White Paper: **April 2022**

Best Practices for Kubernetes Management

Reduce container complexity with Kubernetes automation and orchestration

vmware®

Table of contents

Container adoption will hit 50% of total public cloud deployments as cloud native containerization solutions take center stage in the enterprise cloud[2].

Reducing time to value

The quest for agility has significantly changed the technology landscape over the last decade. In 2020, the trajectory of technology innovation accelerated exponentially and was driven by the pressures of hybrid work. Multi-cloud is ubiquitous, with 93% of enterprises reporting to have a multi-cloud strategy[1]. Similar to infrastructure, enterprises are also looking to modernize over half of their existing applications by 2022 to gain business agility[2]. Container adoption will hit 50% of total public cloud deployments as cloud native containerization solutions take center stage in the enterprise cloud[2]. According to an IDC report, half of enterprise applications will be deployed in containerized hybrid/multi-cloud environments by 2023[3]. These shifts have caused IT teams to manage new and rapidly shifting workloads while simultaneously working towards optimizing cost and performance of infrastructure.

In this white paper, we will examine the role and impact of Kubernetes for the modern, cloud-based containerization journey, and how businesses are starting to navigate the complexities of orchestrating multi-cloud distributed Kubernetes platforms.

Platforms, people, and value

Infrastructure and operations (I&O) teams across organizations are tasked with supporting new digital business initiatives from C-level to DevOps. CIOs link business goals and the technology needed to drive business growth and agility to protect their organizations' competitive foothold. DevOps principles are now playing a more significant role, moving from a cost center to a business enabler and differentiator, and operations teams are using tools to manage cloud sprawl and environment complexity.

The platforms I&O teams use directly impact the value they can deliver. The pressure to deploy applications amid distributed clouds has created new challenges for I&O leaders. To support business initiatives that drive growth, I&O teams are turning to advanced platforms that help manage cloud sprawl in their complex environments.

1 "The State of the Cloud Report," Flexera, 2020.
2 "Worldwide Intelligent CloudOps Software Forecast, 2021-2025," IDC, 2021.
3 "Policy and Automation Address Multicluster Kubernetes Management Challenges," IDC, June 2020.

DevOps: The business enabler

DevOps practices help organizations accelerate application delivery through alignment principles between supporting functions. Of the companies that have released applications to production in the last year, 53% say DevOps is instituted fully across their IT organization, and another 44% indicate DevOps is utilized across some teams, according to a 451 Research study[4]. Faster software releases are ranked the current top benefit of enterprise DevOps methodology[4]. However, the unseen hero is the underlying infrastructure orchestration.

Kubernetes is a key enabling technology for modern DevOps

DevOps teams need to deploy software to production at an ever-increasing pace. Kubernetes (K8s), as an open source container orchestration layer for automating infrastructure deployment, can offer the flexibility to do more rapid application layer iterations and redeployment. To ensure your DevOps teams are moving at the pace you need, sooner rather than later, you must consider how you are managing and scaling your infrastructure with containers.

Container adoption and Kubernetes have truly gone mainstream. According to a Cloud Native Computing survey, 96% of organizations are either using or evaluating Kubernetes[5]. With Kubernetes, organizations can deploy applications quickly and efficiently and manage the containerized applications, regardless of where they live.

However, the sheer scale of Kubernetes clusters adds to a more complex IT environment. Besides the growth projections for global Kubernetes solutions, deployments within organizations are projected to scale up from just a handful to potentially thousands.

I&O becomes core to agility

The operations team is vital to keeping DevOps and developers efficient and focused on innovating. Managing Kubernetes in the cloud is no easy task since business initiatives require setting up and managing clusters across multi-clouds, while maintaining compliance to meet service level objectives.

Counteracting the Kubernetes trough of disillusionment

With all the benefits and innovation that Kubernetes brings to the modern application, it is tempting to dive right in and start adopting. However, the reality of containers and Kubernetes platforms is that they introduce new, unforeseen challenges for I&O teams when planning to modernize applications on Kubernetes.

4 "Voice of the Enterprise: DevOps, Organizational Dynamics survey," 451 Research, October 2021.
5 "The year Kubernetes crossed the chasm," Cloud Native Computing Foundation, 2021.

Multi-cloud and hybrid cloud add complexity

Organizations often start small with their containerization journey, but it will not stay that way for long. When more and more teams adopt containers and Kubernetes to develop and deliver their applications, the whole landscape gets complex quickly. There could be multiple teams deploying multiple applications onto multiple clusters in a variety of different environments, such as on-premises, private, or public clouds.

When application teams run Kubernetes clusters on different clouds, it brings even more complexity to the I&O team. It is difficult to consolidate policy management for multiple clusters and troubleshoot across disparate cloud environments where Kubernetes clusters might sit. Multicluster management solutions need to deliver robust functionality across diverse container platform environments that span multiple clouds and on-premises—and most customers will not have a standardized platform across all[6].

Hybrid cloud is also a reality. On-premises systems have advantages in terms of customization, control, and continuity in the event of network disruptions[7]. According to Forrester, hybrid systems that combine elements across on-premises and cloud resources look increasingly appealing due to growing risks of business disruption from climate change, recurring pandemics, cyberattacks, and political upheavals. But the proliferation of infrastructure types means that uniformity is a thing of the past, requiring a shift in the infrastructure management paradigm.

I&O tax for existing applications

As fast as organizations modernize their applications, many are still having to use legacy applications for day-to-day operations. Kubernetes can bring new life to these essential applications by breaking up software monoliths and allowing more rapid fixes until they are ready to modernize the application layer. IDC found an even mix of new vs. existing applications being containerized—49% of existing, migrated applications will be refactored over time[6].

Resource-hungry applications are the next area enterprises will seek to optimize so they can control costs. In the meantime, containerizing legacy applications helps I&O teams improve infrastructure utilization with higher density, enabling more modern application development flows through microservices, improved software packaging, and distribution. This reduces time-consuming updates for application teams and ensures I&O teams can control spending more efficiently while application teams work on a refactoring plan. However, I&O teams will need to ensure they have the right staff onboard to manage Kubernetes.

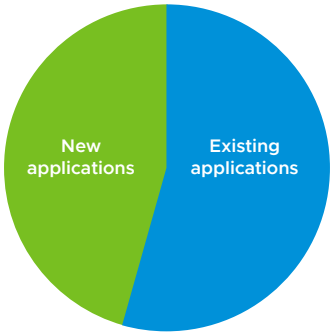

FIGURE 1
Comparison between new and existing applications being containerized, as found by IDC[6].

6 "Worldwide Software-Defined Compute," IDC, 2021.
7 "US Tech Market Outlook By Category for 2021 and 2022," Forester, 2021.

Default Kubernetes security is not enough

Kubernetes complexity makes it challenging for I&O teams to enforce their organization's security posture or compliance requirements. Security posture is also seen as a big hurdle to container adoption[8]. Security is top of mind for C-level executives with 75% of CEOs believing a strong cyber security strategy is critical to engender trust with key stakeholders[9]. Unsecured Kubernetes clusters are vulnerable to all kinds of attacks. Plus, if the attack surface keeps growing across a myriad of clouds, on-premises data centers, IoT devices, personal computers, edge devices, and more, then this creates more points of vulnerability. In addition to a steep learning curve and shortage of skilled labor, exposures due to misconfigurations are the biggest cause for Kubernetes security incidents.

Kubernetes provides many security controls and risk-prevention features. Containers, for instance, are replaced with new versions instead of simply being patched or updated, quickly weeding out vulnerabilities. Despite these inherent advantages, the Kubernetes ecosystem is constantly fluctuating, resulting in an overwhelming stream of alerts and fixes for IT personnel to keep tabs on. This makes it all too easy for something vital to get overlooked. Even with the appropriate configuration, attacks are inevitable, but the fundamental structure of containerized applications can help significantly reduce the blast radius of a cyberattack, shrinking the amount of damage caused by intruders by preventing them from accessing other containers or applications once they have infiltrated the cluster.

One of the most powerful capabilities in the never-ending battle against cyberattacks is role-based access control (RBAC), a security feature already built into Kubernetes. Used to adjust access or permissions based on the needs of the individual user or application, RBAC enables organizations to further restrict intruder access and reduce blast radius. This preventive measure requires I&O teams to be thoughtful—and picky—about how much access is granted to each individual user or application. That way, if compromised, the attacker's ability to delete or repurpose resources is limited. To fully leverage this feature, I&O teams need to be intentional and communicative since the likelihood of withholding necessary permissions to rightful accounts during the adjustment period is high and can cause further headaches.

The reality, unfortunately, is that Kubernetes security mitigation is incredibly complex. With every new container deployed, a new point of entry is opened for attackers to exploit. And, since most container management tasks are handled autonomously, it is impossible to account for every potential access point and therefore also impossible to completely prevent infiltration. However, the right configurations—when thoughtfully employed by experienced personnel or overseen by Kubernetes management systems—can significantly reduce the impact of an attack that could devastate your organization.

8 "Beginner's Guide to Container Security," Forbes, 2021.
9 KPMG Cyber Security Considerations 2022.

Tech labor/skills shortage and blurred responsibilities

It is difficult for existing I&O teams to keep up with the growth in digital projects without the right personnel in place to help them manage their containerization strategy.

Lack of talent

In 2021, 64% of respondents said that talent availability is the largest challenge to emerging technology adoption, compared with just 4% in 2020[10].

Organizations are aware of the high costs and high demand for employees with Kubernetes skills, which are the most in demand for modern operational roles. According to a Gartner report, talent shortages are rising. In 2021, 64% of respondents said that talent availability is the largest challenge to emerging technology adoption, compared with just 4% in 2020. Thus, the labor and skills shortage continues to be the greatest threat to U.S. businesses[10].

Lack of internal experience and expertise remains the biggest challenge when it comes to choosing (55%) and managing (53%) Kubernetes. In fact, 61% of organizations are looking for solutions that are easy to deploy, operate, and maintain, and many will need assistance to bridge existing skills gaps and speed the transition to modern practices[11].

Higher employee turnover rates

Besides the difficulty of finding qualified employees, keeping them amid the Great Resignation era is hard, too. A record 4.5 million American workers quit their jobs in November 2021, and there is no end in sight for the Great Resignation movement[12]. The time-consuming nature of managing IT infrastructure resources across clouds can quickly take its toll on staff, creating a whole new realm of problems within organizations.

Excessive turnover can also make security vulnerabilities and workflow inefficiencies worse. Infrastructure management tasks may go overlooked during staff transitions, and shared knowledge can also be lost, all of which increases the risk of security breaches. Meanwhile, production and development may be slowed, or screech to a halt during the time required to familiarize new hires with organizations' specific Kubernetes infrastructure. This can lead to a dip in overall productivity as well as a larger backlog of alerts, anomalies, and issues for new recruits to address straight out of the gate.

10 "Businesses struggle with labor shortage, inflation and supply chain disruption amid COVID-19 resurgence – Highlights from Macroeconomic Outlook, Business Trends," 451 Research, 2021
11 "The State of Kubernetes 2021," VMware survey.
12 "No end in sight for the Great Resignation; workers keep quitting for better pay, benefits," Computerworld, 2022.

For IT teams in the trenches, however, it isn't about the bottom line or even the steep learning curve. Much of the frustration stems from the tedious, repetitive infrastructure tasks that keep them from working on Kubernetes projects or even focusing energies on developing skills that might be useful later in their career, which is another indicator of job satisfaction. By automating the minutiae—and doing it properly to prevent excessive toil to rectify anomalies—leaders can free up their teams' time for that meaningful work in addition to addressing inefficiencies. This results in a win for both employees and employers.

Operating through complexity: Multiple stakeholders and blurred responsibilities

Multiple teams are also taking ownership of Kubernetes operations today[11]. Operations (62%) and development teams (55%) are most often in the mix, but application owners (29%) and even C-level executives (16%) are getting involved[11] in the selection, operations, and management aspects. Organizations hoping to rapidly build and deploy custom applications on the cloud will need to ensure their teams have the control, consistency, and flexibility across IT operators, DevOps, and developers.

For operators, manually provisioning, configuring, and managing a fleet of Kubernetes clusters across clouds is incredibly difficult and time-consuming. The risk of potential errors and inconsistencies is ever-present, and manual management can often lead to security vulnerabilities and inefficiencies. For DevOps, discrepancies between development and production environments can hinder the development process, adding to the potential roadblocks that come with disparate platforms and inconsistent integrations. In addition, without real-time visibility into Kubernetes cluster telemetry, DevOps will face challenges optimizing and adapting their deployments. For developers, vendor lock-in becomes a major hurdle, whether it is due to the limitations of a particular cloud environment, Kubernetes management suite, or software. Developers must be able to choose their own path based on their application needs, and locking them into a rigid environment hinders their development capabilities and slows their ability to ship code faster.

Best practices for Kubernetes deployment

During the early days of Kubernetes when cluster creation took more effort, organizations opted to use one Kubernetes cluster with multitenancy separation. Multitenancy models use namespaces to separate tenants and workloads. At most, organizations would use a few large clusters and isolate workloads for different purposes using namespaces. For example, organizations could create dev, test, or production workloads within the same cluster, but separated by namespaces.

Kubernetes cluster provisioning is much simpler, making it easy to quickly spin up new clusters. Organizations are looking for the performance, flexibility, and security benefits that a multicluster Kubernetes deployment brings.

Kubernetes cluster provisioning is much simpler, making it easy to quickly spin up new clusters. Organizations are looking for the performance, flexibility, and security benefits that a multicluster Kubernetes deployment brings.

Today, however, Kubernetes cluster provisioning is much simpler, making it easy to quickly spin up new clusters. Organizations are looking for the performance, flexibility, and security benefits that a multicluster Kubernetes deployment brings.

The benefits of multi-cloud deployments

Organizations demand a level of agility from their I&O teams that naturally lends itself to working with multiple cloud providers. Kubernetes orchestration makes it possible to move workloads from one cloud infrastructure to another or run it across multiple cloud providers. The advantages gained using multi-cloud outweigh the efforts of managing two or three cloud providers. If one cloud excels in AI or is best for databases, then using that cloud provider makes sense. IT can run their workloads and applications on the cloud that best aligns with their business requirements and/or run on-premises for certain workloads. Furthermore, multi-cloud and multicluster deployments reduce the risk of vendor lock-in and help organizations negotiate better pricing and other terms.

Multi-cloud and multicluster enable applications to be deployed in, or across, multiple availability zones and regions, improving application availability for global applications. Sometimes those clusters are hosted in the same datacenter, like legacy applications or cloud, and sometimes are distributed over multiple data centers, anywhere on the planet, or across multiple clouds.

Gain flexibility

Multi-cloud gives IT the freedom of choice to run their workloads based on their need to use cloud services and innovations from multiple cloud providers. Organizations opt for a multi-cloud strategy to avoid vendor lock-in and run workloads in the private cloud due to security and compliance—mergers and acquisitions can force organizations into a multi-cloud reality. Further, when you run multiple clusters in Kubernetes, you gain fine-grained control over how each cluster is configured. You can use a different version of Kubernetes for each cluster. The configuration flexibility of multicluster deployments is beneficial if you have an application that depends on a certain setup or version of a tool in the stack. It is also valuable if you want to test new versions of Kubernetes in an isolated dev/test cluster before upgrading production clusters to the new version.

Meet compliance requirements

Cloud applications need to comply with a myriad of security policies and regulations. A multi-cloud strategy reduces the scope of compliance for each individual cluster. For example, if you need to keep some workloads on-premises or keep data within a certain geographic region due to regulatory requirements, you can deploy a cluster in a location that addresses those needs, while running other clusters elsewhere.

Benefits of multicluster deployments

There is an increasing need for distributed multicluster Kubernetes architecture with smaller, more specialized, and dedicated clusters per application, per environment, per team, or per SLA. This approach can bring significant benefits, such as:

There is an increasing need for distributed multicluster Kubernetes architecture with smaller, more specialized, and dedicated clusters per application, per environment, per team, or per SLA.

Better isolation

Applications deployed in namespaces on one cluster share the same hardware, network, and operating system, as well as certain cluster-wide services such as API server, controller manager, scheduler, and DNS. Such a soft multitenancy model causes concern about potential security and performance issues. Thus, using clusters as the isolation boundary is the preferred way to provide hardened multitenancy, using the underlying hypervisor to isolate workloads much more effectively.

Faster time to market

The faster you can deploy Kubernetes clusters, the sooner developers can create new code or update existing code. Smaller, specialized clusters accelerate the task of adding resources to clusters and LCM operations. Multicluster deployments keep your developers focused on developing applications.

Higher availability

Another benefit that multicluster architecture brings is the reduction of the blast radius. Cluster issues, especially those that are related to shared services, will not subsequently bring down all the applications running on the cluster. This helps you gain overall higher availability for your applications.

Customized configurations

Different applications require different configurations. For example, some applications may need GPU worker nodes, a certain CNI plugin, or prefer a specific public or private cloud as the underlying IaaS. With clusters as the isolation boundary for applications, you can equip Kubernetes with the exact configuration that the applications need. You can also control the lifecycle of each cluster. For example, you will not need to force all your applications to run on a newer version of Kubernetes if some of them are not yet ready.

Enhanced security

Kubernetes provides many security controls and risk-prevention features. Despite these inherent advantages, the Kubernetes ecosystem is constantly fluctuating, resulting in an overwhelming stream of alerts and fixes for IT personnel to keep tabs on. This makes it all too easy for something important to get overlooked.

Increased scalability

Running more than one cluster may improve your ability to scale workloads. If everything runs in a single cluster, it is harder to determine which specific workloads need more resources or more replicas, especially if you lack good performance data for specific workloads.

Getting to value with Kubernetes

The day-to-day challenges that IT operators, DevOps, developers, and business leaders face with complex, multi-cloud Kubernetes deployments continue to grow.

The day-to-day challenges that IT operators, DevOps, developers, and business leaders face with complex, multi-cloud Kubernetes deployments continue to grow.

Delivering controlled and consistent Kubernetes

VMware Tanzu® Mission Control™ is a Kubernetes management platform that can seamlessly manage multiple clusters across clouds. Tanzu Mission Control offers businesses a centralized management hub with a unified policy engine that simplifies multi-cloud and multicluster Kubernetes management across stakeholder teams within the enterprise. IT operators can reduce complexity, increase consistency, and offer a better developer experience with Tanzu Mission Control. Whether you are a Kubernetes expert or newcomer, Tanzu Mission Control can be the entry point to rapidly provisioning and managing distributed Kubernetes clusters.

Given the growth projections for global Kubernetes solutions, Tanzu Mission Control offers significant benefits at every stage of the application containerization journey.

Modern infrastructure for cloud native

Tanzu Mission Control is a key component of the packaged VMware Tanzu for Kubernetes Operations solution.

Tanzu for Kubernetes Operations is a curated platform of Tanzu capabilities that provides the foundation for building a modern Kubernetes-based container infrastructure at scale across all clouds. Tanzu for Kubernetes Operations simplifies container management with tools, automation, and data-driven insights that boost developer productivity, secure applications, and optimize infrastructure performance across all your clouds.

Overcome the challenges of a Kubernetes deployment

Tanzu Mission Control overcomes the challenges organizations face managing a Kubernetes deployment with the growth of multi-cloud and complex IT environments. Amid looming security fears and a shortage of skilled IT and security staff, Tanzu Mission Control is empowering business leaders to modernize at their own pace.

Challenges	Persona	Tanzu Mission Control Benefits
Multi-cloud complexity and cloud sprawl	**Executive and C-level** Leaders are concerned about future-proofing environments.	Robust set of features that is extendable so IT teams can adapt as new technology becomes available.
	IT operator Manual Kubernetes cluster management is labor intensive and error-prone.	Centralized policy management and life-cycle management decrease manual efforts.
	DevOps/Developers DevOps is hindered by lack of consistency and platform telemetry.	Centralizing Kubernetes management tasks brings consistency and baseline diagnostics so DevOps can adapt.
Security	**Executive and C-level** Containers increase the attack surface.	Apply strict security policies for multi-cloud, Kubernetes clusters.
	IT operator Individually enforcing policies and configurations across clouds can be time-consuming.	Centrally managed policy engine ensures conformance and out-of-the-box security policies.
Tech labor and skills shortage	**Executive and C-level** Shortage of talent and high turnover rates impact time to value.	Reducing Kubernetes management tasks enables employees to focus on more innovative projects and increase job satisfaction.
	IT operator Manually provisioning and configuring clusters impact productivity and DevOps teams.	Improve user experience for DevOps and development teams by facilitating consistency.
	DevOps/Developers Inconsistency between development and production environments can slow down innovation.	Self-service access to clusters enables essential automation for improved productivity and job satisfaction.

Tanzu Mission Control vs. DIY

Based on industry standard benchmarks[13]

Increased productivity

Save 203 hours per developer per year

Improved efficiency

93% time savings to provision a cluster

Enhanced security

97% time savings to run a CIS security test

The proof is in the numbers

Starting a Kubernetes deployment can be complex and time-consuming initially due in part to a global skills shortage of Kubernetes talent. VMware performed a three-year ROI analysis by analyzing the economic benefits of operationalizing Kubernetes with Tanzu Mission Control.

Tanzu Mission Control vs. DIY

Based on industry standard benchmarks[13]

Increased productivity: Save 203 hours per developer per year
Improved efficiency: 93% time savings to provision a cluster
Enhanced security: 97% time savings to run a CIS security test

Be ready for anything

No matter which direction business strategists choose, organizations must adapt to remain competitive. Accelerating application delivery with Kubernetes helps organizations stay agile and resilient. IT leaders can turn to Tanzu Mission Control to maximize their Kubernetes investment throughout the DevOps lifecycle. In addition, Tanzu Mission Control helps accelerate the adoption of Kubernetes to expedite the delivery of modernized applications and deliver significant operational savings.

Read the VMware Tanzu Mission Control and the VMware Tanzu for Kubernetes Operations solution briefs to learn more.

13 VMware Internal Customer Research, 2022.

Item No: Best Practices for Kubernetes Management 4/22.