Kubernetes Data Protection Powered by Veritas NetBackup

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

Introduction

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 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 can 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.

Enterprises rely on Kubernetes to provide a consistent infrastructure for modern digital apps across on-premises and multiple clouds. Like other workloads, Kubernetes 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 multiple clusters and across multiple Kubernetes distributions ensures outages, errors, and downtime can be easily avoided while application resiliency and portability remain constant. In addition to what we do today to protect workloads from the edge to the core to the cloud, we extended our industry-leading data protection solution, Veritas NetBackup™, to include Kubernetes support, eliminating the need for point solutions. This approach gives Kubernetes customers the confidence to create their mission-critical workloads and modern digital applications while leveraging their existing infrastructure investments with NetBackup's comprehensive data protection tools in a sustainable cost model. NetBackup for Kubernetes provides native platform protection by providing optimized, application-centric, unified protection.

Key Takeaways

NetBackup for Kubernetes:

- Provides autonomous management with K8s native integration, agentless protection, and automatic workload protection
- Provides extensible data movement with choice of backup target, faster recovery from snapshots, and longer-term tiering of backup data
- Enables self-service K8s protection security using role-based access control (RBAC)
- Delivers fully unified data protection and ransomware resiliency, including anomaly detection and malware scanning, from edge to core to cloud

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 and a NetBackup Kubernetes Operator (KOps) for integration with the Kubernetes cluster. Morever, NetBackup integrates with Kubernetes-native snapshots using the Container Storage Interface (CSI).

The intuitive NetBackup web interface and policy-driven backups are secured using RBAC and empower Kubernetes admins with namespace-aware recovery. Data protection is efficient and automatic—add a Kubernetes cluster and NetBackup will dynamically discover namespaces and protect them with intelligent polices or labels that have been associated with a protection plan. Administrators can also configure different retention policies for each snapshot and backup copy. (See Figure 1).

NetBackup now offers administrators greater control over their application by defining which resources to include or exclude and the ability to apply resource limits. With resource limits administrators can throttle the number of concurrent data protection workflows or even change how often NetBackup queries the Kubernetes cluster to discover new applications that may need protection.

Once a snapshot is taken, NetBackup's native data mover dynamically tiers data off to the storage of your choice for duplication and ransomware resiliency.

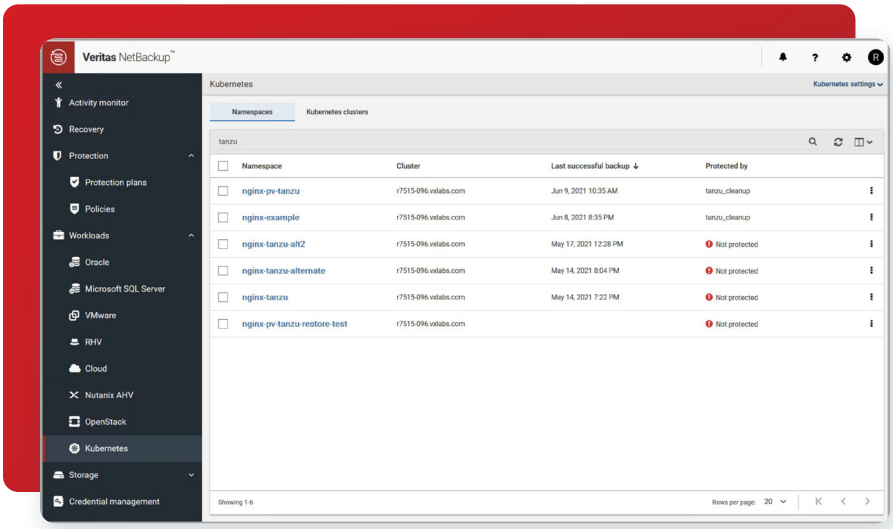

Figure 1. NetBackup's automatic discovery of Kubernetes namespaces on a Kubernetes cluster.

Application-Centric Approach

With Kubernetes, you are not protecting a single container, but a complex, distributed application. Because a single Kubernetes 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.

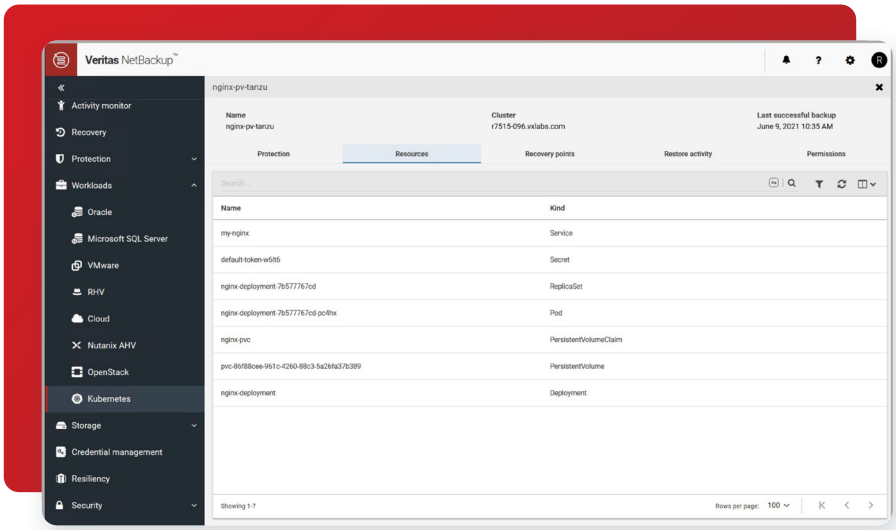

Figure 2. A granular view of the resources in a Kubernetes namespace in NetBackup.

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 Kubernetes 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 resiliency against a ransomware attack or other malicious activity.

Unified Protection for the Entire Application

Kubernetes gives enterprises the ability to bundle and run apps together in containers as well as run those apps in any cloud. Our Kubernetes-native solution unlocks portability by allowing a Kubernetes backup t to be recovered to another Kubernetes environment or distribution. NetBackup for Kubernetes was fundamentally designed to unlock the power of K8s—portability and elasticity—to provide integrated data protection and resiliency. NetBackup for Kubernetes ensures your data is protected and recoverable with enterprise-grade management—from edge to core to cloud.

Holistic Kubernetes-Native Data Protection

Kubernetes 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 protect mission-critical applications deployed in this mode. With Veritas, organizations can apply the same data protection and governance policies to every workload, including Kubernetes.

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. This design enables customers to adopt Kubernetes and containerization confidently, knowing Veritas has architected their data protection solution the right way.

How it Works

As shown in Figure 3, a Kubernetes architecture contains multiple components. When deploying NetBackup for Kubernetes, the following additional components will be installed in the cluster: the NetBackup Kubernetes Operator (KOps) container image, the corresponding Helm chart, and a data mover. These components are available from the Veritas Download Center.

Initial configuration involves exchanging API tokens and certificate thumbprints with the NetBackup server and the Kubernetes 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. NetBackup leverages native CSI snapshots, and with NetBackup's elastic data mover, snapshots can be tiered to any NetBackup-supported storage while capturing metadata for the NetBackup catalog. With the ability to recover quickly from the snapshot directly or from the backup copy, NetBackup offers administrators full ransomware protection and resiliency.

From an architecture perspective, a single Kubernetes cluster can be configured for protection from one or more NetBackup Primary Servers (also commonly referred to as a NetBackup domain). A single NetBackup domain can also be used to protect multiple Kubernetes clusters.

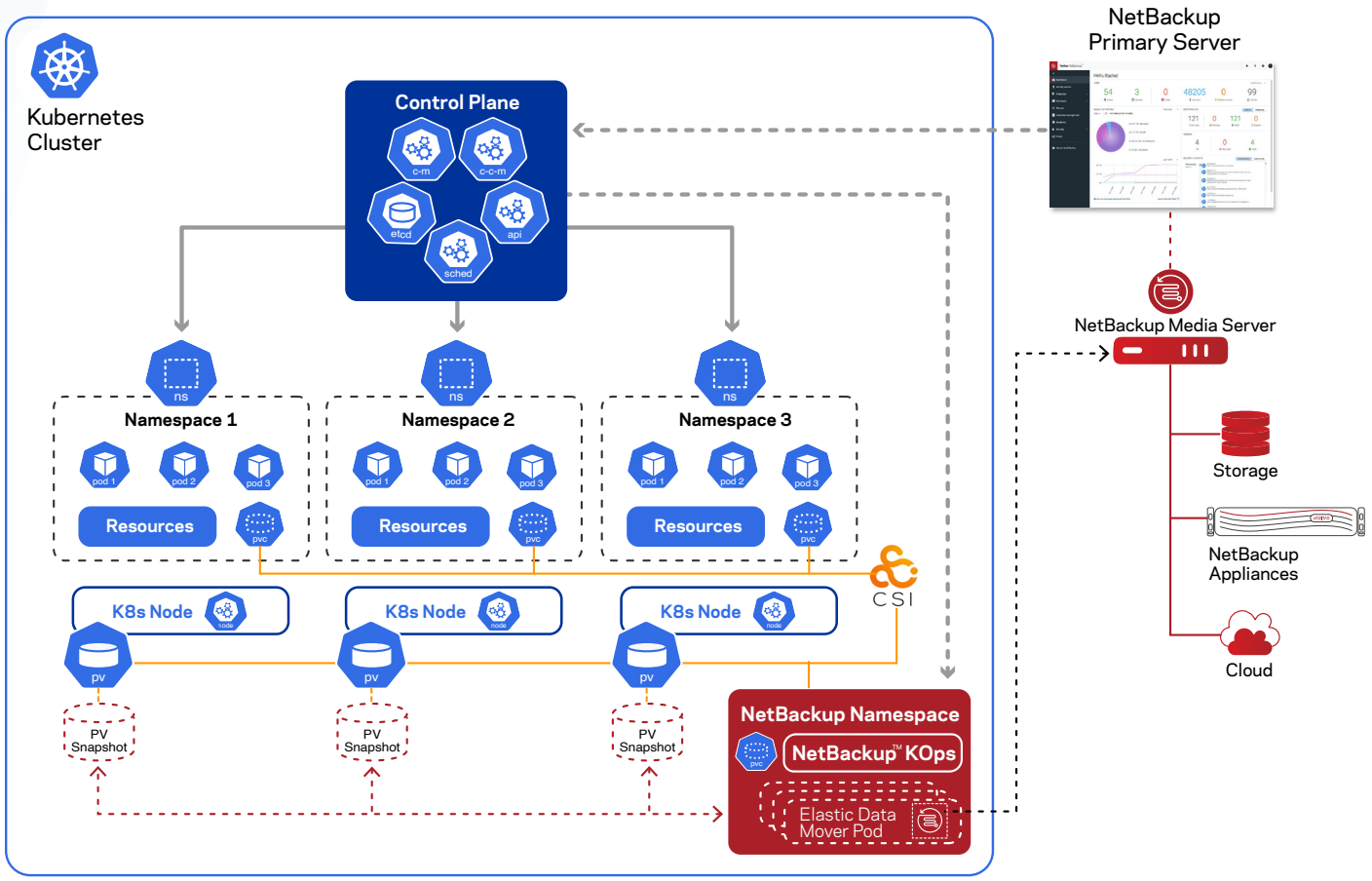

Figure 3. Kubernetes architecture showing NetBackup KOps, the NetBackup Kubernetes Operator.

Learn More

Take full advantage of the unique capabilities that Kubernetes offers and rely on trusted data protection from Veritas NetBackup to ensure the integrity of your container-based data and applications. To learn more about Veritas' solution for Kubernetes, visit https://www.veritas.com/solution/kubernetes. To learn more about Kubernetes, visit kubernetes.io.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—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.

VERITAS

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

For global contact information visit:
veritas.com/company/contact

V1401 01/22