COHESITY

VMware vSphere Data Protection Best Practices with Cohesity

Version 1.4

March 2026

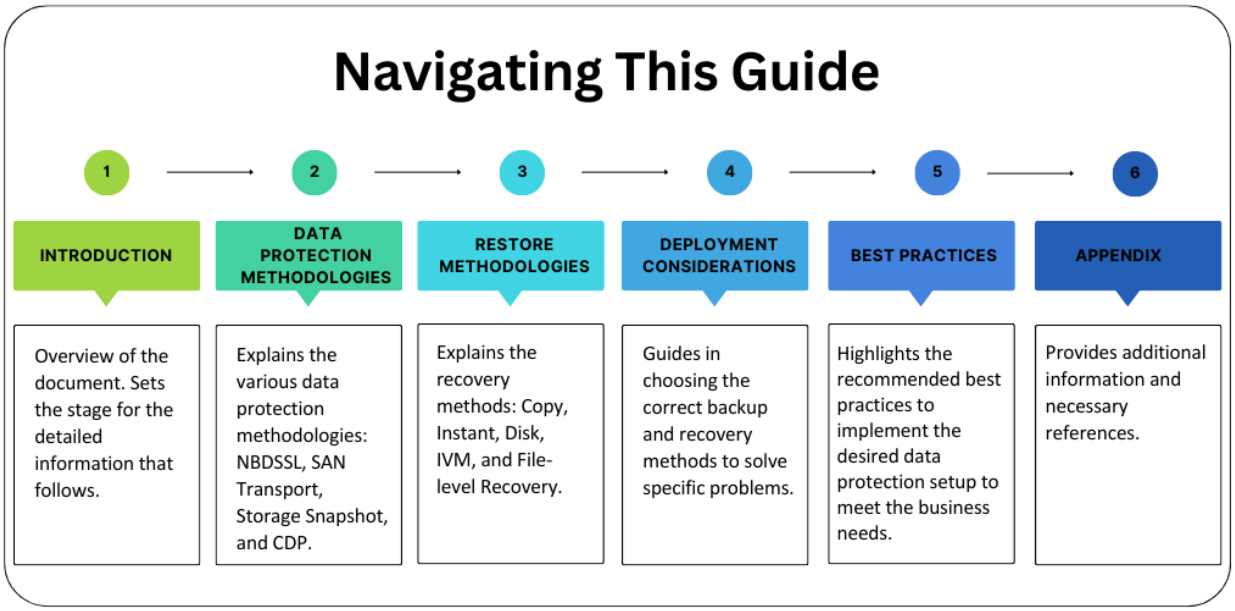
ABSTRACT

An overview of VMware vSphere data protection and recovery workflows and the best practices and related recommendations. Note that the guide does not cover protection of other VMware products such as VMware Cloud Director and VMware Cloud.

Table of Contents

Figures

Tables


Navigating This Guide
1
2
3
4
5
6
INTRODUCTION
DATA PROTECTION METHODOLOGIES
RESTORE METHODOLOGIES
DEPLOYMENT CONSIDERATIONS
BEST PRACTICES
APPENDIX
Overview of the document. Sets the stage for the detailed information that follows.
Explains the various data protection methodologies: NBDSSL, SAN Transport, Storage Snapshot, and CDP.
Explains the recovery methods: Copy, Instant, Disk, IVM, and File-level Recovery.
Guides in choosing the correct backup and recovery methods to solve specific problems.
Highlights the recommended best practices to implement the desired data protection setup to meet the business needs.
Provides additional information and necessary references.

VMware vSphere Data Protection with Cohesity

Cohesity Data Cloud is Secure and manages your entire data estate with a single platform. It reduces your attack surface, lowers the cost, and minimizes risk. Cohesity Data Cloud features enable protecting data at the enterprise scale, eliminating silos, and reducing TCO using a modern platform. Cohesity provides flexible deployment options such as Software-as-a-service (SaaS), Self-managed, and Service-provider-managed, to meet your business goals and objectives.

You can protect and manage your workloads and execute all available protection workflows seamlessly with a single pane of glass.

This guide focuses on VMware vSphere Data Protection and does not cover the protection of other VMware products such as VMware Cloud Director, VMware Cloud, etc. Its objectives are to provide a high-level overview of available protection and recovery workflows along with their related recommendations and best practices. The best practice recommendations in this guide are not meant as a replacement for tuning resources based on specific user environments or technical documentation published on https://docs.cohesity.com/HomePage/Content/home.htm.

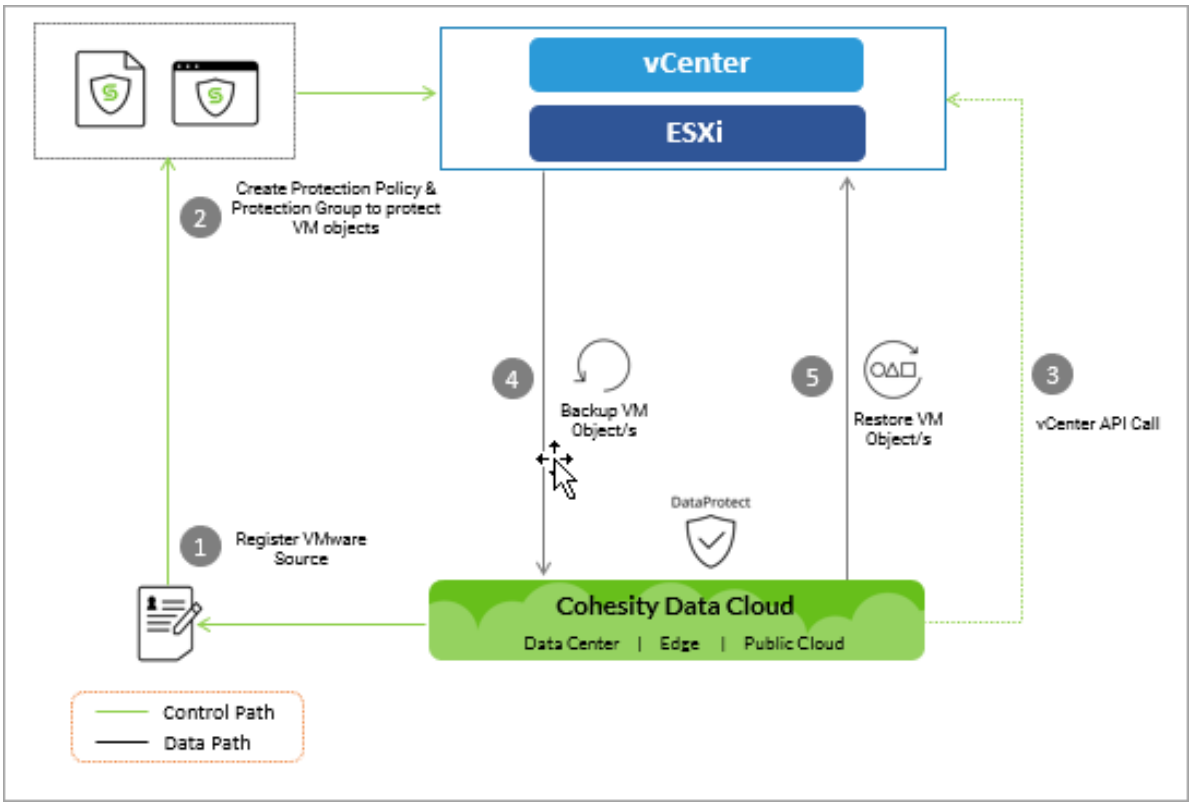
VMware Data Protection Methodologies

Let's look at the architectural flow of Cohesity VMware data protection and the various protection methods that Cohesity offers.

Cohesity Data Cloud natively integrates with VMware vSphere and leverages the available VMware vSphere Storage APIs for Data Protection (VADP) and VMware vSphere APIs for I/O Filtering (VAIO), eliminating the need to install in-guest agents across the VMs.

Cohesity Architecture for VMware Data Protection

Figure 1: Cohesity Architecture for VMware Data Protection



NOTE: Cohesity does not generalize any specific backup method to be a better choice than the others. The effectiveness of a backup method depends on various factors such as the underlying infrastructure, specific SLAs, and existing bottlenecks.

Cohesity Differentiators for VMware Data Protection

1. One Platform—Cohesity cluster is a true scale-out and fully redundant architecture allowing non-disruptive upgrades across software and hardware offering fully protected writes.
2. Best-in-class global space efficiency—Offers advanced features such as variable-length, sliding window dedupe, and Zstd Compression.
3. Faster backups and recovery with MegaFiles—Cohesity's proprietary technology MegaFile divides large virtual disks into smaller parts, which allows reading the disk faster with multiple parallel streams. It then distributes the smaller parts across multiple Cohesity nodes, allowing parallel-distributed ingest and enable faster backups.
4. Minimize the latency issues such as VMware VM Stun on production applications—With Cohesity's faster backups, the protection run completes in less time reducing the VM snapshot lifespan at the vCenter. With a reduced VM snapshot lifespan, the associated VM stun impact is also greatly minimized. VMs running very high change rate applications could be impacted by the VM stun issue during backups to which Cohesity provides a solution with its parallel-distributed data ingest feature.
5. Recover at scale—With Cohesity's instant mass restore, users can quickly recover multiple VMs and virtual infrastructure in a sandbox environment or a clean room during ransomware or cyber incident recovery scenarios.
6. Cohesity SnapTree™ Technology—SnapTree is a 'Distributed-Redirect-on-Write' (DROW) snapshot mechanism that provides speed and scalability in addition to the inherent benefits of RoW snapshot. The design is optimized for write performance, so any changes are redirected to new blocks. Additionally, all nodes participate in this process, thereby leveraging the scalability elements of the Cohesity cluster.
7. Improved recovery performance—With Cohesity SnapTree™ Technology and Hydrated snapshots, Cohesity allows for quicker recoveries as it does not have to traverse through chains of backup snapshots. It only needs one hop to reach the selected PiT.

Prerequisites

1. *VMware privileges for Cohesity*—The Cohesity cluster must perform various actions on the source. For the Cohesity cluster to perform these actions, the user specified to connect to the source (the one used to register the source) must have adequate privileges. For more information on the required privileges refer to Ensure Adequate Privileges for Cohesity.
2. *Firewall port requirements*—You must open certain ports in the firewall to allow the Cohesity cluster to transmit and receive data. The cluster sends different types of traffic (Management, backup, restore, replication, etc.) over the network. Refer to Manage Firewall Ports and Virtualization-VMware for all the required ports and for VMware protection ports, respectively.

Protect VM—NBDSSL (Default)

Cohesity provides NBDSSL as a default and as an out-of-the-box backup method—with no additional settings/configuration needed. This method (Transport mode) leverages existing LAN connectivity between ESXi hosts and Cohesity to transfer the VM protection data (VADP snapshot) over to the Cohesity cluster and does not require specialized infrastructure or configurations. The simplicity and ease of configuration and administration make this method the most widely used in environments running 10 Gbps or higher bandwidth networks. See the Protection group section in the online help for stepwise instructions to protect VMs. For more information, see Cohesity VM Backup Workflow - NBDSSL.

NOTE: VMware does not support protecting VMs with NBDSSL over WAN. VMware supports and recommends NBDSSL for LAN networks with 10 Gbps or higher bandwidth.

Protect VM—Leverage Storage Snapshot

Cohesity provides in-built support for qualified third-party storage arrays (Snapshot Providers) for leveraging Storage Array-based snapshots for VMware VM backups. Cohesity-qualified storage arrays (snapshot providers) are Cisco HyperFlex, Nutanix, NetApp, Nimble, HPE Alletra 5000/6000, Pure FlashArray and IBM FlashSystem.

- ***For IBM, Pure, HPE Alletra and Nimble storage systems (Storage Snapshot v2)***—Cohesity integrates with VMware to leverage Storage Snapshot and transfer the data using iSCSI or FC. In this protection mechanism, the VMware VADP snapshot is created and is alive only until the corresponding snapshot in the storage array is created. Hence reducing the VMware snapshot lifecycle.

  NOTE:

  - Starting Cohesity release 7.2, Storage Snapshot v2 is the default and only available option when the VM is provisioned on Pure FlashArray, Nimble, Alletra 5000/6000 or IBM FlashSystem SAN Storage.
  - SAN connectivity (FC or iSCSI) between Cohesity and the Storage Array is a pre-requisite.
  - In this workflow the VM backup data is transferred from Storage Array to Cohesity nodes over the configured iSCSI or FC SAN medium.

- ***For NetApp storage systems (Storage Snapshot v1)***—Cohesity integrates with VMware, triggers a Storage Snapshot and transfers the data using NBDSSL. In this protection mechanism, the VMware VADP snapshot is created and is alive only until the corresponding snapshot in the NetApp storage array is created. Hence reducing the VMware snapshot lifecycle.
- ***For Cisco HyperFlex*** —Cohesity triggers the vendor-specific native snapshots and transfers the data to Cohesity.
- ***For Nutanix systems***—Cohesity triggers the vendor-specific native snapshots (no VADP snapshots) and transfers the data to Cohesity.

This feature is only applicable for the VMs residing on storage carved from Cohesity-qualified storage arrays. To enable storage snapshots during VM protection, users need to register the storage snapshot provider in the Cohesity UI and also enable the toggle option "***Leverage Storage Snapshots for Data Protection***" in the protection group. If storage snapshot creation fails, Cohesity helps protect VMs by

falling back to the process described in the section: **Cohesity Architecture for VMware Data Protection.**

NOTE: Protecting VM with NBDSSL over WAN is not supported. VMware supports and recommends NBDSSL for LAN networks with 10 Gbps or higher bandwidth.

Refer to step #15 *Leverage Storage Snapshots for Data Protection* in Add or Edit a Protection Group for Virtual Servers for the how-to steps and for more information.

For more information, see VM Backup with NBDSSL and Storage Snapshot v1 (NetApp Only) and VM Backup with iSCSI or FC SAN and Storage Snapshot v2 (Pure, Nimble, Alletra and IBM)

Protect VM—SAN Transport (FC OR iSCSI)

In this backup method, Cohesity leverages VMware SAN Transport Mode to transfer the VM protection data over Fiber Channel or iSCSI SAN to the Cohesity cluster. VMware keeps the VADP snapshot alive until the backup process completes and consolidates the snapshot thereafter. To enable SAN transport mode, users need to first zone the storage array with the Cohesity cluster nodes, configure the device mapping in the storage array, and scan the devices on Cohesity. Also, the toggle option "**Leverage SAN Transport for Data Protection**" needs to be selected in the protection group to use the SAN transport mode. Cohesity also provides an extra option to failover to the NBDSSL protection mechanism in case the SAN transport mode is unable to complete the protection process. See the SAN transport section (Point# 16) in online help to understand how to set the same during protection group creation or edit.

For more information, see Cohesity VM Backup Workflow – SAN Transport (FC+iSCSI).

Protect VM—Continuous Data Protection (CDP)

Cohesity Continuous Data Protection offers near zero RPO. This backup method is intended for VM backup and Disaster Recovery use cases. Cohesity uses the VMware API for I/O Filtering (VAIO) based solution for providing Continuous Data Protection. In this process, Cohesity deploys a Cohesity I/O Filter Daemon on the ESXi hosts and attaches the Cohesity IO Filter (VMware Storage Profiles) to each VM disk being protected. Every IO from Guest OS to disk is intercepted by the Cohesity IO filter and transferred to the Cohesity cluster. CDP protection is not a standalone offering and is interleaved with VADP backups in the protection group. CDP is enabled at the protection policy level along with the backup definition. At the Cohesity cluster, it maintains both the VM disk snapshot and CDP logs as available PiT for recovery. The First Protection run is a VADP full backup, following which the CDP IOs are logged in Cohesity CDP logs. The scheduled backup runs are incremental as usual. Cohesity maintains the CDP log as per the defined CDP retention in the policy. During recovery, the user can choose the available PiT from the CDP log or alternately use the periodic Cohesity snapshots.

If CDP detects a hole in the received IOs (missed IOs) caused due to events such as disk removal, disk resize, network issues, etc. a VADP incremental snapshot is triggered to get the CDP to a stable state.

For more information, see Cohesity Continuous Data Protection (CDP).

Figure 2: CDP Policy

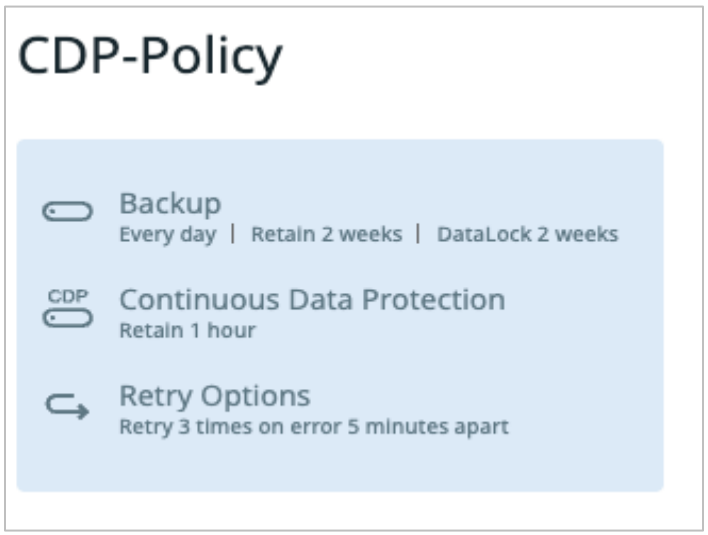


Table 1: Summary - Cohesity Protection Methods and Comparisons

	VM Backup	VM Backup with Storage Snapshot	VM Backup with SAN Transport	VMware Continuous Data Protection (CDP)
Transport Mode	NBDSSL via LAN	Over FC/iSCSI SAN NBDSSL via LAN (NetApp only)	Over FC/iSCSI	LAN
VADP Snapshot Lifetime	Until Backup Completes	Until Storage Snapshot is created	Until Backup Completes	Until completion of 1st Full Backup
Storage Snapshot Support	N/A	Yes	N/A	N/A
Reduction in Stun Issue	Yes	Yes	Yes	N/A
Support for App Consistency	Yes	Yes	Yes	Yes
Additional Settings Required	No	Yes	Yes	Yes (Protection Policy)
Fallback option available	No	No	Yes, to NBDSSL	N/A

	VM Backup	VM Backup with Storage Snapshot	VM Backup with SAN Transport	VMware Continuous Data Protection (CDP)
Register Storage Array Source	No	Yes	No	N/A
User Considerations	Simple, default and Out-Of-The Box protection method. For more information, see VM Backup Using NBDSSL	Leverages Storage Snapshots if you have IO-intensive VMs in your VM farm. For more information, see VM Backup with NBDSSL and Storage Snapshot	LAN-free Backup for Traffic segregation and improved backup transfer speed. For more information, see VM Backup using Continuous Data Protection	Offers near Zero RPO For more information, see VM Backup using Continuous Data Protection

VMware Restore Methodologies

This section describes the various restore methods for VMware VM Recovery that Cohesity offers.

Recovery from Cohesity VMware backups can be performed at different levels of granularity and to both the original and alternate locations. Cohesity provides flexibility to perform Full or Partial Recovery operations per business requirements. Full VM Recovery allows you to recover the entire VMware VM while partial recovery allows you to recover individual files and folders, individual virtual disks, or simply use the Instant Volume Mount recovery. Using the “Existing VM Handling” (None, Overwrite Existing VM or Keep Existing VM) feature allows you to choose how you want to handle the original VM when recovering to the original location.

Full VM Recovery

- VMware VM Copy Recovery
    - VMware VM Differential Recovery
- VMware VM Instant Recovery
- VMware VM Test & Dev (Cloning)

Partial VM Recovery

- VMware File Level Recovery
- VMware Disk Recovery
- VMware Instant Volume Mount (IVM) Recovery

NOTE: Starting Cohesity release 7.3.1, you can cross recover VMware VMs between VMware On-Prem sources and Azure VMware Solution. Refer to Appendix for more information.

Full VM Recovery

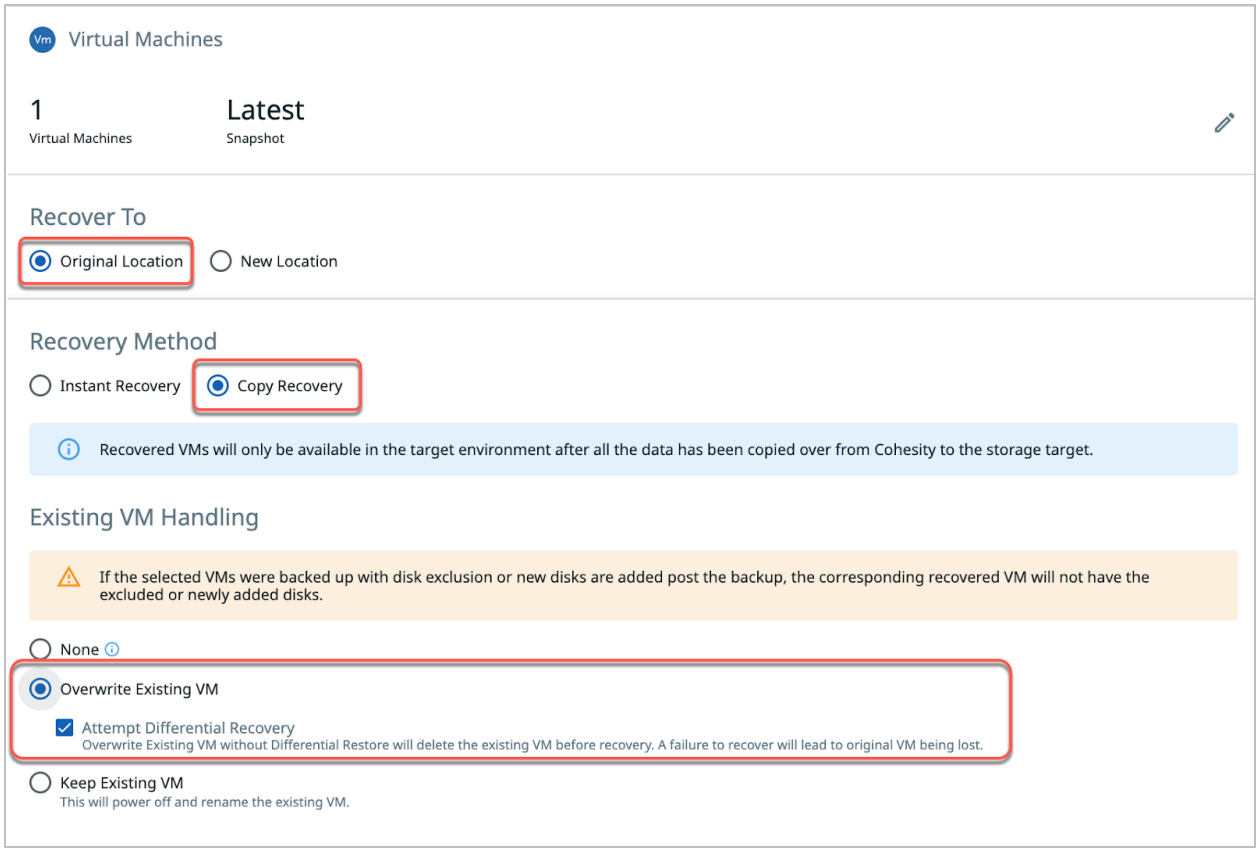
VMware VM Copy Recovery

You can recover your protected VMware VMs from a Cohesity cluster or a currently registered Cloud Archive. In this recovery process, Cohesity leverages VMware VDDK APIs for the data movement between the VMware environment and the Cohesity cluster. In this case, the entire VM is restored and is made available for user access only after the recovery completion, offering predictable VM performance. This is the only recovery option available if you choose to use SAN Transport for recovery.

VMware VM Differential Recovery

Cohesity provides the extra ability on top of the Copy Recovery process to restore only the blocks that have changed since the last good point in time from which restore has been initiated. This option is available only if you have selected “Overwrite Existing VM” and the Recovery Type option as “Copy Recovery” in the Recover Job.

Figure 3: Full VM Recovery



VMware VM Instant Recovery

Cohesity provides a way to restore your VMs in less time and make them instantly available for clients' access. In this process, the Cohesity internal view is mounted as an NFS datastore on the ESXi. The VM is recovered from backup and powered ON from the Cohesity datastore, making it available almost instantly. In the background, Cohesity initiates a storage vMotion to transfer the data to the VM’s primary datastore. The recovered VM consumes Cohesity datastore for Disk IO activity while Storage vMotion is in progress. Upon storage vMotion completion, the Cohesity-mounted datastore is unmounted from the ESXi hosts, and the recovered VM starts using its primary datastore for its Disk IO activity.

Cohesity allows Instant Recovery of multiple VMs simultaneously enabling users to Recover at Scale (aka Instant Mass Restore) from any available Point In Time. This feature enables its users to recover multiple VMs instantaneously in recovery scenarios such as ransomware and cyber incidents in a sandbox environment. Please note that there is currently no limit to the number of VMs you can restore using Instant Recovery.

VMware VM Test & Dev (Cloning)

Cohesity empowers developers to instantiate the latest backup of their production application stack and run it directly off Cohesity, providing a unified foundation for copy data management. Instant, zero-space clones enable businesses to quickly spin up test/dev environments from a backup, enabling rapid test and development from actual data without any capacity overhead.

Cohesity provides the ability to clone objects from snapshots created by a Protection Group. The cloned objects are copied to a new location, rehydrated, and restored to a running state. For example, when a VMware object is cloned in an on-premises Cohesity cluster, new VM files (such as VMDKs) are created from snapshots and stored in a view on the Cohesity cluster. This view becomes the datastore for these VM files. The Cohesity cluster creates new VMs in the selected resource pool by mounting the view containing the new VMDKs as the datastore on the ESXi hosts. Refer to Clone VMs for how-to steps.

After the required testing operation on the Clone VMs is complete, the user needs to Teardown the Cloned VMs created by the Clone Task. Refer to Tear Down a Clone for how-to steps.

The following actions occur during a teardown of a Cloned VM:

1. The Cohesity cluster deletes the compute instances of the cloned VMs in the ESXi host.
2. The VM files (such as VMDK and VMX) are deleted on the view acting as a datastore.
3. If no VMs are using the view (datastore), the view is unmounted from all ESXi hosts.

Partial VM Recovery

VMware File Level Recovery

Cohesity provides the ability to recover files and folders from a snapshot created earlier by a Protection Group. This recovery method presents two recovery options:

- *Recover Files or Folders*—Recover files or folders to the original location or a new location. You could recover files and folders using the VMware tool, existing Cohesity agent, or by deploying an ephemeral Cohesity agent on the target VM.
- *Download a File or Folder*—Download a file or folder from an existing snapshot. Downloading files and folders does not require a Cohesity agent. If you are recovering a single file, this option downloads the file to your browser's download folder. For all other selections, this creates a recovery task. When the task is completed, from the Recoveries page in Cohesity UI, click the task name and then click Download Files to download the generated zip file.

VMware Disk Recovery

Cohesity Restore mechanism provides a way to granularly restore individual VM disks. In this workflow, the virtual disk is extracted from the Snapshot and stored temporarily in the View (datastore) on the Cohesity cluster. The disk is then migrated (Storage vMotion) to the specified datastore and then attached to the original VM or an alternate VM (as desired) in the same vCenter. The disk becomes available upon recovery completion, and a rescan might be required at the Guest OS level for disk access.

VMware Instant Volume Mount (IVM) Recovery

Cohesity Restore mechanism provides a way to granularly restore a volume from a disk. This feature allows the selected backup volumes to be made available at the target location where you can then complete the desired operations. Instant mounting is only available for backup volumes stored locally. Use cases include volume presentation to 3rd party software for granular recovery of Microsoft Exchange, SQL, and SharePoint data.

IVM of Windows VMs—Cohesity view is mounted as an NFS datastore on the ESXi host, and VMDKs are just attached to the VM, and the VM may or may not bring the disks online. Cohesity cluster does not explicitly bring the disks online within the VM. If the option “Ensure Disks are Online” is selected in the workflow, the Cohesity cluster explicitly brings disks online on the VM and mounts the volume almost instantaneously. Cohesity agent (existing agent or a new ephemeral agent) and VMware tools are required on the VM for bringing disks online and mounting the volume.

IVM of Linux VMs—Cohesity view is mounted as a mount point on the VM. Further, the volumes selected in the IVM workflow are loop mounted, and their path is displayed on the Recovery job details page in the Cohesity UI. Cohesity agent (existing agent or a new ephemeral agent) and VMware tools are required for mount operation.

After the required operations on the IVM mounts are complete, the user needs to perform a Teardown operation of the recovery job from Cohesity UI.

Table 2: Cohesity Recovery Methods and Comparisons

Factors \ Restore Method	Copy Recovery	Instant Restore	File Level Restore	Disk Restore	Instant Volume Mount
Full VM Restore	Yes	Yes	No	No	No
Restore of unindexed VMs	Yes	Yes	Yes *Using browse option	Yes	Yes
Differential Restore	Yes *Only if, Overwrite Existing VM is selected	No	NA	NA	NA
Restored VM throughput	Predictable	Considerate	NA	NA	NA

Factors \ Restore Method	Copy Recovery	Instant Restore	File Level Restore	Disk Restore	Instant Volume Mount
Storage vMotion Required	No	Yes	No	Yes	No
Cohesity Sub task (Restore in parallel / sequential)	1 sub-task per disk	1 task for all VMDKs being restored	Parallel	1 sub-task per disk	Parallel (Multiple volumes to 1 VM)
User Considerations	Need VM to be served from the primary storage faster without any performance degradation. For more information, see VM Restore using Copy Recovery	Need Instant access to essential services for VMs like AD or DNS, which other VMs depend on for their operations. For more information, see VM Restore using Instant Recovery	Need to restore File and Folders. Requires Indexing, Cohesity Agent, and VMware Tools for recovery. For more information, see VM File/Folder Restore using File Level Recovery	Need to restore virtual disks only and not the whole VM. For more information, see VM Disk Restore	Need to restore a volume from a VM disk. For more information, see VM Instant Volume Mount

Deployment Considerations - VMware VM Protection

It is important to choose a particular backup or recovery workflow that solves a given problem. This section provides a decision tree on when a workflow should be used.

VM Backup Using NBDSSL

This is the default backup method for VMware Data Protection that is available as an out-of-the-box feature with Cohesity. Use this when:

- Your existing infrastructure does not support the other backup methods or if your backup requirements do not demand utilizing the benefits of other methods (SAN Transport and Storage Snapshots).
- You have only the default VMware infrastructure available for protection.
- You know that your VMKernel and VMware LAN infrastructure can take the load of the VM traffic as well as the VM backup/restore process (Snapshot lifecycle, data transfer, etc.).

Make sure you have a LAN network bandwidth of 10 Gbps or higher. Refer to Add or Edit a Protection Group for Virtual Servers for the how-to steps and for more information.

> **NOTE**: Protecting VM with NBDSSL over WAN is not supported. VMware supports and recommends NBDSSL for LAN networks with 10 Gbps or higher bandwidth.

VM Backup with NBDSSL and Storage Snapshot v1 (NetApp Only)

> **NOTE**: Cohesity Storage Snapshot v1 is only used when the VM is provisioned on NetApp NFS datastore. Does not apply to any other Storage Snapshot Provider.

Use when you have a specific set of high transactional busy VMs provisioned on NetApp NFS datastore and are experiencing VMware VM Stun issues.

- Data transfer in this mode happens via LAN. Make sure that your VMKernel and VMware LAN infrastructure can take the load of the VM traffic as well as the VM backup/restore process and do not get overwhelmed by the transfer of data.
- Make sure that the infrastructure can take the load of the Temporary VM that is created during the process.
- By default, this mode falls back to VADP VM Snapshot only if storage snapshot creation fails.
- This workflow is only supported if the VMs being protected reside on NetApp storage array and if the NetApp storage array is a registered source in the Cohesity cluster.
- You can leverage only one storage snapshot provider for a particular Protection Group.

- To leverage storage snapshots, the VM being protected should not have disks provisioned from multiple storage systems. All the disks being protected may be from different datastores but from a single storage system.
- When mounting NFS NetApp volumes as datastores on the ESXi host, you must select the datastore type as NFS.
- By default, the Cohesity cluster refreshes the added NetApp source volumes every 8 hours. If new NetApp volumes are mounted on the ESXi host, you must ensure to refresh the NetApp source on the Cohesity cluster manually.

If you wish to configure VMWare VM backup leveraging Storage Snapshot, refer to section How to configure VM backup leveraging Cohesity Storage Snapshots for Data Protection of the Appendix.

VM Backup with iSCSI or FC and Storage Snapshot v2 (Pure, Nimble, Alletra and IBM)

> **NOTE**: Starting Cohesity release 7.2, Storage Snapshot v2 is the default and only available option when the VM is provisioned on Pure FlashArray, Nimble, Alletra 5000/6000 or IBM FlashSystem SAN Storage. In this workflow the VM backup data is transferred from Storage Array to Cohesity nodes over the configured iSCSI or FC SAN medium.

Use when you have a specific set of high transactional busy VMs experiencing VMware VM Stun issues.

- Data transfer in this mode happens via configured iSCSI or FC SAN.
- Ensure the iSCSI/FC connectivity between the Storage Array and Cohesity Nodes is configured and in place.

  > **NOTE**: iSCSI/FC SAN connectivity requirement does not apply when protecting VMware VMs that are provisioned from NetApp NFS datastore.

- By default, this mode falls back to VADP VM Snapshot only if storage snapshot creation fails.
- This workflow is only supported if the VMs being protected reside on Cohesity-qualified storage arrays (Pure FlashArray, Nimble, Alletra 5000/6000 or IBM FlashSystem) and if that storage array is a registered source in the Cohesity cluster.
- You can leverage only one storage snapshot provider for a particular Protection Group.
- To leverage storage snapshots, the VM being protected should not have disks provisioned from multiple storage systems. All the disks being protected may be from different datastores but from a single storage system.
- When mounting Pure, IBM, Nimble or HPE Alletra 5000/6000 volumes as datastores on the ESXi host, you must select the datastore type as VMFS.

If you wish to configure VMWare VM backup leveraging Storage Snapshot, refer to section How to configure VM backup leveraging Cohesity Storage Snapshots for Data Protection of the Appendix.

VM Backup using SAN Transport Mode (FC or iSCSI)

Use this method when you need to segregate your backup traffic and do not want to use your VMware LAN infrastructure for backup data transfer.

- SAN Transport mode is supported only with Physical Cohesity Cluster deployment.
- Use when you do not have VMs residing on vVol or VSAN datastores. This is a VMware limitation.
- Viable approach for ESXi clusters with limited L3 ethernet and/or firewall/security considerations. For example, you have 1 Gbps LAN network availability and SAN network bandwidth is higher.
- Make sure zoning is properly configured from the Storage Array to the Cohesity node (with FC adapters). Zoning is not required for an iSCSI configuration.
- Make sure that the required LUN mapping is correctly configured at the storage system level. This involves granting Cohesity Node WWN access to the datastore (LUN/Vol).
- Scanning/Discovery of LUNs must be done before backup initiation. Make sure the script to perform LUN discovery and bridge_proxy service restart is run on the Cohesity cluster when:
  - You add VMs to protection that reside on new LUNs.
  - You add new nodes to existing Cohesity Cluster.
- LUN discovery is also required every time new Datastore/LUNs/Vols are provisioned, or new FC Nodes (3rd party storage vendor, or Cohesity) are added.
- Cohesity recommends enabling the option “Allow NBDSSL Transport Fallback” so that the VM protection does not fail when there is a SAN communication issue. However, make sure the Production LAN bandwidth is 10 Gbps or higher and can withstand the production and backup traffic. This may result in violating SLAs but will make sure that the data is protected.
- Restoring using SAN transport is limited to Copy Recovery only. However, VMs backed up with this method can be restored with all other restore methods using LAN.
- Cohesity allow enabling either *Leverage Storage Snapshots* or *Leveraging SAN Transport for Data Protection* but not both.

If you wish to configure VMWare VM backup leveraging SAN Transport for Data Protection, refer to section How to configure VM backup leveraging SAN Transport for Data Protection of the Appendix.

VM Backup using Continuous Data Protection

Use this method when your business-critical VMs require Near Zero RPO.

- In the workflow, Cohesity deploys an IO Filter Daemon at the vCenter Cluster level and attaches the IO Filter storage profile to all the VM disks being protected.
- Every VM disk IO is intercepted by the IO filter and transferred to Cohesity over a configured network.
- CDP supports protecting VMs with tolerant high change rates starting with Cohesity 7.0 and higher. The Cohesity cluster should be sized appropriately to support this.
- CDP is not a standalone offering, and it interleaves with regular VADP-based protection.
- CDP allows for recovery using CDP snapshots as well as regular VADP Snapshots as needed.
- You can perform a point-in-time recovery of VMs, files and folders, Virtual Disks, and IVM of a CDP-based Protection Group by selecting the points in the timeline bar on the recovery page.

Refer to Cohesity CDP for VMware for the how-to steps and for more information.

VM Restore using Copy Recovery

Use this method when you need predictable VM performance on the recovered VM immediately upon recovery. This may be needed for recovering VMs running IO-intensive business-critical applications.

- In this recovery workflow, the VM is available after the full recovery process is complete. Use this recovery method for VMs\ applications that have tolerant RTO definitions as per business objectives.
- When recovering to the original location with the “Existing VM handling” option “Overwrite Existing VM” selected, be informed that the actual original VM will be deleted before recovery. The recovered VM will have the original VM name.
- This is the only available recovery option when using SAN Transport mode. Also, note that all SAN transport prerequisites must be met.

Refer to Recover VMs to the Original Location for more information and steps to recover VMs to the original location.

Refer to Recover VMs to a New Location for more information and steps to recover VMs to a new location.

NOTE: Starting release 7.3.1, Cohesity now supports teardown of failed VM recovery and VMDK recovery tasks, allowing you to clean up residual resources left behind when these tasks are not completed successfully.

VM Restore using Differential Recovery

This recovery option is only available if recovering using Copy recovery to the Original Location.

- Use when you only need to restore the differential data between the current VM state and the selected Point in Time. Any newly added data in the original VM is deleted.
- Use when you need a quick restore as compared to Copy Recovery.
- In the original VM, if there are any newly added disks or any disks that are excluded during backup, then the recovered VM will not have these newly added disks, and the disks excluded during backup.

Refer to Recover VMs to the Original Location for more information and steps to perform Differential Recovery of VMs.

VM Restore using Instant Recovery

Use this method when you need the business critical VM such as Active Directory, DNS, DHCP, NTP, etc. made operational instantly and cannot wait for the entire restore process (data copy) to complete.

- Use when the recovered VM needs immediate access with agreeable performance. The recovered VM will be spawned from the Cohesity datastore to bring the applications back into business immediately and will migrate the VMs to the primary datastore in the background.
- VMware Storage vMotion limits apply to this mode of restore and should be taken into consideration during planning.
- Multiple VMs can be brought to an operational state in less time (Instant Mass Restore\ \ Recover@Scale). An ideal use-case is a ransomware attack or Cyber Incident scenario, where you could recover the critical VMs or the virtualized infrastructure faster/quicker in a cleanroom using IMR without imposing a risk to the production environment.

Refer to Recover VMs to the Original Location for more information and steps to Recover VMs to the Original Location.

Refer to Recover VMs to a New Location for steps to Recover VMs to a New Location.

NOTE: Starting release 7.3.1, Cohesity now supports teardown of failed VM recovery and VMDK recovery tasks, allowing you to clean up residual resources left behind when these tasks are not completed successfully.

VM File/Folder Restore using File Level Recovery

Use this when you need to restore only a few files or folders from a protected VM, and when VM data is not entirely corrupted.

- This mode applies only to File Systems that Cohesity Indexing supports, such as NTFS, BtRFS, XFS, EXT 2, 3 & 4.
- These files can also be downloaded to the local system.
- File-level recovery is performed by using either the VMware tool, existing Cohesity agent or by deploying an ephemeral Cohesity agent on the target VM.
- File Level Recovery using Cohesity Agent is faster than recovering using VMware Tools.
    - Either install or pre-install a Cohesity agent which enables users who do not have elevated logins to restore VM files.
    - Or use VMware Tools installed and running on the VM to perform the file restore. You must enter the credentials required to access the target VM.
- If you recover files and folders of VMware VMs using VMware Tools, then consider the following:
    - A VMware Tools service restart during a Recovery operation may disrupt Recovery.
    - The maximum recovery speed is 1-2 MBps due to a known VMware limitation. For more details, see the VMware KB 2144004
    - Cohesity recommends that you not use VMware Tools if the size of the recovered files or folders exceeds 10 GB or 10,000 files.
    - Ensure you run VMware tools in sync with the vCenter and ESXi host versions. For compatibility of VMware Tools with guest operating systems, see the VMware KB 70728.
    - For Windows VMs:
        - ACLs cannot be restored even if you have enabled the Preserve File/Folder Attributes option. Only the VM data will be restored.
        - Recovery of reparse points (such as shared folders, mount points, or junction points) cannot be restored.
    - For Linux VMs:
        - The Preserve File/Folder Attributes option restores only basic user, group, world permissions, and timestamps. Advanced permissions and file attributes such as ACLs are not restored.
        - Permissions for guest files and folders are retained only when the user running the restore operation has permission to change the group ownership on the restored files and folders. If the user does not have change group ownership permissions, the restore operation will fail. In this case, retry the operation without enabling the Preserve File/Folder Attributes option.
        - VMware APIs do not support the creation of files in the root folder.
        - VMware APIs cannot restore symbolic links.

- Restoring files to a folder is not supported if the user account doesn't have write permission to that folder (even if the user has sudo permissions). Cohesity recommends using a root user or a user account with write privileges to the target folder.
- If you restore files and folders using a guest user account that does not have permission to change file/folder ownership, the restored files are owned by the guest user account used to perform the restore. If you restore files and folders using a guest user account that has permission to change file/folder ownership, the restored files are owned by (or the ownership is retained by) the guest user account used to create the files and folders.
- When a parent folder is restored, all its subfolders are restored also; Empty folders can be restored only when the parent folder is restored.
- Restoring hard links is supported; hard links restored with their source files use the same index node (inode).

Refer to Recover Files or Folders to the Original Location for steps to Recover Files and Folders to the Original Location.

Refer to Recover Files or Folders to a New Location for steps to Recover Files and Folders to a New Location.

VM Disk Restore

Use this when you need to restore 1 or more disks to a VM.

- Make sure that the disks are made available after the restore process is completed and is persisted.
- VMware Storage vMotion limits apply to this mode of restore and should be taken into consideration during planning.
- If one or more disks are overwritten during recovery, the target VM will automatically be powered off before the recovery and can optionally be powered ON automatically after the recovery.
- A rescan for disk discovery might be needed after restoring.

Refer to Recover Virtual Disks to the Original Location for steps to recover the virtual disk to the original location.

Refer to Recover Virtual Disks to a New Location for steps to recover the virtual disk to a new location.

NOTE: Starting release 7.3.1, Cohesity now supports teardown of failed VM recovery and VMDK recovery tasks, allowing you to clean up residual resources left behind when these tasks are not completed successfully.

VM Instant Volume Mount

Use this when you need to restore only a logical partition or volume quickly on the original or new location.

- Requires Cohesity agent and VMware tools for mount operations. Refer to section 3.2.3 for details.
- Use cases include granular recovery of Microsoft Exchange, SQL, and SharePoint data by third-party software.
- Rescan for volume discovery might be needed after the restore.

Refer to Instant Volume Mount to the Original Location for steps to perform Instant Volume Mount to the Original Location.

Refer to Instant Volume Mount to a New Location for steps to perform Instant Volume Mount to a New Location.

Best Practices - VMware VM Protection

This section outlines Cohesity VMware Data Protection best practices that guide you towards setting up a desired Data Protection to comply with your business requirements and objectives.

Cohesity's VM Protection Best Practices

- For Tier0 (mission-critical) VMs requiring immediate access on recovery, Cohesity recommends protecting such VMs in a single protection group to leverage the benefits of Instant Mass Recovery.
- If you have VMs with high transactional and high change rate applications that might experience degraded performance due to VM stun issues associated with VADP snapshots, Cohesity-suggested leverage Adapter-based backups. Alternatively, you could also consider leveraging storage snapshots if your environment supports it. Refer to VMware VM Stun for more information.
- If you are leveraging Pure or Nimble storage snapshots for VMware VM backup in a pre 7.2 release and you intent to upgrade the Cohesity Cluster to 7.2 or later, ensure the SAN connectivity between Cohesity cluster and the Storage Array is in place (Pre-Requisite for Storage Snapshot v2) before the upgrade to avoid VM backup failures.
- If you intend to leverage storage snapshots for IBM FlashSystem, ensure the SAN connectivity between Cohesity cluster and IBM FlashSystem storage array is in place. Leveraging storage snapshots with IBM FlashSystem is supported from 7.1.1 release onwards.
- Cohesity recommends using CDP protection for business-critical VMs demanding near-zero RPO to meet business objectives. CDP protection has some additional overhead on Compute and network resources. Strategize CDP protection considering the Change rate, number of disks per VM, and the Cohesity cluster sizing. CDP is also best suited for Cohesity DR use-case when configured with Cohesity replication between production and DR Cohesity Clusters.
- VMware has a set of best practices to help better utilize NBDSSL transport for backups. Refer to the VMware best practices documentation for more information. Analyze your existing VMware infrastructure implementation If you consider implementing any of the suggested VMware side configurations.
- Cohesity highly recommends adding the Backup VLAN in Cohesity Cluster Network settings if the Backup VLAN is non-routable. Refer to Backing up VMs in the Multi VLAN Environment for more information and Manage VLANs link for how-to steps.
- Cohesity recommends enabling the option "Network for data transfer" on the registered source to force Cohesity communication over a desired ESXi Host's Backup IP address in environments configured with multiple IPs. Refer to Leveraging Cohesity "Network for Data Transfer" to Allow Backup Traffic via Specific IP Address for more details. Also, refer to the VMware section (**Network for Data Transfer**) of Register or Edit a Hypervisor Source for how-to steps.

- Cohesity recommends using Auto Protect with Tag-based VM selection while protecting many VMs for ease of management. Keep in mind that the VMs should be tagged correctly in vCenter. You can use the Tags with Auto Protect option to easily select all VMs (OR Operator) or only common VMs (AND Operator) within the selected Tags. Refer to Cohesity article 000007174 for how-to steps.

  NOTE: VM Tagging at the vCenter needs to be done with good planning. Incorrect VM tags could lead to undesired protection results. A good example could be spawning a few hundred Test-Dev VMs and incorrectly tagging them with a tag associated with Cohesity Auto-Protect. Such a scenario could lead to backing up the Test-Dev VMs, which are not the desired backup candidates. This will lead to further undesired extended backup windows and increased resource usage.

- Cohesity recommends that you appropriately tag VMs in vCenter, which are not a candidate for backups, and use Tag-based Exclusion. For instance, you could spawn multiple Test-Dev VMs from a template with a Tag named “NoBackup” and configure Exclusion. Using this tag name in the protection group will exclude all the Test-Dev VMs in the protection run.

- When protecting a VM ensure you are protecting the required VM disks only. For example, you have a VM hosting a database service like SQL and the database is protected using Cohesity database adapter. In this case when you protect this VM at a VM Level, ensure you are only protecting the VM OS disk and exclude the VM disks hosting the database data and logs. You can Include or Exclude disk by leveraging option **“Enable Disk Inclusion/Exclusion”** and defining Include (Protect only these disks) or Exclude (Exclude these disks from protection) settings in the Protection Group’s Additional Settings. Refer to Add or Edit a Protection Group for Virtual Servers for more details.

- With custom protection policies, the DataLock option is enabled by default (configurable), and Cohesity highly recommends keeping it that way. It is Cohesity’s WORM (write once read many) feature which guarantees that your backups and archives cannot be tampered with or deleted. DataLock is enabled by default on the existing system protection policies (Bronze, Silver, and Gold) and cannot be modified.

- Cohesity provides flexibility to adjust the protection priorities dynamically or enforce limits to help prioritize production processes. The following are the recommended parameters that you might want to consider enabling based on your existing infrastructure deployment and workload assignments. Refer to the section "vCenter or Standalone ESXi Host" in Register or Edit a Hypervisor Source for how-to steps and for more information.

  - **Latency Based Adaptive Throttling**—adaptively throttle the running of tasks created by the Protection Groups protecting this source. This throttling helps to ensure that the datastores on the source (vCenter Server) are not adversely affected by the Protection Groups.

    NOTE: Cohesity cluster enables the collection of Storage IO Control (SIOC) statistics on the datastores if not already enabled. The Cohesity cluster uses the statistics from SIOC to calculate the observed latency of datastores. If throttling and the collection of SIOC statistics were initially enabled and then throttling is disabled, the Cohesity cluster does not change the SIOC collection statistic settings on the datastores. This will be an environment-wide change with no fine-grained control.

  - **Cap concurrent streams per datastore**—This setting limits the number of streams concurrently backed up per datastore. This helps to reduce any performance impact on the datastore. You can configure it to override required datastores as desired.

- **Cap concurrent VM Backups**—This setting limits the number of VMs that can be backed up concurrently in a vCenter.
- **Auto Cancel Backups if Datastore is running low on space**—Toggle this setting on if you want to set the minimum required free space for the datastore. Once set, Cohesity automatically prevents new backups from starting and also cancels currently running jobs if the datastore does not meet this requirement. Cohesity recommended using the % option instead of GiB values for the free space threshold.

NOTE: The percentage option is more flexible because it auto-adjusts when the datastore shrinks or expands, even if a VM has multiple datastores. This means, if two virtual disks of a VM reside in datastores of size 500 GB and 1 TB each, 10% of free space will apply to both the datastores.

NOTE: Enabling throttling can increase how much time a Protection Group run takes to complete, resulting in SLA violations. You may want to increase the SLA for the Protection Group as needed.

- Define a Quiet Time in the protection policy to prevent starting a protection run during any defined time period in a week based on your business needs. For example, you may want to configure hourly backups that run during weekdays but not on weekends.
- VMware VM migration between vCenter is no longer a break in the VM backup chain. Starting with Cohesity DataPlatform 7.0.1, Cohesity allows registering the source and destination vCenters in the Cohesity cluster and enabling (Toggle option) "Detect VM migration across vCenter to Preserve backup chain". This will preserve the previous backups and users can choose to continue protecting (incremental) the migrated VM via new vCenter source by creating a new protection group.

NOTE: Cohesity will display "vCenter Migrated" against the VM in the "Add Object" page of the Protection Group creation workflow.

- When using Jumbo Frames, make sure that every network hop between client hosts, such as any cluster nodes, hypervisor hosts, and the Cohesity cluster has the MTU set to the same value (MTU - 9000). Refer to Set MTU link for steps.
- Creating snapshots of VMs that have physical compatibility RDM disk is not supported by VMware and hence not supported by the Cohesity cluster. Cohesity recommends excluding such disks by selecting the option "Exclude Physical Compatibility RDM Disk" in the protection group. If you must backup the physical compatibility RDM data, consider using agent-based backups. Refer to VMware Snapshot Limitations for more details.

NOTE:

- Cohesity allows excluding disks from the protection run. This feature enables users to exclude unwanted disks (For example: disks dedicated to storing Temp files, Physical Mode RDM, etc.) from protection. This can be defined Implicitly at the VM level (while selecting the source objects to backup) or Explicitly at the Protection Group level. Refer to step 4 of Add or Edit a Protection Group for Virtual Servers.
- Starting release 7.3, Cohesity now supports disk inclusion to protect specific disks in a protection run. This can be defined Implicitly at the VM level (while selecting the source objects to backup) or Explicitly at the Protection Group level. Refer to steps 4 of Add or Edit a Protection Group for Virtual Servers.
- Starting release 7.2.1, Cohesity automatically backs up the VM's DataSets file during VM protection and also provide the ability to recover the DataSets file, enhancing data protection and recovery options.

Cohesity's CDP for VM Best Practices

- Cohesity CDP is very sensitive to Time Synchronization with the source. Cohesity recommends the following for accurate restore point selection. A mismatched time could lead to an incorrect time stamp association with the recovery point in time selection.
  - The Time Zone settings configured in the VM Guest OS and on the ESXi hosts should match.
  - The time between the VM Guest OS and the ESXi hosts should be in sync.
  - The time between the ESXi hosts and the Cohesity cluster should be in sync.
- When configuring CDP protection in an environment with multiple Cohesity clusters, Cohesity recommends protecting VMs from a single vCenter Cluster with one Cohesity cluster only. Cohesity does not support multiple Cohesity clusters managing a single vCenter compute cluster for CDP.

Cohesity's VM Recovery Best Practices

- When attempting a File-Level Recovery, make sure the target VM is not undergoing a Storage vMotion operation. Recovering files to a VM where vMotion is in process is not supported.
- Cohesity recommends using a dedicated VMKernel adapter on each ESXi host for Backup and Restore Traffic. This helps in achieving predictable recovery performance.
- For very active MS SQL and Oracle Database servers running on VMs, Cohesity recommends using adapter-based backup. Database recovery with an adapter-based approach is a much faster process.
- Use Copy Recovery to recover VMs hosting business applications with tolerant RTO and for VMs (such as database servers) that require predictable performance upon access.
- Use Instant Recovery (Instant Mass Recovery) to recover VMs hosting business-critical applications and for VMs on which recovery of other applications depends such as Active Directory, DNS, DHCP, NTP, etc.

- Use Instant Recovery (Instant Mass Recovery) to Recover@Scale during a ransomware attack or cyber incident scenario, where you could recover the critical VMs or the virtualized infrastructure faster/quicker in a sandbox environment without imposing a risk to the production environment.
- While performing recovery in a DR scenario, disable all non-critical services in the Cohesity cluster to achieve optimal recovery throughput. Non-critical services include Backups (incoming), Replication (incoming and outgoing), Archival (outgoing), Indexing, Space Reclamation, and Cluster Housekeeping Services.
- The vSphere ESXi default configuration allows for only 32 NFS mounts per ESXi host starting VMware vSphere 7.x and higher. This is a VMware limitation. Cohesity recommends increasing the maximum number of NFS mounts on an ESXi host from 32 to 256 (as applicable) should the recovery jobs fail due to this limitation. Refer to VMware KB for steps and Full Recovery Workflow (Instant Recovery and Copy Recovery) for more details on workflow.
- If you have VM disk(s) excluded during backup and you need to maintain the VM disk configuration post recovery, leverage recovery option **"Exclude Disk Handling — Create Excluded Disk as an Empty Disk"**. Cohesity will create blank disks for every excluded disk saving you from the effort of creating new disks post recovery. This feature is especially helpful if you have many VMs with excluded disks. Please note that this feature is only supported with Instant Recovery and Copy Recovery. Not supported with Differential Copy Recovery.

Appendix

VMware VM Stun

A “stun” operation means pausing the execution of the VM at an instruction boundary and allowing in-flight disk I/Os to complete. Usually, anything that involves complex disk changes while the VM is running will require stunning the VM. This is because VMware usually needs to close the virtual disks (VMDK), and that can only be done if we first quiesce I/Os.

VMware stuns (quiesces) the virtual machine (VM) when a VM snapshot is created and deleted/consolidated. The stun time depends on the number of disks (vmdk), IO change rate to the vmdk, and the data delta between the base and delta disk. During backup, VMs with a high change rate running for a longer duration will experience performance impact due to increased VM Stun time.

Backing up VMs in the Multi VLAN Environment

In Production environments, it is common to have VMware Networks configured with multiple VLANs each dedicated for specific traffic such as Mgmt, iSCSI storage, VM Backup, VM, etc. Some of these VLANs such as the Storage and Backup VLANs may be configured as non-routable VLANs at the network layer. Add the Backup VLANs to the Cohesity cluster Network settings without which the backup/restore could fail due to connection issues. Adding the VLAN in the Cohesity cluster Networking ensures that the Cohesity cluster has a network route available to ESXi Hosts and makes sure the backup/restore happens over the defined Backup VLAN.

Leveraging Cohesity “Network for Data Transfer” to Allow Backup Traffic via Specific IP Address

Some production environments can have their ESXi servers with multiple NICs installed, and each NIC could be physically connected to 1G and 10G Networks. In a typical scenario, the 1G network connection could be for vSphere Management and the 10G for VM data. Hence, each ESXi host would have multiple IP addresses configured across 1G and 10G connected networks without logical separation of backup traffic. When the Protection run starts, Cohesity queries the vCenter and acquires the ESXi hostname as FQDN. When Cohesity tries to communicate with the ESXi host with the acquired FQDN, the DNS server may resolve the Management IP residing on the 1G network and all backup traffic could flow via the management path.

This is undesirable as it will impact performance. To overcome this issue, Cohesity recommends enabling the option “Network for data transfer” for the registered source vCenter and defining the backup subnet IP and CIDR prefix. This will create the respective Host Mapping in Cohesity networking for every ESXi host in the specified subnet. For the ESXi host with multiple VMkernel adapters, the Cohesity cluster will use the IP address that belongs to the specified subnet for the backup and recovery of VMs on the ESXi host.

VMware vCenter Sessions and its Management

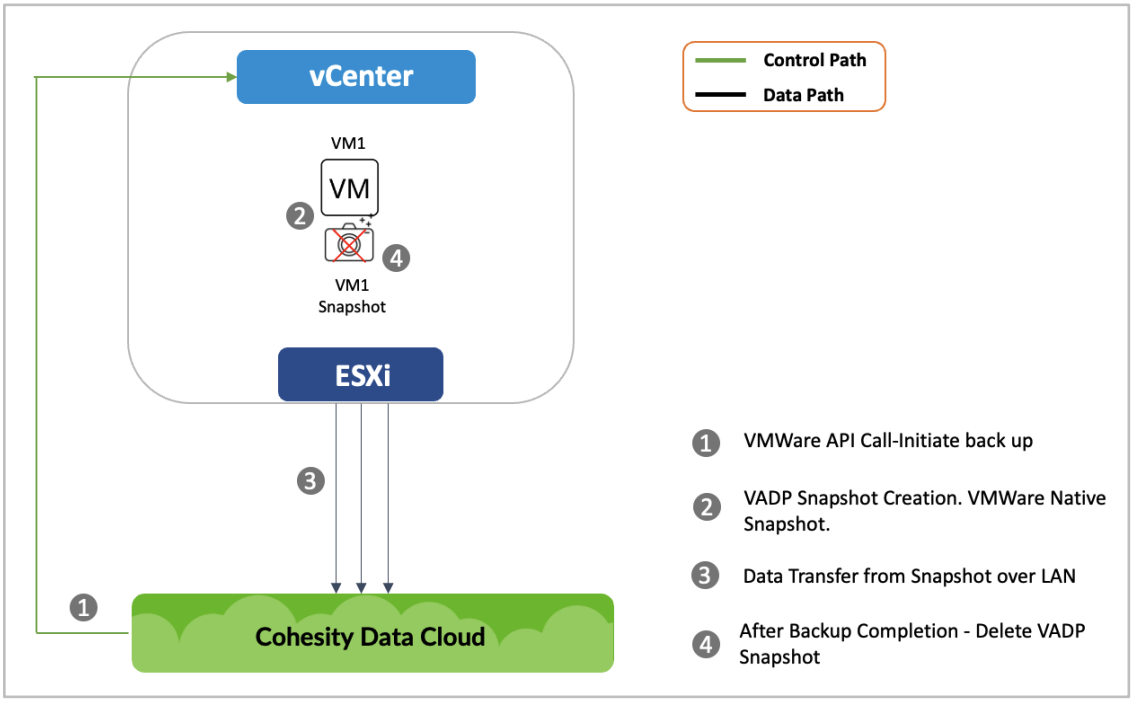
When connecting to a vCenter server using a web client, a session is created and used all the time for vCenter management. Similarly, for backup activity, when a vCenter is registered with the Cohesity cluster, communication between the Cohesity cluster and the vCenter server is established by creating a session. However, this session is either created by using vCenter APIs (SOAP and Rest API) or VDDK APIs depending on the Backup activity. From a Backup perspective, Cohesity creates sessions for activities such as registered vCenter inventory update queries (periodic), capture source performance matrices (periodic), and backup processes (control and data). Cohesity has the intelligence to efficiently manage the vCenter sessions through reusing sessions between backup tasks, consuming prefetched VM information, eliminating idle and duplicate sessions, etc.

Full Recovery Workflow (Instant Recovery and Copy Recovery)

During Full VM recovery using Instant Recovery, the Cohesity view of the selected PiT is mounted on the ESXi hosts as NFS datastores, and the VM recovery data is migrated from the Cohesity datastore to the VM's primary datastore. By default, VMware limits the maximum number of NFS mounts to 8 (up to vSphere 6.7) or to 32 (vSphere 7.x and higher). Should this limit cause restore failures, follow VMware KB to increase the limit to 256 NFS mounts.

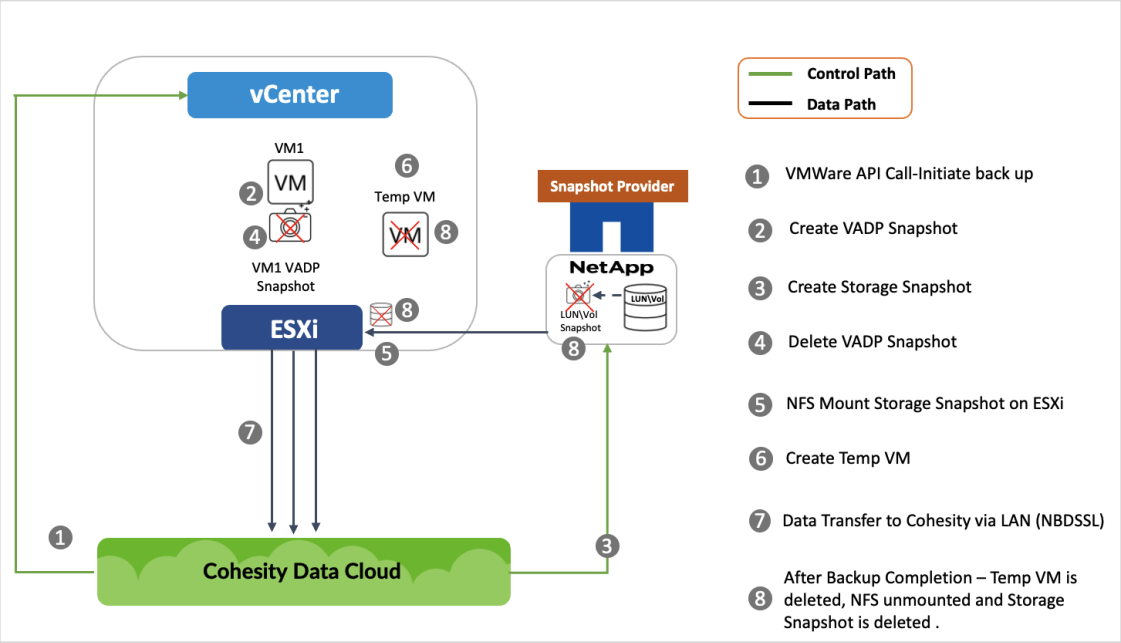
Cohesity VM Backup Workflow - NBDSSL

Figure 4: VM Backup Workflow – NBDSSL



Cohesity VM Backup Workflow - NBDSSL & Storage Snapshot v1 (NetApp only)

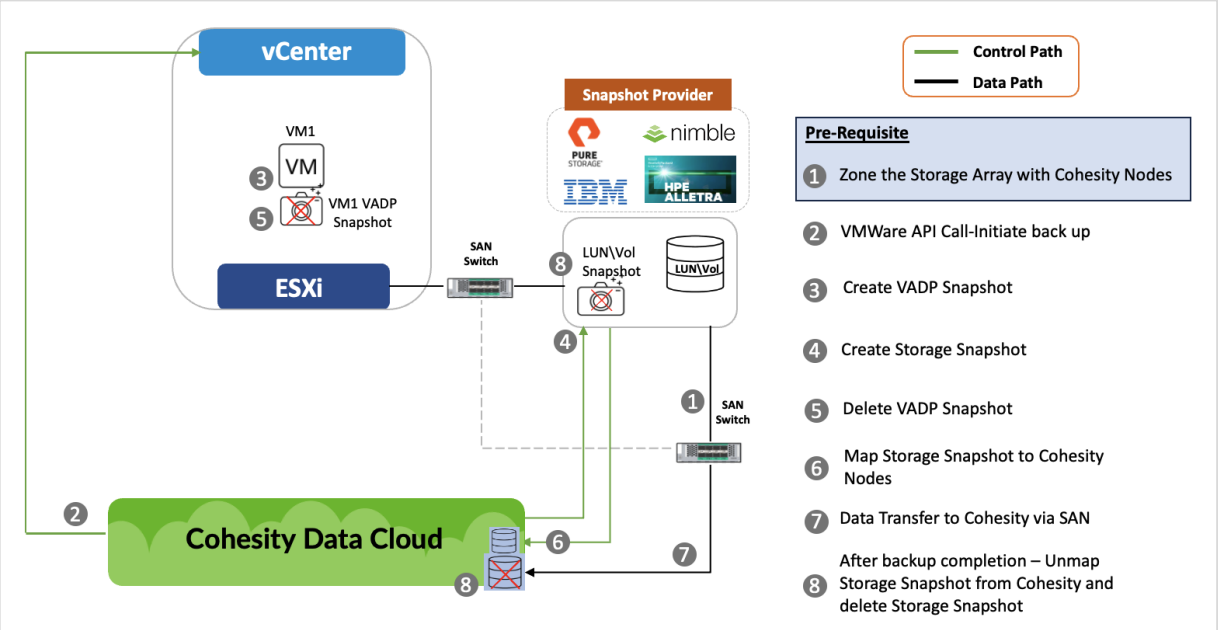
Figure 5: VM Backup Workflow - NBDSSL & Storage Snapshot v1 (NetApp Only)



NOTE: A Temp VM is created in vSphere vCenter after the VMware VADP snapshot is deleted, using the corresponding Storage Snapshot. This is used to invoke VDDK APIs during data transfer and is deleted as soon as the protection process completes.

Cohesity VM Backup Workflow – iSCSI or FC & Storage Snapshot v2 (Pure, Nimble, Alletra and IBM)

Figure 6: VM Backup Workflow – iSCSI or FC & Storage Snapshot v2 (Pure, Nimble, Alletra and IBM)



How to configure VM backup leveraging Cohesity Storage Snapshots for Data Protection

Pre-Requisites

- Ensure the Storage Array is Cohesity qualified Storage Snapshot provider.

  Cohesity provides in-built support for the following qualified third-party storage arrays (Snapshot Providers) to leveraging Storage Array-based snapshots for VMware VM backups.

Vendor	Protocol	DataStore Type	Storage Snapshot	SAN Transport Mode
Pure Storage array	ISCSI, FC	VMFS	Yes	Yes
Nimble Storage/ HPE Alletra 5000/ HPE Alletra 6000	ISCSI, FC	VMFS	Yes	Yes

Vendor	Protocol	DataStore Type	Storage Snapshot	SAN Transport Mode
IBM FlashSystem	ISCSI, FC	VMFS	Yes	Yes
NetApp	NFS	NFS	Yes	No

- SAN protocols
  - iSCSI
  - FC
- SAN Connectivity - Storage Snapshot v2 leverages SAN transport in the backend. Hence, make sure the SAN connectivity between the Cohesity Cluster and the Snapshot Provider is in place. This responsibility lies with the Customer's SAN Admin.
- Manage Firewall ports - Ensure the TCP ports requirements for each storage array are met. Refer to Manage Firewall ports section of the product documentation for details.
- User Permissions
  - For Storage Snapshot provider user permissions (for registration) refer to Register a Storage Snapshot Provider
  - VMware user permissions to leverage storage snapshots refer to Adequate Privileges for Cohesity on the Source section of product documentation
- In case of iscsi SAN, Ensure Cohesity cluster can perform iscsi discovery on Storage array

  SSH to Cohesity cluster and execute the following command:

  iscsiadm -m discovery -t sendtargets -p <ipaddress>

iSCSI SAN - Steps to Protect VMware VM Leveraging Storage Snapshots

1. Ensure Cohesity cluster can perform iscsi discovery on Storage array.

   SSH to Cohesity cluster and execute the following command:

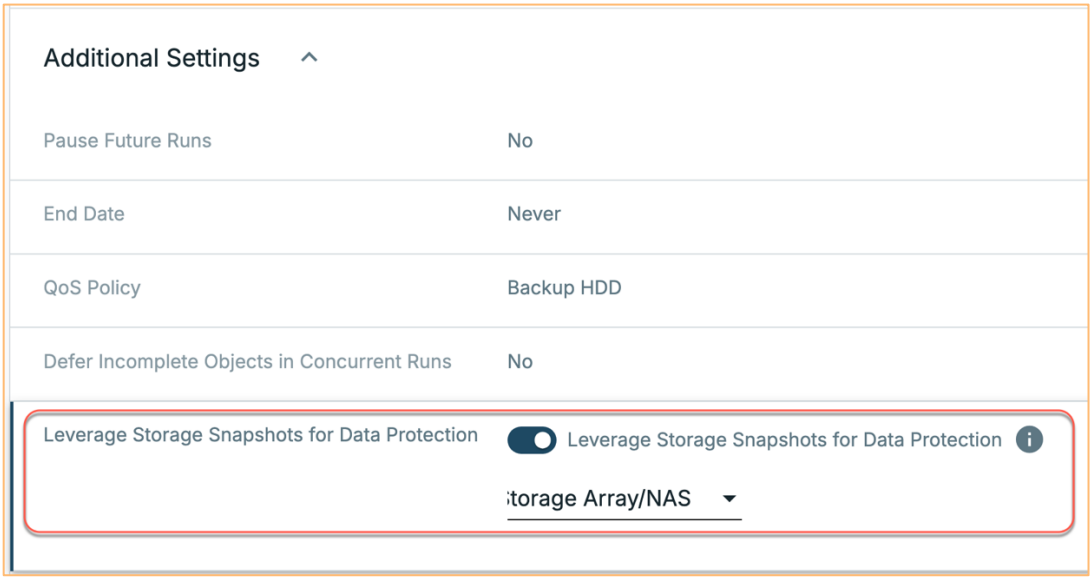
   iscsiadm -m discovery -t sendtargets -p <ipaddress>

   Example:

```
[support@sapsol-bqkp51040023-node-2 ~]$ sudo iscsiadm -m discovery -t sendtargets -p 10.15.0.60
10.15.0.60:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
10.15.0.62:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
10.15.0.63:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
10.15.0.61:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
[support@sapsol-bqkp51040023-node-2 ~]$
```

2. Register the Storage Array as a Snapshot Provider in Cohesity UI. Refer to Register a Storage Snapshot Provider section of the product documentation for more details.

3. Create a Protection Group to protect the VMware VM. Refer to Add or Edit a Protection Group for Virtual Servers section of the product documentation for more details.
4. Ensure to enable option "**Leverage Storage Snapshots for Data Protection**" in the Protection Group's Additional Setting.

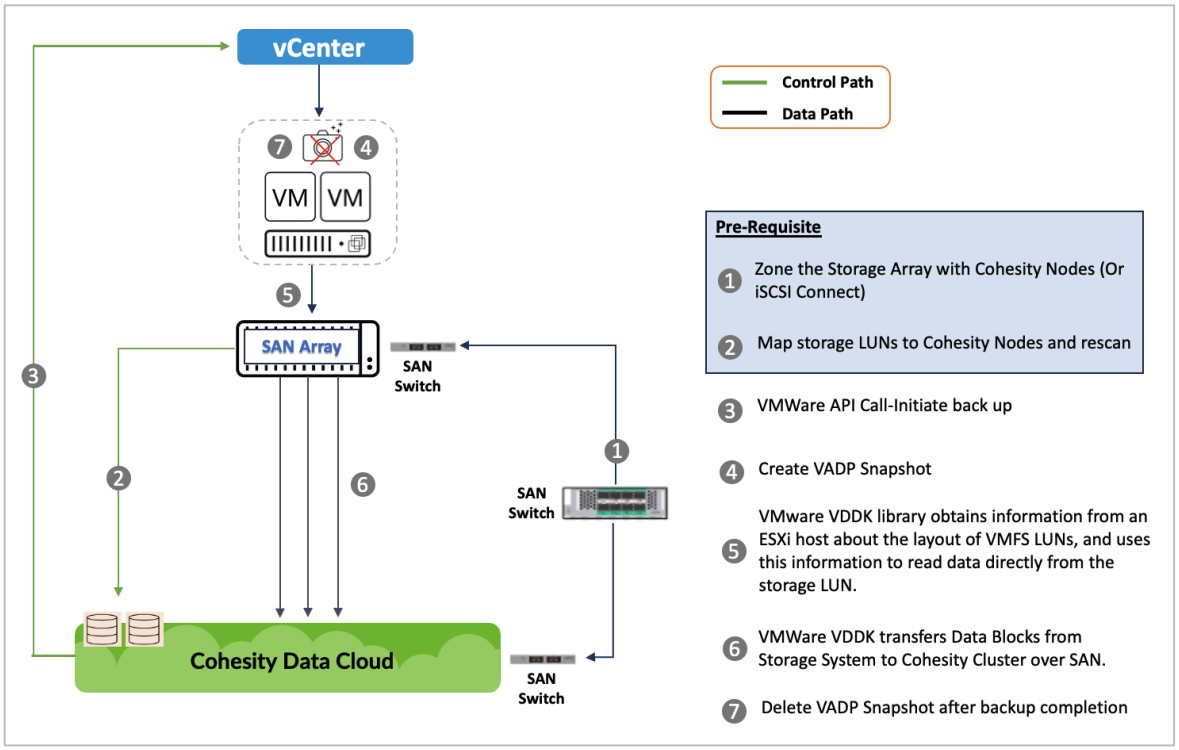


FC SAN - Steps to Protect VMware VM Leveraging Storage Snapshots

1. Ensure the FC SAN connectivity between the Cohesity Cluster and the Snapshot Provider is in place. This responsible lies with the SAN Storage Administrator.
2. Register the Storage Array as a Snapshot Provider in Cohesity UI. Refer to Register a Storage Snapshot Provider section of the product documentation for more details.
3. Create a Protection Group to protect the VMware VM. Refer to Add or Edit a Protection Group for Virtual Servers section of the product documentation for more details.
4. Ensure to enable option "**Leverage Storage Snapshots for Data Protection**" in the Protection Group's Additional Setting.

Cohesity VM Backup Workflow - SAN Transport (FC / iSCSI)

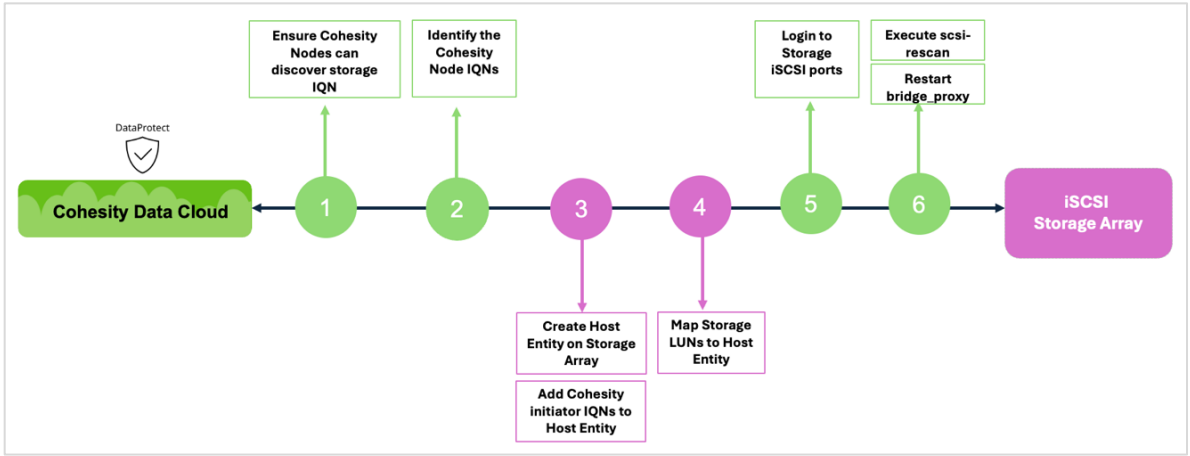
Figure 7: VM Backup Workflow - SAN Transport (FC)



How to configure VM backup leveraging SAN Transport for Data Protection

iSCSI SAN Configuration Steps

Figure 8: General iSCSI SAN Connectivity Steps



SAN transport is storage agnostic and any SAN array with FC or iSCSI capabilities can be configured with Cohesity. The following iscsi SAN configuration example is indicative and must only be used for a general understanding of the requirements. Cohesity expects the SAN Storage Administrator to configure the iSCSI SAN environment as per their respective storage vendor requirements.

1. Ensure Cohesity Nodes can discover storage IQN (Pure Storage)
   - SSH to Cohesity cluster and execute the following command

     `iscsiadm -m discovery -t sendtargets -p <ipaddress>`

     Example:

```
[support@sapsol-bqkp51040023-node-2 ~]$ sudo iscsiadm -m discovery -t sendtargets -p 10.[redacted].60
10.[redacted].60:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
10.[redacted].62:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
10.[redacted].63:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
10.[redacted].61:3260,3302 iqn.2010-06.com.purestorage:flasharray.1f51348bd737b9ca
[support@sapsol-bqkp51040023-node-2 ~]$
```

2. Identify the Cohesity Node IQNs
   - SSH to Cohesity Cluster
   - Disable Secure Shell Access
   - Execute command: `allssh.sh 'cat /etc/iscsi/initiatorname.iscsi'`

     Example:

```
[support@sapsol-bqkp51040023-node-2 ~]$ allssh.sh 'cat /etc/iscsi/initiatorname.iscsi'
=========== 10.[redacted].36 ===========
InitiatorName=iqn.2016-09.com.cohesity:[redacted]
=========== 10.[redacted].38 ===========
InitiatorName=iqn.2016-09.com.cohesity:[redacted]
=========== 10.[redacted].39 ===========
InitiatorName=iqn.2016-09.com.cohesity:[redacted]
=========== 10[redacted].1.37 ===========
InitiatorName=iqn.2016-09.com.cohesity:[redacted]
[support@sapsol-bqkp51040023-node-2 ~]$
```

3. Create Host Entity on Storage Array and Add Cohesity initiator IQNs to Host Entity

   Example: Create Host Entity on Storage Array

```
pureuser@SAC01-PM-PURE02> purehost create cohesity-[redacted]080
Name                          WWN  IQN  NQN
cohesity-[redacted]080        -    -    -
pureuser@[redacted]-PM-PURE02>
```

   Example: Add Cohesity initiator IQNs to Host Entity

```
pureuser@[redacted]-PM-PURE02>
pureuser@[redacted]-PM-PURE02> purehost setattr cohesity-[redacted]080 --addiqnlist iqn.2016-09.com.cohesity:1[redacted]080-181140264658176
,iqn.2016-09.com.cohesity:[redacted]080-1811402
63745228,iqn.2016-09.com.cohesity:[redacted]080-181140263442702
Name                      WWN  IQN                                                    NQN  Host Group
cohesity-[redacted]080    -    iqn.2016-09.com.cohesity:[redacted]8080-181140263442702  -    -
                               iqn.2016-09.com.cohesity:[redacted]8080-181140263745228
                               iqn.2016-09.com.cohesity:[redacted]8080-181140264658176
pureuser@[redacted]-PM-PURE02>
pureuser@[redacted]-PM-PURE02>
```

4. Map Storage LUNs to Host Entity.

   Map the Storage Volumes (where the VM resides) to Cohesity Host Entity.

```
pureuser(      1-PM-PURE02> purehost connect cohesity-                  3080 --vol pure02-      t-vc01-datastore1
Name                        Vol                                  LUN
cohesity-                  080  pure02-      -vc01-datastore1  1
pureuser(      PM-PURE02>
pureuser(      PM-PURE02>
```

   NOTE:

   - You must map a volume to Cohesity, else the next step – Login to Storage iSCSI ports IQN will fail.
   - You must manually map all storage volumes associated with the VMs you intend to protect.

5. Login to Storage iSCSI ports (Pure Storage iscsi IQN).

   - SSH to Cohesity Cluster
   - Disable Secure Shell Access
   - Execute command: iscsiadm -m node –targetname <target iqn> -p <target IP address> -–login

```
[support@sapsol-bqkp51040023-node-2 ~]$ sudo iscsiadm -m node -T iqn.2010-06.com.purestorage:flasharray.                ca -p 10.    .60 --lo
gin
Logging in to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                9ca, portal: 10.    .60,3260]
Login to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                9ca, portal: 10.    .60,3260] successful.
[support@sapsol-bqkp51040023-node-2 ~]$ sudo iscsiadm -m node -T iqn.2010-06.com.purestorage:flasharray.                9ca -p 10.    .61 --lo
gin
Logging in to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                b9ca, portal: 10.    .61,3260]
Login to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                9ca, portal: 10.    61,3260] successful.
[support@sapsol-bqkp51040023-node-2 ~]$ sudo iscsiadm -m node -T iqn.2010-06.com.purestorage:flasharray.                9ca -p 10.    .62 --lo
gin
Logging in to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                b9ca, portal: 10.    62,3260]
Login to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                9ca, portal: 10.    .62,3260] successful.
[support@sapsol-bqkp51040023-node-2 ~]$ sudo iscsiadm -m node -T iqn.2010-06.com.purestorage:flasharray.                9ca -p 10.    .63 --lo
gin
Logging in to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                9ca, portal: 10.    .63,3260]
Login to [iface: default, target: iqn.2010-06.com.purestorage:flasharray.                9ca, portal: 10.    .63,3260] successful.
```

   NOTE: After every node\cluster reboot, you need to manually login into the storage iscsi ports.

6. Execute scsi-rescan and Restart bridge_proxy.

   You may SSH to Cohesity and manually execute `scsi-rescan` and `restart bridge_proxy`

   - `allssh.sh "/usr/bin/scsi-rescan -r -a -i"`
   - `allssh.sh "bridge_proxy.sh stop"`
   - `allssh.sh "bridge_proxy.sh start"`

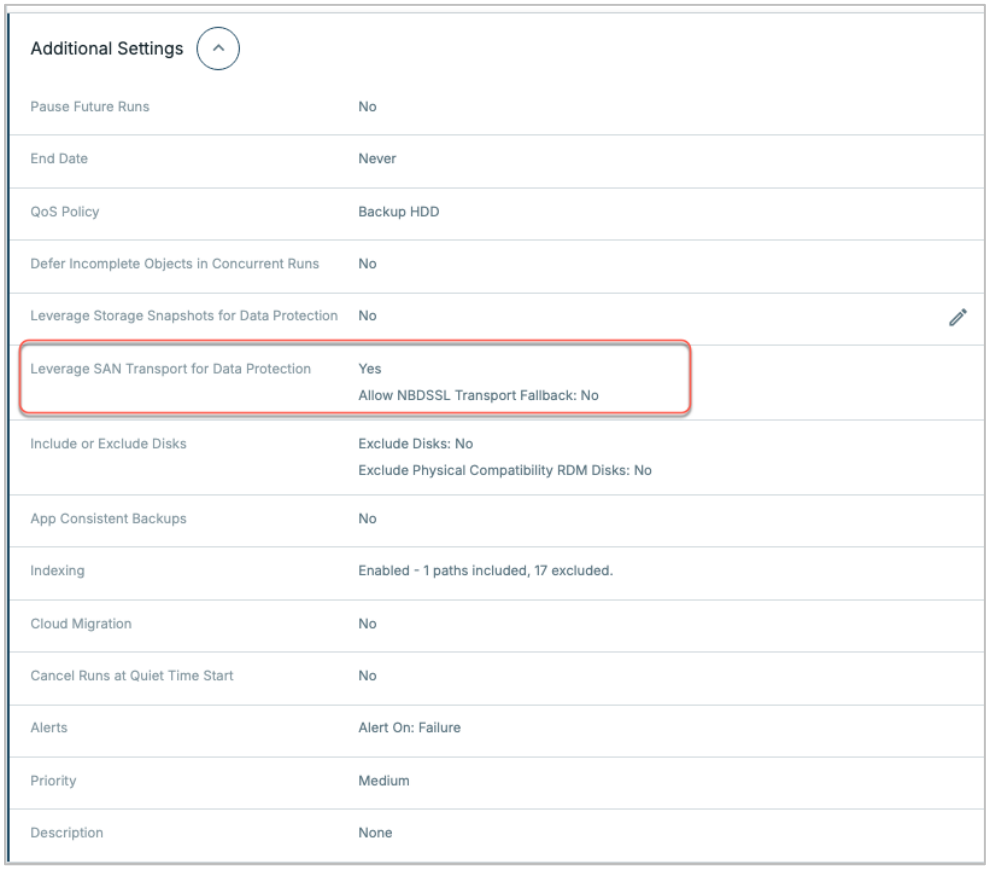
   For a scripted approach, please engage with Cohesity Support.

   NOTE: You must restart the bridge_proxy service when,

   - You add VMs to protection that reside on new LUNs.
   - You add new nodes to existing Cohesity Cluster.

iSCSI SAN – Protect VM Leveraging SAN Transport Mode

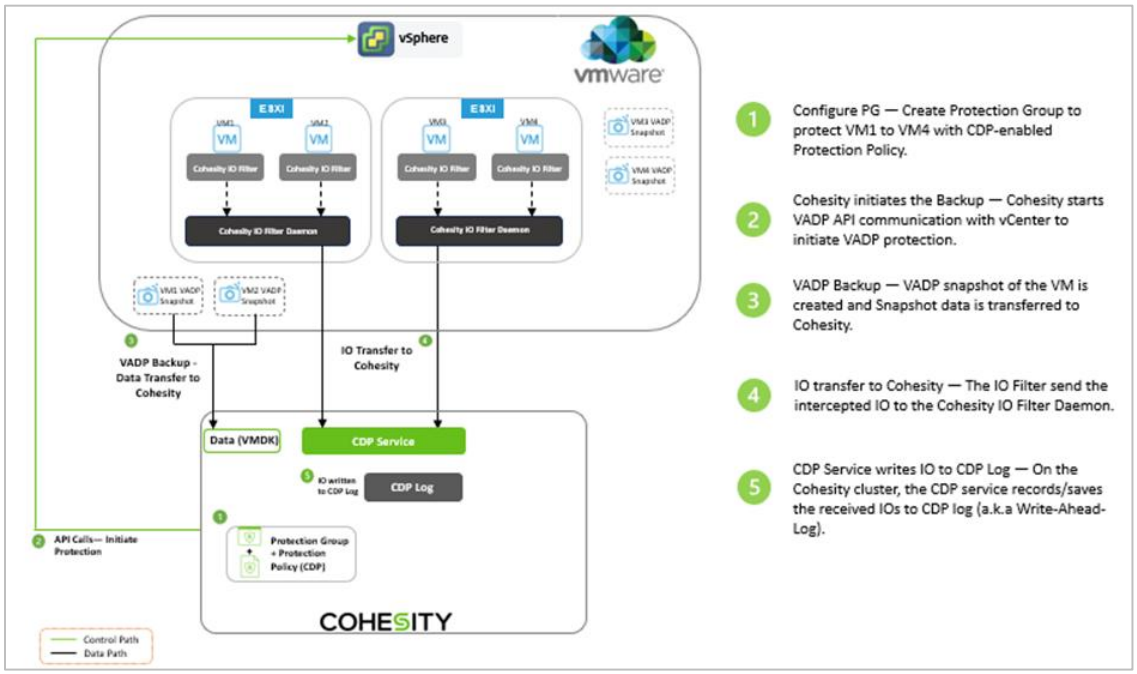
1. Create a Protection Group to protect the VMware VM. Refer to Add or Edit a Protection Group for Virtual Servers section of the product documentation for more details.
2. Ensure to enable option "**Leverage SAN Transport for Data Protection"** in the Protection Group's Additional Setting.



3. Set "Allow NBDSSL Transport Fallback" to Yes, if you wish to continue backup via NDBSSL if the SAN transport is unavailable for any reason. Or set it to NO if you want to enforce strict SAN transport mode for backing up VMware VMs, this setting will fail the backup if SAN transport is unavailable for any reason.

Cohesity Continuous Data Protection (CDP)

Figure 9: Cohesity Continuous Data Protection



Cross VM recovery—VMware On-Prem to Azure VMware Solution (AVS)

Supported Configuration

Figure 10: Cross VM Recovery – On-Prem to AVS using CloudArchive

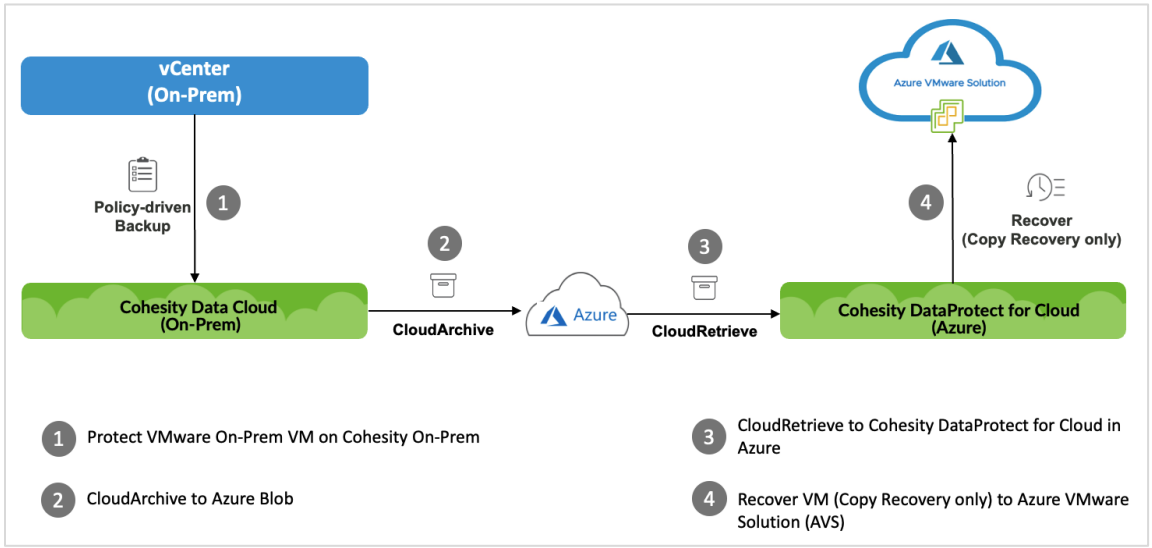


Figure 11: Cross VM Recovery – On-Prem to AVS using Cohesity Replication

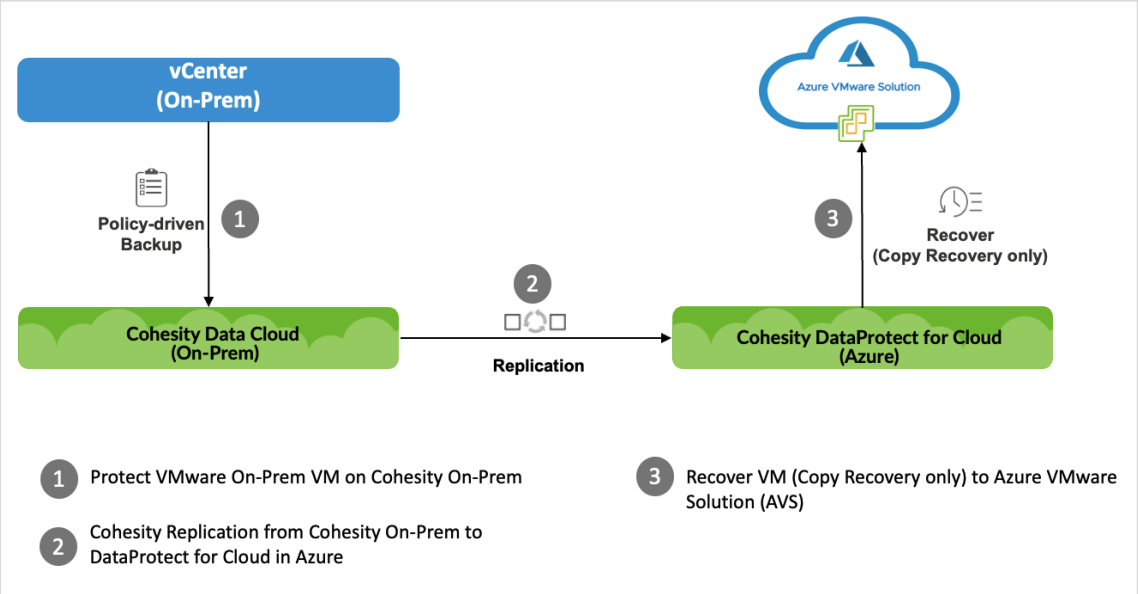
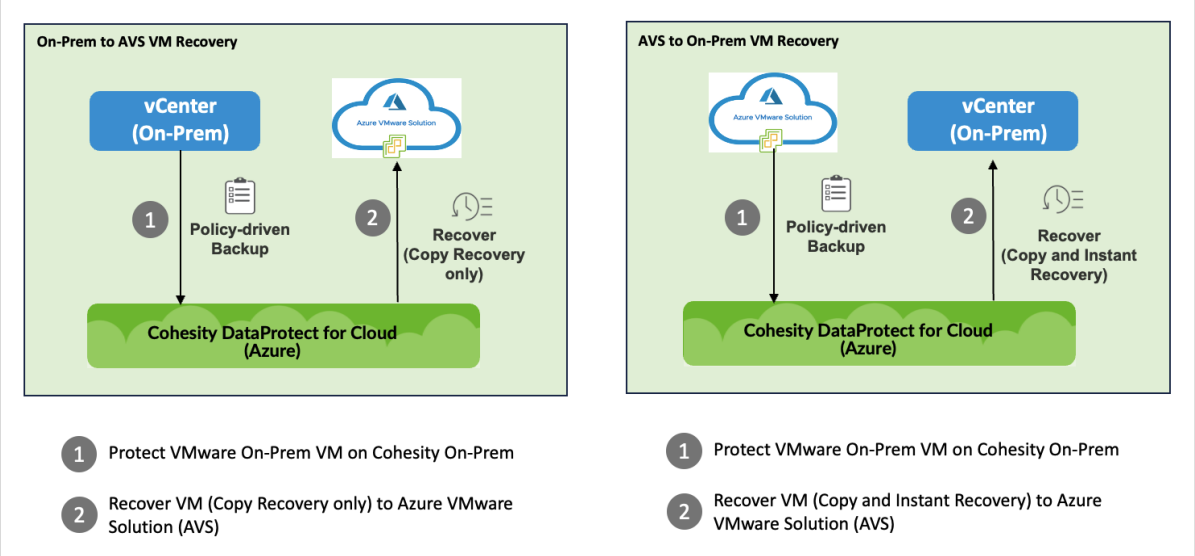


Figure 12: Cross VM Recovery – AVS to On-Prem using Cohesity DataProtect for Cloud in Azure



Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sadik Sayed is a Senior Solutions Architect at Cohesity. In his role, he focused on Virtualization Data Protection — VMware vSphere, VMware Cloud Director, VMware Cloud Foundation, Microsoft HyperV and Nutanix AHV.

Other essential contributors include:

- Karthick Radhakrishnan, Director, Solution Architecture
- Nanda Kishore, Senior Manager, Technical Account Management
- Anand Arun, Technical Director, Engineering
- Gautam Bhasin, Director, Product Management
- Mary Juliya, Technical Editor

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.4	Mar 2026	Steps to configure SAN connectivity
1.3	Feb 2026	• Cross environment VM recovery (On-Prem to AVS) • Storage Snapshot v2 updates
1.2	Nov 2025	Release 7.3 updates
1.1	Mar 2024	Editorial changes
1.0	Aug 2023	First release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 42 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.