to communicate.
- Containerized applications cannot rely on fixed IP addresses or host names to find services.
- Podman uses Container Network Interface (CNI) to create a software-defined network and attaches all containers on the host to that network. Kubernetes and OpenShift create a software-defined network between all containers in a pod.
- Within the same project, Kubernetes injects a set of variables for each service into all pods.
- OpenShift templates automate creating applications consisting of multiple resources. Template parameters allow using the same values when creating multiple resources.



## Chapter 8

# Troubleshooting Containerized Applications

### Goal

Troubleshoot a containerized application deployed on OpenShift.

### Objectives

- Troubleshoot an application build and deployment on OpenShift.
- Implement techniques for troubleshooting and debugging containerized applications.

### Sections

- Troubleshooting S2I Builds and Deployments (and Guided Exercise)
- Troubleshooting Containerized Applications (and Guided Exercise)

### Lab

- Troubleshooting Containerized Applications

# Troubleshooting S2I Builds and Deployments

## Objectives

After completing this section, you should be able to:

- Troubleshoot an application build and deployment steps on OpenShift.
- Analyze OpenShift logs to identify problems during the build and deploy process.

## Introduction to the S2I Process

The Source-to-Image (S2I) process is a simple way to automatically create images based on the programming language of the application source code in OpenShift. While this process is often a convenient way to quickly deploy applications, problems can arise during the S2I image creation process, either by the programming language characteristics or the runtime environment that require both developers and administrators to work together.

It is important to understand the basic workflow for most of the programming languages supported by OpenShift. The S2I image creation process is composed of two major steps:

- Build step: Responsible for compiling source code, downloading library dependencies, and packaging the application as a container image. Furthermore, the build step pushes the image to the OpenShift registry for the deployment step. The `BuildConfig` (BC) OpenShift resources drive the build step.
- Deployment step: Responsible for starting a pod and making the application available for OpenShift. This step executes after the build step, but only if the build step succeeded. The `Deployment` OpenShift resources drive the deployment step.

For the S2I process, each application uses its own `BuildConfig` and `Deployment` objects, the name of which matches the application name. The deployment process aborts if the build fails.

The S2I process starts each step in a separate pod. The build process creates a pod named `<application-name>-build-<number>-<string>`. For each build attempt, the entire build step executes and saves a log. Upon a successful build, the application starts on a separate pod named as `<application-name>-<string>`.

The OpenShift web console can be used to access the details for each step. To identify any build issues, the logs for a build can be evaluated and analyzed by clicking the `Builds` link from the left panel, depicted as follows.

Figure 8.1: Build instances of a project

For each build attempt, a history of the build, tagged with a number, is provided for evaluation. Clicking on the build name leads to the details page of the build:

Figure 8.2: Detailed view of a build instance

For each build attempt, a history of the build, tagged with a number, is provided for evaluation. Clicking on the build name leads to the details page of the build.

The **Logs** tab of the build details page shows the output generated by the build execution. Those logs are handy to identify build issues.

Use the **Deployment** link under **Workloads** section from the left panel to identify issues during the deployment step.

After selecting the appropriate deployment object, details show in the **Details** section.

The `oc` command-line interface has several subcommands for managing the logs. Likewise in the web interface, it has a set of commands which provides information about each step. For example, to retrieve the logs from a build configuration, run the following command:

```
[user@host ~]$ oc logs bc/<application-name>
```

If a build fails, after finding and fixing the issues, run the following command to request a new build:

```
[user@host ~]$ oc start-build <application-name>
```

By issuing that command, OpenShift automatically spawns a new pod with the build process.

Deployment logs can be checked with the `oc` command:

```
[user@host ~]$ oc logs deployment/<application-name>
```

If the deployment is running or has failed, the command returns the logs of the process deployment process. Otherwise, the command returns the logs from the application's pod.

## Describing Common Problems

Sometimes, the source code requires some customization that may not be available in containerized environments, such as database credentials, file system access, or message queue information. Those values usually take the form of internal environment variables. Developers using the S2I process may need to access this information.

The `oc logs` command provides important information about the build, deploy, and run processes of an application during the execution of a pod. The logs may indicate missing values or options that must be enabled, incorrect parameters or flags, or environment incompatibilities.



### Note

Application logs must be clearly labeled to identify problems quickly without the need to learn the container internals.

## Troubleshooting Permission Issues

OpenShift runs S2I containers using Red Hat Enterprise Linux as the base image, and any runtime difference may cause the S2I process to fail. Sometimes, the developer runs into permission issues, such as access denied due to the wrong permissions, or incorrect environment permissions set by administrators. S2I images enforce the use of a different user than the `root` user to access file systems and external resources. Also, Red Hat Enterprise Linux 8 enforces SELinux policies that restrict access to some file system resources, network ports, or process.

Some containers may require a specific user ID, whereas S2I is designed to run containers using a random user as per the default OpenShift security policy.

The following Dockerfile creates a Nexus container. Note the `USER` instruction indicating the `nexus` user should be used:

```
FROM ubi8/ubi:8.1
...contents omitted...
RUN chown -R nexus:nexus ${NEXUS_HOME}

USER nexus
WORKDIR ${NEXUS_HOME}
```

```
VOLUME ["/opt/nexus/sonatype-work"]
...contents omitted...
```

Trying to use the image generated by this Dockerfile without addressing volume permissions drives to errors when the container starts:

```
[user@host ~]$ oc logs nexus-1-wzjrn
...output omitted...
... org.sonatype.nexus.util.LockFile - Failed to write lock file
...FileNotFoundException: /opt/nexus/sonatype-work/nexus.lock (Permission denied)
...output omitted...
... org.sonatype.nexus.webapp.WebappBootstrap - Failed to initialize
...StateException: Nexus work directory already in use: /opt/nexus/sonatype-work
...output omitted...
```

To solve this issue, relax the OpenShift project security with the command `oc adm policy`:

```
[user@host ~]$ oc adm policy add-scc-to-user anyuid -z default
```

This `oc adm policy` command enables OpenShift executing container processes with non-root users. But the file systems used in the container must also be available for the running user. This is specially important when the container contains volume mounts.

To avoid file system permission issues, local folders used for container volume mounts must satisfy the following:

- The user executing the container processes must be the owner of the folder, or have the necessary rights. Use the `chown` command to update folder ownership.
- The local folder must satisfy the SELinux requirements to be used as a container volume. Assign the `container_file_t` group to the folder by using the `semanage fcontext -a -t container_file_t <folder>` command, then refresh the permissions with the `restorecon -R <folder>` command.

## Troubleshooting Invalid Parameters

Multi-container applications may share parameters, such as login credentials. Ensure that the same values for parameters reach all containers in the application. For example, for a Python application that runs in one container, connected with another container running a database, make sure that the two containers use the same user name and password for the database. Usually, logs from the application pod provide a clear idea of these problems and how to solve them.

A good practice to centralize shared parameters is to store them in **ConfigMaps**. Those **ConfigMaps** can be injected through the **Deployment** into containers as environment variables. Injecting the same **ConfigMap** into different containers ensures that not only the same environment variables are available, but also the same values. See the following pod resource definition:

```
apiVersion: v1
kind: Pod
...output omitted...
spec:
 containers:
```

```

- name: test-container
...output omitted...
env:
 - name: ENV_1 ❶
 valueFrom:
 configMapKeyRef:
 name: configMap_name1
 key: configMap_key_1
...output omitted...
envFrom:
 - configMapRef:
 name: configMap_name_2 ❷
...output omitted...

```

- ❶ An ENV\_1 environment variable is injected into the container. Its value is the value for the configMap\_key\_1 entry in the configMap\_name1 configMap.
- ❷ All entries in configMap\_name\_2 are injected into the container as environment variables with the same name and values.

## Troubleshooting Volume Mount Errors

When redeploying an application that uses a persistent volume on a local file system, a pod might not be able to allocate a persistent volume claim even though the persistent volume indicates that the claim is released.

To resolve the issue, delete the persistent volume claim and then the persistent volume. Then recreate the persistent volume:

```
[user@host ~]$ oc delete pv <pv_name>
[user@host ~]$ oc create -f <pv_resource_file>
```

## Troubleshooting Obsolete Images

OpenShift pulls images from the source indicated in an image stream unless it locates a locally-cached image on the node where the pod is scheduled to run. If you push a new image to the registry with the same name and tag, you must remove the image from each node the pod is scheduled on with the command `podman rmi`.

Run the `oc adm prune` command for an automated way to remove obsolete images and other resources.



## References

More information about troubleshooting images is available in the *Images* section of the OpenShift Container Platform documentation accessible at:

### Creating Images

[https://docs.openshift.com/container-platform/4.10/openshift\\_images/create-images.html](https://docs.openshift.com/container-platform/4.10/openshift_images/create-images.html)

Documentation about how to consume ConfigMap to create container environment variables can be found in the *Consuming in Environment Variables* of the

### Configure a Pod to use ConfigMaps

<https://kubernetes.io/docs/tasks/configure-pod-container/configure-pod-configmap/#define-container-environment-variables-using-configmap-data>

## ► Guided Exercise

# Troubleshooting an OpenShift Build

In this exercise, you will troubleshoot an OpenShift build and deployment process.

## Outcomes

You should be able to identify and solve the problems raised during the build and deployment process of a Node.js application.

## Before You Begin

Make sure you have completed the *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Retrieve the lab files and verify that Docker and the OpenShift cluster are running by running the following command.

```
[student@workstation ~]$ lab troubleshoot-s2i start
```

## Instructions

- 1. Load the configuration of your classroom environment. Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```

- 2. Enter your local clone of the D0180-apps Git repository and checkout the master branch of the course's repository to ensure you start this exercise from a known good state:

```
[student@workstation ~]$ cd ~/D0180-apps
[student@workstation D0180-apps]$ git checkout master
...output omitted...
```

- 3. Create a new branch to save any changes you make during this exercise:

```
[student@workstation D0180-apps]$ git checkout -b troubleshoot-s2i
Switched to a new branch 'troubleshoot-s2i'
[student@workstation D0180-apps]$ git push -u origin troubleshoot-s2i
...output omitted...
* [new branch] troubleshoot-s2i -> s2i
Branch 'troubleshoot-s2i' set up to track remote branch 'troubleshoot-s2i' from
'origin'.
```

- 4. Log in to OpenShift using the configured user, password and Master API URL.

```
[student@workstation D0180-apps]$ oc login -u "${RHT_OCP4_DEV_USER}" \
> -p "${RHT_OCP4_DEV_PASSWORD}" "${RHT_OCP4_MASTER_API}"
Login successful.
...output omitted...
```

Create a new project named `youruser-nodejs`.

```
[student@workstation D0180-apps]$ oc new-project ${RHT_OCP4_DEV_USER}-nodejs
Now using project "youruser-nodejs" on server ...
...output omitted...
```

- ▶ 5. Build a new Node.js application using the Hello World image located at <https://github.com/yourgituser/D0180-apps/> in the `nodejs-helloworld` directory.
- 5.1. Run the `oc new-app` command to create the Node.js application. The command is provided in the `~/D0180/labs/troubleshoot-s2i/``command.txt` file.

```
[student@workstation D0180-apps]$ oc new-app \
> --context-dir=nodejs-helloworld \
> https://github.com/${RHT_OCP4_GITHUB_USER}/D0180-apps#troubleshoot-s2i \
> -i nodejs:16-ubi8 --name nodejs-hello --build-env \
> npm_config_registry=http://${RHT_OCP4_NEXUS_SERVER}/repository/nodejs
--> Found image e9b0166 ...output omitted...

 Node.js 16
...output omitted...
--> Creating resources ...
 imagestream.image.openshift.io "nodejs-hello" created
 buildconfig.build.openshift.io "nodejs-hello" created
 deployment.apps "nodejs-hello" created
 service "nodejs-hello" created
--> Success
 Build scheduled, use 'oc logs -f buildconfig/nodejs-hello' to track its
progress.
 Application is not exposed. You can expose services to the outside world by
executing one or more of the commands below:
 'oc expose svc/nodejs-hello'
 Run 'oc status' to view your app.
```

The `-i` indicates the builder image to use, `nodejs:12` in this case.

The `--context-dir` option defines which folder inside the project contains the source code of the application to build.

The `--build-env` option defines an environment variable to the builder pod. In this case, it provides the `npm_config_registry` environment variable to the builder pod, so it can reach the NPM registry.



### Important

In the previous command, there must be no spaces between `registry=` and the URL of the Nexus server.

- 5.2. Wait until the application finishes building by monitoring the progress with the `oc get pods -w` command. The pod transitions from a status of `running` to `Error`:

```
[student@workstation D0180-apps]$ oc get pods -w
NAME READY STATUS RESTARTS AGE
nodejs-hello-1-build 1/1 Running 0 15s
nodejs-hello-1-build 0/1 Error 0 73s
^C
```

The build process fails, and therefore no application is running. Build failures are usually consequences of syntax errors in the source code or missing dependencies. The next step investigates the specific causes for this failure.

- 5.3. Evaluate the errors raised during the build process.

The build is triggered by the build configuration (bc) created by OpenShift when the S2I process starts. By default, the OpenShift S2I process creates a build configuration named as the name given: `nodejs-hello`, which is responsible for triggering the build process.

Run the `oc` command with the `logs` subcommand in a terminal window to review the output of the build process:

```
[student@workstation D0180-apps]$ oc logs bc/nodejs-hello
Cloning "https://github.com/yourgituser/D0180-apps" ...
Commit: f7cd8963ef353d9173c3a21dccc402f3616840b (Initial commit...
...output omitted...
STEP 8: RUN /usr/libexec/s2i/assemble
--> Installing application source ...
--> Installing all dependencies
npm ERR! code ETARGET
npm ERR! notarget No matching version found for express@~4.14.2.
npm ERR! notarget In most cases you or one of your dependencies are requesting
npm ERR! notarget a package version that doesn't exist.
npm ERR! notarget
npm ERR! notarget It was specified as a dependency of 'src'
npm ERR! notarget

npm ERR! A complete log of this run can be found in:
npm ERR! /opt/app-root/src/.npm/_logs/2019-10-25T12_37_56_853Z-debug.log
`error: build error: error building at STEP "RUN /usr/libexec/s2i/assemble": error
while running runtime: exit status 1
`

...output omitted...
```

The log shows an error occurred during the build process. This output indicates that there is no compatible version for the `express` dependency. But the reason is that the format used by the `express` dependency is not valid.

## ► 6. Update the build process for the project.

The developer uses a nonstandard version of the Express framework that is available locally on each developer's workstation. Due to the company's standards, the version must be downloaded from the Node.js official registry and, from the developer's input, it is compatible with the 4.14.x version.

### 6.1. Fix the `package.json` file.

Use your preferred editor to open the ~/D0180-apps/nodejs-helloworld/package.json file. Review the dependencies versions provided by the developers. It uses an incorrect version of the Express dependency, which is incompatible with the supported version provided by the company (~4.14.2). Update the dependency version as follows.

```
{
 "name": "nodejs-helloworld",
 ...output omitted...
 "dependencies": {
 "express": "4.14.x"
 }
}
```



### Note

Notice the x in the version. It indicates that the highest version should be used, but the version must begin with 4.14..

## 6.2. Commit and push the changes made to the project.

From the terminal window, run the following command to commit and push the changes:

```
[student@workstation D0180-apps]$ git commit -am "Fixed Express release"
...output omitted...
1 file changed, 1 insertion(+), 1 deletion(-)
[student@workstation D0180-apps]$ git push
...output omitted...
To https://github.com/yourgituser/D0180-apps
 ef6557d..73a82cd troubleshoot-s2i -> troubleshoot-s2i
```

## ► 7. Relaunch the S2I process.

### 7.1. To restart the build step, execute the following command:

```
[student@workstation D0180-apps]$ oc start-build bc/nodejs-hello
build.build.openshift.io/nodejs-hello-2 started
```

The build step is restarted, and a new build pod is created. Check the log by running the `oc logs` command.

```
[student@workstation D0180-apps]$ oc logs -f bc/nodejs-hello
Cloning "https://github.com/yourgituser/D0180-apps" ...
Commit: ea2125c1bf4681dd9b79ddf920d8d8be38cf3b (Fixed Express release)
...output omitted...
Pushing image ...image-registry.svc:5000/nodejs/nodejs-hello:latest...
...output omitted...
Push successful
```

The build is successful, however, this does not indicate that the application is started.

- 7.2. Evaluate the status of the current build process. Run the `oc get pods` command to check the status of the Node.js application.

```
[student@workstation D0180-apps]$ oc get pods
```

According to the following output, the second build completed, but the application is in error state.

NAME	READY	STATUS	RESTARTS	AGE
nodejs-hello-1-build	0/1	Error	0	7m59s
nodejs-hello-2-build	0/1	Completed	0	54s
nodejs-hello-7b99966464-fw4r8	0/1	CrashLoopBackOff	1	18s

The name of the application pod (`nodejs-hello-7b99966464-fw4r8`) is generated randomly, and may differ from yours.

- 7.3. Review the logs generated by the application pod.

```
[student@workstation D0180-apps]$ oc logs nodejs-hello-7b99966464-fw4r8
...output omitted...
npm info using npm@8.1.2
npm info using node@v16.13.1
npm ERR! missing script: start
...output omitted...
```



### Note

The `oc logs nodejs-hello-7b99966464-fw4r8` command dumps the logs from the deployment pod. In the case of a successful deployment, that command dumps the logs from the application pod, as previously shown.

If the deployment logs do not display the error, then check the logs of the application pod by running the `oc logs POD` command replacing POD with the name of the pod that has a status of CrashLoopBackOff.

The application fails to start because the `start` script declaration is missing.

## ► 8. Fix the problem by updating the application code.

- 8.1. Update the `package.json` file to define a startup command.

The previous output indicates that the `~/D0180-apps/nodejs-helloworld/package.json` file is missing the `start` attribute in the `scripts` field. The `start` attribute defines a command to run when the application starts. It invokes the `node` binary, which runs the `app.js` application.

To fix the problem, add to the `package.json` file the following attribute. Do not forget the comma after the bracket.

```
...
 "description": "Hello World!",
 "main": "app.js",
 "scripts": { "start": "node app.js" },
 "author": "Red Hat Training",
...
```

8.2. Commit and push the changes made to the project:

```
[student@workstation D0180-apps]$ git commit -am "Added start up script"
...output omitted...
1 file changed, 3 insertions(+)
[student@workstation D0180-apps]$ git push
...output omitted...
To https://github.com/yourgituser/D0180-apps
 73a82cd..a5a0411 troubleshoot-s2i -> troubleshoot-s2i
```

Continue the deploy step from the S2I process.

8.3. Restart the build step.

```
[student@workstation D0180-apps]$ oc start-build bc/nodejs-hello
build.build.openshift.io/nodejs-hello-3 started
```

8.4. Evaluate the status of the current build process. Run the command to retrieve the status of the Node.js application. Wait for the latest build to finish.

NAME	READY	STATUS	RESTARTS	AGE
nodejs-hello-1-build	0/1	Error	0	26m
nodejs-hello-2-build	0/1	Completed	0	19m
nodejs-hello-3-build	1/1	Running	0	9s
nodejs-hello-7b99966464-fw4r8	0/1	CrashLoopBackOff	8	19m
nodejs-hello-6dc88b7b7-dvtcz	0/1	Pending	0	0s
nodejs-hello-6dc88b7b7-dvtcz	0/1	Pending	0	0s
nodejs-hello-6dc88b7b7-dvtcz	0/1	ContainerCreating	0	0s
nodejs-hello-3-build	0/1	Completed	0	37s
nodejs-hello-6dc88b7b7-dvtcz	0/1	ContainerCreating	0	2s
nodejs-hello-6dc88b7b7-dvtcz	1/1	Running	0	3s
nodejs-hello-7b99966464-fw4r8	0/1	Terminating	8	19m
nodejs-hello-7b99966464-fw4r8	0/1	Terminating	8	19m
nodejs-hello-7b99966464-fw4r8	0/1	Terminating	8	19m

According to the output, the build is successful, and the application is able to start with no errors. The output also provides insight into how the deployment pod (nodejs-hello-3-build) was created, and that it completed successfully and terminated. As the new application pod is available (nodejs-hello-7b99966464-dvtcz), the old one (nodejs-hello-7b99966464-fw4r8) is rolled out.

8.5. Review the logs generated by the nodejs-hello application pod.

```
[student@workstation D0180-apps]$ oc logs nodejs-hello-6dcdb8b7b7-dvtcz
Environment:
 DEV_MODE=false
 NODE_ENV=production
 DEBUG_PORT=5858
Launching via npm...
npm info it worked if it ends with ok
npm info using npm@8.1.2
npm info using node@v16.13.1
npm info lifecycle nodejs-helloworld@1.0.0~prestart: nodejs-helloworld@1.0.0
npm info lifecycle nodejs-helloworld@1.0.0~start: nodejs-helloworld@1.0.0

> nodejs-helloworld@1.0.0 start
> node app.js

Example app listening on port 8080!
```

The application is now running on port 8080.

#### ► 9. Test the application.

- 9.1. Run the oc command with the expose subcommand to expose the application:

```
[student@workstation D0180-apps]$ oc expose svc/nodejs-hello
route.route.openshift.io/nodejs-hello exposed
```

- 9.2. Retrieve the address associated with the application.

```
[student@workstation D0180-apps]$ oc get route -o yaml
apiVersion: v1
items:
- apiVersion: route.openshift.io/v1
 kind: Route
 ...output omitted...
 spec:
 host: nodejs-hello-${RHT_OCP4_DEV_USER}-nodejs.${RHT_OCP4_WILDCARD_DOMAIN}
 port:
 targetPort: 8080-tcp
 to:
 kind: Service
 name: nodejs-hello
 ...output omitted...
```

- 9.3. Access the application from the workstation VM by using the curl command:

```
[student@workstation D0180-apps]$ curl -w "\n" \
> http://nodejs-hello-${RHT_OCP4_DEV_USER}-nodejs.${RHT_OCP4_WILDCARD_DOMAIN}
Hello world!
```

The output demonstrates the application is up and running.

## Finish

On `workstation`, run the `lab troubleshoot-s2i finish` script to complete this exercise.

```
[student@workstation DO180-apps]$ lab troubleshoot-s2i finish
```

This concludes the exercise.

# Troubleshooting Containerized Applications

## Objectives

After completing this section, you should be able to:

- Implement techniques for troubleshooting and debugging containerized applications.
- Use the port-forwarding feature of the OpenShift client tool.
- View container logs.
- View OpenShift cluster events.

## Forwarding Ports for Troubleshooting

Occasionally developers and system administrators need special network access to a container that would not be needed by application users. For example, developers may need to use the administration console for a database or messaging service, or system administrators may make use of SSH access to a container to restart a terminated service. Such network access, in the form of network ports, are usually not exposed by the default container configurations, and tend to require specialized clients used by developers and system administrators.

Podman provides port forwarding features by using the `-p` option along with the `run` subcommand. In this case, there is no distinction between network access for regular application access and for troubleshooting. As a refresher, the following is an example of configuring port forwarding by mapping the port from the host to a database server running inside a container:

```
[user@host ~]$ podman run --name db -p 30306:3306 mysql
```

The previous command maps the host port 30306 to the port 3306 on the db container. This container is created from the `mysql` image, which starts a MySQL server that listens on port 3306.

OpenShift provides the `oc port-forward` command for forwarding a local port to a pod port. This is different than having access to a pod through a service resource:

- The port-forwarding mapping exists only in the workstation where the `oc` client runs, while a service maps a port for all network users.
- A service load balances connections to potentially multiple pods, whereas a port-forwarding mapping forwards connections to a single pod.

Here is an example of the `oc port-forward` command:

```
[user@host ~]$ oc port-forward db 30306 3306
```

The preceding command forwards port 30306 from the developer machine to port 3306 on the db pod, where a MySQL server (inside a container) accepts network connections.

**Note**

When running this command, be sure to leave the terminal window running. Closing the window or canceling the process stops the port mapping.

While the `podman run -p` method of mapping (port-forwarding) can only be configured when the container is started, the mapping with the `oc port-forward` command can be created and destroyed at any time after a pod was created.

**Note**

Creating a service of `NodePort` type for a database pod would be similar to running `podman run -p`. However, Red Hat discourages the usage of the `NodePort` approach to avoid exposing the service to direct connections. Mapping with port-forwarding in OpenShift is considered a more secure alternative.

## Enabling Remote Debugging with Port Forwarding

Another use for the port forwarding feature is enabling remote debugging. Many integrated development environments (IDEs) provide the capability to remotely debug an application.

For example, Red Hat CodeReady Studio allows users to utilize the Java Debug Wire Protocol (JDWP) to communicate between its debugger and the Java Virtual Machine. When enabled, developers can step through each line of code as it is being executed in real time.

For JDWP to work, the Java Virtual Machine (JVM) where the application runs must be started with options enabling remote debugging. For example, WildFly and JBoss EAP users must configure these options on application server startup. The following line in the `standalone.conf` file enables remote debugging by opening the JDWP TCP port 8787, for a WildFly or EAP instance running in standalone mode:

```
JAVA_OPTS="$JAVA_OPTS \
> -agentlib:jdwp=transport=dt_socket,address=8787,server=y,suspend=n"
```

When the server starts with the debugger listening on port 8787, a port forwarding mapping needs to be created to forward connections from a local unused TCP port to port 8787 in the EAP pod. If the developer workstation has no local JVM running with remote debugging enabled, the local port can also be 8787.

The following command assumes a WildFly pod named `jappserver` running a container from an image previously configured to enable remote debugging:

```
[user@host ~]$ oc port-forward jappserver 8787:8787
```

Once the debugger is enabled and the port forwarding mapping is created, users can set breakpoints in their IDE of choice and run the debugger by pointing to the application's host name and debug port (in this instance, 8787).

## Accessing Container Logs

Podman and OpenShift provide the ability to view logs in running containers and pods to facilitate troubleshooting. But neither of them is aware of application specific logs. Both expect the application to be configured to send all logging output to the standard output.

A container is simply a process tree from the host OS perspective. When Podman starts a container either directly or on the RHOCP cluster, it redirects the container standard output and standard error, saving them on disk as part of the container's ephemeral storage. This way, the container logs can be viewed using podman and oc commands, even after the container was stopped, but not removed.

To retrieve the output of a running container, use the following podman command:

```
[user@host ~]$ podman logs containerName
```

In OpenShift, the following command returns the output for a container within a pod:

```
[user@host ~]$ oc logs podName -c containerName
```



### Note

The `-c containerName` arguments are optional if there is only one container, as `oc` defaults to the only running container and returns the output.

## OpenShift Events

Some developers consider Podman and OpenShift logs to be too low-level, making troubleshooting difficult. Fortunately, OpenShift provides a high-level logging and auditing facility called events.

OpenShift events signal significant actions like starting a container or destroying a pod.

To read OpenShift events, use the `get` subcommand with the `events` resource type for the `oc` command, as follows:

```
[user@host ~]$ oc get events
```

Events listed by the `oc` command this way are not filtered and span the whole RHOCP cluster. Using a pipe to standard UNIX filters such as `grep` can help, but OpenShift offers an alternative in order to consult cluster events. The approach is provided by the `describe` subcommand.

For example, to only retrieve the events that relate to a `mysql` pod, refer `Events` field from the output of `oc describe pod mysql` command:

```
[user@host ~]$ oc describe pod mysql
...output omitted...
Events:
 FirstSeen LastSeen Count From Reason Message
 Wed, 10 ... Wed, 10 ... 1 {scheduler} scheduled Successfully as...
...output omitted...
```

## Accessing Running Containers

The `podman logs` and `oc logs` commands can be useful for viewing output sent by any container. However, the output does not necessarily display all of the available information if the application is configured to send logs to a file. Other troubleshooting scenarios may require inspecting the container environment as seen by processes inside the container, such as verifying external connectivity.

As a solution, Podman and OpenShift provide the `exec` subcommand, allowing the creation of new processes inside a running container, with the standard output and input of these processes redirected to the user terminal. The following screen display the usage of the `podman exec` command:

```
[user@host ~]$ podman exec options container command arguments
```

The general syntax for the `oc exec` command is:

```
[user@host ~]$ oc exec options pod -c container -- command arguments
```

To execute a single interactive command or start a shell, add the `-it` options. The following example starts a Bash shell for the `myhttpd` pod:

```
[user@host ~]$ oc exec -it myhttpd /bin/bash
```

You can use this command to access application logs saved to disk (as part of the container ephemeral storage). For example, to display the Apache error log from a container, run the following command:

```
[user@host ~]$ podman exec apache-container cat /var/log/httpd/error_log
```

## Overriding Container Binaries

Many container images do not contain all of the troubleshooting commands users expect to find in regular OS installations, such as `telnet`, `netcat`, `ip`, or `traceroute`. Stripping the image from basic utilities or binaries allows the image to remain slim, thus, running many containers per host.

One way to temporarily access some of these missing commands is mounting the host binaries folders, such as `/bin`, `/sbin`, and `/lib`, as volumes inside the container. This is possible because the `-v` option from `podman run` command does not require matching `VOLUME` instructions to be present in the `Containerfile` of the container image.



### Note

To access these commands in OpenShift, you need to change the pod resource definition in order to define `volumeMounts` and `volumeClaims` objects. You also need to create a `hostPath` persistent volume.

The following command starts a container, and overrides the image's `/bin` folder with the one from the host. It also starts an interactive shell inside the container:

```
[user@host ~]$ podman run -it -v /bin:/bin image /bin/bash
```

**Note**

The directory of binaries to override depends on the base OS image. For example, some commands require shared libraries from the `/lib` directory. Some Linux distributions have different contents in `/bin`, `/usr/bin`, `/lib`, or `/usr/lib`, which would require to use the `-v` option for each directory.

As an alternative, you can include these utilities in the base image. To do so, add instructions in a `Containerfile` build definition. For example, examine the following excerpt from a `Containerfile` definition, which is a child of the `rhel7.5` image. The `RUN` instruction installs the tools that are commonly used for network troubleshooting:

```
FROM ubi7/ubi:7.7

RUN yum install -y less dig ping iputils && \
 yum clean all
```

When the image is built and the container is created, it will be identical to a `rhel7.5` container image, plus the extra available tools.

## Transferring Files to and from Containers

When troubleshooting or managing an application, you might need to retrieve or transfer files to and from running containers, such as configuration files or log files. There are several ways to move files into and out of containers, as described in the following list.

### Volume mounts

Another option for copying files from the host to a container is the usage of volume mounts. You can mount a local directory to copy data into a container. For example, the following command sets `/conf` host directory as the volume to use for the Apache configuration directory in the container. This provides a convenient way to manage the Apache server without having to rebuild the container image.

```
[user@host ~]$ podman run -v /conf:/etc/httpd/conf -d do180/apache
```

`podman cp`

The `cp` subcommand allows users to copy files both into and out of a running container. To copy a file into a container named `todoapi`, run the following command.

```
[user@host ~]$ podman cp standalone.conf \
> todoapi:/opt/jboss/standalone/conf/standalone.conf
```

To copy a file from the container to the host, flip the order of the previous command.

```
[user@host ~]$ podman cp todoapi:/opt/jboss/standalone/conf/standalone.conf .
```

The `podman cp` command has the advantage of working with containers that were already started, while the following alternative (volume mounts) requires changes to the command used to start a container.

**podman exec**

For containers that are already running, the `podman exec` command can be piped to pass files both into and out of the running container by appending commands that are executed in the container. The following example shows how to pass in and execute a SQL file inside a MySQL container:

```
[user@host ~]$ podman exec -i container mysql -uroot -proot \
> < /path/on/host/db.sql
```

Using the same concept, it is possible to retrieve data from a running container and place it in the host machine. A useful example of this is the usage of the `mysqldump` utility, which creates a backup of MySQL database from the container and places it on the host.

```
[user@host ~]$ podman exec -it containerName sh \
> -c 'exec mysqldump -h"$MYSQL_PORT_3306_TCP_ADDR" \
> -P"$MYSQL_PORT_3306_TCP_PORT" \
> -uroot -p"$MYSQL_ENV_MYSQL_ROOT_PASSWORD" items' > db_dump.sql
```

The preceding command uses the container environment variables to connect to the MySQL server to execute the `mysqldump` command and redirects the output to a file on the host machine. It assumes that the container image provides the `mysqldump` utility, so there is no need to install the MySQL administration tools on the host.

The `oc rsync` command provides functionality similar to `podman cp` for containers running under OpenShift pods.



## References

More information about port-forwarding is available in the *Port Forwarding* section of the OpenShift Container Platform documentation at

### Architecture

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.10/html-single/architecture/index/](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.10/html-single/architecture/index/)

More information about the CLI commands for port-forwarding are available in the *Port Forwarding* chapter of the OpenShift Container Platform documentation at

### Developing Applications

[https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.10/html-single/building\\_applications/index](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.10/html-single/building_applications/index)

## ► Guided Exercise

# Configuring Apache Container Logs for Debugging

In this exercise, you will configure an Apache httpd container to send the logs to the `stdout`, then review Podman logs and events.

## Outcomes

You should be able to configure an Apache httpd container to send debug logs to `stdout` and view them using the `podman logs` command.

## Before You Begin

Make sure you have completed the *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Retrieve the lab files and verify that Docker and the OpenShift cluster are running by running the following command.

```
[student@workstation ~]$ lab troubleshoot-container start
```

## Instructions

- ▶ 1. Configure a Apache web server to send log messages to the standard output and update the default log level.
  - 1.1. The default log level for the Apache httpd image is `warn`. Change the default log level for the container to `debug`, and redirect log messages to `stdout` by overriding the default `httpd.conf` configuration file. To do so, create a custom image from the `workstation` VM.  
Briefly review the custom `httpd.conf` file located at `~/D0180/labs/troubleshoot-container/conf/httpd.conf`.
    - Observe the `LogLevel` directive in the file. The directive changes the default log level to `debug`.
    - Observe the `ErrorLog` directive in the file. The directive sends the httpd error log messages to the container's standard output.
    - Observe the `CustomLog` directive in the file. The directive redirects the httpd access log messages to the container's standard output.

```
ErrorLog "/dev/stdout"
...output omitted...
LogLevel debug
```

```
...output omitted...
```

```
CustomLog "/dev/stdout" common
```

- 2. Build a custom container to save an updated configuration file to the container.

- 2.1. From the terminal window, run the following commands to build a new image.

```
[student@workstation ~]$ cd ~/DO180/labs/troubleshoot-container
[student@workstation troubleshoot-container]$ podman build \
> -t troubleshoot-container .
STEP 1: FROM quay.io/redhattraining/httpd-parent
...output omitted...
STEP 5: COMMIT troubleshoot-container
e23d...c1de
[student@workstation troubleshoot-container]$ cd ~
```

- 2.2. Verify that the image is created.

```
[student@workstation ~]$ podman images
```

The new image must be available in the local storage.

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
localhost/troubleshoot-container	latest	e23df...	9 seconds ago	137MB
quay.io/redhattraining/httpd-parent	latest	0eba3...	4 weeks ago	137MB

- 3. Create a new httpd container from the custom image.

```
[student@workstation ~]$ podman run \
> --name troubleshoot-container -d \
> -p 10080:80 troubleshoot-container
4c8bb12815cc02f4eef0254632b7179bd5ce230d83373b49761b1ac41fc067a9
```

- 4. Review the container's log messages and events.

- 4.1. View the debug log messages from the container using the `podman logs` command:  
Notice the debug logs, available in the standard output.

```
[student@workstation ~]$ podman logs -f troubleshoot-container
... [mpm_event:notice] [pid 1:tid...] AH00489: Apache/2.4.37 ...
... [mpm_event:info] [pid 1:tid...] AH00490: Server built: Apr 5 2019 07:31:21
... [core:notice] [pid 1:tid...] AH00094: Command line: 'httpd -D FOREGROUND'
... [core:debug] [pid 1:tid ...]: AH02639: Using SO_REUSEPORT: yes (1)
... [mpm_event:debug] [pid 6:tid ...]: AH02471: start_threads: Using epoll
... [mpm_event:debug] [pid 7:tid ...]: AH02471: start_threads: Using epoll
... [mpm_event:debug] [pid 8:tid ...]: AH02471: start_threads: Using epoll
```

- 4.2. Open a new terminal and access the home page of the web server by using the `curl` command:

```
[student@workstation ~]$ curl http://127.0.0.1:10080
Hello from the httpd-parent container!
```

- 4.3. Review the new entries in the log. Look in the terminal running the podman logs command to see the new entries.

```
...output omitted...
10.0.2.2 - - [31/Mar/2022:14:06:03 +0000] "GET / HTTP/1.1" 200 39
```

- 4.4. Stop the Podman command with **Ctrl+C**.

## Finish

On workstation, run the following script to complete this lab.

```
[student@workstation ~]$ lab troubleshoot-container finish
```

This concludes the guided exercise.

## ▶ Lab

# Troubleshooting Containerized Applications

### Outcomes

You should be able to identify and solve the problems raised during the build and deployment process of a Node.js application.

### Before You Begin

Make sure you have completed the *Guided Exercise: Configuring the Classroom Environment* from Chapter 1 before executing any command of this practice.

Open a terminal on workstation as the student user and run the following command:

```
[student@workstation ~]$ lab troubleshoot-review start
```

### Instructions

1. Load the configuration of your classroom environment. Run the following command to load the environment variables created in the first guided exercise:
2. Enter your local clone of the D0180-apps Git repository and checkout the master branch of the course's repository to ensure you start this exercise from a known good state:
3. Create a new branch named troubleshoot-review and push it to save any changes you make during this exercise:
4. Log in to OpenShift using the configured user, password and Master API URL.
5. Create a new project named *youruser-nodejs-app*:
6. In the *youruser-nodejs-app* project, create a new application named *nodejs-dev*. Use the image stream *nodejs:16-ubi8* and the source code in the *nodejs-app* directory, located in the Git repository branch *troubleshoot-review* that you created in an earlier step. Set the *npm\_config\_registry* environment variable value with `http:// ${RHT_OCP4_NEXUS_SERVER}/repository/nodejs`.  
Expect the build process for the application to fail. Monitor the build process and identify the build failure.
7. Update the version of the *express* dependency in the *package.json* file with a value of *4.x*. Commit and push the changes to the Git repository.
8. Rebuild the application. Verify that the application builds without errors.
9. Verify that the application is not running because of a runtime error. Review the logs and identify the problem.
10. The log indicates that the *server.js* file attempts to load a module named *http-error*, which is not available. Change the required module in the first line of the *server.js* to *html-errors*, which is a valid module in the *packages* file. Commit and push changes to

- the application to the Git repository. Rebuild the application. After the application builds, verify that the application is running.
11. Create a route for the application and test access to the application. Expect an error message. Review the logs to identify the error.
  12. Replace `process.environment` with `process.env` in the `server.js` file to fix the error. Commit and push the application changes to the Git repository. Rebuild the application. When the new application deploys, verify that application does not generate errors when you access the application URL.
  13. Change to the `/home/student` directory.

```
[student@workstation nodejs-app]$ cd
[student@workstation ~]$
```

## Evaluation

Grade your work by running the `lab troubleshoot-review grade` command from your `workstation` machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab troubleshoot-review grade
```

## Finish

From `workstation`, run the `lab troubleshoot-review finish` command to complete this lab.

```
[student@workstation ~]$ lab troubleshoot-review finish
```

This concludes the lab.

## ► Solution

# Troubleshooting Containerized Applications

### Outcomes

You should be able to identify and solve the problems raised during the build and deployment process of a Node.js application.

### Before You Begin

Make sure you have completed the *Guided Exercise: Configuring the Classroom Environment* from Chapter 1 before executing any command of this practice.

Open a terminal on workstation as the student user and run the following command:

```
[student@workstation ~]$ lab troubleshoot-review start
```

### Instructions

1. Load the configuration of your classroom environment. Run the following command to load the environment variables created in the first guided exercise:

```
[student@workstation ~]$ source /usr/local/etc/ocp4.config
```

2. Enter your local clone of the D0180-apps Git repository and checkout the master branch of the course's repository to ensure you start this exercise from a known good state:

```
[student@workstation ~]$ cd ~/D0180-apps
[student@workstation D0180-apps]$ git checkout master
...output omitted...
```

3. Create a new branch named troubleshoot-review and push it to save any changes you make during this exercise:

```
[student@workstation D0180-apps]$ git checkout -b troubleshoot-review
Switched to a new branch 'troubleshoot-review'
[student@workstation D0180-apps]$ git push -u origin troubleshoot-review
...output omitted...
* [new branch] troubleshoot-review -> troubleshoot-review
Branch 'troubleshoot-review' set up to track remote branch 'troubleshoot-review'
from 'origin'.
```

4. Log in to OpenShift using the configured user, password and Master API URL.

```
[student@workstation D0180-apps]$ oc login -u "${RHT_OCP4_DEV_USER}" \
> -p "${RHT_OCP4_DEV_PASSWORD}" "${RHT_OCP4_MASTER_API}"
Login successful.
...output omitted...
```

5. Create a new project named *youruser-nodejs-app*:

```
[student@workstation ~]$ oc new-project ${RHT_OCP4_DEV_USER}-nodejs-app
Now using project "youruser-nodejs-app" on server "https://
api.cluster.lab.example.com"
...output omitted...
```

6. In the *youruser-nodejs-app* project, create a new application named *nodejs-dev*. Use the image stream *nodejs:16-ubi8* and the source code in the *nodejs-app* directory, located in the Git repository branch *troubleshoot-review* that you created in an earlier step. Set the *npm\_config\_registry* environment variable value with *http://\${RHT\_OCP4\_NEXUS\_SERVER}/repository/nodejs*.

Expect the build process for the application to fail. Monitor the build process and identify the build failure.

- 6.1. Run the *oc new-app* command to create the Node.js application.

```
[student@workstation ~]$ oc new-app --name nodejs-dev \
> https://github.com/${RHT_OCP4_GITHUB_USER}/D0180-apps#troubleshoot-review \
> -i nodejs:16-ubi8 --context-dir=nodejs-app --build-env \
> npm_config_registry=http://${RHT_OCP4_NEXUS_SERVER}/repository/nodejs
--> Found image a2b5ec2 ...output omitted...

Node.js 16
...output omitted...
--> Creating resources ...
imagestream.image.openshift.io "nodejs-dev" created
buildconfig.build.openshift.io "nodejs-dev" created
deployment.apps "nodejs-dev" created
service "nodejs-dev" created
--> Success
Build scheduled, use 'oc logs -f buildconfig/nodejs-dev'` to track its
progress.
Application is not exposed. You can expose services to the outside world by
executing one or more of the commands below:
'oc expose service/nodejs-dev'
Run '+oc status' to view your app.
```

- 6.2. Monitor build progress with the *oc logs -f bc/nodejs-dev* command:

```
[student@workstation ~]$ oc logs -f bc/nodejs-dev
Cloning "https://github.com/yourgituser/D0180-apps" ...
...output omitted...
STEP 8: RUN /usr/libexec/s2i/assemble
--> Installing application source ...
--> Installing all dependencies
npm ERR! code ETARGET
```

```
npm ERR! notarget No matching version found for express@4.20.
npm ERR! notarget In most cases you or one of your dependencies are requesting
npm ERR! notarget a package version that doesn't exist.
npm ERR! notarget
npm ERR! notarget It was specified as a dependency of 'src'
npm ERR! notarget

npm ERR! A complete log of this run can be found in:
npm ERR! /opt/app-root/src/.npm/_logs/2019-10-28T11_30_27_657Z-debug.log
subprocess exited with status 1
subprocess exited with status 1
error: build error: error building at STEP "RUN /usr/libexec/s2i/assemble": exit
status 1
```

The build process fails, and therefore no application is running. The build log indicates that there is no version of the `express` package that matches a version specification of `4.20.x`.

- 6.3. Use the `oc get pods` command to confirm that the application is not deployed:

```
[student@workstation ~]$ oc get pods
NAME READY STATUS RESTARTS AGE
nodejs-dev-1-build 0/1 Error 0 2m
```

7. Update the version of the `express` dependency in the `package.json` file with a value of `4.x`. Commit and push the changes to the Git repository.

- 7.1. Edit the `package.json` file in the `nodejs-app` subdirectory, and change the version of the `express` dependency to `4.x`. Save the file.

```
[student@workstation DO180-apps]$ cd nodejs-app
[student@workstation nodejs-app]$ sed -i s/4.20/4.x/ package.json
```

The file contains the following content:

```
[student@workstation nodejs-app]$ cat package.json
{
 "name": "nodejs-app",
 "version": "1.0.0",
 "description": "Hello World App",
 "main": "server.js",
 "author": "Red Hat Training",
 "license": "ASL",
 "dependencies": {
 "express": "4.x",
 "html-errors": "latest"
 }
}
```

- 7.2. Commit and push the changes made to the project.

From the terminal window, run the following command to commit and push the changes:

```
[student@workstation nodejs-app]$ git commit -am "Fixed Express release"
...output omitted...
1 file changed, 1 insertion(+), 1 deletion(-)
[student@workstation nodejs-app]$ git push
...output omitted...
To https://github.com/yourgituser/D0180-apps/
 ef6557d..73a82cd troubleshoot-review -> troubleshoot-review
```

8. Rebuild the application. Verify that the application builds without errors.

- 8.1. Use the `oc start-build` command to rebuild the application.

```
[student@workstation nodejs-app]$ oc start-build bc/nodejs-dev
build.build.openshift.io/nodejs-dev-2 started
```

- 8.2. Use the `oc logs` command to monitor the build process logs:

```
[student@workstation nodejs-app]$ oc logs -f bc/nodejs-dev
Cloning "https://github.com/yourgituser/D0180-apps" ...
...output omitted...
Pushing image ...image-registry.svc:5000/nodejs-app/nodejs-dev:latest ...
...output omitted...
Push successful
```

The build succeeds if an image is pushed to the internal OpenShift registry.

9. Verify that the application is not running because of a runtime error. Review the logs and identify the problem.

- 9.1. Use the `oc get pods` command to check the status of the deployment of the application pod. Eventually, you see that the first application deployment has a status of CrashLoopBackoff.

NAME	READY	STATUS	RESTARTS	AGE
nodejs-dev-1-build	0/1	Error	0	4m27s
nodejs-dev-1-deploy	0/1	Completed	0	28s
nodejs-dev-1-skf56	0/1	CrashLoopBackOff	2	25s
nodejs-dev-2-build	0/1	Completed	0	58s

- 9.2. Use the `oc logs -f deployment/nodejs-dev` command to follow the logs for the application deployment:

```
[student@workstation nodejs-app]$ oc logs -f deployment/nodejs-dev
Environment:
 DEV_MODE=false
 NODE_ENV=production
 DEBUG_PORT=5858
...output omitted...

Error: Cannot find module 'http-error'

...output omitted...
```

```

npm info nodejs-app@1.0.0 Failed to exec start script
...output omitted...
npm ERR! code ELIFECYCLE
npm ERR! errno 1
npm ERR! nodejs-app@1.0.0 start: node `server.js`
npm ERR! Exit status 1
npm ERR!
npm ERR! Failed at the nodejs-app@1.0.0 start script.
npm ERR! This is probably not a problem with npm. There is likely additional
logging output above.
npm timing npm Completed in 159ms
...output omitted...

```

The log indicates that the `server.js` file attempts to load a module named `http-error`. The dependencies variable in the packages file indicates that the module name is `html-errors`, not `http-error`.

10. The log indicates that the `server.js` file attempts to load a module named `http-error`, which is not available. Change the required module in the first line of the `server.js` to `html-errors`, which is a valid module in the `packages` file. Commit and push changes to the application to the Git repository. Rebuild the application. After the application builds, verify that the application is running.
  - 10.1. Correct the spelling of the module in the first line of the `server.js` from `http-error` to `html-errors`. Save the file.

```
[student@workstation nodejs-app]$ sed -i s/http-error/html-errors/ server.js
```

The file contains the following content:

```

[student@workstation nodejs-app]$ cat server.js
var createError = require("html-errors");

var express = require('express');
app = express();

app.get('/', function (req, res) {
 res.send('Hello World from pod: ' + process.env.HOSTNAME + '\n')
});

app.listen(8080, function () {
 console.log('Example app listening on port 8080!');
});

```

- 10.2. Commit and push the changes made to the project.

```

[student@workstation nodejs-app]$ git commit -am "Fixed module typo"
...output omitted...
1 file changed, 1 insertion(+), 1 deletion(-)
[student@workstation nodejs-app]$ git push
...output omitted...
To https://github.com/yourgituser/D0180-apps/
 ef6557d..73a82cd troubleshoot-review -> troubleshoot-review

```

- 10.3. Use the `oc start-build` command to rebuild the application.

```
[student@workstation nodejs-app]$ oc start-build bc/nodejs-dev
build.build.openshift.io/nodejs-dev-3 started
```

- 10.4. Use the `oc logs` command to monitor the build process logs:

```
[student@workstation nodejs-app]$ oc logs -f bc/nodejs-dev
Cloning "https://github.com/yourgituser/D0180-apps" ...
...output omitted...
Pushing image ...-image-registry.svc:5000/nodejs-app/nodejs-dev:latest ...
...output omitted...
Push successful
```

- 10.5. Use the `oc get pods -w` command to monitor the deployment of pods for the `nodejs-dev` application:

NAME	READY	STATUS	RESTARTS	AGE
nodejs-dev-1-build	0/1	Error	0	11m
nodejs-dev-1-deploy	0/1	Completed	0	7m11s
nodejs-dev-2-9nds4	1/1	<b>Running</b>	0	56s
nodejs-dev-2-build	0/1	Completed	0	7m41s
nodejs-dev-2-deploy	0/1	Completed	0	61s
nodejs-dev-3-build	0/1	Completed	0	94s

After a third build, the second deployment results in a status of **Running**.

11. Create a route for the application and test access to the application. Expect an error message. Review the logs to identify the error.

- 11.1. Use the `oc expose` command to create a route for the `nodejs-dev` application:

```
[student@workstation nodejs-app]$ oc expose svc nodejs-dev
route.route.openshift.io/nodejs-dev exposed
```

- 11.2. Use the `oc get route` command to retrieve the URL of `nodejs-dev` route:

NAME	HOST/PORT	...
nodejs-dev	nodejs-dev-your_user-nodejs-app.wildcard_domain	...

- 11.3. Use the `curl` to access the route. Expect an error message to display.

```
[student@workstation nodejs-app]$ curl \
> nodejs-dev-${RHT_OCP4_DEV_USER}-nodejs-app.${RHT_OCP4_WILDCARD_DOMAIN}
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
```

```
<pre>Internal Server Error</pre>
</body>
</html>
```

11.4. Review the logs for the nodejs-dev deployment:

```
[student@workstation nodejs-app]$ oc logs -f deployment/nodejs-dev
Environment:
 DEV_MODE=false
 NODE_ENV=production
 DEBUG_PORT=5858
Launching via npm...
npm info it worked if it ends with ok
npm info using npm@6.14.8
npm info using node@v12.19.1
npm info lifecycle nodejs-app@1.0.0~prestart: nodejs-app@1.0.0
npm info lifecycle nodejs-app@1.0.0~start: nodejs-app@1.0.0

Example app listening on port 8080!
TypeError: Cannot read property 'HOSTNAME' of undefined
...output omitted...
```

The corresponding section of the server.js file is:

```
app.get('/', function (req, res) {
 res.send('Hello World from pod: ' + process.env.HOSTNAME + '\n')
});
```

A process object in Node.js contains a reference to a env object, not a environment object.

12. Replace process.environment with process.env in the server.js file to fix the error. Commit and push the application changes to the Git repository. Rebuild the application. When the new application deploys, verify that application does not generate errors when you access the application URL.

12.1. Replace process.environment with process.env in the server.js file to fix the error.

```
[student@workstation nodejs-app]$ sed -i \
> 's/process.environment/process.env/' server.js
```

The file contains the following content:

```
[student@workstation nodejs-app]$ cat server.js
var createError = require('http-errors');

var express = require('express');
app = express();

app.get('/', function (req, res) {
 res.send('Hello World from pod: ' + process.env.HOSTNAME + '\n')
});
```

```
app.listen(8080, function () {
 console.log('Example app listening on port 8080!');
});
```

12.2. Commit and push the changes made to the project.

```
[student@workstation nodejs-app]$ git commit -am "Fixed process.env"
...output omitted...
1 file changed, 1 insertion(+), 1 deletion(-)
[student@workstation nodejs-app]$ git push
...output omitted...
To https://github.com/yourgituser/D0180-apps/
 ef6557d..73a82cd troubleshoot-review -> troubleshoot-review
```

12.3. Use the `oc start-build` command to rebuild the application.

```
[student@workstation nodejs-app]$ oc start-build bc/nodejs-dev
build.build.openshift.io/nodejs-dev-4 started
```

12.4. Use the `oc logs` command to monitor the build process logs:

```
[student@workstation nodejs-app]$ oc logs -f bc/nodejs-dev
Cloning "https://github.com/yourgituser/D0180-apps" ...
...output omitted...
Pushing image ...image-registry.svc:5000/nodejs-app/nodejs-dev:latest ...
...output omitted...
Push successful
```

12.5. Use the `oc get pods` command to monitor the deployment of pods for the `nodejs-dev` application:

NAME	READY	STATUS	RESTARTS	AGE
nodejs-dev-1-build	0/1	Error	0	21m
nodejs-dev-1-deploy	0/1	Completed	0	17m
nodejs-dev-2-build	0/1	Completed	0	17m
nodejs-dev-2-deploy	0/1	Completed	0	11m
nodejs-dev-3-build	0/1	Completed	0	11m
nodejs-dev-3-deploy	0/1	Completed	0	20s
<b>nodejs-dev-3-wlpps</b>	1/1	<b>Running</b>	0	17s
nodejs-dev-4-build	0/1	Completed	0	48s

After a fourth build, the third deployment has a status of `Running`.

12.6. Use the `curl` command to test the application. The application displays a `Hello World` message containing the host name of the application pod:

```
[student@workstation nodejs-app]$ curl \
> nodejs-dev-${RHT_OCP4_DEV_USER}-nodejs-app.${RHT_OCP4_WILDCARD_DOMAIN}
Hello World from pod: nodejs-dev-3-wlpps
```

13. Change to the `/home/student` directory.

```
[student@workstation nodejs-app]$ cd
[student@workstation ~]$
```

## Evaluation

Grade your work by running the `lab troubleshoot-review grade` command from your workstation machine. Correct any reported failures and rerun the script until successful.

```
[student@workstation ~]$ lab troubleshoot-review grade
```

## Finish

From workstation, run the `lab troubleshoot-review finish` command to complete this lab.

```
[student@workstation ~]$ lab troubleshoot-review finish
```

This concludes the lab.

# Summary

---

In this chapter, you learned:

- Applications typically log activity, such as events, warnings and errors, to aid the analysis of application behavior.
- Container applications should print log data to standard output, instead of to a file, to enable easy access to logs.
- To review the logs for a container deployed locally with Podman, use the `podman logs` command.
- Use the `oc logs` command to access logs for `BuildConfig` and `Deployment` objects, as well as individual pods within an OpenShift project.
- The `-f` option allows you to monitor the log output in near real-time for both the `podman logs` and `oc logs` commands.
- Use the `oc port-forward` command to connect directly to a port on an application pod. You should only leverage this technique on non-production pods, because interactions can alter the behavior of the pod.

## Chapter 9

# Comprehensive Review

### Goal

Review tasks from *Red Hat OpenShift I: Containers & Kubernetes*

### Objectives

- Review tasks from *Red Hat OpenShift I: Containers & Kubernetes*

### Sections

- Comprehensive Review

### Lab

- Comprehensive Review of Introduction to Containers, Kubernetes, and Red Hat OpenShift

# Comprehensive Review

---

## Objectives

After completing this section, you should have reviewed and refreshed the knowledge and skills learned in *Red Hat OpenShift I: Containers & Kubernetes*.

## Reviewing Red Hat OpenShift I: Containers & Kubernetes

Before beginning the comprehensive review for this course, you should be comfortable with the topics covered in each chapter.

You can refer to earlier sections in the textbook for extra study.

### **Chapter 1, Introducing Container Technology**

Describe how applications run in containers orchestrated by Red Hat OpenShift Container Platform.

- Describe the difference between container applications and traditional deployments.
- Describe the basics of container architecture.
- Describe the benefits of orchestrating applications and OpenShift Container Platform.

### **Chapter 2, Creating Containerized Services**

Provision a service using container technology.

- Create a database server from a container image.

### **Chapter 3, Managing Containers**

Make use of prebuilt container images to create and manage containerized services.

- Manage a container's lifecycle from creation to deletion.
- Save container application data with persistent storage.
- Describe how to use port forwarding to access a container.

### **Chapter 4, Managing Container Images**

Manage the lifecycle of a container image from creation to deletion.

- Search for and pull images from remote registries.
- Export, import, and manage container images locally and in a registry.

### **Chapter 5, Creating Custom Container Images**

Design and code a Containerfile to build a custom container image.

- Describe the approaches for creating custom container images.
- Create a container image using common Containerfile commands.

## ***Chapter 6, Deploying Containerized Applications on OpenShift***

Deploy single container applications on OpenShift Container Platform.

- Describe the architecture of Kubernetes and Red Hat OpenShift Container Platform.
- Create standard Kubernetes resources.
- Create a route to a service.
- Build an application using the Source-to-Image facility of OpenShift Container Platform.
- Create an application using the OpenShift web console.

## ***Chapter 7, Deploying Multi-Container Applications***

Deploy applications that are containerized using multiple container images.

- Describe considerations for containerizing applications with multiple container images.
- Deploy a multi-container application on OpenShift Platform.
- Deploy an Application on OpenShift using a template.

## ***Chapter 8, Troubleshooting Containerized Applications***

Troubleshoot a containerized application deployed on OpenShift.

- Troubleshoot an application build and deployment on OpenShift.
- Implement techniques for troubleshooting and debugging containerized applications.

## ► Lab

# Containerizing and Deploying a Software Application

In this review, you will containerize a Nexus server, build and test it using Podman, and deploy it to an OpenShift cluster.

## Outcomes

You should be able to:

- Write a Containerfile that successfully containerizes a Nexus server.
- Build a Nexus server container image and deploy it using Podman.
- Deploy the Nexus server container image to an OpenShift cluster.

## Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Run the set-up script for this comprehensive review.

```
[student@workstation ~]$ lab comprehensive-review start
```

The lab files are located in the `~/D0180/labs/comprehensive-review` directory. The solution files are located in the `~/D0180/solutions/comprehensive-review` directory.

## Instructions

Use the following steps to create and test a containerized Nexus server both locally and in OpenShift:

1. Create a container image that starts an instance of a Nexus server:
  - The `~/D0180/labs/comprehensive-review/image` directory contains files for building the container image. Execute the `get-nexus-bundle.sh` script to retrieve the Nexus server files.
  - Write a Containerfile that containerizes the Nexus server. The Containerfile must be located in the `~/D0180/labs/comprehensive-review/image` directory. The Containerfile must also:
    - Use a base image of `ubi8/ubi:8.5` and set an arbitrary maintainer.
    - Set the ARG variable `NEXUS_VERSION` to `2.14.3-02`, and set the environment variable `NEXUS_HOME` to `/opt/nexus`.
    - Install the `java-1.8.0-openjdk-devel` package.

- Run a command to create a `nexus` user and group. They both have a UID and GID of `1001`. Change the permissions of the  `${NEXUS_HOME} /`  directory to `775`.

- Unpack the `nexus-2.14.3-02-bundle.tar.gz` file to the  `${NEXUS_HOME} /`  directory. Add the `nexus-start.sh` to the same directory.

Run a command, `ln -s ${NEXUS_HOME}/nexus-$ ${NEXUS_VERSION} ${NEXUS_HOME}/nexus2`, to create a symlink in the container. Run a command to recursively change the ownership of the Nexus home directory to `nexus:nexus`.

- Make the container run as the `nexus` user, and set the working directory to `/opt/nexus`.
- Define a volume mount point for the `/opt/nexus/sonatype-work` container directory. The Nexus server stores data in this directory.
- Set the default container command to `nexus-start.sh`.

There are two `*.snippet` files in the `~/D0180/labs/comprehensive-review/image` directory that provide the commands needed to create the `nexus` account and install Java. Use the files to assist you in writing the `Containerfile`.

- Build the container image with the name `nexus`.

## 2. Build and test the container image using Podman with a volume mount:

- Use the script `~/D0180/labs/comprehensive-review/deploy/local/run-persistent.sh` to start a new container with a volume mount.
- Review the container logs to verify that the server is started and running.
- Test access to the container service using the URL: `http://127.0.0.1:18081/nexus`.
- Remove the test container.

## 3. Deploy the Nexus server container image to the OpenShift cluster. You must:

- Tag the Nexus server container image as `quay.io/${RHT_OCP4_QUAY_USER}/nexus:latest`, and push it corresponding public repository on quay.io.
- Create an OpenShift project with a name of  `${RHT_OCP4_DEV_USER} -review`.
- Edit the `deploy/openshift/resources/nexus-deployment.yaml` and replace `RHT_OCP4_QUAY_USER` with your Quay username. Create the Kubernetes resources.
- Create a route for the Nexus service. Verify that you can access `http://nexus- ${RHT_OCP4_DEV_USER} -review.${RHT_OCP4_WILDCARD_DOMAIN}/nexus/` from workstation.

## Evaluation

After deploying the Nexus server container image to the OpenShift cluster, verify your work by running the lab grading script:

```
[student@workstation ~]$ lab comprehensive-review grade
```

## Finish

On workstation, run the `lab comprehensive-review finish` command to complete this lab.

```
[student@workstation ~]$ lab comprehensive-review finish
```

This concludes the lab.

## ► Solution

# Containerizing and Deploying a Software Application

In this review, you will containerize a Nexus server, build and test it using Podman, and deploy it to an OpenShift cluster.

## Outcomes

You should be able to:

- Write a Containerfile that successfully containerizes a Nexus server.
- Build a Nexus server container image and deploy it using Podman.
- Deploy the Nexus server container image to an OpenShift cluster.

## Before You Begin

Make sure you have completed *Guided Exercise: Configuring the Classroom Environment* from *Chapter 1* before executing any command of this practice.

Run the set-up script for this comprehensive review.

```
[student@workstation ~]$ lab comprehensive-review start
```

The lab files are located in the `~/D0180/labs/comprehensive-review` directory. The solution files are located in the `~/D0180/solutions/comprehensive-review` directory.

## Instructions

Use the following steps to create and test a containerized Nexus server both locally and in OpenShift:

1. Create a container image that starts an instance of a Nexus server:
  - The `~/D0180/labs/comprehensive-review/image` directory contains files for building the container image. Execute the `get-nexus-bundle.sh` script to retrieve the Nexus server files.
  - Write a Containerfile that containerizes the Nexus server. The Containerfile must be located in the `~/D0180/labs/comprehensive-review/image` directory. The Containerfile must also:
    - Use a base image of `ubi8/ubi:8.5` and set an arbitrary maintainer.
    - Set the ARG variable `NEXUS_VERSION` to `2.14.3-02`, and set the environment variable `NEXUS_HOME` to `/opt/nexus`.
    - Install the `java-1.8.0-openjdk-devel` package.

**Chapter 9 |** Comprehensive Review

- Run a command to create a **nexus** user and group. They both have a UID and GID of **1001**. Change the permissions of the  `${NEXUS_HOME} /`  directory to **775**.
- Unpack the `nexus-2.14.3-02-bundle.tar.gz` file to the  `${NEXUS_HOME} /`  directory. Add the `nexus-start.sh` to the same directory.  
Run a command, `ln -s ${NEXUS_HOME}/nexus-$NEXUS_VERSION ${NEXUS_HOME}/nexus2`, to create a symlink in the container. Run a command to recursively change the ownership of the Nexus home directory to `nexus:nexus`.
- Make the container run as the **nexus** user, and set the working directory to `/opt/nexus`.
- Define a volume mount point for the `/opt/nexus/sonatype-work` container directory. The Nexus server stores data in this directory.
- Set the default container command to `nexus-start.sh`.

There are two `*.snippet` files in the `~/D0180/labs/comprehensive-review/image` directory that provide the commands needed to create the **nexus** account and install Java. Use the files to assist you in writing the Containerfile.

- Build the container image with the name **nexus**.

1.1. Execute the `get-nexus-bundle.sh` script to retrieve the Nexus server files.

```
[student@workstation ~]$ cd ~/D0180/labs/comprehensive-review/image
[student@workstation image]$./get-nexus-bundle.sh
100.0%
Nexus bundle download successful
```

1.2. Write a Containerfile that containerizes the Nexus server. Go to the `~/D0180/labs/comprehensive-review/image` directory and create the Containerfile.

- Specify the base image to use:

```
FROM ubi8/ubi:8.5
```

- Enter an arbitrary name and email as the maintainer:

```
FROM ubi8/ubi:8.5
MAINTAINER username <username@example.com>
```

- Set a build argument for `NEXUS_VERSION` and an environment variable for `NEXUS_HOME`:

```
FROM ubi8/ubi:8.5
MAINTAINER username <username@example.com>

ARG NEXUS_VERSION=2.14.3-02
ENV NEXUS_HOME=/opt/nexus
```

- Install the `java-1.8.0-openjdk-devel` package using `yum` command.

```
FROM ubi8/ubi:8.5
MAINTAINER username <username@example.com>

ARG NEXUS_VERSION=2.14.3-02
ENV NEXUS_HOME=/opt/nexus

RUN yum install -y --setopt=tsflags=nodocs java-1.8.0-openjdk-devel && \
 yum clean all -y
```

- Create the server home directory and service account and group. Make home directory owned by the service account and change the permissions to 775.

```
RUN groupadd -r nexus -f -g 1001 && \
 useradd -u 1001 -r -g nexus -m -d ${NEXUS_HOME} -s /sbin/nologin \
 -c "Nexus User" nexus && \
 chown -R nexus:nexus ${NEXUS_HOME} && \
 chmod -R 755 ${NEXUS_HOME}
```

- Make the container run as the nexus user.

#### USER nexus

- Install the Nexus server software at NEXUS\_HOME and add the startup script. Note that the ADD directive will extract the Nexus files.

```
ADD nexus-${NEXUS_VERSION}-bundle.tar.gz ${NEXUS_HOME}
ADD nexus-start.sh ${NEXUS_HOME}/
```

- Create the nexus2 symbolic link pointing to the Nexus server directory. Recursively change the ownership of the \${NEXUS\_HOME} directory to nexus:nexus.

```
RUN ln -s ${NEXUS_HOME}/nexus-${NEXUS_VERSION} \
${NEXUS_HOME}/nexus2
```

- Make /opt/nexus the current working directory:

#### WORKDIR \${NEXUS\_HOME}

- Define a volume mount point to store the Nexus server persistent data:

```
VOLUME ["/opt/nexus/sonatype-work"]
```

- Set the CMD instruction to nexus-start.sh script file.

```
CMD ["sh", "nexus-start.sh"]
```

The completed Containerfile reads as follows:

```

FROM ubi8/ubi:8.5

MAINTAINER username <username@example.com>

ARG NEXUS_VERSION=2.14.3-02
ENV NEXUS_HOME=/opt/nexus

RUN yum install -y --setopt=tsflags=nodocs java-1.8.0-openjdk-devel \
 && yum clean all -y

RUN groupadd -r nexus -f -g 1001 && \
 useradd -u 1001 -r -g nexus -m -d ${NEXUS_HOME} -s /sbin/nologin \
 -c "Nexus User" nexus && \
 chown -R nexus:nexus ${NEXUS_HOME} && \
 chmod -R 755 ${NEXUS_HOME}

USER nexus

ADD nexus-${NEXUS_VERSION}-bundle.tar.gz ${NEXUS_HOME}
ADD nexus-start.sh ${NEXUS_HOME}/

RUN ln -s ${NEXUS_HOME}/nexus-${NEXUS_VERSION} ${NEXUS_HOME}/nexus2

WORKDIR ${NEXUS_HOME}

VOLUME ["/opt/nexus/sonatype-work"]

CMD ["sh", "nexus-start.sh"]

```

1.3. Build the container image with the name `nexus`.

```

[student@workstation image]$ podman build --layers=false -t nexus .
STEP 1: FROM ubi8/ubi:8.5
Getting image source signatures
...output omitted...
STEP 13: COMMIT ...output omitted...localhost/nexus:latest
...output omitted...

```

2. Build and test the container image using Podman with a volume mount:

- Use the script `~/D0180/labs/comprehensive-review/deploy/local/run-persistent.sh` to start a new container with a volume mount.
- Review the container logs to verify that the server is started and running.
- Test access to the container service using the URL: `http://127.0.0.1:18081/nexus`.
- Remove the test container.

2.1. Execute the `run-persistent.sh` script. Replace the container name as shown in the output of the `podman ps` command.

```
[student@workstation images]$ cd ~/DO180/labs/comprehensive-review
[student@workstation comprehensive-review]$ cd deploy/local
[student@workstation local]$./run-persistent.sh
80970007036bbb313d8eeb7621fada0ed3f0b4115529dc50da4dccef0da34533
```

2.2. Review the container logs to verify that the server is started and running.

```
[student@workstation local]$ podman ps \
> --format="{{.ID}} {{.Names}} {{.Image}}"
81f480f21d47 inspiring_poincare localhost/nexus:latest
[student@workstation local]$ podman logs inspiring_poincare | grep JettyServer
...output omitted...
... INFO [jetty-main-1] ...jetty.JettyServer - Running
... INFO [main] ...jetty.JettyServer - Started
```

2.3. Use the curl command to test the container using the URL:  
<http://127.0.0.1:18081/nexus>.

```
[student@workstation local]$ curl -v 127.0.0.1:18081/nexus/ 2>&1 | \
> grep -E 'HTTP|<title>'
> GET /nexus/ HTTP/1.1
< HTTP/1.1 200 OK
<title>Nexus Repository Manager</title>
```

2.4. Remove the test container.

```
[student@workstation local]$ podman rm -f inspiring_poincare
81f480f21d475af683b4b003ca6e002d37e6aaa581393d3f2f95a1a7b7eb768b
```

3. Deploy the Nexus server container image to the OpenShift cluster. You must:

- Tag the Nexus server container image as `quay.io/${RHT_OCP4_QUAY_USER}/nexus:latest`, and push it corresponding public repository on quay.io.
- Create an OpenShift project with a name of  `${RHT_OCP4_DEV_USER} -review`.
- Edit the `deploy/openshift/resources/nexus-deployment.yaml` and replace `RHT_OCP4_QUAY_USER` with your Quay username. Create the Kubernetes resources.
- Create a route for the Nexus service. Verify that you can access `http://nexus- ${RHT_OCP4_DEV_USER} -review.${RHT_OCP4_WILDCARD_DOMAIN}/nexus/` from workstation.

3.1. Log in to your Quay.io account.

```
[student@workstation local]$ podman login -u ${RHT_OCP4_QUAY_USER} quay.io
Password: your-quay-password
Login Succeeded!
```

3.2. Publish the Nexus server container image to your \quay.io registry.

```
[student@workstation local]$ podman push localhost/nexus:latest \
> quay.io/${RHT_OCP4_QUAY_USER}/nexus:latest
Getting image source signatures
...output omitted...
Writing manifest to image destination
Storing signatures
```

- 3.3. Repositories created by pushing images to quay.io are private by default. Refer to the **Repositories Visibility** section of the Quay appendix to read details about how change repository visibility.

- 3.4. Create the OpenShift project:

```
[student@workstation local]$ cd ~/DO180/labs/comprehensive-review/deploy/openshift
[student@workstation openshift]$ oc login -u ${RHT_OCP4_DEV_USER} \
> -p ${RHT_OCP4_DEV_PASSWORD} ${RHT_OCP4_MASTER_API}
Login successful.
...output omitted...
[student@workstation openshift]$ oc new-project ${RHT_OCP4_DEV_USER}-review
Now using project ...output omitted...
```

- 3.5. Replace RHT\_OCP4\_QUAY\_USER in the resources file with your Quay username and create the Kubernetes resources:

```
[student@workstation openshift]$ export RHT_OCP4_QUAY_USER
[student@workstation openshift]$ envsubst < resources/nexus-deployment.yaml | \
> oc create -f -
service/nexus created
persistentvolumeclaim/nexus created
deployment.apps/nexus created

[student@workstation openshift]$ oc get pods
NAME READY STATUS RESTARTS AGE
nexus-77c479bb4f-kscz7 0/1 ContainerCreating 0 11s
```

- 3.6. Expose the service by creating a route:

```
[student@workstation openshift]$ oc expose svc/nexus
route.route.openshift.io/nexus exposed.
[student@workstation openshift]$ oc get route -o yaml
apiVersion: v1
items:
- apiVersion: route.openshift.io/v1
 kind: Route
...output omitted...
 spec:
 host: nexus-${RHT_OCP4_DEV_USER}-review.${RHT_OCP4_WILDCARD_DOMAIN}
...output omitted...
```

- 3.7. Use a browser to connect to the Nexus server web application at [http://nexus-\\${RHT\\_OCP4\\_DEV\\_USER}-review.\\${RHT\\_OCP4\\_WILDCARD\\_DOMAIN}/nexus/](http://nexus-${RHT_OCP4_DEV_USER}-review.${RHT_OCP4_WILDCARD_DOMAIN}/nexus/).

## Evaluation

After deploying the Nexus server container image to the OpenShift cluster, verify your work by running the lab grading script:

```
[student@workstation ~]$ lab comprehensive-review grade
```

## Finish

On workstation, run the `lab comprehensive-review finish` command to complete this lab.

```
[student@workstation ~]$ lab comprehensive-review finish
```

This concludes the lab.



## Appendix A

# Implementing Microservices Architecture

### Goal

Refactor an application into microservices.

### Objectives

- Divide an application across multiple containers to separate distinct layers and services.

### Sections

- Implementing Microservices Architectures (with Guided Exercise)

# Implementing Microservices Architectures

---

## Objectives

After completing this section, you should be able to:

- Divide an application across multiple containers to separate distinct layers and services.
- Describe typical approaches to breaking up a monolithic application into multiple deployable units.
- Describe how to break the To Do List application into three containers matching its logical tiers.

## Benefits of Breaking Up a Monolithic Application into Containers

Traditional application development typically has many distinct functions packaged as a single deployment unit, or a monolithic application. Traditional development may also deploy supporting services, such as databases and other middleware services, on the same server as the application. While monolithic applications can still be deployed into a container, many of the advantages of a container architecture, such as scalability and agility, are not as prevalent. Breaking up monoliths requires careful consideration and it is recommended that in microservices applications each microservice runs the minimum functionality that can be executed in isolation on each container.

Having smaller containers and breaking up an application and its supporting services into multiple containers provides many advantages, such as:

- Higher hardware utilization, because smaller containers are easier to fit into available host capacity.
- Easier scaling, because parts of the application can be scaled to support an increased workload without scaling other parts of the application.
- Easier upgrades, because developers can update parts of the application without affecting other parts of the same application.

Two popular ways of breaking up an application are as follows:

- Tiers: based on architectural layers.
- Services: based on application functionality.

## Dividing Based on Layers (Tiers)

A common way developers organize applications is in tiers, based on how close the functions are to end users and how far from data stores. A good example of the traditional 3-tier architecture is presentation, business logic, and persistence.

This logical architecture usually corresponds to a physical deployment architecture, where the presentation layer would be deployed to a web server, the business layer to an application server, and the persistence layer to a database server.

Breaking up an application into tiers allows developers to specialize in particular technologies based on the application's tiers. For example, some developers focus on web applications, while others prefer database development. Another advantage is the ability to provide alternative tier implementations based on different technologies; for example, creating a mobile application as another front end for an existing application. The mobile application would be an alternative presentation tier, reusing the business and persistence tiers of the original web application.

Smaller applications usually have the presentation and business tiers deployed as a single unit. For example, to the same web server, but as the load increases, the presentation layer is moved to its own deployment unit to spread the load. Smaller applications might even embed the database. Developers often build and deploy more demanding applications in this monolithic fashion.

When developers break up a monolithic application into tiers, they usually apply several changes:

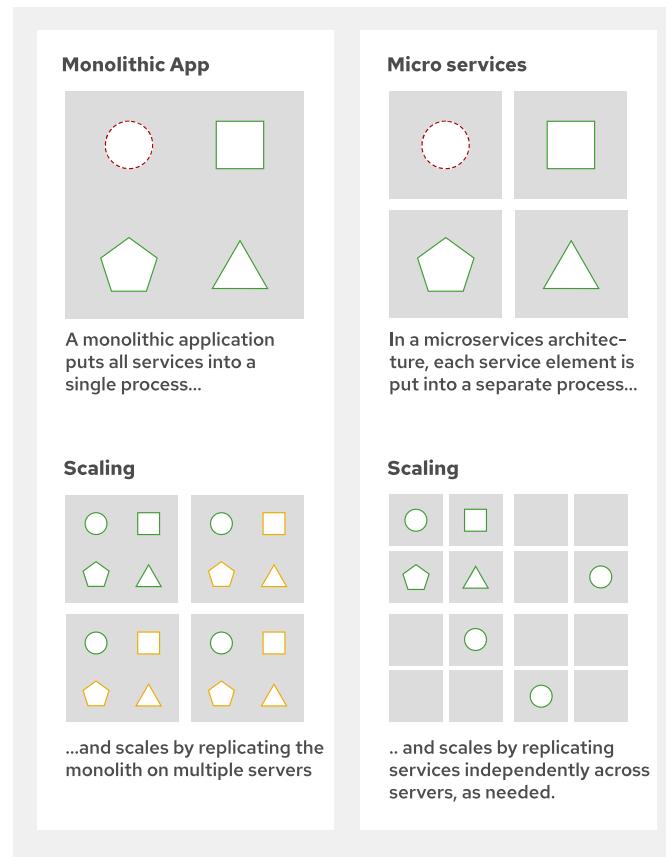
- Connection parameters to a database and other middleware services, such as messaging, were hard-coded to fixed IP addresses or host names, usually `localhost`. They need to be parameterized to point to external servers that might be different from development to production.
- In the case of web applications, Ajax calls cannot be made using relative URLs. They need to use an absolute URL pointing to a fixed public DNS host name.
- Modern web browsers refuse Ajax calls to servers different from the one containing the script that makes the call, as a security measure. The application needs to have permissions for cross-origin resource sharing (CORS).

After application tiers are divided so that they can run from different servers, there should be no problem running them from different containers.

## Dividing Based on Discrete Services

Most complex applications are composed of many semi-independent services. For example, an online store would have a product catalog, shopping cart, payment, shipping, and so on.

When a particular service in a monolithic application degrades, scaling the service to improve performance implies scaling all of the other constituent application services. If however the degraded service is part of a microservices architecture, the affected service is scaled independent of the other application services. The following figure illustrates service scaling for both a monolithic and microservices-based architecture:



**Figure A.1: Comparison of application scaling in a monolithic architecture versus a microservices architecture**



### Note

In the previous diagram:

- Red dashed line figures represent services that are overutilized.
- Yellow solid line figures represent services that are underutilized.
- Green solid line figures represent services that are correctly sized.

Both traditional service-oriented architectures (SOA) and more recent microservices architectures package and deploy those function sets as distinct units. This allows each function set to be developed by its own team, updated, and scaled without disturbing other function sets (or services). Cross-functional concerns such as authentication can also be packaged and deployed as services that are consumed by other service implementations.

Splitting each concern into a separated server might result in many applications. They are logically architected, packaged, and deployed as a small number of units, sometimes even as a single monolithic unit using a service approach.

Containers enable architectures based on services to be materialized during deployment. That is the reason microservices and containers usually come together. However, containers alone are not

enough; they need to be complemented by orchestration tools to manage dependencies among services.

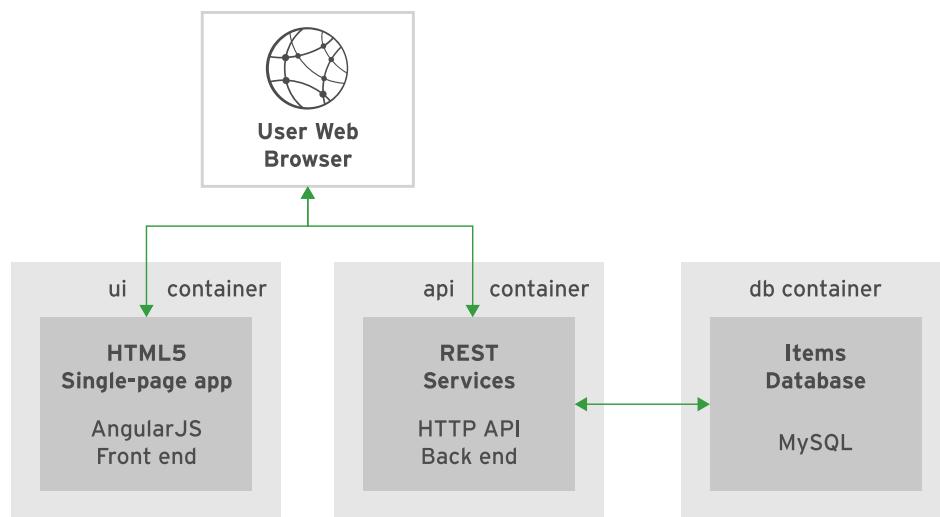
The microservices architecture takes service-based architectures to the extreme. A service is as small as it can be (without breaking a function set) and is deployed and managed as an independent unit, instead of part of a bigger application. This allows existing microservices to be reused to create new applications.

To break an application into services, it needs the same kind of change as when breaking into tiers; for example, parameterize connection parameters to databases and other middleware services and deal with web browser security protections.

## Refactoring the To Do List Application

The To Do List application is a simple application with a single function set, so breaking it up into services is not really meaningful. However, refactoring it into presentation and business tiers, that is, into a front end and a back end to deploy into distinct containers, illustrates the same kind of changes that breaking up a typical application into services would need.

The following figure shows the To Do List application deployed into three containers, one for each tier:



**Figure A.2: To Do List application broken into tiers and each deployed as containers**

Comparing the source code of the original monolithic application with the refactored one, this is an overview of the changes:

- The front-end JavaScript in `script/items.js` uses `workstation.lab.example.com` as the host name to reach the back end.
- The back end uses environment variables to get the database connection parameters.
- The back end has to reply to requests using the HTTP `OPTIONS` verb with headers telling the web browser to accept requests coming from different DNS domains using `CORS`.

Other versions of the back end service might have similar changes. Each programming language and REST framework have their own syntax and features.



## References

### **Monolithic application page in Wikipedia**

[https://en.wikipedia.org/wiki/Monolithic\\_application](https://en.wikipedia.org/wiki/Monolithic_application)

### **CORS page in Wikipedia**

[https://en.wikipedia.org/wiki/Cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing)

## ► Guided Exercise

# Refactoring the To Do List Application

In this lab, you will refactor the `To Do List` application into multiple containers that are linked together, allowing the front-end HTML 5 application, the Node.js REST API, and the MySQL server to run in their own containers.

## Outcomes

You should be able to refactor a monolithic application into its tiers and deploy each tier as a microservice.

## Before You Begin

Run the following command to set up the working directories for the lab with the `To Do List` application files:

```
[student@workstation ~]$ lab appendix-microservices start
```

## Instructions

### ► 1. Move the HTML Files

The first step in refactoring the `To Do List` application is to move the front-end code from the application into its own running container. This step guides you through moving the HTML application and its dependent files into their own directory for deployment to an Apache server running in a container.

- 1.1. Move the HTML and static files to the `src/` directory from the monolithic Node.js `To Do List` application:

```
[student@workstation ~]$ cd ~/D0180/labs/appendix-microservices/apps/html5/
[student@workstation html5]$ mv \
> ~/D0180/labs/appendix-microservices/apps/nodejs/todo/* \
> ~/D0180/labs/appendix-microservices/apps/html5/src/
```

- 1.2. The current front-end application interacts with the API service using a relative URL. Because the API and front-end code will now run in separate containers, the front-end needs to be adjusted to point to the absolute URL of the `To Do List` application API.

Open the `/home/student/D0180/labs/appendix-microservices/apps/html5/src/script/item.js` file. At the bottom of the file, look for the following method:

```
app.factory('itemService', function ($resource) {
 return $resource('api/items/:id');
});
```

Replace that code with the following content:

```
app.factory('itemService', function ($resource) {
 return $resource('http://workstation.lab.example.com:30080/todo/api/
 items/:id');
});
```

Make sure there are no line breaks in the new URL, save the file, and exit the editor.

## ► 2. Build the HTML Image

- 2.1. Login to the Red Hat Container Catalog with your Red Hat account.

```
[student@workstation html5]$ podman login registry.redhat.io
Username: your_username
Password: your_password
Login Succeeded!
```

- 2.2. Build the child Apache image:

```
[student@workstation html5]$ cd ~/D0180/labs/appendix-microservices/deploy/html5
[student@workstation html5]$./build.sh
STEP 1: FROM registry.redhat.io/rhel8/httpd-24:1
Getting image source signatures
Copying blob 1b6a9fa02570 done
...output omitted...
Storing signatures
STEP 2: COPY ./src/ ${HOME}/
STEP 3: COMMIT do180/todo_frontend
dda10a4bf12ff987331e482e5cd87658abc5724da4b5b7d136874a9e471acf71
```

- 2.3. Verify that the image is built correctly:

```
[student@workstation html5]$ podman images
REPOSITORY TAG IMAGE ID CREATED
SIZE
localhost/do180/todo_frontend latest dda10a4bf12f About a minute ago
438 MB
registry.redhat.io/rhel8/httpd-24 1 adcf72f31a0b 13 days ago
438 MB
...
```

## ► 3. Modify the REST API to Connect to External Containers

- 3.1. The REST API currently uses hard-coded values to connect to the MySQL database. Edit the /home/student/D0180/labs/appendix-microservices/apps/nodejs/models/db.js file, which holds the database configuration. Update the dbname, username, and password values to use environment variables instead. Also, update the params.host to point to the host name of the host running the MySQL container and update the params.port to reflect the redirected port to the container. Both values are available as the MYSQL\_SERVICE\_HOST and MYSQL\_SERVICE\_PORT environment variables, respectively. Replaced contents should look like this:

```
module.exports.params = {
 dbname: process.env.MYSQL_DATABASE,
 username: process.env.MYSQL_USER,
 password: process.env.MYSQL_PASSWORD,
 params: {
 host: process.env.MYSQL_SERVICE_HOST,
 port: process.env.MYSQL_SERVICE_PORT,
 dialect: 'mysql'
 }
};
```

**Note**

This file can be copied and pasted from `/home/student/D0180/solutions/appendix-microservices/apps/nodejs/models/db.js`.

- 3.2. Configure the back end to handle Cross-origin resource sharing (CORS). This occurs when a resource request is made from a different domain from the one in which the request was made. Because the API needs to handle requests from a different DNS domain (the front-end application), it is necessary to create security exceptions to allow these requests to succeed. Make the following modifications to the application in the editor of your preference in order to handle CORS.

Add `"restify-cors-middleware": "1.1.1"` as a new dependency to the `package.json` file located at `/home/student/D0180/labs/appendix-microservices/apps/nodejs/package.json`. Remember to put a comma at the end of the previous dependency. Make sure the end of the file looks like this:

```
"sequelize": "5.21.1",
"mysql2": "2.0.0",
"restify-cors-middleware": "1.1.1"
}
```

Update the `app.js` file located at `/home/student/D0180/labs/appendix-microservices/apps/nodejs/app.js` to configure CORS usage. Require the `restify-cors-middleware` module at the second line, and then update the contents of the file to match the following:

```
var restify = require('restify');
var corsMiddleware = require('restify-cors-middleware');
var controller = require('./controllers/items');
...output omitted...
var server = restify.createServer()
 .use(restify.plugins.fullResponse())
 .use(restify.plugins.queryParser())
 .use(restify.plugins.bodyParser());

const cors = corsMiddleware({ origins: ['*'] });

server.pre(cors.preflight);
```

**Appendix A |** Implementing Microservices Architecture

```
server.use(cors.actual);

controller.context(server, '/todo/api', model);
```

The origins with value `[ "*" ]` instructs the server to allow any domains. In a production server, this value would usually be an array of domains known to require access to the API.

**► 4. Build the REST API Image**

- 4.1. Build the REST API child image using the following command. This image uses the Node.js image.

```
[student@workstation html5]$ cd ~/DO180/labs/appendix-microservices/deploy/nodejs
[student@workstation nodejs]$./build.sh
STEP 1: FROM quay.io/redhattraining/do180-todonodejs-12
Getting image source signatures
...output omitted...
STEP 6: CMD ["/bin/bash", "-c", "./run.sh"]
STEP 7: COMMIT do180/todonodejs
18f8d5dd8e25ed19a54750c8b96ae075adf437f5f0ba5ebbfcc7b9fe4b75526b3
```

- 4.2. Run the `podman images` command to verify that all of the required images are built successfully:

```
[student@workstation nodejs]$ podman images
REPOSITORY TAG IMAGE ID CREATED
SIZE
localhost/do180/todonodejs latest 18f8d5dd8e25 About a
minute ago 852 MB
localhost/do180/todo_frontend latest dda10a4bf12f 10 minutes
ago 438 MB
...output omitted...
```

**► 5. Run the Containers**

- 5.1. Use the `run.sh` script to run the containers:

```
[student@workstation nodejs]$ cd linked/
[student@workstation linked]$./run.sh
• Creating database volume: OK
• Launching database: OK
• Importing database: OK
• Launching To Do application: OK
```

- 5.2. Run the `podman ps` command to confirm that all three containers are running:

```
[student@workstation linked]$ podman ps
... IMAGE ... PORTS NAMES
... localhost/do180/todo_frontend:latest ... 0.0.0.0:30000->80/tcp todo_frontend
... localhost/do180/todonodejs:latest ... 0.0.0.0:30080->30080/tcp todoapi
... registry.redhat.io/rhel8/mysql-80:1 ... 0.0.0.0:30306->3306/tcp mysql
```

► **6. Test the Application**

- 6.1. Use the `curl` command to verify that the REST API for the To Do List application is working correctly:

```
[student@workstation linked]$ curl -w "\n" 127.0.0.1:30080/todo/api/items/1
>{"description": "Pick up newspaper", "done": false, "id":1}
```

- 6.2. Open Firefox on the workstation machine and navigate to 127.0.0.1:30000, where you should see the To Do List application.
- 6.3. Change back to the user's home folder.

```
[student@workstation linked]$ cd ~
[student@workstation ~]$
```

## Finish

On `workstation`, run the `lab appendix-microservices finish` script to complete this lab.

```
[student@workstation ~]$ lab appendix-microservices finish
```

This concludes the guided exercise.

# Summary

---

In this chapter, you learned:

- Breaking a monolithic application into multiple containers allows for greater application scalability, makes upgrades easier, and allows higher hardware utilization.
- The three common tiers for logical division of an application are the presentation tier, the business tier, and the persistence tier.
- Cross-Origin Resource Sharing (CORS) can prevent Ajax calls to servers different from the one where the pages were downloaded. Be sure to make provisions to allow CORS from other containers in the application.
- Container images are intended to be immutable, but configurations can be passed in either at image build time or by creating persistent storage for configurations.

## Appendix B

# Creating a GitHub Account

### Goal

Describe how to create a GitHub account for labs in the course.

# Creating a GitHub Account

## Objectives

After completing this section, you should be able to create a GitHub account and create public Git repositories for the labs in the course.

## Creating a GitHub Account

You need a GitHub account to create one or more *public* git repositories for the labs in this course. If you already have a GitHub account, you can skip the steps listed in this appendix.



### Important

If you already have a GitHub account, ensure that you only create *public* git repositories for the labs in this course. The lab grading scripts and instructions require unauthenticated access to clone the repository. The repositories must be accessible without providing passwords, SSH keys, or GPG keys.

To create a new GitHub account, perform the following steps:

1. Navigate to <https://github.com> using a web browser.
2. Enter the required details and then click **Create account**.

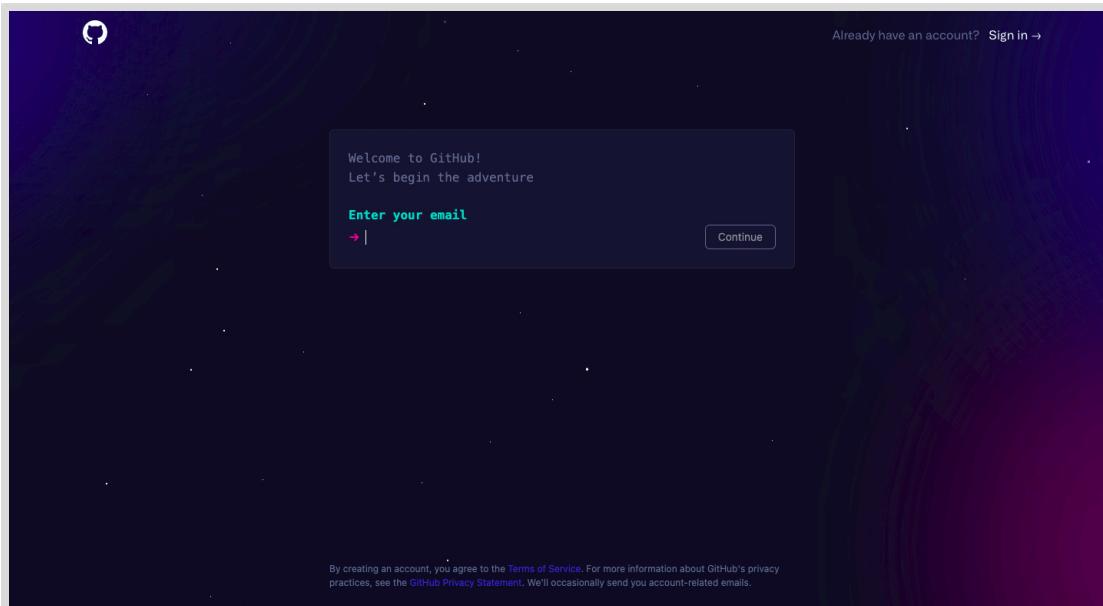
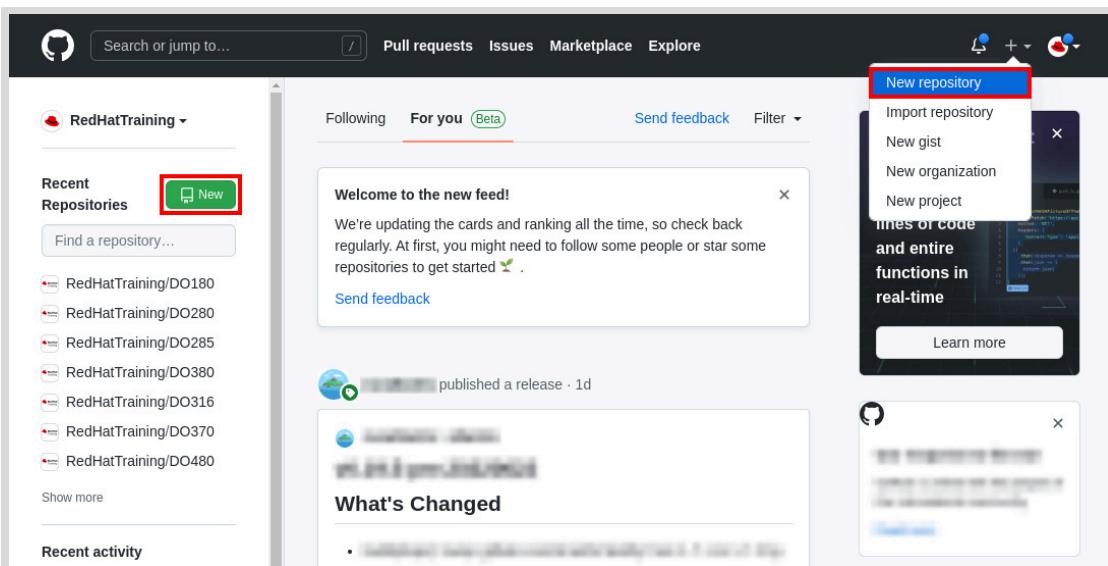


Figure B.1: Creating a GitHub account

3. You will receive an email with instructions on how to activate your GitHub account. Verify your email address and then sign in to the GitHub website using the username and password you provided during account creation.

4. After you have logged in to GitHub, you can create new Git repositories by clicking **New** in the **Repositories** pane on the left of the GitHub home page.



**Figure B.2: Creating a new Git repository**

Alternatively, click the plus icon (+) in the upper-right corner (to the right of the bell icon) and then click **New repository**.

## References

### **Signing up for a new GitHub account**

<https://docs.github.com/en/get-started/signing-up-for-github/signing-up-for-a-new-github-account>

### **Creating a new repository**

<https://docs.github.com/en/repositories/creating-and-managing-repositories/creating-a-new-repository>



## Appendix C

# Creating a Quay Account

### Goal

Describe how to create a Quay account for labs in the course.

# Creating a Quay Account

## Objectives

After completing this section, you should be able to create a Quay account and create public container image repositories for the labs in the course.

## Creating a Quay Account

You need a Quay account to create one or more *public* container image repositories for the labs in this course. If you already have a Quay account, you can skip the steps to create a new account listed in this appendix.



### Important

If you already have a Quay account, ensure that you only create *public* container image repositories for the labs in this course. The lab grading scripts and instructions require unauthenticated access to pull container images from the repository.

To create a new Quay account, perform the following steps:

1. Navigate to <https://quay.io> using a web browser.
2. Click **Sign in** in the upper-right corner (next to the search bar).
3. On the **Sign in** page, you can log in using your Red Hat credentials (created in *Appendix D, Creating a Red Hat Account*).

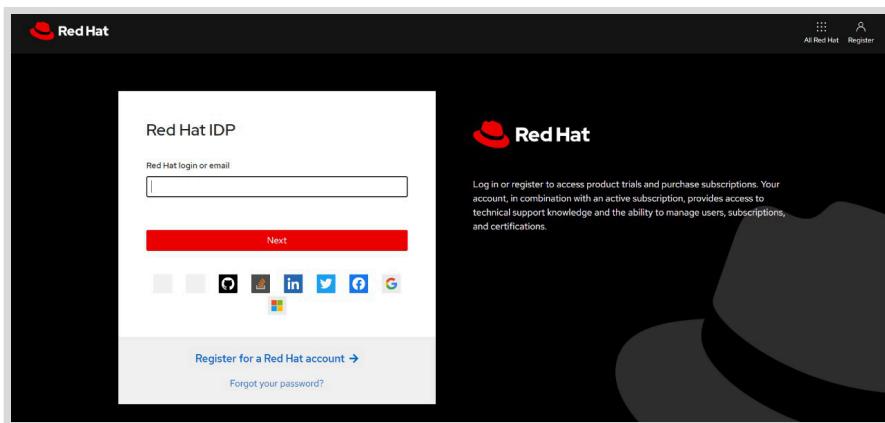
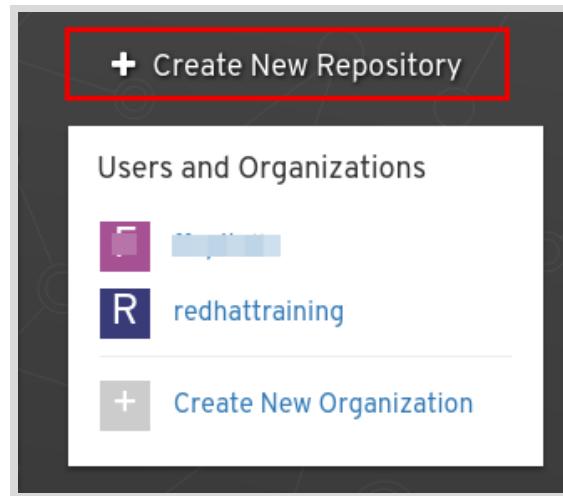


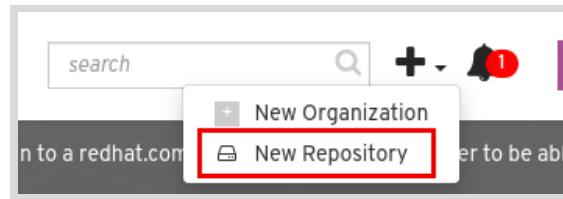
Figure C.1: Sign in using Red Hat credentials.

After you have logged in to Quay you can create new image repositories by clicking **Create New Repository** on the **Repositories** page.



**Figure C.2: Creating a new image repository**

Alternatively, click the plus icon (+) in the upper-right corner (to the left of the bell icon), and then click **New Repository**.



**Figure C.3: Creating a new image repository**

## Working with CLI tools

If you created your account with Red Hat, Google or Github, you need to set an account password to use CLI tools like Podman or Docker.

1. Click <YOUR\_USERNAME> in the upper-right corner.
2. Click **Account Settings**.
3. Click **User Settings** on the left column.
4. Click the **Set password** link.

 **References**

**Getting Started with Quay.io**  
<https://docs.quay.io/solution/getting-started.html>

# Repository Visibility

## Objectives

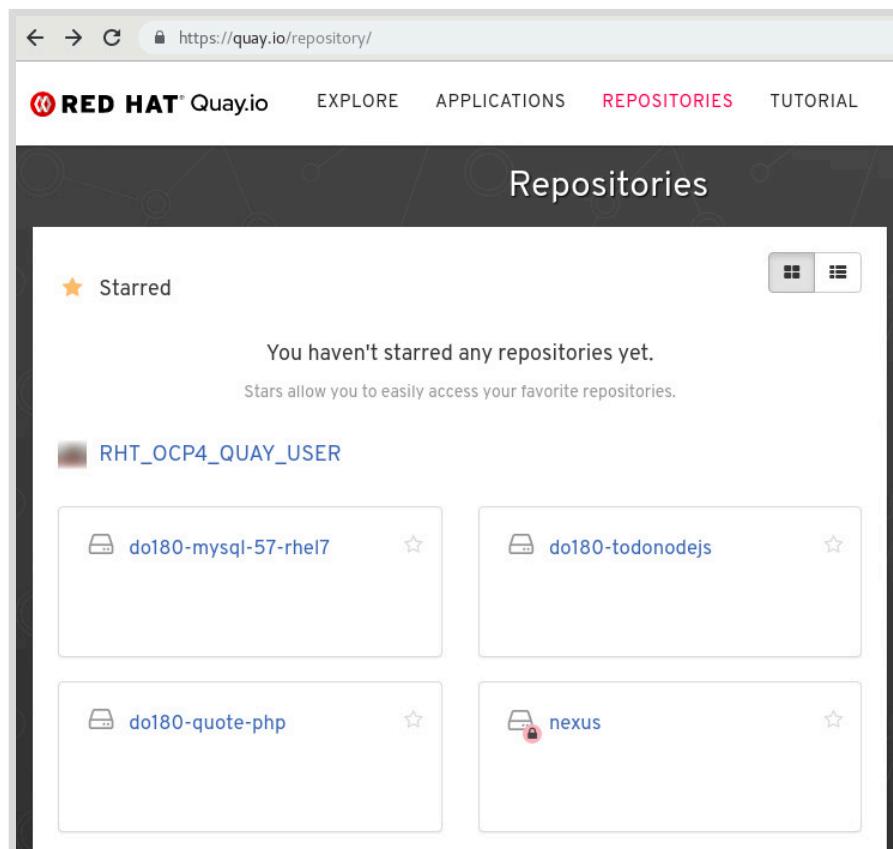
After completing this section, you should be able to control repository visibility on Quay.io.

## Quay.io Repository Visibility

Quay.io offers the possibility of creating public and private repositories. Public repositories can be read by anyone without restrictions, despite write permissions must be explicitly granted. Private repositories have both read and write permissions restricted. Nevertheless, the number of private repositories in quay.io is limited, depending on the namespace plan.

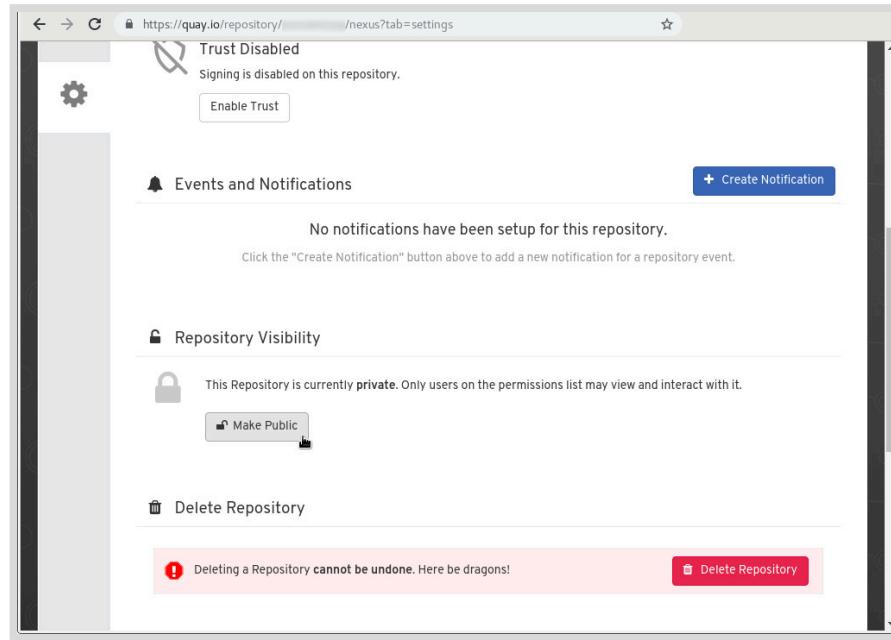
## Default Repository Visibility

Repositories created by pushing images to quay.io are private by default. In order OpenShift (or any other tool) to fetch those images you can either configure a private key in both OpenShift and Quay, or make the repository public, so no authentication is required. Setting up private keys is out of scope of this document.



## Updating Repository Visibility

In order to set repository visibility to public select the appropriate repository in <https://quay.io/repository/> (log in to your account if needed) and open the **Settings** page by clicking on the gear icon on the bottom left. Scroll down to the **Repository Visibility** section and click the **Make Public** button.



Get back to the list of repositories. The lock icon besides the repository name have disappeared, indicating the repository became public.



## Appendix D

# Creating a Red Hat Account

### Goal

Describe how to create a Red Hat account for labs in the course.

# Creating a Red Hat Account

## Objectives

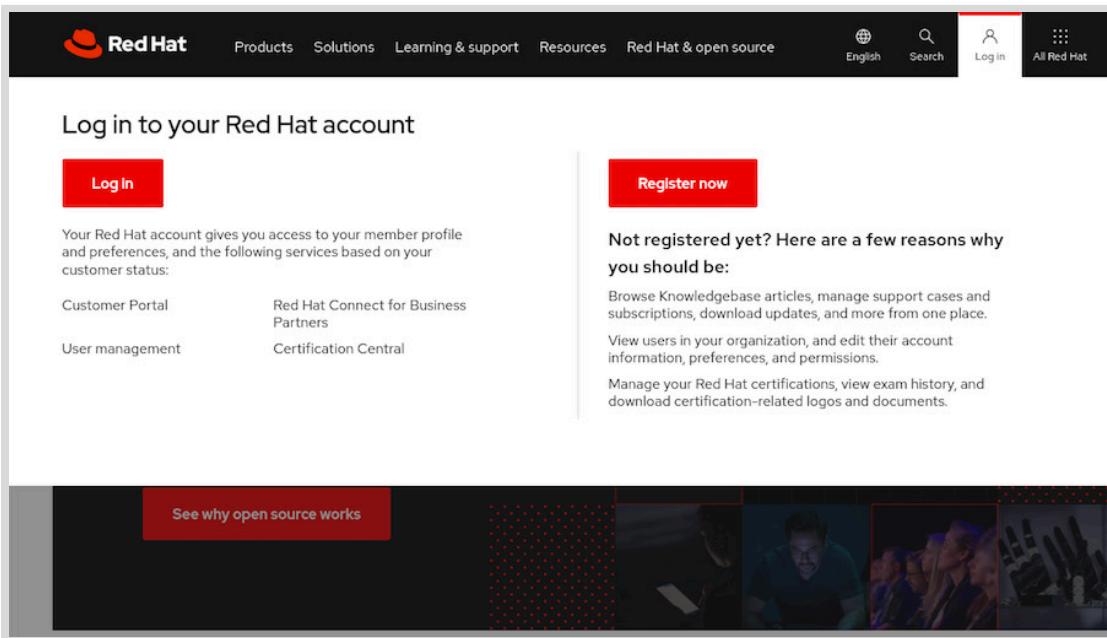
After completing this section, you should be able to create a Red Hat account to access the Red Hat Container Catalog images for the labs in the course.

### Creating a Red Hat Account

You need a Red Hat account to access the Red Hat Container Catalog images. If you already have a Red Hat account, you can skip this steps.

To create a new Red Hat account, perform the following steps:

1. Navigate to <https://redhat.com> using a web browser.
2. Click **Log in** in the upper-right corner.
3. Click **Register now** on the right side pane.



**Figure D.1: Register a new account**

4. Set Account type as Personal.

The screenshot shows the 'Create a Red Hat account' page. At the top is the Red Hat logo. Below it is the heading 'Create a Red Hat account'. A sub-instruction says 'Sign up and use this Red Hat account to access all of Red Hat's applications, communities, support, and more.' A note below states: 'Red Hat will collect your contact and account information to create your Red Hat account. We use your personal data to identify you and to provide you with information, support, and customer service. For more information, please see Red Hat's [privacy statement](#)'. A section titled 'Join an existing account' provides instructions on how to access company subscriptions by joining an existing account or contacting customer service. A note at the bottom right indicates '\* Required fields'.

**Account type**  
Choose account type \*  
 Corporate  
A corporate Red Hat account allows a set of users within your organization to centrally make purchases or administer systems.  
 Personal  
A personal Red Hat account is for purchasing or administering your own personal systems.

**Figure D.2: Set account type**

5. Fill in the remainder of the form with your personal information. In this form you also select the username and password for this account.
6. Click **CREATE MY ACCOUNT**.

The screenshot shows the 'Fill in personal information' step of the account creation process. It features two input fields: 'City \*' with a placeholder 'Enter city' and 'State/Province \*' with a placeholder 'Enter state/province'. Below these is a large red button labeled 'CREATE MY ACCOUNT'. At the bottom left is a link '« Back to login page'.

**Figure D.3: Fill in personal information form**



## References

### Red Hat Customer Portal

<https://access.redhat.com/>



## Appendix E

# Useful Git Commands

### Goal

Describe useful Git commands that are used for the labs in this course.

# Git Commands

## Objectives

After completing this section, you should be able to restart and redo exercises in this course. You should also be able to switch from one incomplete exercise to perform another, and later continue the previous exercise where you left off.

## Working with Git Branches

This course uses a Git repository hosted on GitHub to store the application course code source code. At the beginning of the course, you create your own fork of this repository, which is also hosted on GitHub.

During this course, you work with a local copy of your fork, which you clone to the **workstation** VM. The term **origin** refers to the remote repository from which a local repository is cloned.

As you work through the exercises in the course, you use separate Git branches for each exercise. All changes you make to the source code happen in a new branch that you create only for that exercise. Never make any changes on the **master** branch.

A list of scenarios and the corresponding Git commands that you can use to work with branches, and to recover to a known good state are listed below.

## Redoing an Exercise from Scratch

To redo an exercise from scratch after you have completed it, perform the following steps:

1. You commit and push all the changes in your local branch as part of performing the exercise. You finished the exercise by running its **finish** subcommand to clean up all resources:

```
[student@workstation ~]$ lab your-exercise finish
...output omitted...
```

2. Change to your local clone of the D0180-apps repository and switch to the **master** branch:

```
[student@workstation ~]$ cd ~/D0180-apps

[student@workstation D0180-apps]$ git checkout master
...output omitted...
```

3. Delete your local branch:

```
[student@workstation D0180-apps]$ git branch -d your-branch
...output omitted...
```

4. Delete the remote branch on your personal GitHub account:

## Appendix E | Useful Git Commands

```
[student@workstation D0180-apps]$ git push origin --delete your-branch
...output omitted...
```

5. Use the `start` subcommand to restart the exercise:

```
[student@workstation D0180-apps]$ cd ~
[student@workstation ~]$ lab your-exercise start
...output omitted...
```

## Abandoning a Partially Completed Exercise and Restarting it from Scratch

You may run into a scenario where you have partially completed a few steps in the exercise, and you want to abandon the current attempt, and restart it from scratch. Perform the following steps:

1. Run the exercise's `finish` subcommand to clean up all resources.

```
[student@workstation ~]$ lab your-exercise finish
...output omitted...
```

2. Enter your local clone of the D0180-apps repository and discard any pending changes on the current branch using `git stash`:

```
[student@workstation ~]$ cd ~/D0180-apps
[student@workstation D0180-apps]$ git stash
...output omitted...
```

3. Switch to the `master` branch of your local repository:

```
[student@workstation D0180-apps]$ git checkout master
...output omitted...
```

4. Delete your local branch:

```
[student@workstation D0180-apps]$ git branch -d your-branch
...output omitted...
```

5. Delete the remote branch on your personal GitHub account:

```
[student@workstation D0180-apps]$ git push origin --delete your-branch
...output omitted...
```

6. You can now restart the exercise by running its `start` subcommand:

```
[student@workstation D0180-apps]$ cd ~
[student@workstation ~]$ lab your-exercise start
...output omitted...
```

## Switching to a Different Exercise from an Incomplete Exercise

You may run into a scenario where you have partially completed a few steps in an exercise, but you want to switch to a different exercise, and revisit the current exercise at a later time.

Avoid leaving too many exercises uncompleted to revisit late. These exercises tie up cloud resources and you may use up your allotted quota on the cloud provider and on the OpenShift cluster you share with other student. If you think it may be a while until you can go back to the current exercise, consider abandoning it and later restarting from scratch.

If you prefer to pause the current exercise and work on the next one, perform the following steps:

1. Commit any pending changes in your local repository and push them to your personal GitHub account. You may want to record the step where you stopped the exercise:

```
[student@workstation ~]$ cd ~/D0180-apps

[student@workstation D0180-apps]$ git commit -a -m "Paused at step X.Y"
...output omitted...
[student@workstation D0180-apps]$ git push
...output omitted...
```

2. Do not run the `finish` command of the original exercise. This is important to leave your existing OpenShift projects unchanged, so you can resume later.
3. Start the next exercise by running its `start` subcommand:

```
[student@workstation ~]$ lab your-exercise start
...output omitted...
```

4. The next exercise switches to the `master` branch and optionally creates a new branch for its change. This means the changes made to the original exercise in the original branch are left untouched.
5. Later, after you have completed the next exercise, and you want to go back to the original exercise, switch back to its branch:

```
[student@workstation ~]$ git checkout original-branch
...output omitted...
```

Then you can continue with the original exercise at the step where you left off.



### References

#### Git branch man page

<https://git-scm.com/docs/git-branch>

#### What is a Git branch?

<https://git-scm.com/book/en/v2/Git-Branching-Branches-in-a-Nutshell>

#### Git Tools - Stashing

<https://git-scm.com/book/en/v2/Git-Tools-Stashing-and-Cleaning>