Enterprise Storage and Data Protection for Red Hat OpenShift

An Enterprise foundation for running containerized applications with confidence.

White Paper | October 2022

Contents

Executive Summary

Containers are rapidly becoming a mainstream solution for building and running IT services that help businesses reduce management overhead and deliver new innovations. The Red Hat OpenShift Container Platform provides additional features to complement Kubernetes, making it a turnkey container platform as a service (PaaS) with a significantly improved developer and operator experience. However, OpenShift does not natively provide all the functionality stateful containerized applications need.

Veritas software-defined storage and data protection is designed to provide an enterprise foundation for your containerized applications running in OpenShift. With more than half (55 percent) of organizations actively using containers, and another 18 percent in the discovery stage[1], Veritas enables you to run your stateful containerized applications in OpenShift with several advanced features focused on three key principles:

- **Resiliency:** Enterprise-grade persistent storage for OpenShift that works with direct-attached storage (DAS) and storage area network (SAN), and has integrated disaster recovery (DR) capability that protects your containerized applications from unplanned downtime.
- **Mobility:** Easily move your applications and data across OpenShift clusters for improved resiliency, with the ability to back up and recover workloads to alternate Kubernetes distributions—including public cloud services.
- **Efficiency:** Veritas delivers a simple, intuitive operating experience that extends OpenShift functionality, giving you the performance and protection your enterprise applications need, while improving resource utilization and reducing infrastructure costs.

Veritas offers a comprehensive solution based on InfoScale and NetBackup that can help ensure your containerized applications have the foundation they need to be production-ready. This document provides an overview of how Veritas works in OpenShift with seamless integration that enables you to easily deploy and manage persistent storage and data protection for enterprise applications and services.

Solution Overview

As containers become more frequently deployed to serve a wider variety of use cases, OpenShift deployments often include several types of containerized applications, each with their own storage and protection requirements. Figure 1 shows an overview of how InfoScale and NetBackup interact with OpenShift to support storage and protection requirements for any type of application running within OpenShift.

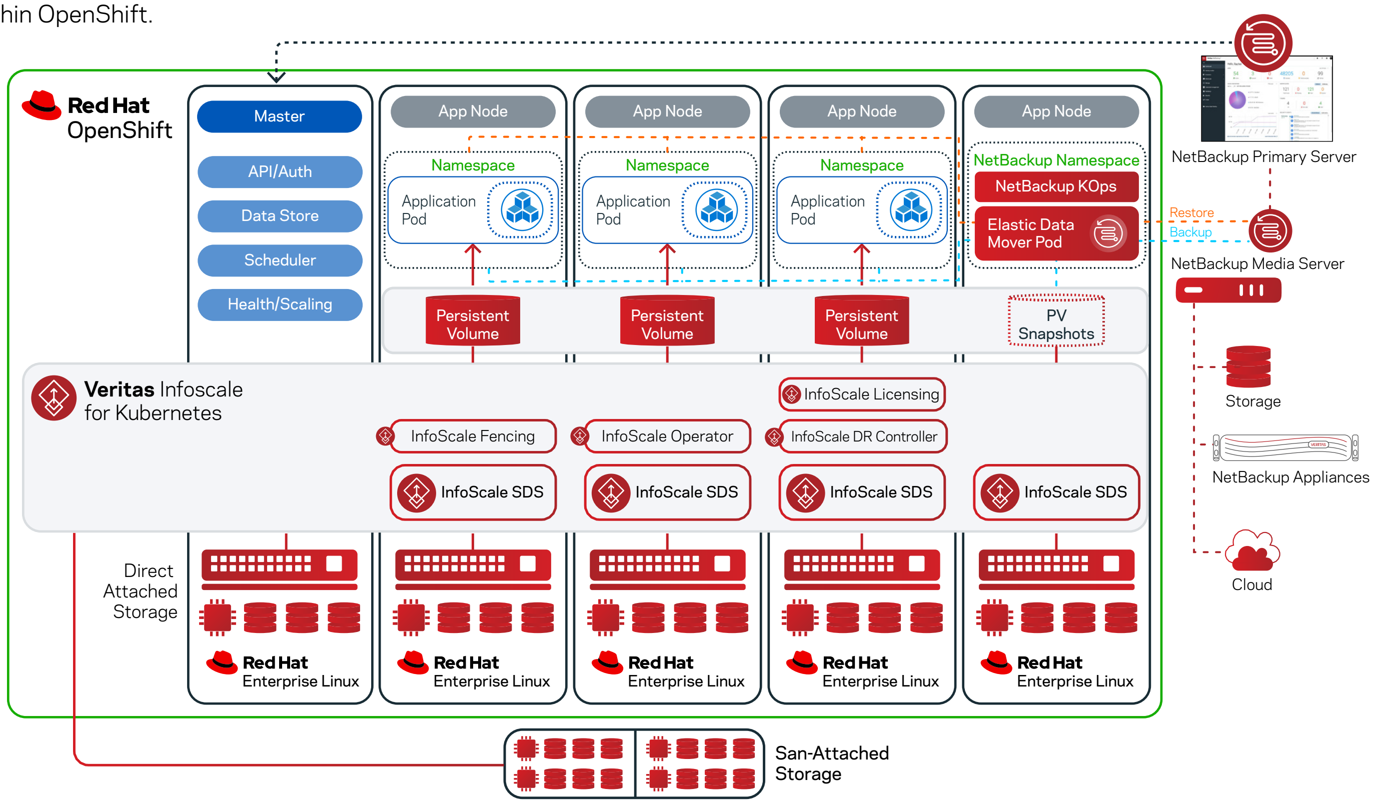


Figure 1. InfoScale persistent storage and NetBackup data protection for OpenShift clusters

The Veritas storage and data protection solution for OpenShift includes:

- **Enterprise persistent storage**—powered by InfoScale, and uses either SAN attached storage or direct-attached storage to provide software-defined persistent storage for an OpenShift cluster
- **Data protection**—powered by NetBackup, with native support for Kubernetes workloads designed specifically to protect containerized applications, including those running in OpenShift

The Veritas solution for OpenShift has several advanced features that enables freedom of architecture and flexibility for your containerized applications. With mobility across physical, virtual, and cloud platforms, you can focus on delivering innovation knowing that your IT services are protected and resilient.

Stateful and mission-critical applications running in OpenShift typically require persistent data storage, which is not available natively within OpenShift. InfoScale for Kubernetes provides a Container Storage Interface (CSI) plug-in that provides advanced software-defined storage services in OpenShift for containerized applications. InfoScale's enterprise functionality integrates with OpenShift to provide a container management platform suitable for running stateful and mission-critical applications that require the following:

- **Advanced persistent storage:** InfoScale's software-defined deployment architecture allows you to use SAN and direct-attached storage to support the persistent storage requirement for stateful containerized applications. You can use InfoScale's Flexible Storage Sharing (FSS) feature to provide high-performance storage using the disks directly attached to the OpenShift cluster nodes. This can provide better performance than SAN-based storage, at a reduced cost.
- **Application and system availability:** InfoScale's advanced I/O fencing capabilities let you bring failed nodes and/or application pods back online quickly, without worrying that data has become corrupted. By quickly removing access to shared data from failed nodes or pods, InfoScale prevents the corruption of data that may be in use by other nodes or pods. This approach enables the applications to remain online and servicing requests while administrators work to repair the failures.
- **Disaster recovery and site resiliency:** InfoScale's DR manager for OpenShift can be deployed as an operator-based feature that allows you to migrate and take over operations for planned and unplanned recovery operations. InfoScale manages the resiliency process with optimized replication between clusters that maintains write-order fidelity, and replicates application state and OpenShift cluster metadata.

InfoScale is deployed as a containerized application within OpenShift and is accessible in Operatorhub.io directly within the OpenShift user interface. Figure 2 provides an overview of how InfoScale integrates with OpenShift to provide persistent storage for containerized applications.

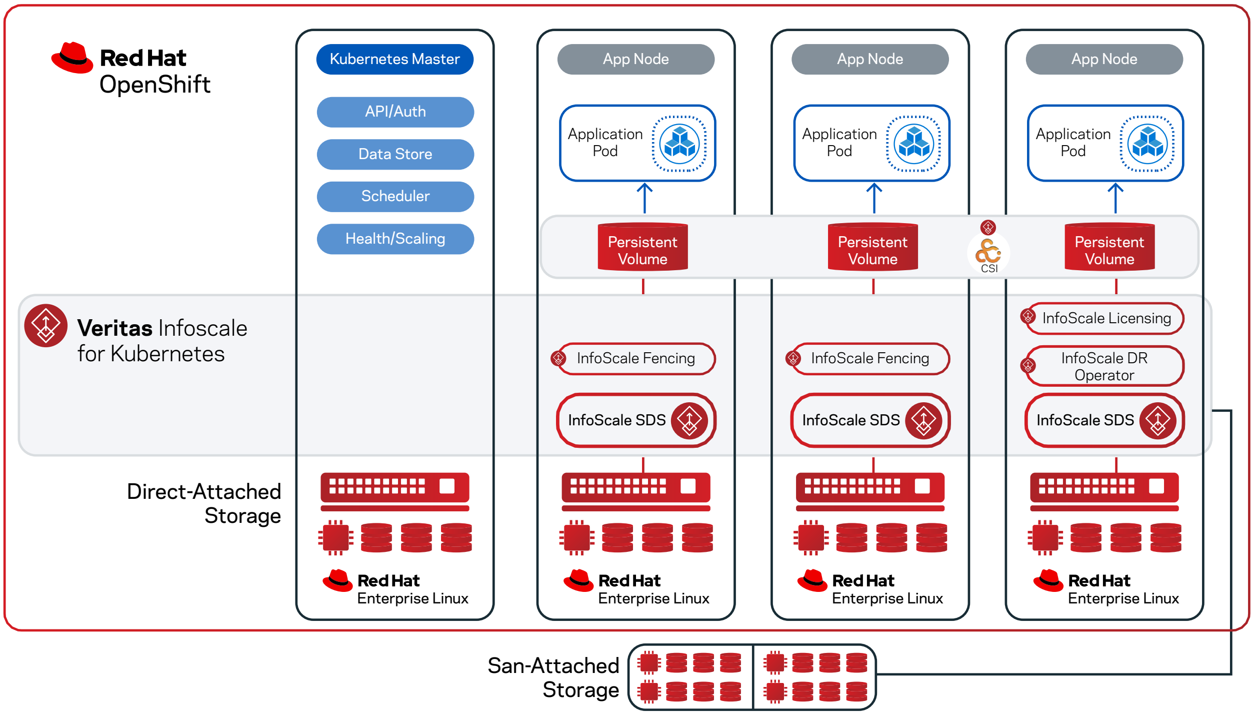


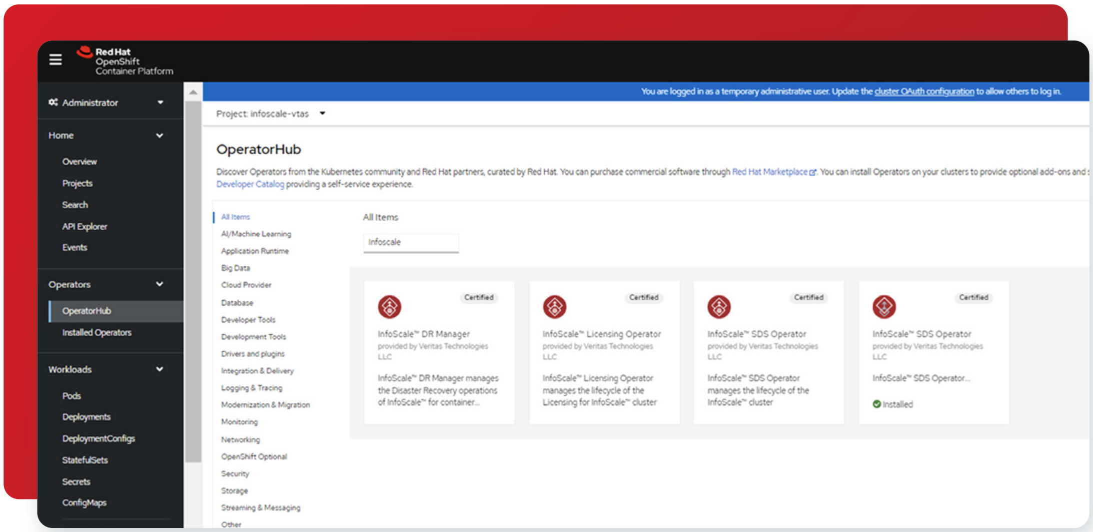
Figure 2. InfoScale configuration overview in OpenShift

Containerized applications with shared storage provided by InfoScale are automatically protected against data corruption due to a split-brain scenario. Split-brain can occur in any clustered environment in the event of a node/hardware failure that disrupts cluster communications and membership. InfoScale provides advanced I/O fencing by preventing data from being written by nodes within the OpenShift cluster that has failed due to hardware or network communication failures. If a node failure is detected by OpenShift, the InfoScale fencing driver can ensure the persistent volumes being used by application pods on the failed node are no longer accessible by fencing this node out of the cluster. This prevents data corruption by allowing only the working nodes to continue normal operations. In the event of a communication loss between cluster nodes (also known as worker nodes), InfoScale's fencing driver relays this information to OpenShift, which can then mark the node as failed and move pods to another node.

Configuration Overview

All of the required components needed to install and use InfoScale persistent storage in OpenShift are available in Operatorhub.io, which can be accessed directly from within the OpenShift user interface. The following InfoScale components are available in Operatorhub.io:

- **InfoScale SDS Operator:** Manages the InfoScale storage cluster within OpenShift, and provides infrastructure resiliency and persistent storage for your critical containerized applications.
- **InfoScale DR Manager:** Manages disaster recovery and migration for containerized applications in OpenShift; In the event of an entire OpenShift cluster failure, application components can be restored on another cluster.
- **InfoScale Licensing Operator:** Provides the license management functionality needed to operate the InfoScale storage cluster in OpenShift.



You are logged in as a temporary administrative user. Update the cluster OAuth configuration to allow others to log in.

OperatorHub

Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Marketplace. You can install Operators on your clusters to provide optional add-ons and s
Developer Catalog providing a self-service experience.

InfoScale™ DR Manager
provided by Veritas Technologies LLC
InfoScale™ DR Manager manages the Disaster Recovery operations of InfoScale™ for container...

InfoScale™ Licensing Operator
provided by Veritas Technologies LLC
InfoScale™ Licensing Operator manages the lifecycle of the Licensing for InfoScale™ cluster

InfoScale™ SDS Operator
provided by Veritas Technologies LLC
InfoScale™ SDS Operator manages the lifecycle of the InfoScale™ cluster

InfoScale™ SDS Operator
provided by Veritas Technologies LLC
InfoScale™ SDS Operator...

Figure 3. InfoScale available in Operatorhub.io as seen from the OpenShift user interface

Installing the InfoScale SDS operator is a simple process and can be done within the OpenShift user interface. Once the InfoScale SDS operator is installed, the persistent storage cluster can also be configured within the OpenShift user interface and can use disks local to the OpenShift worker nodes, or volumes on an external SAN to form a storage cluster. Users have the option to specify devices to exclude from InfoScale's view (for example, /dev/sda), and by default InfoScale uses a single disk group called vrts_kube_dg for all CSI operations. InfoScale SDS has several enterprise features to support stateful enterprise applications, including:

- **Dynamic provisioning:** Create persistent volumes using different storage classes, where the storage is dynamically allocated by pods requesting the storage. You can reclaim storage when previously provisioned storage is available for other applications to use, and you can also resize an existing volume as needed.
- **Volume snapshots:** Create space-optimized copies of persistent volumes that can be provisioned statically or dynamically. Snapshots can be used to reinstate volume contents on the original volume or on a new persistent volume that you provision.

- **Volume cloning:** Create an exact duplicate of a specified existing persistent volume. Volume clones can be used by any persistent volume claim and can be deleted without affecting the original volume.

A detailed overview of the InfoScale install and configuration process in OpenShift can be found here.

Deployment Architecture

InfoScale uses a hyperconverged architecture where all worker nodes in the OpenShift cluster must be used to create the InfoScale storage cluster. InfoScale is deployed as a containerized application on all the worker nodes specified in the Custom Resource YAML file.

InfoScale provides different types of storage classes that can be used depending on the performance and resiliency requirements of your applications. InfoScale storage classes are defined and managed using YAML files included with the InfoScale software package. Persistent volumes can be created in OpenShift using any of the InfoScale storage classes. The storage classes enable different configurations for the underlying storage hardware (standard, resiliency, performance), resulting in different levels of performance and resiliency for your applications.

InfoScale storage offers different access modes that determine how persistent volumes are mounted and used. This allows you to provision storage more granularly, based on your application's requirements and operational standards. The different storage access modes are:

- **ReadWriteOnce (RWO):** The volume can be mounted and used as read-write by a single node
- **ReadOnlyMany (ROX):** The volume can be mounted and used by many nodes in read only mode
- **ReadWriteMany (RWX):** The volume can be mounted and used as read/write by many nodes

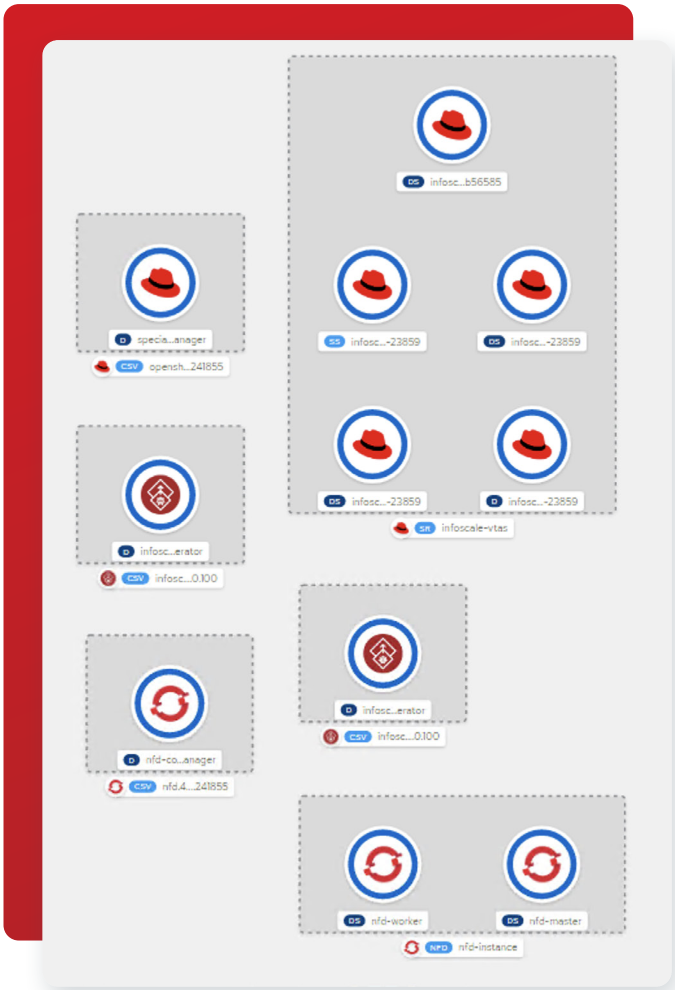


Figure 4. InfoScale topology overview in OpenShift

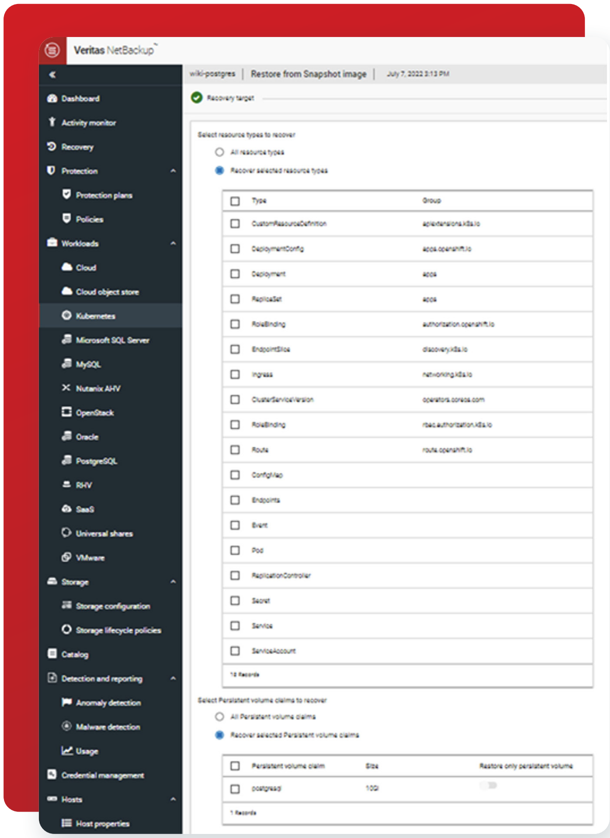
InfoScale storage clusters can be scaled to 16 worker nodes, and can be created using nearly any type of underlying storage—either DAS or SAN. A full list of supported storage devices can be found here.

Data Protection

NetBackup reduces complexity, scales with growth, and provides a foundation for OpenShift data protection that delivers broad platform support to improve data resiliency and mobility for containerized applications. NetBackup protects all components of containerized applications in OpenShift at the project and individual resource level. NetBackup provides comprehensive protection and recovery options that give you:

- **Advanced recoverability:** Easily roll back persistent volume backups. Restore an entire project or multiple projects within the same cluster, to alternate OpenShift clusters, or to different Kubernetes distributions—on-premises or in the cloud.
- **Granular recovery:** Recover individual resource types and persistent volumes in an OpenShift project with a single-pass backup that provides multiple options for recovery.

NetBackup is fully Kubernetes aware, and seamlessly protects your applications by discovering and managing the snapshot and recovery of all components within an OpenShift project, including all persistent storage volumes, configuration files, and custom resources. Figure 5 shows an example of a recovery operation in the NetBackup web user interface.



wiki-postgres | Restore from Snapshot image | July 7, 2022 3:13 PM

✓ Recovery target

Select resource types to recover

○ All resource types

● Recover selected resource types

□	Type	Group
□	CustomResourceDefinition	apiextensions.k8s.io
□	DeploymentConfig	apps.openshift.io
□	Deployment	apps
□	ReplicaSet	apps
□	RoleBinding	authorization.openshift.io
□	EndpointSlice	discovery.k8s.io
□	Ingress	networking.k8s.io
□	ClusterServiceVersion	operators.coreos.com
□	RoleBinding	rbac.authorization.k8s.io
□	Route	route.openshift.io
□	ConfigMap	
□	Endpoints	
□	Event	
□	Pod	
□	ReplicationController	
□	Secret	
□	Service	
□	ServiceAccount	

18 Records

Select Persistent volume claims to recover

○ All Persistent volume claims

● Recover selected Persistent volume claims

□	Persistent volume claim	Size	Restore only persistent volume
□	postgresql	10Gi	

1 Records

Figure 5. NetBackup provides recovery granularity for OpenShift clusters with a single-pass backup operation

Configuration Overview

NetBackup uses Helm charts to streamline the deployment of all the required Kubernetes resources. Veritas provides a full suite of RESTful application programming interfaces (APIs) with role-based access control (RBAC) that enables self-service for users to align with their CI/CD pipeline and native tools. In NetBackup 8.2 or later, you can access NetBackup APIs in your own environment with the Swagger interface at https://<primary-server-name>/api-docs/index.html. As NetBackup now includes native functionality to manage data protection for Kubernetes workloads, the process to connect NetBackup to an OpenShift cluster is simple:

1. A NetBackup namespace is created within the OpenShift cluster and the NetBackup kOps operator is installed in that namespace using a Helm chart. The NetBackup Elastic Data Mover pod also operates within this namespace and is deployed dynamically as backup jobs run.

2. From the primary server, the OpenShift cluster is registered and namespaces within the cluster are discovered. Data protection policies are then defined to indicate what namespaces and resources are protected, the schedule, frequency, retention, target storage for backups, and other optional requirements such as encryption and immutable storage.

3. Based on the policy defined, the media server is then used to copy the contents of a snapshot to a target storage system, either on-premises or in the cloud. The backup involves using the Container Storage Interface (CSI) drivers to create a volume snapshot of an OpenShift project. Then, a Backup from Snapshot job can be initiated, and the NetBackup Elastic Data Mover pod is deployed to copy the snapshot contents to a target storage device.

Figure 6 shows an overview of NetBackup configured to provide data protection services for an OpenShift cluster.

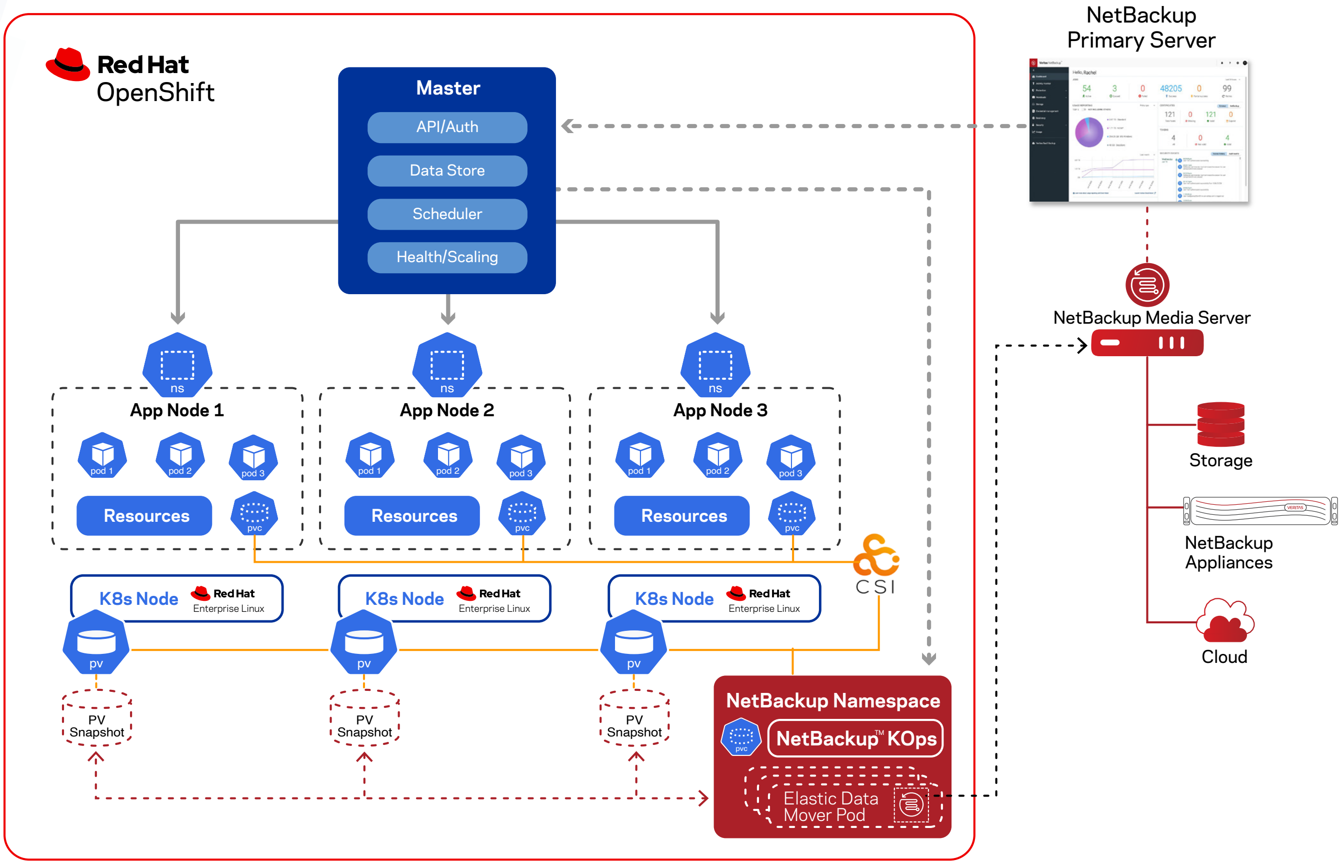
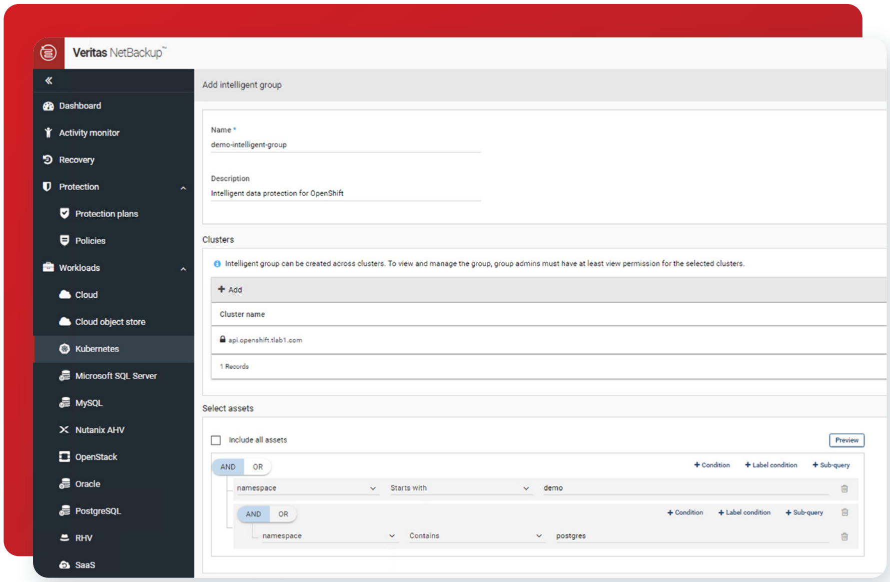


Figure 6. NetBackup deployment architecture overview

NetBackup provides several options for configuring backup policies, including protection plans and the ability to use intelligent groups that can help automate data protection for your OpenShift clusters. Protection plans are customized by the end user, and define when backups are executed, how long backups are retained, and the type of storage to use as a backup target. When using Intelligent Groups to protect workloads in OpenShift, you can automate the backup process for multiple workloads, and new workloads are automatically included in a backup job without the need for manual configuration. The content to be protected is determined dynamically when a backup job runs. Figure 7 shows an example of an intelligent group for workloads running within an OpenShift cluster.



Add intelligent group

Name *
demo-intelligent-group

Description
Intelligent data protection for OpenShift

Clusters

Intelligent group can be created across clusters. To view and manage the group, group admins must have at least view permission for the selected clusters.

Cluster name
api.openshift.tlab1.com

1 Records

Select assets

□ Include all assets

AND
namespace | Starts with | demo
AND
namespace | Contains | postgres

Figure 7. NetBackup Intelligent Group for workloads in an OpenShift cluster

Integrated Security

Ransomware and cyberattacks have become a major concern for companies, making security one of the top requirements when selecting a data protection solution. NetBackup has several native security features that extend to Kubernetes workloads to better secure your containerized applications in OpenShift against malware and ransomware attacks. NetBackup security features include encryption for data in flight and data at rest, Transport Layer Security (TLS) for all traffic between servers, role-based access control for administration, security at the operating system level by limiting root users, turning off unused ports, and other security measures to protect your data. With NetBackup Appliances, you have additional security features such as immutable storage, hardened operating systems, isolated recovery, and anomaly detection. NetBackup also delivers auditing and alerting features to quickly identify unexpected changes in the NetBackup environment, and for regulatory compliance.

Unified Storage and Data Protection

OpenShift helps simplify Kubernetes with a comprehensive, intuitive user experience. but it relies on third parties for the data management functionality that typical enterprise applications need. With Veritas, your OpenShift environment will have the storage and data protection needed by stateful applications, along with several other benefits:

- InfoScale helps eliminate data loss and downtime risks such as hung processes and inaccessible storage that could otherwise go undetected
- NetBackup recovery granularity allows you to protect OpenShift clusters easily with a single process that offers several options for data and resource recoverability
- Distribution mobility allows you to move your containerized applications between platforms and Kubernetes distributions (on-prem or in the cloud)
- High performance persistent storage with integrated data integrity management that works with nearly any type of hardware, giving you freedom of architecture while avoiding vendor lock-in

Conclusion

Running applications in Red Hat OpenShift can help businesses deliver more efficient innovation, but this operating model has some gaps in the enterprise functionality needed by most applications. IT architects and managers are challenged with finding the best way to provide enterprises with persistent storage and data protection for their containerized applications. Veritas solves this problem with an enterprise-focused solution for storage management and data protection that works seamlessly with OpenShift. Veritas provides:

- **Enterprise persistent storage:** InfoScale's software-defined architecture and operator-based deployment allow users to easily provision enterprise-grade software-defined persistent storage for containerized applications running in OpenShift, using any local or external SAN storage.
- **Flexible data protection:** Ensure that your OpenShift projects are fully protected, with granular recovery capability and the flexibility to recover in the same environment, or to an alternate location (including cloud).
- **Integrated user experience:** NetBackup and InfoScale seamlessly work with OpenShift using native integration points that make the overall user experience easy and intuitive.

With a focus on usability and functionality, InfoScale and NetBackup work together to enable businesses to take advantage of the benefits of containerization, with advanced protection and storage management that extends OpenShift to provide the functionality needed by stateful enterprise applications. Veritas storage and data protection is ideally suited for production Red Hat OpenShift deployments, and delivers the functionality and confidence to run containerized applications with maximum availability and protection.

[1] Source: 451 Research Voice of the Enterprise: DevOps,H1 2020

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. 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