White Paper: **December 2022**

Top 5 Kubernetes Operations Challenges and How to Mitigate

What security, infrastructure, and operations team leads need to know

vmware®

Table of Contents

The State of Kubernetes in 2022 Survey[2], published by VMware, also shows hypergrowth in the number of clusters deployed, with almost 30% of respondents indicating that they have more than fifty clusters today.

Introduction

The latest CNCF Annual Survey[1] from the Cloud Native Computing Foundation indicates that 96% of organizations are either using or evaluating Kubernetes—a record high since this survey began in 2016. The State of Kubernetes in 2022 Survey[2], published by VMware, also shows hypergrowth in the number of clusters deployed, with almost 30% of respondents indicating that they have more than fifty clusters today. Moreover, multi-cloud continues to gain ground as the predominant target infrastructure. According to nearly half of The State of Kubernetes survey respondents, Kubernetes clusters are running across multiple clouds.

However, the rapid proliferation of Kubernetes clusters across disparate clouds exacerbates operational challenges. This whitepaper describes and provides steps for eliminating the top five Kubernetes operational challenges based on common customer scenarios. We especially focus on customers running many clusters across multiple clouds and define solutions from VMware Tanzu that have helped those customers mitigate their challenges.

1: Cluster lifecycle management requires a lot of effort

One of the immediate challenges of operating your Kubernetes clusters is keeping up with the fast release pace of upstream Kubernetes and making sure each of your cluster types can be quickly provisioned and scaled. In addition, it is critical to ensure upgrades and patching are correctly performed, at the appropriate time, and without disrupting the existing workload.

Up until the 1.22 release, upstream Kubernetes followed a quarterly release cycle. Since April 2022, the releases have slowed down, but Kubernetes still releases updates three times a year, not to mention the numerous patch releases that drop monthly. Add to that the critical bug fixes that can take place anytime outside of those "normal" release cycles, leading to a plethora of actions that demand your time.

This relentless Kubernetes release pace, driven by a prolific, global, open-source community, is one of the key factors contributing to Kubernetes' dominance and management complexity. For your operations team, it can become daunting to keep pace with all these releases in order to deliver the latest features and functions to your applications team. More importantly, you also need to ensure your clusters are functioning properly and securely.

The amount of management work involved will multiply if you run many clusters across many environments for many teams. Managing it manually can be both time consuming and error-prone, making it essential for you to use automation to help tackle this challenge. You will need tools to help you manage the cluster lifecycle smoothly and automatically, and it is better if your Kubernetes platform has built-in automation so you do not need to develop and maintain any tooling separately.

1 "CNCF Annual Survey 2021," Cloud Native Computing Foundation, February 2022.
2 "The State of Kubernetes in 2022," VMware, 2022.

2: Cluster observability becomes more important with modern applications

Highly distributed, cloud native applications create monitoring challenges at a much greater order of magnitude than traditional monitoring tools can handle. When you have hundreds or thousands of containers running, often across multiple environments or clouds, potential visibility gaps and even blackouts may occur if the traditional monitoring tools cannot keep up with the rate of container changes or updates.

According to the VMware 2022 State of Observability Survey[3], more than 40% of survey participants say that one application request can touch more than twenty-five different technologies.

In addition, the adoption of cloud native services and APIs is skyrocketing. According to the VMware 2022 State of Observability Survey[3], more than 40% of survey participants say that one application request can touch more than twenty-five different technologies. Having an accurate visual representation of an application map and communication between microservices, as well as topology discovery, is essential.

Moreover, the adoption of Kubernetes and the DevOps practice enables organizations to push code to production much faster and more frequently, sometimes even daily. Pushing code to production so often requires real-time visibility for developers, operations, and site reliability engineering teams. This helps teams assess the immediate impact of those code pushes and whether they need to roll anything back.

All of the above is prompting organizations to rethink monitoring. With the introduction of Kubernetes and the increasing number of applications running on it, you will inevitably need to bring in new monitoring tools to help address the visibility and monitoring challenges. You also need an observability tool that can provide all levels of visibility from infrastructure all the way to application components. This will help your operations and DevOps teams monitor, observe, and analyze application and infrastructure health, as well as performance at scale across clouds.

3: Securing Kubernetes clusters can be challenging

Security has been ranked as one of the top challenges of running and managing Kubernetes by many Kubernetes-related surveys. According to The State of Kubernetes survey, meeting security and compliance requirements is the number one Kubernetes challenge. Among various other security concerns, applying policies consistently across clusters and teams and controlling access to clusters are ranked as the top two security concerns.

Why is securing Kubernetes so hard? Securing traditional applications is not an easy task, and the distributed and ephemeral nature of cloud native applications adds tons of complexity. There are also many more layers in the Kubernetes stack that you need to secure, each of which comes with its own security

3 "The State of Observability 2022," VMware, 2022.

considerations. Adopting DevOps practices often translates to a much faster and more automated application delivery process but can render most traditional security measures inadequate or obsolete. In addition, general Kubernetes talent is a highly sought-after resource in the talent market today, not to mention the even smaller subset of Kubernetes security personnel.

In the Kubernetes or cloud native world, the buzzword DevSecOps suggests security should be an integrated part of the entire platform, solution, and process. It is risky for security to be a separate add-on step outside the loop rather than being integrated into every step of your software development and delivery process from code, test, to deploy to infrastructure. It is preferable to have security automation baked into your overall platform and process, so you can execute during the fast release cycle.

4: Delivering consistency to developers is challenging with Kubernetes

According to The State of Kubernetes survey, 46% of the organizations are currently running Kubernetes across multiple clouds, which is a 10% increase from the 2021 survey.

Consistency becomes an increasingly formidable challenge when more and more enterprises start to run Kubernetes-based applications across multiple clouds. According to The State of Kubernetes survey, 46% of the organizations are currently running Kubernetes across multiple clouds, which is a 10% increase from the 2021 survey.

This multi-cloud reality poses a big challenge for Kubernetes operators. How do you ensure consistency across your entire Kubernetes footprint, no matter where your cluster lives? How can you offer your developers a consistent user experience while they consume Kubernetes from different clouds or vendors? More importantly, how can you ensure the proper security and compliance requirements are being met, no matter where your workloads run?

For this purpose, you will need a management platform that aggregates and consolidates your disparate Kubernetes presence across environments. This tool should help abstract a lot of operational tasks that are specific to different clouds and distributions, allowing you to provide consistent cluster behavior for both developers and operators. Operational tasks such as cluster lifecycle management, configuration and policy management, security management, access management, and more can, and should be, centralized.

5: Finding Kubernetes skills is difficult

Last but not the least, Kubernetes operations are challenged by skills shortages. Although Kubernetes is quickly maturing and more talent is drawn to this space, it is still hard to find the right Kubernetes expertise in the market. Many organizations need extensive integration with existing systems, tools, and processes and require a certain degree of customization to meet business imperatives. In addition to mastering Kubernetes, a highly skilled Kubernetes team member needs to be able to seamlessly navigate your existing IT ecosystem.

According to The State of Kubernetes survey, this year's number one challenge when selecting a Kubernetes distribution remains inadequate internal experience and expertise, chosen by 51% of respondents.

Therefore, it is not surprising to see many organizations struggling—to bring existing staff up to speed (and keep them there)—and bring in new hires with the required Kubernetes skills. According to The State of Kubernetes survey, this year's number one challenge when selecting a Kubernetes distribution remains inadequate internal experience and expertise, chosen by 51% of respondents. The number two challenge also stayed the same: hard-to-hire needed expertise (37%).

In other words, despite fast Kubernetes adoption, the expertise shortage generates an urgent need for organizations to fill the knowledge gap. You will need practical Kubernetes solutions to get you up and running quickly with more automated operations. Moreover, you will need top-notch enterprise support to assist you with running and managing your new platform. Professional services can help bridge the knowledge gap and provide the necessary training, best practices, and guidance to quickly establish that platform, customize it to meet your business imperatives, and support your platform operations team. No wonder 40% of The State of Kubernetes survey respondents indicated that the availability of commercial support or professional services was the top criterion for choosing a Kubernetes distribution.

How VMware Tanzu for Kubernetes Operations can help

Centralized and automated lifecycle management

Tanzu for Kubernetes Operations includes a full Kubernetes runtime platform which greatly simplifies the deployment and operations of Kubernetes clusters, including cluster lifecycle management. It offers built-in cluster lifecycle management capabilities and leverages cluster API, a Kubernetes sub-project focused on providing declarative APIs and tooling to simplify provisioning, upgrading, and operating multiple Kubernetes clusters. Cluster API is where the community is heading when it comes to Kubernetes cluster management.

If you are operating multiple clusters, Tanzu for Kubernetes Operations also provides a management control plane where you can centralize all your clusters and manage their lifecycle. Tanzu for Kubernetes Operations helps further reduce the operational burden while significantly increasing efficiency.

Unified, global observability for Kubernetes clusters

Tanzu for Kubernetes Operations offers full stack Kubernetes observability. It delivers out-of-the-box integrations with all the popular Kubernetes environments so operations teams can observe any Kubernetes cluster and any workload across multiple clouds. With Tanzu for Kubernetes Operations, you can immediately observe Kubernetes environments and auto-discover Kubernetes workloads. Customizable dashboards provide full-stack metrics from all Kubernetes layers—clusters, nodes, pods to containers, and system metrics. Once discovered, you can apply security to the service-to-service connections in those clusters.

With Tanzu for Kubernetes Operations, your platform operations team and DevOps team can quickly troubleshoot applications, Kubernetes, and infrastructure.

With Tanzu for Kubernetes Operations, your platform operations team and DevOps team can quickly troubleshoot applications, Kubernetes, and infrastructure.

Enhanced and compliant Kubernetes security

Tanzu for Kubernetes Operations addresses security through multiple layers. The Kubernetes runtime uses hardened node images to strengthen the overall security stance. It also includes a built-in container registry that can scan container images for vulnerabilities before they are deployed. In addition, platform operators can use its central management plane to consistently apply access, security, and network policies across clusters and teams, to help with configuration and policy management as well as identity and access control. Tanzu for Kubernetes Operations also provides service mesh capabilities across clusters and clouds, which teams can utilize to build data security policies and bake security testing into their existing DevOps tool chain. Further, Tanzu for Kubernetes Operations offers application and data-level security policies, such as attribute-based access control (ABAC) policies, end-to-end encryption policies, API segmentation, parameter validation, and threat protection policies.

Improved cluster consistency for reliable routes to deployment

Tanzu for Kubernetes Operations includes a centralized management plane to provide a consolidated management experience for platform operators, increasing the consistency of multi-cloud Kubernetes deployments and distributions. With this management plane, platform operators can centrally manage the lifecycle of the VMware Tanzu clusters across multiple clouds, which makes provisioning, scaling, and upgrading of clusters much easier. Operations teams can also utilize GitOps to improve the consistent delivery of clusters through the management plane, offering a more consistent route to production for developers to move more quickly. Furthermore, the management plane has a powerful policy engine that enables consistent and scalable guardrails on your Kubernetes clusters across clouds and distributions. For example, operators can consistently and centrally manage access, security, data protection, registry, network, quota policies, and even custom policies, and apply them to a group of clusters or namespaces in any environment across clouds.

VMware Tanzu offers training and support for digital transformations

The Tanzu for Kubernetes Operations platform is built with automation to simplify every step from deployment to managing Kubernetes. In addition, enterprise-grade support for the full platform and its open-source components, along with world-class professional services, can help accelerate your adoption of Kubernetes and get you up and running quickly.

Tanzu Activation Services, is designed specifically for Tanzu for Kubernetes Operations customers, and is delivered by the VMware Tanzu Labs team, which comprises hundreds of the world's top Kubernetes consultants, PMs, and engineers. VMware Tanzu Labs personnel can assist you with installation, configuration, and integration of your Tanzu for Kubernetes Operations platform to accelerate onboarding, in addition to migrating a minimum of one application to your new Kubernetes platform.

Next steps

Kubernetes has gone mainstream, and no matter the industry or the size of your organization, you are likely to face these challenges when operating the Kubernetes platform that runs your most mission-critical applications. Choosing the right technology, the right platform, and the right partner to start this journey is critical in terms of minimizing the impact of any operational challenges moving forward.

To get started, we invite you to reach out to your VMware Tanzu sales representative to schedule a meeting.

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