



Veeam Backup Free Edition

Version 9.0

User Guide

January, 2016

© 2015 Veeam Software.

All rights reserved. All trademarks are the property of their respective owners.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means, without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright, or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Important! Please read the End User Software License Agreement before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

CONTENTS

CONTENTS	3
CONTACTING VEEAM SOFTWARE	5
ABOUT THIS GUIDE	6
INTRODUCTION	7
VEEAMZIP	8
Backup Infrastructure	9
VeeamZIP Options	10
DATA RECOVERY	12
FILE COPY	13
VM MIGRATION	14
VEEAM EXPLORER FOR STORAGE SNAPSHOTS	15
VCLLOUD DIRECTOR SUPPORT	16
VeeamZIP for vCloud Director VMs	17
Restore of vCloud Director VMs	19
TAPE DEVICE SUPPORT	22
Supported Devices	23
Tape Device Deployment	24
Tape Environment	26
Media Pools	28
Tape Protection	31
Data Retention	32
Tape Parallel Processing	33
File to Tape Jobs	34
VM Restore	35
File Restore	36
ADMINISTRATION	37
SWITCHING BETWEEN MODES	38
LOGGING ON TO VEEAM BACKUP FREE EDITION	39
SETTING UP THE BACKUP INFRASTRUCTURE	40
Managing Credentials	41
Managing Passwords for Data Encryption	46
Adding VMware vSphere Servers	50
Adding Microsoft Hyper-V Servers	56
Adding Microsoft Windows Servers	68
Adding Linux Servers	75
Adding Microsoft SMB3 Servers	81
Adding vCloud Director	91
Managing Servers	96
CREATING VEEAMZIP FILES	98
Creating VeeamZIP Files for VMware VMs	99
Creating VeeamZIP Files for Hyper-V VMs	101
PERFORMING RESTORE	103
Performing Restore in VMware vSphere Environment	104

Performing Restore in Microsoft Hyper-V Environment	138
PERFORMING FILE COPY	168
Copying Files and Folders Manually	169
Creating File Copy Jobs	170
Managing Folders.....	176
Editing and Deleting Files.....	177
PERFORMING QUICK MIGRATION	178
WORKING WITH STORAGE SNAPSHOTS	184
Setting Up Backup Infrastructure for Work with Storage System	185
Working with Veeam Explorer for Storage Snapshots.....	204
WORKING WITH TAPE MEDIA	253
Getting Started with Tapes.....	254
Deploying Tape Devices.....	255
Working with Media Pools.....	266
Working with Tape Libraries	274
Working with Tapes.....	276
Creating File to Tape Jobs.....	287
Restoring Backups from Tape	296
Restoring Files from Tape.....	299
Restoring Encrypted Data from Tapes	303
WORKING WITH vCLOUD DIRECTOR VMs.....	306
Viewing vCloud Director VMs	307
Creating VeeamZIP Files for vCD VMs	308
Performing Restore from vCD Backups.....	309
PERFORMING CONFIGURATION BACKUP AND RESTORE	317
Creating Configuration Backups.....	318
Restoring Configuration Data.....	322
SPECIFYING VEEAM BACKUP & REPLICATION OPTIONS	334
Specifying Session History Settings	335
Specifying Data Processing Settings.....	336
VIEWING REALTIME STATISTICS	337
ASSIGNING ROLES TO USERS	338

CONTACTING VEEAM SOFTWARE

At Veeam Software we value the 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, please visit our Customer Center Portal at www.veeam.com/support.html 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 offices location, please visit www.veeam.com/contacts.html.

Online Support

If you have any questions about Veeam Backup Free Edition, you can use the following resources:

- Full documentation set: <https://www.veeam.com/documentation-guides-datasheets.html>
- Community forum at forums.veeam.com

ABOUT THIS GUIDE

This user guide provides information about main features of Veeam Backup Free Edition. The document applies to version 9.0 and all subsequent versions until it is replaced with a new edition.

Intended Audience

The user guide is intended for anyone who wants to use Veeam Backup & Replication. It is primarily aimed at virtual environment administrators, consultants, analysts and any other IT professionals using the product.

Document Revision History

Revision #	Date	Change Summary
Revision 1	1/12/2016	Initial version of the document for the Veeam Backup & Replication 9.0.

INTRODUCTION

Veeam® Backup & Replication™ is a data protection and disaster recovery solution for VMware vSphere and Hyper-V virtual environments of any size and complexity. Combining all of the necessary functions in one intuitive interface, Veeam Backup & Replication serves to solve the most critical problems of virtualized infrastructure management and protect mission-critical VMs from hardware and software failures.

Veeam Backup & Replication can operate in two functionality modes: **full mode** and **free mode**.

- When you run Veeam Backup & Replication in the full functionality mode, you get a commercial version of the product that provides access to all Veeam Backup & Replication functionality.
- When you run Veeam Backup & Replication in the free functionality mode, you get a free version of the product — Veeam Backup Free Edition that provides limited capabilities. You can back up single VMs (create VeeamZIP™ files), recover VM data from VeeamZIP files, backups storage snapshots, perform file copy operations, migrate VMs and work with tape media.

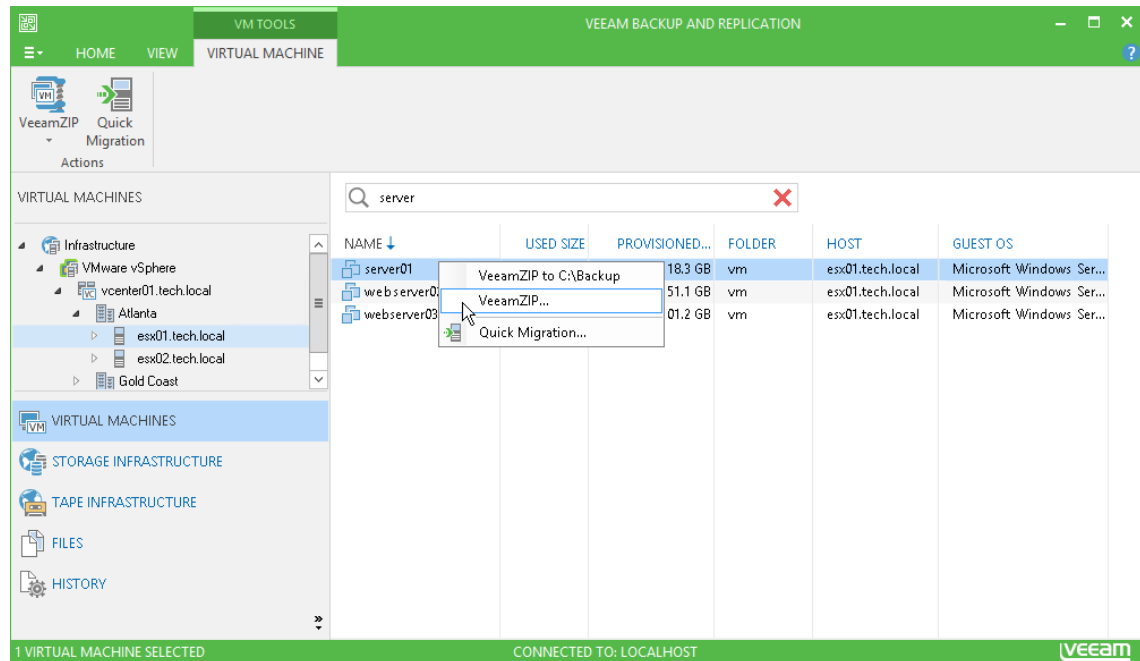
This help describes the capabilities of Veeam Backup Free Edition. To learn about the capabilities provided by Veeam Backup & Replication, do one of the following:

- **Switch to the full functionality mode** and press **[F1]** on the keyboard or select **Help > Help** from the main menu.
- Access Veeam's documentation on the website: <https://www.veeam.com/documentation-guides-datasheets.html>

VeeamZIP

With Veeam Backup Free Edition, you can create VeeamZIP files for VMware vSphere and Hyper-V VMs.

VeeamZIP is similar to full VM backup. When you create a VeeamZIP file, Veeam Backup Free Edition copies VM data, compresses it and stores it to a full backup file (VBK) that acts as an independent restore point. You can store a created VeeamZIP file to a folder on the local host or to a network share.



In Veeam Backup Free Edition, you can run the VeeamZIP job only for one VM. If you need to process several VMs, you can start a number of VeeamZIP jobs simultaneously.

VeeamZIP jobs can only be run manually: you cannot schedule them or save and run them later. Similar to backup jobs in Veeam Backup & Replication, VeeamZIP jobs are run in the background. Even if you close the Veeam Backup Free Edition console, the process will still continue to operate.

In Veeam Backup Free Edition, VeeamZIP jobs are not registered in the Veeam Backup & Replication database and are not available in the list of backups. Backups created in Veeam Backup & Replication are not available in the list of backups, too. To restore data from backups and VeeamZIP files, you will need to import them when working with the **Restore** wizard.

Important!

If you plan to create VeeamZIP files for VMs that run Microsoft Windows Server 2012 R2 and reside on a volume with Data Deduplication enabled, it is recommended to deploy Veeam Backup Free Edition on a machine running Windows Server 2012 R2. Otherwise, certain types of restore operations for these VMs such as Windows File Level Recovery may fail.

Backup Infrastructure

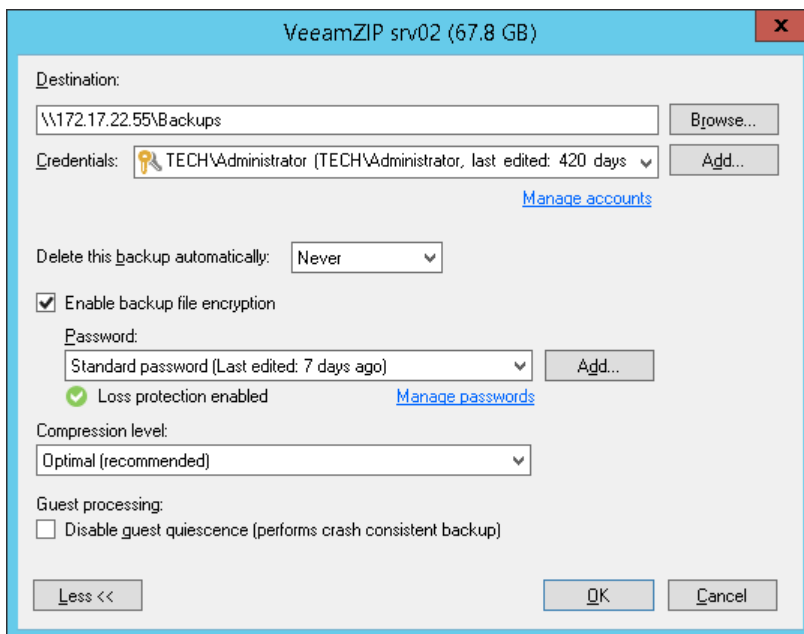
In Veeam Backup Free Edition, you cannot configure backup proxies and backup repositories and point a VeeamZIP job to them.

- In the VMware vSphere environment, VM data is retrieved from the source ESX(i) host and processed on the Veeam backup server that performs the role of the default backup proxy. Therefore, the backup traffic goes from the source host to the backup destination through the Veeam backup server.
- In the Hyper-V environment, VM data is processed on the source Hyper-V host that performs the role of the default backup proxy. The backup traffic goes from the source Hyper-V host to the backup destination, bypassing the Veeam backup server. The Veeam backup server controls the job performance.

VeeamZIP Options

Veeam Backup Free Edition offers the following advanced options for VeeamZIP files creation:

- Data encryption
- Retention settings
- Data compression
- VM guest OS quiescence



Data Encryption

You can encrypt VeeamZIP files to protect your information from unauthorized access. To create an encrypted VeeamZIP file, you must enable the encryption option and specify a password in VeeamZIP task options.

The VeeamZIP creation process with encryption enabled includes the following steps:

1. You enable encryption for a VeeamZIP task and specify a password.
2. Based on this password, Veeam Backup Free Edition generates the necessary key to protect VM data.
3. Veeam Backup Free Edition encrypts data blocks on the Veeam backup server side and transfers them to the destination storage.
4. On the target storage, encrypted data blocks are stored to a resulting VeeamZIP file.

Restore of an encrypted VeeamZIP file includes the following steps:

1. You import a VeeamZIP file and define a password to decrypt the file.
2. Veeam Backup Free Edition uses the provided password to generate the key and unlock the VeeamZIP file.
3. Veeam Backup Free Edition retrieves data blocks from the VeeamZIP file, sends them to the source side and decrypts them on the Veeam backup server.

Retention Settings

You can specify retention settings for the created VeeamZIP file: define if the file must remain on the target storage or must be deleted with time.

Veeam Backup Free Edition offers the following retention settings for VeeamZIP files:

- VeeamZIP files are never deleted.
- VeeamZIP files are automatically deleted after some period of time: on the same night, the next night, in 3 days, in a week and so on.

Data compression

In Veeam Backup Free Edition, you can select one of the following compression levels:

- **None** compression level is recommended if you use storage devices with hardware compression and deduplication tools to store created VeeamZIP files.
- **Dedupe-friendly** is an optimized compression level for very low CPU usage. It is recommended if you want to decrease the load on the Veeam backup server (for VMware environments) and source Hyper-V host (for Hyper-V environments).
- **Optimal** (default setting) is the recommended compression level providing the best ratio between the size of the VeeamZIP file and time of its creation.
- **High** compression level provides additional 10% compression ratio over **Optimal**, but at the cost of about 8x CPU usage.
- **Extreme** compression provides the smallest size of the VeeamZIP file but reduces the VeeamZIP job performance. We recommend that you run backup proxies on computers with modern multi-core CPUs (6 cores recommended) if you intend to use the extreme compression.

VM Guest OS Quiescence

Veeam Backup Free Edition uses VMware Tools quiescence for VMware VMs and native Hyper-V quiescing mechanisms for Hyper-V VMs to capture VM data. Veeam Backup Free Edition quiesces, or freezes, a running VM to bring its file system and application data to a consistent state suitable for backup. Restoring a transactionally consistent VeeamZIP file ensures successful recovery of VM applications without any data loss.

By default, VM guest OS quiescence is enabled. You can disable it if necessary: for example, if you create VeeamZIP files for VMware VMs without VMware Tools installed or Hyper-V VMs running applications without VSS support.

Note: During VM data processing, Veeam Backup Free Edition checks the NTFS MFT file on Windows-based VMs to identify blocks of the Windows pagefile and excludes these blocks from processing. Windows pagefiles are dynamic in nature and change intensively, even if VMs do not change much. Pagefile exclusion results in increased VM data processing performance.

Data Recovery

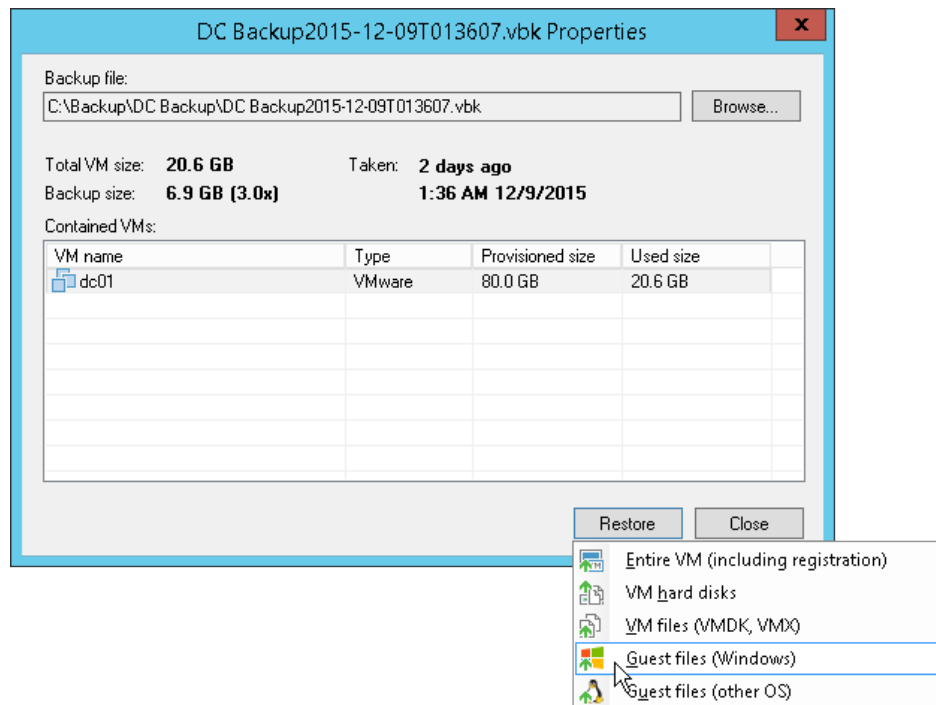
Veeam Backup Free Edition offers a variety of restore options:

- From VeeamZIP files created for VMware VMs, you can restore an entire VM, VM guest OS files, VM hard disks and VM files (VMDK, VMX and so on).
- From VeeamZIP files created for Hyper-V VMs, you can restore an entire VM, VM guest OS files and VM files (VHD, VHDX, XML and so on).

To restore VM data, you can use a VeeamZIP file created in Veeam Backup Free Edition or any backup file or VeeamZIP file created in Veeam Backup & Replication.

Veeam Backup Free Edition does not support batch restore for full VM recovery: at a time, you can perform restore of a single VM only. That is, if you create a backup file for a number of VMs in Veeam Backup & Replication and use this file for restore in Veeam Backup Free Edition, you will need to select only one VM.

Note: Instant VM Recovery capabilities are not available in Veeam Backup Free Edition.



File Copy

As well as in Veeam Backup & Replication, in Veeam Backup Free Edition you can perform file copy operations.

File copying is the most natural way to deliver an ISO file to an ESX(i) or Hyper-V host and exchange VMs, VM templates and files between ESX(i), Hyper-V, Windows and Linux hosts.

Veeam Backup Free Edition ensures security and works over 6 times faster than SCP.

New File Copy Job

Source

Select items to be copied with this job.

Name

Source

Destination

Schedule

Summary

Server:

fileserver01.tech.local

Items to copy:

Item	Host
C:\Backup	srv02.tech.local
C:\Backup	fileserver01.tech.local

Add...

Remove

< Previous

Next >

Finish

Cancel

VM Migration

Veeam Quick Migration enables you to promptly migrate one or more VMs between ESX(i) hosts, datastores or both. Veeam Backup Free Edition allows migration of VMs in any state with minimal disruption to business operations and end user access to services.

Note: Quick Migration functionality is available only for VMware VMs.

When you migrate a VM, Veeam Backup Free Edition analyzes your virtual infrastructure, its configuration and the state of VMs and selects the most appropriate relocation method. Whenever possible, Veeam Backup Free Edition coordinates its operations with vCenter and uses native VMware vCenter migration mechanisms: vMotion and Storage vMotion. When VMware vCenter migration methods cannot be used (for example, your VMware vSphere license does not provide support for vMotion and Storage vMotion, or you need to migrate VMs from one standalone ESX(i) host to another), Veeam Backup Free Edition employs its proprietary SmartSwitch technology to relocate VMs.

Veeam Quick Migration provides means for fast background migration of VMs ensuring continuous uptime of your virtual environment. Quick Migration supports hot VM migration with SmartSwitch and cold VM migration with cold switch.

Migration of a VM is performed in several stages.

1. Veeam Backup Free Edition copies the VM configuration file (VMX) to the target host and registers the VM on that host.
2. Veeam Backup Free Edition triggers a VM snapshot and copies VM disk content to the new destination.
3. Veeam Backup Free Edition moves to the new location the VM state and changes that were made after the snapshot creation. Veeam Backup Free Edition uses different approaches to move the VM state between hosts with compatible and non-compatible CPUs:
 - If you move a VM between two hosts with compatible CPUs, Veeam Backup Free Edition uses SmartSwitch: it suspends a VM to move its state file and changes made after the snapshot creation. The VM is then resumed on the new host. This mechanism ensures minimum downtime and completely eliminates data loss during migration.
 - If you move a VM between two hosts with non-compatible CPUs, Veeam Backup Free Edition stops the VM to move changes made after the snapshot creation and then starts the VM on the new host.

Veeam Explorer for 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 really fast. Administrators can take snapshots several times a day or even schedule them as often as every hour.

However, in the virtual environment storage snapshots add more difficulty to the restore process. Storage snapshots are created per volume. A volume typically holds disks of multiple VMs. For this reason, restore from storage snapshots is not a simple rollback operation: it is a multi-task process. To restore a VM from the storage snapshot manually, you typically need to perform the following actions:

1. Present the storage snapshot to an ESX(i) host.
2. Perform an HBA rescan.
3. Mount the storage snapshot to the ESX(i) host.
4. Browse the storage snapshot to locate the VM files (VMDK).
5. Add the VM to the inventory or copy the VM files to another VMFS datastore.
6. Power on the VM.
7. Perform cleanup operations after recovery is completed.

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

To make VM recovery from storage snapshots fast and easy, Veeam Backup Free Edition offers Veeam Explorer™ for Storage Snapshots. Veeam Explorer for Storage Snapshots is a new technology in Veeam Backup Free Edition that lets you restore VMware VM data directly from storage snapshots on EMC VNX(e), HP 3PAR StoreServ, HP StoreVirtual and NetApp. Veeam Explorer for Storage Snapshots has been designed and developed in collaboration with HP and NetApp and uses native means of these storage systems for restore.

Veeam Explorer™ for Storage Snapshots offers a variety of restore options:

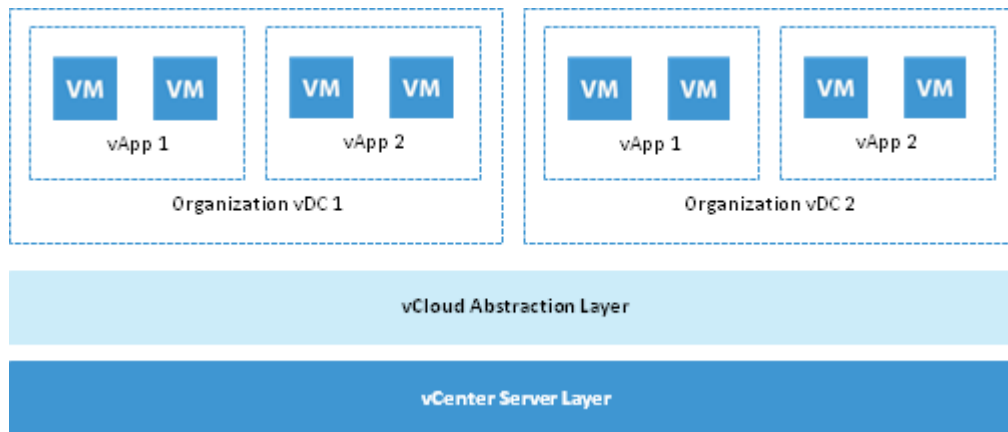
- You can restore an entire VM.
- You can restore VM guest OS files (Microsoft Windows, Linux, FreeBSD and other).
- You can restore Microsoft Active Directory objects from virtualized Microsoft Active Directory servers.
- You can restore Microsoft Exchange objects from virtualized Microsoft Exchange servers.
- You can restore Microsoft SharePoint objects from virtualized Microsoft SharePoint servers.
- You can restore Microsoft SQL Server databases from virtualized Microsoft SQL Servers.
- You can restore Oracle database from virtualized Oracle servers.

vCloud Director Support

Backup and restore of vCloud Director vApps and VMs has always been a hot topic. Up to now backup tools offered no option of backup in the vCloud Director environment. The only way was to perform backup at the level of the underlying vCenter Server. For restore, the administrators would first need to restore VMs to the vCenter Server level and then bring them to vCloud Director through import.

Veeam Backup Free Edition provides support for vCloud Director. It uses vCloud Director API to help you create VeeamZIP files for separate VMs and restore VMs directly to the vCloud Director hierarchy.

When Veeam Backup Free Edition creates VeeamZIP files for VMs, it captures not only data of VMs being a part of vApps, but also vApp metadata. As a result, you can restore vCloud Director VMs back to the vCloud Director hierarchy and do not need to perform any additional actions on import and VM configuration.



VeeamZIP for vCloud Director VMs

Veeam Backup Free Edition lets you create VeeamZIP files for separate vCloud Director VMs. When Veeam Backup Free Edition creates VeeamZIP files, it additionally captures vApp metadata. vApp metadata includes:

- General information about the vApp where VMs reside, such as: vApp name, description, VM descriptions
- Information about vApp networks and organization networks to which the vApp is connected
- VMs startup options
- User information
- Lease
- Quota
- Storage template and so on

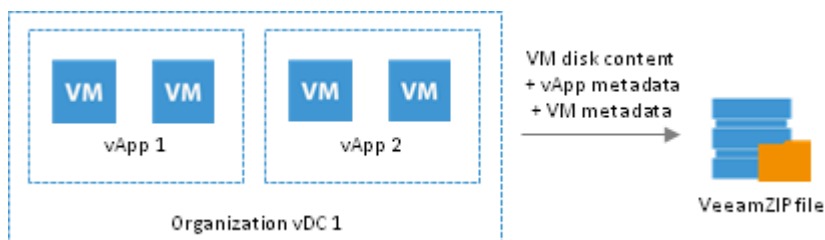
vApp metadata is stored together with the VM content in the VeeamZIP file. Capturing vApp metadata is extremely important for restore: without it, you will not be able to restore the VM back to vCloud Director.

With Veeam Backup Free Edition, you can create VeeamZIP files for **regular VMs** and **linked clone VMs**.

VeeamZIP for Regular VMs

When you create VeeamZIP files for regular VMs, Veeam Backup Free Edition captures and stores to the backup file the following data:

- VM disk content
- vApp metadata
- VM metadata

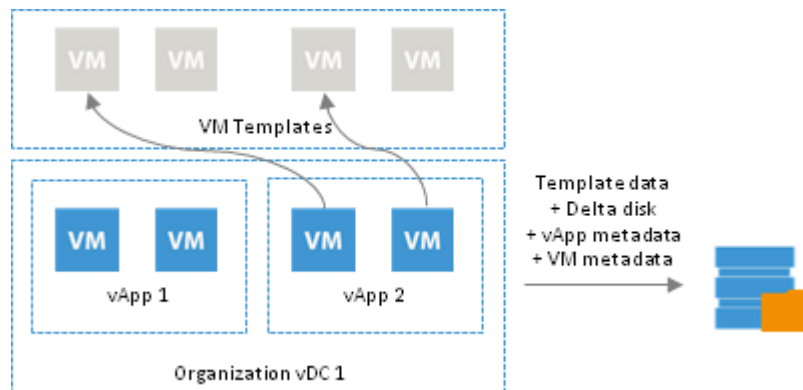


VeeamZIP for Linked Clone VMs

When you create VeeamZIP files for linked clone VMs, Veeam Backup Free Edition captures and stores to the VeeamZIP file the following data:

- Content of the template to which the VM is linked
- Content of the VM user disk — delta disk
- vApp metadata
- VM metadata

Veeam Backup Free Edition consolidates data of the VM template and delta disk and saves it as a regular VM disk in the VeeamZIP file. Data merging guarantees proper VM restore: even if a VM template is lost by the time of recovery, you will still be able to restore the linked clone VM from the VeeamZIP file.



Restore of vCloud Director VMs

Veeam Backup Free Edition enables full-fledged restore of VMs to vCloud Director. For restore, Veeam Backup Free Edition uses VM metadata saved to a VeeamZIP file and restores specific VM attributes. As a result, you get a fully-functioning VM in vCloud Director, do not need to import the restored VM to vCloud Director and adjust the VM settings manually.

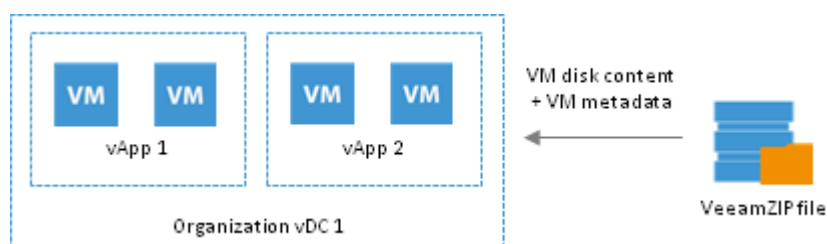
vCloud Director VMs can be restored to the same vCloud Director hierarchy or to a different vCloud Director environment. Restore options include:

- Full restore for vApps and VMs
- Restore of VM disks
- Restore of VM files
- Guest OS file-level restore

Restore of Regular VMs to vCloud Director

If you restore a regular VM back to the vCloud Director hierarchy, the restore process includes the following steps:

1. Veeam Backup Free Edition uses the captured vApp metadata to define the vApp settings and VM initial location in the vCloud Director hierarchy.
2. Veeam Backup & Replication restores the VM from the VeeamZIP file to its initial location or to other location. Additionally, Veeam Backup Free Edition restores all VM settings.



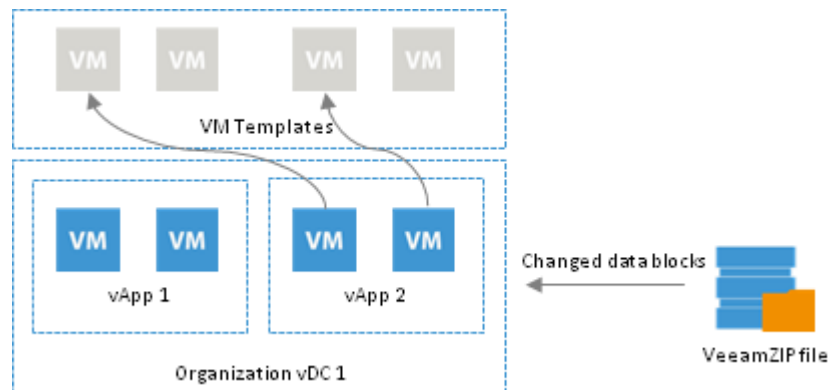
Restore of Linked Clone VMs to vCloud Director

Veeam Backup Free Edition lets you restore linked clone VMs – VMs that were deployed from a VM template using the fast provisioning technology. There are several mechanisms for processing linked clone VMs.

Restore of Existing VMs

If you are restoring a vCD linked clone VM that exists in the vCloud Director hierarchy, the restore process includes the following steps:

1. Veeam Backup Free Edition uses the captured vApp metadata to define the initial settings of the VM.
2. Veeam Backup Free Edition calculates a signature for the consolidated VM disk in the VeeamZIP file (containing the VM template data and data of the delta file) and the signature for the VM existing in vCloud Director. Veeam Backup Free Edition then compares the disk signatures to define what data blocks have changed.
3. Veeam Backup Free Edition restores only changed data blocks from the VeeamZIP file and writes them to the user delta file.

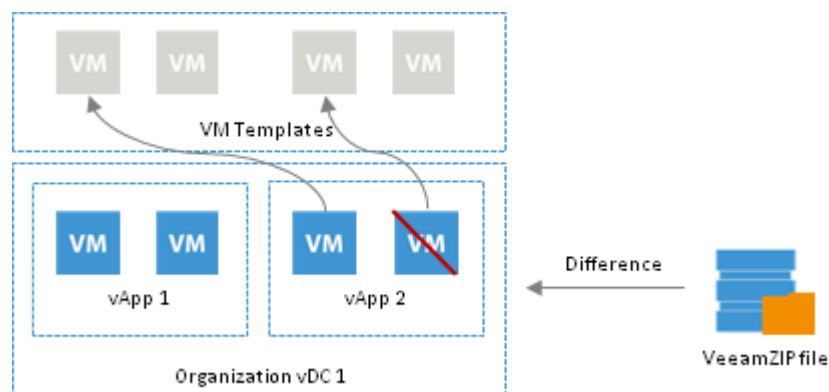


Restore of Deleted VMs

If you are restoring a VM that no longer exists in vCloud Director hierarchy, the restore process includes the following steps:

1. Veeam Backup Free Edition uses vCloud Director to create a new linked clone VM from the VM template that the user selects. The new VM has a blank user delta file.
2. Veeam Backup Free Edition calculates a signature for the consolidated VM disk in the VeeamZIP file (containing the VM template data and data of the delta file) and the signature for the created VM in vCloud Director. Veeam Backup Free Edition then compares the disk signatures to define what data blocks need to be restored.
3. Veeam Backup Free Edition restores only those data blocks that need to be restored from the VeeamZIP file and writes them to the blank user delta file.

By default, Veeam Backup Free Edition links the VM to the same VM template that was used by the initial VM. During restore, Veeam Backup Free Edition checks the settings of the VM template to which the restored VM is linked: verifies connection settings, makes sure the disk size coincide and so on.

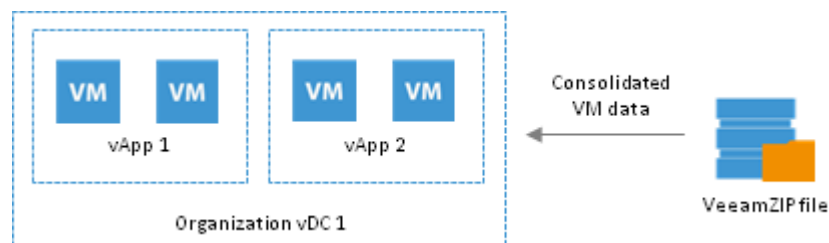


Restore of Linked Clone VMs as Regular VMs

In some cases, Veeam Backup Free Edition can restore a VM from a VeeamZIP file as a regular VM. This type of restore is accomplished in the following situations:

- You have intentionally chosen to restore a linked clone VM as a regular VM.
- You are restoring a VM to the Organization vDC which has the fast provisioning option disabled.
- A VM template to which the restored VM should be linked is not accessible in the location to which the VM is restored.

In this case, Veeam Backup Free Edition uses the same algorithm as for restore of full VMs in the virtual environment. It retrieves the data of the consolidated VM disk from the VeeamZIP file and restores the VM in the vCloud Director hierarchy.



Tape Device Support

Veeam provides native tape support that is fully integrated into Veeam Backup Free Edition. You can administrate all operations on tapes from your Veeam console.

Long-term archiving and compliance are listed as primary reasons for using tape. Tape appears to be one of the most widely used media for offsite backup. Using backup to tape, you can implement the '3-2-1' backup approach (3 copies, 2 types of media, 1 offsite location) considered as a best practice for data protection and disaster recovery. Veeam Backup Free Edition offers support for tape devices and allows you to archive your data to tape and restore it from tape whenever needed.

Storing data to tapes provides you with the same data managing options as disk repositories. In particular, you can store full and incremental backups, apply user-defined retention settings to the archived data, select restore points and so on. Compared to disk storage, tape archive requires more time to retrieve files for restore if the tapes are stored offsite.

Supported Devices

Veeam Backup Free Edition supports the following devices:

- Linear Tape-Open tape libraries starting from 3 generation (LTO3) or later.
- Physical libraries and standalone drives, virtual tape libraries.
- Partitions of the physical or virtual tape libraries presented to the Veeam backup server.

Note: If you plan to run both Veeam Backup Free Edition and 3rd party tape-recording software (for example, in your evaluation lab), consider that Veeam Backup Free Edition by default will periodically lock the drive to perform rescan, preventing other software from recording.

Industry Format

Veeam Backup Free Edition uses the MTF (Microsoft Tape Format) industry format to write data to tape.

Supported Connection Types

You can connect the tape device directly or remotely.

- Direct connection:
 - Fibre Channel (FC)
 - Serial Attached SCSI (SAS)
 - SCSI
- Remote connection:
 - iSCSI

Unknown Medium Changers

Veeam supports medium changers that have no Windows drivers available. Such devices must be connected over SCSI.

It is recommended that you use tape devices with original equipment manufacturer (OEM) drivers.

System Requirements and Limitation

Veeam Backup Free Edition has the following requirements and limitations to tape devices:

- If multiple driver installation modes are supported for your storage device, make sure the driver is installed in the mode that allows for multiple open handles from a host to a drive to exist at the same time.

Tape Device Deployment

Tape devices are connected to Veeam Backup Free Edition via a tape server. As a tape server, you can use any Microsoft Windows server managed by Veeam Backup Free Edition. In small installations, you can connect the tape device or devices to the Veeam backup server and assign the role of the tape server to it. The tape connected devices are recognized by the Veeam Backup Free Edition automatically.

Tape traffic loads the tape server a lot. Using the Veeam backup server as the tape server may be sufficient for small environments with low traffic workloads. However, if you plan to back up data to tape intensely, consider allocating a dedicated tape server to offload the Veeam backup server. You can also reconnect your tape device to a dedicated tape server. After the tape device is reconnected, the tape infrastructure appears in Veeam Backup Free Edition unchanged.

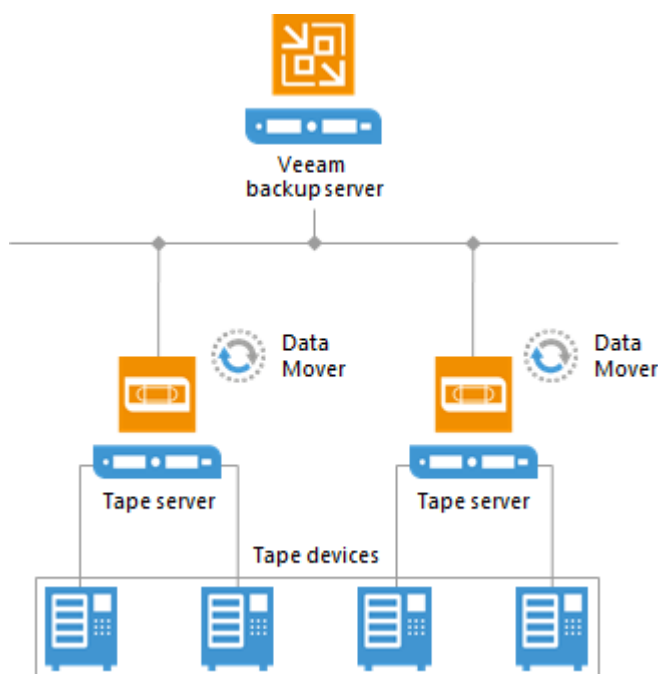
Using a separate tape server is useful in the following cases:

- To balance the traffic load in installations with intense data transferring,
- To configure remote data archiving: you can connect the tape devices to any tape server accessible by Veeam Backup Free Edition by network.
- To deploy a number of tape servers managed by one Veeam backup server.

With Veeam Backup Free Edition, the data transfer during archiving and restore processes is enabled with Veeam Data Mover services. The Data Movers run on tape servers and other components of backup infrastructure. They receive tasks from the Veeam backup server and communicate to each other to transfer the data.

The Data Movers are light-weight services that take a few seconds to deploy. Deployment is fully automated: when you assign a tape server role to a server, Veeam Backup Free Edition installs the necessary components on this server and starts the required services on it.

You can connect the tape device to the tape device directly over Fibre Channel (FC), Serial Attached SCSI (SAS), SCSI or remotely with iSCSI (you can use Microsoft iSCSI initiator to establish the connection).



Veeam Backup Free Edition allows deploying a number of tape servers. You can connect one or several tape devices to one tape server. However, you cannot connect one tape server to several Veeam backup servers simultaneously.

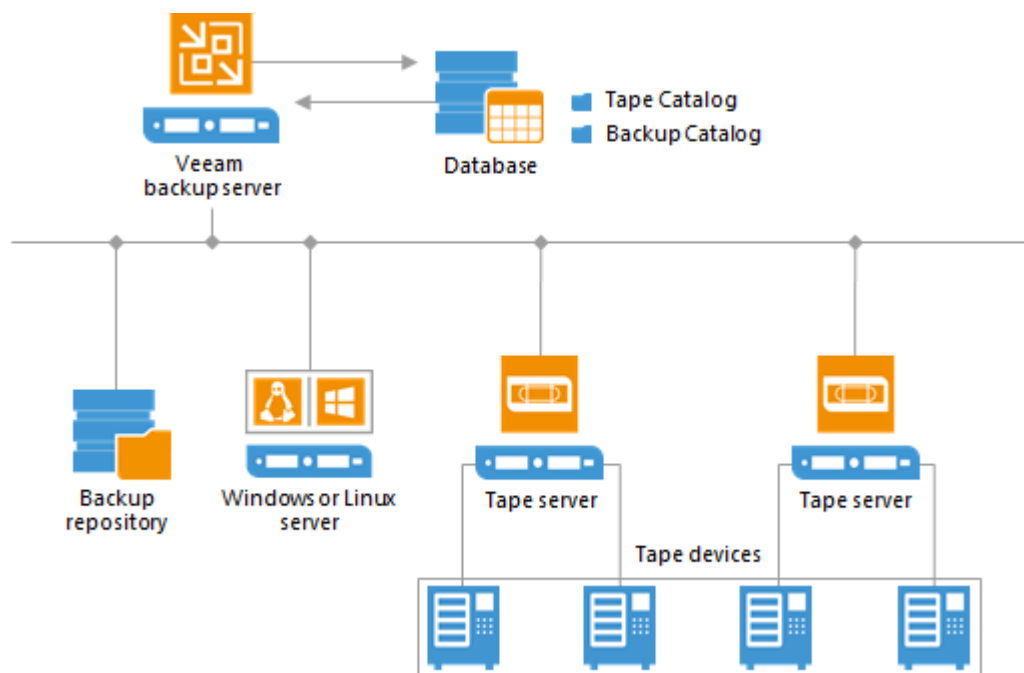
Tip: You can easily reconnect a tape server to another Veeam backup server without reconfiguring the tape device. Veeam backup server will recognize the library settings automatically. After reconnecting the tape library, you must configure file to tape jobs anew or copy the Veeam Backup Free Edition database configuration file on the new Veeam backup server. For more information, see [Performing Configuration Backup and Restore](#).

Upgrading Existing Tape Installations

If you have used Veeam Backup Free Edition v7 to work with tape media, the Veeam Backup Free Edition database has information about previously connected tape devices. During upgrade, Veeam Backup Free Edition will automatically reconfigure the tape device connection and assign the role of the tape server to the Veeam backup server.

Tape Environment

To administrate tape backup and restore procedures, you must add the tape server to your Veeam Backup Free Edition console. Adding the tape server to the backup infrastructure makes possible to transfer data between disk storages and the tape archive.



The tape backup and restore process involves the following components:

Veeam Backup Server

The Veeam backup server is the server running Veeam Backup Free Edition. It is the core component in the backup infrastructure. The Veeam backup server tasks include the following operations:

- Recognizing all tape devices that are connected to it and is able to manage all drives, slots and tapes.
- Administering tape archiving: scheduling and triggering tape jobs and initiating restore tasks.
- Communicating with the Veeam backup database.

Tape Device

When connected to the Veeam backup server, tape devices provide reading and writing capabilities, while all administration is performed by the Veeam backup server. You can connect multiple tape devices.

Tape Servers

To connect to the tape devices, Veeam Backup Free Edition uses tape servers.

The tape server is a backup infrastructure component transferring data between data source and tape device. The tape server runs Veeam Data Mover service that creates a communication point over which the data between the tape device and backup repositories or file servers is transferred.

The tape server deployment is fully automated: to create a tape server, you must assign the tape server role to a necessary server in the backup infrastructure. You can create a dedicated tape server or assign the tape server role to the Veeam backup server.

Veeam Backup Database

Veeam Backup Free Edition catalogs information about all archived data and stores this information in the Veeam backup database.

The catalog lets quickly detect location of the required items on tape. The catalog correlates the archived files and their restore points to the names of the corresponding tapes, both online or offline, and the names of the media sets within which the data was written. When you start restore, Veeam Backup Free Edition prompts for the tapes you need to bring online. As a result, you can restore data from tape much quicker when necessary.

Veeam Backup Free Edition uses the Tape Catalog to store information about files/folders archived to tape media with file to tape jobs. The content of the Tape Catalog can be examined in the **Files** view.

Backup Repositories and File Servers

When retrieving data to back up, or restoring data to disk, Veeam Backup Free Edition can connect to any machine that has been added as a managed server to the Veeam Backup Free Edition console.

Storing devices include the following types:

- Windows server, including physical boxes
- Linux server, including physical boxes
- Deduplicating storage appliances
- NAS devices (by specifying the SMB path to the share).

Media Pools

Media pools are logical containers created in Veeam Backup Free Edition to organize and administrate tapes. Veeam Backup Free Edition works only with tapes that are placed to one of media pools. To do this, you need to run importing procedure against all new tapes. Importing registers tapes in the Veeam Backup database after which Veeam Backup Free Edition places tapes to one of the media pools. You can always view information about tapes in the media pools, both online and offline, and data written to them.

Custom Media Pools

Custom media pools are target destinations for tape jobs. They manage empty (or available for overwriting) tapes to allow the tape jobs write data. You can create as many custom media pools as you need. One media pool can be target for unlimited number of tape jobs.

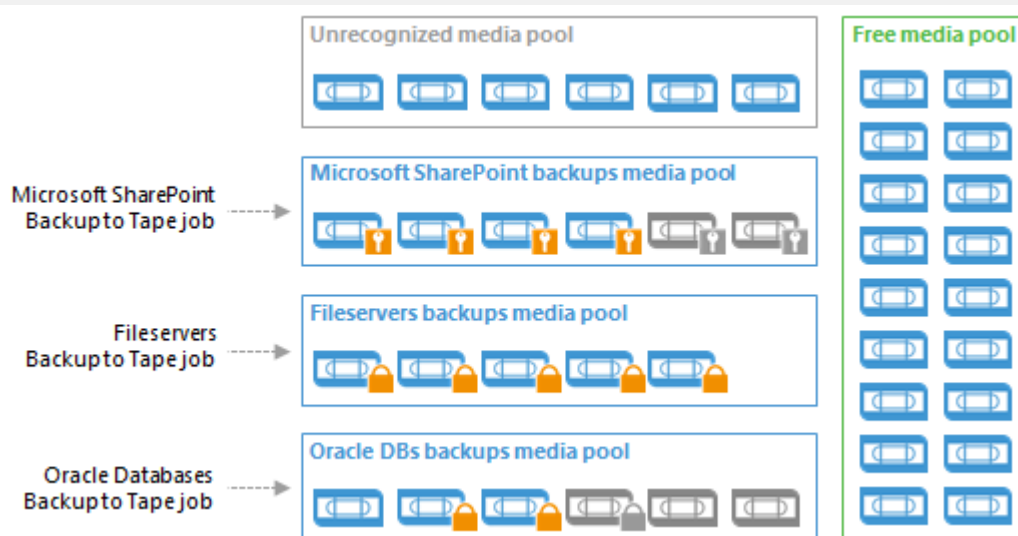
For each custom media pool, you can configure rules. Such rules are further applied to every tape that belongs to this media pool.

You can apply the following rules:

- Configure tape replenishment: you can allocate some particular tapes or let the media pool take a free tape when required.
- Create media sets: media sets allow you to create sets of tapes with data for a particular time period.
- Set the data retention period: this setting lets you choose the period for which the data on tapes will be protected from overwriting.
- Enable parallel processing: you can allow the media pool to use multiple tape drives simultaneously for writing data to tape. With parallel processing enabled, the media pool can process simultaneously several tape jobs.
- Encrypt the data written to tapes.

When a tape is allocated to a custom media pool, it gets a media pool tag written to its header. Such tape will always be tied to its media pool: when you bring a tape with expired data online, Veeam Backup Free Edition places it automatically to the media pool where the tape was written.

Note: You can manually move tapes to other media pools, however keep in mind that the tapes will be marked as free.



Service Media Pools

Service media pools are used to automatically sort tapes and manage their free capacity for writing data. Service media pools are automatically created by Veeam Backup Free Edition. The following predefined media pools are available:

- **Free** — a media pool containing empty tapes. You can use this media pool to replenish custom pools with new tapes when needed.
- **Unrecognized** — a media pool containing tapes that were loaded to tape device. They need further identification by user that can be done by running the inventory or catalog job.
- **Imported** — a media pool containing non-empty tapes. These include tapes identified by the tape catalog job.

This media pool can also contain tapes that were written in one tape library and then loaded to another tape library connected to the same Veeam backup server. If information about such tapes has not been removed from the tape catalog, these tapes will be available under the **Imported** media pool in the second tape library.

- **Retired** — a media pool containing retired tapes that reached the maximal number of re-writes. This media pool may also contain tapes with some mechanical breakdown.

You cannot create, modify or delete service media pools.

Media Sets

Media set is a set of tapes used for continuously writing backup data. Media set is one of parameters in media pool configuration.

A new media set always starts with a free tape. Within one media set, the new data block is appended to a previous one on a tape. Veeam Backup Free Edition stores information about all tapes that belong to each media set. You can view the list of names or barcodes of tapes that are associated with a particular media set.

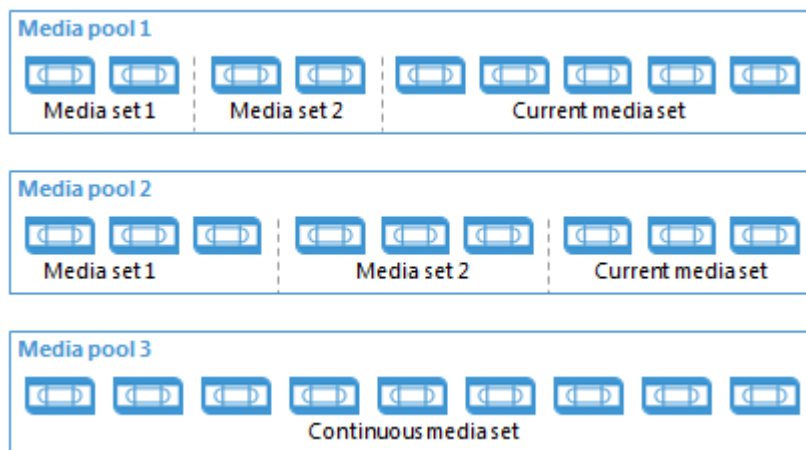
Media sets are used to explicitly distinguish data recorded to particular sets of tapes. You can choose between the following configuration options:

- **Creating a new media set for each backup session.** In this case, Veeam Backup Free Edition will produce a separate set of tapes for each tape backup session.
- **Starting a new media set for a certain period of time,** for example, each week. As a result, you will have a separate set of tapes containing all backups that have been written to tape during a week.
- **Always continuing one media set.** Use this option if you do not need to split your tape archives into separate sets of tapes.

When planning media sets configuration, you should balance between convenient viewing of data and efficiency of using the tapes. Media sets help create distinct packs of tapes, which will be convenient, for example, if you need to bring certain tapes from an offsite storage location to restore data. However, it may use the tapes ineffectively as the new media sets always require a new tape. This option is helpful when you have a lot of backups stored offsite.

Always continuing one media set option is most efficient in terms of tape capacity usage, for the new data would be written to the same tape until it is full. However, in this case the data will be split across tapes and you may require a larger number of tapes to get a particular backup set for restore. This option is usually used in environments where the tapes are not exported from libraries.

Veeam Backup Free Edition stores information about all tapes that belong to each media set. You can view the list of names or barcodes of tapes that are associated with a particular media set.



In some cases, Veeam forcibly starts a new media set, even if media pool settings do not instruct Veeam to do so. It happens when a job starts, but the tape that was planned for writing data cannot be used. In this situation, Veeam takes a new tape, and starts a new media set on it. For example, the situation may be as following:

1. The required tape is offline.
If you bring such tape online before the tape job starts, it will be used as planned.
2. The required tape is hardware or software protected.
3. In library failover on the following events: library is offline and all drives are busy. When a tape library is failed over on these events, Veeam starts a new media set even if the global media pools are configured to always continue one media set.

Note that if a new media set is started, both scheduled or forced, the previous media set cannot be resumed.

Backup Sets

When a tape job runs, it analyzes disk storage and spots files that match the tape job parameters. The tape job queues the files and writes them to tape. The set of files that are archived to tape within one tape job session is a backup set.

Depending on size and number of archived files, a backup set may require different amounts of tape space. For example, if the amount of data is large, it may take several tapes.



Tape Protection

Tape protection is an option that sets endless retention period for particular tapes selected by user. The protection option overrides retention settings of the media pool.

Generally, you use retention settings to set the overwrite protection period for tapes. The retention period is set for a media pool and is applied to all tapes that belong to this pool. However, some tapes may contain data for which you may want to set a longer protection, for example, the tapes that contain particularly valuable data. To do this, you can set tape protection without modifying the settings of the media pool which would affect other tapes.

You can set protection for any tape, online or offline, that contains data. If the offline tape is in a media vault, the media vault will inherit its retention setting automatically.



The protection can be switched off at any time. The retention period will change back to value set for the media pool.

When the tapes are protected, the following operations are prohibited for them:

- Erasing tapes
- Marking tapes as free
- Removing tapes from catalog

To perform these operations, you need to switch the protection off first.

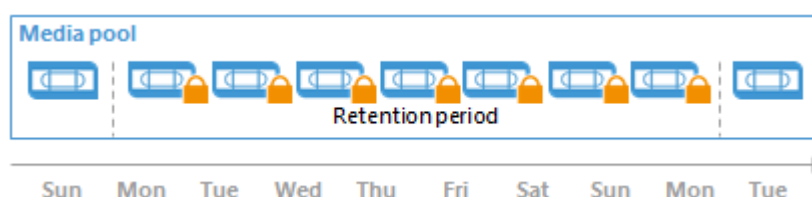
Data Retention

Data retention period is a period of time when data written to tapes is protected from overwriting.

Retention period is set by user for media pool and is applied to all tapes in this media pool. To set the retention policy, you can choose between the following options:

- Never overwrite data
- Define a particular time period to protect data
- Not to protect data at all.

When a tape is write-protected by a retention period setting, Veeam Backup Free Edition will not use this tape for any tape job until the retention period ends. If a tape contains several backup sets, it will expire when the backup set with the longest retention period expires.



You can change the retention at any time. When you change the retention policy, you can select if this modification works for tapes that will be written after you apply this change or also to tapes that are already recorded. In the latter case, the retention settings of the recorded tapes will change immediately and will be applied to tapes that are both online and offline.

Note: If you choose to set a shorter retention period and apply the retention settings to all tapes, some of your tapes may immediately become outdated. Such tapes will be queued for overwriting. Be careful when applying a new retention policy in order not to lose any data you need, or use the protection option. For more information, see [Tape Protection](#).

Managing Outdated Tapes

The tapes containing outdated data are handled in the following way:

- **If the expired tape is online**, it will be overwritten next time a tape job requires a free tape. The expired tape can be used only by the same media pool unless you erase the tape manually or move it to another media pool. The tapes are rewritten by the FIFO method.
- **If the expired tape is offline**, you can re-load it back to the library. Tapes that were written in particular media pool will be automatically placed to the same media pool unless you move the tape to another media pool or erase the tape manually.

Tape Parallel Processing

If your tape library has multiple drives, you can enable parallel processing for tape jobs. Parallel processing allows you to use several drives simultaneously for processing tape data. This option is useful if you have a lot of tape jobs running at the same time or you have a lot of data that must be written to tape in a limited backup window.

This option is enabled for custom media pools. You can limit the maximum number of drives that a specific media pool can use simultaneously.

File to Tape Jobs

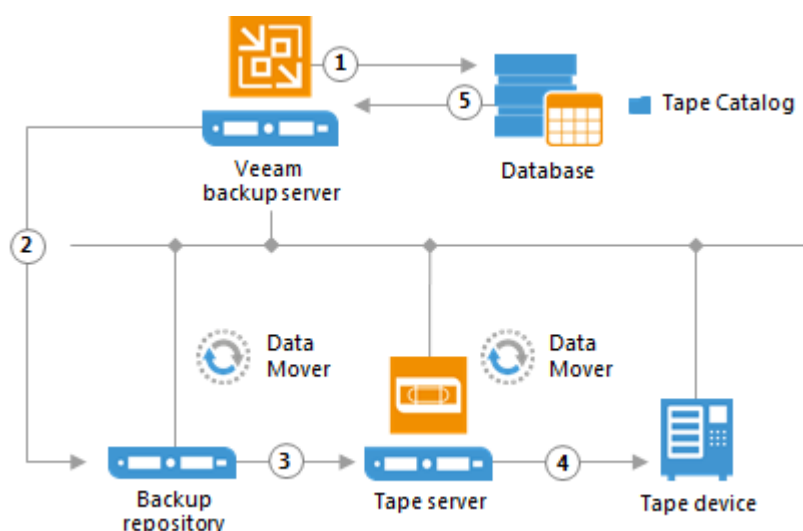
File to tape job allows you to back up to tape any Microsoft Windows or Linux files. You can also write to tape Veeam backups as files.

The file to tape job compares the source files to the files stored in tape archive and copies the changes to tape. You can create both full and incremental backups of files on tape. Veeam Backup Free Edition supports file backup from any server which has been added as a managed server to the Veeam Backup console (that is, Windows or Linux server, including physical boxes). You can also archive files residing on NAS devices.

How File to Tape Works

When Veeam Backup Free Edition executes a file to tape job (started manually or on schedule), it performs the following operations:

1. The file to tape job detects files that match the job criteria.
2. The files are queued for archiving. The following scenarios are used:
 - If it is a first job run or a scheduled full backup, all selected files are queued for archiving.
 - If it is an incremental backup run, Veeam Backup Free Edition addresses the Tape Catalog in the Veeam Backup Free Edition database to detect if any data has been modified since the latest backup. Detected changes are queued for archiving.
3. Veeam Backup Free Edition connects to the Data Movers and starts the data transfer process.
4. The source Data Mover retrieves data from the source servers and target Data Mover sends data to tape.
5. The tape job addresses the media pool that is set for this job as target. The media pool allots tapes for writing data according to the following configuration options:
 - Tapes consumption
 - Media sets
 - Tape retention
6. While tape recording is performed, Veeam Backup service updates data in the Tape Catalog in Veeam Backup database. The Veeam Backup console displays refreshed information about files archived to tape and shows job statistics.



VM Restore

You can restore VMs from backups created in the full version of Veeam Backup Free Edition. You can restore VM backups from tape to a disk repository. You need to choose a VM and a desired restore point. If the tapes are online in your tape device, Veeam Backup Free Edition will get the needed data automatically. If the tapes are offline, Veeam Backup Free Edition will list the names of the required tapes.

How Restoring VM from Tape Works

When Veeam Backup Free Edition restores a VM that is archived to tape, it performs the following operations:

1. Veeam Backup Free Edition checks the Backup Catalog in the Veeam Backup Free Edition database to discover the tapes containing the needed backup files. If the tapes are offline, Veeam Backup Free Edition prompts the user to insert the required tapes.
2. Veeam Backup Free Edition connects to the Data Mover service deployed on a tape server.
3. The Data Mover copies the relevant backup files from the tapes to a staging repository.
4. The VM is restored to disk by the regular VM restore procedure.
5. Veeam Backup Free Edition updates the Backup Catalog and Tape Catalog in the Veeam Backup database and deletes the backup files from the staging repository.

File Restore

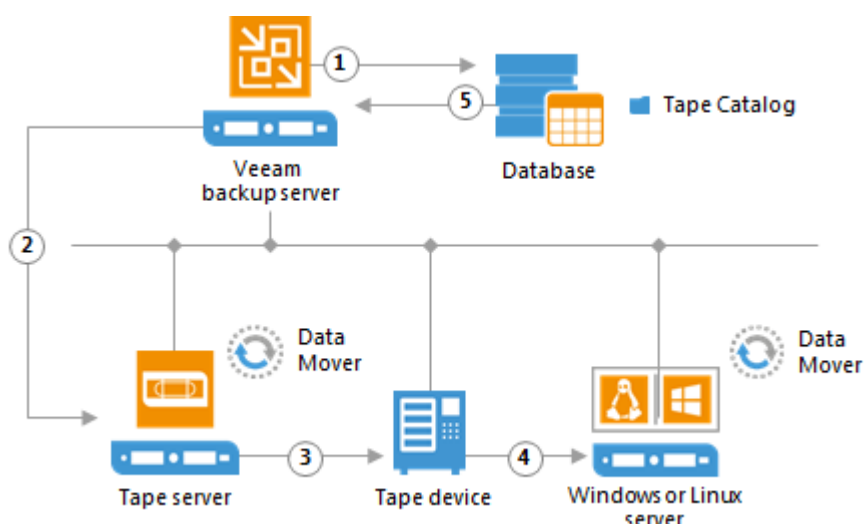
You can restore files and folders that were previously archived with file to tape jobs. Restoring capabilities allows you to restore files to their original location or another server, preserving ownership and access permissions. The file restore process allows you to restore files to any restore point available on tape. With Veeam Backup Free Edition, you can quickly search the catalog for files and folders stored on tape.

If the tapes are online in your tape device, Veeam Backup Free Edition will get the needed data automatically. If the tapes are offline, Veeam Backup Free Edition will list the names of the required tapes.

How Restoring Files from Tape Works

When Veeam Backup Free Edition restores files archived to tape, it performs the following operations:

1. Veeam Backup Free Edition checks the Tape Catalog in the Veeam Backup Free Edition database to discover the tapes containing the needed restore point of the files. If the tapes are offline, Veeam Backup Free Edition prompts the user to insert the required tapes.
2. Veeam Backup Free Edition connects to the Data Mover service deployed on a tape server.
3. The Data Mover copies the relevant files from the tapes to a chosen target location, same or new one.
4. Veeam Backup Free Edition updates the Tape Catalog in the Veeam Backup database.



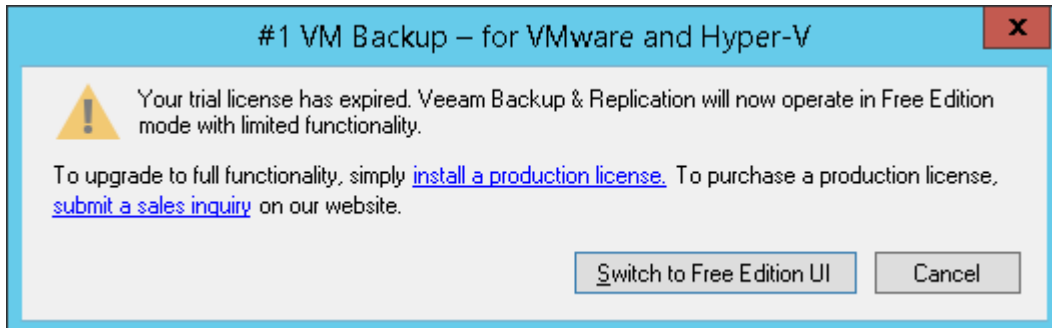
ADMINISTRATION

This section describes administrative tasks you can perform in Veeam Backup Free Edition, both for VMware and Microsoft Hyper-V virtual environments:

- [Switching Between Modes](#)
- [Logging On to Veeam Backup Free Edition](#)
- [Setting Up the Backup Infrastructure](#)
- [Creating VeeamZIP Files](#)
- [Performing Restore](#)
- [Performing File Copy](#)
- [Performing Quick Migration](#)
- [Working with Veeam Explorer for Storage Snapshots](#)
- [Working with vCloud Director VMs](#)
- [Working with Tape Media](#)
- [Performing Configuration Backup and Restore](#)
- [Specifying Veeam Backup & Replication Options](#)

Switching Between Modes

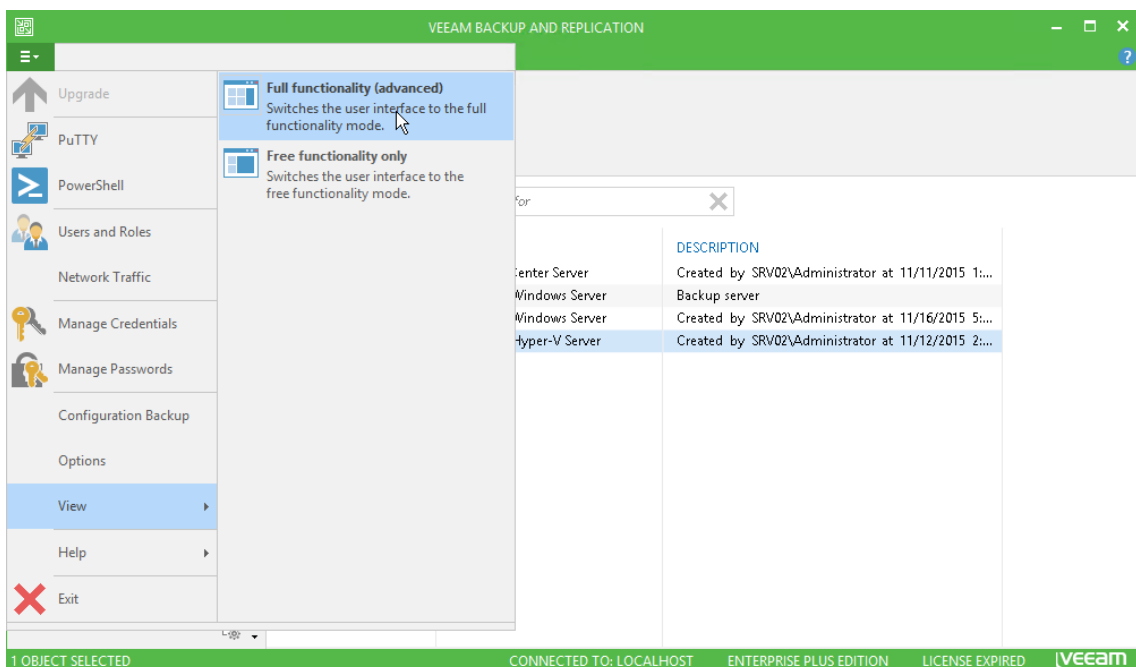
Veeam Backup & Replication operates in the full functionality mode if you have a valid license installed. You can use either a trial license or a purchased full license. When your license expires, you will see a notification that will prompt you to install a new license or switch to the free functionality mode.



To switch to the free functionality mode and use Veeam Backup Free Edition, click **Switch to Free Edition UI**. You can also switch to the free functionality mode if you select **View > Free functionality only** from the main menu.

To switch back to the full mode and enable full functionality of Veeam Backup & Replication, do either of the following:

- Install a valid license: select **Help > License** from the main menu. In the displayed window, click **Install License** and browse to the necessary license file.
- Select **View > Full functionality (advanced)** from the main menu. Note that if you do not have a valid license installed, you will not be able to use the functionality provided by the full mode.



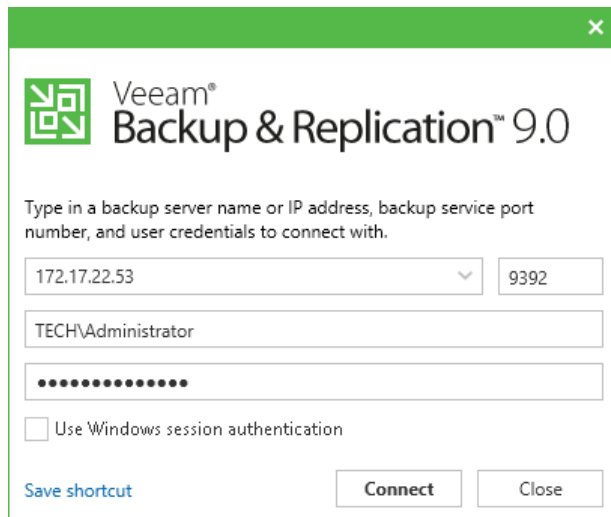
Logging On to Veeam Backup Free Edition

To log on to Veeam Backup Free Edition, you must open the Veeam Backup Free Edition console and specify connection settings to access the backup server.

1. To open the Veeam Backup Free Edition console, do one of the following:
 - Double-click the console icon on the desktop.
 - From the Microsoft Windows **Start** menu, select **All Programs > Veeam > Veeam Backup Free Edition Console**.
 - Use the Microsoft Windows search to find the **Veeam Backup Free Edition Console** program on the computer.
2. In the **Server** field, type the name or IP address of the backup server or select it from the list of recent connections. By default, the console connects to the backup server installed locally — localhost.
3. In the **Port** field, enter the port over which you want to connect to the backup server. The port number is set at the **Port Configuration** step of the setup wizard for Veeam Backup Free Edition. By default, port 9392 is used.
4. In the **Username** and **Password** fields, enter credentials of the user account that you want to use to connect to the backup server. The user account must be added to the Local Users group on the backup server or a group of domain users who have access to the backup server.

You can also select the **Use Windows session authentication** check box. In this case, you will log on to Veeam Backup Free Edition using the account under which you are currently logged on to Microsoft Windows.

5. To create a shortcut for the connection, click **Save shortcut**. You can create as many shortcuts as you need.



The screenshot shows the Veeam Backup & Replication 9.0 console login window. It has a green title bar with a close button. The window contains the Veeam logo and the text 'Veeam Backup & Replication 9.0'. Below this, it says 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' There are three input fields: a dropdown menu for the server name (showing '172.17.22.53'), a text box for the port number (showing '9392'), and a text box for the username (showing 'TECH\Administrator'). Below these is a password field with masked characters. There is a checkbox labeled 'Use Windows session authentication' which is currently unchecked. At the bottom, there are three buttons: 'Save shortcut' (in blue), 'Connect', and 'Close'.

Setting Up the Backup Infrastructure

Before creating VeeamZIP files and performing restore operations, you need to add virtual infrastructure servers to the backup infrastructure. Virtual infrastructure servers are ESX(i) and Hyper-V hosts on which the VMs for which you want to create VeeamZIP files reside. Additionally, you can connect Microsoft Windows and Linux servers that you plan to use as targets for file copy operations.

Note: An ESX Server is essentially a Linux server and a Microsoft Hyper-V Server is essentially a Microsoft Windows server. You can add ESX and Microsoft Hyper-V servers as virtualization servers and as standard file servers, depending on roles that you want to assign to them.

Managing Credentials

You can use the Credentials Manager to create and maintain a list of credentials records that you plan to use to connect to components in the backup infrastructure.

The Credentials Manager lets you create the following types of credentials records:

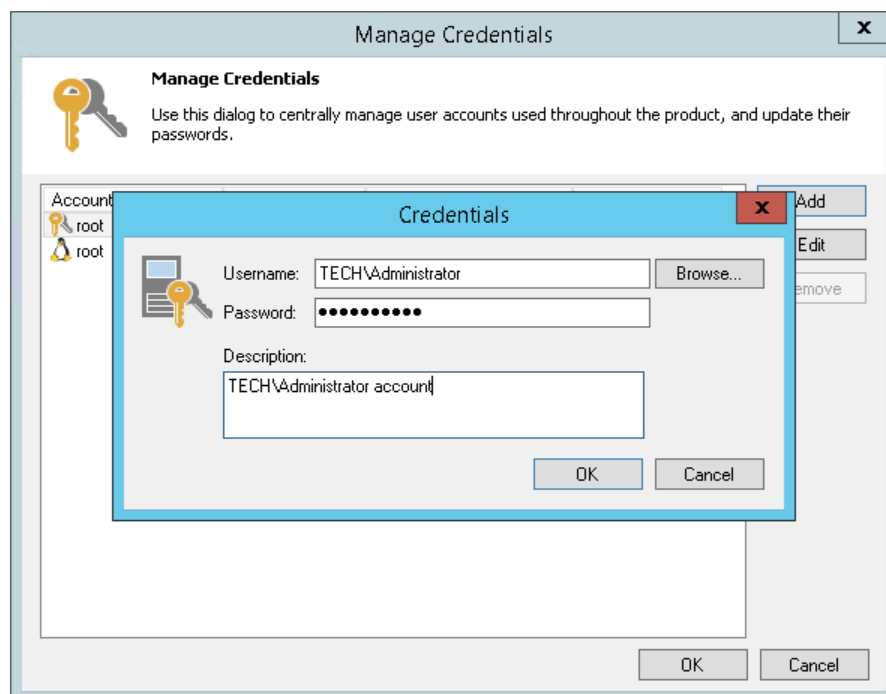
- Microsoft Windows credentials record
- Linux credentials record (user name and password)
- Linux credentials record (Identity/Pubkey)

Microsoft Windows Credentials Records

You can create a credentials record for the account that you plan to use to connect to a Microsoft Windows sever.

To create a new credentials record for a Microsoft Windows server:

1. From the main menu, select **Manage Credentials**.
2. Click **Add > Standard account**.
3. In the **Username** field, enter a user name for the account that you want to add. You can also click **Browse** to select an existing user account.
4. In the **Password** field, enter a password for the account that you want to add. To view the entered password, click and hold the eye icon on the right of the field.
5. In the **Description** field, enter a description for the created credentials record. As there can be a number of similar account names, for example, *Administrator*, it is recommended that you provide a meaningful unique description for the credentials record so that you can distinguish it in the list. The description is shown in brackets, following the user name.



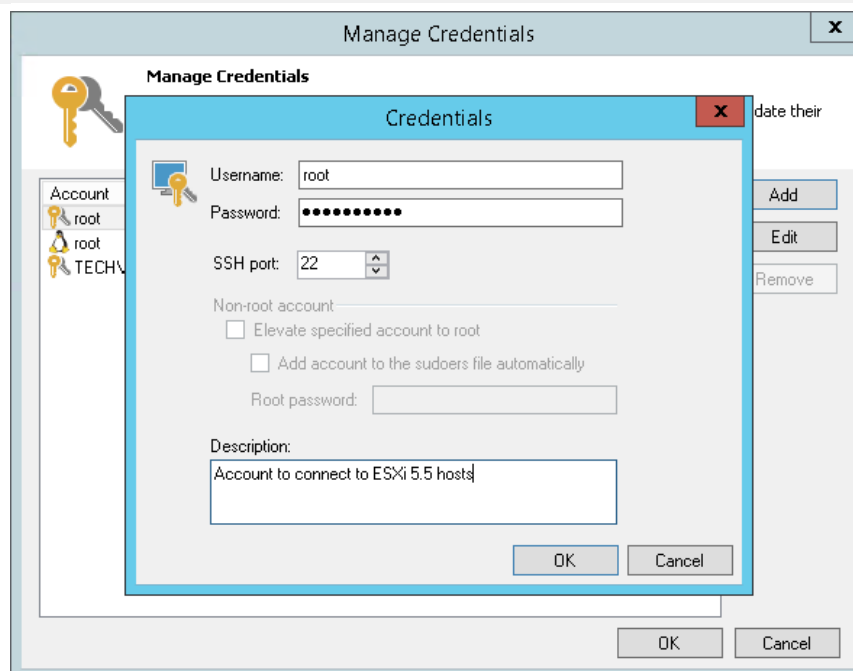
Linux Credentials Records (User Name and Password)

You can create a credentials record for the account that you plan to use to connect to a Linux sever .

To create a new credentials record with a user name and password for a Linux server:

1. From the main menu, select **Manage Credentials**.
2. Click **Add > Linux account**.
3. In the **Username** field, enter a user name for the account that you plan to add.
4. In the **Password** field, enter a password for the account that you want to add. To view the entered password, click and hold the eye icon on the right of the field.
5. In the **SSH port** field, specify the SSH port over which you want to connect to a Linux server. By default, port 22 is used.
6. If you specify data for a non-root account that does not have root permissions on a Linux server, you can use the **Non-root account** section to grant sudo rights to this account.
 - a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
 - b. To add the user account to sudoers file, select the **Add account to the sudoers file automatically** check box. If you do not enable this option, you will have to manually add the user account to the sudoers file.
7. In the **Description** field, enter a description for the created credentials record. As there can be a number of similar account names, for example, *Administrator*, it is recommended that you provide a meaningful unique description for the credentials record so that you can distinguish it in the list. The description is shown in brackets, following the user name.

Important! In the sudoers file, enable the `NOPASSWD:ALL` option for the user account that you want to elevate to root. Otherwise, jobs addressing a Linux server will fail as sudo will request the password. You can create a separate user account intended for work with Veeam Backup Free Edition on a Linux-based VM, grant root privileges to this account and specify settings of this account in the Credentials Manager. It is recommended that you avoid additional commands output for this user (like messages echoed from within `~/.bashrc` or command traces before execution) because they may affect Linux VM processing.



Linux Credentials Record (Identity/Pubkey)

You can log on to a Linux server or VM running Linux OS using the Identity/Pubkey authentication method. The Identity/Pubkey authentication method helps protect against malicious applications like keyloggers, strengthens the security level and simplifies launch of automated tasks.

To use the Identity/Pubkey authentication method, you must generate a pair of keys — a public key and private key:

- Public key is stored on Linux server(s) to which you plan to connect from the backup server. The key is kept in a special `authorized_keys` file containing a list of public keys.
- Private key is stored on the client machine — backup server. The private key is protected with a passphrase. Even if the private key is intercepted, the eavesdropper will have to provide the passphrase to unlock the key and use it.

For authentication on a Linux server, the client must prove that it has the private key matching the public key stored on the Linux server. To do this, the client generates a cryptogram using the private key and passes this cryptogram to the Linux server. If the client uses the "correct" private key for the cryptogram, the Linux server can easily decrypt the cryptogram with a matching public key.

Veeam Backup Free Edition has the following limitations for the Identity/Pubkey authentication method:

- Veeam Backup Free Edition does not support keys that are stored as binary data, for example, in a file of DER format.
- Veeam Backup Free Edition supports only keys whose passphrase is encrypted with algorithms supported by PuTTY:
 - AES (Rijndael): 128-bit, 192-bit and 256-bit CBC or CTR (SSH-2 only)
 - Blowfish: 128-bit CBC
 - Triple-DES: 168-bit CBC

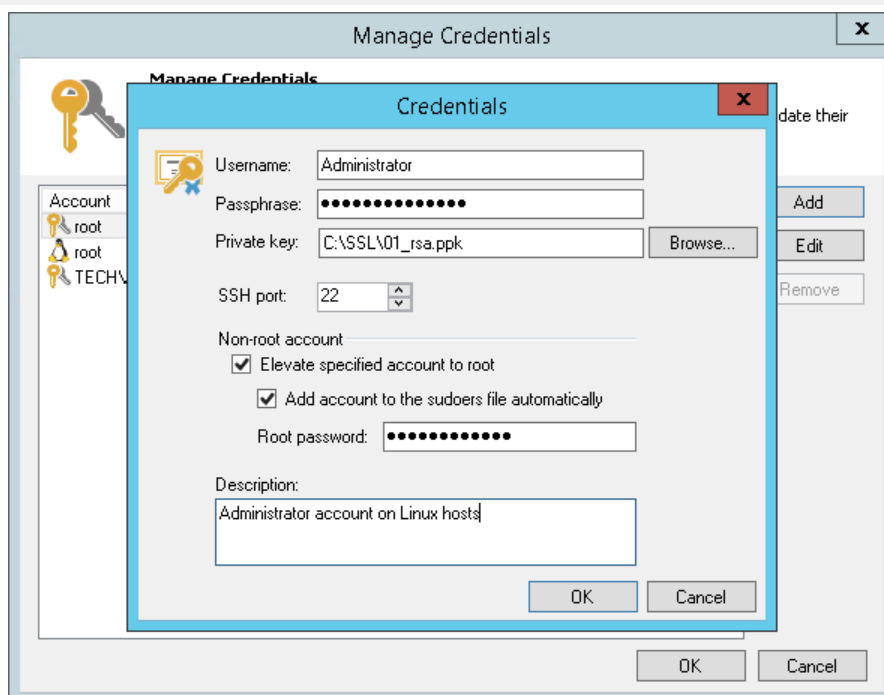
To add a credentials record using the Identity/Pubkey authentication method:

1. Generate a pair of keys using a key generation utility, for example, `ssh-keygen`.
2. Place the public key on a Linux server. To do this, add the public key to the `authorized_keys` file in the `.ssh/` directory in the home directory on the Linux server.
3. Place the private key in some folder on the backup server or in a network shared folder.
4. In Veeam Backup Free Edition, from the main menu select **Manage Credentials**.
5. Click **Add > Linux private key**.
6. In the **Username** field, specify a user name for the created credentials record.
7. In the **Passphrase** field, specify a passphrase for the private key on the backup server. To view the entered passphrase, click and hold the eye icon on the right of the field.
8. In the **Private key** field, enter a path to the private key or click **Browse** to select a private key.
9. In the **SSH port** field, specify a number of the SSH port that you plan to use to connect to a Linux server. By default, port 22 is used.
10. If you specify data for a non-root account that does not have root permissions on a Linux server, you can use the **Non-root account** section to grant sudo rights to this account.
 - a. To provide a non-root user with root account privileges, select the **Elevate specified account to root** check box.
 - b. To add the user account to sudoers file, select the **Add account to the sudoers file automatically** check box. If you do not enable this option, you will have to manually add the user account to the sudoers file.

11. In the **Description** field, enter a description for the created credentials record. As there can be a number of similar account names, for example, *Administrator*, it is recommended that you supply a meaningful unique description for the credentials record so that you can distinguish it in the list. The description is shown in brackets, following the user name.

Important!

In the sudoers file, enable the `NOPASSWD:ALL` option for the user account that you want to elevate to root. Otherwise, jobs addressing a Linux server will fail as sudo will request the password.



Editing and Deleting Credentials

You can edit and delete credentials records that you have created.

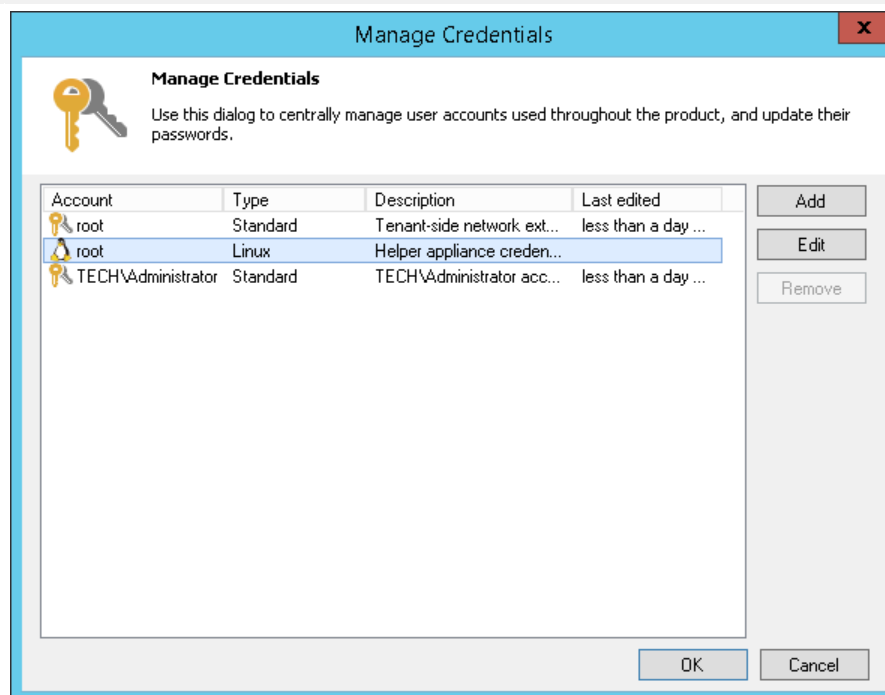
To edit a credentials record:

1. From the main menu, select **Manage Credentials**.
2. Select the credentials record in the list and click **Edit**.
3. If the credentials record is already used for any component in the backup infrastructure, Veeam Backup Free Edition will display a warning. Click **Yes** to confirm your intention.
4. Edit settings of the credentials record as required.

To delete a credentials record:

1. From the main menu, select **Manage Credentials**.
2. Select the credentials record in the list and click **Remove**. You cannot delete a record that is already used for any component in the backup infrastructure.

Note: The Credentials Manager contains two system credentials records: a credentials record for the Veeam FLR appliance and a credentials records for the tenant-side network extension appliance. You cannot delete these credentials records. However, you can edit them: change a password and record description.



Managing Passwords for Data Encryption

You can use the Password Manager to create and maintain a list of passwords that you plan to use for data encryption. Password management can be helpful in the following situations:

- You want to create new passwords for VeeamZIP files.
- You want to edit an existing password, for example, change its hint, or delete a password.

Tip:

Periodical change of passwords is a security best practice. You can create new passwords as often as you need based on your company security needs and regulatory requirements.

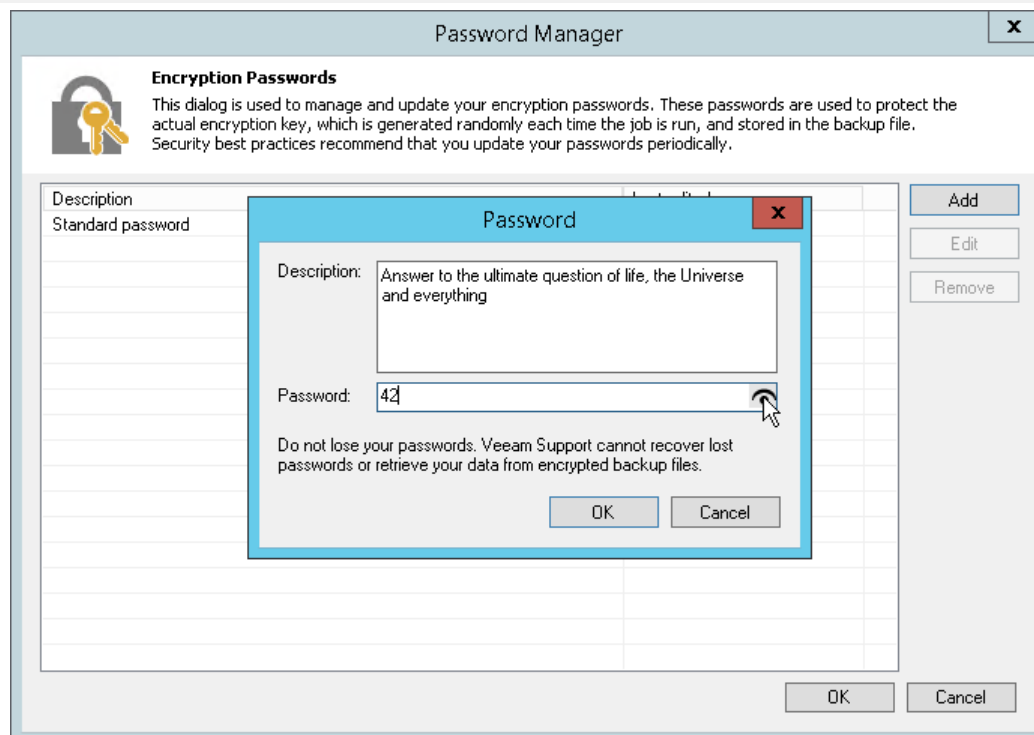
Creating Passwords

You can use the Password Manager to create one or more passwords.

To create a new password:

1. From the main menu, select **Manage Passwords**.
Veeam Backup Free Edition will open the Password Manager.
1. In the Password Manager, click **Add**.
2. In the **Description** field, specify a hint for the created password. It is recommended that you provide a meaningful hint that will help you recall the password. The password hint is displayed when you import an encrypted file on the backup server and access this file.
3. In the **Password** field, enter a password. To view the entered password, click and hold the eye icon on the right of the field.

Important! Always save a copy of the password you create in a secure place. If you lose the password, you will not be able to restore it.

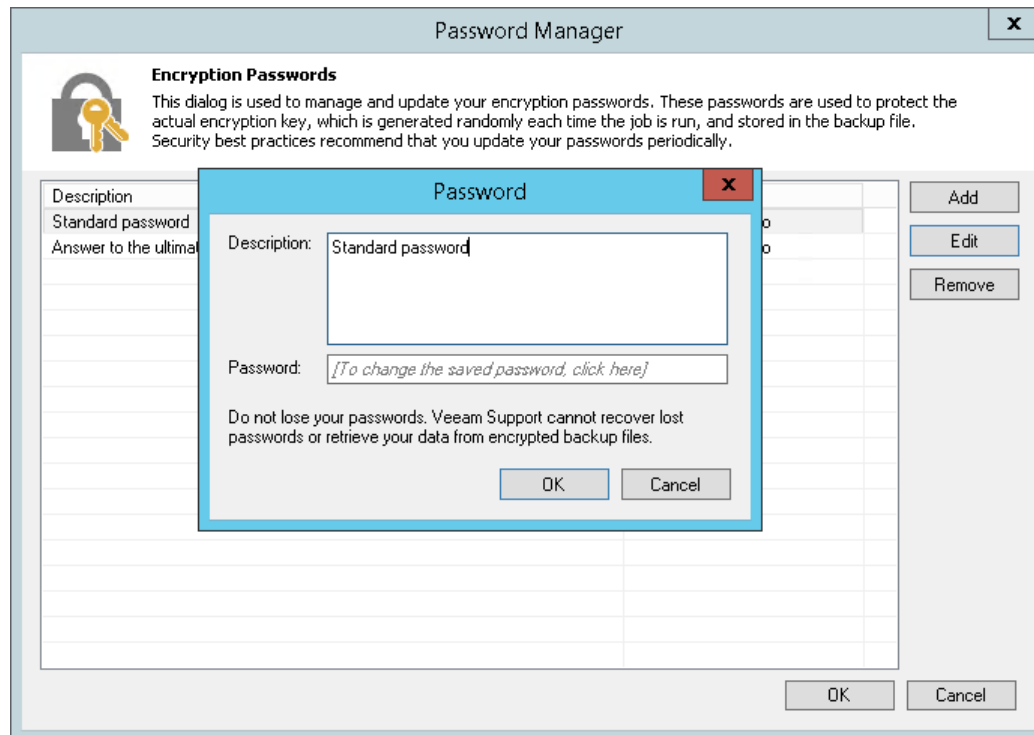


Editing Passwords

You can edit passwords you have created using the Password Manager.

To edit a password:

1. From the main menu, select **Manage passwords**.
Veeam Backup Free Edition will open the Password Manager.
2. In the Password Manager, select the password and click **Edit**.
3. Edit the password data: hint and password, as required.



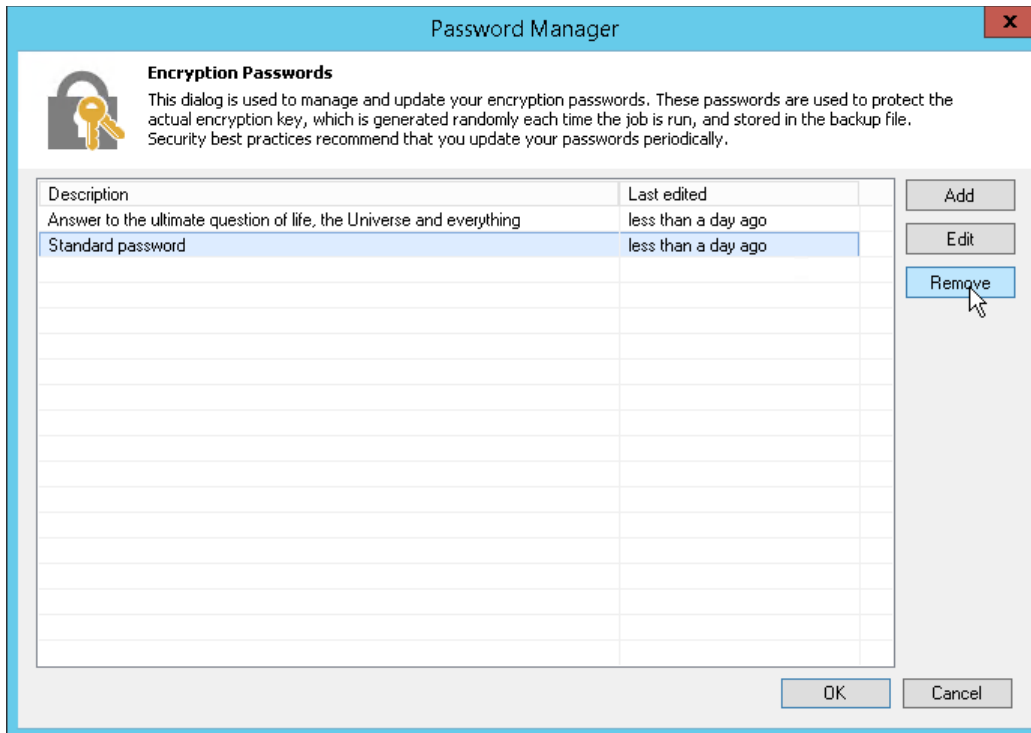
Deleting Passwords

You can delete passwords using the Password Manager.

You cannot remove a password that is currently used by any job on the backup server. To remove such password, you first need to delete a reference to this password in the job settings.

To delete a password:

1. From the main menu, select **Manage passwords**.
Veeam Backup Free Edition will open the Password Manager.
2. In the Password Manager, select the password and click **Remove**.



Adding VMware vSphere Servers

You must add to the backup infrastructure VMware vSphere servers on which VMs that you plan to process reside.

You can add vCenter Servers and ESX(i) hosts. If an ESX(i) host is managed by the vCenter Server, it is recommended that you add the vCenter Server, not a standalone ESX(i) host. Connecting the vCenter Server instead of standalone ESX(i) hosts provides more flexibility at work.

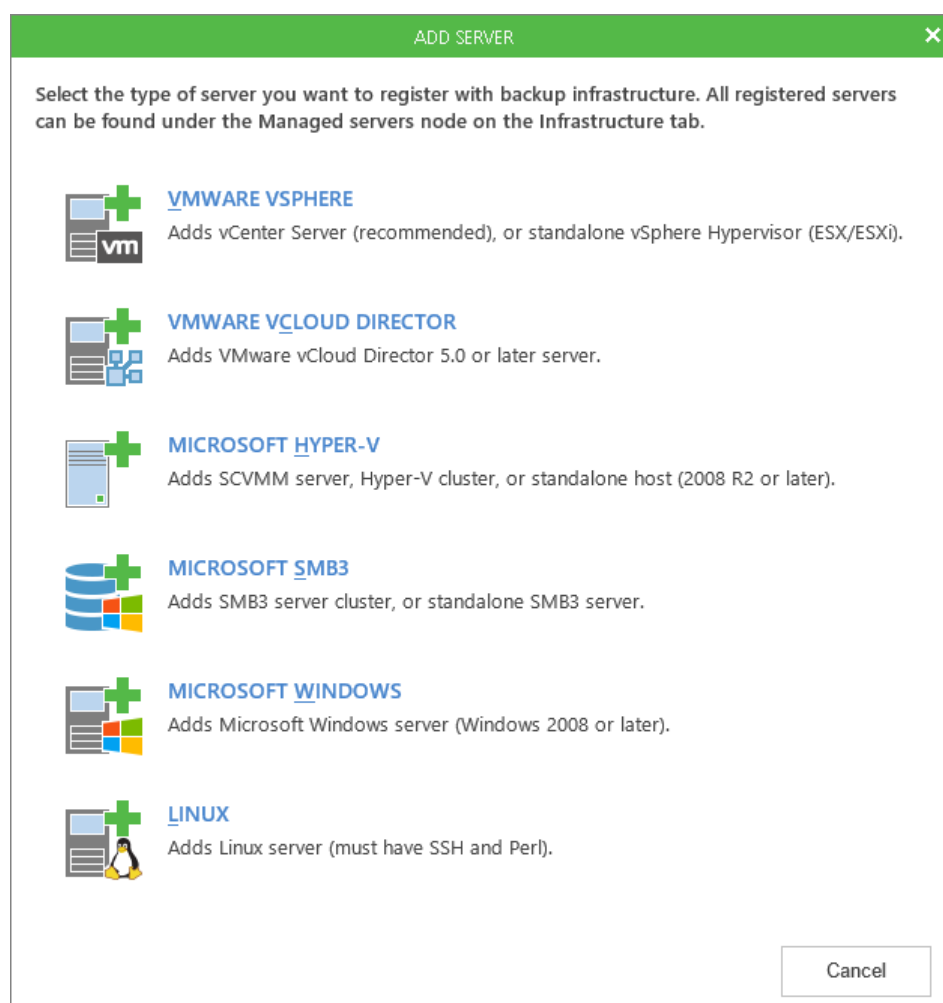
To add a VMware vSphere server, use the **New VMware Server** wizard.

Step 1. Launch New VMware Server Wizard

To launch the wizard, do one of the following:

- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. Then click **Add Server** on the toolbar.
- Open the **Virtual Machines** view, in the inventory pane right-click the **Infrastructure** node and select **Add server**.
- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. In the working area, click **Add Server**.

In the **Add Server** window, click **VMware vSphere**.



Step 2. Specify Server Name or Address

At the **Name** step of the wizard, specify an address and description for the VMware vSphere server.

1. Enter a full DNS name or IP address of the vCenter Server or standalone ESX(i) host.
2. 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.

The screenshot shows the 'New VMware Server' wizard window. The title bar is 'New VMware Server'. The window is divided into a sidebar on the left and a main content area on the right. The sidebar has a 'Name' tab selected, with other tabs being 'Credentials', 'SSH Connection', and 'Summary'. The main content area has a heading 'Name' and a sub-heading 'Specify DNS name or IP address of VMware server.' Below this, there are two text input fields. The first field is labeled 'DNS name or IP address:' and contains the text 'vcenter01.tech.local'. The second field is labeled 'Description:' and contains the text 'vCenter Server 01|'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

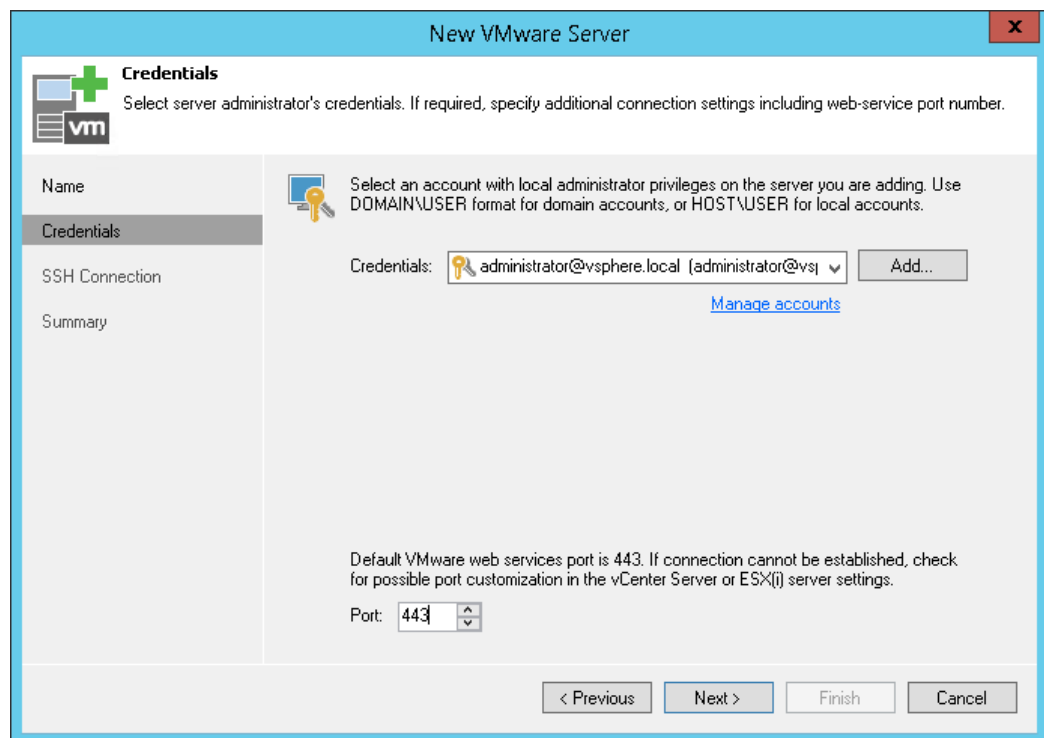
Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials and port settings for the VMware vSphere server.

1. From the **Credentials** list, select credentials for the account that has administrator privileges on the VMware vSphere server.

If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).

2. By default, Veeam Backup Free Edition uses port 443 to communicate with vCenter Servers and ESX(i) hosts. If a connection with the vCenter Server or ESX(i) host over this port cannot be established, you can customize the port number in vCenter Server/ESX(i) host settings and specify the new port number in the **Port** field.



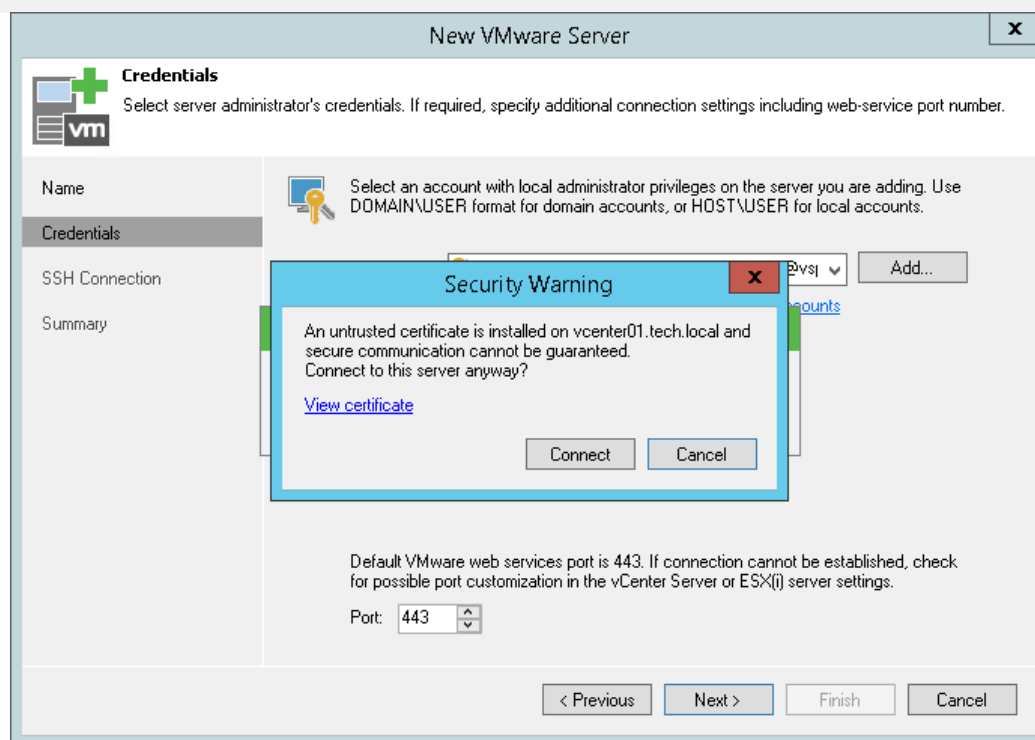
The screenshot shows the 'New VMware Server' wizard window, specifically the 'Credentials' step. The window has a blue title bar and a sidebar on the left with tabs: 'Name', 'Credentials' (selected), 'SSH Connection', and 'Summary'. The main area contains instructions: 'Select server administrator's credentials. If required, specify additional connection settings including web-service port number.' Below this, there's a key icon and text: 'Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.' The 'Credentials' field shows 'administrator@vsphere.local' with a dropdown arrow and an 'Add...' button. A 'Manage accounts' link is below it. At the bottom, there's a 'Port' field with '443' and a spinner. Navigation buttons at the bottom are '< Previous', 'Next >', 'Finish', and 'Cancel'.

3. When you add a vCenter Server or ESX(i) host, Veeam Backup Free Edition saves to the configuration database a thumbprint of the SSL certificate installed on the vCenter Server or ESX(i) host. During every subsequent connection to the server, Veeam Backup Free Edition 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 Free Edition displays a warning.

- If you trust the server, click **Connect**.
- If you do not trust the server, click **Cancel**. Veeam Backup Free Edition will display an error message, and you will not be able to connect to the server.

Note: If you update the certificate on the server, you must acknowledge the new certificate in the server connection settings. To do this, in the **Backup Infrastructure** view open the server settings, pass through the **Edit Server** wizard and click **Trust** to acknowledge the key.



Step 4. Specify SSH Settings

This step is available only if you are adding an ESX host. If you are adding a vCenter Server or ESXi host, the wizard will skip this step, and you will pass to the **Summary step** of the wizard.

If necessary, you can use an SSH connection for file copying operations. SSH connection settings are optional. If you do not want to use SSH, clear the **Use service console connection to this server** check box. In this case, Veeam Backup Free Edition will work with the ESX host in the agentless mode.

To use a SSH connection:

1. Make sure that the **Use service console connection to this server** check box is selected.
2. From the **Credentials** list, select credentials to connect to the service console of the ESX host. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).

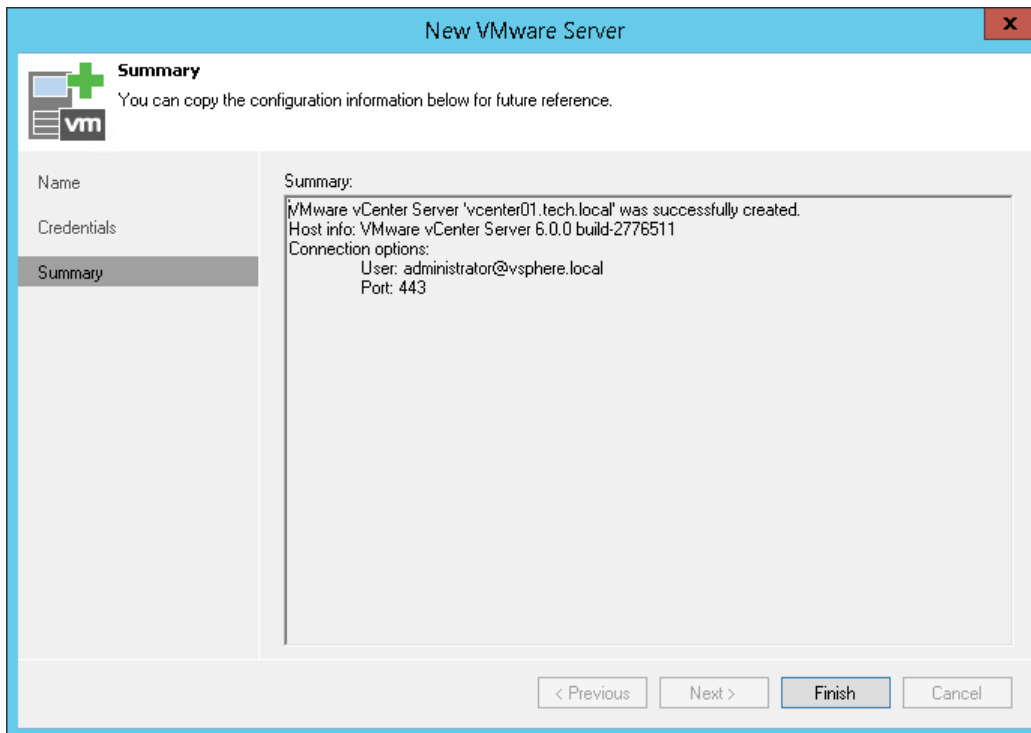
3. To configure advanced SSH settings, click **Advanced**.
 - a. In the **Service console connection** section, specify an SSH timeout. By default, the SSH timeout is set to 20000 ms. If a task targeted at the ESX host is inactive after the specified timeout, Veeam Backup Free Edition will automatically terminate the task.
 - b. In the **Data transfer options** section, specify connection settings for file copy operations. Enter a range of ports that will be used as transmission channels between the source host and target host (one port per task). By default, Veeam Backup Free Edition uses port range 2500-5000. If the virtual environment is not large and data traffic will not be significant, you can specify a smaller range of ports, for example, 2500-2510 to run 10 concurrent jobs at the same time.
 - c. If the ESX host is deployed outside NAT, in the **Preferred TCP connection role** section select the **Run server on this side** check box. In the NAT scenario, the outside client cannot initiate a connection to the server on the NAT network. As a result, services that require initiation of the connection from outside can be disrupted. With this option selected, you will be able to overcome this limitation and initiate a 'server-client' connection — that is, a connection in the direction of the ESX host.

The screenshot shows the 'New VMware Server' wizard window. The title bar is blue with the text 'New VMware Server' and a red close button. The main window has a light blue header with a green plus icon and the text 'SSH Connection'. Below the header, there is a description: 'Provide credentials for service console connection, and adjust secure shell (SSH) port number if needed. Service console connection to ESX server is optional.' On the left, there is a sidebar with four tabs: 'Name', 'Credentials', 'SSH Connection' (which is selected and highlighted in grey), and 'Summary'. The main area of the window contains a checkbox labeled 'Use service console connection to this server' which is checked. Below this, there is a 'Credentials' section with a dropdown menu showing 'root (root, last edited: 2 days ago)' and an 'Add...' button. A link 'Manage accounts' is also present. At the bottom of the main area, there is a link 'Advanced...' with the text 'Customize advanced connection settings, such as SSH and data mover ports' above it. At the very bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of VMware vSphere server adding.

1. Review details of the VMware vSphere server.
2. Click **Finish** to exit the wizard.



Adding Microsoft Hyper-V Servers

You must add to the backup infrastructure Microsoft Hyper-V hosts on which VMs you plan to work with are located.

You can connect standalone Microsoft Hyper-V hosts, Microsoft Hyper-V clusters or SCVMM servers. If a Microsoft Hyper-V host is added to a cluster, it is recommended that you add to the backup infrastructure a cluster, not a standalone Microsoft Hyper-V host. Connecting clusters and SCVMM instead of standalone Microsoft Hyper-V hosts provides more flexibility at work.

Before adding a Microsoft Hyper-V server, [check prerequisites](#). Then use the **New Hyper-V Server** wizard to add the server.

Before You Begin

Before you add a Microsoft Hyper-V server to the backup infrastructure, check the following prerequisites:

- File and printer sharing must be enabled in network connection settings of the added Microsoft Hyper-V host. On every connected Microsoft Hyper-V host, Veeam Backup Free Edition deploys a set of components:
 - Veeam Installer Service
 - Veeam Data Mover Service
 - Veeam Hyper-V Integration Service

If file and printer sharing is not enabled on the host, Veeam Backup Free Edition will fail to deploy these components.

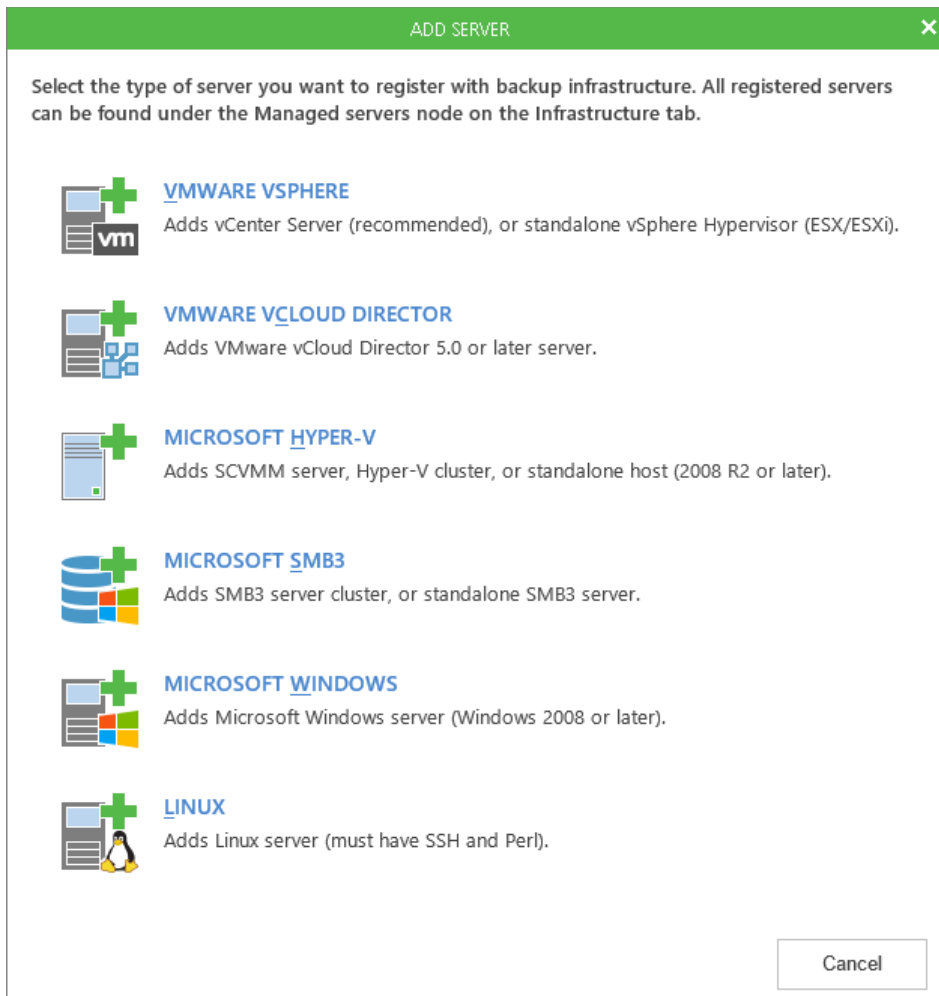
- [For SCVMM] SCVMM Admin UI must be installed on the backup server. Otherwise, you will not be able to add SCVMM servers to the backup infrastructure.

Step 1. Launch New Hyper-V Server Wizard

To launch the wizard, do one of the following:

- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. Then click **Add Server** on the toolbar.
- Open the **Virtual Machines** view, in the inventory pane right-click the **Infrastructure** node and select **Add server**.
- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. In the working area, click **Add Server**.

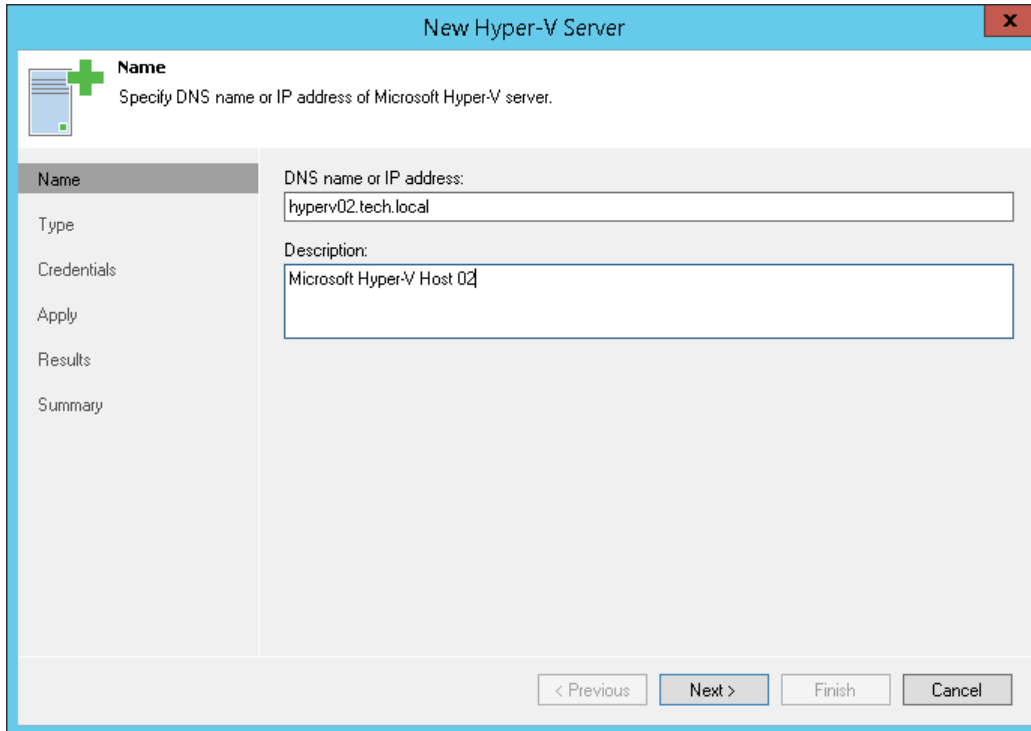
In the **Add Server** window, click **Microsoft Hyper-V**.



Step 2. Specify Server Name or Address

At the **Name** step of the wizard, specify an address and description for the Microsoft Hyper-V server.

1. Enter a full DNS name or IP address of the Microsoft Hyper-V server.
2. 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.



The screenshot shows the 'New Hyper-V Server' wizard window. The title bar is blue with the text 'New Hyper-V Server' and a close button. The main area has a light blue header with a green plus icon and the text 'Name' and 'Specify DNS name or IP address of Microsoft Hyper-V server.' Below this is a list of steps: 'Name', 'Type', 'Credentials', 'Apply', 'Results', and 'Summary'. The 'Name' step is selected. The main content area has two text boxes: 'DNS name or IP address:' with the value 'hyperv02.tech.local' and 'Description:' with the value 'Microsoft Hyper-V Host 02'. At the bottom are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

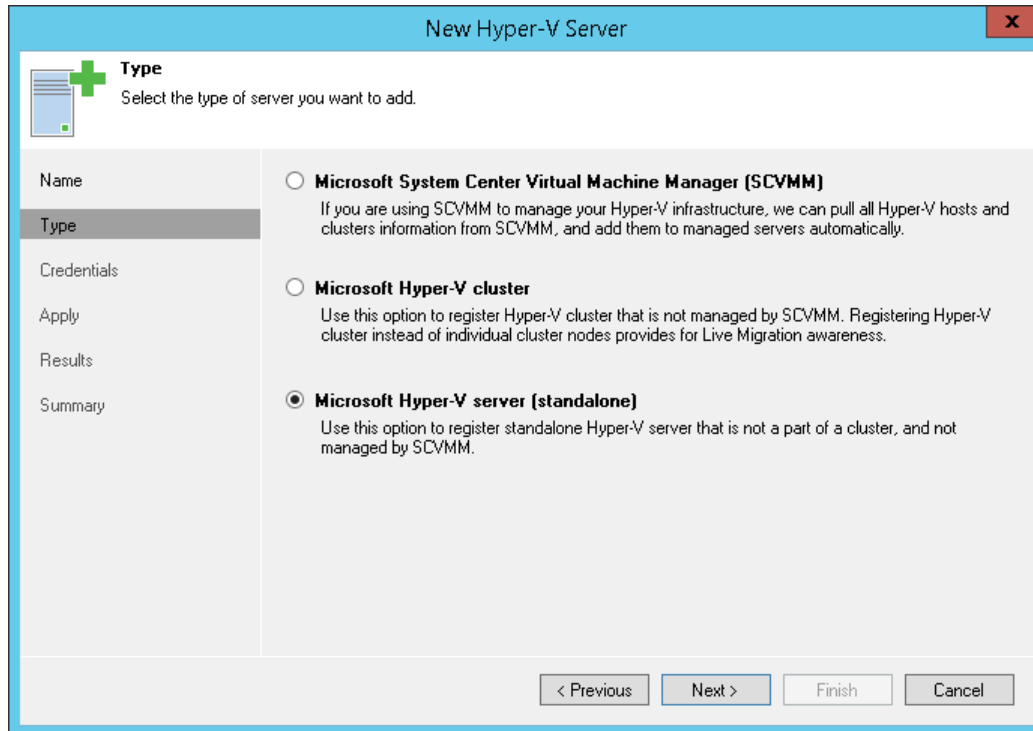
Name	DNS name or IP address:
Type	hyperv02.tech.local
Credentials	Description:
Apply	Microsoft Hyper-V Host 02
Results	
Summary	

< Previous Next > Finish Cancel

Step 3. Choose Server Type

At the **Type** step of the wizard, select the type of server that you want to add.

- Select **Microsoft System Center Virtual Machine Manager** if you want to add SCVMM that manages several Microsoft Hyper-V hosts. Veeam Backup Free Edition will pull information about Microsoft Hyper-V hosts and clusters managed by SCVMM and add them to the list of servers as a part of the SCVMM hierarchy.
- Select **Microsoft Hyper-V cluster** if you want to add a Microsoft Hyper-V cluster not managed by SCVMM.
- Select **Microsoft Hyper-V server** if you want to add a standalone Microsoft Hyper-V host that is not a part of the Microsoft Hyper-V cluster and is not managed by SCVMM.



The screenshot shows the 'New Hyper-V Server' wizard window. The title bar is blue with the text 'New Hyper-V Server' and a close button. The main area has a light blue header with a green plus icon and the text 'Type' and 'Select the type of server you want to add.' Below this is a list of three options, each with a radio button and a description. The first option is 'Microsoft System Center Virtual Machine Manager (SCVMM)' with a description about pulling information from SCVMM. The second option is 'Microsoft Hyper-V cluster' with a description about registering a cluster instead of individual nodes. The third option is 'Microsoft Hyper-V server (standalone)' which is selected with a radio button and a description about registering a standalone server. At the bottom right are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

New Hyper-V Server

Type
Select the type of server you want to add.

Name

Type

Credentials

Apply

Results

Summary

- ☐ **Microsoft System Center Virtual Machine Manager (SCVMM)**
If you are using SCVMM to manage your Hyper-V infrastructure, we can pull all Hyper-V hosts and clusters information from SCVMM, and add them to managed servers automatically.
- ☐ **Microsoft Hyper-V cluster**
Use this option to register Hyper-V cluster that is not managed by SCVMM. Registering Hyper-V cluster instead of individual cluster nodes provides for Live Migration awareness.
- ☒ **Microsoft Hyper-V server (standalone)**
Use this option to register standalone Hyper-V server that is not a part of a cluster, and not managed by SCVMM.

< Previous Next > Finish Cancel

Step 4. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for the Microsoft Hyper-V server.

1. From the **Credentials** list, select credentials for the account that has administrator privileges on the Microsoft Hyper-V server. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).

Veeam Backup Free Edition will use the provided credentials to deploy the following components on every added server:

- Veeam Installer Service
- Veeam Data Mover Service (Transport)
- Veeam Hyper-V Integration Service

If you are adding SCVMM, the same credentials will be applied to all Microsoft Hyper-V hosts managed by SCVMM. If some Microsoft Hyper-V hosts use their own credentials different from those you have provided, Veeam Backup Free Edition will fail to deploy components on these hosts. You will have to specify credentials for such Microsoft Hyper-V hosts separately.

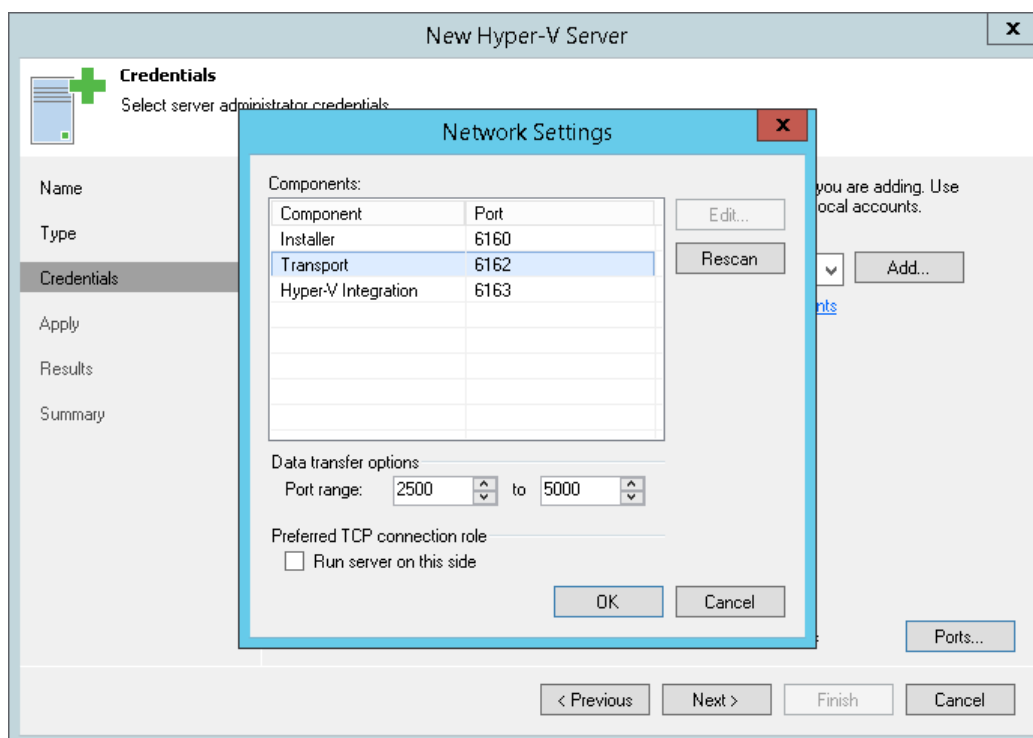
After you connect SCVMM, expand it in the inventory pane to see the list of managed Microsoft Hyper-V hosts. Right-click the host, select **Properties** and use the **Edit Hyper-V Server** wizard to specify the credentials for this host.

The screenshot shows the 'New Hyper-V Server' wizard at the 'Credentials' step. The window title is 'New Hyper-V Server'. On the left is a sidebar with steps: Name, Type, Credentials (selected), Apply, Results, and Summary. The main area has a heading 'Credentials' with a green plus icon and the text 'Select server administrator credentials.' Below this, there's a key icon and instructions: 'Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.' A 'Credentials:' label is followed by a dropdown menu showing 'hyperv02\Administrator (hyperv02\Administrato' and an 'Add...' button. A 'Manage accounts' link is also present. At the bottom, there's a 'Ports...' button and a note: 'Click Ports to customize network ports to be used by individual components'. The bottom of the window has navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

2. To customize network ports used by Veeam Backup Free Edition components, click **Ports**. By default, Veeam Backup Free Edition components use the following ports:
 - Veeam Installer Service: port 6160
 - Veeam Data Mover Service (Transport): port 6162
 - Veeam Hyper-V Integration Service: port 6163

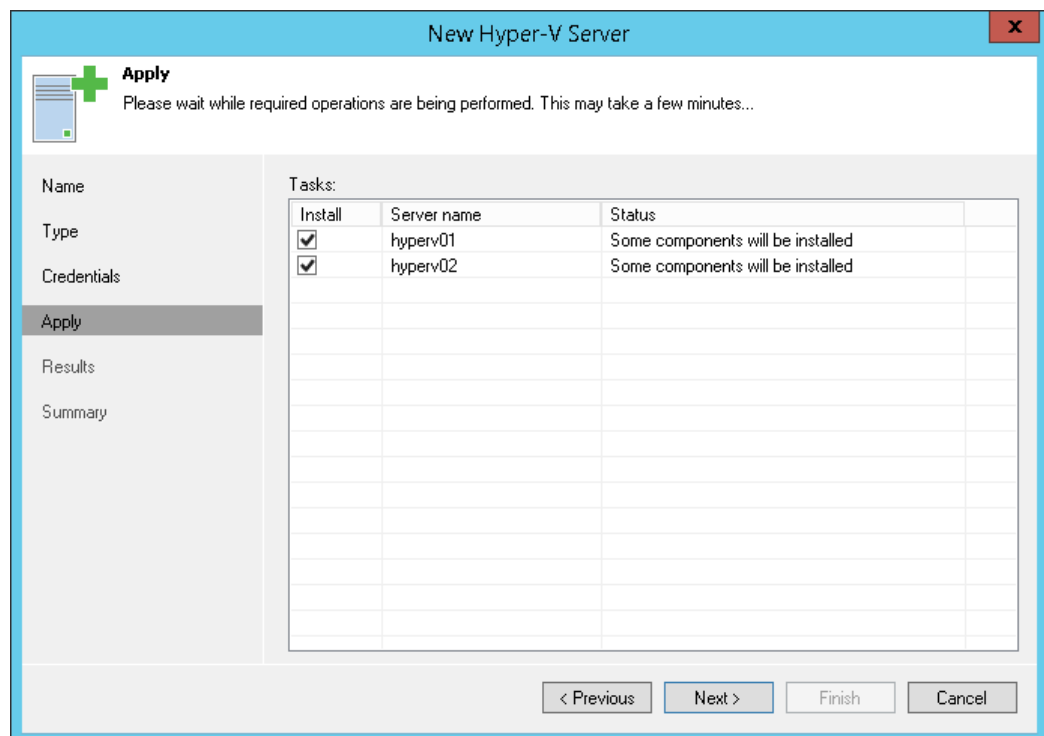
If necessary, adjust port numbers.

3. In the **Data transfer options** section of the **Network Settings** window, specify connection settings for file copy operations. Provide a range of ports that will be used as transmission channels between the source host and target host (one port per task). By default, Veeam Backup Free Edition uses port range 2500-5000. If the virtual environment is not large and data traffic will not be significant, you can specify a smaller range of ports, for example, 2500-2510 to run 10 concurrent jobs at the same time.
4. If the Microsoft Hyper-V host is deployed outside NAT, in the **Preferred TCP connection role** section select the **Run server on this side** check box. In the NAT scenario, the outside client cannot initiate a connection to the server on the NAT network. As a result, services that require initiation of the connection from outside can be disrupted. With this option selected, you will be able to overcome this limitation and initiate a 'server-client' connection — that is, a connection in the direction of the Microsoft Hyper-V host.



At the **Apply** step of the wizard, review what Veam Backup Free Edition components are already installed on the server and what components will be installed.

- If necessary, you can instruct Veeam Backup Free Edition to install components on hosts that were initially excluded later. To do this, open the **Backup Infrastructure** view, in the inventory pane select the added SCVMM or Microsoft Hyper-V cluster. In the working area right-click the Microsoft Hyper-V host and select **Properties**.



- The recommended number of concurrent tasks is calculated automatically based on available host resources. Microsoft Hyper-V hosts with multi-core CPUs can handle more concurrent tasks. For example, for a 4-core CPU, it is recommended that you specify maximum 4 concurrent tasks, for an 8-core CPU — 8 concurrent tasks. When defining the number of concurrent tasks, keep in mind network traffic throughput in the virtual infrastructure.

The **Max concurrent tasks** field is displayed only for standalone Microsoft Hyper-V hosts. To limit the number of concurrent tasks for hosts managed by SCVMM or Microsoft Hyper-V cluster, you need to set this value in settings of each Microsoft Hyper-V host in the SCVMM hierarchy or cluster separately. To do this, open the **Backup Infrastructure** view, in the inventory pane select the added SCVMM or Microsoft Hyper-V cluster, in the working area right-click the Microsoft Hyper-V host and select **Properties**.

The screenshot shows the 'New Hyper-V Server' wizard in the 'Apply' step. The window title is 'New Hyper-V Server'. On the left, there is a vertical navigation pane with the following items: Name, Type, Credentials, Apply (highlighted), Results, and Summary. The main area contains the following text:

Apply
Please review your settings and click Next to continue.

Due to these modifications the following components will be installed or removed on the target host:

Transport	already exists
Hyper-V Integration	already exists

This Hyper-V server will act as the backup proxy for jobs running in the on-host backup mode.

Max concurrent tasks:
4

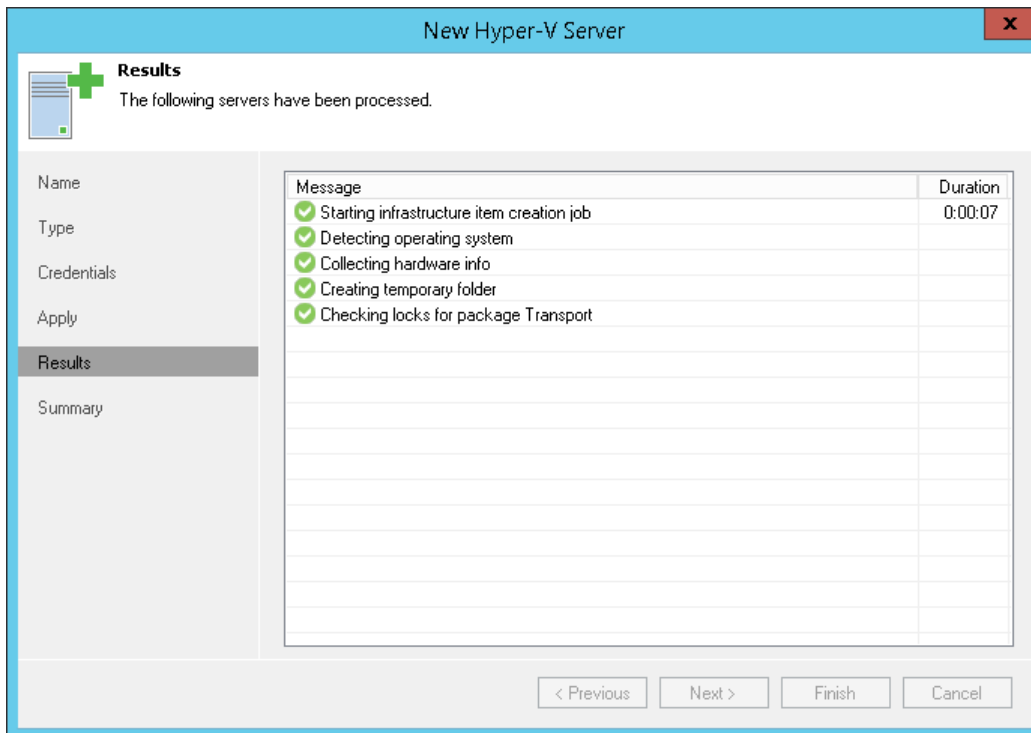
After you click Next missed components will be installed on the target host.

At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 6. Assess Results

At the **Results** step of the wizard, complete the procedure of Microsoft Hyper-V server adding.

1. Review details of the Microsoft Hyper-V server.
2. Click **Next**, then click **Finish** to exit the wizard.



Step 7. Specify Settings for Connected Volumes

After you have added a Hyper-V host to Veeam Backup Free Edition, you can configure the following settings for this host:

- **Enable or disable changed block tracking**
- **Specify volume-specific settings:** choose a VSS provider and specify the number of concurrent Hyper-V snapshots
- **Enable or disable failover to a software VSS provider**

Before you specify settings for a Hyper-V host, you must perform a volume rescan operation for the added Hyper-V host. During the rescan operation, Veeam Backup Free Edition retrieves information about disks and volumes that are currently connected to the Hyper-V host and writes this information to the Veeam Backup Free Edition database.

Veeam Backup Free Edition automatically performs the rescan operation once a day. You can also start the rescan operation manually:

1. Open the **Files** view.
2. Click the **Microsoft Hyper-V** node in the inventory tree.
3. Select the necessary Hyper-V host in the working area and click **Rescan** on the ribbon. Alternatively, you can right-click the necessary Hyper-V host in the working area and select **Rescan**.

Changed Block Tracking Settings

By default, Veeam Backup Free Edition enables changed block tracking for processing all VMs that reside on a connected Hyper-V host. You may disable changed block tracking, for example, for testing purposes.

Change block tracking is enabled and disabled at the level of a Hyper-V host. To disable changed block tracking:

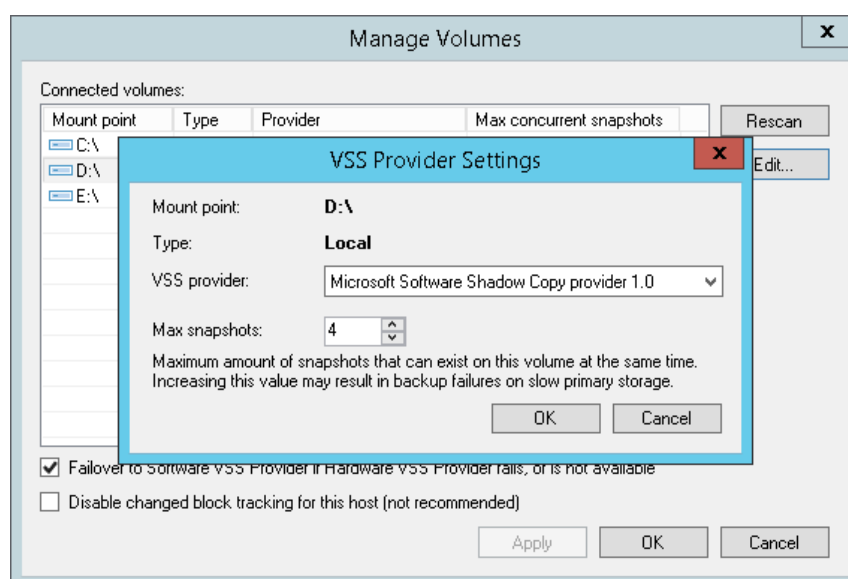
1. Open the **Files** view.
2. Click the **Microsoft Hyper-V** node in the inventory tree.
3. Select the necessary Hyper-V host in the working area and click **Manage Volumes** on the ribbon. Alternatively, you can right-click the necessary Hyper-V host in the working area and select **Manage Volumes**.
4. In the **Manage Volumes** window, select the **Disable changed block tracking for this host** check box.

Volume-Specific Settings

You can define volume-specific settings for a Hyper-V host: select what VSS provider must be used for Hyper-V snapshot creation and specify the maximum number of concurrent Hyper-V snapshots that must exist for a volume.

To specify volume-specific settings:

1. Open the **Files** view.
2. Click the **Microsoft Hyper-V** node in the inventory tree.
3. Select the necessary Hyper-V host in the working area and click **Manage Volumes** on the ribbon. Alternatively, you can right-click the necessary Hyper-V host in the working area and select **Manage Volumes**.
4. Select the necessary volume in the list and click **Edit**.
5. To take a VSS snapshot of a specific volume, Veeam Backup Free Edition uses one of VSS providers available for this volume. To explicitly define what VSS provider should be used on a particular volume, select the necessary VSS provider from the **VSS provider** list. If a VSS provider is not set explicitly selected, Veeam Backup Free Edition will scan the list of available VSS providers and select the most appropriate one automatically.
6. By default, tasks working with the same volume can take up to 4 snapshots of a volume simultaneously. If necessary, you can increase or decrease the number of snapshots that can exist at the same time. It is not recommended to increase the number of snapshots for slow storage: a great number of snapshots existing at the same time may cause VM processing failures.

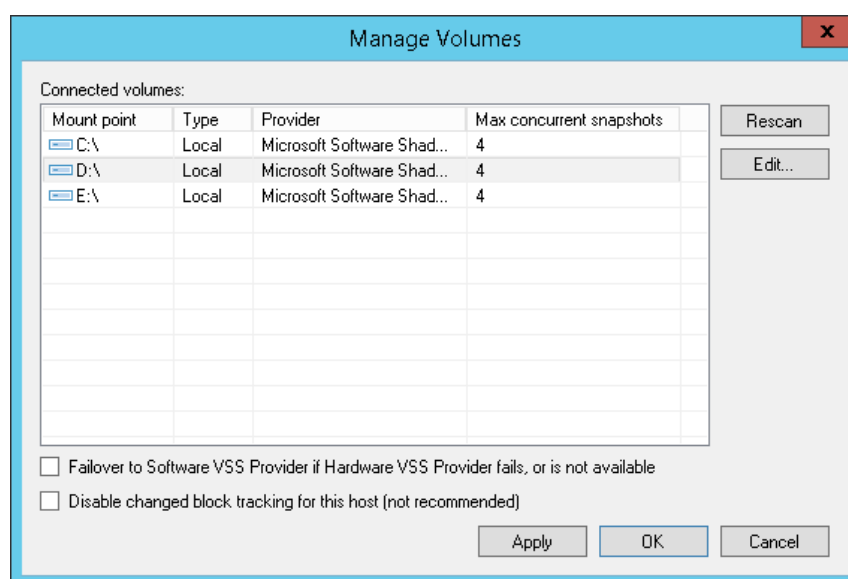


VSS Provider Failover Settings

By default, Veeam Backup Free Edition automatically fails over from a hardware VSS provider to a software VSS provider if a problem occurs. If you have selected to use a hardware VSS provider, Veeam Backup Free Edition engages the specified hardware VSS provider for volume snapshot creation. If the hardware VSS provider fails for some reason, Veeam Backup Free Edition engages a software VSS provider to create a volume snapshot.

By default, the failover option is enabled. To disable failover to a software VSS provider:

1. Open the **Files** view.
2. Click the **Microsoft Hyper-V** node in the inventory tree.
3. Select the necessary Hyper-V host in the working area and click **Manage Volumes** on the ribbon. Alternatively, you can right-click the necessary Hyper-V host in the working area and select **Manage Volumes**.
4. In the **Manage Volumes** window, clear the **Failover to Software VSS Provider if Hardware VSS Provider fails to create a snapshot** check box.



Adding Microsoft Windows Servers

You must add to the backup infrastructure Microsoft Windows servers that you plan to use as backup infrastructure components and servers that you plan to use for various types of restore operations.

Before adding a Microsoft Windows server, [check prerequisites](#). Then use the **New Windows Server** wizard to add the server.

Before You Begin

Before you add a Microsoft Windows server to the backup infrastructure, check network connection settings of this server.

File and printer sharing must be enabled in network connection settings of the added Microsoft Windows server. On every connected Microsoft Windows server, Veeam Backup Free Edition deploys two components:

- Veeam Installer Service
- Veeam Data Mover Service
- Veeam Mount Server

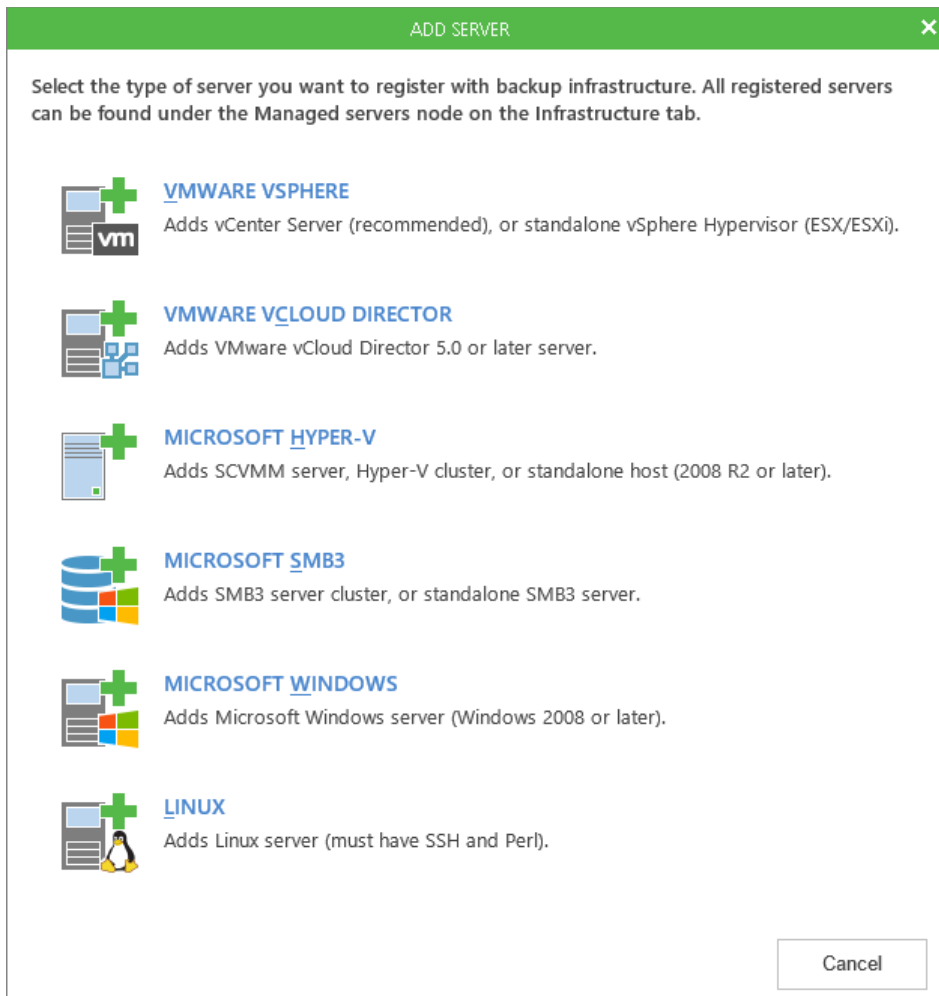
If file and printer sharing is not enabled, Veeam Backup Free Edition will fail to deploy these components.

Step 1. Launch New Windows Server Wizard

To launch the wizard, do one of the following:

- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. Then click **Add Server** on the toolbar.
- Open the **Virtual Machines** view, in the inventory pane right-click the **Infrastructure** node and select **Add server**.
- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. In the working area, click **Add Server**.

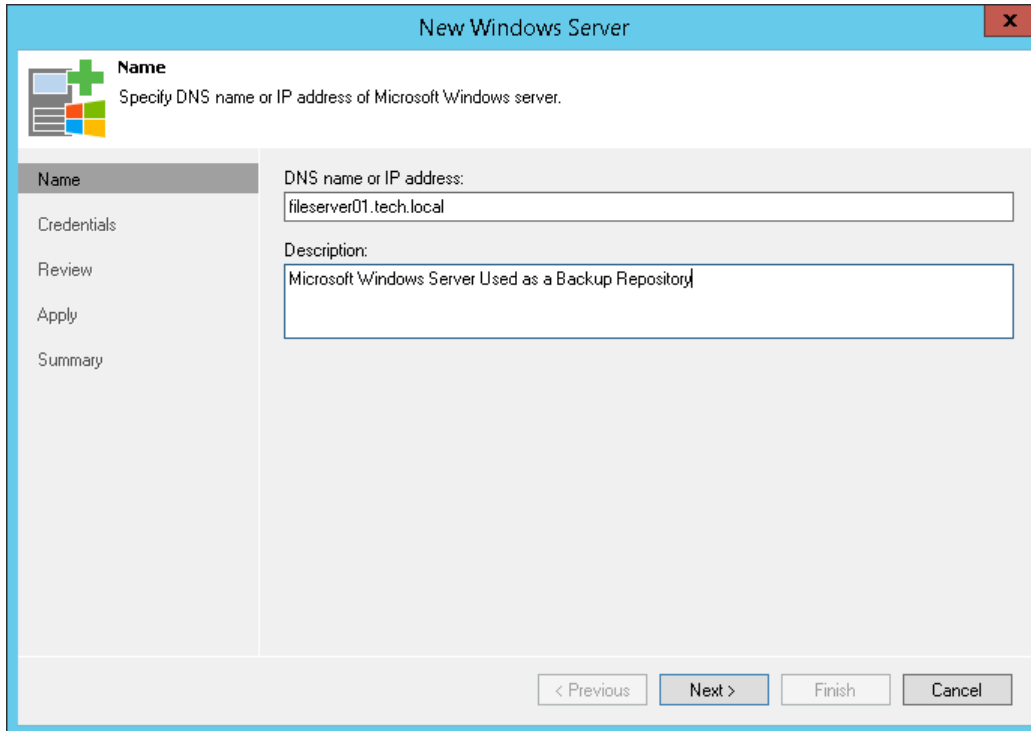
In the **Add Server** window, click **Microsoft Windows**.



Step 2. Specify Server Name or Address

At the **Name** step of the wizard, specify an address and description for the Microsoft Windows server.

1. Enter a full DNS name or IP address of the Microsoft Windows server.
2. 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.



The screenshot shows a window titled "New Windows Server" with a close button (X) in the top right corner. The window has a blue header bar. Below the header, there is a section with a green plus icon and a server icon, followed by the text "Name" and "Specify DNS name or IP address of Microsoft Windows server." On the left side, there is a vertical list of steps: "Name", "Credentials", "Review", "Apply", and "Summary". The "Name" step is currently selected. The main area of the window contains two text input fields. The first field is labeled "DNS name or IP address:" and contains the text "fileserver01.tech.local". The second field is labeled "Description:" and contains the text "Microsoft Windows Server Used as a Backup Repository". At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

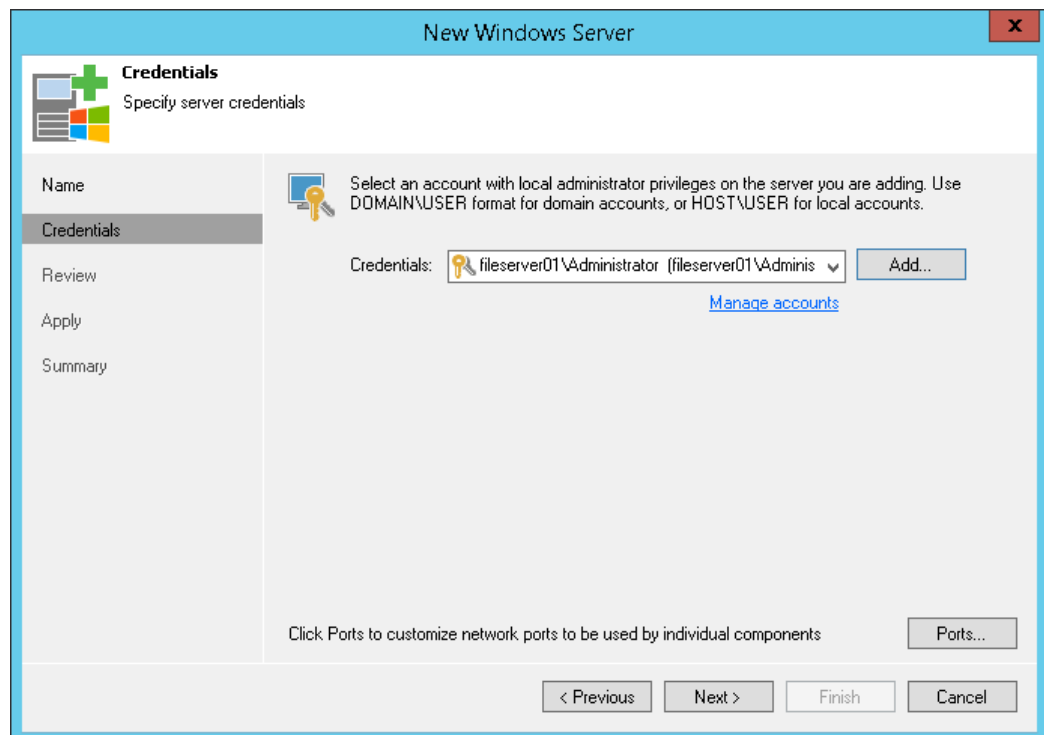
Step 3. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for the Microsoft Windows server.

1. From the **Credentials** list, select credentials for the account that has administrator privileges on the Microsoft Windows server. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).

Veeam Backup Free Edition will use the provided credentials to deploy the following components on the added server:

- Veeam Installer Service
- Veeam Data Mover Service (Transport)
- Veeam Mount Server



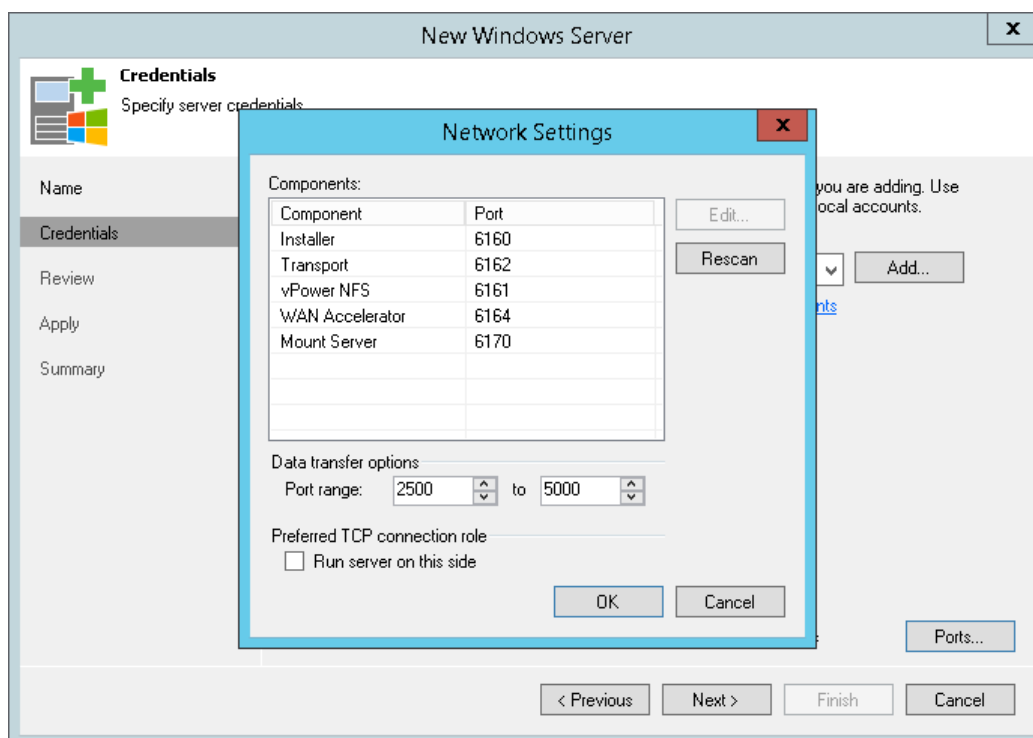
2. To customize network ports used by Veeam Backup Free Edition components, click **Ports**. By default, Veeam Backup Free Edition components use the following ports:

- Veeam Installer Service: port 6160
- Veeam Data Mover Service (Transport): port 6162
- Veeam vPower NFS Service: port 6161
- Veeam WAN Accelerator Service: port 6164
- Veeam Mount Server: port 6170

If necessary, adjust port numbers.

3. In the **Data transfer options** section of the **Network Settings** window, specify connection settings for file copy operations. Provide a range of ports that will be used as transmission channels between the source server and target server (one port per task). By default, Veeam Backup Free Edition uses port range 2500-5000. If the virtual environment is not large and data traffic will not be significant, you can specify a smaller range of ports, for example, 2500-2510 to run 10 concurrent jobs at the same time.

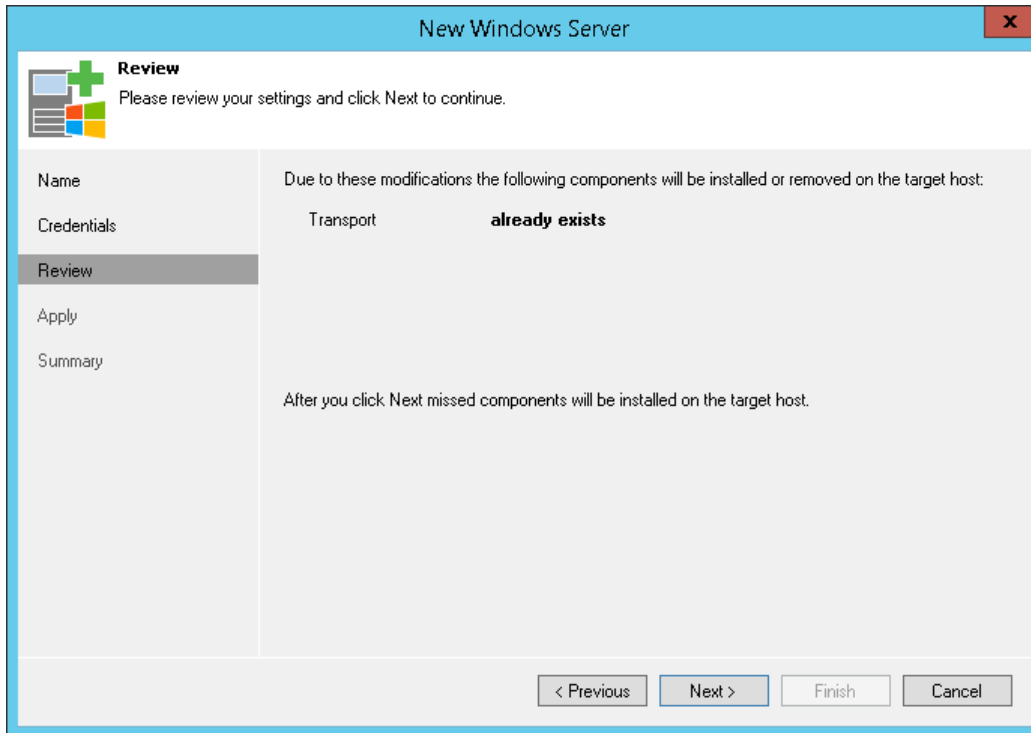
4. If the Microsoft Windows server is deployed outside NAT, in the **Preferred TCP connection role** section select the **Run server on this side** check box. In the NAT scenario, the outside client cannot initiate a connection to the server on the NAT network. As a result, services that require initiation of the connection from outside can be disrupted. With this option selected, you will be able to overcome this limitation and initiate a 'server-client' connection — that is, a connection in the direction of the Microsoft Windows server.



Step 4. Review Components

At the **Review** step of the wizard, review what Veeam Backup Free Edition components are already installed on the server and what components will be installed.

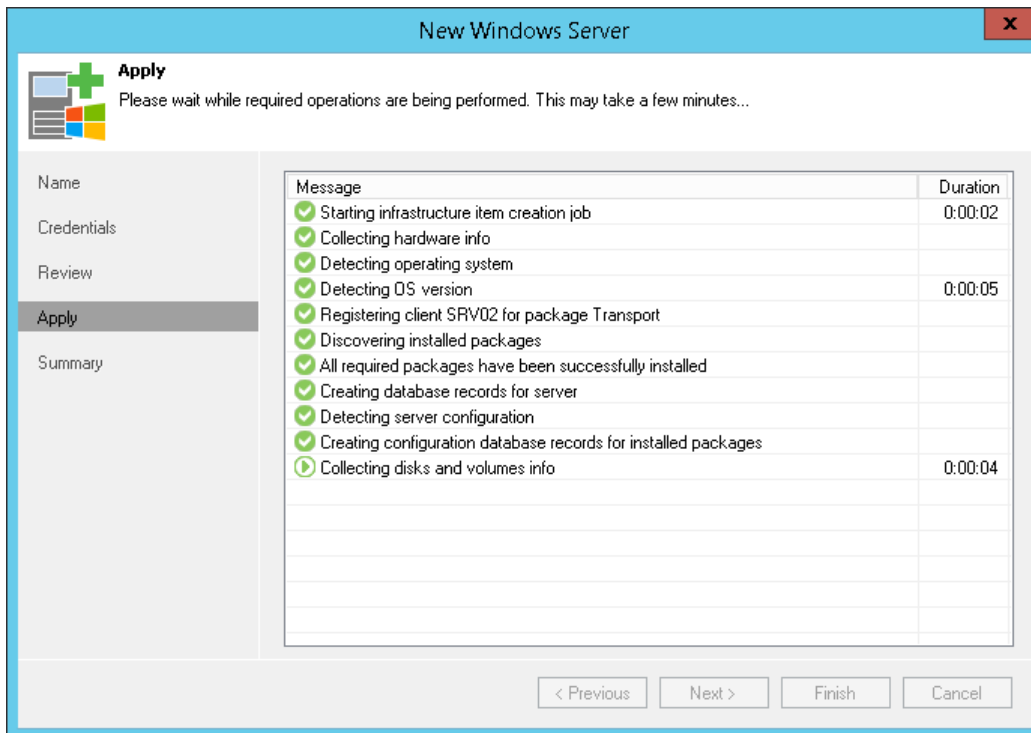
1. Review the components.
2. Click **Next** to add the Microsoft Windows server to the backup infrastructure.



Step 5. Finish Working with Wizard

At the **Apply** step of the wizard, complete the procedure of Microsoft Windows server adding.

1. Review details of the Microsoft Windows server.
2. Click **Next**, then click **Finish** to exit the wizard.



Adding Linux Servers

You must add to the backup infrastructure Linux servers that you plan to use for various types of restore operations.

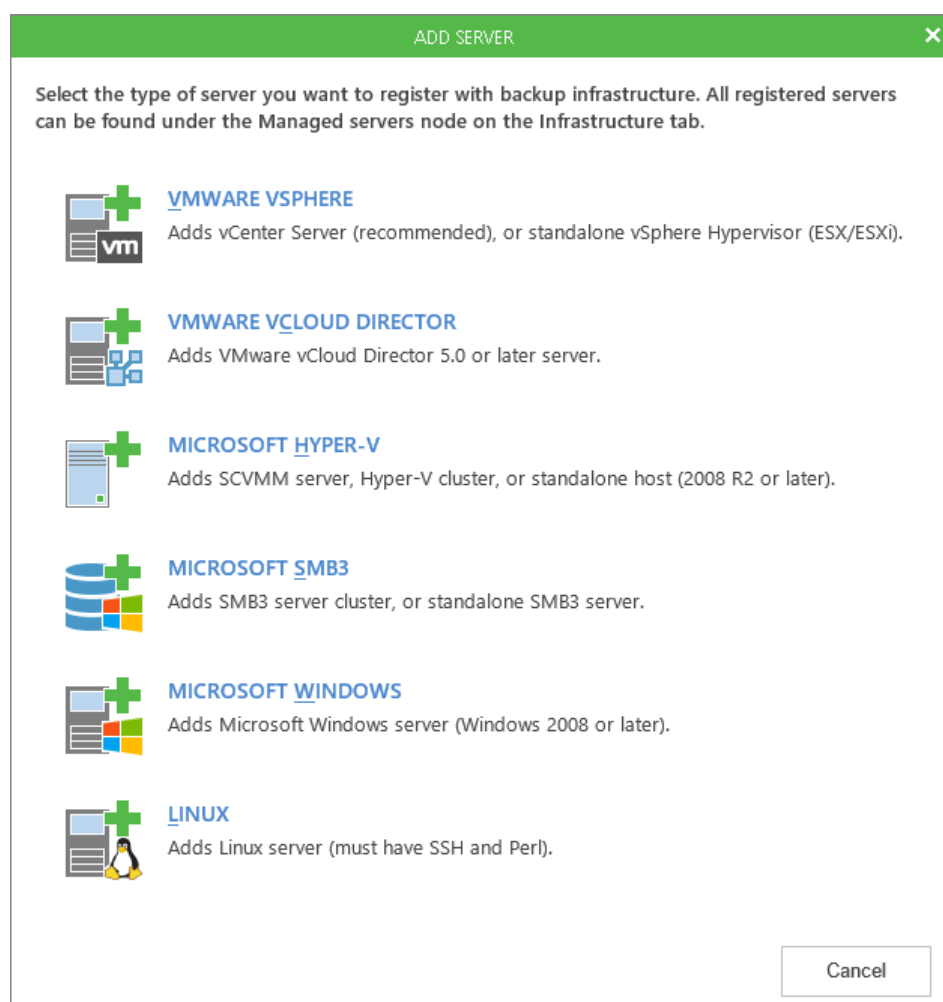
To add a Linux server, use the **New Linux Server** wizard.

Step 1. Launch New Linux Server Wizard

To launch the wizard, do one of the following:

- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. Then click **Add Server** on the toolbar.
- Open the **Virtual Machines** view, in the inventory pane right-click the **Infrastructure** node and select **Add server**.
- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. In the working area, click **Add Server**.

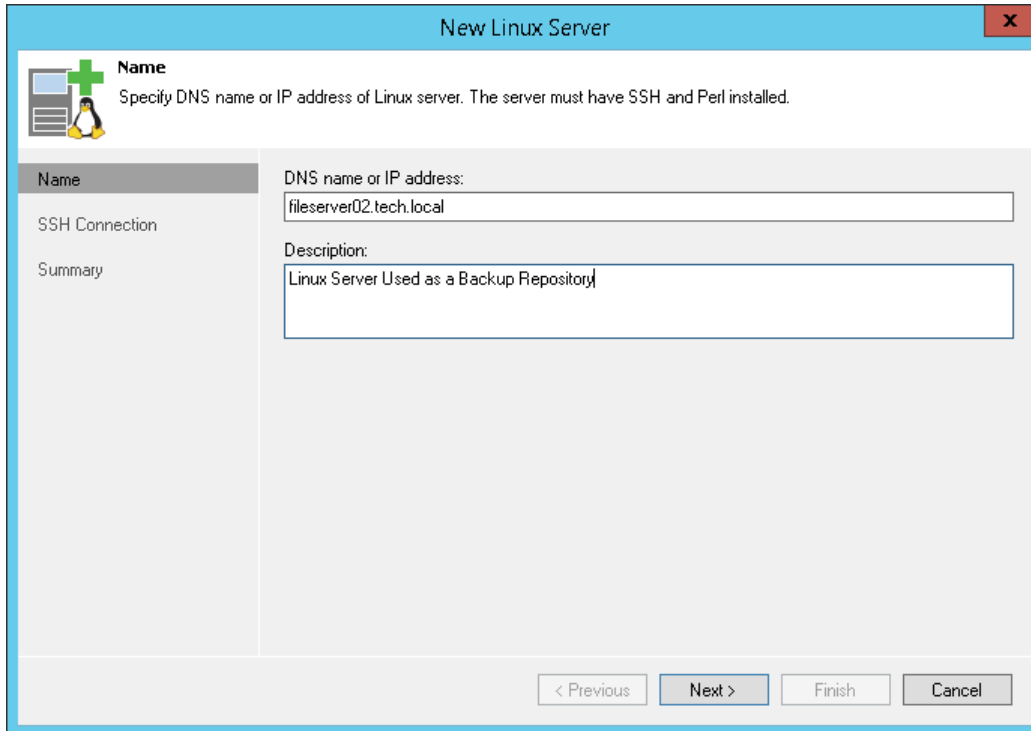
In the **Add Server** window, click **Linux**.



Step 2. Specify Server Name or Address

At the **Name** step of the wizard, specify an address and description for the Linux server.

1. Enter a full DNS name or IP address of the Linux server.
2. 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.



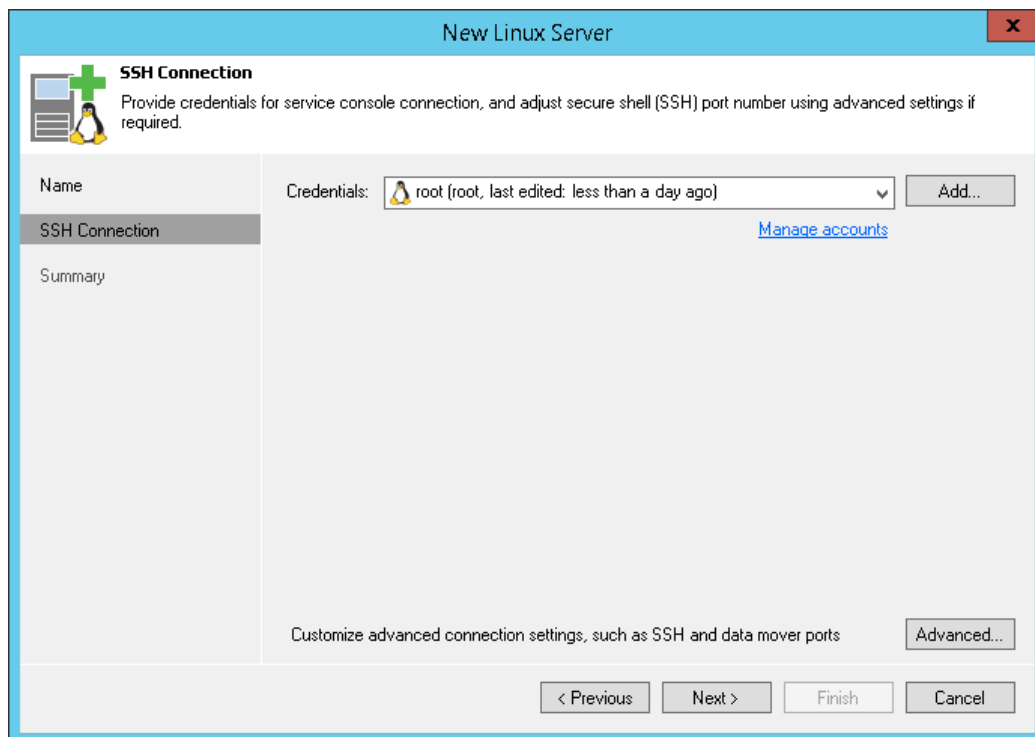
The screenshot shows a window titled "New Linux Server" with a close button (X) in the top right corner. The window has a light blue header bar. Below the header, there is a section with a green plus icon and a penguin icon, followed by the title "Name" and the instruction "Specify DNS name or IP address of Linux server. The server must have SSH and Perl installed." On the left side, there is a sidebar with four items: "Name" (selected), "SSH Connection", "Summary", and "Summary". The main area of the window is divided into two sections. The top section is labeled "DNS name or IP address:" and contains a text input field with the value "fileserver02.tech.local". The bottom section is labeled "Description:" and contains a text input field with the value "Linux Server Used as a Backup Repository". At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Credentials and SSH Port

At the **SSH Connection** step of the wizard, specify credentials for the Linux server.

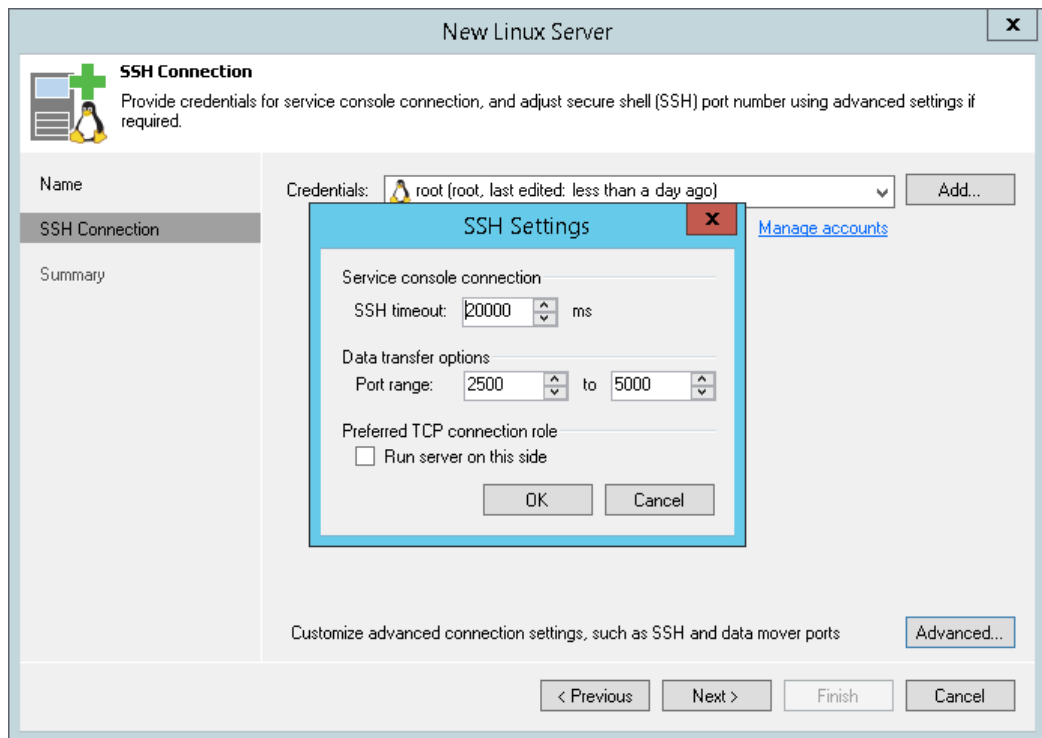
1. From the **Credentials** list, select credentials for the account that has administrator privileges on the Linux server. You can select a credentials record that uses the password authentication method or credentials record that uses the Identity/Pubkey authentication method.

If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).



The screenshot shows the 'New Linux Server' wizard window. The title bar is 'New Linux Server'. The main window has a blue header with a green plus icon and the text 'SSH Connection'. Below the header, it says 'Provide credentials for service console connection, and adjust secure shell (SSH) port number using advanced settings if required.' On the left, there is a sidebar with 'Name', 'SSH Connection', and 'Summary'. The 'SSH Connection' section is selected. In the main area, there is a 'Credentials:' dropdown menu showing 'root (root, last edited: less than a day ago)' and an 'Add...' button. Below the dropdown is a link 'Manage accounts'. At the bottom of the main area, there is a text 'Customize advanced connection settings, such as SSH and data mover ports' and an 'Advanced...' button. At the very bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

2. To configure advanced SSH settings, click **Advanced**.
 - a. In the **Service console connection** section, specify an SSH timeout. By default, the SSH timeout is set to 20000 ms. If a task targeted at the Linux server is inactive after the specified timeout, Veeam Backup Free Edition will automatically terminate the task.
 - b. In the **Data transfer options** section of the **Network Settings** window, specify connection settings for file copy operations. Provide a range of ports that will be used as transmission channels between the source host and target host (one port per task). By default, Veeam Backup Free Edition uses port range 2500-5000. If the virtual environment is not large and data traffic will not be significant, you can specify a smaller range of ports, for example, 2500-2510 to run 10 concurrent jobs at the same time.
 - c. If the Linux server is deployed outside NAT, in the **Preferred TCP connection role** section select the **Run server on this side** check box. In the NAT scenario, the outside client cannot initiate a connection to the server on the NAT network. As a result, services that require initiation of the connection from outside can be disrupted. With this option selected, you will be able to overcome this limitation and initiate a 'server-client' connection — that is, a connection in the direction of the Linux server.



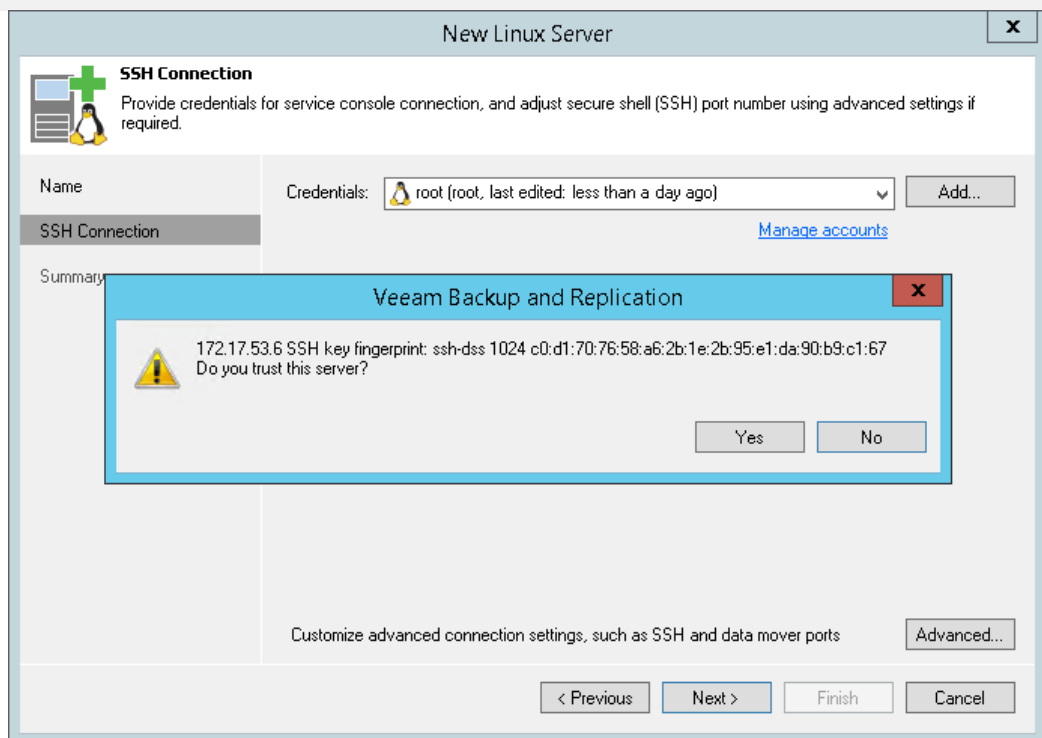
3. When you add a Linux server, Veeam Backup Free Edition saves a fingerprint of the Linux host SSH key to the configuration database. During every subsequent connection to the server, Veeam Backup Free Edition uses the saved fingerprint to verify the server identity and avoid the man-in-the-middle attack.

To let you identify the server, Veeam Backup Free Edition 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 Free Edition will display an error message, and you will not be able to connect to the server.

Note:

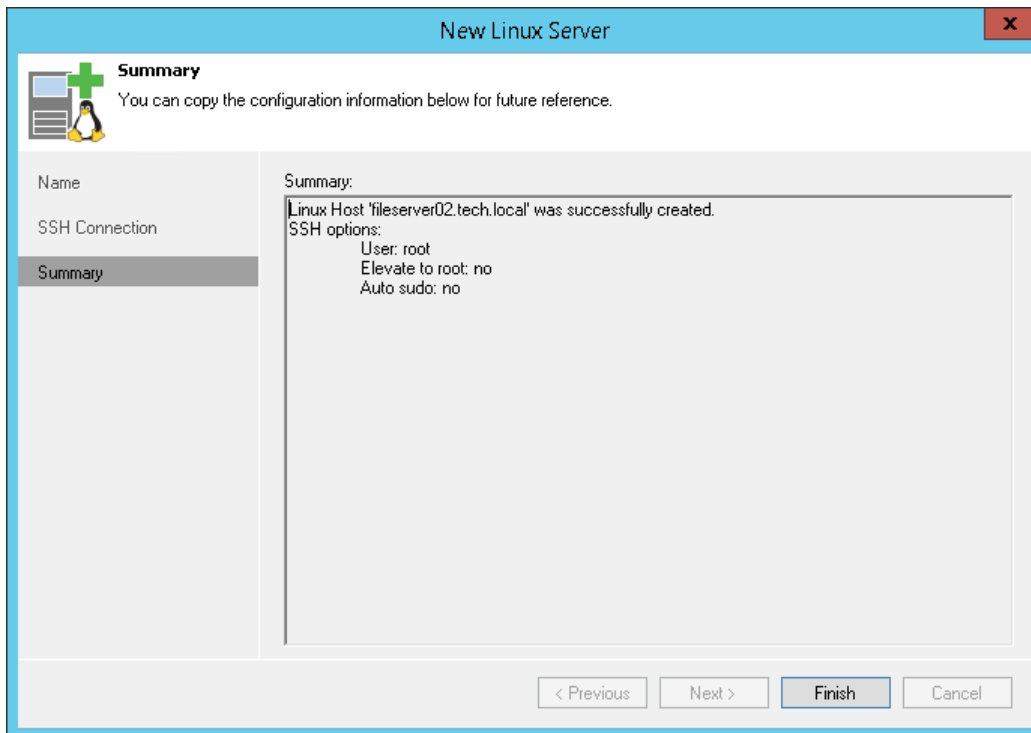
If you update the SSH key on the server, you must acknowledge the new key in the server connection settings. To do this, in the **Backup Infrastructure** view open the server settings, pass through the **Edit Server** wizard and click **Trust** to acknowledge the new key.



Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of Linux server adding.

1. Review details of the Linux server.
2. Click **Next**, then click **Finish** to exit the wizard.



Adding Microsoft SMB3 Servers

Veeam Backup Free Edition supports Microsoft Hyper-V VMs whose disks reside on Microsoft SMB3 file shares and lets you create VeeamZIP files for such VMs.

To work with VMs residing on Microsoft SMB3 file shares, you must add to the backup infrastructure the following components:

- Microsoft Hyper-V host on which VMs are registered
- Microsoft SMB3 server or cluster hosting shared folders with VM disks

Before adding a Microsoft SMB3 server or cluster, [check prerequisites](#). Then use the **New SMB3 Server** wizard to add the server or cluster.

Before You Begin

Before you add a Microsoft SMB3 server or cluster to the backup infrastructure, check the following prerequisites:

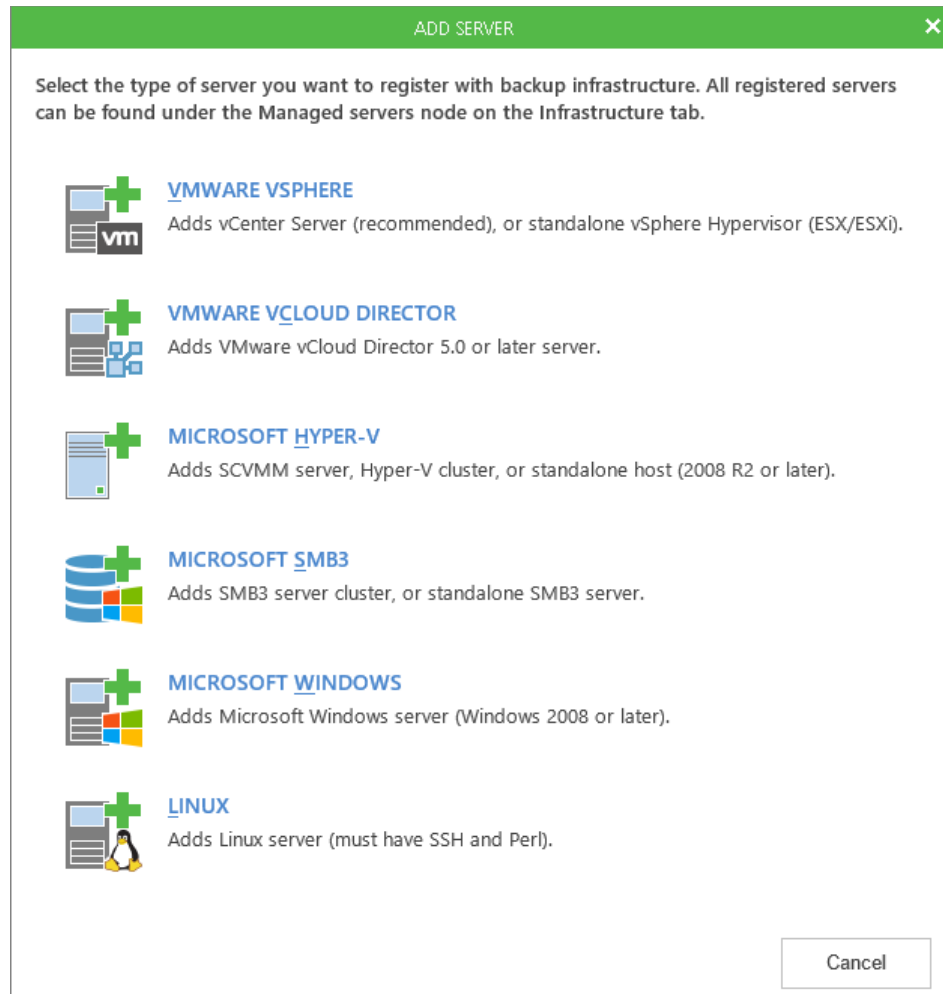
1. Microsoft SMB3 servers must run Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2. Veeam Backup Free Edition supports only these types of Microsoft SMB3 servers.
2. Microsoft SMB3 shared folders must be properly configured. For a full list of requirements for Microsoft SMB3 shared folders, see the *Requirements* and supported configurations section at <http://technet.microsoft.com/en-us/library/jj612865.aspx>.
3. VMs must not reside on hidden shared folders or default shared folders such as C\$ or D\$. When re-scanning Microsoft SMB3 file shared folders, Veeam Backup Free Edition skips these types of folders.
4. To read/write data from/to an SMB3 share, Veeam Backup Free Edition uses the account that you provide when adding the Microsoft SMB3 server or cluster. Make sure that this account has Full Control permissions in the security settings for SMB3 shares configured on the scale-out file server.

Step 1. Launch New SMB3 Server Wizard

To launch the **New SMB3 Server** wizard, do either of the following:

- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. Then click **Add Server** on the toolbar.
- Open the **Virtual Machines** view, in the inventory pane right-click the **Infrastructure** node and select **Add server**.
- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. In the working area, click **Add Server**.

In the **Add Server** window, click **Microsoft SMB3**.



Step 2. Specify Server Name or Address

At the **Name** step of the wizard, specify an address and description for the Microsoft SMB3 server or cluster.

1. Enter a full DNS name or IP address of the Microsoft SMB3 server or cluster.
2. 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.

New SMB3 Server

Name
Specify DNS name or IP address of Microsoft SMB3 server.

Name

Type

Credentials

Apply

Result

Summary

DNS name or IP address:
smb01.tech.local

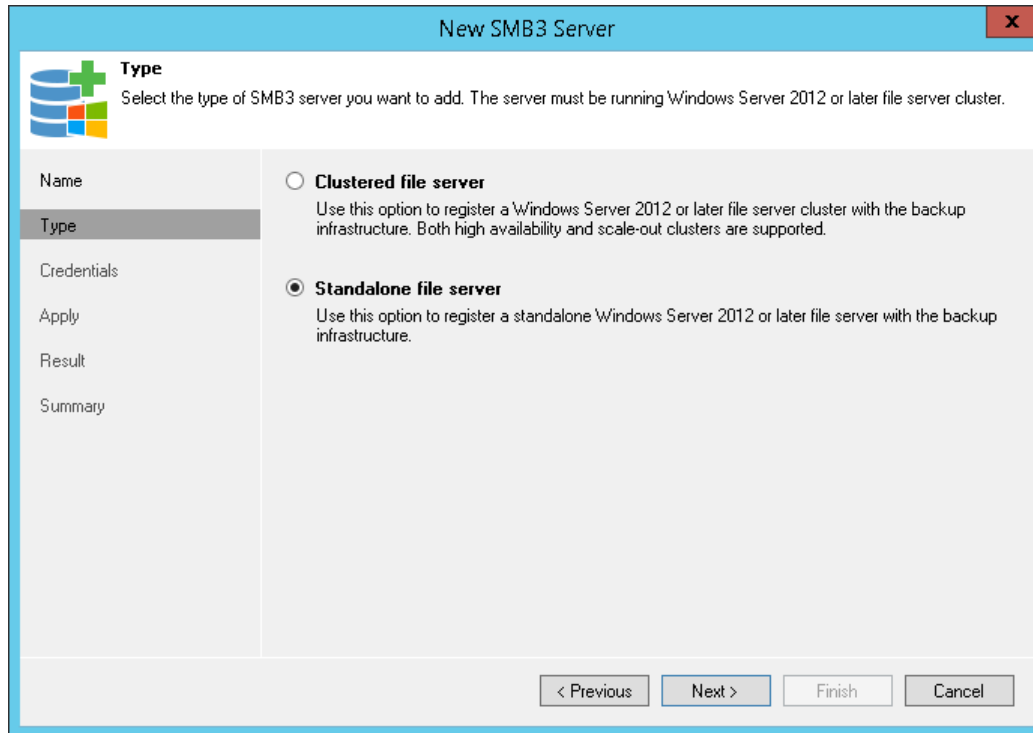
Description:
SMB Server with VMs

< Previous Next > Finish Cancel

Step 3. Specify Server Type

At the **Type** step of the wizard, select what type of Microsoft SMB3 server you want to add.

- Select **Clustered file server** if you want to add a Microsoft SMB3 cluster to the backup infrastructure. Veeam Backup Free Edition supports high availability and scale-out Microsoft SMB3 clusters.
- Select **Standalone file server** if you want to add a standalone Microsoft SMB3 server to the backup infrastructure.



The screenshot shows the 'New SMB3 Server' wizard window. The title bar is 'New SMB3 Server'. The main area is titled 'Type' and contains the instruction: 'Select the type of SMB3 server you want to add. The server must be running Windows Server 2012 or later file server cluster.' On the left, there is a sidebar with a list of steps: Name, Type (selected), Credentials, Apply, Result, and Summary. In the main area, there are two radio button options: 'Clustered file server' (unselected) and 'Standalone file server' (selected). Below each option is a brief description. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

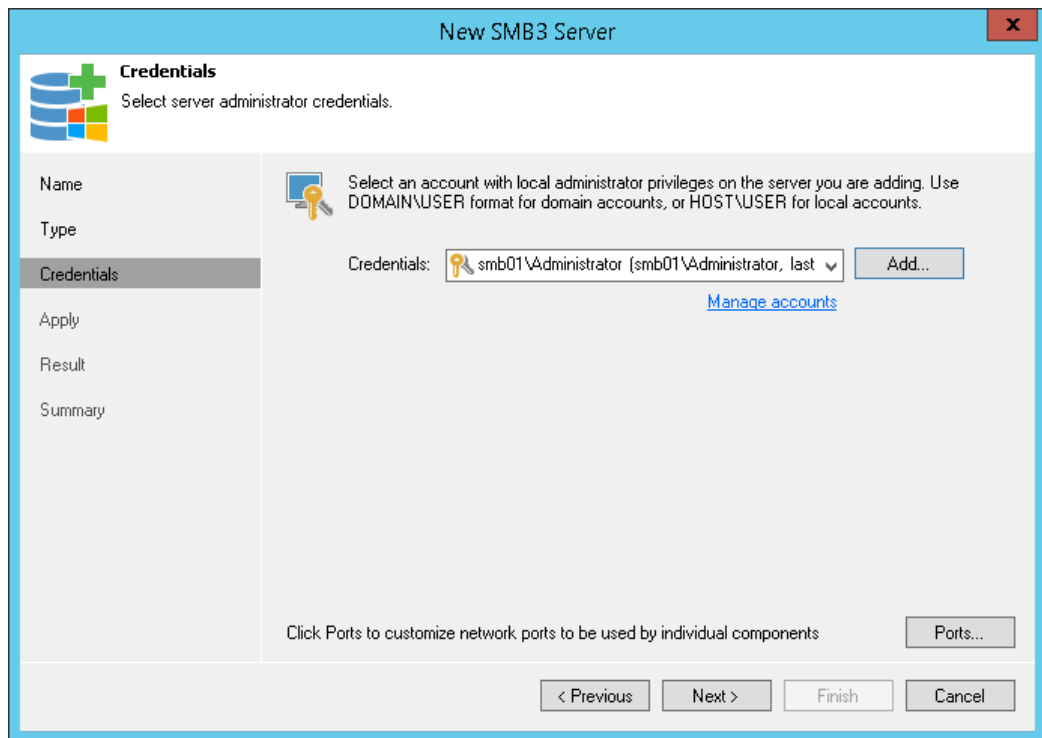
Step 4. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for the Microsoft SMB3 server or cluster.

1. From the **Credentials** list, select credentials for the account that has administrator privileges on the Microsoft SMB3 server or cluster. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).
 - For domain user accounts, the user name must be specified in the *DOMAIN\USERNAME* format.
 - For local user accounts, the user name must be specified in the *HOSTNAME\USERNAME* format.

Veeam Backup Free Edition will use the provided credentials to deploy the following components on the Microsoft SMB3 server or cluster nodes:

- Veeam Installer Service
- Veeam Data Mover Service (Transport)
- Veeam Hyper-V Integration Service



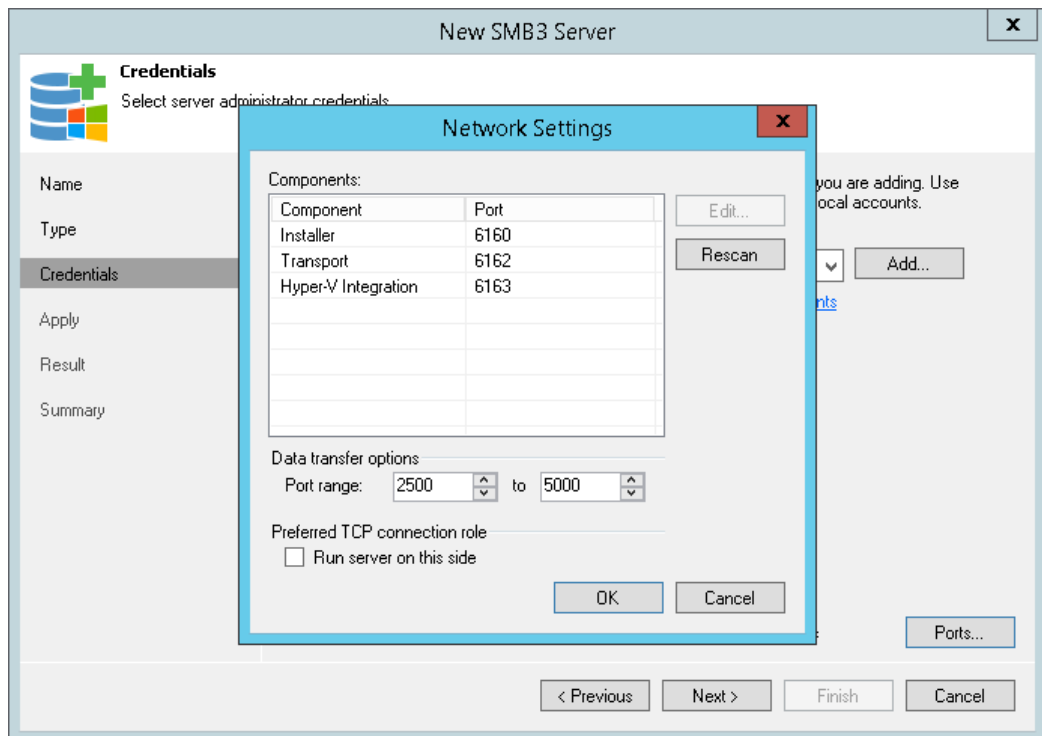
2. To customize network ports used by Veeam Backup Free Edition components, click **Ports**. By default, Veeam Backup Free Edition components use the following ports:

- Veeam Installer Service: port 6160
- Veeam Data Mover Service (Transport): port 6162
- Veeam Hyper-V Integration Service: port 6163

If necessary, adjust port numbers.

3. In the **Data transfer options** section of the **Network Settings** window, specify connection settings for file copy operations. Provide a range of ports that will be used as transmission channels between the source server and target server (one port per task). By default, Veeam Backup Free Edition uses port range 2500-5000. If the virtual environment is not large and data traffic will not be significant, you can specify a smaller range of ports, for example, 2500-2510 to run 10 concurrent jobs at the same time.

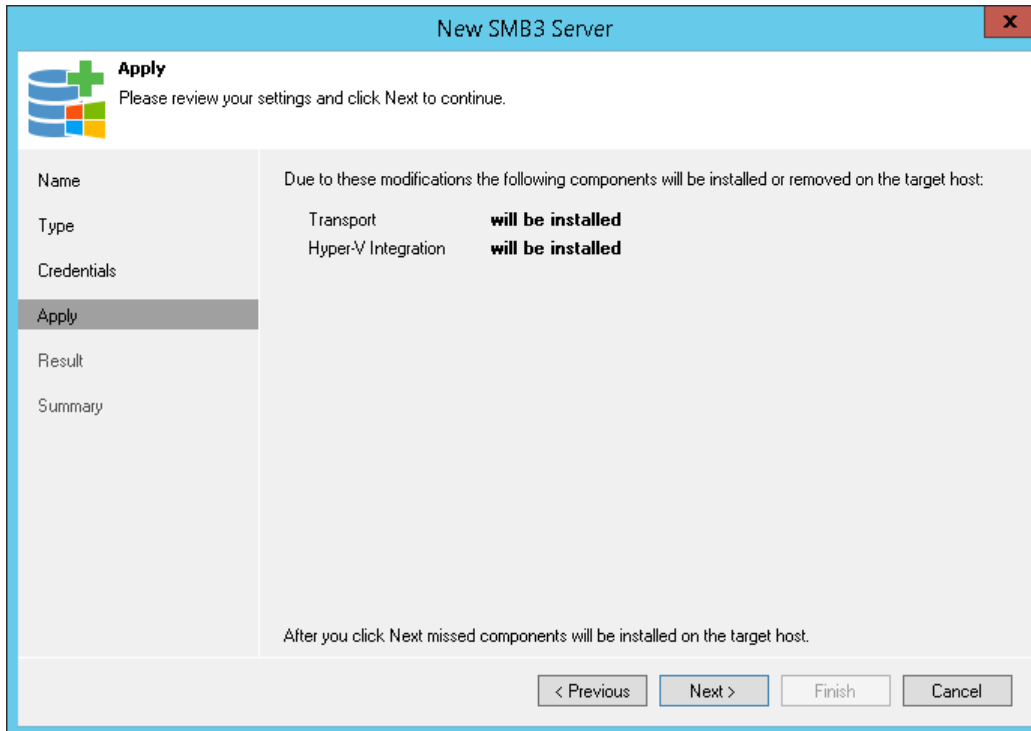
4. If the Microsoft SMB3 server or cluster is deployed outside NAT, in the **Preferred TCP connection role** section select the **Run server on this side** check box. In the NAT scenario, the outside client cannot initiate a connection to the server on the NAT network. As a result, services that require initiation of the connection from outside can be disrupted. With this option selected, you will be able to overcome this limitation and initiate a 'server-client' connection — that is, a connection in the direction of the Microsoft SMB3 server or cluster.



Step 5. Review Components

At the **Apply** step of the wizard, review what Veeam Backup Free Edition components are already installed on the server and what components will be installed.

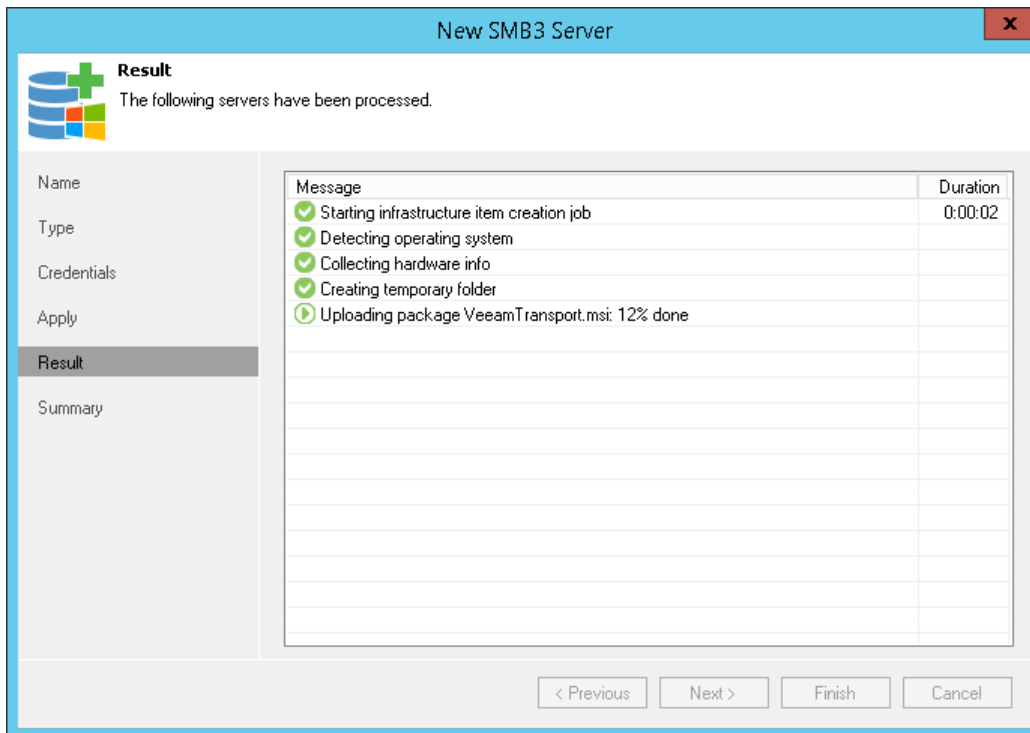
1. Review the components.
2. Click **Next** to add the Microsoft SMB3 server or cluster to the backup infrastructure.



Step 6. Finish Working with Wizard

At the **Result** step of the wizard, complete the procedure of Microsoft SMB3 server or cluster adding.

1. Review details of the Microsoft SMB3 server or cluster.
2. Click **Next**, then click **Finish** to exit the wizard.



Step 7. Configure SMB3 Shares

After you have added a Microsoft SMB3 server, you can configure the following settings for shared folders hosted on this server:

- Enable or disable changed block tracking
- Define the number of concurrent Hyper-V snapshots for a shared folder

Before you specify settings for a Microsoft SMB3 server, you must perform a rescan operation for shared folders on this server. During the rescan operation, Veeam Backup Free Edition retrieves information about shared folders that are currently hosted on a Microsoft SMB3 server, updates the list of shared folders and writes this information to the Veeam Backup Free Edition database.

Veeam Backup Free Edition automatically rescans the list of shared folders once a day. You can also start the rescan operation manually:

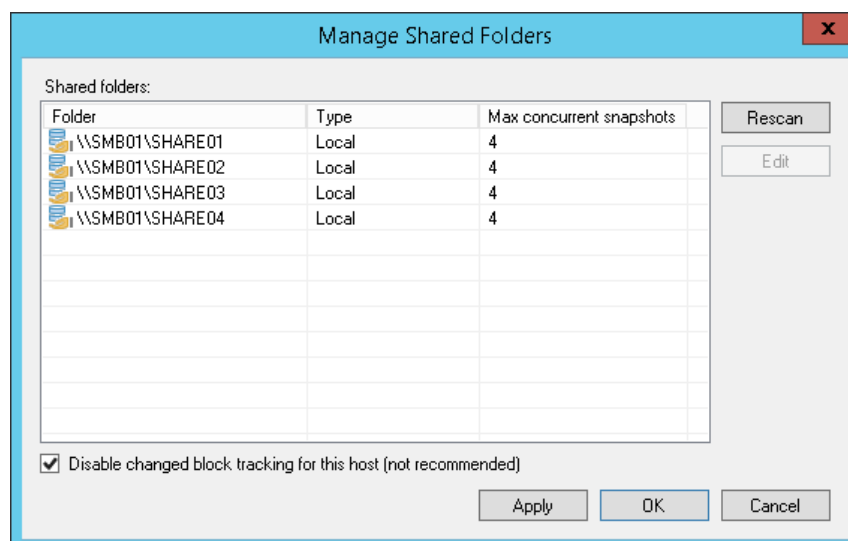
1. Open the **Files** view.
2. Click the **SMB Servers** node in the inventory tree.
3. Select the necessary Microsoft SMB3 server in the working area and click **Rescan** on the ribbon. Alternatively, you can right-click the necessary Microsoft SMB3 server in the working area and select **Rescan**.

Changed Block Tracking Settings

By default, Veeam Backup Free Edition enables changed block tracking for processing all VMs that reside on shared folders hosted by a Microsoft SMB3 server. You may disable changed block tracking, for example, for testing purposes.

Change block tracking is enabled and disabled at the level of a Hyper-V host. To disable changed block tracking:

1. Open the **Files** view.
2. Click the **SMB Servers** node in the inventory tree.
3. Select the necessary Microsoft SMB3 server in the working area and click **Manage Volumes** on the ribbon. Alternatively, you can right-click the necessary Microsoft SMB3 server in the working area and select **Manage Volumes**.
4. In the **Manage Volumes** window, select the **Disable changed block tracking for this host** check box.

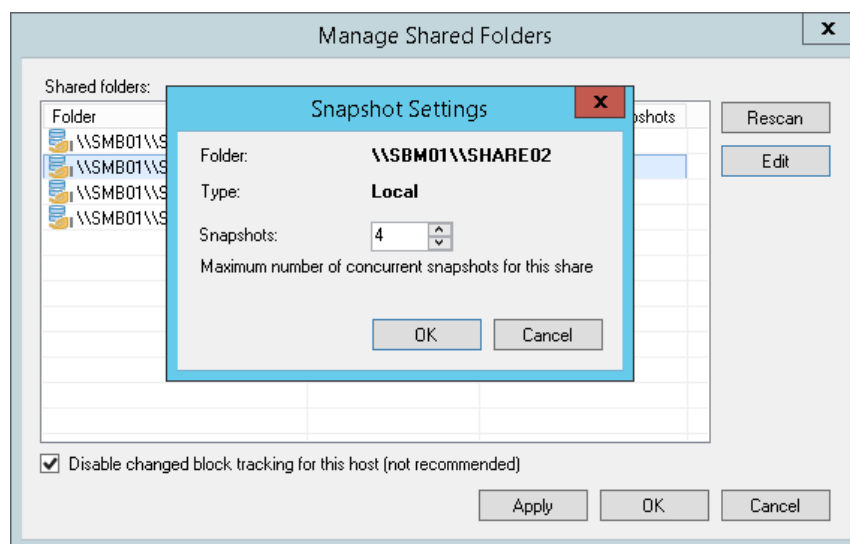


Shared Folder Settings

You can specify the maximum number of concurrent Hyper-V snapshots that must exist for a shared folder hosted by a Microsoft SMB3 server.

To specify shared folder settings:

1. Open the **Files** view.
2. Click the **SMB Servers** node in the inventory tree.
3. Select the necessary Microsoft SMB3 server in the working area and click **Manage Volumes** on the ribbon. Alternatively, you can right-click the necessary Microsoft SMB3 server in the working area and select **Manage Volumes**.
4. Select the necessary shared folder in the list and click **Edit**.
5. By default, tasks working with the same shared folder can take up to 4 snapshots of a folder simultaneously. If necessary, you can increase or decrease the number of snapshots that can exist at the same time. It is not recommended to increase the number of snapshots for slow storage: a great number of snapshots existing at the same time may cause VM processing failures.



Adding vCloud Director

To work with vApps and VMs managed by VMware vCloud Director, you must add VMware vCloud Director to the backup infrastructure.

After you add VMware vCloud Director to the backup infrastructure, the VMware vCloud Director hierarchy is displayed in the **Virtual Machines > View > vCloud Director** view in Veeam Backup Free Edition. You can work with VMs managed by VMware vCloud Director directly from the Veeam Backup Free Edition console.

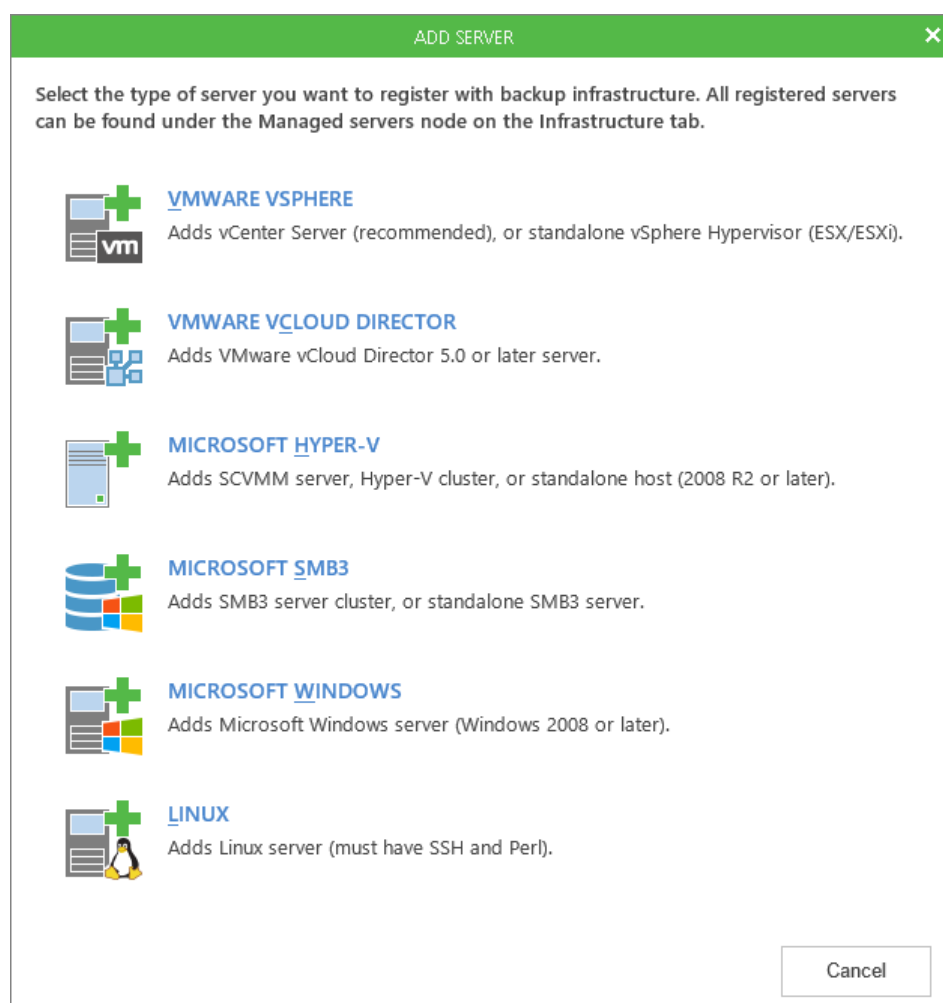
To add the VMware vCloud Director host, use the **New VMware vCloud Director** wizard.

Step 1. Launch New VMware vCloud Director Wizard

To launch the **New VMware vCloud Director** wizard:

- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. Then click **Add Server** on the toolbar.
- Open the **Virtual Machines** view, in the inventory pane right-click the **Infrastructure** node and select **Add server**.
- Open the **Virtual Machines** view, in the inventory pane select the **Infrastructure** node. In the working area, click **Add Server**.

In the **Add Server** window, select **VMware vCloud Director**.



Step 2. Specify Server Name or Address

At the **Name** step of the wizard, specify connection settings for the VMware vCloud Director. If the VMware vCloud Director infrastructure comprises several cells, you can specify connection settings for any cell in the VMware vCloud Director hierarchy.

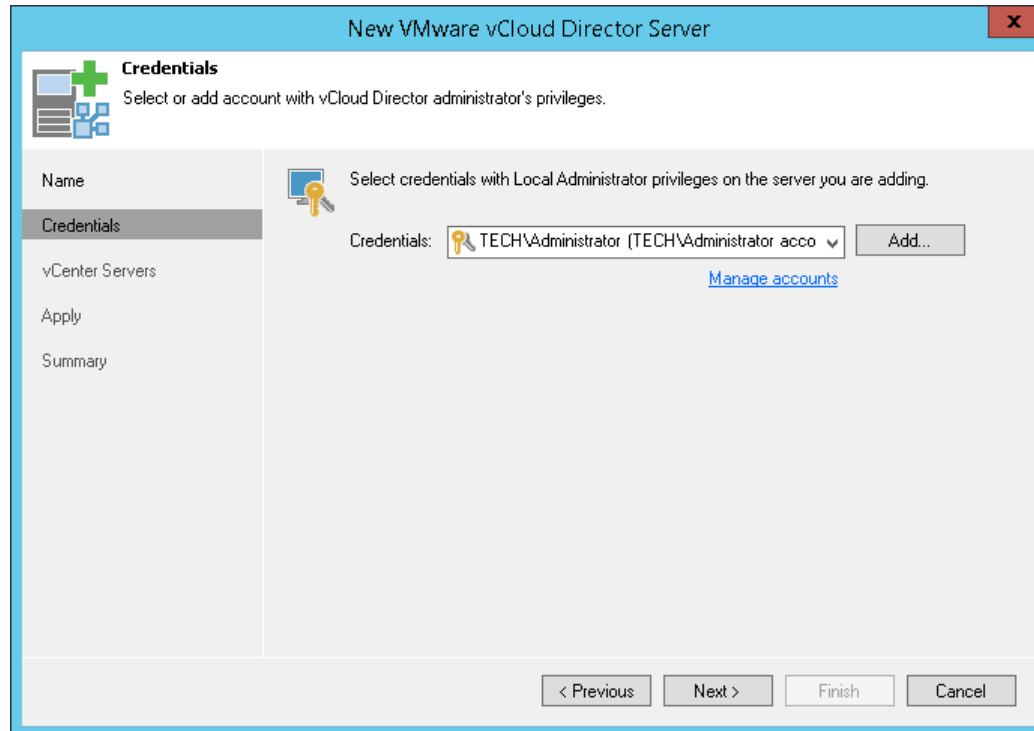
1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the VMware vCloud Director server or any cell in the VMware vCloud Director infrastructure.
2. In the **URL** field, enter a URL of the VMware vCloud Director server. By default, Veeam Backup Free Edition uses the following URL: `https://<vcdservername>:443`, where `<vcdservername>` is the name or IP address of the VMware vCloud Director server that you have specified in the field above and 443 is the default port for communication with VMware vCloud Director.
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.

The screenshot shows the 'New VMware vCloud Director Server' wizard window. The title bar is blue with a red close button. The main area is white with a blue header bar. The header bar contains a green plus icon and the text 'Name'. Below the header bar, the text 'Specify DNS name or IP address of VMware vCloud Director server.' is displayed. The main area is divided into two sections. The left section is a sidebar with a list of steps: 'Name', 'Credentials', 'vCenter Servers', 'Apply', and 'Summary'. The 'Name' step is selected and highlighted. The right section contains three input fields: 'DNS name or IP address:' with the value '172.17.42.16', 'URL:' with the value 'https://172.17.42.16:443', and 'Description:' with the value 'vCloud Director'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 3. Specify vCloud Director Credentials

At the **Credentials** step of the wizard, specify credentials to connect to the VMware vCloud Director.

From the **Credentials** list, select credentials for the account that has administrator privileges on VMware vCloud Director. If you have not set up credentials beforehand, click the **Manage accounts** link at the bottom of the list or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).



Step 4. Specify Credentials for Underlying vCenter Servers

At the **vCenter Servers** step of the wizard, specify credentials for every VMware vCenter Server added to VMware vCloud Director. If the VMware vCenter Server is already added to the backup infrastructure, you do not need to specify credentials for it once again. Veeam Backup Free Edition will automatically detect the credentials you provided when adding this vCenter Server and use them.

1. From the **vCenter servers** list, select a VMware vCenter Server.
2. Click **Account** on the right and select credentials to connect to the VMware vCenter Server. By default, Veeam Backup Free Edition uses the same credentials that you have specified for VMware vCloud Director at the previous step of the wizard.

If you have not set up the credentials beforehand, click the **Manage accounts** link at the bottom of the list or click **Add** on the right to add the credentials. For more information, see [Managing Credentials](#).

3. Veeam Backup Free Edition automatically detects a port used to communicate with the VMware vCenter Server. If necessary, you can change the connection port for the VMware vCenter Server. Click **vCenter** on the right and adjust the port number.
4. When you add a VMware vCenter Server, Veeam Backup Free Edition saves a thumbprint of the SSL certificate installed on the VMware vCenter Server to the configuration database. During every subsequent connection to the server, Veeam Backup Free Edition uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

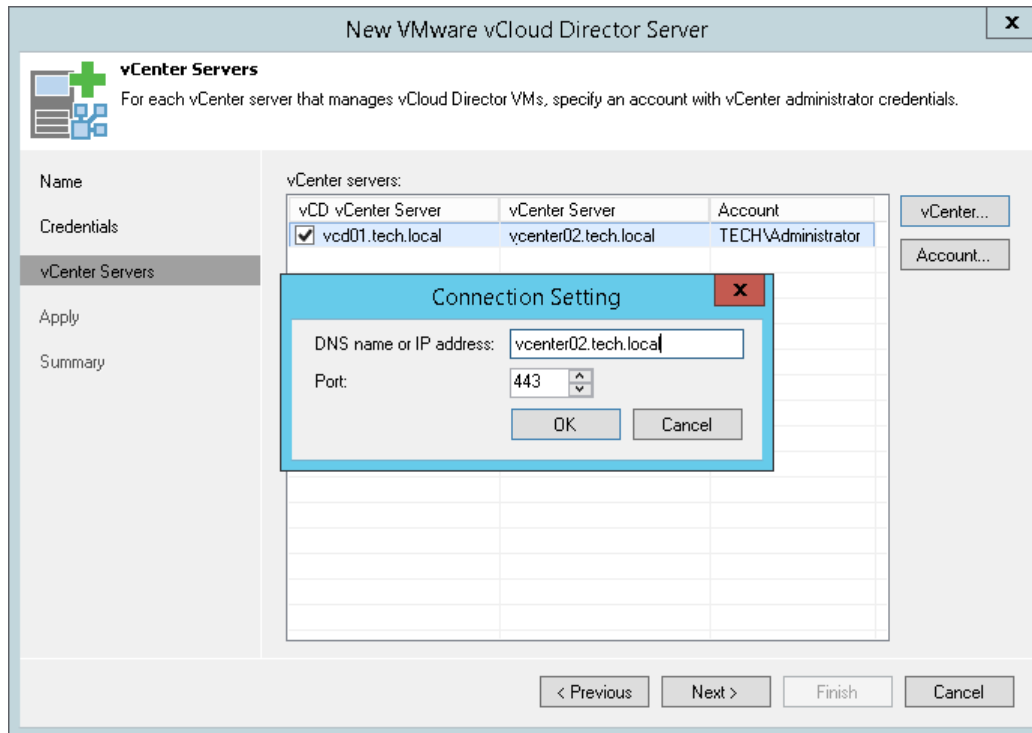
If the certificate installed on the server is not trusted, Veeam Backup Free Edition displays a warning.

- If you trust the server, click **Connect**.
- If you do not trust the server, click **Cancel**. Veeam Backup Free Edition will display an error message, and you will not be able to connect to the server.

5. Repeat steps 1-3 for all VMware vCenter Servers added to vCloud Director.

Note:

After you update the certificate on the server, you must acknowledge the new certificate in the server connection settings. To do this, in the **Backup Infrastructure** view open the server settings, pass through the **Edit Server** wizard and click **Trust** to acknowledge the key.

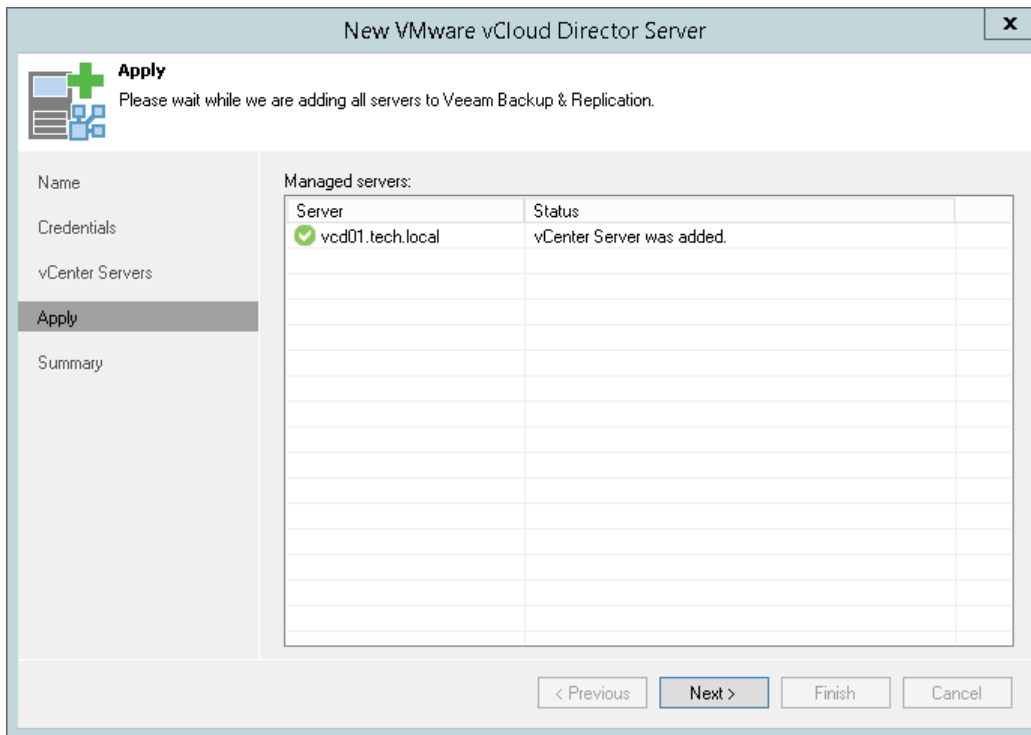


Step 5. Finish Working with Wizard

At the **Apply** step of the wizard, complete the procedure of VMware vCloud Director adding.

1. Review details of the VMware vCloud Director.
2. Click **Next**, then click **Finish** to exit the wizard.

If VMware vCenter Servers underlying VMware vCloud Director are already added to the backup infrastructure, they will not be added for the second time. Veeam Backup Free Edition will create associations with the VMware vCenter Servers and display them in the VMware vCloud Director hierarchy.



Managing Servers

You can edit settings of added servers, update server components and remove server from Veeam Backup Free Edition.

In This Section

- [Updating Server Components](#)
- [Editing Server Settings](#)
- [Removing Servers](#)

Updating Server Components

Every time you launch Veeam Backup Free Edition, Veeam Backup Free Edition automatically checks if components installed on managed servers are up to date. If a later version of a component is available, Veeam Backup Free Edition displays the **Components Update** window and prompts you to upgrade components on managed servers. Components upgrade may be necessary, for example, after you have upgraded the Veeam Backup Free Edition console.

You manually check if components upgrade is required. To do so, select **Upgrade** from the main menu. If components on all managed servers are up to date, the menu item will be disabled.

To upgrade components on managed servers:

1. In the **Components Update** window, select a server and click **Details**. Veeam Backup Free Edition will display the current and latest available versions for installed components.
2. In the **Components Update** window, select check boxes next to servers for which you want to upgrade components and click **Next**.

You can update components on every managed server separately. If components installed on the server require upgrade, Veeam Backup Free Edition displays a warning icon next to the server in the management tree.

To update components for a managed server:

1. Open the **Files** view.
2. Select the **VMware vSphere** or **Microsoft Hyper-V** node in the inventory pane.
3. Select the necessary server in the working area and click **Upgrade** on the ribbon.

Alternatively, you can open the **Infrastructure** view, select the **Managed Servers** node in the inventory pane, right-click the necessary server in the working area and select **Upgrade**.

Editing Server Settings

To edit settings of a server in the backup infrastructure:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed servers**.
3. In the working area, select the server and click **Edit Server** on the ribbon or right-click the server and select **Properties**.
4. You will follow the same steps as you have followed when adding the server. Edit server settings as required.

Removing Servers

To remove a server from the backup infrastructure, do either of the following:

- Open the **Virtual Machines** view. Select the necessary server in the inventory pane, click the **Server** tab and then click the **Remove Server** button on the toolbar.
- Open the **Virtual Machines** view. Right-click the necessary server in the inventory pane and select **Remove**.

Creating VeeamZIP Files

You can create VeeamZIP files for separate VMs in VMware and Microsoft Hyper-V environments.

Creating VeeamZIP Files for VMware VMs

You can quickly back up running and powered off VMs with VeeamZIP. Creating a VeeamZIP file can be helpful if you want create an ad-hoc backup for VMs, archive VMs before decommissioning and so on.

Prior to performing creating a VeeamZIP file of a VMware VM, check the following prerequisites:

- Make sure that the source host is added to the backup infrastructure.
- Make sure that there is enough space on the backup destination.

Note: In Veeam Backup Free Edition, you can run a VeeamZIP job for one VM only. If you have a valid trial or full license installed, you can run a VeeamZIP job for a number of VMs at a time.

To create a VeeamZIP file, follow the next steps:

1. Open the **Virtual Machines** view.
2. In the infrastructure tree, click the ESX(i) host or VM container in which the necessary VM resides.
3. In the working area, select the necessary VM and click **VeeamZIP** on the ribbon or right-click the necessary VM and select **VeeamZIP**.

To quickly find the necessary VM, type the VM name or a part of it in the search field at the top of the working area and click the **Start search** button on the right or press **[ENTER]**.

4. In the **Destination** section, specify a location in which you want to store the VeeamZIP file.
 - To store the VeeamZIP file in a local folder on the Veeam backup server, select **Local or shared folder**, click **Browse** on the right and select a folder in which the VeeamZIP file must be stored.
 - To store a VeeamZIP file in a shared folder, select **Local or shared folder** and type in the UNC name of the shared folder in the field below. Keep in mind that the UNC name always starts with two back slashes (\\).

If the shared folder requires authentication, select the necessary credentials from the **Credentials** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add necessary credentials. For more information, see [Managing Credentials](#).

5. Use the **Delete this backup automatically** list to specify retention settings for the created VeeamZIP file. By default, VeeamZIP files are not removed and kept in the specified location for an indefinite period of time.
6. To encrypt the created VeeamZIP file, select the **Enable backup file encryption** check box. From the **Password** list, select a password that you want to use to encrypt the VeeamZIP file. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see [Managing Passwords for Data Encryption](#).
7. From the **Compression level** list, select a compression level for the created backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
8. By default, Veeam Backup Free Edition uses VMware Tools quiescence to create a transactionally consistent image of VMs. You can optionally disable VM quiescence. To do this, clear the **Disable guest quiescence** check box. In this case, Veeam Backup Free Edition will create a crash-consistent VM backup.

9. Click **OK**. The VeeamZIP task will start immediately. Veeam Backup Free Edition will create a full backup file (VBK) and store it in the specified location. The VM name, date and time of the file creation are appended to the file name so you can easily find the necessary VeeamZIP file afterwards.
10. As the job runs, you can track the job performance in the real-time mode. To see the job results once it completes, open the **History** view, expand the **Jobs** node and click **Backup**. Then double-click the job session in the list.

Tip:

Veeam Backup Free Edition keeps the settings of the latest VeeamZIP job. To quickly start a VeeamZIP job with the settings of the previous job, right-click the necessary VM and select **VeeamZIP to** from the shortcut menu. The VeeamZIP job will start immediately. The created VeeamZIP file will be stored to the same location as the previously created VeeamZIP file.

The screenshot shows the 'VeeamZIP crm_db (27.7 GB)' configuration window. It includes fields for 'Destination' (\\172.17.22.55\Backups) with a 'Browse...' button, 'Credentials' (TECH\Administrator) with an 'Add...' button and a 'Manage accounts' link. There is a 'Delete this backup automatically' dropdown set to 'Never'. The 'Enable backup file encryption' checkbox is checked, with a 'Password' dropdown (Standard password) and an 'Add...' button, plus a 'Manage passwords' link. 'Loss protection enabled' is checked with a green checkmark. The 'Compression level' is set to 'Optimal (recommended)'. Under 'Guest processing', the 'Disable guest quiescence' checkbox is unchecked. At the bottom are 'Less <<', 'OK', and 'Cancel' buttons.

Creating VeeamZIP Files for Hyper-V VMs

You can quickly back up running and powered off VMs with VeeamZIP. Creating a VeeamZIP file can be helpful if you want create an ad-hoc backup for VMs, archive VMs before decommissioning and so on.

Prior to performing creating a VeeamZIP file of a VMware VM, check the following prerequisites:

- Make sure that the source host is added to the backup infrastructure.
- Make sure that there is enough space on the backup destination.

Note: In Veeam Backup Free Edition, you can run a VeeamZIP job for one VM only. If you have a valid trial or full license installed, you can run a VeeamZIP job for a number of VMs at a time.

To create a VeeamZIP file, follow the next steps:

1. Open the **Virtual Machines** view.
2. In the infrastructure tree, click the Hyper-V host or VM container in which the necessary resides.
3. In the working area, select the necessary VM and click **VeeamZIP** on the ribbon or right-click the necessary VM and select **VeeamZIP**.

To quickly find the necessary VM, type the VM name or a part of it in the search field at the top of the working area and click the **Start search** button on the right or press **[ENTER]**.

4. In the **Destination** section, specify a location in which you want to store the VeeamZIP file.
 - To store the VeeamZIP file in a local folder on the Veeam backup server, select **Local or shared folder**, click **Browse** on the right and select a folder in which the VeeamZIP file must be stored.
 - To store a VeeamZIP file in a shared folder, select **Local or shared folder** and type in the UNC name of the shared folder in the field below. Keep in mind that the UNC name always starts with two back slashes (\\).

If the shared folder requires authentication, select the necessary credentials from the **Credentials** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add necessary credentials. For more information, see [Managing Credentials](#).

5. Use the **Delete this backup automatically** list to specify retention settings for the created VeeamZIP file. By default, VeeamZIP files are not removed and kept in the specified location for an indefinite period of time.
6. To encrypt the created VeeamZIP file, select the **Enable backup file encryption** check box. From the **Password** list, select a password that you want to use to encrypt the VeeamZIP file. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see [Managing Passwords for Data Encryption](#).
7. From the **Compression level** list, select a compression level for the created backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
8. By default, Veeam Backup Free Edition uses native Hyper-V quiescing mechanisms to create a transactionally consistent image of VMs. You can optionally disable VM quiescence. To do this, clear the **Disable guest quiescence** check box. In this case, Veeam Backup Free Edition will create a crash-consistent VM backup.

9. Click **OK**. The VeeamZIP task will start immediately. Veeam Backup Free Edition will create a full backup file (VBK) and store it in the specified location. The VM name, date and time of the file creation are appended to the file name so you can easily find the necessary VeeamZIP file afterwards.
10. As the job runs, you can track the job performance in the real-time mode. To see the job results once it completes, open the **History** view, expand the **Jobs** node and click **Backup**. Then double-click the job session in the list.

Tip:

Veeam Backup Free Edition keeps the settings of the latest VeeamZIP job. To quickly start a VeeamZIP job with the settings of the previous job, right-click the necessary VM and select **VeeamZIP to** from the shortcut menu. The VeeamZIP job will start immediately. The created VeeamZIP file will be stored to the same location as the previously created VeeamZIP file.

The screenshot shows the 'VeeamZIP sqlsrv03 (19.1 GB)' dialog box. It contains the following fields and options:

- Destination:** A text box with the path '\\172.17.22.55\Backups' and a 'Browse...' button.
- Credentials:** A dropdown menu showing 'TECH\Administrator (TECH\Administrator, last edited: 420 days)' and an 'Add...' button. A 'Manage accounts' link is below.
- Delete this backup automatically:** A dropdown menu set to 'Never'.
- Enable backup file encryption:** A checked checkbox.
- Password:** A dropdown menu showing 'Standard password (Last edited: 7 days ago)' and an 'Add...' button. A 'Manage passwords' link is below.
- Loss protection enabled:** A checked green checkbox.
- Compression level:** A dropdown menu set to 'Optimal (recommended)'.
- Guest processing:** A checkbox for 'Disable guest quiescence (performs crash consistent backup)' which is currently unchecked.
- Buttons:** 'Less <<', 'OK', and 'Cancel' at the bottom.

Performing Restore

If important VM data in your production environment gets accidentally corrupted or lost, you can use one of disaster recovery options to restore VM data from VeeamZIP files.

In This Section

- [Performing Restore in VMware vSphere Environment](#)
- [Performing Restore in Microsoft Hyper-V Environment](#)

Performing Restore in VMware vSphere Environment

Veeam Backup Free Edition offers a variety of data recovery options to protect your virtual environment. You can perform recovery using a VeeamZIP file created in Veeam Backup Free Edition or choose a VeeamZIP file or a backup file created with Veeam Backup & Replication. Keep in mind that only a full backup file (VBK) can be used for restore.

Performing Full VM Restore

You can restore an entire VM and start it on the target host if necessary.

A VM can be restored to its original location or to a new location:

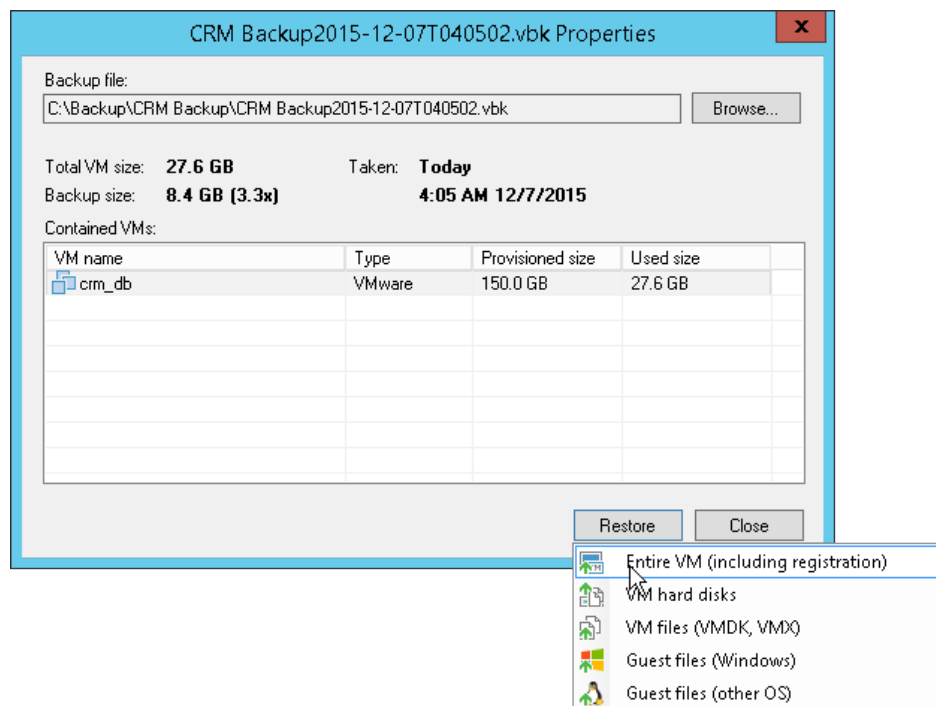
- When you restore a VM to its original location, you keep the original VM settings. This type of restore ensures the quickest recovery and minimizes the number of mistakes that can be caused by changes in VM settings. The primary VM is automatically turned off and deleted before the restore.
- When you restore a VM to a new location, you need to specify new VM settings such as a new VM name, a new host and datastore where the VM will reside, disk format (thin or thick provisioned) and network properties. Veeam Backup Free Edition will change the VM configuration file and store the VM data to the location of your choice.

Step 1. Choose File

You can restore a VM from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

To choose a file:

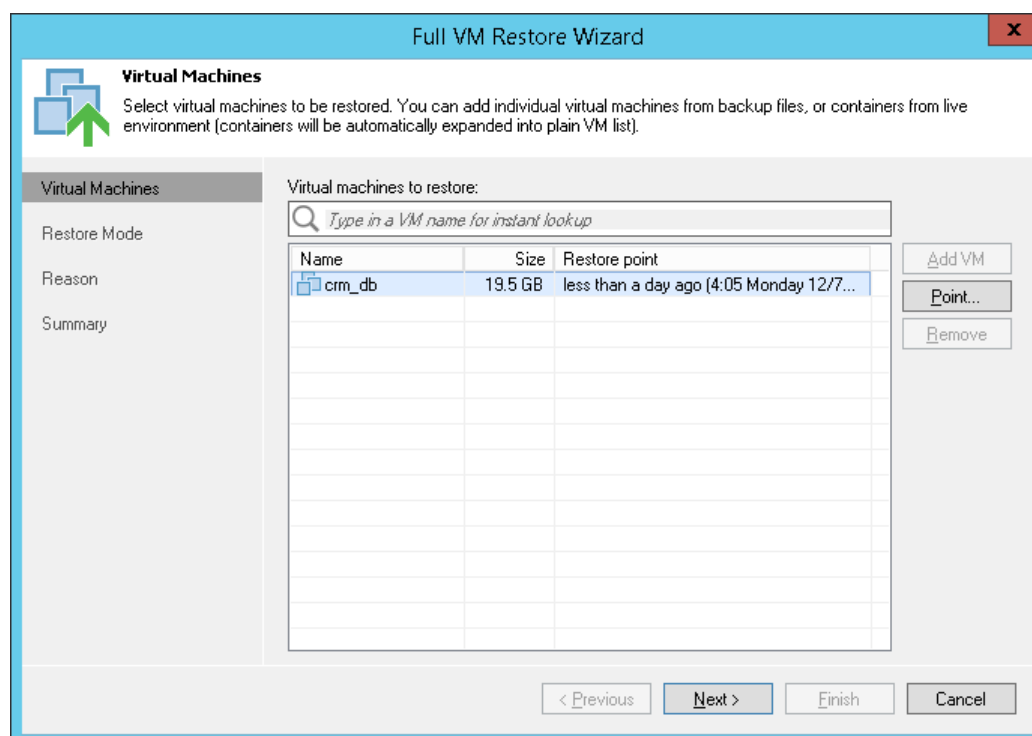
1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM that you want to restore.
3. Click **Restore** and select **Entire VM (including registration)**. The **Full VM Restore** wizard will be launched.



Step 2. Select VM

At the **Virtual Machines** step of the wizard, select the VM that you want to restore and the restore point for the VM.

1. In the **Virtual machines to restore** list, select the VM.
2. Click **Point** on the right.
3. In the **Restore Points** window, select a restore point from which you want to restore the VM.



Step 3. Select Restore Mode

At the **Restore Mode** step of the wizard, choose the necessary restore mode for the VM.

1. Select a restore mode:
 - Select **Restore to the original location** if you want to restore the VM to its original location with its initial settings. If this option is selected, you will immediately pass to **Summary step** of the wizard.
 - Select **Restore to a new location, or with different settings** if you want to restore the VM to a different location and/or with different settings (such as VM location, network settings, the format of restored virtual disks and so on). If this option is selected, the **Full VM Restore** wizard will include additional steps for customizing VM settings.
2. Select the **Restore VM tags** check box if you want to restore tags that were assigned to the original VM, and assign them to the restored VM.
3. [For VM restore to the original location] Select the **Quick rollback** check box if you want to use incremental restore for the VM. Veeam Backup Free Edition will get data blocks that are necessary to revert the VM to an earlier point in time, and will restore only these data blocks from the VeeamZIP file. Incremental restore significantly reduces the restore time and has little impact on the production environment.

It is recommended that you enable this option if you restore a VM after a problem that occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not enable this option if the problem has occurred at the VM hardware level, storage level or due to a power loss.

Note: In Veeam Backup Free Edition, you cannot point a job to a specific backup proxy. Veeam Backup Free Edition uses the default backup proxy configured on the Veeam backup server.

Full VM Restore Wizard

Restore Mode
Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Reason
Summary

☐ **Restore to the original location**
Quickly initiate restore of selected VMs to the original location, and with the original name and settings. This option minimizes the chance of user input error.

☒ **Restore to a new location, or with different settings**
Customize restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the default settings.

☒ **Restore VM tags**
Select this option to restore VM tags that were assigned to the VM when backup was taken.

☐ **Quick rollback (restore changed blocks only)**
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous Next > Finish Cancel

Step 4. Select Destination Host for Restored VM

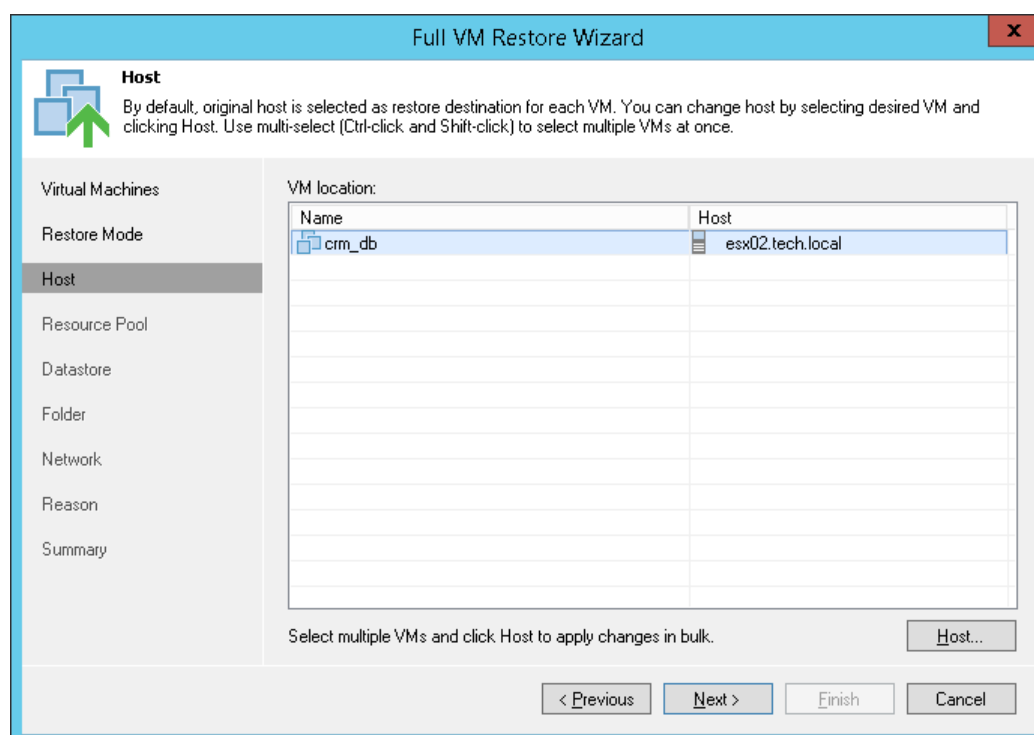
The **Host** step of the wizard is available if you have chosen to change the location and settings for the restored VM.

To specify a destination host:

1. Select a VM in the list and click **Host**. To apply changes in bulk, select several VMs in the list and click **Host**.
2. Choose a host or cluster where the selected VM must be registered.

To facilitate selection, you can use the search field at the bottom of the **Select Host** window:

1. Click the button on the left of the field to select the necessary type of object that should be searched for: *Cluster* or *Host*.
2. Enter an object's name or a part of it and click the **Start search** button on the right or press **[ENTER]**.



Step 5. Select Destination Resource Pool

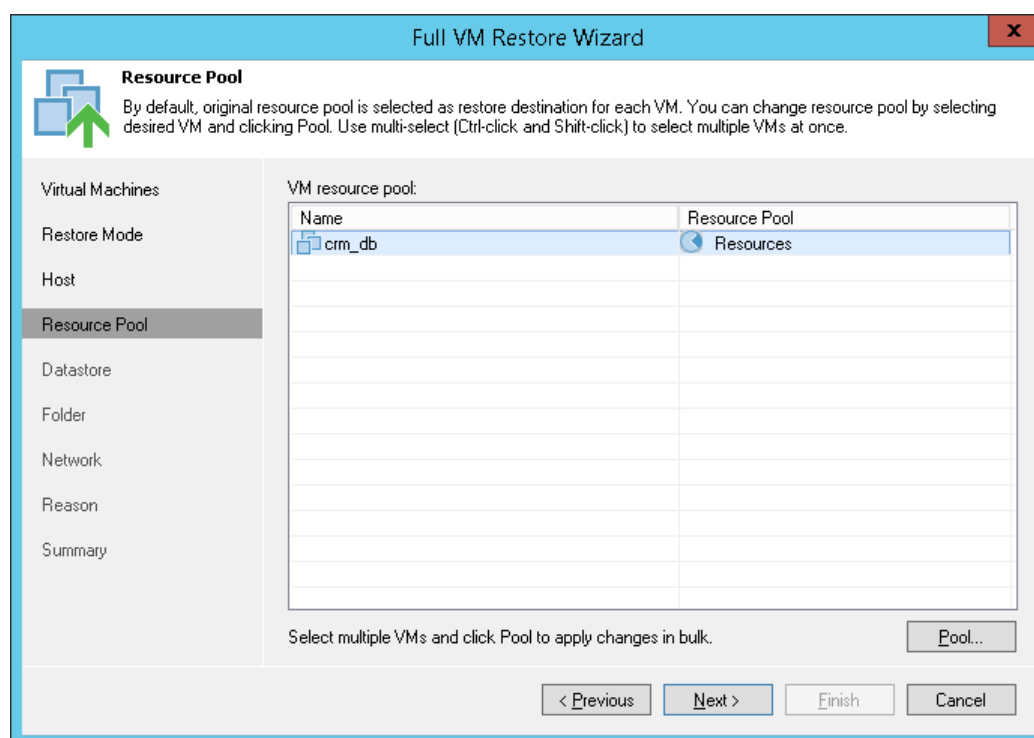
The **Resource Pool** step of the wizard is available if you have chosen to change the location and settings for the restored VM.

To specify a destination resource pool:

1. Select a VM in the list and click **Pool**. To apply changes in bulk, select several VMs in the list and click **Pool**.
2. Select a resource pool to which the VM(s) must be placed.
3. If necessary, select a vApp in which the VM(s) must be included.

To facilitate selection, you can use the search field at the bottom of the **Select Resource Pool** window:

1. Enter a resource pool name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Step 6. Select Destination Datastore

The **Datastore** step of the wizard is available if you have chosen to change the location and settings for the restored VM.

You can place an entire VM to a particular datastore or choose to store configuration files and disk files of the restored VM in different locations.

To specify a destination datastore:

1. Select a VM in the list and click **Datastore**. To apply changes in bulk, select several VMs in the list and click **Datastore**.
2. Point to a datastore where VM files must be stored.

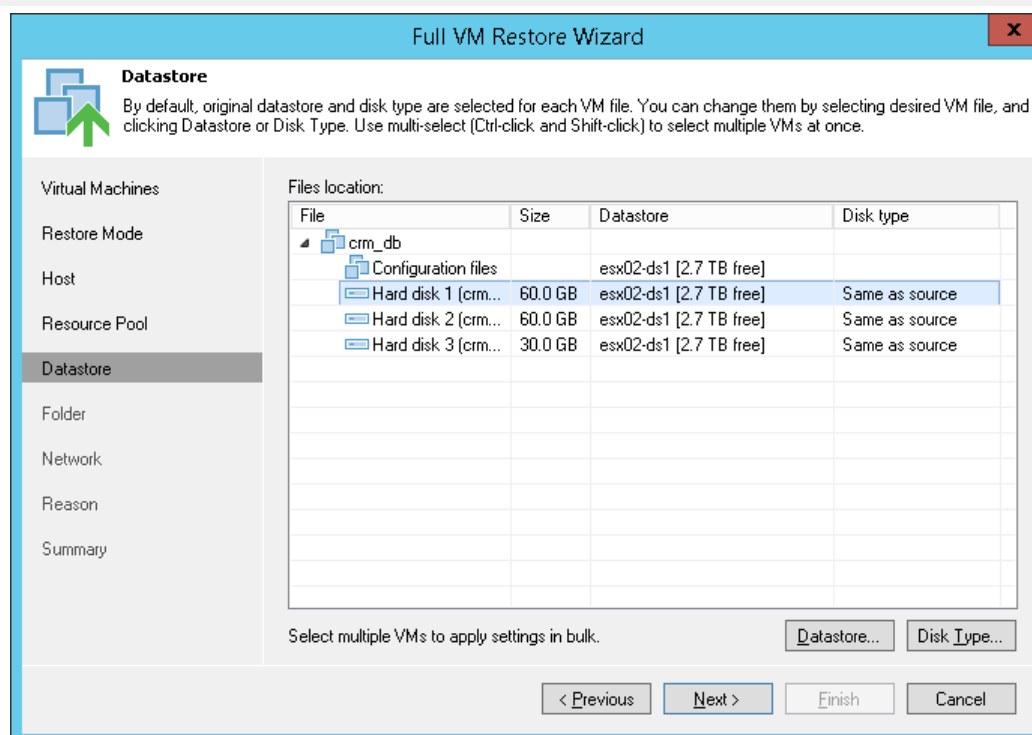
If configuration and disk files of the VM must be placed to different datastores:

1. Expand the VM in the list.
2. Select the necessary file type and click **Datastore**.
3. Select a datastore where the selected objects must be stored. To facilitate selection, you can use the search field at the bottom of the **Select Datastore** window: enter a datastore name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

By default, Veeam Backup Free Edition preserves the format of restored VM disks. If disks of the original VM are provisioned as thick, Veeam Backup Free Edition will restore the VM from the backup with thick disks. If necessary, you can change the disk format of a restored VM.

1. Expand a VM in the list
2. Select the disk and click **Disk Type**.
3. In the **Disk Type Settings** section, choose the format that will be used to restore virtual disks of the VM: same as the source disk, thin or thick.

Note: Disk format change is supported only for VMs with Virtual Hardware version 7 or later.



Step 7. Select Destination Folder and Change VM Names

The **Folder** step of the wizard is available if you have chosen to change the location and settings for the restored VM.

To specify a destination VM folder:

1. Select a VM in the list and click **Folder**.
2. Choose a folder to which the VM will be placed. To facilitate selection, use the search field at the bottom of the window: enter a folder name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

Note: If you restore a VM to a standalone ESX(i) host not managed by vCenter Server, you cannot select a destination folder: this option will be disabled.

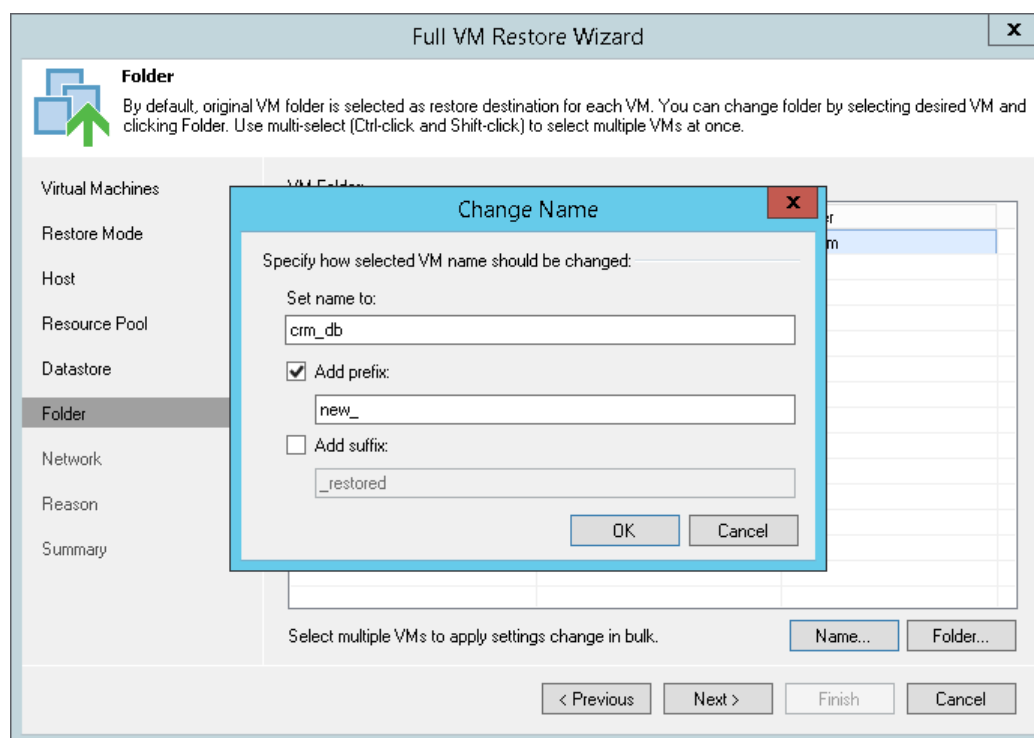
By default, Veeam Backup Free Edition restores a VM with its original name. However, you can change the name of the restored VM. For example, if you restore a VM to its original location, you may need to change its name to avoid potential problems.

To change the VM name:

1. Select a VM in the list and click **Name**.
2. In the **Change Name** section, enter a new name explicitly or specify a change name rule by adding a prefix and/or suffix to the original VM name.

You can change the VM name directly in the list:

1. Select a VM in the list.
2. Click the **New Name** field
3. Enter the name to be assigned to the restored VM.



Step 8. Select Destination Network

The **Network** step of the wizard is available if you have chosen to change the location and settings for the restored VM.

If you plan to restore a VM to a new location, for example, another site with a different set of networks, you can map source site networks to target site networks. Veeam Backup Free Edition will use the network mapping table to update configuration files of the VM on the fly, during the restore process.

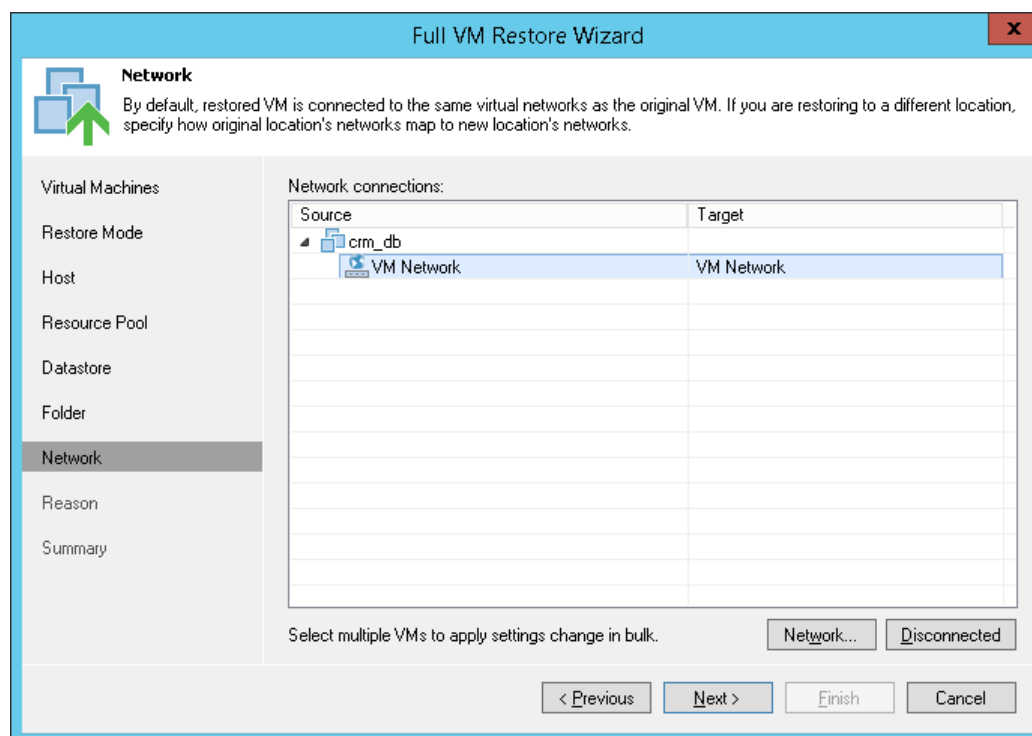
To change networks to which the restored VM will be connected:

1. Select a VM in the list and click **Network**. To apply changes in bulk, select several VMs in the list and click **Network**.

If a VM is connected to multiple networks, expand the VM, select the network to map and click **Network**. The **Select Network** section displays all networks to which the destination host or cluster is connected.

2. From the list of available networks, choose a network to which the VM must have access upon restore. To facilitate selection, use the search field at the bottom of the window: enter a network name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

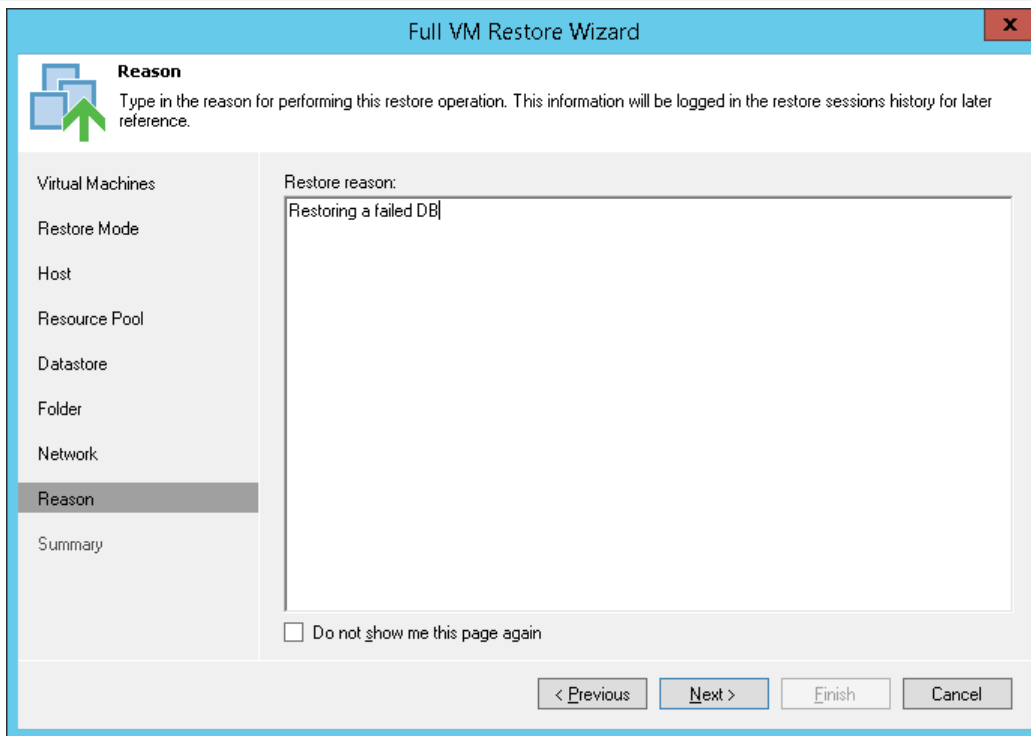
If you do not want to connect the restored VM to any virtual network, select the VM in the list and click **Disconnected**.



Step 9. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the selected VMs. The information you provide will be saved in the session history and you can reference it later.

Tip: If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

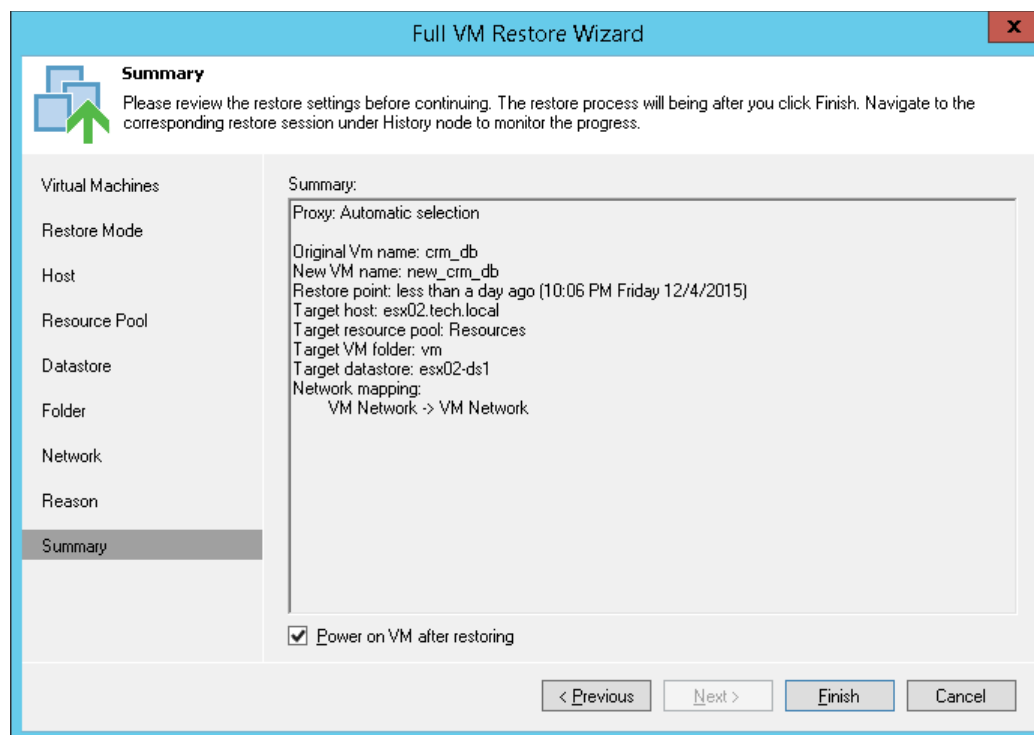


The screenshot shows the 'Full VM Restore Wizard' window, specifically the 'Reason' step. The window has a blue title bar with the text 'Full VM Restore Wizard' and a close button. On the left, there is a vertical list of steps: 'Virtual Machines', 'Restore Mode', 'Host', 'Resource Pool', 'Datastore', 'Folder', 'Network', 'Reason' (which is highlighted with a grey background), and 'Summary'. Above this list, there is a 'Reason' section with a blue icon of two overlapping squares and a green arrow pointing up. The text next to the icon says: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' To the right of the list, there is a large text area labeled 'Restore reason:' containing the text 'Restoring a failed DB'. Below this text area is a checkbox labeled 'Do not show me this page again'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 10. Verify Recovery Settings

At the **Summary** step of the wizard, specify additional settings for VM restore:

1. If you want to start the restored VM on the target host, select the **Power on VM after restoring** check box.
2. Check the specified settings and click **Finish**. Veeam Backup Free Edition will restore selected VMs in the specified destination.



Restoring VM Hard Disks

If a VM hard drive becomes corrupted for some reason (for example, with a virus), you can restore it from the VM backup or VeeamZIP file. You can attach the recovered hard drive to the original VM as a new drive, replace the corrupted drive of the original VM with it or connect it to any other VM. With the virtual drive restore, you can preserve the format of a recovered drive or convert the drive to the thin or thick format.

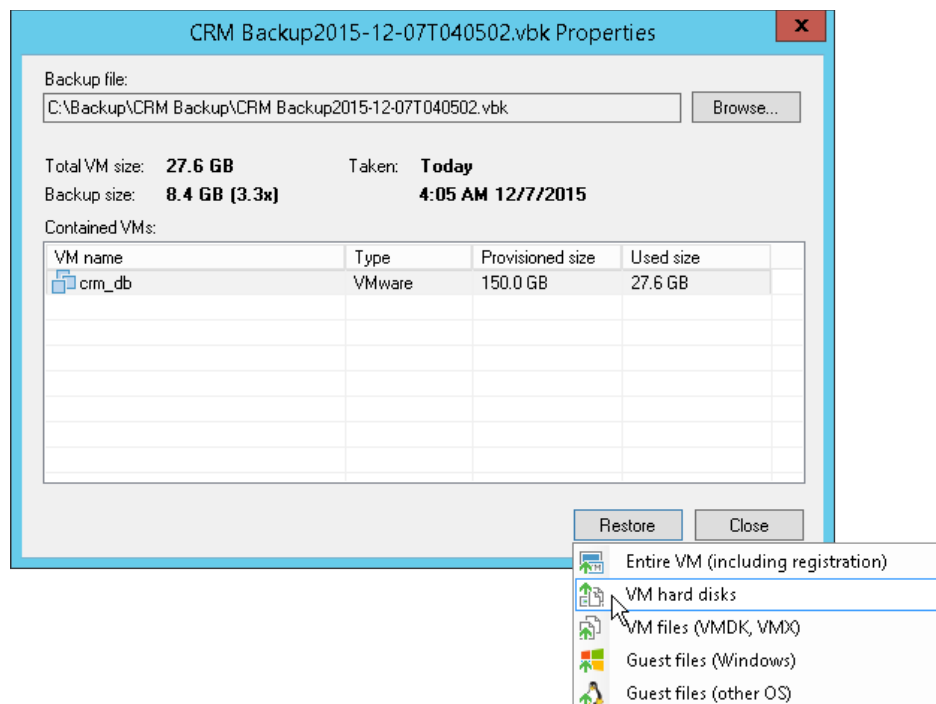
Note: During the virtual hard disk restore, Veeam Backup Free Edition turns off the target VM to reconfigure its settings and attach restored disks. For this reason, it is recommended to stop all active processes on the VM for the restore period.

Step 1. Choose File

You can restore VM hard disks from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

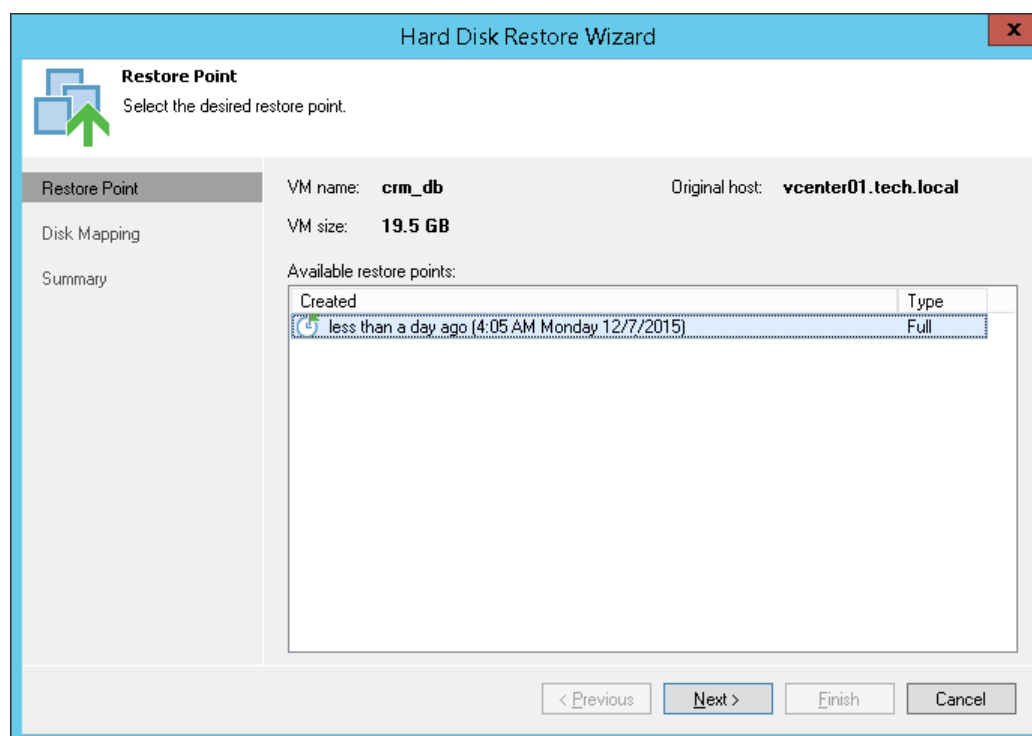
To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM whose disks you want to restore.
3. Click **Restore** and select **VM hard disks**. The **Hard Disk Restore** wizard will be launched.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point from which you want to restore the VM disk(s).



Step 3. Select Virtual Hard Disks to Restore

At the **Disk Mapping** step, select virtual hard disks to restore, choose a VM to which the disks must be attached and define additional restore properties.

1. By default, Veeam Backup Free Edition maps restored disks to the original VM. If the original VM was relocated or if you want to attach disks to another VM, you need to select the target VM manually. Click **Browse** and select the necessary VM from the virtual environment.

To facilitate selection, you can use the search field at the bottom of the window: click the button on the left of the field to select the necessary type of object that must be searched for, enter a VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.
2. Select check boxes next to virtual hard disks that you want to restore.
3. To define virtual disk properties, select a disk in the list and click **Change**. In the **Virtual Disk Properties** section, pick a datastore where the restored hard disk must be located and select a virtual device node.
 - If you want to replace an existing virtual disk, select an occupied virtual node.
 - If you want to attach the restored disk to the VM as a new drive, select a node that is not yet occupied.
4. Veeam Backup Free Edition preserves the format of the restored virtual hard disks. To change disk format, select the required option from the **Restore disks** list – same as on the original VM, force thin or force thick. Disk format change is supported only for VMs with Virtual Hardware version 7 or later.

5. [For hard disk restore to the original location and with original format] Select the **Quick rollback** check box if you want to use incremental restore for the VM disk. Veeam Backup Free Edition will data blocks that are necessary to revert the VM disk to an earlier point in time, and will restore only these data blocks from the VeeamZIP file. Incremental restore significantly reduces the restore time and has little impact on the production environment.

It is recommended that you enable this option if you restore a VM disk after a problem that occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not enable this option if the problem has occurred at the VM hardware level, storage level or due to a power loss.

Hard Disk Restore Wizard

Disk Mapping
Map virtual disks from backup to virtual device nodes on target VM.

Virtual Machine:

Restore Point:

Virtual disk	Virtual Device Node	Datastore
☐ crm_db_1.vmdk	SCSI 0:1	esx01-das1
☒ crm_db.vmdk	SCSI 0:0	esx01-das1
☒ crm_db_2.vmdk	SCSI 0:2	esx01-das1

Restore disks:

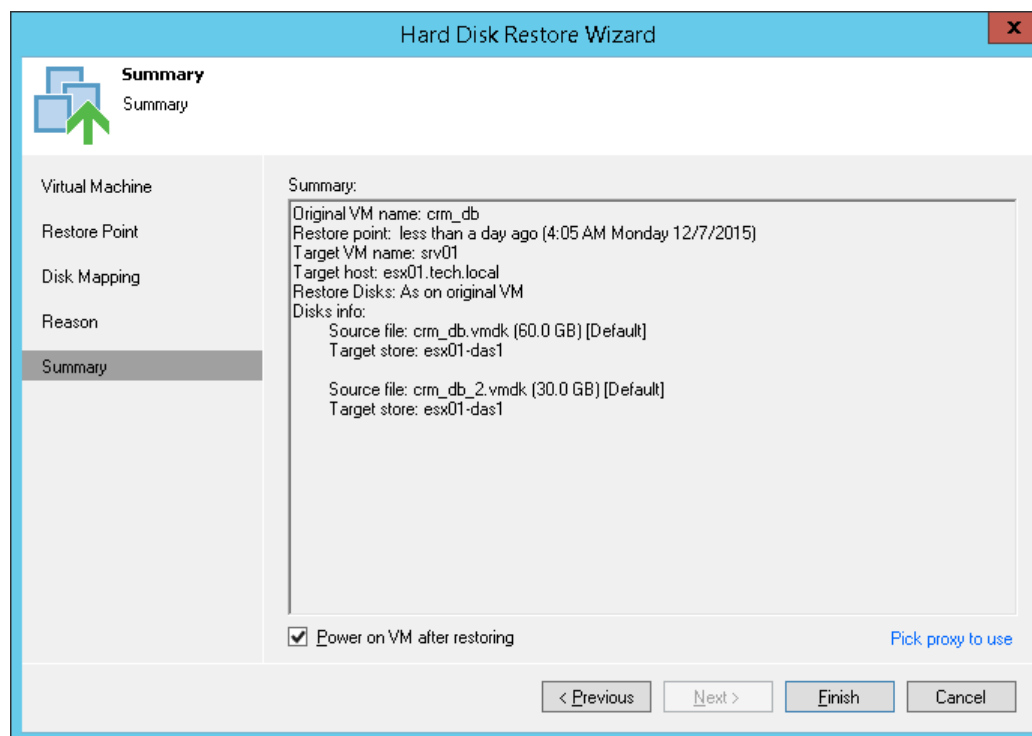
☐ Quick rollback (restore changed blocks only)
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous Next > Finish Cancel

Step 4. Verify Recovery Settings

At the **Summary** step of the wizard, complete the procedure of VM disk(s) restore.

1. Review details for the configured restore task.
2. To start a VM immediately after the restore process is complete, select the **Power on VM after restoring** check box.
3. Click **Finish** to start VM disk(s) restore.



The screenshot shows the 'Hard Disk Restore Wizard' window, specifically the 'Summary' step. The window has a blue title bar and a sidebar on the left with icons for 'Virtual Machine', 'Restore Point', 'Disk Mapping', 'Reason', and 'Summary'. The 'Summary' step is selected and highlighted. The main area displays the following information:

Summary:

- Original VM name: crm_db
- Restore point: less than a day ago (4:05 AM Monday 12/7/2015)
- Target VM name: srv01
- Target host: esx01.tech.local
- Restore Disks: As on original VM
- Disks info:
 - Source file: crm_db.vmdk (60.0 GB) [Default]
 - Target store: esx01-das1
 - Source file: crm_db_2.vmdk (30.0 GB) [Default]
 - Target store: esx01-das1

At the bottom, there is a checkbox labeled 'Power on VM after restoring' which is checked. To the right of this checkbox is a link that says 'Pick proxy to use'. At the very bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Restoring VM Files

You can restore specific VM files (VMDK, .VMX and others) if any of these files becomes deleted or the VMFS/NTFS datastore is corrupted. Instead of pulling the whole VM image to the production storage, you can restore a single VM file.

To recover VM files, follow the next steps:

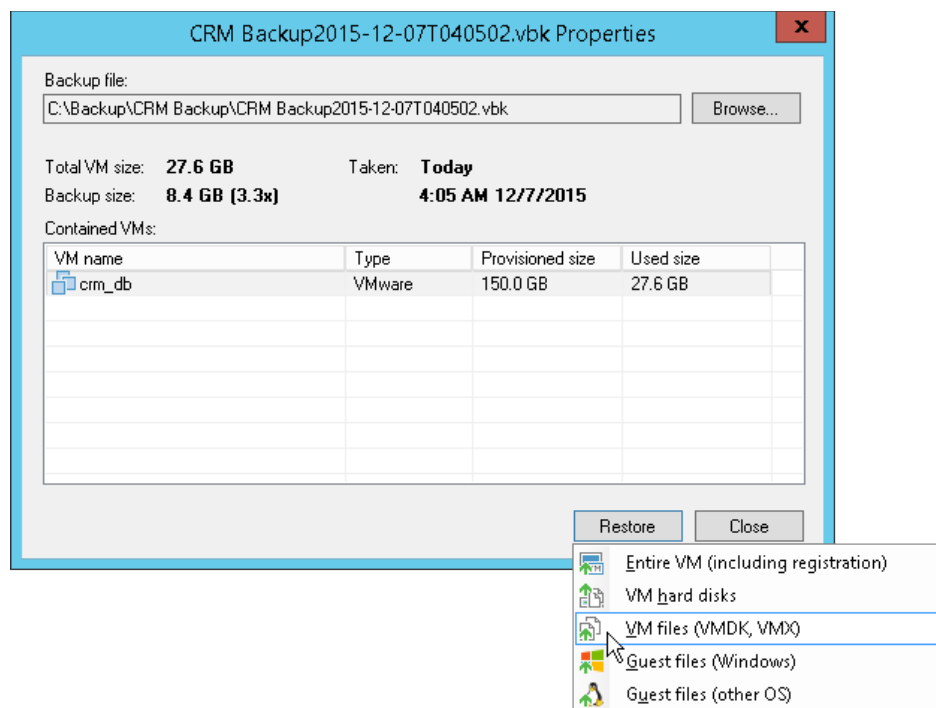
1. Choose a file
2. Select a VM
3. Select VM files and destination
4. Finish working with the wizard

Step 1. Choose File

You can restore VM files from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

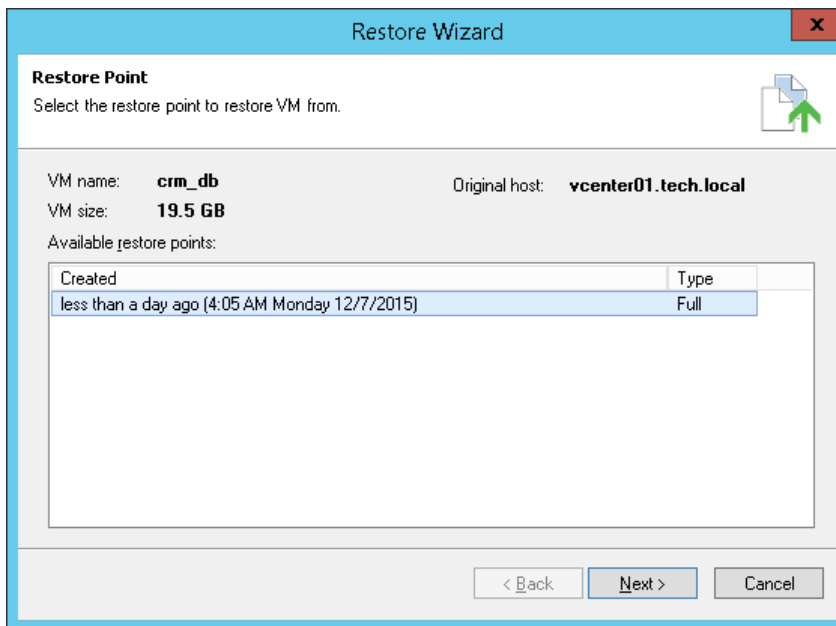
To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup Free Edition, the list may contain a number of VMs. Select the VM whose files you want to restore.
3. Click **Restore** and select VM files (VMDK, VMX). The **Restore** wizard will be launched.



Step 2. Select VM

At the **Restore Point** step of the wizard, select the restore point from which you want to restore the VM file(s).



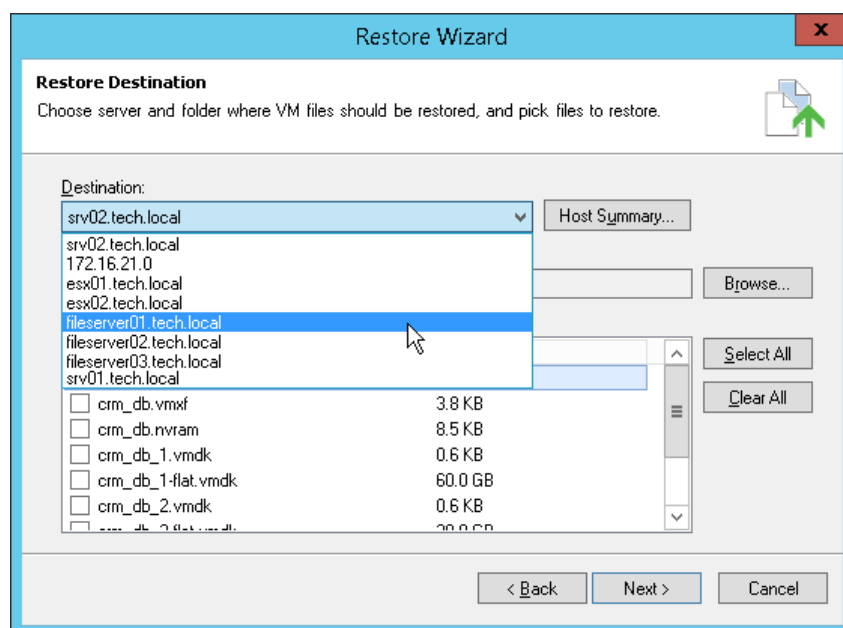
The screenshot shows the 'Restore Wizard' window with the 'Restore Point' step selected. The window title is 'Restore Wizard'. The main heading is 'Restore Point' with a sub-instruction: 'Select the restore point to restore VM from.' There is a green arrow icon pointing up. Below this, the VM details are displayed: 'VM name: **crm_db**' and 'Original host: **vcenter01.tech.local**'. The 'VM size: **19.5 GB**' is also shown. Under 'Available restore points:', there is a table with two columns: 'Created' and 'Type'. The table contains one row: 'less than a day ago (4:05 AM Monday 12/7/2015)' and 'Full'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Created	Type
less than a day ago (4:05 AM Monday 12/7/2015)	Full

Step 3. Select VM Files and Destination

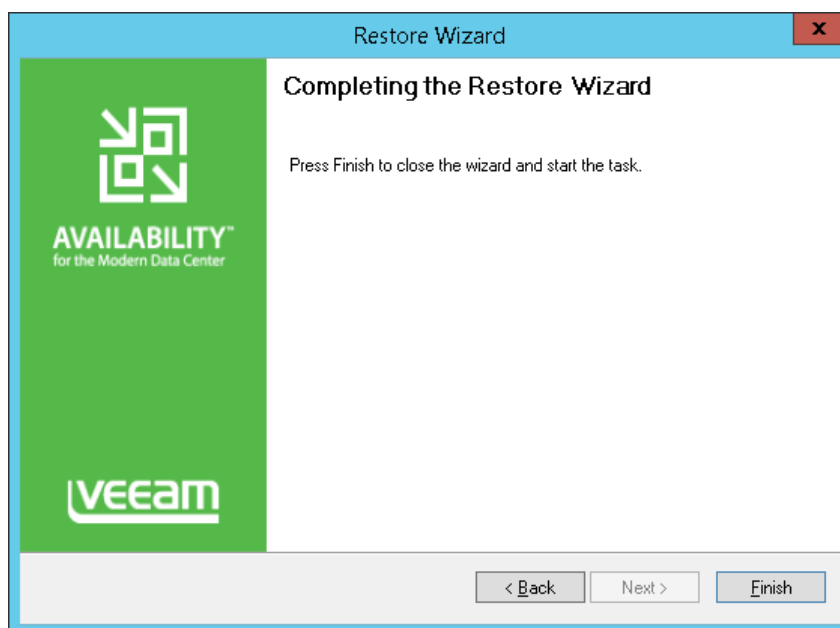
At the **Restore Destination** step of the wizard, select the VM files you want to restore and destination where the restored files must be stored.

1. From the **Destination** list, select where to store VM files: to an ESX(i) host, on the backup server or on a Microsoft Windows server added to the backup infrastructure.
2. Use the **Host Summary** button to view information on available storage resources. In the **Server Properties** section, click **Populate** to load the list of storage locations, their capacity and available space.
3. In the **Path to folder** section, specify a path to the folder on the selected host where files must be restored. To create a dedicated folder for restored files, click **Make New Folder** at the bottom of the window.
4. In the **VM files to restore** section, select check boxes next to files that you want to restore. By default, all VM files are selected.



Step 4. Finish Working with Wizard

At the last step of the wizard, click **Finish** to start VM files restore.



Restoring VM Guest OS Files (FAT, NTFS, ReFS)

You can restore individual VM guest OS files and folders from VeeamZIP files or backups of VMs with FAT, NTFS and ReFS file systems.

When you perform file-level recovery, the VM image is not extracted from the backup. Virtual disks files from the backup are published directly into the Veeam backup server file system with the proprietary driver. For accessing virtual disk content, Veeam Backup Free Edition uses a separate program — Virtual Disk Driver (VDD) that is provided with the product. After VM disks are mounted, you can use Veeam Backup Browser or Microsoft Windows Explorer to copy necessary files and folders to the local machine drive, save them on a network shared folder or simply point any applications to restored files and work with them as usual.

Note:

Guest OS file-level restore for ReFS is supported only if Veeam Backup Free Edition is installed on Microsoft Windows 2012 or Microsoft Windows 2012 R2 machine.

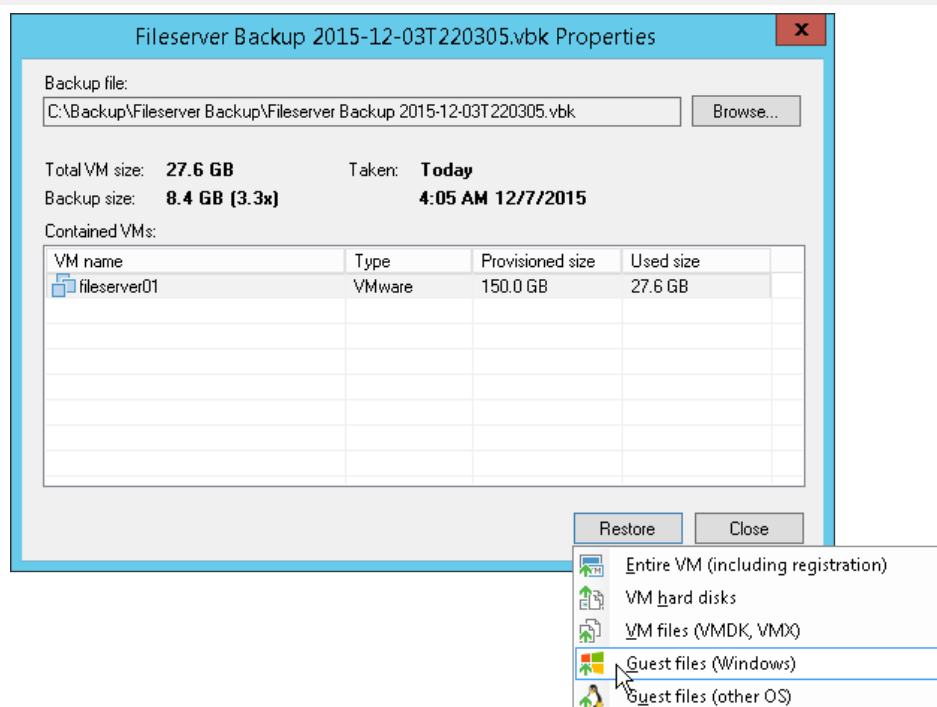
Step 1. Choose File

You can restore VM guest OS files from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

To choose a file:

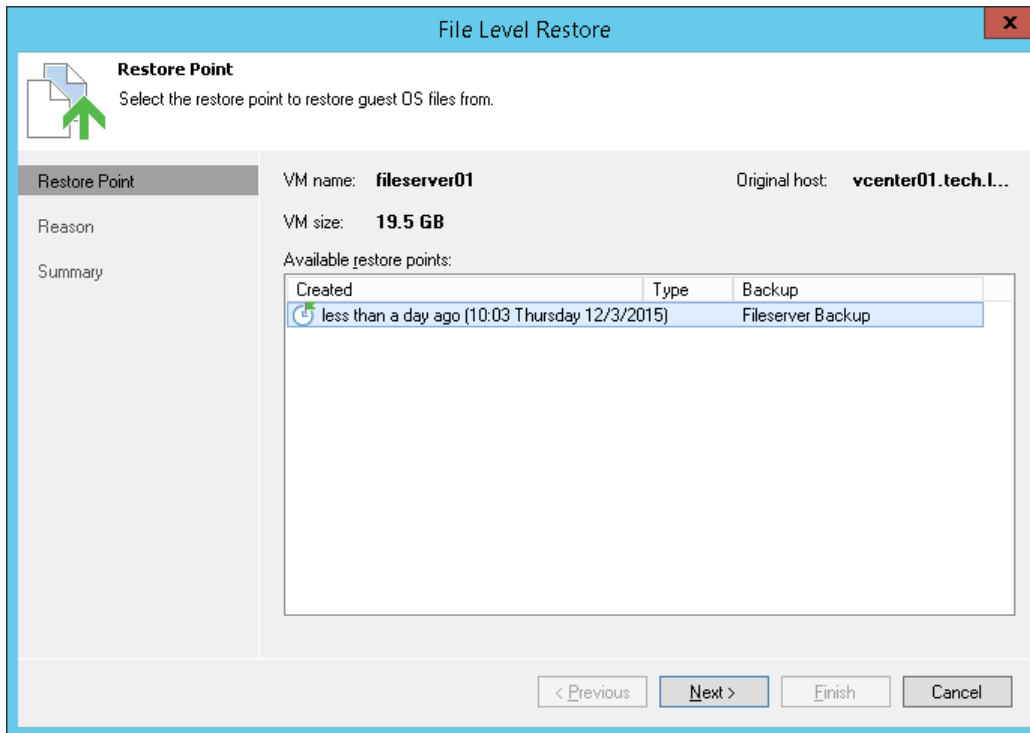
1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM whose guest OS files you want to restore.
3. Click **Restore** and select **Guest files (Windows)**.

Important! You cannot perform file-level restore while the VM from which you want to restore VM guest OS files is being backed up.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point from which you want to restore VM guest OS files.



File Level Restore

Restore Point
Select the restore point to restore guest OS files from.

Restore Point | Reason | Summary

VM name: **fileserver01** | Original host: **vcenter01.tech.l...**
VM size: **19.5 GB**

Available restore points:

Created	Type	Backup
 less than a day ago (10:03 Thursday 12/3/2015)	Fileserver Backup	

< Previous | **Next >** | Finish | Cancel

Step 3. Specify Restore Reason

At the **Restore Reason** step of the wizard, enter a reason for restoring VM guest OS files. The information you provide will be saved in the session history and you can reference it later.

Tip: If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.

The screenshot shows the 'File Level Restore' wizard window. The title bar is blue and says 'File Level Restore'. The main window has a light blue header with a document icon and the word 'Reason'. Below the header, there is a sidebar on the left with four items: 'Virtual Machine', 'Restore Point', 'Reason' (which is highlighted with a grey background), and 'Summary'. The main area of the window is white and contains the text 'Restore reason:' followed by a large text box. The text box contains the text 'Restoring deleted files'. Below the text box, there is a checkbox labeled 'Do not show me this page again'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Reason
Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.

Virtual Machine
Restore Point
Reason
Summary

Restore reason:
Restoring deleted files

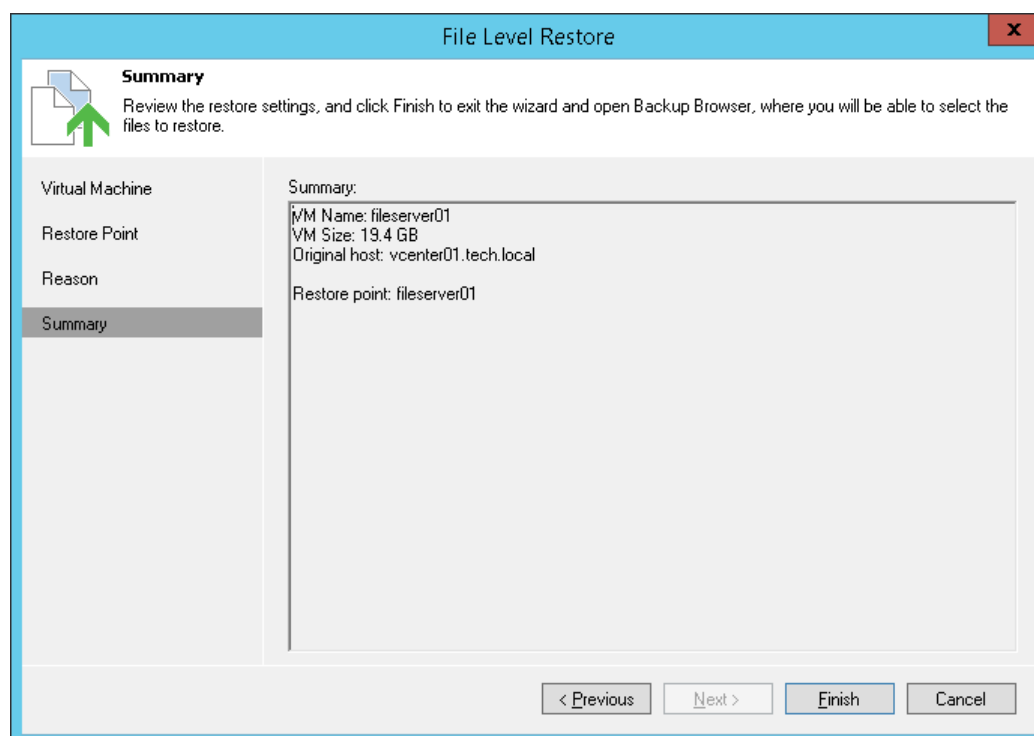
☐ Do not show me this page again

< Previous Next > Finish Cancel

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of VM guest OS files restore.

1. Review details of the restore task.
2. Click **Finish** to start restoring VM guest OS files from the backup or replica.



Step 5. Save Restored Files

When the restore process is complete, Veeam Backup Free Edition opens the Veeam Backup browser with the file system tree of the restored VM. Note that names of the restored VM hard disks may differ from the original ones.

You can perform the following operations with VM guest OS files in the Veeam Backup browser:

- Save files and folders to the original location
- Save files and folders to a folder on the backup server or network shared folder
- Launch Veeam Explorers for application item restore
- Open files in Microsoft Windows Explorer

After you finish restoring files, you can close the Veeam Backup browser.

Saving Files to Original Location

To save files or folders to their original location, right-click the necessary file or folder in the file system tree or in the details pane on the right and select one of the following commands:

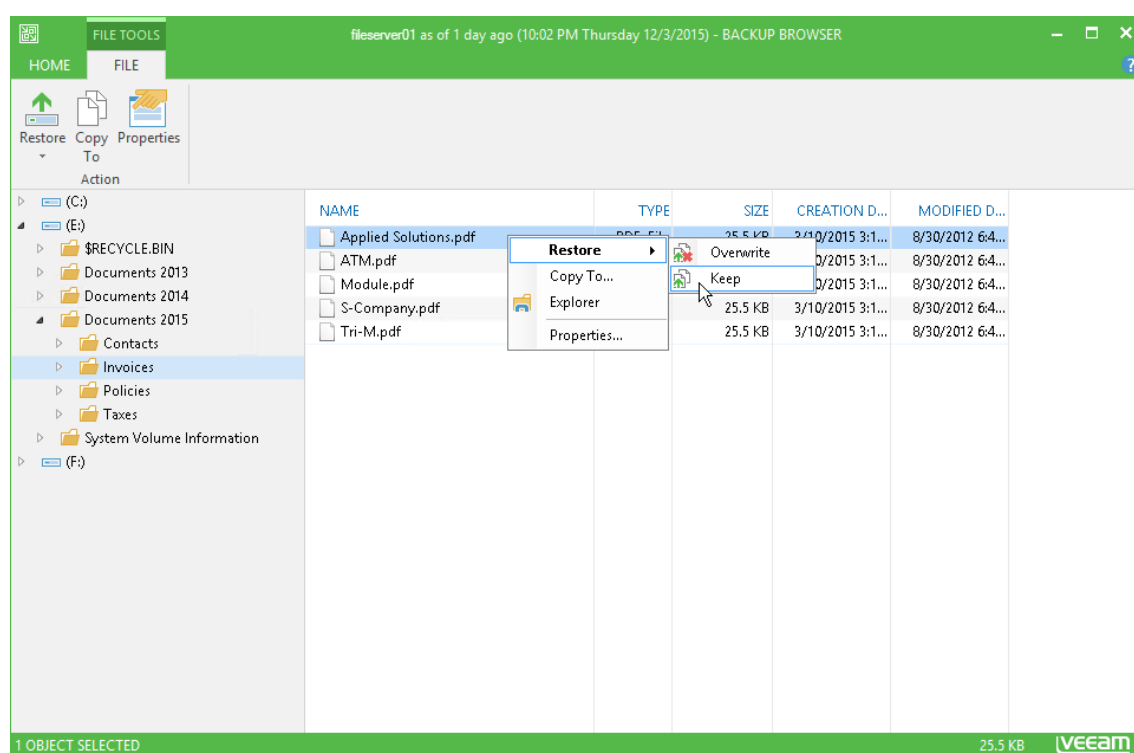
- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**. Veeam Backup Free Edition will add the *RESTORED-* prefix to the original file name and store the restored file in the same folder where the original file resides.

Important!

Restore to the initial location may fail for the following reasons:

- VMware Tools are not installed on the target VM.
- You have excluded the system disk from the VM backup.

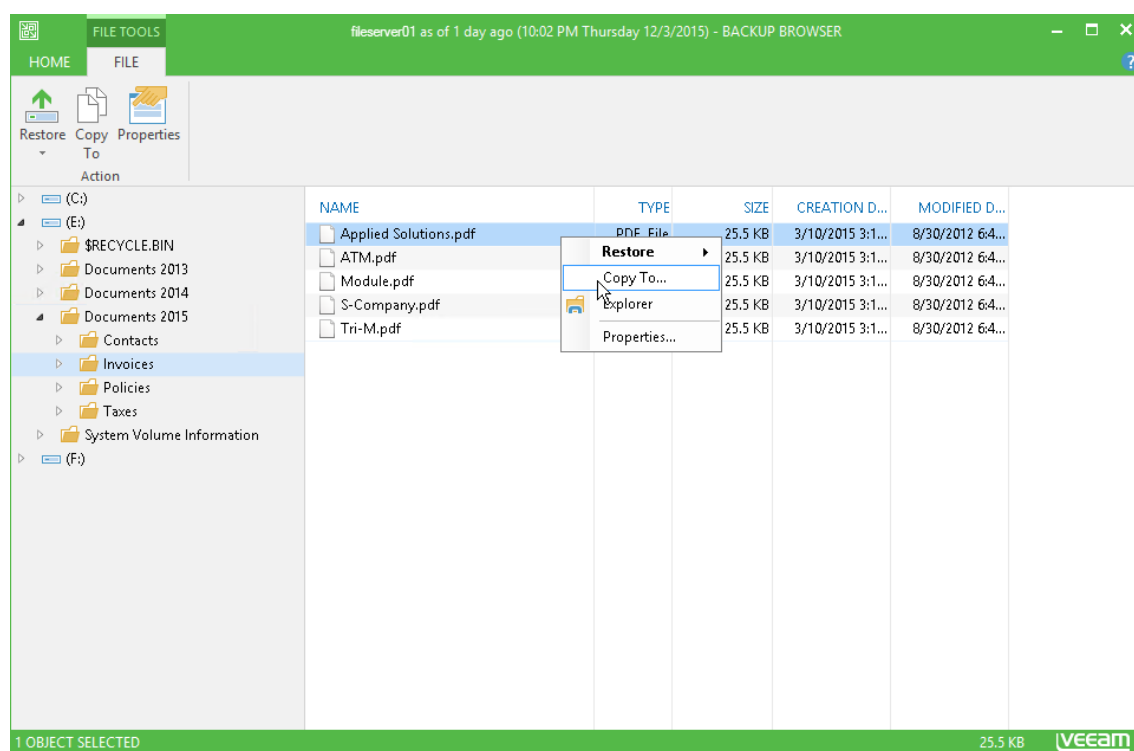
To restore guest OS files in such situation, you can use 1-click file-level restore or copy files to the selected folder and then move them to their initial location.



Saving Files to a New Location

To save restored files or folders on the local machine or in a network shared folder:

1. Right-click the necessary file or folder in the file system tree or in the details pane on the right and select **Copy To**.
2. Choose to preserve their original NTFS permissions or not:
 - Select the **Preserve permissions and ownership** check box to keep the original ownership and security permissions for restored objects. Veeam Backup Free Edition will copy selected files and folders along with associated Access Control Lists, preserving granular access settings.
 - Leave the **Preserve permissions and ownership** check box not selected if you do not want to preserve the original ownership and access settings for restored objects. Veeam Backup Free Edition will change security settings: the user who launched the Veeam Backup Free Edition console will be set as the owner of the restored object, while access permissions will be inherited from the folder to which the restored object is copied.
3. If prompted, in the **Credentials** window specify settings of the user account to access the destination location.



Launching Veeam Explorers

If you are restoring VM guest OS files of the virtualized Microsoft Active Directory Server, Microsoft Exchange Server, Microsoft SharePoint Server or Microsoft SQL Server or Oracle, you can launch a Veeam Explorer for the necessary application directly from the Veeam Backup browser.

- To start Veeam Explorer for Microsoft Active Directory, browse to the Microsoft Active Directory database file (DIT) in the Veeam Backup browser, select it and click **Active Directory Items** on the **Home** tab or simply double-click the DIT file.
- To start Veeam Explorer for Microsoft Exchange, browse to the Microsoft Exchange database file (EDB) in the Veeam Backup browser, select it and click **Exchange Items** on the **Home** tab or double-click the EDB file.
- To start Veeam Explorer for Microsoft SharePoint, browse to the Microsoft SharePoint content database (MDF) in the Veeam Backup browser, select it and click **SharePoint Items** on the **Home** tab or double-click the MDF file.
- To start Veeam Explorer for Microsoft SQL Server, browse to the Microsoft SQL Server database file in the Veeam Backup browser, select it and click **SQL Server Databases** on the **Home** tab or double-click the Microsoft SQL Server database file. For more information about default locations of Microsoft SQL Server database files, see <http://technet.microsoft.com/en-us/library/ms143547.aspx>.
- To start Veeam Explorer for Oracle, browse to the Microsoft Oracle content database in the Veeam Backup browser, select it and click **Oracle** on the **Home** tab or double-click the database file.

Working with Windows Explorer

You can use Microsoft Windows Explorer to work with restored files and folders.

1. Click **Explore** on the ribbon in the Veeam Backup browser or right-click the necessary folder and select **Explore**.
2. Veeam Backup Free Edition will launch Microsoft Windows Explorer. Browse to the necessary VM guest OS files.

You can also start Microsoft Windows Explorer from the **Start** menu of Microsoft Windows and browse to the necessary VM guest OS files. VM disks are mounted under the `C:\veeamflr\<vmname>\<volume n>` folder of the backup server.

It is recommended that you use the Veeam Backup browser instead of Microsoft Windows Explorer for file-level restore. Use of the Veeam Backup browser has the following advantages:

1. You can browse the VM guest OS file system ignoring the file system ACL settings.
2. You can preserve permissions and ownership during file-level restore.

If you open the VM file system via the Microsoft Windows Explorer, these capabilities will not be available.

For more information, see *SeBackupPrivilege* and *SeRestorePrivilege* at [https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx).

Closing Veeam Backup Browser

You can browse to VM guest OS files only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Backup Free Edition unmounts VM disks from the backup server.

It is recommended that you close the Veeam Backup browser after you have finished restoring VM guest OS files. When the Veeam Backup browser is open on the backup server, the backup file whose VM guest OS file system is displayed in the browser is locked on the backup repository. As a result, some scheduled operations that use this backup file may fail.

Veeam Backup Free Edition checks if there is any activity in the Veeam Backup browser with an interval of 5 minutes. If the user or Veeam Backup Free Edition components and services have not performed any actions for 30 minutes, Veeam Backup Free Edition displays a warning that the Veeam Backup browser is to be closed within 5 minutes.

After the warning is displayed, you can perform one of the following actions:

- You can close the Veeam Backup browser manually.
- You can click **Cancel** to postpone the close operation. In this case, the Veeam Backup browser will remain open for 5 minutes. After this period expires, Veeam Backup Free Edition will display the warning again.
- You can perform no action at all. In this case, the Veeam Backup browser will be automatically closed in 5 minutes.

Restoring VM Guest OS Files (Multi-OS Restore Wizard)

Because Microsoft Windows cannot read other file systems natively, Veeam Backup Free Edition provides multi-OS file-level recovery that allows reading data from 16 different OS file systems.

OS	Supported File Systems
Linux	ext ext2 ext3 ext4 ReiserFS JFS XFS
BSD	UFS UFS2
Mac	HFS, HFS+ (volumes up to 2 TB)
Solaris	UFS ZFS (except any pool versions of Oracle Solaris)
Novell Netware, Novell Open Enterprise Server	NSS (NSS file/folder permissions are not restored).

To restore files from VM guest OS'es, Veeam Backup Free Edition utilizes its patent-pending approach using a special FLR helper. The FLR helper is a virtual appliance running a stripped-down Linux kernel that has a minimal set of components. The appliance is very small, at around 20 MB, and takes only 10 seconds to boot.

The FLR helper appliance is created directly on the selected ESX(i) host. Whenever you perform file-level restore, Veeam Backup Free Edition automatically starts the appliance and mounts the VMDK files to the FLR appliance as virtual hard drives. VMDK files are mounted directly from backup files without prior extraction of the backup content.

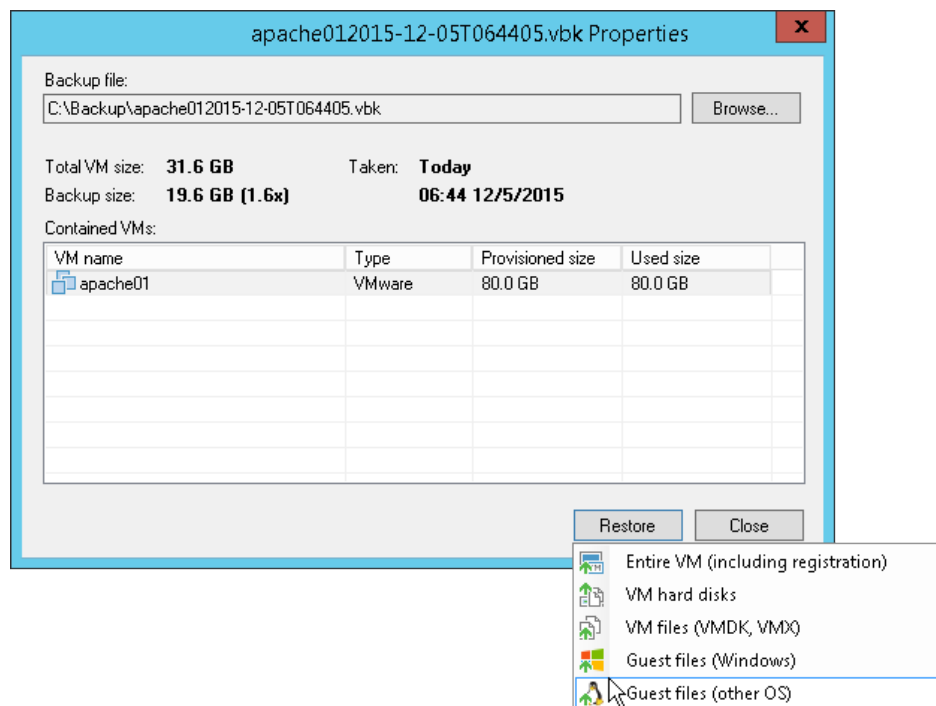
Once the restore process is complete, the wizard displays the file browser window, providing you with direct access to the VM file system. You can then copy necessary files and folders to your local machine drive or save them anywhere within the network. Alternatively, you can allow users to restore files on their own by enabling the FTP server on the virtual appliance.

Step 1. Choose File

You can restore VM guest OS files from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

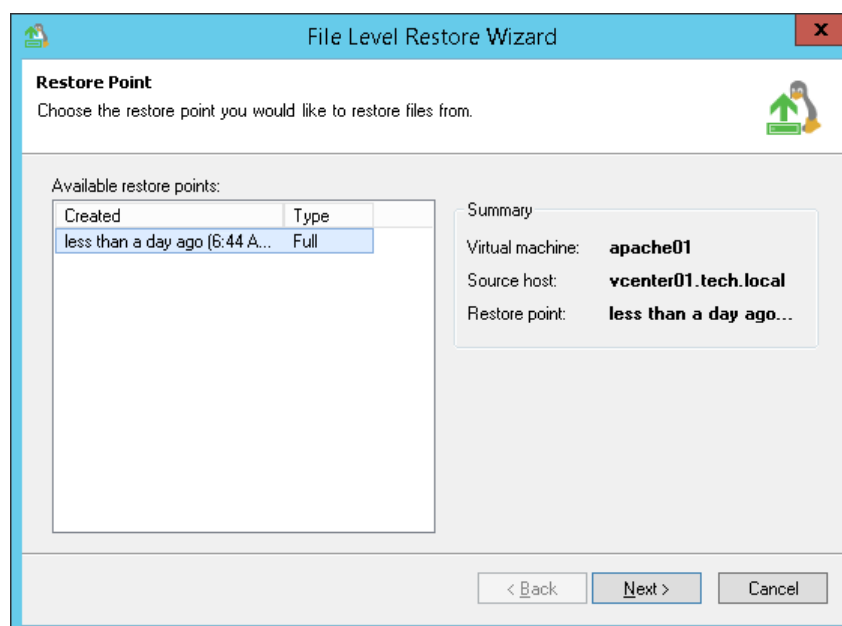
To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM whose guest OS files you want to restore.
3. Click **Restore** and select **Guest files (other OS)**. The **File Level Restore** wizard will be launched.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point from which you want to restore VM guest OS files.



Step 3. Select Location for Proxy Appliance

At the **Ready** step of the wizard, select an ESX(i) host on which you want to place the proxy appliance. When the restore process starts, Veeam Backup Free Edition will register the proxy appliance on the ESX(i) host and mount disks of the restored VM to this proxy appliance. The file system tree of the restored VM will be displayed in the file browser. After you restore necessary files and finish working with the file browser, the VM disks will be unmounted from the proxy appliance, and the proxy appliance will be deleted from the ESX(i) host.

To locate the appliance:

1. Click **Customize** at the bottom of the window.
2. In the **FLR Appliance Configuration** window, select an ESX(i) host on which the proxy appliance must be registered.
3. In the **Resource pool** field, specify a resource pool to which the proxy appliance must be placed.
4. In the **Network** section, specify an IP address and other network settings for the proxy appliance. The proxy appliance must be placed in the same network where the backup server resides.
5. To enable FTP access to the restored file system, select the **Enable FTP server on appliance** check box. As a result, users will be able to access the proxy appliance via FTP, browse the file system of the restored VM and download necessary files on their own.
6. If you are performing restore of a VM with the Novell Storage services file system, select the **Restore Novell Storage Services file system** check box. Veeam Backup Free Edition will deploy a specific proxy appliance that supports the Novell file system.
7. Click **OK**.

Important!

When choosing an ESX(i) host for the Novell file system proxy appliance, make sure that it allows running VMs with 64-bit guest OS'es.

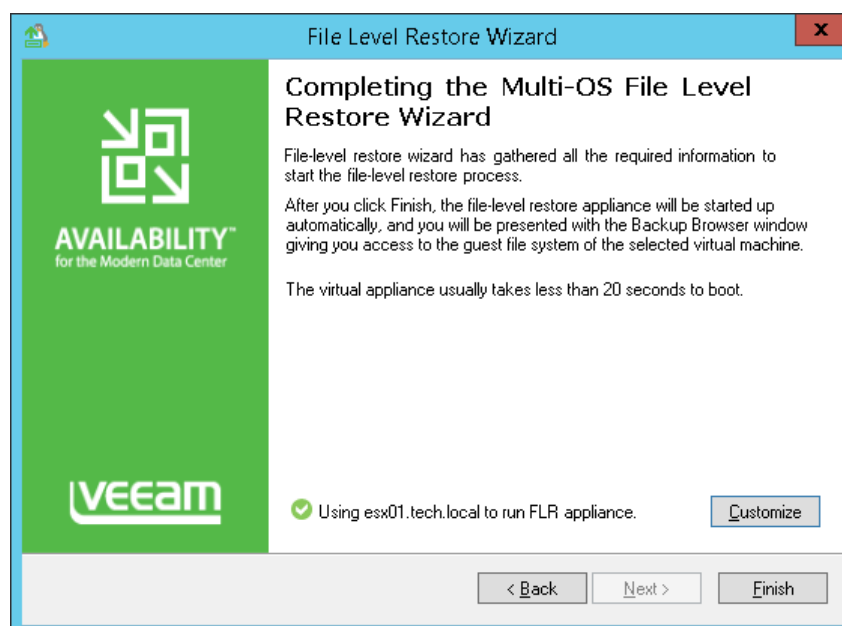
The screenshot shows a dialog box titled "FLR Appliance Configuration" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Host:** A text field containing "esx01.tech.local" and a "Choose..." button.
- Statistics:** A box showing "VMs: 36 total" and "17 running".
- Resource pool:** A text field containing "Resources" and a "Choose..." button.
- Network:** A text field containing "VM Network" and a "Choose..." button.
- IP Address Options:**
 - ☒ Obtain an IP address automatically
 - ☐ Use the following IP address:
 - IP address: [. . .]
 - Subnet mask: [. . .]
 - Default gateway: [. . .]
- ☒ Enable FTP server on appliance (advanced)
- ☐ Restore from Novell Storage Services (NSS) file system

At the bottom right, there are "OK" and "Cancel" buttons.

Step 4. Finish Working with Wizard

At the last step of the wizard, click **Finish** to start restoring VM guest OS files. The file-level restore appliance may take about 10-40 seconds to boot.



Step 5. Save Restored Files

When the restore process is complete, Veeam Backup Free Edition opens the Veeam Backup browser displaying the file system tree of the restored VM.

You can save the restored files and folders to their original location, new location or access files on FTP.

Note: You can browse the VM guest OS files and access restored files on the FTP only while the Veeam Backup browser with the restored files is open. After the Veeam Backup browser is closed, the VM disks will be unmounted from the proxy appliance, and the proxy appliance will be deleted from the ESX(i) host.

Saving Files to Original Location

To save files and folders to the original location, right-click the necessary file or folder in the file system tree or in the details pane on the right and select one of the following commands:

- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**. Veeam Backup Free Edition will add the *RESTORED-* prefix to the original file name and store the restored file in the same folder where the original file resides.

To restore files to the original location, Veeam Backup Free Edition uses the account for VM guest OS access specified in the backup job settings. If this account does not have sufficient rights to access the target VM, you will be prompted to enter credentials. In the **Credentials window**, specify a user account to access the destination location (server or shared folder). You can use the account under which you are currently logged on, or a different account.

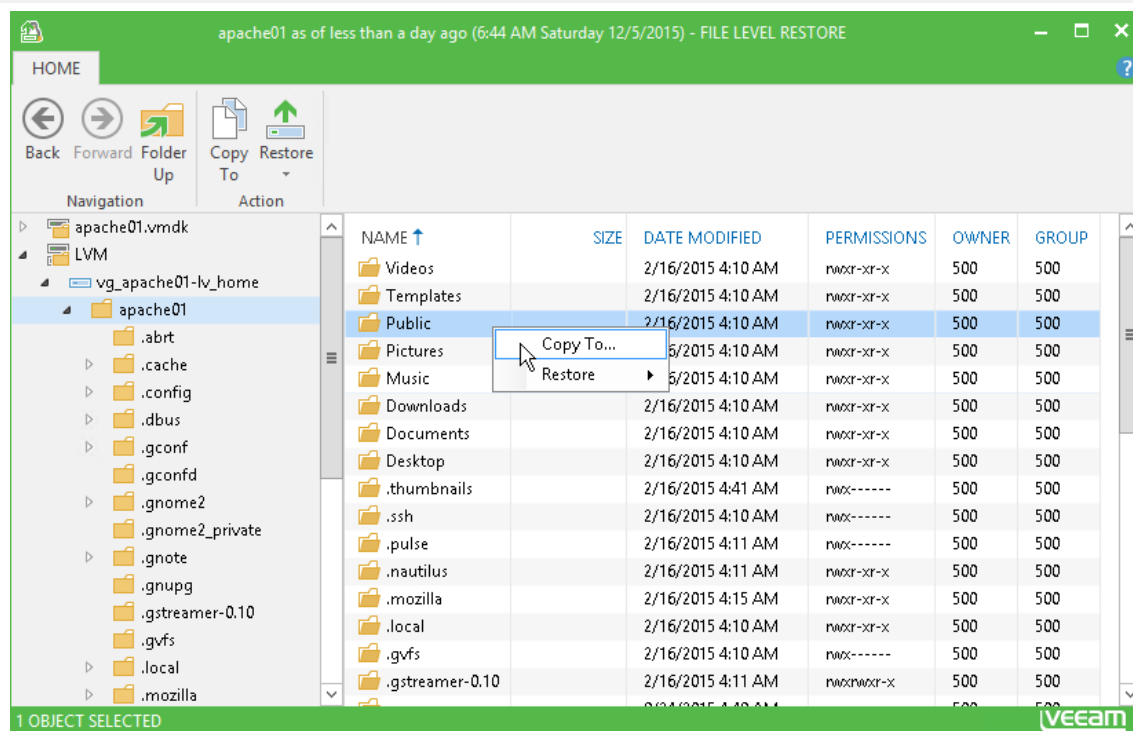
Saving Files to New Location

To save files and folders to a new location:

1. Right-click the necessary file or folder and select **Copy to**.
2. In the **Select Destination** window, select the destination server (local or remote) from the list or provide a path to the shared folder.
 - If you are recovering files to a Linux server, you can select the destination server from the list or add a destination server ad-hoc. To do this, scroll down the list of servers and choose **Specify a different host** at the end of the list. Follow the steps of the wizard to add a Linux server that will be used as a destination host.

The server you add ad-hoc will not appear in the list of managed hosts in Veeam Backup Free Edition: its purpose is to host the files that you recover. It will only remain visible in the Veeam Backup browser until all currently active file-level restore sessions are completed.
 - If you are recovering files to a shared folder, specify a path to the destination folder.
3. If you want to preserve original permissions and ownership for recovered files, select the **Preserve permissions and ownership** check box.
4. If prompted, in the **Credentials** window specify settings of the user account to access the destination location.

Important! To restore original permissions and ownership settings, the account you have specified should have privileges to change the owner on the selected server or shared folder.



Accessing Files over FTP

If you have chosen to enable FTP server on the FLR appliance, the restored file system will also be available over FTP at `ftp://<FLR_appliance_IP_address>`. Other users in the same network can access the FLR appliance to restore the files they need.

Performing Restore in Microsoft Hyper-V Environment

Veeam Backup Free Edition offers a variety of data recovery options to protect your virtual environment. If important data accidentally gets lost or corrupted, you can use Veeam Backup Free Edition to restore an entire VM and specific VM files or individual VM guest OS files from backups.

You can perform recovery using a VeeamZIP file created in Veeam Backup Free Edition or choose a VeeamZIP file or a backup file created in Veeam Backup & Replication. Keep in mind that only a full backup file (VBK) can be used for restore.

Performing Full VM Recovery

You can restore an entire VM and start it on the target host if necessary.

A VM can be restored to its original location or to a new location:

- When you restore a VM to its original location, you keep the original VM settings. The primary VM is automatically turned off and deleted before the restore. This type of restore ensures the quickest recovery and minimizes the number of mistakes that can be caused by changes in VM settings.
- When you restore a VM to a new location, you need to specify new VM settings such as a new VM name, a host and volume where the VM will reside and network properties. Veeam Backup Free Edition will change the VM configuration file and store the VM data to the location of your choice.

Note:

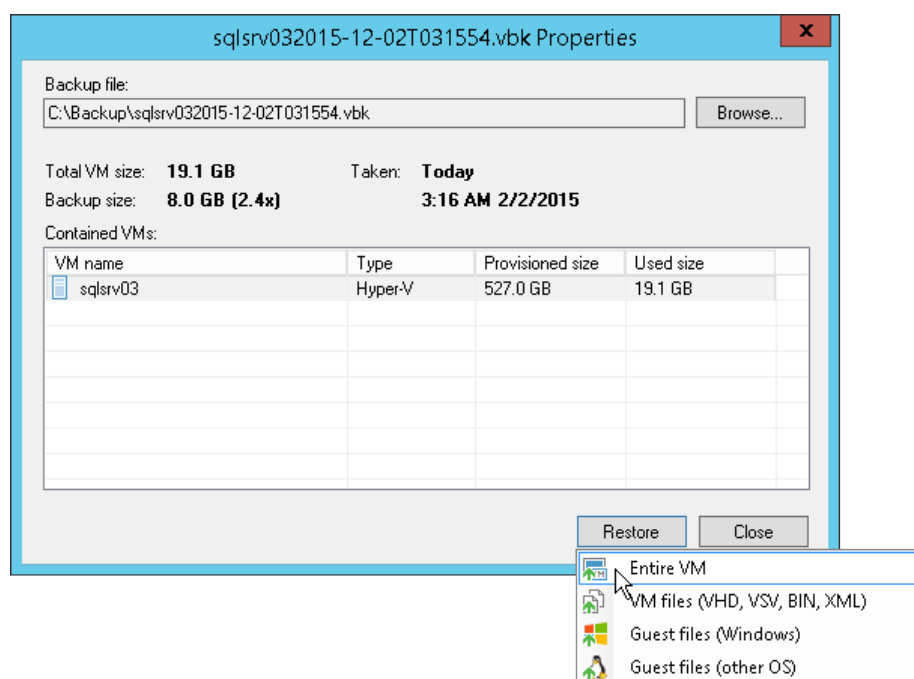
- If a VM you plan to restore was running on a Windows 2008 R2 machine with the Hyper-V role enabled, you can restore it to a Windows Server 2008 R2 machine with the Hyper-V role enabled, Windows Server 2012 machine with the Hyper-V role enabled or Windows Server 2012 R2 machine with the Hyper-V role enabled.
- If a VM you plan to restore was running on a Windows 2012 machine with the Hyper-V role enabled, you can restore it to a Windows 2012 machine with the Hyper-V role enabled or Windows Server 2012 R2 machine with the Hyper-V role enabled.
- If a VM you plan to restore was running on a Windows 2012 R2 machine with the Hyper-V role enabled, you can only restore it to a Windows 2012 R2 machine with the Hyper-V role enabled.

Step 1. Choose File

You can restore a VM from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

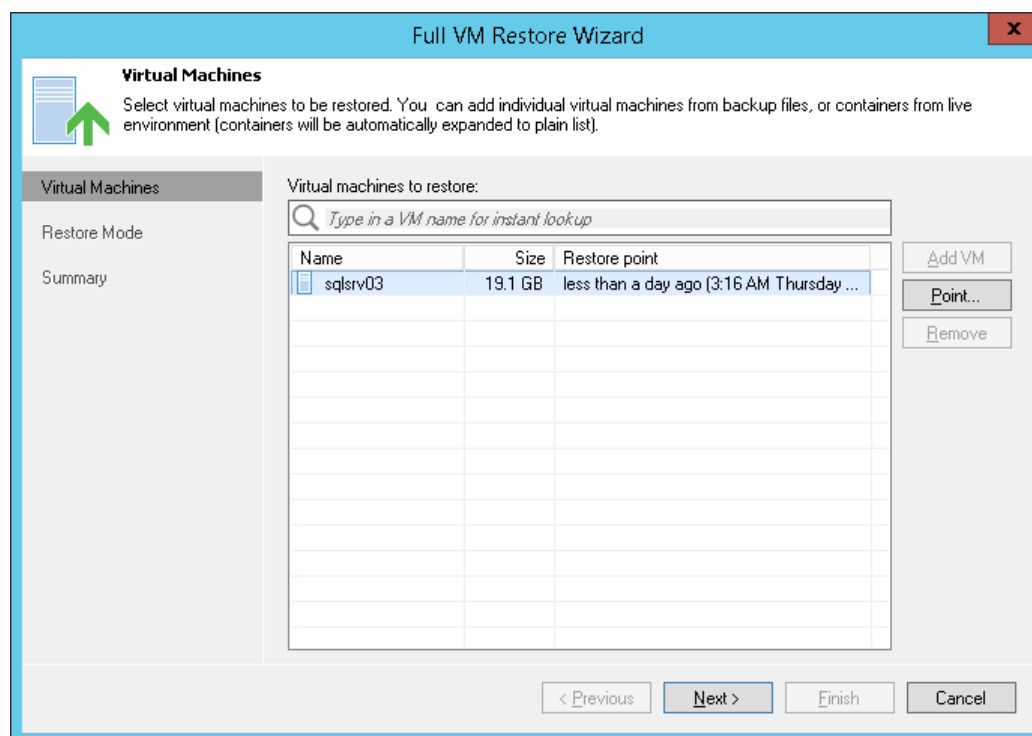
To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM you want to restore.
3. Click **Restore** and select **Entire VM**. The **Full VM Restore** wizard will be launched.



Step 2. Select VM

At the **Virtual Machines** step of the wizard, select the VM that you want to restore.

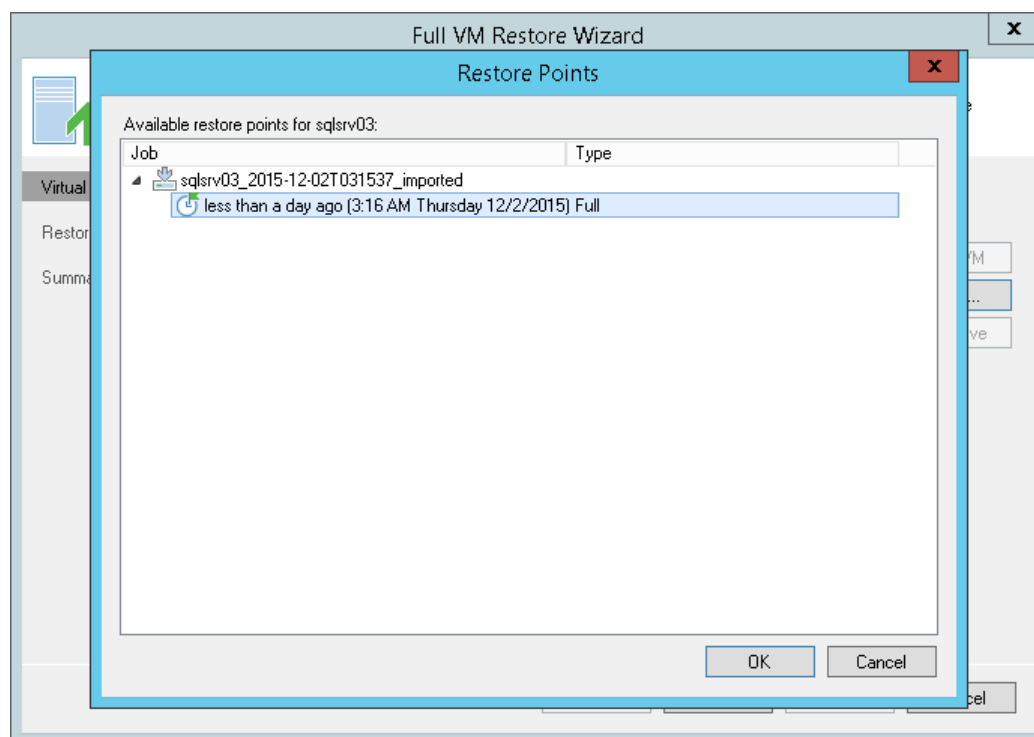


Step 3. Select Restore Point

You can select the necessary restore point for the VM(s) that you want to restore.

To select a restore point for a VM:

1. In the **Virtual machines to restore** list, select the VM.
2. Click **Point** on the right.
3. In the **Restore Points** window, select a restore point from which you want to restore the VM.

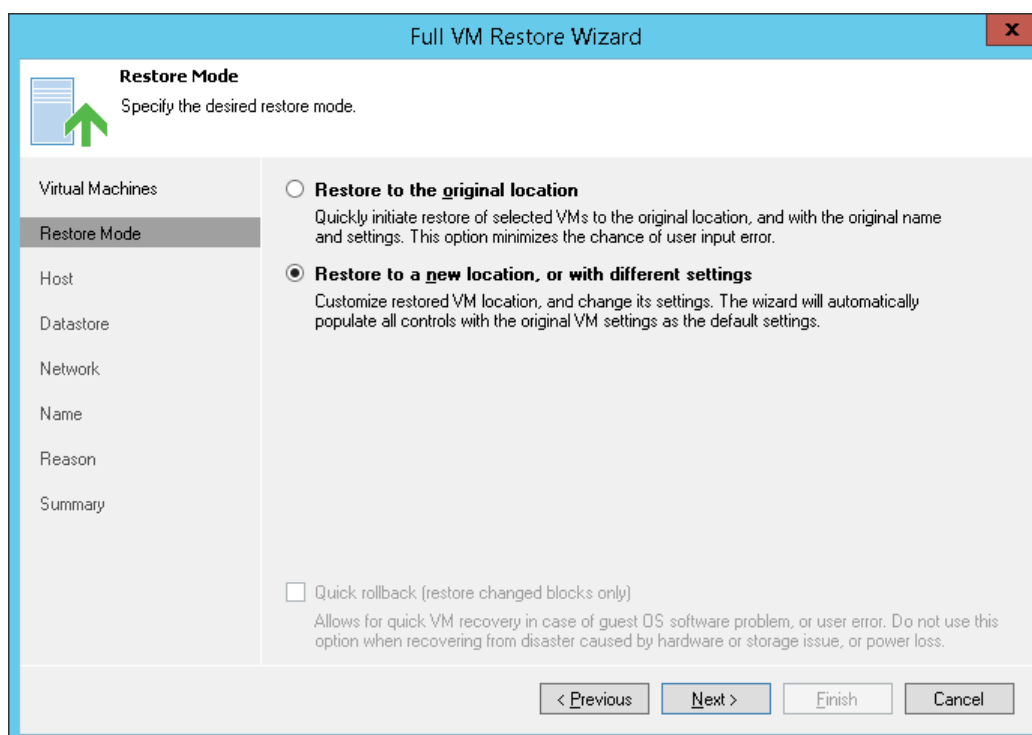


Step 4. Select Restore Mode

At the **Restore Mode** step of the wizard, choose the necessary restore mode:

1. Choose a restore mode:
 - Select **Restore to original location** if you want to restore VMs with their initial settings and to their original location.
 - Select **Restore to a new location, or with different settings** if you want to restore VMs to a different location and/or with different settings (such as VM location, network settings and so on). If this option is selected, the **Full VM Restore** wizard will include additional steps for customizing VMs settings.
2. [For VM restore to the original location] Select the **Quick rollback** check box if you want to perform incremental restore for the VM. Veeam Backup Free Edition will query its CBT module to get data blocks that are necessary to revert the VM to an earlier point in time, and will restore only these data blocks from the backup. Quick restore significantly reduces the restore time and has little impact on the production environment.

It is recommended that you enable this option if you restore a VM after a problem that occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not enable this option if the problem has occurred at the VM hardware level, storage level or due to a power loss.



Step 5. Select Destination Host for Restored VM

The **Host** step of the wizard is available if you have chosen to change the location and settings for the restored VM.

To specify a destination host:

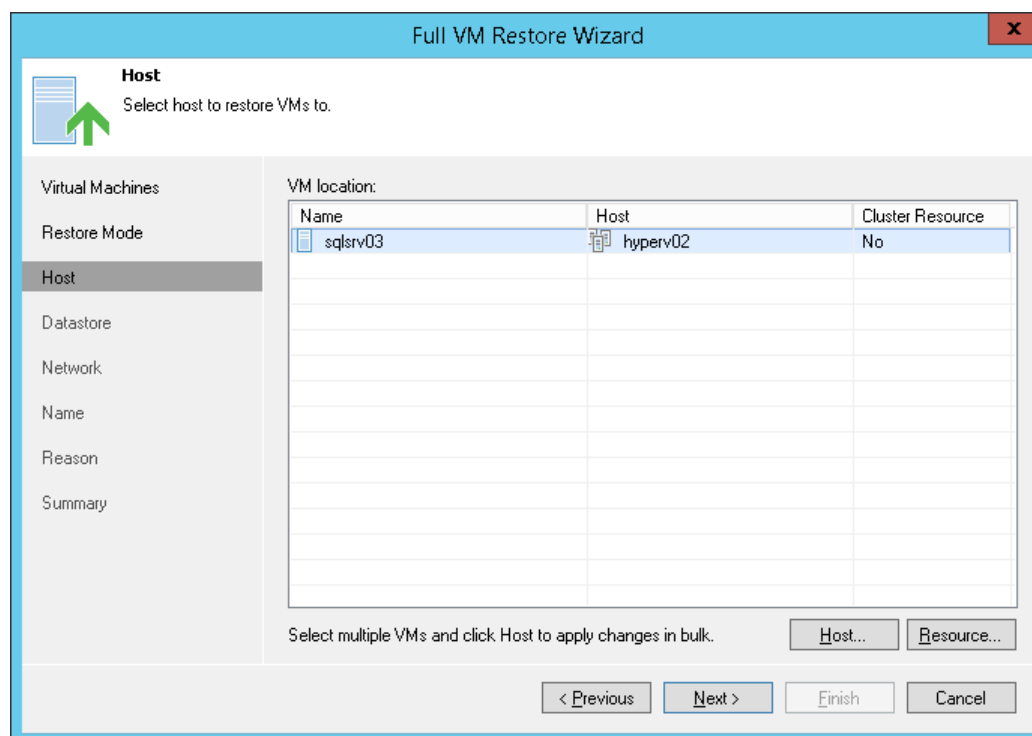
1. Select a VM in the list and click **Host**. To apply changes in bulk, select several VMs in the list and click **Host**.
2. Choose a standalone or clustered host where the selected VM must be registered.

To facilitate selection, you can use the search field at the bottom of the window:

1. Click the button on the left of the field to select the necessary type of object that should be searched for: *SCVMM*, *Cluster* or *Host*.
2. Enter an object's name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

If you choose to register the restored VM on a host being a part of a Hyper-V failover cluster, you can specify additional failover settings.

1. Select a VM in the list and click **Resource**.
2. Select the **Register VM as a cluster resource** option if the restored VM must be configured as a cluster resource. In this case, if the destination host is brought offline or fails for any reason, the VM will fail over to another node in the cluster.



Step 6. Select Destination Datastore

The **Datastore** step of the wizard is available if you have chosen to change the location and settings for recovered VMs.

You can place an entire VM to a particular location or choose to store configuration files and disk files of a restored VM in different locations.

To specify a destination location:

1. Select a VM in the list and click **Path**. To apply changes in bulk, select several VMs in the list and click **Path**.
2. Point to a folder where VM files must be stored.

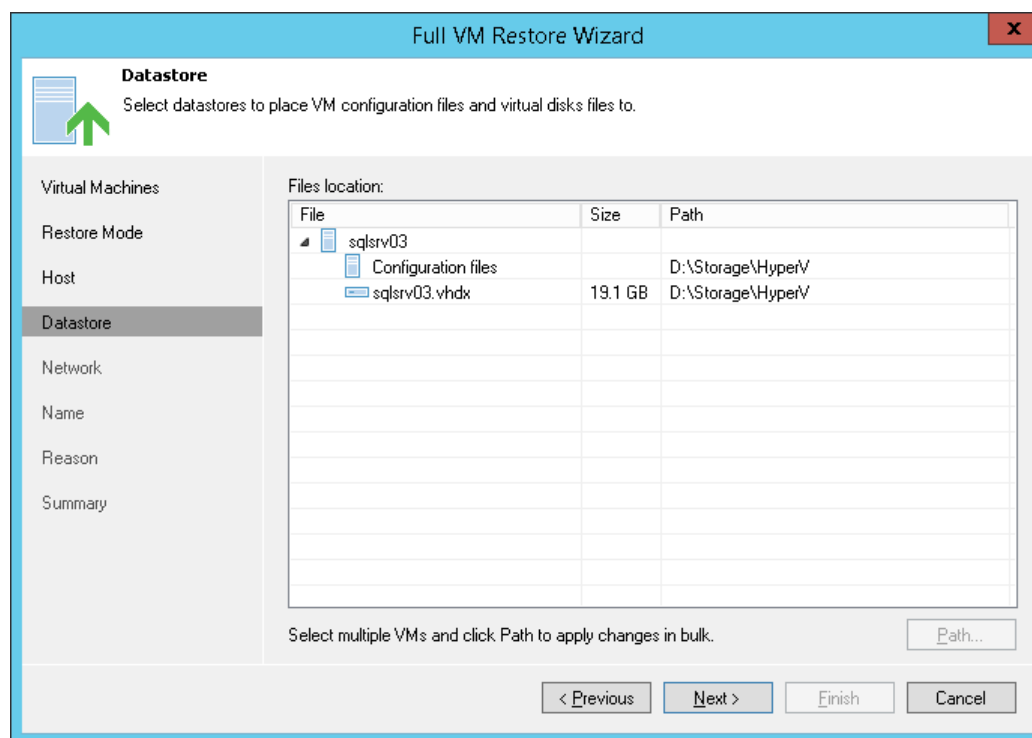
If configuration and disk files of a VM must be placed to different locations:

1. Expand the VM in the list.
2. Select the necessary file type.
3. Click **Path** and point to a folder where VM files must be stored. To create a dedicated folder for storing files of the recovered VM, click **Make New Folder** at the bottom of the window.

You can choose a Microsoft SMB3 shared folder as a destination for the restored VM.

1. Select the VM in the list and click **Path** at the bottom of the window.
2. Type a path to the Microsoft SMB3 shared folder in the search field at the bottom of the **Select Folder** window. The path must be specified in the UNC format, for example:
\\172.16.11.38\Share01.

The host or cluster on which you register the VM must have access to the Microsoft SMB3 shared folder. If you are using SCVMM 2012 or SCVMM 2012 R2, the server hosting the SMB3 share must be registered in SCVMM as a storage device. For more information, see <http://technet.microsoft.com/en-us/library/jj614620.aspx>.



Step 7. Select Destination Network

The **Network** step of the wizard is available if you have chosen to change the location and settings for recovered VMs.

If you plan to restore a VM to a new location, for example, another site with a different set of networks, you can map source site networks to target site networks. Veeam Backup Free Edition will use the network mapping table to update configuration files of VMs on the fly, during the restore process.

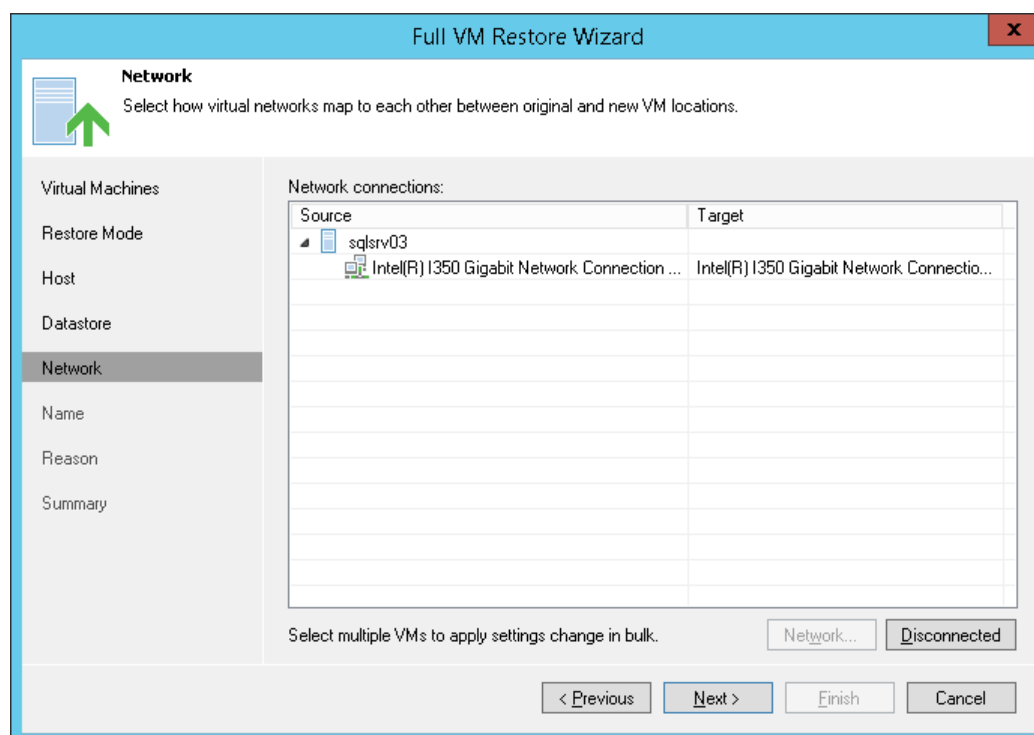
To change networks to which restored VMs will be connected:

1. Select a VM in the list and click **Network**. To apply changes in bulk, select several VMs in the list and click **Network**.

If a VM is connected to multiple networks, expand the VM, select the network to map and click **Network**.

2. The **Select Network** section displays all networks to which the destination host or cluster is connected. From the list of available networks, choose a network to which the selected VM must have access upon restore. To facilitate selection, use the search field at the bottom of the window: enter a network name or a part of it and click the **Start search** button on the right or press [ENTER].

If you do not want to connect the restored VM to any virtual network, select the VM in the list and click **Disconnected**.



Step 8. Specify VM Names and VM UUID Handling

The **Name** step of the wizard is available if you have chosen to change the location and settings for recovered VMs.

You can change a name of each restored VM and select whether you want to preserve its UUID or change it. It is recommended that you specify a new name and generate a new UUID for a VM to prevent conflicts if the original VM still resides in the production environment. The name and ID change is not required if the original VM no longer exists, for example, it was permanently deleted.

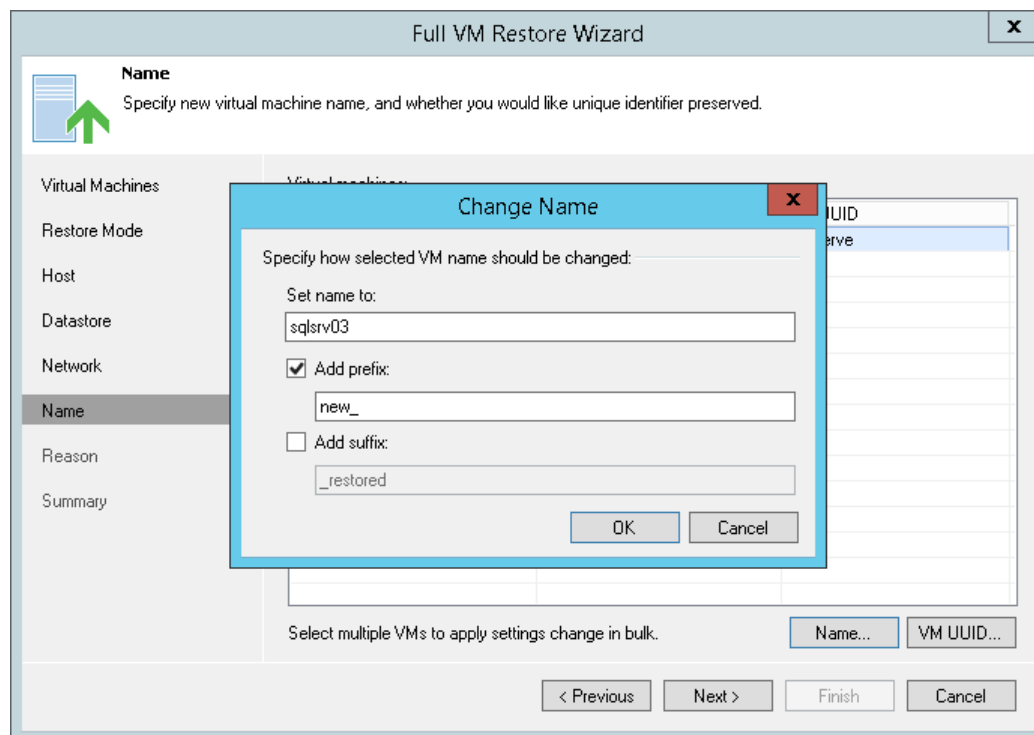
To change a VM name:

1. Select a VM in the list and click **Name**. To apply changes in bulk, select several VMs and click **Name**.
2. In the **Change Name** window, enter a new name explicitly or specify a change name rule by adding a prefix and/or suffix to the VM name.
3. You can also change VM names directly in the list: select a VM, click the **New Name** field and enter the name to be assigned to the recovered VM.

You can specify how Veeam Backup Free Edition must handle unique identifiers of the restored VM. By default, a recovered VM is identified with the same UUIDs as the original VM. If necessary, however, you can choose to assign a new UUID to the restored VM.

To view or change VM identification settings:

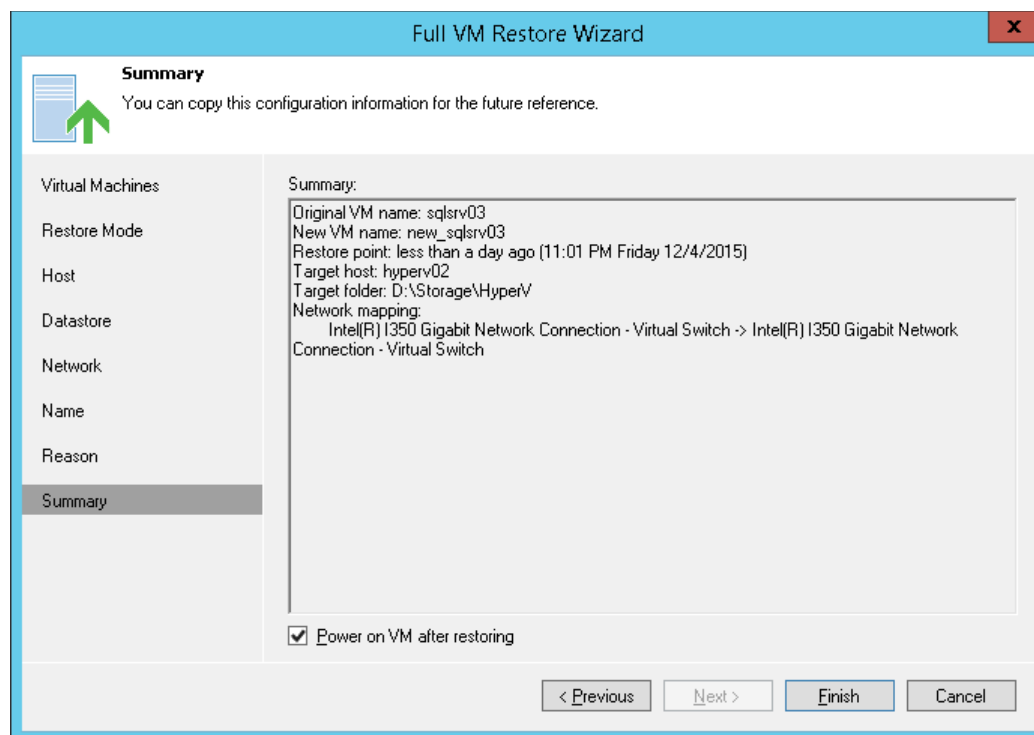
1. Select one or more VMs in the list and click **VM UUID**.
2. Select to preserve the VM ID or generate a new VM ID:
 - Select **Preserve virtual machine UUID** if the original VM was decommissioned and the restored VM will be used in place of the original one.
 - Select **Generate new virtual machine UUID** if you perform VM restore to clone the original VM. This option will help you avoid UUID conflicts if the original VM and its duplicate will operate in parallel in the same location.



Step 9. Verify Recovery Settings

At the **Summary** step of the wizard, specify additional settings for VM restore:

1. If you want to start the restored VM on the target host, select the **Power on VM after restoring** check box.
2. Check the specified settings and click **Finish**. Veeam Backup Free Edition will restore selected VMs in the specified destination.



Restoring VM Files (VHD, VHDX, VSD, BIN, XML)

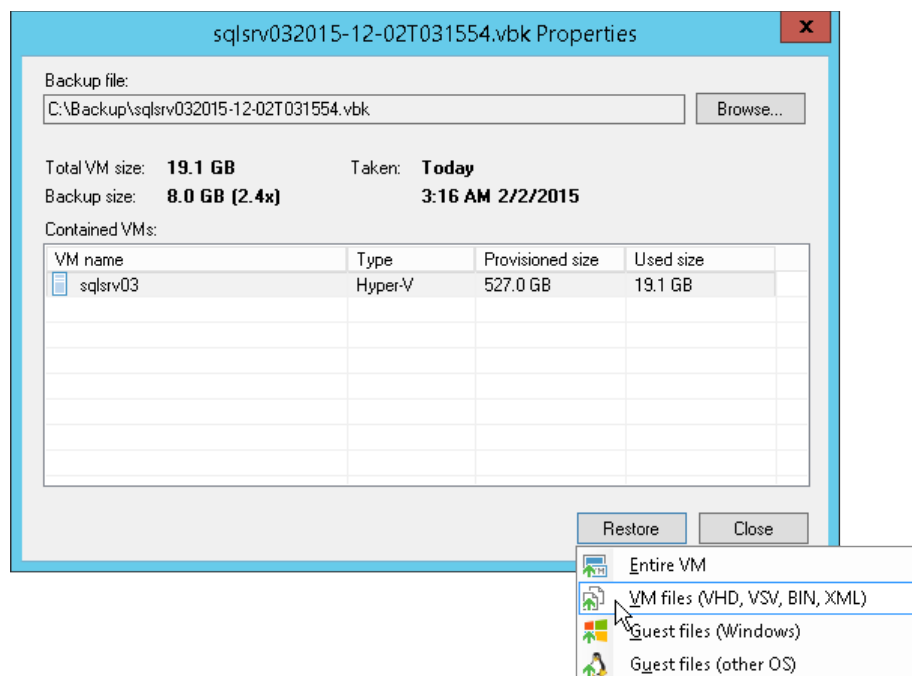
Veeam Backup Free Edition allows you to restore specific VM files: .vhd, .vhdx, .xml and others. You can use VM files recovery to replace deleted or corrupted VM files.

Step 1. Choose File

You can restore VM files from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

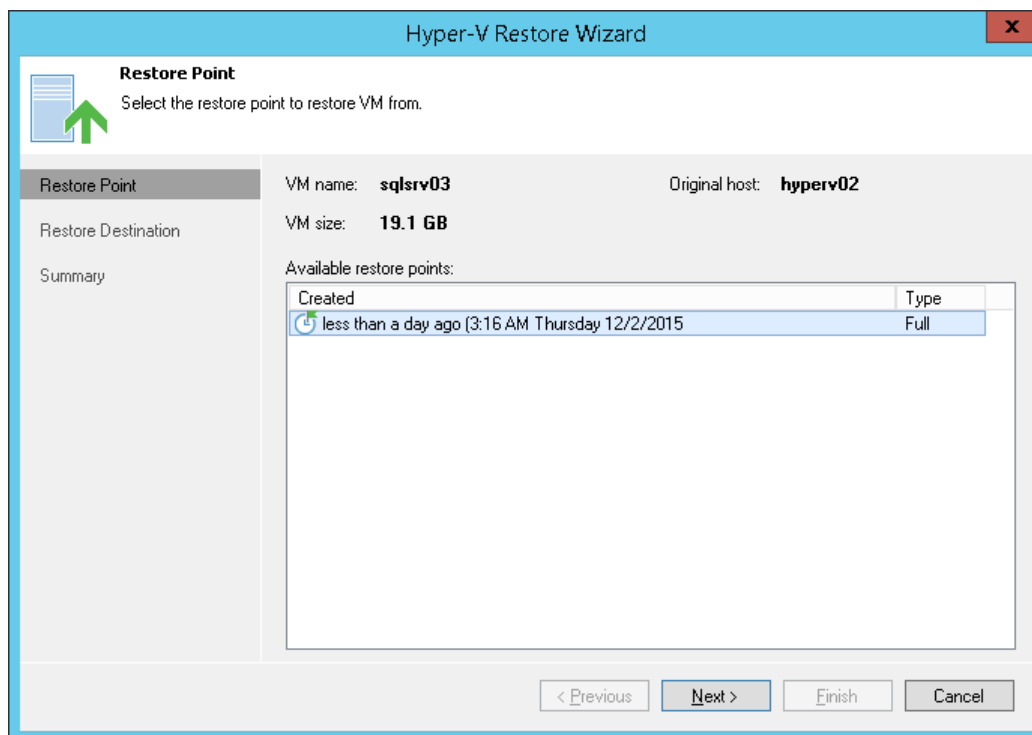
To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM whose files you want to restore.
3. Click **Restore** and select **VM files (VHD, VSV, BIN, XML)**. The **Restore** wizard will be launched.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point from which you want to restore the VM file(s).



The screenshot shows the 'Hyper-V Restore Wizard' window at the 'Restore Point' step. The window has a blue title bar and a sidebar on the left with three options: 'Restore Point' (selected), 'Restore Destination', and 'Summary'. The main area displays the following information:

- VM name: **sqlsrv03**
- Original host: **hyperv02**
- VM size: **19.1 GB**
- Available restore points:

Created	Type
 less than a day ago (3:16 AM Thursday 12/2/2015)	Full

At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 3. Select VM Files and Destination

At the **Restore Destination** step of the wizard, select the VM files you want to restore and destination where the restored files must be stored.

1. From the **Server** list, select where to store VM files: to a Microsoft Hyper-V host, on the backup server or on a Microsoft Windows server added to the backup infrastructure. Use the **Details** button to view or change connection settings of the destination host or server.
2. In the **Path to folder** section, specify a path to the folder on the selected host where files must be restored. To create a dedicated folder for restored files, click **New Folder** at the bottom of the window.
3. In the **VM files to restore** section, select check boxes next to files that you want to restore. By default, all VM files are selected.

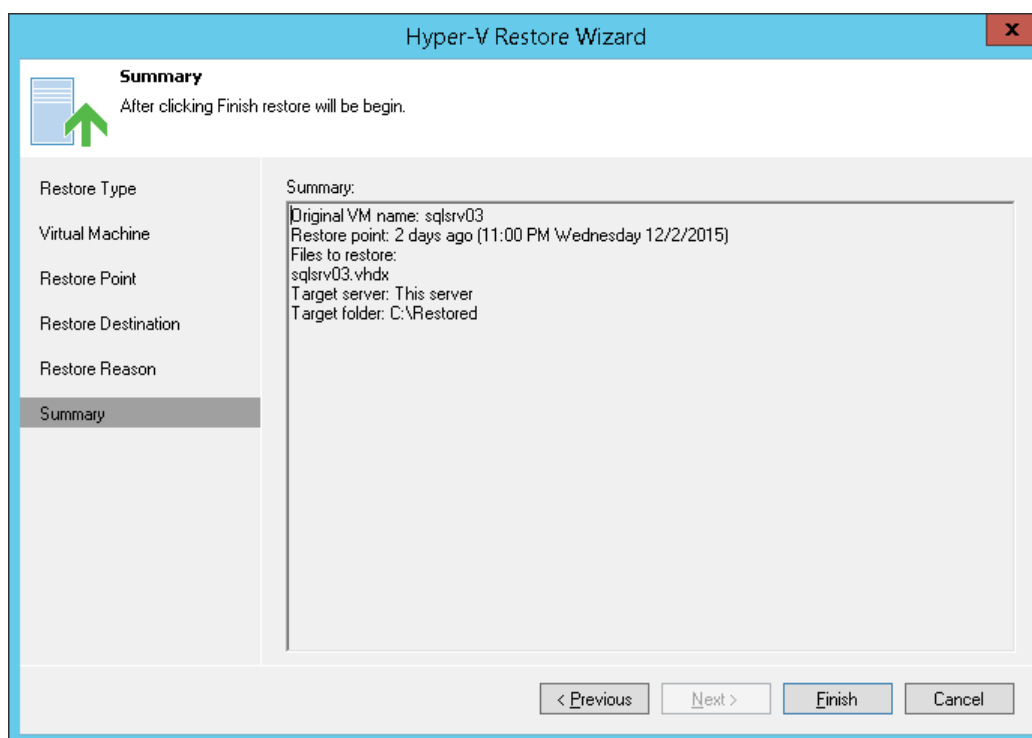
The screenshot shows the 'Hyper-V Restore Wizard' window, specifically the 'Restore Destination' step. The window has a blue title bar and a sidebar on the left with navigation options: 'Restore Type', 'Virtual Machine', 'Restore Point', 'Restore Destination' (which is highlighted), 'Restore Reason', and 'Summary'. The main area contains instructions: 'Choose server and folder where VM files should be restored, and pick files to restore.' Below this, there are three sections: 1. 'Server:' with a dropdown menu showing 'srv02.tech.local' and a 'Details' button. 2. 'Path to folder:' with a text box containing 'C:\Restored' and a 'Browse...' button. 3. 'VM files to restore:' which contains a table with two columns: 'Name' and 'Size'. The table lists two files: '0204A5AB-3523-4946-B658-B8AD5B3...' (16.0 KB) and 'sqlsrv03.vhdx' (19.1 GB). The checkbox for 'sqlsrv03.vhdx' is checked. To the right of the table are 'Select All' and 'Clear All' buttons. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Name	Size
☐ 0204A5AB-3523-4946-B658-B8AD5B3...	16.0 KB
☒ sqlsrv03.vhdx	19.1 GB

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of VM file(s) restore.

1. Review details for the restore task.
2. Click **Finish** to start VM file(s) restore.



Restoring VM Guest Files (FAT, NTFS, ReFS)

In Veeam Backup Free Edition, you can recover individual guest OS files and folders from VeeamZIP files or backups of VMs with FAT, NTFS and ReFS file systems.

When you perform file-level recovery, the VM image is not extracted from the backup. The content of a backup file is mounted directly to the backup server (to the `C:\veeamflr\<vmname>` folder) and displayed in the inbuilt Veeam Backup browser. After that you can copy necessary files and folders to your local machine drive and save them anywhere within the network or simply point applications to the files and use them normally.

Note: Guest OS file-level restore for ReFS is supported only if Veeam Backup Free Edition is installed on Microsoft Windows 2012 or Microsoft Windows 2012 R2 machine.

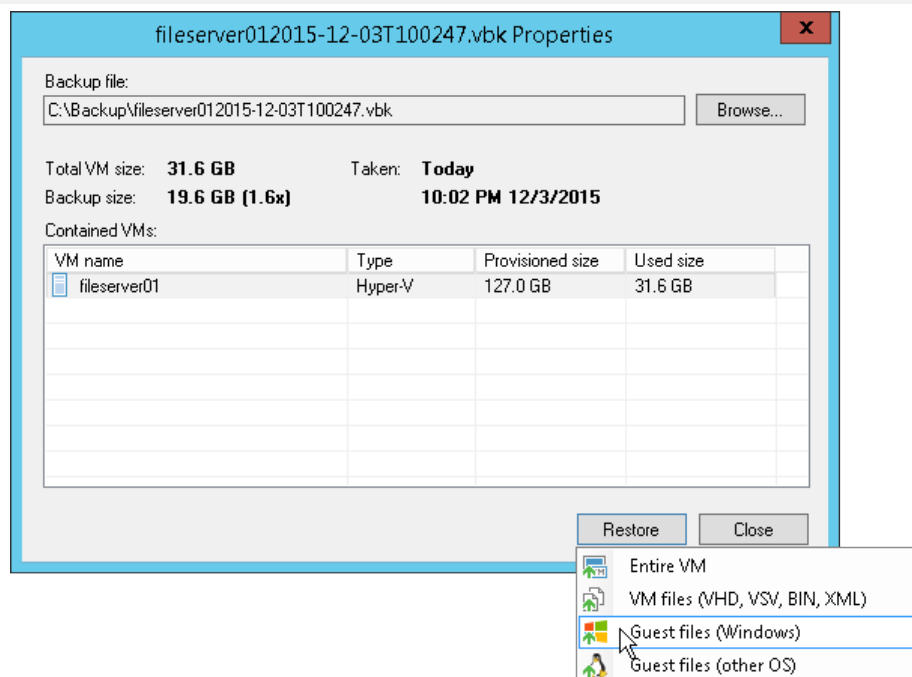
Step 1. Choose File

You can restore VM guest OS files from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM whose guest OS files you want to restore.
3. Click **Restore** and select **Guest files (Windows)**. The Veeam Backup browser will be displayed, and you will be able to **save restored files** to the necessary location.

Important! You cannot perform file-level restore while the VM from which you want to restore VM guest OS files is being backed up.



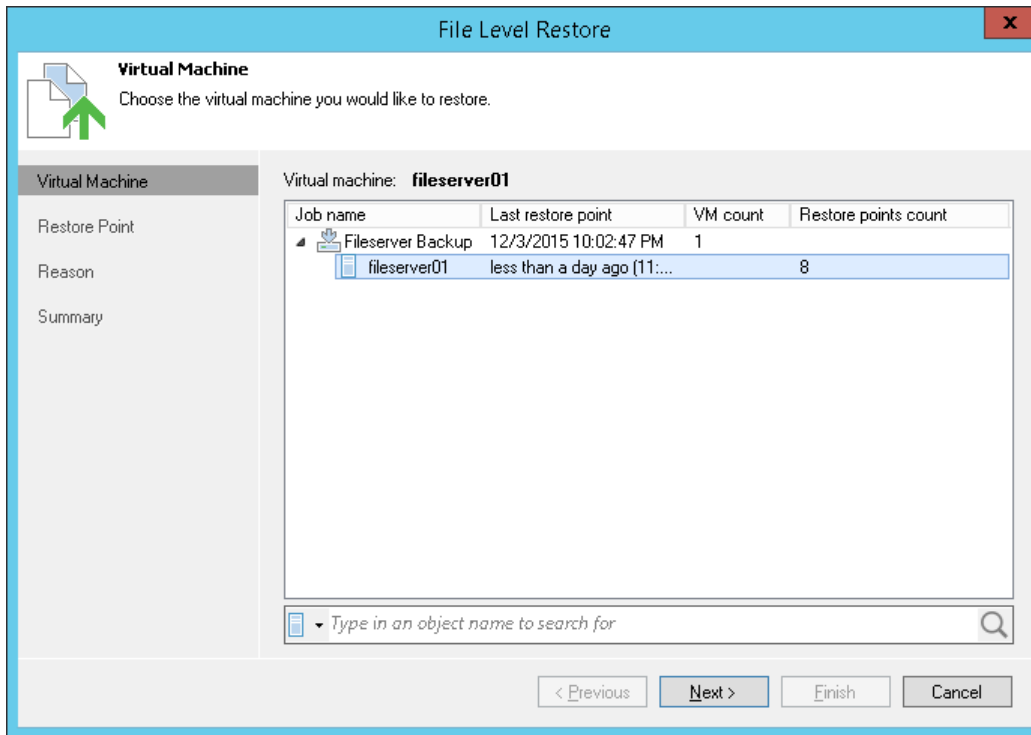
Step 2. Select VM

At the **Virtual Machine** step of the wizard, select the VM whose guest OS files you want to restore:

1. In the **Virtual machine** list, expand the necessary backup.
2. Select the VM.

To quickly find a VM, you can use the search field at the bottom of the window.

1. Enter a VM name or a part of it in the search field.
2. 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 the restore point from which you want to restore the VM guest OS files.

File Level Restore

Restore Point
Select the restore point to restore guest OS files from.

Restore Point | Reason | Summary

VM name: **fileserver01** | Original host: **hyperv02**
VM size: **31.6 GB**

Available restore points:

Created	Type	Backup
less than a day ago (10:02 AM Thursday ...)	Full	fileserver012015-12-03T...

< Previous | **Next >** | Finish | Cancel

Step 4. Specify Restore Reason

At the **Restore Reason** step of the wizard, enter a reason for restoring VM guest OS files. The information you provide will be saved in the session history and you can reference it later.

Tip: If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.

The screenshot shows the 'File Level Restore' wizard window. The title bar is blue and says 'File Level Restore'. The window has a sidebar on the left with four items: 'Virtual Machine', 'Restore Point', 'Reason' (which is highlighted with a grey background), and 'Summary'. The main area has a header 'Reason' with a document icon and a green arrow pointing up. Below the header is a text box with the instruction: 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' The text box contains the text 'Restoring a deleted file'. Below the text box is a checkbox labeled 'Do not show me this page again'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

File Level Restore

Reason
Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.

Virtual Machine
Restore Point
Reason
Summary

Restore reason:
Restoring a deleted file

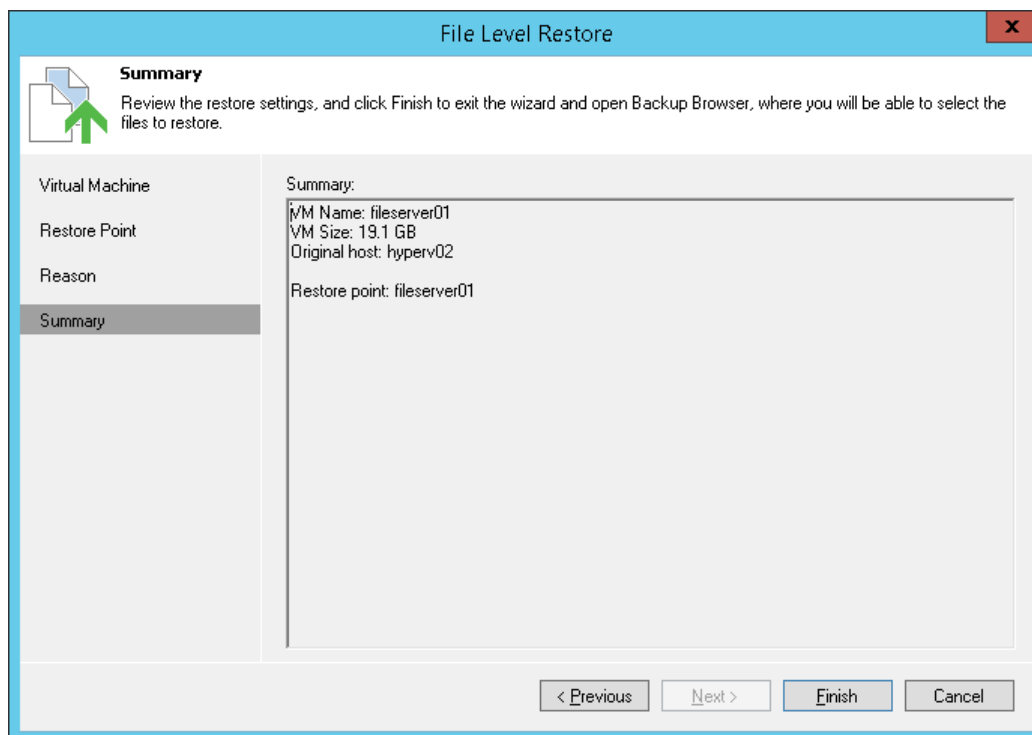
☐ Do not show me this page again

< Previous Next > Finish Cancel

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of VM guest OS files restore.

1. Review details of the restore task.
2. Click **Finish** to start restoring VM guest OS files from the backup.



Step 6. Save Restored Files

After the restore process is complete, Veeam Backup Free Edition opens the Veeam Backup browser displaying the file system tree of the restored VM. Note that names of the restored VM hard disks may differ from the original ones.

You can perform the following operations with VM guest OS files in the Veeam Backup browser:

- Save files and folders to the original location
- Save files and folders to a folder on the backup server or network shared folder
- Launch Veeam Explorers for application item restore
- Open files in Microsoft Windows Explorer

After you finish restoring files, you can close the Veeam Backup browser.

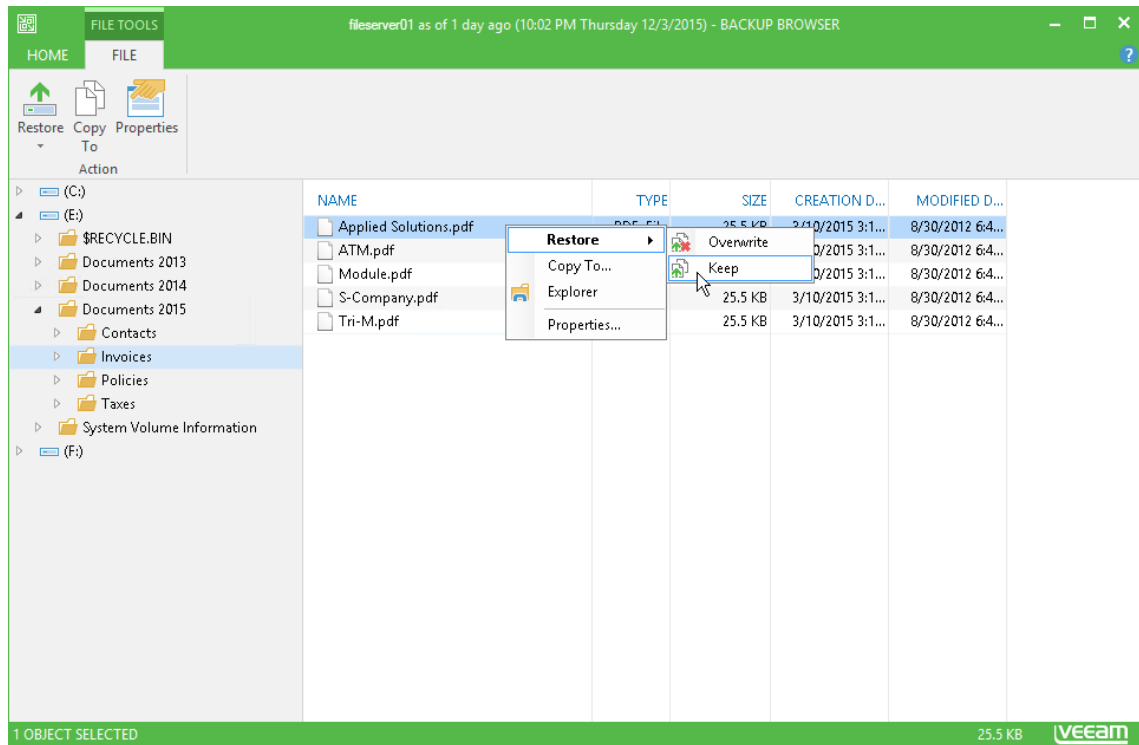
Note: You can browse to the VM guest OS files mounted to the backup server only while the Veeam Backup browser with the restored files is open. After the Veeam Backup browser is closed, the VM disks will be unmounted from the backup server.

Saving Files to Original Location

To save files or folders to their original location, right-click the necessary file or folder in the file system tree or in the details pane on the right and select one of the following commands:

- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**. Veeam Backup Free Edition will add the *RESTORED-* prefix to the original file name and store the restored file in the same folder where the original file resides.

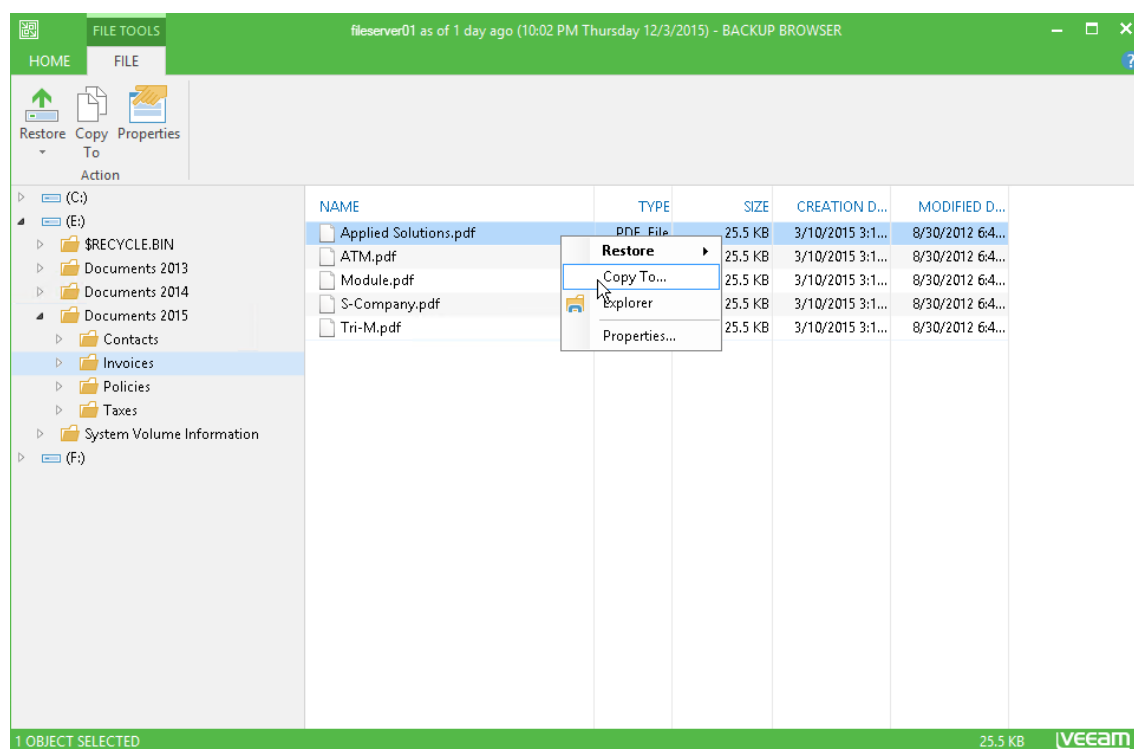
IMPORTANT! Restore to the initial location may fail if you have excluded the system disk from the VM backup. To restore guest OS files in such situation, you can use 1-click file-level restore or copy files to the selected folder and then move them to the original location.



Saving Files to New Location

To save restored files or folders on the local machine or in a network shared folder:

1. Right-click the necessary file or folder in the file system tree or in the details pane on the right and select **Copy To**.
2. Choose to preserve their original NTFS permissions or not:
 - Select the **Preserve permissions and ownership** check box to keep the original ownership and security permissions for restored objects. Veeam Backup Free Edition will copy selected files and folders along with associated Access Control Lists, preserving granular access settings.
 - Leave the **Preserve permissions and ownership** check box not selected if you do not want to preserve the original ownership and access settings for restored objects. Veeam Backup Free Edition will change security settings: the user who launched the Veeam Backup Free Edition console will be set as the owner of the restored object, while access permissions will be inherited from the folder to which the restored object is copied.
3. If prompted, in the **Credentials** window specify settings of the user account to access the destination location.



Launching Veeam Explorers

If you are restoring VM guest OS files of the virtualized Microsoft Active Directory Server, Microsoft Exchange Server, Microsoft SharePoint Server or Microsoft SQL Server or Oracle, you can launch a Veeam Explorer for the necessary application directly from the Veeam Backup browser.

- To start Veeam Explorer for Active Directory, browse to the Microsoft Active Directory database file (DIT) in the Veeam Backup browser, select it and click **Active Directory Items** on the **Home** tab or simply double-click the DIT file.
- To start Veeam Explorer for Exchange, browse to the Microsoft Exchange database file (EDB) in the Veeam Backup browser, select it and click **Exchange Items** on the **Home** tab or simply double-click the EDB file.
- To start Veeam Explorer for SharePoint, browse to the Microsoft SharePoint content database (MDF) in the Veeam Backup browser, select it and click **SharePoint Items** on the **Home** tab or simply double-click the MDF file.
- To start Veeam Explorer for Microsoft SQL, browse to the Microsoft SQL database file in the Veeam Backup browser, select it and click **SQL Server Databases** on the **Home** tab or simply double-click the Microsoft SQL database file. For more information about default locations of Microsoft SQL database files, see <http://technet.microsoft.com/en-us/library/ms143547.aspx>.
- To start Veeam Explorer for Oracle, browse to the Microsoft Oracle content database in the Veeam Backup browser, select it and click **Oracle** on the **Home** tab or double-click the database file.

Working with Windows Explorer

You can use Microsoft Windows Explorer to work with restored files and folders.

1. Click Explore on the ribbon in the Veeam Backup browser or right-click the necessary folder and select **Explore**.
2. Veeam Backup Free Edition will launch Microsoft Windows Explorer. Browse to the necessary VM guest OS files.

You can also start Microsoft Windows Explorer from the **Start** menu of Microsoft Windows and browse to the necessary VM guest OS files. VM disks are mounted under the `C:\veeamflr\<vmname>\<volume n>` folder of the backup server.

It is recommended that you use the Veeam Backup browser instead of Microsoft Windows Explorer for file-level restore. Use of the Veeam Backup browser has the following advantages:

1. You can browse the VM guest OS file system ignoring the file system ACL settings.
2. You can preserve permissions and ownership during file-level restore.

If you open the VM file system via the Microsoft Windows Explorer, these capabilities will not be available.

For more information, see *SeBackupPrivilege* and *SeRestorePrivilege* at [https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb530716(v=vs.85).aspx).

Closing Veeam Backup Browser

You can browse to VM guest OS files mounted to the backup server only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Backup Free Edition unmounts VM disks from the backup server.

It is recommended that you close the Veeam Backup browser after you have finished restoring VM guest OS files. When the Veeam Backup browser is open on the backup server, the backup file whose VM guest OS file system is displayed in the browser is locked on the backup repository. As a result, some scheduled operations that use this backup file may fail.

Veeam Backup Free Edition checks if there is any activity in the Veeam Backup browser with an interval of 5 minutes. If the user or Veeam Backup Free Edition components and services have not performed any actions for 30 minutes, Veeam Backup Free Edition displays a warning that the Veeam Backup browser is to be closed within 5 minutes.

After the warning is displayed, you can perform one of the following actions:

- You can close the Veeam Backup browser manually.
- You can click **Cancel** to postpone the close operation. In this case, the Veeam Backup browser will remain open for 5 minutes. After this period expires, Veeam Backup Free Edition will display the warning again.
- You can perform no action at all. In this case, the Veeam Backup browser will be automatically closed in 5 minutes.

Restoring VM Guest OS Files (Multi-OS Restore Wizard)

Because Windows cannot read other file systems natively, Veeam Backup Free Edition provides multi-OS file-level recovery that allows reading data from 16 different OS file systems.

OS	Supported File Systems
Linux	ext ext2 ext3 ext4 ReiserFS JFS XFS
BSD	UFS UFS2
Mac	HFS, HFS+ (volumes up to 2 TB)
Solaris	UFS ZFS (except any pool versions of Oracle Solaris)

To restore files from VM guest OS'es, Veeam Backup Free Edition utilizes its patent-pending approach using a special FLR helper. The FLR helper is a virtual appliance running a stripped-down Linux kernel that has a minimal set of components. The appliance is very small, at around 20 MB, and takes only 10-20 seconds to boot.

The FLR helper appliance is created directly on the selected Hyper-V host. Whenever you perform file-level restore, Veeam Backup Free Edition automatically starts the appliance and mounts the VM disks to the FLR appliance as virtual hard drives. VM disks are mounted directly from backup files without prior extraction of the backup content.

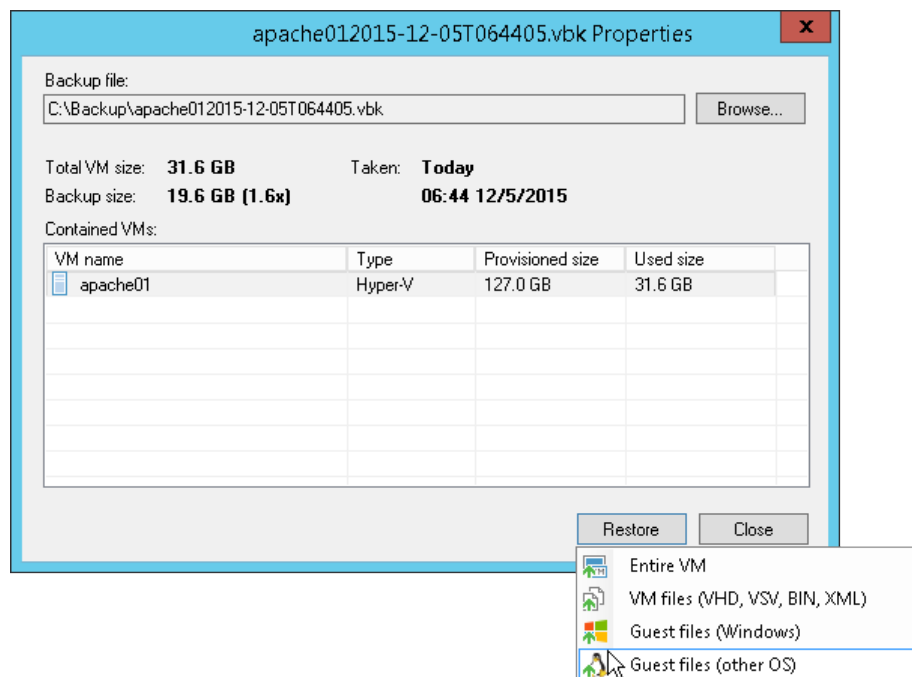
Once the restore process is complete, the wizard displays the file browser window, providing you with direct access to the VM file system. You can then copy necessary files and folders to your local machine drive or save them anywhere within the network. Alternatively, you can allow users to restore files on their own by enabling the FTP server on the virtual appliance.

Step 1. Choose File

You can restore VM guest OS files from a VeeamZIP file created in Veeam Backup Free Edition and from a backup file or a VeeamZIP file created in Veeam Backup & Replication.

To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM whose guest OS files you want to restore.
3. Click **Restore** and select **Guest files (other OS)**. The **File Level Restore** wizard will be launched.

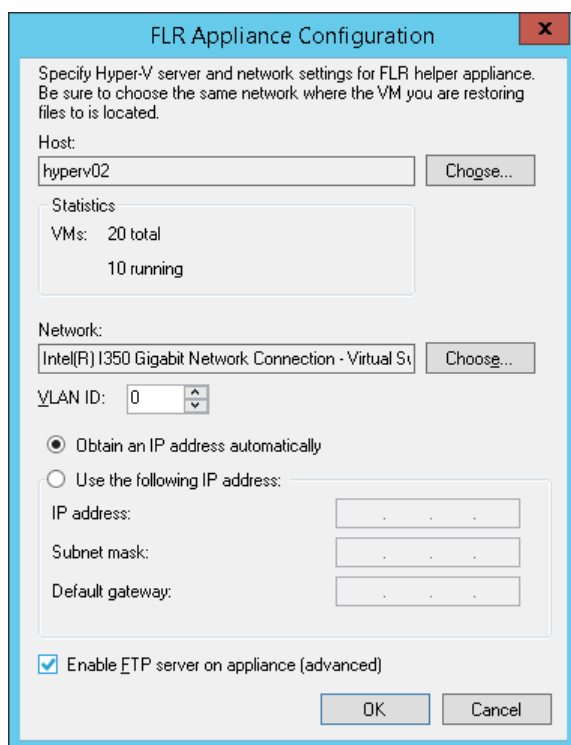


Step 2. Select Location for Proxy Appliance

At the **Ready** step of the wizard, select a Microsoft Hyper-V host for placing the proxy appliance. When the restore process starts, Veeam Backup Free Edition will register the proxy appliance on the Microsoft Hyper-V host and mount disks of the restored VM to this proxy appliance. The file system tree of the restored VM will be displayed in the file browser. After you restore necessary files and finish working with the file browser, the VM disks will be unmounted from the proxy appliance and the proxy appliance will be deleted from the Microsoft Hyper-V host.

To locate the appliance:

1. Click **Customize** at the bottom of the window.
2. In the **FLR Appliance Configuration** window, select the Microsoft Hyper-V host on which the proxy appliance will be registered.
3. In the **Network** section, specify an IP address and other network settings for the proxy appliance. The proxy appliance must be placed in the same network where the backup server resides.
4. If you use VLAN IDs, set the correct VLAN ID of the network where the proxy appliance must reside.
5. To enable FTP access to the restored file system, select the **Enable FTP server on appliance** check box. As a result, users will be able to access the proxy appliance via FTP, browse the file system of the restored VM and download necessary files on their own.
6. Click **OK**.



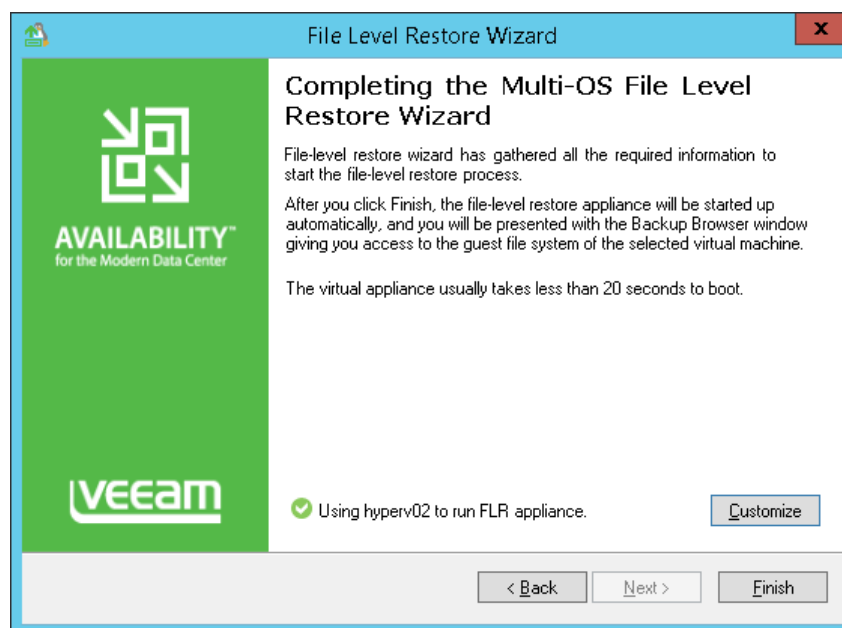
The screenshot shows the 'FLR Appliance Configuration' dialog box. It has a title bar with a close button (X). The main area contains instructions: 'Specify Hyper-V server and network settings for FLR helper appliance. Be sure to choose the same network where the VM you are restoring files to is located.' Below this, there are sections for 'Host' and 'Network'. The 'Host' section has a text box with 'hyperv02' and a 'Choose...' button. The 'Network' section has a text box with 'Intel(R) I350 Gigabit Network Connection - Virtual S' and a 'Choose...' button. Below the network selection, there is a 'VLAN ID' spinner box set to '0'. There are two radio buttons: 'Obtain an IP address automatically' (selected) and 'Use the following IP address:'. The latter has three text boxes for 'IP address:', 'Subnet mask:', and 'Default gateway:', each with a placeholder '...'. At the bottom, there is a checked checkbox 'Enable FTP server on appliance (advanced)' and 'OK' and 'Cancel' buttons.

Note: If the proxy appliance is deployed on Microsoft Hyper-V Server 2008 R2 or Microsoft Windows 2008 R2 server with the Hyper-V role enabled, Veeam Backup Free Edition will not be able to browse VHDX virtual disks. Veeam Backup Free Edition will only browse .VHD virtual disks. To browse VHDX virtual disks, deploy the proxy appliance on:

- Microsoft Hyper-V Server 2012
- Microsoft Windows 2012 server with the Hyper-V role enabled
- Microsoft Hyper-V Server 2012 R2
- Microsoft Windows 2012 R2 server with the Hyper-V role enabled

Step 3. Finish Working with Wizard

At the last step of the wizard, click **Finish** to start restoring VM guest OS files. The file-level restore appliance may take about 10-40 seconds to boot.



Step 4. Save Restored Files

When the restore process is complete, Veeam Backup Free Edition opens the Veeam Backup browser displaying the file system tree of the restored VM.

You can save the restored files and folders to their original location, new location or access files on FTP.

Note: You can browse the VM guest OS files and access restored files on the FTP only while the Veeam Backup browser with the restored files is open. After the Veeam Backup browser is closed, the VM disks will be unmounted from the proxy appliance, and the proxy appliance will be deleted from the ESX(i) host.

Saving Files to Original Location

To save files and folders to the original location, right-click the necessary file or folder in the file system tree or in the details pane on the right and select one of the following commands:

- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**. Veeam Backup Free Edition will add the *RESTORED-* prefix to the original file name and store the restored file in the same folder where the original file resides.

To restore files to the original location, Veeam Backup Free Edition uses the account for VM guest OS access specified in the backup job settings. If this account does not have sufficient rights to access the target VM, you will be prompted to enter credentials. In the **Credentials window**, specify a user account to access the destination location (server or shared folder). You can use the account under which you are currently logged on, or a different account.

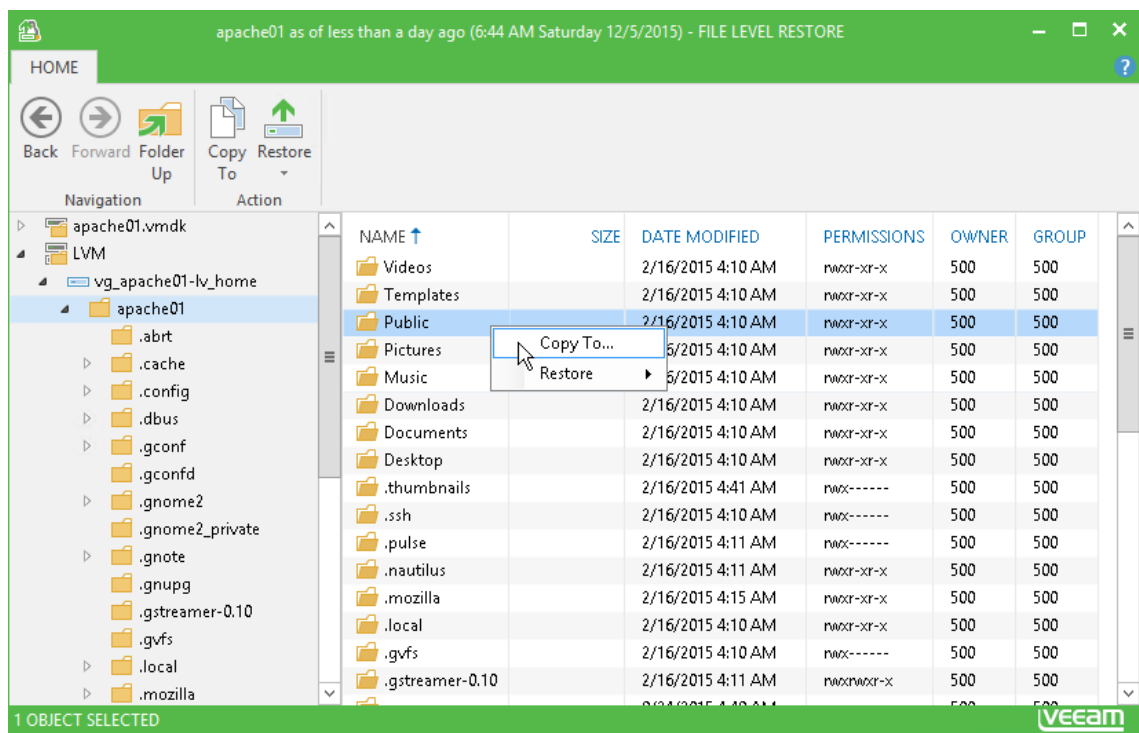
Saving Files to New Location

To save files and folders to a new location:

1. Right-click the necessary file or folder and select **Copy to**.
2. In the **Select Destination** window, select the destination server (local or remote) from the list or provide a path to the shared folder.
 - If you are recovering files to a Linux server, you can select the destination server from the list or add a destination server ad-hoc. To do this, scroll down the list of servers and choose **Specify a different host** at the end of the list. Follow the steps of the wizard to add a Linux server that will be used as a destination host.

The server you add ad-hoc will not appear in the list of managed hosts in Veeam Backup Free Edition: its purpose is to host the files that you recover. It will only remain visible in the Veeam Backup browser until all currently active file-level restore sessions are completed.
 - If you are recovering files to a shared folder, specify a path to the destination folder.
3. If you want to preserve original permissions and ownership for recovered files, select the **Preserve permissions and ownership** check box.
4. If prompted, in the **Credentials** window specify settings of the user account to access the destination location.

Important! To restore original permissions and ownership settings, the account you have specified should have privileges to change the owner on the selected server or shared folder.



Accessing Files over FTP

If you have chosen to enable FTP server on the FLR appliance, the restored file system will also be available over FTP at `ftp://<FLR_appliance_IP_address>`. Other users in the same network can access the FLR appliance to restore the files they need.

Performing File Copy

Veeam Backup Free Edition enables you to copy files and folders between ESX(i), Microsoft Hyper-V, Microsoft Windows and Linux hosts as well as schedule file copying jobs.

- [Copying Files and Folders Manually](#)
- [Creating File Copy Jobs](#)
- [Managing Folders](#)
- [Editing and Deleting Files](#)

Copying Files and Folders Manually

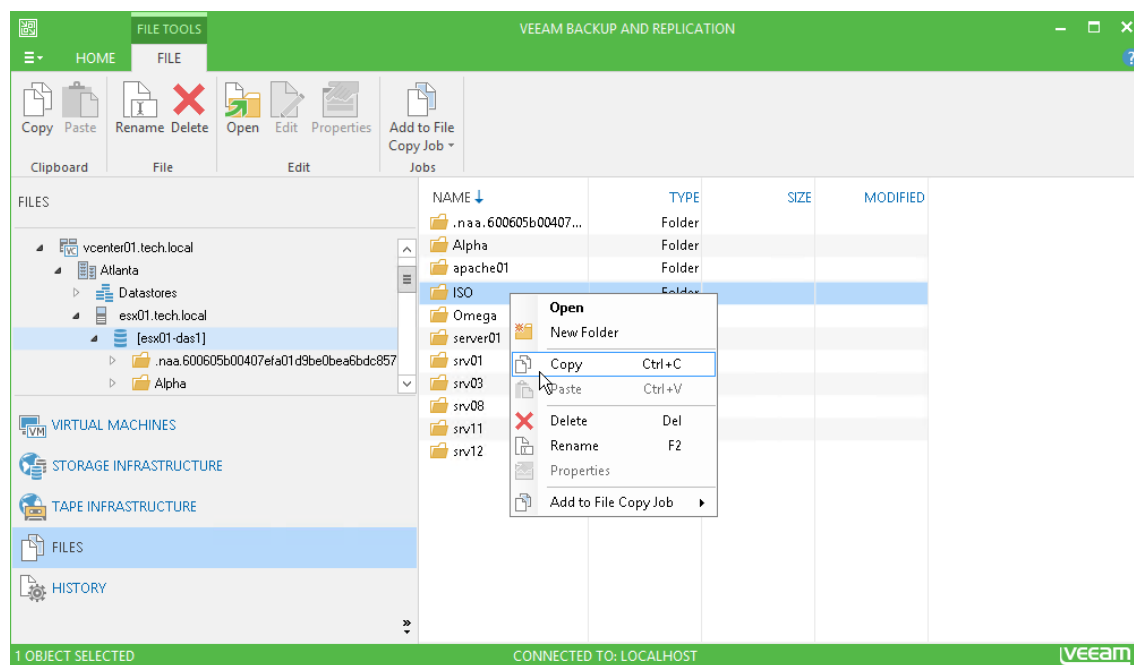
You can manually copy and move files and folders between hosts, Microsoft Windows servers and Linux hosts in the backup infrastructure.

Before you begin the copying operation, make sure that the source and target hosts or servers are added to the backup infrastructure.

To copy files and folders:

1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the source server or host.
3. Right-click files and folders that you want to copy and select **Copy**.
4. In the inventory pane, expand the file tree of the target server or host.
5. Right-click a destination folder and select **Paste**.

You can also use a drag-n-drop operation to copy files and folders between the source and target hosts or servers.



Creating File Copy Jobs

To schedule a copying process for files and folders, you must configure a file copy job. You can run the file copy job immediately after its creation, schedule or save the job.

Before you configure a file copy job, **check prerequisites**. Then use the **New File Copy Job** wizard to create a job.

Before You Begin

Before you configure a file copy job, check the following prerequisites:

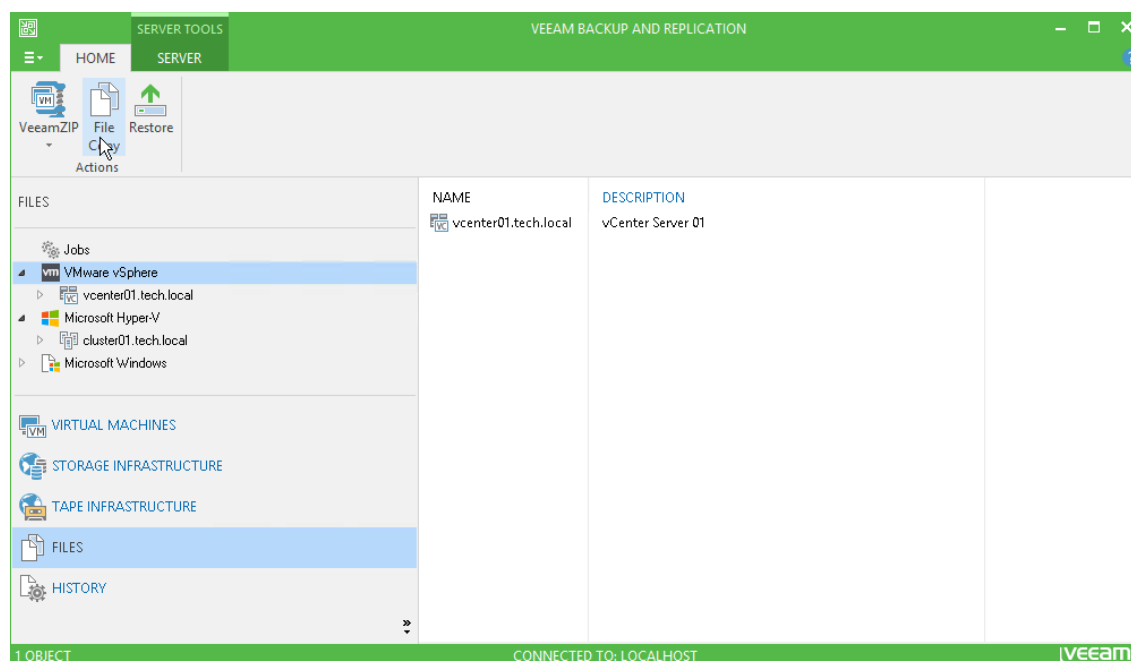
Backup infrastructure components that will take part in the file copying process must be added to the backup infrastructure and properly configured. These include a source and target host or server between which files and folders will be copied.

Step 1. Launch New File Copy Job Wizard

To launch the **New File Copy Job** wizard, do either of the following:

- On the **Home** tab, click **File Copy**.
- Open the **Files** view, in the working area right-click the necessary files and folders and select **Add to File Copy Job > New job**. Veeam Backup Free Edition will start the **New File Copy Job** wizard and add selected files and folders to this job. You can add other files and folders to the job later on, when you pass through the wizard steps.

You can add files and folders to already existing jobs. To do this, open the **Files** view, in the working area right-click necessary objects and select **Add to file copy job > name of the job**.



Step 2. Specify Job Name and Description

At the **Name** step of the wizard, enter the name and description of the created job.

1. In the **Name** field, enter a name for the file copy job.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created a job, date and time when the job was created.

New File Copy Job

Name
Type in a name and description for this file copy job.

Name:
Daily File Copy

Description:
Daily File Copy Job

< Previous **Next >** Finish Cancel

Step 3. Select Files and Folders to Be Copied

At the **Source** step of the wizard, select files and folders that you want to copy.

1. From the **Host** list, choose a host or server on which files or folders that you want to copy reside.
2. Click **Add** and select files or folders that must be copied. The selected items will be added to the list.

To remove a file or folder from the list, select it and click **Remove**.

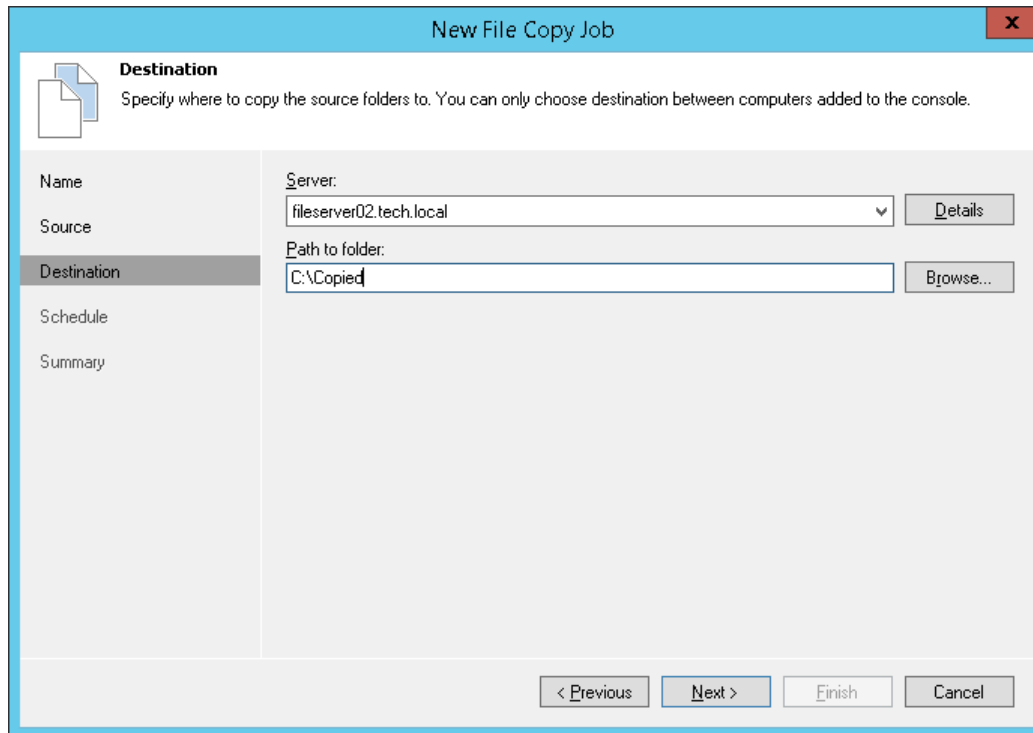
The screenshot shows the 'New File Copy Job' wizard in the 'Source' step. The window has a blue title bar with the text 'New File Copy Job' and a close button. On the left is a sidebar with a tree view containing 'Name', 'Source' (selected), 'Destination', 'Schedule', and 'Summary'. The main area is titled 'Source' with a subtitle 'Select items to be copied with this job.' and a document icon. Below this, there is a 'Server:' dropdown menu currently showing 'fileserver01.tech.local'. Underneath is a table titled 'Items to copy:' with two columns: 'Item' and 'Host'. The first row of the table contains 'C:\Data' and 'fileserver01.tech.local'. To the right of the table are 'Add...' and 'Remove' buttons. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Item	Host
C:\Data	fileserver01.tech.local

Step 4. Select Destination for Copying

At the **Destination** step of the wizard, select a destination to which files or folders must be copied.

1. From the **Server** list, select the target host or server.
2. Click **Details** on the right of the **Server** field to view or edit server properties.
3. Click **Browse** next to the **Path to folder** field and select a folder where copied items must be stored. To create a dedicated folder for copied files or folders, use the **New Folder** button at the bottom of the **Select Folder** window.



The screenshot shows the 'New File Copy Job' wizard window. The title bar is 'New File Copy Job'. The main window has a sidebar on the left with tabs: 'Name', 'Source', 'Destination' (selected), 'Schedule', and 'Summary'. The main area is titled 'Destination' and contains the text: 'Specify where to copy the source folders to. You can only choose destination between computers added to the console.' Below this, there are two input fields: 'Server:' with a dropdown menu showing 'fileserv02.tech.local' and a 'Details' button to its right; and 'Path to folder:' with a text box containing 'C:\Copied' and a 'Browse...' button to its right. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 5. Define the Job Schedule

At the **Schedule** step of the wizard, you can select to run the file copy job manually or schedule the job to run on a regular basis.

To specify the job schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the job manually to copy files or folders.
2. Define scheduling settings for the job:
 - To run the job at specific time daily, on defined week days or with specific periodicity, select **Daily at this time**. Use the fields on the right to configure the necessary schedule.
 - To run the job once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.
 - To run the job repeatedly throughout a day with a set time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*. Click **Schedule** and use the time table to define the permitted time window for the job. In the **Start time within an hour** field, specify the exact time when the job must start.

The repeatedly run job are started by the following rules:

- Veeam Backup Free Edition always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
- If you define permitted hours for the job, after the denied interval is over, Veeam Backup Free Edition will immediately start the job and then run the job by the defined schedule.

For example, you have configured a job to run with a 2-hour interval and defined permitted hours from 9:00 AM to 5:00 PM. According to the rules above, the job will first run at 9:00 AM, when the denied period is over. After that, the job will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.

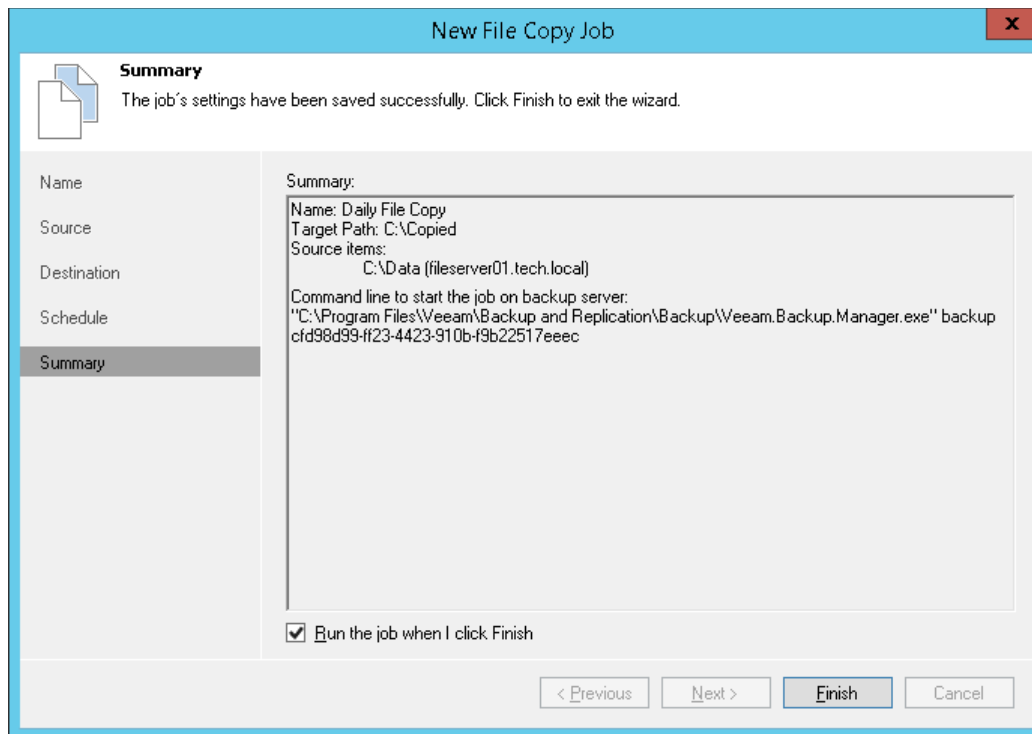
- To run the job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right.
- To chain jobs, use the **After this job** field. In the common practice, jobs start one after another: when job A finishes, job B starts and so on. If you want to create a chain of jobs, you should define the time schedule for the first job in the chain. For the rest of the jobs in the chain, at the **Schedule** step of the wizard, select the **After this job option** and choose the preceding job from the list.

The screenshot shows the 'New File Copy Job' wizard, specifically the 'Schedule' step. The window has a blue title bar with the text 'New File Copy Job' and a red close button. On the left, there is a sidebar with a tree view containing 'Name', 'Source', 'Destination', 'Schedule' (which is selected and highlighted), and 'Summary'. The main area of the window has a light blue header with a document icon and the title 'Schedule'. Below the header, it says 'Please specify job scheduling options. If you do not set the schedule, the job will need to be run manually.' The main content area contains a checkbox labeled 'Run the job automatically' which is checked. Below this checkbox are four radio button options: 'Daily at this time:', 'Monthly at this time:', 'Periodically every:', and 'After this job:'. The 'Daily at this time:' option is selected. It has a time input field set to '10:00 PM', a frequency dropdown set to 'Everyday', and a 'Days...' button. The 'Monthly at this time:' option has a time input field set to '10:00 PM', a frequency dropdown set to 'Fourth', a day dropdown set to 'Saturday', and a 'Months...' button. The 'Periodically every:' option has a frequency input field set to '1', a unit dropdown set to 'Hours', and a 'Schedule...' button. The 'After this job:' option has a dropdown menu showing 'Apache Backup (Daily Job for Apache)'. At the bottom of the window, there are four buttons: '< Previous', 'Create', 'Finish', and 'Cancel'.

Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of file copy job configuration.

1. Review details for the created file copy job.
2. 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.
3. Click **Finish** to close the wizard.



Managing Folders

You can create, rename and delete folders in the **Files** view of Veeam Backup Free Edition.

To create a folder:

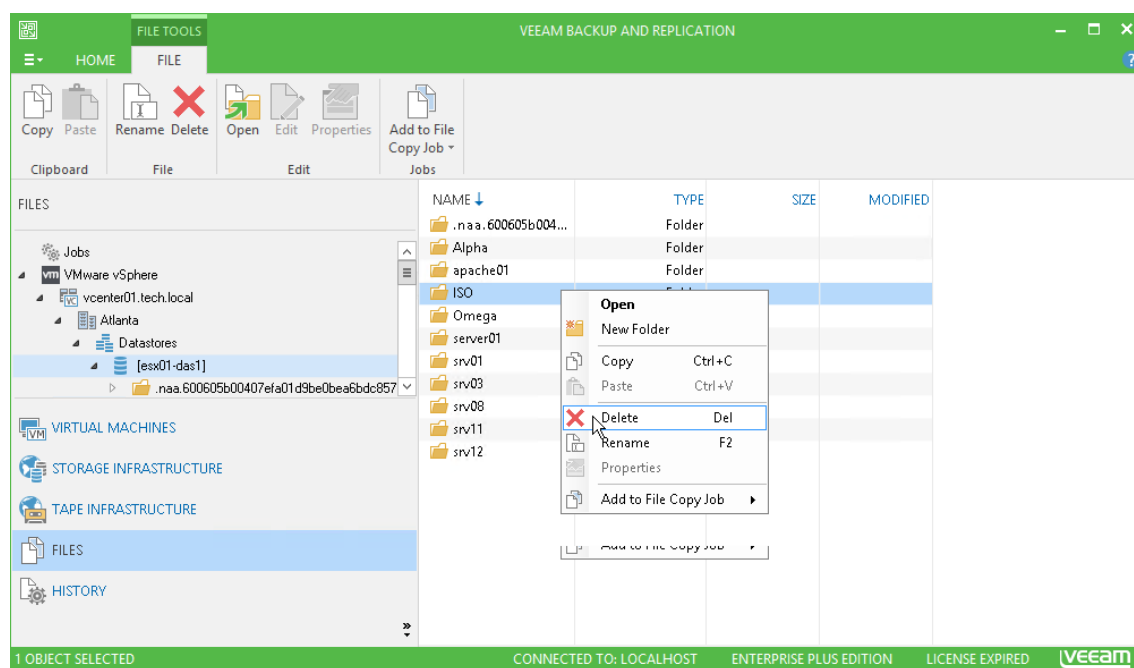
1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the necessary server or host.
3. In the working area, right-click anywhere on the blank area and select **New Folder**.

To rename a folder:

1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the necessary server or host.
3. In the working area, select the folder and click **Rename** on the ribbon or right-click the folder and select **Rename**.
4. Enter a new name for the folder and press **[ENTER]**.

To remove a folder:

1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the necessary server or host.
3. In the working area, select the folder and click **Delete** on the ribbon or right-click the folder and select **Delete**.



Editing and Deleting Files

You can edit files and delete them in the **Files** view of Veeam Backup Free Edition. For example, you may want to edit a configuration file of the VM (VMX) or need to delete from the storage files of unused VMs.

To edit a file:

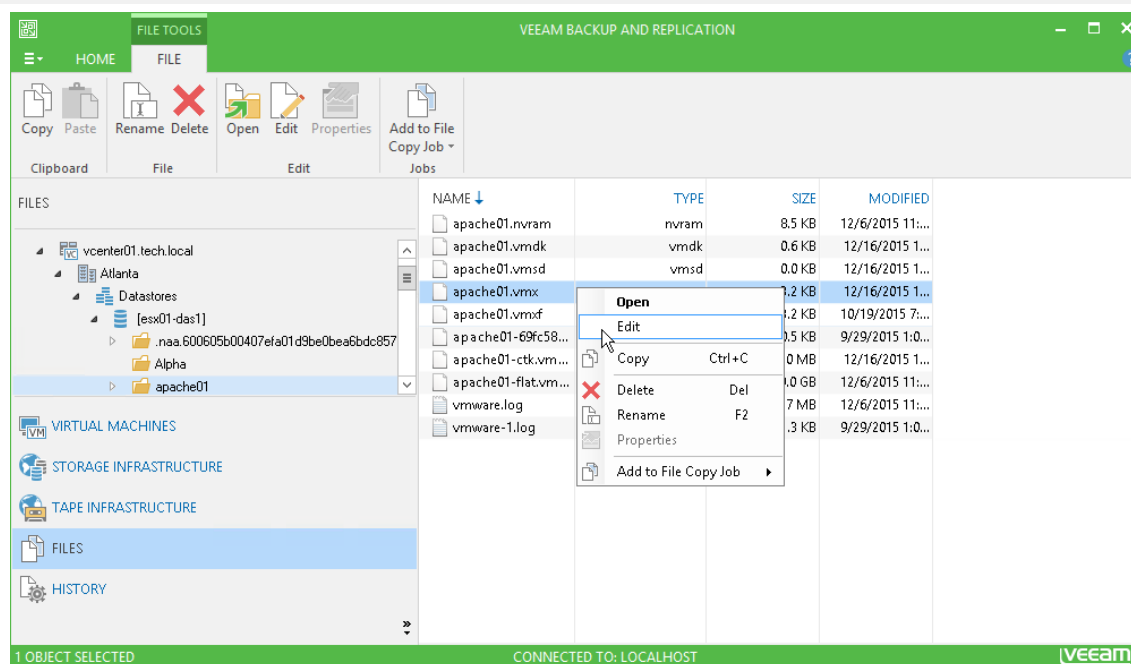
1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the necessary server or host.
3. In the working area, select the file and click **Edit** on the ribbon or right-click the folder and select **Edit**.
4. Veeam Backup Free Edition will open the selected file in the editor. Edit the file as required and click **Save** on the file editor toolbar or press **[CTRL+S]**.

To delete a file:

1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the necessary server or host.
3. In the working area, select the file and click **Delete** on the ribbon or right-click the folder and select **Delete**.

Note:

To delete a folder on VSAN, you must remove a real folder, not a symbolic link to this folder. The real folder is named with GUID, for example, *c07a2953-8096-5b20-a11a-002590c5857c*, while the symbolic link contains the folder name, for example, *srv02_vm*. If you delete the folder symbolic link, the delete operation will fail, and the folder will not be removed.



Performing Quick Migration

You can relocate one or more VMs with quick migration. Quick migration can be used to move VMs from one ESX(i) host to another one, move VM disks to another datastore or both. You can perform "hot" quick migration for running VMs or "cold" quick migration for VMs that are powered off.

Quick migration is not job-driven: it cannot be saved as a job or scheduled to run later. Veeam Backup Free Edition will start relocating VMs immediately after you finish working with the **Quick Migration** wizard.

Before starting quick migration, **check prerequisites**. Then use the **Quick Migration** wizard to migrate VMs.

Before You Begin

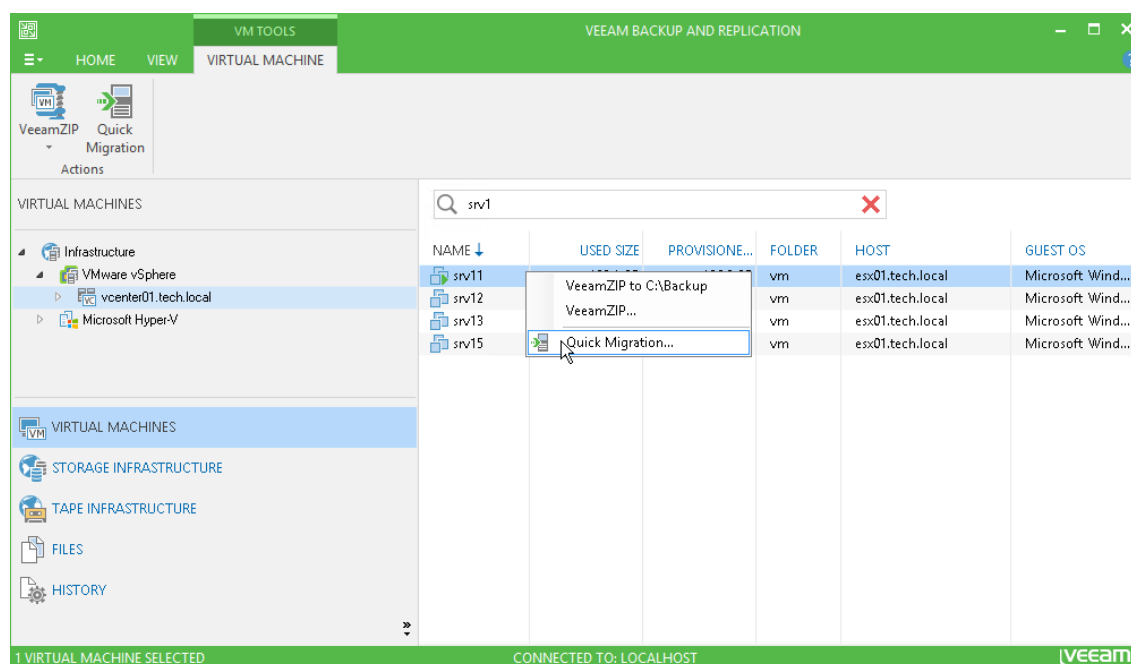
Before you perform quick migration, check the following prerequisites:

- Backup infrastructure components that will take part in quick migration must be added to the backup infrastructure and properly configured. These include the source and target ESX(i) hosts.
- The target datastore must have enough free space to store disks of the migrated VM(s).
- If you want use VMware vSphere vMotion to relocate VMs between hosts and/or VMware vSphere Storage vMotion to relocate VM disks between datastores, make sure that you have a VMware vSphere license covering these features.

Step 1. Launch Quick Migration Wizard

To launch the **Quick Migration** wizard, do the following:

- Open the **Virtual Machines** view. In the working area, select one or more VMs and click **Quick Migration** on the **Virtual Machine** tab.
- Open the **Virtual Machines** view. In the working area, right-click one or more VMs and select **Migration**.



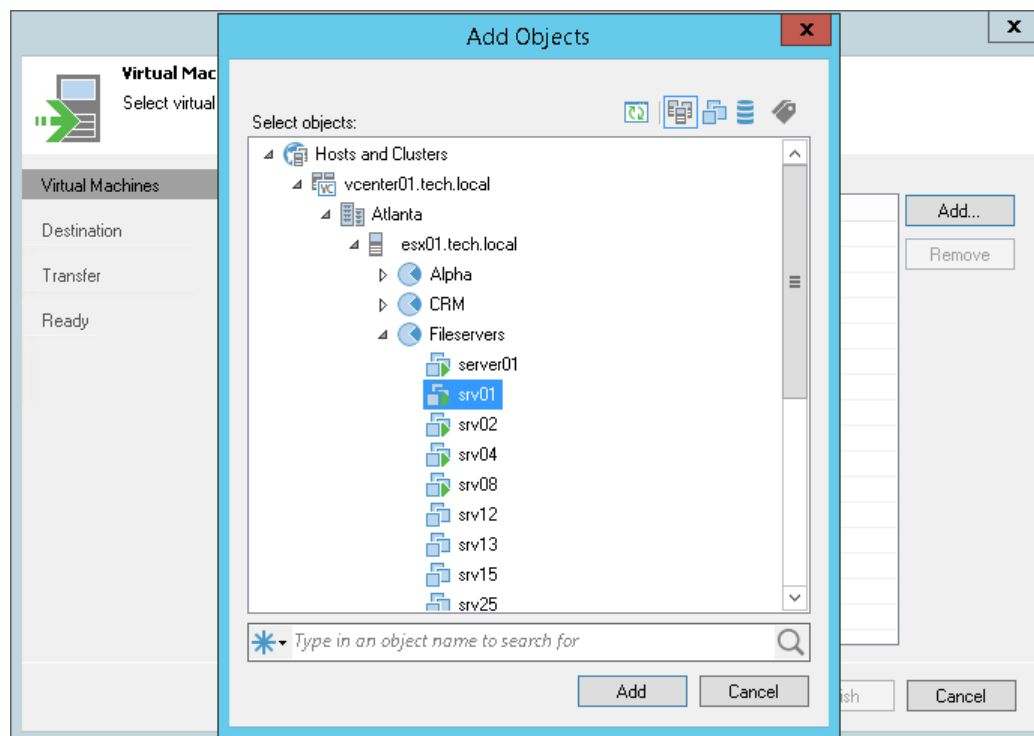
Step 2. Select Virtual Machines to Relocate

At the **Virtual Machines** step of the wizard, select the VM(s) and VM containers that you want to relocate.

1. Click **Add**.
2. Use the toolbar at the top right corner of the window to switch between views: **Hosts and Clusters**, **VMs and Templates**, **Datastores and VMs** and **Tags**. Depending on the view you select, some objects may not be available. For example, if you select the **VMs and Templates** view, no resource pools, hosts or clusters will be displayed in the tree.
3. Select the necessary object and click **Add**.

To quickly find the necessary object, you can use the search field at the bottom of the **Add Objects** window.

1. Click the button to the left of the search field and select the necessary type of object to search for: *Everything*, *Folder*, *Cluster*, *Host*, *Resource pool*, *VirtualApp* or *Virtual machine*.
2. Enter the object name or a part of it in the search field.
3. Click the **Start search** button on the right or press **[ENTER]**.



Step 3. Specify VM Destination

At the **Destination** step of the wizard, select the destination to which the selected VM(s) must be relocated.

1. Click **Choose** next to the **Host or cluster** field and select an ESX(i) host or cluster where the relocated VM must be registered.
2. If all or majority of relocated VMs must belong to the same resource pool, click **Choose** next to the **Resource pool** field and select the target resource pool.

If you want to place relocated VMs to different resource pools:

- a. Click the **Pick resource pool for selected VMs** link.
 - b. In the **Choose Resource Pool** window, click **Add VM** on the right and select the VMs.
 - c. Select the added VM in the **VM resource pool** list and click **Resource Pool** at the bottom of the window.
 - d. From the list of available resource pools, select the target resource pool.
3. If all or majority of relocated VMs must be placed to the same folder, click **Choose** and select the folder.

If you want to place relocated VMs to different folders:

- a. Click the **Pick VM folder for selected VMs** link.
- b. In the **Choose Folder** window, click **Add VM** on the right and select the VMs.
- c. Select the added VM in the **VM folder** list and click **VM Folder** at the bottom of the window.
- d. From the list of available folders, select the target folder.

The **VM folder** section is disabled if you selected a standalone ESX(i) host as a target for VM relocation.

4. If all or majority of relocated VMs must be stored on the same datastore, click **Choose** and select the datastore. Veeam Backup Free Edition displays only those datastores that are accessible by the selected ESX(i) host. If you have chosen relocate VMs to a cluster, Veeam Backup Free Edition will display only shared datastores.

If you want to place relocated VMs to different datastores:

- a. Click the **Pick datastore for selected virtual disks** link.
- b. In the **Choose VM Files Location** window, click **Add VM** on the right and select the VM that must be placed on datastores.
- c. Select the added VM in the **Files location** list and click **Datastore** at the bottom of the window.
- d. From the list of available datastores, select the target datastore.

You can choose to store VM configuration files and disk files in different locations.

- a. Add the VM to the **Files location** list, expand the VM and select the required type of files.
- b. Click **Datastore** at the bottom of the window and choose the destination for the selected type of files.

5. By default, Veeam Backup Free Edition saves disks of relocated VMs in the thin format. If necessary, you can change the disk format. For example, if the original VM uses thick disks, you can change the disk format of the relocated VM to thin provisioned and save on disk space required to store VM data.

Disk format change is available only for VMs using virtual hardware version 7 or later.

To change VM disk format:

- a. Click the **Pick datastore for selected virtual disks** link.
- b. In the **Choose VM Files Location** window, click **Add VM** on the right and select the VM whose disk format you want to change.
- c. Select the added VM in the list and click **Disk type** at the bottom of the window.
- d. In the **Disk Type Settings** section, choose the format that will be used to restore VM disk files: same as the source disk, thin or thick.

The screenshot shows the 'Quick Migration Wizard' window, specifically the 'Destination' step. The window has a blue title bar and a sidebar on the left with four steps: 'Virtual Machines', 'Destination' (selected), 'Transfer', and 'Ready'. The main area contains the following fields and controls:

- Host or cluster:** A text box containing 'esx02.tech.local' and a 'Choose...' button.
- Resource pool:** A text box containing 'Resources' and a 'Choose...' button.
- VM folder:** A text box containing 'vm' and a 'Choose...' button.
- Datastore:** A text box containing 'esx02-ds1 [2.8 TB free]' and a 'Choose...' button.
- Below the 'Datastore' field, there is a blue link that says 'Pick datastore for selected virtual disks'.
- At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

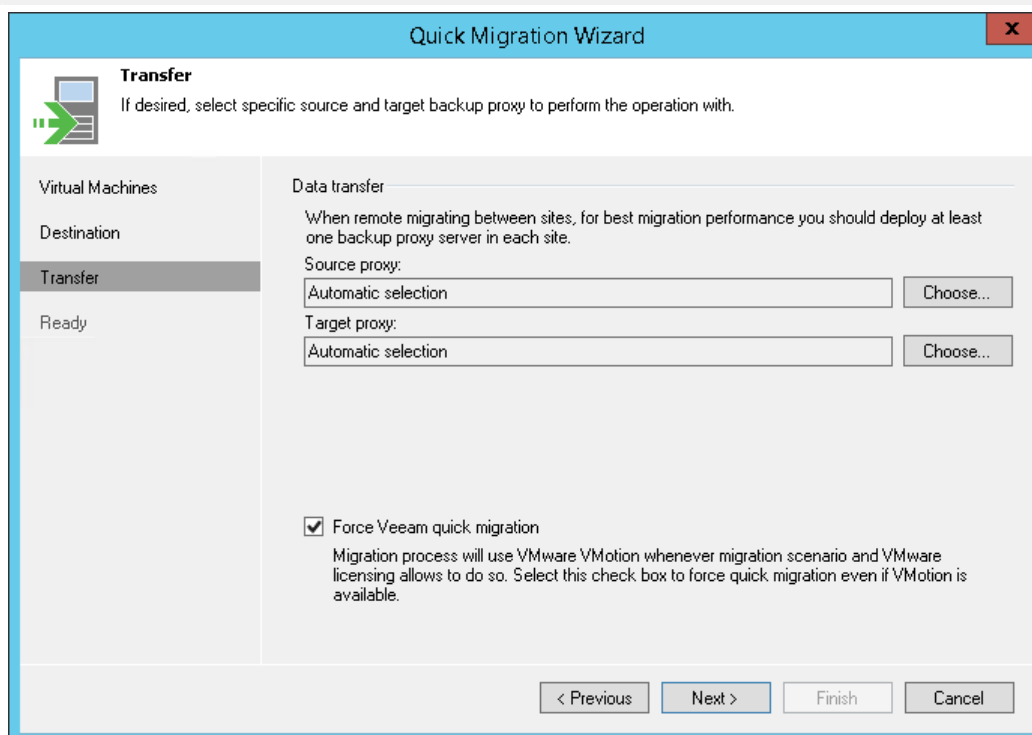
Step 4. Select Infrastructure Components for Data Transfer

At the **Transfer** step of the wizard, you can optionally select which migration mechanism to use: VMware vMotion or Veeam Quick Migration.

- If you want to use VMware vMotion to relocate the VM(s), leave the **Force Veeam quick migration** check box not selected. In this case, Veeam Backup Free Edition will attempt to use the VMware vMotion mechanism to migrate the selected VM(s). If VMware vMotion cannot be used for some reason, for example, if you do not have a VMware vSphere license for this functionality, Veeam Backup Free Edition will use its native migration mechanism.
- If you do not want to use VMware vMotion, select the **Force Veeam quick migration** check box. Veeam Backup Free Edition will use its native migration mechanism.

To learn more about migration mechanisms, see [VM Migration](#).

Note: In Veeam Backup Free Edition, you cannot select backup proxies to be used for VM quick migration. Veeam Backup Free Edition uses the default backup proxy: the Veeam backup server in the VMware environment and the source Hyper-V host in the Hyper-V environment.



The screenshot shows the 'Quick Migration Wizard' window, specifically the 'Transfer' step. The window has a blue title bar with the text 'Quick Migration Wizard' and a close button. On the left, there is a sidebar with four steps: 'Virtual Machines', 'Destination', 'Transfer' (which is highlighted with a grey background), and 'Ready'. Above the sidebar, there is a green icon of a computer with a right-pointing arrow and the title 'Transfer'. Below the icon, it says 'If desired, select specific source and target backup proxy to perform the operation with.' The main area of the wizard is divided into two sections. The top section is titled 'Data transfer' and contains the following text: 'When remote migrating between sites, for best migration performance you should deploy at least one backup proxy server in each site.' Below this text are two rows of input fields. The first row is labeled 'Source proxy:' and contains a text box with 'Automatic selection' and a 'Choose...' button. The second row is labeled 'Target proxy:' and also contains a text box with 'Automatic selection' and a 'Choose...' button. The bottom section of the main area contains a checked checkbox labeled 'Force Veeam quick migration' and a paragraph of text: 'Migration process will use VMware VMotion whenever migration scenario and VMware licensing allows to do so. Select this check box to force quick migration even if VMotion is available.' At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Quick Migration Wizard

Transfer
If desired, select specific source and target backup proxy to perform the operation with.

Virtual Machines
Destination
Transfer
Ready

Data transfer
When remote migrating between sites, for best migration performance you should deploy at least one backup proxy server in each site.

Source proxy:
Automatic selection Choose...

Target proxy:
Automatic selection Choose...

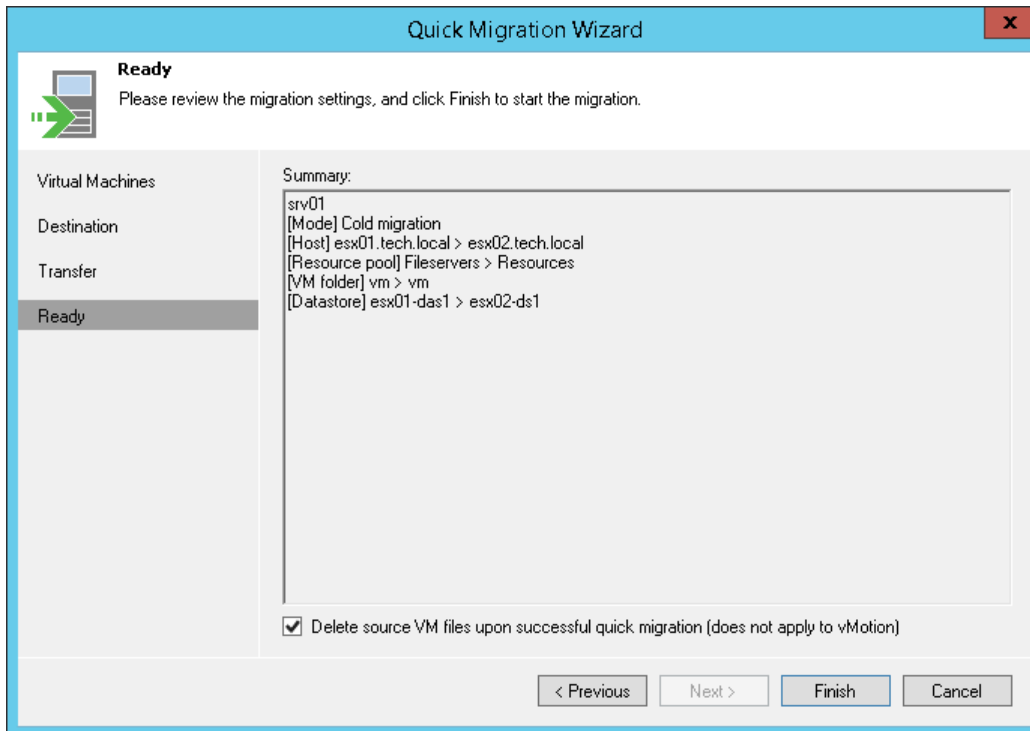
☒ Force Veeam quick migration
Migration process will use VMware VMotion whenever migration scenario and VMware licensing allows to do so. Select this check box to force quick migration even if VMotion is available.

< Previous Next > Finish Cancel

Step 5. Finish Working with Wizard

At the **Ready** step of the wizard, Veeam Backup Free Edition will check if the selected VM(s) can be relocated.

1. Review details of the quick migration task.
2. By default, when VM migration completes successfully, Veeam Backup Free Edition waits for a heartbeat signal from the VM on the target host. If the heartbeat is received, the original VM on the source host is deleted. If you do not want to delete the original VM on the source host, clear the **Delete source VM files upon successful migration** check box. Note that you cannot use this option if you have selected to relocate the VM(s) using VMware vMotion.
3. Click **Finish** to close the wizard and start the migration process.



Working with Storage Snapshots

With Veeam Explorer for Storage Snapshots, you can create restore VMware VM data directly from storage system snapshots. Veeam Backup Free Edition supports the following storage systems:

- EMC VNX and VNXe
- NetApp
- HP 3PAR StoreServ
- HP StoreVirtual P4000 series and HP StoreVirtual VSA

Setting Up Backup Infrastructure for Work with Storage System

Before you start working with storage snapshots in Veeam Backup Free Edition, make sure that you have properly configured your backup infrastructure:

1. You have added to the backup infrastructure VMware vCenter Server or ESX(i) hosts with VMs whose disks are located the storage system. For more information, see [Adding VMware vSphere Servers](#).
2. You have added to Veeam Backup Free Edition the storage system on which VM disks are located. For more information, see [Adding Storage Systems](#).
3. (For HP 3PAR StoreServ) You have enabled the HP StoreServ 3PAR Web Services API Server. For more information, see [Enabling HP 3PAR StoreServ Web Services API Server](#).

Note: Work with storage snapshots in Veeam Backup Free Edition is performed in the **Storage Infrastructure** view. When you install Veeam Backup Free Edition, the **Storage Infrastructure** view will not be displayed. To display it, add at least one VMware vCenter Server or ESX(i) host to the backup infrastructure.

Adding Storage Systems

To start using storage snapshots for backup and restore, you must add the storage system to the backup infrastructure.

After you add the storage system, the storage system topology appears in the **Storage Infrastructure** view.

When you add the storage system, Veeam Backup Free Edition automatically rescans it. As a part of rescan, Veeam Backup Free Edition performs the following operations:

1. Veeam Backup Free Edition retrieves the information about the storage system topology.
2. Veeam Backup Free Edition retrieves information about VMware datastores from VMware vCenter Server and matches storage volumes to these VMware datastores. Matching helps Veeam Backup Free Edition understand what VMs host their disks on storage volumes. Additionally, it helps Veeam Backup Free Edition get the information about VMs on storage snapshots: Veeam Backup Free Edition assumes that disks of VMs located on storage volumes are also located on storage snapshots.
3. Veeam Backup Free Edition rescans storage snapshots. As a result of snapshot rescan, Veeam Backup Free Edition determines exactly what VMs are located on storage snapshots. If for some reason Veeam Backup Free Edition fails to rescan all storage snapshots, it rescans the last storage snapshot in the hierarchy and propagates the retrieved information to all other storage snapshots.

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

- [EMC VNX/VNXe](#)
- [HP StoreVirtual](#)
- [HP 3PAR StoreServ](#)
- [NetApp](#)

Adding EMC VNX/VMXe

Before you add the EMC VNX(e) storage to the backup infrastructure, [check prerequisites](#). Then use the **New VNX(e) Storage** wizard to add the storage system.

Before You Begin

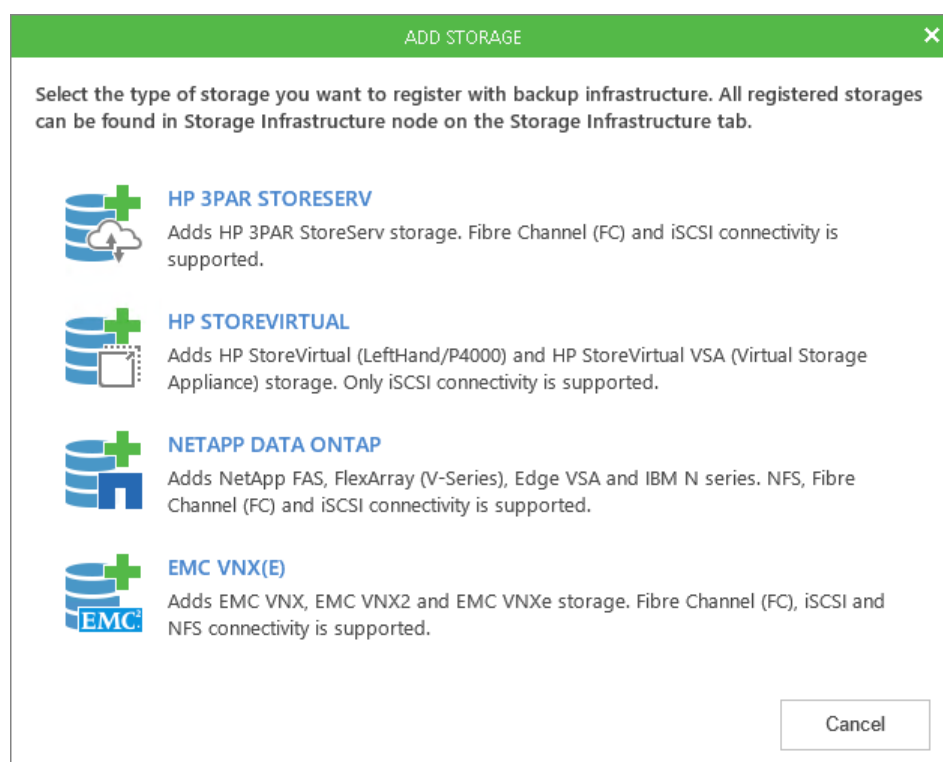
Before adding the EMC VNX(e) storage to the backup infrastructure, check the following prerequisites:

To work with EMC VNX(e) storages, Veeam Backup Free Edition uses the VNX snapshot technology. Make sure that you have a license that covers the VNX snapshot technology. The SnapView snapshot technology is not supported.

Step 1. Launch New VNXe Storage Wizard

To launch the **New EMC VNX(e) Host** wizard, do one of the following:

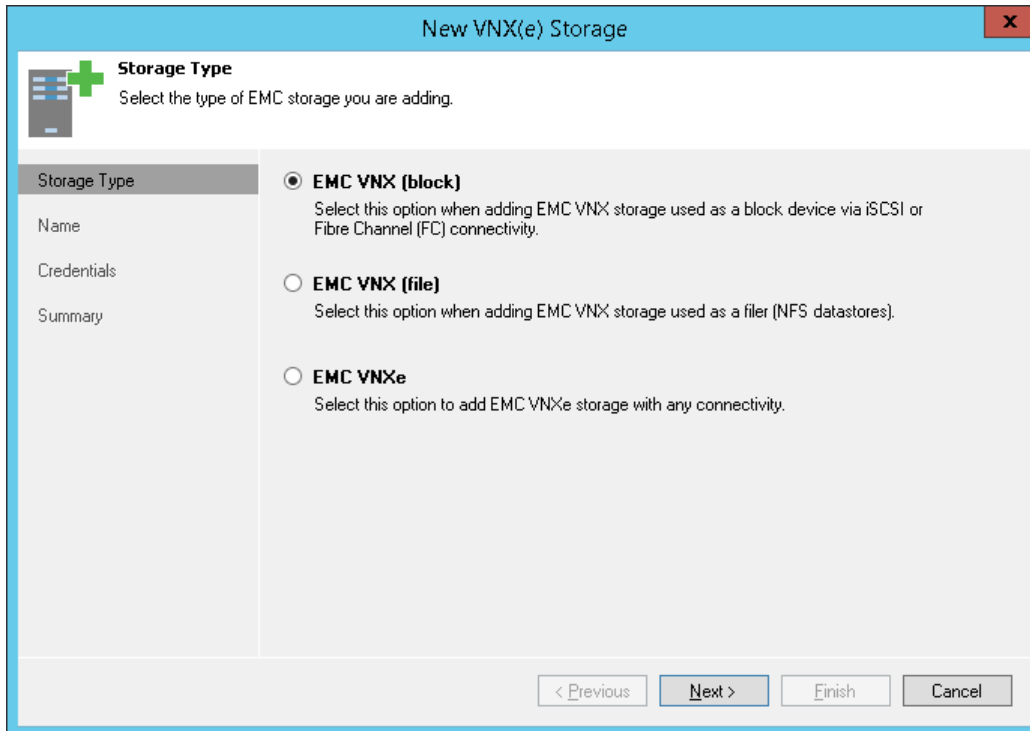
- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **EMC VNX(e)**.
- Open the **Storage Infrastructure** view, in the inventory pane right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **EMC VNX(e)**.
- Open the **Storage Infrastructure** view, in the inventory pane right-click the **VNX(e)** node and select **Add Storage**.



Step 2. Select Storage Type

At the **Storage Type** step of the wizard, select the type of the EMC VNX(e) storage.

- Select **EMC VNX (block)** to add an EMC VNX block storage working over Fibre Channel and iSCSI.
- Select **EMC VNX (file)** to add an EMC VNX file storage working over NFS.
- Select **EMC VNXe** to add an EMC VNXe storage working over Fibre Channel, iSCSI or NFS.



The screenshot shows a wizard window titled "New VNX(e) Storage". The "Storage Type" step is selected, indicated by a green plus icon and the text "Select the type of EMC storage you are adding." The left sidebar contains a list of steps: "Storage Type", "Name", "Credentials", and "Summary". The main area displays three radio button options:

- ☒ **EMC VNX (block)**
Select this option when adding EMC VNX storage used as a block device via iSCSI or Fibre Channel (FC) connectivity.
- ☐ **EMC VNX (file)**
Select this option when adding EMC VNX storage used as a filer (NFS datastores).
- ☐ **EMC VNXe**
Select this option to add EMC VNXe storage with any connectivity.

At the bottom right, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Storage Name or Address

At the **Name** step of the wizard, specify the name and description for the EMC VNX(e) storage system.

1. In the **DNS name or IP address** field, specify a DNS name or IP address of the EMC VNX(e) 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.

New VNX(e) Storage

Name
Register storage by providing IP address or DNS name of storage processor (SP) for VNX Block, or management interface for VNXe and VNX File.

Storage Type

Name

Credentials

Summary

DNS name or IP address:
172.16.21.105

Description:
EMC VNX Storage

< Previous Next > Finish Cancel

Step 4. Specify Credentials

At the **Credentials** step of the wizard, specify credentials for the user account with administrator privileges on the EMC VNX(e) storage system.

1. From the **Credentials** list, select credentials to connect to the EMC VNX(e) 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 [Managing Credentials](#).
2. [For EMC VNX block storage] Select the scope to which the user account whose credentials you provide belongs:
 - Select **Global** if the user account can administrate all VNX systems in the domain.
 - Select **Local** if the user account can administrate only a single VNX system in the domain.
 - Select **LDAP** if the user account can administrate all VNX systems that use the LDAP server for authentication.
3. [For EMC VNX file storage] When you add the storage system, Veeam Backup Free Edition saves a fingerprint of the SSH key of the management server to the configuration database. During every subsequent connection to the server, Veeam Backup Free Edition uses the saved fingerprint to verify the server identity and avoid the man-in-the-middle attack.

To let you identify the server, Veeam Backup Free Edition 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 Free Edition will display an error message, and you will not be able to connect to the server.

Note: If you update the SSH key on the server, you must acknowledge the new key in the server connection settings. To do this, in the **Storage Infrastructure** view open the server settings, pass through the **Edit Storage** wizard and click **Trust** to acknowledge the new key.

The screenshot shows the 'New VNX(e) Storage' wizard window. The title bar is blue with the text 'New VNX(e) Storage' and a close button. The main area has a light blue header with a green plus icon and the text 'Credentials' and 'Type in storage administrator credentials.' Below this is a sidebar with a tree view containing 'Storage Type', 'Name', 'Credentials' (selected), and 'Summary'. The main content area has a key icon and the text 'Select credentials with Local Administrator privileges on the server you are adding.' Below this is a 'Credentials' field with a key icon, a dropdown menu showing 'administrator (administrator, last edited: less th...', and an 'Add...' button. To the right of the dropdown is a blue link 'Manage accounts'. Below the 'Credentials' field is a 'Scope' dropdown menu showing 'Global'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, you can choose what EMC VNX(e) volumes you want to rescan.

When you add the EMC VNX(e) storage system, Veeam Backup Free Edition performs the storage system rescan. It scans storage volumes, locates VMs on these volumes, retrieves information about datastores from VMware vSphere servers and matches storage volumes to these datastores.

The EMC VNX(e) hierarchy can be very extensive, and the rescan process can take much time. To minimize the rescan time, you can instruct Veeam Backup Free Edition to rescan only specific volumes.

To rescan specific volumes:

1. At the **Summary** step of the wizard, click **Choose volumes to scan**.
2. In the **Choose Volumes** window, select which volumes you want to rescan:
 - To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list.
 - To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

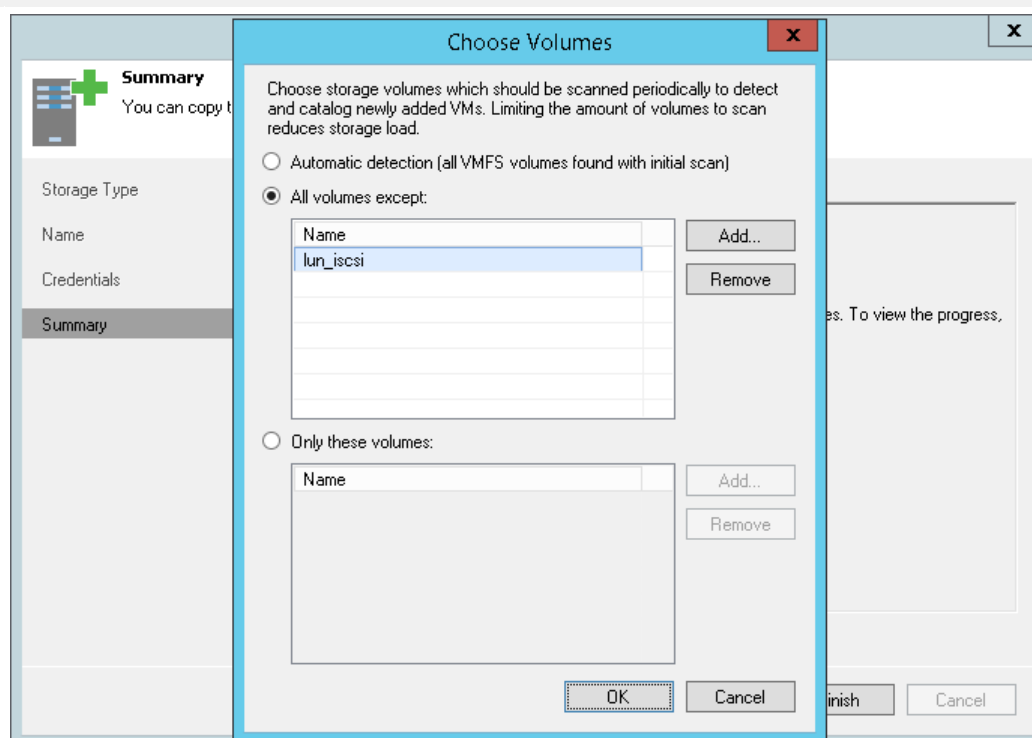
If you leave the **Automatic detection** option selected, Veeam Backup Free Edition will rescan all volumes in the EMC VNX(e) hierarchy.

3. Click **OK**.
4. Click **Finish**.

Veeam Backup Free Edition will add the EMC VNX(e) storage system and start the rescan process. The rescan details are displayed in the **System** window. You can close this window and review the rescan details later in the **History** view of Veeam Backup Free Edition.

Important!

If you plan to process VMs with Backup from Storage Snapshots, you must rescan volumes on which disks of these VMs are located.



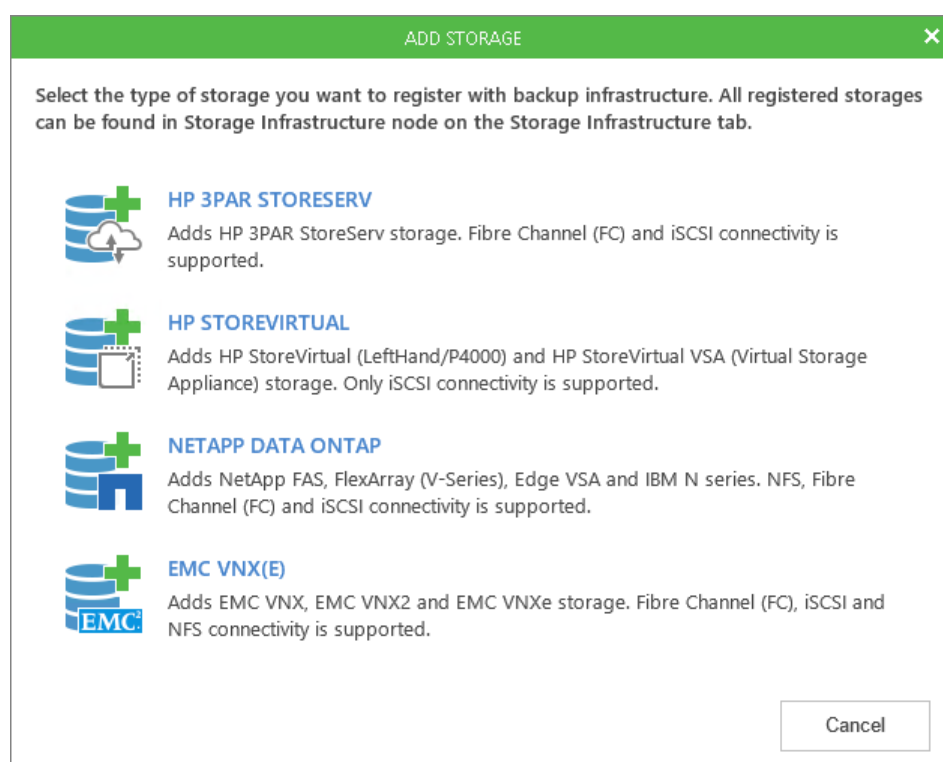
Adding HP StoreVirtual Storage System

To add the HP StoreVirtual storage to the backup infrastructure, use the **New HP StoreVirtual Storage** wizard.

Step 1. Launch New HP StoreVirtual Storage Wizard

To launch the **New HP StoreVirtual Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **HP StoreVirtual**.
- Open the **Storage Infrastructure** view, in the inventory pane right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **HP StoreVirtual**.
- Open the **Storage Infrastructure** view, in the inventory pane right-click the **HP StoreVirtual** node and select **Add Storage**. You can also right-click anywhere in the working area and select **Add Storage**.



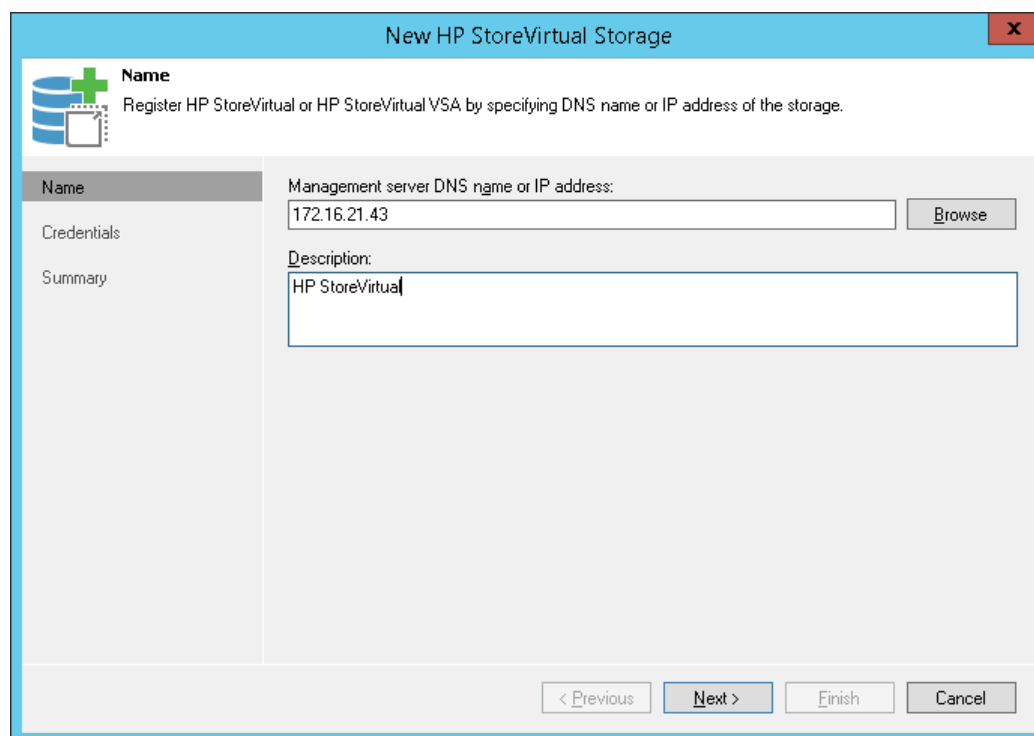
Step 2. Specify Storage Name or Address

At the **Name** step of the wizard, specify the storage address and description.

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

You can also type a DNS name or IP address of the HP 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 HP management group, date and time when the HP management group was added.



The screenshot shows a Windows-style dialog box titled "New HP StoreVirtual Storage". On the left is a sidebar with a tree view containing "Name" (selected), "Credentials", and "Summary". The main area has a header "Name" with a sub-instruction: "Register HP StoreVirtual or HP StoreVirtual VSA by specifying DNS name or IP address of the storage." Below this, there are two input fields. The first is labeled "Management server DNS name or IP address:" and contains the text "172.16.21.43"; a "Browse" button is to its right. The second is labeled "Description:" and contains the text "HP StoreVirtual". At the bottom of the dialog are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Credentials

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

1. From the **Credentials** list, select credentials to connect to the HP 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 [Managing Credentials](#).

The user name and password values are case-sensitive.

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

To let you identify the server, Veeam Backup Free Edition 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 Free Edition will display an error message, and you will not be able to connect to the server.

Note: If you update the SSH key on the server, you must acknowledge the new key in the server connection settings. To do this, in the **Storage Infrastructure** view open the server properties, pass through the **Edit Server** wizard and click **Trust** to acknowledge the new key.

The screenshot shows the 'New HP StoreVirtual Storage' wizard window, specifically the 'Credentials' step. The window has a blue title bar and a red close button. On the left, there is a sidebar with a 'Credentials' icon and a list containing 'Name', 'Credentials', and 'Summary'. The main area has a heading 'Credentials' with a subtext 'Type in storage administrator credentials.' Below this, there is a section titled 'Select credentials with Local Administrator privileges on the server you are adding.' which contains a 'Credentials:' label, a dropdown menu showing 'administrator (administrator, last edited: less th...', and an 'Add...' button. A blue link 'Manage accounts' is also present. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, you can choose what HP StoreVirtual volumes you want to rescan.

When you add the HP StoreVirtual storage system, Veeam Backup Free Edition performs the storage system rescan. It scans storage volumes, locates VMs on these volumes, retrieves information about datastores from VMware vSphere servers and matches storage volumes to these datastores.

The HP StoreVirtual hierarchy can be very extensive, and the rescan process can take much time. To minimize the rescan time, you can instruct Veeam Backup Free Edition to rescan only specific volumes.

To rescan specific volumes:

1. At the **Summary** step of the wizard, click **Choose volumes to scan**.
2. In the **Choose Volumes** window, select which volumes you want to rescan:
 - To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list.
 - To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

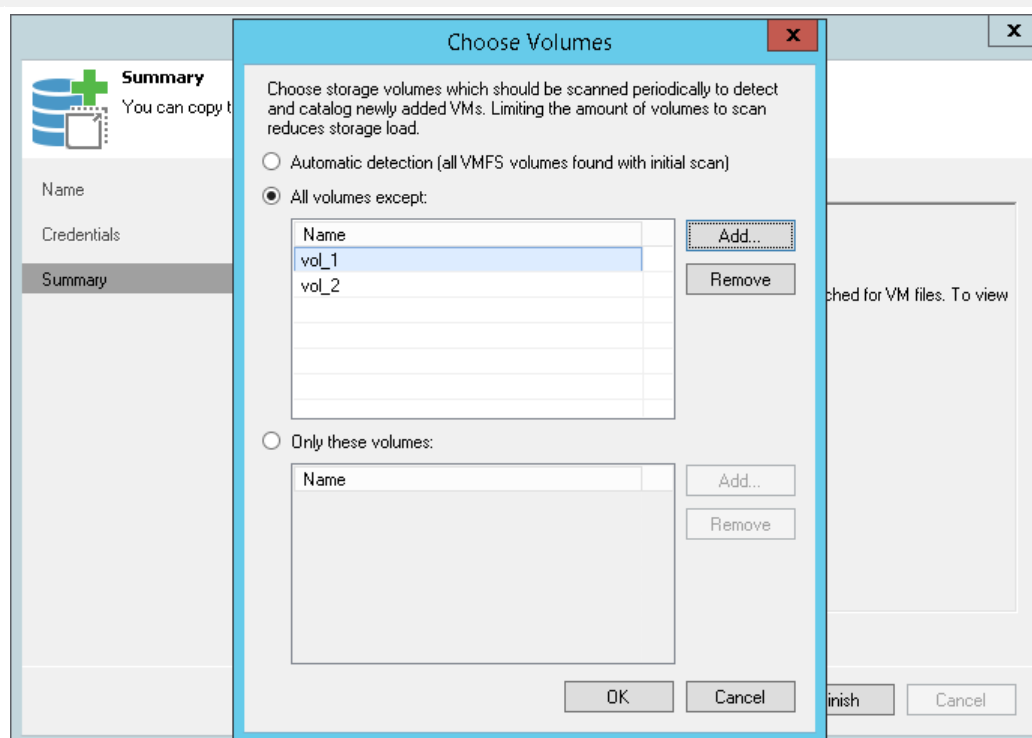
If you leave the **Automatic detection** option selected, Veeam Backup Free Edition will rescan all volumes in the HP StoreVirtual hierarchy.

3. Click **OK**.
4. Click **Finish**.

Veeam Backup Free Edition will add the HP StoreVirtual storage system and start the rescan process. The rescan details are displayed in the **System** window. You can close this window and review the rescan details later in the **History** view of Veeam Backup Free Edition.

Important!

If you plan to process VMs with Backup from Storage Snapshots, you must rescan volumes on which disks of these VMs are located.



Adding HP 3PAR StoreServ Storage System

Before you add the HP 3PAR StoreServ storage to the backup infrastructure, [check prerequisites](#). Then use the **New HP 3PAR StoreServ Storage** wizard to add the storage system.

Before You Begin

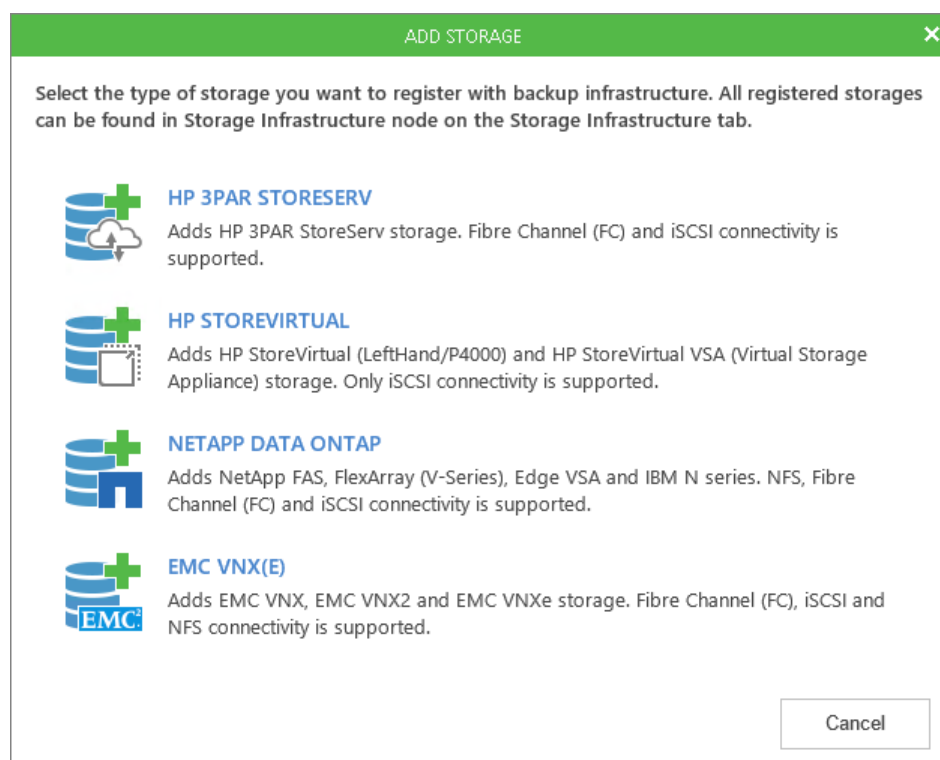
Before adding the HP 3PAR StoreServ storage to the backup infrastructure, check the following prerequisites:

1. A properly configured backup proxy must be added to the backup infrastructure. The backup proxy is required for storage system rescan.
2. The HP 3PAR Web Services API server must be enabled.
3. The license for the HP 3PAR StoreServ storage system must support HP 3PAR Virtual Copy.

Step 1. Launch New HP StoreServ Storage Wizard

To launch the **New HP 3PAR StoreServ Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **HP 3PAR StoreServ**.
- Open the **Storage Infrastructure** view, in the inventory pane right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **HP 3PAR StoreServ**.
- Open the **Storage Infrastructure** view, in the inventory pane right-click the **HP 3PAR StoreServ** node and select **Add Storage**. You can also right-click anywhere in the working area and select **Add Storage**.



Step 2. Specify HP 3PAR Web Services API Address

Veeam Backup Free Edition works with the HP 3PAR StoreServ storage system via the HP 3PAR Web Services API. The HP 3PAR Web Services API delivers a programming interface for performing storage management tasks with HP 3PAR StoreServ storage systems.

At the **Name** step of the wizard, provide information about the HP 3PAR Web Services API.

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the HP 3PAR Web Services API Server.
2. In the **URL** field, enter a URL of the HP 3PAR Web Services API. By default, Veeam Backup Free Edition uses the following URL: *https://<websapiserver>:8080*, where *<websapiserver>* is the name or IP address of the HP 3PAR Web Services API Server that you have specified in the field above.
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.

The screenshot shows a wizard window titled "New HP 3PAR StoreServ Storage". The window has a blue header bar with a close button (X) in the top right corner. Below the header, there is a sidebar on the left with a tree view containing "Name", "Credentials", and "Summary". The "Name" step is selected and highlighted. The main area of the wizard is titled "Name" and contains the instruction "Type in HP 3PAR StoreServ storage name and description." Below this instruction, there are three input fields: "DNS name or IP address:" with the value "172.18.44.8", "URL:" with the value "https://172.18.44.8:8080", and "Description:" with the value "HP 3PAR". At the bottom of the window, there are four buttons: "< Previous", "Next >" (which is highlighted with a blue border), "Finish", and "Cancel".

Step 3. Specify Credentials

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

1. From the **Credentials** list, select credentials to connect to the HP 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 [Managing Credentials](#).
2. When you add the storage system, Veeam Backup Free Edition saves a fingerprint of the SSH key of the HP 3PAR Web Services API Server to the Veeam Backup Free Edition database. During every subsequent connection to the server, Veeam Backup Free Edition uses the saved fingerprint to verify the server identity and avoid the man-in-the-middle attack.

To let you identify the server, Veeam Backup Free Edition 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 Free Edition will display an error message, and you will not be able to connect to the server.

Note: If you update the SSH key on the server, you must acknowledge the new key in the server connection settings. To do this, in the **Storage Infrastructure** view open the server properties, pass through the **Edit Server** wizard and click **Trust** to acknowledge the new key.

The screenshot shows the 'New HP 3PAR StoreServ Storage' wizard window. The title bar is blue with the text 'New HP 3PAR StoreServ Storage' and a close button. The main area has a light blue header with a green plus icon and the text 'Credentials' and 'Type in storage administrator credentials.' Below this is a sidebar with 'Name', 'Credentials', and 'Summary' sections. The 'Credentials' section is active, showing a list of credentials. A key icon is next to the text 'Select credentials with Local Administrator privileges on the server you are adding.' Below this, the 'Credentials' field shows 'administrator (administrator, last edited: less th...' with a dropdown arrow and an 'Add...' button. A blue link 'Manage accounts' is also visible. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, you can choose what HP 3PAR volumes you want to rescan.

When you add the HP 3PAR storage system, Veeam Backup Free Edition performs the storage system rescan. It scans storage volumes, locates VMs on these volumes, retrieves information about datastores from VMware vSphere servers and matches storage volumes to these datastores.

The HP 3PAR hierarchy can be very extensive, and the rescan process can take much time. To minimize the rescan time, you can instruct Veeam Backup Free Edition to rescan only specific volumes.

To rescan specific volumes:

1. At the **Summary** step of the wizard, click **Choose volumes to scan**.
2. In the **Choose Volumes** window, select which volumes you want to rescan:
 - To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list.
 - To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

If you leave the **Automatic detection** option selected, Veeam Backup Free Edition will rescan all volumes in the HP 3PAR hierarchy.

3. Click **OK**.
4. Click **Finish**.

Veeam Backup Free Edition will add the HP 3PAR storage system and start the rescan process. The rescan details are displayed in the **System** window. You can close this window and review the rescan details later in the **History** view of Veeam Backup Free Edition.

Important!

If you plan to process VMs with Backup from Storage Snapshots, you must select to rescan volumes on which disks of these VMs are located

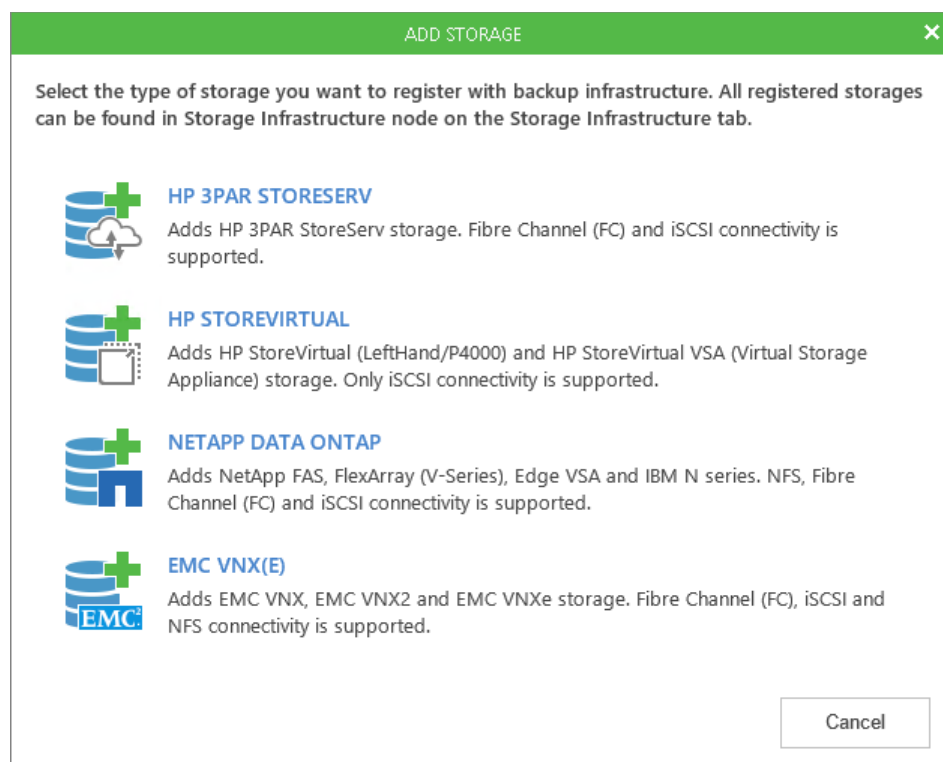
Adding NetApp Storage System

To add NetApp storage to the backup infrastructure, use the **New NetApp Storage** wizard.

Step 1. Launch New NetApp Storage Wizard

To launch the **New NetApp Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **NetApp**.
- Open the **Storage Infrastructure** view, in the inventory pane select the **NetApp** node and click **Add Storage** on the ribbon.
- Open the **Storage Infrastructure** view, in the inventory pane right-click the **NetApp** node and select **Add Storage**. You can also right-click anywhere in the working area and select **Add Storage**.



Step 2. Specify Server Name or Address

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

1. In the **Management server DNS name or IP address** field, specify a DNS name or IP address of the NetApp storage system.

You can also browse for NetApp storage systems that exist in your environment:

- a. On the right of the **Management server DNS name or IP address** field, click **Browse**.
 - b. In the **NetApp Storage System Discovery** window, enter an IP address of the NetApp storage system or IP address of the subnet where the storage is located and click **Discover**. Veeam Backup Free Edition will search the whole subnet for storage systems. For example, if you enter 172.16.1.12 as an IP address, Veeam Backup Free Edition will search storage systems in subnet 172.16.1.* and display the list of storage systems found in this subnet.
 - c. In the list below, select the NetApp storage system you want to add.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the NetApp storage system, date and time when the storage system was added.

New NetApp Storage

Name
Register NetApp storage by specifying DNS name or IP address.

Name
Management server DNS name or IP address:
172.16.21.90 **Browse**

Description:
NetApp 7-model

< Previous **Next >** Finish Cancel

Step 3. Specify Credentials and Protocol Type

At the **Credentials** step of the wizard, specify credentials for the user account to connect to the NetApp storage system, and select the transport protocol.

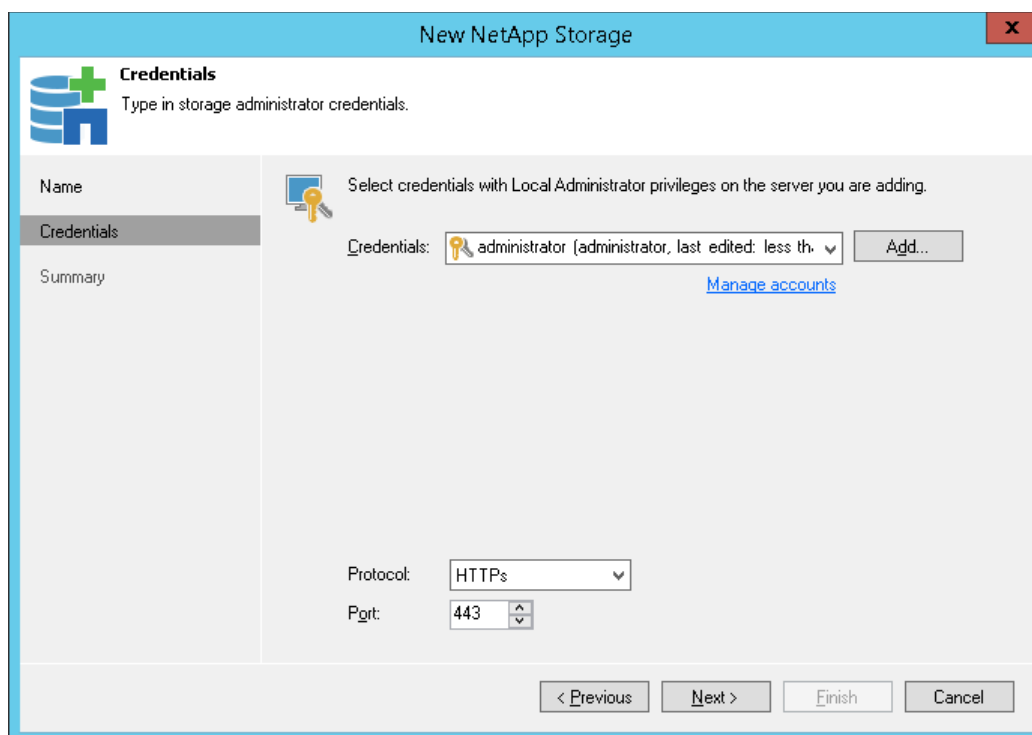
1. From the **Credentials** list, select credentials to connect to the NetApp storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** filed to add the credentials. For more information, see [Managing Credentials](#).

The account you select must have administrative privileges on the NetApp storage system.

2. From the **Protocol** list, select the type of protocol over which you want to communicate with the NetApp storage system: *HTTP* or *HTTPS*.

The default transport protocol is HTTPS. However, you can configure the NetApp storage system to communicate with Veeam Backup Free Edition over the HTTP protocol if needed.

3. The default port for communication with the NetApp storage system is 443. If necessary, you can customize the port number in the NetApp storage system settings and specify the new port number in the **Port** field.



The screenshot shows the 'New NetApp Storage' wizard window. The title bar is blue with the text 'New NetApp Storage' and a close button. The main window has a light blue header with a NetApp logo and the title 'Credentials'. Below the header, it says 'Type in storage administrator credentials.' On the left, there is a sidebar with 'Name' and 'Credentials' (selected) and 'Summary'. The main area has a key icon and the text 'Select credentials with Local Administrator privileges on the server you are adding.' Below this, there is a 'Credentials' field with a dropdown menu showing 'administrator (administrator, last edited: less th...' and an 'Add...' button. A link 'Manage accounts' is also present. At the bottom, there are 'Protocol' and 'Port' fields. The 'Protocol' dropdown is set to 'HTTPS' and the 'Port' spinner is set to '443'. At the very bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 4. Rescan Storage System

At the **Summary** step of the wizard, you can choose what NetApp volumes you want to rescan.

When you add the NetApp storage system, Veeam Backup Free Edition performs the storage system rescan. It scans storage volumes and LUNs, locates VMs on these volumes and shares, retrieves information about datastores from VMware vSphere servers and matches volumes and LUNs to these datastores.

The NetApp hierarchy can be very extensive, and the rescan process can take much time. To minimize the rescan time, you can instruct Veeam Backup Free Edition to rescan only specific volumes.

To rescan specific volumes:

1. At the **Summary** step of the wizard, click **Choose volumes to scan**.
2. In the **Choose Volumes** window, select which volumes you want to rescan:
 - To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list.
 - To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

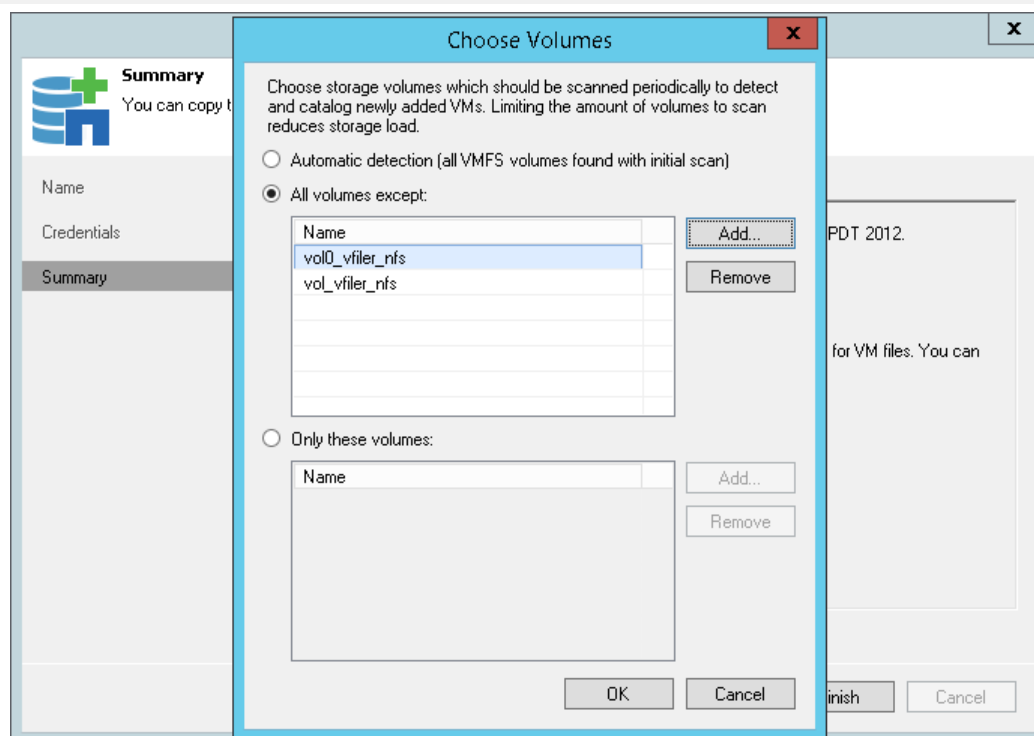
If you leave the **Automatic detection** option selected, Veeam Backup Free Edition will rescan all volumes in the NetApp hierarchy.

3. Click **OK**.
4. Click **Finish**.

Veeam Backup Free Edition will add the NetApp storage system and start the rescan process. The rescan details are displayed in the **System** window. You can close this window and review the rescan details later in the **History** view of Veeam Backup Free Edition.

Important!

- If you plan to process VMs with Backup from Storage Snapshots, you must select to rescan volumes on which disks of these VMs are located.
- If you plan to create backup jobs that will trigger NetApp snapshots on NetApp SnapMirror or SnapVault, you must select to rescan target volumes on SnapMirror or SnapVault.



Enabling HP 3PAR StoreServ Web Services API Server

This step must be performed if you plan to work with the HP 3PAR StoreServ storage system.

Veeam Backup Free Edition uses the HP 3PAR Web Services API server to communicate with the HP 3PAR StoreServ storage system. When you add the HP 3PAR StoreServ storage to the backup infrastructure, Veeam Backup Free Edition attempts to enable the server automatically. If Veeam Backup Free Edition fails to enable the server automatically (for example, if it does not have enough privileges to do this), you need to enable the server manually.

Important! The HP 3PAR Web Services API is a part of the HP 3PAR OS starting from version 3.1.2. Veeam Backup Free Edition does not support earlier versions of HP 3PAR OS.

To check if the HP 3PAR Web Services API server is enabled and enable it if needed:

1. Log on to the Processor with administrator privileges:

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

2. View the current state of the Web Services API Server:

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

3. If the Web Services API Server is disabled, start it:

```
#startwsapi
```

4. If the HTTP or HTTPS state is disabled, enable one of them:

```
#setwsapi -http enable
```

or

```
#setwsapi -https enable
```

Working with Veeam Explorer for Storage Snapshots

After you have added the storage system to the backup infrastructure, you can perform the following operations:

- [Re-Scanning Storage Systems](#)
- [Creating and Deleting Snapshots](#)
- [Restoring VM Data from Storage Snapshots](#)

Re-Scanning Storage Systems

You can rescan the storage system added to the backup infrastructure. Storage rescan may be required, for example, if you create or delete volume snapshots on the storage system. Storage rescan will help you discover these changes and update the storage system hierarchy in the Veeam Backup Free Edition console.

Storage system rescan can be performed automatically or manually.

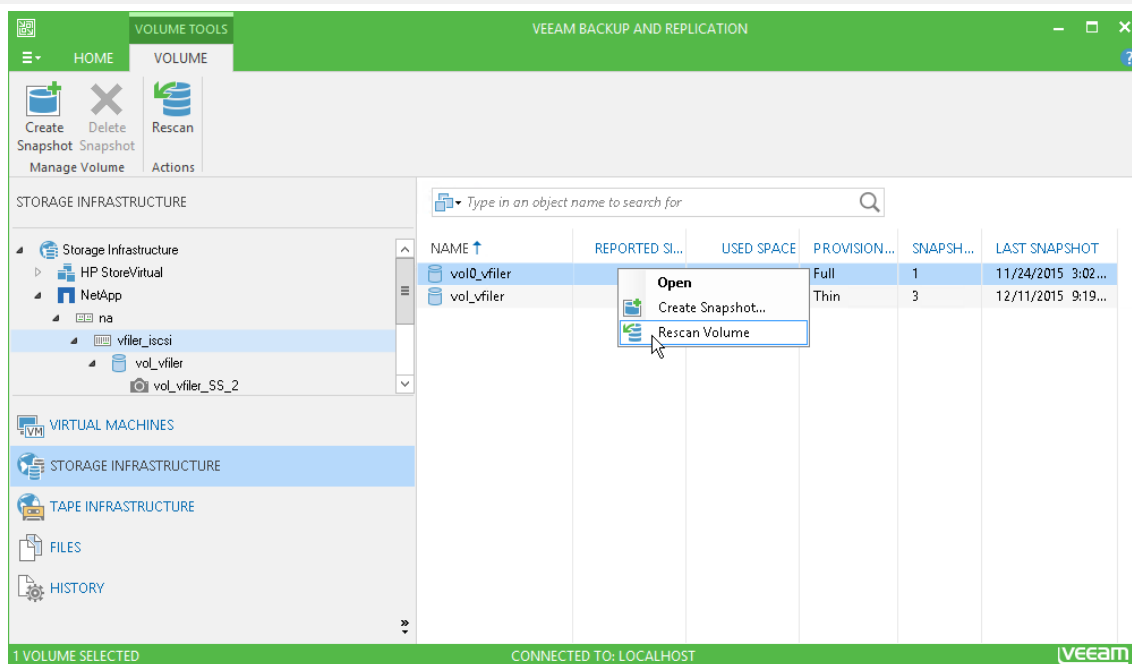
- **Automatic storage rescan:** Veeam Backup Free Edition uses the following processes to rescan the storage system:
 - *Storage Monitor* runs in the background. This process detects new snapshots and volumes and performs their rescan with a time interval of 10 minutes.
 - *Storage Discovery* is started every 7 days. This process performs rescan of the whole storage system or selected volumes (if you limited the rescan scope when you added the storage system to Veeam Backup Free Edition).
- **Manual storage rescan:** if necessary, you can start *Storage Discovery* process manually. Storage discovery can be performed against any node in the storage system hierarchy: storage system itself, specific volume and so on.

Before you begin storage discovery, make sure that you have a properly configured backup proxy in your backup infrastructure. Otherwise, Veeam Backup Free Edition will not be able to match storage volumes to VMware datastores and locate VMs on these storage volumes.

To perform storage discovery:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the tree of the storage system.
3. Select a node in the storage system hierarchy: storage system, volume and so on.
4. Click **Rescan** on the ribbon or right-click the node in the hierarchy and select **Rescan Storage**.

Important! If you chose to rescan only specific volumes when you added the storage system, the rescan operation for the storage system will discover only these selected volumes. To change the storage discovery scope, open the storage settings and select the necessary volumes at the **Summary** step of the wizard. For details, see [Adding Storage System](#).



Choosing Volumes to Rescan

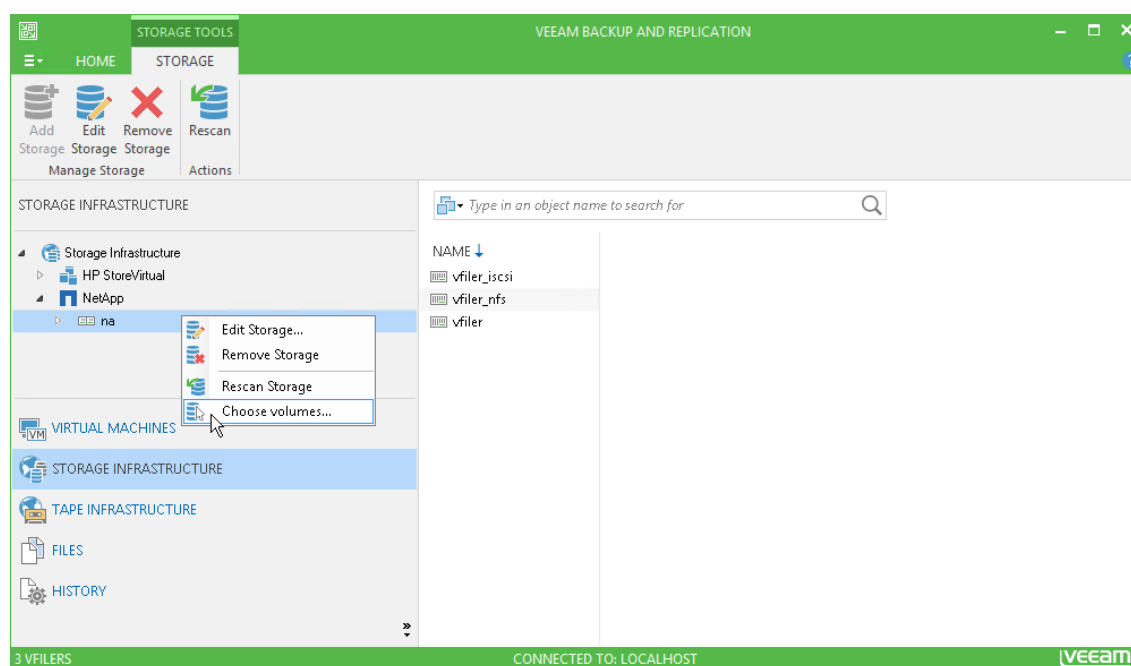
The storage system hierarchy can be very extensive, and the rescan process can take much time. To minimize the rescan time, you can instruct Veeam Backup Free Edition to rescan only specific volumes.

To rescan specific volumes:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, select the storage system type.
3. In the working area, right-click the root node of the storage system and click **Choose volumes**.
4. In the **Choose Volumes** window, select which volumes you want to rescan:
 - To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list.
 - To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

If you leave the **Automatic detection** option selected, Veeam Backup Free Edition will rescan all volumes in the storage system hierarchy.

5. Click **OK**.
6. Click **Finish**.



Creating and Deleting Snapshots

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

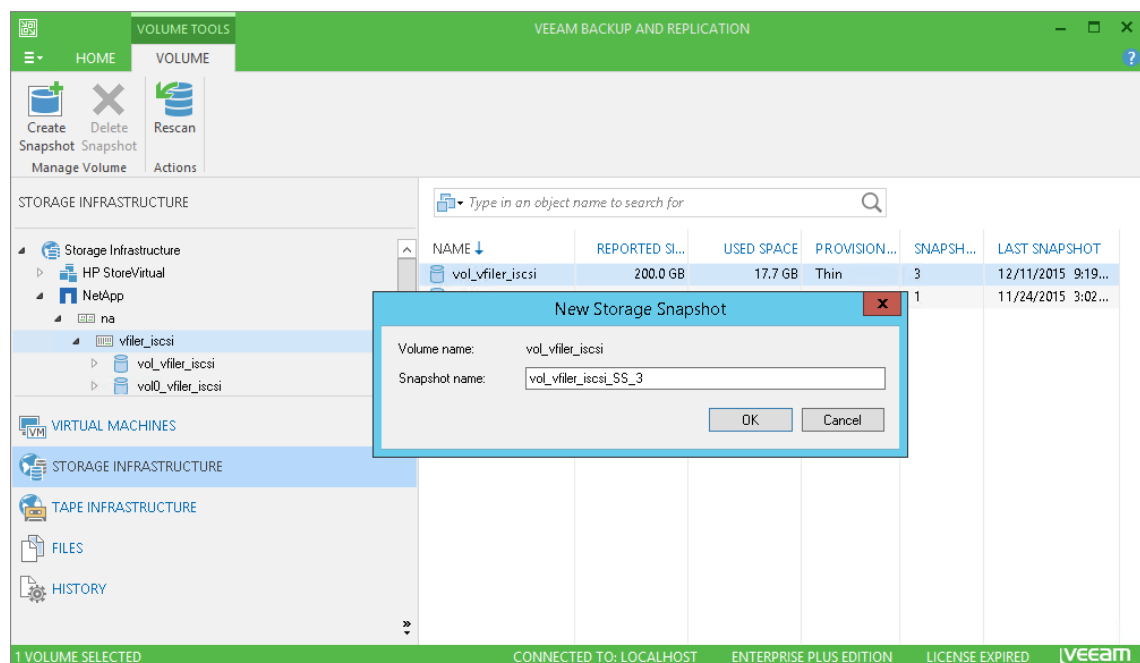
To create a volume snapshot:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the tree of the storage system.
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 this option is available).
5. [For HP StoreVirtual] 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 on the volume with VMware Tools. This will bring VM data to a consistent state before the snapshot is taken. If this option is not selected, Veeam Backup Free Edition will create a point-in-time snapshot.

Note: To create application-managed snapshots for the HP StoreVirtual storage system, make sure that Application Aware Snapshot Manager is properly installed and configured. If the Application Aware Snapshot Manager is not installed, Veeam Backup Free Edition will report an error, and the snapshot will not be created. For more information, see the HP P4000 Application-Aware Snapshot Manager Deployment Guide at <http://h10032.www1.hp.com/ctg/Manual/c03037557.pdf>.

To delete a volume snapshot:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand a tree of the storage system.
3. Right-click the necessary snapshot and select **Delete Snapshot**.



Restoring VM Data from Storage Snapshots

If VM data gets lost or corrupted, you can restore it from storage snapshots.

The restore process is similar to restore from image-level backups of VMs. Veeam Backup Free Edition offers the following restore options for storage snapshots:

- [Performing Instant VM Recovery](#)
- [Restoring VM guest OS files \(Microsoft Windows\)](#)
- [Restoring VM guest OS files \(Linux, Unix and other\)](#)
- [Restoring application items](#)

Performing Instant VM Recovery

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

Before performing Instant VM Recovery, [check prerequisites](#). Then use the **Instant Recovery** wizard to restore a VM from the storage snapshot.

Before You Begin

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

- If you are recovering a VM to the production network, make sure that the initial VM is powered off to avoid conflicts.
- The storage system must be added to the backup infrastructure.
- [For HP 3PAR StoreServ storage systems and NetApp storage systems working over Fibre Channel] The ESX(i) host that you select for storage snapshots mounting must meet the following requirements:
 - a. The ESX(i) host must have access to the storage system over a Fibre Channel connection.
 - b. The ESX(i) host must be added to the list of servers that have access to storage snapshots from which you plan to restore VM data.
 - c. [For NetApp storage systems] You must create an initiator group on the NetApp storage system. The initiator group must contain a WWN of the ESX(i) host to which you plan to mount the storage snapshot.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see Veeam Backup & Replication User Guide for VMware vSphere.

Mind the following limitations:

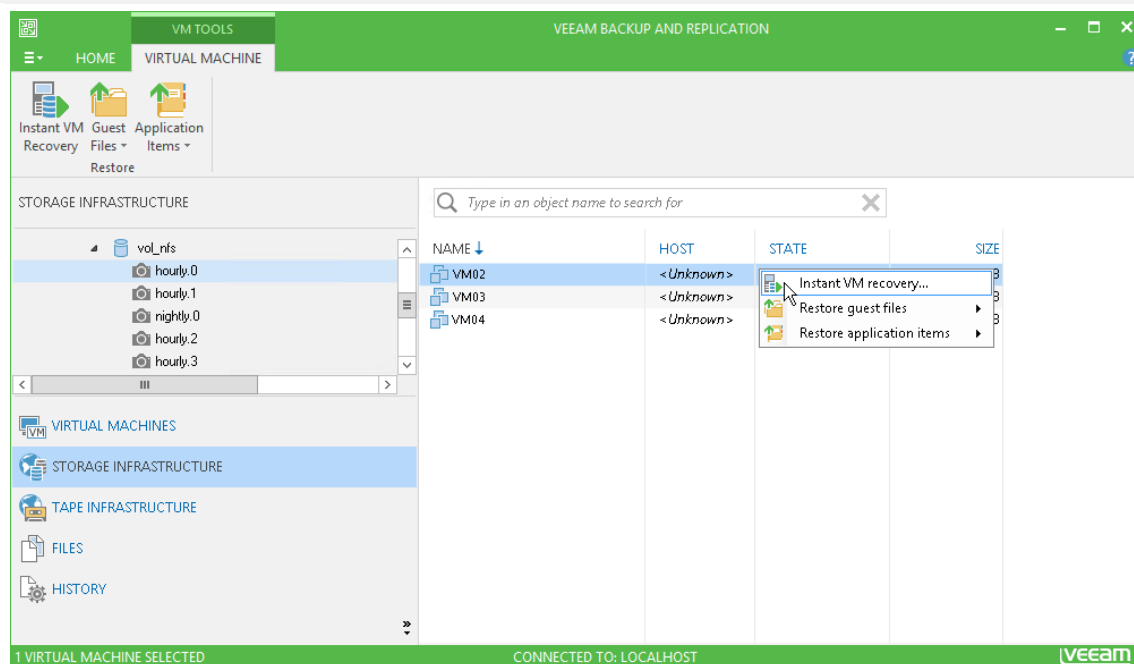
VMs with virtual disk files located on different storage volumes are not supported. You will be able to restore VM data only from VM disks residing on the same datastore as the VMX file.

Step 1. Launch Instant Recovery Wizard

To launch the **Instant Recovery** wizard:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the storage system tree and select the necessary volume snapshot.
3. In the working area, select the VM and click **Instant VM Recovery** on the toolbar. You can also right-click the VM you want to restore and select **Instant VM Recovery**.

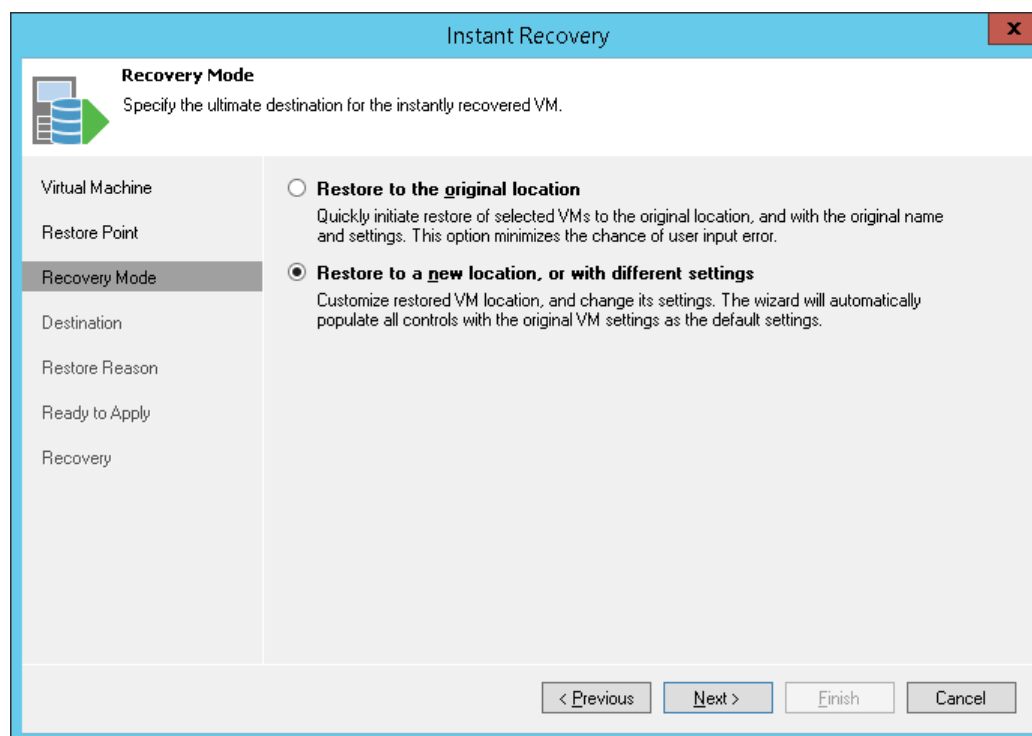
Tip: To quickly find the necessary VM, use the search field at the top of the window: enter a VM name or a part of it and press **[ENTER]**.



Step 2. Select Restore Mode

At the **Recovery Mode** step of the wizard, choose the necessary restore mode:

- Select **Restore to the original location** if you want to restore the VM with its initial settings and to its original location. If this option is selected, you will pass directly to the **Restore Reason** step of the wizard.
- Select **Restore to a new location, or with different settings** if you want to restore the VM to a different location and/or with different settings. If this option is selected, the **Instant Recovery** wizard will include additional steps for customizing VM settings.



Step 3. Select Destination for Recovered VM

The **Destination** step of the wizard is available if you have chosen to change the location and settings of the restored VM.

Select a destination for the recovered VM:

1. In the **Host** field, specify a host on which the VM must run. Veeam Backup Free Edition will create a clone/virtual copy of the storage snapshot, mount it to the selected ESX(i) host and start the VM on this ESX(i) host.
2. In the **VM folder** field, select a folder to which the restored VM must be placed.
3. In the **Restored VM name** field, enter a name under which the restored VM must be registered. By default, Veeam Backup Free Edition uses the original name of the VM. If you are restoring the VM to the same ESX(i) host or the same datacenter where the original VM is registered and the original VM still resides there, it is recommended that you change the VM name to avoid conflicts.
4. In the **Resource pool** list, select a resource pool to which the restored VM must be placed.

Instant Recovery

Destination
Choose ESX server to run the recovered virtual machine on. You can choose to power on VM automatically, unless you need to adjust VM settings first (such as change VM network).

Virtual Machine
Restore Point
Recovery Mode
Destination
Restore Reason
Ready to Apply
Recovery

Host: esx01.tech.local Choose...

VM folder: vm Choose...

Restored VM name: VM02_restored

Resource pool:

- Resources
 - Alpha
 - CRM
 - Data
 - Fileservers
 - Replicas
 - Shell
 - webserver

< Previous Next > Finish Cancel

Step 4. Specify Restore Reason

At the **Restore Reason** step of the wizard, enter the reason for performing Instant VM Recovery. The information you provide will be saved in the session history and you can view it later.

Instant Recovery

Restore Reason
Provide the reason for performing this restore. This information will be saved in the restore sessions history for later reference.

Virtual Machine
Restore Point
Recovery Mode
Destination
Restore Reason
Ready to Apply
Recovery

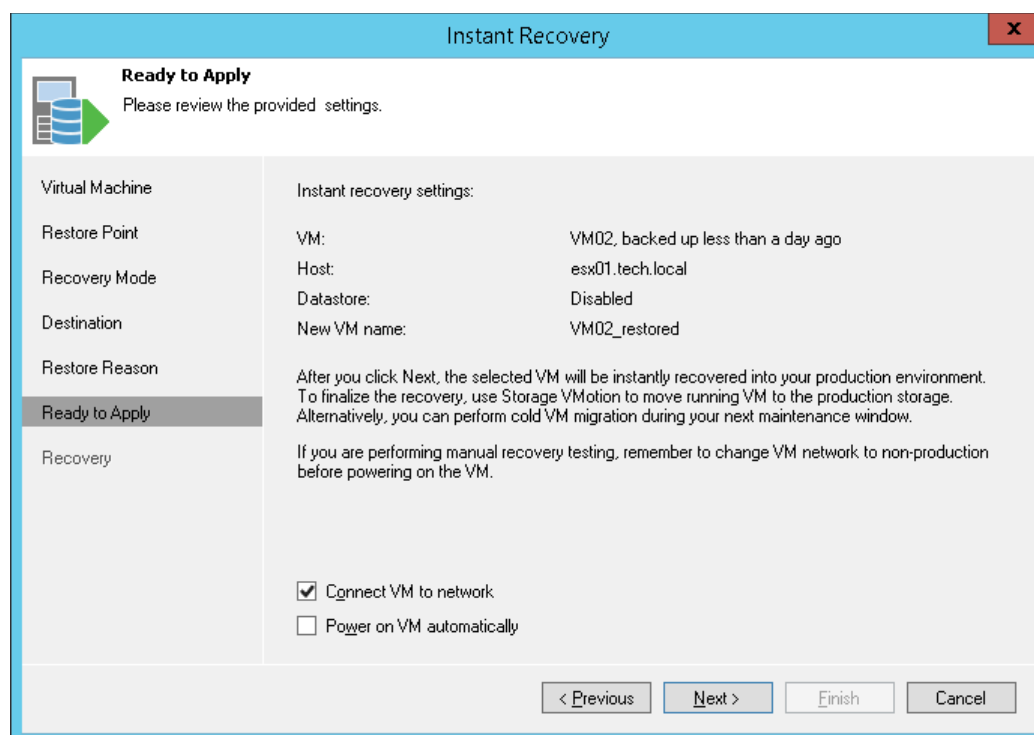
Restore reason:
Restoring a corrupted VM

< Previous Next > Finish Cancel

Step 5. Verify Instant VM Recovery Settings

At the **Ready to Apply** step of the wizard, specify additional settings for Instant VM Recovery:

1. If you are recovering a production VM that has failed and want to restore it with initial network settings, select the **Connect VM to network** check box. If you are recovering a VM for testing disaster recovery and the original VM is still running, leave this check box not selected. Before you power on a VM, you will have to manually change VM network configuration: disconnect it from the production network and connect it to an isolated non-production network to avoid conflicts.
2. To start the VM immediately after recovery, select the **Power on VM automatically** check box. If you are recovering the VM to the production network, make sure that the initial VM is powered off to avoid conflicts.
3. Check the settings for Instant VM Recovery and click **Next**. Veeam Backup Free Edition will restore the VM on the selected ESX(i) host.



Step 6. Finalize Instant VM Recovery

All currently running Instant VM Recovery sessions are displayed in the **Storage Infrastructure** view, under the **Instant Recovery** node.

To check the progress of the Instant VM Recovery session and view session details:

1. Open the **Storage Infrastructure** view.
2. Select the **Instant Recovery** node.
3. Right-click the necessary session in the working area and select **Properties**. You can also double-click the necessary session in the list.

After the VM has been successfully restored, you can finalize Instant VM Recovery in two ways:

- Migrate the recovered VM to production
- Unpublish the recovered VM

To migrate the recovered VM to production:

1. Open the **Storage Infrastructure** view.
2. Select the **Instant Recovery** node.
3. Right-click the necessary Instant VM Recovery session in the working area and select **Migrate to production**. Veeam Backup Free Edition will launch the **Quick Migration** wizard. During migration, Veeam Backup Free Edition will restore the VM from the storage snapshot and then additionally move changes that were made while the VM was running in the Instant Recovery mode.

To unpublish the restored VM:

1. Open the **Storage Infrastructure** view.
2. Select the **Instant Recovery** node.
3. Right-click the necessary session in the working area and select **Stop publishing**.

You can also unpublish the VM using the **History** view:

1. Open the **History** view.
2. Select the **Restore > Instant VM recovery** node.
3. In the working area, right-click the necessary session and select **Stop session**.

Restoring VM Guest OS Files (Microsoft Windows)

You can restore individual Microsoft Windows guest OS files from the storage snapshot. Veeam Backup Free Edition supports file-level restore for the following Microsoft Windows file systems:

- FAT
- NTFS
- ReFS

When you perform guest OS file restore, you must select an ESX(i) host in your virtual environment. Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot on which the VM disks reside and mounts the clone/virtual copy to the selected ESX(i) host as a new LUN/volume.

After that, Veeam Backup Free Edition accesses the configuration file of the VM (VMX) on the mounted clone/virtual copy and uses this configuration file to register a temporary VM on the selected ESX(i) host. Disks of the restored VM are mounted to this temporary VM. After disks are mounted, you can copy necessary VM guest OS files and folders to their initial location, local machine drive or save them in a network shared folder.

Before you start file-level restore, [check prerequisites](#). Then use the **File Level Restore** wizard to restore necessary files and folders.

Before You Begin

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

- If you plan to restore VM guest OS files for ReFS, make sure that Veeam Backup Free Edition is installed on a machine running Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2.
- If you plan to restore VM guest OS files to their initial location, VMware Tools must be installed on the target VM.
- The storage system must be added to the backup infrastructure.
- [For HP 3PAR StoreServ storage systems and NetApp storage systems working over Fibre Channel] The ESX(i) host that you select for storage snapshots mounting must meet the following requirements:
 - a. The ESX(i) host must have access to the storage over a Fibre Channel connection.
 - b. The ESX(i) host must be added to the list of servers having access to storage snapshots from which you plan to restore VM guest OS files.
 - c. [For NetApp storage system] You must create an initiator group on the NetApp storage system. The initiator group must contain a WWN of the ESX(i) host to which you plan to mount the storage snapshot.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see *Veeam Backup & Replication User Guide for VMware vSphere*.

Mind the following limitations:

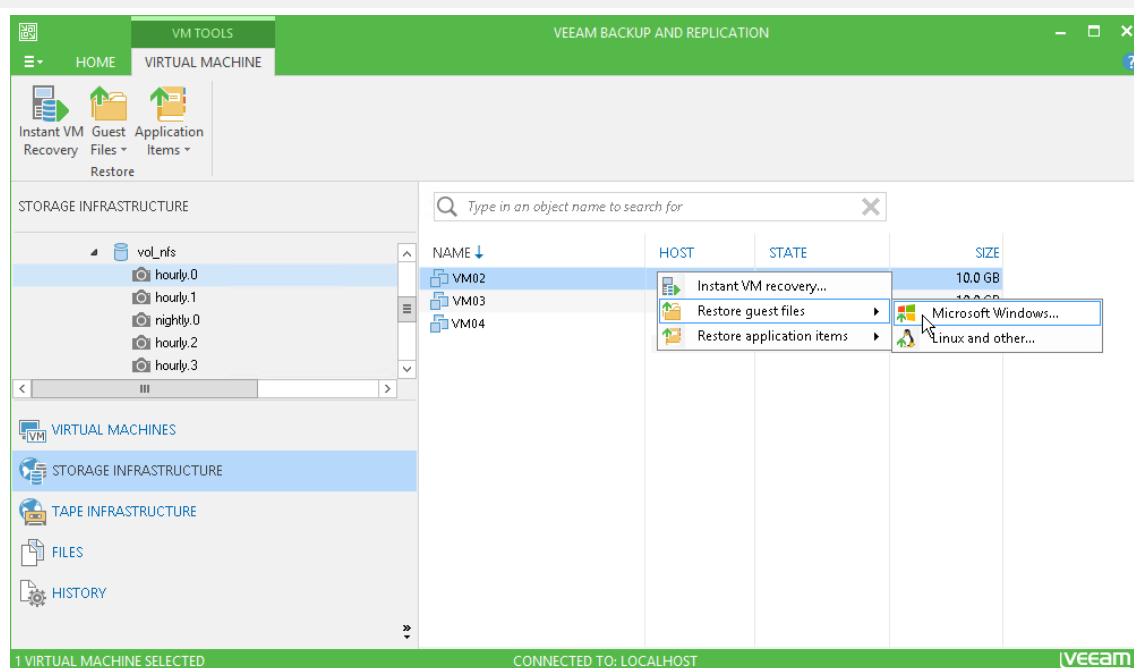
- You cannot restore files directly to the original location if disks of the VM are located on NetApp SnapVault or SnapMirror. Use the **Copy to** option instead.
- VMs with virtual disk files located on different storage volumes are not supported. You will be able to restore VM data only from VM disks residing on the same datastore as the VMX file.

Step 1. Launch Restore Wizard

To launch the **File-Level Recovery** wizard:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the storage system tree and select the necessary volume snapshot.
3. In the working area, select the VM and click **Guest Files > Windows Guest Files** on the toolbar. You can also right-click the VM you want to restore and select **Restore Windows guest files**.

Tip: To quickly find the necessary VM, use the search field at the top of the window: enter a VM name or a part of it and press **[ENTER]**.

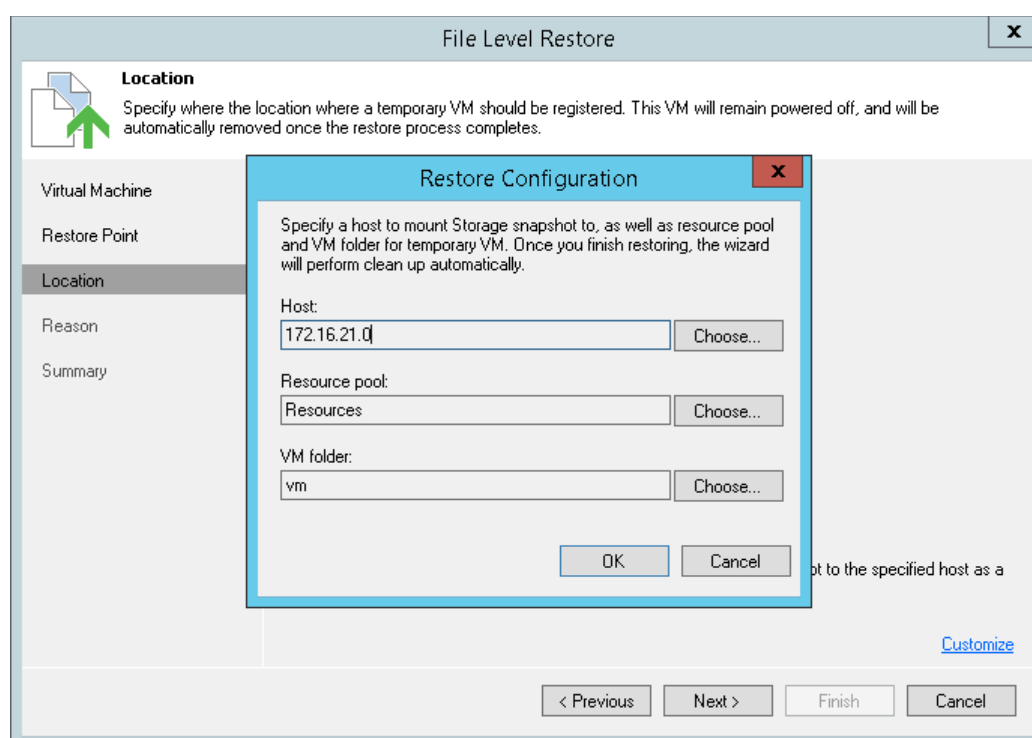


Step 2. Select ESX(i) Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot will be mounted. On the selected ESX(i) host, Veeam Backup Free Edition will create a temporary VM and mount disks of the restored VM to this temporary VM.

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

1. At the **Location** step of the wizard, click **Customize**.
2. Click **Choose** next to the **Host** field and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Click **Choose** next to the **Resource pool** field and select a resource pool to which the temporary VM must be placed.
4. Click **Choose** next to the **VM folder** field and select a folder to which the temporary VM must be placed.
5. Click **OK**.



Step 3. Save Restored Files

At the **Summary** step of the wizard, click **Finish** to start the VM guest OS files restore process.

Once the restore process is complete, Veeam Backup Free Edition will open the Veeam Backup browser displaying the file system tree of the restored VM. Note that names of the restored VM hard disks may differ from the original ones.

You can perform the following operations with VM guest OS files in the Veeam Backup browser:

- Save files and folders to the original location
- Save files and folders to a folder on the backup server or in network shared folder
- Launch Veeam Explorers for application item restore
- Open files in Microsoft Windows Explorer

After the restore process is complete, close the Veeam Backup browser.

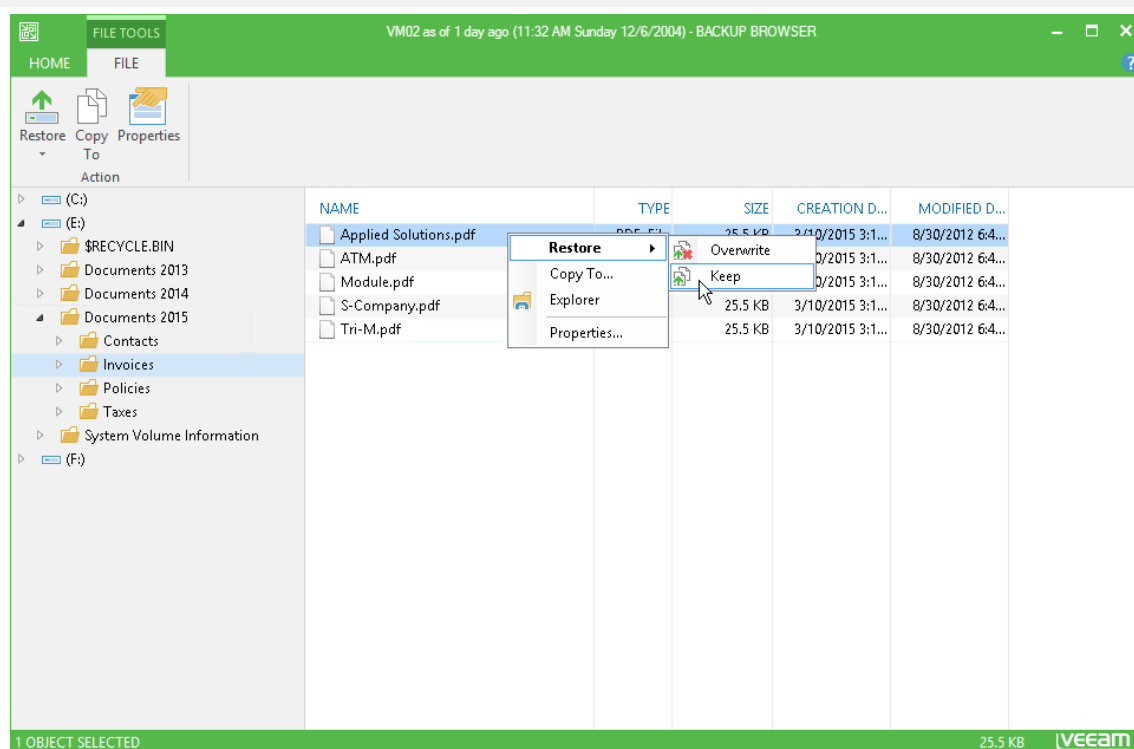
Saving Files to Original Location

To save files or folders to their initial location, right-click a file or folder in the Veeam Backup browser and select one of the following commands:

- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**. Veeam Backup Free Edition will add the *RESTORED-* prefix to the original file name and save the restored file in the same location where the original file resides.

Important!

Restore to the initial location may fail if VMware Tools are not installed on the target VM. To restore guest OS files in such situation, you can use 1-click file-level restore or save files to any other location and then move them to their initial location.

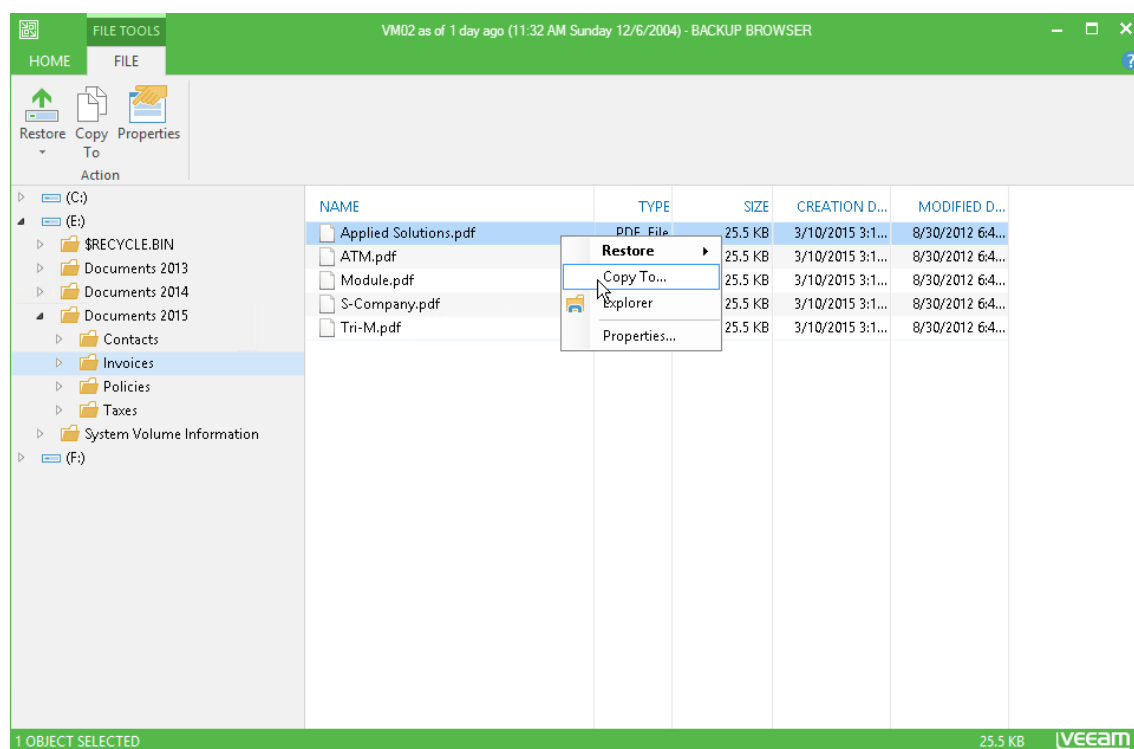


Saving Files to New Location

To save restored files or folders to a folder on the backup server or in a network shared folder, right-click a file or folder in the Veeam Backup browser and select **Copy To** and select a location to which the file or folder must be copied.

When restoring file objects, you can choose to preserve their original NTFS permissions:

- Select the **Preserve permissions and ownership** check box to keep the original ownership and security permissions for restored objects. Veeam Backup Free Edition will copy files and folders with associated Access Control Lists and preserve granular access settings.
- Leave the **Preserve permissions and ownership** check box not selected if you do not want to preserve the original ownership and access settings for restored objects. Veeam Backup Free Edition will change security settings: the user who launched the Veeam Backup Free Edition console will be set as the owner of restored objects. Access permissions will be inherited from the folder to which restored objects are copied.



Launching Veeam Explorers

If you are restoring VM guest OS files of the virtualized Microsoft Active Directory Server, Microsoft Exchange Server, Microsoft SharePoint Server, Microsoft SQL Server or Oracle, you can launch a Veeam Explorer for the necessary application directly from the Veeam Backup browser.

- To start Veeam Explorer for Active Directory, browse to the Microsoft Active Directory database file (DIT) in the Veeam Backup browser, select it and click **Application Items > Active Directory Items** on the **Home** tab or double-click the DIT file.
- To start Veeam Explorer for Exchange, browse to the Microsoft Exchange database file (EDB) in the Veeam Backup browser, select it and click **Application Items > Exchange Items** on the **Home** tab or double-click the EDB file.
- To start Veeam Explorer for SharePoint, browse to the Microsoft SharePoint content database (MDF) in the Veeam Backup browser, select it and click **Application Items > SharePoint Items** on the **Home** tab or double-click the MDF file.
- To start Veeam Explorer for Microsoft SQL, browse to the Microsoft SQL database file in the Veeam Backup browser, select it and click **Application Items > SQL Server Databases** on the **Home** tab or double-click the Microsoft SQL database file. For more information, see <http://technet.microsoft.com/en-us/library/ms143547.aspx>.
- To start Veeam Explorer for Oracle, browse to the Microsoft Oracle content database in the Veeam Backup browser, select it and click **Oracle** on the **Home** tab or double-click the database file.

Working with Windows Explorer

You can use Microsoft Windows Explorer to work with restored files and folders.

To open Microsoft Windows Explorer:

1. Click **Explore** on the ribbon in the Veeam Backup browser or right-click the necessary folder and select **Explore**.
2. Veeam Backup Free Edition will launch Microsoft Windows Explorer. Browse to the necessary VM guest OS files.

You can also start Microsoft Windows Explorer from the **Start** menu of Microsoft Windows and browse to the necessary VM guest OS files. VM disks are mounted under the `C:\veeamflr\<vmname>\<volume n>` folder on the backup server.

Closing Veeam Backup Browser

You can browse restored files and folders only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Backup Free Edition unmounts the VM disks from the temporary VM.

It is recommended that you close the Veeam Backup browser after you have finished restoring files and folders. In the opposite case, the backup file(s) from which you restore VM guest OS files may remain locked and operations using the file(s) may fail.

Veeam Backup Free Edition checks if there is any activity in the Veeam Backup browser every 5 minutes. If the user or Veeam Backup Free Edition components and services have not performed any actions for 30 minutes, Veeam Backup Free Edition displays a warning notifying that the Veeam Backup browser will be closed within 5 minutes.

After the warning is displayed, you can perform one of the following actions:

- You can close the Veeam Backup browser manually.
- You can click **Cancel** to postpone the close operation. In this case, the Veeam Backup browser will remain open for 5 minutes. After this period expires, Veeam Backup Free Edition will display the warning again.
- You can perform no action. In this case, the Veeam backup browser will be automatically closed in 5 minutes.

Restoring VM Guest OS Files (Linux, Unix and other)

You can restore VM guest OS files from the storage snapshot. Veeam Backup Free Edition supports guest-file restore for the most commonly used file systems on Linux, Solaris, BSD, Unix and Novell Storage Services.

When you perform VM guest OS file restore, you must select an ESX(i) host in your virtual environment. Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot on which the VM disks reside and mounts the clone/virtual copy to the selected ESX(i) host as a new LUN/volume.

To the mounted clone/virtual copy, Veeam Backup Free Edition copies an ISO of the proxy appliance, a helper VM. The proxy appliance is rather small — around 42 MB; it requires 1024 MB RAM and takes only 10 seconds to boot. Veeam Backup Free Edition automatically starts the proxy appliance on the ESX(i) host and mounts disks of the restored VM to the proxy appliance as virtual hard drives. VMDK files are mounted directly from storage snapshots. After disks are mounted, you can copy necessary VM guest OS files and folders to their initial location, local machine drive or save them in a network shared folder.

Before you start file-level restore, [check prerequisites](#). Then use the **File Level Restore** wizard to restore the necessary files and folders.

Before You Begin

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

- If you plan to restore VM guest OS files to their initial location, VMware Tools must be installed on the target VM.
- If the kernel version of the target Linux system is 2.6.18 or later, Veeam Backup Free Edition will be able to restore ACL for recovered VM guest OS files. To let Veeam Backup Free Edition detect the target Linux system architecture and kernel version, the following utilities must be installed on the VM OS: *arch* and *uname*.
- Veeam Backup Free Edition must have access to the guest OS of the target VM 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.
- [For Linux/Unix-based target VM] Veeam Backup Free Edition uses the SSH protocol to communicate with the target Linux/Unix VM and requires the SCP utility on the target VM. Make sure that the SSH daemon is properly configured and SCP utility is available on the target VM.
- The storage system must be added to Veeam Backup Free Edition.
- [For HP 3PAR StoreServ storage systems and NetApp storage systems working over Fibre Channel] The ESX(i) host that you select for storage snapshots mounting must meet the following requirements:
 - a. The ESX(i) host must have access to the storage over a Fibre Channel connection.
 - b. The ESX(i) host must be added to the list of servers having access to storage snapshots from which you plan to restore VM data.
 - c. [For NetApp storage systems] You must create an initiator group on the NetApp storage system. The initiator group must contain a WWN of the ESX(i) host to which you plan to mount the storage snapshot.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see *Veeam Backup & Replication User Guide for VMware vSphere*.

Mind the following limitations:

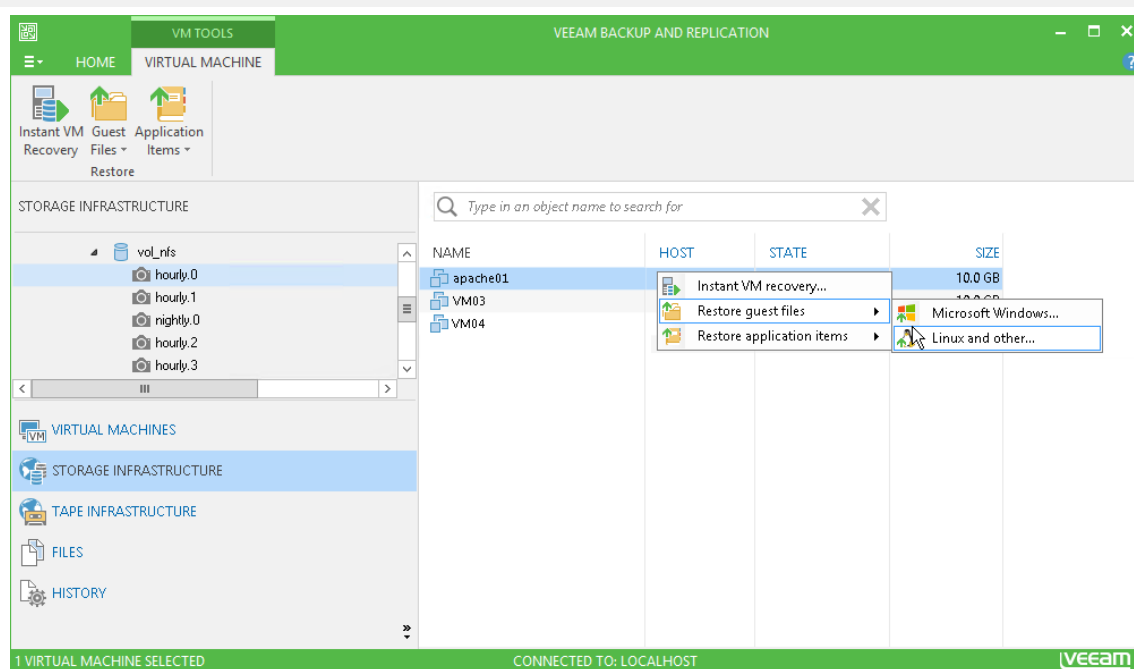
- You cannot restore files directly to the original location from backups of BSD, Mac, Novell and Solaris VMs. Use the **Copy to** option instead.
- You cannot restore files directly to the original location if disks of the VM are located on NetApp SnapVault or SnapMirror. Use the **Copy to** option instead.
- VMs with virtual disk files located on different storage volumes are not supported. You will be able to restore VM data only from VM disks residing on the same datastore as the VMX file.

Step 1. Launch Veeam File Level Restore Wizard

To launch the **File-Level Recovery** wizard:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, expand the storage system tree and select the necessary volume snapshot.
3. In the working area, select the VM and click **Guest Files > Other OS** on the toolbar. You can also right-click the VM you want to restore and select **Restore Linux guest files**.

Tip: To quickly find the necessary VM, use the search field at the top of the window: enter a VM name or a part of it and press **[ENTER]**.



Step 2. Select Location for the Proxy Appliance

At the **Ready to Apply** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot will be mounted. On the selected ESX(i) host, Veeam Backup Free Edition will also place a proxy appliance and mount disks of the restored VM to this proxy appliance.

To specify destination for the snapshot clone/virtual copy and proxy appliance:

1. Click the **Customize** link at the bottom of the window.
2. In the **FLR Appliance Configuration** window, select an ESX(i) host to which the snapshot clone must be mounted and on which the proxy appliance must be registered.
3. In the **Resource pool** field, specify a resource pool to which the proxy appliance must be placed.
4. In the **Network** section, specify an IP address and other network settings for the proxy appliance. The proxy appliance must be placed in the same network where the backup server resides.
5. To enable FTP access to the restored file system, select the **Enable FTP server on appliance** check box. As a result, your users will be able to access the proxy appliance via FTP, browse the file system of the restored VM and download necessary files on their own.
6. If you are performing restore of a VM with the Novell Storage services file system, select the **Restore from Novell Storage Services (NSS) file system** check box. In this case, Veeam Backup Free Edition will deploy a specific proxy appliance that supports the Novell file system.
7. Click **OK**.

Important! When choosing an ESX(i) host for the Novell file system proxy appliance, make sure that it allows running VMs with 64-bit guest OSes.

FLR Appliance Configuration

Specify ESX(i) server, resource pool and network settings for FLR helper appliance. Be sure to choose the same network where the VM you are restoring files to is located.

Host:
ess01.tech.local Choose...

Statistics
VMs: 36 total
17 running

Resource pool:
Resources Choose...

Network:
VM Network Choose...

☒ Obtain an IP address automatically
☐ Use the following IP address:

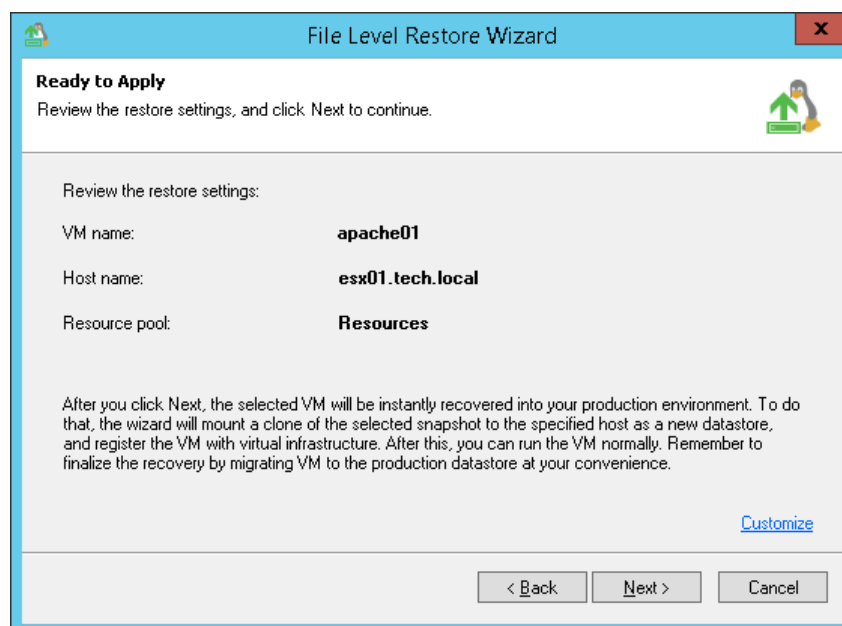
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

☒ Enable FTP server on appliance (advanced)
☐ Restore from Novell Storage Services (NSS) file system

OK Cancel

Step 3. Start Restore Process

At the **Ready to Apply** step of the wizard, click **Next** to start the restore process. The file-level restore appliance may take about 10-20 seconds to boot.



Step 4. Save Restored Files

When the restore process is complete, Veeam Backup Free Edition opens the Veeam Backup browser displaying the file system tree of the restored VM.

You can save the restored files and folders to their original location, new location or access files on FTP.

Note: You can browse to the VM guest OS files and access restored files on the FTP only while the Veeam Backup browser with the restored files is open. After the Veeam Backup browser is closed, the VM disks will be unmounted from the proxy appliance. The proxy appliance will be deleted and the storage snapshot will be unmounted from the ESX(i) host (unless this storage snapshot is used by other restore operations).

Saving Files to Original Location

To save files and folders to the original location, right-click a file or folder in the Veeam Backup browser and select one of the following commands:

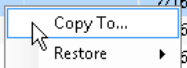
- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**. Veeam Backup Free Edition will add the *RESTORED-* prefix to the original file name and save the restored file in the same location where the original file resides.

To restore files to the original location, Veeam Backup Free Edition uses the account for VM guest OS access specified in the backup job settings. If this account does not have sufficient rights to access the target VM, you will be prompted to enter credentials. In the **Credentials window**, specify a user account to access the destination location (server or shared folder). You can use the account under which you are currently logged on or a different account.

To save files and folders to a new location:

- The server you add ad-hoc will not appear in the list of managed hosts in Veeam Backup Free Edition: its purpose is to host the files that you recover. It will only remain visible in the Veeam Backup browser until all currently active file-level restore sessions are completed.

To restore original permissions and ownership settings of restored files and folders, the account you have specified must have privileges to change the owner on the selected server or in the shared folder.



If you have chosen to enable FTP server on the FLR appliance, the restored file system will also be available over FTP at `ftp://<FLR_appliance_IP_address>`. Other users in the same network can access the FLR appliance and restore files they need.

Restoring Application Items

You can use Veeam Explorers to restore application items directly from storage snapshots.

Before You Begin

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

- The storage system must be added to the backup infrastructure.
- [For HP 3PAR StoreServ storage systems and NetApp storage systems working over Fibre Channel] The ESX(i) host that you select for storage snapshots mounting must meet the following requirements:
 - a. The ESX(i) host must have access to the storage over a Fibre Channel connection.
 - b. The ESX(i) host must be added to the list of servers having access to storage snapshots from which you plan to restore VM data.
 - c. [For NetApp storage systems] You must create an initiator group on the NetApp storage system. The initiator group must contain a WWN of the ESX(i) host to which you plan to mount the storage snapshot.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see *Veeam Backup & Replication User Guide for VMware vSphere*.

Mind the following limitations:

VMs with virtual disk files located on different storage volumes are not supported. You will be able to restore VM data only from VM disks residing on the same datastore as the VMX file.

Restoring Application Items from Microsoft Active Directory

Veeam Backup Free Edition integrates with Veeam Explorer for Microsoft Active Directory — a tool that lets you browse Microsoft Active Directory databases in VM disks located on storage snapshots and restore Microsoft Active Directory items (objects and containers) and their attributes back into the production Microsoft Active Directory database.

Before you can start working with Veeam Explorer for Microsoft Active Directory, you need to extract the Microsoft Active Directory database from the storage snapshot. You can do it in two ways:

- You can use the **Microsoft Active Directory Object Restore** wizard. In this case, Veeam Backup Free Edition will automatically extract the Microsoft Active Directory database from the storage snapshot and open it in Veeam Explorer for Microsoft Active Directory. For more information, see [Using the Microsoft Active Directory Object Restore Wizard](#).
- You can perform VM guest OS files recovery for the virtualized Microsoft Active Directory server, manually locate the Microsoft Active Directory database and open it in Veeam Explorer for Microsoft Active Directory. For more information, see [Opening Microsoft Active Directory Database Manually](#).

Using Microsoft Active Directory Object Restore Wizard

When you run the **Microsoft Active Directory Object Restore** wizard, Veeam Backup Free Edition automatically extracts the Microsoft Active Directory database from the storage snapshot and opens it in Veeam Explorer for Microsoft Active Directory.

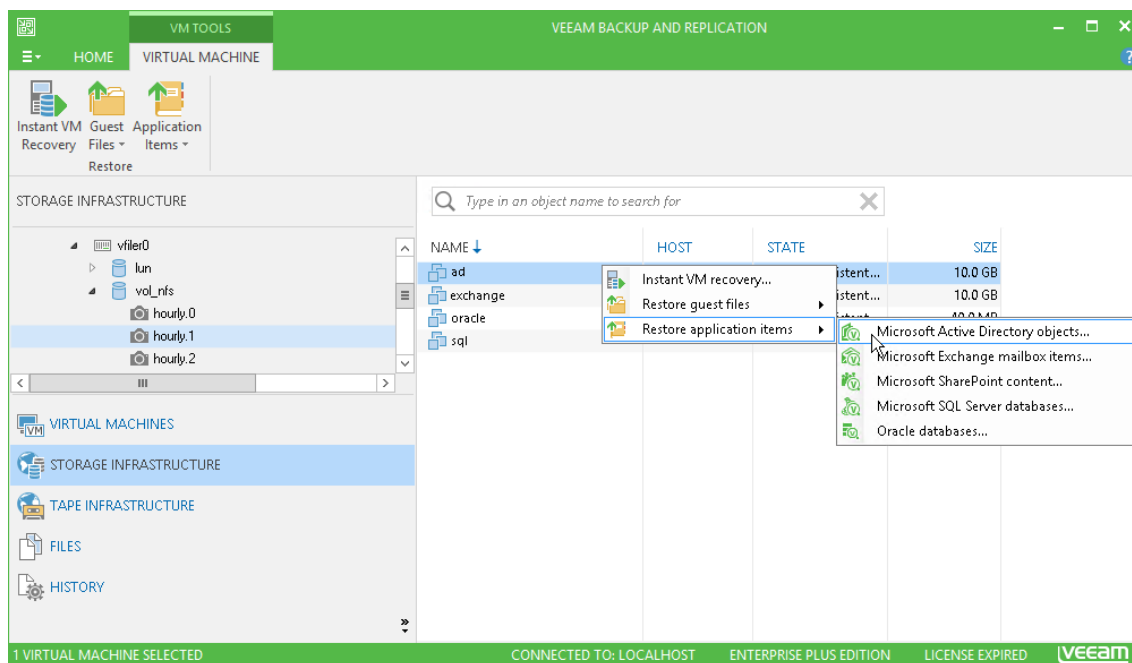
As part of this procedure, Veeam Backup Free Edition performs the following actions:

1. Veeam Backup Free Edition creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to the ESX(i) host.
2. Veeam Backup Free Edition accesses the configuration file of the virtualized Microsoft Active Directory server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.
3. Veeam Backup Free Edition mounts disks of the restored Microsoft Active Directory server to the temporary VM.
4. Veeam Backup Free Edition locates the Microsoft Active Directory database and opens it in Veeam Explorer for Microsoft Active Directory.

Step 1. Launch Microsoft Active Directory Object Restore Wizard

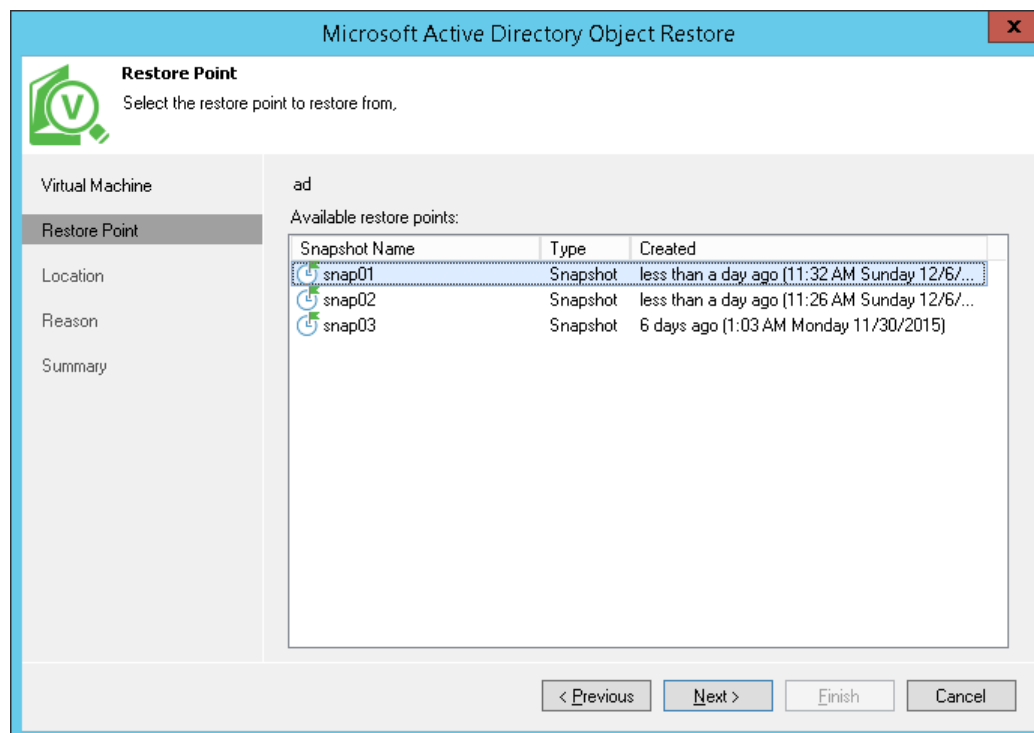
To launch the **Microsoft Active Directory Item Level Restore** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the inventory pane, expand the storage system tree and select the necessary volume snapshot. In the working area, select the necessary VM and click **Application Items > Active Directory Items** on the ribbon or right-click the VM and select **Microsoft Active Directory items**. In this case, you will pass immediately to the **Location** step of the wizard.
- In the **Storage Infrastructure** view, type a VM name or a part of it in the search field above the VM list and press [ENTER]. In the working area, select the necessary VM and click **Application Items > Active Directory Items** on the ribbon or right-click the VM and select **Microsoft Active Directory items**. In this case, you will pass to the **Restore Point** step of the wizard.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, Veeam Backup Free Edition will display all storage snapshots on which VM disks are available. Every snapshot acts as an independent restore point. Select the snapshot from which you want to restore Microsoft Active Directory objects.



Step 3. Select ESX(i) Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot must be mounted. On the selected ESX(i) host, Veeam Backup Free Edition will create a temporary VM and mount the disks of the virtualized Microsoft Active Directory to this temporary VM.

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

1. At the **Location** step of the wizard, click **Customize**.
2. Click **Choose** next to the **Host** field and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Click **Choose** next to the **Resource pool** field and select a resource pool to which the temporary VM must be placed.
4. Click **Choose** next to the **Folder** field and select a folder to which the temporary VM must be placed.
5. Click **OK**.

Microsoft Active Directory Object Restore

Location
Specify where the location where a temporary VM should be registered. This VM will remain powered off, and will be automatically removed once the restore process completes.

Virtual Machine
Restore Point
Location
Reason
Summary

Restore Configuration

Specify a host to mount Storage snapshot to, as well as resource pool and VM folder for temporary VM. Once you finish restoring, the wizard will perform clean up automatically.

Host: 172.16.21.0 Choose...

Resource pool: Resources Choose...

VM folder: vm Choose...

OK Cancel

Customize

< Previous Next > Finish Cancel

Step 4. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring a database from the Microsoft Active Directory if necessary. The information you provide will be saved in the session history and you can view it later.

Tip: If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

Microsoft Active Directory Object Restore

Reason
Provide the restore reason for the future reference.

Virtual Machine
Restore Point
Location
Reason
Summary

Restore reason:
Restoring AD DB

☐ Do not show me this page again

< Previous Next > Finish Cancel

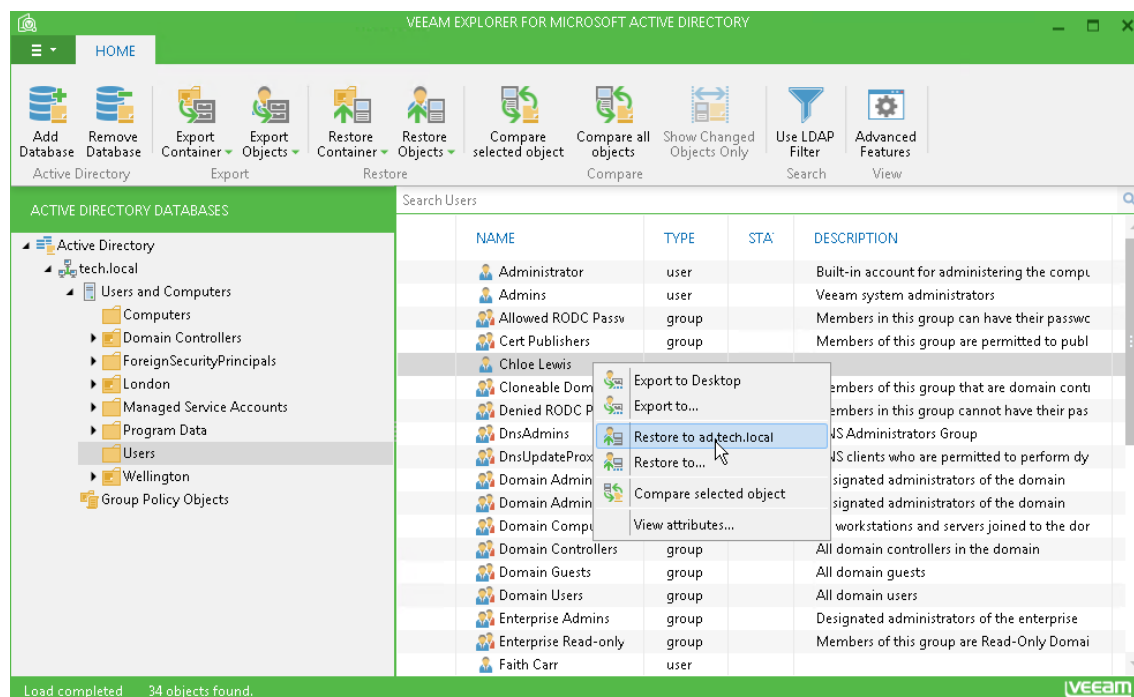
Step 5. Open Database in Veeam Explorer for Microsoft Active Directory

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

Veeam Backup Free Edition will automatically locate the Microsoft Active Directory database and open it in Veeam Explorer for Microsoft Active Directory. You can browse the database and restore items you need.

Detailed information about Veeam Explorer for Microsoft Active Directory is provided in the Veeam Explorer for Microsoft Active Directory help. To open the help, do one of the following:

- Open Veeam Explorer for Microsoft Active Directory and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Microsoft Active Directory.



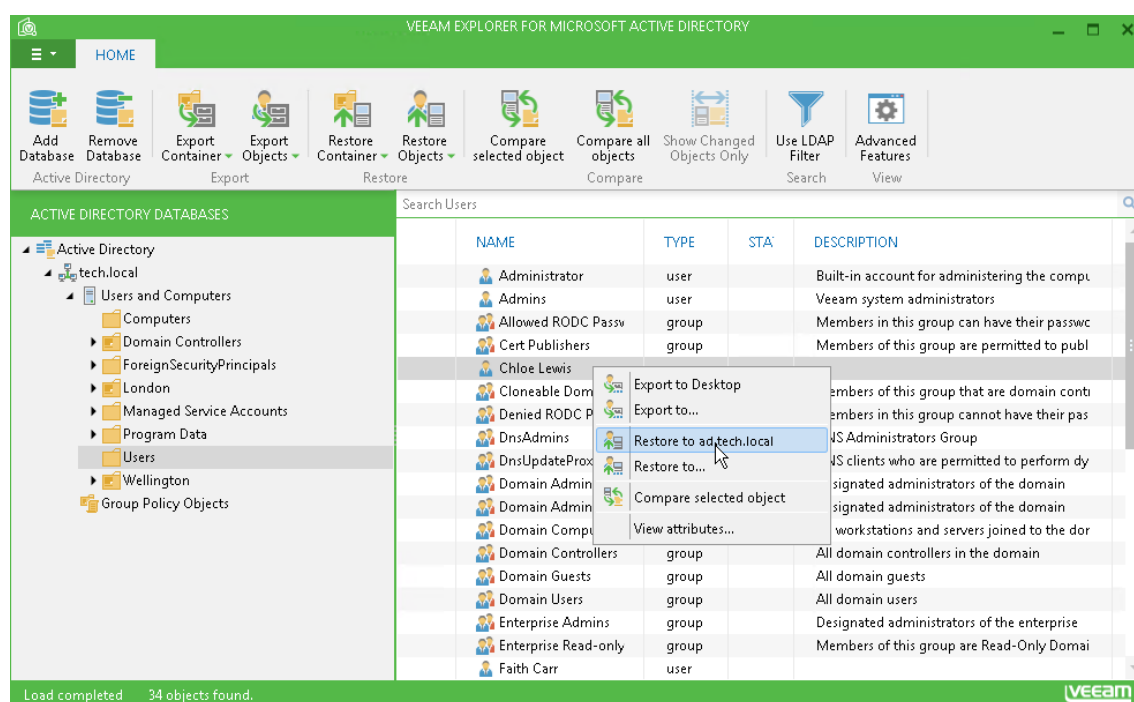
Opening Microsoft Active Directory Database Manually

You can restore the Microsoft Active Directory database from the storage snapshot with file-level restore and open it manually in Veeam Explorer for Microsoft Active Directory.

1. Perform VM guest OS files restore for the virtualized Microsoft Active Directory server. For more information, see [Restoring VM Guest OS Files \(Microsoft Windows\)](#).
2. In the Veeam Backup browser, locate the Microsoft Active Directory database file (NTDS.dit) and double-click it or select the NTDS.dit file and click **Application Items > Active Directory Items** on the ribbon.
3. Veeam Backup Free Edition will open the database in Veeam Explorer for Microsoft Active Directory. After that, you can browse the database and restore Microsoft Active Directory objects.

Detailed information about Veeam Explorer for Microsoft Active Directory is provided in the Veeam Explorer for Microsoft Active Directory help. To open the help, do one of the following:

- Open Veeam Explorer for Microsoft Active Directory and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Microsoft Active Directory.



Restoring Application Items from Microsoft Exchange

Veeam Backup Free Edition integrates with Veeam Explorer for Microsoft Exchange — a tool that lets you browse Microsoft Exchange mailbox stores in VM disks located on storage snapshots and restore Microsoft Exchange items you need.

Before you can start working with Veeam Explorer for Microsoft Exchange, you need to extract the Microsoft Exchange database (EDB file) from the storage snapshot. You can do it in two ways:

- You can use the **Microsoft Exchange Item Level Restore** wizard. In this case, Veeam Backup Free Edition will automatically extract the Microsoft Exchange database from the storage snapshot and open it in Veeam Explorer for Microsoft Exchange. For more information, see [Using the Microsoft Exchange Item Level Restore Wizard](#).
- You can perform VM guest OS files recovery for the virtualized Microsoft Exchange server, manually locate the restored Microsoft Exchange database and open it in Veeam Explorer for Microsoft Exchange. For more information, see [Opening EDB File Manually](#).

Using Microsoft Exchange Item Level Restore Wizard

When you run the **Microsoft Exchange Item Level Restore** wizard, Veeam Backup Free Edition automatically extracts the Microsoft Exchange database (EDB file) from the storage snapshot and opens it in Veeam Explorer for Microsoft Exchange.

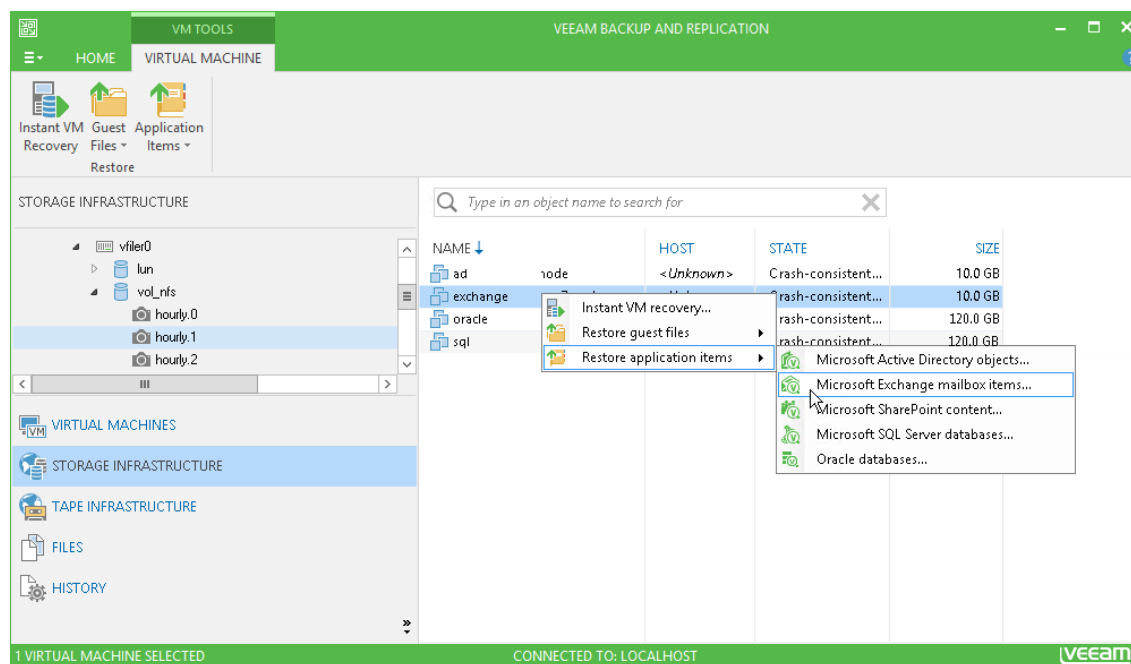
As part of this procedure, Veeam Backup Free Edition performs the following steps:

1. Veeam Backup Free Edition creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to the ESX(i) host.
2. Veeam Backup Free Edition accesses the configuration file of the virtualized Microsoft Exchange server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.
3. Veeam Backup Free Edition mounts disks of the restored Microsoft Exchange server to the temporary VM.
4. Veeam Backup Free Edition scans the Microsoft Exchange Event log to locate the EDB file and the ese .d11 file on the mounted disks. The ese .d11 file is required for configuring Veeam Explorer for Exchange.
5. After the EDB file is successfully located, Veeam Backup Free Edition opens it in Veeam Explorer for Exchange, and you can browse it to find necessary items.

Step 1. Launch Microsoft Exchange Item Level Restore Wizard

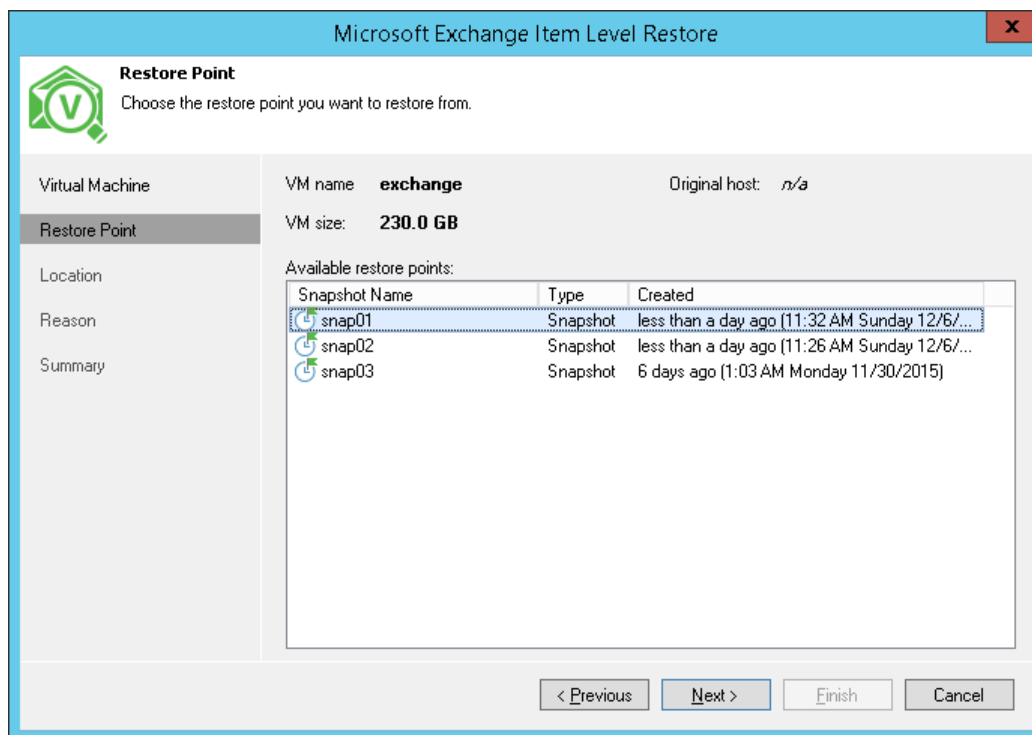
To launch the **Microsoft Exchange Item Level Restore** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the inventory pane, expand the storage system tree and select the necessary volume snapshot. In the working area, select the necessary VM and click **Application Items > Exchange Items** on the ribbon or right-click the VM and select **Microsoft Exchange items**. In this case, you will pass immediately to the **Location** step of the wizard.
- Type a VM name or a part of it in the search field above the VM list and press **[ENTER]**. In the working area, select the necessary VM and click **Application Items > Exchange Items** on the ribbon or right-click the VM and select **Microsoft Exchange items**. In this case, you will pass to the **Restore Point** step of the wizard.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, Veeam Backup Free Edition will display all storage snapshots on which VM disks are available. Every snapshot acts as an independent restore point. Select the snapshot from which you want to restore Microsoft Exchange mailbox items.

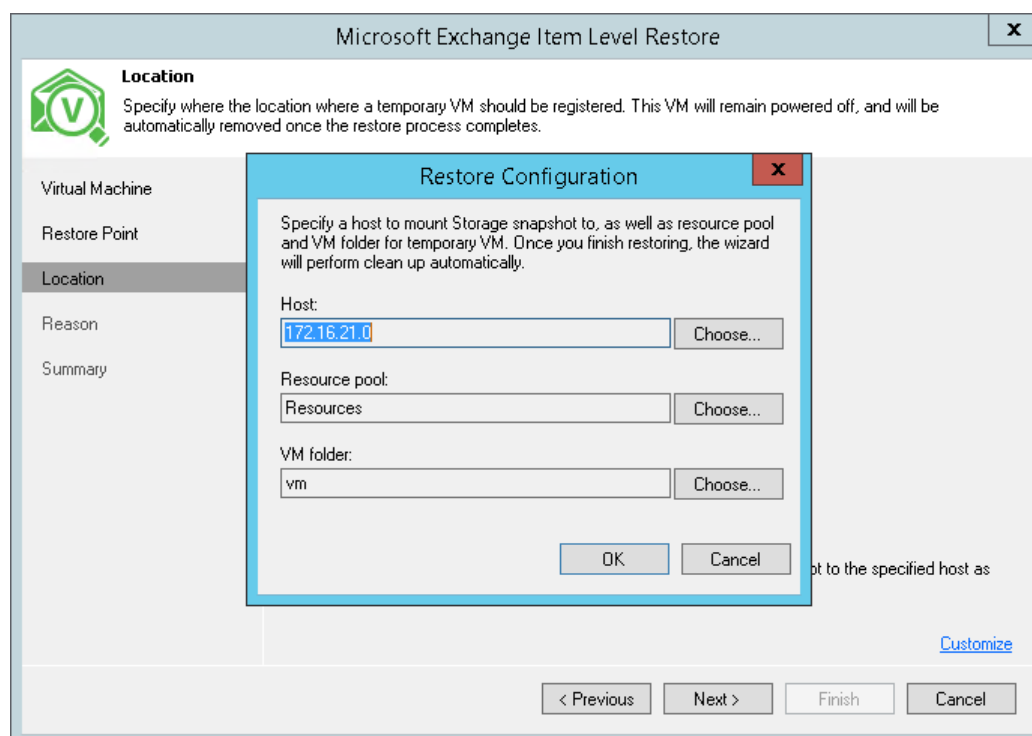


Step 3. Select ESX(i) Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot will be mounted. On the selected ESX(i) host, Veeam Backup Free Edition will create a temporary VM and mount the disks of the virtualized Microsoft Exchange server to this temporary VM.

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

1. At the **Location** step of the wizard, click **Customize**.
2. Click **Choose** next to the **Host** field and select an ESX(i) host to which the snapshot clone must be mounted and on which the temporary VM must be created.
3. Click **Choose** next to the **Resource pool** field and select a resource pool to which the temporary VM must be placed.
4. Click **Choose** next to the **Folder** field and select a folder to which the temporary VM must be placed.
5. Click **OK**.



Step 4. Specify Restore Reason

At the **Reason** step of the wizard, enter the reason for restoring data from Microsoft Exchange if necessary. The information you provide will be saved in the session history and you can view it later.

Tip: If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

Microsoft Exchange Item Level Restore

Reason
Provide the restore reason for future reference.

Virtual Machine
Restore Point
Location
Reason
Summary

Restore reason:
Restoring mailbox items

☐ Do not show me this page again

< Previous Next > Finish Cancel

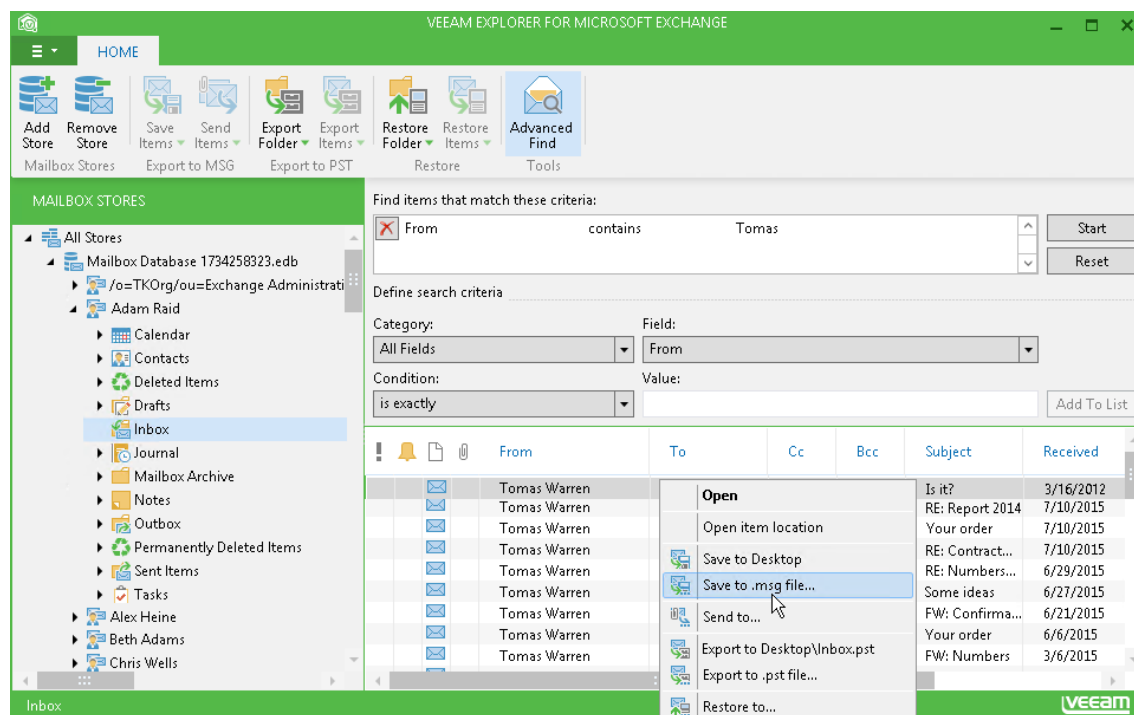
Step 5. Open EDB File in Veeam Explorer for Microsoft Exchange

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

Veeam Backup Free Edition will automatically locate the Microsoft Exchange database and open it in Veeam Explorer for Microsoft Exchange. You can browse the database and restore items you need.

Detailed information about Veeam Explorer for Microsoft Exchange is provided in the Veeam Explorer for Microsoft Exchange help. To open the help, do one of the following:

- Open Veeam Explorer for Microsoft Exchange and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Microsoft Exchange.



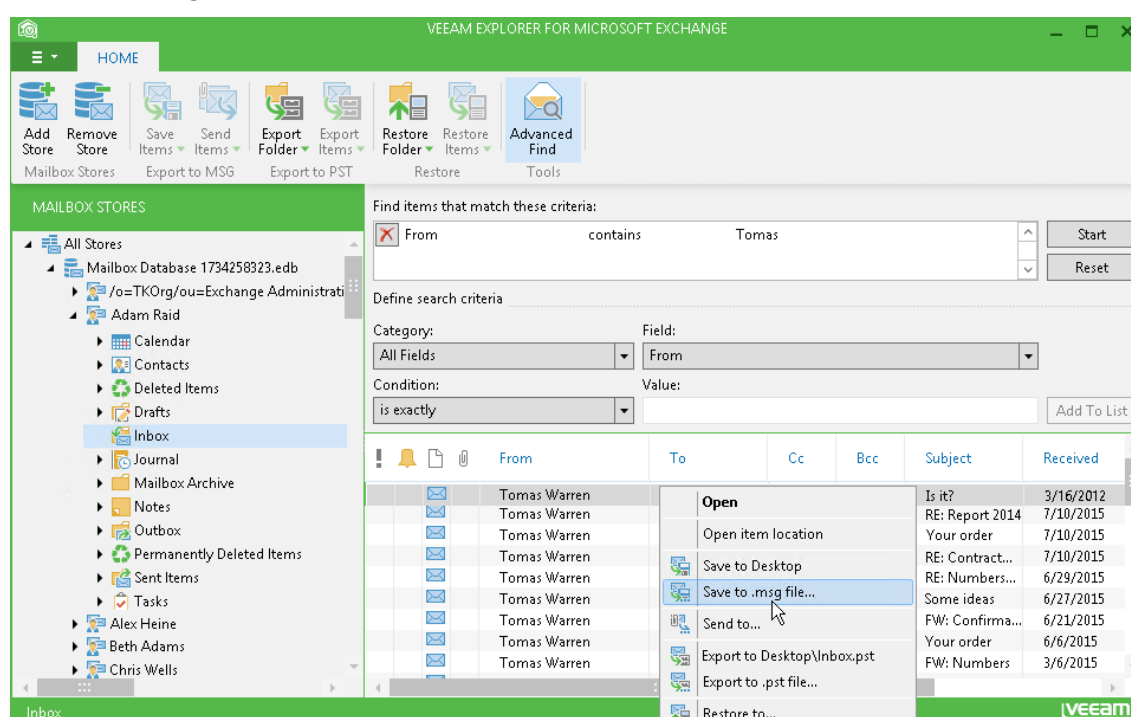
Opening EDB File Manually

If Veeam Backup Free Edition fails to locate the Microsoft Exchange database on the restored VM for some reason, you can restore it with file-level restore and open it manually.

1. Perform VM guest OS files restore for the virtualized Microsoft Exchange server. For more information, see [Restoring VM Guest OS Files \(Microsoft Windows\)](#).
2. In the Veeam Backup browser, locate the EDB file and double-click it or select the EDB file and click **Application Items > Exchange Items** on the ribbon.
3. Veeam Backup Free Edition will open the selected database in Veeam Explorer for Microsoft Exchange. After that, you can browse the database and restore items you need.

Detailed information about Veeam Explorer for Microsoft Exchange is provided in the Veeam Explorer for Microsoft Exchange help. To open the help, do one of the following:

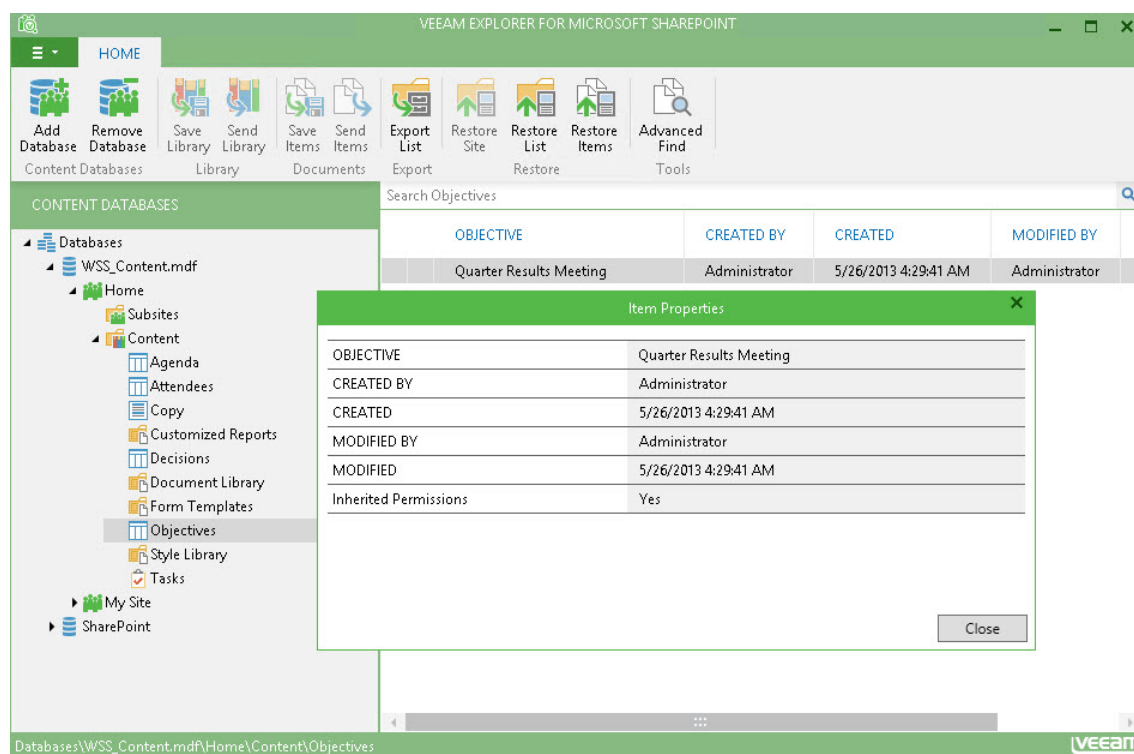
- Open Veeam Explorer for Microsoft Exchange and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Microsoft Exchange.



Restoring Application Items from Microsoft SharePoint

Veeam Backup Free Edition integrates with Veeam Explorer for Microsoft SharePoint — a tool that lets you browse Microsoft SharePoint content databases in VM disks located on storage snapshots and restore documents, items and document libraries you need.

Before you can start working with Veeam Explorer for Microsoft SharePoint, you need to extract the Microsoft SharePoint content database (MDF file) from the storage snapshot. To do this, you can perform VM guest OS files recovery for the virtualized Microsoft SharePoint server, manually locate the content database and open it in Veeam Explorer for Microsoft SharePoint. For more information, see [Opening Content Database Manually](#).



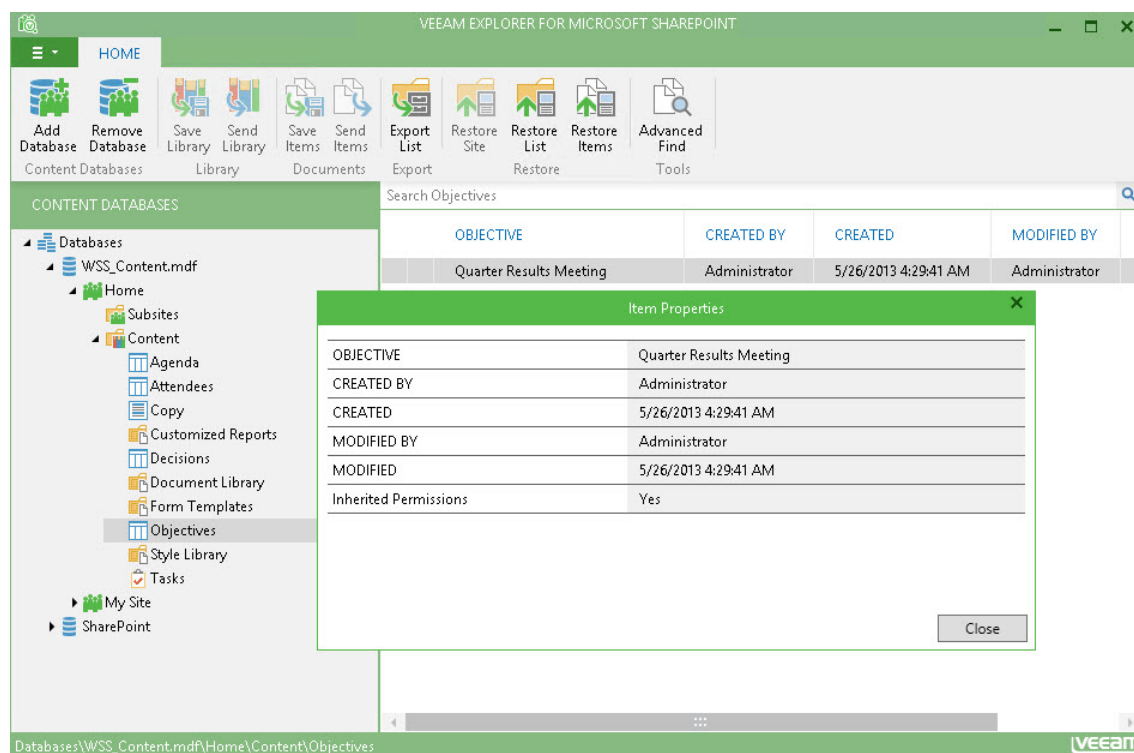
Opening Content Database Manually

You can restore the Microsoft SharePoint content database from the storage snapshot with file-level restore and open it manually.

1. Perform VM guest OS files restore for the virtualized Microsoft SharePoint server. For more information, see [Restoring VM Guest OS Files \(Microsoft Windows\)](#).
2. In the Veeam Backup browser, locate the MDF file and double-click it or select the file and click **Application Items > SharePoint Items** on the ribbon.
3. Veeam Backup Free Edition will attach the content database to the Microsoft SQL Server on which the Veeam Backup Free Edition database is deployed and open the database in Veeam Explorer for Microsoft SharePoint. After that, you can browse the database and restore items you need.

Detailed information about Veeam Explorer for Microsoft SharePoint is provided in the Veeam Explorer for Microsoft SharePoint help. To open the help, do one of the following:

- Open Veeam Explorer for Microsoft SharePoint and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Microsoft SharePoint.



Restoring Databases from Microsoft SQL

Veeam Backup Free Edition integrates with Veeam Explorer for Microsoft SQL — a tool that lets you browse Microsoft SQL databases in VM disks located on storage snapshots and restore Microsoft SQL databases.

Before you can start working with Veeam Explorer for Microsoft SQL, you need to extract the Microsoft SQL database from the storage snapshot. You can do it in two ways:

- You can use the **Microsoft SQL Server Database Restore** wizard. In this case, Veeam Backup Free Edition will automatically extract the Microsoft SQL database from the storage snapshot and open it in Veeam Explorer for Microsoft SQL. For more information, see [Using the Microsoft SQL Server Database Restore Wizard](#).
- You can perform VM guest OS files recovery for the virtualized Microsoft SQL server, manually locate the restored Microsoft SQL database and open it in Veeam Explorer for Microsoft SQL. For more information, see [Opening Microsoft SQL Server Database Manually](#).

Using the Microsoft SQL Server Database Restore Wizard

When you run the **Microsoft SQL Server Database Restore** wizard, Veeam Backup Free Edition automatically extracts the Microsoft SQL database from the storage snapshot and opens it in Veeam Explorer for Microsoft SQL.

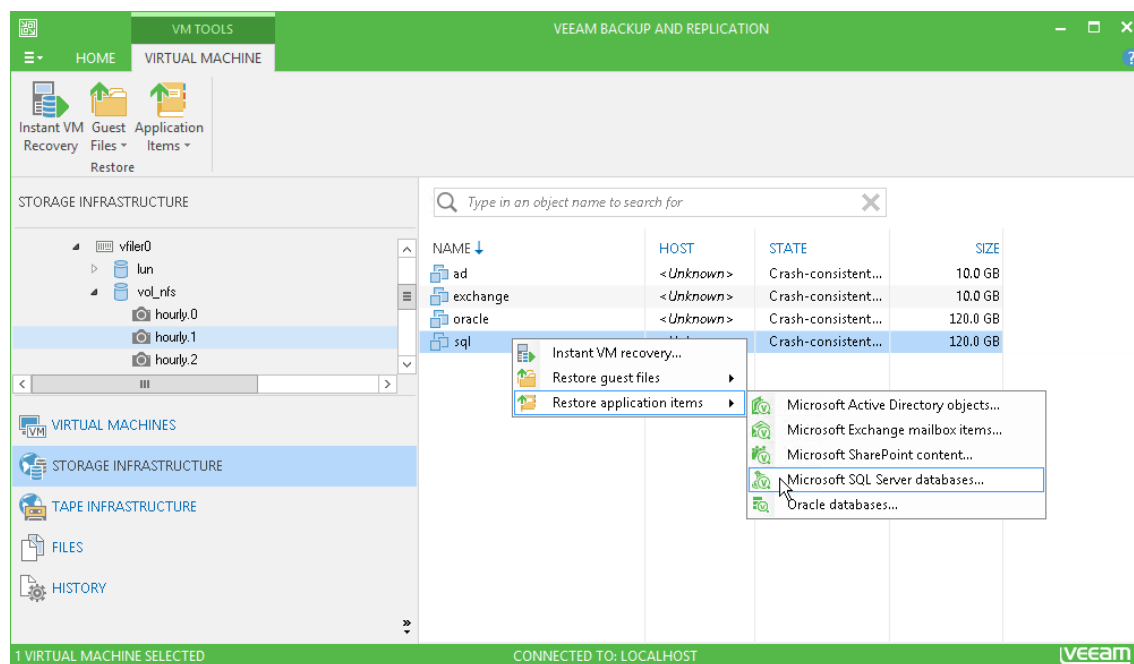
As part of this procedure, Veeam Backup Free Edition performs the following actions:

1. Veeam Backup Free Edition creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to the ESX(i) host.
2. Veeam Backup Free Edition accesses the configuration file of the virtualized Microsoft SQL server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.
3. Veeam Backup Free Edition mounts disks of the restored Microsoft SQL server to the temporary VM.
4. Veeam Backup Free Edition locates the Microsoft SQL database and attaches the content database to a staging Microsoft SQL Server. As a staging server, Veeam Backup Free Edition uses the Microsoft SQL Server on which the Veeam Backup Free Edition database is deployed.
5. Veeam Backup Free Edition opens the restored database in Veeam Explorer for Microsoft SQL.

Step 1. Launch Microsoft SQL Server Database Restore Wizard

To launch the **Microsoft SQL Server Database Restore** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the inventory pane, expand the storage system tree and select the necessary volume snapshot. In the working area, select the necessary VM and click **Application Items > SQL Server Databases** on the ribbon or right-click the VM and select **Microsoft SQL items**. In this case, you will pass immediately to the **Location** step of the wizard.
- In the **Storage Infrastructure** view, type a VM name or a part of it in the search field above the VM list and press **[ENTER]**. In the working area, select the necessary VM and click **Application Items > SQL Server Databases** on the ribbon or right-click the VM and select **Microsoft SQL items**. In this case, you will pass to the **Restore Point** step of the wizard.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, Veeam Backup Free Edition will display all storage snapshots on which VM disks are available. Every snapshot acts as an independent restore point. Select the snapshot from which you want to restore the Microsoft SQL database.

The screenshot shows the 'Microsoft SQL Server Database Restore' wizard window. The title bar reads 'Microsoft SQL Server Database Restore'. The main area is titled 'Restore Point' with the instruction 'Choose the restore point to restore from.' On the left, a sidebar contains the following items: 'Virtual Machine' (selected), 'Restore Point', 'Location', 'Reason', and 'Summary'. The 'Virtual Machine' section shows 'sql01'. The 'Restore Point' section has two radio buttons: 'Restore from the latest available backup' (unselected) and 'Restore from this restore point:' (selected). Below these is a table of snapshots:

Snapshot Name	Type	Created
snap01	Snapshot	less than a day ago (11:32 AM Sunday 12/6/...
snap02	Snapshot	less than a day ago (11:26 AM Sunday 12/6/...
snap03	Snapshot	6 days ago (1:03 AM Monday 11/30/2015)

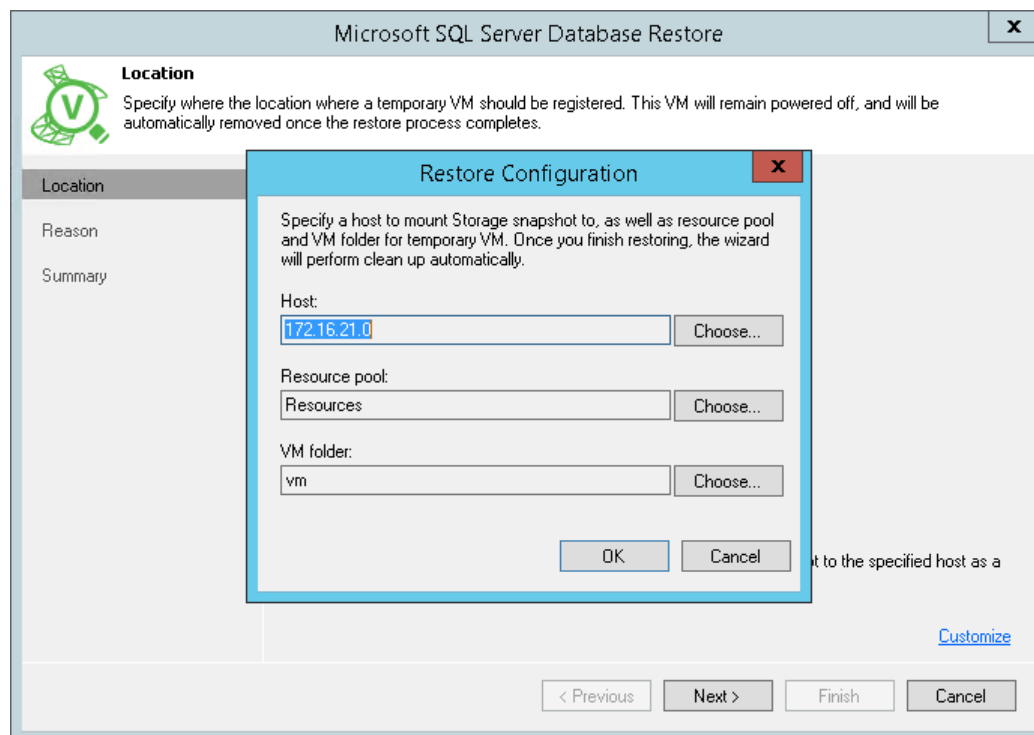
At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 3. Select ESX(i) Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot must be mounted. On the selected ESX(i) host, Veeam Backup Free Edition will create a temporary VM and mount the disks of the virtualized Microsoft SQL Server to this temporary VM.

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

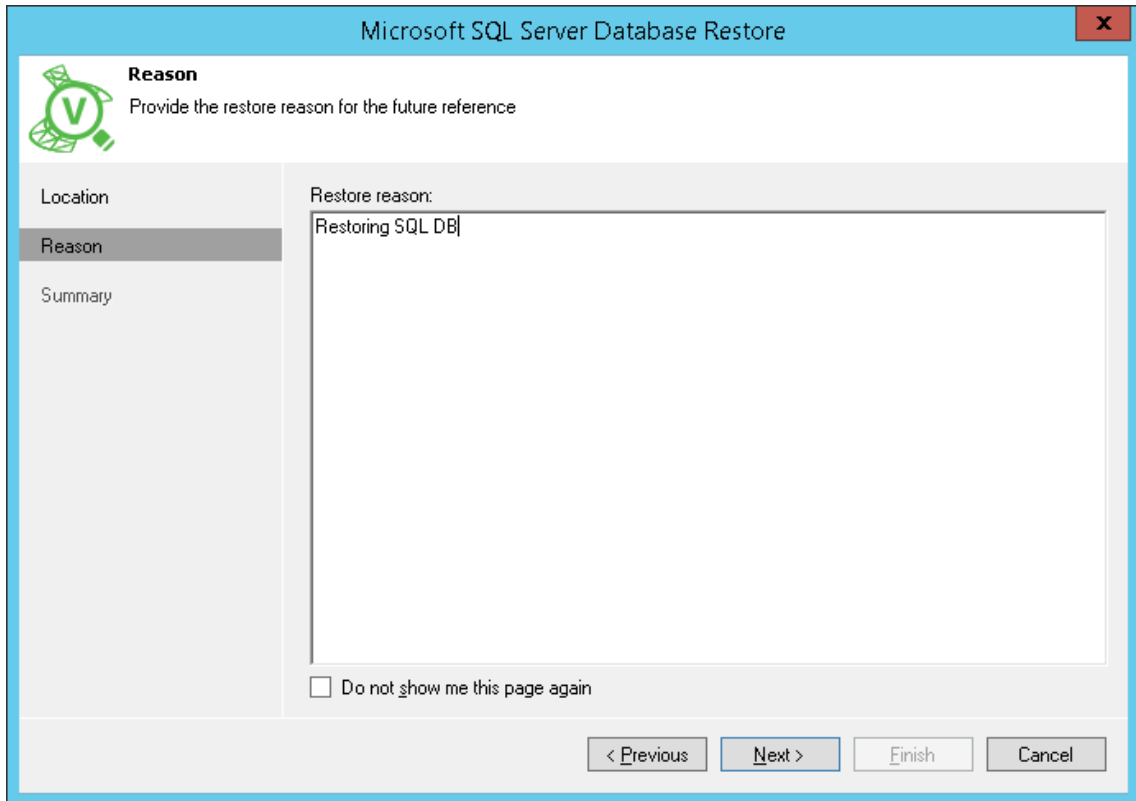
1. At the **Location** step of the wizard, click **Customize**.
2. Click **Choose** next to the **Host** field and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Click **Choose** next to the **Resource pool** field and select a resource pool to which the temporary VM must be placed.
4. Click **Choose** next to the **Folder** field and select a folder to which the temporary VM must be placed.
5. Click **OK**.



Step 4. Specify Restore Reason

At the **Reason** step of the wizard, enter the reason for restoring a database from the Microsoft SQL Server if necessary. The information you provide will be saved in the session history and you can view it later.

Tip: If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.



The screenshot shows the 'Microsoft SQL Server Database Restore' wizard window. The title bar is blue with the text 'Microsoft SQL Server Database Restore' and a red close button. The main window has a light blue header with a green 'V' icon and the text 'Reason' and 'Provide the restore reason for the future reference'. On the left, there is a sidebar with four items: 'Location', 'Reason' (which is highlighted with a grey background), and 'Summary'. The main area on the right is titled 'Restore reason:' and contains a large text box with the text 'Restoring SQL DB'. Below the text box is a checkbox labeled 'Do not show me this page again'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

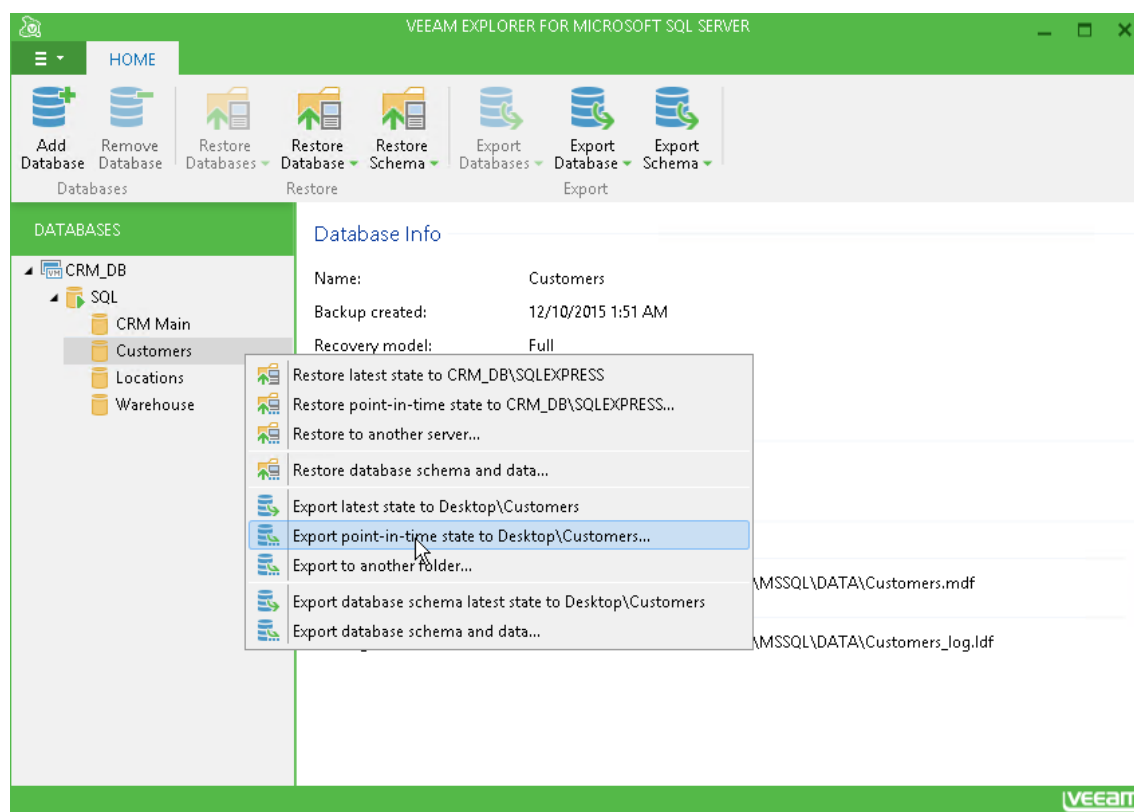
Step 5. Open Database in Veeam Explorer for Microsoft SQL

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

Veeam Backup Free Edition will automatically locate the Microsoft SQL database and attach the content database to the staging Microsoft SQL Server. After that, Veeam Backup Free Edition will open the Veeam Explorer for Microsoft SQL and add the restored database to it.

Detailed information about Veeam Explorer for Microsoft SQL is provided in the Veeam Explorer for Microsoft SQL help. To open the help, do one of the following:

- Open Veeam Explorer for Microsoft SQL Server and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Microsoft SQL.



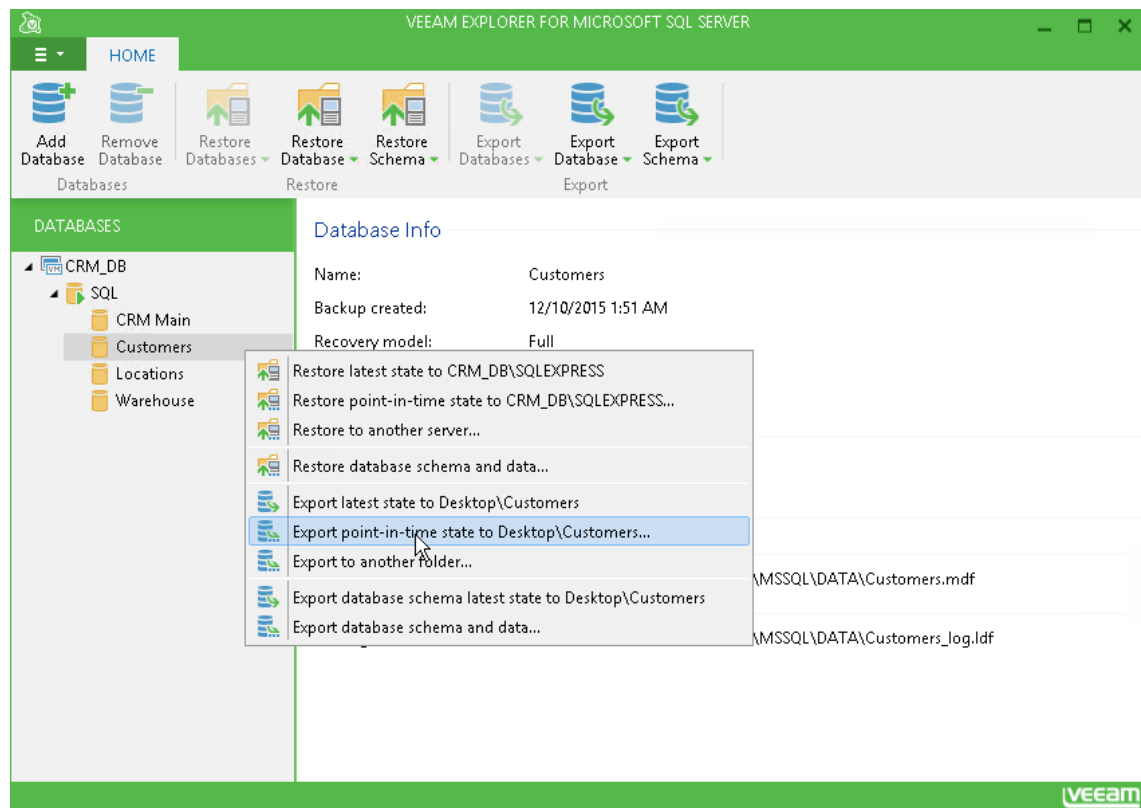
Opening Microsoft SQL Server Database Manually

You can restore the Microsoft SQL Server database from the storage snapshot with file-level restore and open it manually.

1. Perform VM guest OS files restore for the virtualized Microsoft SQL server. For more information, see [Restoring VM Guest OS Files \(Microsoft Windows\)](#).
2. In the Veeam Backup browser, locate the MDF file and double-click it or select the file and click **Application Items > SQL Server Databases** on the ribbon.
3. Veeam Backup Free Edition will attach the restored database to the Microsoft SQL Server on which the Veeam Backup Free Edition database is deployed and open the selected database in Veeam Explorer for Microsoft SQL. After that, you can restore the database to the necessary Microsoft SQL Server.

Detailed information about Veeam Explorer for Microsoft SQL is provided in the Veeam Explorer for Microsoft SQL help. To open the help, do one of the following:

- Open Veeam Explorer for Microsoft SQL Server and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Microsoft SQL.



Restoring Databases from Oracle

Veeam Backup Free Edition integrates with Veeam Explorer for Oracle — a tool that lets you browse Oracle databases in VM disks located on storage snapshots and restore Oracle databases.

Before you can start working with Veeam Explorer for Oracle, you need to extract the Oracle database from the storage snapshot. You can do it in two ways:

- You can use the **Oracle Database Restore** wizard. In this case, Veeam Backup Free Edition will automatically extract the Oracle database from the storage snapshot and open it in Veeam Explorer for Oracle. For more information, see [Using the Oracle Database Restore Wizard](#).
- You can perform VM guest OS files recovery for the virtualized Oracle server, manually locate the restored Oracle database and open it in Veeam Explorer for Oracle. For more information, see [Opening Oracle Database Manually](#).

Using the Oracle Restore Wizard

When you run the **Oracle Database Restore** wizard, Veeam Backup Free Edition automatically extracts the Oracle database from the storage snapshot and opens it in Veeam Explorer for Oracle.

As part of this procedure, Veeam Backup Free Edition performs the following actions:

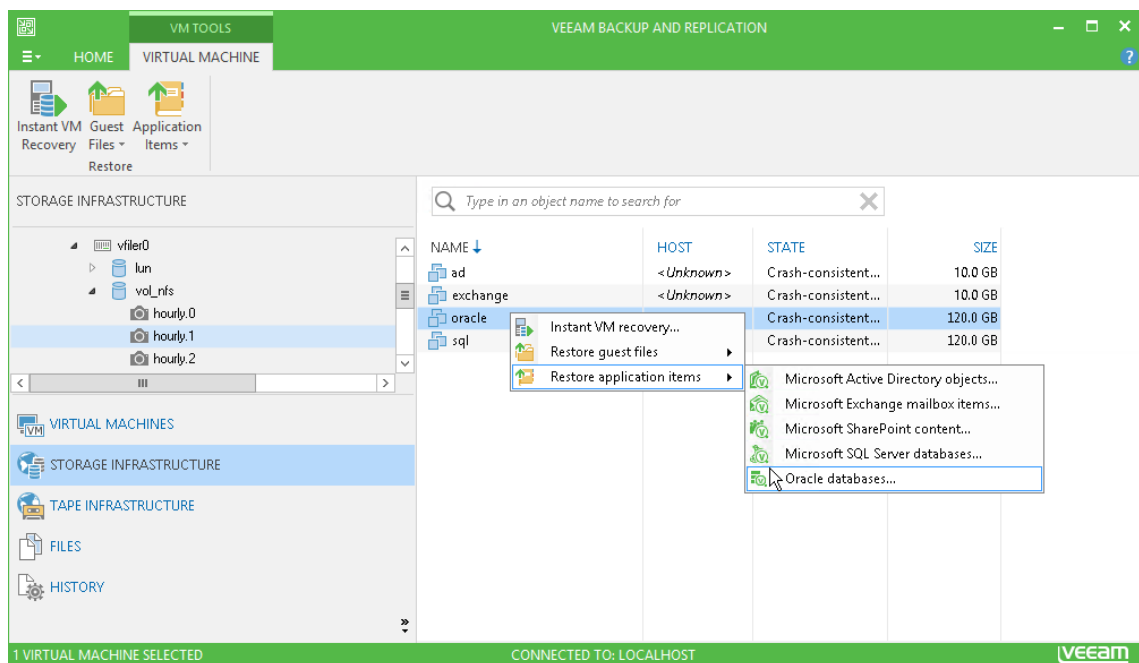
1. Veeam Backup Free Edition creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to the ESX(i) host.
2. Veeam Backup Free Edition accesses the configuration file of the virtualized Oracle server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.
3. Veeam Backup Free Edition mounts disks of the restored Oracle server to the temporary VM.
4. Veeam Backup Free Edition locates the Oracle database and attaches the database to a staging Oracle server.
5. Veeam Backup Free Edition opens the restored database in Veeam Explorer for Oracle.

Step 1. Launch Oracle Database Restore Wizard

To launch the **Oracle Database Restore** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the inventory pane, expand the storage system tree and select the necessary volume snapshot. In the working area, select the necessary VM and click **Application Items > Oracle** on the ribbon or right-click the VM and select **Oracle databases**. In this case, you will pass immediately to the [Location](#) step of the wizard.
- Type a VM name or a part of it in the search field above the VM list and press **[ENTER]**. In the working area, select the necessary VM and click **Application Items > Oracle** on the ribbon or right-click the VM and select **Oracle databases**. In this case, you will pass to the [Restore Point](#) step of the wizard.

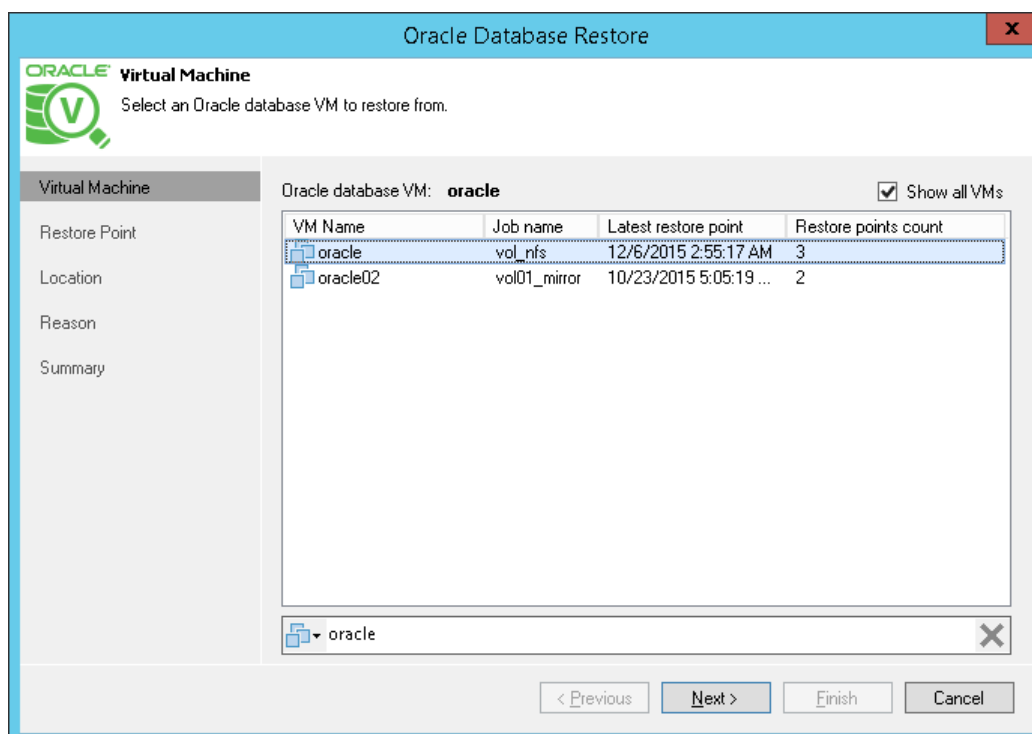
To quickly find the necessary VM, you can use the search field at the top of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.



Step 2. Select VM

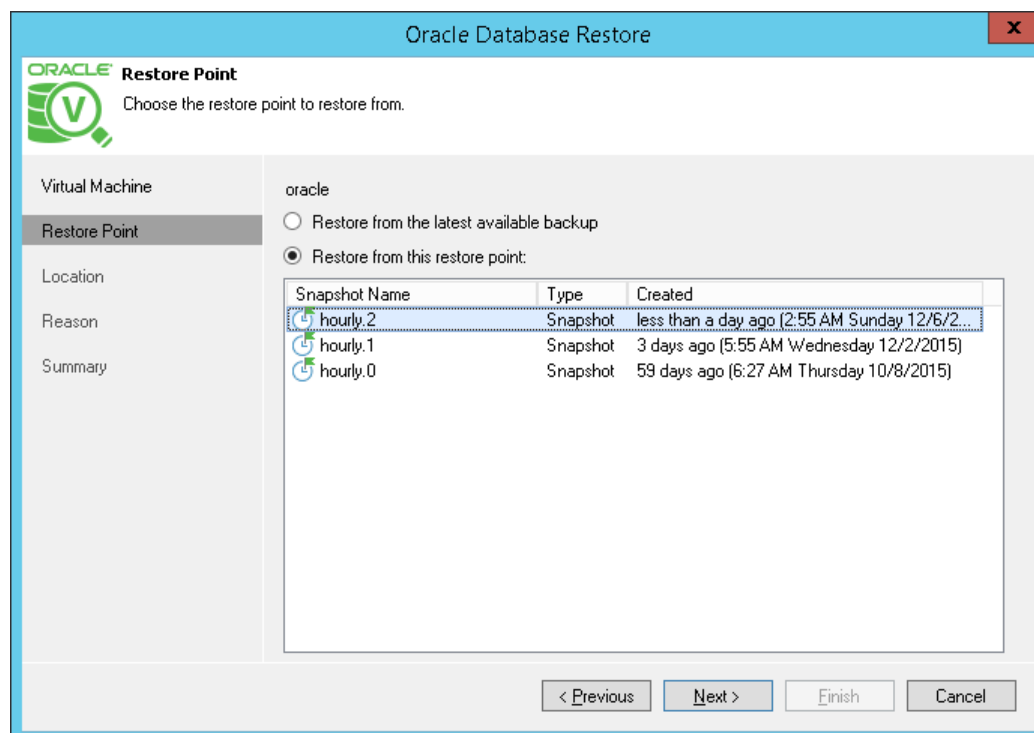
At the **Virtual Machine** step of the wizard, Veeam Backup Free Edition displays all Oracle VMs with disks on storage volumes. Select the necessary VM in the list. If the necessary VM is not displayed automatically, select the **Show all VMs** check box. Veeam Backup Free Edition will display all VMs with disks on storage volumes.

To quickly find the necessary 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 the necessary restore point for the VM. Every snapshot of a volume acts as an independent restore point.



Step 4. Select ESX(i) Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot must be mounted. On the selected ESX(i) host, Veeam Backup Free Edition will create a temporary VM and mount the disks of the virtualized Oracle VM to this temporary VM.

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

1. At the **Location** step of the wizard, click **Customize**.
2. Click **Choose** next to the **Host** field and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Click **Choose** next to the **Resource pool** field and select a resource pool to which the temporary VM must be placed.
4. Click **Choose** next to the **Folder** field and select a folder to which the temporary VM must be placed.
5. Click **OK**.

Oracle Database Restore

Location
Specify where the location where a temporary VM should be registered. This VM will remain powered off, and will be automatically removed once the restore process completes.

Virtual Machine
Restore Point
Location
Reason
Summary

Restore Configuration

Specify a host to mount Storage snapshot to, as well as resource pool and VM folder for temporary VM. Once you finish restoring, the wizard will perform clean up automatically.

Host: 172.16.21.0 Choose...

Resource pool: Resources Choose...

VM folder: vm Choose...

OK Cancel

Customize

< Previous Next > Finish Cancel

Step 5. Specify Restore Reason

At the **Reason** step of the wizard, enter the reason for restoring a database from the Oracle VM if necessary. The information you provide will be saved in the session history and you can view it later.

Tip: If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

Oracle Database Restore

Reason
Provide the restore reason for the future reference

Virtual Machine
Restore Point
Location
Reason
Summary

Restore reason:
Restoring Oracle DB

☐ Do not show me this page again

< Previous Next > Finish Cancel

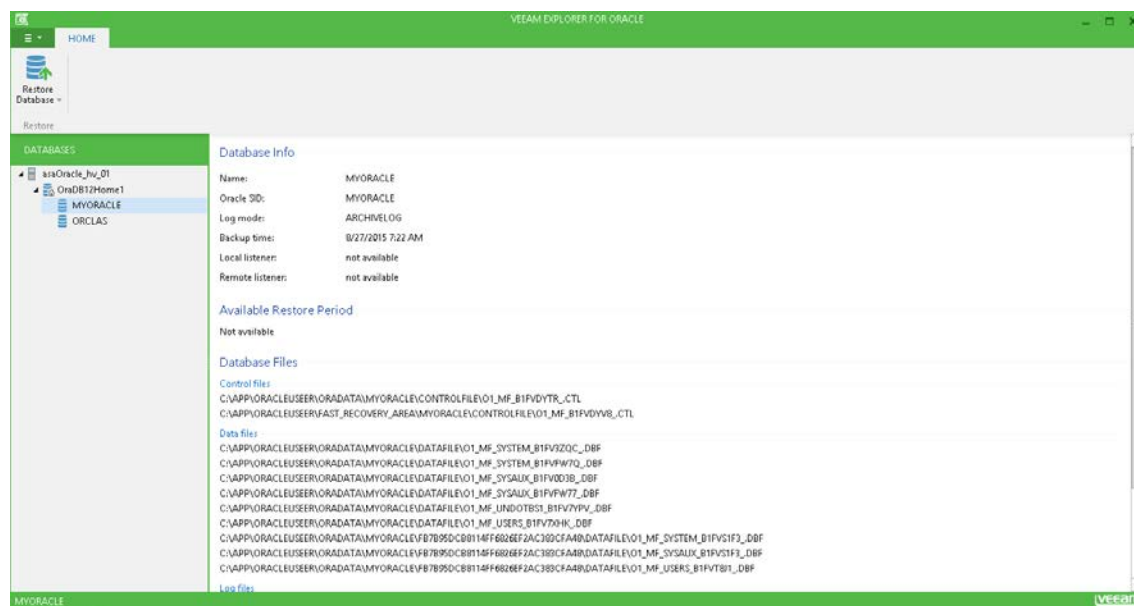
Step 6. Open the Database in Veeam Explorer for Oracle

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

Veeam Backup Free Edition will automatically locate the Oracle database and attach the content database to the staging server. After that, Veeam Backup Free Edition will open the Veeam Explorer for Oracle and add the restored database to it.

Detailed information about Veeam Explorer for Oracle is provided in the Veeam Explorer for Oracle help. To open the help, do one of the following:

- Open Veeam Explorer for Oracle and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Oracle.



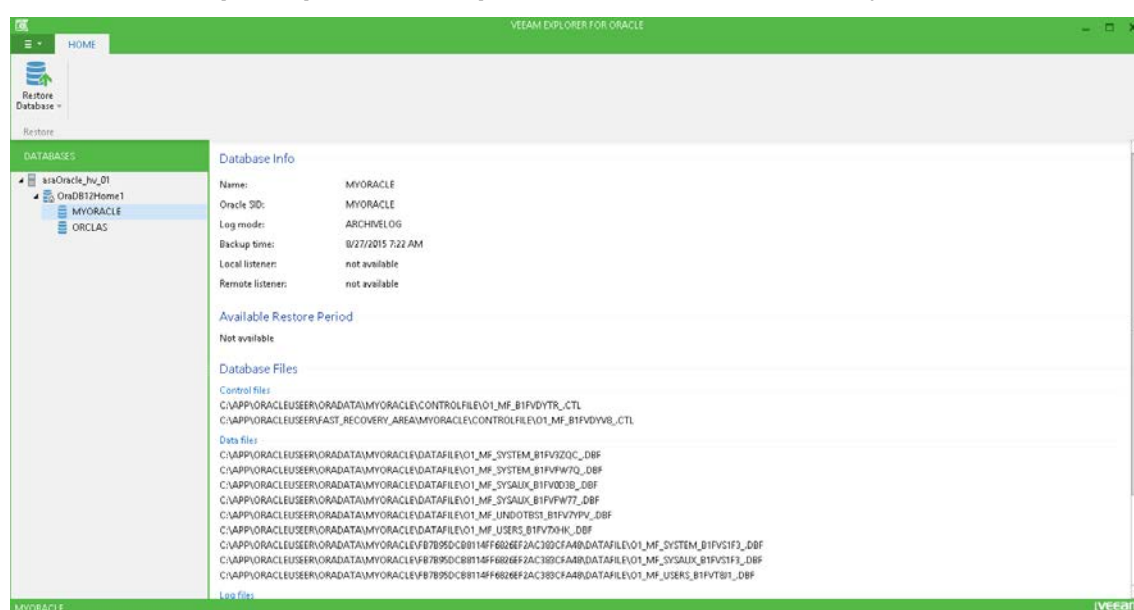
Opening Oracle Database Manually

You can restore the Oracle database from the storage snapshot with file-level restore and open it manually.

1. Perform VM guest OS files restore for the virtualized Oracle server. For more information, see [Restoring VM Guest OS Files \(Microsoft Windows\)](#).
2. In the Veeam Backup browser, locate the database file and double-click it or select the file and click **Application Items > Oracle databases** on the ribbon.
3. Veeam Backup Free Edition will attach the restored database to the staging server and open the selected database in Veeam Explorer for Oracle. After that, you can restore the database to the necessary Oracle server.

Detailed information about Veeam Explorer for Oracle is provided in the Veeam Explorer for Oracle help. To open the help, do one of the following:

- Open Veeam Explorer for Oracle and press **[F1]**.
- Select **Help > Help** or **Online Help** from the main menu of Veeam Explorer for Oracle.



Working with Tape Media

Veeam provides native support for backing up your data to tape. Tape backup is an easy and high-reliable storing scheme protecting your backups from disaster or occasional loss.

To start backing up data to tape, you need to deploy the tape backup infrastructure and configure Veeam Backup Free Edition to meet your secondary destination storage policies.

To back up data to tape, you need to create a tape job that can run manually or on schedule. To restore data from tape, you need to insert the tapes containing the needed data and start the restore process that runs fully automated.

With Veeam Backup Free Edition, you can perform the following operations:

- Back up to tape files with user data: Veeam Backup Free Edition allows you to back up any files with no limitation to file format. To back up files, you need to create a dedicated file to tape job that is able to archive full and incremental backups of user files. As a data source, you can select any Windows or Linux server that is accessible by the Veeam backup server. You can also write to tape Veeam backups as files.
- Restore files that were previously archived to tape with file to tape job. The Files from Tape wizard allows you to navigate through the tape archive selecting the files you need and restore them to original location or any other disk or folder in your backup infrastructure.
- Restore Veeam VM backups from tape to repository. The Restore Backup from Tape to Repository wizard will help you to choose a restore point available on tape and set the target repository.

Getting Started with Tapes

To start working with tapes in Veeam Backup Free Edition, you need to complete the following steps:

1. Connect the tape device to a tape server.
2. Add the tape server to Veeam Backup Free Edition.
3. Load tapes to the tape device (if not yet loaded) and run the importing procedure for them.
4. Create one or more custom media pools that will be used as targets for files to tape jobs.
5. Configure and run files to tape jobs.
6. Restore files from tape or restore VM backups to repository.

Deploying Tape Devices

To add the tape devices to Veeam Backup Free Edition, you need to perform the following steps:

1. **Connect the tape devices to the machine that will act as the tape server.** You can choose between the following options:
 - Deploy a dedicated Microsoft Windows server, physical or virtual, accessible by Veeam Backup Free Edition.
 - Use the Veeam backup server as the tape server.
2. **Add this machine to Veeam Backup Free Edition as a tape server.**

If you connect tape devices to the Veeam backup server, you also need to go through the adding procedure.

Connecting Tape Devices

To deploy a tape device, you must perform the following steps:

1. Connect the tape device to the machine that will perform the role of the tape server. You can connect the tape device in two ways:
 - Directly over Fibre Channel (FC), Serial Attached SCSI (SAS), SCSI
 - Remotely with iSCSI (you can use Microsoft iSCSI initiator to establish the connection).

2. Install an appropriate device driver on the tape server if the driver is available.

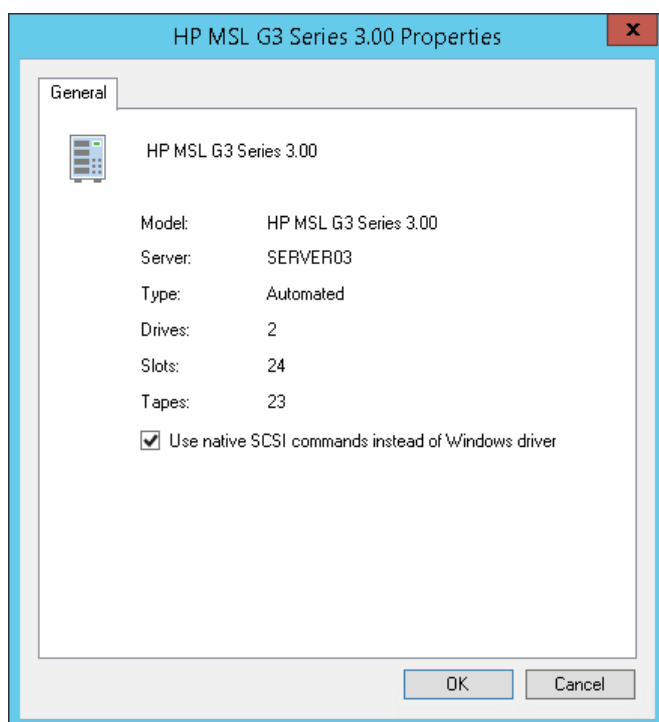
If multiple driver installation modes are supported for your storage device, make sure the driver is installed in the mode that allows for multiple open handles from a host to a drive to exist at the same time.

For example, if installing a driver for IBM System Storage TS3100 Tape Library or TS3200 Tape Library, you should use the install_nonexclusive.exe installer as described in the product Readme.

Please refer to your storage system manufacturer recommendations on choosing the appropriate setup option.

3. If the medium changer driver is not available, check that the tape device is connected over SCSI.

Open the **Tape Infrastructure** view, expand the **Libraries** node and select the needed library. Click **Properties** on the ribbon. You can also right-click the necessary library in the working area and select **Properties**. Select the **Use native SCSI commands instead of Windows driver** check box.



After you connected the tape device to the selected server, you need to add this server to Veeam Backup Free Edition as a tape server. Veeam Backup Free Edition will automatically scan attached tape devices and display all discovered tape libraries and tape drives under the **Libraries** node in the **Tape Infrastructure** view. Afterward, the auto-discovery process will be performed periodically every 3 minutes.

To each tape server you can connect a number of tape devices that will appear as list under the **Libraries** node in the **Tape Infrastructure** view.

Veeam Backup Free Edition allows deploying a number of tape servers. However, if you have a number of Veeam backup servers, you cannot connect one tape server to several Veeam backup servers simultaneously.

Tip: If you have a number of Veeam backup servers, you can easily reconnect a tape server to another Veeam backup server without reconfiguring the tape device: Veeam backup server will recognize the library settings automatically. Note that when you reconnect the tape server, the tape jobs will not run with another Veeam backup server unless you copy the configuration.

Reconnecting Tape Devices to Tape Server

If you have the tape devices connected directly, you can reconfigure your tape infrastructure and start using a dedicated tape server. In this case, all tape device settings will remain unchanged.

To reconnect the tape device, you must perform the following steps:

1. Choose a machine that will act as the tape server. The tape server must be a dedicated Microsoft Windows server, physical or virtual, accessible by Veeam Backup Free Edition.
2. Reconnect the tape device to the machine that will perform the role of the tape server. You can connect the tape device directly over Fibre Channel (FC), Serial Attached SCSI (SAS), SCSI) or remotely with iSCSI (you can use Microsoft iSCSI initiator to establish the connection).
3. Add the server as the tape server to Veeam Backup Free Edition: the connected tape device will be discovered automatically.

Working with Tape Servers

Tape servers are network appliances that are used to connect tape libraries to the Veeam backup server.

To be able to connect a tape device to Veeam Backup Free Edition, you need to deploy a tape server and add it to Veeam backup console.

Adding Tape Servers

When you have deployed a tape server and connected the tape device to it, you need to add the tape server to the Veeam backup server. To do so, you must assign the role of the tape server to a Windows server that is already added to the list of managed servers.

To add a tape server, follow the next steps:

Step 1. Launch the New Tape Server Wizard

To launch the wizard, do one of the following:

- Open the **Tape Infrastructure** view and click **Add Tape Server** on the ribbon.
- Open the **Tape Infrastructure** view, right-click the **Tape Infrastructure** node and select **Add Tape Server**.

Step 2. Choose a Server

At the **Server** step of the wizard, select a physical or virtual server to which the tape devices are connected and that you want to add as the tape server.

1. From the **Choose server** list, select the server that you want to add as the tape server.
 - If the devices are connected to the Veeam backup server, choose **This server**. The tape server role will be assigned to your backup server.
 - If the devices are connected to a separated server, enter the server name or IP address. The tape server must run Microsoft Windows. If the server is not added to Veeam Backup Free Edition yet, you can click **Add New** to open the **New Windows Server** wizard.
2. In the **Description** field, provide a description for future reference.

New Tape Server

**Server**

Choose a server to install tape server components on. You can only select between Microsoft Windows servers added to the managed servers tree in the console.

Server

Traffic

Review

Apply

Summary

Choose server:

172.17.53.10

Add New...

Description:

tapeserver 01

< Previous

Next >

Finish

Cancel

Step 3. Configure Traffic Throttling Rules

At the **Traffic** step of the wizard, configure throttling rules to limit the outbound traffic rate for the tape server. Throttling rules will help you manage bandwidth usage and minimize the impact of tape jobs on network performance.

The list of throttling rules contains only those rules that are applicable to the tape server you are adding. The rule is applied to the tape server if its IP address falls under the source IP range of the rule. To view the rule settings, select it in the list and click the **View** button on the right.

You can also open global throttling settings and modify them directly from the wizard by clicking **Manage network traffic throttling rules** at the bottom of the window.

New Tape Server

Traffic
Review the network traffic rules that apply to this server.

Server
Traffic
Review
Apply
Summary

Network traffic rules control encryption and throttling of network traffic based on the destination. Throttling is global, with set bandwidth split equally across all backup proxies falling into the rule.
The following network traffic rules apply to this proxy:

Destination IP range	Encryption	Throttling	Time period	

[Manage network traffic rules](#)

View

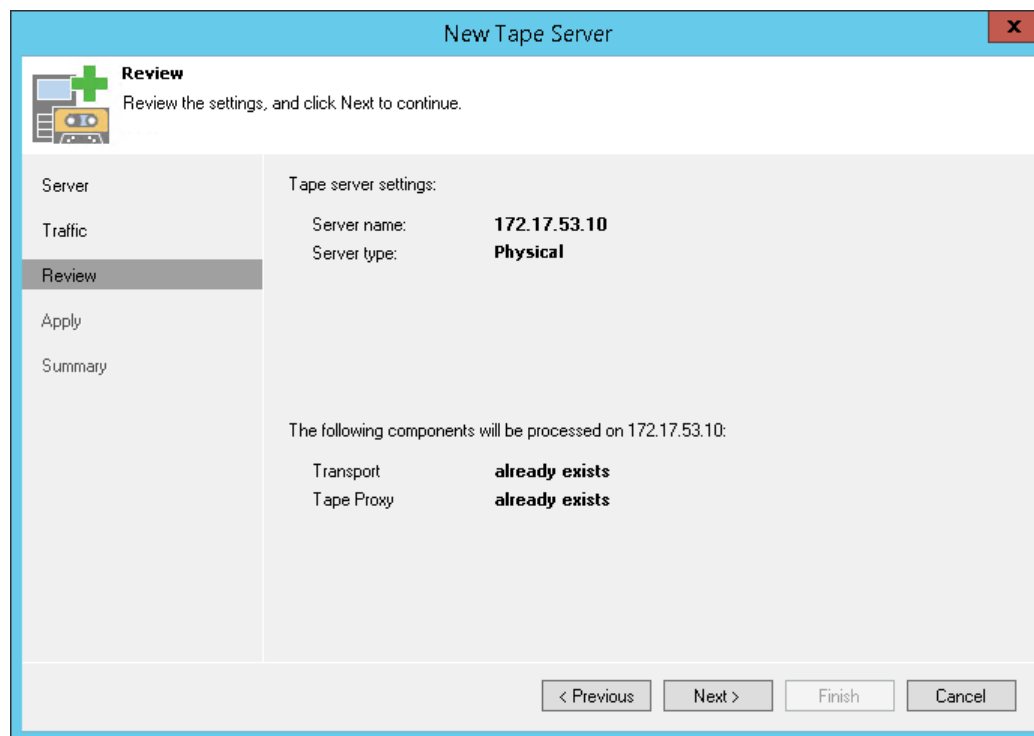
< Previous Next > Finish Cancel

Step 4. Review Components

At the **Review** step of the wizard, Veeam Backup Free Edition will display the list of components required for work of the tape server:

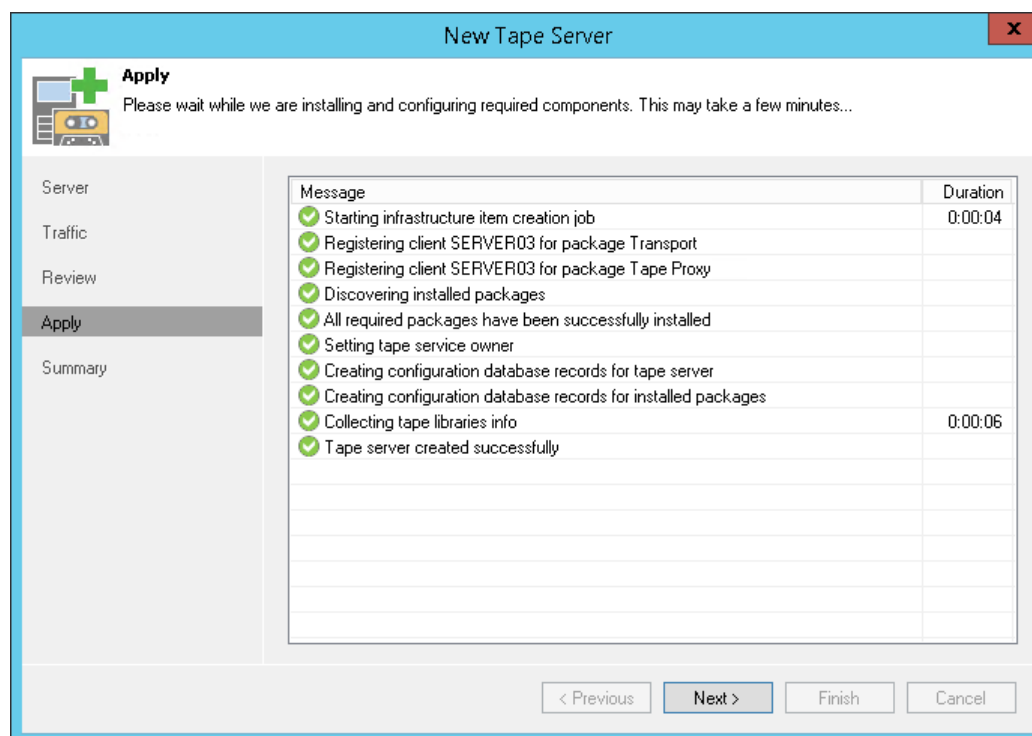
- Veeam Transport
- Veeam Tape service

If any of them is missing, Veeam Backup Free Edition will automatically install them on the selected server.



Step 5. Assess Results

At the **Apply** step of the wizard, Veeam Backup Free Edition will add the tape server to the backup infrastructure in the real time mode.

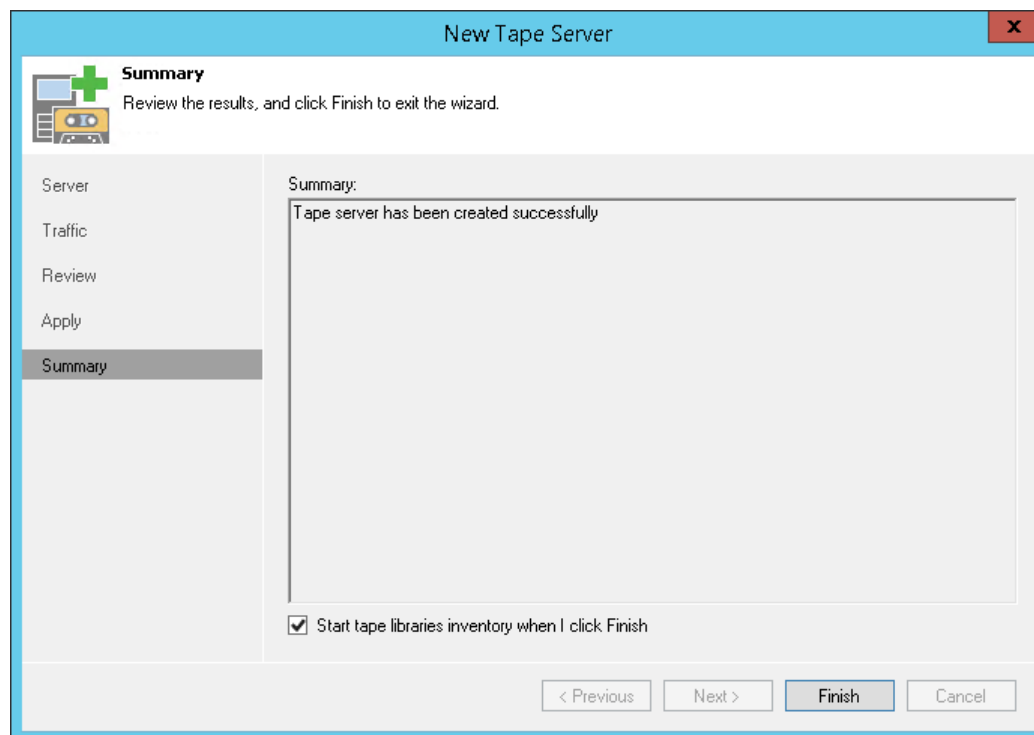


Step 6. Finish Working with the Wizard

At the **Summary** step of the wizard, finalize the procedure of the tape server configuration.

1. Review details of the added tape server.
2. To inventory tape libraries connected to the tape server, select the **Start tape libraries inventory when I click Finish** check box. Veeam Backup Free Edition will start the inventory process when you finish working with the wizard.

If you do not enable this option, you will have to inventory tape libraries manually. For more information, see [Inventorying Tapes](#).



Modifying Tape Servers

To edit settings of an added tape server:

1. Open the **Tape Infrastructure** view.
2. Select the **Servers** node in the inventory pane.
3. Select the necessary server in the working area and click **Edit Tape Server** on the ribbon. You can also right-click the necessary server in working area and select **Properties**.
4. Then edit the tape server settings as required.

Rescanning Tape Servers

In order to update the list of managed tape devices, Veeam Backup Free Edition automatically rescans the tape servers every 3 minutes. You can perform manual rescan of a tape server, for example, if you want to implement the changes made to the tape infrastructure immediately.

To rescan a tape server:

1. Open the **Tape Infrastructure** view.
2. To rescan all tape servers, right-click the **Servers** node and select **Rescan**.
3. To rescan a particular tape server, select the **Servers** node in the inventory pane. Select the necessary server in the working area and click **Rescan** on the ribbon. You can also right-click the necessary server in working area and select **Rescan**.

Updating Tape Servers

Every time you launch Veeam Backup Free Edition, it automatically checks if the components installed on managed servers are up to date. You will be unable to work with tape libraries that are connected to the outdated servers.

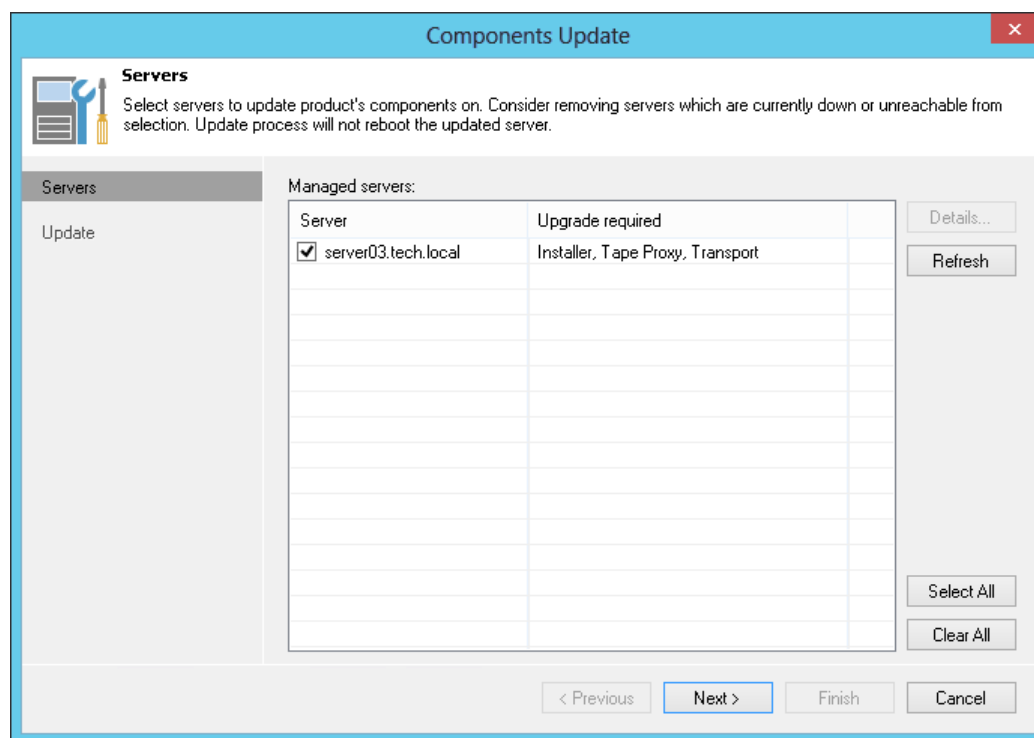
If there is a later version of a component available (usually, if you have upgraded Veeam Backup Free Edition), the **Components Update** window will be displayed, prompting you to update components on managed tape servers.

You can also open the **Components Update** window by doing one of the following:

- Open the main menu and select **Upgrade** from the main menu.
- Open the **Tape Infrastructure** view, select the **Servers** node and click **Upgrade** on the ribbon.
- Open the **Tape Infrastructure** view, right-click the necessary tape server in the working area and select **Upgrade**.

If components on all managed servers are up to date, the **Upgrade** item will be disabled.

The **Components Update** section lists tape servers that have outdated components deployed. To see the current and the latest available versions for deployed components, select a server in the list and click **Details**. Select check boxes next to servers for which you want to upgrade components and click **Next**.



Removing Tape Server

To remove a tape server:

1. Open the **Tape Infrastructure** view.
2. Select the **Servers** node in the inventory pane.
3. Select the tape server in the working area and click **Remove Tape Server** on the ribbon. You can also right-click the necessary tape server in the working area and select **Remove**.

When you remove a tape server, Veeam Backup Free Edition unassigns the tape server role from it, so it is no longer used as a tape server. The actual server remains connected to Veeam Backup Free Edition.

Important! You cannot remove a tape server if any of tape jobs is running at the moment. Before you remove the tape server, stop all tape jobs.

Working with Media Pools

All tape media are divided into media pools — logical groups of tapes. There are two types of media pools in Veeam Backup Free Edition: predefined media pools and custom media pools.

Predefined media pools are **Free**, **Unrecognized**, **Imported** and **Retired** service pools created by Veeam Backup Free Edition. They cannot be modified or removed.

Custom media pools serve as targets for files to tape jobs. They provide tapes for writing new data and organize storing of the archived data according to the rules configured for them.

To be able to configure files to tape jobs, you need to first create custom media pools.

Creating Custom Media Pools

To create a custom media pool, use the **New Media Pool** wizard. This section will guide you through all steps of the wizard and provide explanation on available options.

Step 1. Launch the New Media Pool Wizard

To run the **New Media Pool** wizard, do either of the following:

- Open the **Tape Infrastructure** view and click **Add Media Pool** on the ribbon.
- Open the **Tape Infrastructure** view, right-click the **Media Pools** node and choose **Add Media Pool**.

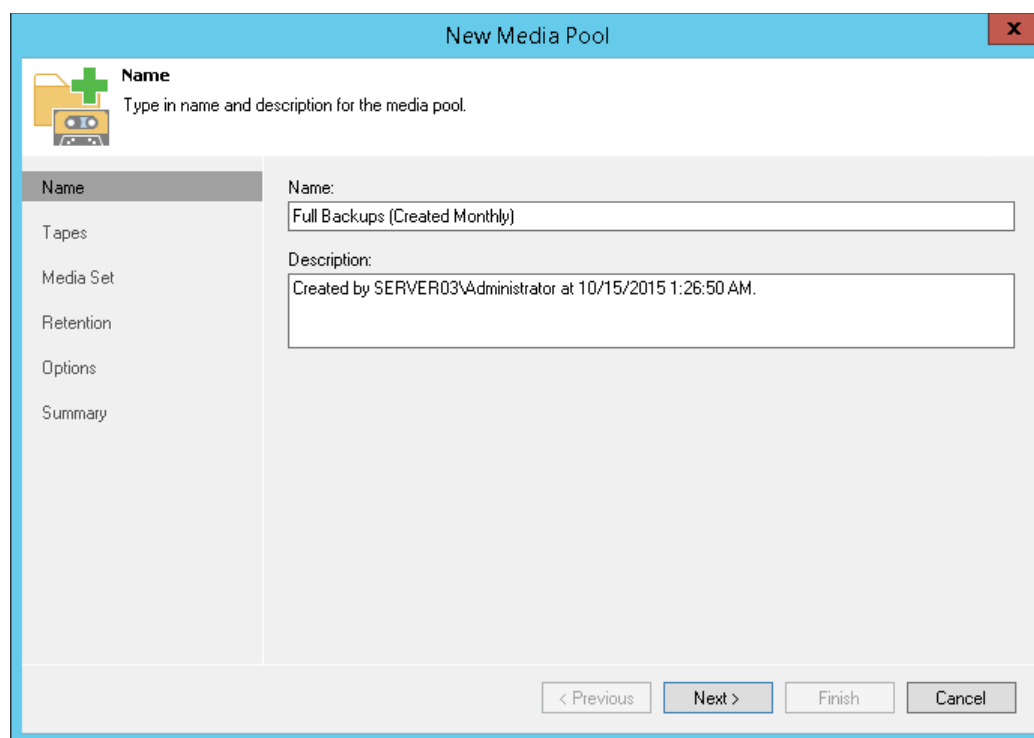
Tip:

You can also launch the **New Media Pool** wizard when configuring tape jobs (that is, directly from the **New File To Tape Job** wizard). For more details, see [Creating File to Tape Jobs](#).

Step 2. Specify Media Pool Name

At the **Name** step of the wizard, define basic description for the new media pool.

1. In the **Name** field, enter a name for the created media pool.
2. In the **Description** field, enter a description of the new media pool. The default description contains information about the user who created the media pool, date and time when the media pool was created.



New Media Pool

Name
Type in name and description for the media pool.

Name:
Full Backups (Created Monthly)

Description:
Created by SERVER03\Administrator at 10/15/2015 1:26:50 AM.

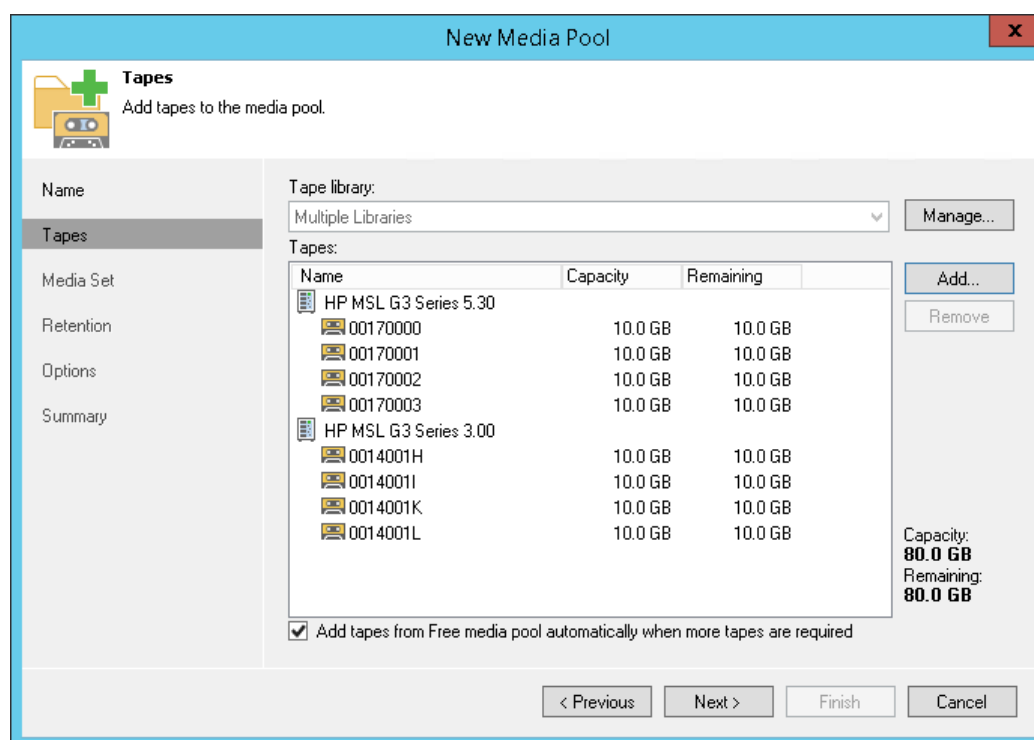
< Previous Next > Finish Cancel

Step 3. Add Tapes to Media Pool

At the **Tapes** step of the wizard, you can configure global media pool settings and allocate tapes for the pool.

1. In the **Tape library** field, select the library from which the tapes will be allocated for the media pool. The list contains the tape libraries managed by this Veeam backup server.
2. To allocate specific tapes from the library, click the **Add** in the **Tapes** field and select tapes that should be added to the media pool. Allocated tapes will be reserved for the created media pool; other custom media pools will not be able to use these tapes. The capacity and free space on the allocated tapes will be displayed in the bottom right corner.
3. To make the media pool replenishable, select the **Add tapes from Free media pool automatically when more tapes are required** check box.

With this option enabled, additional tapes will be allocated from the **Free** media pool when needed. That is, when a backup to tape or files to tape job uses all available tapes from this media pool, Veeam Backup & Replication will automatically add the required number of tapes from the **Free** media pool to let the job complete. If the option is disabled, the job will pause and prompt the backup administrator to add new tapes to the media pool.



Step 4. Specify Media Set Options

For each media pool, specify how new media sets are created. A *media set* is consequent data stream that can span several tapes (for example, a weekly backup stored on tapes). At the **Media Set** step of the wizard, specify how this data stream will be organized.

1. In the **Media set name** field, define the pattern according to which created media set(s) will be named. The default variables are `##id%` (the number of the media set) and `%date%` (the date of creation of the media set).

You can additionally use the following variables:

- `%time%` — the time of creation of the media set
- `%day%` — the day in month on which the media set is created
- `%dayofweek%` — the day of week on which the media set is created
- `%month%` — the month of creation of the media set
- `%year%` — the year of creation of the media set
- `%job%` — the name of job for which the media set is created

2. In the **Automatically create new media set** section, specify conditions for creating new media sets on tapes allocated to the media pool. The following options are available:
 - **Do not create, always continue using current media set.** If this option is selected, each subsequent backup session will write its backup set to the existing media set: it will append backup content to the content that was written to tape with a previous backup session. If, however, a backup set is started with a new tape, Veeam Backup Free Edition will create a new media set for it.
 - **Create new media set for every backup session.** If this option is selected, a new media set will be created for each new backup session. Each backup session will write its backup set starting with a new tape.
 - **Daily at.** If this option is selected, you can specify day and time when new media sets should be created. For example, if at the end of the week you send weekly media sets to offsite storage, you can schedule creation of new media sets at the beginning of each week.

New Media Pool

Media Set
Specify media set name and how often a new media set should be automatically created.

Name
Media set name:
Media set #%id% %date%

Tapes

Media Set
Automatically create new media set

☒ Do not create, always continue using current media set

☐ Create new media set for every backup session

☐ Daily at 12:00 PM Everyday Days...

< Previous Next > Finish Cancel

Step 5. Specify Retention Settings

At the **Retention** step of the wizard, specify overwrite rules for cases when all tapes allocated to the media pool are full (and there are no more free tapes available). You can select one of the following options:

- **Do not protect data (cyclically overwrite tapes as required).** If this option is selected, tapes allocated to the pool will be overwritten, starting with the tape that stores the oldest archive.
- **Protect data for (time interval).** If this option is selected, archives on tapes will be preserved for the specified period. When this period is over, data will be overwritten, starting with the tape that stores the oldest archive.

This setting must accord with the retention policy specified for the backup chain that you plan to archive to tape. The retention period for archives on tape must be greater or equal to the time interval for which restore points are kept on the backup repository. In the opposite case, with every new job cycle, Veeam Backup & Replication may write the same set of files to tape, instead of adding new ones. For example, there are 14 backup files on the backup repository that are kept for 14 days. The backup to tape job archives files once a week. The retention policy for the media pool is set to 7 days. In this case, Veeam Backup & Replication will first write 14 backup files from the backup repository to tape. After a 7-day interval, Veeam Backup & Replication will start recording the whole set of backup files from the backup repository to tape anew, overwriting backup files on tape with their copies from the backup repository.

- **Never overwrite data.** If this option is selected, data on tapes will not be overwritten. If there is not enough tape capacity for the archiving job to complete, Veeam Backup Free Edition will pause the job and prompt the backup administrator to add new tapes to the media pool.

Note: You cannot set the retention period if you have configured the media set to **Do not create, always continue using current media set** option. Tapes written in such media sets are never overwritten.

New Media Pool

Retention
Specify the tape retention settings for this media pool.

Name
Tapes
Media Set
Retention
Options
Summary

Data retention policy

- ☐ Do not protect data (cyclically overwrite tapes as required)
- ☐ Protect data for 1 Weeks
- ☒ Never overwrite data

Offline media tracking

☐ Move all offline tapes from this media pool into the following media vault:
Vault: Add New...

< Previous Next > Finish Cancel

Note that the media vaults are not available in the Veeam Backup Free Edition.

Step 6. Add Optional Media Pool Settings

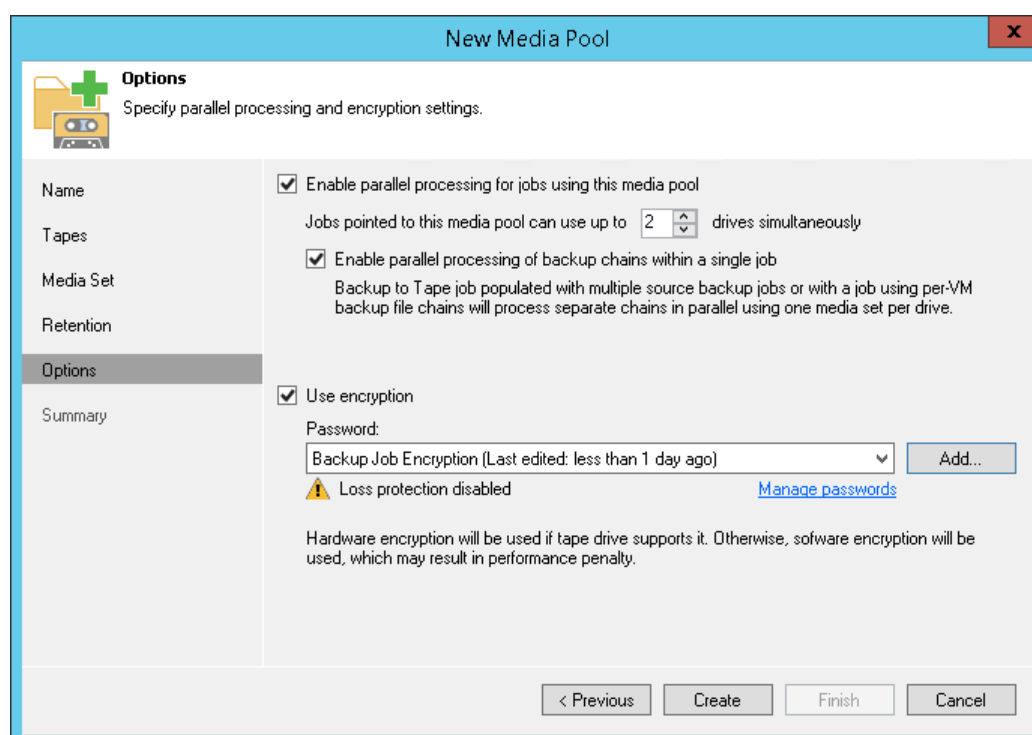
At the **Options** step of the wizard, you can enable parallel processing and encryption.

1. Select the **Enable parallel processing for jobs using this media pool** check box if you want to process multiple tape jobs simultaneously. Set the maximum number of drives that the media pool can use in parallel.

If your source repository is set to per-VM backup files, you can process multiple source VM backup chains within the tape job simultaneously. Select the **Enable parallel processing of backup chains within a single job** check box to split the source VM chains across multiple drives.

2. To enable encryption, select the **Use encryption** check box. This option allows you to encrypt the content of files or backups archived to tapes in the media pool.

From the **Password** field, select a password you want to use to encrypt files archived to tape. You can also click **Add** or use the **Manage passwords** link to add a password.



The screenshot shows the 'New Media Pool' wizard at the 'Options' step. The window title is 'New Media Pool'. On the left is a sidebar with icons and labels: 'Name', 'Tapes', 'Media Set', 'Retention', 'Options' (highlighted), and 'Summary'. The main area is titled 'Options' with a subtitle 'Specify parallel processing and encryption settings.' and a folder icon. It contains three sections of settings:

- Parallel Processing:** A checked checkbox 'Enable parallel processing for jobs using this media pool'. Below it, a text field shows 'Jobs pointed to this media pool can use up to 2 drives simultaneously'.
- Parallel Processing of Backup Chains:** A checked checkbox 'Enable parallel processing of backup chains within a single job'. Below it, a text field explains: 'Backup to Tape job populated with multiple source backup jobs or with a job using per-VM backup file chains will process separate chains in parallel using one media set per drive.'
- Encryption:** A checked checkbox 'Use encryption'. Below it, a 'Password:' label is followed by a dropdown menu showing 'Backup Job Encryption (Last edited: less than 1 day ago)' and an 'Add...' button. Below the dropdown is a warning icon and text: 'Loss protection disabled' with a link to 'Manage passwords'.

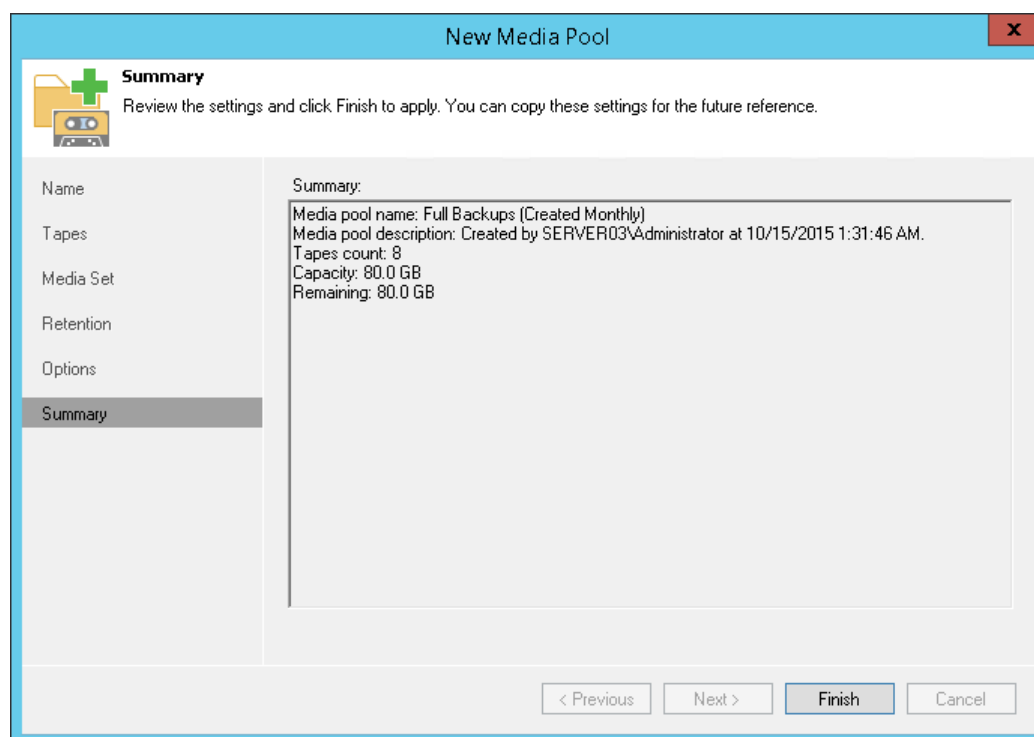
At the bottom of the main area, a text block states: 'Hardware encryption will be used if tape drive supports it. Otherwise, software encryption will be used, which may result in performance penalty.'

At the bottom of the window are four buttons: '< Previous', 'Create', 'Finish', and 'Cancel'.

Step 7. Finish Working with the Wizard

Review the media pool settings and click **Finish** to complete the wizard.

A new media pool will be available under the **Tape Infrastructure > Media Pools** node in the **Tape Infrastructure** view.



Modifying Media Pools

If necessary, you can modify settings of a media pool. Note that you can only change custom media pools; predefined media pools cannot be modified.

To modify media pool settings:

1. Open the **Tape Infrastructure** view.
2. Right-click the necessary media pool and choose **Properties**. Alternatively, select a media pool and click **Edit Media Pool** on the ribbon.
3. Go through the **Edit Media Pool** wizard to change the necessary settings.
4. Apply changes.

Removing Media Pools

If you no longer need a media pool, you can remove it:

1. Open the **Tape Infrastructure** view.
2. Right-click the necessary media pool and choose **Remove Media Pool** from the shortcut menu. Alternatively, select a media pool and click **Remove Media Pool** on the ribbon.
3. In the displayed dialog box, click **OK** to confirm deletion.

When you delete a media pool, its tapes are moved to the **Imported** media pool. Note that unlike other move operations, the data is not erased. You can use the tapes in the **Imported** media pool for restore operations.

Mind the following limitations:

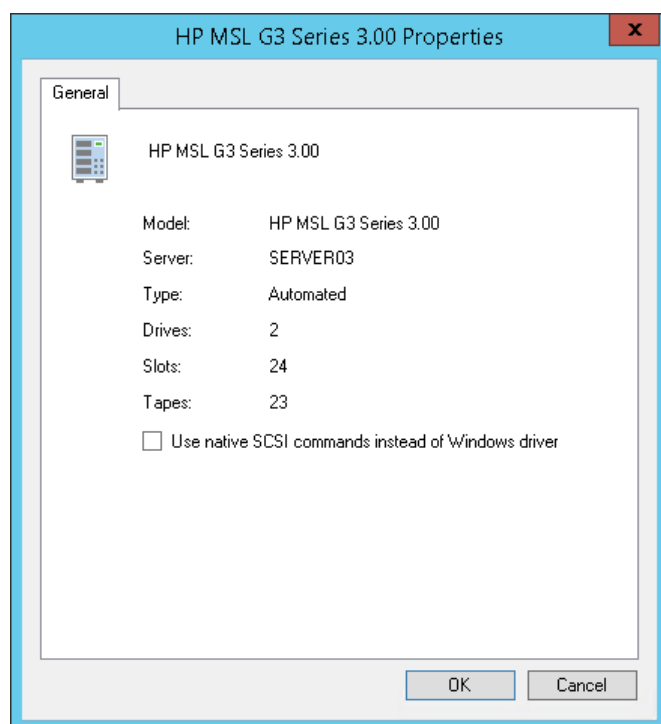
- You can only remove custom media pools; predefined media pools cannot be removed.
- You cannot remove a media pool that is used in a files to tape job. To be able to remove such a pool, first point corresponding jobs to other custom media pools.

Working with Tape Libraries

All tape libraries managed by Veeam Backup Free Edition are shown as a list of devices under the **Libraries** node in the **Tape Infrastructure** view. All connected devices are discovered automatically during the rescan procedure. When you add a new tape device to the tape server, it appears in your console after rescan.

To view properties of a tape library, open the **Tape Infrastructure** view, expand the **Libraries** node and select the needed library. Click **Properties** on the ribbon. You can also right-click the necessary library in the working area and select **Properties**.

Select the **Use native SCSI commands instead of Windows driver** check box if your library is an unknown media changer. For more information about unknown media changers, see Supported Devices.



Rescanning Tape Libraries

You can rescan a selected to update its network status.

To rescan a tape library:

1. Open the **Tape Infrastructure** view.
2. Select the **Libraries** node in the inventory pane. Select a necessary library in the working area and click **Rescan Library** on the ribbon. You can also right-click the necessary library in the working area and select **Rescan**.

Renaming Tape Libraries

The Veeam backup console shows the list of all tape devices as a list of libraries. By default, the connected libraries are shown with their production model names. For clearer visibility, you can rename them.

To rename a tape library:

1. Open the **Tape Infrastructure** view.
2. Select the **Libraries** node in the inventory pane. Select a necessary library in the working area and click **Rename Library** on the ribbon. You can also right-click the necessary library in the working area and select **Rename**.

Removing Tape Libraries

If you want to stop using a tape device, you can remove it from your Veeam backup console.

Only the libraries in the offline status can be removed. To remove a tape library, you need to physically disconnect it from the tape server first. Alternatively, you can remove the tape server to which the tape library is connected. Otherwise, the tape library will be discovered during the next rescan and reappear in the **Libraries** list.

If the tape library is added to a global media pool, the tape jobs will be automatically redirected to the next tape library in the list. If the tape library is the only one in the media pool, first redirect the jobs to other media pools manually.

Tip:

If you remove the tape server, the tape devices remain connected to it. You can connect the tape server back to your console. In this case, Veeam Backup Free Edition will recognize all tape devices that were previously added to it with tapes and media pools (in case they remain in the Veeam database). You can also connect the tape server to another Veeam backup server. Veeam Backup Free Edition will recognize the tape devices automatically, however you will need to create the media pools anew.

To remove a tape library:

1. Disconnect the tape library or the tape server.
2. Open the **Tape Infrastructure** view.
3. Select the **Libraries** node in the inventory pane. Select a necessary library in the working area and click **Remove Library** on the ribbon. You can also right-click the necessary library in the working area and select **Remove Library**.
4. In the displayed dialog box, click **OK** to confirm deletion.

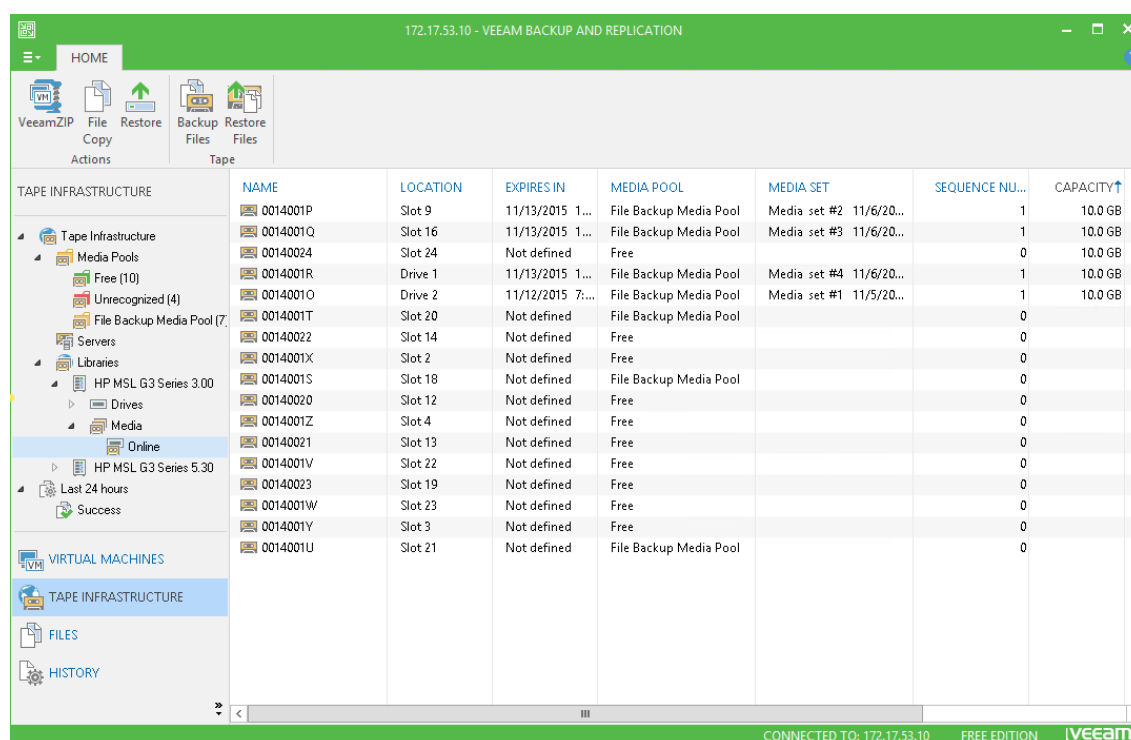
Working with Tapes

All tapes managed by Veeam Backup Free Edition belong to one of media pools. Generally, the new tapes are in the **Free** media pool. Tapes that were written in some custom media pools stay tied to their media pools.

If you offload tapes from you tape device, their status changes to Offline, but they stay visible in the console.

Tape media in Veeam Backup Free Edition are displayed in the **Tape Infrastructure** view, either under the **Media Pools** or under the **Libraries > LibraryName node > Media > Online/Offline**. You can work with both online and offline tapes:

- Tapes that are currently loaded to the tape device are available under the **Online** node.
- Tapes that have been unloaded from the tape device are shown under the **Offline** node.



NAME	LOCATION	EXPIRES IN	MEDIA POOL	MEDIA SET	SEQUENCE NU...	CAPACITY
0014001P	Slot 9	11/13/2015 1...	File Backup Media Pool	Media set #2 11/6/20...	1	10.0 GB
0014001Q	Slot 16	11/13/2015 1...	File Backup Media Pool	Media set #3 11/6/20...	1	10.0 GB
00140024	Slot 24	Not defined	Free		0	10.0 GB
0014001R	Drive 1	11/13/2015 1...	File Backup Media Pool	Media set #4 11/6/20...	1	10.0 GB
0014001O	Drive 2	11/12/2015 7:...	File Backup Media Pool	Media set #1 11/5/20...	1	10.0 GB
0014001T	Slot 20	Not defined	File Backup Media Pool		0	
00140022	Slot 14	Not defined	Free		0	
0014001X	Slot 2	Not defined	Free		0	
0014001S	Slot 18	Not defined	File Backup Media Pool		0	
00140020	Slot 12	Not defined	Free		0	
0014001Z	Slot 4	Not defined	Free		0	
00140021	Slot 13	Not defined	Free		0	
0014001V	Slot 22	Not defined	Free		0	
00140023	Slot 19	Not defined	Free		0	
0014001W	Slot 23	Not defined	Free		0	
0014001Y	Slot 3	Not defined	Free		0	
0014001U	Slot 21	Not defined	File Backup Media Pool		0	

All tapes are grouped to predefined and custom media pools available under the **Tape Infrastructure > Media Pools** node.

Veeam Backup Free Edition can use only online tapes for files to tape jobs.

If you work with a standalone tape drive and all its tapes are offline, Veeam Backup Free Edition will display a message informing that you need to insert a tape into the drive. At the same time, Veeam Backup Free Edition will hint what tape has been recently used for archiving.

You can insert any tape into the tape drive:

- If the tape you have inserted is registered in the Veeam backup database and the current media set can still be used, Veeam Backup Free Edition will continue writing to this media set and append the new content to the content recently written on the tape.
- If the tape you have inserted is not registered in the Veeam backup database, it will be processed as follows:
 - A new empty tape will be placed to the **Free** media pool and used for writing data.
 - A tape containing any data written on another Veeam backup server or with another tape backup solution will be placed to the **Unrecognized** media pool. You need to perform catalogization for such tapes.

Importing Tapes

When you need to load free tapes, or if you need to restore data from tapes, you need to load these tapes into your tape device and import them. Importing is recognizing tapes that are loaded into your tape device.

When you load tapes into the mail slot, they are not visible in the Veeam backup console. To start using tapes, you need to introduce them to the Veeam Backup Free Edition by running the importing procedure. The importing procedure conveys the tapes from the mail slot to the library working slots, scans them and sends information about them to Veeam backup database. After importing, Veeam Backup Free Edition can use the tapes to read or write data.

Importing must be performed manually each time you load tapes into your tape device.

To import a tape:

1. Open the **Tape Infrastructure** view.
2. Select the tape library node under the **Libraries** node and click **Import Tapes** on the ribbon. Alternatively, you can right-click the tape library node and select **Import Tapes** from the shortcut menu.

Importing runs differently for tapes that are registered in the local Veeam backup database and those that are not. Choose an appropriate procedure for the following tapes:

- [Importing empty tapes](#)
- [Importing tapes written on this backup server](#)
- [Importing tapes written on another Veeam server](#)

Importing Empty Tapes

To import new tapes, follow the next steps:

1. Insert the tapes into the tape device.
2. Open the **Tape Infrastructure** view, expand the **Libraries** node and select the library to which you have loaded the tapes. Click **Import Tapes** on the ribbon. You can also right-click the necessary library in the working area and select **Import Tapes**.
3. The tapes will appear in the **Unrecognized** media pool.
4. Right-click the tapes and select **Inventory tape**.
5. The tapes will be moved to the **Free** media pool.

Tapes can be used for automatic or manual replenishment of custom media pools. They can be further used to replenish custom media pools:

- Automatically, if the media pools are configured for automatic replenishment.
- Manually by moving tapes from the **Free** media pool to particular custom media pools.

If you want to refill the free tape resources in your tape device, you can overwrite tapes containing outdated Veeam archives. For more information, see [Importing Tapes Written on This Backup Server](#).

Tip:

To understand which of the tapes can be overwritten, you can check their expiration date. In the **Tape Infrastructure** view, open the **Media Pools** node and select the media pool that you want to replenish. Check the **Expires in** field in the working area. You can sort the tapes by the expiration date and get the list of tapes that can be reused.

Importing Tapes Written on This Backup Server

If the tapes that you want to import were written on the same Veeam backup server, the Veeam backup database has information about them.

- When you import tapes written on a tape library with a barcode reader and information about these tapes is available in the Veeam Backup Free Edition database, Veeam Backup Free Edition immediately recognizes these tapes after importing. You will be able to view data written to these tapes and run restore procedures.
- When you import tapes written on a tape library without a barcode reader, you need to additionally inventory these tapes to be able to work with them.

To import tapes without barcode labels:

1. Insert the tapes into the tape device.
2. Open the **Tape Infrastructure** view, expand the **Libraries** node and select the library to which you have loaded the tapes. Click **Import Tapes** on the ribbon. You can also right-click the necessary library in the working area and select **Import Tapes**.
3. The tapes will appear in the **Unrecognized** media pool.
4. Right-click the tapes you need and select **Inventory Tape**.
5. The tapes will be moved to the media pools in which they were originally written.

You can view the data written on these tapes and run restore procedures.

Note that if the tapes have expired, they will be overwritten by tape rotation scheme set for this media pool.

Importing Tapes Written on Another Veeam Server

Veeam Backup Free Edition supports restoring data from tapes that were recorded on another Veeam backup server. To read data from such tapes, Veeam Backup Free Edition must first scan the tapes and store the information about them to the Veeam backup database.

To import tapes, follow the next steps:

1. Insert the tapes into the tape device.
2. Open the **Tape Infrastructure** view, expand the **Libraries** node and select the library to which you have loaded the tapes. Click **Import Tapes** on the ribbon. You can also right-click the necessary library in the working area and select **Import Tapes**.
3. The tapes will appear in the **Unrecognized** media pool.
4. Right-click the tapes you want to import and select **Catalog Tape**.
5. The tapes will be moved to the **Imported** media pool. The **Imported** media pool will be created automatically. When the tapes are imported, you can view and restore data written to them.

Inventorying Tapes

When you load new tapes in your tape device for the first time, these tapes are presented to Veeam Backup Free Edition as **Unrecognized**. To identify unrecognized tapes, you need to run tape inventory job against them.

Tape inventory job is a relatively fast process of reading metadata written on tape with the aim of detecting name of the media set and the sequence number for the tape. Tape inventory jobs helps Veeam Backup Free Edition identify empty tapes and detect non-empty tapes belonging to specific media set.

You can perform tape inventory for a whole tape library or run the job against selected tapes only.

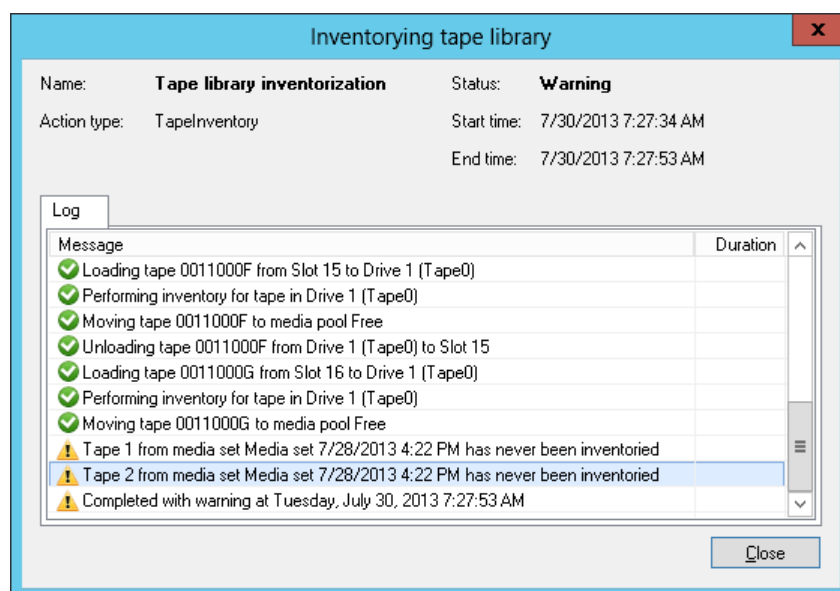
To start tape inventory for a whole tape library:

1. Open the **Tape Infrastructure** view.
2. Expand the **Libraries** node and select the library you want to inventory.
3. Click **Inventory Library** on the ribbon. Alternatively, you can right-click the tape library and select **Inventory Library** from the shortcut menu. Veeam Backup Free Edition will perform inventory for all online tapes in the library.

To start tape inventory for selected tapes:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media**.
3. Select the necessary tapes in the list and click **Inventory** on the ribbon. Alternatively, you can right-click the selected tapes and choose **Inventory Tape**.

The inventory log will display job session results. To access the inventory session details, you can open the **History** view and locate the necessary session under the **Jobs > Tape** node.



As a result of inventory, Veeam Backup Free Edition places tapes in predefined pools:

- Empty tapes are moved to the **Free** pool. You can use these tapes for archiving backups and files
- Tapes that contain data written on another Veeam backup server remain in the **Unrecognized** pool. Veeam Backup Free Edition displays the detected media set name and sequence number for these tapes. If you want to restore data from a specific media set, you need to run the tape catalog job for all tapes in this media set.

After the tapes are inventoried, you can decide on further steps: for example, you can mark unrecognized tapes as free if you do not need archived content, or allocate tapes from the **Free** pool to a custom pool.

Cataloging Tapes

Cataloging tapes is required for tapes that contain some data but are not registered in the Veeam database. For example, cataloging is required for tapes that were written on another Veeam backup server. After the cataloging procedure, you can restore data from the tapes.

When a catalog job is performed, Veeam Backup Free Edition first performs tape inventory, reads the information about backup contents on tape from the on tape catalog information, scans tape contents and updates the database with details of new detected backup sets.

You can perform tape catalog job for a whole tape library or for selected tapes.

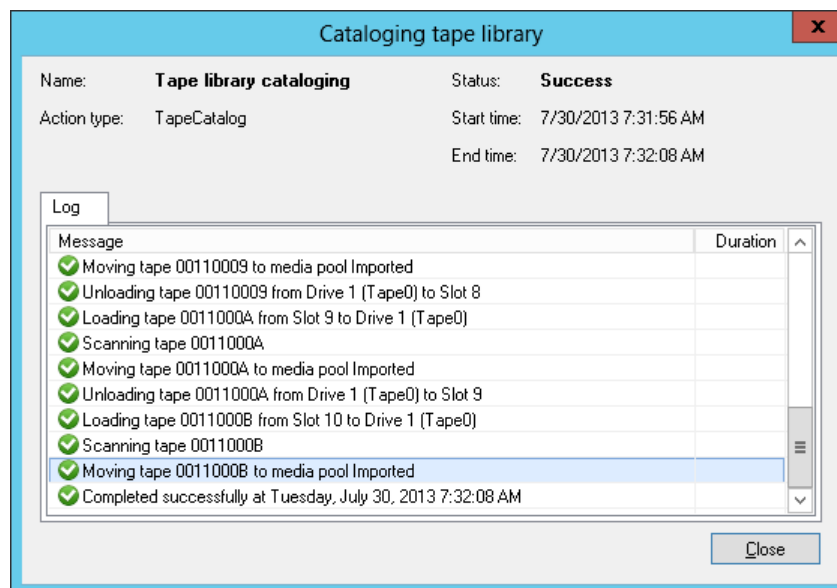
To catalog a whole tape library:

1. Open the **Tape Infrastructure** view.
2. Open the **Tape Infrastructure** view, expand the **Libraries** node and select the library you want to catalog. Click **Catalog Library** on the ribbon. Alternatively, you can right-click the tape library and select **Catalog Library**.

To catalog selected tapes:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media**.
3. Select the necessary tapes in the list and click **Catalog** on the ribbon. Alternatively, you can right-click the selected tapes and choose **Catalog Tape**.

The catalog log will display job session results. To access the catalog session details, you can open the **History** view and locate the necessary session under the **Jobs > Tape** node.



Rescanning of tapes during the catalog job may take a lot of time. To speed up the catalogization process, you might do one of the following:

- First, run inventory job to identify tape media sets and decide which tapes should be included in catalogization process. Run the catalog job only against tapes in the necessary media set.
- If you work with a tape library, you can run the catalog job against the whole media set at once.
- If you work with a standalone drive, start catalogization from the last tape in the media set (as this tape usually stores on tape catalog information).

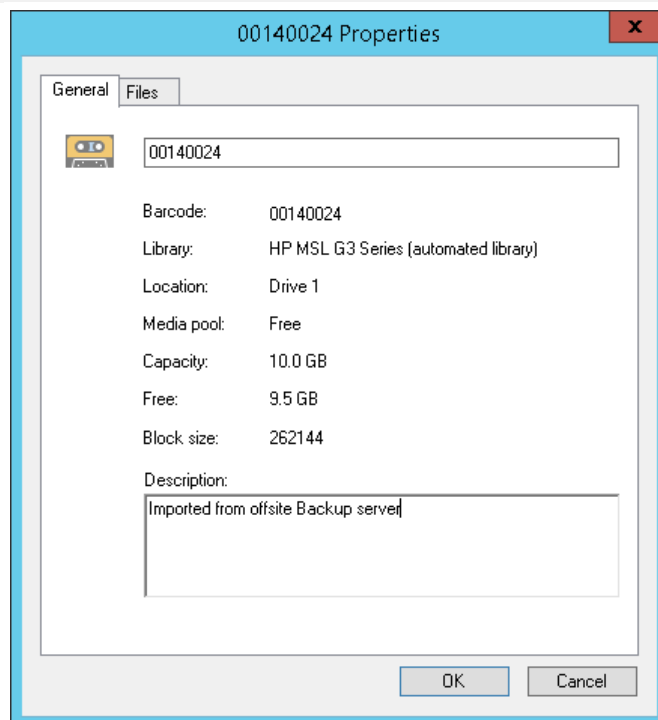
Identifying Tapes

When performing periodic auto-rescan, Veeam Backup Free Edition reads barcodes on tapes. If a tape is identified with a barcode, the barcode is displayed as the **Name** property of the tape. If a tape does not have a barcode, Veeam Backup Free Edition will automatically create the tape name using the pattern 'Tape N'.

If necessary, you can change the name of a tape:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries** > *LibraryName* node > **Media** > **Online/Offline**.
3. Select the tape you want to rename and click **Properties** on the ribbon. Alternatively, you can right-click the tape and choose **Properties**.
4. Change tape name and description as required.
5. Click **OK** to save changes.

Note: If you manage several tape libraries on the same Veeam backup server and use barcodes to identify tapes in these libraries, make sure that all barcodes are unique. If some tapes have identical barcodes, Veeam Backup Free Edition may fail to manage them correctly.



Removing Tapes from Catalog

If you do not want to store information about a tape and contents on this tape in Veeam Backup Free Edition database, you can remove the tape from the catalog. Removing from catalog can be performed for offline tapes. For example, you can perform removal from catalog if a physical tape no longer exists, and the tape should no longer be displayed among media in the Veeam Backup Free Edition console.

You can remove only tapes that are offline.

To remove one or more tapes from the catalog:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Offline**.
3. Select offline tapes you want to remove from the catalog and click **Remove from Catalog** on the ribbon. Alternatively, you can right-click selected tapes and choose **Remove from Catalog** from the shortcut menu.
4. In the opened dialog box, click **Yes** to confirm removal.

Important! You cannot remove protected tapes from the catalog. To remove such tapes, you need to switch the protection off first.

Moving Tapes to a Custom Media Pool

Veeam Backup Free Edition allows you to move tapes between custom pools. You can also move tapes from any pool to the **Free** media pool.

Important! When you move a tape to any media pool, Veeam Backup Free Edition marks this tape as free.

To move tapes from one custom media pool to another:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Online**.
3. Select tapes you want to move and click **Move to** on the ribbon. Choose the target media pool from the list.
Alternatively, you can right-click selected tapes and choose **Move to Media Pool**. Next, choose the target media pool from the list.

Note: You cannot move tapes that are protected. To move such tapes, you need to switch the protection off first.

Erasing Tapes

If you do not need contents stored on tape, you can erase tapes. Veeam Backup Free Edition supports two options for erasing data:

- **Short erase (fast)** — use this option to speed up the erase process. The short erase operation does not physically erase data written on the tape. It simply loads the tape to the drive and wipes the tape header. Note that short erase is not supported by some tape devices.
- **Long erase (slow)** – use this option to clear all data written to tape. The long erase operation loads the tape to the drive, rewinds the tape and physically erases all data written to the tape.

To erase tapes:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Online**.
3. Select tapes you want to erase and click **Erase** on the ribbon. Choose the type of erase and click **OK**.
Alternatively, you can right-click selected tapes and choose **Erase Tape**. Next, choose how the tape should be erased and click **OK**.

Important! You cannot erase protected tapes. To erase such tapes, you need to switch the protection off first.

Marking Tapes as Free

Instead of erasing tapes, you can mark tapes as free. During this operation, Veeam Backup Free Edition deletes from backup and tape catalogs information about backup contents stored on tape. Data written to tape remains intact.

To mark tapes as free:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Online**.
3. Select tapes you want to mark as free and click **Mark as Free** on the ribbon.
Alternatively, you can right-click selected tapes and choose **Mark as Free** from the shortcut menu.
4. In the displayed dialog box, click **Yes**.

After a tape is marked as free, Veeam Backup Free Edition removes from the catalog information about contents on this tape.

Important! You cannot mark protected tapes as free. To mark such tapes as free, you need to switch the protection off first.

Protecting Tapes

If you have a number of tapes for which you need to change the retention to 'never overwrite', you can protect them. Protection option sets lifelong retention period for the selected tapes overriding the retention settings of the media pool.

You can set protection for both online or offline tapes that contain data.

If the tapes are protected, they cannot be erased or marked as free by Veeam Backup Free Edition or manually. To erase such tape, you need to switch the protection off first.

The protection can be switched off at any time. The retention settings will be changed to the value set for the media pool.

To enable protection:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Online**.
3. Select tapes you want to protect and click **Protect** on the ribbon.
Alternatively, you can right-click selected tapes and choose **Protect** from the shortcut menu.

Important! You cannot protect free tapes, that is, tapes that do not have any data written on them.

Ejecting Tapes

Ejecting moves the tape that is currently in drive to a library slot. The tape stays in the library and is online. Ejecting prevents tapes, for example, from being occasionally overwritten.

You can select a tape to eject, or select a drive and eject the tape from it. Eject command is enabled only for tapes that are in drives or for drives with loaded tapes.

To eject a tape from a drive:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Online**.
3. Select a tape located in drive that you want to eject and click **Eject** on the ribbon.
Alternatively, you can right-click selected tape and choose **Eject Tape**.

To eject a tape from a drive:

1. Open the **Tape Infrastructure** view.
2. Navigate to the **Libraries > LibraryName** node > **Drives**.
3. Select a drive from where you want to eject the tape and click **Eject Tape** on the ribbon.
Alternatively, you can right-click selected tape and choose **Eject**.

Tip: You can also instruct a tape job to eject tape from drive after the job completes. To do so, navigate to the **Options** step of backup to tape job or file to tape job and select the **Eject media once the job finishes** check box.

Exporting Tapes

If you want to offload tapes, you need to export them first. Exporting moves the tape from the standard slot in the tape library to the I/E slot (or Mail slot). When they are in the I/E slot, you can take them from the library and, for example, carry to a storing location.

To export a tape to an I/E slot:

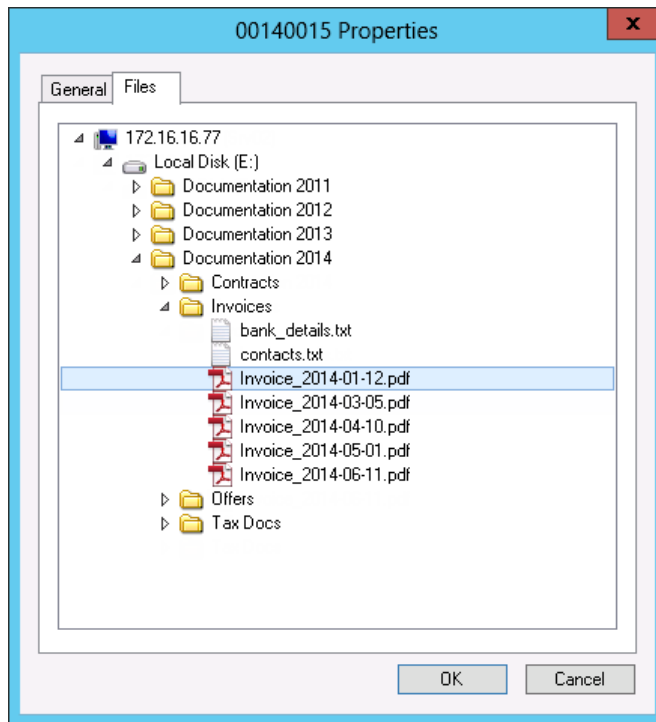
1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Online**.
3. Select a tape you want to export and click **Export** on the ribbon.
Alternatively, you can right-click selected tape and choose **Export Tape** from the shortcut menu.

Note: Export is available only for the devices that support corresponding operations and include I/E slot.

Viewing Data on Tapes

To view data contents that is currently stored on tape:

1. Open the **Tape Infrastructure** view.
2. Navigate to the list of tapes either under the **Media Pools** or under the **Libraries > LibraryName** node > **Media > Online**.
3. Select the necessary tape and click **Properties** on the ribbon. Alternatively, you can right-click the tape and choose **Properties**.
4. Open the **Files** tab.



Tapes Availability and Write-Protection

Before archiving data to tape media, Veeam Backup Free Edition detects available tapes in the target media pool. Unavailable tapes are filtered out and are not used for writing data. A tape may be unavailable for one of the following reasons:

- The tape cannot be used according to the retention policy set for the media pool.
- The tape is offline.
- The tape has the write-protect switch set.

If your tape is write-protected and you want to write data to this tape, you must eject the tape from the drive and drag the write protection switch off. After you insert the tape back to the drive, you must inventory the tape to mark it as writable in the Veeam Backup Free Edition database.

Creating File to Tape Jobs

To write files to tape, you should create a file to tape job using the **New File To Tape Job** wizard. This section will guide you through all steps of the wizard and provide explanation on available options.

To create a file to tape job, follow the next steps:

Step 1. Launch the New File To Tape Job Wizard

To run the **New File to Tape Job** wizard, do either of the following:

- On the **Home** tab, click **Backup Files**.
- Open the **Files** view, right-click the **Jobs** node and select **Tape Job > Files to Tape**.

Alternatively, you can:

- Open the **Files** view, browse to the necessary files, select the files and choose **Add to Tape Job > New job** from the ribbon menu.
- Open the **Files** view, browse to the required files, right-click the necessary files and choose **Add to Tape Job > New job**.

Step 2. Specify Job Name and Description

At the **Name** step of the wizard, you should define basic settings for the created files to tape job.

1. In the **Name** field, enter a name for the created job.
2. In the **Description** field, enter a description of the created job. The default description contains information about the user who created the job, date and time when the job was created.

New File to Tape Job

Name
Type in a name and description for this job. File to tape job performs scheduled backup of selected files to tape.

Name:
Payroll Reports to Tape (Q1-Q2)

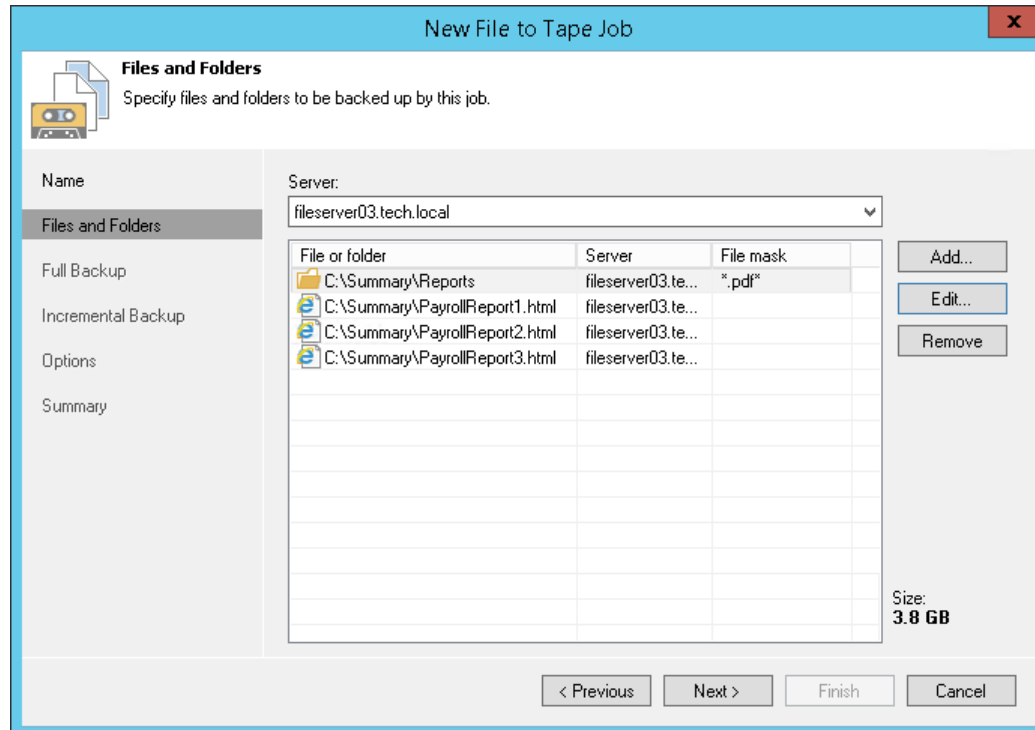
Description:
Created by TECH\Administrator at 11/6/2015 2:52 PM.

< Previous Next > Finish Cancel

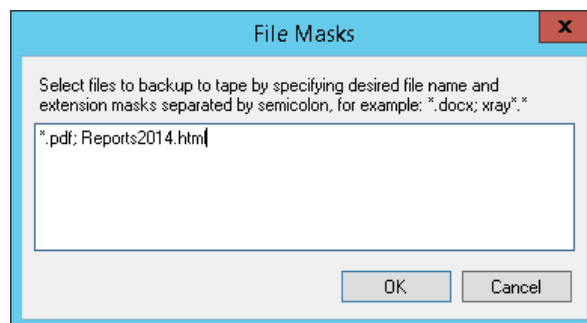
Step 3. Choose Files and Folders to Archive

At the **Files and Folders** step of the wizard, select files and folders that you want to back up.

From the **Server** list, choose a machine on which the necessary files or folders reside. Click **Add** and browse to the file or folder that you want to back up. The selected item will be added to the list. To remove a file or folder from the list, select it and click **Remove**.



If you include a folder to the job, all of the folder contents will be archived. If necessary, you can choose only specific files from the included folder. To do so, select a folder in the list and click **Edit**. In the **File Masks** window, specify names of files in the folder that should be archived. You can use exact file names or create name masks (for example, *.evt or *.pdf). Separate file names and masks with semicolons.



Step 4. Choose Media Pool for Full Backup

At the **Full Backup** step of the wizard, choose a media pool that will be used for archiving full backups of the selected files and create a schedule for full file backups.

1. From the **Media pool for full backups** list, choose a media pool that will be used for full file backups.
2. To schedule periodic creation of full file backups, select the **Run the full backup automatically** check box and specify the schedule according to which the job will create full file backups. If this option is disabled, you will need to start the job manually to create full backups of files.

Tip: If you have not previously created a media pool with the required settings, you can click the **Add New** button and create a new media pool without closing the job wizard. For more details, see [Creating Custom Media Pools](#).

New File to Tape Job

Full Backup
Choose media pool and set schedule for full backups.

Name
Files and Folders
Full Backup
Incremental Backup
Options
Summary

Media pool for full backups:
File Backup Media Pool (HP MSL G3 Series 3.00) Add New...

Tapes: 7
Capacity: 70.0 GB
Remaining: 70.0 GB

☒ Run the full backup automatically

☒ Daily at this time: 6:00 PM On these days Days...
☐ Monthly at this time: 10:00 PM Fourth Saturday Months...

< Previous Next > Finish Cancel

Step 5. Specify Media Pool for Increments

At the **Incremental Backup** step of the wizard, choose a media pool that will be used for archiving incremental backups of the selected files and create a schedule for incremental file backups.

1. From the **Media pool for incremental backup** list, choose a media pool that will be used for incremental file backups.
2. To schedule periodic creation of incremental file backups, select the **Run incremental backup automatically** check box and specify the schedule according to which the job will create incremental file backups. If this option is disabled, you will need to start the job manually to create incremental backups of files.

Tip: If you have not previously created a media pool with the required settings, you can click the **Add New** button and create a new media pool without closing the job wizard. For more details, see [Creating Custom Media Pools](#).

The screenshot shows the 'New File to Tape Job' wizard window. The title bar reads 'New File to Tape Job'. The main window has a blue header with the title and a close button. Below the header is a sidebar with a tree view containing 'Name', 'Files and Folders', 'Full Backup', 'Incremental Backup' (selected), 'Options', and 'Summary'. The main area is titled 'Incremental Backup' and contains the instruction 'Choose media pool and set schedule for incremental backups.'.

Media pool for incremental backup:
File Backup Media Pool (HP MSL G3 Series 3.00) [Add New...]

Tapes: 7
Capacity: 70.0 GB
Remaining: 70.0 GB

☒ Run incremental backup automatically

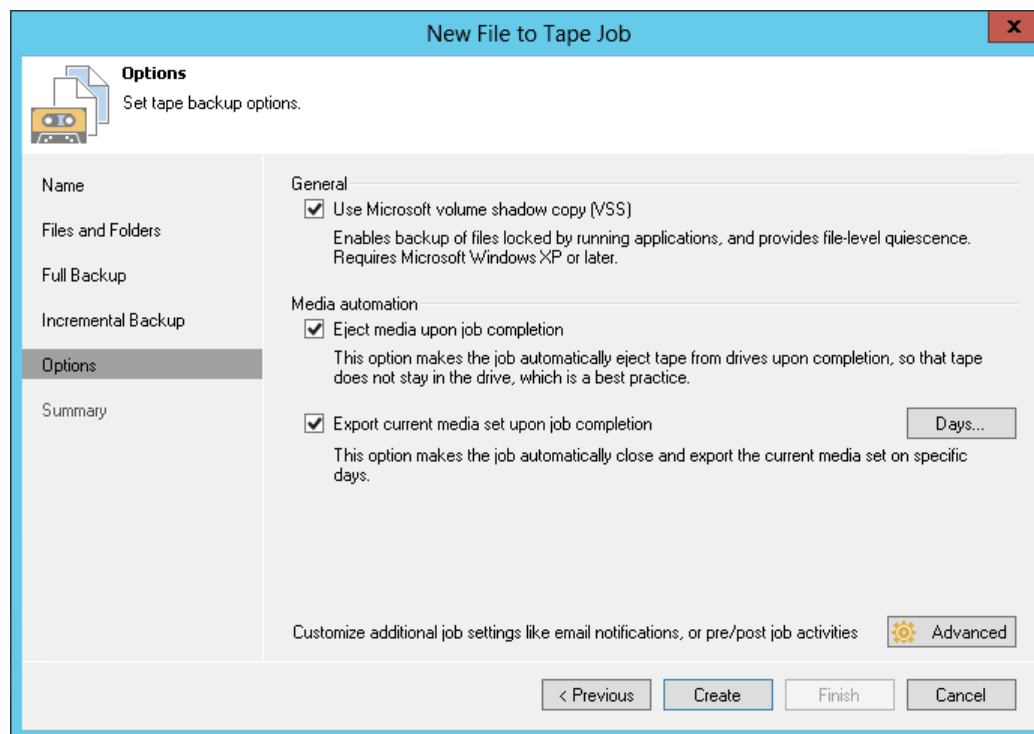
☒ Daily at this time: 4:00 AM [On week-days] [Days...]
☐ Monthly at this time: 10:00 PM [Fourth] [Saturday] [Months...]

< Previous Next > Finish Cancel

Step 6. Specify Archiving Options

At the **Options** step of the wizard, specify archiving and media automation options:

1. Select the **Use Microsoft volume shadow copy (VSS)** check box to enable backup of files with the help of Microsoft shadow volume copies. This option enables backup of files locked by application and provides file-level quiescence. This possibility can only be applied for files from servers running under Windows Server 2003 or later Windows-family OSs.
2. Select the **Eject media upon job completion** check box if the tape should be automatically ejected from the tape drive and placed into a slot when the job finishes.
3. Select the **Export current media set upon job completion** check box if the tapes belonging to the media set should be placed to Import/Export (Mail) slot for further export (for example, for export to a remote office). If you want to export tapes on specific days only (for example, every Saturday, when a backup to tape job completes), click **Days** and schedule export on the necessary days).



Step 7. Specify Advanced Job Settings

You can specify the following advanced settings for the files to tape job:

- **Notifications Settings**
- **Advanced Settings**

Tip: After you specify necessary settings for the files to tape job, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new files to tape job, Veeam Backup Free Edition will automatically apply default settings to the new job.

Notifications Settings

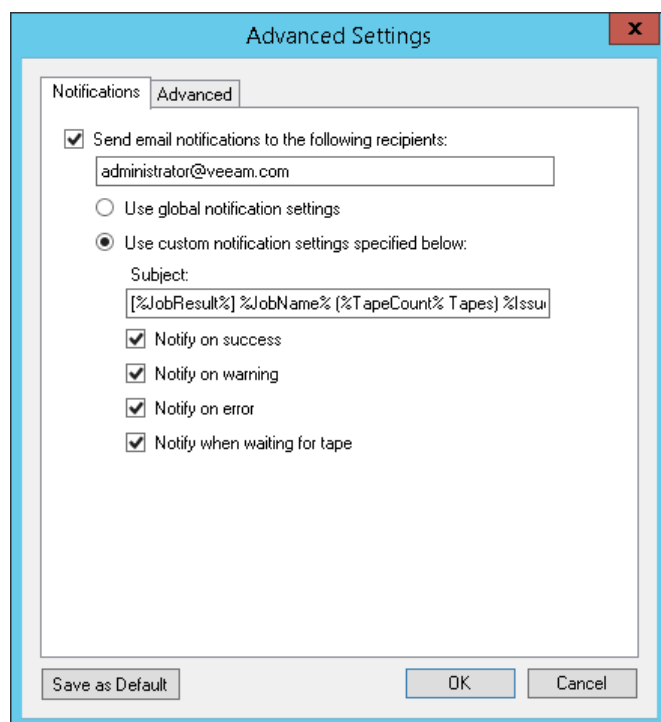
At the **Notifications** tab, you can specify notification settings for the files to tape job.

At the **Options** step of the wizard, click **Advanced**. Select the **Notifications** tab.

1. Select the **Send email notifications to the following recipients** check box if you want to receive notifications by email in case of job failure or success. In the field below, specify a recipient's email address. You can enter several addresses separated by a semicolon.

Email notifications will be sent if you configure general email notification settings in Veeam Backup Free Edition.

2. You can choose to use global notification settings or specify custom notification settings.
 - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup Free Edition will apply to the job global email notification settings specified for the Veeam backup server.
 - To configure a custom notification for a job, select **Use custom notification settings**. You can specify the following notification settings:
 - i. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: `%Time%` (completion time), `%JobName%`, `%JobResult%`, `%VmCount%` (the number of VMs in the job) and `%Issues%` (the number of VMs in the job that have been processed with the *Warning* or *Failed* status).
 - ii. Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, fails or completes with a warning.
 - iii. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not select this option, Veeam Backup Free Edition will send one notification per every job retry.



Advanced Settings

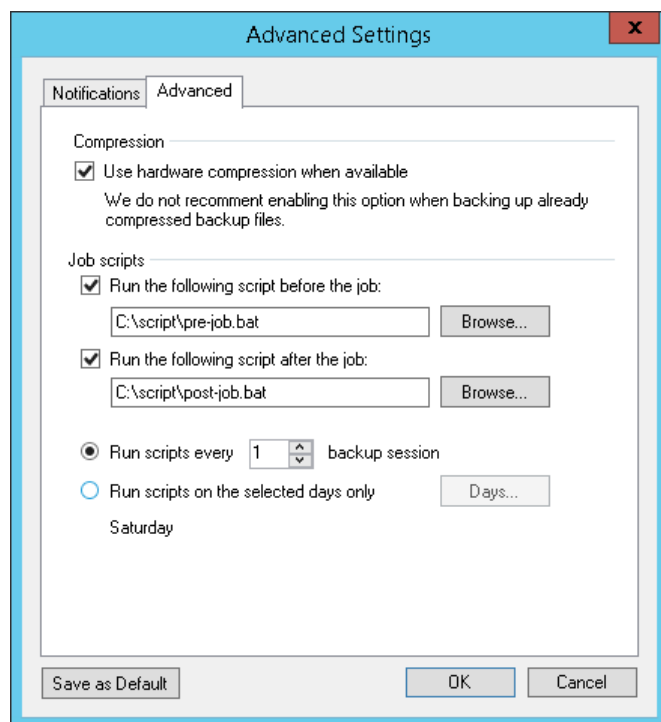
At the **Advanced** tab, you can enable hardware compression or specify custom scripts that you want to run before and/or after the files to tape job.

At the **Options** step of the wizard, click **Advanced**. Select the **Advanced** tab.

1. Select the **Use hardware compression if available** check box if the tape drive should compress data before writing it to tape.

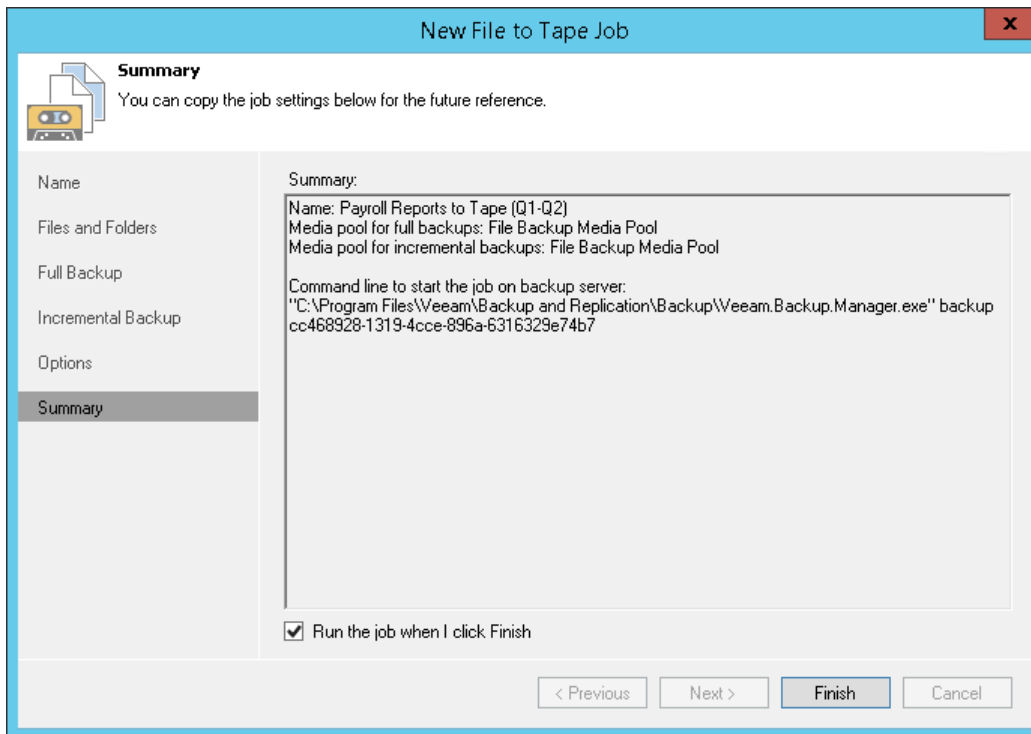
Important! Enable the hardware compression only if your tape library provides support for hardware compression.

2. Select the **Run the following script before the job** and/or **Run the following script after the job** check boxes and click **Browse** to choose executable file(s). You can select to execute pre- and post-job actions after a number of job sessions or on specific week days.
 - If you select the **Run every... backup session** option, specify the number of the job sessions after which the script(s) must be executed.
 - If you select the **Run on selected days only** option, click **Days** and specify week days on which the script(s) must be executed.



Step 8. Finish Working with the Wizard

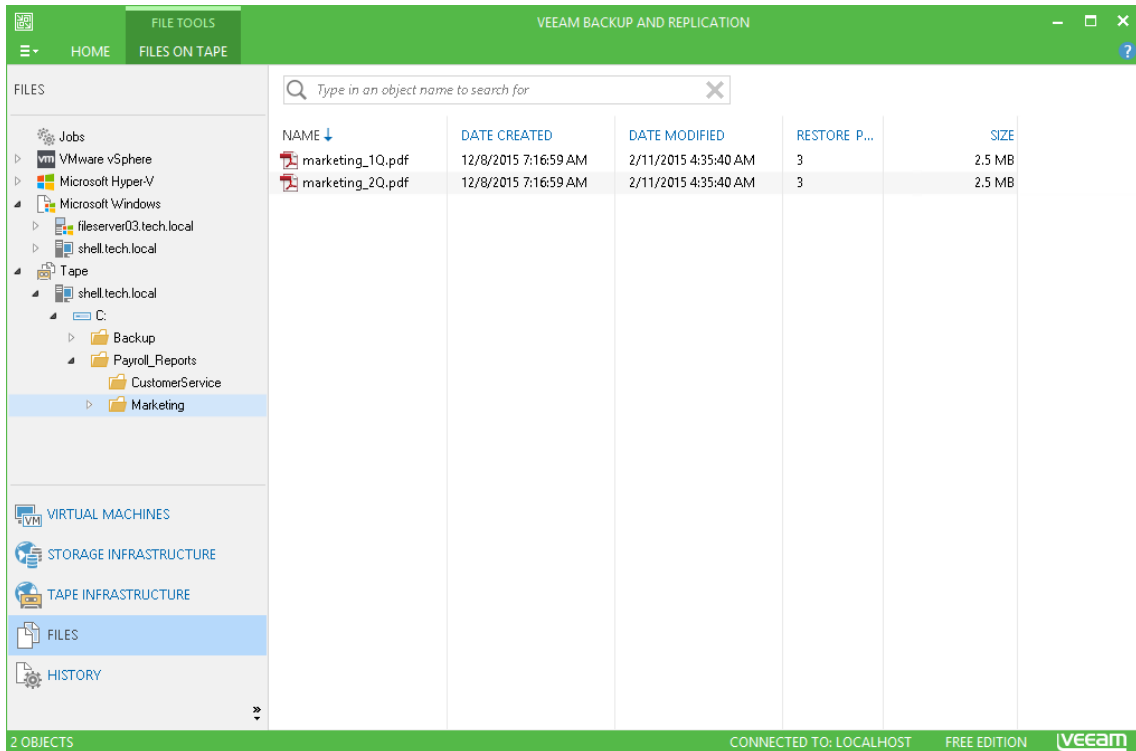
After you have specified schedule settings, click **Create**. Select the **Run the job when I click Finish** check box if you want to start archiving files to tape job right after you complete working with the wizard. Click **Finish** to close the wizard.



View Files on Tape

After the files to tape job completes, you can view the created archive on tape:

1. Open the **Files** view and press F5 to refresh it.
2. Expand the **Tape** node and locate the files archive. Veeam Backup Free Edition preserves the source hierarchy of folders for archived files. You can use the created archive for file recovery.



The screenshot shows the Veeam Backup and Replication console. The top bar is green with 'VEEAM BACKUP AND REPLICATION' and window controls. Below it, a green bar contains 'HOME' and 'FILES ON TAPE'. The left sidebar is titled 'FILES' and shows a tree structure. Under 'Tape', 'Marketing' is selected. The main pane shows a table with 2 objects.

NAME	DATE CREATED	DATE MODIFIED	RESTORE P...	SIZE
marketing_1Q.pdf	12/8/2015 7:16:59 AM	2/11/2015 4:35:40 AM	3	2.5 MB
marketing_2Q.pdf	12/8/2015 7:16:59 AM	2/11/2015 4:35:40 AM	3	2.5 MB

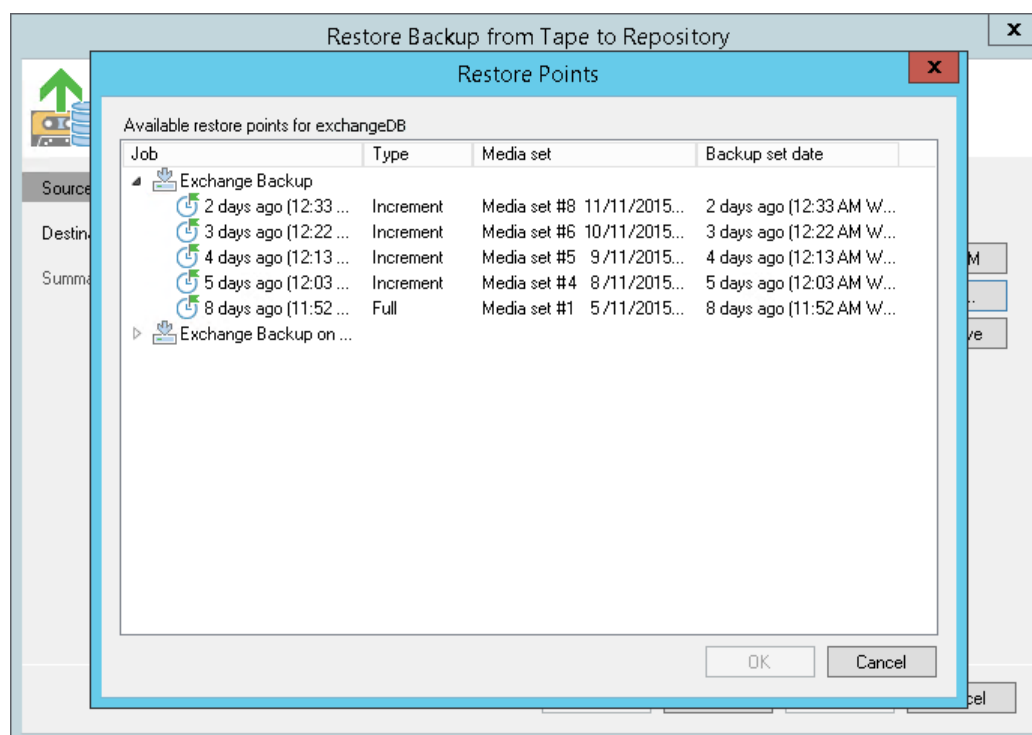
At the bottom, a green bar shows '2 OBJECTS', 'CONNECTED TO: LOCALHOST', 'FREE EDITION', and the Veeam logo.

Step 3. Select a Restore Point

By default, Veeam Backup & Replication will restore backup with the latest state of the archived VM. However, if you want to restore a backup for the VM to an earlier state, select a VM in the list and click **Point** on the right. In the **Restore Points** section, select a restore point that should be used to restore VM backup.

Note: If you choose a full backup point in the list, Veeam Backup & Replication will restore only this full backup. If you choose an increment, Veeam Backup & Replication will restore a chain consisting of a full backup and forward increments, necessary to restore VMs to the required point-in-time.

If you have chosen to restore multiple VMs, you can select a different restore point for every VM specifically.



Step 4. Choose Backup Destination

At the **Destination** step of the wizard, select where the backup files for the selected VMs should be restored:

- To restore VM backup files to a repository, select the **Backup repository** option and choose the necessary repository from the list.
- To restore VM backup files to the Veeam backup server, shared folder or to any other machine connected to Veeam backup server, select the **Server** option. Choose the necessary server from the list and specify path to the target folder in the **Path to folder** field.

If you choose to restore files to a shared folder, make sure that the account under which Veeam Backup Service runs has write permissions to the target folder. If the account does not have sufficient permissions, Veeam Backup Free Edition will prompt you to enter credentials for the account that can be used for writing to the target folder.

Restore Backup from Tape to Repository

Destination
Specify where to stage the backup files required for VM restore.

Source
Destination
Summary

Restore backup files to

☐ Backup repository:
Backup Share (Created by FILESERVER03\Administrator at 11/11/2015 4:27 AM.)
106.2 GB free of 126.5 GB

☒ Server:
fileserver03.tech.local
Details

Path to folder:
C:\Shared
Browse...
106.2 GB free of 126.5 GB

Required space: 90.1 GB

< Previous Next > Finish Cancel

Step 5. Finish Working with the Wizard

Review the settings and click **Finish** to restore selected VM backups.

Restore Backup from Tape to Repository

Summary
Review the restore settings and click Finish to start the restore.

Source
Destination
Summary

Summary:
Server: fileserver03.tech.local
Path: C:\Shared
VM name: exchangeDB
VM size: 0.0 KB
Restore point: 2 days ago (12:33 AM Wednesday 11/11/2015)

< Previous Next > **Finish** Cancel

Restoring Files from Tape

To restore files backed up to tape, use the **Files from Tape Restore** wizard. This section will guide you through all steps of the wizard and provide explanation on available options. To restore files from tape, follow the next steps:

Step 1. Launch the Files from Tape Wizard

To run the **Files from Tape** wizard, open the **Home** tab and click **Restore Files** on the ribbon.

Alternatively, you can:

- Open the **Files** view, expand the **Tapes** node and browse to the necessary files on tape. Select the files and choose **Restore Files from Tape** on the ribbon.
- Open the **Files** view, expand the **Tapes** node and browse to the necessary files on tape. Select the files and choose **Restore files from tape**.

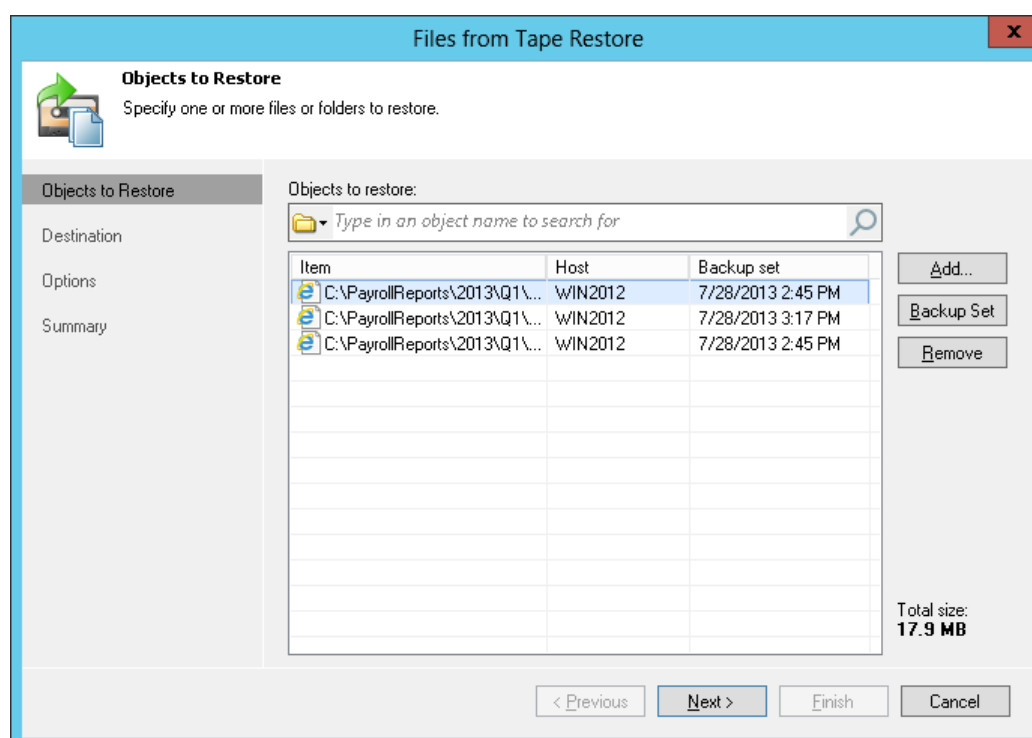
Step 2. Choose Files to Restore

At the **Objects to Restore** step, choose files and folders that you want to restore.

Click **Add** and browse to the file or folder that should be restored. The selected item will be added to the list. To quickly find file or folder, use the search field at the top of the list: enter an object name or a part of it and click the search button on the right or press **[ENTER]**.

If you have chosen files to restore in the **Files** view, the list of objects to restore will be populated with selected files.

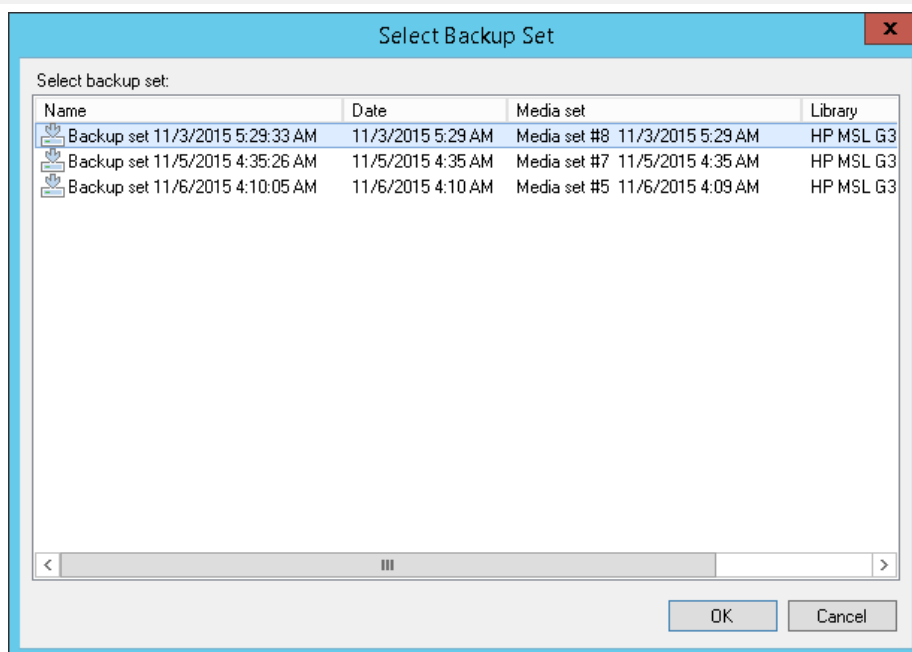
To remove a file or folder from the list, select it and click **Remove**.



By default, Veeam Backup Free Edition will restore the latest version of files available on tape. If you want to restore files from another restore point, select the necessary file and click **Backup Set**. In the list of available backup sets, select the necessary archiving session and click **OK**.

Note:

When you restore an entire folder from tape, Veeam Backup Free Edition restores all files that have ever existed in the folder and been archived to tape. To restore files in the folder, Veeam Backup Free Edition scans the selected backup set and backup sets that were created previously. If a file is not found in the selected backup set, Veeam Backup Free Edition will restore the most recent version of the file from a backup set preceding the selected backup set.



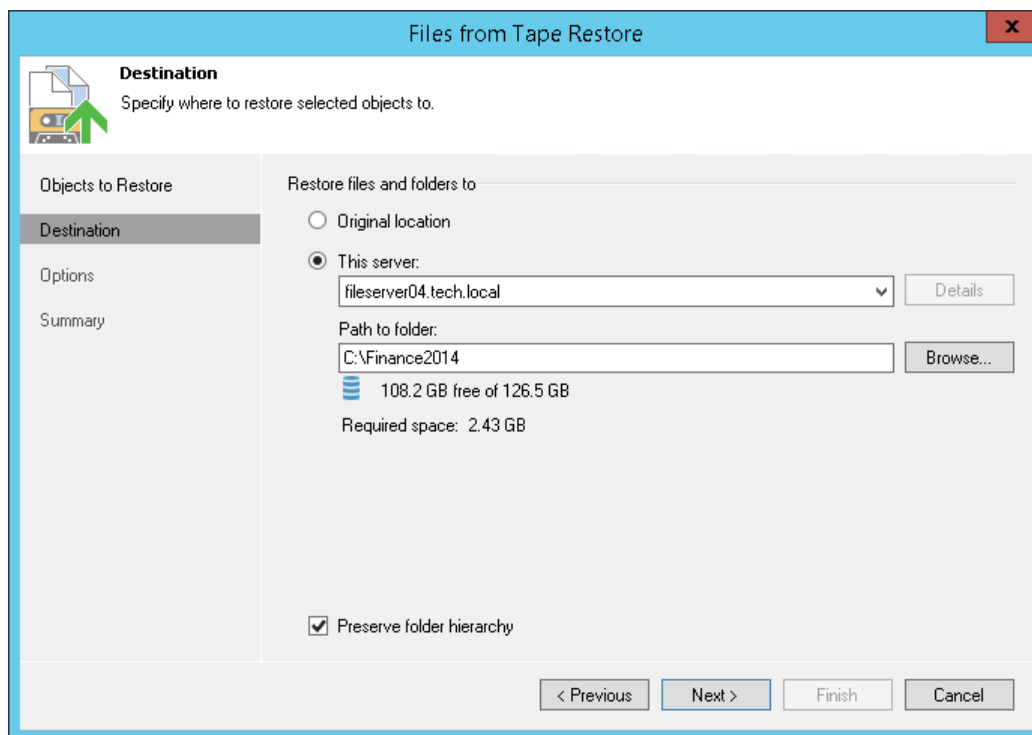
Step 3. Specify Restore Destination

At the **Destination** step of the wizard, specify destination where the archived files will be restored. You can use one of the following options:

- **Original location.** Use this option to restore a file to the location where the original file resides (or resided). This type of restore is only possible if the original machine is connected to Veeam Backup Free Edition and powered on.
- **This server.** Use this option if you want to restore the file to the Veeam backup server, shared folder or to any other machine connected to Veeam backup server. From the server list, choose a machine to which files should be restored and specify path to the target folder.

If you choose to restore files to a shared folder, make sure that the account under which Veeam Backup Service runs has write permissions to the target folder. If the account does not have sufficient permissions, Veeam Backup Free Edition will prompt you to enter credentials for the account that can be used for writing to the target folder.

When restoring files to a location other than original, Veeam Backup Free Edition preserves the folder hierarchy. To restore files to the specified target folder without keeping the folder structure, clear the **Preserve folder hierarchy** check box.

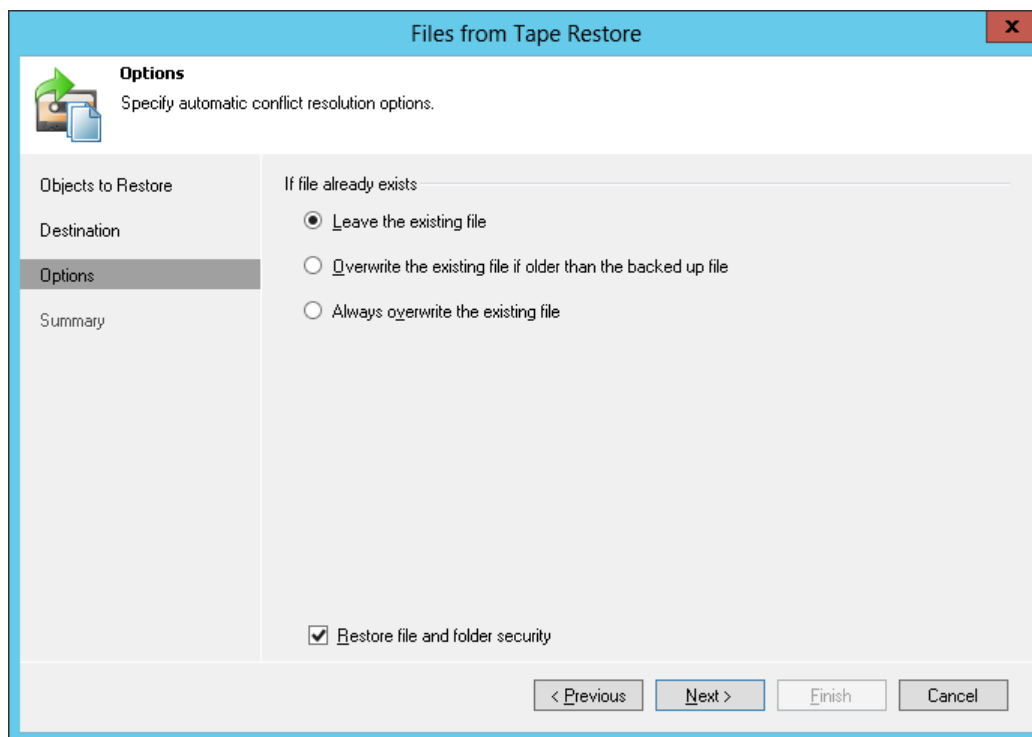


Step 4. Specify Restore Options

At the **Options** step of the wizard, specify overwrite options in case the file already exists in the target folder:

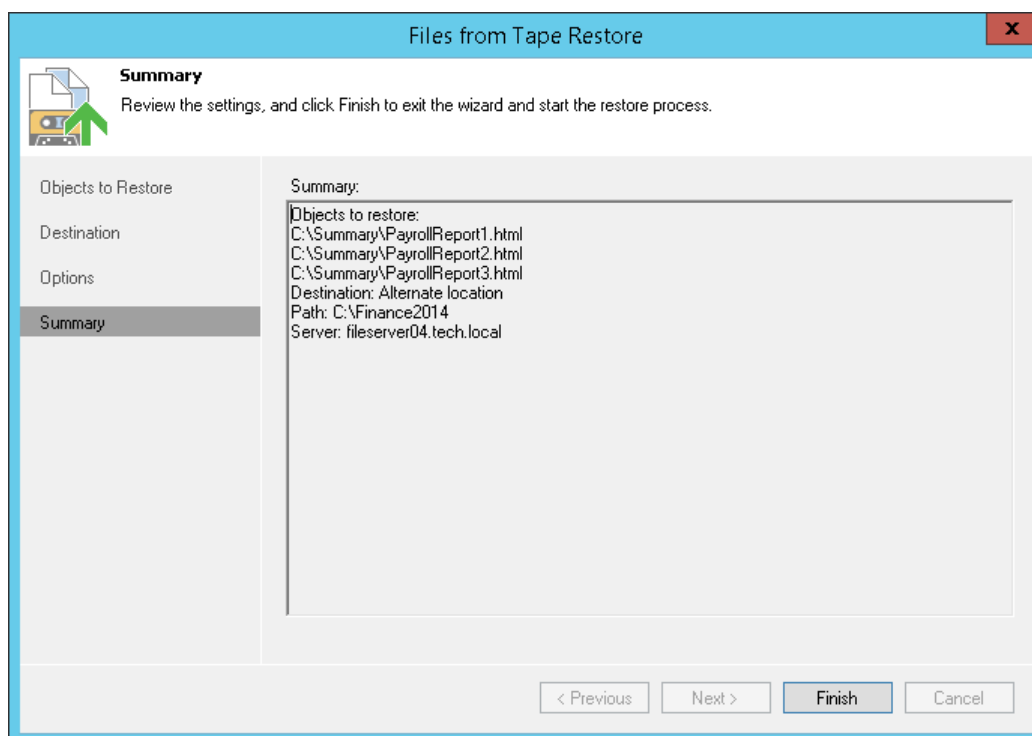
- **Leave the existing file.** Select this option if you do not want to overwrite the existing file with the restored one.
- **Overwrite the existing file if older than the backed up file.** Select this option if you want to overwrite the existing file only if it is older than the restored file.
- **Always overwrite the existing file.** Select this option if you want to overwrite the existing file with the restored file in all cases.

Select the **Restore file and folder security** check box if you want the restored files to keep their original ownership and security permissions. In the opposite case, Veeam Backup Free Edition will change security settings: the user account under which the Veeam Backup Service runs will be set as the owner of the restored objects, while access permissions will be inherited from the target folder to which the objects are restored.



Step 5. Finish Working with the Wizard

Review the settings and click **Finish** to restore selected files and folders.



Restoring Encrypted Data from Tapes

When you restore data from encrypted tapes, Veeam Backup Free Edition performs data decryption automatically in the background or requires you to provide a password.

- If encryption keys required to unlock the tape are available in the Veeam Backup Free Edition database, you do not need to enter the password to decrypt the tape. Veeam Backup Free Edition uses keys from the database to unlock the encrypted tape. Data decryption is performed in the background and data restore from encrypted tapes does not differ from that from an unencrypted ones.

Automatic tape decryption is performed if the following conditions are met:

1. You encrypt and decrypt tapes on the same Veeam backup server.
 2. The tape is loaded to the tape library and information about this tape is available in the catalog.
 3. The password specified in the settings of the media pool to which the tape belongs is the same as the password that was used for tape encryption.
- If encryption keys are not available in the Veeam Backup Free Edition database, you can provide a password or a set of passwords to unlock the encrypted tape. For more information, see [Decrypting Tapes with Password](#).

Decrypting Tapes with Password

When you restore encrypted files or backups from tape, you need to specify a password that was used to encrypt data archived to tape.

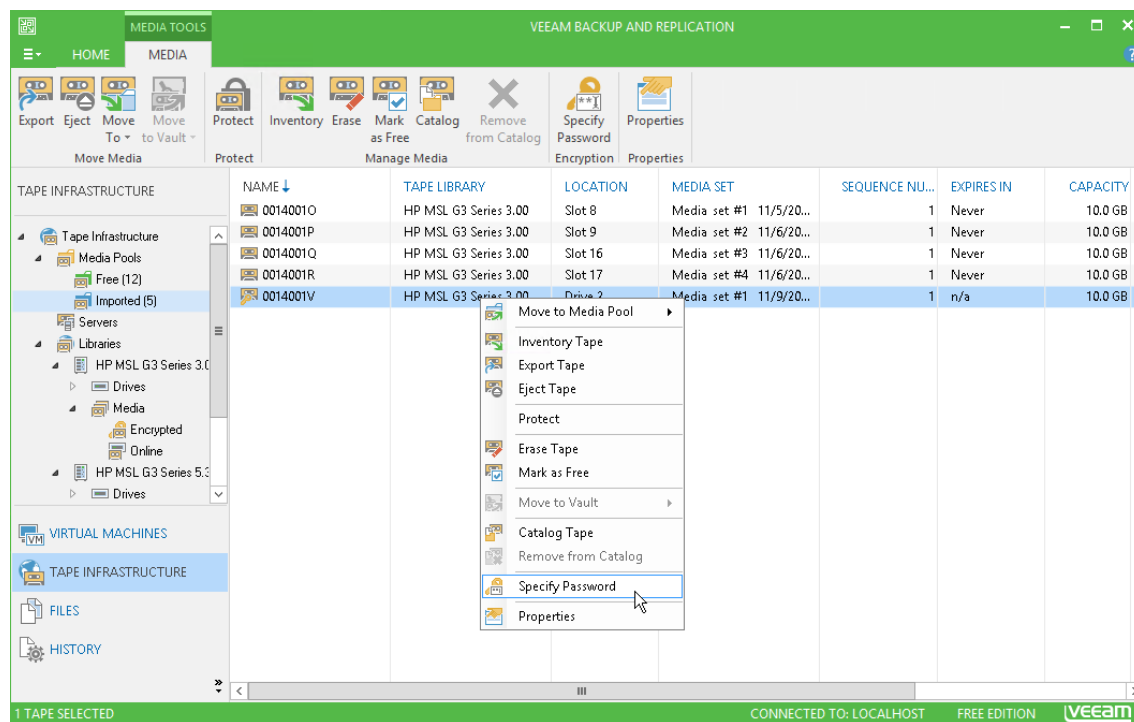
To unlock encrypted tapes:

1. Insert encrypted tapes into the tape library.
2. Catalog the tapes so that Veeam Backup Free Edition can read data archived on tape. After you perform catalogization, encrypted tapes will be displayed under the **Media > Encrypted** node in the corresponding tape library. On the cataloged tape, Veeam Backup Free Edition displays the key icon to mark it as encrypted.
3. In the inventory pane, select the **Encrypted** node under **Media** node.
4. In the working area, select the imported tape and click **Specify password** on the ribbon or right-click the tape and select **Specify password**.
5. In the **Description** field of the **Specify Password** window, Veeam Backup Free Edition displays a hint for the password that was used to encrypt the tape. Use the hint to recall the password.
6. In the **Password** field, enter the password for the tape.
7. If the imported tape is a part of a backup set but is not the last tape in this set, perform catalogization once again.

When Veeam Backup Free Edition creates a backup set, it writes catalog data to the last tape in this set.

- If the imported group of tapes contains the last tape in the backup set, Veeam Backup Free Edition retrieves catalog data from the last tape during the initial catalogization process (see point 2 of this procedure).
- If the imported group of tapes does not contain the last tape in the backup set, Veeam Backup Free Edition needs to additionally catalog files on imported tapes.

If you enter a correct password, Veeam Backup Free Edition will decrypt the tape media. The tape will be moved under the corresponding media pool in the inventory pane. You can perform restore operations for data archived to tape as usual.



Working with vCloud Director VMs

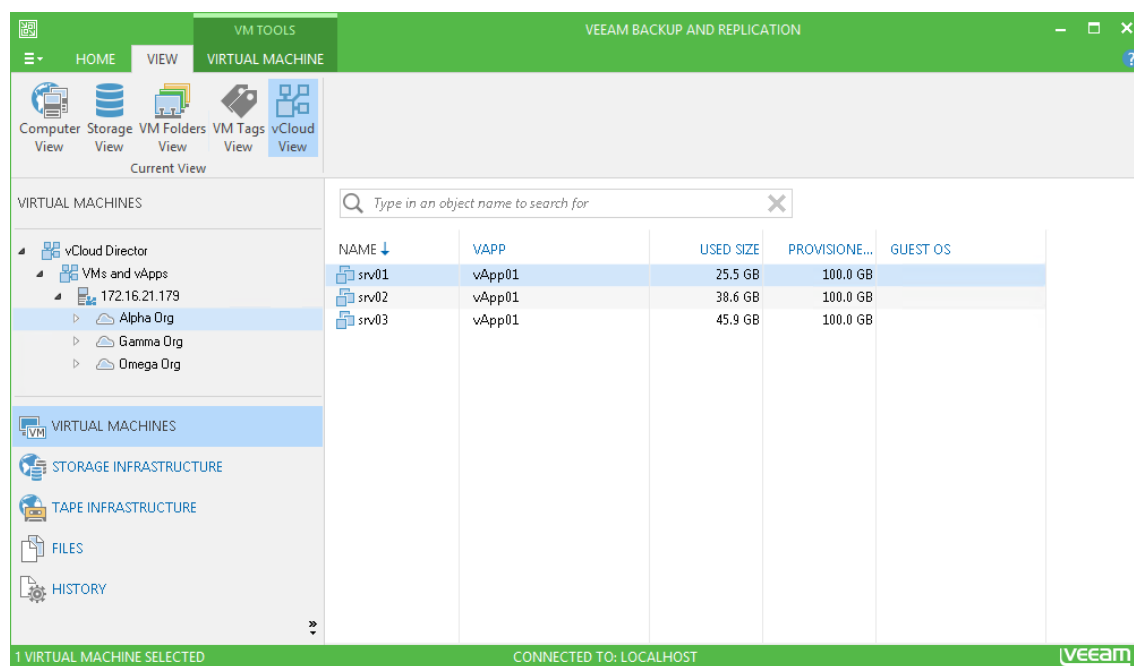
You can perform backup and restore operations for VMs managed by VMware vCloud Director.

Viewing vCloud Director VMs

After you have added the vCloud Director server, you can view the vCloud Director hierarchy directly in the Veeam Backup Free Edition console and work with VMs managed with vCloud Director. To open the vCloud Director hierarchy:

1. In Veeam Backup Free Edition, open the **Virtual Machines** view.
2. Click the **View** tab on the ribbon.
3. On the **View** tab, click **vCloud View**.

The hierarchy of the added vCloud Director server will become available in the inventory pane, VMs managed by vCloud Director will be displayed in the working area. You can work with these VMs just as if you worked with VMs managed by vCenter Servers or registered on ESX(i) hosts added to Veeam Backup Free Edition.



The screenshot shows the Veeam Backup and Replication console with the 'View' tab selected. The 'vCloud View' is active, displaying a hierarchy of vCloud Director objects in the left pane and a table of virtual machines in the main pane.

Left Pane Hierarchy:

- vCloud Director
 - VMs and vApps
 - 172.16.21.179
 - Alpha Org
 - Gamma Org
 - Omega Org

Main Pane Table:

NAME ↓	VAPP	USED SIZE	PROVISIONE...	GUEST OS
srv01	vApp01	25.5 GB	100.0 GB	
srv02	vApp01	38.6 GB	100.0 GB	
srv03	vApp01	45.9 GB	100.0 GB	

Status Bar: 1 VIRTUAL MACHINE SELECTED | CONNECTED TO: LOCALHOST | Veeam

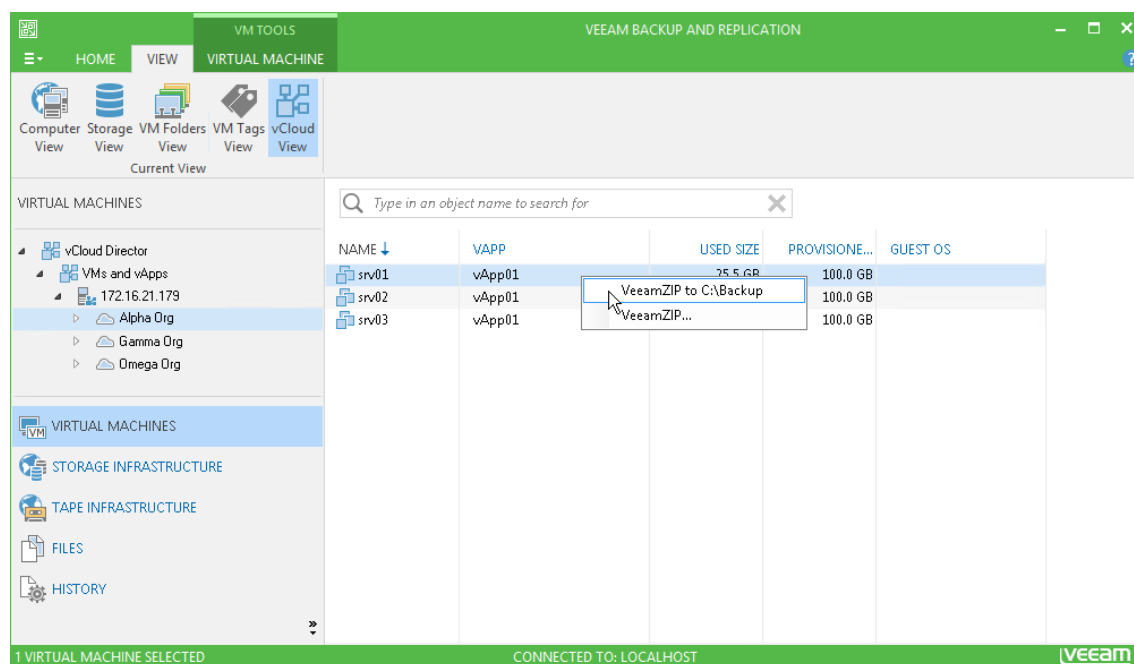
Creating VeeamZIP Files for vCD VMs

From the user's side, creating a VeeamZIP file for vCD VMs is practically the same as creating VeeamZIP files for regular VMs.

To create a backup of VMs with VeeamZIP, follow the next steps:

1. Open the **Virtual Machines** view.
2. Click the **View** tab on the ribbon.
3. On the **View** tab, click **vCloud Director View**.
4. In the infrastructure tree, click the vApp in which the necessary VM resides.
5. In the working area, right-click the VM and select **VeeamZIP**. You can also select the necessary VM and click **VeeamZIP** on the toolbar.

To quickly find a VM, type the full or partial VM name in the search field at the top of the working area and click the **Start search** button on the right or press **[ENTER]** on the keyboard.



Performing Restore from vCD Backups

Veeam Backup Free Edition offers a number of options for restoring VM data from vCD backups. You can perform the following operations:

- Restore a VM to VMware vCloud Director
- Restore an entire VM to the VMware vSphere infrastructure
- Restore VM hard disks
- Restore VM files (VMX, VMDK and other)
- Restore VM guest OS files

Restoring VMs to vCloud Director

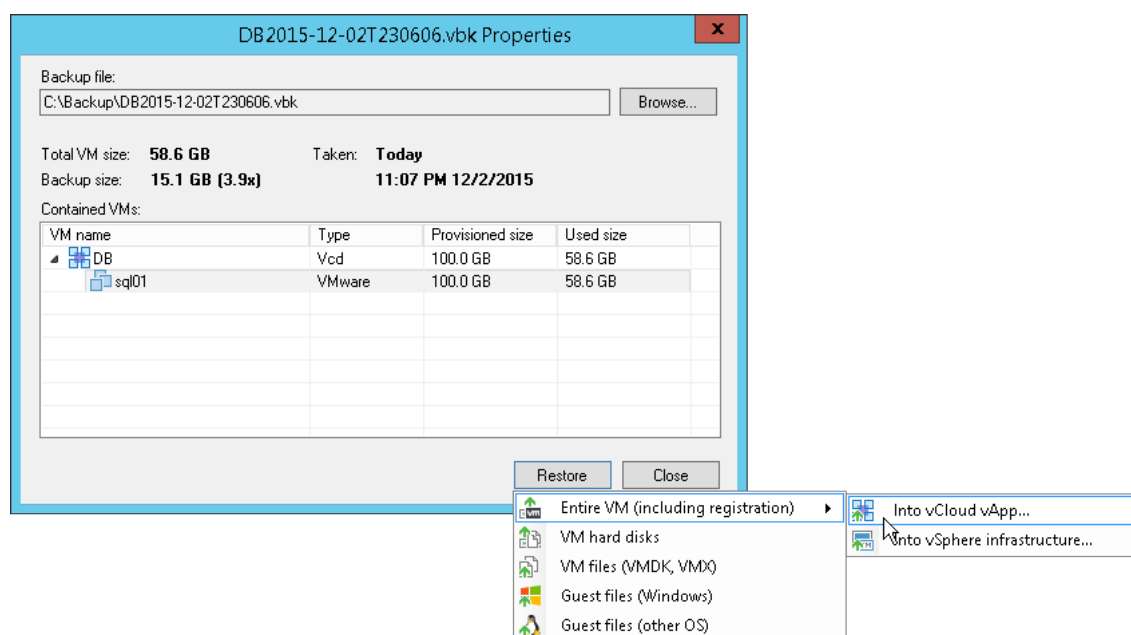
Veeam Backup Free Edition lets you restore a VM from VeeamZIP files back to the vCloud Director hierarchy.

The VM can be restored to its initial location or to any other location of your choice. You can restore a VM that already exists — for example, in case the initial VM is corrupted or you want to revert to an earlier state of the VM, or a VM that no longer exists — for example, if it was deleted by mistake. If you restore a VM that already exists, the initial VM is overwritten with that from the VeeamZIP file.

Step 1. Choose VeeamZIP File

To choose a VeeamZIP file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM that you want to restore.
3. Click **Restore** and select **Entire VM (including registration) > Into vCloud vApp**. The **Full vCloud Restore** wizard will be launched.



Step 2. Select Restore Mode

At the **Restore Mode** step of the wizard, choose the necessary restore mode and backup proxy for VM data transport:

1. Choose a restore mode:
 - Select **Restore to original location** if you want to restore the VM(s) with initial settings and to the original location. If this option is selected, you will immediately pass to the **Summary** step of the wizard.
 - Select **Restore to a new location, or with different settings** if you want to restore the VM(s) to a different location and/or with different settings (such as VM location, network settings, fast provisioning settings and so on). If this option is selected, the **vCloud Full VM Restore** wizard will include additional steps for customizing VM settings.
2. [For VM restore to the original location] Select the **Quick rollback** check box if you want to use incremental restore for the VM(s). Veeam Backup Free Edition will use CBT to get data blocks that are necessary to revert the VM(s) to an earlier point in time, and will restore only these data blocks from the backup. Quick rollback significantly reduces the restore time and has little impact on the production environment.

It is recommended that you enable this option if you restore the VM(s) after a problem that occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not enable this option if the problem has occurred at the VM hardware level, storage level or due to a power loss.

vCloud Full VM Restore

Restore Mode
Specify whether selected objects should be restored back to the original location, or to a new location or with different settings.

Restore Type
Objects to Restore
Restore Mode
Location
VM Network
Fast Provisioning
Datastores
Reason
Summary

☐ **Restore to the original location**
Quickly initiate restore of selected VMs to the original location, and with the original name and settings. This option minimizes the chance of user input error.

☒ **Restore to a new location, or with different settings**
Customize restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the default settings.

[Pick proxy to use](#)

☐ **Quick rollback (restore changed blocks only)**
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

< Previous Next > Finish Cancel

Step 3. Select VM Location

The **Location** step of the wizard is available if you have chosen to change the location and settings for the restored VM(s).

By default, Veeam Backup Free Edition restores the VM to its initial location. To restore the VM a different location:

1. Select the VM in the list and click **vApp**.
2. From the vCloud Director hierarchy, choose a vApp in which the restored VM must be registered.

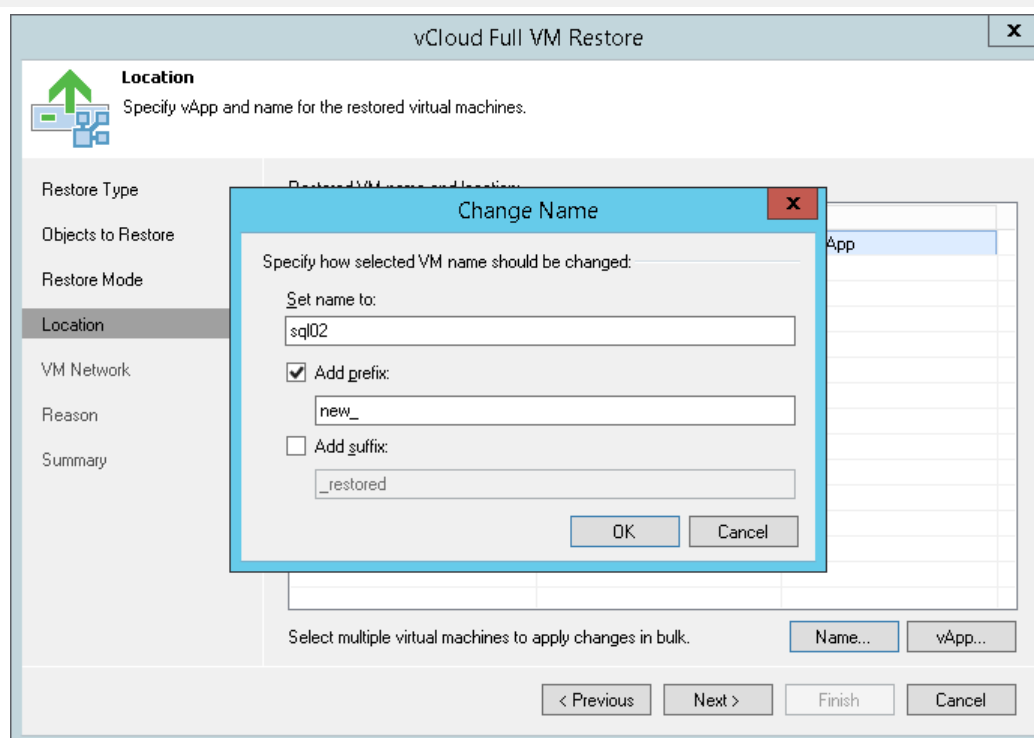
To facilitate selection, use the search field at the bottom of the window: enter the vApp name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

To change the VM name:

1. Select a VM in the list and click **Name**.
2. In the **Change Name** window, enter a new name explicitly or specify a change name rule by adding a prefix and/or suffix to the initial VM name.
3. You can also change VM names directly in the list: select a VM, click the **New Name** field and enter the name to be assigned to the recovered VM.

Important!

If you are restoring a linked clone VM to a different location, make sure that fast provisioning is enabled at the level of the target Organization vDC. Otherwise Veeam Backup Free Edition will restore the VM as a regular VM.



Step 4. Select Destination Network

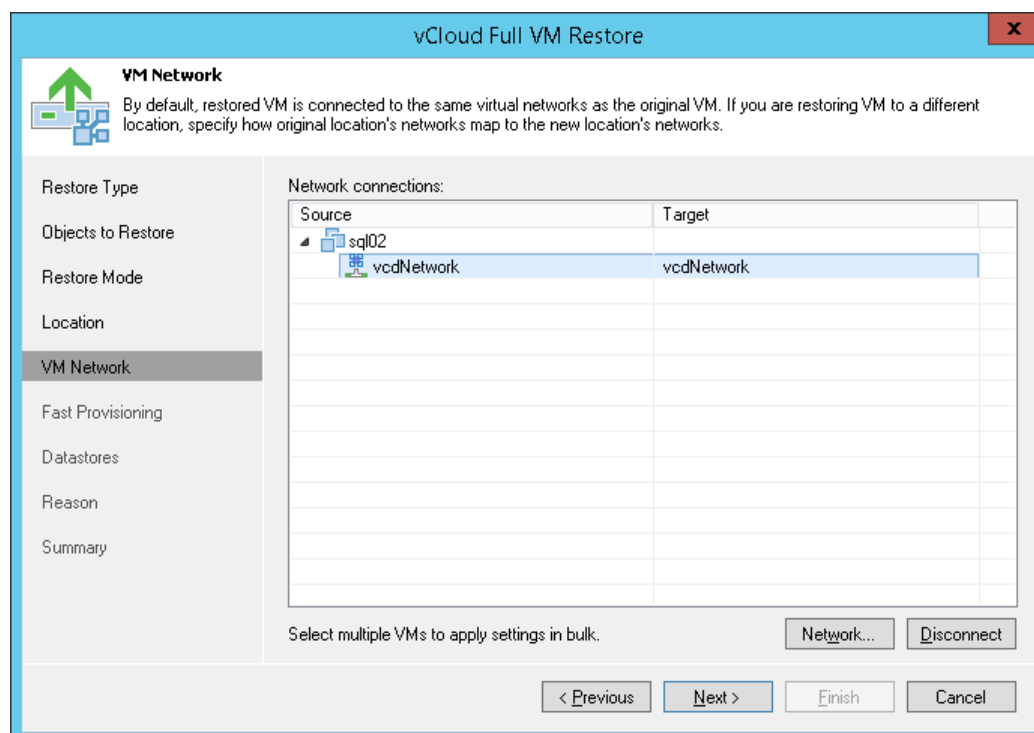
The **VM Network** step of the wizard is available if you have chosen to change the location and settings of the restored VM(s).

To select networks to which the restored VM must be connected:

1. Select a VM in the list and click **Networks**.
2. The **Select Network** window displays all networks that are configured for the destination vApp. From the list of available networks, choose a network to which the restored VM must have access upon restore.

To facilitate selection, use the search field at the bottom of the window: enter a network name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

To prevent the restored VM from accessing any network, select it in the list and click **Disconnected**.



Step 5. Select Template to Link

The **Fast Provisioning** step of the wizard is available if you have chosen to change the settings of the restored VM(s).

To select a VM template:

1. Select a VM in the list and click **Set Template**.
2. From the VMware vCloud Director hierarchy, choose a template to which the restored VM must be linked.

To facilitate selection, use the search field at the bottom of the window: enter a VM template name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

If you want to disable fast provisioning for the VM and restore it as a regular VM, select the VM in the list and click **Disable**.

vCloud Full VM Restore

Fast Provisioning

Specify restore settings for virtual machines that use Fast Provisioning feature.

Restore Type

Objects to Restore

Restore Mode

Location

VM Network

Fast Provisioning

Datstores

Reason

Summary

Fast provisioning templates:

VM	Template	Target vApp
sql02	Disabled	vApp01

Select multiple virtual machines to apply changes in bulk.

Template...Disable

< Previous

Next >

Finish

Cancel

Step 6. Select Storage Profile and Datastores

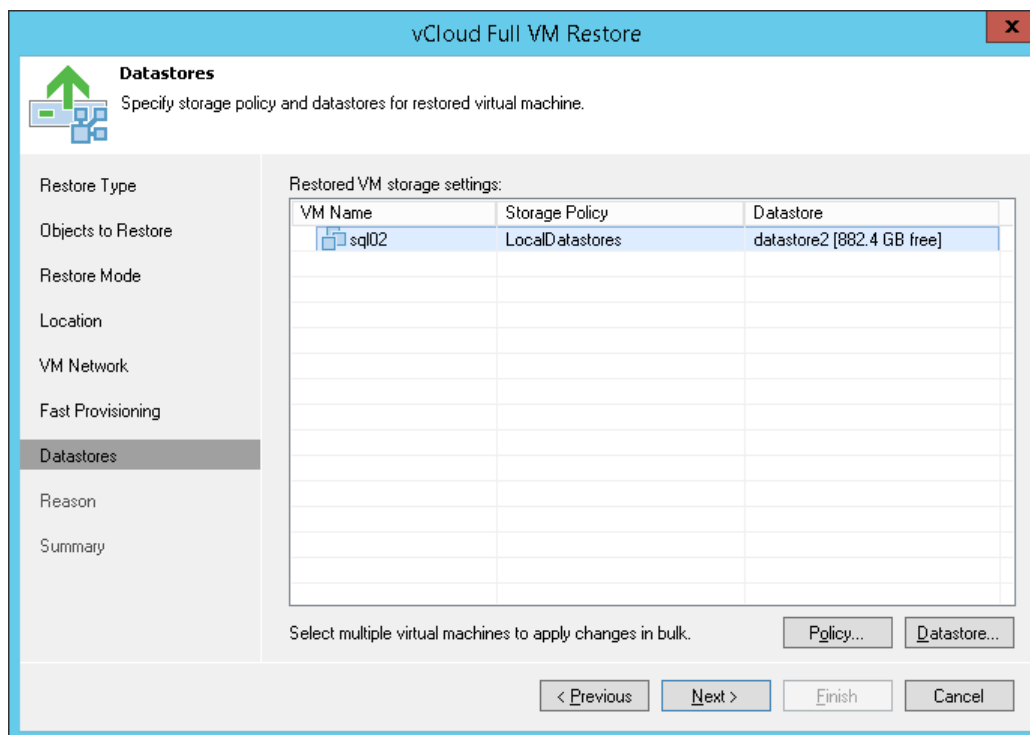
The **Datastores** step of the wizard is available if you have chosen to change the settings of the restored VM(s).

To select a storage profile for the restored VM:

1. Select a VM in the list and click **Storage Profile**.
2. In the displayed window, select the necessary profile for the VM.

If you have selected to disable fast provisioning at the previous step of the wizard, you must select a datastore on which disks of the restored VM will be placed.

1. Select a VM in the list and click **Datastore**.
2. In the displayed window, select the datastore on which the VM disks must be located.

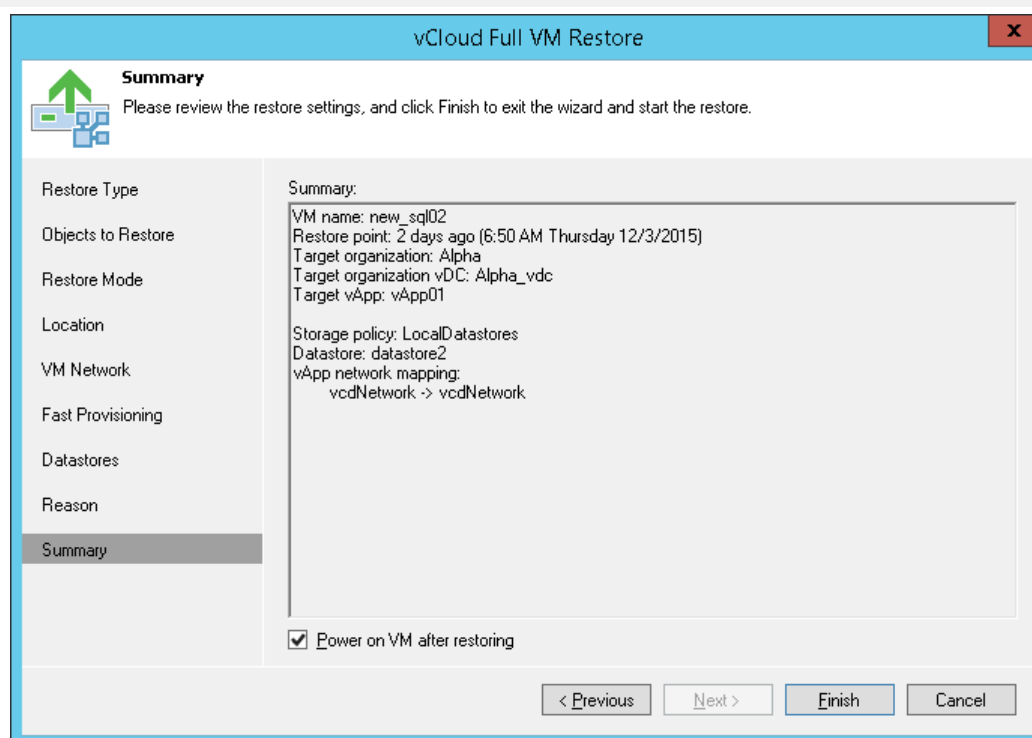


Step 7. Verify Recovery Settings

At the **Summary** step of the wizard, specify additional settings for VM(s) restore:

1. If you want to start the restored VM(s), select the **Power on VM after restoring** check box.
2. Check the settings for VM(s) restore and click **Finish**. Veeam Backup Free Edition will recover the VM(s) in the specified destination.

Note: Veeam Backup Free Edition checks the lease term for the restored VM(s). In case the lease period has expired, the lease will be automatically updated.



Restoring VMs to VMware vSphere Infrastructure

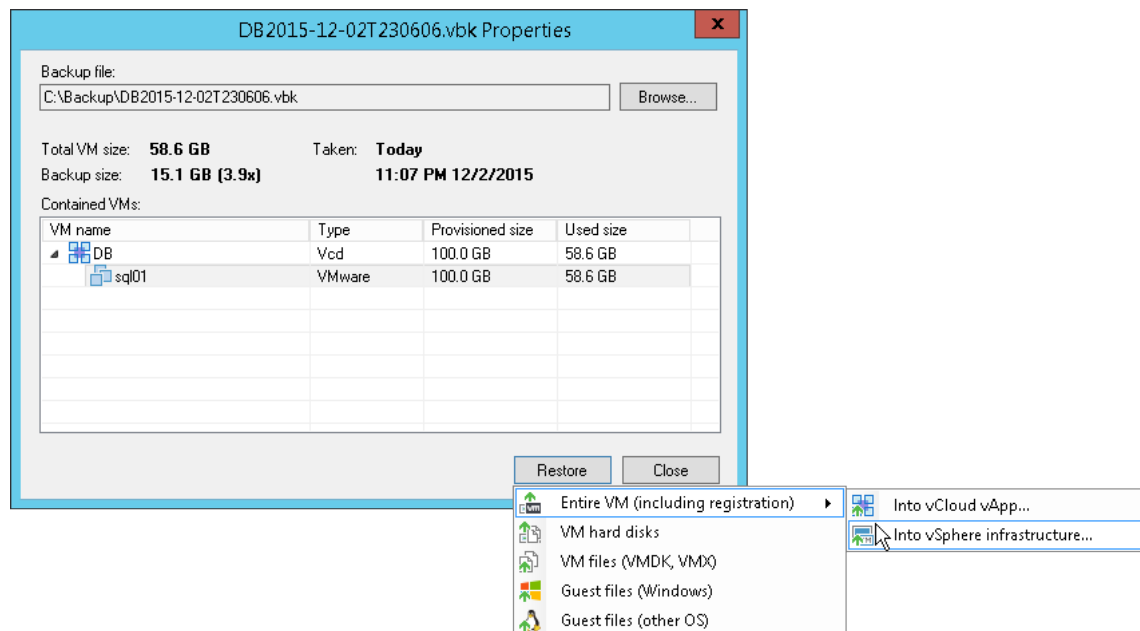
In addition to restoring a VM to the vCloud Director hierarchy, you can also restore it to the VMware vSphere infrastructure. In this situation, Veeam Backup Free Edition neglects the vApp metadata saved to the VeeamZIP file and performs a regular full VM restore process: the VM is restored to the vCenter Server or ESX(i) host and is not registered in vCloud Director.

To restore a VM to vCloud Director, follow the next steps:

To choose a file:

1. On the **Home** tab, click **Restore** on the toolbar. In the displayed window, click **Browse** and select the necessary file. Alternatively, you can simply double-click the file in the file browser (for example, in Windows Explorer).
2. In the **Contained VMs** list, you will see a list of VMs from the file. If you have chosen a backup file or a VeeamZIP file created in Veeam Backup & Replication, the list may contain a number of VMs. Select the VM that you want to restore.
3. Click **Restore** and select **Entire VM (including registration) > Into virtual infrastructure**. The **Full VM Restore** wizard will be launched.

Full VM restore for VMs managed by vCloud Director does not differ from full VM restore for regular VMs. For more information, see [Performing Full VM Restore](#).



Restoring VM Files

The process of VM files restore for vCD VMs does not differ from that for regular VMware VMs. For more information, see [Restoring VM Files](#).

Restoring VM Hard Disks

The process of VM hard disks restore for vCD VMs does not differ from that for regular VMware VMs. For more information, see [Restoring VM Hard Disks](#).

Restoring VM Guest OS Files

The process of VM hard disks restore for vCD VMs does not differ from that for regular VMware VMs. For more information, see [Restoring VM Guest Files](#) and [Multi-OS File-Level Restore](#).

Performing Configuration Backup and Restore

You can back up and restore the configuration database that Veeam Backup Free Edition uses.

During configuration backup, Veeam Backup Free Edition exports data from the configuration database and saves it to a backup file on the backup repository. If the backup server fails for some reason, you can re-install the backup server and quickly restore its configuration from the configuration backup. You can also use configuration backups to apply the configuration of one backup server to another backup server in the backup infrastructure.

It is recommended that you regularly perform configuration backup for every backup server in the backup infrastructure. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead if any problem with backup servers occurs.

Creating Configuration Backups

When you perform configuration backup, Veeam Backup Free Edition retrieves data for the backup server from the configuration database, writes this data into a set of XML files and archives these XML files to a backup file of the BCO format.

Veeam Backup Free Edition exports information about the following objects:

- **Backup infrastructure components and objects:** hosts, servers, global settings configured on the backup server and so on.
- **Sessions:** job sessions performed on the backup server.
- **Tapes:** tape libraries connected to the backup server.

Configuration backup is job-driven. You can schedule it to run regularly or start it manually. You can choose a location in which the configuration backup must be stored and specify the necessary retention settings.

By default, Veeam Backup Free Edition is configured to create a configuration backup daily. The resulting configuration backup file is stored in the `\VeeamConfigBackup\%BackupServer%` folder on the default backup repository. However, for security's sake, it is recommended that you store configuration backups on the backup repository other than the default one or any other storage. If the backup server fails, its configuration data will remain, and you will be able to recover the failed backup server.

Note:

When you configure a new backup repository, Veeam Backup Free Edition offers you to change the configuration backup file location from the default backup repository to the new backup repository. Click **Yes**, and Veeam Backup Free Edition will automatically change the backup target in the configuration backup job settings and will use this target in future.

Configuration backups that were created before the target change will remain on the default backup repository. You can manually copy them to the new backup repository to have all restore points of the configuration backup in one place.

Scheduling Configuration Backups

You can instruct Veeam Backup Free Edition to perform configuration backup automatically by schedule.

Important!

If you plan to migrate configuration data to the database used by another backup server, stop all running jobs and disable scheduled jobs before creating the configuration backup. In the opposite case, job sessions may be failing after configuration restore. For more information, see [Migrating Configuration Database](#).

To schedule a configuration backup:

1. From the main menu, select **Configuration Backup**.
2. Make sure that the **Enable configuration backup to the following repository** check box is selected.
3. In the **Restore points to keep** field, specify the number of restore points that you want to maintain on the backup repository.
4. Click **Schedule** next to the **Perform backup on** field and specify the time schedule according to which the configuration backup must be created.
5. To create an encrypted backup, select the **Encrypt configuration backup** check box. From the **Password** field, select a password you want to use for encryption. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see [Creating Encrypted Configuration Backups](#).

The screenshot shows the 'Configuration Backup Settings' dialog box. It is divided into two main sections: 'Backup' and 'Restore'. In the 'Backup' section, the 'Enable configuration backup to the following repository:' checkbox is checked. Below it, a dropdown menu shows 'Backup Repository (Created by Veeam Backup)' with a status bar indicating '20.5 GB free of 59.7 GB'. The 'Restore points to keep:' is set to 10. The 'Perform backup on:' is set to 'Daily at 10:00 AM' with a 'Schedule...' button. The 'Last successful backup:' is '12/7/2015 12:06 AM' with a 'Backup now' button. The 'Encrypt configuration backup' checkbox is also checked. The 'Password:' dropdown shows 'Standard (Last edited: 4 days ago)' with an 'Add...' button. Below the password field, there are two status indicators: 'Loss protection enabled' with a green checkmark and a 'Manage passwords' link, and 'Configuration backup contains encrypted data.' with a green checkmark. The 'Restore' section has a 'Restore the configuration backup to this server:' checkbox and a 'Restore...' button. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

Running Configuration Backups Manually

You can create a configuration backup manually when you need it, for example, if you want to capture a state of the configuration database at a specific point in time.

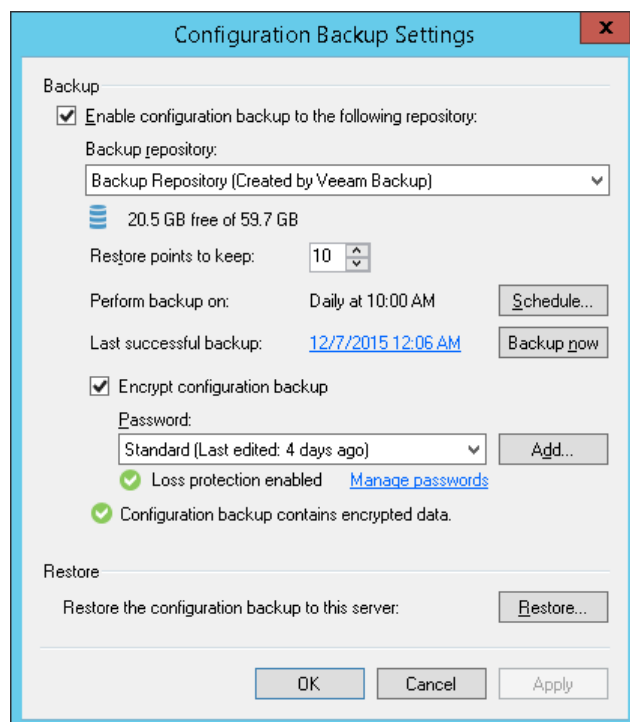
Important!

If you plan to migrate configuration data to the database used by another backup server, stop all running jobs and disable scheduled jobs before creating the configuration backup. In the opposite case, job sessions may be failing after configuration restore. For more information, see [Migrating Configuration Database](#).

To create a configuration backup manually:

1. From the main menu, select **Configuration Backup**.
2. Make sure that the **Enable configuration backup to the following repository** check box is selected.
3. In the **Restore points to keep** field, specify the number of restore points that you want to maintain on the backup repository.
4. To create an encrypted backup, select the **Encrypt configuration backup** check box. From the **Password** field, select a password you want to use for encryption. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see [Creating Encrypted Configuration Backups](#).
5. Click **Backup now**.

Veeam Backup Free Edition will back up the configuration database and store a new restore point to the selected backup repository.

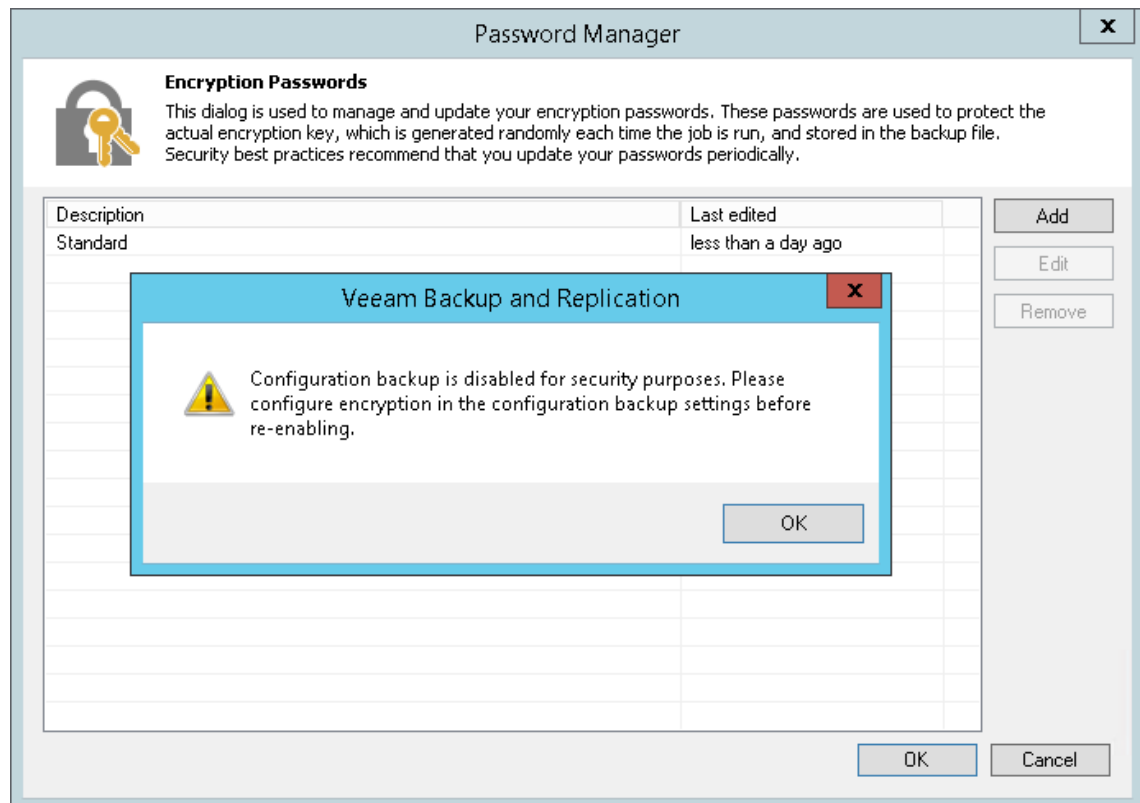


Creating Encrypted Configuration Backups

Veeam Backup Free Edition requires that you encrypt the configuration backup if you have created at least one password in the Password Manager on the backup server.

When you encrypt jobs or tapes with passwords, Veeam Backup Free Edition creates a set of keys that are employed in the encryption process. Some encryption keys, for example, storage keys and metakeys, are stored in the configuration database. If a configuration backup was non-encrypted, data from it could be freely restored on any backup server. Encryption keys saved to the configuration database and the content of encrypted files might become accessible for unintended audience.

If the Password Manager contains at least one password and you do not enable encryption for the configuration backup, Veeam Backup Free Edition disables configuration backup. To enable the configuration backup, you must enable encryption in the configuration backup job settings.



After you enable the encryption option, Veeam Backup Free Edition will create encrypted configuration backups. Beside encryption keys, the created backups capture credential records specified in the Credentials Manager. When you restore data from such backup, you will not have to enter passwords for credentials records again (unless the passwords for credentials records have changed by the time of restore).

To encrypt the configuration backup:

1. From the main menu, select **Configuration Backup**.
2. Select the **Encrypt configuration backup** check box.
3. From the **Password** field, select a password you want to use for encryption. If you have not created a password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see [Managing Passwords for Data Encryption](#).

Restoring Configuration Data

To restore data from the configuration backup, you can use one of two methods: data restore and data migration.

Data restore can be helpful in the following situations:

- The configuration database got corrupted and you want to recover data from the configuration backup.
- The Microsoft SQL Server on which the configuration database resides got corrupted, and you want to deploy the configuration database on a new Microsoft SQL Server, and restore data from the configuration backup to it.
- You want to roll back the configuration database to a specific point in time.
- You want to restore data to a new configuration database on the same Microsoft SQL server, for example, for testing purposes.

Data migration can be helpful if you need to move the backup server and configuration database to another location, for example, offsite. In this case, you can configure a backup server, deploy a Microsoft SQL Server in the target location and then restore data from the configuration backup to a database on this server. As a result, you will get a "replica" of the backup server without additional adjustments and fine-tuning.

It is recommended that you use Veeam Backup Free Edition tools to create configuration backups and migrate the configuration database. If you use other tools, for example, native Microsoft SQL Server tools, after migration some information such as secure configuration data may be not accessible.

Restoring Configuration Database

You can restore a configuration backup on the same backup server where the backup was created or on another backup server.

Before you start the restore process, [check prerequisites](#). Then use the **Veeam Backup & Replication Configuration Restore** wizard to restore the configuration database.

Before You Begin

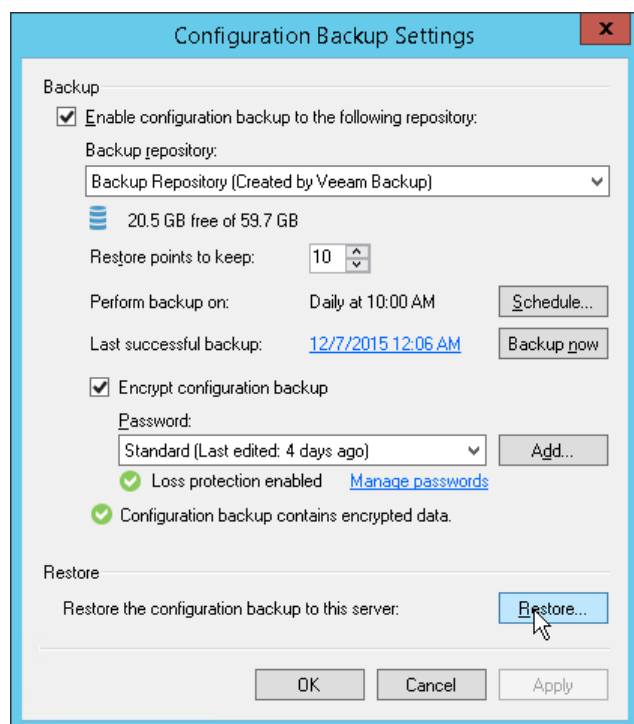
Before you start the restore process, check the following prerequisites:

1. Stop all jobs that are currently running. During restore of configuration, Veeam Backup Free Edition temporarily stops the Veeam Backup Service and jobs.
2. Check the version of the backup server. On the backup server running Veeam Backup Free Edition 9.0, you can restore configuration backups created with the following product versions: 7.0 Update 4, 8.0 and 9.0.

Step 1. Launch Configuration Database Restore Wizard

To launch the **Veeam Backup and Replication Configuration Restore** wizard, do either one of the following:

- From the main menu, select **Configuration Backup**. In the **Restore** section, click **Restore**.
- In Microsoft Windows Explorer, open the folder where configuration backups are stored (by default, Backup\VeeamConfigBackup\<BackupServerName> on the volume with most disk space on the backup server) and double-click the necessary configuration backup file.



Step 2. Select Restore Mode

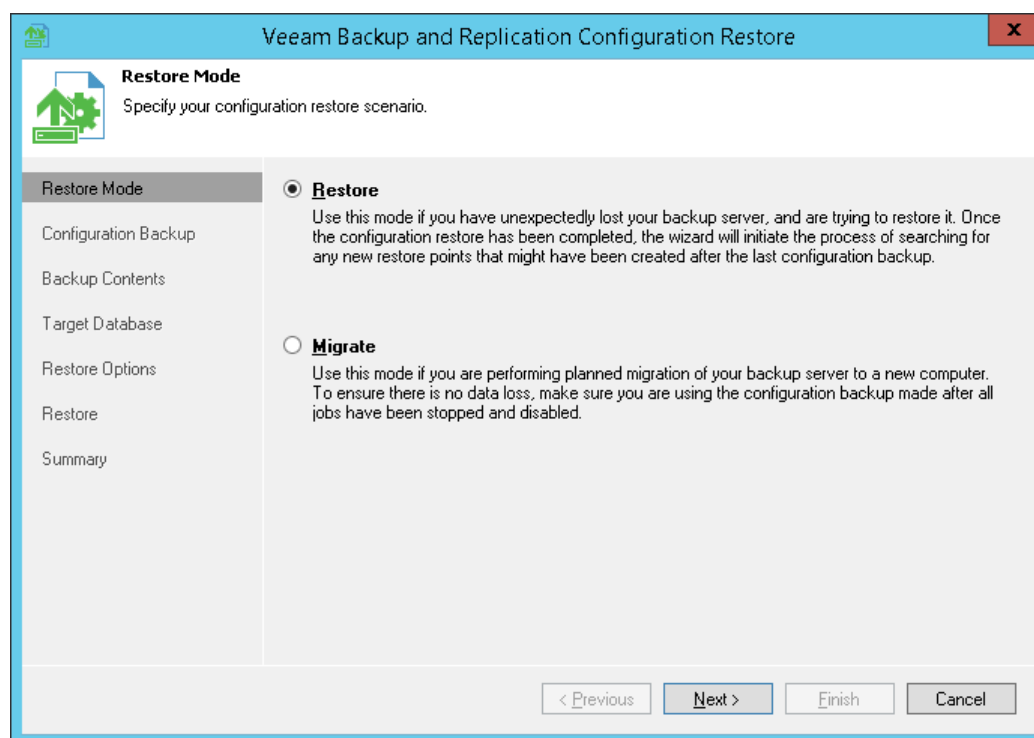
At the **Restore Mode** step of the wizard, choose a restore mode that you want to use.

- Select **Restore** if you want to restore data from the configuration backup to the database used by the initial backup server.

In the Restore mode, Veeam Backup Free Edition retrieves configuration data from the backup and stores it to the target database. After that, Veeam Backup Free Edition performs additional rescan of VM replicas, backup repositories and tape libraries connected to the backup server. Rescan helps synchronize potential changes between the backup infrastructure and restored database that took place from the moment when the configuration backup was created till the present time. As a result, the target configuration database will contain information about restore points that were created after the configuration backup was taken, and this information is displayed in the Veeam Backup Free Edition console.

- Select **Migrate** if you want to restore data from the configuration backup to the database used by another backup server.

In the Migrate mode, Veeam Backup Free Edition retrieves configuration data from the backup and stores it to the target database. No rescan operation is performed.

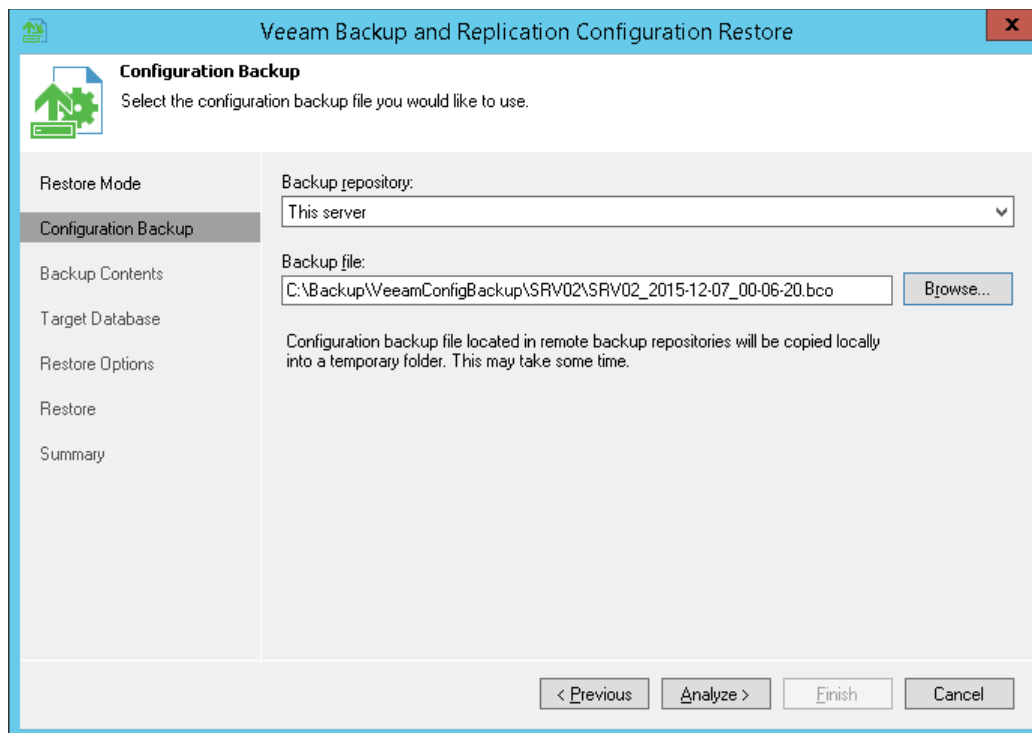


Step 3. Select Configuration Backup

At the **Configuration Backup** step of the wizard, select a configuration backup from which you want to restore data.

1. From the **Backup repository** list, select a server or backup repository on which the configuration backup file is located.
2. Click **Browse** next to the **Backup file** field and select the backup file.

If you select to restore configuration data from a backup on a remote backup repository, during restore Veeam Backup Free Edition will first copy the backup file to a temporary folder on the backup server. After you finish the restore process and close the wizard, Veeam Backup Free Edition will automatically delete the configuration file from the temporary folder.



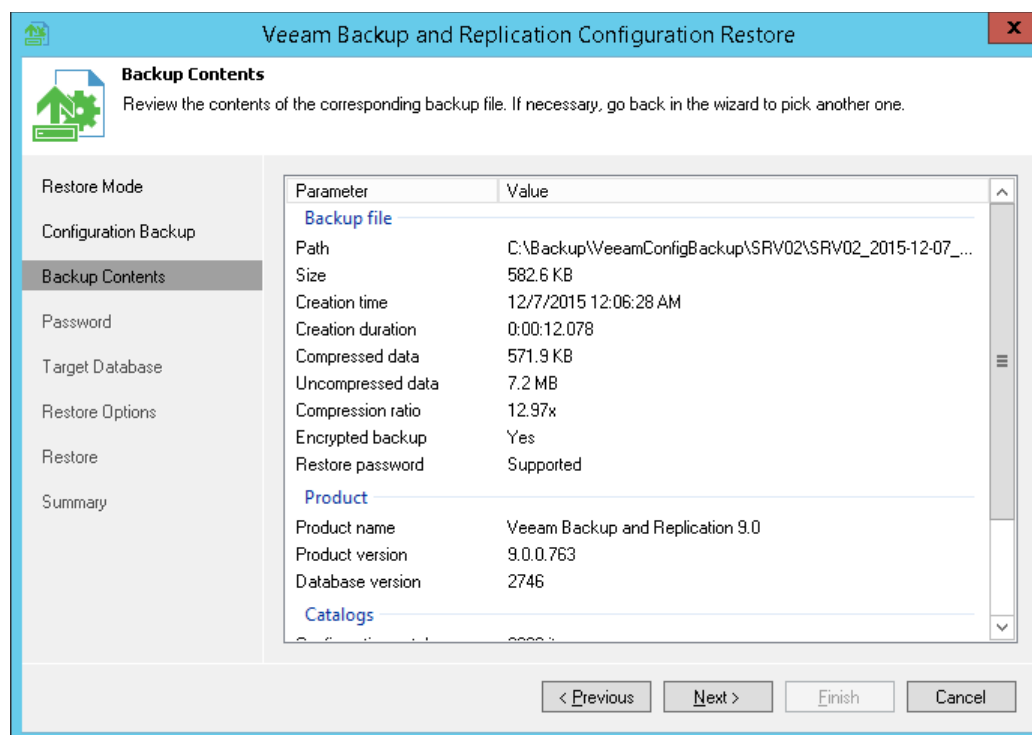
The screenshot shows the 'Veeam Backup and Replication Configuration Restore' wizard window. The title bar is blue with a close button. The main window has a light blue header with a gear icon and the title 'Configuration Backup'. Below the header, it says 'Select the configuration backup file you would like to use.' On the left is a vertical sidebar with a list of steps: 'Restore Mode', 'Configuration Backup' (highlighted), 'Backup Contents', 'Target Database', 'Restore Options', 'Restore', and 'Summary'. The main area contains a 'Backup repository:' dropdown menu with 'This server' selected. Below it is a 'Backup file:' text box containing the path 'C:\Backup\VeeamConfigBackup\SRV02\SRV02_2015-12-07_00-06-20.bco', followed by a 'Browse...' button. A note states: 'Configuration backup file located in remote backup repositories will be copied locally into a temporary folder. This may take some time.' At the bottom are four buttons: '< Previous', 'Analyze >', 'Finish', and 'Cancel'.

Step 4. Review Configuration Backup Parameters

At the **Backup Contents** step of the wizard, Veeam Backup Free Edition will analyze the content of the selected backup file and display the following settings:

- **Backup file settings:** settings of the configuration backup file itself.
- **Product settings:** version of Veeam Backup Free Edition installed on the initial backup server and configuration database version.
- **List of catalogs:** catalogs storing backup configuration data.

Review the displayed settings and click **Next**.

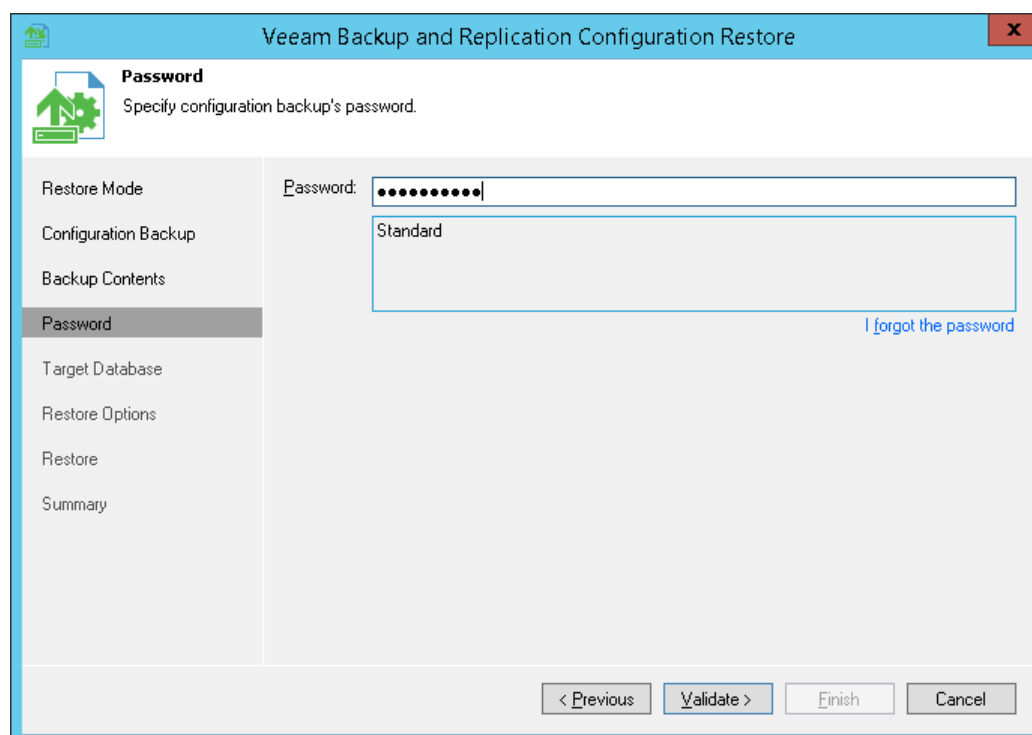


Step 5. Specify Password

The **Password** step of the wizard is available if you have enabled the encryption option in the configuration backup properties.

Enter the password to decrypt configuration backup data:

1. Check the password hint to recall the password.
1. In the **Password** field, enter the password to decrypt the configuration backup file.



Step 6. Specify Target Database

At the **Target Database** step of the wizard, specify a target Microsoft SQL server and database to which configuration data must be restored.

1. In the **Database name** field, specify a name of the database to which configuration data must be restored. By default, Veeam Backup Free Edition uses the name of the initial database.

If you specify a name of the database that does not exist, Veeam Backup Free Edition will create it on the Microsoft SQL Server.

2. From the **Server name** list, select a Microsoft SQL server on which the database is deployed or must be deployed. In the list of Microsoft SQL Servers Veeam Backup Free Edition displays all servers from the network where the backup server resides. To update the list of servers, click **Refresh** on the right.

3. In the **Authentication** section, select the authentication mode to connect to the Microsoft SQL Server instance: **Windows Authentication** or **SQL Server Authentication**. If you select the Microsoft SQL Server authentication mode, specify the user name and password of the account that you want to use. To view the entered password, click and hold the eye icon on the right of the field.

The screenshot shows the 'Veeam Backup and Replication Configuration Restore' wizard. The 'Target Database' step is active, showing a sidebar with options: Restore Mode, Configuration Backup, Backup Contents, Password, Target Database (selected), Restore Options, Restore, and Summary. The main area is titled 'Target Database' and contains the instruction 'Specify the Veeam Backup & Replication database to restore configuration to.' It is divided into two sections: 'Connection' and 'Authentication'. In the 'Connection' section, the 'Database name' is 'VeeamBackup04' and the 'Server name' is 'SRV02\VEEAMSQL2012'. In the 'Authentication' section, 'Windows authentication' is selected. At the bottom are buttons for '< Previous', 'Connect >', 'Finish', and 'Cancel'.

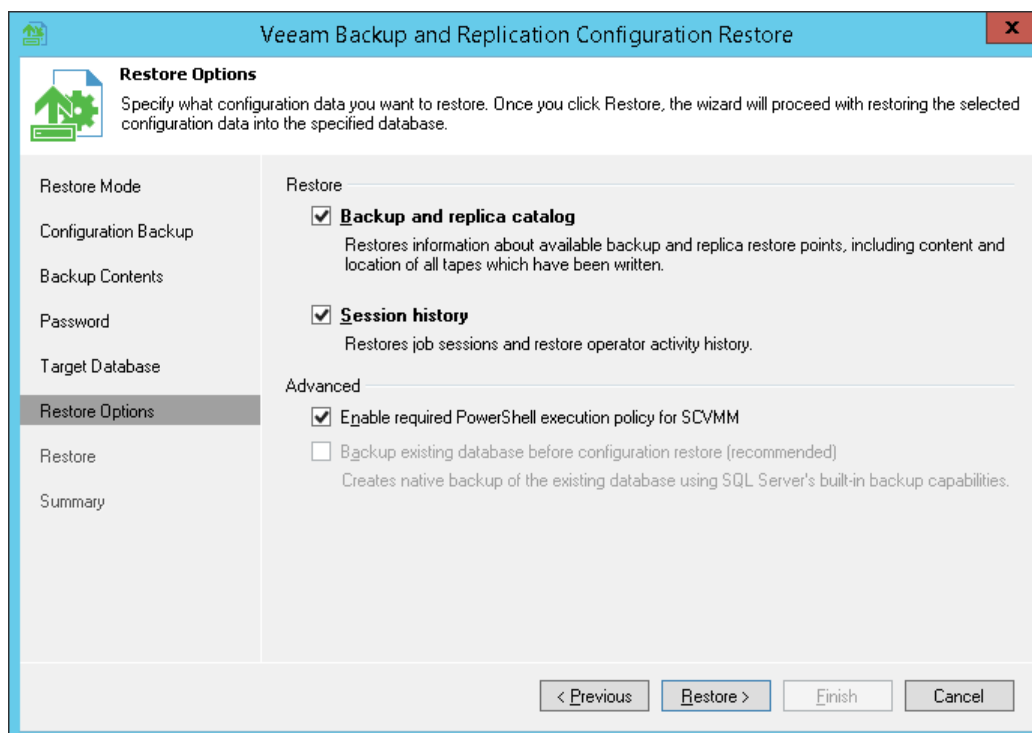
Step 7. Specify Restore Options

At the **Restore Options** step of the wizard, specify additional restore options.

1. In the **Restore** section, select what data you want to restore from the configuration backup. Veeam Backup Free Edition always restores configuration data for backup infrastructure components, jobs and global settings specified at the level of the backup server. You can additionally restore the following data:
 - **Backup and replica catalog:** data about all backups and replicas registered on the backup server.
2. If you are restoring configuration data to the same database, select the **Backup existing database before configuration restore** check box. This option will help you protect the current database from accidental errors during the restore process. During restore, Veeam Backup Free Edition will first back up the current database using the native tools of Microsoft SQL Server. After that, Veeam Backup Free Edition will purge the current database and import data from the configuration backup to it. In such scenario, if an error occurs during the restore process, you will be able to restore the current database from the Microsoft SQL backup using Microsoft SQL Management Studio or SQL scripts.

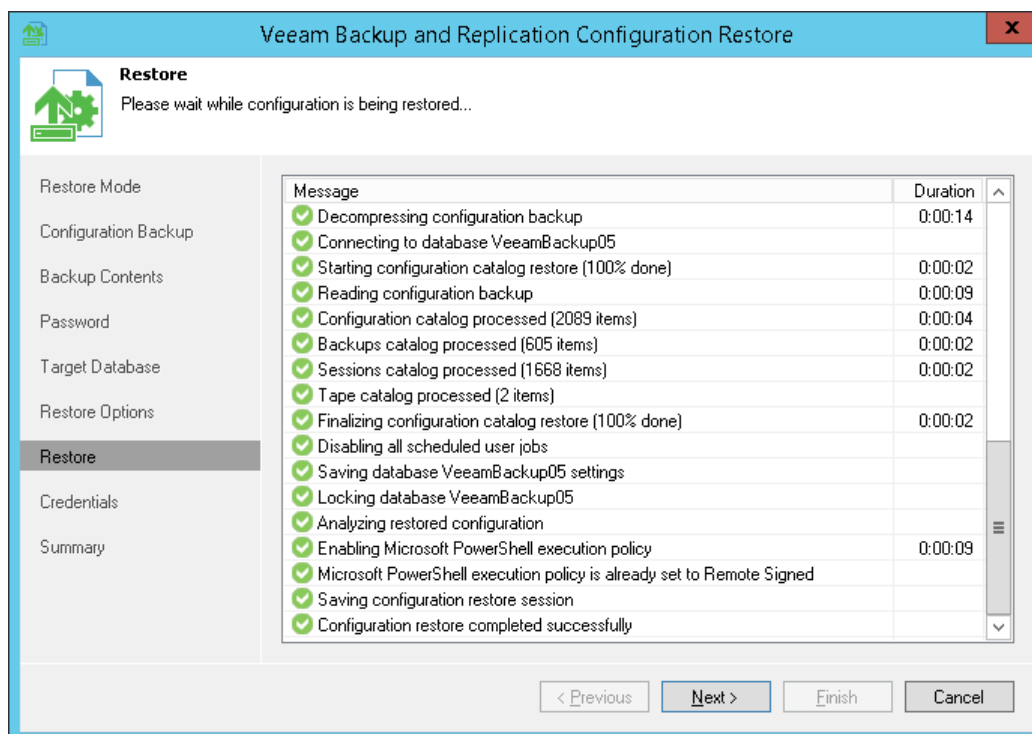
The created Microsoft SQL database backup is named by the following pattern: *VeeamBackup<DatabaseName><date>.bak* and stored to the default Microsoft SQL backups location, for example: %Program Files%\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup\.

- Click **Restore**. Veeam Backup Free Edition will stop currently running jobs and Veeam Backup Free Edition services and will restore the database to the specified location.



Step 8. Review Restore Settings

At the **Restore** step of the wizard, Veeam Backup Free Edition will display the progress on the restore process. Wait for the restore process to complete and click **Next**.



If you have chosen to restore data in the Migrate mode and the configuration backup file does not meet the Migrate mode requirements, Veeam Backup Free Edition will display a warning and offer you to switch to the Restore mode. The Restore mode requires more time but guarantees that information about all new restore points will be available in the restored database.

- To switch to the **Restore** mode, in the warning window click **Yes**.
- To carry on data restore in the **Migrate** mode, in the warning window click **No**.
- To stop the restore process, in the warning window click **Cancel**.

For more information, see [Migrating Configuration Database](#).

Step 9. Finalize Restore Process

After the restore process has finished, you may need to perform the following actions to finalize the configuration database restore:

1. [Specify credentials for backup infrastructure objects.](#)
2. [Perform components upgrade.](#)

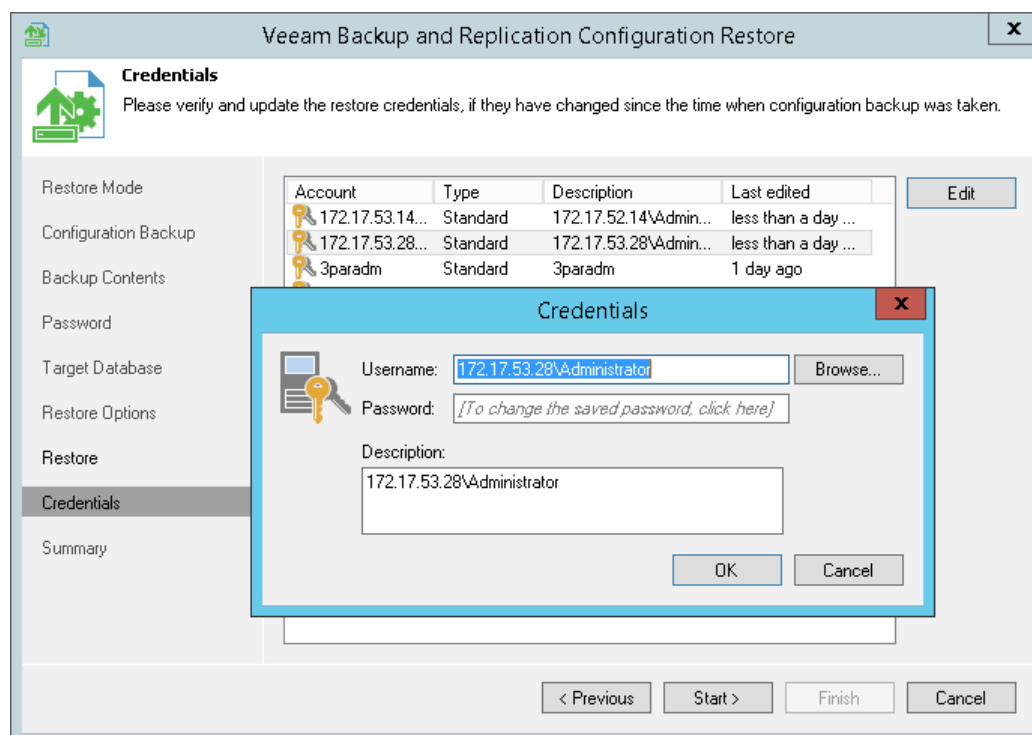
Specifying Credentials

The **Credentials** step of the wizard is available if you have enabled encryption for configuration backup.

Veeam Backup Free Edition displays a list of credentials records that existed on the backup server at the time when the configuration backup was created. If by the time of restore passwords for credentials records have changed, you can specify new values for these records.

To specify new passwords:

1. Select a credentials record in the list and click **Edit**.
2. Enter the necessary password.
3. Repeat the procedure for all credentials records in the list.



Performing Components Upgrade

After the restore process is complete, Veeam Backup Free Edition will check if services on backup infrastructure components must be upgraded and display a list of outdated components.

To upgrade backup infrastructure components, select check boxes next to the necessary components and click **Next**. If some component fails to upgrade, you can get back to a previous step of the wizard and repeat the procedure or close the wizard and upgrade the components manually. For more information, see [Upgrading Server Components](#).

Step 10. Synchronize Backups and Tape Libraries

After the configuration database is restored, Veeam Backup Free Edition can perform a synchronization operation for backups and replicas created on the backup server and tape libraries connected to the backup server.

The synchronization operation for backups and replicas is performed in the following situations:

1. You are restoring a database from the backup created with Veeam Backup Free Edition 7.0 in the **Restore** mode.
2. You are restoring a database from the backup created with Veeam Backup Free Edition 8.0 in the **Restore** mode and you have selected to restore data from the **Backup and replica catalog**.

The synchronization operation for tape libraries is performed in the following situations:

1. You are restoring a database from the backup created with Veeam Backup Free Edition 7.0 in the **Restore** mode.
2. You are restoring a database from the backup created with Veeam Backup Free Edition 8.0 in the **Restore** mode and you have selected to restore data from the **Backup and replica catalog**.

Wait for the synchronization operation to complete.

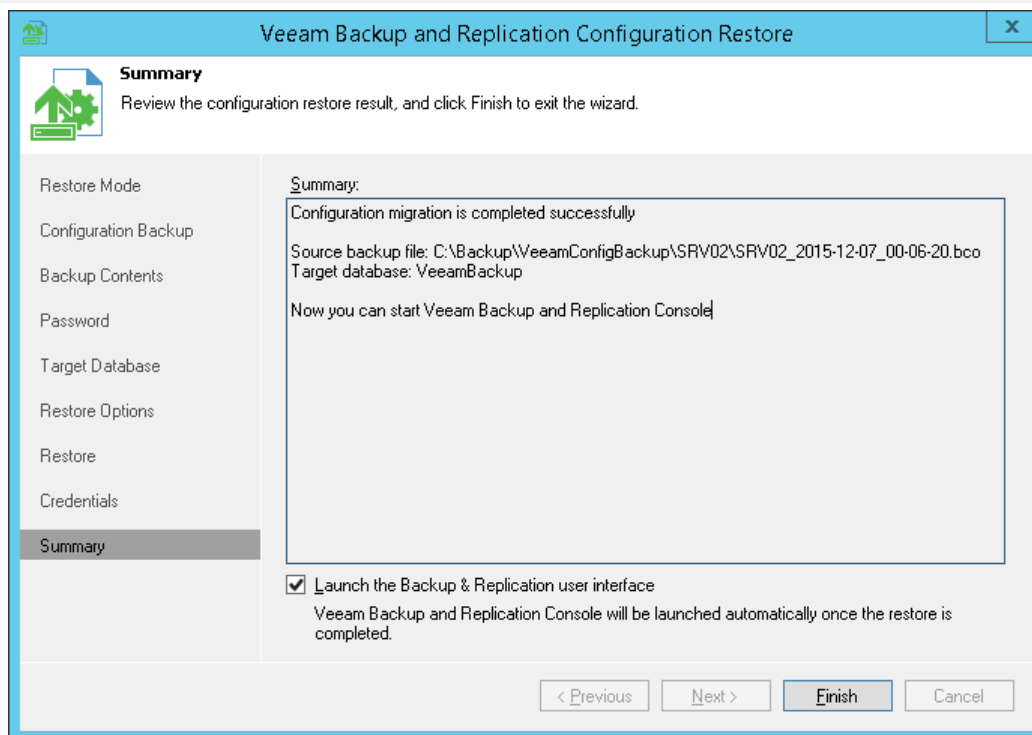
Note: Veeam Backup Free Edition has a set of limitations for restoring tape data from configuration backups created with Veeam Backup Free Edition 7.0. For more information, see <http://veeam.com/kb1935>.

Step 11. Finish Working with Wizard

At the **Summary** step of the wizard, finalize the process of configuration data restore.

1. Review the restore process results.
2. If you want to start Veeam Backup Free Edition after you finish working with the wizard, select the **Launch the Backup & Replication user interface** check box.
3. Click **Finish** to exit the wizard.

Note: If you restore data from the configuration backup in the **Restore** mode, all jobs on the backup server will be disabled after the restore process is complete. You need to enable them manually.



Migrating Configuration Backup

To migrate configuration data to a database used by another backup server, perform the following steps:

1. Before you create the configuration backup, stop all running jobs and disable all scheduled jobs on the backup server from which you migrate configuration data.

Do not start and/or enable any jobs. If you start a job before migration is completed, Veeam Backup Free Edition will produce a new restore point in the chain and update the chain metadata. The created configuration backup will not contain information about this new restore point. When you migrate data from the configuration backup to the database and start the job again, Veeam Backup Free Edition will fail to synchronize the chain metadata with data in the database. As a result, the job will fail.
2. Launch the **Configuration Database Restore** wizard. At the **Restore Mode** step of the wizard, select **Migrate**.
3. Follow the next steps of the wizard and specify other configuration migration settings as described in [Restoring Configuration Database](#).

Before starting configuration data restore in the Migrate mode, Veeam Backup Free Edition performs an additional check. If you have selected to use the Migrate mode and the configuration backup does not meet the requirements, Veeam Backup Free Edition will offer you to switch to the Restore mode. In the Restore mode, Veeam Backup Free Edition will perform additional rescan of VM replicas, backup repositories and tape libraries connected to the backup server. The database will be updated to include information about new restore points, and subsequent job sessions will be working in a proper way.

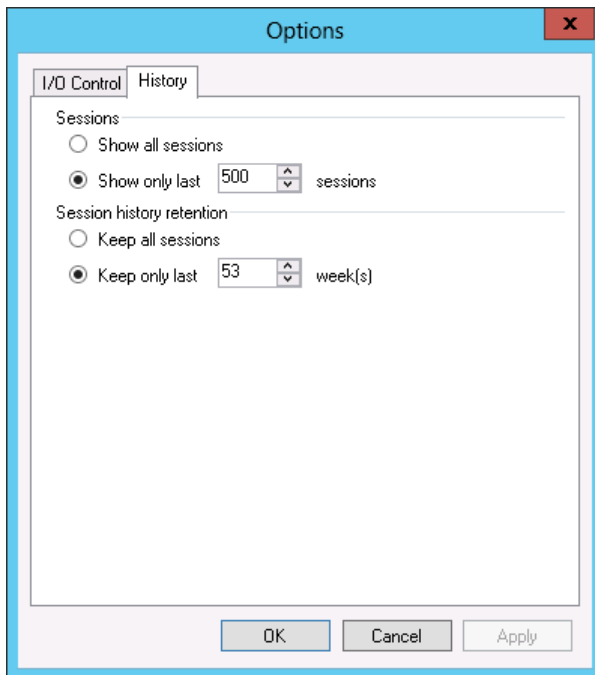
Specifying Veeam Backup & Replication Options

You can set up general settings for Veeam Backup Free Edition. General settings are applied to all jobs, backup infrastructure components and other objects managed by the backup server.

Specifying Session History Settings

You can specify session history settings for jobs performed on the backup server.

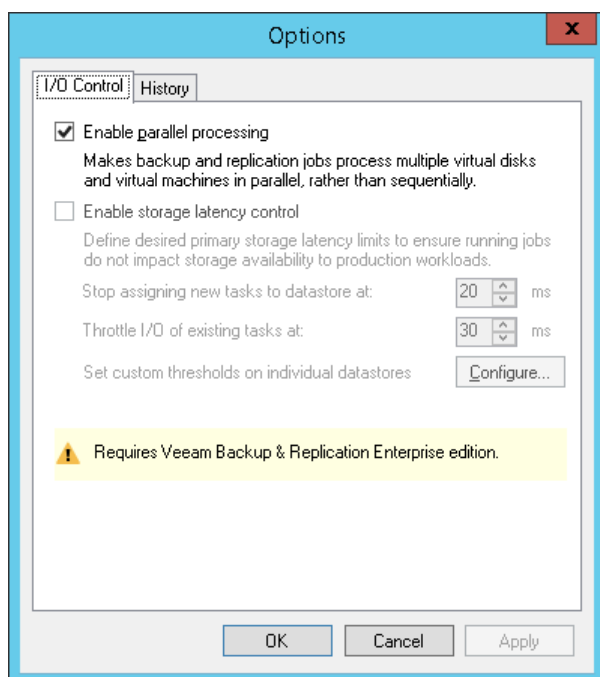
1. From the main menu, select **Options**.
2. Click the **History** tab.
3. In the **Sessions** section, specify the number of sessions to display in the **Sessions** list of the **History** view.
4. In the **Session history retention** section, specify the number of weeks for which Veeam Backup Free Edition must keep session information in the configuration database.



Specifying Data Processing Settings

You can select the data processing mode for VM disks in jobs (parallel or sequential). To specify data processing settings:

1. From the main menu, select **Options**.
2. Click the **I/O Control** tab.
3. By default, Veeam Backup Free Edition uses the parallel data processing mode for VM disks. To disable parallel processing, clear the **Enable parallel processing** check box. In this case, Veeam Backup Free Edition will process VM disks sequentially, one by one.

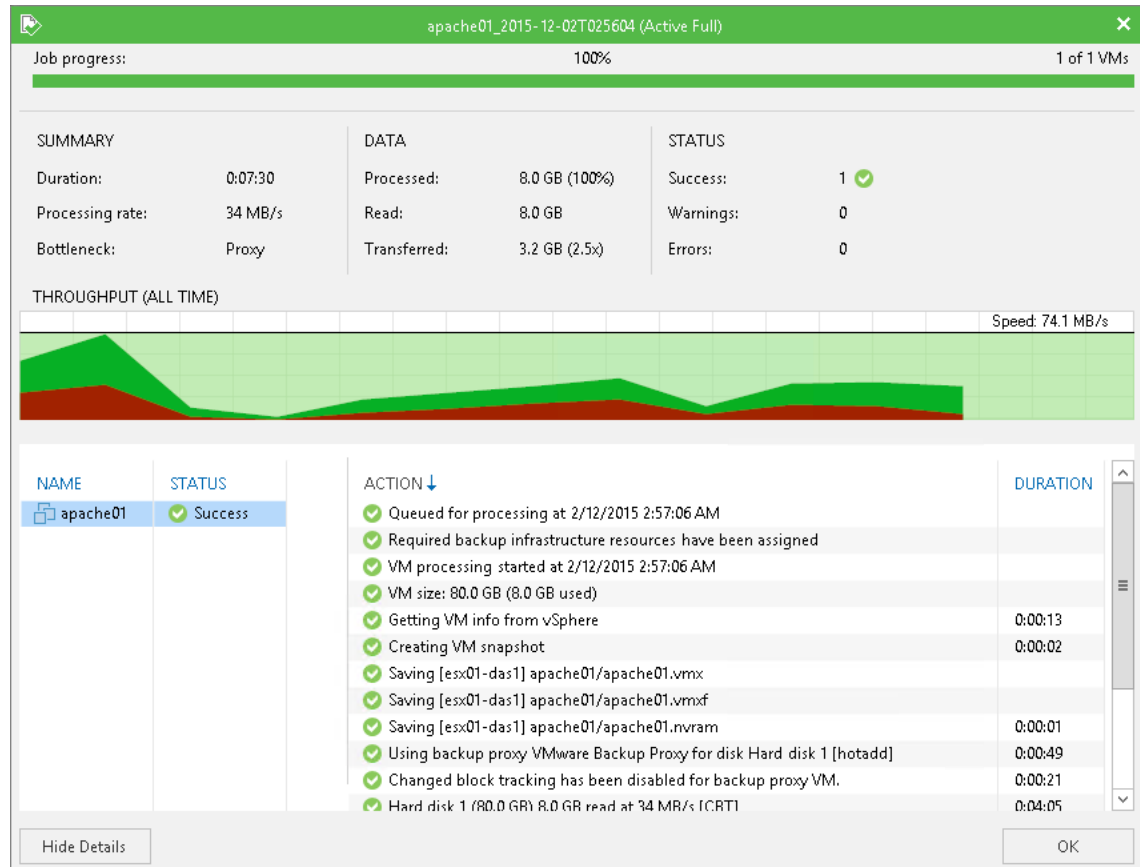


Viewing Realtime Statistics

You can view detailed statistics on every VeeamZIP task.

To view statistics for a VeeamZIP task, do either of the following:

- Open the **History** view. In the inventory pane select **Jobs**. In the working area, double-click the necessary task.
- Open the **History** view. In the inventory pane select **Jobs**. In the working area, right-click the necessary task and select **Statistics**.



Assigning Roles to Users

You can assign one of the following roles to users or groups of users who plan to work with Veeam Backup Free Edition:

- Veeam Restore Operator
- Veeam Backup Viewer
- Veeam Backup Operator
- Veeam Backup Administrator

A role assigned to the user defines the user activity scope: what operations in Veeam Backup Free Edition the user can perform. Role security settings affect the following operations:

- Starting and stopping tasks
- Performing restore operations

Users having different roles can perform a different set of operations:

Role	Operations
Veeam Restore Operator	Can perform restore operations.
Veeam Backup Viewer	Has the “read-only” access to Veeam Backup Free Edition. Can view existing task session details.
Veeam Backup Operator	Can create VeeamZIP files.
Veeam Backup Administrator	Can perform all administrative activities in Veeam Backup Free Edition.

You can assign several roles to one user. For example, if the user should be able to start jobs and perform restore operations, you can assign the **Veeam Backup Operator** and **Veeam Restore Operator** roles to this user.

To assign a role to the user or user group:

1. From the main menu, select **Users and Roles**.
2. Click **Add**.
3. In the **User or group** field, enter a name of a user or user group in the *DOMAIN\USERNAME* format.
4. From the **Role** list, select the necessary role to be assigned.

Important!

The user account under which the Veeam Backup Service runs must be assigned the Veeam Backup Administrator role. By default, during installation the Veeam Backup Administrator role is assigned to users in the Local Administrators group. If you change the default settings, make sure that you assign the Veeam Backup Administrator role to the necessary user account.

If the Veeam Backup Service is started under the LocalSystem account, you do not need to assign any roles to this account.

