Techstrong Research

PulseMeter

Sponsored by KASTEN by Veeam

In collaboration with aws

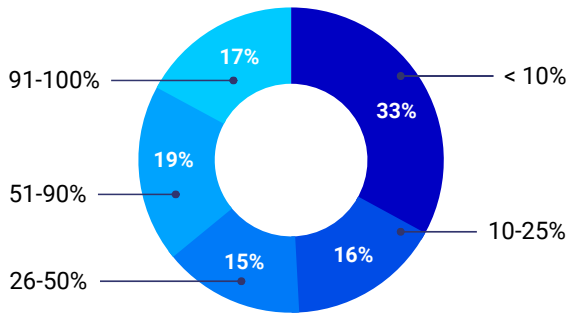
Kubernetes is gaining steam, with 36% of respondents running more than 50% of their business-critical apps on Kubernetes (K8s). As we projected in the Techstrong Research 2023 cloud-native trends report, tool maturity and adoption will accelerate enterprise K8s use and application modernization. Backup, restore and disaster recovery capabilities remain vital for enterprises to protect critical application data platformed on Kubernetes.

Current Kubernetes backup is often a mix of manual scripts, on-premises solutions, cloud-based solutions, open source and cloud provider offerings. With this many options, organizations need to think about how to perform K8s backup consistently in an environment complicated by the number of cloud platform options (including on-premises). Moreover, it's also important to take a considerate and planned approach to K8s backup with native and vendor-agnostic tools, figuring out the mix of real-time, daily, ad-hoc and weekly backups depending on the criticality and sensitivity of the protected data.

In mid-2023, Techstrong Research polled our community of DevOps, cloud native, cybersecurity and digital transformation readers and viewers to take their pulse on Kubernetes backup and data protection trends. Despite the clear momentum for Kubernetes adoption, there isn't a consensus on the best approach to cover backup and recovery for all platforms and distributions. The most significant challenge respondents face is addressing the skills gap (29%), with security (19%) and monitoring/troubleshooting (18%) also creating problems. When it comes to platform and distribution support, the big three cloud platforms dominate. Still, there are enough on-premises K8s deployments that it's worth paying attention to whether workloads are moving back on-premises, likely due to cost concerns.

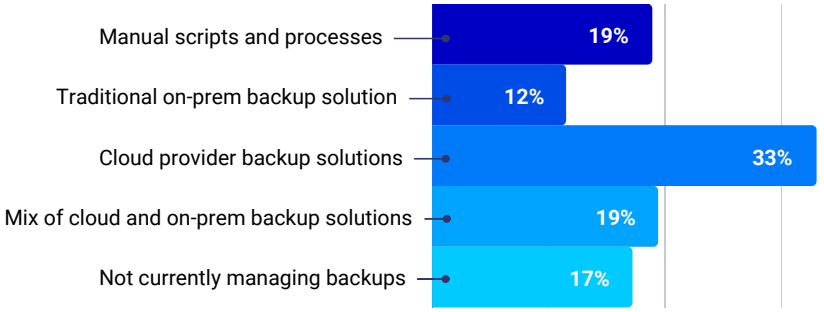
What % of your business-critical apps are running on Kubernetes?

36% of respondents run a majority (over 50%) of critical apps on Kubernetes. That number will grow substantially over the next 18 - 24 months.



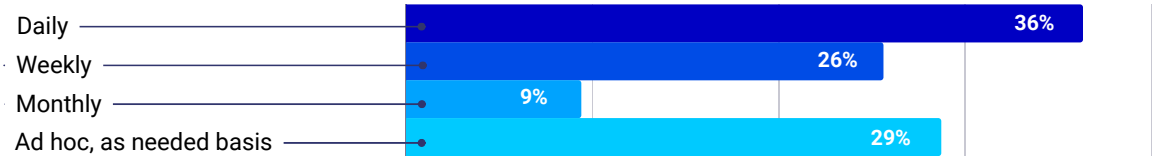
How do you currently manage the backup and disaster recovery process for your Kubernetes workloads?

Responses split evenly between not backing up and manual processes, a mix of cloud and on-premises backup and traditional solutions, and cloud provider backup solutions. This mix of solutions creates an opportunity for more effective, modern solutions as more business-critical workloads move to containerized environments.



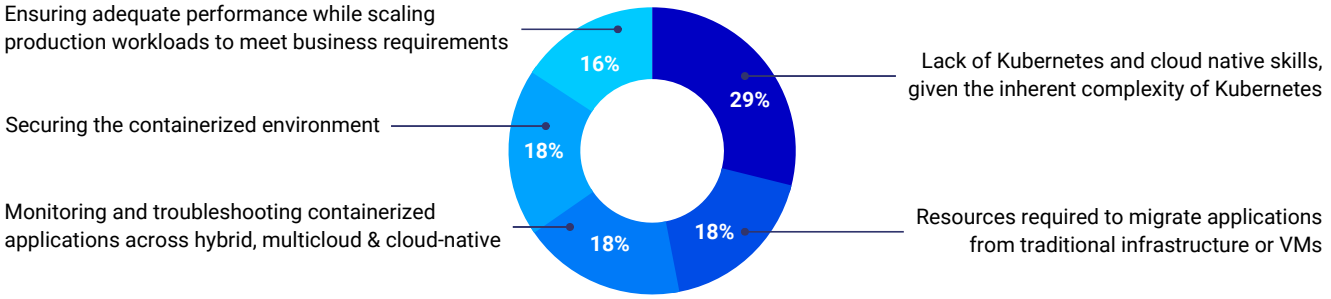
How often do you perform backup operations (full or incremental) for your Kubernetes workloads?

A majority of respondents do either daily or weekly backups, and a surprising number (29%) do backups in an ad hoc manner. That's not reliable or consistent enough for enterprises to support production workloads.



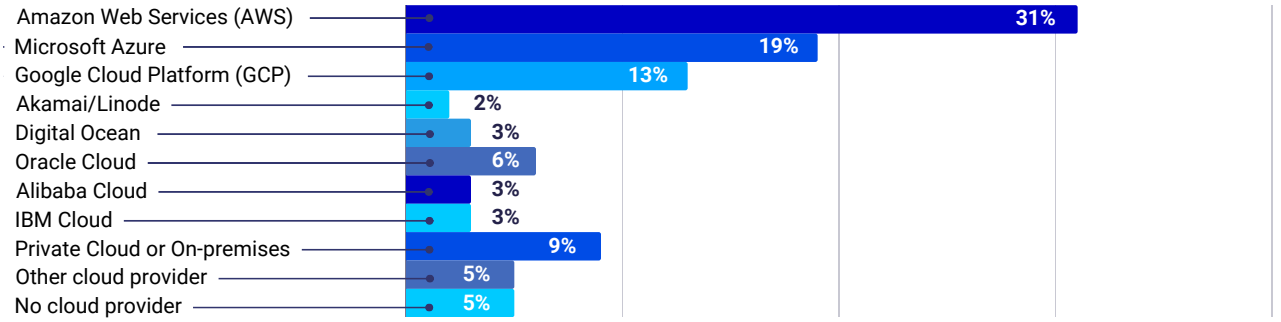
What challenges does your organization face when moving business-critical applications to containers and Kubernetes?

The Kubernetes skills gap (29%) is the largest hurdle for companies considering moving business-critical apps to Kubernetes. Security and monitoring/troubleshooting are also significant challenges.



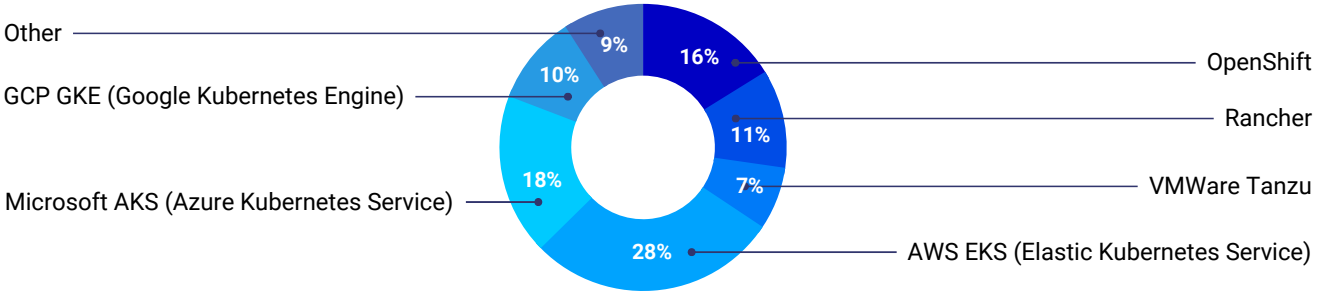
Which cloud platform(s) do you need to support for your Kubernetes backup and restore strategy?

AWS, Azure and Google Cloud remain the dominant cloud platforms for Kubernetes backup and restore (63%). Private cloud was only listed by 9% as a required platform, but that means on-premises is not dead and may make a rebound as cost considerations push workloads back to the corporate data center.



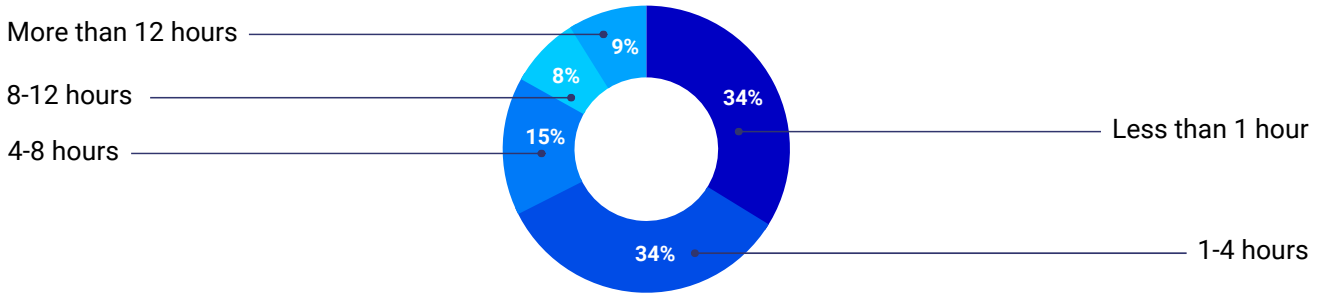
Which Kubernetes platforms do you need to support for your Kubernetes backup and disaster recovery strategy?

Drilling into specific Kubernetes platforms, managed services, EKS (28%) and AKS (18%) are the most popular. OpenShift (16%) and Rancher (11%) are next. Given the skills challenges, this is predictable and driving interest in managed services of all types.



What is your target mean-time-to-recover/restore (MTTR) for your Kubernetes workloads in case of a disaster or system failure?

68% of respondents target a MTTR of less than four hours, split evenly between less than one hour and one to four hours. The remaining one-third (32%) surprisingly accept an MTTR of more than four hours.



What are the most important features to have in a Kubernetes backup & restore solution?

While organizations want reliability and security, respondents indicated that useability and frictionless integration with current tools were more important.

Techstrong Research Analyst View

What's clear from the PulseMeter poll is that the big cloud platforms are the preferred deployment environment for mission-critical Kubernetes applications. Between the big three (AWS, Azure, GCP) and the use of managed services for Kubernetes (EKS, AKS), organizations are looking for someone else to manage the hardware and environment. Yet, on-premises is the next most-popular platform, so private clouds are still a thing.

From a tooling standpoint, having to support both cloud-based and on-premises environments and multiple distributions means the best leverage will come from looking for a backup "utility" that can support a variety of platforms and distributions, providing cloud-agnostic data protection. Depending on the size and scope of the environment, open source technology may work, but open source requires additional work given the lack of automatic app discovery, a simple UI, monitoring, alerting & reporting and multi-cluster management.

In terms of challenges, lack of skills continues to be the most significant impediment to wider adoption. Thus, top feature requirements like pre-built integrations and an easy UI experience reflect the need to ease the learning curve. Security and monitoring/troubleshooting are also listed as significant challenges, which align with the next two feature requirements of scalability/reliability and strong encryption/data protection. To support the further deployment of mission-critical apps on K8s, organizations need skilled resources, agnostic and easy-to-implement/operate tools, and assurance that their data will be protected and available.

The bottom line is that organizations need to think in terms of a "backup utility" supporting consistent K8s backup across platforms and cloud providers/on-premises, so business leaders can be assured business-critical apps will be secure, resilient and scalable.