COHESITY

Version 1.0

December 2024

Hyper-V Data Protection Best Practices with Cohesity

ABSTRACT

An overview of Microsoft Hyper-V data protection, recovery workflows, the best practices, and related recommendations.

Table of Contents

Figures

Microsoft Hyper-V Data Protection with Cohesity

Cohesity Data Cloud is secure and manages your entire data estate on 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 Microsoft Hyper-V Data Protection. 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 to replace tuning resources based on specific user environments or technical documentation published on https://docs.cohesity.com/HomePage/Content/home.htm.

Hyper-V Data Protection Methodologies

Let's look at the Cohesity supported Hyper-V deployments, the architectural flow of Hyper-V data protection, and the protection methods that Cohesity offers.

Cohesity Differentiators for Hyper-V 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 enabling faster backups.
4. Recover at scale—With Cohesity's instant mass restore, users can quickly recover multiple VMs and virtual infrastructure during a DR event. Additionally, this feature allows mass VM recovery in a sandbox environment or a clean room during ransomware or cyber incident recovery scenarios.
5. 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.
6. 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.

Cohesity Supported Hyper-V Deployment Types

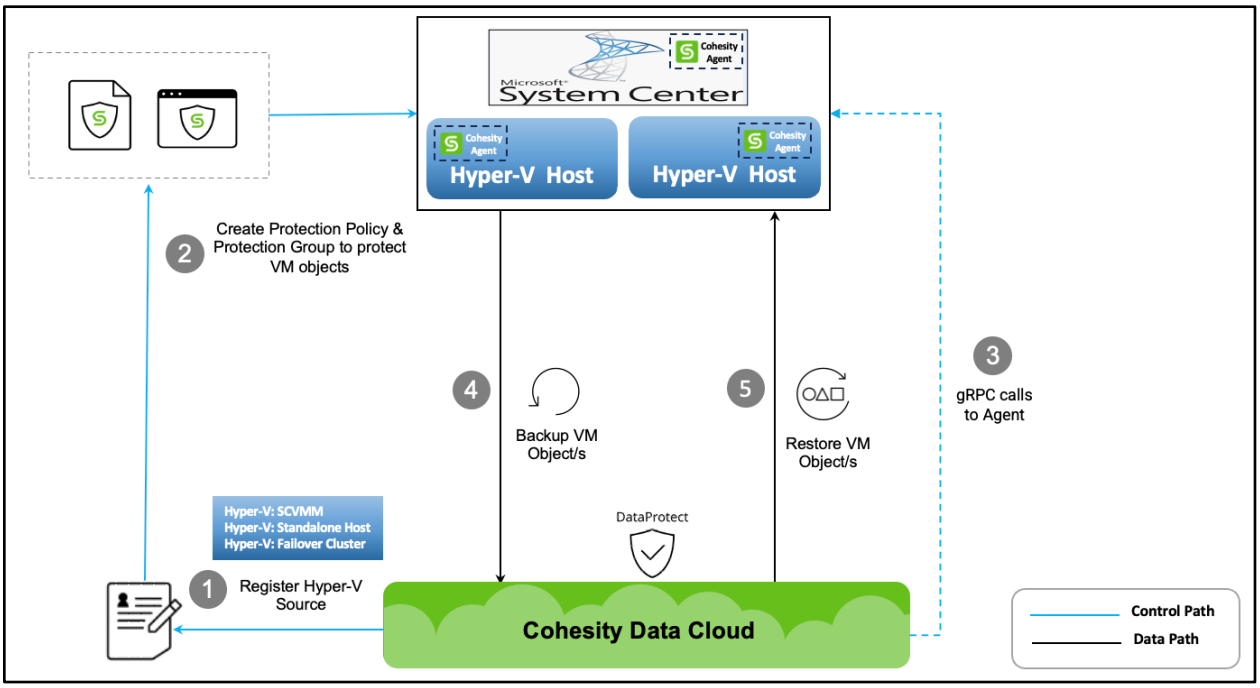
Cohesity supports the protection of the following Hyper-V deployment types.

1. Hyper-V SCVMM— System Center Virtual Machine Management (SCVMM) is a tool for managing and configuring virtualized data centers built on Microsoft Hyper-V. It is used to configure all data center components needed to run a virtual environment, such as virtualization servers, storage resources, and networking components, as well as provision hosts and VMs
2. Hyper-V Standalone Host—A Windows Server deployment with Microsoft Hyper-V role installed. It provides a simple and reliable virtualization solution to help you improve your server utilization and reduce costs in small environments.
3. Hyper-V Failover Cluster—Windows Failover Clustering is a tool to achieve VM and Application high availability avoiding a single point of failure. Hyper-V virtualization environment is managed using the Failover Cluster Manager tool in a Hyper-V Failover Cluster configuration.

Cohesity Architecture for Hyper-V Data Protection

Cohesity Data Cloud integrates with Hyper-V and leverages the available Hyper-V APIs, eliminating the need to install in-guest agents across the VMs for backups.

Figure 1: Cohesity Architecture for VMware Data Protection



Prerequisites

1. Cohesity Agent must be installed on all the Hyper-V hosts and the SCVMM before registering the Hyper-V source.
2. If the environment has a proxy endpoint connected to an SCVMM server, the Cohesity Agent must be installed on a proxy endpoint before registration.
3. The Cohesity agent version installed on the Hyper-V must not be higher than the Cohesity cluster version. For more information, see Agent Compatibility Within a Cluster.
4. The Hyper-V 2012R2 server edition does not have a native CBT available. Hence, the Cohesity Agent should be installed with the Add-on Component **File System CBT** required for efficient incremental backups.
5. Hyper-V 2016 (server and core edition) and later has RCT available. Hence the Cohesity Agent should be installed without Add-on Components (CBT). Refer to Product Documentation for steps to install the Cohesity agent.
6. Ensure the required Hyper-V privileges for Cohesity are met. Refer to Product Documentation for more information.
   a. Hyper-V SCVMM—You can register the Hyper-V SCVMM as a source in Cohesity.

- You must provide a Domain user with Administrative privileges during the source register.
- You must install the Cohesity Agent on the SCVMM and each Hyper-V host that is managed under the SCVMM.

NOTE: Refer to Ensure Adequate Privileges for Cohesity - Microsoft Hyper-V for more information.

b. Hyper-V Standalone Host—Cohesity Agent installed with Local System account privileges.
c. Hyper-V Failover Cluster—The Failover Cluster needs to have read permissions to all the Hyper-V cluster nodes (hosts).

7. Ensure the Cohesity cluster can resolve the FQDN of the registered Hyper-V Source and vice versa.
8. If antivirus software is installed and running on a Hyper-V host, then you must configure exclusions for the Cohesity Agent service and other services for optimal operations. Refer to Antivirus Software Exclusions and Microsoft Documentation for more information.
9. Performing Hyper-V recovery (VM, File Folder, and Instant Volume Mount) requires the Cohesity cluster to be joined to the same domain as the Hyper-V cluster.
10. 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 for all the required ports and for Virtualization-Microsoft SCVMM and Hyper-V for Hyper-V protection ports.

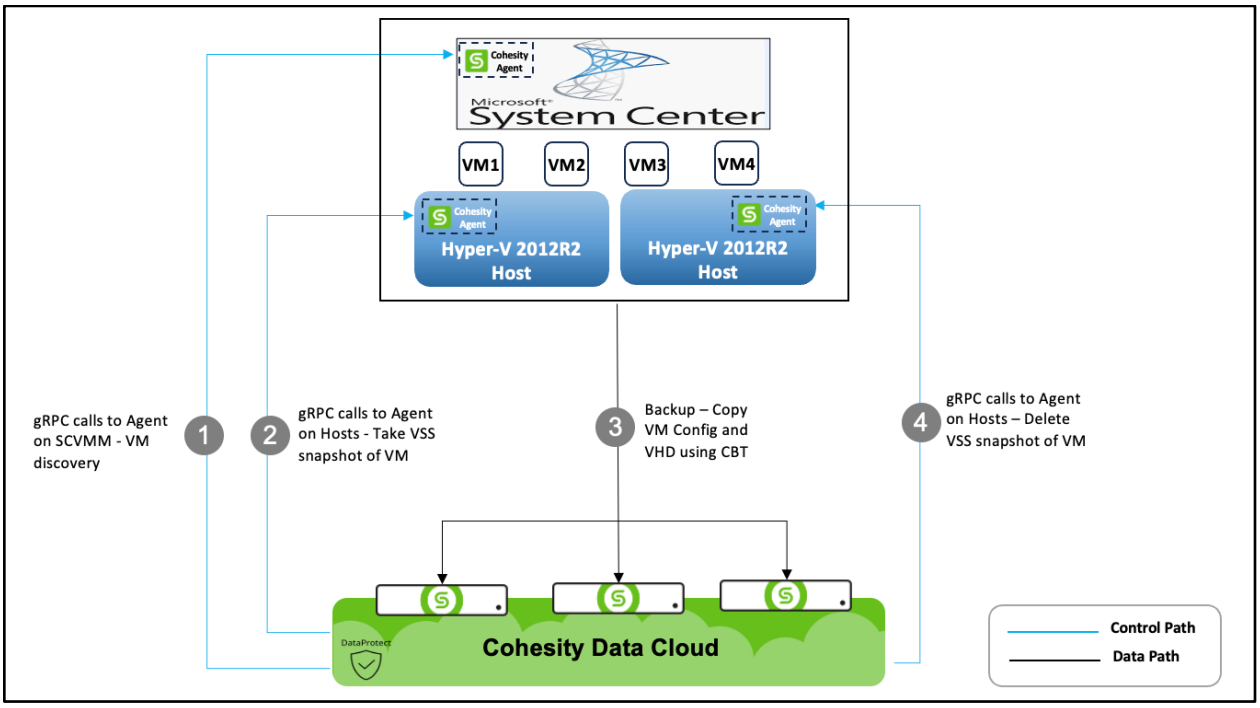
Backup Workflow - Hyper-V 2012R2 with SCVMM

Change Block Tracking (CBT) is required for performing incremental backups of individual VMs hosted by Hyper-V. Microsoft Windows Server 2012R2 does not have native CBT tech. Hence Cohesity File System CBT (installed with Cohesity Agent) is required for Hyper-V 2012R2 protection.

NOTE: Hyper-V 2008 and Hyper-V 2012 are not supported. To protect these versions, use the physical agent-based backups.

NOTE: With File System CBT, the CBT information is stored at the host level. If the VM is migrated to another host or if the host is rebooted the next backup for the VM will be a full backup.

Figure 2: Backup workflow - Hyper-V 2012R2 with SCVMM

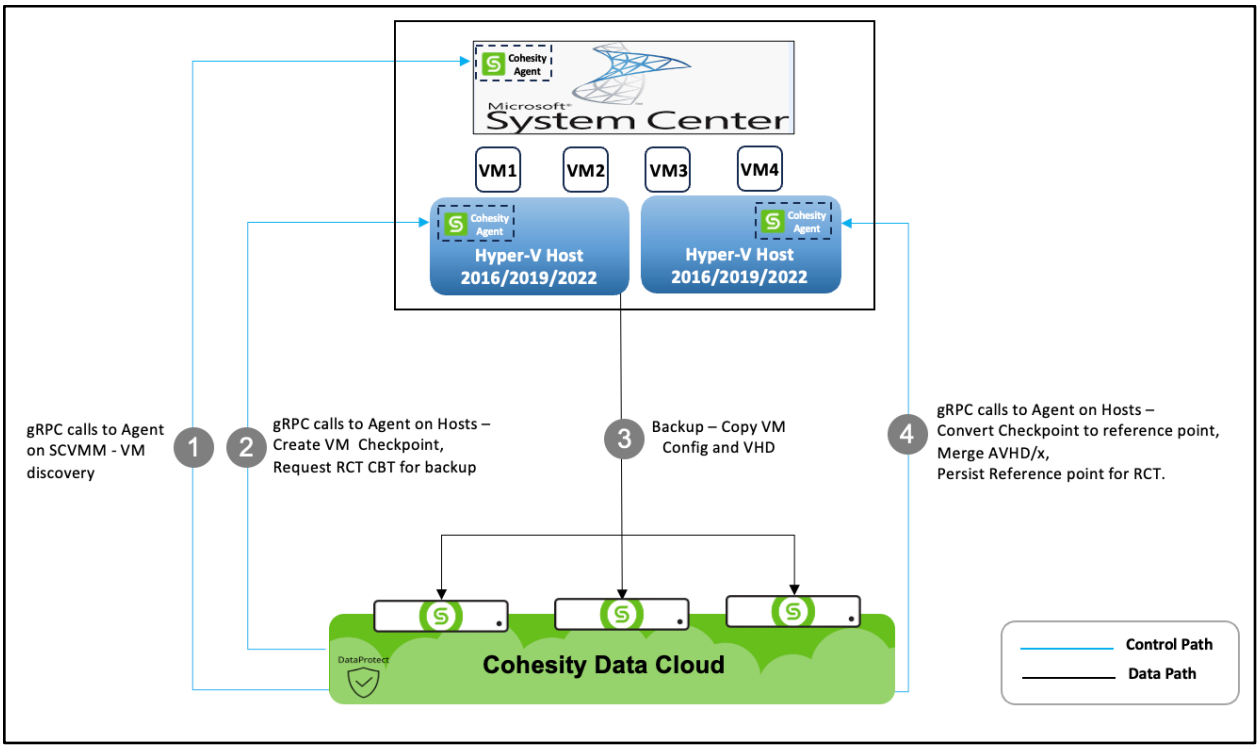


Backup Workflow - Hyper-V 2016/2019/2022 with SCVMM

Change Block Tracking (CBT) is required for performing an incremental backup of individual VMs hosted by Hyper-V. Microsoft has introduced Resilient Change Tracking (RCT) starting Windows Server 2016 as a CBT technology for incremental backups.

NOTE: You must however install the Cohesity agent on all the Hyper-V hosts without the Add-on components, Volume CBT, or File System CBT.

Figure 3: Backup workflow - Hyper-V 2016/2019/2022 with SCVMM

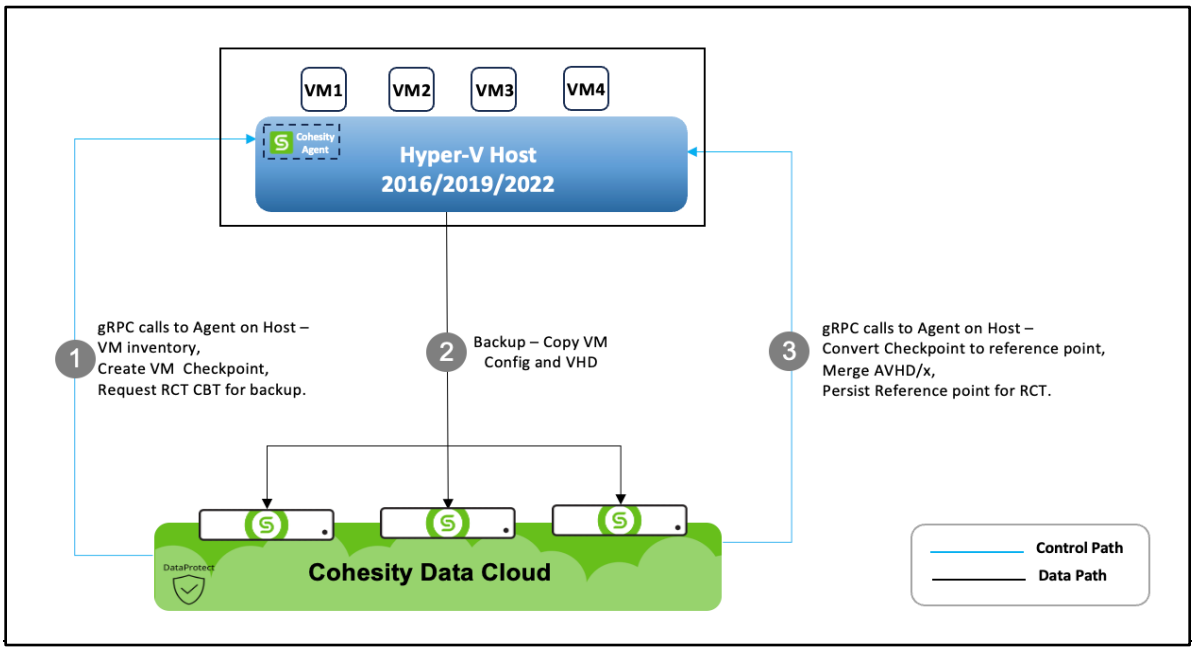


Backup Workflow - Standalone Hyper-V 2016/2019/2022

Change Block Tracking (CBT) is required for performing incremental backup of individual VMs hosted by Hyper-V. Microsoft has introduced Resilient Change Tracking (RCT) in Windows Server 2016 as CBT technology for incremental backups.

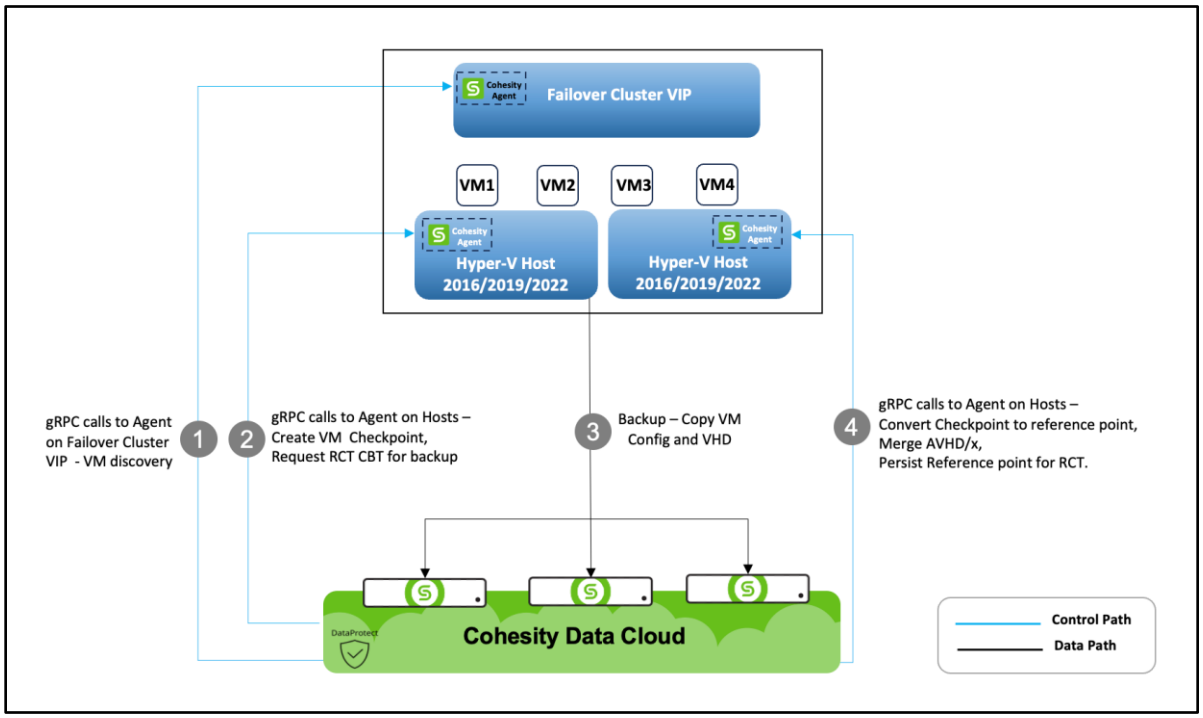
NOTE: You must, however, install the Cohesity agent on all the Hyper-V hosts without the Add-on components Volume CBT or File System CBT.

Figure 4: Backup workflow - Standalone Hyper-V 2016/2019/2022



Backup Workflow - Hyper-V 2016/2019/2022 Failover Cluster

Figure 5: Backup workflow - Hyper-V 2016/2019/2022 Failover Cluster



Hyper-V Restore Methodologies

This section describes the various restore methods for Hyper-V VM Recovery that Cohesity offers.

Recovery from Cohesity Hyper-V 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. A Full VM Recovery allows you to recover the entire Hyper-V VM while partial recovery allows you to recover individual files and folders, or simply use the Instant Volume Mount recovery.

Full VM Recovery

- Hyper-V VM Copy Recovery
- Hyper-V VM Instant Recovery
- Hyper-V VM Test & Dev (Cloning)

Partial VM Recovery

- Hyper-V File Level Recovery
- Hyper-V Instant Volume Mount (IVM) Recovery

Full VM Recovery

Hyper-V VM Copy Recovery

You can recover your protected Hyper-V VMs from a Cohesity cluster or a currently registered Cloud Archive. In this recovery process, Cohesity performs an SMB mount of the backup snapshot on the Hyper-V hosts and migrates the data from the view to Hyper-V storage. In this case, the entire VM is restored and made available for user access only after the recovery is complete, offering predictable VM performance.

NOTE: To perform a Copy recovery, disable the Instant Recovery option from the Recovery Options list.

Hyper-V 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 performs an SMB mount of the backup snapshot on the Hyper-V host. The VM is recovered from backup and powered ON from the Cohesity SMB mount making it available almost instantly. In the background, Cohesity initiates a data migration to transfer the data to the VM’s primary storage location. The recovered VM consumes Cohesity SMB mount for Disk IO activity while data migration is in progress. Upon data migration completion, the Cohesity SMB mount is unmounted from the Hyper-V hosts and the recovered VM starts using its primary storage location 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 or a cleanroom environment. Please note that there is currently no limit to the number of VMs you can restore using Instant Recovery.

Hyper-V 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 testing 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. 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 Hyper-V host.
2. The VM files are deleted on the view acting as a datastore.
3. If no VMs are using the view, the view is unmounted from all Hyper-V hosts.

Partial VM Recovery

Hyper-V 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.
- *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.

Pre-requisites and Considerations

- For Windows target VM:
  - Target VM belongs to Active Directory.
  - The Windows Remote Management (WinRM) service is enabled on the target VM: winrm quickconfig.
  - Remote powershell must be enabled from Hyper-V host to VM.
  - The Hyper-V Guest Service Interface is enabled on the target VM: Enable-VMIntegrationService -Name 'Guest Service Interface.
- For Linux target VM:
  - Cohesity Linux agent must be installed on the target VM.

Hyper-V Instant Volume Mount (IVM) Recovery

Cohesity Restore mechanism provides a way to granularly restore 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 performs SMB mount of the backup snapshot on the Hyper-V hosts and VHD/VHDX files 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.

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.

Pre-requisites and Considerations

- Only Windows VMs are supported.
- Dynamic Disks (LDM and LVM) are not supported.
- The Bring Disks Online option requires the following:
  - VM must be part of Active Directory, the VM and the Hyper-V host must be in the same AD.
  - Users must execute "winrm quickconfig" to enable winrm on the target VM and remote powershell must be enabled from Hyper-V host to VM.
- Instant volume mount and file level recovery from Gen 1 to Gen 2 type VMs is not supported.
- If SCVMM is unregistered from the Cohesity cluster, ensure you tear down all instant volume mounts. Not tearing them down can prevent the VM from being backed up when the source is registered with a different Cohesity cluster.
- Instant volume mounting Hyper-V 2012 R2 VMs without a SCSI controller is not supported. This is because Hyper-V disallows dynamically adding a SCSI controller, which is required to add the virtual disks.

- On 2012 R2 VMs, if an instant volume mount disk is attached during a Protection Group run, that snapshot cannot be application-consistent. If this occurs, the event viewer may contain a VSS-catastrophic error or similar message.

Table 1: Cohesity Recovery Methods and Comparisons

Factors / Restore Method	Copy Recovery	Instant Restore	File Level Restore	Instant Volume Mount
Full VM Restore	Yes	Yes	No	No
Restore of unindexed VMs	Yes	Yes	Yes *using the browse option	Yes
Restored VM throughput	Predictable	Variable (depends on cluster resource utilization)	NA	NA
Data migration required	Yes	Yes	No	No
User Considerations	Need VM to be served from the primary storage faster without any performance degradation.	Need Instant access to essential services VMs like AD or DNS, which other VMs depend on for their operations.	Need to restore File and Folders. Requires Indexing.	Need to restore a volume from a VM disk

Deployment Considerations - Hyper-V 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 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.

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.

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 SMB mount to bring the applications back into business immediately and will migrate the VMs to the primary storage in the background.
- 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 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.

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.

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 Instant Volume Mount

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

- 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 – Hyper-V VM Protection

This section outlines Cohesity Hyper-V 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 Tier 0 (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.
- Cohesity supports Hyper-V VM Auto Protect with Tag-based VM selection while protecting a large number of VMs for ease of management. Keep in mind that the VMs should be tagged correctly in SCVMM. 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 SCVMM 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 SCVMM, that 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.
- 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.
- When protecting a Hyper-V environment involving mixed VM configuration versions, it is recommended to protect the VMs in separate protection groups. VMs with configuration version 5 should not be mixed with version 8 and higher in a single protection group. Protect the version 5 VMs in their separate protection group.

  NOTE: VM version 5 is protected using VSS snapshot, while VM version 8 and higher leverages RCT.
- Ensure powershell is not blocked by host security software on the Hyper-V hosts to avoid source registration or backup failures.
- 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.
- 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.

Cohesity's VM Recovery Best Practices

- 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.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Sadik Sayed is a Technical Solutions Engineer at Cohesity. In his role, he focuses on NAS and Virtualization backup solutions with Cohesity.

Other essential contributors included:

- Anurag Tyagi, Cohesity Engineering
- Shishir Misra, Senior Product Manager

Document Version History

VERSION	DATE	DOCUMENT HISTORY
Version 1.0	Dec 2024	Original Document

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 44 of the Fortune 100.

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