Five Best Practices for Improving Cloud Native Platform Operations

Get Started

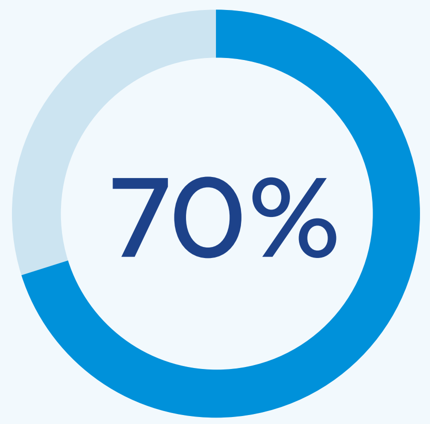
Introduction

To remain competitive in today's ever-changing IT landscape, organizations are making app modernization a top priority. Most enterprises are taking advantage of multiple cloud platforms and services to facilitate this, with 76 percent using two or more clouds today, and 86 percent planning to by 2023.[1]

While I&O is always under significant pressure to optimize costs, a focus on delivering innovation faster is taking center stage, especially for technology teams that report directly to the business.

At the same time, it is extremely difficult to secure, run and manage modern apps at scale. With hundreds of cloud users across the distributed enterprise consuming thousands of different services across multiple clouds, the scale of operations is beyond the complexity that traditional tools or processes can handle.

This ebook outlines five best practices for improving your organization's cloud native operations.



By 2024, cloud native apps will increase to 70 percent from 10 percent of all apps in 2020.[2]

[1] HashiCorp. "HashiCorp State of the Cloud Strategy Survey: Welcome to the Multi-Cloud Era." 2021.

[2] IDC. "IDC FutureScape: Worldwide IT Industry 2021 Predictions." October 2020. Doc # US46942020.

1. Establish a Cloud Center of Excellence

When it comes to driving success in the public cloud, many companies find that the biggest hurdle they must overcome is not related to technology but to people and processes. Leading organizations are establishing a formalized Cloud Center of Excellence (CCoE)—also known as a cloud business office, cloud strategy office or cloud program office—consisting of a cross-functional team tasked with supporting and governing the execution of the organization's cloud strategy. This team usually comprises finance operations practitioners, cloud operations, platform operations, security architects and line-of-business leaders.

If your organization does not have a CCoE in place, this is your first step toward improving cloud native operations.

Look for a leading solution that can deliver intelligent insights to help you optimize costs, improve governance and strengthen your cloud security posture.

The CCoE is responsible for three areas of excellence:

Cloud financial management

Cloud operations

Cloud security and compliance

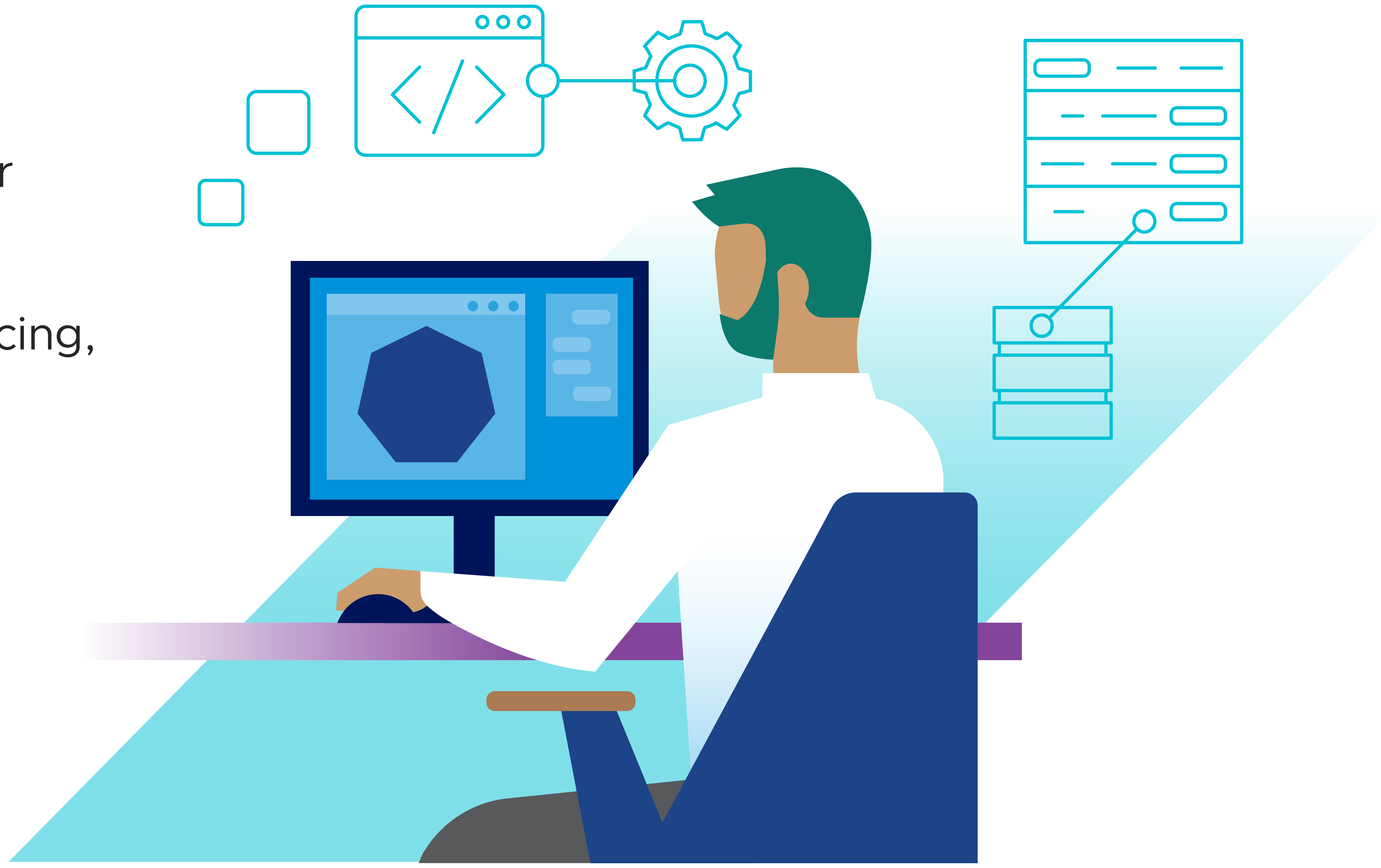
2. Standardize on a Kubernetes platform

Even as container adoption goes mainstream, provisioning and managing a distributed container infrastructure at scale is complex and prone to inconsistencies and inefficiencies. In addition, managing security and traffic for distributed applications that reside in multi-cloud environments requires capabilities beyond that of traditional, perimeter-based approaches.

Leading solutions are available to simplify container management with tools, automation and data-driven insights that boost developer productivity, secure applications and data, and optimize infrastructure performance across all your clouds.

To streamline provisioning and management, implement solutions that provide:

- A consistent Kubernetes runtime across on-premises, public clouds and at the edge
- A centralized management plane for simplified, multi-cloud, multi-cluster management
- Full-stack observability across container infrastructure across clouds
- End-to-end connectivity and security for distributed applications
- Enterprise-grade, integrated load balancing, ingress and container networking



3. Gain visibility into the entire cloud environment

To improve cloud native platform operations, it is critical to have visibility into cost and security across your entire cloud environment. Cloud service providers offer native monitoring tools that can be helpful to an extent but have limitations, especially when it comes to getting detailed context and real-time, unified visibility across hybrid cloud or multi-cloud environments.

When evaluating a cloud management solution for your business, keep a few questions in mind in terms of visibility:

- Does it provide granular visibility across different workload environments?
- Can it show relationships and dependencies between cloud services, not just in isolation?
- How often is data updated? Weekly, daily or near real-time?
- Can I visualize information by category—projects, cloud providers, teams and so on?
- Can it track and optimize my cloud spend?

In addition to having the right tools for visibility into your infrastructure, it is important to have a coordinated approach to collecting, organizing and analyzing your data. As a best practice, implement consistent tagging policies by application, owner, resource, department and so on to break down reliable information by the categories most important to you.

VMware cloud native platform ops at a glance

- ✓ Full-stack visibility
- ✓ Consistent operations at scale
- ✓ Intrinsic security

4. Detect security risks and misconfigurations

Security is the greatest obstacle to achieving an ideal multi-cloud state.[3] However, after you have attained complete visibility of your cloud environment, you can more effectively detect risks and misconfiguration vulnerabilities.

Many cloud security detection tools provide isolated information. For example, they can show that within a security group, a resource type is not compliant with a certain rule. But this information does not provide insight into the level of risk, how it is connected to other resources, or recommendations for next steps.

Suffice to say, security and traffic management for distributed apps that reside in multi-cloud environments require capabilities beyond that of traditional, perimeter-based approaches.

To better prioritize security issues and make your job easier, look for a leading multi-cloud security solution that can

- Visualize cloud resource relationships and misconfigurations in context
- Detect security risks in real time across cloud platforms
- Track progress for detections and remediations
- Secure the container lifecycle in development and production
- Offer application and data-level security policies
- Enforce networking, security and compliance requirements

[3] VMware, Inc. "VMware FY22 H1 Benchmark."

5. Remediate issues with automation

With the rate at which workloads are deployed in the cloud, automation is key when it comes to operations, performance, governance and security.

As a best practice, address cloud security policies through fully automated actions that apply universally across cloud teams and resources. Examples include policies that deny accidental changes to baseline security monitoring controls or those that require boundary permissions for all users and roles. The policies you choose to automate, and at which level, depend on your organization. The CCoE is responsible for defining where to automate policies and where to use manual actions.

From an operational standpoint, automation enables consistent multi-cloud and hybrid cloud operations, identifies bottlenecks and accelerates continuous application and infrastructure optimization. And from an application development perspective, developers can use the frameworks and tools they prefer and plug into an automated, secure software supply chain to deliver their application to production.

Address multi-cloud challenges with modern tools

Today's organizations adopting multi-clouds and Kubernetes face challenges like siloed development and management, slow time to production for new applications, and difficulty optimizing costs, security and connectivity of cross-cloud apps at scale.

This complexity goes beyond traditional tools or processes. Fortunately, there are modern tools designed to address multi-cloud challenges from both an infrastructure and application perspective.

CloudHealth® by VMware is a robust multi-cloud management platform that simplifies financial management, streamlines operations, and improves cross-organizational collaboration through consolidated visibility and reporting across your entire cloud environment.

CloudHealth Secure State is an intelligent cloud security and compliance platform that helps reduce risk and protect millions of cloud resources by remediating security misconfigurations and scaling best practices at cloud speed.

VMware Tanzu® for Kubernetes Operations provides the foundation for building, operating and managing a modern, Kubernetes-based container infrastructure across multi-cloud. It simplifies provisioning and management of Kubernetes with tools, automation and data-driven insights to boost developer productivity, secure applications and data, and optimize infrastructure performance across your entire multi-cloud IT estate.

Transform your business, not just IT
VMware modernizes the world's biggest companies. Wherever you are in your multi-cloud journey, let us lead you through the next stage of your transformation. Visit tanzu.vmware.com/why-tanzu to schedule a demo.

As a primary contributor to the Cloud Native Computing Foundation, **VMware is the most trusted vendor** for enterprise workloads running across clouds, according to Management Insights.

Source: VMware, Inc. "FY22 VMware Workloads Tracker, Management Insights." January 2022.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001

Item No: 6890-VMW-BEST-PRACTICES-CLOUD-NATIVE-PLATFORMS-EBK_R3-20220630 6/22