Brought to you by:

Red Hat

Managing Your Kubernetes Clusters

for dummies®
A Wiley Brand

Understand multi cluster management challenges

Learn keys to manage Kubernetes clusters

Leverage best practices

Lawrence C. Miller

Red Hat Special Edition

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications; develop cloud-native applications; standardize on its industry-leading operating system; and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future. Learn more at **www.redhat.com.**

Learn more about Red Hat Advanced Cluster Management for Kubernetes. Visit **www.redhat.com/clustermanagement** for details on cluster management products along with the key use cases.

Managing Your Kubernetes Clusters

Red Hat Special Edition

by Lawrence C. Miller

for dummies®
A Wiley Brand

Managing Your Kubernetes Clusters For Dummies®, Red Hat Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-76761-9 (pbk); ISBN: 978-1-119-76762-6 (ebk) Some blank pages in the print version may not be included in the ePDF version.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Manager: Carrie Burchfield-Leighton

Executive Editor: Steve Hayes

Sr. Manager Editor: Rev Mengle

Business Development Representative: Molly Daugherty

Production Editor: Tamilmani Varadharaj

Table of Contents

Introduction

IT infrastructure isn't static. Technology advancements and business demands have pushed IT departments to embrace hybrid environments comprised of virtualized workloads, private and public clouds, container-based applications, and Kubernetes clusters. As the platforms have changed, so too have the requirements for IT operations. Now more than ever, managing IT operations means

- Focusing on enabling services rather than managing systems
- Establishing trusted processes to ensure compliance and meeting service levels rather than controlling everything
- Automating the infrastructure to deliver greater responsiveness

To successfully address these challenges, IT departments need a unified management solution that provides a consistent cross-platform experience and enables enterprises to accelerate service delivery while maintaining complete operational and life cycle management.

About This Book

Managing Your Kubernetes Clusters For Dummies, Red Hat Special Edition, consists of four chapters that explore

- The growth of Kubernetes clusters and other modern computing trends (Chapter 1)
- Kubernetes cluster management challenges (Chapter 2)
- How to address Kubernetes cluster management challenges (Chapter 3)
- Key considerations for managing your Kubernetes clusters (Chapter 4)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (although I don't recommend upside down or backwards).

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless. Mainly, I assume that you have a technical background and understand IT operations and cloud environments, but you need some help addressing Kubernetes cluster management challenges. Perhaps you're a chief information officer (CIO), chief technology officer (CTO), IT director or manager, or an IT or cloud architect. As such, this book is written primarily for technical readers. However, don't be discouraged if you haven't yet earned your pocket protector and nerd stripes. I explain any technical concepts, jargon, and acronyms in this book.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway! It's a great book, and when you finish reading it, you just may know quite a lot about the future of multi-cloud management.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:


REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays.


TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff nerds are made of.


TIP

Tips are appreciated, never expected — and I sure hope you appreciate these useful nuggets of information.


WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

If you find yourself at the end of this book wondering, "Where can I learn more?" check out the following resources:

- **Red Hat management topic page:** Learn more about IT management in general and Red Hat's technology capabilities at `www.redhat.com/management`.
- **Red Hat Advanced Cluster Management for Kubernetes:** Learn more about Red Hat's cluster management product along with the key use cases at `www.redhat.com/clustermanagement`.
- **Red Hat blog:** Get the latest information about Red Hat's ecosystem of customers, partners, and communities at `www.redhat.com/en/blog`.
- **Red Hat OpenShift blog:** Get the latest information about Red Hat's OpenShift Container Platform at `www.openshift.com/blog`.

IN THIS CHAPTER

- Recognizing the growth of multi-cloud
- Building cloud-native applications
- Leveraging Kubernetes clusters

Chapter 1
Seeing the Growth of Kubernetes Clusters and Looking at Modern Cloud Computing Trends

In this chapter, you explore the growth of enterprise multi-cloud strategies and their associated challenges, why modernizing applications is crucial to success in the cloud, and the role of Kubernetes clusters in modern enterprise application portfolios.

Cloud Strategies and Technologies Are Evolving

The rapid growth of cloud computing in recent years has increasingly led to complex multi-cloud architectures in many organizations. Multi-cloud environments often evolve as the result of a strategic decision to use best-of-breed tools and services regardless of cloud provider, or as the result of specific requirements and preferences of individual business units and DevOps teams.

The *Flexera 2020 State of the Cloud Report* found that 93 percent of enterprises globally have a multi-cloud strategy averaging 2.2 public and 2.2 private clouds, and 41 percent integrate data between clouds. This strategy is highlighted in Figure 1-1.

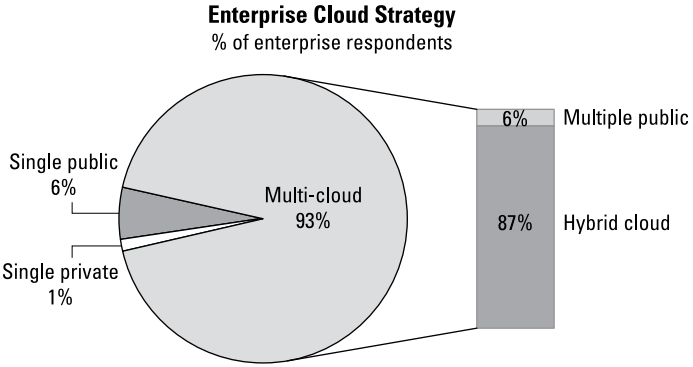

FIGURE 1-1: Nearly all enterprises today have a multi-cloud strategy.

WARNING

Yet surprisingly, only one-third of these organizations use multi-cloud management tools today to address their multi-cloud management challenges. These challenges include the following:

- Difficult and error prone to manage at scale
- Inconsistent security controls across environments
- Overwhelming to verify components, configurations, policies, and compliance

Application Modernization Is Imperative

With the rapid growth and increasing complexity of multi-cloud architectures, application modernization has become a top priority for enterprises. These organizations recognize that simply "lifting and shifting" legacy monolithic applications to the cloud will not meet the demands of their users and customers and fail to fully deliver the agility and scalability benefits of the cloud.

REMEMBER

Enterprise cloud strategies have become prevalent because they enable business agility. Cloud environments are highly automated and focused on providing both developers and IT operations teams with cost-effective, on-demand access to highly scalable computing and infrastructure resources.

As a result, these companies are refactoring their legacy apps and developing new apps, using a cloud-native approach built on a microservices architecture with multiple containers spanning multiple clusters and cloud providers.

Kubernetes Clusters Are Everywhere

Google originally developed Kubernetes based on its Borg platform, which manages the orchestration of more than 2 billion container deployments every week. As a result of the widespread adoption of container technology and the massive scalability of Kubernetes cluster, enterprise use of Kubernetes clusters is also growing rapidly.

TECHNICAL STUFF

According to the *Flexera 2020 State of the Cloud Report*, 58 percent of organizations are currently using Kubernetes and another 22 percent plan to use it in the near future. According to 451 Research, the projected market for application container technologies will grow to $4.3 billion in 2022. Finally, the Cloud Native Computing Foundation's bi-annual survey found that four out of ten enterprise companies (with 5,000 or more employees) are running Kubernetes in production environments.

Kubernetes (also known as k8s or "kube") is an open-source container orchestration platform that automates many of the manual processes involved in deploying, managing, and scaling containerized applications.

As modern cloud-native applications move from development to production, infrastructure and operations (I&O) teams require multiple fit-for-purpose Kubernetes clusters to support DevOps

continuous integration/continuous delivery (CI/CD) pipelines. I&O teams deploy Kubernetes clusters for many reasons:

- **Application availability:** Highly redundant cluster configurations reduce application downtime
- **Disaster recovery:** Deployment across multiple regions and clouds ensures application survivability during a disaster or outage
- **Reduced latency:** Rapid scale out capabilities maximize application performance and reduce latency during peak demand
- **Edge deployments:** Clusters can be deployed at scale with a small infrastructure footprint common in many edge environments
- **CapEx reduction:** Clusters can scale on-demand to meet capacity requirements as needed, thereby reducing the need for upfront investment in infrastructure
- **Choice and flexibility:** Open-source container and cluster technology available across clouds helps avoid vendor lock-in and promote maximum choice and flexibility in best-of-breed deployments
- **Industry mandates:** Clusters can be configured and managed to address specific security, privacy, and geopolitical data residency requirements, among others

REMEMBER

According to *Assessing Patterns for Deploying Distributed Kubernetes Clusters* doc # G00465217, by industry analyst Tony Iams, "As Kubernetes gains adoption across the industry, scenarios are arising in which I&O teams are finding they must deploy and manage multiple clusters, either in a single region on-premises or in the cloud, or across multiple regions . . . for a number of reasons, including multi-tenancy, disaster recovery, and with hybrid, multi-cloud, or edge deployments."

Growth in cluster deployments is accelerating across organizations of all sizes in various industries. For example, take a look at the following:

- **Small-medium businesses (SMBs)** including retail stores with small clusters across hundreds of locations and organizations that initially plan for 10 to 15 clusters but quickly grow to hundreds
- **Large enterprises** consisting of global organizations with hundreds of clusters hosting thousands of applications and "big box" retailers with thousands of nationwide stores
- **Edge-scale telcos** with hundreds of zones and thousands of clusters and nodes across complex topologies

REMEMBER

The ability to run containers on one or more public cloud environments, in virtual machines, or on bare metal servers means that Kubernetes can be deployed almost anywhere.

IN THIS CHAPTER

- Looking at single, multiple, and distributed cluster environments
- Addressing security and compliance requirements
- Ensuring application availability

Chapter 2
Understanding Kubernetes Cluster Management Challenges

Like the cloud itself, Kubernetes cluster management is a journey. Whether your organization is just getting started with a single Kubernetes cluster (let's face it, no organization ever says "we're just going to deploy one cluster") or is already operating in a multi-cluster environment, there are several key challenges that must be addressed, including multi-cluster management, security and compliance, and availability.

In this chapter, you learn more about these challenges to help you define an effective multi-cluster strategy to help your organization succeed on its Kubernetes journey.

Multi-Cluster Management

A journey of a thousand miles that begins with a single step. Your Kubernetes journey also begins with a single . . . cluster. You may have already defined some policies for your Kubernetes environment, but as you begin to allow various team members to access

the cluster, configuration drift sets in and makes it difficult to enforce these policies as your environment grows. At this early stage of the journey, it is also not uncommon for the process of building and pushing applications to a production cluster to be largely manual and error prone. Cluster provisioning may also be complex and not well understood by the various team members.

REMEMBER

Key challenges in a single cluster environment include the following:

- Controlling cluster configuration drift
- Eliminating manual, error-prone application deployment processes from development to production
- Simplifying cluster provisioning

As your Kubernetes environment grows to multiple clusters, it becomes yet more time-consuming, error prone, and difficult to manage. Organizations must often contend with multiple consoles, distributed business applications, and inconsistent policies and security controls across diverse clusters deployed on-premises and/or in public clouds. Configuration drift is exacerbated, and infrastructure and operations (I&O) and DevOps teams struggle due to a lack of end-to-end visibility and control of their Kubernetes resources.

REMEMBER

Key challenges in a multiple cluster environment include the following:

- Implementing and enforcing effective policy and governance across development, testing, and production clusters
- Ensuring consistent cluster provisioning
- Creating a single source of truth for application deployment and policy definitions
- Finding and modifying resources across clusters

Finally, as enterprises realize the full benefits of clusters, they expand their Kubernetes clusters to span multiple public, private, and edge clouds in different geographies with enterprise distributed clusters. If they are still managing their clusters individually, the difficulty grows exponentially: Simple checks for failing components, misconfigurations, policy and compliance checks,

and so on, becomes a monumental task without advanced management capabilities.

REMEMBER

Key challenges in an enterprise distributed cluster environment include the following:

- Enabling single pane of glass, end-to-end visibility across clusters for efficient DevOps
- Deploying and distributing applications at scale
- Enabling single sign-on (SSO) for distributed applications
- Managing audit and compliance activities

To address these challenges, regardless of where your organization is on its Kubernetes journey, you need an advanced cluster management solution that can help you answer the following questions:

- How can I manage the life cycle of multiple clusters, regardless of where they are deployed (for example, on premises and across different public clouds) using a single control plane?
- How can I monitor usage across multiple clouds?
- How do I automate provisioning and deprovisioning of my clusters, placement of workloads based on capacity and policy, and consistent deployment of application updates from development to production?

In Chapter 3, I help you answer these important questions.

Security and Compliance

Many IT organizations mistakenly believe that Kubernetes is secure by design. This notion is dangerous and wrong. Although Kubernetes does obfuscate much of the underlying infrastructure and communications between pods and clusters, "security by obscurity" has never been an effective long-term security strategy.

Kubernetes allows organizations to massively scale their applications on demand. Unfortunately, if the application containers and/or Kubernetes cluster environment are not properly secured, an attacker can exploit critical vulnerabilities — at massive scale.

Conversely, a properly secured Kubernetes multi-cluster environment can be a force multiplier. By creating a baseline "golden" configuration and maintaining strict configuration and change management with well-defined, enforceable, and verifiable policies, IT security teams can quickly secure a global Kubernetes multi-cluster environment.

When planning a security and compliance strategy for your multi-cluster environment, consider the following questions:

- How do I ensure all my clusters are compliant with standard and custom-defined policies?
- How do I set consistent security policies across diverse environments and ensure enforcement?
- How do I ensure deep visibility for auditing the configuration of applications and clusters?
- How do I consume aggregated metrics and logs from all my clusters?
- How do I get alerted on any configuration drift and remediate it?
- How do I update and manage all my applications across clusters, including application and cluster updates?

Robust security capabilities should be a defining characteristic — if not *the* defining characteristic — of your cluster management solution. If it isn't, find another solution. Security in your Kubernetes cluster environment is that important. Key capabilities and features to look for include the following:

- **Embedded role-based access control (RBAC)** for granular permissions management based on default roles (such as Cluster Admin, Admin, Edit, and View), as well as custom roles, with complete logging and auditing capabilities.
- **Built-in policy controllers and an extensible policy framework** for Center for Internet Security (CIS), U.S. Federal Information Security Management Act (FISMA), U.S. Health

Insurance Portability and Accountability Act (HIPAA), U.S. National Institute of Standards and Technology (NIST), and Payment Card Industry (PCI) Data Security Standards (DSS), as well as certificate management, identity and access management (IAM), and Kubernetes configuration with security definitions based on standards, categories, and controls.

- **Identification, categorization, and alerting** capabilities for security and compliance violations including Common Vulnerabilities and Exposures (CVEs), configuration drift, version control, and audit criteria.

Availability

When Marc Andreessen wrote that "Software is eating the world" nearly a decade ago, he wasn't kidding. Applications have become the lifeblood of organizations, and when critical applications are down, they aren't eating — and enterprises are losing money due to lost productivity, lost revenue, and lost opportunities.

Although it may seem counterintuitive, the highly distributed nature of container-based cloud-native applications helps to drive uptime and performance in our modern, "always on" world by eliminating single points of failure in the application architecture. However, without proper orchestration management, a clustered environment can quickly become a complex quagmire of "multiple single points of failure."

Important application availability questions for IT Operations teams, DevOps, and Site Reliability Engineers (SREs) to consider include the following:

- How do I maximize application uptime?
- How can I quickly get to the root cause of failed components?
- How can I get a simplified understanding of my cluster health and the impact it may have on application availability?
- How do I ensure adequate performance capacity while managing costs?
- How can I minimize the impact of outages due to a disaster or other event?

IN THIS CHAPTER

- Driving container adoption throughout the organization
- Managing clusters across their entire life cycle
- Using policies to automate governance, risk, and compliance controls
- Taking application life cycle management to the next level

Chapter 3
Addressing Kubernetes Cluster Management Challenges

In this chapter, you learn how Red Hat Advanced Cluster Management for Kubernetes can help your organization address common cluster management challenges associated with consumability; multi-cluster life cycle management; governance, risk, and compliance (GRC); and application life cycle management issues.

Simplified Management for Consumability

Today, many organizations are focused on applying containerization technologies to modernize their business application portfolio, as well as to optimize costs and utilization of their compute resources. They hope to move quickly and gain the benefits of agile cloud delivery models, but often stumble when trying to

make containers truly consumable across the organization. Consumability is critical to broadly driving container and cluster adoption throughout an enterprise.

Of course, consumability means different things to different stakeholders within an organization:

- **To developers:** Consumability is about making it easy to get access to new clusters. How do you create clusters in different clouds for your organization? When you get a new cluster, how do you ensure that it is configured based on your organization's standards? Then, how do you ensure you can deliver apps dynamically to clusters?
- **To IT operations and Site Reliability Engineers (SREs):** Consumability is about simplifying how you manage the configuration for all namespaces in a single cluster that also scales out as you add more clusters under management. It's also about simplifying how you aggregate health and inventory data about these clusters in an interface that is easy to search and easy to visualize in dashboards like Grafana.

  Grafana is a multi-platform open-source visualization and analytics application used for querying, visualization, alerting, and investigation of key metrics defined by the organization.
- **To security teams:** Consumability is about ensuring that your developers and operators/SREs are comply with your enterprise cluster standards. A built-in audit and enforcement framework makes it easy to create policies and assign them dynamically. When violations occur, events can be tied into your official response systems.


TECHNICAL STUFF

Unified Multi-Cluster Life Cycle Management

A unified multi-cluster life cycle management console helps developers, IT operations and SREs, and security teams manage Kubernetes clusters throughout the entire life cycle from creation, to updating, to de-provisioning.

WARNING

Common challenges associated with multi-cluster life cycle for different stakeholders include

- **IT operations and SREs**
  - Disparate logins and tools from multiple cloud providers and clusters are confusing and inconvenient.
  - Manual management of Day 2 (ongoing) operations such as patching and upgrading at the individual cluster level is time consuming and error prone.
- **Developers**
  - DevOps teams need best practices and templates to get started with GitOps.
  - Considerable effort is required to build a cluster, connect necessary services, and deliver running code from a build pipeline.
- **Security teams**
  - As more clusters are added to the environment, ensuring that security controls are applied to individual clusters is a manual, error-prone process.
  - Using different tools to manage security posture across a multi-cluster domain is inefficient and increases complexity.

TIP

Key features and benefits of unified multi-cluster life cycle management in a cluster management solution such as Red Hat Advanced Cluster Management include

- **Cluster life cycle management:** Gain Day 1 experience with cluster life cycle management using Hive, Red Hat OpenShift's provisioning integration with Red Hat Advanced Cluster Management's console and application programming interface (API) for Red Hat OpenShift clusters. You can quickly create and upgrade new Red Hat OpenShift Container Platform clusters or import existing OpenShift Container Platform and managed Kubernetes clusters to bring under management.
- **Dynamic search:** Use an intuitive graphical console to identify, isolate, and resolve issues impacting distributed workloads.

- **Visual Web Terminal (based on Kui):** Run operations directly from dashboards with a single command-line interface (CLI) for multi-cluster environments compatible with Helm, kubectl, oc, istioctl, as well as Bash and grep commands.
- **Multi-cluster endpoint agent:** Asynchronous work request model aggregates information from multiple managed clusters to the centralized Red Hat Advanced Cluster Management for Kubernetes hub cluster console.

Policy-Based Governance, Risk, and Compliance

Kubernetes clusters inevitably grow very rapidly in enterprise environments as businesses quickly realize the capabilities and benefits of containerized applications running in clusters. But there is a fine line between growth and sprawl.

Ensuring your Kubernetes cluster can grow to support your business needs rather than sprawl into an unmanageable, well . . . cluster, requires well-defined and enforceable policies to support governance, risk, and compliance efforts.

Policies can be used to automate cluster configurations and maintain consistency in security and compliance controls. Policy violations can be quickly identified, categorized, prioritized, alerted on, and remediated to reduce configuration drift and maintain your overall security and compliance posture.


TIP

Key features and benefits of policy-based governance, risk, and compliance in a cluster management solution such as Red Hat Advanced Cluster Management include

- **Out-of-the-box policy templates for security and configuration controls:** Use prebuilt security and configuration controllers to enforce policy on Kubernetes configuration, identity and access management (IAM), and certificate management across your clusters.
- **Governance and risk dashboard:** Use the governance and risk dashboard to view and manage the number of security risks and policy violations in all of your clusters and applications.

- **Customized policy violation views:** Customize policies for various compliance standards, governance dashboard views, and views for most impacted controls for specific standards.
- **Open source extensible policy framework:** Develop custom policy controllers and seamlessly integrate them for centralized management into the governance and risk dashboard.

Advanced Application Life Cycle Management

Advanced application life cycle management capabilities in a cluster management solution use open standards and enable organizations to deploy applications using placement rules that are integrated into existing continuous integration (CI)/continuous delivery (CD) pipelines and governance controls.

TIP

Key features and benefits of advanced application life cycle management in a cluster management solution such as Red Hat Advanced Cluster Management include

- **Application topology view:** Quickly view the health of service endpoints and pods associated with your application topology — with all the connected dependencies such as image versions, associated placement rules, Kubernetes resources, and ConfigMaps.
- **Channels and subscriptions:** Enable GitOps and automatically deploy applications to specific clusters by subscribing to different workload (resource) channels, such as Git Repository, Helm repository, ObjectStore, and resource templates.
- **Placement rules:** Deploy workloads to clusters based on placement rule definitions to ensure that they only run on specific clusters with matching labels.

IN THIS CHAPTER

- Simplifying management with a single pane of glass
- Ensuring core cluster management capabilities are supported
- Managing security and compliance at scale
- Automating container management from the cradle to the grave
- Accelerating time to results

Chapter 4
Five Considerations for Managing Your Kubernetes Clusters

In this chapter, you explore five key considerations to keep in mind when looking for a management solution for your Kubernetes clusters.

Centralized Management

Look for a cluster management solution that gives you a single pane of glass view of your entire environment including on premises, private and public clouds (such as Amazon Web Services [AWS], Google Cloud Platform, and Microsoft Azure) as well as the different technologies you use including virtualization, containers and orchestrations, and operating systems.

While it's important to use a cluster management solution that works across your entire Kubernetes environment and supports core capabilities, be wary of platforms that attempt to do

everything. Often, a platform does one or two things really well but then bolts on a bunch of other tools and services that don't necessarily run well and aren't fully integrated, which could cause the platform to become unusable, overly complex, and unstable. Keep things simple and determine which core capabilities are most important to support your multi-cluster environment.

End-to-End Cluster Management

Using open source container and orchestration technologies lets you rapidly create, update, and tear down Kubernetes clusters. Your cluster management tool needs to do the following:

- Enable reliable and consistent management at scale.
- Support and encourage Infrastructure as Code (IaC) best practices and design principles.
- Manage clusters across multiple datacenters and public cloud services.
- Monitor health across all clusters and pods.
- Provide visibility and alerting of problems across clusters.

Security and Compliance

Security and management are top priorities for every organization today, but it is a common fallacy to assume that Kubernetes is inherently secure. Take a more proactive approach to security when managing your clusters and applications with tools that enable security and compliance at scale through policy definition and enforcement, role-based access control (RBAC), configuration baseline monitoring, and built-in compliance auditing and reporting. Use policies to automatically configure and maintain the consistency of your security and the controls required by your geographic region (including global, national, regional, and local mandates), industry standards, and internal governance. When considering policy-based governance, risk, and compliance, choose a management solution that

- Remediates configuration drift in a robust, seamless manner
- Creates and enforces policies at a cluster level to prevent unintentional or malicious configuration drift
- Gets details on cluster compliance to the defined policies
- Enables evidence collection for audit purposes
- Uses and contributes policies to an open-source community to help streamline and share hardened assets for quick start and rapid time-to-value production scenarios

Central Life Cycle Management of Containerized Apps

Managing containerized applications gives you the tools to deliver workloads intermittently to all your clusters. This process happens automatically and with certain controls in place for enterprise and production environments. Central life cycle management tools include the following:

- Placement policies that are integrated into existing continuous integration (CI)/continuous delivery (CD) pipelines and governance controls
- Open standards
- Deployment of applications across clusters based on channel and subscription definitions
- Quick views of service endpoints and pods associated with your application topology
- Cluster labels and application placement rules to easily move workloads across clusters — even between multiple cloud providers
- Deployment and maintenance of Day-2 operations of business applications distributed across your cluster domain

Achieving Faster Results

One aspect that's traditionally missing from some products in the market is the opportunity for cultural transformation with integrated dashboards and tooling that brings your development, infrastructure, and operations teams together into one place to do their work. With the right Kubernetes cluster management solution, you can break those old silos of work and encourage teams to work together to achieve faster results.

Notes

Notes

Manage your Kubernetes clusters at scale

As modern cloud-native applications move from development to production, infrastructure and operations teams require multiple fit-for-purpose Kubernetes clusters to support DevOps pipelines. As a result, growth in cluster deployments for many IT organizations is accelerating, and managing it all can become difficult. Understand the challenges of managing Kubernetes clusters, how to address them with proper management, and what the key considerations are when looking for the right solution to help.

Inside…

- The rise of hybrid and multi-cloud
- Challenges of managing Kubernetes clusters across multi-cloud environments
- Key considerations for managing your Kubernetes clusters

Lawrence C. Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 150 *For Dummies* books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-76761-9
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.