Hitachi Ops Center Protector

7.10

Microsoft Hyper-V Application Guide

This document is intended for systems administrators who want to protect Hyper-V using Hitachi Ops Center Protector. It is assumed that the reader has a good working knowledge Hyper-V, Hitachi Block Storage administration and network administration.

MK-99PRT008-09
March 2025

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Contents

Preface

This guide describes how to backup and restore Microsoft Hyper-V using Ops Center Protector.

Ops Center Protector orchestrates the creation, retention and restoration of application-consistent and crash consistent snapshots and clones for Hyper-V. VMs can be protected by creating snapshots or clones on Hitachi Block Storage. Data protection policies are combined with data flow diagrams to automate local and remote, snapshots and replications for end-to-end data protection and recovery solutions. Snapshots and clones then can be used to revert production VMs to specific points in time and to create copies for repurposing scenarios.

Software version

This document revision applies to Ops Center Protector version 7.10. Please refer to the accompanying Release Notes for information on what's changed in this release.

Intended audience

This document is intended for systems administrators who want to protect Hyper-V using Hitachi Ops Center Protector. It is assumed that the reader has a good working knowledge Hyper-V, Hitachi Block Storage administration and network administration.

If you are new to Ops Center Protector, we recommend that you start by referring to the *Hitachi Ops Center Protector User’s Guide*, so that you understand the basic concepts, workflows and user interface.

Related documents

Main product guides:

- *Hitachi Ops Center Protector Software Release Notes*.
- *Hitachi Ops Center Protector Quick Start Guide*.
- *Hitachi Ops Center Protector User’s Guide*.
- *Hitachi Ops Center Protector Oracle Application Guide*.
- *Hitachi Ops Center Protector VMware Application Guide*.
- *Hitachi Ops Center Protector Hyper-V Application Guide*.
- *Hitachi Ops Center Protector Microsoft SQL Application Guide*

Programming guides:

- *Hitachi Ops Center Protector REST API User Guide*.
- *Hitachi Ops Center Protector REST API Reference Guide*.
- *Hitachi Ops Center Protector REST API Change Log*.

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. ▪ Indicates emphasized words in list items.
Italic	▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` ▪ Variables in headings.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing.

Convention	Description
	{ a | b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
📄	Note	Calls attention to additional information.
💡	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
❗	Important	Highlights information that is essential to the completion of a task.
⚠	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
⚠	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
⚠	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

Product user documentation is available on: https://docs.hitachivantara.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.feedback@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 1: Before you begin

Supported configurations

The following Microsoft Hyper-V configurations and technologies are supported:

- Individual VMs acting as Protector nodes in their own right (as for a physical machine).
- Microsoft Windows Server with Hyper-V role (see support matrix to determine supported versions)
- Microsoft Hyper-V Server (see support matrix to determine supported versions)
- Hyper-V configurations consisting of a single standalone machine
- Hyper-V configurations based on Windows Failover cluster
  - Must utilize Cluster Shared Volumes (CSV) based on the NTFS filesystem

The following data protection technologies are supported:

- Block based snapshots, local and remote replications of VMs

The following configurations and technologies are not supported

- Shielded VMs
- Hyper-V Replica
- VMs on clustered Hyper-V configurations utilizing ReFS based Cluster Shared Volumes (CSV)
- VMs on clustered Hyper-V configurations not utilizing Cluster Shared Volumes (CSV)
- Hyper-V virtual machines with a configuration version < 6.2
- Physical disks directly connected to a virtual machine (e.g. pass though disks, disks utilizing a virtual fibre channel adapter)

  > **Note:** These disks will be skipped during the backup process. The VM configuration and the supported disks will be protected

- Protecting Hyper-V VMs with virtual disks which are located on unsupported Block storage (see Hitachi Block prerequisites (on page 11))

Prerequisites

It is important that the following prerequisites are met before you attempt to implement any of the Microsoft Hyper-V data protection policies described in this guide.

To ensure that your hardware and software environment is fully supported, please refer to https://compatibility.hitachivantara.com/assets/ops-protector.

For detailed information on installing the Ops Center Protector Master, and Client components, please refer to the *Hitachi Ops Center Protector User’s Guide*.

Application prerequisites

In order to successfully protect a Hyper-V environment a number of prerequisites must be met.

- Protector Client software is installed on all nodes which are part of a Microsoft Hyper-V setup.
  - In case of clustered setups, the client must be installed on all nodes
- A Hyper-V account is provided, for use by Protector, having the specified Microsoft Hyper-V user privileges (on page 30)
- In order to configure protection for clustered Hyper-V setups, all cluster nodes must be running.

  Note: This is a requirement for the setup. Once configured scheduled or RPO based backups will work even if only a subset of the cluster nodes is online.
- For application level consistency, ensure that the Hyper-V integration services are enabled and functional for the VM.

For block based data protection, ensure that:

- LUN(s) are provisioned with the appropriate size on the source and destination block storage devices. This must include space for performing restore operations.
- The virtual machines are located on a single supported block storage.

Hitachi Block prerequisites

The following prerequisites are mandatory if you plan to perform snapshotting and/or replication of Hitachi Block volumes. Please also refer to the Protector support matrices at https://compatibility.hitachivantara.com/assets/ops-protector .

- A machine (known as an ISM) must be assigned that controls the Block storage device. This node must be a supported Windows or Linux machine with the Protector Client software installed.

  Caution: ISM nodes and their associated CMDs used to control storage devices must not be shared with applications other than those forming part of the Ops Center suite.
- All primary data (paths or application data) to be snapshotted or replicated within the same data protection policy must exist on the same storage device.

- The block storage hardware must:
  - Support the data protection technologies you intend to use
  - Have the correct firmware version installed
  - Have the correct SVOS version installed
- For all replication types the P-VOLs must be setup in the host group
- In order to resize logical devices represented by the Block Host node that are part of a replication or snapshot pair the array account must have the Support Personal permission.
- For UR, journals must be set up, although for HM800 and later arrays Protector can create journals
- For GAD, the quorum disks or quorum-less disks must be provided. In most cases, one quorum device between participating storage systems is satisfactory. Please refer to the *Global-Active Device User Guide* for best practices
- For GAD, the array should be configured to allow virtualized LDEVs if they are required (where supported by the array)
- Port security must be enabled.
- Primary volumes must be set up using other Hitachi tools prior to selection in Protector
- For application consistent snapshots, the application must be installed and configured to use P-VOLs on a storage array, see the relevant application guide for details on the application configuration
- The password for authorizing a Block Device node must contain only useable CCI command characters: `A-Za-z0-9’-./:@\_`
- The device must have adequate shared memory (see Provisioning and Technical Guides)
- Pools must be created using Storage Navigator prior to selecting the Target Storage in Ops Center Protector:
  - For standard mode (non-cascading) TI the TI Pools must be set up
  - For cascade mode TI the Dynamic Provisioning Pools must be set up to also be a hybrid pool, otherwise a TI pool will also be required
  - For SI, TC, UR and GAD the Dynamic Provisioning Pools must be set up
- The following licensed features may be required depending on the features being used:
  - Dynamic Provisioning
  - Storage Navigator
  - Thin Image (for TI snapshot and RTI replication scenarios)
  - ShadowImage (for SI replication scenarios)
  - TrueCopy (for TC replication scenarios)
  - Universal Replicator (for UR replication scenarios)
  - Global-Active Device (for GAD replication scenarios)
  - Remote Replication Extended (for 3DC scenarios)

- The Protector ISM node controlling the block storage device must have:
  - The correct version of Hitachi CCI installed.
  - If CCI is not installed in the default location there are two options:
    1. Add a symbolic link from the default location to the install directory
    2. Configure Protector to use CCI in the custom location using the following instructions:
       a. Stop the Protector services on the ISM node
       b. Go to the directory <Protector home>\db\config
       c. Make the change to all files matching hitachivirtualstorageplatform*.cfg
       d. Change the <BinDirectory> value from C:/HORCM/etc to the correct installation path

          ```
          <!-- Install directory of CCI, override to change
          installation directory. -->
          ```

          ```
          <BinDirectory>C:/HORCM/etc</BinDirectory>
          ```

       e. Ensure the change has been made to all files at per 3 including the default one.
       f. Start the Protector services on the ISM node
  - Access to a dedicated Command Device (CMD) on the storage device, set up as follows:

    > ⚠ **WARNING:** When running the Analyzer probe server, API Configuration Manager, and Protector ISM Client on the same VM, all components share the same command device, but API Configuration Manager and Protector ISM Client must access the storage systems using different credentials. This means that API Configuration Manager and Protector ISM client must use different login accounts when accessing the storage system.

    - Security disabled
    - User authentication enabled
    - Device group definition disabled
    - The CMD must be visible to the host OS where the Protector proxy resides
    - The CMD must be offline
    - The CMD must be added to the meta_resource only.
    - Multiple active command devices may be visible to a Protector proxy as long as each one represents a different block storage device. Behaviour is undefined if multiple active command devices represent the same block storage device, unless these are configured in the Protector proxy node fail-over priority list.
    - Fibre channel and IP command devices are supported.
    - Multipath for Command Devices is supported

- A dedicated user (specified when creating the Hitachi Block Device node) for Protector must be created on the storage device with at least the following roles:
  - Storage Administrator (Provisioning)
  - Storage Administrator (Local Copy)
  - Storage Administrator (Remote Copy)
  - Security Administrator (View & Modify).

  The user must also have access to Resource Group 0 on the storage device.
- Fibre connectivity (including zoning) or iSCSI connectivity and pre-configured RCU paths between arrays for remote replication technologies
- If physical and software block devices are being configured in a single Protector environment it is essential that they do not share an ISM node.

Chapter 2: Microsoft Hyper-V Backup Workflows

The following topics describe the steps required to configure policies and data flows to implement a number of different data protection scenarios.

For a detailed introduction on how to work with the Protector user interface, please refer to *Hitachi Ops Center Protector User's Guide*.

About Hyper-V policy classifications

The Hyper-V policy classification defines which virtual machines will be protected to which level of consistency as part of a policy.

When items are added to the inclusion or exclusion lists displayed in the Hyper-V Classification Wizard (on page 31), the Hyper-V Resource Selection Wizard (on page 33) is launched. This wizard enables virtual machines to be selected based via browsing, or by pattern matching of virtual machine name, configuration path or host running the VM.

The list of VMs included in the classification is evaluated at different times depending on how they are specified:

Evaluation is only performed once, when browsing and selecting the virtual machine directly.

Evaluation is done every time the operation is triggered if VMs are:

- Implicitly selected using a virtual machine location (path) or virtual machine host (hypervisor)
- Specified using a name pattern (i.e. using wildcards, e.g. Sales*)

Tip: With this method of classification, VMs will be automatically added to the backup (without reactivating the data flow) when they are added to a selected path or host or given a name that matches the defined pattern. For continuous replications it will be necessary to trigger the relevant operation to cause re-evaluation

Every Hyper-V object selected in the classification is resolved to a list of VMs. For example, when selecting a virtual machine location, all VMs with configurations in that location are selected. If any included VMs utilize additional paths, these will be added too. This ensures that backed up virtual machines can be fully restored.

Tip: Use the preview selection functionality of the Hyper-V Classification Wizard (on page 31) to preview which VMs will be included for a given Hyper-V Node based on the provided inclusion and exclusion lists.

Virtual machine consistency

The consistency of virtual machine backups differs based on the consistency level chosen in the policy. Before the block-based backup is performed Protector will create a checkpoint for every virtual machine.

Application consistent checkpoints will use Hyper-V integration services to quiesce the data inside the VM. In case of Windows VMs, Protector will utilize VSS within the virtual machine to save application and filesystem data to disk. For Linux, the Hyper-V integration will request a quiesce, however usually this will only cause the filesystem buffers to be saved to disk. If an application consistent VM checkpoint cannot be created, Protector will create a crash consistent checkpoint instead.

Crash consistent checkpoints will create a checkpoint of the virtual disks as they are.

Block based workflows

This section addresses the workflows for block based backups.

How to create VM restore points with block snapshots

Before you begin

It is assumed that the following tasks have been performed:

- The Protector Master software has been installed and licensed on a dedicated node.
- The Protector Client software has been installed on all nodes of the Hyper-V setup which should be protected.
- The Protector Client software has been installed on the node that will act as a proxy for the Hitachi storage device where the Hyper-V data is located. Note that for a Thin Image snapshot, the source and destination LDEVs are located on the same device
- The block storage device has been set up as per the Protector requirements and prerequisites. Refer to Hitachi Block prerequisites (on page 11).
- Permissions have been granted to enable the Protector UI, required activities and participating nodes to be accessed. In this example all nodes will be left in the default resource group, so there is no need to allocate nodes to user defined resource groups.
- A Hyper-V user has been created that provides the required privileges as detailed in Microsoft Hyper-V user privileges (on page 30). This user will be required when creating the Hyper-V node in the steps that follow.

This task describes the steps to follow when snapshotting VMs that reside on a Hitachi Block storage device. The data flow and policy are as follows:

Figure 1 Hyper-V Block Snapshot Data Flow

Table 1 Hyper-V Snapshot Policy

Classification Type	Parameters	Value
Hyper-V	Include / Exclude	Refer to About Hyper-V policy classifications (on page 15) for details on how to specify VMs that are to be included in a backup.
	Virtual Machine Consistency	Application consistent checkpoints.

Operation Type	Parameters	Value	Assigned Nodes
Snapshot	Mode	Hardware	Hyper-V application node
	Hardware Type	Hitachi Block	
	Run Options	Run on RPO	
	RPO	2 hours	
	Retention	2 days	

Procedure

1. Locate the source *OS Host* node in the **Node Inventory** and check that the nodes are authorized and online

   These nodes represent the Protector Clients installed on your Hyper-V environment.

2. Create a new *Hyper-V* node (unless a suitable one already exists) using the Hyper-V Node Wizard (on page 26).

   The *Hyper-V* node type is grouped under **Hypervisor** in the **Node Type Wizard**.

   a. Select **one node** which is part of your **Hyper-V environment**

   b. Specify the **Username** and **Password** of a user having the required privileges as detailed in Microsoft Hyper-V user privileges (on page 30).

c. Select which **configuration** you want to the Hyper-V node to represent. In case of a standalone Hyper-V system you will only have one option. In the case of a clustered system, you must choose if the application node should represent just this host or the complete cluster.

3. Locate the node in the **Nodes Inventory** that will control the Hitachi Block Device (via a CMD) where the Hyper-V data is located. Check that the node is authorized and online.

   This node is used by Protector to orchestrate snapshot creation and is identified as the **Proxy Node** when creating the Hitachi Block Device node in the next step. This node is known as an ISM (Intelligent Storage Manager) node. The ISM node does not appear in the data flow.

4. Create a new Hitachi Block Device node (unless one already exists) using the **Block Storage Node Wizard** and check that it is authorized and online.

   The Hitachi *Block Device* node type is grouped under **Storage** in the **Node Type Wizard**. Note that this node does not appear in a Hyper-V snapshot data flow diagram, but is identified when assigning the snapshot policy.

5. Define a policy as shown in the table above using the **Policy Wizard**, Hyper-V Classification Wizard (on page 31) and **Snapshot Operation Wizard**.

   The *Hyper-V* classification is grouped under **Hypervisor** in the **Policy Wizard**.

6. Draw a data flow as shown in the figure above, that shows only the *Hyper-V* source node, using the **Data Flow Wizard**.

   At this stage the snapshot icon ⟲ is not shown.

7. Assign the *Snapshot* operation to the *Hyper-V* source node. The *Hyper-V-Snapshot* policy will then be assigned automatically.
   The **Block Snapshot Configuration Wizard** is displayed.

8. Select the **Storage Node** corresponding to the Hitachi Block storage device where the Hyper-V Server's data is located. Then select a **Snapshot Pool** from one of the available Thin Image or hybrid pools.

9. Leave the remaining **Advanced Configuration** options at their default settings, then click **OK**.

   > ⚠ **Caution:** If you want to preserve Hyper-V snapshots after restoring from VMs them, use **Cascade mode** (the default setting) when assigning the snapshot operation on the data flow. This will enable the **Mount duplicate** option in the Hyper-V Restore Wizard (on page 38) when performing a restore.

   The snapshot icon ⟲ is now shown superimposed over the source node.

10. Compile and activate the data flow, checking carefully that there are no errors.

11. Locate the active data flow in the **Monitor Inventory** and open its **Monitor Details**.

    The policy will be invoked automatically to create a snapshot repeatedly according to the RPO specified in the policy. The policy can also be manually triggered from the source node in the monitor data flow.

12. Watch the active data flow via the **Monitor Details** to ensure the policy is operating as expected.

You should periodically see:

- Backup jobs appearing in the **Jobs** area below the data flow that show progress percentage, ending in *Progress - Completed*.
- Information messages appearing in the **Logs** area below the data flow indicating rules activation and snapshot events.

13. Review the status of the Hitachi *Block Device* to ensure snapshots are being created. New snapshots will appear in the **Block Snapshot Inventory** periodically as dictated by the *RPO* of the policy. Old snapshots will be removed periodically as dictated by the *Retention Period* of the policy.

Chapter 3: Microsoft Hyper-V Restore workflows

How to restore VMs from a block snapshot or replication

Before you begin

It is assumed that a Hyper-V policy that creates hardware snapshots or replications has been implemented and that at least one snapshot or replication has been created. See How to create VM restore points with block snapshots (on page 16) for an example of how to do this.

This task describes the steps to follow when using a block snapshot or replication backup to:

- restore entire VMs
- clone entire VMs for repurposing

All the above scenarios follow the same basic workflow:

Procedure

1. Identify the destination where the VMs are to be restored, then ensure that it is prepared to receive them by locating the Hyper-V Server node in the **Nodes Inventory** and checking it is authorized and online.

   ⚠ **Caution:** When restoring virtual machines to the original system and location, ensure that the virtual machine and its directories no longer exist.

2. Locate the snapshot or replication to be restored by navigating to the **Restore Dashboard**, then click the **Hitachi Block** button to open the **Block Restore Inventory**.

   You must click the **Search** button to view the list of available snapshots and replications in the inventory.
3. Click on the snapshot or replication that you want to restore to open the **Block Snapshot/Replication Details**.
   The snapshot or replication details are displayed, along with the list of VMs in this backup.
4. Click **Restore** to open the Hyper-V Restore Wizard (on page 38) to restore the original VMs or create clones.
5. Select the option to **restore selected virtual machines.** Click next.
6. Select the VMs for the restore. Click next.
7. Choose whether to restore to the **Original location** or create a **Clone**. Click **Next**.
8. If creating a **Clone**:
   a. Specify a **Cloned Virtual Machine Name Prefix**, this will be prepended to the existing name of each VM being restored.
   b. Specify a destination Hyper-V node and directory.

9. Select **virtual machine restore** options as detailed in Hyper-V Restore Wizard – Virtual Machine restore options (on page 42) options. Click **Next**
10. Select the mount mode and specify the **Mount Pool** if necessary, then click **Finish**. The mount mode determines how the temporary volume, from which the backed up VM(s) are to be taken, will be created during the restore process. For replications, the mount mode is always set to **Mount original**.

    > ⚠ **Caution:** Select the mount mode depending on the behaviour required:
    >
    > - **Mount original** - Mounts the original (Level 1) snapshot and copies the virtual machine data to the target location. Virtual machines will be copied before they are registered with Hyper-V. Virtual machines will also only powered on once the copy is complete.
    >
    >   This option will expose your original backup to the Hyper-V host. Any changes will persist even after the unmount. While Protector will not perform any changes, nothing is preventing users or other processes from modifying the data.
    > - **Mount duplicate** - Protector will create a cascaded duplicate of the original snapshot and perform the restore from the duplicate. The original snapshot is preserved. Use **Cascade mode** (the default setting) in the **Block Snapshot Configuration Wizard** when assigning the snapshot operation on the data flow to enable **Mount duplicate** when restoring.

    A `Processing` message will appear briefly, then the wizard will close and the **Jobs Inventory** will be displayed. A new *Restore Job* will appear at the top of the Jobs list, with the *Progress* entry initially indicating processing and finally indicating successful completion.
11. Once the restore process is complete, further steps may be needed to fix-up the VM(s).

    The amount of fix-up work required depends on the applications accessing or running on the restored VM(s).
12. Restart any applications that access or run on the restored VM(s).
13. Resume any backup policies for the restored VM(s). If you have restored data to a new location for repurposing (test and development work for example), you should consider if it is necessary to implement a new backup policy to protect this new instance(s).

    > ⚠ **Caution:** When restoring virtual machines to the original location, they will get a new ID. Due to this, existing policies may no longer cover them if the VMs were explicitly selected for backup. Use the preview functionality of the Hyper-V Classification Wizard to ensure that the virtual machines are included in future backups.

How to export VMs from a block snapshot or replication to a filesystem

Before you begin

It is assumed that a Hyper-V policy that creates hardware snapshots or replications has been implemented and that at least one snapshot or replication has been created. See How to create VM restore points with block snapshots (on page 16) for guidance on how to do this.

This task describes the steps to follow when exporting VMs to a filesystem using a block snapshot or replication backup.

Procedure

1. Identify the destination where the VMs are to be exported, then ensure that it is prepared to receive them by locating the Hyper-V node in the **Nodes Inventory** and checking it is authorized and online.
2. Locate the snapshot or replication to be restored by navigating to the Restore Dashboard, then click the Hitachi Block button to open the Block Restore Inventory.

   You must click the Search button to view the list of available snapshots and replications in the inventory.
3. Click on the snapshot or replication that you want to restore to open the Block Snapshot/ Replication Details.

   The snapshot or replication details are displayed, along with the list of VMs in this backup.
4. Click Restore to open the Hyper-V Restore Wizard to restore the original VMs or create clones.
5. Select the option to **export virtual machines to filesystem.** Click next.
6. Select the VMs for the export. Click next.
7. Specify a destination Hyper-V node and directory. Click next.
8. Select the mount mode and specify the Mount Pool if necessary, then click Finish.

   The mount mode determines how the temporary volume, from which the backed up VM(s) are to be taken, will be created during the restore process. For replications, the mount mode is always set to Mount original.

> ⚠ **Caution:** Select the mount mode depending on the behaviour required:
>
> - **Mount Original** - Mounts the original snapshot and exports the virtual machine data to the target location.
>
>   This option will expose your original backup to the Hyper-V host. Any changes will persist even after the unmount. While Protector will not perform any changes, nothing is preventing users or other processes from modifying the data.
>
> - **Mount duplicate** - Protector will create a cascaded duplicate of the original snapshot and perform the restore from the duplicate. The original snapshot is preserved. Use Cascade mode (the default setting) in the Block Snapshot Configuration Wizard when assigning the snapshot operation on the data flow to enable Mount duplicate when exporting.

A Processing message will appear briefly, then the wizard will close, and the Jobs Inventory will be displayed. A new Restore Job will appear at the top of the Jobs list, with the Progress entry initially indicating processing and finally indicating successful completion.

9. Once the restore process is complete the virtual machine export will be available in the destination directory.

How to mount virtual disks from a block snapshot or replication to a VM

Before you begin

It is assumed that a Hyper-V policy that creates hardware snapshots or replications has been implemented and that at least one snapshot or replication has been created. See How to create VM restore points with block snapshots (on page 16) for guidance on how to do this.

> **Note:** Snapshots and replications cannot be used for mount operations if they are currently mounted elsewhere.

This task describes the steps to follow when mounting virtual disks contained within a block snapshot or replication, to an existing VM. This procedure will result in all of the virtual disks from the selected VM backup being mounted as new virtual disks on the target VM. The newly mounted virtual disks appear in addition to any existing virtual disks:

Procedure

1. Identify the destination where the virtual disks are to be mounted. The destination host must be represented by a Protector Hyper-V node. If the destination is not represented in Protector, then create one using the Hyper-V Node Wizard (on page 26)
2. Ensure that the mount location is prepared to receive the virtual disks by locating the host node in the Nodes Inventory and checking it is authorized and online.
3. Locate the Hyper-V snapshot or replication, containing the virtual disks to be mounted, by clicking the Restore link on the Navigation Sidebar to open the Restore Dashboard. Then click the Hitachi Block button to open the Block Restore Inventory. You must click the Search button to view the list of available snapshots.
4. Select the Hyper-V snapshot or replication that contains the virtual disks to be mounted. Then click Mount to open the Hyper-V Mount Wizard (on page 45) which will guide you through the mount process.
5. Select the Virtual Machine that contains the virtual disks to be mounted. Click Next.
6. Select the Hyper-V Node where the mount target VM is located. Then select the target VM. Click Next.
7. Select the mount mode and specify the Mount Pool if necessary, then click Finish.

   The mount mode determines how the temporary volume, from which the backed up VM(s) are to be taken, will be created during the restore process. For replications, the mount mode is always set to Mount original.

⚠ **Caution:** Select the mount mode depending on the behaviour required:

- **Mount Original** - Mounts the original snapshot.

  This option will expose your original backup to the Hyper-V host. Any changes will persist even after the unmount. While Protector will not perform any changes, nothing is preventing users or other processes from modifying the data.

- **Mount duplicate** - Protector will create a cascaded duplicate of the original snapshot and perform the restore from the duplicate. The original snapshot is preserved. Use Cascade mode (the default setting) in the Block Snapshot Configuration Wizard when assigning the snapshot operation on the data flow to enable Mount duplicate when exporting.

A Processing message will appear briefly, then the wizard will close, and the Jobs Inventory will be displayed. A new Restore Job will appear at the top of the Jobs list, with the Progress entry initially indicating processing and finally indicating successful completion.

8. Once the mount job is complete, further steps may be needed to fix-up the application data on the VM before using it. The amount of fix-up work required depends on the applications hosted on the VM.
9. It may be necessary to restart the OS on the VM before the newly mounted virtual disks can be used.

How to restore individual files from a block snapshot or replication

Before you begin

It is assumed that a Hyper-V policy that creates hardware snapshots or replications has been implemented and that at least one snapshot or replication has been created. See How to create VM restore points with block snapshots (on page 16) for guidance on how to do this.

Note: Snapshots and replications cannot be used for mount operations if they are currently mounted elsewhere.

This task describes the steps to follow when restoring specific files from virtual disks, contained within a block snapshot or replication, to an existing VM:

Procedure

1. Mount the virtual disks containing the files that are to be restored using the following procedure:
   - How to mount virtual disks from a block snapshot or replication to a VM (on page 23) – mount the virtual disks to a machine other than the one it originated from, to avoid a UUID conflict.
2. Locate the files on the newly mounted or restored VM and copy them to the required location.

3. Unconfigure the mounted virtual disks inside the VM.
4. Unmount the VM using Protector.

Chapter 4: Reference

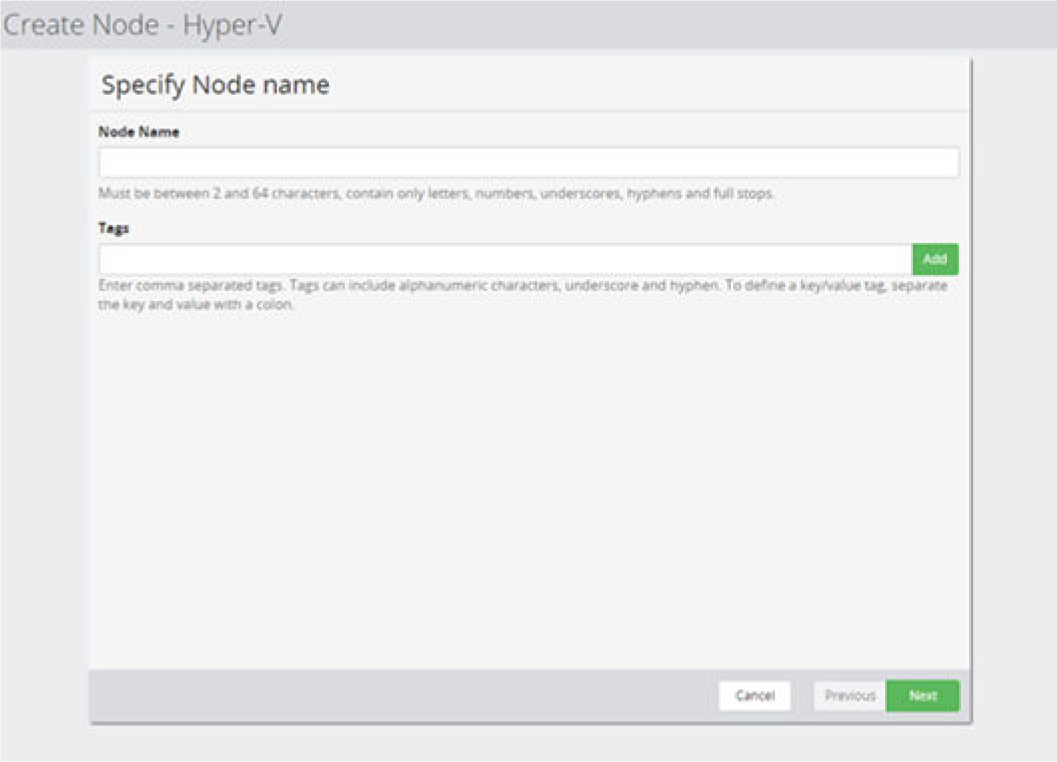
This section provides salient reference information that supports the workflows detailed in this guide.

Nodes UI Reference

This section describes the Nodes UI pertaining to the node types that are used to backup Hyper-V.

Hyper-V Node Wizard

This wizard is launched when a new Hyper-V Node is added to the Nodes Inventory.



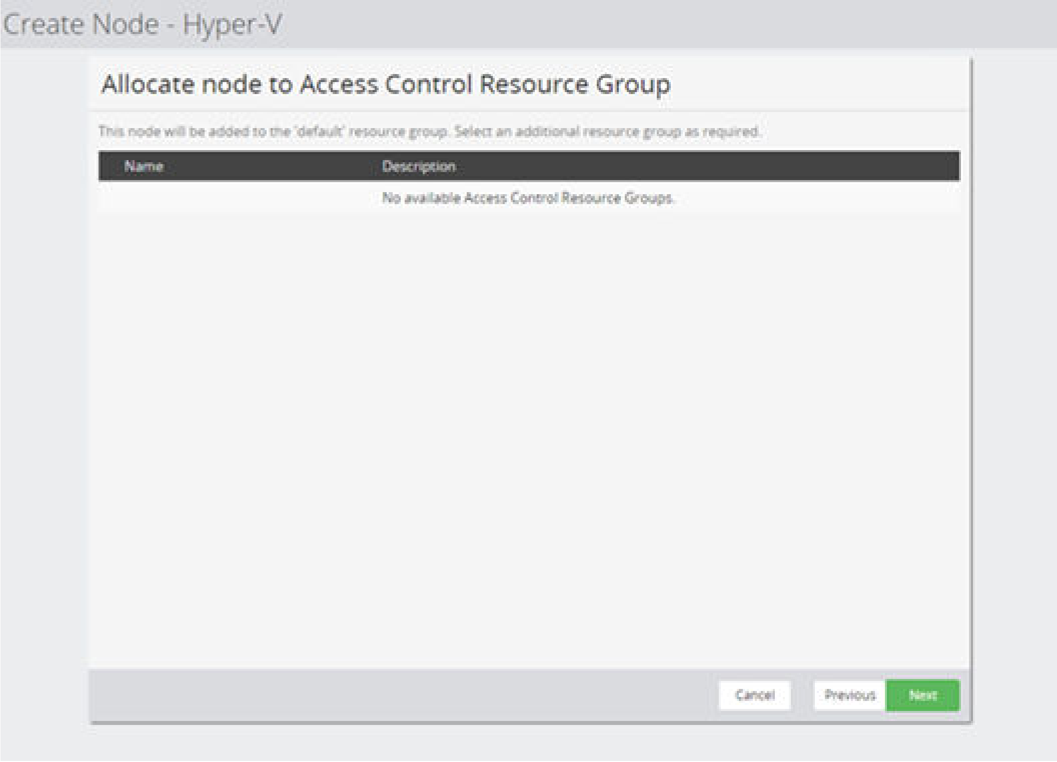
Must be between 2 and 64 characters, contain only letters, numbers, underscores, hyphens and full stops.

Enter comma separated tags. Tags can include alphanumeric characters, underscore and hyphen. To define a key/value tag, separate the key and value with a colon.

Figure 2 Hyper-V Node Wizard - Specify Node name

Control	Description
Node Name	Enter a name for the Hyper-V node.

Control	Description
Tags	Add the tags to be associated with the object being created



Create Node - Hyper-V

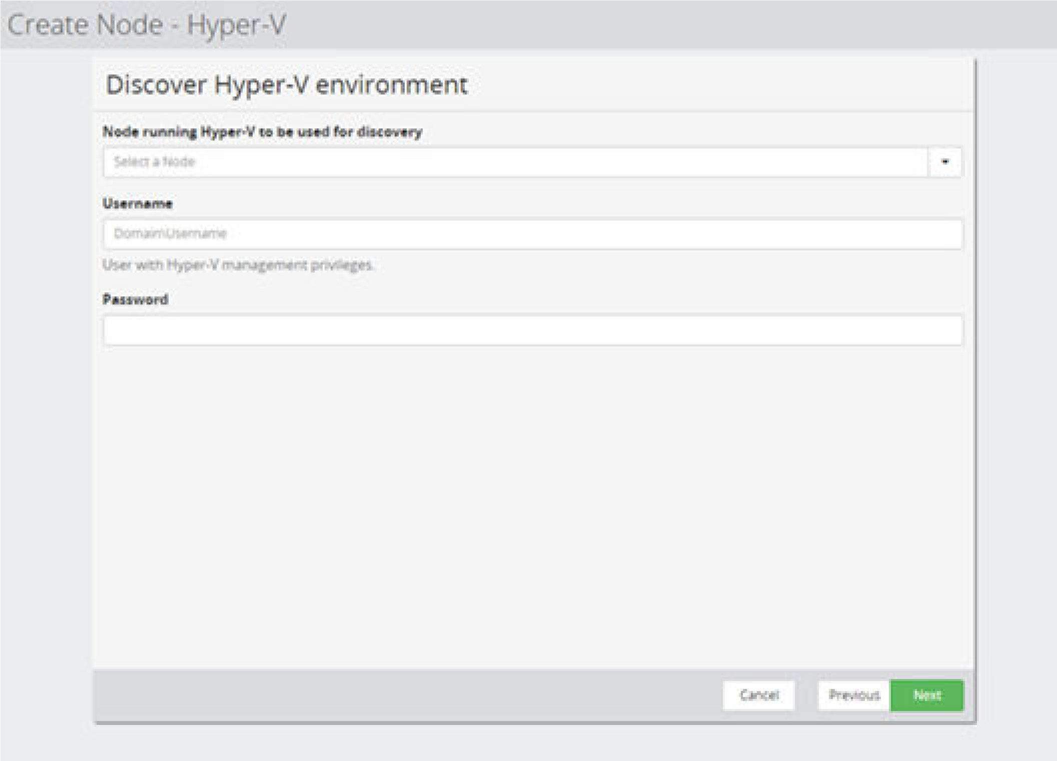
Allocate node to Access Control Resource Group

This node will be added to the 'default' resource group. Select an additional resource group as required.

Name	Description
	No available Access Control Resource Groups.

Figure 3 Hyper-V Node Wizard - Allocate node to Access Control Resource Group

Control	Description
Resource Groups	Select the resource group(s) to which this node will be allocated for the purposes of RBAC. All nodes are automatically allocated to the 'default' resource group.



Create Node - Hyper-V

Discover Hyper-V environment

Node running Hyper-V to be used for discovery

Select a Node

Username

Domain\Username

User with Hyper-V management privileges.

Password

Figure 4 Hyper-V Node Wizard - Select node running Hyper-V server

Control	Description
Node running Hyper-V	Select an OS Host node which is part of the Microsoft Hyper-V standalone or cluster environment
Username	Enter the username that will be used to perform backups and restores on this Hyper-V environment. The user requires privileges as detailed in Microsoft Hyper-V user privileges (on page 30).
Password	Enter the password for the username provided above

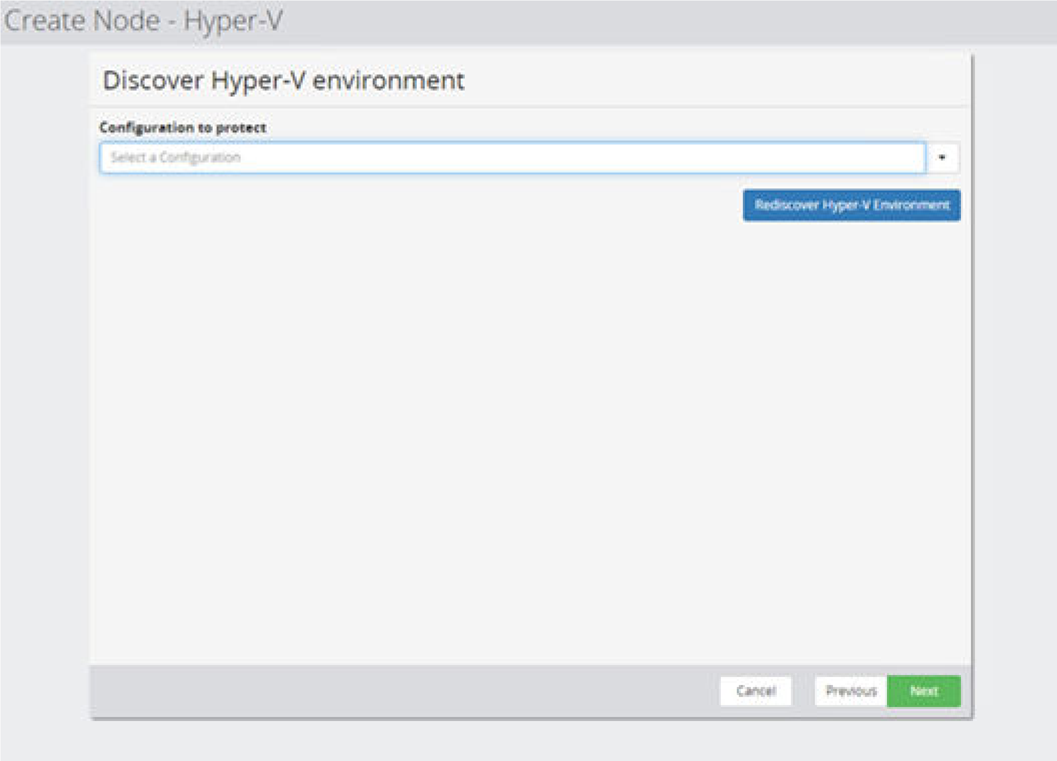
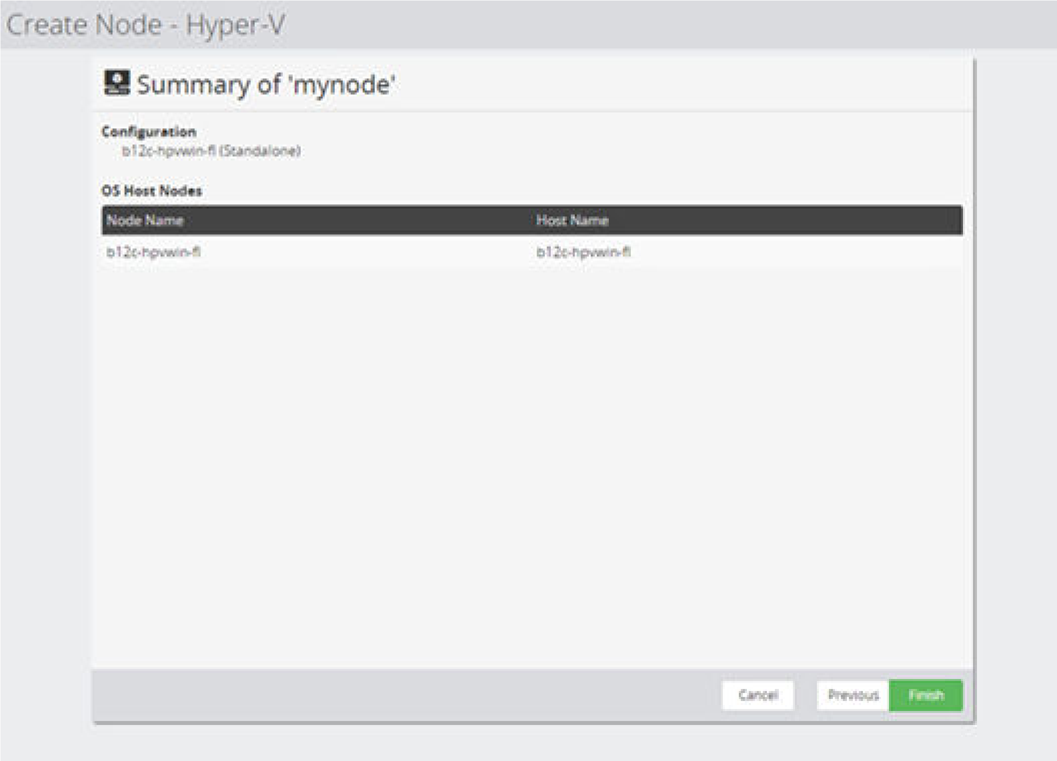


Figure 5 Hyper-V Node Wizard - Discover Hyper-V environment

Control	Description
Configuration to protect	Select the Hyper-V environment you want this node to represent
Rediscover Hyper-V Environment	Click in case you want to refresh the list of available Hyper-V configuration



Create Node - Hyper-V

Summary of 'mynode'

Configuration
b12c-hpvwin-fl (Standalone)

OS Host Nodes

Node Name	Host Name
b12c-hpvwin-fl	b12c-hpvwin-fl

Figure 6 Hyper-V Node Wizard - Summary

Control	Description
Summary	Summary of the settings entered.

Microsoft Hyper-V user privileges

To lookup, protect and restore Hyper-V virtual machines Protector requires credentials that are valid for all machines comprising the Hyper-V node.

In case of a cluster, these credentials must be domain credentials. For a standalone configuration, a local user is sufficient.

The user needs to be a member of the following groups in the domain and all nodes of the Hyper-V setup:

- Users
- Domain Users
- Backup Operators
- Hyper-V Administrators
- Remote Management Users

In addition, for a cluster the user requires the permission to administrate the cluster. The following command needs to be executed on every cluster node:

```
Grant-ClusterAccess -User domain\username -Full
```

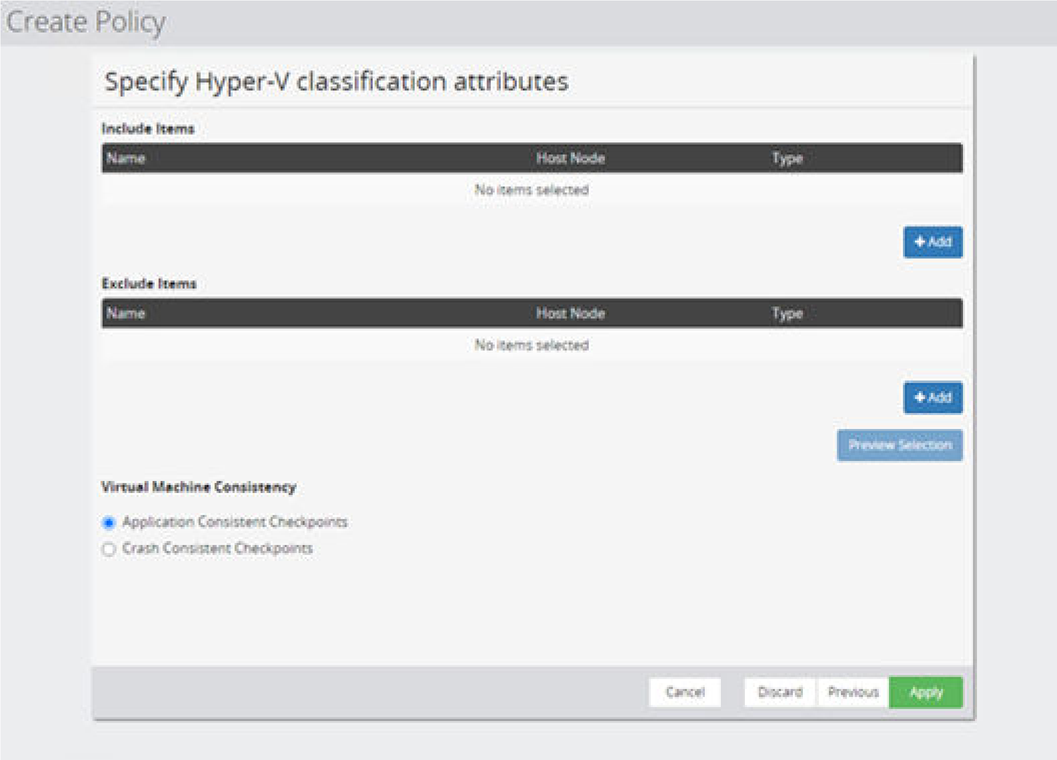
Policies UI Reference

This section describes the Policies UI pertaining to the policies that are applied to backup Microsoft Hyper-V.

Hyper-V Classification Wizard

This wizard is launched when a new Hyper-V classification is added to policy.

The Hyper-V classification is used as a means to conveniently specify the Hyper-V resources which should be included in a backup. Refer to About Hyper-V policy classifications (on page 15) for details about how this classification works with host and block based operations.



Create Policy

Specify Hyper-V classification attributes

Include Items

Name	Host Node	Type
No items selected		

Exclude Items

Name	Host Node	Type
No items selected		

Virtual Machine Consistency

● Application Consistent Checkpoints

○ Crash Consistent Checkpoints

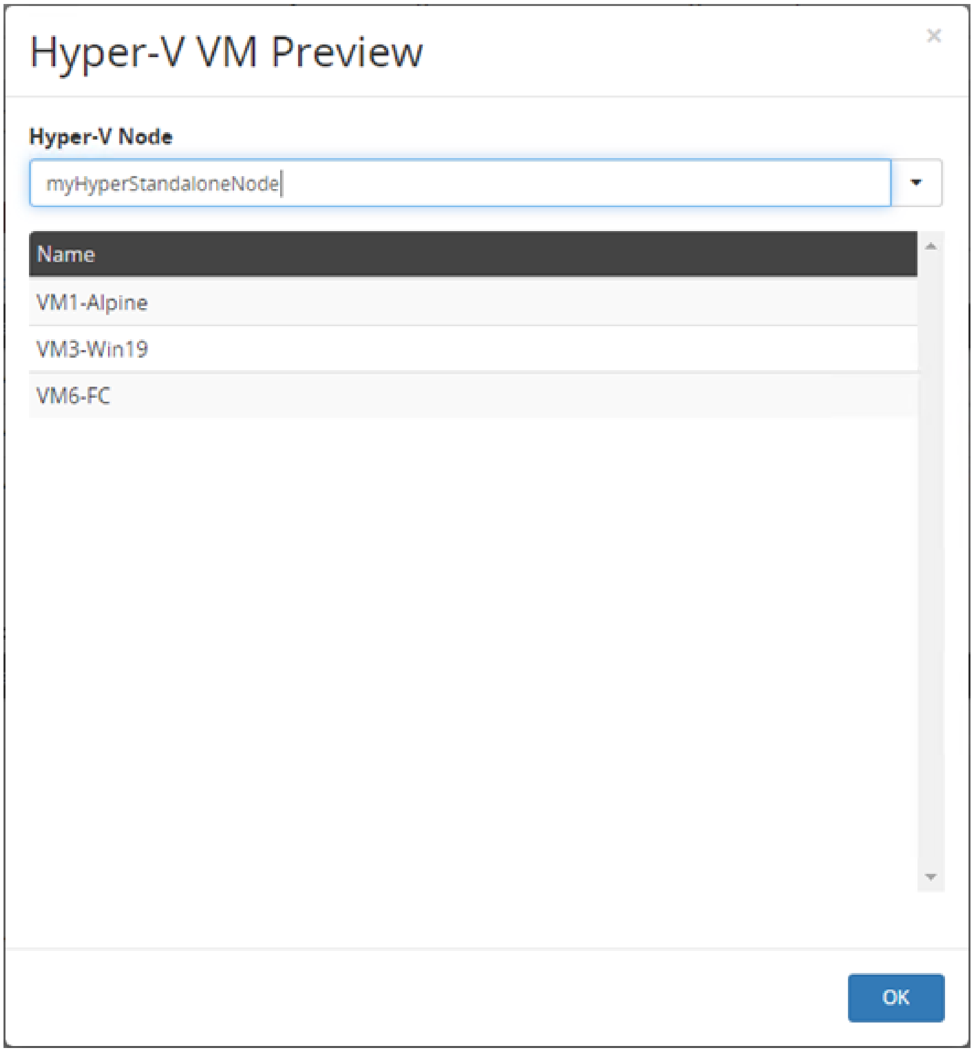
Figure 7 Hyper-V Wizard - Specify Hyper-V classification attributes

Control	Description
Included Items	Lists the Hyper-V resources that will be included in the backup.
Add	Opens the Hyper-V Resource Selection Wizard (on page 33) to enable Hyper-V Resources to be added to the include/exclude items list above.
Excluded Items	Lists the Hyper-V VMs that will be excluded from the backup policy.
Remove	Each row has a remove button at the end of the row. When clicked the selected Hyper-V resource is removed from the include/exclude list.

Control	Description
Preview Selection	Opens the Hyper-V Classification Preview Wizard (on page 32) Hyper-V Classification Preview Wizard, that will preview which VMs will be included if the classification is applied to a selected Hyper-V node.
Virtual Machine Consistency	Select which level of consistency is desired for the virtual machines: ▪ **Application consistent checkpoints** will use Hyper-V integration services to quiesce the data inside the VM. ▪ **Crash consistent checkpoints** will just use the data currently available on the virtual disks.

Hyper-V Classification Preview Wizard

This wizard is displayed when the user previews a Hyper-V policy classification.



Hyper-V VM Preview

Hyper-V Node: myHyperStandaloneNode

Name
VM1-Alpine
VM3-Win19
VM6-FC

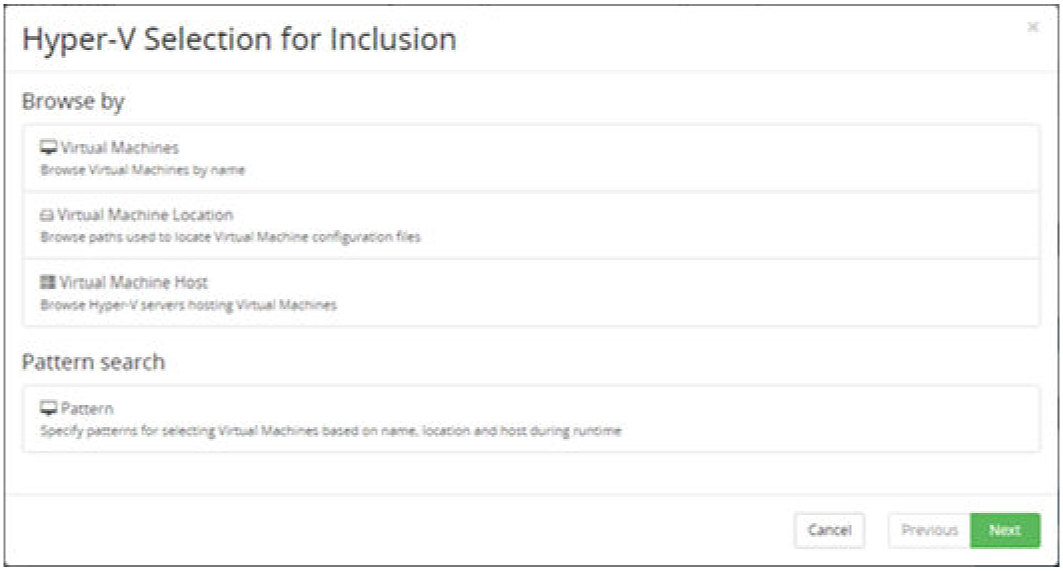
Figure 8 Hyper-V Classification Preview Wizard

Control	Description
Hyper-V Node	Select the Hyper-V app node you want to preview the classification for.
Virtual Machine List	Lists all virtual machines that would be considered for backup, based on the classification.

Hyper-V Resource Selection Wizard

This wizard is displayed when the user includes or excludes Hyper-V resources in a policy.

Caution: Protector tracks Hyper-V VMs via their unique ID. If the id of an explicitly selected VM is changed (e.g. by deleting and restoring the VM) it will not be included in the backup and an error will be logged.



Hyper-V Selection for Inclusion

Browse by

Virtual Machines
Browse Virtual Machines by name

Virtual Machine Location
Browse paths used to locate Virtual Machine configuration files

Virtual Machine Host
Browse Hyper-V servers hosting Virtual Machines

Pattern search

Pattern
Specify patterns for selecting Virtual Machines based on name, location and host during runtime

Figure 9 Hyper-V VM Selection for Inclusion

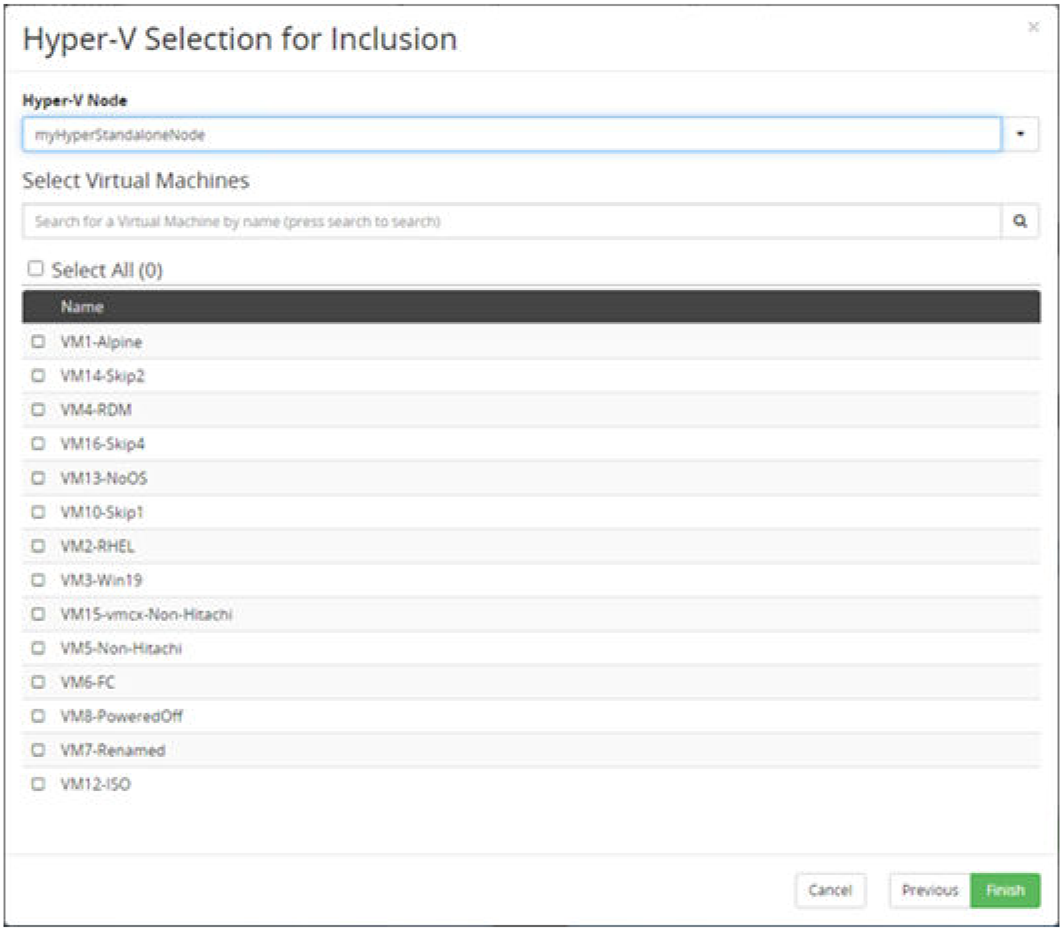
Control	Description
Virtual Machines	Displays flat list of the virtual machines configured on a Hyper-V node. One more VMs can be selected.. See Hyper-V Resource Selection Wizard – Browse Virtual Machines (on page 34) below.
Virtual Machine Locations	Displays a hierarchical view of a Hyper-V node's file system. See Hyper-V Resource Selection Wizard – Browse by Virtual Machine Locations (on page 35) below. **Note:** Protector will select all virtual machines, that have a configuration file under the select path. The list of VMs per path is re-evaluated at the beginning of each backup.

Chapter 4: Reference

Control	Description
Virtual Machine Host	Displays a hierarchical view of Hyper-V nodes and VMs. It is possible to select one or more nodes of a cluster as well as individual VMs. See Hyper-V Resource Selection Wizard – Browse by Virtual Machine Hosts (on page 36) below. **Note:** If a host is selected Protector will select all virtual machines available on that host. The list of available virtual machines per host is re-evaluated at the beginning of each backup.
Pattern	Select if you want to specify a resource by type and name pattern match. See Hyper-V Resource Selection Wizard – Pattern search (on page 37) below.

Hyper-V Resource Selection Wizard – Browse Virtual Machines

This page of the wizard is displayed when the browse by virtual machines option is selected in the initial wizard page above.



Hyper-V Selection for Inclusion

Hyper-V Node

myHyperStandaloneNode

Select Virtual Machines

Search for a Virtual Machine by name (press search to search)

□ Select All (0)

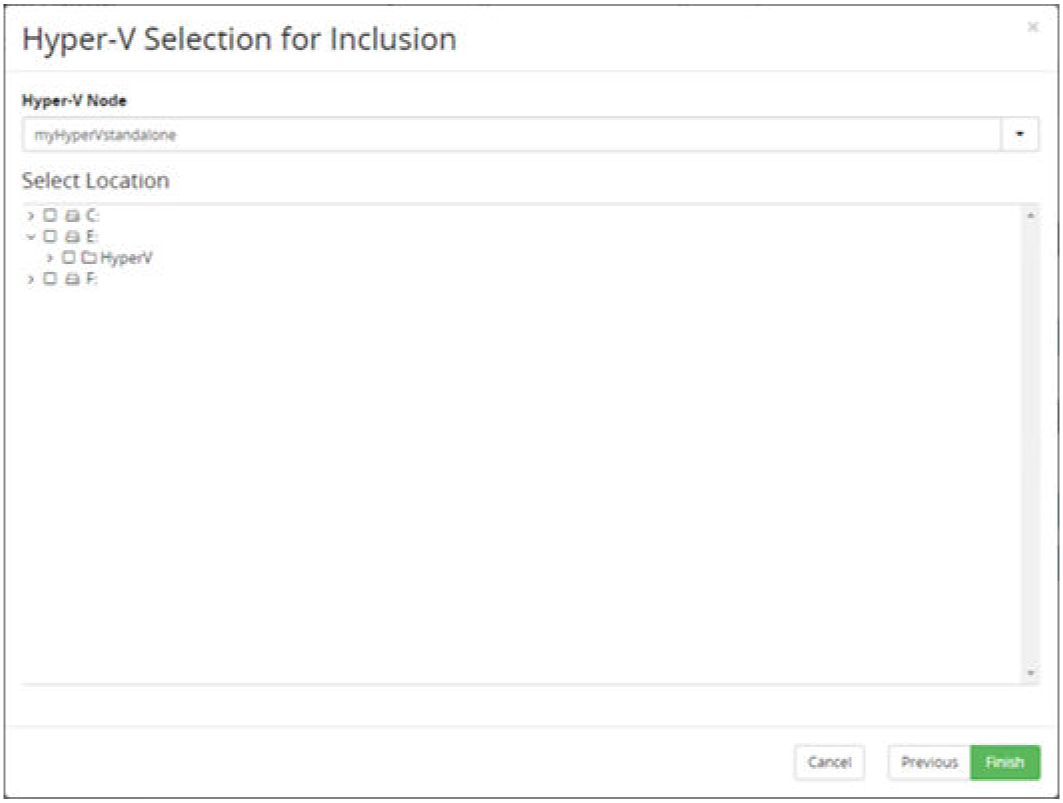
	Name
□	VM1-Alpine
□	VM14-Skip2
□	VM4-RDM
□	VM16-Skip4
□	VM13-NoOS
□	VM10-Skip1
□	VM2-RHEL
□	VM3-Win19
□	VM15-vmcx-Non-Hitachi
□	VM5-Non-Hitachi
□	VM6-FC
□	VM8-PoweredOff
□	VM7-Renamed
□	VM12-ISO

Figure 10 Hyper-V Policy Wizard - Classification – Browse Virtual Machines

Control	Description
Hyper-V Node	Select the Hyper-V app node you want to select VMs from.
Search	Enter a part of a virtual machine name and confirm to filter the list of virtual machines.
Virtual Machine List	Select one or more machines.

Hyper-V Resource Selection Wizard – Browse by Virtual Machine Locations

This page of the wizard is displayed when the browse by virtual machine paths option is selected in the initial wizard page above.



Hyper-V Selection for Inclusion

Hyper-V Node: myHyperVstandalone

Select Location

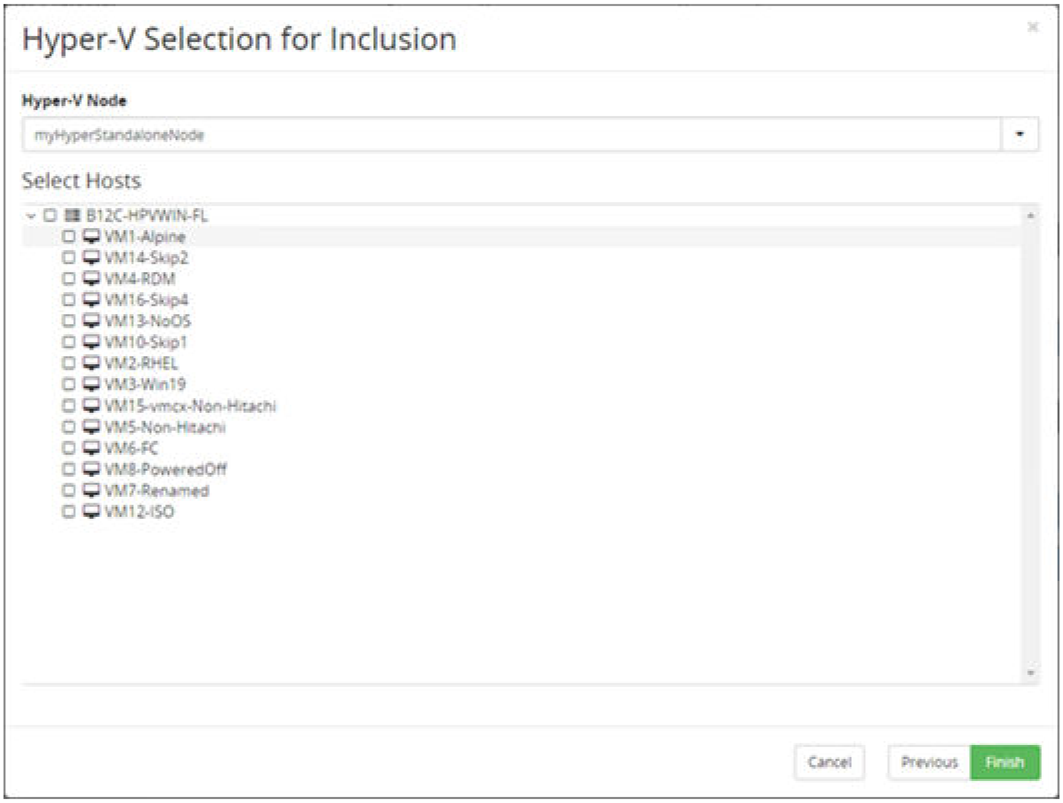
Figure 11 Hyper-VM - Browse by Virtual Machine Locations

Control	Description
Hyper-V Node	Select the Hyper-V app node you want to select paths from.
Location	Select one or more paths. Protector will search for virtual machines under the defined path at the beginning of each backup.

Control	Description
	Note: ▪ A virtual machine will only be selected for a backup if the virtual machine configuration is located under the specified path. If any included VMs utilize additional paths, these will be added as to the backup as well. This ensures that backed up virtual machines can be fully restored. ▪ For clustered Hyper-V nodes it is only possible to select paths which are located on cluster shared volumes, as only these paths are available on all nodes

Hyper-V Resource Selection Wizard – Browse by Virtual Machine Hosts

This page of the wizard is displayed when the browse by virtual machine host option is selected in the initial wizard page above.



Hyper-V Selection for Inclusion

Hyper-V Node

myHyperStandaloneNode

Select Hosts

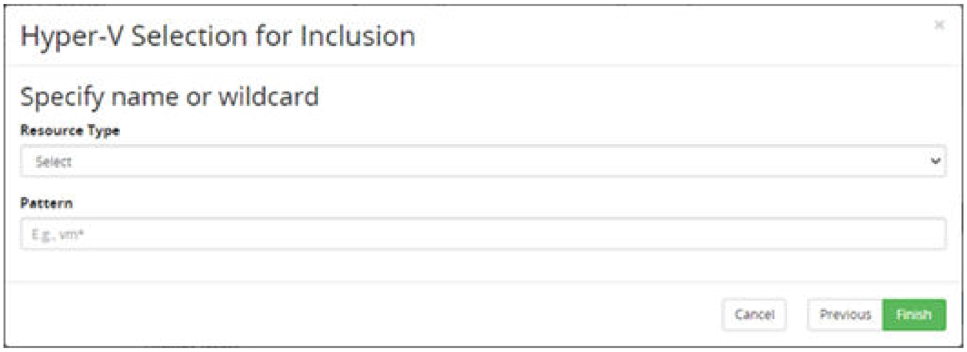
- □ B12C-HPVWIN-FL
  - □ VM1-Alpine
  - □ VM14-Skip2
  - □ VM4-RDM
  - □ VM16-Skip4
  - □ VM13-NoOS
  - □ VM10-Skip1
  - □ VM2-RHEL
  - □ VM3-Win19
  - □ VM15-vmcx-Non-Hitachi
  - □ VM5-Non-Hitachi
  - □ VM6-FC
  - □ VM8-PoweredOff
  - □ VM7-Renamed
  - □ VM12-ISO

Figure 12 Hyper-V VM Selection - Browse by Virtual Machine Hosts

Control	Description
Hyper-V Node	Select the Hyper-V app node you want to select hosts or VMs from.
Hosts	Select either individual virtual machines or complete hosts. In case a host is selected, Protector will determine the list of VMs available on the host at the beginning of the backup.

Hyper-V Resource Selection Wizard – Pattern search

This page of the wizard is displayed when the pattern search option is selected in the initial wizard page above.



Hyper-V Selection for Inclusion

Specify name or wildcard

Figure 13 Hyper-V Resource Selection Wizard – Pattern search

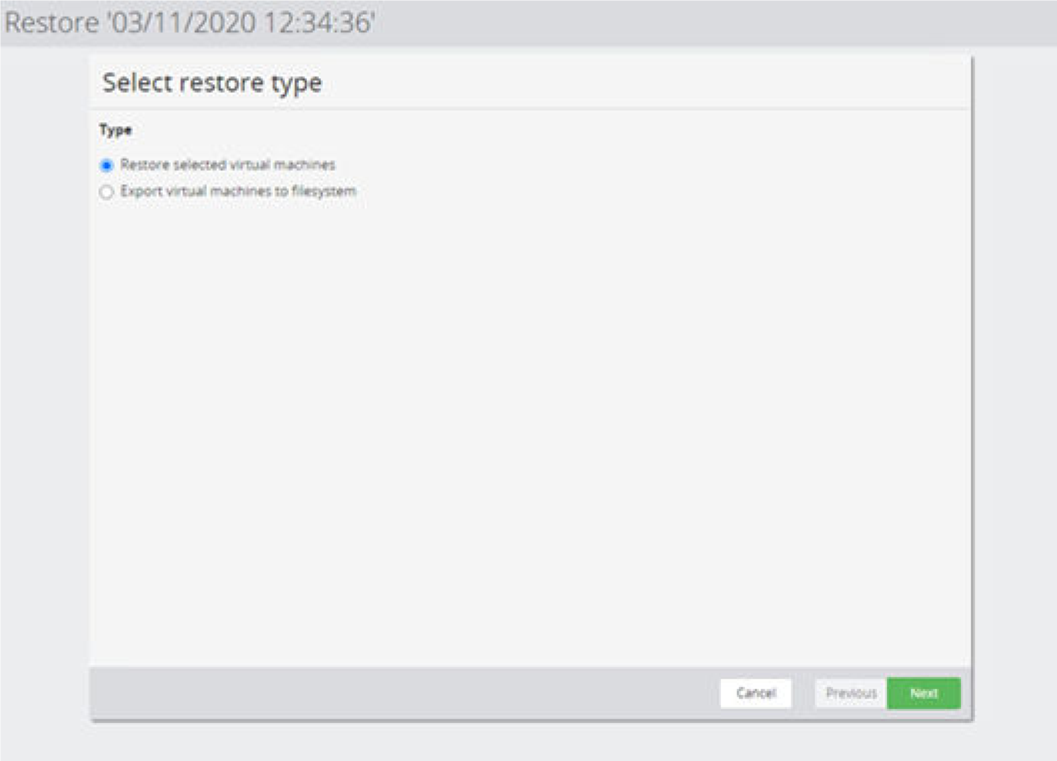
Control	Description
Resource Type	Select a Hyper-V resource type, that will be matched by the provided name pattern. Available options: ▪ Virtual Machine ▪ Virtual Machine Location (Path) ▪ Virtual Machine Host
Pattern	Enter a case insensitive pattern that will be used to match the resource type by name. The '?' character matches any single character, while the '*' character can be used to match any sequence of characters. E.g.: `IH_*` would match any resource of the given type whose name begins `IH_`. **Note:** Resources are re-evaluated against the name pattern every time the policy is executed. New resources having a name that matches this pattern, added after the policy is activated, will be automatically included in the backup.

Restore UI Reference

This section describes the Restore UI pertaining to Hyper-V backups.

Hyper-V Restore Wizard

This wizard is displayed when you restore a Hyper-V snapshot from a Hitachi Block device.



Restore '03/11/2020 12:34:36'

Select restore type

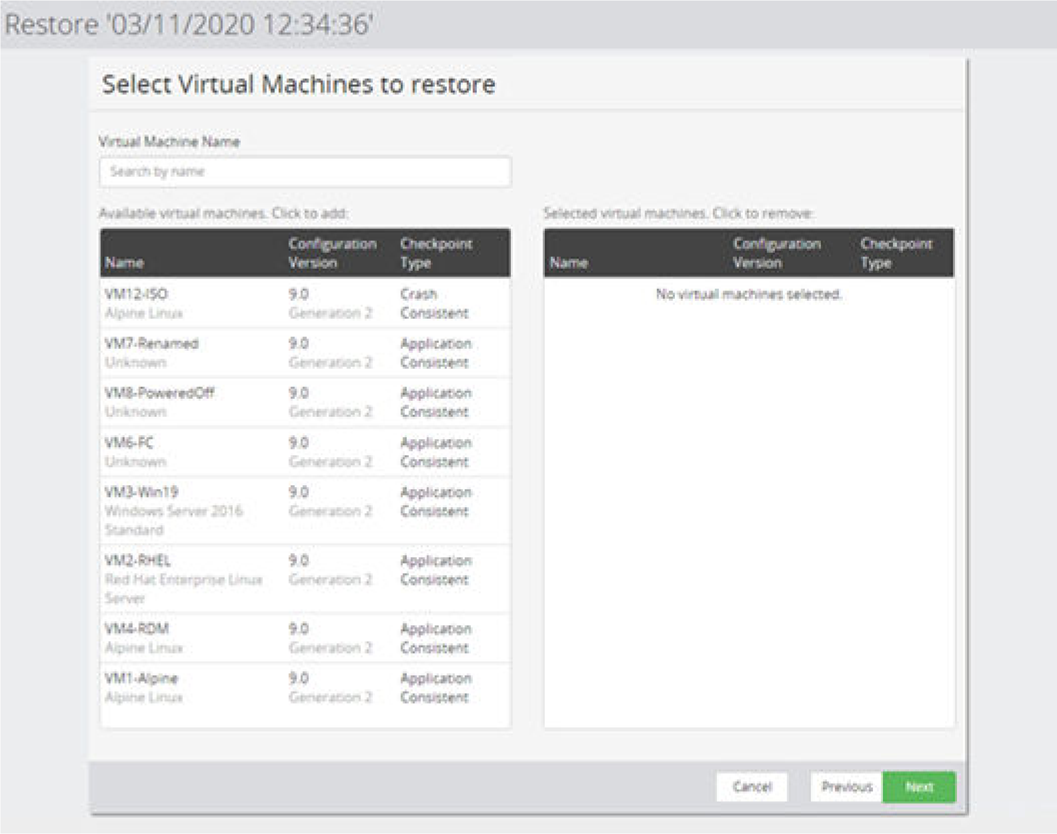
Type

● Restore selected virtual machines

○ Export virtual machines to filesystem

Figure 14 Restore Hyper-V Snapshot Wizard - Select Restore Scope

Control	Description
Restore selected virtual machines	One or more virtual machines from backup will be restored as virtual machines and registered with Hyper-V.
Export virtual machines to filesystem	One or more virtual machines from backup will be exported to the filesystem. The exported files will not be registered with Hyper-V.



Restore '03/11/2020 12:34:36'

Select Virtual Machines to restore

Virtual Machine Name

Search by name

Available virtual machines. Click to add:

Name	Configuration Version	Checkpoint Type
VM12-ISO Alpine Linux	9.0 Generation 2	Crash Consistent
VM7-Renamed Unknown	9.0 Generation 2	Application Consistent
VM8-PoweredOff Unknown	9.0 Generation 2	Application Consistent
VM6-FC Unknown	9.0 Generation 2	Application Consistent
VM3-Win19 Windows Server 2016 Standard	9.0 Generation 2	Application Consistent
VM2-RHEL Red Hat Enterprise Linux Server	9.0 Generation 2	Application Consistent
VM4-RDM Alpine Linux	9.0 Generation 2	Application Consistent
VM1-Alpine Alpine Linux	9.0 Generation 2	Application Consistent

Selected virtual machines. Click to remove:

Name	Configuration Version	Checkpoint Type

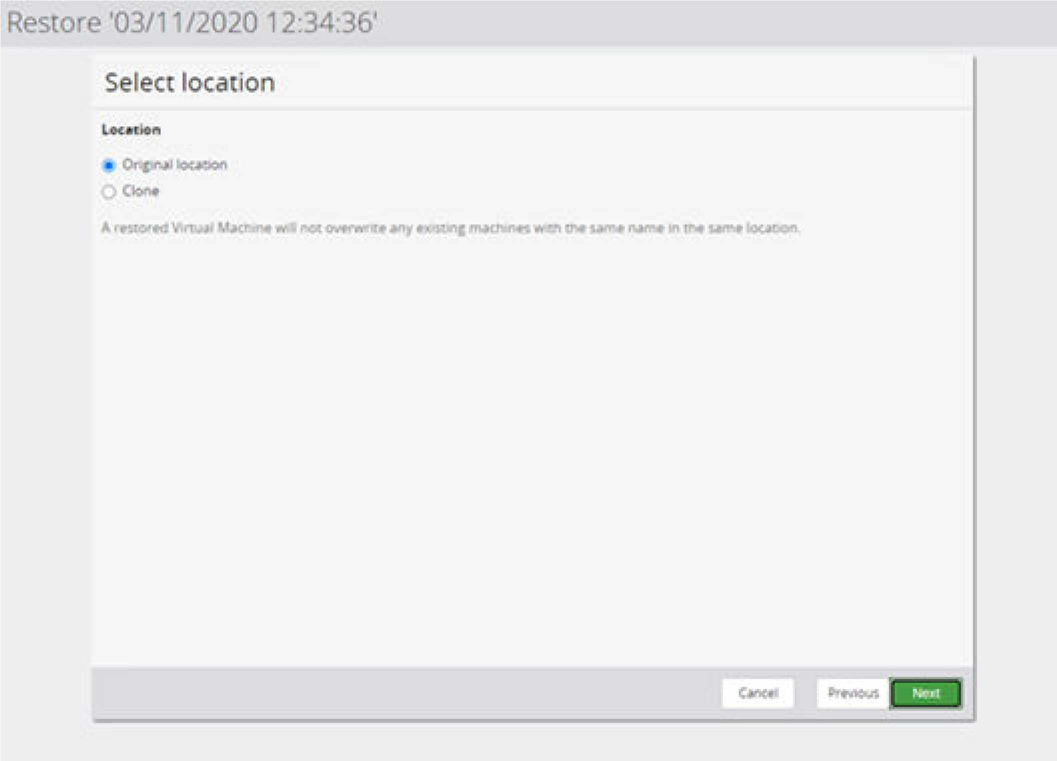
No virtual machines selected.

Figure 15 Restore Hyper-V Snapshot Wizard - Select VMs to Restore

Control	Description
Virtual Machine Name	Enter part of a virtual machine name to filter the list of available virtual machines.
Available VMs (left)	Select the VMs for the restore. Selected virtual machines will be removed from the list of available VMs and added to the list of selected virtual machines.
Selected VMs (right)	Lists the virtual machines which are selected for restore. Clicking on a selected VM will move it back to the list of available virtual machines.

Hyper-V Restore Wizard - Restore location

This page of the wizard is displayed when the "Restore selected virtual machines" option was selected on the initial page of the wizard above.



Restore '03/11/2020 12:34:36'

Select location

Location

● Original location

○ Clone

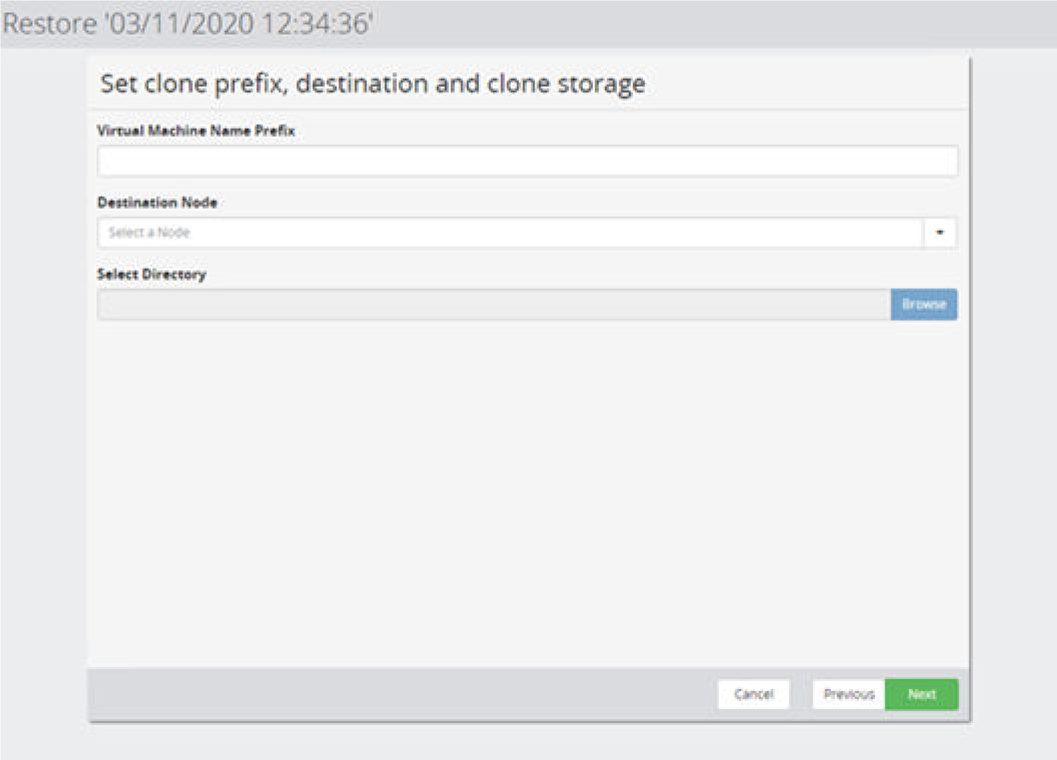
A restored Virtual Machine will not overwrite any existing machines with the same name in the same location.

Figure 16 Restore Hyper-V Snapshot Wizard - Select Location

Control	Description
Original Location	This will restore the virtual machine to the source Hyper-V node and to the original path. **Note:** If the original VM still exists, or the path is still in use the virtual machine will not be restored to avoid issues with the existing VM. Use clone restore to restore the virtual machine to an alternate location. **Caution:** While virtual machines are restored to the original location, the restored VM will have a new ID. Due to this it may no longer be included in backups if the VM was explicitly selected for backup.
Clone	This will restore the virtual machine to a selected Hyper-V node and location. The virtual machine name will be prefixed to avoid naming conflicts.

Hyper-V Restore Wizard – Set Clone prefix and destination

This wizard page is only displayed if a clone restore was requested in the Hyper-V Restore Wizard - Restore location (on page 39) page.



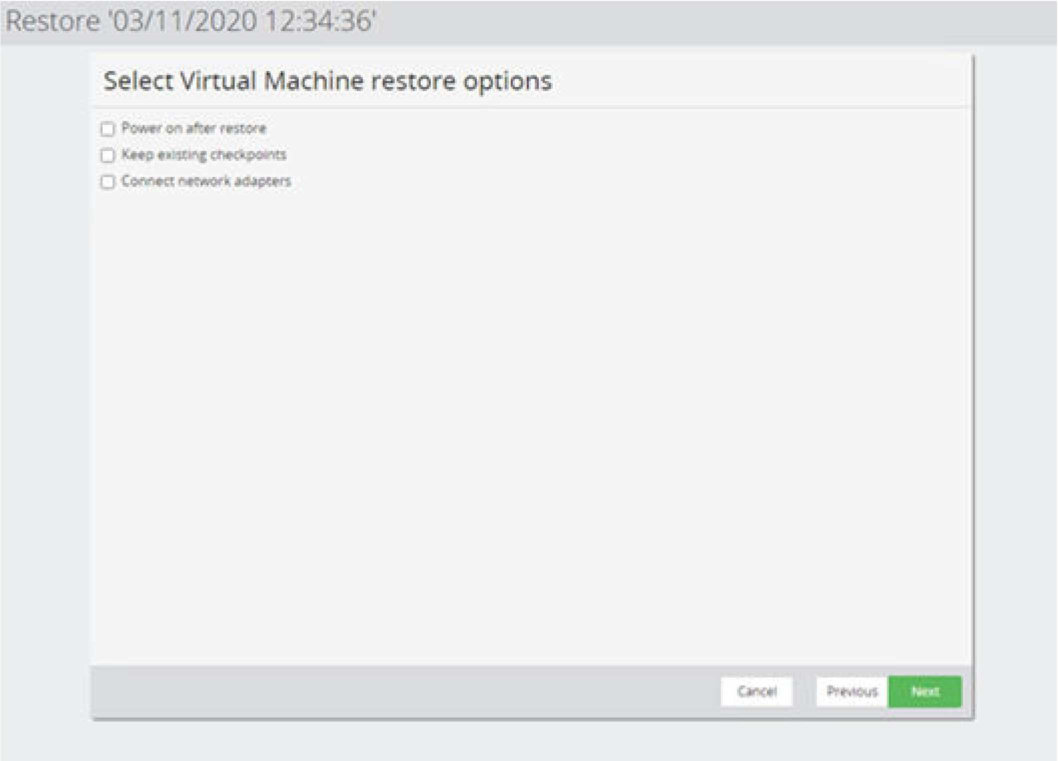
Restore '03/11/2020 12:34:36'

Set clone prefix, destination and clone storage

Figure 17 Restore Hyper-V Snapshot Wizard - Clone Prefix and Destination

Control	Description
Virtual Machine Name Prefix	Enter the VM name prefix which will be used when restoring the virtual machines.
Destination Node	Select the destination Hyper-V node the VM should be restored to.
Directory	Select the destination directory the virtual machines should be restored to. A sub directory will be created for each individual virtual machine. **Note:** For clustered Hyper-V nodes it is only possible to select paths which are located on cluster shared volumes, as only these paths are available on all nodes

Hyper-V Restore Wizard – Virtual Machine restore options



Restore '03/11/2020 12:34:36'

Select Virtual Machine restore options

□ Power on after restore

□ Keep existing checkpoints

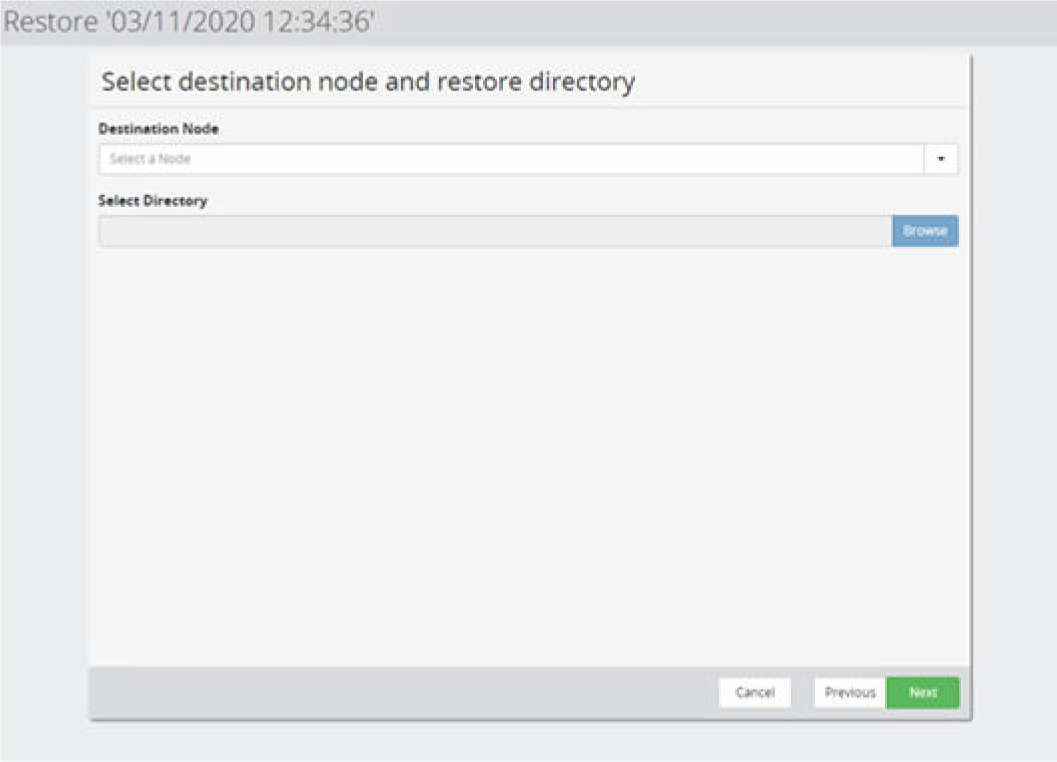
□ Connect network adapters

Figure 18 Restore Hyper-V Snapshot Wizard - Virtual Machine restore options

Control	Description
Power on after restore	The virtual machine will be powered on after the restore. **Note:** If this is selected and a cascaded mount is used, the virtual machine will be powered on and made available while the data copy continues in the background.
Keep existing checkpoints	If selected VM checkpoints created before the backup will be retained.
Connect network adapters	Select if the network cards should be connected after the restore. **Tip:** Do not select this if you are restoring to a Hyper-V node which uses different networks than the source. **Caution:** Selecting this option may cause IP address conflicts if the original virtual machine is up and connected to the network.

Hyper-V Restore Wizard – Export destination node and directory

This wizard page is only displayed if the user selected to export the virtual machines to filesystem.



Restore '03/11/2020 12:34:36'

Select destination node and restore directory

Destination Node

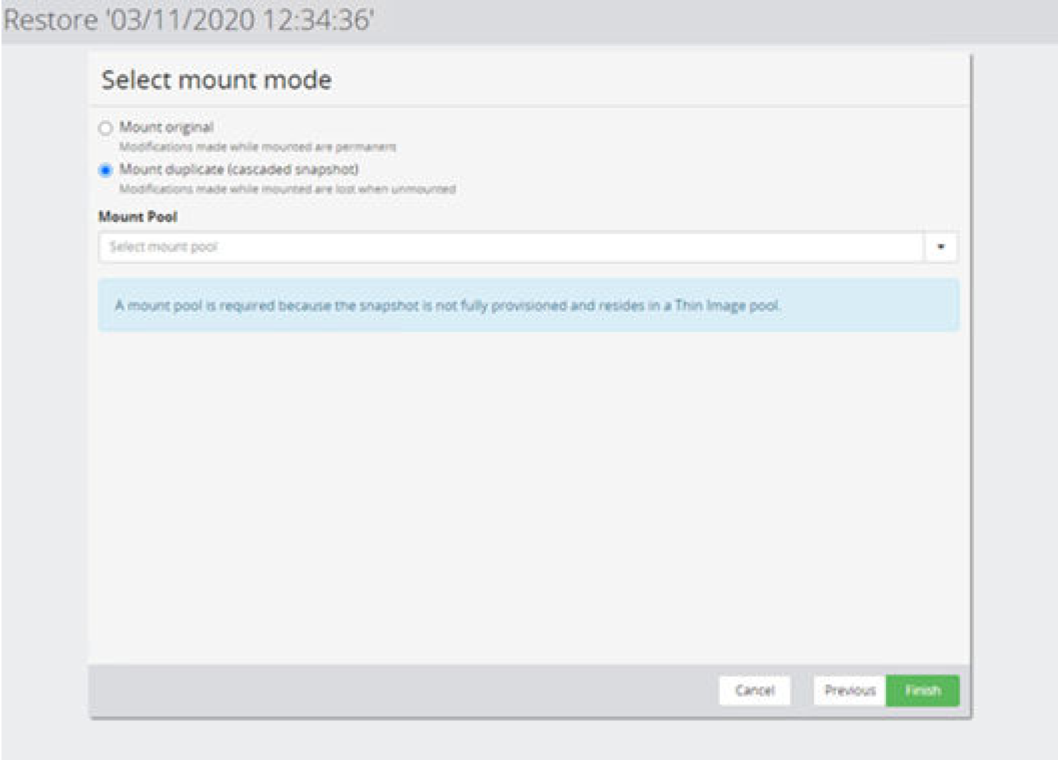
Select a Node

Select Directory

Figure 19 Restore Hyper-V Snapshot Wizard - Select Destination Node and Restore Directory

Control	Description
Destination Node	Select the Hyper-V node where you want to export the virtual machines to.
Directory	Enter the directory on the Hyper-V node you want to store the virtual machines in. A sub directory will be created for every virtual machine.

Hyper-V Restore Wizard – Select Mount Mode



Restore '03/11/2020 12:34:36'

Select mount mode

○ Mount original
Modifications made while mounted are permanent

● Mount duplicate (cascaded snapshot)
Modifications made while mounted are lost when unmounted

Mount Pool
Select mount pool

A mount pool is required because the snapshot is not fully provisioned and resides in a Thin Image pool.

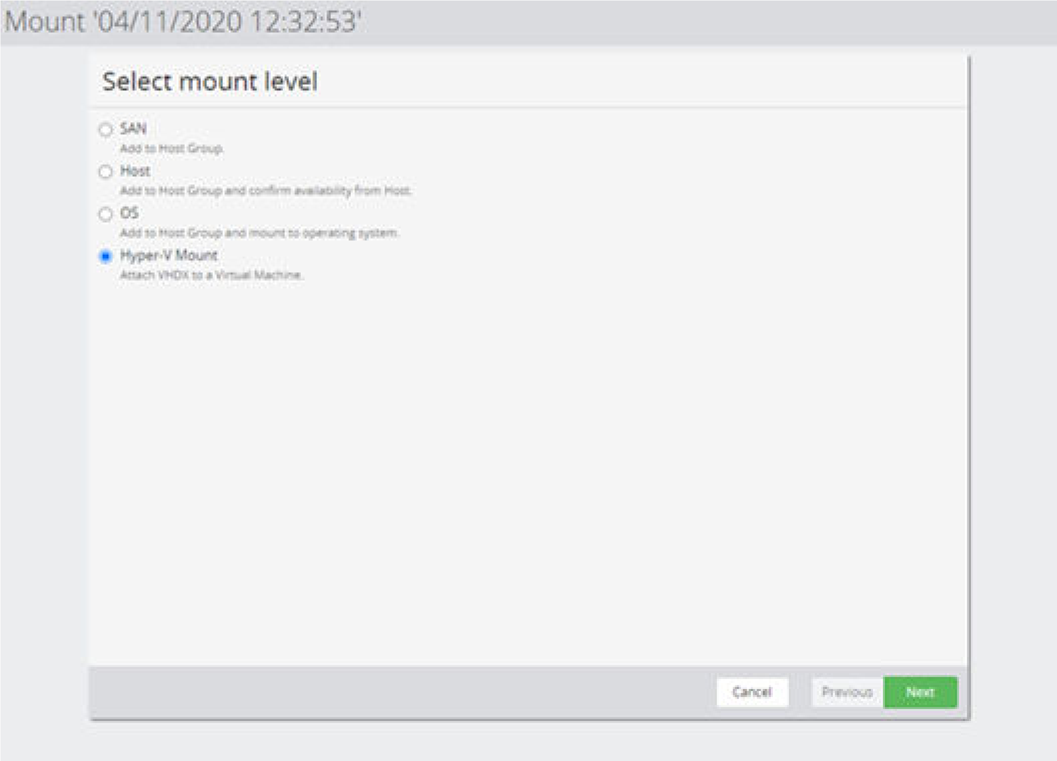
Figure 20 Restore Hyper-V Snapshot Wizard - Select Mount Mode

Control	Description
Mount Original	Mounts the original (Level 1) snapshot and copies the virtual machine data to the target location. **Tip:** When this option is used virtual machines will always be copied before they are registered with Hyper-V. Virtual machines will also only powered on once the copy is complete. **Caution:** This option will expose your original backup to the Hyper-V host. Any changes will persist even after the unmount. While Protector will not perform any changes, nothing is preventing users or other processes from modifying the data.
Mount duplicate (cascaded snapshot)	Only enabled if the original (Level 1) snapshot was created in cascade mode. Mounts a copy of the original snapshot (i.e. a Level 2 snapshot). **Note:** When this option is used with in combination with the „Power on VM“ option, the VM can be used while the data is copied in the background (via Hyper-V storage migration).

Control	Description
Mount Pool	Not available for replications. Depending on the parameters specified for the snapshot operation on the data flow, a mount pool might be required. A message is displayed in a blue rectangle to explain if and why a mount pool is required.

Hyper-V Mount Wizard

This wizard is displayed when you mount a Hyper-V snapshot or replication from a Hitachi Block device.



Mount '04/11/2020 12:32:53'

Select mount level

○ SAN
Add to Host Group.

○ Host
Add to Host Group and confirm availability from Host.

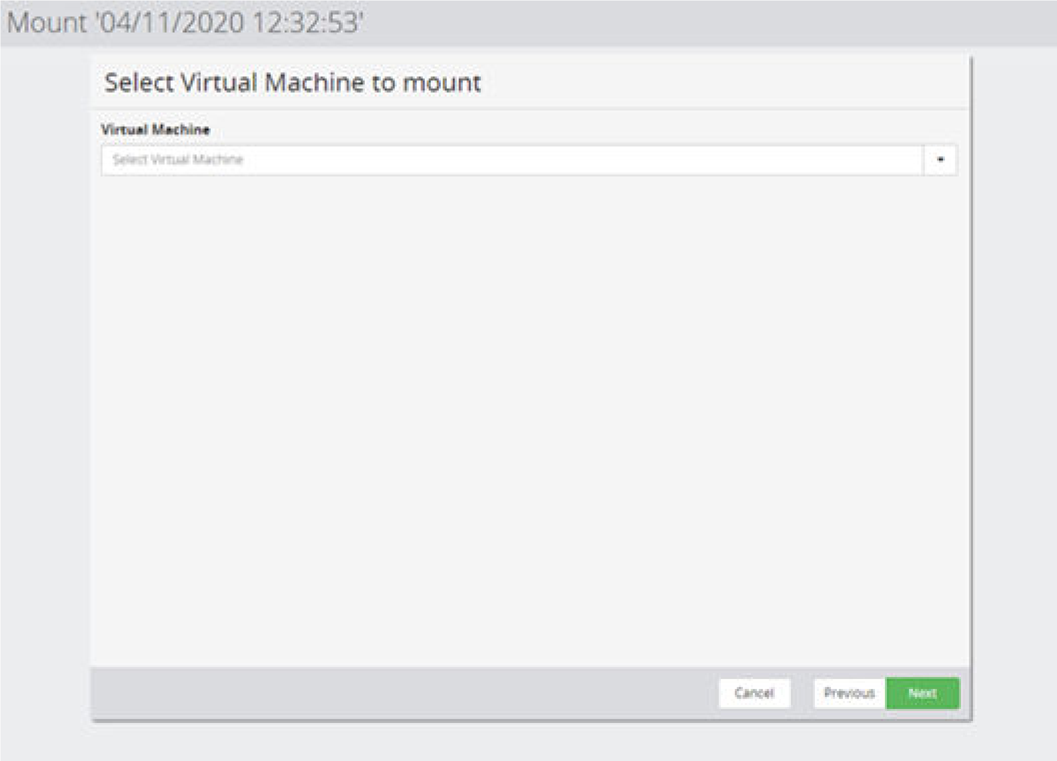
○ OS
Add to Host Group and mount to operating system.

● Hyper-V Mount
Attach VHDX to a Virtual Machine.

Figure 21 Snapshot Mount Wizard - Select Mount Level

Control	Description
SAN	Adds the snapshot or replication to a Host Group.
Host	Adds the snapshot or replication to a Host Group and confirms that it is available from the specified Host.
OS	Adds the snapshot or replication to a Host Group and mounts it on the specified Host's operating system.

Control	Description
Hyper-V Mount	Attaches all virtual disks of a selected VM on the snapshot to a virtual machine on the target node.



Mount '04/11/2020 12:32:53'

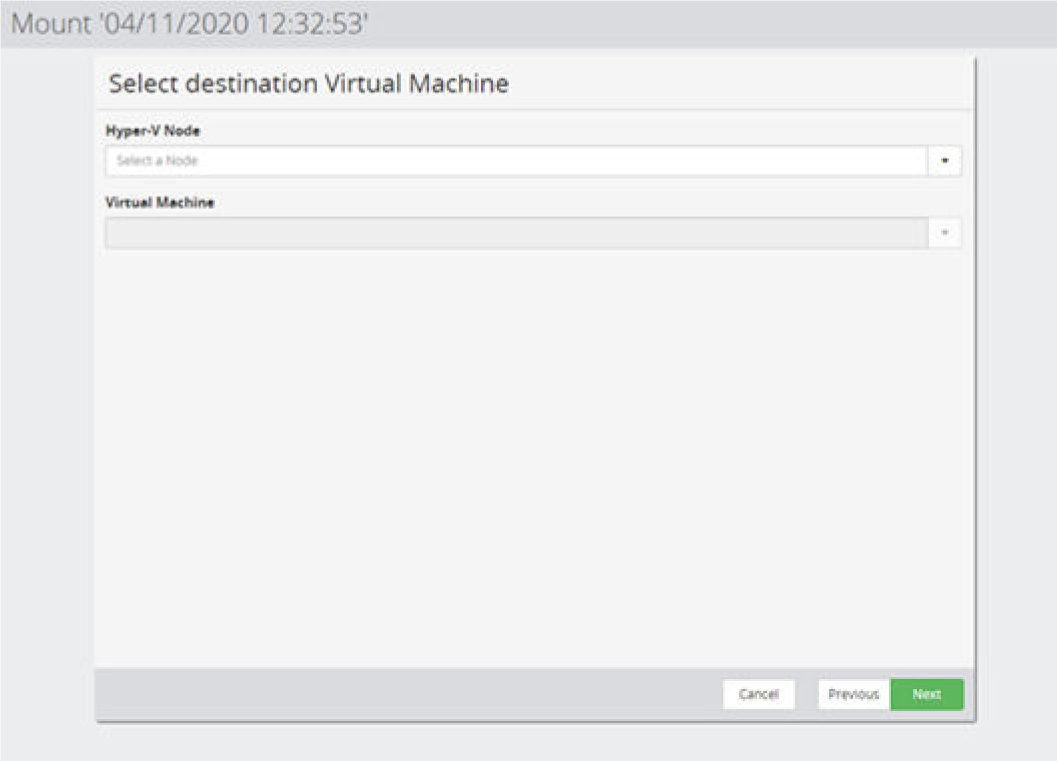
Select Virtual Machine to mount

Virtual Machine

Select Virtual Machine

Figure 22 Mount Hyper-V Wizard - Select Virtual Machine to Mount

Control	Description
Virtual Machine	Select the specific VM within this snapshot that is to have its disks mounted.



Mount '04/11/2020 12:32:53'

Select destination Virtual Machine

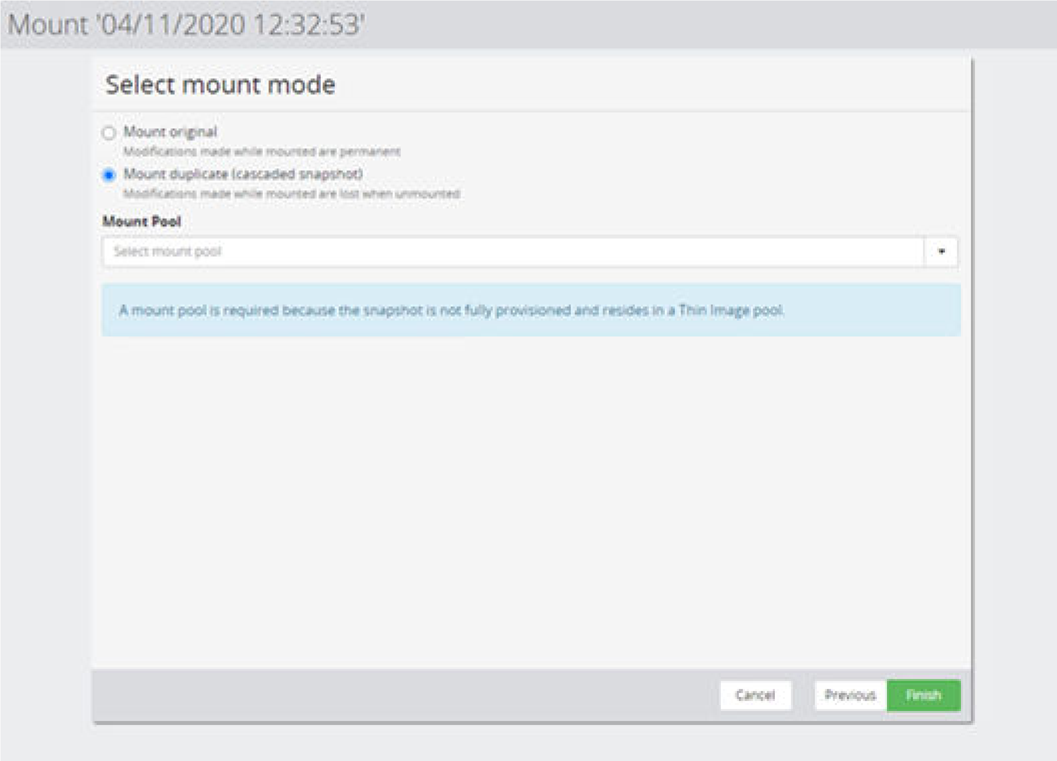
Hyper-V Node

Select a Node

Virtual Machine

Figure 23 Mount Hyper-V Wizard - Select Virtual Machine

Control	Description
Hyper-V Node	Select the Hyper-V node where the VM’s disks will be mounted.
Virtual Machine	Select the target virtual machine the disks will be attached to.



Mount '04/11/2020 12:32:53'

Select mount mode

○ Mount original
Modifications made while mounted are permanent

● Mount duplicate (cascaded snapshot)
Modifications made while mounted are lost when unmounted

Mount Pool

Select mount pool

A mount pool is required because the snapshot is not fully provisioned and resides in a Thin Image pool.

Figure 24 Mount Hyper-V Wizard - Select Mount Mode

Control	Description
Mount Original	Mounts the original (Level 1) snapshot and copies the virtual machine data to the target location. ⚠ **Caution:** This option will expose your original backup to the Hyper-V host. Any changes made to the virtual disks or the data on the snapshot will persist after unmount.
Mount duplicate (cascaded snapshot)	Only enabled if the original (Level 1) snapshot was created in cascade mode. Mounts a copy of the original snapshot (i.e. a Level 2 snapshot). ⚠ **Caution:** Any changes made to the virtual disks will be lost when they are unmounted.
Mount Pool	Not available for replications. Depending on the parameters specified for the snapshot operation on the data flow, a mount pool might be required. A message is displayed in a blue rectangle to explain if and why a mount pool is required.

Chapter 5: Troubleshooting

This chapter provides guidelines for how to troubleshoot issues that might occur when using Ops Center Protector.

Troubleshooting Hyper-V

This section provides guidelines for how to troubleshoot issues that might occur when using Hyper-V.

A virtual machine is not included in a backup.

Problem:

When performing a backup, it does not include a virtual machine. Protector does not report any errors for the virtual machine during the backup job.

Solution:

The Hyper-V classification does most likely not include this virtual machine.

Review and update the Hyper-V classification of the policy. Use the preview functionality for a list of VMs included by the policy.

A virtual machine is no longer included in backups after it has been restored.

Problem:

A virtual machine has been restored, now it is no longer included in backups.

Cause:

When selecting a virtual machine explicitly (via browse) in a Hyper-V classification, Protector will refer to this VM via its ID. Restoring a virtual machine assigns a new ID to the restored VM. As the classification still refers to the original ID, the restored VM will not be included in the backup.

Solution:

Update the Hyper-V classification to include the restored VM and re-activate the data flow.

Restore to original fails stating the node does longer exists

Problem:

When you try to restore to the original, an error is displayed, indicating that the node no longer exists.

Solution:

Perform a clone restore instead

Restore to Hyper-V cluster fails as virtual machine already exist

Problem:

Restoring a virtual machine to a Hyper-V cluster fails, stating that the virtual machine already exists, however, Hyper-V Manager does not list the VM.

Cause:

This is usually caused by a partially deleted VM. In case of a clustered Hyper-V there is the virtual machine and an associated cluster role. When the virtual machine is deleted via the Microsoft's Failover Cluster Manager or SCVMM both the VM And the role are deleted. However, if the virtual machine is deleted via PowerShell or Hyper-V Manager the cluster role may remain.

Solution:

Ensure both the virtual machine and the associated cluster role are deleted, before you re-try the restore.

Verification of Hyper-V credential fails

Problem:

When creating or editing a Hyper-V node the provided credentials are rejected.

Solution:

double check you provided the correct domain, user, and password

verify Hyper-V and WMI services are running on all nodes, which are part of the Hyper-V setup

In case of a clustered Hyper-V environment, verify the cluster service is running on all nodes

Virtual FC adapters, pass through disks or mapped ISOs are missing after a restore

Problem:

After restoring the virtual machine, it does no longer contain virtual fibre channel adapters, mapping to pass through disks or mappings to ISOs.

Solution:

It is currently not possible to protect or restore these connections to external resources. Use your Hyper-V management tool to re-add them.

VM is skipped during backup because config version is too small

Problem:

During a backup job, a virtual machine is skipped. The associated error message shows that the configuration version is too low.

Solution:

Use the Microsoft’s Hyper-V Manager or PowerShell to upgrade the virtual machine version. See https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/upgrade-virtual-machine-version-in-hyper-v-on-windows-or-windows-server for additional guidance.

Glossary

Archive

A copy that is created for long-term retention.

Asynchronous journalling

Transactions are written to disk and also placed in a journal log file, to protect against data loss in the event of a system failure. Transactions from the log file are sent to the destination machine.

Asynchronous replication

Transactions are held in memory before being sent over the network. If the network is unavailable then transactions are written to disk and sent to the destination machine when the connection is re-established. Asynchronous replication is optimal for connections with sporadic efficiency.

Backup

A copy that is created for operational and disaster recovery.

Bandwidth throttling

Used to control when and what proportion of available network bandwidth is used by Ops Center Protector for replication.

Batch backup

A process by which the repository is updated periodically using scheduled resynchronizations. This method involves a scan of the source machine's file system, but only the changed bytes are transferred and stored. This method is useful for data that does not change often, such as data contained on the operating system disk. Linux based source nodes are only able to perform batch backups.

Clone

An operation where a copy of the database is created in another storage location in a local or remote site.

Continuous Data Protection (CDP)

A method of capturing the state of a file system in near real time. CDP shares much of the functionality of Live Backup, except that RPO is measured in minutes, data is retained for a much shorter period of time and is not indexed by the MDS. Typically, CDP and Live Backup are used in conjunction. CDP is only supported on source nodes running the Microsoft Windows operating system.

Data flow

Identifies the data sources, movers and destinations participating in a backup, along with interconnection paths between them. Policies are assigned to each node to determine what type of data is backed up.

Data source

A machine hosting a file system or application where the Protector client software is installed.

Deduplication

A method of reducing the amount of storage space that your organization requires, to archive data, by replacing multiple instances of identical data with references to a single instance of that data.

Destination node

A machine that is capable of receiving data for the purposes of archiving. This machine might be the Ops Center Protector Repository or Block device.

License key

A unique, alphanumeric code that is associated with the unique machine ID that is generated during the Ops Center Protector installation. The license key must be activated in order to use the software.

Live backup

A backup technique that avoids the need for bulk data transfers by continuously updating the repository with changes to the source file system. This is similar to CDP but with longer retention periods and RPOs being available. Live backups perform byte level change updates whereas batch backups perform block level change updates.

Master node

The machine that controls the actions of other nodes within the Ops Center Protector network.

Metadata Store (MDS)

Records metadata that describes items that are held in repositories. The MDS supports indexing of stored data, thus enabling fast searches when locating data for restoration.

Mover

Defines the type of data movement operation to be performed between source and destination nodes, during the creation of a data flow. Batch movers perform block level data transfers on a scheduled basis, whereas continuous movers perform byte level data transfers on a near-continuous basis.

Node Group

Multiple machines of the same type can be assigned to one or more node groups. Within the Data Flow page, you can assign policies to nodes within node groups en-mass.

Policy

A configurable data protection objective that is mapped to machines or groups, and to the data management agents that implement the policy. Multiple policies can be assigned to a single node.

Recovery Point Objective (RPO)

The frequency at which a backup will occur. This governs the point in time to which data can be recovered should a restore be needed.

Replication

An operation where a copy of the data is created in another local or remote location automatically.

Repository

A destination node that stores data from one or more source nodes. The Ops Center Protector Repository supports batch backup, archiving, and versioning policies.

Snapshot (Thin Image)

A point in time copy of the data that is based on references to the original data.

Source node

Any node (server, workstation or virtual machine) that hosts data to be protected by Ops Center Protector. The source node has an Active Data Change Agent, which is responsible for monitoring the host file system and performing the relevant actions defined by the policies. Nodes need to be configured as a source node if they need to transfer locally stored data to a destination node, or implement data tracking, blocking and auditing functions. A node can be both a source and destination simultaneously.

Synchronous replication

Transactions are transferred to the remote storage device immediately and the write operation is signaled as completed only once data is confirmed as written to both primary and secondary volumes. Synchronous replication is optimal for connections with high efficiency.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1,000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1,000^3$ bytes
1 terabyte (TB)	1,000 GB or $1,000^4$ bytes
1 petabyte (PB)	1,000 TB or $1,000^5$ bytes
1 exabyte (EB)	1,000 PB or $1,000^6$ bytes

Logical capacity values (for example, logical device capacity, cache memory capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact