Tanzu Data Protection Powered by NetBackup

Software-defined data protection at scale, on-premises and in the cloud.

The current stage of IT transformation features rapid adoption of Kubernetes (K8s) in the enterprise. Containers have become the de facto standard for implementing microservices-based architectures to build web-scale applications with shorter development cycles. Organizations are choosing to adopt Kubernetes for the benefits of containers, better utilization of resources, scalability, the power of orchestration and for the value of the distributed cloud. However, a Kubernetes environment is no less susceptible to risks—ransomware attacks or human errors have the potential to compromise the underlying infrastructure, which in turn will negatively impact or disable Kubernetes outright. This vulnerability is why Kubernetes data protection is important. A transformation gap is formed when the ability to manage risks is misaligned with the expectation these apps are up and running no matter what.

KEY TAKEAWAYS

NetBackup Kubernetes for VMware Tanzu:

- Simplifies and optimizes management with K8s native integration and agentless protection.
- Is RBAC-enabled for secure access.
- Provides efficient data management with self-service.
- Delivers unified data protection from edge to core to cloud.

THE POWER OF VMWARE TANZU AND VERITAS NETBACKUP

Enterprises rely on VMware Tanzu to provide a consistent, conformant Kubernetes infrastructure environment across on-premises and multiple clouds. Like other workloads, Kubernetes still exists on infrastructure, whether it is physical, virtual or cloud. Each of these infrastructure types is vulnerable to risks, including ransomware, network outages, natural disasters and human error.

Veritas understands the importance of protecting Kubernetes deployments. The ability to back up and restore across clusters ensures outages, errors and downtime are easily avoidable and application resiliency and portability remain constant. In addition to what we do today to protect workloads from edge to core to cloud, we extended our industry-leading data protection solution, Veritas NetBackup™, to include Kubernetes support, eliminating the need for point solutions. This approach gives Tanzu customers confidence to create their mission-critical workloads and modern digital applications while leveraging their existing VMware investments with NetBackup's comprehensive data protection tools in a sustainable cost model. NetBackup for Kubernetes provides native protection for Tanzu by providing optimized, application-centric, unified protection.

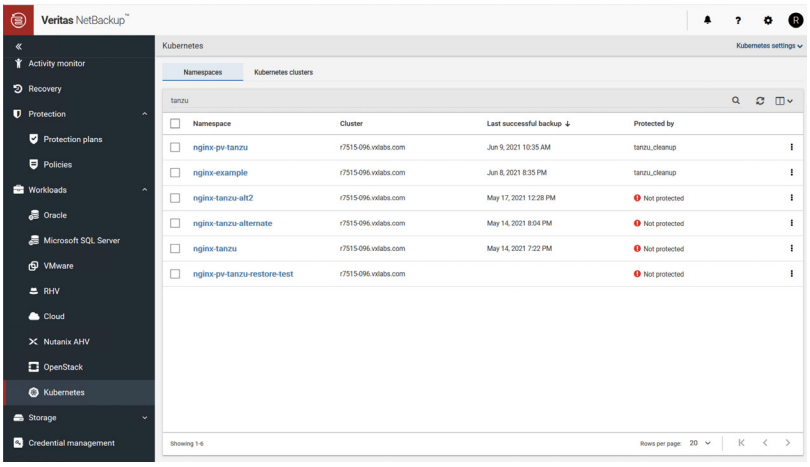

Figure 1. NetBackup's automatic discovery of Kubernetes namespaces on a VMware Tanzu cluster.

OPTIMIZED PROTECTION

NetBackup for Kubernetes is platform-native and is specifically designed to protect and optimize Kubernetes environments using native Kubernetes constructs. We leverage Helm charts for deployment, a NetBackup

Kubernetes Operator for integration with the Kubernetes cluster and integrate with Velero to facilitate Kubernetes-native snapshots using the Container Storage Interface (CSI).

The intuitive NetBackup web interface and policy-driven backups are secured using role-based access control (RBAC) and empowers Tanzu admins with namespace-aware recovery as a service. Data protection is efficient—add a Tanzu cluster as a Kubernetes workload and NetBackup automatically discovers all user namespaces and resources within them (see Figure 1). Administrators can also define resource limits to throttle the number of concurrent data protection workflows or even change how often NetBackup queries the Tanzu cluster to identify new applications that need protection. NetBackup for Tanzu protection provides simplified management using intelligent automation to orchestrate data protection processes.

APPLICATION-CENTRIC APPROACH

With Kubernetes, you are not protecting a single container, but a complex distributed application. Because a single Tanzu application can be made up of as many as a hundred different components, it is imperative to discover all the components and their relationship to each other within the namespace (see Figure 2). Doing so ensures you can both protect and recover all these resources as a single entity. If data protection and recovery are not well orchestrated, the application may not be able to recover efficiently, which introduces risk. Containerized applications running within Kubernetes are prime targets for threats like ransomware and ensuring it is also recoverable in any situation is equally important.

NetBackup was designed for Kubernetes in its core and designed with appreciation for an application-centric approach. NetBackup provides discovery and protection of all components that make up a Tanzu application, giving you the confidence of knowing all your workloads can be recovered efficiently and quickly.

Ensuring all data protected is compliant—and in the case of corruption, recoverable to the last known good state—is the only reliable way to ensure long-term recoverability. Having a robust catalog of recovery points is crucial for an organization's success.

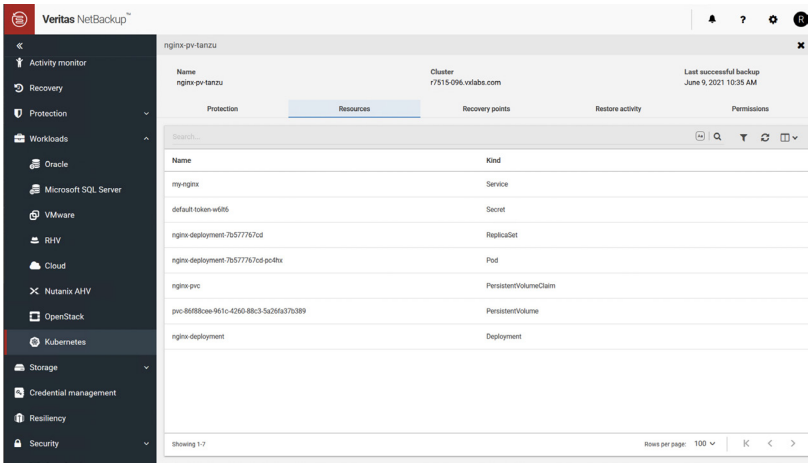

Figure 2. A granular view of resources in a Tanzu user namespace in NetBackup.

UNIFIED PROTECTION FOR THE ENTIRE APPLICATION

Tanzu upholds VMware's longtime promise of enabling organizations to run any app on any cloud. Our Kubernetes-native solution unlocks portability by allowing a Tanzu backup to be recovered to another Tanzu environment hosted in any other cloud. NetBackup for Kubernetes was fundamentally designed to unlock the power of K8s—portability and elasticity—to provide integrated data protection and resiliency. NetBackup Kubernetes protection for Tanzu ensures your data is protected and recoverable with enterprise-grade management.

HOW IT WORKS

Figure 3 shows a VMware Tanzu architecture with additional components. NetBackupKOps represents the NetBackup™ Kubernetes Operator installed into the Tanzu cluster in the same namespace as Velero. Both the NetBackup™ Kubernetes Operator container image and the corresponding Helm chart used for deployment are available from the Veritas Download Center.

Initial configuration involves exchanging API tokens and certificate thumbprints with the NetBackup server and the Tanzu cluster to facilitate secure, bi-directional communication. Once the initial configuration is completed, you can use NetBackup's web interface or RESTful APIs to build, operate and manage data protection workflows without needing to log into the backup application. Velero lets us take CSI-compliant snapshots and helps protect data to compatible S3 object storage while capturing metadata for the NetBackup catalog.

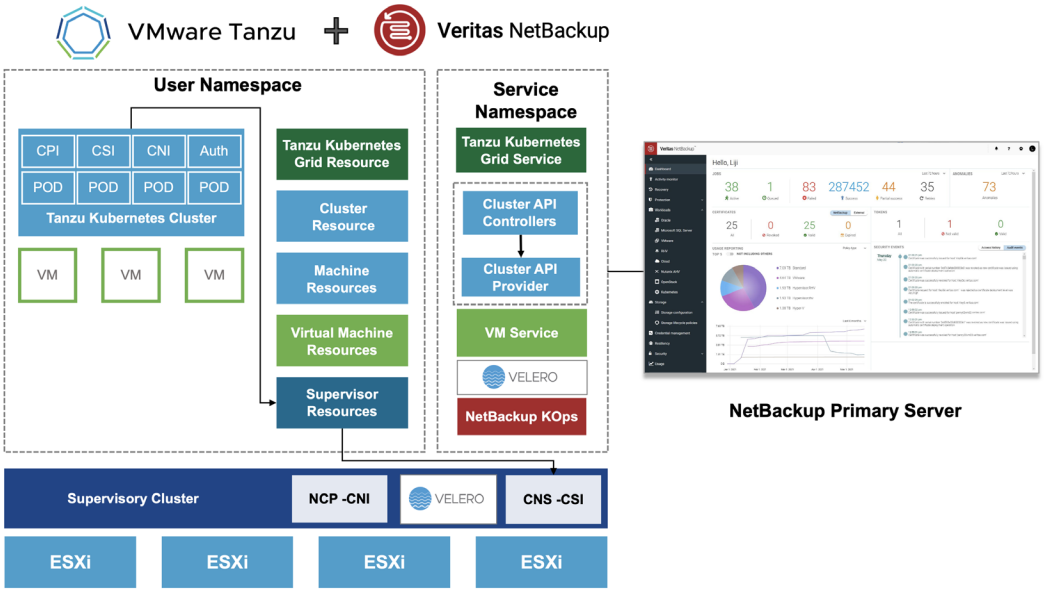

Figure 3. Derived from VMware Tanzu Kubernetes Grid Service documentation shown along with Veritas NetBackup.

From an architecture perspective, you can also configure a single Tanzu cluster for protection from one or more NetBackup primary servers. Each NetBackup primary server is also commonly referred to as a NetBackup domain. You can also use a single NetBackup domain to protect multiple Tanzu clusters.

HOLISTIC KUBERNETES-NATIVE DATA PROTECTION

VMware Tanzu bridges the gap between IT operations and developers. It gives developers secure, self-service access to fully compliant and conformant Kubernetes on-premises and in public clouds. The Veritas Enterprise Data Services Platform natively understands Kubernetes workloads and takes a holistic approach to protecting mission-critical applications deployed in this mode. With Veritas, organizations can apply the same data protection and governance policies to every workload, including VMware Tanzu.

Unlike other data protection and availability solutions for Kubernetes, NetBackup takes a unified approach that is Kubernetes-native and integrates DevSecOps processes from the beginning of the development cycle through deployment and operations. NetBackup's innovation has been extended to K8s, which means it is an integral part of the NetBackup framework.

NetBackup is built to protect Kubernetes in its core without requiring any extra licensing. It is trusted by 87 percent of the Fortune Global 500 and is fully Kubernetes-native. NetBackup for Kubernetes was fundamentally designed to give you the application-centric data protection and enterprise-grade resiliency you require. Protect your multi-tiered Kubernetes apps and DevSecOps initiatives using the NetBackup web UI or RESTful APIs for optimized data protection. Our solution is platform and storage agnostic, while leveraging cloud-native attributes designed to provide unified cross-platform recoverability.

LEARN MORE

Take full advantage of VMware Tanzu's unique Kubernetes capabilities with NetBackup and ensure the integrity of your container-based data and applications. To learn more about NetBackup for Kubernetes, visit Veritas.com/NetBackup.

Throughout the 18 years of our partnership, Veritas and VMware have strived to evolve in step with major market innovations, including hybrid and multi-cloud adoption, and today we are aligned to support the emergence of Kubernetes and cloud-native applications. To learn more about VMware Tanzu, visit VMware.com/Tanzu.

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

V1362 06/21