



Architecting and Operating OpenShift Clusters: OpenShift for Infrastructure and O..



PREV

Cover



AA



NEXT



hift Archite...

William Caban

Architecting and Operating OpenShift Clusters

OpenShift for Infrastructure and Operations Teams

William Caban
Columbia, MD, USA

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484249840 (<http://www.apress.com/9781484249840>). For more detailed information, please visit <http://www.apress.com/source-code> (<http://www.apress.com/source-code>).

ISBN 978-1-4842-4984-0 e-ISBN 978-1-4842-4985-7
<https://doi.org/10.1007/978-1-4842-4985-7>

© William Caban 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark. The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

To my wife, Maria, who has always supported my constantly traveling job and my urge to drive technical excellence. You are, and always will be, my perfect wife and the supermom to our wonderful children.

To my son Seth and to my daughter Juliette for their patience with the many days and weekends I had to unplug from everything to stay home writing. Thank you for your understanding and support. You two are the greatest son and the greatest daughter a father can have.

To my parents, Willie and Annie, without whom none of my success would be possible.

Introduction

The rapid evolution of the Kubernetes platform and the ecosystem around it represents an excellent opportunity to drive modernization inside an organization while defining new operational paradigms.

This book is for the architects and operations teams of those organizations using OpenShift as one of their tools in their transformation. This is for the organization's hidden heroes that need to have a good understanding of how different elements interact in such a platform to be able to optimize it for their organization's specific workloads. This is not a book listing all the existing commands for every possible option, but a book explaining how the platform comes together to understand the possible locations in features into where to apply fine-tunings for their optimization.

Acknowledgments

This book is the result of my quest to find a way to provide additional technical information about *OpenShift Container Platform (OCP)* and *OKD* to answer the type of questions I see from the operations teams in our customers today. The same questions my former self had many years ago when I started migrating from upstream Kubernetes into a supported Kubernetes distribution.

This book has been possible thanks to the support from a brilliant Red Hat OpenShift-SME community, the Red Hat OpenShift Business Unit, and each one of the product managers and their teams which are the ones that make the OpenShift magic happen. From these, I would like to give a special thank you to Marc Curry, Ben Breard, Brian Harrington, Paul Morie, and William Oliveira. Thank you for the times you took to reply an e-mail or hop in a call to answer my many questions trying to understand the behind-the-scenes plumbing of the many features.

Also, some of the information in this book has been possible thanks to the extended community from which I would like to give a special thank you to Salah Chaou and Alpika Singh (DriveScale Inc.), Christopher Kurka (HPE), and Bin Zhou (Lenovo).

TABLE OF CONTENTS

Chapter 1: The OpenShift Architecture

Linux Containers

Linux Container: Under the Hood

Container Specifications

Container Runtime and Kubernetes

Introduction to OpenShift Architecture Components

Kubernetes Constructs

OpenShift Constructs

Master Nodes

Infrastructure Nodes

App Nodes

OpenShift Consoles

OpenShift Routers

OpenShift Registry

Summary

Chapter 2: High Availability

Control Plane and Data Plane

HA for Control Plane

HA for ETCD

HA for Master Services

HA for OpenShift Consoles

HA for Logging, Metrics, and Monitoring

HA for Data Plane

HA for OpenShift Router

HA for Container Registry

Summary

Chapter 3: Networking

[East-West Traffic](#)

[OpenShift SDN](#)

[Flannel](#)

[OpenShift with Third-Party SDN](#)

[North-South Traffic](#)

[HAProxy Template Router](#)

[Summary](#)

[Chapter 4: Storage](#)

[OpenShift Storage](#)

[Kubernetes Storage Constructs](#)

[PersistentVolume Status](#)

[Reclaim Policy](#)

[Access Modes](#)

[OpenShift PersistentVolume Plugins](#)

[FlexVolume](#)

[With Master-Initiated Attach/Detach](#)

[Without Master-Initiated Attach/Detach](#)

[CSI](#)

[OpenShift Ephemeral](#)

[OpenShift Container Storage](#)

[OCS Converged Mode](#)

[OCS Independent Mode](#)

[OCS Storage Provisioning](#)

[Storage Classes](#)

[OpenShift with Third-Party Storage](#)

[DriveScale Composable Platform](#)

[HPE 3PAR](#)

[HPE Nimble](#)

[NetApp Trident](#)

[OpenEBS \(OSS, MayaData\)](#)

[Summary](#)

[Chapter 5: Load Balancers](#)

[Load Balancer Overview](#)

[Load Balancer Considerations](#)

[Considerations for Master Nodes](#)

[Considerations for Infrastructure Nodes](#)

[Considerations for Specialized Protocols](#)

[Summary](#)

[Chapter 6: Deployment Architectures](#)

[Minishift](#)

[OCP 3.11 Deployment Architectures](#)

[Prerequisites](#)

[Activate and Assign OpenShift Subscriptions](#)

[Prepare OCP 3.11.x Installer on Bastion](#)

[Enable Password-less SSH](#)

[OpenShift Ansible Inventory File](#)

[Sample Deployment Scenarios](#)

[Single Node Deployment \(All-in-One\)](#)

[Non-HA Control Plane Deployment](#)

[Full-HA Control Plane Deployment](#)

[Deploying OpenShift](#)

[Uninstalling OpenShift](#)

[Bastion Node as Admin Jumphost](#)

[OpenShift 4.x Deployments \(AWS\)](#)

[Prerequisites](#)

[OpenShift 4.x Deployment Architecture](#)

[OCP4 Deployment to AWS \(IPI Mode\)](#)

[Installing OCP4 on AWS](#)

[Deployment Progress](#)

[Configuring the Identity Provider](#)

[Summary](#)

[Chapter 7: Administration](#)

[User and Groups](#)

[Virtual Groups and Virtual Users](#)

[Authentication, Authorization, and OpenShift RBAC](#)

[RBAC](#)

[Default Cluster Roles](#)

[Security Context Constraints](#)

[SECCOMP Profiles](#)

[Enabling Unsafe SYSCTL](#)

[Identity Providers](#)

[Managing Users and Groups](#)

[Using Service Accounts](#)

[Quotas and Limit Ranges](#)

[OpenShift Service Catalogs](#)

[OpenShift Templates](#)

[Summary](#)

[Chapter 8: Architecting OpenShift Jenkins Pipelines](#)

[CI/CD Pipelines As a Service with OpenShift](#)

[Jenkins Pipeline Build Strategy](#)

[Creating the Pipeline BuildConfig](#)

[Deploying the Pipeline BuildConfig](#)

[Jenkinsfile with Source Code](#)

[Multiproject Pipelines](#)

[OpenShift Client Plugin](#)

[Custom Jenkins Images](#)

[Integrating External CI/CD Pipelines](#)

[Summary](#)

[Chapter 9: Day-2 Operations](#)

[Managing Leftover Objects](#)

[Garbage Collection](#)

[Node Optimizations](#)

[Node Resource Allocation](#)

[Setting Max Pods Per Node](#)

[Using the Tuned Profile](#)

[Eviction Policy](#)

[Pod Scheduling](#)

[Pod Priority](#)

[Summary](#)

[Chapter 10: Advanced Network Operations](#)

[Network Optimizations](#)

[Jumbo Frames and VXLAN Acceleration](#)

[Tuning Network Devices](#)

[Routing Optimizations](#)

[Route-Specific Optimizations Annotations](#)

[IP Whitelists](#)

[OpenShift Router Sharding](#)

[Supporting Non-HTTP/HTTPS/TLS Applications](#)

[Using IngressIP and ExternalIP](#)

[Using NodePorts and HostPorts](#)

[Multiple NIC per POD](#)

[OpenShift ServiceMesh](#)

[Summary](#)

[Chapter 11: OCP 4.1 UPI Mode Bare-Metal with PXE Boot Deployment](#)

[UPI Mode](#)

[Bare-Metal with PXE Boot Example](#)

[UPI Bare-Metal with PXE Boot](#)

[Prerequisites](#)

[Preparing the Installation](#)

[Considerations with UPI Mode with PXE Boot](#)

[Downloading RHCOS and Installation Binaries](#)

[Preparing the PXE Boot Images](#)

[Installation](#)

[Creating the Configuration](#)

[Generating the Ignition Files](#)

[Bootstrap and Master Nodes](#)

[Worker Nodes](#)

[Summary](#)

[Index](#)

ABOUT THE AUTHOR AND ABOUT THE TECHNICAL REVIEWER

ABOUT THE AUTHOR

William Caban

has more than 25 years of experience in IT and has been consulting and designing large-scale datacenter solutions in multiple vertical markets. He has worked for diverse customers ranging from financial institutions, healthcare institutions, and service providers. His personal motto is “Changing the world one ‘bit’ at a time.” He has written several courses and training guides in the past. This is his first book with Apress.



ABOUT THE TECHNICAL REVIEWER

James Cryer

is a Lead Principal Engineer with over 8 years of experience working with Cloud-native solutions on AWS, GCP, and Azure. James has a passion for architecting and developing highly available, fault-tolerant, and secure systems. James’ experience is broad; he has worked in a variety of sectors with companies such as the BBC, Investec Asset Management, and, more recently, Sophos. When away from his laptop, James loves to travel with his wife and child, get outdoors, and read.



[Browse](#) / [Resource Centers](#) / [Playlists](#) / [History](#) / [Topics](#) /

◀ PREV
[Cover](#)

NEXT ▶
[1. The OpenShift Archite...](#)