



Technical Report

# **NetApp Converged Infrastructure Data Protection with Veritas NetBackup**

Kamini Singh and Jyh-shing Chen, NetApp  
Liji Kuruvilla, Veritas  
February 2021 | TR-4879

In partnership with



## **Abstract**

This technical report provides a high-level overview of NetApp® Converged Infrastructure and Veritas NetBackup. It summarizes the configuration and backup and recovery workflow for the Microsoft SQL Server on VMware use case. This powerful combination provides a comprehensive data protection solution to help businesses satisfy requirements around data protection and data compliance for a broad range of applications and workloads and achieve recovery point and recovery time objectives.

## TABLE OF CONTENTS

<b>Introduction to NetApp Converged Infrastructure .....</b>	<b>4</b>
<b>Data protection methods, terminologies, and native tools .....</b>	<b>5</b>
Backup, restore, and medium .....	5
Backup schedule and retention period .....	6
Recovery point objective and recovery time objective .....	6
Snapshot and replication .....	6
Crash consistency and application consistency .....	7
ONTAP features and NetApp tools for NetApp Converged Infrastructure data protection .....	7
<b>Introduction to Veritas NetBackup .....</b>	<b>8</b>
Veritas NetBackup architecture .....	9
Veritas NetBackup with NetApp Converged Infrastructure .....	10
<b>Using Veritas NetBackup with NetApp Converged Infrastructure .....</b>	<b>11</b>
Example NetApp Converged Infrastructure with Veritas NetBackup environment .....	11
Configuration and backup and recovery workflows for VMware instant access .....	13
Configuration and backup and recovery workflows for MS SQL instant access .....	20
<b>Where to find additional information .....</b>	<b>23</b>
<b>Acknowledgement .....</b>	<b>24</b>
<b>Version history .....</b>	<b>24</b>

## LIST OF TABLES

Table 1) Software, version, and location deployed .....	12
---	----

## LIST OF FIGURES

Figure 1) NetApp Converged Infrastructure example with compute servers, network switches, and a redundant NetApp storage system in a highly available configuration. ....	4
Figure 2) ONTAP 9 provides common data management from the edge to core to cloud. ....	5
Figure 3) Veritas NetBackup provides broad workload support from the edge to core to cloud. ....	9
Figure 4) NetBackup architecture. ....	10
Figure 5) Architecture components for using Veritas NetBackup for data protection of NetApp Converged Infrastructure. ....	11
Figure 6) Example NetApp Converged Infrastructure with Veritas NetBackup solution architecture. ....	12
Figure 7) Installing Veritas NetBackup Client on Microsoft SQL Server. ....	13
Figure 8) Configured storage servers with MSDP and Advanced Disk categories. ....	14

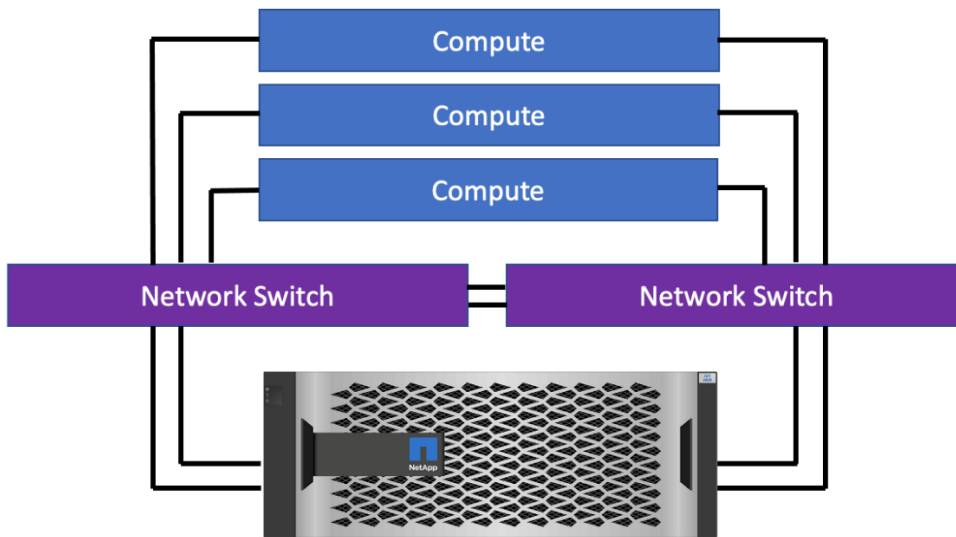
Figure 9) Configured disk pools.....	14
Figure 10) Configured storage units. ....	14
Figure 11) Discovered VMs in the VMware infrastructure. ....	15
Figure 12) Configured protection plan. ....	15
Figure 13) Veritas NetBackup supports NetApp StorageGRID as a cloud storage provider. ....	16
Figure 14) Associate a VM intelligent group to a protection plan.....	16
Figure 15) Activity Monitor shows the jobs with different types of activities for the Microsoft SQL server. ....	17
Figure 16) Different options for performing recovery in NetBackup. ....	17
Figure 17) Recover the entire VM by using the Restore Virtual Machine option. ....	18
Figure 18) Add files/folders on Microsoft SQL Server that you want to restore. ....	18
Figure 19) Activity Monitor shows the restore job for a VM. ....	19
Figure 20) Download files and folders from backup. ....	19
Figure 21) Instant access VM created for the Microsoft SQL Server.....	20
Figure 22) Add MS SQL Server instance into NetBackup. ....	20
Figure 23) Add MS SQL credentials into NetBackup.....	21
Figure 24) Define MS SQL protection plan.....	21
Figure 25) BackupNow operation for MS SQL database backup. ....	22
Figure 26) Recovery points for MS SQL.....	22
Figure 27) MS SQL—Configure MS SQL instant access recovery options. ....	23

# Introduction to NetApp Converged Infrastructure

The ever-increasing data size and the valuable insights data can provide make data services and data protection both critical and challenging. First, data must be available as well as protected to meet data recovery, business continuity, or compliance requirements. Second, data must be made readily available for data analysis, for example, through artificial intelligence (AI) and machine learning (ML) based approaches, to help businesses improve their solutions and create business values. Third, the data service infrastructures and the data protection methodologies must accommodate the growth of data as business grows. In addition, data mobility is increasingly becoming critical due the need to move data from the edge, where is it created, to the core and cloud to use resources available there for data analysis or archival purposes.

NetApp® Converged Infrastructure provides the data management and data protection features and capabilities from NetApp AFF / FAS storage arrays with additional compute and network infrastructures to deliver highly available, highly scalable, and highly flexible solutions that customers can easily deploy. Figure 1 illustrates an example converged infrastructure with compute servers, network switches, and redundant NetApp storage in a highly available configuration. With verified architectures that use components that are supported on the interoperability matrices of the infrastructure providers, the thoroughly tested converged infrastructures minimize deployment risks and accelerate time to value for solution deployments.

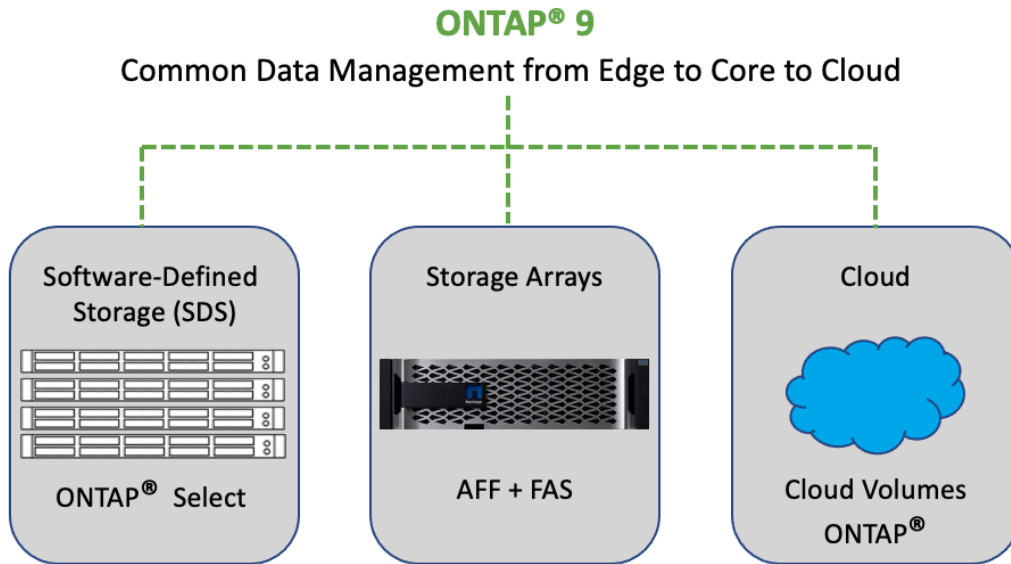
**Figure 1) NetApp Converged Infrastructure example with compute servers, network switches, and a redundant NetApp storage system in a highly available configuration.**



Data fabric powered by NetApp facilitates the mobility of data across the hybrid cloud ecosystem and enables businesses to seamlessly move data from where it was generated to where it is needed. As illustrated in Figure 2, customers can choose the optimal location and platforms for their data and take advantage of the NetApp ONTAP® data management features and capabilities both on premises and in the cloud. In addition, customers can choose to deploy storage solutions with a flexible software defined storage, a high-performance all-flash storage, or a hybrid storage system with both SSDs and hard disks.

While AFF / FAS hardware-based ONTAP storage systems are required for NetApp Converged Infrastructure, the additional software-defined and cloud choices help customers balance performance, capacity, and costs, all while taking advantage of the storage efficiency and data protection features from all available NetApp storage systems to reduce costs of data management, ensure data availability and mobility, and achieve solution objectives.

Figure 2) ONTAP 9 provides common data management from the edge to core to cloud.



## Data protection methods, terminologies, and native tools

There are various methods that a company can adopt to protect its valuable data against different threat scenarios and to meet regulatory and compliance requirements. Having a data protection plan and performing regular backups allow companies to recover data when data is accidentally deleted, attacked by malware, locked away by ransomware, or completely lost due to a disaster.

Companies might have different requirements for different types of data sets. Some data might only require a daily backup, while some might not need to be backed up at all if there are extra copies made for development and testing and can be easily recreated.

For mission critical data that could disrupt your business when it is not available, careful evaluation is needed to answer questions such as how often the data needs to be backed up, where the backups should reside, how quickly the recovery can and should take place, and so on. For businesses that are relying on providing data for revenue generation, the data services might even need to be protected by a solution that can withstand a site outage and disaster in order to minimize the impact and to ensure continuous business operations.

Here are some of the frequently used methods and terminologies that might be helpful when discussing, evaluating, and planning for data protection strategies and implementations for NetApp Converged Infrastructure. Also included is a list of native NetApp tools that you can use for data protection.

### Backup, restore, and medium

Backup is a tried-and-true method of protecting business critical data. Historically, backing up to tape was the gold standard due to the limited size of disks and storage space available. With the availability of higher capacity hard disks, high performance SSDs and cheaper storage from the public cloud providers, backup can now be cost-effectively stored on disks for quick access or in the cloud to reduce on-premises storage footprint and costs.

Backing up a large data set requires time, so a typical backup plan might include a full backup to cover the entire data set once a week and a daily incremental backup to archive changes that happen every day.

When data is backed up, you can restore it at a later time when needs arise. The recovery process depends on the strategy implemented. For example, for a full plus incremental backup strategy, a complete recovery will involve restoring from a full backup first and then applying subsequent incremental backups sequentially to recover the entire data set.

## **Backup schedule and retention period**

Depending on the use cases and data sets, you can schedule the backup operation for a data set to happen at a desirable frequency or schedule. For example, some data might require backup every five minutes or every hour, while other data might only require a daily backup. Some backups might only need to be made available within two weeks after the backup, while other backups might need to be available for several years due to regulatory and compliance requirements.

Depending on the infrastructure and tools used, you might be specifying the number of copies to retain instead of the retention period if you have a capacity limitation and you can estimate the size of the backup copies.

In addition, you can potentially take advantage of multiple infrastructures and specify different amounts of retention periods based on the medium used and tier the backup data from one type of medium to another after a certain amount of time. For example, you might keep recent backup copies on premises for quick recovery and have a policy to tier older backups to the cloud to reduce on-premises storage costs while meeting the compliance requirements.

## **Recovery point objective and recovery time objective**

The recovery point objective (RPO) measures how much data, in terms of time, you can afford to lose, or the point up to which you can recover your data. For a daily backup plan, a company might lose a day's worth of data as the changes made to the data since the last backup could potentially be lost. For the business-critical and mission-critical data services, they might require zero RPO and an associated plan to protect data without any potential data loss.

The recovery time objective (RTO) measures how much time you can afford to not have the data available, or how quickly data services need to be brought back up. For example, a company might have a backup and recovery implementation which uses traditional tapes for certain data sets due to its size. As a result, to restore the data from the backup tapes, it might take several hours. If there was an infrastructure failure, it must also include time to bring the infrastructure back up in addition to restoring data. For mission-critical data services, it might require low RTO and can only tolerate a failover time on the order of seconds, or minutes, to quickly bring the data services back up and to ensure business continuity.

## **Snapshot and replication**

A snapshot captures a point-in-time copy of the information needed to restore a data set. It can be a copy of the data itself, or a set of pointers that help identify the data at the time a snapshot is taken. A snapshot using pointer-based technologies can be completed quickly as the pointer information is much less than the amount of the actual data. The copied set of pointers provide a way to restore data. For this to work properly, data that was copied with a snapshot cannot be deleted if there are still pointer references to the data.

For data services that cannot tolerate data loss (zero RPO) and require very quick recovery (low RTO) after a failure or disaster scenario, continuous data replication technologies with quick failover between the primary and secondary data locations can be used to help meet the desired objectives. When the deployment uses two locations that are geographically separated by a certain distance, the replicated data on the second site can also protect businesses from a site failure scenario.

## Crash consistency and application consistency

As more applications are deployed on virtual machines (VMs) residing on a virtual infrastructure, it is important that the backups of the data files performed are consistent for the VMs. As far as the data in the backup is concerned, it is similar to the scenario where the VM crashed at the time of the backup. For example, you can leverage the Microsoft Shadow Volume Copy service on the Windows OS to create a snapshot of the data for the backup software to go over and back up.

While a crash consistent backup can enable a VM to be restored, it might not be able to restore a consistent view of data for an application such as Microsoft SQL Server running on the VM as some of its database I/O might still be in memory and not yet committed to disk. An application consistent backup is application aware and ensures that disk I/Os are flushed from memory and committed first before a snapshot is taken. This additional level of backup consistency allows a restore operation to bring the application back to a consistent state and reduces the effort needed to recover the application.

## ONTAP features and NetApp tools for NetApp Converged Infrastructure data protection

Traditionally, ONTAP replication technologies served the need for data archiving and disaster recovery. The foundation for these is NetApp Snapshot™ technology. With the availability of cloud services, ONTAP replication technologies have been extended to support data transfer between endpoints in the data fabric powered by NetApp. The following briefly discusses several ONTAP features and additional NetApp tools that customers can use to protect data in their NetApp Converged Infrastructure.

### RAID 4 / RAID DP / RAID-TEC

ONTAP uses three different RAID levels to protect against disk failures in a RAID group. With RAID 4 protection, ONTAP can use one spare disk to replace and reconstruct the data from one failed disk within the RAID group. With NetApp RAID DP® protection, ONTAP can use up to two spare disks to replace and reconstruct the data from up to two simultaneously failed disks within the RAID group. With NetApp RAID-TEC® protection, ONTAP can use up to three spare disks to replace and reconstruct the data from up to three simultaneously failed disks within the RAID group. RAID-TEC is recommended if the size of the disks used in the aggregate is greater than 4 TiB.

### NetApp Snapshot

NetApp Snapshot technology has been a widely used feature by customers as it is instantaneous and space efficient. A Snapshot copy is a read-only, point-in-time image of a volume. When ONTAP creates a Snapshot copy, it references metadata rather than copying data blocks, which makes it so efficient. The image consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the last Snapshot copy was made. You can use a Snapshot copy to recover individual files or LUNs, or to restore the entire contents of a volume.

### NetApp SnapMirror

NetApp SnapMirror® is a storage level replication solution. You can create a data protection mirror relationship to a destination within a cluster or between two clusters to protect your data. The data replication can be synchronous or asynchronous. For greater disaster protection, you can create a mirror relationship to a destination in a different cluster located at a different site, which can also be a cloud location. If the cluster on which the source volume resides experiences a disaster, you can direct clients to the destination volume on the cluster peer until the source volume is available again.

### NetApp SnapVault

NetApp SnapVault® is a disk-to-disk backup solution that you can use to offload tape backups. A SnapVault relationship is created between a primary volume and a secondary volume. The data in the

primary volume is backed up to the secondary volume with an initial baseline transfer and additional incremental transfers afterwards. In the event of data loss or corruption on a system, backed-up data can be restored from the SnapVault secondary volume with less downtime and uncertainty than is associated with conventional tape backup and restore operations.

## NetApp SnapLock

NetApp SnapLock® is a high-performance compliance solution for organizations that use “write once, read many” (WORM) storage to retain files in unmodified form for regulatory and governance purposes. SnapLock provides special purpose volumes in which files can be stored and committed to a non-erasable, non-rewritable state either forever or for a designated retention period. SnapLock allows this retention to be performed at the granularity of individual files through standard open file protocols such as CIFS and NFS.

## NetApp MetroCluster

NetApp MetroCluster is an ONTAP feature that customers can configure to have continuous data replication from one storage cluster to another. With MetroCluster IP, the two sites can be geographically separated up to 700 km apart to provide a disaster recovery solution that meets zero RPO and low RTO requirements to ensure continuous business data services. Once properly configured, the data written to one storage cluster is automatically replicated to another site. In case of a site disaster, the surviving site can continue the data services automatically with the help of ONTAP Mediator services running on a third site which monitors the solution and automates the switchover operation upon a site disaster to ensure data services can continue from the survival site.

## NetApp SnapCenter

NetApp SnapCenter® software leverages storage-based data management to provide an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems. SnapCenter leverages Snapshot, NetApp SnapRestore®, NetApp FlexClone®, SnapMirror, and SnapVault technologies to provide fast, space-efficient, application-consistent, disk-based backups and restores. It includes both the SnapCenter Server and individual lightweight plug-ins. You can automate deployment of plug-ins to remote application hosts, schedule backup, verification, and clone operations, and monitor all data protection operations. SnapCenter can be deployed on premises, in a hybrid cloud environment, and also in the public cloud for data protections.

## NetApp SnapCenter Plug-In for VMware vSphere

NetApp SnapCenter Plug-in for VMware vSphere enables VM-consistent and crash-consistent backup and restore operations for VMs and datastores from the vCenter server. You define resource groups and attach backup policies to them for backups to take place automatically according to the schedules. You can back up VMs, underlying VMDKs, and datastores. When you back up a datastore, you back up all the VMs in that datastore. You can create mirror copies of backups on another volume that has a SnapMirror relationship to the primary backup. You can perform a disk-to-disk backup replication on another volume that has a SnapVault relationship to the primary backup volume. When necessary, you can restore VMs, VMDKs, or attach virtual disks to a VM for file restorations. You can also restore a deleted VMs to an ESXi host you select.

# Introduction to Veritas NetBackup

Data has become one of the most critical assets for businesses around the globe. Veritas Technologies, a leader named by Gartner Magic Quadrant for data center backup and recovery solutions, help organizations of all sizes protect their data so that they can ensure business continuity and gain insights from their data to create business values. Using the Veritas platforms, companies can speed up their



digital transformation and tackle IT and business challenges. They can take advantage of the multicloud data management and data protection capabilities to achieve workload portability, backup storage optimization, and compliance readiness.

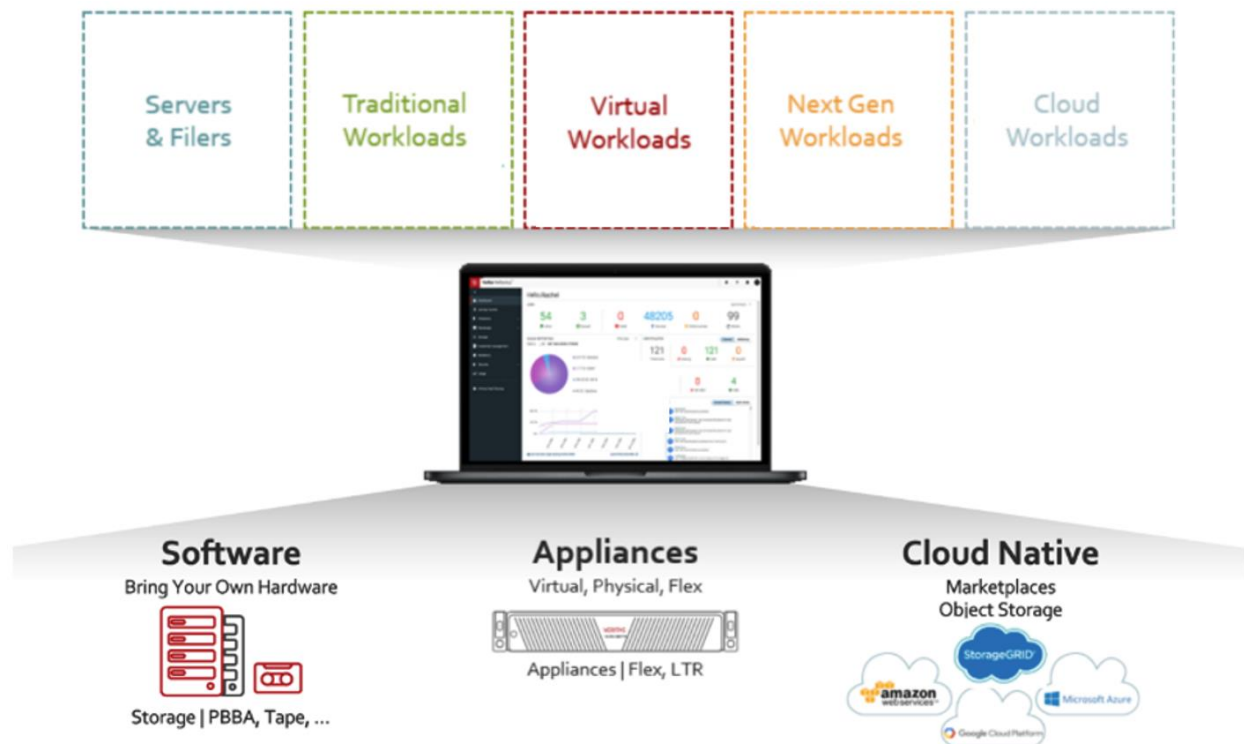
In addition to the ONTAP features and NetApp tools discussed above, customers can use enterprise backup and recovery solutions such as Veritas NetBackup to protect NetApp Converged Infrastructure alongside their heterogeneous environments. NetApp Converged Infrastructure and Veritas NetBackup together offer a comprehensive data protection solution that ensures rapid recovery of business-critical data across physical, virtual, hybrid and multi-cloud environments while scaling to any size workload. Veritas offers a wide variety of products for enterprise data protection, such as NetBackup, Backup Exec, System Recovery, and various backup appliances, to simplify the solution deployment. Due to the COVID-19 pandemic, enterprises around the world are accelerating their digital transformation to support their remote workforce. The resiliency and efficiency of IT services are more critical than ever.

## Veritas NetBackup architecture

With NetBackup, companies can standardize on a single platform across hybrid and multi-cloud environments. NetBackup allows you to define the protection needs at a high level and then automate service-level objectives (SLOs) throughout your infrastructure. NetBackup Resiliency provides a simple, non-disruptive way of validating enterprise resiliency plans for assurance and compliance through automated recovery and rehearsal of critical applications.

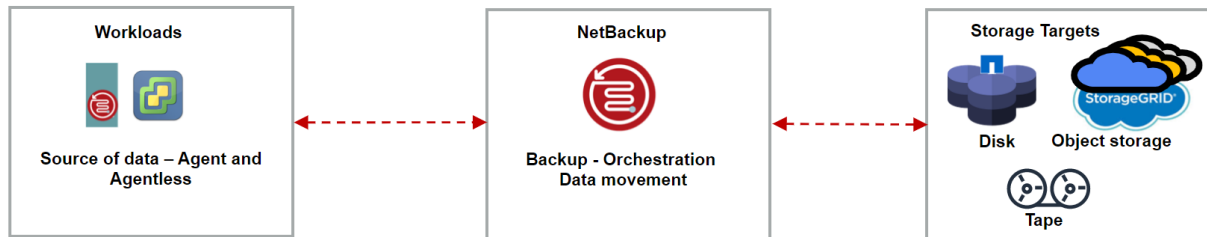
Figure 3 illustrates how Veritas NetBackup provides a unified, comprehensive, secure data protection platform across the edge to core to cloud, reducing the impact and risks associated with system downtime.

Figure 3) Veritas NetBackup provides broad workload support from the edge to core to cloud.



NetBackup uses a scalable architecture made up of one or more NetBackup servers that receive data from client agents and stores them on storage targets such as disk, tape, or object storage. See Figure 4.

Figure 4) NetBackup architecture.



NetBackup provides a complete, flexible data protection solution for a variety of platforms. NetBackup includes both the server and the client software. Server software resides on a system that manages jobs (master server) or manages storage devices (media server). Both client/agent-based and agentless protection options are available depending on the type of workload. You can provision media servers on demand as customer data protection needs scale. The workloads might be applications, operating systems, containers, hypervisors, Big Data, or hyper-converged systems.

Veritas Deduplication engine, integral to NetBackup servers, help store large amounts of data in an optimized manner on locally attached disk or object storage systems. The protected data is highly portable and can also be sent in an optimized manner to other cloud/offsite locations. This allows customers to maintain an air-gapped copy of their data, and helps counter reduce risk from malware.

The latest NetBackup software brings many new benefits to enterprise customers, including ransomware resiliency, disaster recovery orchestration and cloud migration for business-critical application stacks, broad workload and hypervisor support, self-service, role-based access control (RBAC), and data portability between multicloud environments and between storage tiers. See <https://veritas.com/netbackup> for more information about NetBackup.

## Veritas NetBackup with NetApp Converged Infrastructure

There are various potential NetBackup configurations that you can deploy to protect NetApp Converged Infrastructure. As a backup storage target, customers can use NetApp FAS, AFF, and E-series storage arrays with iSCSI SAN connectivity. In addition, customers can also use StorageGRID object storage as a backup target using S3 protocol.

NetApp FAS operates in the enterprise class SAN and NAS environment. It is a unified storage that supports multiple storage protocols over the network using file-based protocols like NFS, CIFS, and HTTP. FAS systems can also present storage over the storage network by using block-based protocols such as FC, FCoE, and iSCSI.

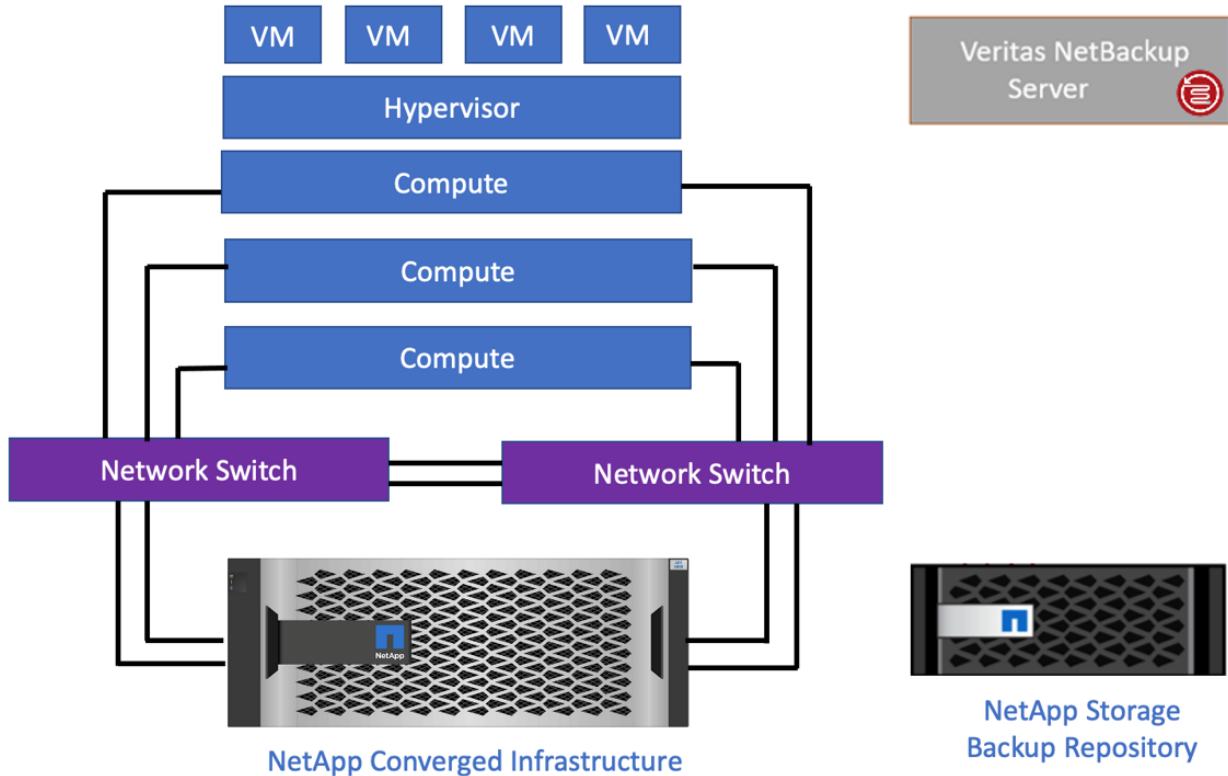
NetApp AFF systems use similar hardware architecture to FAS. AFF is optimized for SSD drives on the back end while the FAS systems support both HDD and SSD. The unified AFF system can provide the same SAN and NAS data protocol connectivity. Customers can also use AFF with NVMe over FC protocol for systems with 32G FC ports to reduce I/O latency and increase I/O performance.

NetApp E-Series provides enterprise data protection, including robust disaster recovery (sync and async), data protection with high-efficiency Snapshot copies. It is architected for the highest reliability and availability and it uses redundant I/O paths with automated failover. Customers can use its web-based UI for online configuration, expansion, and maintenance. It also provides advanced monitoring and diagnostic features for fast problem resolution, proactive tracking of SSD wear life, and alert notifications.

StorageGRID is a software-defined, object-based storage solution that supports industry-standard Amazon S3 API. StorageGRID uses intelligent, policy-driven data management to store, protect, and preserve data. It enables you to create metadata-driven object lifecycle policies to optimize durability, performance, cost, and location across multiple geographies.

Veritas NetBackup with the various NetApp storage options provide a robust backup and disaster recovery solution for a broad set of enterprise applications and workloads. Figure 5 shows the general architecture components for using Veritas NetBackup for the data protection of NetApp Converged Infrastructure.

Figure 5) Architecture components for using Veritas NetBackup for data protection of NetApp Converged Infrastructure.



## Using Veritas NetBackup with NetApp Converged Infrastructure

### Example NetApp Converged Infrastructure with Veritas NetBackup environment

An example NetApp Converged Infrastructure with Veritas NetBackup solution architecture is illustrated in Figure 6. The NetApp Converged Infrastructure with compute, network, and NetApp storage components provides a highly available infrastructure for a VMware virtualized solution and the bare metal server for installing the Veritas NetBackup software components.

The VMware cluster, with two or more computer servers, provides the virtual infrastructure for enterprise solution deployment such as Microsoft SQL servers and other application running on additional VMs. The NetBackup master server and media server are deployed on a bare metal Red Hat Enterprise Linux (RHEL) operating system using on one of the compute servers in the infrastructure.

Depending on the customer objectives, the customer can deploy the NetApp AFF, FAS, E-series, or StorageGRID backup targets to provide the external storage for the NetBackup media server to use. For example, when using AFF, FAS, and E-series as a backup target, they can communicate with the media server through the iSCSI SAN network. On the other hand, S3 protocol is used over network for the StorageGRID system to communicate with the media server.

Figure 6) Example NetApp Converged Infrastructure with Veritas NetBackup solution architecture.

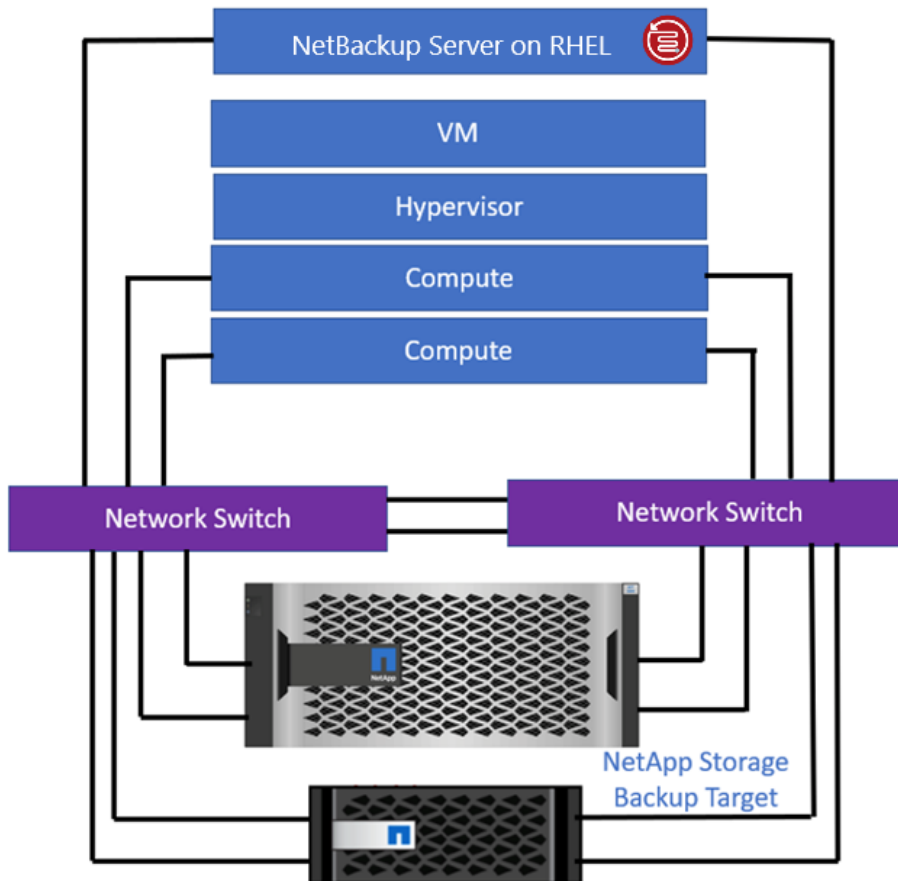


Table 1 below lists the software components and versions used in the NetApp Converged Infrastructure data protection with Veritas NetBackup solution validation environment to protect a Microsoft SQL server deployed on the VMware virtual infrastructure.

Table 1) Software, version, and location deployed.

Software	Release	Location
NetApp ONTAP	9.7	NetApp Converged Infrastructure
NetApp SANtricity®	11.70	NetApp E-Series
Veritas NetBackup	8.3	Red Hat Enterprise Linux
Red Hat Enterprise Linux	7.7	NetApp Converged Infrastructure
VMware vSphere	7.0	NetApp Converged Infrastructure
VMware vCenter Server	7.0	VMware Virtual Infrastructure
NetApp Virtual Storage Console	9.7.1	VMware Virtual Infrastructure
NetApp VAAI Plug-in for ESXi	1.1.2	VMware Virtual Infrastructure
Microsoft Windows Server	2019	VMware Virtual Infrastructure
Microsoft SQL Server	2017 / 2019	VMware Virtual Infrastructure

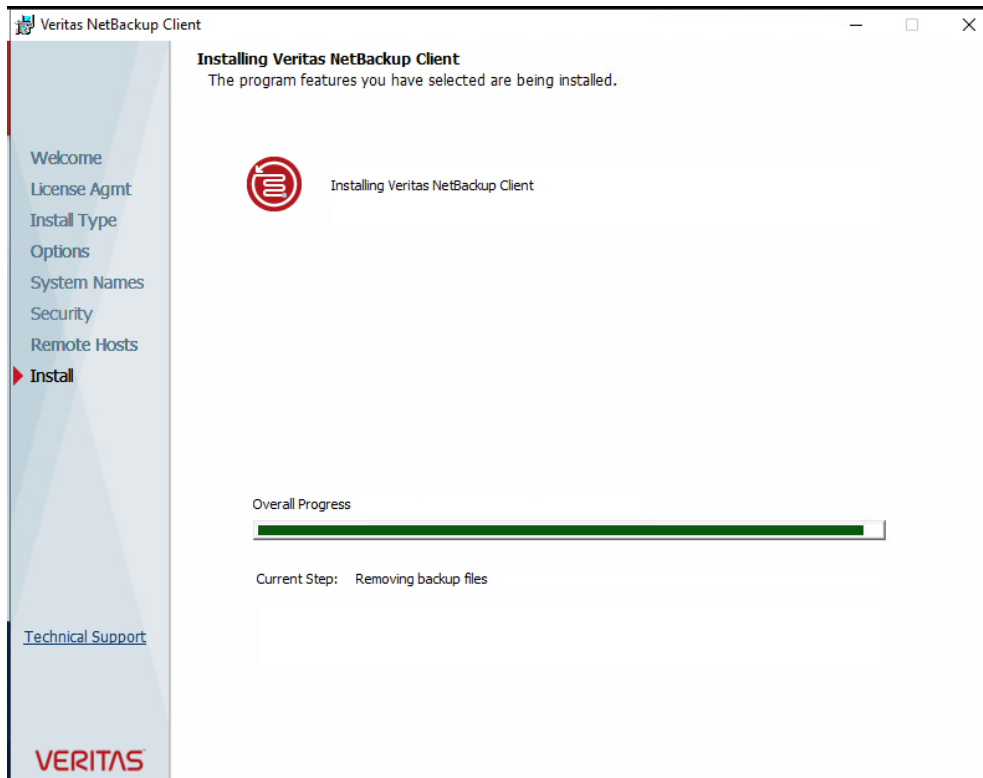
## Configuration and backup and recovery workflows for VMware instant access

The following section highlights some of the configurations and backup and recovery workflows for the Microsoft SQL Server on VMware use case to illustrate how to protect a solution deployed on NetApp Converged Infrastructure with Veritas NetBackup.

The first step is to install the NetBackup master server software on a bare metal RHEL server available on the infrastructure. The master server manages backups, archives, and restores and it is where the NetBackup catalog resides. The catalog has internal databases that contain information about NetBackup configuration and backups.

To help create an application consistent backup for the Microsoft Windows SQL server, install the NetBackup client software for Windows, as shown in Figure 7.

**Figure 7) Installing Veritas NetBackup Client on Microsoft SQL Server.**



The basic NetBackup storage configuration includes the configuration of storage servers, disk pools, and storage units. To configure the storage servers that will be used as backup destinations, log in to the Veritas NetBackup web UI. Different storage server categories are available, including Media Server Deduplication Pool (MSDP), Advanced Disk, and so on. Figure 8 shows an example of having two different categories of storage servers configured.

Figure 8) Configured storage servers with MSDP and Advanced Disk categories.

Storage						
Storage servers		Disk pools	Storage units	Universal shares		
Search...				Q	Y	+Add
<input type="checkbox"/> Name ^	Storage server type	Category	Media servers	Supports Accelerator	Supports snapshot	
<input type="checkbox"/> veritas-01.nva....	PureDisk	MSDP	1	Yes	No	
<input type="checkbox"/> veritas-01.nva....	AdvancedDisk	AdvancedDisk	1	No	No	

For the deduplication pool, the backup image is broken into segments and only the unique segments are saved to reduce space usage. Figure 9 and Figure 10 show examples of the configured disk pools and the storage units where you select the corresponding disk pools and media servers.

Figure 9) Configured disk pools.

Storage						
Storage servers		Disk pools	Storage units	Universal shares		
Search...				Q	Y	+Add
<input type="checkbox"/> Name	Used space	Volumes	Storage server type	Category	Storage server	
<input type="checkbox"/> dedup_pool_m...	65.75 GB of 1.08 TB	PureDiskVolume	PureDisk	MSDP	veritas-01.nva....	
<input type="checkbox"/> advanced_poo...	32.27 MB of 99.9 TB	/advdisk	AdvancedDisk	AdvancedDisk	veritas-01.nva....	

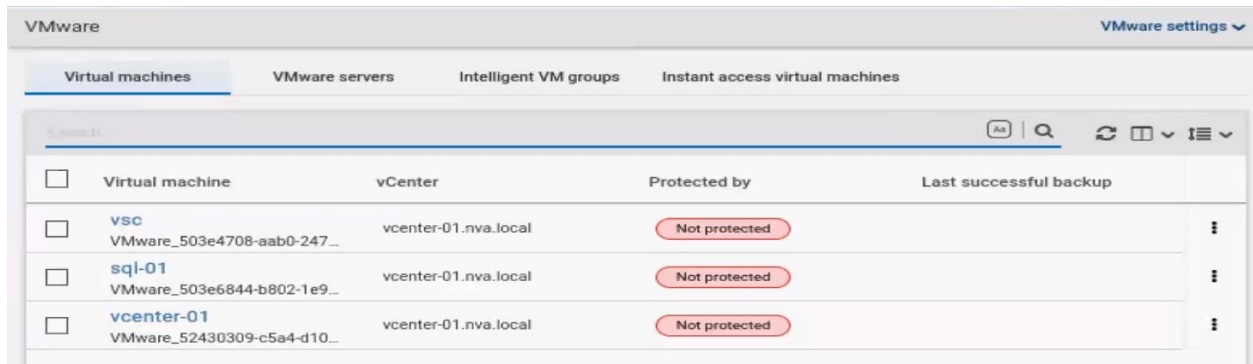
Figure 10) Configured storage units.

Storage						
Storage servers		Disk pools	Storage units	Universal shares		
Search...				Q	Y	+Add
<input type="checkbox"/> Name ^	Media servers	Category	Used space	Fragment size	Disk pool	
<input type="checkbox"/> advanced_stu...	Any available	AdvancedDisk	32.27 MB of 99.9 TB	1 GB	advanced_pool_m...	
<input type="checkbox"/> dedup_stu_ma...	Any available	MSDP	65.75 GB of 1.08 TB	50 GB	dedup_pool_master	

You can use the NetBackup web UI to add your VMware virtual infrastructure by just specifying the vCenter information—hostname, port, username, and password. After the VMware vCenter credentials are validated, a discovery operation queries the VMware infrastructure and identifies all the VMs within the environment. See Figure 11.

Intelligent VM groups can be created based on a set of filters called queries. NetBackup automatically selects VMs based on the queries and adds them to the group. You can then apply protection to the group. Note that an intelligent group automatically reflects changes in the VM environment and eliminates the need to manually revise the list of VMs in the group.

Figure 11) Discovered VMs in the VMware infrastructure.



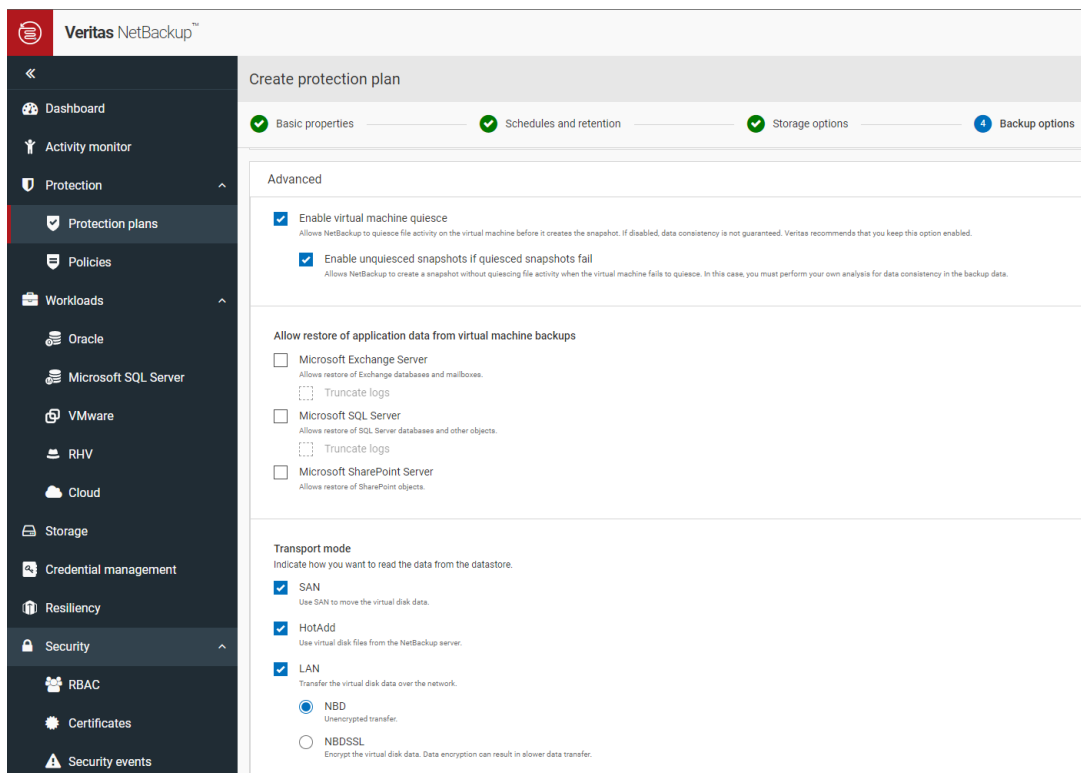
The screenshot shows the VMware interface with a table of discovered virtual machines. The table has columns for selection, virtual machine name, vCenter, protection status, and last successful backup. Three VMs are listed: vsc, sql-01, and vcenter-01, all of which are currently 'Not protected'.

<input type="checkbox"/>	Virtual machine	vCenter	Protected by	Last successful backup
<input type="checkbox"/>	vsc VMware_503e4708-aab0-247...	vcenter-01.nva.local	Not protected	
<input type="checkbox"/>	sql-01 VMware_503e6844-b802-1e9...	vcenter-01.nva.local	Not protected	
<input type="checkbox"/>	vcenter-01 VMware_52430309-c5a4-d10...	vcenter-01.nva.local	Not protected	

Both VM and intelligent VM groups are assets that can be subscribed to a protection plan. This step assigns predefined backup settings to those assets. The next step is to create protection plans for the VMware workload.

Under the Schedules and Retention tab, specify the backup schedule and start window. Under Storage options, select the backup storage where you want to store the data. Backup options enable you to select the NetBackup server to use for orchestrating agentless VMware backups. For a VMware environment, you have multiple transport options, such as SAN, NBD and HotAdd, when moving protected VM data between the VMware datastore and the backup host. Select the option that is applicable to your environment and refer to the NetBackup documentation for additional detail and best practices.

Figure 12) Configured protection plan.



The screenshot shows the 'Create protection plan' configuration screen in Veritas NetBackup. The interface includes a sidebar with navigation options like Dashboard, Activity monitor, Protection, Protection plans, Policies, Workloads, and Storage. The main area shows the 'Backup options' tab selected, with sections for 'Advanced' settings and 'Transport mode'. The 'Advanced' section includes checkboxes for 'Enable virtual machine quiesce' and 'Enable unquiesced snapshots if quiesced snapshots fail'. The 'Transport mode' section includes checkboxes for 'SAN', 'HotAdd', and 'LAN', with 'NBD' selected as the transport method.

**Veritas NetBackup™**

Create protection plan

Basic properties Schedules and retention Storage options **Backup options**

**Advanced**

☒ Enable virtual machine quiesce  
Allows NetBackup to quiesce file activity on the virtual machine before it creates the snapshot. If disabled, data consistency is not guaranteed. Veritas recommends that you keep this option enabled.

☒ Enable unquiesced snapshots if quiesced snapshots fail  
Allows NetBackup to create a snapshot without quiescing file activity when the virtual machine fails to quiesce. In this case, you must perform your own analysis for data consistency in the backup data.

**Allow restore of application data from virtual machine backups**

☐ Microsoft Exchange Server  
Allows restore of Exchange databases and mailboxes.  
Truncate logs

☐ Microsoft SQL Server  
Allows restore of SQL Server databases and other objects.  
Truncate logs

☐ Microsoft SharePoint Server  
Allows restore of SharePoint objects.

**Transport mode**  
Indicate how you want to read the data from the datastore.

☒ SAN  
Use SAN to move the virtual disk data.

☒ HotAdd  
Use virtual disk files from the NetBackup server.

☒ LAN  
Transfer the virtual disk data over the network.

☒ NBD  
Unencrypted transfer.

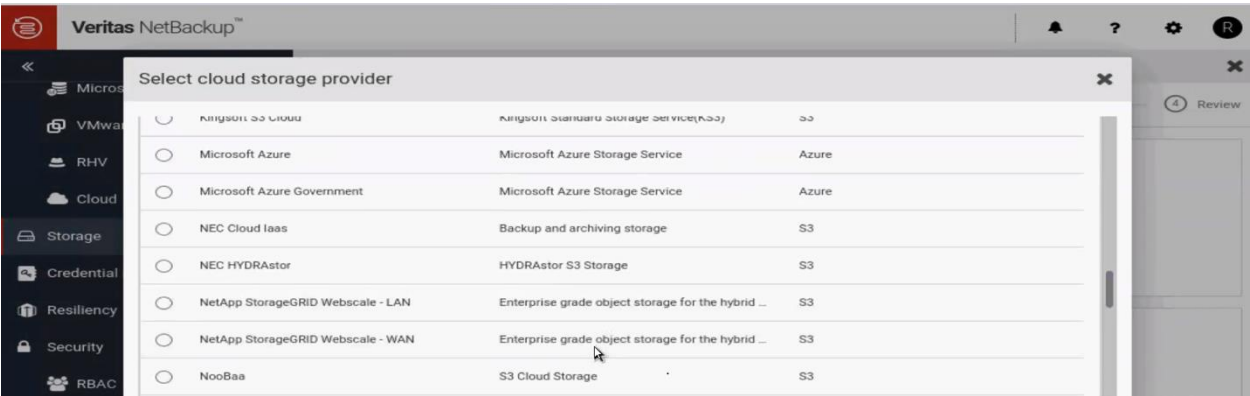
☐ NBDSSL  
Encrypt the virtual disk data. Data encryption can result in slower data transfer.



Figure 12 shows some of the available VMware backup options within a protection plan. You can also capture the Application State for Microsoft Exchange, SQL, or SharePoint workloads along with the VM backup after the agent software is deployed on the SQL VM. You can create multiple protection plans: one for protecting just the VM, while another protection plan can have the Application State Capture field selected to also protect SQL, Exchange, or SharePoint applications.

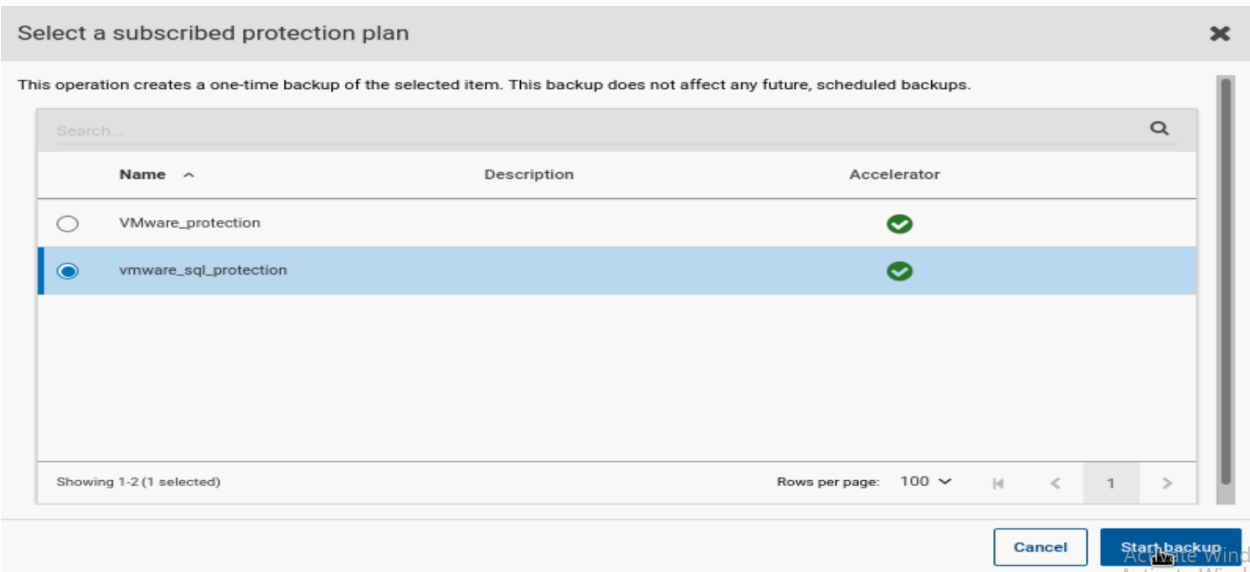
Protection plans give you the ability to write data to more than one location—a primary copy is a good candidate to be stored on deduplicated storage with another copy stored elsewhere for long-term retention (LTR). If both primary and secondary storage targets are deduplication-compatible, or object storage-based, the data can be moved in an optimized manner without the need for rehydration. NetApp StorageGRID object storage is among the supported cloud storage providers using the S3 compatible storage API. See Figure 13.

Figure 13) Veritas NetBackup supports NetApp StorageGRID as a cloud storage provider.



The last step in configuring protection for workloads is to associate the protection plan with the intelligent VM groups. After you have completed this association, the assets are protected as defined within the protection plan. See Figure 14.

Figure 14) Associate a VM intelligent group to a protection plan.





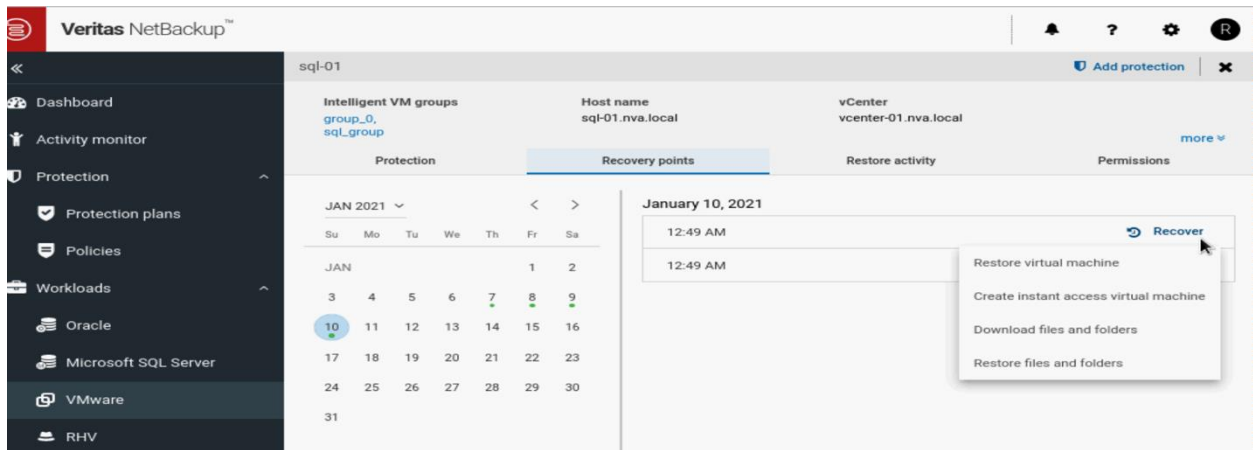
Backup jobs can be monitored in the Activity Monitor, as shown in Figure 15.

**Figure 15) Activity Monitor shows the jobs with different types of activities for the Microsoft SQL server.**

Activity monitor						
Jobs      Daemons      Processes						
Search						
Job ID	Type	Client or display name	Job state	Status code	Policy name	Sc
221	Image Cleanup		Partial success	1		
220	Backup	sql-01	Done	0	vmware_sql_prote...	DI
219	Backup	sql-01	Done	0	VMware_protectio...	DI

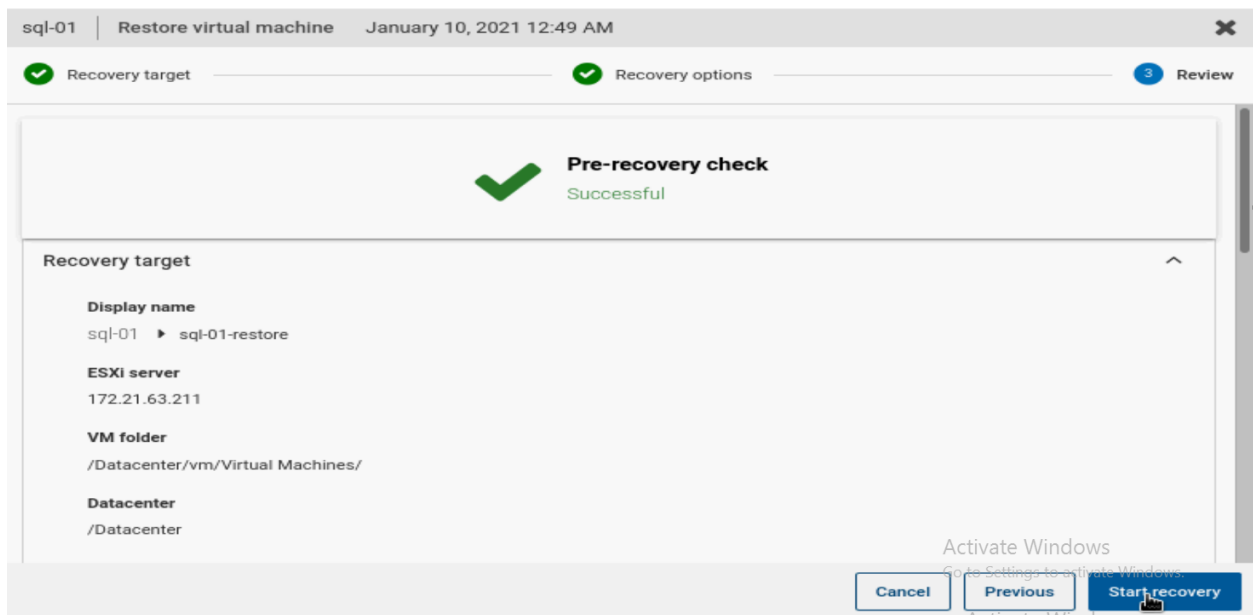
After the backup jobs are completed, you can go over the recovery process / workflow for verification or for actual recovery. In NetBackup, there are several VMware options to recover or restore from VM backups, as shown in Figure 16. You can restore the protected VM, restore files and folders, download files and folder directly from the backup image, or create an instant access VM, where a live VM can be powered up directly from the image data on backup storage.

**Figure 16) Different options for performing recovery in NetBackup.**



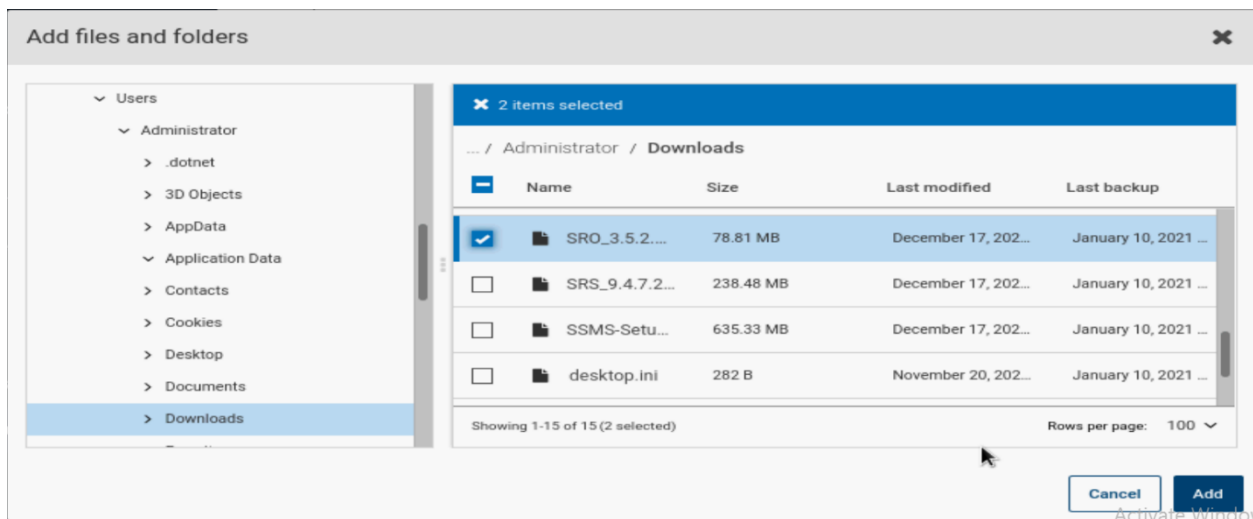
You can select the Recover Virtual Machine option to recover the entire VM. Figure 17 shows an example of a pre-recovery check that validates the provided information before the recovery process is started.

Figure 17) Recover the entire VM by using the Restore Virtual Machine option.



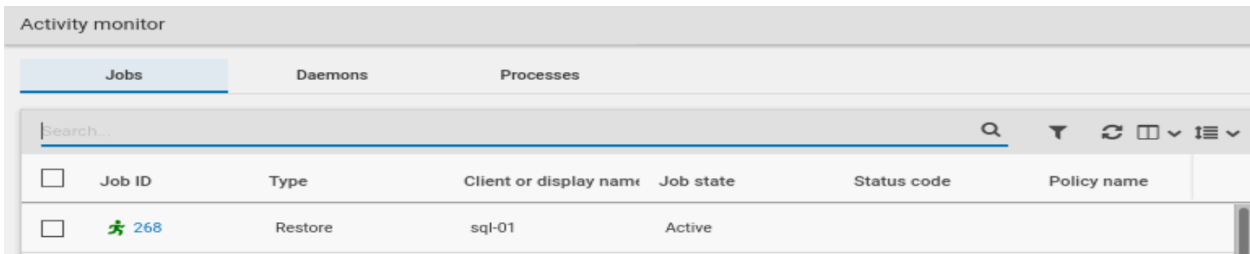
Restore Files and Folders is another option available to recover your data. Before restoring your data, you must first choose the required files and folders that you want to restore, as shown in Figure 18.

Figure 18) Add files/folders on Microsoft SQL Server that you want to restore.



After you have added the files and folders and filled out the necessary information, restore jobs start running that you can observe under Activity Monitor, as shown in Figure 19.

Figure 19) Activity Monitor shows the restore job for a VM.

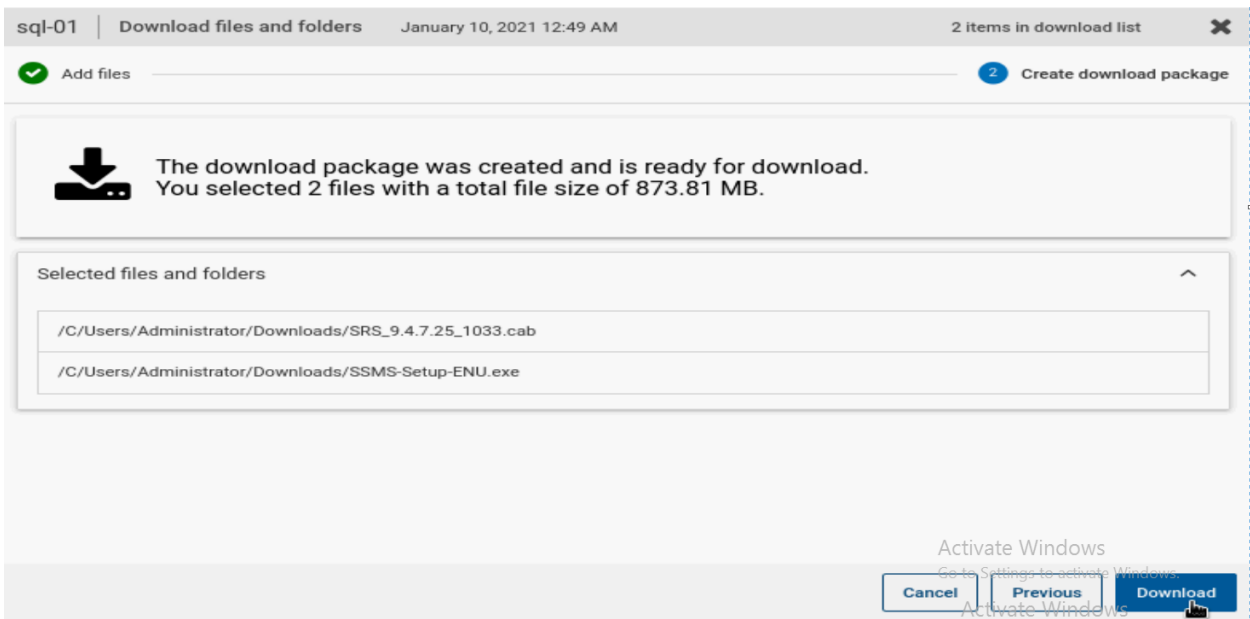


The screenshot shows the 'Activity monitor' window with three tabs: 'Jobs', 'Daemons', and 'Processes'. The 'Jobs' tab is selected. Below the tabs is a search bar and a table of jobs. The table has columns: Job ID, Type, Client or display name, Job state, Status code, and Policy name. One job is listed with Job ID 268, Type 'Restore', Client 'sql-01', and Job state 'Active'.

Job ID	Type	Client or display name	Job state	Status code	Policy name
268	Restore	sql-01	Active		

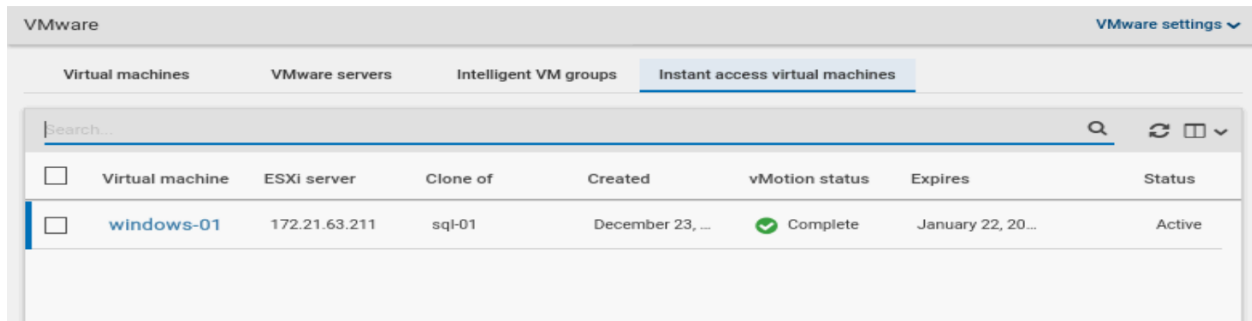
Another option is to download files and folders from the backup image by using Download Files and Folders. Similar to an online shopping cart, the VMware administrator can select specific files and/ or folders from a live browsable representation of the backup image to create a download package, as shown in Figure 20. The VM administrator can extract this download package to a workstation without the need to perform a restore operation.

Figure 20) Download files and folders from backup.



Last, but perhaps one of the most powerful options for the recovery workflow, is to create an instant access VM. This just-in-time instantiated VM is powered directly from the backup storage and registered within the vCenter environment, enabling you to treat this like any other VM in your environment. This feature requires the backup image to be stored on an MSDP storage server. See Figure 21.

Figure 21) Instant access VM created for the Microsoft SQL Server.



The screenshot shows the VMware vSphere interface with the 'Instant access virtual machines' tab selected. A table lists the virtual machines, with one instance named 'windows-01' highlighted.

	Virtual machine	ESXi server	Clone of	Created	vMotion status	Expires	Status
<input type="checkbox"/>	windows-01	172.21.63.211	sql-01	December 23, ...	Complete	January 22, 20...	Active

While the above highlights the configuration and the backup and restore workflow for NetBackup to protect the Microsoft SQL Server on VMware deployed on the NetApp Converged Infrastructure, you can use NetBackup to protect a broad range of applications and workloads running on the same infrastructure.

## Configuration and backup and recovery workflows for MS SQL instant access

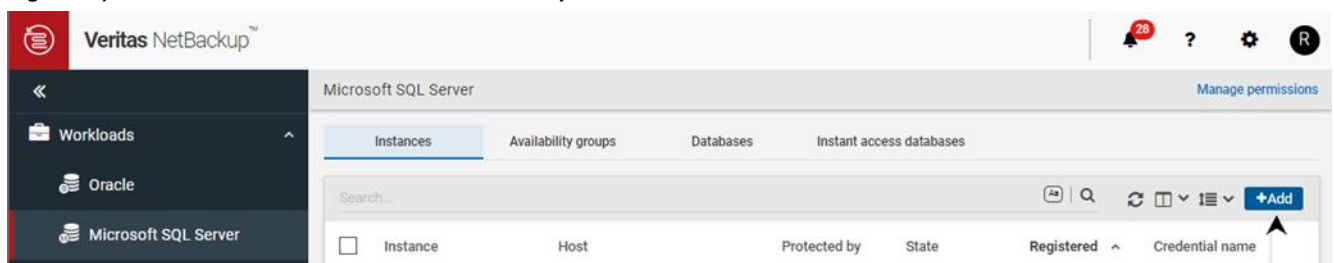
In addition to protecting MS SQL using the VMware Application State Capture method, NetBackup instant access functionality also extends to SQL as a workload, regardless of the underlying infrastructure. With instant access, the SQL database is available almost instantaneously, achieving a near-zero RTO. NetBackup mounts the database's snapshot directly on the backup storage device and treats the snapshot as a normal database.

Database administrators (DBAs) need fast access to already protected databases for many reasons. Often, ad hoc user requests come at any time of the day, including when a crisis strikes, and DBAs must be able to recover multiple databases quickly. The instant access feature enables quick recovery directly from the NetBackup media server with no data movement. DBAs can access individual files or mount in place, providing production access to databases, if needed.

You can use a single protection plan to protect multiple SQL Server instances/instance databases or a plan to protect availability groups/availability databases. You can also perform manual discovery of instances spread over multiple clients. Read-scale availability groups can also be discovered by specifying one of the replicas in the availability group and then initiating a discovery task. The NetBackup client software must be present on the SQL hosts.

The workflow is similar to that of VMware. Under Workloads → Microsoft SQL Server, click Add to specify the MS SQL Server host name and instance name. See Figure 22.

Figure 22) Add MS SQL Server instance into NetBackup.



The Permissions screen displays the roles that have access to the SQL credentials. To allow for full discovery of SQL Server assets, add or select from existing server credentials for the instances or replicas. Refer to the NetBackup Web UI Microsoft SQL Server Administrator's Guide for [requirements for](#)

[the SQL Server credentials](#). See Figure 23. The database or availability group discovery begins after the credentials are validated. Discovered SQL assets appear after the discovery process completes.

Figure 23) Add MS SQL credentials into NetBackup.

Veritas NetBackup™

Manage credentials

Credential name \*

Enter the credential name

Tag

Enter a tag for this credential

Description

Enter description

Credentials for Microsoft SQL Server

☐ Use credentials that are defined locally on the client

☒ Use these specific credentials

User name \*

Password \*

Domain \*

You can browse instances, databases, and availability groups to view their details, such as the protection plans in use, how they are protected, and available recovery points.

Create a protection plan for the workload type, Microsoft SQL Server, and define an appropriate schedule. Enabling the Perform Snapshot Backups option is a prerequisite for performing instant access operations, along with using the deduplication storage unit. See Figure 24.

Figure 24) Define MS SQL protection plan.

Veritas NetBackup™

Create protection plan

Basic properties Schedules and retention Storage options Backup options

Snapshots

☒ Perform snapshot backups

Method Automatic

Backup storage \* None selected

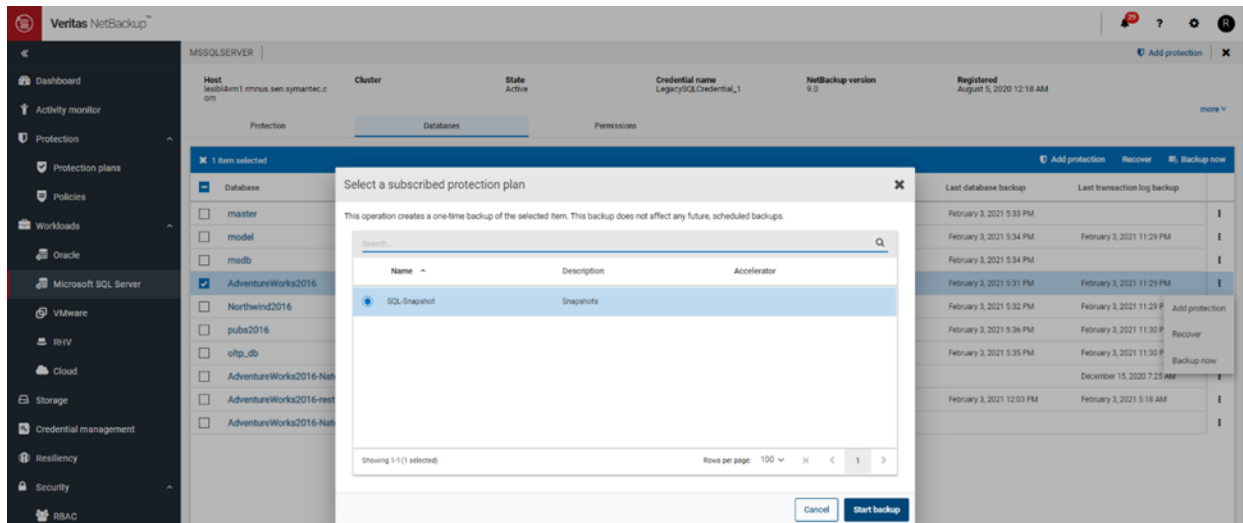
Select Backup Storage

Storage name	Accelerator	Instant access	Replication	Used space
<input type="radio"/> lexib4vm1-advdpk-OP-stu	x	x	x	12.62 % 25.24 GB of 200 GB used
<input checked="" type="radio"/> bluec01vm18-msdp-OP-stu	✓	✓	x	15.84 % 30.28 GB of 191.19 GB used

For our test, we select the AdventureWorks database and protect it immediately by using an immediate BackupNow job.

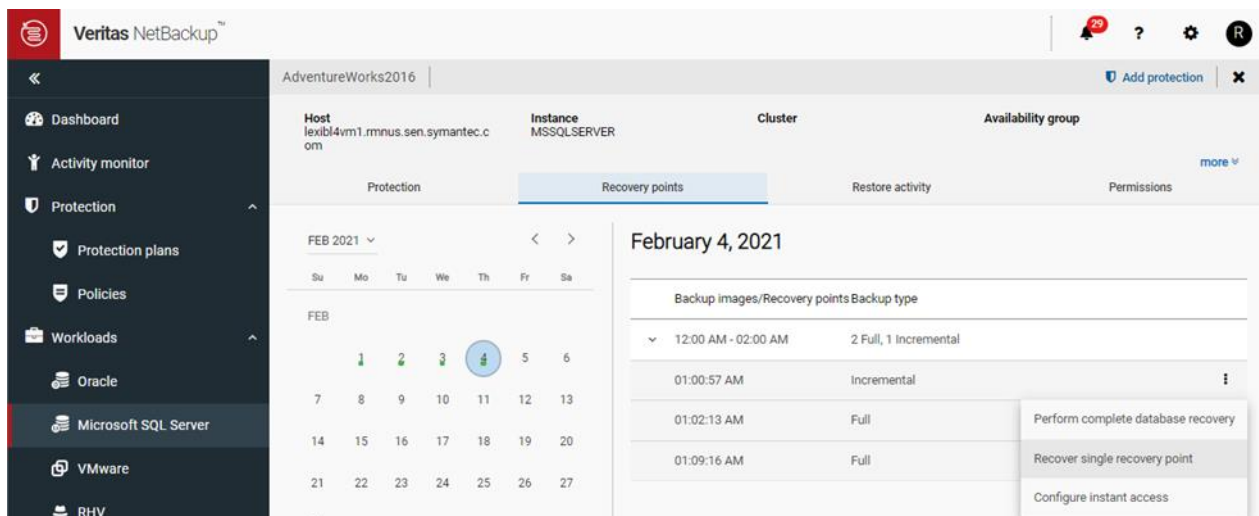
To launch a backup, from the Instances tab, choose the correct instance that contains the database that you want to protect (in this case, MSSQLSERVER). After you have selected the correct database, initiate the job by clicking BackupNow and specify an appropriate protection plan. See Figure 25. Review the Activity Monitor to verify that the job has completed.

**Figure 25) BackupNow operation for MS SQL database backup.**



From the same context menu for the database, click Recover to see available recovery points. Select a recovery point from the calendar (represented by green dots) and check the available recovery options. See Figure 27.

**Figure 26) Recovery points for MS SQL.**



You can configure an instant access database from a full, transaction log, or an incremental backup. You can also choose to add the database automatically to the existing SQL Server instance or redirect it to another registered SQL Server.

Figure 27) MS SQL—Configure MS SQL instant access recovery options.

The screenshot displays the Veritas NetBackup web interface. On the left is a dark sidebar with navigation links: Dashboard, Activity monitor, Protection (expanded), Workloads, Oracle, Microsoft SQL Server (selected), VMware, RHV, Cloud, and Storage. The main content area is titled 'AdventureWorks2016' and 'Configure instant access' for an 'Incremental' backup from 'February 4, 2021 1:00 AM'. It features a progress bar with three steps: 1. Recovery target, 2. Recovery options (current), and 3. Review. A message states: 'NetBackup will add the database to the instance and start the database.' Below this is a 'Restore to' section with fields for 'Host' (lexibl4vm1), 'Instance' (MSSQLSERVER), and 'Database name' (AdventureWorks2016). A 'Change instance' button is next to the instance field. The bottom section, 'Instance credentials for recovery target', contains fields for 'User name' (DOMAIN\user name) and 'Password' (Enter password).

You can also easily implement all these instant access features from the web UI into enterprise data protection workflows by using RESTful APIs. The NetBackup API uses the HTTP protocol to communicate with NetBackup by using JSON message format, and authentication is secured by using JSON Web Token (JWT) or an API key.

Together, Veritas NetBackup and NetApp Converged Infrastructure offer a powerful, comprehensive backup solution to help businesses meet RPOs, RTOs, and simplify administration of backups and restores. Nevertheless, for their backup and recovery plans to be effective, companies must first carefully evaluate the business requirements of their data protection solutions. After a well thought out plan is formulated, careful implementation, as well as thorough testing of the various backup and recovery scenarios are recommended. These workflow exercises and evaluations provide data for companies to assess their protection plans and workflow details in order to build up confidence in meeting their business requirements and RPO / RTO objectives.

## Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp Product Documentation  
<https://docs.netapp.com>
- NetApp ONTAP 9 Data Protection Power Guide  
<https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-dap/Data%20protection.pdf>
- TR-4704: Deploying Veritas NetBackup with NetApp E-Series Storage  
<https://www.netapp.com/media/16433-tr-4704.pdf>
- Veritas NetBackup  
<https://www.veritas.com/protection/netbackup>
- Veritas NetBackup Installation Guide  
[https://www.veritas.com/content/support/en\\_US/doc/27801100-138646475-0/v13834345-138646475](https://www.veritas.com/content/support/en_US/doc/27801100-138646475-0/v13834345-138646475)
- Veritas NetBackup Cloud Administrator's Guide  
[https://www.veritas.com/content/support/en\\_US/doc/58500769-139494412-0/v66973353-139494412](https://www.veritas.com/content/support/en_US/doc/58500769-139494412-0/v66973353-139494412)

- NetBackup Web UI Microsoft SQL Server Administrator's Guide  
[https://www.veritas.com/content/support/en\\_US/doc/138617403-138850236-0/v137933787-138850236](https://www.veritas.com/content/support/en_US/doc/138617403-138850236-0/v137933787-138850236)
- Veritas NetBackup Compatibility List  
[https://download.veritas.com/resources/content/live/OSVC/100046000/100046445/en\\_US/nbu\\_82\\_hc1.html?\\_gda\\_=1608718703\\_da475cf23e06759535996b88572367bb#netbackup\\_compatibility\\_lists](https://download.veritas.com/resources/content/live/OSVC/100046000/100046445/en_US/nbu_82_hc1.html?_gda_=1608718703_da475cf23e06759535996b88572367bb#netbackup_compatibility_lists)
- Long-Term Retention with Veritas NetBackup  
<https://www.veritas.com/content/dam/Veritas/docs/white-papers/wp-cloudstorage-with-netbackup-ltr-solution.pdf>
- Veritas NetBackup Planning and Performance Tuning Guide  
[https://www.veritas.com/content/support/en\\_US/doc/21414900-146141073-0/v19525319-146141073](https://www.veritas.com/content/support/en_US/doc/21414900-146141073-0/v19525319-146141073)
- Ransomware Guide  
[https://www.cisa.gov/sites/default/files/publications/CISA\\_MS-ISAC\\_Ransomware%20Guide\\_S508C.pdf](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf)

## Acknowledgement

The authors would like to acknowledge Gary Garcia from Veritas and Jeanie Walter, Mitch Blackburn, Alonso Devega, Bobby Oommen, Steven Pruchniewski, Joe Drake, and Carol Chan from NetApp for the assistance and guidance offered during this project execution.

## Version history

Version	Date	Document version history
Version 1.0	February 2021	Initial release.



Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

### **Copyright Information**

Copyright © 2018-2021 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

### **Trademark Information**

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4879-0221