IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: VMware

Growth of multicloud and multicluster Kubernetes architectures creates a new set of enterprise IT security, cost, and performance challenges. Policy-driven automation offers scalable strategies for consistent configuration, control, and compliance.

Policy and Automation Address Multicluster Kubernetes Management Challenges

June 2020

Written by: Mary Johnston Turner, Research Vice President, Cloud Management

Introduction

Businesses around the world are facing significant and unexpected economic pressures. Cost, security, and agility are top priorities as organizations pivot to support work from home while managing unpredictable loads on computing resources and accelerating distributed application development to rapidly add critical new features.

DevOps programs centered on cloud-native, container-based applications developed using automated continuous integration and continuous delivery (CI/CD) and infrastructure configuration automation continue to be top priorities. Cloud-native applications are typically built using microservices deployed in containers to support highly distributed development, automated testing, and continuous deployment of code updates. This drives faster time to market and more efficient use of people and resources. IDC expects that by 2023, more than 500 million digital applications and services will be developed using cloud-native approaches.

AT A GLANCE

KEY STATS

According to IDC expectations:

- By 2022, 70% of enterprises will deploy unified VMs, Kubernetes, and multicloud management processes and tools.
- By 2023, half of enterprise applications will be deployed in containerized hybrid cloud/multicloud environments.
- By 2023, more than 500 million digital applications and services will be developed using cloud-native approaches.

With the rapid, ongoing growth of cloud-native applications reshaping enterprise software portfolios, more and more organizations are deploying distributed multicluster Kubernetes container platforms across many locations, geographies, and clouds. This IDC Technology Spotlight highlights how policy-driven, multicluster configuration and life-cycle management automation technologies are emerging to better standardize, secure, and control critical container infrastructure across multicloud environments. The paper also discusses how VMware Tanzu Mission Control is helping standardize and scale container configuration life-cycle management.

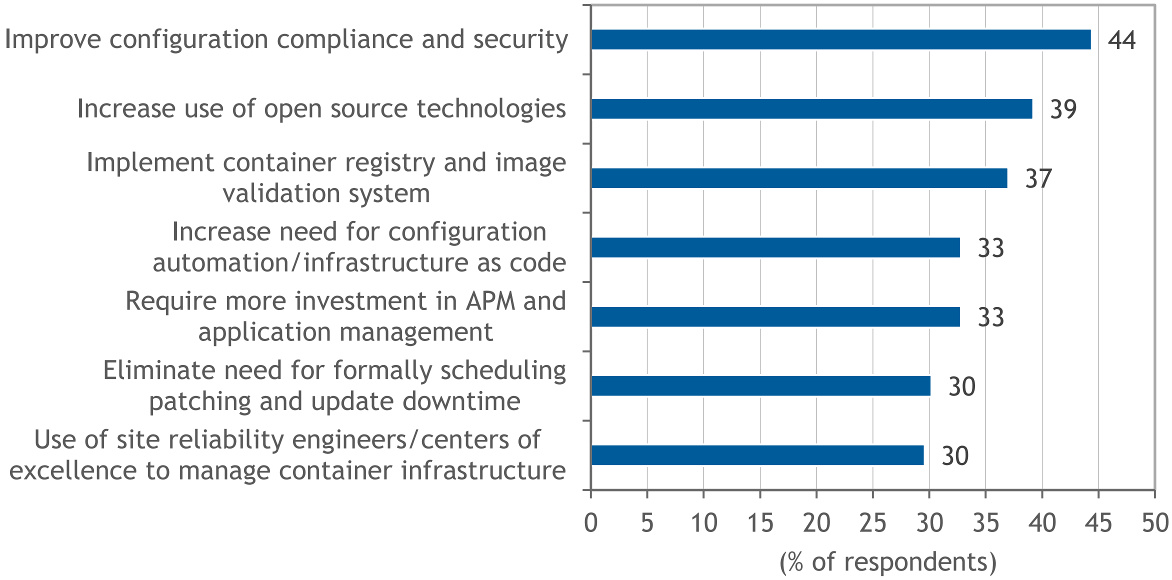
Multicluster Distributed Kubernetes Challenges and Opportunities

Kubernetes has become the de facto industry standard technology for the orchestration of container clusters, both on-premises and in public clouds. Kubernetes is supported by a large, active open source community. It provides a vendor-agnostic orchestration engine and API that provide an abstraction layer for large-scale deployment, scaling, and orchestration of containers across clusters of compute nodes.

In the early days of cloud-native development, many organizations relied on a few large container clusters to support many applications and developers. However, as use of containers and Kubernetes has grown, architectures are shifting toward reliance on larger numbers of small distributed clusters located across datacenters, cloud platforms, and edge locations. Typically, the provisioning, configuration and day-to-day life-cycle management of clusters has been left to local system administrators. This has often resulted in the proliferation of silos of inconsistent configurations, updates, and monitoring strategies that increase the risk of security breaches or performance problems due to inconsistent configurations and updates. With different teams managing different clusters in different locations and clouds, it can become very difficult to ensure that all clusters adhere standards.

IDC believes that by 2023, half of enterprise applications will be deployed in containerized hybrid cloud/multicloud environments. IDC's research identifies the need to improve configuration and security compliance as the number 1 enterprise IT concern related to how containers will change the way the organization manages infrastructure and applications (see Figure 1).

FIGURE 1: *Impact of Containers on Enterprise Infrastructure and Application Management Priorities*



n = 189 enterprise IT decision makers representing U.S. organizations with $1+ billion annual revenue

Note: Multiple responses were allowed.

Source: IDC's Containers and Cloud Management Survey, May 2019

The rapidly increasing use of distributed multicluster container environments will change the way enterprises manage and optimize the resources. Specifically, it will require greater emphasis on consistent, automated, configuration compliance and security as well as new investment in advanced observability and analytics.

Value of Multicluster Policy-Driven Configuration Automation

Unlike traditional virtual machine (VM) and bare metal environments where applications and infrastructure are tightly linked and change slowly, containers and Kubernetes constantly adjust to changing application demand. In many environments, an individual container may exist for only seconds or minutes, unlike VMs that can last for days, weeks, or longer. Containers are not patched and updated while running; rather, new containers are created and used to replace older containers that are destroyed.

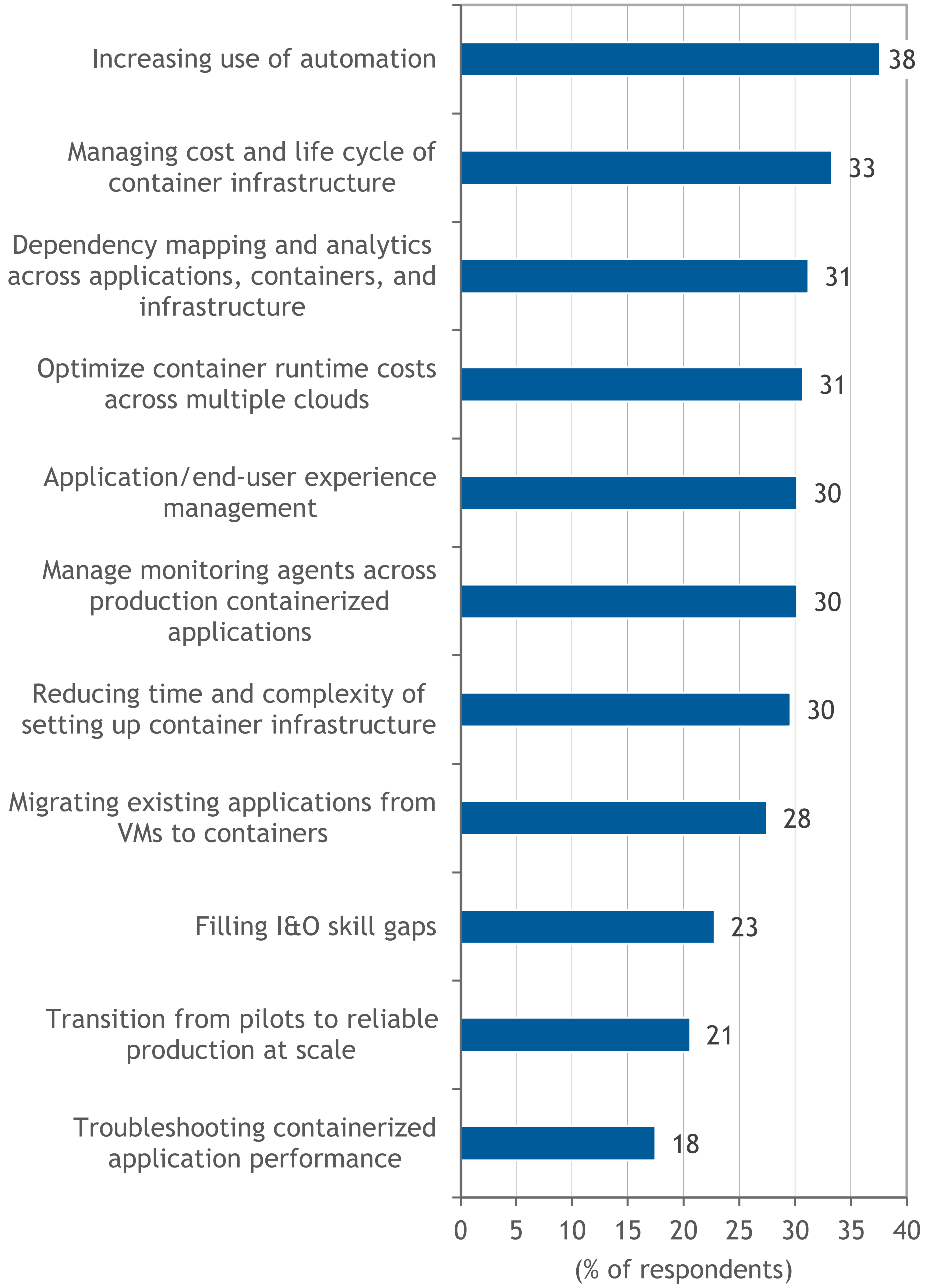
The ephemeral nature of containers is only part of the management challenge. Application software deployed onto containerized infrastructure is packaged differently than traditional applications. Specifically, containerized applications are broken down into many microservices, and each container is then packaged as an immutable image that includes all the related operating systems (OSs) and libraries needed to run the code. Every time application code changes, or when an OS issues a new security patch or a library is updated, the container itself may need to be updated and replaced as well.

Image repositories curate tested and approved images that can be updated as part of automated CI/CD development toolchains. Any one logical application may have dependencies on dozens of microservices. The reality is that container images can be updated very frequently, even multiple times a day. In highly distributed environments, different microservices may be deployed on different cloud platforms or services, but a change to any one microservice may impact dependencies in another. Constant change creates challenges for maintaining consistent configuration security, data governance, cost controls, and end-to-end performance.

Within a container cluster, Kubernetes automates the scaling and deployment of new images. However, it does not govern the configuration of the cluster itself and does not help enterprises maintain consistent configurations and life-cycle management across multiple clusters. As the number of individual clusters grows, and they become more physically distributed, the risks related to inconsistent cluster configurations rises as well.

Automation is required to keep up with the rate, scale, and complexity of change in distributed multicluster Kubernetes environments. However, traditional approaches to automation that rely on reactive, human intervention to identify needs, write prescriptive code, and determine when to kick off workflows just aren't sufficient. IDC believes policy-driven multicluster configuration automation, paired with proactive observability, is required to manage risk and optimize multicluster infrastructure and service stability and performance. IDC's research consistently identifies the need to increase automation as the top priority when managing containerized applications in large-scale production environments (see Figure 2).

FIGURE 2: ***Top Management Priorities for Running Containerized Applications in Production***



n = 189 enterprise IT decision makers representing U.S. organizations with $1+ billion annual revenue

Note: Multiple responses were allowed.

Source: IDC's Containers and Cloud Management Survey, May 2019

Operational challenges that can often be handled on an ad hoc basis within a single cluster or datacenter can rapidly spin out of control as more clusters and services are added. It is very important that enterprises working to increase the size of their multicluster Kubernetes resources consider a number of requirements when evaluating multicluster Kubernetes management solutions. These requirements include the following:

- Ability to define and automatically maintain configuration policies consistently across clusters, whether they reside in on-premises datacenters, third-party hosters, public cloud platforms, or edge systems
- Ability to easily identify and group together dependent namespaces across clusters to maintain appropriate configuration dependencies across multiple microservices that make up a single logical application
- Simplicity of integration with existing, noncontainerized management tools and workflows, particularly with regard to providing visibility across infrastructure provisioning and development toolchains
- Ability to attach to standard Kubernetes APIs, regardless of where they are deployed or sourced, to ensure that policies can be consistently automated across multiple clouds and container platforms
- Option for SaaS or cloud-hosted access or other methods to ensure smooth operations during unexpected shutdowns when staff may be physically unable to access datacenters and edge systems

Most enterprises expect to maintain hybrid and multicloud infrastructure architectures supporting VMs and Kubernetes for a number of years. Consistent configuration and control across these widely distributed resources are vital to ensuring that distributed, microservices-based applications conform to configuration security and compliance requirements while delivering on expected application performance service-level agreements (SLAs).

Considering VMware Tanzu Mission Control

VMware Tanzu Mission Control (TMC) provides centralized, policy-driven management for multicloud and multicluster Kubernetes environments. This newly released SaaS-delivered service is vendor agnostic and able to attach to any conformant Kubernetes cluster. TMC leverages open source technologies to enable most key functionalities.

The initial release of TMC includes the ability to:

- Define and consistently apply configuration policies automatically to specific cluster groups. For example, test, development, and production clusters could automatically be configured for different network access or configuration requirements regardless of whether they are deployed on-premises, in a hosted datacenter, or in a public cloud.
- Tag and group namespaces together across multiple clusters to create a unified workspace that represents logical applications. Configuration policies can be confirmed and applied across the workspace on a reliable and repeatable basis.
- Maintain global observability across clusters that are residing in disparate environments – on-premises or in public clouds — with cluster health visualization for quick troubleshooting.

- Automate cluster inspections to check if the clusters are configured according to industry compliance and security standards, such as Cloud Native Computing Foundation conformance inspection and Center for Internet Security benchmark inspection.
- Automate cluster data protection — snapshots, backup, and restoration — based on the open source Velero project.
- Centralize cluster life-cycle management via TMC UI, API, or CLI. Initial release supports AWS EC2 for this feature, with other environments such as vSphere and Azure on the road map.

TMC enables administrators to avoid laborious, error-prone cluster-by-cluster configuration management, helping improve administrative efficiency and ensure more consistent security, compliance, and performance even as the number and diversity of clusters increase.

TMC is part of VMware's Tanzu portfolio, which offers products and services to help enable modern application development and delivery while simplifying multicloud operations. This introduces opportunities for more integration with, for example, Tanzu Kubernetes Grid to rapidly provision new Kubernetes clusters, Tanzu Observability for multicluster microservices monitoring and full stack analytics, and Tanzu Service Mesh for additional policy management.

For customers that want to closely integrate Kubernetes management with existing vSphere, vCenter, and vRealize solutions, VMware Cloud Foundation 4, powered by vSphere 7 with Kubernetes, offers a solution that tightly integrates Kubernetes management with vCenter to provide vSphere administrators with real-time visibility into container cluster consumption, health, and configuration status.

Actions taken by developers using native Kubernetes to self-provision development resources will be immediately visible to VMware administrators as part of their vCenter inventory and be accessible by vRealize Automation, vRealize Operations, and vRealize Log Insight. This permits VM administrators to proactively manage infrastructure operations across multiple development teams and logical applications in multicloud environments.

Challenges

Most enterprises will run a mix of containers and VMs for the foreseeable future and will rely on a mix of on-premises, hosted, and public cloud platforms. This will create the need for organizational change, investment in new tools, and design of new processes and will require traditional VM administrators, cloud managers, and Kubernetes administrators to collaborate closely.

Infrastructure and operations executives transforming their organizations should learn how their internal software development teams are planning to modernize application development processes and understand how and when those evolving application architectures will impact infrastructure management and security. They will also need to update governance and policy development programs to ensure close collaboration across IT, development, and line-of-business (LOB) roles to ensure that configuration and security policies align with business priorities.

Conclusion

IDC expects that by 2022, 70% of enterprises will deploy unified VMs, Kubernetes, and multicloud management processes and tools as they work to standardize, streamline, and scale rapidly changing applications and workflows. Even in uncertain times, enterprises need to invest in tools that will help reduce costs, increase productivity, and enable the company to better engage with customers while maintaining agility and security. VMware customers that expect Kubernetes to be part of their modern application architecture should be thinking ahead to ensure consistent configuration control and application performance as the number and diversity of clusters grow across multiple Kubernetes distributions.

About the Analyst

Mary Johnston Turner, *Research Vice President, Cloud Management*

Mary Johnston Turner is Research Vice President for Cloud Management, part of IDC's Infrastructure and Operations Management software research team. Her research focuses on emerging software and solutions for cloud, container and DevOps IT operations, cost optimization, automation, performance, and analytics. She contributes to vendor analysis, enterprise IT buyer advisory, and custom consulting activities.

MESSAGE FROM THE SPONSOR

VMware Tanzu

VMware Tanzu is a family of products and services for modernizing applications and infrastructure with the goal of delivering better software to production continuously. The portfolio simplifies multi-cloud operations, while freeing developers to move faster and access the right resources for building the best applications. To learn more about Tanzu, visit ***https://tanzu.vmware.com/***

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.