Veeam Backup & Replication

Version 12

Integration with Storage Systems Guide

August, 2023

NOTE

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

Contacting Veeam Software

At Veeam Software we value feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up-to-date information about company contacts and office locations, visit the Veeam Contacts Webpage.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: veeam.com/documentation-guides-datasheets.html
- Veeam R&D Forums: forums.veeam.com

About This Document

This user guide provides information about integration, main features, and use of Veeam Backup & Replication with storage systems. The document applies to version 9.5 Update 4 and all subsequent versions until it is replaced with a new edition.

Intended Audience

The user guide is intended for anyone who wants to build the data protection and disaster recovery strategy using Veeam Backup & Replication and storage systems that host VM disks. It is primarily aimed at backup administrators, consultants, analysts and any other IT professionals using the product.

Storage System Snapshot Integration

Veeam Backup & Replication allows you to back up VMware vSphere VMs by creating snapshots of storage volumes where the VMs reside and using the snapshots as data source for the backup.

In VMware vSphere environment, Veeam Backup & Replication offers the following options:

- VMware integration
- NAS integration
- Veeam Agent for Microsoft Windows integration

Veeam Backup & Replication allows you to add storage systems to the backup infrastructure, create snapshots of the storage volumes where the VMs reside and then use the snapshots as data source for backups.

> **IMPORTANT**
>
> You cannot back up Hyper-V-based VMs with the help of the integration. Instead, you can add to the backup infrastructure the storage systems whose volumes host backup data and use the capabilities of NAS or Veeam Agent for Microsoft Windows.

In the Hyper-V environment, Veeam Backup & Replication offers the following options:

- Veeam Agent for Microsoft Windows integration which allows you to use Volume Shadow Copy Service (VSS) and capabilities of native snapshots to create backups.
- NAS integration which allows you to add storage systems as NAS filers and create storage snapshots of volumes with NAS file shares.

Before you start working with storage systems in Veeam Backup & Replication, you must properly configure the backup infrastructure. For more information on configuring the backup infrastructure, see Backup Infrastructure for Storage Integration.

Check the prerequisites for a specific storage systems before you add a storage system to your backup infrastructure. For more information on storage requirements and limitations, see Requirements and Limitations.

VMware Integration

To build the data protection and disaster recovery strategy, you can use the capabilities of native snapshots created on production storage systems that host VM disks.

- Backup from Storage Snapshots. You can use storage snapshots to create backups and replicas of VMware vSphere VMs hosted on storage systems. Backup from Storage Snapshots speeds up backup and replication operations and reduces the impact of VMware vSphere snapshot removal on the production environment.
- Data Recovery from Storage Snapshots. You can restore VM data directly from storage snapshots. Restore from Storage Snapshots automates the process of VM data recovery and reduces recovery time in 10 times or more.
- Snapshot Orchestration. You can configure backup jobs to periodically create storage snapshots on primary or secondary storage arrays.
- Backup from Storage Snapshots with Snapshot Retention. You can configure backup jobs to create backup files in the backup repository and, additionally, storage snapshots on the primary or secondary storage arrays.
- On-Demand Sandbox for Storage Snapshots. You can start VMs whose disks are hosted on storage systems in the On-Demand Sandbox. On-Demand Sandbox can be used for testing, training, troubleshooting and so on.

To start working with storage systems, you must properly configure the backup infrastructure. For more information, see Backup Infrastructure for Storage Snapshots. After that, you can use storage snapshots for data protection and disaster recovery operations.

Depending on the storage system type, you can perform the following operations:

Operation/ Storage Type	Dell Unity XT/Unity, VNX(e)	HPE 3PAR StoreServ, HPE Primera, HPE Alletra 9000	HPE StoreVirtual / LeftHand / P4000 series	HPE Nimble, HPE Alletra 6000, HPE Alletra 5000	NetApp ONTAP, FAS/AFF/ASA, FlexArray (V-Series), Fujitsu ETERNUS HX/AX, IBM N series, Lenovo ThinkSystem DM Series	Cisco HyperFlex	IBM FlashSystem (StorWize), IBM SVC, Lenovo Storage V Series	Universal Storage API Integrated Systems
Backup from Storage Snapshots								
Backup from primary storage arrays	✓	✓	✓	✓	✓	✓	✓	✓

Operation/ Storage Type	Dell Unity XT/Unity, VNX(e)	HPE 3PAR StoreServ, HPE Primera, HPE Alletra 9000	HPE StoreVirtual / LeftHand / P4000 series	HPE Nimble, HPE Alletra 6000, HPE Alletra 5000	NetApp ONTAP, FAS/AFF/ASA, FlexArray (V-Series), Fujitsu ETERNUS HX/AX, IBM N series, Lenovo ThinkSystem DM Series	Cisco HyperFlex	IBM FlashSystem (StorWize), IBM SVC, Lenovo Storage V Series	Universal Storage API Integrated Systems
Backup from secondary storage arrays	×	✓[1]	×	✓[1]	✓[1]	×	✓[1]	✓[3]
Data Recovery from Storage Snapshots								
Restore from primary storage arrays	✓	✓	✓	✓	✓	×	✓	✓
Restore from secondary storage arrays	✓	✓	✓	✓	✓	×	✓	✓[3]
Snapshot Orchestration								
Snapshot-only job for primary storage arrays	×	✓	×	✓	✓	×	✓	✓

Operation/ Storage Type	Dell Unity XT/Unity, VNX(e)	HPE 3PAR StoreServ, HPE Primera, HPE Alletra 9000	HPE StoreVirtual / LeftHand / P4000 series	HPE Nimble, HPE Alletra 6000, HPE Alletra 5000	NetApp ONTAP, FAS/AFF/ASA, FlexArray (V-Series), Fujitsu ETERNUS HX/AX, IBM N series, Lenovo ThinkSystem DM Series	Cisco HyperFlex	IBM FlashSystem (StorWize), IBM SVC, Lenovo Storage V Series	Universal Storage API Integrated Systems
Snapshot-only job for secondary storage arrays	×	✓[1]	×	✓[1]	✓[1]	×	✓[1]	✓[3]
Backup from Storage Snapshots with Snapshot Retention								
Backup job with snapshot retention on primary storage arrays	×	✓	×	✓	✓	×	✓	✓
Backup job with snapshot retention on secondary storage arrays	×	✓[1]	×	✓[1]	✓[1]	×	✓[1]	✓[3]
Other Operations								
Storage rescan	✓	✓	✓	✓	✓	✓[2]	✓	✓

Operation/ Storage Type	Dell Unity XT/Unity, VNX(e)	HPE 3PAR StoreServ, HPE Primera, HPE Alletra 9000	HPE StoreVirtual / LeftHand / P4000 series	HPE Nimble, HPE Alletra 6000, HPE Alletra 5000	NetApp ONTAP, FAS/AFF/ASA, FlexArray (V-Series), Fujitsu ETERNUS HX/AX, IBM N series, Lenovo ThinkSystem DM Series	Cisco HyperFlex	IBM FlashSystem (StorWize), IBM SVC, Lenovo Storage V Series	Universal Storage API Integrated Systems
Snapshot creation and deletion (manual)	✓	✓	✓	✓	✓	×	✓	✓
Data retrieval from achived snapshots	×	×	×	×	×	×	×	✓[3]

[1] Replication feature:

- **HPE 3PAR StoreServ, HPE Primera, HPE Alletra 9000** – Remote Copy Periodic (Asynchronous) and Remote Copy Peer Persistence. For Remote Copy Peer Persistence, snapshots are created on the target volume only.
- **HPE Nimble, HPE Alletra 6000, HPE Alletra 5000** – Snapshot Replication and synchronous replication.
- **NetApp ONTAP, FAS, AFF, and ASA Series, FlexArray (V Series), Fujitsu ETERNUS HX/AX, IBM N series, and Lenovo ThinkSystem DM Series** – snapshot replication with SnapMirror/SnapVault.
- **IBM FlashSystem (StorWize), IBM SVC, Lenovo Storage V Series** – synchronous replication with MetroMirror or HyperSwap; snapshot transfer with Global Mirror.

[2] Infrastructure only.

[3] The following features are supported: **Pure Storage FlashArray** with ActiveCluster Replication, Replication (asynchronous) and Offload. To check compatibility and configuration of other storage systems, contact vendors.

Backup from Storage Snapshots

Backup from Storage Snapshots lets you speed up backup and replication for VMware vSphere VMs whose disks are hosted on storage systems. When you perform Backup from Storage Snapshots, Veeam Backup & Replication leverages storage snapshots for VM data processing. Backup from Storage Snapshots lets you reduce impact of backup and replication activities on the production environment and improve RPOs.

VM Data Processing

Veeam Backup & Replication supports an accelerated procedure of creating backups for VMs that host their disks on storage systems. This section describes differences between regular data processing and Backup from Storage Snapshots.

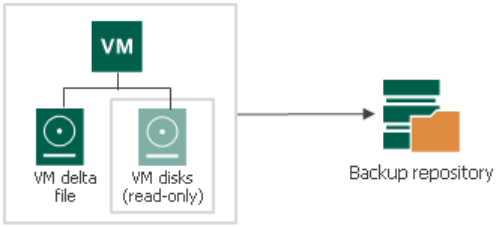
Regular VM Data Processing

In the regular processing course, Veeam Backup & Replication uses a VMware vSphere snapshot. The VMware vSphere snapshot "freezes" the VM state and data at a specific point in time. This way, the VM data is brought to a consistent state suitable for backup or replication.

During regular VM data processing, Veeam Backup & Replication performs the following actions:

1. Triggers a VMware vSphere snapshot for a VM. VM disks are put to the read-only state, and every virtual disk of the VM receives a delta file named like *vmname-00001.vmdk*.
2. Copies VM data from read-only disks of the VM. All changes that the user makes to the VM while backup or replication is performed are written to delta files.
3. When VM processing is finished, the VMware vSphere snapshot is committed. VM disks resume writes, and data from delta files is merged to the VM disks. After data is merged, the VMware vSphere snapshot is removed.

Regular VM data processing may take long. If backup or replication is performed for a VM running a highly transactional application, the delta file may grow large. The snapshot commit process will take much time, and the VM may hang up during this process. To overcome this situation, you can use Backup from Storage Snapshots.



Backup from Storage Snapshots

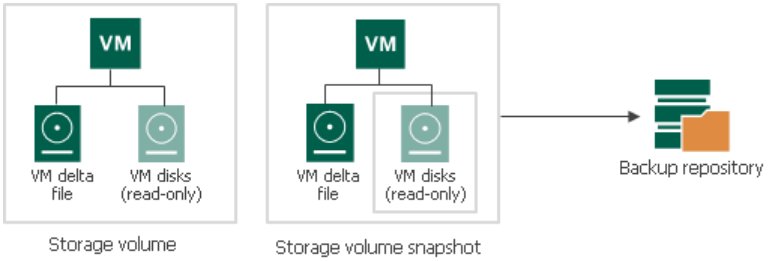
Backup from Storage Snapshots lets you speed up backup and replication operations. For Backup from Storage Snapshots, Veeam Backup & Replication complements the VMware vSphere snapshot technology with the storage snapshots technology, and uses storage snapshots as a source of data for backup and replication. These storage snapshots are temporary and are removed after backup or replication finishes.

During Backup from Storage Snapshots, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication triggers a VMware vSphere snapshot for VMs whose disks are hosted on the storage system.

2. Veeam Backup & Replication triggers a temporary storage snapshot of the volume or LUN hosting the VM itself and the created VMware vSphere snapshot.
3. The VMware vSphere VM snapshot on the original storage volume is deleted immediately after the temporary storage snapshot is created. Veeam Backup & Replication accesses the "cloned" VMware vSphere snapshot on the temporary storage snapshot and copies VM data from it.
4. When VM processing is finished, the temporary storage snapshot capturing the VMware vSphere snapshot is removed.

As a result, the VMware vSphere snapshot exists for a very short time, namely several seconds. Delta files do not grow large, and the time of VMware vSphere snapshot commit decreases.



Backup from Primary Storage Arrays

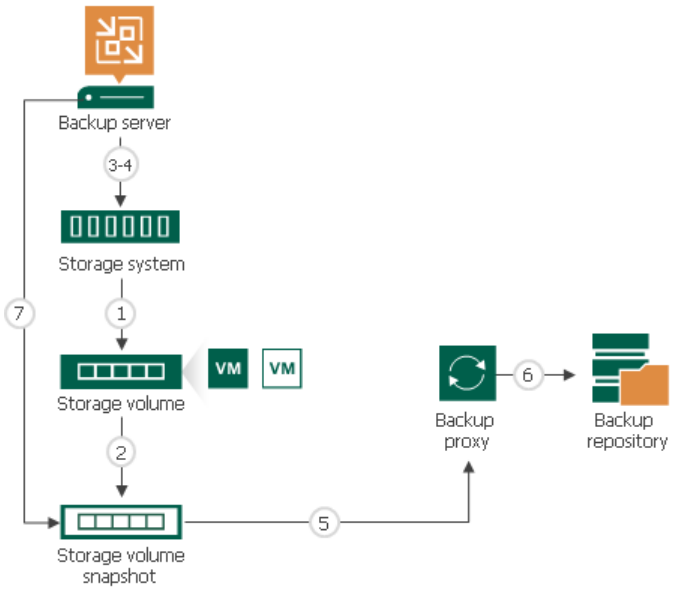
Backup from primary storage array allows you to use the Backup from Storage Snapshots feature and create backups from snapshots created on primary storage arrays.

How Backup from Primary Storage Works

When you run a job with Backup from Storage Snapshots enabled, Veeam Backup & Replication performs the following actions:

1. Analyzes which VMs in the job host their disks on the storage system. Checks the backup infrastructure and detects if there is a backup proxy that has a direct connection to the storage system.
2. Triggers the vCenter Server to create VMware vSphere snapshots for these VMs.
3. Gets Changed Block Tracking information for VMs hosted on the storage system.
4. Instructs the storage system to create a temporary snapshot of the storage volume or LUN that hosts VM disks and VMware vSphere snapshots.
5. Instructs the vCenter Server to remove VMware vSphere VM snapshots. The "cloned" VMware vSphere snapshots remain on the created temporary storage snapshots.
6. Mounts the temporary storage snapshot as a new volume to this backup proxy.
7. Reads and transports VM data blocks through the backup proxy to the backup repository. For incremental backup or replication, Veeam Backup & Replication uses obtained CBT data to retrieve only changed data blocks from the temporary storage snapshot.

8. When VM data processing is finished, Veeam Backup & Replication unmounts the temporary storage snapshot from the backup proxy and instructs the storage system to remove the temporary storage snapshot.



Mixed Job Scenarios

Backup from Storage Snapshots is used only for those VMs whose disks are hosted on supported storage systems. As backup and replication jobs typically process a number of VMs that may reside on different types of storage, Veeam Backup & Replication processes VMs in mixed jobs in the following way:

- If a job processes a number of VMs whose disks are hosted on different types of storage, Veeam Backup & Replication uses Backup from Storage Snapshots only for VMs whose disks are hosted on supported storage systems. Other VMs are processed in a regular manner.
- If a VM has several disks, some hosted on supported storage systems and some hosted on another type of storage, Veeam Backup & Replication does not use Backup from Storage Snapshots to such VM. All disks of such VM are processed in a regular manner.

During a job, Veeam Backup & Replication processes VMs residing on different types of storage at different time:

1. Veeam Backup & Replication first triggers VMware vSphere snapshots and storage snapshots for VMs hosted on supported storage systems.
2. After the storage snapshot is created, Veeam Backup & Replication triggers VMware vSphere snapshots for other VMs. These VMs are processed in the regular data processing mode further on, in parallel with VMs whose disks are hosted on supported storage systems.

Configuring Backup from Storage Snapshots

You can instruct Veeam Backup & Replication to use Backup from Storage Snapshots for backup and replication. During backup and replication jobs, Veeam Backup & Replication reads data of processed VMs from temporary storage snapshots, which speeds up backup and replication operations and improves RPOs.

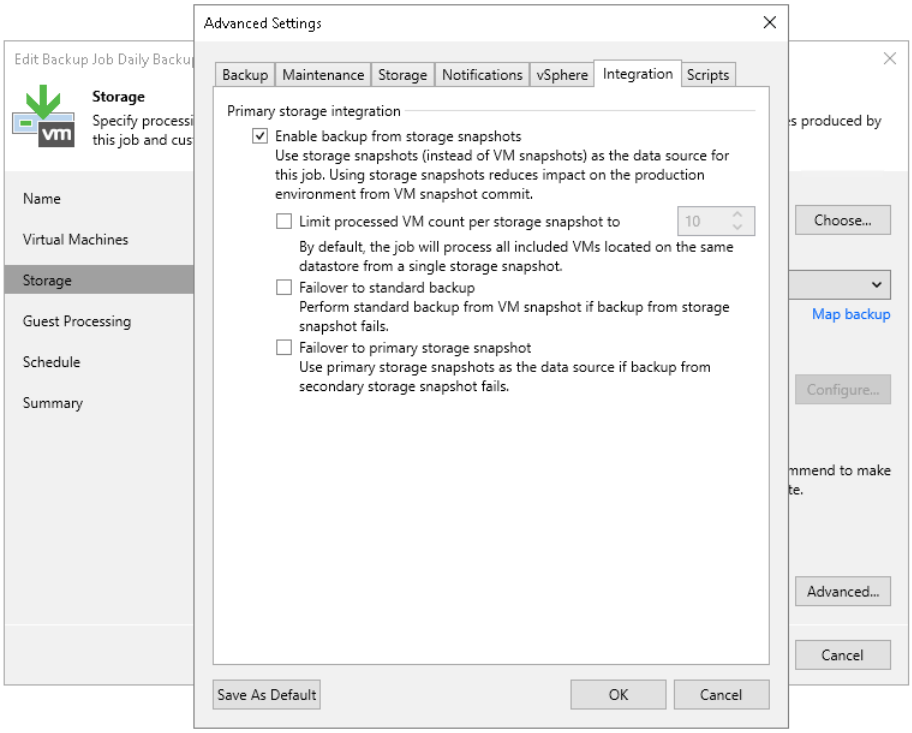
Prerequisites

Before you perform Backup from Storage Snapshots, check the following prerequisites:

- You must install the Enterprise Plus edition of Veeam Backup & Replication on the backup server.
- You must configure the backup infrastructure in a proper way:
  - You must add to the backup infrastructure a backup proxy that will be used for backup or replication, and properly configure this backup proxy. For more information, see Configuring Backup Proxy.
  - You must add to the backup infrastructure vCenter Server or ESXi hosts with VMs whose disks are hosted on the storage system.
  - You must add the storage system to the backup infrastructure.
- You must check limitations for Backup from Storage Snapshots. For more information, see Backup from Storage Snapshots.

Key Job Settings

The key job setting responsible for the Backup from Storage Snapshots on primary storage arrays is the **Enable backup from storage snapshots** check box in the **Advanced** settings of the **Storage** step of the wizard.



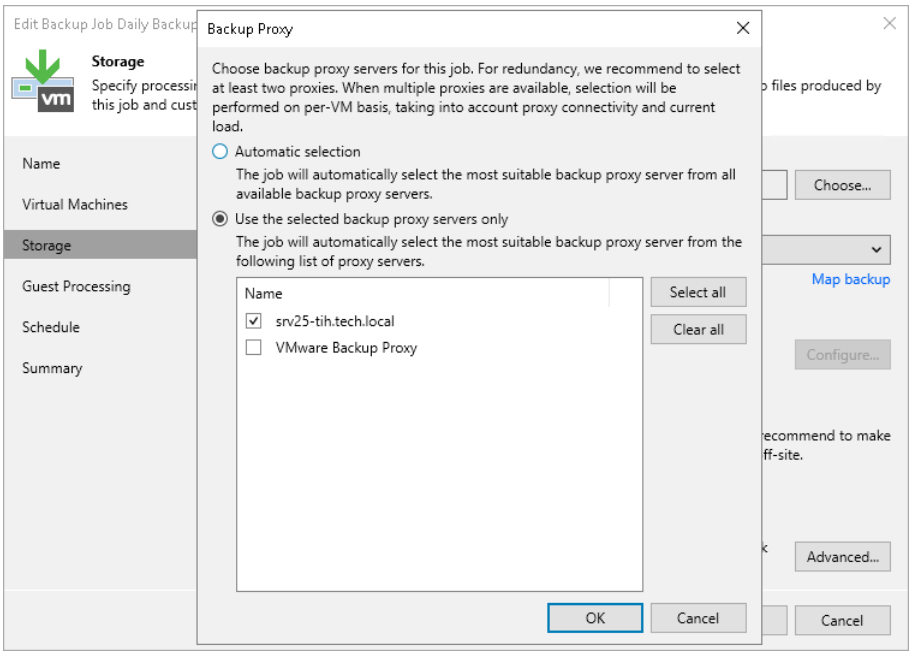
Configuring Backup from Primary Storage Arrays

To back up and replicate VMs using Backup from Storage Snapshots:

1. Configure a backup or replication job. At the **Storage** step of the backup or replication job wizard, select a backup proxy that will be used for data transfer. You can assign the backup proxy explicitly or choose the automatic mode of backup proxy selection.

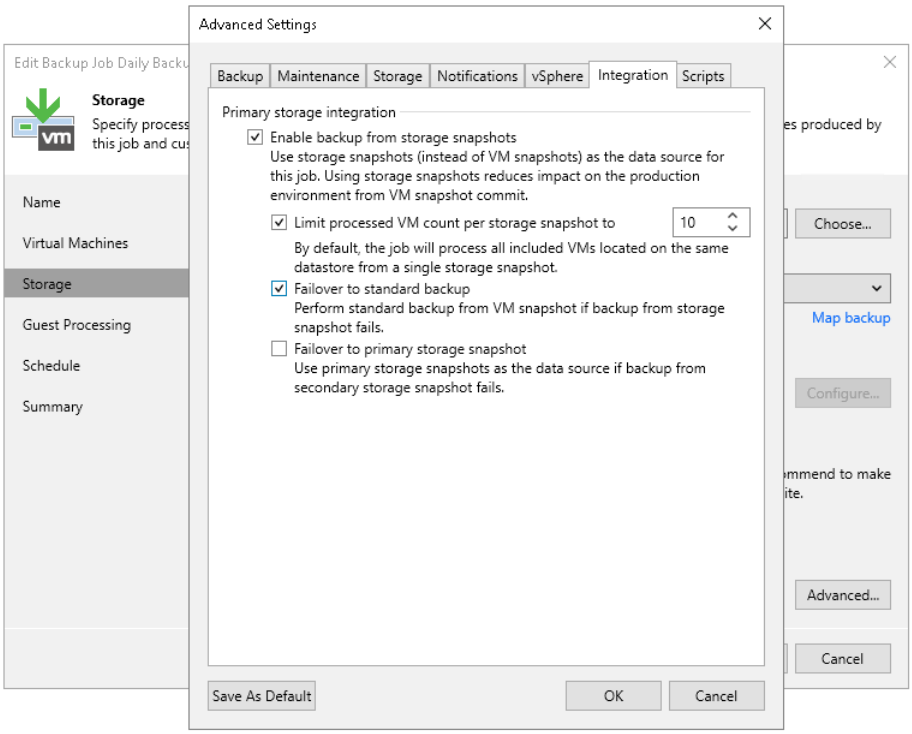
IMPORTANT

The backup proxy that you select must be added to the list of backup proxies in storage system connection settings. Otherwise, Veeam Backup & Replication may fail over to the regular data processing mode. To ensure that failover will take place if Veeam Backup & Replication does not detect a backup proxy, at the **Storage** step of the backup or replication job wizard, click **Advanced**. On the **Integration** tab, select the **Failover to standard backup** check box. The **Failover to standard backup** option will also work if Veeam Backup & Replication fails to create storage snapshots for the storage volumes. As a result, all VMs residing on the volumes will be processed by regular data processing mode.



2. At the **Storage** step of the wizard, click **Advanced**, then click the **Integration** tab. Check that the **Enable backup from storage snapshots** check box is selected. By default, this option is enabled for all newly created jobs.

3. If you add to the job multiple VMs whose disks are hosted on the same volume or LUN, select the **Limit processed VM count per storage snapshot to <N>** check box and specify the number of VMs for which one temporary storage snapshot must be created. Veeam Backup & Replication will divide VMs into several groups and trigger a separate storage snapshot for every VM group. As a result, the job performance will increase. For more information, see Limitation on Number of VMs per Snapshot.



Backup from Secondary Storage Arrays

If the primary storage array is associated with a secondary storage array, you can use the secondary storage array as a data source for backup. Backup from snapshots on secondary storage arrays reduces impact on the production storage. During backup, operations on VM data reading are performed on the side of the secondary storage array, and the primary storage array is not affected.

The following table shows storage systems and replication features that can be used for backup from storage snapshots on secondary storage arrays.

Veeam Backup & Replication feature term \ Storage system	HPE Primera, HPE 3PAR, HPE Alletra 9000	Lenovo V Series, IBM FlashSystem (StorWize), IBM SVC	HPE Nimble, HPE Alletra 5000/6000	NetApp ONTAP FAS, AFF, and ASA Series, FlexArray (V Series), Fujitsu ETERNUS HX/AX, IBM N series, Lenovo ThinkSystem DM Series	Pure Storage FlashArray
Snapshot transfer	Remote Copy Periodic (Asynchronous)	Global Mirror (Global Mirror with Change Volumes is not supported)	Snapshot Replication	SnapMirror SnapVault	Asynchronous Replication
Synchronous replication	Remote Copy Peer Persistence* * Snapshots are created on the target volume only.	HyperSwap Metro Mirror	Synchronous Replication	×	ActiveCluster Replication

How Backup from Secondary Storage Systems Works

Backup from snapshots on secondary storage arrays is similar to Backup from Storage Snapshots on the primary storage array. The algorithm slightly differs for snapshot transfer and synchronous replication.

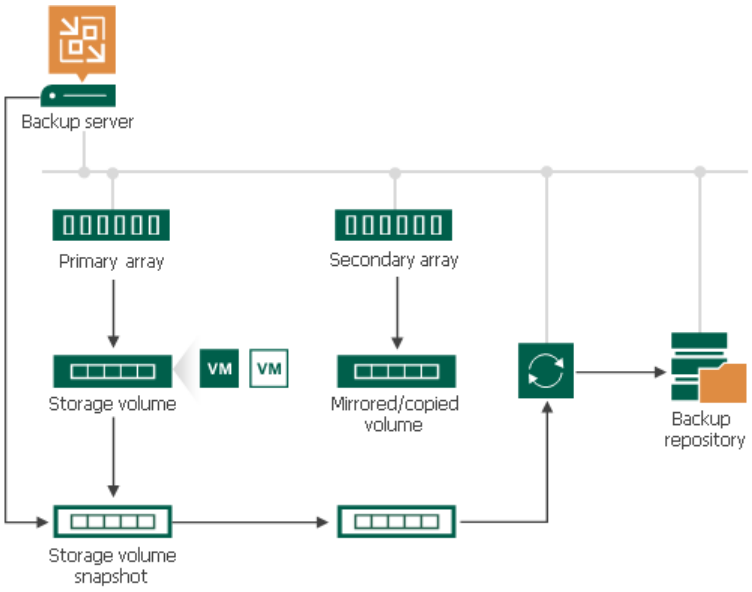
1. Veeam Backup & Replication analyzes which VMs in the job host their disks on the storage system and checks the backup infrastructure to detect if there is a backup proxy that has a direct connection to the storage system.
2. Veeam Backup & Replication detects whether the storage system uses synchronous replication or snapshot transfer, and whether backup from secondary storage array is possible.
3. Veeam Backup & Replication triggers a VMware vSphere snapshot for a VM whose disks are hosted on the primary storage array.
4. Veeam Backup & Replication instructs the storage system to create an application-consistent temporary storage snapshot. If snapshot transfer is used — on the primary storage array. If synchronous replication — on the primary and secondary storage arrays. However, only snapshot on the secondary storage array will be used.

   The created temporary snapshots capture the VMware vSphere VM snapshot. The VMware vSphere VM snapshot is then deleted.

5. [For snapshot transfer] The following steps apply if snapshot transfer is detected:
    a. The temporary storage snapshot is transferred from the primary storage array to the secondary storage array.
    b. The transferred temporary storage snapshot is mounted to the detected backup proxy.
    c. The backup job retrieves VM data from the mounted temporary storage snapshot.
    d. When the job finishes processing the VM, Veeam Backup & Replication instructs the storage system to delete the temporary snapshot on the primary storage array. The transported snapshot on the secondary storage becomes long-term snapshot and remains in the snapshot chain until it is removed by the retention policy.
6. [For synchronous replication] The following steps apply if synchronous replication is detected:
    a. The created temporary storage snapshot is mounted to the detected backup proxy.
    b. When the job finishes processing the VM, Veeam Backup & Replication instructs the storage system to delete the temporary snapshot on the primary and secondary storage arrays.

Note the following:

- [For HPE Nimble] On HPE Nimble storage systems, snapshot transport is triggered as soon as you create a new storage snapshot. For this reason, launch of snapshot transport and deletion of VMware vSphere snapshots are performed in parallel.
- [For NetApp ONTAP and HPE Nimble] Veeam Backup & Replication creates auxiliary snapshots on the primary storage system. The number of storage snapshots in the snapshot chain cannot be fewer than 1.



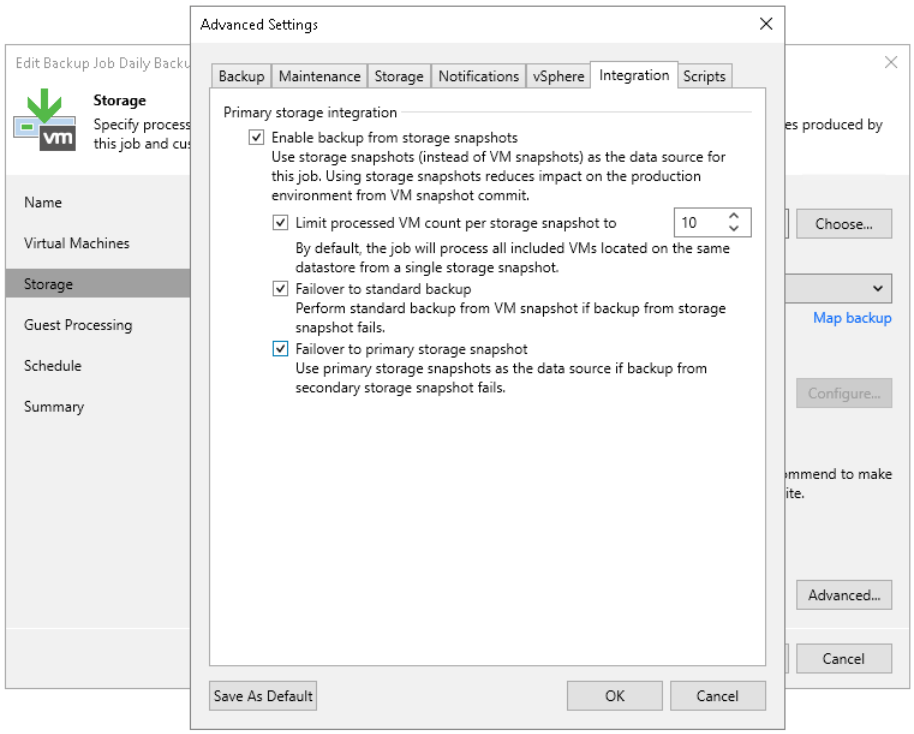
Failover to Backup from Snapshots on Primary Storage Arrays

In some cases, Veeam Backup & Replication may fail to back up VM data from temporary storage snapshots on the secondary storage array. This can happen, for example, if Veeam Backup & Replication fails to connect to the secondary storage array or a license required for volume or LUN export is not installed (in case of NetApp SnapMirror or SnapVault).

To overcome this situation, you can instruct the backup job to fail over to the Backup from Storage Snapshots on the primary storage array. In this case, Veeam Backup & Replication will create a temporary storage snapshot on the primary storage array and attempt to transport it to the secondary storage array. If the transport process fails, Veeam Backup & Replication will retrieve VM data from the created temporary snapshot on the primary storage array. Note, however, that Backup from Storage Snapshots on the primary storage system will produce additional load on the production environment.

To let Veeam Backup & Replication fail over to Backup from Storage Snapshots on the primary storage array, you must enable the **Failover to primary storage snapshot option** in the backup job settings.

> **NOTE**
>
> Failover to Backup from Storage Snapshots on the primary storage array is not supported for HPE 3PAR Peer Persistence. For other storage systems with synchronous replication, failover can be used only if the secondary storage array is not detected at the beginning of the job. If the connection with the secondary storage array is lost later, the job will fail.



Configuring Backup from Snapshots on Secondary Storage Arrays

You can configure a backup job to perform Backup from Storage Snapshots on secondary storage arrays.

Prerequisites

Before you run the backup job, check the following prerequisites:

- You must configure a secondary storage array for the primary storage system where VMs that you plan to back up are hosted.
    - [For HPE Nimble] You must configure Volume Collection replication from the primary storage array to the secondary storage array. For more information, see the HPE Nimble documentation.

    - [For NetApp ONTAP] You must configure volume SnapMirror/SnapVault relationships between the primary and secondary storage arrays. MirrorAndVault Relationships will be identified by Veeam Backup & Replication as SnapVault. For more information, see the NetApp documentation.
    - [For HPE 3PAR Peer Persistence and HPE 3PAR Remote Copy] You must create a Remote Copy Group (RCG) with relevant type (Synchronous or Periodic).

- Check prerequisites in the following Veeam KB articles: DataCore SANsymphony, Dell PowerMax requirements, Dell PowerStore requirements, Fujitsu ETERNUS AF/DX Series, Hitachi VSP requirements, HPE XP requirements, INFINIDAT InfiniBox F Series, NEC Storage M Series requirements, NEC Storage V Series requirements, NetApp SolidFire/HCI, Pure Storage FlashArray, Tintri IntelliFlash/Western Digital/Tegile.
    - When you add storage arrays to the backup infrastructure, you must add to the rescan scope volumes and LUNs on which VM disks are located (both for primary and secondary storage arrays). For more information, see Adding Storage Systems.

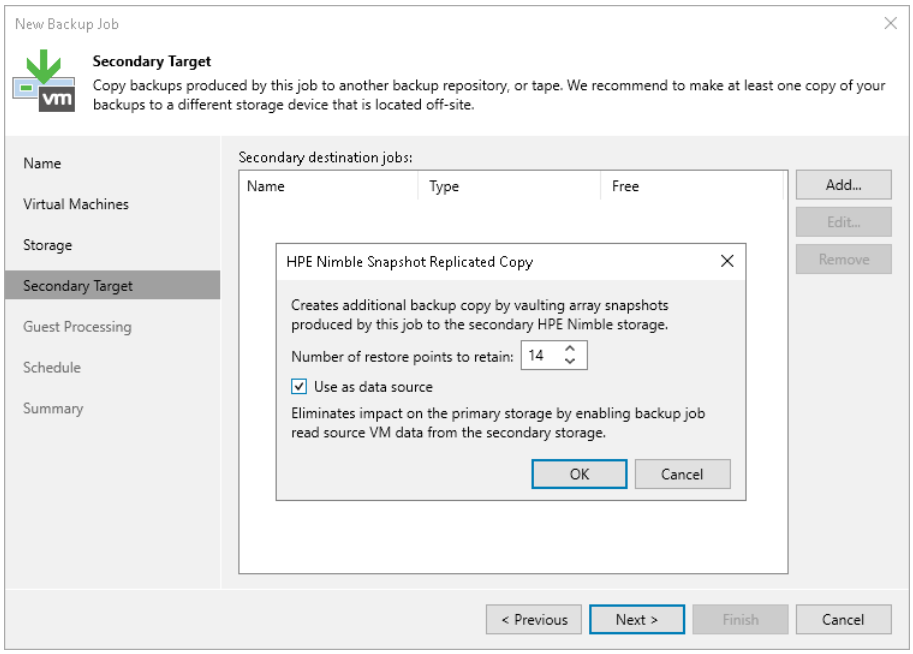
- You must configure the backup infrastructure in a proper way.
    - Add to the backup infrastructure a backup proxy that will be used for backup, and properly configure this backup proxy. For more information, see Configuring Backup Proxy.
    - Add to the backup infrastructure vCenter Server hosts or ESXi hosts with VMs whose disks are hosted on the storage system.
    - Add the primary storage system and secondary storage array to the backup infrastructure.
- You must install a license for Veeam Backup & Replication Enterprise Plus edition on the backup server.
- You must check limitations for Backup from Storage Snapshots. For more information, see Backup from Storage Snapshots.
- [For NetApp ONTAP] You must install a license for storage snapshot export on NetApp SnapMirror or SnapVault. For more information, see Required Licenses for NetApp.

Key Job Settings

The key job settings responsible for Backup from Storage Snapshots on secondary storage arrays are:

- At the **Storage** step of the wizard, the **Configure secondary destinations for this job**.
- At the **Storage** step of the wizard, in the **Advanced** settings, the **Enable backup from storage snapshots** check box. By default, this option is enabled.

- At the **Secondary Target** step of the wizard, the added replication feature of a secondary storage array and the **Use as the data source** check box.

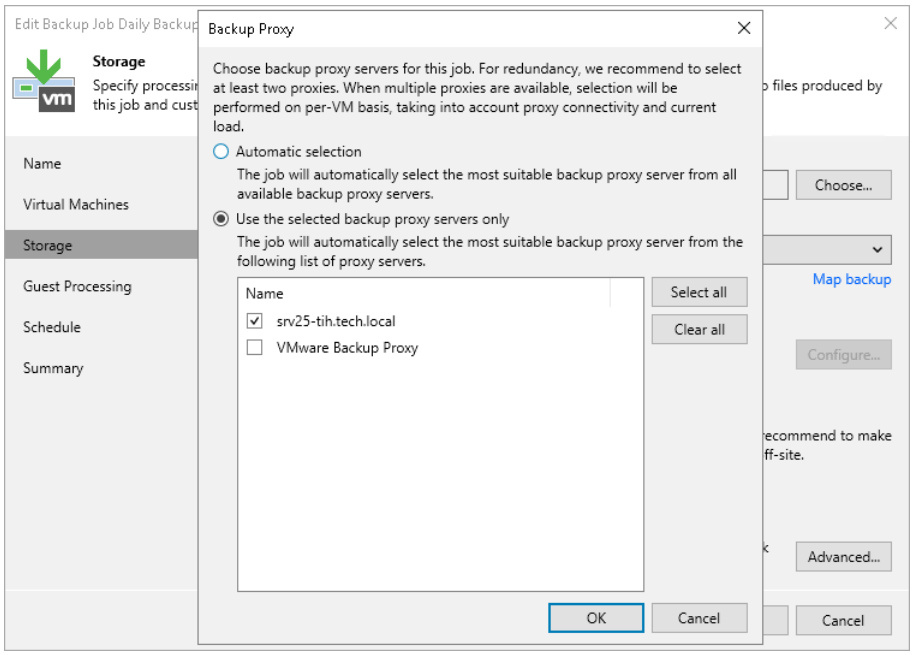


Configuring Backup from Snapshots on Secondary Storage Arrays

To back up VMs from snapshots on secondary storage arrays:

1. Configure a backup job. At the **Storage** step of the backup job wizard, do the following:
    a. Select a backup proxy that will be used for data transfer. You can assign the backup proxy explicitly or choose the automatic mode of backup proxy selection.

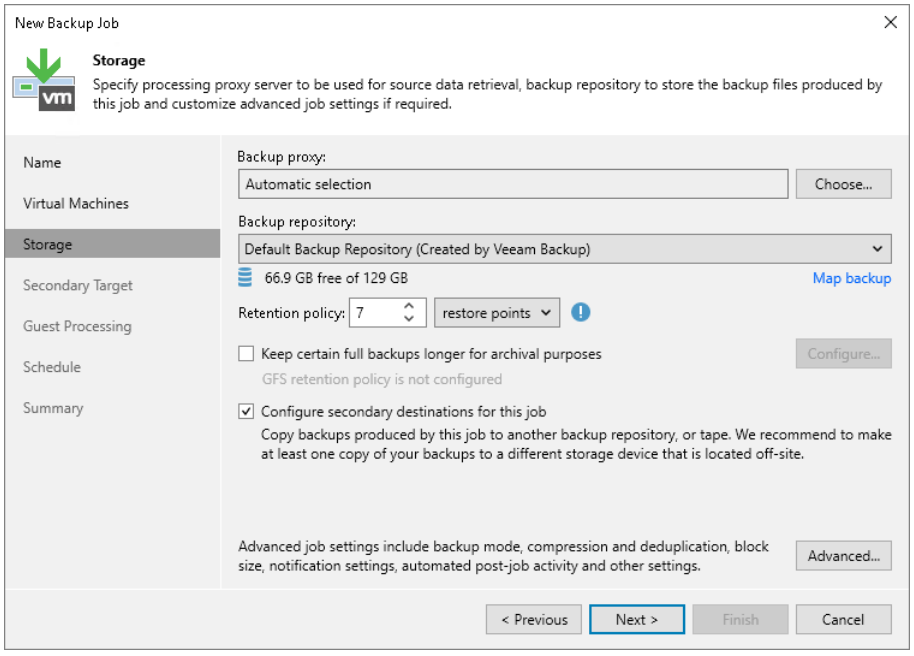
> **NOTE**
>
> A backup proxy that you select must be added to the list of backup proxies in storage system connection settings. If the backup proxy is not added to the list in storage system connection settings, Veeam Backup & Replication may fail over to the regular data processing mode. To switch on the failover, at the **Storage** step of the backup or replication job wizard, click **Advanced** and select the **Failover to standard backup** check box.
>
> For more information, see Adding Storage Systems.



b. From the **Backup repository** list, select a backup repository where you want to store backup files.

c. In the **Retention policy** section, specify the number of backup restore points that you want to keep.

d. Select the **Configure secondary destinations for this job** check box.

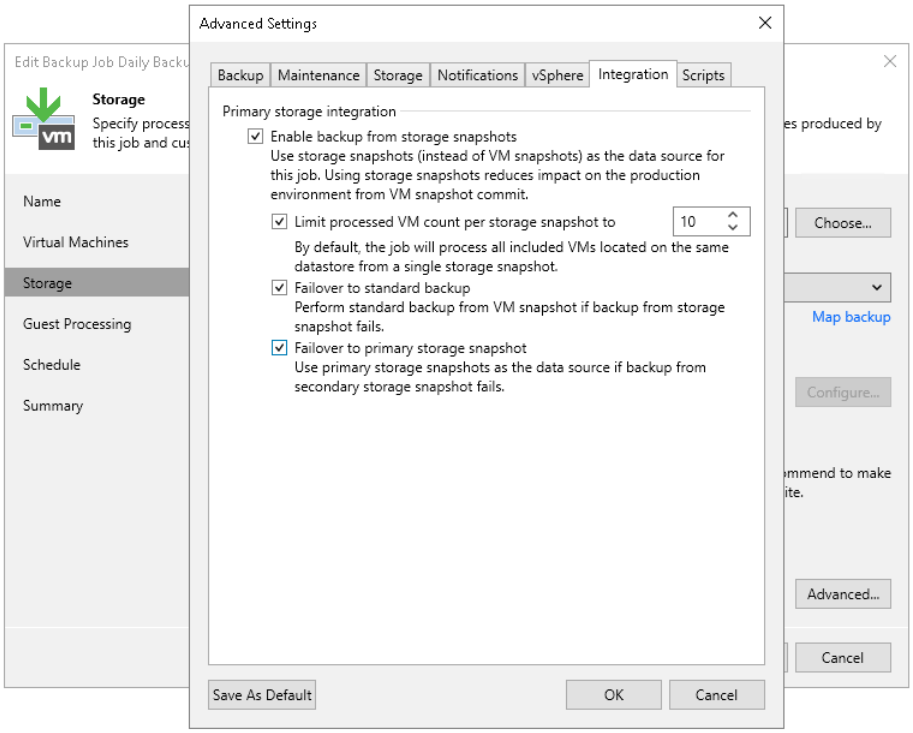


e. Click **Advanced**, then click the **Integration** tab. Make sure that the **Enable backup from storage snapshots** check box is selected.

f. If you add to the job many VMs whose disks are located on the same volume or LUN, select the **Limit processed VM count per storage snapshot to <N>** check box and specify the number of VMs for which one temporary storage snapshot must be created. Veeam Backup & Replication will divide VMs into several groups and trigger a separate temporary storage snapshot for every VM group. As a result, the job performance will increase. For more information, see Limitation on Number of VMs per Snapshot.

g. If Veeam Backup & Replication fails to create a temporary storage snapshot, VMs whose disks are located on the storage system will not be processed by the job. To fail over to the regular data processing mode and back up such VMs, select the **Failover to standard backup** check box.

h. If Veeam Backup & Replication cannot create a temporary storage snapshot on the secondary storage array, the job will not back up VMs whose disks are located to the storage system. To fail over to Backup from Storage Snapshots on the primary storage system, select the **Failover to primary storage snapshot** check box. For more information, see Failover to Backup from Snapshots on Primary Storage Arrays.



2. At the **Secondary Target** step of the wizard, click **Add** and select a replication feature that Veeam Backup & Replication will use to create backups.

   If you select a synchronous replication feature (for example, IBM Spectrum Virtualize with Metro Mirror, Pure Storage Array ActiveCluster Replication or other), the **Use as the data source** option is enabled by default and cannot be changed. Veeam Backup & Replication will create backups from temporary snapshots created on the secondary storage array, snapshots created on the primary storage array will not be used for backup.

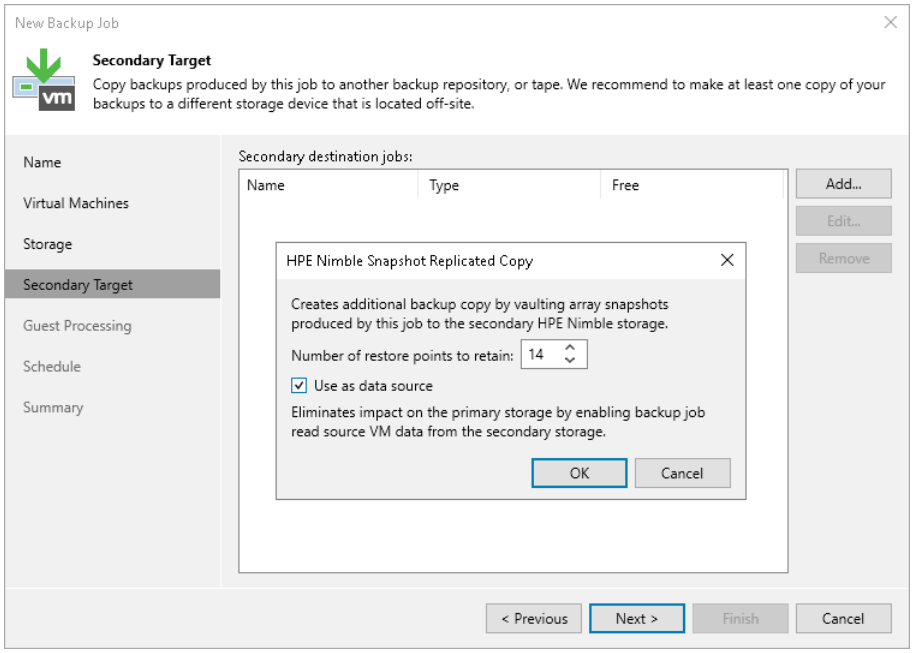
> **NOTE**
>
> [For synchronous replication] If you do not select an option to create snapshots on the primary storage array at the **Secondary Target** step and select only the synchronous replication feature, Veeam Backup & Replication will create only temporary snapshots. The snapshot chain (long-term snapshots) will not be created neither on the primary storage array nor on the secondary storage array. To create a snapshot chain, add the option to create snapshots on the primary storage array and specify the **Number of snapshot copies to retain**. In this case, long-term snapshots will be created simultaneously on the primary and secondary storage arrays, that is, coordinated snapshots will be created. Veeam Backup & Replication will retain the same number or snapshots on both storage arrays.

If you select a snapshot transfer feature (for example, IBM SVC Global Mirror or other), Veeam Backup & Replication will also add a snapshot to a snapshot chain. In this case, configure the following:

a. In the **Number of snapshot copies to retain** field, specify the number of long-term storage snapshots to retain on the secondary storage array. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the chain.

   [For NetApp SnapMirror] This option is not applicable. On this secondary storage system, Veeam Backup & Replication maintains the same number of storage snapshots as on primary storage arrays.

b. Select the **Use as the data source** check box to use the secondary storage array as a source for backups.

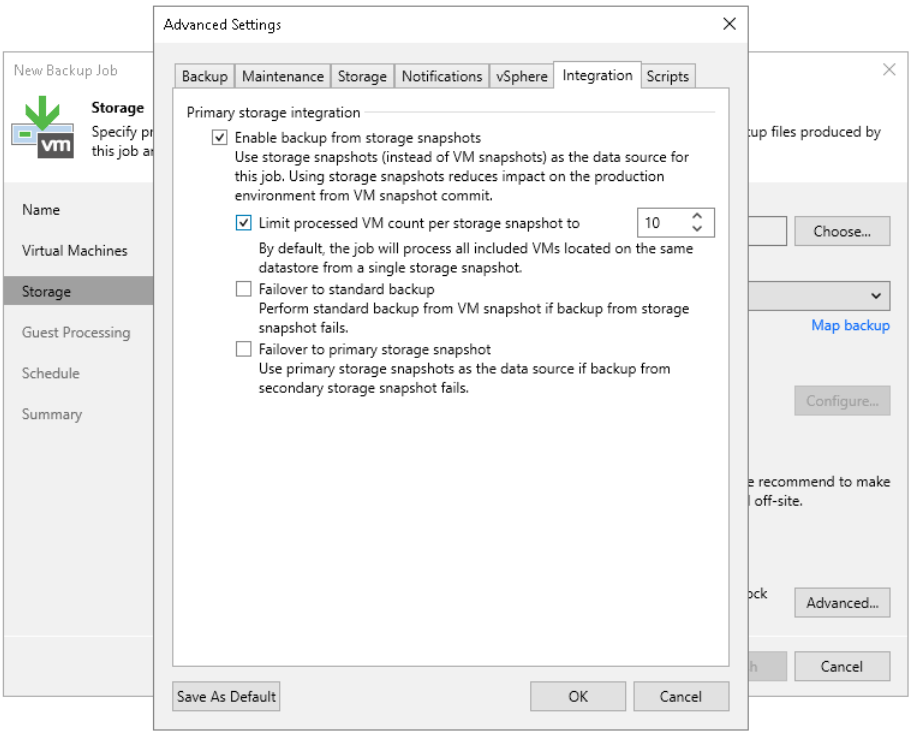


3. Specify other backup job settings as required.
4. Click **Next**, then click **Finish** to save the job settings.

Limitation on Number of VMs per Snapshot

By default, during Backup from Storage Snapshots Veeam Backup & Replication creates VMware vSphere snapshots for all VMs defined in the backup job that reside on the same volume or LUN, and then triggers a storage snapshot for this volume or LUN. The more VMs reside on the volume or LUN, the more time it takes to create VM snapshots. To speed up the backup or replication process, you can limit the number of VMs per storage snapshot.

To limit the number of VMs per storage snapshot, you must enable the **Limit processed VM count per storage snapshot to <N>** option and specify the number of VMs per snapshot in the job settings.



With the limitation option enabled, Veeam Backup & Replication processes VMs in several cycles:

1. Veeam Backup & Replication divides VMs into several groups, as defined in the **Limit processed VM count per storage snapshot to <N>** option.
2. Veeam Backup & Replication triggers VMware vSphere snapshots for VMs in the first group.
3. Veeam Backup & Replication triggers a storage snapshot for the volume or LUN where the VMs are hosted.
4. Veeam Backup & Replication deletes VMware vSphere snapshots for the VMs in the first group.
5. Veeam Backup & Replication copies data of VMs in the first group from the storage snapshot.
6. Veeam Backup & Replication removes the storage snapshot.
7. Steps 2-6 are repeated for every remaining group of VMs.

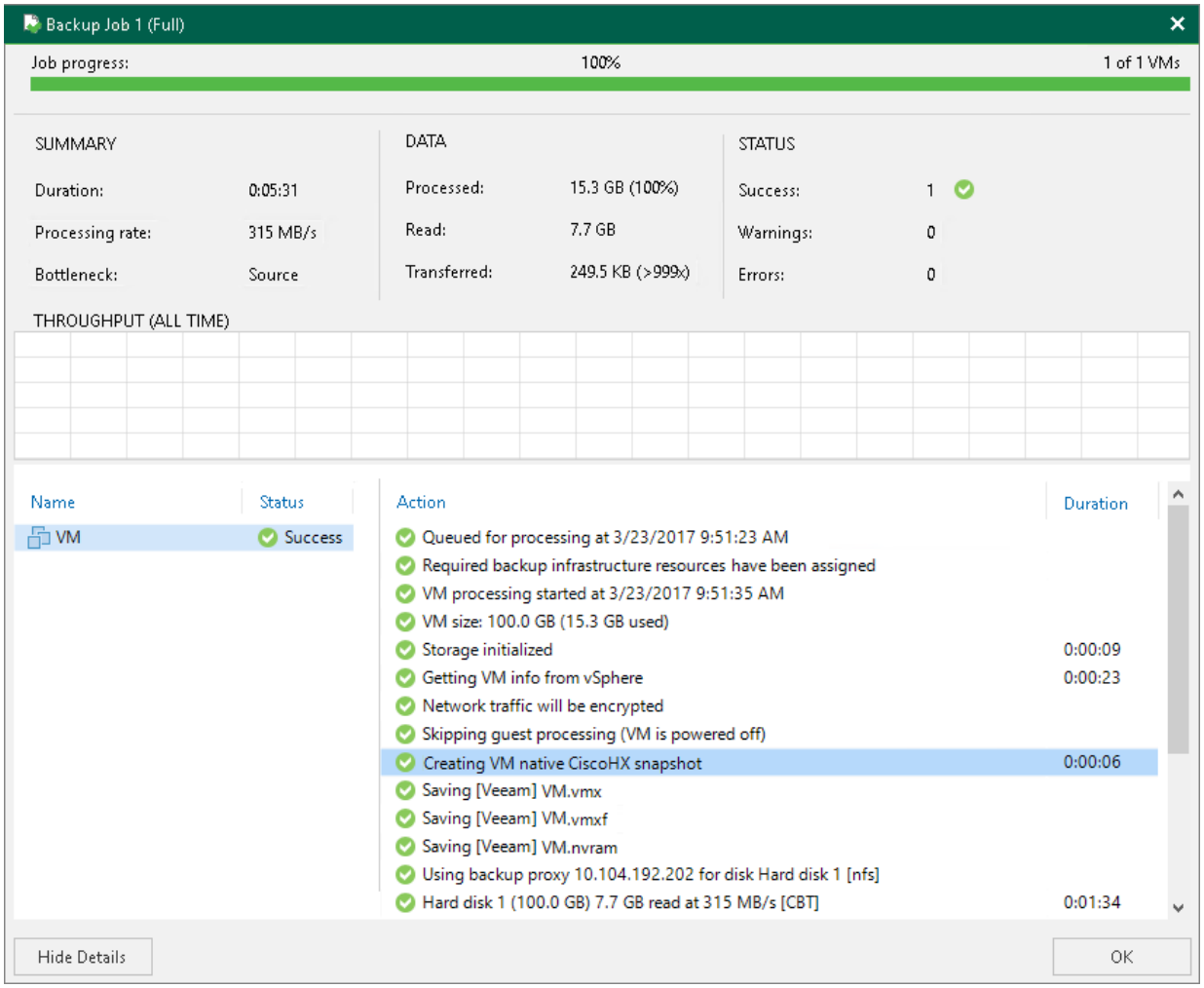
For example, you add to the job 15 VMs whose disks are hosted on the same volume and set the **Limit processed VM count per storage snapshot to <N>** option to 10. Veeam Backup & Replication will divide all VMs into 2 groups — a group of 10 VMs and group of 5 VMs. Veeam Backup & Replication will perform the data processing cycle for the first group of VMs. When VM data processing is over, Veeam Backup & Replication will start processing the second group of VMs.

Backup from Cisco HyperFlex Snapshots

Veeam Backup & Replication integrates with Cisco HyperFlex and allows you to improve performance of backup and replication of VMware vSphere VMs hosted on Cisco HyperFlex.

For backup and replication of VMs hosted on Cisco HyperFlex, Veeam Backup & Replication uses Cisco HyperFlex VM snapshots to preserve VMs in a consistent state suitable for backup or replication. Cisco HyperFlex creates space efficient VM snapshots almost instantly. Veeam Backup & Replication, in its turn, uses HyperFlex snapshots for VM data processing, which helps speed up backup and replication operations, reduce impact of backup and replication activities on the production environment and improve RPOs.

Implementation of integration with Cisco HyperFlex is different from those provided for other supported storage systems. When Veeam Backup & Replication processes VMs hosted on Cisco HyperFlex, it leverages snapshots created at the VM level, not snapshots created at the storage volumes level.

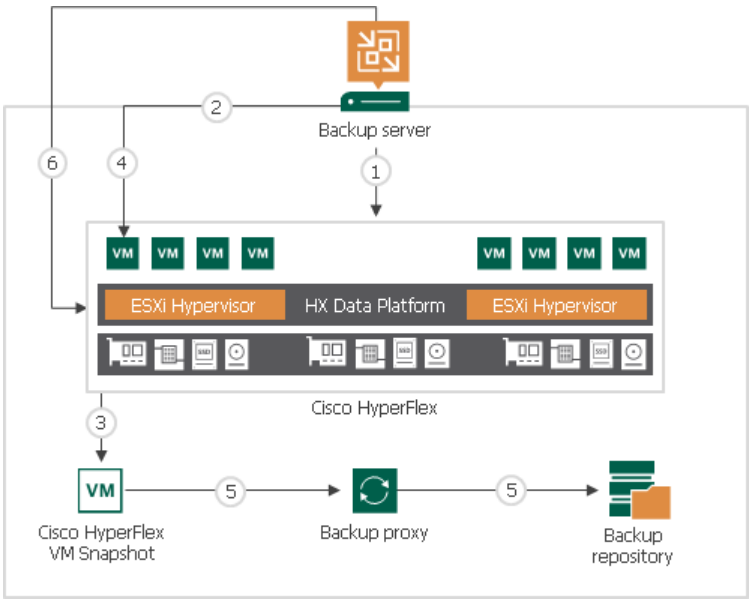


How Backup from Cisco HyperFlex Snapshots Works

When you perform backup or replication from Cisco HyperFlex snapshots, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication analyses which VMs in the job are hosted on Cisco HyperFlex.
2. If application-aware processing is enabled, Veeam Backup & Replication quiesces data and applications on VMs guest OSes.

3. Veeam Backup & Replication triggers Cisco HyperFlex VM snapshots for every processed VM.
4. If application-aware processing is enabled, Veeam Backup & Replication resumes quiesced I/O activities on VMs guest OSes.
5. Veeam Backup & Replication reads new virtual disk data blocks (for full job session) or changed virtual disk data blocks with CBT (for incremental job sessions) from Cisco HyperFlex NFS stores and transports them to the backup repository or target datastore.
6. After VM data processing is finished, Veeam Backup & Replication triggers removal of the Cisco HyperFlex VM snapshots.



Configuring Backup Proxies

This section describes how to configure VMware backup proxies for using Cisco HyperFlex snapshots and also which transport modes and methods of data retrieving proxies can use.

Requirements

To enable backup and replication from Cisco HyperFlex snapshots, you must configure one or more backup proxies in the backup infrastructure. Backup proxies must meet the following requirements:

- Check requirements listed in Configuring Backup Proxy for Storage Integration.
- The backup proxy that you plan to use must have NFS access to the network handling traffic between Cisco HyperFlex and ESXi hosts where the backed-up or replicated VMs reside.

Methods of Data Retrieving for Direct NFS Access Transport Mode

Backup proxies that work in the Direct NFS access transport mode and process data of VMs hosted on Cisco HyperFlex can read VM data from NFS stores over the NFS HyperFlex data network. Depending on the backup infrastructure configuration, backup proxies can read data over the following data paths:

- **Backup from Storage Snapshots over IO Visor on ESXi hosts**. The IO Visor is a Cisco HyperFlex software module that runs on every ESXi host that is a part of the Cisco HyperFlex cluster. It presents HyperFlex NFS datastores to the ESXi hosts and optimizes the data paths in the HyperFlex cluster.

  Backup over IO Visor is the preferred method. It provides the high speed of VM data reading and balances the load across the HyperFlex cluster. To read VM data over IO Visor, backup proxies must be connected to the same HyperFlex data network as the processed VMs. You must also configure a firewall rule on the ESXi hosts to allow Veeam Backup & Replication to interact with the IO Visor. For more information, see Configuring Firewall Rules for Cisco HyperFlex IOVisor Processing.

  If the firewall rules are not configured, Veeam Backup & Replication will fail over to Backup from Storage Snapshot over the HyperFlex Controller Cluster IP by default.

- **Backup from Storage Snapshots over HyperFlex Controller Cluster IP**. In this processing mode, all traffic is handled by a single HX controller that holds the HyperFlex Controller Cluster IP.

  To read VM data over HyperFlex Controller Cluster IP, backup proxies must be connected to the same HyperFlex data network as the processed VMs. Veeam Backup & Replication will configure all necessary firewall settings within the HyperFlex Controllers automatically during the storage discovery process. Veeam Backup & Replication automatically detects new HyperFlex controllers and applies firewall changes.

Selecting Proxies and Transport Modes

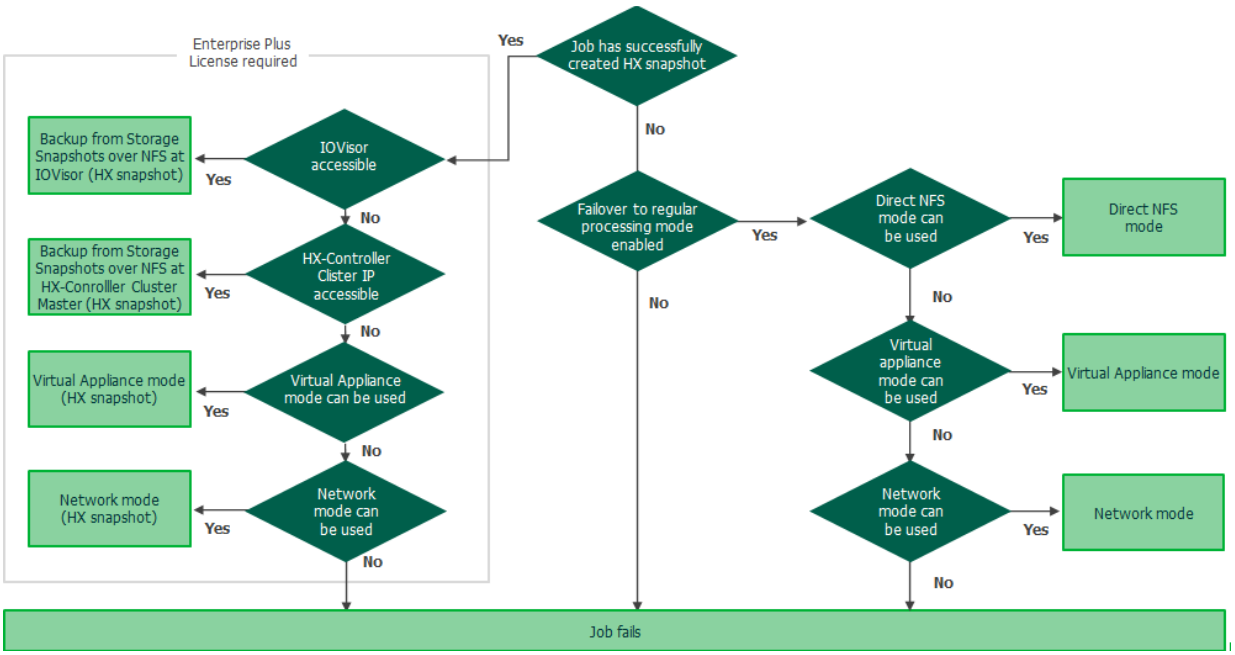
You can instruct Veeam Backup & Replication to read data from Cisco HyperFlex snapshots in the following transport modes: Direct storage access, Virtual appliance or Network. The recommended mode is Direct storage access working over NFS protocol. It provides the best performance and low overhead on ESXi hosts. In this mode, Veeam Backup & Replication bypasses the ESXi host, reads and writes data directly to Cisco HyperFlex NFS data network.

When a job starts, Veeam Backup & Replication analysis which proxies can be used for processing VMs and selects a proxy for each VM. If multiple proxies can be used for a VM, Veeam Backup & Replication selects a proxy with the most prioritized transport mode.

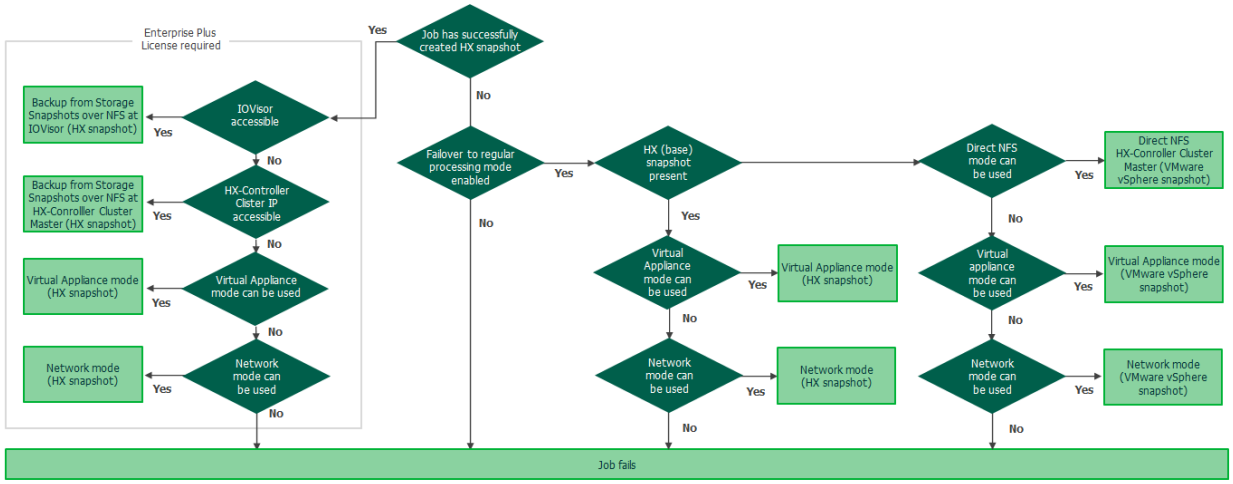
The following diagrams show how Veeam Backup & Replication prioritizes transport modes for each proxy. The diagrams also show how Veeam Backup & Replication chooses proxies when Cisco HyperFlex snapshots cannot be created. In this case, Veeam Backup & Replication performs standard data processing. Note that to use regular data processing, you must enable Failover to standard backup option.

For more information on whether a proxy can use a specific transport mode, see the necessary topics in Transport Modes section of the Veeam Backup & Replication User Guide.

Transport Mode Selection for HyperFlex version 4.5(2a) or later



Transport Mode Selection for HyperFlex version prior to 4.5 (2a)



Configuring Firewall Rules for Cisco HyperFlex IO Visor Processing

The Cisco HyperFlex IO Visor is a software component that runs on all ESXi hosts within a Cisco HyperFlex cluster. It works as an NFS server for Veeam traffic.

You need to allow NFS traffic from the backup proxies to ESXi hosts. As Cisco IO Visor based NFS communication uses dynamic ports, you need to create an ESXi firewall rule with inbound ports 0-65535 and the backup proxy IP addresses as allowed IP addresses.

Configuring Backup Proxies for Backup from Storage Snapshot with Virtual Appliance or Network mode

If you plan to use the Virtual appliance or Network mode to process VMs hosted on Cisco HyperFlex, you must configure the backup infrastructure in the following way:

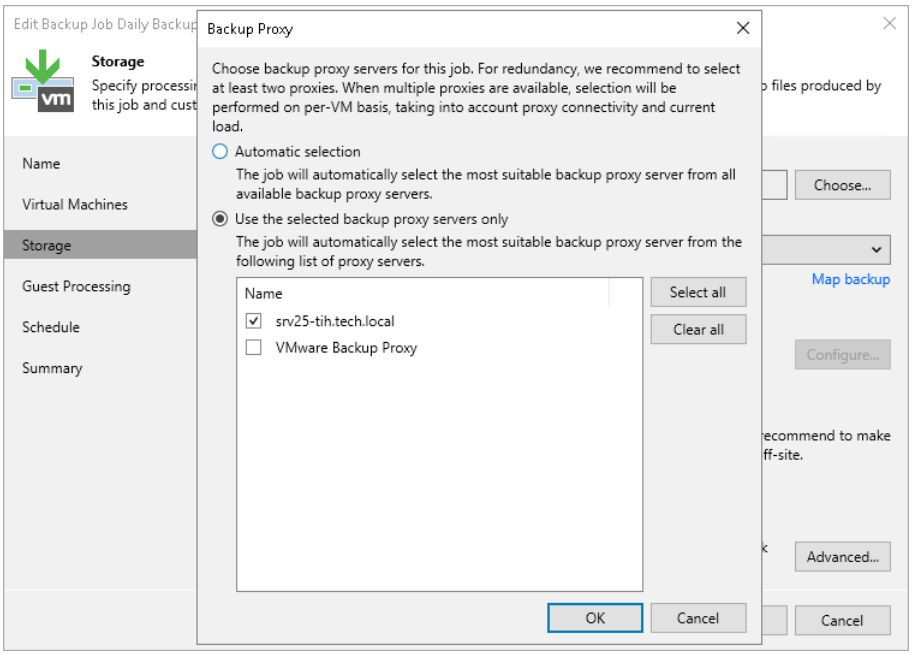
1. You must add Cisco HyperFlex to the backup infrastructure to allow Veeam Backup & Replication to create HyperFlex snapshots.
2. You must configure the backup proxies to work in the Virtual appliance or Network transport mode. For more information, see the Virtual appliance and Network Mode sections of the Veeam Backup & Replication User Guide.
3. If you plan to use the Virtual appliance mode, it is recommended that you enable an optimization for NFS datastores in Veeam Backup & Replication to avoid VM stuns as described in this VMware KB article. To do this:
   a. Create a backup proxy on every host in the VMware vSphere cluster where VMs that you plan to back up or replicate reside.
   b. On the machine where the Veeam Backup & Replication console is installed, open Registry Editor.
   c. Navigate to the key: `HKLM\Software\Veeam\Veeam Backup and Replication\`.
   d. Create a new DWORD with the name `EnableSameHostHotaddMode`, and set its value to 2.

      If a backup proxy on the same host as a processed VM is unavailable, Veeam Backup & Replication will use an available backup proxy on a different host, but force it to use the Network transport mode, so that no stun occurs.

Configuring Backup from Cisco HyperFlex Snapshots

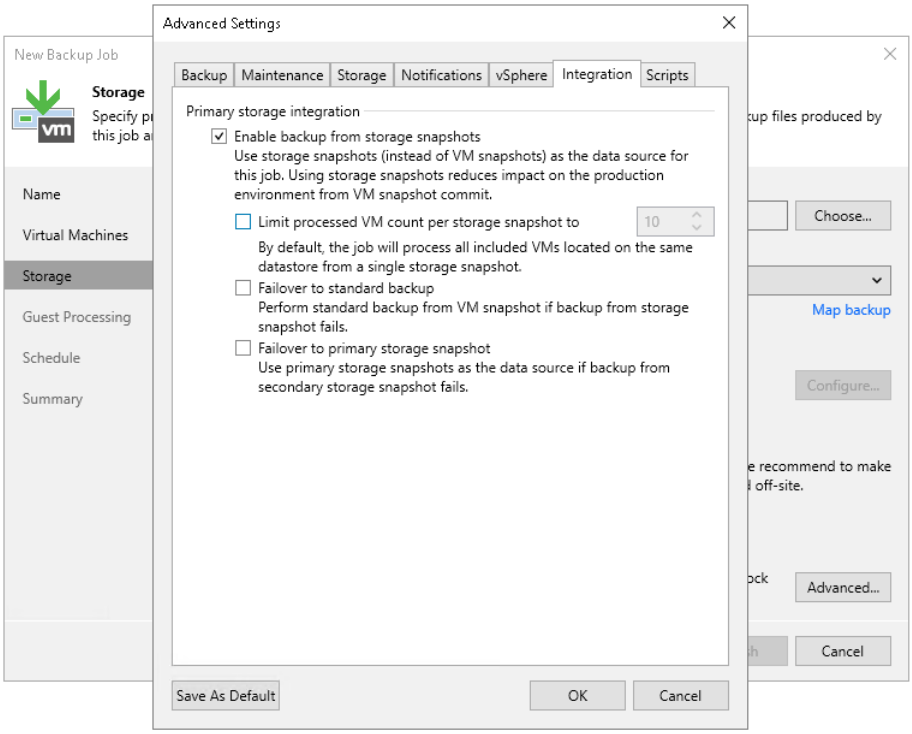
To back up and replicate from Cisco HyperFlex snapshots:

1. Configure a backup or replication job. At the **Storage** step of the backup or replication job wizard, select a backup proxy that will be used for data transport. You can assign the backup proxy explicitly or choose the automatic mode of backup proxy selection.



2. At the **Storage** step of the wizard, click **Advanced**, then click the **Integration** tab. Make sure that the **Enable backup from storage snapshots** check box is selected. By default, this option is enabled for all newly created jobs.

3. If Veeam Backup & Replication fails to process VMs in the full integration mode, VMs hosted on Cisco HyperFlex will not be backed up or replicated. To fail over to the regular data processing mode, select the **Failover to standard backup** check box.

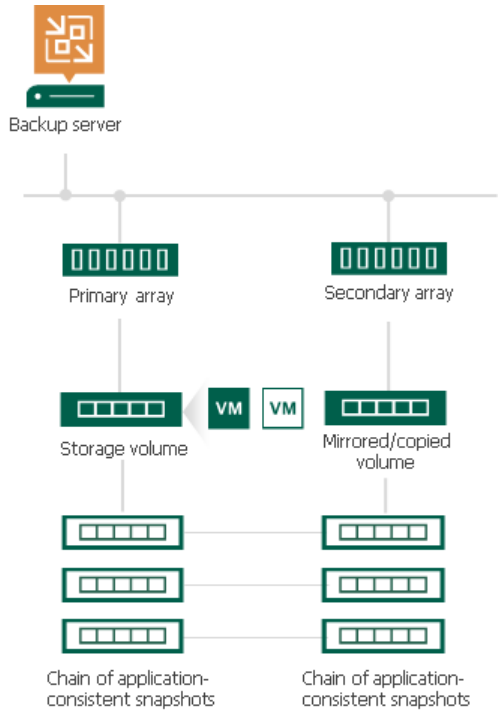


Snapshot Orchestration

Veeam Backup & Replication lets you perform Snapshot Orchestration — build a snapshot chain on primary and secondary storage arrays. To create only long-term snapshots on storage arrays, you can run a snapshot-only job.

The snapshot-only job is similar to scheduling automatic snapshot creation in the storage management console. A snapshot-only job does not create Veeam backup files in the backup repository. It creates only long-term storage snapshots on the storage system by a schedule that is defined in the job settings.

Depending on the backup job settings, the created snapshots can be application-consistent or crash-consistent.



Configuring Snapshot-Only Jobs

You can use snapshot-only jobs to create a chain of storage snapshots on the primary storage array and, optionally, on the secondary storage array.

Prerequisites

The ability to create snapshot-only jobs depends on the Veeam Backup & Replication license edition. For snapshot-only jobs on the primary storage arrays, you can use any license edition. For snapshot-only jobs on the secondary storage arrays, the license edition depends on the used storage system and replication feature. The following table shows the dependency.

License Edition/ Storage System	NetApp ONTAP FAS, AFF, and ASA Series, FlexArray (V Series), Fujitsu ETERNUS HX/AX, IBM N series, Lenovo ThinkSystem DM Series	HPE Primera, HPE 3PAR, HPE Alletra 9000	Lenovo V Series, IBM FlashSystem (StorWize), IBM SVC	HPE Nimble, HPE Alletra 5000/6000	Universal Storage API Integrated Systems
Enterprise	SnapMirror	Remote Copy Peer Persistence	HyperSwap Metro Mirror	Synchronous replication	Synchronous replication feature
Enterprise Plus	SnapVault SnapMirror	Remote Copy Peer Persistence Remote Copy Periodic (Asynchronous)	HyperSwap Metro Mirror Global Mirror	Snapshot replication Synchronous replication	Snapshot transfer feature Synchronous replication feature Snapshot archiving feature

If you use the appropriate license edition and secondary storage arrays with synchronous replication (for example, IBM Spectrum Virtualize with Metro Mirror or other), Veeam Backup & Replication uses the synchronous replication feature by default. On such storage array systems, long-term snapshots are always created simultaneously on the primary and secondary storage arrays, that is, coordinated snapshots are created. Veeam Backup & Replication maintains the same number of long-term snapshots on the primary and secondary arrays. For snapshot-only jobs, this means that you do not need to add the synchronous replication feature to the job and configure it.

Key Job Settings

The key settings for the snapshot-only job are:

- At the **Storage** step of the wizard, a primary storage system selected as a repository.
- At the **Storage** step of the wizard, the **Retention policy** field.
- [Optional] At the **Storage** step of the wizard, the **Configure secondary destinations for this job**.

- [Optional] At the **Secondary Target** step of the wizard, the added replication feature of a secondary storage array and the **Number of snapshot copies to retain** field.

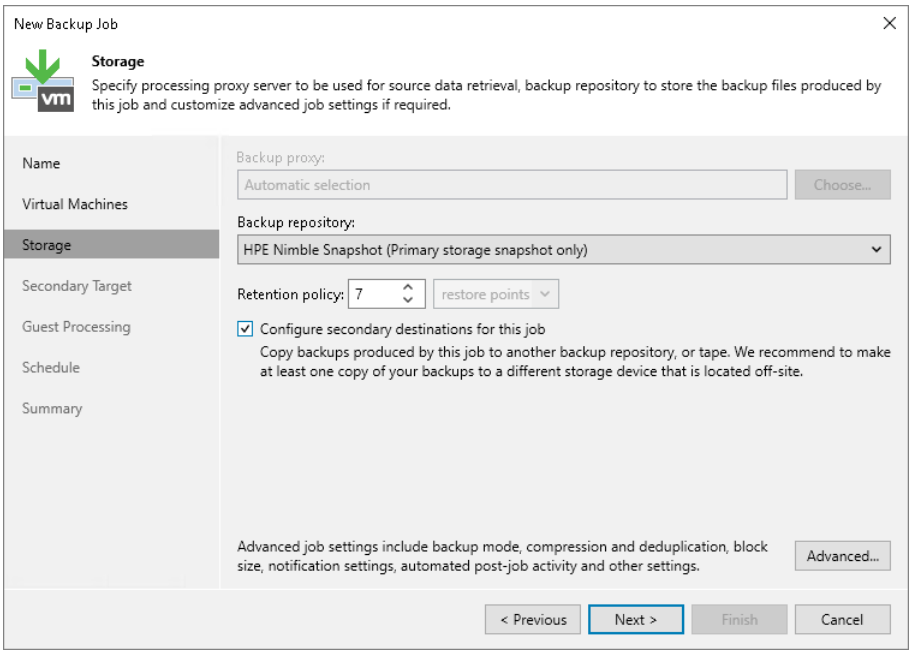
Configuring Snapshot-Only Jobs

To configure a snapshot-only job:

1. Open the **Home** view.
2. Click **Backup Job** > **VMware** or **vCloud** on the ribbon. Veeam Backup & Replication will launch the **New Backup Job** wizard.
3. At the **Name** step of the wizard, specify a name and description for the backup job.
4. At the **Virtual Machines** step of the wizard, click **Add** and select VMs whose disks are hosted on the storage system.
5. At the **Storage** step of the wizard, select a primary storage array from the **Backup repository** list.

   In the **Retention policy** field, specify the number of long-term storage snapshots that you want to maintain in the snapshot chain on the primary storage array. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the chain (if it does not contain any restore points that fall under the retention period).

   If you want to additionally create long-term storage snapshots on the secondary storage array, select the **Configure secondary destinations for this job** check box.



6. If you have enabled a secondary destination for the job, at the **Secondary Target** step of the wizard, add replication or archiving features that Veeam Backup & Replication will use to create long-term snapshots in the secondary destination.

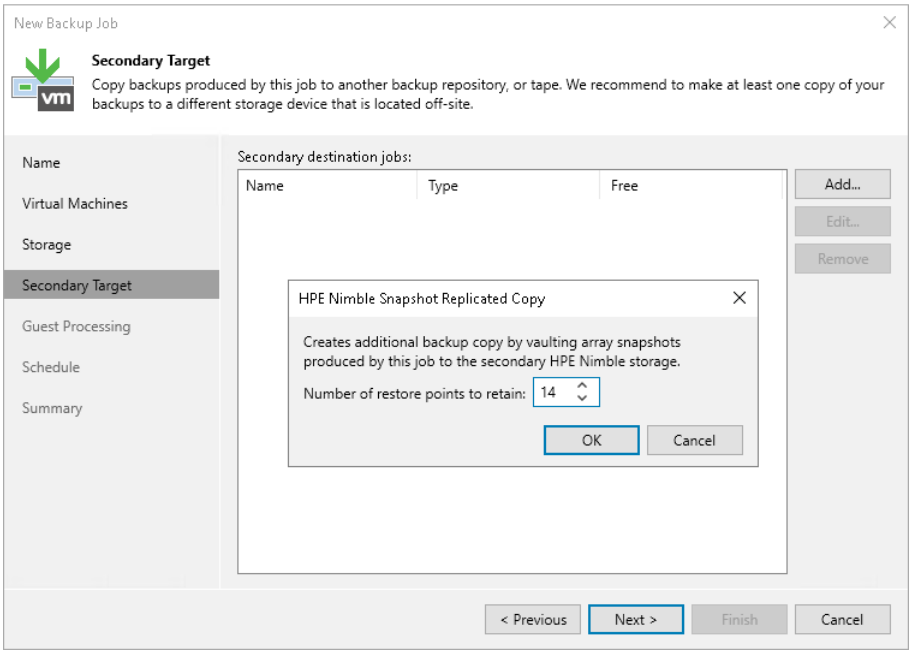
   You cannot select the synchronous replication feature explicitly. Veeam Backup & Replication uses secondary storage arrays with synchronous replication by default if detects the configured ones. In this case, the snapshot retention for both primary and secondary storage arrays is configured at the step 5 of this procedure.

To add other replication or archiving features, click **Add**. In the **Number of snapshot copies to retain** field, specify the number of long-term storage snapshots that you want to maintain in the snapshot chain on the secondary storage array or offload target. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the chain.

[For NetApp SnapMirror] The **Number of snapshot copies to retain** option is not applicable to NetApp SnapMirror. On this secondary storage system, Veeam Backup & Replication maintains the same number of storage snapshots as on primary storage systems. MirrorAndVault Relationships will be identified by Veeam Backup & Replication as SnapVault.

[For NetApp 7-mode] If you use SnapMirror relationships between QTrees, you can define different retention policy settings for the primary NetApp storage system and NetApp SnapMirror. For example, you can configure the backup job to maintain 14 snapshots on the primary NetApp storage system and 10 snapshots of QTree directories on NetApp SnapMirror.

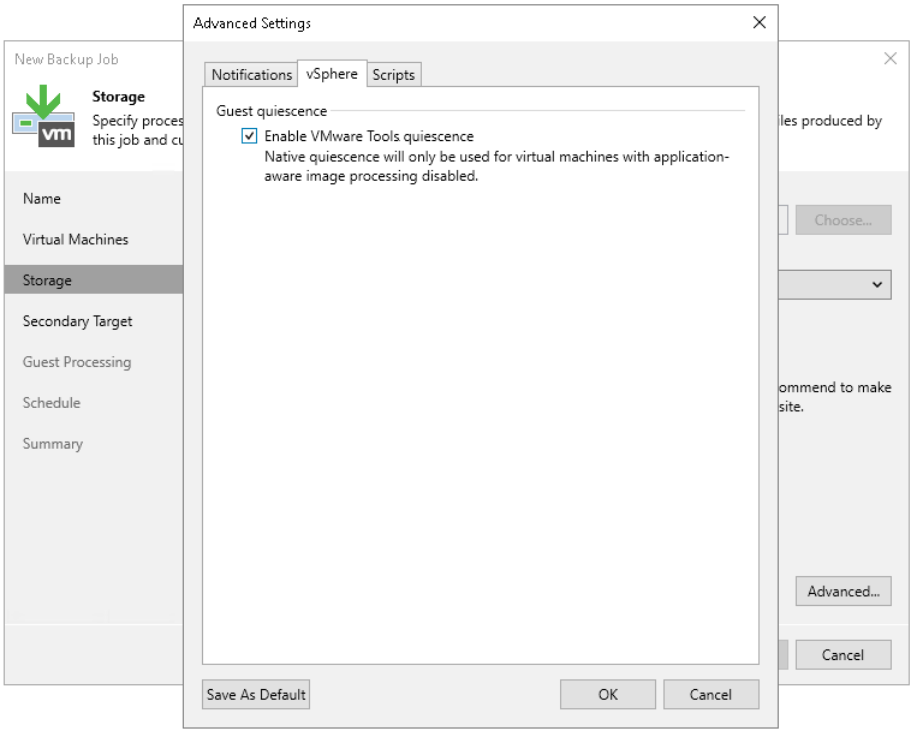
[For HPE 3PAR] The **Number of snapshot copies to retain** option is not applicable to HPE 3PAR Peer Persistence.



7. To create application-consistent long-term storage snapshots, you can enable VMware Tools quiescence or application-aware processing. If you do not enable either of these options, Veeam Backup & Replication will produce a crash-consistent long-term storage snapshot.

   To enable VMware Tools quiescence, in the advanced settings of the backup job select the **Enable VMware Tools quiescence** check box.

Veeam Backup & Replication will create VMware vSphere snapshots for VMs whose disks are hosted on the storage system. After VMware vSphere snapshots are created, Veeam Backup & Replication will trigger a storage snapshot. For more information, see the Specify Advanced Backup Settings section in Veeam Backup & Replication User Guide.

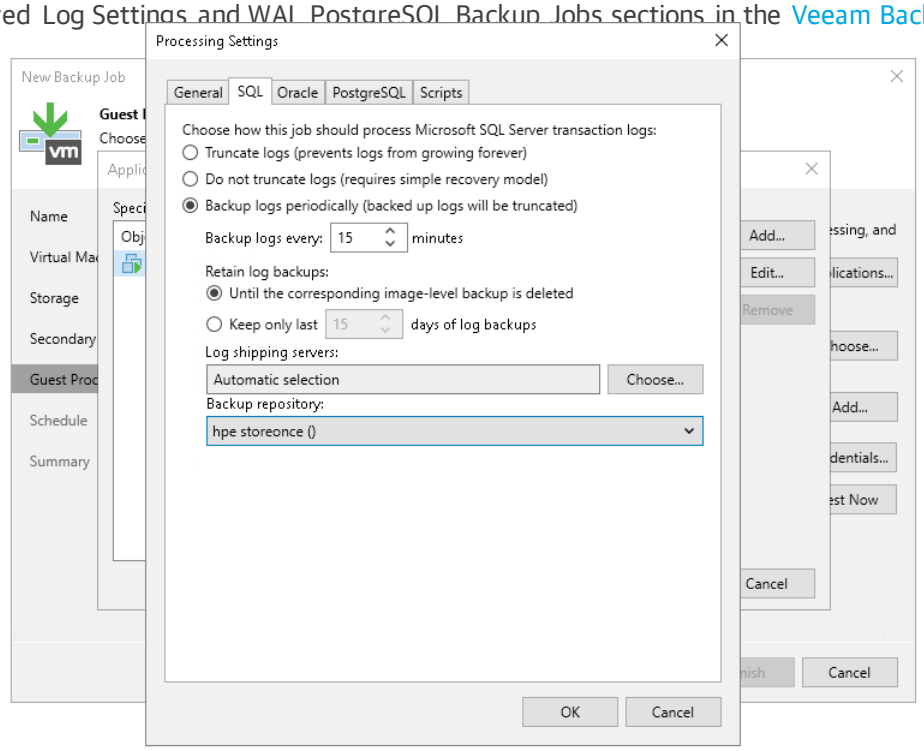


8. You can enable application-aware processing to create a transactionally consistent snapshot. To do so, select the **Enable application-aware processing** check box at the **Guest Processing** step of the wizard. Specify necessary settings for application-aware image processing. For more information on settings, see the Specify Guest Processing Settings section in Veeam Backup & Replication User Guide.

   If you are going to process logs, set a repository for storing them. To do so, after you have selected the **Enable application-aware processing** check box, click **Applications**. Select any VM and click **Edit**. In the **Processing Settings** window, select **SQL**, **Oracle** or **PostgreSQL**. Select **Backup logs periodically** (for Microsoft SQL VMs) or **Backup logs every N minutes** (for Oracle and PostgreSQL VMs). The **Backup repository** field will appear. Choose the backup repository from the drop-down list.

   > **NOTE**
   >
   > You specify the backup repository for the whole job, not just for a VM you have selected.

For more information on log settings, see the Microsoft SQL Server Transaction Log Settings, Oracle Archived Log Settings and WAL PostgreSQL Backup Jobs sections in the Veeam Backup & Replication User Guide.



9. During the job session, Veeam Backup & Replication will quiesce applications running inside VMs using application-aware processing. For more information on how application-aware processing works, see the Application-Aware Processing section in Veeam Backup & Replication User Guide.

   Job session flow:

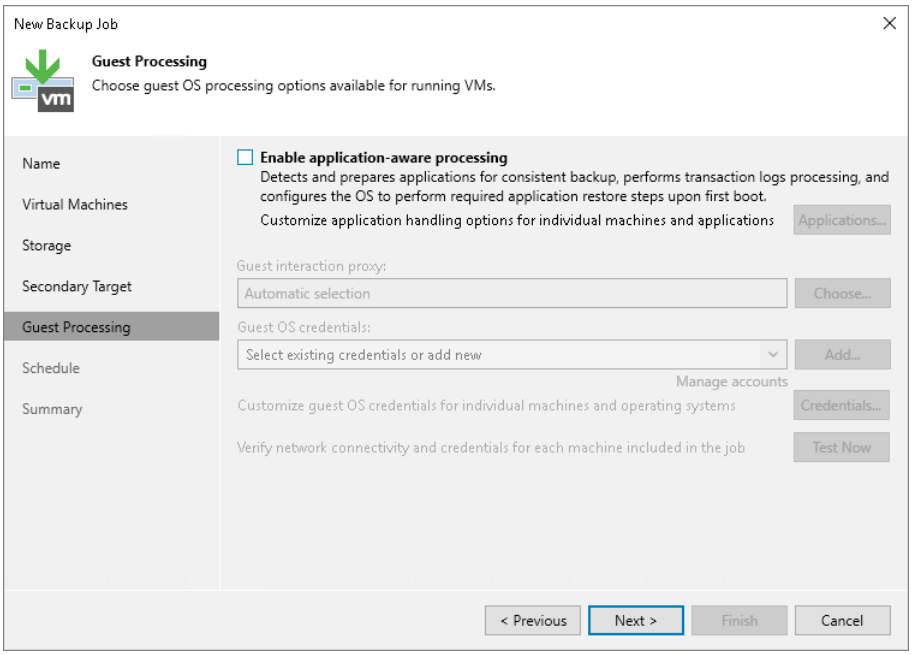
   - Veeam Backup & Replication quiesces applications running inside VMs using application-aware processing (performs VSS freeze).
   - After applications inside the VM are quiesced, Veeam Backup & Replication creates a VMware snapshot. This does not apply to freeze-only VMs.

     A VM is freeze-only if it meets these conditions:

     - The disks of this VM can be located on one or more storage volumes,
     - These storage volumes only contain the disks of this VM. They do not contain the disks of any other VM that are included in the same job.

- Then Veeam Backup & Replication triggers a storage snapshot.

The freeze-only VMs (those VMs for which a VMware snapshot was not created) are processed in successive order after creating storage snapshots for the other VMs.



10. At the **Schedule** step of the wizard, select the **Run the job automatically** check box and specify the schedule by which storage snapshots must be created. For more information, see the Define Job Schedule section in the Veeam Backup & Replication User Guide.

11. At the **Summary** step of the wizard, review settings of the added storage system. Select the **Run the job when I click Finish** check box if you want to start the job right after you finish working with the wizard. Click **Finish** to save the backup job settings.

TIP

To learn which VMs were processed by a snapshot job (a snapshot-only job or a backup job with storage snapshot retention) open the **Storage Infrastructure** view and navigate to the necessary storage snapshot. If a VM was processed by a snapshot job, Veeam Backup & Replication displays the job name in the **Protected by** column.

Backup from Storage Snapshots with Snapshot Retention

You can configure a backup job to create regular backup files in the backup repository and, additionally, maintain a snapshot chain on the storage system. Veeam Backup & Replication lets you create long-term storage snapshots in the following destinations:

- Primary storage array where VM disks are hosted
- Secondary storage arrays

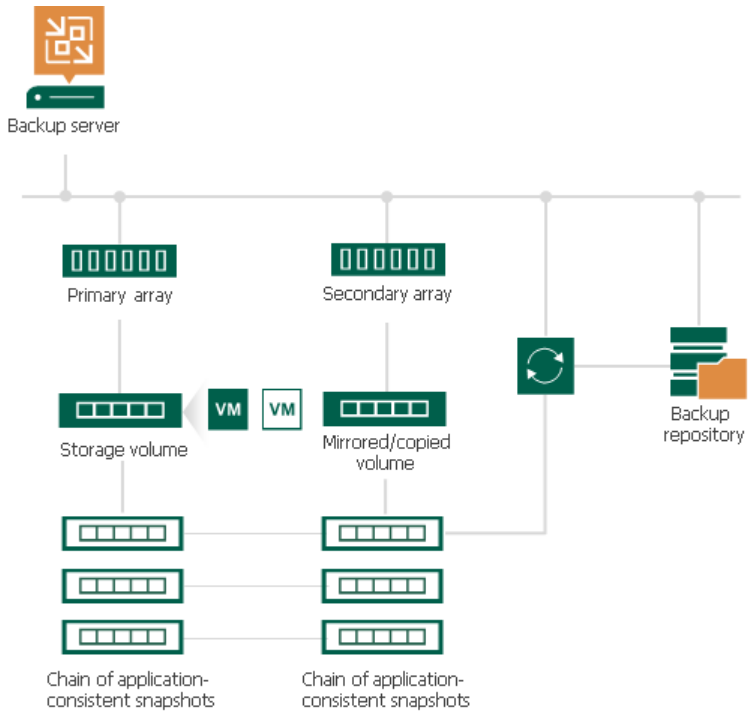
Depending on the backup job settings, the created storage snapshots can be application-consistent or crash-consistent.

How Backup from Storage Snapshots with Snapshot Retention Works

The backup job of this type is performed in the following way:

1. Veeam Backup & Replication triggers the vCenter Server to create a VMware vSphere snapshot for a VM.
2. Veeam Backup & Replication instructs the storage system to create two snapshots of a volume or LUN capturing VM disks:
    - A long-term snapshot on the storage system. This snapshot remains in the snapshot chain until it is removed by the retention policy.
    - A temporary snapshot for backup or replication operations. This snapshot is removed after backup or replication is complete.
3. Veeam Backup & Replication removes the created VMware vSphere snapshot from the VM snapshot list.
4. Veeam Backup & Replication uses the temporary storage snapshot as a data source for backup and replication.
5. Veeam Backup & Replication performs cleanup operations and removes the temporary snapshot on the storage array.

6. Veeam Backup & Replication checks the number of long-term storage snapshots in the snapshot chain. If the number exceeds the value defined in retention policy settings, Veeam Backup & Replication instructs the storage system to remove the earliest snapshot from the snapshot chain.



Configuring Backup Jobs with Storage Snapshot Retention

You can configure a backup job to create backup files and a chain of long-term storage snapshots on the primary storage array, on the secondary storage arrays or both.

Prerequisites

Before you perform backup, configure the backup infrastructure in a proper way:

- You must configure a secondary storage array for the primary storage system where VMs that you plan to back up are hosted.
    - [For HPE Nimble] You must configure Volume Collection replication from the primary storage array to the secondary storage array. For more information, see the HPE Nimble documentation.
    - [For NetApp ONTAP] You must configure volume SnapMirror/SnapVault relationships between the primary and secondary storage arrays. MirrorAndVault Relationships will be identified by Veeam Backup & Replication as SnapVault. For more information, see the NetApp documentation.
    - [For HPE 3PAR Peer Persistence and HPE 3PAR Remote Copy] You must create a Remote Copy Group (RCG) with relevant type (Synchronous or Periodic).
    - Check prerequisites in the following Veeam KB articles: DataCore SANsymphony, Dell PowerMax requirements, Dell PowerStore requirements, Fujitsu ETERNUS AF/DX Series, Hitachi VSP requirements, HPE XP requirements, INFINIDAT InfiniBox F Series, NEC Storage M Series requirements, NEC Storage V Series requirements, NetApp SolidFire/HCI, Pure Storage FlashArray, Tintri IntelliFlash/Western Digital/Tegile.
    - When you add storage arrays to the backup infrastructure, you must add to the rescan scope volumes and LUNs on which VM disks are located (both for primary and secondary storage arrays). For more information, see Adding Storage Systems.

- You must configure the backup infrastructure in a proper way.
  - Add to the backup infrastructure a backup proxy that will be used for backup, and properly configure this backup proxy. For more information, see Configuring Backup Proxy.
  - Add to the backup infrastructure vCenter Server hosts or ESXi hosts with VMs whose disks are hosted on the storage system.
  - Add the primary storage system and secondary storage array to the backup infrastructure.
- You must install a license for Veeam Backup & Replication Enterprise Plus edition on the backup server.
- You must check limitations for Backup from Storage Snapshots. For more information, see Backup from Storage Snapshots.
- [For NetApp ONTAP] You must install a license for storage snapshot export on NetApp SnapMirror or SnapVault. For more information, see Required Licenses for NetApp.

Key Job Settings

The key job settings responsible for Backup from Storage Snapshots with snapshot retention are:

- At the **Storage** step of the wizard, the **Configure secondary destinations for this job**.
- At the **Storage** step of the wizard, in the **Advanced** settings, the **Enable backup from storage snapshots** check box.
- At the **Secondary Target** step of the wizard, the added option to create snapshots on the primary storage array or a feature of a secondary storage array, or both, the **Use as the data source** check box, and the **Number of snapshot copies to retain** field.

Configuring Backup Job with Storage Snapshot Retention

To configure a backup job:

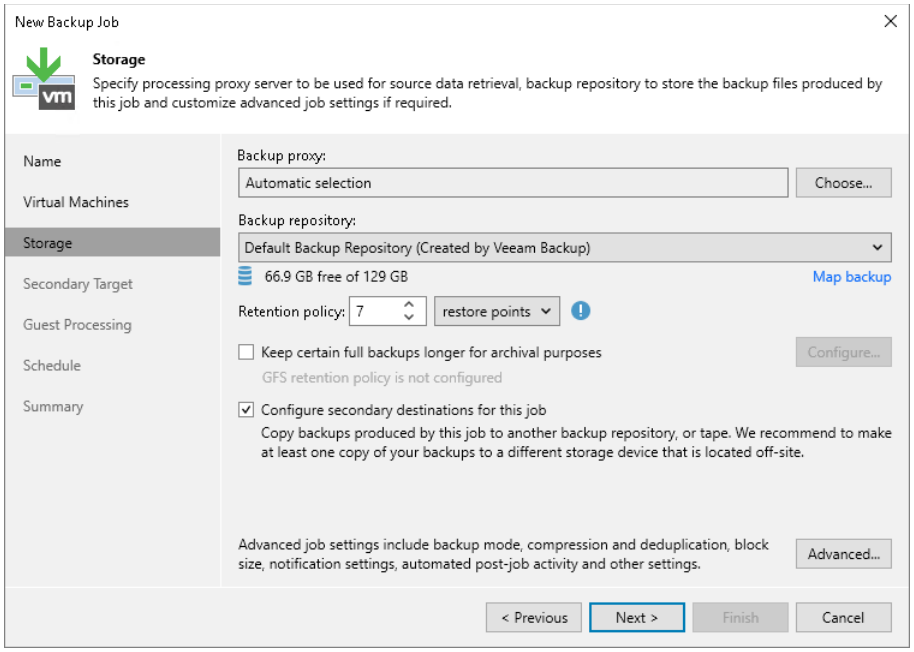
1. Open the **Home** view.
2. Click **Backup Job** > **VMware** or **Cloud Director** on the ribbon. Veeam Backup & Replication will launch the **New Backup Job** wizard.
3. At the **Name** step of the wizard, specify a name and description for the backup job.
4. At the **Virtual Machines** step of the wizard, select VMs whose disks are hosted on a storage system.
5. At the **Storage** step of the backup job wizard, do the following:
   a. Select a backup proxy that will be used for data transfer. You can assign the backup proxy explicitly or choose the automatic mode of backup proxy selection.

> **NOTE**
>
> A backup proxy that you select must be added to the list of backup proxies in storage system connection settings. If the backup proxy is not added to the list in storage system connection settings, Veeam Backup & Replication may fail over to the regular data processing mode. To switch on the failover, at the **Storage** step of the backup or replication job wizard, click **Advanced** and select the **Failover to standard backup** check box.
>
> For more information, see Adding Storage Systems.

b. From the **Backup repository** list, select a backup repository where you want to store backup files.

c. In the **Retention policy** section, specify the number of backup restore points that you want to keep.

d. Select the **Configure secondary destinations for this job** check box.

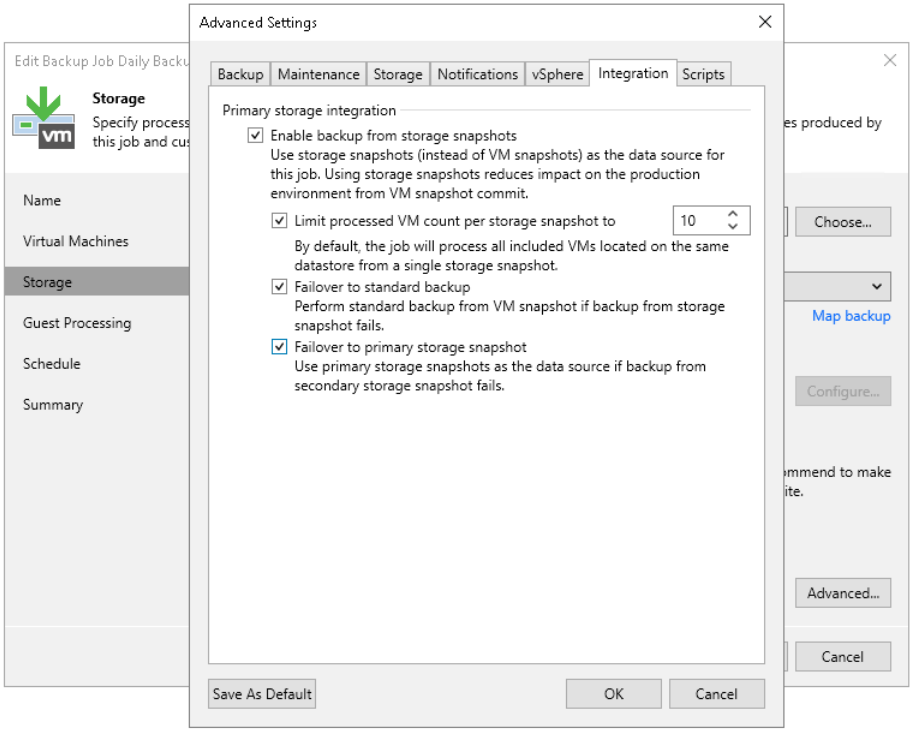


e. Click **Advanced**, then click the **Integration** tab. Make sure that the **Enable backup from storage snapshots** check box is selected. By default, this option is enabled for all newly created jobs.

f. If you add to the job many VMs whose disks are located on the same volume or LUN, select the **Limit processed VM count per storage snapshot to <N>** check box and specify the number of VMs for which one temporary storage snapshot must be created. Veeam Backup & Replication will divide VMs into several groups and trigger a separate temporary storage snapshot for every VM group. As a result, the job performance will increase. For more information, see Limitation on Number of VMs per Snapshot.

g. If Veeam Backup & Replication fails to create a temporary storage snapshot, VMs whose disks are located on the storage system will not be processed by the job. To fail over to the regular data processing mode and back up such VMs, select the **Failover to standard backup** check box.

h. If Veeam Backup & Replication cannot create a temporary storage snapshot on the secondary storage array, the job will not back up VMs whose disks are located to the storage system. To fail over to Backup from Storage Snapshots on the primary storage system, select the **Failover to primary storage snapshot** check box. For more information, see Failover to Backup from Snapshots on Primary Storage Arrays.



6. At the **Secondary Target** step of the wizard, click **Add** and select where to create long-term snapshots, that is, snapshots for a snapshot chain. You can select an option to create snapshots on the primary storage array, using a replication feature of a secondary array, or both. Also, configure the number of snapshots to retain in the snapshot chain and configure which feature to use as the data source for backup operations, if required.

   If you want to create a snapshot chain on the secondary storage array with synchronous replication, you must add an option to create snapshots on the primary storage array and specify the **Number of snapshot copies to retain**. Long-term snapshots will be created simultaneously on the primary and secondary storage arrays, that is, coordinated snapshots will be created. Veeam Backup & Replication will retain the same number or snapshots on both storage arrays. If you also want to use the secondary storage array as a source for backup, add the synchronous replication feature to the list of the used features. Check that the **Use as the data source** check box is enabled.

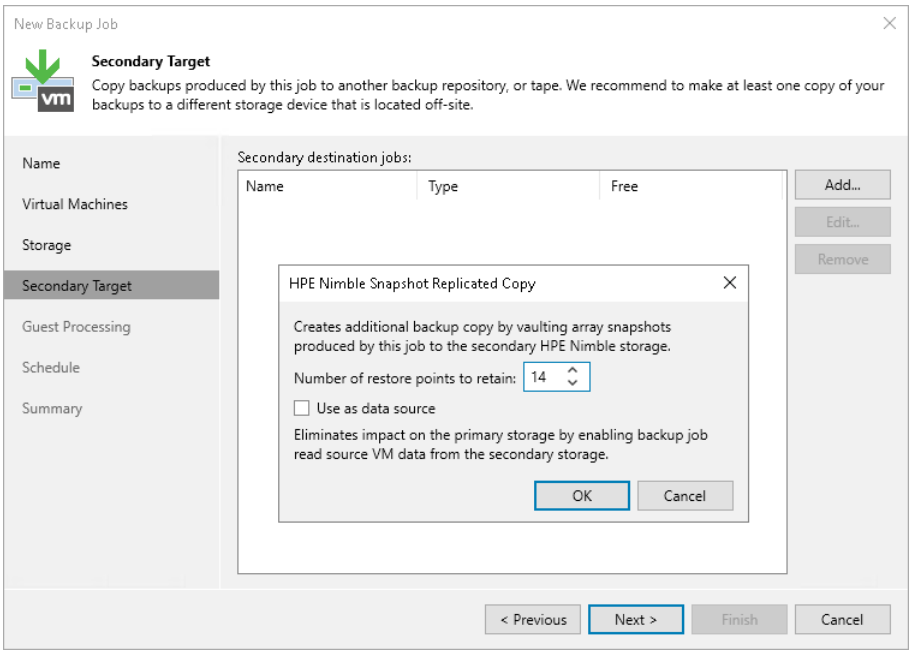
   If you want to create a snapshot chain on the primary storage system or secondary storage system with snapshot transfer or archiving feature, do the following:

   a. Add an option to create snapshots on the primary storage array, snapshot transfer or archiving feature.

   b. In the **Number of snapshot copies to retain** field, specify the number of long-term storage snapshots to retain on the storage array, that is, the number of snapshots in the snapshot chain. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the chain.

      [For NetApp SnapMirror] This option is not applicable. On this secondary storage system, Veeam Backup & Replication maintains the same number of storage snapshots as on primary storage arrays.

c. [For snapshot transfer] Select the **Use as the data source** check box to use the secondary storage array as a source for backups.



7. Specify other backup job settings as required.
8. Click **Next**, then click **Finish** to save the job settings.

> **TIP**
>
> To learn which VMs were processed by a snapshot job (a snapshot-only job or a backup job with storage snapshot retention) open the **Storage Infrastructure** view and navigate to the necessary storage snapshot. If a VM was processed by a snapshot job, Veeam Backup & Replication displays the job name in the **Protected by** column.

Data Recovery from Storage Snapshots

Veeam Backup & Replication lets you restore VMware VM data directly from native storage snapshots. This technology automates the process of data recovery for VMs hosted on storage systems, eliminates intermediate restore and manual operations. As a result, you can restore necessary VM data from storage snapshots in seconds.

The following data recovery methods support data recovery from storage snapshots:

- Instant Recovery
- Instant Disk Recovery
- FAT, NTFS or ReFS Restore
- Linux, Unix and Other File System Restore
- Application item restore

Traditional Restore vs. Restore from Storage Snapshots

Many organizations use storage snapshots for data protection. Storage snapshots allow for very low RPO: they have minimal impact on storage performance and can be created in seconds. You can schedule snapshots to be created several times a day or even every hour.

In virtual environments, restore from storage snapshots can be difficult. Storage snapshots are created per-volume, and a volume typically hosts disks of several VMs. For this reason, restore from storage snapshots is not a simple rollback operation — it is a multi-task process. If restore from storage snapshots is performed manually, you must do the following:

1. Present a storage snapshot to an ESXi host.
2. Perform an HBA rescan.
3. Mount the storage snapshot to an ESXi host.
4. Browse the storage snapshot to locate VM files.
5. Add the VM to the inventory or copy VM files to another VMFS datastore.
6. Power on the VM.
7. Perform restore operations.
8. Perform cleanup operations after VM data restore is complete.

As a result, the restore process takes much time. If you need to restore guest OS files and application objects from a VM on the storage snapshot, the procedure will be even more complicated.

If you recover data from storage snapshots, storage snapshots are mounted to ESXi hosts automatically. You only need to select an ESXi host where the storage snapshot will be mounted, all other operations are performed automatically.

When you restore data from storage snapshots, they are not converted into backups. VM data is restored directly from native storage system snapshots. You do not have to install any agents or perform additional configuration actions.

How Restore from Storage Snapshots Works

For restore operations, Veeam Backup & Replication uses a copy of the volume snapshot, not the volume snapshot itself.

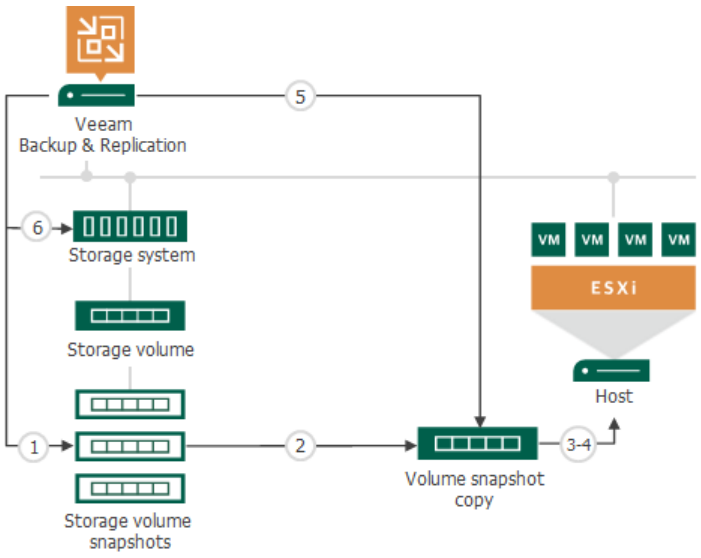
The volume snapshot copy is a read-write clone of the volume snapshot. The volume snapshot copy protects the volume metadata integrity on the volume snapshot. During file-level restore and Instant Recovery, the ESXi host where the volume snapshot is mounted updates metadata on the volume snapshot. Use of the volume snapshot copy helps protect the volume snapshot from these changes.

When you restore VM data from storage snapshots, Veeam Backup & Replication performs the following actions:

1. User starts the restore process for a VM on the storage snapshot.
2. Veeam Backup & Replication triggers the storage system to create a copy or a clone of this storage snapshot.
   - If you restore several VMs from one storage snapshot, Veeam Backup & Replication does not create several snapshot copies. Instead, it uses one snapshot copy for restore.
   - If you start several restore operations (for example, Instant Recovery and VM guest OS restore) for the same VM from the storage snapshot, Veeam Backup & Replication creates several snapshot copies and works with them during restore.
3. User selects an ESXi host in the virtual environment, and the created snapshot copy is presented to this ESXi host as a new volume. The ESXi host is added to the list of *Allowed Servers* for the snapshot copy. As a result, the ESXi host has access to the snapshot copy and can read and write data to/from it.
4. [For iSCSI protocol] Veeam Backup & Replication makes sure that the IP address of the storage system is in the list of static targets on the ESXi host.

   [For iSCSI and FC protocols] The storage system issues an HBA rescan command to the vCenter Server. Once rescan is finished, the snapshot copy appears in the discovered targets list on the ESXi host. After that, the storage system performs re-signature for storage volumes.

   [For NFS protocol] The datastore gets registered on the ESXi host through the IP address or FQDN + share name.
5. User performs necessary restore operations in the Veeam Backup & Replication console.
6. After restore is completed, Veeam Backup & Replication issues a command to the storage system. The storage system deletes the snapshot copy from the ESXi host and performs cleanup operations.



Instant Recovery from Storage Snapshots

You can instantly recover a VM from a storage snapshot without prior de-staging and intermediate restores. Instant Recovery accelerates VM restore, improves RTOs and decreases downtime of production VMs.

Prerequisites for Instant Recovery from Storage Snapshots

Before you perform Instant Recovery, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for data recovery from storage snapshots.
- If you recover a VM to the production network, make sure that the original VM is powered off to avoid conflicts.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESXi host, you must register the ESXi host with a WWN ID on the storage system.
- [For NetApp ONTAP storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see Required Licenses for NetApp.

Performing Instant Recovery from Storage Snapshots

For more information on performing Instant Recovery, see the Performing Instant Recovery to VMware vSphere section in Veeam Backup & Replication User Guide.

Instant Disk Recovery from Storage Snapshots

You can instantly recover a VM disk from a storage snapshot without prior de-staging and intermediate restores. Instant Disk Recovery accelerates VM restore, improves RTOs and decreases downtime of production VMs.

> **NOTE**
>
> First Class Disks (FCD) are not supported for Instant Disk Recovery from storage snapshots.

Prerequisites for Instant Disc Recovery from Storage Snapshots

Before you perform Instant Disk Recovery, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for data recovery from storage snapshots.
- If you recover a VM disk to the existing disk, this will delete the existing disk.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESXi host, you must register the ESXi host with a WWN ID on the storage system.
- [For NetApp ONTAP storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see Required Licenses for NetApp.

Performing Instant Disk Recovery from Storage Snapshots

For more information on performing Instant Disk Recovery, see the Performing Instant Disk Recovery section in Veeam Backup & Replication User Guide.

FAT, NTFS or ReFS Restore from Storage Snapshots

You can restore VM guest OS files from a storage snapshot. Veeam Backup & Replication supports file-level restore for the following Microsoft Windows file systems:

- FAT
- NTFS
- ReFS

When you perform guest OS file restore, you select an ESXi host in the virtual environment. Veeam Backup & Replication creates a clone of the storage snapshot where the VM disks are hosted, and mounts the clone to the selected ESXi host as a new datastore.

Veeam Backup & Replication accesses the configuration file of the VM (VMX) on the mounted clone and uses this configuration file to register a temporary VM on the ESXi host. Disks of the restored VM are mounted to this temporary VM. After disks are mounted, you can copy VM guest OS files and folders to their original location, local machine drive or save them in a network shared folder.

Prerequisites for FAT, NTFS or ReFS Restore from Storage Snapshots

Before you restore VM guest OS files from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for data recovery from storage snapshots.
- If you plan to restore VM guest OS files to their original location, you must make sure that VMware tools are installed on the target VM.
- If you plan to restore guest OS files from a VM running Microsoft Windows ReFS, the Veeam Backup & Replication console must be installed on a machine running Microsoft Windows Server 2012 or later.
- If you plan to restore files from a VM running Microsoft Windows Server 2012 or later, and data deduplication is enabled for some VM volumes, the Veeam Backup & Replication console must be installed on a machine running Microsoft Windows Server 2012 or later. Data deduplication must be enabled on this machine.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to the ESXi host, you must register the ESXi host with a WWN ID on the storage system.
- [For NetApp ONTAP storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see Required Licenses for NetApp.

Performing Instant Recovery from Storage Snapshots

For more information on performing restore from FAT, NTFS or ReFS, see the Restoring VM Guest OS Files (NAT, NTFS or ReFS) section in Veeam Backup & Replication User Guide.

Linux, Unix and Other File System Restore from Storage Snapshots

You can restore VM guest OS files from a storage snapshot. Veeam Backup & Replication supports file-level restore for the most commonly used file systems on Linux, Solaris, BSD, Unix and Micro Focus OES. For the full list of supported file systems, see the Platform Support section of the in the Veeam Backup & Replication User Guide.

How Restore Works

When you perform guest OS file restore, Veeam Backup & Replication provides the following options for mounting VM disks from a snapshot:

- Mounting disks to a helper host. As a helper host, you can select the target host where you want to restore files from the snapshot or any other Linux server. We recommend you to specify the same server to which you want to restore the files. This will improve the performance.
- Mounting disks to a helper appliance. The helper appliance is a helper VM running a stripped down Linux kernel that has minimal set of components. The appliance is quite small — around 50 MB. It requires 2048 MB RAM and 2 CPU.

When you perform file-level restore, Veeam Backup & Replication does the following:

1. On an ESXi host in your virtual environment, Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot where the VM disks are hosted. Veeam Backup & Replication mounts the clone/virtual copy to the selected ESXi host as a new datastore.
2. [If you have selected to mount disks to a helper appliance] Veeam Backup & Replication copies an ISO of the helper appliance to the datastore and starts the helper appliance.
3. Veeam Backup & Replication mounts the restored VM disks to the helper appliance or helper host as virtual hard drives. VMDK files are mounted directly from storage snapshots.
4. After disks are mounted, Veeam Backup & Replication launches the Veeam Backup browser where mounted VM disks are displayed. In the browser, you can restore files and folders to their original location, local machine drive or save them in a network shared folder.
5. Depending on which restore command you use, the operations differ:
   - You select the **Restore** or **Restore to** command to restore files to the original location or to another VMware vSphere VM.

     The helper host or helper appliance connects to the VM to which you restore files (target VM) over SSH or VIX API/vSphere Web Services if a connection over SSH cannot be established. Then Veeam Backup & Replication deploys on the VM the agent which performs restore.
   - If you restore files to a new location, select the **Copy to** command.

     The helper host or helper appliance connects to the VM to which you restore files (target VM) over the network. Then Veeam Backup & Replication deploys on the VM the agent which performs restore.
6. When the restore process is finished, Veeam Backup & Replication deletes the datastore, unmounts the clone/virtual copy from the ESXi host and then deletes this copy.
7. [If you have selected to mount disks to a helper appliance] Veeam Backup & Replication unregisters the helper appliance.

Prerequisites for FAT, NTFS or ReFS Restore from Storage Snapshots

Before you restore VM guest OS files from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for data recovery from storage snapshots.
- If you plan to restore VM guest OS files to their original location, make sure that VMware Tools are installed on the target VM.
- Veeam Backup & Replication restores ACL for recovered VM guest OS files. To let Veeam Backup & Replication detect the target Linux system architecture and kernel version, make sure that arch and uname are installed on the VM guest OS.
- Veeam Backup & Replication must have access to the guest OS of the target VM to be able to deploy a coordination process. The coordination process performs a number of administrative actions on the target VM guest OS, for example, collects information about mount points.
- The mount server, whether it is a helper host or a helper appliance, must have access over a network to a VM whose files you restore or direct access to vCenter or ESXi host where the VM resides. If the mount server is connected to a VM whose files you restore through VIX API/vSphere Web Services, you must use a root account for a target VM, otherwise the restore process will fail.
- For Linux target VM, consider the following:
  - If you want to restore files over network, make sure that the SSH daemon is configured and SCP utility is available on the target VM.
  - SELinux must be disabled on the target VM.
  - A range of ports that are used for data transfer must be open on the target VM.

    For more information on configuring connection settings for Linux servers, see the Specify Credentials and SSH Settings step of the **New Linux Server** wizard in the Veeam Backup & Replication User Guide.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESXi host, you must register the ESXi host with a WWN ID on the storage system.
- [For NetApp ONTAP storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see Required Licenses for NetApp.

Performing Linux, Unix and Other File System Restore from Storage Snapshots

For more information on performing restore from Linux, Unix and other file systems, see the Restoring VM Guest OS Files (Multi-OS) section in Veeam Backup & Replication User Guide.

Application Item Restore from Storage Snapshots

Veeam Backup & Replication integrates with Veeam Explorers to let you restore items from the following applications:

- Microsoft Active Directory
- Microsoft Exchange

- Microsoft SharePoint
- Microsoft SQL Server
- Oracle
- PostgreSQL

When you perform application item restore, Veeam Backup & Replication automatically extracts the application databases from a storage snapshot and opens them in Veeam Explorer.

As part of this procedure, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication creates a clone/virtual copy of a storage snapshot and mounts the clone/virtual copy to an ESXi host.
2. Veeam Backup & Replication accesses the configuration file of the virtualized application server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESXi host.
3. Veeam Backup & Replication mounts disks of the application server to the temporary VM.
4. Veeam Backup & Replication locates the application databases and opens them in Veeam Explorer.

Before you restore application items from a storage snapshot, check prerequisites.

Before you start restoring application items with Veeam Explorer, extract application databases from the storage snapshot.

After you extract the application databases, you can proceed to the restore process in Veeam Explorer. To learn more about application item restore, see the following sections in Veeam Explorers User Guide:

- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft SQL Server
- Veeam Explorer for Oracle
- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for PostgreSQL

Before You Begin

Before you restore application items from a storage snapshot, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for data recovery from storage snapshots.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESXi host, you must register the ESXi host with a WWN ID on the storage system.
- [For NetApp ONTAP storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see Required Licenses for NetApp.

Extracting Application Databases

Before you start restoring application items with Veeam Explorer, you need to extract application databases from a storage snapshot. You can do it in two ways:

- You can use the wizard. In this case, Veeam Backup & Replication will automatically extract application databases from a storage snapshot and open it in Veeam Explorer. For more information, see Using Application Item Extract Wizard.
- You can restore VM guest OS files from a backup of a virtualized application server, manually locate application databases in Veeam Backup browser, double-click the database file, click **Application Items** and then select the application on the ribbon. For more information on performing guest OS file restore, see the Guest OS File Restore section in Veeam Backup & Replication User Guide.

Using Application Item Extract Wizard

Before you restore application items from a storage snapshot, check prerequisites. Then use the wizard to extract the application databases.

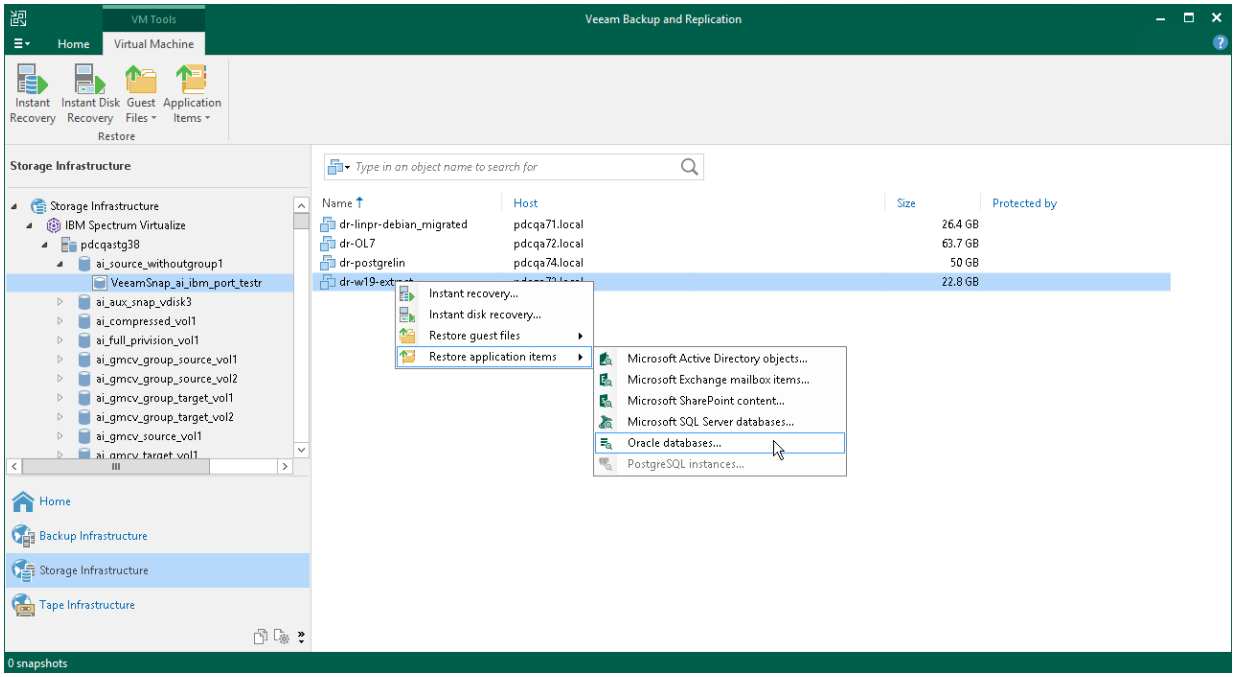
1. Launch the wizard.
2. Select a VM.
3. Select a restore point.
4. Select an ESXi host for snapshot mounting.
5. Specify a restore reason.
6. Open the application database in Veeam Explorer.

Step 1. Launch Application Item Extract Wizard

To launch the wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware vSphere** > **Restore from backup** or **Restore from replica** > **Application items restore** and then select the application.
- Open the **Storage Infrastructure** view. In the inventory pane, select the volume snapshot. In the working area, select the VM, click **Application Items** and then select the application. You can also right-click the VM, select **Restore application items** and then select the application. In this case, you will go immediately to the Location step of the wizard.
- Open the **Home** view. In the inventory pane, select **Storage snapshots**. In the working area, expand the volume, select the VM, click **Application Items** and then select the application. You can also right-click the VM, select **Restore application items** and then select the application. In this case, you will go immediately to the Restore Point step of the wizard.

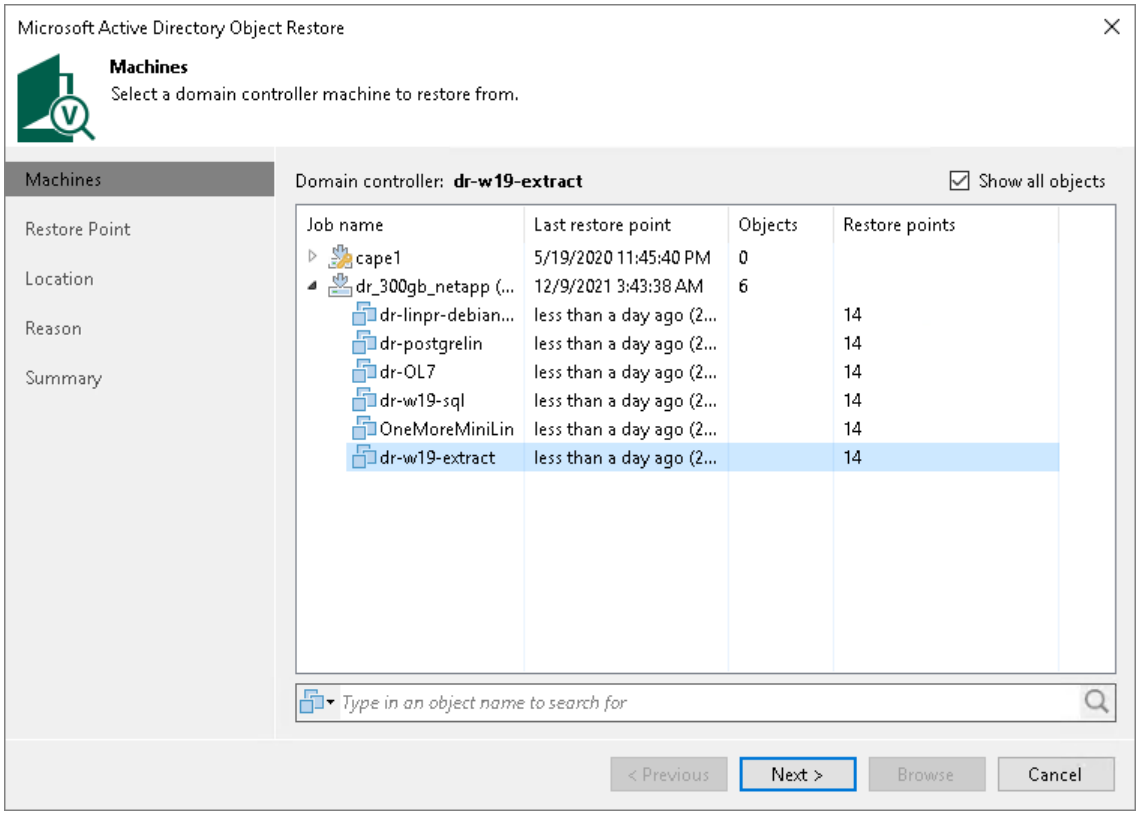
To quickly find a VM, you can use the search field at the top of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.



Step 2. Select VM

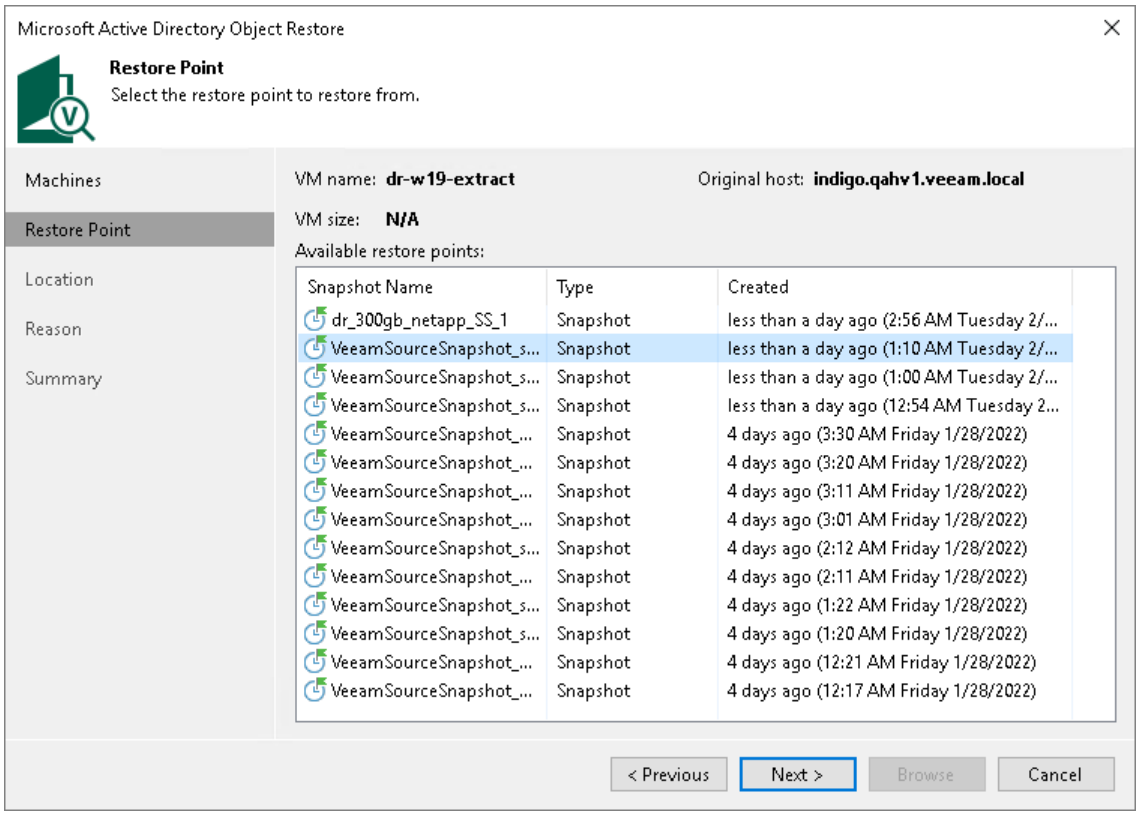
At the **Machines** step of the wizard, Veeam Backup & Replication displays all VMs whose disks are located on the storage system. Select the VM from the list. If the necessary VM is not displayed in the list, select the **Show all VMs** check box. Veeam Backup & Replication will display all VMs whose disks are located on the storage system.

To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.



Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to extract the application databases. Every storage snapshot acts as an independent restore point.

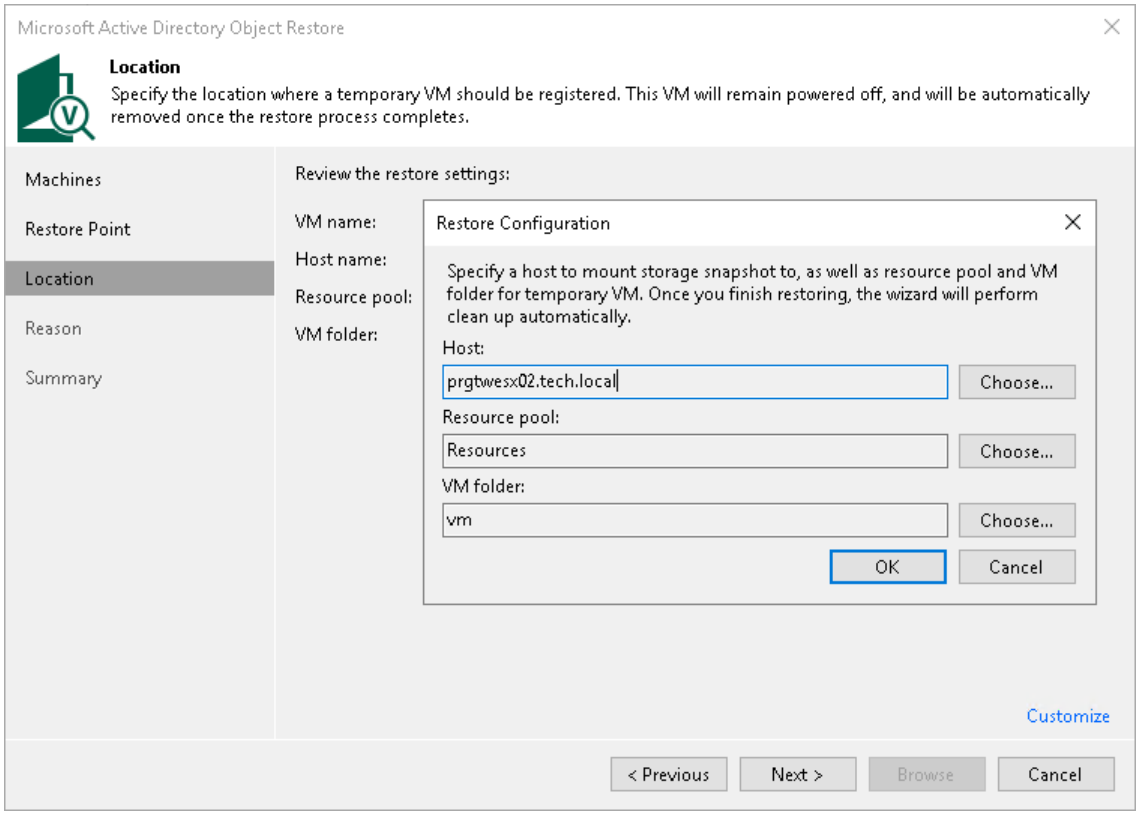


Step 4. Select ESXi Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESXi host where the clone/virtual copy of the storage snapshot must be mounted. On the selected ESXi host, Veeam Backup & Replication will create a temporary VM and mount disks of the virtualized application to this temporary VM.

To specify a destination for the snapshot clone/virtual copy and temporary VM:

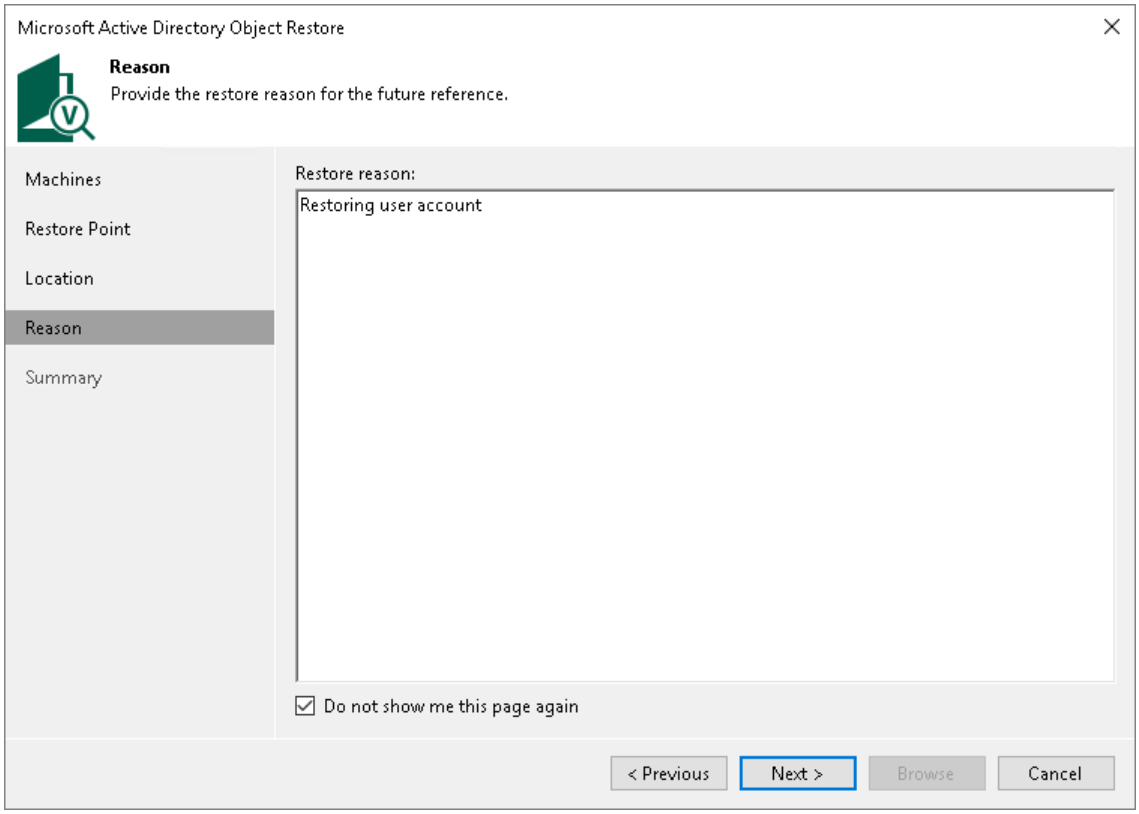
1. At the **Location** step of the wizard, click **Customize**.
2. Next to the **Host** field, click **Choose** and select an ESXi host where the snapshot clone/virtual copy must be mounted and where the temporary VM must be created.
3. Next to the **Resource pool** field, click **Choose** and select a resource pool where you want to place the temporary VM.
4. Next to the **Folder** field, click **Choose** and select a folder where you want to place the temporary VM.
5. Click **OK**.



Step 5. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the application databases. The information you provide will be saved in the session history, and you will be able to view it later.

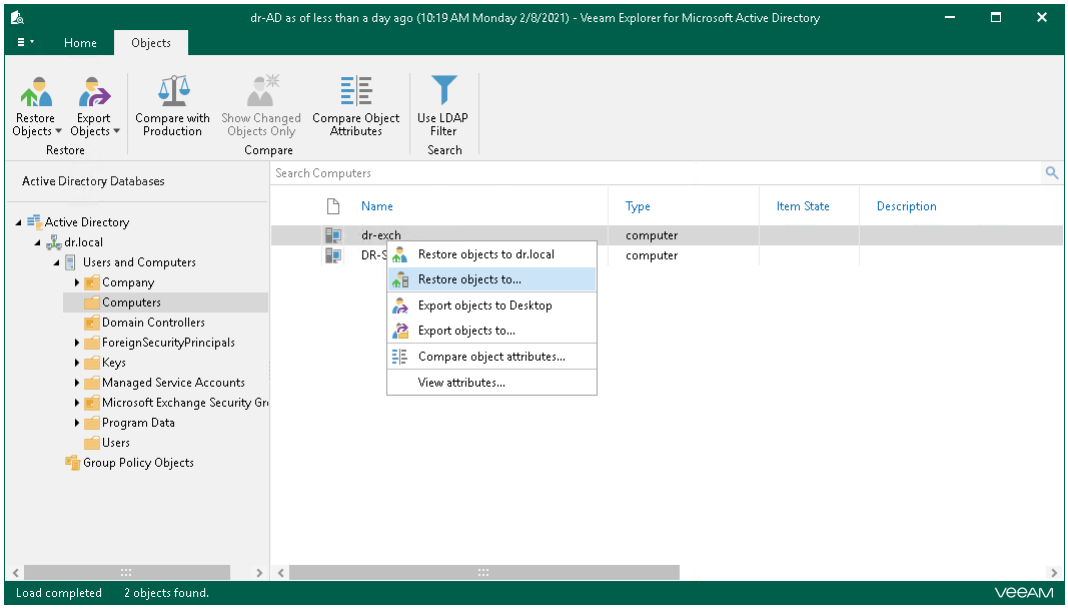
If you do not want to see this step in future, select the **Do not show me this page again** check box.



Step 6. Open Application Databases in Veeam Explorer

At the **Summary** step of the wizard, click **Browse** to start the restore process.

Veeam Backup & Replication will automatically locate the application databases and open it in Veeam Explorer. You can browse the databases and restore the items that you need.



Retrieving Archived Snapshots

To access data from archived snapshots, you must first retrieve the snapshot. During the snapshot retrieval process, a copy of the archived snapshot is created on the storage system from which the snapshot was archived (offloaded). This copy is stored on the storage system until you delete the copy manually as described in Deleting Snapshots.

Data retrieval is required if you want to restore workloads from archived snapshots. Archived snapshots are shown under the icon.

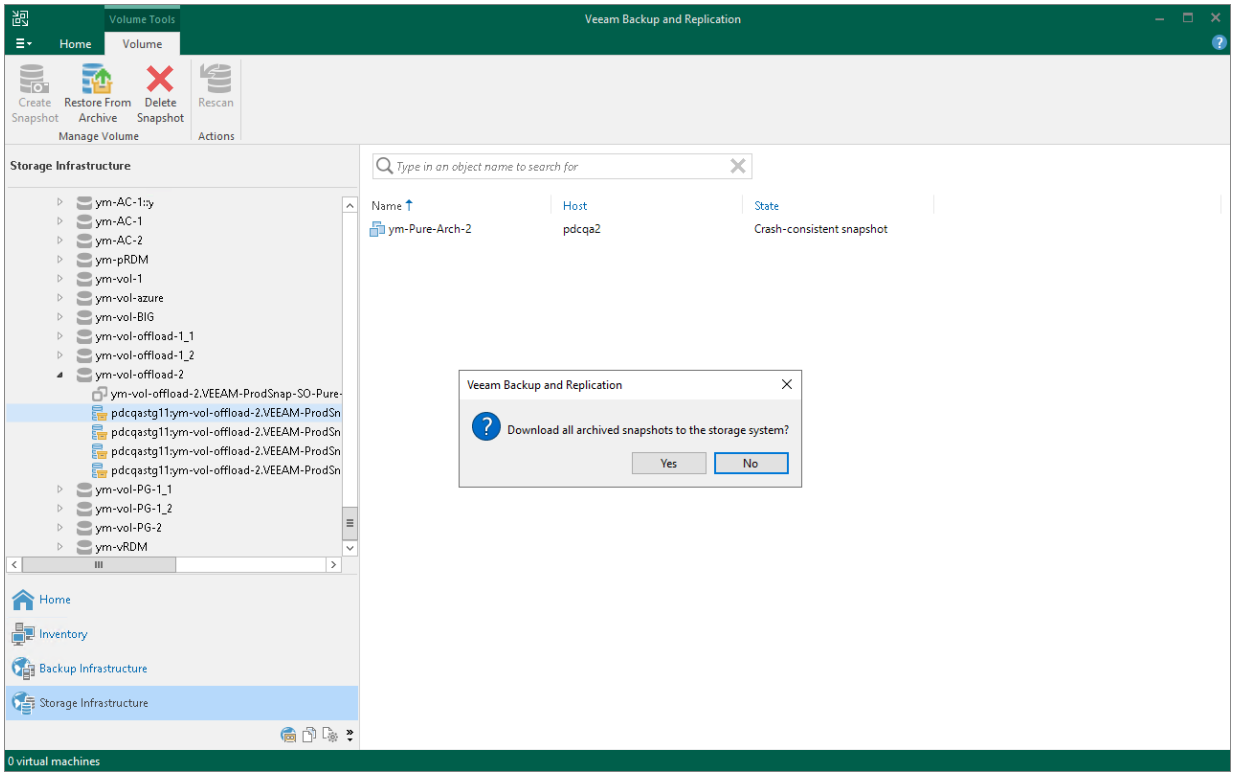
Veeam Backup & Replication supports retrieving data from snapshots archived from the Pure Storage FlashArray storage system using Offload functionality.

To retrieve an archived snapshot:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the storage system tree.
3. Right-click the necessary snapshot and select **Restore from archive**. Alternatively, you can click **Restore from Archive** on the ribbon.
4. In the **Veeam Backup & Replication** window, click **Yes**.

After the retrieval finishes, Veeam Backup & Replication will show the retrieved snapshots under the icon.

> **NOTE**
>
> Consider the following:
>
> - One archived snapshot can have only one retrieved copy. You can retrieve the archived snapshot again only after you delete the retrieved copy as described in Deleting Snapshots.
> - Snapshot retention does not apply to retrieved snapshots.



Creating and Deleting Snapshots

You can create and delete storage snapshots in the Veeam Backup & Replication console. The create/delete snapshot operations do not differ from operations that you perform in the management console of the storage system.

Creating Snapshots

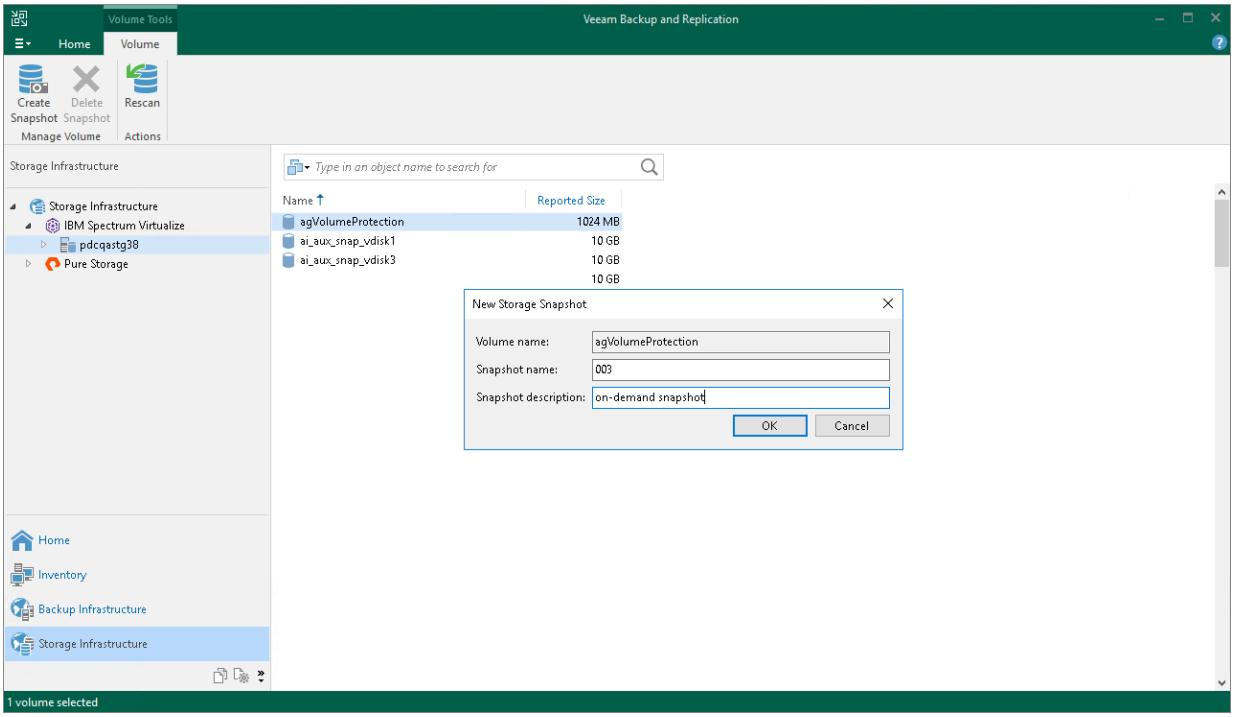
To create a volume snapshot:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the storage system tree.
3. Right-click the necessary volume and select **Create Snapshot**.
4. In the **New Storage Snapshot** window, specify a name for the created snapshot and provide a description for the snapshot (if the snapshot description field is available).
5. [For HPE StoreVirtual/LeftHand/P4000 series] To quiesce VMs on the volume, select the **Create application-managed snapshot** check box. The storage system will trigger a command to the vCenter Server to quiesce VMs with VMware Tools. VM quiescence will bring VM data to a consistent state before the snapshot is taken. If the **Create application-managed snapshot** option is not enabled, Veeam Backup & Replication will trigger a point-in-time snapshot.

NOTE

Consider the following:

- To create application-managed snapshots on HPE StoreVirtual/LeftHand/P4000 series, make sure that Application Aware Snapshot Manager is properly installed and configured. If the Application Aware Snapshot Manager is not installed, Veeam Backup & Replication will report an error, and the snapshot will not be created. For more information, see HPE StoreVirtual Application-Aware Snapshot Manager Deployment Guide.
- [For storage systems with synchronous replication] Veeam Backup & Replication does not trigger a storage system to replicate snapshots created manually. However, the storage system itself can replicate the snapshot.

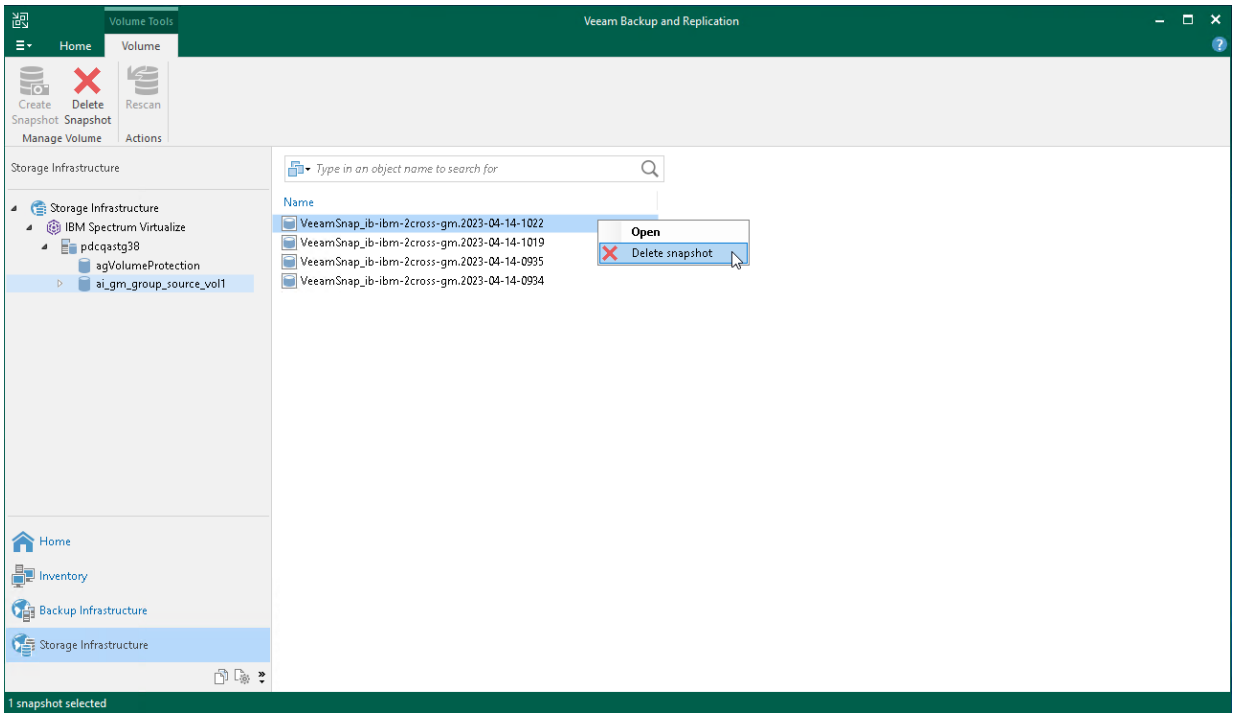


Deleting Snapshots

To delete a volume snapshot:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the storage system tree.

3. Right-click the necessary snapshot and select **Delete snapshot**.



NAS Integration

Veeam Backup & Replication allows you to integrate your storage systems with NAS file shares residing on them into your infrastructure. For more information, see the Adding Enterprise Storage System as NAS Filer section of the Veeam Backup & Replication User Guide.

To start working with storage systems, you must properly configure the backup infrastructure. For more information, see Backup Infrastructure for Storage Integration. After that, you can use storage snapshots for data protection and disaster recovery operations.

You can perform NAS file share backup from storage snapshots and storage rescan for the following storage systems:

- Dell PowerScale (formerly Isilon)
- Lenovo ThinkSystem DM Series
- NetApp ONTAP
- Nutanix Files Storage

NAS File Share Backup from Storage Snapshots

For backup from storage snapshots, Veeam Backup & Replication uses storage snapshots as a source of data for backup.

During backup from storage snapshots, Veeam Backup & Replication triggers a storage snapshot of the volume where the NAS file share is located.

Veeam Backup & Replication performs file share backup to the backup storage in the following way:

1. When a new backup job session starts, Veeam Backup & Replication triggers a storage snapshot.
2. Veeam Backup & Replication assigns a file proxy to process the file share data.
3. The file proxy enumerates files and folders on the file share and creates a cyclic redundancy check (CRC) tree.
4. The file proxy transfers the CRC tree to the cache repository.
5. The cache repository saves the CRC tree.

   When the cache repository receives a new CRC tree structure from the proxy, it compares it with the CRC tree created during the previous run of the backup session. If any files or folders of the file share have changed since the previous backup session run, the cache repository instructs the file proxy to start reading changed data from the source file share.
6. The file proxy reads new data from the file share.
7. The file proxy creates data packages and transfers them to the target backup repository.

   Data packages comprise backup data files (each 64 MB in size) and metadata files that contain names and versions of backup files and allocation of data in backup files.
8. Veeam Backup & Replication checks file versions in the backup repository against retention settings and moves backup data from the backup repository to the archive repository if necessary.
9. Veeam Backup & Replication deletes the storage snapshot.

For Dell PowerScale (formerly Isilon) and Nutanix Files Storage: File Change Tracking

You have an option to use the file change tracking technology provided by the NAS manufacturer. It lets you speed up the backup operation. For information on the file change tracking technology setup, see the **Specify File Share Processing Settings** step of the **New File Share** wizard in the Veeam Backup & Replication User Guide.

In this case, Veeam Backup & Replication performs file share backup to the backup storage in the following way:

1. When a new backup job session starts, Veeam Backup & Replication triggers a storage snapshot.
2. [For all job sessions after the first one] Veeam Backup & Replication requests the storage system to return the difference between current and previous snapshots.
3. Veeam Backup & Replication assigns a file proxy to process the file share data.
4. The file proxy enumerates files and folders on the file share and creates a cyclic redundancy check (CRC) tree.
5. The file proxy transfers the CRC tree to the cache repository.

6. The cache repository saves the CRC tree.

   When the cache repository receives a new CRC tree structure from the proxy, it compares it with the CRC tree created during the previous run of the backup session. If any files or folders of the file share have changed since the previous backup session run, the cache repository instructs the file proxy to start reading changed data from the source file share.

7. The file proxy reads new data from the file share.
8. The file proxy creates data packages and transfers them to the target backup repository.

   Data packages comprise backup data files (each 64 MB in size) and metadata files that contain names and versions of backup files and allocation of data in backup files.

9. Veeam Backup & Replication checks file versions in the backup repository against retention settings and moves backup data from the backup repository to the archive repository if necessary.
10. [For all job sessions after the first one] Veeam Backup & Replication deletes the previous storage snapshot, keeping the newest storage snapshot.

Veeam Agent Integration

Veeam Backup & Replication allows you to integrate your storage systems with Veeam Agent for Microsoft Windows installed on computers in your infrastructure. For more information, see the Backup from Storage Snapshots section in the Veeam Agent Management Guide.

To start working with storage systems, you must properly configure the backup infrastructure. For more information, see Backup Infrastructure for Storage Integration. After that, you can use storage snapshots for data protection and disaster recovery operations.

For requirements and limitations for Veeam Agent integration, see Considerations and Limitations section in the Veeam Agent Management Guide.

For information on how backups from storage snapshots are created, see the Storage Snapshots Support section in the Veeam Agent Management Guide.

You can perform backup from storage snapshots and storage rescan for the following storage systems:

- Dell Unity XT/Unity, VNX(e)
- Fujitsu ETERNUS HX/AX
- HPE 3PAR StoreServ
- HPE Nimble
- HPE Primera
- HPE StoreVirtual/LeftHand/P4000 series
- IBM N series
- IBM FlashSystem (StorWize), IBM SVC, Lenovo Storage V Series
- Lenovo ThinkSystem DM Series
- NetApp FAS/AFF/ASA, FlexArray (V-Series)
- Universal Storage API Integrated Systems

Backup Infrastructure for Storage Integration

Before you start working with storage systems in Veeam Backup & Replication, you must properly configure the backup infrastructure. As part of this process, you must perform the following actions:

1. Configure a backup proxy. The backup proxy is required for storage systems rescan and backup from storage snapshots.
2. Add storage systems. You must add the storage systems on which the backup data is hosted to the backup infrastructure. If you plan to work with secondary storage arrays, you must add them to the backup infrastructure as well.

Check the prerequisites for a specific storage systems before you add a storage system to your backup infrastructure.

Configuring Backup Proxy for Storage Integration

For some operations with storage snapshots, Veeam Backup & Replication requires a backup proxy. The backup proxy is used for two purposes:

- Rescan (storage discovery) process on storage volumes
- Backup from storage snapshots

For some operations with storage snapshots, Veeam Backup & Replication requires a backup proxy. The backup proxy is used for the Rescan (Storage Discovery) Process on storage volumes.

When Veeam Backup & Replication performs rescan and backup operations, it needs to read the content on storage volumes and snapshots. To do this, Veeam Backup & Replication uses a backup proxy as a helper. Storage volumes and snapshots are mounted as new volumes to the backup proxy. As a result, Veeam Backup & Replication can access mounted volumes and snapshots over the backup proxy and read the backup data from them.

General Requirements

- For VMware integration
  - You must assign to a Microsoft Windows or a Linux machine the role of a backup proxy. This can be a dedicated machine or backup server performing the role of the default backup proxy.
  - [For Linux proxies] We recommend that you add only one proxy to one initiator group. Otherwise, you may encounter issues on proxies with the number of devices that correspond to storage snapshot clones. During the backup process, devices may be unintentionally created on all proxies added to the initiator group, for example, if two backup jobs that use proxies from the initiator group work simultaneously. The created devices will be accumulated.
  - For backup from storage snapshots, the transport mode for VMware backup proxy must be set to **Automatic selection** or **Direct storage access**.
  - For backup from storage snapshots, access to the production volumes is not required. Backup proxy only accesses the snapshot/clone of the production datastore to read the data.
  - For Linux backup proxy, to check compatibility with a storage system, see the system requirements provided by the storage system vendor.
- The backup proxy and the storage system must support the same IP version.
- [For VMware and Veeam Agent integration] For HPE 3PAR, if storage LUNs reside in a virtual domain, the backup proxy to which LUNs are exported must reside in the same virtual domain. If LUNs reside outside a virtual domain, the backup proxy must also reside outside any available virtual domain.
- [For Veeam Agent and NAS integration] Check requirements for the general-purpose backup proxy. For more information, see the General-Purpose Backup Proxy section in the User Guide for VMware vSphere.

iSCSI Protocol

- [For Microsoft Windows] The backup proxy must have a Microsoft iSCSI Software initiator enabled.
- [For Linux] The backup proxy must have an Open-iSCSI Software initiator enabled.

- iSCSI traffic between the backup proxy and storage system must be allowed.

> **NOTE**
>
> For storage rescan, Veeam Backup & Replication uses its own initiator. For this reason, a Microsoft iSCSI Software initiator and Open-iSCSI may not be enabled when you perform storage rescan. For Backup from Storage Snapshots, however, the Microsoft iSCSI Software initiator and Open-iSCSI must be enabled.

SMB (CIFS) Protocol

SMB (CIFS) traffic between the backup proxy and storage system must be allowed.

Fibre Channel Protocol

- The backup proxy must have a Fibre channel adapter installed and must have access to the storage system over Fibre Channel fabric.
- To let Veeam Backup & Replication present snapshots of LUNs to the backup proxy, you must register the backup proxy with a WWN ID on the storage system.
- Fibre Channel devices must be properly installed on the backup proxy. For example, see the vendor documentation and check that the proxy OS and the Fibre Channel adapter are compatible. Also, check that the WWN ID of the backup proxy is properly zoned on the Fibre Channel switch.

NFS Protocol

NFS traffic between the backup proxy and storage system must be allowed.

Adding Storage Systems

To use storage snapshots for data protection and disaster recovery operations, you must add the storage system to the backup infrastructure. If you plan to work with secondary storage arrays, you must add them to the backup infrastructure as well.

Before adding a storage system to the backup infrastructure, check Requirements and Limitations.

If you want Veeam Backup & Replication to automatically rescan the storage system after you add it, select the relevant check box at the last step of the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

The topology of the storage system added to the backup infrastructure is displayed in the **Storage Infrastructure** view in the Veeam Backup & Replication console. On the **Home** view, in the **Backups** > **Snapshots** node, you can see volumes with storage snapshots and VMs stored on these volumes.

> **NOTE**
>
> If only Veeam Agents or NAS backup processing is selected for a storage system, volumes with snapshots and VMs of such storage system are not displayed under the **Backups** > **Snapshots** node. The storage system itself is still displayed in the **Storage Infrastructure** view.

You can add the following storage systems to the backup infrastructure:

- Dell Unity XT/Unity, VNXe, VNX
- Dell PowerScale (formerly Isilon)
- Adding HPE Nimble and Alletra 5000/6000
- Adding HPE 3PAR StoreServ, HPE Primera and Alletra 9000
- HPE StoreVirtual/LeftHand/P4000 series
- IBM Spectrum Virtualize
- Lenovo ThinkSystem DM Series
- NetApp Data ONTAP
- Nutanix Files Storage
- Universal Storage API Integrated Systems

> **NOTE**
>
> Only NAS backup jobs can access Dell PowerScale (formerly Isilon) and Nutanix Files storage systems.

Adding Cisco HyperFlex

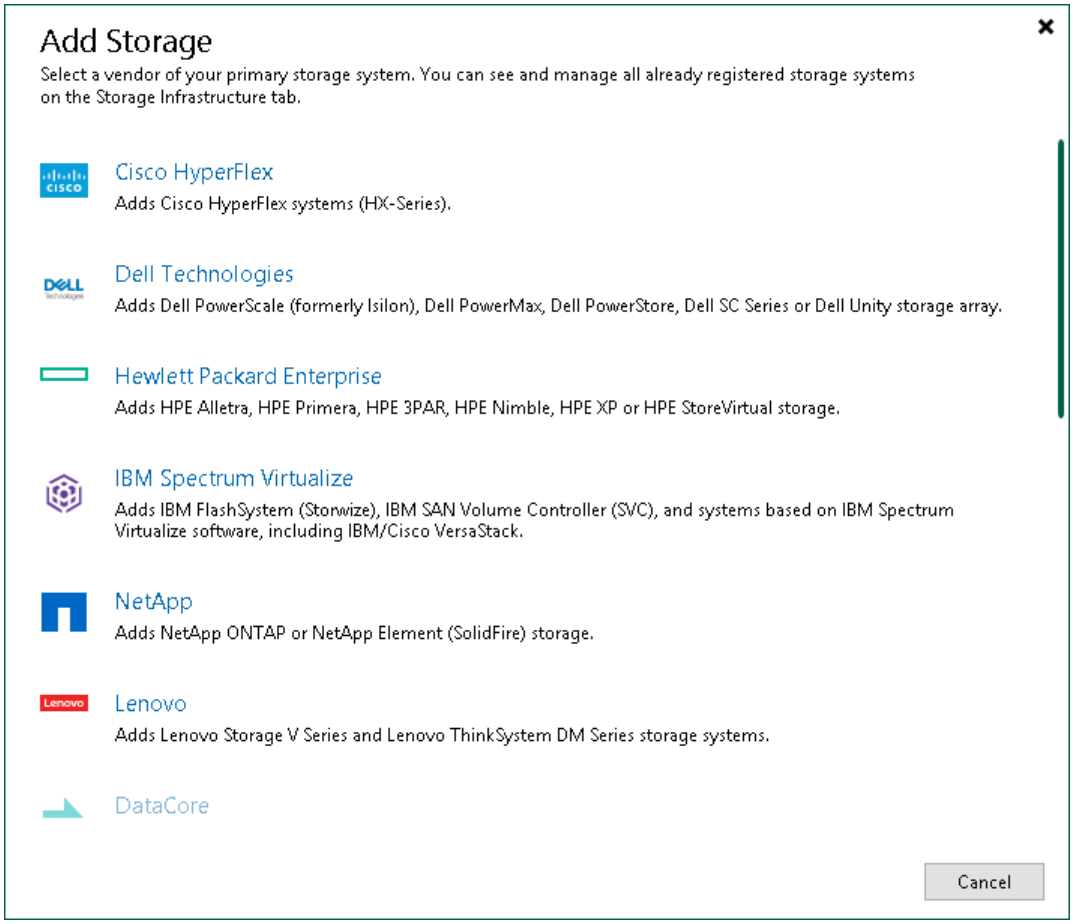
Before you add a Cisco HyperFlex storage system to the backup infrastructure, check prerequisites. Then use the **New Cisco HyperFlex System** wizard to add the storage system.

Step 1. Launch New Cisco HyperFlex System Wizard

To launch the **New Cisco HyperFlex System** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Cisco HyperFlex**.
- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Cisco HyperFlex**.
- You can use this method if at least one Cisco HyperFlex storage system is added to the backup infrastructure.

  Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Cisco HyperFlex** node under **Storage Infrastructure** and select **Add Storage**. You can also select the **Cisco HyperFlex** node in the inventory pane, right-click anywhere in the working area and select **Add storage**.

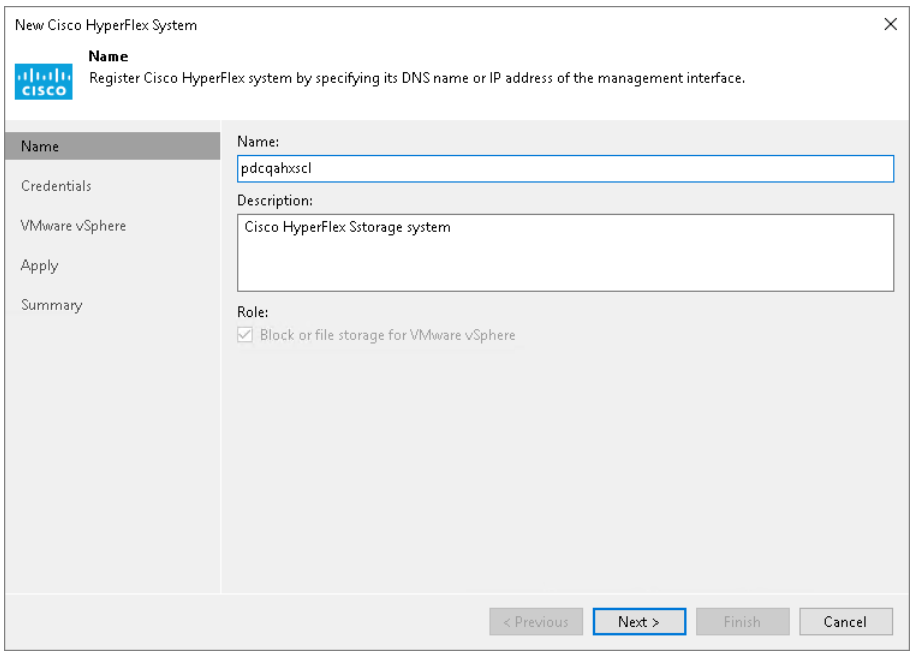


Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name and description:

1. In the **DNS name or IP address** field, enter a full DNS name or IPv4 address of the Cisco HyperFlex cluster management interface.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the server was added.

Only VMware backup jobs are allowed to access this storage system, so the **VMware backup** check box is selected automatically in the **Role** field.



Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system:

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

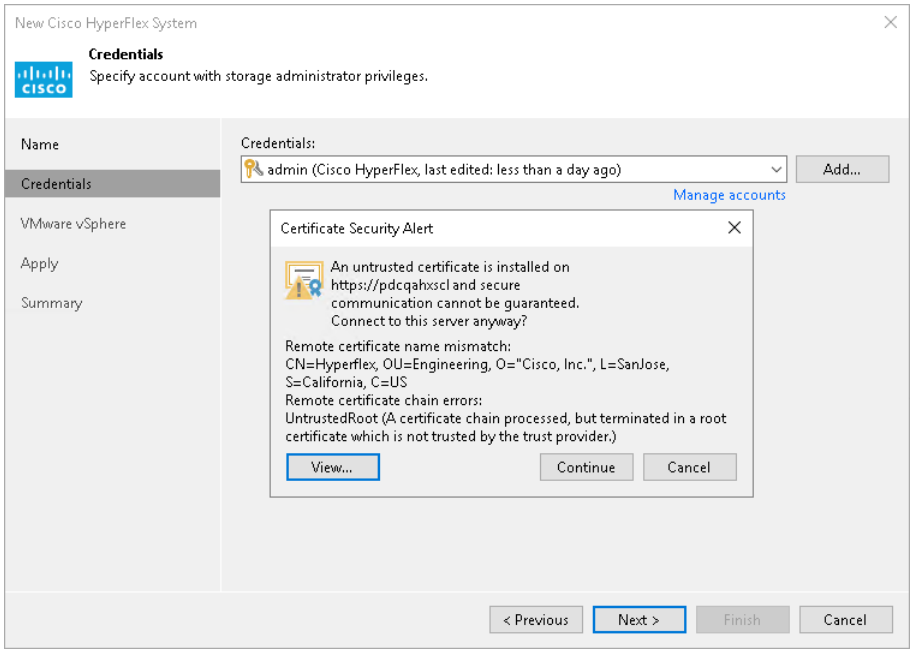
2. When you add a storage system, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate installed on the Cisco HyperFlex RESTful API server. During every subsequent connection to the server, Veeam Backup & Replication uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

   If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

   - To view detailed information about the certificate, click **View**.
   - If you trust the server, click **Continue**.
   - If you do not trust the server, click **Cancel**.

     Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

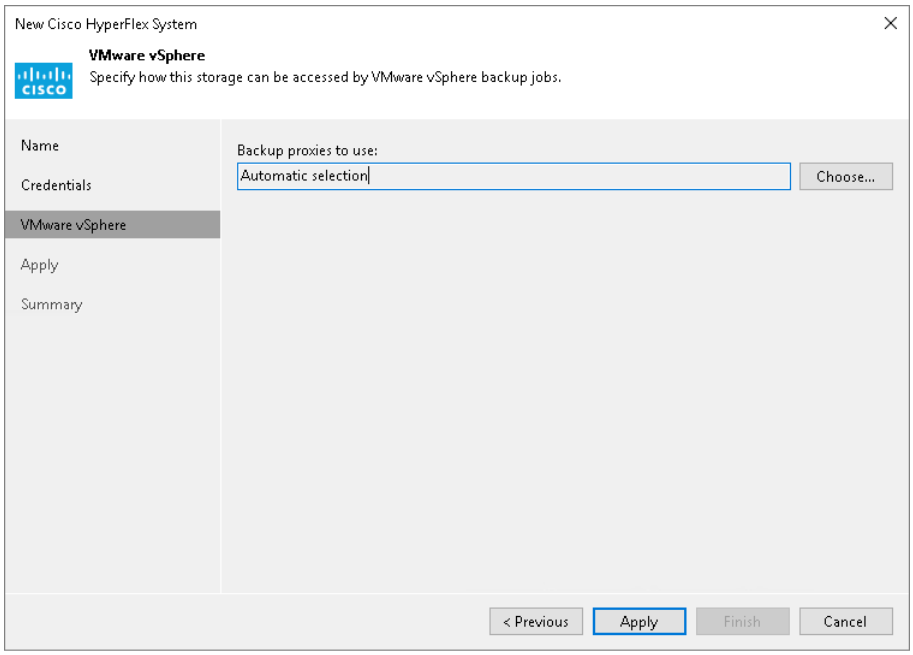
   When you update a certificate on a server, this server becomes unavailable in the Veeam Backup & Replication console. To make the server available again, acknowledge the new certificate at the **Credentials** step of the edit storage system wizard.



Step 4. Specify VMware Access Options

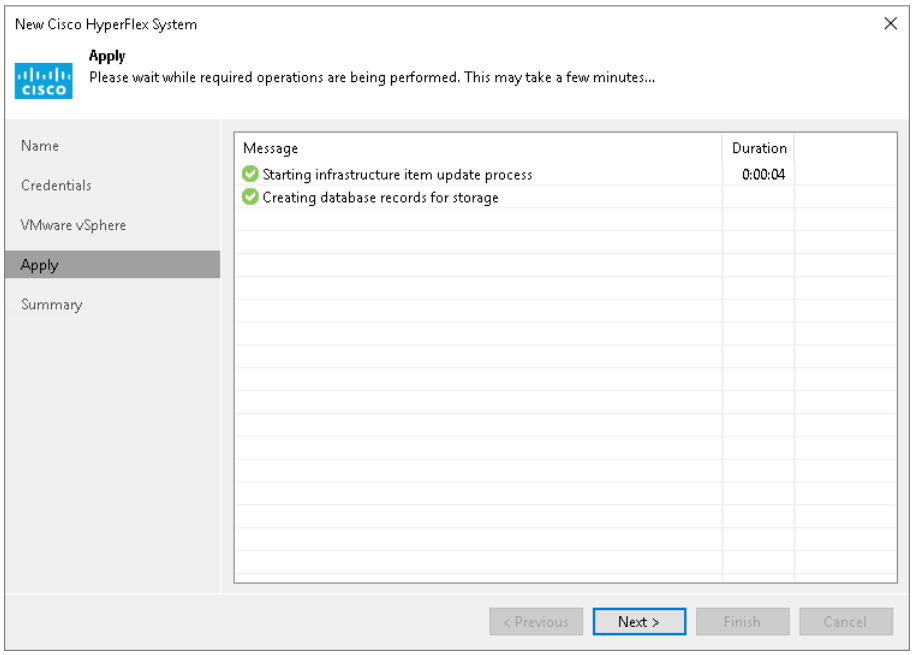
At the **VMware vSphere** step of the wizard, select backup proxies that you plan to use for backup and replication of VMs hosted on Cisco HyperFlex. Veeam Backup & Replication will check what data retrieval methods are available for these backup proxies. For more information, see Methods of Data Retrieval.

- Leave **Automatic selection** to let Veeam Backup & Replication check which data retrieval method is used for each backup proxy in the backup infrastructure. Veeam Backup & Replication will choose an optimal backup proxy for processing.
- Click **Choose** and select **Use the selected backup proxy servers only** to define backup proxies that can be used for processing. In this case, Veeam Backup & Replication will check which data retrieval method is used and will select an optimal proxy only among the selected backup proxies.



Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

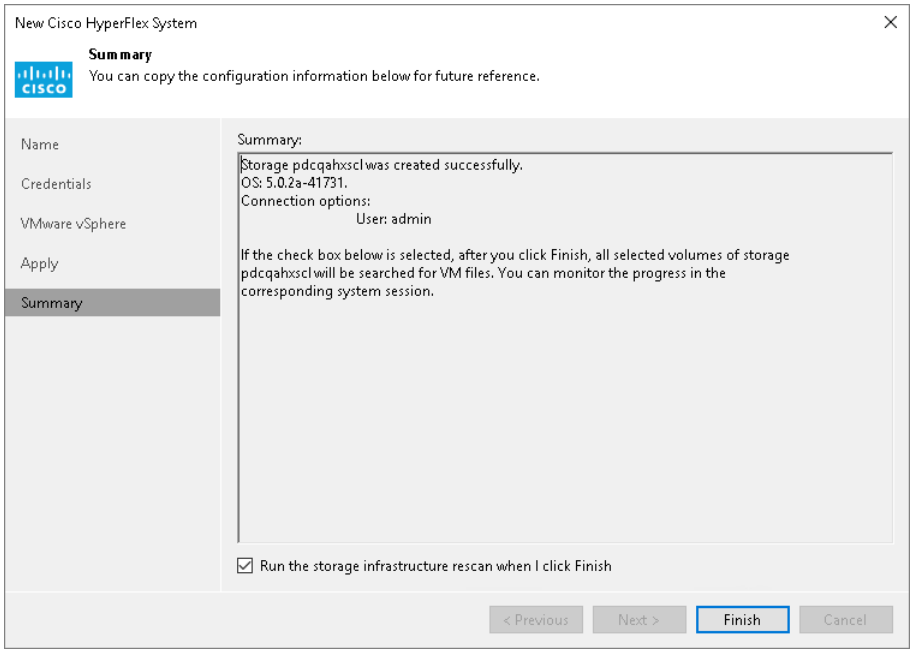


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding Dell

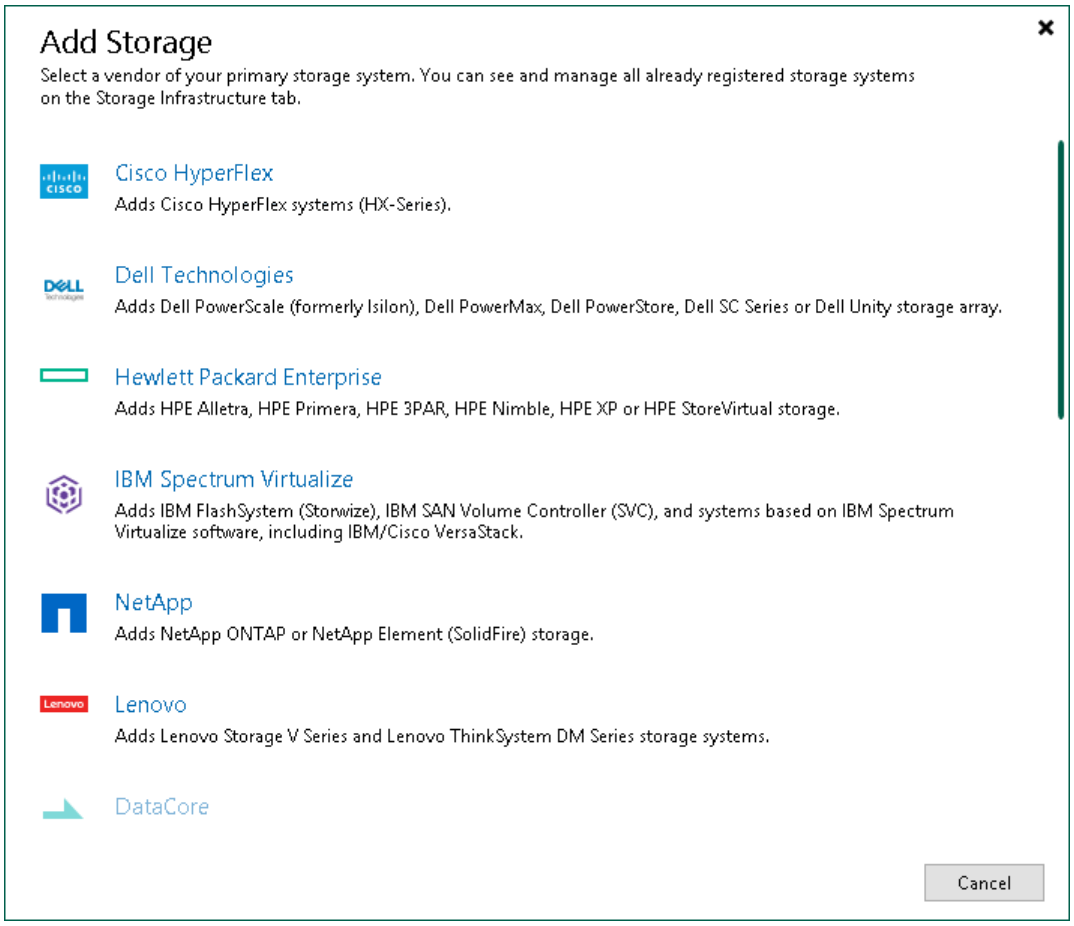
Before you add a Dell storage system to the backup infrastructure, check prerequisites. Then use the **New DELL Storage** wizard to add the storage system.

Step 1. Launch Add Storage Wizard

To launch the wizard for adding a Dell storage system, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Dell Technologies**.
- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Dell Technologies**.
- You can use this method if at least one Dell storage system is added to the backup infrastructure.

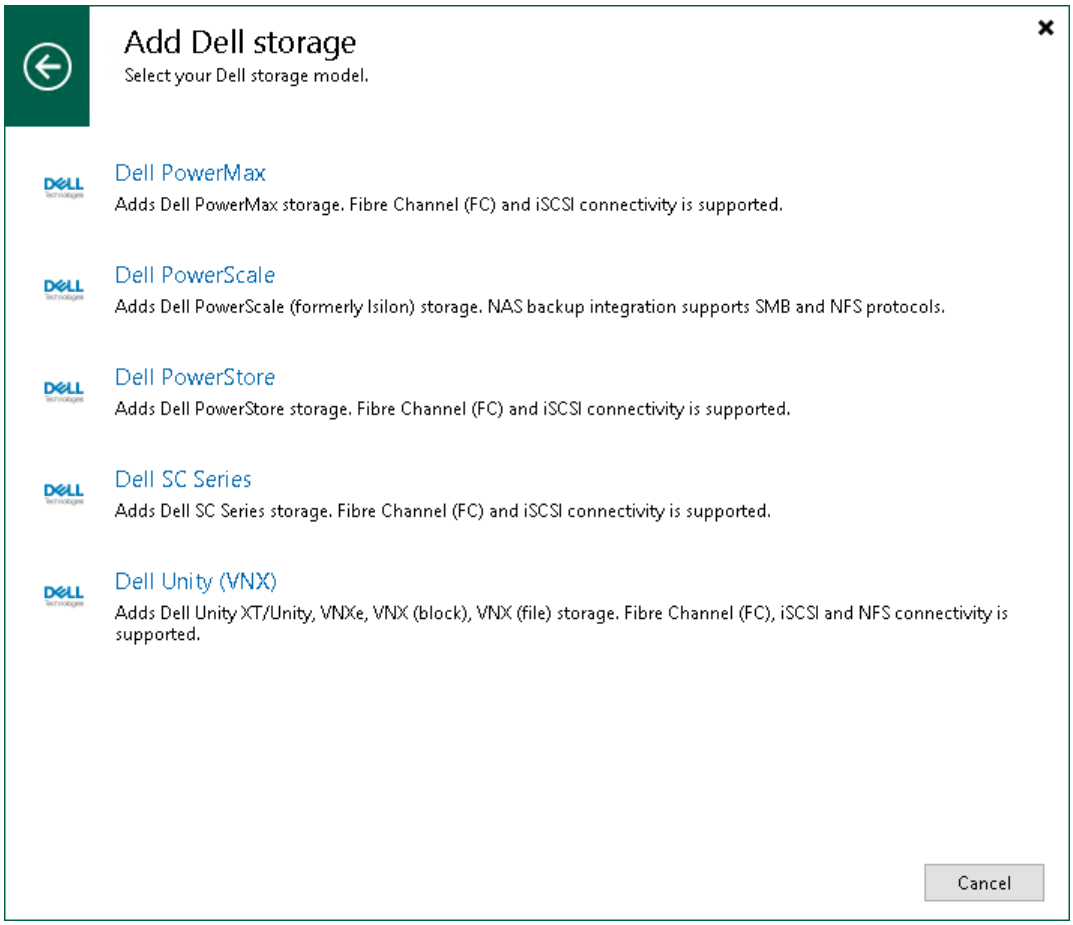
  Open the **Storage Infrastructure** view. In the inventory pane, right-click the *<Dell storage model name>* node and select **Add storage**. Alternatively, you can select the *<Dell storage model name>* node in the inventory pane, right-click anywhere in the working area and select **Add storage**.



Step 2. Add Dell Storage

In the **Add Dell storage** window, select which Dell storage type you want to add:

- Dell PowerMax (Veeam Backup & Replication will open the wizard for Universal Storage API integrated systems)
- Dell PowerScale (formerly Isilon)
- Dell PowerStore (Veeam Backup & Replication will open the wizard for Universal Storage API integrated systems)
- Dell SC Series (Veeam Backup & Replication will open the wizard for Universal Storage API integrated systems)
- Dell Unity XT/Unity, VNXe, VNX



Adding Dell PowerScale (formerly Isilon)

To add Dell PowerScale (formerly Isilon) storage system to the backup infrastructure, do the following:

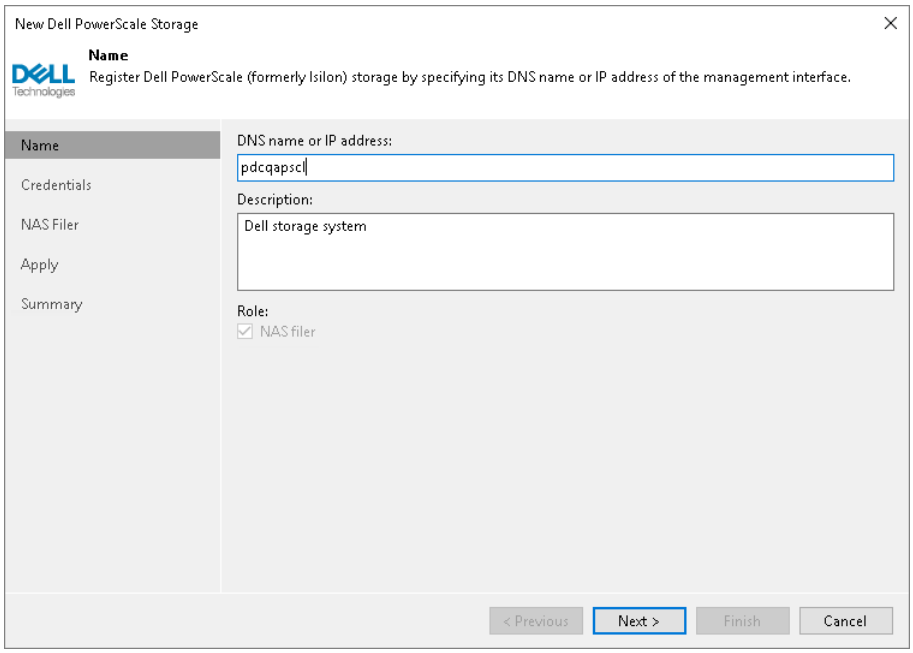
1. Specify storage name or address and storage role.
2. Specify credentials.
3. Specify NAS access options.
4. Apply settings.
5. Finish working with wizard.

Step 1. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name and description:

1. In the **DNS name or IP address** field, specify a DNS name or IPv4 address of the storage system.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.

Only NAS backup jobs are allowed to access this storage system, so the **NAS filer** check box is selected automatically in the **Role** section.



Step 2. Specify Credentials

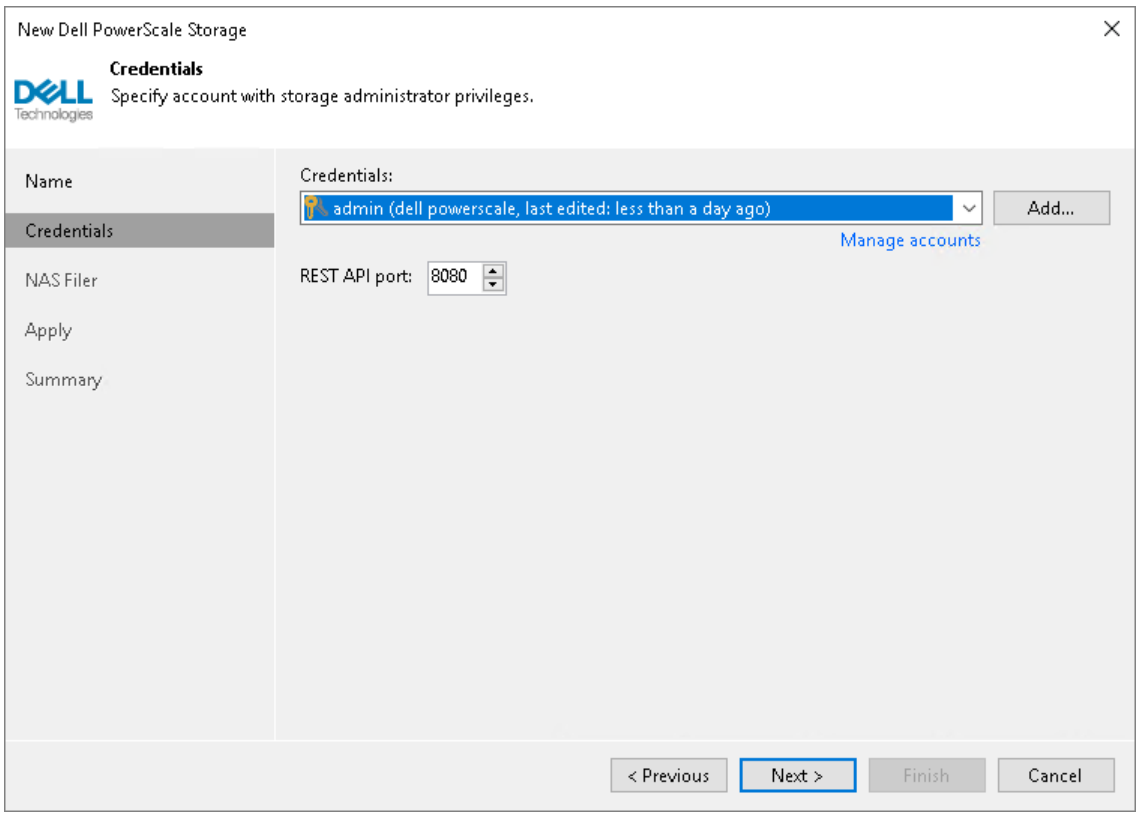
At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system: from the **Credentials** drop-down list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

- To view detailed information about the certificate, click **View**.
- If you trust the server, click **Continue**.
- If you do not trust the server, click **Cancel**.

  Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

In the **REST API port** dialog, select the necessary port.



Step 3. Specify NAS Access Options

At the **NAS Filer** step of the wizard, specify options for accessing the storage system:

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required SMB and NFS export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required export rules automatically** check box.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   a. To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

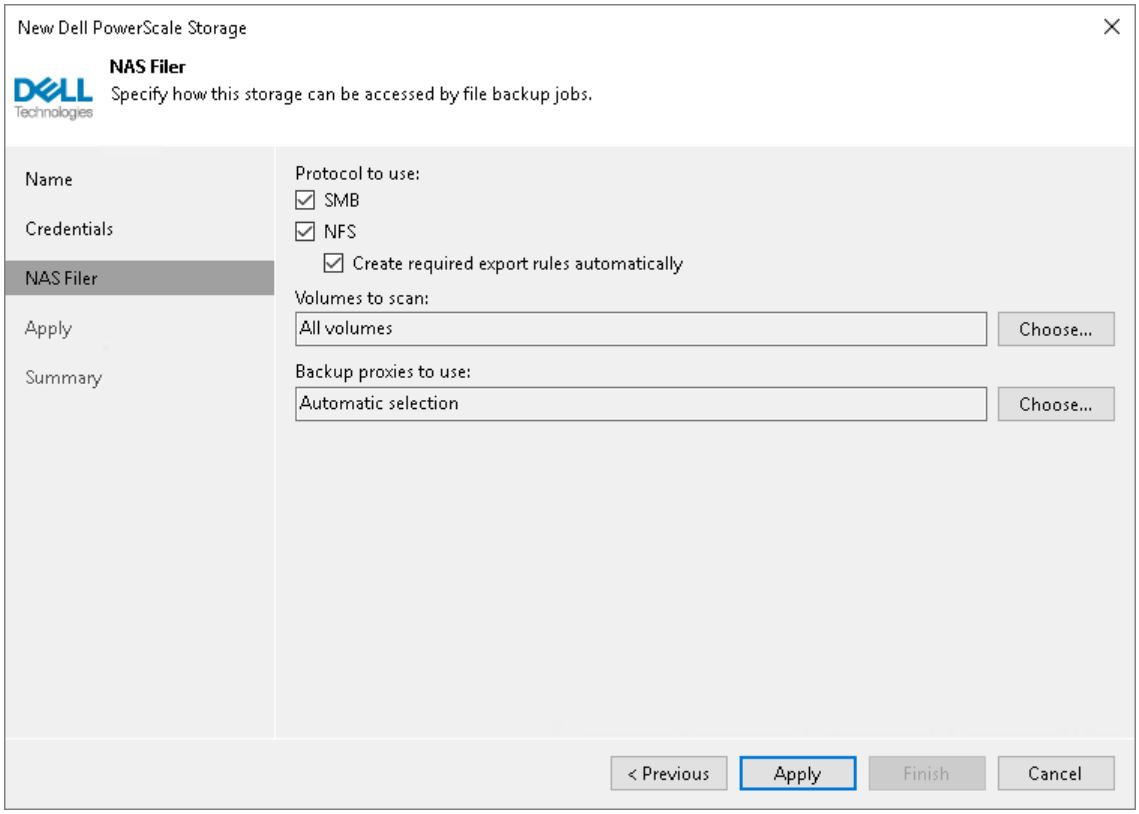
   b. To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   c. If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
4. To rescan storage systems and perform Backup from Storage Snapshots, you must configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.

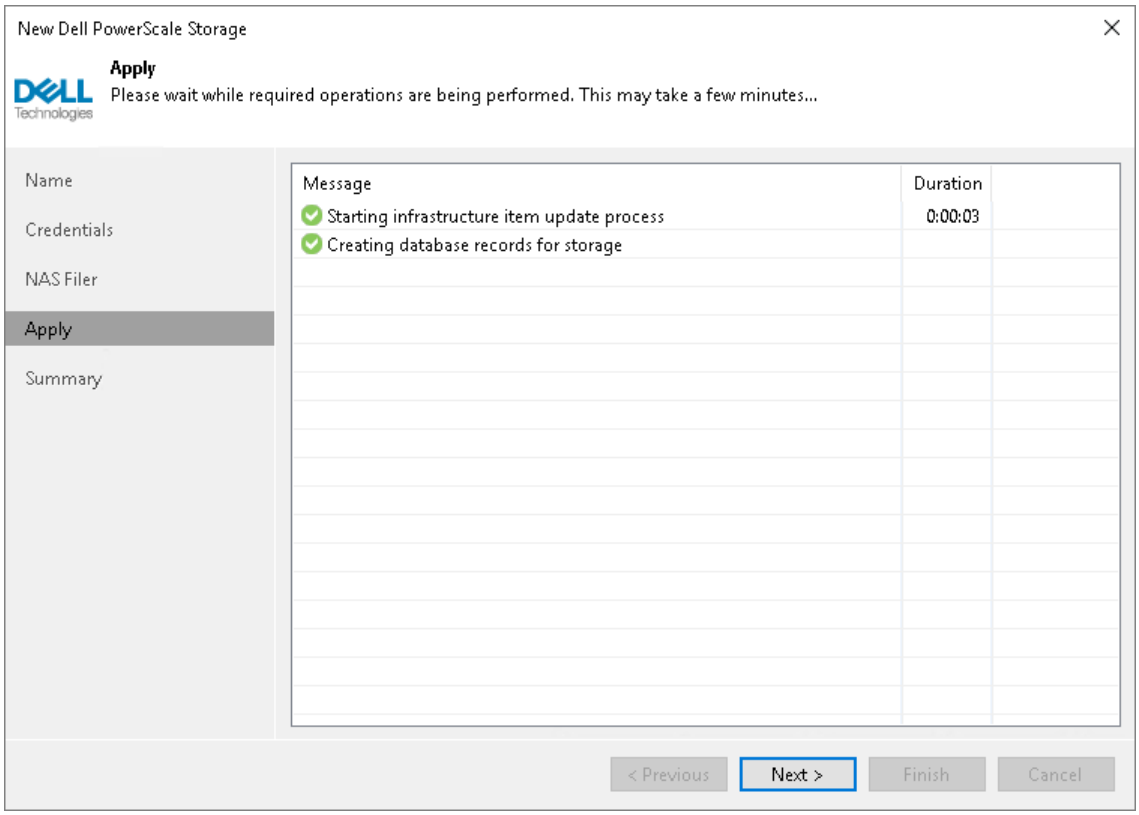
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed is performed if one of backup proxies fails or loses connection with the storage system.



Step 4. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

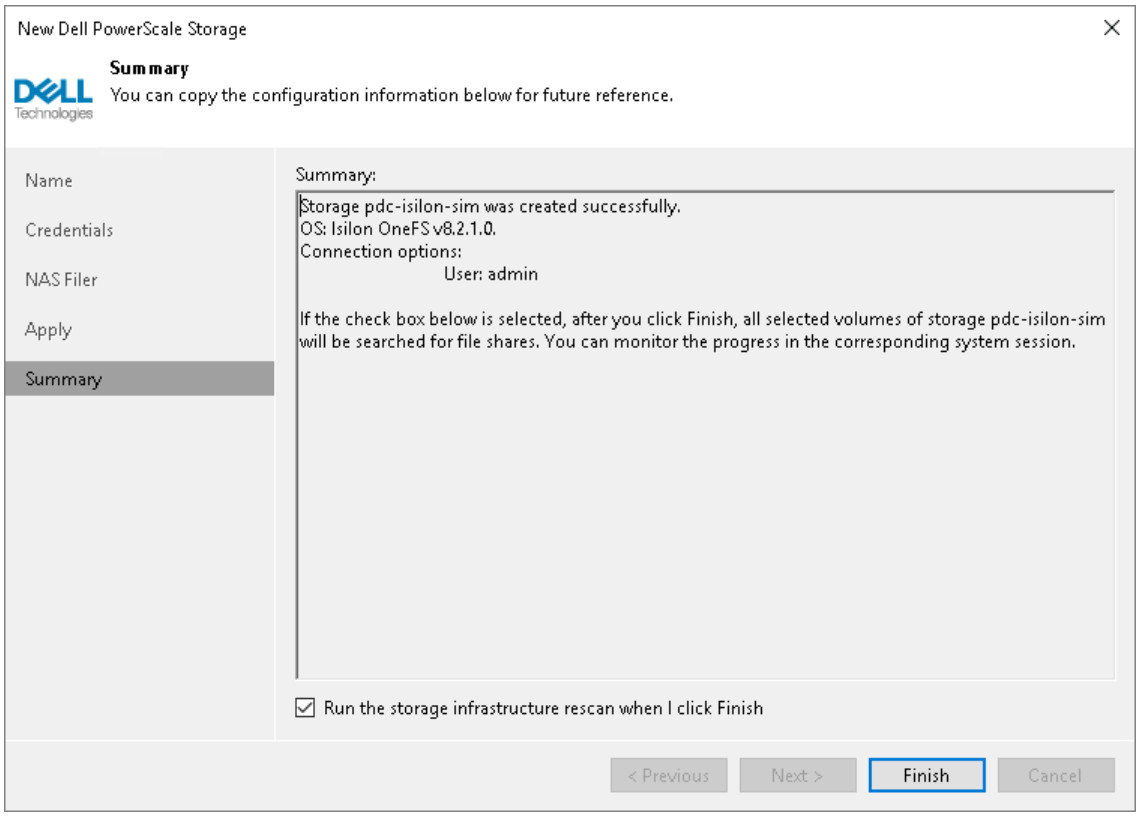


Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding Dell Unity XT/Unity, VNXe, VNX

To add Dell Unity XT/Unity, VNXe, VNX storage system to the backup infrastructure, do the following:

1. Select storage type.
2. Specify storage name or address and storage role.
3. Specify credentials.
4. Specify VMware access options.
5. Specify Veeam Agent access options.
6. Apply settings.
7. Finish working with wizard.

To add Dell Unity XT/Unity, VNXe, VNX storage system to the backup infrastructure, do the following:

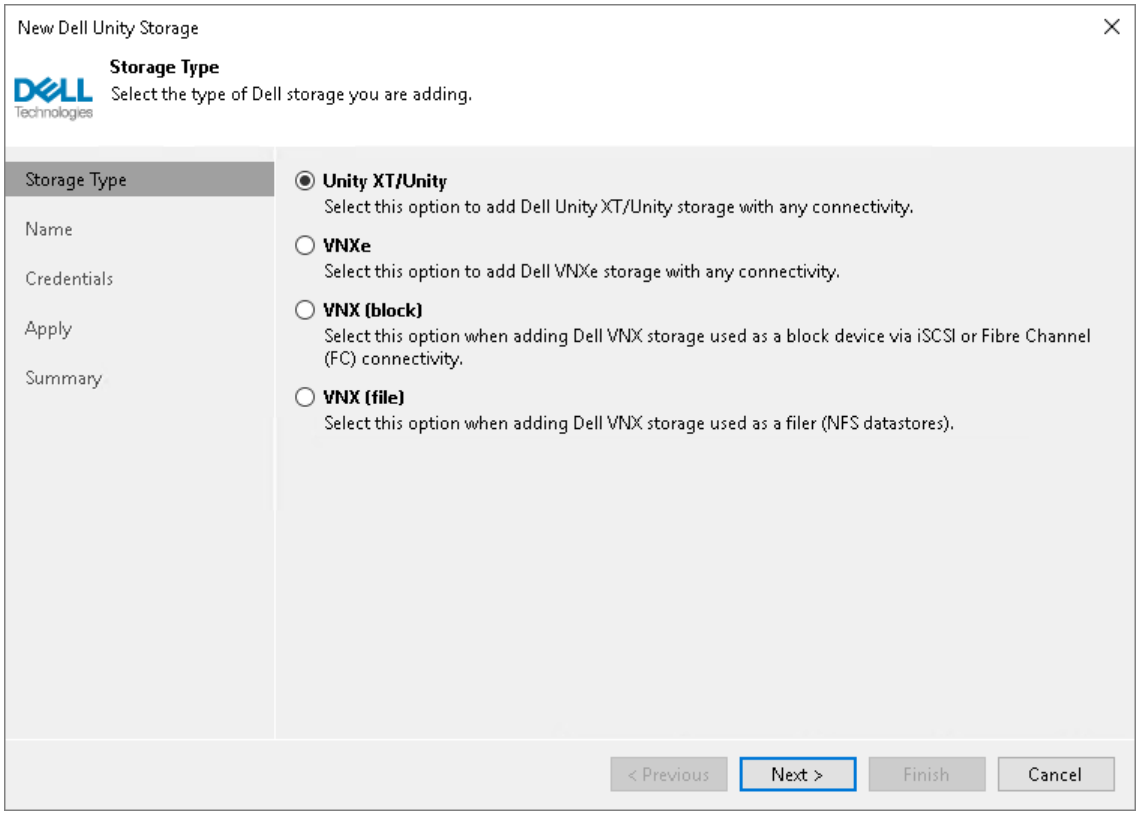
1. Select storage type.
2. Specify storage name or address and storage role.
3. Specify credentials.

4. Specify Veeam Agent access options.
5. Apply settings.
6. Finish working with wizard.

Step 1. Select Dell Unity XT/Unity, VNXe, VNX Storage Type

At the **Storage Type** step of the wizard, select the storage type:

- Select **Unity XT/Unity** to add a Dell Unity XT/Unity storage system.
- Select **VNXe** to add a Dell VNXe storage system.
- Select **VNX (block)** to add a Dell VNX block storage system working over iSCSI or Fibre Channel.
- Select **VNX (file)** to add a Dell VNX file storage system working over NFS.



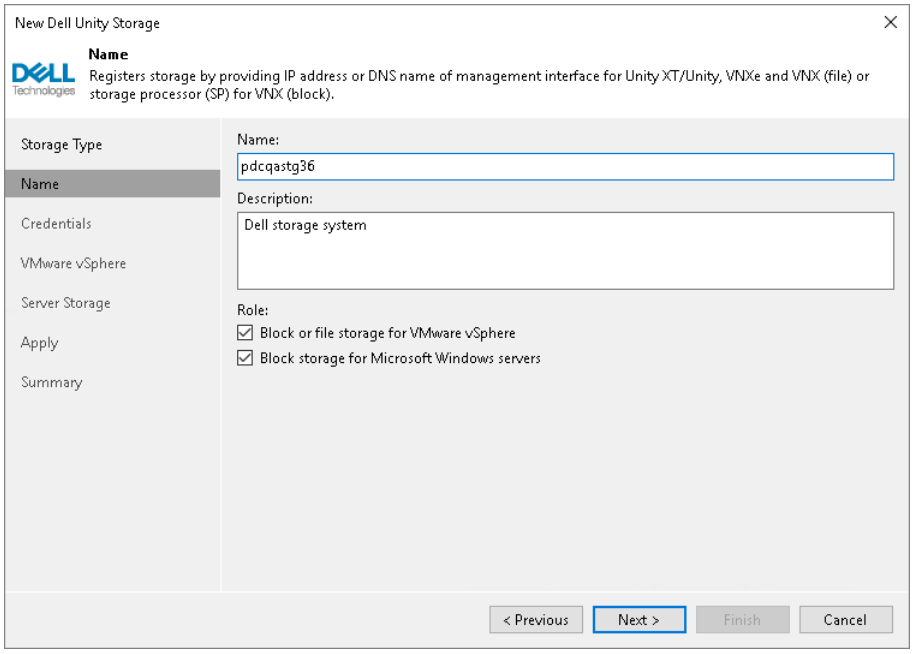
Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **DNS name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.
   b. [For Unity XT/Unity, VNXe, VNX (block)] Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



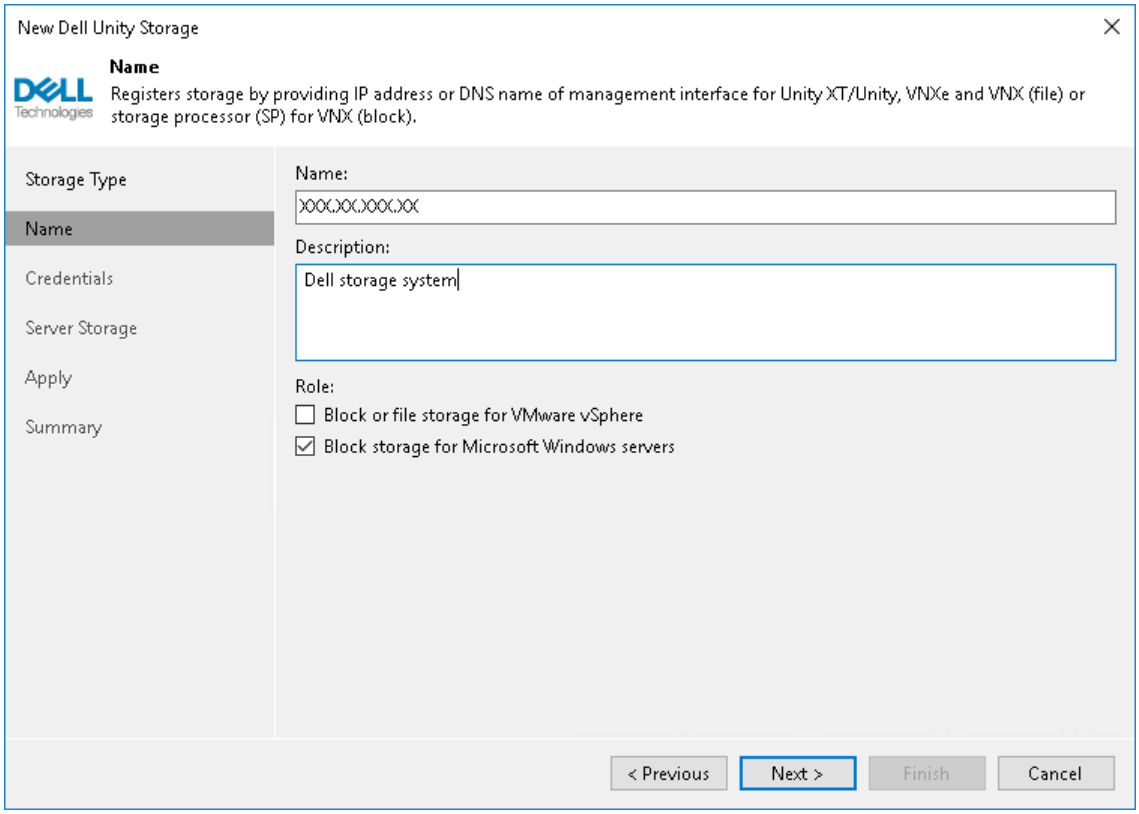
Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role:

1. In the **DNS name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.
   b. [For Unity XT/Unity, VNXe, VNX (block)] Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system:

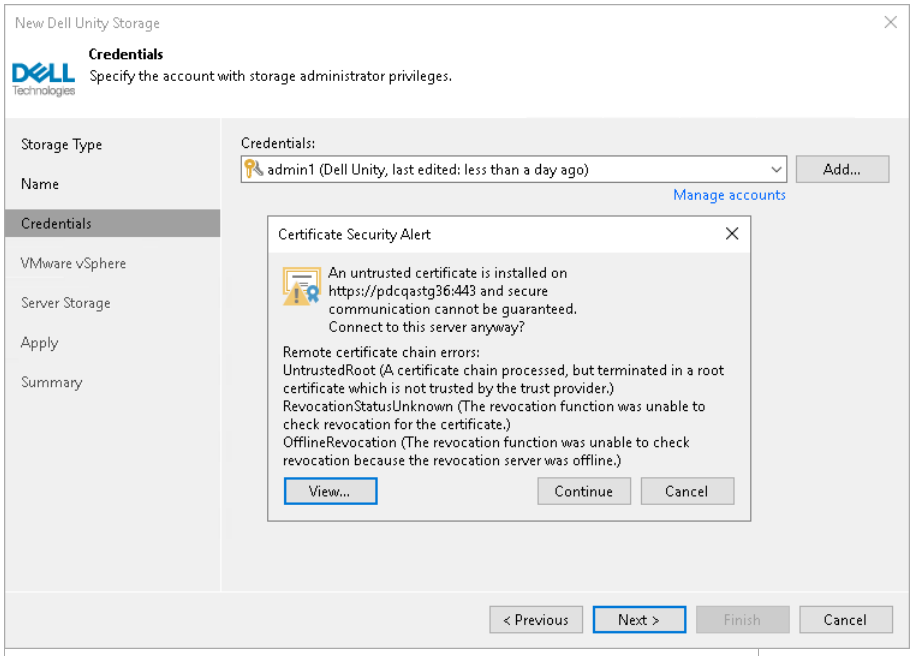
1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.
2. [For Dell VNX block storage] Select the scope to which the user account belongs:
   - Select **Global** if the user can administer all VNX systems in the domain.
   - Select **Local** if the user can administer only a single VNX storage system in the domain.
   - Select **LDAP** if the user can administer all VNX systems that use the LDAP server for authentication.
3. When you add a storage system, Veeam Backup & Replication saves to the configuration database the following information:
   - [For Dell Unity XT/Unity, VNXe] A thumbprint of the TLS certificate installed on the management server.
   - [For Dell VNX file storage] A fingerprint of the SSH key of the management server.

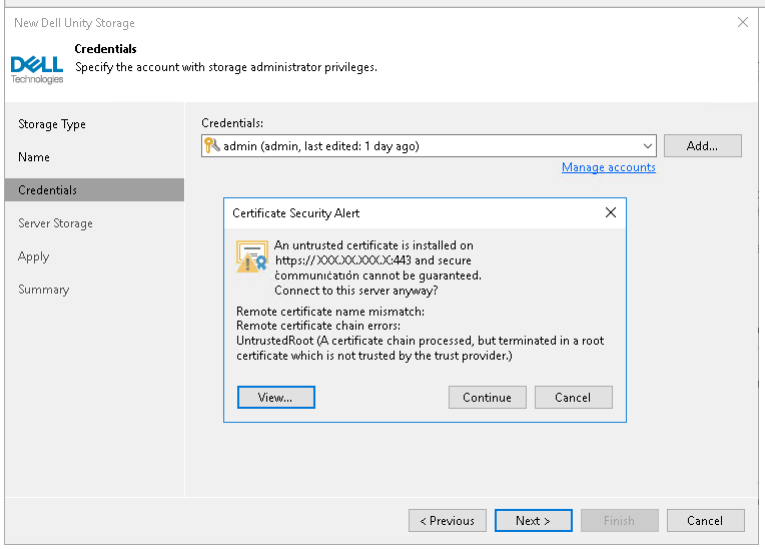
   During every subsequent connection to the server, Veeam Backup & Replication uses the saved information to verify the server identity and avoid man-in-the-middle attacks.

   [For Dell Unity XT/Unity, VNXe] If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.
   - To view detailed information about the certificate, click **View**.
   - If you trust the server, click **Continue**.
   - If you do not trust the server, click **Cancel**. In this case, Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

   [For Dell VNX file storage] To let you identify the server, Veeam Backup & Replication displays the SSH key fingerprint. To accept the fingerprint and connect to the server, click **Yes**. If you click **No**, Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

When you update a certificate or SSH key on a server, this server becomes unavailable in the Veeam Backup & Replication console. To make the server available again, acknowledge the new certificate or SSH key at the **Credentials** step of the edit storage system wizard.





Step 4. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

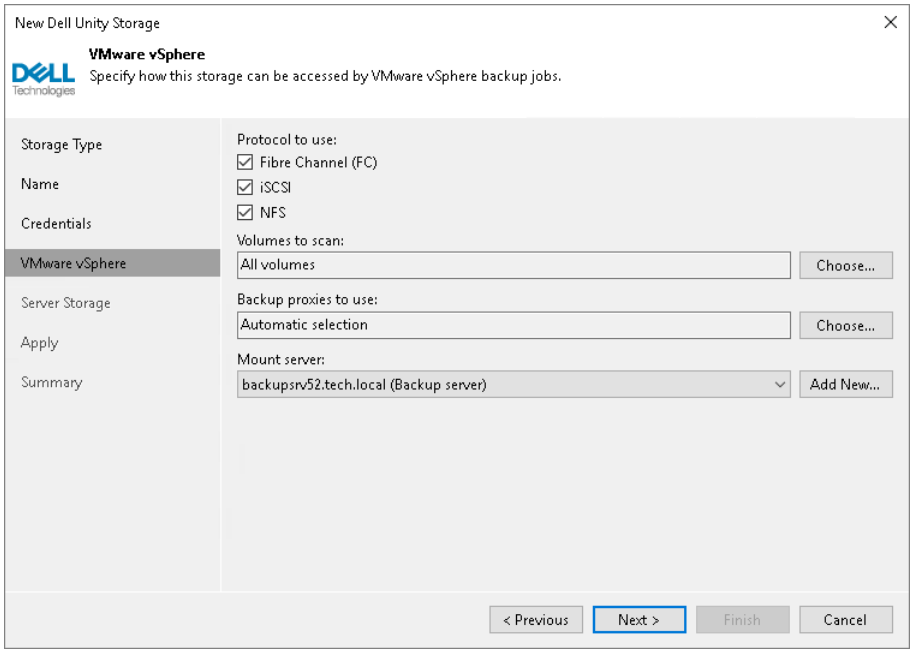
   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you must configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses connection to the storage system.

   > **IMPORTANT**
   >
   > If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

4. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 4. Specify Veeam Agent Access Options

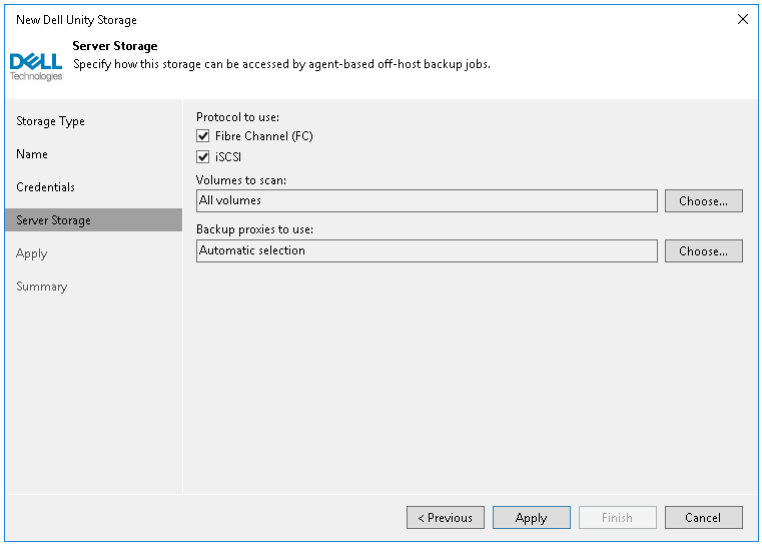
At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.



Step 5. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

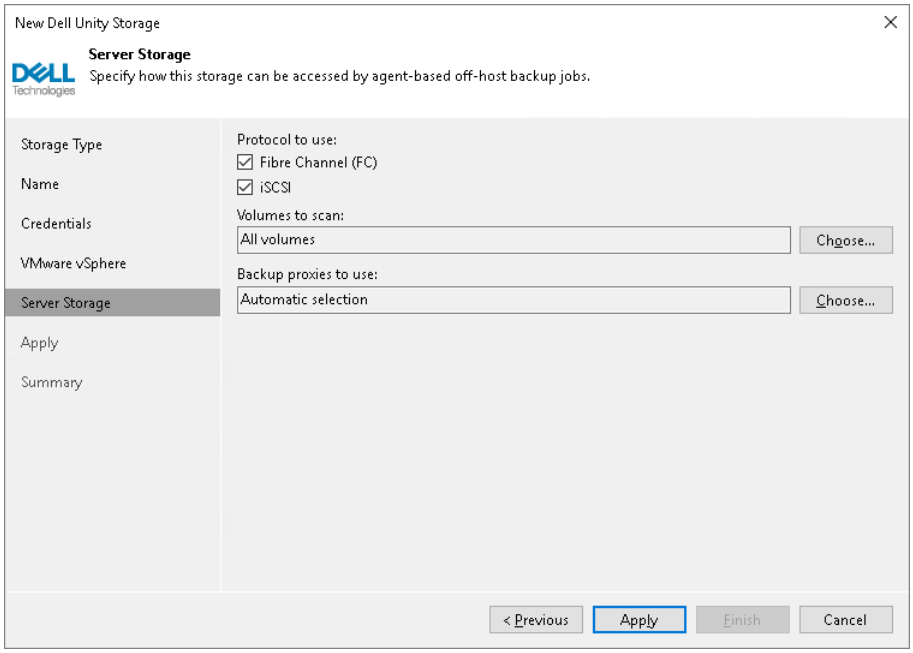
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

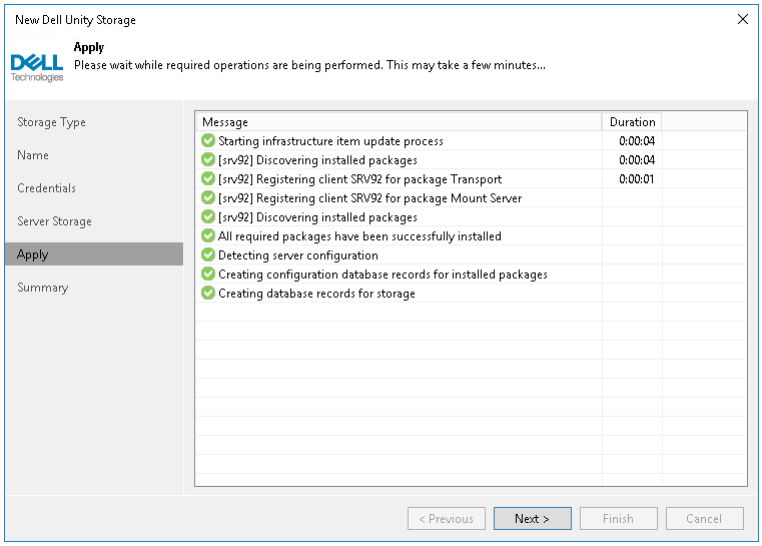
3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



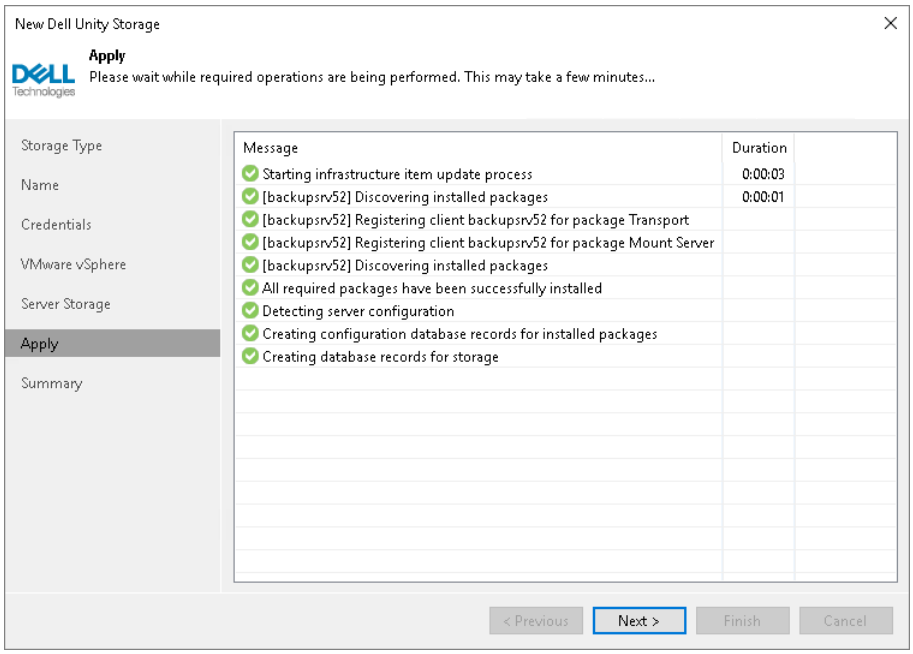
Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.



Step 6. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

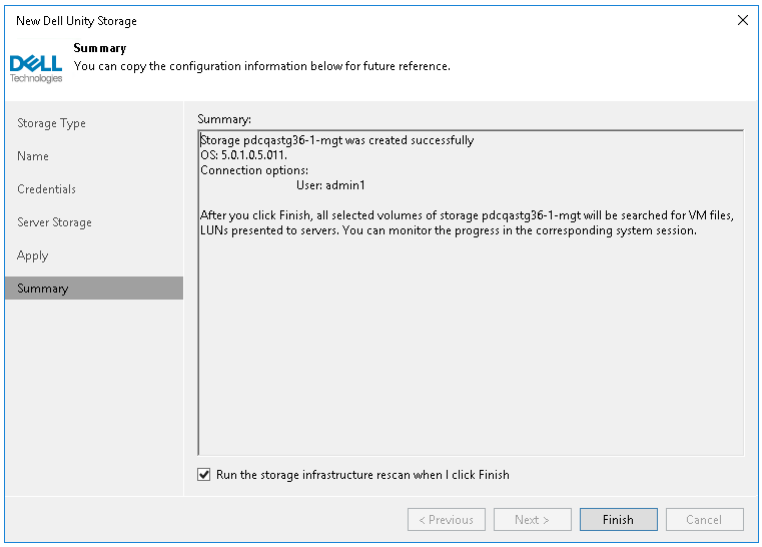


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

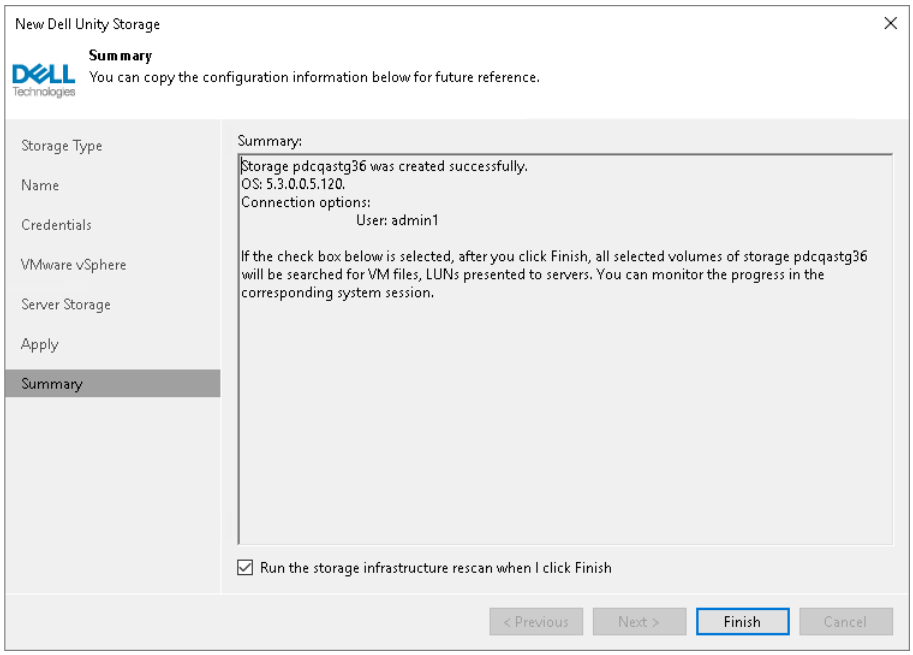


Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding Hewlett Packard Enterprise

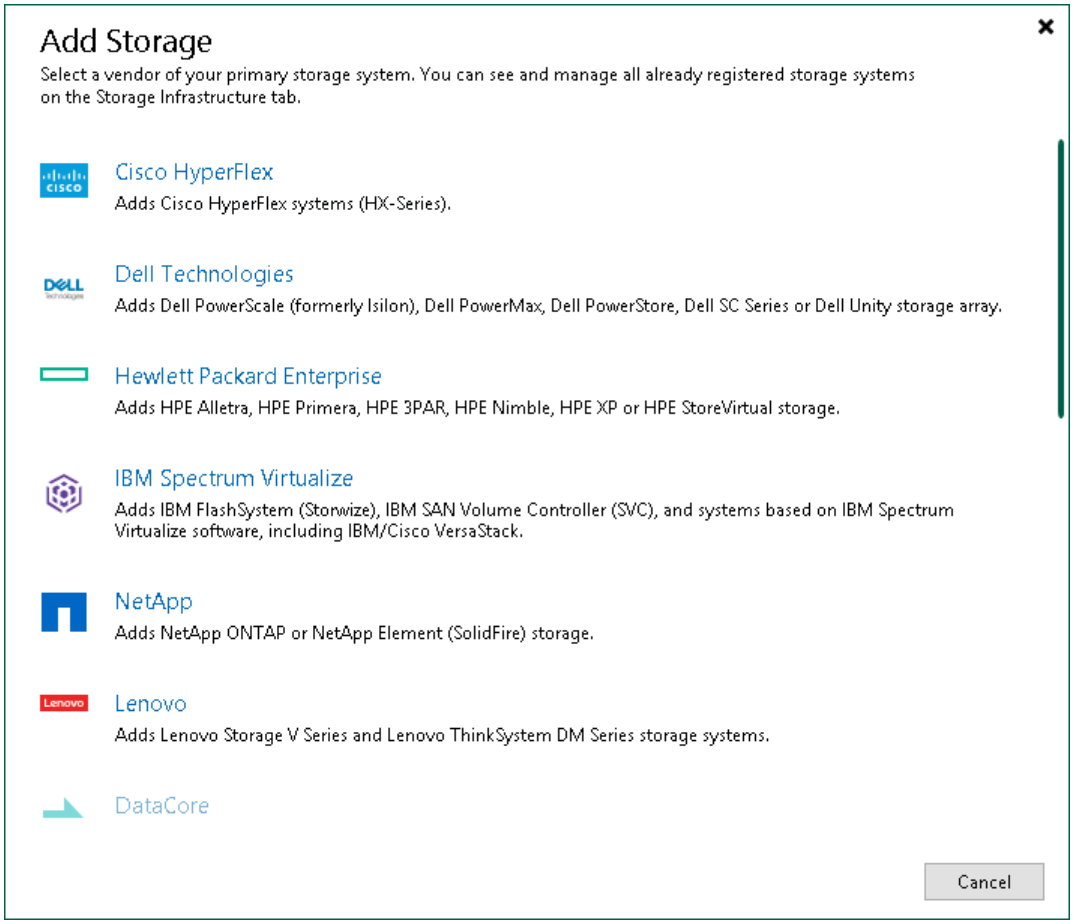
Before you add a Hewlett Packard Enterprise storage system to the backup infrastructure, check prerequisites. Then use the **New HPE Storage** wizard to add the storage system.

Step 1. Launch Add Storage Wizard

To launch the wizard for adding an HPE storage system, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise**.
- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise**.
- You can use this method if at least one HPE Nimble, 3PAR StoreServ or StoreVirtual/LeftHand/P4000 series storage system is added to the backup infrastructure.

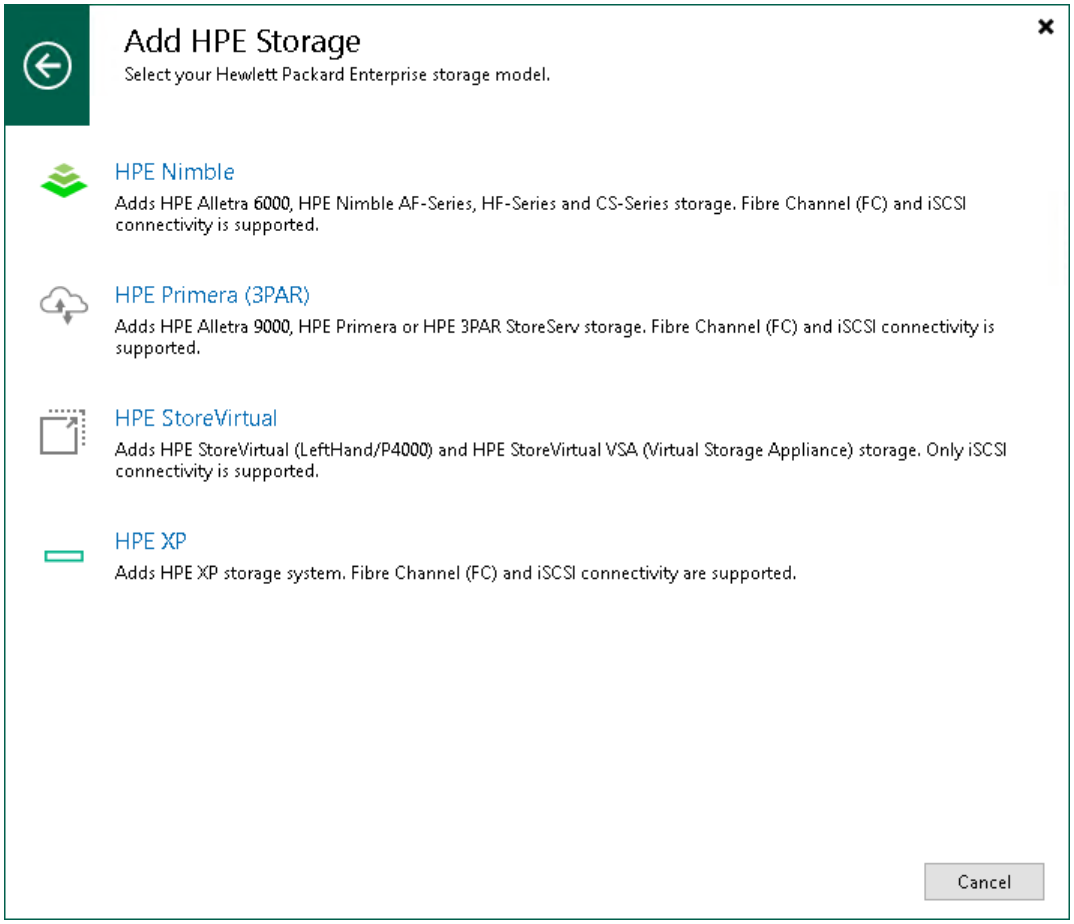
  Open the **Storage Infrastructure** view. In the inventory pane, right-click the *<HPE storage model name>* node and select **Add storage**. Alternatively, you can select the *<HPE storage model name>* node in the inventory pane, right-click anywhere in the working area and select **Add storage**.



Step 2. Add HPE Storage

In the **Add HPE Storage** window, select which HPE Storage type you want to add:

- HPE Nimble and Alletra 5000/6000
- HPE 3PAR StoreServ, HPE Primera and Alletra 9000
- HPE StoreVirtual/LeftHand/P4000 series
- HPE XP (Veeam Backup & Replication will open the wizard for Universal Storage API integrated systems)



Adding HPE Nimble and Alletra 5000/6000

To add an HPE Nimble storage system to the backup infrastructure, do the following:

1. Specify storage name or address and storage role.
2. Specify credentials.
3. Specify VMware access options.
4. Specify Veeam Agent access options.
5. Apply settings.
6. Finish working with the wizard.

To add an HPE Nimble storage system to the backup infrastructure, do the following:

1. Specify storage name or address and storage role.

2. Specify credentials.
3. Specify Veeam Agent access options.
4. Apply settings.
5. Finish working with the wizard.

Step 1. Specify Storage Name or Address and Storage Role

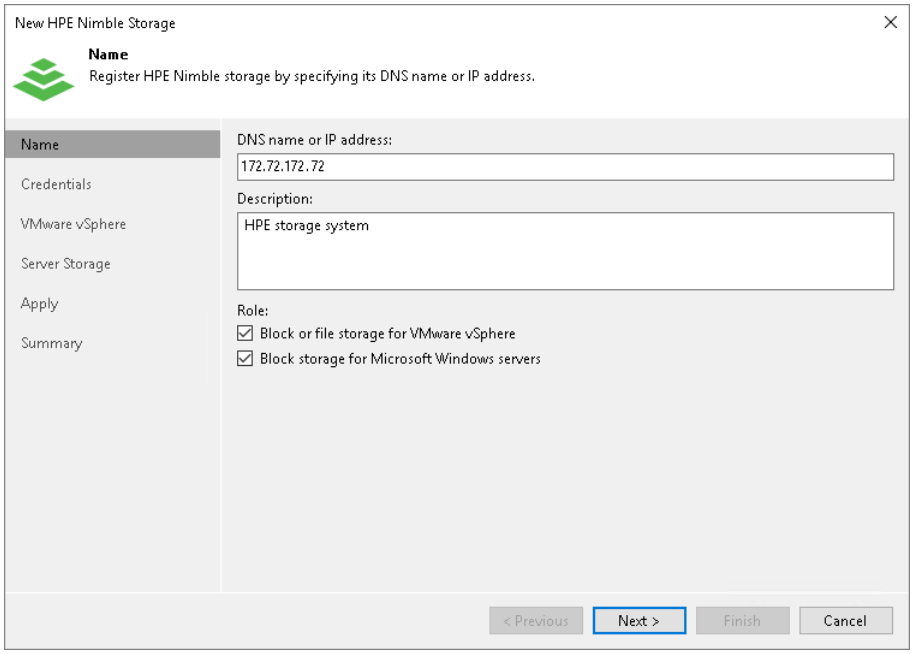
At the **Name** step of the wizard, specify the storage system name, description and storage role.

> **NOTE**
>
> Make sure that the **Access** setting is set to **Volume Only** for VMware hosts on all Nimble volumes that are used as VMware datastores.
>
> If the **Access** setting within the Nimble storage system is set to **Volume & Snapshots** for VMware hosts, the VMware host detects all snapshots as volumes at volume rescan when Veeam Backup & Replication mounts Nimble snapshots to a backup proxy. When Veeam Backup & Replication subsequently unmounts the snapshots after the backup is complete, alerts and alarms may be triggered on the VMware host regarding inaccessible storage. The VMware host can even become unresponsive as a result. Be aware, the VMware hosts may require a reboot during a maintenance period for the new LUN access permissions to take effect.

1. In the **DNS name or IP address** field, specify a DNS name or IPv4 address of the storage system.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 1. Specify Storage Name or Address and Storage Role

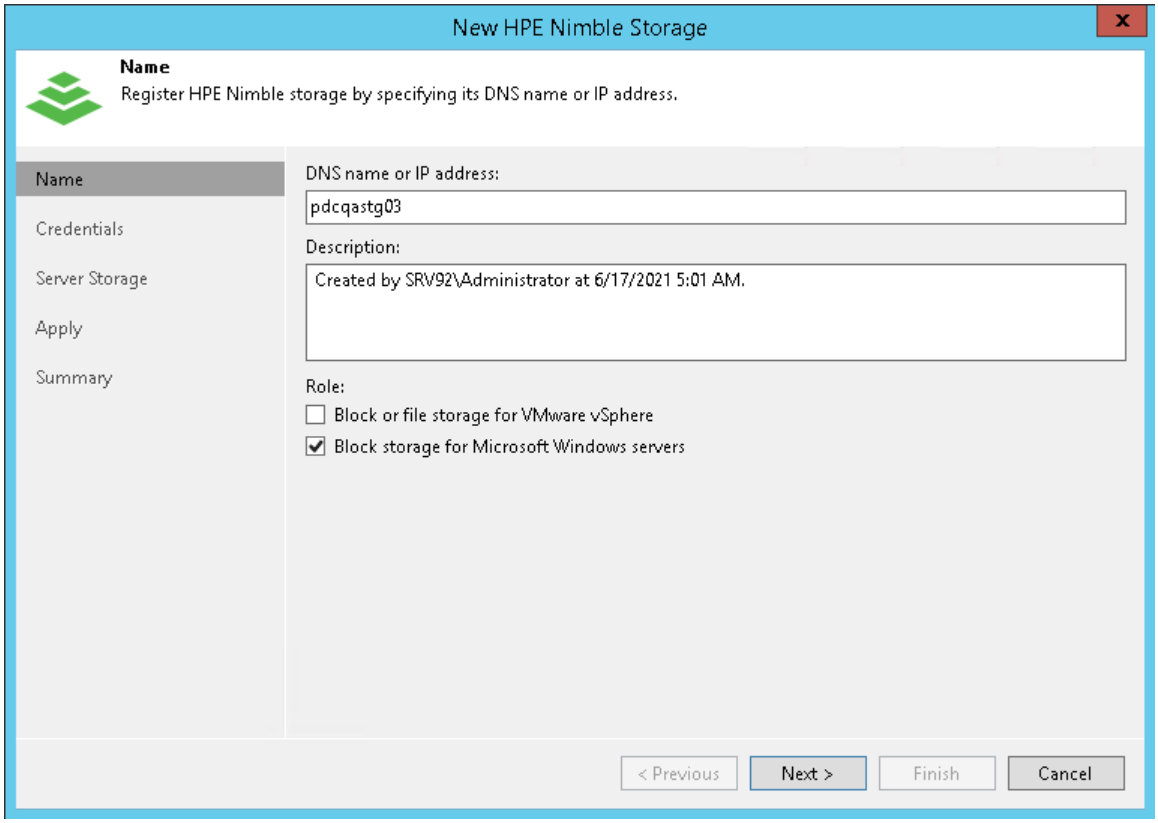
At the **Name** step of the wizard, specify the storage system name, description and storage role.

> **NOTE**
>
> Make sure that the **Access** setting is set to **Volume Only** for VMware hosts on all Nimble volumes that are used as VMware datastores.
>
> If the **Access** setting within the Nimble storage system is set to **Volume & Snapshots** for VMware hosts, the VMware host detects all snapshots as volumes at volume rescan when Veeam Backup & Replication mounts Nimble snapshots to a backup proxy. When Veeam Backup & Replication subsequently unmounts the snapshots after the backup is complete, alerts and alarms may be triggered on the VMware host regarding inaccessible storage. The VMware host can even become unresponsive as a result. Be aware, the VMware hosts may require a reboot during a maintenance period for the new LUN access permissions to take effect.

1. In the **DNS name or IP address** field, specify a DNS name or IPv4 address of the storage system.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 2. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

   The user account that you select must have Administrator or Power User permissions on the HPE Nimble storage system.

2. Veeam Backup & Replication uses HPE Nimble RESTful API to communicate with the storage system. By default, commands to the RESTful API server are sent over port 5392. If you use another port for HPE Nimble RESTful API, you can change the port number.

3. When you add a storage system, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate installed on the management server.

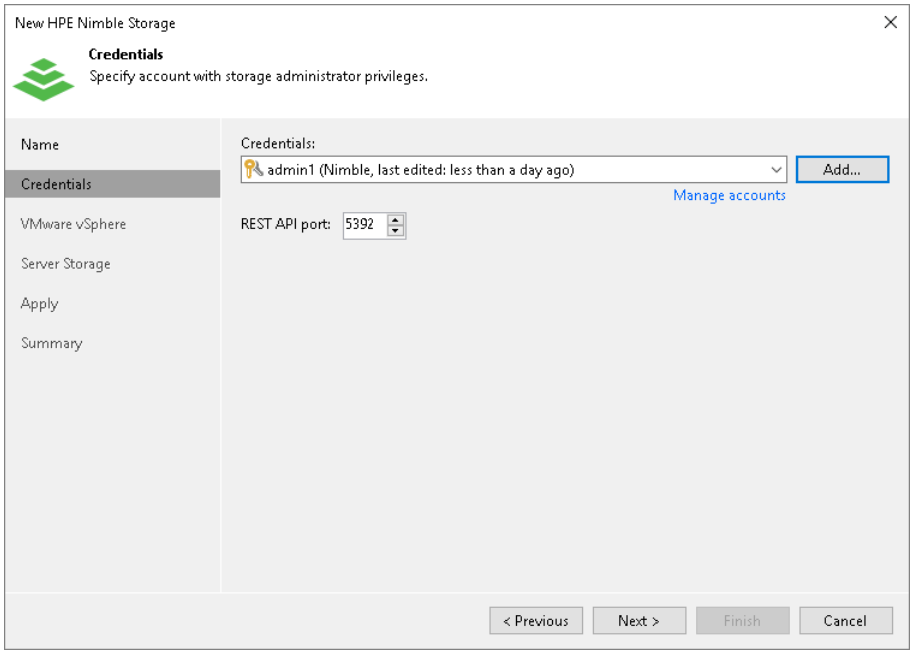
   During every subsequent connection to the server, Veeam Backup & Replication uses the saved information to verify the server identity and avoid man-in-the-middle attacks.

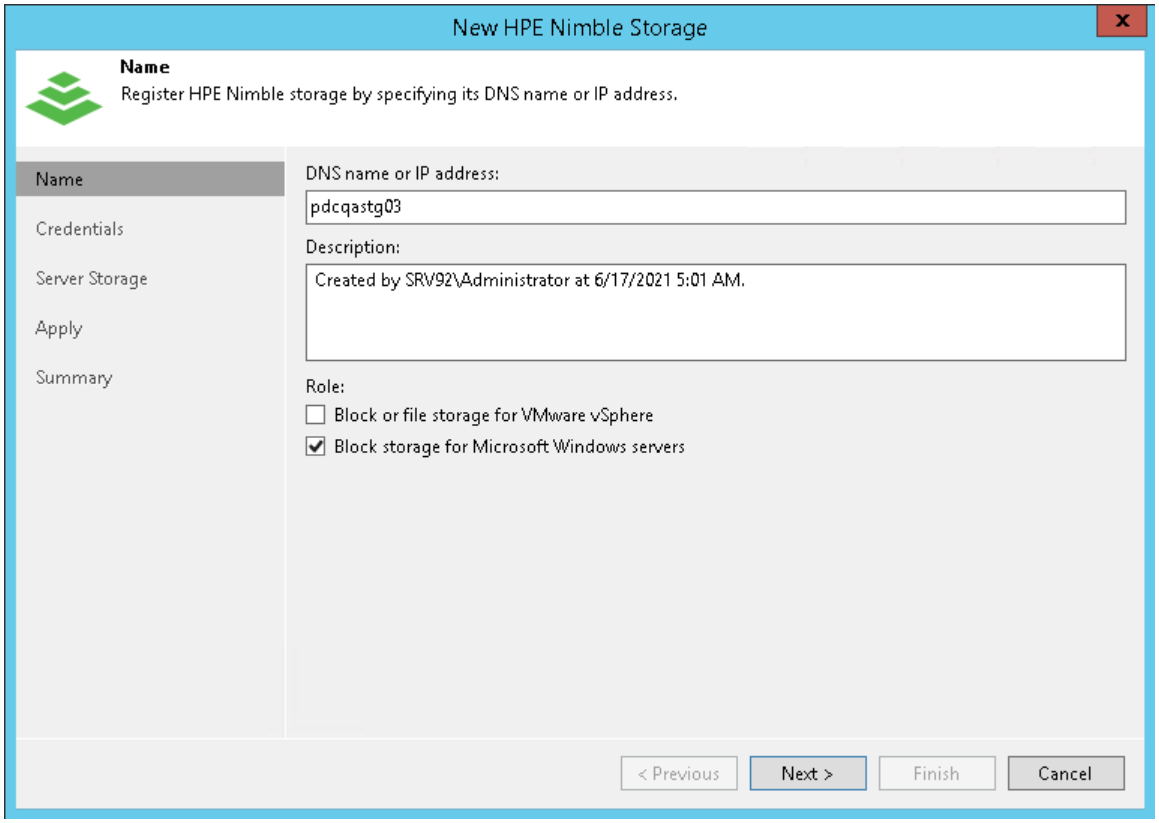
   If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

   - To view detailed information about the certificate, click **View**.
   - If you trust the server, click **Continue**.

- If you do not trust the server, click **Cancel**.

  Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.





Step 3. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   a. To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   b. To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   c. If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

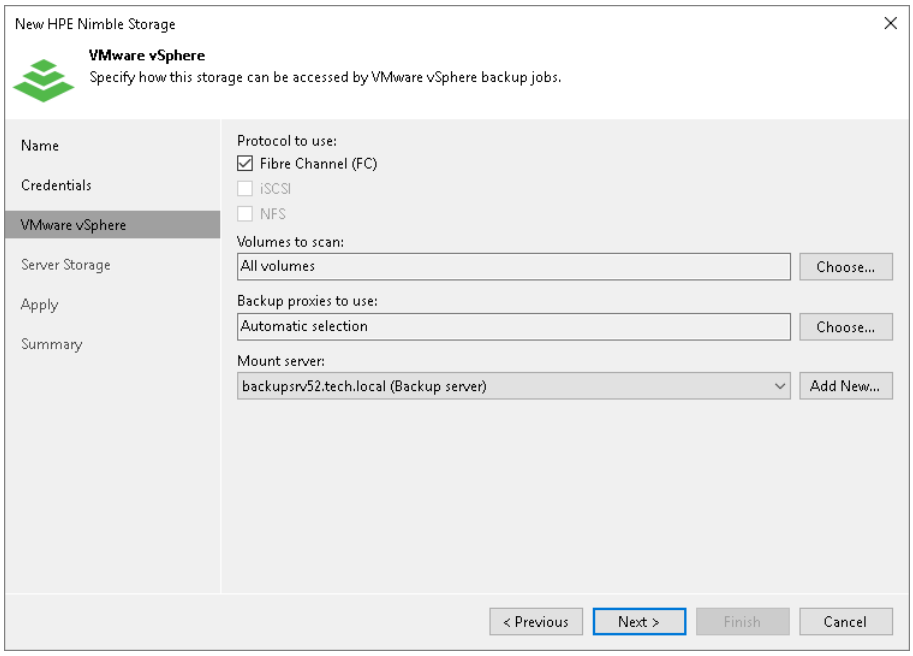
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

   > **IMPORTANT**
   >
   > If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

4. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 3. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.

The linked image cannot be dis...

Step 4. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

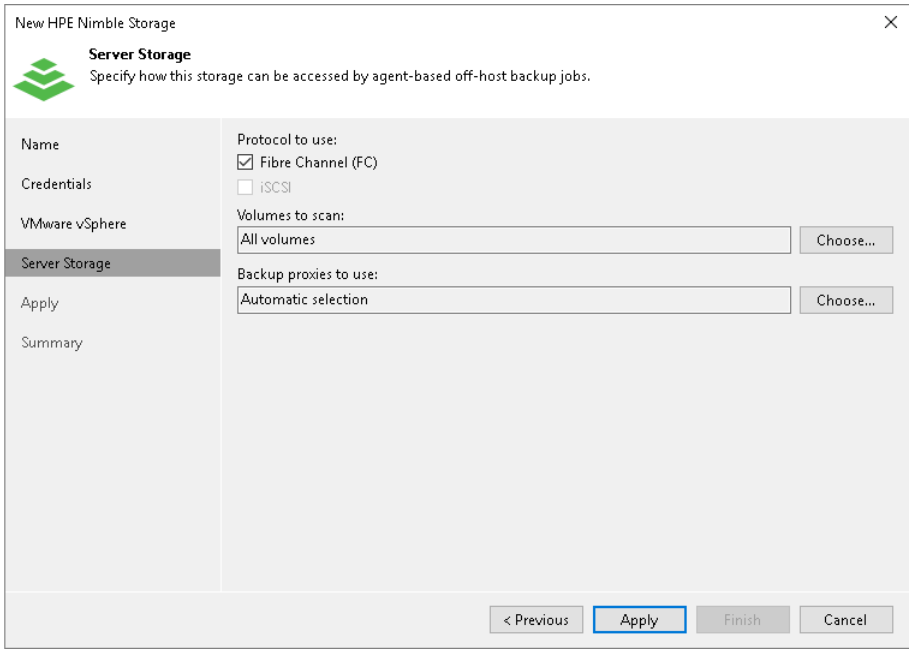
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

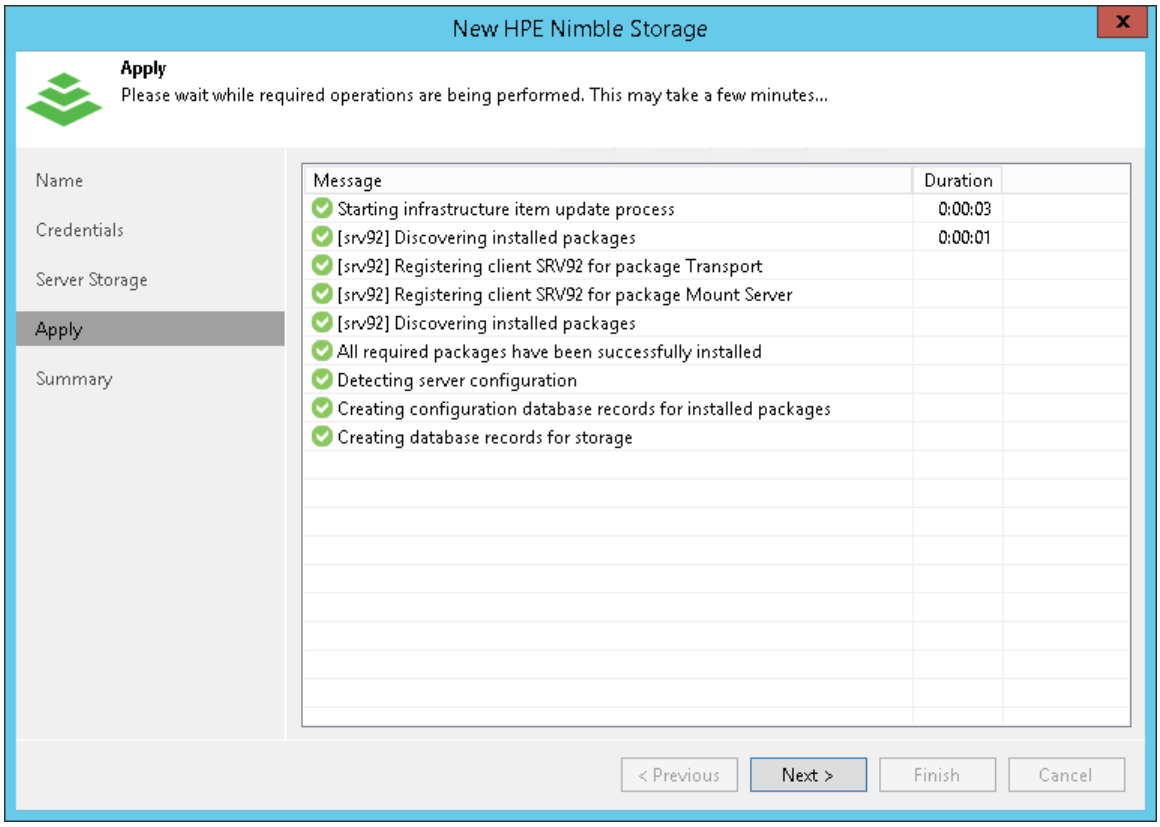
3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



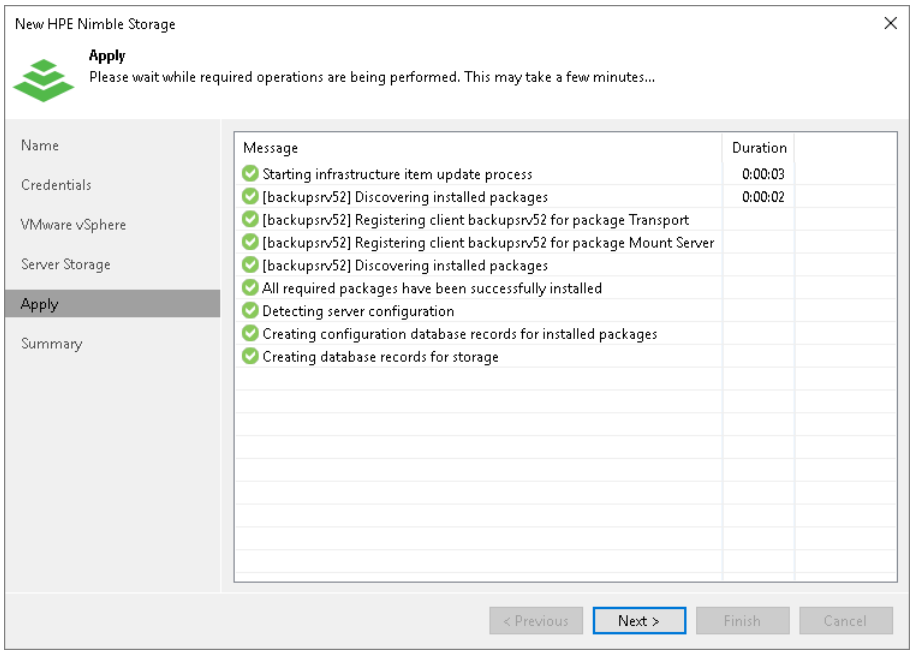
Step 4. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.



Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

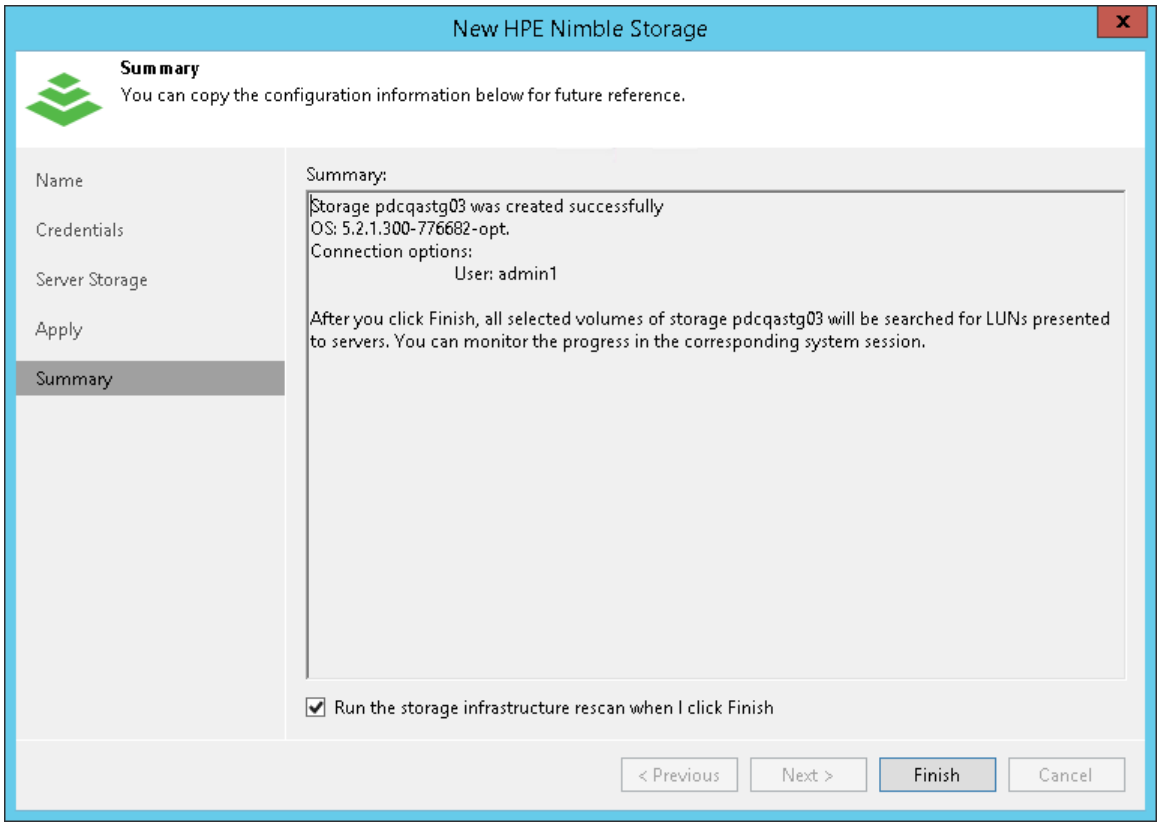


Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

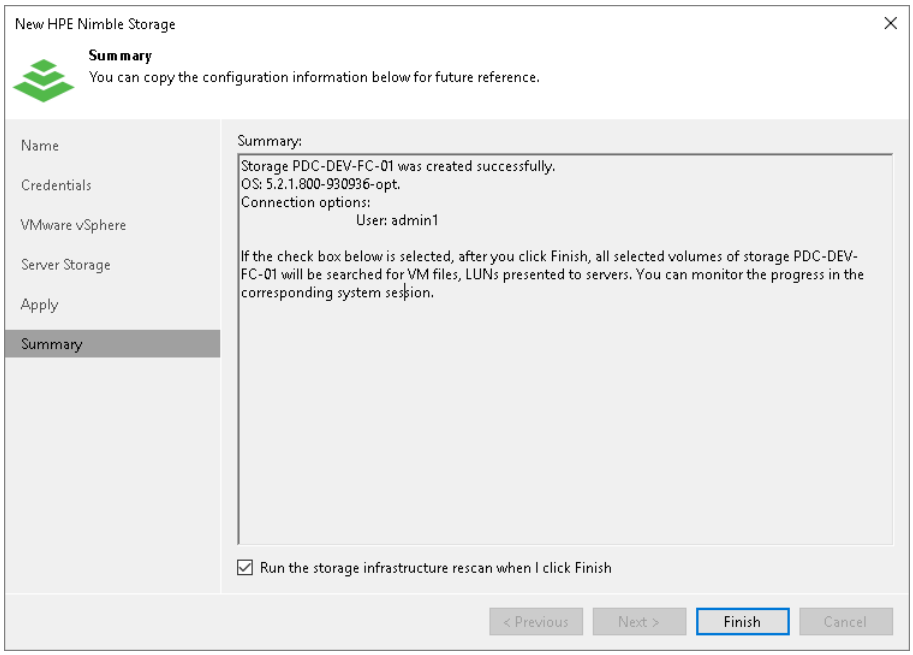


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding HPE 3PAR StoreServ, HPE Primera and Alletra 9000

Before you add an HPE 3PAR StoreServ or HPE Primera storage system to the backup infrastructure, check prerequisites. After that, do the following:

1. Enable HPE 3PAR Web Services API Server.
2. Specify HPE 3PAR Web Services API address and storage role.
3. Specify credentials.
4. Specify VMware access options.
5. Specify Veeam Agent access options.
6. Apply settings.
7. Finish working with the wizard.

Before you add an HPE 3PAR StoreServ or HPE Primera storage system to the backup infrastructure, check prerequisites. After that, do the following:

1. Enable HPE 3PAR Web Services API Server.
2. Specify HPE 3PAR Web Services API address and storage role.
3. Specify credentials.
4. Specify Veeam Agent access options.

5. Apply settings.
6. Finish working with the wizard.

Step 1. Enable HPE 3PAR Web Services API Server

Veeam Backup & Replication uses the HPE 3PAR Web Services API (WSAPI) server to communicate with HPE Primera and HPE 3PAR StoreServ storage systems.

Before you use the WSAPI server, you must make sure that the server is enabled and enable it if needed.

Enabling WSAPI Server Through SSH

To enable the WSAPI server, do the following:

1. Log on to the Processor with administrator privileges:

```
#ssh <administrator account>@<SP IP Address>
```

2. Run the following command to view the current state of the WSAPI server:

```
#showwsapi

-- -State- -HTTP_State-
HTTP_Port -HTTPS_State- HTTPS_Port -Version-
Enabled   Active Enabled       8008
Enabled       8080         1.1
```

3. If the WSAPI server is not running, run the following command to start it:

```
#startwsapi
```

4. If the HTTP port is disabled, run the following command to enable it:

```
#setwsapi -http enable
```

If the HTTPS port is disabled, run the following command to enable it:

```
#setwsapi -https enable
```

Enabling WSAPI Server Through Management Console

To enable the WSAPI server, do the following:

1. In your storage system management console, click **3PAR StoreServ**. Select *Systems*.
2. Select the storage system from the list.
3. In the next window, select *Services* in the drop-down list.

The state of the WSAPI server is displayed in the **WSAPI Provider** tab.

If it is not enabled, click the **Edit** button and enable the server.

Step 2. Specify HPE 3PAR Web Services API Address and Storage Role

Veeam Backup & Replication uses the HPE 3PAR Web Services API to work with HPE 3PAR StoreServ storage systems. The HPE 3PAR Web Services API delivers a programming interface for performing storage management tasks.

At the **Name** step of the wizard, provide information about the HPE 3PAR Web Services API Server, provide a description and storage role.

1. In the **DNS name or IP address** field, enter a full DNS name, or IPv4 or IPv6 address of the HPE 3PAR Web Services API Server or HPE Primera server. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Web Services API server URL** field, enter a URL of the HPE 3PAR Web Services API Server. By default, Veeam Backup & Replication uses the following URL:

   https://< websapiserver>:8080

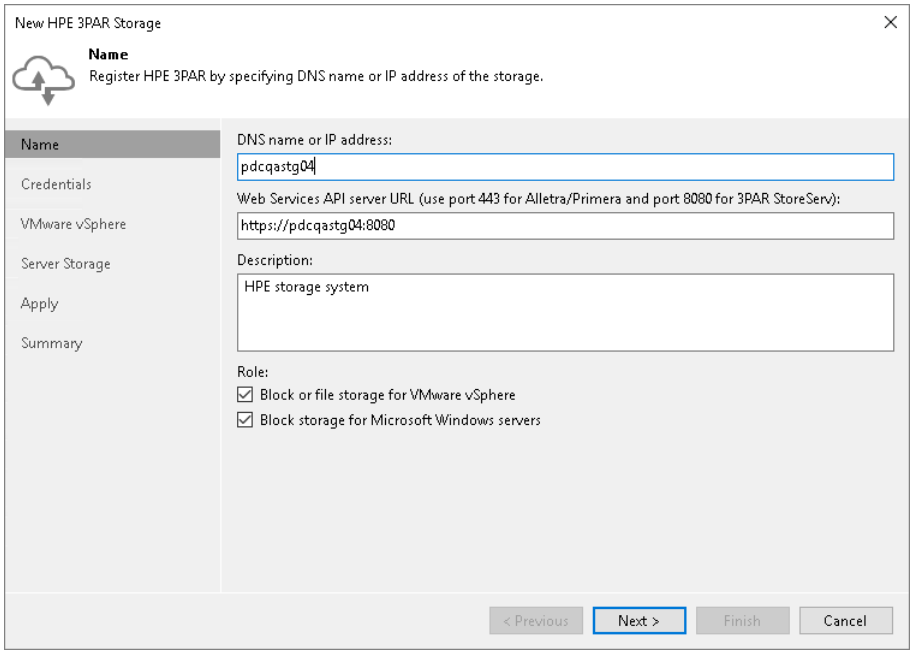
   where *<websapiserver>* is the name or IP address of the HPE 3PAR Web Services API Server.

   > **NOTE**
   >
   > If you add the storage system using an IPv6 address, make sure that the IP part is enclosed in square brackets: *https://[< websapiserver>]:8080.*

3. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the server, date and time when the server was added.
4. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 2. Specify HPE 3PAR Web Services API Address and Storage Role

Veeam Backup & Replication uses the HPE 3PAR Web Services API to work with HPE 3PAR StoreServ storage systems. The HPE 3PAR Web Services API delivers a programming interface for performing storage management tasks.

At the **Name** step of the wizard, provide information about the HPE 3PAR Web Services API Server, provide a description and storage role.

1. In the **DNS name or IP address** field, enter a full DNS name, or IPv4 or IPv6 address of the HPE 3PAR Web Services API Server or HPE Primera server. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **URL** field, enter a URL of the HPE 3PAR Web Services API Server. By default, Veeam Backup & Replication uses the following URL:

   https://< websapiserver>:8080

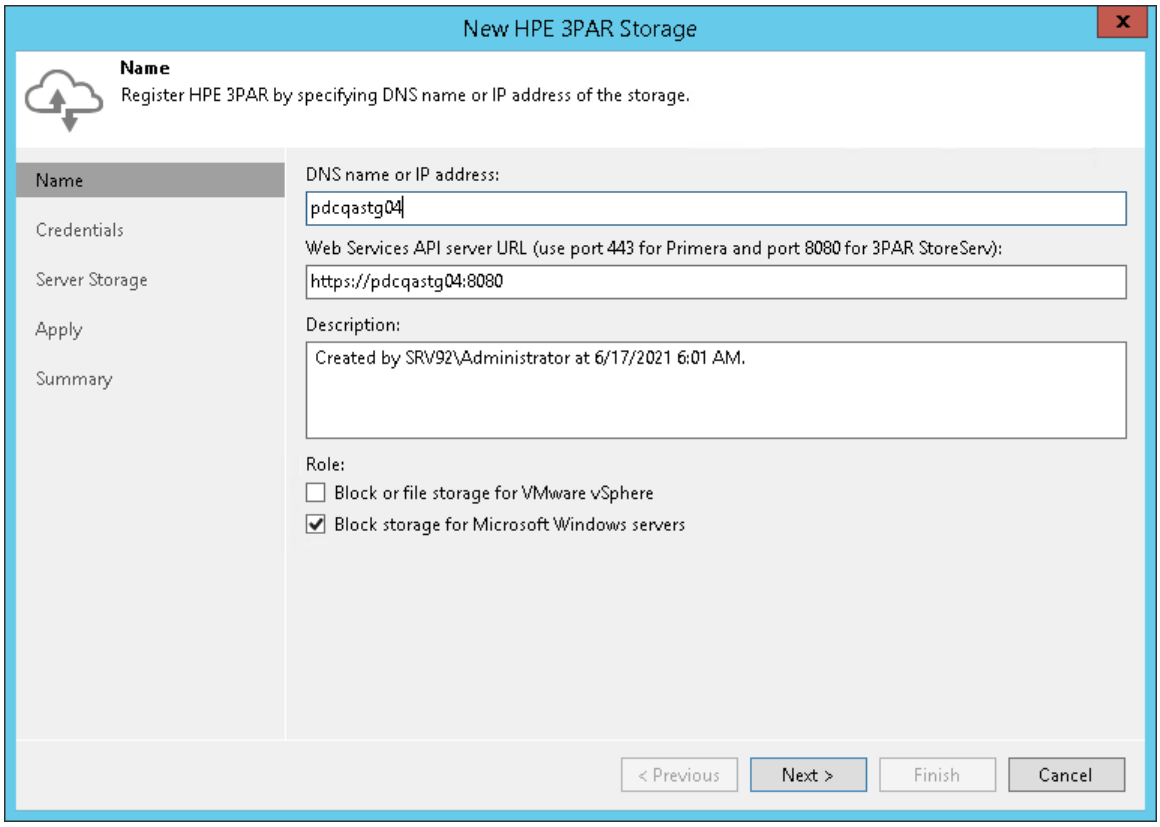
   where *<websapiserver>* is the name or IP address of the HPE 3PAR Web Services API Server.
3. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the server, date and time when the server was added.
4. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:

   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.

   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the HPE 3PAR Web Services API Server.

1. From the **Credentials** list, select credentials to connect to the HPE 3PAR Web Services API Server. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the necessary credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

   > **IMPORTANT**
   >
   > The user account must have the 'edit' user role on the HPE 3PAR Web Services API Server.

2. When you add a storage system, Veeam Backup & Replication saves to the configuration database a TLS certificate thumbprint and an SSH key fingerprint of the HPE 3PAR Web Services API Server. During every subsequent connection to the server, Veeam Backup & Replication uses the saved information to verify the server identity and avoid the man-in-the-middle attack.

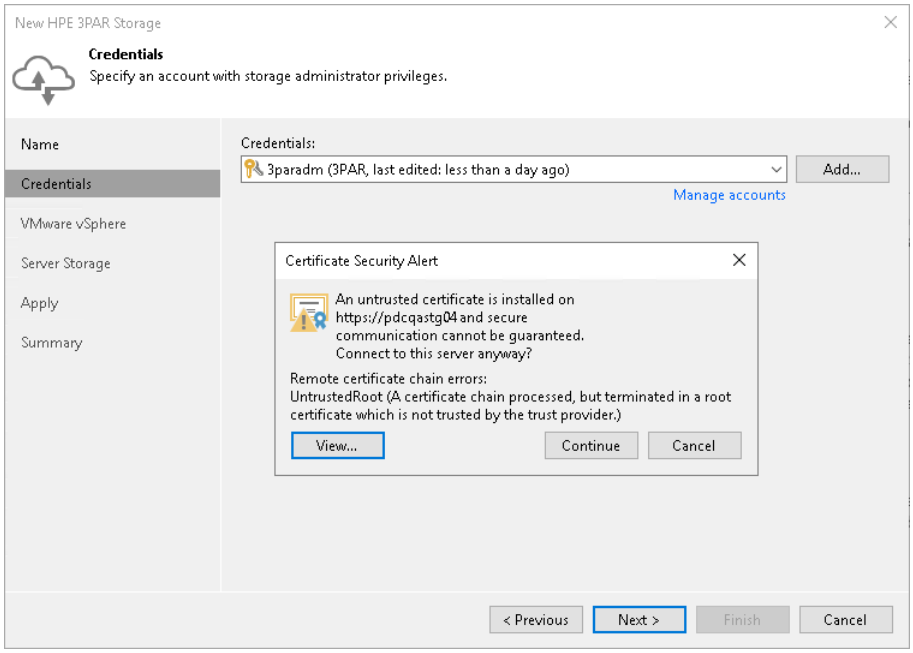
   If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

   - To view detailed information about the certificate, click **View**.
   - If you do not trust the server, click **Cancel**.

     Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.
   - If you trust the server, click **Continue**.

     Veeam Backup & Replication will display the SSH key fingerprint. To accept the fingerprint and connect to the server, click **Yes**.

When you update a certificate or SSH key on a server, this server becomes unavailable in the Veeam Backup & Replication console. To make the server available again, acknowledge the new certificate or SSH key at the **Credentials** step of the edit storage system wizard.



The linked image cannot be dis...

Step 4. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify HPE 3PAR Web Services API Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   a. To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   b. To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   c. If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

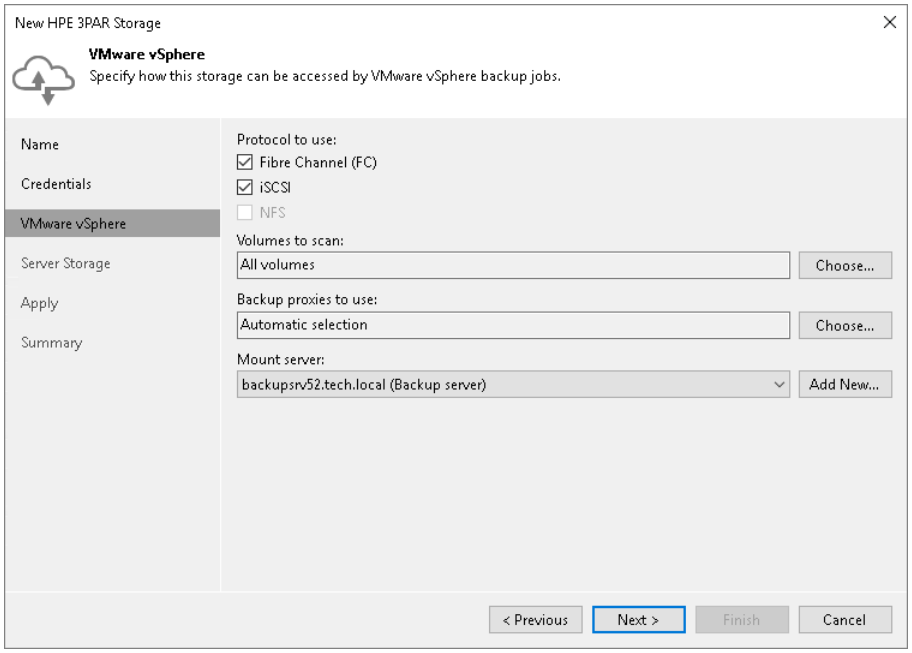
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

   > **IMPORTANT**
   >
   > If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

4. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 4. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify HPE 3PAR Web Services API Address and Storage Role step of the wizard.

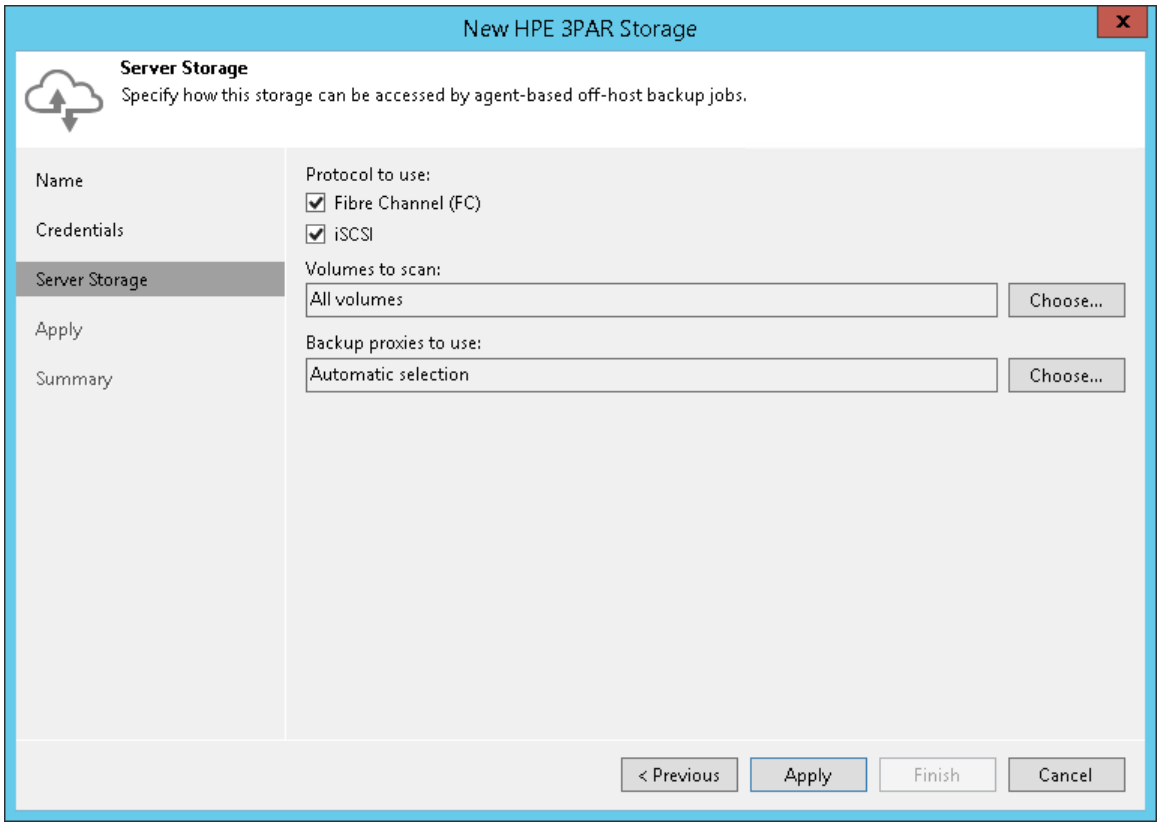
1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.



Step 5. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify HPE 3PAR Web Services API Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

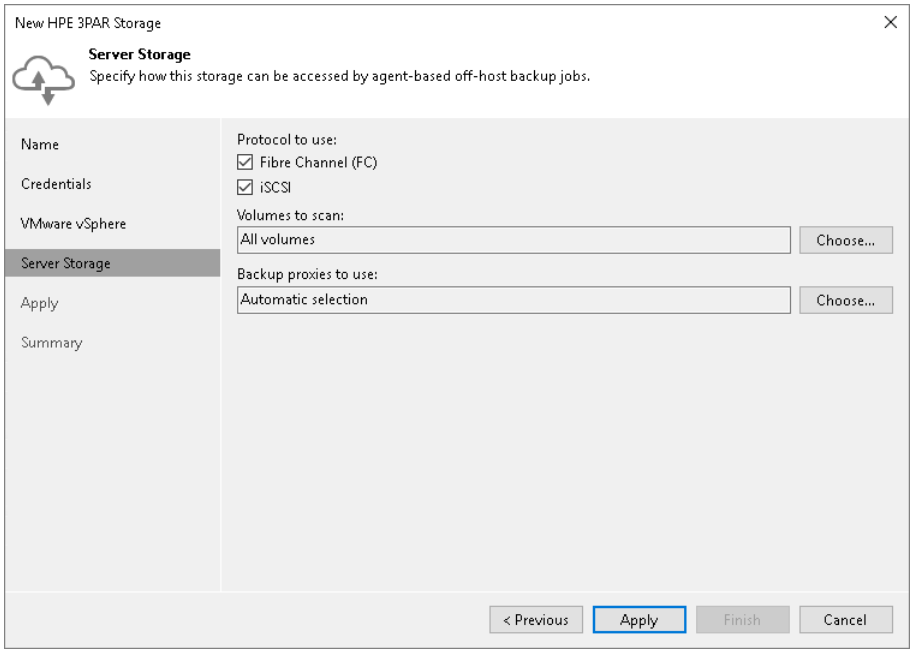
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

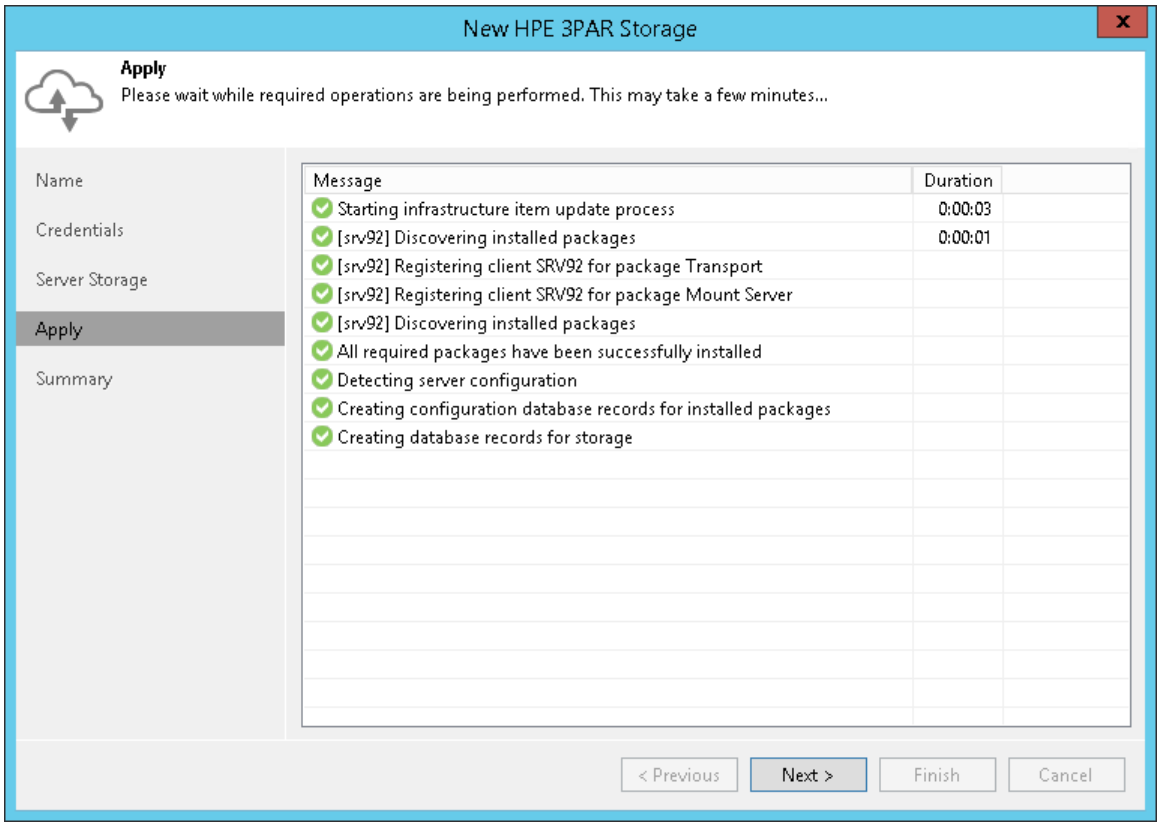
3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



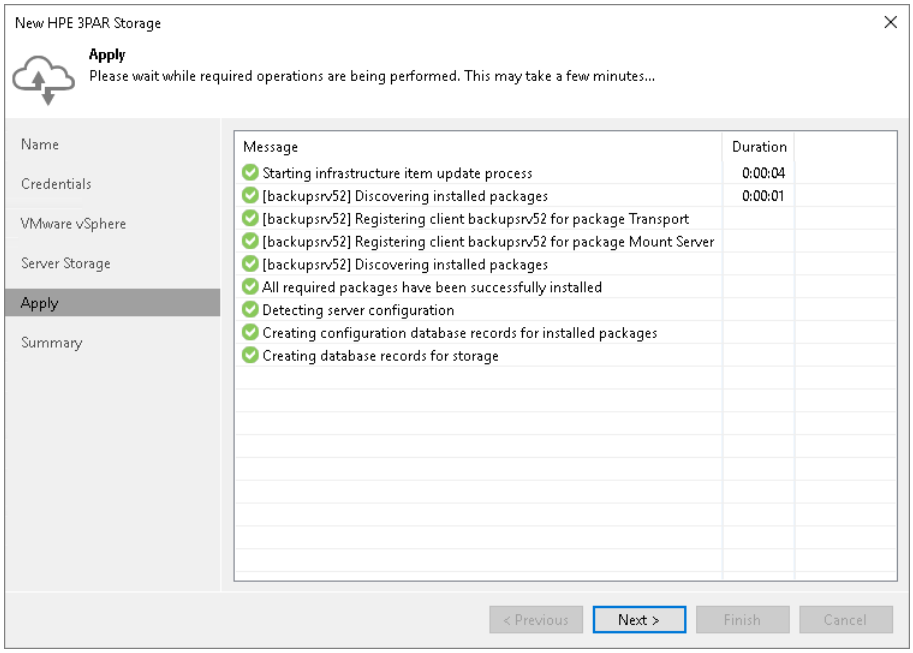
Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.



Step 6. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

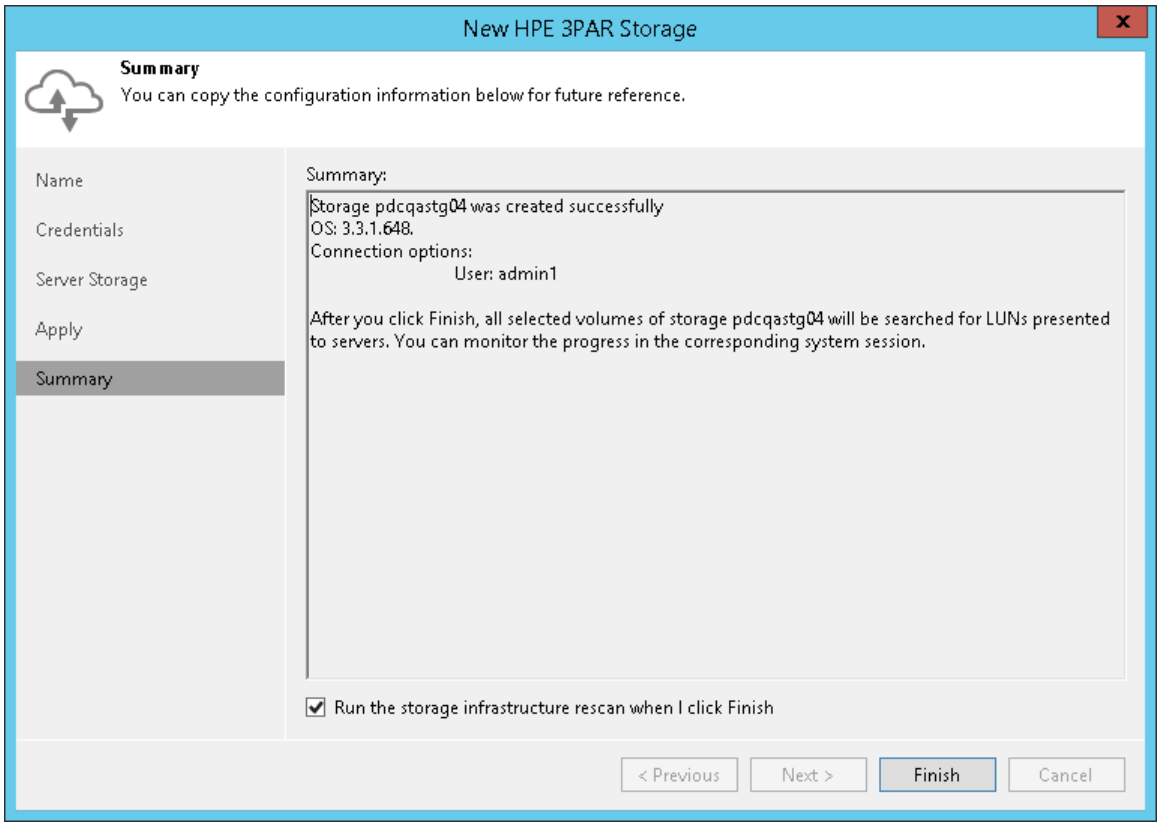


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

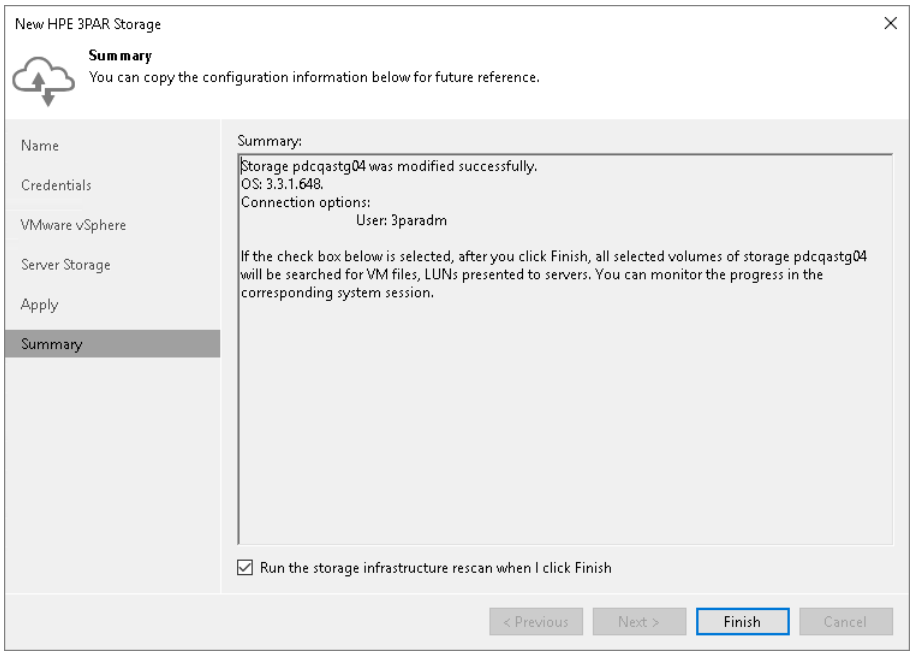


Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding HPE StoreVirtual

To add an HPE StoreVirtual/LeftHand/P4000 series storage system to the backup infrastructure, do the following:

1. Specify storage name or address and storage role.
2. Specify credentials.
3. Specify VMware access options.
4. Specify Veeam Agent access options.
5. Apply settings.
6. Finish working with the wizard.

To add an HPE StoreVirtual/LeftHand/P4000 series storage system to the backup infrastructure, do the following:

1. Specify storage name or address and storage role.
2. Specify credentials.
3. Specify Veeam Agent access options.
4. Apply settings.
5. Finish working with the wizard.

Step 1. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. On the right of the **Management server DNS name or IP address** field, click **Browse** and select an HPE storage management group.

   You can also type a DNS name or IPv4 address of the storage management server or storage cluster in the **Management server DNS name or IP address** field.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the management group, date and time when the HPE management group was added.

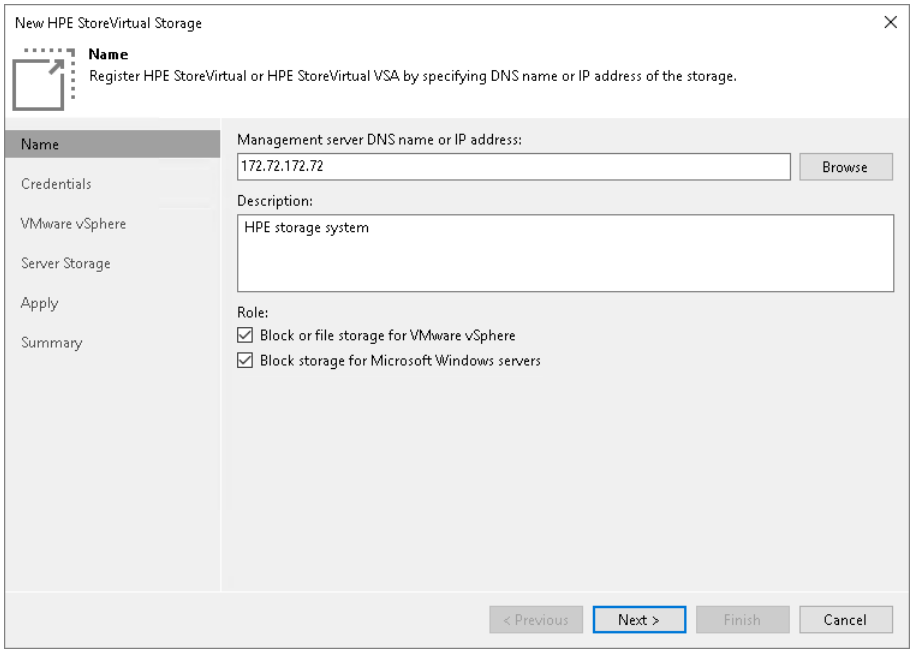
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:

   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.

   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 1. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. On the right of the **Management server DNS name or IP address** field, click **Browse** and select an HPE storage management group.

   You can also type a DNS name or IPv4 address of the storage management server or storage cluster in the **Management server DNS name or IP address** field.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the management group, date and time when the HPE management group was added.

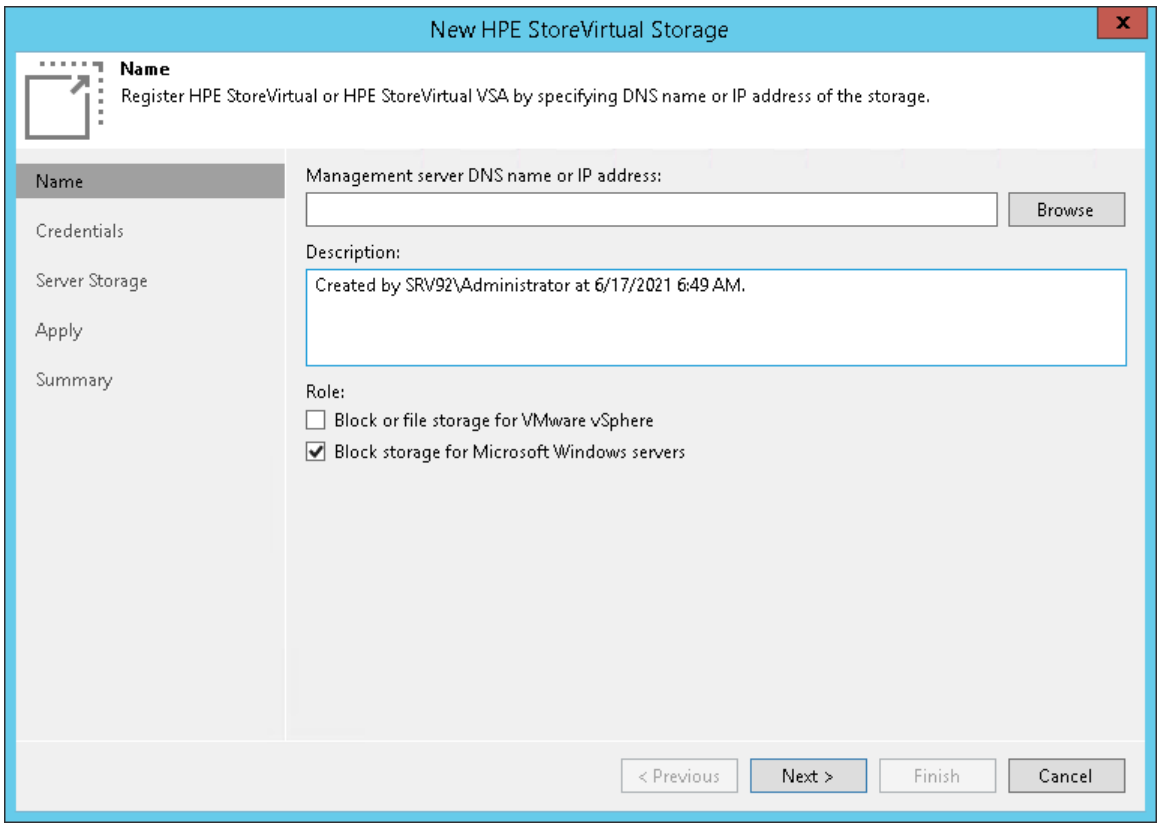
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:

   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.

   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 2. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the management group.

1. From the **Credentials** list, select credentials to connect to the management group. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

   > **NOTE**
   >
   > User name and password values are case-sensitive.

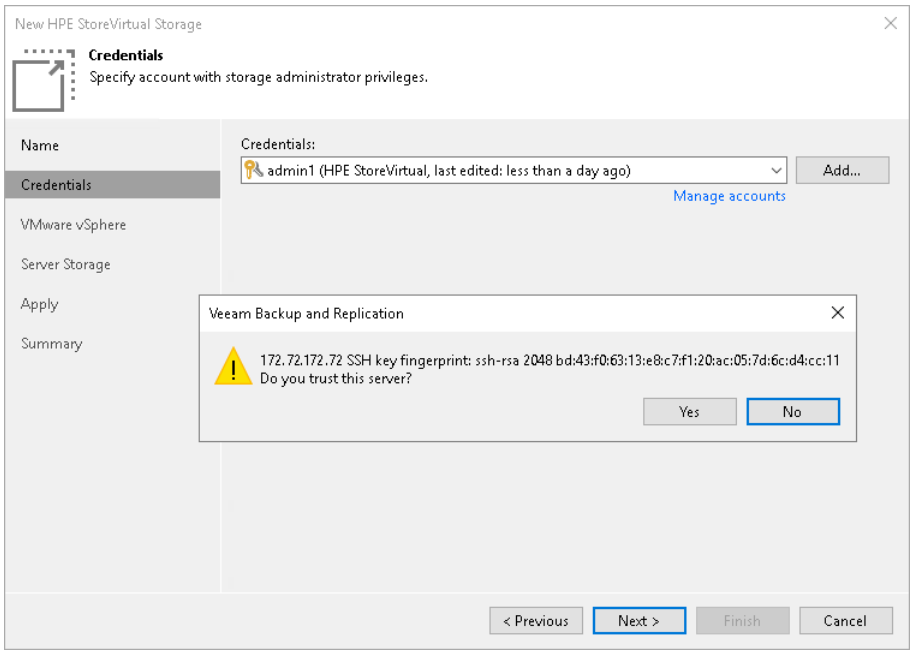
2. When you add a storage system, Veeam Backup & Replication saves a fingerprint of the SSH key of the management server to the configuration database. During every subsequent connection to the server, Veeam Backup & Replication uses the saved fingerprint to verify the server identity and avoid man-in-the-middle attacks.

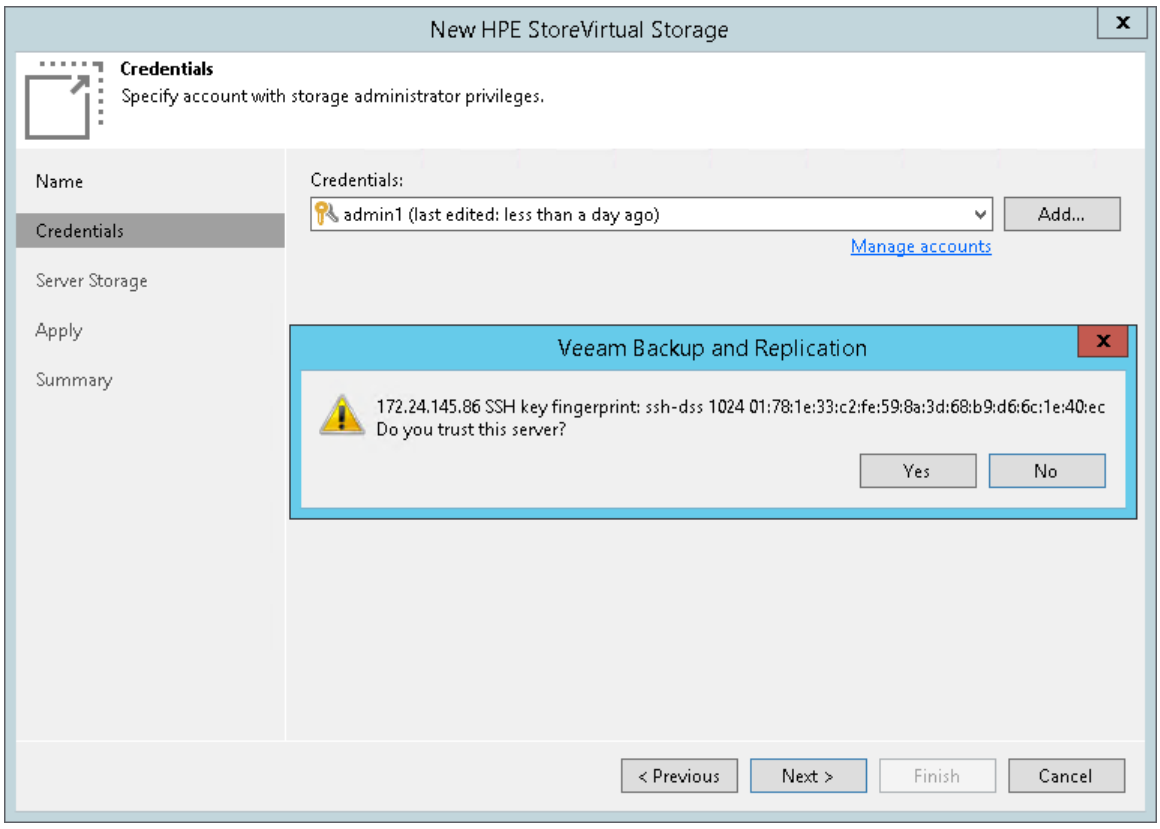
   To let you identify the server, Veeam Backup & Replication displays the SSH key fingerprint.

   - If you trust the server and want to connect to it, click **Yes**.

- If you do not trust the server, click **No**. Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

When you update an SSH key on a server, this server becomes unavailable in the Veeam Backup & Replication console. To make the server available again, acknowledge the new SSH key at the **Credentials** step of the edit storage system wizard.





Step 3. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   a. To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   b. To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   c. If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

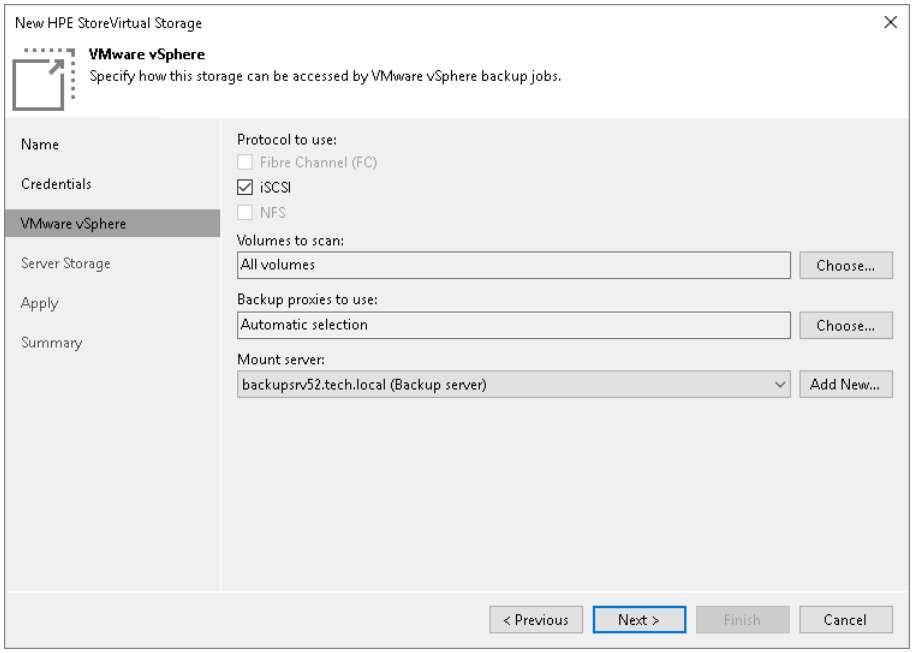
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

   > **IMPORTANT**
   >
   > If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

4. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 3. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

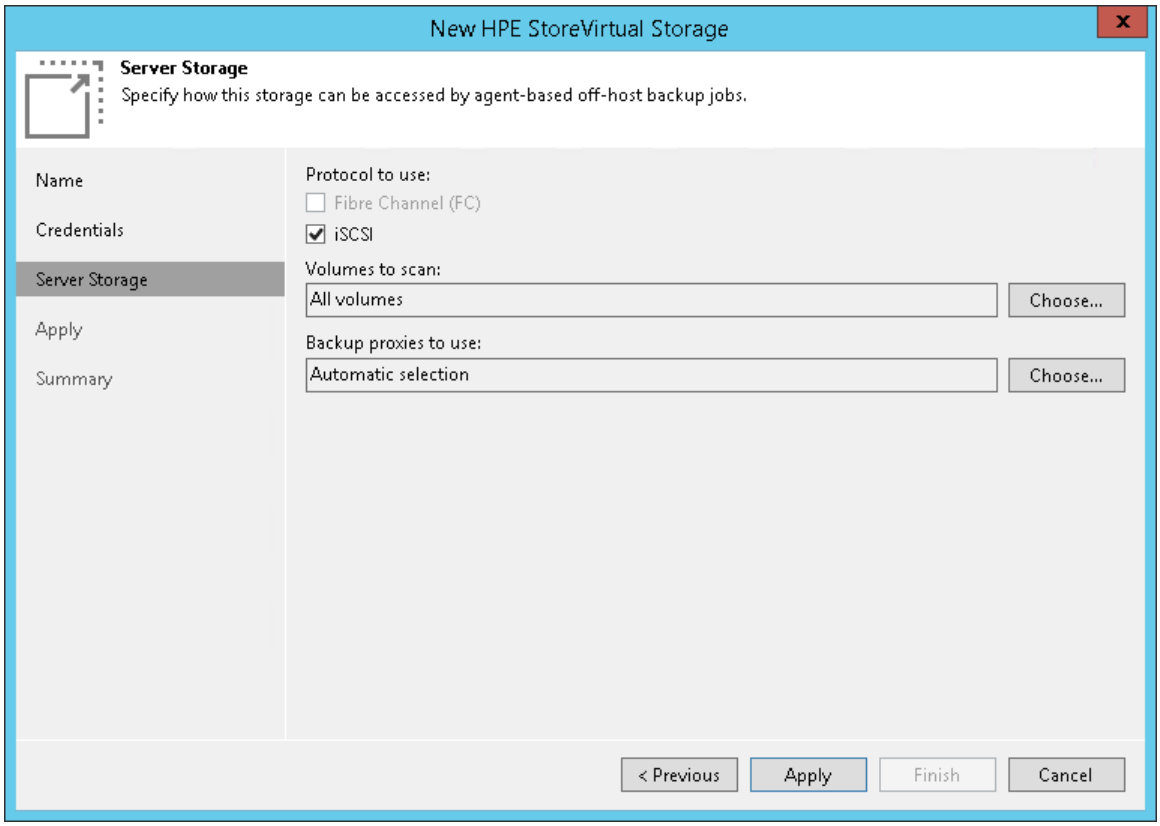
1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.



Step 4. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to** scan field. In the **Edit Volumes** window, select volumes you want to rescan:

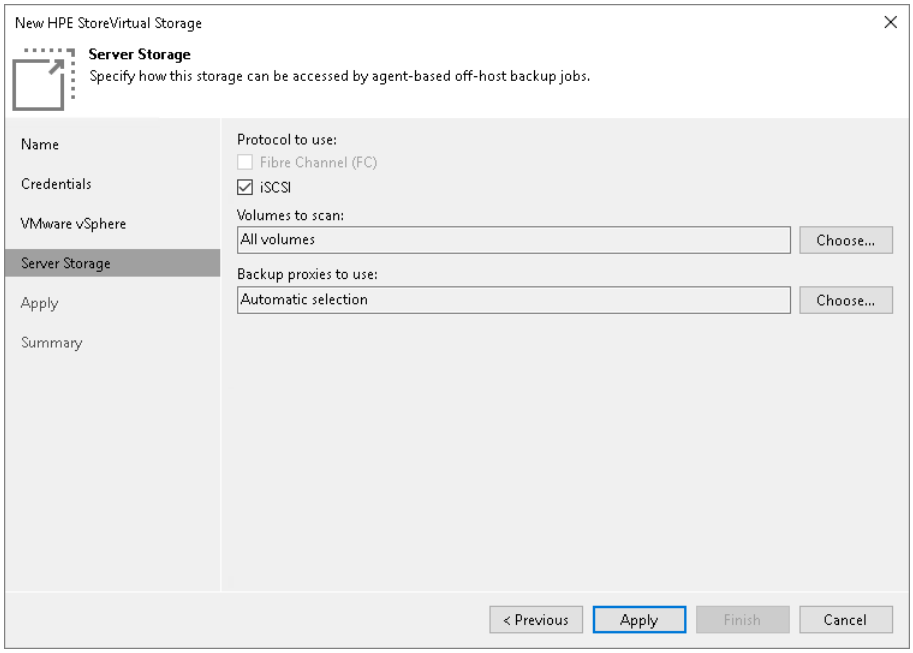
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

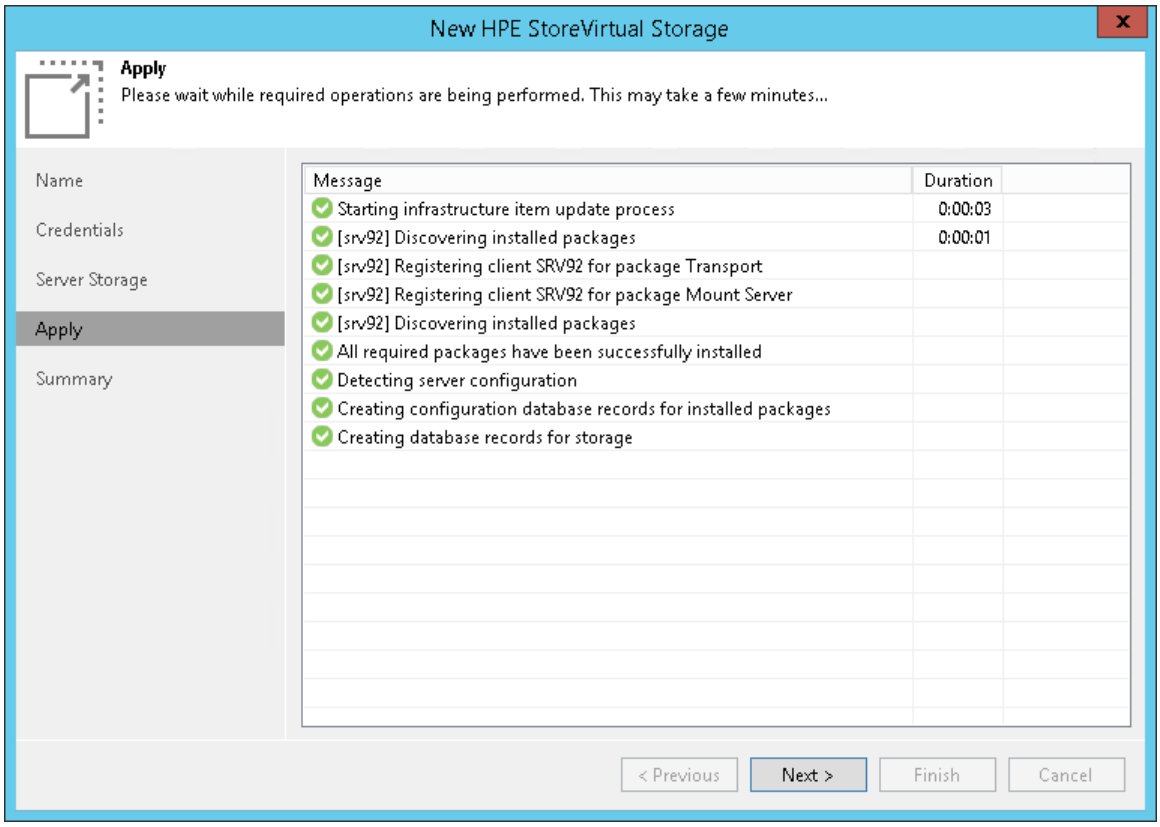
3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



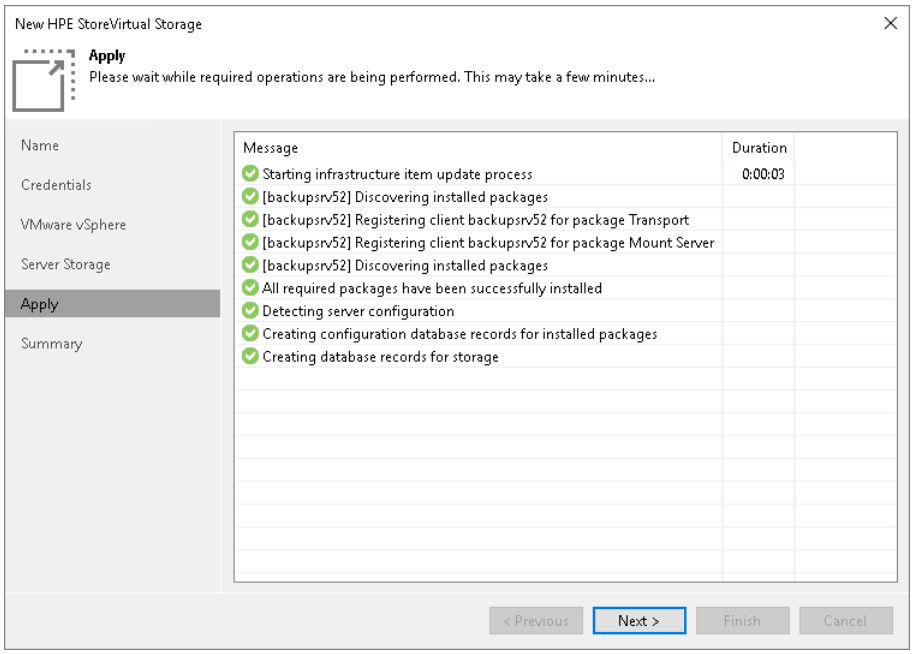
Step 4. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.



Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

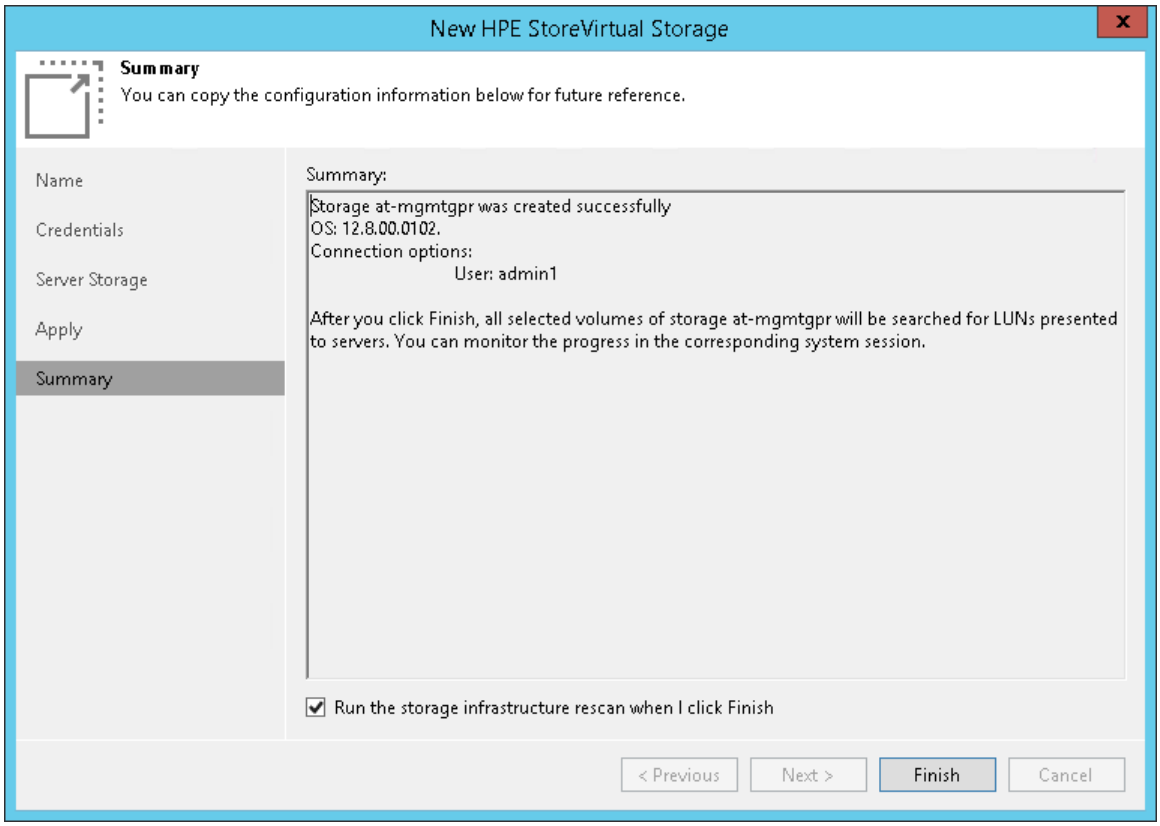


Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

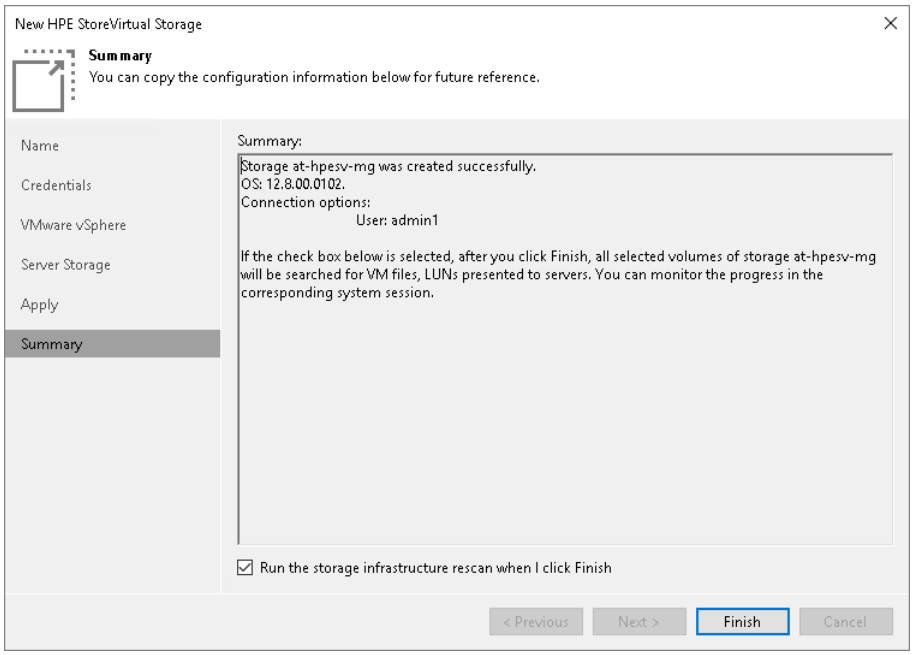


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding IBM Spectrum Virtualize

Before you add a storage system to the backup infrastructure, check prerequisites. Then use the **New IBM Spectrum Virtualize Storage** wizard.

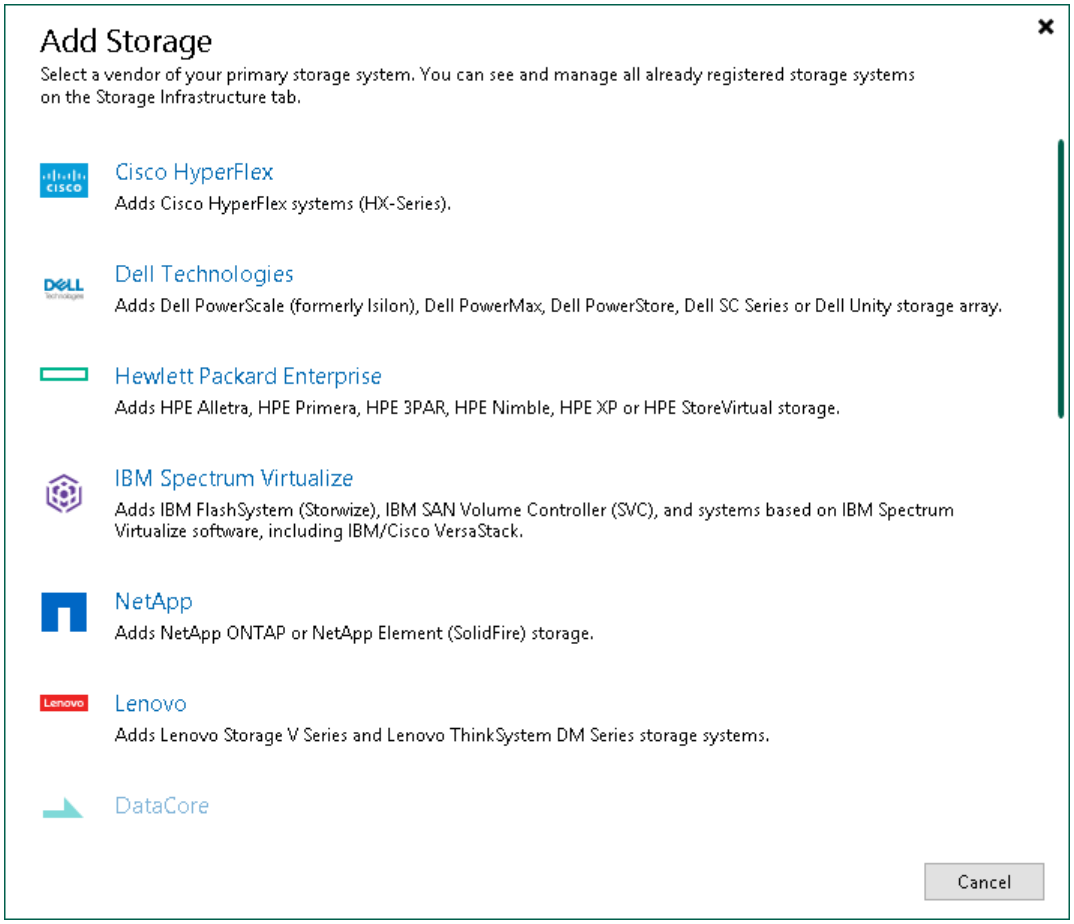
Before you add a storage system to the backup infrastructure, check prerequisites. Then use the **New IBM Spectrum Virtualize Storage** wizard.

Step 1. Launch New IBM Spectrum Virtualize Storage Wizard

To launch the **New IBM Spectrum Virtualize Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **IBM Spectrum Virtualize**.
- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **IBM Spectrum Virtualize**.
- You can use this method if at least one IBM Spectrum Virtualize storage system is added to the backup infrastructure.

  Open the **Storage Infrastructure** view. In the inventory pane, right-click the **IBM Spectrum Virtualize** node under **Storage Infrastructure** and select **Add storage**. You can also select the **IBM Spectrum Virtualize** node in the inventory pane, right-click anywhere in the working area and select **Add storage**.



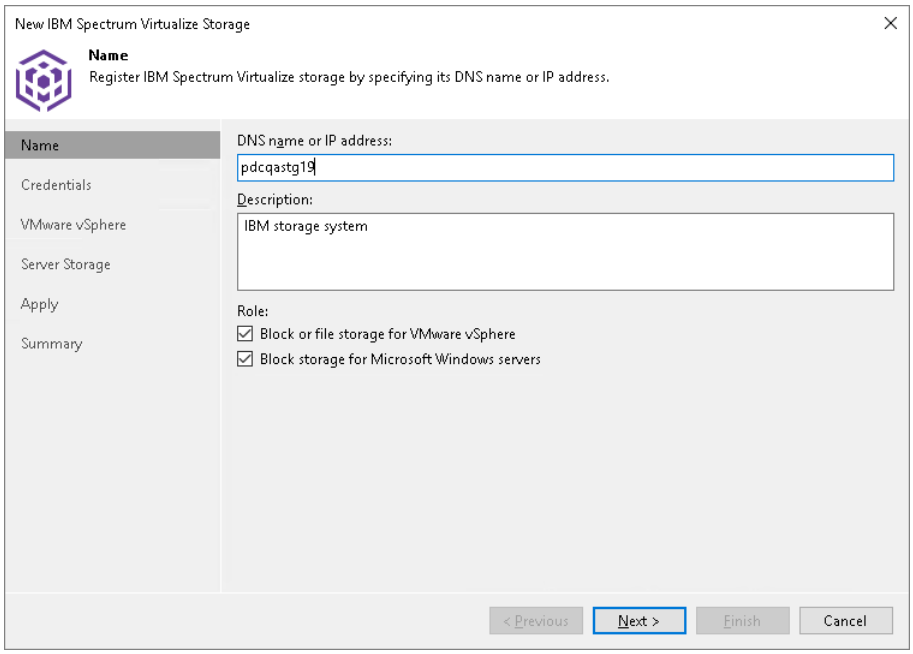
Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **DNS Name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



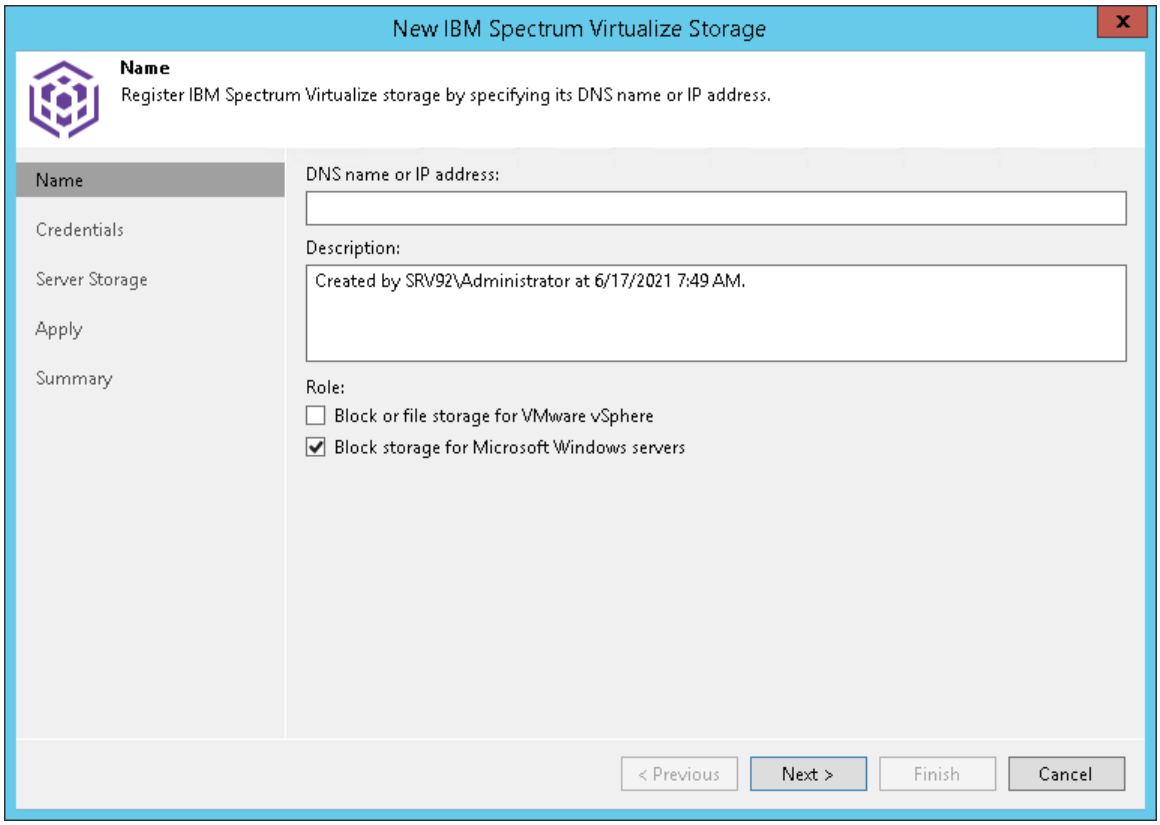
Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **DNS Name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



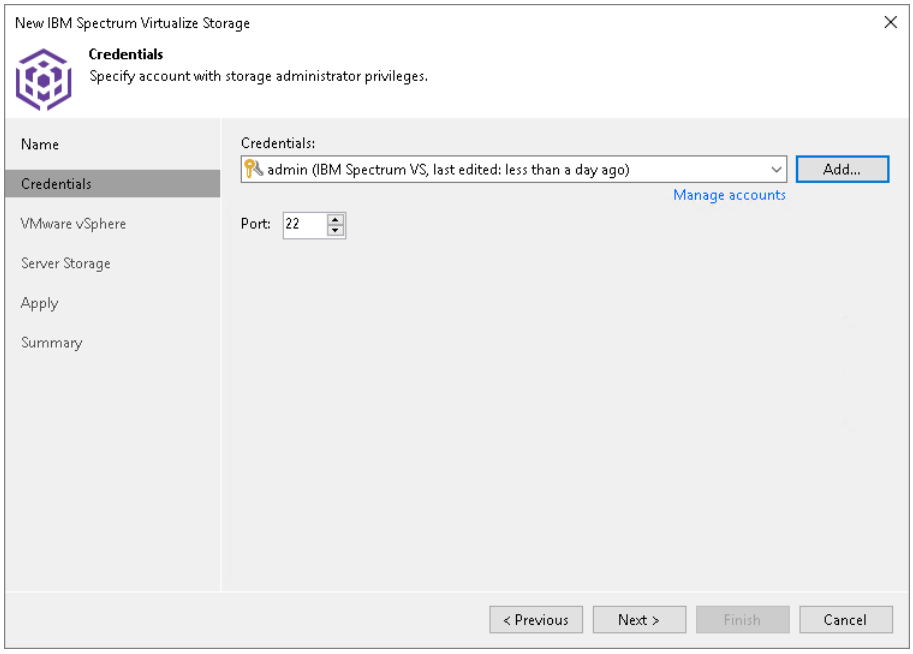
Step 3. Specify Credentials

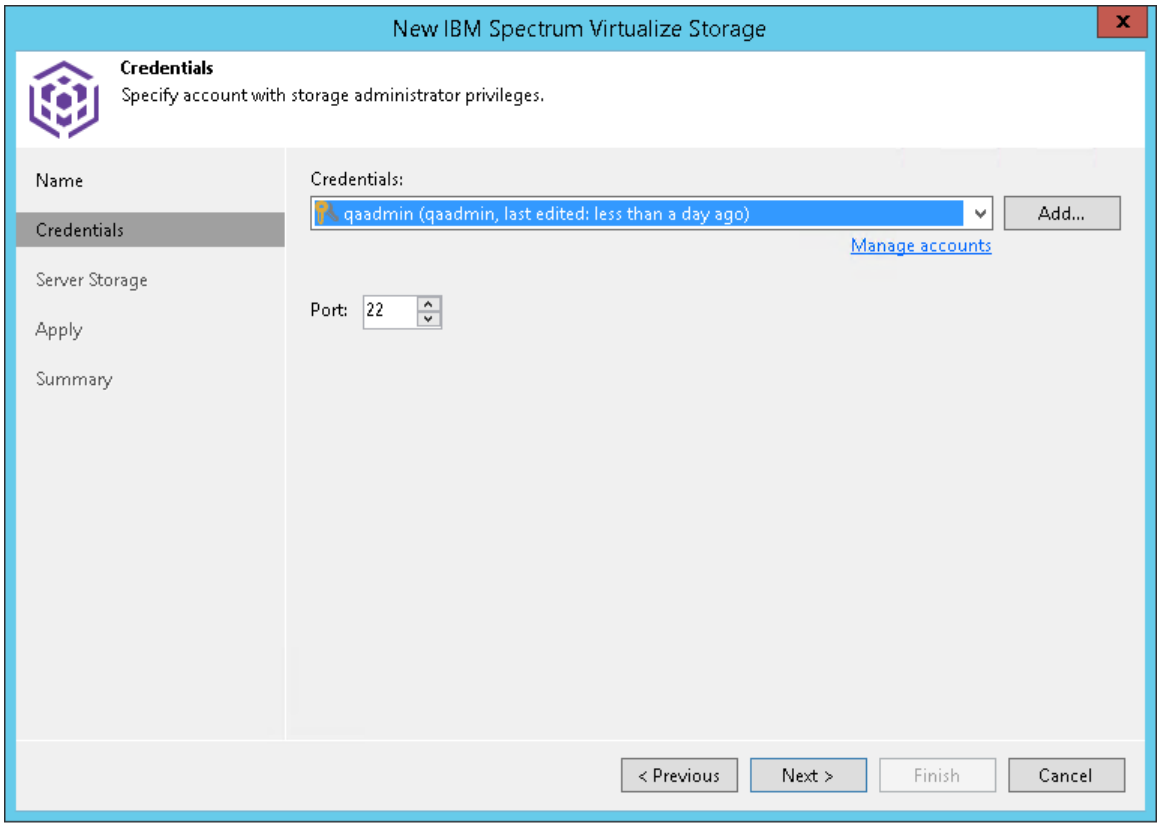
At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the Credentials list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the Manage accounts link or click Add on the right of the Credentials field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

   > **NOTE**
   >
   > User name and password values are case-sensitive.

2. The default port for communication with the storage system is 22. If necessary, you can change the port number in storage system settings and specify the new port number in the **Port** field.





Step 4. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   a. To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   b. To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   c. If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

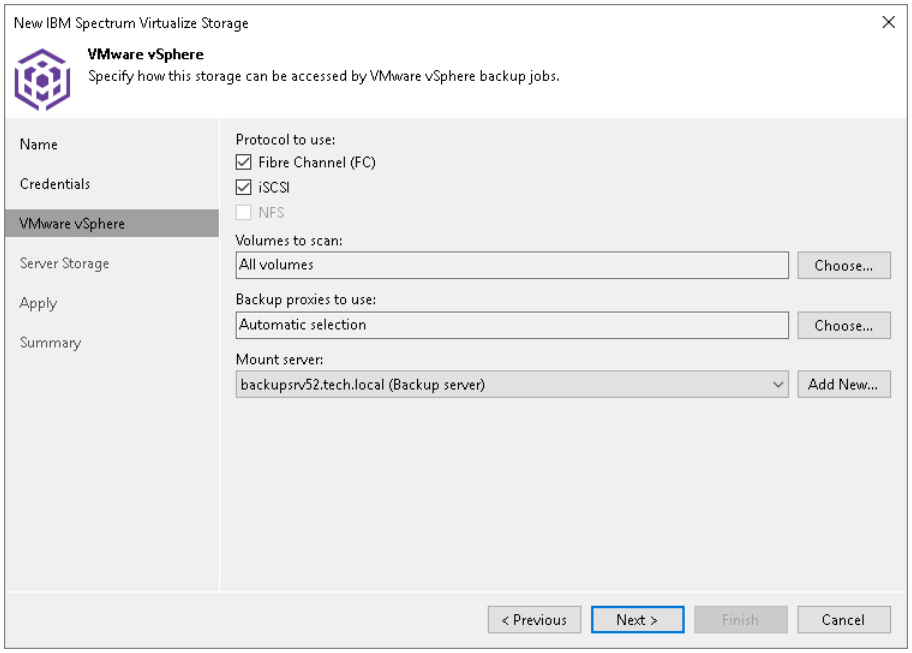
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

   > **IMPORTANT**
   >
   > If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

4. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 4. Specify Veeam Agent Access Options

At the **Storage Server** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

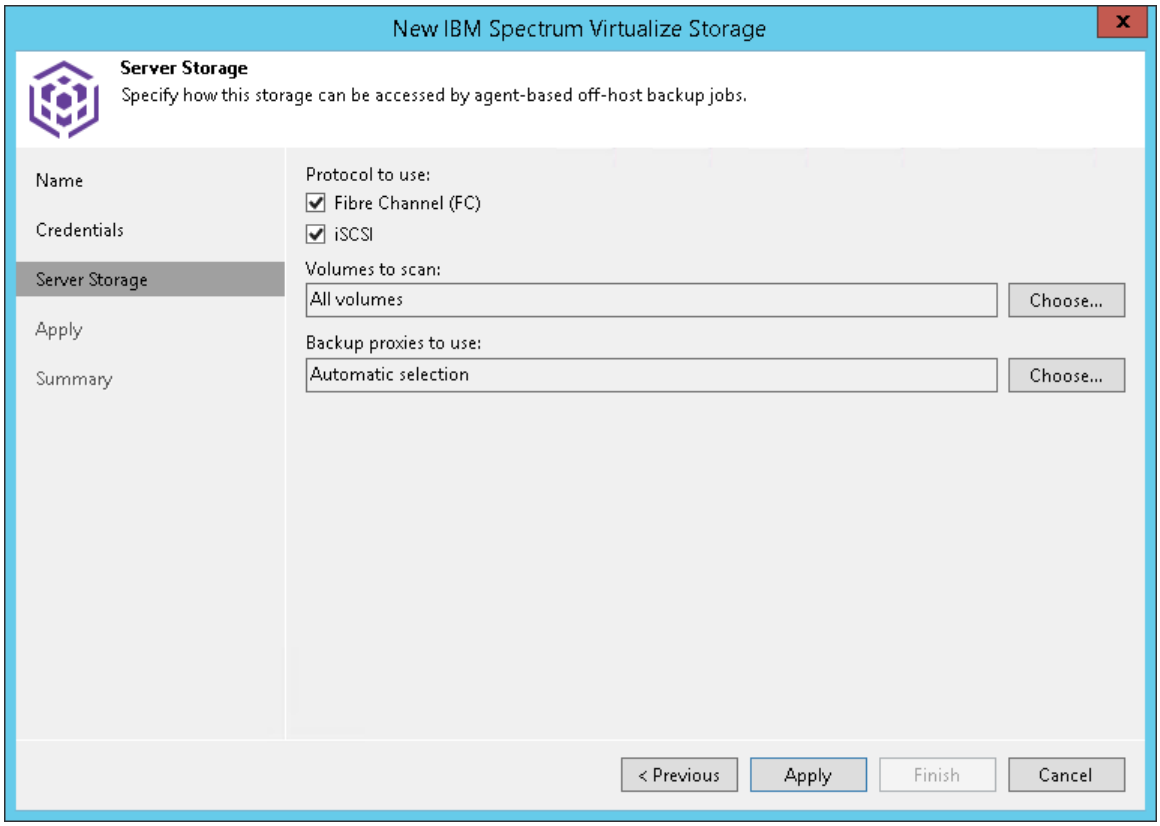
1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.



Step 5. Specify Veeam Agent Access Options

At the **Storage Server** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

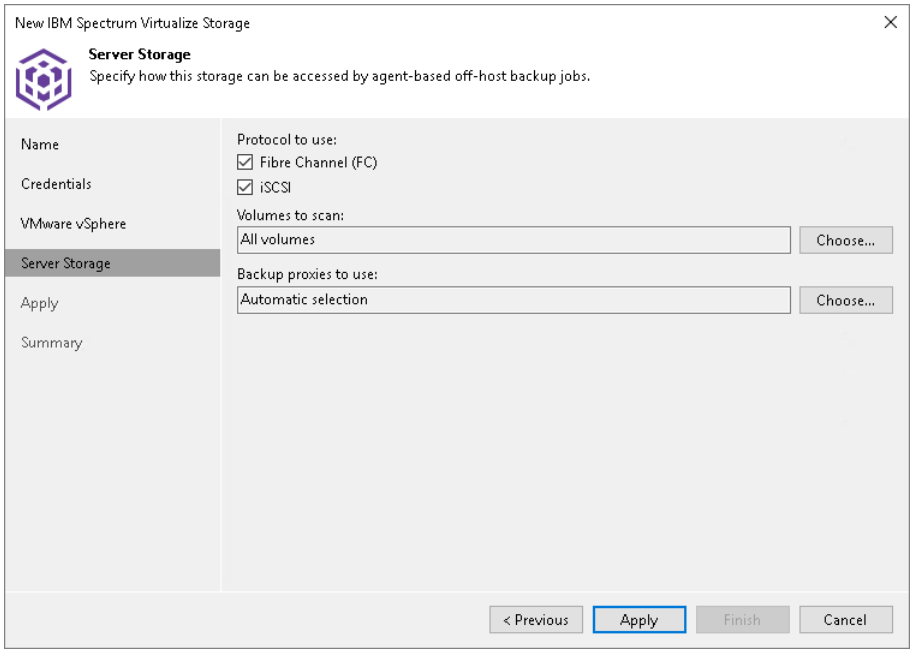
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

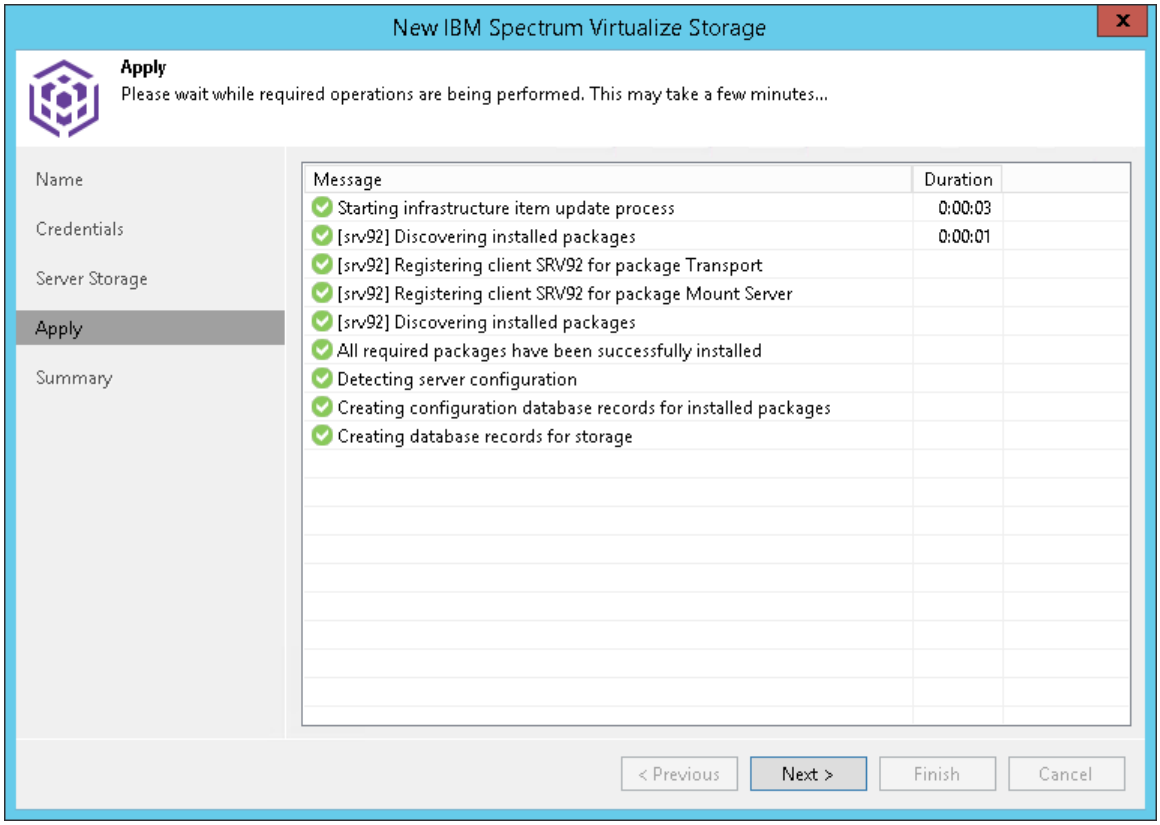
3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



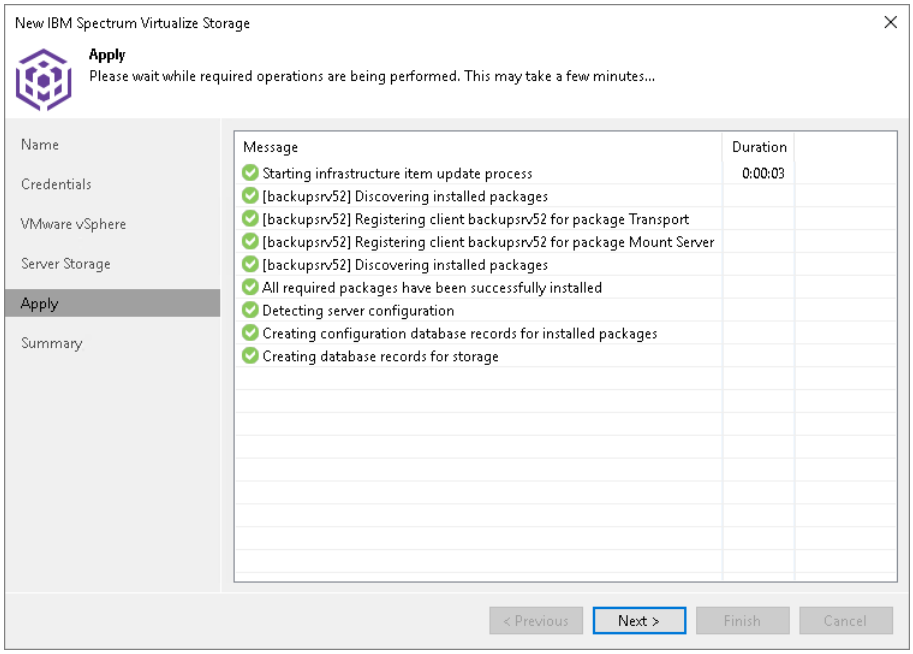
Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.



Step 6. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

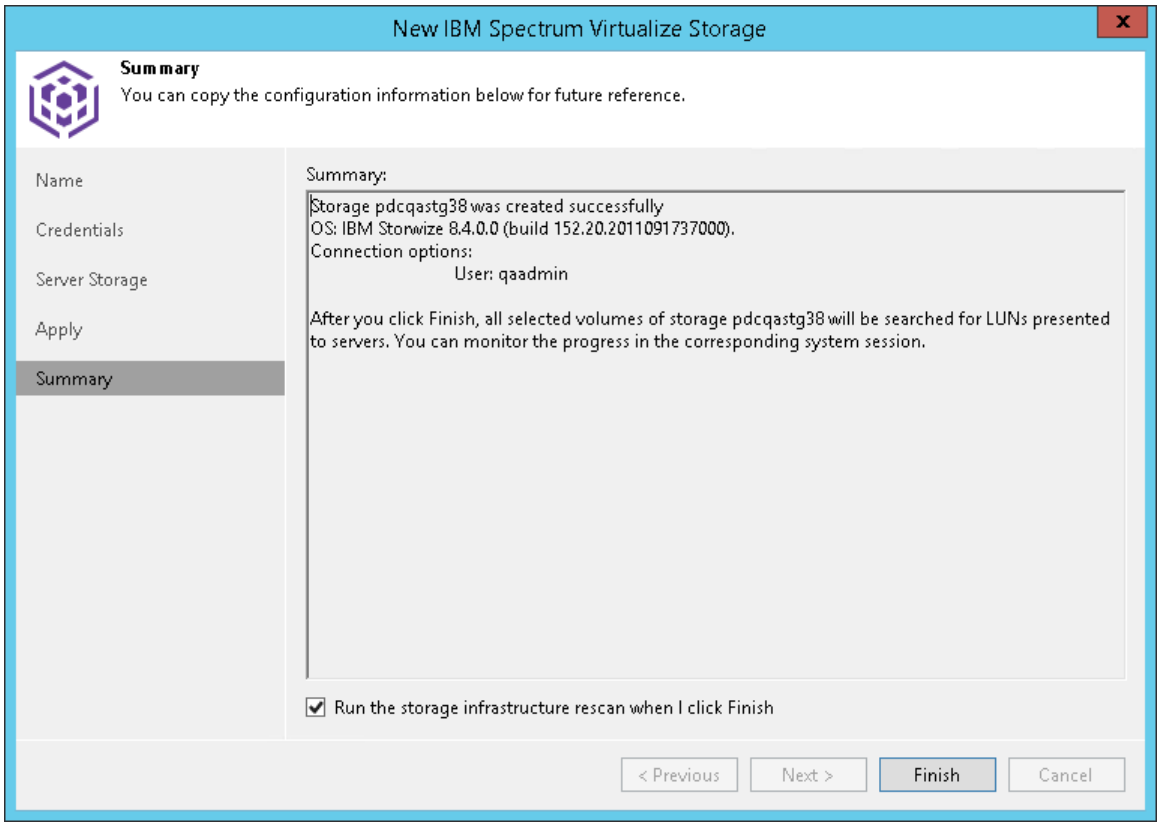


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

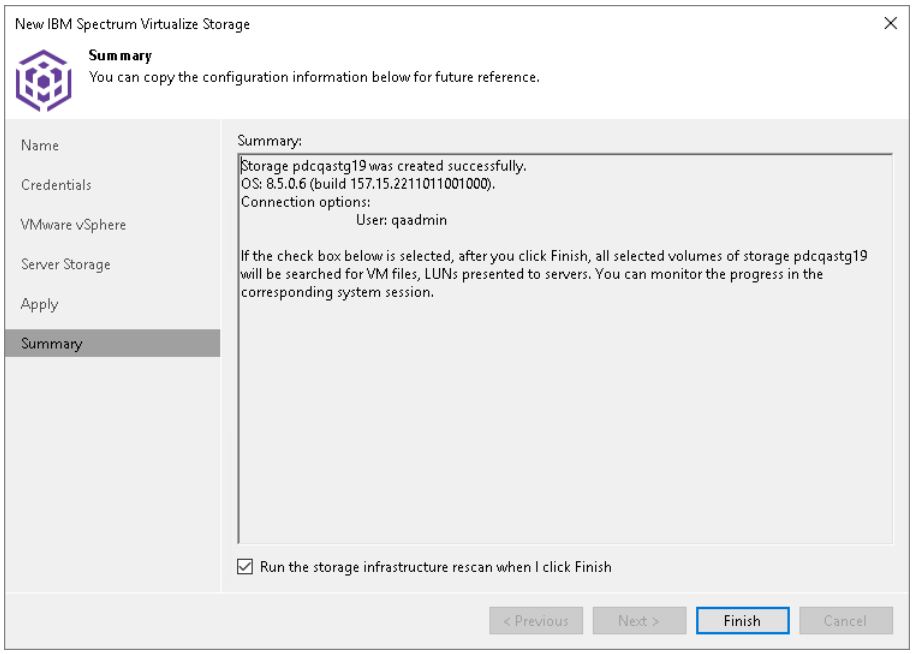


Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding Lenovo

Before you add a Lenovo storage system to the backup infrastructure, check prerequisites. Then use the wizard to add the storage system.

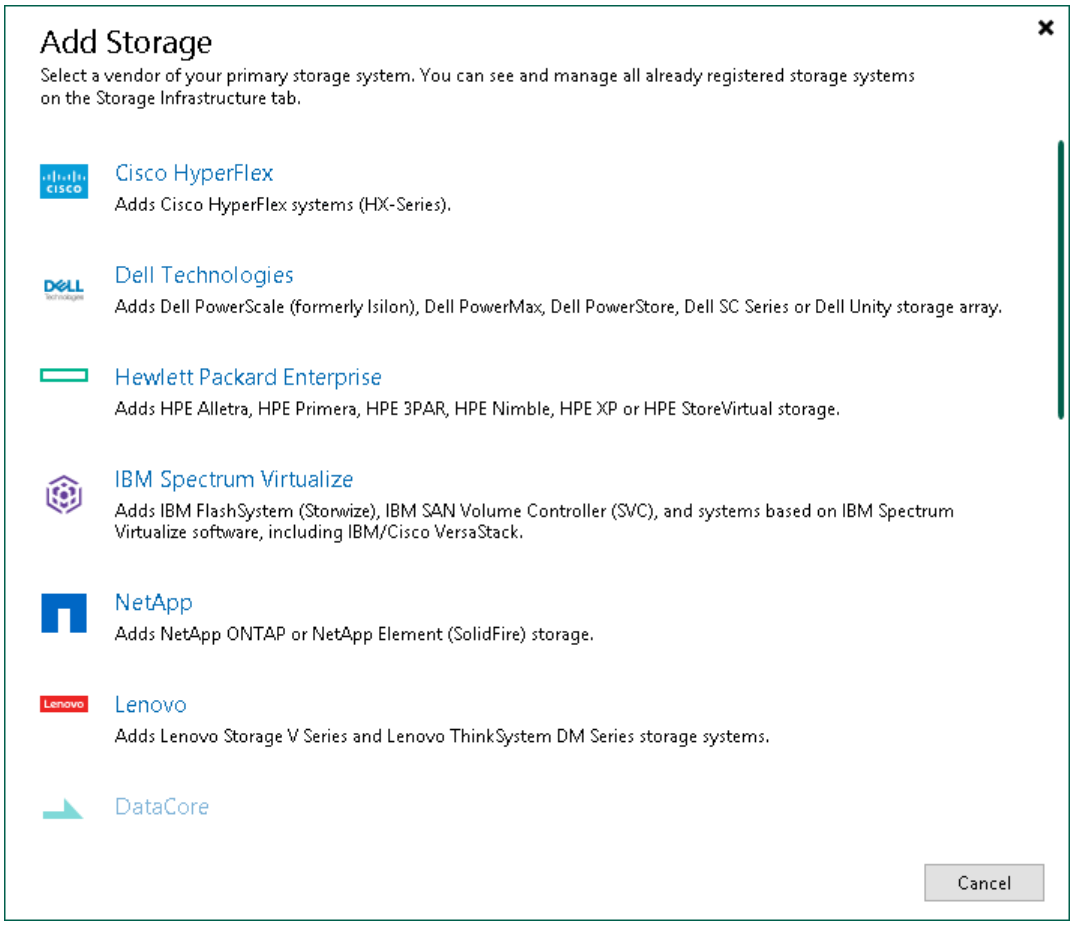
1. Launch the Add Storage wizard.
2. Select the Lenovo storage type.

Step 1. Launch Add Storage Wizard

To launch the wizard for adding a Lenovo storage system, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Lenovo**.
- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Lenovo**.
- You can use this method if at least one Lenovo storage system is added to the backup infrastructure.

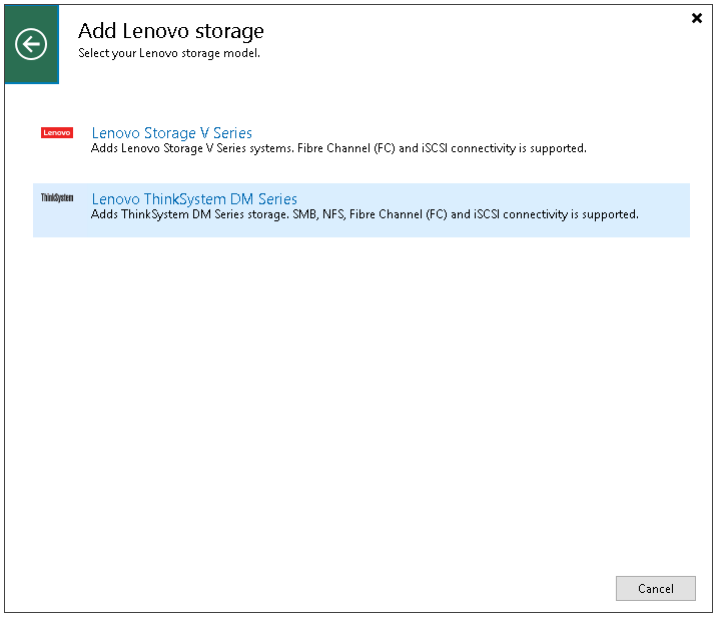
  Open the **Storage Infrastructure** view. In the inventory pane, right-click the *<Lenovo storage model name>* node and select **Add storage**. Alternatively, you can select the *<Lenovo storage model name>* node in the inventory pane, right-click anywhere in the working area and select **Add storage**.



Step 2. Add Lenovo Storage

In the **Add Lenovo storage** window, select which Lenovo storage type you want to add:

- Lenovo V Series
- Lenovo ThinkSystem DM Series



Adding Lenovo V Series

The Lenovo V Series is based on the IBM Spectrum Virtualize storage system. That is why Veeam Backup & Replication opens the IBM Spectrum Virtualize wizard. For more information on the steps of the wizard, see Adding IBM Spectrum Virtualize.

Adding Lenovo ThinkSystem DM Series

To add Lenovo ThinkSystem DM Series storage system to the backup infrastructure, do the following:

To add Lenovo ThinkSystem DM Series storage system to the backup infrastructure, do the following:

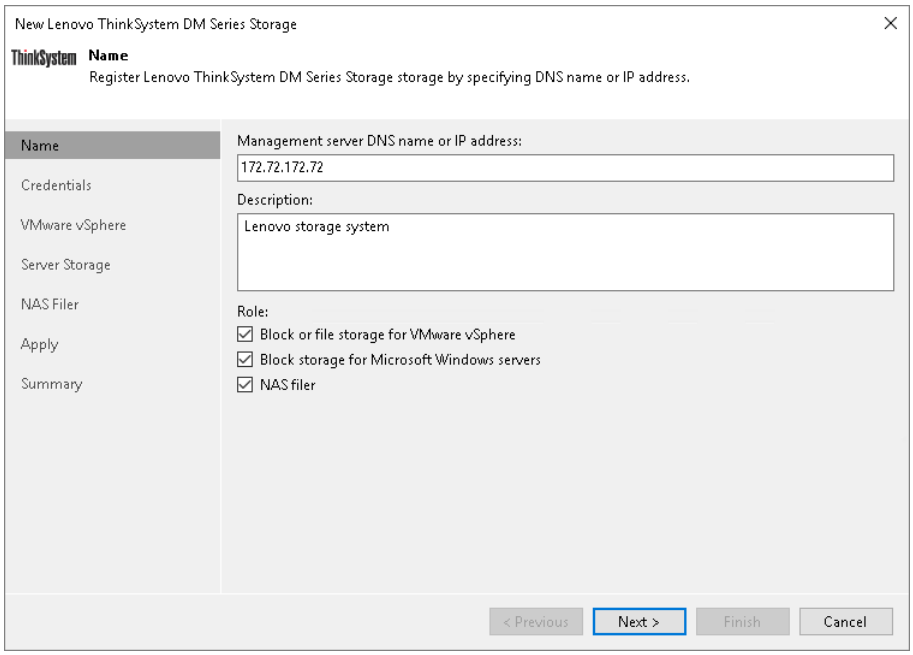
Step 1. Specify Lenovo ThinkSystem Server Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **Management server DNS name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.
   c. Select the **NAS filer** check box to allow NAS backup jobs.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



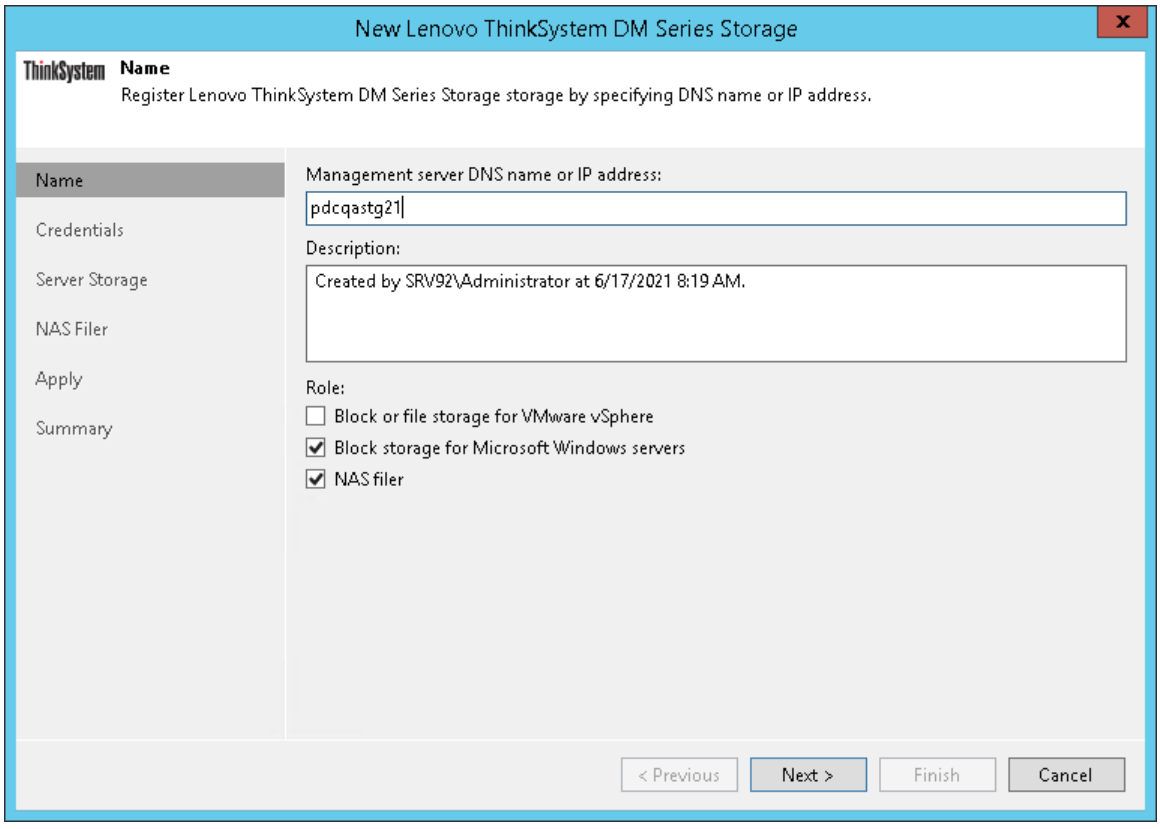
Step 1. Specify Lenovo ThinkSystem Server Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **Management server DNS name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.
   c. Select the **NAS filer** check box to allow NAS backup jobs.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 2. Specify Credentials and Protocol Type

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system, and select the communication protocol.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.
2. From the **Protocol** list, select the type of protocol over which you want to communicate with the storage system: *HTTP* or *HTTPs*. The default protocol is HTTPs.
3. The default port for communication with the storage system is 443. If necessary, you can change the port number in storage system settings and specify the new port number in the **Port** field.

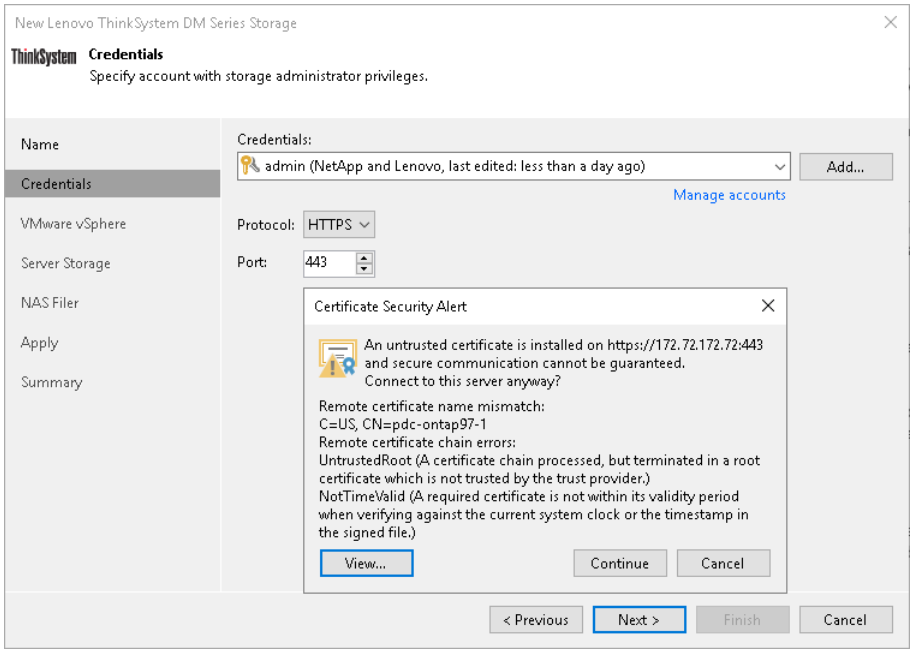
When you add a storage system, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate installed on the management server. During every subsequent connection to the server, Veeam Backup & Replication uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

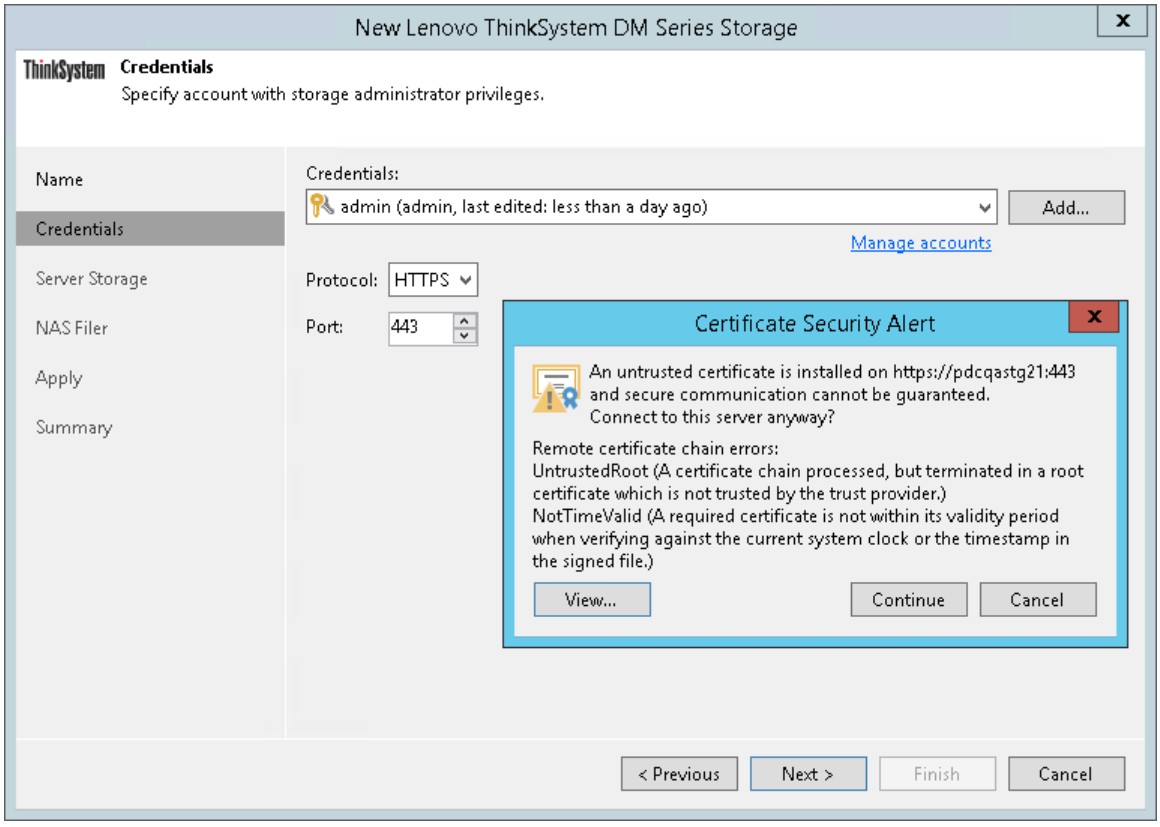
If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

- To view detailed information about the certificate, click **View**.
- If you trust the server, click **Continue**.
- If you do not trust the server, click **Cancel**.

  Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

When you update a certificate on a server, this server becomes unavailable in the Veeam Backup & Replication console. To make the server available again, acknowledge the new certificate at the **Credentials** step of the edit storage system wizard.





Step 3. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify Lenovo ThinkSystem Server Name or Address step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. [For Lenovo ThinkSystem storage system working over NFS] During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required NFS export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required export rules automatically** check box.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

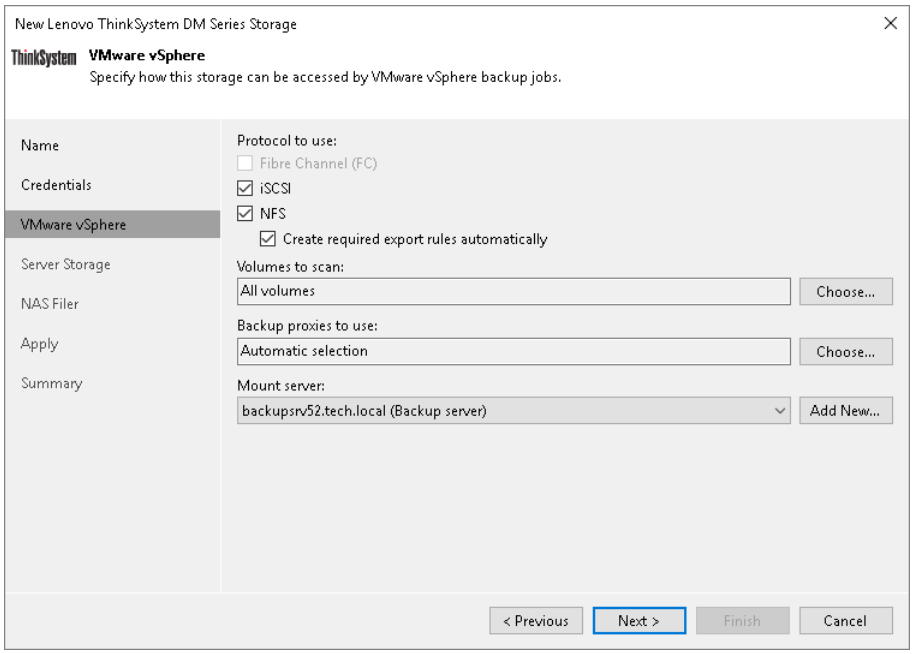
   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

4. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **IMPORTANT**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

5. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 3. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Lenovo ThinkSystem Server Name or Address step of the wizard.

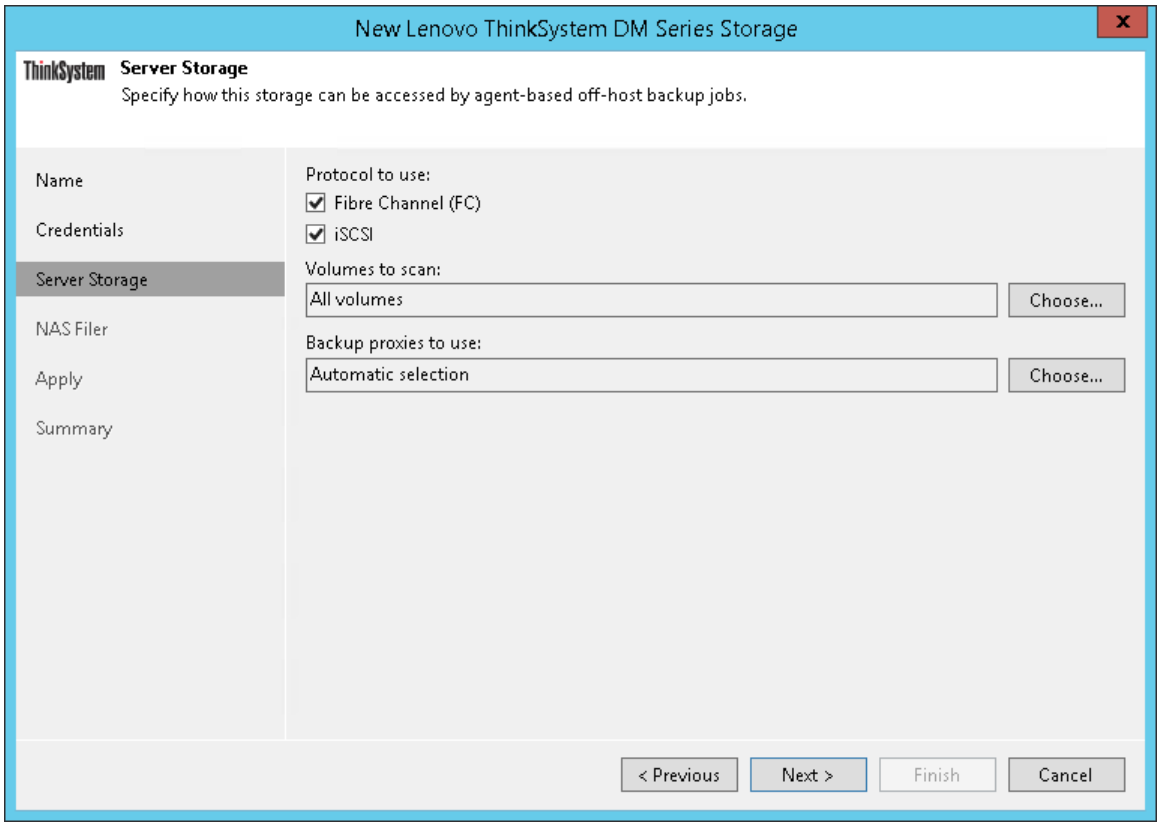
1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.



Step 4. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Lenovo ThinkSystem Server Name or Address step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

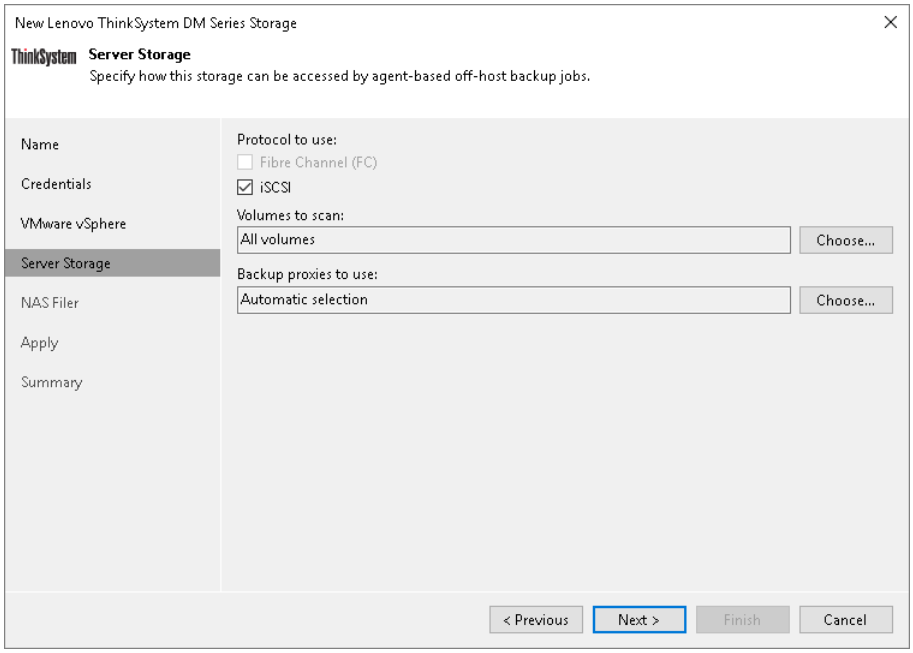
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



Step 4. Specify NAS Access Options

At the **NAS Filer** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **NAS filer** check box at the Specify Lenovo ThinkSystem Server Name or Address step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required NFS export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required export rules automatically** check box.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

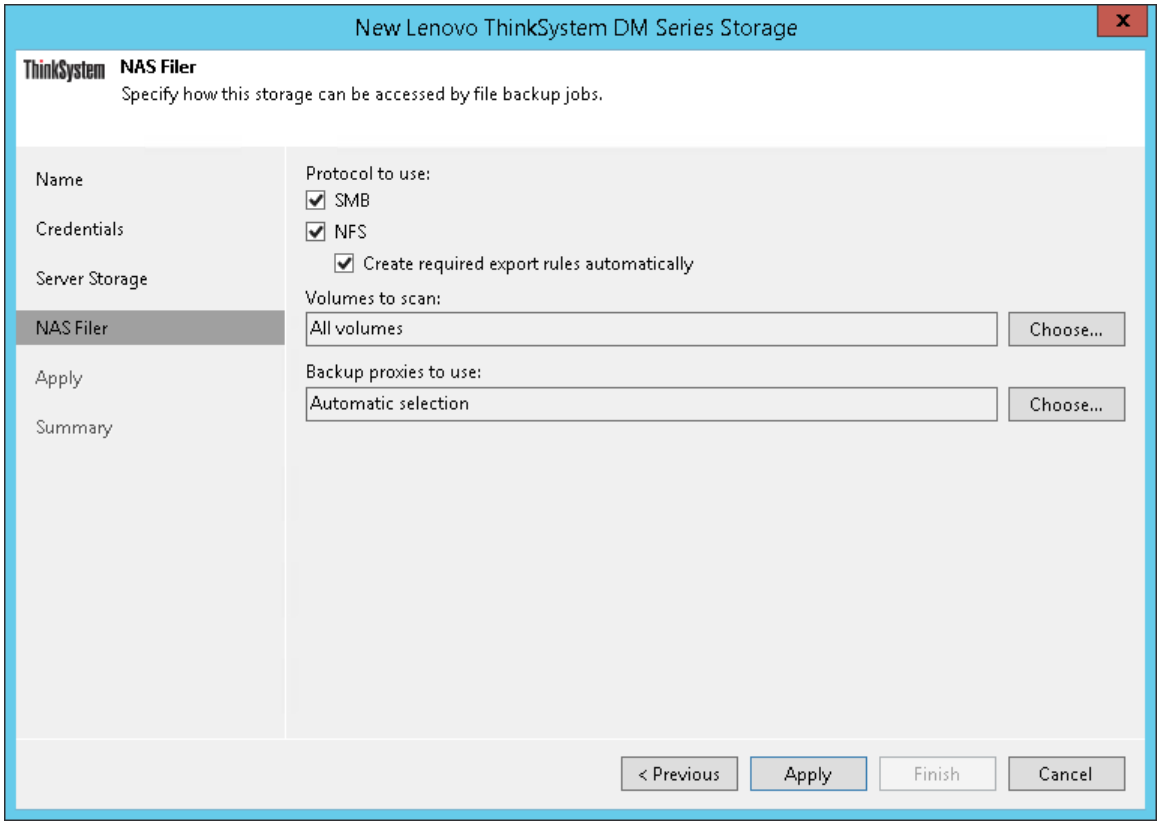
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
4. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.

IMPORTANT

In order to back up file shares residing on this storage system, do not forget to do the following:

1. Run the storage infrastructure rescan to discover file shares. You can either select this option at the last step of the wizard, as described in Finish Working with Wizard, or manually start the storage discovery, as described in Rescanning Storage Systems.
2. Add the storage system or its part as a file share to the inventory of the virtual infrastructure, as described in the Adding Enterprise Storage System as NAS Filer section of the Veeam Backup & Replication User Guide.



Step 5. Specify NAS Access Options

At the **NAS Filer** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **NAS filer** check box at the Specify Lenovo ThinkSystem Server Name or Address step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required NFS export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required export rules automatically** check box.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

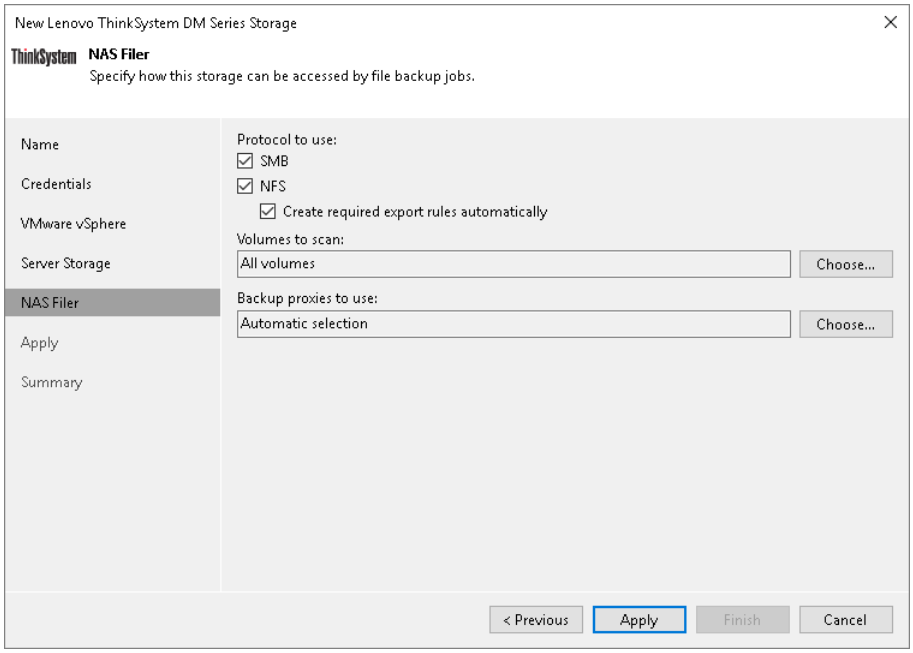
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which file share disks reside.

4. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

IMPORTANT

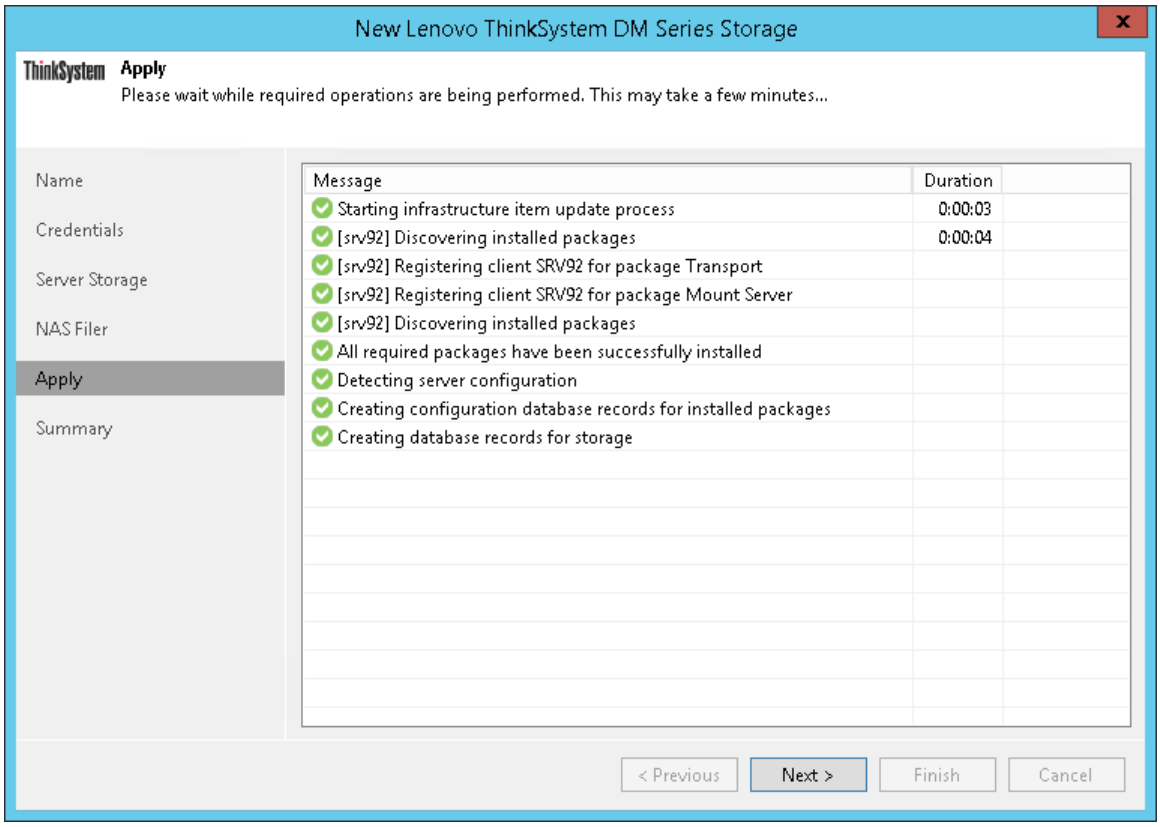
To back up file shares residing on this storage system, do not forget to do the following:

1. Run the storage infrastructure rescan to discover file shares. You can either select this option at the last step of the wizard, as described in Finish Working with Wizard, or manually start the storage discovery, as described in Rescanning Storage Systems.
2. Add the storage system or its part as a file share to the inventory of the virtual infrastructure, as described in the Adding Enterprise Storage System as NAS Filer section of the Veeam Backup & Replication User Guide.



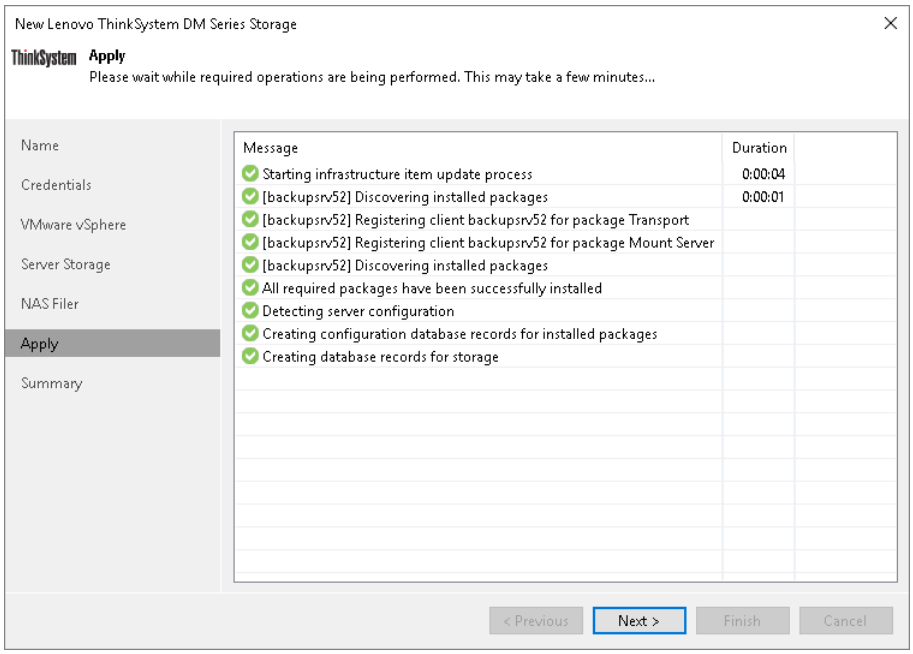
Step 5. Apply Settings

At the **Apply** step of the wizard, wait until Veeam Backup & Replication adds the storage system to the backup infrastructure. After that, click **Next**.



Step 6. Apply Settings

At the **Apply** step of the wizard, wait until Veeam Backup & Replication adds the storage system to the backup infrastructure. After that, click **Next**.

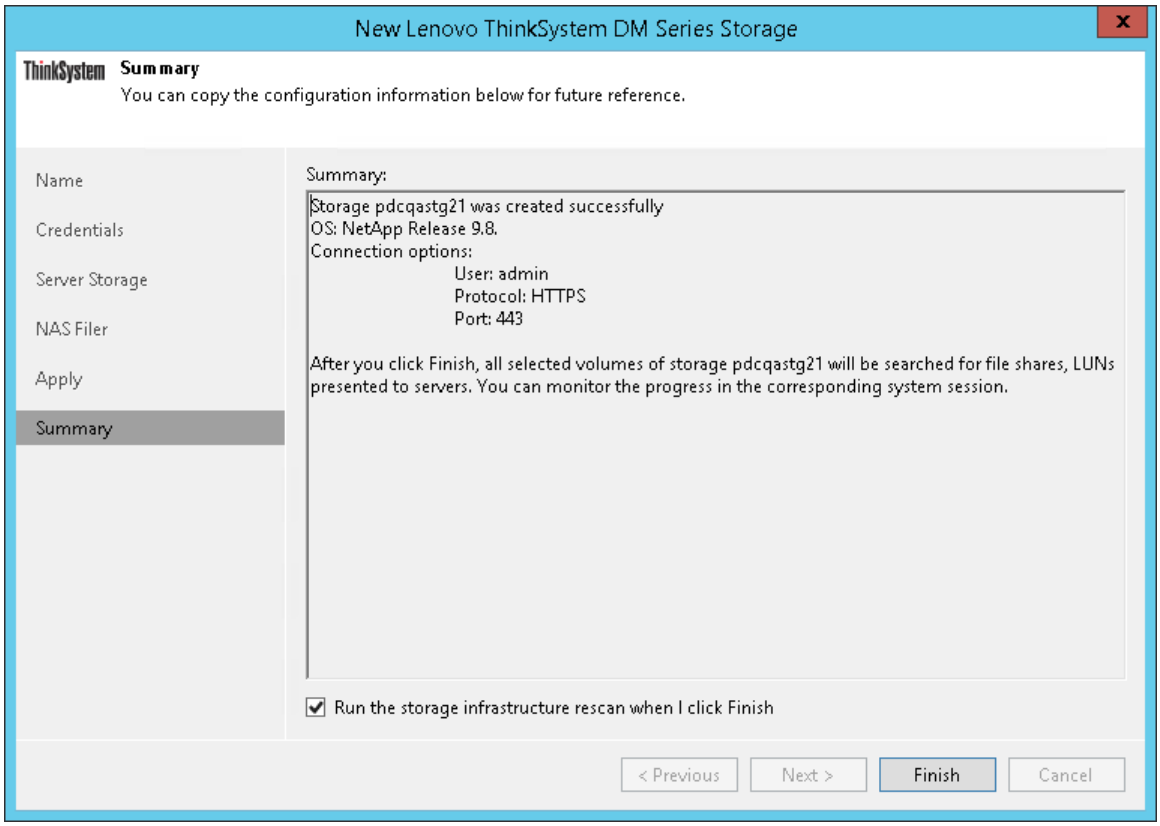


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

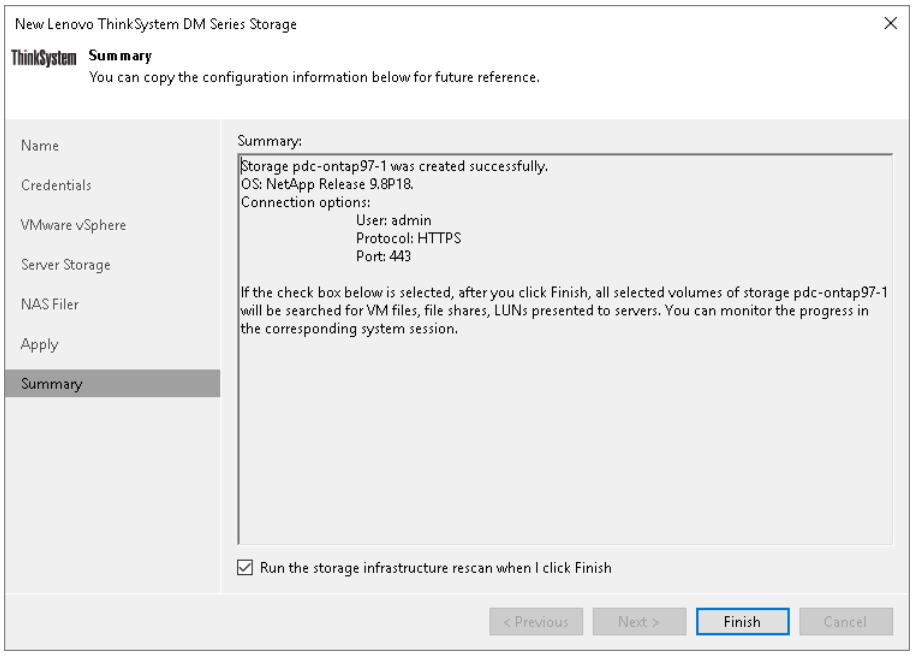


Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding NetApp Data ONTAP

Before you add to the backup infrastructure a NetApp storage system running Data ONTAP, check prerequisites. Then use the **New NetApp Data ONTAP Storage** wizard to add the storage system.

Before you add to the backup infrastructure a NetApp storage system running Data ONTAP, check prerequisites. Then use the **New NetApp Data ONTAP Storage** wizard to add the storage system.

Step 1. Launch New NetApp Data ONTAP Storage Wizard

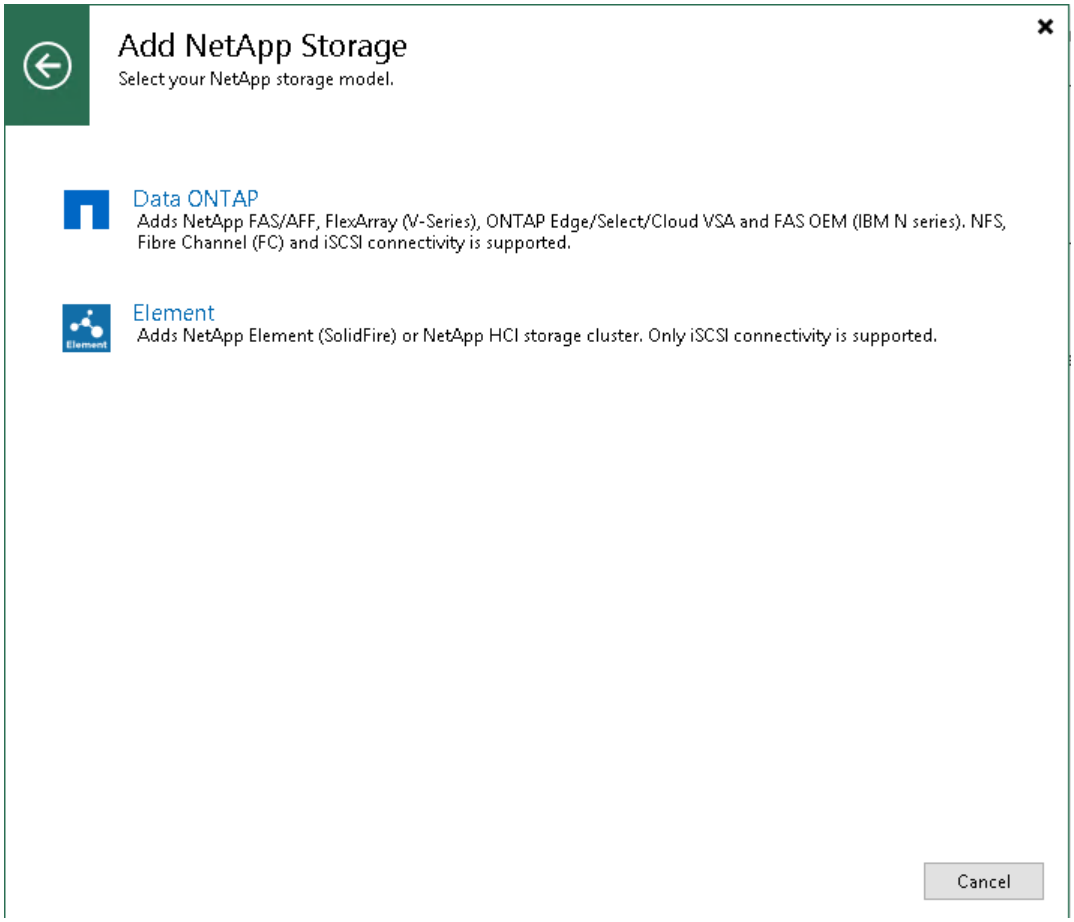
To launch the **New NetApp Data ONTAP Storage** wizard, perform the following steps.

1. Open the **Storage Infrastructure** view and do one of the following:
   - In the working area, click **Add Storage**.
   - In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**.
2. In the displayed window, select **NetApp** > **Data ONTAP**.

You can use this method to launch the wizard if at least one NetApp Data ONTAP storage system or Lenovo ThinkSystem DM Series storage system is added to the backup infrastructure:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, right-click the **ONTAP** storage system and select **Add Storage**.

   Alternatively, you can select the necessary NetApp storage system in the inventory pane, right-click anywhere in the working area and select **Add storage**.



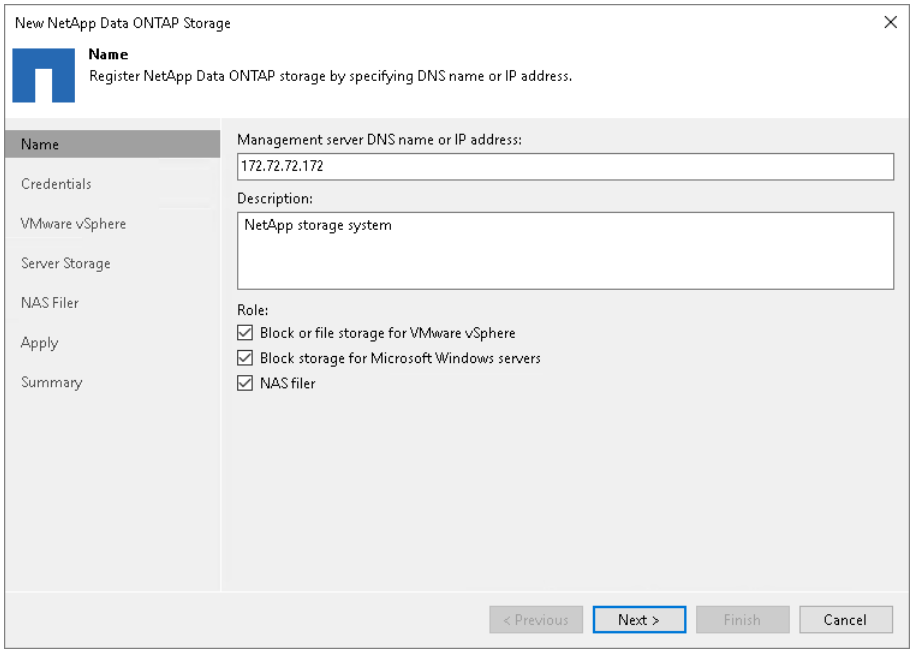
Step 2. Specify NetApp Server Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **Management server DNS name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.
   c. Select the **NAS filer** check box to allow NAS backup.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



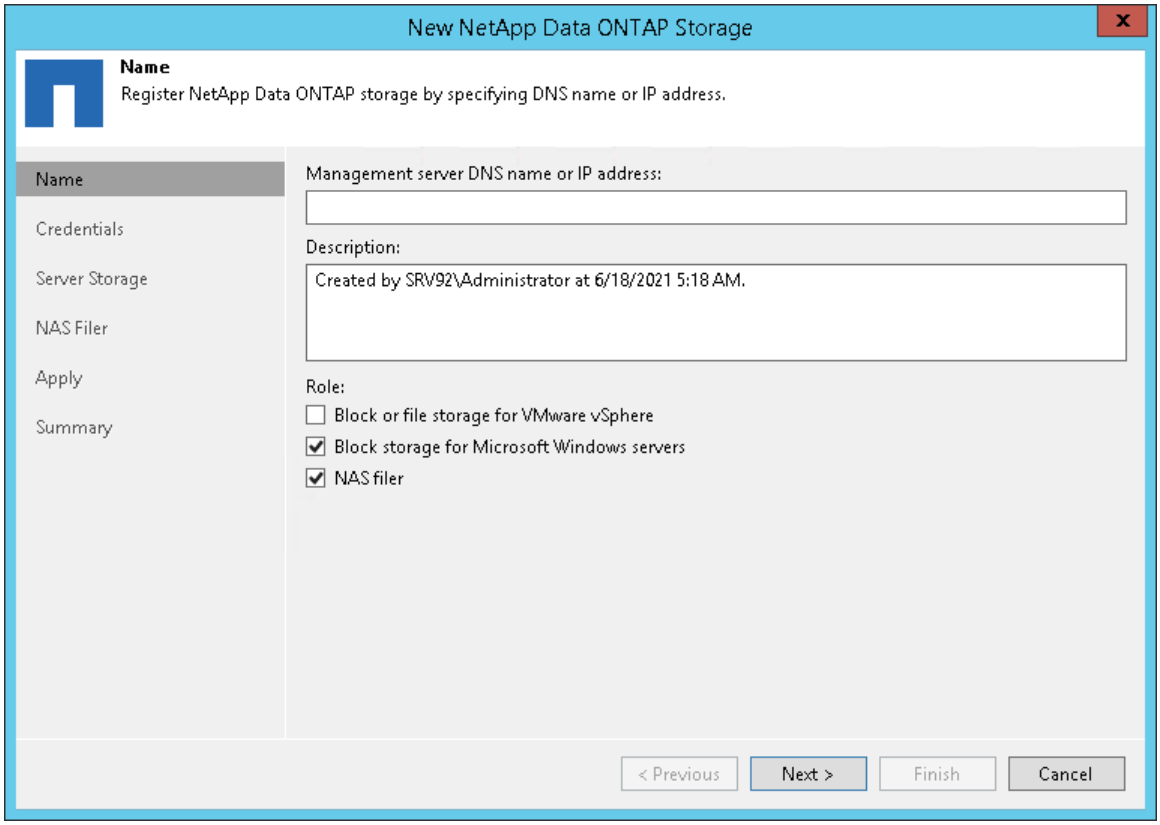
Step 2. Specify NetApp Server Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **Management server DNS name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.
   c. Select the **NAS filer** check box to allow NAS backup.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



Step 3. Specify Credentials and Protocol Type

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system, and select the communication protocol.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.
2. From the **Protocol** list, select the type of protocol over which you want to communicate with the storage system: *HTTP* or *HTTPs*.

   The default protocol is HTTPs. However, you can configure the storage system to communicate with Veeam Backup & Replication over the HTTP protocol if needed.
3. The default port for communication with the storage system is 443. If necessary, you can change the port number in storage system settings and specify the new port number in the **Port** field.

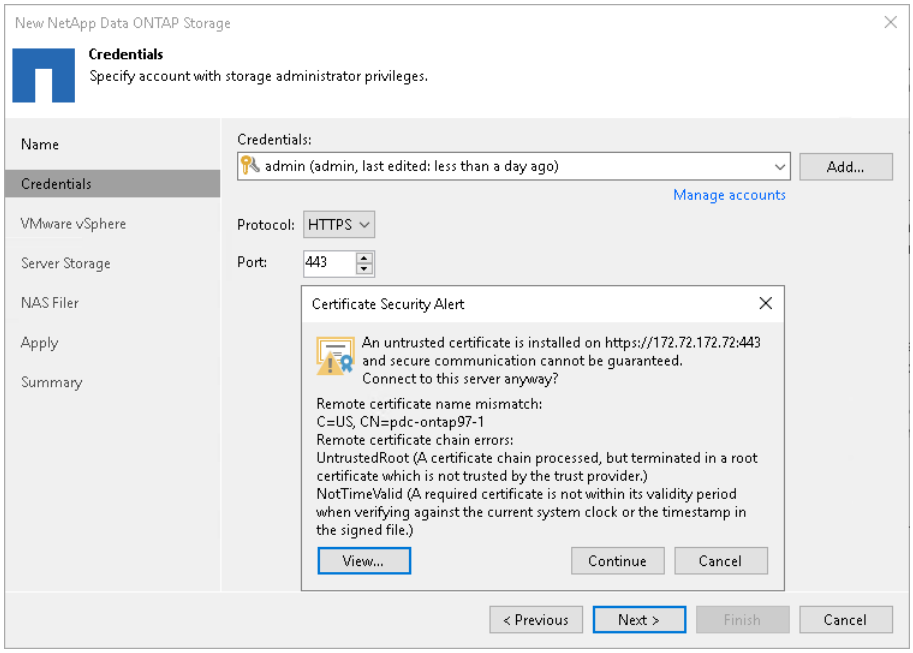
When you add a storage system, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate installed on the NetApp management server. During every subsequent connection to the server, Veeam Backup & Replication uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

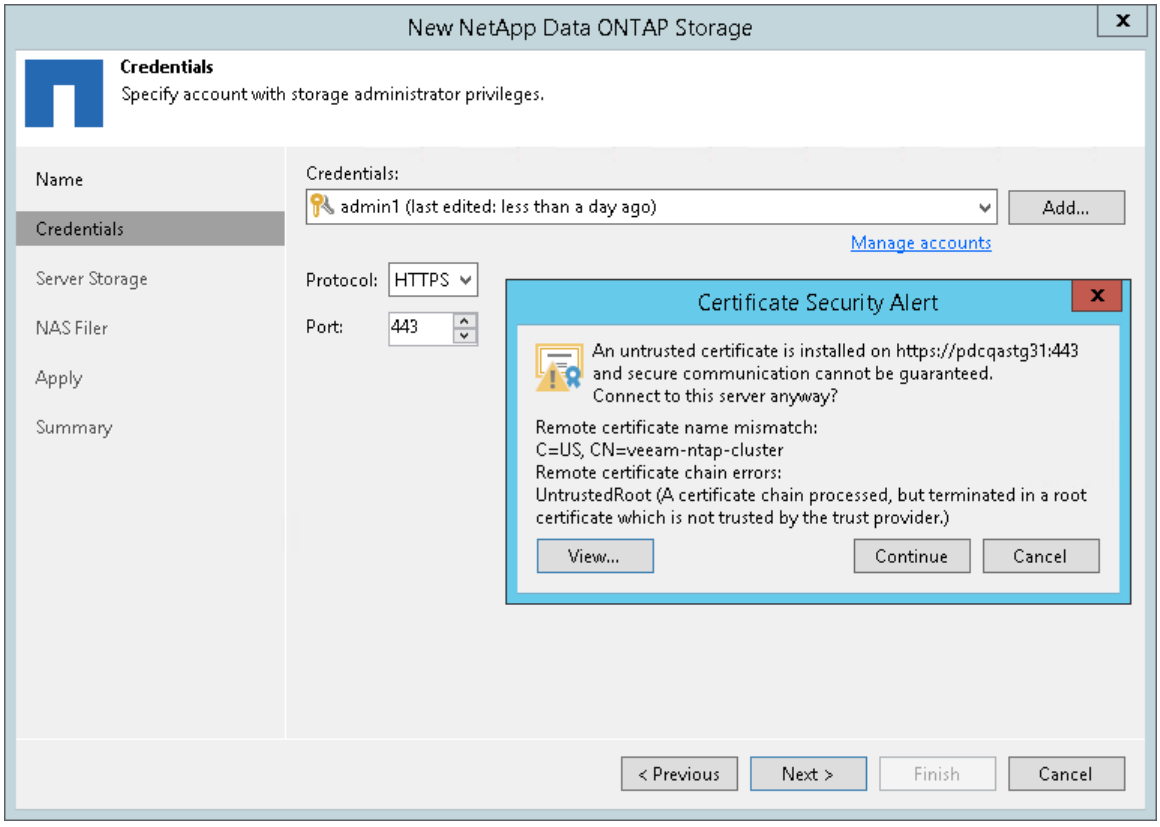
If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

- To view detailed information about the certificate, click **View**.
- If you trust the server, click **Continue**.
- If you do not trust the server, click **Cancel**.

  Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

When you update a certificate on a server, this server becomes unavailable in the Veeam Backup & Replication console. To make the server available again, acknowledge the new certificate at the **Credentials** step of the edit storage system wizard.





Step 4. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify NetApp Server Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. [For NetApp ONTAP storage system working over NFS] During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required NFS export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required NFS export rules automatically** check box.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   > **NOTE**
   >
   > If you use NetApp MetroCluster, you will not be able to select volumes from infrastructure.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

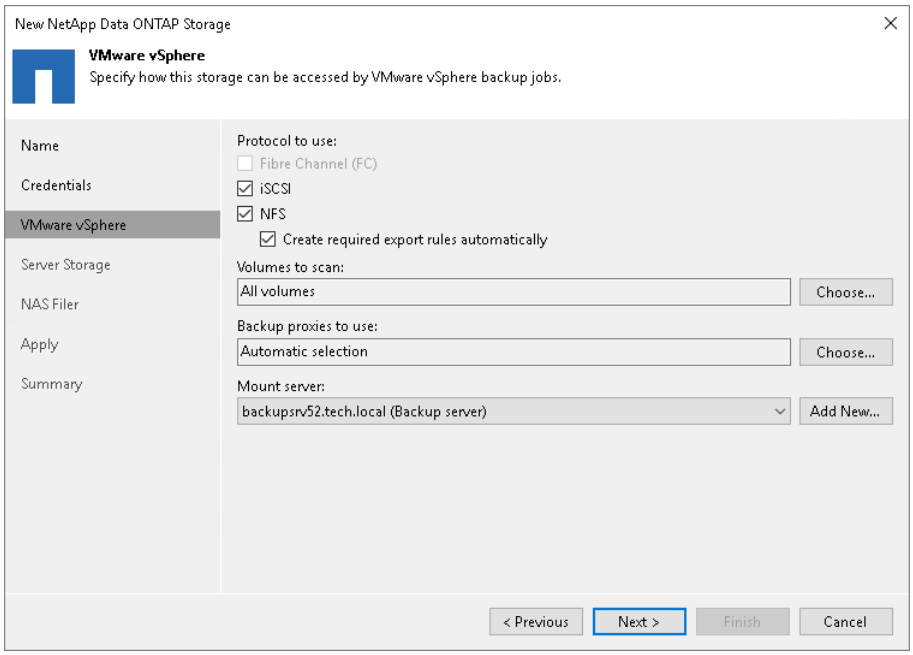
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

4. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **IMPORTANT**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

5. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 4. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify NetApp Server Name or Address and Storage Role step of the wizard.

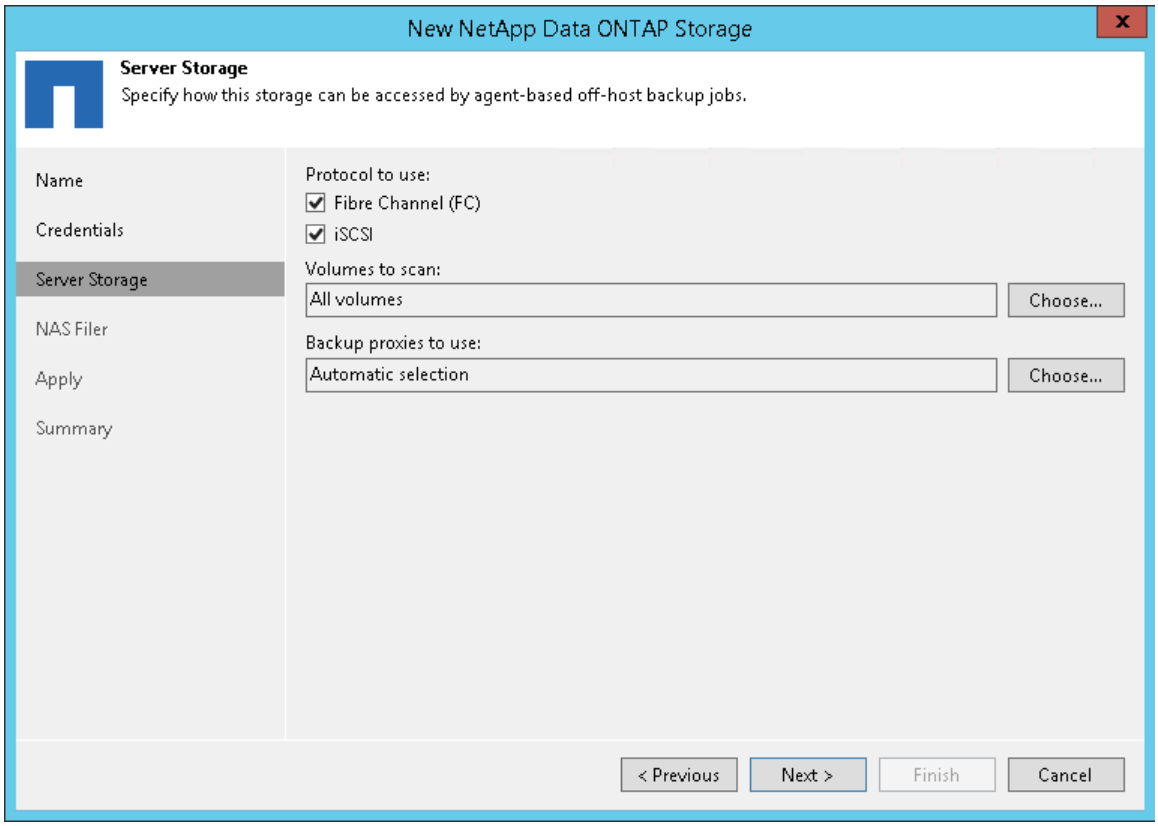
1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.



Step 5. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows** servers check box at the Specify NetApp Server Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

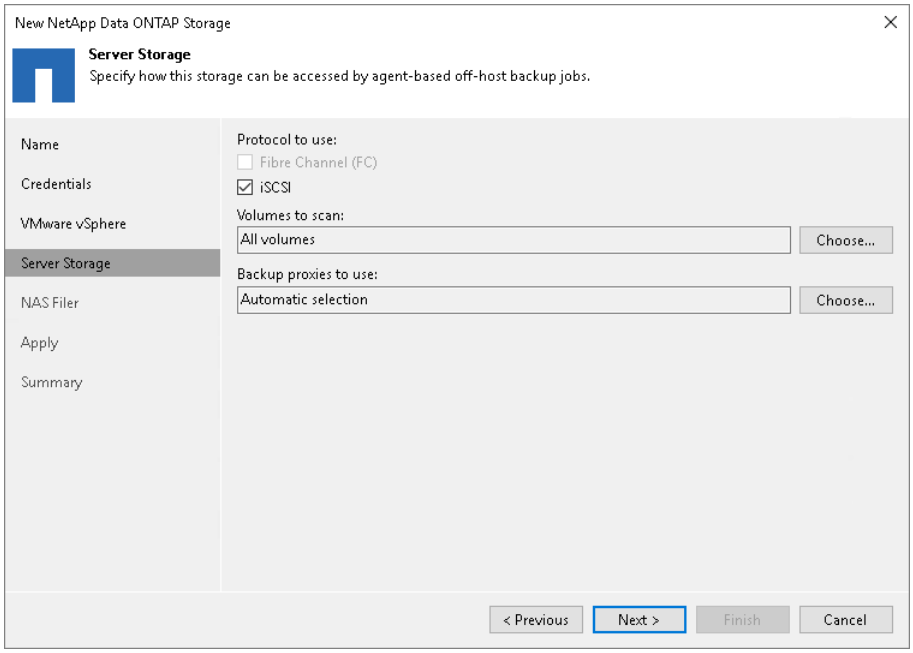
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



Step 5. Specify NAS Access Options

At the **NAS Filer** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **NAS Filer** check box at the Specify NetApp Server Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required export rules automatically** check box. This option works both for SMB and NFS protocols.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

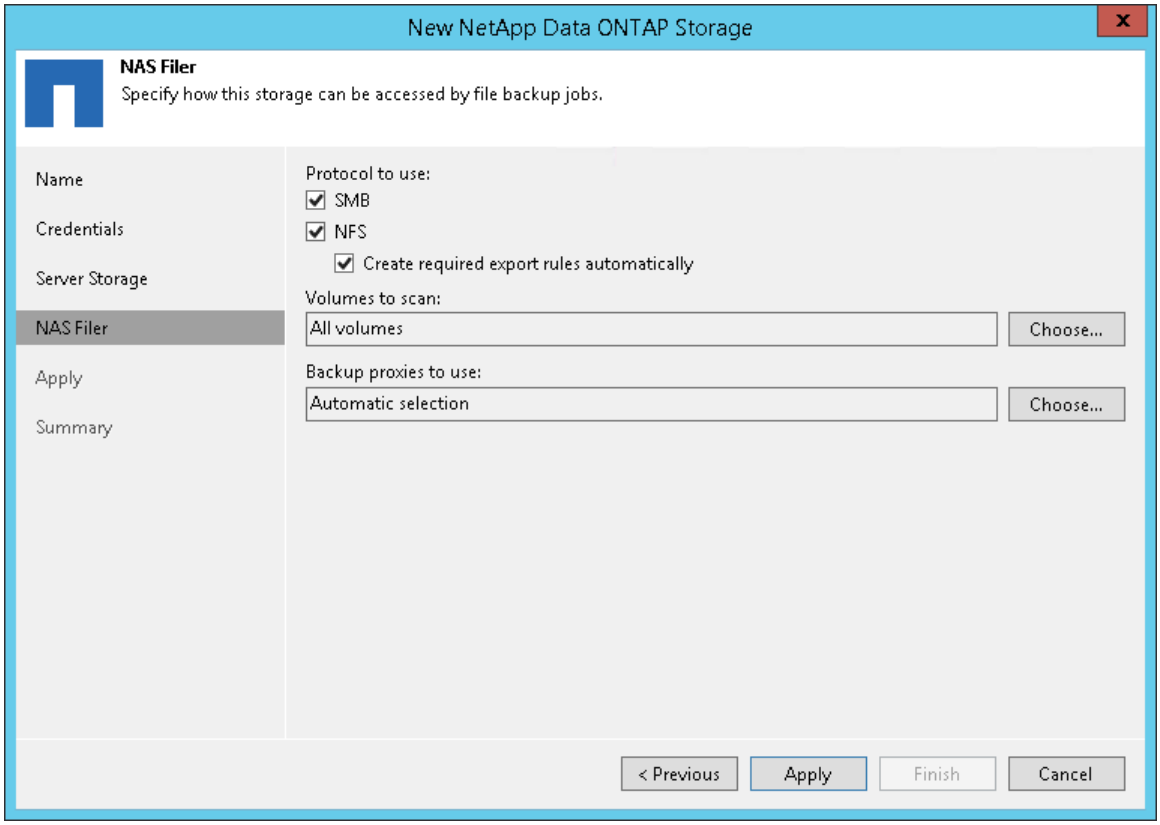
   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
4. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.

IMPORTANT

In order to back up file shares residing on this storage system, do not forget to do the following:

1. Run the storage infrastructure rescan to discover file shares. You can either select this option at the last step of the wizard, as described in Finish Working with Wizard, or manually start the storage discovery, as described in Rescanning Storage Systems.
2. Add the storage system or its part as a file share to the inventory of the virtual infrastructure, as described in the Adding Enterprise Storage System as NAS Filer section of the Veeam Backup & Replication User Guide.



Step 6. Specify NAS Access Options

At the **NAS Filer** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **NAS Filer** check box at the Specify NetApp Server Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required export rules automatically** check box. This option works both for SMB and NFS protocols.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

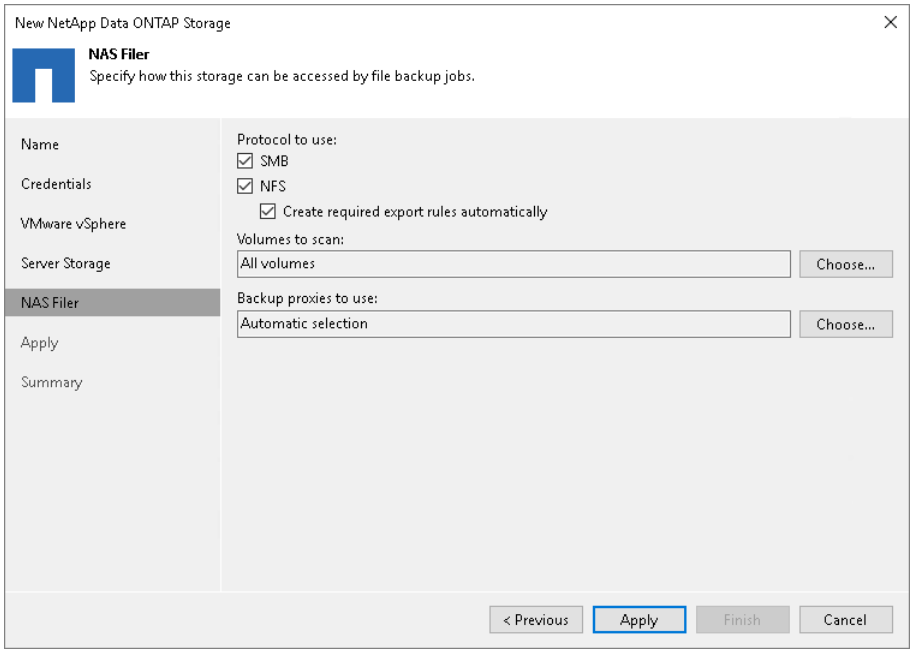
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which file share disks reside.

4. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

IMPORTANT

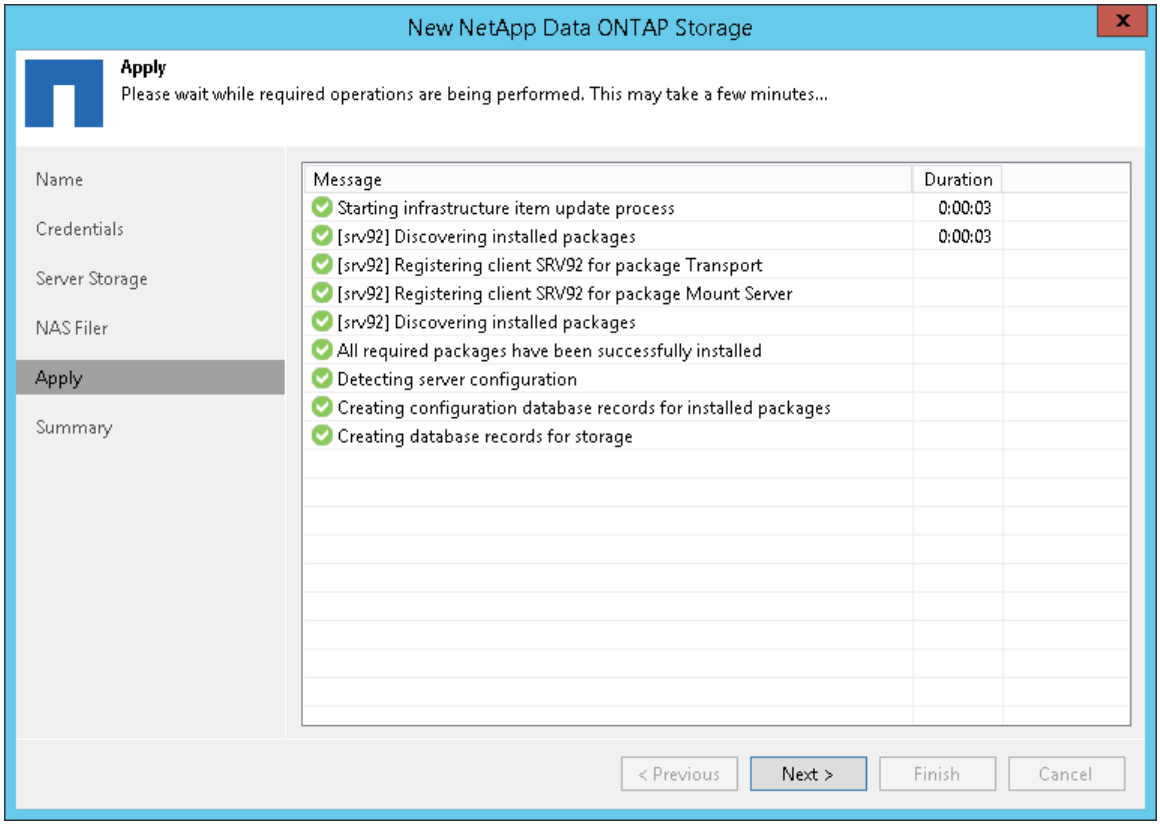
To back up file shares residing on this storage system, do not forget to do the following:

1. Run the storage infrastructure rescan to discover file shares. You can either select this option at the last step of the wizard, as described in Finish Working with Wizard, or manually start the storage discovery, as described in Rescanning Storage Systems.
2. Add the storage system or its part as a file share to the inventory of the virtual infrastructure, as described in the Adding Enterprise Storage System as NAS Filer section of the Veeam Backup & Replication User Guide.



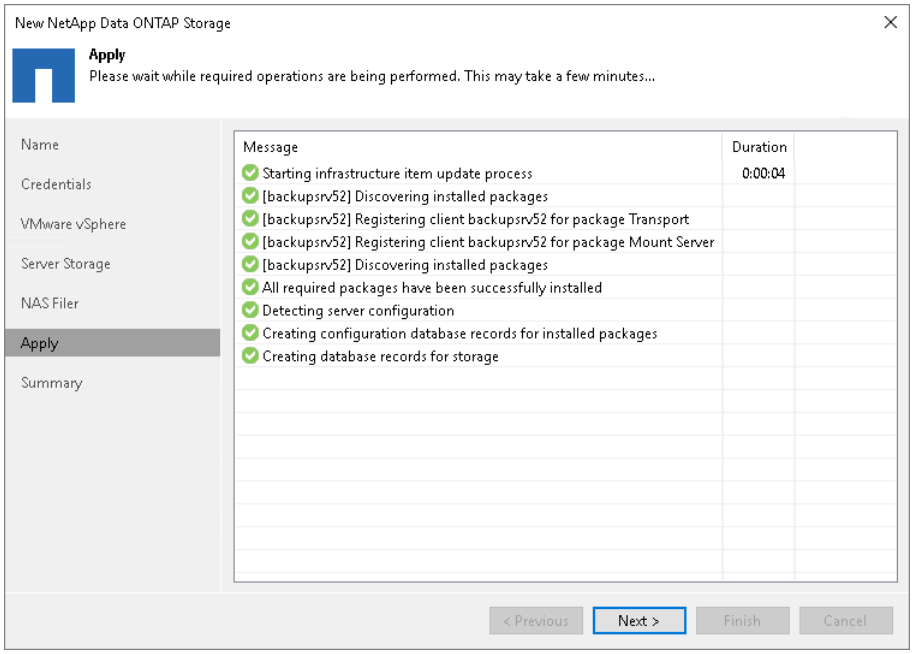
Step 6. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.



Step 7. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

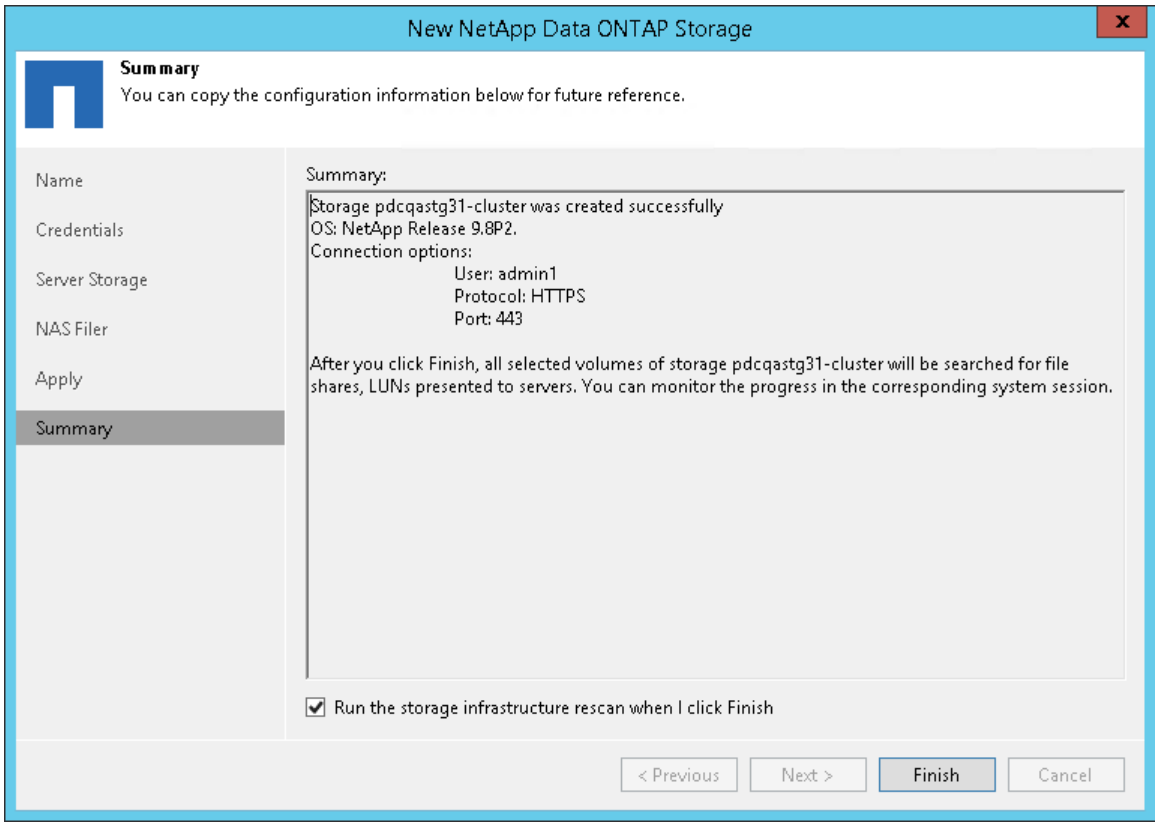


Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

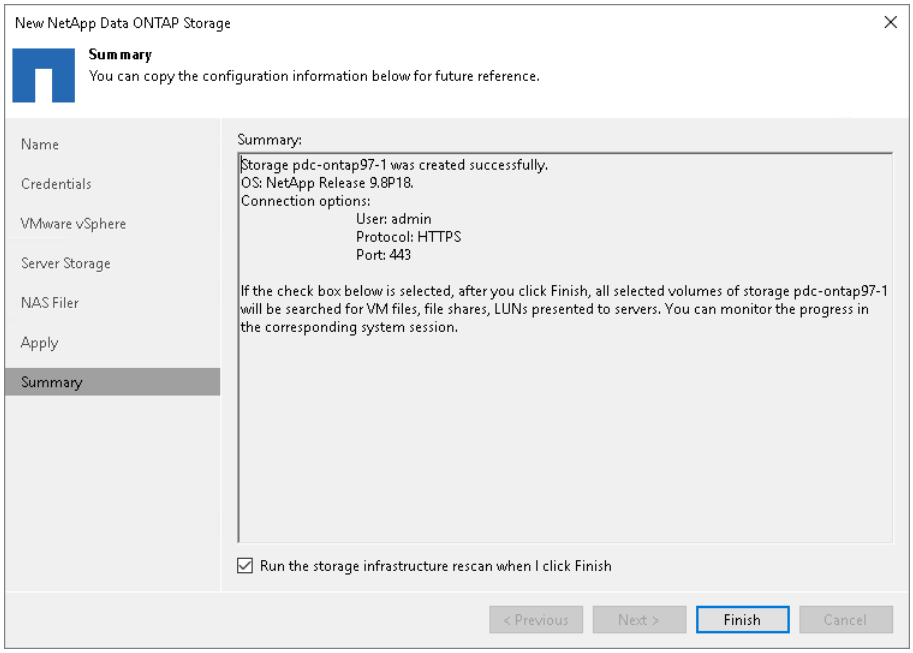


Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding Nutanix Files Storage

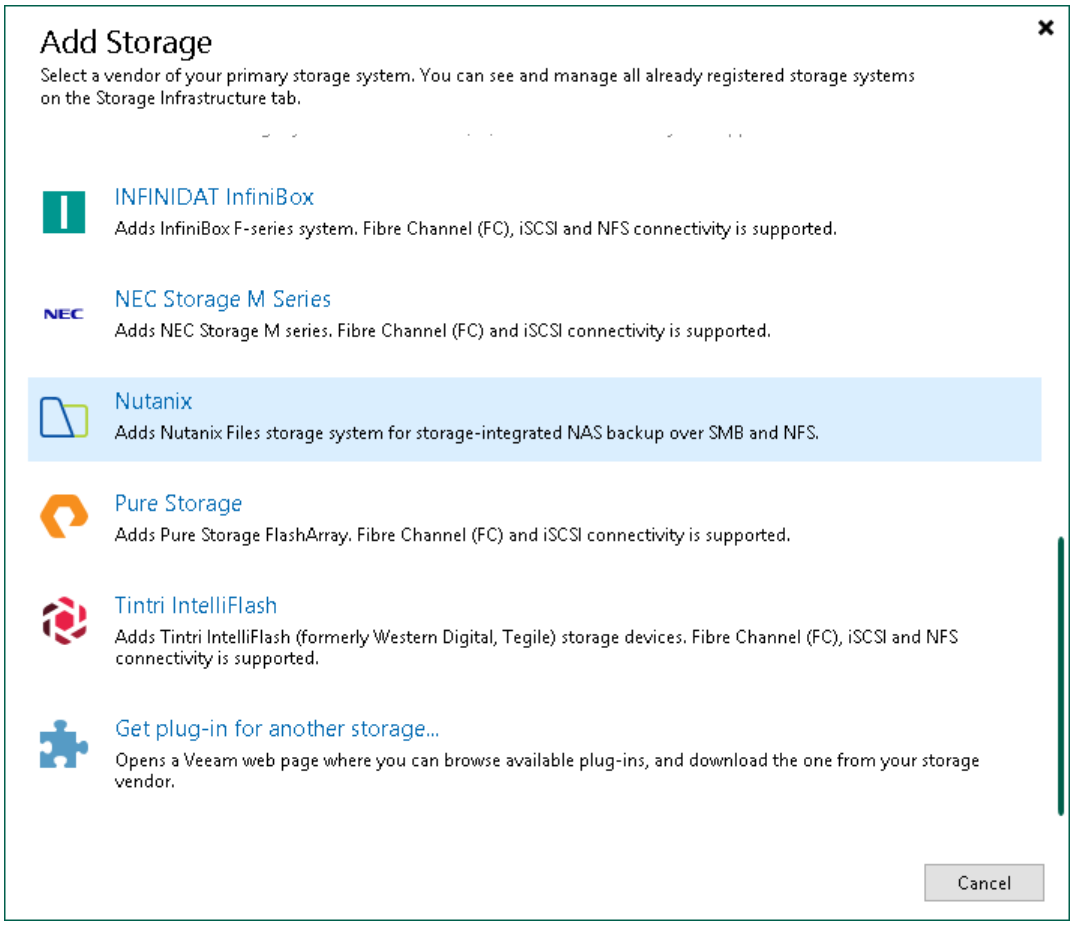
To add the storage system, use the **New Nutanix Files Storage** wizard.

Step 1. Launch New Nutanix Files Storage Wizard

To launch the **New Nutanix Files Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Nutanix**.
- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Nutanix**.
- You can use this method if at least one Nutanix Files storage system is added to the backup infrastructure.

  Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Nutanix** node and select **Add storage**. You can also select the **Nutanix** node in the inventory pane, right-click anywhere in the working area and select **Add storage**.

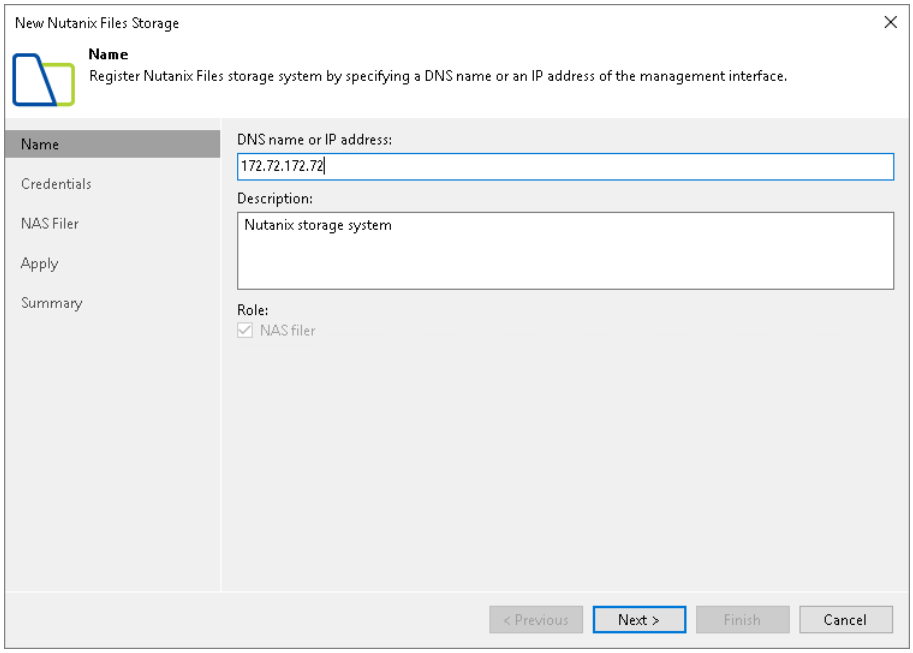


Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name and description:

1. In the **DNS name or IP address** field, specify a DNS name or client-side IPv4 address of a file server VM (FSVM).
2. In the **Description** field, provide a description for future reference.

Only NAS backup jobs are allowed to access this storage system, so the NAS filer check box is selected automatically in the **Role** section.



Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials of a Nutanix user account with administrator privileges and REST API access to the storage system. Also, specify a port through which the user will access the storage system.

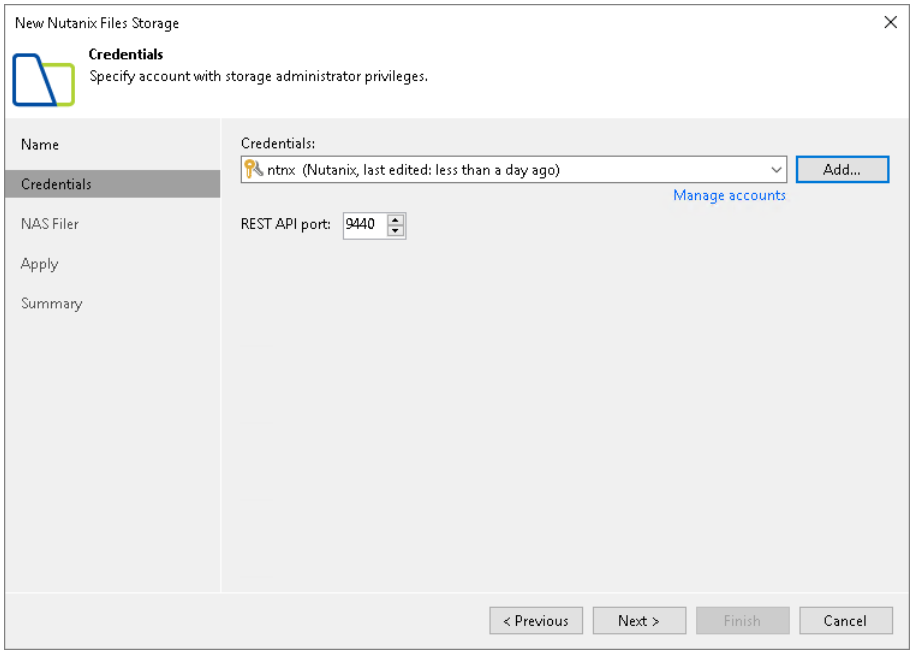
If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

After you click **Next**, Veeam Backup & Replication checks the TLS certificate installed on the storage system. If the certificate is not trusted, Veeam Backup & Replication displays a warning. In the warning window, you can do the following:

- Click **View** for the detailed information about the certificate.
- Click **Continue** to trust the certificate.
- Click **Cancel** if you do not trust the certificate. However, in this case you will not be able to connect to the storage system.

Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate. During every subsequent connection to the storage system, Veeam Backup & Replication uses the saved thumbprint to verify the storage system identity and avoid the man-in-the-middle attack. For details on managing TLS Certificates, see the Backup Server Certificate section in Veeam Backup & Replication User Guide.

When you update a certificate on the storage system, this storage system becomes unavailable in the Veeam Backup & Replication console. To make the storage system available again, acknowledge the new certificate at the **Credentials** step of the edit storage system wizard.



Step 4. Specify NAS Access Options

At the **NAS Filer** step of the wizard, specify options to access the storage system:

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. During the storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required SMB and NFS export rules in the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the **Create required export rules automatically** check box.
3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   a. To exclude specific volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

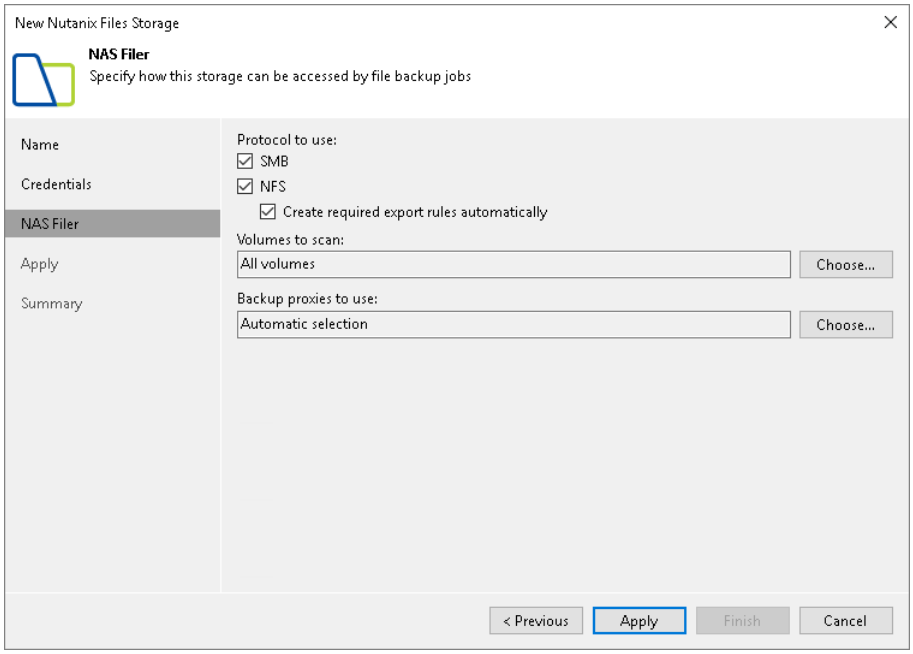
   b. To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.

   c. To rescan all volumes in the storage hierarchy, leave **All existing volumes** check box selected.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
4. To rescan storage systems and perform Backup from Storage Snapshots, you must configure backup proxies. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies:

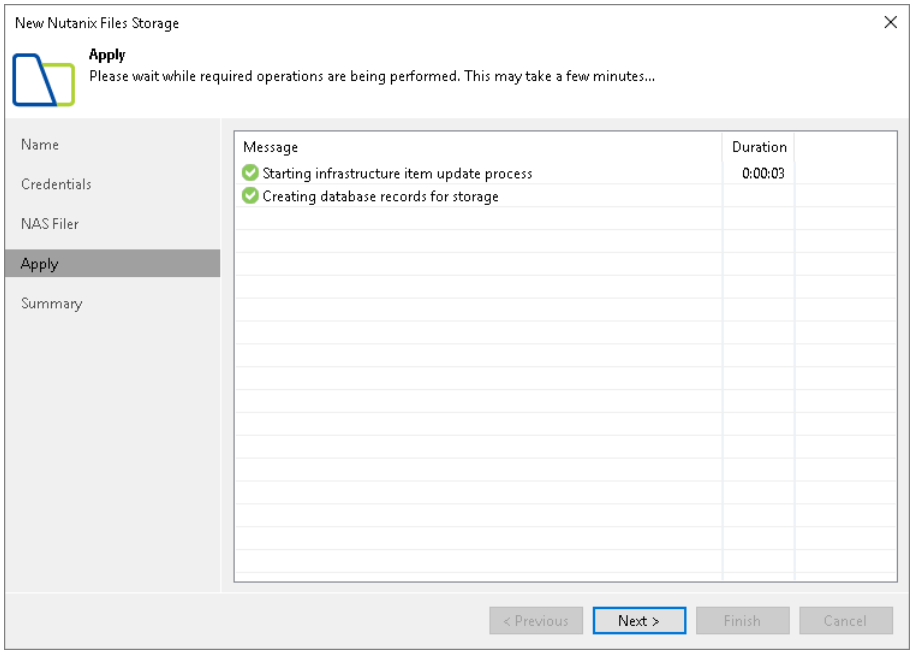
   - Select **Automatic selection** to let Veeam Backup & Replication pick backup proxies automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performedis performed if one of backup proxies fails or loses connection with the storage system.



Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

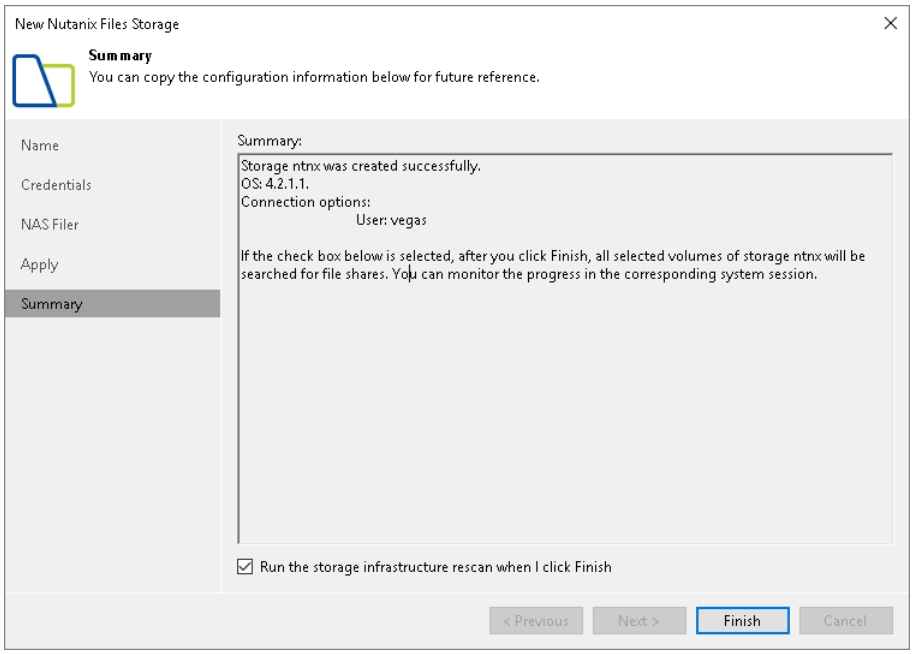


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Adding Universal Storage API Integrated Systems

Before you add a Universal Storage API integrated system to the backup infrastructure, check prerequisites. Then use the storage installation wizard.

1. Launch the storage installation wizard.
2. Specify storage name or address and storage role.
3. Specify credentials.
4. Specify VMware access options.
5. Specify Veeam Agent access options.
6. Apply settings.
7. Finish working with the wizard.

Before you add a Universal Storage API integrated system to the backup infrastructure, check prerequisites. Then use the storage installation wizard.

1. Launch the storage installation wizard.
2. Specify storage name or address and storage role.
3. Specify credentials.
4. Specify Veeam Agent access options.

5. Apply settings.
6. Finish working with the wizard.

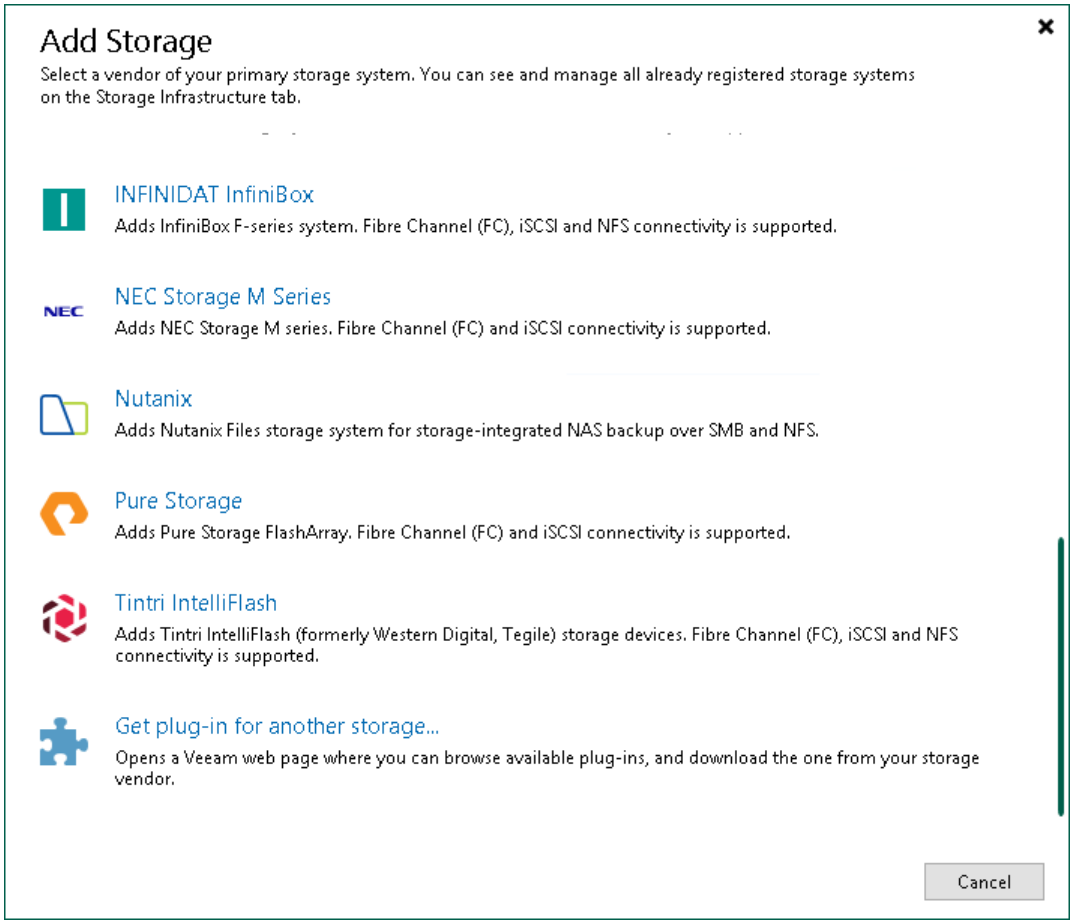
Step 1. Launch Storage Installation Wizard

To launch a storage installation wizard for Universal Storage API integrated systems, perform the following steps.

1. Open the **Storage Infrastructure** view and do one of the following:
   - In the working area, click **Add Storage**.
   - In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**.
2. In the **Add Storage** window, select the storage system that you want to add.

   To launch the installation wizard for:
   - NetApp SolidFire storage systems, in the displayed window select **NetApp** > **Element**.
   - DELL SC Series storage systems, in the displayed window select **Dell Technologies** > **Dell SC Series**.
   - Dell PowerMax storage systems, in the displayed window select **Dell Technologies** > **Dell PowerMax**.
   - Dell PowerStore storage systems, in the displayed window select **Dell Technologies** > **Dell PowerStore**.
   - HPE XP storage systems, in the displayed window select **Hewlett Packard Enterprise** > **HPE XP**.

   If a storage system that you want to add is not shown in the list, click **Get plug-in for another storage**.



Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **DNS Name or IP address** field, specify a DNS name or IP address of the storage system.

   For some storage systems, you can specify IPv6 addresses. For the list of supported systems, see General Requirements and Limitations. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.

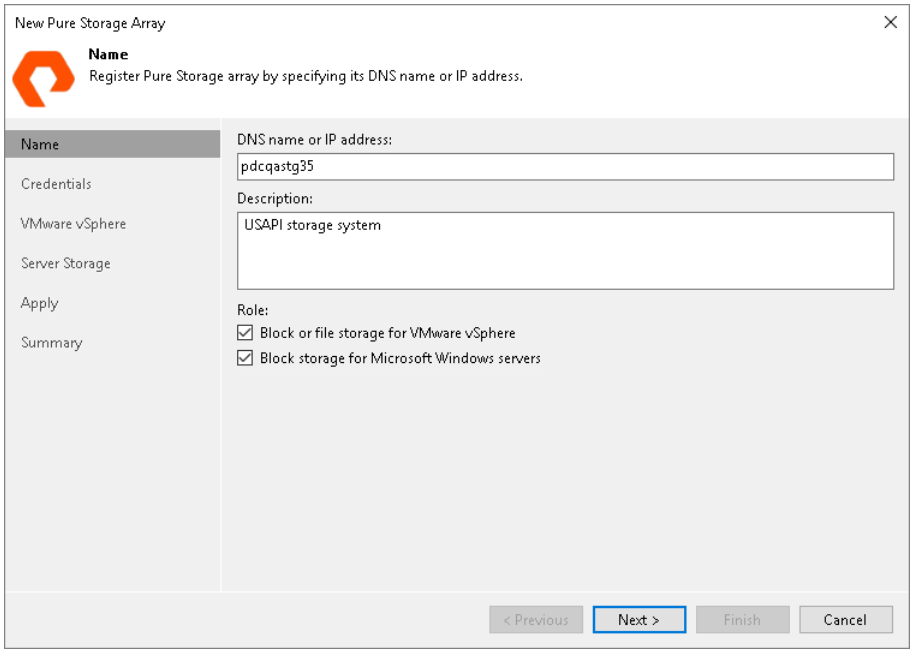
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:

   a. Select the **Block or file storage for VMware vSphere** check box to allow VMware backup.

   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



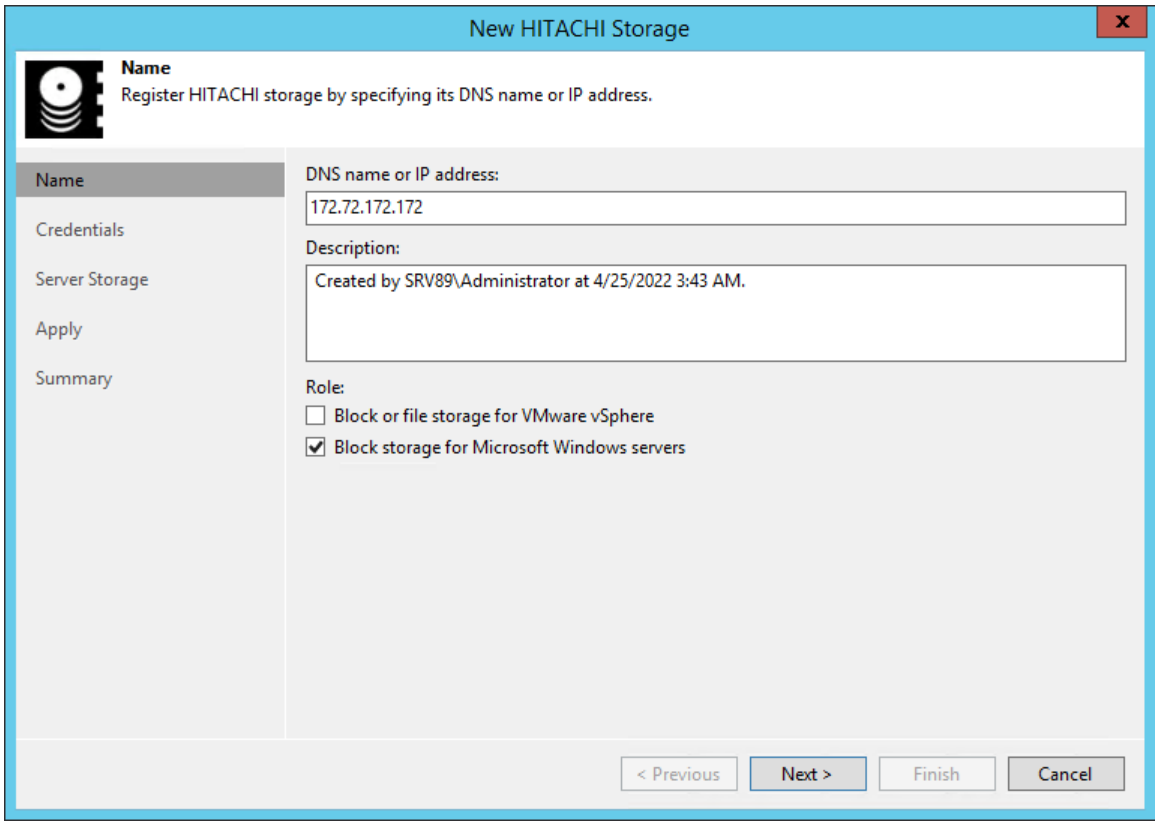
Step 2. Specify Storage Name or Address and Storage Role

At the **Name** step of the wizard, specify the storage system name, description and storage role.

1. In the **DNS Name or IP address** field, specify a DNS name, or IPv4 or IPv6 address of the storage system. Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.
3. In the **Role** section, select the types of backup jobs that are allowed to access this storage system:
   a. The **Block or file storage for VMware vSphere** option is not available for Microsoft Hyper-V integration.
   b. Select the **Block storage for Microsoft Windows servers** check box to allow backup of Veeam Agents.

   When you select any of these check boxes, additional steps of the wizard will appear.

   If you do not select any check box, Veeam Backup & Replication displays an error. To proceed with the wizard, select at least one check box.



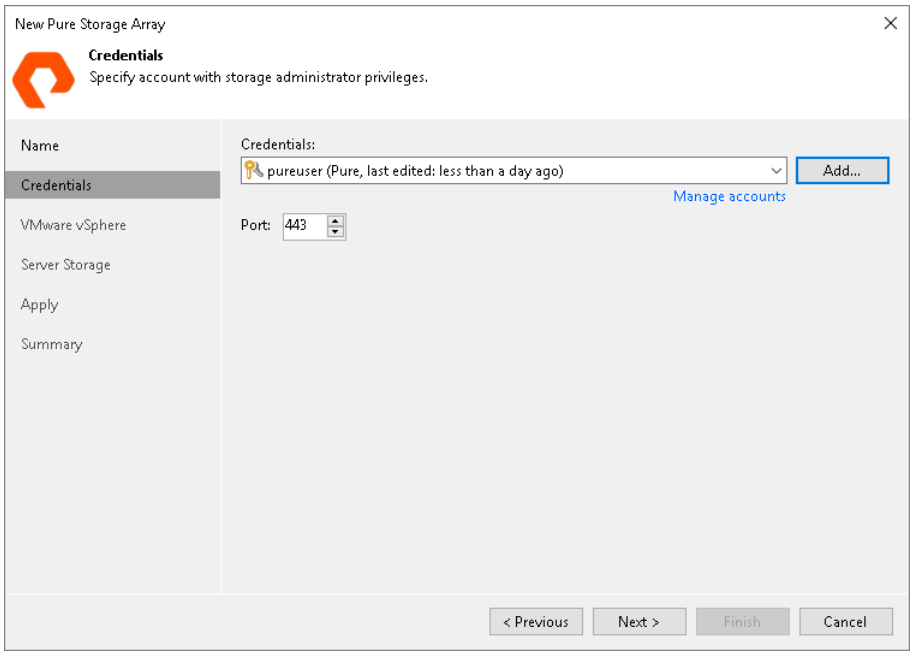
Step 3. Specify Credentials

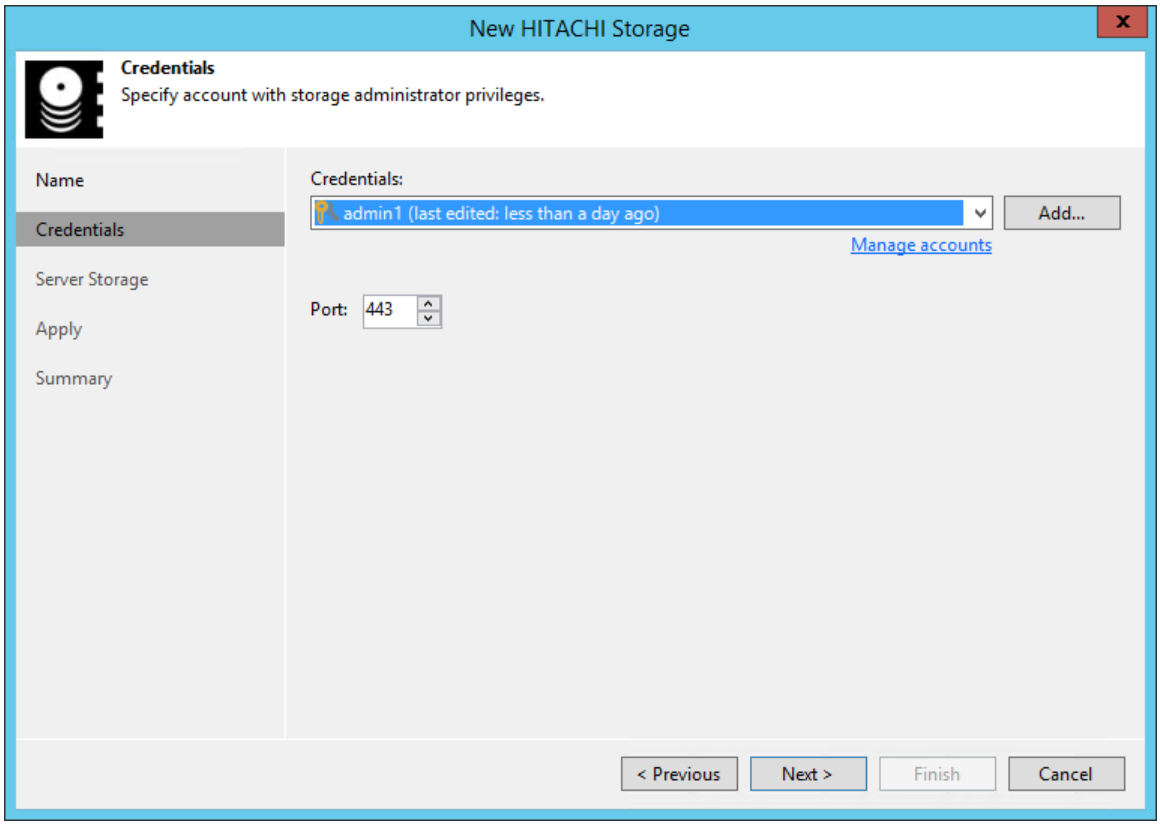
At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see the Credentials Manager section in Veeam Backup & Replication User Guide.

   > **NOTE**
   >
   > User name and password values are case-sensitive.

2. In the **Port** field, specify a number of the port that you plan to use to connect to a server.





Step 4. Specify VMware Access Options

At the **VMware vSphere** step of the wizard, specify options for accessing the storage system. You will see this step if you have selected the **Block or file storage for VMware vSphere** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

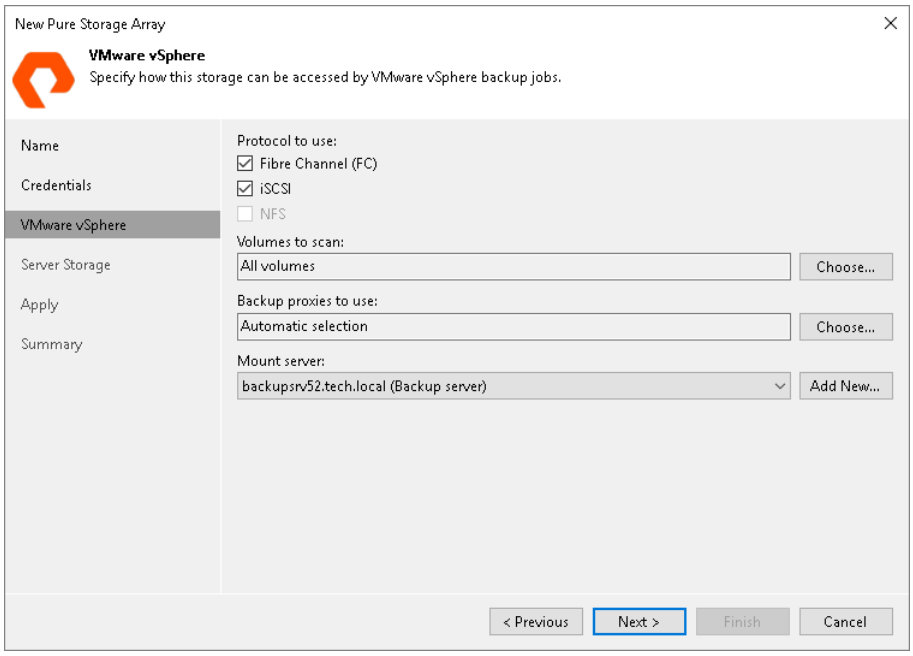
   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

   > **IMPORTANT**
   >
   > If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.

4. From the **Mount Server** list, select a server that you want to use as a mount server for file-level and application items restore, or click **Add New** to add a new one. For more information, see Mount Server section in Veeam Backup & Replication User Guide.



Step 4. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

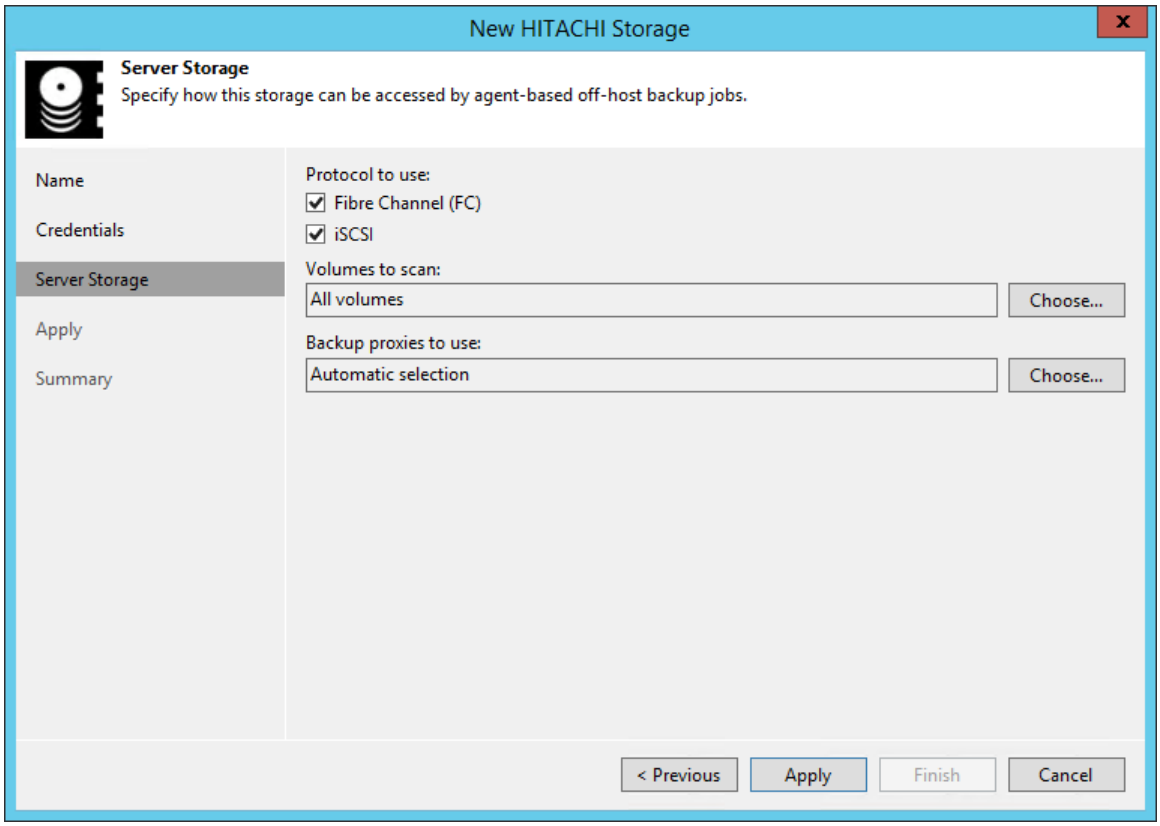
1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
3. To rescan storage systems, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan. It is recommended that you select at least two backup proxies to ensure that rescan is performed if one of backup proxies fails or loses its connectivity to the storage system.



Step 5. Specify Veeam Agent Access Options

At the **Server Storage** step of the wizard, specify options for accessing the storage system. You will see this step if you selected the **Block storage for Microsoft Windows servers** check box at the Specify Storage Name or Address and Storage Role step of the wizard.

1. In the **Protocol to use** section, select check boxes next to protocols over which you want to work with the storage system.
2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes to rescan, click **Choose** to the right of the **Volumes to scan** field. In the **Edit Volumes** window, select volumes you want to rescan:

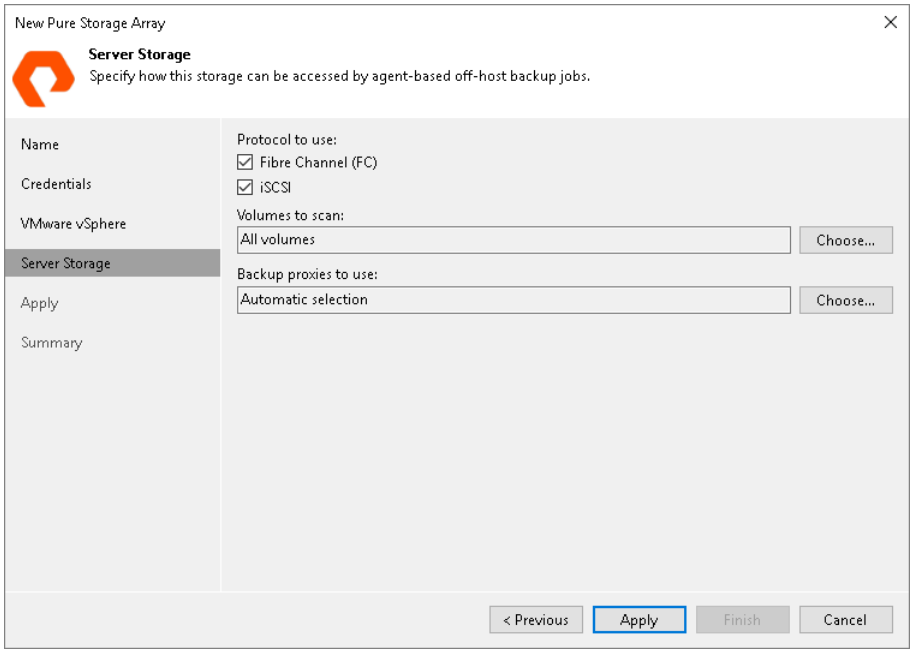
   - To exclude volumes from rescan, select **All volumes except** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - To rescan only specific volumes, select **Only the following volumes** and click **Add**. Click **From infrastructure** to select volumes from your storage infrastructure, or **By wildcard** to select volumes using a wildcard character.
   - If you leave **All existing volumes** check box selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

   After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

   > **IMPORTANT**
   >
   > If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope the volumes on which the protected machine disks reside.

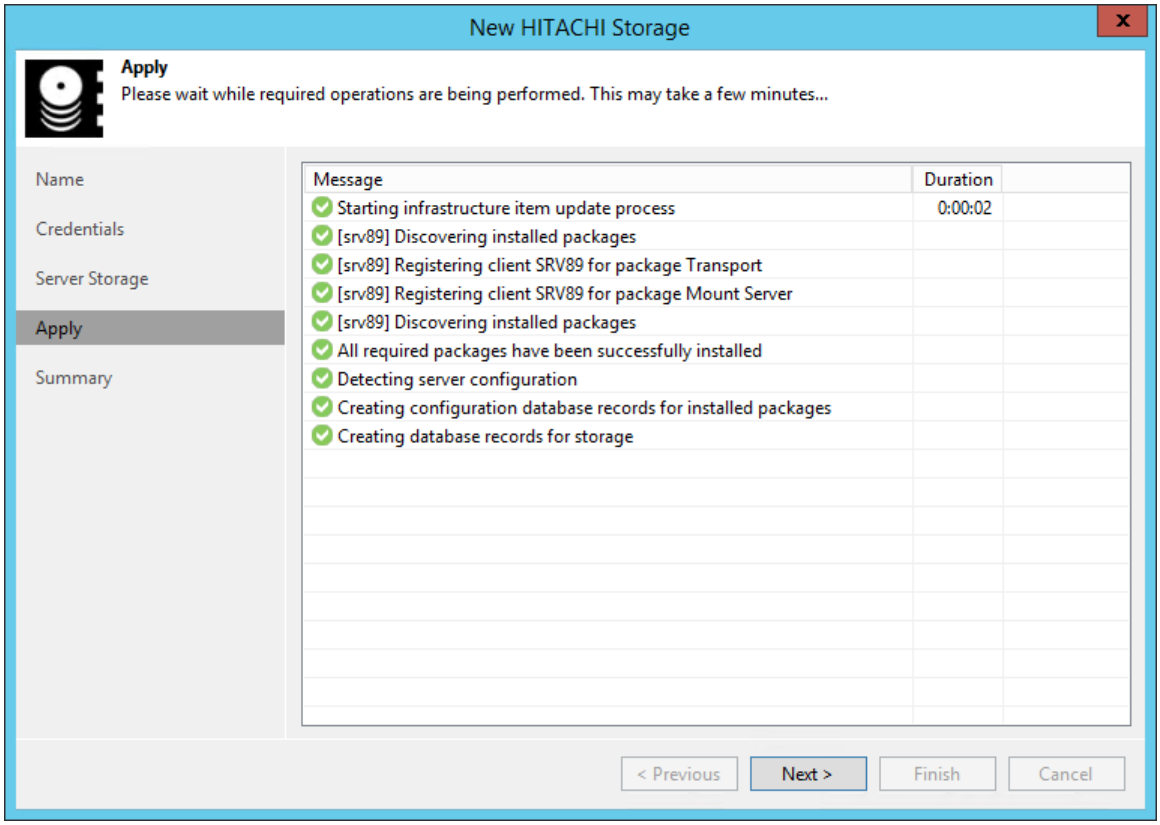
3. To rescan storage systems and perform Backup from Storage Snapshots, you need to configure a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.
   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

> **NOTE**
>
> If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail.



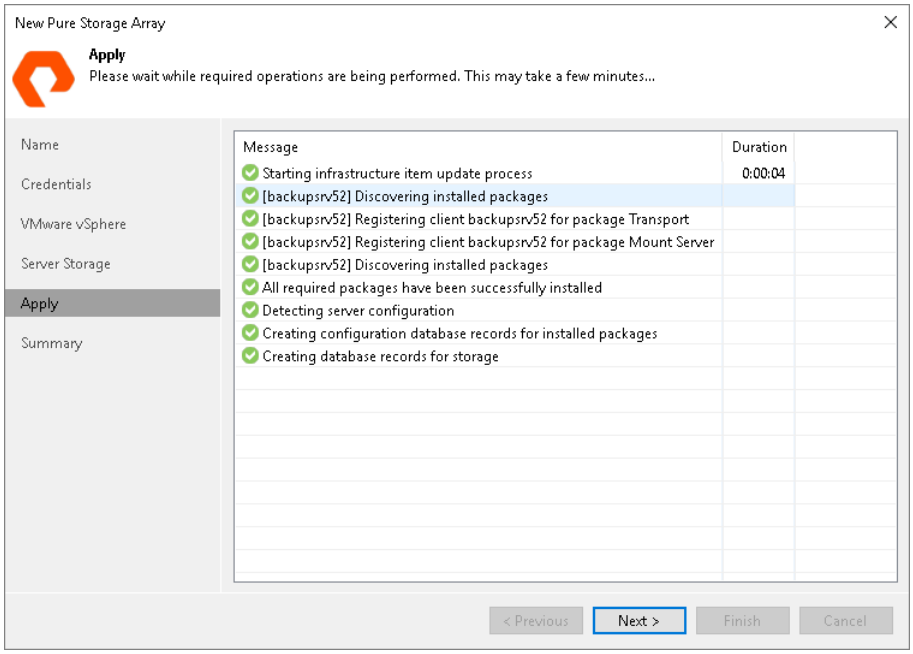
Step 5. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.



Step 6. Apply Settings

At the **Apply** step of the wizard, wait for the storage system to be added to the backup infrastructure. After that, click **Next**.

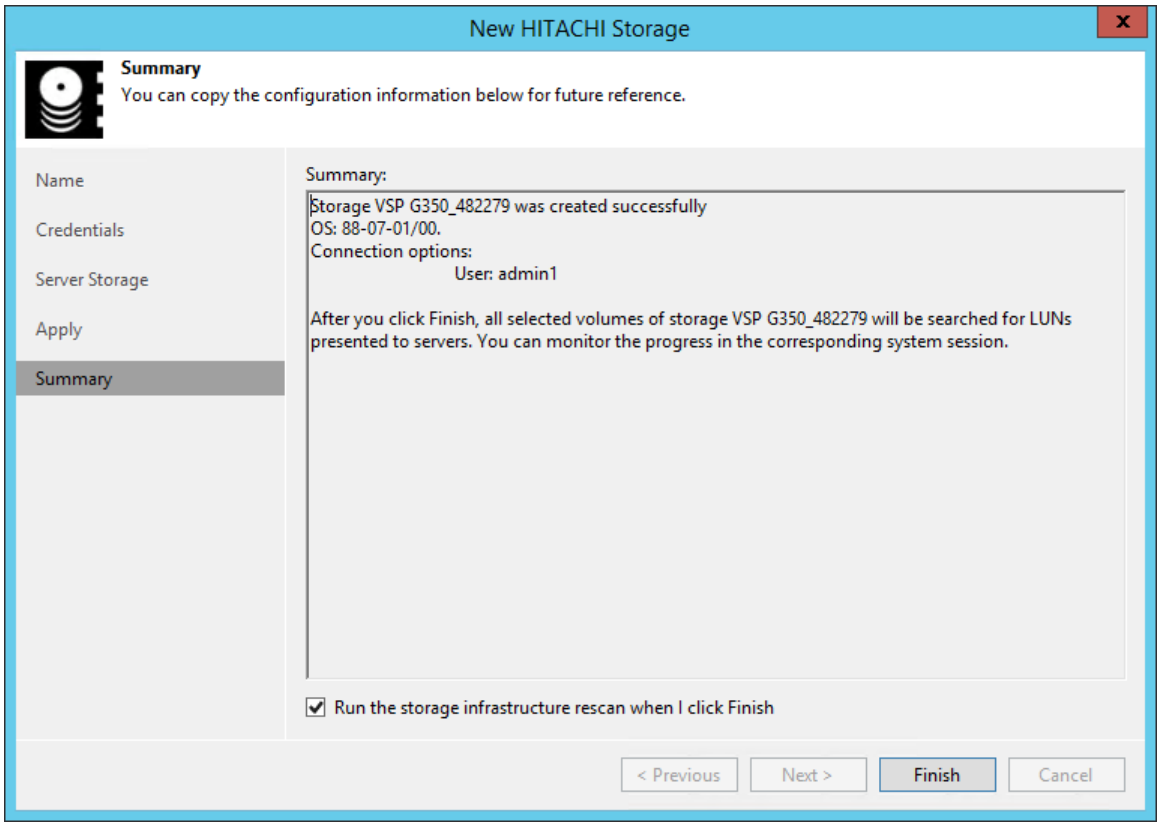


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.

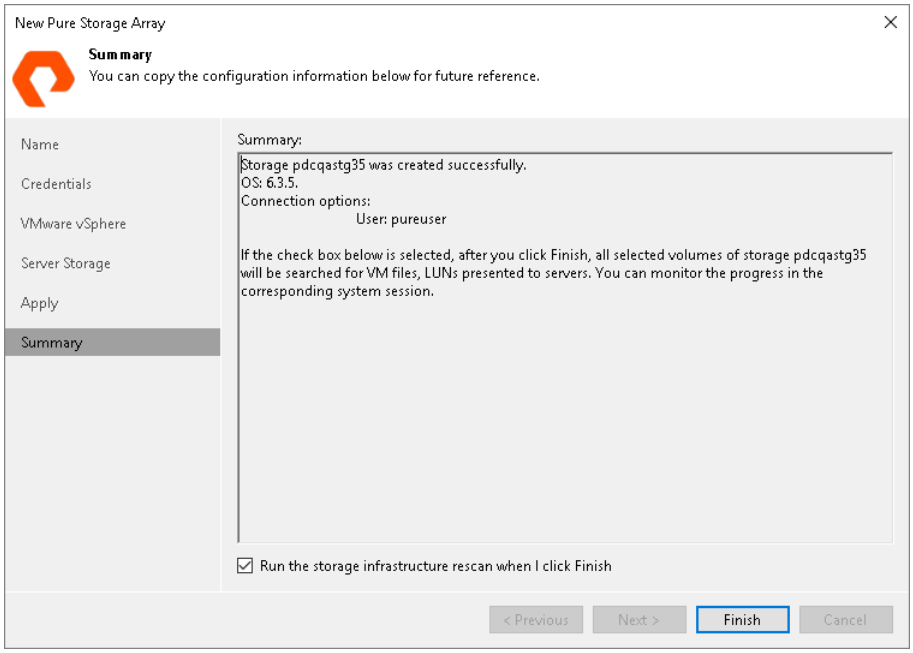


Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system.

Select the **Run the storage infrastructure rescan when I click Finish** check box if you want to start the rescan right after you finish working with the wizard. For more information on the rescan process, see Rescan (Storage Discovery) Process.

Click **Finish** to close the wizard.



Rescanning Storage Systems

You can rescan a storage system added to the backup infrastructure. Storage system rescan gets and updates the information that is necessary for the backup, replication and restore processes. Storage system rescan may be required, for example, if you create or delete snapshots manually on the storage system, not using Veeam Backup & Replication. It also updates a storage system hierarchy in the Veeam Backup & Replication console. For more information about the storage system rescan process, see Rescan (Storage Discovery) Process.

Storage system rescan can be performed automatically or manually.

Before you start a storage rescan, make sure that you have a properly configured backup proxy in the backup infrastructure. Otherwise, Veeam Backup & Replication will not be able to collect data about VMs in the snapshots for which VMFS or NFS rescan is required.

> **NOTE**
>
> Veeam Backup & Replication does not perform rescan on VMs whose disks are located on VVol datastores.

Limiting Rescan Scope

Rescan of the whole storage system hierarchy can take much time. To minimize the rescan time, you can instruct Veeam Backup & Replication to rescan only specific volumes.

To limit the rescan scope, open the storage system connection settings and navigate to the **VMware/NAS/Veeam Agent Access Options** step of the wizard. Select the volumes you want to rescan.

For more information, see **Specify VMware/NAS/Veeam Agent Access Options** step of the relevant **Add Storage** wizard.

Rescan (Storage Discovery) Process

The Storage Discovery process performs rescan of the whole storage system or selected volumes. It can be performed against the following nodes in the storage system hierarchy:

- Vendor
- Storage system
- Storage volume

In case you have limited rescan scope, storage discovery will be performed only for the specified volumes. For details, see Limiting Rescan Scope.

> **NOTE**
>
> If only Veeam Agents or NAS backup processing is selected for a storage system, storage volumes are not displayed and rescan of the specified volumes is not available.

Stages of Rescan

1. [For VMware, NAS, Veeam Agent integration] General infrastructure

   Receiving storage system information.

   a. Defining the storage system data hierarchy (volumes, shares, LUNs, snapshots).

   b. Getting the information about each volume added to rescan scope (name, ID, size, SCSI Unique ID for LUNs, local paths for shares).

   c. Defining basic information about storage snapshots (name, id, creation time).

   d. Getting information about storage adapters (targets).

   e. Receiving other relevant information.

2. [For VMware, NAS, Veeam Agent integration] Availability from backup proxies

   Verifying the possibility of using proxies for backup/rescan/data transmission directly from the storage systems.

   a. Analyzing the selected proxies and checking iSCSI/NFS/SMB servers availability from these proxies.

   b. Matching proxies with available servers. The LUNs/share files available from these servers are considered available from the relevant proxies.

   Availability through Fibre Channel is not checked. If a proxy is added to a storage system list, the access is considered set.

3. [For VMware integration] vCenter/ESXi rescan

   a. Identifying the list of vCenter/ESXi datastores added to Veeam Backup & Replication.

   b. Matching the vCenter/ESXi datastores with volumes (LUNs/share files) added to Veeam Backup & Replication. Making the list of VMs located on datastores.

   c. Creating/updating information files for the VMs in the snapshots of relevant volumes.

      If the VMFS/NFS rescan has not been executed for a volume earlier, we assume that all the snapshots of the volume are for those VMs that have been in the datastore at the moment of rescan.

      If the VMFS/NFS rescan has been executed for a volume earlier, Veeam Backup & Replication skips the next step (updating the VMware hosts information for each VM).

   d. Updating the VMware hosts information for each VM.

4. [For VMware integration] VMFS/NFS rescan

   Scanning the snapshot file system.

   a. Creating storage snapshot clones.

      If a storage system can export snapshots directly to a proxy, snapshot clones are not created.

   b. Exporting storage snapshot clones to the proxy.

   c. Identifying the snapshot file system type.

   d. If the snapshot file system type corresponds with VMFS or NFS, Veeam Backup & Replication searches for the VMX files located in the snapshots.

      Thus the system identifies the VMs located in the snapshots. If this stage has not been performed for these snapshots earlier, the snapshot content shown in Veeam Backup & Replication may be changed on this stage: some VMs may be added or deleted.

e. Defining the VMs size.

f. Removing the storage snapshot clones from the proxy.

g. Deleting the storage snapshot clones.

> **NOTE**
>
> Consider the following:
>
> - Veeam Backup & Replication performs VMFS/NFS rescan of a snapshot only once as snapshots do not change.
> - If rescan was launched automatically and vCenter/ESXi rescan was performed, VMFS/NFS rescan is skipped. If vCenter/ESXi rescan is not possible, VMFS/NFS rescan is performed for snapshots that were not scanned yet.
> - If you launch rescan manually or create a snapshot manually, VMFS/NFS rescan is performed for snapshots that were not scanned yet.

How to Start Storage Discovery

The following actions and processes initiate the Storage Discovery process:

- Storage Monitor

  The Storage Monitor process runs in the background. Every 10 minutes the process checks:

  - Appearance or removal of snapshots in the supervised volumes
  - Changes in the snapshot names in the supervised volumes
  - Changes in the name of the supervised volume itself
  - Appearance or removal of volumes (including changes due to alteration in the rescan scope Volumes to scan)

  If changes are detected, the Storage Monitor initiates the rescan of the container entity, including all rescan stages except VMFS/NFS rescan:

  - Alteration in a snapshot starts rescan of the volume
  - Alteration in a volume starts rescan of the storage system

  If more than 30% of the volumes need to be rescanned, the Storage Monitor starts rescan of the whole storage system.

- Automatic storage rescan

  Rescan of all storage systems, including all rescan stages except VMFS/NFS rescan, starts once a week.

- Adding vCenter Server/ESXi

  Rescan of all storage systems without VMFS/NFS Rescan.

- Adding a backup proxy

  Rescan of all storage systems without vCenter/ESXi and VMFS/NFS Rescan.

- Starting Veeam Backup Service

  Rescan of all storage systems.

- Adding a storage system as a NAS filer

  Rescan of storage systems with NAS integration.

- Selecting **Run the storage infrastructure rescan when I click Finish** check box in a storage system adding wizard

  Rescan of the added storage system, all stages except VMFS/NFS rescan.

- Manual storage rescan

  If necessary, you can start the Storage Discovery process manually. Storage discovery can be performed against the following nodes in the storage system hierarchy: vendor, storage system or storage volume.

  To manually start storage discovery:

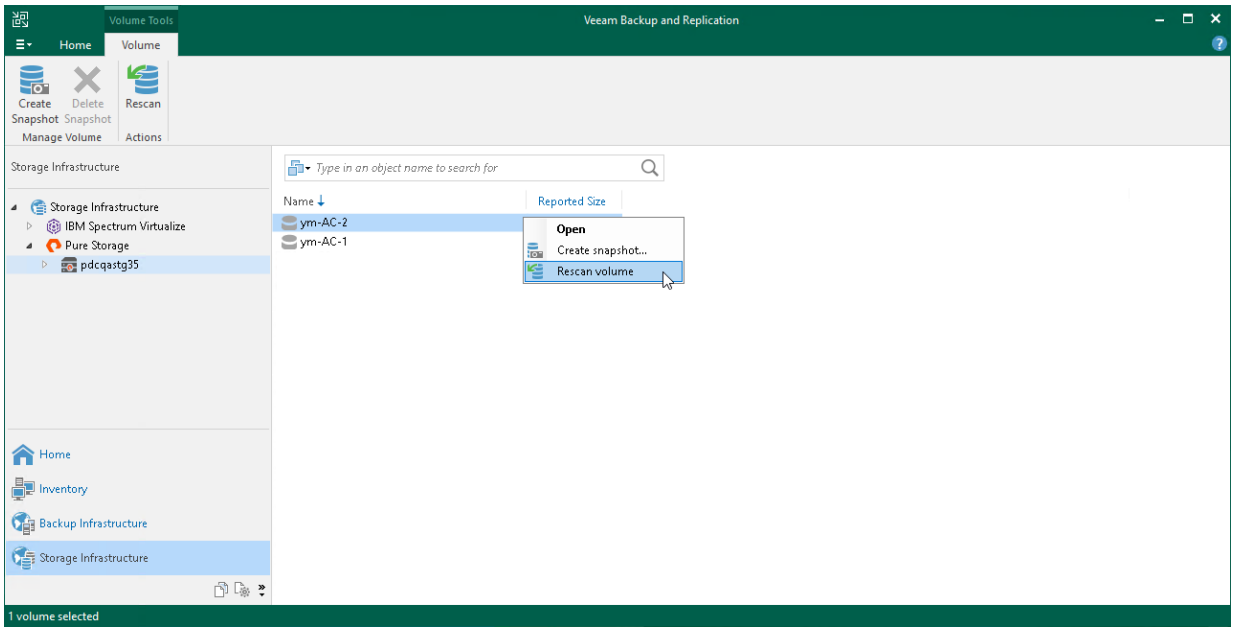
  a. Open the **Storage Infrastructure** view.

  b. In the inventory pane, expand the storage system tree.

  c. Select a node in the storage system hierarchy: vendor, storage system or volume.

  d. Click **Rescan** on the ribbon or right-click the node in the hierarchy and select **Rescan storage** or **Rescan volume**.

> **IMPORTANT**
>
> The rescan operation is performed only for volumes included in the rescan scope. For information how to change the rescan scope, see Limiting Rescan Scope.



Removing Storage Systems

You can remove a storage system from the backup infrastructure.

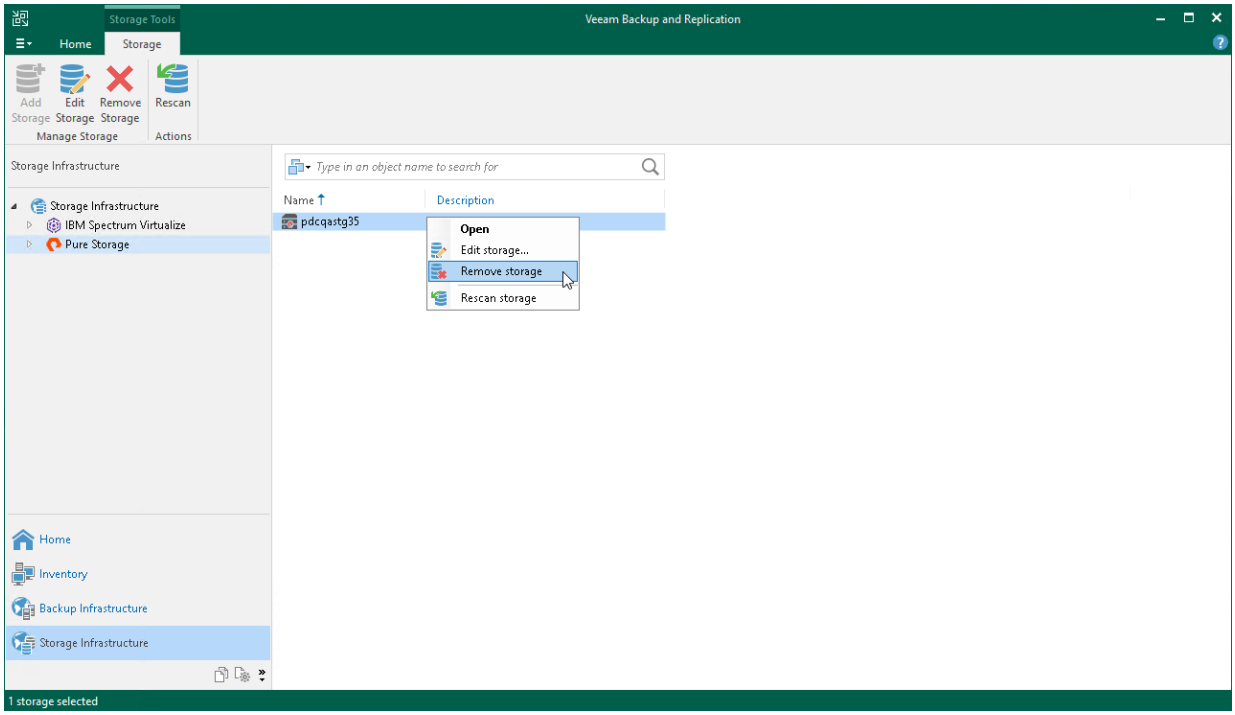
Consider the following:

- When you remove a storage system from the backup infrastructure, Veeam Backup & Replication also finds and removes service objects created by Veeam Backup & Replication on the storage system, for example, hosts and snapshots with *"VeeamAUX"* in names.
- [For VMware integration] You cannot remove a storage system from the backup infrastructure if you have snapshot jobs or backup jobs with the **Secondary Target** settings configured for this storage system. You must delete the jobs first.

When you remove a storage system from the backup infrastructure, Veeam Backup & Replication also finds and removes service objects created by Veeam Backup & Replication on the storage system, for example, hosts and snapshots with *"VeeamAUX"* in names.

To remove a storage system:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane or in the working area, right-click the storage system and select **Remove storage**.



Requirements and Limitations

Backup from Storage Snapshots and Veeam Explorer for Storage Snapshots have a set of requirements and limitations.

Backup from Storage Snapshots has a set of requirements and limitations.

- System Requirements
- Permissions
- General Requirements and Limitations
- Dell VNXe, VNX, SC Limitations
- NetApp Data ONTAP/Lenovo Thinksystem DM Limitations

System Requirements

Veeam Backup & Replication offers integration with the following storage systems:

Dell PowerScale (formerly Isilon)

- Filer integration for NAS backup functionality
- NFS or SMB (CIFS) connectivity
- OneFS 8.1.2 to 9.4

Dell VNX, VNX2, VNXe and Unity XT/Unity

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Dell VNX/VNX2 all OE versions are supported
- Dell VNXe OE versions 3.x
- Dell Unity XT/Unity OE versions 5.0 to 5.2

Fujitsu ETERNUS HX/AX

- NFS, Fibre Channel or iSCSI connectivity
- ONTAP 7-mode versions 8.2 up to 8.2.5
- ONTAP cluster-mode versions 9.1 to 9.13.1 (Version 9.13.1 has some issues. For more details, see this Veeam KB article.)
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- Synchronous SnapMirror is not supported

HPE 3PAR StoreServ

- Fibre Channel (FC) or iSCSI connectivity
- 3PAR OS versions 3.2.2 up to 3.3.1 MU5
- WSAPI 1.5 and later
- iSCSI VLAN tags are supported
- Virtual Domains are supported

HPE Nimble Storage AF-Series, HF-Series and CS-Series

- Fibre Channel (FC) or iSCSI connectivity
- Nimble OS from 5.0 up to 6.1.2

HPE Alletra 5000/6000

- Fibre Channel (FC) or iSCSI connectivity
- OS version 6.0

HPE Primera

- Fibre Channel (FC) or iSCSI (starting from OS versions 4.3 or later) connectivity
- OS versions 4.x
- Virtual Domains are supported

HPE Alletra 9000

- Fibre Channel (FC) or iSCSI connectivity
- OS version 9.3 or later
- Virtual Domains are supported

HPE StoreVirtual (formerly LeftHand/P4000 Series) and StoreVirtual VSA

- iSCSI connectivity only
- LeftHand OS versions 9.5 up to 12.8
- HPE SV3200 (LeftHand OS version 13) is not supported

IBM FlashSystem (formerly Spectrum Virtualize, includes IBM StorWize and IBM SVC)

- Fibre Channel (FC) or iSCSI connectivity
- IBM Spectrum Virtualize OS version 8.2 or later

IBM N Series

- NFS, Fibre Channel or iSCSI connectivity
- ONTAP 7-mode versions 8.2 up to 8.2.5
- ONTAP cluster-mode versions 9.1 to 9.13.1 (Version 9.13.1 has some issues. For more details, see this Veeam KB article.)
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- Synchronous SnapMirror is not supported

Lenovo DM Series

- NFS, Fibre Channel or iSCSI connectivity
- ONTAP 7-mode versions 8.2 up to 8.2.5

- ONTAP cluster-mode versions 9.1 to 9.13.1 (Version 9.13.1 has some issues. For more details, see this Veeam KB article.)
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- Synchronous SnapMirror is not supported

Lenovo Storage V Series

- Fibre Channel (FC) or iSCSI connectivity
- Spectrum Virtualize 8.2 or later

NetApp FAS/AFF/ASA, FlexArray (V-Series), ONTAP Edge/Select/Cloud VSA

- NFS, Fibre Channel or iSCSI connectivity
- ONTAP 7-mode versions 8.2 up to 8.2.5
- ONTAP cluster-mode versions 9.1 to 9.13.1 (Version 9.13.1 has some issues. For more details, see this Veeam KB article.)
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- NetApp Synchronous SnapMirror is not supported

Nutanix Files

- Filer integration for NAS backup functionality
- NFS or SMB (CIFS) connectivity
- Nutanix File Server 3.8.1.3 to 4.2.0

Universal Storage API Integrated Systems

To start working with the following storage systems, you must install storage system plug-ins.

DataCore SANsymphony

- Fibre Channel (FC) or iSCSI connectivity
- DataCore SANsymphony 10.0 PSP12 or later

Dell PowerMax

- Fibre Channel (FC) or iSCSI connectivity
- Dell PowerMax/VMAX All Flash (PowerMax OS microcode family 5978 or later)
- Unisphere for PowerMax 9.2.1.6 or later

Dell PowerStore

- Fibre Channel (FC) or iSCSI connectivity
- Dell PowerStore T and PowerStore X series (PowerStore OS 2.0 or later)

Dell SC Series (formerly Compellent)

- Fibre Channel (FC) or iSCSI connectivity
- Storage Center OS 7.4.2 or later
- FluidFS volumes and Live Volumes are not supported

Fujitsu ETERNUS AF and DX Series

- Fibre Channel (FC) or iSCSI connectivity
- ETERNUS AF series: AF250 S2, AF650 S2, AF150 S3, AF250 S3, AF650 S3
- ETERNUS DX series: DX60 S4, DX100 S4, DX200 S4, DX500 S4, DX600 S4, DX8900 S4, DX60 S5, DX100 S5, DX200 S5, DX500 S5, DX600 S5, DX900 S5
- Storage firmware version:
  - ETERNUS AF S2 and DX S4 series (except DX8900 S4): V10L88-1000 or later
  - ETERNUS AF S3 and DX S5 series, DX8900 S4: V11L30-5000 or later

Hitachi VSP

- Fibre Channel (FC) or iSCSI connectivity
- VSP E series (93-03-01-60/00 or later)
- VSP F series (88-07-01-x0/00 or later)
- VSP G series (88-07-01-x0/00 or later)
- VSP 5100 and VSP 5500 (90-05-01-00/00 or later)
- VSP 5200 and VSP 5600 (90-08-01-00/00 or later)

HPE XP

- Fibre Channel (FC) or iSCSI connectivity
- HPE XP8 (90-05-01-00/00 or later)

INFINIDAT Infinibox F-Series

- NFS, Fibre Channel (FC) or iSCSI connectivity
- InfiniBox 5.0 or later

> **NOTE**
>
> You must add to the backup infrastructure only one of the two InfiniBox storage arrays for which Active/Active Replication is configured, or exclude the replicating volumes on one of these arrays from rescan. For details on how to exclude volumes from rescan, see the Rescanning Storage Systems section in the Veeam Backup & Replication User Guide.

NEC Storage M Series

- Fibre Channel (FC) or iSCSI connectivity
- M120, M320, M320F, M520, M720, M720F (Storage Control Software revision 1234 or later)

NEC Storage V Series

- Fibre Channel (FC) or iSCSI connectivity
- V100, V300 (93-04-21-XX or later)

NetApp SolidFire/HCI

- iSCSI connectivity
- Element OS version 10.0 or later

Pure Storage FlashArray

- Fibre Channel (FC) or iSCSI connectivity
- Purity 4.10 or later

Tintri IntelliFlash (formerly Western Digital IntelliFlash, Tegile)

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Tintri IntelliFlash 3.11 or later

Permissions

To perform data protection and disaster recovery operations with storage snapshots, the account used to connect to a storage system must have necessary permissions.

In This Section

- NetApp Data ONTAP/Lenovo Thinksystem DM Permissions
- Universal Storage API Integrated Systems Permissions

NetApp Data ONTAP/Lenovo Thinksystem DM Permissions

The account used to connect to a NetApp Data ONTAP/Lenovo Thinksystem DM storage system must have the following permissions:

7-Mode

- login-http-admin
- api-system-*
- api-license-* (api-license-list-info)
- api-volume-*
- api-net-*
- api-options-*
- api-vfiler-*
- api-qtree-*
- api-nfs-*
- api-snapshot-*
- api-lun-*
- api-iscsi-*
- api-feature-*
- api-registry-*
- api-fcp-*
- api-file-*
- api-igroup-*
- api-clone-*
- api-snapvault-*
- api-snapmirror-*
- api-cf-*

- cli-options
- security-api-vfiler

CDOT (VMware Integration)

Command/Directory	Access/Query Level
DEFAULT	readonly
cluster	readonly
metrocluster	readonly
fcp	readonly
file	readonly
igroup	all
iscsi	all
network	readonly
node	readonly
security	readonly
security login	readonly
set	readonly
snapmirror	all
system	readonly
version	readonly
qtree	readonly
lun	all

Command/Directory	Access/Query Level
nfs	all
snapshot	all
volume	all
vserver	all

Only as SVM (VMware Integration)

Command/Directory	Access/Query Level
DEFAULT	none
lun	all
lun igroup	all
network	readonly
security	readonly
security login	readonly
snapmirror	all
system	readonly
version	readonly
volume	all
volume file	readonly
volume qtree	all
volume snapshot	all

Command/Directory	Access/Query Level
vserver	all
vserver fcp	all
vserver iscsi	all
vserver nfs	all

CDOT (NAS Backup Integration)

Command/Directory	Access/Query Level
DEFAULT	readonly
security	readonly
security login	readonly
volume snapshot	all
vserver	all
vserver nfs	all

Only as SVM (NAS Backup Integration)

Command/Directory	Access/Query Level
DEFAULT	none
lun	readonly
network	readonly
security	readonly

Command/Directory	Access/Query Level
security login	readonly
snapmirror	readonly
version	readonly
volume	readonly
volume snapshot	all
vserver	all

CDOT (Veeam Agent Integration)

Command/Directory	Access/Query Level
cluster	readonly
lun	all
metrocluster	readonly
network	readonly
system license	readonly
system node	readonly
version	readonly
volume	all
volume snapshot	all
vserver	all

Only as SVM (Veeam Agent Integration)

Command/Directory	Access/Query Level
lun	all
network	readonly
version	readonly
volume	all
volume snapshot	all
vserver	all

Universal Storage API Integrated Systems Permissions

The account used to connect to a Universal Storage API integrated system must be assigned a necessary role in the storage system console and have a set of necessary permissions.

- For Dell PowerMax, the account must be assigned the Storage Administrator role.
- For Fujitsu ETERNUS, the account must be assigned the Software role.
- For NetApp SolidFire/HCI, the account must have the following permissions:
  - Volumes
  - Cluster Admins
- For Western Digital IntelliFlash, the account must be assigned the Veeam Admin Role.
- For DataCore, the account must have the following permissions:
  - General
  - Port
  - Host
  - Virtual disk
  - Snapshot
  - Physical disk
- For Hitachi VSP, the account must be assigned the following roles:
  - Storage Administrator (View Only)
  - Storage Administrator (Provisioning)

    - Storage Administrator (Local Copy)
- For HPE XP, the account must be assigned the following roles:
    - Storage Administrator (View Only)
    - Storage Administrator (Provisioning)
    - Storage Administrator (Local Copy)
- For Dell PowerStore, the account must be assigned the following roles:
    - Administrator
    - Storage Administrator
    - Storage Operator
- For NEC Storage M Series, the account must be assigned the Administrator role.
- For NEC Storage V Series, the account must be assigned the following roles:
    - Storage Administrator (View Only)
    - Storage Administrator (Provisioning)
    - Storage Administrator (Local Copy)

General Requirements and Limitations

The following limitations apply to all storage systems supported by Veeam Backup & Replication.

Backup Infrastructure (VMware, Veeam Agent integration)

[For VM Agent integration] Backup infrastructure for storage snapshots has the following requirements and limitations:

- Before you add a storage system to Veeam Backup & Replication, make sure SAN initiator groups for production ESXi hosts and for proxy hosts are isolated and snapshot clones will not be exported to production environment. Otherwise, you may encounter production infrastructure issues such as doubling of the root RGK4IT_VMware_Cluster_Boot Volume to ESXi.
- [For IBM Spectrum Virtualize 8.4.2 and later with iSCSI connectivity] During Backup from Storage Snapshots and storage rescan, storage snapshot export to a proxy is required. If the default proxy is used, Veeam Backup & Replication creates a service host with the *"VeeamAUX"* prefix in the default portset of the storage system. If you want to send traffic using a custom portset, you can manually specify the required portset in the service host settings. If another proxy is used, check that the host that performs the proxy role has the required portset in the host settings.
- CHAP authentication is not supported for storage systems working over iSCSI.
- SAS connections are not supported.
- Veeam Backup & Replication does not display volumes and snapshots with the *'"VeeamAUX"'* prefix in the storage hierarchy. Such volumes are used for service purposes and are filtered out.

IPv6 Support

IPv6 is supported for the following storage systems:

- Dell Unity XT/Unity, VNXe
- Dell PowerStore
- Fujitsu ETERNUS HX/AX (management connections only)
- Hitachi VSP (data connections for VSP 5000; management and data connections for others)
- HPE Primera, HPE Alletra 9000
- HPE 3PAR StoreServ (management connections only)
- IBM (all supported systems, management connections only)
- NEC Storage M Series (management connections only)
- NEC Storage V Series
- NetApp (except 7-mode)
- Pure Storage FlashArray

If only management IPv6 connection is supported for a storage system, you can add this storage system to backup infrastructure using IPv6 address. However, all data traffic will be transferred over IPv4.

> **NOTE**
>
> Temporary IPv6 addresses are not supported for backup infrastructure components and backed-up machines. For more information about using temporary addresses, see this RFC section.

To use IPv6 addresses and resolve names using IPv6, configure IPv6 communication as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.

Kerberos Authentication

For Kerberos requirements and limitations, see Kerberos Authentication Requirements and Limitations.

Backup from Storage Snapshots (VMware integration)

Backup from storage snapshots has the following limitations:

- Backup from storage snapshots does not support vRDM disks. vRDM disks are skipped from processing.
- Backup from storage snapshots cannot be used for VMs whose disks are located on VVol datastores.
- Backup from storage snapshots cannot be used to back up VM templates.
- Backup from storage snapshots cannot be used to back up encrypted VMs.
- Processing of VMs with VMware vSphere snapshots may take much longer to start compared to using the Direct SAN Access transport mode with iSCSI/FC SAN. In case these delays are unacceptable, we recommend to either delete the VMware vSphere snapshots or avoid using storage snapshots integration to protect such VMs.
- [For HPE Nimble] To backup from Nimble Group secondary arrays, you must configure Nimble Connection Manager on Microsoft Windows-based backup proxies.
- For storage systems working over NFS:
  - VMs that you plan to back up or replicate must not have VMware vSphere snapshots. VMs with snapshots are processed during regular backup job.
  - If you enable the **Enable VMware tools quiescence** option in the job settings, Veeam Backup & Replication will not use Backup from Storage Snapshots to process running Microsoft Windows VMs that have VMware Tools installed.
  - Backup from Storage Snapshots is not supported for SLES operating systems working over IPv6.
- [For HPE 3PAR StoreServ] Export types such as 'Hosts and port' and 'Port' are not supported. If you create such export types for a proxy or ESXi host, Veeam Backup & Replication will automatically create exports with the 'Host' or 'Host set' types instead.

Snapshot Orchestration and Backup from Storage Snapshots with Snapshot Retention (VMware integration)

Snapshot jobs (snapshot-only jobs and backup jobs with storage snapshot retention) have the following requirements and limitations:

- If you remove or re-add a storage array that is already associated with a snapshot job, Veeam Backup & Replication will restart the retention cycle. You will need to manually remove old snapshots that are no longer needed.

- [For Veeam Backup & Replication prior cumulative patch 20230412 for v12] If you use replication or archiving features and plan to create a snapshot chain on the secondary storage array, check that all VMs that you add to the job reside on volumes with the configured feature. If any VM resides on a volume without the configured feature, snapshot on the secondary storage will not be created for this VM and all other VMs in the job that reside on at least one of the same volumes as this VM.
- You cannot configure a job to create storage snapshots on arrays of different storage vendors.
- For IBM Spectrum Virtualize:
  - Before you add this storage system to the backup infrastructure, make sure that a license for the IBM Spectrum Virtualize storage system supports IBM FlashCopy.
  - When you add IBM Spectrum Virtualize storage systems with HyperSwap function to the backup infrastructure, Veeam Backup & Replication, by default, works with primary storage volumes.
- For HPE 3PAR StoreServ:
  - Enable HPE 3PAR Web Services API server. Veeam Backup & Replication uses the HPE 3PAR Web Services API server to work with the HPE StoreServ storage system.
  - A license for the HPE 3PAR StoreServ storage system must support HPE 3PAR Virtual Copy.
  - You can use backup jobs to create a snapshot chain either on a primary or on a secondary storage array, but you cannot configure snapshot creation on both storage arrays at the same time.
- For snapshot-only jobs:
  - If a VM added to the job has several disks that reside on the same volume, you cannot exclude specific VM disks from the backup as Veeam Backup & Replication creates snapshots at the volume level.
  - Veeam Backup & Replication does not support guest file indexing for snapshot-only jobs.
  - You cannot perform backup of VMs residing on a VMware datastore that comprises several extents (usually due to the use of several LUNs).

Data Recovery from Storage Snapshots (VMware integration)

Data Recovery from Storage Snapshots has the following limitations:

- During restore of VM guest OS files from storage snapshots, data is transferred over LAN through the Network Block Device protocol (NBD). Therefore, restore performance may not be optimal.
- You cannot perform any kind of restore operation (Instant VM Recovery, VM guest OS files restore and application items restore) if a VMware datastore comprises several extents (usually due to the use of several LUNs).
- Veeam Explorer for Storage Snapshots does not support VMs whose disks are located on VVol datastores.
- For snapshots created by jobs, Veeam Backup & Replication supports multi-home restore (when VM disks are hosted on different VMware datastores).
- For snapshots created not by jobs, for example, native storage snapshots, consider the following:
  - Veeam Backup & Replication supports restore operations and also restores only disks residing on the same datastore as the VMX file.
  - You will not be able to restore VM disks that contain an absolute path in the VMX file.
  - You will not be able to perform Instant Recovery and restore VM guest OS files to the original location from snapshots on secondary storage arrays.

- If you remove or re-add a storage array to the backup infrastructure, you will be able to restore data only from those VM disks that are hosted on the same datastore as the VMX file.
- You cannot restore data of a VM whose disks are hosted on storage systems of different storage vendors.
- If you plan to restore data from archived snapshots, you must first retrieve the snapshot as described in Retrieving Data from Achived Snapshots. If VM disks are stored on multiple archived volume snapshots (multi-home VM), you need to retrieve all the snapshots from archives.
- You cannot restore files directly to the original location from backups of BSD, Mac and Solaris VMs. You cannot restore files directly to the original location from NSS filesystems. Use the **Copy to** option instead.
- If the original VM is removed from vSphere infrastructure or migrated to another datastore, you will not be able to perform VM guest OS files restore to the original location.
- [For HPE 3PAR StoreServ] Export types such as "Hosts and port" and "Port" are not supported. If you create such export types for a proxy or ESXi host, Veeam Backup & Replication will automatically create exports with the "Host" or "Host set" types instead.

Kerberos Authentication for Storage Systems

This section lists requirements, limitations and peculiarities in work of storage systems that use Kerberos authentication.

General Requirements and Limitations

For management connection:

- Kerberos authentication is supported for the following storage systems: Dell Unity XT/Unity, Dell VNX block storage, HPE 3PAR StoreServ, HPE Primera, HPE Alletra 9000, HPE Nimble, HPE Alletra 6000, HPE Alletra 5000, Pure Storage FlashArray, INFINIDAT InfiniBox F Series, Dell SC Series, Dell PowerStore, Dell PowerMax, Hitachi VSP, HPE XP, NetApp ONTAP, Lenovo DM Series, NetApp Element, Tintri IntelliFlash.
- Storage systems that use SSH are not supported.

[For VMware integration] For data connections, that is, usage during backup and restore:

- Storage systems with NFS 4.1 connectivity are supported: NetApp ONTAP, Dell Unity XT/Unity, Tintri.
- The following Kerberos protocols are supported: krb5, krb5i and krb5p.
- [For NetApp ONTAP] The Create required export rules automatically option must be disabled.

User Name Formats

When adding storage systems that use Kerberos, specify user names in the following formats:

- Dell PowerStore: domain\username, username@domain
- Dell SC Series: username, domain\username, username@domain
- Dell Unity XT/Unity: username@domain
- Dell VNX block storage: username
- Hitachi VSP: username
- HPE 3PAR StoreServ, HPE Primera, HPE Alletra 9000: username
- HPE Nimble, HPE Alletra 6000, HPE Alletra 5000: username, domain\username, username@domain
- HPE XP: username
- INFINIDAT InfiniBox F Series: username
- NetApp Element: username
- NetApp ONTAP, Lenovo DM Series: domain\username
- Pure Storage FlashArray: username
- Tintri IntelliFlash: username, domain\username, username@domain

Backup and Rescan (VMware integration)

Which protocol Veeam Backup & Replication tries to use during backup and storage rescan depends on the type of the used backup proxy.

- If a Microsoft Windows-based proxy is used, Veeam Backup & Replication first tries to connect without Kerberos at first. If the connection fails, Veeam Backup & Replication tries to connect using Kerberos protocols in the following order: krb5p, krb5i, krb5.

  You can change the order using a registry value: `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\NFSKerberosEncryptionLevel (DWORD}`.

  The values can be the following:

  - 0 — non-Kerberos -> krb5p -> krb5i -> krb5 (default value)
  - 1 — krb5 -> non-Kerberos -> krb5p -> krb5i
  - 2 — krb5i -> non-Kerberos -> krb5p -> krb5
  - 3 — krb5p -> non-Kerberos -> krb5i -> krb5

- If a Linux-based proxy is used, the used protocol depends on how the *mount* command is implemented in the used Linux distributive.

  You can specify the order using a registry value: `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\SanNfsLinuxMountOptions {REG_MULTI_SZ}`.

  This registry value allows you to override Linux proxy mount settings for Backup from Storage Snapshots and storage NFS rescan. You need to specify NFS share path, semicolon and the list of mount parameters separated by commas. In the NFS share path, you can use wildcards: * to represent any number of letters, and ? for a single letter. For example, `172.24.24.*;rw,soft,vers=4.1,timeo=300,retrans=10,sec=krb5`.

Restore (VMware integration)

During restore from a storage snapshot, Veeam Backup & Replication creates an NFS datastore using non-Kerberos protocol. If the connection fails, Veeam Backup & Replication tries to use Kerberos protocols in the following order: krb5, krb5i.

You can change the protocol using a registry value: `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication\SanRestoreNfsKerberosEncryptionLevel (DWORD}`.

The values can be the following:

- 0 — non-Kerberos -> krb5 -> krb5i (default value)
- 1 — non-Kerberos
- 2 — krb5
- 3 — krb5i

Cisco HyperFlex Requirements and Limitations

[For VMware integration] If you plan to perform backup and replication from Cisco HyperFlex storage snapshots, consider the following limitations:

- License for Veeam Backup & Replication Enterprise Plus edition is installed on the backup server.
- Cisco HyperFlex system is added to the backup infrastructure. For more information, see Adding Cisco HyperFlex Storage System.
- VMs must be hosted on the supported Cisco HyperFlex system. For more information, see the System Requirements section in the Veeam Backup & Replication User Guide.
- Backup proxy is properly configured in the backup infrastructure. For more information, see Configuring Backup Proxies.
- VMs must not have VMware vSphere snapshots created using traditional ESXi snapshot technology. Snapshots created using the NFS native snapshot technology may be present.

  During backup or replication, Veeam Backup & Replication fails to trigger Cisco HyperFlex snapshots on VMs that already have VMware vSphere snapshots created using traditional ESXi snapshot technology. You can instruct Veeam Backup & Replication to process these VMs in the regular data processing mode. To do this, enable the **Failover to standard backup** option in job settings.
- Disks of a processed VM must be hosted on the same Cisco HyperFlex NFS store. If some VM disks are hosted on an NFS store other than the store where the VM configuration file resides, such VM will be processed in the regular backup mode.
- The **Limit processed VM count per storage snapshots to N** option is not applicable to Cisco HyperFlex since snapshots for VMs hosted on Cisco HyperFlex are created at the VM level, not volume level.
- For working with REST API, use default route and default port: `https://{hostname}:443`.

Dell VNXe, VNX, SC Limitations

If you plan to perform operations with Dell storage snapshots, consider the following limitations:

- Dell VNXe
- Dell VNX Block
- Dell VNX File
- Dell SC

Dell VNXe

The following limitations apply to Dell VNXe storage systems:

- [For VMware, Veeam Agent integration] Concurrent operations from the same LUN (such as backup and restore) are not supported due to Dell VNXe limitation.
- [For VMware, Veeam Agent integration] In Dell VNXe, you cannot export more than one storage snapshot for a LUN or LUN group concurrently. For this reason, Veeam Backup & Replication can perform only one task that uses storage snapshots at the same time.
- [For VMware integration] In Veeam Backup & Replication, tasks have the following priority levels (starting with the highest priority): restore task > backup job > rescan task. If you start several jobs or tasks that use storage snapshots, Veeam Backup & Replication will check what priority tasks have and perform the following actions:
  - If a LUN snapshot is exported for storage rescan and you start a backup job or restore task at the same time, the rescan process will fail.
  - If a LUN snapshot is exported for a backup job and you start another backup job at the same time, the second backup job will be waiting until the first backup job is finished.
  - If a LUN snapshot is exported for a restore task and you start a backup job at the same time, the backup job will fail (or failover to the regular processing mode if the necessary settings are enabled in the backup job).
  - If a LUN snapshot is exported for a backup job and you start a restore task at the same time, the restore task will be waiting until the backup job is finished.

  This limitation does not apply to Dell Unity XT/Unity storage systems.

Dell VNX Block

[For VMware, Veeam Agent integration] The following limitations apply to Dell VNX Block storage systems:

- Veeam Backup & Replication supports LUNs that reside on Storage Pools.
- To take LUN snapshots, Veeam Backup & Replication uses the VNX snapshot technology. Make sure that you have a license that covers this technology. The SnapView snapshot technology is not supported.

Dell VNX File

[For VMware integration] The following limitations apply to Dell VNX File storage systems:

- A read-only checkpoint can have only one writable snapshot. If a read-only checkpoint already has a writable snapshot, Veeam Backup & Replication uses this writable snapshot for restore.
- Writable snapshots are not detected by the storage rescan process and are not displayed in the storage system hierarchy.

Dell SC

[For VMware, Veeam Agent integration] Make sure that multiple proxy servers are not part of a single Server object.

NetApp Data ONTAP/Lenovo Thinksystem DM Limitations

If you plan to perform operations with NetApp Data ONTAP/Lenovo Thinksystem DM storage snapshots, consider the following limitations:

- Volumes with NetApp SnapLock enabled are not supported.
- [For VMware integration] Veeam Backup & Replication may fail to perform backup from secondary storage arrays if SVM/volumes have identical names between primary and secondary storage arrays.
- [For VMware, Veeam Agent integration] When the storage is added as a specific SVM, and not as a whole cluster, you must set up Aggregation List for vServer so that FlexClone Volume will work properly. Otherwise, errors like this will arise: "*Cannot create volume. Reason: aggregate aggr1 is not in aggr-list of Vserver svm-dr-nfs".*
- [For VMware, NAS, Veeam Agent integration] Depending on the protocol type and operating mode of the storage system, Veeam Backup & Replication uses different technologies to perform Backup from storage snapshots.

  You may need to install additional licenses. You need to install one license, even if several technologies can be used for snapshot clone creation.
- [For VMware, NAS integration] NetApp FlexGroups are not supported for storage snapshot integration scenarios (including NAS Backup).
- [For VMware integration] Backup jobs from storage snapshots with secondary target are not supported if several SnapMirror/SnapVault relationships are configured for one source volume.
- [For VMware integration] Multi-home restore is not supported for NetApp 7-mode with NFS protocol (all snapshots) and for SnapMirror Target Snapshots with NFS or iSCSI/FC protocol.
- [For VMware, NAS integration] The snapshot directory must be visible in the NFS or SMB shares. To learn more about making the snapshot directory visible, see NFS and SMB (CIFS) Protocols.

Rescan of NetApp Storage Systems

cDot

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
Primary Storage System			
iSCSI/FC	Possible	Possible	Not possible
NFS	Possible (not used)	Possible	Possible
Secondary Storage System: SnapMirror and SnapVault			

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
iSCSI/FC	Possible	Not possible	Not possible
NFS	Possible	Possible	Possible

7-Mode

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
Primary Storage System			
iSCSI/FC	Possible	Possible (not used)	Possible
NFS	Possible (not used)	Possible (not used)	Possible (not used)
Secondary Storage System: SnapMirror and SnapVault			
iSCSI/FC	Possible	Possible (not used) for SnapVault Not possible for SnapMirror	Possible for SnapVault Not possible for SnapMirror
NFS	Possible (not used)	Possible (not used)	Possible (not used)

NOTE

During storage rescan, Veeam Backup & Replication adds its export rules for the storage. New rules are added at the beginning of the list, shifting existing rules down in the list.

Backup from Storage Snapshots

cDot

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
Primary Storage System			
iSCSI/FC	Possible	Possible	Not possible

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
NFS	Possible (not used)	Possible (not used)	Possible
Secondary Storage System: SnapMirror and SnapVault			
iSCSI/FC	Possible	Not possible	Not possible
NFS	Possible (not used)	Possible (not used)	Possible

7-Mode

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
iSCSI/FC	Possible	Possible (not used)	Possible
NFS	Possible (not used)	Possible (not used)	Possible (not used)
Secondary Storage System: SnapMirror and SnapVault			
iSCSI/FC	Possible	Possible (not used) for SnapVault Not possible for SnapMirror	Possible for SnapVault Not possible for SnapMirror
NFS	Possible (not used)	Possible (not used)	Possible (not used)

NOTE

During backup from storage snapshots, Veeam Backup & Replication adds its export rules for the storage. New rules are added at the beginning of the list, shifting existing rules down in the list.

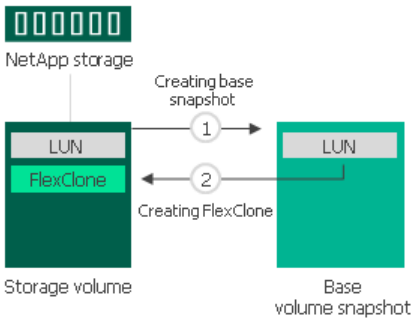
FlexClone

[For VMware, Veeam Agent integration] The FlexClone technology lets you create a transparent, space-efficient copy of a LUN. FlexClones are created in seconds and require little space on the storage. Unlike traditional LUN clones, FlexClones are independent and do not cause any problems with volume snapshot deletion.

For Backup from Storage Snapshots, Veeam Backup & Replication creates a FlexClone in the following way:

1. Veeam Backup & Replication creates a temporary snapshot of a volume hosting a LUN to capture the momentary state of this LUN.
2. After that, Veeam Backup & Replication creates a LUN clone.

This temporary volume snapshot is used as a base for a FlexClone. However, the base snapshot is not tied to the FlexClone, as a backing snapshot in traditional LUN cloning. Veeam Backup & Replication can delete it without any impact for the FlexClone at any time.

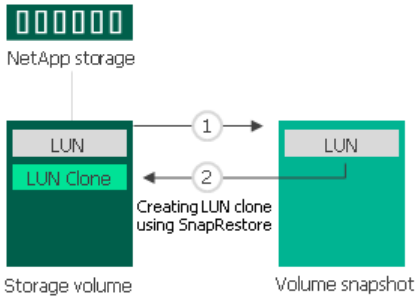


SnapRestore

[For VMware, Veeam Agent integration] For NetApp storage systems that work in the cDot operating mode and have a SnapRestore license installed, Veeam Backup & Replication can use the NetApp SnapRestore technology for Backup from Storage Snapshots.

Veeam Backup & Replication creates a storage snapshot in the following way:

1. Veeam Backup & Replication creates a snapshot of a volume holding backup data.
2. Veeam Backup & Replication creates a LUN clone using SnapRestore.



Traditional LUN Cloning

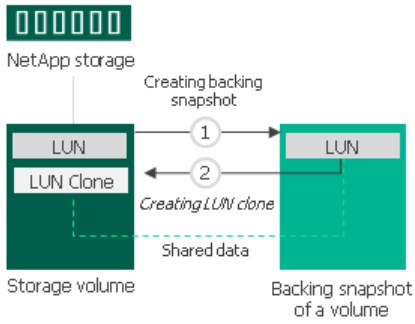
[For VMware, Veeam Agent integration] For NetApp storage systems that do not have a FlexClone license installed, Veeam Backup & Replication uses the NetApp traditional LUN cloning technology.

Traditional LUN clones are created with the help of a backing snapshot.

1. Veeam Backup & Replication creates a backing snapshot for a LUN holding backup data. The backing snapshot is a snapshot of a volume where the LUN is located. The backing snapshot acts as a helper, or medium, for the LUN clone. It contains a momentary image of the LUN and captures the exact state of the LUN at the necessary point in time.

2. After that, Veeam Backup & Replication creates a LUN clone.

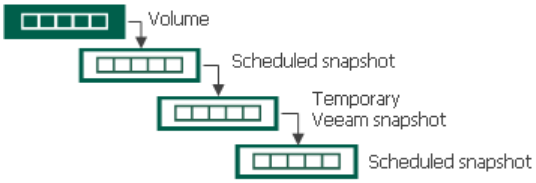
The LUN clone bases on the backing snapshot and shares its data with the backing snapshot.
Veeam Backup & Replication cannot delete the backing snapshot before the LUN clone is removed. Deletion of the backing snapshot will corrupt the LUN clone.



In case of traditional LUN cloning, backing snapshots created by Veeam Backup & Replication may be locked and may fail to be deleted automatically with cleanup operations. This can happen, for example, if you schedule the NetApp storage system to create daily volume snapshots, and the scheduled operation begins before Veeam Backup & Replication deletes the backing snapshot that was used for backup or replication.

In this situation, the created backing snapshot will become a part of the snapshot chain. The scheduled snapshot and all subsequent snapshots will reference this snapshot, and Veeam Backup & Replication will be unable to remove it. As a result, your retention policy for scheduled snapshots may be disrupted.

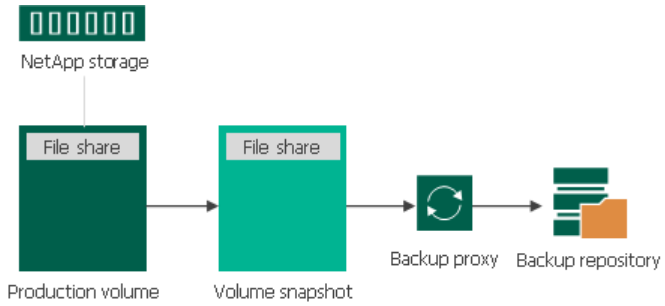
To avoid this situation, it is recommended that you install a FlexClone license on the NetApp storage system. In this case, Veeam Backup & Replication will use the FlexClone technology for LUN cloning.



NFS and SMB (CIFS) Protocols

[For VMware, NAS integration] If the NetApp storage system operates over SMB (CIFS) (for NAS integration) or over NFS (both for VMware and NAS integration), you do not have to install any additional licenses to use Backup from Storage Snapshots.

For Backup from Storage Snapshots, Veeam Backup & Replication creates a snapshot of a volume on which the file share with backup data resides. The created volume snapshot is used as a source of data.
Veeam Backup & Replication uses the client on the backup proxy and the proxy reads the data from the shared folder storing the volume snapshot.



Requirements for NFS Protocol

Make sure that the following requirements are met:

- [For VMware, NAS integration] NFS access rules (SVM export policies) are created. VBR can create the NFS access rules automatically. You can turn off this option, but in this case make sure the settings are correct.
- [For VMware integration] If you are using a secondary NetApp in backup process, its volumes are mounted (have configured mount path).
- [For VMware, NAS integration] The snapshot directory (.snapshot) is visible in the NFS volumes. To ensure that, login to your NetApp Ontap System Manager, select the NFS volume, click **Snapshot Copies** - **Configuration Settings** and select the box **Make Snapshot directory (.snapshot) visible**.

Requirements for SMB (CIFS) Protocol

[For NAS integration] Make sure that the following requirements are met:

- SMB (CIFS) access rules (SVM export policies) are created. VBR can create the SMB access rules automatically. You can turn off this option, but in this case make sure the settings are correct.
- Permissions for access to the SMB share are properly configured. To ensure that, login to your NetApp Ontap System Manager, select the SMB share in **Storage** - **Shares**, click **Edit** to open share settings, and configure permissions in the **Permissions** tab.
- The snapshot directory (~snapshot) is visible in the SMB share. To ensure that, login to your NetApp Ontap System Manager, select the SMB share in **Storage** - **Shares**, click **Edit** to open share settings, and select the **Show Snapshots** check box in the **Options** tab.

Restore from Storage Snapshots

cDot

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
Primary Storage System			

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)
iSCSI/FC	Possible	Possible	Not possible
NFS	Possible	Possible	Not possible
Secondary Storage System: SnapMirror and SnapVault			
iSCSI/FC	Possible	Not possible	Not possible
NFS	Possible	Not possible	Not possible

7-Mode

Storage Type	FlexClone (recommended)	SnapRestore	No license (Traditional LUN cloning)	NDMP
Primary Storage System				
iSCSI/FC	Possible	Possible (not used)	Possible	Not possible
NFS	Possible	Possible[1]	Not possible	Possible
Secondary Storage System: SnapMirror and SnapVault				
iSCSI/FC	Possible	Possible for SnapVault Not possible for SnapMirror	Possible for SnapVault Not possible for SnapMirror	Not possible
NFS	Not possible for SnapVault[2] Possible for SnapMirror	Possible for SnapVault[1] Not possible for SnapMirror	Not possible	Possible

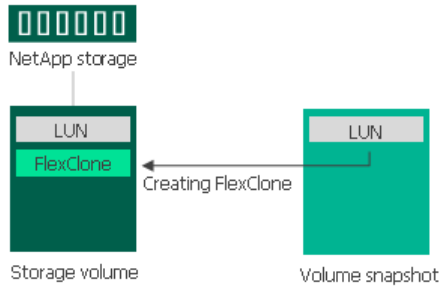
[1] Veeam Backup & Replication copies VM files from the /vol/volname/VMFolder/ folder from the snapshot to the /vol/vvolname/Veeam_Restore_VMname/VMFolder/ folder. The restore wizards work with copied files.

[2] Can be used only for file-level restore. To enable restore, you can use registry values. For more information, contact Veeam Customer Support.

FlexClone

For NetApp storage systems that have a FlexClone license installed, Veeam Backup & Replication uses the NetApp FlexClone technology for restore from storage snapshots.

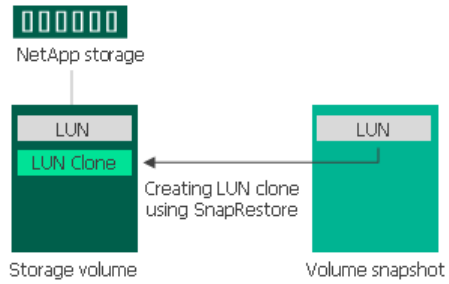
During restore from storage snapshots, Veeam Backup & Replication creates a FlexClone of a LUN. The storage snapshot from which you want to restore data is used as a base copy. The FlexClone is then mounted to an ESXi host, and you can restore the necessary VM data from it.



SnapRestore

For NetApp storage systems that have a SnapRestore license installed, Veeam Backup & Replication uses the NetApp SnapRestore technology for restore from storage snapshots.

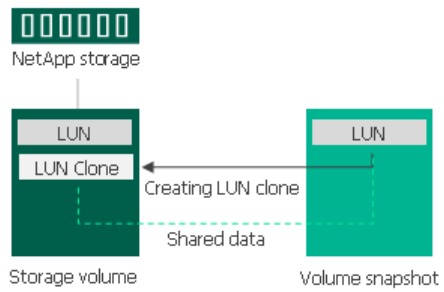
When you restore data from storage snapshot, Veeam Backup & Replication triggers NetApp to create a clone of a LUN using SnapRestore. To do this, NetApp restores LUN data to a new location on the volume where the original LUN is located. As a result, you have a read-write copy of the LUN holding VM data, and can use this copy for restore operations.



Traditional LUN Cloning

For NetApp storage systems that do not have the FlexClone license installed, Veeam Backup & Replication uses the NetApp traditional LUN cloning technology.

During restore from storage snapshots, Veeam Backup & Replication creates a LUN clone. The storage snapshot from which you want to restore data is used as a backing copy. The LUN clone is then mounted to an ESXi host, and you can restore VM data from it.



NFS Protocol

When you perform restore from storage snapshot on NetApp storage systems working over the NFS protocol, Veeam Backup & Replication triggers NetApp to clone an NFS share that holds VM data. NetApp creates a copy of the NFS share and places this copy on the same volume where the original NFS share is located. This copy is used as a data source for restore operations.

After a copy of the NFS share is created, Veeam Backup & Replication mounts the NFS share copy to an ESXi host as a new datastore, and you can restore VM data from the mounted NFS share copy.

If you have several VMs that reside on the same storage snapshot, Veeam Backup & Replication will create only one NFS datastore per snapshot. During restore, VMs from the same snapshot are copied to the same folder on the volume where the original NFS share is located. When you start the restore process for the first VM on the storage snapshot, the folder is presented as a datastore to an ESXi host. After you finish the restore process for the last VM on the storage snapshot, the folder is unmounted from the ESXi host.

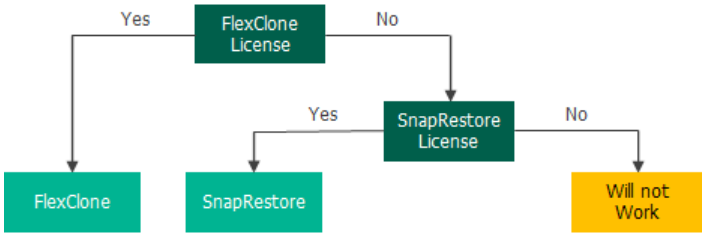
Depending on whether you restore from a primary or secondary storage system, the operation mode of the NetApp storage system, Veeam Backup & Replication uses different technologies to create a clone of an NFS share.

Cloning Primary Storage System

cDot

If the NetApp storage system operates in the cDot mode, you must have a FlexClone or SnapRestore license installed.

- If you have a FlexClone license installed, Veeam Backup & Replication uses the FlexClone technology.
- If you have a SnapRestore license installed, Veeam Backup & Replication uses the SnapRestore technology.
- If neither FlexClone nor SnapRestore license is installed, VM data restore will fail.



7-mode

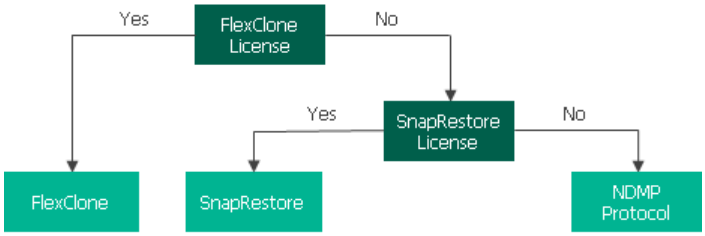
If the NetApp storage system operates in the 7-mode, you must have a FlexClone or SnapRestore license installed, or the NDMP protocol enabled.

Veeam Backup & Replication uses the following technologies for LUN clone creation:

- If you have a FlexClone license installed, Veeam Backup & Replication uses the FlexClone technology.
- If you have a SnapRestore license installed, Veeam Backup & Replication uses the SnapRestore technology.
- If neither FlexClone nor SnapRestore license is installed, Veeam Backup & Replication uses the NDMP protocol. If the NDMP protocol is not enabled, VM data restore will fail.

IMPORTANT

[For Instant Recovery] Veeam Backup & Replication performs actual Instant Recovery only if a FlexClone license is installed. If the SnapRestore license is installed or the NDMP protocol is enabled, Veeam Backup & Replication performs entire VM restore instead of Instant Recovery. As a result, the restore process takes more time and may fail due to exceeding the default protocol timeout.



Cloning Secondary Storage System

Cloning SnapVault

cDot

If the NetApp storage system operates in the cDot, you must have a FlexClone license installed. In the opposite case, VM data restore will fail.

7-mode

If the NetApp storage system operates in the 7-mode, you must have a SnapRestore license installed or the NDMP protocol enabled.

- If you have a SnapRestore license installed, Veeam Backup & Replication uses the SnapRestore technology.
- If a SnapRestore license is not installed, Veeam Backup & Replication uses the NDMP protocol. If the NDMP protocol is not enabled, VM data restore will fail.

IMPORTANT

[For Instant Recovery] If you restore data from NetApp SnapVault, Veeam Backup & Replication performs entire VM restore instead of Instant Recovery. As a result, the restore process takes more time and may fail due to exceeding the default protocol timeout.

Cloning SnapMirror

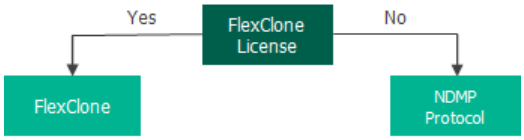
cDot

If the NetApp storage system operates in cDot, you must have a FlexClone license installed. In the opposite case, VM data restore will fail.

7-mode

If the NetApp storage system operates in the 7-mode, you must have a FlexClone license installed or the NDMP protocol enabled.

- If you have a FlexClone license installed, Veeam Backup & Replication uses the FlexClone technology.
- If a FlexClone license is not installed, Veeam Backup & Replication uses the NDMP protocol. If the NDMP protocol is not enabled, VM data restore will fail.



IMPORTANT

[For Instant Recovery] If you restore data from NetApp SnapMirror, Veeam Backup & Replication performs actual Instant Recovery only if a FlexClone license is installed. If the NDMP protocol is enabled, Veeam Backup & Replication performs entire VM restore instead of Instant Recovery. As a result, the restore process takes more time and may fail due to exceeding the default protocol timeout.

Universal Storage API Integrated Systems

Veeam Backup & Replication offers built-in integrations with storage systems to help decrease impact on the production environment and significantly improve RPOs. Storage vendors, in turn, can leverage the Veeam Universal Storage API framework to integrate their storage solutions with Veeam Backup & Replication. With this kind of integration, you can use snapshots of Universal Storage API integrated systems to perform backup and restore operationsThis kind of integration can be used in Veeam Agent integration only..

The following storage systems are supported:

- DataCore SANsymphony
- Dell PowerMax
- Dell PowerStore
- Dell SC Series
- Fujitsu ETERNUS AF/DX Series
- Hitachi VSP
- HPE XP
- INFINIDAT InfiniBox F Series
- NEC Storage M Series
- NEC Storage V Series
- NetApp SolidFire/HCI
- Pure Storage FlashArray
- Tintri IntelliFlash/Western Digital/Tegile

To start working with Universal Storage API integrated systems, you must perform the following steps:

1. Download the necessary storage system plug-in from the Veeam Download page.
2. Install the storage system plug-in.
3. Configure the backup infrastructure for storage integration.

Prerequisites for API Integrated Systems

You can use snapshots of Universal Storage API integrated systems in Veeam Agent integration only.

[For VMware, Veeam Agent integration] Before you add storage systems to Veeam Backup & Replication, check the following prerequisites:

- You must install the storage system plug-in. For more information, see Installing Storage System Plug-Ins.
- Check prerequisites in the following Veeam KB articles: DataCore SANsymphony, Dell PowerMax requirements, Dell PowerStore requirements, Fujitsu ETERNUS AF/DX Series, Hitachi VSP requirements, HPE XP requirements, INFINIDAT InfiniBox F Series, NEC Storage M Series requirements, NEC Storage V Series requirements, NetApp SolidFire/HCI, Pure Storage FlashArray, Tintri IntelliFlash/Western Digital/Tegile.

Installing Storage System Plug-Ins

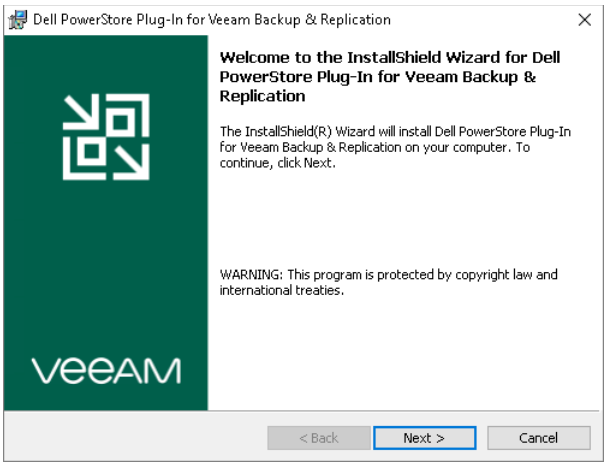
Before you start working with Universal Storage API integrated systems, make sure you have installed the Universal Storage API integrated system plug-in on the Veeam backup server.

To install the plug-in, perform the following steps:

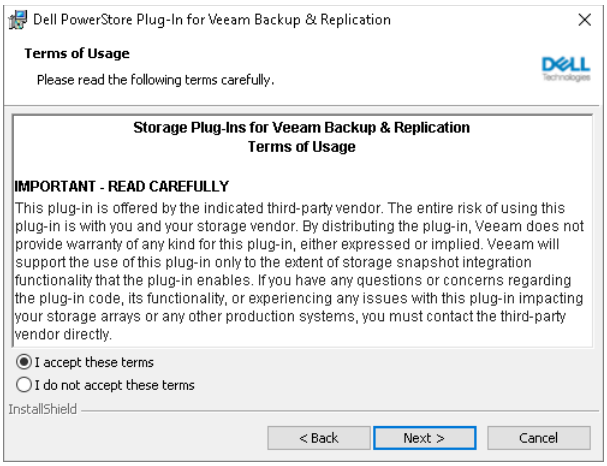
1. Run the plug-in installation file.

   The latest version of the Universal Storage API integrated system plug-in is available at the Veeam Download page.

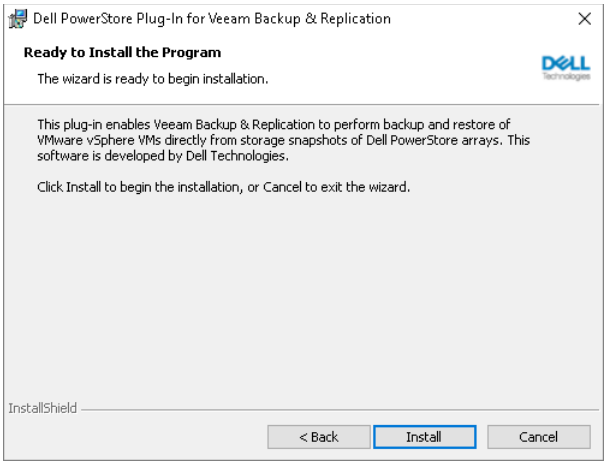
2. On the welcome screen of the setup wizard click the **Next** button to proceed to the installation configuration.



3. At the **Terms of Usage** step of the wizard, select **I accept these terms**.



4. At the **Ready to Install the Program** step of the wizard, click **Install** to begin installation.



5. When the installation process completes, click **Finish** to close the wizard.

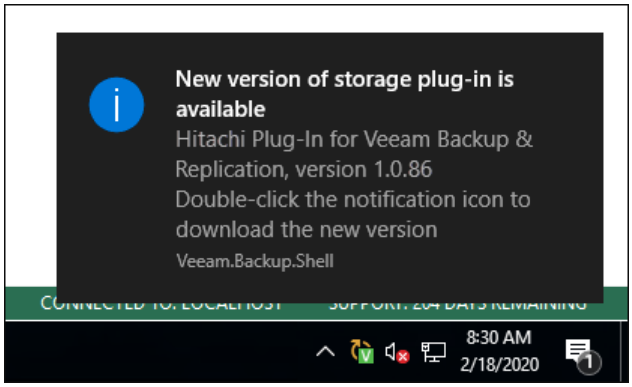
After you install the plug-in, you must configure the backup infrastructure to be able to use storage snapshots for data protection. For more information, see Backup Infrastructure for Storage Integration.

Update Notifications

Veeam Backup & Replication uses update notifications to inform you about new versions of Universal Storage API integrated system plug-ins. When a new version of a plug-in becomes available on the website, Veeam Backup & Replication displays an icon in the system tray. An icon is displayed once a week.

To get a new version of a plug-in, double-click the Veeam Backup & Replication icon in the system tray. Veeam Backup & Replication will open the Veeam Download page where you can download the plug-in.

To install the plug-in, follow the steps described in the Installing Storage System Plug-Ins section.



Uninstalling Storage System Plug-Ins

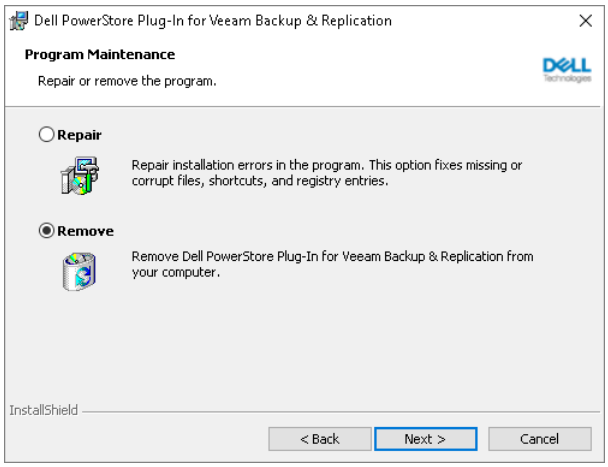
Before you uninstall a Universal Storage API integrated system plug-in, you need to remove from the backup infrastructure the storage systems for which the plug-in was installed. For more information on how to remove storage systems, see Removing Storage Systems.

If you do not remove the storage systems beforehand, all information connected to them will still be present in the Veeam Backup & Replication configuration database: you will see snapshots, jobs and so on. However, the storage systems themselves will not be visible in the UI, and you will not able to perform any operations with them. If you reinstall the plug-in, you will be able to perform the operations once again.

To uninstall a Universal Storage API integrated system plug-in:

1. Launch the plug-in installation EXE file.
2. In the wizard, proceed to the **Program Maintenance Mode** step.
3. Select **Remove.**
4. Proceed to the final step of the wizard and click **Remove**.

Alternatively, you can navigate to **Control Panel** > **Programs** > **Programs and Features**. In the list of installed programs, right-click the necessary plug-in and select **Uninstall**.



On-Demand Sandbox for Storage Snapshots

In On-Demand Sandbox, you can start VMs from snapshots existing on the production storage array. You can use On-Demand Sandbox to test VMs, troubleshoot issues, perform training and so on.

On-Demand Sandbox configuration where VMs from storage snapshots are started is similar to configuration of the regular On-Demand Sandbox. To start a VM from the storage snapshot in the isolated environment, you must configure the following objects:

- **Virtual lab**. The virtual lab must mirror the networking scheme of the production environment. You can configure a new virtual lab or use an existing virtual lab. Any type of the virtual lab configuration is supported: basic single-host, advanced single-host or advanced multi-host. For more information, see Veeam Backup & Replication User Guide for VMware vSphere.
- **Application group**. The application group must contain one or several VMs that you want to start in the On-Demand Sandbox. You can select VMs from volumes or LUNs on the storage system. During the SureBackup job, Veeam Backup & Replication will detect the latest snapshot for this volume or LUN and start the VM from this snapshot. For more information, see Veeam Backup & Replication User Guide for VMware vSphere.
- **SureBackup job**. You must link the application group with VMs and virtual lab to the SureBackup job. For more information, see Veeam Backup & Replication User Guide for VMware vSphere.

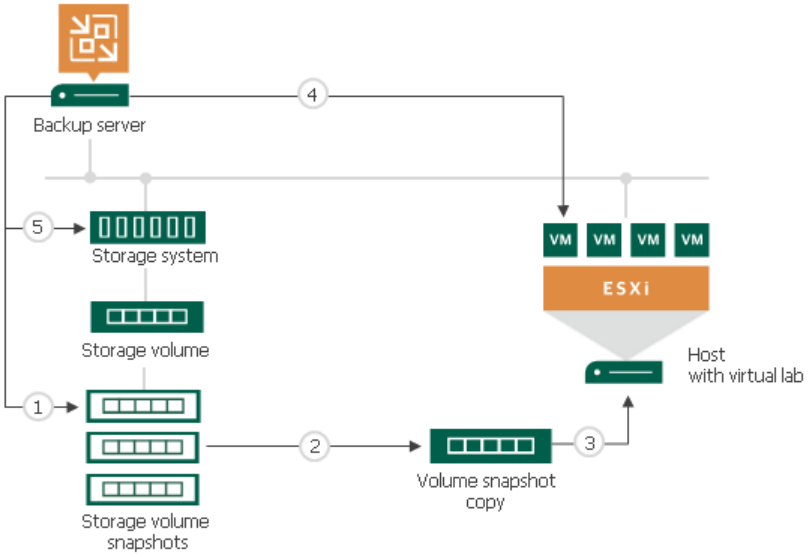
How On-Demand Sandbox for Storage Snapshots Works

To start a VM from a storage snapshot in On-Demand Sandbox, Veeam Backup & Replication needs to present this storage snapshot to an ESXi host as a datastore. To do this, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication detects the latest storage snapshot for the VM whose disks are located on the storage system.
2. Veeam Backup & Replication triggers the storage system to create a copy of the storage snapshot. The snapshot copy helps protect the storage snapshot from changes.

   To create a snapshot copy, Veeam Backup & Replication uses the same technology as for Data Recovery from Storage Snapshots. For more information, see the Data Recovery from Storage Snapshots section in the Veeam Backup & Replication User Guide.
3. The snapshot copy is presented as a new datastore to the ESXi host on which the virtual lab is registered.
4. Veeam Backup & Replication performs regular operations required for On-Demand Sandbox: reconfigures the VMX file, starts the VM, performs necessary tests for it and so on.

5. After you finish working with VMs and power off On-Demand Sandbox, Veeam Backup & Replication performs cleanup operations: powers off the VM and the proxy appliance in the virtual lab, unmounts the datastore from the ESXi host and triggers the storage system to remove the snapshot copy.



Number of Mounted NFS Datastores

You can add to the application group several VMs that reside on different storage snapshots. In this case, Veeam Backup & Replication will trigger several snapshot copies (one per each storage snapshot) and present the equal number of datastores to the ESXi host.

The number of NFS datastores that can be mounted to the ESXi host is limited by VMware vSphere. If number of snapshot copies is great, Veeam Backup & Replication may fail to present all of them as datastores to the ESXi host. In this case, VMs in the application group will not be started and the SureBackup job will fail. For more information about limitations, see this VMware KB article.

To overcome this situation, Veeam Backup & Replication offers the mechanism of the snapshot copy re-mounting:

1. If Veeam Backup & Replication detects that there are not enough resources to mount a datastore, it displays a warning and offers you to free up resources on the ESXi host.
2. During the next 20 minutes, Veeam Backup & Replication attempts to mount the datastore with the time interval of 2 minutes.
3. If resources are freed and Veeam Backup & Replication manages to mount the datastore, VMs in the application group are started and the SureBackup job continues to run. If resources on the ESXi hosts are not freed within 20 minutes, the SureBackup job fails.

Limitations for On-Demand Sandbox for Storage Snapshots

Before you start using On-Demand Sandbox for storage snapshots, check limitations for Data Recovery from Storage Snapshots. For more information, see the General Limitations section in the Veeam Backup & Replication User Guide.