



Veeam Backup & Replication

Version 9.5 Update 4

User Guide for VMware vSphere

April, 2019

© 2019 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.

NOTE:

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

Contents

CONTACTING VEEAM SOFTWARE	12
ABOUT THIS DOCUMENT	13
ABOUT VEEAM BACKUP & REPLICATION	14
PLANNING AND PREPARATION	15
PLATFORM SUPPORT	16
SYSTEM REQUIREMENTS	18
REQUIRED PERMISSIONS	31
USED PORTS	34
NAMING CONVENTIONS	52
SECURITY CONSIDERATIONS	53
KERBEROS AUTHENTICATION FOR GUEST OS PROCESSING	55
LICENSING	59
LICENSED OBJECTS	60
TYPES OF LICENSES	61
OBTAINING LICENSE	62
INSTALLING LICENSE	63
VIEWING LICENSE INFORMATION	65
VIEWING LICENSED OBJECTS	67
REVOKING LICENSE	69
EXCEEDING LICENSE LIMIT	70
LICENSE EXPIRATION	72
UPDATING LICENSE	73
Updating License Manually	74
Updating License Automatically	76
AUTOMATIC LICENSE USAGE REPORTING	79
COMMUNITY EDITION AND FULL VERSION	80
GETTING TO KNOW VEEAM BACKUP & REPLICATION	81
VEEAM BACKUP & REPLICATION UI	82
Main Menu	83
Navigation Pane	84
Ribbon and Tabs	85
Views	86
Working Area	88
Changing Color Theme	89
PRODUCT EDITIONS	90
DEPLOYMENT	91

INSTALLING VEEAM BACKUP & REPLICATION	92
Before You Begin	93
UPGRADING TO VEEAM BACKUP & REPLICATION 9.5 UPDATE 4	105
UPDATING VEEAM BACKUP & REPLICATION	107
UNINSTALLING VEEAM BACKUP & REPLICATION	109
INSTALLING VEEAM BACKUP & REPLICATION CONSOLE	110
Before You Begin	111
INSTALLING VEEAM BACKUP & REPLICATION IN UNATTENDED MODE	116
Before You Begin	117
Installation Command-Line Syntax	118
INSTALLING UPDATES IN UNATTENDED MODE	135
BACKUP INFRASTRUCTURE	137
BACKUP INFRASTRUCTURE COMPONENTS	138
Backup Server	139
Backup & Replication Console	153
Virtualization Servers and Hosts	156
Backup Proxy	183
Backup Repository	203
External Repository	274
Scale-Out Backup Repository	289
Guest Interaction Proxy	328
Gateway Server	331
Mount Server	334
Veeam vPower NFS Service	336
WAN Accelerators	338
Log Shipping Servers	339
Tape Servers	340
NDMP Servers	341
Veeam Backup Enterprise Manager	342
DEPLOYMENT SCENARIOS	343
Simple Deployment	344
Advanced Deployment	345
Distributed Deployment	347
RESOURCE SCHEDULING	348
Limitation of Concurrent Tasks	349
Limitation of Read and Write Data Rates for Backup Repositories	352
Network Traffic Management	353
Performance Bottlenecks	360
LOCATIONS	362

Creating and Assigning Locations to Infrastructure Objects	365
Editing Locations	367
Deleting Locations	368
Exporting and Importing Locations List	369
VEEAM BACKUP & REPLICATION SETTINGS.....	370
Specifying I/O Settings	371
Specifying Email Notification Settings	374
Specifying SNMP Settings	377
Specifying Other Notification Settings.....	381
Specifying Session History Settings	384
Configuring Security Settings	385
ROLES AND USERS.....	396
UPDATE NOTIFICATION	398
Installing Updates	399
SERVER COMPONENTS UPGRADE	400
LOGGING	402
Exporting Logs.....	403
CONFIGURATION BACKUP AND RESTORE.....	407
Configuration Backup	408
Restoring Configuration Data	415
Migrating Configuration Database.....	428
BACKUP	429
ABOUT BACKUP	430
How Backup Works.....	431
Backup Architecture	433
Backup Chain.....	436
Changed Block Tracking	458
Data Compression and Deduplication	460
Data Exclusion	463
Transaction Consistency	474
Guest Processing.....	479
Microsoft SQL Server Logs Backup and Restore	492
Oracle Logs Backup and Restore.....	502
Backup Job Scheduling.....	512
Health Check for Backup Files	519
Compact of Full Backup File	524
Resume on Disconnect	526
Snapshot Hunter	527
CREATING BACKUP JOBS.....	529

Before You Begin	530
PERFORMING ACTIVE FULL BACKUP	564
QUICK BACKUP	565
Retention Policy for Quick Backups	566
Performing Quick Backup	567
IMPORTING BACKUPS	568
Importing Encrypted Backups	570
Importing Transaction Logs.....	571
Importing Backup Files from Scale-Out Backup Repositories	572
EXPORTING BACKUPS.....	573
Performing Export.....	574
Viewing Session Statistics	579
MANAGING BACKUPS	581
Viewing Properties	582
Removing from Configuration	583
Deleting from Disk	584
Removing Missing Restore Points.....	585
MANAGING CAPACITY TIER DATA.....	588
Moving to Capacity Tier.....	589
Copying to Performance Tier	591
Viewing Capacity Tier Sessions Statistic.....	592
MANAGING JOBS.....	596
Editing Job Settings	597
Cloning Jobs	598
Disabling and Removing Jobs.....	600
Starting and Stopping Jobs	601
Starting and Stopping Transaction Log Backup Jobs.....	603
Reconfiguring Jobs with Microsoft SQL Server VMs.....	605
REPORTING	606
Viewing Real-Time Statistics	607
Viewing Job Session Results.....	610
Viewing Job and Job Session Reports.....	611
REPLICATION	612
ABOUT REPLICATION.....	613
How Replication Works	614
Replication Architecture.....	616
Replication Chain	620
Changed Block Tracking	621
Advanced Replication Technologies	622

Network Mapping and Re-IP.....	626
CREATING REPLICATION JOBS	627
Before You Begin	628
MANAGING REPLICAS	662
Viewing Replica Properties	663
Removing from Configuration	664
Deleting from Disk	665
REPLICA FAILOVER AND FAILBACK.....	666
Replica Failover	667
Permanent Failover	673
Failover Plan	675
Planned Failover	685
Undo Failover	691
Replica Failback	694
Commit Failback.....	708
Undo Failback	710
VEEAMZIP	712
CREATING VEEAMZIP BACKUPS.....	713
BACKUP COPY	715
ABOUT BACKUP COPY	716
How Backup Copy Works.....	717
Backup Copy Architecture	718
Restore Point Selection	720
Backup Copy Job	722
Retention Policy for Backup Copy Jobs.....	728
Health Check for Backup Files	748
Compact of Full Backup File	750
Active Full Backup Copies.....	752
Backup Copy Jobs Mapping	753
CREATING BACKUP COPY JOBS	756
Before You Begin	757
EDITING BACKUP COPY JOBS	773
VIEWING BACKUP COPY PROPERTIES	775
LINKING BACKUP JOBS TO BACKUP COPY JOBS	776
STARTING BACKUP COPY INTERVALS MANUALLY.....	778
CREATING ACTIVE FULL BACKUPS	779
REMOVING BACKUPS FROM TARGET REPOSITORIES.....	780
REMOVING MISSING RESTORE POINTS	782
VM COPY.....	785

COPYING VMs	786
Before You Begin	787
FILE COPY	803
CREATING FILE COPY JOBS	804
Before You Begin	805
COPYING FILES AND FOLDERS MANUALLY.....	811
MANAGING FOLDERS.....	812
EDITING AND DELETING FILES	813
QUICK MIGRATION	814
QUICK MIGRATION ARCHITECTURE	815
MIGRATING VMs.....	816
Before You Begin	817
RECOVERY VERIFICATION	824
SUREBACKUP	825
How SureBackup Works.....	826
Backup Recovery Verification Tests	827
Application Group	832
Virtual Lab	842
SureBackup Job.....	862
XML Files with VM Roles Description.....	883
Manual Recovery Verification	885
SUREREPLICA	886
How SureReplica Works.....	887
Replica Recovery Verification Tests	889
Application Group	890
Virtual Lab Configuration	891
SureBackup Job for VM Replicas.....	896
ON-DEMAND SANDBOX.....	899
ON-DEMAND SANDBOX FOR STORAGE SNAPSHOTS	900
MIXED SCENARIOS.....	902
CONFIGURING ON-DEMAND SANDBOX.....	903
DATA RECOVERY	905
INSTANT VM RECOVERY	906
Performing Instant VM Recovery.....	907
ENTIRE VM RESTORE	920
Quick Rollback	921
Restoring Entire VM	923
VM FILES RESTORE	939
Restoring VM Files	940

VIRTUAL DISKS RESTORE	945
Restoring Virtual Disks	946
EC2 INSTANCE DISKS EXPORT.....	954
Exporting Disks	955
GUEST OS FILE RECOVERY	961
Restore from FAT, NTFS or ReFS	962
Restore from Linux, Unix and Other File Systems	977
Restore from Other File Systems	987
Viewing File Restore Session Statistics	988
APPLICATION ITEMS RESTORE	989
Using Veeam Explorer for Microsoft Active Directory	990
Using Veeam Explorer for Microsoft Exchange	991
Using Veeam Explorer for Microsoft SharePoint	992
Using Veeam Explorer for Microsoft OneDrive for Business	993
Using Veeam Explorer for Microsoft SQL Server	994
Using Veeam Explorer for Oracle.....	995
RESTORE TO MICROSOFT AZURE	996
HOW RESTORE TO MICROSOFT AZURE WORKS.....	997
RESTORE WORKFLOW	999
CONFIGURING INITIAL SETTINGS	1000
Adding Microsoft Azure Accounts.....	1001
Adding Microsoft Azure Stack Accounts	1007
Creating Custom Role for Azure Account.....	1011
Configuring Helper Appliances	1013
Configuring Azure Proxies	1019
Removing Azure Proxies.....	1028
CREATING BACKUP FILES	1029
RESTORING MACHINES	1030
Before You Begin	1031
RESTORE TO AMAZON EC2	1046
HOW RESTORE TO AMAZON EC2 WORKS	1047
AWS ACCOUNT PERMISSIONS	1048
RESTORING MACHINES	1050
Before You Begin	1051
SECURE RESTORE.....	1065
HOW SECURE RESTORE WORKS.....	1067
ANTIVIRUS XML CONFIGURATION FILE	1068
VIEWING MALWARE SCAN RESULTS.....	1072
STAGED RESTORE.....	1073

VCLLOUD DIRECTOR SUPPORT	1075
VIEWING VMWARE VCLLOUD DIRECTOR VMs	1076
BACKUP AND RESTORE OF VAPPS.....	1077
BACKUP OF VCLLOUD DIRECTOR VMs	1078
Data to Back Up	1079
vCD Backup Jobs	1081
Performing Backup of VMware vCloud Director VMs	1082
Creating VeeamZIP Files for VMware vCloud Director VMs	1084
RESTORE OF VCLLOUD DIRECTOR VMs.....	1085
Restoring Regular VMs to vCloud Director.....	1086
Restoring Linked Clone VMs to vCloud Director.....	1087
Performing Instant VM Recovery for VMs	1089
Restoring vCloud vApps	1101
Restoring VMs into vCloud vApp	1112
Restoring Entire VMs into vSphere Infrastructure.....	1123
Restoring VM Files	1124
Restoring VM Hard Disks	1125
Restoring VM Guest OS Files	1126
VMWARE CLOUD ON AWS SUPPORT.....	1127
WAN ACCELERATION	1130
GLOBAL DATA DEDUPLICATION	1131
WAN ACCELERATORS	1132
WAN Accelerator Sizing.....	1134
Adding WAN Accelerators	1138
Removing WAN Accelerators.....	1144
WAN GLOBAL CACHE	1145
Many to One WAN Acceleration.....	1146
Population of Global Cache	1147
HOW WAN ACCELERATION WORKS	1152
DATA BLOCK VERIFICATION	1153
DATA TRANSPORT ON WAN DISCONNECT	1154
DATA ENCRYPTION.....	1155
ENCRYPTION STANDARDS.....	1157
ENCRYPTION ALGORITHMS	1158
Encryption Keys	1159
How Data Encryption Works.....	1164
How Data Decryption Works.....	1166
How Decryption Without Password Works.....	1168
ENCRYPTED OBJECTS	1170

Backup Job Encryption	1171
Backup Copy Job Encryption	1173
VeeamZIP Encryption	1176
Tape Encryption	1177
ENCRYPTION BEST PRACTICES	1179
RESTORING DATA FROM ENCRYPTED BACKUPS	1181
Decrypting Data with Password	1182
Decrypting Data Without Password	1183
RESTORING ENCRYPTED DATA FROM TAPES	1187
Decrypting Tapes with Password	1188
Decrypting Tapes Without Password	1190
INTEGRATION WITH STORAGE SYSTEMS	1194
TAPE DEVICES SUPPORT	1195
VEEAM AGENT MANAGEMENT	1196
VEEAM CLOUD CONNECT	1197
ADVANCED VMWARE VSPHERE FEATURES	1198
VM TAGS	1199
ENCRYPTED VMS	1201
STORAGE PROFILES	1203
VEEAM BACKUP & REPLICATION UTILITIES	1204
EXTRACT UTILITY	1205
Using Extract Utility in GUI	1206
Using Extract Utility in Interactive Mode	1207
Using Extract Utility from Command Line	1208
VEEAM.BACKUP.DBCONFIG.EXE UTILITY	1211
Using Veeam.Backup.DBConfig.exe Utility	1212
VEEAM BACKUP VALIDATOR	1216
Working with Veeam Backup Validator	1217
Validating Content of Backup File	1218

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, visit the Veeam Customer Support 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, visit www.veeam.com/contacts.html.

Online Support

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

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

About This Document

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

Intended Audience

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

Document Revision History

Revision #	Date	Change Summary
Revision 8	4/14/2019	Updated section: Backup Copy .
Revision 7	3/26/2019	Updated for Veeam Backup & Replication 9.5 Update 4a: System Requirements .
Revision 6	3/1/2019	<ul style="list-style-type: none">Information about data migration check for copy and restore operations from external repositories added: Locations.Updated sections: Types of Licenses, Obtaining License, Viewing Licensed Objects and Revoking License.
Revision 5	2/25/2019	Information about license details added: Viewing License Information .
Revision 4	2/14/2019	Information about how retention policy for deleted items works updated: Retention Policy for Deleted Items .
Revision 3	2/6/2019	<ul style="list-style-type: none">Information about minimal set of permissions to perform restore to Amazon EC2 added: AWS Account Permissions.Information about creating a custom role with minimal permissions to perform restore to Microsoft Azure added: Creating Custom Role for Azure Account.
Revision 2	1/30/2019	System requirements for backup infrastructure components updated: System Requirements .
Revision 1	1/22/2019	Initial version of the document for Veeam Backup & Replication 9.5 Update 4.

About Veeam Backup & Replication

Veeam® Backup & Replication™ is a backup solution developed for VMware vSphere and Microsoft Hyper-V virtual environments. Veeam Backup & Replication provides a set of features for performing data protection and disaster recovery tasks.

This document contains a high-level overview of Veeam Backup & Replication, its architecture, features, data protection and disaster recovery concepts necessary to understand Veeam Backup & Replication background operations and processes.

Planning and Preparation

Before you install Veeam Backup & Replication, you must make sure that the virtual environment and machines that you plan to use as backup infrastructure components meet product hardware recommendations and system requirements.

Platform Support

Veeam Backup & Replication provides support for the following versions of the VMware vSphere platform.

Virtual Infrastructure

Specification	Requirement
Platform	<ul style="list-style-type: none">vSphere 6.xvSphere 5.xVMware Cloud on AWS
Hypervisor	<ul style="list-style-type: none">ESXi 6.xESXi 5.x <p>Free ESXi is not supported. Veeam Backup & Replication leverages vSphere and vStorage APIs that are disabled by VMware in free ESXi.</p>
Management Server (optional)	<ul style="list-style-type: none">vCenter Server 6.x (optional)vCenter Server 5.x (optional)

VMs

Specification	Requirement
Virtual Hardware	<ul style="list-style-type: none">All types and versions of virtual hardware are supported, including 62 TB VMDK.Virtual machines with disks engaged in SCSI bus sharing are not supported, because VMware does not support snapshotting such VMs.RDM virtual disks in physical mode, independent disks, and disks connected via in-guest iSCSI initiator are not supported, and are skipped from processing automatically. Network shares and mount points targeted to 3rd party storage devices are also skipped as these volumes/disks are not visible in the VM configuration file.
OS	<ul style="list-style-type: none">All operating systems supported by VMware.Application-aware processing for Microsoft Windows 2003 SP1 and later except Nano Server, due to the absence of VSS framework.
Software	<ul style="list-style-type: none">VMware Tools (optional, recommended). VMware Tools are required for the following operations: application-aware processing, file-level restore from Microsoft Windows guest OS and SureBackup testing functions.Open VM Tools (OVT, optional). Open VM Tools are a set of services and modules used by VMware for interaction with VMs running Linux or other VMware supported Unix-like guest operating systems.All latest OS service packs and patches (required for application-aware processing).

vCloud Director

Specification	Requirement
vCloud Director	vCloud Director 8.x up to 9.5

File-Level Restore

OS	Supported File Systems
Microsoft Windows	<ul style="list-style-type: none">FAT, FAT32NTFSReFS (ReFS is supported only if Veeam Backup & Replication is installed on Microsoft Windows Server 2012 or later).
Linux	<ul style="list-style-type: none">ext2, ext3, ext4ReiserFSJFSXFSBtrfs <p>DRBD (Distributed Replicated Block Devices) are not supported.</p>
BSD	UFS, UFS2
Mac	HFS, HFS+ (volumes up to 2 TB)
Micro Focus OES	<p>File-level restore is supported for Micro Focus Open Enterprise Server (Micro Focus OES). Micro Focus NetWare is not supported (Veeam Backup & Replication may fail to detect NSS volumes).</p> <p>AD-enabled NSS volumes on Open Enterprise Server 2015 are supported. Restore of NSS file/folder permissions is not supported.</p>
Solaris	<ul style="list-style-type: none">UFSZFS (except any pool versions of Oracle Solaris) <p>The FLR appliance uses module ZFSonLinux version 0.7.0. For this reason, Veeam Backup & Replication supports only those versions of pools and features that are available in ZFSonLinux version 0.7.0.</p>

You cannot restore pipes and other file system objects. File-level restore supports recovery of files and folders only.

The multi-OS wizard works not only with basic disks, but also Linux LVM (Logical Volume Manager) and ZFS pools. Encrypted LVM volumes are not supported.

System Requirements

Make sure that servers that you plan to use as backup infrastructure components meet system requirements listed below.

- [Backup server](#)
- [Veeam Backup & Replication console](#)
- [Backup proxy server](#)
- [Backup repository server](#)
- [WAN accelerator](#)
- [Backup target](#)
- [Storage integration](#)
- [Tape](#)
- [Tape server](#)
- [Gateway server](#)
- [Mount server](#)
- [Veeam Backup Enterprise Manager](#)
- [VSS-aware applications](#)
- [Veeam Explorers](#)

Limitations and Recommendations

Coexistence with Mission-Critical Production Servers

It is not recommended that you install Veeam Backup & Replication and its components on mission-critical machines in the production environment such as vCenter Server, Domain Controller, Microsoft Exchange Server, Small Business Server/ Windows Server Essentials and so on. If possible, install Veeam Backup & Replication and its components on dedicated machines. Backup infrastructure component roles can be co-installed.

Microsoft Windows Server Core

You can assign roles of a backup proxy, backup repository, WAN accelerator, Veeam Cloud Connect infrastructure components and tape infrastructure components to machines running Microsoft Windows Server Core.

Mind that you cannot install Veeam Backup & Replication and Veeam Backup Enterprise Manager on a machine running Microsoft Windows Server Core.

Domain Member

The machine on which you plan to install Veeam Backup & Replication does not necessarily need to be a domain member. However, if you plan to restore Microsoft Exchange items from the Veeam Backup Enterprise Manager UI, you must install Veeam Backup Enterprise Manager on the domain member server from the Microsoft Active Directory forest in which Microsoft Exchange mailboxes are located.

All-in-One Installations

For all-in-one installations, you can subtract 2 GB of memory resources from each but one role. These 2 GB are allotted to the OS itself, assuming each component is installed on the dedicated server.

Backup Server

Specification	Requirement
Hardware	<p><i>CPU:</i> x86-64 processor (4 cores recommended).</p> <p><i>Memory:</i> 4 GB RAM plus 500 MB RAM for each concurrent job. Memory consumption varies according to number of VMs in the job, size of VM metadata, size of production infrastructure, etc.</p> <p>Additionally, for users with tape installations (for file to tape jobs processing more than 1,000,000 files):</p> <ul style="list-style-type: none">• 1,5 GB RAM for file to tape backup for each 1,000,000 files• 2,6 GB RAM for file restore for each 1,000,000 files• 1,3 GB RAM for catalog jobs for each 1,000,000 files <p><i>Disk Space:</i> 5 GB* for product installation and 4.5 GB for Microsoft .NET Framework 4.6 installation. 10 GB per 100 VM for guest file system catalog folder (persistent data). Additional free disk space for Instant VM Recovery cache folder (non-persistent data, at least 10 GB recommended).</p> <p><i>Network:</i> 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for offsite backup and replication. High latency and reasonably unstable WAN links are supported.</p> <p>*Here and throughout this document GB is considered as 2³⁰ bytes, TB as 2⁴⁰ bytes.</p>
OS	<p>Only 64-bit version of the following operating systems are supported*:</p> <ul style="list-style-type: none">• Microsoft Windows Server 2019• Microsoft Windows Server 2016• Microsoft Windows Server 2012 R2• Microsoft Windows Server 2012• Microsoft Windows Server 2008 R2 SP1• Microsoft Windows Server 2008 SP2• Microsoft Windows 10 (including version 1903)• Microsoft Windows 8.x• Microsoft Windows 7 SP1 <p>*Running Veeam backup server or any of Veeam backup infrastructure components on Insider versions of Microsoft Windows OS (both Client and Server) is not supported.</p>

Software	<p>During setup, the system configuration check is performed to determine if all prerequisite software is available on the machine where you plan to install Veeam Backup & Replication. If some of the required software components are missing, the setup wizard will offer you to install missing software automatically. This refers to:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 4.6 • Microsoft Windows Installer 4.5 • Microsoft SQL Server Management Objects • Microsoft SQL Server System CLR Types • Microsoft Report Viewer Redistributable 2015 • Microsoft Universal C Runtime <p>The following software must be installed manually:</p> <ul style="list-style-type: none"> • Microsoft PowerShell 2.0. • Firefox, Google Chrome, Microsoft Edge or Microsoft Internet Explorer 10.0 or later.
SQL Database	<p>Local or remote installation of the following versions of Microsoft SQL Server (both Full and Express Editions are supported):</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 (Microsoft SQL Server 2016 SP1 Express Edition is included in the setup)* • Microsoft SQL Server 2014 • Microsoft SQL Server 2012 (Microsoft SQL Server 2012 SP4 Express Edition is included in the setup)** • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 <p>Veeam Backup & Replication and Veeam Backup Enterprise Manager configuration databases can be deployed in Microsoft SQL AlwaysOn Availability Groups. For more information, see the Veeam KB2301 article.</p> <p>*For machines running Microsoft Windows Server 2012 or later. **For machines running Microsoft Windows 7, Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2.</p>

Mind the following:

- If you plan to back up VMs running Microsoft Windows Server 2012 R2 or later, and Data Deduplication is enabled for some VM volumes, it is recommended that you deploy the Veeam Backup & Replication console and mount server on a machine running same or later version of Microsoft Windows Server with Data Deduplication feature enabled. Otherwise, some types of restore operations for these VMs (such as Microsoft Windows File Level Recovery) may fail.
- Due to its limitations, Microsoft SQL Server Express Edition can only be used for evaluation purposes or in case of a small-scale production environment. For environments with a lot of VMs, it is necessary to install a fully functional commercial version of Microsoft SQL Server.

For more information, see [Backup Server](#).

Veeam Backup & Replication Console

Specification	Requirement
Hardware	<p><i>CPU:</i> x86-64 processor.</p> <p><i>Memory:</i> 2 GB RAM</p> <p><i>Disk Space:</i> 500 MB for product installation and 4.5 GB for Microsoft .NET Framework 4.5.2 installation.</p> <p><i>Network:</i> 1 Mbps connection to the backup server. High latency and low bandwidth impact user interface responsiveness.</p>
OS	<p>Only 64-bit version of the following operating systems are supported:</p> <ul style="list-style-type: none">• Microsoft Windows Server 2019• Microsoft Windows Server 2016• Microsoft Windows Server 2012 R2• Microsoft Windows Server 2012• Microsoft Windows Server 2008 R2 SP1• Microsoft Windows Server 2008 SP2• Microsoft Windows 10 (including version 1903)• Microsoft Windows 8.x• Microsoft Windows 7 SP1
Software	<ul style="list-style-type: none">• Microsoft .NET Framework 4.6 (included in the setup)• Windows Installer 4.5 (included in the setup)• Microsoft PowerShell 2.0• Firefox, Google Chrome, Microsoft Edge or Microsoft Internet Explorer 10.0 or later

For more information, see [Backup & Replication Console](#).

Backup Proxy Server

Specification	Requirement
Hardware	<p><i>CPU:</i> modern x86 processor with minimum of 2 cores (vCPUs), plus 1 core (vCPU) for each additional concurrent task. Using faster processors improves data processing performance. For more information, see Limitation of Concurrent Tasks.</p> <p><i>Memory:</i> 2 GB RAM plus 200 MB for each concurrent task. Using faster memory (DDR3/DDR4) improves data processing performance.</p> <p><i>Disk Space:</i> 300 MB.</p> <p><i>Network:</i> 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.</p>

OS	<p>Both 32-bit and 64-bit versions of the following operating systems are supported:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 (including version 1809) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows 10 (including version 1903) • Microsoft Windows 8.x • Microsoft Windows 7 SP1 • Microsoft Windows Vista SP2
Software	<p>For a vSphere 5.5 or later backup proxy server running on Microsoft Windows Server 2008 or earlier: Microsoft Visual C++ 2008 SP1 Redistributable Package (x64). Installation package can be downloaded from http://vee.am/runtime.</p>

For more information, see [Backup Proxy](#).

IMPORTANT!

To protect VMs running on ESXi 5.5 and newer, you must deploy backup proxies on machines running a 64-bit version of Microsoft Windows. VDDK 5.5 and newer does not support 32-bit versions of Microsoft Windows.

Backup Repository Server

Specification	Requirement
Hardware	<p><i>CPU:</i> x86 processor (x86-64 recommended).</p> <p><i>Memory:</i> 4 GB RAM, plus up to 2 GB RAM (32-bit OS) or up to 4 GB RAM (64-bit OS) for each concurrent job depending on backup chain's length and backup files sizes. For more information, see Limitation of Concurrent Tasks.</p> <p><i>Network:</i> 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.</p>

OS	<p>Both 32-bit and 64-bit (recommended) versions of the following operating systems are supported:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 (including version 1809) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows 10 (including version 1903) • Microsoft Windows 8.x • Microsoft Windows 7 SP1 • Microsoft Windows Vista SP2 • Linux (bash shell, SSH and Perl are required). Check the full list of required Perl modules in the Veeam KB2216 article. <p>64-bit edition of Linux must be able to run 32-bit programs. Pure 64-bit Linux editions are not supported (Perl installation must support 32-bit variables).</p>
----	--

For more information, see [Backup Repository](#).

NOTE:

If you plan to use a Microsoft Windows backup repository with Data Deduplication, make sure that you set up the Microsoft Windows server correctly. For more information, see the [Veeam KB1893](#) article.

WAN Accelerator

Specification	Requirement
Hardware	<p><i>CPU:</i> x86-64 processor. Using multi-core processors improves data processing performance, and is highly recommended on WAN links faster than 10 Mbps.</p> <p><i>Memory:</i> 8 GB RAM. Using faster memory (DDR3/DDR4) improves data processing performance.</p> <p><i>Disk Space:</i> Disk space requirements depend on the WAN Accelerator role. For more information, see WAN Accelerator Sizing.</p> <p><i>Network:</i> 1 Gbps or faster for on-site backup and replication, and 1 Mbps or faster for off-site backup and replication. High latency and reasonably unstable WAN links are supported.</p>
OS	<p>Only 64-bit version of the following operating systems are supported:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 (including version 1809) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2008 SP2 • Microsoft Windows 10 (including version 1903) • Microsoft Windows 8.x • Microsoft Windows 7 SP1 • Microsoft Windows Vista SP2

For more information, see [WAN Accelerators](#).

NOTE:

Global cache is not leveraged by Source WAN Accelerators, and so does not need to be allocated and populated on WAN Accelerators used only as source ones.

Backup Target

Backups can be performed to the following disk-based storage:

- Local (internal) storage of the backup repository server.
- Direct Attached Storage (DAS) connected to the backup repository server, including external USB/eSATA drives, USB pass through and raw device mapping (RDM) volumes.
- Storage Area Network (SAN). Backup repository server must be connected into the SAN fabric via hardware or virtual HBA, or software iSCSI initiator.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) share (direct operation), or NFS share (must be mounted on a Linux backup repository server).
- Dell EMC Data Domain (DD OS version 5.6, 5.7, 6.0, 6.1, 6.2) with DDBoost license. Both Ethernet and Fibre Channel (FC) connectivity is supported.
- ExaGrid (firmware version 5.0.0 or later).
- HPE StoreOnce (firmware version 3.15.1 or later) with Catalyst license. Both Ethernet and Fibre Channel (FC) connectivity is supported.
- Quantum DXi (firmware version 3.4.0 or later) with NAS support (DXi4700, DXi4700, DXi6900, DXi6900-S).

Storage Integration

Backup from Storage Snapshots and Veeam Explorer for Storage Snapshots are supported for the following storage devices:

Cisco HyperFlex (HX-Series/SpringPath)

- NFS connectivity only
- HyperFlex 2.0 or later (Backup from Storage Snapshots, Full Integration mode)
- Basic authentication is not supported for SSO users in HyperFlex starting from version 3.0

Dell EMC VNX, VNX2, VNXe and Unity

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Dell EMC VNXe/Unity OE versions 3.x through 4.4

HPE 3PAR StoreServ

- Fibre Channel (FC) or iSCSI connectivity
- 3PAR OS versions 3.1.2 up to 3.3.1 MU2

iSCSI VLAN tags are supported. Virtual Domains are supported.

HPE Nimble Storage AF-Series, HF-Series and CS-Series

- Fibre Channel (FC) or iSCSI connectivity
- Nimble OS 2.3 or later

HPE StoreVirtual (LeftHand / P4000 series) and StoreVirtual VSA

- iSCSI connectivity only
- LeftHand OS versions 9.5 through 12.7
- HPE SV3200 (LeftHand OS version 13) is not supported

Huawei OceanStor

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Huawei OceanStor V3 and F V3 Series with software version V300R006 or later
- Huawei OceanStor Dorado V3 Series with software version V300R001 or later
- Huawei OceanStor V5 and F V5 Series with software version V500R007 or later

IBM Spectrum Virtualize (IBM Storwize, IBM SVC, Lenovo Storage V series)

- Fibre Channel (FC) or iSCSI connectivity
- IBM Spectrum Virtualize OS 7.6 or later

INFINIDAT Infinibox F-series

- NFS, Fibre Channel (FC) or iSCSI connectivity
- InfiniBox version 3.0 or later

NetApp FAS/AFF, FlexArray (V-Series), ONTAP Edge/Select/Cloud VSA and FAS OEM (IBM N series and Lenovo DM series)

- NFS, Fibre Channel, iSCSI
- ONTAP versions 8.1 up to 9.5
- 7-mode or cluster-mode
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- NetApp Synchronous SnapMirror is not supported

NetApp SolidFire/HCI

- iSCSI connectivity
- NetApp SolidFire support requires Element OS version 9.0 or later
- NetApp HCI support requires Element OS version 10.0 or later

Pure Storage FlashArray

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Purity version 4.8 or later
- Purity ActiveCluster is supported

Tape

Specification	Requirement
Hardware	LTO3 or later tape libraries (including VTL) and standalone drives are supported. Tape device must be directly attached to the backup server, to a tape server via SAS, FC or iSCSI interface. Note that VMware does not support connecting tape libraries to ESX(i) for VM pass-through.
Software	<ul style="list-style-type: none">• Tape devices without device-specific, vendor-supplied OEM drivers for Windows installed will appear in Windows Device Manager as Unknown or Generic and require enabling native SCSI commands mode.• No other backup server must be interacting with the tape device.

Tape Server

Specification	Requirement
Hardware	<p><i>CPU:</i> x86 processor (x86-64 recommended).</p> <p><i>Memory:</i> 2 GB RAM plus 200MB for each concurrent task. Restoring VMs directly from tape requires 400MB of RAM per 1TB of virtual disk size. Additionally (for file to tape jobs processing more than 1,000,000 files):</p> <ul style="list-style-type: none">• 800 MB RAM for file to tape backup for each 1,000,000 files• 800 MB RAM catalog jobs for each 1,000,000 files <p><i>Disk Space:</i> 300 MB, plus 10 GB for temporary data storage for backup and restore operations.</p> <p><i>Network:</i> 1 Gbps or faster.</p>
OS	<p>Both 32-bit and 64-bit (recommended) versions of the following operating systems are supported:</p> <ul style="list-style-type: none">• Microsoft Windows Server 2019• Microsoft Windows Server 2016 (including version 1809)• Microsoft Windows Server 2012 R2• Microsoft Windows Server 2012• Microsoft Windows Server 2008 R2 SP1• Microsoft Windows Server 2008 SP2• Microsoft Windows 10 (including version 1903)• Microsoft Windows 8.x• Microsoft Windows 7 SP1• Microsoft Windows Vista SP2

Gateway Server

Specification	Requirement
Platform	Physical or virtual machine
OS	Both 32-bit and 64-bit versions of the following operating systems are supported: <ul style="list-style-type: none">• Microsoft Windows Server 2019• Microsoft Windows Server 2016 (including version 1809)• Microsoft Windows Server 2012 R2• Microsoft Windows Server 2012• Microsoft Windows Server 2008 R2 SP1• Microsoft Windows Server 2008 SP2• Microsoft Windows 10 (including version 1903)• Microsoft Windows 8.x• Microsoft Windows 7 SP1• Microsoft Windows Vista SP2

For more information, see [Gateway Server](#).

Mount Server

On the mount server machine, Veeam Backup & Replication installs the Veeam Mount Service. The Veeam Mount Service requires .NET 4.6. If .NET 4.6 is not installed on the machine, Veeam Backup & Replication will install it automatically. For more information, see [Mount Server](#).

If you plan to restore VM guest OS files from VMs running Microsoft Windows ReFS, you must install Veeam Backup & Replication components on machines running specific OS versions. For more information, see [Veeam Backup & Replication Console](#).

[For Microsoft Windows 2008R2/7, Microsoft Windows 2008] Make sure that you have SHA-2 code signing support installed. Normally, this component is included in Microsoft Windows updates. For more information, see [Microsoft Docs](#).

Veeam Backup Enterprise Manager Server

A machine where you plan to install [Veeam Backup Enterprise Manager](#) must meet the system requirements. For more information, see the [System Requirements](#) section in the Enterprise Manager User Guide.

VSS-Aware Applications

You can create transactionally consistent backups or replicas of VMs that run the following applications:

Application	Requirement
Microsoft Active Directory	<p>Veeam Backup & Replication supports domain controller backups for the following operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 (including version 1809) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 • Microsoft Windows Server 2003 SP2 <p>Minimum supported domain and forest functional level is Windows 2003.</p>
Microsoft Exchange	<p>The following versions of Microsoft Exchange are supported:</p> <ul style="list-style-type: none"> • Microsoft Exchange 2019 (compatibility level*) • Microsoft Exchange 2016 • Microsoft Exchange 2013 SP1 • Microsoft Exchange 2013 • Microsoft Exchange 2010 SP1, SP2, or SP3
Microsoft SharePoint	<p>The following versions of Microsoft SharePoint Server (virtualized either on VMware or Hyper-V platform) are supported:</p> <ul style="list-style-type: none"> • Microsoft SharePoint 2019 (compatibility level**) • Microsoft SharePoint 2016 • Microsoft SharePoint 2013 • Microsoft SharePoint 2010 <p>All editions are supported (Foundation, Standard, Enterprise).</p>
Microsoft SQL Server	<p>The following versions of Microsoft SQL Server are supported (for application-aware processing and transaction log backup):</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2017 (only for Windows) • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2012 SP4 • Microsoft SQL Server 2008 R2 SP3 • Microsoft SQL Server 2008 SP4 • Microsoft SQL Server 2005 SP4 <p>All editions of Microsoft SQL Server are supported.</p> <p>The database whose logs you want to back up must use the <i>Full</i> or <i>Bulk-logged</i> recovery model. In this case, all changes of the Microsoft SQL Server state will be written to transaction logs, and you will be able to replay transaction logs to restore the Microsoft SQL Server. You can use the Microsoft SQL Server Management Studio to switch to one of these models. For more information, see Microsoft Docs.</p>

<p>Oracle on Windows OS</p>	<p>Veeam Backup & Replication supports Oracle Database 11g, 12c and 18c backups for the following operating systems:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 • Microsoft Windows Server 2003 SP2 <p>For details, see Oracle documentation at the following links:</p> <ul style="list-style-type: none"> • Oracle Database 11g Release 2 • Oracle Database 12c Release 1 • Oracle Database 12c Release 2 • Oracle Database 18c
<p>Oracle on Linux OS</p>	<p>Veeam Backup & Replication supports Oracle Database 11g Release 2 backups for the following operating systems:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 5 Update 2 or later • CentOS 5 Update 2 or later • Oracle Linux 5 Update 2 (with the Red Hat Compatible Kernel) or later • Oracle Linux 5 Update 5 (with the Unbreakable Enterprise Kernel) or later • SUSE Linux Enterprise Server 11 or later • SUSE Linux Enterprise Server 12 SP1 or later <p>For details, see Database Installation Guide for Linux.</p> <hr/> <p>Veeam Backup & Replication supports Oracle Database 12c Release 1 backups for the following operating systems:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 5 Update 6 or later • CentOS 5 Update 6 or later • Oracle Linux 5 Update 6 or later • SUSE Linux Enterprise Server 11 SP2 or later • SUSE Linux Enterprise Server 12 SP1 or later <p>For details, see Database Installation Guide for Linux.</p> <hr/> <p>Veeam Backup & Replication supports Oracle Database 12c Release 2 backups for the following operating systems:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 6 Update 4 or later • CentOS 6 Update 4 or later • Oracle Linux 6 Update 4 or later • SUSE Linux Enterprise Server 12 SP1 or later <p>For details, see Installation Guide for Linux.</p>

	<p>Veeam Backup & Replication supports Oracle Database 18c backups for the following operating systems:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 6.4 or later • Oracle Linux 6.4 • SUSE Linux Enterprise Server 12 SP1 or later <p>For details, see Database Installation Guide for Linux.</p>
<p>Oracle Database configuration</p>	<p>Automatic Storage Management (ASM) is supported for Oracle 11g and later; requires <i>ASMLib</i> present.</p> <p>Important notes:</p> <ul style="list-style-type: none"> • Oracle Real Application Clusters (RAC) are not supported. • Oracle Database Express Edition is supported for Windows-based machines only. • Configurations with different versions of Oracle Database deployed on the same server are not supported. • To create Oracle database backups, all Oracle server that use Data Guard must be added to the backup job.

* Veeam Backup & Replication supports set of technologies, features, and services of Microsoft Exchange 2016.

** Veeam Backup & Replication supports set of technologies, features, and services of Microsoft SharePoint 2016.

Veeam Explorers

- [Veeam Explorer for Microsoft Active Directory](#)
- [Veeam Explorer for Microsoft Exchange](#)
- [Veeam Explorer for Microsoft SharePoint](#)
- [Veeam Explorer for Microsoft SQL](#)
- [Veeam Explorer for Oracle](#)

Required Permissions

The accounts used for installing and using Veeam Backup & Replication must have the following permissions:

Account	Required Permission
Setup Account	The account used for product installation must have the local Administrator permissions on the target machine.
Veeam Backup & Replication Console Permissions	<p>The account used to start the Veeam Backup & Replication console must have the local Administrator permissions on the machine where the console is installed.</p> <p>To perform file-level restore for Microsoft Windows VMs, the account must have the following permissions and privileges:</p> <ul style="list-style-type: none"> • Local Administrator permissions to start the Veeam Backup & Replication console • <i>SeBackupPrivilege</i> and <i>SeRestorePrivilege</i> to connect to the Veeam backup server and start the restore process <p>In most environments, <i>SeBackupPrivilege</i> and <i>SeRestorePrivilege</i> are assigned to user accounts added to the Administrators group. For more information, see Microsoft Docs.</p> <p>Accounts that are members of the Protected Users Active Directory group cannot be used to access the backup server remotely over the Veeam Backup & Replication console. For more information, see Microsoft Docs.</p>
Veeam Backup Service Account	The account used to run the Veeam Backup Service must be a local System account or must have the local Administrator permissions on the backup server.
Target/Source Host Permissions	<p>Root permissions on the source ESX(i) host.</p> <p>Root or equivalent permissions on the Linux backup repository.</p> <p>Write permission on the target folder and share.</p> <p>If the vCenter Server is added to the backup infrastructure, an account that has administrative permissions is required. You can either grant the Administrator role to the account or configure granular vCenter Server permissions for certain Veeam Backup & Replication operations in the VMware vSphere environment. For more information, see the Required Permissions guide.</p>
Microsoft SQL Server	<p>You require different sets of Microsoft SQL permissions in the following cases:</p> <ul style="list-style-type: none"> • Installation (remote or local): current account needs CREATE ANY DATABASE permission on the SQL server level. After database creation this account automatically gets a <i>db_owner</i> role and can perform all operations with the database. If the current account does not have this permission, a Database Administrator may create an empty database in advance and grant the <i>db_owner</i> role to the account that will be used for installing Veeam Backup & Replication. • Upgrade: current account should have sufficient permissions for that database. To grant these permissions through role assignment, it is recommended that you use the account with <i>db_owner</i> role. • Operation: the account used to run Veeam Backup Service requires <i>db_datareader</i> and <i>db_datawriter</i> roles as well as permissions to execute stored procedures for the configuration database on the Microsoft SQL Server. Alternatively, you can assign <i>db_owner</i> role for this database to the service account.

Veeam Backup Enterprise Manager	<p>Local Administrator permissions on the Veeam Backup Enterprise Manager server to install Veeam Backup Enterprise Manager.</p> <p>To be able to work with Veeam Backup Enterprise Manager, users must be assigned the Portal Administrator, Restore Operator or Portal User role. For more information, see the Required Permissions section in the Enterprise Manager User Guide.</p>
Guest OS Processing	<p>The account used for guest processing of VMs that run VSS-aware applications must have the following user rights assigned:</p> <ul style="list-style-type: none"> • <i>Logon as a batch job</i> granted • <i>Deny logon as a batch job</i> not set

Required Permissions for Transactionally Consistent Backups

When creating transactionally consistent backups of VMs, make sure to configure your accounts according to the requirements listed in the following table. For more information about transactionally consistent backups, see [Guest Processing](#).

Account	Required Permission
Veeam Explorer for Microsoft SQL Server	<p>To back up Microsoft SQL Server data, the following roles must be assigned:</p> <ul style="list-style-type: none"> • <i>Administrator</i> role on the target VM. • <i>Sysadmin</i> role on the target Microsoft SQL Server. <p>To provide minimal permissions, the account must be assigned the following roles and permissions:</p> <ul style="list-style-type: none"> • SQL Server instance-level role: <i>public</i>. • Database-level roles: <i>db_backupoperator</i>, <i>db_denydatareader</i>, <i>public</i>; for system databases (master, model, msdb) – <i>db_backupoperator</i>, <i>db_datareader</i>, <i>public</i>; for system database (msdb) – <i>db_datawriter</i>. • Securables: <i>view any definition</i>, <i>view server state</i>.
Veeam Explorer for Microsoft Active Directory	To back up Microsoft Active Directory data, the account must be a member of the <i>Domain Admins</i> group.
Veeam Explorer for Microsoft Exchange	To back up Microsoft Exchange data, the account must be granted <i>Full Access</i> to Microsoft Exchange database and its log files.

<p>Veeam Explorer for Oracle</p>	<p>The account specified at the Specify Guest Processing Settings step must be configured as follows:</p> <ul style="list-style-type: none"> • For a Windows-based VM, the account must be a member of both the <i>Local Administrator</i> group and the <i>ORA_DBA</i> group (if OS authentication is used). In addition, if <i>ASM</i> is used, then such an account must be a member of the <i>ORA_ASMADMIN</i> group (for Oracle 12 and higher). • For a Linux-based VM, the account must be a Linux user elevated to <i>root</i>. <p>To back up Oracle databases, make sure the account specified on the Oracle tab has been granted <i>SYSDBA</i> privileges. You can use either the same account that was specified at the Specify Guest Processing Settings step if such an account is a member of the <i>ORA_DBA</i> group for a Windows-based VM and <i>OSASM, OSDBA and OINSTALL</i> groups for a Linux-based VM, or you can use, for example, the <i>SYS</i> Oracle account or any other Oracle account that has been granted <i>SYSDBA</i> privileges.</p>
<p>Veeam Explorer for Microsoft SharePoint</p>	<p>To back up Microsoft SharePoint server, the account must be assigned the <i>Farm Administrator</i> role.</p> <p>To back up Microsoft SQL databases of the Microsoft SharePoint Server, the account must have the same privileges as that of Veeam Explorer for Microsoft SQL Server.</p>

Used Ports

This section covers typical connection settings for the backup infrastructure components.

NOTE:

During installation, Veeam Backup & Replication automatically creates firewall rules for default ports to allow communication for the application components.

Backup Server Connections

The following table describes network ports that must be opened to ensure proper communication of the backup server with backup infrastructure components.

From	To	Protocol	Port	Notes
Virtualization Servers				
Backup server	vCenter Server	HTTPS TCP	443	Default port used for connections to vCenter Server. If you use vCloud Director, make sure you open port 443 on underlying vCenter Servers.
		HTTPS TCP	10443	Port used for communication with vCenter Server. This port is not required for VMware Cloud on AWS.
	ESX(i) server	HTTPS TCP	443	Default port used for connections to ESX(i) host. [For VMware vSphere earlier than 6.5] Not required if vCenter connection is used. In VMware vSphere versions 6.5 and later, port 443 is required by VMware web services. Note: When configuring firewalls, consider opening port 443 on ESX(i) hosts even if you add vCenter Server to the backup infrastructure. Port 443 may be required for backup and restore without vCenter Server, for example, if you back up a VM that hosts vCenter Server and restore it when vCenter Server is down. This port is not required for VMware Cloud on AWS.
		TCP	902	Port used for data transfer to ESX(i) host. This port is not required for VMware Cloud on AWS.

		TCP	22	<p>Port used as a control channel (only for jobs that use an ESX target with the console agent enabled).</p> <p>This port is not required for VMware Cloud on AWS.</p>
	vCloud Director	HTTPS TCP	443	Default port used for connections to vCloud Director.
Other Servers				
Backup server	Microsoft SQL Server hosting the Veeam Backup & Replication configuration database	TCP	1433	<p>Port used for communication with Microsoft SQL Server on which the Veeam Backup & Replication configuration database is deployed (if you use a Microsoft SQL Server default instance).</p> <p>Additional ports may need to be open depending on your configuration. For more information, see Microsoft Docs.</p>
	DNS server with forward/reverse name resolution of all backup servers	UDP	53	Port used for communication with the DNS Server.
	Veeam Update Notification Server (dev.veeam.com)	TCP	80	Default port used to download information about available updates from the Veeam Update Notification Server over the Internet.
	Veeam License Update Server (autolk.veeam.com)	TCP	443	Default port used for license auto-update.
Backup Server				
Backup server	Backup server	TCP	9501	Port used locally on the backup server for communication between Veeam Broker Service and Veeam services and components.
Remote Access				
Management client PC (remote access)	Backup server	TCP	3389	Default port used by the Remote Desktop Services. If you use third-party solutions to connect to the backup server, other ports may need to be open.

Veeam Backup & Replication Console Connections

The following table describes network ports that must be opened to ensure proper communication with the Veeam Backup & Replication console installed remotely.

From	To	Protocol	Port	Notes
Veeam Backup & Replication Console	Backup server	TCP	9392	Port used by the Veeam Backup & Replication console to connect to the backup server.
Veeam Backup & Replication Console	Backup server	TCP	10003	Port used by the Veeam Backup & Replication console to connect to the backup server only when managing the Veeam Cloud Connect infrastructure.
Veeam Backup & Replication Console	Mount server (if the mount server is not located on the console)	TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.

Microsoft Windows Servers Connections

The following table describes network ports that must be opened to ensure proper communication with Microsoft Windows servers managed by Veeam Backup & Replication.

These ports must be opened for every Microsoft Windows server that you add to Veeam Backup & Replication. If you want to use the server as a backup component, for example, a backup proxy, you must additionally open ports required by the component role. See the ports required for each component role respectively.

From	To	Protocol	Port	Notes
Backup server	Microsoft Windows server	TCP UDP	135, 137 to 139, 445	Ports required for deploying Veeam Backup & Replication components.
Backup proxy		TCP	6160	Default port used by the Veeam Installer Service.
Backup repository		TCP	2500 to 5000	Default range of ports used as data transmission channels and for collecting log files. For every TCP connection that a job uses, one port from this range is assigned.
Gateway server		TCP	6161	[For Microsoft Windows servers running the vPower NFS Service] Default port used by the Veeam vPower NFS Service.
Mount server		TCP	6162	Default port used by the Veeam Data Mover Service.
WAN accelerator		TCP	49152 to 65535	Dynamic RPC port range. For more information,

Tape server			(for Microsoft Windows 2008 and newer)	see this Microsoft KB article .
--------------------	--	--	--	---

Linux Servers Connections

The following table describes network ports that must be opened to ensure proper communication with Linux servers managed by Veeam Backup & Replication.

These ports must be opened for every Linux server that you add to Veeam Backup & Replication. If you want to use the server as a backup component, for example, a backup repository, you must additionally open ports required by the component role. See the ports required for each component role respectively.

From	To	Protocol	Port	Notes
Backup server	Linux server	TCP	22	Port used as a control channel from the console to the target Linux host.
		TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
Linux server	Backup server	TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.

Backup Proxy Connections

The following table describes network ports that must be opened to ensure proper communication of backup proxies with other backup components.

From	To	Protocol	Port	Notes
Backup server	Backup proxy	See Microsoft Windows Servers Connections .		
Backup proxy	vCenter Server	HTTPS	443	Default VMware web service port that can be customized in vCenter settings.
	ESX(i) server	TCP	902	VMware data mover port. This port is not required for VMware Cloud on AWS.
		HTTPS	443	Default VMware web service port that can be customized in ESX host settings. Not required if vCenter connection is used. This port is not required for VMware Cloud on AWS.

Backup proxy	Linux server	TCP	22	Port used as a control channel from the backup proxy to the target Linux host.
	Microsoft Windows server	TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range. For more information, see this Microsoft KB article .
	Shared folder CIFS (SMB) share	TCP UDP	135, 137 to 139, 445	Ports used as a transmission channel from a backup proxy to the target CIFS (SMB) share. Traffic goes between a backup proxy and CIFS (SMB) share only if a gateway server is not specified explicitly in CIFS (SMB) backup repository settings (Automatic selection option is used). If a gateway server is specified explicitly, traffic goes between a gateway server and CIFS (SMB) share. For more information about required ports, see the Gateway server > Shared folder line below in this table.
	Gateway server	TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range. For more information, see this Microsoft KB article .
Gateway server (if a gateway server is specified explicitly in CIFS (SMB) backup repository settings)	Shared folder CIFS (SMB) share	TCP UDP	135, 137 to 139, 445	Ports used as a transmission channel from a gateway server to the target CIFS (SMB) share.
Backup proxy	Backup proxy	TCP	2500 to 5000	Default range of ports used as transmission channels for replication jobs. For every TCP connection that a job uses, one port from this range is assigned.

Backup Repository Connections

The following table describes network ports that must be opened to ensure proper communication with backup repositories.

From	To	Protocol	Port	Notes
Backup proxy	Microsoft Windows server performing the role of the backup repository	See Microsoft Windows Server Connections .		
Backup proxy	Linux server performing the role of the backup repository	See Linux Servers Connections .		
Backup repository	Backup proxy	TCP	2500 to 5000	Default range of ports used as transmission channels for replication jobs. For every TCP connection that a job uses, one port from this range is assigned.
Source backup repository	Target backup repository	TCP	2500 to 5000	Default range of ports used as transmission channels for backup copy jobs. For every TCP connection that a job uses, one port from this range is assigned. Ports 2500 to 5000 are used for backup copy jobs that do not utilize WAN accelerators. If the backup copy job utilizes WAN accelerators, make sure that ports specific for WAN accelerators are open.
Microsoft Windows Server running vPower NFS service	Backup repository gateway server working with backup repository	TCP	2500 to 5000	Default range of ports used as transmission channels during Instant VM Recovery, SureBackup or Linux file-level recovery. For every TCP connection that a job uses, one port from this range is assigned.

Object Storage Repository Connections

The following table describes network ports that must be opened to ensure proper communication with object storage repositories.

From	To	Protocol	Port	Notes
Backup server	Amazon S3 Object Storage	TCP	443	Used to communicate with Amazon S3 Object Storage.
	Microsoft Azure Object Storage	TCP	443	Used to communicate with Microsoft Azure Object Storage.

	IBM Cloud Object Storage	TCP	Customizable and depends on device configuration	Used to communicate with IBM Cloud Object Storage.
	S3 Compatible Object Storage	TCP	Customizable and depends on device configuration	Used to communicate with S3 Compatible Object Storage.

For more information, see [Object Storage Repository](#).

Dell EMC Data Domain System Connections

From	To	Protocol	Port	Notes
Backup server or Gateway server	Dell EMC Data Domain	TCP	111	Port used to assign a random port for the mountd service used by NFS and DDBOOST. Mountd service port can be statically assigned.
		TCP	2049	Main port used by NFS. Can be modified via the 'nfs set server-port' command. Command requires SE mode.
		TCP	2052	Main port used by NFS MOUNTD. Can be modified via the 'nfs set mountd-port' command in SE mode.
Backup server	Gateway server	See Gateway Server Connections .		

For more information, see <https://community.emc.com/docs/DOC-33258>.

HPE StoreOnce Connection

From	To	Protocol	Port	Notes
Backup server or Gateway server	HPE StoreOnce	TCP	9387	Default command port used for communication with HPE StoreOnce.
			9388	Default data port used for communication with HPE StoreOnce.
Backup server	Gateway server	See Gateway Server Connections .		

Gateway Server Connections

The following table describes network ports that must be opened to ensure proper communication with gateway servers.

From	To	Protocol	Port	Notes
Backup server	Gateway server	See Microsoft Windows Server Connections .		
		TCP UDP	135, 137 to 139, 445	Ports required for deploying Veeam Backup & Replication components.
Gateway server (if a gateway server is specified explicitly in CIFS (SMB) backup repository settings)	Shared folder CIFS (SMB) share	TCP UDP	135, 137 to 139, 445	Ports used as a transmission channel from a gateway server to the target CIFS (SMB) share.

Mount Server Connections

The following table describes network ports that must be opened to ensure proper communication with mount servers.

From	To	Protocol	Port	Notes
Backup server	Mount server	See Microsoft Windows Server Connections .		
		TCP	6170	Port used for communication with a local or remote Mount Service.
Mount server (or machine running the Veeam Backup & Replication console)	Backup server	TCP	9401	Port used for communication with the Veeam Backup Service.
Mount server (or machine running the Veeam Backup & Replication console)	Backup repository	TCP	2500 to 5000	Default range of ports used for communication with a backup repository.
Mount server	Helper appliance	TCP	22	Default SSH port used as a control channel.
		TCP	2500 to 2600	Default range of ports used for communicating with the appliance.

Mount server	VM guest OS	See VM Guest OS Connections .
---------------------	-------------	---

Microsoft Windows Server Running vPower NFS Service Connections

From	To	Protocol	Port	Notes
Backup server	Microsoft Windows server running vPower NFS Service	TCP	6160	Default port used by the Veeam Installer Service.
		TCP	6161	Default RPC port used by the Veeam vPower NFS Service.
ESX(i) host	Microsoft Windows server running vPower NFS Service	TCP UDP	111	Standard port used by the port mapper service.
		TCP UDP	1058+ or 1063+	Default mount port. The number of port depends on where the vPower NFS service is located: <ul style="list-style-type: none"> 1058+: If the vPower NFS service is located on the backup server. 1063+: If the vPower NFS service is located on a separate Microsoft Windows machine. <p>If port 1058/1063 is occupied, the succeeding port numbers will be used.</p>
		TCP UDP	2049+	Standard NFS port. If port 2049 is occupied, the succeeding port numbers will be used.
Backup repository or Gateway server working with backup repository	Microsoft Windows server running vPower NFS Service	TCP	2500 to 5000	Default range of ports used as transmission channels during Instant VM Recovery, SureBackup or Linux file-level recovery. <p>For every TCP connection that a job uses, one port from this range is assigned.</p>

Proxy Appliance (Multi-OS FLR) Connections

From	To	Protocol	Port	Notes
Backup server	Helper appliance	TCP	22	Port used as a communication channel from the backup server to the proxy appliance in the multi-OS file-level recovery process.

		TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
	VM guest OS	TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
Helper appliance	VM guest OS	TCP	22	Port used as a communication channel from the proxy appliance to the Linux guest OS during multi-OS file-level recovery process.
		TCP	20	[If FTP option is used] Default port used for data transfer.
		TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
VM guest OS	Helper appliance	TCP	22	Port used as a communication channel from the proxy appliance to Linux guest OS during multi-OS file-level recovery process.
		TCP	21	[If FTP option is used] Default port used for protocol control messages.
Helper appliance	Backup repository	TCP	2500 to 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.

SureReplica Recovery Verification Connections

From	To	Protocol	Port	Notes
Backup server	vCenter Server	HTTPS TCP	443	Default port used for connections to vCenter Server.
	ESX(i) server	HTTPS TCP	443	Default port used for connections to ESX(i) host. Not required if vCenter connection is used.

		TCP	22	Port used as a control channel (only for jobs that use an ESX target with the console agent enabled).
	Proxy appliance	TCP	443	Port used for communication with the proxy appliance in the virtual lab.
			22	Port used for communication with the proxy appliance in the virtual lab.
	Applications on VMs in the virtual lab	—	—	Application-specific ports to perform port probing test. For example, to verify a DC, Veeam Backup & Replication probes port 389 for a response.
Internet-facing proxy server	VMs in the virtual lab	HTTP	8080	Port used to let VMs in the virtual lab access the Internet.

WAN Accelerator Connections

The following table describes network ports that must be opened to ensure proper communication between WAN accelerators used in backup copy jobs and replication jobs.

From	To	Protocol	Port	Notes
Backup server	WAN accelerator (source and target)	See Microsoft Windows Server Connections .		
		TCP	6160	Default port used by the Veeam Installer Service.
		TCP	6162	Default port used by the Veeam Data Mover Service.
		TCP	6164	Controlling port for RPC calls.
WAN accelerator (source and target)	Backup repository (source and target)	TCP	2500 to 5000	Default range of ports used by the Veeam Data Mover Service for transferring files of a small size such as NVRAM, VMX, VMXF, GuestIndexData.zip and others. A port from the range is selected dynamically.
WAN accelerator	WAN accelerator	TCP	6164	Controlling port for RPC calls.
		TCP	6165	Default port used for data transfer between WAN accelerators. Ensure this port is open in firewall between sites where WAN accelerators are deployed.

Tape Server Connections

The following table describes network ports that must be opened to ensure proper communication with tape servers.

From	To	Protocol	Port	Notes
Backup server	Tape server	See Microsoft Windows Server Connections .		
		TCP	6166	Controlling port for RPC calls.
Tape server	Backup repository, gateway server or proxy server	See Microsoft Windows Server Connections .		

Dell EMC VNX(e) Storage Connections

From	To	Protocol	Port	Notes
Backup server	VNX File	SSH	22	Default command port used for communication with VNX File over SSH.
	VNX Block	HTTPS	443	Default port used for communication with Dell EMC VNX Block.
	VNXe	HTTPS	443	Default port used for communication with Dell EMC VNXe and sending RESTful API calls.
Backup proxy	VNX Block	TCP	3260	Default iSCSI target port.
	VNXe			
	VNX File	TCP, UDP	2049, 111	Standard NFS ports. Port 111 is used by the port mapper service.
	VNXe			

HPE 3PAR StoreServ Storage Connections

From	To	Protocol	Port	Notes
Backup server	HPE 3PAR StoreServ storage system	HTTP	8008	Default port used for communication with the HPE 3PAR StoreServ storage system over HTTP.
		HTTPS	8080	Default port used for communication with the HPE 3PAR StoreServ storage system over HTTPS.
		SSH	22	Default command port used for communication with HPE 3PAR StoreServ over SSH.

Backup proxy	HPE 3PAR StoreServ storage system	TCP	3260	Default iSCSI target port.
---------------------	-----------------------------------	-----	------	----------------------------

HPE Lefthand Storage Connections

From	To	Protocol	Port	Notes
Backup server	HPE Lefthand storage system	SSH	16022	Default command port used for communication with HPE Lefthand.
Backup proxy	HPE Lefthand storage system	TCP	3260	Default iSCSI target port.

HPE Nimble Storage Connections

From	To	Protocol	Port	Notes
Backup server	HPE Nimble storage system	TCP	5392	Default command port used for communication with Nimble storage (used for Nimble OS 2.3 and later).
Backup proxy	Nimble storage system	TCP	3260	Default iSCSI target port.

IBM Spectrum Virtualize Storage Connections

From	To	Protocol	Port	Notes
Backup server	IBM Spectrum Virtualize storage system	SSH	22	Default command port used for communication with IBM Spectrum Virtualize storage over SSH.
Backup proxy	IBM Spectrum Virtualize storage system	TCP	3260	Default iSCSI target port.

NetApp Storage Connections

From	To	Protocol	Port	Notes
Backup server	NetApp storage system	HTTP	80	Default command port used for communication with NetApp over HTTP.
		HTTPS	443	Default command port used for communication with NetApp over HTTPS.

Backup proxy	NetApp storage system	TCP, UDP	2049, 111	Standard NFS ports. Port 111 is used by the port mapper service.
		TCP	3260	Default iSCSI target port.

VM Guest OS Connections

The following table describes network ports that must be opened to ensure proper communication of the backup server with the runtime coordination process deployed inside the VM guest OS for application-aware processing and indexing.

From	To	Protocol	Port	Notes
Backup server	Linux VM guest OS	TCP	22	Default SSH port used as a control channel.
	Guest interaction proxy	TCP	6190	Port used for communication with the guest interaction proxy.
		TCP	6290	Port used as a control channel for communication with the guest interaction proxy.
Guest interaction proxy	ESX(i) server	TCP	443	Default port used for connections to ESX(i) host. [For VMware vSphere earlier than 6.5] Not required if vCenter connection is used. In VMware vSphere versions 6.5 and later, port 443 is required by VMware web services.
Guest interaction proxy or Mount server	Microsoft Windows VM guest OS	TCP, UDP	135, 137 to 139, 445	Ports required to deploy the runtime coordination process on the VM guest OS.
		TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range used by the runtime process deployed inside the VM for guest OS interaction (when working over the network, not over VIX API). For more information, see this Microsoft KB article .
		TCP	6167, 2500 to 5000	[For Microsoft SQL logs shipping] Port used by the runtime process on the VM guest OS from which Microsoft SQL logs are collected.
	Linux VM guest OS	TCP	22	Default SSH port used as a control channel.
TCP		2500 to 5000	Default range of ports used as transmission channels during Linux file-level recovery and for Oracle log backup. For every TCP connection that a job uses, one port from this range is assigned.	

Microsoft Windows VM guest OS	Guest interaction proxy or mount server	TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range used by the runtime process deployed inside the VM for guest OS interaction (when working over the network, not over VIX API). For more information, see this Microsoft KB article . Note: Microsoft Exchange expands a standard Windows dynamic RPC port range. For more information, see the Used Ports section in the Veeam Explorers User Guide.
--------------------------------------	---	-----	---	--

* If you use default Microsoft Windows firewall settings, you do not need to configure dynamic RPC ports: during setup, Veeam Backup & Replication automatically creates a firewall rule for the runtime process. If you use firewall settings other than default ones or application-aware processing fails with the "*RPC function call failed*" error, you need to configure dynamic RPC ports.

Veeam U-AIR Wizards Connections

The following table describes network ports that must be opened to ensure proper communication of U-AIR wizards with other components.

From	To	Protocol	Port	Notes
U-AIR wizards	Veeam Backup Enterprise Manager	TCP	9394	Default port used for communication with Veeam Backup Enterprise Manager. Can be customized during Veeam Backup Enterprise Manager installation.

Azure Proxy Connection

From	To	Protocol	Port	Notes
Backup server	Azure proxy	TCP	443	Default management and data transport port required for communication with the Azure proxy. The port must be opened on the backup server and backup repository storing VM backups.

Azure Stack Connection

From	To	Protocol	Port	Notes
Backup server	Azure Stack	HTTPS	443, 30024	Default management and data transport port required for communication with the Azure Stack.

Microsoft Active Directory Domain Controller Connections During Application Item Restore

The following table describes network ports that must be opened to ensure proper communication of the backup server with the Microsoft Active Directory VM during application-item restore.

From	To	Protocol	Port	Notes
Backup server	Microsoft Active Directory VM guest OS	TCP	135	Port required for communication between the domain controller and backup server.
		TCP, UDP	389	LDAP connections.
		TCP	636, 3268, 3269	LDAP connections.
		TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range used by the runtime coordination process deployed inside the VM guest OS for application-aware processing (when working over the network, not over VIX API). * For more information, see this Microsoft KB article .

Microsoft Exchange Server Connections During Application Item Restore

The following table describes network ports that must be opened to ensure proper communication of the Veeam backup server with the Microsoft Exchange Server system during application-item restore.

From	To	Protocol	Port	Notes
Backup server	Microsoft Exchange 2003/2007 CAS Server	TCP	80, 443	WebDAV connections.
	Microsoft Exchange 2010/2013 CAS Server	TCP	443	Microsoft Exchange Web Services Connections.

Microsoft SQL Server Connections During Application Item Restore

The following table describes network ports that must be opened to ensure proper communication of the backup server with the VM guest OS system during application-item restore.

From	To	Protocol	Port	Notes
Backup server	Microsoft SQL VM guest OS	TCP	1433, 1434 and other	Port used for communication with the Microsoft SQL Server installed inside the VM. Port numbers depends on configuration of your Microsoft SQL server. For more information, see Microsoft Docs .

SMTP Server Connections

The following table describes network ports that must be opened to ensure proper communication of the backup server with the SMTP server.

From	To	Protocol	Port	Notes
Backup server	SMTP server	TCP	25	Port used by the SMTP server. Port 25 is most commonly used but the actual port number depends on configuration of your environment.

Veeam Backup Enterprise Manager Connections

[Veeam Backup Enterprise Manager Connections](#)

Veeam Explorers Connections

- [Veeam Explorer for Microsoft Active Directory Connections](#)
- [Veeam Explorer for Microsoft Exchange Connections](#)
- [Veeam Explorer for Microsoft SharePoint Connections](#)
- [Veeam Explorer for Microsoft SQL Server Connections](#)
- [Veeam Explorer for Oracle Connections](#)

Veeam Cloud Connect Connections

[Veeam Cloud Connect Connections](#)

Veeam Agent for Windows Connections

[Veeam Agent for Windows Connections](#)

Veeam Agent for Linux Connections

[Veeam Agent for Linux Connections](#)

Veeam Plug-ins for Enterprise Applications

- [Veeam Plug-in for SAP HANA](#)
- [Veeam Plug-in for Oracle RMAN](#)

Internet Connections

If you use an HTTP(S) proxy server to access the Internet, make sure that WinHTTP settings are properly configured on Microsoft Windows machines with Veeam backup infrastructure components. For information on how to configure WinHTTP settings, see [Microsoft Docs](#).

NOTE:

Tenants cannot access Veeam Cloud Connect infrastructure components through HTTP(S) proxy servers. For information on supported protocols for Veeam Cloud Connect, see the [Used Ports](#) section in the Veeam Cloud Connect Guide.

Naming Conventions

Do not use Microsoft Windows reserved names for names of the backup server, managed servers, backup repositories, jobs, tenants and other objects created in Veeam Backup & Replication: CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8 and LPT9. If you use a reserved name, Veeam Backup & Replication may not work as expected. For more information on naming conventions in Microsoft Windows, see [Microsoft Docs](#).

Security Considerations

When you set up the backup infrastructure, one thing that you must not overlook is security. The backup infrastructure can be potentially used as a backdoor to gain access to your systems and data.

This section includes a number of recommendations that will help you prevent potential security issues and reduce the risk of compromising sensitive data.

Backups and Replicas

A potential source of vulnerability is the backup or replica itself. To secure data stored in backups and replicas, consider the following recommendations:

- **Ensure physical security of target servers.** Check that only authorized personnel have access to the room where your target servers (backup repositories and hosts) reside.
- **Restrict user access to backups and replicas.** Check that only authorized users have permissions to access backups and replicas on target servers.
- **Encrypt data in backups.** Use Veeam Backup & Replication built-in encryption to protect data in backups. To guarantee security of data in backups, follow [Encryption Best Practices](#).

Data Communication Channel

Backup data can be intercepted in-transit, when it is communicated from source to target over a network. To secure the communication channel for backup traffic, consider the following recommendations:

- **Isolate backup traffic.** Use an isolated network to transport data between backup infrastructure components – backup server, backup proxies, repositories and so on.
- **Encrypt network traffic.** By default, Veeam Backup & Replication encrypts network traffic travelling between public networks. To ensure secure communication of sensitive data within the boundaries of the same network, you can also encrypt backup traffic in private networks. For details, see [Enabling Network Data Encryption](#).

Internet Access for Backup Servers

Some Veeam Backup & Replication functionality requires that backup servers have outbound Internet access. For example, to enable product update check, automatic license update and license usage reporting, a backup server must be connected to the Internet and be able to send requests to servers on the Internet.

However, inbound connectivity to backup servers from the Internet must not be allowed. If you want to manage backup servers remotely over the Internet, you can deploy the Veeam Backup & Replication console on a jump server. Service providers who want to manage backup servers remotely can use the Veeam Backup Remote Access functionality. For more information, see the [Using Remote Access Console](#) section in the Veeam Cloud Connect Guide.

The account used for RDP access must not have Local Administrator privileges on the jump server, and you must never use the saved credentials functionality for RDP access or any other remote console connections. To restrict users from saving RDP credentials, you can use Group Policies. For more information, see [Experts Exchange](#).

Credentials

An attacker who gained high-privilege access to backup infrastructure servers can get credentials of user accounts and compromise other systems in your environment.

Particularly, backup proxies must be considered the target for compromise. During backup, proxies obtain from the backup server credentials required to access virtual infrastructure servers. A person having administrator privileges on a backup proxy can intercept the credentials and use them to access the virtual infrastructure.

One of the most possible causes of a credential theft are missing guest OS updates and use of outdated authentication protocols. To mitigate risks, consider the following recommendations:

- **Ensure timely guest OS updates on backup infrastructure servers.** Install the latest updates and patches on backup infrastructure servers to minimize the risk of exploiting guest OS vulnerabilities by attackers.
- **Choose strong encryption algorithms for SSH.** To communicate with Linux servers deployed as part of the backup infrastructure, Veeam Backup & Replication uses SSH. Make sure that for the SSH tunnel you use a strong and proven encryption algorithm, with sufficient key length. Ensure that private keys are kept in a highly secure place, and cannot be uncovered by a 3rd party.
- **Avoid using password authentication to connect to remote servers over SSH.** Using key-based SSH authentication is generally considered more secure than using password authentication and is not vulnerable to MITM attacks.

Veeam Backup & Replication Database

Another security concern you must consider is protecting the Veeam Backup & Replication configuration database. The database stores credentials of user accounts required to connect to virtual servers and other systems in the backup infrastructure. All passwords stored in the database are encrypted. However, a user with administrator privileges on the backup server can decrypt the passwords, which presents a potential threat.

To secure the Veeam Backup & Replication configuration database, consider the following recommendations:

- **Restrict user access to the database.** Check that only authorized users can access the backup server and the server that hosts the Veeam Backup & Replication configuration database (if the database runs on a remote server).
- **Encrypt data in configuration backups.** Enable data encryption for configuration backup to secure sensitive data stored in the configuration database. For details, see [Creating Encrypted Configuration Backups](#).

Veeam Cloud Connect

Veeam Cloud Connect secures communication between the provider side and tenant side with TLS. If an attacker obtains a provider's private key, backup traffic can be eavesdropped and decrypted. The attacker can also use the certificate to impersonate the provider (man-in-the middle attack).

Veeam Cloud Connect providers must consider the following recommendations:

Keep the certificate in a secure place. Make sure that the TLS certificate is kept in a highly secure place and cannot be uncovered by a 3rd party.

Kerberos Authentication for Guest OS Processing

Starting from version 9.5 Update 4, Veeam Backup & Replication supports Kerberos authentication for guest OS processing of VMware vSphere VMs. However NTLM authentication is still required for communication between Veeam backup infrastructure servers (backup server, backup proxies, backup repositories, guest interaction proxies, log shipping servers, mount servers).

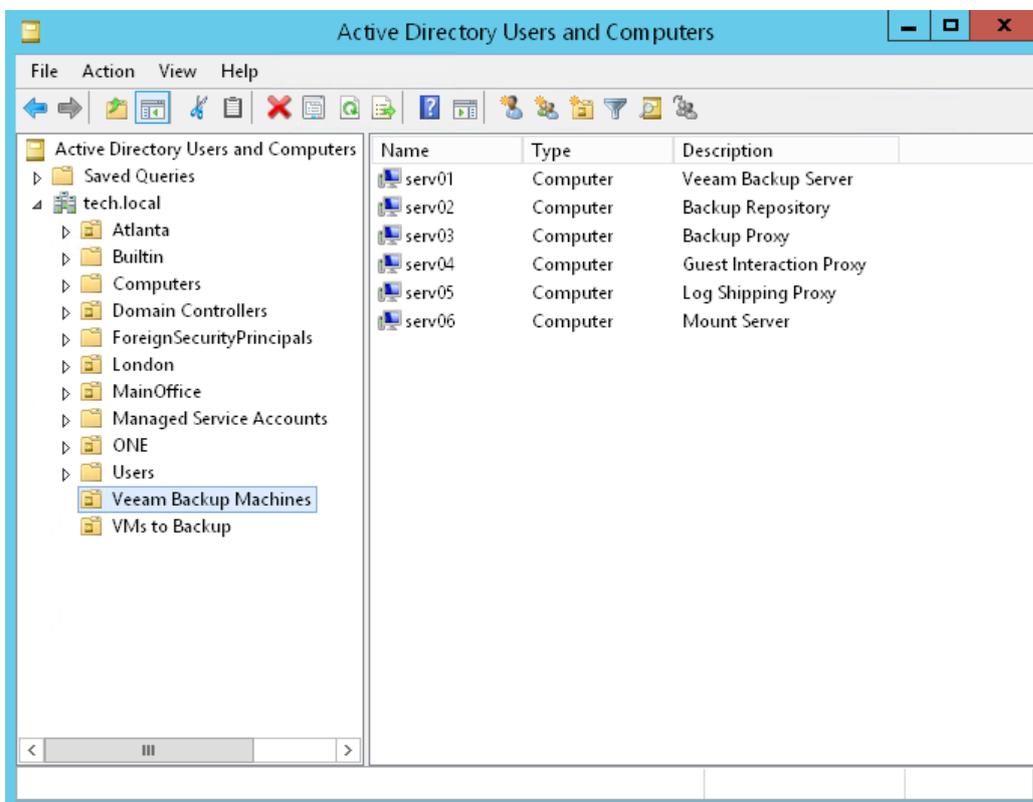
To back up or replicate VMware vSphere VMs where Kerberos is used, you must make sure that NTLM traffic is allowed in Veeam backup infrastructure machines. To do this, you must configure Active Directory group policies as shown below or in a similar way.

Configuring Active Directory Group Policies

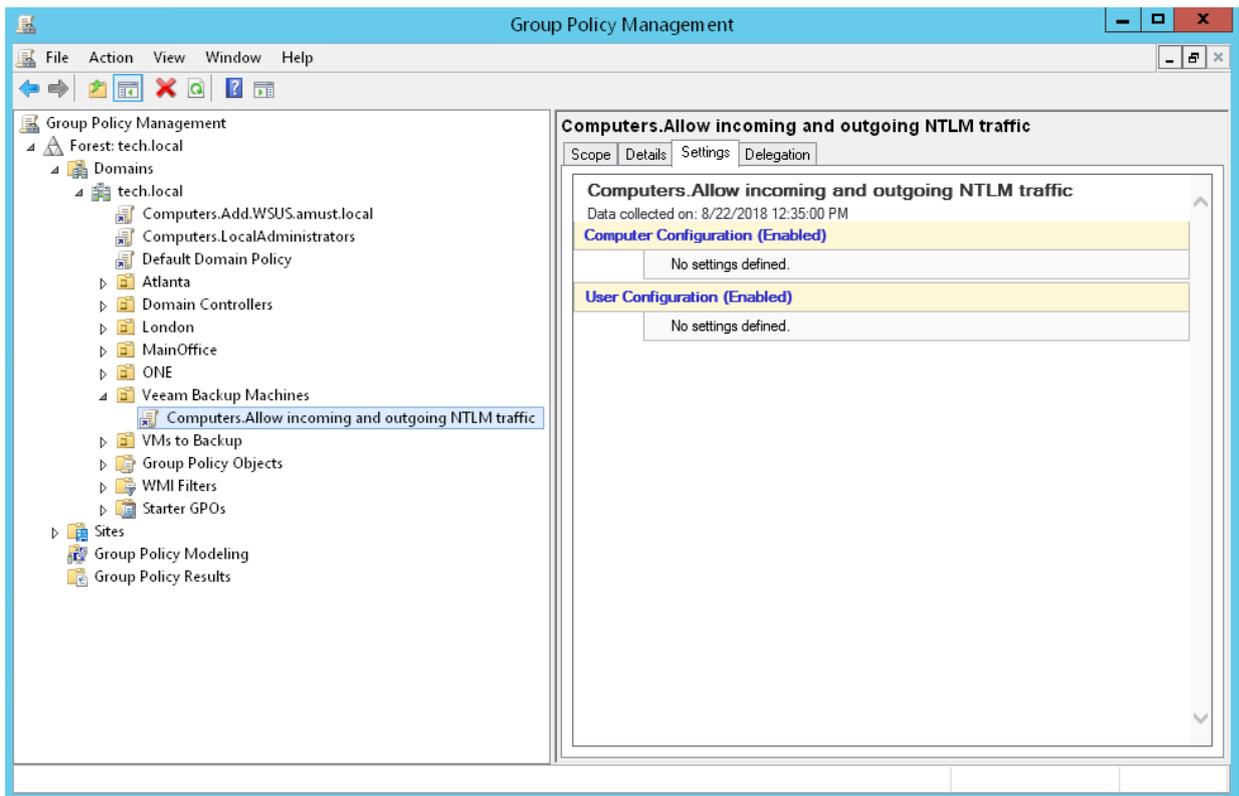
If you want to back up or replicate VMs where Kerberos protocol is used, you must make sure that NTLM traffic is allowed in the Veeam backup infrastructure machines. You can add all Veeam infrastructure servers to a separate Active Directory organizational unit and create a GPO that allows NTLM traffic for this unit.

To allow NTLM traffic in Veeam infrastructure servers, do the following:

1. On the domain controller server or management workstation, open the **Active Directory Users and Computers** MMC snap-in.
2. Create a new Active Directory organizational unit and move all Veeam infrastructure servers to the organizational unit.

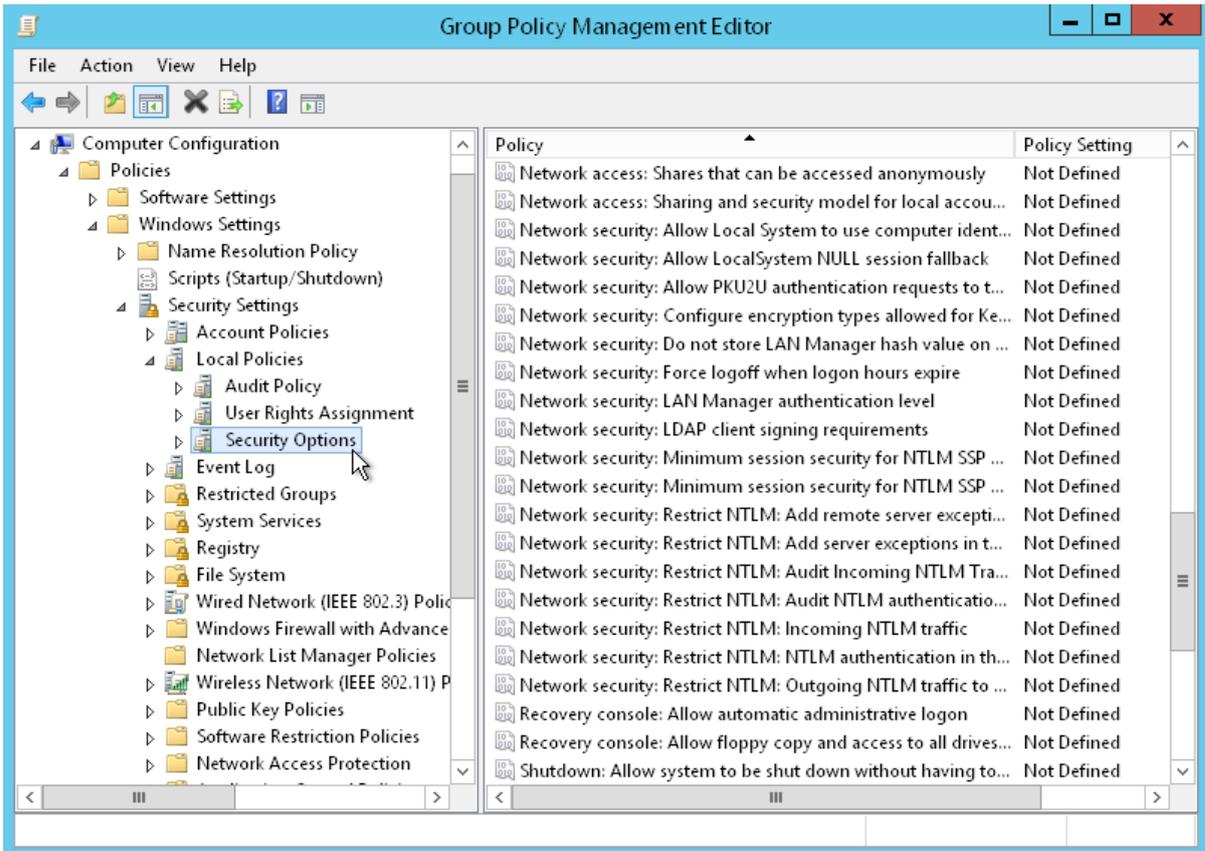


4. Open **Group Policy Management** and create a new GPO for the organizational unit with Veeam infrastructure servers.

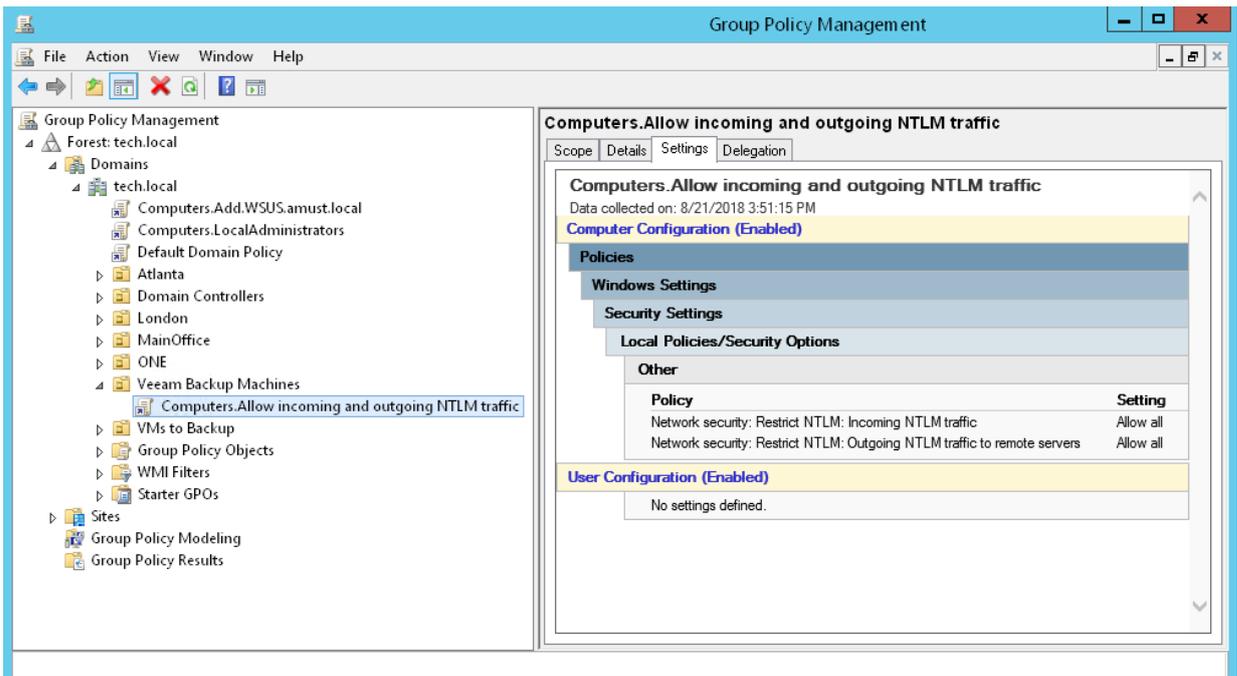


6. Right-click the created GPO and select **Edit**.

- In the infrastructure tree of the **Group Policy Management Editor** interface, go to *Policies/Windows Settings/Security Settings/Local Policies/Security Options*.



- In the **Security Options** folder, go to properties of the following two policies and change the policy setting to *Allow all*:
 - Network Security: Restrict NTLM: Incoming NTLM traffic
 - Network Security: Restrict NTLM: Outgoing traffic to remote servers



After you configure group policies for NTLM traffic, Veeam backup infrastructure servers will be able to authenticate to each other using NTLM, while the servers will use Kerberos to authenticate to guest OS of VMs.

Licensing

To work with Veeam Backup & Replication, you must obtain a license key and install it on the backup server. If you do not install the license key, the product will operate in the *Community* (free) edition. For more information, see [Community Edition and Full Version](#).

Licensed Objects

Veeam licenses Veeam Backup & Replication in two ways: per-instance and per-socket.

Per-Instance Licensing

Veeam Backup & Replication can be licensed by the number of instances. Instances are units (or tokens) that you can use to protect your virtual, physical or cloud-based workloads. You must obtain a license with the total number of instances for workloads that you plan to protect in Veeam Backup & Replication.

Workloads that have been processed in the past 31 days are considered protected. Every protected workload consumes instances from the license scope. The number of instances that a workload requires depends on the workload type and product edition. For details, see [Veeam Licensing Policy](#).

This licensing model allows you to obtain a license with a certain number of instances without knowing in advance what types of workloads you plan to protect. When a need arises, you can revoke instances from a protected workload, and reuse them to protect other workloads regardless of the workload type.

Mind the following:

- VM templates are regarded as protected VMs and consume license instances.
- VMs processed with backup copy and tape jobs are not regarded as protected VMs and do not consume license instances. These types of jobs provide an additional protection level for VMs that are already protected with backup jobs.
- VMs processed by snapshot-only jobs are regarded as protected VMs and consume license instances. Veeam Backup & Replication will revoke instances from these VMs if you re-add a storage array to the backup infrastructure.

Veeam Backup & Replication keeps track of instances consumed by protected workloads. If the number of consumed instances exceeds the license limit, Veeam Backup & Replication displays a warning when you open the Veeam Backup & Replication console. For more information, see [Exceeding License Limit](#).

Per-Socket Licensing

With the per-socket licensing model, Veeam Backup & Replication is licensed by the number of CPU sockets on protected hosts. A license is required for every occupied motherboard socket as reported by the hypervisor API.

License is required only for source hosts – hosts on which VMs that you back up or replicate reside. Target hosts (for replication and migration jobs) do not need to be licensed.

NOTE:

If you use an existing per-socket license that was obtained for earlier versions of Veeam Backup & Replication, Veeam Software adds up to 6 instances free of charge to your license scope. You can use these instances to protect any type of supported workloads except VMware and Hyper-V VMs – they are covered by the licensed CPU sockets on virtualization hosts.

If the number of licensed sockets is less than 6, you can use the number of instances that equals the number of licensed sockets. For example, if the number of licensed sockets is 5, you can use 5 instances. If the number of licensed sockets is 100, you can use 6 instances.

For more information on licensing, see [Veeam Licensing Policy](#).

Types of Licenses

Veeam Software offers the following types of paid licenses for Veeam Backup & Replication:

- **Subscription license** – full license that expires at the end of the subscription term. The subscription license term is normally 1-3 years from the date of license issue.
- **Rental license** – full license with the license expiration date set according to the chosen rental program (normally 1-12 months from the date of license issue). The rental license can be automatically updated upon expiration.

Rental licenses are provided to Veeam Cloud & Service Providers (VCSPs) only. For more information, see the [Rental License](#) section in the Veeam Cloud Connect Guide.

- **Perpetual license** – permanent full license. The perpetual license term is normally 10 years from the date of license issue. The support and maintenance period included with the license is specified in months or years. Typically, one year of basic support and maintenance is included with the perpetual license.

The following terms apply to Veeam Backup & Replication paid licenses:

License Type	Licensing Period	Grace Period	Licensing
Subscription license	1-3 years	30 days	Per-instance
Rental license	1-12 months	60 days	Per-instance
Perpetual license	10 years	n/a	Per-socket

IMPORTANT!

[For *per-VM* licenses] After upgrade to Veeam Backup & Replication 9.5 Update 4, you must obtain and install on the backup server a new per-instance license. To ensure a smooth license update procedure, Veeam Backup & Replication offers you a 90-day grace period after the product is upgraded. During this period, you can continue processing workloads with an old per-VM license.

Mind that during the 90-day grace period the license status in the **License Information** window will be displayed as *Expired (<number> days of grace period remaining)*. If you do not install a new license after the grace period expires, you will not be able to process workloads (existing jobs will fail with the *Error* status).

In addition to paid licenses, Veeam Backup & Replication offers two types of free per-instance licenses:

- **Evaluation license** – license used for product evaluation. The evaluation license is valid for 30 days from the moment of product download.
- **NFR license** – license used for product demonstration, training and education. The person to whom the license is provided agrees that the license is not for resell or commercial use.

Obtaining License

You can obtain an evaluation or paid license for the product when you download the product from the Veeam website.

Obtaining an Evaluation License

To obtain an evaluation license:

1. [Sign in to Veeam](#).
2. At the [Download Veeam products](#) page, click the product link.
3. In the **Get trial key** section, click the **Request Trial Key** link to download the evaluation license.

The evaluation license is valid for 30 days from the moment of product download.

Obtaining a Paid License

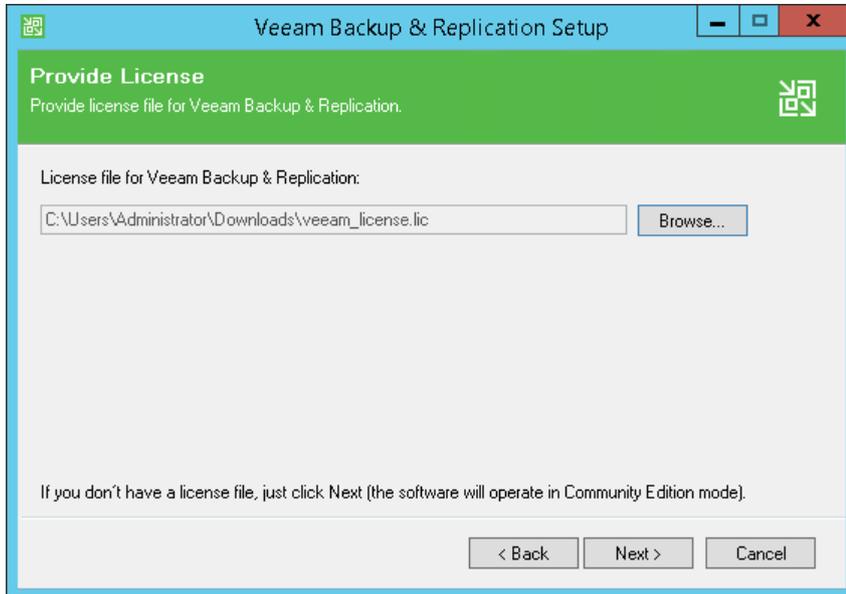
To obtain a paid license, refer to the [Veeam Backup & Replication Pricing](#) page.

TIP:

To renew your maintenance plan, contact Veeam Renewals Team at renewals@veeam.com.

Installing License

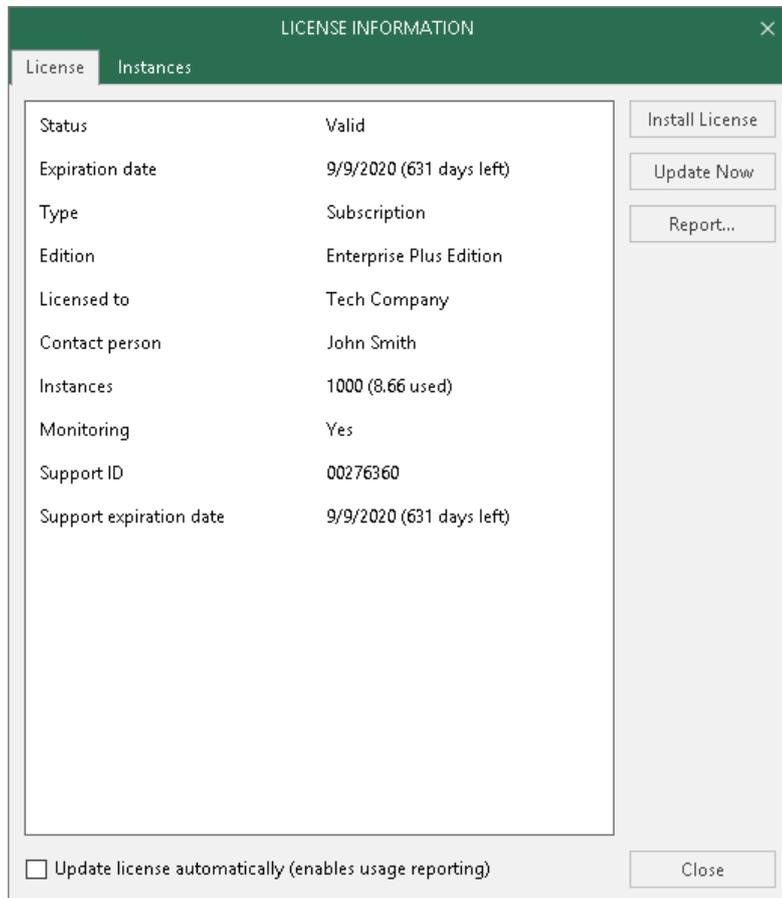
When you install Veeam Backup & Replication, you are asked to specify a path to the license file. If you do not specify a path to the license file, Veeam Backup & Replication will run in the community (free) version. For more information about product versions, see [Community Edition and Full Version](#).



You can install or change the license after product installation:

1. From the main menu, select **License**.
2. To install or change the license, click **Install License** and browse to the LIC file.

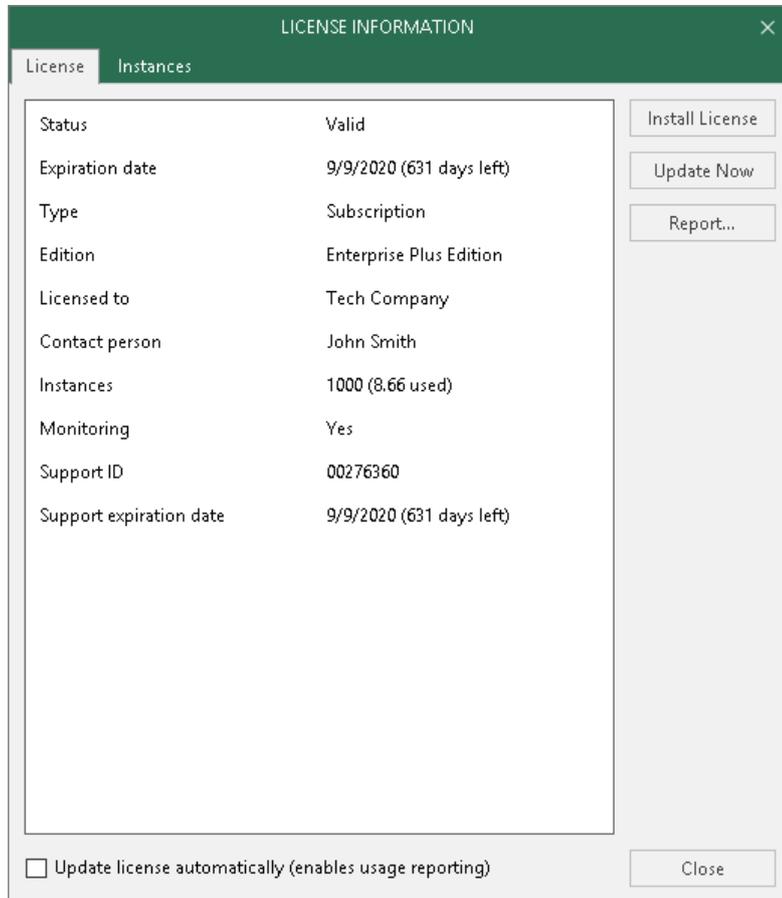
If backup servers are connected to Veeam Backup Enterprise Manager, Veeam Backup Enterprise Manager collects information about all licenses installed on backup servers. When Veeam Backup Enterprise Manager replicates databases from backup servers, it also synchronizes license data: checks if the license installed on the backup server coincides with the license installed on the Veeam Backup Enterprise Manager server. If the licenses do not coincide, the license on the backup server is automatically replaced with the license installed on the Veeam Backup Enterprise Manager server.



Viewing License Information

You can view details of the installed license in the **License** tab of the **License Information** window.

To open the **License Information** window, from the main menu select **License**.



The following details are available for the current license:

- **Status** – license status (*Valid, Invalid, Expired, Not Installed, Warning, Error*).
- **Expiration date** – date when the license expires.
- **Type** – license type (*Perpetual, Subscription, Rental, Evaluation, NFR, Free*).
- **Edition** – license edition (*Community, Standard, Enterprise, Enterprise Plus*).
- **Licensed to** – name of a person or organization to which the license was issued.
- **Contact person** – name of a contact person in an organization to which the license was issued.
- [For *perpetual* licenses] **CPU Sockets (Hyper-V)** – number of licensed CPU sockets on protected Microsoft Hyper-V hosts.
- [For *perpetual* licenses] **CPU Sockets (vSphere)** – number of licensed CPU sockets on protected VMware ESX(i) hosts.
- **Instances** – number of instances that you can use to protect workloads.

- [For *per-instance* licenses] **Monitoring** – parameter that indicates whether Veeam ONE allows monitoring of the Veeam backup server on which the current license is installed (*Yes, No*).

For details, see the [Types of Licenses](#) section in the Veeam ONE Deployment Guide.

- **Support ID** – support ID required for contacting Veeam Support.
- **Support expiration date** – date when support expires.

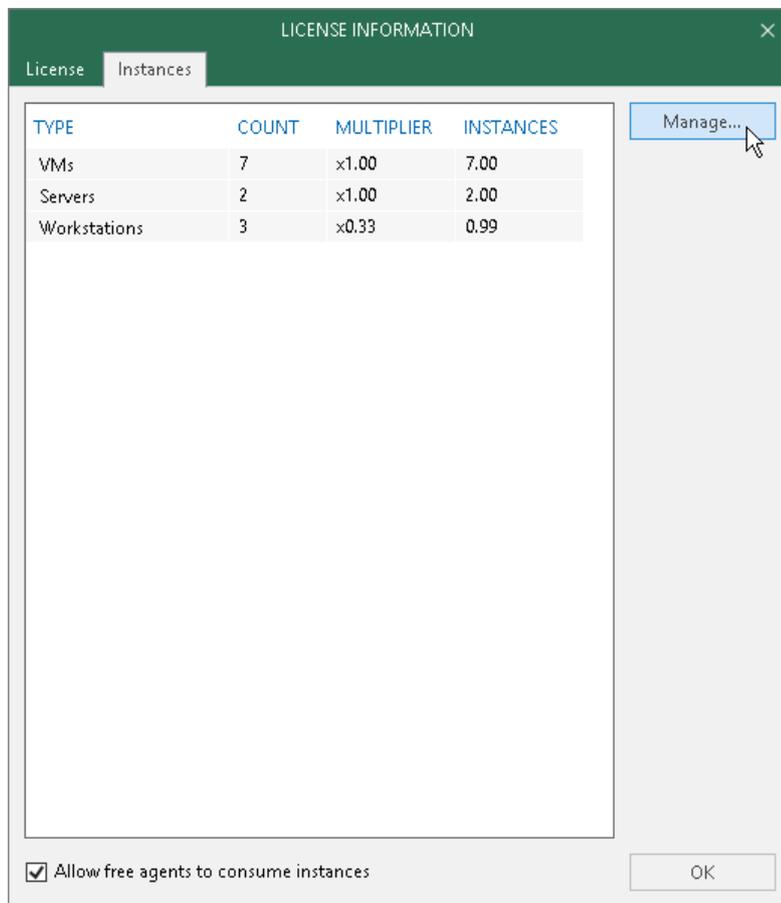
Viewing Licensed Objects

When you run a job, Veeam Backup & Replication applies a license to a protected workload (for *per-instance* licenses) or to the virtualization host on which processed VMs reside (for *per-socket* licenses). You can view to which objects the license is currently applied.

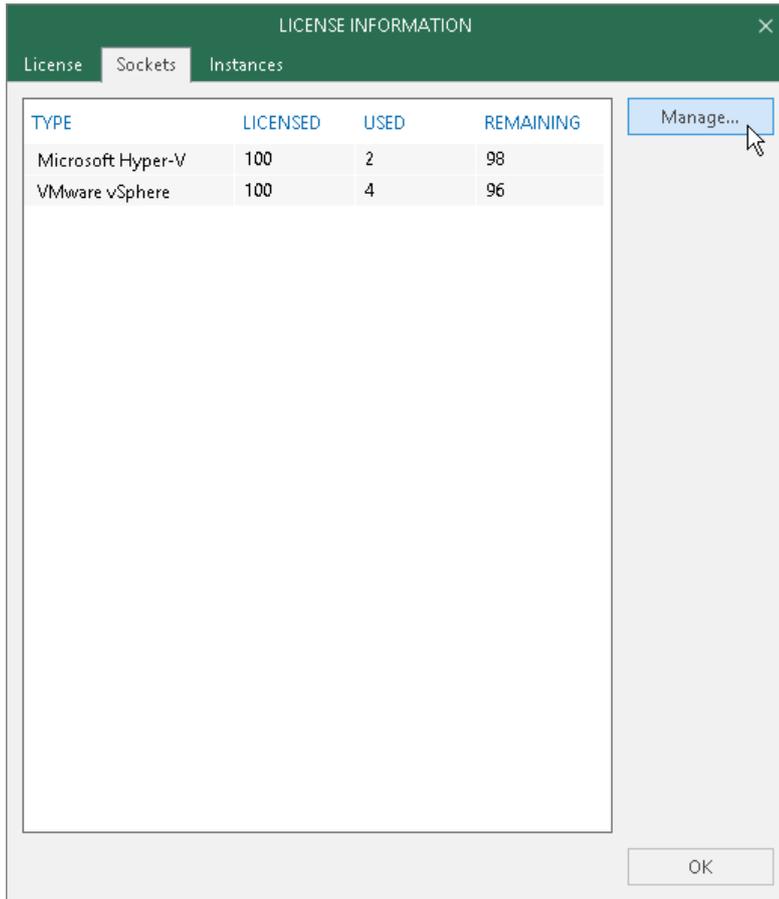
To view a list of licensed objects:

1. From the main menu, select **License**.
2. In the **License Information** window:
 - o For protected workloads, open the **Instances** tab and click **Manage**.

The number of license instances that a protected workload consumes depends on the workload type and product edition. For example, 1 VM in the *Enterprise Plus* edition of Veeam Backup & Replication consumes 1 instance, whereas 1 workstation machine in the same product edition consumes 0.33 instances. For details, see [Veeam Licensing Policy](#).



- For licensed hosts, open the **Sockets** tab and click **Manage**.

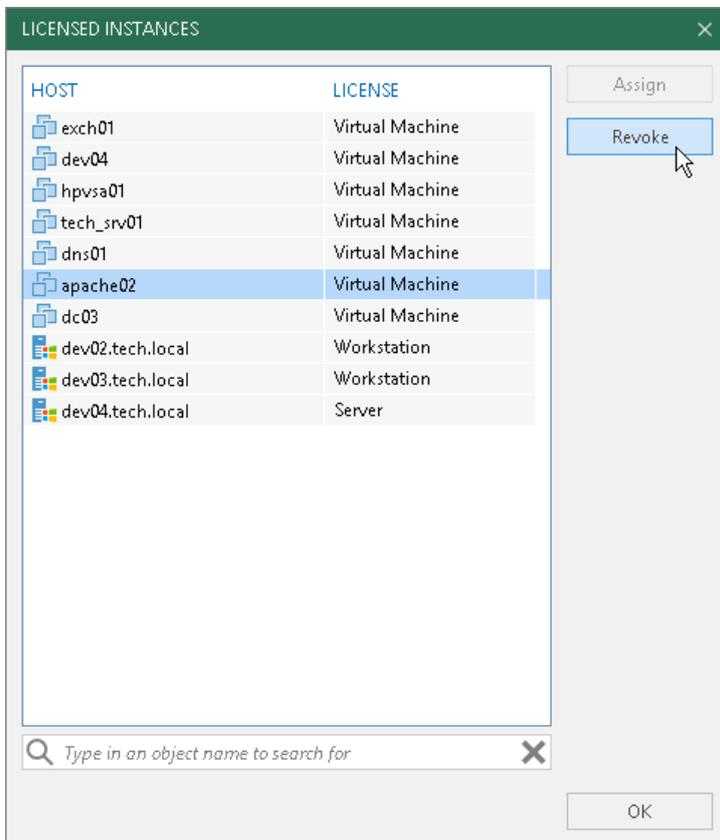


Revoking License

You can revoke licenses from protected workloads or licensed hosts, and re-apply them to other objects that you plan to protect. License revoking can be helpful, for example, if a licensed host goes out of service or you do not want to protect some workloads anymore.

To revoke a license, do the following:

1. From the main menu, select **License**.
2. In the **License Information** window:
 - For protected workloads, open the **Instances** tab and click **Manage**.
 - For licensed hosts, open the **Sockets** tab and click **Manage**.
3. In the displayed window, select a protected workload or a licensed host and click **Revoke**. Veeam Backup & Replication will revoke the license from the selected object, and the license will be freed for other objects in the backup infrastructure.



Exceeding License Limit

In some cases, the number of consumed instances may exceed the license limit. For example, when some workloads are temporarily protected for testing or POC.

For *Subscription* and *Rental* per-instance licenses, Veeam Backup & Replication allows you to protect more workloads than covered by the number of instances specified in the license. An increase in the number of protected workloads is allowed throughout the duration of the contract (license key).

The license limit can be exceeded by a number of instances, or a percentage of the total number of instances specified in the license (depends on which number is greater). The exceeding limit varies according to the license type.

License Type	Exceeding Limit	Description
Perpetual license	Not allowed	Workloads that are exceeding the license limit are not processed.
Subscription license	Up to 5 instances (or 5% of the total instance count)	All protected workloads are processed normally, Veeam Backup & Replication does not display a warning message.
	5-10 instances (or 5%-10% of the total instance count)	All protected workloads are processed normally, once a week a warning message is displayed when you open the Veeam Backup & Replication console.
	Over 10 instances (or 10% of the total instance count)	Workloads that are exceeding the license limit are not processed. A warning message is displayed every time you open the Veeam Backup & Replication console.
Rental license	Up to 10 instances (or 10% of the total instance count)	All protected workloads are processed normally, Veeam Backup & Replication does not display a warning message.
	10-20 instances (or 10%-20% of the total instance count)	All protected workloads are processed normally, once a week a warning message is displayed when you open the Veeam Backup & Replication console.
	Over 20 instances (or 20% of the total instance count)	Workloads that are exceeding the license limit are not processed. A warning message is displayed every time you open the Veeam Backup & Replication console.

For example, you have a *Subscription* license with 500 instances to protect your workloads. According to the table above, you are allowed to use up to 10 instances or 10% of the total instance count (whichever number is greater) over the license limit. As the number of instances in your license is 500, you are allowed to use additional 50 instances (50 makes 10% of 500, and 50 is greater than 10). Consider the following:

- Until the license limit is not exceeded by more than 5% of the total instance count (up to 25 instances), Veeam Backup & Replication processes all protected workloads with no restrictions.
- When the license limit is exceeded by 5%-10% (25.01 to 50 instances), Veeam Backup & Replication processes protected workloads, and displays a warning message once a week when you open the Veeam Backup & Replication console. In the message, Veeam Backup & Replication provides information on the number of exceeded instances and the number of instances by which the license can be further exceeded.

- If the license limit is exceeded by more than 10% (50.01 instances and more), Veeam Backup & Replication does not process the workloads exceeding the limit, and displays a warning message every time you open the Veeam Backup & Replication console. In the message, Veeam Backup & Replication provides information on the number of instances by which the license is exceeded.

License Expiration

To ensure a smooth license update and provide sufficient time to install a new license file, Veeam Backup & Replication offers a grace period.

The duration of the grace period depends on the type of license. For more information, see [Types of Licenses](#).

During the grace period, you can perform all types of data protection and disaster recovery operations. However, Veeam Backup & Replication will inform you about the license expiration when you open the Veeam Backup & Replication console. The license status in the **License Information** window will appear as *Expired (<number> days of grace period remaining)*.

You must update your license before the end of the grace period. If you do not update the license, the following measures will be taken:

- [For evaluation and NFR licenses] Veeam Backup & Replication will switch to the *Community* edition. For more information, see [Community Edition and Full Version](#).
- [For paid licenses] Functionality available in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication will not be available. Workloads will not be processed by existing jobs (jobs will fail with the *Error* status). However, you will be able to restore machine data from existing backups.

Updating License

To be able to use all data protection and disaster recovery features, you must update your license upon expiry. There are two methods to update the license in Veeam Backup & Replication:

- [Update the license manually](#)
- [Update the license automatically](#)

Updating License Manually

You can update the license manually on demand. When you update the license manually, Veeam Backup & Replication connects to the Veeam License Update Server, downloads a new license from it (if the license is available) and installs it on the backup server.

The new license key differs from the previously installed license key in the license expiration date and support expiration date. If you have obtained a license for a greater number of instances, counters in the new license also display the new number of licensed instances.

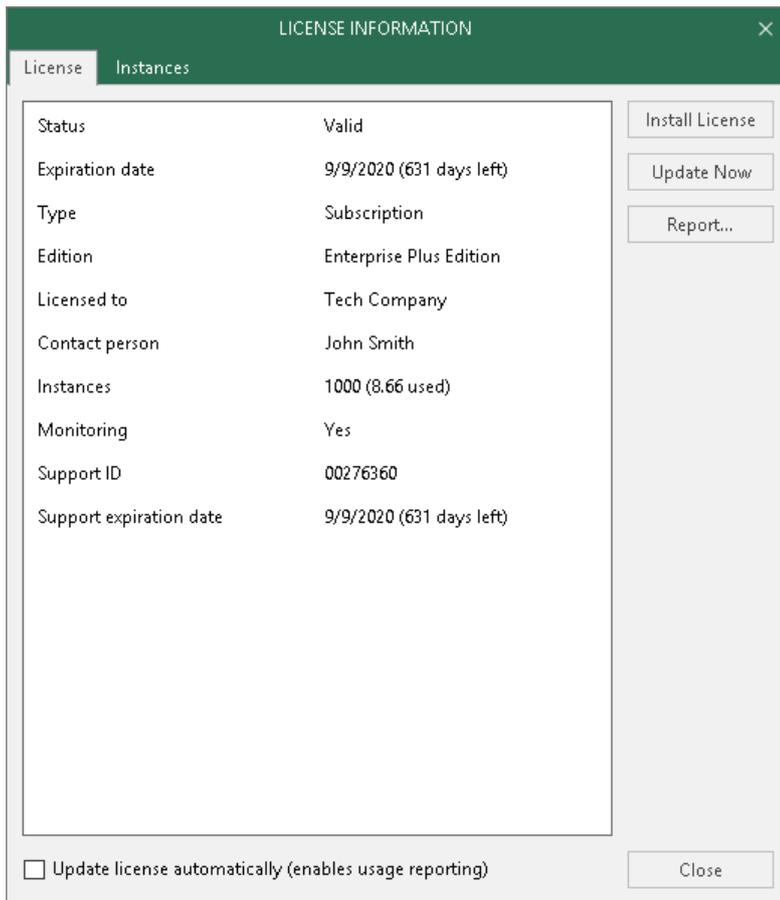
Manual license update can complete with the following results:

- **Operation is successful.** A new license key is successfully generated, downloaded and installed on the backup server or Veeam Backup Enterprise Manager server.
- **A new license is not required.** The currently installed license key does not need to be updated.
- **The Veeam License Update Server has failed to generate a new license.** Such situation can occur due to some error on the Veeam License Update Server side.
- **Veeam Backup & Replication has received an invalid answer.** Such situation can occur due to connectivity issues between the Veeam License Update Server and Veeam Backup & Replication.
- **Licensing by the contract has been terminated.** In such situation, Veeam Backup & Replication automatically disables automatic license update on the backup server or Veeam Backup Enterprise Manager server.

To update the license:

1. From the main menu, select **License**.
2. In the **License Information** window, click **Update Now**.

Statistics on the manual license update process is available under the **System** node in the **History** view. You can double-click the **License key auto-update** job to examine session details for the license update operation.



Updating License Automatically

You can instruct Veeam Backup & Replication to automatically update the license installed on the backup server or Veeam Backup Enterprise Manager server. Automatic license update removes the need to download and install the license manually each time when you purchase the license extension. If the automatic update option is enabled, Veeam Backup & Replication proactively communicates with the Veeam License Update Server to obtain and install a new license before the current license expires.

Requirements and Limitations for Automatic License Update

- Automatic license update is available in all editions of Veeam Backup & Replication operating in the full functionality mode.
- Only licenses that contain a real contract number in the Support ID can be updated with the **Update license key automatically** option.
- If you are managing backup servers with Veeam Backup Enterprise Manager, all license management tasks must be performed in the Veeam Backup Enterprise Manager console. Automatic update settings configured in Veeam Backup Enterprise Manager override automatic update settings configured in Veeam Backup & Replication. For example, if the automatic update option is enabled in Veeam Backup Enterprise Manager but disabled in Veeam Backup & Replication, automatic update will be performed anyway. For more information, see [Veeam Backup Enterprise Manager User Guide](#).

How Automated License Update Works

To update installed licenses automatically, Veeam Backup & Replication performs the following actions:

1. After you enable automatic license update, Veeam Backup & Replication starts sending requests to the Veeam License Update Server on the web (autolk.veeam.com) and checks if a new license key is available. Veeam Backup & Replication sends requests once a week. Communication with the Veeam License Update Server is performed over the HTTPS protocol.
2. Seven days before the expiration date of the current license, Veeam Backup & Replication starts sending requests once a day.
3. When a new license key becomes available, Veeam Backup & Replication automatically downloads it and installs on the backup server or Veeam Backup Enterprise Manager server.

The new license key differs from the previously installed license key in the license expiration date and support expiration date. If you have obtained a license for a greater number of instances, counters in the new license also display the new number of licensed instances.

Automatic license update can complete with the following results:

- **Operation is successful.** A new license key is successfully generated, downloaded and installed on the backup server or Veeam Backup Enterprise Manager server.
- **A new license is not required.** The currently installed license key does not need to be updated.
- **The Veeam License Update Server has failed to generate a new license.** Such situation can occur due to some error on the Veeam License Update Server side.
- **Veeam Backup & Replication has received an invalid answer.** Such situation can occur due to connectivity issues between the Veeam License Update Server and Veeam Backup & Replication.
- **Licensing by the contract has been terminated.** In such situation, Veeam Backup & Replication automatically disables automatic license update on the backup server or Veeam Backup Enterprise Manager server.

Automatic Update Retries

If Veeam Backup & Replication fails to update the license, it displays a notification in the session report and sends an email notification to users specified in the global email settings (if global email settings are configured on the backup server). You can resolve the issue, while Veeam Backup & Replication will keep retrying to update the license.

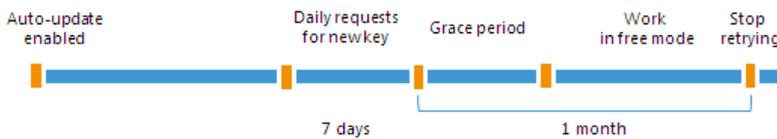
Veeam Backup & Replication retries to update the license key in the following way:

- If Veeam Backup & Replication fails to establish a connection to the Veeam License Update Server, retry takes place every 60 min.
- If Veeam Backup & Replication establishes a connection but you are receiving the "*General license key generation error has occurred*" message, the retry takes place every 24 hours.

The retry period ends one month after the license expiration date or the support expiration date (whichever is earlier). The retry period is equal to the number of days in the month of license expiration. For example, if the license expires in January, the retry period will be 31 day; if the license expires in April, the retry period will be 30 days.

If the retry period is over but the new license has not been installed, the automatic update feature is automatically disabled.

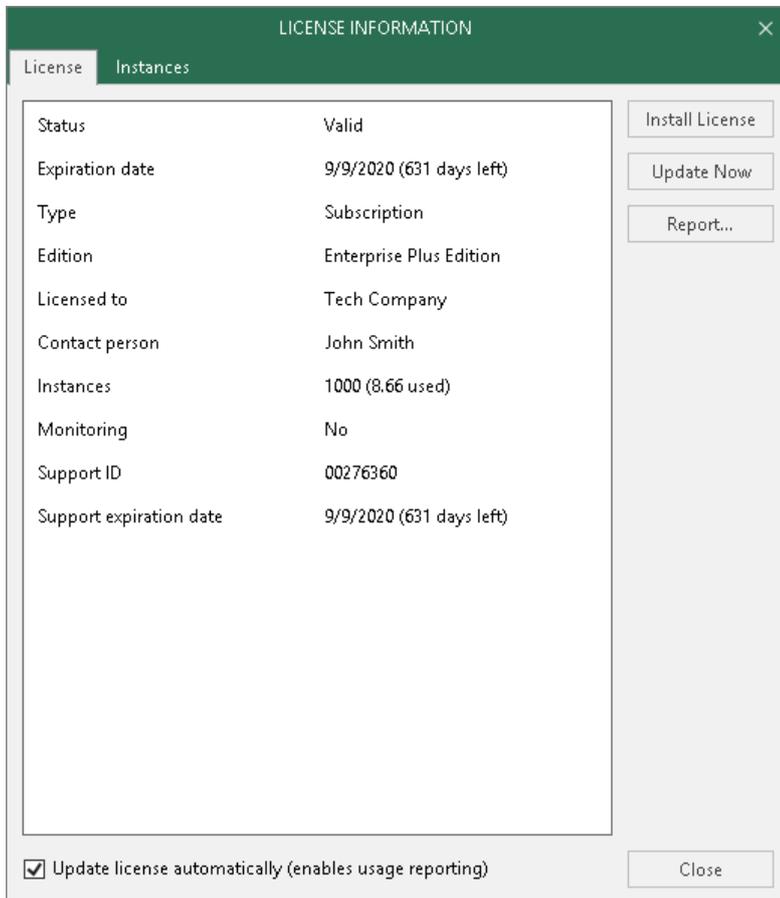
For more information about error cases, see [Appendix A. License Update Session Data](#).



Enabling Automatic License Update

By default, automatic license update is disabled. To enable automatic license update:

1. From the main menu, select **License**.
2. In the **License Information** window, select the **Update license key automatically** check box.



Statistics on the automatic license update process is available under the **System** node in the **History** view. You can double-click the **License key auto-update** job to examine session details for the scheduled or ad-hoc automatic license update.

NOTE:

Enabling license auto update activates [Automatic License Usage Reporting](#). You cannot use license auto update without automatic usage reporting.

Automatic License Usage Reporting

When license auto update is enabled for [Rental](#) licenses, Veeam Backup & Replication performs automatic license usage reporting.

As part of reporting, Veeam Backup & Replication collects statistics on the current license usage and sends it periodically to the Veeam License Update Server. The report provides information about the contract ID, product installation ID, and the maximum number of licensed objects that were managed by Veeam Backup & Replication over the past week (high watermark). The reporting process runs in the background mode, once a week at a random time and day.

The type of reported objects is defined by the product and the installed license. The report can include information about VMs, workstations or servers protected with Veeam backup agents, and so on.

The collected data does not include information on the usage of Veeam Backup & Replication by any individual person identifiable for Veeam, or any data protected by Veeam Backup & Replication.

The collected data allows our back-end system to automatically approve your monthly usage reports as long as they do not deviate from the high watermark value significantly. This helps to keep our report processing costs low, thus allowing us to maintain low rental prices for our solution. Veeam may also use collected data for any other internal business purposes it deems appropriate, including (but not limited to) evaluation, improvement and optimization of Veeam licensing models.

By enabling license auto update you agree with collection, transmission and use of the reporting data. You must not enable license auto update in case you do not agree with such collection, transmission and use.

Community Edition and Full Version

Veeam Backup & Replication is available in two versions: full version and *Community* (free) edition.

- When you run Veeam Backup & Replication in the full version, you get a commercial version of the product that provides access to all product functions (the list of available features depends on the product edition).

For information about product editions, pricing and features available for them, see [Editions Comparison](#).

- When you run Veeam Backup & Replication in the *Community* edition, you get a free version of the product that allows you to use 10 instances to protect your workloads.

Functionality available in the *Community* edition is the same as in the *Standard* edition of the product. For more information, see [Veeam Backup & Replication Community Edition](#).

If you have a valid license installed on the backup server, Veeam Backup & Replication operates in the full version. As soon as your license expires, Veeam Backup & Replication will notify you about it. If you do not purchase a new paid license, the following measures will be taken:

- [For evaluation and NFR licenses] Veeam Backup & Replication will switch to the *Community* edition.
- [For paid licenses] Functionality available in the *Enterprise* and *Enterprise Plus* editions of Veeam Backup & Replication will not be available. Workloads will not be processed by existing jobs (jobs will fail with the *Error* status). However, you will be able to restore machine data from existing backups.

Getting to Know Veeam Backup & Replication

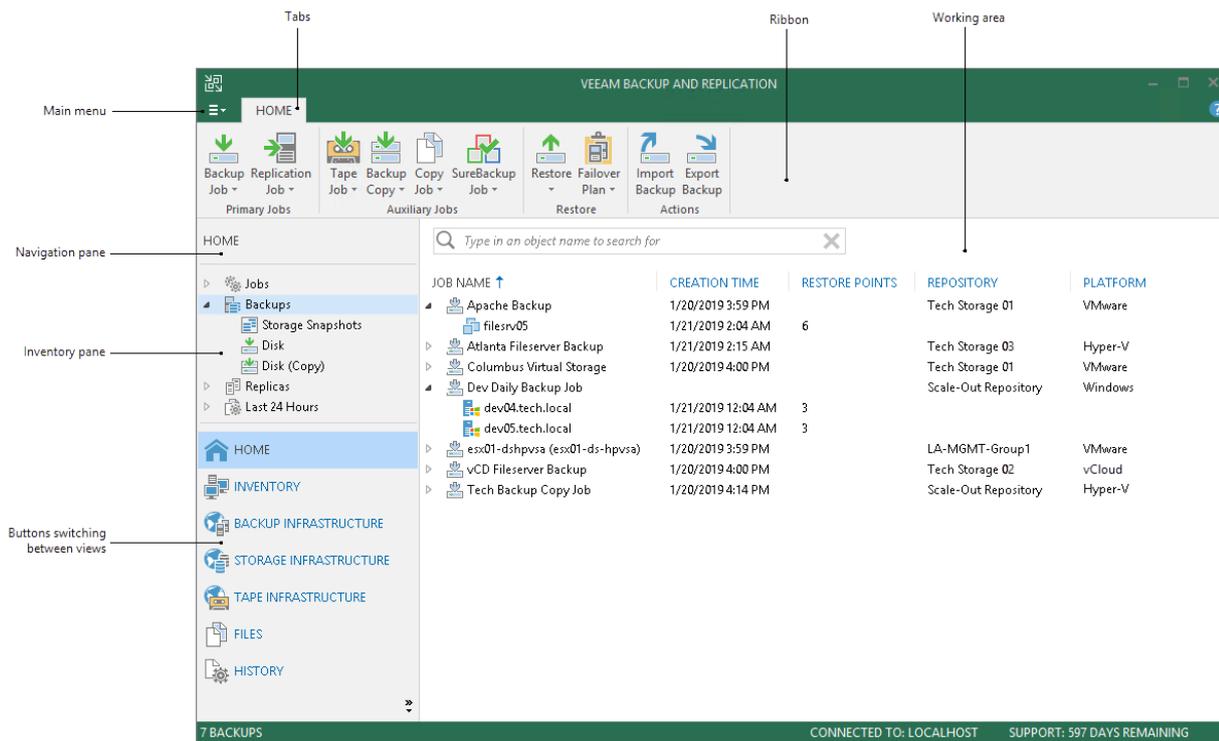
After you install Veeam Backup & Replication, you can get familiar with the product UI, learn about product editions and modes, and find out what functionality these editions and modes offer.

- [Veeam Backup & Replication UI](#)
- [Product Editions](#)

Veeam Backup & Replication UI

The user interface of Veeam Backup & Replication is designed to let you quickly find commands that you need and perform data protection and disaster recovery tasks.

- [Main Menu](#)
- [Navigation Pane](#)
- [Ribbon and Tabs](#)
- [Views](#)
- [Working Area](#)



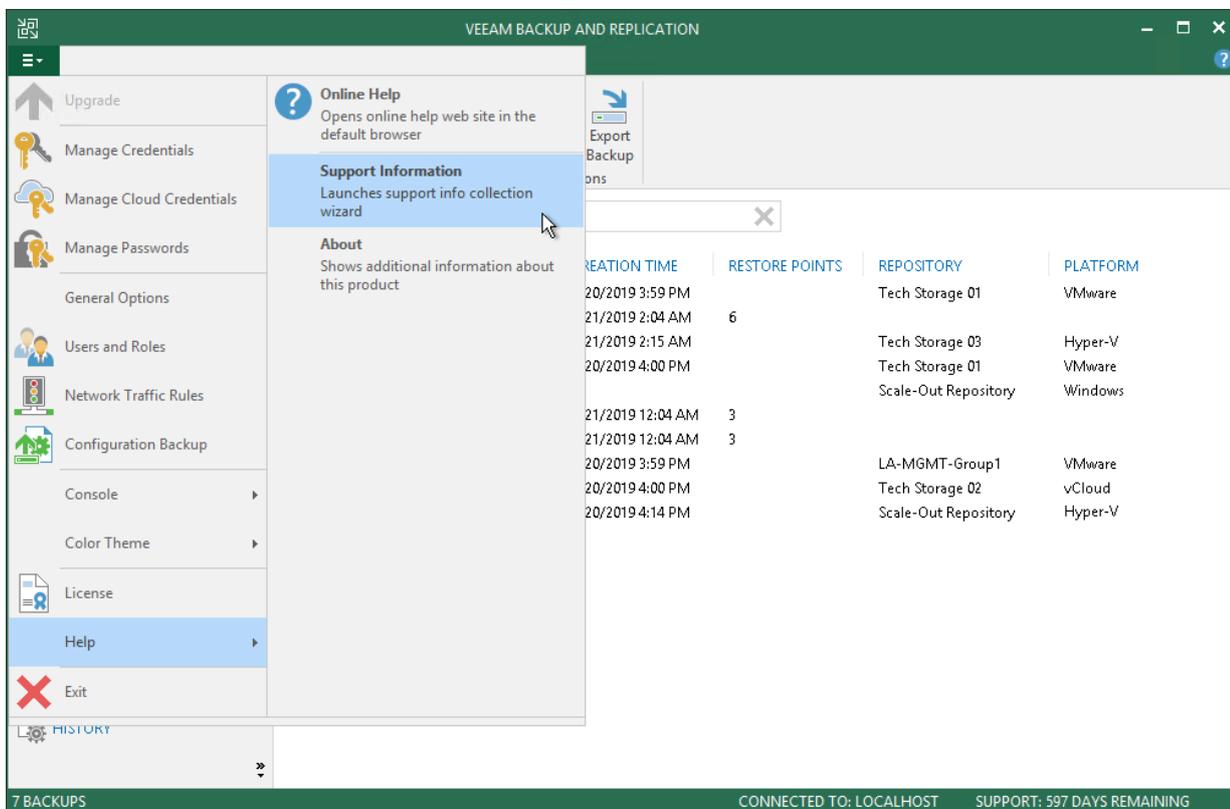
TIP:

To open online help, press **F1** in any Veeam Backup & Replication wizard or window. You will be redirected to the corresponding section of the user guide.

Main Menu

The main menu in Veeam Backup & Replication contains commands related to general application settings. You can perform the following operations using the main menu:

- [Upgrade backup infrastructure components](#)
- [Manage credentials](#)
- [Manage cloud credentials](#)
- [Manage passwords](#)
- [Configure application settings](#)
- [Set up user roles](#)
- [Configure network traffic rules](#)
- [Perform configuration backup and restore](#)
- Start PuTTY and Microsoft PowerShell consoles, and open a remote desktop connection to the backup server
- [Change color theme](#)
- [Work with licenses](#)
- [View Veeam Backup & Replication help](#) and [export program logs](#)
- Exit Veeam Backup & Replication



Navigation Pane

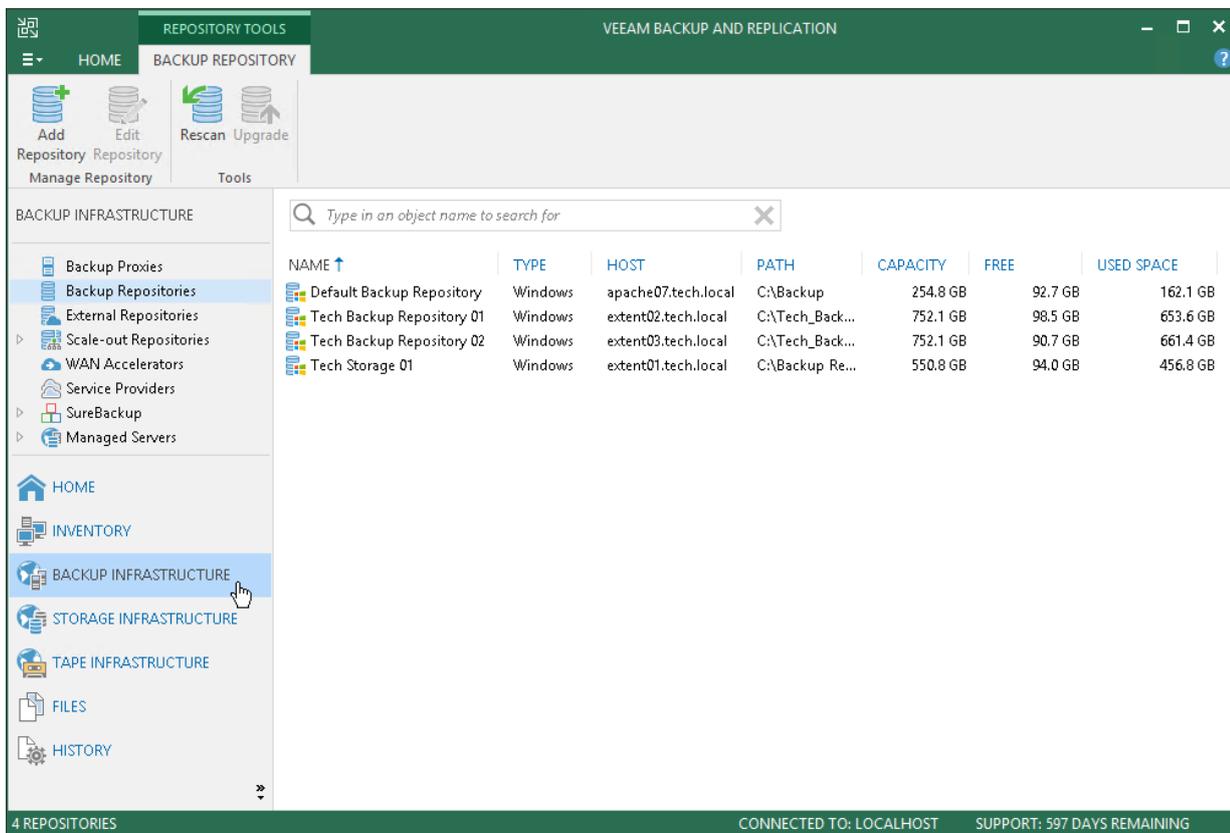
The navigation pane, located on the left of the window, provides centralized navigation and lets you easily access Veeam Backup & Replication items organized in views.

The navigation pane consists of two areas:

- The upper pane, or the inventory pane, displays a hierarchy or list of items relevant for a specific view.

Items displayed in the inventory pane differ depending on the active view. For example, in the **Backup Infrastructure** view, the inventory pane displays a list of backup infrastructure components – virtualization servers, backup proxies, backup repositories and so on. In the **Inventory** view, the inventory pane displays a list of servers added to the backup infrastructure.

- The lower pane contains a set of buttons that let you switch between views.



Ribbon and Tabs

Operation commands in Veeam Backup & Replication are organized in logical groups and displayed under tabs on the ribbon. The ribbon is displayed at the top of the main application window.

On the ribbon, the following tabs are displayed:

- The **Home** tab provides quick access to the most common operations. It lets you configure different types of jobs, perform restore and import operations. This tab is always available, no matter which view is currently active.
- Other tabs contain commands specific for certain items and appear when these items are selected. For example, if you open the **Home** view and select a backup job in the working area, the **Job** tab containing buttons for operations with jobs will appear on the ribbon. If you open the **Files** view and select a file or folder, the **File Tools** tab containing buttons for operations with files will appear on the ribbon.

TIP:

Commands for operations with items in Veeam Backup & Replication are also available from the shortcut menu.

You can minimize the ribbon. To do so, right-click anywhere on the ribbon and select **Minimize the Ribbon**. To restore the ribbon, right-click on the minimized ribbon and clear the **Minimize the Ribbon** option.

The screenshot displays the Veeam Backup and Replication application window. The ribbon at the top is set to the 'JOB' tab, showing buttons for 'Start', 'Stop', 'Retry', 'Active Full', 'Statistics', 'Report', 'Edit', 'Clone', 'Disable', and 'Delete'. Below the ribbon, the 'HOME' view is active, showing a list of jobs. The 'Apache Backup' job is selected, and its details are shown in the main area. The job progress is 99%, and the summary table shows the following data:

SUMMARY		DATA		STATUS		THROUGH
Duration:	02:59	Processed:	28.2 GB (99%)	Success:	0	
Processing rate:	2 MB/s	Read:	202.0 MB	Warnings:	1 ⚠	
Bottleneck:	Proxy	Transferred:	60.6 MB (3.3x)	Errors:	0	0.0 KB/s

Below the summary table, the 'ACTION' column shows the following items:

- Changed block tracking is enabled
- Processing filesrv05
- All VMs have been queued for processing

The bottom status bar indicates '1 JOB SELECTED', 'CONNECTED TO: LOCALHOST', and 'SUPPORT: 597 DAYS REMAINING'.

Views

Veeam Backup & Replication displays its items in views. When you click the button of a specific view in the navigation pane, the view content is displayed in the working area of Veeam Backup & Replication.

Veeam Backup & Replication offers the following views:

- The **Home** view is intended for work with jobs. It also displays a list of created backups and replicas that can be used for various restore operations, and provides statistics on recently performed jobs.
- The **Inventory** view displays the inventory of the virtual infrastructure. The inventory can be presented from different perspectives: **Compute**, **Storage**, **VM Folders** and **VM Tags**. You can use this view to work with VMs, and VM containers or groups.
- The **Backup Infrastructure** view displays a list of backup infrastructure components: servers, hosts, backup proxies, backup repositories and so on. You can use this view for backup infrastructure setup — here you can configure backup infrastructure components that will be used for data protection and disaster recovery tasks.
- The **Storage Infrastructure** view displays a list of storage systems, volumes and snapshots. You can use this view to restore VM data from storage snapshots.
- The **Tape Infrastructure** view displays a hierarchy of tape libraries connected to the tape server. You can use this view to archive data to tapes and restore data from tapes.
- The **Cloud Connect Infrastructure** view displays components of the Veeam Cloud Connect infrastructure. This view can be used by SP to manage TLS certificates, configure cloud gateways and create accounts for users who plan to work with cloud resources.
- The **Files** view displays a file tree of servers added to the backup infrastructure. You can use this view for file copying operations.
- The **History** view displays statistics on operations performed with Veeam Backup & Replication.

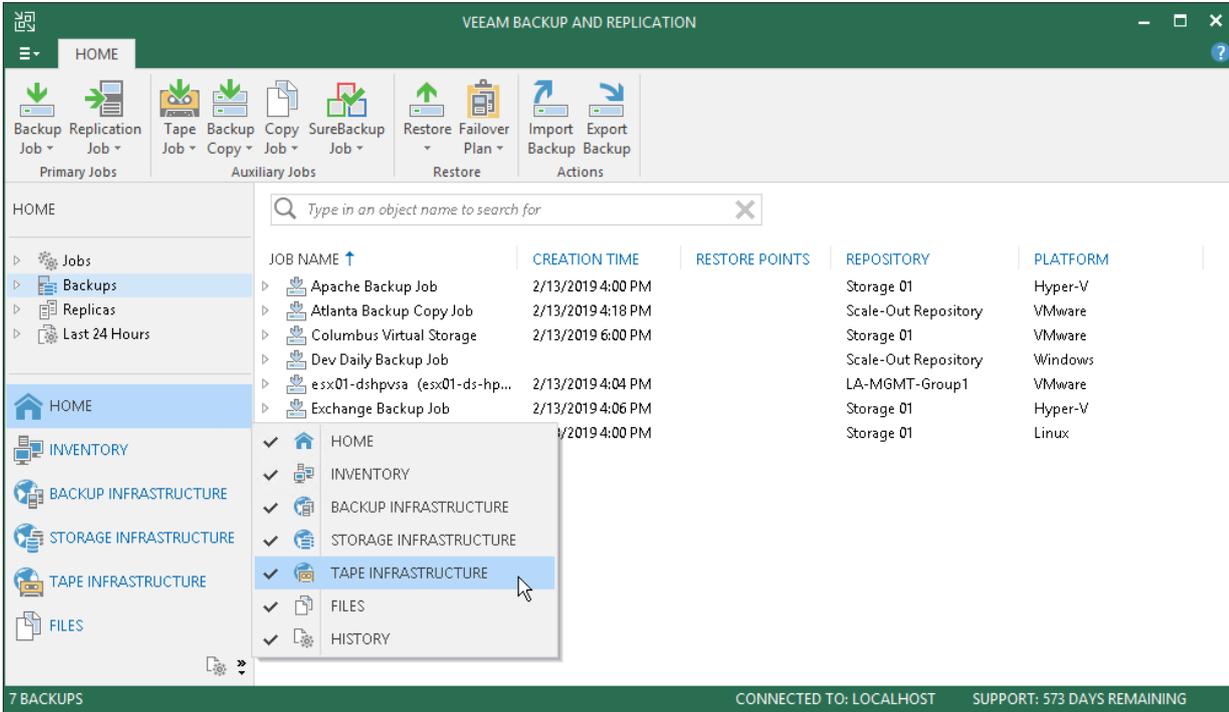
In some situations, some views may not be displayed. Mind the following:

- Right after installation, Veeam Backup & Replication displays only **Backup Infrastructure** and **History** views. To display other views, you must add at least one server or virtualization host to the backup infrastructure.
- Right after installation, Veeam Backup & Replication does not save changes that you make to the navigation pane or views: for example, if you resize panes, display or hide specific views. After you restart the Veeam Backup & Replication console, the main window settings are back to default ones. To save these settings, you must add at least one server or virtualization host to the backup infrastructure.
- To display the **Cloud Connect Infrastructure** view, you must install a valid license that supports the Veeam Cloud Connect functionality.

You can hide views that you do not plan to use. For example, if you do not use tapes for data archiving, you can hide the **Tape Infrastructure** view.

To hide a view:

1. Click the arrow icon below the buttons in the navigation pane.
2. Click the view in the list.



Working Area

The working area of Veeam Backup & Replication displays a list of items relating to a specific view.

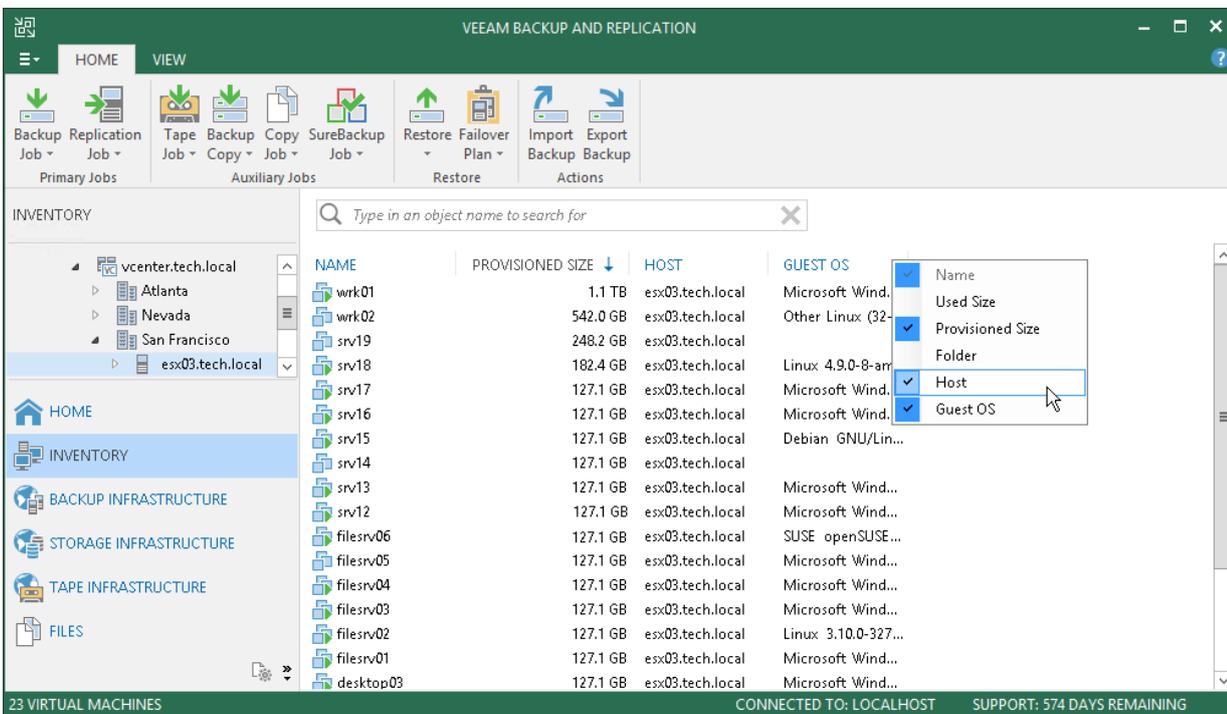
The working area looks different depending on the view that is currently active. For example, if you open the **History** view, the working area will display a list of job sessions and restore tasks performed with Veeam Backup & Replication. If you open the **Inventory** view, the working area will display a list of VMs that reside on servers connected to Veeam Backup & Replication.

Every item is described with a set of properties that are presented as column headers. You can click column headers to sort items by a specific property. For example, to sort VMs by the amount of provisioned storage space, click the **Provisioned Size** header.

TIP:

To hide or display columns in the working area, right-click any column header and do the following:

- Clear the check boxes next to the columns that you want to hide.
- Select the check boxes next to the hidden columns to make them visible.



Changing Color Theme

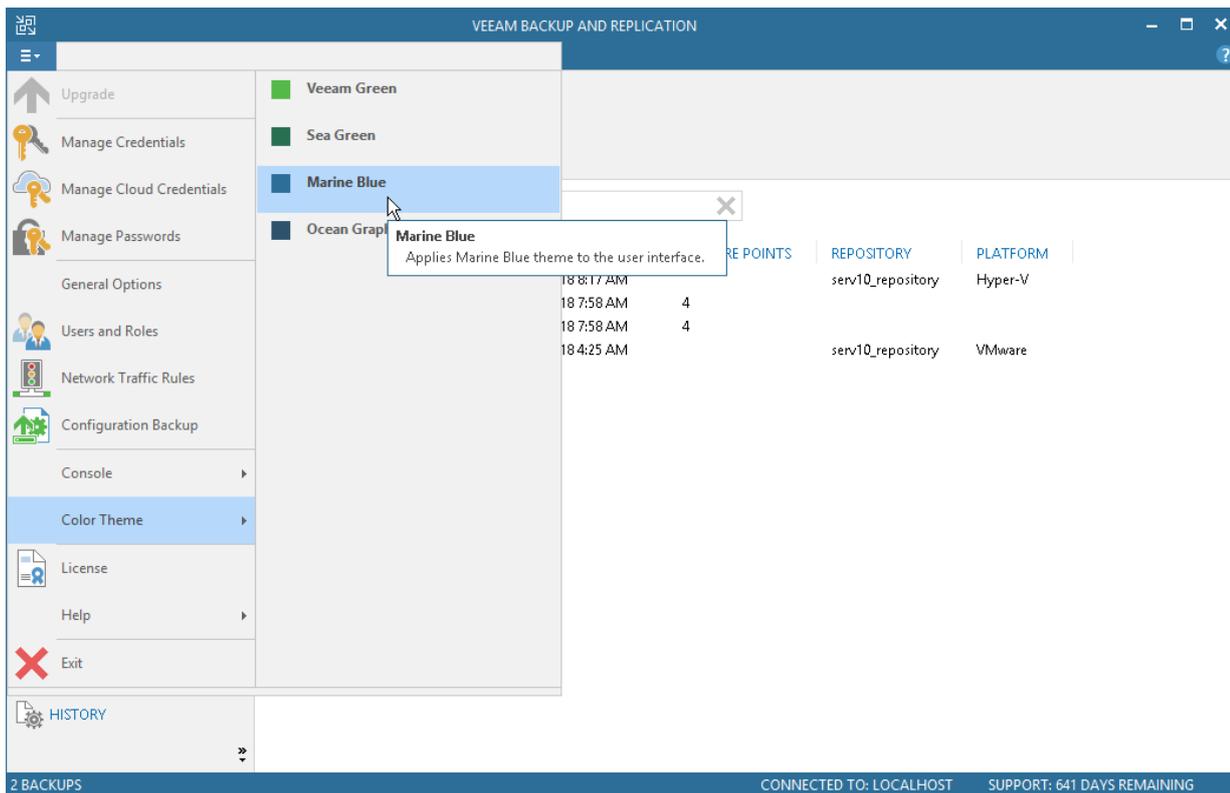
By default, Veeam Backup & Replication uses a 'Sea Green' color theme for the UI. If necessary, you can change the color theme. Changing the color theme can be helpful, for example, if you connect to different backup servers from one remote machine on which the Veeam Backup & Replication console is installed. In this case, you will be able to easily differentiate with which backup server you are currently working.

To change the color theme for Veeam Backup & Replication:

1. From the main menu, select **Color Theme**.
2. Choose one of color themes: *Veeam Green*, *Sea Green*, *Marine Blue*, *Ocean Graphite*.

NOTE:

Color theme settings are applicable for a specific combination of a backup server and user account. For example, the color theme is initially set to the default one. You log on to the Veeam Backup & Replication console under some user account and change the color theme to **Marine Blue**. If you log on to the same backup server under the same account next time, the color theme will be set to **Marine Blue**. If you log on to the same backup server under another account, Veeam Backup & Replication will use the color theme that was previously set for this account — that is, the default color theme.



Product Editions

Veeam Backup & Replication is available in four editions: Community, Standard, Enterprise, and Enterprise Plus Edition. For more information about product editions, pricing and features available for them, see [Editions Comparison](#).

Deployment

To start working with Veeam Backup & Replication, you must configure a backup server – install Veeam Backup & Replication on a machine that meets the system requirements. To do this, you can use the setup wizard or install the product in the unattended mode.

When you install Veeam Backup & Replication, the Veeam Backup & Replication console is automatically installed on the backup server. If you want to access Veeam Backup & Replication remotely, you can install the Veeam Backup & Replication console on a dedicated machine.

Installing Veeam Backup & Replication

Before you install Veeam Backup & Replication, [check prerequisites](#). Then use the **Veeam Backup & Replication** setup wizard to install the product.

Before You Begin

Before you install Veeam Backup & Replication, check the following prerequisites:

- A machine on which you plan to install Veeam Backup & Replication must meet the system requirements. For more information, see [System Requirements](#).
- A user account that you plan to use for installation must have sufficient permissions. For more information, see [Required Permissions](#).
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see [Used Ports](#).
- Veeam Backup & Replication requires .NET Framework 4.6. If .NET Framework 4.6 is not installed, the Veeam Backup & Replication setup will install it on the backup server.
- Veeam Backup & Replication requires Microsoft SQL Server deployed either locally on the backup server or remotely. If Microsoft SQL Server is not installed, the Veeam Backup & Replication setup will install it locally on the backup server:
 - For machines running Microsoft Windows 7, Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, the setup will install Microsoft SQL Server 2012 SP4 Express Edition.
 - For machines running Microsoft Windows Server 2012 or later, the setup will install Microsoft SQL Server 2016 SP1 Express Edition.

If Microsoft SQL Server was installed by the previous product version, Veeam Backup & Replication will connect to the existing configuration database, upgrade it (if necessary) and use it for work.

- You must remove Veeam Backup & Replication components of versions that are not supported by the upgrade procedure from the target machine. You may also need to remove earlier versions of other Veeam products and components.

Step 1. Start Setup Wizard

To start the setup wizard:

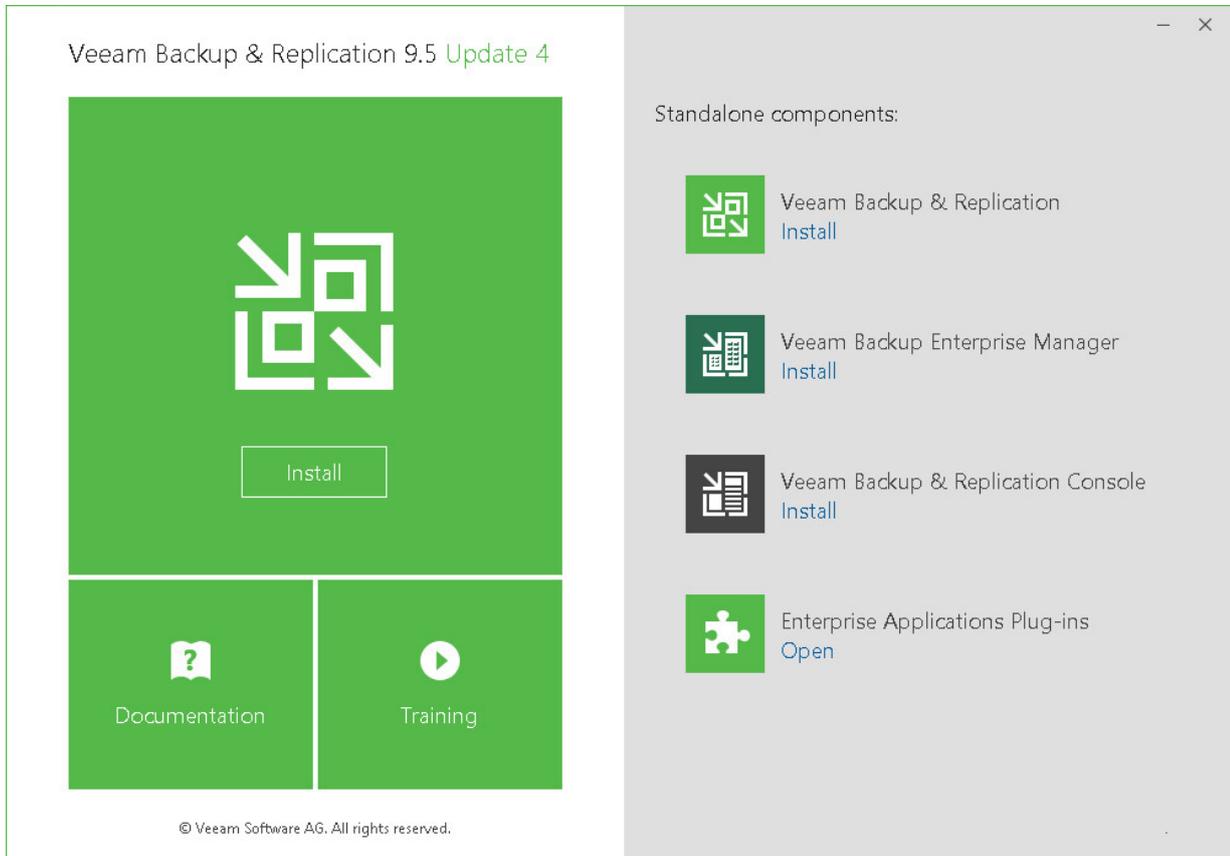
1. Download the latest version of the Veeam Backup & Replication installation image from the [Download Veeam products](#) page.
2. Mount the installation image to the machine on which you plan to install Veeam Backup & Replication or burn the image file to a flash drive or other removable storage device. If you plan to install Veeam Backup & Replication on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM.

To extract the content of the ISO, you can also use the latest versions of utilities that can properly extract data from ISOs of large size and can properly work with long file paths.

3. After you mount the image or insert the disk, Autorun will open a splash screen with installation options. If Autorun is not available or disabled, run the `Setup.exe` file from the image or disk.
4. In the **Veeam Backup & Replication** section of the splash screen, click **Install**.

IMPORTANT!

It is strongly recommended that you install Veeam Backup & Replication using Autorun or the `Setup.exe` file. If you run other installation files from the ISO folders, you may miss some components that need to be installed, and Veeam Backup & Replication may not work as expected.

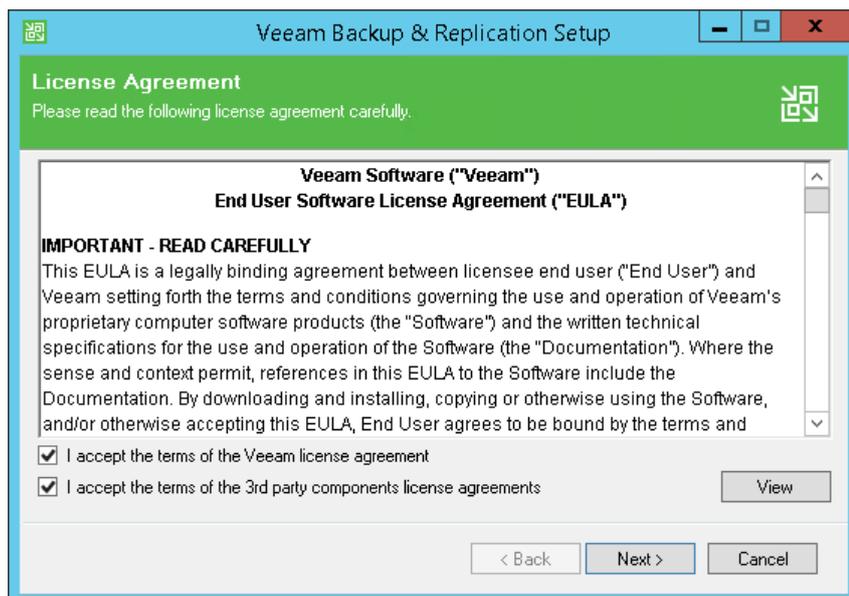


Step 2. Read and Accept License Agreement

At the **License Agreement** step of the wizard, you must accept the license agreement for Veeam and 3rd party components that Veeam incorporates. If you do not accept the license agreement, you will not be able to pass to next step of the setup wizard.

1. Read the license agreement.
To view the license agreement for 3rd party components, click **View**.
2. Select the **I accept the terms of the Veeam license agreement** check box.

3. Select the **I accept the terms of the 3rd party components license agreement** check box.



Step 3. Provide License File

At the **Provide License** step of the wizard, you must specify what license for Veeam Backup & Replication you want to install. You can install the following types of licenses:

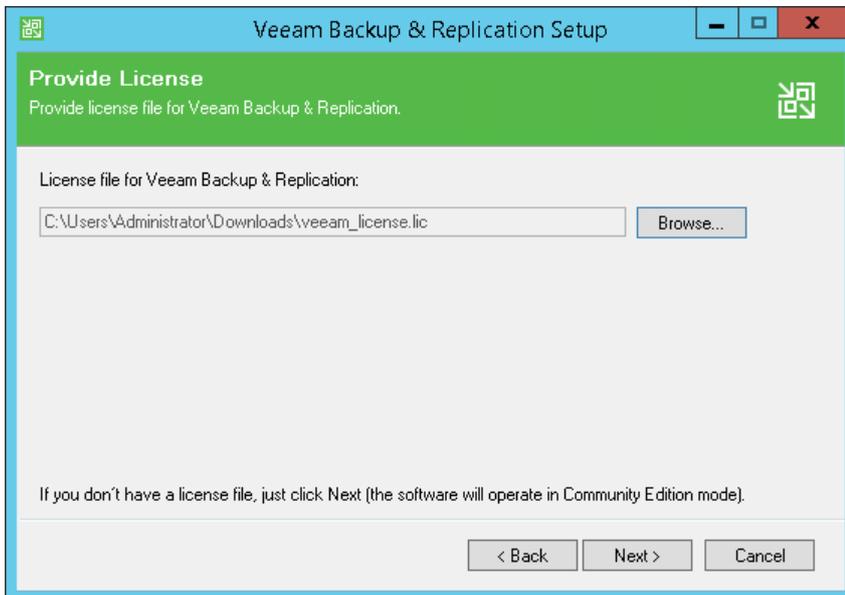
- Evaluation license that was sent to you after you downloaded the product.
- Purchased full license.
- No license.

In this case, after installation Veeam Backup & Replication will operate in the Community Edition mode. You can switch to the full version of the product if you install the license. For more information, see [Community Edition and Full Version](#).

If a valid license is already installed on the machine, the setup wizard will inform you about it. In this case, you can skip the **Provide License** step and move to the next step of the wizard.

To install a license:

1. Next to the **License file for Veeam Backup & Replication** field, click **Browse**.
2. Select a valid license file for Veeam Backup & Replication.



Step 4. Review Components and Select Installation Folder

At the **Program Features** step of the wizard, you can check what components the setup wizard will install on the machine and choose the installation folder.

The setup wizard installs the following components:

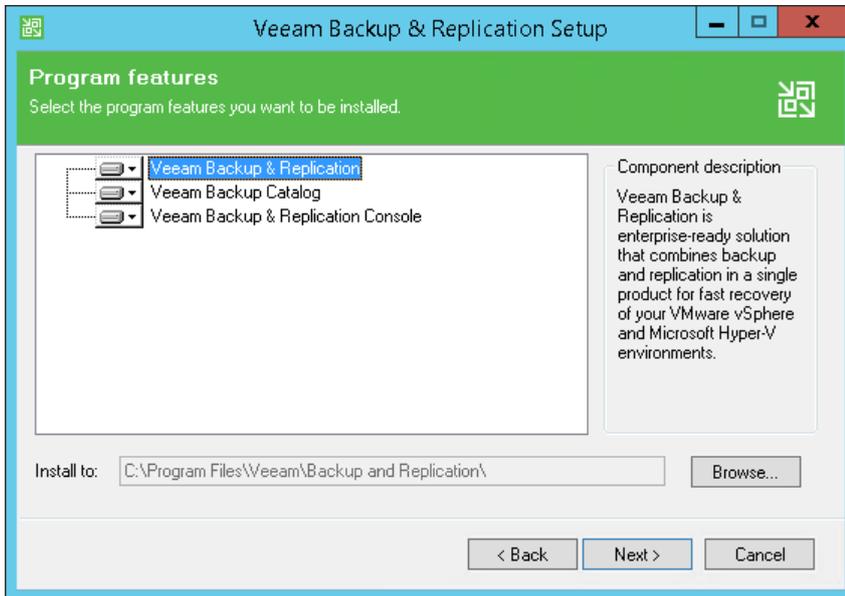
- Veeam Backup & Replication
- Veeam Backup Catalog (component responsible for storing VM guest OS indexing data)
- Veeam Backup & Replication Console

The setup wizard also installs the following components in the background:

- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Oracle
- Veeam Explorer for Microsoft SQL Server
- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for Microsoft OneDrive for Business
- Veeam Backup PowerShell Snap-In These components do not require additional licenses. They are integrated with Veeam Backup & Replication.

To choose the installation folder:

1. On the right of the **Install to** field, click **Browse**.
2. In the **Browse for Folder** window, select the installation folder for the product. The default installation folder is `C:\Program Files\Veeam\Backup and Replication\`.



Step 5. Install Missing Software

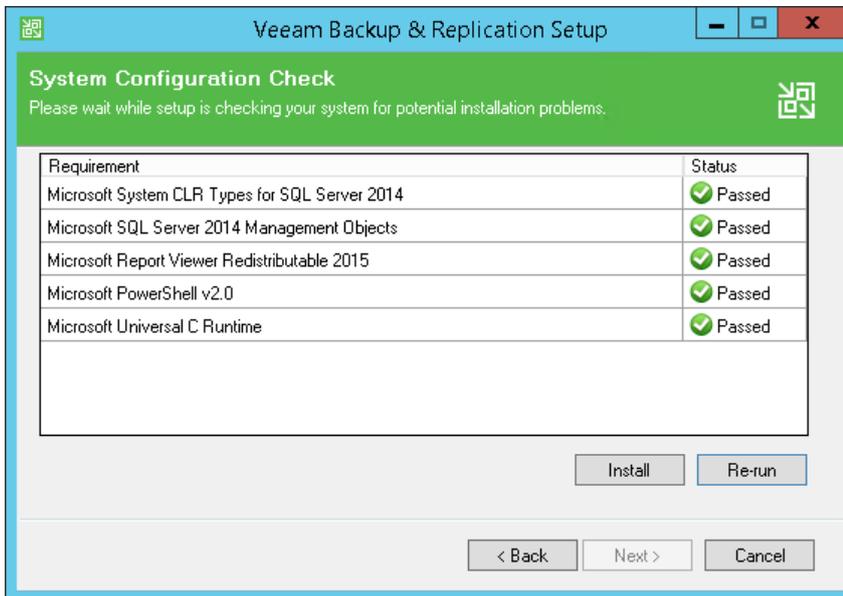
At the **System Configuration Check** step of the wizard, the setup wizard checks if all prerequisite software is installed on the machine. If required software components are missing, the setup wizard will offer you to install them.

You can install missing components automatically or manually.

- To install missing components automatically, click **Install**. The setup wizard will not interrupt the installation process and install the missing components during the current work session.
- To install missing components manually:
 - a. Click **Cancel** and exit the setup wizard.
 - b. Install and enable the necessary components manually on the machine.
 - c. Start the setup wizard again, pass to the **System Configuration Check** step of the wizard and click **Re-run** to repeat the verification.

NOTE:

If all required components are already installed on the machine, the **System Configuration Check** step will be skipped.



Step 6. Specify Installation Settings

At the **Default Configuration** step of the wizard, you can select to install Veeam Backup & Replication with default installation settings or specify custom installation settings.

By default, the setup wizard installs Veeam Backup & Replication with the following settings:

- **Installation folder:** `C:\Program Files\Veeam\Backup and Replication`.
- **vPower cache folder:** the `NfsDatastore` folder on a volume with the maximum amount of free space, for example, `C:\ProgramData\Veeam\Backup\NfsDatastore`.

The vPower cache folder stores the write cache for machines that are started from backups during recovery verification or restore operations. Make sure that you have at least 10 GB of free disk space to store the write cache.

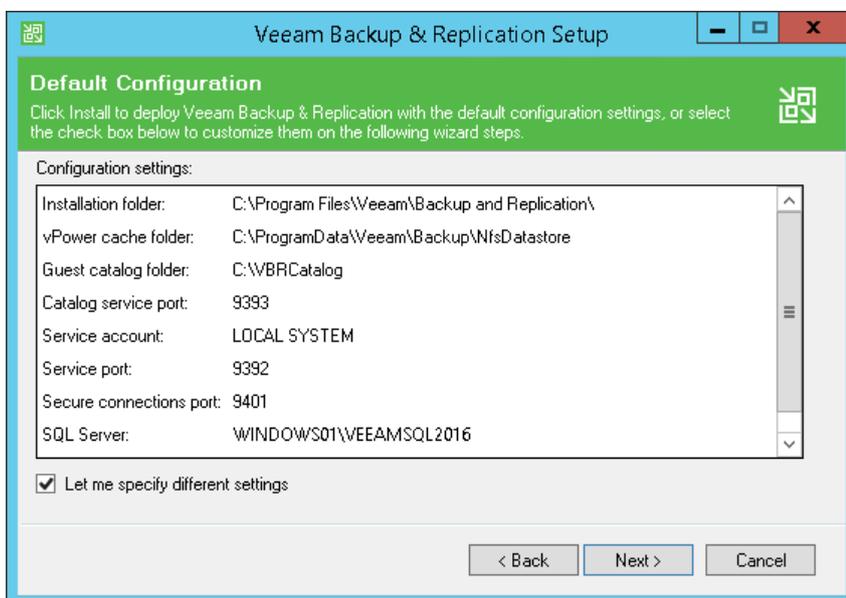
- **Guest catalog folder:** the `VBRCatalog` folder on a volume with the maximum amount of free space, for example, `C:\VBRCatalog`.
The guest catalog folder stores indexing data for VM guest OS files. Indexing data is required for browsing and searching for VM guest OS files inside backups and performing 1-click restore.
- **Catalog service port:** `9393`. The catalog service port is used by the Veeam Guest Catalog Service to replicate catalog data from backup servers to Veeam Backup Enterprise Manager.
- **Service account:** `LOCAL SYSTEM`. The service account is the account under which the Veeam Backup Service runs.
- **Service port:** `9392`. The service port is used by Veeam Backup Enterprise Manager to collect data from backup servers. In addition to it, the Veeam Backup & Replication console uses this service port to connect to the backup server.
- **Secure connections port:** `9401`. The secure connections port is used by the mount server to communicate with the backup server.

- **SQL Server:** *LOCALHOST|VEEAMSQL2012* or *LOCALHOST|VEEAMSQL2016*. During installation, the Veeam Backup & Replication setup installs a new instance of Microsoft SQL Server locally on the backup server:
 - For machines running Microsoft Windows 7, Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, the setup installs Microsoft SQL Server 2012 SP4 Express Edition.
 - For machines running Microsoft Windows Server 2012 or later, the setup installs Microsoft SQL Server 2016 SP1 Express Edition.
- **Database name:** *VeeamBackup*. Veeam Backup & Replication deploys the Veeam Backup & Replication configuration database on the locally installed instance of Microsoft SQL Server.

To use default installation settings:

1. Leave the **Let me specify different settings** check box not selected.
2. Click **Install**. The installation process will begin.

To use custom installation settings, select the **Let me specify different settings** check box. The setup wizard will include additional steps that will let you configure installation settings.



Step 7. Specify Service Account Settings

The **Service Account** step of the wizard is available if you have selected to configure installation settings manually.

You can select an account under which you want to run the Veeam Backup Service:

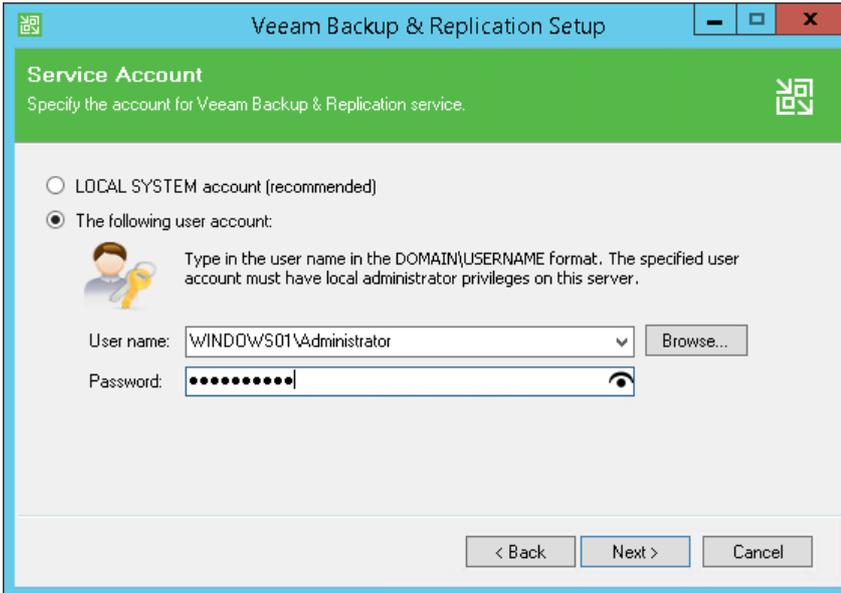
- LOCAL SYSTEM account (recommended, used by default)
- Another user account

The user name of the account must be specified in the *DOMAIN|USERNAME* format.

The user account must have the following rights and permissions:

- The account must be a member of the *Administrators* group on the machine where Veeam Backup & Replication is installed.
- The account must have *db_owner* rights for the configuration database.

Veeam Backup & Replication automatically grants the *Log on as service* right to the specified user account.



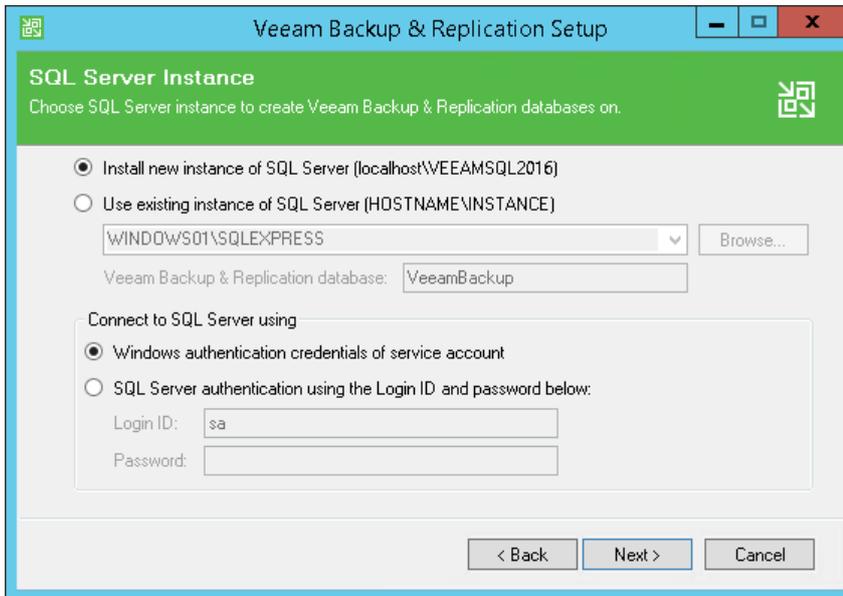
Step 8. Select Microsoft SQL Server

The **SQL Server Instance** step of the wizard is available if you have selected to configure installation settings manually.

You can select a Microsoft SQL Server on which you want to deploy the configuration database, and choose the authentication mode.

1. Select a Microsoft SQL Server:
 - If a Microsoft SQL Server is not installed locally or remotely, select the **Install new instance of SQL Server** option. The setup will install Microsoft SQL Server locally on the backup server:
 - For machines running Microsoft Windows 7, Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, the setup will install Microsoft SQL Server 2012 SP4 Express Edition.
 - For machines running Microsoft Windows Server 2012 or later, the setup will install Microsoft SQL Server 2016 SP1 Express Edition.
 - If a Microsoft SQL Server is already installed locally or remotely, select the **Use existing instance of SQL Server** option. Enter the instance name in the *HOSTNAME|INSTANCE* format. In the **Database** field, specify a name for the Veeam Backup & Replication configuration database.
2. Select an authentication mode to connect to the Microsoft SQL Server instance: Microsoft Windows authentication or SQL Server authentication. If you select the SQL Server authentication, enter credentials for the Microsoft SQL Server account.

If the configuration database already exists on the Microsoft SQL Server (for example, it was created by a previous installation of Veeam Backup & Replication), the setup wizard will notify about it. To connect to the detected database, click **Yes**. If necessary, Veeam Backup & Replication will automatically upgrade the database to the latest version.



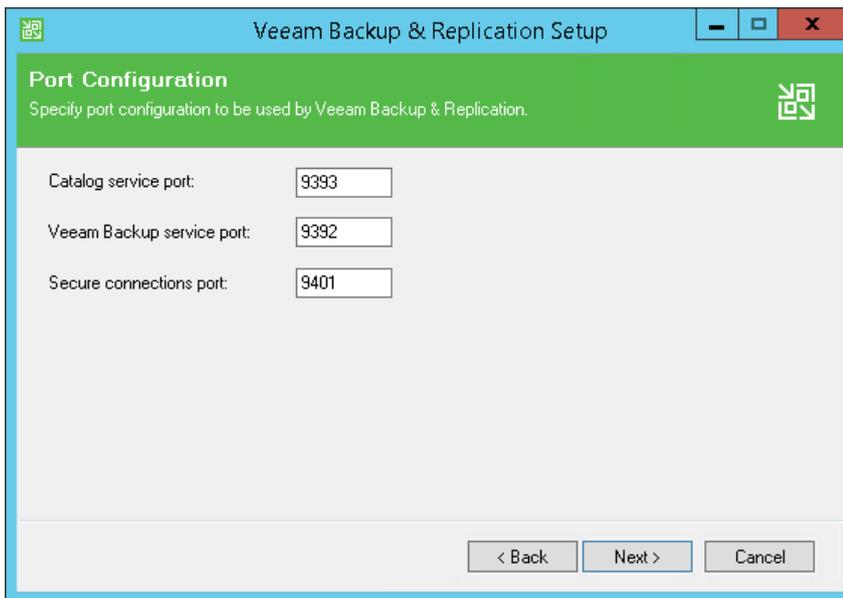
Step 9. Specify Service Ports

The **Port Configuration** step of the wizard is available if you have selected to configure installation settings manually.

You can customize port number values that will be used for communication between backup infrastructure components:

- Catalog service port. The catalog service port is used by the Veeam Guest Catalog Service to replicate catalog data from backup servers to Veeam Backup Enterprise Manager. By default, port 9393 is used.
- Veeam Backup Service port. The service port is used by Veeam Backup Enterprise Manager to collect data from backup servers. In addition to it, the Veeam Backup & Replication console uses this service port to connect to the backup server. By default, port 9392 is used.

- Secure connections port. The secure connections port is used by the mount server to communicate with the backup server. By default, port 9401 is used.



Step 10. Specify Data Locations

The **Data Locations** step of the wizard is available if you have selected to configure installation settings manually.

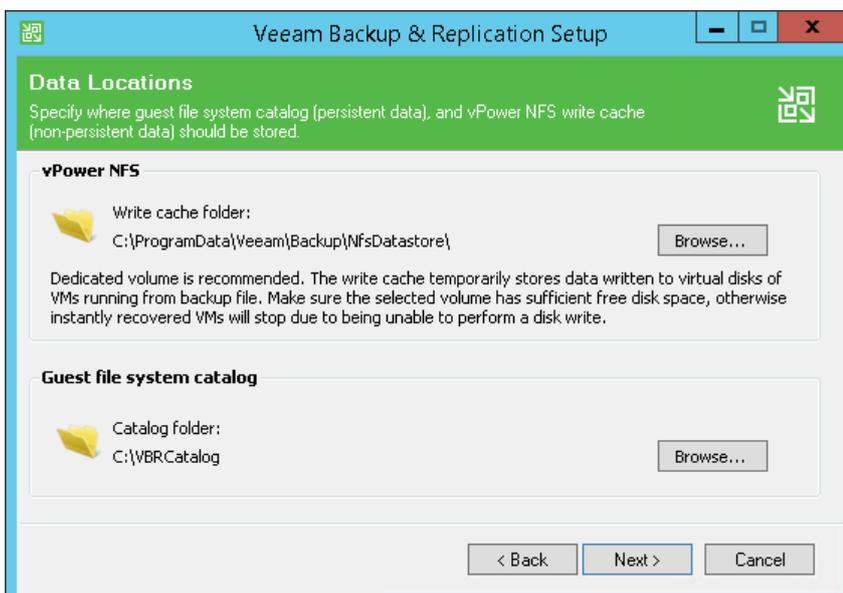
You can specify where the write cache and indexing data must be stored.

1. In the **vPower NFS** section, specify a path to the vPower cache folder. The vPower cache folder stores the write cache for machines that are started from backups during recovery verification or restore operations. Make sure that you have at least 10 GB of free disk space to store the write cache.

By default, the setup wizard creates the vPower cache folder on a volume with the maximum amount of free space, for example, `C:\ProgramData\Veeam\Backup\NfsDatastore`.

2. In the **Guest file system catalog** section, specify a path to the folder where index files must be stored.

By default, the setup wizard creates the `VBRCatalog` folder on a volume with the maximum amount of free space, for example: `C:\VBRCatalog`.

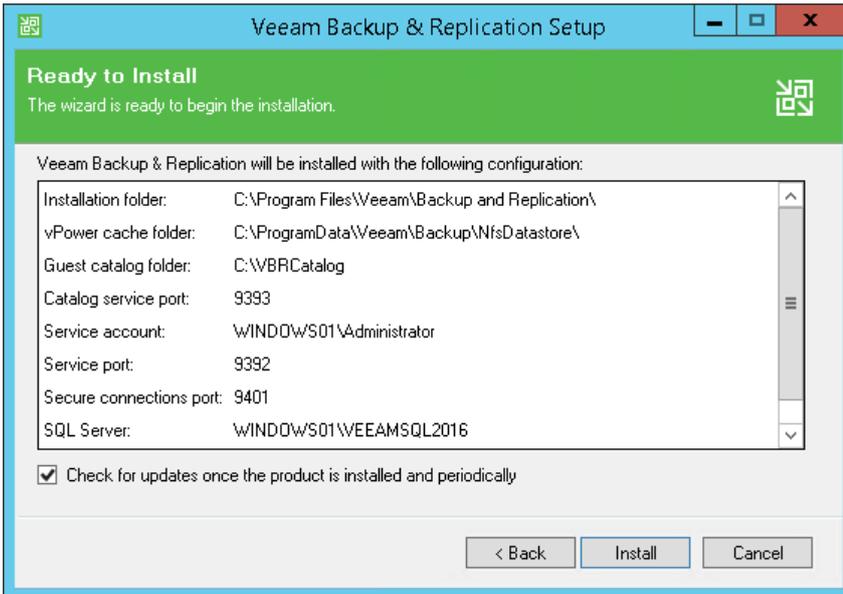


Step 11. Begin Installation

The **Ready to Install** step of the wizard is available if you have selected to configure installation settings manually.

You can review installation settings and start the installation process.

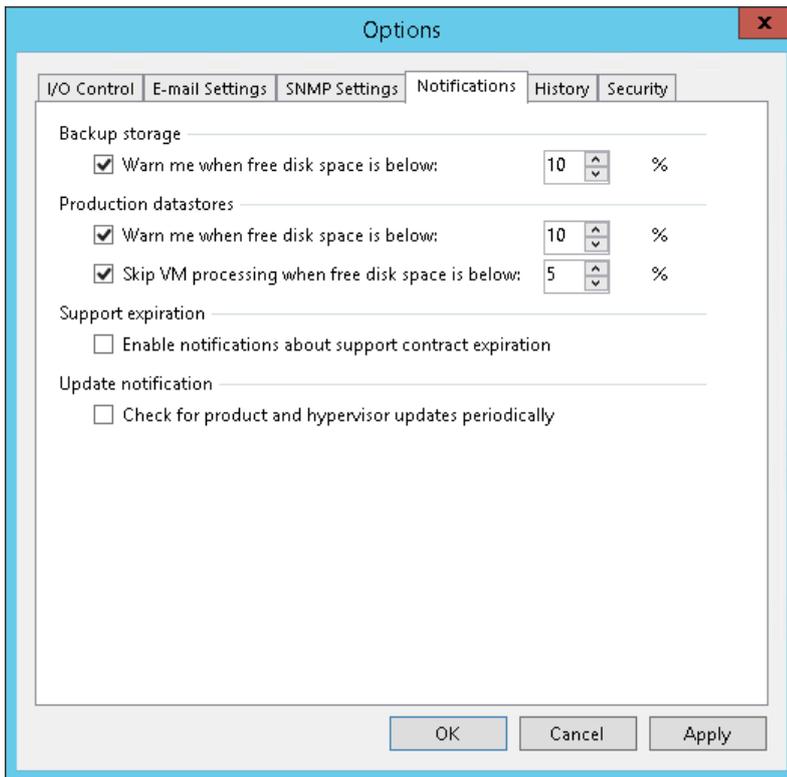
1. If you want Veeam Backup & Replication to periodically check and notify you about product updates, select the **Check for updates once the product is installed and periodically** check box.
2. Click **Install** to begin the installation.
3. Wait for the installation process to complete and click **Finish** to exit the setup wizard.



Step 12. Install Available Patches

It is recommended that you periodically check for Veeam Backup & Replication patches and updates and install them when they are available. Installation of updates and patches lets you make sure that you use the latest version of the product and use its functionality to the full.

You can check for product updates manually or configure Veeam Backup & Replication to automatically notify you about available updates and patches. For more information, see [Specifying Other Notification Settings](#).



TIP:

When you install updates for Veeam Backup & Replication, in the update wizard, select the **Update remote components automatically** check box. Veeam Backup & Replication will automatically update its components on all servers added to the backup infrastructure. For more information, see [Server Components Upgrade](#).

Upgrading to Veeam Backup & Replication 9.5 Update 4

To perform upgrade of Veeam Backup & Replication to version 9.5 Update 4, you must be running version 9.5 (any update) or 9.0 Update #2 on the supported operating system (refer to the [System Requirements](#) section of this document). To upgrade from previous versions, contact Veeam Customer Support.

Upgrade Checklist

Check the following prerequisites before upgrading Veeam Backup & Replication:

1. Are you using Veeam ONE to monitor your backup infrastructure? If yes, upgrade it first. Veeam ONE supports monitoring of backup servers versions 9.5 and 9.0.
2. Are you running Veeam Backup & Replication 9.0 Update 2 or later? If yes, perform the upgrade procedure described [below](#). To upgrade from previous versions, contact Veeam Customer Support.
3. Are you using a per-VM license for VMs or Veeam Agents on your backup server? If yes, obtain a replacement per-instance license from the Veeam Customer Support Portal before upgrading.
4. Are you using a *Perpetual* per-socket license for VMs along with a license for Veeam Agents on your backup server? If yes, obtain a merged license with sockets and instances in the same file from the Veeam Customer Support Portal before upgrading.
5. Check if the backup server you plan to upgrade is installed on the supported operating system. If not, you must migrate the server to the supported OS first, before performing the upgrade. For information on how to perform the migration, see [this Veeam KB article](#).
6. Check if your Veeam Backup & Replication or Veeam Backup Enterprise Manager configuration database is hosted on Microsoft SQL Server 2005. If yes, you must upgrade the Microsoft SQL Server to version 2008 or later first. We recommend Microsoft SQL Server 2014 or later for performance considerations.
7. Are you using Veeam Agents operating in the standalone mode together with Veeam Backup & Replication? If yes, after you upgrade Veeam Backup & Replication to version 9.5 Update 4, you must upgrade Veeam Agent on protected computers to version 3.0 or later.
8. Are you using Cloud Connect? If yes, check with your Cloud Connect service provider if they have already upgraded their system to at least the version you are upgrading to.
9. Make sure there is no active processes, such as any running jobs and restore sessions. We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic and backup copy jobs, so that they do not start during the upgrade.
10. Perform backup of the corresponding SQL Server configuration databases used by backup and Enterprise Manager servers, so that you can easily go back to the previous version in case of issues with upgrade. Note that the built-in configuration backup functionality does not protect Enterprise Manager configuration.
11. Are you using Veeam Backup Enterprise Manager? If yes, start the upgrade procedure from this component. Note that Enterprise Manager 9.5 Update 4 supports version 9.5 and 9.0 backup servers, so you can potentially run both old and new product versions side by side.

Performing Upgrade

To upgrade Veeam Backup & Replication to version 9.5 Update 4, perform the following steps:

1. Download the latest version of the Veeam Backup & Replication ISO from the [Veeam Backup & Replication Download](#) page.
2. Make sure the latest run for all existing jobs has completed successfully. Re-run the failed jobs.
3. Make sure there are no running jobs, restore sessions, Instant VM Recovery sessions and SureBackup jobs. We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic and backup copy jobs temporarily to prevent them from starting during the upgrade.
4. Mount the product ISO and use autorun, or run the `Setup.exe` file.
5. Click the **Upgrade** tile to launch the upgrade wizard.
6. Follow the same steps as described in the [Installing Veeam Backup & Replication](#) section. Be sure to select the same SQL database and instance that was used by the previous product version.

At the **Ready to Install** step of the upgrade wizard, select the **Update remote components automatically** check box to automatically upgrade Veeam Backup & Replication components on all servers added to the backup infrastructure. For more information, see [Server Components Upgrade](#).

7. Wait for the setup program to perform the upgrade.
8. Open the Veeam Backup & Replication console. If necessary, the automated upgrade wizard will automatically appear, prompting you to upgrade the product components running on remote servers. Follow the wizard to complete the upgrade process.
9. If some remote servers are unavailable at the time of upgrade, you can run the upgrade wizard at any time later from the main product menu, or by closing and re-opening the Veeam Backup & Replication console. Note that the out-of-date product components cannot be used by jobs until they are updated to the backup server version.
10. Enable any scheduled jobs that you have disabled before the upgrade.

Note that immediately after upgrade, the backup server performance may decrease. This happens due to the maintenance job that optimizes the configuration database. The process may take up to an hour depending on the database size.

IMPORTANT!

You must upgrade Veeam components on all remote servers with which the backup server communicates during data protection and disaster recovery tasks. If you do not upgrade components on remote servers, Veeam Backup & Replication jobs will fail. For more information, see [Server Components Upgrade](#).

Unattended Upgrade

Veeam Backup & Replication does not support product upgrade in the unattended mode. However, you can perform the following steps:

1. Uninstall the previous version of the product.
2. Install a newer version of the product in the unattended mode. You must connect to the configuration database that was used by the previous product version.

For information on how to install Veeam Backup & Replication in the unattended mode, see [Installing Veeam Backup & Replication in Unattended Mode](#).

Updating Veeam Backup & Replication

Apart from major version releases of Veeam Backup & Replication (e.g. *9.0*, *9.5*, *9.5 Update 4*), Veeam Software provides cumulative updates (e.g. *9.5 Update 4a*). Cumulative updates contain bug fixes, performance enhancements and introduce new features.

Prerequisites

Before you install a cumulative update for Veeam Backup & Replication 9.5 Update 4, check the following prerequisites:

- Make sure you have Veeam Backup & Replication 9.5 Update 4 installed (RTM build number – 9.5.4.2399, or GA build number – 9.5.4.2615).

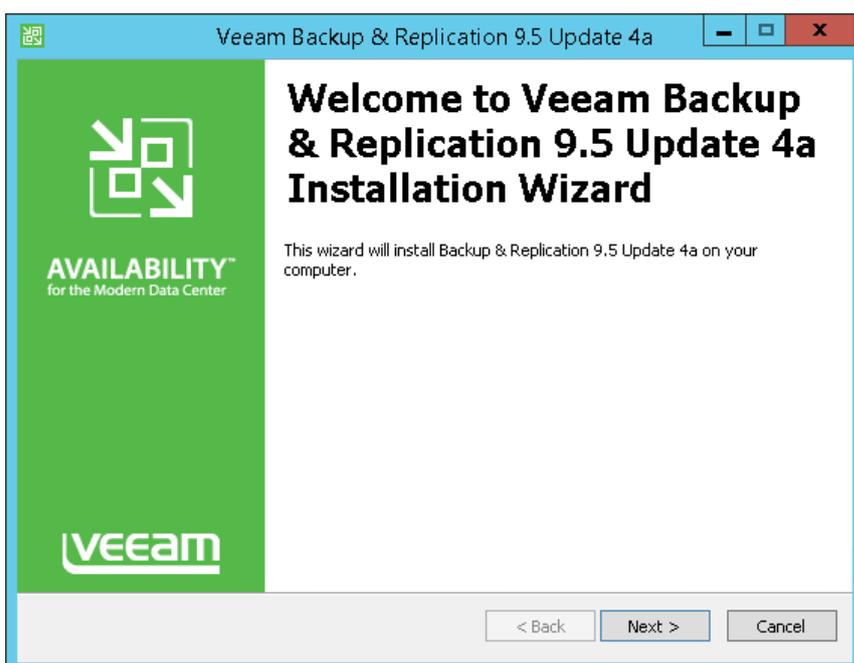
For information on how to upgrade from product versions 9.0 Update 2 or 9.5, see [Upgrading to Veeam Backup & Replication 9.5 Update 4](#).

- Disable all Veeam Backup & Replication jobs and finish all restore processes.
- Close Veeam Backup & Replication processes in the Task Manager.

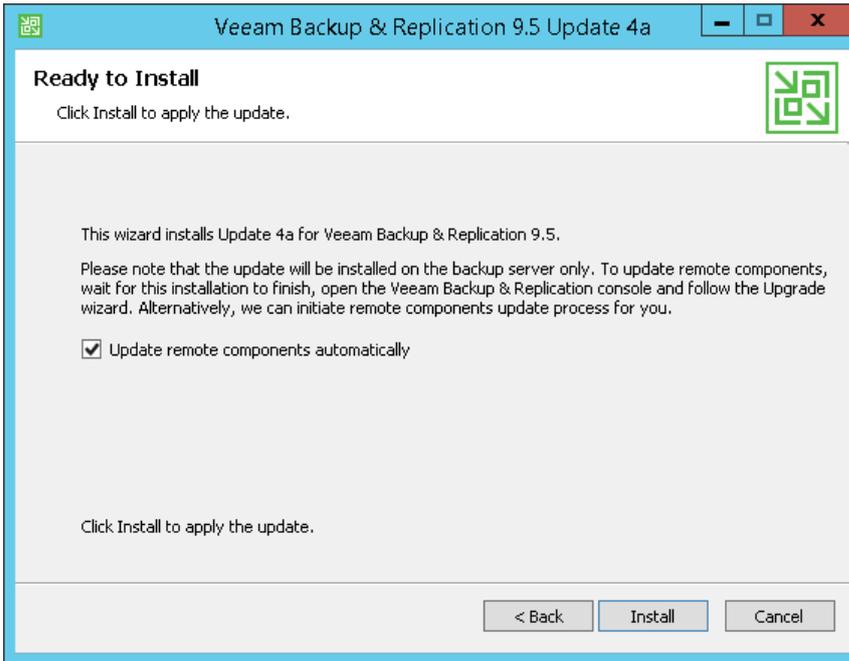
Performing Update

To install the latest update for Veeam Backup & Replication 9.5 Update 4, perform the following steps:

1. Go to the [Veeam Backup & Replication Download](#) page.
2. In the **Latest Updates** section, click **Overview/Download**.
You will be redirected to the Veeam KB article where you can download the update.
3. In the **More Information** section of the Veeam KB article, click **DOWNLOAD UPDATE**.
4. Run the downloaded `veeam_backup_9.5.4.XXXX.updateX_setup.exe` file to launch the update wizard.
5. In the update wizard, click **Next**.



6. Select the **Update remote components automatically** and click **Install**.



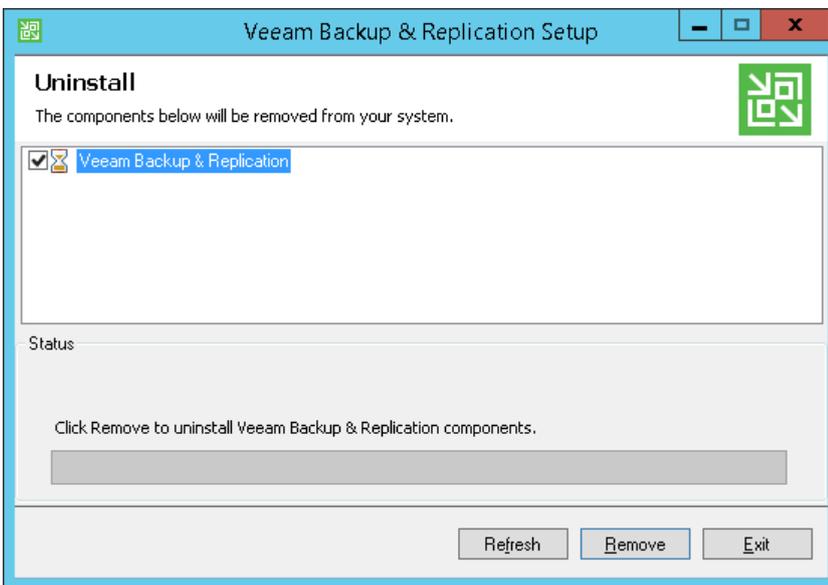
For information on how to update Veeam Backup & Replication in the unattended mode, see [Installing Updates in Unattended Mode](#).

Uninstalling Veeam Backup & Replication

To uninstall Veeam Backup & Replication:

1. From the **Start** menu, select **Control Panel > Programs and Features**.
2. In the programs list, right-click **Veeam Backup & Replication** and select **Uninstall**. If you have Veeam Backup Enterprise Manager installed on this machine, Veeam Backup & Replication will uninstall both components. Wait for the process to complete.
3. If the program list contains additional Veeam Backup & Replication components, right-click the remaining components and select **Uninstall**.

The Veeam Backup & Replication configuration database is not removed during the uninstall process. All configuration data stored in the database remains as well.



Installing Veeam Backup & Replication Console

By default, the Veeam Backup & Replication console is installed on the backup server automatically when you install Veeam Backup & Replication. You do not need to install the console manually.

However, in addition to the default console, you can install the Veeam Backup & Replication console on a dedicated machine to access the backup server remotely. You can install as many remote consoles as you need. For more information, see [Backup & Replication Console](#).

Before you install the Veeam Backup & Replication console, [check prerequisites](#). Then use the **Veeam Backup & Replication Console Setup** wizard to install the console.

Before You Begin

Before you install the Veeam Backup & Replication console, check the following prerequisites:

- The Veeam Backup & Replication console must be of the same version as Veeam Backup & Replication installed on the backup server.
- A machine on which you plan to install the Veeam Backup & Replication console must meet the system requirements. For more information, see [System Requirements](#).
- A user account that you plan to use for installation must have sufficient permissions. For more information, see [Required Permissions](#).
- Backup infrastructure components communicate with each other over specific ports. These ports must be open. For more information, see [Used Ports](#).
- The Veeam Backup & Replication console requires .NET Framework 4.6. If .NET Framework 4.6 is not installed, the Veeam Backup & Replication setup will install it on the machine.

Step 1. Start Setup Wizard

To start the setup wizard:

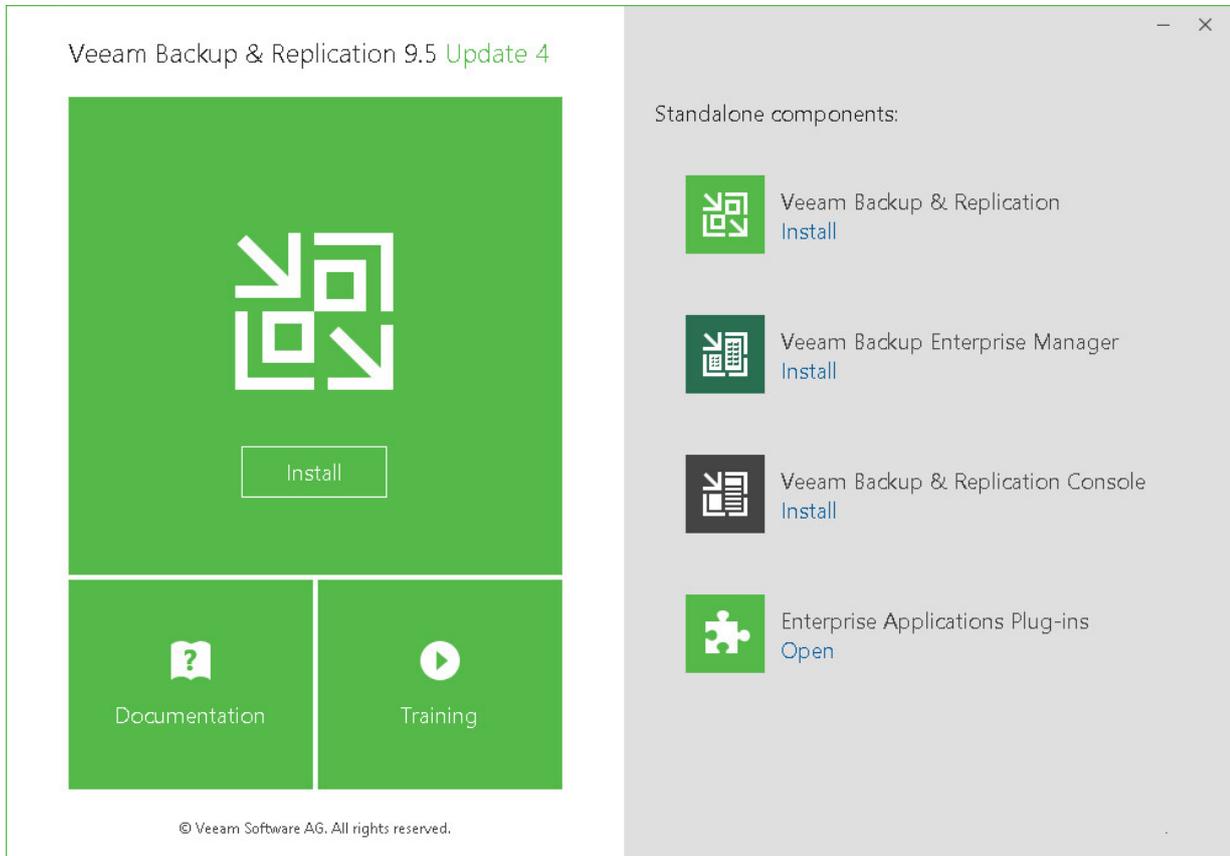
1. Download the latest version of the Veeam Backup & Replication installation image from www.veeam.com/downloads.html.
2. Use disk image emulation software to mount the installation image to the machine where you plan to install Veeam Backup & Replication or burn the image file to a flash drive or other removable storage device. If you plan to install Veeam Backup & Replication on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM.

To extract the content of the ISO, you can also use the latest versions of utilities that can properly extract data from ISOs of large size and can properly work with long file paths.

3. After you mount the image or insert the disk, Autorun will open a splash screen with installation options. If Autorun is not available or disabled, run the `Setup.exe` file from the image or disk.
4. On the splash screen, click **Veeam Backup & Replication Console**.

IMPORTANT!

It is strongly recommended that you install the Veeam Backup & Replication console using Autorun or the `Setup.exe` file. If you run other installation files from the ISO folders, you may miss some components that need to be installed, and Veeam Backup & Replication may not work as expected.

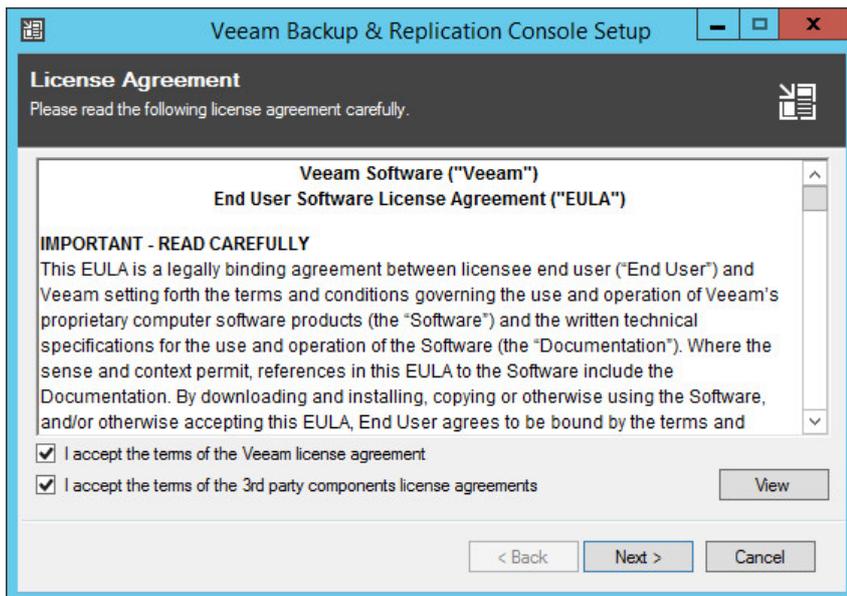


Step 2. Read and Accept License Agreement

At the **License Agreement** step of the wizard, you must accept the license agreement for Veeam and 3rd party components that Veeam incorporates. If you do not accept the license agreement, you will not be able to pass to next step of the setup wizard.

1. Read the license agreement.
To view the license agreement for 3rd party components, click **View**.
2. Select the **I accept the terms of the Veeam license agreement** check box.
3. Select the **I accept the terms of the 3rd party components license agreement** check box.

4. Click **Next**.

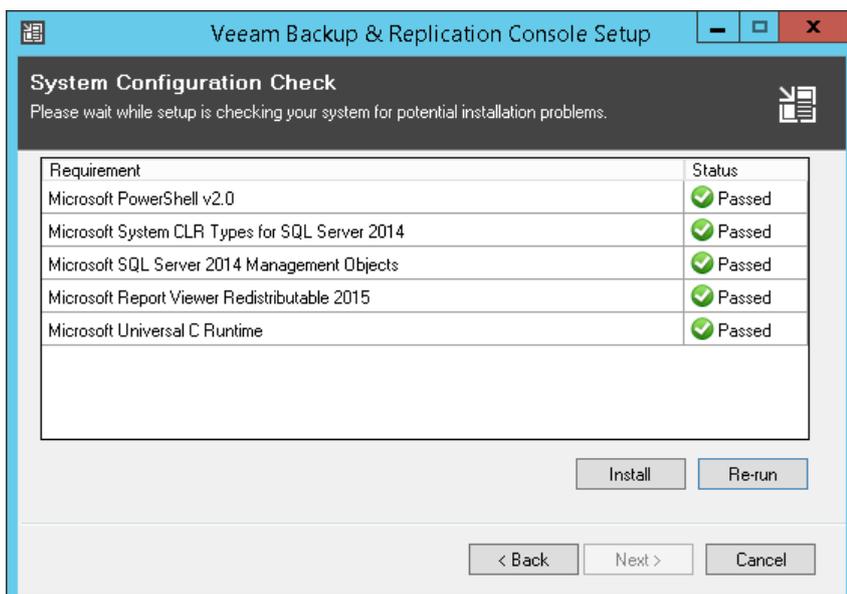


Step 3. Install Missing Software

At the **System Configuration Check** step of the wizard, the setup wizard checks if all prerequisite software is installed on the machine. If required software components are missing, the setup wizard will offer you to install them.

You can install missing components automatically or manually.

- To install missing components automatically, click **Install**. The setup wizard will not interrupt the installation process and install the missing components in the work current session.
- To install missing components manually:
 - a. Click **Cancel** and exit the setup wizard.
 - b. Install and enable the necessary components manually on the machine.
 - c. Start the setup wizard again, pass to the **System Configuration Check** step of the wizard and click **Re-run** to repeat the verification.



Step 4. Specify Installation Settings

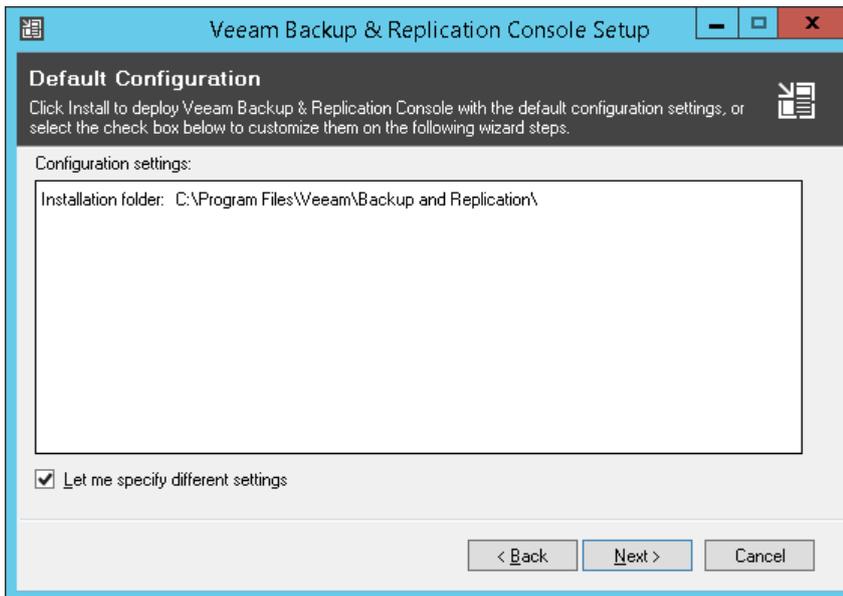
At the **Default Configuration** step of the wizard, you can select to install the Veeam Backup & Replication console with default installation settings or specify custom installation settings.

By default, the setup wizard installs the Veeam Backup & Replication console with the following settings: installation folder – C:\Program Files\Veeam\Backup and Replication.

To use default installation settings:

1. Leave the **Let me specify different settings** check box not selected.
2. Click **Install**. The installation process will begin.

To specify custom installation settings, select the **Let me specify different settings** check box. The setup wizard will include additional steps that will let you configure installation settings.



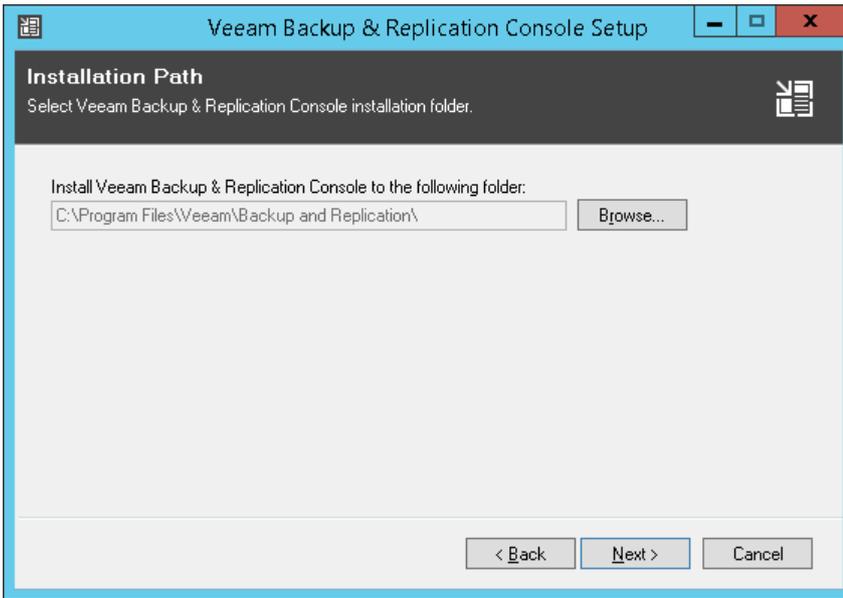
Step 5. Specify Installation Path

The **Installation Path** step of the wizard is available if you have selected to configure installation settings manually.

At the **Installation Path** step of the wizard, you can choose the installation folder for the Veeam Backup & Replication console.

1. On the right of the **Install Veeam Backup & Replication Console to the following folder** field, click **Browse**.

2. In the **Browse for Folder** window, select the installation folder for the product. The default folder is C:\Program Files\Veeam\Backup and Replication\.

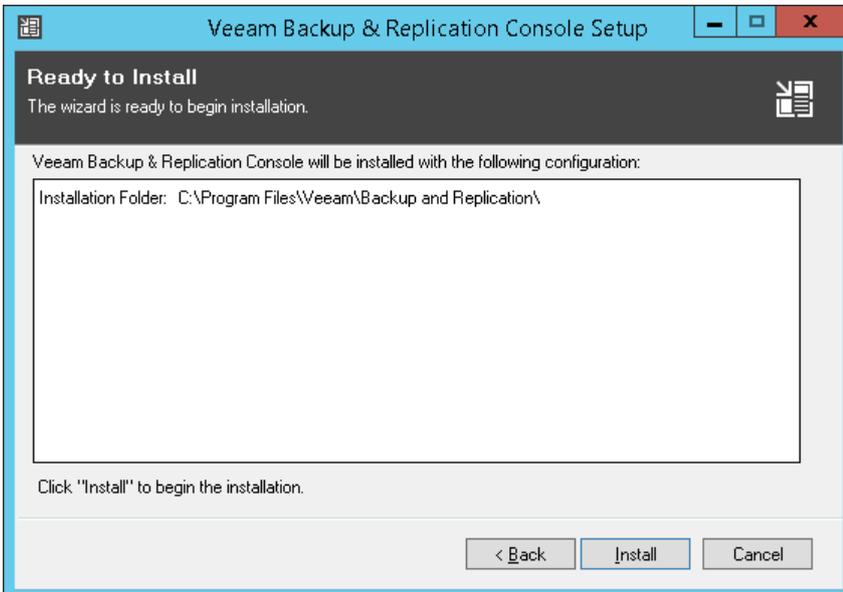


Step 6. Begin Installation

The **Ready to Install** step of the wizard is available if you have selected to configure installation settings manually.

At the **Ready to Install** step of the wizard, you can review the installation settings and start the installation process.

1. Click **Install** to begin the installation.
2. Wait for the installation process to complete and click **Finish** to exit the setup wizard.



Installing Veeam Backup & Replication in Unattended Mode

You can install Veeam Backup & Replication in the unattended mode using the command line interface. The unattended installation mode does not require user interaction. You can use it to automate the installation process in large deployments.

Installation Order

Veeam Backup & Replication components must be installed in the order specified below. The order depends on the type of server that you plan to deploy: backup server or Veeam Backup Enterprise Manager server.

Backup Server

If you want to deploy the backup server (server running Veeam Backup & Replication), you must install components in the following order:

1. [Veeam Backup Catalog](#)
2. [Veeam Backup & Replication Server](#)
3. Veeam Explorers:
 - [Veeam Explorer for Active Directory](#)
 - [Veeam Explorer for Exchange](#)
 - [Veeam Explorer for Oracle](#)
 - [Veeam Explorer for SharePoint and Veeam Explorer for Microsoft OneDrive for Business](#)
 - [Veeam Explorer for Microsoft SQL](#)

Veeam Backup & Replication Console

If you want to deploy the Veeam Backup & Replication console, you must install [Veeam Backup & Replication Console](#).

Veeam Backup Enterprise Manager Server

If you want to deploy the Veeam Backup Enterprise Manager server (server running Veeam Backup Enterprise Manager), you must install components in the following order:

1. [Veeam Backup Catalog](#)
2. [Veeam Backup Enterprise Manager](#)

Veeam Cloud Connect Portal

If you want to deploy Veeam Cloud Connect Portal, you must install components in the following order:

1. [Veeam Backup Enterprise Manager](#)
2. [Veeam Cloud Connect Portal](#)

Before You Begin

Before you start unattended installation, make sure that you perform the following steps:

1. [For backup server] Pre-install the following components on the target machine:
 - Microsoft SQL Server 2008 or later (all editions including Express Edition are supported)
 - Microsoft .NET Framework 4.6
 - Microsoft Report Viewer Redistributable 2015
 - Microsoft Universal C Runtime
 - Microsoft SQL Server 2014 System CLR Types
 - Microsoft SQL Server 2014 Management Objects
2. [For Veeam Explorers] Make sure that the version of a Veeam Explorer that you plan to install matches the version of the Veeam Backup & Replication console on the target machine.
3. [For Veeam Backup Enterprise Manager server] Pre-install the following components on the target machine:
 - Microsoft SQL Server 2008 or later (all editions including Express Edition are supported)
 - Microsoft Report Viewer Redistributable 2015
 - Microsoft Universal C Runtime
 - Microsoft SQL Server 2014 System CLR Types
 - Microsoft SQL Server 2014 Management Objects
 - IIS components: Default Document Component, Directory Browsing Component, HTTP Errors Component, Static Content Component, Windows Authentication Component, URL Rewrite Module 2.0
 - Update 4.0.3 for Microsoft .NET Framework 4.0
For more information, see [this Microsoft KB article](#).
4. Download the Veeam Backup & Replication installation image from the Veeam website. You can burn the downloaded image to a flash drive or mount the image to the target machine using disk image emulation software.
5. Check the system requirements. For more information, see [System Requirements](#).
6. Log on to the target machine under the account that has the local Administrator permissions on the machine. For more information, see [Required Permissions](#).
7. Obtain a license file. The license file is required for Veeam Backup Enterprise Manager installation and is optional for Veeam Backup & Replication installation. If you do not specify a path to the license file during Veeam Backup & Replication installation, Veeam Backup & Replication will operate in the Community Edition mode.

Installation Command-Line Syntax

You can install the following Veeam Backup & Replication components in the unattended mode:

- [Veeam Backup Catalog](#)
- [Veeam Backup & Replication Server](#)
- [Veeam Backup & Replication Console](#)
- [Veeam Explorer for Microsoft Active Directory](#)
- [Veeam Explorer for Microsoft SQL Server](#)
- [Veeam Explorer for Microsoft Exchange](#)
- [Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business](#)
- [Veeam Explorer for Oracle](#)
- [Veeam Backup Enterprise Manager](#)
- [Veeam Cloud Connect Portal](#)

Veeam Backup Catalog

To install Veeam Backup Catalog, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>"  
ACCEPT_THIRDPARTY_LICENSES="1" [INSTALLDIR="<path_to_installdir  
>"] [VM_CATALOGPATH="<path_to_catalog_shared_folder>"] [VBRC_SERVICE_USER="<Veeam_Guest  
Catalog_Service_account>"] [VBRC_SERVICE_PASSWORD="<Veeam_Guest_Catalog_Service_account  
_password>"] [VBRC_SERVICE_PORT="<Veeam_Guest_Catalog_Service_port>"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	<p>Creates an installation log file with the verbose output.</p> <p>Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared.</p> <p>Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\Catalog.txt"</p>
/q	n	Yes	<p>Sets the user interface level to "no", which means no user interaction is needed during installation.</p>
/i	setup file	Yes	<p>Installs Veeam Backup Catalog. Specify a full path to the setup file as the parameter value.</p> <p>Example: /i "C:\Veeam\VeeamBackupCatalog64.msi"</p>

ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.
INSTALLDIR	path	No	<p>Installs the component to the specified location.</p> <p>By default, Veeam Backup & Replication uses the <code>Backup Catalog</code> subfolder in the <code>C:\Program Files\Veem\Backup and Replication\</code> folder.</p> <p>Example: <code>INSTALLDIR="C:\Catalog\"</code>. The component will be installed to the <code>C:\Catalog\Backup Catalog</code> folder.</p>
VM_CATALOGPATH	path	No	<p>Specifies a path to the catalog folder where index files must be stored.</p> <p>By default, Veeam Backup & Replication creates the <code>VBRCatalog</code> folder on a volume with the maximum amount of free space, for example <code>C:\VBRCatalog</code>.</p> <p>Example: <code>VM_CATALOGPATH="C:\Backup\"</code>. Index files will be stored to the <code>C:\Backup\VBRCatalog</code> folder.</p>
VBRC_SERVICE_USER	user	No	<p>Specifies a user account under which the Veeam Guest Catalog Service will run. The account must have full control NTFS permissions on the <code>VBRCatalog</code> folder where index files are stored.</p> <p>If you do not specify this parameter, the Veeam Guest Catalog Service will run under the Local System account.</p> <p>Together with the <code>VBRC_SERVICE_USER</code> parameter, you must specify the <code>VBRC_SERVICE_PASSWORD</code> parameter.</p> <p>Example: <code>VBRC_SERVICE_USER="BACKUPSERVER\Administrator"</code></p>
VBRC_SERVICE_PASSWORD	password	No	<p>This parameter must be used if you have specified the <code>VBRC_SERVICE_USER</code> parameter.</p> <p>Specifies a password for the account under which the Veeam Guest Catalog Service will run.</p> <p>Example: <code>VBRC_SERVICE_PASSWORD="1234"</code></p>
VBRC_SERVICE_PORT	port	No	<p>Specifies a TCP port that will be used by the Veeam Guest Catalog Service. By default, port number 9393 is used.</p> <p>Example: <code>VBRC_SERVICE_PORT="9393"</code></p>

Example

Suppose you want to install Veeam Backup Catalog with the following configuration:

- No user interaction
- Path to the MSI file: `E:\Veeam\VeeamBackupCatalog64.msi`

- Installation folder: default
- Catalog folder: default
- Service user account: VEEAM\Administrator
- Service user account password: 1243
- TCP communication port: 9391

The command to install Veeam Backup Catalog with such configuration will have the following parameters:

```
msiexec.exe /qn /i "E:\Veeam\VeeamBackupCatalog64.msi" ACCEPT_THIRDPARTY_LICENSES="1"
VBR_SERVICE_USER="VEEAM\Administrator" VBR_SERVICE_PASSWORD="1234"
VBR_SERVICE_PORT="9391"
```

Veeam Backup & Replication Server

To install the Veeam Backup & Replication server, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPTEULA="YES"
ACCEPT_THIRDPARTY_LICENSES="1" [INSTALLDIR="<path_to_installdir >"]
[VBR_LICENSE_FILE="<path_to_license_file>"]
[VBR_SERVICE_USER="<Veeam_B&R_Service_account>"]
[VBR_SERVICE_PASSWORD="<Veeam_B&R_Service_account_password>"]
[VBR_SERVICE_PORT="<Veeam_B&R_Service_port>"]
[VBR_SECURE_CONNECTIONS_PORT="<SSL_port>"] [VBR_SQLSERVER_SERVER="<SQL_server>"]
[VBR_SQLSERVER_DATABASE="<database_name>"] [VBR_SQLSERVER_AUTHENTICATION="0"]
[VBR_SQLSERVER_USERNAME="<SQL_auth_username>"]
[VBR_SQLSERVER_PASSWORD="<SQL_auth_password>"]
[VBR_NFSDATASTORE="<path_to_vPower_NFS_root_folder
>"] [VBR_CHECK_UPDATES="1"] [VBR_AUTO_UPGRADE="YES"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\Backup.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs the Veeam Backup & Replication server. Specify a full path to the setup file as the parameter value. Example: /i "C:\Veeam\Server.x64.msi"
ACCEPTEULA	boolean	Yes	Confirms that you accept the Veeam license agreement.

ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.
INSTALLDIR	path	No	<p>Installs the component to the specified location. By default, Veeam Backup & Replication uses the <code>Backup</code> subfolder of the <code>C:\Program Files\Veeam\Backup and Replication\</code> folder.</p> <p>Example: <code>INSTALLDIR="c:\backup\"</code>. The component will be installed to the <code>C:\backup\Backup</code> folder.</p>
VBR_LICENSE_FILE	license path	No	<p>Specifies a full path to the license file. If you do not specify this parameter, Veeam Backup & Replication will operate in the Community Edition mode.</p> <p>Example: <code>VBR_LICENSE_FILE="C:\Users\Administrator\Desktop\enterprise - veeam_backup_trial_0_30.lic"</code></p>
VBR_SERVICE_USER	user	No	<p>Specifies the account under which the Veeam Backup Service will run. The account must have full control NTFS permissions on the <code>VBRCatalog</code> folder where index files are stored and the <i>Database owner</i> rights for the configuration database on the Microsoft SQL Server where the configuration database is deployed.</p> <p>If you do not specify this parameter, the Veeam Backup Service will run under the Local System account.</p> <p>Together with the <code>VBR_SERVICE_USER</code> parameter, you must specify the <code>VBR_SERVICE_PASSWORD</code> parameter.</p> <p>Example: <code>VBR_SERVICE_USER="BACKUPSERVER\Administrator"</code></p>
VBR_SERVICE_PASSWORD	password	No	<p>This parameter must be used if you have specified the <code>VBR_SERVICE_USER</code> parameter.</p> <p>Specifies a password for the account under which the Veeam Backup Service will run.</p> <p>Example: <code>VBR_SERVICE_PASSWORD="1234"</code></p>
VBR_SERVICE_PORT	port	No	<p>Specifies a TCP port that will be used by the Veeam Backup Service.</p> <p>By default, the port number 9392 is used.</p> <p>Example: <code>VBR_SERVICE_PORT="9395"</code></p>
VBR_SECURE_CONNECTIONS_PORT	port	No	<p>Specifies a port used for communication between the mount server and the backup server. By default, port 9401 is used.</p> <p>Example: <code>VBR_SECURE_CONNECTIONS_PORT="9402"</code></p>

VBR_SQLSERVER_SERVER	SQL server\instance	No	<p>Specifies a Microsoft SQL server and instance on which the configuration database will be deployed.</p> <p>By default, Veeam Backup & Replication uses the (local)\VEEAMSQL2012 server for machines running Microsoft Windows 7, Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, and (local)\VEEAMSQL2016 for machines running Microsoft Windows Server 2012 or later.</p> <p>Example: VBR_SQLSERVER_SERVER="BACKUPSERVER\VEEAMSQL2016_MY"</p>
VBR_SQLSERVER_DATABASE	database	No	<p>Specifies a name for the configuration database.</p> <p>By default, the configuration database is deployed with the VeeamBackup name.</p> <p>Example: VBR_SQLSERVER_DATABASE="VeeamBackup"</p>
VBR_SQLSERVER_AUTHENTICATION	0/1	No	<p>Specifies if you want to use the SQL Server authentication mode to connect to the Microsoft SQL Server where the Veeam Backup & Replication configuration database is deployed.</p> <p>Set this parameter to 1 if you want to use the SQL Server authentication mode. If you do not specify this parameter, Veeam Backup & Replication will connect to the Microsoft SQL Server in the Microsoft Windows authentication mode (default value is 0).</p> <p>Together with this parameter, you must specify the following parameters: VBR_SQLSERVER_USERNAME and VBR_SQLSERVER_PASSWORD.</p> <p>Example: VBR_SQLSERVER_AUTHENTICATION="1"</p>
VBR_SQLSERVER_USERNAME	user	No	<p>This parameter must be used if you have specified the VBR_SQLSERVER_AUTHENTICATION parameter.</p> <p>Specifies a LoginID to connect to the Microsoft SQL Server in the SQL Server authentication mode.</p> <p>Example: VBR_SQLSERVER_USERNAME="sa"</p>
VBR_SQLSERVER_PASSWORD	password	No	<p>This parameter must be used if you have specified the VBR_SQLSERVER_AUTHENTICATION parameter.</p> <p>Specifies a password to connect to the Microsoft SQL Server in the SQL Server authentication mode.</p> <p>Example: VBR_SQLSERVER_PASSWORD="1234"</p>

VBR_NFSDATASTORE	path	No	<p>Specifies the vPower cache folder to which the write cache will be stored. By default, Veeam Backup & Replication uses the folder on a volume with the maximum amount of free space, for example, <code>C:\ProgramData\Veeam\Backup\NfsDatastore\</code>.</p> <p>Example: <code>VBR_NFSDATASTORE="C:\ProgramData\Veeam\Backup\NfsDatastore2\"</code></p>
VBR_CHECK_UPDATES	0 or 1	No	<p>Specifies if you want Veeam Backup & Replication to automatically check for new product patches and versions.</p> <p>Set this parameter to 0 if you do not want to check for updates. If you do not specify this parameter, Veeam Backup & Replication will automatically check for updates (default value is 1).</p> <p>Example: <code>VBR_CHECK_UPDATES="0"</code></p>
VBR_AUTO_UPGRADE	Boolean	No	<p>Specifies if you want Veeam Backup & Replication to automatically upgrade existing components in the backup infrastructure. Veeam Backup & Replication performs automatic upgrade after the Veeam Backup Service is started on the backup server.</p> <p>Set this parameter to YES to enable automatic upgrade.</p> <p>Example: <code>VBR_AUTO_UPGRADE="YES"</code></p>

Example

Suppose you want to install Veeam Backup & Replication with the following configuration:

- Installation log location: `C:\logs\log1.txt`
- No user interaction
- Path to the MSI file: `E:\Veeam\Server.x64.msi`
- Installation folder: `D:\Program Files\Veeam`
- License file location: `C:\License\veeam_license.lic`
- Service user account: `VEEAM\Administrator`
- Service user account password: 1243
- Service port: default
- TLS port: default
- Configuration database and database name: default
- Path to the vPower NFS folder: `D:\vPowerNFS`

The command to install Veeam Backup & Replication with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\logs\log1.txt" /qn /i "E:\Veeam\Server.x64.msi" ACCEPTTEULA="YES"
ACCEPT_THIRDPARTY_LICENSES="1" INSTALLDIR="D:\Program Files\Veeam"
VBR_LICENSE_FILE="C:\License\veeam_license.lic" VBR_SERVICE_USER="VEEAM\Administrator"
VBR_SERVICE_PASSWORD="1234" VBR_NFSDATASTORE="D:\vPowerNFS"
```

Veeam Backup & Replication Console

To install the Veeam Backup & Replication console, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPTTEULA="YES"
ACCEPT_THIRDPARTY_LICENSES="1" [INSTALLDIR="<path_to_installdir >"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\Console.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs the Veeam Backup & Replication console. Specify a full path to the setup file as the parameter value. Example: /i "C:\Veeam\Shell.x64.msi"
ACCEPTTEULA	boolean	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.
INSTALLDIR	path	No	Installs the component to the specified location. By default, Veeam Backup & Replication uses the Console subfolder of the C:\Program Files\Veeam\Backup and Replication\ folder. Example: INSTALLDIR="c:\backup\". The component will be installed to the C:\backup\Console folder.

Example

Suppose you want to install the Veeam Backup & Replication console with the following configuration:

- No user interaction
- Path to the MSI file: E:\Veeam\Shell.x64.msi
- Installation folder: C:\Backup

The command to install the Veeam Backup & Replication console with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\logs\log1.txt" /qn /i "E:\Veeam\Shell.x64.msi" ACCEPT_EULA="YES"
ACCEPT_THIRDPARTY_LICENSES="1" INSTALLDIR="C:\Backup\"
```

Veeam Explorer for Microsoft Active Directory

To install Veeam Explorer for Microsoft Active Directory, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPT_EULA="1"
ACCEPT_THIRDPARTY_LICENSES="1"
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\VEAD.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam Explorer for Microsoft Active Directory. Specify a full path to the setup file as the parameter value. Example: /i "C:\Explorers\VeeamExplorerforActiveDirectory.msi"
ACCEPT_EULA	0/1	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.

Veeam Explorer for Microsoft SQL Server

To install Veeam Explorer for Microsoft SQL Server, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPT_EULA="1"  
ACCEPT_THIRDPARTY_LICENSES="1"
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\VESQL.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam Explorer for Microsoft SQL Server. Specify a full path to the setup file as the parameter value. Example: /i "C:\Explorers\VeeamExplorerforSQL.msi"
ACCEPT_EULA	0/1	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.

Veeam Explorer for Microsoft Exchange

To install Veeam Explorer for Microsoft Exchange, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPT_EULA="1"  
ACCEPT_THIRDPARTY_LICENSES="1"
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\VEX.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam Explorer for Microsoft Exchange. Specify a full path to the setup file as the parameter value. Example: /i "C:\Explorers\VeeamExplorerforExchange.msi"
ACCEPT_EULA	0/1	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.

Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business

Veeam Explorer for Microsoft SharePoint is installed together with Veeam Explorer for Microsoft OneDrive for Business from the same setup file.

To install Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPT_EULA="1"
ACCEPT_THIRDPARTY_LICENSES="1"
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\VESP.txt"

/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business. Specify a full path to the setup file as the parameter value. Veeam Backup & Replication installs both Veeam Explorer for Microsoft SharePoint and Veeam Explorer for Microsoft OneDrive for Business from the same setup file. Example: /i "C:\Explorers\VeeamExplorerforSharePoint.msi"
ACCEPT_EULA	0/1	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.

Veeam Explorer for Oracle

To install Veeam Explorer for Oracle, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPT_EULA="1"
ACCEPT_THIRDPARTY_LICENSES="1"
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\VEO.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam Explorer for Oracle. Specify a full path to the setup file as the parameter value. Example: /i "C:\Explorers\VeeamExplorerforOracle.msi"
ACCEPT_EULA	0/1	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.

Veeam Backup Enterprise Manager

To install Veeam Backup Enterprise Manager, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPTTEULA="YES"
ACCEPT_THIRDPARTY_LICENSES="1" [INSTALLDIR="<path_to_installdir >"]
VBREM_LICENSE_FILE="<path_to_license_file>"
[VBREM_SERVICE_USER="<Veeam_EM_Service_account>"] [VBREM_SERVICE_PASSWORD="<Veeam_EM_Service_account_password>"] [VBREM_SERVICE_PORT="<Veeam_EM_Service_port>"]
[VBREM_SQLSERVER_SERVER="<SQL_server>"]
[VBREM_SQLSERVER_DATABASE="<database_name>"] [VBREM_SQLSERVER_AUTHENTICATION="0"]
[VBREM_SQLSERVER_USERNAME="<SQL_auth_username>"]
[VBREM_SQLSERVER_PASSWORD="<SQL_auth_password>"]
[VBREM_TCPPORT="<TCP_port_for_web_site>"] [VBREM_SSLPORT="<SSL_port_for_web_site>"]>"
[VBREM_THUMBPRINT="<certificate_hash>"]
[VBREM_RESTAPISVC_PORT="<TCP_port_for_RestApi_service>"]
[VBREM_RESTAPISVC_SSLPORT="<SSL_port_for_RestApi_service>"]
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\EM.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs Veeam Backup Enterprise Manager. Specify a full path to the setup file as the parameter value. Example: /i "C:\Veeam\EnterpriseManager\BackupWeb_x64.msi"
ACCEPTTEULA	boolean	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.

INSTALLDIR	path	No	<p>Installs the component to the specified location.</p> <p>By default, Veeam Backup & Replication uses the Enterprise Manager subfolder of the C:\Program Files\Veeam\ folder.</p> <p>Example: <code>INSTALLDIR="c:\Backup\"</code>. The component will be installed to the C:\Backup\Enterprise Manager folder.</p>
VBREM_LICENSE_FILE	license path	Yes	<p>Specifies a full path to the license file.</p> <p>Example: <code>VBREM_LICENSE_FILE="C:\Users\Administrator\Desktop\enterprise - veeam_backup_trial_0_30.lic"</code></p>
VBREM_SERVICE_USER	user	No	<p>Specifies the account under which the Veeam Backup Enterprise Manager Service will run. The account must have full control NTFS permissions on the <code>VBRCatalog</code> folder where index files are stored and the <i>Database owner</i> rights for the Veeam Backup Enterprise Manager configuration database on the Microsoft SQL Server that you plan to use.</p> <p>If you do not specify this parameter, the Veeam Backup Enterprise Manager Service will run under the Local System account.</p> <p>Together with the <code>VBREM_SERVICE_USER</code> parameter, you must specify the <code>VBREM_SERVICE_PASSWORD</code> parameter.</p> <p>Example: <code>VBREM_SERVICE_USER="BACKUPSERVER\Administrator"</code></p>
VBREM_SERVICE_PASSWORD	password	No	<p>Specifies a password for the account under which the Veeam Backup Enterprise Manager Service will run.</p> <p>Example: <code>VBREM_SERVICE_PASSWORD="1234"</code></p>
VBREM_SERVICE_PORT	Port	No	<p>Specifies a TCP port that will be used by the Veeam Backup Enterprise Manager Service.</p> <p>By default, the port number 9394 is used.</p> <p>Example: <code>VBREM_SERVICE_PORT = "9394"</code></p>

VBREM_SQLSERVER_SERVER	SQL server\instance	No	<p>Specifies a Microsoft SQL Server and instance on which the Veeam Backup Enterprise Manager configuration database will be deployed.</p> <p>By default, Veeam Backup & Replication uses the (local)\VEEAMSQL2012 server for machines running Microsoft Windows 7, Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2, and (local)\VEEAMSQL2016 for machines running Microsoft Windows Server 2012 or later.</p> <p>Example: VBREM_SQLSERVER_SERVER="BACKUPSERVER\VEEAMSQL2012_MY"</p>
VBREM_SQLSERVER_DATABASE	database	No	<p>Specifies a name of the Veeam Backup Enterprise Manager database.</p> <p>By default, the database is deployed with the VeeamBackupReporting name.</p> <p>Example: VBREM_SQLSERVER_DATABASE="VeeamBackupReporting01"</p>
VBREM_SQLSERVER_AUTHENTICATION	0/1	No	<p>Specifies if you want to use the Microsoft SQL Server authentication mode to connect to the Microsoft SQL Server where the Veeam Backup Enterprise Manager is deployed.</p> <p>Set this parameter to 1 if you want to use the SQL Server authentication mode. If you do not specify this parameter, Veeam Backup Enterprise Manager will connect to the Microsoft SQL Server in the Microsoft Windows authentication mode (default value is 0).</p> <p>Together with this parameter, you must specify the following parameters: VBREM_SQLSERVER_USERNAME and VBREM_SQLSERVER_PASSWORD.</p> <p>Example: VBREM_SQLSERVER_AUTHENTICATION="1"</p>
VBREM_SQLSERVER_USERNAME	user	No	<p>This parameter must be used if you have specified the VBREM_SQLSERVER_AUTHENTICATION parameter.</p> <p>Specifies a LoginID to connect to the Microsoft SQL Server in the SQL Server authentication mode.</p> <p>Example: VBREM_SQLSERVER_USERNAME="sa"</p>
VBREM_SQLSERVER_PASSWORD	password	No	<p>This parameter must be used if you have specified the VBREM_SQLSERVER_AUTHENTICATION parameter.</p> <p>Specifies a password to connect to the Microsoft SQL Server in the SQL Server authentication mode.</p> <p>Example: VBREM_SQLSERVER_PASSWORD="1234"</p>

VBREM_TCPPORT	port	No	Specifies a TCP port that will be used by the Veeam Backup Enterprise Manager website. By default, the port number 9080 is used. Example: <code>VBREM_TCPPORT="9080"</code>
VBREM_SSLPORT	port	No	Specifies a port that will be used by the Veeam Backup Enterprise Manager website. By default, the port number 9443 is used. Example: <code>VBREM_SSLPORT="9443"</code>
VBREM_THUMBPRINT	hash	No	Specifies the certificate to be used by Veeam Backup Enterprise Manager Service and Veeam RESTful API Service. If this parameter is not specified, a new certificate will be generated by <code>openssl.exe</code> . Example: <code>VBREM_THUMBPRINT="0677d0b8f27cacc966b15d807b41a101587b488"</code>
VBREM_RESTAPISVC_PORT	port	No	Specifies a TCP port that will be used by the Veeam Backup Enterprise Manager RESTful API Service. By default, the port number 9399 is used. Example: <code>VBREM_RESTAPISVC_PORT="9399"</code>
VBREM_RESTAPISVC_SSLPORT	port	No	Specifies a port that will be used by the Veeam RESTful API Service. By default, the port number 9398 is used. Example: <code>VBREM_RESTAPISVC_SSLPORT="9398"</code>
VBREM_CONFIG_SCHANNEL	0/1	No	Specifies if the TLS 1.2 protocol will be used for secure communication with the Veeam Backup Enterprise Manager website.

Example

Suppose you want to install Veeam Backup Enterprise Manager with the following settings:

- Installation log location: `C:\logs\log1.txt`
- No user interaction
- Path to the MSI file: `E:\Veeam\EnterpriseManager\BackupWeb_x64.msi`
- Installation folder: `D:\Program Files\Veeam`
- License file location: `C:\License\veeam_license.lic`
- Service user account: `VEEAM\Administrator`
- Service user account password: `1243`
- Service port: default

- Microsoft SQL Server database: BACKUPSERVER\VEEAMSQL2012_MY
- Database name: VeeamReporting01
- TCP and TLS ports: default
- Certificate: default
- TCP port for RESTful API: 9396
- TLS port for RESTful API: 9397

The command to install Veeam Backup Enterprise Manager with such configuration will have the following parameters:

```
msiexec.exe /L*v "C:\logs\log1.txt" /qn /i
"E:\Veeam\EnterpriseManager\BackupWeb_x64.msi" ACCEPTEULA="YES"
ACCEPT_THIRDPARTY_LICENSES="1" INSTALLDIR="D:\Program Files\Veeam"
VBREM_LICENSE_FILE="C:\License\veeam_license.lic"
VBREM_SERVICE_USER="VEEAM\Administrator" VBREM_SERVICE_PASSWORD="1234"
VBREM_SQLSERVER_SERVER="BACKUPSERVER\VEEAMSQL2012_MY"
VBREM_SQLSERVER_DATABASE="VeeamReporting01" VBREM_RESTAPISVC_PORT="9396"
```

Veeam Cloud Connect Portal

Veeam Cloud Connect Portal requires Veeam Backup Enterprise Manager of the same version to be installed on the target machine.

To install Veeam Cloud Connect Portal, use a command with the following syntax:

```
msiexec.exe [/L*v "<path_to_log>"] /qn /i "<path_to_msi>" ACCEPTEULA="YES"
ACCEPT_THIRDPARTY_LICENSES="1" [INSTALLDIR="<path_to_installdir >"]
VBCP_SSLPORT="<SSL_port">
```

The command has the following parameters:

Option	Parameter	Required	Description
/L	*v logfile	No	Creates an installation log file with the verbose output. Specify a full path to the log file as the parameter value. A setup log file created during the previous installation is cleared. Example: /L*v "C:\ProgramData\Veeam\Setup\Temp\Logs\CloudPortal.txt"
/q	n	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
/i	setup file	Yes	Installs the Veeam Cloud Connect Portal. Specify a full path to the setup file as the parameter value. Example: /i "C:\Cloudportal\BackupCloudPortal_x64.msi"

ACCEPTTEULA	boolean	Yes	Confirms that you accept the Veeam license agreement.
ACCEPT_THIRDPARTY_LICENSES	0/1	Yes	Confirms that you accept the license agreement for 3rd party components that Veeam incorporates.
INSTALLDIR	path	No	<p>Installs the component to the specified location.</p> <p>By default, Veeam Backup & Replication uses the <code>CloudPortal</code> subfolder of the <code>C:\Program Files\Veeam\Backup and Replication\</code> folder.</p> <p>Example: <code>INSTALLDIR="c:\backup\"</code>. The component will be installed to the <code>C:\backup\CloudPortal</code> folder</p>
VBCP_SSLPORT	port	No	<p>Specifies a port that will be used by the Veeam Cloud Connect Portal website.</p> <p>By default, the port number 6443 is used.</p> <p>Example: <code>VBREM_SSLPORT="7443"</code></p>

Example

Suppose you want to install Veeam Cloud Connect Portal with the following configuration:

- No user interaction
- Path to the MSI file: `E:\Cloud portal\BackupCloudPortal_x64.msi`
- Installation folder: `C:\Backup`
- TLS port: default

The command to install Veeam Cloud Connect Portal with such configuration will have the following parameters:

```
msiexec.exe /qn /L*v "C:\logs\log1.txt" /qn /i "E:\Cloud
portal\BackupCloudPortal_x64.msi" ACCEPTTEULA="YES" ACCEPT_THIRDPARTY_LICENSES="1"
INSTALLDIR="C:\Backup\"
```

Installing Updates in Unattended Mode

Veeam Backup & Replication updates can be installed in the unattended mode.

To install a Veeam Backup & Replication update, perform the following steps:

1. [Download the update installation archive.](#)
2. [Install the update on the backup server.](#)

IMPORTANT!

The script that installs Veeam Backup & Replication updates must be run with elevated privileges (run as Administrator).

Step 1. Download Update Installation Archive

1. Download the installation archive for the Veeam Backup & Replication update from the [Latest Updates](#) page.
2. Extract the executable file from the downloaded archive.
3. Save the extracted file locally on the backup server where you plan to install the update, or place it in a network shared folder.

Step 2. Install Update

To install the Veeam Backup & Replication update on the backup server, use the following command syntax:

```
%patch% [/silent][/noreboot][/log <log_path>] [VBR_AUTO_UPGRADE=1]
```

The command has the following parameters:

Option	Parameter	Required	Description
%patch%	path	Yes	Specifies a path to the update installation file on the backup server or in a network shared folder.
silent	—	Yes	Sets the user interface level to "no", which means no user interaction is needed during installation.
noreboot	—	No	Suppresses reboot if reboot is required during the Veeam Backup & Replication update installation.
log	path	No	Specifies a full path to the log file for the Veeam Backup & Replication update installation.

VBR_AUTO_UPGRADE	Boolean	No	<p>Starts automatic upgrade for existing components in the backup infrastructure. Set this parameter to <code>YES</code> to enable components upgrade.</p> <p>Automatic components upgrade is performed after the Veeam Backup Service on the backup server is started.</p>
------------------	---------	----	---

For example:

You want to install the Veeam Backup & Replication update with the following options:

- Path to the update installation file: `C:\Temp\veeam_backup_9.5.4.2753.update4a_setup.exe`
- Silent install: enabled
- Noreboot: enabled
- Path to the log file: `C:\Logs\veeam.log`
- Components auto upgrade: enabled

The command to install the Veeam Backup & Replication update will be the following:

```
C:\Temp\veeam_backup_9.5.4.2753.update4a_setup.exe /silent /noreboot /log
C:\Logs\veeam.log VBR_AUTO_UPGRADE=1
```

Installation Results

You can use the last exit code to verify if the installation process has completed successfully.

- In `cmd.exe`, use the `%ERRORLEVEL%` variable to check the last exit code.
- In Microsoft Windows PowerShell, use the `$LastExitCode` variable to check the last exit code.

Veeam Backup & Replication does not provide any confirmation about the results of automatic components upgrade. To check if components have been successfully upgraded, use the Veeam Backup & Replication console.

Backup Infrastructure

Veeam Backup & Replication is a modular solution that lets you build a scalable backup infrastructure for environments of different sizes and configuration. The installation package of Veeam Backup & Replication includes a set of components that you can use to configure the backup infrastructure. Some components are mandatory and provide core functionality; some components are optional and can be installed to provide additional functionality for your business and deployment needs. You can co-install Veeam Backup & Replication components on the same machine, physical or virtual, or you can set them up separately for a more scalable approach.

Backup Infrastructure Components

The Veeam backup infrastructure comprises a set of components. Some components can be deployed with the help of the setup file. Other components can be deployed via the Veeam Backup & Replication console.

Backup Server

The backup server is a Windows-based physical or virtual machine on which Veeam Backup & Replication is installed. It is the core component in the backup infrastructure that fills the role of the "configuration and control center". The backup server performs all types of administrative activities:

- Coordinates backup, replication, recovery verification and restore tasks
- Controls job scheduling and resource allocation
- Is used to set up and manage backup infrastructure components as well as specify global settings for the backup infrastructure

In addition to its primary functions, a newly deployed backup server also performs the roles of the default backup proxy and the backup repository (it manages data handling and data storing tasks).

Backup Server Services and Components

The backup server uses the following services and components:

- **Veeam Backup Service** is a Windows service that coordinates all operations performed by Veeam Backup & Replication such as backup, replication, recovery verification and restore tasks. The Veeam Backup Service runs under the *Local System* account or account that has the *Local Administrator* permissions on the backup server.
- **Veeam Broker Service** interacts with the virtual infrastructure to collect and cache the virtual infrastructure topology. Jobs and tasks query information about the virtual infrastructure topology from the broker service, which accelerates job and task performance.
- **Veeam Guest Catalog Service** manages guest OS file system indexing for VMs and replicates system index data files to enable search through guest OS files. Index data is stored in the Veeam Backup Catalog – a folder on the backup server. The Veeam Guest Catalog Service running on the backup server works in conjunction with search components installed on Veeam Backup Enterprise Manager and (optionally) a dedicated Microsoft Search Server.
- **Mount Service** mounts backups and replicas for file-level access, browsing the VM guest file system and restoring VM guest OS files and application items to the original location.
- **Backup Proxy Services.** In addition to dedicated services, the backup server runs a set of Data Mover Services. For details, see [Backup Proxy](#).
- **Veeam Backup & Replication Configuration Database** stores data about the backup infrastructure, jobs, sessions and so on. The database instance can be located on a SQL Server installed either locally (on the same machine where the backup server is running) or remotely. For more information, see the following guidelines: https://bp.veeam.expert/resource_planning/backup_server_database.html.
- **Veeam Backup & Replication Console** provides the application user interface and allows user access to the application's functionality.
- **Veeam Backup PowerShell Snap-In** is an extension for Microsoft Windows PowerShell 2.0 or later. Veeam Backup PowerShell adds a set of cmdlets to allow users to perform backup, replication and recovery tasks through the command-line interface of PowerShell or run custom scripts to fully automate operation of Veeam Backup & Replication.

Credentials Manager

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:

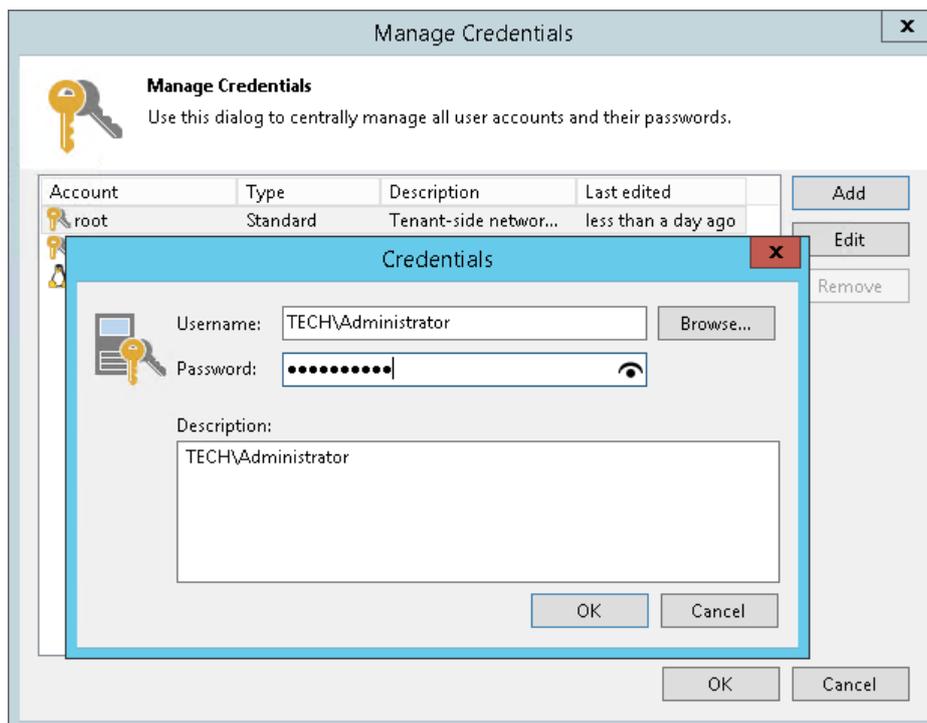
- [Standard account \(Microsoft Windows\)](#)
- [Linux account \(user name and password\)](#)
- [Linux private key \(Identity/Pubkey\)](#)

Standard Accounts (Microsoft Windows)

You can create a credentials record for an account that you plan to use to connect to a Microsoft Windows server or VM running Microsoft Windows OS.

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 Accounts (User Name and Password)

You can create a credentials record for the account that you plan to use to connect to a Linux server or VM running Linux OS.

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

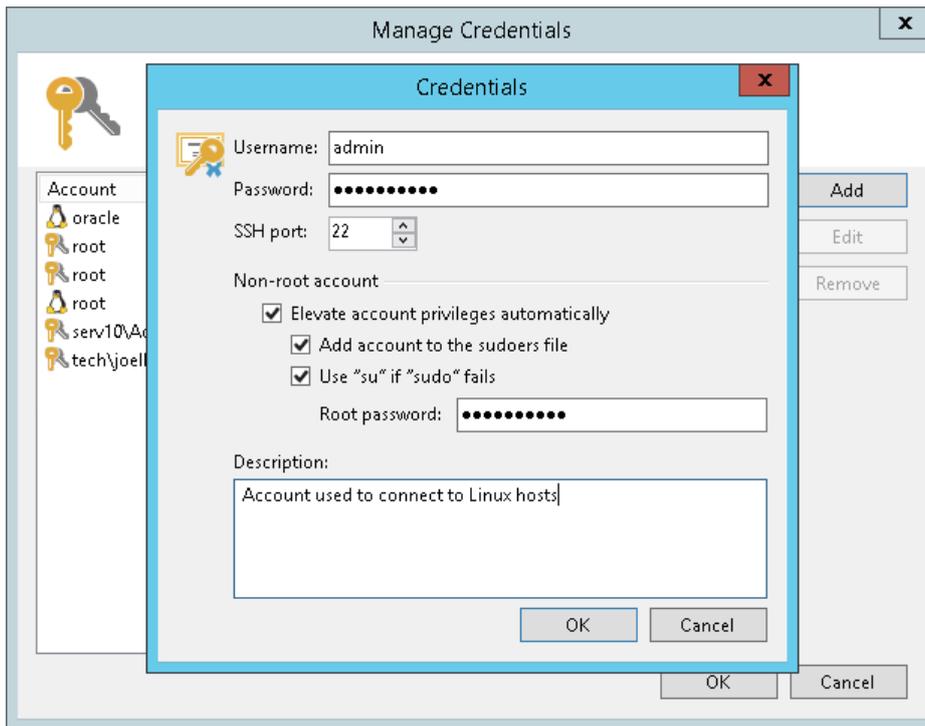
1. From the main menu, select **Manage Credentials**.
2. Click **Add > Linux account**.
3. In the **Username** field, enter a user name for the account that you plan to add.
4. In the **Password** field, enter a password for the account that you want to add. To view the entered password, click and hold 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. In the **Root password** field, enter the password for the root account.

If you do not enable this option, you will have to manually add the user account to the sudoers file.
 - c. When registering a Linux server, you have an option to failover to using the su command for distros where the sudo command is not available.

To enable the failover, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the password for the root account.
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, *Root*, 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!

- You can create a separate user account intended for work with Veeam Backup & Replication 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.
- Cases when root password is required to elevate account rights to root using sudo are no longer supported.



Linux Private Keys (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 servers 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 & Replication has the following limitations for the Identity/Pubkey authentication method:

- Veeam Backup & Replication does not support keys that are stored as binary data, for example, in a file of DER format.
- Veeam Backup & Replication 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:

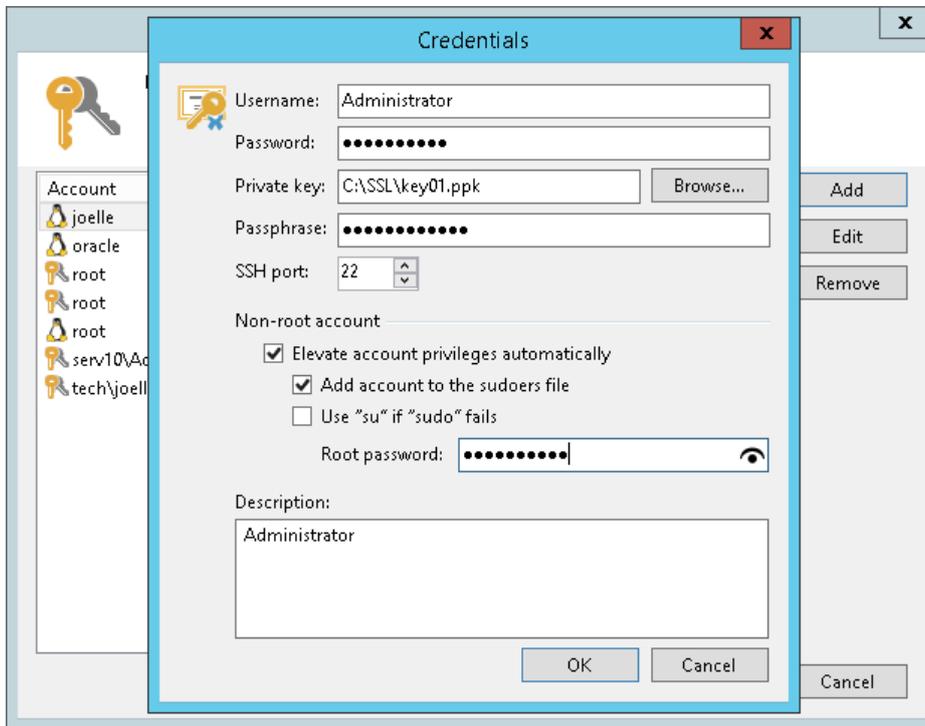
1. Generate a pair of keys using a key generation utility, for example, ssh-keygen.
2. Place the public key on a Linux server. To do this, add the public key to the `authorized_keys` file in the `.ssh/` directory in the home directory on the Linux server.
3. Place the private key in some folder on the backup server or in a network shared folder.
4. In Veeam Backup & Replication, 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 **Password** field, specify the password for the user account. The password is required in all cases except when you use root or a user with enabled `NOPASSWD:ALL` setting in `/etc/sudoers`.
8. In the **Private key** field, enter a path to the private key or click **Browse** to select a private key.
9. 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.
10. 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.
11. 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. In the **Root password** field, enter the password for the root account.

If you do not enable this option, you will have to manually add the user account to the sudoers file.
 - c. When registering a Linux server, you have an option to failover to using the su command for distros where the sudo command is not available.

To enable the failover, select the **Use "su" if "sudo" fails** check box and in the **Root password** field, enter the password for the root account.
12. In the **Description** field, enter a description for the created credentials record. As there can be a number of similar account names, for example, *Root*, 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!

Cases when root password is required to elevate account rights to root using sudo are no longer supported.



Editing and Deleting Credentials Records

You can edit or 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 & Replication will display a warning. Click **Yes** to confirm your intention.
4. Edit settings of the credentials record as required.

To delete a credentials record:

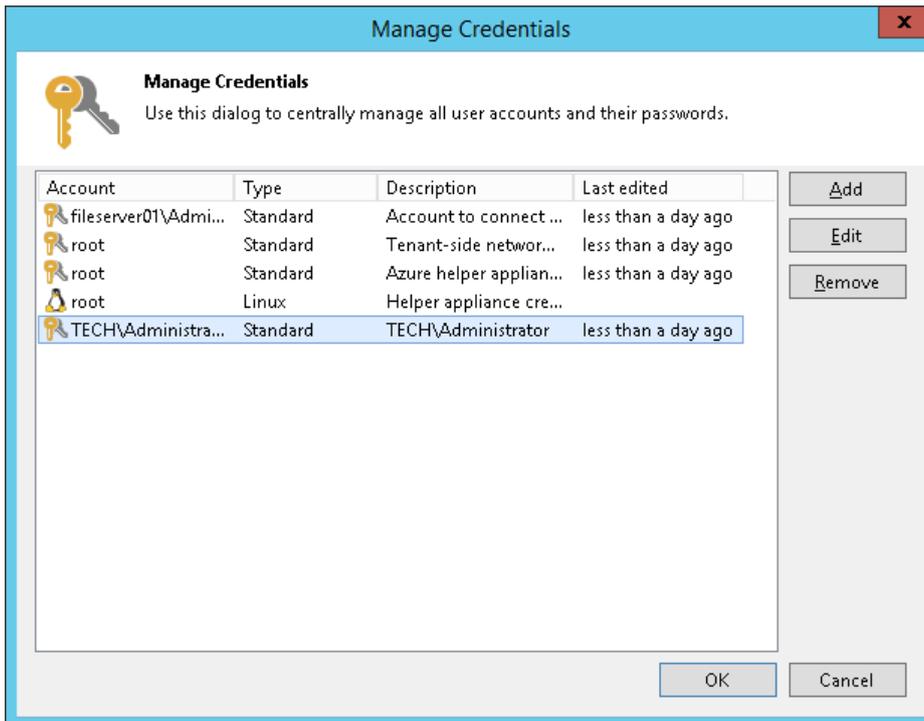
1. From the main menu, select **Manage Credentials**.
2. Select the credentials record in the list and click **Remove**. You cannot delete a record that is already used for any component in the backup infrastructure.

NOTE:

The Credentials Manager contains 3 system credentials records:

- A credentials record for the Veeam FLR appliance
- A credentials record for the tenant-side network extension appliance
- A credentials record for Microsoft Azure helper appliance.

You cannot delete these credentials records. However, you can edit them: change a password and record description.



Cloud Credentials Manager

You can use the Cloud Credentials Manager to create and maintain a list of credentials records that you plan to use to connect to cloud services.

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

- [Veeam Cloud Connect Accounts](#)
- [Amazon AWS Accounts](#)
- [Microsoft Azure Storage Accounts](#)
- [Microsoft Azure Compute Accounts](#)

Veeam Cloud Connect Accounts

You can add a credentials record for a tenant account – an account that you plan to use to connect to a service provider (SP).

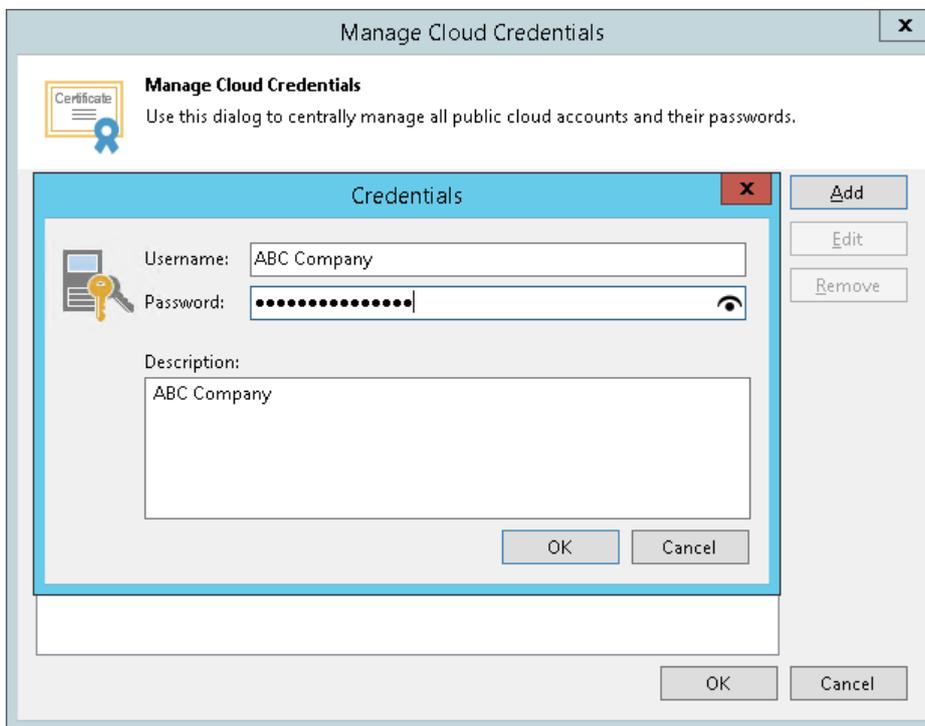
Before you add a credentials record, the SP must register a tenant account on the SP Veeam backup server. Tenants without accounts cannot connect to the SP and use Veeam Cloud Connect resources. For more information, see the [Registering Tenant Accounts](#) section in the Veeam Cloud Connect Guide.

To create a credentials record for a tenant account:

1. From the main menu, select **Manage Cloud Credentials**.
2. Click **Add > Veeam Cloud Connect service provider account**.
3. In the **Username** field, enter a user name for the account that the SP has provided to you.

Note that if the SP allocated to you replication resources in VMware vCloud Director, you must enter a user name for the vCloud Director tenant account in the following format: *Organization|Username*. For example: *TechCompanyOrg|Administrator*.

4. In the **Password** field, enter a password for the account that the SP has provided to you. 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.



Amazon AWS Accounts

You can create a credentials record for an account that you plan to use to connect to Amazon Web Services (AWS).

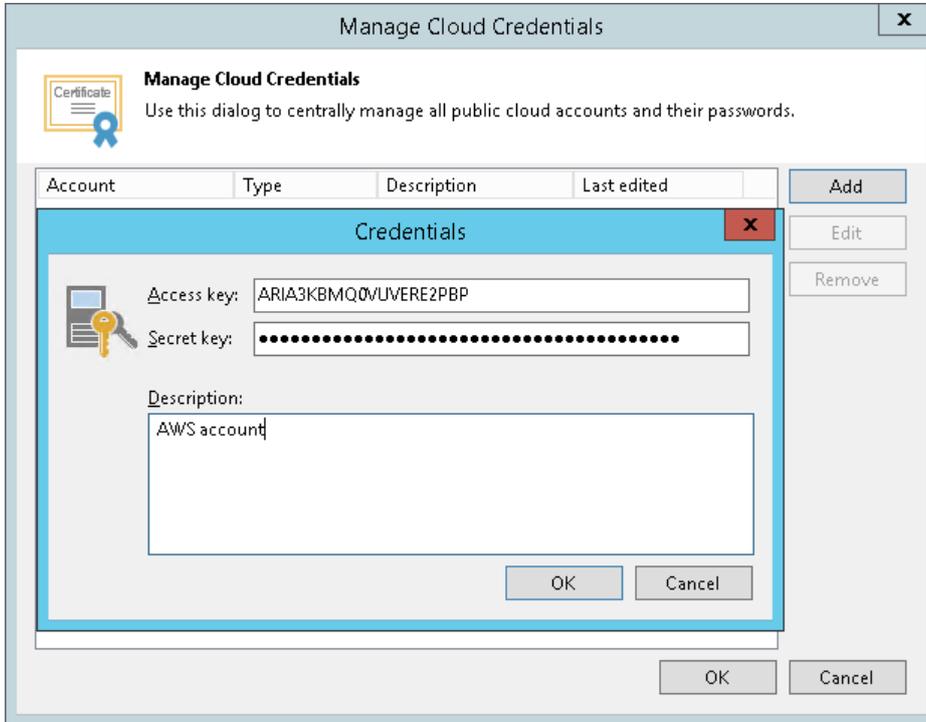
To create a record for an AWS account:

1. From the main menu, select **Manage Cloud Credentials**.
2. Click **Add > Amazon AWS access key**.
3. In the **Access key** field, enter an access key ID.
4. In the **Secret key** field, enter a secret access key. To view the entered secret key, click and hold the eye icon on the right of the field.

- In the **Description** field, enter a description for the created credentials record.

IMPORTANT!

It is recommended that the account used to connect to AWS has administrative permissions – access to all AWS actions and resources.



Microsoft Azure Storage Accounts

You can create a credentials record for an account that you plan to use to connect to Microsoft Azure Blob storage.

The following types of storage accounts are supported.

Storage account type	Supported performance tiers	Supported access tiers
Storage	Standard	Cool, Hot, Premium
Storage V2		
BlobStorage		

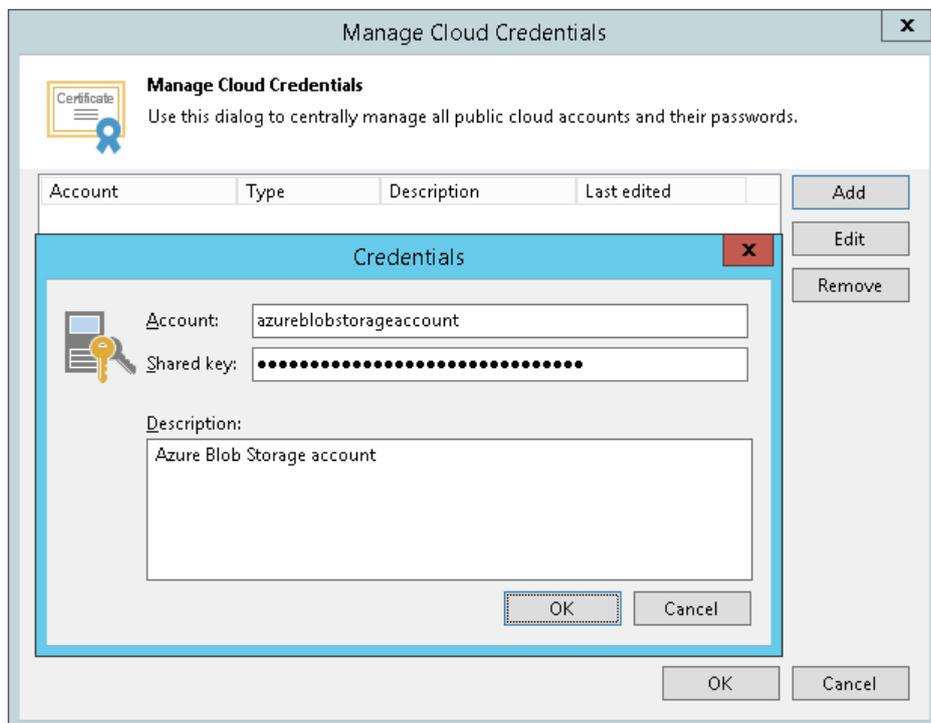
To create a record for a Microsoft Azure storage account:

- From the main menu, select **Manage Cloud Credentials**.
- Click **Add > Microsoft Azure storage account**.
- In the **Account** field, enter the storage account name.
- In the **Shared key** field, enter the storage account shared key. To view the entered key, click and hold the eye icon on the right of the field.

5. In the **Description** field, enter an optional description for the credentials record.

TIP:

If you do not have a Microsoft Azure storage account, you can create it in the Azure portal, as described in the [Azure Storage Documentation](#).



Microsoft Azure Compute Accounts

You can create a credentials record for accounts that will be used for restore to Microsoft Azure.

To create a record for a Microsoft Azure or Microsoft Azure Stack account:

1. From the main menu, select **Manage Cloud Credentials**.
2. Click **Add > Microsoft Azure compute account**.
3. Follow the steps of the **Initial Configuration** wizard as described in [Adding Microsoft Azure Accounts](#) or [Adding Microsoft Azure Stack Accounts](#) sections.

Editing and Deleting Credentials Records

You can edit or delete existing cloud credentials records.

To edit a credentials record:

1. From the main menu, select **Manage Cloud Credentials**.
2. Select the credentials record in the list and click **Edit**.
3. 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.

TIP:

You can use the Cloud Credentials Manager to change the password for a tenant account provided by the SP. For more information, see the [Changing Password for Tenant Account](#) section in the Veeam Cloud Connect Guide.

Password Manager

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. You can use one password per job or share the same password between several jobs on the backup server.
- 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.

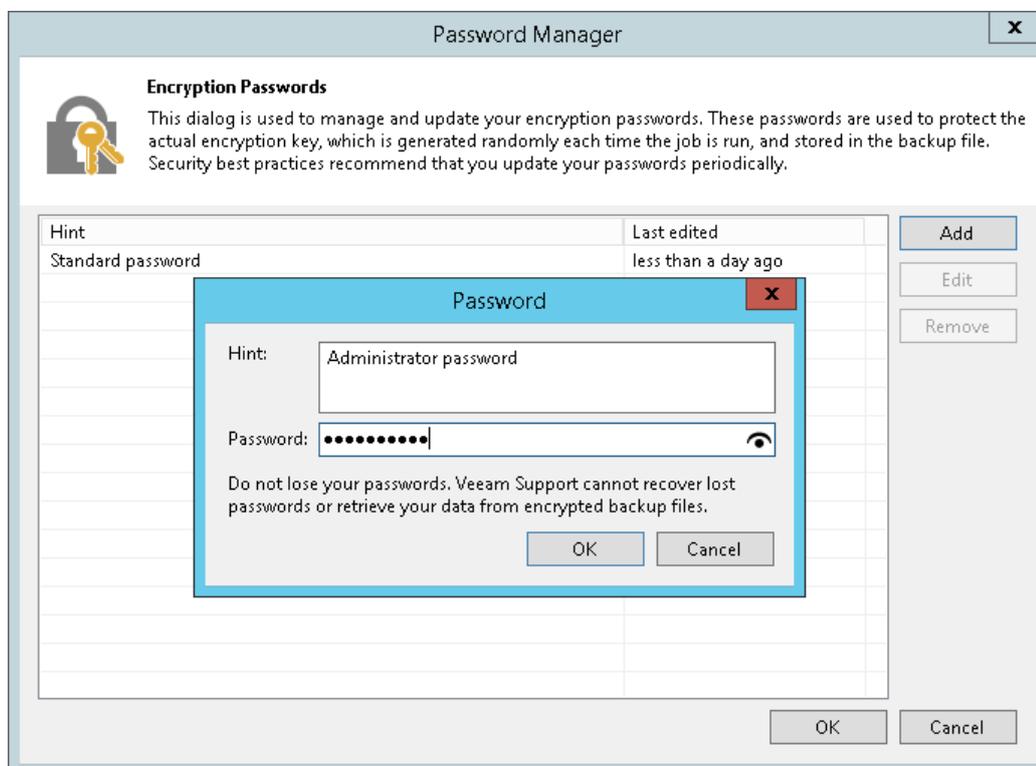
To create a new password:

1. From the main menu, select **Manage Passwords**. Alternatively, you can use job properties to create a new password:
 - a. Open the **Home** view.
 - b. In the inventory pane, select **Jobs**.
 - c. In the working area, right-click the backup or backup copy job and select **Edit**.
 - d. At the **Storage** step of the wizard (for backup job) or **Target** step of the wizard (for backup copy job), click **Advanced**.
 - e. Click the **Storage** tab.
 - f. In the **Encryption** section of the **Advanced Setting** window, select the **Enable backup file encryption** check box and click the **Manage passwords** link.
Veeam Backup & Replication will open the Password Manager.
2. In the Password Manager, click **Add**.
3. 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.

4. 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.

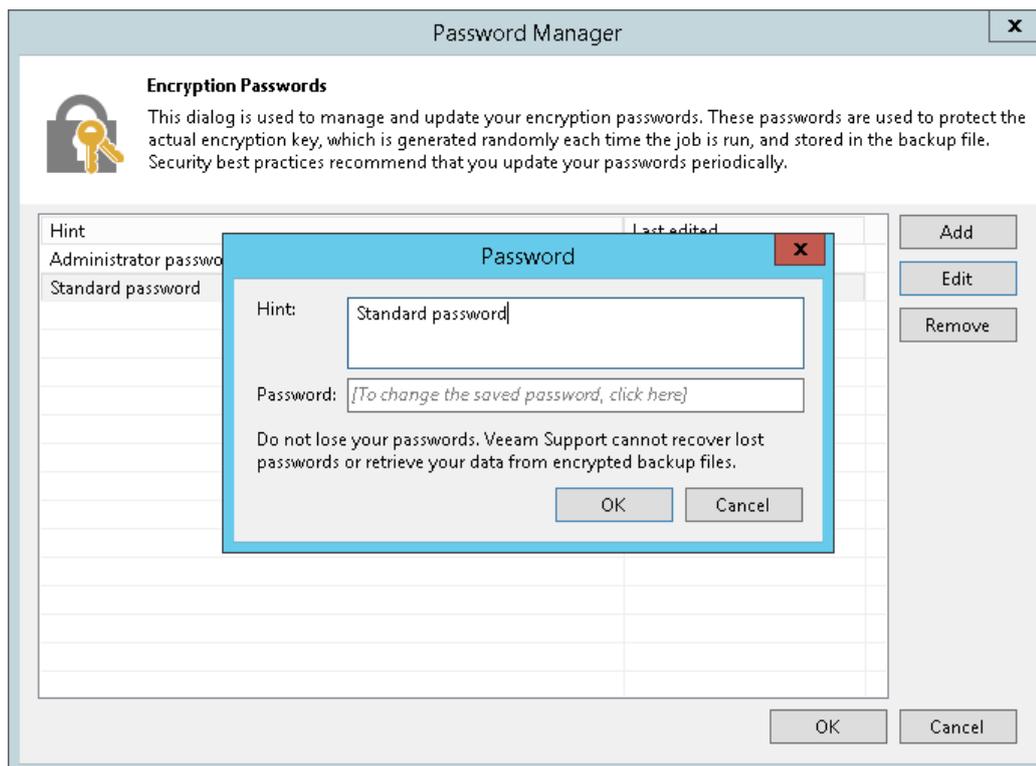
To edit a password:

1. From the main menu, select **Manage passwords**. Alternatively, you can use job properties to edit the password:
 - a. Open the **Home** view.
 - b. In the inventory pane, select **Jobs**.
 - c. In the working area, right-click the backup or backup copy job and select **Edit**.
 - d. At the **Storage** step of the wizard (for backup job) or **Target** step of the wizard (for backup copy job), click **Advanced**.
 - e. Click the **Storage** tab.
 - f. In the **Encryption** section of the **Advanced Setting** window, select the **Enable backup file encryption** check box and click the **Manage passwords** link.

Veeam Backup & Replication 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**. Alternatively, you can use job properties to delete passwords:
 - a. Open the **Home** view.
 - b. In the inventory pane, select **Jobs**.
 - c. In the working area, right-click the backup or backup copy job and select **Edit**.
 - d. At the **Storage** step of the wizard (for backup job) or **Target** step of the wizard (for backup copy job), click **Advanced**.
 - e. Click the **Storage** tab.
 - f. In the **Encryption** section of the **Advanced Setting** window, select the **Enable backup file encryption** check box and click the **Manage passwords** link.

Veeam Backup & Replication will open the Password Manager.

Backup & Replication Console

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. The console lets you log in to Veeam Backup & Replication and perform all kind of data protection and disaster recovery operations as if you work on the backup server.

The console does not have a direct access to the backup infrastructure components and configuration database. Such data as user credentials, passwords, roles and permissions are stored on the backup server side. To access this data, the console needs to connect to the backup server and query this information periodically during the work session.

To make users work as uninterrupted as possible, the remote console maintains the session for 5 minutes if the connection is lost. If the connection is re-established within this period, you can continue working without re-logging to the console.

Backup & Replication Console Deployment

The console is installed locally on the backup server by default. You can also use it in a standalone mode – install the console on a dedicated machine and access Veeam Backup & Replication remotely over the network.

You can install as many remote consoles as you need so that multiple users can access Veeam Backup & Replication simultaneously. Veeam Backup & Replication prevents concurrent modifications on the backup server. If several users are working with Veeam Backup & Replication at the same time, the user who saves the changes first has the priority. Other users will be prompted to reload the wizard or window to get the most recent information about the changes in the configuration database.

If you have multiple backup servers in the infrastructure, you can connect to any of them from the same console. For convenience, you can save several shortcuts for these connections.

IMPORTANT!

You cannot use the same console to connect to backup servers with different versions of Veeam Backup & Replication. Mind this if you have more than one backup server in your backup environment, and these backup servers run different versions of Veeam Backup & Replication. For example, if one of your backup servers run version 9.5 Update 3, and another backup server runs version 9.5 Update 4, you will need to use 2 separate consoles for connecting to these servers.

The console supports automatic update. Every time you connect to the backup server locally or remotely, the console checks for updates. If the backup server has a patch or updates installed, the console will be updated automatically.

Mind the following:

- Upgrade to another Veeam Backup & Replication major product version is not supported. If you upgrade Veeam Backup & Replication to another major version, you must upgrade the console to the same version manually. Automatic upgrade is not supported for Preview, Beta or RTM versions of Veeam Backup & Replication.
- Downgrade of the console is not supported. If the console is of a higher version than the backup server (for example, you have upgraded the console manually), the connection to the server will fail.

If other Veeam Backup & Replication components, such as Veeam Cloud Connect Portal or Veeam Backup Enterprise Manager, are installed on the machine where the console runs, these components will also be upgraded.

Backup & Replication Console Components

When you install a remote console on a machine, Veeam Backup & Replication installs the following components:

- Veeam Backup PowerShell Snap-In
- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Oracle
- Veeam Explorer for Microsoft SQL
- Veeam Explorer for Microsoft SharePoint
- Veeam Explorer for Microsoft OneDrive for Business
- Mount server

Backup & Replication Console User Access Rights

To log in to Veeam Backup & Replication via the console, the user 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. The user can perform the scope of operations permitted by his or her role in Veeam Backup & Replication. For more information, see [Assigning Roles to Users](#).

Requirements for Backup & Replication Console

A machine on which you install the Veeam Backup & Replication console must meet the following requirements:

- The machine must meet the system requirements. For more information, see [System Requirements](#).
- The remote console can be installed on a Microsoft Windows machine (physical or virtual).
- If you install the console remotely, you can deploy it behind NAT. However, the backup server must be outside NAT. The opposite type of deployment is not supported: if the backup server is deployed behind NAT and the remote console is deployed outside NAT, you will not be able to connect to the backup server.

Limitations for Backup & Replication Console

The Veeam Backup & Replication console has the following limitations:

- You cannot perform restore from the configuration backup via the remote console.
- The machines on which the remote console is installed are not added to the list of managed servers automatically. For this reason, you cannot perform some operations, for example, import backup files that reside on the remote console machine or assign roles of backup infrastructure components to this machine. To perform these operations, you must add the remote console machine as a managed server to Veeam Backup & Replication. For more information, see [Managing Servers](#).

Logging on to Veeam Backup & Replication

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

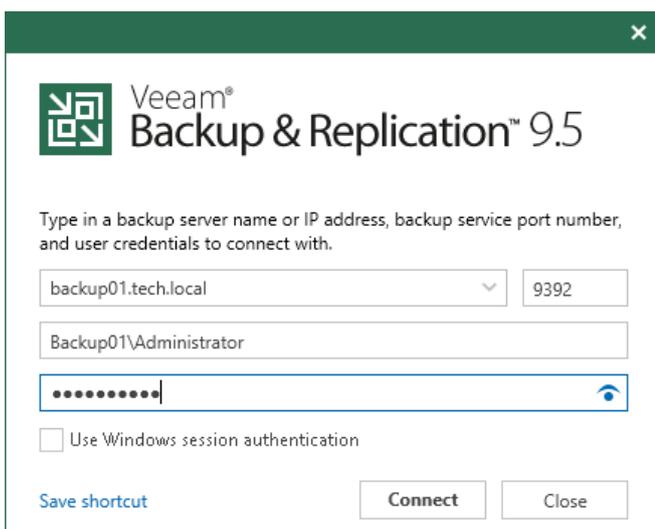
1. To open the Veeam Backup & Replication console, do one of the following:
 - Double-click the console icon on the desktop.
 - From the Microsoft Windows **Start** menu, select **All Programs > Veeam > Veeam Backup & Replication Console**.
 - Use the Microsoft Windows search to find the **Veeam Backup & Replication 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 & Replication. 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 & Replication 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.

NOTE:

If you create a shortcut for a connection, the credentials for this connection will be stored in the Windows Credentials Manager. The credentials are saved after the first successful logon.



The screenshot shows the Veeam Backup & Replication 9.5 connection dialog box. It has a dark green header with the Veeam logo and the text 'Veeam Backup & Replication™ 9.5'. Below the header, there is a prompt: 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' The dialog contains several input fields: a dropdown menu for the server name (currently showing 'backup01.tech.local'), a text box for the port number (currently showing '9392'), a text box for the username (currently showing 'Backup01\Administrator'), and a password field with a blue eye icon for toggling visibility. There is also an unchecked checkbox labeled 'Use Windows session authentication'. At the bottom, there are three buttons: 'Save shortcut' (in blue), 'Connect', and 'Close'.

Virtualization Servers and Hosts

You can add the following types of servers and hosts to the backup infrastructure:

- [VMware vSphere Server](#)
- [VMware vCloud Director](#)
- [Microsoft Windows Server](#)
- [Linux Server](#)

You can add physical machines and VMs to the backup infrastructure and assign different roles to them. The table below describes which roles can be assigned to the different types of servers.

Server Type	Source Host	Target Host	Backup Proxy	Backup Repository
VMware vSphere Server (standalone ESX(i) host or vCenter Server)	●	●	○	○
VMware vCloud Director	●	○	○	○
Microsoft Windows server	○	○	●	●
Linux server	○	○	○	●

Related Topics

- [Rescanning Servers](#)
- [Editing Server Settings](#)
- [Removing Servers](#)

Adding VMware vSphere Servers

You must add to the backup infrastructure VMware vSphere servers that you plan to use as source and target for backup, replication and other activities.

You can add vCenter Servers and ESX(i) hosts. If an ESX(i) host is managed by a vCenter Server, it is recommended that you add the vCenter Server, not a standalone ESX(i) host. If you move VMs between ESX(i) hosts managed by the vCenter Server, you will not have to re-configure jobs in Veeam Backup & Replication. Veeam Backup & Replication will automatically locate migrated VMs and continue processing them as usual.

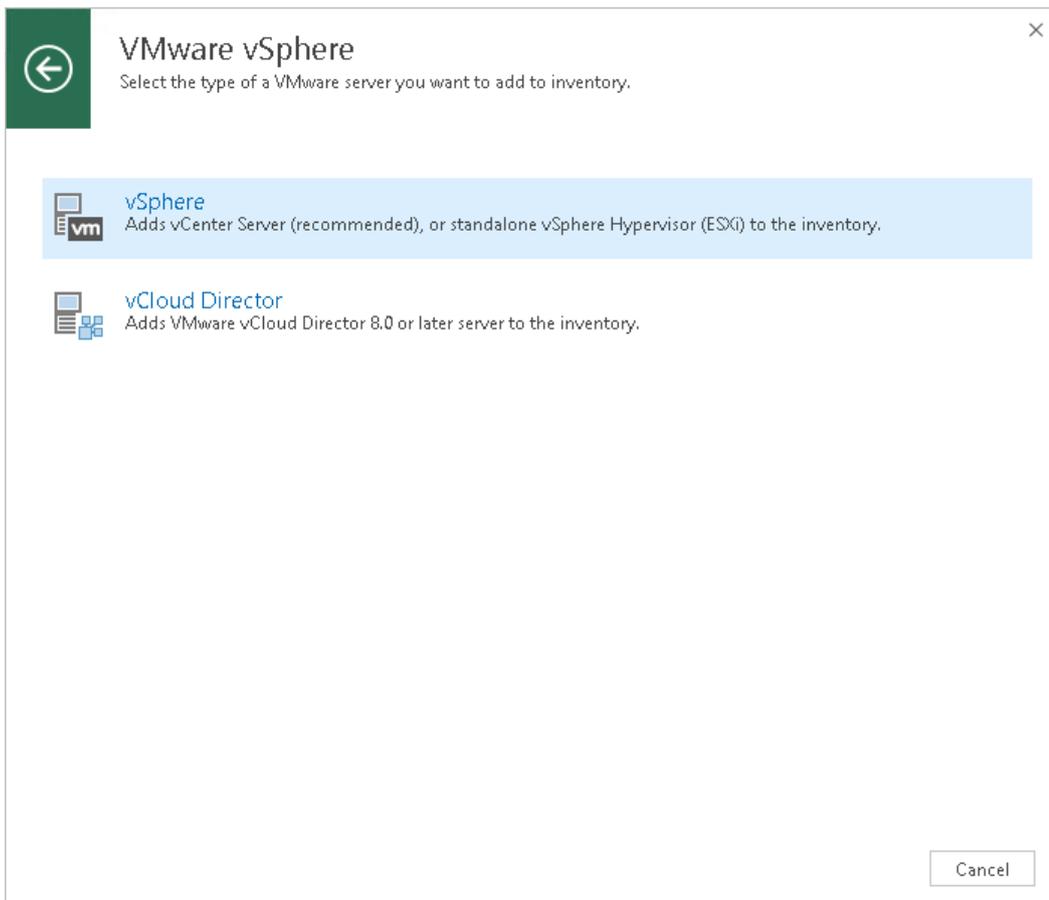
To add a VMware vSphere server, use the **New VMware Server** wizard.

Step 1. Launch New VMware Server Wizard

To launch the **New VMware Server** wizard, do one of the following:

- Open the **Backup Infrastructure** view. In the inventory pane, select the **Managed Servers** node and click **Add Server** on the ribbon or right-click the **Managed Servers** node and select **Add Server**. In the **Add Server** window, click **VMware vSphere > vSphere**.

- Open the **Inventory** view, in the inventory pane select the **VMware vSphere** node and click **Add Server** on the ribbon. You can also right-click the **VMware vSphere** node and select **Add Server**.



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.

If you add a VMware Cloud on AWS vCenter Server, use its Fully Qualified Domain Name (FQDN). Make sure the name you specify ends with <vmc.vmware.com>.

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 'New VMware Server' wizard window. The window has a blue title bar and a sidebar on the left with a 'vm' logo. The sidebar contains a list of steps: 'Name' (selected), 'Credentials', 'SSH Connection', and 'Summary'. The main area is titled 'Name' and contains the instruction 'Specify DNS name or IP address of VMware server.' Below this are two input fields: 'DNS name or IP address:' with the text 'vcenter01.tech.local' and 'Description:' with the text 'vCenter Server 01'. At the bottom right are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

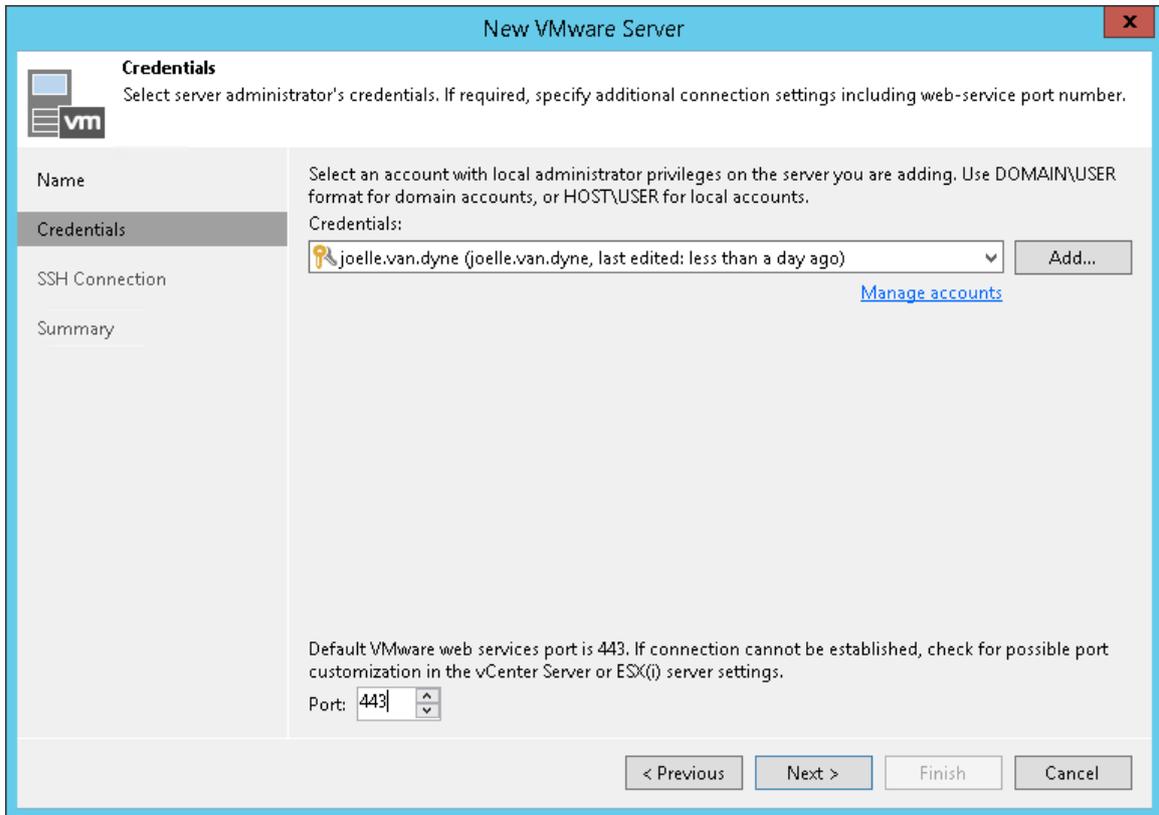
Step 3. Specify Credentials

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](#).

- By default, Veeam Backup & Replication 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.



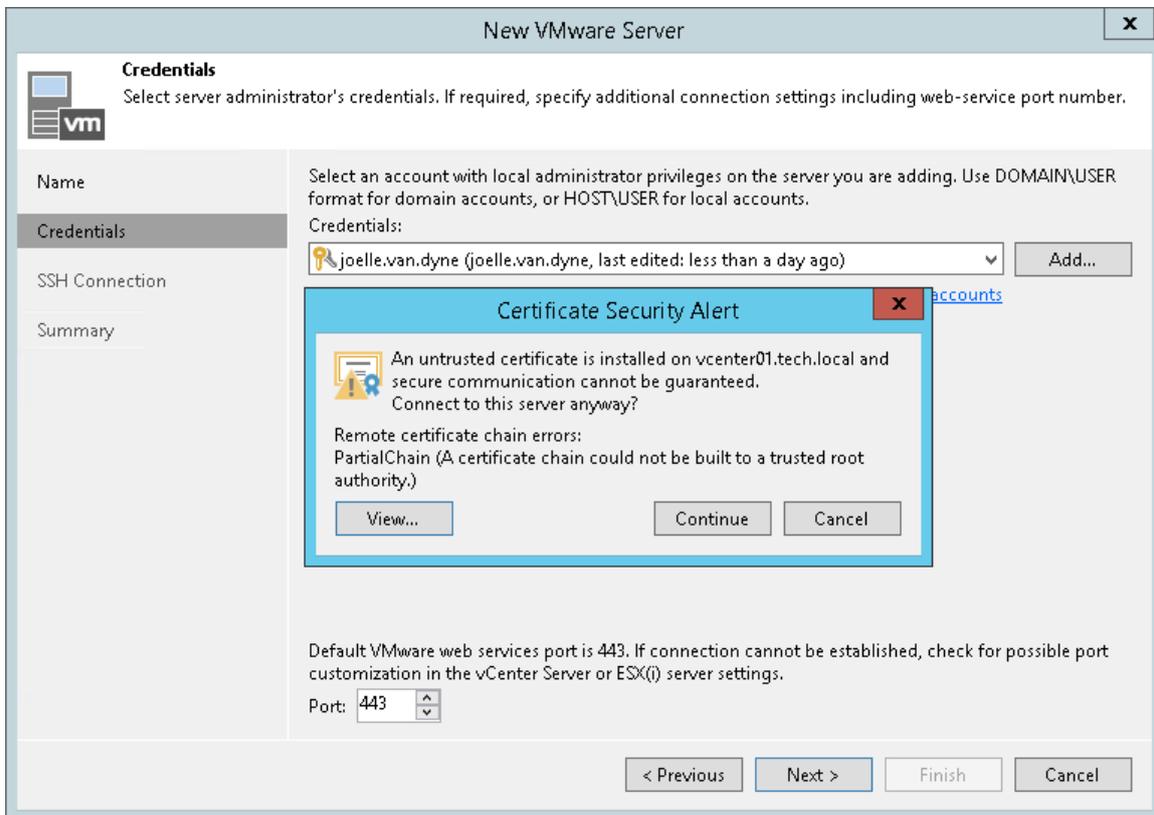
- When you add a vCenter Server or ESX(i) host, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate installed on the vCenter Server or ESX(i) host. During every subsequent connection to the server, Veeam Backup & Replication uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack. For details on managing TLS Certificates, see [TLS Certificates](#).

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

- To view detailed information about the certificate, click **View**.
- If you trust the server, click **Continue**.
- If you do not trust the server, click **Cancel**. Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

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

The **SSH Connection** 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 & Replication will work with the ESX host in the agentless mode.

To use an SSH connection:

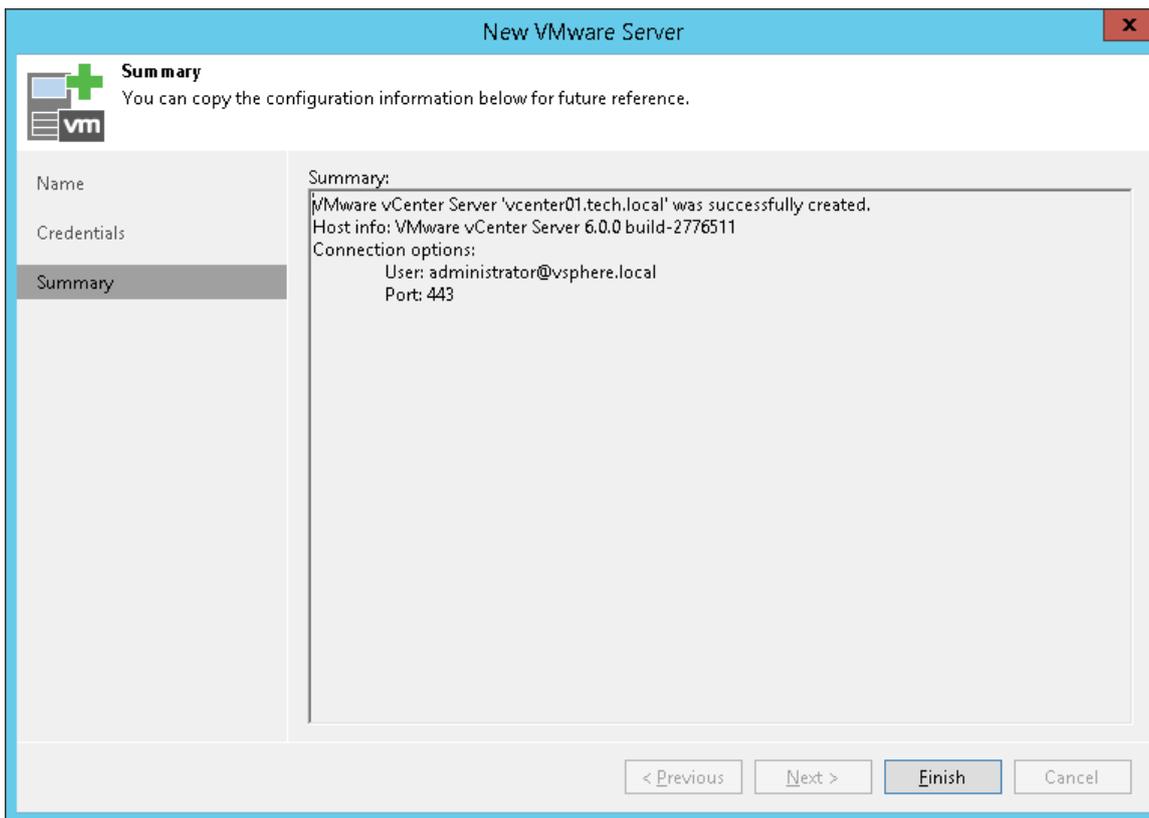
1. Make sure that the **Use service console connection to this server** check box is selected.
2. From the **Credentials** list, select credentials to connect to the service console of the ESX host. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on 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 & Replication 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 & Replication 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.

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 VMware vCloud Director

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

When you add VMware vCloud Director to the backup infrastructure, the VMware vCloud Director hierarchy is displayed in the **Inventory > vCloud Director** view in Veeam Backup & Replication. You can work with VMs managed by VMware vCloud Director directly in the Veeam Backup & Replication console.

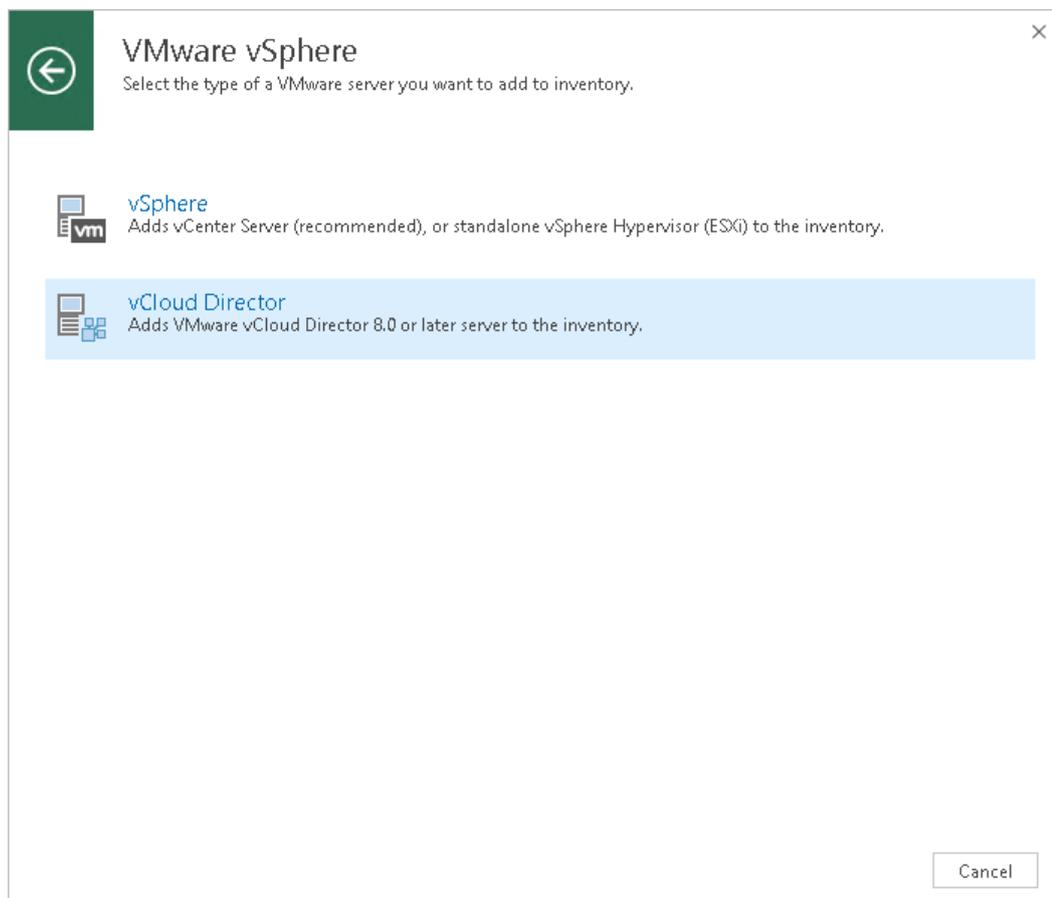
To add the VMware vCloud Director host, use the **New VMware vCloud Director** wizard.

Step 1. Launch New VMware vCloud Director Server Wizard

To launch the **New VMware vCloud Director Server** wizard, do the following:

1. Open the **Backup Infrastructure** view.

2. In the inventory pane, right-click the **Managed Servers** node and select **Add Server**. Alternatively, you can click **Add Server** on the ribbon.
3. In the **Add Server** window, click **VMware vSphere** > **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 & Replication 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 a wizard window titled "New VMware vCloud Director Server". The "Name" step is selected in the left-hand navigation pane. The main area contains the following fields:

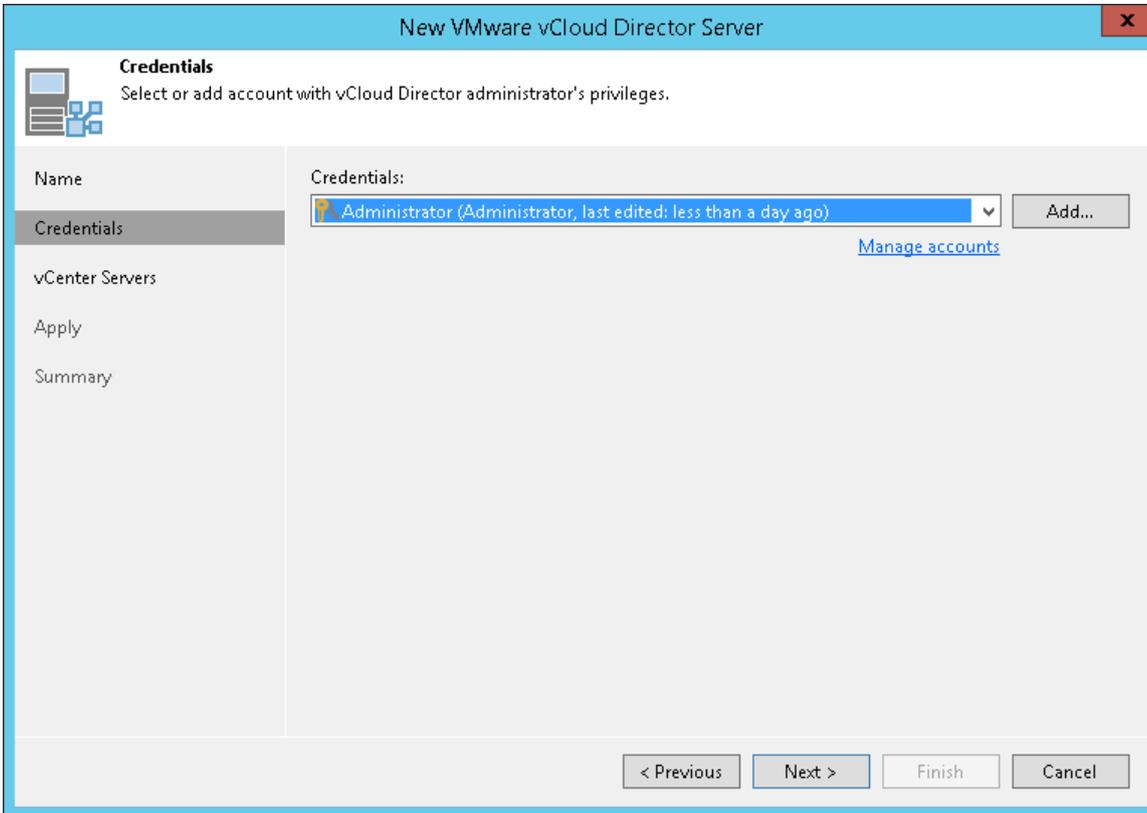
- DNS name or IP address:** 172.16.21.179
- URL:** https://172.16.21.179:443
- Description:** Created by SERV02\Administrator at 12/26/2018 2:39 AM.

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

Step 3. Specify VMware 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 system administrator privileges on VMware vCloud Director (you cannot use the organization administrator account to add 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](#).



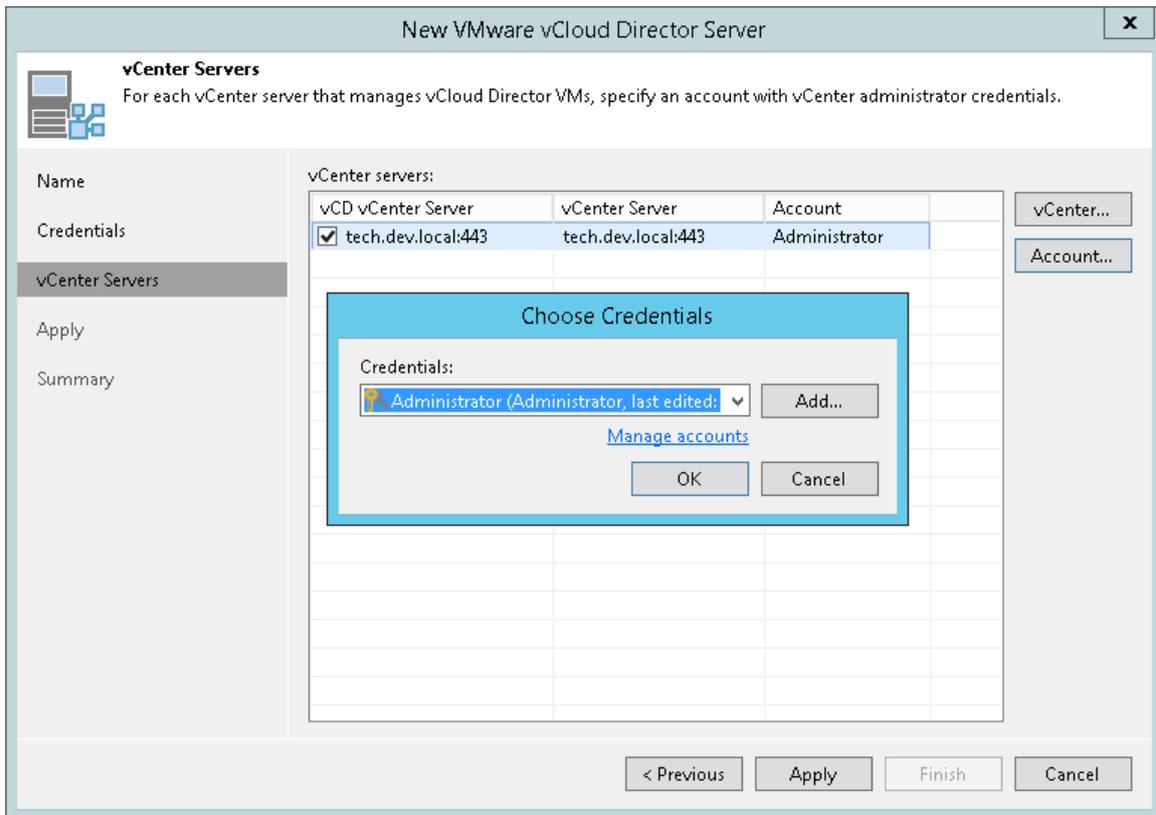
Step 4. Specify Credentials for Underlying vCenter Servers

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

1. From the **vCenter servers** list, select a vCenter Server.
2. Click **Account** on the right and select credentials to connect to the vCenter Server. By default, Veeam Backup & Replication 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 & Replication automatically detects a port used to communicate with the vCenter Server. If necessary, you can change the connection port for the vCenter Server. Click **vCenter** on the right and adjust the port number.

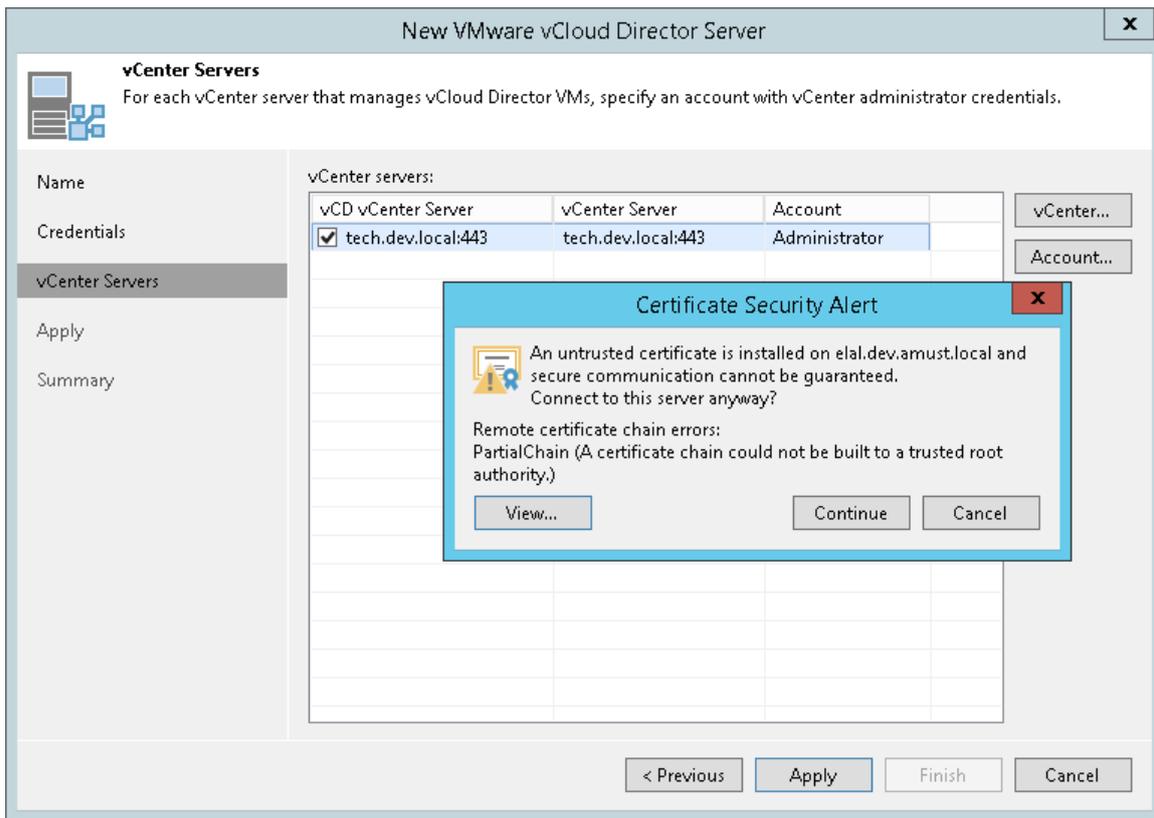


4. When you add a vCenter Server, Veeam Backup & Replication saves a thumbprint of the TLS certificate installed on the vCenter Server to the configuration database. During every subsequent connection to the server, Veeam Backup & Replication uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack. For details on managing TLS Certificates, see [TLS Certificates](#).

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

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

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



5. Repeat steps 1-3 for all 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

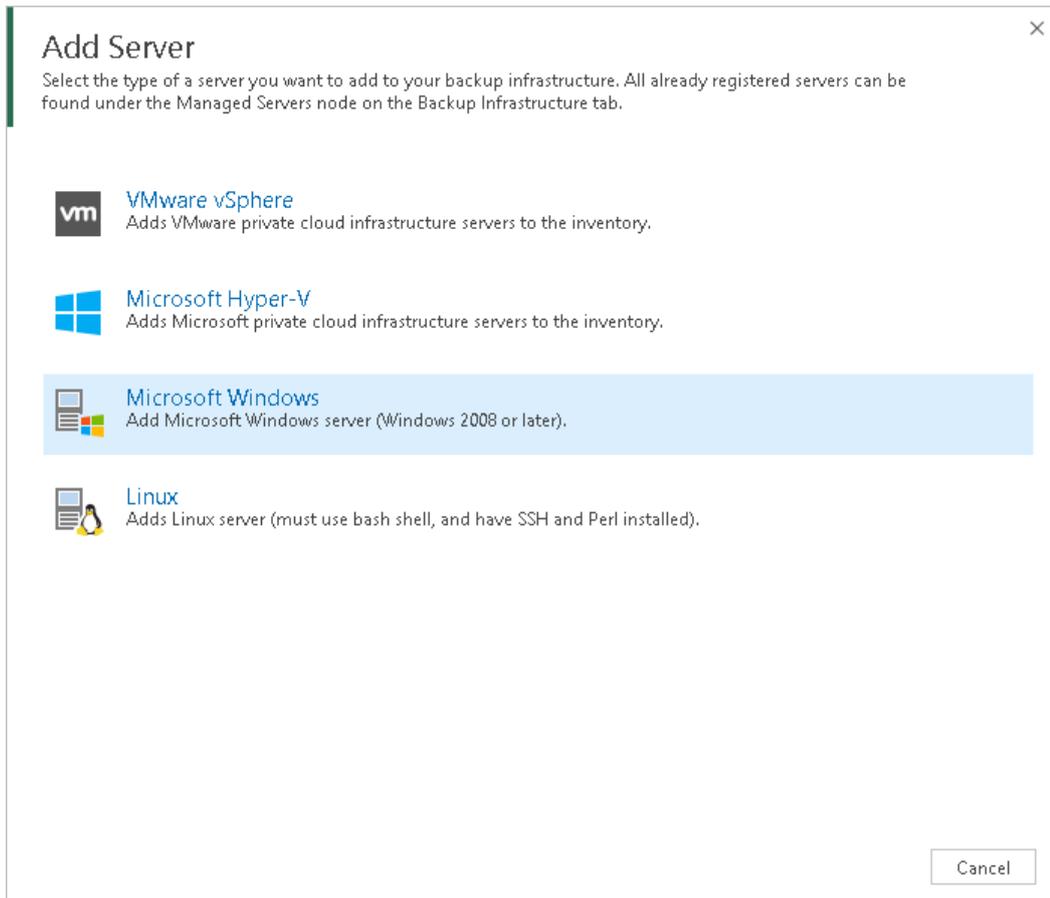
At the **Apply** step of the wizard, complete the procedure of VMware vCloud Director adding.

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

Step 1. Launch New Windows Server Wizard

To launch the **New Windows Server** wizard, do one of the following:

- Open the **Backup Infrastructure** or **Files** view, in the inventory pane select the **Microsoft Windows** node and click **Add Server** on the ribbon.
- Open the **Backup Infrastructure** view. In the inventory pane, select the **Managed Servers** node and click **Add Server** on the ribbon or right-click the **Managed Servers** node and select **Add Server**. In the **Add Server** window, select **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.

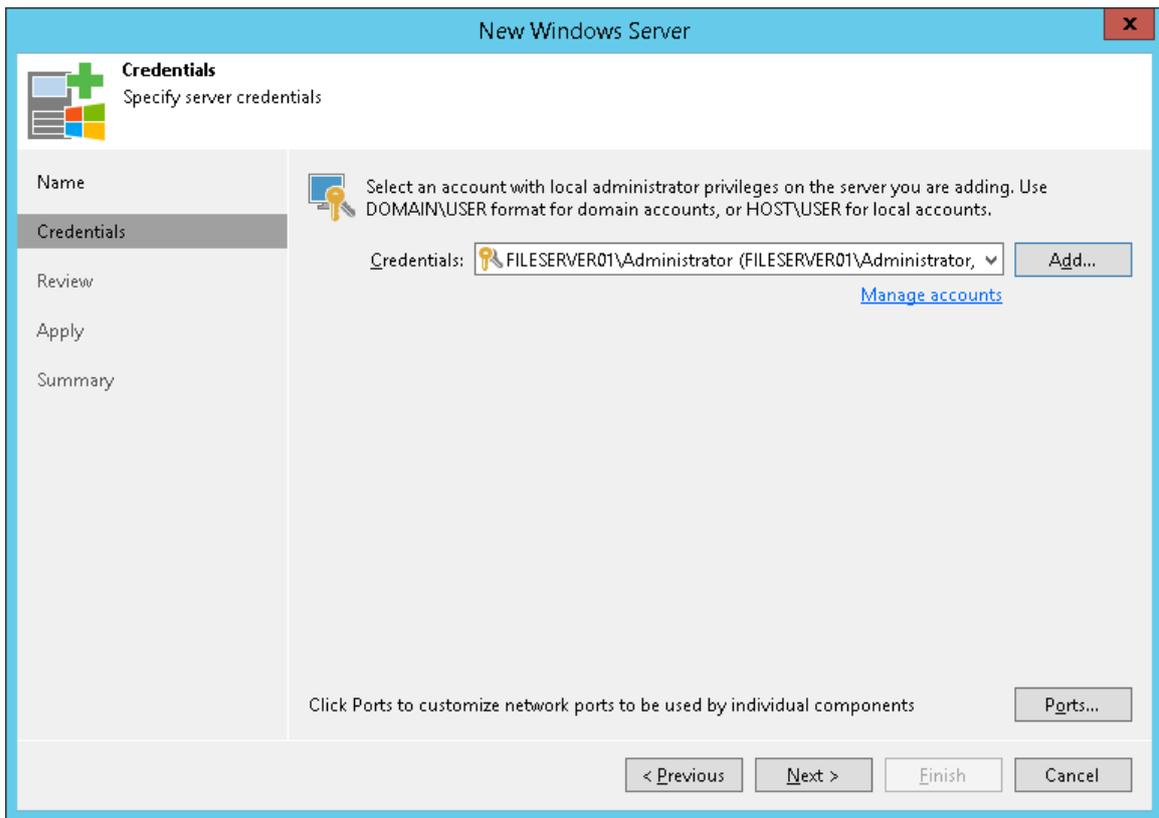
The screenshot shows the 'New Windows Server' wizard window. The window title is 'New Windows Server'. The main area is titled 'Name' and contains the instruction 'Specify DNS name or IP address of Microsoft Windows server.' Below this, there are two input fields: 'DNS name or IP address:' with the value 'fileserver01.tech.local' and 'Description:' with the value 'File Server 01'. On the left side, there is a navigation pane with options: 'Name', 'Credentials', 'Review', 'Apply', and 'Summary'. At the bottom, 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 & Replication will use the provided credentials to deploy its components on the added server.

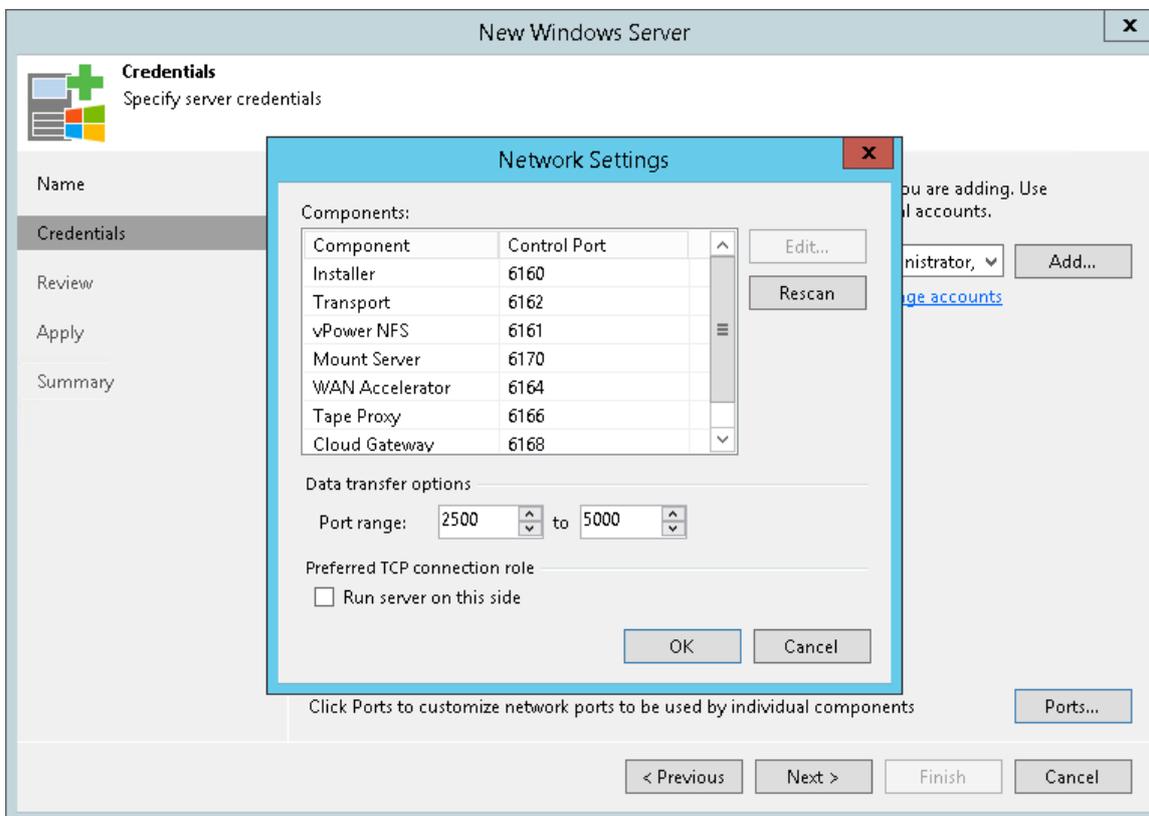


2. To customize network ports used by Veeam Backup & Replication components, click **Ports**. By default, Veeam Backup & Replication components use the following ports:
 - Veeam Installer Service: port 6160
 - Veeam Data Mover Service (Transport): port 6162
 - Veeam vPower NFS Service: 6161
 - Veeam Mount Service: 6170
 - Veeam WAN Accelerator Service: 6164
 - Veeam Tape Proxy Service: 6166
 - Veeam Cloud Gateway Service: 6168
 - Veeam Distribution Service: 9380

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 & Replication 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.

- 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.

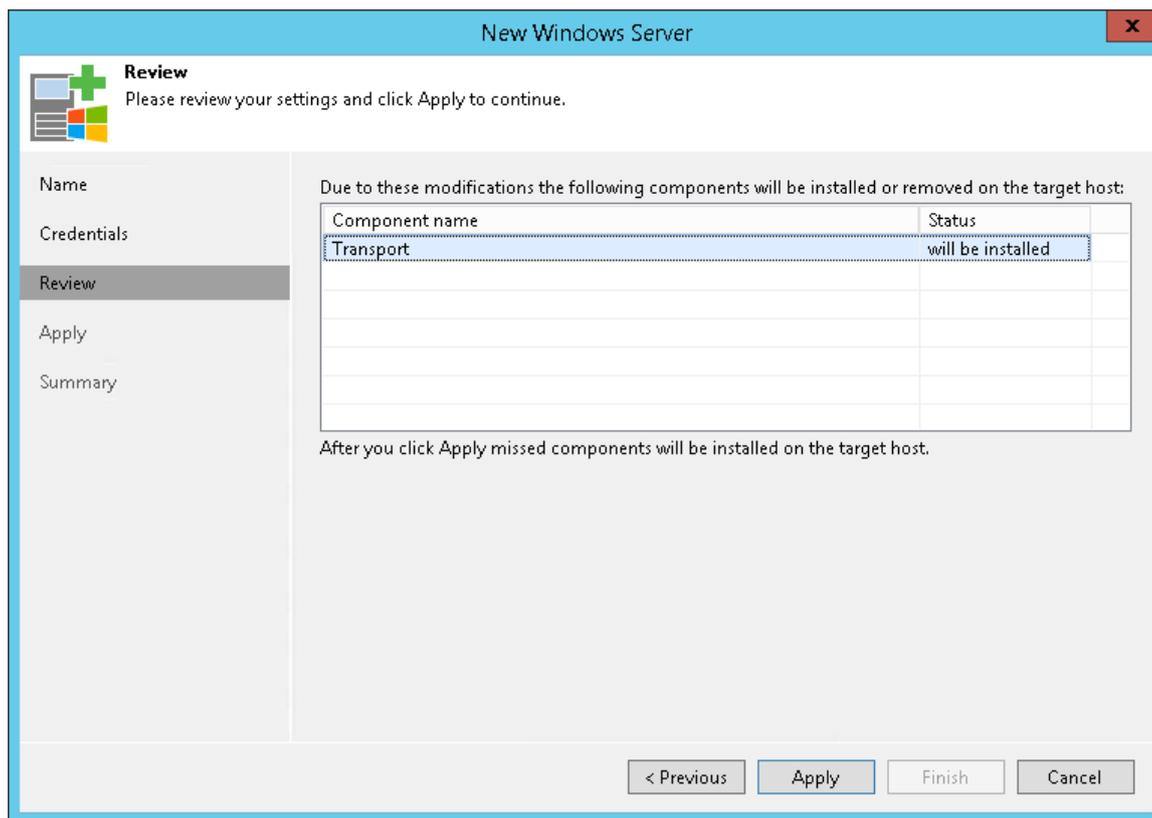


Step 4. Review Components

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

- Review the components.

2. Click **Apply** to add the Microsoft Windows server to the backup infrastructure.

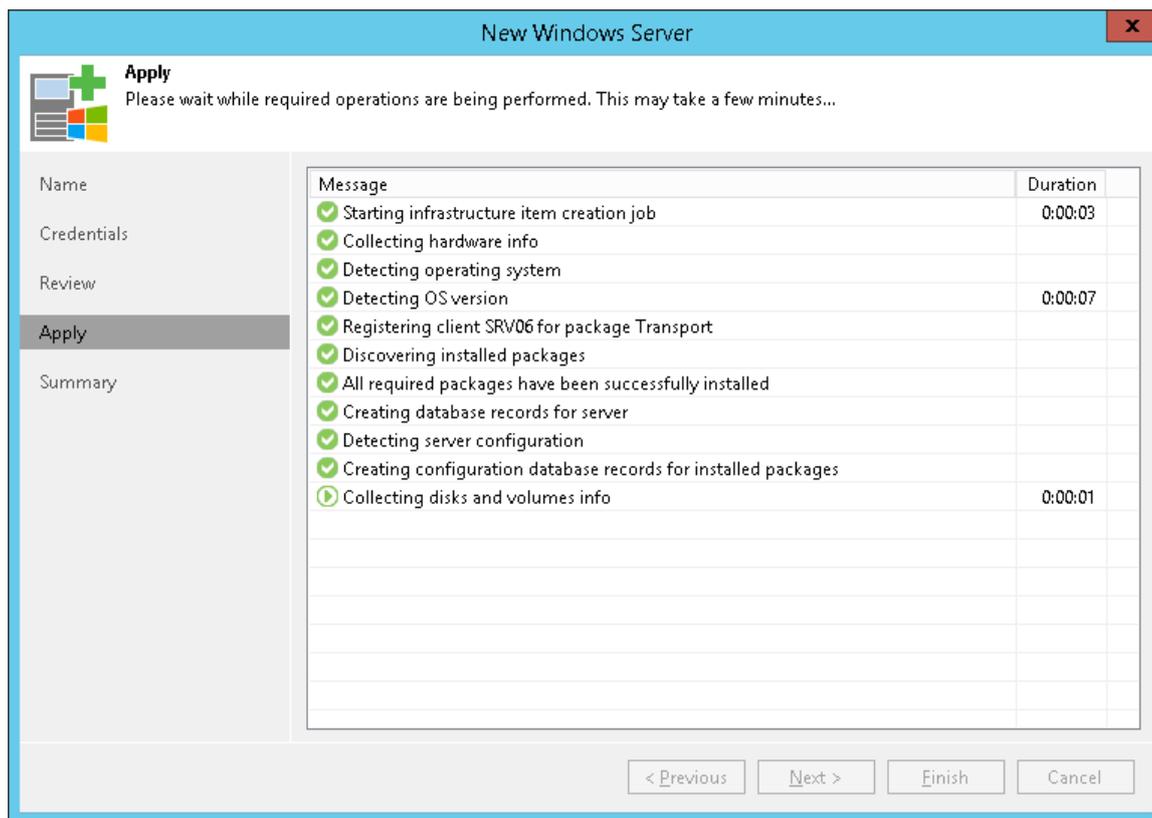


Step 5. Finish Working with Wizard

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 as backup repositories and servers that you plan to use for various types of restore operations.

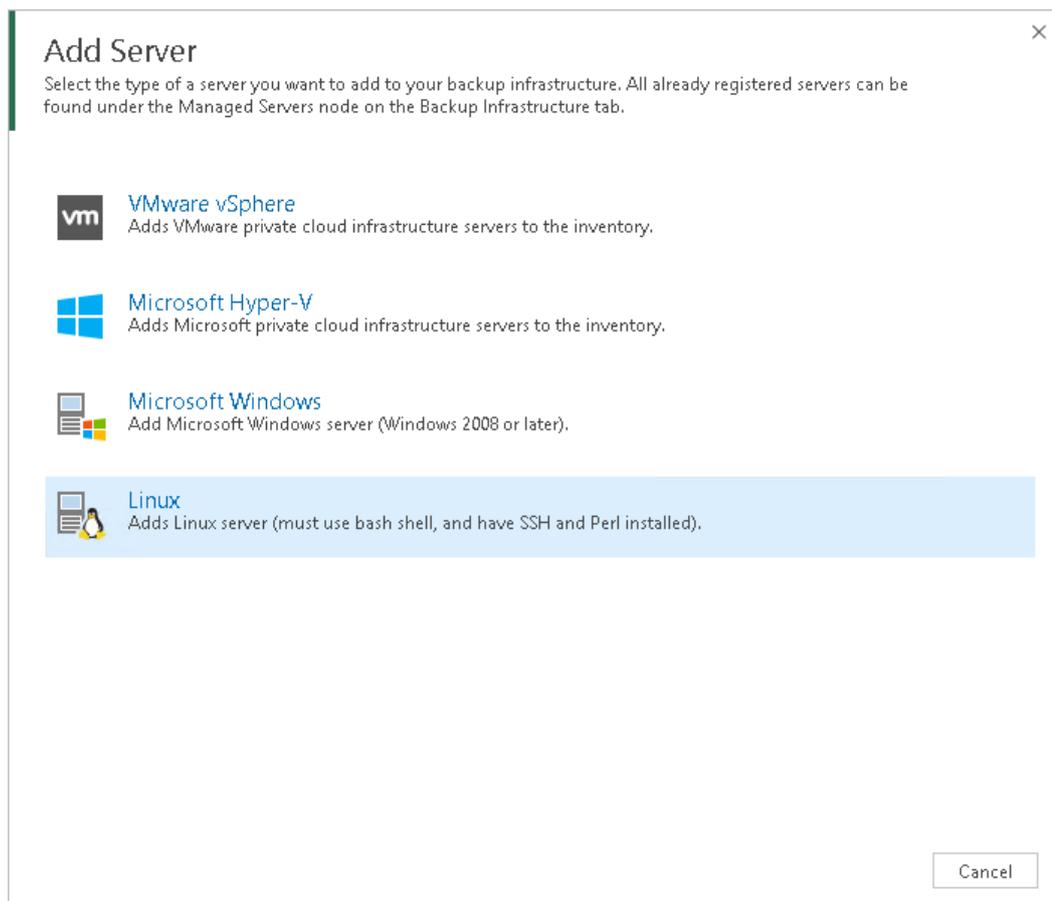
To add a Linux server, use the **New Linux Server** wizard.

Step 1. Launch New Linux Server Wizard

To launch the **New Linux Server** wizard, do one of the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, right-click the **Managed Servers** node and select **Add Server**. Alternatively, you can click **Add Server** on the ribbon.

3. In the **Add Server** window, select **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.

New Linux Server

Name
Specify DNS name or IP address of Linux server. The server must have SSH and Perl installed.

Name
DNS name or IP address:
172.17.53.63

Description:
Linux File Server

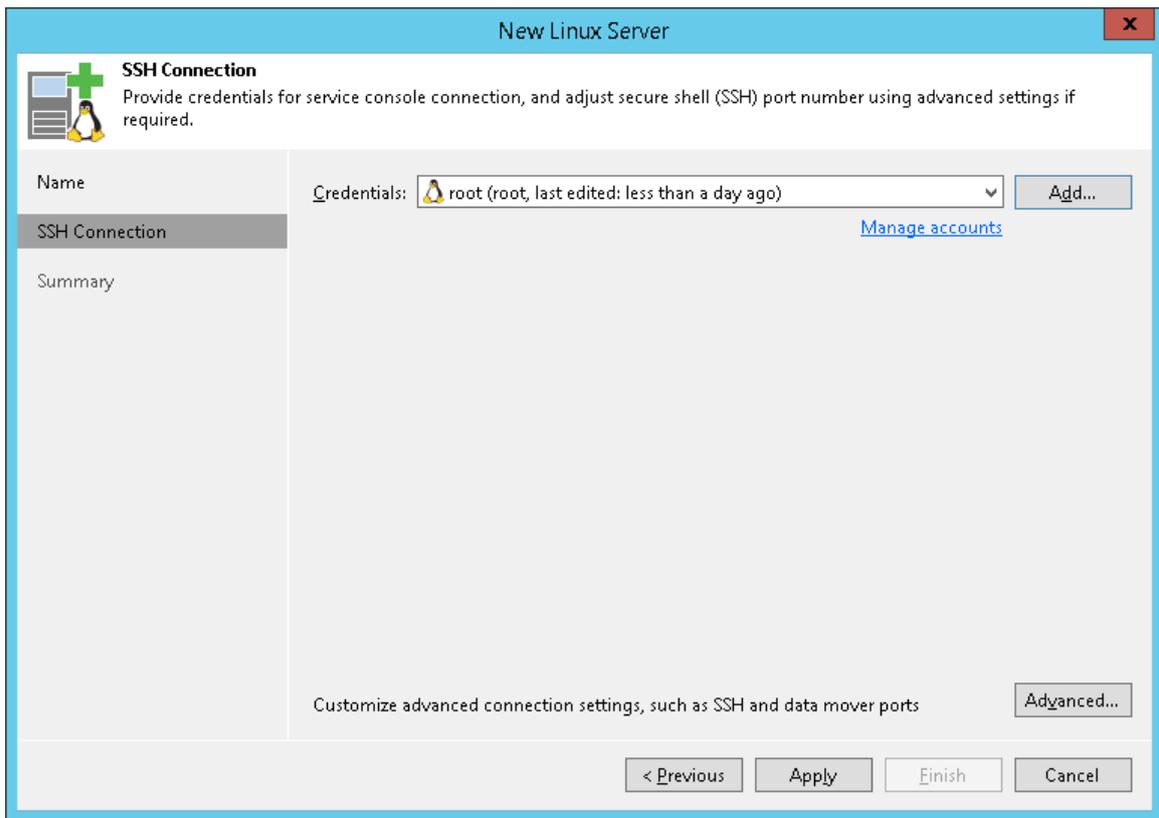
< Previous Next > Finish Cancel

Step 3. Specify Credentials and SSH Settings

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

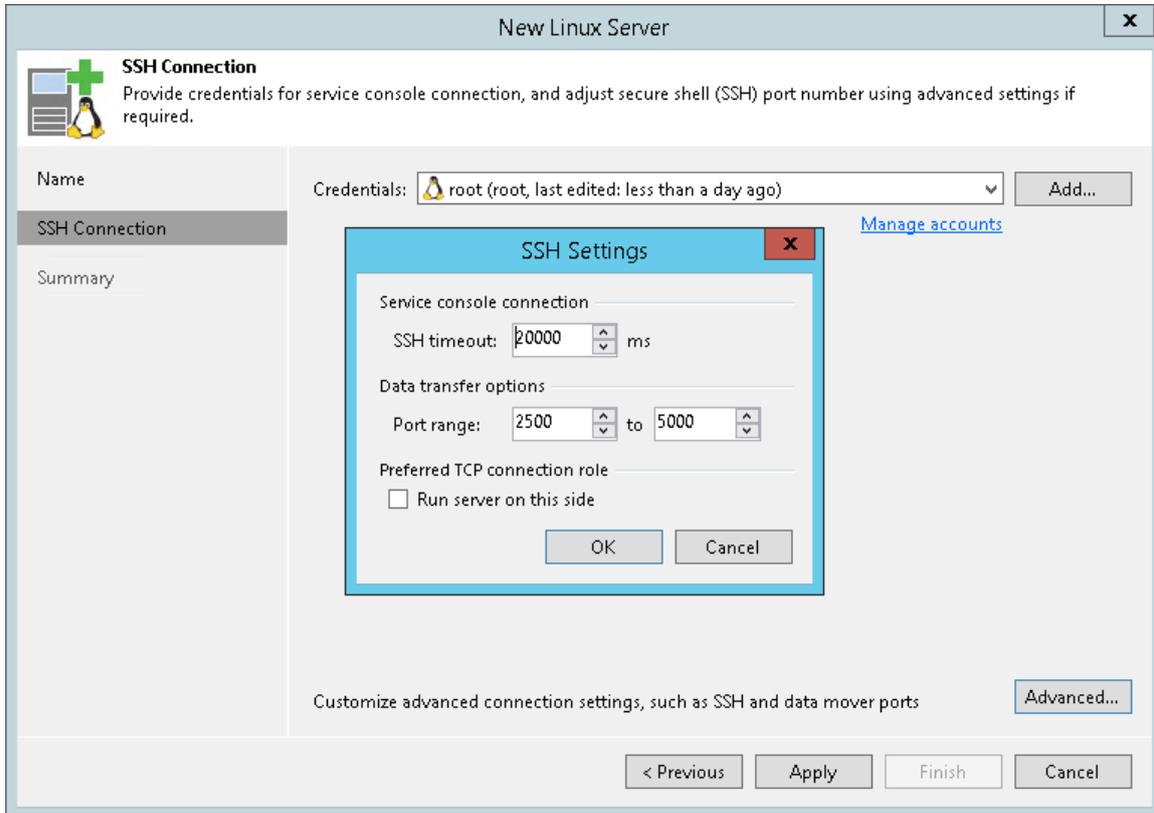
1. From the **Credentials** list, select credentials for the account that has administrator privileges on the Linux server. You can select a credentials record that uses the password authentication method or credentials record that uses the Identity/Pubkey authentication method.

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](#).



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 & Replication will automatically terminate the task.
 - b. In the **Data transfer options** section, 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 & Replication 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.



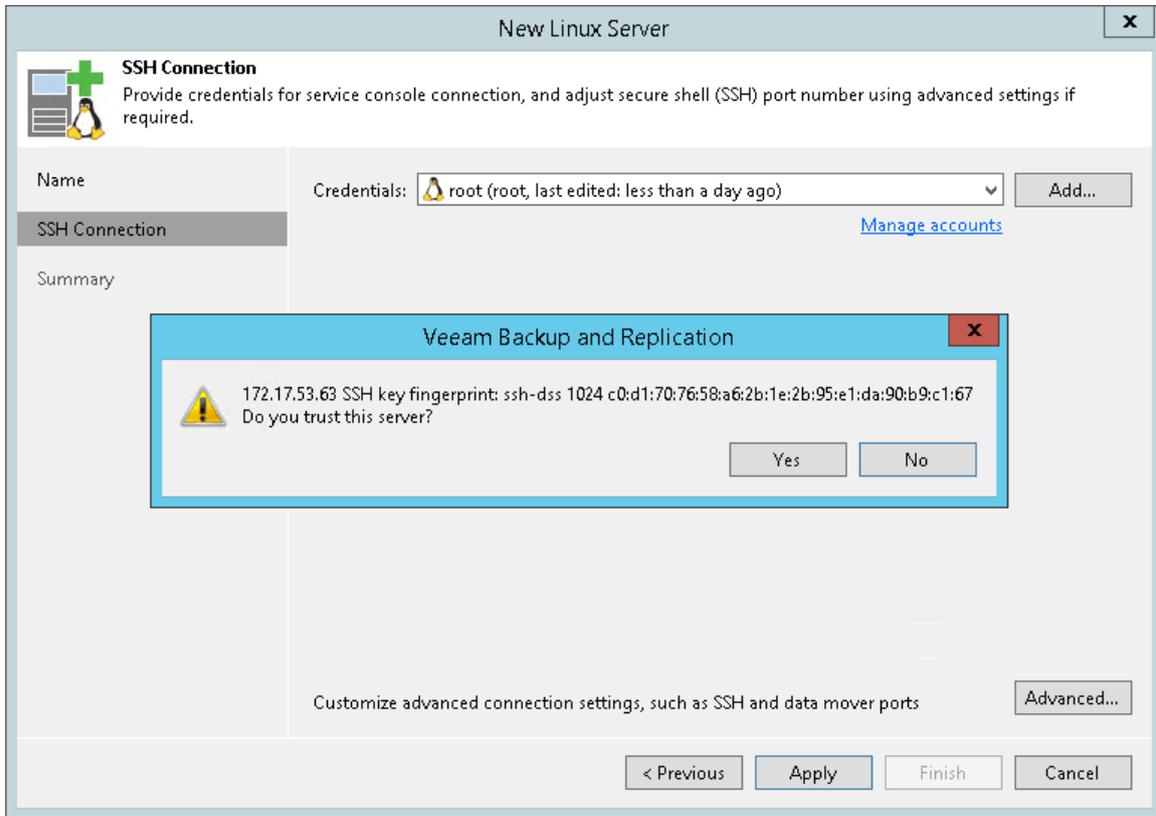
3. When you add a Linux server, Veeam Backup & Replication saves a fingerprint of the Linux host SSH key to the configuration database. During every subsequent connection to the server, Veeam Backup & Replication uses the saved fingerprint to verify the server identity and avoid the man-in-the-middle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

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

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

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.

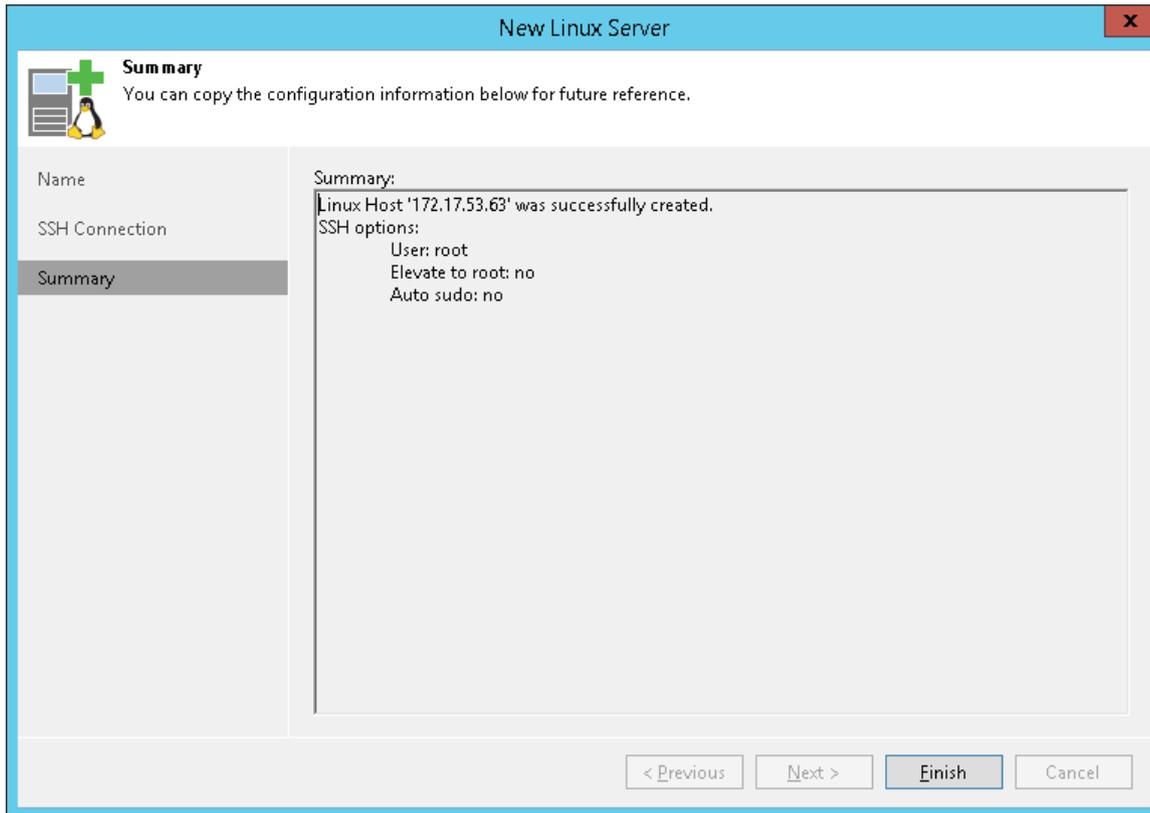


Step 4. Finish Working with Wizard

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.



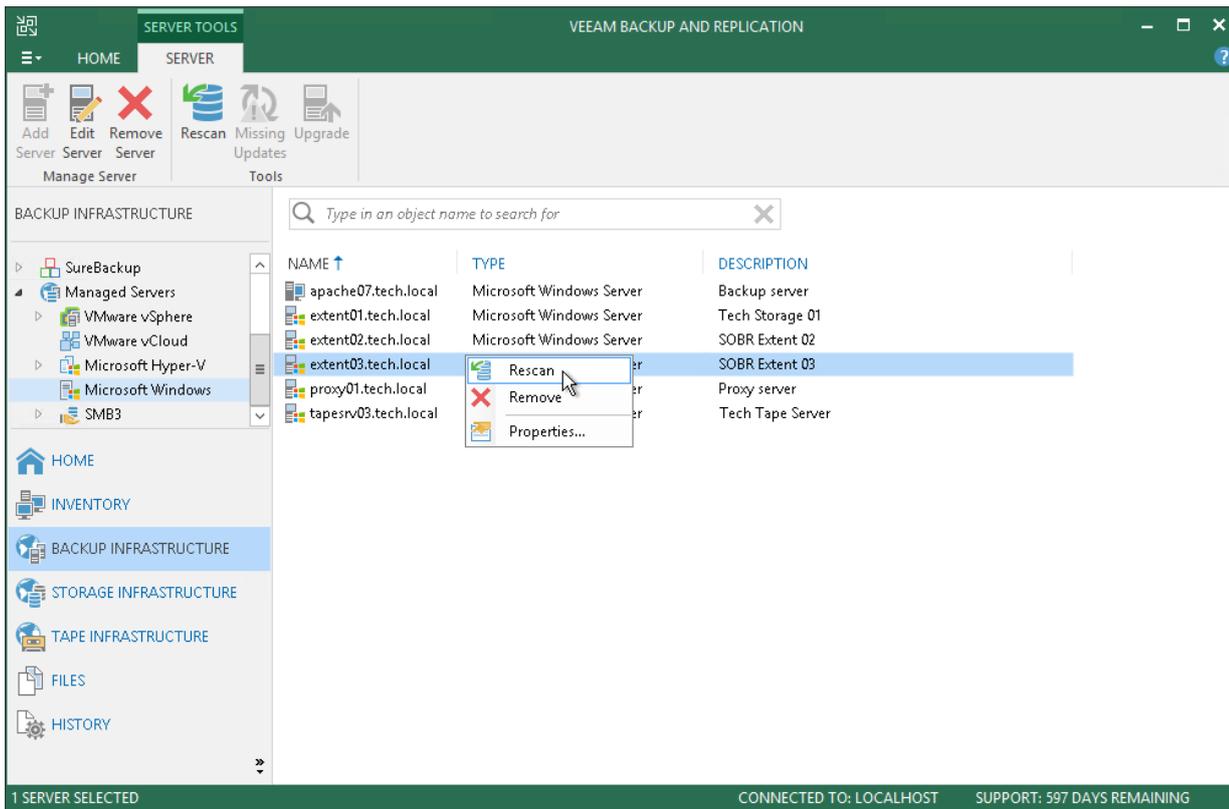
Rescanning Servers

In some cases, you may need to rescan hosts or servers in the backup infrastructure. The rescan operation may be required if you have added or removed new disks and volumes to/from the host or server and want to display actual information in Veeam Backup & Replication. During the rescan operation, Veeam Backup & Replication retrieves information about disks and volumes that are currently connected to a host or server and stores this information to the configuration database.

Veeam Backup & Replication automatically performs a rescan operation every 4 hours. You can also start the rescan operation manually:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed servers**.

3. In the working area, select the server or host and click **Rescan** on the ribbon. Alternatively, you can right-click the server or host and select **Rescan**.

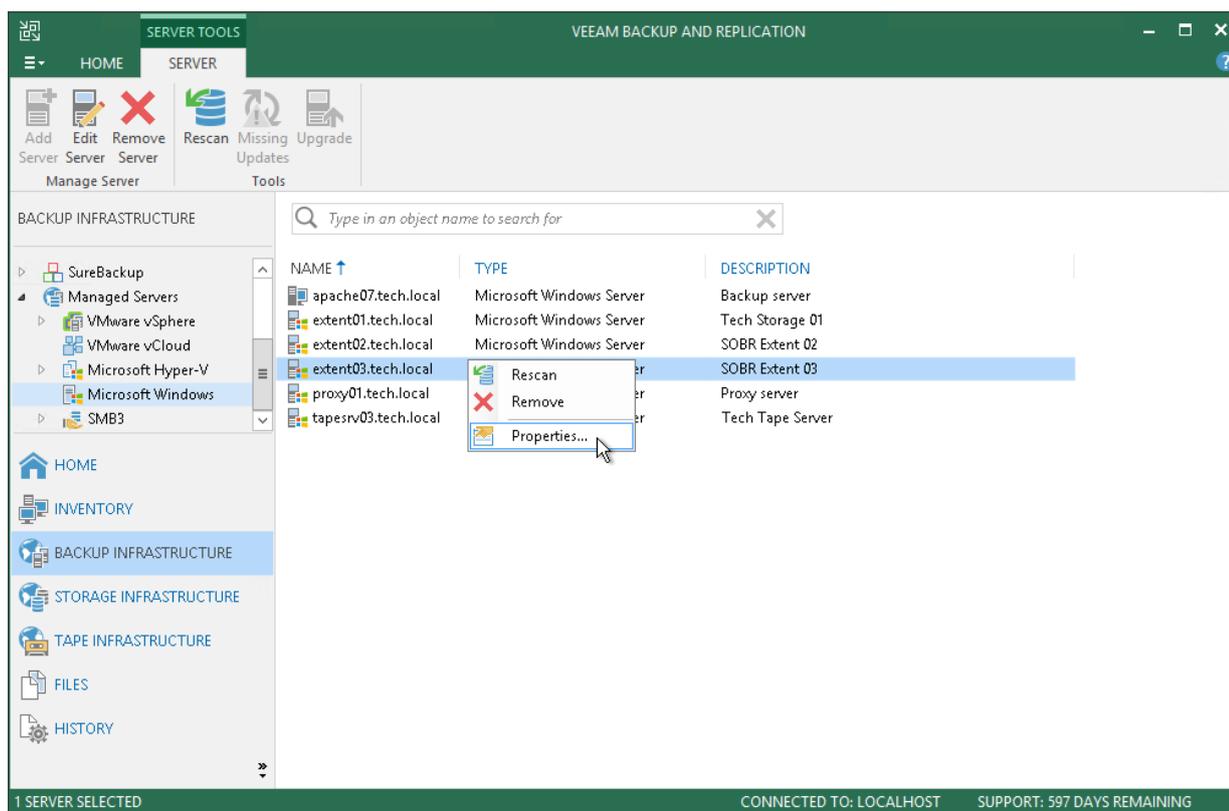


Editing Server Settings

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

If you do not plan to use some server anymore, you can remove it from the backup infrastructure.

You cannot remove a server that has any dependencies. For example, you cannot remove a server that is referenced by a backup or replication job, performs the role of a backup proxy or backup repository. To remove such server, you will need to delete all referencing jobs and roles first.

When you remove a server that is used as a target host or backup repository, backup files and replica files are not removed from disk. You can easily import these files later to Veeam Backup & Replication if needed.

NOTE:

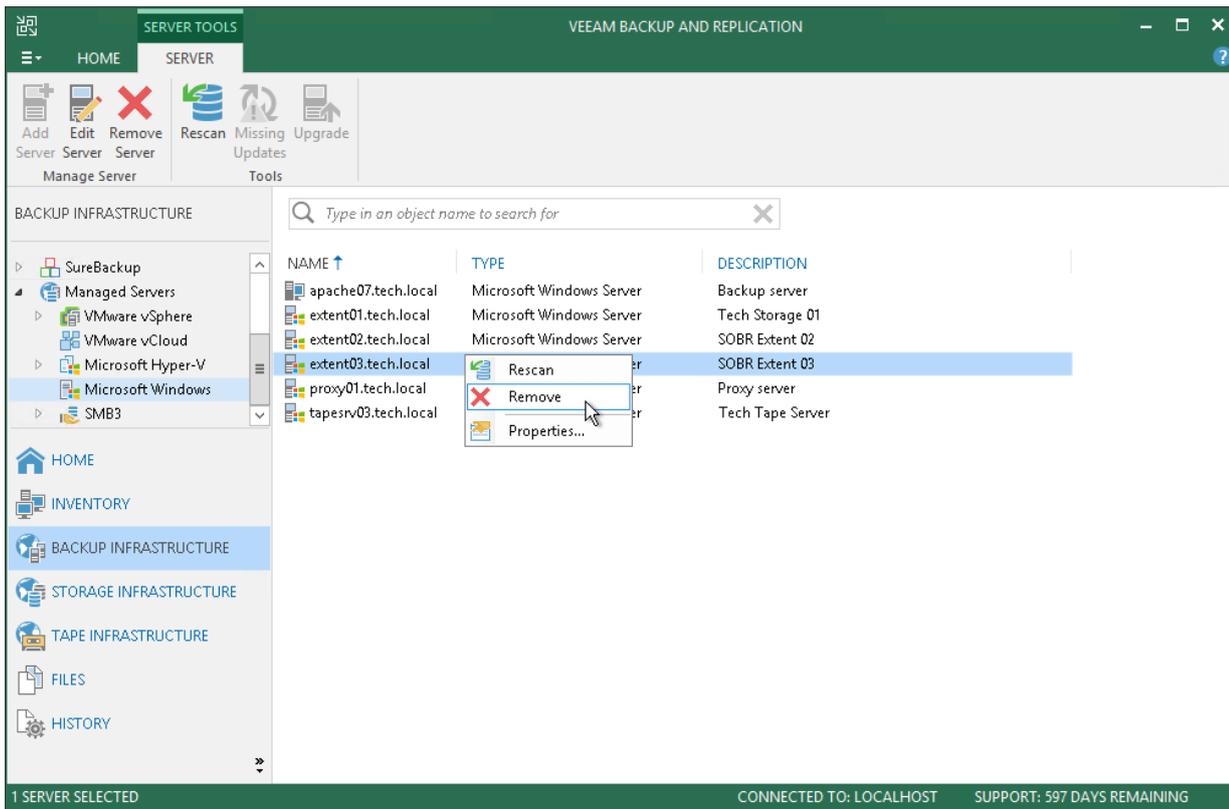
When you remove VMware vCloud Director from the backup infrastructure, vCenter Servers added to vCloud Director are not removed. To remove the vCenter Server, in the inventory pane expand the **vCenter Servers** node, right-click the vCenter Server and select **Remove**.

You cannot remove vCenter Servers added to VMware vCloud Director until the VMware vCloud Director server is removed from the backup infrastructure.

To remove a server from 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 **Remove Server** on the ribbon or right-click the server and select **Remove**.



Backup Proxy

A backup proxy is an architecture component that sits between the backup server and other components of the backup infrastructure. While the backup server administers tasks, the proxy processes jobs and delivers backup traffic.

Basic backup proxy tasks include the following:

- Retrieving VM data from the production storage
- Compressing
- Deduplicating
- Encrypting
- Sending it to the backup repository (for example, if you run a backup job) or another backup proxy (for example, if you run a replication job)

Backup Proxy Transport Modes

Depending on the type of backup proxy and your backup architecture, the backup proxy can use one of the following data transport modes:

- Direct storage access
- Virtual appliance
- Network

If the VM disks are located on the storage system and the storage system is added to the Veeam Backup & Replication console, the backup proxy can also use the Backup from Storage Snapshots mode.

You can explicitly select the transport mode or let Veeam Backup & Replication automatically choose the mode. For details, see [Transport Modes](#) and [Backup from Storage Snapshots](#).

Backup Proxy Deployment

By default, the role of the proxy is assigned to the backup server itself. However, this is sufficient only for small installations with low traffic load. For large installations, it is recommended to deploy dedicated backup proxies.

Use of backup proxies lets you easily scale your backup infrastructure up and down based on your demands. To optimize performance of several concurrent jobs, you can use a number of backup proxies. In this case, Veeam Backup & Replication will distribute the backup workload between available backup proxies. You can deploy backup proxies both in the primary site and in remote sites.

To deploy a proxy, you need to add a Windows-based server to Veeam Backup & Replication and assign the role of a backup proxy to the added server. Backup proxies run light-weight services that take a few seconds to deploy. Deployment is fully automated. Veeam Backup & Replication installs the necessary components and starts the required services on it.

Backup Proxy Services and Components

The backup proxy uses the following services and components:

- **Veeam Installer Service** is an auxiliary service that is installed and started on any Windows server once it is added to the list of managed servers in the Veeam Backup & Replication console. This service analyzes the system, installs and upgrades necessary components and services depending on the role selected for the server.
- **Veeam Data Mover** is a component that performs data processing tasks on behalf of Veeam Backup & Replication, such as retrieving source VM data, performing data deduplication and compression, and storing backed up data on the target storage.

Requirements for Backup Proxy

A machine performing the role of a backup proxy must meet the following requirements:

- The machine must meet the system requirements. For more information, see [System Requirements](#).
- The role of a backup proxy can be assigned to a dedicated Microsoft Windows server (physical or virtual).
- You must add the machine to the Veeam Backup & Replication console as a managed server.

The primary role of the backup proxy is to provide an optimal route for backup traffic and enable efficient data transfer. Therefore, when deploying a backup proxy, you need to analyze the connection between the backup proxy and storage with which it is working. Depending on the type of connection, the backup proxy can be configured in one of the following ways (starting from the most efficient):

- A machine used as a backup proxy should have direct access to the storage on which VMs reside or the storage where VM data is written. This way, the backup proxy will retrieve data directly from the datastore, bypassing LAN.
- The backup proxy can be a VM with HotAdd access to VM disks on the datastore. This type of proxy also enables LAN-free data transfer.
- If neither of the above scenarios is possible, you can assign the role of the backup proxy to a machine on the network closer to the source or the target storage with which the proxy will be working. In this case, VM data will be transported over LAN using NBD protocol.

Limitations for Backup Proxy

The change block tracking mechanism (CBT) is disabled if you back up proxies that use the Virtual appliance (HotAdd) mode to process VM data. For more information on CBT, see [Changed Block Tracking](#).

Transport Modes

Job efficiency and time required for job completion greatly depends on the transport mode. The transport mode is a method that is used by the Veeam Data Mover to retrieve VM data from the source and write VM data to the target.

For data retrieval, Veeam Backup & Replication offers the following modes (starting from the most efficient):

- [Direct storage access](#)
- [Virtual appliance](#)

- [Network](#)

The Veeam Data Mover responsible for data retrieval runs on a backup proxy. Correspondingly, the transport mode can be defined in the settings of the backup proxy that performs the job.

When configuring backup proxy settings, you can manually select a transport mode, or let Veeam Backup & Replication select the most appropriate mode automatically. If you use automatic mode selection, Veeam Backup & Replication will scan backup proxy configuration and its connection to the VMware vSphere infrastructure to choose the optimal transport mode. If several transport modes are available for the same backup proxy, Veeam Backup & Replication will choose the mode in the following order: Direct storage access > Virtual appliance > Network.

The selected transport mode is used for data retrieval. For writing data to the target, Veeam Backup & Replication picks the transport mode automatically, based on the configuration of the backup proxy and transport mode limitations.

For all transport modes, Veeam Backup & Replication leverages VMware vStorage APIs for Data Protection (VADP). VADP can be used for VMware vSphere starting from version 4.

Applicability and efficiency of each transport mode primarily depends on the type of datastore used by the source host – local or shared, and on the backup proxy type – physical or virtual. The table below shows recommendations for installing the backup proxy, depending on the storage type and desired transport mode.

Production Storage Type	Direct Storage Access	Virtual Appliance	Network Mode
Fiber Channel (FC) SAN	Install a backup proxy on a physical server with a direct FC access to the SAN.	Install a backup proxy on a VM running on an ESX(i) host connected to the storage device.	This mode is <i>not recommended</i> on 1 Gb Ethernet but works well with 10 Gb Ethernet.
iSCSI SAN	Install a backup proxy on a physical or virtual machine.		Install a backup proxy on any machine on the storage network.
NFS Storage	Install a backup proxy on a physical or virtual machine.		
Local Storage	Not supported.	Install a backup proxy on a VM on every ESX(i) host.	Install a backup proxy on any machine in the storage network.
VMware Cloud on AWS	Not supported.	Install a backup proxy on a VM running on an ESX(i) host connected to the VSAN storage device.	Not supported.

Direct Storage Access

In the Direct storage access mode, Veeam Backup & Replication reads/writes data directly from/to the storage system where VM data or backups are located. This mode comprises two transport modes:

- [Direct SAN access](#)
- [Direct NFS access](#)

Direct SAN Access

The Direct SAN access transport mode is recommended for VMs whose disks are located on shared VMFS SAN LUNs that are connected to ESX(i) hosts over FC, FCoE, iSCSI, and on shared SAS storage.

In the Direct SAN access transport mode, Veeam Backup & Replication leverages VMware VADP to transport VM data directly from and to FC and iSCSI storage over the SAN. VM data travels over the SAN, bypassing ESX(i) hosts and the LAN. The Direct SAN access transport method provides the fastest data transfer speed and produces no load on the production network.

The Direct SAN access transport mode can be used for all operations where the backup proxy is engaged:

- Backup
- Replication
- VM copy
- Quick migration
- Entire VM restore
- VM disk restore
- Replica failback

Requirements for the Direct SAN Access Mode

To use the Direct SAN access transport mode, make sure that the following requirements are met:

- It is strongly recommended that you assign the role of a backup proxy working in the Direct SAN access mode to a physical machine. If you assign this role to a VM, the backup proxy performance may not be optimal.
- A backup proxy using the Direct SAN access transport mode must have a direct access to the production storage via a hardware or software HBA. If a direct SAN connection is not configured or not available when a job or task starts, the job or task will fail.
- SAN storage volumes presented as VMware datastores must be exposed to the OS of the backup proxy that works in the Direct SAN access transport mode.

The volumes must be visible in Disk Management but must not be initialized by the OS. Otherwise, the VMFS filesystem will be overwritten with NTFS, and volumes will become unrecognizable by ESX(i) hosts. To prevent volumes initialization, Veeam Backup & Replication automatically sets the SAN Policy within each proxy to Offline Shared.

- [For restore operations] A backup proxy must have write access to LUNs where VM disks are located.

Limitations for the Direct SAN Access Mode

- The Direct SAN access transport mode is not supported for VMs residing on vSAN. You can use Virtual appliance and Network transport modes to process such VMs. For details on vSAN restrictions, see [VDDK 5.5 Release Notes](#).
- The Direct SAN access transport mode cannot be used if at least one VM disk is located on a VVol.

- Veeam Backup & Replication uses the Direct SAN access transport mode to read and write VM data only during the first session of the replication job. During subsequent replication job sessions, Veeam Backup & Replication will use the Virtual appliance or Network transport mode on the target side. The source side proxy will keep reading VM data from the source datastore in the Direct SAN access transport mode.

Veeam Backup & Replication writes VM data to the target datastore in the Direct SAN access transport mode only if disks of a VM replica are thick-provisioned. If disks are thin-provisioned, Veeam Backup & Replication will write VM data in the Network or Virtual appliance mode. By default, Veeam Backup & Replication replicates VM disks in the thin format. To write VM data to the target datastore in the Direct SAN access transport mode, select to convert VM disks to the thick format at the **Destination** step of the replication job wizard.

- The Direct SAN access transport mode can be used to restore only thick VM disks.
- The Direct SAN access transport mode cannot be used for incremental restore due to [VMware limitations](#). Either disable CBT for VM virtual disks for the duration of the restore process or select another transport mode for incremental restore.

For VMware vSphere 5.5 and later

IDE and SATA disks can be processed in the Direct SAN access transport mode.

For VMware vSphere 5.1 and earlier

- IDE disks can be backed up in the Direct SAN access transport mode. Restore of IDE disks in the Direct SAN access transport mode is not supported.
- If a VM disk fails to be processed in the Direct SAN access transport mode, Veeam Backup & Replication failover to the Network mode is not possible.
- If some of VM disks are located not on the SAN LUNs, Veeam Backup & Replication will process the VM disks using the Network mode.

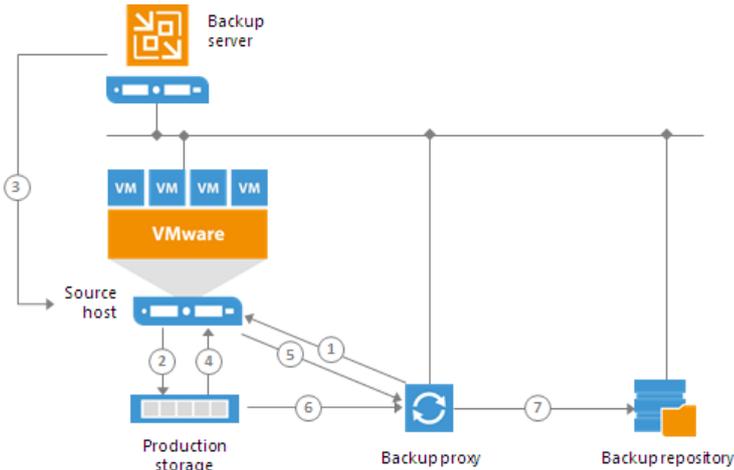
Data Backup in Direct SAN Access Mode

To retrieve VM data blocks from a SAN LUN during backup, the backup proxy uses metadata about the layout of VM disks on the SAN.

Data backup in the Direct SAN access transport mode includes the following steps:

1. The backup proxy sends a request to the ESX(i) host to locate the necessary VM on the datastore.
2. The ESX(i) host locates the VM.
3. Veeam Backup & Replication triggers VMware vSphere to create a VM snapshot.
4. The ESX(i) host retrieves metadata about the layout of VM disks on the storage (physical addresses of data blocks).
5. The ESX(i) host sends metadata to the backup proxy.
6. The backup proxy uses metadata to copy VM data blocks directly from the source storage over the SAN.

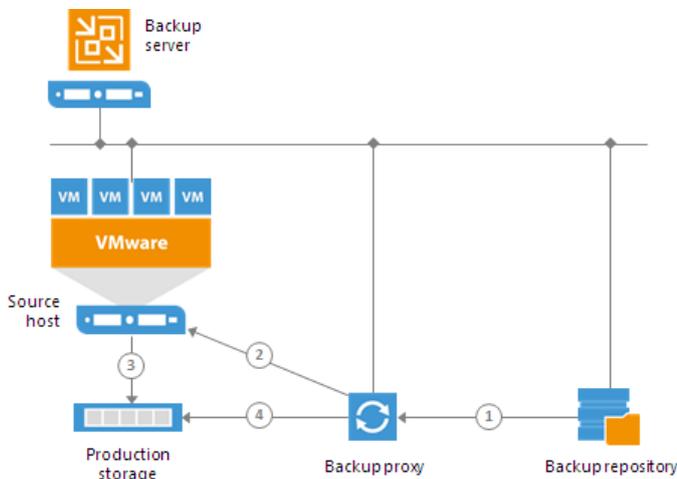
7. The backup proxy processes copied data blocks and sends them to the target.



Data Restore in Direct SAN Access Mode

Data restore in the Direct SAN access transport mode includes the following steps:

1. The backup proxy retrieves data blocks from the backup repository or a datastore in the target site.
2. The backup proxy sends a request to the ESX(i) host in the source site to restore data to a necessary datastore.
3. The ESX(i) host in the source site allocates space on the datastore.
4. Data blocks are written to the datastore.



The Direct SAN access transport mode can be used to restore VMs only with thick disks. Before VM data is restored, the ESX(i) host needs to allocate space for the restored VM disk on the datastore:

- When thick disks are restored, the ESX(i) host allocates space on disk before writing VM data.
- When thin disks are restored, the ESX(i) host attempts to allocate space on the fly, as requests for data blocks restore are received.

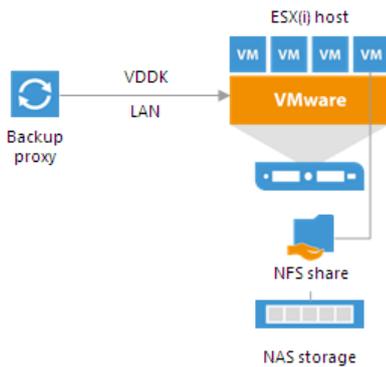
As a result, restore of thin disks involves extra allocation overhead if compared to restore of thick disks, which results in decreased performance.

To restore VMs with thin disks, you can use the Virtual appliance mode or the Network mode. If you plan to process a VM that has both thin and thick disks, you can select the Direct SAN access transport mode and choose to failover to the Network mode if SAN becomes inaccessible. In this case, Veeam Backup & Replication will use the Direct SAN access transport mode to restore thick disks and the Network transport mode to restore thin disks. Alternatively, you can restore all VM disks as thick.

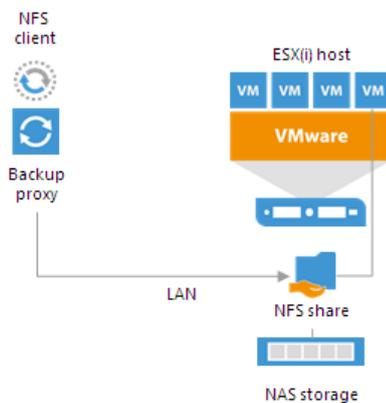
Direct NFS Access

The Direct NFS access is a recommended transport mode for VMs whose disks are located on NFS datastores.

The Direct NFS access mode provides an alternative to the Network mode. When Veeam Backup & Replication processes VM data in the Network mode, it uses VMware VDDK to communicate with the ESX(i) host. This produces additional load on the ESX(i) host.



In the Direct NFS access mode, Veeam Backup & Replication bypasses the ESX(i) host and reads/writes data directly from/to NFS datastores. To do this, Veeam Backup & Replication deploys its native NFS client on the backup proxy and uses it for VM data transport. VM data still travels over LAN but there is no load on the ESX(i) host.



The Direct NFS access mode can be used for all operations where the backup proxy is engaged:

- Backup
- Replication
- Quick migration
- VM copy
- Entire VM restore
- VM disk restore
- Replica failback

Requirements for the Direct NFS Access Mode

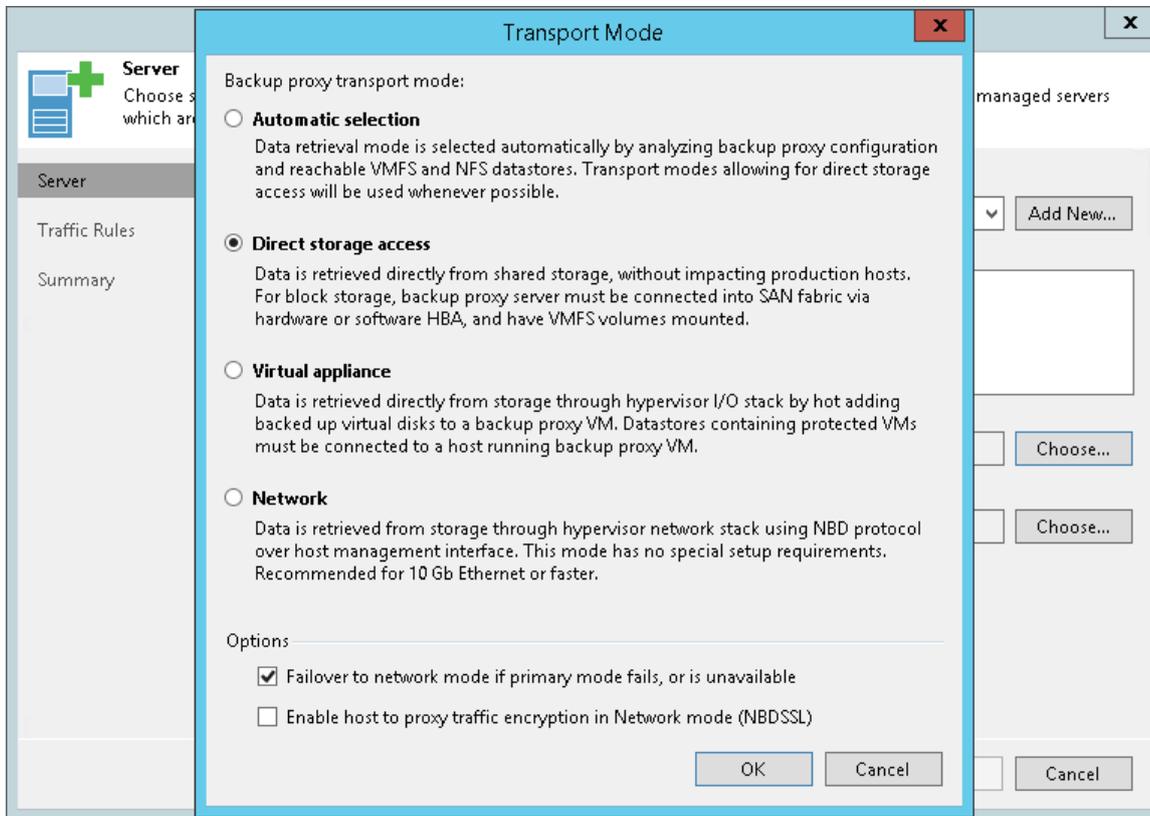
- Direct NFS access mode can be used in VMware vSphere environments running NFS version 3 and 4.1.
- The backup proxy used for VM data processing must have access to the NFS datastores where VM disks are located. For more information, see [Backup Proxy for Direct NFS Access Mode](#).
- If NFS volumes are mounted on the ESX(i) host under names, not IP addresses, the volume names must be resolved by DNS from the backup proxy.

Limitations for Direct NFS Access Mode

- Veeam Backup & Replication cannot parse delta disks in the Direct NFS access mode. For this reason, the Direct NFS access mode has the following limitations:
 - The Direct NFS access mode cannot be used for VMs that have at least one snapshot.
 - Veeam Backup & Replication uses the Direct NFS transport mode to read and write VM data only during the first session of the replication job. During subsequent replication job sessions, the VM replica will already have one or more snapshots. For this reason, Veeam Backup & Replication will use another transport mode to write VM data to the datastore on the target side. The source side proxy will keep reading VM data from the source datastore in the Direct NFS transport mode.
- If you enable the **Enable VMware tools quiescence** option in the job settings, Veeam Backup & Replication will not use the Direct NFS transport mode to process running Microsoft Windows VMs that have VMware Tools installed.
- If a VM has some disks that cannot be processed in the Direct NFS access mode, Veeam Backup & Replication processes these VM disks in the Network transport mode.

Backup Proxy for Direct NFS Access Mode

Veeam Backup & Replication deploys its NFS agent on every backup proxy when you assign the backup proxy role to a Microsoft Windows server (physical or virtual). To instruct the backup proxy to use the Direct NFS access mode, you must choose the **Automatic selection** or **Direct storage access** option in the backup proxy settings.



To read and write data in the Direct NFS transport mode, the backup proxy must meet the following requirements:

1. The backup proxy must have access to the NFS datastore.
2. The backup proxy must have *ReadOnly/Write* permissions and root access to the NFS datastore.

Backup Proxy Selection

Veeam Backup & Replication selects backup proxies working in the Direct NFS access transport mode by the following rules:

- If you instruct Veeam Backup & Replication to select a backup proxy automatically for a job or task, Veeam Backup & Replication picks a backup proxy with the minimum number of hops to the NFS datastore. If there are several backup proxies with the equal number of hops in the backup infrastructure, Veeam Backup & Replication picks the least busy backup proxy in the backup infrastructure.

If all backup proxies with the minimum number of hops are busy at the moment, Veeam Backup & Replication waits until these backup proxies are free. Veeam Backup & Replication does not pick a backup proxy that has a greater number of hops to the NFS datastore and works in the Direct NFS access or Virtual appliance transport mode.

- If you select one or more backup proxies explicitly for a job or task, Veeam Backup & Replication does not regard the number of hops to the NFS datastore. Veeam Backup & Replication picks the least busy backup proxy working in the Direct NFS access transport mode.

If all backup proxies working in the Direct NFS access transport mode are busy, Veeam Backup & Replication waits until these backup proxies are free. Veeam Backup & Replication does not pick a backup proxy working in the Virtual appliance transport mode.

To detect the number of hops from a backup proxy to the NFS datastore, Veeam Backup & Replication uses the host discovery process. During host discovery, Veeam Backup & Replication obtains information about the number of hops, checks to which NFS datastores the backup proxy has access and what permissions the backup proxy has on NFS datastores.

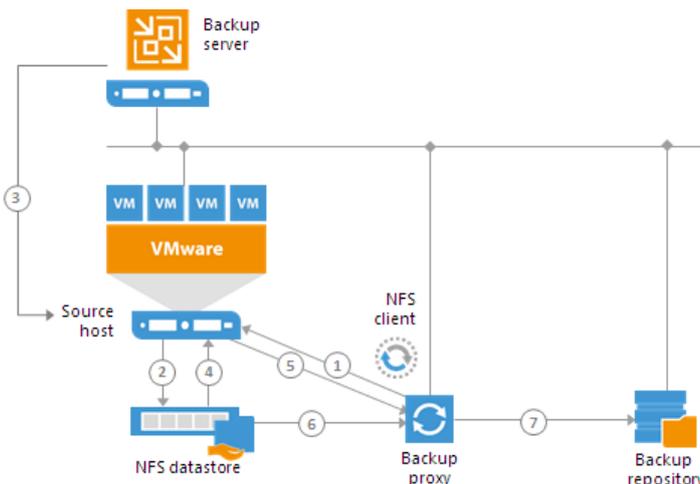
The host discovery process rescans all Microsoft Windows machines to which the backup proxy role is assigned. The process starts automatically every 4 hours. Host discovery is also triggered when you change the transport mode settings and choose to use the Direct storage access for the backup proxy.

If necessary, you can start the host discovery process manually. To do this, perform the **Rescan** operation for a machine to which the backup proxy role is assigned.

Data Backup in Direct NFS Access Mode

Data backup in the Direct NFS access transport mode is performed in the following way:

1. The backup proxy sends a request to the ESX(i) host to locate a VM on the NFS datastore.
2. The ESX(i) host locates the VM.
3. Veeam Backup & Replication triggers VMware vSphere to create a VM snapshot.
4. The ESX(i) host retrieves metadata about the layout of VM disks on the storage (physical addresses of data blocks).
5. The ESX(i) host sends metadata to the backup proxy.
6. The backup proxy uses metadata to copy VM data blocks directly from the NFS datastore over LAN.
7. The backup proxy processes copied data blocks and sends them to the target over LAN.

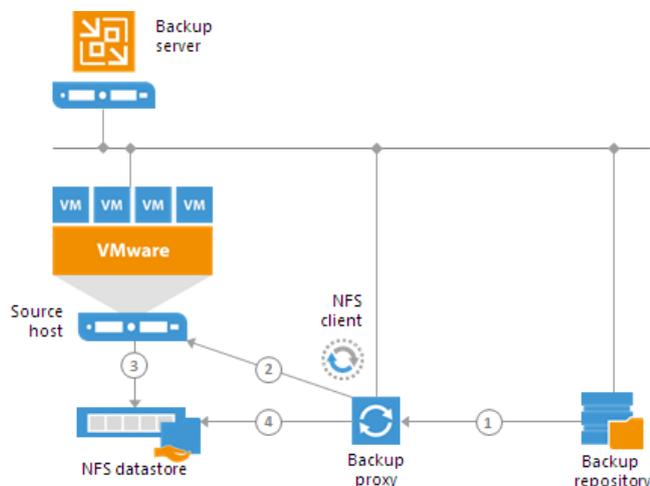


Data Restore in Direct NFS Access Mode

Data restore in the Direct NFS access transport mode is performed in the following way:

1. The backup proxy retrieves data blocks from the backup repository or a datastore in the target site.

2. The backup proxy sends a request to the ESX(i) host to restore data to an NFS datastore.
3. The ESX(i) host allocates space on the NFS datastore.
4. Data blocks obtained from the backup proxy are written to the NFS datastore over LAN.



Virtual Appliance

The Virtual appliance mode is not so efficient as the Direct storage access mode but provides better performance than the Network mode. The Virtual appliance mode is recommended if the role of a backup proxy is assigned to a VM.

In the Virtual appliance mode, Veeam Backup & Replication uses the VMware SCSI HotAdd capability that allows attaching devices to a VM while the VM is running. During backup, replication or restore disks of the processed VM are attached to the backup proxy. VM data is retrieved or written directly from/to the datastore, instead of going through the network.

The Virtual appliance transport mode can be used for all operations where the backup proxy is engaged:

- Backup
- Replication
- VM copy
- Quick migration
- Entire VM restore
- VM disk restore
- Replica failback

Requirements for the Virtual Appliance mode

To use the Virtual appliance transport mode, make sure that the following requirements are met:

- The role of a backup proxy must be assigned to a VM.
- The ESX(i) host on which the backup proxy is deployed must have access to the datastore hosting disks of VMs that you plan to process.
- If you plan to process VMs that store disks on the NFS datastore, you must deploy the backup proxy on the same ESX(i) host where these VMs reside.

- The backup server and backup proxy must have the latest version of VMware Tools installed.
- SCSI 0:X controller must be present on a backup proxy. In the opposite case, VM data processing in the Virtual appliance transport mode will fail.

Limitations for the Virtual Appliance mode

- If a backup proxy used to process a source VM resides on a VMFS 3 datastore, it must be formatted with proper block size to be able to mount the largest virtual disk of hot-added VMs:
 - 1 MB block size – 256 GB maximum file size
 - 2 MB block size – 512 GB maximum file size
 - 4 MB block size – 1024 GB maximum file size
 - 8 MB block size – 2048 GB maximum file size

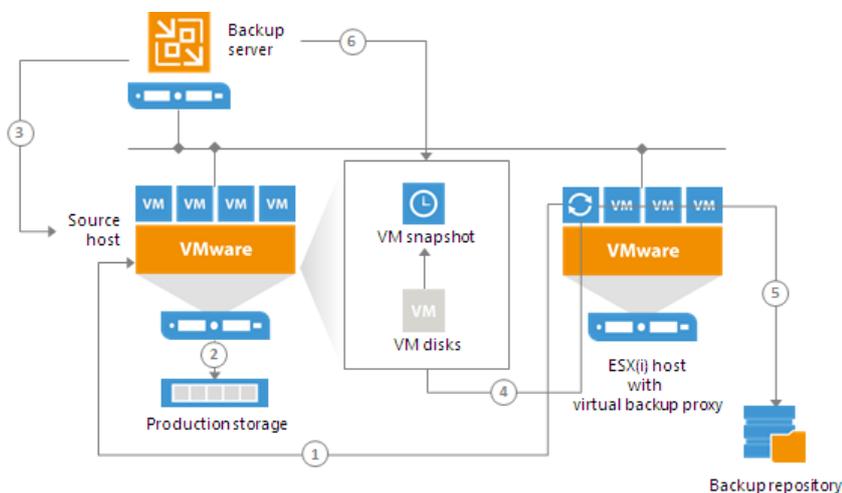
This limitation does not apply to VMFS-5 volumes that always have 1 MB file block size.

- For vSphere 5.1 the maximum supported VMDK size is 1.98 TB. For vSphere 5.5 and later the maximum supported VMDK size is 62 TB.
- Backup and restore of IDE disks in the Virtual appliance mode is not supported.
- Backup and restore of SATA disks in the Virtual appliance mode is supported if you use VMware vSphere 6.0 and later.

Data Backup and Restore in Virtual Appliance Mode

The process of data retrieval in the Virtual appliance transport mode includes the following steps:

1. The backup proxy sends a request to the ESX(i) host to locate the necessary VM on the datastore.
2. The ESX(i) host locates the VM.
3. Veeam Backup & Replication triggers VMware vSphere to create a VM snapshot.
4. VM disks are attached (hot-added) to the backup proxy.
5. Veeam Backup & Replication reads data directly from disks attached to the backup proxy.
6. When the VM processing is complete, VM disks are detached from the backup proxy and the VM snapshot is deleted.



The process of data restore in the Virtual appliance mode works in a similar manner. VM disks from the backup are attached to the backup proxy and Veeam Backup & Replication transports VM data to the target datastore. After the restore process is finished, VM disks are detached from the backup proxy.

ESXi host interacts with VMware Cloud on AWS through VMware vCenter. Veeam Backup & Replication performs backup through the networkless Virtual appliance (HotAdd) mode.

Virtual Appliance Mode for VMs on VSAN

To transport data of VMs residing on VSAN in the Virtual appliance mode, you must assign the backup proxy role to a VM.

The backup proxy VM must meet the following requirements:

- The backup proxy VM must reside on any of ESXi hosts connected to a VSAN cluster.
Veeam Backup & Replication will retrieve data of processed VMs over the I/O stack of the ESX(i) host on which the backup proxy is deployed.
- Disks of the backup proxy VM must reside on the VSAN cluster.

If you have several backup proxies on ESXi hosts in the VSAN cluster, Veeam Backup & Replication chooses the most appropriate backup proxy to reduce the backup traffic on the VSAN cluster network. To choose a backup proxy, Veeam Backup & Replication checks HDDs directly attached to every ESXi host and calculates the amount of VM data on these HDDs. The preference is given to the ESXi host that has a direct access to an HDD with the maximum amount of VM data. This approach helps reduce workload on the ESXi I/O stack during data transport.

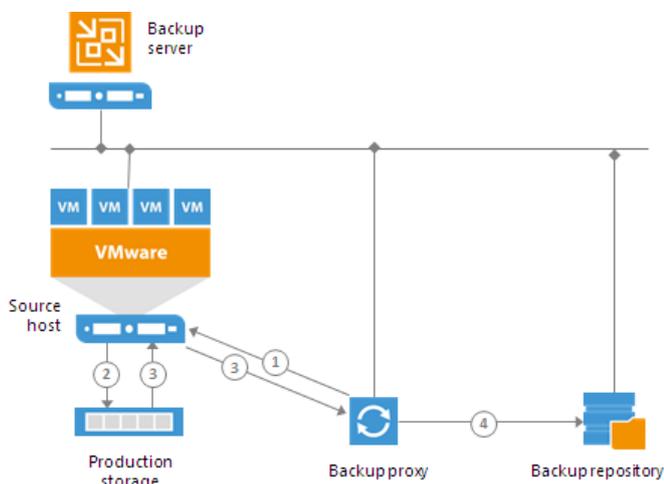
NOTE:

Even if disks of a VM are located on a host where the backup proxy is deployed, VSAN traffic may still be observed between hosts in the cluster. This behavior depends on the VSAN cluster itself and cannot be modified in Veeam Backup & Replication.

Network Mode

The Network mode can be used with any infrastructure configuration. In this mode, data is retrieved via the ESX(i) host over LAN using the Network Block Device protocol (NBD).

The Network mode is not a recommended data transport mode because of low data transfer speed over LAN. To take the load off the LAN, Veeam Backup & Replication provides two alternative modes: [Direct Storage Access](#) and [Virtual Appliance](#). The Network mode is the only applicable mode when the backup proxy role is assigned to a physical machine and the host uses local storage.



The process of data retrieval in Network mode includes the following steps:

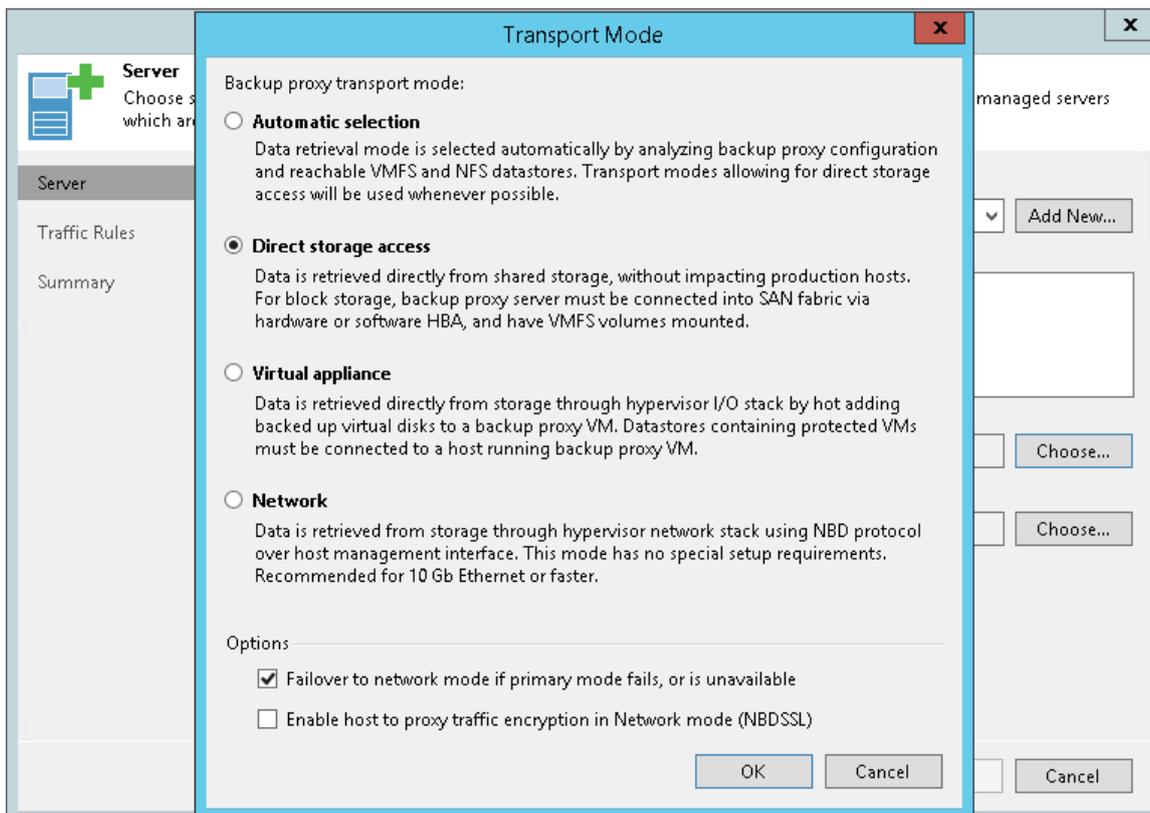
1. The backup proxy sends a request to the ESX(i) host on which the processed VM is registered to locate the VM on the datastore.
2. The ESX(i) host locates the processed VM on the datastore.
3. Veeam Backup & Replication instructs VMware vSphere to create a VMware vSphere VM snapshot, copies VM data blocks from the source storage and sends them to the backup proxy over LAN.
4. The backup proxy sends the data to target.

Veeam Backup & Replication processes VM disks in parallel. If VM disks are located on different storage types (for example, on the SAN and local storage), Veeam Backup & Replication uses different transport modes to process VM disks. In such scenario, it is strongly recommended that you select the **Failover to network mode if primary mode fails, or is unavailable** option when configuring the mode settings for the backup proxy.

Failover to Network Mode

You can instruct Veeam Backup & Replication to switch to the Network transport mode and transfer VM data over LAN if the primary transport mode – Direct storage access or Virtual appliance – cannot be used for some reason. This option is enabled by default to ensure that jobs and tasks can be completed successfully in any situation.

Note that data transport over LAN puts additional load on your production network and may potentially affect performance if you accomplish data protection and disaster recovery tasks in business hours.



Adding VMware Backup Proxies

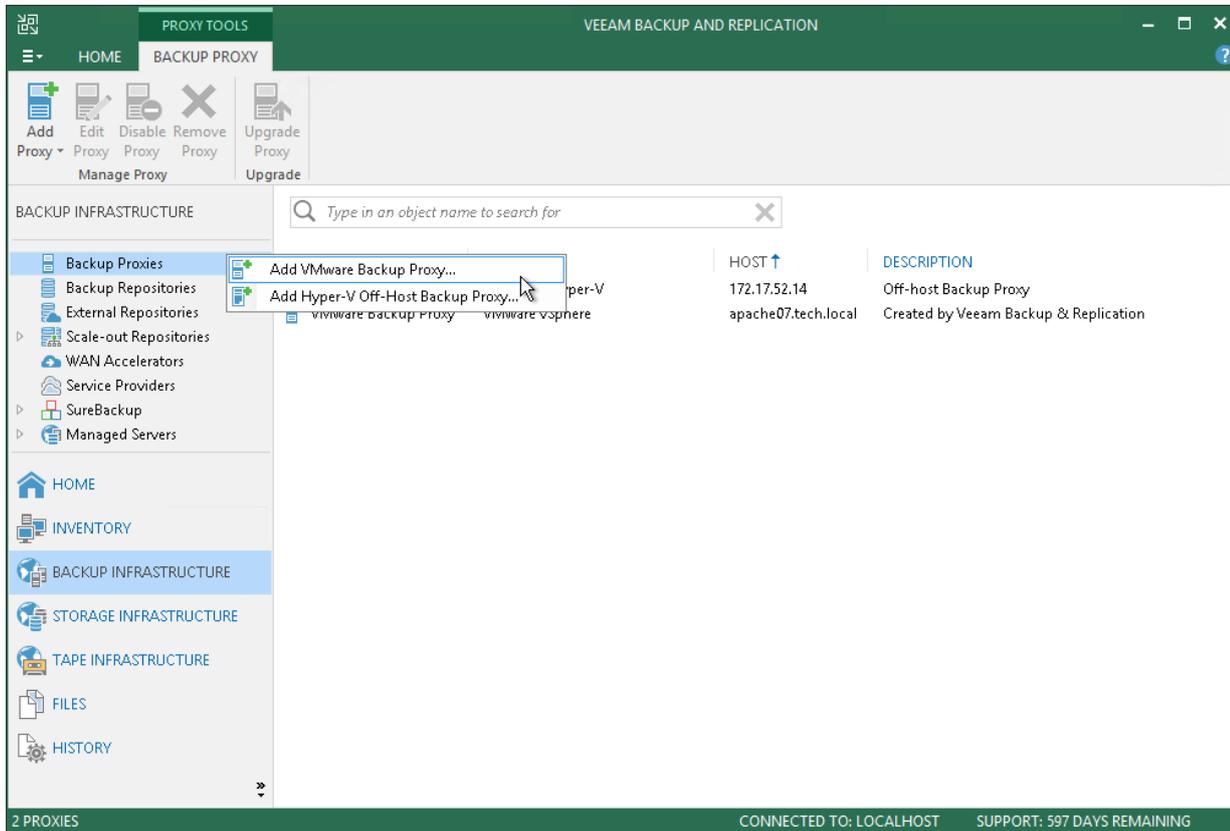
You can configure one or more backup proxies in the backup infrastructure.

To add a backup proxy, use the **New VMware Proxy** wizard.

Step 1. Launch New VMware Proxy Wizard

To launch the **New VMware Proxy** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select the **Backup Proxies** node, click **Add Proxy** on the ribbon and select **VMware**.
- Open the **Backup Infrastructure** view, in the inventory pane right-click the **Backup Proxies** node and select **Add VMware Backup Proxy**.



Step 2. Choose Microsoft Windows Server

At the **Server** step of the wizard, specify server settings for the backup proxy.

1. From the **Choose server** list, select a Microsoft Windows server to which you want to assign the backup proxy role. If the server is not added to the backup infrastructure yet, you can click **Add New** to open the **New Windows Server** wizard. For more information, see [Adding Microsoft Windows Servers](#).
2. In the **Proxy description** field, provide a description for future reference. The default description contains information about the user who added the backup proxy, date and time when the backup proxy was added.
3. In the **Transport mode** field, select a mode that the backup proxy must use for VM data transport. By default, Veeam Backup & Replication analyzes the backup proxy configuration, defines to which datastores it has access and automatically selects the best transport mode depending on the type of connection between the backup proxy and datastores.

If necessary, you can manually select the data transport mode. Click **Choose** on the right of the **Transport mode** field and select one of the following modes: *Direct storage access*, *Virtual appliance* or *Network*.

4. In the **Options** section of the **Transport Mode** window, specify additional options for the selected transport mode:

- [For Direct storage access and Virtual appliance transport modes] If the primary transport mode fails during the job session, Veeam Backup & Replication will automatically fail over to the Network transport mode. To disable failover, clear the **Failover to network mode if primary mode fails, or is unavailable** check box.
 - [For Network mode] You can choose to transfer VM data over an encrypted TLS connection. To do this, select the **Enable host to proxy traffic encryption in Network mode (NBDSSL)** check box. Traffic encryption puts more stress on the CPU of an ESX(i) host but ensures secure data transfer.
5. In the **Connected datastores** field, specify datastores to which the backup proxy has a direct SAN or NFS connection. By default, Veeam Backup & Replication automatically detects all datastores that the backup proxy can access.

You can set up the list of datastores manually if you want the backup proxy to work with specific datastores. Click **Choose** on the right of the **Connected datastores** field, choose **Manual selection** and add datastores with which the backup proxy must work in the Direct storage access mode.

6. In the **Max concurrent tasks** field, specify the number of tasks that the backup proxy must handle in parallel. If this value is exceeded, the backup proxy will not start a new task until one of current tasks finishes.

Veeam Backup & Replication creates one task per every VM disk. The recommended number of concurrent tasks is calculated automatically based on available resources. Backup proxies 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.

NOTE:

In some cases, the backup proxy may not be able to use some transport modes due to known limitations. For more information, see [Transport Modes](#).

The screenshot shows the 'New VMware Proxy' configuration window. The window title is 'New VMware Proxy'. On the left, there is a sidebar with three items: 'Server', 'Traffic Rules', and 'Summary'. The 'Server' item is selected. The main area contains the following fields and controls:

- Choose server:** A dropdown menu showing 'proxy01.tech.local' and an 'Add New...' button.
- Proxy description:** A text box containing 'Proxy 01'.
- Transport mode:** A dropdown menu showing 'Automatic selection' and a 'Choose...' button.
- Connected datastores:** A dropdown menu showing 'Automatic detection (recommended)' and a 'Choose...' button.
- Max concurrent tasks:** A spinner box showing '4' with a green checkmark icon to its right.

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

Step 3. Configure Traffic Throttling Rules

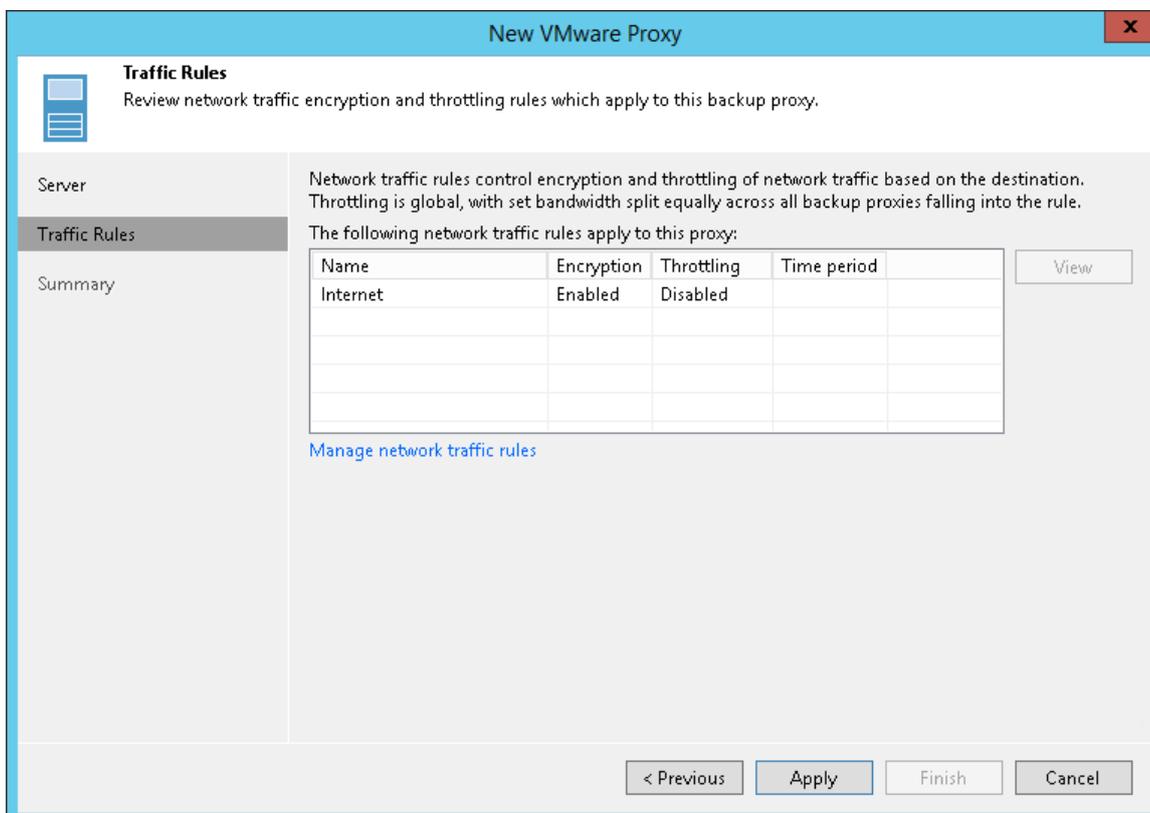
At the **Traffic Rules** step of the wizard, configure throttling rules to limit the outbound traffic rate for the backup proxy. Throttling rules can help you manage bandwidth usage and minimize impact of data protection and disaster recovery tasks on network performance. For more information, see [Setting Network Traffic Throttling Rules](#).

The list of throttling rules contains only the rules that are applicable to the backup proxy. The rule is applied to the backup proxy if the backup proxy IP address falls into the source IP range of the rule.

To view rule settings:

1. Select the rule in the list.
2. Click **View** on the right of the rule list.

You can open global throttling settings and modify them directly from the **New VMware Proxy** wizard. To do this, click the **Manage network traffic throttling rules** link at the bottom of the wizard.

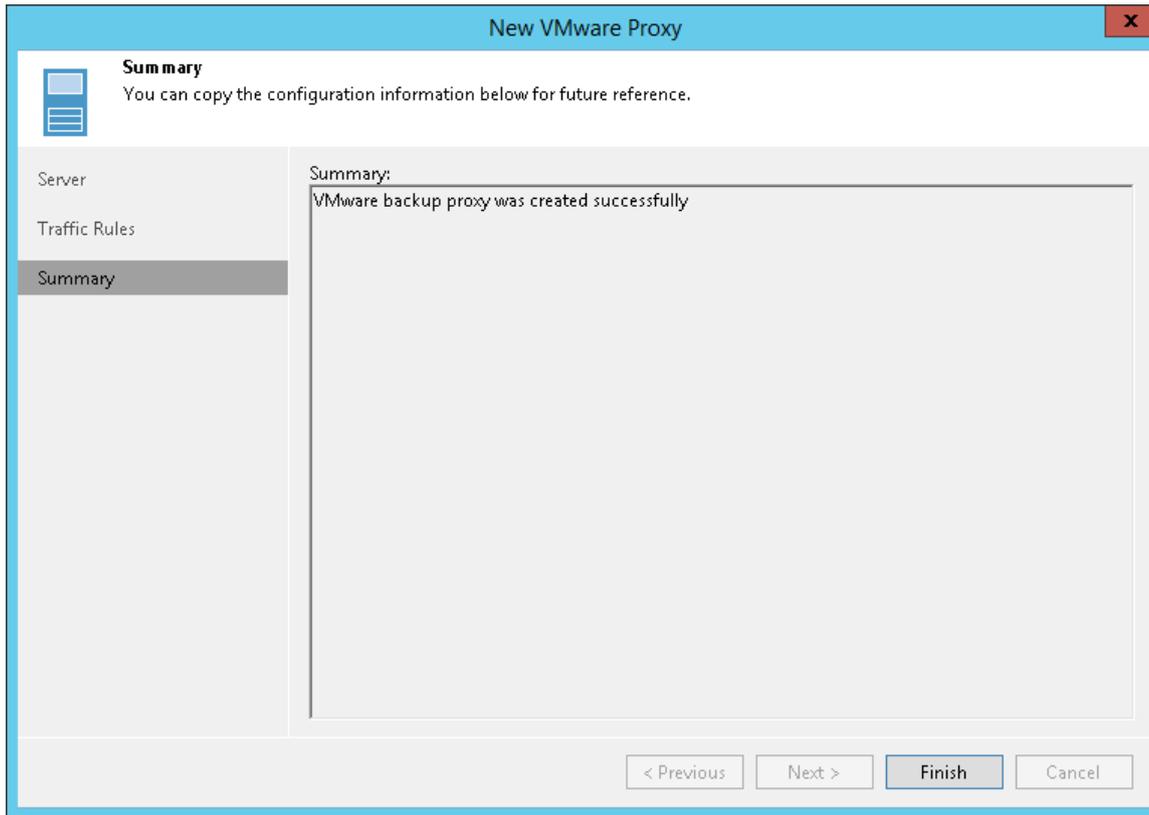


Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of backup proxy configuration.

1. Review details of the backup proxy.

2. Click **Finish** to exit the wizard.



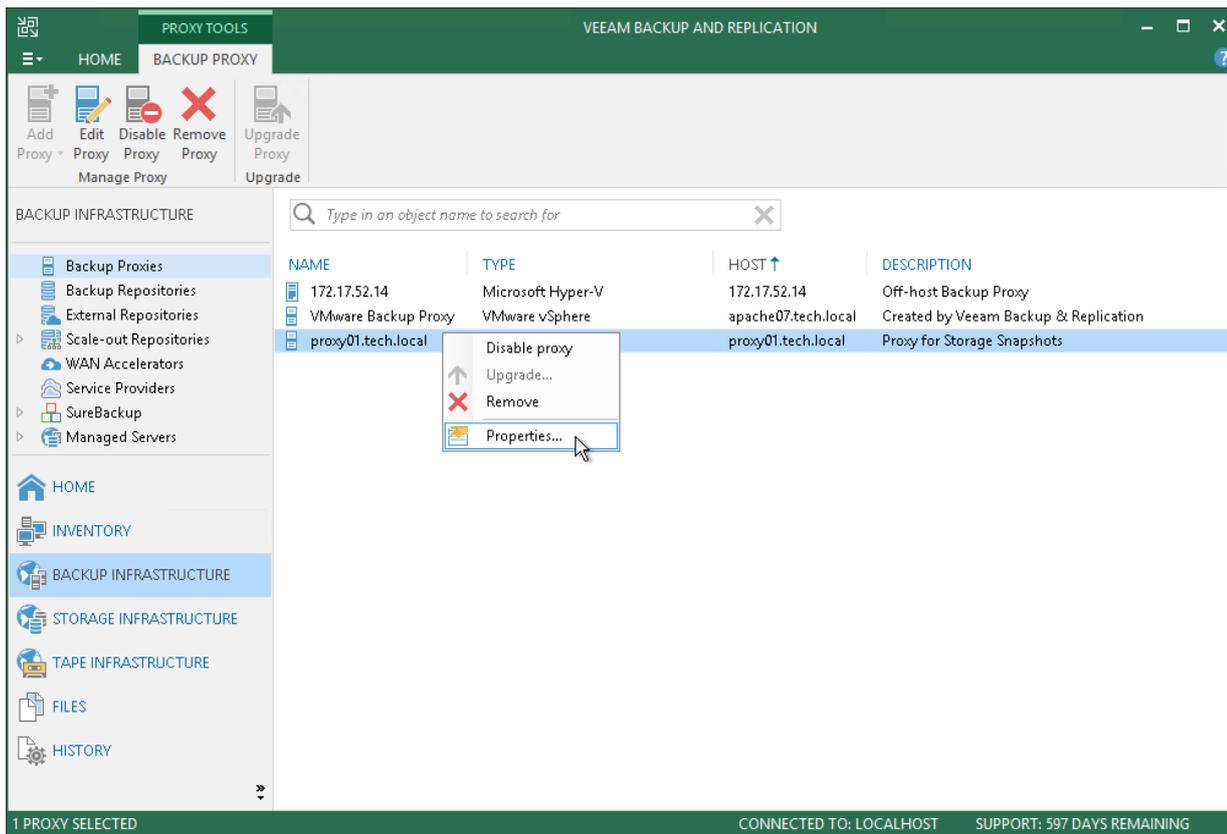
Editing Backup Proxy Settings

You can edit settings of backup proxies you have configured.

To edit backup proxy settings:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the working area, select the backup proxy and click **Edit Proxy** on the ribbon or right-click the backup proxy and select **Properties**.

4. Edit backup proxy settings as required.



Disabling and Removing Backup Proxies

You can temporarily disable a backup proxy or remove it from the backup infrastructure.

Disabling Backup Proxies

When you disable a backup proxy, Veeam Backup & Replication does not use this backup proxy for any jobs configured on the backup server. Backup proxy disabling can be helpful if you instruct Veeam Backup & Replication to automatically select backup proxies for jobs and do not want Veeam Backup & Replication to use specific backup proxies.

You can disable all backup proxies, including the default backup proxy installed on the backup server. Do not disable all backup proxies at once. Otherwise, Veeam Backup & Replication will not be able to perform backup, replication and restore operations that use backup proxies.

To disable a backup proxy:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the working area, select the backup proxy and click **Disable Proxy** on the ribbon or right-click the backup proxy and select **Disable proxy**.

You can enable a disabled backup proxy at any time:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.

3. In the working area, select the backup proxy and click **Disable Proxy** on the ribbon once again or right-click the backup proxy and select **Disable proxy**.

Removing Backup Proxies

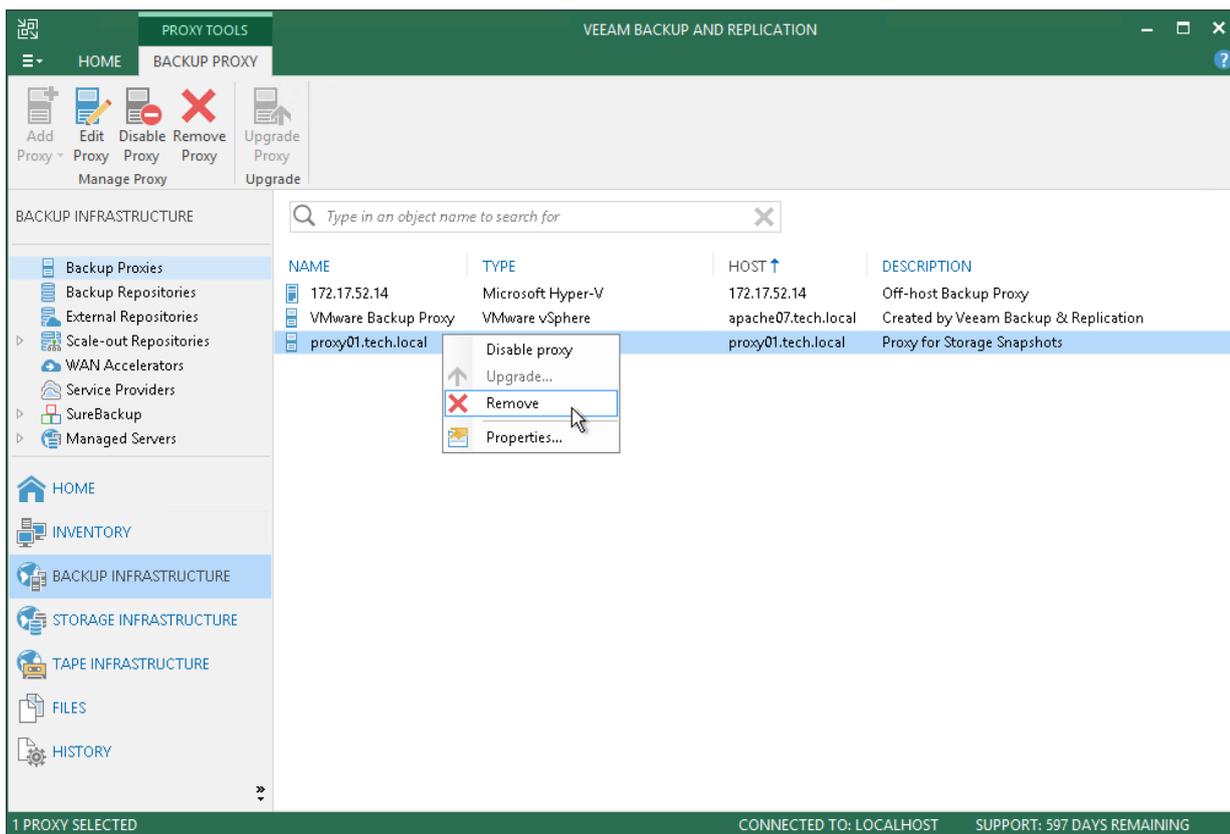
You can permanently remove a backup proxy from the backup infrastructure. When you remove a backup proxy, Veeam Backup & Replication unassigns the backup proxy role from the server, and this server is no longer used as a backup proxy. The actual server remains in the backup infrastructure.

You can remove all backup proxies, including the default backup proxy installed on the backup server. Do not remove all backup proxies at once. Otherwise, Veeam Backup & Replication will not be able to perform backup, replication and restore operations that use backup proxies.

You cannot remove a backup proxy that is explicitly selected in any backup, replication or VM copy job. To remove such backup proxy, you first need to delete a reference to this backup proxy in the job settings.

To remove a backup proxy:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Proxies** node.
3. In the working area, select the backup proxy and click **Remove Proxy** on the ribbon or right-click the backup proxy and select **Remove**.



Backup Repository

A backup repository is a storage location where Veeam keeps backup files, VM copies and metadata for replicated VMs. To configure a backup repository, you can use the following storage types:

- **Direct attached storage.** You can add virtual and physical servers as backup repositories:
 - [Microsoft Windows Servers](#)
 - [Linux Servers](#)
- **Network attached storage.** You can add [CIFS \(SMB\) shares](#) as backup repositories.
- **Deduplicating storage appliances.** You can add the following deduplicating storage appliances as backup repositories:
 - [Dell EMC Data Domain](#)
 - [ExaGrid](#)
 - [HPE StoreOnce](#)
 - [Quantum DXi](#)
- **Object storage.** You can use cloud storage services as backup repositories. For details, see [Object Storage](#).

NOTE:

Do not configure multiple backup repositories pointing to the same location or using the same path.

Microsoft Windows Server

You can use a Microsoft Windows server with local or directly attached storage as a backup repository. The storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric.

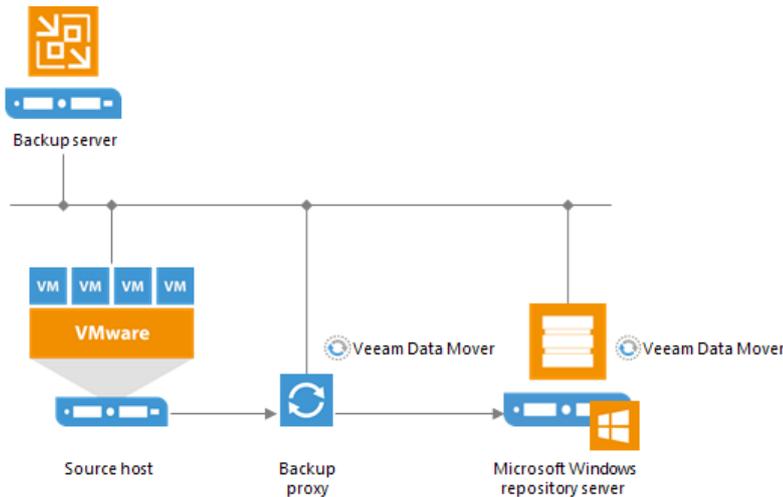
Microsoft Windows Repository Deployment

To communicate with a Microsoft Windows-based repository, Veeam Backup & Replication uses two Data Mover Services that are responsible for data processing and transfer:

- Veeam Data Mover on a backup proxy
- Veeam Data Mover on the Microsoft Windows repository

When any job addresses the backup repository, the Data Mover Service on the backup proxy establishes a connection with the Data Mover Service on the backup repository, enabling efficient data transfer over LAN or WAN.

The Data Mover is installed automatically when you add a server to Veeam Backup & Replication as a managed server.



vPower NFS Server

Windows repositories can be configured to function as vPower NFS Servers. In this case, Veeam Backup & Replication will run the Veeam vPower NFS Service directly on the backup repository (namely, on the managing Windows server to which storage is attached) and provide ESX(i) hosts with transparent access to backed up VM images stored on the backup repository. For more information, see [Veeam vPower NFS Service](#).

Requirements for Microsoft Windows Server Based Repositories

A machine performing the role of a repository must meet the following requirements:

- The machine must meet the system requirements. For more information, see [System Requirements](#).
- The role of the repository can be assigned to a Microsoft Windows machine (physical or virtual).
- You must add the machine to the Veeam Backup & Replication console as a managed server.

Linux Server

You can add Linux server with local, directly attached storage or mounted NFS as a backup repository. The storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), NFS share, or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric.

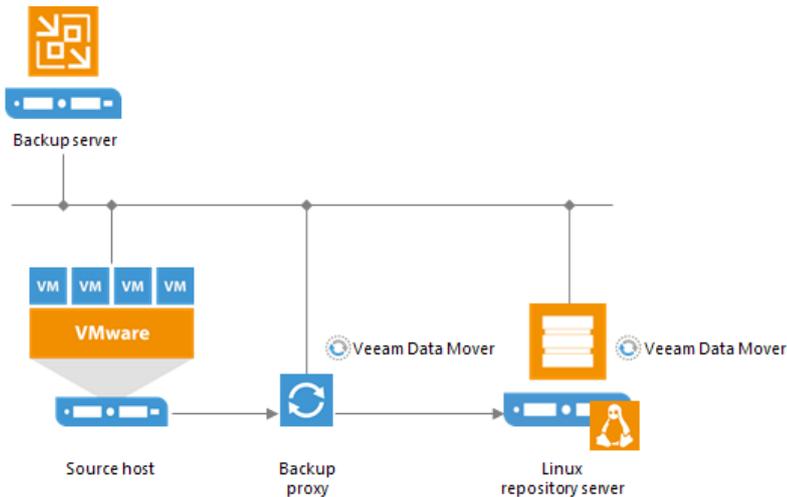
Linux Backup Repository Deployment

To communicate with a Linux-based repository, Veeam Backup & Replication uses two Data Mover Services that are responsible for data processing and transfer:

- Veeam Data Mover on the backup proxy
- Veeam Data Mover on the Linux backup repository

Linux repository does not host the Veeam Data Mover permanently. When any task addresses a Linux repository, Veeam Backup & Replication deploys and starts the Veeam Data Mover on the backup repository.

The Data Mover Service establishes a connection with the source-side Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.



Requirements for Linux Backup Repositories

A machine performing the role of a repository must meet the following requirements:

- The machine must meet the system requirements. For more information, see [System Requirements](#).
- The role of the repository can be assigned to a Linux machine (physical or virtual).
- You must add the machine to the Veeam Backup & Replication console as a managed server.
- Veeam Backup & Replication uses the SSH protocol to communicate with Linux backup repositories and requires the SCP utility on Linux repositories. Make sure that the SSH daemon is properly configured and SCP utility is available on the Linux host.

CIFS (SMB) Share

You can use CIFS (SMB) shares as backup repositories.

SMB Backup Repository Deployment

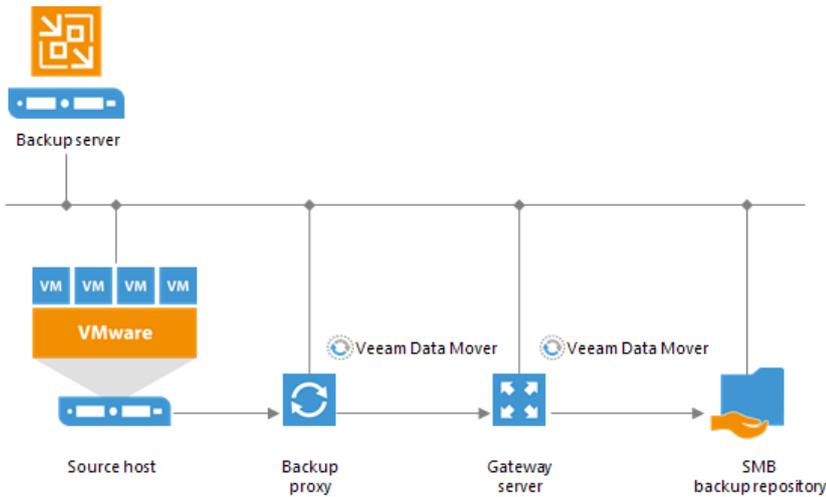
To communicate with an SMB backup repository, Veeam Backup & Replication uses two Data Mover Services that are responsible for data processing and transfer:

- Veeam Data Mover on the backup proxy
- Veeam Data Mover on the gateway server

An SMB share cannot host Veeam Data Movers. For this reason, to communicate with the SMB share, you need to deploy a gateway server. Veeam Backup & Replication will automatically deploy a Veeam Data Mover on this gateway server. For more information, see [Gateway Server](#).

When any job addresses the backup repository, the Data Mover Service on the gateway server establishes a connection with the Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.

If you plan to move VM data to an offsite SMB repository over a WAN link, it is recommended that you deploy an additional gateway server in the remote site, closer to the SMB repository.



Requirements for SMB Backup Repositories

A machine performing the role of an SMB repository must meet the following requirements:

- The machine must meet the system requirements. For more information, see [System Requirements](#).
- The role of the repository can be assigned to a Microsoft Windows machine (physical or virtual).

Dell EMC Data Domain

You can use Dell EMC Data Domain storage systems with Data Domain Boost (DD Boost) as backup repositories.

To support the DD Boost technology, Veeam Backup & Replication leverages the following Dell EMC Data Domain components:

- **DD Boost library.** The DD Boost library is a component of the Dell EMC Data Domain system. The DD Boost library is embedded into the Veeam Data Mover Service setup. When you add a Microsoft Windows server to the backup infrastructure, the DD Boost Library is automatically installed on the added server together with the Data Mover Service.
- **DD Boost server.** The DD Boost server is a target-side component. The DD Boost server runs on the OS of the Dell EMC Data Domain storage system.

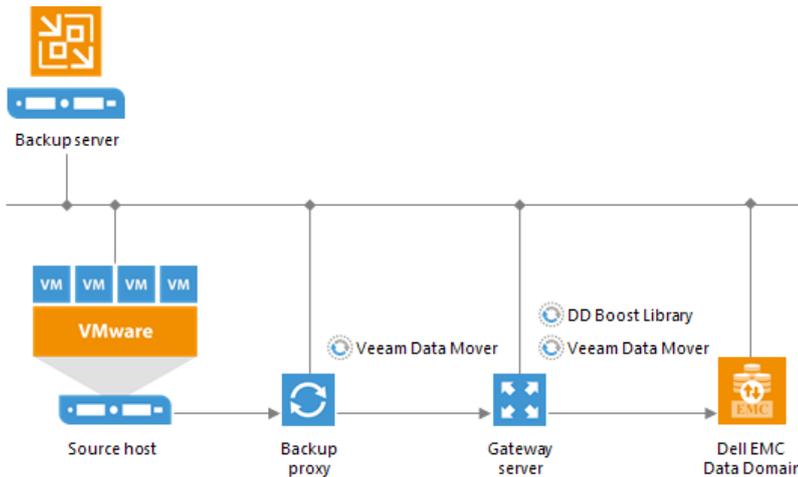
Dell EMC Data Domain Deployment

To communicate with Dell EMC Data Domain, Veeam Backup & Replication uses two Data Mover Services that are responsible for data processing and transfer:

- Veeam Data Mover on the backup proxy
- Veeam Data Mover on the gateway server

The Dell EMC Data Domain storage cannot host Veeam Data Mover Service. For this reason, to communicate with the Dell EMC Data Domain storage, you need to deploy a gateway server. Veeam Backup & Replication will automatically deploy a Veeam Data Mover on this gateway server. For more information, see [Gateway Server](#).

When any job addresses the backup repository, the Data Mover Service on the gateway server establishes a connection with the Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.



You define what gateway server to use when you assign a backup repository role to Dell EMC Data Domain. You can define the gateway server explicitly or instruct Veeam Backup & Replication to select it automatically.

IMPORTANT!

For Dell EMC Data Domain storage systems working over Fibre Channel, you must explicitly define the gateway server that will communicate with Dell EMC Data Domain. As a gateway server, you must use a Microsoft Windows server that is added to the backup infrastructure and has access to Dell EMC Data Domain over Fibre Channel.

Supported Protocols

Veeam Backup & Replication supports Dell EMC Data Domain storage systems working over the following protocols:

- TCP/IP protocol: Veeam Backup & Replication communicates with the Dell EMC Data Domain server by sending commands over the network.
- Fibre Channel protocol: Veeam Backup & Replication communicates with the Dell EMC Data Domain Fibre Channel server by sending SCSI commands over Fibre Channel.

Limitations for Dell EMC Data Domain

If you plan to use Dell EMC Data Domain as a backup repository, mind the following limitations:

- Use of Dell EMC Data Domain with DD Boost does not guarantee improvement of job performance. It reduces the load on the network and improves the network throughput.
- NFS services must be enabled on Dell EMC Data Domain. Otherwise, Veeam Backup & Replication will not be able to access the storage system.
- Dell EMC Data Domain does not support the reverse incremental backup method.
- You cannot use Dell EMC Data Domain backup repositories as sources or targets for file copy jobs.
- When you create a backup job targeted at an Dell EMC Data Domain backup repository, Veeam Backup & Replication will offer you to switch to optimized job settings and use the 4 MB size of data block for VM data processing. It is recommended that you use optimized job settings. Large data blocks produce a smaller metadata table that requires less memory and CPU resources to process.

- The length of forward incremental and forever forward incremental backup chains (chains that contain one full backup and a set of subsequent incremental backups) cannot be greater than 60 restore points. To overcome this limitation, schedule full backups (active or synthetic) to split the backup chain into shorter series. For example, to perform backups at 30-minute intervals 24 hours a day, you must schedule synthetic fulls every day. In this scenario, intervals immediately after midnight may be skipped due to duration of synthetic processing. For more information, see [How Synthetic Full Backup Works](#).
- If you connect to an Dell EMC Data Domain backup repository over Fibre Channel, you must explicitly define a gateway server to communicate with Dell EMC Data Domain. As a gateway server, you must use a Microsoft Windows server that is added to the backup infrastructure and has access to the Dell EMC Data Domain backup repository over Fibre Channel.
- During backup repository rescan, Veeam Backup & Replication detects if the hard stream limit is set for a storage unit, and displays this information in backup repository rescan statistics. If the hard stream limit is exceeded when Veeam Backup & Replication runs tasks against the backup repository, Veeam Backup & Replication will fail to create new I/O streams.

For more information about working with Dell EMC Data Domain, see <https://www.veeam.com/kb1956>.

Dell EMC Data Domain Supported Features

The DD Boost technology offers a set of features for advanced data processing. Veeam Backup & Replication supports the following features:

- [Distributed Segment Processing](#)
- [Advanced Load Balancing and Link Failover](#)
- [Virtual Synthetics](#)

In addition to these technologies, Veeam Backup & Replication supports [in-flight data encryption](#) and [per storage unit streams](#).

NOTE:

You cannot configure Managed File Replication using Veeam Backup & Replication. However, you can import and map backups replicated between Data Domain storage systems to backup, backup copy or replication jobs, or perform restore operations from such backups.

Distributed Segment Processing

Distributed Segment Processing lets Dell EMC Data Domain “distribute” the deduplication process and perform a part of data deduplication operations on the backup proxy side.

Without Distributed Segment Processing, Dell EMC Data Domain performs deduplication on the Dell EMC Data Domain storage system. The backup proxy sends unfiltered data blocks to Dell EMC Data Domain over the network. Data segmentation, filtering and compression operations are performed on the target side, before data is written to disk.

With Distributed Segment Processing, operations on data segmentation, filtering and compression are performed on the backup proxy side. The backup proxy sends only unique data blocks to Dell EMC Data Domain. As a result, the load on the network reduces and the network throughput improves.

Advanced Load Balancing and Link Failover

Advanced Load Balancing and Link Failover allow you to balance data transfer load and route VM data traffic to a working link in case of network outage problems.

Without Advanced Load Balancing, every backup server connects to Data Domain on a dedicated Ethernet link. Such configuration does not provide an ability to balance the data transfer load across the links. If a network error occurs during the data transfer process, the backup job fails and needs to be restarted.

Advanced Load Balancing allows you to aggregate several Ethernet links into one interface group. As a result, Dell EMC Data Domain automatically balances the traffic load coming from several backup servers united in one group. If some link in the group goes down, Dell EMC Data Domain automatically performs link failover, and the backup traffic is routed to a working link.

Virtual Synthetics

Veeam Backup & Replication supports Virtual Synthetic Fulls by Dell EMC Data Domain. Virtual Synthetic Fulls let you synthesize a full backup on the target backup storage without physically copying data from source datastores. To construct a full backup file, Dell EMC Data Domain uses pointers to existing data segments on the target backup storage. Virtual Synthetic Fulls reduce the workload on the network and backup infrastructure components and increase the backup job performance.

In-Flight Data Encryption

Veeam Backup & Replication supports in-flight encryption introduced in Dell EMC Data Domain Boost 3.0. If necessary, you can enable data encryption at the backup repository level. Veeam Backup & Replication will leverage the Dell EMC Data Domain technology to encrypt data transported between the DD Boost library and Data Domain system.

Per Storage Unit Streams

Veeam Backup & Replication supports per storage unit streams on Dell EMC Data Domain. The maximum number of parallel tasks that can be targeted at the backup repository (the **Limit maximum concurrent tasks to N** setting) is applied to the storage unit, not the whole Dell EMC Data Domain system.

Supported Protocols

Veeam Backup & Replication supports Dell EMC Data Domain storage systems working over the following protocols:

- TCP/IP protocol: Veeam Backup & Replication communicates with the Dell EMC Data Domain server by sending commands over the network.
- Fibre Channel protocol: Veeam Backup & Replication communicates with the Dell EMC Data Domain Fibre Channel server by sending SCSI commands over Fibre Channel.

Accelerated Restore of Entire VM

To speed up entire VM restore on Dell EMC Data Domain, Veeam Backup & Replication uses the mechanism of sequential data reading from backups and parallel VM disks restore.

Dell EMC Data Domain storage systems are optimized for sequential I/O operations. However, data blocks of VM disks in backup files are stored not sequentially, but in the random order. If data blocks of VM disks are read at random, the restore performance from backups on Dell EMC Data Domain degrades.

To accelerate the restore process, Veeam Backup & Replication creates a map of data blocks in backup files. It uses the created map to read data blocks of VM disks from backup files sequentially, as they reside on disk. Veeam Backup & Replication writes data blocks to target in the order in which they come from the target Veeam Data Mover, restoring several VM disks in parallel.

This accelerated restore mechanism is enabled by default, and is used for the entire VM restore scenario.

NOTE:

To further accelerate the process of entire VM restore, Veeam Backup & Replication reads VM data from Dell EMC Data Domain in multiple threads.

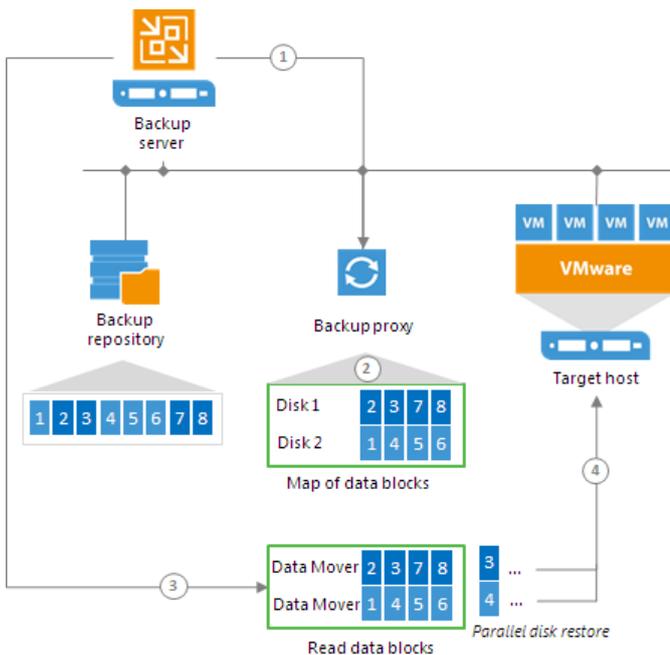
How Accelerated Restore Works

Entire VM restore from backups on Dell EMC Data Domain is performed in the following way:

1. Veeam Backup & Replication opens all backup files in the backup chain, reads metadata from these backup files and caches this metadata on the backup proxy that is assigned for the restore task.
2. Veeam Backup & Replication uses the cached metadata to build a map of data blocks. The map contains references to VM data blocks, sorted by VM disks.
3. Every VM disks is processed in a separate task. For every task, Veeam Backup & Replication starts a separate Veeam Data Mover on the backup proxy.

Veeam Data Movers read data blocks of VM disks from the backup repository sequentially, as these blocks reside on disk, and put read data blocks to the buffer on the backup proxy.

4. Data blocks are written to target in the order in which they come from the target Veeam Data Mover.



Backup Proxy for Accelerated Restore

Veeam Backup & Replication restores all disks of a VM through one backup proxy. If you instruct Veeam Backup & Replication to select a backup proxy for the restore task automatically, it picks the least loaded backup proxy in the backup infrastructure. If you assign a backup proxy explicitly, Veeam Backup & Replication uses the selected backup proxy.

For every VM disk, Veeam Backup & Replication starts a separate Veeam Data Mover on the backup proxy. For example, if you restore a VM with 10 disks, Veeam Backup & Replication starts 10 Veeam Data Movers on the backup proxy.

The backup proxy assigned for the entire VM restore task must have enough RAM resources to be able to restore VM disks in parallel. For every VM disk, 200 MB of RAM is required. The total amount of required RAM resources is calculated by the following formula:

```
Total amount of RAM = Number of VM disks * 200 MB
```

Before starting the restore process, Veeam Backup & Replication checks the amount of RAM resources on the backup proxy. If the backup proxy does not have enough RAM resources, Veeam Backup & Replication displays a warning in the job session details and automatically fails over to a regular VM disks processing mode (data of VM disks is read at random and VM disks are restored sequentially).

Limitations for Accelerated Restore

The accelerated restore of entire VM has the following limitations:

- Accelerated restore works on Dell EMC Data Domain systems with DD Boost.
- If you restore a VM with dynamically expanding disks, the restore process may be slow.
- If you restore a VM using the Network transport mode, the number of VM disks restored in parallel cannot exceed the number of allowed connections to an ESXi host. For more information, see <https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkDataStruct.5.5.html>.
- If Dell EMC Data Domain is added as an extent to a scale-out backup repository, you must set the backup file placement policy to Locality. If the backup file placement policy is set to Performance, parallel VM disk restore will be disabled.

ExaGrid

You can use ExaGrid appliances as backup repositories.

Adaptive Deduplication

ExaGrid uses adaptive deduplication. Data deduplication is performed on the target storage system. After VM data is written to disk, ExaGrid analyses bytes in the newly transferred data portions. ExaGrid compares versions of data over time and stores only the differences to disk.

ExaGrid deduplicates data at the storage level. Identical data is detected throughout the whole storage system, which increases the deduplication ratio.

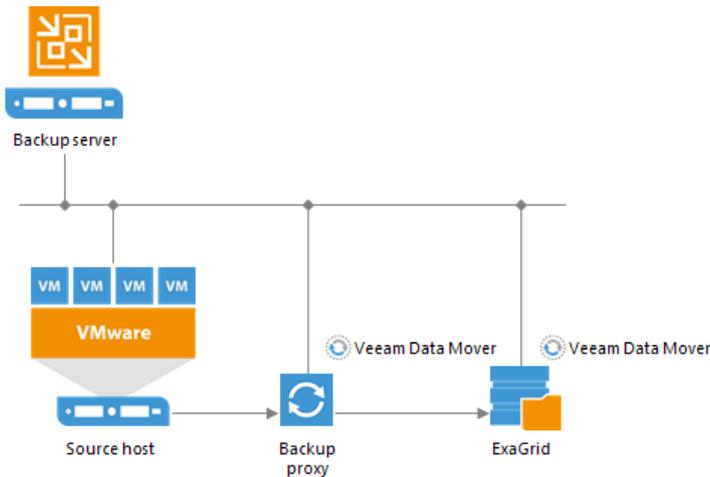
ExaGrid Deployment

To communicate with ExaGrid, Veeam Backup & Replication uses two Data Mover Services that are responsible for data processing and transfer:

- Veeam Data Mover on the backup proxy
- Veeam Data Mover on the ExaGrid appliance

ExaGrid does not host the Veeam Data Mover permanently. When any task addresses an ExaGrid storage, Veeam Backup & Replication deploys and starts the Veeam Data Mover on the ExaGrid appliance.

The Data Mover Service establishes a connection with the Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.



Requirements and Recommendations for ExaGrid

To perform backup to ExaGrid appliances, it is recommended to configure backup repositories and jobs in the following way:

Backup repositories

Configure ExaGrid backup repositories in the following way:

1. Create at least one share on each ExaGrid appliance. Enable the **ExaGrid-Veeam Accelerated Data Mover transport** option for the created share. Leave default compression and deduplication settings for the share.
2. In Veeam Backup & Replication, perform the following actions:
 - a. Configure ExaGrid backup repositories and point them at the created shares on each ExaGrid appliance. Set the **Limit maximum concurrent tasks to N** option to 10 tasks. This limit can be tuned up or down with assistance from ExaGrid Customer Support.
 - b. Add ExaGrid backup repositories as extents to a scale-out backup repository.

Backup Jobs

Configure backup jobs in the following way:

1. Backup job settings:
 - a. Use the forward incremental backup method.
 - b. Enable synthetic full backups and schedule them to run on a weekly basis.
 - c. Enable active full backups and schedule them to run on a monthly basis.
2. Backup target: Assign backup jobs to the scale-out backup repository with ExaGrid appliances as extents.

NOTE:

Do not create multiple backup repositories directed at the same folder/path on the same device.

For more information and recommendations on working with ExaGrid appliances, see the [Veeam KB2056](#) article.

HPE StoreOnce

You can use HPE StoreOnce storage appliances as backup repositories.

To work with HPE StoreOnce, Veeam Backup & Replication leverages the HPE StoreOnce Catalyst technology and two HPE StoreOnce components:

- **HPE StoreOnce Catalyst agent.** The HPE StoreOnce Catalyst agent is a component of the HPE StoreOnce Catalyst software. The HPE StoreOnce Catalyst agent is embedded into the Veeam Data Mover Service setup. When you add a Microsoft Windows server to the backup infrastructure, the HPE StoreOnce Catalyst agent is automatically installed on the added server together with the Data Mover Service.
- **HPE StoreOnce appliance.** The HPE StoreOnce appliance is an HPE StoreOnce storage system on which Catalyst stores are created.

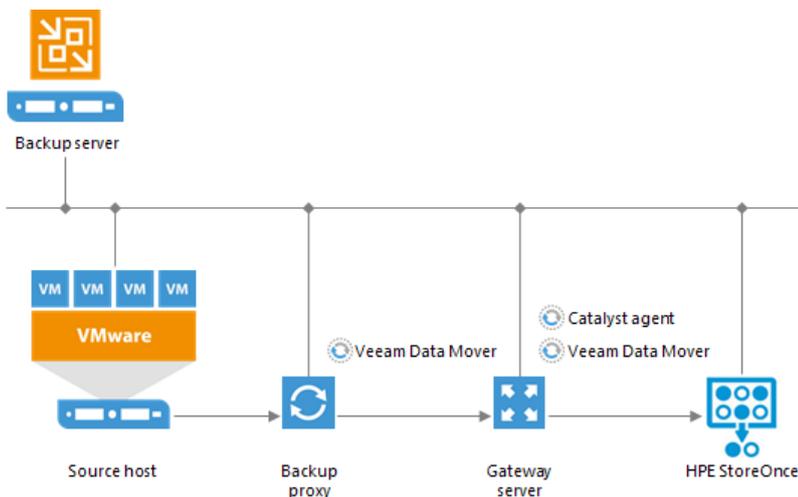
HPE StoreOnce Deployment

To communicate with HPE StoreOnce, Veeam Backup & Replication uses two Data Mover Services that are responsible for data processing and transfer:

- Veeam Data Mover on the backup proxy
- Veeam Data Mover on the gateway server

The HPE StoreOnce storage cannot host Veeam Data Mover Service. For this reason, to communicate with the HPE StoreOnce storage, you need to deploy a gateway server. Veeam Backup & Replication will automatically deploy a Veeam Data Mover on this gateway server. For more information, see [Gateway Server](#). For communicating with the HPE StoreOnce storage appliances, the gateway server must run a 64-bit Microsoft Windows version.

When any job addresses the backup repository, the Data Mover Service on the gateway server establishes a connection with the Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.



The gateway server is selected when you assign a backup repository role to the HPE StoreOnce appliance. You can define the gateway server explicitly or instruct Veeam Backup & Replication to select it automatically.

TIP:

For work with HPE StoreOnce, Veeam Backup & Replication uses the Catalyst agent installed on the gateway server. If you want to reduce the load on the network between the source and target side, assign the gateway server role to a machine on the source side, closer to the backup proxy.

Limitations for HPE StoreOnce

If you plan to use HPE StoreOnce as a backup repository, mind the following limitations. Limitations apply only if you use HPE StoreOnce in the integration mode, not the shared folder mode.

- When you create a backup job targeted at HPE StoreOnce, Veeam Backup & Replication will offer you to switch to optimized job settings and use the 4 MB size of data block for VM data processing. It is recommended that you use optimized job settings. Large data blocks produce a smaller metadata table that requires less memory and CPU resources to process.
- The HPE StoreOnce backup repository always works in the **Use per-VM backup files** mode. For more information, see [Per-VM Backup Files](#).
- HPE StoreOnce does not support the reverse incremental backup method.
- HPE StoreOnce does not support the forever forward incremental backup method. When creating a backup job, you must enable synthetic and/or active full backups. Otherwise, you will not be able to create a backup job.
- The HPE StoreOnce backup repository does not support the **Defragment and compact full backup file** option (for backup and backup copy jobs).
- You cannot use HPE StoreOnce backup repositories as sources or targets for file copy jobs.
- You cannot copy backup files (VBK, VIB and VRB) manually to the HPE StoreOnce backup repository. To copy such files, use backup copy jobs.
- You cannot use the HPE StoreOnce backup repository as a cloud repository.
- You cannot target Veeam Agent backup jobs at the HPE StoreOnce backup repository in the integration mode. However, you can target such jobs at the HPE StoreOnce repository added to the backup infrastructure as a CIFS share.
- HPE StoreOnce has a limit on the number of concurrently opened files. Due to this limit, the maximum length of backup chains (chains that contain one full backup and a set of subsequent incremental backups) on HPE StoreOnce is also limited and depends on the particular storage model:

Product	Maximum number of restore points per backup chain
VSA	
VSA Gen3	7
VSA Gen4	7 to 14 (for version 4.1.1 varies depending on the amount of available memory)
Proliant Gen7	
6200	14 (per node)

Proliant Gen8	
2700	7
2900	14
4500	14
4700	14
4900	28
6500	28 (per node)
Proliant Gen9	
3100	7
3500	14
5100	21
5500	35
6600	42 (per node)
Proliant Gen10	
3620	14
3640	14
5200	28
5250	28
5650	42

Several Backup Repositories on HPE StoreOnce

You can configure several backup repositories on one HPE StoreOnce appliance and associate them with different gateway servers.

Mind the following:

- If you configure several backup repositories on HPE StoreOnce and add them as extents to a scale-out backup repository, make sure that all backup files from one backup chain are stored on one extent. If backup files from one backup chain are stored to different extents, the transform operations performance will be lower. For more information about transform operations performance, see <https://www.veeam.com/blog/hp-storeonce-catalyst-integration-coming-in-v9.html>.

- HPE StoreOnce has a limit on the number of opened files that applies to the whole appliance. Tasks targeted at different backup repositories on HPE StoreOnce and run in parallel will equally share this limit.
- For HPE StoreOnce working over Fibre Channel, there is a limitation on the number of connections from one host. If you connect several backup repositories to one gateway, backup repositories will compete for connections.
- Deduplication on HPE StoreOnce works within the limits of one object store.

Operational Modes

Depending on the storage configuration and type of the backup target, HPE StoreOnce can work in the following modes:

- [Source-side deduplication](#)
- [Target-side deduplication](#)
- [Shared folder mode](#)

Source-Side Data Deduplication

HPE StoreOnce performs source-side deduplication if the backup target meets the following requirements:

- You have a Catalyst license installed on HPE StoreOnce.
- You use a Catalyst store as a backup repository.
- The Catalyst store is configured to work in the Low Bandwidth mode (Primary Transfer Policy).
- The HPE StoreOnce Catalyst is added to the backup repository as a deduplicating storage appliance, not as a shared folder.

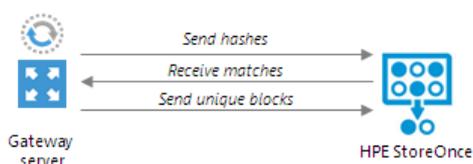
To deduplicate data on the source side, HPE StoreOnce uses the HPE StoreOnce Catalyst agent. The HPE StoreOnce Catalyst agent is a component of the HPE StoreOnce Catalyst software. It is installed on the gateway server communicating with the HPE StoreOnce appliance.

HPE StoreOnce deduplicates data on the source side, before writing it to target:

1. During the backup job session, HPE StoreOnce analyzes data incoming to the HPE StoreOnce appliance in chunks and computes a hash value for every data chunk. Hash values are stored in an index on disk.
2. The HPE StoreOnce Catalyst agent calculates hash values for data chunks in a new data flow and sends these hash values to target.
3. HPE StoreOnce identifies which data blocks are already saved on disk and communicates this information to the HPE StoreOnce Catalyst agent. The HPE StoreOnce Catalyst agent sends only unique data blocks to target.

As a result, the load on the network reduces, the backup job performance improves, and you can save on disk space.

Catalyst agent



Target-Side Data Deduplication

HPE StoreOnce performs target-side deduplication if the backup target is configured in the following way:

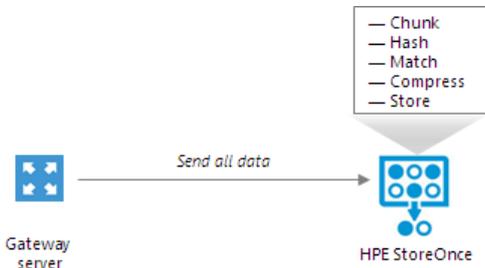
- For a Catalyst store:
 - The Catalyst store works in the High Bandwidth mode (Primary Transfer Policy is set to High Bandwidth).
 - The Catalyst license is installed on the HPE StoreOnce (required).
 - The Catalyst store is added to the backup repository as a deduplicating storage appliance, not as a shared folder.
- For a CIFS store:
 - The Catalyst license is not required.
 - The CIFS store is added as a shared folder backup repository to the backup infrastructure.

For more information about working with CIFS stores, see [Shared Folder Mode](#).

HPE StoreOnce deduplicates data on the target side, after the data is transported to HPE StoreOnce:

1. HPE StoreOnce analyzes data incoming to the HPE StoreOnce appliance in chunks and creates a hash value for every data chunk. Hash values are stored in an index on the target side.
2. HPE StoreOnce analyzes VM data transported to target and replaces identical data chunks with references to data chunks that are already saved on disk.

As a result, only new data chunks are written to disk, which helps save on disk space.



Shared Folder Mode

If you do not have an HPE StoreOnce Catalyst license, you can add the HPE StoreOnce appliance as a shared folder backup repository. In this mode, HPE StoreOnce will perform target-side deduplication.

If you work with HPE StoreOnce in the shared folder mode, the performance of backup jobs and transform operations is lower (in comparison with the integration mode, when HPE StoreOnce is added as a deduplicating storage appliance).

HPE StoreOnce Supported Features

The HPE StoreOnce Catalyst technology offers a set of features for advanced data processing. Veeam Backup & Replication supports the following features:

- [Synthetic Full Backups](#)
- [Accelerated vPower-Enabled Operations](#)

- [Accelerated Data Recovery](#)
- [WAN-based Catalyst Store Support](#)

HPE StoreOnce replication is not supported.

Synthetic Full Backups

HP StoreOnce Catalyst improves synthetic full backup file creation and transformation performance. When Veeam Backup & Replication creates or transforms a synthetic full backup, HPE StoreOnce does not physically copy data between the existing backup chain and the target full backup file. Instead, it performs a metadata-only operation – updates pointers to existing data blocks on the storage device. As a result, the operation completes much faster. This mechanism helps improve performance of primary backup jobs and backup copy jobs that are scheduled to create periodic archive full backups (GFS).

Accelerated vPower-Enabled Operations

Integration with HPE StoreOnce improves performance of vPower-enabled operations – Instant VM Recovery, SureBackup and On-Demand Sandbox – from backups residing on HPE StoreOnce. To benefit from maximum vPower performance, HPE StoreOnce must be running firmware version 3.15.1 or later.

Accelerated Data Recovery

Integration with HPE StoreOnce improves data recovery performance for different restore scenarios: Instant VM Recovery, file-level recovery and application items recovery with Veeam Explorers.

WAN-based Catalyst Store Support

Veeam Backup & Replication provides advanced support for WAN-based HPE Catalyst stores. If a WAN connection to HPE StoreOnce is weak, you can instruct Veeam Backup & Replication to compress VM data and calculate checksums for data blocks going from the source side to HPE StoreOnce.

Supported Protocols

Veeam Backup & Replication supports HPE StoreOnce storage systems working over the following protocols:

- TCP/IP protocol: Veeam Backup & Replication communicates with the HPE StoreOnce appliance by sending commands over the LAN.
- Fibre Channel protocol: Veeam Backup & Replication communicates with the HPE StoreOnce appliance by sending SCSI commands over Fibre Channel.

Data processing over Fibre Channel (FC) connectivity enables local area network-free backup to HP StoreOnce, eliminates the load from backup activities and increases availability of LAN resources to production workloads.

Quantum DXi

You can use Quantum DXi appliances as backup repositories.

Quantum DXi Deduplication

Quantum DXi appliances use Quantum's patented data deduplication technology. During backup data transfer, Quantum analyses blocks in a data stream. Instead of copying redundant data blocks Quantum uses reference pointers to existing blocks on the storage device.

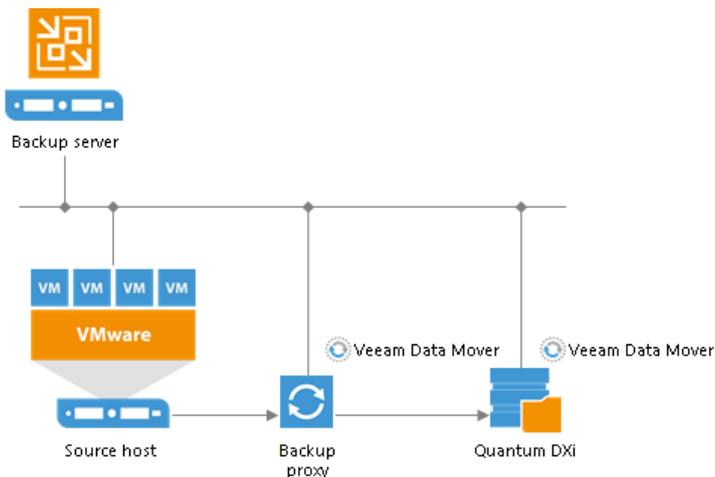
Quantum DXi Deployment

To communicate with Quantum DXi, Veeam Backup & Replication uses two Data Mover Services that are responsible for data processing and transfer:

- Veeam Data Mover on the backup proxy
- Veeam Data Mover on the Quantum DXi appliance

Quantum DXi does not host the Veeam Data Mover permanently. When any task addresses a Quantum DXi storage, Veeam Backup & Replication deploys and starts the Veeam Data Mover on the Quantum DXi system.

The Data Mover Service establishes a connection with the Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.



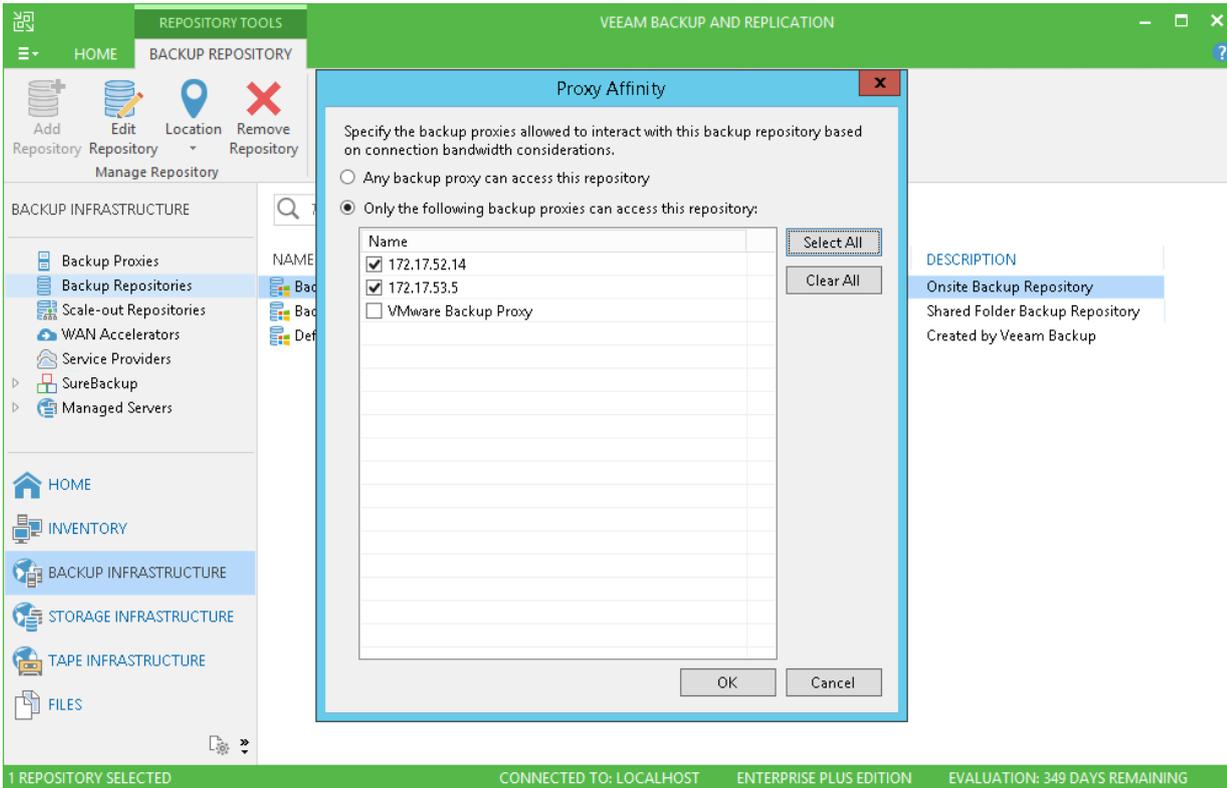
For more information and recommendations on working with Quantum DXi appliances, see <https://www.veeam.com/kb2671>.

Proxy Affinity

By default, Veeam Backup & Replication assigns backup proxies and repositories for jobs or tasks independently of each other. If you need to bind backup proxies to specific backup repositories and use them together, you can define proxy affinity settings. Proxy affinity determines what backup proxies are eligible to access a specific backup repository and read/write data from/to this backup repository.

Proxy affinity lets you control assignment of resources in the backup infrastructure and reduce administration overhead. For example, in case of a geographically distributed infrastructure, you can restrict a backup repository in the local site from communicating with backup proxies in a remote site. Or you can configure proxy affinity rules based on a connection speed between backup proxies and backup repositories.

Proxy affinity settings are specified at the level of a backup repository. By default, Veeam Backup & Replication lets all backup proxies in the backup infrastructure access the backup repository. Using proxy affinity settings, you can define a list of backup proxies that can access this backup repository.



Proxy affinity can be set up for the following types of backup repositories:

- Backup repositories
- Scale-out backup repositories
- Cloud repositories (proxy affinity settings are configured on the tenant side)

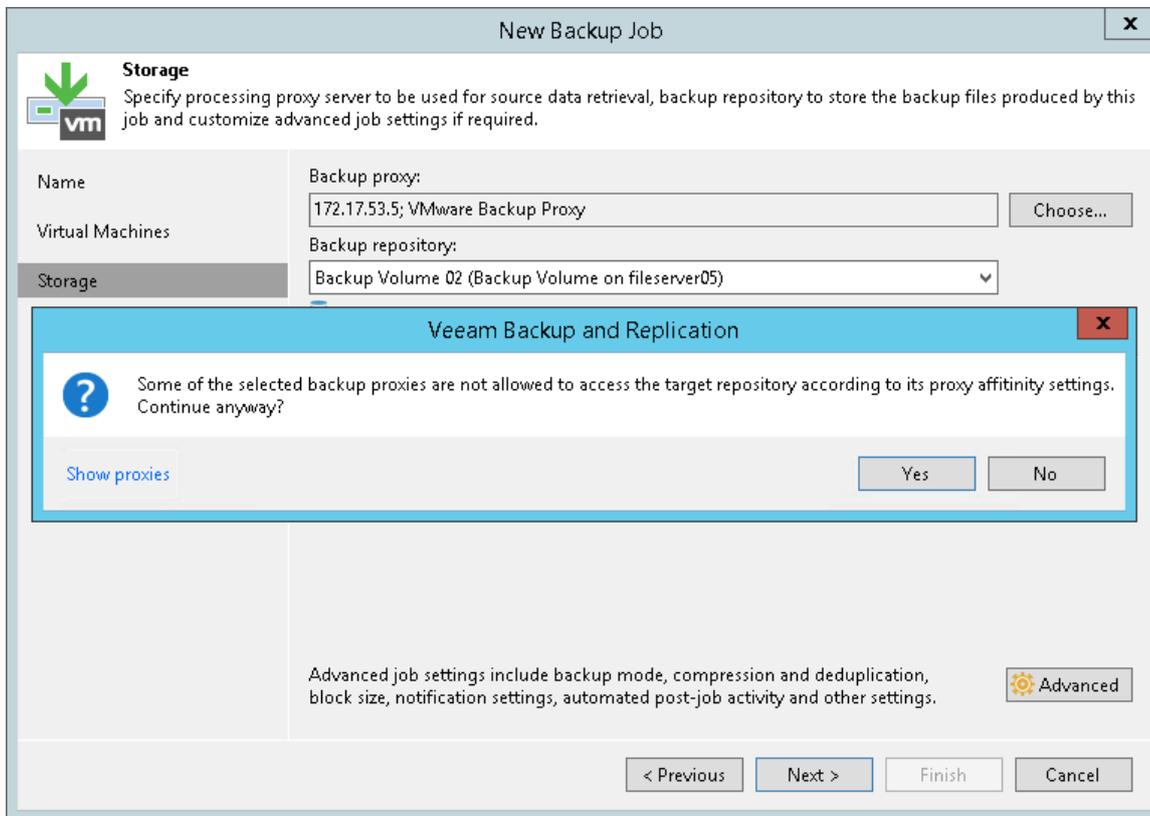
Proxy affinity rules are applied for the following types of jobs and tasks that engage backup proxies and repositories:

- Backup jobs, including VMware vCloud backup and backup jobs from storage snapshots on primary and target storage arrays
- VeeamZIP
- VM copy
- Entire VM restore
- Hard disk restore

Proxy affinity rules are not applied for replication jobs.

Proxy affinity rules are not restrictive. You can think of affinity rules as a priority list. If backup proxies from the proxy affinity list cannot be used for some reason, for example, these backup proxies are inaccessible, Veeam Backup & Replication automatically fails over to the regular processing mode. It displays a warning in the job or task session and picks the most appropriate backup proxy from the list of proxies selected for the job or task.

When you target a job at a backup repository for which proxy affinity settings are configured, you must make sure that you assign a backup proxy from the proxy affinity list for job or task processing. If you assign a backup proxy that is not bound to this backup repository, Veeam Backup & Replication will display a warning. For job processing, Veeam Backup & Replication will use the backup proxy that you define in the job settings, which may result in degraded job performance.



Proxy Affinity for Scale-Out Backup Repositories

In case of a scale-out backup repository, you can configure proxy affinity settings at the extent level. Proxy affinity settings cannot be configured at the scale-out backup repository level.

Extent selection rules have a higher priority than proxy affinity rules. Veeam Backup & Replication first selects an extent and then picks a backup proxy according to the proxy affinity rules specified for this extent.

For example, you have 2 backup proxies: *Backup Proxy 1* and *Backup Proxy 2*. You create a backup job and target it at a scale-out backup repository configured in the following way:

- Scale-out backup repository policy is set to Data Locality.
- Scale-out backup repository has 2 extents: *Extent 1* has 100 GB of free space and is bound to *Backup Proxy 1*; *Extent 2* has 1 TB of free space and is bound to *Backup Proxy 2*.

In the backup job settings, you define that *Backup Proxy 1* must be used for job processing.

When you run the backup job, Veeam Backup & Replication will store backup files to *Extent 2* since it has more free space. For job processing, it will pick *Backup Proxy 1* and will display a message in the job statistics that requirements of proxy affinity rules cannot be met.

In case of restore from a scale-out backup repository, backup files may be located on different extents. In this case, Veeam Backup & Replication picks a backup proxy according to the following priority rules (starting from the most preferable one):

1. Backup proxy is added to the affinity list for all extents.

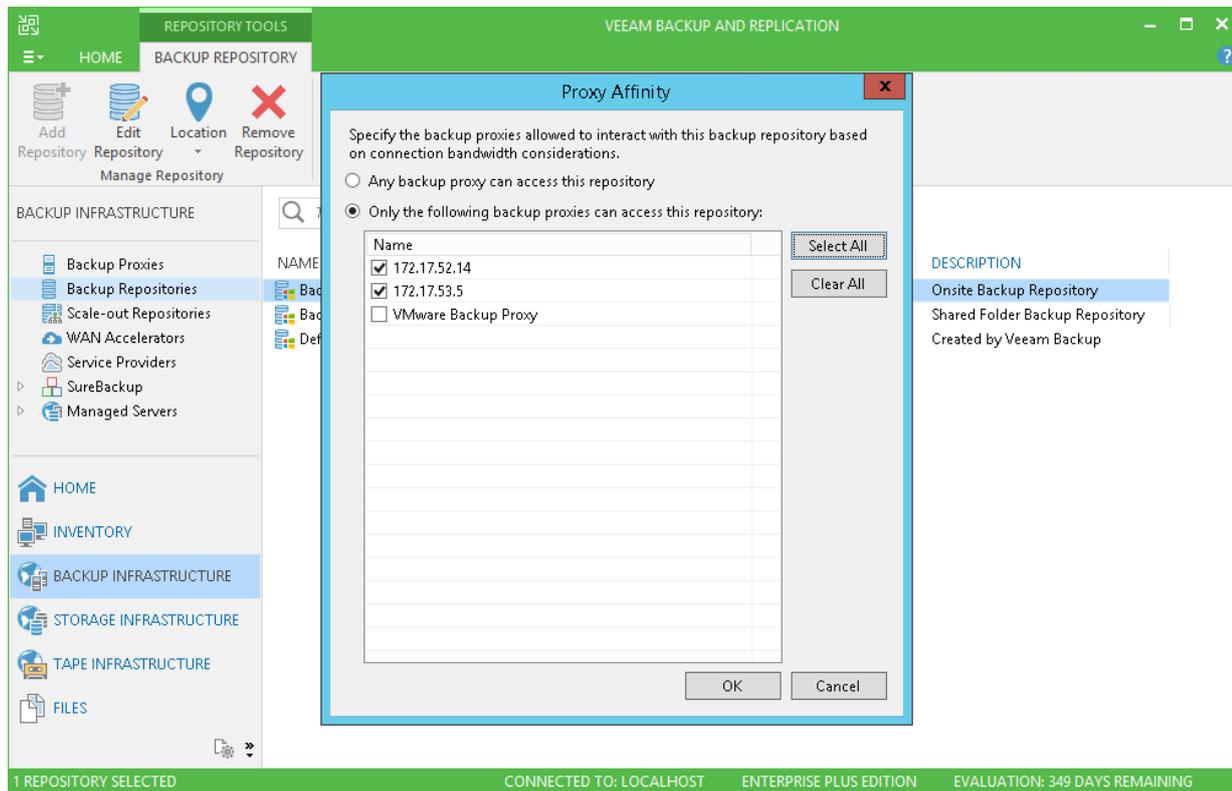
2. Backup proxy is added to the affinity list for the extent where the full backup file is stored.
3. Backup proxy is added to the affinity list for at least one extent.

Specifying Proxy Affinity Settings

For every backup repository, you can configure proxy affinity settings – define a list of backup proxies that can work with this backup repository. Proxy affinity binds backup proxies to specific backup repositories. When transporting data to/from the backup repository, Veeam Backup & Replication picks a backup proxy from the proxy affinity list rather than backup proxies specified in job or task settings.

To configure a proxy affinity list for a backup repository:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Backup Repositories**.
3. In the working area, select the backup repository and click **Proxy Affinity** on the ribbon or right-click the backup repository and select **Proxy affinity**.
4. In the **Proxy Affinity** window, select **Only the following backup proxies can access this repository** and select check boxes next to backup proxies that you want to bind to the backup repository.



Fast Clone

To enhance synthetic operations on Microsoft Windows and shared folder backup repositories, Veeam Backup & Replication uses the Fast Clone technology. Fast Clone lets you create synthetic full backups and GFS backups without moving data blocks between files. Instead, Veeam Backup & Replication leverages the spaceless full backup technology and references data blocks that are already present on the volume. Fast Clone increases the speed of synthetic backup creation and transformation, reduces disk space requirements and load on the storage devices.

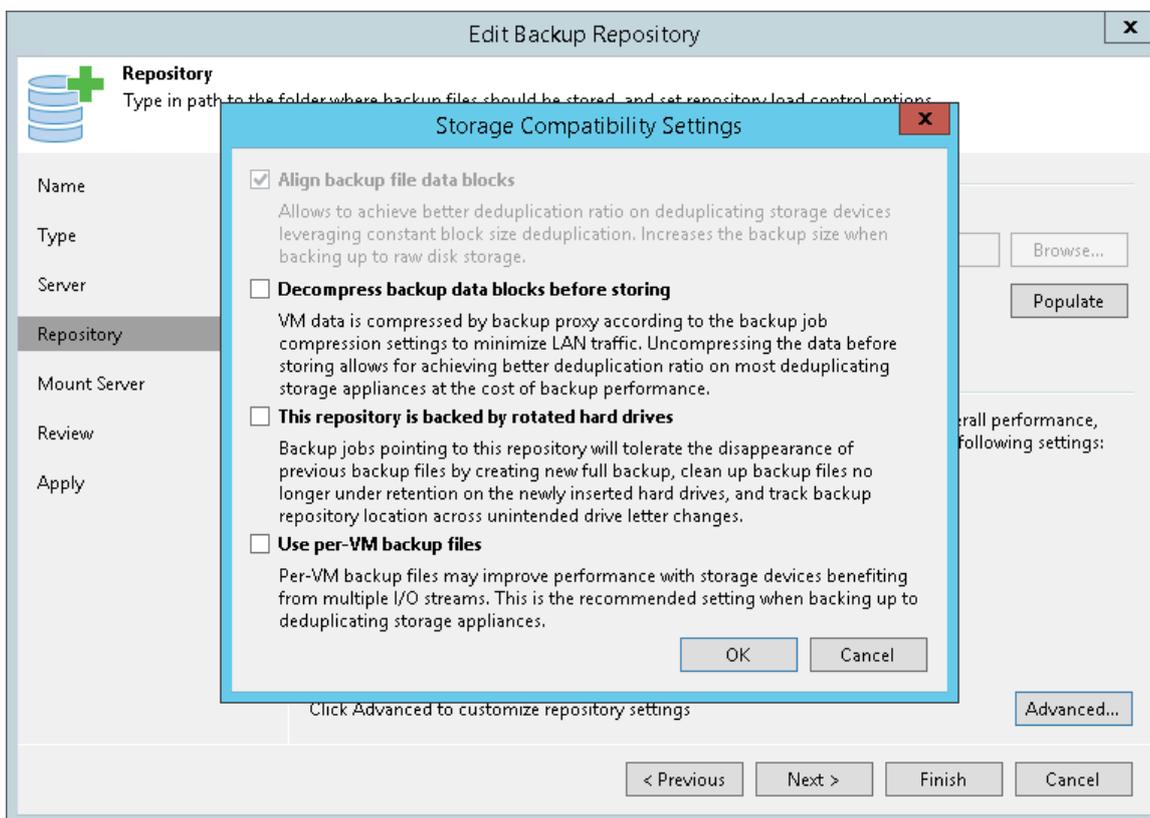
Fast Clone is based on block cloning. Block cloning is Microsoft functionality available on ReFS 3.0. Block cloning allows applications to quickly copy data blocks between different files or within the limits of one file. When an application needs to copy data, the file system does not physically copy data on the underlying storage. Instead, it performs a low-cost metadata operation – it 'projects' data blocks from one region on the ReFS volume to another one.

Block cloning increases data copying performance as the file system does not need to read/write data from/to the underlying storage. It also helps reduce the amount of redundant data. For more information, see [Microsoft Docs](#).

Backup Repository Configuration

To configure a backup repository with Fast Clone support, you must use the repository that resides on Microsoft Windows 2016 Server (and later), Microsoft Windows 10 Pro for Workstations, or shared folder SMB 3.11. Veeam Backup & Replication automatically detects if the server or shared folder meets the specified requirements and if Fast Clone can be used for work with data stored on this backup repository.

Fast Clone requires that the starting and ending file offsets are aligned to cluster boundaries. For this reason, Veeam Backup & Replication automatically enables the **Align backup file data blocks** option for backup repositories that support Fast Clone. Data blocks are aligned at a 4KB or 64 KB block boundary, depending on the volume configuration.



Veeam Backup & Replication supports Fast Clone on all types of backup repositories: simple, scale-out and cloud. Fast Clone works on backup repositories that meet the following requirements:

Microsoft Windows Backup Repository

- OS: Microsoft Windows 2016 Server (and later), Microsoft Windows 10 Pro for Workstations
- File system: ReFS 3.x

Shared Folder Backup Repository

Type of Job/Task	Requirements to backup infrastructure components
Backup job	<p>Protocol: SMB 3.11</p> <p>OS: Microsoft Windows 2016 (and later) or Microsoft Windows 10 Pro for Workstations on the following backup infrastructure components:</p> <ul style="list-style-type: none">• Manual gateway selection: Gateway server.• Automatic gateway selection: Mount server associated with the backup repository, or backup server. For reverse incremental backup chains, Microsoft Windows 2016 or Windows 10 Pro for Workstations must additionally be installed on backup proxies assigned for the job.
Backup copy job	<p>Protocol: SMB 3.11</p> <p>OS: Microsoft Windows 2016 (and later) or Microsoft Windows 10 Pro for Workstations on the following backup infrastructure components:</p> <ul style="list-style-type: none">• Manual gateway selection: Gateway server.• Automatic gateway selection: [For direct data transport path] Mount server associated with the backup repository, or backup server. [For data transport path over WAN accelerators] Microsoft Windows 2016 (and later) or Microsoft Windows 10 Pro for Workstations on the target WAN accelerator.

Mind the following:

- Due to Microsoft limitations, all backup files in the backup chain must be stored on the same volume. For more information, see Restrictions and Remarks at [Microsoft Docs](#).
- By default, Veeam Backup & Replication uses Fast Clone for all backup repositories that meet the specified requirements. You can disable this option with a registry key. For more information, contact Veeam Customer Support.

Operations with Fast Clone

Veeam Backup & Replication leverages Fast Clone for the following synthetic operations:

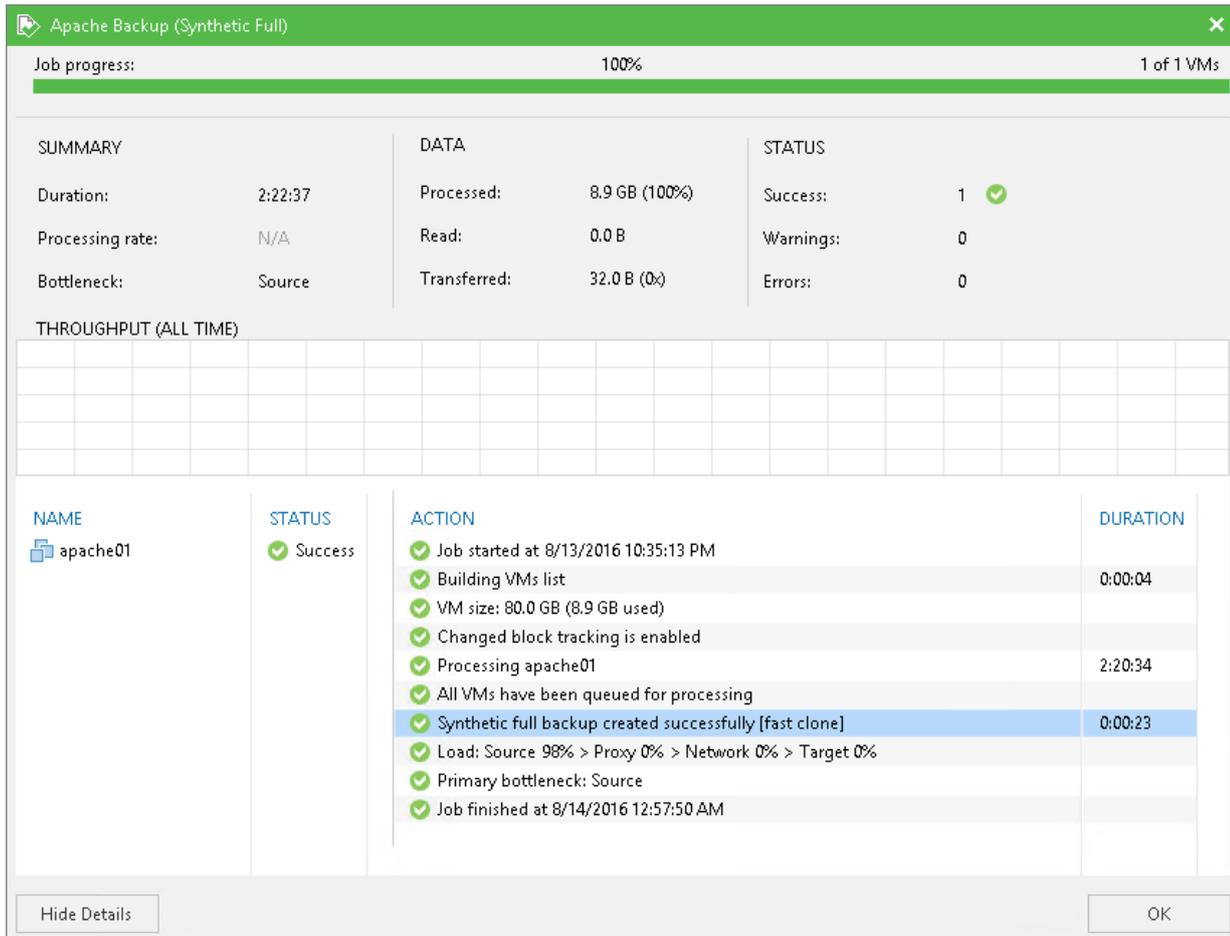
In backup jobs:

- Merge of backup files
- Synthetic full backup
- Reverse incremental backup transformation
- Compact of full backup file

In backup copy job:

- Merge of backup files
- Creation of GFS backups (synthetic method)
- Compact of full backup file

When Veeam Backup & Replication performs a synthetic operation with Fast Clone, it reports this information to the session details for this operation.



Limitations for Fast Clone

- Veeam Backup & Replication does not use Fast Clone for backup repositories configured with previous versions of the product. After upgrade, such backup repositories will work as backup repositories without Fast Clone support. To leverage Fast Clone, you must remove such backup repositories from the backup infrastructure and add them once again.
- Fast Clone requires that source and destination files are stored on the same ReFS volume. If you add a backup repository with Fast Clone support as an extent to a scale-out backup repository, make sure that you enable the Data Locality placement policy for this scale-out backup repository. If backup files are stored on different extents, Fast Clone will not be used.
- If you move backups to a backup repository with Fast Clone support, you must perform active full backup for all existing backup chains (manually or automatically by schedule). You can also schedule the backup file compact operation instead of active full backup.
- Veeam Backup & Replication enables the **Align backup file data blocks** option for backup repositories with Fast Clone support after backup repositories are created. When you pass through the **New Backup Repository** wizard, the **Align backup file data blocks** check box is not selected by default. You can either select the check box or leave it empty – Veeam Backup & Replication will enable the option anyway.

- When you copy data from a ReFS volume to another location, the file system downloads cloned data blocks. For this reason, copied data occupy more space in the target location than it used to occupy in the source location. This can happen, for example, if you evacuate an extent that supports block cloning from a scale-out backup repository and migrate VM backup data to another extent: copied data will require more space than it originally took.

If you plan to assign the role of a backup repository to Microsoft Windows Server 2016 version 1709 and later or Microsoft Windows 10 Pro for Workstations, mind the following limitations:

- Fast Clone and Windows data deduplication cannot be used simultaneously. Thus, if you target a backup job to a repository supporting Fast Clone and enable Windows data deduplication, the Fast Clone technology will not be used for this job.
- If you target a backup job to a CIFS ReFS repository and enable Windows data deduplication, the job will fail. Veeam Backup & Replication does not support such scenario.

Object Storage Repository

Object storage repositories are part of [Capacity Tier](#) that expands your scale-out backup repository abilities and simplifies offloading existing backup data from your extents directly to cloud-based object storage such as S3 Compatible, Amazon S3, Microsoft Azure Blob Storage, IBM Cloud Object Storage.

Adding Object Storage Repositories

You can add the following types of object storage repositories:

- [S3 Compatible Object Storage](#)
- [Amazon S3 Object Storage](#)
- [Microsoft Azure Object Storage](#)
- [IBM Cloud Object Storage](#)

NOTE:

Consider the following:

- The addition of object storage repositories requires Veeam Backup & Replication Enterprise Edition or higher.
- Make sure to open required ports to communicate with object storage repositories in advance, as described in [Used Ports](#).

Adding S3 Compatible Object Storage

S3 Compatible storage is any device that conforms to the Amazon S3 protocol.

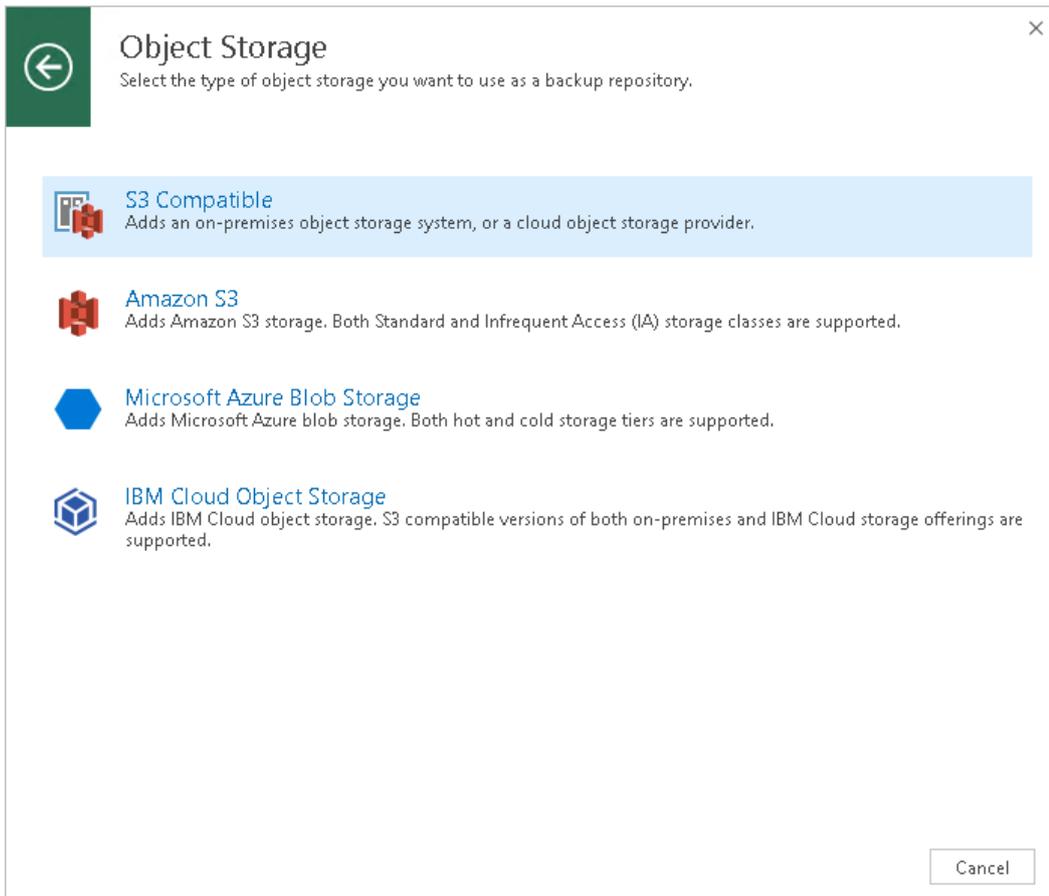
To add S3 Compatible object storage, do the following:

1. [Launch New Object Repository Wizard](#)
2. [Specify Repository Name](#)
3. [Specify Repository Account](#)
4. [Specify Object Storage Settings](#)
5. [Finish Working with Wizard](#)

Step 1. Launch New Object Repository Wizard

To launch the **New Object Repository** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select the **Backup Repositories** node and click **Add Repository** on the ribbon. In the **Add Backup Repository** dialog, select **Object Storage > S3 Compatible**.
- Open the **Backup Infrastructure** view, in the inventory pane right-click the **Backup Repositories** node and select **Add Backup Repository**. In the **Add Backup Repository** dialog, select **Object Storage > S3 Compatible**.



Step 2. Specify Repository Name

At the **Name** step of the wizard, specify a name and optional description for the object storage repository.

The screenshot shows a wizard window titled "New Object Storage Repository". The current step is "Name", which prompts the user to "Type in a name and description for this object storage repository." The left sidebar has "Name" selected. The "Name" field contains "S3-Compatible Object Storage" and the "Description" field contains "Created by EPSILON\Administrator at 11/15/2018 4:35 AM." Navigation buttons at the bottom include "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Repository Account

At the **Account** step of the wizard, specify the following:

1. In the **Service point** field, specify the end-point of your S3 Compatible object storage.
2. In the **Region** field, specify a region.
3. In the **Credentials** drop-down list, select valid user credentials to access your S3 Compatible object storage.

If you already have a credentials record that was configured upfront, select such a record in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in [Cloud Credentials Manager](#).

If your organization uses NAT or different types of firewalls and your access to the internet is limited, you can employ a dedicated gateway server to govern inbound/outbound traffic management. You can use either Windows or Linux machine for this purposes. For more information on how to add such a server to your environment, see [Adding Microsoft Windows Servers](#) and [Adding Linux Servers](#) respectively.

To use a gateway server, select the **Use gateway server** checkbox and choose an appropriate server from the list.

The screenshot shows a window titled "New Object Storage Repository" with a close button in the top right corner. The window is divided into a left sidebar and a main content area. The sidebar has four items: "Name", "Account" (which is selected and highlighted), "Bucket", and "Summary". The main content area has a sub-header "Account" with a sub-instruction "Specify account to use for connecting to S3 compatible storage system." Below this, there are several input fields: "Service point:" with the value "https://172.17.53.37:9000"; "Region:" with the value "us-east-1"; "Credentials:" with a masked password field and an "Add..." button; and a checkbox labeled "Use the following gateway server:" which is checked. Below the checkbox is a dropdown menu with the value "storage1.tech.local". A note below the dropdown reads: "Select a gateway server to proxy access to the object storage system. If no gateway server is specified, all scale-out backup repository extents must have direct network access to the storage". At the bottom of the window are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 4. Specify Object Storage Settings

At the **Bucket** step of the wizard, specify the following:

1. In the **Bucket** drop-down list, select a bucket that contains available folders.
Make sure the bucket you want to use to store your data was created upfront.
2. In the **Folder** field, select a cloud folder to which you want to map your object storage repository and which will be used to store offloaded data. For more information about how data is stored, see [Understanding Object Storage Repository Structure](#).
To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

IMPORTANT!

Never add more than one object storage repository that is mapped to the same cloud folder. Although not prohibited by the system, mapping the same cloud folder to several object storage repositories at the same time leads to unpredictable system behavior and inevitable data loss.

To define a soft limit for your object storage consumption that can be exceeded temporarily, select the **Limit object storage consumption** checkbox and provide the value in TB or PB.

New Object Storage Repository

Bucket
Specify object storage system bucket to use.

Name

Account

Bucket

Summary

Bucket: objectstorage

Folder: Object Storage Repository

Limit object storage consumption to: 10 TB

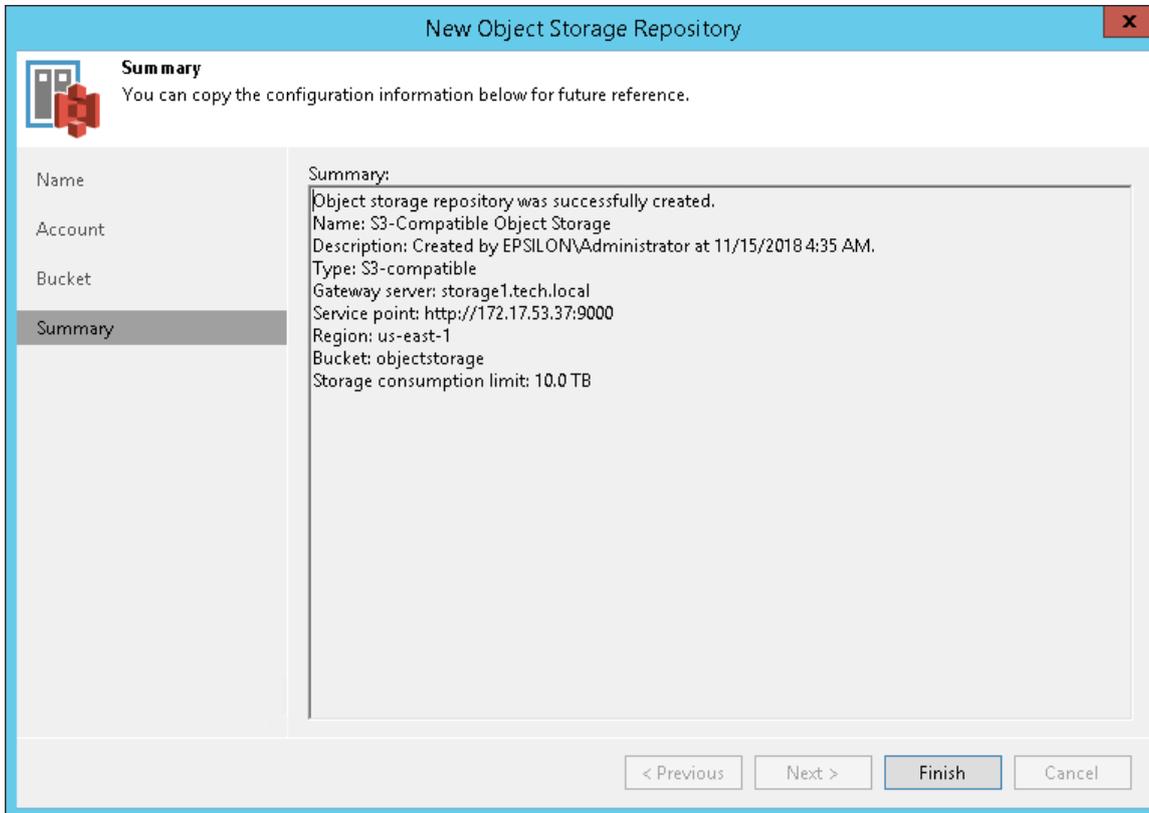
This is a soft limit to help control your cloud storage spend. If the specified limit is exceeded, the already running data tiering tasks will be allowed to complete, but no new tasks will start.

< Previous Next > Finish Cancel

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of object storage repository configuration:

1. Review details of the object storage repository.
2. Click **Finish** to exit the wizard.



Adding Amazon S3 Object Storage

To add Amazon S3 object storage, do the following:

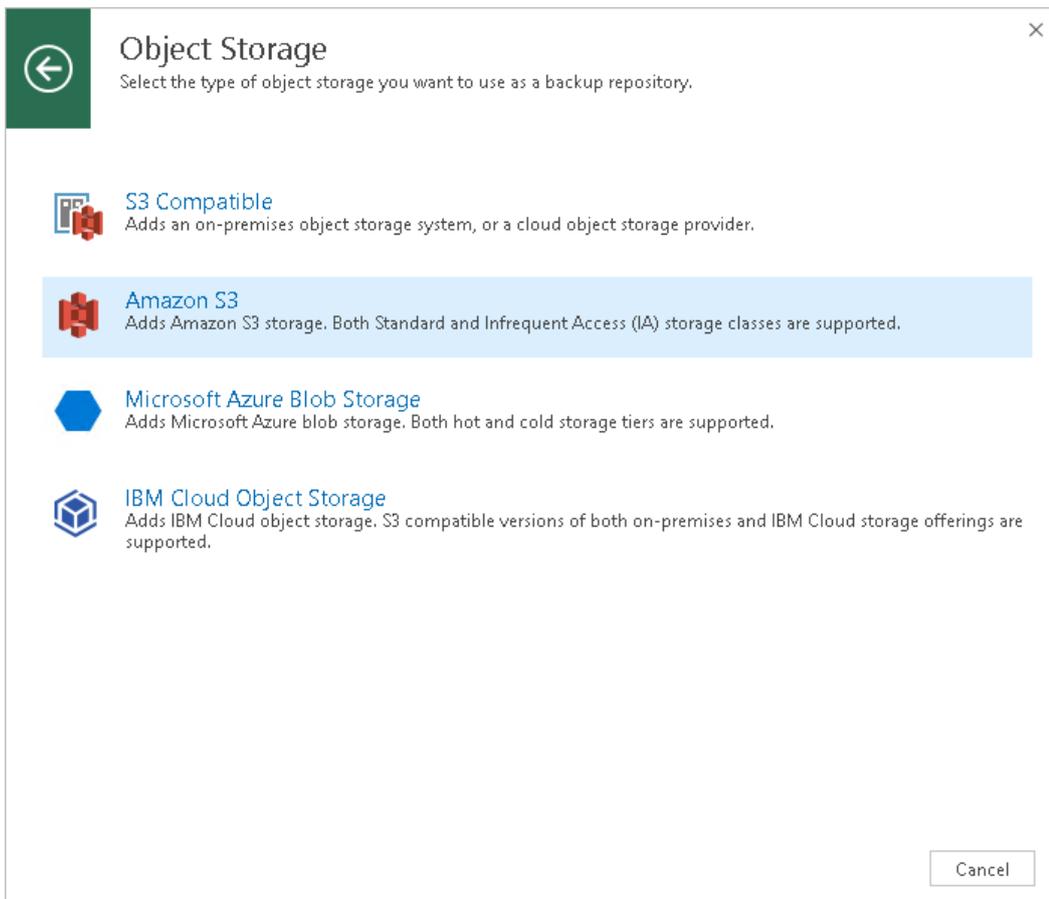
1. [Launch New Object Repository Wizard](#)
2. [Specify Repository Name](#)
3. [Specify Repository Account](#)
4. [Specify Object Storage Settings](#)
5. [Finish Working with Wizard](#)

Step 1. Launch New Object Repository Wizard

To launch the **New Object Repository** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select the **Backup Repositories** node and click **Add Repository** on the ribbon. In the **Add Backup Repository** dialog, select **Object Storage > Amazon S3**.

- Open the **Backup Infrastructure** view, in the inventory pane right-click the **Backup Repositories** node and select **Add Backup Repository**. In the **Add Backup Repository** dialog, select **Object Storage > Amazon S3**.



Step 2. Specify Repository Name

At the **Name** step of the wizard, specify a name and optional description for the object storage repository.

The screenshot shows a wizard window titled "New Object Storage Repository". The current step is "Name", indicated by a red icon and the heading "Name". Below the heading is the instruction "Type in a name and description for this object storage repository." On the left side, there is a navigation pane with four items: "Name" (selected), "Account", "Bucket", and "Summary". The main area contains two text input fields. The first is labeled "Name:" and contains the text "Amazon Object Storage". The second is labeled "Description:" and contains the text "Created by VM\Administrator at 10/8/2018 4:25 AM." At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Repository Account

At the **Account** step of the wizard, specify the following:

1. In the **Credentials** drop-down list, select valid user credentials to access your Amazon S3 object storage.
If you already have a credentials record that was configured upfront, select such a record in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in [Cloud Credentials Manager](#).
2. In the **Data center region** drop-down list, select a region type.

If your organization uses NAT or different types of firewalls and your access to the internet is limited, you can employ a dedicated gateway server to govern inbound/outbound traffic management. You can use either Windows or Linux machine for this purposes. For more information on how to add such a server to your environment, see [Adding Microsoft Windows Servers](#) and [Adding Linux Servers](#) respectively.

To use a gateway server, select the **Use gateway server** checkbox and choose an appropriate server from the list.

Account
Specify Amazon AWS account to use for connecting to Amazon S3 storage bucket.

Name

Account

Bucket

Summary

Credentials:

XXXXXXXX (last edited: less than a day ago) Add...

[Manage cloud accounts](#)

Data center region:

Global
GovCloud (US)
China

Use the following gateway server:

storage1.tech.local

Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.

< Previous Next > Finish Cancel

Step 4. Specify Object Storage Settings

At the **Bucket** step of the wizard, specify the following:

1. In the **Data center region** drop-down list, select a region that contains available buckets.
2. In the **Bucket** drop-down list, select a bucket that contains available folders.
Make sure the bucket you want to use to store your data was created upfront.
3. In the **Folder** field, select a cloud folder to which you want to map your object storage repository and which will be used to store offloaded data. For more information about how data is stored, see [Understanding Object Storage Repository Structure](#).

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

IMPORTANT!

Never add more than one object storage repository that is mapped to the same cloud folder. Although not prohibited by the system, mapping the same cloud folder to several object storage repositories at the same time leads to unpredictable system behavior and inevitable data loss.

To define a soft limit for your object storage consumption that can be exceeded temporarily, select the **Limit object storage consumption** checkbox and provide the value in TB or PB.

If you plan to access your backup data in an infrequent manner, select the **Enable infrequent access storage class** checkbox to mark each block as *Standard IA* (Standard Infrequent Access). For more information about infrequent access, see [this Amazon article](#).

New Object Storage Repository

Bucket
Specify Amazon S3 bucket to use.

Name

Account

Bucket

Summary

Data center region:
US East (Ohio)

Bucket:
veeam-tw

Folder:
Object Storage

Limit object storage consumption to: 10 TB
This is a soft limit to help control your cloud storage spend. If the specified limit is exceeded, the already running data tiering tasks will be allowed to complete, but no new tasks will start.

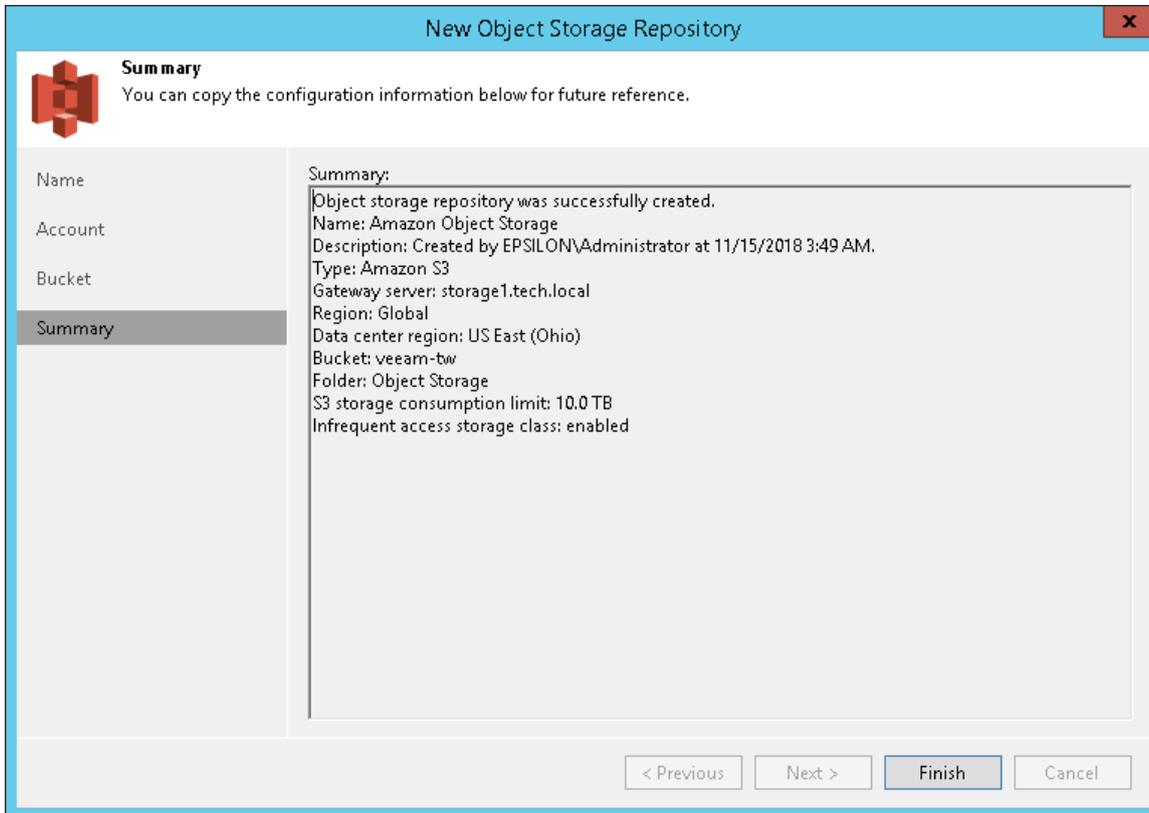
Use infrequent access storage class (may result in additional costs)
Provides lower price per GB at the cost of higher retrieval and early deletion fees, and so is best suited for storing quarterly and yearly backups which you are unlikely to have to restore from.

< Previous Next > Finish Cancel

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of object storage repository configuration:

1. Review details of the object storage repository.
2. Click **Finish** to exit the wizard.



Adding Microsoft Azure Object Storage

To add Microsoft Azure blob storage, do the following:

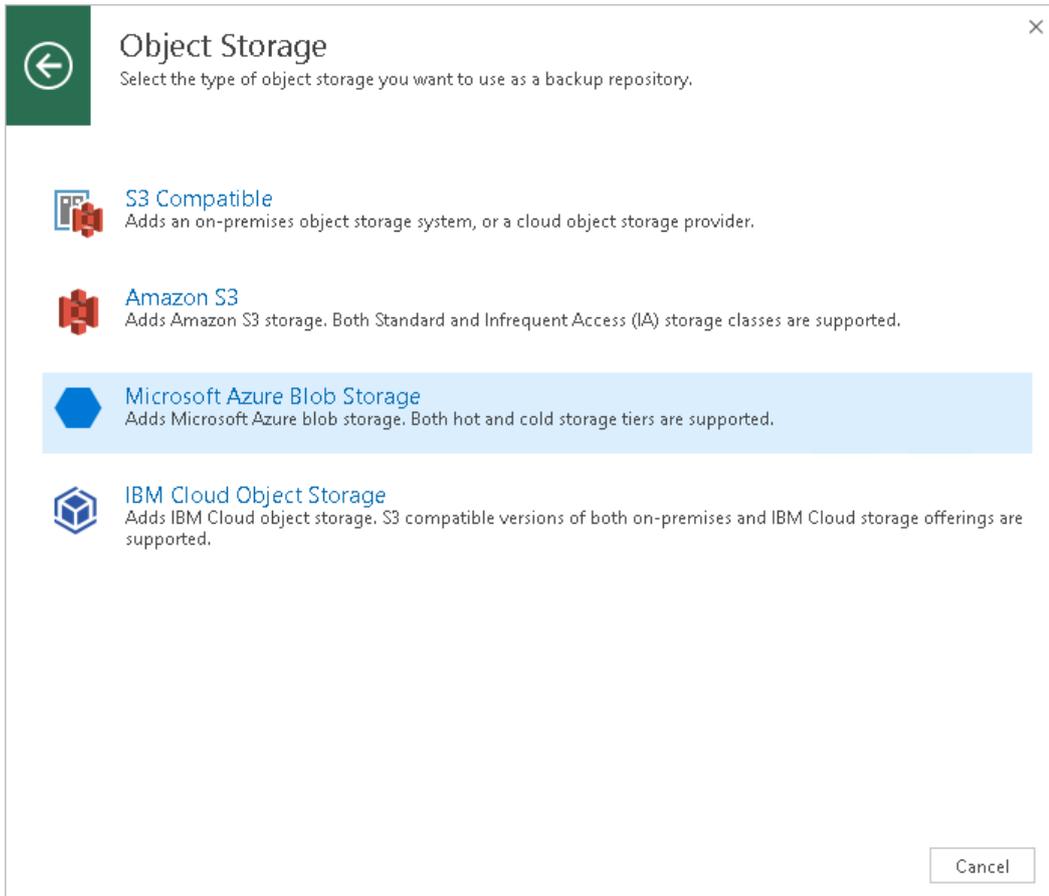
1. [Launch New Object Repository Wizard](#)
2. [Specify Repository Name](#)
3. [Specify Repository Account](#)
4. [Specify Object Storage Settings](#)
5. [Finish Working with Wizard](#)

Step 1. Launch New Object Repository Wizard

To launch the **New Object Repository** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select the **Backup Repositories** node and click **Add Repository** on the ribbon. In the **Add Backup Repository** dialog, select **Object Storage > Microsoft Azure Blob Storage**.

- Open the **Backup Infrastructure** view, in the inventory pane right-click the **Backup Repositories** node and select **Add Backup Repository**. In the **Add Backup Repository** dialog, select **Object Storage > Microsoft Azure Blob Storage**.



Step 2. Specify Repository Name

At the **Name** step of the wizard, specify a name and optional description for the object storage repository.

The screenshot shows a wizard window titled "New Object Storage Repository". The current step is "Name", indicated by a blue hexagon icon and the text "Name" and "Type in a name and description for this object storage repository." The left sidebar has "Name" selected, with "Account", "Container", and "Summary" below it. The main area contains two text input fields: "Name:" with the value "Azure Object Storage" and "Description:" with the value "Created by VM\Administrator at 10/8/2018 4:44 AM.". At the bottom, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Repository Account

At the **Account** step of the wizard, specify the following:

1. In the **Credentials** drop-down list, select valid user credentials to access your Azure Blob storage.
If you already have a credentials record that was configured upfront, select such a record in the drop-down list. Otherwise, click **Add** and provide your account name and a shared key. For more information about supported account types, see [Microsoft Azure Storage Accounts](#).
2. In the **Region** drop-down list, select an Azure region.

If your organization uses NAT or different types of firewalls and your access to the internet is limited, you can employ a dedicated gateway server to govern inbound/outbound traffic management. You can use either Windows or Linux machine for this purposes. For more information on how to add such a server to your environment, see [Adding Microsoft Windows Servers](#) and [Adding Linux Servers](#) respectively.

To use a gateway server, select the **Use gateway server** checkbox and choose an appropriate server from the list.

The screenshot shows the 'New Object Storage Repository' wizard window, specifically the 'Account' step. The window title is 'New Object Storage Repository'. Below the title bar, there is a blue hexagonal icon and the text 'Account Specify account to use for connecting to Microsoft Azure blob storage.' On the left side, there is a navigation pane with 'Account' selected, and other options like 'Name', 'Container', and 'Summary'. The main area contains the following fields: 'Credentials:' with a dropdown menu showing 'XXXXXXXX (last edited: less than a day ago)' and an 'Add...' button; 'Region:' with a dropdown menu showing 'Azure Global (Standard)' and a list of other regions: 'Azure Global (Standard)', 'Azure Germany', 'Azure China', and 'Azure Government'; a checkbox labeled 'Use the following gateway server:' which is checked, and a dropdown menu showing 'storage1.tech.local'; and a text box with the instruction: 'Select a gateway server to proxy access to Microsoft Azure blob storage. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 4. Specify Object Storage Settings

At the **Container** step of the wizard, specify the following:

1. In the **Container** drop-down list, select an Azure container.
Make sure the container you want to use to store your data was created upfront.

NOTE:

The default *Root* container is not supported. For more information about this container, see [this Microsoft article](#).

2. In the **Folder** field, select a cloud folder to which you want to map your object storage repository and which will be used to store offloaded data. For more information on how data is stored, see [Understanding Object Storage Repository Structure](#).

To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

IMPORTANT!

Never add more than one object storage repository that is mapped to the same cloud folder. Although not prohibited by the system, mapping the same cloud folder to several object storage repositories at the same time leads to unpredictable system behavior and inevitable data loss.

To define a soft limit for your object storage consumption that can be exceeded temporarily, select the **Limit object storage consumption** checkbox and provide the value in TB or PB.

The screenshot shows a wizard window titled "New Object Storage Repository" with a close button (X) in the top right corner. The main area is titled "Container" and contains the instruction "Specify Microsoft Azure blob storage container to use." On the left, there is a navigation pane with four items: "Name", "Account", "Container" (which is selected and highlighted), and "Summary". The main content area has the following fields and controls:

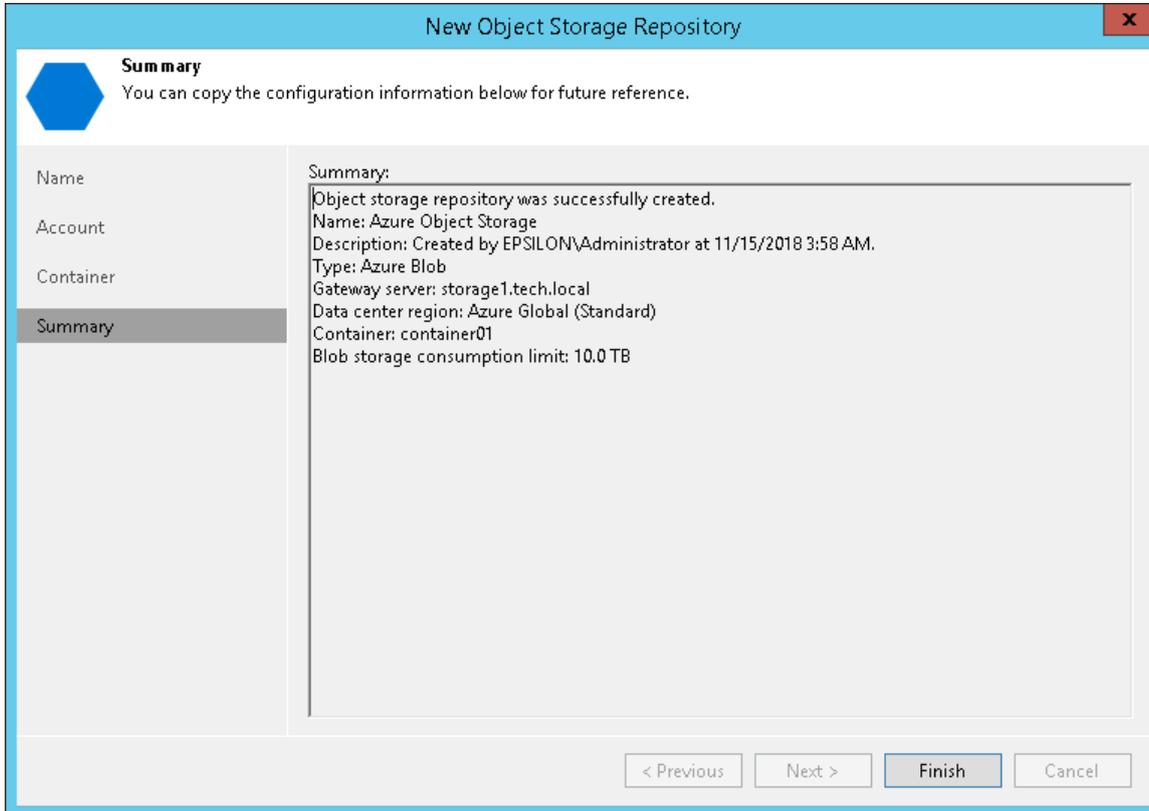
- "Container:" dropdown menu with "container01" selected.
- "Folder:" text input field containing "Object Storage" and a "Browse..." button.
- A checked checkbox labeled "Limit object storage consumption to:" followed by a numeric spinner set to "10" and a unit dropdown menu set to "TB".
- A descriptive text block: "This is a soft limit to help control your cloud storage spend. If the specified limit is exceeded, the already running data tiering tasks will be allowed to complete, but no new tasks will start."

At the bottom of the wizard, 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 object storage repository configuration:

1. Review details of the object storage repository.
2. Click **Finish** to exit the wizard.



Adding IBM Cloud Object Storage

To add IBM cloud object storage, do the following:

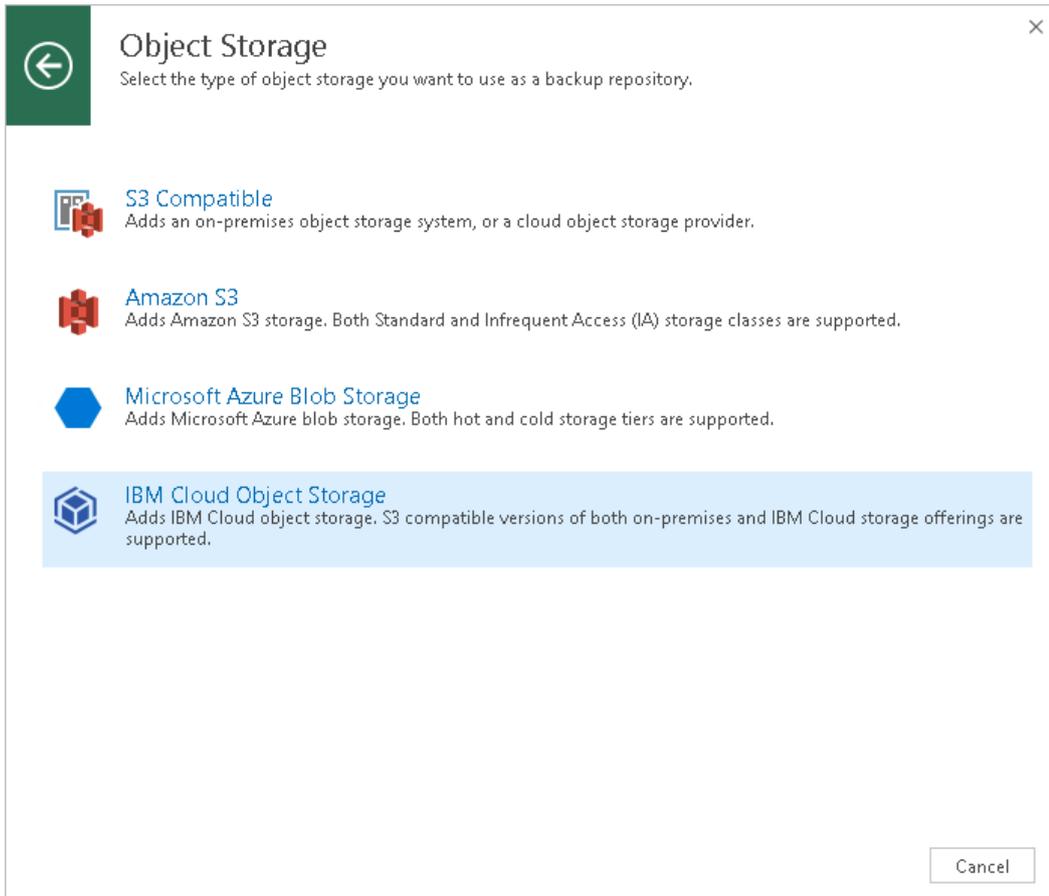
1. [Launch New Object Repository Wizard](#)
2. [Specify Repository Name](#)
3. [Specify Repository Account](#)
4. [Specify Object Storage Settings](#)
5. [Finish Working with Wizard](#)

Step 1. Launch New Object Repository Wizard

To launch the **New Object Repository** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select the **Backup Repositories** node and click **Add Repository** on the ribbon. In the **Add Backup Repository** dialog, select **Object Storage > IBM Cloud Object Storage**.

- Open the **Backup Infrastructure** view, in the inventory pane right-click the **Backup Repositories** node and select **Add Backup Repository**. In the **Add Backup Repository** dialog, select **Object Storage > IBM Cloud Object Storage**.



Step 2. Specify Repository Name

At the **Name** step of the wizard, specify a name and optional description for the object storage repository.

The screenshot shows a wizard window titled "New Object Storage Repository". The current step is "Name", indicated by a blue header and a sidebar on the left. The sidebar lists "Name", "Account", "Bucket", and "Summary", with "Name" selected. The main area contains a "Name:" label and a text box with "IBM Object Storage". Below it is a "Description:" label and a larger text box with "Created by GAMMA\Administrator at 11/22/2018 11:51 PM.". At the bottom right, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Repository Account

At the **Account** step of the wizard, specify the following:

1. In the **Service point** field, specify the end-point of your IBM cloud object storage.
2. In the **Region** field, specify a region.
3. In the **Credentials** drop-down list, select valid user credentials to access your IBM cloud object storage.

If you already have a credentials record that was configured upfront, select such a record in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in [Cloud Credentials Manager](#).

If your organization uses NAT or different types of firewalls and your access to the internet is limited, you can employ a dedicated gateway server to govern inbound/outbound traffic management. You can use either Windows or Linux machine for this purposes. For more information on how to add such a server to your environment, see [Adding Microsoft Windows Servers](#) and [Adding Linux Servers](#) respectively.

To use a gateway server, select the **Use gateway server** checkbox and choose an appropriate server from the list.

Account
Specify account to use for connecting to IBM Cloud Object Storage storage.

Name

Account

Bucket

Summary

Service point:
https://my_service_point.com

Region:
us-east-1

Credentials:
XXXXXXXXXXXXXXXXXX (last edited: less than a day ago) Add...

[Manage cloud accounts](#)

Use the following gateway server:
gamma.tech.local

Select a gateway server to proxy access to the object storage system. If no gateway server is specified, all scale-out backup repository extents must have direct network access to the storage

< Previous Next > Finish Cancel

Step 4. Specify Object Storage Settings

At the **Bucket** step of the wizard, specify the following:

1. In the **Bucket** drop-down list, select a bucket that contains available folders.
Make sure the bucket you want to use was created upfront.
2. In the **Folder** field, select a cloud folder to which you want to map your object storage repository and which will be used to store offloaded data. For more information about how data is stored, see [Understanding Object Storage Repository Structure](#).
To select a folder, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

IMPORTANT!

Never add more than one object storage repository that is mapped to the same cloud folder. Although not prohibited by the system, mapping the same cloud folder to several object storage repositories at the same time leads to unpredictable system behavior and inevitable data loss.

To define a soft limit for your object storage consumption that can be exceeded temporarily, select the **Limit object storage consumption** checkbox and provide the value in TB or PB.

New Object Storage Repository

Bucket
Specify object storage system bucket to use.

Name

Account

Bucket

Summary

Bucket:
b0c4679c-aec0-49f9-b4e1-b7b542b75154

Folder:
TW_Object_Storage

Limit object storage consumption to: 10 TB

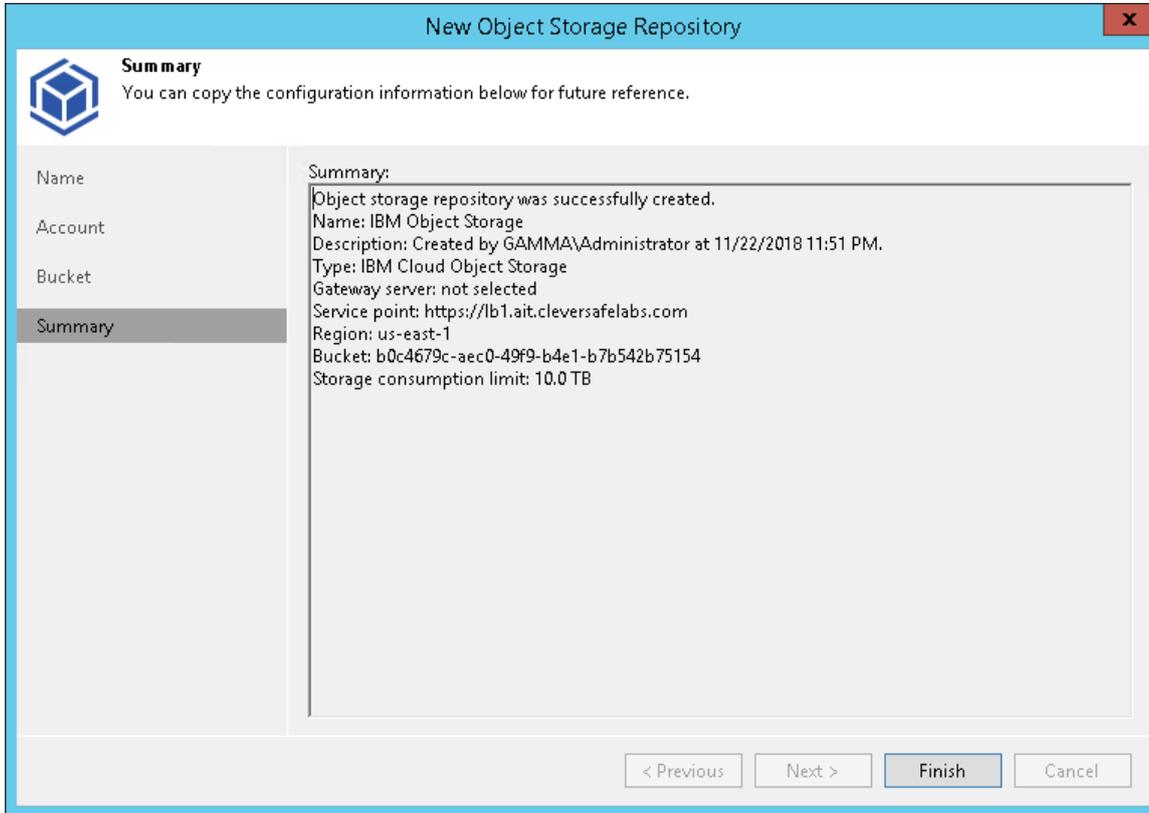
This is a soft limit to help control your cloud storage spend. If the specified limit is exceeded, the already running data offload tasks will be allowed to complete, but no new tasks will start.

< Previous Next > Finish Cancel

Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of object storage repository configuration:

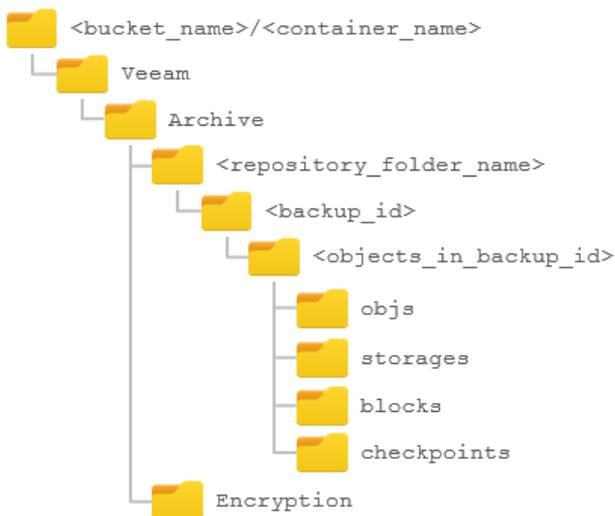
1. Review details of the object storage repository.
2. Click **Finish** to exit the wizard.



Understanding Object Storage Repository Structure

When backup data is being offloaded, Veeam creates and maintains the predefined directory structure in buckets and containers of your object storage repository.

The structure is as follows:



Directory	Description	Misc
<bucket_name> or <container_name>	A bucket or container name. Buckets and containers must be created in advance.	N/A
Veeam/Archive/	Standard folders created by Veeam.	
<repository_folder_name>	A repository folder that you create when adding a new object storage repository.	
<backup_id>	Contains objects in a backup.	These folders will be automatically removed during data removal.
<objects_in_backup_id>	An identifier of an object in a backup. <ul style="list-style-type: none"> If a backup was created using the Per-VM method, then each VM will be placed to its own directory. If a backup was created as a single storage, then all the VMs will be placed to a single directory. 	
objs	Contains meta information.	
storages	Contains a replicated version of offloaded backup files with metadata that also remain on the source extents.	
blocks	Contains offloaded data blocks created by the offload session, as described in Data Transfer .	
checkpoints	Contains meta information about the latest state of the offloaded backup chains. Such meta information is updated upon every successful offload session.	
Encryption	Contains auxiliary system information to work with encrypted backups.	

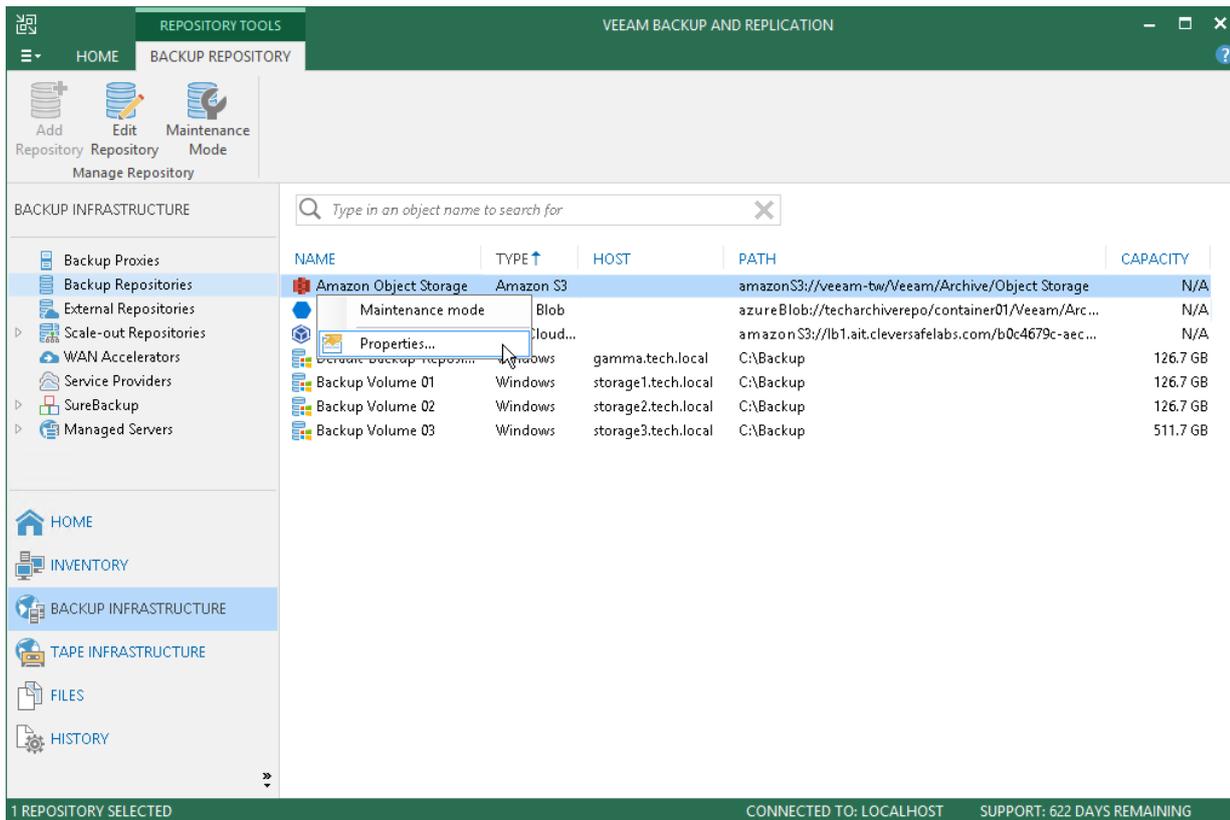
Editing Settings of Object Storage Repository

After you have added an object storage repository, you may want to edit its settings.

To edit object storage settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Backup Repositories**.
3. In the working area, select an object storage repository and click **Edit Repository** on the ribbon or right-click an object storage repository and select **Properties**.

- Follow the steps of the **Edit Object Storage Repository** wizard and edit settings as required. Mind that some settings cannot be modified and will remain disabled while being edited.



Removing Object Storage Repository

You can remove any object storage repository from the application scope if you no longer need it.

Consider the following:

- An object storage repository cannot be removed until it is part of a scale-out backup repository.

In this case, the **Remove** command will be unavailable. To exclude an object storage repository from the scale-out backup repository scope, deselect the **Move backup files to a cheaper storage as they are age out of the operational restores window** checkbox, as described in [Excluding Capacity Tier from Scale-Out Repositories](#).

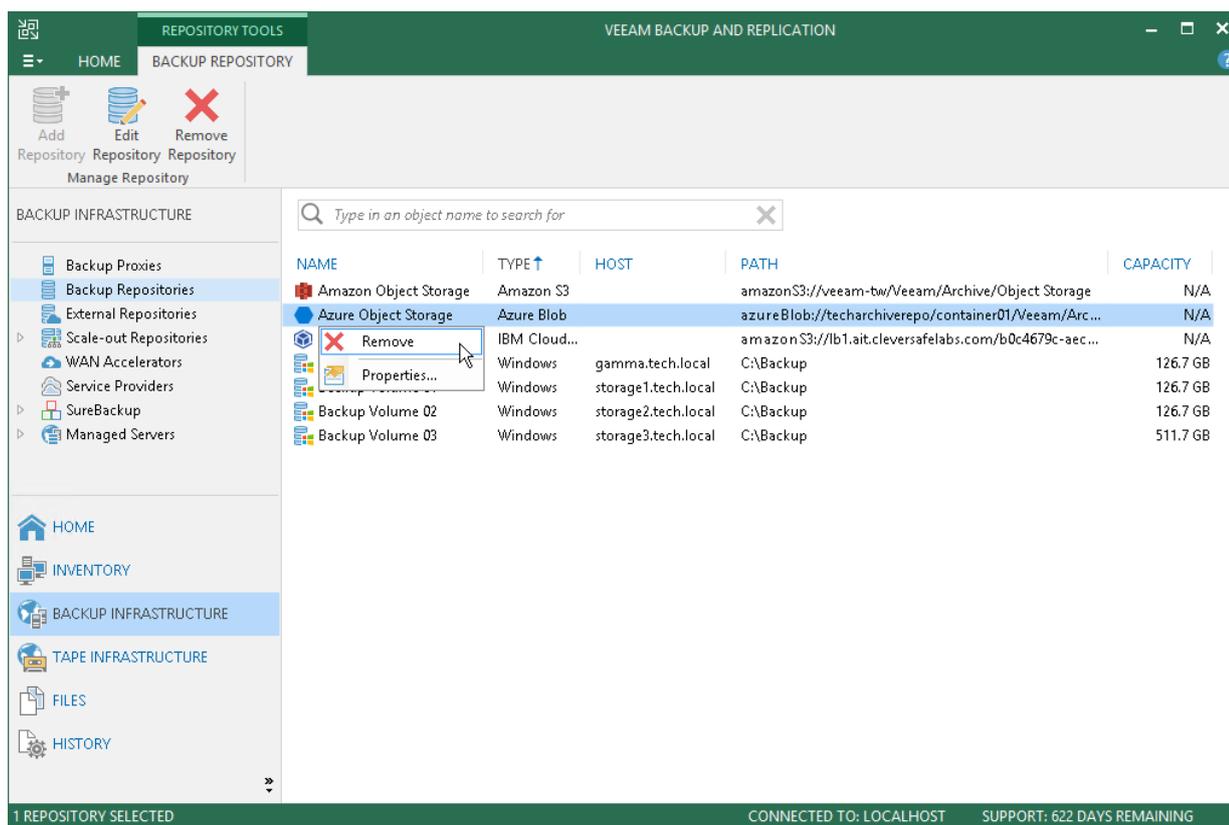
- When an object storage repository is being removed from the environment, the actual offloaded data remains completely unaffected.

To learn how to remove the backup data, see [Removing Backups from Object Storage Repository](#).

To remove an object storage repository, do the following:

- Open the **Backup Infrastructure** view.
- In the inventory pane, select **Backup Repositories**.

3. In the working area, select an object storage repository and click **Remove Repository** on the ribbon or right-click an object storage repository and select **Remove**.



Switching to Maintenance Mode

Maintenance mode imposes limitations on usage of object storage repositories, as described in [Maintenance Mode Limitations](#).

Consider the following:

- An object storage repository can only be put into maintenance mode until it is a member of a scale-out backup repository.

If an object storage repository was not added as part of any of your scale-out backup repositories, then the **Maintenance mode** option will not be available.

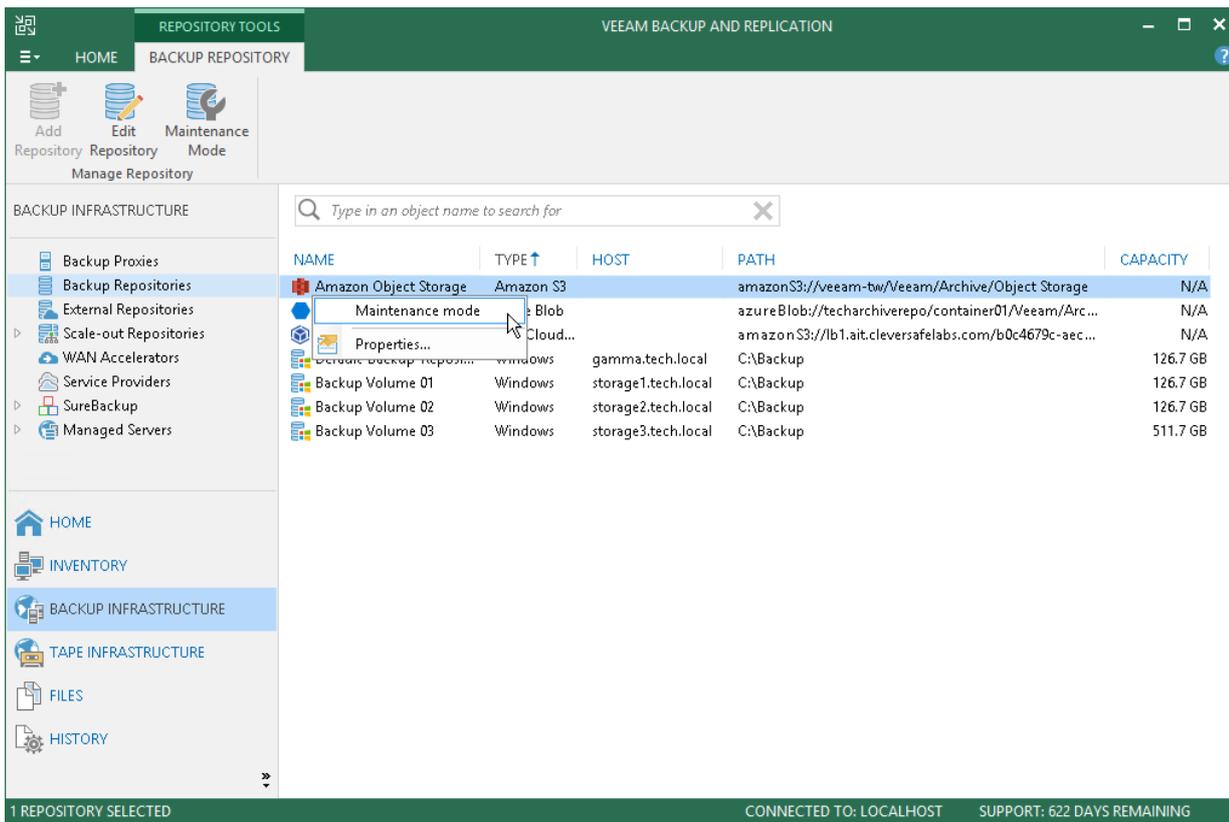
- If an object storage repository that is being used and which stores offloaded backup data was, at some point, excluded from capacity tier, then such a repository will be put into maintenance mode automatically.

For more information about how to exit the maintenance mode for such excluded repositories, see [Excluding Capacity Tier from Scale-Out Repositories](#).

To put on object storage repository into maintenance mode, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Backup Repositories**.
3. In the working area, select an object storage repository and click **Maintenance mode** on the ribbon or right-click an object storage repository and select **Maintenance mode**.

To switch back to normal, repeat steps 1 and 2, and at the step 3, deselect the **Maintenance mode** checkbox.



Maintenance Mode Limitations

The following table lists limitations that are imposed right after an object storage repository is put into maintenance mode.

Activity	Restriction Level	Related Topic
Data transfer / Synchronization	○	Data Transfer
Move to capacity tier	○	Moving to Capacity Tier
Copy to performance tier	○	Copying to Performance Tier
Restore	○	Data Restore
Export as .vbk	○	Exporting Backups
Removal of backups from configuration	●	Removing from Configuration
Retention policies	Synchronization is skipped for backup chains located in object storage repositories. Obsolete restore points will only be removed from a backup chain of your extents.	Retention Policy

Removal of object storage repositories		Removing Object Storage Repository
Removal of backups or VMs created with the Per-VM method		Removing Backups from Object Storage Repository
Removal of a VM from a single storage	Synchronization is skipped for backup chains located in object storage repositories. A virtual machine will only be removed from a backup chain of your extents.	Deleting from Disk
Modifications of object storage repositories settings		Editing Settings of Object Storage Repository
Modifications of capacity tier settings		Add Capacity Tier, Excluding Capacity Tier from Scale-Out Repositories
Scale-out backup repository rescan	Synchronization is skipped for object storage repositories.	Rescanning Scale-Out Repositories
Removal of a scale-out backup repository from the configuration database		Removing Scale-Out Backup Repositories
Evacuation of storage or indexes from on-premise extents		Evacuating Backups from Performance Tiers

Removing Backups from Object Storage Repository

To remove offloaded backup data from object storage repositories, use the **Delete from disk** feature to synchronize the state of backup chains located on your extents with that in object storage. For more information on how to use this feature, see [Delete from Disk](#).

Consider the following:

- When removing offloaded backup files from the backup chain that was created with the Per-VM method, then all the associated offloaded blocks of data will be altogether removed from object storage.

For more information about Per-VM backups, see [Per-VM Backup Files](#).

- When removing offloaded backup files from the backup chain that was created as a single storage backup file, then nothing will be removed until either of the following occurs:
 - All the VMs were removed from the backup.
 - The backup itself was removed.

- If an object storage repository has been put into maintenance mode, the removal of data from such a repository will not be possible until it is switched back to normal.

For more information, see [Switching to Maintenance Mode](#).

- Data can only be removed from object storage repositories until no other backups have any references to it.

For example, you may want to remove a piece of data consisting of blocks being referred to by another backups (.vbk, .vib, or .vrb files). In such a scenario, the removal of such blocks will be skipped.

- Associated indexes will be updated for consistency purposes.

For more information, see [Indexes](#).

- During data removal, not only will blocks be removed, but also the entire folder structure starting from the repository folder (<repository_folder_name>) will be completely purged.

For more information about how Veeam stores data in object storage, see [Understanding Object Storage Repository Structure](#).

- If backup files with metadata that are located on your extents have been removed locally in any way other than by using the [Deleting from Disk](#) feature, Veeam will not be able to synchronize the backup chain state with that of object storage. Therefore, the offloaded blocks of data will continue to remain in cloud storage. To remove such blocks, use your cloud platform abilities.

Backup Repositories with Rotated Drives

A backup repository can use rotated drives. Rotated drives can be detachable USB or eSATA hard drives. This scenario can be helpful if you want to store backups on several external hard drives that you plan to regularly move between different locations.

To use rotated drives, you must enable the **This repository is backed by rotated hard drives** option in the advanced settings of the backup repository. When this option is enabled, Veeam Backup & Replication recognizes the backup target as a backup repository with rotated drives and uses a specific algorithm to make sure that the backup chain created on these drives is not broken.

Limitations for Backup Repositories with Rotated Drives

Backup repositories with rotated drives have the following limitations:

- You cannot store archive full backups (GFS backups) created with backup copy jobs on backup repositories with rotated drives.
- You cannot store per-VM backup files on backup repositories with rotated drives.
- You cannot rescan backup repositories with rotated drives.
- Scale-out backup repositories do not support rotated drives. If you enable the **This repository is backed by rotated hard drives** setting on an extent, Veeam Backup & Replication will ignore this setting and will work with such repository as with a standard extent.

How Repository with Rotated Drives Works

Microsoft Windows Backup Repository

A job targeted at a backup repository with rotated drives is performed in the following way.

For backup jobs:

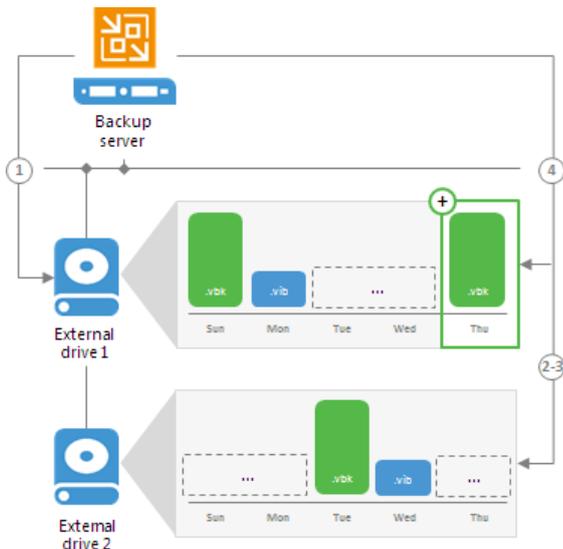
1. Veeam Backup & Replication creates a regular backup chain on the currently attached drive.
2. When a new job session starts, Veeam Backup & Replication checks if the backup chain on the currently attached drive is consistent. The consistent backup chain must contain a full backup and all incremental backups that have been produced by the job. This requirement applies to all types of backup chains: forever forward incremental, forward incremental and reverse incremental.

If external drives have been swapped, and the full backup or any incremental backups are missing from the currently attached drive, Veeam Backup & Replication starts the backup chain anew. It creates a new full backup file on the drive, and this full backup is used as a starting point for subsequent incremental backups.

3. [For external drives attached to Microsoft Windows servers] Veeam Backup & Replication checks the retention policy set for the job. If some backup files in the backup chain are outdated, Veeam Backup & Replication removes them from the backup chain.
4. When you swap drives again, Veeam Backup & Replication checks the backup chain for consistency and creates a new full backup.

NOTE:

When you specify retention settings for a backup job targeted at a backup repository with rotated drives, you must define the total number of restore points that you want to retain on all drives in the set. For example, if you set retention to 14, the job will keep the total of 14 restore points across all drives.



For backup copy jobs:

1. Veeam Backup & Replication creates a regular backup chain on the currently attached drive.
2. When you swap drives, and the attached drive is empty, Veeam Backup & Replication creates a full backup on it. If there is a backup chain on the drive, Veeam Backup & Replication creates a new incremental backup and adds it to the backup chain. The latest incremental backup existing in the backup chain is used as a starting point for the new incremental backup.
3. [For external drives attached to Microsoft Windows servers] Veeam Backup & Replication checks the retention policy set for the job. If some backup files in the backup chain are outdated, Veeam Backup & Replication removes them from the backup chain.

NOTE:

When you specify retention settings for a backup copy job targeted at a backup repository with rotated drives, you must define the number of restore points per drive. For example, if you set retention to 7, the job will keep 7 restore points on every drive in the set.

Drive Detection

Drive letters for external drives may change when you add new volumes or storage hardware such as CD-ROM on the server. On Microsoft Windows backup repositories, Veeam Backup & Replication can keep track of drives and detect them even if the drive letter changes.

To detect a drive correctly, Veeam Backup & Replication must have a record about it in the configuration database. Consider the following requirements:

- When you insert a drive for the first time, the drive is not registered in the configuration database. Such drive must have the same letter as the one specified in the **Path to folder** field in backup repository settings. For more information, see [Configuring Path and Load Control Settings](#).
If the drive has some other letter, Veeam Backup & Replication will not be able to detect and use it.
- When you insert a drive that has already been used and has some restore points on it, the drive is already registered in the configuration database. Veeam Backup & Replication will be able to detect and use it, even if the drive letter changes.

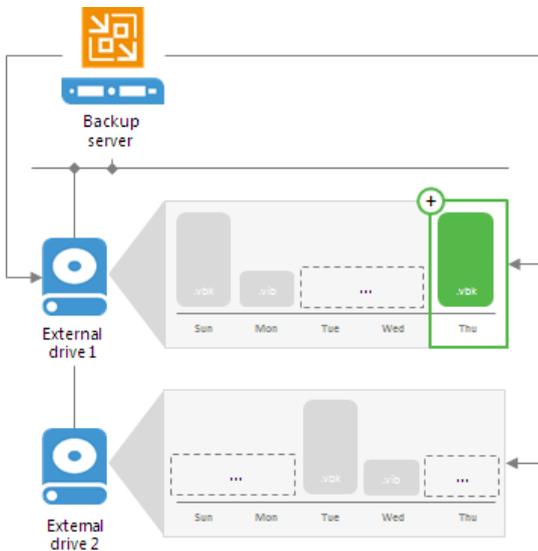
Linux and Shared Folder Backup Repository

If you use a Linux server or CIFS share as a backup repository with rotated drives, Veeam Backup & Replication employs a "cropped" mechanism of work with rotated drives. Veeam Backup & Replication keeps information only about the latest backup chain in the configuration database. Information about previous backup chains is removed from the database. For this reason, the retention policy set for the job may not work as expected.

A job targeted at a backup repository with rotated drives is performed in the following way:

1. During the first run of the job, Veeam Backup & Replication creates a regular backup full backup on the drive that is attached to the backup repository server.
2. During the next job session, Veeam Backup & Replication checks if the current backup chain on the attached drive is consistent. The consistent backup chain must contain a full backup and all incremental backups subsequent to it. This requirement applies to all types of backup chains: forever forward incremental, forward incremental and reverse incremental.
 - If the current backup chain is consistent, Veeam Backup & Replication adds a new restore point to the backup chain.
 - If external drives have been swapped, and the current backup chain is not consistent, Veeam Backup & Replication always starts a new backup chain (even if restore points from previous backup chains are available on the attached drive). Veeam Backup & Replication creates a new full backup file on the drive, and this full backup is used as a starting point for subsequent incremental backups.

As soon as Veeam Backup & Replication starts a new backup chain on the drive, it removes information about restore points from previous backup chains from the configuration database. Backup files corresponding to these previous restore points are not deleted, they remain on disk. This happens because Veeam Backup & Replication applies the retention policy only to the current backup chain, not to previous backup chains.



Restore from Rotated Drives

If you swap the drive, earlier-made backups are not available for restore immediately. To be able to restore, run any job the target of which is the required repository. All backups performed earlier will be displayed and available for restore.

You can also go to the **Disk Management** settings of the repository server and change the current drive letter to the letter of the drive which contains backups.

Adding Backup Repositories with Rotated Drives

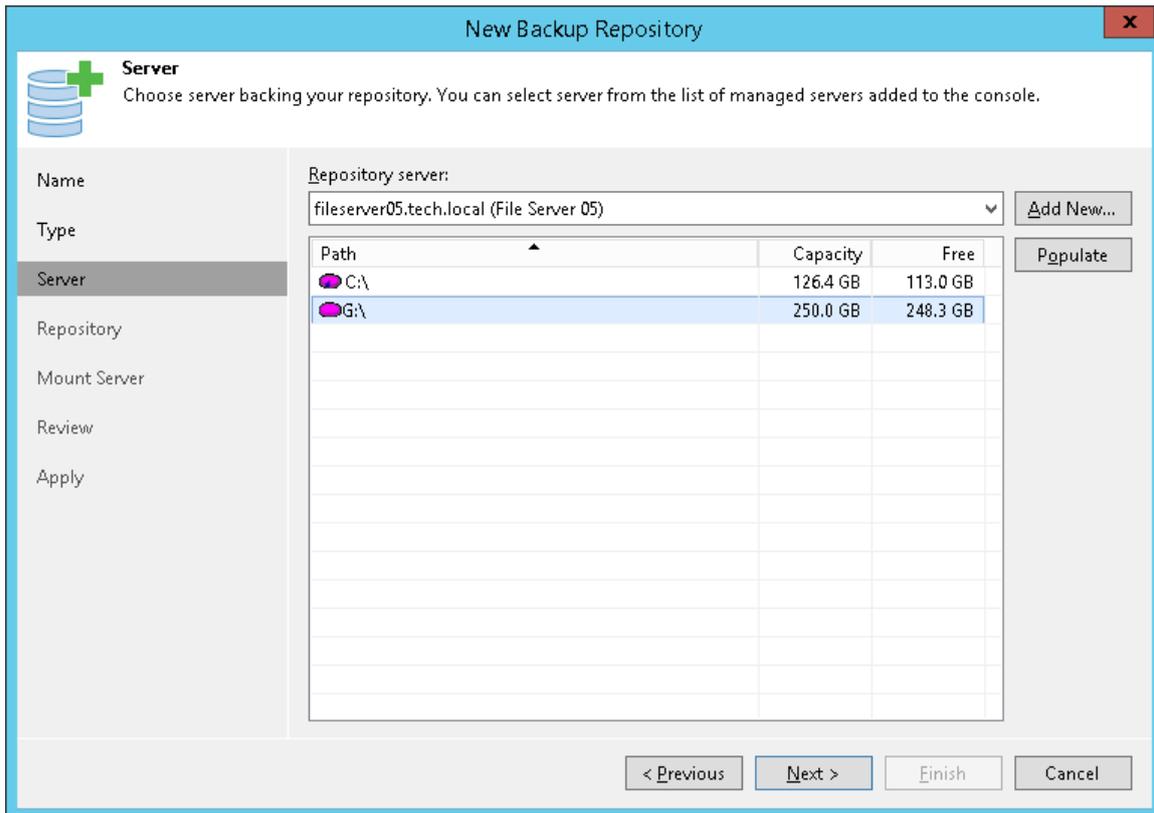
To add a backup repository with rotated drives:

1. Attach one of external drives from the set to a Microsoft Windows or Linux server. The server must be added to the backup infrastructure. For more information, see [Managing Servers](#).

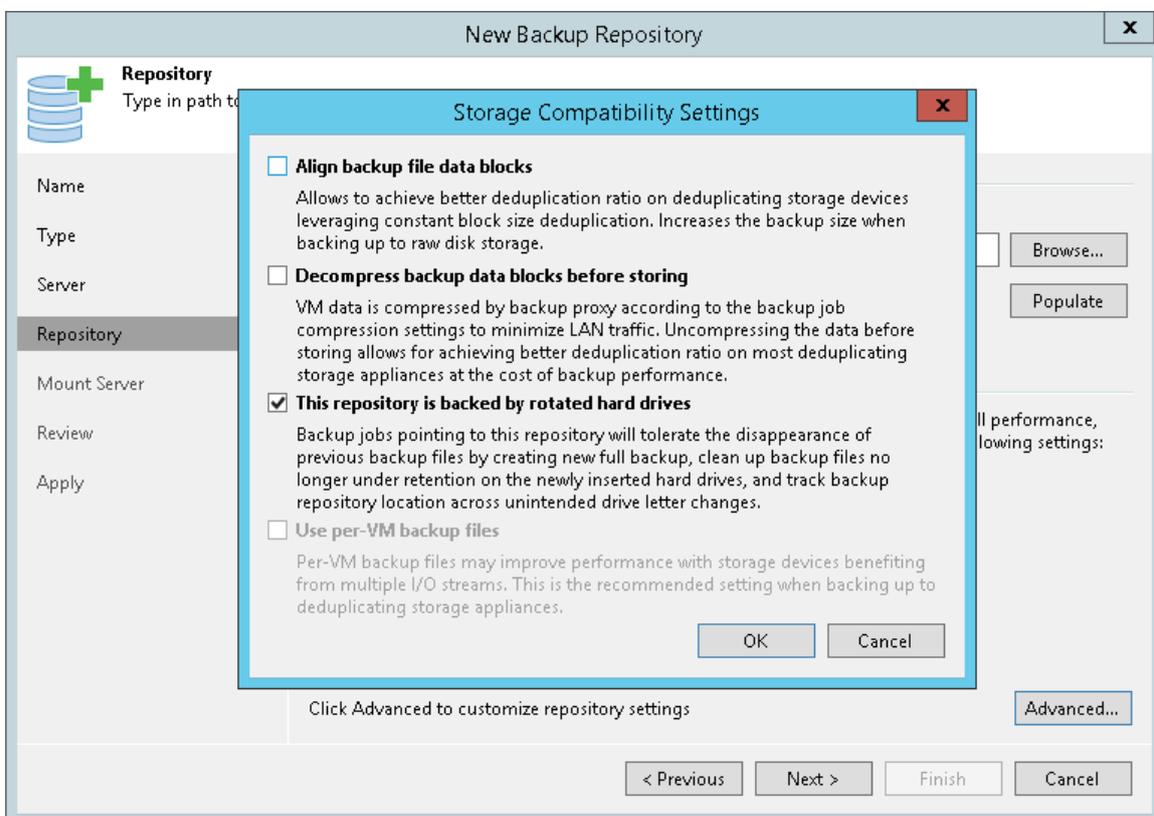
You can also attach the external hard drive to the backup server itself. In this case, the VM traffic will path through the backup server, which will produce additional workload on it.

2. Launch the **Add New Backup Repository** wizard.

- At the **Server** step of the wizard, select the server to which the drive is attached.



- At the **Repository** step of the wizard, click **Advanced** and select the **This repository is backed by rotated hard drives** check box.



- Configure other settings of the backup repository as required and finish working with the wizard.

Adding Backup Repositories

This section describes how to add direct attached storage, network attached storage, and deduplicating storage appliances as backup repositories.

For information on how to add object storage repositories, see [Object Storage](#).

Before adding a backup repository, [check prerequisites](#). Then use the **New Backup Repository** wizard to add the backup repository.

Before You Begin

Before you configure a backup repository, check the following prerequisites.

Dell EMC Data Domain

- Dell EMC Data Domain must meet software and/or hardware requirements. For more information, see [System Requirements](#).
- The DD Boost license must be installed on the Dell EMC Data Domain system, DD Boost must be enabled and configured.
- The gateway server that you plan to use for work with Dell EMC Data Domain must be added to the backup infrastructure.

If the Dell EMC Data Domain storage system does not meet these requirements, you can add it as a CIFS (SMB) folder. In this case, Veeam Backup & Replication will not use the DD Boost technology to work with Dell EMC Data Domain. For more information, see [Dell EMC Data Domain](#).

ExaGrid

- ExaGrid must meet software and/or hardware requirements. For more information, see [System Requirements](#).
- To use ExaGrid as a backup repository, you must configure an ExaGrid share in a proper way in ExaGrid Manager. For more information, see ExaGrid documentation.

HPE StoreOnce

- HPE StoreOnce must meet software and/or hardware requirements. For more information, see [System Requirements](#).
- The HPE StoreOnce Catalyst license must be installed on the HPE StoreOnce system.
- You must use a Catalyst store as a backup target.
- The gateway server that you plan to use for work with HPE StoreOnce system must be added to the backup infrastructure.
- The client account that you plan to use to connect to HPE StoreOnce must have access permissions on the Catalyst store where backup data will be kept.

If the HPE StoreOnce storage system does not meet these requirements, you can add it as a shared folder. In this case, Veeam Backup & Replication will perform target-side deduplication. For more information, see [HPE StoreOnce](#).

Quantum DXi

- Quantum DXi must meet software and/or hardware requirements. For more information, see [System Requirements](#).
- To use Quantum DXi as a backup repository, you must configure a Quantum DXi share in a proper way. For more information, see [Quantum DXi documentation](#).

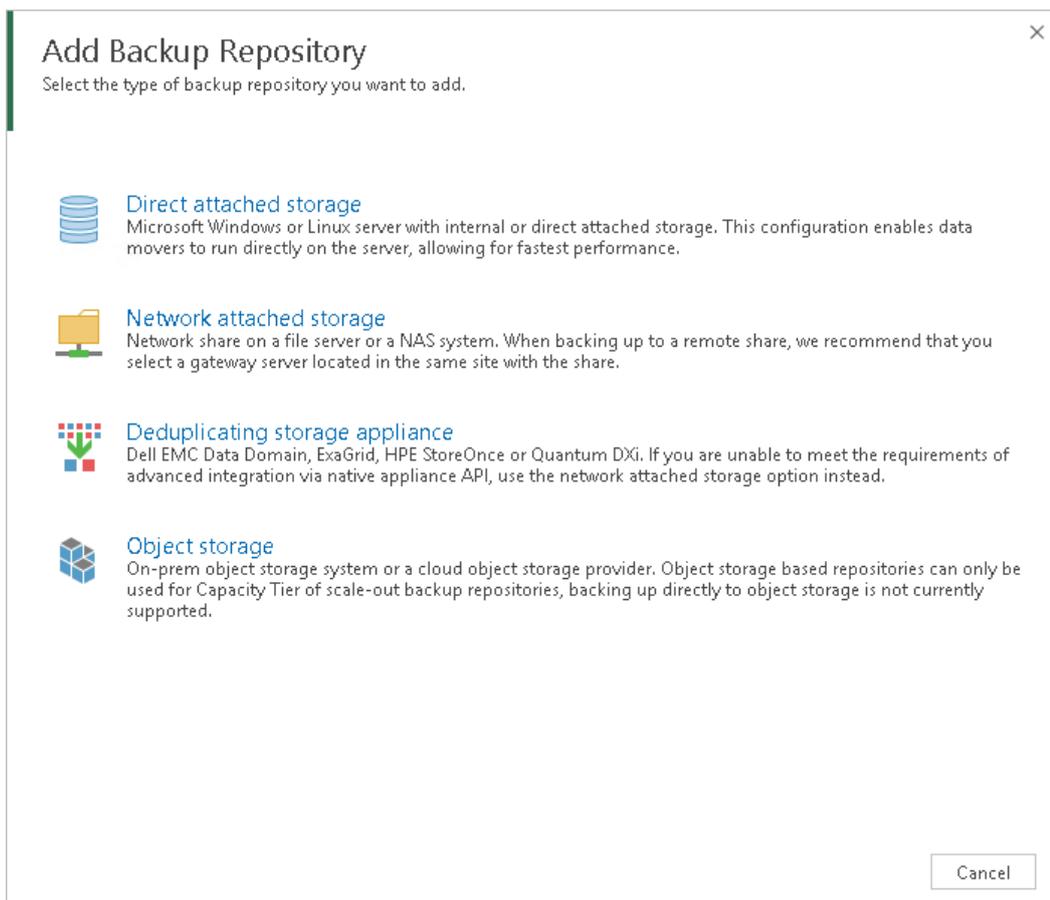
Step 1. Launch New Backup Repository Wizard

To launch the **New Backup Repository** wizard, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, right-click the **Backup Repositories** node and select **Add Backup Repository**. Alternatively, you can click **Add Repository** on the ribbon.
3. In the **Add Backup Repository** window, select the type of the backup repository you want to add.

The **New Backup Repository** wizard will guide you through steps for adding direct attached storage, network attached storage, and deduplicating storage appliances as backup repositories.

For information on how to add object storage repositories, see [Adding Object Storage Repositories](#).



Step 2. Specify Backup Repository Name and Description

At the **Name** step of the wizard, specify a name and description for the backup repository.

1. In the **Name** field, specify a name for the backup repository.

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

The screenshot shows a wizard window titled "New Backup Repository". On the left is a sidebar with a "Name" icon and a list of steps: Name, Server, Repository, Mount Server, Review, and Apply. The "Name" step is selected. The main area has a "Name" label and a text box containing "Backup Volume 01". Below it is a "Description" label and a larger text box containing "Onsite Backup Repository". At the bottom right are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Specify Server or Shared Folder Settings

Options that you can specify at the **Server** step of the wizard depend on the type of backup repository you are adding.

In this section:

- [Microsoft Windows or Linux Server](#)
- [Shared Folder](#)
- [EMC Data Domain](#)
- [ExaGrid or Quantum DXi](#)
- [HPE StoreOnce](#)

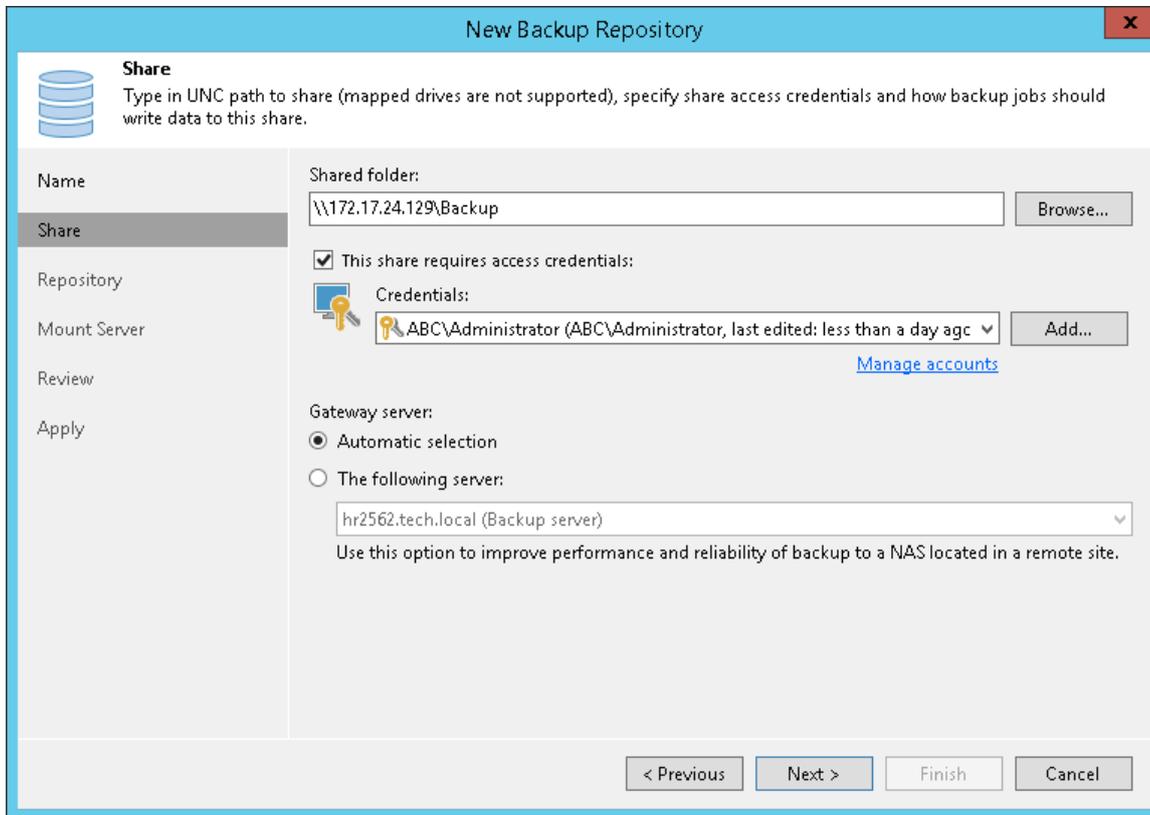
Microsoft Windows or Linux Server

To configure settings for a Microsoft Windows or Linux server:

1. From the **Repository server** list, select a Microsoft Windows or Linux server that you want to use as a backup repository. The **Repository server** list contains only those servers that are added to the backup infrastructure. If the server is not added to the backup infrastructure yet, you can click **Add New** on the right to open the **New Windows Server** or **New Linux Server** wizard.

Note that you cannot add ExaGrid or Quantum DXi servers as Linux backup repositories. ExaGrid and Quantum DXi are integrated with Veeam Backup & Replication, and thus must be added as [deduplicating storage appliances](#).

In some cases, the automatic selection mechanism may cause problems as Veeam Backup & Replication may use different gateway servers for different job sessions. For example, during one job session Veeam Backup & Replication may use a 64-bit gateway server to create a backup file. If during the next job session Veeam Backup & Replication uses a 32-bit gateway server, Veeam Backup & Replication will fail to open the created backup file on the backup repository. To overcome this situation, you must explicitly define the gateway server.



EMC Data Domain

To configure settings for EMC Data Domain:

1. Specify connection settings for EMC Data Domain:
 - If EMC Data Domain works over TCP, in the **Type in Data Domain server name** field enter a full DNS name or IP address of the EMC Data Domain server.
 - If EMC Data Domain works over Fibre Channel, select the **Use Fibre Channel (FC) connectivity** check box. In the **Type in Data Domain server name** field, enter a name of the Data Domain Fibre Channel server. To get the Data Domain Fibre Channel server name, in Data Domain System Manager open the **Data Management > DD Boost > Fibre Channel** tab.
2. In the **Credentials** field, specify credentials of the user account to connect to the EMC Data Domain server or EMC Data Domain Fibre Channel server. 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](#).

To connect to the EMC Data Domain server, you must use credentials for the DD Boost User. To specify the DD Boost User account settings, in Data Domain System Manager, open the **Data Management > DD Boost Settings** tab.

3. To use in-flight encryption between the backup proxy and EMC Data Domain, select the **Enable DDBoost encryption** check box and choose the encryption level – *Medium* or *High*. The encryption option works for EMC Data Domain 5.5 and later.

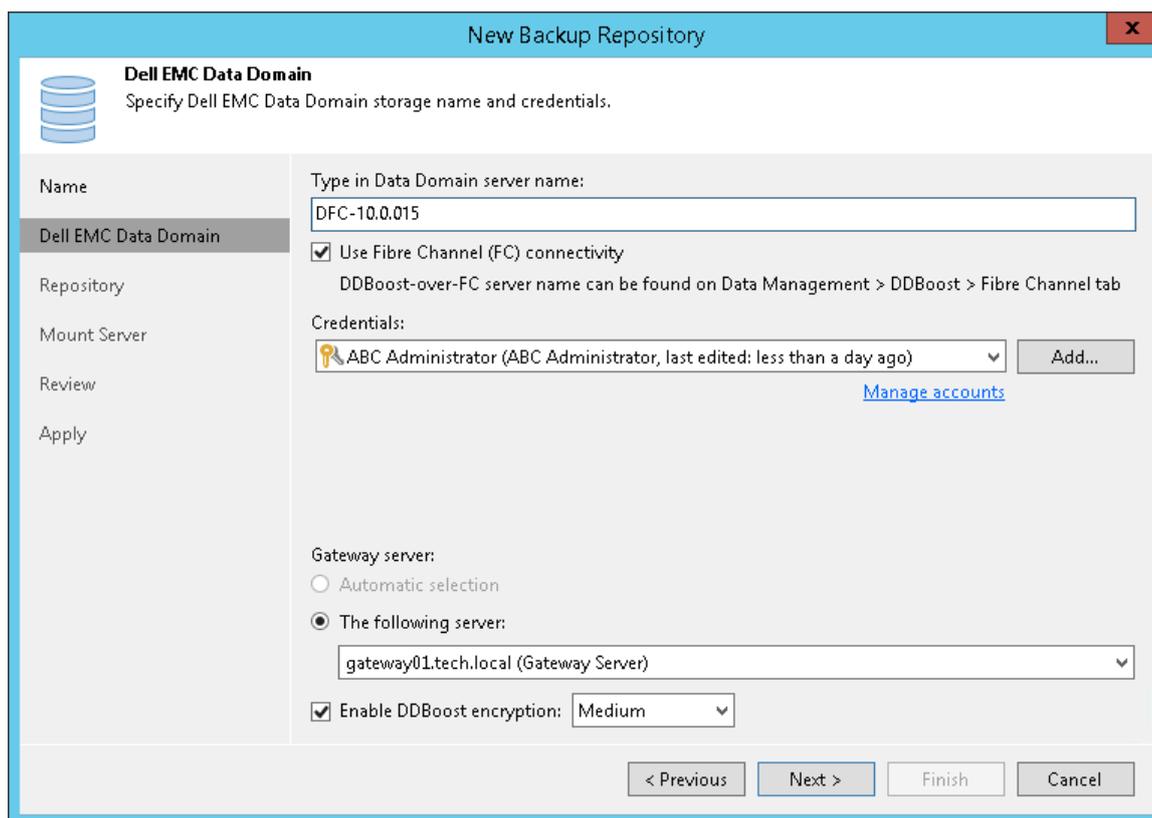
4. In the **Gateway server** section, specify settings for the gateway server:

- If a network connection between the source datastore and EMC Data Domain appliance is fast, choose **Automatic selection**. In this case, Veeam Backup & Replication will automatically select a gateway server.
- If you perform backup over WAN or slow connections, choose **The following server**. From the list below, select a Microsoft Windows server on the target site that you want to use as a gateway server. The server must have a direct access to the EMC Data Domain appliance and must be located as close to the appliance as possible.

In some cases, the automatic selection mechanism may cause problems as Veeam Backup & Replication may use different gateway servers for different job sessions. For example, during one job session Veeam Backup & Replication may use a 64-bit gateway server to create a backup file. If during the next job session Veeam Backup & Replication uses a 32-bit gateway server, Veeam Backup & Replication will fail to open the created backup file on the backup repository. To overcome this situation, you can explicitly define the gateway server.

IMPORTANT!

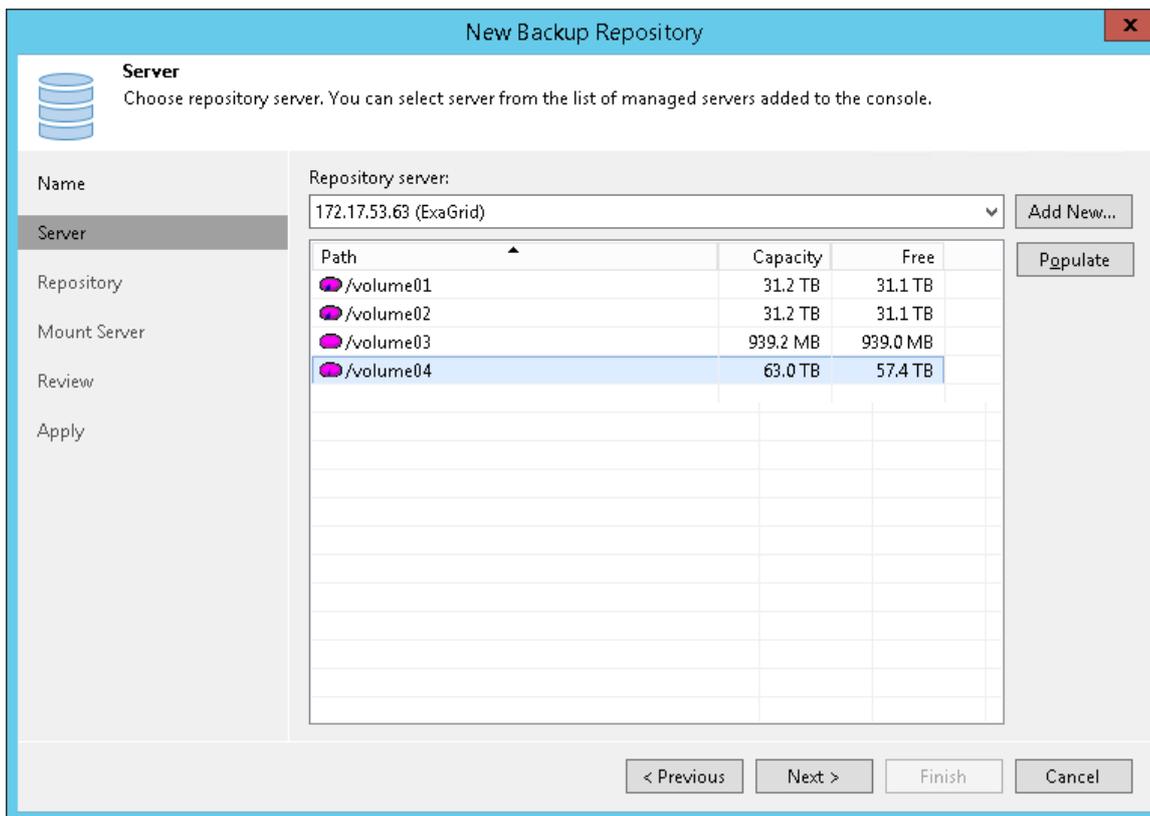
If you connect to EMC Data Domain over Fibre Channel, you must explicitly define the gateway server to communicate with EMC Data Domain. The server you select must be added to the backup infrastructure and must have access to the EMC Data Domain appliance over Fibre Channel.



ExaGrid or Quantum DXi Deduplicating Appliance

To configure settings for ExaGrid or Quantum DXi deduplicating appliance:

1. From the **Repository server** list, select an appliance that you want to use as a backup repository. The **Repository server** list contains only those servers that are added to the backup infrastructure. If the server is not added to the backup infrastructure yet, you can click **Add New** to open the **New Linux Server** wizard. For more information, see [Managing Servers](#).
2. Click **Populate** to see the appliance capacity and available free space.



HPE StoreOnce Deduplicating Appliance

To configure settings for HPE StoreOnce:

1. In the **Type in HPE StoreOnce server name** field, enter a full DNS name or IP address of the HPE StoreOnce appliance.
2. If HPE StoreOnce works over Fibre Channel, select the **Use Fibre Channel (FC) connectivity** check box.
3. In the **Credentials** field, specify credentials of the client account to connect to the HPE StoreOnce appliance. 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](#).

The client account that you plan to use to connect to HPE StoreOnce must have access permissions on a Catalyst store where backup data will be kept. To check the client account permissions, in the HPE StoreOnce management console, select the Catalyst store and open the **Permissions** tab for it.

4. In the **Gateway server** section, specify settings for the gateway server:

- If you want Veeam Backup & Replication to pick the gateway server automatically, choose **Automatic selection**. In this case, Veeam Backup & Replication will automatically select a gateway server.
- If you want to define the gateway server explicitly, choose **The following server**. From the list below, select a Microsoft Windows server that you want to use as a gateway server.

In some cases, the automatic selection mechanism may cause problems as Veeam Backup & Replication may use different gateway servers for different job sessions. For example, during one job session Veeam Backup & Replication may use a 64-bit gateway server to create a backup file. If during the next job session Veeam Backup & Replication uses a 32-bit gateway server, Veeam Backup & Replication will fail to open the created backup file on the backup repository. To overcome this situation, you can explicitly define the gateway server.

IMPORTANT!

If you connect to HPE StoreOnce over Fibre Channel, you must explicitly define the gateway server to communicate with HPE StoreOnce appliance. The server you select must be added to the backup infrastructure and must have access to the HPE StoreOnce appliance over Fibre Channel.

5. If a WAN connection between the gateway server and the HPE StoreOnce appliance is weak, select the **Gateway server and StoreOnce are connected over WAN** check box. Veeam Backup & Replication will compress VM data transported from the gateway server to the HPE StoreOnce appliance, and calculate checksums for data blocks going from the gateway server to the HPE StoreOnce appliance.

New Backup Repository

HPE StoreOnce
Specify HPE StoreOnce storage name and credentials.

Name

Type in HPE StoreOnce server name:
COFC-10.0.0.53

Use Fibre Channel (FC) connectivity
Requires that gateway server is connected into SAN fabric.

Credentials:

ABC Administrator (ABC Administrator, last edited: less than a day ago) Add...
[Manage accounts](#)

Gateway server:

Automatic selection

The following server:
gateway02.tech.local (Gateway Server)

Gateway server and StoreOnce are connected over WAN
Enables network traffic compression and checksumming by Catalyst. Using this functionality may reduce backup performance over fast links.

< Previous Next > Finish Cancel

Step 4. Configure Path and Load Control Settings

At the **Repository** step of the wizard, specify path and load control repository settings.

1. In the **Location** section, specify a path to the folder where backup files must be stored. Click **Populate** to check capacity and available free space in the selected location.
 - For Dell EMC Data Domain, click **Browse** and select a location from the list of available paths.
 - For HPE StoreOnce, select a Catalyst store from the list.
2. Use the **Load control** section to limit the number of concurrent tasks and data ingestion rate for the backup repository. These settings will help you control the load on the backup repository and prevent possible timeouts of storage I/O operations.
 - Select the **Limit maximum concurrent tasks** check box and specify the maximum allowed number of concurrent tasks for the backup repository. If this value is exceeded, Veeam Backup & Replication will not start a new task until one of current tasks finishes. For more information, see [Limiting the Number of Concurrent Tasks](#).
 - Select the **Limit read and write data rates to** check box and specify the maximum rate to restrict the total speed of reading and writing data to the backup repository disk. For more information, see [Limiting Combined Data Rate for Backup Repositories](#).

NOTE:

The **Limit read and write data rates to** settings does not apply to health checks performed as part of backup and backup copy jobs. Even if you limit read/write rate for a backup repository, the health check will consume resources of the backup repository regardless of this setting. Bear this limitation in mind when configuring basic and health check schedules for backup and backup copy jobs.

New Backup Repository

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location
Path to folder: C:\Backups Browse...
Capacity: Populate
Free space:

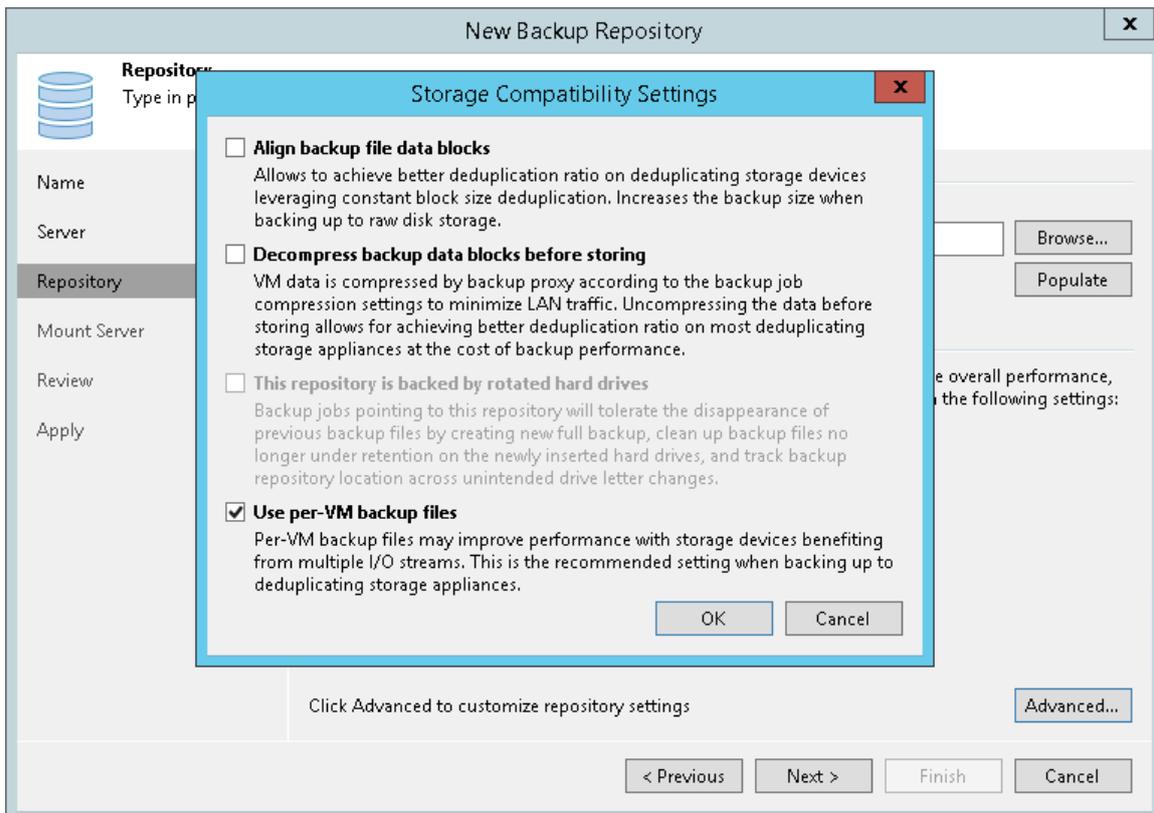
Load control
Running too many concurrent tasks against the same repository may reduce overall performance, and cause I/O operations to timeout. Control storage device saturation with the following settings:
 Limit maximum concurrent tasks to: 4
 Limit read and write data rates to: MB/s

Click Advanced to customize repository settings Advanced...

< Previous Next > Finish Cancel

3. Click **Advanced** to configure additional settings for the backup repository:

- For storage systems using a fixed block size, select the **Align backup file data blocks** check box. Veeam Backup & Replication will align VM data saved to a backup file at a 4 KB block boundary. This option provides better deduplication across backup files but can result in greater amount of unused space on the storage device and a higher level of fragmentation.
- When you enable compression for a backup job, Veeam Backup & Replication compresses VM data at the source side and then transports it to the target side. Writing compressed data to a deduplicating storage appliance results in poor deduplication ratios as the number of matching blocks decreases. To overcome this situation, select the **Decompress backup data blocks before storing** check box. If data compression is enabled for a job, Veeam Backup & Replication will compress VM data on the source side, transport it to the target side, decompress VM data on the target side and write raw VM data to the storage device to achieve a higher deduplication ratio.
- If you plan to use rotated drives for the backup repository, select the **This repository is backed by rotated hard drives** check box. For more information, see [Configuring Backup Repositories with Rotated Drives](#).
- To create a separate backup file for every VM in the job, select the **Use per-VM backup files** check box. This setting is recommended if you use a deduplicating storage appliance as a backup repository. Veeam Backup & Replication will write VM data to the backup repository in several streams, which will improve the backup job performance. However, in this case Veeam Backup & Replication will not deduplicate data between VMs added to the job. For more information, see [Per-VM Backup Files](#).



Settings for Deduplicating Storage Appliances

If you use a deduplicating storage appliance as a backup repository, Veeam Backup & Replication automatically sets advanced settings to the following ones:

Dell EMC Data Domain

- The **Align backup file data blocks** option is disabled by default.
- The **Decompress backup data blocks before storing** option is enabled by default.
- The **This repository is backed by rotated hard drives** option is disabled.
- The **Use per-VM backup files** option is enabled by default.

ExaGrid or Quantum DXi

- The **Align backup file data blocks** option must not be enabled.
- The **Decompress backup data blocks before storing** option is disabled by default.
- The **This repository is backed by rotated hard drives** option is disabled by default.
- The **Use per-VM backup files** option should be enabled.
- **Limit max concurrent tasks** is equal to 10 (recommended, by default).

HPE StoreOnce

- The **Align backup file data blocks** option must not be enabled.
- The **Decompress backup data blocks before storing** option is enabled by default.
- The **This repository is backed by rotated hard drives** option is disabled.
- The **Use per-VM backup files** option is enabled.

Step 5. Specify Mount Server Settings

At the **Mount Server** step of the wizard, specify settings for the mount server that you plan to use for file-level and application items restore.

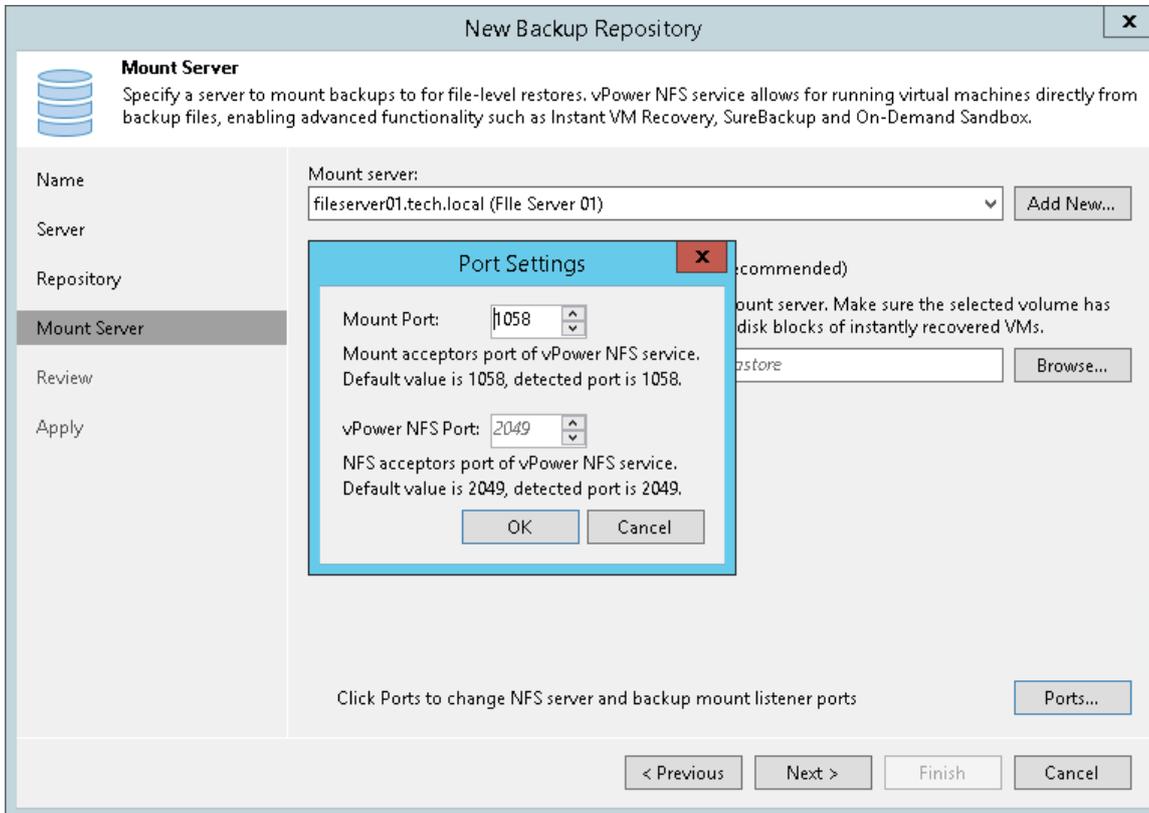
1. From the **Mount Server** list, select a server that you want to use as a mount server. The mount server is required for file-level and application items restore. During the restore process, Veeam Backup & Replication will mount the VM disks from the backup file residing on the backup repository to the mount server. As a result, VM data will not have travel over the network, which will reduce the load on the network and speed up the restore process. For more information, see [Mount Server](#).

The **Mount Server** list contains only Microsoft Windows servers that are added to the backup infrastructure. If the server is not added to the backup infrastructure yet, click **Add New** on the right to open the **New Windows Server wizard**. For more information, see [Adding Microsoft Windows Servers](#).

2. To make the backup repository accessible by the Veeam vPower NFS Service, select the **Enable vPower NFS server on the mount server** check box. Veeam Backup & Replication will enable the vPower NFS Service on the mount server you have selected.
3. In the **Folder** field, specify a folder that will be used as a vPower NFS root folder. For more information, see [Veeam vPower NFS Service](#).
4. To customize network ports used by the vPower NFS Service, click **Ports**. For information on ports used by default, see [Used Ports](#).

IMPORTANT!

Do not enable Microsoft Windows NFS services on the machine where you install the Veeam vPower NFS Service. If Microsoft NFS services and Veeam vPower NFS Service are enabled on the same machine, both services may fail to work correctly.

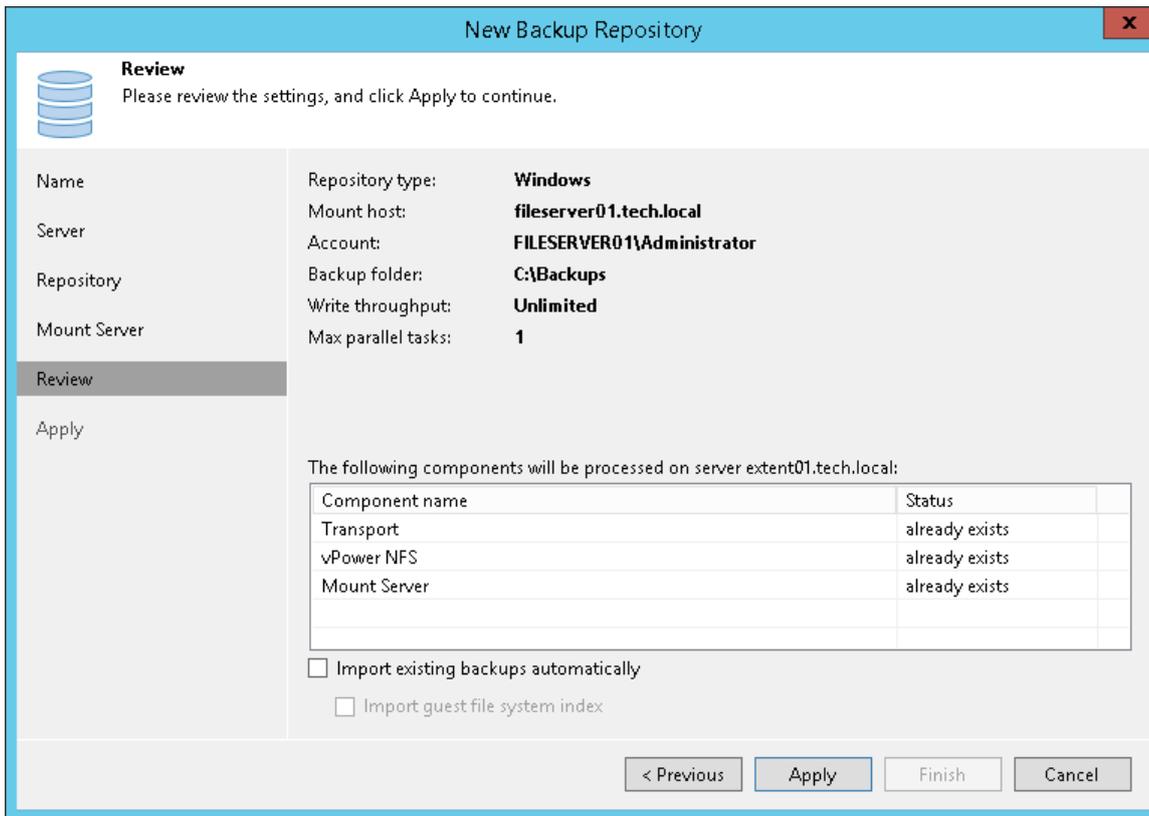


Step 6. Review Properties and Components

At the **Review** step of the wizard, review details of the backup repository and specify importing settings.

1. Review the backup repository settings and list of components that will be installed on the backup repository server.
2. If the backup repository contains backups that were previously created with Veeam Backup & Replication, select the **Import existing backups automatically** check box. Veeam Backup & Replication will scan the backup repository to detect existing backup files and display them in the Veeam Backup & Replication console under the **Imported > Backups** node.

- If the backup repository contains guest file system index files that were previously created by Veeam Backup & Replication, select the **Import guest file system index** check box. Index files will be imported with backup files, and you will be able to search for guest OS files inside imported backups.

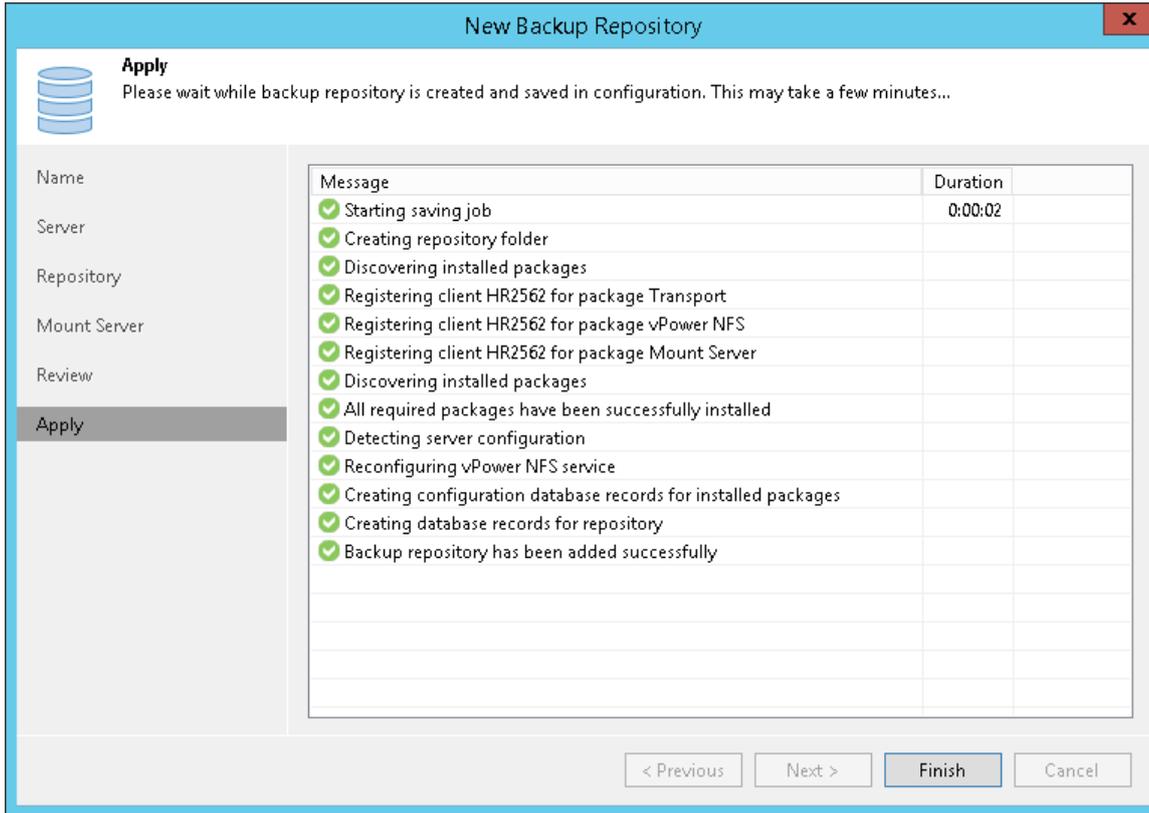


Step 7. Finish Working with Wizard

At the **Apply** step of the wizard, complete the procedure of backup repository configuration.

- Wait for the backup repository to be added to the backup infrastructure. The process may take several minutes.
- Review details for the added backup repository.

3. Click **Finish** to exit the wizard.



Rescanning Backup Repositories

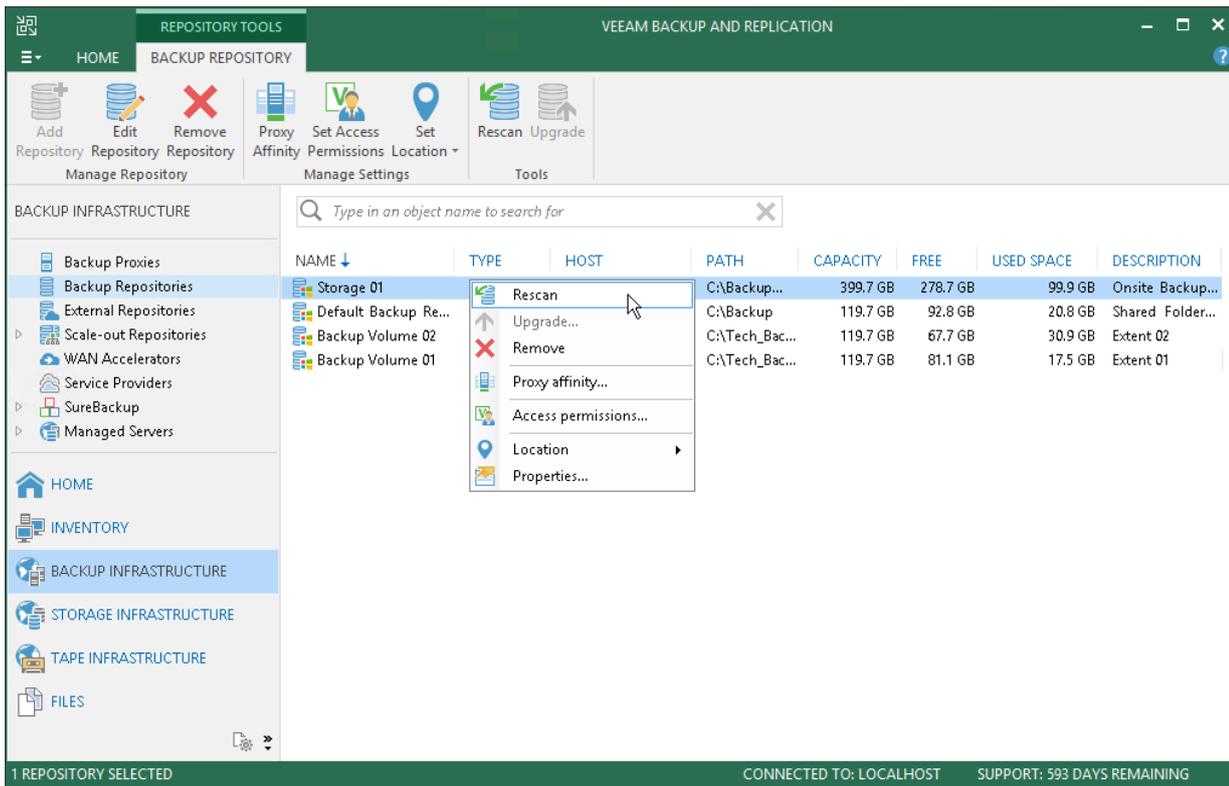
You can rescan a backup repository configured in the backup infrastructure. Backup repository rescan may be required, for example, if you have archived backups from a backup repository to tape and deleted backup files on the backup repository. Or you have copied backups to the backup repository manually and want to work with them in Veeam Backup & Replication.

During the rescan operation, Veeam Backup & Replication gathers information about backups that are currently available on the backup repository and updates the list of backups in the configuration database.

To rescan a backup repository:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories** node.

- In the working area, select the backup repository and click **Rescan Repository** on the ribbon or right-click the backup repository and select **Rescan repository**.



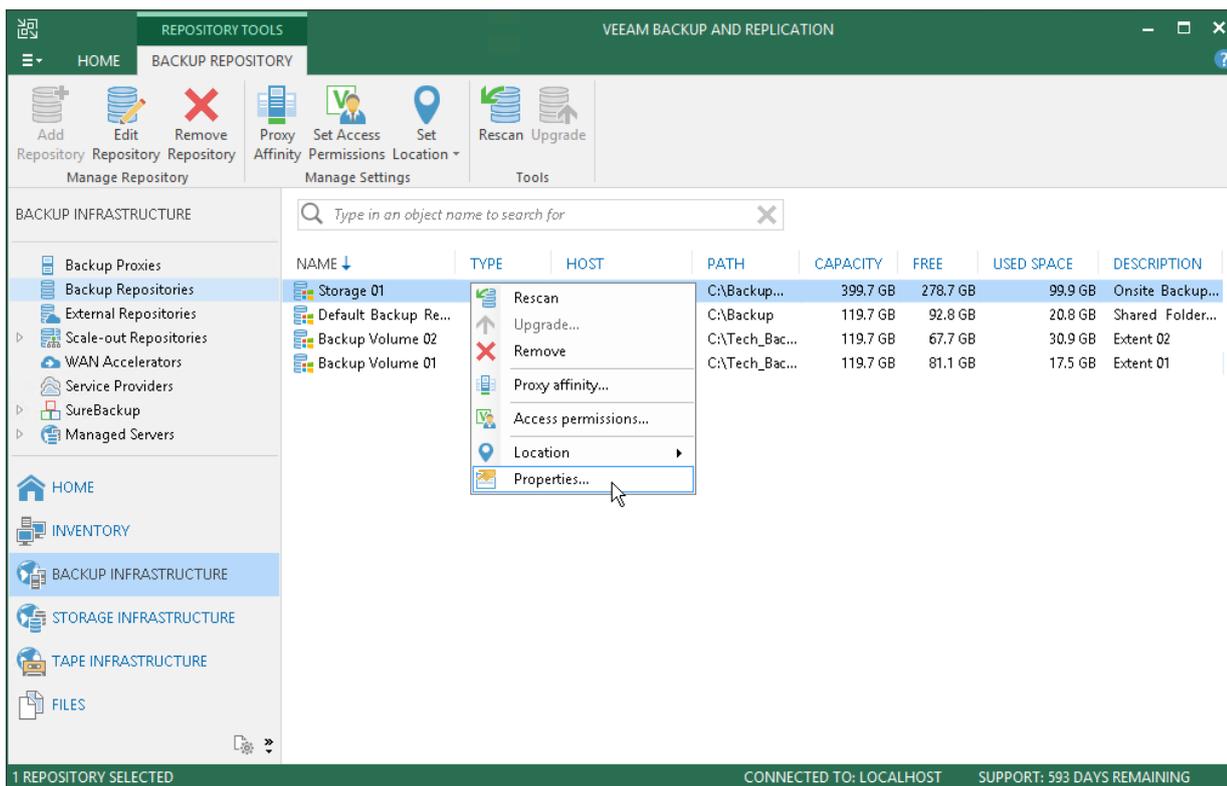
Editing Settings of Backup Repositories

You can edit settings of backup repositories you have added to the backup infrastructure.

To edit settings of a backup repository:

- Open the **Backup Infrastructure** view.
- In the inventory pane, select the **Backup Repositories** node.
- In the working area, select the backup repository and click **Edit Repository** on the ribbon or right-click the backup repository and select **Properties**.

4. Edit the backup repository settings as required.



Removing Backup Repositories

You can permanently remove a backup repository from the backup infrastructure. When you remove a backup repository, Veeam Backup & Replication unassigns the backup repository role from the server and this server is no longer used as a backup repository. The actual server remains in the backup infrastructure.

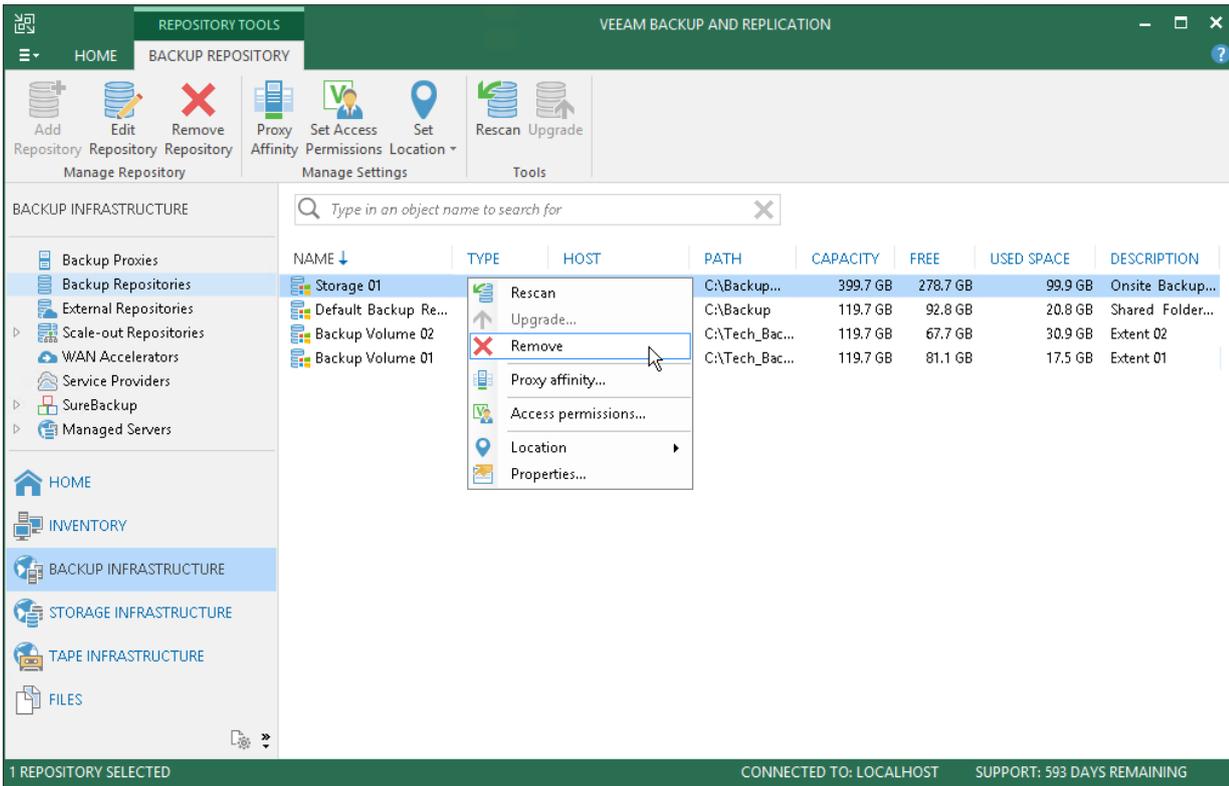
Veeam Backup & Replication does not remove backup files and other data stored on the backup repository. You can re-connect the backup repository at any time and import backups from this backup repository to Veeam Backup & Replication.

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

To remove a backup repository:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the **Backup Repositories** node.

- In the working area, select the backup repository and click **Remove Repository** on the ribbon or right-click the backup repository and select **Remove**.



External Repository

Veeam Backup & Replication allows you to add [Amazon S3](#) object storage repositories that contain backups created with N2WS Backup & Recovery.

N2WS Backup & Recovery is a Veeam solution that creates backups of [Elastic Block Stores](#) (EBS) disk volumes of [Amazon EC2](#) instances. Such backups are placed directly to Amazon S3 object storage which you can add to the Veeam Backup & Replication console as an external repository.

To upload backed-up data to Amazon S3 object storage, N2WS Backup & Recovery uses Veeam VM Backup API to preserve the backup structure in the native Veeam format.

After you add Amazon S3 object storage as an external repository to the Veeam Backup & Replication console, you can perform the following operations:

- [Restore EC2 instances to AWS](#)
- [Restore machines to Microsoft Azure](#)
- [Restore guest OS files](#)
- [Export EC2 instance disks.](#)
- [Copy EC2 backups to on-premises repositories](#)
- [Govern retention policies](#)
- [Remove EC2 backups from external repositories](#)

NOTE:

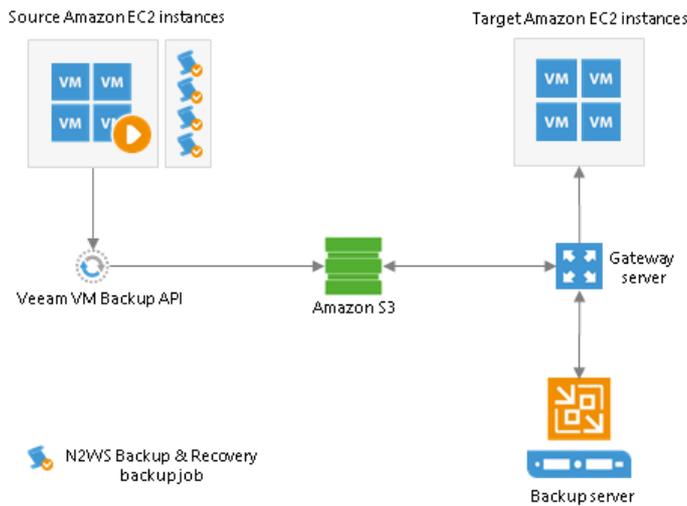
Mind the following:

- During the process of copying EC2 instance backups, or restore to Amazon EC2 or Microsoft Azure, EC2 instance data may migrate from one geographic location to another. In this case, Veeam Backup & Replication displays a warning and stores a record about data migration to job or task session details. For more information, see [Locations](#).
- You cannot use an external repository as a target for backup or backup copy jobs.

The following figure represents the overall workflow of backed-up data upload to Amazon S3 object storage by N2WS Backup & Recovery:

- The *Source Amazon EC2 instances* group represents Amazon EC2 VMs.
One of these instances is hosting the N2WS server, the backup jobs of which are backing up EBS disk volumes of EC2 VMs to the Amazon S3 object storage repository.
- N2WS Backup & Recovery uploads backed-up data to the Amazon S3 object storage repository using Veeam VM Backup API.

- The Veeam backup server accesses Amazon S3 object storage over a gateway server to fetch the storage data and restore it to *Target Amazon EC2 instances*.



How External Repository Works

Continue with this section to learn more on how external repositories work.

Ownership

Ownership defines what entity can own an Amazon S3 object storage repository at a time. Ownership protects data integrity and is implemented to adhere to the [Amazon Eventual Consistency](#) model.

How Does Taking Ownership Occur

After N2WS Backup & Recovery has finished its initial backup job session, it becomes the rightful owner of both an Amazon S3 object storage repository and backup files in that repository.

Taking ownership of such a repository along with its backup files by the Veeam Backup & Replication client consists of the following consecutive steps:

Step 1. Taking ownership of a repository.

Reclaiming ownership of a repository occurs every time a client adds Amazon S3 object storage as an external repository to the Veeam Backup & Replication console.

Step 2. Taking ownership of backup files in the repository.

Becoming an owner of backup files in Amazon S3 object storage is only possible after N2WS Backup & Recovery launches the backup job session which is referring to backups you are trying to take ownership of (i.e. backup files that are located in the repository you have added at the step one).

During its session, N2WS Backup & Recovery verifies the owner of a repository and If it finds out that the owner has been changed, it changes the owner of each backup file in that repository by creating a new checkpoint that refers to a new rightful owner. Such a checkpoint will be used during subsequent sessions of a backup job to repeat owner verification.

It is possible, however, that after you add an external repository, N2WS Backup & Recovery never launches the associated backup job again. In such a scenario, Veeam Backup & Replication will not be able to manage retention policies, but you will still be able to restore external repository data, remove backups from external repositories and perform backup copy.

Taking Ownership by Another Veeam Backup & Replication Client

Ownership of a repository along with its backup files can only be granted to one Veeam Backup & Replication client at a time.

Therefore, if a client *A* adds an external repository that has previously been added by the client *B*, the client *B* completely loses its ownership privileges.

Losing privileges means that the client *B* will no longer be able to manage retention policies. All the previously created backup copy jobs and restore sessions will be failing.

Ownership, however, can easily be reclaimed by re-adding the same Amazon S3 object storage anew.

Cache

Veeam Backup & Replication caches data that is being retrieved from external repositories every time a backup copy job or restore session is executed.

Such an approach helps not only to reduce the amount of cost-expensive operations incurred by Amazon, but also decrease the amount of traffic being sent over the network.

Consider the following:

- Cache is created on a gateway server while the following activities are being processed:
 - Backup copy jobs.
 - Restore sessions.
- Cache is not created upon the addition of Amazon S3 object storage as an external repository to the Veeam Backup & Replication console.
- Cache consists of metadata of blocks being retrieved from external repositories.
- Cache is written to:
 - On a Windows-based gateway server: `C:\ProgramData\Veeam\Backup\AmazonS3Cache`
 - On a Linux-based gateway server: `\var\veeam\backup\AmazonS3Cache`
- Cache is reused and updated during each subsequent execution of a backup copy job or restore session.
- Cache size limit is 10GB. Once reached, Veeam will purge obsolete cache by 20% preserving most frequently used parts. Purging is done by the maintenance job.
- Cache is removed in the following cases:
 - An external repository has been removed from the Veeam Backup & Replication console.
 - The gateway server has been changed in the settings of the external repository configuration.
 - The backup file has been removed from the external repository.
 - During the maintenance job session.
- Cache can be removed manually without affecting the backup infrastructure in any negative way.

Encryption

Backups in Amazon S3 object storage might be encrypted by N2WS Backup & Recovery backup jobs. Moreover, password for such encrypted backups may change on a daily basis.

For example, there is a backup chain in Amazon S3 object storage that consists of 10 restore points, each of which was encrypted with different password. Therefore, there are 10 different passwords in total that have been used.

To be able to decrypt each restore point in such a backup chain without having to provide each previously used password separately, Veeam Backup & Replication implements the ability of backward hierarchical decryption.

Backward hierarchical decryption requires only the latest password to be provided so that all the previously created restore points can be decrypted as well.

As an example, there are three restore points: A, B, and C. The point A was encrypted with password 1, B with password 2, and C with password 3. Therefore, you will only need to know the password of the C point to decrypt points C, B, and A.

Password is provided at the [Specify Cloud Storage Details](#) step of the new external repository wizard.

NOTE:

To create a backup copy job it is necessary to provide a password for encrypted backups.

Managing Retention Policy

A retention policy is set in the N2WS Backup & Recovery backup job configuration settings and defines the number of restore points to keep in Amazon S3 object storage repositories.

Retention policies are initially managed by N2WS Backup & Recovery until a Veeam Backup & Replication client reclaims ownership of a repository and all the backup files in such a repository.

Once ownership is reclaimed, N2WS Backup & Recovery ceases to govern retention policies and the Veeam Backup & Replication client becomes responsible for removing obsolete restore points from Amazon S3 object storage altogether.

The restore points that fall under the retention policy will be removed upon the next successful session of the maintenance job.

When a Veeam Backup & Replication client removes an external repository from its scope, it relinquishes its ownership which then goes directly to N2WS Backup & Recovery until another Veeam Backup & Replication client reclaims it anew and so forth.

IMPORTANT!

A retention policy can only be applied by the Veeam Backup & Replication client that is the rightful owner of an Amazon S3 object storage repository and its backup files.

Maintenance Job

The maintenance job is a system job that is executed automatically every 24 hours.

The maintenance job does the following:

- Purges obsolete restore points that fall under the retention policy.

To be able to purge obsolete restore points from external repositories due to the retention policy threshold, a Veeam Backup & Replication client must be the owner of a repository and its backup files.

- Purges cache by 20% of the size limit. By default, the size limit is 10GB.
- Saves its session results to the configuration database.

The session results can be found in the **History** view under the **System** node.

Adding External Repository

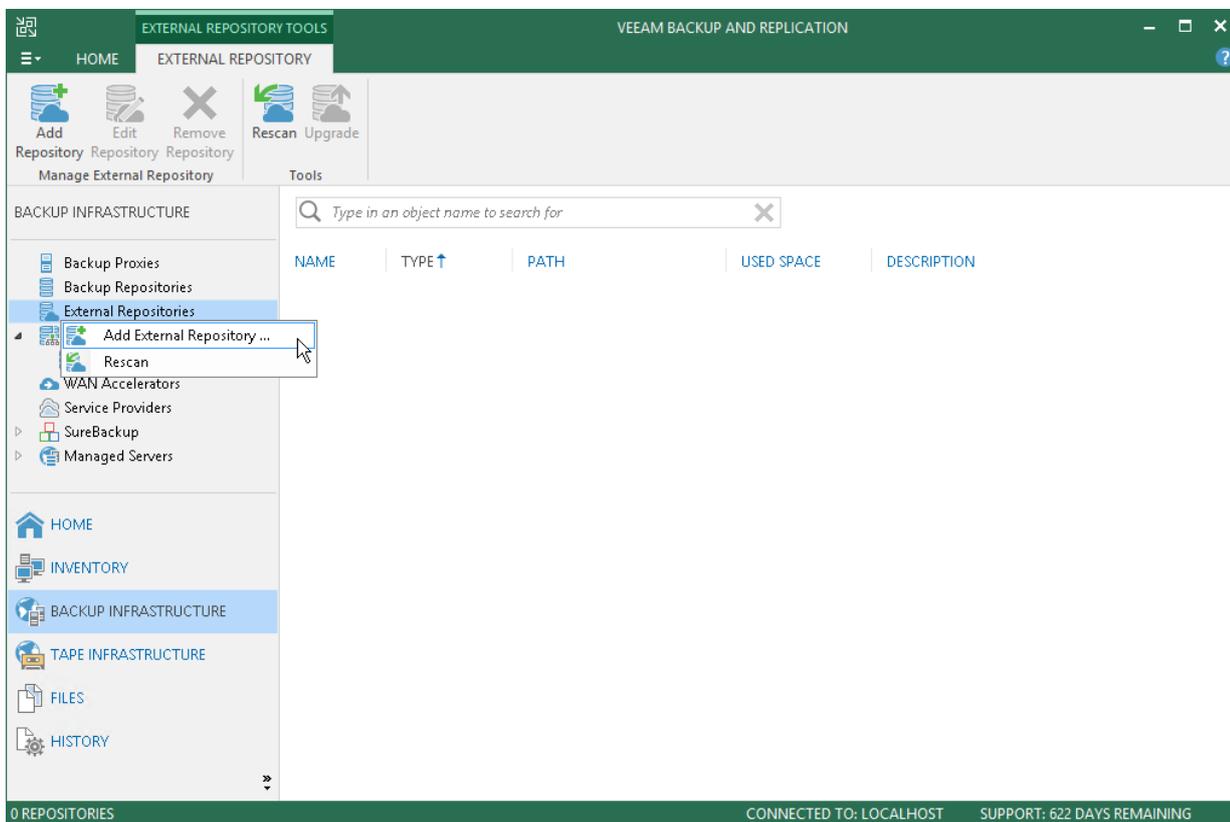
To add one or more external repositories to the backup infrastructure, do the following:

1. [Launch New External Repository Wizard](#)
2. [Specify External Repository Name and Description](#)
3. [Specify Cloud Repository Account](#)
4. [Specify Cloud Storage Details](#)
5. [Finish Working with Wizard](#)

Step 1. Launch New External Repository Wizard

To launch the **New Backup Repository** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select the **External Repositories** node and click **Add Repository** on the ribbon.
- Open the **Backup Infrastructure** view, in the inventory pane right-click the **External Repositories** node and select **Add External Repository**.

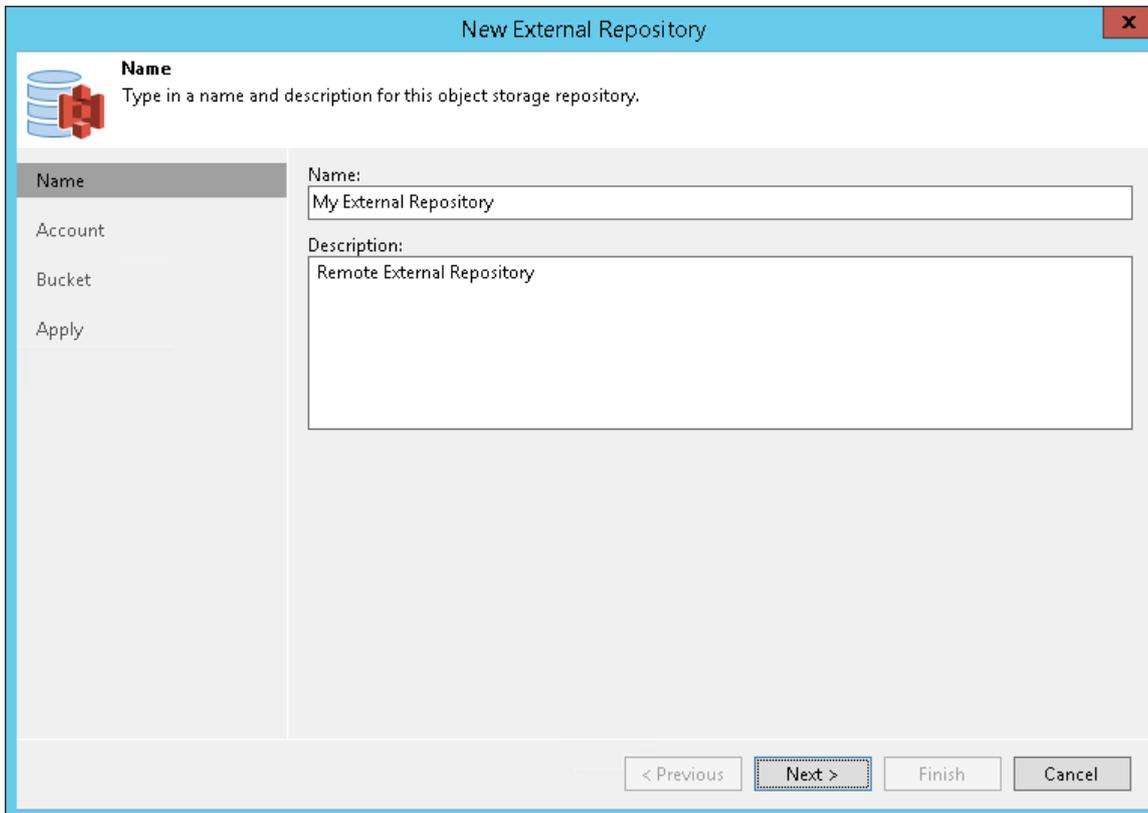


Step 2. Specify External Repository Name and Description

At the **Name** step of the wizard, specify a name and description for the external repository.

1. In the **Name** field, specify a name for the external repository.
2. In the **Description** field, provide a description for future reference.

The default description contains information about the user who added the external repository, date and time when the external repository was added.



Step 3. Specify Cloud Repository Account

At this step of the wizard, specify the following:

1. In the **Credentials** drop-down list, select valid user credentials to access your Amazon S3 object storage.

If you already have a credentials record that was configured upfront, select such a record in the drop-down list. Otherwise, click **Add** and provide your access and secret keys, as described in [Cloud Credentials Manager](#).

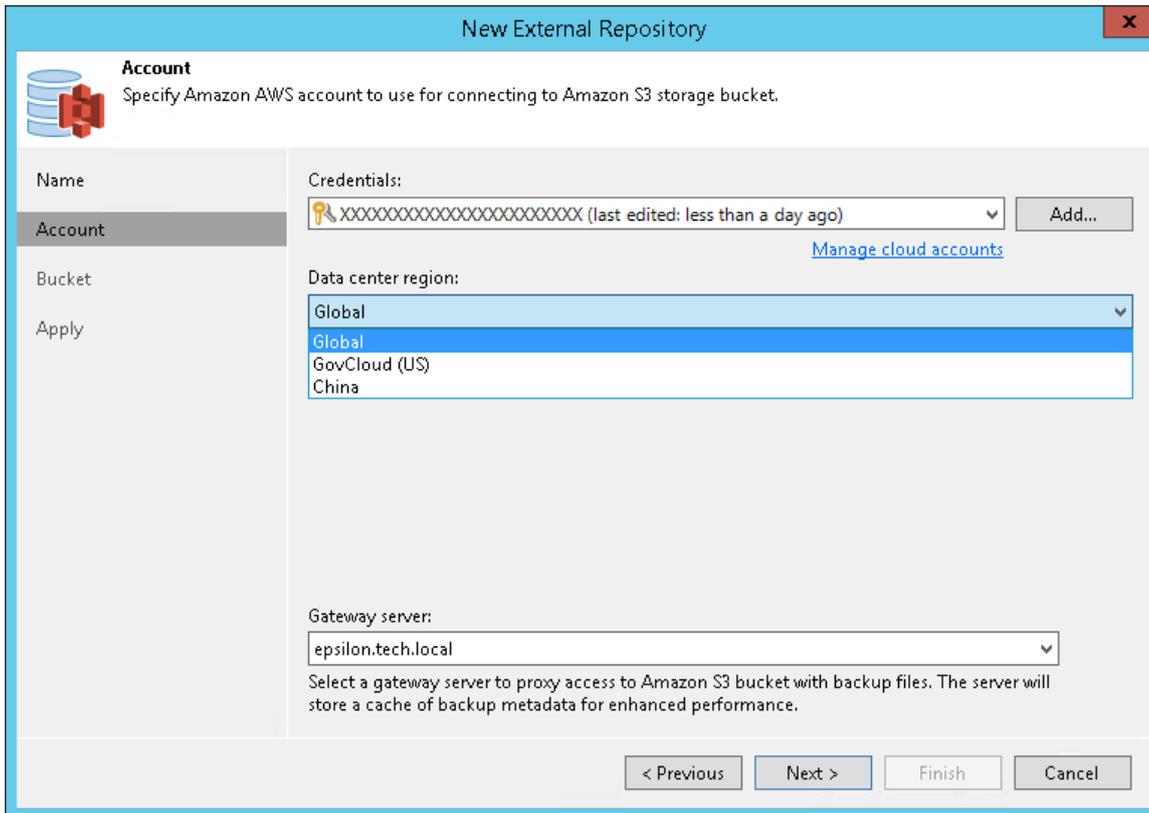
2. In the **Data center region** drop-down list, specify the region type.
3. In the **Gateway server** drop-down list, select a dedicated gateway server to access the internet.

You may need to configure such a gateway server, for example, if your organization uses NAT or different types of firewalls and your access to the internet is limited. You can use either Windows or Linux machine for this purposes. For more information on how to add such a server to your environment, see [Adding Microsoft Windows Servers](#) and [Adding Linux Servers](#) respectively.

During the addition of a gateway server, Veeam installs the *transport* service on the selected machine. The transport service is responsible for handling ingress/egress requests that are sent to/from the gateway server during working with the external repository data in Veeam Backup & Replication. If the transport service becomes outdated, it must be upgraded, as described in [Upgrading External Repositories](#).

Gateway servers also store cached data, as described in [Understanding Cache](#).

The default gateway server is the machine on which the Veeam Backup & Replication solution is installed.



Step 4. Specify Cloud Storage Details

At this step of the wizard, specify the following:

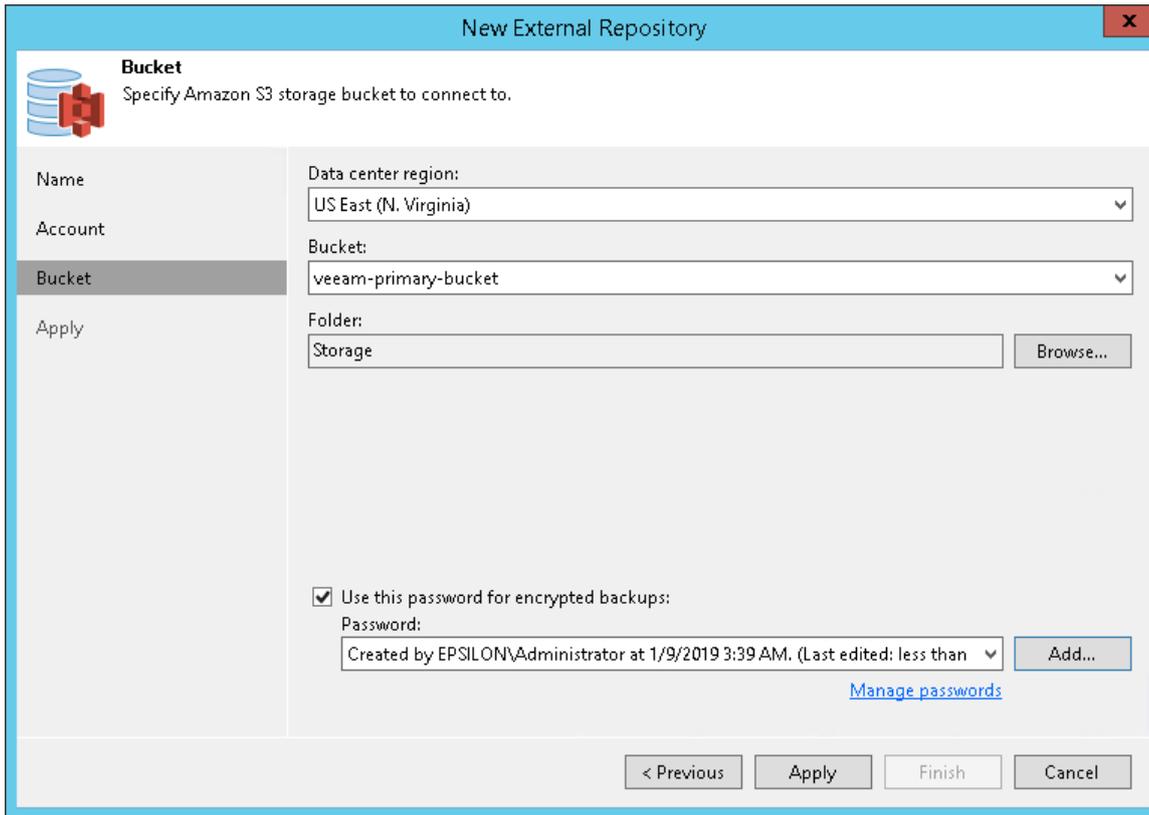
1. In the **Data center region** drop-down list, select a region that contains available buckets.
2. In the **Bucket** drop-down list, select a bucket that contains available folders.
Make sure the bucket you want to use was created upfront.
3. Click **Browse** to select a folder that contains backups created with N2WS Backup & Recovery which you want to import to your Veeam Backup & Replication console.
A folder you select at this step is also created with N2WS Backup & Recovery.

NOTE:

If another Veeam Backup & Replication client has already added the same folder, you will be prompted whether to reclaim ownership of such a folder. For more information about ownership, see [Understanding Ownership](#).

If the selected folder contains encrypted backups, select the **Use this password for encrypted backups** checkbox and provide a password. If you skip this step for encrypted backups, then such backups will be added to the **External (Encrypted)** node, as described in the [Viewing External Repository Data](#) section.

For more information about encryption, see [Encryption](#).



The screenshot shows a window titled "New External Repository" with a close button (X) in the top right corner. The window has a blue header bar. Below the header, there is a "Bucket" icon (a stack of blue disks with a red cube) and the text "Specify Amazon S3 storage bucket to connect to." On the left side, there is a vertical navigation pane with four items: "Name", "Account", "Bucket" (which is highlighted with a grey background), and "Apply". The main area of the window contains the following fields and controls:

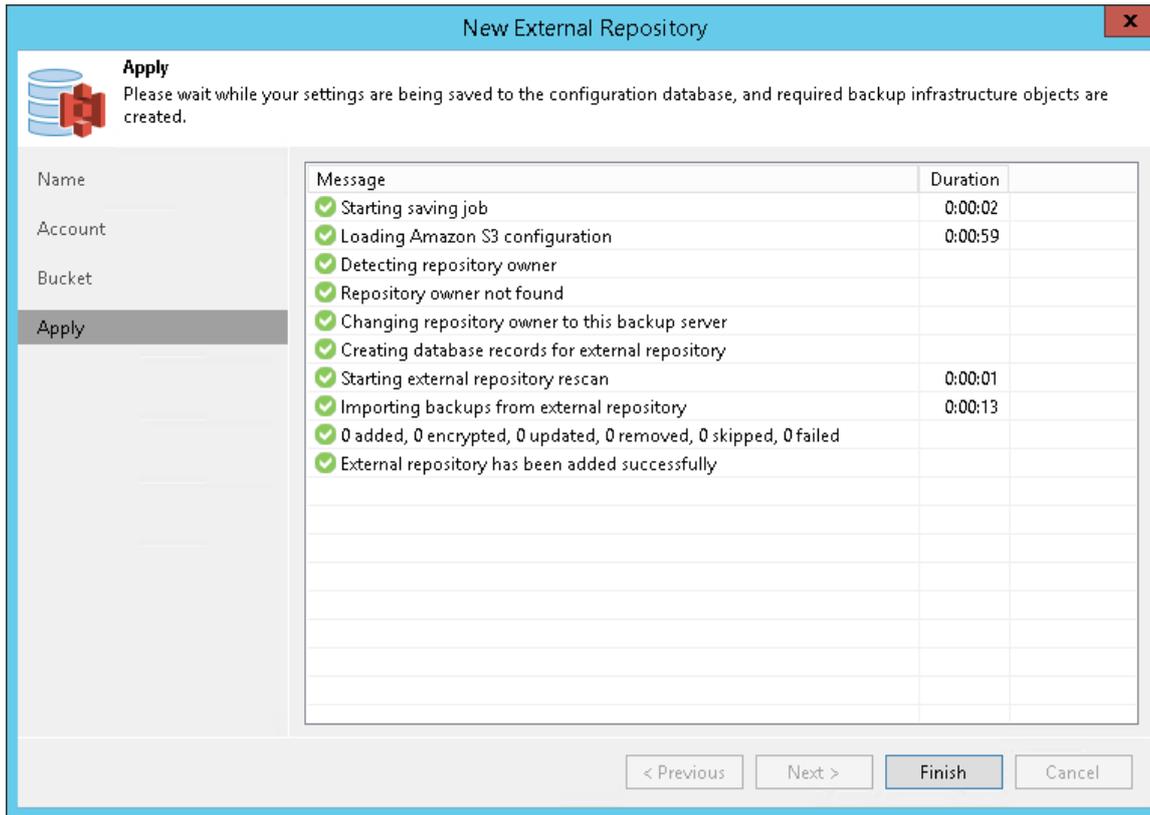
- "Data center region:" dropdown menu with "US East (N. Virginia)" selected.
- "Bucket:" dropdown menu with "veeam-primary-bucket" selected.
- "Folder:" text input field containing "Storage" and a "Browse..." button to its right.
- A checked checkbox labeled "Use this password for encrypted backups:".
- A "Password:" text input field containing "Created by EPSILON\Administrator at 1/9/2019 3:39 AM. (Last edited: less than" and a dropdown arrow.
- An "Add..." button to the right of the password field.
- A blue link labeled "Manage passwords" below the password field.

At the bottom of the window, there are four buttons: "< Previous", "Apply", "Finish", and "Cancel".

Step 5. Finish Working with Wizard

At the **Apply** step of the wizard, wait until Veeam establishes a connection to Amazon S3 object storage and click **Finish**.

To learn how to view external repository backups, see [Viewing External Repository Data](#).



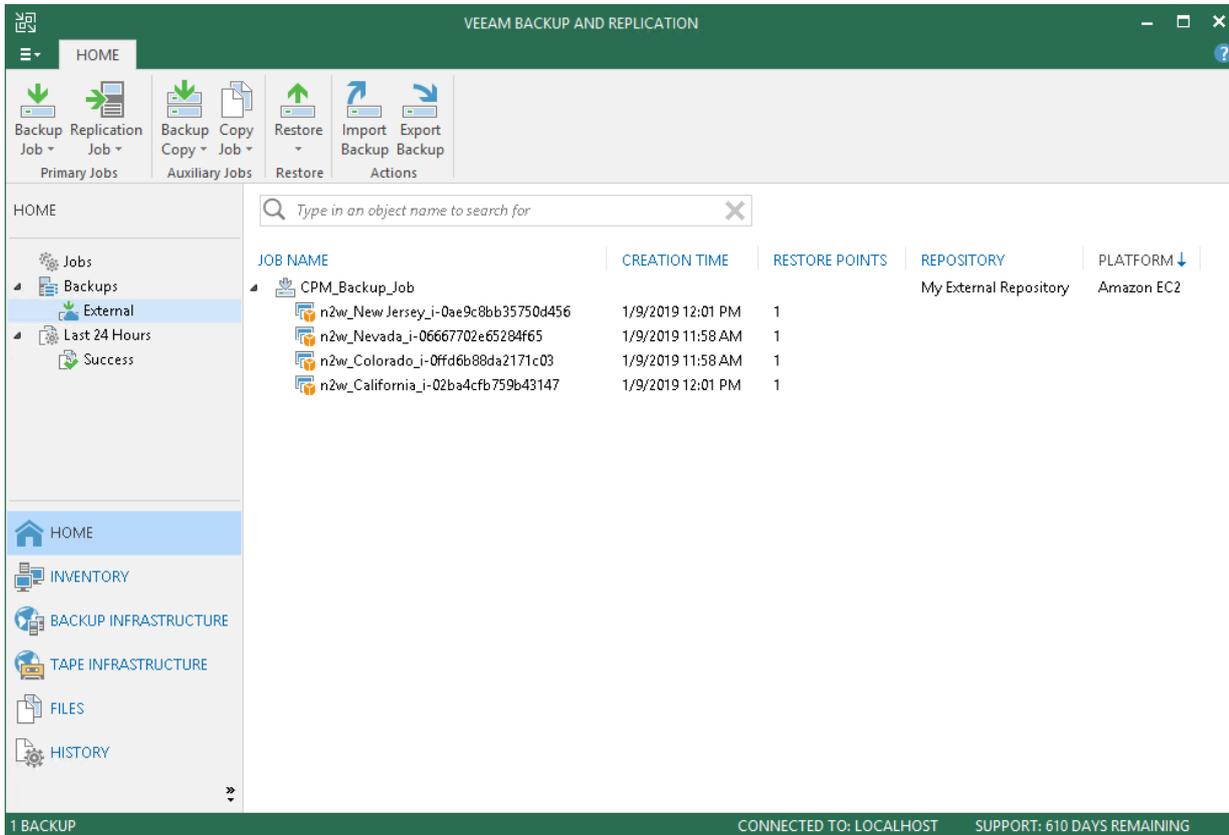
Viewing External Repository Data

Once you have added an external repository, the following nodes become available in the **Home** view, under the **Backups** node:

- **External.** Under this node, you can find all the backups that are not encrypted or were decrypted explicitly by providing a password at the [Specify Cloud Storage Details](#) step.

- **External (Encrypted).** This node contains encrypted backups only.

To decrypt such backups, select a backup job and click **Specify Password** on the ribbon menu. Then, provide a password and click **OK**.



Restoring and Copying Data from External Repository

You can perform the following data protection and disaster recovery operations with Amazon EC2 instances:

- [Restore EC2 instances to AWS](#)
- [Restore machines to Microsoft Azure](#)
- [Restore guest OS files](#)
- [Copy EC2 backups to on-premises repositories](#)

Removing Backups from External Repository

If you want to remove EC2 instance backups from external repositories, you can use the **Delete from disk** operation.

Consider the following:

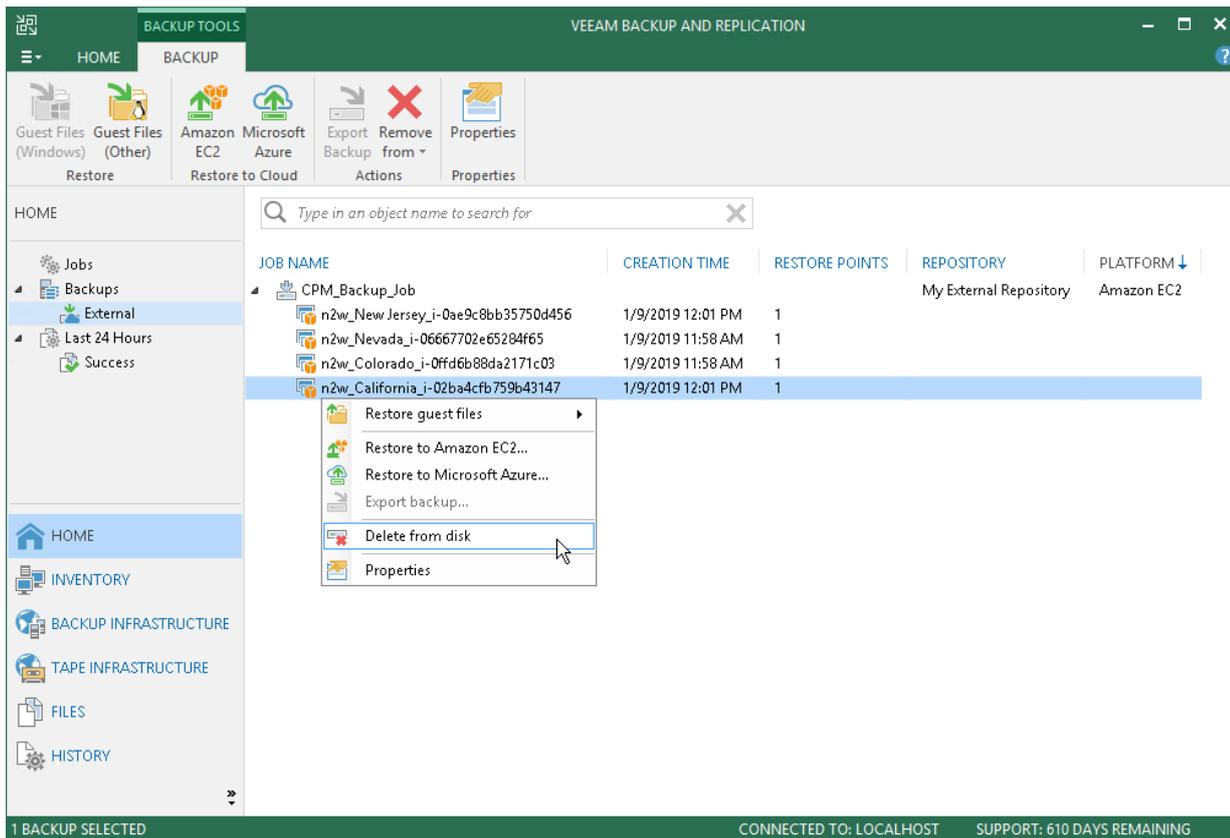
- Data will be removed from the Veeam Backup & Replication console, configuration database and associated Amazon S3 object storage repository.
- Data cannot be removed if the maintenance job is in progress.
- Data cannot be removed if at least one restore session of external repository data is in progress.

- Ownership is not required to remove data from external repositories.

To remove EC2 instance backups from an external repository, do the following:

1. Open the **Home** view.
2. In the inventory pane, expand the **Backups** node and click **External**.
3. In the working area, select a backup or a separate EC2 instance in the backup and click **Remove from > Disk** on the ribbon.

Alternatively, you can right-click a backup or an EC2 instance and select **Delete from disk**.



Rescanning External Repository

To synchronize your external repository state with that of Amazon S3 object storage, you can use the rescan feature.

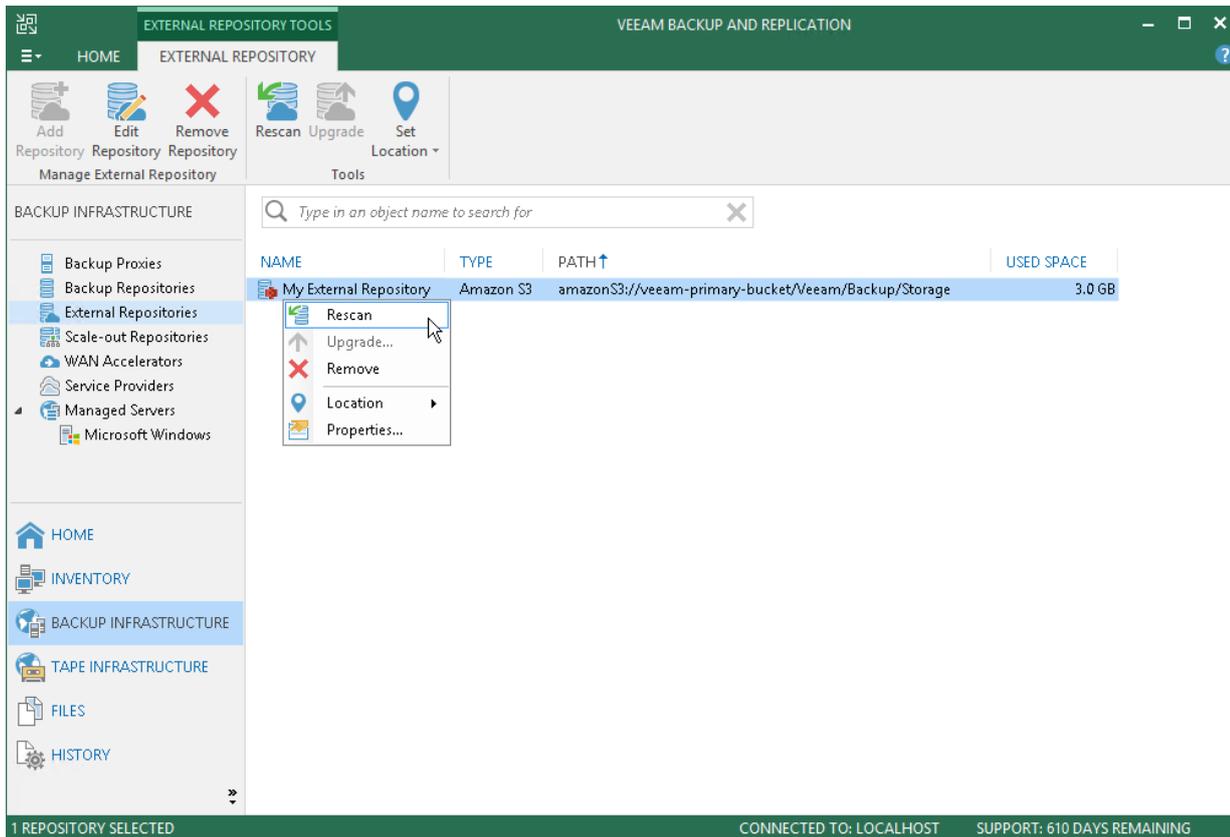
Consider the following:

- By default, rescan is done automatically every 24 hours and synchronizes your external repository state with that of Amazon S3 object storage to fetch newly created restore points and other required metadata.
- Rescan is done automatically upon the addition of a new external repository to the application scope.
- Rescan session results are saved to the configuration database and can be found in the **History** view under the **System** node.

To rescan external repositories manually, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **External Repositories**.
3. Select a repository you want to rescan and click **Rescan** on the ribbon menu or right-click a repository and select **Rescan**.

If you have more than one external repository added to the scope, you may want to rescan all the repositories altogether. For that, right-click the root **External Repositories** node in the navigation pane and select **Rescan**.



Upgrading External Repositories

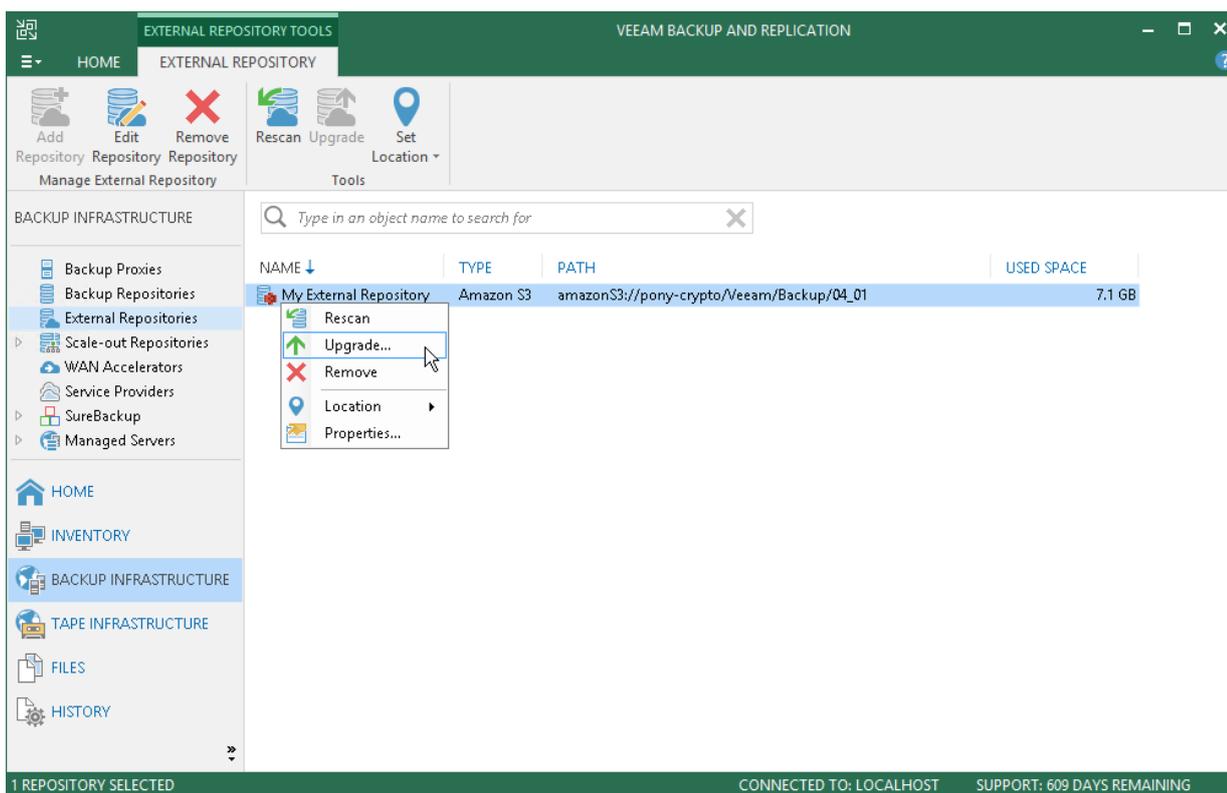
Upgrade of external repositories allows you to upload a new version of the *transport* service which is responsible for handling ingress/egress requests that are sent to/from the gateway server during working with the external repository data in Veeam Backup & Replication.

Upload of the *transport* service is done directly to a gateway server which you specify at the [Specify Cloud Repository Account](#) step of the **New External Repository** wizard.

To upgrade an external repository, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **External Repositories**.

3. Select a repository you want to upgrade and click **Upgrade** on the ribbon menu or right-click a repository and select **Upgrade**.



Removing External Repositories

You can remove any external repository from the application scope if you no longer need it.

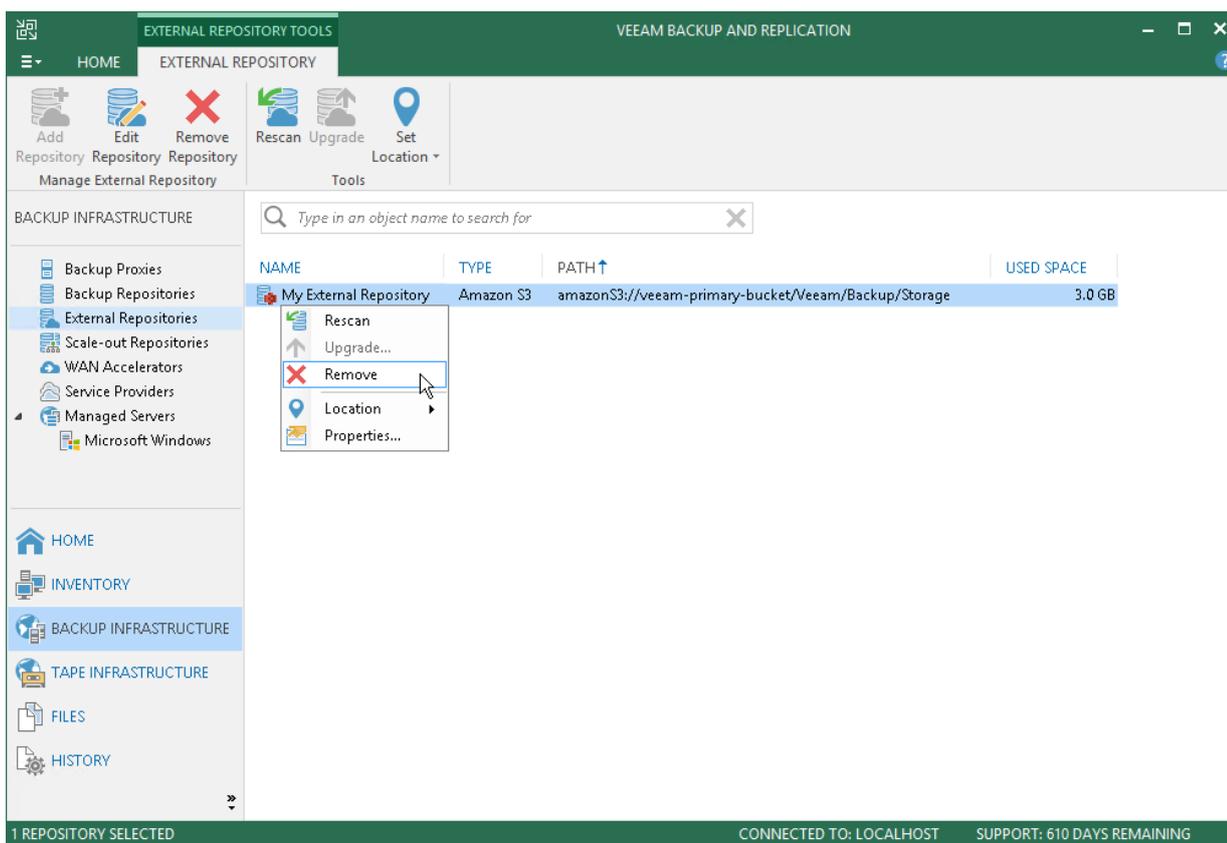
When an external repository is being removed, Veeam does the following:

- Removes the corresponding checkpoint in associated Amazon S3 object storage to relinquish ownership (if any).
- Removes associated external repository records from the configuration database.
- Removes associated cache from the gateway server.

To remove an external repository, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **External Repositories**.

3. In the working area, select an external repository and click **Remove Repository** on the ribbon or right-click the external repository and select **Remove**.



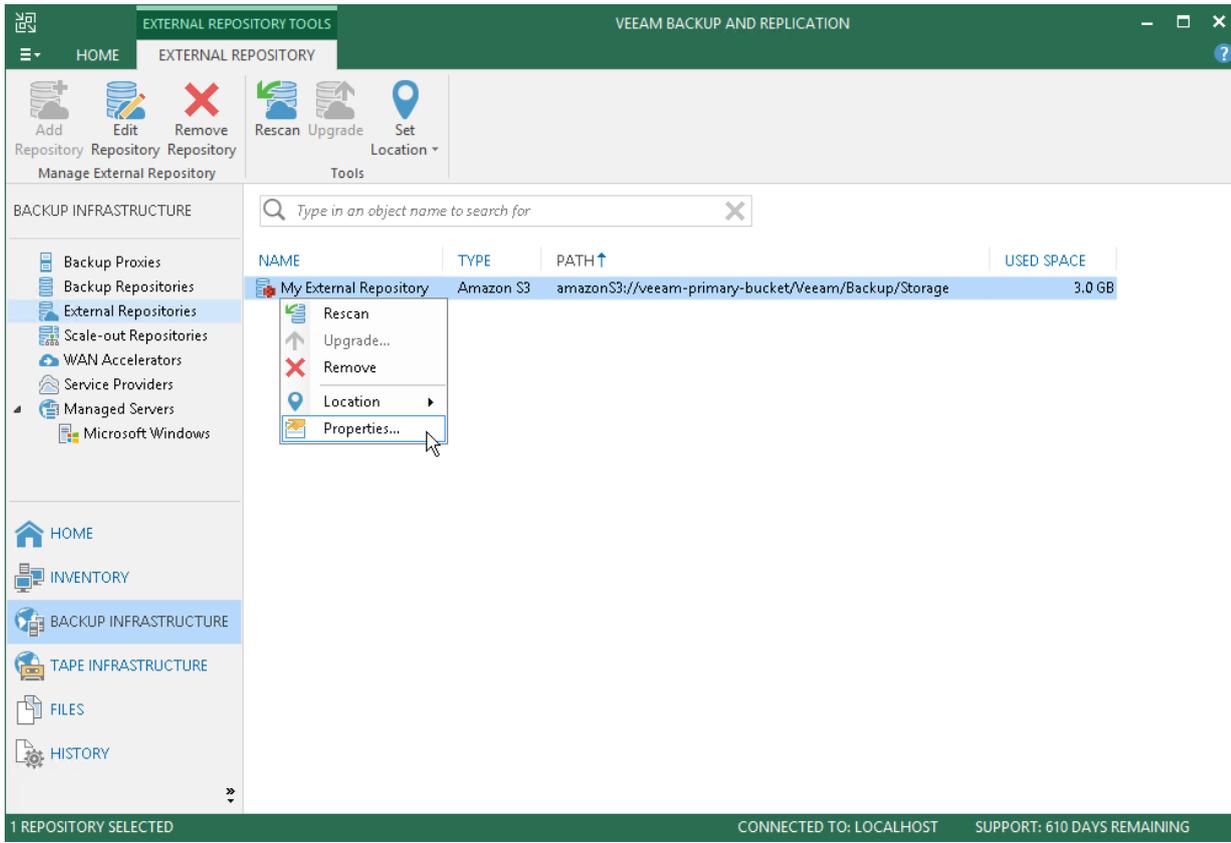
Editing Settings of External Repository

After you have added an external repository, you may want to edit its settings.

To edit external repository settings, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **External Repositories**.
3. In the working area, select an external repository and click **Edit Repository** on the ribbon or right-click the external repository and select **Properties**.

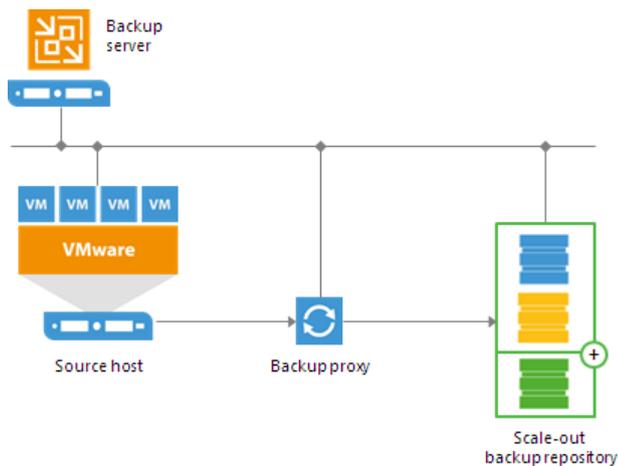
4. Follow the steps of the **Edit External Repository** wizard and edit settings as required.
Mind that some settings cannot be modified and will remain disabled during editing.



Scale-Out Backup Repository

You can configure a scale-out backup repository in the backup infrastructure. The scale-out backup repository is a logical entity – it groups several backup repositories called extents. When you configure the scale-out backup repository, you actually create a pool of storage devices and systems, summarizing their capacity. For long-term storage, you can instruct Veeam Backup & Replication to offload data from extents to the cloud. For details, see [Capacity Tier](#).

You can expand the scale-out backup repository at any moment. For example, if backup data grows and the backup repository reaches the storage limit, you can add a new storage system to the scale-out backup repository. The free space on this storage system will be added to the capacity of the scale-out backup repository. As a result, you will not have to move backups to a backup repository of a larger size.



To deploy a scale-out backup repository, you must configure a number of backup repositories and add them to a scale-out backup repository as extents. You can mix backup repositories of different types in one scale-out backup repository:

- Microsoft Windows backup repositories
- Linux backup repositories
- Shared folders
- Deduplicating storage appliances

For example, you can add a Microsoft Windows backup repository and deduplicating storage appliance to the same scale-out backup repository.

A scale-out backup repository can be used for the following types of jobs and tasks:

- Backup jobs.
- Backup copy jobs.
You can copy backups that reside on scale-out backup repositories and store backup copies on scale-out backup repositories.
- VeeamZIP tasks.
- Backup jobs created by Veeam Agent for Linux 2.0 or later.
- Backup jobs created by Veeam Agent for Microsoft Windows 2.0 or later.

Backup files stored on the scale-out repository can be used for all types of restores, replication from backup and backup copy jobs. You can verify such backups with SureBackup jobs. The scale-out backup repository can be used as a staging backup repository for restore from tape media. Files restored from the tape media are placed to the extents according to data placement policy configured for the scale-out backup repository. For more information, see [Backup File Placement](#).

Limitations for Scale-out Backup Repositories

The scale-out backup repository has the following limitations:

- The scale-out backup repository functionality is available only in Enterprise and Enterprise Plus editions of Veeam Backup & Replication.

If you configure a scale-out backup repository and then downgrade to the Standard license, you will not be able to run jobs targeted at the scale-out backup repository. However, you will be able to perform restore from the scale-out backup repository.

- You cannot use the scale-out backup repository as a target for the following types of jobs:
 - Configuration backup job
 - Replication jobs (including replica seeding)
 - VM copy jobs
 - Veeam Agent backup jobs created by Veeam Agent for Microsoft Windows 1.5 or earlier and Veeam Agent for Linux 1.0 Update 1 or earlier.
- You cannot add a backup repository as an extent to the scale-out backup repository if any job of unsupported type is targeted at this backup repository or if the backup repository contains data produced by jobs of unsupported types (for example, replica metadata). To add such backup repository as an extent, you must first target unsupported jobs to another backup repository and remove the job data from the backup repository.
- Scale-out backup repositories do not support rotated drives. If you enable the **This repository is backed by rotated hard drives** setting on an extent, Veeam Backup & Replication will ignore this setting and will work with such repository as with a standard extent.
- If a backup repository is added as an extent to the scale-out backup repository, you cannot use it as a regular backup repository.
- You cannot add a scale-out backup repository as an extent to another scale-out backup repository.
- You cannot add a backup repository as an extent if this backup repository is already added as an extent to another scale-out backup repository.
- You cannot add a backup repository as an extent if this backup repository is already used as a backup destination by vCloud Director organizations.
- You cannot add a backup repository on which some activity is being performed (for example, a backup job or restore task) as an extent to the scale-out backup repository.
- If you use Enterprise Edition of Veeam Backup & Replication, you can create 2 scale-out backup repositories.

For each scale-out backup repository, you can add 1 object storage repository and 4 extents: 3 active, and 1 inactive (that is put to the Maintenance mode). You can add inactive extents, for example, if any of active extents has no free space, and you want to evacuate backup data from it.

If you add 4 extents and do not put any of them to the Maintenance mode, the jobs targeted at the scale-out backup repository will fail.

Enterprise Plus Edition has no limitations on the number of scale-out backup repositories or extents.

- The Extract and Backup Validator utilities do not work with backups stored on scale-out backup repositories.
- To let Veeam Backup & Replication automatically import backups during rescan of a scale-out backup repository, names of VBM files and paths to VBM files (starting from the backup repository root to VBM files) must contain only allowed characters:
 - Alphanumeric characters: a-zA-Z0-9
 - Special characters: _-+=@^

Names of VBM file and paths to VBM files must not contain spaces.

If a name of the VBM file or path to the VBM file contains prohibited characters, Veeam Backup & Replication will fail to import such backup during rescan of the scale-out backup repository. To import such backup, you can replace prohibited characters with the underscore character, for example: `C:\My Repository\Backup_Job\Backup_Job.vbm`. You do not need to rename backup files themselves.

- Veeam Backup & Replication does not split one backup file across multiple extents.

Extents

The scale-out backup repository can comprise one or more extents. The extent is a standard backup repository configured in the backup infrastructure. You can add any backup repository, except the cloud repository, as an extent to the scale-out backup repository.

The backup repository added to the scale-out backup repository ceases to exist as a backup repository. You cannot target jobs to this backup repository. Instead, you have to target jobs to the configured scale-out backup repository.

On every extent, Veeam Backup & Replication creates the `definition.erm` file. This file contains a description of the scale-out backup repository and information about its extents.

Extents inherit most configuration settings from the underlying backup repositories. The following settings are inherited:

- Number of tasks that can be performed simultaneously
- Read and write data rate limit
- Data decompression settings
- Block alignment settings

The following settings are not inherited:

- Rotated drive settings. Rotated drive settings are ignored and cannot be configured at the level of the scale-out backup repository.
- Per-VM backup file settings. Per-VM settings can be configured at the level of the scale-out backup repository.

Limitations, specific for certain types of backup repositories, apply to extents. For example, if you add Dell EMC Data Domain as an extent to the scale-out backup repository, you will not be able to create a backup chain longer than 60 points on this scale-out backup repository.

Extents of the scale-out backup repository should be located in the same site. Technically, you can add extents that reside in different sites to the scale-out backup repository. However, in this case Veeam Backup & Replication will have to access VM backup files on storage devices in different locations, and the backup performance will degrade.

Backup File Placement

Veeam Backup & Replication stores backup files on all extents of the scale-out backup repository.

When you configure a scale-out backup repository, you must set the backup file placement policy for it. The backup file placement policy describes how backup files are distributed between extents. You can choose one of two policies:

- [Data locality](#)
- [Performance](#)

The backup file placement policy is not strict. If the necessary extent is not accessible, Veeam Backup & Replication will disregard the policy limitations and attempt to place the backup file to the extent that has enough free space for the backup file.

For example, you have set the Performance policy for the scale-out backup repository and specified that full backup files must be stored on *Extent 1* and incremental backup files must be stored on *Extent 2*. If before an incremental backup job session *Extent 2* goes offline, the new incremental backup file will be placed to *Extent 1*.

Data Locality

If you set the Data locality policy for a scale-out backup repository, all backup files that belong to the same backup chain are stored on the same extent of the scale-out backup repository.

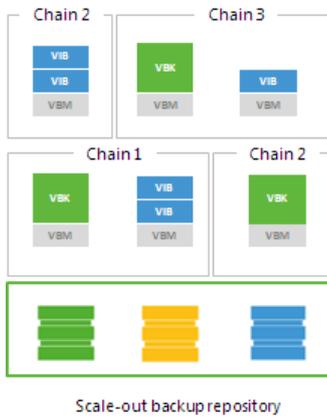


The Data locality policy does not put any limitations to backup chains. A new backup chain may be stored on the same extent or another extent. For example, if you create an active full backup, Veeam Backup & Replication may store the full backup file to another extent, and all dependent incremental backup files will be stored together with this full backup file.

However, if you use a deduplicating storage appliance as an extent to the scale-out backup repository, Veeam Backup & Replication will attempt to place a new full backup (active or synthetic) to the extent where the full backup from the previous backup chain resides. Such behavior will help increase the data deduplication ratio.

Performance

If you set the Performance policy for a scale-out backup repository, full backup files and incremental backup files that belong to the same backup chain are stored on different extents of the scale-out backup repository. If necessary, you can explicitly specify on which extents full backup files and incremental backup files must be stored.



The Performance policy can improve performance of transform operations if you use raw data devices as extents. When Veeam Backup & Replication performs transform operations, it needs to access a number of backup files on the backup repository. If these files are located on different storage devices, the I/O load on the devices hosting backup files will be lower.

If you set the Performance policy, you must make sure that the network connection between extents is fast and reliable. You must also make sure all extents are online when the backup job, backup copy job or a restore task starts. If any extent hosting backup files in the current backup chain is not available, the backup chain will be broken, and Veeam Backup & Replication will not be able to complete the task. To avoid data loss in this situation, you can enable the **Perform full backup when required extent is offline** option for the scale-out backup repository. With this option enabled, Veeam Backup & Replication will create a full backup instead of incremental backup if some files are missing from the backup chain.

Extent Selection

To select an extent for backup file placement, Veeam Backup & Replication checks the following conditions:

1. Availability of extents on which backup files reside. If some extent with backup files from the current backup chain is not accessible, Veeam Backup & Replication will trigger a full backup instead of incremental (if this option is enabled). For more information, see [Adding Backup Repository Extents](#).
2. Backup placement policy set for the scale-out backup repository.
3. Load control settings – maximum number of tasks that the extent can process simultaneously.
4. Amount of free space available on the extent – the backup file is placed to the extent with the most amount of free space.
5. Availability of files from the current backup chain – extents that host incremental backup files from the current backup chain (or current VM) have a higher priority than extents that do not host such files.

Extent Selection for Backup Repositories with Performance Policy

If you set the Performance policy for the scale-out backup repository, Veeam Backup & Replication always stores full backup files and incremental backup files that belong to the same backup chain on different extents. To choose the extent to which a backup file can be stored, Veeam Backup & Replication applies this policy and policies mentioned above.

For example, a scale-out backup repository has 2 extents that have 100 GB and 200 GB of free space. You set the Performance policy for the scale-out backup repository and define that all types of backup files (full and incremental) can be placed on both extents.

When a backup job runs, Veeam Backup & Replication picks the target extent in the following manner:

1. During the first job session, Veeam Backup & Replication checks to which extent a full backup file can be stored. As both extents can host the full backup file, Veeam Backup & Replication checks which extent has more free space, and picks the extent that has 200 GB of free space.
2. During incremental job session, Veeam Backup & Replication checks to which extent an incremental backup file can be stored. As both extents can host the incremental backup file, Veeam Backup & Replication picks the extent that does not store the full backup file – the extent that has 100 GB of free space.

Backup Size Estimation

At the beginning of the job session, Veeam Backup & Replication estimates how much space the backup file requires and checks the amount of free space on extents. Veeam Backup & Replication assumes that the following amount of space is required for backup files:

- The size of a full backup file is equal to 50% of source VM data.
- The size of an incremental backup file is equal to 10% of source VM data.

In case of reverse incremental backup chains, during incremental job sessions Veeam Backup & Replication allocates 10% of source VM data on the extent where a rollback file is placed and additional 10% on the extent where the full backup file resides.

This mechanism is also applied to backup files created with backup copy jobs.

Mind the following:

- On every extent of a scale-out backup repository, Veeam Backup & Replication reserves 1% of storage space to guarantee correct update of backup metadata files (VBM) and success of merge operations.
- Make sure that you have enough free space on the extent where the full backup file resides. Veeam Backup & Replication requires 10% of the size of the full backup file to perform merge operations in the backup chain. If the disk space is low, merge operations may fail.
- Veeam Backup & Replication does not timely update the information about the amount of free space on the extent, if several active tasks are targeted at this extent. For more information, see the [Veeam KB2282](#) article.

Capacity Tier

Capacity Tier augments your scale-out backup repository abilities and allows you to store your backup data in cloud-based object storage such as:

- Amazon S3
- Microsoft Azure Blob Storage

- IBM Cloud Object Storage
- S3 Compatible

Such an approach helps you comply with possible data storage regulations your organization might be adhering to. For example, you might be running out of space, as your extents are only capable of keeping no more than 10 restore points at a time, or your organization policies allow you to store only certain amount of data on your extents, whereas the rest of the data should be stored elsewhere because of its outdated state.

To safely reclaim valuable storage space on your on-premises devices and make it easier to place the backup data to cloud repositories, Veeam Backup & Replication implements proprietary mechanisms that help you efficiently offload your data from the extents to cloud-based object storage every 4 hours.

NOTE:

Before start using Capacity Tier as an object storage repository, make sure to check your cloud storage provider pricing plans to avoid additional costs that might be incurred when offloading and downloading your backup data.

How Capacity Tier Works

A typical capacity tier environment consists of one or more scale-out backup repositories that encompasses the following:

- One or more extents.
- One object storage repository.

Every 4 hours Veeam collects the backup data from the extents and transfers it to object storage according to policies that define how and when such data should be offloaded.

To offload the backup data, Veeam uses the **SOBR Offload** job, which does the following:

- Verifies whether backup chains located on the extents satisfy validation criteria and, therefore, must be offloaded to object storage.
- Collects verified backup chains from each extent and sends them directly to object storage in the form of blocks.
- Saves each session results to the configuration database so that you can review them upon request.

For more information, see [SOBR Offload Job](#).

Configuring Capacity Tier

To configure a capacity tier environment, do the following:

- Add one or more backup repositories (or use existing ones) that would be used as your extents.
For more information, see [Adding Backup Repositories](#).
- Add an object storage repository that is targeted to a cloud-based object storage.
For more information, see [Adding Object Storage Repositories](#).
- Create a scale-out backup repository (or modify an existing one) and add the extents you have created at the step one.
For more information, see [Adding Scale-Out Repositories](#).

- Augment your scale-out backup repository with an object storage repository and configure policies that will define how and when your backup data should be offloaded.

For more information, see [Add Capacity Tier](#).

- Create a backup job and map this job to a scale-out backup repository.

For more information, see [Specify Backup Storage Settings](#).

Managing Capacity Tier Data

You can do the following with the backup data in object storage:

- Restore offloaded backup data directly from object storage back to your production servers or to Azure or Amazon EC2 cloud platforms.

For more information, see [Data Restore](#).

- Download offloaded backup data from object storage back to the source extents.

For more information, see [Managing Capacity Tier Data](#).

- Manage retention policies to purge obsolete restore points from both the extents and object storage.

For more information, see [Retention Policy](#).

Data Transfer

To manage capacity tier data, Veeam uses the following jobs:

- The **SOBR Offload** job.

This job offloads data from the extents to object storage repositories and is executed in the following manner:

- Every 4 hours.
- When you use the **Move to capacity tier** option, as described in [Moving to Capacity Tier](#).

- The **SOBR Download** job.

This job is executed when you copy data from object storage repositories back to the source extents using the **Copy to performance tier** option, as described in [Copying to Performance Tier](#).

SOBR Offload Job

To collect your data from the extents and transfer it to object storage repositories, Veeam uses the *Offload* job which is executed automatically every 4 hours.

The complete name of the offload job is built up of a scale-out backup repository name + the *Offload* prefix. That is, if your scale-out backup repository name is Amazon, then the offload job session name will be *Amazon Offload*.

The offload job governs the following:

- [Validation Process](#)
- [Data Transfer](#)

Validation Process

Before your data can safely be offloaded to object storage repositories, Veeam performs the following mandatory verifications and required actions:

- Verifies whether data that is about to be offloaded belongs to an inactive backup chain.
For more information, see [Backup Chain Legitimacy](#).
- Verifies whether source extents are available and have not been put into maintenance mode.
Consider that data will not be offloaded from Linux-based extents that have internet access via HTTP(S) proxy. All Linux-based extents configured in your scale-out backup repository must have direct access to the internet.
- Verifies whether an object storage repository has not been put into maintenance mode.
For more information, see [Switching to Maintenance Mode](#).
- Verifies whether policies that define how and when the backup data should be offloaded are met.
Policies are configured, as described in [Add Capacity Tier](#).
- Builds and maintains indexes to verify whether data that is being transferred is unique and has not been offloaded earlier.
For more information, see [Indexes](#).
- Synchronizes the backup chain state between the local and object storage repository to maintain retention policies.
For more information, see [Retention Policy](#).

Data Transfer

After the validation process is complete, the **SOBR Offload** job does the following:

- Collects backup files that have passed verification.
Such verified backup files are collected from all the extents added to a scale-out backup repository.
- Extracts data blocks from these files and offloads these blocks to object storage, leaving the backup files only with metadata (i.e. free of data blocks).

Such backup files (without data blocks) will remain on the source extents and will also be replicated to the object storage repository.

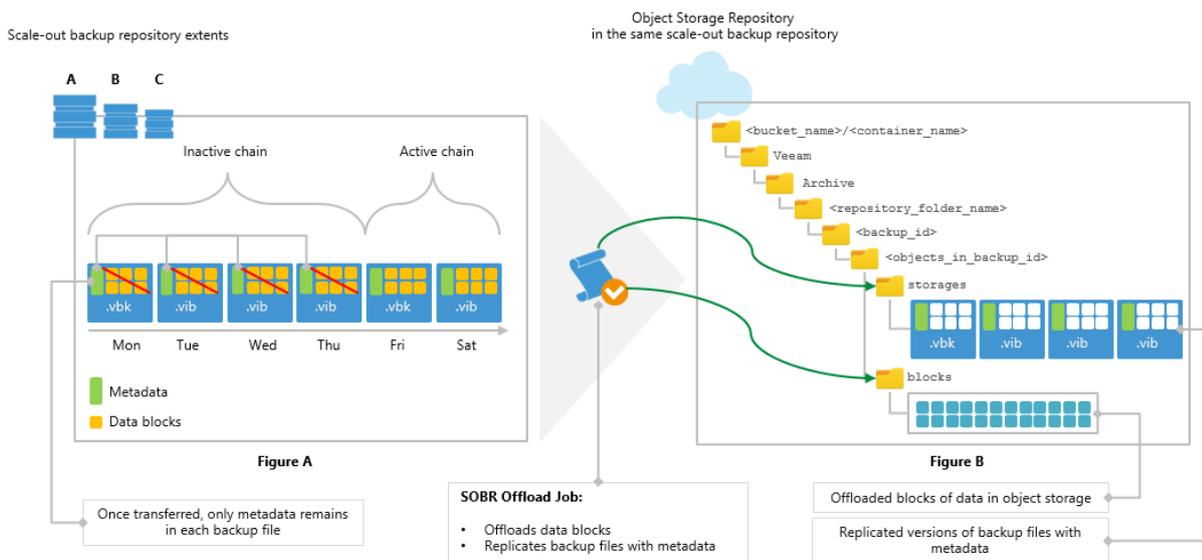
Having a copy of these files on your extents allows you to:

- Download offloaded data back to the extents, as described in [SOBR Download Job](#).
- Restore your data back to production servers, as described in [Data Restore](#).

Having replicated versions of these files in object storage repositories allows you to:

- Synchronize the backup chain state of your object storage with that of your extents, as described in [Synchronizing Capacity Tier Data](#).

The following figure illustrates an abstract transfer process.



The *Figure A* demonstrates a pool of extents (*A*, *B* and *C*) that are added to a scale-out backup repository (SOBR) and an object storage repository that is added to the same SOBR.

Suppose that the extent *A* has an inactive backup chain consisting of one *.vbk* file and three *.vib* files, that is, four restore points in total. Each of these files comprises metadata (represented as green vertical blocks) and the actual blocks of data (represented as yellow squares). During the offload session, Veeam will collect all the orange squares – that is, actual blocks of data – from all the backup files (*.vbk* and *.vib*) and offload these blocks to the object storage repository represented in the *Figure B*.

Each offloaded block might be of different size, which is defined during configuring storage optimization. The offloaded blocks are placed to the *blocks* directory of your object storage repository.

Backup files with metadata will also be replicated to the object storage repository and will be placed to the *storages* directory. As per example, these files are one *.vbk* file and three *.vib* files shown in the *Figure B*.

Such an approach will be applied to all inactive backup chains of all the extents added to SOBR.

Offload Session Statistics

The offload job session results are saved to the configuration database and available for viewing, as described in [Viewing Offload Job Session Results](#).

SOBR Download Job

The **SOBR Download** job is initiated right after you select the **Copy to performance tier** option. The job collects offloaded blocks of data from object storage repositories and copies them back to the source extents from which these blocks were once offloaded. For more information, see [Copying to Performance Tier](#).

Consider the following:

- Before copying requested data blocks, Veeam verifies whether any of such blocks exist on any of the extents of your scale-out backup repository. If found, Veeam uses these blocks instead of downloading the exact same blocks of data from the object storage repository.
- If a source extent is unable to accommodate data being copied due to lack of free storage space, Veeam will find another extent within the associated scale-out backup repository that has sufficient storage capacity to receive the data. If your scale-out backup repository has no extents other than the one running out of space, the copy will not be possible.

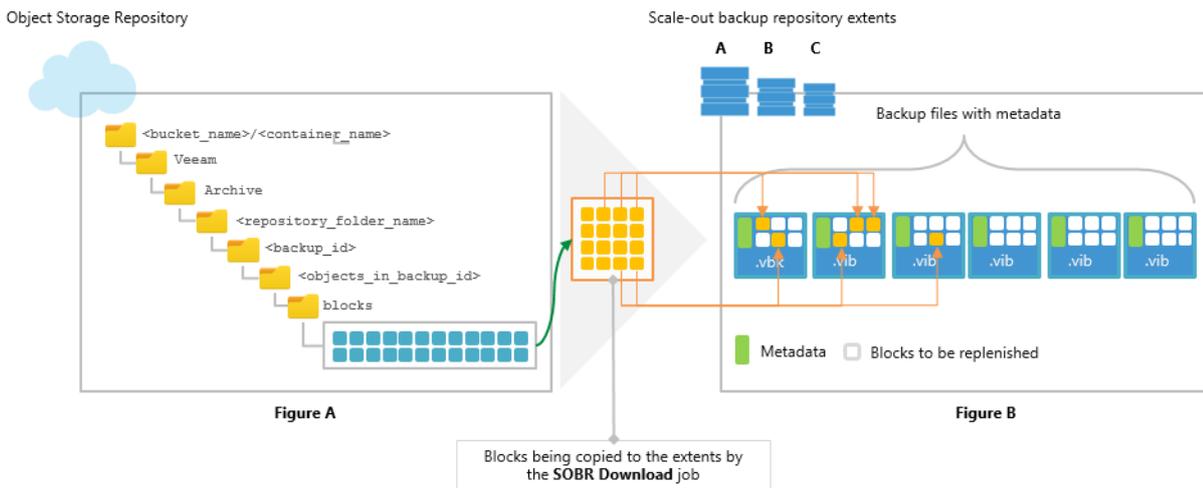
- If you have removed any of your extents from a scale-out backup repository without evacuating backup files with metadata, the copy will not be possible.

Backup files with metadata are created, as described in [SOBR Offload Job](#).

- The **SOBR Download** job session results are saved to the configuration database and available for viewing, as described in [Viewing Download Job Session Results](#).

The following figure shows an example of replenishing on-premises storage with the data blocks being copied from the object storage repository.

- The *Figure A* represents an object storage repository containing blocks of data to be copied.
- The *Figure B* represents extents that store backup files with metadata to be replenished.



Backup Chain Legitimacy

Before transferring data to object storage repositories, Veeam validates the backup chain state to ensure that the restore points to be offloaded belong to an inactive backup chain.

Inactive Backup Chain for Backup Job

When a backup job is being executed for the first time, Veeam creates an initial full backup file that contains complete information about the VMs that are being backed up. Each subsequent backup job sessions initiate creation of new incremental backup files that contain only changes which have occurred since the last backup session.

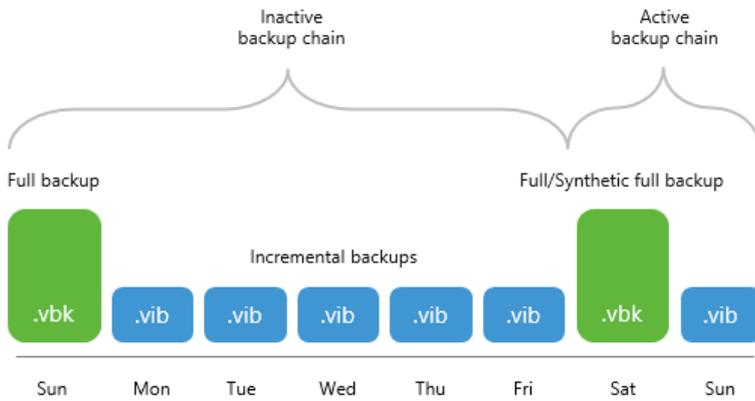
Such a chain can be considered active as there are more incremental backups have yet to be created, depending on the backup job schedule configuration. For more information, see [Define Job Schedule](#).

To send data to object storage repositories, the active backup chain must be reset, that is, transformed into inactive.

To transform an active backup chain into inactive, a new *Active Full* (or *Synthetic Full*) backup file must be created for such a chain. This can be done either manually, as described in [Performing Active Full Backup](#), or you can configure a schedule, according to which new active full backups will be created automatically, as described in [Active Full Backup](#).

Once a new full backup file is created and the offload session is being executed, Veeam collects all the restore points (full and incremental) that were created prior to the latest active full, and prepares them to be transferred to the object storage repository, as described in [SOBR Offload Job](#).

The following figure shows both inactive and active backup chains created with the incremental method. The inactive backup chain consisting of one `.vbk` file and five `.vib` files can easily be offloaded once it satisfies validation criteria, whereas the active backup chain consisting of a `.vbk` file and a `.vib` file would continue to grow with another incremental backups until it is reset by another full backup and so on.



The same applies to backup chains created with the reverse *-incremental* method, except for in this method, all the `.vrb` files starting from the third restore point will be considered inactive automatically, as illustrated in the *Figure A* below. That said, you do not have to create an *Active Full* (nor *Synthetic Full*) backup manually unless you want to offload all the restore points including a `.vbk` file and the first two `.vrb` files, as illustrated in the *Figure B*.

NOTE:

Mind that a full backup file and the first two incremental backup files (that is, two `.vrb` files that immediately follow a `.vbk` file) will never be offloaded until another full backup file is created successfully, as illustrated in the *Figure B*.

Consider the following examples:

- The *Figure A* shows a backup chain consisting of 1 `.vbk` file and 6 `.vrb` files, of which only 4 `.vrb` files (represented as gray blocks) can be offloaded.

- The *Figure B* shows a backup chain consisting of 2 *.vbk* files and 7 *.vrb* files, of which only 6 *.vrb* files and a *.vbk* file (also represented as gray blocks) can be offloaded.

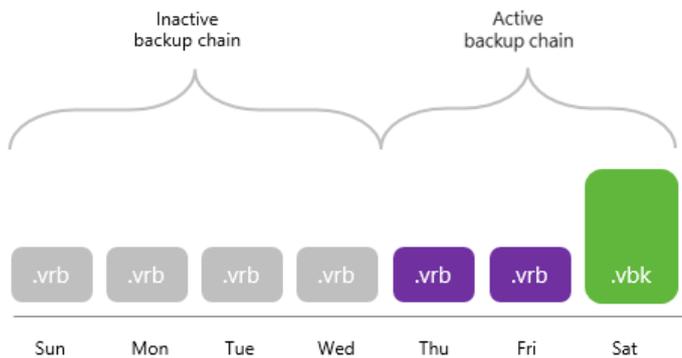


Figure A

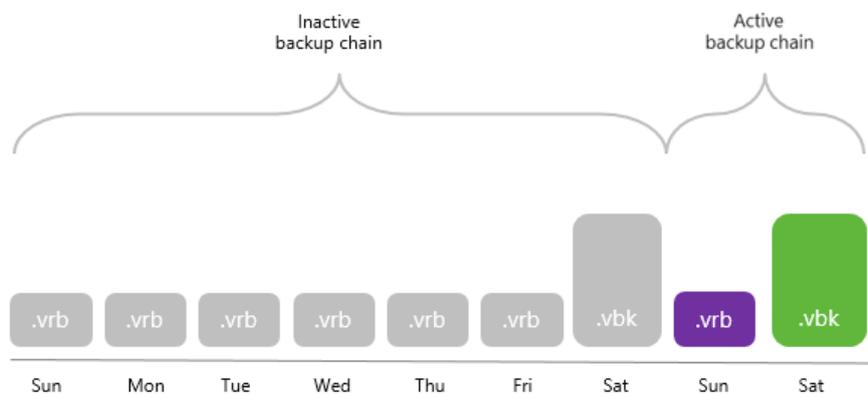


Figure B

Backup chains can be of different structure, depending on whether your backups were created using the per-VM method or as a single storage when all the VMs are placed into a single file (*.vbk* – for full backups and *.vib/.vrb* – for incremental backups). Both structure types can be offloaded to object storage repositories as long as these types are inactive.

For more information on how Veeam creates and manages backup chains, see [Backup Chain](#).

Inactive Backup Chain for Backup Copy Job

When offloading backup chains created by backup copy jobs, only full backup files that have a GFS flag on them will be offloaded. That said, you must select the **Keep the following restore points as full backups for archival purposes** checkbox and (optionally) combine it with the **Read the entire restore point from source backup instead of synthesizing it from increments** checkbox at the **Target** step of the **New Backup Copy Job** wizard.

For more information on how to configure a backup copy job and how the GFS retention works, see [Creating Backup Copy Jobs](#) and [GFS Retention Policy](#) respectively.

Consider the following figures:

- The *Figure A* shows a backup chain consisting of 2 *.vbk* files and 5 *.vib* files created with the *synthetic full* method.

The *Weekly Full Backup* file (represented as a gray block) can be offloaded to object storage since it has a GFS flag assigned to it (as per example, the flag is *Weekly*), whereas the second *.vbk* file cannot be offloaded until it is also assigned a GFS flag, which happens after another full backup file is created.

- The *Figure B* shows a backup chain consisting of 3 *.vbk* files and 11 *.vib* files created with the *active full* method.

In this figure, a *Weekly Full Backup* file (represented as a gray block in the middle) has a *Weekly* flag, therefore, this full backup file can be offloaded to object storage. The second weekly full backup file (represented as an orange block in the rightmost side) also has a *Weekly* flag assigned, but since this file is active and is to be succeeded by another incremental backups during subsequent sessions of your backup copy job, it will not be offloaded until another full backup file is created and so on.

The first backup file (represented as a green block on the left) will never be offloaded since it does not have any GFS flag assigned.

NOTE:

The following types of backup files are never offloaded for backup chains created by backup copy jobs:

- Full backup files (*.vbk*) that have not been assigned any GFS flag.
- Incremental backup files (*.vib*).

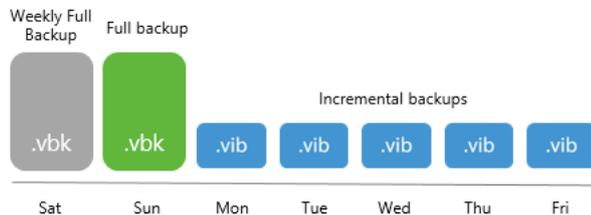


Figure A

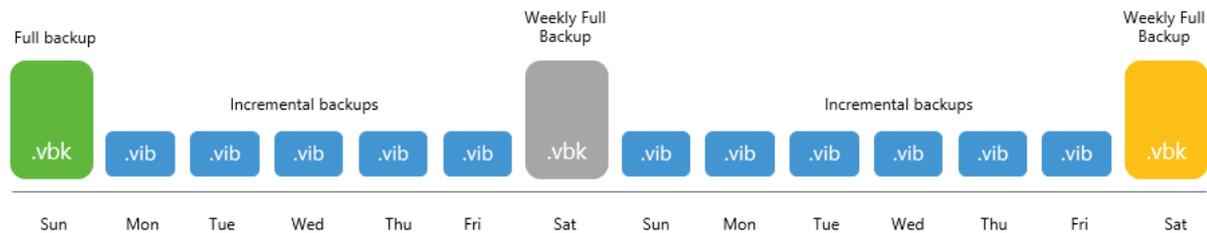


Figure B

Indexes

To reduce the amount of cost-expensive operations incurred by your cloud storage provider, as well as to decrease redundant traffic being sent over the network while offloading your data to object storage repositories, Veeam Backup & Replication uses indexes.

Indexes behavior is as follows:

- Indexes are created (or updated) during each offload session and consist of hash values of blocks that are being transferred to the object storage repository. These hashes are retrieved from meta information of your backup files (*.vbk*, *.vib*, or *.vrb*).
- Indexes are stored in the *ArchiveIndex* directory that is located on the source extent from which the backup data was offloaded.

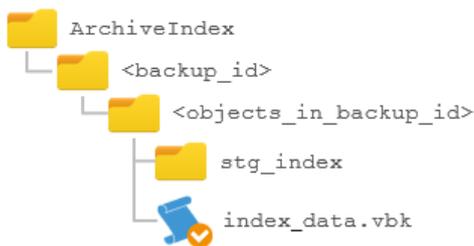
On each subsequent offload session, Veeam will reuse these indexes to verify whether new blocks that are about to be transferred to the object storage repository have not been offloaded earlier. Verification is done by comparing existing indexes hashes with that of a block being transferred.

- Indexes are built per backup chain and cannot have any cross references to any other backup chains.
- Indexes are updated every time a backup chain is modified. For example, some data might have been removed due to the retention policy threshold, or you may have removed it manually. Both scenarios will modify your indexes upon the next successful offload session to maintain consistency.
- Corrupted indexes can be rebuilt anew by using the **Rescan** feature, as described in [Rescanning Scale-Out Repositories](#).

Once rebuilt, Veeam will have to wait for 24 hours before it can offload any data again. This is done to comply with the [Eventual Consistency](#) model of Amazon S3.

ArchiveIndex Directory Structure

When Veeam creates indexes, it also creates and maintains the following directory structure on each extent from which the data is being offloaded.



Directory	Description
ArchiveIndex	The root directory for keeping indexes. This directory is created in the repository of an extent.
<backup_id>	Contains objects in a backup file.
<objects_in_backup_id>	An identifier of an object in a backup file. <ul style="list-style-type: none"> ▪ If a backup was created using the Per-VM method, then each VM will be placed to its own directory. ▪ If a backup was created as a single storage, then all the VMs will be placed to a single directory.
stg_index	Contains actual indexes of the offloaded backup files (.vbk, .vib, or .vrb).
index_data.vbk	Contains meta information on hash values stored in index files.

Retention Policy

A retention policy defines the number of restore points you want to keep on your extents and is configured at the [Specify Backup Storage Settings](#) step of the backup job configuration wizard.

The restore points that fall under the retention policy will be removed from both the extents and object storage repositories in the following manner:

- An earliest offloaded restore point (that is, a backup file with metadata) will be removed from the backup chain of the associated extent.

Backup files with metadata are created, as described in [SOBR Offload Job](#).

- Offloaded data blocks that correspond to the restore point that is being removed will be purged from the object storage repository upon the next successful session of the offload job.

Make sure that an object storage repository has not been put into maintenance mode, as this mode prevents the synchronization of the on-premises backup chain state with that of object storage. If the offload job fails to synchronize a backup chain state due to the aforementioned mode being applied, the synchronization attempts will be repeated during subsequent sessions until the backup chain state is synchronized successfully.

- Associated indexes will be updated for consistency purposes.

For more information, see [Indexes](#).

Data Restore

Object storage data recovery does not differ from that of a standard backup data recovery and can be performed by using any of the following methods:

- [Instant VM Recovery](#)
- [Entire VM Recovery](#)
- [VM Files Restore](#)
- [Virtual Disks Restore](#)
- [Guest OS File Recovery](#)

When your data is being restored, Veeam reuses available indexes that help avoid downloading redundant data which may already exist on any of your extents. Such an approach helps reduce cost-expensive operations incurred by your cloud storage providers.

Data recovery can also be done directly to Amazon EC2 or Microsoft Azure, as described in the [Restore to Amazon EC2](#) and [Restore to Microsoft Azure](#) sections respectively.

Adding Scale-Out Repositories

Before adding a scale-out backup repository, [check prerequisites](#). Then use the **New Scale-out Backup Repository** wizard to configure the scale-out backup repository.

Before You Begin

Before you add a scale-out backup repository to the backup infrastructure, check the following prerequisites:

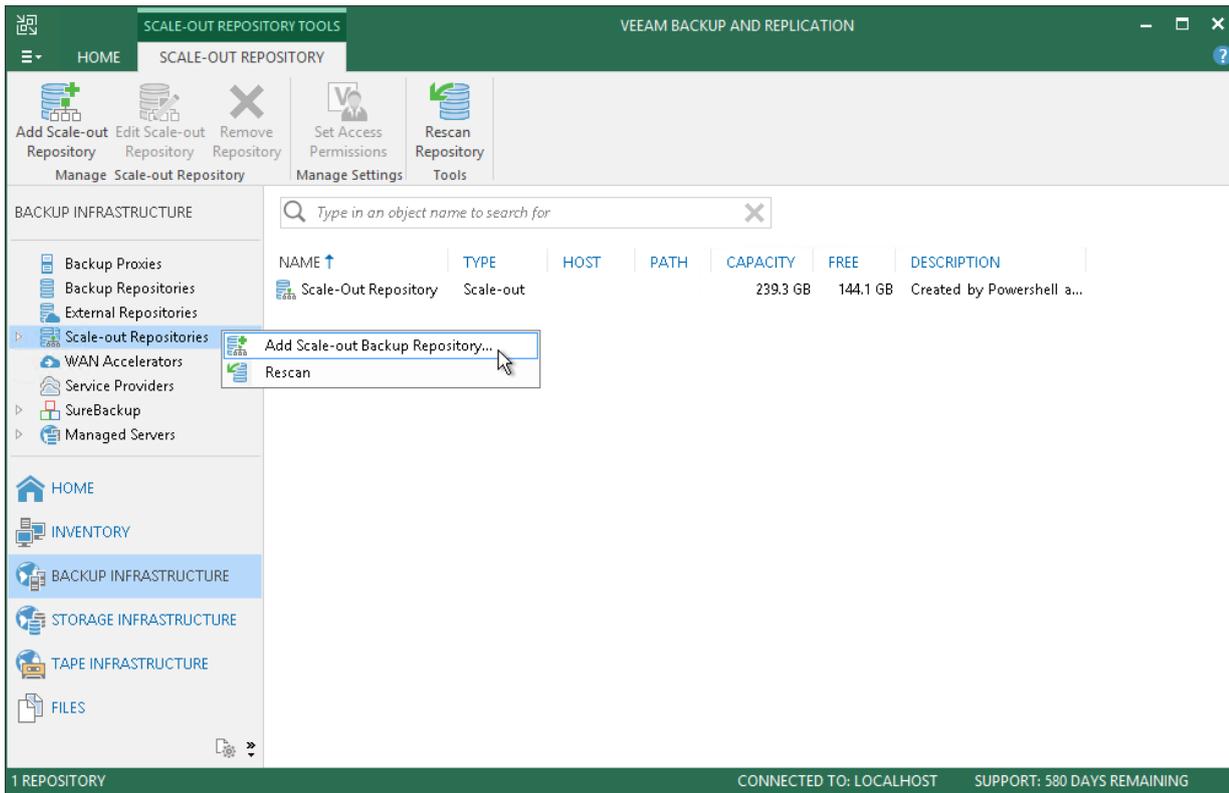
- Backup repositories that you plan to add as extents to the scale-out backup repository must be added to the backup infrastructure. For more information, see [Adding Backup Repositories](#).
- You must check limitations for scale-out backup repositories. For more information, see [Scale-Out Backup Repository](#).

Step 1. Launch New Scale-Out Backup Repository Wizard

To launch the **New Scale-out Backup Repository** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select **Scale-out Repositories** and click **Add Scale-out Repository** on the ribbon.

- Open the **Backup Infrastructure** view, in the inventory pane right-click **Scale-out Repositories** and select **Add Scale-out Backup Repository**.



Step 2. Specify Scale-Out Backup Repository Name

At the **Name** step of the wizard, specify a name and description for the scale-out backup repository.

1. In the **Name** field, specify a name for the scale-out backup repository.

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

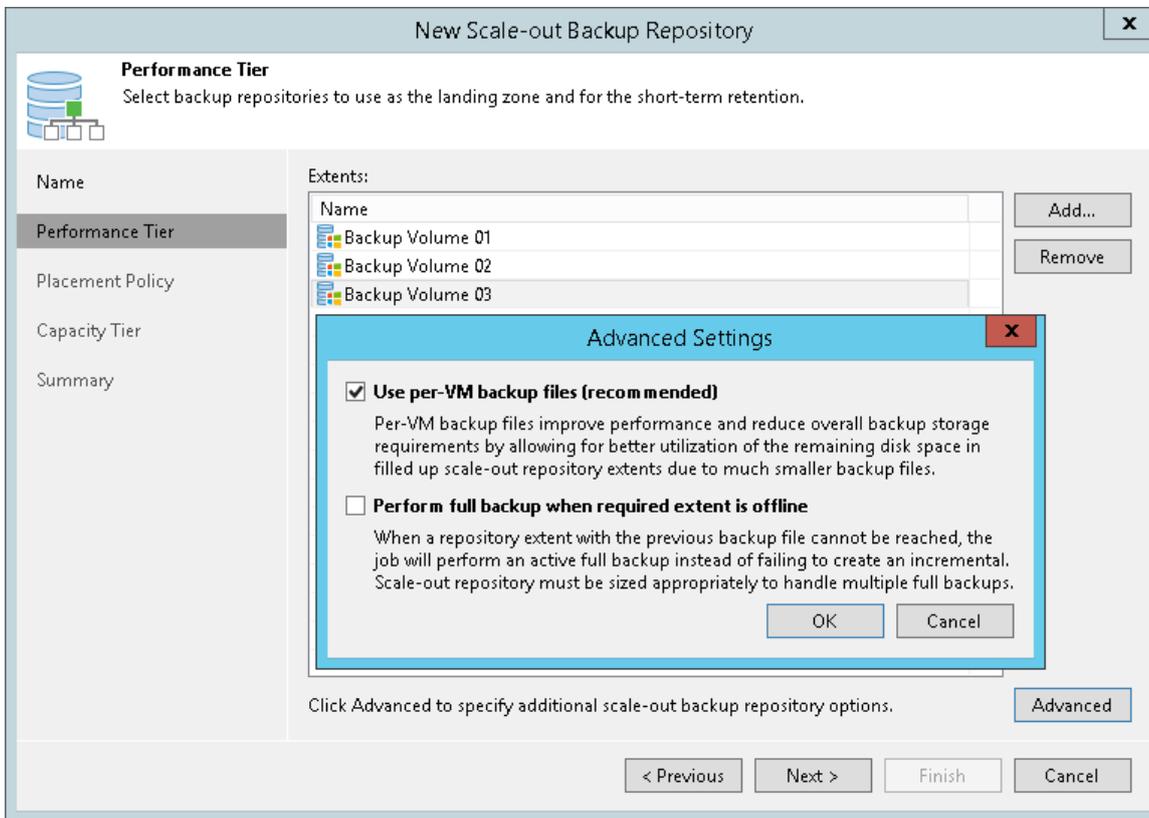
The screenshot shows a wizard window titled "New Scale-out Backup Repository". The window has a sidebar on the left with the following items: "Name" (selected), "Performance Tier", "Placement Policy", "Capacity Tier", and "Summary". The main area contains a "Name" field with the text "Scale-out Backup Repository" and a "Description" field with the text "Extensible Backup Repository". At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel".

Step 3. Add Backup Repository Extents

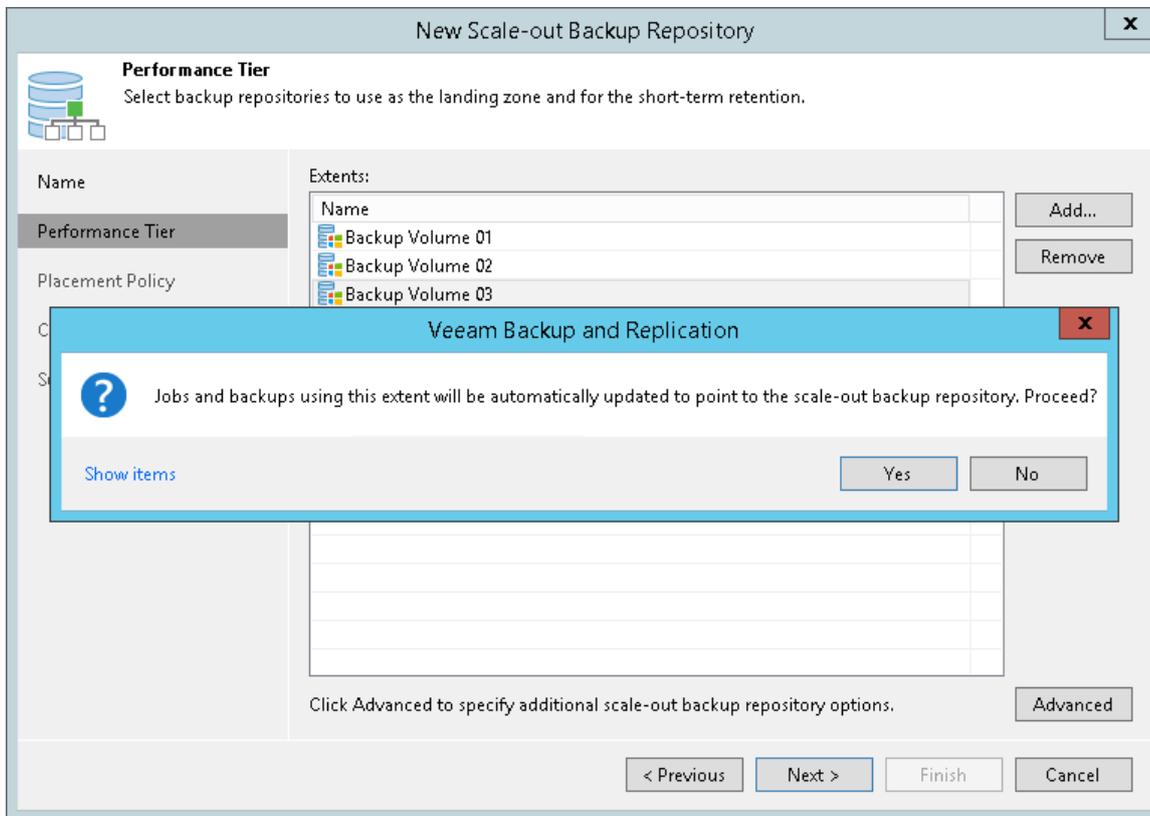
At the **Performance Tier** step of the wizard, specify which backup repositories you want to add as extents, and configure options for the scale-out backup repository.

1. On the right of the **Extents** list, click **Add**.
2. In the **Extents** window, select check boxes next to backup repositories that you want to add as extents.
3. Click **OK**.
4. At the lower right corner of the **Extents** list, click **Advanced**.
5. Specify advanced options for the scale-out backup repository:
 - a. Select the **Use per-VM backup files** check box if you want to create a separate backup chain for every VM in the job. With this option enabled, during one backup job session Veeam Backup & Replication will produce a number of backup files — one per every VM, and will write these files to the backup repository in multiple streams simultaneously. It is recommended that you enable this option to achieve better storage and compute resource utilization, especially if you use as a backup repository a deduplicating storage appliance that supports multiple write streams.

- b. To preserve the consistency of backup chains on the scale-out backup repository, select the **Perform full backup when required extent is offline** check box. If an extent that contains previous restore points from the current backup chain gets offline, the backup chain will be broken. Veeam Backup & Replication will not be able to add a new incremental backup file. With this option enabled, Veeam Backup & Replication will create a full backup file instead of an incremental backup file. If you enable this option, you must make sure that you have enough free space on the scale-out backup repository to host a full backup file.



If a backup repository that you add as an extent is already used by jobs of supported type or there are backups pointing at the backup repository (for example, independent backups created with VeeamZIP), Veeam Backup & Replication will offer you to update a link to the backup repository in the job properties. Click **Yes** to update the link and target the jobs and backups at the scale-out backup repository. If you click **No**, you will not be able to pass to the next steps of the wizard.



Step 4. Specify Backup Placement Policy

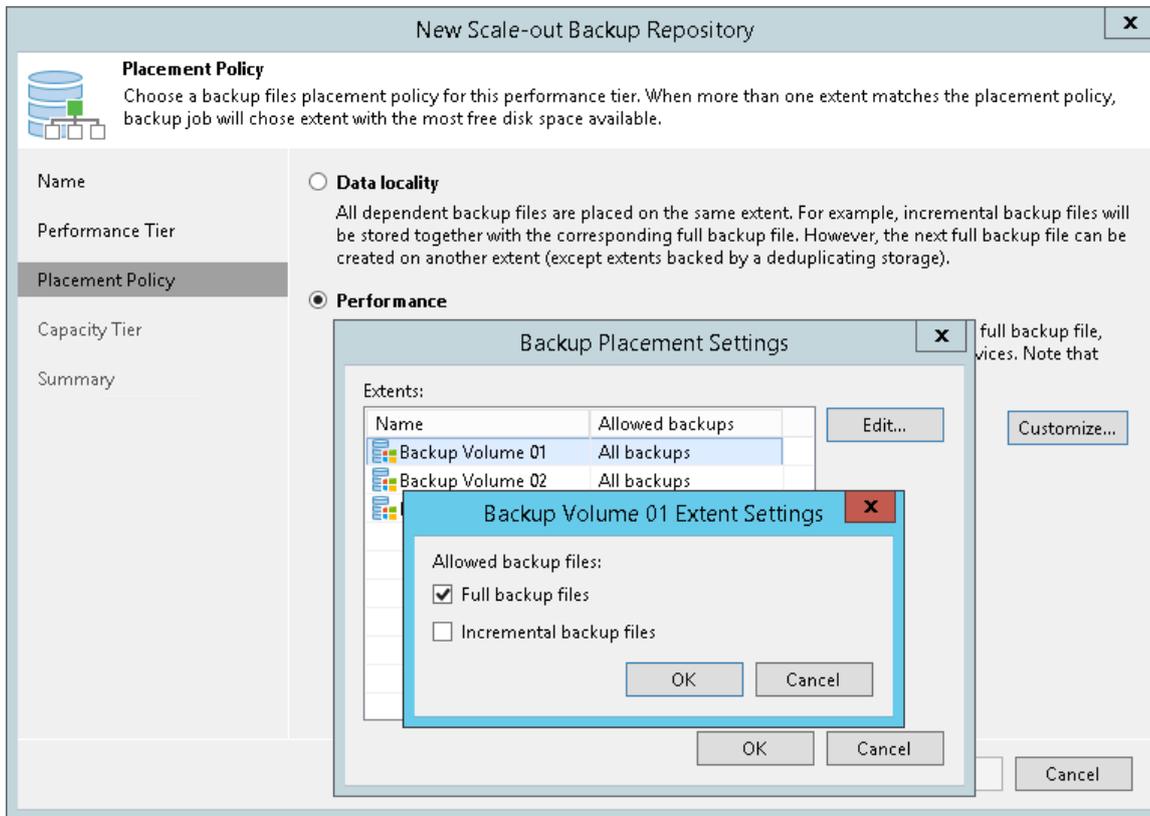
At the **Policy** step of the wizard, specify how you want to store backup files on extents of the scale-out backup repository.

1. Set the backup file placement policy for the scale-out backup repository:
 - Select **Data locality** if you want to store backup files that belong to the same backup chain together. In this case, a full backup file and subsequent incremental backup files will be stored to the same extent of the scale-out backup repository. The new backup chain may be stored to the same extent or to another extent (unless you use a deduplicating storage appliance as an extent).
 - Select **Performance** if you want to store full and incremental backup files to different extents of the scale-out backup repository. If you set the Performance policy, you must make sure that the network connection is fast and reliable so that Veeam Backup & Replication can access all backup files from the backup chain.

For more information, see [Backup File Placement](#).

2. If you select the **Performance** policy, you can restrict which types of backup files can be stored on a specific extent. For example, if you have added three extents to the scale-out backup repository, you may want to store full backup files on one extent and incremental backup files – on the other two extents.
 - a. Click **Customize**.
 - b. In the **Backup Placement Settings** window, select an extent and click **Edit**.

- c. Select a check box next to the type of backup files that you want to store on the extent: **Full backup files** or **Incremental backup files**. By default, Veeam Backup & Replication can store both full and incremental backup files on the same extent.



Step 5. Add Capacity Tier

At the **Capacity Tier** step of the wizard, specify an object storage repository to which you want to offload your data and configure policies to trigger data transfer.

Consider the following when adding an object storage repository:

- You can only add one object storage per scale-out backup repository.
- An object storage repository cannot be added as part of two or more different scale-out backup repositories at the same time.
- If an object storage repository that is being added already contains offloaded data, you will be prompted to synchronize this data with your extents. For more information, see [Synchronizing Capacity Tier Data](#).

To configure capacity tier, do the following:

1. Select the **Extend scale-out backup repository capacity with object storage** checkbox.
2. Select an object storage repository to which you want to offload your data.

Make sure this storage has been added to your environment upfront. In case a cloud storage repository has not yet been configured, click **Add** and follow the associated steps of the wizard, as described in [Adding Object Storage Repository](#).

3. Click **Window** and specify at what time interval the offload job session can be executed to offload your data to object storage.

4. Configure policies to determine whether the backup data located on your extents should be offloaded to object storage:

- a. The **Move backups to object storage as they age out of the operational restores window** checkbox is selected by default and cannot be deselected in this version of Veeam Backup & Replication.
- b. In the **Move backup files older than X days** field, specify the value that will define a period after which the backup data on your extents would be considered outdated and, therefore, should be offloaded to object storage. Consider that "0" is a legitimate value, which you can specify to offload the data on the same day on which your backups were created.

To override this policy, click **Override**, select the **Move oldest backup files sooner if scale-out backup repository is reaching capacity** checkbox and define a threshold in percent to force data transfer if a scale-out backup repository has reached the specified threshold.

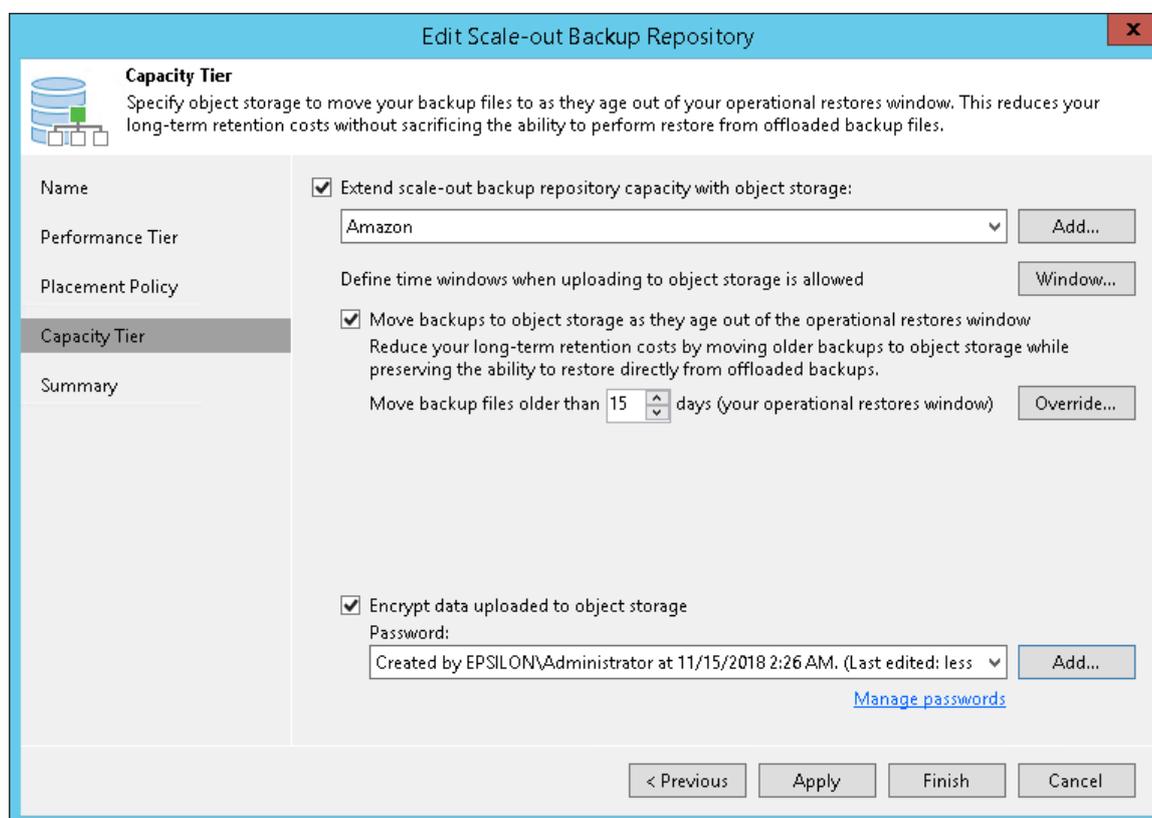
When using this option, Veeam will offload the oldest inactive backup chains to attain the overall scale-out backup repository capacity below the specified threshold level.

5. To offload your data encrypted, select **Encrypt data uploaded to object storage** and provide a strong password. With this option selected, the entire collection of blocks along with the metadata will be encrypted while being offloaded.

If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password.

Once you have finished configuring **Capacity Tier** settings, each time the policies you just defined are met, all the data that is located on your extents and falls under policies thereof will be offloaded directly to the object storage repository automatically.

To transfer data to object storage, Veeam uses the *offload* job that includes additional mandatory verifications to determine whether data that is about to be offloaded is legitimate. For more information, see [SOBR Offload Job](#).

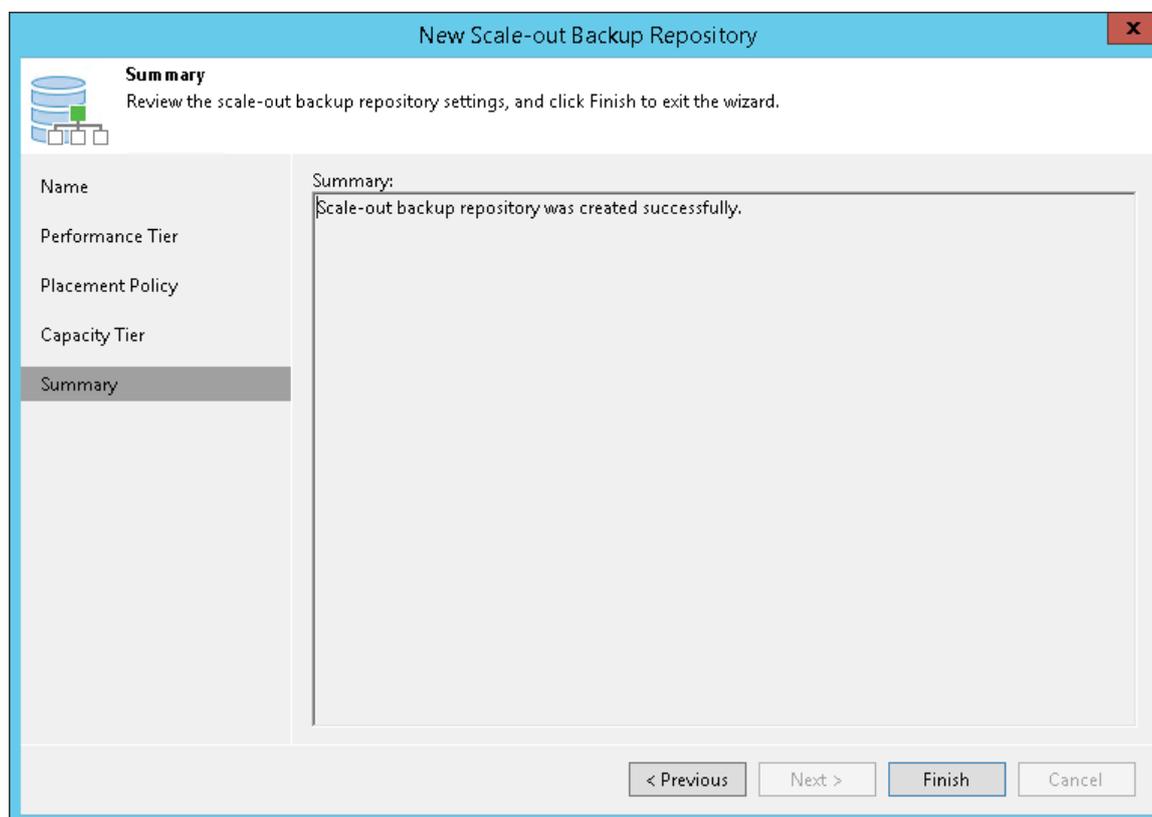


Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of scale-out backup repository configuration.

Wait for the scale-out backup repository to be added to the backup infrastructure. The process may take some time.

1. Review details of the scale-out backup repository.
2. Click **Finish** to exit the wizard.



Synchronizing Capacity Tier Data

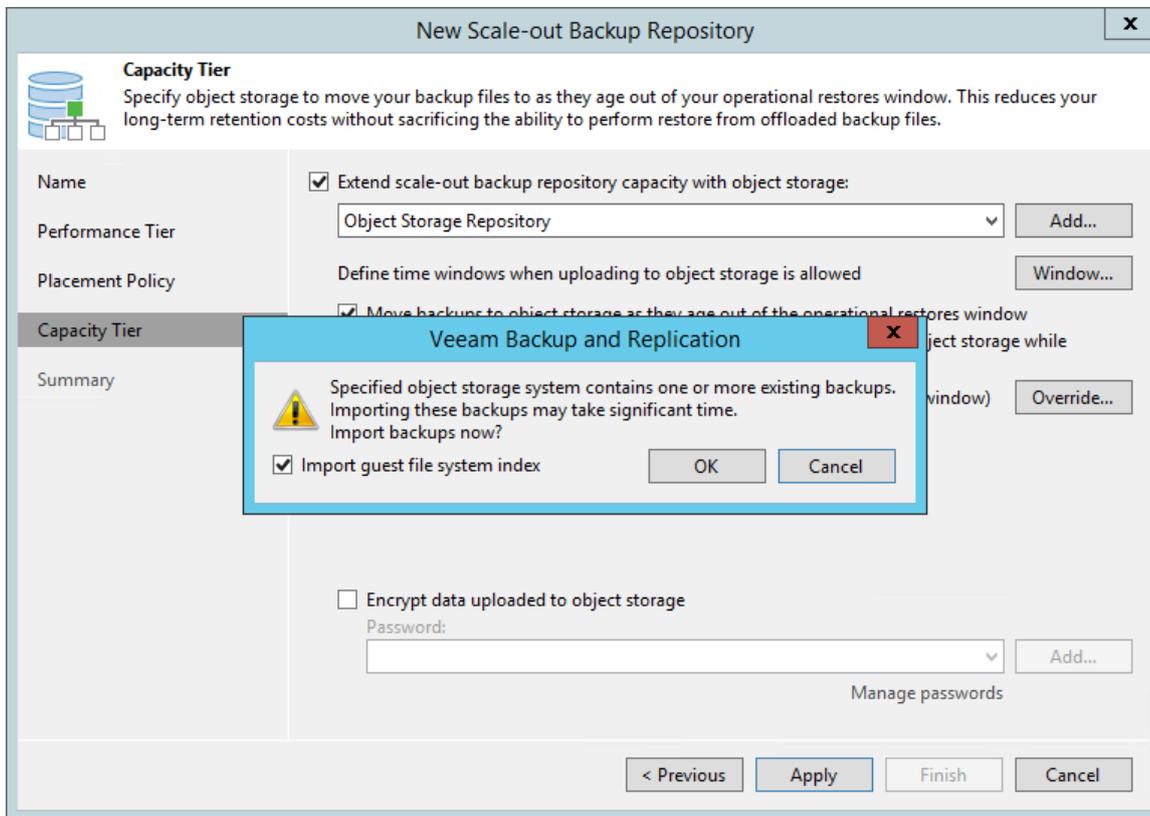
When you add an object storage repository that already contains offloaded data, you will be prompted to synchronize this data with your extents.

Consider the following:

- An object storage repository can only be added after existing data (if any) is synchronized.
- During synchronization, Veeam downloads backup files with metadata located in the object storage repository to the extents that are part of a scale-out backup repository that is being added.
These files are created, as described in [SOBR Offload Job](#).
- Extents to which the data is going to be downloaded (synchronized), will be selected automatically, depending on the available resources.
- The actual data blocks will not be downloaded and will continue to remain in the object storage repository.
- When synchronizing encrypted storage, make sure to provide the same exact password with which the data in such storage was encrypted.

After the synchronization is complete, all the associated backups located in object storage will become available as imported and will be displayed in the **Home** view, under the **Backups > Imported** node in the inventory pane.

The following figure shows an example of prompting you to synchronize existing object storage data with your extents.



Service Actions with Scale-Out Backup Repositories

You can perform service actions with extents of scale-out backup repositories:

- [Put extents to the Maintenance mode](#)
- [Evacuate backups from extents](#)

Maintenance Mode

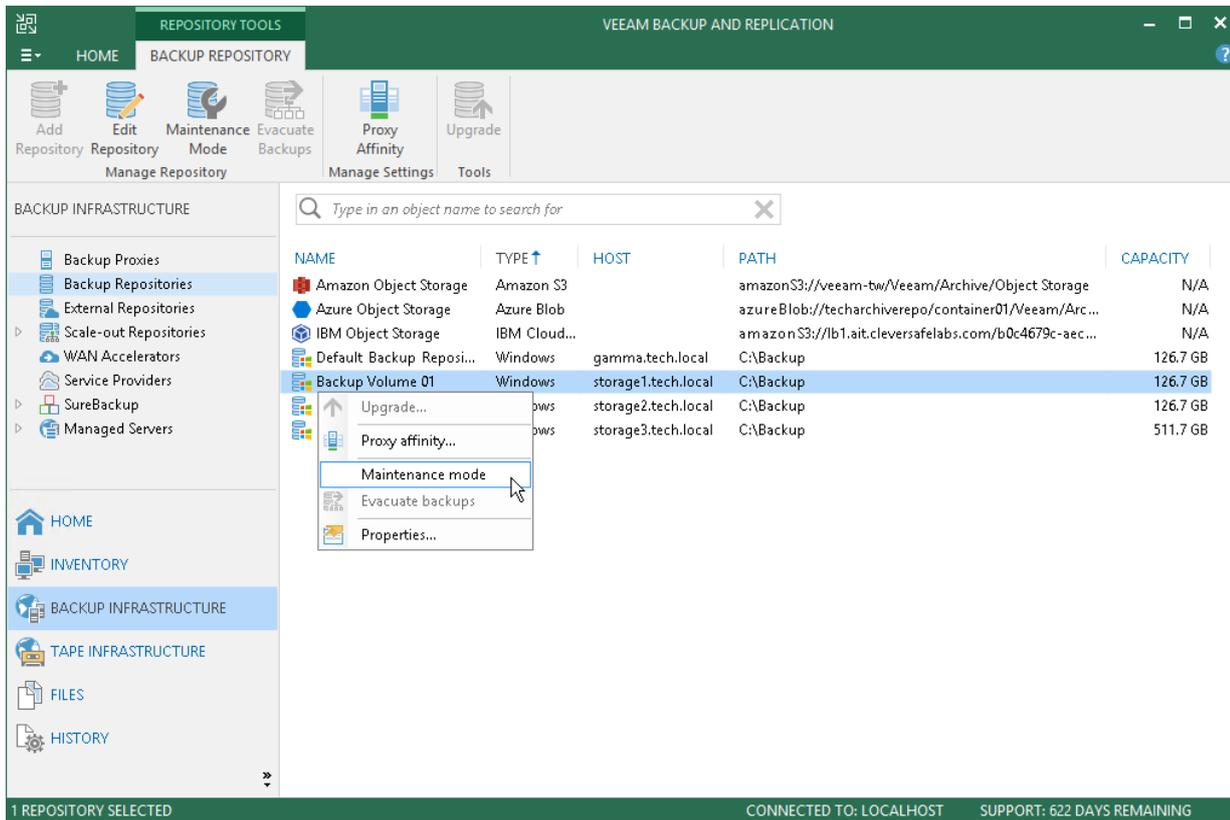
In some cases, you may want to perform service actions with extents of the scale-out backup repository. For example, you need to upgrade the backup repository server and add more memory to it. Or you want to replace a storage device backing the extent and need to relocate backup files. Before you start service actions, you must put the extent to the Maintenance mode.

An extent in the Maintenance mode operates with the limited functionality:

- Veeam Backup & Replication does not start new tasks targeted at this extent.
- You cannot restore VM data from backup files residing on the extent. You also cannot restore VM data from backup files residing on other extents if a part of the backup chain resides on the extent in the Maintenance mode.

When you switch the Maintenance mode, Veeam Backup & Replication launches the *Repository Maintenance* job. The *Repository Maintenance* job checks the status of jobs and tasks targeted at the extent and puts the extent to one of the following modes:

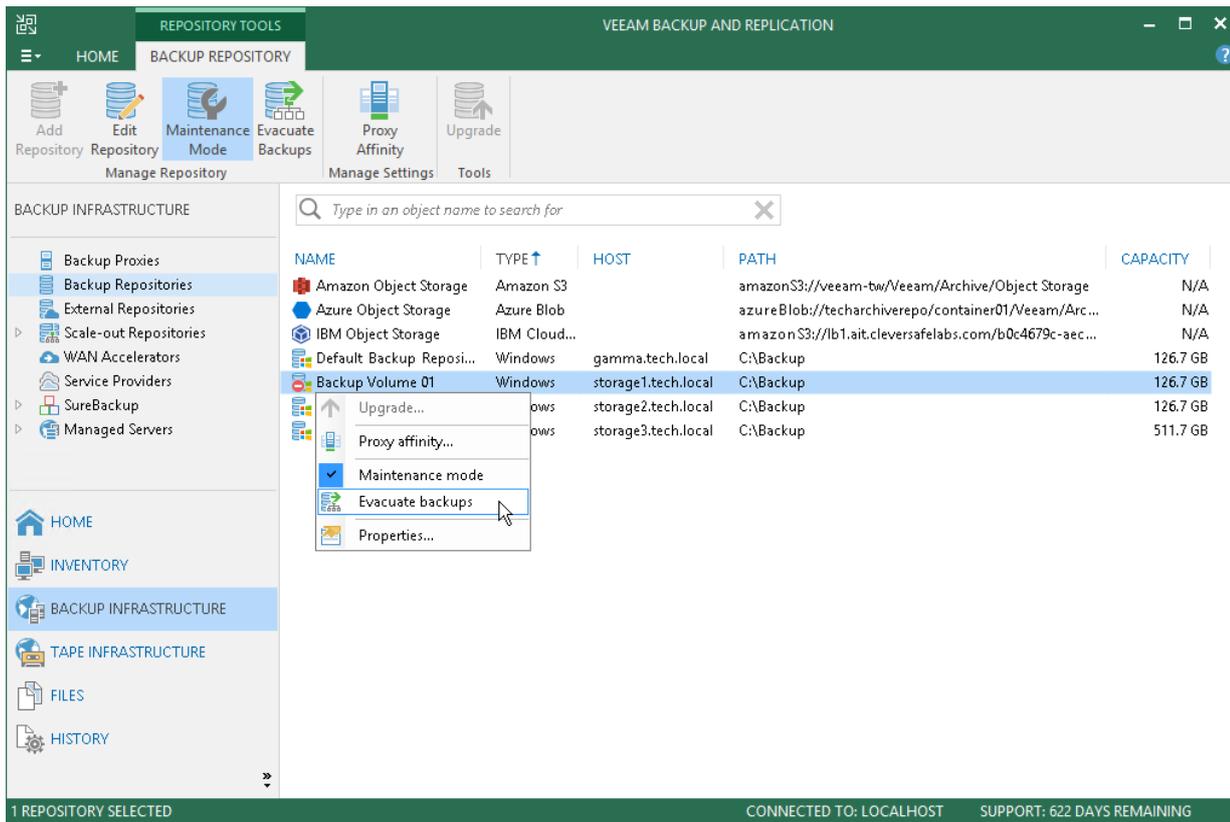
- If no tasks using the extent are currently running, the job puts the extent to the Maintenance mode immediately.
- If the extent is busy with any task, for example, a backup job, the job puts the extent to the *Maintenance pending* state and waits for the task to complete. When the task is complete, the extent is put to the Maintenance mode.



Backup Files Evacuation

If you want to exclude an extent from the scale-out backup repository, you first need to evacuate backup files from this extent. When you evacuate backups, Veeam Backup & Replication moves backup files from the extent to other extents that belong to the same scale-out backup repository. As a result, the backup chains remain consistent and you can work with them in a usual way.

The extent must be put to the Maintenance mode before you evacuate backups from it. If the extent is in the normal operational mode, the **Evacuate** option will not be available for this extent.



When selecting the target extent for evacuated files, Veeam Backup & Replication attempts to keep to the backup placement settings specified for remaining extents. For example, you have 3 extents in the scale-out backup repository with the following backup file placement settings:

- On *Extent 1*, full backup files are stored.
- On *Extent 2* and *Extent 3*, incremental backup files are stored.

If you evacuate backup files from *Extent 2*, Veeam Backup & Replication will relocate them to *Extent 3*.

Editing Settings of Scale-Out Backup Repositories

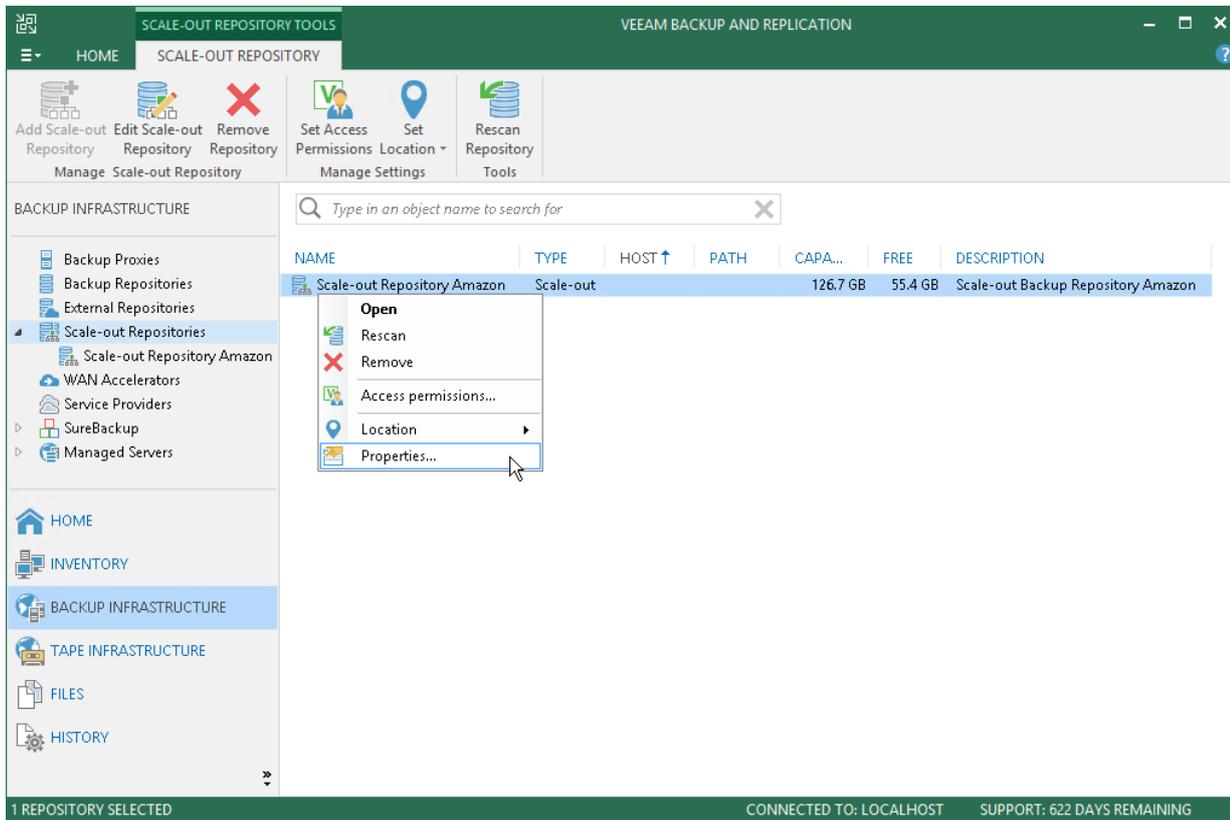
You can edit settings of the scale-out backup repository, for example, if you want to change the backup file placement policy or specify other advanced settings for the backup repository.

Mind the following:

- If you enable or disable the **Use per-VM backup file** option, Veeam Backup & Replication will apply new settings after a new full backup file is created.
- If you enable or disable the **Perform full backup when required extent is offline** option, Veeam Backup & Replication will apply the new settings starting from the next session of the job targeted at this scale-out backup repository.
- If you change the backup file placement policy settings, Veeam Backup & Replication will apply the new settings starting from the next session of the job targeted at this scale-out backup repository.

To change the scale-out backup repository settings:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **Scale-out Repositories**.
3. In the working area, select the scale-out repository and click **Edit Scale-out Repository** on the ribbon or right-click the scale-out backup repository and select **Properties**.
4. Follow the steps of the **Edit Scale-out Backup Repository** wizard and edit settings as required.



Rescanning Scale-Out Repositories

Veeam Backup & Replication periodically rescans scale-out backup repositories. During the rescan process, it gets the following information:

- State of every extent added to the scale-out backup repository – online or offline.
- Status of Veeam Data Movers on extents – up-to-date or outdated.
- Space available on the scale-out backup repository.

The rescan operation is performed automatically by a rescan process that works permanently in the background. The process is started every 24 hours. It can be also started when a new task session starts, and the Veeam Backup Service requires information about the infrastructure to be refreshed.

In addition to the automated rescan process, you can manually start rescan of the scale-out backup repository. Backup repository rescan may be helpful, for example, if you want to discover backup files that were manually relocated from one extent to another one.

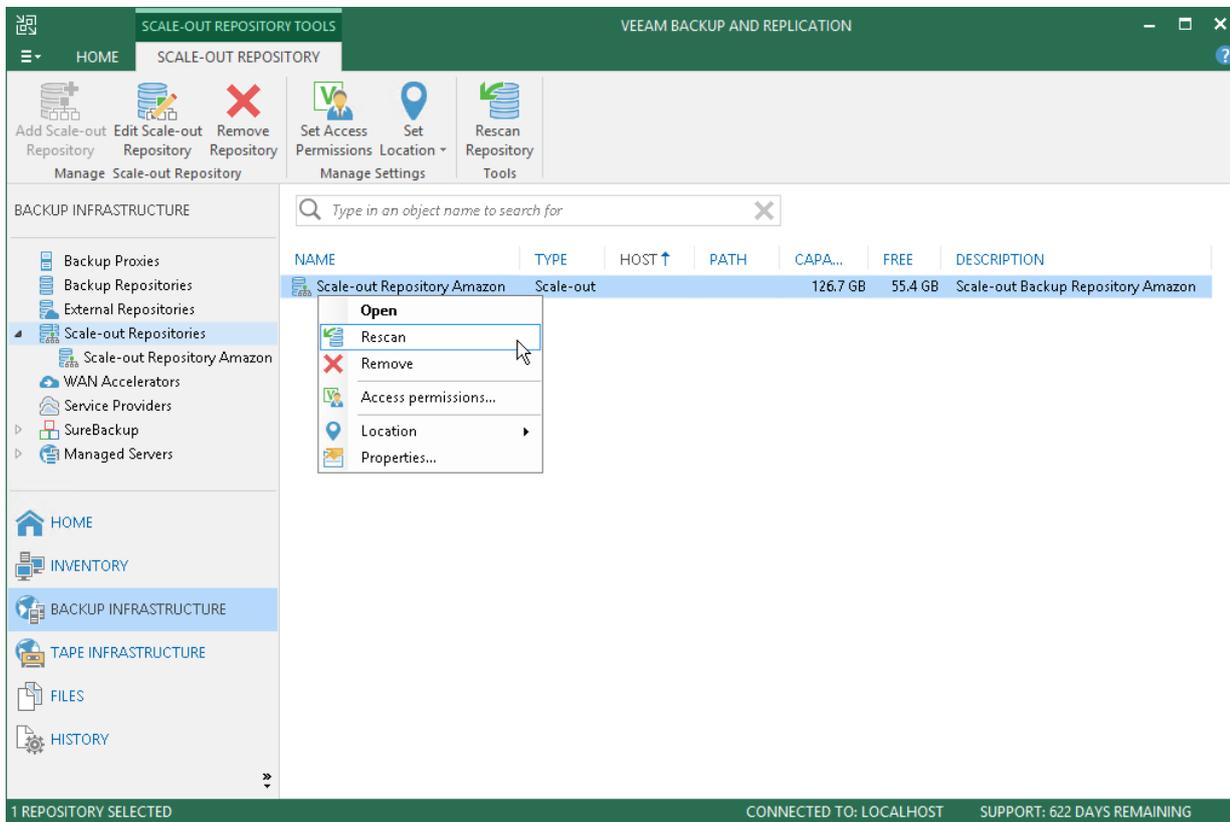
Consider the following:

- Information about backup files location is updated only if you perform manual rescan of scale-out backup repositories.
- Veeam Backup & Replication rescans scale-out backup repositories when you perform backup files import.
- To successfully rediscover relocated backups files created by backup copy jobs, make sure to disable these jobs manually prior to rescanning.

For more information, see [Disabling and Removing Jobs](#).

To start the rescan process:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane select **Scale-out Repositories**.
3. In the working area, select the scale-out repository and click **Rescan Repository** on the ribbon or right-click the scale-out backup repository and select **Rescan repository**.



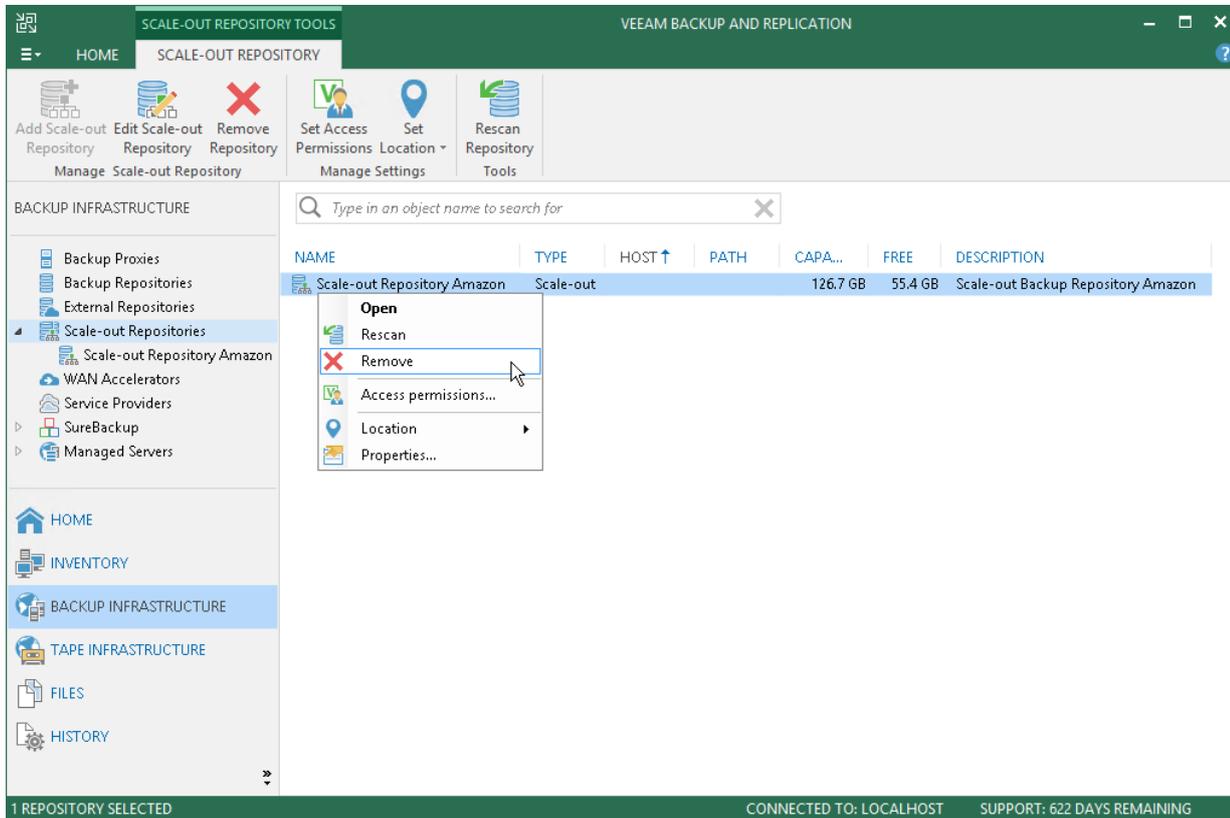
Removing Scale-Out Backup Repositories

You can remove the scale-out backup repository at any time. When you remove the scale-out backup repository, Veeam Backup & Replication unassigns the extent role from all underlying backup repositories, and they become backup repositories. Backup files are not removed from backup repositories – they remain on disk.

You cannot remove a scale-out backup repository at which at least one job is currently targeted. First, you need to target jobs to another backup repository in the backup infrastructure.

To remove a scale-out backup repository:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **Scale-out Repositories**.
3. In the working area, select the scale-out repository and click **Remove Repository** on the ribbon or right-click the backup repository and select **Remove**.



Extending Scale-Out Repositories

You can add a backup repository as an extent to the scale-out backup repository at any time. For example, the scale-out backup repository may run low on space, and you will need to add storage capacity to it.

To add a backup repository as an extent to the scale-out backup repository:

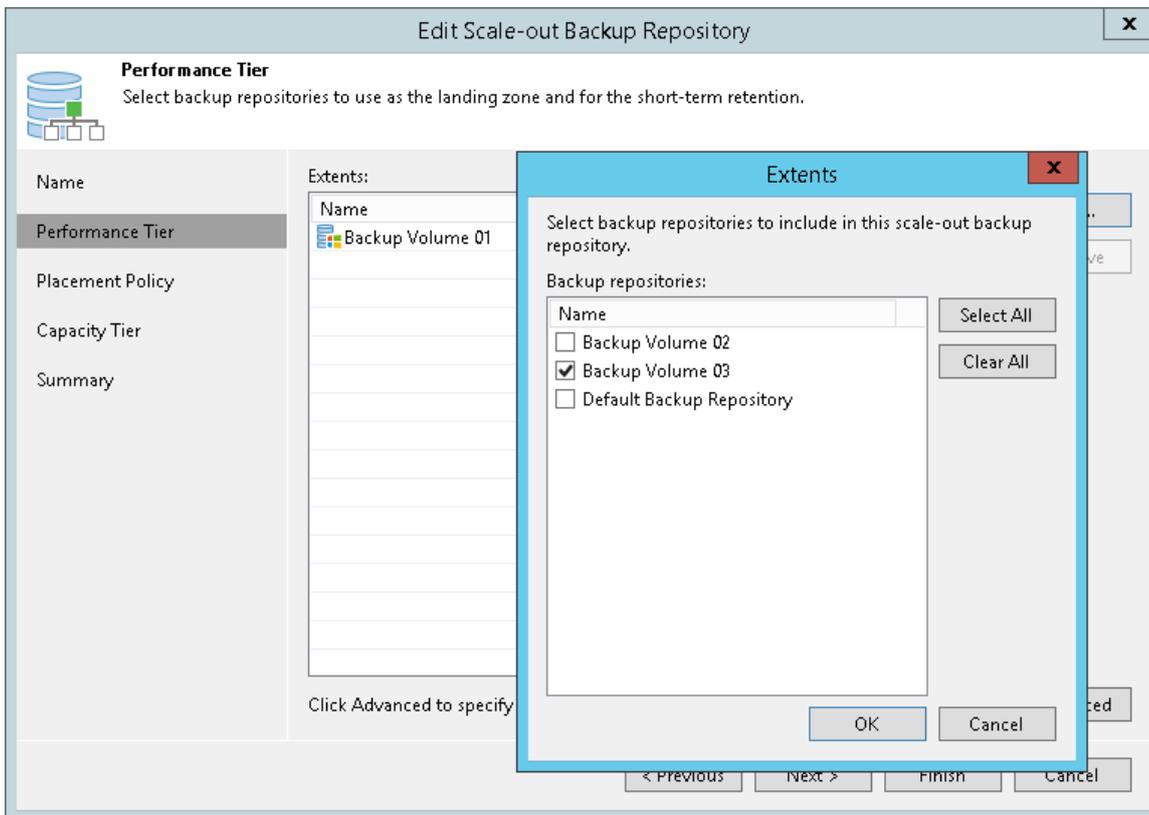
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **Scale-out Repositories**.
3. In the working area, select the scale-out repository and click **Edit Scale-out Repository** on the ribbon or right-click the backup repository and select **Properties**.
4. Move to the **Performance tier** step of the wizard.
5. Click **Add**.
6. In the **Extents** window, select a check box next to the backup repository that you want to add as an extent to the scale-out backup repository.

If a backup repository that you add as an extent is already used by jobs of supported type or there are backups pointing at the backup repository (for example, independent backups created with VeeamZIP), Veeam Backup & Replication will offer you to update a link to the backup repository in the job properties. Click **Yes** to update the link and target the jobs and backups at the scale-out backup repository. If you click **No**, you will not be able to pass to the next steps of the wizard.

7. Pass through the next wizard steps and finish working with the wizard. The new extent will be added to the scale-out backup repository.

NOTE:

After you add a backup repository as an extent to the scale-out backup repository, you will not be able to use this backup repository as a backup repository. To use such backup repository as simple, you will have to remove it from the scale-out backup repository.



Removing Extents from Scale-Out Repositories

You can remove an extent from the scale-out backup repository, for example, if you do not want to store backup files on the underlying storage anymore. When you remove an extent, Veeam Backup & Replication puts the underlying backup repository to the Maintenance mode and unassigns the extent role from it. The backup repository ceases to exist as a part of the scale-out backup repository and becomes a backup repository.

If the extent contains backup files, it is strongly recommended that you perform the following actions before you remove the extent:

1. Put the extent to the Maintenance mode.
2. Evacuate backups from the extent.

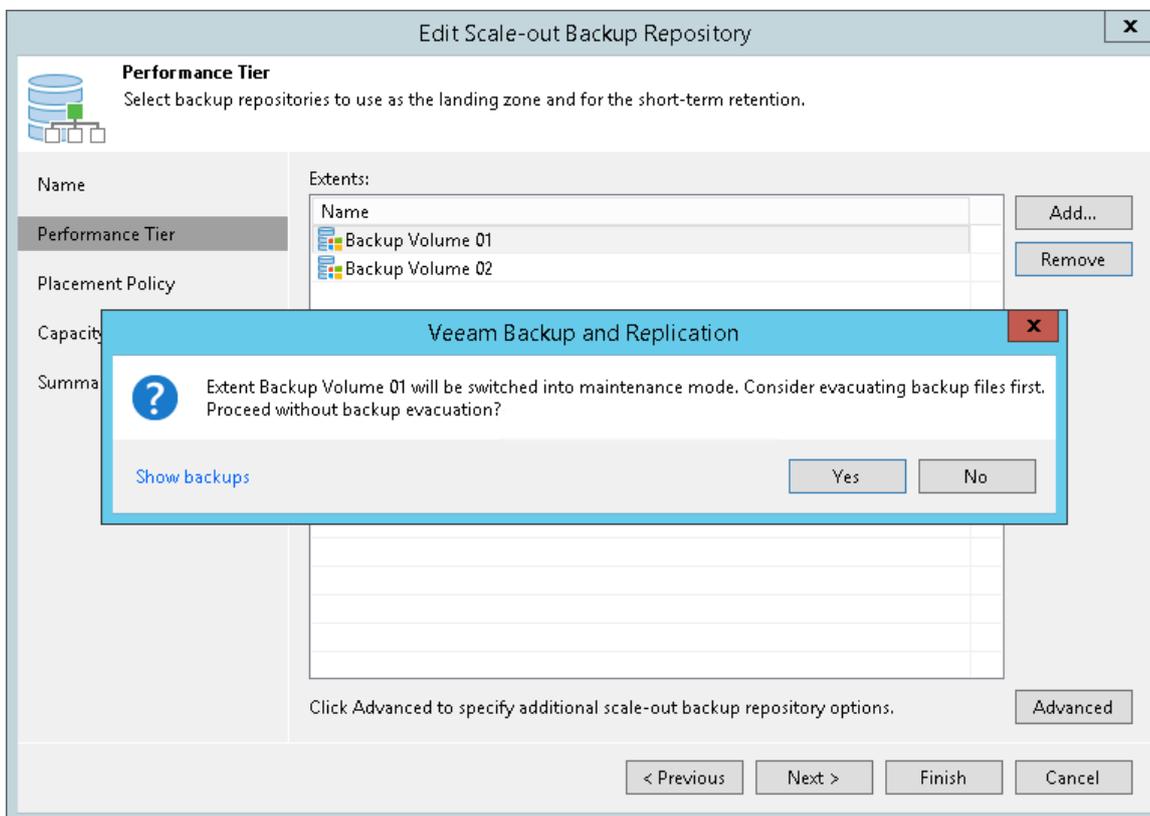
In this case, backup files will be moved to other extents of the scale-out backup repository, and the backup chain will remain consistent. If you do not evacuate backups from the extent, the backup chain may get broken as some restore points will be missing from it.

To remove an extent from the scale-out backup repository:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **Scale-out Repositories**.
3. In the working area, select the scale-out backup repository and click **Edit Scale-out Repository** on the ribbon or right-click the scale-out backup repository and select **Properties**.
4. Move to the **Performance tier** step of the wizard.
5. In the **Extents** list, select the extent and click **Remove**.

If the extent contains backup files, Veeam Backup & Replication will offer you to evacuate them. To evacuate files, click **No**, close the wizard and evacuate backup files. For more information, see [Evacuating Backups from Extents](#).

If you do not want to evacuate backup files, click **Yes** and proceed with the wizard.



Excluding Capacity Tier from Scale-Out Repositories

You can exclude an object storage repository from the scale-out backup repository scope, for example, if you no longer want to utilize any cloud-based services to store your data.

Consider that when you exclude an object storage repository that is being used and which stores offloaded backup data, then such a repository will be put into maintenance mode automatically.

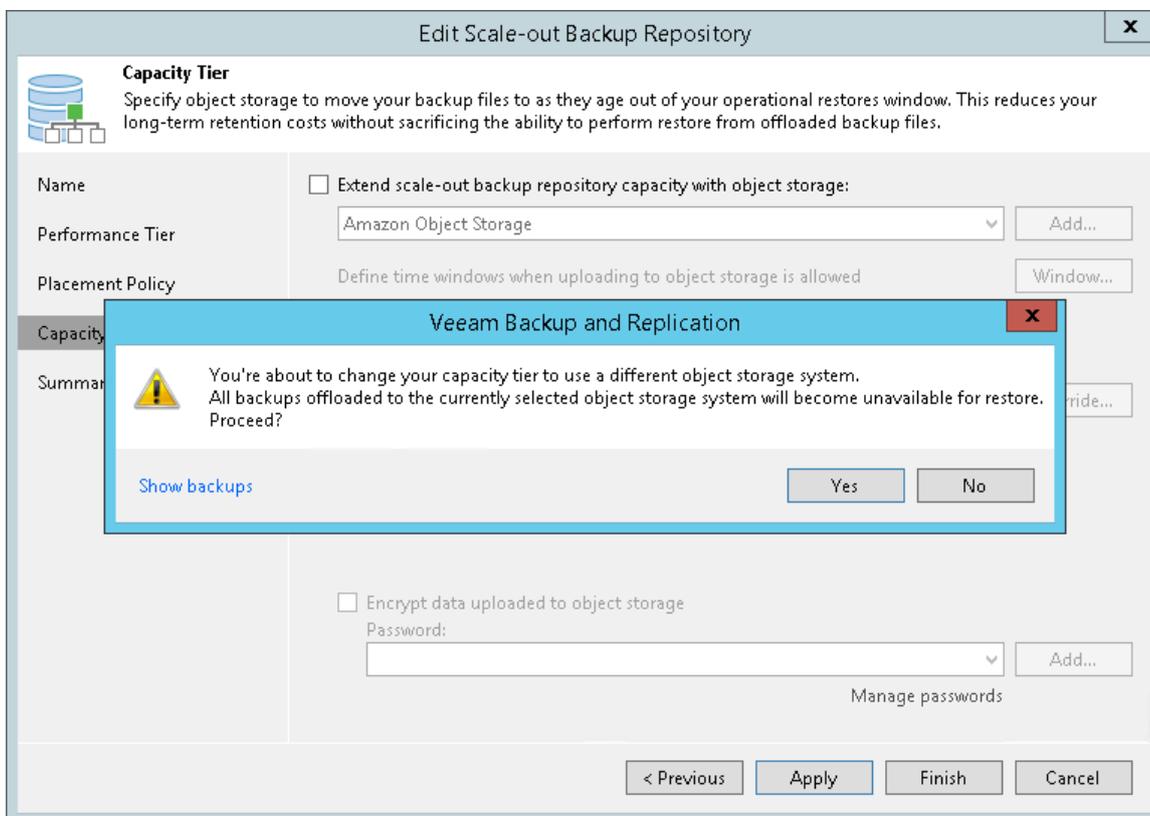
Once in maintenance mode, you will not be able to restore your data from such a repository.

To switch back to normal, you will have to add the repository thereof as part of any other capacity tier and synchronize existing backup chains with your extents. After the synchronization is complete, all the existing backups will become available as imported. For more information, see [Synchronizing Capacity Tier Data](#).

To exclude an object storage repository from the scale-out backup repository scope, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **Scale-out Repositories**.
3. In the working area, select a scale-out backup repository and click **Edit Scale-out Repository** on the ribbon or right-click a scale-out backup repository and select **Properties**.
4. Move to the **Capacity** tier step of the wizard.
5. Deselect the **Extend scale-out backup repository capacity with object storage** checkbox.

You will be asked to confirm the action in the dialog shown below, whereupon an object storage repository will be immediately put into maintenance mode.



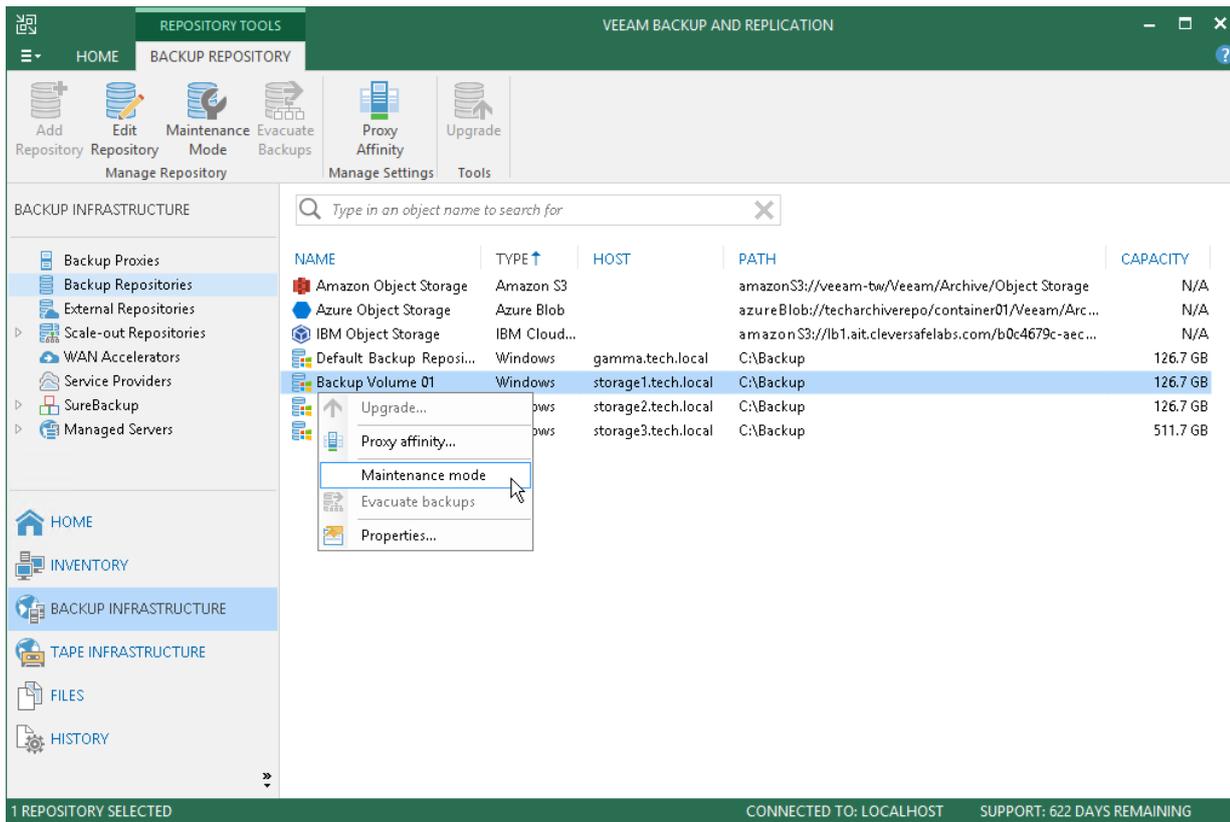
Switching to Maintenance Mode

You can put an extent of the scale-out backup repository to the Maintenance mode if you need to perform service actions on the extent, for example, upgrade it or install a patch on it. You must also put the extent to the Maintenance mode before you evacuate backups from this extent.

To put an extent to the Maintenance mode:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select the scale-out backup repository under **Scale-out Repositories**.
3. In the working area, select the extent and click **Maintenance Mode** on the ribbon or right-click the extent and select **Maintenance mode**.

To bring the extent back to the normal operational mode, select the extent and click **Maintenance Mode** on the ribbon or right-click it and select **Maintenance mode** once again.



Evacuating Backups from Extents

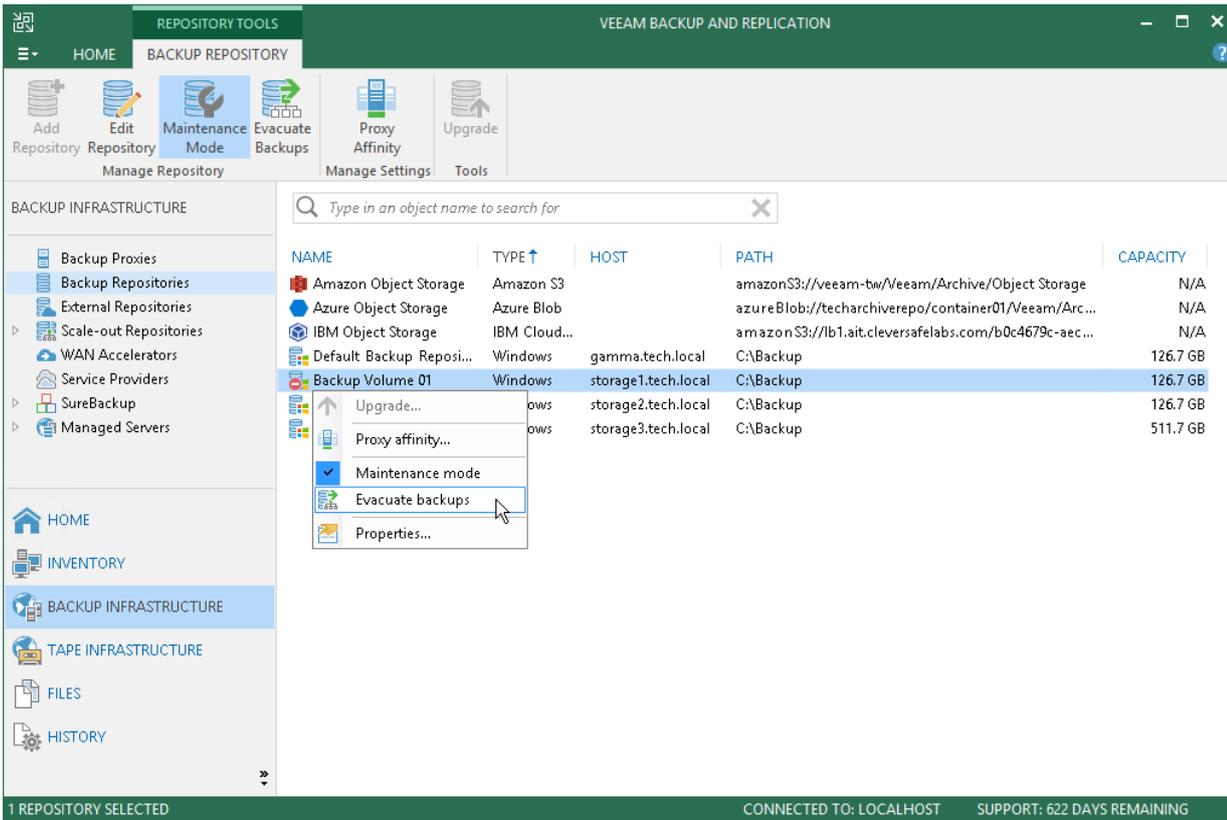
If you want to remove an extent from the scale-out backup repository, you first need to evacuate backups from this extent. When you evacuate backups, Veeam Backup & Replication moves backup files from the extent to other extents that belong to the same scale-out backup repository.

You must put the extent to the Maintenance mode before you evacuate backups from it. For more information, see [Switching to Maintenance Mode](#).

To evacuate backup files from the extent:

1. [Recommended] Stop and disable jobs targeted at the extent from which you plan to evacuate backups.
2. Open the **Backup Infrastructure** view.
3. In the inventory pane, select the scale-out backup repository under **Scale-out Repositories**.
4. In the working area, select the extent and click **Evacuate Backups** on the ribbon or right-click the extent and select **Evacuate backups**.
5. If you have disabled jobs, enable them.

After you evacuate backups, you can proceed to removing the extent from the scale-out backup repository. For more information, see [Removing Extents from Scale-Out Repositories](#).



Discovering Backups on Scale-Out Backup Repositories

To discover on which extent of the scale-out backup repository a particular backup file is stored, you can examine the job session statistics or check the backup properties.

To view the job session statistics:

1. Open the **Home** view.
2. In the inventory pane, click **Backup** under **Jobs**.
3. In the working area, right-click the job and select **Statistics**.

- In the bottom left pane of the window, click the VM name. In the **Action** pane, locate the message: *Using N scale-out repository extent.*

DC (Full) 100% 1 of 1 VMs

SUMMARY		DATA		STATUS	
Duration:	19:14	Processed:	60.0 GB (100%)	Success:	1 ✓
Processing rate:	15 MB/s	Read:	15.4 GB	Warnings:	0
Bottleneck:	Source	Transferred:	9.2 GB (1.7x)	Errors:	0

THROUGHPUT (ALL TIME) Speed: 20.4 MB/s

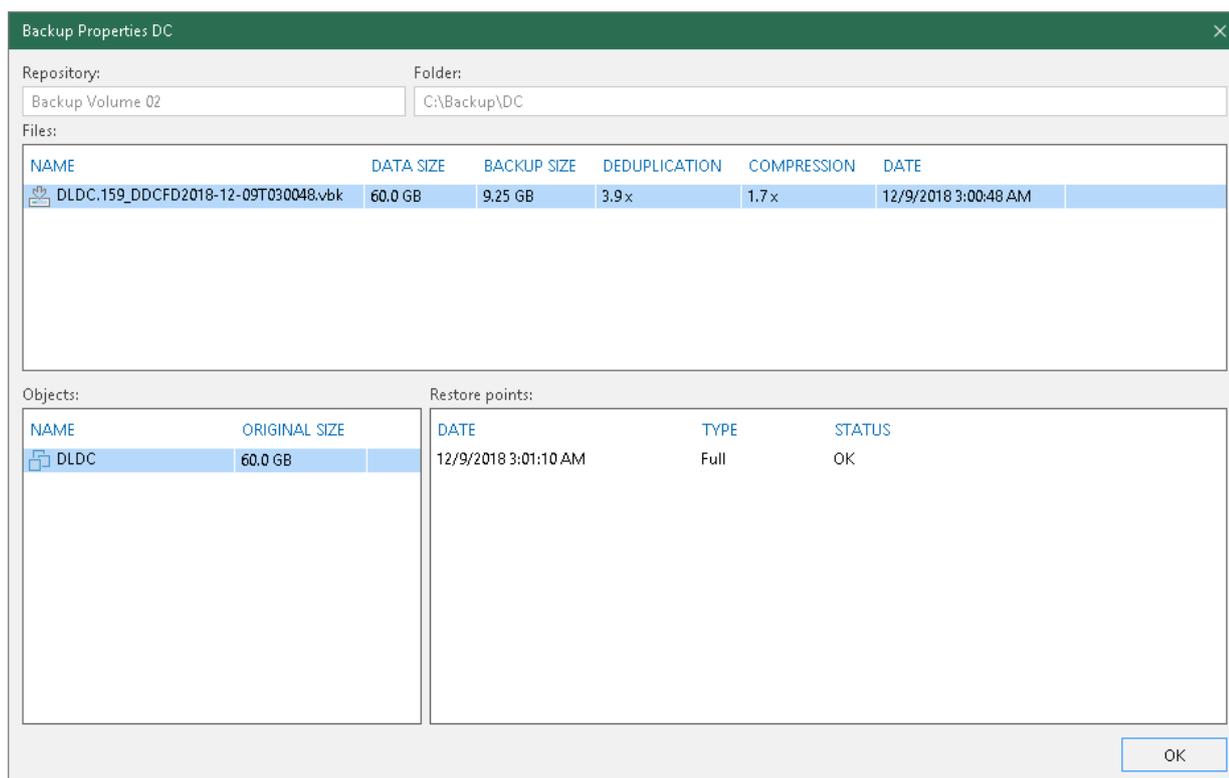
NAME	STATUS	ACTION	DURATI...
DLDC	Success ✓	<ul style="list-style-type: none"> ✓ Queued for processing at 12/9/2018 3:00:49 AM ✓ Required backup infrastructure resources have been assigned ✓ Using Backup Volume 02 scale-out repository extent ✓ No available proxies are running on ESX(i) management interface subnet. Using... ✓ VM processing started at 12/9/2018 3:00:55 AM ✓ VM size: 60.0 GB ✓ Getting VM info from vSphere 00:02 ✓ Creating VM snapshot 00:02 ✓ Saving [Store2] DLDC_DLDC.vmx 00:00 ✓ Saving [Store2] DLDC_DLDC.vmx 00:00 ✓ Saving [Store2] DLDC_DLDC.nvram 00:00 ✓ Using backup proxy VMware Backup Proxy for disk Hard disk 1 [nbd] 00:00 	

Hide Details OK

To view the backup properties:

- Open the **Home** view.
- In the inventory pane, select **Disk** under **Backups**.
- In the working area, right-click the backup and select **Properties**.

- In the **Backup Properties** window, click the backup file and check the **Repository** field at the top left corner of the window. Veeam Backup & Replication will display on which extent the backup file resides.



Receiving Scale-Out Backup Repository Reports

Veeam Backup & Replication is capable of sending reports that contain information about processing results of your scale-out backup repositories data.

Consider the following:

- Reports are sent only after you have enabled email notifications, as described in [Configuring Global Email Notification Settings](#).
- Reports are sent daily at 9:00 AM.
- Reports are sent for all notification types such as *Success*, *Warning* and *Error*.
- The title of a report is built up of "*Scale-out Backup Repository*" + a repository name. That said, if your scale-out backup repository name is Amazon, then the report title would be *Scale-out Backup Repository Amazon*.

Each report is divided into sections and contains the following information:

- **Performance Tier** (upper-left) section:
 - **Used Space.** Shows the used disk space of your scale-out backup repository.
 - **Capacity.** Shows the total storage capacity of your scale-out backup repository.
- **Capacity Tier** (upper-right) section:
 - **Used Space.** Shows the occupied storage space in your object storage repository.
 - **Space Limit.** Shows the space limit (if any). A space limit is specified when adding a new object storage repository, as described in [Adding Object Storage Repositories](#).

- **Performance Tier** (middle) section:
 - **Extent.** Shows extents of a scale-out backup repository.
 - **Capacity.** Shows the total storage capacities of your extents.
 - **Used Space.** Shows the amount of disk space used on your extents.
 - **Status.** Shows the status of each extent, as described in [Description of Report Statuses](#).

- **Capacity Tier** (lower) section:
 - **Extent.** Shows the name of an object storage repository.
 - **Space Limit.** Shows the space limit (if any).
 - **Used Space.** Shows the occupied storage space in your object storage repository.
 - **Status.** Shows the status of an object storage repository, as described in [Description of Report Statuses](#).

If an automatic offload job session exits with any status other than *Success*, you will see the associated status message in this field. For more information about the offload job, see [SOBR Offload Job](#).

Description of Report Statuses

The following table lists possible combinations of *Warning* and *Error* messages shown under the **Status** column of a report.

If none of the conditions listed in the **Extent state** column is true, then the report status will be shown as *Success*.

Extent type	Extent state	Status message	Report type
Performance tier	Maintenance mode	Maintenance mode	Warning
	Threshold limit exceeded. Threshold is specified in the Backup storage section, as described in Specifying Other Notification Settings .	Reaching capacity	Warning
	Unavailable	Offline	Error
Capacity tier	Maintenance mode	Maintenance mode	Warning
	Space limit exceeded. Space limit is specified when adding a new object storage repository, as described in Adding Object Storage Repositories .	Out of capacity	Error
	Unavailable	Offline	Error

	Threshold limit exceeded. Threshold is specified in the Backup storage section, as described in Specifying Other Notification Settings .	Reaching capacity	Warning
--	---	-------------------	---------

Report Examples

Success Reports

The following figure shows an example of a report consisting of two extents (*Backup Volume 01* and *Backup Volume 02*); both share *253.3 GB* of storage capacity, of which *52.4 GB* is occupied.

Both extents have OK status, which means that neither extent was put into maintenance mode, nor has any of these extents exceeded the allowed threshold limit.

This report also includes the **Capacity Tier** section consisting of object storage with no **Space Limit** applied. This object storage stores *29.6 GB* of data and has the *OK* status.

Scale-out backup repository Amazon				Success
Remote Object Storage				
Wednesday, December 19, 2018 4:04:12 AM				
Performance Tier		Capacity Tier		
Used Space	52.4 GB	Used Space	29.6 GB	
Capacity	253.3 GB (70% free)	Space Limit	Not set	
Performance Tier				
Extent	Capacity	Used Space	Status	
Backup Volume 01	126.7 GB (67% free)	30.3 GB	OK	
Backup Volume 02	126.7 GB (73% free)	22.1 GB	OK	
Capacity Tier				
Extent	Space Limit	Used Space	Status	
Amazon S3 Object Storage	Not set	29.6 GB	OK	

Warning Reports

The figure below demonstrates a report with the *Warning* status.

As per example, the *Backup Volume 01* extent has been put into maintenance mode, and the *Backup Volume 02* extent has exceeded the allowed threshold both of which have caused a report to be generated with the *Warning* status.

Scale-out backup repository Amazon				Warning
Remote Object Storage				
Wednesday, December 19, 2018 4:58:35 AM				
Performance Tier		Capacity Tier		
Used Space	82.0 GB	Used Space	29.6 GB	
Capacity	253.3 GB (58% free)	Space Limit	Not set	
Performance Tier				
Extent	Capacity	Used Space	Status	
Backup Volume 01	126.7 GB (43% free)	60.0 GB	Maintenance mode	
Backup Volume 02	126.7 GB (73% free)	22.1 GB	Reaching capacity	
Capacity Tier				
Extent	Space Limit	Used Space	Status	
Amazon S3 Object Storage	Not set	29.6 GB	OK	

Error Reports

In the figure below a report has been generated with the *Error* status caused by the *Amazon S3 Object Storage* extent which has exceeded its allowed space limit.

Scale-out backup repository Amazon				Error
Remote Object Storage				
Thursday, December 20, 2018 3:55:02 AM				
Performance Tier		Capacity Tier		
Used Space	82.0 GB	Used Space	29.6 GB	
Capacity	253.3 GB (58% free)	Space Limit	2.0 GB (0% free)	
Performance Tier				
Extent	Capacity	Used Space	Status	
Backup Volume 01	126.7 GB (43% free)	60.0 GB	OK	
Backup Volume 02	126.7 GB (73% free)	22.1 GB	OK	
Capacity Tier				
Extent	Space Limit	Used Space	Status	
Amazon S3 Object Storage	2.0 GB (0% free)	29.6 GB	Out of capacity	

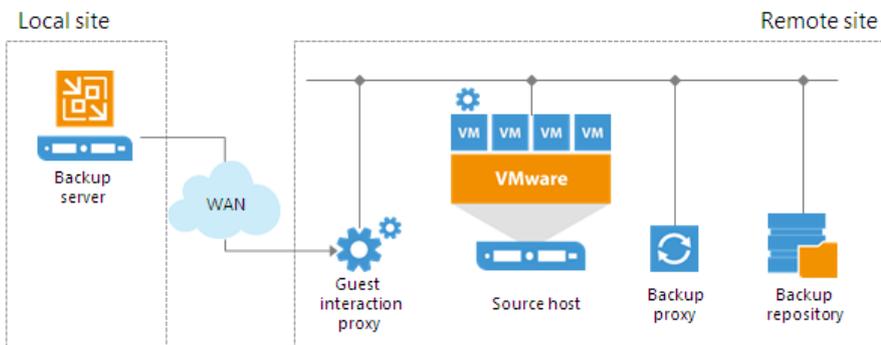
Guest Interaction Proxy

The guest interaction proxy is a backup infrastructure component that sits between the backup server and processed VM. This component is needed if the backup or replication jobs perform the following processing of VMs:

- Application-aware processing
- Guest file system indexing
- Transaction logs processing

To interact with the VM guest OS, Veeam Backup & Replication needs to deploy a runtime process in each VM. The task of deploying the runtime process in a VM is performed by the guest interaction proxy.

The guest interaction proxy allows you to communicate with the VM guest OS even if the backup server and processed VM run in different networks.



IMPORTANT!

The guest interaction proxy deploys the runtime process only in Microsoft Windows VMs. In VMs with another guest OS, the runtime process is deployed by the backup server.

Guest Interaction Proxy Deployment

You can use multiple guest interaction proxies to improve performance. Multiple guest interaction proxies will deploy runtime processes in VMs faster compared to the same operation performed by one guest interaction proxy.

In a backup infrastructure with multiple remote sites, you can deploy a guest interaction proxy in each site. This can reduce load on the backup server and produce less traffic between the backup server and remote site.

Requirements for Guest Interaction Proxy

A machine performing the role of a guest interaction proxy must meet the following requirements:

- The role of a guest interaction proxy can be assigned to a Microsoft Windows server (physical or virtual).
- You must add the machine to the Veeam Backup & Replication console as a managed server.
- Guest interaction proxy must have either a LAN or VIX connection to the VM that will be processed. You do not have to set up both connections – only one connection is required. For more information about setting up a connection to the VM, see <https://www.veeam.com/kb1788>.

The guest interaction proxy role can be performed by any machine that meets the requirements, including backup proxy, backup repository, WAN accelerator or backup server.

NOTE:

The guest interaction proxy functionality is available in the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication.

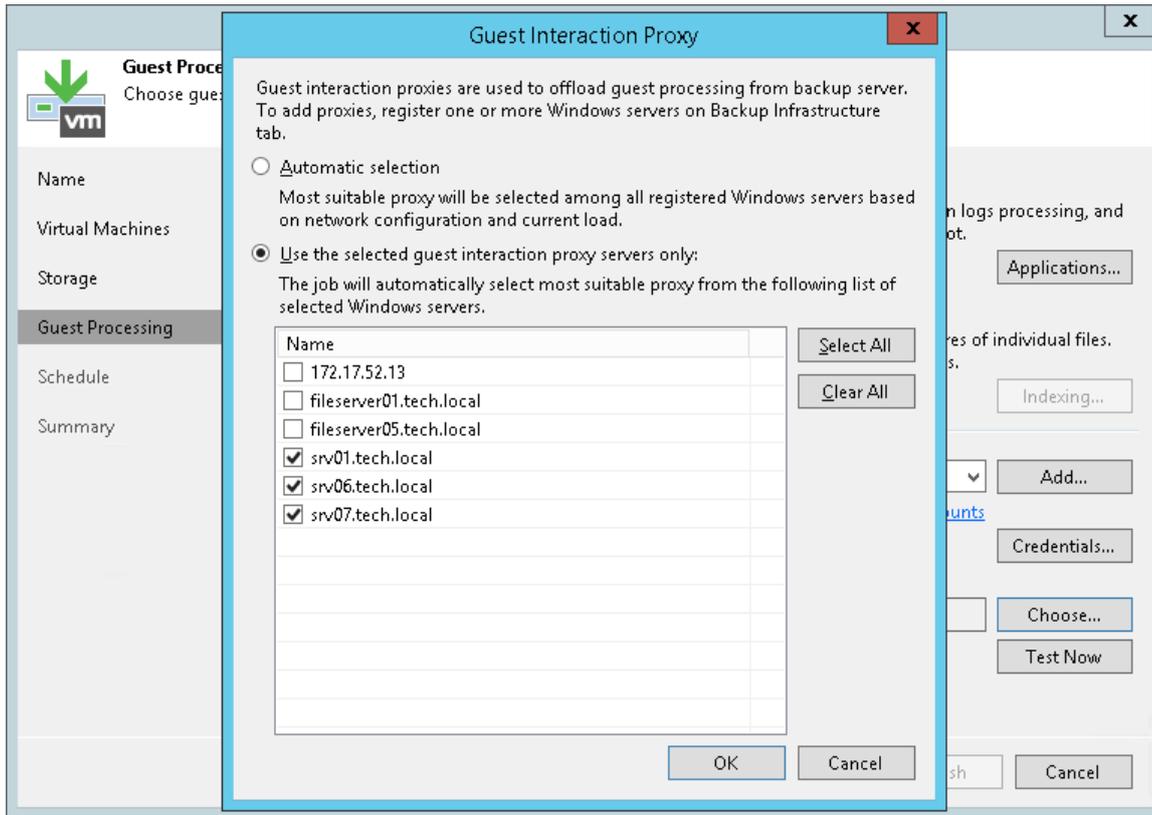
Guest Interaction Proxy Selection

When you add a Microsoft Windows machine to the backup infrastructure, Veeam Backup & Replication deploys the Data Mover Service on it. The Data Mover Service includes the components responsible for runtime process deployment during guest OS interaction.

To assign a guest interaction proxy for the job, you must select a Microsoft Windows machine that will perform the role of the guest interaction proxy at the **Guest Processing** step of the backup or replication job wizard. You can assign the guest interaction proxy manually, or let Veeam Backup & Replication do it automatically. Veeam Backup & Replication uses the following priority rules to select the guest interaction proxy:

1. A machine in the same network as the protected VM that does not perform the backup server role.
2. A machine in the same network as the protected VM that performs the backup server role.
3. A machine in another network that does not perform the backup server role.
4. A machine in another network that performs the backup server role.

If Veeam Backup & Replication finds several available machines of equal priority, it selects the less loaded machine. The load is defined by the number of tasks that the machine already performs.



Failover from Guest Interaction Proxy to Backup Server

If the guest interaction proxy fails to connect to a Microsoft Windows VM, the guest interaction proxy will not be able to access the VM and deploy a runtime process in it. In this case, the backup server will take over the role of guest interaction proxy and deploy the runtime process in the VM.

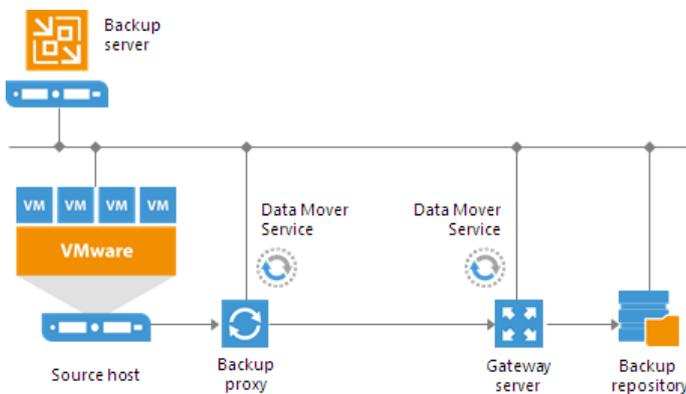
Gateway Server

A gateway server is an auxiliary backup infrastructure component that “bridges” the backup server and backup repository. The gateway server is required if you deploy the following types of backup repositories in the backup infrastructure:

- Shared folder backup repositories
- Dell EMC Data Domain deduplicating storage appliance
- HPE StoreOnce deduplicating storage appliance

Such backup repositories cannot host Data Mover Services – Veeam components that establish a connection between a backup proxy and backup repository (in case of backup jobs) or between backup repositories (in case of backup copy jobs). To overcome this limitation, Veeam Backup & Replication uses gateway servers.

In the backup infrastructure, a gateway server hosts the target Veeam Data Mover. Veeam Backup & Replication establishes a connection between the source Veeam Data Mover and target Veeam Data Mover, and transports data from/to backup repositories via gateway servers.



Gateway Servers Deployment

The role of a gateway server can be assigned to a Microsoft Windows machine added to the backup infrastructure. To configure a gateway server, you must first add a machine that you plan to use as a gateway server to the backup infrastructure using the **New Windows Server wizard**. After that, you must go through the **Add New Backup Repository** wizard and define gateway server settings. You can select a gateway server explicitly or instruct Veeam Backup & Replication to select it automatically.

- If you select a gateway server explicitly, Veeam Backup & Replication uses the selected machine as a gateway server. Synthetic operations are also performed on this gateway server.
- If you instruct Veeam Backup & Replication to select the gateway server automatically, Veeam Backup & Replication uses the following backup infrastructure components:

Type of Job	Gateway server	Synthetic operations
Backup job	Backup proxy that was assigned the first to process VM data for a backup job.	Synthetic operations are performed on the mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server.

Backup copy job	<ul style="list-style-type: none"> • Direct data path: mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server. • Over WAN accelerators: source and/or target WAN accelerator (depending on the shared folder backup repository location). 	<p>Synthetic operations are performed on the mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server.</p> <p>These rules are applied to the direct data path and processing over WAN accelerators.</p>
Tape job	<p>If there is a direct connection between a backup repository and tape device, the role of a gateway server is assigned to the tape server.</p> <p>Otherwise, the role of a gateway server is assigned to the backup server.</p>	<p>Synthetic operations are performed on the mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server.</p>
Veeam Agent backup job	Backup server	Synthetic operations are performed on the backup server.
Restore operations	Backup proxy used for a restore operation	—
Replication from backup	Target backup proxy assigned for a replication operation	—

In the common case, a machine to which you assign the role of a gateway server must be located as close to the backup repository as possible. However, if you use a deduplicating storage appliance with source-side data deduplication, it is reasonable to assign the role of a gateway server to a machine that is located closer to the backup proxy. This will help you reduce the amount of traffic travelling over the network. For more information, see [EMC Data Domain](#) and [HPE StoreOnce](#).

For backup jobs Veeam Backup & Replication may use one or several gateway servers to process VMs. The number of gateway servers depends on the backup repository settings:

- If the **Use per-VM backup files** option is disabled, Veeam Backup & Replication selects one gateway server for the whole backup repository.
- If the **Use per-VM backup files** option is enabled, Veeam Backup & Replication selects a gateway server per every VM in the job.

For example, a backup job processes 2 VMs. The job is targeted at a backup repository for which the **Use per-VM backup files** option is enabled. In this case, Veeam Backup & Replication will detect which backup proxies were used to process VMs in the job. If VMs were processed with 2 different backup proxies, Veeam Backup & Replication will assign the role of gateway servers to these backup proxies. If VMs were processed with the same backup proxy, Veeam Backup & Replication will assign the role of a gateway server to this backup proxy, and will use it for both VMs in the job.

For scale-out backup repositories, Veeam Backup & Replication uses one gateway server per every extent. The rules of gateway server selection are described above.

Requirements for Gateway Servers

A machine that performs the role of a gateway server must meet the following requirements:

- The machine must meet the system requirements. For more information, see [System Requirements](#).
- The gateway server can run on a physical or virtual machine.

- The gateway server can run on a Microsoft Windows machine.
- You must add the machine to the Veeam Backup & Replication console as a managed server.
- The machine must have access to the backup repository – shared folder, EMC Data Domain or HPE StoreOnce.

Limitations for Gateway Servers

The following limitations apply to a machine that performs the role of a gateway server:

- For deduplicating storage appliances working over Fibre Channel, you must explicitly select a gateway server that will communicate with the appliance. As a gateway server, you must use a Microsoft Windows machine that is added to the backup infrastructure and has access to the appliance over Fibre Channel.
- For HPE StoreOnce deduplicating storage appliances, you must assign the role of a gateway server to a 64-bit machine.

Related Topics

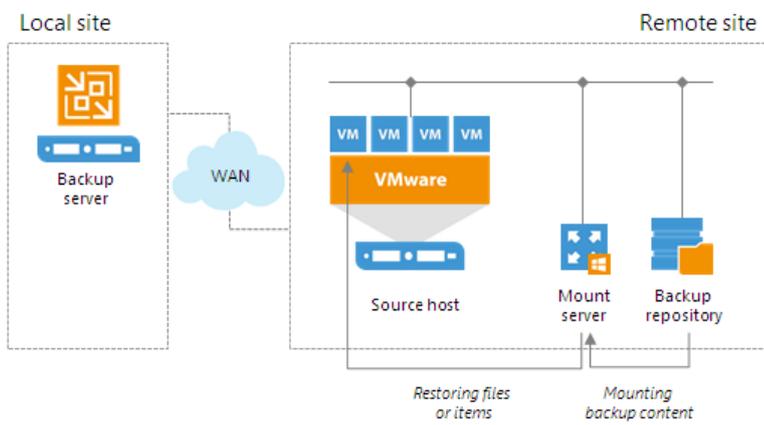
- [Backup Repository](#)
- [Scale-Out Backup Repository](#)
- [Dell EMC Data Domain](#)
- [HPE StoreOnce](#)
- [Specifying Server or Shared Folder Settings](#)

Mount Server

The mount server is required if you restore VM guest OS files and application items to the original location or perform secure restore. The mount server lets you route VM traffic by an optimal way, reduce load on the network and speed up the restore process.

When you perform file-level, application item or secure restore, Veeam Backup & Replication needs to mount the content of the backup file to a staging server (or the original VM for restore to the Microsoft SQL Server and Oracle VMs). Once the VM backup is mounted, Veeam Backup & Replication copies files or items to their destination via this mount server or VM. For more information about possible mount points, see [File-Level Restore Scenarios](#).

The staging server must be located in the same site as the backup repository where backup files are stored. In this case, you will be able to keep the VM traffic in one site. If the staging server is located in some other site, the data will need to travel across the network between the sites.



Mount Server Deployment

The mount server is created for every backup repository and is associated with it. When you configure a backup repository, you define which server you want to use as a mount server for this backup repository. By default, Veeam Backup & Replication assigns the mount server role to the following machines:

- **Backup repository.** For Microsoft Windows backup repositories, the mount server role is assigned to the backup repository server itself.
- **Veeam backup server.** For Linux, shared folder backup repositories and deduplicating storage appliances, the mount server role is assigned to the Veeam backup server.
- **Veeam Backup & Replication console.** The mount server role is also assigned to a machine on which the Veeam Backup & Replication console is installed. Note that this type of mount server is not registered in the Veeam Backup & Replication configuration database.

For scale-out backup repositories, you must define the mount server for every extent.

If you do not want to use default mount servers, you can assign the mount server role to any 64-bit Microsoft Windows machine in the backup infrastructure. It is recommended that you configure at least one mount server in each site and associate this mount server with the backup repository residing in this site. The mount server and backup repository must be located as close to each other as possible.

NOTE:

For cloud repositories and hosts that store replicas or backups from storage snapshots, the mount server role is assigned to the Veeam backup server. For such repositories, you cannot assign the mount server role to a different machine.

Mount Servers Services and Components

On the mount server machine, Veeam Backup & Replication installs the Veeam Mount Service. The Veeam Mount Service requires .NET 4.6. If .NET 4.6 is not installed on the machine, Veeam Backup & Replication will install it automatically.

Requirements for Mount Servers

A machine that performs the role of a mount server must meet the following requirements:

- You can assign the role of a mount server to a Microsoft Windows machine.
- You can assign the role of a mount server to a 64-bit machine.
- The mount server must have access to the backup repository with which it is associated and to the original VM (VM to which you restore files or application items). For restore from storage snapshots, the mount server must also have access to the ESX(i) host on which the temporary VM is registered.

Veeam vPower NFS Service

The vPower technology enables the following features:

- Recovery verification
- Instant VM Recovery
- Staged restore
- Universal Application-Item Recovery (U-AIR)
- Multi-OS file-level restore

The key construct of the vPower technology is the vPower NFS Service. The vPower NFS Service is a Microsoft Windows service that runs on a Microsoft Windows machine and enables this machine to act as an NFS server.

On the vPower NFS server, Veeam Backup & Replication creates a special directory – the vPower NFS datastore. When you start a VM from the backup, Veeam Backup & Replication "publishes" VMDK files of the VM from the backup on the vPower NFS datastore. Technically, Veeam Backup & Replication emulates the presence of VMDK files on the vPower NFS datastore – the VMDK files themselves are still located in the backup file on the backup repository.

The vPower NFS datastore is then mounted to the ESX(i) host. As a result, the ESX(i) host can "see" backed up VM images via the vPower NFS datastore and work with them as with regular VMDK files. The emulated VMDK files function as pointers to the real VMDK files in the backup on the backup repository.

IMPORTANT!

Veeam vPower NFS datastores are service datastores that can be used for vPower operations only. You cannot use them as regular VMware vSphere datastores – for example, you cannot place files of replicated VMs on such datastores.

vPower NFS Server Location

If you store backups on a Microsoft Windows backup repository, it is strongly recommended that you enable the vPower NFS server on this backup repository. In this case, Veeam Backup & Replication will be able to set up a direct connection between the backup repository and ESX(i) to which the vPower NFS datastore is mounted.

The Veeam vPower NFS Service can also run on any Microsoft Windows server in the backup infrastructure, including the backup server itself. However, in this case the recovery verification performance may decrease. The connection between the ESX(i) host and backup repository will be split into two parts:

1. From ESX(i) host to the vPower NFS server
2. From the vPower NFS server to the backup repository

vPower-Specific Settings

To establish a connection between the ESX(i) host and vPower NFS server, you must make sure that the ESX(i) host has a proper network interface configuration and can access the vPower NFS server.

When connecting to the vPower NFS server, the ESX(i) host uses a VMkernel interface. For this reason, the ESX(i) host must have a VMkernel interface. Otherwise, Veeam Backup & Replication will fail to mount the vPower NFS datastore on the ESX(i) host.

By default, VMkernel interfaces are not available for non-ESXi versions of VMware vSphere hosts. You will have to add them manually.

- If the vPower NFS server and ESX host are located in the same network, the ESX host must have a VMkernel interface in the same IP network as the vPower NFS server.
- If the vPower NFS server and ESX host are located in different networks and use a router for network access, in addition to creating a new VMkernel interface, you will have to manually specify routing settings in the IP routing table on the ESX host.

TIP:

To check if an ESX host can access the vPower NFS server, you can use the *vmkping* utility on the ESX host. The *vmkping* utility is similar to the ping tool. The only difference is that ICMP packets are sent via the VMkernel interface rather than the service console interface.

WAN Accelerators

WAN accelerators are dedicated components that Veeam Backup & Replication uses for WAN acceleration. WAN accelerators are responsible for global data caching and data deduplication. For more information, see [WAN Acceleration](#).

Log Shipping Servers

Log shipping servers are dedicated components that Veeam Backup & Replication uses for backup of Microsoft SQL Server transaction logs and Oracle archive logs. For more information, see [Microsoft SQL Server Logs Backup and Restore](#) and [Oracle Logs Backup and Restore](#),

Tape Servers

Tape servers are dedicated components responsible for transferring data between data source and tape device. For more information, see the [Tape Devices Support Guide](#).

NDMP Servers

If your NAS device supports the NDMP protocol, you can back up data from it to tape. To do this, you need to add the NAS device as an NDMP server. For more information, see [NDMP Servers Backup to Tape](#).

Veeam Backup Enterprise Manager

Veeam Backup Enterprise Manager is an optional component intended for distributed enterprise environments with multiple backup servers. Veeam Backup Enterprise Manager federates backup servers and offers a consolidated view of these servers through a web browser interface. You can centrally control and manage all jobs through a single "pane of glass", edit and clone jobs, monitor job state and get reporting data across all backup servers. Veeam Backup Enterprise Manager also enables you to search for VM guest OS files in all current and archived backups across your backup infrastructure, and restore these files in one click.

Veeam Backup Enterprise Manager Deployment

Veeam Backup Enterprise Manager can be installed on a physical or virtual machine. You can deploy it on the backup server or use a dedicated machine.

Veeam Backup Enterprise Manager Services and Components

Veeam Backup Enterprise Manager uses the following services and components:

- **Veeam Backup Enterprise Manager Service** coordinates all operations of Veeam Backup Enterprise Manager, aggregates data from multiple backup servers and provides control over these servers.
- **Veeam Backup Enterprise Manager Configuration Database** is used by Veeam Backup Enterprise Manager for storing data. The database instance can be located on a SQL Server installed either locally (on the same machine as Veeam Backup Enterprise Manager Server) or remotely.
- **Veeam Guest Catalog Service** replicates and consolidates VM guest OS file system indexing data from backup servers added to Veeam Backup Enterprise Manager. Index data is stored in Veeam Backup Enterprise Manager Catalog (a folder on the Veeam Backup Enterprise Manager Server) and is used to search for VM guest OS files in backups created by Veeam Backup & Replication.

Deployment Scenarios

Veeam Backup & Replication can be used in virtual environments of any size and complexity. The architecture of the solution supports onsite and offsite data protection, operations across remote sites and geographically dispersed locations. Veeam Backup & Replication provides flexible scalability and easily adapts to the needs of your virtual environment.

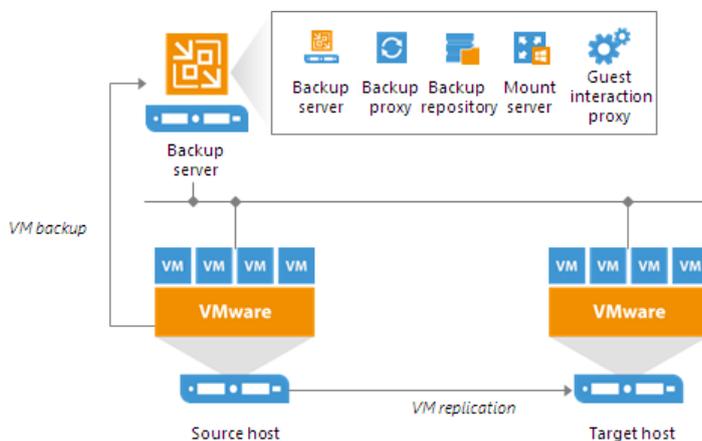
Before installing Veeam Backup & Replication, familiarize yourself with common deployment scenarios and carefully plan your backup infrastructure layout.

Simple Deployment

In a simple deployment scenario, one instance of Veeam Backup & Replication is installed on a physical or virtual Windows-based machine. This installation is referred to as a backup server.

Simple deployment implies that the backup server performs the following roles:

- It functions as a management point, coordinates all jobs, controls their scheduling and performs other administrative activities.
- It acts as the default backup proxy for handling job processing and transferring backup traffic. All services necessary for the backup proxy functionality are installed on the backup server locally.
- It is used as the default backup repository. During installation, Veeam Backup & Replication checks volumes of the machine on which you install the product and identifies a volume with the greatest amount of free disk space. On this volume, Veeam Backup & Replication creates the *Backup* folder that is used as the default backup repository.
- It is used as a mount server and guest interaction proxy.



If you plan to back up and replicate only a small number of VMs or evaluate Veeam Backup & Replication, this configuration is enough to get you started. Veeam Backup & Replication is ready for use right out of the box – as soon as it is installed, you can start using the solution to perform backup and replication operations. To balance the load of backing up and replicating your VMs, you can schedule jobs at different times.

NOTE:

If you decide to use simple deployment scenario, it is recommended that you install Veeam Backup & Replication on a VM, which will enable you to use the Virtual appliance transport mode, allowing for LAN-free data transfer. For details, see [Transport Modes](#).

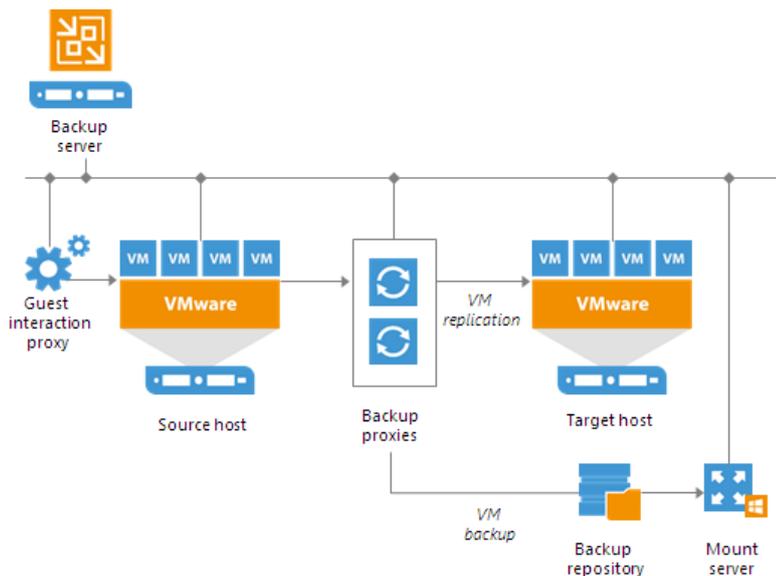
The drawback of a simple deployment scenario is that all data is handled and stored on the backup server locally. For medium-size or large-scale environments, the capacity of a single backup server may not be enough. To take the load off the backup server and balance it throughout your backup infrastructure, we recommend that you use the advanced deployment scenario. For details, see [Advanced Deployment](#).

Advanced Deployment

In large-scale virtual environments with a large number of jobs, the load on the backup server is heavy. In this case, it is recommended that you use the advanced deployment scenario that moves the backup workload to dedicated backup infrastructure components. The backup server here functions as a "manager" for deploying and maintaining backup infrastructure components.

The advanced deployment includes the following components:

- Virtual infrastructure servers – VMware vSphere hosts used as source and target for backup, replication and VM copy.
- Backup server – a configuration and control center of the backup infrastructure.
- Backup proxy – a "data mover" component used to retrieve VM data from the source datastore, process it and deliver to the target.
- Backup repository – a location used to store backup files, VM copies and auxiliary replica files.
- Dedicated mount servers – component required for VM guest OS files and application items restore to the original location.
- Dedicated guest interaction proxies – components used to deploy the runtime process in Microsoft Windows VMs.



With the advanced deployment scenario, you can easily meet your current and future data protection requirements. You can expand your backup infrastructure horizontally in a matter of minutes to match the amount of data you want to process and available network throughput. Instead of growing the number of backup servers or constantly tuning job scheduling, you can install multiple backup infrastructure components and distribute the backup workload among them. The installation process is fully automated, which simplifies deployment and maintenance of the backup infrastructure in your virtual environment.

In virtual environments with several proxies, Veeam Backup & Replication dynamically distributes backup traffic among these proxies. A job can be explicitly mapped to a specific proxy. Alternatively, you can let Veeam Backup & Replication choose the most suitable proxy. In this case, Veeam Backup & Replication will check settings of available proxies and select the most appropriate one for the job. The proxy server to be used should have access to the source and target hosts as well as to the backup repository to which files will be written.

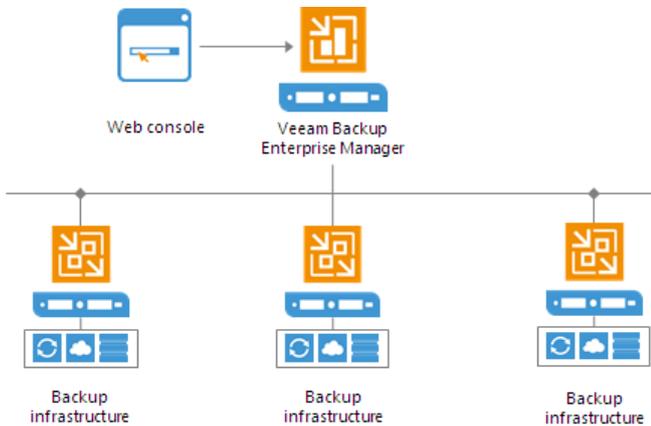
The advanced deployment scenario can be a good choice for backing up and replicating offsite. You can deploy a backup proxy in the production site and another one in the DR site, closer to the backup repository. When a job is performed, backup proxies on both sides establish a stable connection, so this architecture also allows for efficient transport of data over a slow network connection or WAN.

To regulate backup load, you can specify the maximum number of concurrent tasks per proxy and set up throttling rules to limit proxy bandwidth. The maximum number of concurrent tasks can also be specified for a backup repository in addition to the value of the combined data rate for it.

Another advantage of the advanced deployment scenario is that it contributes to high availability – jobs can migrate between proxies if one of them becomes overloaded or unavailable.

Distributed Deployment

The distributed deployment scenario is recommended for large geographically dispersed virtual environments with multiple backup servers installed across different sites. These backup servers are federated under Veeam Backup Enterprise Manager – an optional component that provides centralized management and reporting for these servers through a web interface.



Veeam Backup Enterprise Manager collects data from backup servers and enables you to run backup and replication jobs across the entire backup infrastructure through a single "pane of glass", edit them and clone jobs using a single job as a template. It also provides reporting data for various areas (for example, all jobs performed within the last 24 hours or 7 days, all VMs engaged in these jobs and so on). Using indexing data consolidated on one server, Veeam Backup Enterprise Manager provides advanced capabilities to search for VM guest OS files in VM backups created on all backup servers (even if they are stored on backup repositories on different sites), and recover them in a single click. Search for VM guest OS files is enabled through Veeam Backup Enterprise Manager itself.

With flexible delegation options and security roles, IT administrators can delegate the necessary file restore or VM restore rights to authorized personnel in the organization – for example, allow database administrators to restore Oracle or SQL server VMs.

If you use Veeam Backup Enterprise Manager in your backup infrastructure, you do not need to install licenses on every backup server you deploy. Instead, you can install one license on the Veeam Backup Enterprise Manager server and it will be applied to all servers across your backup infrastructure. This approach simplifies tracking license usage and license updates across multiple backup servers.

In addition, VMware administrators will benefit from Veeam plug-in for vSphere Web Client that can be installed using Veeam Backup Enterprise Manager. They can analyze cumulative information on used and available storage space view and statistics on processed VMs, review success, warning, failure counts for all jobs, easily identify unprotected VMs and perform capacity planning for repositories, all directly from vSphere.

Resource Scheduling

Veeam Backup & Replication has the built-in mechanism of resource scheduling. Resource scheduling lets Veeam Backup & Replication automatically define what backup infrastructure resources are required for data protection and disaster recovery jobs and tasks, select optimal resources and assign them for the jobs and tasks.

Resource scheduling is performed by the Veeam Backup Service running on the backup server. When a job or task starts, it communicates with the service and informs it about the resources it needs. The service analyzes job settings, parameters specified for backup infrastructure components, current load on the components, and automatically allocates optimal resources to the job.

For resource scheduling, Veeam Backup Service uses the following settings and features:

- [Limitation of Concurrent Tasks](#)
- [Limitation of Read and Write Data Rates for Backup Repositories](#)
- [Network Traffic Management](#)
- [Performance Bottlenecks](#)

Limitation of Concurrent Tasks

When you start a data protection or disaster recovery job, Veeam Backup & Replication analyzes the list of VMs added to the job, and creates a separate task for every disk of every VM to be processed.

Veeam Backup & Replication then defines what backup infrastructure components must be used for the job, checks what backup infrastructure components are currently available, and assigns necessary components to process the created job tasks.

Backup infrastructure components typically process several tasks at the same time. You can limit the number of tasks that backup infrastructure components must process concurrently. Task limitations help you balance the workload across the backup infrastructure and avoid performance bottlenecks.

Veeam Backup & Replication lets you limit the number of concurrent tasks for the following backup infrastructure components:

- [Backup proxies](#)
- [Backup repositories](#)

NOTE:

Task limits set for backup infrastructure components influence the job performance. For example, you add a VM with 4 disks to a job and assign a backup proxy that can process maximum 2 tasks concurrently for the job. In this case, Veeam Backup & Replication will create 4 tasks (1 task per each VM disk) and start processing 2 tasks in parallel. The other 2 tasks will be pending.

How Task Limitation Works

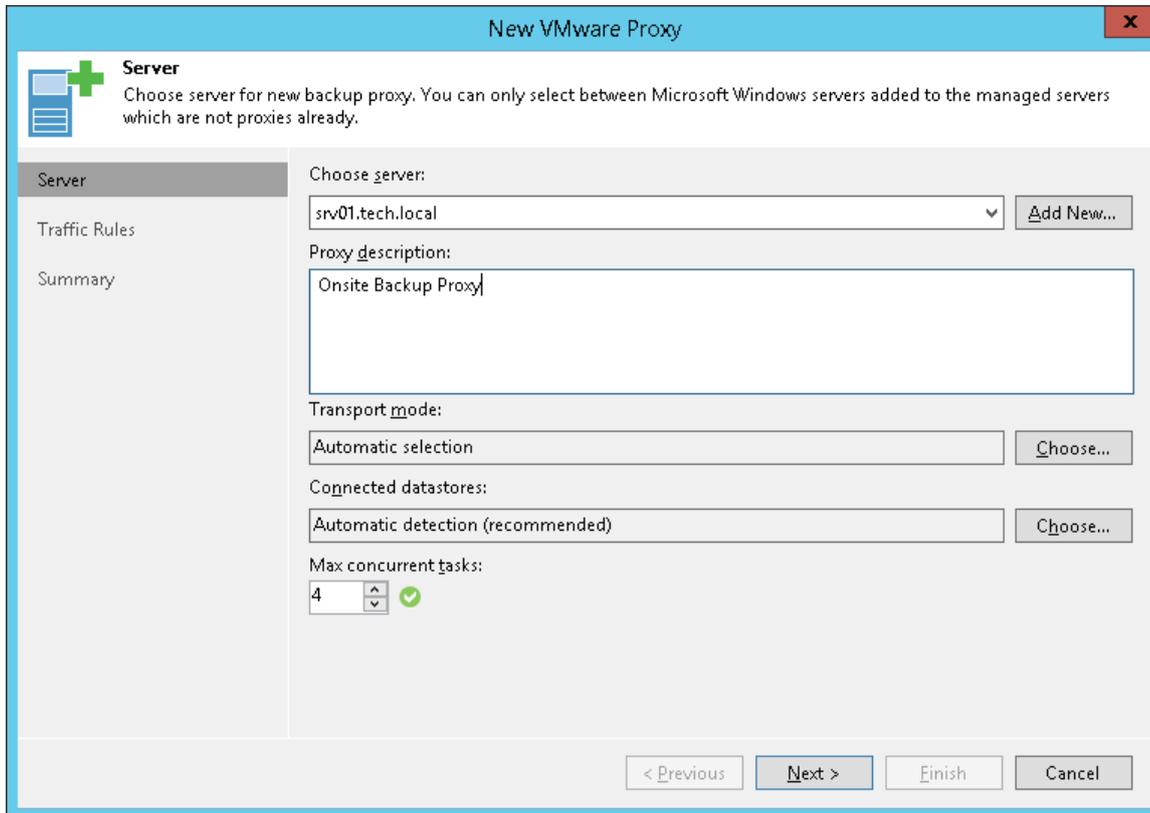
Task limiting is performed by the Veeam Backup Service. The Veeam Backup Service is aware of all backup proxies and backup repositories in the backup infrastructure, and task limitation settings configured for them.

When a job starts, it informs the Veeam Backup Service about the list of tasks created for the job, and backup infrastructure resources that must be used for the job. The Veeam Backup Service detects the number of tasks that required backup infrastructure components are currently processing, and analyzes the number of allowed tasks for these components. If the number of currently processed tasks has reached the allowed limit, the backup infrastructure component will not start processing a new task until one of the currently running tasks finishes.

Task Limitation for Backup Proxies

To limit the number of concurrent tasks on a backup proxy, you must define the **Max concurrent tasks** setting for the backup proxy.

The maximum number of concurrent tasks depends on the number of CPU cores available on the backup proxy. It is strongly recommended that you define task limitation settings using the following rule: 1 task = 1 CPU core. For example, if a backup proxy has 4 CPU cores, it is recommended that you limit the number of concurrent tasks for this backup proxy to 4.



Task Limitation for Backup Repositories

To limit the number of concurrent tasks on a backup repository, you must enable the **Limit maximum concurrent tasks to <N>** option on the backup repository and define the necessary task limit.

The maximum number of concurrent tasks depends on the number of CPU cores available on the backup repository. It is strongly recommended that you define task limitation settings using the following rule: 1 task = 1 CPU core.

It is recommended to configure 2 GB RAM per core. In case of shared folder backup repositories, the same amount of resources is required for gateway servers.

Synthetic operations performed on the backup repository (such as synthetic full backup, backup files merge and transform) are also regarded as tasks. The number of tasks performed during these operations depends on the type of backup chains stored on the backup repository:

- For regular backup chains, Veeam Backup & Replication creates 1 task per job.
- For per-VM backup chains, Veeam Backup & Replication creates 1 task per every VM chain (that is, every VM added to the job).

If you use backup repositories for backup copy jobs, you must also consider tasks for read operations.

NOTE:

When you limit the number of tasks for the backup repository, bear in mind the storage throughput. If the storage system is not able to keep up with the number of tasks that you have assigned, it will be the limiting factor. It is recommended that you test components and resources of the backup infrastructure to define the workload that they can handle.

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location
Path to folder: C:\Backups
Capacity:
Free space:

Load control
Running too many concurrent tasks against the same repository may reduce overall performance, and cause I/O operations to timeout. Control storage device saturation with the following settings:
 Limit maximum concurrent tasks to: 4
 Limit read and write data rates to: MB/s

Click Advanced to customize repository settings

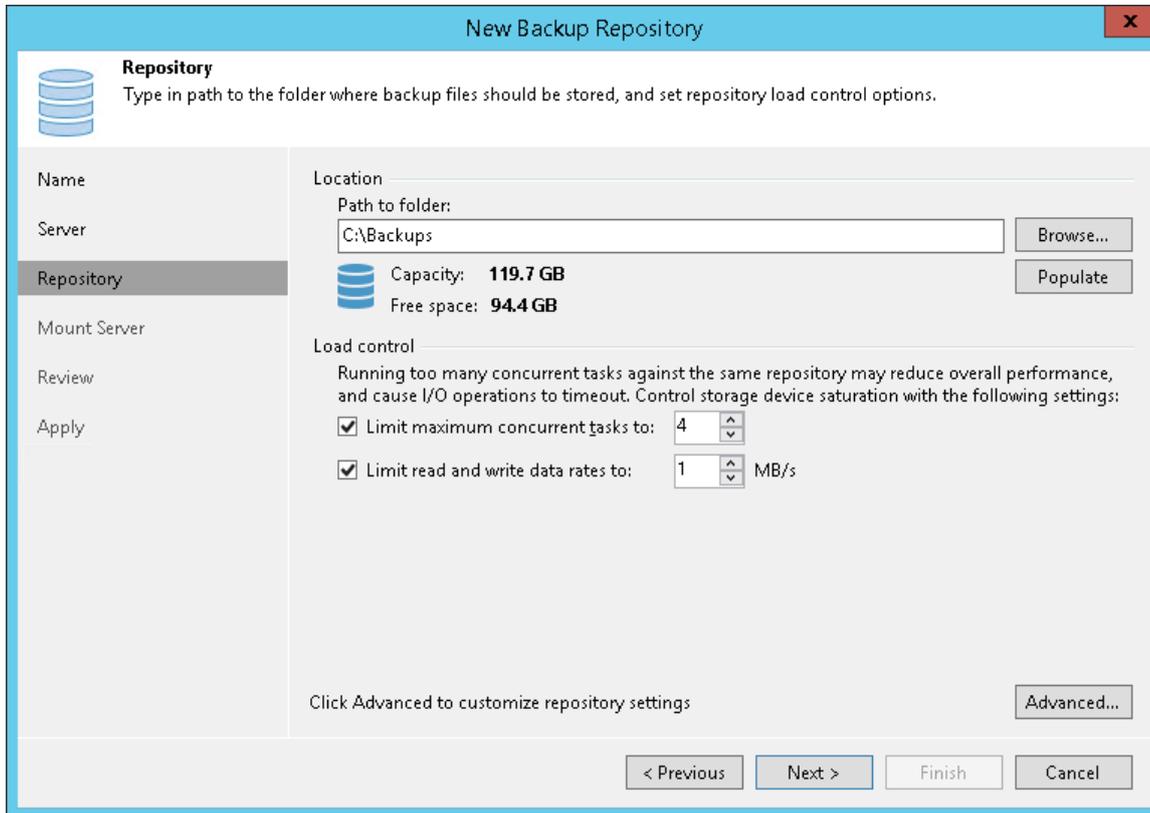
< Previous Next > Finish Cancel

Task Limitation for Components with Several Roles

One machine can perform several roles. For example, you can assign roles of the backup proxy and backup repository to the same machine, or use a backup proxy as a gateway server for a shared folder backup repository. In such situation, you must make sure that the backup infrastructure component is able to process the cumulative number of tasks specified for different roles.

Limitation of Read and Write Data Rates for Backup Repositories

Veeam Backup & Replication can limit the speed with which Veeam Backup & Replication must read and write data to/from the backup repository. The data read and write speed is controlled with the **Limit read and write data rates to <N> MB/s** option that you can enable in backup repository settings.



The Veeam Backup Service is aware of read and write data rate settings configured for all backup repositories in the backup infrastructure. When a job targeted at a backup repository starts, the Veeam Backup Service informs the Veeam Data Mover running on this backup repository about the allowed read/write speed set for this repository so that the Veeam Data Mover can limit the read/write speed to the specified value.

If the backup repository is used by a number of tasks simultaneously, Veeam Backup & Replication splits the allowed read/write speed rate between these tasks equally. Note that the specified limit defines the allowed read speed and the allowed write speed at the same time.

For example, you set the **Limit read and write data rates to** option to 8 MB/s and start two backup jobs. Each job processes 1 VM with 1 VM disk. In this case, Veeam Backup & Replication will create 2 tasks and target them at the backup repository. The data write rate will be split between these 2 tasks equally: 4 MB/s for one task and 4 MB/s for the other task.

If at this moment you start some job reading data from the same backup repository, for example, a backup copy job processing 1 VM with 1 disk, Veeam Backup & Replication will assign the read speed rate equal to 8 MB/s to this job. If you start 2 backup copy jobs at the same time (each processing 1 VM with 1 disk), Veeam Backup & Replication will split the read speed rate between these 2 jobs equally: 4 MB/s for one backup copy job and 4 MB/s for the other backup copy job.

Network Traffic Management

You can specify the following network settings to manage network traffic in the backup infrastructure:

- [Setting Network Traffic Throttling Rules](#)
- [Managing Data Transfer Connections](#)
- [Enabling Network Data Encryption](#)
- [Specifying Preferred Networks for Data Transfer](#)

Configuring Network Traffic Throttling Rules

To limit the impact of Veeam Backup & Replication tasks on network performance, you can throttle network traffic for jobs. Network traffic throttling prevents jobs from utilizing the entire bandwidth available in your environment and makes sure that enough traffic is provided for other network operations. It is especially recommended that you throttle network traffic if you perform offsite backup or replicate VMs to a DR site over slow WAN links.

Network traffic throttling is implemented through rules. Network throttling rules apply to components in the Veeam backup infrastructure, so you do not have to make any changes to the network infrastructure.

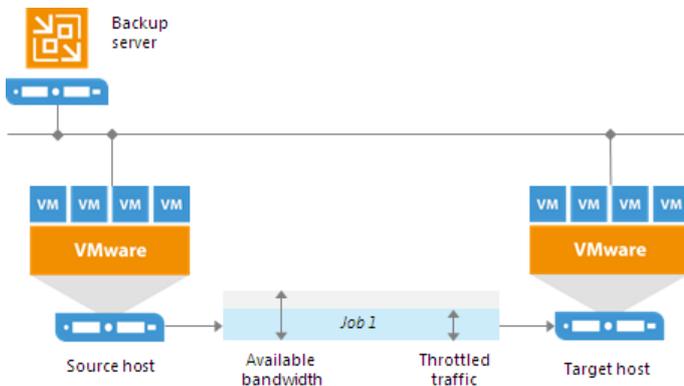
Network traffic throttling rules are enforced globally, at the level of the backup server. Every rule limits the maximum throughput of traffic going between backup infrastructure components on which Veeam Data Movers are deployed. Depending on the scenario, traffic can be throttled between the following components:

- Backup to a Microsoft Windows or Linux backup repository: a backup proxy and backup repository
- Backup to an SMB share, Dell EMC Data Domain and HPE StoreOnce: backup proxy and gateway server
- VM copy: backup proxy and backup repository
- Backup copy: source and target backup repositories or gateway servers, or WAN accelerators (if WAN accelerators are engaged in the backup copy process)
- Replication: source and target backup proxies or WAN accelerators (if WAN accelerators are engaged in the replication process)
- Backup to tape: backup repository and tape server

Rules are set for a pair of IP address ranges and are applied to the source and target components between which data is transferred over the network. The range can include a single IP address.

How Network Traffic Throttling Works

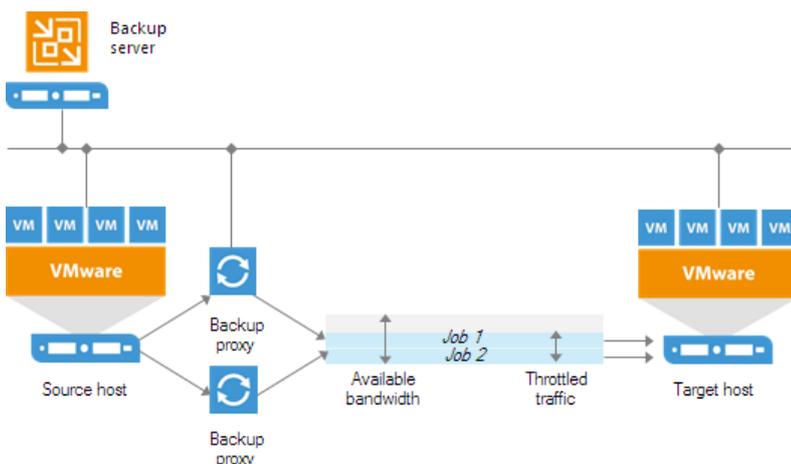
When a new job starts, Veeam Backup & Replication checks network traffic throttling rules against a pair of components assigned for the job. If the source and target IP addresses fall into specified IP ranges, the rule is applied. For example, if for a network traffic throttling rule you specify 192.168.0.1 – 192.168.0.255 as the source range and 172.16.0.1 – 172.16.0.255 as the target range, and the source component has IP address 192.168.0.12, while the target component has IP address 172.16.0.31, the rule will be applied. The network traffic going from source to target will be throttled.



NOTE:

Throttling rules are reversible – they function in two directions. If the IP address of the component on the source side falls into the target IP range, and the IP address of the component on the target side falls into the source IP range, the rule will be applied in any case.

Veeam Backup & Replication equally splits available bandwidth between all jobs that use backup infrastructure components to which a network throttling rule applies. For example, if you run one job that uses a pair of backup infrastructure components to which the rule applies, the job will get the entire bandwidth allowed by the rule. If you run two jobs at a time, the allowed bandwidth will be equally split between them. As soon as one of the jobs completes, the bandwidth assigned to it will be freed, and the remaining job will use the entire bandwidth allowed by the rule.



Throttling rules can be scheduled to only be active during specific time intervals (for example, during business hours). This way, you can minimize the impact of job performance spikes on the production network. Alternatively, you can select to apply throttling rules regardless of the time.

Several Network Throttling Rules

If you create several traffic throttling rules for the same range of IP addresses, make sure that time intervals when these rules are enforced do not overlap. For example, to manage network traffic during business and non-business hours, you can create two network traffic throttling rules:

- Rule 1 limits the speed to 1 Mbps Monday through Friday from 7 AM to 7 PM.
- Rule 2 limits the speed to 10 Mbps on weekends and from 7 PM to 7 AM on weekdays.

In this case, Veeam Backup & Replication will limit the data transfer speed to 1 Mbps during business hours, while during non-business hours the speed will be limited to 10 Mbps.

If several throttling rules use the same target IP address range but have different speed limits, the rule with the lowest transfer speed will be used. For example, you have configured two rules:

- Rule 1 limits the speed to 4 Mbps: source IP range 192.168.0.1 - 192.168.0.30 and target IP range 192.168.0.1 - 192.168.0.255
- Rule 2 limits the speed to 1 Mbps: source IP range 192.168.0.1 - 192.168.0.255 and target IP range 192.168.0.1 - 192.168.0.255

Veeam Backup & Replication will use the lowest transfer speed for backup infrastructure components that fall into the source and target IP ranges – that is, a 1 Mbps rule.

Setting Network Traffic Throttling Rules

To create a network throttling rule:

1. From the main menu, select **Network Traffic Rules**.
2. In the **Global Network Traffic Rules** window, click **Add**.
3. In the **Source IP address range** section, specify a range of IP addresses for backup infrastructure components on the source side.
4. In the **Target IP address range** section, specify a range of IP addresses for backup infrastructure components on the target side.
5. Select the **Throttle network traffic** check box.
6. In the **Throttle to** field, specify the maximum speed that must be used to transfer VM data from source to target.
7. In the **Apply throttling** section, specify the time interval during which the rule must be enforced. You can select to use throttling rules all the time or schedule traffic throttling at specific time intervals, for example, during business hours to minimize the impact of data protection activities on the production network.

TIP:

You can view which network traffic throttling rules apply to a backup proxy at the **Traffic** step of the backup proxy wizard.

Add New Network Traffic Rule

Source IP address range:
192 . 168 . 0 . 1 to 192 . 168 . 0 . 255

Target IP address range:
192 . 168 . 0 . 1 to 192 . 168 . 0 . 255

Action:
 Encrypt network traffic
 Throttle network traffic

Throttle to:
1 Mbps

Apply throttling:
 All the time
 During the specified time periods only:

Monday through Friday from 5:00 AM to 9:59 PM

OK Cancel

Managing Data Transfer Connections

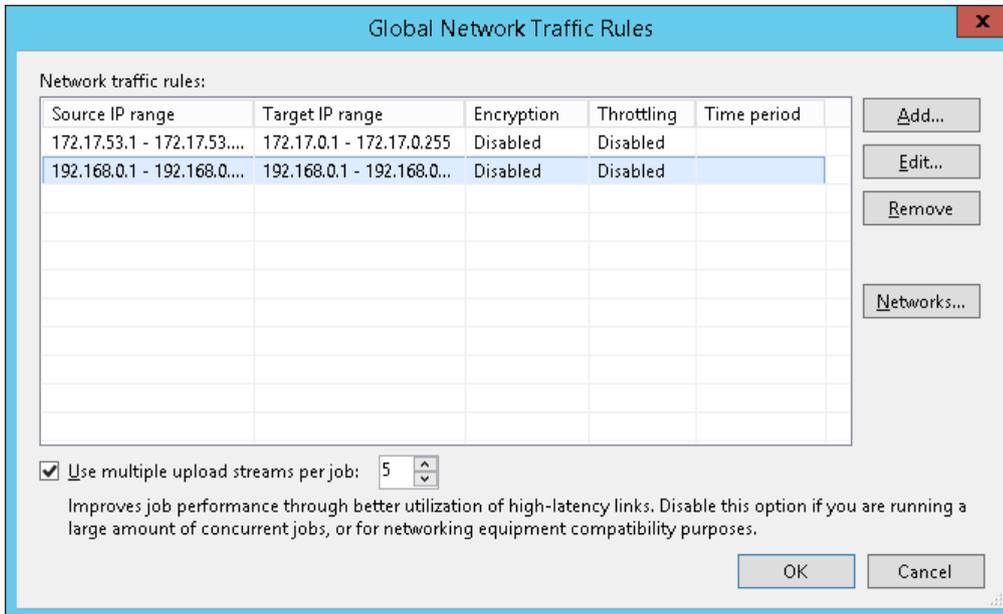
By default, Veeam Backup & Replication uses multithreaded data transfer for every job session. VM data going from source to target is transferred over 5 TCP/IP connections. However, if you schedule several jobs to run at the same time, load on the network may be heavy. If the network capacity is not sufficient to support multiple data transfer connections, you can disable multithreaded data transfer or change the number of TCP/IP connections.

To change the number of connections:

1. From the main menu, select **Network Traffic**.
2. In the **Global Network Traffic Rules** window, specify new data transfer settings:
 - To disable multithreaded data transfer, clear the **Use multiple upload streams per job** check box. Veeam Backup & Replication will use only one TCP/IP transfer connection for every job session.
 - To change the number of TCP/IP connections, leave the **Use multiple upload streams per job** check selected and specify the necessary number of connections in the field on the right.

NOTE:

Veeam Backup & Replication performs a CRC check for the TCP traffic going between the source and the target. When you perform backup, replication or VM copy operations, Veeam Backup & Replication calculates checksums for data blocks going from the source. On the target, it re-calculates checksums for received data blocks and compares them to the checksums created on the source. If the CRC check fails, Veeam Backup & Replication automatically re-sends data blocks without any impact on the job.



Enabling Network Data Encryption

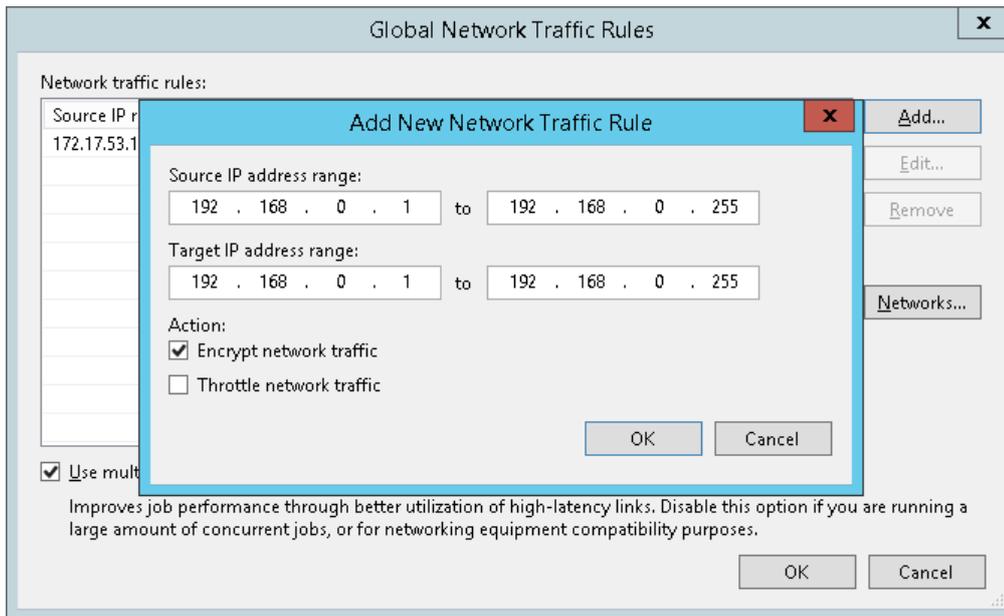
You can enable network traffic encryption for data going between the source side and target side. Network traffic encryption helps you raise the security level for your data. If encrypted data is intercepted in the middle of data transfer, the eavesdropper will not be able to decrypt it and get access to it.

Veeam Backup & Replication encrypts the network traffic according to the 256-bit Advanced Encryption Standard (AES). Data transferred between public networks is encrypted by default. If you want to enable network data encryption within the same network, you must create a network traffic rule for this network and enable the data encryption option for this rule.

To enable network traffic encryption within the same network:

1. From the main menu, select **Network Traffic**.
2. In the **Global Network Traffic Rules** window, click **Add**.
3. In the **Source IP address range** section, specify a source range of IP addresses in the network for which you want to enable data encryption.
4. In the **Target IP address range** section, specify a target range of IP addresses in the same network.
5. Select the **Encrypt network traffic** check box.

As a result, data traffic going between backup infrastructure components whose IP addresses fall into the source and target IP address ranges will be encrypted.



Specifying Preferred Networks for Data Transfer

You can choose networks over which Veeam Backup & Replication must transport VM data when you perform data protection and disaster recovery tasks. This option can be helpful if you have a non-production network and want to route VM data traffic over this network instead of the production one.

Preferred network rules are applied to the following backup infrastructure components:

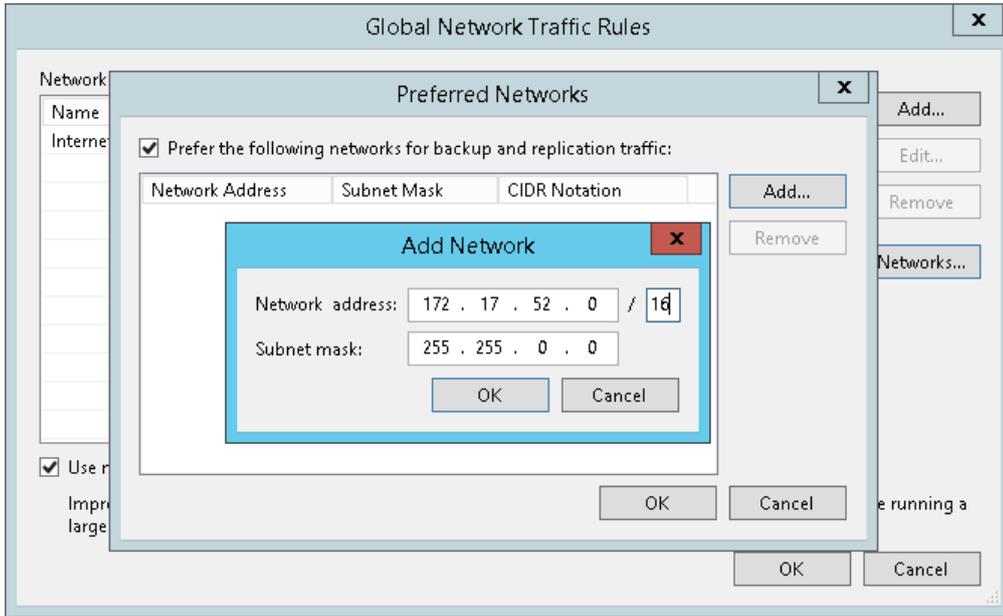
- Backup proxies
- Backup repositories
- WAN accelerators
- Gateways (used with backup repositories)
- Log shipping servers
- Tape servers
- Supported storage systems (except Cisco HyperFlex)

To define networks for data transfer, you must create a list of preferred networks. When Veeam Backup & Replication needs to transfer VM data, it uses networks from this list. If a connection over preferred networks cannot be established for some reason, Veeam Backup & Replication will automatically fail over to the production network.

To set a network priority list:

1. From the main menu, select **Network Traffic**.
2. In the **Global Network Traffic Rules** window, click **Networks**.
3. In the **Preferred Networks** window, select the **Prefer the following networks for backup and replication traffic** check box.
4. Click **Add**.

5. Specify a network address using a CIDR notation or a network mask and click **Add**.
6. Repeat steps 4-5 for all networks that you want to add.



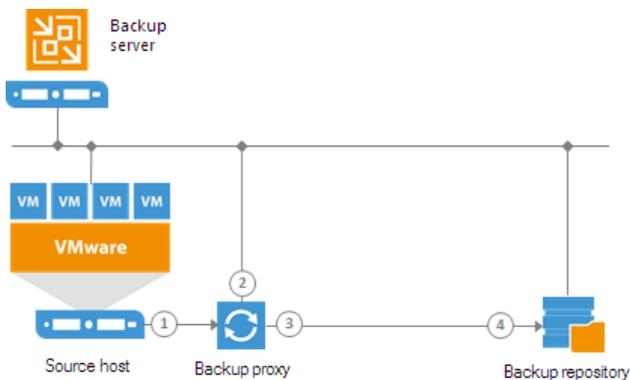
Performance Bottlenecks

As any backup application handles a great amount of data, it is important to make sure the data flow is efficient and all resources engaged in the backup process are optimally used. Veeam Backup & Replication provides advanced statistics about the data flow efficiency and lets you identify bottlenecks in the data transmission process.

Veeam Backup & Replication processes VM data in cycles. Every cycle includes a number of stages:

1. Reading VM data blocks from the source
2. Processing VM data on the backup proxy
3. Transporting data over the network
4. Writing data to the target

When one data processing cycle is over, the next cycle begins. VM data therefore goes over the "data pipe".



To evaluate the data pipe efficiency, Veeam Backup & Replication analyzes performance of all components in the data flow working as the cohesive system, and evaluates key factors on the source and target sides. Veeam Backup & Replication checks the following points in the data pipe:

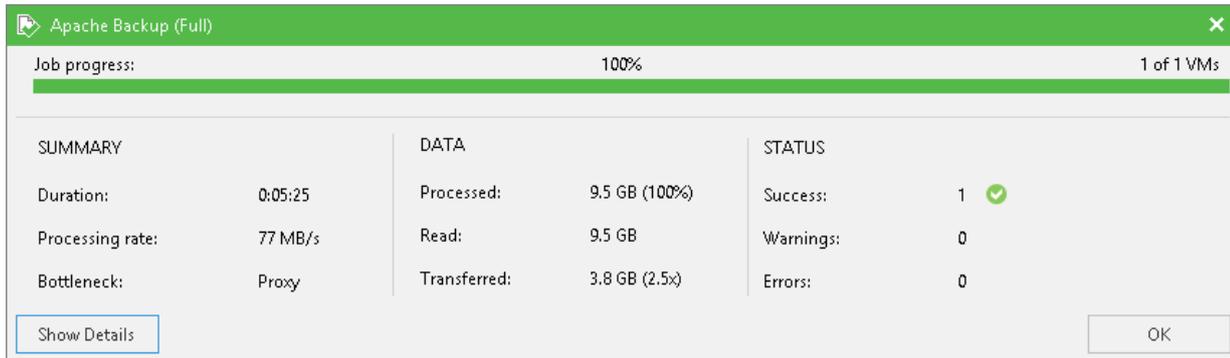
1. **Source** – source disk reader component responsible for retrieving data from the source storage.
2. **Proxy** – backup proxy component responsible for processing VM data.
3. **Source WAN accelerator** – WAN accelerator deployed on the source side. Used for backup copy and replication jobs working via WAN accelerators.
4. **Network** – network queue writer component responsible for getting processed VM data from the backup proxy and sending it over the network to the backup repository or another backup proxy.
5. **Target WAN Accelerator** – WAN accelerator deployed on the target side. Used for backup copy and replication jobs working via WAN accelerators.
6. **Target** – target disk writer component (backup storage or replica datastore).

The resource usage level for these points is evaluated in percent. This percent rate defines the amount of time for which components are busy during the job. An efficient data flow assumes that there is no latency at any point of the data pipe, and all its components work for approximately equal amount of time.

If any of the components operates inefficiently, there may appear a bottleneck in the data path. The insufficient component will work 100% of time while the others will be idling, waiting for data to be transferred. As a result, the whole data flow will slow down to the level of the slowest point in the data path, and the overall time of data processing will increase.

To identify a bottleneck in the data path, Veeam Backup & Replication detects the component with the maximum workload: that is, the component that works for the most time of the job. For example, you use a low-speed storage device as the backup repository. Even if VM data is retrieved from the SAN storage on the source side and transported over a high-speed link, VM data flow will still be impaired at the backup repository. The backup repository will be trying to consume transferred data at the rate that exceeds its capacity, and the other components will stay idle. As a result, the backup repository will be working 100% of job time, while other components may be employed, for example, for 60% only. In terms of Veeam Backup & Replication, such data path will be considered insufficient.

The bottleneck statistics for a job is displayed in the job session data. The bottleneck statistics does not necessarily mean that you have a problem in your backup infrastructure. It informs you about the weakest component in the data path. However, if you feel that the job performance is low, you may try taking some measures to get rid of the bottleneck. For example, in the case described above, you can limit the number of concurrent tasks for the backup repository.



Throttling as Bottleneck

In addition to main points in the data pipe, Veeam Backup & Replication may report throttling as a bottleneck. This can happen in the following cases:

- If you limit the read and write data rates for a backup repository, a backup repository may become a bottleneck. Veeam Backup & Replication will report *Throttling* in the bottleneck statistics.
- If you set up network throttling rules, network may become a bottleneck. Veeam Backup & Replication will report *Throttling* in the bottleneck statistics.

Locations

To control data migration in the virtual infrastructure, Veeam Backup & Replication introduces a notion of location. A location defines a geographic region, or country, in which an infrastructure object resides. You can create a list of locations, and assign to backup infrastructure objects information about locations to which they belong.

Veeam Backup & Replication allows you to assign information about locations to the following infrastructure objects:

- Virtual infrastructure objects: vCenter Servers, datacenters, clusters and hosts.
- Backup infrastructure objects: backup repositories, external repositories, scale-out backup repositories, tape libraries and tape vaults.
- Agent management objects: protection groups.
- Veeam Cloud Connect for service providers: cloud repositories and hardware plans.

Information about infrastructure objects location is stored in the Veeam Backup & Replication configuration database. When VM data in the virtual infrastructure migrate from one location to another, Veeam Backup & Replication displays a warning and stores a record about data migration to job or task session details. In addition to it, Veeam Backup & Replication logs this information to Microsoft Windows event logs. For example, if you back up VMs from a host that resides in Germany to a backup repository that resides in Australia, Veeam Backup & Replication will display a warning that VM data changes its location in the backup job wizard, display information about data migration in the backup job session details and log it to Microsoft Windows event logs.

Exchange Backup Job (Active Full) 0 of 3 VMs

Job progress: 37%

SUMMARY		DATA		STATUS	
Duration:	08:08	Processed:	41.8 GB (37%)	Success:	0
Processing rate:	97 MB/s	Read:	38.4 GB	Warnings:	0
Bottleneck:	Proxy	Transferred:	24.9 GB (1.5x)	Errors:	0

THROUGHPUT (LAST 5 MIN)

Speed: 90.7 MB/s

NAME	STATUS	ACTION	DURATI...
dc03	10%	Queued for processing at 1/25/2019 5:49:48 AM	
exch01	21%	Required backup infrastructure resources have been assigned	
dns01	99%	VM processing started at 1/25/2019 5:49:54 AM	
		VM size: 120.0 GB (27.5 GB used)	
		Getting VM info from vSphere	00:08
		Creating VM snapshot	00:02
		Potential data sovereignty violation: target Storage 01 location (UK) does not m...	
		Saving [esx02-ds1] exch01/exch01.vmx	00:00
		Saving [esx02-ds1] exch01/exch01.nvram	00:00
		Using backup proxy proxy01.tech.local for disk Hard disk 1 [hotadd]	00:23
		Hard disk 1 (120.0 GB) 19.9 GB read at 51 MB/s [CBT]	06:50

Hide Details OK

Veeam Backup & Replication displays information about VM data migration in statistics for the following types of jobs:

- Backup jobs – Veeam Backup & Replication compares the location of the source host on which VMs are registered with the location of the target backup repository or cloud repository.
- Backup copy jobs – Veeam Backup & Replication compares the location of the source host with the location of the target host.
- VeeamZIP tasks (except the cases when you select to store the VeeamZIP file in a local or shared folder) – Veeam Backup & Replication compares the location of the source host on which VMs are registered with the location of the target backup repository.
- Replication jobs – Veeam Backup & Replication compares the location of the source host on which VMs are registered with the location of the target host.
- Replica failback tasks – Veeam Backup & Replication compares the location of the source host with the location of the host to which the VM is restored.
- VM copy jobs – Veeam Backup & Replication compares the location of the source host on which VMs are registered with the location of the target backup repository or target host.
- Quick migration tasks – Veeam Backup & Replication compares the location of the source host on which VMs are registered with the location of the target host.
- Entire VM restore tasks – Veeam Backup & Replication compares the location of the source host with the location of the host to which VMs are restored.
- External repository tasks:
 - Backup copy jobs: Veeam Backup & Replication compares the location of the source external repository with the location of the target backup repository.
 - Restore to Amazon EC2: Veeam Backup & Replication compares the geographic region of the backed up EC2 instance with the geographic region of the target EC2 instance.
 - Restore to Microsoft Azure: Veeam Backup & Replication always displays a warning about VM data migration when restore to Microsoft Azure is performed from external repositories.
- SureBackup jobs – Veeam Backup & Replication compares the source location with the target location. The target location is always a host on which the virtual lab is registered. The source location may be one of the following:
 - If a VM is added to the application group, Veeam Backup & Replication compares the host on which the VM is registered (or was registered at the moment of backup) with the target location.
 - If a VM is added to the SureBackup job from the linked job, Veeam Backup & Replication compares the backup repository on which the backup file resides with the target location.
- Tape tasks:
 - Backup to tape jobs: In backup to tape jobs, Veeam Backup & Replication compares the location of the source job or repository with the location of the tape library in the target media pool. If the media pool spans multiple tape libraries, Veeam Backup & Replication analyzes locations of all libraries in the media pool.
 - Vaults: If a tape job exports offline backups to a vault, Veeam Backup & Replication compares the location of the source job or repository with the location of the vault. If a GFS tape job exports tapes to multiple vaults, Veeam Backup & Replication analyzes all vaults configured for target media pools of the GFS tape job.

- Media pools: Veeam Backup & Replication compares locations of all tape libraries added to the media pool. If the media pool exports tapes to a vault, Veeam Backup & Replication analyzes all vaults configured for the media pool.

Limitations for Locations

For SureReplica jobs, Veeam Backup & Replication does not compare information about source and target hosts location.

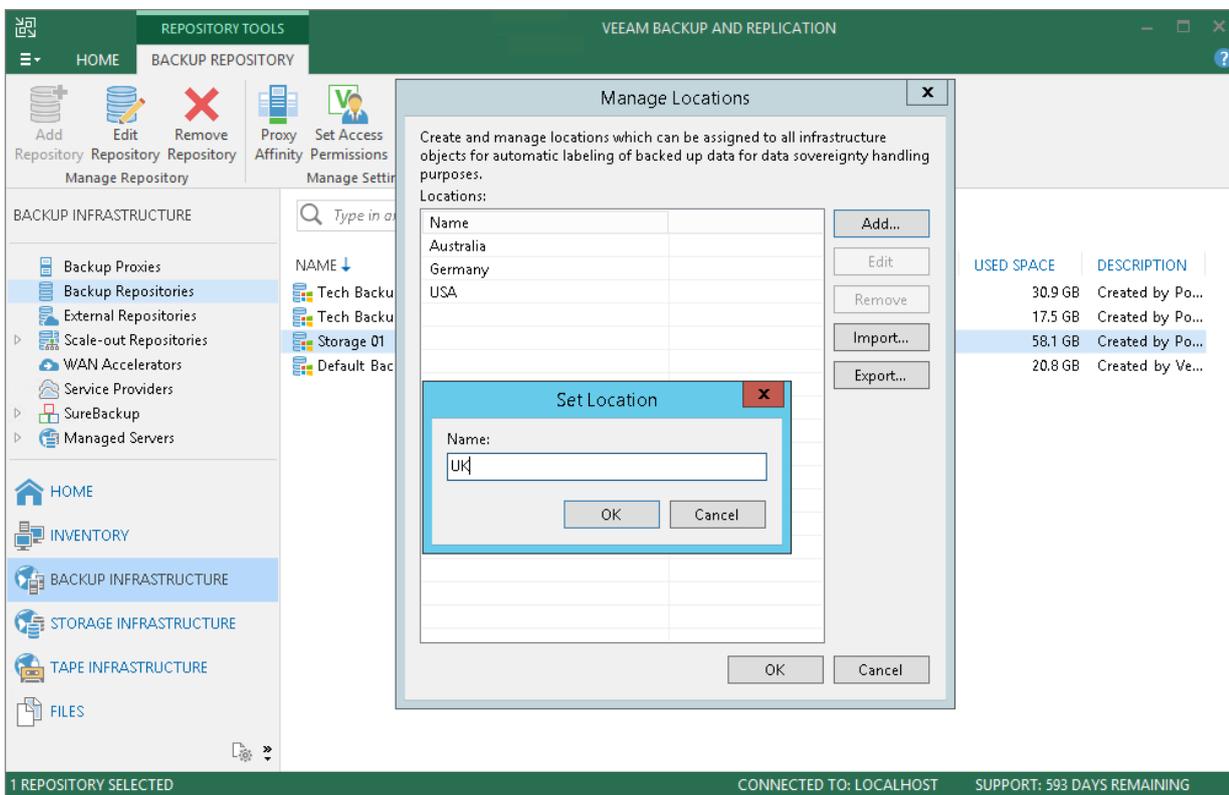
Veeam Backup & Replication does not display a warning about VM data migration for file copy jobs.

Creating and Assigning Locations to Infrastructure Objects

You can create a list of locations in Veeam Backup & Replication and assign locations to infrastructure objects. If you assign a location to root infrastructure host (SCVMM), it will be applied to all child hosts (clusters and HV Hosts). You can also assign the location to a child host.

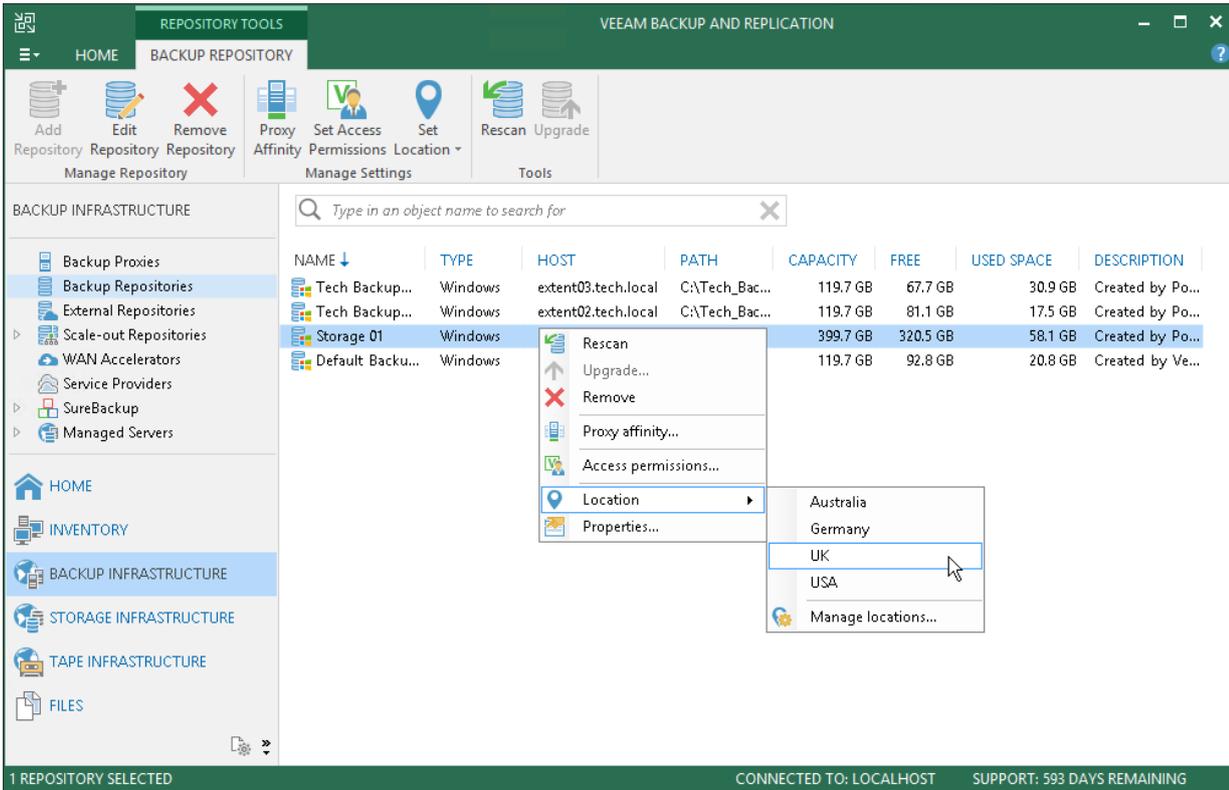
To create a location:

1. In the **Inventory** or **Backup Infrastructure** view, right-click the infrastructure object and select **Location > Manage locations**.
2. In the **Manage Locations** window, click **Add**.
3. In the **Name** field, enter a name of the location.



0.83"

To assign a location to an infrastructure object, in the **Inventory** or **Backup Infrastructure** view, right-click the infrastructure object and select **Location > <Location name>**. If the location is not in the list, select **Location > Manage Locations** and add the location to the list.



NOTE:

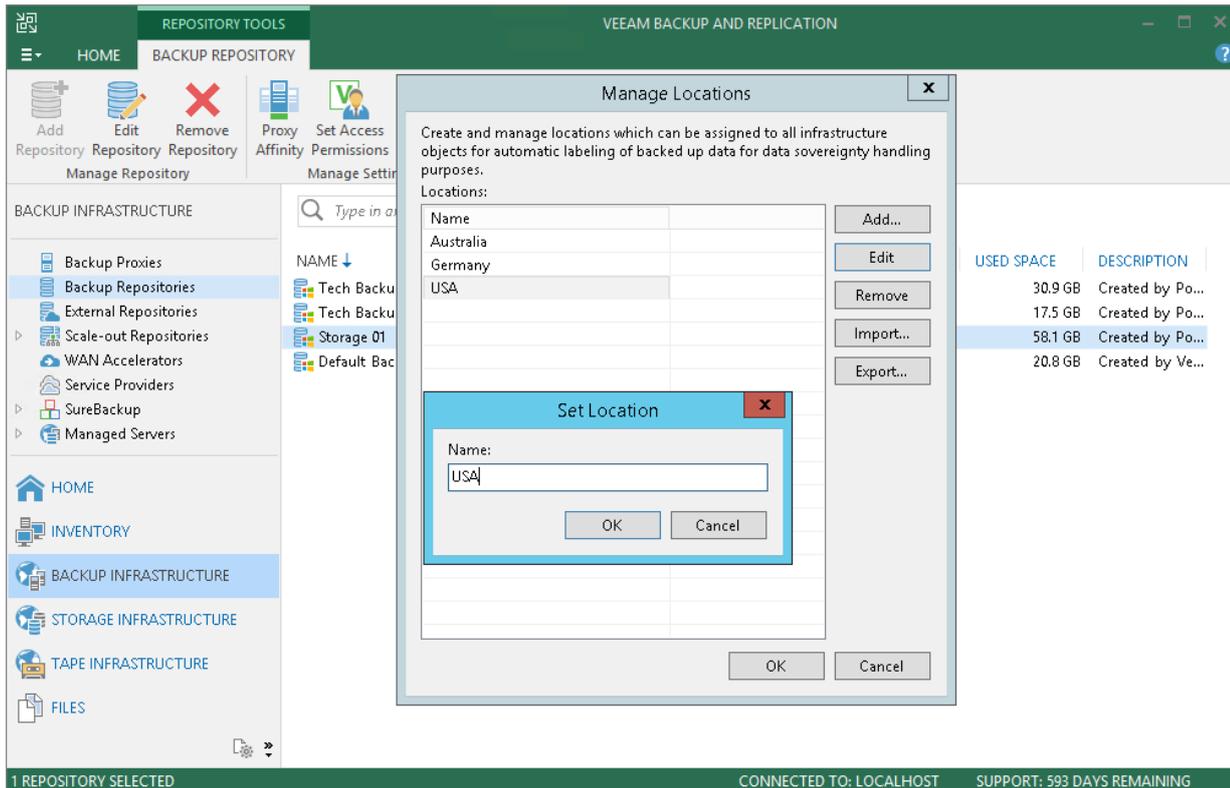
When assigning a location to a scale-out backup repository, the location will be global for all extents. If you add an extent whose location differs from the global location, it will be changed in favor of the location of the scale-out repository.

Editing Locations

You can edit a location in the locations list, for example, if you want to change the location name.

To edit a location:

1. In the **Inventory** or **Backup Infrastructure** view, right-click the infrastructure object and select **Location > Manage locations**.
2. In the **Manage Locations** window, select the location and click **Edit**.
3. In the **Name** field, change the location name as required.

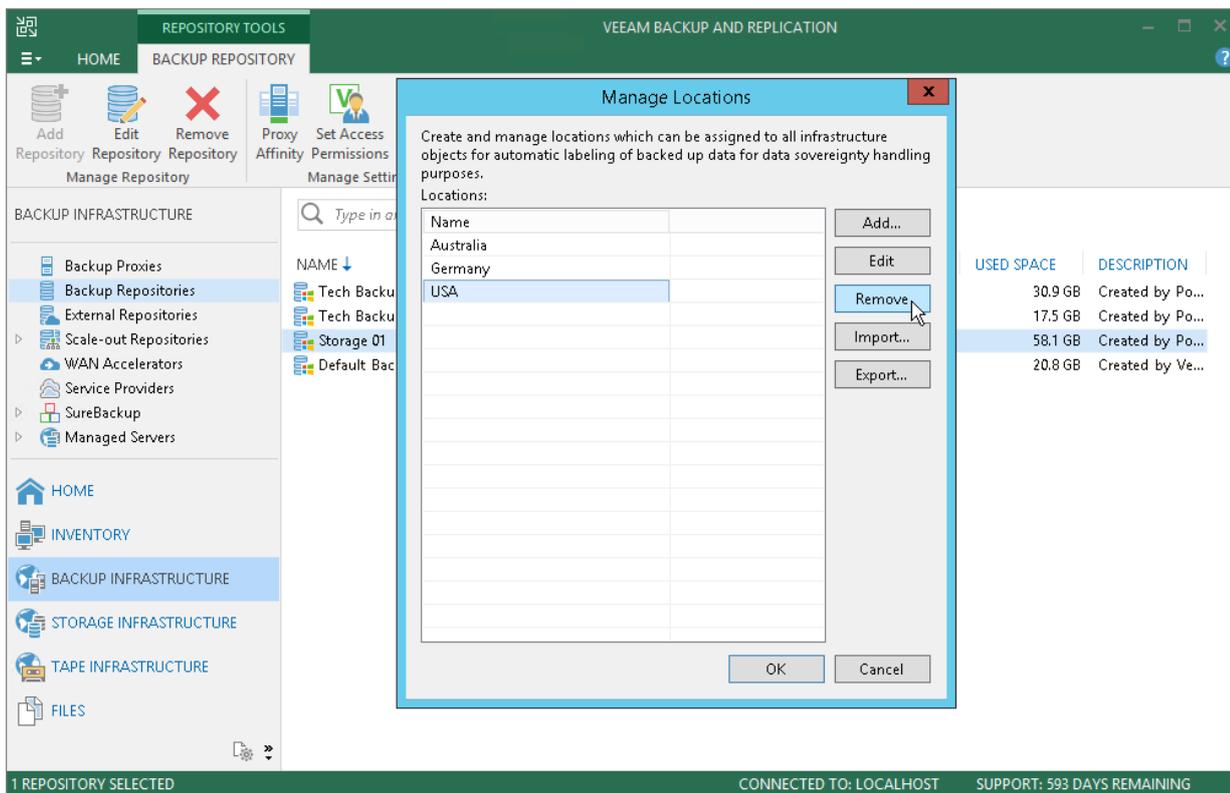


Deleting Locations

You can delete a location from the locations list, for example, if you no longer host infrastructure objects in this location.

To delete a location:

1. In the **Inventory** or **Backup Infrastructure** view, right-click the infrastructure object and select **Location > Manage Locations**.
2. In the **Manage Locations** window, select the location and click **Delete**. If the location is currently assigned to some infrastructure objects, Veeam Backup & Replication will display a warning with the list of objects that belong to this location. Click **Yes** to confirm the location deletion.



Exporting and Importing Locations List

You can export and import the list of locations to/from a file of XML format.

The import and export functionality facilitates the process of locations creation and maintenance. For example, if you need to set up the same list of locations throughout the whole backup infrastructure, you can create a list of locations on one backup server manually, export this list to an XML file, and then import the list on other backup servers and machines running the Veeam Backup & Replication console.

TIP:

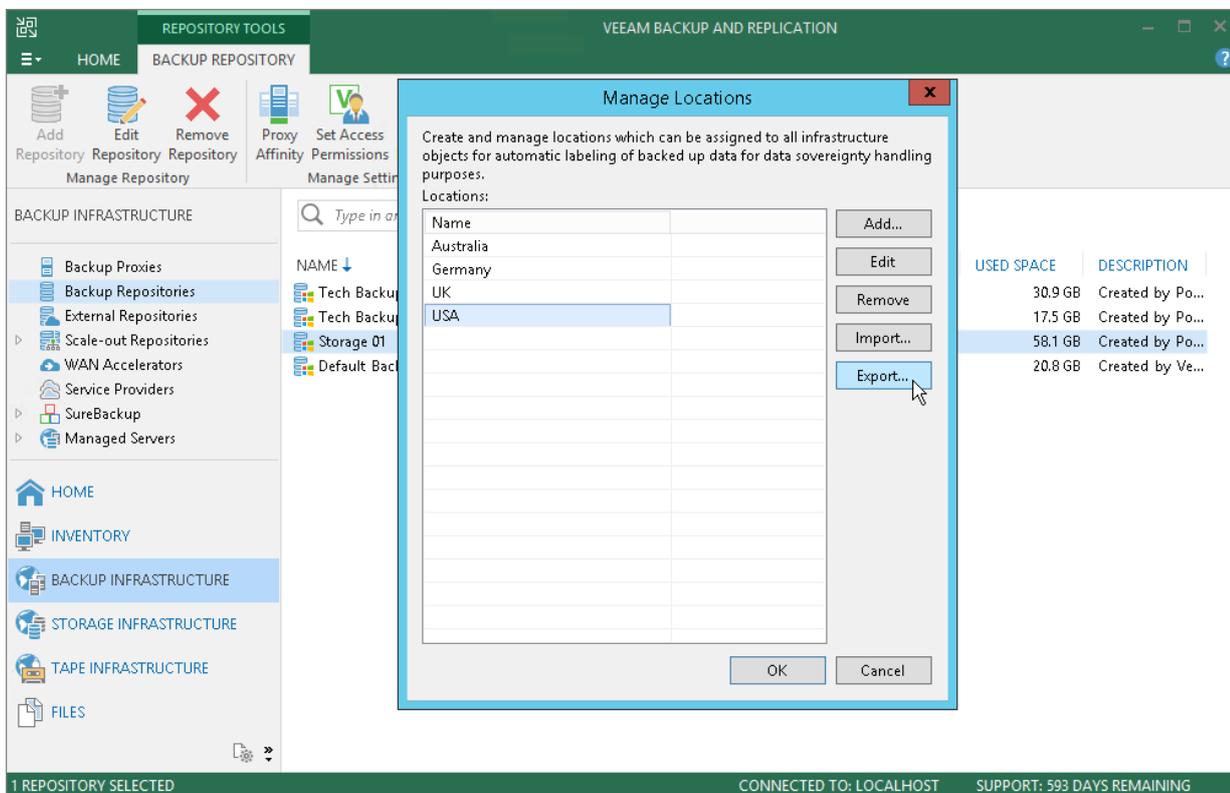
If you delete and recreate a location, Veeam Backup & Replication will create an object with a new ID in the database and consider it as a new location. Thus, to preserve the uniqueness of the location, use the location export/import operations.

To export the locations list:

1. In the **Inventory** or **Backup Infrastructure** view, right-click an infrastructure object and select **Location > Manage locations**.
2. In the **Manage Locations** window, click **Export** and specify a name of the XML file to which the locations list must be exported.

To import the locations list:

1. In the **Inventory** or **Backup Infrastructure** view, right-click an infrastructure object and select **Location > Manage locations**.
2. In the **Manage Locations** window, click **Import** and browse to the XML file from which the locations list must be imported.



Veeam Backup & Replication Settings

You can set up general settings for Veeam Backup & Replication. General settings are applied to all jobs, backup infrastructure components and other objects managed by the backup server.

Specifying I/O Settings

You can specify data processing settings.

Mind the following:

- The **Enable storage latency control** option is available in Veeam Backup & Replication Enterprise and Enterprise Plus Editions.
- The **Set custom thresholds on individual datastores** option is available in Veeam Backup & Replication Enterprise Plus Edition only.
- The **Enable storage latency control** option is not supported for vVOLs/vSAN storage.

To specify data processing settings:

1. From the main menu, select **General Options**.
2. Click the **I/O Control** tab.
3. To control the I/O load on the production storage, select the **Enable storage latency control** check box. When you enable storage latency control, Veeam Backup & Replication monitors storage read latency on production datastores during data protection and disaster recovery activities. To monitor the storage latency, Veeam Backup & Replication uses real-time metrics from the hypervisor. By default, metrics from the hypervisor are collected every 20 seconds. These settings are inherited from VMware vSphere.

Specify two thresholds:

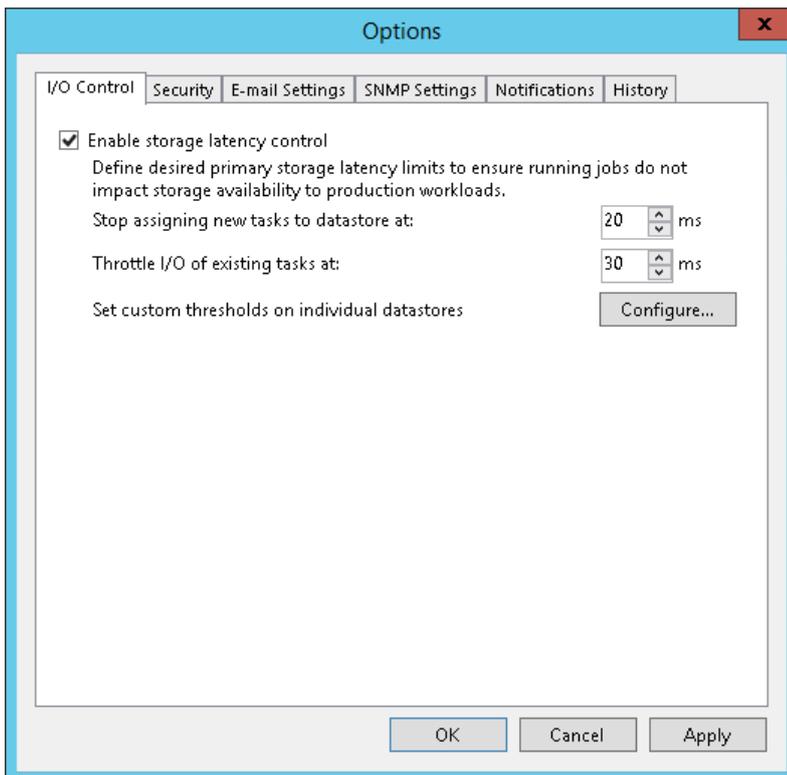
- a. In the **Stop assigning new tasks to datastore at** field, specify the I/O latency limit at which Veeam Backup & Replication must not assign new tasks targeted at the datastore.
- b. In the **Throttle I/O of existing tasks at** field, specify the I/O latency limit at which Veeam Backup & Replication must decrease the speed of data retrieval or writing to/from the datastore. When the I/O latency for this datastore reaches this value, the Veeam Data Mover working with this datastore will slow down data retrieval or writing.

The value in the **Stop assigning new tasks to datastore at** field cannot be greater than the value in the **Throttle I/O of existing tasks at** field.

NOTE:

If you enable the storage latency control option, Veeam Backup & Replication starts processing VM disks residing on the same datastore with a 40-60 second time offset. This offset helps Veeam Backup & Replication evaluate the current I/O load on the datastore. For example, if you launch a job processing a VM with two disks, Veeam Backup & Replication will start processing the first VM disk, wait for 40-60 seconds to evaluate the I/O workload on the datastore, and then start processing the second VM disk.

Keep in mind this behavior. If you schedule jobs that process multiple VM disks residing on the same datastore to start at the same time, the jobs performance will degrade.

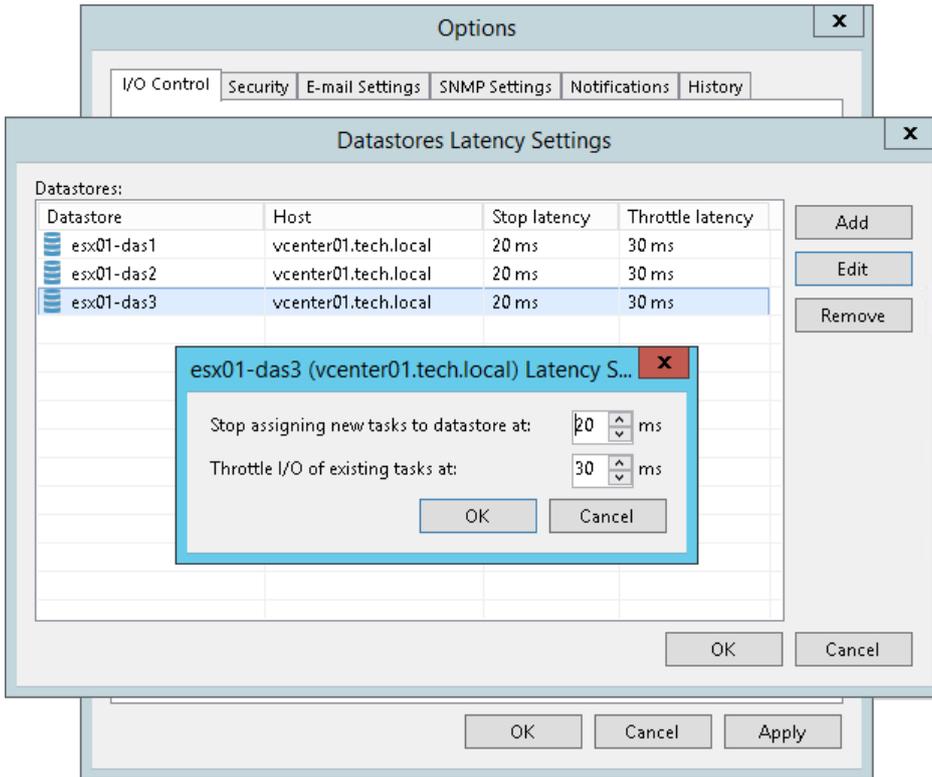


You can set the I/O latency limit for every storage in the virtual infrastructure separately.

To set the I/O latency limit for every storage separately:

1. From the main menu, select **General Options**.
2. Click the **I/O Control** tab.
3. Click **Configure**.
4. Click **Add > Datastore**, select the necessary datastore and click **OK** to add it to the storage list.
5. Select the added datastores in the list and click **Edit**.

6. Specify the I/O thresholds for the datastores as described above.



Specifying Email Notification Settings

You can receive email notifications with results on jobs performed on the backup server.

To receive email notifications, you must perform the following tasks:

- [Configure global email notification settings in Veeam Backup & Replication](#)
- [Configure job notification settings](#)

TIP:

To receive email notification about all jobs performed on the backup server in one email, configure email notification settings in Veeam Backup Enterprise Manager.

Configuring Global Email Notification Settings

To configure global email notification settings:

1. From the main menu, select **General Options**.
2. Open the **E-mail Settings** tab.
3. Select the **Enable e-mail notifications** check box.
4. In the **SMTP server** field, enter a full DNS name or IP address of the SMTP server that will be used for sending email notifications.
5. Click the **Advanced** button to specify user credentials and connection options:
 - a. Specify the port number and connection timeout for the SMTP server.
 - b. To use a secure connection for email operations, select the **Connect using SSL** check box.
 - c. If you need to connect to the SMTP server using a specific account, select the **This SMTP server requires authentication** check box and select the necessary credentials from the **Log on as** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see [Managing Credentials](#).
6. In the **From** field, specify an email from which email notifications must be sent.
7. In the **To** field, specify the recipient addresses. Use a semicolon to separate multiple addresses. Recipients specified in this field will receive notification about every job managed by the backup server. You can leave the field empty if required.

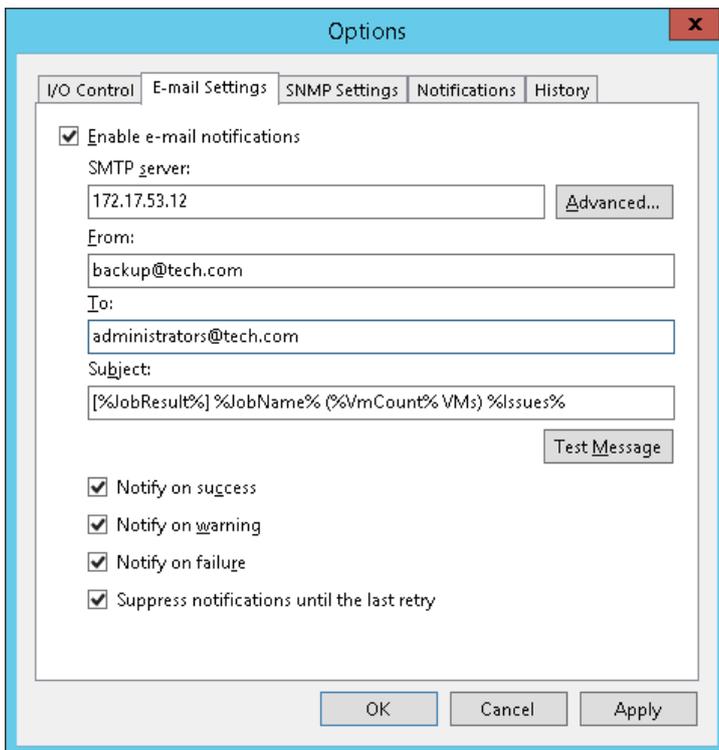
For every particular job, you can specify additional recipients. For more information, see [Configuring Job Notification Settings](#).

NOTE:

If you specify the same email recipient in both job notification and global notification settings, Veeam Backup & Replication will send two separate notifications to this recipient in the following cases:

- If a subject for the email message specified in job notification and global notification settings is different.
- If a list of email recipients specified in job notification and global notification settings is different.

8. In the **Subject** field, specify a subject for the sent message. You can use the following variables in the subject:
 - a. *%Time%* – completion time
 - b. *%JobName%*
 - c. *%JobResult%*
 - d. *%VmCount%* – number of VMs in the job
 - e. *%Issues%* – number of VMs in the job that have been processed with the *Warning* or *Failed* status
9. Select the **Notify on success**, **Notify on warning** and/or **Notify on failure** check boxes to receive email notification if a job is run successfully, not successfully or with a warning.
10. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.
11. Veeam Backup & Replication allows sending a test email to check if all settings have been configured correctly. To send a test email, click **Test Message**.



Configuring Job Notification Settings

To configure job notification settings:

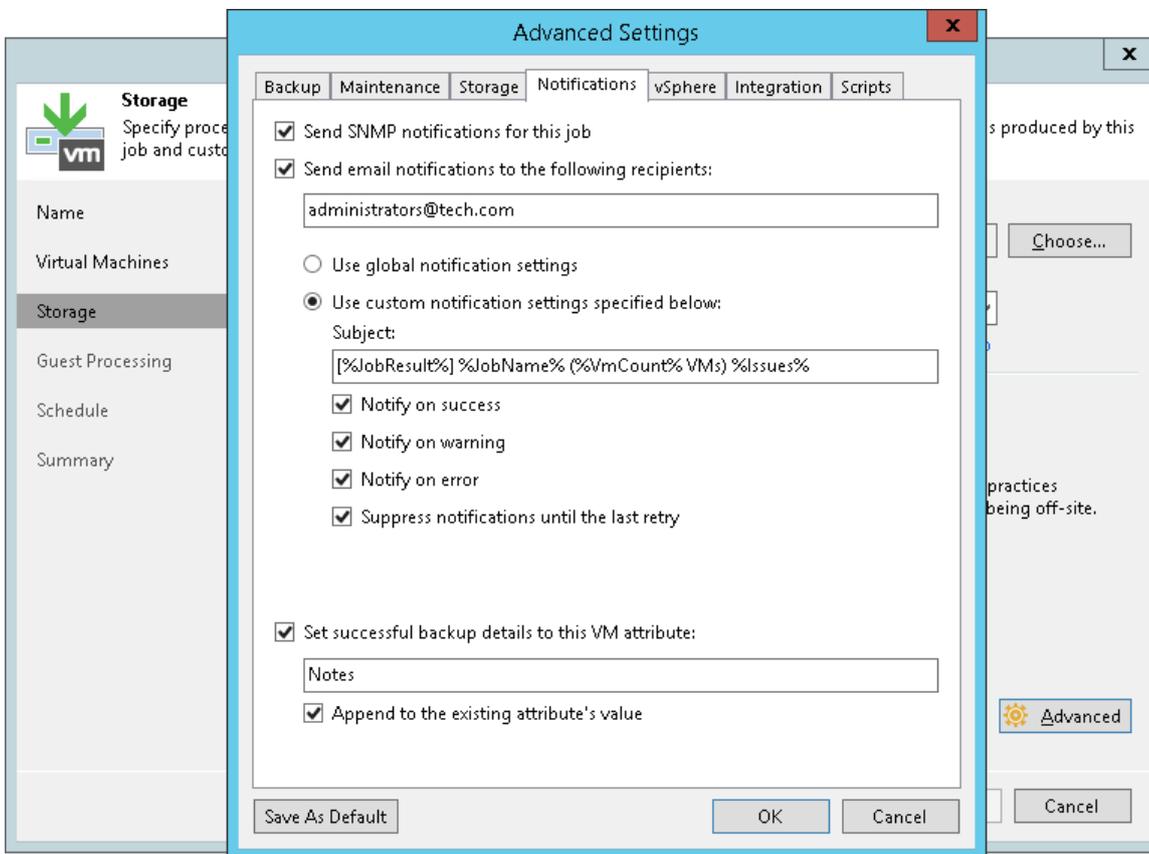
1. Open advanced settings of the job.
2. On the **Notifications** tab, select the **Send email notifications to the following recipients** check box.
3. In the field below, enter an email address to which a notification must be sent. You can enter several email addresses separated with a semicolon.

NOTE:

If you specify the same email recipient in both job notification and global notification settings, Veeam Backup & Replication will send two separate notifications to this recipient in the following cases:

- If a subject for the email message specified in job notification and global notification settings is different.
- If a list of email recipients specified in job notification and global notification settings is different.

4. You can choose to use global notification settings for the job or specify custom notification settings.
 - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see [Configuring Global Email Notification Settings](#).
 - To configure a custom notification for the job, select **Use custom notification settings** and specify notification settings as required.



Specifying SNMP Settings

You can receive SNMP traps with results on jobs performed on the backup server. You can use SNMP traps to feed data to other monitoring systems such as CA Unicenter, BMC Patrol, IBM Tivoli or HPE OpenView. SNMP traps can be sent to 5 different destinations.

To receive SNMP traps, you must perform the following tasks:

- [Configure global SNMP settings](#)
- [Configure SNMP service properties](#)
- [Configure SNMP settings for jobs](#)

Configuring Global SNMP Settings

To configure global SNMP settings:

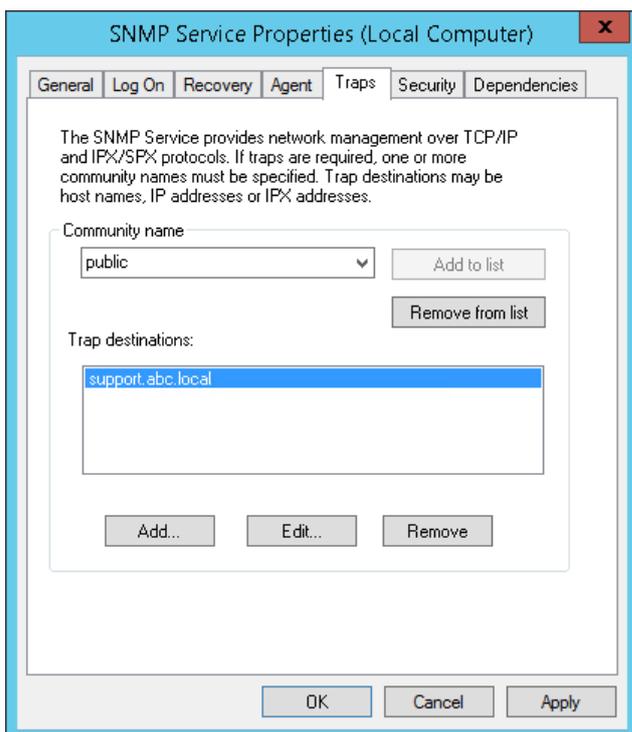
1. From the main menu, select **General Options**.
2. Click the **SNMP Settings** tab.
3. In the **Receiver** field, specify an IP address of the SNMP recipient.
4. In the field on the right, enter the port number to be used.
5. In the **Community String** field, enter the community identifier.

The screenshot shows a dialog box titled "Options" with a close button (X) in the top right corner. The dialog has several tabs: "I/O Control", "Security", "E-mail Settings", "SNMP Settings" (which is selected), "Notifications", and "History". The "SNMP Settings" tab contains five rows of configuration fields. Each row consists of a "Receiver" field (IP address), a port number dropdown menu, and a "Community String" field. The first row is filled with "172.17.53.28", "22", and "public". The second row is filled with "172.17.53.29", "22", and "public". The remaining three rows are empty, with "0" in the port dropdown menus. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

Configuring SNMP Service Properties

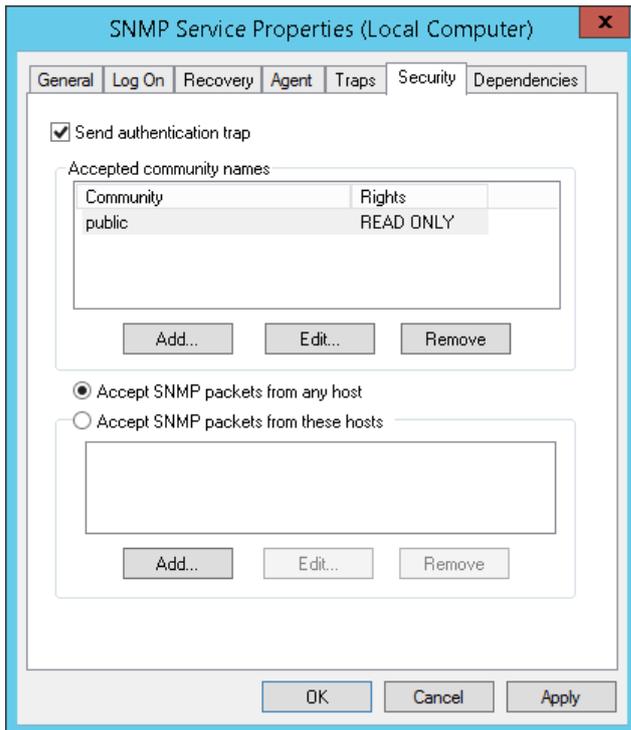
To configure SNMP service properties on recipients' computers:

1. Install a standard Microsoft SNMP agent from the Microsoft Windows distribution on the computer.
2. From the **Start** menu, select **Control Panel > Administrative Tools > Services**.
3. Double-click **SNMP Service** to open the **SNMP Service Properties** window.
4. Click the **Traps** tab.
5. Add the public string to the **Community name** list and name of the necessary host to the **Trap destinations** list.



6. Click the **Security** tab.
7. Make sure the **Send authentication trap** check box is selected.
8. Add the public string to the **Accepted community names** list.
9. Select the **Accept SNMP packets from any host** check box.

10. Click **OK** to save changes.

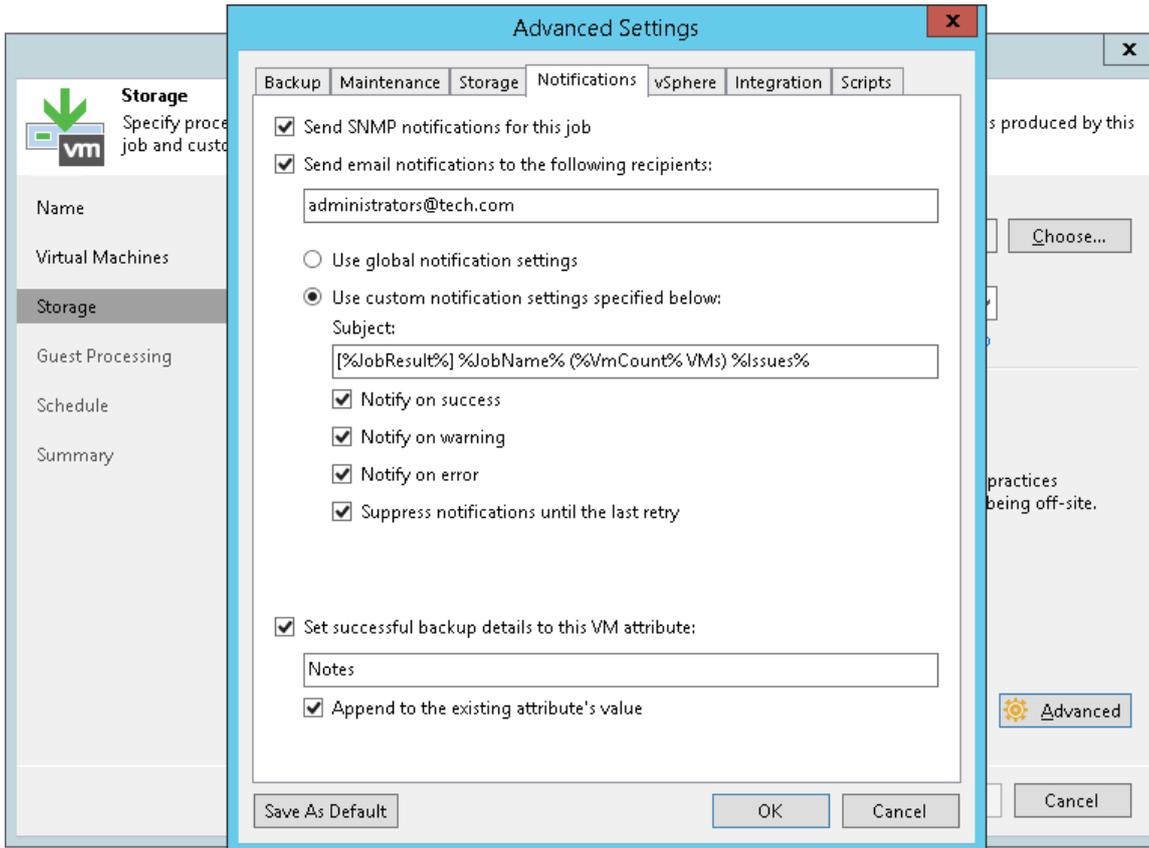


Configuring SNMP Settings for Jobs

To receive SNMP traps with results of a specific job:

1. Open advanced settings of the job.

2. On the **Notifications** tab, select the **Send SNMP notifications for this job** check box.



Specifying Other Notification Settings

You can configure Veeam Backup & Replication to automatically notify you about the following events:

- [Low disk space](#)
- [Support contract expiration](#)
- [New product versions, available updates and patches](#)

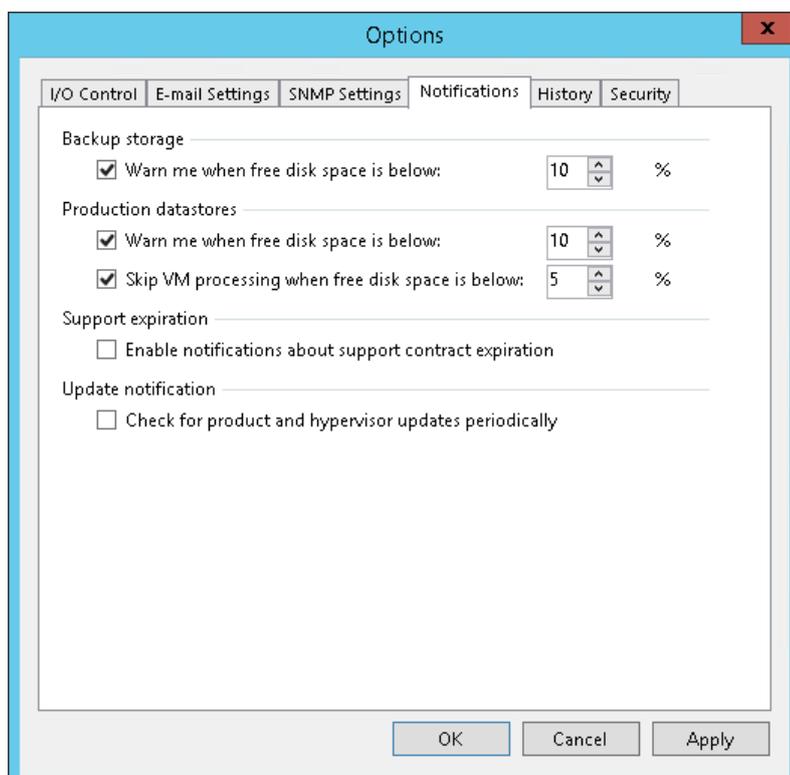
Low Disk Space Notification

When you run a job, Veeam Backup & Replication checks disk space on the target backup repository and production storage. If the disk space is below a specific value, Veeam Backup & Replication will display a warning message in the job session details.

To specify the disk space threshold:

1. From the main menu, select **General Options**.
2. Click the **Notifications** tab.
3. In the **Backup storage** and **Production datastores** sections, select the **Warn me when free disk space is below <N> %** options and specify a desired disk space threshold.
4. In the **Production datastores** section, select the **Skip VMs when free disk is below <N> %** option and specify a desired disk space threshold. When the threshold is reached, Veeam Backup & Replication will terminate backup and replication jobs working with production datastores before VM snapshots are taken. Such behaviour helps ensure that production datastores do not run out of space.

Veeam Backup & Replication also terminates jobs if the amount of free space on the datastore is below 2 GB. You can change this threshold limit using registry keys. For more information, contact Veeam Support.

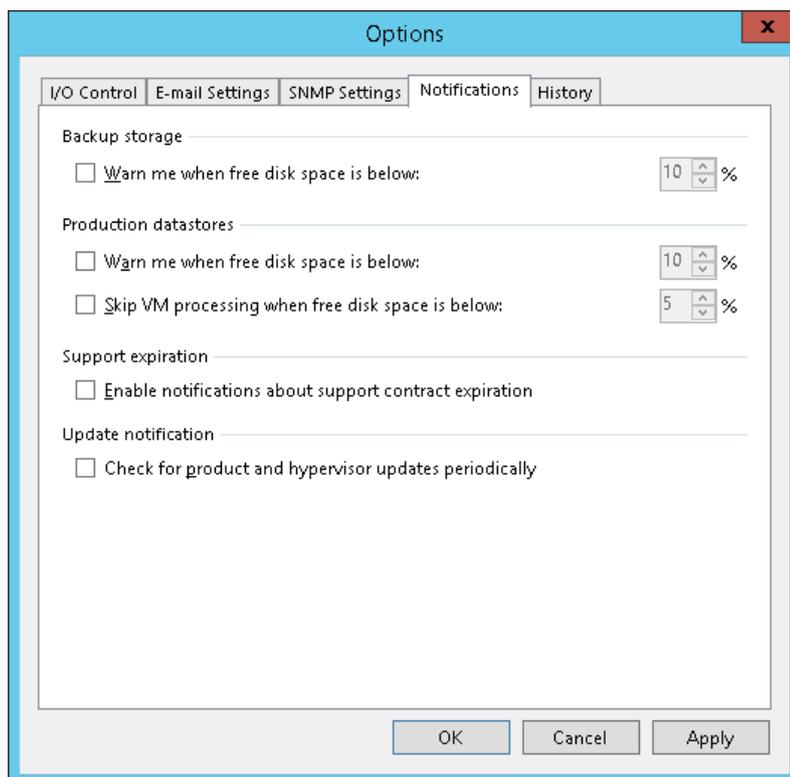


Support Contract Expiration Notification

By default, Veeam Backup & Replication informs email recipients specified in global notification settings about the support expiration date in every email notification. Veeam Backup & Replication starts sending such notifications 14 days before the expiration date. Expiration information is also shown on the splash screen and on the **License Information** window (to display the **License Information** window, select **Help > License** from the main menu).

To stop receiving notifications about support contract expiration:

1. From the main menu, select **General Options**.
2. Click the **Notifications** tab.
3. Clear the **Enable notifications about support contract expiration** check box.



New Product Versions

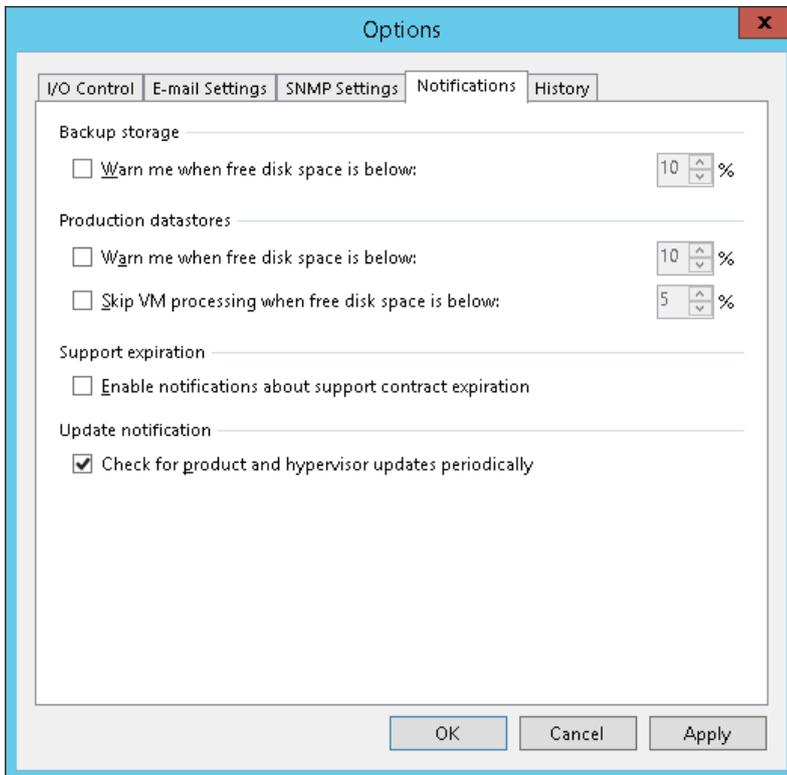
You can configure Veeam Backup & Replication to automatically check for new product versions and patches available on the Veeam website. For more information, see [Update Notification](#).

To enable new product versions and update notifications:

1. From the main menu, select **General Options**.
2. Click the **Notifications** tab.
3. Select the **Check for product and hypervisor updates periodically** check box.

IMPORTANT!

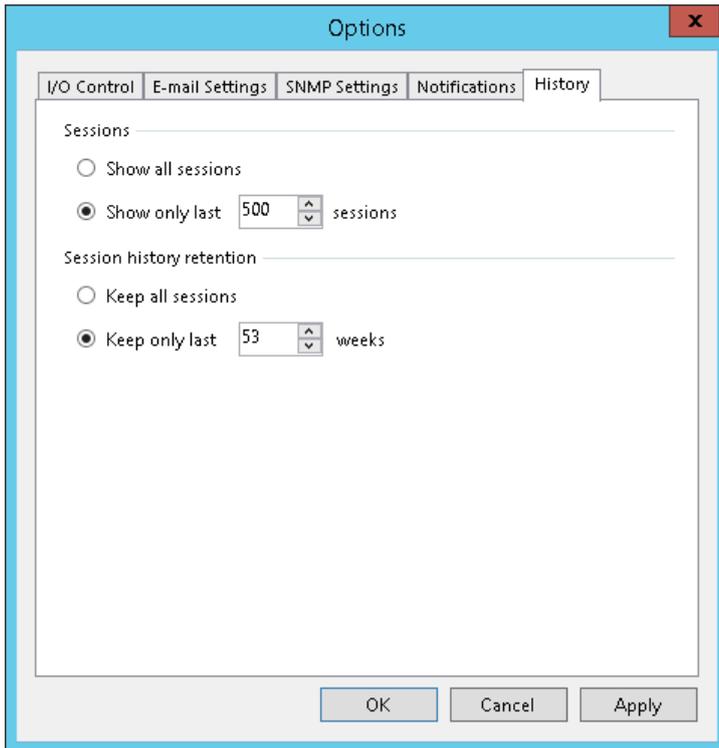
Make sure that the backup server is connected to the Internet. In the opposite case, you will not be able to receive notifications about updates and patches.



Specifying Session History Settings

You can specify session history settings for jobs performed on the backup server.

1. From the main menu, select **General 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 & Replication must keep session information in the configuration database.



Configuring Security Settings

In the **Security** tab, you can configure the following:

- [TLS Certificates](#)
Configure a TLS certificate to establish secure communication between the backup server and VMware vSphere Server or storage systems.
- [Linux Hosts Authentication](#)
Enable the fingerprint check for Linux machines to protect connection from man-in-the-middle attacks.

TLS Certificates

When you configure the Veeam Backup & Replication infrastructure, you can specify what TLS certificate must be used to establish a secure connection between the backup server and VMware vSphere server or storage systems. Veeam Backup & Replication offers the following options for TLS certificates:

- You can choose to keep the default self-signed TLS certificate generated by Veeam Backup & Replication at the process of upgrading to a new version of Veeam Backup & Replication.
- You can use Veeam Backup & Replication to generate a new self-signed TLS certificate. To learn more, see [Generating Self-Signed Certificates](#).
- You can select an existing TLS certificate from the certificates store. To learn more, see [Importing Certificates from Certificate Store](#).
- You can import a TLS certificate from a file in the PFX format. To learn more, see [Importing Certificates from PFX Files](#).

NOTE:

If you plan to use a certificate issued by your own CA, make sure that the certificate meets the following requirements:

1. The following Key Usage extensions are enabled in the certificate: *Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing*.
2. The Key Type in the certificate is set to *Exchange*.

Generating Self-Signed Certificates

You can use Veeam Backup & Replication to generate a self-signed certificate for authenticating parties in the Veeam Backup & Replication infrastructure.

To generate TLS certificates, Veeam Backup & Replication employs the RSA Full cryptographic service provider by Microsoft Windows installed on the Veeam backup server. The created TLS certificate is saved to the *Shared* certificate store. The following types of users can access the generated TLS certificate:

- User who created the TLS certificate
- LocalSystem user account
- Administrators group

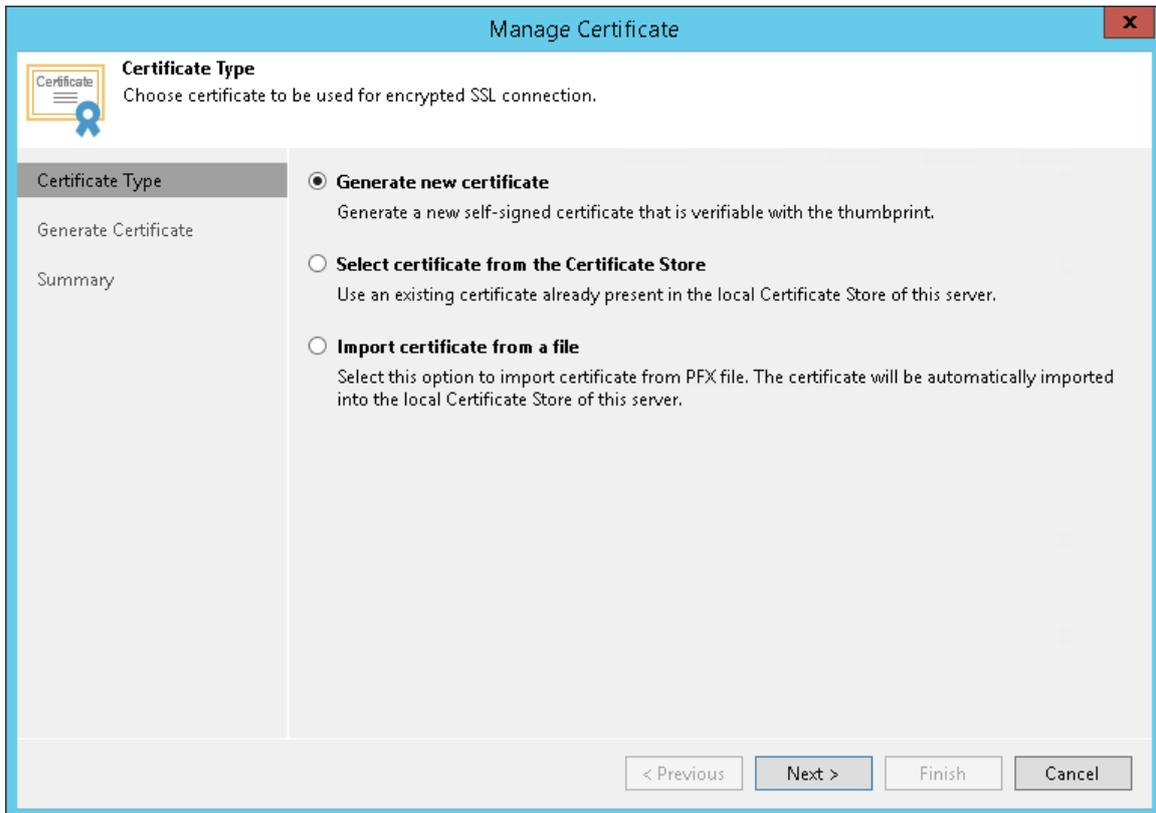
If you use a self-signed TLS certificate generated by Veeam Backup & Replication, you do not need to take any additional actions to deploy the TLS certificate on a protected computer. When Veeam Backup & Replication discovers a VMware vSphere server or a storage system, a matching TLS certificate with a public key is installed on the protected computer automatically. During discovery, Veeam Installer Service deployed on the protected computer retrieves the TLS certificate with a public key from the backup server and installs a TLS certificate with a public key on the protected computer.

NOTE:

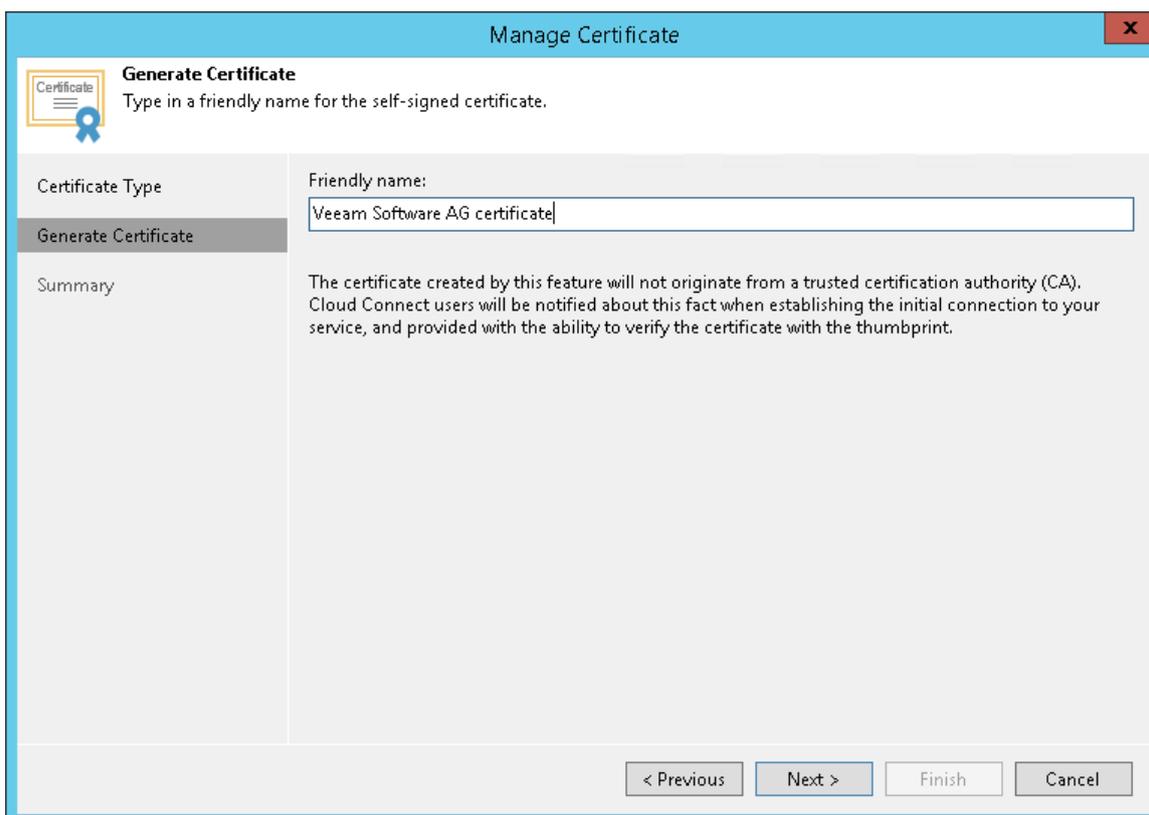
When you generate a self-signed TLS certificate with Veeam Backup & Replication, you cannot include several aliases to the certificate and specify a custom value in the *Subject* field. The *Subject* field value is taken from the Veeam Backup & Replication license installed on the Veeam backup server.

To generate a self-signed TLS certificate:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, select **Generate new certificate**.

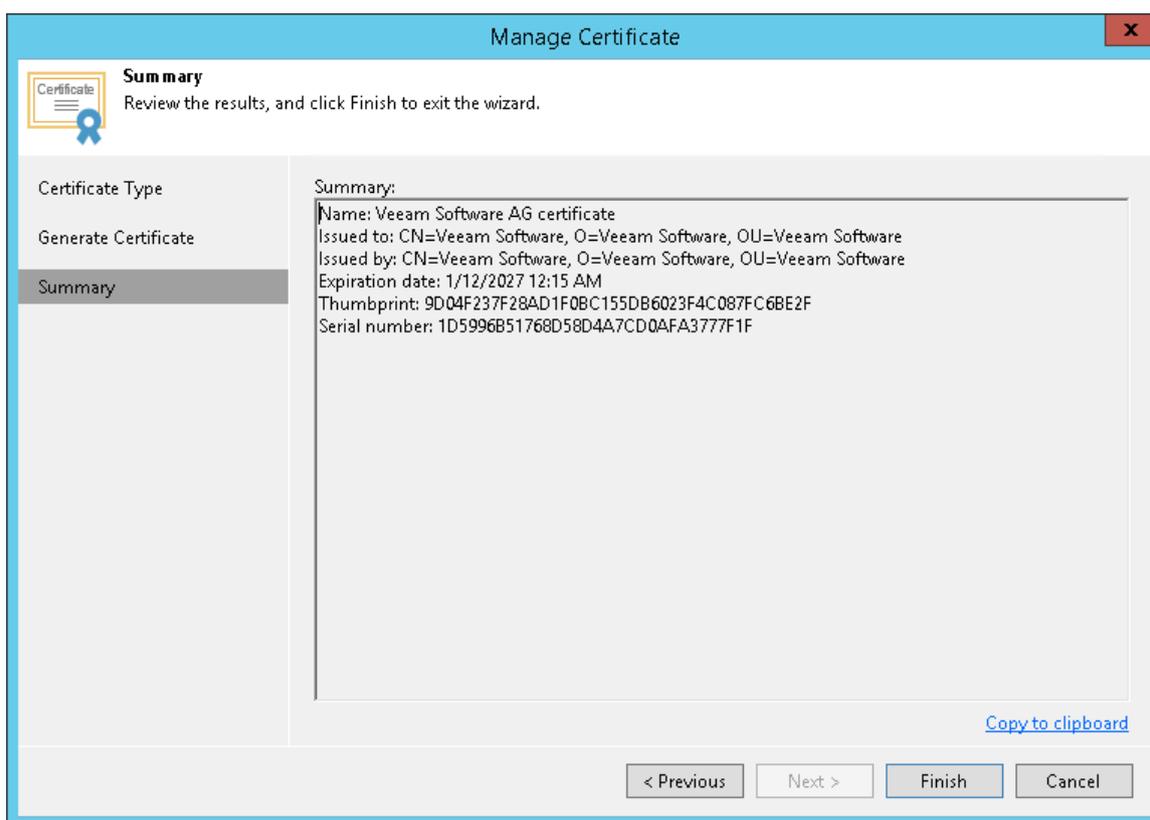


- At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.



- At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the generated TLS certificate. You will be able to use the copied information to verify the TLS certificate with the certificate thumbprint.

7. Click **Finish**. Veeam Backup & Replication will save the generated certificate in the *Shared* certificate store on the Veeam backup server.



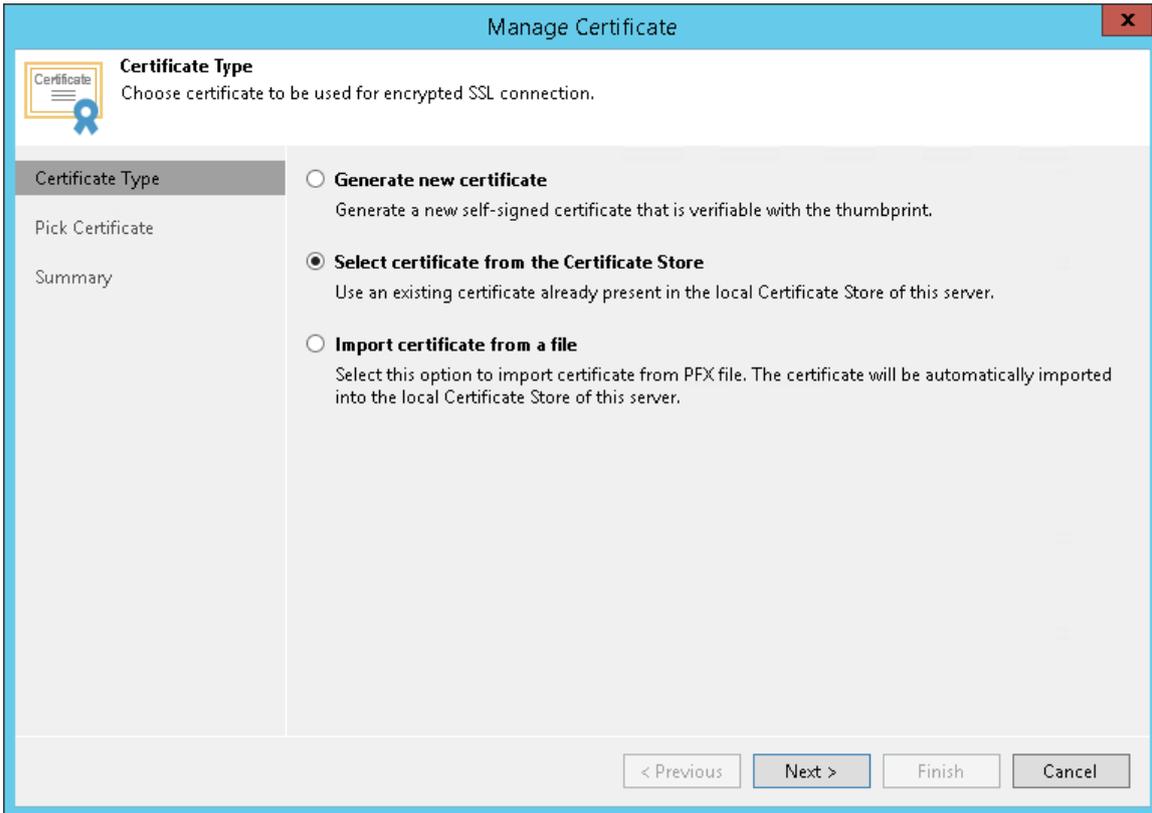
Importing Certificates from Certificate Store

If your organization has a TLS certificate signed by a CA and the TLS certificate is located in the Microsoft Windows Certificate store, you can use this certificate for authenticating parties in the Veeam Backup & Replication infrastructure.

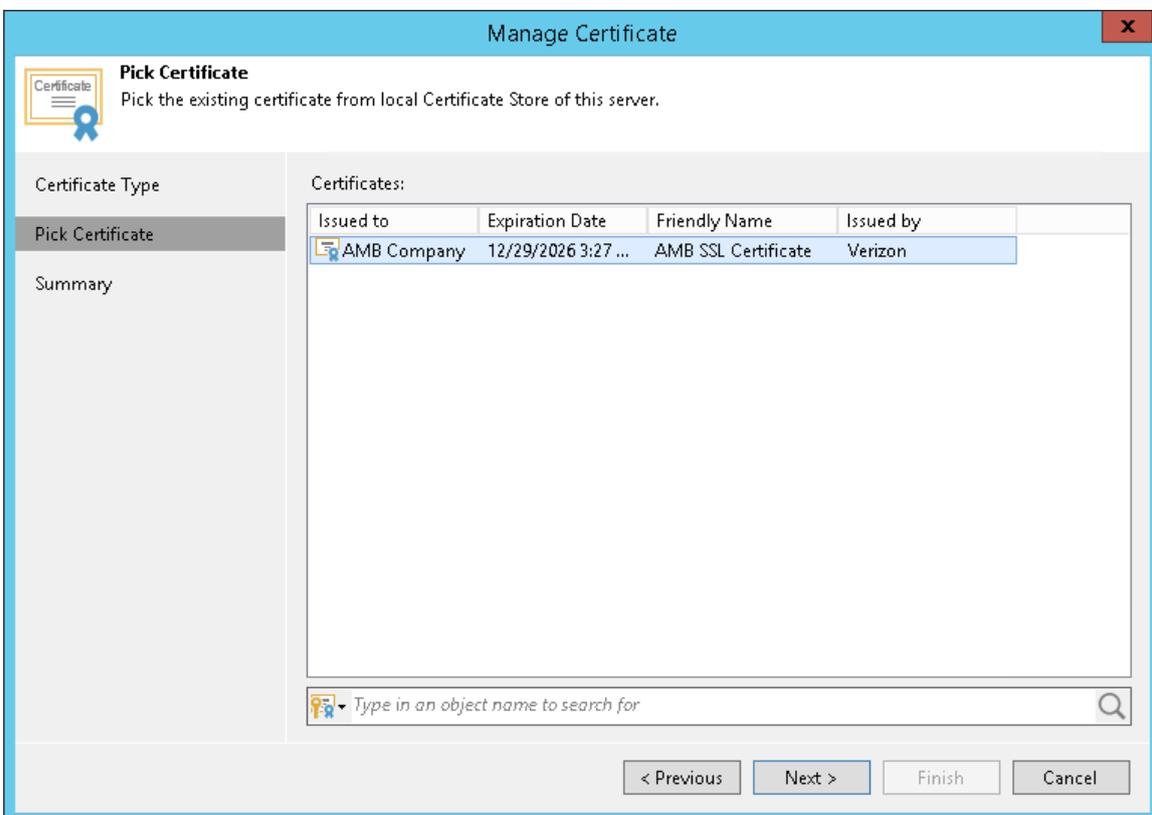
To select a certificate from the Microsoft Windows Certificate store:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.

4. At the **Certificate Type** step of the wizard, choose **Select certificate from the Certificate Store**.



5. At the **Pick Certificate** step of the wizard, select a TLS certificate that you want to use. You can select only certificates that contain both a public key and a private key. Certificates without private keys are not displayed in the list.



6. At the **Summary** step of the wizard, review the certificate properties.

7. Click **Finish** to apply the certificate.

Importing Certificates from PFX Files

You can import a TLS certificate in the following situations:

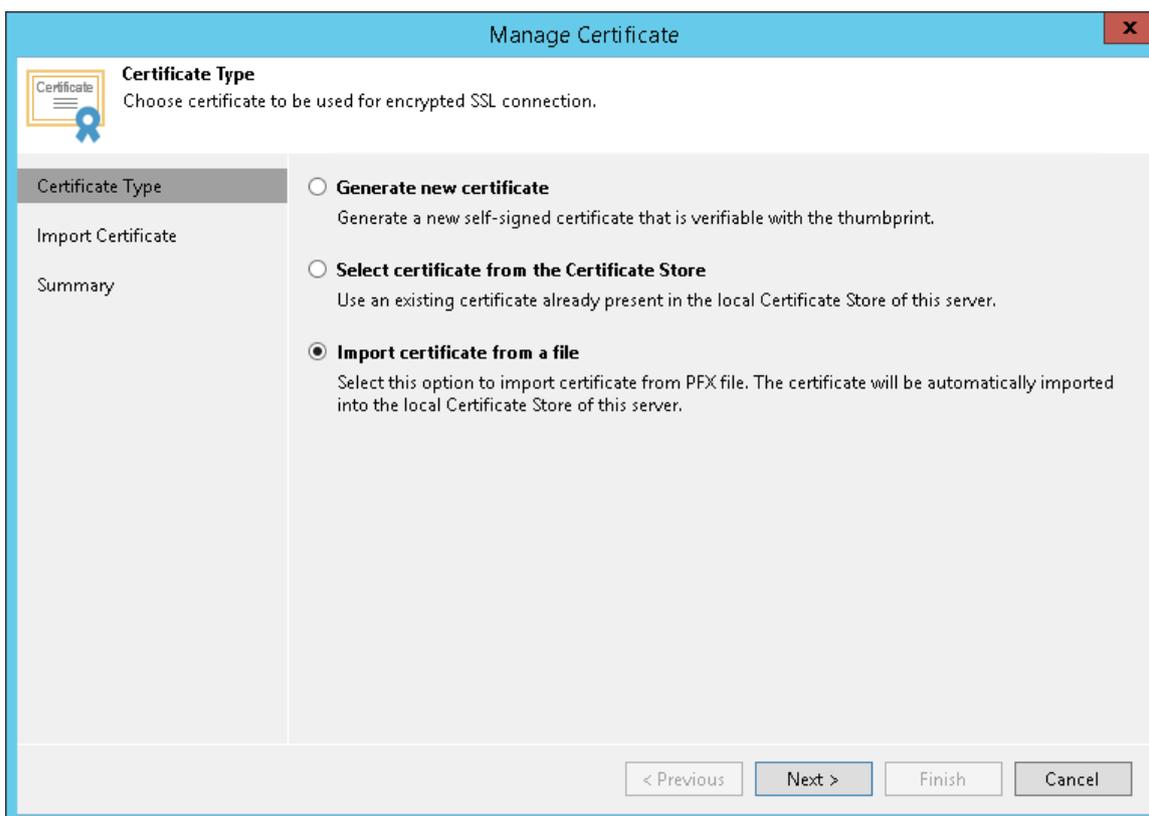
- Your organization uses a TLS certificate signed by a CA and you have a copy of this certificate in a file of PFX format.
- You have generated a self-signed TLS certificate in the PFX format with a third-party tool and you want to import it to Veeam Backup & Replication.

IMPORTANT!

The TLS certificate must pass validation on the Veeam backup server. In the opposite case, you will not be able to import the TLS certificate.

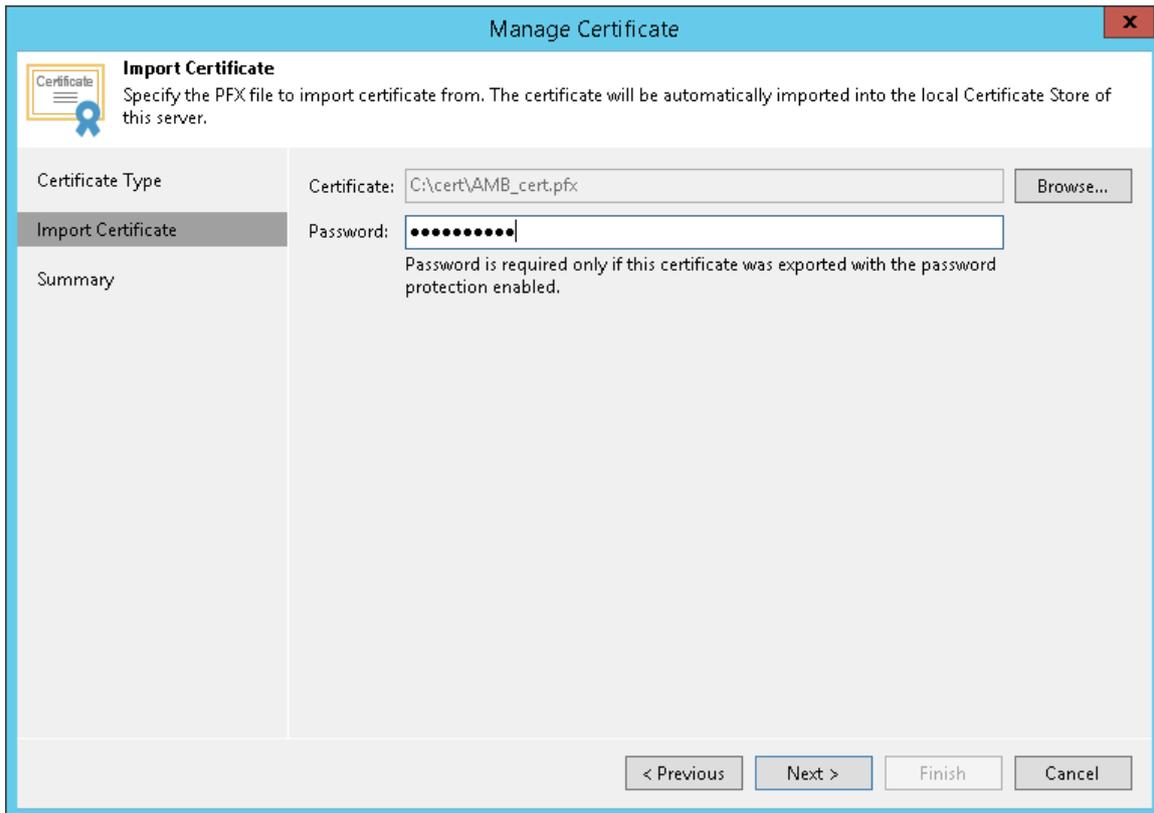
To import a TLS certificate from a PFX file:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, choose **Import certificate from a file**.



5. At the **Import Certificate** step of the wizard, specify a path to the PFX file.

6. If the PFX file is protected with a password, specify the password in the field below.



7. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the TLS certificate. You can use the copied information on a protected computer to verify the TLS certificate with the certificate thumbprint.
8. Click **Finish** to apply the certificate.

Linux Host Authentication

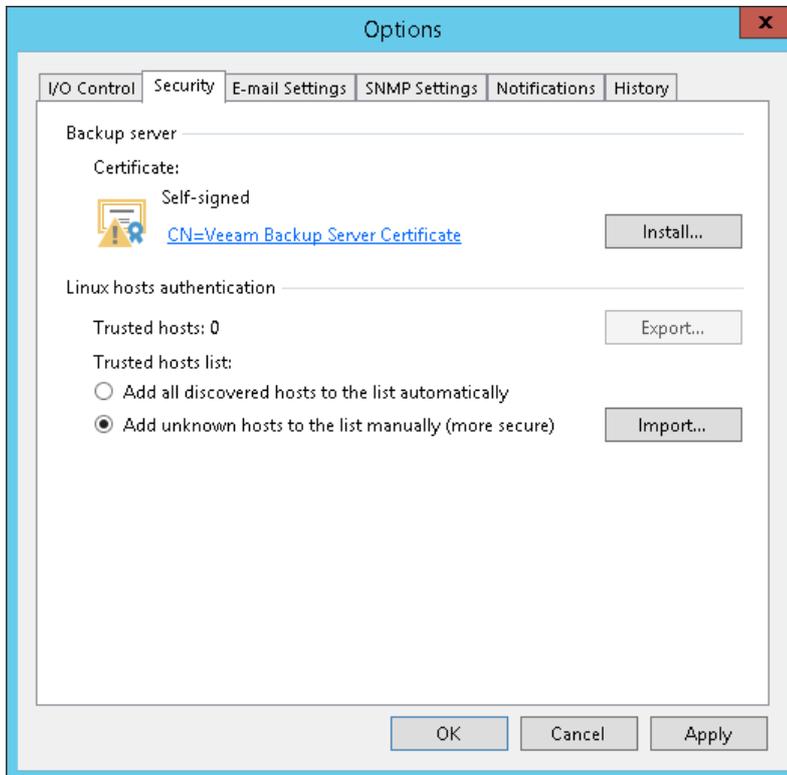
In the **Linux hosts authentication** section of the Veeam Backup & Replication settings, you can specify SSH fingerprint verification settings for protected Linux machines.

You can select one of the following options:

- **Add all discovered hosts to the list automatically** – with this option enabled, Veeam Backup & Replication allows all added Linux VMs and Linux servers to connect to the backup server.
- **Add unknown hosts to the list manually (more secure)** – with this option enabled, only the following Linux machines can connect to the backup server:
 - Protected machines that have already established a connection to the backup server and have their fingerprints stored in the Veeam Backup & Replication database.
Veeam Backup & Replication displays the number of trusted machines in the **Trusted hosts** field. To export the list of trusted machines to the *known_hosts* file, click **Export** and specify a path to the folder to save the file.
 - Protected machines specified in the *known_hosts* file imported to Veeam Backup & Replication. To import the *known_hosts* file, click **Import** and specify a path to the folder where the file resides.

Machines that do not meet the above-mentioned conditions cannot connect to the Veeam backup server and download Veeam Agent for Linux installation packages during discovery. Also, guest OS processing of untrusted VMs will fail.

Veeam Backup & Replication displays these computers under the Untrusted node in the inventory. To start managing an untrusted computer, you need to validate its fingerprint manually in the Veeam Backup & Replication console. To learn more, see [Validating SSH Fingerprints](#).



Validating SSH Fingerprints

Veeam Backup & Replication treats fingerprints of Linux VMs and Linux hosts differently:

- [Validating SSH Fingerprints of Linux VMs](#)
- [Validating SSH Fingerprints of Linux Hosts](#)

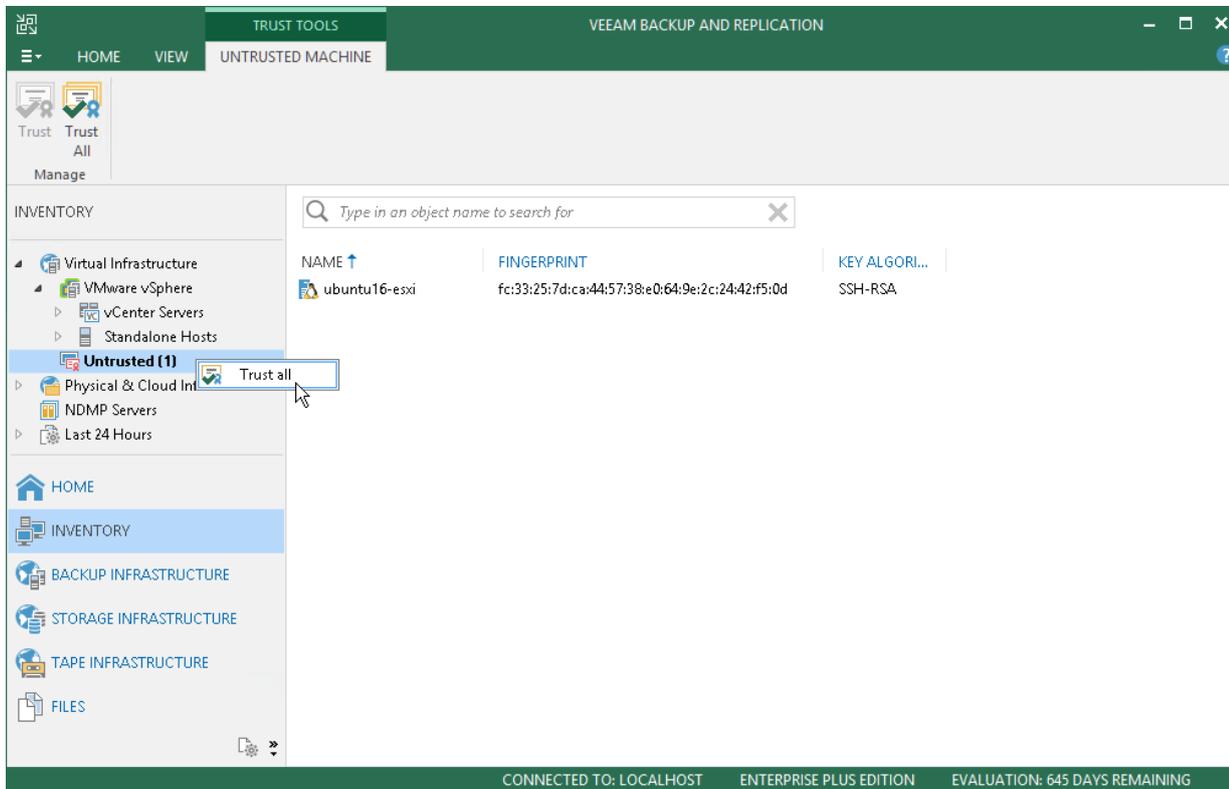
Validating SSH Fingerprints of Linux VMs

When you enable the **Add unknown hosts to the list manually (more secure)** option in Veeam Backup & Replication settings, Linux-based computers whose fingerprints are not stored in the Veeam Backup & Replication database or the `known_hosts` file become unable to communicate to the Veeam backup server. During discovery, Veeam Backup & Replication puts such computers to the *Untrusted* protection group. To start managing an untrusted computer, you need to validate its fingerprint manually in the Veeam Backup & Replication console.

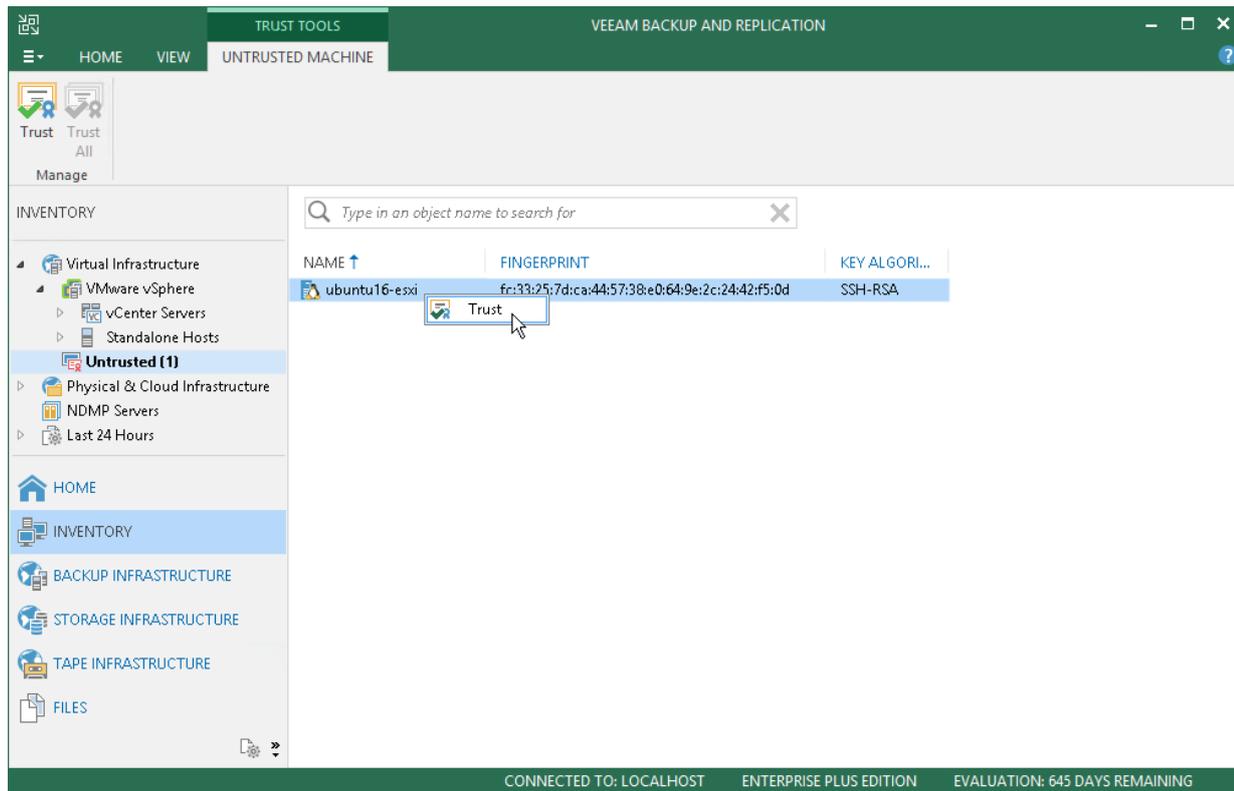
To validate the SSH fingerprint:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Virtual Infrastructure** node and click **Untrusted**.

3. In the working area, Veeam Backup & Replication will display a list of computers whose fingerprints need to be validated. Check fingerprints of the computers in the list and validate them in one of the following ways:
- To validate fingerprints of all untrusted computers at once, select the **Untrusted** node in the inventory pane and click **Trust All** on the ribbon. Alternatively, you can right-click the **Untrusted** node and select **Trust all**.



- To validate a fingerprint of a specific computer in the list, select the necessary computer in the working area and click **Trust** on the ribbon. Alternatively, you can right-click the computer and select **Trust**.

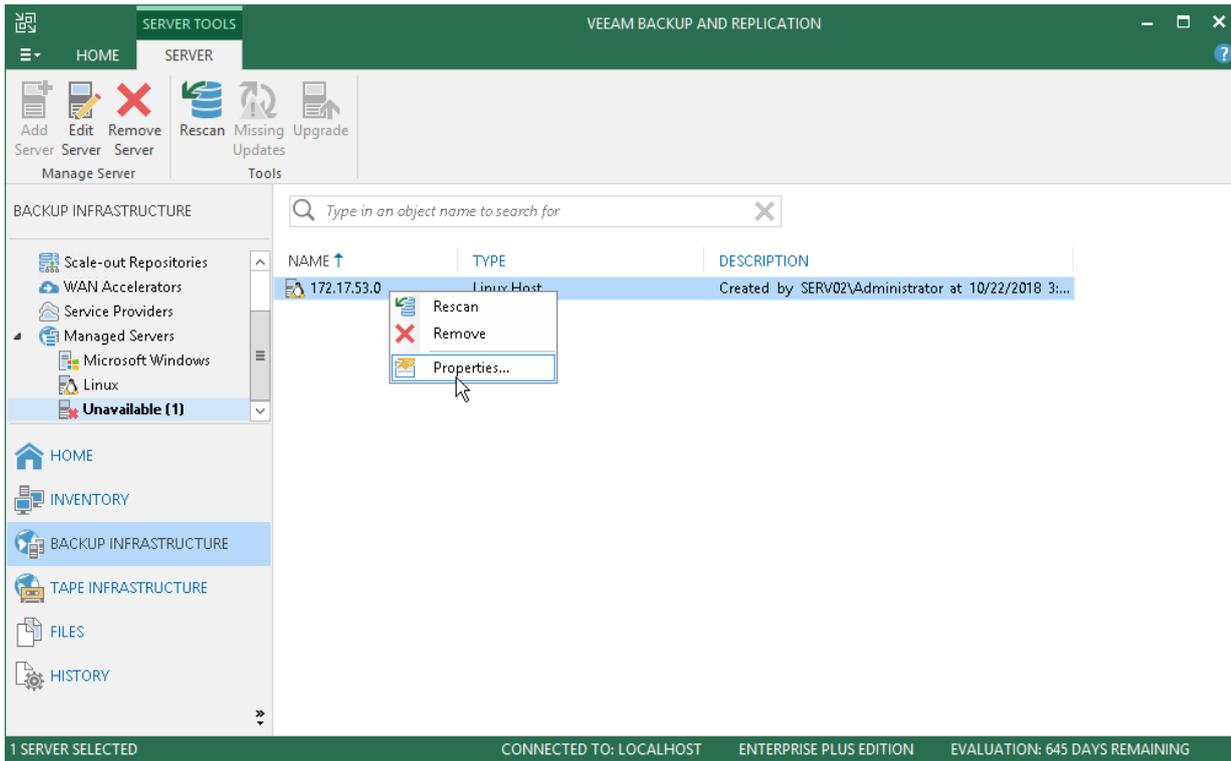


Validating SSH Fingerprints of Linux Hosts

If the SSH public key fingerprint of a Linux host is changed, Veeam Backup & Replication places this host in the **Unavailable** folder. To be able to use this server, do the following:

1. In the **Backup Infrastructure** view, expand the **Managed Servers** node and select **Unavailable**.
2. Right-click the Linux server and select **Properties**.
3. In the **SSH Connection** step of the **Edit Linux Server** wizard, click **Apply**.
4. In the pop-up dialogue window, click **Yes** to confirm that you trust this server.

5. Click **Finish** to close the wizard.



Roles and Users

You can assign one of the following roles to users or groups of users who plan to work with Veeam Backup & Replication:

- Veeam Restore Operator
- Veeam Backup Viewer
- Veeam Backup Operator
- Veeam Backup Administrator
- Veeam Tape Operator

A role assigned to the user defines the user activity scope: what operations in Veeam Backup & Replication the user can perform. Role security settings affect the following operations:

- Starting and stopping jobs
- Performing restore operations

Users having different roles can perform a different set of operations:

Role	Operations
Veeam Restore Operator	Can perform restore operations using existing backups and replicas.
Veeam Backup Viewer	Has the "read-only" access to Veeam Backup & Replication. Can view existing jobs and review the job session details.
Veeam Backup Operator	Can start and stop existing jobs.
Veeam Backup Administrator	Can perform all administrative activities in Veeam Backup & Replication.
Veeam Tape Operator	Can manage tapes and perform the following operations: tape inventory, tape export, tape eject, tape catalog, inventory library, catalog library, rescan library, import tapes, eject tape from drive.

You can assign several roles to the same user. For example, if the user must be able to start jobs and perform restore operations, you can assign the **Veeam Backup Operator** and **Veeam Restore Operator** roles to this user.

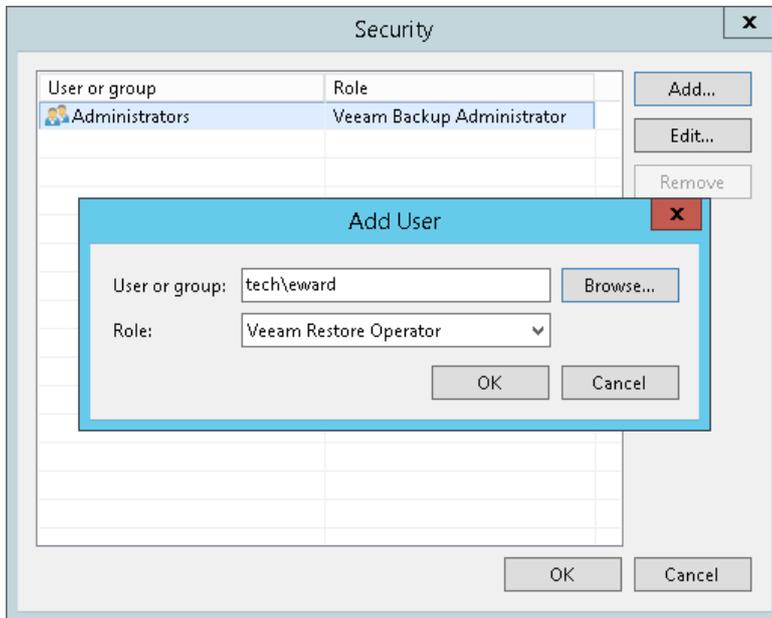
Mind the following:

- The user account under which the Veeam Backup Service runs must have the Veeam Backup Administrator role. By default, during installation the Veeam Backup Administrator role is assigned to users in the Administrators group. If you change the default settings, make sure that you assign the Veeam Backup Administrator role to the necessary user account. It is recommended to assign the Veeam Backup Administrator role to the user account explicitly rather than the group to which the user belongs.

If the Veeam Backup Service is started under the LocalSystem account, you do not need to assign any roles to this account.
- Built-in administrator accounts (Domain\Administrator and Machine\Administrator) always have full access in Veeam Backup & Replication, even if you exclude them from all Veeam Backup & Replication roles.

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.



Update Notification

Veeam Backup & Replication automatically notifies you about updates that must or can be installed to enhance your work experience with the product. Update notifications eliminate the risk of using out-of-date components in the backup infrastructure or missing critical updates that can have a negative impact on data protection and disaster recovery tasks.

Veeam Backup & Replication notifies about the product updates: new patches and product versions.

The update notifications are enabled by default. If you do not want to get notified about available updates, you can disable them. For more information, see [Specifying Other Notification Settings](#).

However, it is recommended that you leave update notifications enabled not to miss critical updates and patches.

How Update Notification Works

To check for updates, Veeam Backup & Replication uses a special XML file on the Veeam Update Notification Server (dev.veeam.com). The XML file contains information about the most up-to-date product version and patches.

Veeam Backup & Replication downloads an XML file from the Veeam Update Notification Server once a week. It also collects information about the installed product. The collected information is compared with the information in the downloaded file. If new product versions, patches and updates are available, Veeam Backup & Replication informs you about them.

NOTE:

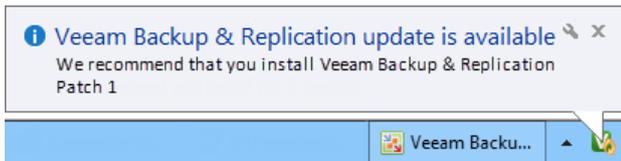
Make sure that the backup server is connected to the Internet and update notification is enabled in Veeam Backup & Replication options. In the opposite case, update notification will not function.

Installing Updates

Veeam Backup & Replication uses update notifications to inform you about new versions of Veeam Backup & Replication, new product patches.

When a new version of Veeam Backup & Replication or a new product patch becomes available on the website, Veeam Backup & Replication displays an icon in the system tray. An icon is displayed once a week.

To install a product update, double-click the Veeam Backup & Replication icon in the system tray. Veeam Backup & Replication will open a KB webpage with the update description and links to the installation archive of the new product version or new patch.



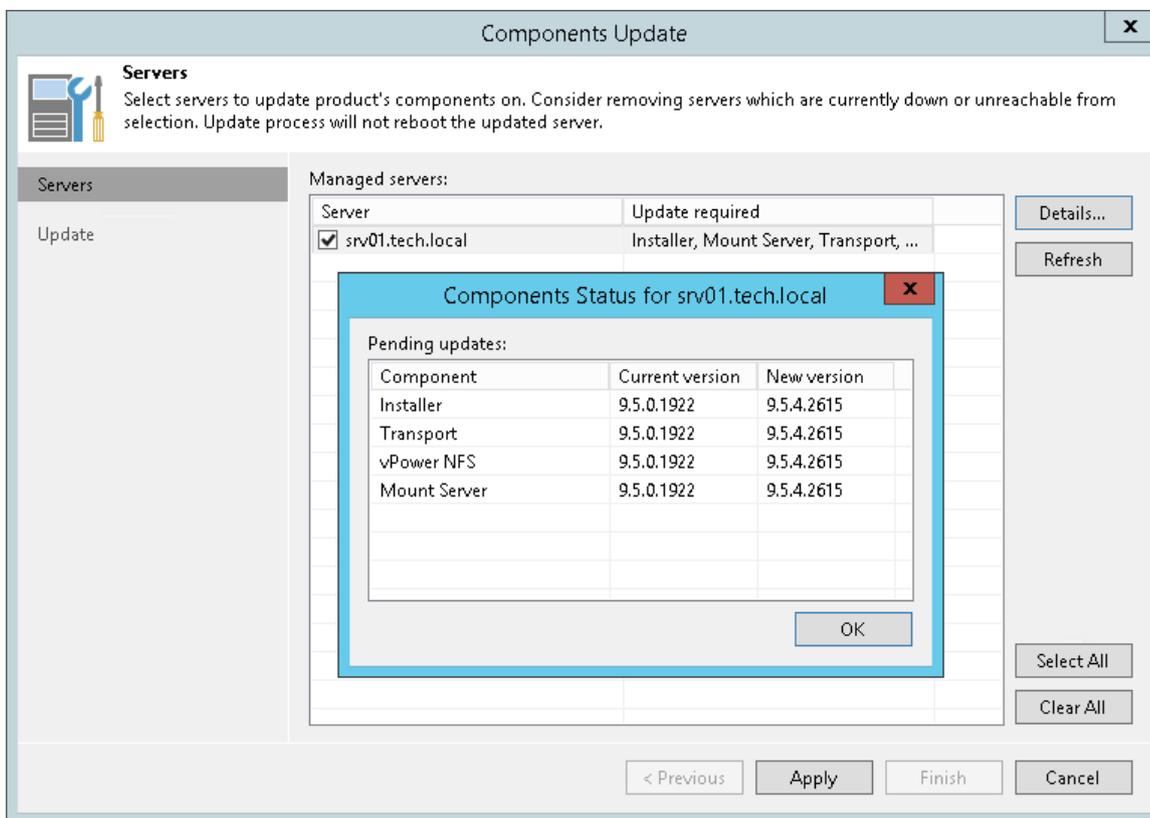
Server Components Upgrade

Every time you launch the Veeam Backup & Replication console, Veeam Backup & Replication automatically checks if Veeam Backup & Replication components installed on managed servers are up to date. If a later version of components is available, Veeam Backup & Replication 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 Veeam Backup & Replication.

You can manually check if components upgrade is required. To do this, 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 & Replication 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**.

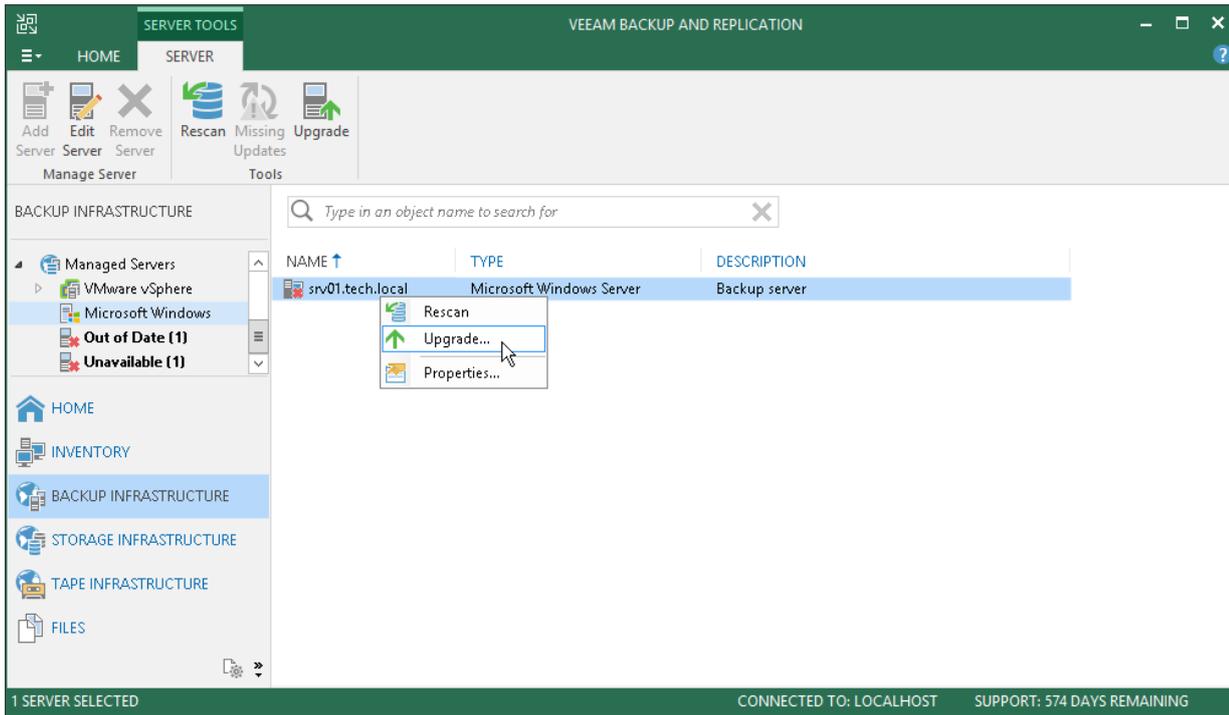


You can update components on every managed server separately. If components installed on the server require upgrade, Veeam Backup & Replication displays a warning icon next to the server.

To update components for a managed server:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **Managed servers**.
3. In the working area, select the server and click **Upgrade** on the ribbon.

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



Logging

Veeam Backup & Replication provides detailed logging of performed activities data protection and disaster recovery tasks.

On the backup server, log files are stored in the following folder: `%ProgramData%\Veeam\Backup`.

Veeam Backup & Replication keeps a separate log file for each of its components: Veeam Shell, Veeam Backup Service, Veeam Guest Catalog Service, Veeam vPower NFS Service, Veeam Installer, Veeam Data Mover and performed jobs.

In addition to logs stored on the backup server, log files are also stored on all servers added to the backup infrastructure:

- On Linux servers and ESX(i) hosts, logs are stored in the following directory: `/var/log/VeeamBackup/` or `/tmp/VeeamBackup`
- On Microsoft Windows servers, logs are stored in the following directory: `%ProgramData%\Veeam\Backup`

You can collect log files from the backup server and servers managed by Veeam Backup & Replication using the **Export Logs** wizard.

Exporting Logs

You can use log files to submit a support ticket. It is recommended that you send all log files when submitting a support ticket to ensure that overall and comprehensive information is provided to Veeam Support Team.

To aggregate all log files in the same location, use the **Export Logs** wizard. To launch the wizard, from the main menu select **Help > Support Information**.

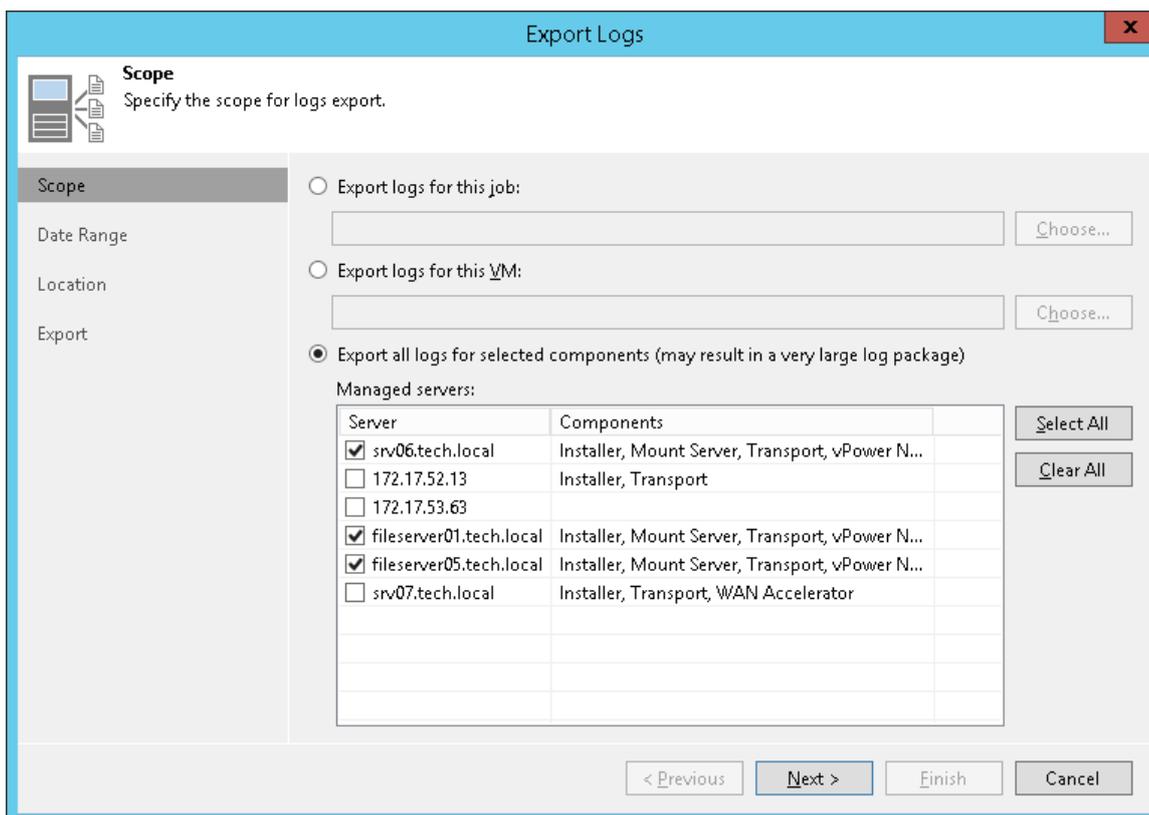
Step 1. Select Virtual Infrastructure Scope

At the **Scope** step of the wizard, define the scope for logs export. You can export logs for the following objects:

- Specific jobs on the backup server
- Specific VMs in the virtual environment
- Specific components in the backup infrastructure

NOTE:

If you export logs from the Veeam Backup & Replication console, the exported logs will be copied to the machine where the console is installed. The log archive will also contain logs from the console machine.

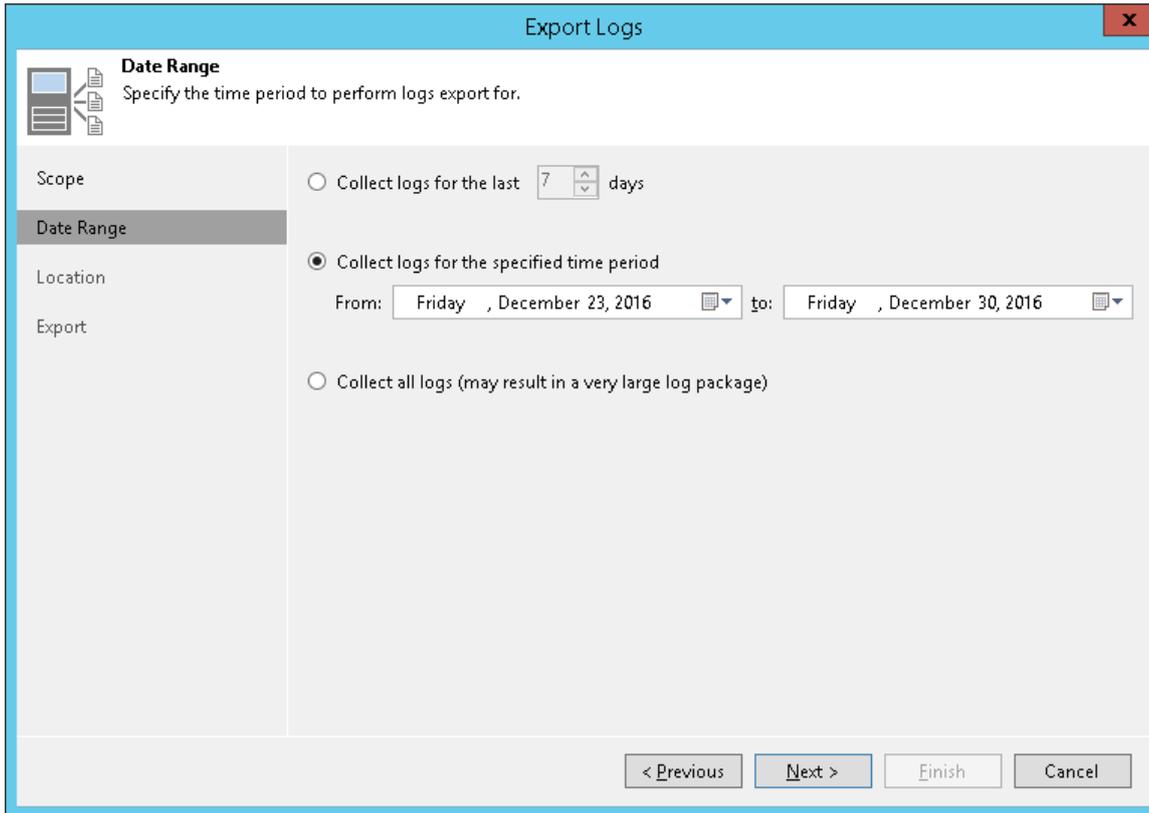


Step 2. Specify Time Interval

At the **Date Range** step of the wizard, define the time interval for which logs must be collected. You can select one of the following options:

- Collect logs for the last N days
- Collect logs for a specific period of time

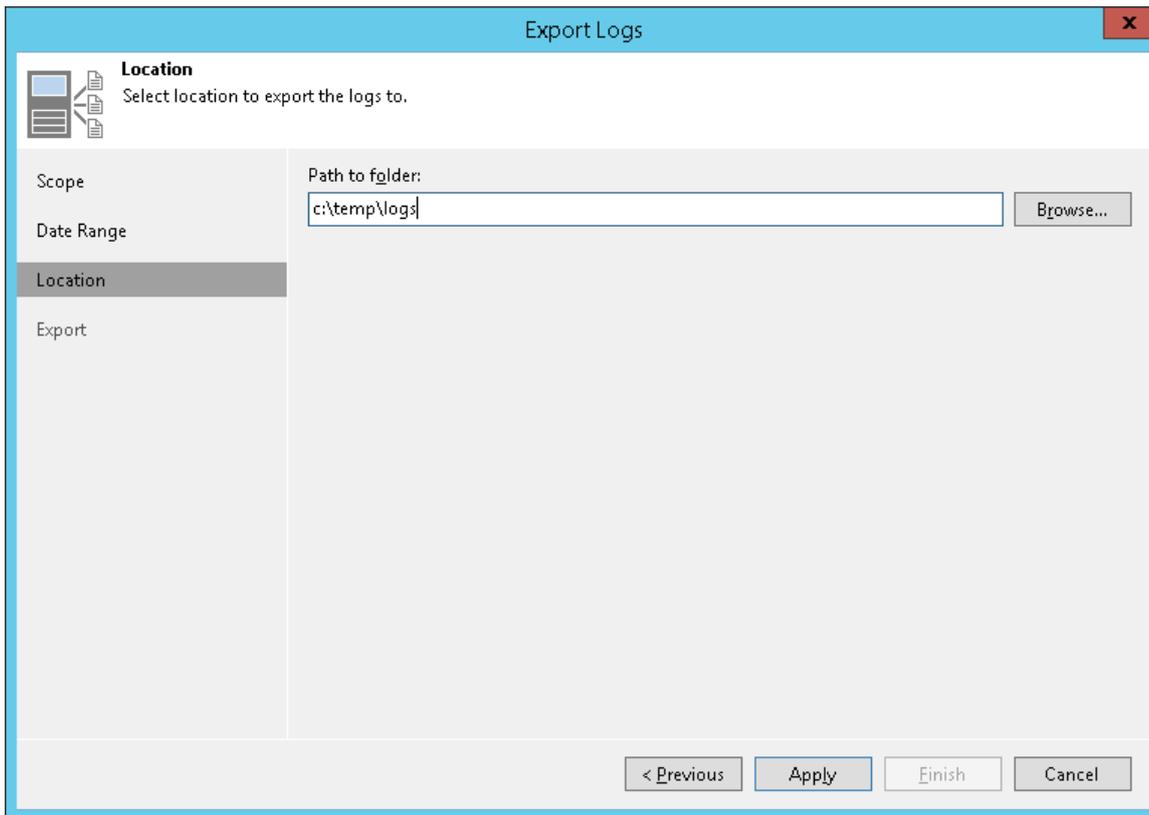
- Collect all available logs



Step 3. Specify Destination Folder

At the **Location** step of the wizard, specify the destination folder to which the logs will be exported.

In the **Path to folder** field, specify a path to an archive with log files that will be created. By default, the archive is placed to the `C:\temp\logs` folder on the backup server.



Configuration Backup and Restore

You can back up and restore the configuration database that Veeam Backup & Replication uses.

During configuration backup, Veeam Backup & Replication 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.

It is not recommended to back up the backup server configuration using backup jobs in Veeam Backup & Replication. For backup, Veeam Backup & Replication uses VM snapshots. During snapshot creation and commit, the VM freezes for some time, which can potentially lead to the following consequences:

- Disconnection from the configuration database. For more information, see the [Veeam KB1681](#) article.
- Disconnection from remote Veeam Backup & Replication agents.
- Disconnection from network storage (for example, storage presented via iSCSI) and so on.

For this reason, you must always use the configuration backup functionality to back up and restore configuration of the backup server.

Configuration Backup

By default, Veeam Backup & Replication is configured to create a configuration backup daily. You can change the schedule or run the backup manually.

See the following topics:

- [Scheduling Configuration Backups](#)
- [Configuring Notification Settings for Configuration Backups](#)
- [Running Configuration Backups Manually](#)
- [Creating Encrypted Configuration Backups](#)

Configuration Backup Files

When you perform configuration backup, Veeam Backup & Replication 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 & Replication exports information about the following objects:

- **Backup infrastructure components and objects:** hosts, servers, backup proxies, repositories, WAN accelerators and jobs, global settings configured on the backup server and so on.
- **Backups:** backups, replicas and backup copies created on the backup server.
- **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 the backup repository in which the configuration backup must be stored and specify the necessary retention settings.

NOTE:

The configuration backup job creates a snapshot of the configuration database and retrieves data required for successful restore from it. If the database size is large, the job may produce significant load on the Microsoft SQL Server. Make sure that you schedule the configuration backup job for a period of low operation intensity on the backup server.

Backup Repository Target

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 do not store configuration backups on the default backup repository or in any other folder on the backup server. In this case, if the backup server fails, its configuration data will remain, and you will be able to recover the failed backup server.

When you configure a new backup repository, Veeam Backup & Replication offers you to change the configuration backup file location from the default backup repository to the new backup repository. Click **Yes**, and Veeam Backup & Replication 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.

IMPORTANT!

You cannot store configuration backups on scale-out backup repositories.

Scheduling Configuration Backups

You can instruct Veeam Backup & Replication to perform configuration backup automatically by schedule.

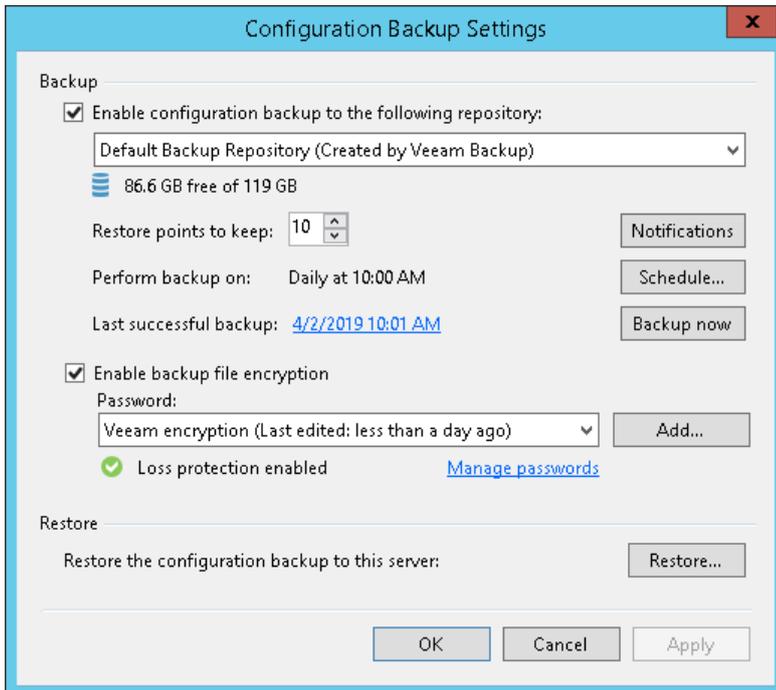
IMPORTANT!

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. From the **Backup repository** list, choose a backup repository on which the configuration backup must be stored.
4. In the **Restore points to keep** field, specify the number of restore points that you want to maintain on the backup repository.
5. Click **Schedule** next to the **Perform backup on** field and specify the time schedule according to which the configuration backup must be created.

- To create an encrypted backup, select the **Enable backup file encryption** 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](#).



Configuring Notification Settings for Configuration Backups

You can configure notifications for the configuration backup:

- From the main menu, select **Configuration Backup**.
- Click **Notifications**.
- Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully.

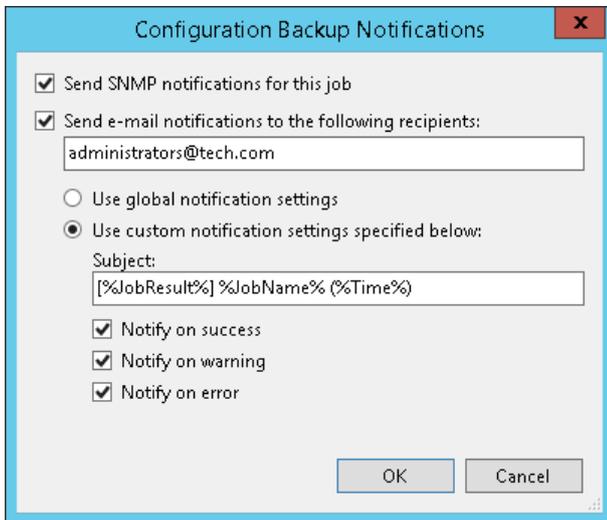
SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see [Specifying SNMP Settings](#).

- Select the **Send email notifications to the following recipients** check box if you want to receive notifications about the job completion status by email. In the field below, specify recipient's email address. You can enter several addresses separated by a semicolon.

Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see [Configuring Global Email Notification Settings](#).

- 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 & Replication will apply to the job global email notification settings specified for the backup server. For more information, see [Configuring Global Email Notification Settings](#).
 - To configure a custom notification for the job, select **Use custom notification settings specified below** check box. You can specify the following notification settings:

- a. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: `%JobResult%`, `%JobName%`, `%Time%` (completion time).
- b. 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.



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.

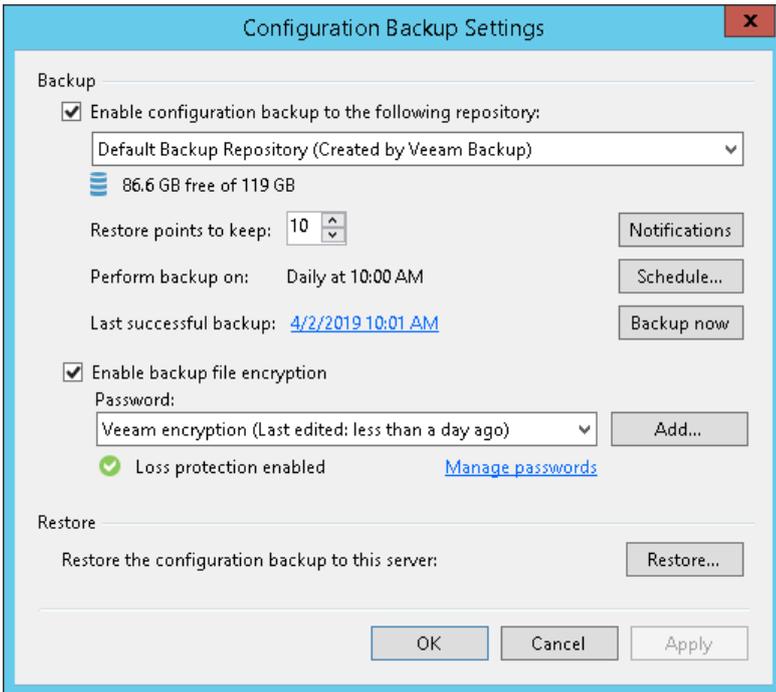
IMPORTANT!

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. From the **Backup repository** list, choose a backup repository on which the configuration backup must be stored.
4. In the **Restore points to keep** field, specify the number of restore points that you want to maintain on the backup repository.
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](#).
6. Click **Backup now**.

Veeam Backup & Replication will back up the configuration database and store a new restore point to the selected backup repository.

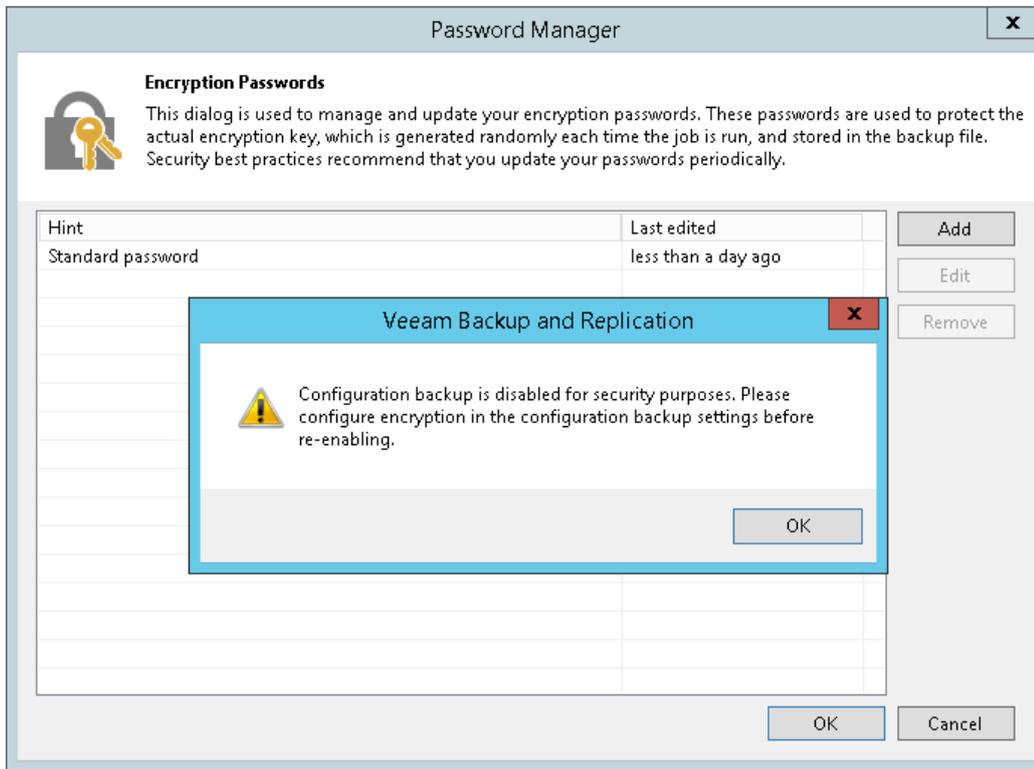


Creating Encrypted Configuration Backups

Veeam Backup & Replication 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 & Replication 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 & Replication disables configuration backup. To enable the configuration backup, you must enable encryption in the configuration backup job settings.

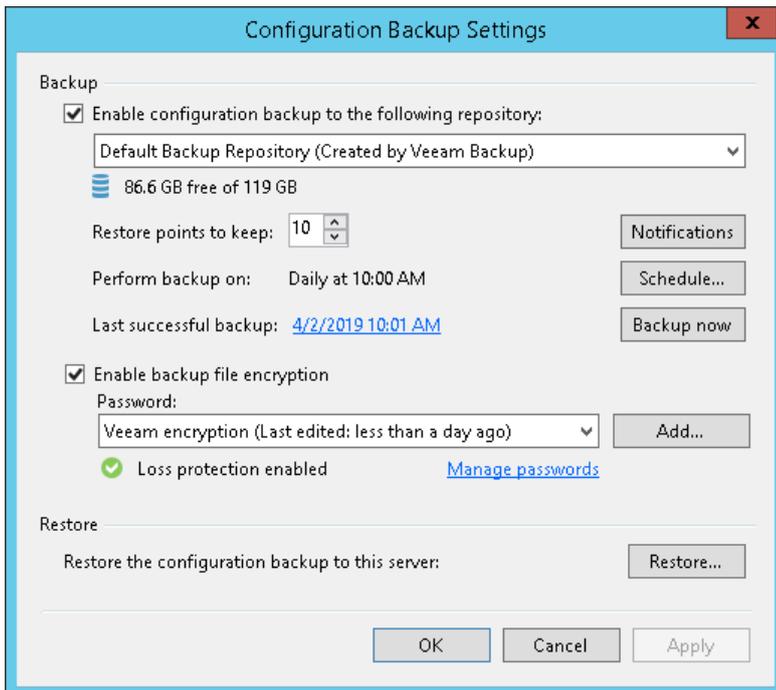


After you enable the encryption option, Veeam Backup & Replication will create encrypted configuration backups. Beside encryption keys, the created backups capture credential records specified in the Credentials Manager. When you restore data from such backup, you will not have to enter passwords for 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.

- 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 & Replication 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:

- Stop all jobs that are currently running. During restore of configuration, Veeam Backup & Replication temporary stops the Veeam Backup Service and jobs.
- Check the version of the backup server. On the backup server running Veeam Backup & Replication 9.5 Update 4, you can restore configuration backups created with the following product versions: 9.0 Update 2 and 9.5.
- Make sure that the certificate chain restored from a configuration backup will successfully pass validation on the target backup server. This precaution is required if the following conditions are met:
 - a. You want to restore configuration database of a backup server used in the Veeam Agent management scenario.
 - b. The backup server whose configuration database you want to restore uses a custom certificate issued by a Certificate Authority instead of the default self-signed certificate to ensure a secure connection in the Veeam Agent management infrastructure.

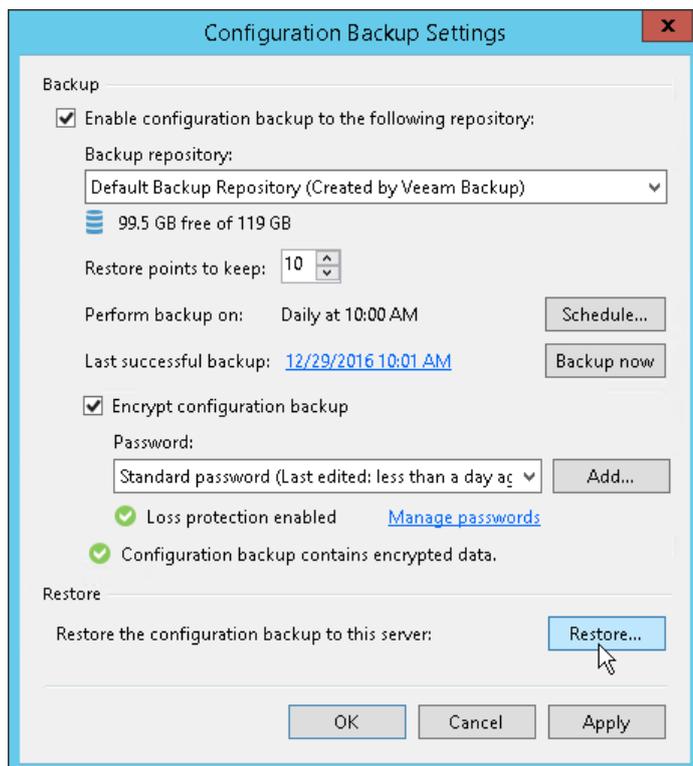
- If you plan to restore configuration data to the database on another Microsoft SQL Server, make sure the account for using Veeam Backup & Replication has sufficient permissions. For more information, see [Required Permissions](#).

You can start configuration restore only from the Veeam Backup & Replication console installed locally on the backup server. You cannot start configuration restore from the console installed on a remote machine.

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

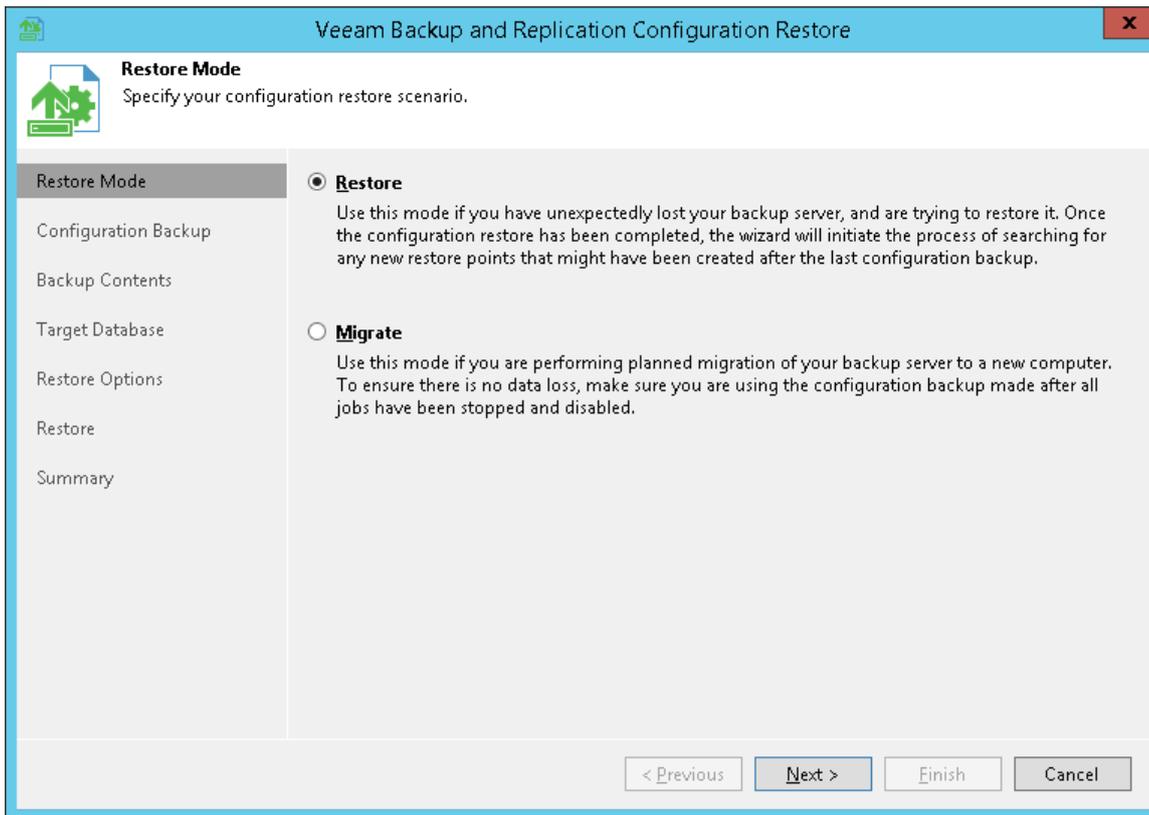
At the **Restore Mode** step of the wizard, choose a restore mode that you want to use.

- 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 & Replication retrieves configuration data from the backup and stores it to the target database. After that, Veeam Backup & Replication 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 & Replication 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 & Replication retrieves configuration data from the backup and stores it to the target database. No rescan operation is performed.

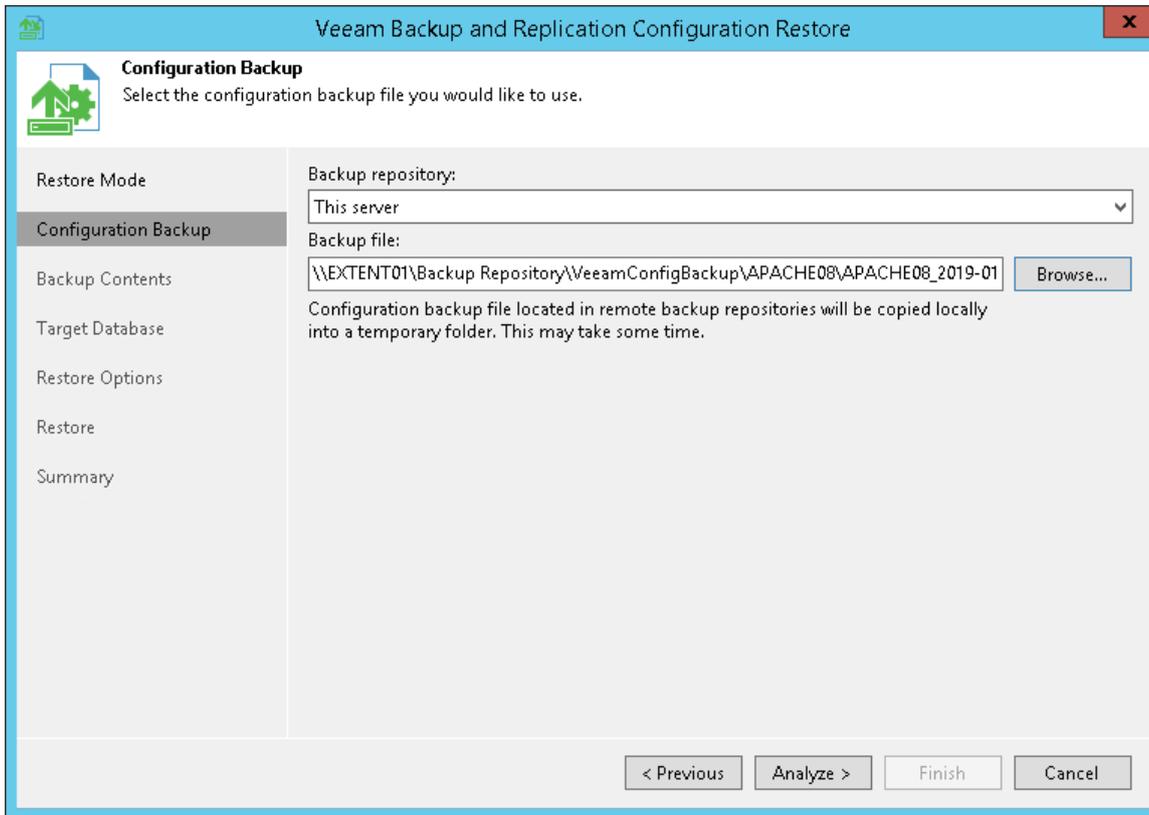


Step 3. Select Configuration Backup

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 & Replication 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 & Replication will automatically delete the configuration file from the temporary folder.

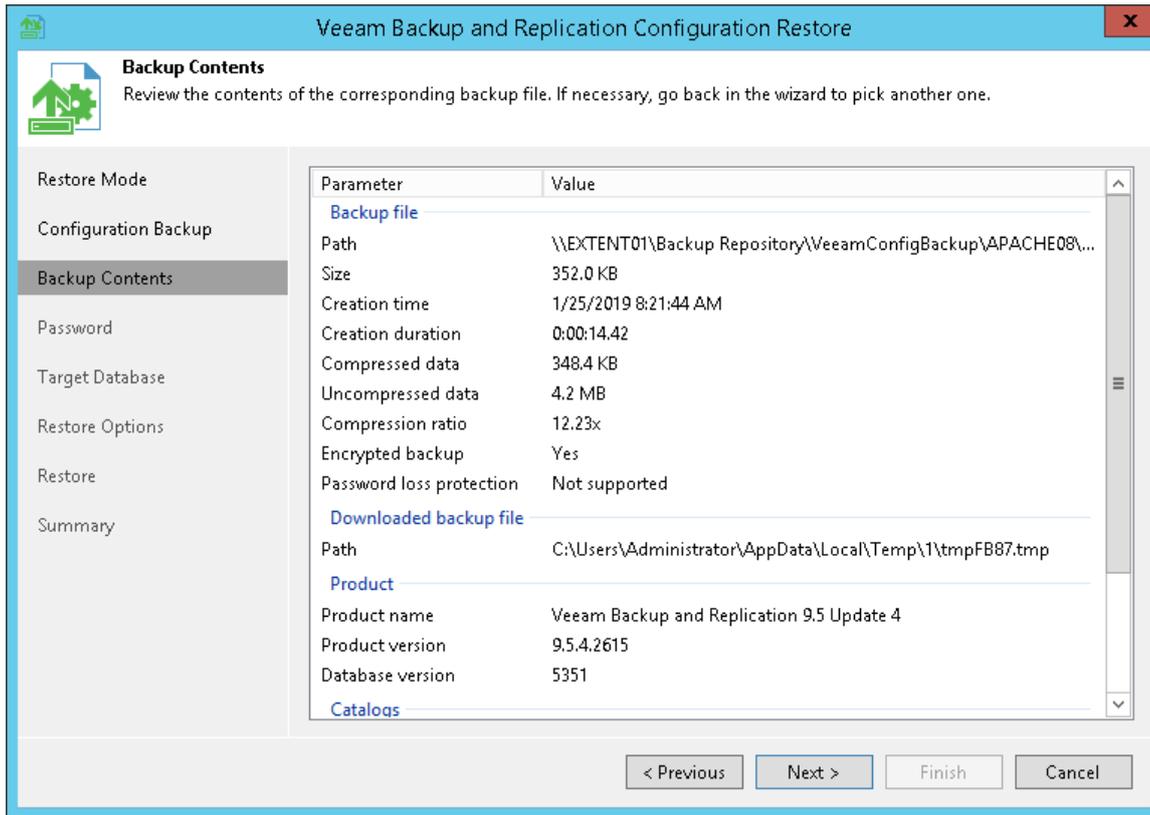


Step 4. Review Configuration Backup Parameters

At the **Backup Contents** step of the wizard, Veeam Backup & Replication 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 & Replication 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.

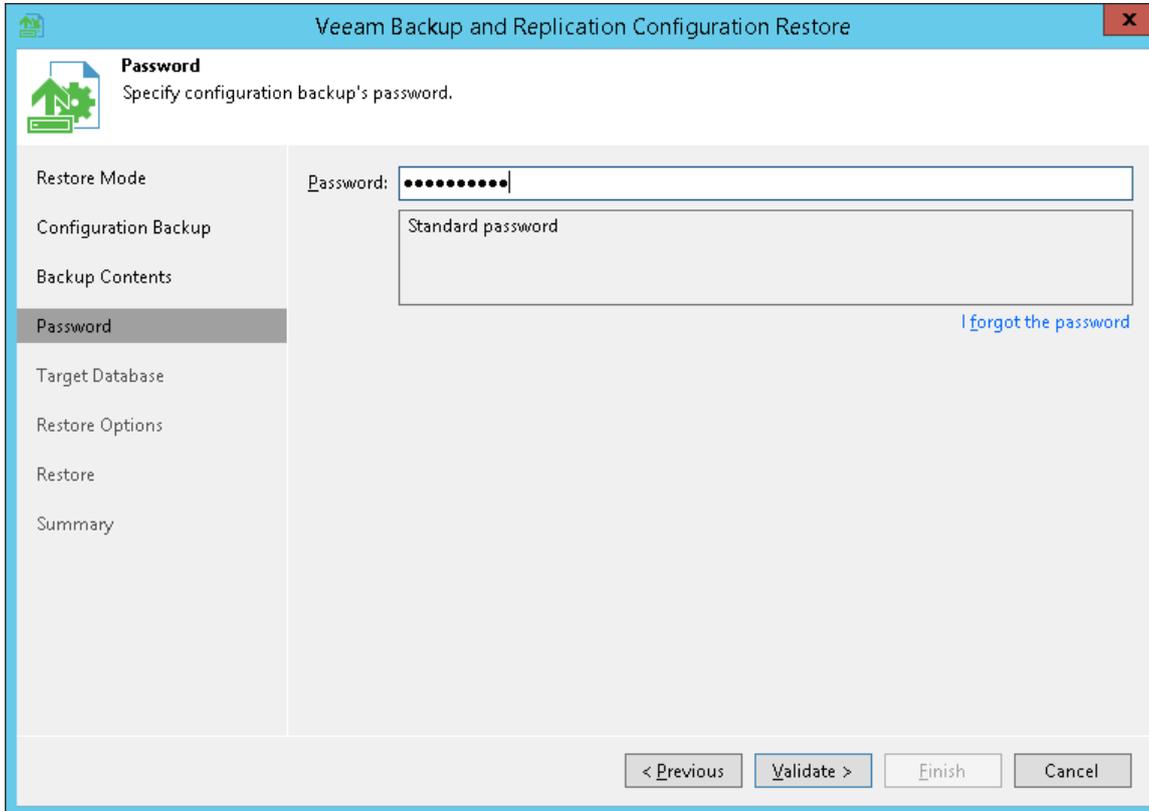
Enter the password to decrypt configuration backup data:

1. Check the password hint to recall the password.
2. In the **Password** field, enter the password to decrypt the configuration backup file.

If you have forgotten or lost the password, click the **I forgot the password** link. For more information, see [Decrypting Data Without Password](#).

NOTE:

If the backup server is not connected to Veeam Backup Enterprise Manager and does not have the Enterprise or Enterprise Plus license installed, you will not see the **I forgot the password** link and will not be able to restore configuration data without a password.



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 & Replication uses the name of the initial database.

If you specify a name of the database that does not exist, Veeam Backup & Replication 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 & Replication 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' dialog box. The 'Target Database' section is active, showing the following configuration:

- Restore Mode:** Configuration Backup
- Backup Contents:** Backup Contents
- Password:** Password
- Target Database:** Target Database (selected)
- Restore Options:** Restore Options
- Restore:** Restore
- Summary:** Summary

Connection:

- Database name: VeeamBackup
- Server name: APACHE08\SQLEXPRESS (with a Refresh button)

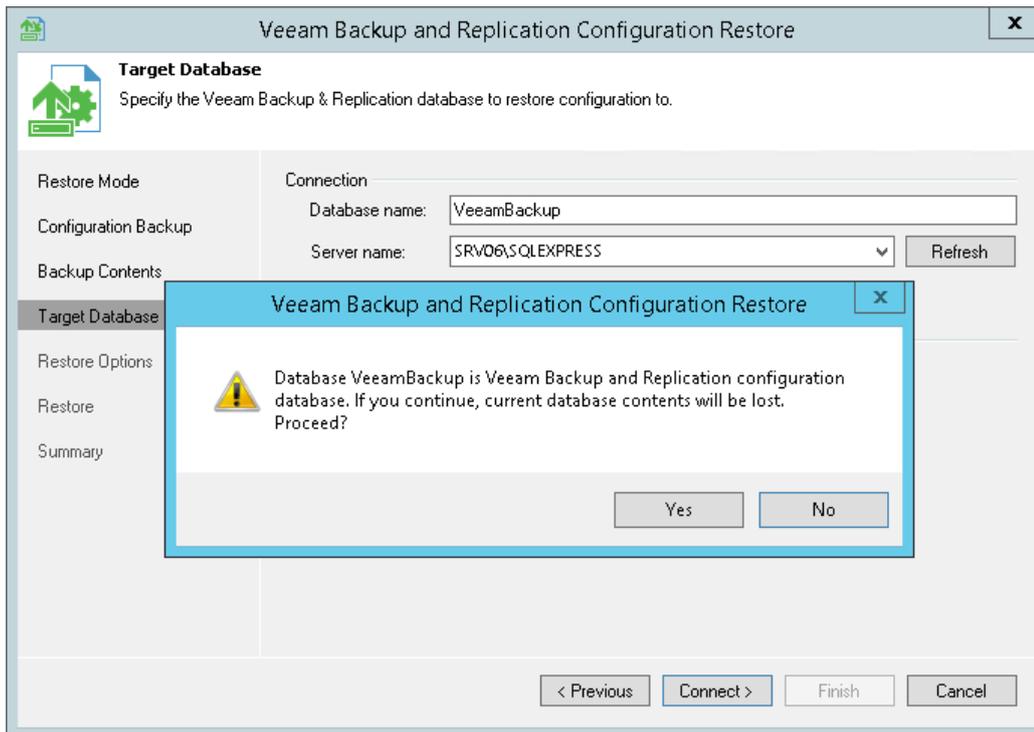
Authentication:

- Windows authentication
- SQL authentication
- Login name: APACHE08\Administrator
- Password: (empty field)

Navigation buttons at the bottom: < Previous, Connect >, Finish, Cancel.

When you restore configuration to an existing database, the configuration restore process will delete the current state of the database contents and replace it with the restored data. Veeam Backup & Replication will display a warning. If you want to replace the contents, click **Yes** to confirm.

If you do not want to lose the current data, restore the configuration to a new database. To do this, click **No** to the warning and specify a non-existing database name in the **Database name** field.



Step 7. Specify Restore Options

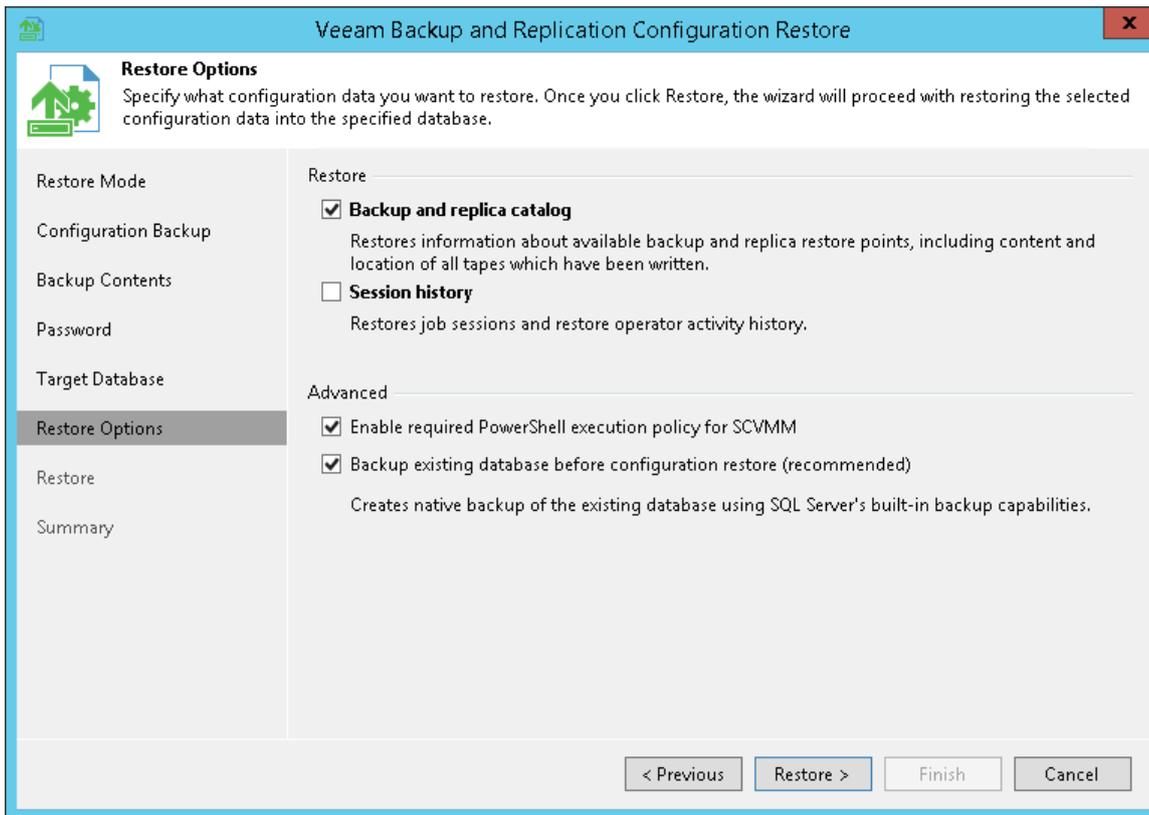
At the **Restore Options** step of the wizard, specify additional restore options.

1. In the **Restore** section, select what data you want to restore from the configuration backup. Veeam Backup & Replication 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 and information about tapes to which backups were written and location of these tapes.
 - **Session history:** data about all sessions performed on the backup server.
2. If you plan to use PowerShell on the restored backup server, select the **Enable required PowerShell policy for SCVMM** check box. During restore, Veeam Backup & Replication will enable the PowerShell execution policy and you will not have to enable it manually afterwards. Enabling this option is identical to running the '*Set-ExecutionPolicy RemoteSigned*' command on the backup server.
3. 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 & Replication will first back up the current database using the native tools of Microsoft SQL Server. After that, Veeam Backup & Replication 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:

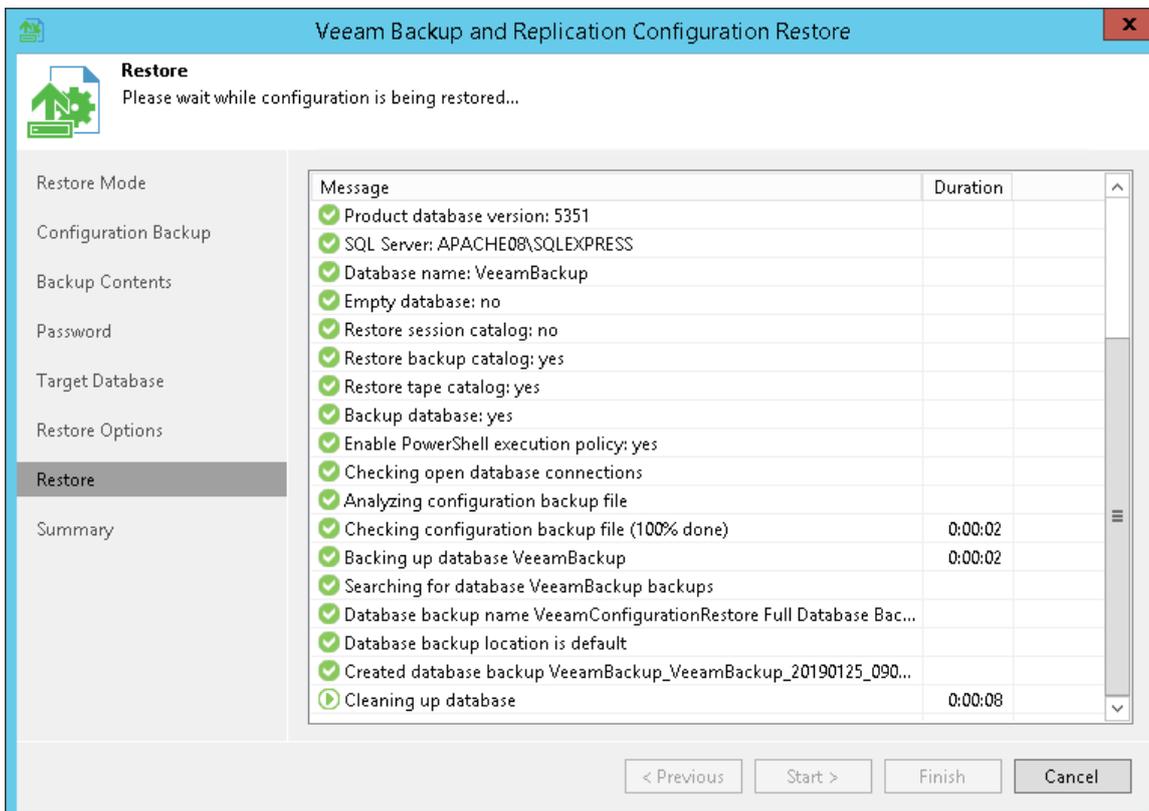
VeeamBackup<DatabaseName><date>.bak and stored to the default Microsoft SQL backups location, for example: %ProgramFiles%\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Backup\.

- Click **Restore**. Veeam Backup & Replication will stop currently running jobs and Veeam Backup & Replication services and will restore the database to the specified location.



Step 8. Review Restore Settings

At the **Restore** step of the wizard, Veeam Backup & Replication 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 & Replication 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. [Specifying credentials for cloud services](#).
3. [Perform components upgrade](#).

Specifying Credentials

At the **Credentials** step of the wizard, Veeam Backup & Replication 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.

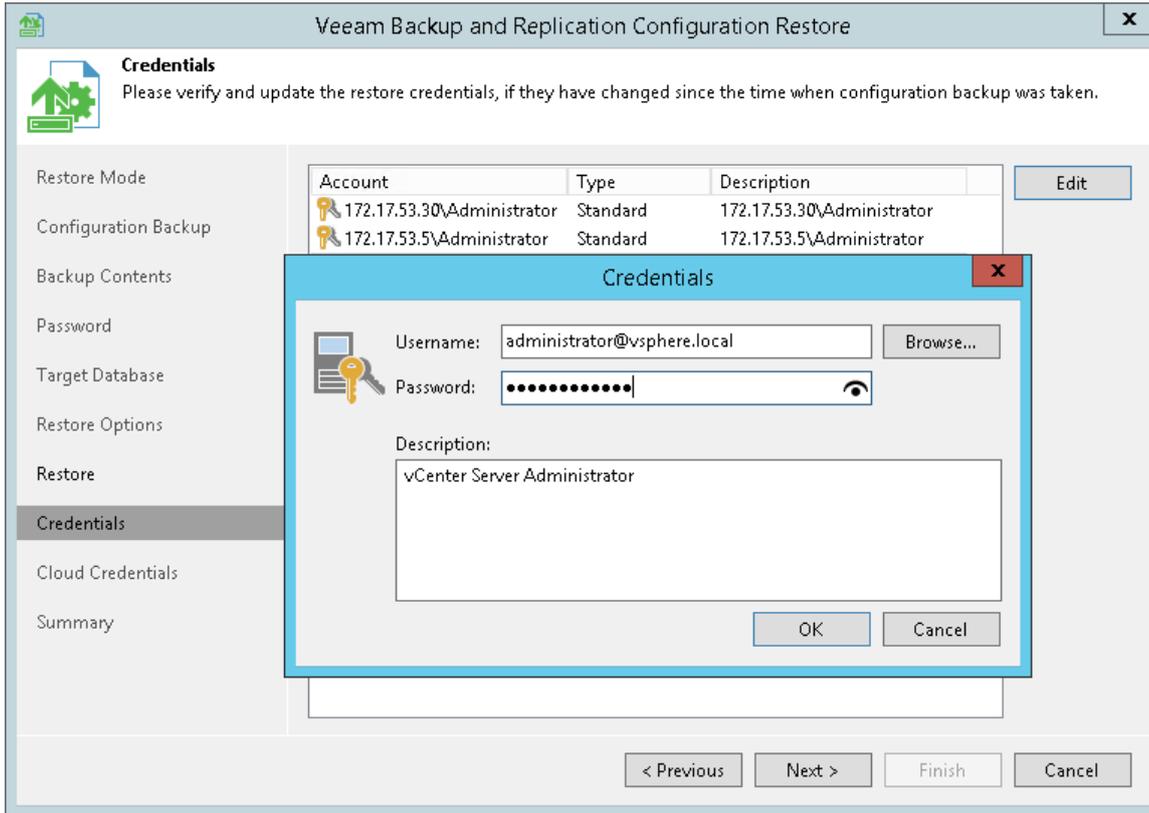
IMPORTANT!

If you have not enabled encryption for configuration backups, Veeam Backup & Replication will not restore passwords for credentials records. You need to re-enter passwords for all credentials records to make sure that backup infrastructure components and jobs work in a proper way after you complete configuration restore.

To edit credentials records:

1. Select a record in the list and click **Edit**.
2. Edit settings of the record as required.

3. Repeat the procedure for all records in the list.



Specifying Cloud Credentials

At the **Cloud Credentials** step of the wizard, Veeam Backup & Replication displays a list of cloud 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 cloud credentials records have changed, you can specify new values for these records.

IMPORTANT!

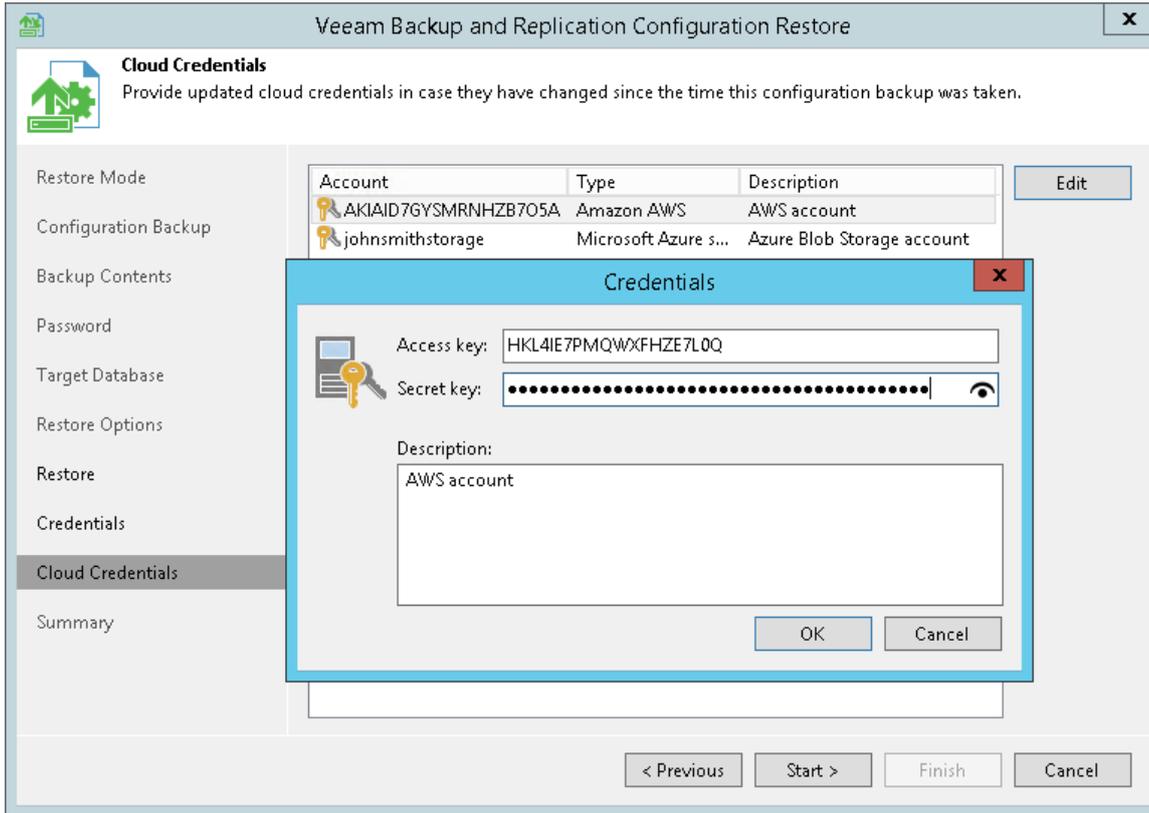
Consider the following:

- If you have not enabled encryption for configuration backups, Veeam Backup & Replication will not restore passwords for cloud credentials records. You need to re-enter passwords for all cloud credentials records to make sure that cloud services and jobs work in a proper way after you complete configuration restore.
- You cannot edit credentials of Microsoft Azure compute accounts in the configuration restore wizard. You can edit Microsoft Azure compute account credentials only after configuration restore in Cloud Credentials Manager. For details, see [Editing Cloud Credentials](#).

To edit cloud credentials records:

1. Select a record in the list and click **Edit**.
2. Edit settings of the record as required.

3. Repeat the procedure for all records in the list.



Performing Components Upgrade

After the restore process is complete, Veeam Backup & Replication 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 [Server Components Upgrade](#).

Step 10. Synchronize Backups and Tape Libraries

After the configuration database is restored, Veeam Backup & Replication 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 if you are restoring a database from a backup created with Veeam Backup & Replication 9.0 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 if you are restoring a database from a backup created with Veeam Backup & Replication 9.0 in the Restore mode and you have selected to restore data from the backup and replica catalog.

Wait for the synchronization operation to complete.

Step 11. Finish Working with Wizard

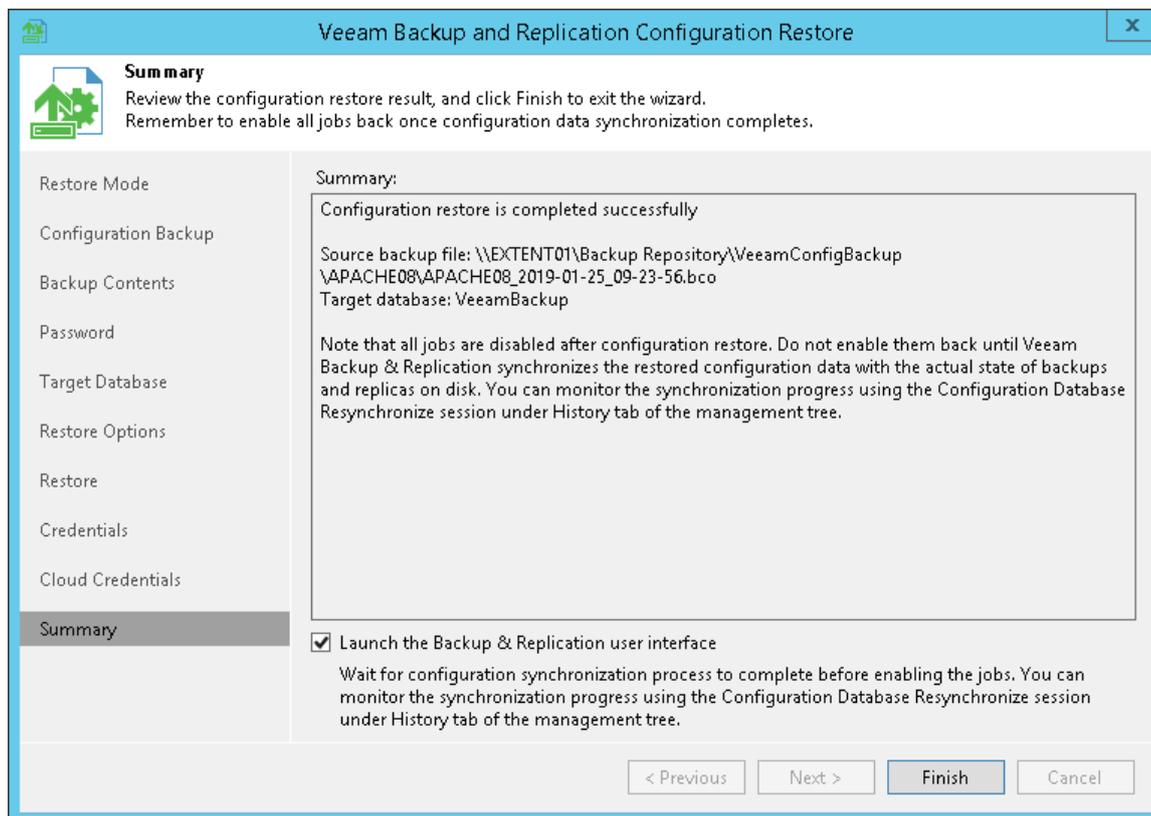
At the **Summary** step of the wizard, finalize the process of configuration data restore.

1. Review the restore process results.

2. If you want to start Veeam Backup & Replication 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 Database

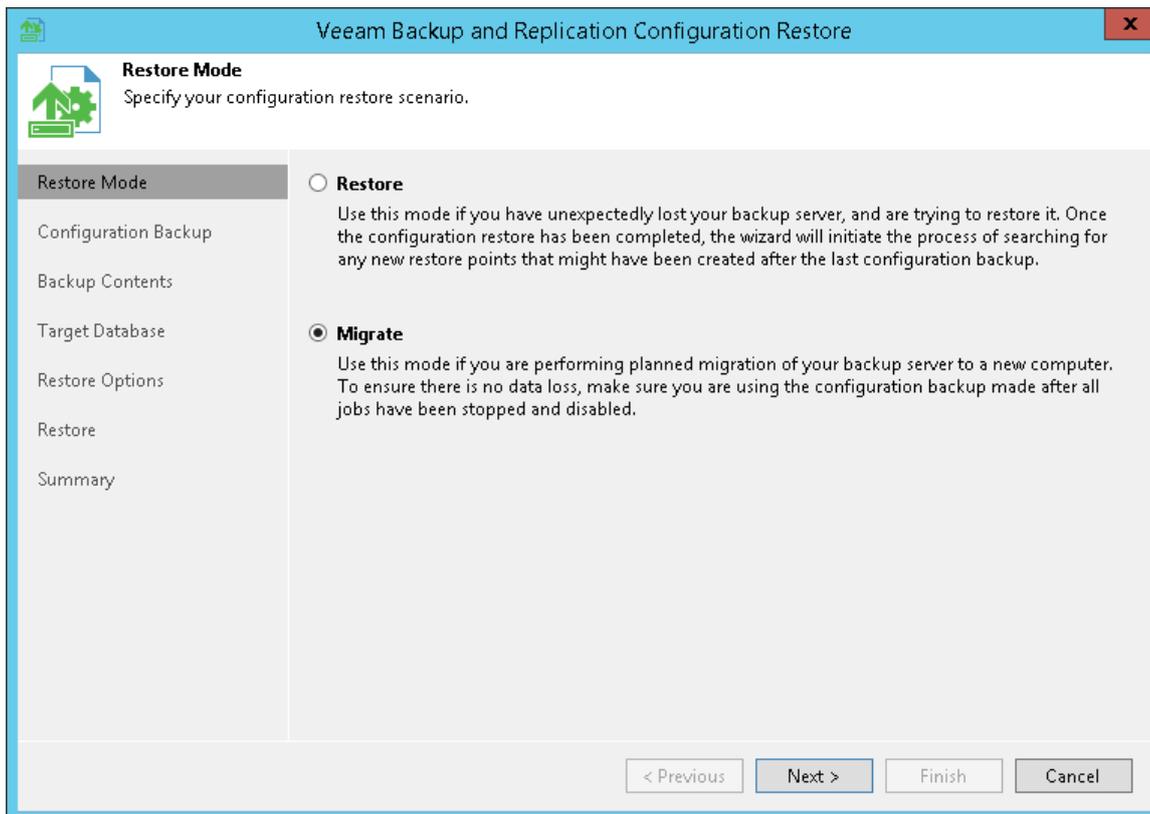
To migrate configuration data to another Microsoft SQL Server, perform the following steps:

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 & Replication 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 & Replication 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. Specify the configuration migration settings as described in the [Restoring Configuration Database](#) section.

Before restoring the configuration data in the Migrate mode, Veeam Backup & Replication performs an additional check. If the configuration backup does not meet the requirements, Veeam Backup & Replication will offer you to switch to the Restore mode. In the Restore mode, Veeam Backup & Replication will perform an 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.



Backup

Veeam Backup & Replication produces image-level backups of VMs. It treats VMs as objects, not as a set of files. When you back up VMs, Veeam Backup & Replication copies a VM image as a whole, at a block level. Image-level backups can be used for different types of restore, including Instant VM Recovery, entire VM restore, VM file recovery, file-level recovery and so on.

The backup technology is typically used for VMs with lower RTOs. When the primary VM fails, you need some time to restore VM data from a compressed and deduplicated backup file.

About Backup

Veeam Backup & Replication is built for virtual environments. It operates at the virtualization layer and uses an image-based approach for VM backup.

Veeam Backup & Replication does not install agent software inside the VM guest OS to retrieve VM data. To back up VMs, it leverages VMware vSphere snapshot capabilities. When you back up a VM, Veeam Backup & Replication requests VMware vSphere to create a VM snapshot. The VM snapshot can be thought of as a cohesive point-in-time copy of a VM including its configuration, OS, applications, associated data, system state and so on. Veeam Backup & Replication uses this point-in-time copy as a source of data for backup.

Veeam Backup & Replication copies VM data from the source datastore at a block level. It retrieves VM data, compresses and deduplicates it, and stores in backup files on the backup repository in Veeam's proprietary format.

In Veeam Backup & Replication, backup is a job-driven process. To perform backup, you need to configure backup jobs. A backup job is a configuration unit of the backup activity. The backup job defines when, what, how and where to back up. One backup job can be used to process one or several VMs. You can instruct Veeam Backup & Replication to run jobs automatically by schedule or start them manually.

The first backup job session always produces a full backup of the VM image. Subsequent backup job sessions are incremental – Veeam Backup & Replication copies only those data blocks that have changed since the last backup job session. To keep track of changed data blocks, Veeam Backup & Replication uses different approaches. For more information, see [Changed Block Tracking](#).

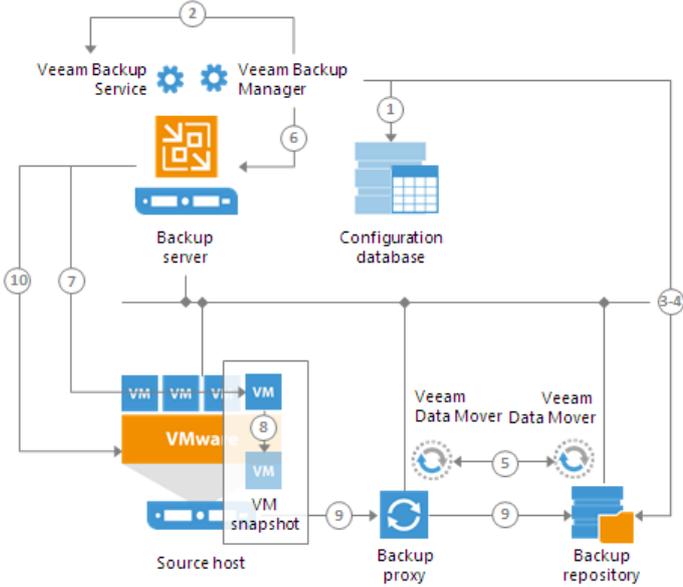
How Backup Works

Veeam Backup & Replication performs VM backup in the following way:

1. When a new backup job session starts, Veeam Backup & Replication starts the Veeam Backup Manager process on the backup server. Veeam Backup Manager reads job settings from the configuration database and creates a list of VM tasks to process. For every disk of VMs added to the job, Veeam Backup & Replication creates a new task.
2. Veeam Backup Manager connects to the Veeam Backup Service. The Veeam Backup Service includes a resource scheduling component that manages all tasks and resources in the backup infrastructure. The resource scheduler checks what backup infrastructure resources are available, and assigns backup proxies and backup repositories to process job tasks.
3. Veeam Backup Manager connects to Veeam Transport Services on the target repository and backup proxy. The Veeam Transport Services, in their turn, start Veeam Data Movers. A new instance of Veeam Data Mover is started for every task that the backup proxy is processing.
4. Veeam Backup Manager establishes a connection with Veeam Data Movers on the backup repository and backup proxy, and sets a number of rules for data transfer, such as network traffic throttling rules and so on.
5. Veeam Data Movers on the backup proxy and backup repository establish a connection with each other for data transfer.
6. Veeam Backup Manager queries information about VMs and virtualization hosts from the Veeam Broker Service.
7. If application-aware image processing is enabled for the job, Veeam Backup & Replication connects to VM guest OSes, deploys runtime processes on VM guest OSes and performs in-guest processing tasks.
8. Veeam Backup & Replication requests vCenter Server or ESXi host to create a VM snapshot. VM disks are put to the read-only state, and every virtual disk receives a delta file. All changes that the user makes to the VM during backup are written to delta files.
9. The source Veeam Data Mover reads the VM data from the read-only VM disk and transfers the data to the backup repository in one of transport modes. During incremental job sessions, the source Veeam Data Mover uses CBT to retrieve only those data blocks that have changed since the previous job session. If CBT is not available, the source Veeam Data Mover interacts with the target Veeam Data Mover on the backup repository to obtain backup metadata, and uses this metadata to detect blocks that have changed since the previous job session.

While transporting VM data, the source Veeam Data Mover performs additional processing. It filters out zero data blocks, blocks of swap files and blocks of excluded VM guest OS files. The source Veeam Data Mover compresses VM data and transports it to the target Veeam Data Mover.

10. After the backup proxy finishes reading VM data, Veeam Backup & Replication requests the vCenter Server or ESXi host to commit the VM snapshot.



Backup Architecture

Veeam Backup & Replication uses the following components for the backup process:

- One or more source hosts with associated datastores
- One or more backup proxies
- Backup repository
- [Optional] One or more guest interaction proxies
- [For shared folder backup repository] Gateway server

All backup infrastructure components engaged in the job make up a data pipe. The source host and backup repository produce two terminal points for the data flow. Veeam Backup & Replication processes VM data in multiple cycles, moving VM data over the data pipe block by block.

Veeam Backup & Replication collects VM data, transforms and transport it to target with the help of Veeam Data Movers. Veeam Backup & Replication uses two-service architecture – one Veeam Data Mover controls interaction with the source host, and the other one controls interaction with the backup repository. The Veeam Data Movers communicate with each other and maintain a stable connection.

When a new backup session starts, Veeam Backup & Replication performs the following actions:

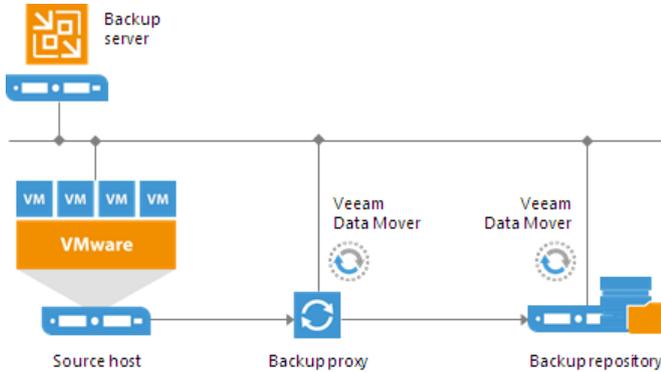
1. Veeam Backup & Replication deploys runtime processes on VM guest OSes via the guest interaction proxy (for Microsoft Windows VMs) or backup server (for VMs with other OSes).
2. The target-side Veeam Data Mover obtains job instructions and communicates with the source-side Veeam Data Mover to begin data collection.
3. The source-side Veeam Data Mover copies VM data from the source storage in one of transport modes. During incremental job runs, the source-side Veeam Data Mover retrieves only those data blocks that have changed since the previous job session.

While copying, the source-side Veeam Data Mover performs additional data processing. It filters out zero data blocks, blocks of swap files and blocks of excluded VM guest OS files, compresses and deduplicates VM data blocks and moves them to the target-side Data Mover Service.

4. The target-side Veeam Data Mover deduplicates similar blocks of data on the target side and writes the result to the backup file on the backup repository.

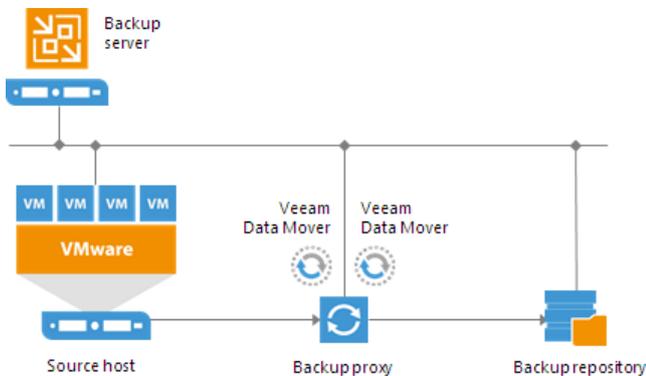
Onsite Backup

To back up to a Microsoft Windows or Linux backup repository in the local site, you need to deploy a backup proxy on a machine that has access to the source datastore, and point the backup job to this backup proxy. In this scenario, the source-side Veeam Data Mover is started on the backup proxy, and the target-side Veeam Data Mover is started on the Microsoft Windows or Linux repository. VM data is sent from the backup proxy to the backup repository over the LAN.



To back up to a shared folder in the local site, you need to deploy a gateway server that has access to the shared folder backup repository. You can assign the role of a gateway server to the backup server itself or any Microsoft Windows machine added to the backup infrastructure.

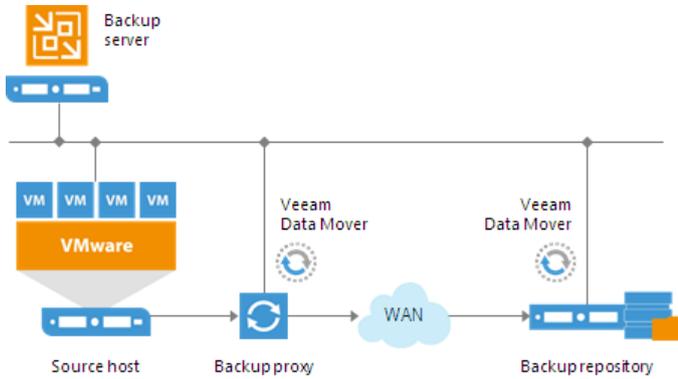
You can use the same Microsoft Windows machine as the backup proxy and gateway server for SMB. In this scenario, Veeam Backup & Replication starts the source-side and target-side Veeam Data Movers on the same machine, and sends VM data from the backup proxy to the shared folder backup repository over the LAN.



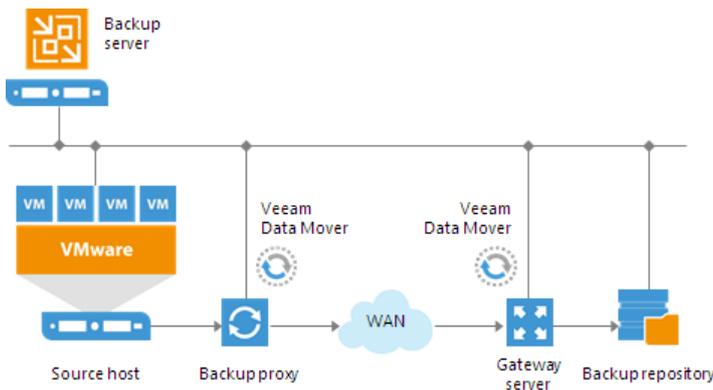
Offsite Backup

The common requirement for offsite backup is that one Veeam Data Mover runs in the production site (closer to the source datastore), and the other Veeam Data Mover runs in the remote site, closer to the backup repository. During backup, Veeam Data Movers maintain a stable connection, which allows for uninterrupted operation over the WAN or slow links.

To back up to a Microsoft Windows or Linux repository in the remote site, you need to deploy a backup proxy in the production site, closer to the source datastore. In this scenario, the source-side Veeam Data Mover is started on the backup proxy, and the target-side Veeam Data Mover is started on the Microsoft Windows or Linux repository. VM data is sent from the backup proxy to the backup repository over the WAN.



To back up VMs to shared folder backup repository in the remote site, you must deploy a backup proxy in the source site and a gateway server in the remote site. The shared folder backup repository must be pointed at the target-side gateway server. During backup, the source-side Veeam Data Mover is started on the source backup proxy in the production site, and the target-side Veeam Data Mover is started on the target gateway server in the remote site. VM data is transferred between the backup proxy and gateway server over the WAN.



Backup Chain

Veeam Backup & Replication creates and maintains the following types of backup files:

- VBK – full backup files that store copies of full VM images.
- VIB or VRB – incremental backup files that store incremental changes of VM images.
- VBM – backup metadata files that store information about the backup job, VMs processed by the backup job, number and structure of backup files, restore points, and so on. Metadata files facilitate import of backups, backup mapping and other operations.

In addition to these file types, Veeam Backup & Replication can create the following files on the backup repository:

- VSB – virtual synthetic backup files used for generation of virtual full backups on tapes. For more information, see [Virtual Full Backups](#).
- VLB and VSM – files that store Microsoft SQL Server transaction log data. For more information, see [Microsoft SQL Server Logs Backup and Restore](#).
- VLB and VOM – files that store Oracle archived log data. For more information, see [Oracle Logs Backup and Restore](#).

All backup files created by the backup job reside in a dedicated job folder on the backup repository. For example, if you create a backup job with the *DC Backup* name, Veeam Backup & Replication will create the `DC Backup` folder on the target backup repository and store all backup files produced with this job in this folder.

Backup files make up a backup chain. The backup chain consists of first full backup file, incremental backup files and, additionally, backup metadata file. Full and incremental backup files correspond to restore points of backed up VMs. You can think of restore points as of "snapshots" of VM data at specific points in time. Restore points let you roll back VMs to the necessary state.

To roll back a VM to a specific point in time, you need a chain of backup files: a full backup file plus a set of incremental backup files dependent on this full backup file. If some file in the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete separate backup files from the backup repository manually. Instead, you must specify retention policy settings that will let you maintain the desired number of backup files on the backup repository.

Veeam Backup & Replication offers 3 backup methods to create backup chains:

- Forever forward incremental backup
- Forward incremental backup
- Reverse incremental backup

By default, during every backup job session Veeam Backup & Replication writes data of all VMs to the same backup file. If necessary, you can instruct Veeam Backup & Replication to create per-VM backup chains – that is, produce a separate backup chain for every VM added to the backup job.

Backup Methods

Veeam Backup & Replication provides three methods for creating backup chains:

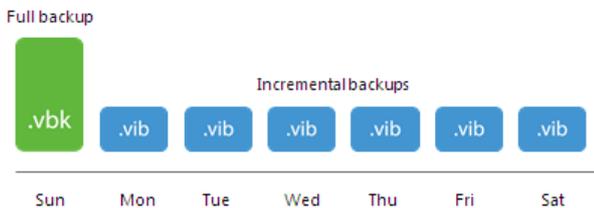
- [Forever forward incremental backup](#)
- [Forward incremental backup](#)
- [Reverse incremental backup](#)

Forever Forward Incremental Backup

The forever forward incremental backup method produces a backup chain that consists of the first full backup file (VBK) and a set of forward incremental backup files (VIB) following it.

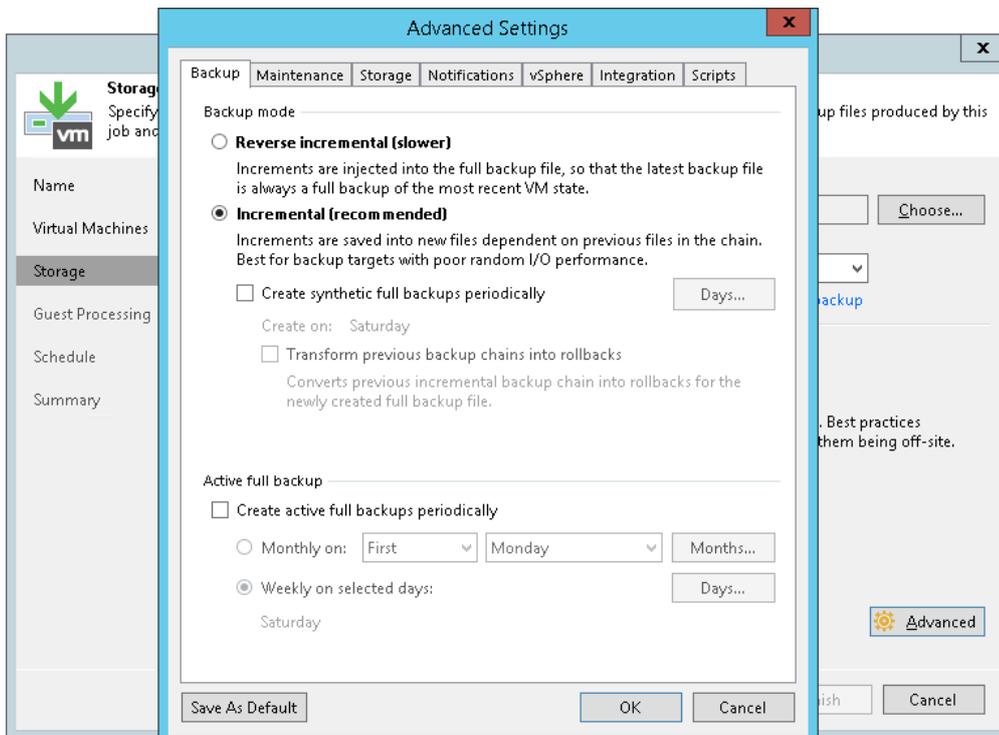
Veeam Backup & Replication creates a forever forward incremental backup chain in the following way:

1. During the first session of a backup job, Veeam Backup & Replication creates a full backup file on the backup repository.
2. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session (full or incremental) and saves these blocks as an incremental backup file in the backup chain.
3. After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy for the job. If Veeam Backup & Replication detects an outdated restore point, it transforms the backup chain to make room for the most recent restore point. For more information, see [Forever Forward Incremental Backup Retention Policy](#).



To use the forever forward incremental backup method, you must select the following options in the backup job settings:

1. Select the **Incremental** backup mode.
2. Do not enable synthetic full backups and/or active full backups. If you enable synthetic and/or active full backups, Veeam Backup & Replication will produce a [forward incremental backup chain](#).

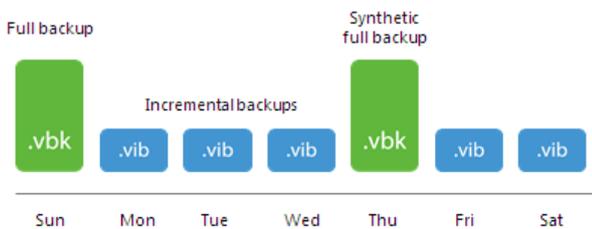


Forward Incremental Backup

The forward incremental backup method produces a backup chain that consists of the first full backup file (VBK) and a set of forward incremental backup files (VIB) following it. Additionally, the forward incremental backup chain contains synthetic full and/or active full backup files that “split” the backup chain into shorter series.

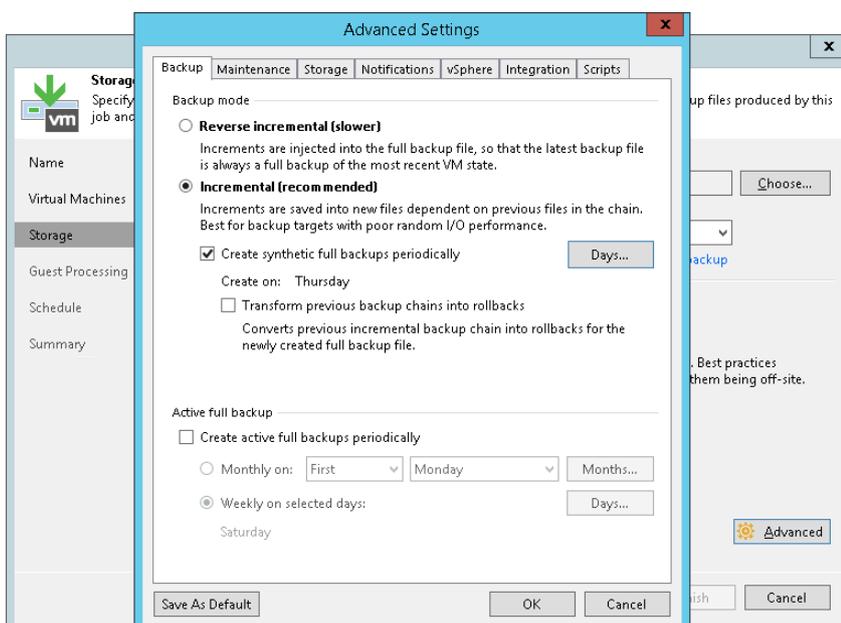
Veeam Backup & Replication creates a forward incremental backup chain in the following way:

1. During the first backup job session, Veeam Backup & Replication creates a full backup file on the backup repository.
2. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session (full or incremental) and saves these blocks as an incremental backup file in the backup chain.
3. On a day when the synthetic full or active full backup is scheduled, Veeam Backup & Replication creates a full backup file and adds it to the backup chain. Incremental restore points produced after this full backup file use it as a new starting point.
4. After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy set for the job. If Veeam Backup & Replication detects an outdated restore point, it attempts to remove this point from the backup chain. For more information, see [Retention for Forward Incremental Backup](#).



The forward incremental backup with synthetic full backup enabled is a default method for backup chain creation. To use the forward incremental backup method, you can leave the default settings or select the following options in the backup job settings:

1. Select the **Incremental** backup mode.
2. Enable synthetic full backups and/or active full backups. If the synthetic full backup and/or active full backups are not enabled, Veeam Backup & Replication will produce a [forever forward incremental backup chain](#).



Reverse Incremental Backup

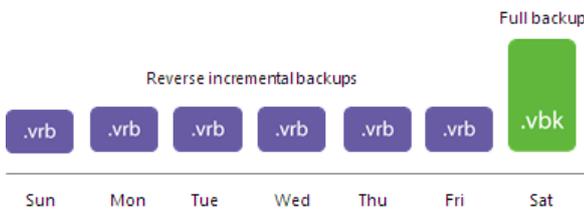
The reverse incremental backup method produces a backup chain that consists of the last full backup file (VBK) and a set of reverse incremental backup files (VRB) preceding it.

Veeam Backup & Replication creates a reverse incremental backup chain in the following way:

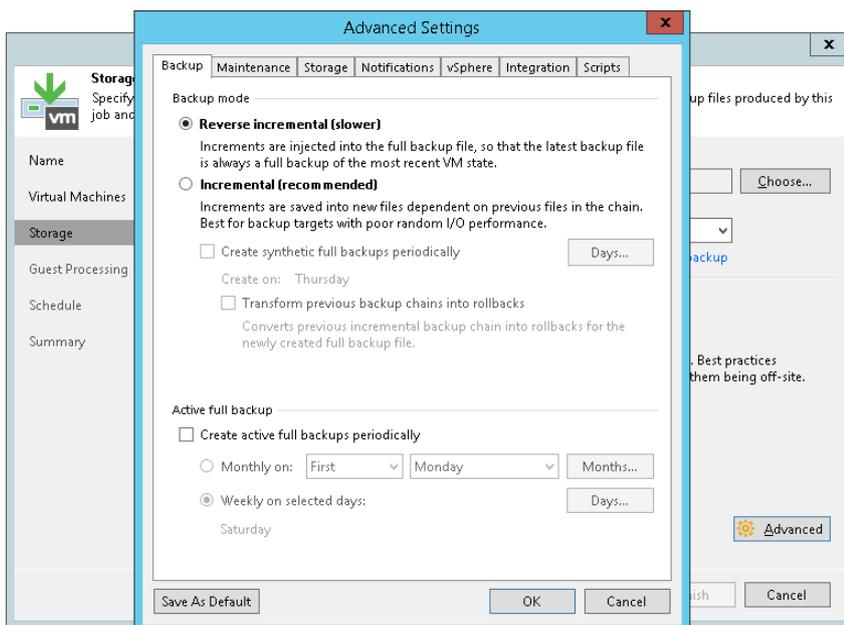
1. During the first backup job session, Veeam Backup & Replication creates a full backup file on the backup repository.
2. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session. Veeam Backup & Replication “injects” copied data blocks into the full backup file to rebuild it to the most recent state of the VM. Additionally, Veeam Backup & Replication creates a reverse incremental backup file containing data blocks that are replaced when the full backup file is rebuilt, and adds this reverse incremental backup file before the full backup file in the backup chain.
3. After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy set for the job. If Veeam Backup & Replication detects an outdated restore point, it removes this point from the backup chain. For more information, see [Retention for Reverse Incremental Backup](#).

As a result, the most recent restore point in the backup chain is always a full backup, and it gets updated after every successful backup job session.

The reverse incremental backup method lets you immediately restore a VM to the most recent state without extra processing because the most recent restore point is a full backup file. If you need to restore a VM to a particular point in time, Veeam Backup & Replication applies the required VRB files to the VBK file to get to the required restore point.



To use the reverse incremental backup method, you must select the **Reverse incremental** option in the backup job settings.



Switching Between Backup Methods

You can easily switch between backup methods. Veeam Backup & Replication does not transform the previously created chain. Instead, it creates a new backup chain next to the existing one in the following manner:

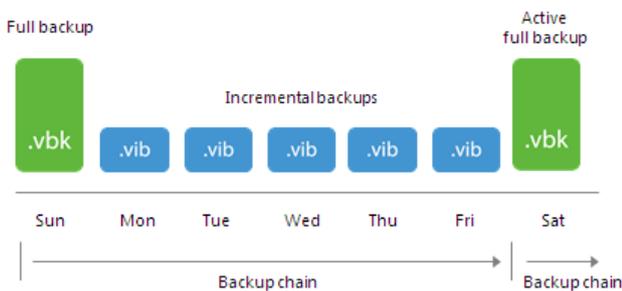
- If you switch from the reverse incremental method to the forever forward incremental or forward incremental method, Veeam Backup & Replication creates a set of incremental backup files next to the reverse incremental chain. The full backup file in the reverse incremental chain is used as a starting point for incremental backup files.
- If you switch from the forever forward incremental or forward incremental method to the reverse incremental method, Veeam Backup & Replication first creates a full backup file next to incremental backup files. During every new job session, Veeam Backup & Replication transforms this full backup file and adds reverse incremental backup files to the backup chain.
- If you switch from the forever forward incremental method to the forward incremental method, Veeam Backup & Replication creates synthetic full backups according to the specified schedule. Old backup chain is deleted when the number of restore points in the new chain reach the retention limit.
- If you switch from the forward incremental method to the forever forward incremental method, synthetic full backups are no longer created. When the number of restore points created since the last full backup reach the retention limit, the old backup chain is deleted. Thereafter, with each restore point creation the earliest increment file will merge with the full backup file.

Active Full Backup

In some cases, you need to regularly create a full backup. For example, your corporate backup policy may require that you create a full backup on weekend and run incremental backup on work days. To let you conform to these requirements, Veeam Backup & Replication lets you create active full backups.

The active full backup produces a full backup of a VM, just as if you run the backup job for the first time. Veeam Backup & Replication retrieves data for the whole VM from the source, compresses and deduplicates it and stores it to the full backup file – VBK.

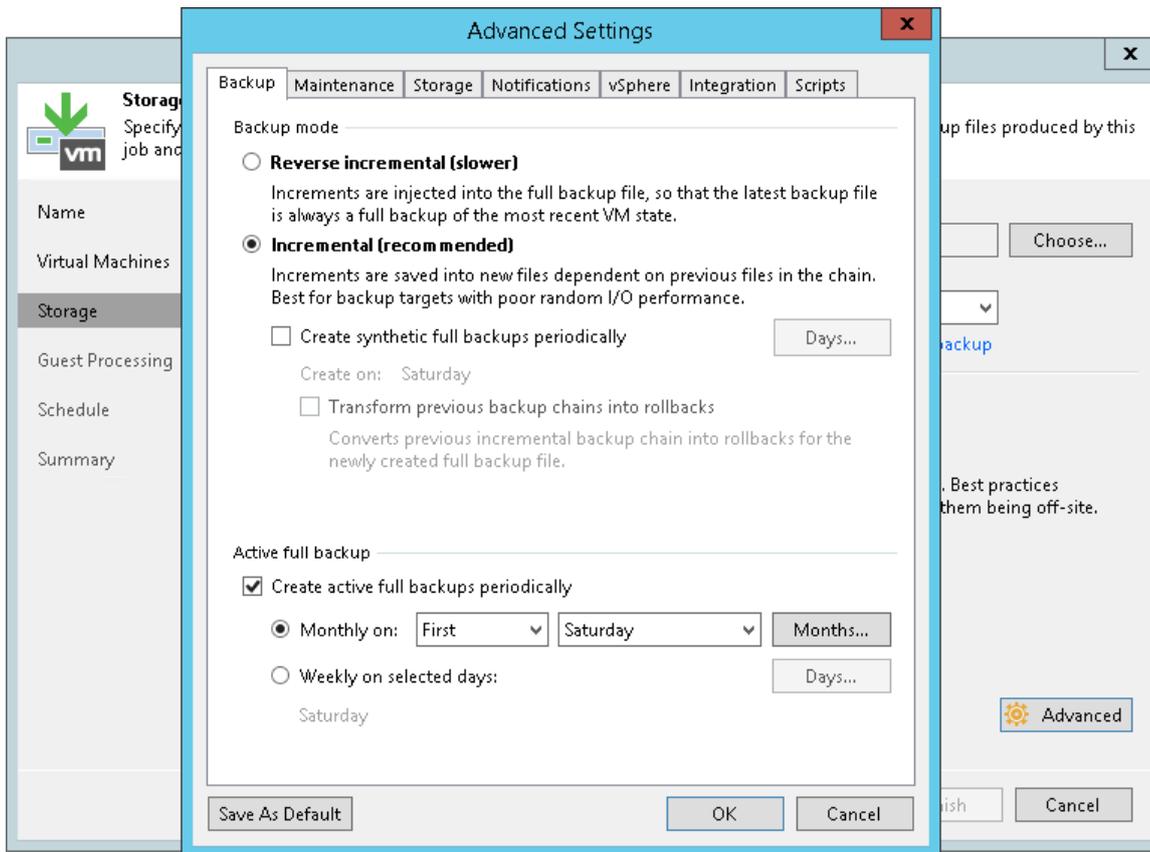
The active full backup resets a backup chain. All incremental backup files use the latest active full backup file as a new starting point. A previously used full backup file remains on disk until it is automatically deleted according to the retention policy.



You can create active full backups manually or schedule a backup job to create active full backups periodically.

- To create an active full backup manually, use the **Active Full** command from the shortcut menu of a corresponding backup job.

- To schedule active full backups, specify scheduling settings in the **Advanced** section of a corresponding backup job. You can schedule active full backups to run weekly, for example, every Saturday, or monthly, for example, every fourth Sunday of a month.



Active Full Backup Schedule

Veeam Backup & Replication automatically triggers a backup job to create an active full backup, even if a regular backup job session is not scheduled on this day. The job session is started at the same time when the parent backup job is scheduled. For example, if you schedule the parent backup job at 12:00 AM Sunday through Friday, and schedule active full backup on Saturday, Veeam Backup & Replication will start a backup job session that will produce an active full backup at 12:00 AM on Saturday.

If the parent backup job is not scheduled to run automatically or disabled, Veeam Backup & Replication will not perform active full backup.

If a regular backup job is scheduled together with active full backup, Veeam Backup & Replication will produce only one backup file – an active full backup that will contain the latest state of the source VM. An incremental backup file that should have been created by the backup job schedule will not be added to the backup chain.

Veeam Backup & Replication creates an active full backup only once a day on which active full backup is scheduled (unless you create a full backup manually). If you run the backup job again on the same day, Veeam Backup & Replication will perform incremental backup in a regular manner.

Synthetic Full Backup

In some situations, running active full backups periodically may not be an option. Active full backups are resource-intensive and consume considerable amount of network bandwidth. As an alternative, you can create synthetic full backups.

In terms of data, the synthetic full backup is identical to a regular full backup. Synthetic full backup produces a VBK file that contains data of the whole VM. The difference between active and synthetic full backup lies in the way how VM data is retrieved:

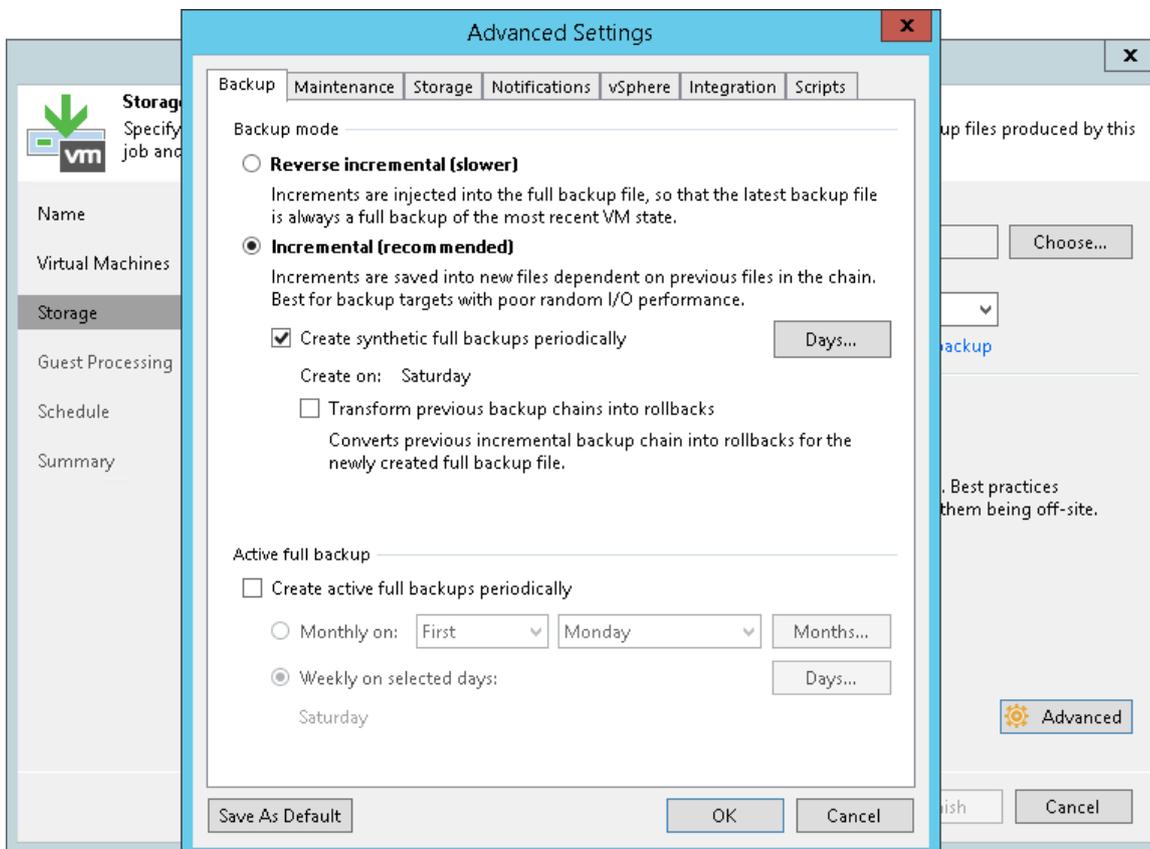
- When you perform active full backup, Veeam Backup & Replication retrieves VM data from the source datastore where the VM resides, compresses and deduplicates it and writes it to the VBK file on the backup repository.
- When you perform synthetic full backup, Veeam Backup & Replication does not retrieve VM data from the source datastore. Instead, it synthesizes a full backup from data you already have on the backup repository. Veeam Backup & Replication accesses the previous full backup file and a chain of subsequent incremental backup files on the backup repository, consolidates VM data from these files and writes consolidated data into a new full backup file. As a result, the created synthetic full backup file contains the same data you would have if you created an active full backup.

The synthetic full backup has a number of advantages:

- The synthetic full backup does not use network resources: it is created from backup files you already have on disk.
- The synthetic full backup produces less load on the production environment: it is synthesized right on the backup repository.

Veeam Backup & Replication treats synthetic full backups as regular full backups. As well as any other full backup file, the synthetic full backup file resets the backup chain. All subsequent incremental backup files use the synthetic full backup file as a new starting point. A previously used full backup file remains on disk until it is automatically deleted according to the retention policy.

To create synthetic full backups, you must enable the **Create synthetic full backups periodically** option and schedule creation of synthetic full backups on specific days in the backup job settings.



How Synthetic Full Backup Works

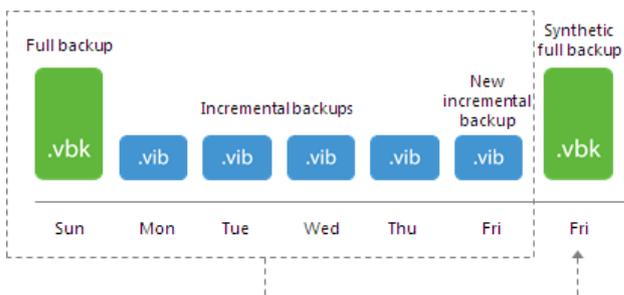
To create a synthetic full backup, Veeam Backup & Replication performs the following steps:

1. On a day when synthetic full backup is scheduled, Veeam Backup & Replication triggers a new backup job session. During this session, Veeam Backup & Replication first performs incremental backup in a regular manner and adds a new incremental backup file to the backup chain.

Veeam Backup & Replication retrieves VM data for this incremental backup file from the production storage. Incremental backup helps Veeam Backup & Replication ensure that the synthetic full backup includes the latest changes of the source VM in the production environment.



2. At the end of the backup job session, the Veeam Data Mover on the backup repository builds a new synthetic full backup using backup files that are already available in the backup chain, including the newly created incremental backup file.



3. When the synthetic full backup is created, the Veeam Data Mover on the backup repository deletes the incremental backup file created at the beginning of the job session. As a result, you have a backup chain that consists of a full backup file, set of incremental backup files and synthetic full backup file.



4. Every next job session creates a new incremental restore point starting from the synthetic full backup until the day on which synthetic full backup is scheduled. On this day, Veeam Backup & Replication creates a new synthetic full backup.

Synthetic Full Backup Schedule

Veeam Backup & Replication automatically triggers a backup job session to create a synthetic full backup, even if a regular backup job session is not scheduled on this day. The job session is started at the same time when the parent backup job is scheduled. For example, if you schedule the parent backup job at 12:00 AM Sunday through Friday, and schedule synthetic full backup on Saturday, Veeam Backup & Replication will start a backup job session that will produce a synthetic full backup at 12:00 AM on Saturday.

If a regular backup job is scheduled together with a synthetic full backup, Veeam Backup & Replication will produce only one backup file – a synthetic full backup that will contain the latest state of the source VM. An incremental backup file that should have been created by the backup job schedule will not be added to the backup chain.

Veeam Backup & Replication creates a synthetic full backup only once a day on which synthetic full backup is scheduled. If you run the backup job again on the same day, Veeam Backup & Replication will perform incremental backup in a regular manner.

Backup Chain Transform

If you select to create synthetic full backups, you can additionally choose to transform a previous forward incremental backup chain into a reverse incremental backup chain. Veeam Backup & Replication will transform the latest backup chain consisting of the full (VBK) and incremental (VIB) backup files into reverse incremental backup files (VRB).

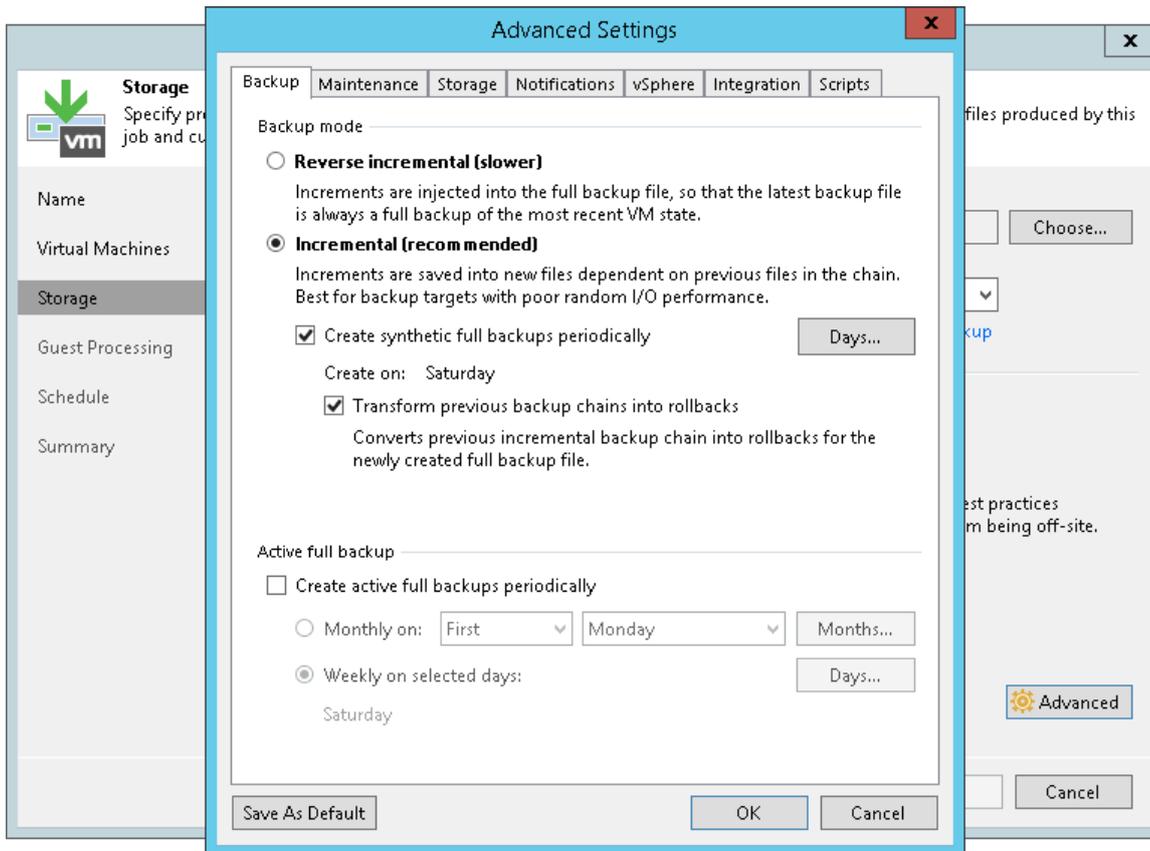
The transform option lets you reduce the amount of space required to store backups. Instead of two full backup files – a regular full backup and synthetic full backup – you will have only one synthetic full backup file on disk. Note, however, that the transform operation takes more time than creating a periodic synthetic full backup.

Veeam Backup & Replication always transforms the latest forward incremental backup chain (chain that consists of a full backup file and subsequent forward incremental backup files). For example, you have a backup chain that consists of one full backup file and set of incremental backup files. In the middle of the chain, you create an active full backup. When Veeam Backup & Replication runs the transform operation, Veeam Backup & Replication transforms the most recent active full backup file plus incremental backup files that follow it. All backup files that precede the active full backup file stay intact.

NOTE:

The transform operation is accounted for as a backup repository task. Make sure you properly plan use of backup repository resources when you schedule backup jobs.

To transform the backup chain, you must enable the **Transform previous backup chains into rollbacks** option in the backup job settings.

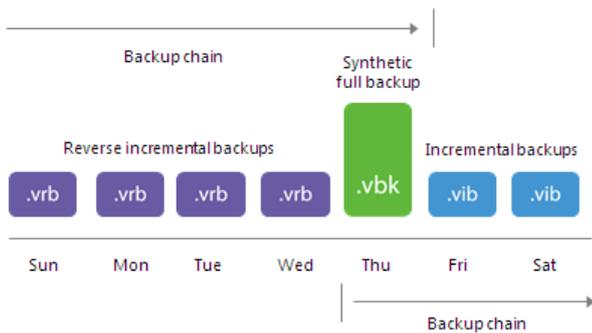


How Backup Chain Transform Works

For example, you have configured a backup job to perform daily forward incremental backups and scheduled synthetic full backups on Thursday. Additionally, you have selected to transform the incremental backup chain into the reverse incremental backup chain. The backup job starts on Sunday. In this case, Veeam Backup & Replication performs backup in the following way:

1. On Sunday, Veeam Backup & Replication creates a full backup file.
2. Monday through Wednesday, Veeam Backup & Replication creates increments and adds them to the backup chain.
3. On Thursday, Veeam Backup & Replication creates a new increment and then transforms the backup chain in the following way:
 - a. Veeam Backup & Replication injects the Monday increment into the Sunday full backup. Modified blocks are pulled out and saved as a reverse incremental file. As a result, you have Monday full backup and Sunday reverse increment.
 - b. Veeam Backup & Replication repeats the process for Tuesday, Wednesday and Thursday increments. As a result, you have the synthetic full backup created on Thursday and a set of reverse increments for Sunday through Wednesday.

- When you run the backup job next time, Veeam Backup & Replication adds a new increment to the backup chain. The synthetic full backup will be used as a starting point.



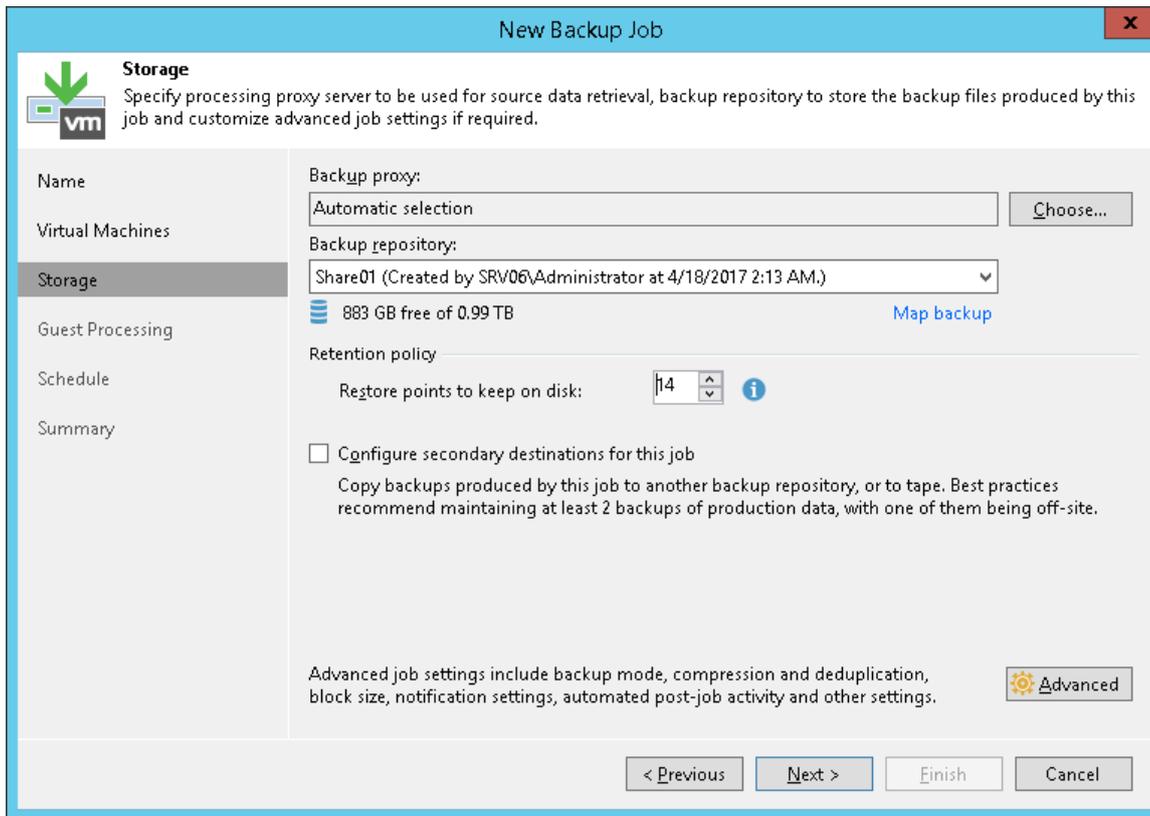
Retention Policy for Mixed Backup Chains

To maintain the necessary number of restore points in mixed backup chains (backup chains that contain reverse incremental and forward incremental backup files), Veeam Backup & Replication deletes an outdated reverse incremental backup file when the job adds a new forward incremental backup file to the chain.

Retention Policy

Every successful backup job session creates a new restore point that lets you roll back VM data to an earlier point in time. To control the number of restore points in the backup chain, you must specify retention policy settings. The retention policy defines how many restore points you want to retain on disk and thus how 'far' you are able to roll back. After the allowed number of restore points is exceeded, Veeam Backup & Replication automatically removes the earliest restore point from the backup chain.

To define the retention policy for a backup job, you must specify the necessary number of restore points in the **Restore points to keep on disk** field in the backup job settings. By default, Veeam Backup & Replication keeps 14 restore points on disk.



Veeam Backup & Replication handles restore points in different ways for forever forward incremental, forward incremental and reverse incremental backup chains:

- [Forever Forward Incremental Backup Retention Policy](#)
- [Retention for Forward Incremental Backup](#)
- [Retention for Reverse Incremental Backup](#)

NOTE:

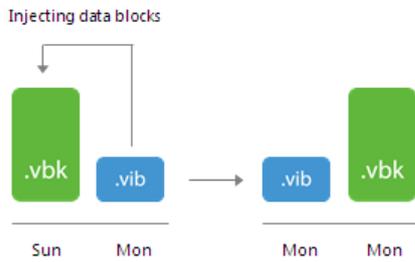
When the allowed number of restore points in the backup chain is exceeded, Veeam Backup & Replication deletes the whole backup file, not separate VMs from it. For more information, see [Removing Restore Points from the Backup Chain](#).

Forever Forward Incremental Backup Retention Policy

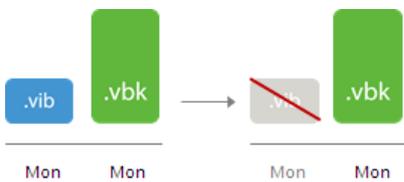
If the number of restore points in forever forward incremental backup chains exceeds retention policy settings, Veeam Backup & Replication transforms the backup chain to make room for the most recent restore point. The transformation process is performed in the following way:

1. Veeam Backup & Replication adds a new incremental backup file to the backup chain and detects that the number of allowed restore points is exceeded.

2. Veeam Backup & Replication re-builds the full backup file to include changes of the incremental backup file following the full backup. To do this, Veeam Backup & Replication injects data blocks from the first incremental backup file in the chain into the full backup file. As a result, the full backup file 'moves' one step forward in the backup chain.

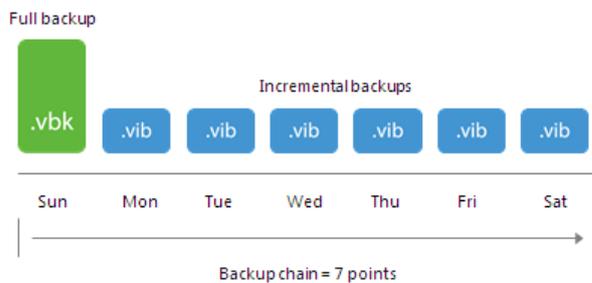


3. The first incremental backup file is removed from the backup chain as redundant. Its data has already been injected into the full backup file, and the full backup file contains the same data as this incremental backup file.



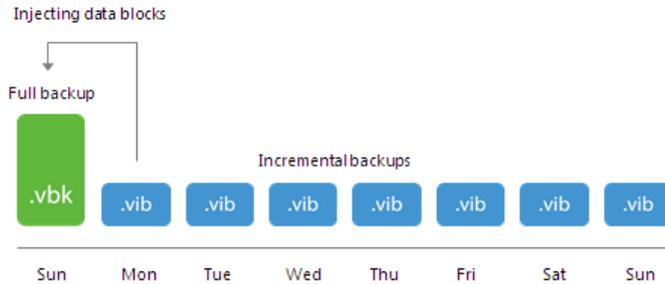
For example, you want to keep 7 restore points in the backup chain. The backup job starts on Sunday and runs daily. In this case, Veeam Backup & Replication will create the backup chain in the following way:

1. During the first backup job session on Sunday, Veeam Backup & Replication creates the first restore point – a full backup file.
2. Monday through Saturday Veeam Backup & Replication adds six incremental backup files to the backup chain.

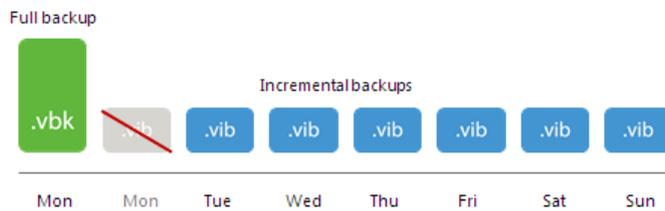


3. The next Sunday, Veeam Backup & Replication adds a new incremental backup file to the backup chain.

4. Veeam Backup & Replication detects that the number of allowed restore points is exceeded, and starts the transform process:
 - a. Veeam Backup & Replication merges data blocks from the incremental backup file created on Monday into the full backup file created on Sunday. This way, the full backup file 'moves' one step forward – from Sunday to Monday.



- b. The incremental backup created on Monday becomes redundant and is removed from the backup chain.



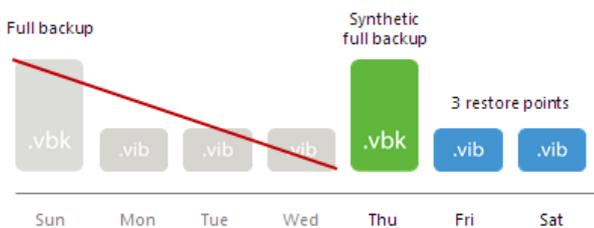
As a result, you have a chain of a full backup file as of Monday and six incremental backup files Tuesday through Sunday.

Forward Incremental Backup Retention Policy

To be able to restore from a forward incremental backup, you need to have a full backup file and a chain of subsequent incremental backup files on disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental backup file before the point to which you want to roll back, you won't be able to restore VM data (since later incremental backup files depend on earlier incremental backup files).

For this reason, if you select forward incremental backup method, in some days there will be more restore points on disk than specified by retention policy settings. Veeam Backup & Replication will remove the full backup chain only after the last incremental backup file in the chain becomes outdated.

For example, the retention policy is set to 3 restore points. A full backup file is created on Sunday, incremental backup files are created Monday through Saturday, and a synthetic full backup is scheduled on Thursday. Although the retention policy is already breached on Wednesday, the full backup is not deleted. Without the full backup, backup chain would be useless, leaving you without any restore point at all. Veeam Backup & Replication will wait for the next full backup file and 2 incremental backup files to be created, and only then will delete the whole previous chain, which will happen on Saturday.



Reverse Incremental Backup Retention Policy

In case of reverse incremental backup, Veeam Backup & Replication immediately deletes the earliest reverse incremental backup file as soon as it becomes outdated.

For example, you configure a backup job in the following way:

- The backup job starts on Sunday.
- The backup method is reverse incremental.
- Retention policy is set to 6 restore points.

Veeam Backup & Replication will start the backup job on Sunday. Monday through Friday, it will add new restore points to the backup chain and rebuild the full backup file. On Saturday, Veeam Backup & Replication will add a new restore point and remove the earliest reverse incremental backup file (VRB) from the backup chain.



Retention Policy for Deleted Items

In some situations, after you configure and run backup jobs in Veeam Backup & Replication, you may want to change something in the virtual infrastructure or in the backup strategy. For example, you may remove some machines from the virtual infrastructure or move them to another location. You may also exclude some machines from jobs that have already run for some time.

Retention policy for deleted items functions differently depending on the per-VM backup file option. For details, see [Per-VM Backup Files](#).

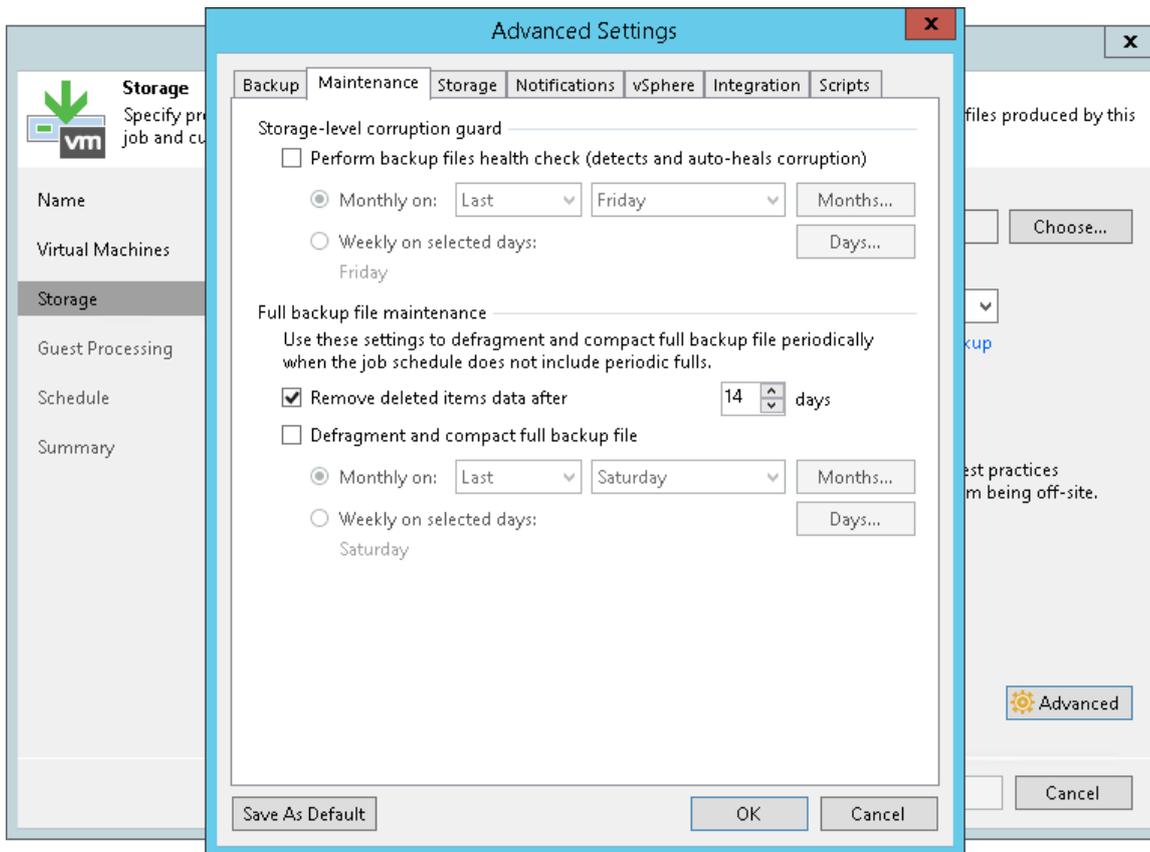
- [If per-VM is enabled] When you enable retention policy for deleted items, Veeam Backup & Replication will remove data for machines that are no longer processed by the backup job from the backup repository.
- [If per-VM is disabled] When you enable retention policy for deleted items, Veeam Backup & Replication will remove the data about deleted items from the backup job and Veeam Backup & Replication database. The stored blocks of deleted machines will remain on the repository. The stored blocks of deleted machines will be removed only when the restore point retention limit is reached or by the compact full backup file option.

Retention policy for deleted items data is set at the level of the backup job. You must enable the **Remove deleted items data after** option in backup job settings and specify the period of time for which data for deleted items must be retained on the backup repository.

Mind the following:

- You must use retention policy for deleted items data carefully. It is strongly recommended that you set the retention policy to 3 days or more to prevent unwanted data loss.

- The **Remove deleted items data after** option lets you control data of deleted or excluded items. In addition to it, Veeam Backup & Replication applies general retention policy rules to maintain the necessary number of restore points in the backup chain. For more information, see [Retention Policy](#).



How Retention Policy for Deleted Items Works

If you enable retention policy for deleted items data in backup job settings, Veeam Backup & Replication performs the following actions:

1. If all machines in the job are processed with the *Success* status, at the end of the backup job session Veeam Backup & Replication gets a list of machines in the backup.
2. For every machine in the backup, Veeam Backup & Replication checks the configuration database and gets the date of the latest backup job session completed with the *Success* status.
3. Veeam Backup & Replication checks if any machine in the backup meets the following conditions:
 - There are no successful backups for the machine for the last N days.
 - There are no corrupted backups for the machine for the last N days.

Where N is the number of days specified in the **Remove deleted items data after N days** setting.

4. If both conditions are true for some machine, Veeam Backup & Replication removes data for this machine from the backup. Note that if per-VM is disabled, it does not free up space on the backup repository. It marks the space as available to be overwritten, and this space is removed during subsequent job sessions or the full backup file compact operation.

Example 1

You create a backup job for 2 VMs and set the retention policy for deleted items to 5 days. The backup job runs once a day for 7 times and processes VMs in the following way:

- VM 1 is successfully processed during all job sessions.
- VM 2 is successfully processed during the 1st and 2nd backup job sessions. Before the 3rd job session, VM 2 is excluded from the job and is not processed by subsequent job sessions.

During the 8th job session, Veeam Backup & Replication will remove data for VM 2 from backups on the backup repository since there are no successful and corrupted backups for VM 2 for the last 5 days.



Example 2

You create a backup job for 2 machines and set the retention policy for deleted machines to 5 days. The backup job runs once a day for 7 times and processes machines in the following way:

- VM 1 is successfully processed during all job sessions.
- VM 2 is successfully processed during the 1st and 2nd backup job sessions. Starting from the 3rd job session, VM 2 fails to be processed, for example, due power loss while machine data is transported.

During the 8th job session, Veeam Backup & Replication will not remove data for VM 2 from backups on the backup repository. Even though there are no successfully created backups for VM 2 for the last 5 days, Veeam Backup & Replication will detect that the configuration database contains information about corrupted backups for VM 2 for the last 5 days.



Limitations for Retention Policy for Deleted Items

- [Per-VM is disabled] Retention policy for deleted items does not function if you enable [synthetic full backups](#) and/or [active full backup](#).
[Per-VM is enabled] Retention policy for deleted items functions without limitations.
- [For vCD backup jobs] To apply retention policy for deleted items, Veeam Backup & Replication checks backups created for the vApp itself, not for a machine in this vApp. Thus, the retention policy is applied only if the job stops creating backups for the entire vApp.

Removal of Restore Points

To keep up with the retention policy, Veeam Backup & Replication deletes the whole backup file from the backup chain, not data for separate VMs from the backup file. In some situations a certain VM may have fewer restore points than it is specified in retention policy settings. This can happen if a backup job processes a number of VMs or VM containers, and some VMs or VM containers fail to be processed during some job sessions.

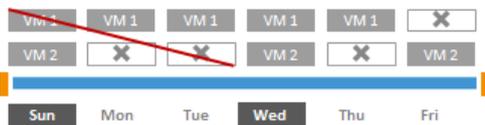
Removal of Restore Points from Forward Incremental Chains

In case of a forward incremental backup chain, Veeam Backup & Replication does not remove a restore point immediately. Instead, Veeam Backup & Replication waits for a new full backup (synthetic or active) to be created and a new backup chain to be started. As soon as the last incremental restore point in the "old" backup chain is marked as redundant, Veeam Backup & Replication removes the whole "old" backup chain from the backup repository. For more information, see [Retention for Incremental Backup](#).

For example, a backup job processes 2 VMs: *VM 1* and *VM 2*. According to the retention policy settings, the backup chain must contain 3 restore points. The backup job has already had 5 job sessions and VMs have been processed in the following way:

- *VM 1* has been successfully backed up 3 times and has 3 restore points
- *VM 2* has failed to be processed in 2 job sessions and has 1 valid restore point

When Veeam Backup & Replication adds a new restore point to the backup chain, it will not remove the earliest restore point. Veeam Backup & Replication will wait until a new full backup file and 2 incremental backup files are added to the backup chain. After that, it will remove the whole outdated backup chain from the backup repository. Restore points in the new backup chain, at the same time, may contain data for both VMs or for one VM only: Veeam Backup & Replication regards backup files as restore points, not separate VMs in these files.

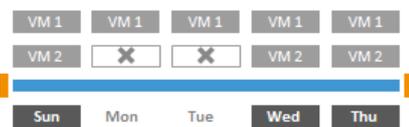


Removal of Restore Points from Reverse Incremental Chains

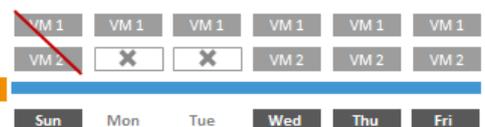
In case of a reverse incremental backup chain, Veeam Backup & Replication immediately deletes a redundant restore point when the allowed number of restore points is exceeded. For more information, see [Retention for Reverse Incremental Backup](#).

For example, a backup job processes two VMs: *VM 1* and *VM 2*. According to the retention policy settings, the backup chain must contain 5 restore points. The backup job has already had 5 job sessions and VMs have been processed in the following way:

- *VM 1* has been successfully backed up 5 times and has 5 valid restore points
- *VM 2* has failed to be processed in 2 job sessions and has 3 valid restore points

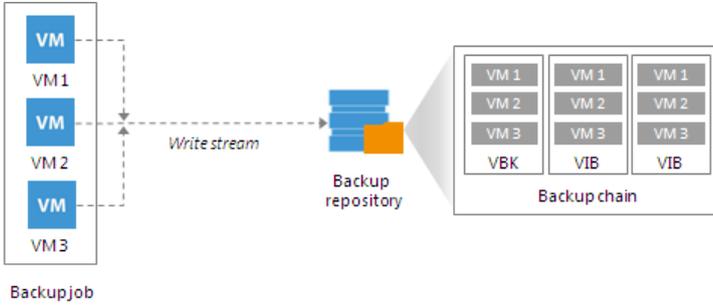


After that, Veeam Backup & Replication runs a new backup job session in which *VM 1* and *VM 2* are successfully processed. When a new restore point is added to the chain, Veeam Backup & Replication removes the earliest restore point because the number of restore points in the backup chain has exceeded 5. As a result, you will have 5 restore points for *VM 1* and 3 restore points for *VM 2*.

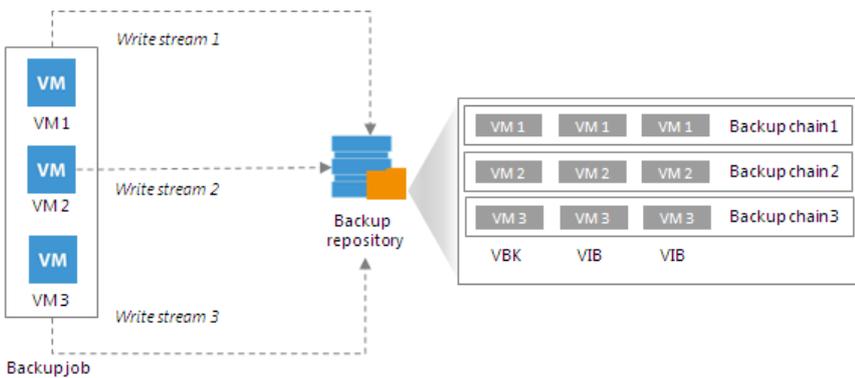


Per-VM Backup Files

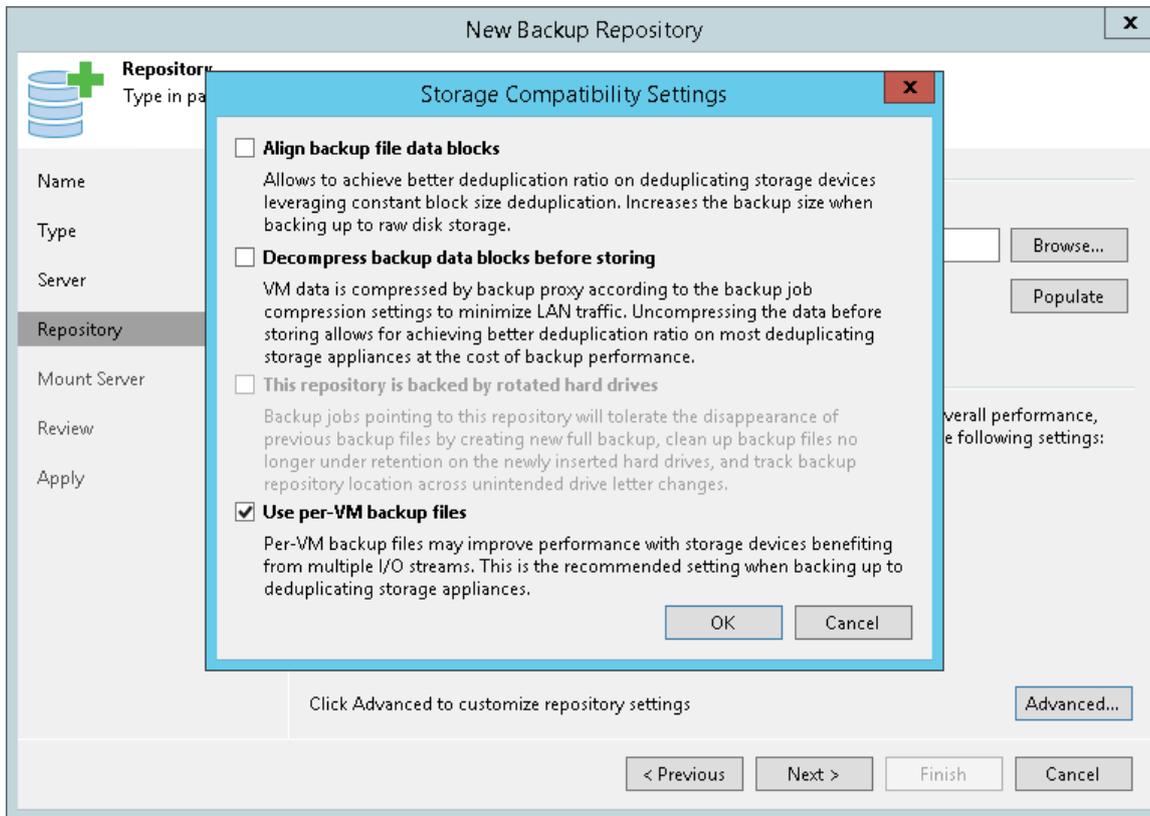
By default, backup jobs write VM data to the backup repository in one write stream, and store data of all VMs to the same backup file. Such behavior can be non-optimal if the target storage device is able to write data in multiple streams simultaneously. In this situation, the backup repository may become the bottleneck for the data transfer, even though its resources will not be fully utilized.



You can instruct Veeam Backup & Replication to create per-VM backup files on the backup repository. In this case, the backup job will use a separate write stream for every VM in the job, and store data of every VM to a separate backup file. Resources of the storage device will be used more efficiently, and the job performance may increase.



To create per-VM backup files, you must enable the **Use per-VM backup files** option at the level of the backup repository. It is recommended that you enable this option for deduplicating storage appliances that support multiple write streams. The option is also enabled for scale-out backup repositories by default.



It is recommended that you balance the number of tasks on backup proxies and backup repository to avoid the situation when some backup infrastructure resources remain idle while others are overloaded.

NOTE:

It is not recommended that you disable the **Limit maximum concurrent tasks to N** option for backup repositories with per-VM backup chains. In case of per-VM backup chains, synthetic operations (synthetic full backup, backup files merge and transform) work in parallel for every VM in the backup. The number of parallel operations is limited by the number of concurrent tasks that can be performed on the backup repository. If you disable the **Limit maximum concurrent tasks to N** option (which results in using an unlimited number of slots), the load on the backup repository may be high.

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location
Path to folder: C:\Backups

Capacity: **1023.7 GB**
Free space: **615.2 GB**

Load control
Running too many concurrent tasks against the same repository may reduce overall performance, and cause I/O operations to timeout. Control storage device saturation with the following settings:

Limit maximum concurrent tasks to:

Limit read and write data rates to: MB/s

Click Advanced to customize repository settings

< Previous Next > Finish Cancel

Limitations for Per-VM Backup Files

- The **Use per-VM backup files** option cannot be enabled for backup repositories with rotated drives.
- If you enable the **Use per-VM backup files** option, data deduplication between VMs will not work. For more information, see [Data Compression and Deduplication](#).
- The Per-VM backup chains functionality is available in Veeam Backup & Replication Enterprise Edition and higher. If you configure backup repositories to produce per-VM backup chains and then install a license that does not support this functionality, you must manually disable the **Use per-VM backup files** option for backup repositories. Otherwise backup jobs targeted at these backup repositories will be failing.

Per-VM Backup Files Option for Existing Backup Repositories

You can enable or disable the **Use per-VM backup files** option for existing backup repositories at which backup jobs are already targeted. The new setting will not have any effect on previously created backup files on the backup repository. It will affect new backup files created after the setting is changed.

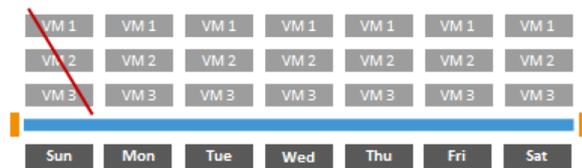
Veeam Backup & Replication applies the new setting starting from the next active full backup. You can create an active full backup manually or wait for Veeam Backup & Replication to automatically create active full backup (if active full backups are scheduled). Synthetic full backups do not affect the **Use per-VM backup files** setting.

Retention for Per-VM Backup Files

If you enable the **Use per-VM backup files** option for the backup repository, Veeam Backup & Replication creates a separate backup chain for every VM added to the job. Backup files are stored together in the folder of the backup job on the backup repository. The job produces one metadata file. This file stores information about all created backup files and backup chains.

Veeam Backup & Replication regards all backup files that are created during one backup job session as one restore point. When Veeam Backup & Replication needs to remove earlier restore points by retention policy, it removes backup files for all VMs that were created during one job session.

For example, you have added 3 VMs to the job, set the retention setting to 5 restore points and run the job 5 times. The job will produce 15 backup files, 5 per each VM in the job. On the 6th job session, the job will remove from the backup chain 3 backup files – the earliest restore points for every VM.



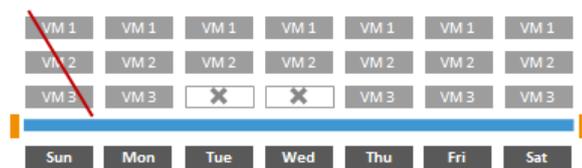
If the job backs up some VMs during the job session and does not manage to back up others, Veeam Backup & Replication will still regard that the restore point is valid. When the earliest restore point gets outdated, Veeam Backup & Replication will remove backup files for all VMs at once, even though backup chains for some VMs may contain fewer backup files than you expect.

The rules of restore points deletion for regular backup chains also apply to per-VM backup chains. For more information, see [Removing Restore Points from the Backup Chain](#).

For example, you have added 3 VMs to the job and set retention policy to 5. The backup job session ran in the following way:

1. During the first three job sessions, Veeam Backup & Replication backed up all VMs.
2. During the 4th and 5th job sessions, *VM 1* and *VM 2* were successfully backed up, and *VM 3* failed.

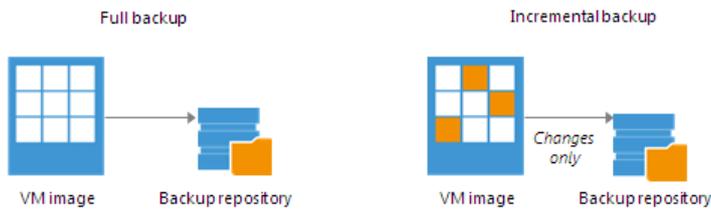
During the 6th job session, Veeam Backup & Replication will delete the earliest restore point for all VMs. As a result, the *VM 1* and *VM 2* will have 5 restore points and *VM 3* will have 3 restore points.



Changed Block Tracking

To perform incremental backup, Veeam Backup & Replication needs to know what data blocks have changed since the previous job session.

For VMware VMs with hardware version 7 and later, Veeam Backup & Replication employs a native VMware vSphere feature – VMware vSphere Changed Block Tracking (CBT). Instead of scanning VMFS, Veeam Backup & Replication queries CBT through VADP and gets the list of blocks that have changed since the last job session. Use of CBT increases the speed and efficiency of block-level incremental backups.



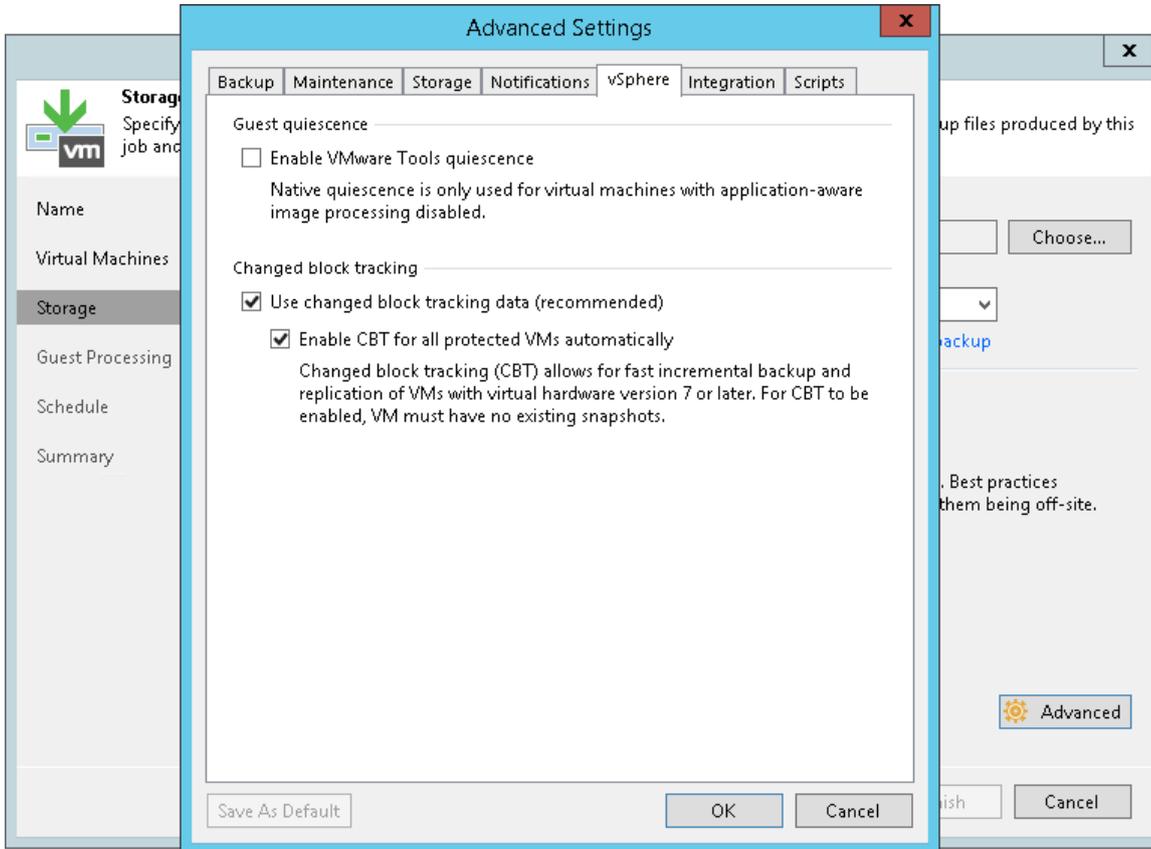
Veeam Backup & Replication uses CBT for the following operations:

- Backup
- Replication
- Entire VM restore
- VM disk restore

Veeam Backup & Replication enables CBT by default. If necessary, you can disable it in job settings.

NOTE:

CBT is disabled if you back up proxies that use Virtual appliance (HotAdd) mode to process VM data.



NOTE:

For VMs with virtual disks in thin format, Veeam Backup & Replication also uses CBT during active full backup sessions to detect unallocated regions of virtual disks and skip them.

In some situations, Veeam Backup & Replication cannot leverage VMware vSphere CBT, for example, if VMs run an earlier version of virtual hardware or CBT is disabled at the ESX host level. If Veeam Backup & Replication cannot leverage VMware vSphere CBT, it fails over to Veeam's proprietary filtering mechanism. Instead of tracking changed blocks of data, Veeam Backup & Replication filters out unchanged data blocks.

During VM processing, Veeam Backup & Replication consolidates virtual disk content, scans through the VM image and calculates a checksum for every data block. Checksums are stored as metadata to backup files next to VM data. When incremental backup is run, Veeam Backup & Replication opens all backup files in the chain of previous full and incremental backups, reads metadata from these files and compares it with checksums calculated for a VM in its current state. If a match is found (which means the block already exists in the backup), the corresponding block is filtered out.

Data Compression and Deduplication

Veeam Backup & Replication provides mechanisms of data compression and deduplication. Data compression and deduplication let you decrease traffic going over the network and disk space required for storing backup files and VM replicas.

Data Compression

Data compression decreases the size of created backups but affects duration of the backup procedure. Veeam Backup & Replication allows you to select one of the following compression levels:

- **None** compression level is recommended if you plan to store backup files and VM replica files on storage devices that support hardware compression and deduplication.
- **Dedupe-friendly** is an optimized compression level for very low CPU usage. You can select this compression level if you want to decrease the load on the backup proxy.
- **Optimal** is the recommended compression level. It provides the best ratio between size of the backup file and time of the backup procedure.
- **High** compression level provides additional 10% compression ratio over the **Optimal** level at the cost of about 10x higher CPU usage.
- **Extreme** compression provides the smallest size of the backup file but reduces the backup 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 level.

Changing Data Compression Settings

You can change data compression settings for existing backup jobs. New settings will not have any effect on previously created backup files in the backup chain. They will be applied to new backup files created after the settings were changed.

Compression settings are changed on the fly. You do not need to create a new full backup to use new settings – Veeam Backup & Replication will automatically apply the new compression level to newly created backup files.

However, if you use the reverse incremental backup method, the newly created backup files will contain a mixture of data blocks compressed at different levels. For example, you have a backup job that uses the reverse incremental backup method and the Optimal level of compression. After several job sessions, you change the compression level to High. In the reverse incremental backup chains, the full backup file is rebuilt with every job session to include new data blocks. As a result, the full backup file will contain a mixture of data blocks: data blocks compressed at the Optimal level and data blocks compressed at the High level. The same behaviour applies to synthetic full backups: synthetic full backups created after the compression level change will contain a mixture of data blocks compressed at different levels.

If you want the newly created backup file to contain data blocks compressed at one level, you can create an active full backup. Veeam Backup & Replication will retrieve data for the whole VM image from the production infrastructure and compress it at the new compression level. All subsequent backup files in the backup chain will also use the new compression level.

Deduplication

Data deduplication decreases the size of backup files. You can enable data deduplication if you add to backup or replication jobs several VMs that have a great amount of free space on their logical disks or VMs that have similar data blocks – for example, VMs that were created from the same template. With data deduplication enabled, Veeam Backup & Replication does not store to the resulting backup file identical data blocks and space that has been pre-allocated but not used.

Veeam Backup & Replication uses Veeam Data Movers to deduplicate VM data on the source and target side.

- The source-side Veeam Data Mover deduplicates VM data at the level of VM disks. Before the source Veeam Data Mover starts processing a VM disk, it obtains digests for the previous restore point in the backup chain from the target-side Veeam Data Mover. The source-side Veeam Data Mover consolidates this information with CBT information from the hypervisor and filters VM disk data based on it. If some data block exists in the previous restore point for this VM, the source-side Veeam Data Mover does not transport this data block to the target. In addition to it, in case of thin disks the source-side Veeam Data Mover skips unallocated space.
- The target-side Veeam Data Mover deduplicates VM data at the level of the backup file. It processes data for all VM disks of all VMs in the job. The target-side Veeam Data Mover uses digests to detect identical data blocks in transported data, and stores only unique data blocks to the resulting backup file.

You can change the inline data deduplication settings for existing backup jobs. New changes will not have any effect on previously created backup files in the backup chain. They will be applied to new backup files created after the settings were changed.

Inline Data Deduplication setting can be changed on the fly. You do not need to create a new full backup to enable/disable this setting. Veeam Backup & Replication will automatically apply the change to newly created backup files.

Storage Optimization

Depending on the type of storage you select as a backup target, Veeam Backup & Replication uses data blocks of different size to process VMs, which optimizes the size of a backup file and job performance. You can choose one of the following storage optimization options:

- The **Local target (large blocks)** option is recommended for backup jobs that can produce very large full backup files – larger than 16 TB. With this option selected, Veeam Backup & Replication uses data block size of 4096 KB.

If you select to use data blocks of small size to deduplicate a large backup file, the backup file will be cut into a great number of data blocks. As a result, Veeam Backup & Replication will produce a very large deduplication metadata table which can potentially overgrow memory and CPU resources of your backup repository. For backup files over 16 TB, it is recommended to choose the **Local target (large blocks)** option. With this option selected, Veeam Backup & Replication will use data blocks of 4 MB. Large data blocks produce a smaller metadata table that requires less memory and CPU resources to process. Note, however, that this storage optimization option will provide the lowest deduplication ratio and the largest size of incremental backup files.

NOTE:

If you upgrade to Veeam Backup & Replication 9.0 from the previous product version, this option will be displayed as **Local target (legacy 8MB block size)** in the list and will still use blocks size of 8 MB. It is recommended that you switch to an option that uses a smaller block size and create an active full backup to apply the new setting.

- The **Local target** option is recommended for backup to SAN, DAS or local storage. With this option selected, Veeam Backup & Replication uses data block size of 1024 KB.

The SAN identifies larger blocks of data and therefore can process large amounts of data at a time. This option provides the fastest backup job performance but reduces the deduplication ratio, because with larger data blocks it is less likely to find identical blocks.

- The **LAN target** option is recommended for backup to NAS and onsite backup. With this option selected, Veeam Backup & Replication uses data block size of 512 KB. This option provides a better deduplication ratio and reduces the size of a backup file because of reduced data block sizes.
- The **WAN target** option is recommended if you are planning to use WAN for offsite backup. With this option selected, Veeam Backup & Replication uses data block size of 256 KB. This results in the maximum deduplication ratio and the smallest size of backup files, allowing you to reduce the amount of traffic over WAN.

Changing Storage Optimization Settings

You can change storage optimization settings for existing backup jobs. New settings will not have any effect on previously created backup files in the backup chain. They will be applied to new backup files created after the settings were changed.

Backup Jobs

To apply new storage optimization settings in backup jobs, you must create an active full backup after you change storage optimization settings. Veeam Backup & Replication will use the new block size for the active full backup and subsequent backup files in the backup chain.

Backup Copy Jobs

To change data block size for a backup copy job, you must perform the following actions:

1. Change data block size in settings of the initial backup job.
2. Create an active full backup with the initial backup job.
3. Create an active full backup with the backup copy job.

Data Exclusion

When you configure a backup or replication job, you can define what data you want to back up and replicate and exclude data that you do not need. Data exclusion helps reduce the size of the VM backup or replica and decrease the load on the network.

You can exclude data at the VM level and at the VM guest OS level.

At the VM level:

- [VMs added as part of the container](#)
- [VM disks](#)
- [VM templates](#) (only for backup)

At the VM guest OS level:

- [Swap files on the VM guest OS](#)
- [Deleted file blocks on the VM guest OS \(BitLocker\)](#)
- [Files and folders on the VM guest OS](#)

NOTE:

To reduce the size of the backup file, Veeam Backup & Replication automatically excludes VM log files from processing.

VMs and VM Disks

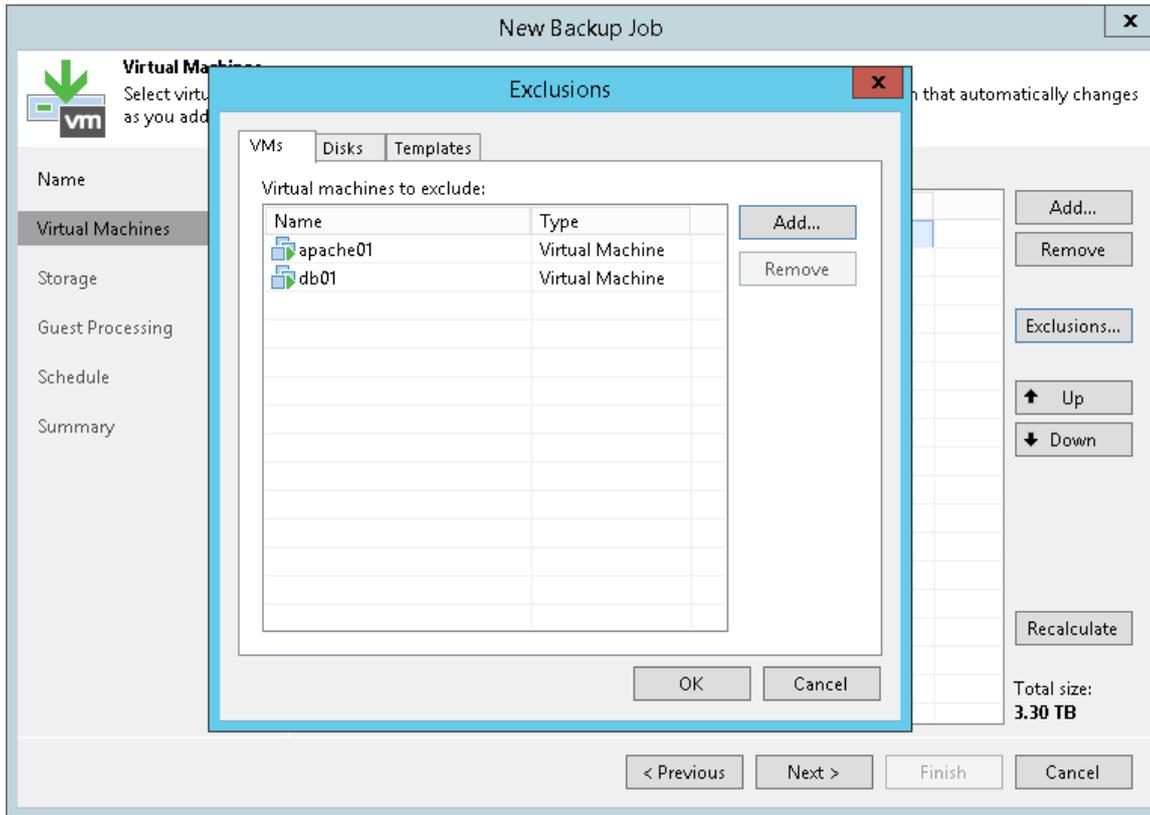
When you configure a backup or replication job, you can exclude the following objects from processing:

- [VMs added as a part of a VM container](#)
- [Individual VM disks](#)
- [For backup jobs] [VM templates](#)

VMs as Part of Container

If you want to back up or replicate a VM container that holds several VMs but want to skip some VMs, you can exclude specific VMs from the job processing. This option will help you reduce the size of the resulting backup or replica and increase the job performance.

You can define which VMs you want to skip at the **Virtual Machines** step of the backup or replication job wizard.



Individual VM Disks

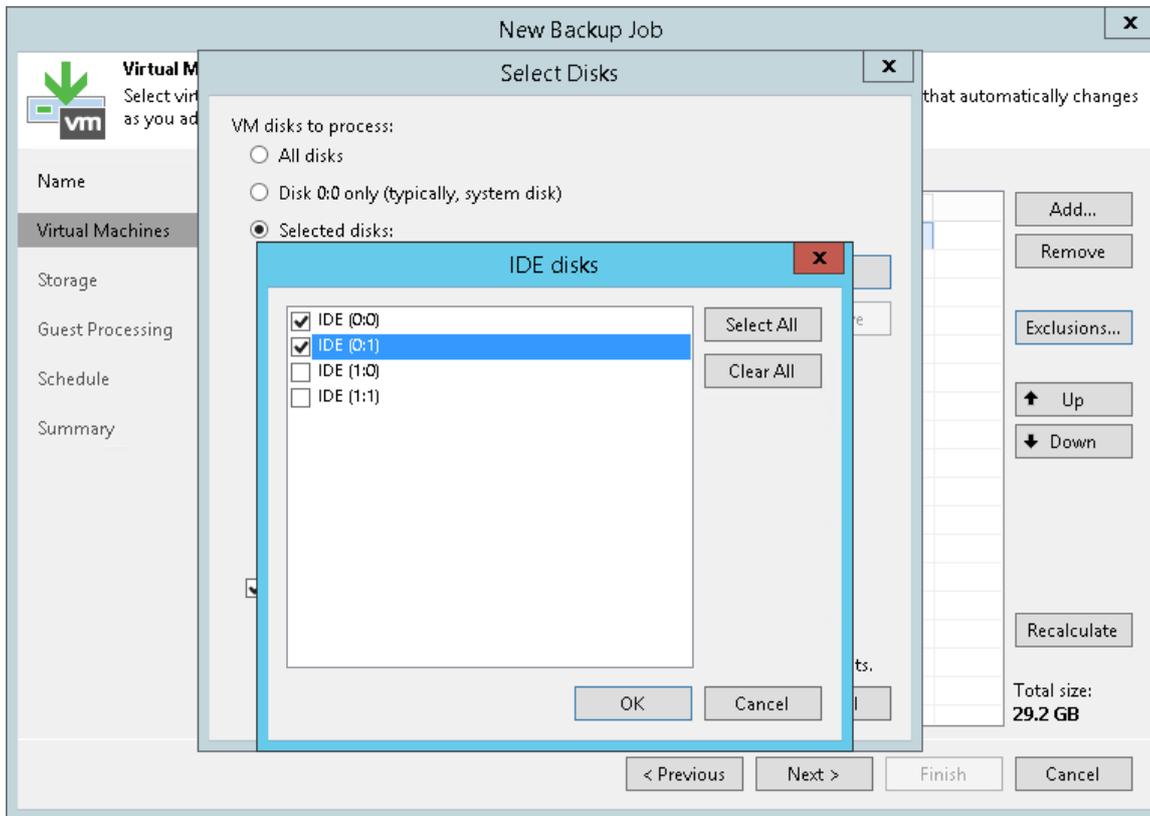
You can choose what VM disks you want to back up or replicate:

- All VM disks
- 0:0 disks (which are commonly the VM system disks)
- Specific IDE, SCSI or SATA disks

For example, you may want to back up or replicate only the system disk instead of creating a backup or replica of a full VM. VM disks exclusion reduces the size of the backup or replica.

You can define which VM disks you want to back up or replicate at the **Virtual Machines** step of the backup or replication job wizard. You can specify disk processing settings granularly for every VM in the job or for the whole VM container. In the latter case, Veeam Backup & Replication will apply the configured rule to all VMs in this container.

You can additionally instruct Veeam Backup & Replication to modify the configuration file of the VM. When you start a VM from the backup or fail over to the VM replica, you will be able to use such VM immediately. You will not have to edit its configuration file and remove excluded disks from it.

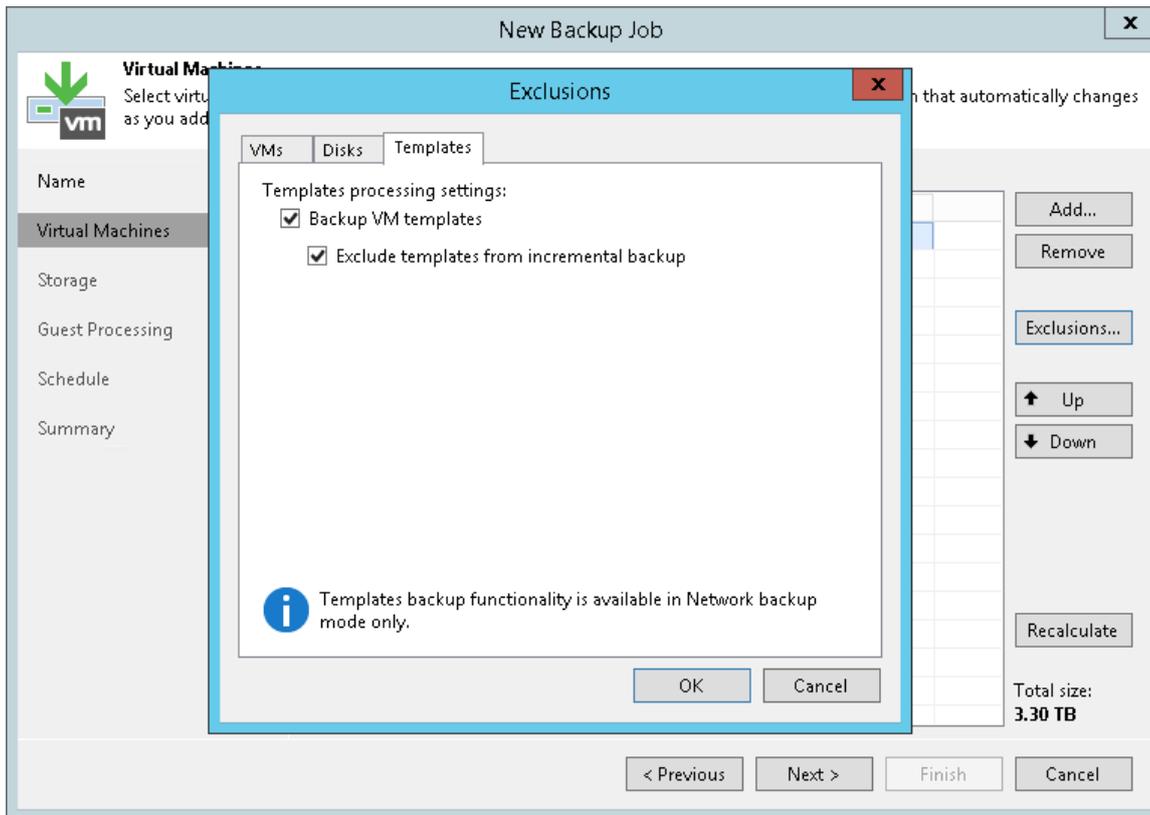


VM Templates

You can include VM templates in the backup. Backing up VM templates provides additional safety of your production environment but requires additional space on the backup repository.

Veeam Backup & Replication allows you to include a VM template only in the full backup and omit it in incremental backups. Note that Veeam Backup & Replication always uses the Network transport mode to copy VM templates data.

You can define how Veeam Backup & Replication must process VM templates at the **Virtual Machines** steps of the wizard.



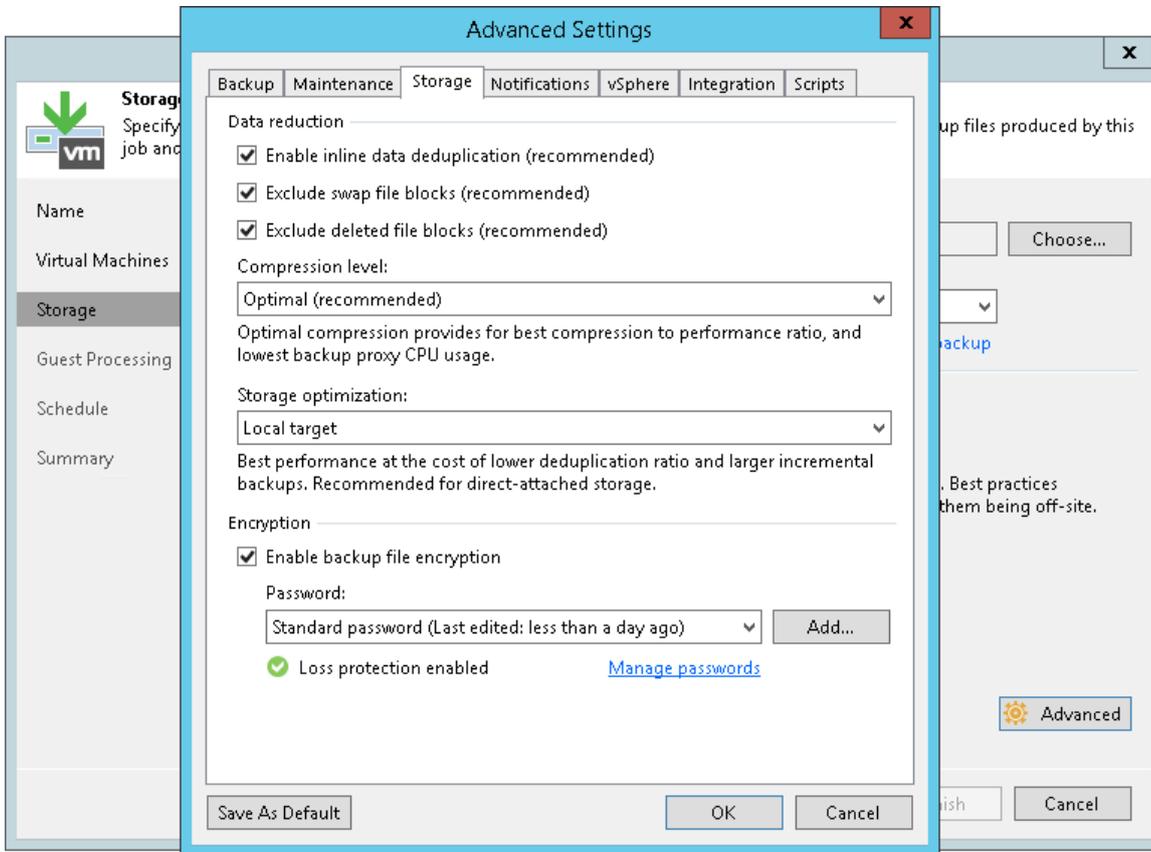
Deleted File Blocks (BitLocker)

By default, Veeam Backup & Replication does not copy "dirty" data blocks (blocks that are marked as deleted on the VM guest OS) to the target location. This option lets you reduce the size of the VM backup or replica and increase the job performance.

If you do not want to exclude deleted file blocks from backups or replicas, you can disable the **Exclude deleted file blocks** option in the backup or replication job settings.

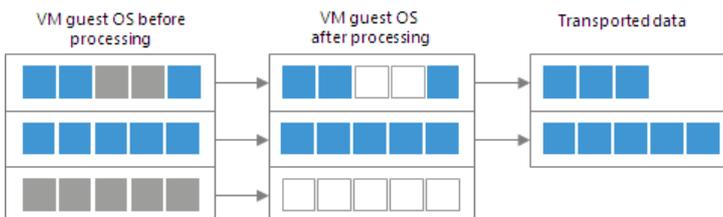
NOTE:

If you enable or disable the **Exclude deleted file blocks** setting for the existing job, Veeam Backup & Replication will apply the new setting from the next job session.



With this option enabled, Veeam Backup & Replication performs the following operations during the job session:

1. Veeam Backup & Replication accesses the MFT file on the VM guest OS to identify deleted file blocks, and zeros out these blocks.
2. Veeam Backup & Replication processes and transports data blocks of the VM image in the following manner:
 - o If a data block of the VM image contains only the deleted file blocks, Veeam Backup & Replication does not read this data block from the source datastore.
 - o If a data block of the VM image contains zeroed out blocks and other data, Veeam Backup & Replication copies this block to the target. Due to data compression, data blocks that are marked as deleted are compressed, and the size of the resulting backup or replica file reduces.



Limitations for Deleted File Blocks Exclusion

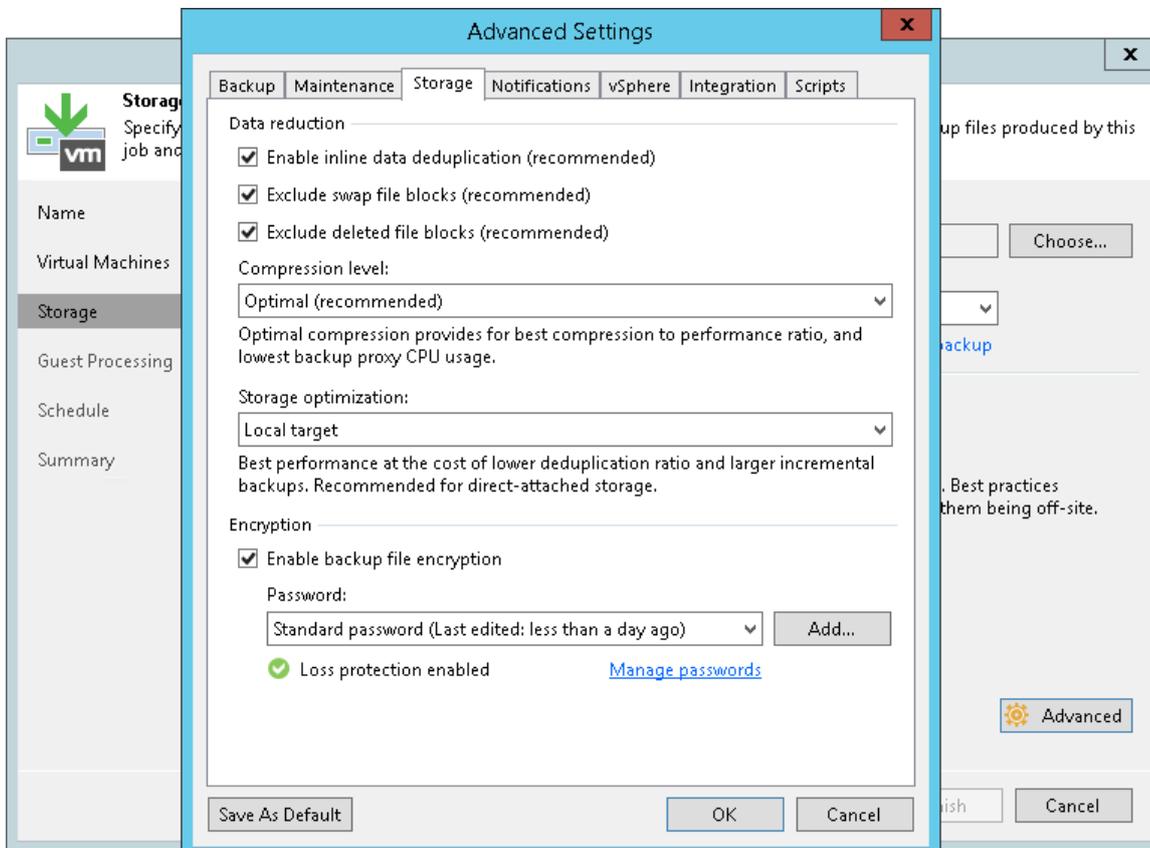
Veeam Backup & Replication can exclude deleted file blocks only on the VM guest OS with Microsoft NTFS.

Swap Files

You can instruct Veeam Backup & Replication to exclude `pagefile.sys` and `hiberfil.sys` files from backups or replicas of Microsoft Windows VMs.

- `hiberfil.sys` is a system file created by the OS for correct work of the hibernate mode.
- `pagefile.sys` is a swap file. Swap files are dynamic in nature and can change intensively between job sessions, even if a VM itself does not change much.

To exclude these files, you must enable the **Exclude swap file blocks** option in the job settings. Veeam Backup & Replication will identify data blocks of these files and exclude them from processing. As a result, the size of incremental backups and replicas will be smaller.



When you exclude `pagefile.sys` and `hiberfil.sys` files, Veeam Backup & Replication performs the following operations during the job session:

1. Veeam Backup & Replication accesses the MFT file on the VM guest OS to identify data blocks of `pagefile.sys` and `hiberfil.sys` files and zeros them out.
2. Veeam Backup & Replication processes and transports data blocks of the VM image in the following manner:
 - If a data block of the VM image contains only blocks of these files, Veeam Backup & Replication does not copy this data block to the target.

- If a data block of the VM image contains blocks of these files and other data, Veeam Backup & Replication copies this block to the target.



Limitations for Swap Files Exclusion

Veeam Backup & Replication can exclude blocks of `pagefile.sys` and `hiberfil.sys` files only on the VM guest OS with Microsoft Windows NTFS.

VM Guest OS Files

If you do not want to back up or replicate some files and folders on the VM guest OS, you can exclude them from the backup or replica. Files exclusion reduces the size of the backup or replica but may affect the job performance.

You can specify file exclusion settings granularly for every VM in the job or for the whole VM container. In the latter case, Veeam Backup & Replication will apply the configured rule to all VMs in this container.

To define which VM guest OS files must and must not be processed, you can use the following options:

- Disable file exclusion. Veeam Backup & Replication will back up or replicate the whole content of the VM guest file system.
- Exclude specific files and folders from the backup or replica. Veeam Backup & Replication will back up or replicate all files and folders except the specified ones.
- Include only specific files and folders in the backup or replica. Veeam Backup & Replication will back up or replicate only the specified files and folders.

To form a list of exclusions or inclusions, you can use the following methods:

- Specify a full path to a folder on the VM guest OS, for example, `C:\Documents\`.
- Specify a full path to a file on the VM guest OS, for example: `C:\Documents\MyReport.docx`.

If a path is not full, Veeam Backup & Replication will expand it relatively the root directory on the computer volume and attempt to detect such files on all computer volumes. For example, you have `C`, `D` and `E` disks on the VM. In the list of exclusions, you specify `Document.docx`.

Veeam Backup & Replication will scan the whole file system and exclude the following files (if any):

`C:\Document.docx`, `D:\Document.docx`, `E:\Document.docx`. If there is a

`C:\MyDocuments\Document.docx` file, it will not be excluded – this file is not located in the root directory.

- Use environmental variables, for example, `%TEMP%`, `%windir%`. Environment variables must be defined for the user account that you use to connect to the VM guest OS and under which the runtime process is started. For example, you connect to the VM guest OS under the *Administrator* account. If you want to use the `%windir%` variable in the list of exclusions or inclusions, you must make sure that the `%windir%` variable is added to the list of user variables for *Administrator* on the VM guest OS.

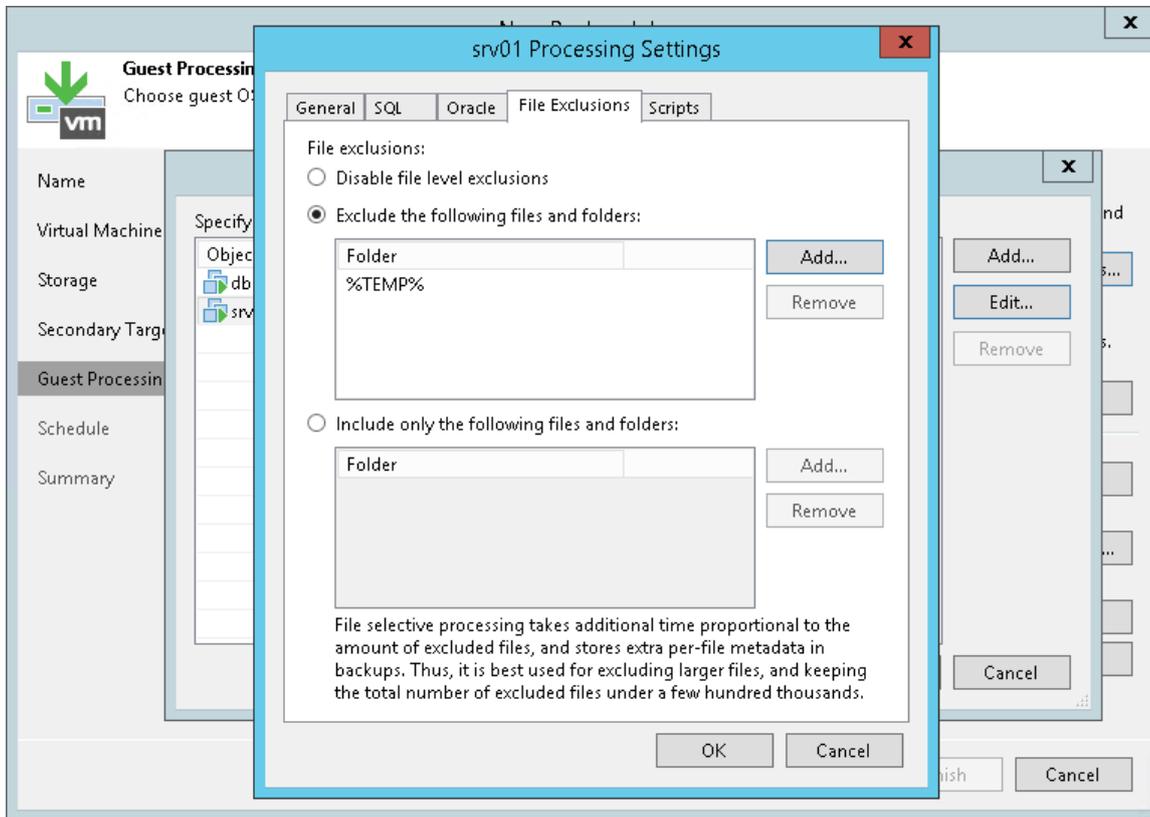
- Use file masks. You can use the following characters for masks:
 - (*) – a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, *.pdf.
 - (?) – a substitution of one character in the file name or path. For example, repor?.pdf
 - (;) – mask separator, for example, report.*;reports.*.

In the table below, `mask` stands for any sequence of characters.

Mask format	Affects paths/files
<code>*mask*</code>	All paths that contain the given sequence.
<code>mask*</code>	If the asterisk character (*) is not specified at the beginning of the mask, the mask will be applied to all volumes on the VM guest OS, and Veeam Backup & Replication will include/exclude files and folders in the root folder on the volume: A:\mask*, B:\mask*, ..., Z:\mask*.
<code><drive_letter>:*mask*</code>	All paths on the specified volume that contain the given sequence.
<code>*mask1*; *mask2*; *mask3*</code>	All paths that contain at least one of the given character sequences: <code>*mask1*</code> or <code>*mask2*</code> or <code>*mask3*</code> .

IMPORTANT!

Be careful when using masks with double wildcard characters. If you specify masks of such type, Veeam Backup & Replication will exclude all files and paths that contain the given mask. For example, if you specify the `*.doc*` mask, Veeam Backup & Replication will exclude files like `MyReport.docx`, `Report.doc.txt` and so on.



Requirements and Limitations for VM Guest Files Exclusion

VM guest OS files exclusion has the following limitations:

- File exclusion works only on Microsoft Windows NTFS.
- File exclusion is available in Enterprise and Enterprise Plus Editions of Veeam Backup & Replication. For more information, see www.veeam.com/backup-version-standard-enterprise-editions-comparison.html (File-selective image level processing).
- To exclude VM guest OS files, Veeam Backup & Replication must be able to deploy the runtime process inside the VM. For this reason, the VM must be running and accessible by an IP address, and credentials for application-aware processing must be valid.
- Veeam Backup & Replication supports both basic and dynamic disks. Volumes on the dynamic disks must not be split – spanned, striped and other types of split volumes are not supported.
- It is not recommended that you use VM guest files exclusion for Microsoft Windows Data Deduplication-Enabled Volumes. If you decide to use VM guest files exclusion for such volumes and set up a list of inclusions, you must add the System Volume Information folder to the list of inclusions.

Exclusion Rules

- If you use file masks for file exclusion, Veeam Backup & Replication will need to scan the VM guest file system, and the time of VM disk processing will increase.
- The number of entries in the list of exclusions or inclusions must not exceed a few hundreds. The number of entries in the list influences the job performance – the more files are included or excluded from the backup or replica, the more time Veeam Backup & Replication requires to process these files.
- It is recommended that you do not exclude system files without the necessity. Veeam Backup & Replication does not perform any checks to verify the VM image integrity.
- Exclusion of small files (less than 2 KB in size) is ineffective and will not reduce the size of the backup or replica significantly.

Exclusion Rules for VMs with Several Volumes

The VM guest file exclusion and inclusion functionality works at the volume level. Consider the following situations:

Data exclusion

A VM has several volumes: `C:\`, `D:\` and `E:\`. You want to exclude from the backup the `Archive` folder that is present on all volumes of the VM. If you add the `C:\Archive` folder to the list of exclusions, Veeam Backup & Replication will back up the following data:

- Whole content of the `C:\` volume except the `Archive` folder
- Whole content of `D:\` and `E:\` volumes

To exclude the `Archive` folder from all volumes of the VM, you must add a relative path to the `Archive` folder to the list of exclusions: `..\Archive\`.

Data inclusion

A VM has several volumes: `C:\`, `D:\` and `E:\`. You want to include to the backup only the `D:\Documents` folder. If you add the `D:\Documents` folder to the list of inclusions, Veeam Backup & Replication will back up the following data:

- `D:\Documents` folder
- Whole content of `C:\` and `E:\` volumes

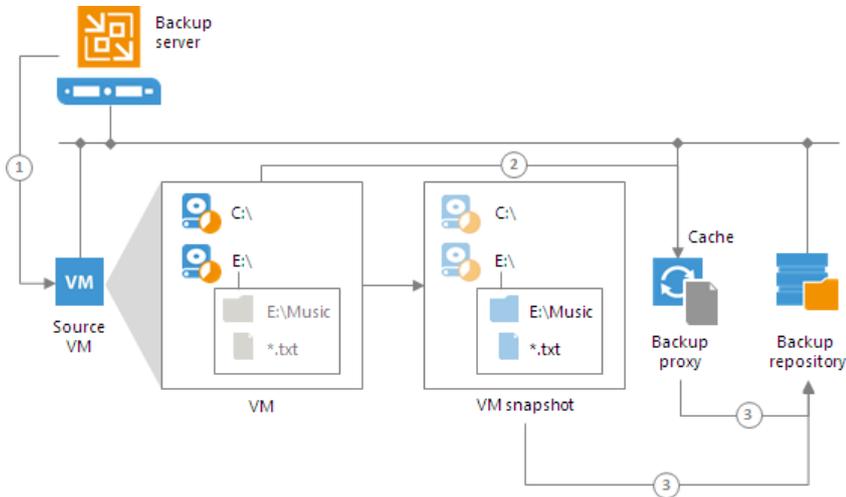
To include only the `D:\Documents` folder to the backup, you must add the `D:\Documents` folder to the list of inclusions and, additionally, exclude unnecessary disks (that contain `C:\` and `D:\` volumes) at the **Virtual Machines** step of the wizard. For more information, see [Step 4. Exclude Objects from Backup Job](#).

How VM Guest OS File Exclusion Works

When you exclude VM guest OS files from the backup or replica, Veeam Backup & Replication performs the following operations:

1. Veeam Backup & Replication checks the job settings to identify what VM guest OS files must be excluded.
2. Veeam Backup & Replication opens the MFT file from the VM guest file system in the memory cache on the backup proxy, and marks data blocks of excluded files as deleted.

- When Veeam Backup & Replication copies VM data to the target, it reads data both from the VM snapshot and memory cache on the backup proxy. On the target, Veeam Backup & Replication creates a "merged" version of VM disks that do not contain excluded VM guest OS files. Due to data compression, data blocks that are marked as deleted are compressed, and the size of the resulting backup or replica file reduces.



During the job session with file exclude, Veeam Backup & Replication makes changes to processed VM disks at the NTFS level using the cache on the backup proxy. However, these changes are not visible to the CBT mechanism. For this reason, Veeam Backup & Replication saves information about excluded data blocks in the backup file and replica metadata. During the next job session with use of CBT, Veeam Backup & Replication retrieves a list of data blocks that were excluded during the previous job session from the backup file or replica metadata and analyzes what data needs to be processed during the current job session. To do this, Veeam Backup & Replication regards the following data:

- Data blocks that are marked as new with CBT
- Data blocks that were excluded during the previous job session
- Data blocks that must be excluded during the current job session

Transaction Consistency

When you back up or replicate a running VM, you need to quiesce, or 'freeze' the VM to bring its file system and application data to a consistent state. If the VM is not quiesced, Veeam Backup & Replication will produce a crash-consistent backup or replica. The crash consistent backup or replica does not preserve data integrity of open files and transactional applications on the VM. Restore from a crash-consistent backup or replica is essentially equivalent to booting the VM after it was manually reset.

A crash-consistent backup or replica may be sufficient for VMs that run applications with low quantity of transactions. If you process VMs with highly transactional applications, you should instruct Veeam Backup & Replication to quiesce the VM and create a transactionally consistent backup or replica. Restore from transactionally consistent backups or replicas guarantees safety of application data.

Veeam Backup & Replication offers two options for creating consistent backups and replicas:

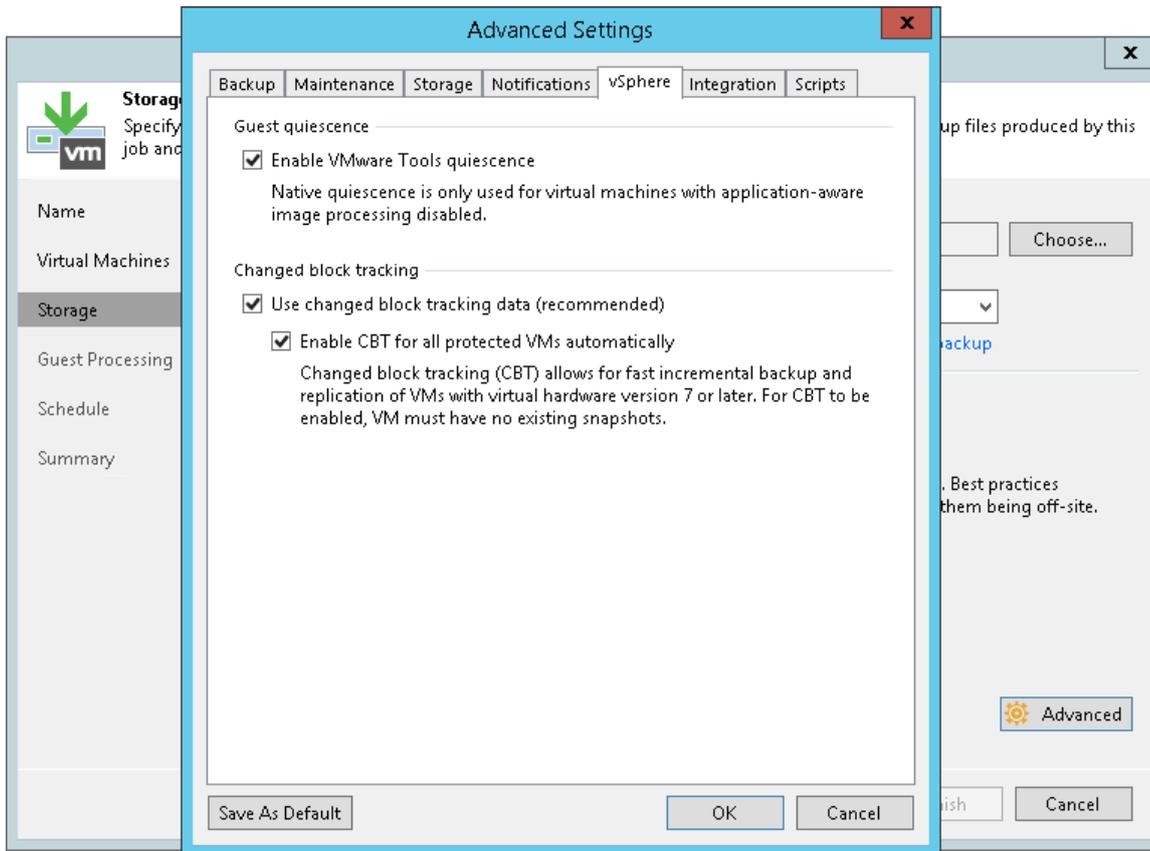
- [Application-aware processing](#) (based on Microsoft VSS). This option is recommended for VMs running applications that support Microsoft VSS.
- [VMware Tools quiescence](#). This option is recommended for VMs running applications that do not support Microsoft VSS, for example, Linux VMs.

To create consistent backups for such VMs, applications should be prepared using special pre-freeze and post-thaw scripts that you should create and store on the backup server beforehand. When the job starts, Veeam Backup & Replication will upload these scripts to the appropriate folders on VM guest. For more information, see [Pre-Freeze and Post-Thaw Scripts](#).

VMware Tools Quiescence

To create transactionally consistent backups and replicas for VMs that do not support Microsoft VSS (for example, Linux VMs), you must enable VMware Tools quiescence for the job. In this case, Veeam Backup & Replication will use the VMware Tools to freeze the file system and application data on the VM before backup or replication.

VMware Tools quiescence is enabled at the job level for all VMs added to the job. By default, this option is disabled.



VMware VSS Component

To quiesce VMs, Veeam Backup & Replication uses the VMware VSS component in VMware Tools. Starting from vSphere 3.5 U2, VMware Tools support Microsoft VSS. To use the VMware VSS component in VMware Tools, the VM must run one of the following OSes:

- Microsoft Windows Server 2003 32-bit or 64-bit.
All latest updates and patches must be installed on the VM guest OS. Microsoft Windows 2003 SP1 at minimum is recommended.
- Microsoft Windows Vista 32-bit or 64-bit
- Microsoft Windows 7 32-bit or 64-bit
- Microsoft Windows Server 2008 32-bit or 64-bit
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 2016

Supported quiescence features differ depending on the type of the VM guest OS:

- For VMs running Windows Vista and Windows 7, the VMware VSS component does not use application writers. As a result, the created VSS snapshots are file-system consistent.
- For VMs running Microsoft Windows Server 2003, the VMware VSS component uses application VSS writers. As a result, the created VSS snapshots are application-consistent.

- For VMs running Microsoft Windows Server 2008 and later, the VMware VSS component may or may not use application writers, depending on the VM platform and state. The created VSS snapshots can be file-system or application-consistent.

For more information about VMware Tools quiescence, see VMware documentation:

<http://pubs.vmware.com/vsphere-55/topic/com.vmware.vddk.pg.doc/vddkBkupVadp.9.6.html>

Choice of Method for VM Quiescence

Application-aware processing is the recommended option for VMs running applications that support Microsoft VSS – Microsoft Exchange, Microsoft Active Directory and other. If you cannot use application-aware processing (for example, you cannot access the VM over the network and deploy Veeam's runtime process on it, or you want to process a Linux VM and want the backup or replica to be consistent at the application and file system level), you should enable VMware Tools quiescence. VMware Tools quiescence will put applications on the VM to a consistent state before the VM snapshot is created.

If you use VMware Tools quiescence, Veeam Backup & Replication will quiesce the VM but will not perform application-specific actions required for proper backup and restore of VMs running highly transactional applications. Application-specific steps include the following tasks:

- Applying application-specific settings to prepare applications for VSS-aware restore at the next VM startup
- Truncating transaction logs after successful backup or replication.

Enabling Both Quiescence Options

You can enable both options for VM quiescence. Such scenario is recommended if you add Microsoft Windows and Linux VMs to the same job. In this case, all VMs will be processed in a transactionally consistent manner – either with application-aware processing or VMware Tools quiescence.

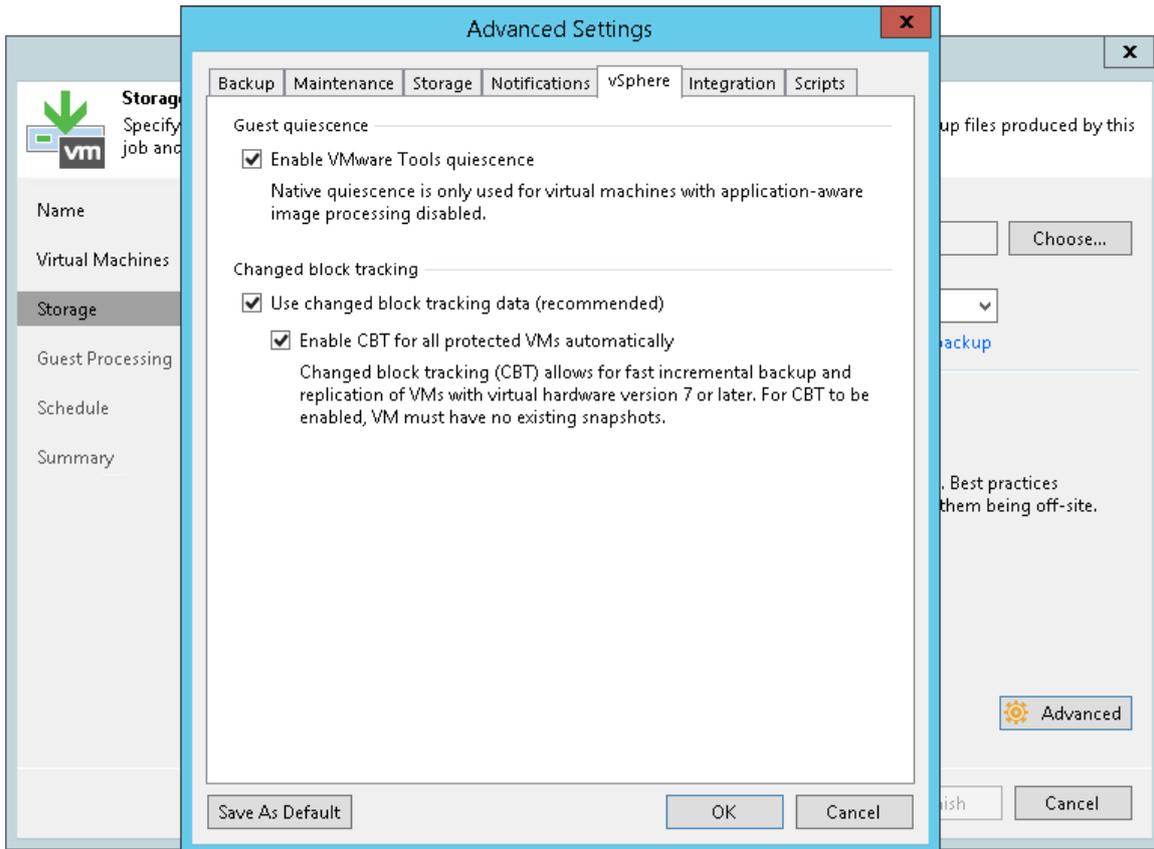
In such scenario, Veeam Backup & Replication will process VMs in the job in the following way:

1. Veeam Backup & Replication will first attempt to use application-aware processing to prepare VMs for backup or replication. If Veeam Backup & Replication manages to quiesce all VMs in the job with application-aware processing, it will not use VMware Tools quiescence.
2. If some VMs cannot be quiesced with application-aware processing or application-aware processing is disabled for some VMs in the job (the **Disable application processing** is set for VMs in the job settings), Veeam Backup & Replication will use VMware Tools quiescence to prepare these VMs for backup or replication.

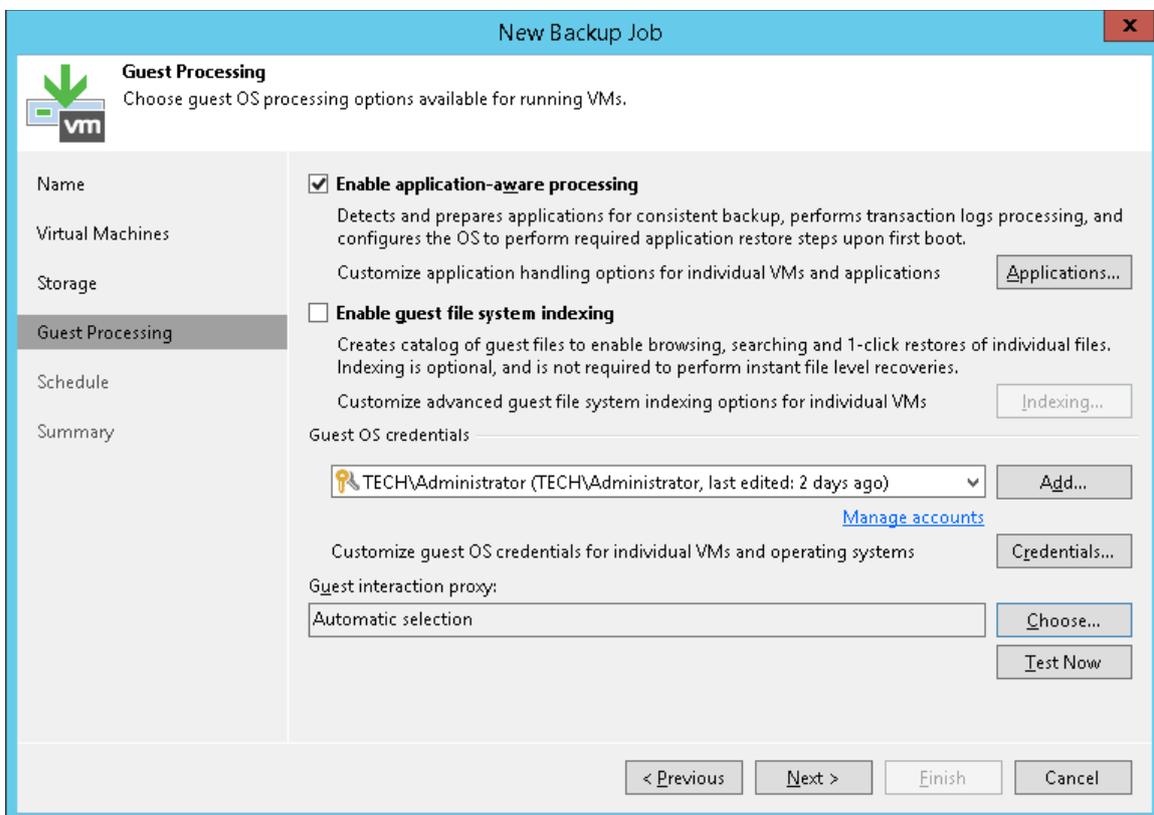
To enable both options:

1. At the **Storage** step of the wizard (for backup) or **Job Settings** step of the wizard (for replication), click **Advanced**.

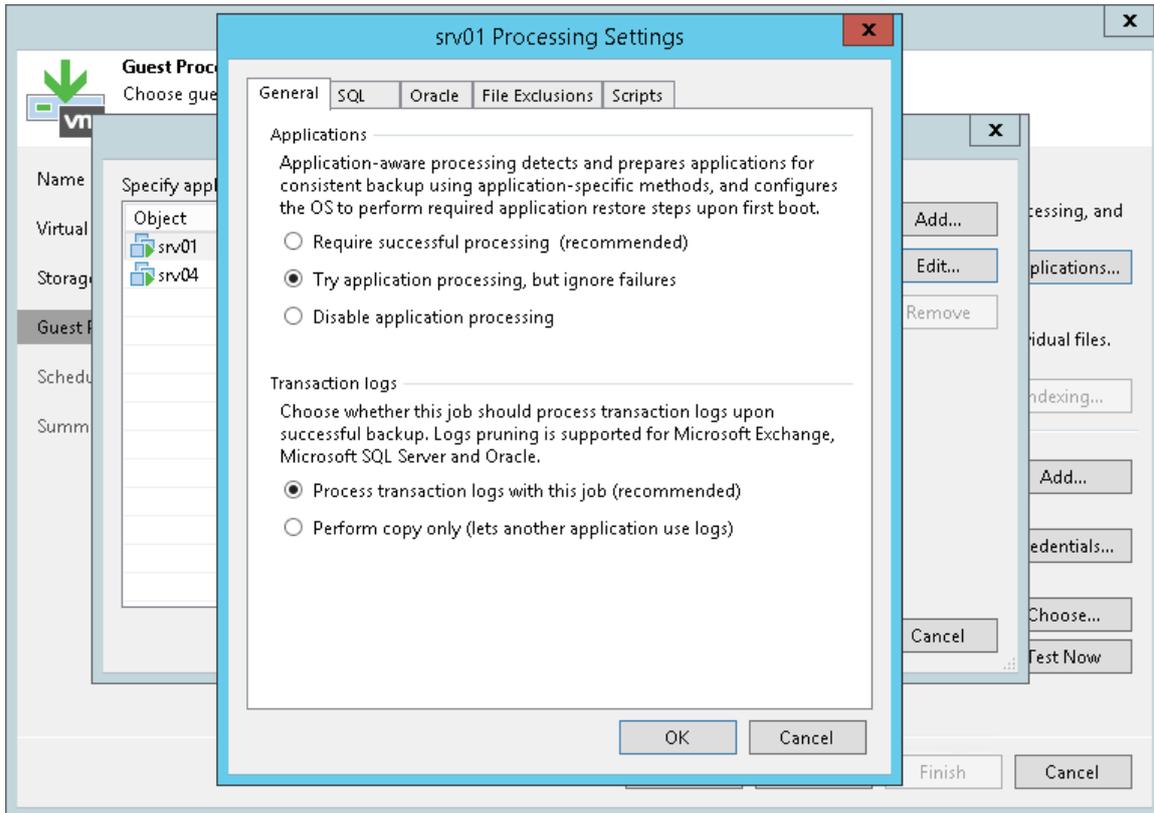
2. On the vSphere tab of the **Advanced Settings** window, select **Enable VMware Tools quiescence**.



3. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.



- When configuring advanced option for individual VMs, select **Try application processing, but ignore failures**. You can also select the **Disable application processing** option for VMs that you want to process with VMware Tools quiescence.



NOTE:

If you enable application-aware processing and VMware Tools quiescence but do not select the **Ignore application processing failures** option, Veeam Backup & Replication will use only application-aware processing for the job.

Guest Processing

If you back up or replicate running VMs, you can enable guest processing options. Guest processing options are advanced tasks that require Veeam Backup & Replication to communicate with the VM guest OS.

Veeam Backup & Replication offers the following guest processing options:

- [Application-aware processing](#). You can create transactionally consistent backups and replicas of VMs running applications that support Microsoft VSS. Application-aware processing guarantees that you can restore VMs without data loss.
- [Pre-freeze and post-thaw scripts](#). You can use pre-freeze and post-thaw scripts to quiesce VMs running applications that do not support Microsoft VSS.
- [Transaction log truncation](#). You can set the backup or replication job to truncate transaction logs on the VM guest OS after the VM is successfully processed.
- [Transaction logs backup for Microsoft SQL Server](#) and [Oracle](#). You can set up the backup job to back up transaction logs from Microsoft SQL Server and Oracle VMs.
- [VM guest file system indexing](#). You can set up the backup job to create a catalog of files and folders on the VM guest OS. The catalog lets you search for VM guest OS files and 1-click restore in Veeam Backup Enterprise Manager.

VM guest file system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the backup created with such backup job. For more information, see the [Preparing for File Browsing and Searching](#) section in the Enterprise Manager User Guide.

- [VM guest OS files exclusion](#). You can exclude/include individual files and folders from/to backup or replicas.

User Account for Guest Processing

General Requirements

A user account for application-aware image processing must have administrator privileges on the VM guest OS. Credentials for Microsoft Windows VMs must be specified in the following format:

- For Active Directory accounts – *DOMAIN|Username*
- For local accounts – *Username* or *HOST|Username*

Domain Controllers

- If you process a Domain Controller, select an account that is a member of the *DOMAIN|Administrators* group to enable guest processing.
- If you back up a Read-Only Domain Controller, a delegated RODC administrator account is sufficient. For more information, see [Microsoft Docs](#).

Transaction Log Backup

If you add a Microsoft SQL Server VM or Oracle VM to the job, make sure that you specify a user account that has enough permissions on the database.

- If you back up a Microsoft SQL VM and want Veeam Explorer for Microsoft SQL Server to automatically identify Microsoft SQL Server databases in the created backup, the user account must have the sysadmin privileges on the Microsoft SQL Server.
- If you back up an Oracle VM, the user account must have SYSDBA privileges on the database.

You can grant access rights to the VM guest OS and SYSDBA role to one user account and specify credentials of this user account in the job settings. If the account that you plan to use to connect to the VM guest OS does not have the SYSDBA role (for example, for security reasons), you will have to specify another account that has SYSDBA rights on the **Oracle** tab of the **VM Processing Settings** window. This account will be used to access the Oracle database. For more information, see [Transaction Log Settings Oracle](#).

Supported Applications

With Veeam Backup & Replication, you can create transactionally consistent backups or replicas of VMs that run the following applications:

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Oracle

To create transactionally consistent backups, make sure you enable application-aware processing in the job settings.

To view and recover backed up application items, you can use the capabilities of Veeam Backup Explorers. For more information, see [Veeam Explorers User Guide](#).

For information on system requirements for applications, see [System Requirements](#).

Runtime Coordination Process

To perform guest processing tasks, Veeam Backup & Replication does not deploy persistent agents inside VMs. Instead, it uses a runtime coordination process. The runtime process is non-persistent — it is deployed on every VM added to the job when the job starts and removed as soon as the job finishes. Use of the runtime process helps avoid agent-related drawbacks such as pre-installing, troubleshooting and updating.

Veeam Backup & Replication can deploy the runtime process on VMs in two ways:

- For VMs running Microsoft Windows, the runtime process is deployed via guest interaction proxies. For more information, see [Guest Interaction Proxy](#).
- For VMs running OSES other than Microsoft Windows, for example, Linux, the runtime process is deployed from the backup server.

NOTE:

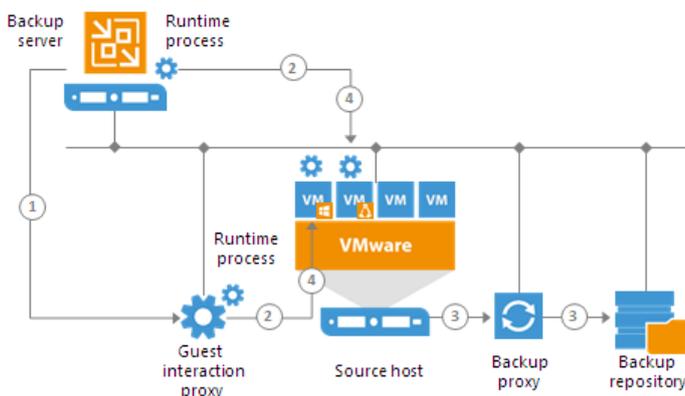
If there are no guest interaction proxies or guest interaction proxies fail for some reason, Veeam Backup & Replication will deploy the runtime process on Microsoft Windows VMs from the backup server.

When you start a job with guest processing tasks enabled, Veeam Backup & Replication performs the following operations:

1. Veeam Backup & Replication defines the machines that will perform the guest interaction proxy role.
2. Veeam Backup & Replication obtains IP addresses from VMware Tools installed on VMs. If Veeam Backup & Replication fails to connect to the VM guest OS over the network, it obtains IP addresses over VIX.

Veeam Backup & Replication deploys the runtime process on VMs:

- [For Microsoft Windows VMs] The guest interaction proxy connects to VMs and deploys the runtime process on them.
 - [For VMs running other OSes] The backup server connects to VMs and deploys the runtime process on them.
3. The job session proceeds as usual.
 4. When the job session completes, Veeam Backup & Replication deletes the runtime process on VMs.



If a network connection breaks during the job session, Veeam Backup & Replication makes attempts to re-establish the connection:

- If a network connection between the backup server/guest interaction proxy and VM guest OS breaks, Veeam Backup & Replication makes one attempt to reconnect.
- If a network connection between the backup server and guest interaction proxy breaks, Veeam Backup & Replication makes 10 attempts to reconnect.

If attempts are unsuccessful, guest processing tasks fail. The job proceeds with the scenario defined in the job settings. For example, if you have instructed a backup job to try application processing but ignore failures, Veeam Backup & Replication will not perform guest processing tasks but will proceed with the VM backup.

Application-Aware Processing

To create transactionally consistent backups or replicas of VMs that run VSS-aware applications such as Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange or Oracle, you must enable application-aware processing for the job.

Application-aware processing is Veeam's proprietary technology based on Microsoft VSS. Microsoft VSS is responsible for quiescing applications on the VM and creating a consistent view of application data on the VM guest OS. Use of Microsoft VSS ensures that there are no unfinished database transactions or incomplete application files when Veeam Backup & Replication triggers the VM snapshot and starts copying VM data to the target. For more information about Microsoft VSS, see [https://technet.microsoft.com/en-us/library/cc785914\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc785914(v=ws.10).aspx).

Application-aware processing for Microsoft Windows Server versions is supported by corresponding versions of VMware vSphere (<https://kb.vmware.com/s/article/2091273>). To use application-aware processing, you must have VMware Tools and the latest updates installed on the VM guest OS.

IMPORTANT!

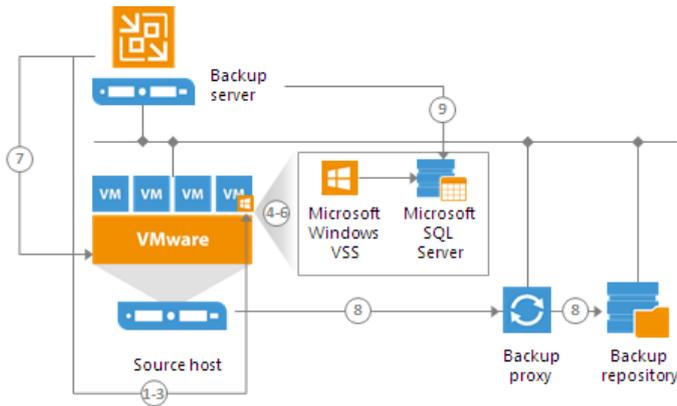
If a VM runs an application that does not support Microsoft VSS (there is no VSS writer for this particular type of application, for example, MySQL), Veeam Backup & Replication will not be able to utilize Microsoft VSS and application-aware processing for this VM. To process such VMs, you can use VMware Tools quiescence with pre-freeze and post-thaw scripts. For more information, see [VMware Tools Quiescence](#) and [Pre-Freeze and Post-Thaw Scripts](#).

How Application-Aware Processing Works

If you enable application-aware processing for the job, Veeam Backup & Replication performs the following operations as a part of the backup or replication process:

1. Veeam Backup & Replication deploys the runtime process on the VM and detects if the VM runs VSS-aware applications.
2. Veeam Backup & Replication collects information about applications installed on VMs; this information is required for VSS-aware restore.
3. Veeam Backup & Replication prepares applications for VSS-aware restore (VSS-aware restore is performed when the VM is started after you restore it from the backup or fail over to a VM replica).
4. Microsoft VSS communicates with applications and quiesces I/O activities at a specific point in time.
5. Veeam Backup & Replication acts as a VSS requestor and triggers a VM VSS snapshot.
6. Veeam Backup & Replication triggers a VMware vSphere snapshot of the VM.
7. Microsoft VSS resumes quiesced I/O activities on the VM guest OS.
8. The job session proceeds as usual.

- If you have instructed Veeam Backup & Replication to truncate transaction logs, Veeam Backup & Replication truncates transaction logs on the VM guest OS after the backup or replica are successfully created.



Pre-Freeze and Post-Thaw Scripts

If you back up or replicate VMs running applications that do not support Microsoft VSS, you can instruct Veeam Backup & Replication to run custom scripts for VMs. For example, the pre-freeze script may quiesce the file system and application data on the VM guest OS to bring the VM to a consistent state before Veeam Backup & Replication triggers a VM snapshot. After the VM snapshot is created, the post-thaw script may bring the VM and applications to their initial state.

You can use pre-freeze and post-thaw scripts for the following types of jobs:

- Backup job
- Replication job
- VM copy job

Pre-freeze and post-thaw scripts can be used for Microsoft Windows and Linux VMs.

- For Microsoft Windows VMs, Veeam Backup & Replication supports scripts in the EXE, BAT, CMD, WSF, JS, and PS1 file format.
- For Linux VMs, Veeam Backup & Replication supports scripts in the SH file format.

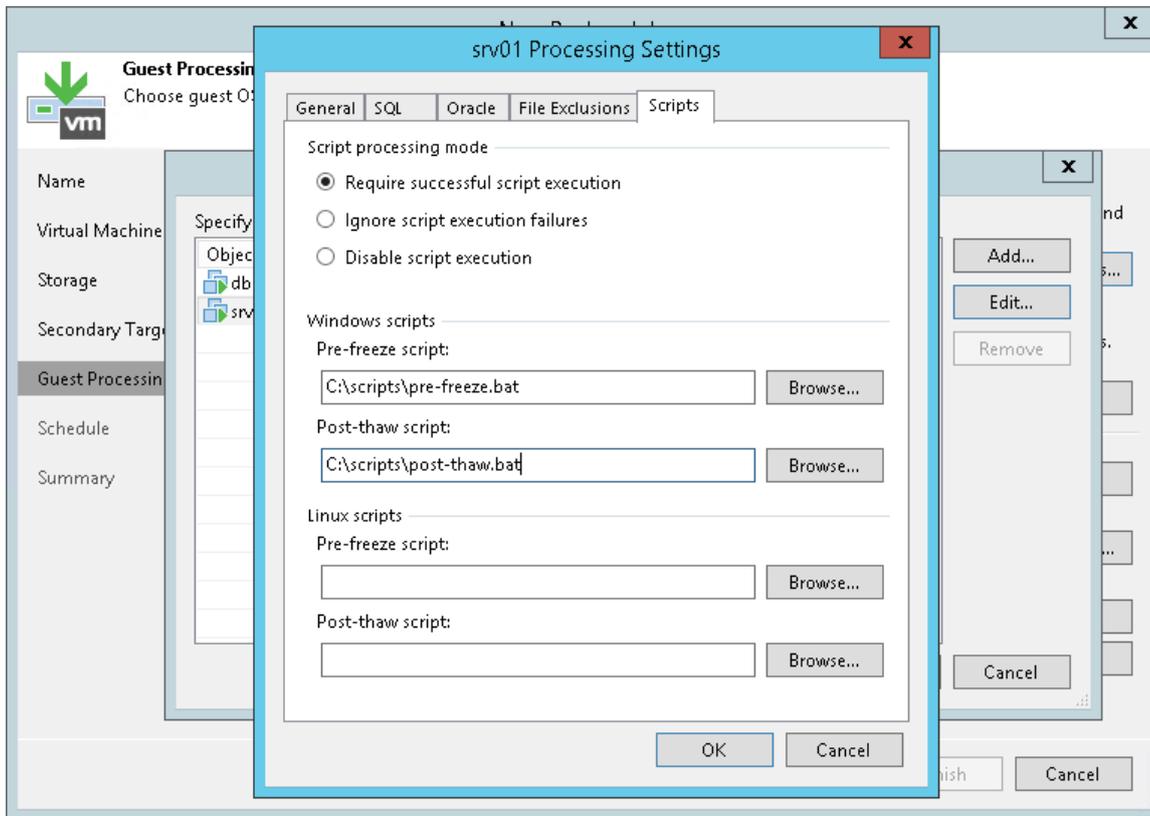
Scripts must be created beforehand. You must specify paths to them in the job settings. Script execution settings can be configured per VM or per container, depending on the objects included in the job.

When the job starts, Veeam Backup & Replication uploads scripts to the VM guest OS and executes them under the account specified in the **Guest OS credentials** section of the job settings.

- Scripts for Microsoft Windows VMs are uploaded to `||<vmname>|admin$` over the network or VIX, if Veeam Backup & Replication fails to connect to the VM guest OS over the network. Scripts are executed from the `C:\Windows` directory.
- Scripts for Linux VMs are uploaded over SSH or VIX, if the SSH connection fails. Scripts are executed from the `/home/<username>` directory of a user that you have specified in **Guest OS credentials**.

The script is considered to be executed successfully if "0" is returned.

The default time period for script execution is 10 minutes. If the script fails to execute before the timeout expires, Veeam Backup & Replication displays an error message in the job session and error or warning messages issued during script execution.



Limitations for Pre-Freeze and Post-Thaw Scripts

Veeam Backup & Replication has the following limitations for pre-freeze and post-thaw scripts:

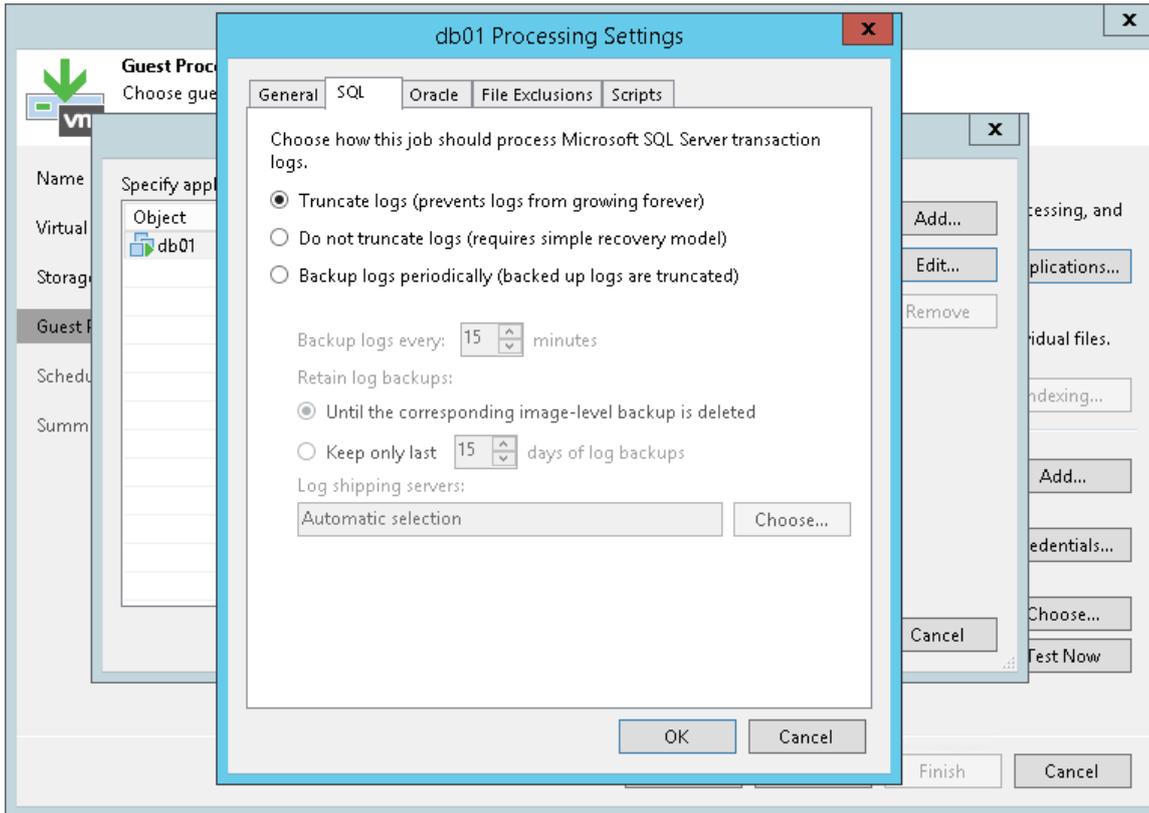
- You cannot stop a job when the pre-freeze or post-thaw script is executed. If the script hangs up, Veeam Backup & Replication waits for 10 minutes and terminates the job.
- If you want to run several scripts that depend on each other, you must upload them to the VM guest OS manually. For example, you have *script1.bat* that sequentially starts *script2.bat*, *script3.bat* and *script4.bat*. In this case, you must specify a path to *script1.bat* in the job properties and upload *script2.bat*, *script3.bat* and *script4.bat* to the VM guest OS.
- It is not recommended to use the standard error (STDERR) stream for error output in Linux scripts. Veeam Backup & Replication will fail to execute scripts with STDERR.

Transaction Log Truncation

If you back up or replicate virtualized database systems that use transaction logs, for example, Microsoft Exchange or Microsoft SQL Server, you can instruct Veeam Backup & Replication to truncate transaction logs so that logs do not overflow the storage space on the VM. Veeam Backup & Replication provides the following options of transaction logs handling:

- [Truncate logs](#)
- [Do not truncate logs](#)

- [Back up logs periodically](#)



Truncate Logs

You can instruct Veeam Backup & Replication to truncate logs after a backup or VM replica is successfully created. With this option selected, Veeam Backup & Replication behaves in the following way:

- If the job completes successfully, Veeam Backup & Replication produces a backup file or VM replica and truncates transaction logs on the original VM. As a result, you have the backup file or replica that contains a VM image at a specific point in time.

In this scenario, you can recover a database to the point in time when the backup file or replica was created. As transaction logs on the VM are truncated, you cannot use them to get the restored database to some point in time between job sessions.

- If the backup or replication job fails, Veeam Backup & Replication does not truncate transaction logs on the VM. In this scenario, you can restore a VM from the most recent backup or replica restore point and use database system tools to apply transaction logs and get the database system to the necessary point in time after the restore point.

Do not Truncate Logs

You can choose not to truncate transaction logs on the VM. This option is recommended if together with Veeam Backup & Replication you use another backup tool.

For example, you can use Veeam Backup & Replication to create a VM image backup and instruct the native Microsoft SQL Server log backup job to back up transaction logs. If you truncate transaction logs with Veeam Backup & Replication, the chain of transaction logs will be broken, and the Microsoft SQL Server log backup job will not be able to produce a consistent log backup.

With this option selected, Veeam Backup & Replication produces a backup file or VM replica and does not trigger transaction log truncation. As a result, you have a backup file or VM replica that contains a VM image captured at a specific point in time, and transaction logs on the VM. You can use transaction logs to restore the VM to any point in time between job sessions. To do this, you must recover the VM from the backup file or perform replica failover and use database system tools to apply transaction logs and get the database system to the necessary point in time.

Back Up Logs Periodically

This option can be used if you back up Microsoft SQL Server VMs and Oracle VMs.

You can choose to back up logs with Veeam Backup & Replication. For more information, see [Microsoft SQL Server Logs Backup and Restore](#) and [Oracle Logs Backup and Restore](#).

Support for Database Availability Groups (DAG)

Veeam Backup & Replication supports any configuration of DAGs, in particular, with all databases active on one node, or with active databases on every node. Transaction logs will be truncated on all DAG members, no matter whether Veeam Backup & Replication backs up an active or passive database.

For more information and recommendations on Microsoft Exchange Server backup, you can also refer to the following:

- [White Paper by Michael Van Horenbeek on how to virtualize and protect Exchange 2016](#)
- [Veeam Knowledge Base article](#)

Copy-Only Backup

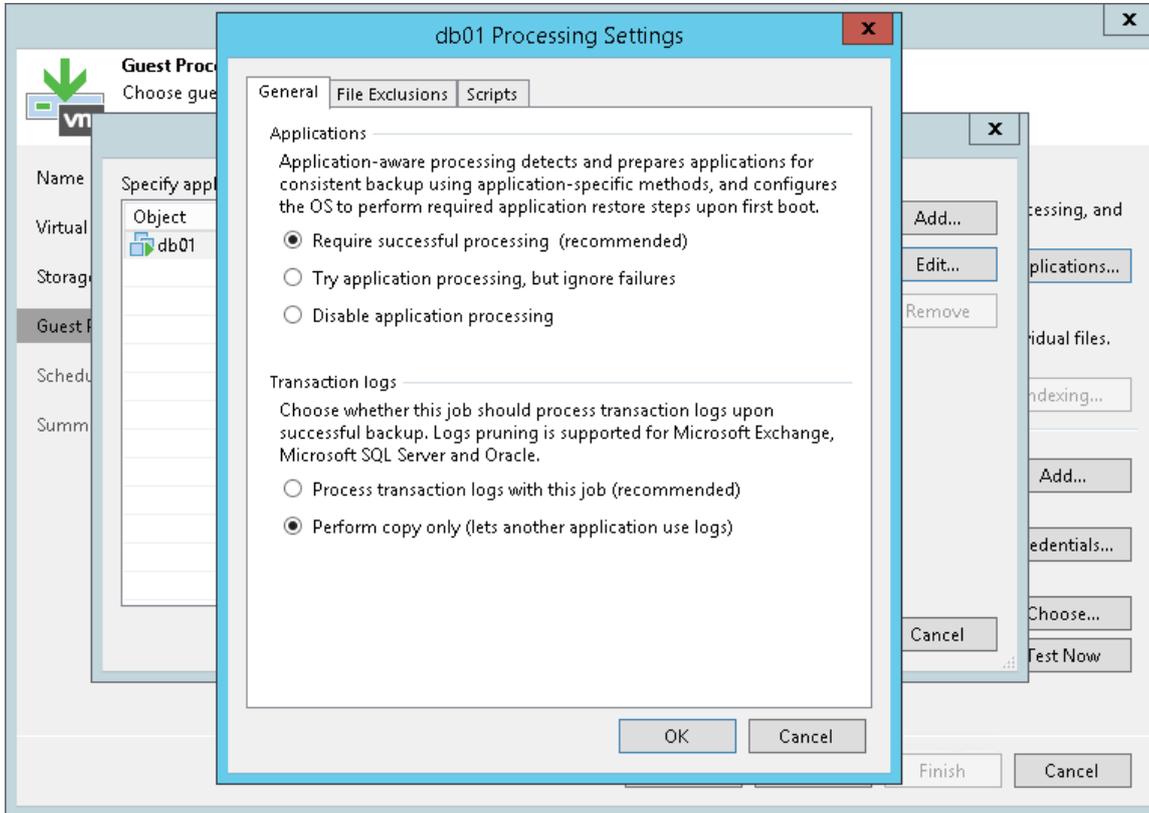
Some organizations prefer to back up Microsoft SQL Server databases and transaction logs with native Microsoft SQL Server tools or 3rd party backup tools. To restore database systems in a proper way, database administrators must be sure that they have database backups and a sequence of transaction log backups associated with these backups at hand.

If you use native Microsoft SQL Server tools or 3rd party backup tools and also want to back up Microsoft SQL Server VMs with Veeam Backup & Replication, you must enable the **Perform copy only** option in the job settings.

The **Perform copy only** option indicates that a chain of database backups is created with native Microsoft SQL Server means or by a 3rd party tool, and instructs Veeam to preserve this chain (backup history). Veeam Backup & Replication backs up the Microsoft SQL Server VM using the *VSS_BS_COPY* method for snapshot creation. The *VSS_BT_COPY* method produces a copy-only backup – the backup that is independent of the existing chain of database backups and does not contain transaction logs data. As a result, the copy-only backup does not change the log sequence number and transaction log backup time.

IMPORTANT!

Veeam Backup & Replication does not truncate transaction logs after copy-only backup. For this reason, if you instruct the backup job to perform copy-only backup, you cannot specify transaction log handing settings for this job.



VM Guest File System Indexing

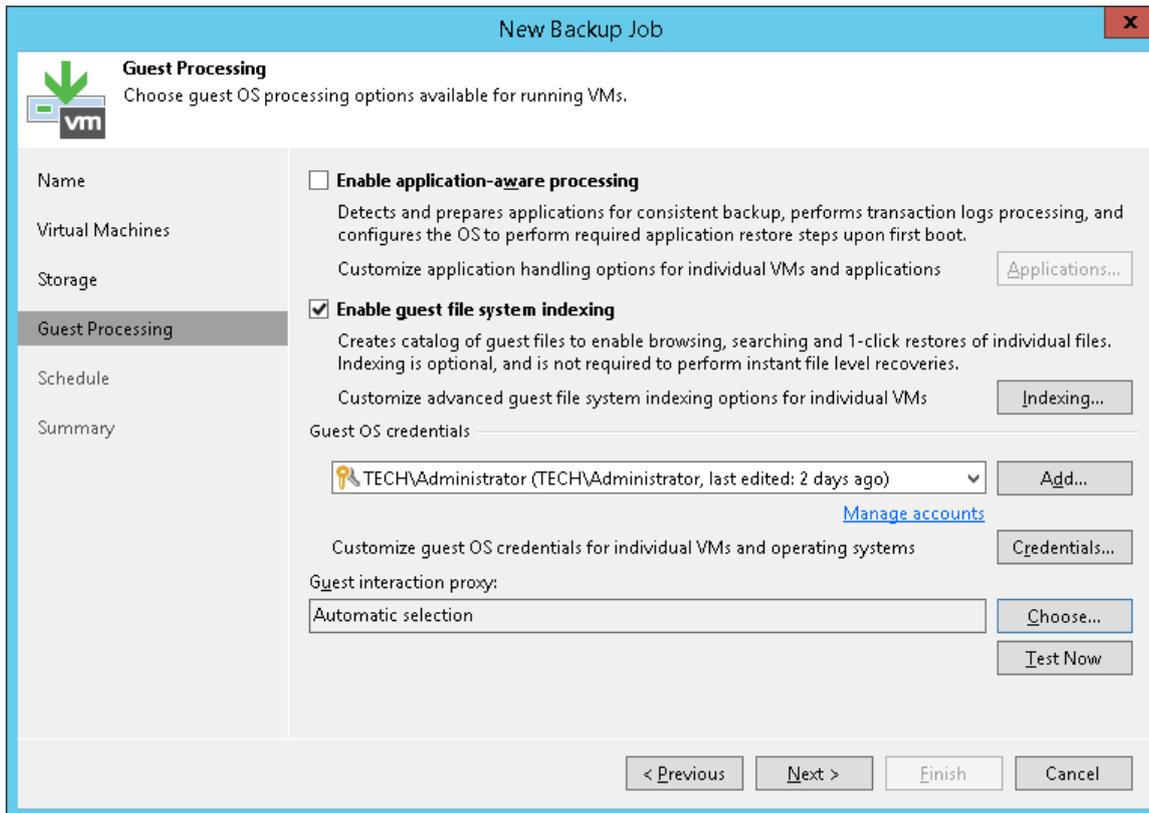
You can instruct Veeam Backup & Replication to create an index of files and folders on the VM guest OS during backup. Guest file indexing allows you to search for VM guest OS files inside VM backups and perform 1-click restore in Veeam Backup Enterprise Manager.

VM guest OS file indexing is enabled at the job level. You can specify granular indexing settings for every VM in the job.

NOTE:

VM guest file system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the backup created with such backup job. For more information, see the [Preparing for File Browsing and Searching](#) section of Enterprise Manager User Guide.

Mind the following: if you do not enable indexing in the backup job, in case of 1-click restore from Linux and other OS backups Veeam Backup Enterprise Manager will not display symlinks to folders in the file system browser.



Requirements for VM Guest OS Indexing

- Veeam Backup & Replication supports file indexing for VMs running Microsoft Windows and Linux OS.
- Linux VMs must have the following tools installed: openssh, mlocate, gzip and tar.

Veeam Backup Catalog

For VM guest OS file indexing, Veeam Backup & Replication uses the Veeam Guest Catalog Service. In the backup infrastructure, the Veeam Guest Catalog Service is installed on the Veeam backup server and Veeam Backup Enterprise Manager server.

- The Veeam Guest Catalog Service on the Veeam backup server works as a local catalog service. It collects indexing data for backup jobs and stores this data in the Veeam Backup Catalog folder.

By default, the indexing data is stored in the `VBRCatalog` folder on the backup server. Veeam Backup & Replication creates the folder on a volume with the maximum amount of free space, for example, `C:\VBRCatalog`.

- The Veeam Guest Catalog Service on Veeam Backup Enterprise Manager works as a global, federal catalog service. It communicates with Veeam Guest Catalog Services on backup servers connected to Veeam Backup Enterprise Manager and performs the following tasks:

- Replicates indexing data from backup servers to create a global catalog for the whole backup infrastructure.

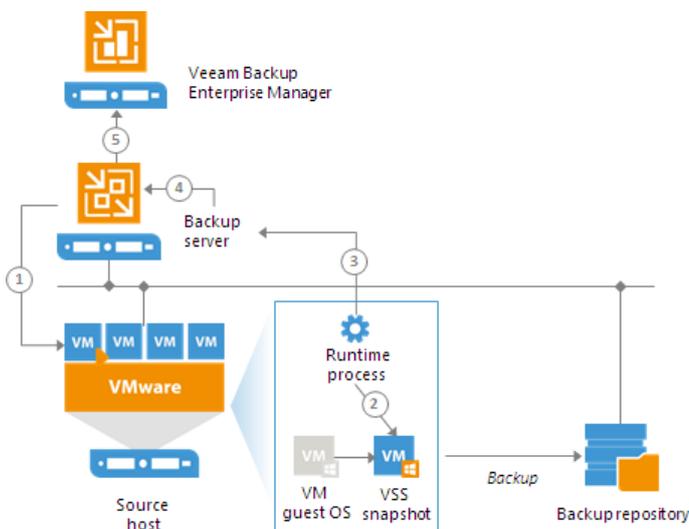
On the Veeam Backup Enterprise Manager server, the default folder for storing indexing data (the `VBRCatalog` folder) is located on a volume with the maximum amount of free space.

- Maintains indexing data retention.
- Allows you to search for VM guest OS files in current and archived backup files.

How VM Guest OS Indexing Works

When you run a backup job with the file indexing option enabled, Veeam Backup & Replication performs the following operations:

1. When the backup job starts, Veeam Backup & Replication connects to the VM whose file system must be indexed and deploys a runtime process inside this VM. The runtime process is responsible for coordinating indexing activities inside the VM.
2. The runtime process starts indexing the VM file system. The indexing procedure is carried out in parallel with the backup procedure. If indexing takes long, Veeam Backup & Replication will not wait for the indexing procedure to complete. It will start copying VM data and continue file indexing inside the VM. If you have enabled application-aware processing for the VM, Veeam Backup & Replication performs indexing using the VSS snapshot, not the VM guest OS itself. As a result, the created file index exactly reflects the state of the backed up VM.
3. When file indexing is complete, the runtime process collects indexing data and writes it to the `GuestIndexData.zip` file. The `GuestIndexData.zip` file is stored to a temporary folder on the backup server.
4. When the backup job completes, Veeam Backup & Replication notifies the local Veeam Guest Catalog Service, and the service saves indexing data in the Veeam Catalog folder on the backup server.
5. During the next catalog replication session, the global Veeam Guest Catalog Service replicates data from the backup server to the Veeam Catalog folder on the Veeam Backup Enterprise Manager server.



Persistent VSS Snapshots

During application-aware processing, Veeam Backup & Replication uses a VSS writer for a corresponding application to freeze application data and bring it to a consistent state.

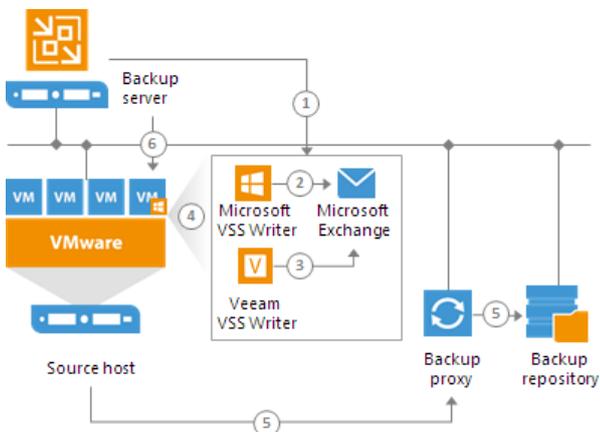
According to Microsoft limitations, applications cannot be kept frozen longer than for 60 seconds (20 seconds for Microsoft Exchange). If the Microsoft VSS writer keeps application data frozen longer than this period, a VSS processing timeout occurs, and Veeam Backup & Replication fails to create a transactionally consistent backup of the VM. The VSS processing timeout is a common problem for highly transactional applications such as Microsoft Exchange.

To overcome this limitation, Veeam Backup & Replication uses the persistent VSS snapshots technology for backup of Microsoft Exchange VMs. If Microsoft Exchange has to be kept frozen for a longer period of time than the allowed one, Veeam Backup & Replication automatically fails over to the persistent VSS snapshot mechanism.

Backup of Microsoft Exchange VMs is performed in the following way:

1. Veeam Backup & Replication triggers the Microsoft VSS framework to prepare Microsoft Exchange on the VM for backup.
2. The Microsoft VSS writer attempts to quiesce Microsoft Exchange.
3. If the Microsoft VSS writer fails to quiesce Microsoft Exchange within the allowed period of time, the control is passed to the native Veeam VSS writer. The Veeam VSS writer holds the freeze operation for the necessary amount of time.
4. After Microsoft Exchange data is brought to a consistent state, the control is passed to the Microsoft VSS provider. The Microsoft VSS framework creates a persistent VSS snapshot for VM disks except the system VM disk.
5. The job session proceeds as usual.
6. After the backup operation is complete, Veeam Backup & Replication triggers Microsoft VSS to remove the persistent VSS snapshot on the production VM. The persistent VSS snapshot holding consistent application data inside the created VM backup remains.

During entire VM restore, Veeam Backup & Replication recovers data from the backup and reverts VM disks to the persistent VSS snapshot inside the backup. As a result, the Microsoft Exchange VM is restored from the backup in a consistent state without data loss.



Limitations for Persistent VSS Snapshot Technology

Veeam Backup & Replication uses the persistent VSS snapshot technology if the VM meets the following requirements:

- The VM runs Microsoft Exchange 2010, Microsoft Exchange 2013 or Microsoft Exchange 2016.
- The VM does not perform the role of a domain controller.
- Microsoft Exchange databases and log files are located on a non-system disk of the VM. During backup, Veeam Backup & Replication does not trigger a persistent VSS snapshot for system VM disks. As a result, system disks are restored in a crash-consistent, not transactionally consistent state.

Microsoft SQL Server Logs Backup and Restore

To protect Microsoft SQL Server VMs, you can instruct the backup job to create image-level VM backups and periodically back up database transaction logs. If Microsoft SQL Server fails, you can restore the Microsoft SQL Server VM from the necessary restore point of the image-level backup. After that, you can use Veeam Explorer for Microsoft SQL Server to apply transaction logs and get databases on the Microsoft SQL Server to the necessary state between backups.

Transaction Log Backup Jobs

To back up transaction logs, you must create a backup job, add Microsoft SQL Server VMs to it and specify advanced settings for transaction logs backup in the job settings. The resulting job will comprise two jobs:

- Parent backup job – the backup job that creates an image-level backup of the Microsoft SQL Server VM. The parent backup job is named *<job_name>*, for example, *DB Backup*. You can configure the parent job in the Veeam Backup & Replication console just like any other backup job.
- Child job – a transaction log backup job. To form a name of the child job, Veeam Backup & Replication adds a suffix to the name of the parent backup job: *<parent_job_name> + SQL Server Transaction Log Backup*, for example, *DB Backup SQL Server Transaction Log Backup*. Veeam Backup & Replication automatically creates the child job if it detects a backup job that is scheduled to back up at least one Microsoft SQL Server VM, and transaction log backup is enabled for this job. Session data of the transaction log backup job is stored in the configuration database and displayed in the Veeam Backup & Replication console.

The parent job runs in a regular manner – it starts by schedule or is started manually by the user. The transaction log backup job is triggered by the parent backup job. This sequence ensures that the VM (and the database) restore point is present when it comes to transaction log replay.

Sessions of Transaction Log Backup Jobs

The transaction log backup job runs permanently in the background, shipping transaction logs to the backup repository at a specific time interval (by default, every 15 minutes). A sequence of time intervals between sessions of the parent backup job makes up a session of the transaction log backup job.

The transaction log backup session starts and stops in the following way:

- The initial session starts when the parent backup job schedule is enabled. After that, the session starts with every new session of the parent backup job.
- The session ends before the next session of the parent backup job or when this parent backup job is disabled.
- When the session ends, Veeam Backup & Replication stops the runtime process and uninstalls it from the VM guest OS. When a new session starts, the runtime process is deployed again.

How Microsoft SQL Server Logs Backup Works

To perform transaction log backup, Veeam Backup & Replication installs the *Veeam Guest SQL Log Shipper* runtime component on the VM guest OS.

The component works during the transaction log backup job session. It collects information about databases that require transaction logs backup. It also detects whether it is possible to ship logs directly to the backup repository or Veeam Backup & Replication must use the log shipping server. When the transaction log backup job session ends, the component is stopped and removed from the VM guest OS. When a new session starts, the component is installed on the VM guest OS again.

The transaction logs backup is performed in the following way:

1. Veeam Backup & Replication launches the parent backup job by schedule.
2. The parent backup job creates an image-level backup of a Microsoft SQL Server VM and stores it on backup repository.
3. A new session of the transaction log backup starts. Veeam Backup & Replication accesses the VM (directly or via the guest interaction proxy) and installs the runtime components for guest processing, database information collection and transaction log handing on the VM guest OS.
4. Veeam Backup & Replication detects what databases currently exist on the Microsoft SQL Server and maps this data with the information kept in the configuration database. This periodic mapping reveals the databases for which Veeam Backup & Replication must process transaction logs during this time interval.

The runtime component backs up transaction log files and stores them as a *.bak file to a temporary folder on the VM guest file system.

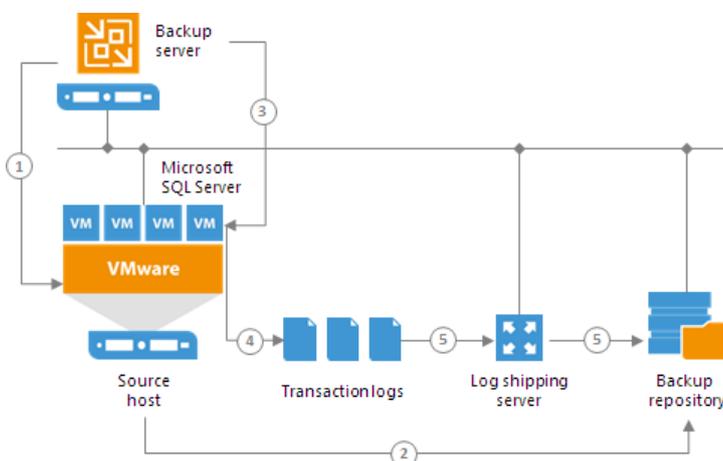
5. Veeam Backup & Replication transports transaction log backup copies from the temporary folder on the Microsoft SQL Server VM to the backup repository, either directly or via the log shipping server, and saves them as VLB files. As soon as copies of transaction log backups are saved to the backup repository, transaction log backups in the temporary folder on the Microsoft SQL Server VM are removed.

The session of the transaction log backup job remains working until the next start of the parent backup job. When a new session of the parent job starts, the transaction log backup job stops the current session and then starts a new session, performing steps 1-5.

Transaction logs that for some reason were not processed during the log backup interval remain in the temporary folder and are processed during the next log backup interval. To detect these remaining logs, Veeam Backup & Replication enumerates log files in the temporary folder.

NOTE:

If a new session of the transaction log backup starts and the parent backup job has not created a new restore point yet, the transaction log backup job will remain in the idle state, waiting for a new restore point to be created.



Retention for Transaction Log Backups

Transaction log backups are stored in files of the proprietary Veeam format – VLB. Veeam Backup & Replication keeps transaction log backups together with the VM image-level backup. The target location of VLB files depend on the type of the backup repository:

- If you store the VM image-level backup on a backup repository, Veeam Backup & Replication writes transaction log backups to the same folder where files of the image-level backup reside.
- If you store the VM image-level backup on a scale-out backup repository, Veeam Backup & Replication writes transaction log backups to the extent where the latest incremental backup file of the VM image-level backup is stored.

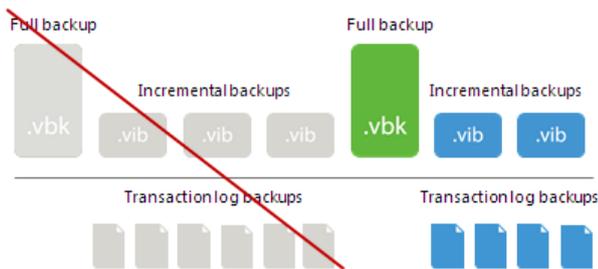
Veeam Backup & Replication removes transaction log backups by retention. You can choose one of the following retention methods:

- [Retain logs according to the image-level backup](#)
- [Retain logs for the specified number of days](#)

Retain Logs with Image-Level Backup

By default, Veeam Backup & Replication retains transaction log backups together with the corresponding image-level backup of the Microsoft SQL Server VM. When Veeam Backup & Replication removes a restore point of the image-level backup from the backup chain, it also removes a chain of transaction logs relating to this image-level backup.

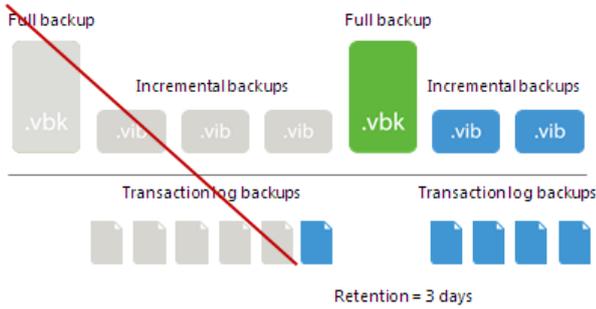
This method allows you to have both the image-level backup and necessary transaction log backups at hand. If you need to recover a database to some state, you can restore the Microsoft SQL Database from the necessary restore point and perform transaction log replay to bring the database to the desired state.



Retain Logs for a Number of Days

You can instruct Veeam Backup & Replication to keep transaction logs only for a specific period of time. This retention setting can be used, for example, if you want to save on storage space and plan to retain transaction log backups for the last few days. In this case, you will be able to restore the database only to one of the most recent states.

If you select this retention method, you must make sure that retention policies for the image-level backup and transaction log backup are consistent. The restore point of the image-level backup must always be preserved. If a backup of the database itself is missing, you will not be able to perform transaction log replay.



Log Shipping Servers

For every Microsoft SQL Server VM whose transaction logs you want to back up, Veeam Backup & Replication defines how to ship logs to the backup repository. Transaction logs can be shipped in the following ways:

- If it is possible to establish a direct connection between the VM guest OS and backup repository, log files will be shipped directly from the VM guest OS to the backup repository. This is the optimal method, as it does not involve additional resources and puts less load on the VM guest OS.
- Otherwise, files will be shipped via log shipping servers. You can instruct Veeam Backup & Replication to choose a log shipping server automatically from the list of available ones, or to use a specific server.

Note that if direct connection is possible, files will be always transferred from VM guest to repository directly (regardless of the configured log shipping server, as this server will not be involved). This approach helps to optimize performance at file transfer.

A log shipping server is a Microsoft Windows server added to the backup infrastructure. You can explicitly define what servers you want to use for log shipping or instruct Veeam Backup & Replication to automatically choose an optimal log shipping server. Veeam Backup & Replication chooses the log shipping server based on two criteria: possible data transfer methods and location of the Microsoft SQL Server VMs and log shipping server.

Data Transfer Methods

Log shipping servers can transport data in two ways:

- Over the network. In this scenario, Veeam Backup & Replication obtains files from the VM guest OS and transfers them over the network.
To offload the VM guest OS, logs are created one by one (not simultaneously). One log creation request is issued for every DB.
- Using VIX. In this scenario, Veeam Backup & Replication obtains transaction logs from the VM guest OS over the VIX, bypassing the network. For each Microsoft SQL Server instance one log creation request is created for all DBs (grouped by instance).

The default method is log shipping over the network.

Location of Log Shipping Server and VMs

When choosing a log shipping server for the job, Veeam Backup & Replication considers the location of the Microsoft SQL Server VM and log shipping server. Veeam Backup & Replication uses the following priority rules to select the log shipping server:

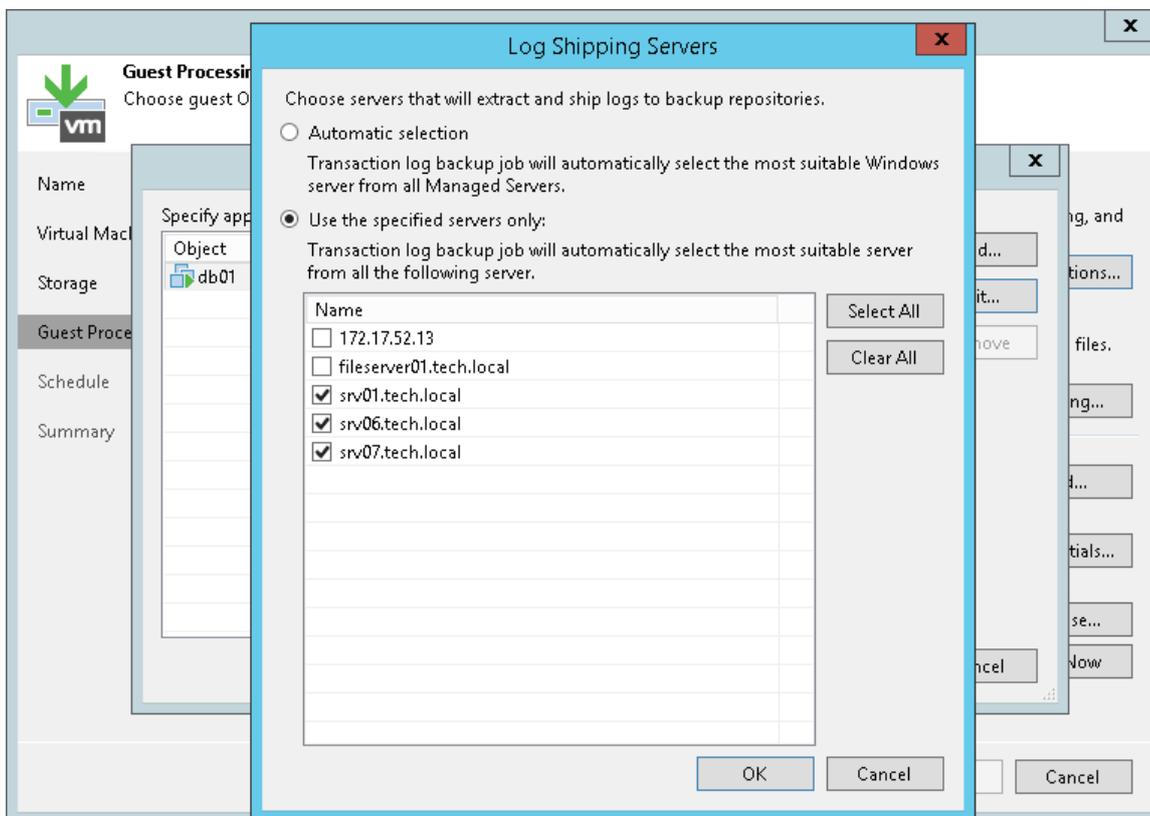
1. Log shipping server is located on the same ESX(i) host as the Microsoft SQL Server VM.
2. Log shipping server and Microsoft SQL Server VM are located in the same network.
3. Log shipping server and Microsoft SQL Server VM are located in different networks (the production infrastructure is isolated from the backup infrastructure).

That is, when choosing a log shipping server, Veeam Backup & Replication will give the top priority to a Microsoft Windows VM that is located on the same ESX(i) host as the Microsoft SQL Server VM and that has a network connection to the Microsoft SQL Server VM.

Log shipping servers are assigned per job session. When a new job session starts, Veeam Backup & Replication detects log shipping servers anew. Veeam Backup & Replication can also re-detect available servers during the job session. If a log shipping server becomes unavailable for some reason, Veeam Backup & Replication will fail over to another log shipping server.

IMPORTANT!

If you do not want to use some servers for transaction logs transport, you can manually define what server Veeam Backup & Replication must use as a log shipping server in the job settings. It is recommended that you assign the log shipping server role to a number of servers for availability purposes.



Transaction Log Backup Statistics

You can view the statistics of the transaction log backup job in the **History** view or in the **Home** view in Veeam Backup & Replication.

In the statistics window, you can examine the overall statistics for the transaction log backup job, as well as view per-VM information.

CRM Backup SQL Server Transaction Log Backup

Last period (all items)

Databases	RPO	Status
Protected: 28	SLA: 100%	Success: 1
Unprotected: 0	Misses: 0	Warning: 0
Excluded: 12	Max delay: 00:00	Errors: 0

Throughput (last 5 min)

Speed: 0.0 KB/s

NAME	STATUS
crm_db	Pending

Latest session

Duration:	02:15	Read:	16.3 MB
Bottleneck:	Log backup	Transferred:	3.2 MB

Last period

RPO	Sessions
SLA: 100%	Success: 1
Misses: 0	Warning: 0
Max delay: 00:00	Errors: 0

Duration	Log size
Average: 02:15	Average: 16.3 MB
Maximum: 02:15	Maximum: 16.3 MB
Sync interval: 05 min	Total: 16.3 MB

Errors Warnings Success

ACTION

ACTION	DURATION
Preparing guest for SQL Server transaction log backup	00:37
Using guest interaction proxy blizz (Same subnet)	
Enumerating SQL Server databases	00:01
Waiting for backup job to complete VSS freeze	00:51
Performing SQL Server transaction log backup for WSS_Content;SharePoint_AdminContent_6b79...	00:15
Skipping simple recovery model databases: Veeam Sample Database 1;Veeam Sample Database...	00:05
Saving 16.3 MB of transaction logs to backup repository	00:10
Transaction log backup completed at 123.7 KB/s with bottleneck: Log backup (Network)	
Waiting for transaction log backup interval to expire	00:38

Hide Details OK

In the upper part of the statistics window, Veeam Backup & Replication displays information about the transaction log backup job for all VMs included in the parent backup job.

The **Last period (all VMs)** section contains statistics data for the selected session of the backup job.

In the **Databases** column, you can view the following information:

- *Protected* – number of databases that were backed up at least once during the last session
- *Unprotected* – number of databases that failed to be backed up during the last session

- *Excluded* – databases excluded from processing. Databases may be excluded for the following reasons:
 - The database status is *Offline*
 - The database recovery model is set to *Simple*
 - The database is read-only
 - The database was deleted after the latest full backup
 - The database is added to the list of exclusions
 - The AutoClose property is enabled for the database

For more information, see <https://www.veeam.com/kb1051>, <https://www.veeam.com/kb2110> and <https://www.veeam.com/kb2104>.

NOTE:

Unprotected databases do not comprise *Excluded* databases, as they have different reasons for being non-processed.

In the **RPO** column, you can view the following information:

- *SLA value* – how many log backup intervals completed in time with successful log backup (calculated as percentage of total number of intervals).
- *Misses* – how many intervals were missed (number of intervals).
- *Max delay* – difference between the configured log backup interval and time actually required for log backup. If exceeded, a warning is issued.

In the **Status** column, the following information is displayed (per job): number of VMs processed successfully, with warnings or with errors.

The **Latest** session section displays the following information for the latest log processing interval for the selected VM:

- *Duration* – duration of log shipment from the VM guest OS to the backup repository since the current log processing interval has started
- *Bottleneck* – operation with the greatest duration in the last completed interval. The operation may have the following bottlenecks:

Display Name	Slowing-down Operation
Log backup	Saving BAK files to a temporary location on VM guest OS
Network	Uploading log files to the log shipping server
Target	Saving files to the target repository

- *Read* – amount of data read from the temporary folder on VM guest OS
- *Transferred* – amount of data transferred to the target repository

The **Last period** section displays the following statistics of log backups per VM for the latest session of the transaction log backup job:

- The **RPO** column displays statistics on log processing interval (calculated as described above)

- The **Sessions** column includes statistics of log backups per VM, calculated as follows:
 - *Success* – number of intervals when all database logs were backed up successfully
 - *Warning* – number of sequential intervals with failed log processing (if not more than 4 intervals in a sequence)
 - *Errors* – number of sequential intervals with failed log processing (more than 4 intervals in a sequence)
- The **Duration** column includes the following information:
 - *Average* – average duration of log data transfer (through all intervals in the session)
 - *Max* – maximal duration of log data transfer (through all intervals in the session)
 - *Sync interval* – duration of periodic intervals specified for log backup in the parent job settings (default is 15 min)
- The **Log size** column displays the following information:
 - *Average* – average amount of data read from the VM guest OS through all intervals
 - *Max* – maximal amount of data read from the VM guest OS over all 15-min intervals
 - *Total* – total amount of data written to the backup repository

NOTE:

- Statistics on transaction log processing is updated periodically, simultaneously for the parent backup job and transaction log backup job.
- For Always On Availability groups, Veeam Backup & Replication collects logs only from one node. Thus, in reports, the status of database replicas will be the same for all nodes (Protected or Excluded).

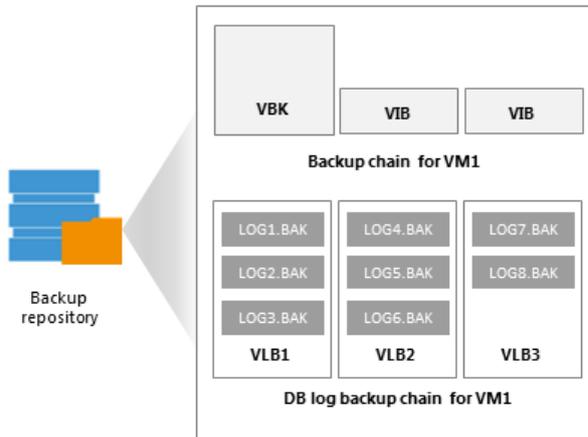
Log Files

At each start of the SQL Server backup job (parent), a new .VLB is created to store log backups in the repository:

- If the **Use per-VM backup files** option is selected for the repository, then Veeam Backup & Replication will create a separate .VLB for each server processed by the job.
- If this option is cleared, then a single .VLB will be created for all servers processed by the job.

For example, if a job processes only one SQL Server, the repository will contain a number of .VLB files for it (a so-called chain).

As described in the section above, during database log backup (child) job session, transaction log backup is performed by native means of the SQL Server and stored as .BAK file to a temporary folder on the SQL Server VM guest file system. Then Veeam Backup & Replication copies .BAK file to the current .VLB in the repository. When the new parent job session starts, another .VLB is created, and the .BAK files that appear after that will be stored there during the child job session. The resulting chain of .VLBs will look like shown below, depicted for a single SQL Server VM1:



Total number of all LOG<N>.BAK files stored at the moment in all VLBs is reported as a **number of restore points for the child job** that backs up database logs. So, in the example above, the log backup job for SQL Server VM1 has created 8 restore points by the moment.

In the Veeam Backup & Replication console this number of restore points for the log backup job can be seen in the **Restore Points** column of the preview pane.

Support for AlwaysOn Availability Groups

AlwaysOn Availability Groups allow you to increase fault tolerance between active and hot-standby databases without involving shared physical disks, which is quite important for virtualization of Microsoft SQL Servers. Veeam Backup & Replication supports AlwaysOn Availability Groups for virtualized Microsoft SQL Server 2012 or later.

Image-level Backup of Microsoft SQL Server VMs

During image-level backup of a Microsoft SQL Server VM, Veeam Backup & Replication requests and analyzes information about databases that are included in the AlwaysOn Availability Groups. Depending on the retrieved information, Veeam Backup & Replication creates a VSS snapshot with or without *COPY_ONLY* flag. The *VSS_BS_COPY* flag for VSS snapshot is triggered if the VM represents a secondary node for at least one AlwaysOn Availability Group.

Veeam Backup & Replication also detects to what cluster the database belongs. If the backup job does not include all VMs from the cluster, an information message will be issued.

Retrieved information is saved for further log identification.

Transaction Log Backup

Transaction log backup can be performed only for those databases that were successfully backed up, either on the primary or on the secondary node of AlwaysOn Availability Group.

The transaction logs processing interval may be the same or may differ through VMs included in AlwaysOn Availability Group. If the interval is different, Veeam Backup & Replication will use minimal value (by default, 15 minutes).

At each log processing interval, Veeam Backup & Replication chooses the AlwaysOn Availability Group node for which transaction logs will be backed up.

Logs are backed up from one node of the AlwaysOn Availability Group. To become a subject for log backup, the node must meet the following criteria:

- Required Veeam Backup & Replication components can be installed on this node (the VM must be running).
- If there are any logs remaining in the temporary folder on the node of AlwaysOn Availability Group, this means these logs were not backed up to the backup repository during the previous session of the transaction log backup job, so this AlwaysOn Availability Group node must be processed first.
- Databases in the AlwaysOn Availability Groups for this node were successfully backed up for the last two processing intervals.
- Veeam Backup & Replication can establish a network connection to the node or VIX connection, if a connection over the network cannot be established
- The VM is in the list of preferred nodes for backup retrieved from the Microsoft SQL Server. If there are no preferred nodes, any node can be chosen.

NOTE:

When configuring a backup job to process Distributed Availability Groups transaction logs, select either primary or the secondary distributed availability group. Otherwise, the log chain of the distributed group databases might become inconsistent. When configuring a backup job to back up transaction logs for other Distributed Availability Groups, use the Perform copy only mode. See [Application-Aware Processing](#) to learn more about the copy only mode. You can also use the exclude feature to prevent Guest-OS database from being processed. See [Exclude Objects from Backup Job](#) to learn more on excluding objects. To read about distributed availability group limitations, see [Configure distributed availability group](#).

Oracle Logs Backup and Restore

Veeam Backup & Replication supports backup of Oracle database archived logs and restore of Oracle databases.

Database archived logs are created by the Oracle system. The Oracle database can run in one of the following logging modes:

- ARCHIVELOG turned on – logs are saved and can be used for recovery purposes.
- ARCHIVELOG turned off – no logs are saved. This mode is not recommended as it does not provide for proper disaster recovery.

With ARCHIVELOG turned on, the Oracle system stores database archived logs to a certain location on the VM guest OS, as specified by the database administrator. Veeam Backup & Replication allows you to set up the following ways of log handling:

- Instruct the backup job to collect log files from the Oracle VM and ship them to the backup repository where they are stored next to image-level backups of the Oracle VM.
- Skip log processing – log files remain untouched on the Oracle VM and are preserved within the image-level backup.

If you enable application-aware processing for an Oracle VM, during the job session Veeam Backup & Replication installs a runtime process on this VM to collect information about the database and process archived logs according to job settings. Application-specific settings are configured at the **Guest Processing** step of the backup job wizard – you can specify how logs should be backed up and/or deleted for Oracle databases.

Requirements for Archived Log Backup

- Veeam Backup & Replication supports archived logs backup and restore for Oracle database version 11 and later. The Oracle database may run on a Microsoft Windows VM or Linux VM.
- Automatic Storage Management (ASM) is supported for Oracle 11 and later.
- Oracle Express Databases are supported if running on Microsoft Windows machines only.
- The database must run in the ARCHIVELOG mode.

Archived Log Backup Jobs

To back up archived logs, you must create a backup job, add Oracle VMs to it and specify advanced settings for archived logs backup in the job settings. The resulting job will comprise two jobs:

- Parent backup job – the backup job that creates an image-level backup of the Oracle VM. The parent backup job is named *<job_name>*, for example, *Daily Job*. You can configure the parent job in the Veeam Backup & Replication console just like any other backup job.
- Child job – an archived log backup job. To form a name of the child job, Veeam Backup & Replication adds a suffix to the name of the parent backup job: *<parent_job_name> + Oracle Backup*, for example, *Daily Job Oracle Backup*. Veeam Backup & Replication automatically creates the child job if it detects a backup job that is scheduled to back up at least one Oracle VM, and archived log backup is enabled for this job. Session data of the archived log backup job is stored in the configuration database and displayed in the Veeam Backup & Replication console.

The parent job runs in a regular manner – it starts by schedule or is started manually by the user. The archived log backup job is triggered by the parent backup job. This sequence ensures that the VM (and the database) restore point is present when you need to use archived logs to restore the database.

Sessions of Archived Log Backup Jobs

The archived log backup job runs permanently in the background, shipping archived logs to the backup repository at a specific time interval (by default, every 15 minutes). A sequence of time intervals between sessions of the parent backup job makes up a session of the archived log backup job.

The archived log backup session starts and stops in the following way:

- The initial session starts when the parent backup job schedule is enabled. After that, the session starts with every new session of the parent backup job.
- The session ends before the next session of the parent backup job or when this parent backup job is disabled.
- When the session ends, Veeam Backup & Replication stops the runtime process and uninstalls it from the VM guest OS. When a new session starts, the runtime process is deployed again.

How Oracle Archived Log Backup Works

The archived logs backup for Oracle VMs is performed in the following way:

1. Veeam Backup & Replication launches the parent backup job by schedule.
2. The parent backup job creates an image-level backup of the Oracle VM and stores this backup to the backup repository.
3. A new session of the archived log backup starts. Veeam Backup & Replication accesses the VM guest OS to perform guest processing, collect database information and handle archived log.

If Oracle runs on a Microsoft Windows server, Veeam Backup & Replication accesses the VM guest OS over a guest interaction proxy. You can instruct Veeam Backup & Replication to select the guest interaction proxy automatically or assign it explicitly.

By default, Veeam Backup & Replication accesses the VM guest OS over the network:

- For Linux VM guest OS – using SSH.
- For Microsoft Windows VM guest OS – using RPC.

If a network connection cannot be established, Veeam Backup & Replication accesses the VM guest OS over VIX.

4. Veeam Backup & Replication deploys the runtime process in the VM guest OS. The runtime process scans the Oracle system and collects information about databases whose logs must be processed, including:

- List of all databases
- Database state – a database is on or off, in which logging mode it runs
- Paths to all database files (configuration logs and so on) and other data required for backup

Veeam Backup & Replication also detects whether it is possible to store logs to the backup repository through a direct access or a log shipping server is required.

The runtime process copies archived log files from the log archive destination (set by the Oracle administrator) to a temporary folder on the VM guest file system.

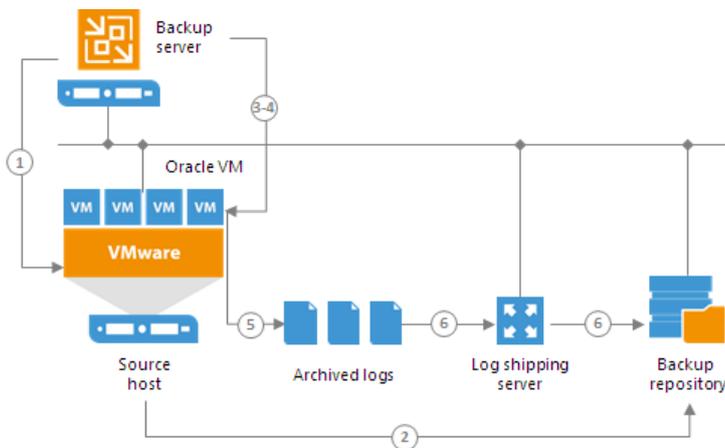
5. Veeam Backup & Replication maps information about the Oracle system collected at step 4 with information kept in the configuration database. This periodic mapping helps reveal databases for which Veeam Backup & Replication must ship archived logs to the backup repository during this time interval.

6. Archived log backup files are transferred from the temporary location on the Oracle VM to the backup repository, either directly or via the log shipping server. The source-side Veeam Data Mover compresses log data to be transferred according to its built-in settings. On the backup repository side, data is compressed according to the parent backup job settings.

Archived logs that for some reason were not processed during the log backup interval remain in the temporary folder and are processed during the next log backup interval. To detect these remaining logs, Veeam Backup & Replication enumerates log files in the temporary folder.

NOTE:

If a new session of the archived log backup starts and the parent backup job has not created a new restore point yet, the archived log backup job will remain in the idle state, waiting for a new restore point to be created.



Retention for Archived Log Backup

Archived log backups are stored in files of the proprietary Veeam format – VLB. Veeam Backup & Replication keeps archived log backups together with the VM image-level backup. The target location of VLB files depend on the type of the backup repository:

- If you store the VM image-level backup on a backup repository, Veeam Backup & Replication writes archived log backups to the same folder where files of the image-level backup reside.
- If you store the VM image-level backup on a scale-out backup repository, Veeam Backup & Replication writes archived log backups to the extent where the latest incremental backup file of the VM image-level backup is stored.

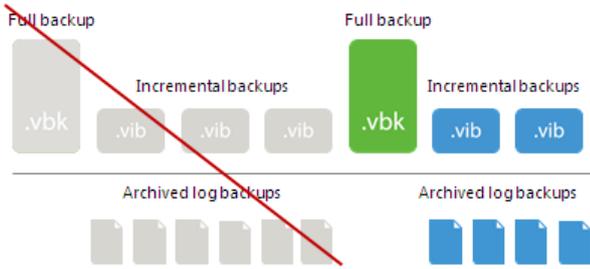
Veeam Backup & Replication removes archived log backups by retention. You can choose one of the following retention methods:

- [Retain logs according to the image-level backup](#)
- [Retain logs for the specified number of days](#)

Retain Logs with Image-Level Backup

By default, Veeam Backup & Replication retains archived log backups together with the corresponding image-level backup of the Oracle VM. When Veeam Backup & Replication removes a restore point of the image-level backup from the backup chain, it also removes a chain of archived logs relating to this image-level backup.

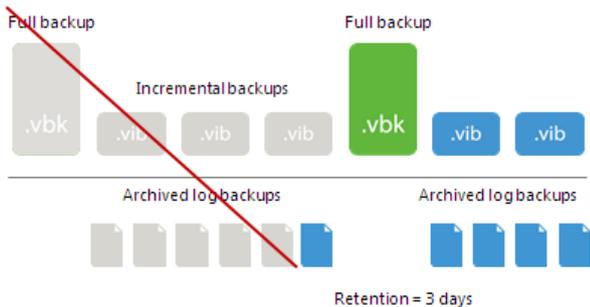
This method allows you to have both the image-level backup and necessary archived log backups at hand. If you need to recover a database to some state, you can restore the Oracle VM from the necessary restore point and use archived logs to bring the database to the desired state.



Retain Logs for a Number of Days

You can instruct Veeam Backup & Replication to keep archived logs only for a specific period of time. This retention setting can be used, for example, if you want to save on storage space and plan to retain archived log backups for the last few days. In this case, you will be able to restore the database only to one of the most recent states.

If you select this retention method, you must make sure that retention policies for the image-level backup and archived log backup are consistent. The restore point of the image-level backup must always be preserved. If a backup of the database itself is missing, you will not be able to use archived logs.



Log Shipping Servers

For every Oracle VM whose archived logs you want to back up, Veeam Backup & Replication defines how to ship logs to the backup repository. Archived logs can be transported in the following ways:

- Directly from the VM guest OS to the backup repository. This method is recommended – it does not involve additional resources and puts less load on the VM guest OS.
- Via log shipping servers. If it is not possible to establish a direct connection between the VM guest OS and backup repository, you can configure Veeam Backup & Replication to use a log shipping server.

A log shipping server is a Microsoft Windows or Linux server added to the backup infrastructure. You can explicitly define what servers you want to use for log shipping or instruct Veeam Backup & Replication to automatically choose an optimal log shipping server. Veeam Backup & Replication chooses the log shipping server based on two criteria: possible data transfer methods and location of the Oracle VM and log shipping server.

Data Transfer Methods

Log shipping servers can transport data in two ways:

- Over the network. In this scenario, Veeam Backup & Replication obtains files from the VM guest OS and transfers them over the network.
- Over VIX. In this scenario, Veeam Backup & Replication obtains archived logs from the VM guest OS over the VIX, bypassing the network.

The default method is log shipping over the network.

Location of Log Shipping Server and VMs

When choosing a log shipping server for the job, Veeam Backup & Replication considers the location of the Oracle VM and log shipping server. Veeam Backup & Replication uses the following priority rules to select the log shipping server:

1. Log shipping server is located on the same ESX(i) host as the Oracle VM.
2. Log shipping server and Oracle VM are located in the same network.
3. Log shipping server and Oracle VM are located in different networks (the production infrastructure is isolated from the backup infrastructure).

That is, when choosing a log shipping server, Veeam Backup & Replication will give the top priority to a VM that is located on the same ESX(i) host as the Oracle VM and that has a network connection to the Oracle VM

Log shipping servers are assigned per job session. When a new job session starts, Veeam Backup & Replication detects log shipping servers anew. Veeam Backup & Replication can also re-detect available servers during the job session. If a log shipping server becomes unavailable for some reason, Veeam Backup & Replication will fail over to another log shipping server.

In the statistics window, you can examine the overall statistics for the archived log backup job, as well as view per-VM information.

Backup Job RH Oracle 11 _95U2 Oracle Redo Log Backup

Last period (all VMs)

Databases		RPO		Status	
Protected:	2	SLA:	50%	Success:	0
Unprotected:	1	Misses:	1	Warning:	1
Excluded:	1	Max delay:	00:00	Errors:	0

Throughput (last 5 min)

Time	Read	Write	Transfer

NAME	STATUS
RH 6.4 Or...	Pending

Latest session

Duration:	0:00:00	Read:	1.2 MB
Bottleneck:	N/A	Transferred:	466.3 KB

Last period

RPO		Sessions	
SLA:	50%	Success:	1
Misses:	1	Warning:	1
Max delay:	00:00	Errors:	0

Duration		Log size	
Average:	00:58	Average:	655.8 MB
Maximum:	01:34	Maximum:	1.3 GB
Sync interval:	15 min	Total:	1.3 GB

Errors **Warnings** **Success**

ACTION ↓	DURATI...
Redo log backup interval is 15 minutes	
Backed up 1.3 GB of redo logs for 2 databases: asmorcl2;orcl1 at 13.9 MB/s with bottleneck: Target (N...	
New redo log backup interval started at 6/5/2017 7:14:34 AM	
Enumerating Oracle databases	0:00:02
Performing Oracle redo log backup for orcl1;asmorcl2	
Saving 1.2 MB of redo logs to backup repository	0:00:05
⚠ Skipping VM asmorcl1 because its state was reverted, perform new image level backup first	
Redo log backup completed at 50.3 KB/s with bottleneck: Target (Network)	
⌚ Waiting for redo log backup interval to expire	0:09:36

Hide Details OK

In the upper part of the statistics window, Veeam Backup & Replication displays information about the log backup job for all VMs included in the parent backup job.

The **Last period (all VMs)** section contains statistics data for the selected session of the backup job.

In the **Databases** column, you can view the following information:

- *Protected* – number of databases that were backed up at least once during the last session
- *Unprotected* – number of databases that failed to be backed up during the last session
- *Excluded* – databases excluded from processing. Databases may be excluded for the following reasons: ARCHIVELOG mode is turned off for the database (the database is in NOARCHIVELOG mode), database was deleted after the latest full backup, or database was added to the list of exclusions.

NOTE:

Unprotected databases do not comprise **Excluded** databases, as they have different reasons for being non-processed. See also <https://www.veeam.com/kb2114> for information on processing databases in NOARCHIVE mode.

In the **RPO** column, you can view the following information:

- *SLA* – how many log backup intervals completed in time with successful log backup (calculated as percentage of total number of intervals).
- *Misses* – how many intervals failed to complete in time with successful log backup (number of intervals).
- *Max delay* – difference between the configured log backup interval and time actually required for log backup. If exceeded, a warning is issued.

In the **Status** column, the following information is displayed (per job): number of VMs processed successfully, with warnings or with errors.

The **Latest session** section displays the following information for the latest log processing interval for the selected VM:

- *Duration* – duration of log shipment from the VM guest OS to the backup repository since the current log processing interval has started
- *Bottleneck* – operation with the greatest duration in the last completed interval. The operation may have the following bottlenecks:

Display Name	Slowing-down Operation
Log backup	Saving archived log files to a temporary location on VM guest OS (to work around, see the Veeam KB article: https://www.veeam.com/kb2093)
Network	Uploading log files to the log shipping server
Target	Saving files to the target repository

- *Read* – amount of data read from the temporary folder on VM guest OS
- *Transferred* – amount of data transferred to the target repository

The **Last period** section displays the following statistics of log backups per VM for the latest session of the log backup job:

- The **RPO** column displays statistics on log processing interval (calculated as described above)
- The **Sessions** column includes statistics of log backups per VM, calculated as follows:
 - *Success* – number of intervals when all database logs were backed up successfully
 - *Warning* – number of sequential intervals with failed log processing (if not more than 4 intervals in a sequence)
 - *Errors* – number of sequential intervals with failed log processing (more than 4 intervals in a sequence)

- The **Duration** column includes the following information:
 - *Average* – average duration of log data transfer (through all intervals in the session)
 - *Maximum* – maximal duration of log data transfer (through all intervals in the session)
 - *Sync interval* – duration of periodic intervals specified for log backup in the parent job settings (default is 15 min)
- The Log size column displays the following information:
 - *Average* – average amount of data read from the VM guest OS through all intervals
 - *Maximum* – maximal amount of data read from the VM guest OS over all 15-min intervals
 - *Total* – total amount of data written to the backup repository

The pane below shows all actions performed during the job run. To filter out actions with the certain status, use the **Errors**, **Warnings** and **Success** buttons.

NOTE:

Statistics on archived log processing is updated periodically, simultaneously for the VM backup job (parent) and archived log backup job (child job).

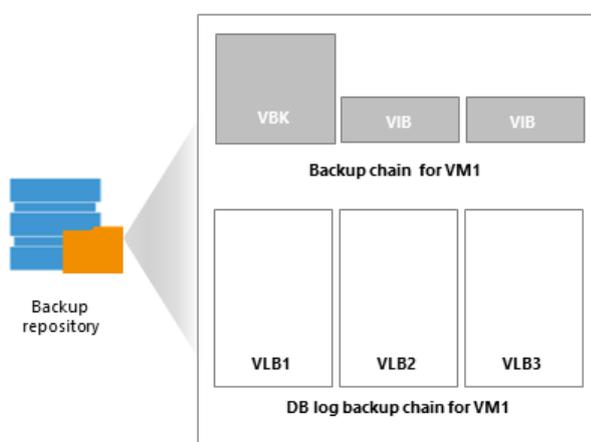
Log Files

At each start of the Oracle backup job ('parent'), a new .VLB is created to store log backups in the repository:

- If the **Use per-VM backup files** option is selected for the repository, then Veeam will create a separate .VLB for each server processed by the job.
- If this option is cleared, then a single .VLB will be created for all servers processed by the job.

For example, if a job processes only one Oracle server, the repository will contain a number of .VLB files for it (a so-called chain).

As described in the section above, during database log backup ('child') job session, log archiving is performed by native means of the Oracle server. Archived logs are stored to a temporary folder on the Oracle VM guest file system. Then Veeam copies archived log to the current .VLB in the repository. When the new 'parent' job session starts, another .VLB is created, and the archived log files that appear after that will be stored there during the 'child' job session. The resulting chain of .VLBs will look like shown below, depicted for a single Oracle VM1:



Total number of all archived logs files stored at the moment in all VLBs is reported as **a number of restore points for the 'child' job** that backs up database logs. So, in the example above, the log backup job for Oracle VM1 has created 8 restore points by the moment.

Backup Job Scheduling

You can start backup jobs manually or schedule them to start automatically at specific time. Veeam Backup & Replication lets you configure the following settings for the job:

- [Scheduling settings](#)
- [Job retry settings](#)
- [Backup window settings](#)

Automatic Startup Schedule

To run a job periodically without user intervention, you can schedule the job to start automatically. The Veeam Backup Service running on the backup server continuously checks configuration settings of all jobs configured on the backup server, and starts them according to their schedule.

Veeam Backup & Replication lets you configure the following scheduling settings for jobs:

- [You can schedule jobs to run at specific time every day or on selected days](#)
- [You can schedule jobs to run periodically at specific time intervals](#)
- [You can schedule jobs to run continuously](#)
- [You can chain jobs](#)

Jobs Started at Specific Time

You can schedule jobs to start at specific time daily, on specific week days or monthly on selected days.

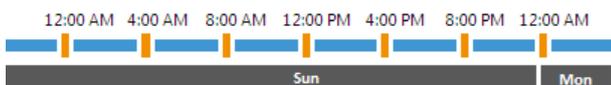
This type of schedule requires that you define the exact time when the job must be started. For example, you can configure the job to start daily at 10:00 PM or every first Sunday of the month at 12:00 AM.



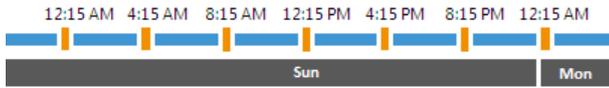
Jobs Started at Specific Time Intervals

You can schedule jobs to start periodically throughout a day at a specific time interval. The time interval between job sessions can be defined in minutes or hours. For example, you can configure a job to start every 30 minutes or every 2 hours.

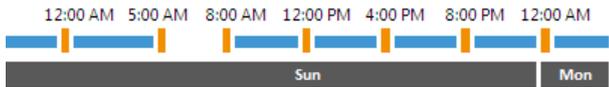
For periodically run jobs, reference time is midnight (12:00 AM). Veeam Backup & Replication always starts counting defined intervals from 12:00 AM, and the first job session will start at 12:00 AM. For example, if you configure a job to run with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.



If necessary, you can specify an offset for periodically run jobs. The offset is an exact time within an hour when the job must start. For example, you can configure the job to start with a 4-hour interval and specify offset equal to 15 minutes. In this case, the job will start at 12:15 AM, 4:15 AM, 8:15 AM, 12:15 PM, 4:15 PM, 8:15 PM, 12:15 AM and so on.

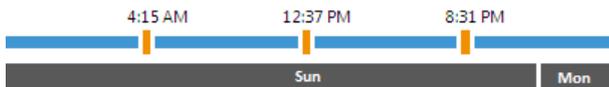


If a session of a periodically run job does not fit into the specified time interval and overlaps the next planned job session, Veeam Backup & Replication starts the next backup job session at the nearest scheduled interval. For example, you set up a job to run with a 4-hour interval. The first job session starts at 12:00 AM, takes 5 hours and completes at 5:00 AM. In this case, Veeam Backup & Replication will start a new job session at 8:00 AM.



Jobs Run Continuously

You can schedule the job to run continuously – that is, in a non-stop manner. A new session of a continuously running job starts as soon as the previous job session completes. Continuously run jobs can help you implement near-continuous data protection (near-CDP) for the most critical applications installed on VMs.



Chained Jobs

In the common practice, data protection jobs configured in the virtual environment start one after another: when job *A* finishes, job *B* starts and so on. You can create a chain of jobs using scheduling settings. To do this, you must define the start time for the first job in the chain. For other jobs in the chain, you must select the **After this job** option and choose the preceding job from the list.

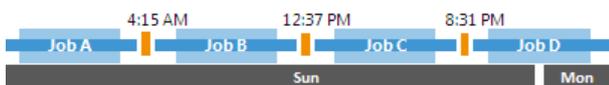
Job chaining is not limited to jobs of specific type only. You can create a chain of jobs of different types. For example, you can:

1. Set a backup job as the first job in the chain.
2. Configure a SureBackup job and chain with the backup job. In this case, Veeam Backup & Replication will automatically verify a backup file created with the backup job after the backup job completes.

NOTE:

If you start the initial job manually, Veeam Backup & Replication will offer you to start jobs chained to it as well. Click **Yes** to start the whole job chain or **No** to start only the first job in the chain.

If you start the initial job manually and chain another job to it while the initial job is running, the chained job will not start when the initial job completes.



Recommendations on Job Chaining

You should use job chaining wisely. Job chaining removes guesswork from job scheduling but has a number of drawbacks:

- You cannot predict precisely how much time the initial job will require and when jobs chained to it will start. Depending on the situation, the job schedule may shift, and some operations may even not be performed as planned.

For example, you configure 2 jobs:

- *Job 1* is scheduled to start at 10:00 PM daily and typically takes 1 hour.
- *Job 2* is scheduled to start after *Job 1* daily. Synthetic full backup is scheduled on Saturday.

Imagine that *Job 1* starts on Saturday and runs for 2.5 hours instead of 1 hour. *Job 2* will then start after midnight on Sunday, and the synthetic full backup planned on Saturday will not be created.

- Errors in job sessions may cause the job schedule to shift. For example, if the initial job in the chain fails, Veeam Backup & Replication will attempt to retry it, and the schedule for chained jobs will shift.
- Load on backup infrastructure resources may be not balanced. Some slots on backup proxies and backup repositories may be available but will not be used since jobs are queued to run one by one. And if you use a backup repository that supports multiple I/O streams, its resources will not be used efficiently.

Instead of job chaining, you can balance the load on backup infrastructure components. To do this, you must limit the number of concurrent tasks on backup proxies and backup repositories. For more information, see [Limiting the Number of Concurrent Tasks](#).

Job Retry

You can instruct Veeam Backup & Replication to retry a job several times if the initial job pass fails. By default, Veeam Backup & Replication automatically retries a failed job for 3 times within one job session. If necessary, however, you can define a custom number of retries in the job settings.

Veeam Backup & Replication retries a job only if the previous job session has failed, and one or several VMs in the job have not been processed. Veeam Backup & Replication does not perform a retry if a job session has finished with the *Success* or *Warning* status. During the job retry, Veeam Backup & Replication processes only those VMs that have failed.

IMPORTANT!

Veeam Backup & Replication does not perform automatic retry for jobs that were started or stopped manually.

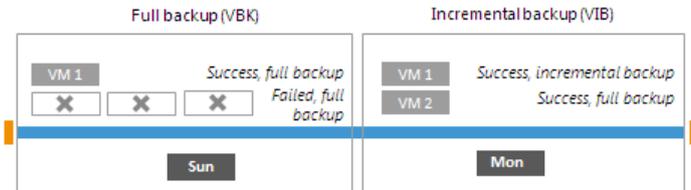
Veeam Backup & Replication always creates one backup file within one job session. If a job processes several VMs and some of them fail to be processed during the first job pass, Veeam Backup & Replication will create a backup file containing data for those VMs that have been successfully processed. During a job retry, Veeam Backup & Replication will attempt to process failed VMs. In case of success, Veeam Backup & Replication will write data of processed VMs to the backup file that was created at the initial job pass.

In some situations, Veeam Backup & Replication may fail to process VMs during all job retries. In this case, failed VMs will be processed during the next job session. Their data will be written to the backup file created within the current job session.

For example, you have configured a job for 2 VMs: *VM 1* and *VM 2*. The job uses the forward incremental method.

During the first job session, Veeam Backup & Replication successfully processed *VM 1* and created a full backup file for it. *VM 2* has failed to be processed during all 3 job retries. In this case, Veeam Backup & Replication will attempt to process the failed *VM 2* within the next job session. Data for *VM 2* will be written to the backup file created within this job session, which will be an incremental backup. As a result, at the end of the second backup job session, you will have 2 files:

- Full backup file containing a full restore point for *VM 1*
- Incremental backup file containing a full restore point for *VM 2* and an incremental restore point for *VM 1*



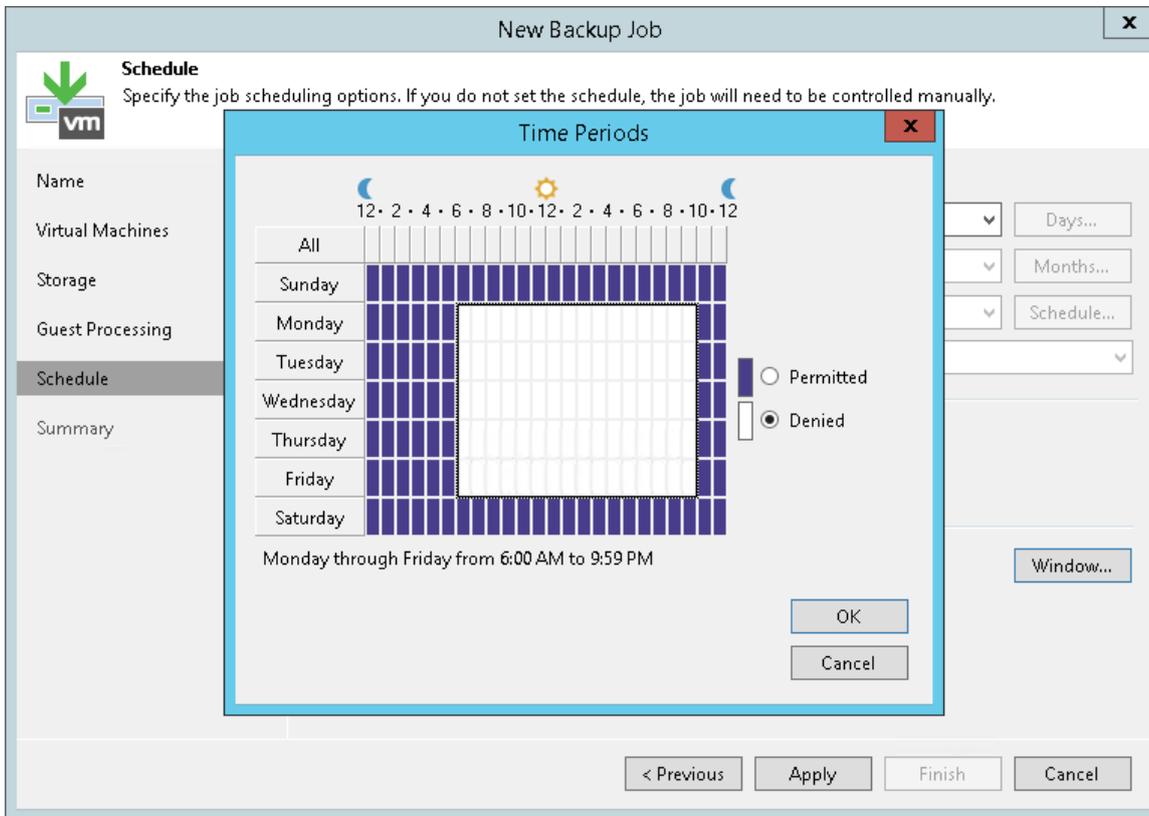
Backup Window

If necessary, you can specify a backup window for jobs. The backup window is a period of time on week days when jobs are permitted to run. If the job exceeds the allowed window, Veeam Backup & Replication will automatically terminate it.

The backup window can be helpful if you do not want data protection jobs to produce unwanted overhead for the production environment or do not want jobs to overlap production hours. In this case, you can define the time interval during which the job must not run.

IMPORTANT!

The backup window affects only the data transport process and health check operations. Other transform operations can be performed on the target repository outside the backup window.

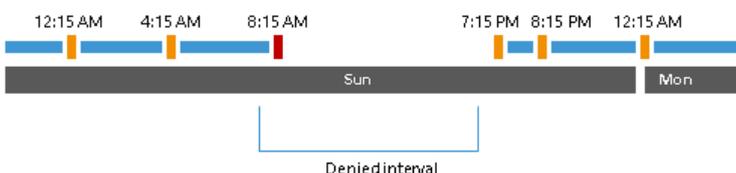


Backup Window for Periodically Run Jobs

If you define the backup window for a job that runs periodically at specific time intervals, Veeam Backup & Replication will immediately start the job after the denied window is over. All subsequent backup job sessions will be performed according to specified scheduling settings.

For example, you have configured a job to run with a 4-hour interval with an offset of 15 minutes. The allowed backup window for the job is 7:00 PM to 8:00 AM. Veeam Backup & Replication will run this job in the following way:

1. The first job session will start at 12:15 AM (since midnight is a reference time for periodically run jobs).
2. The next job session will start at 4:15 AM.
3. The job session at 8:15 AM will not be performed as it falls into the denied period of the backup window.
4. The next job session will start immediately after the denied period is over: at 7:15 PM.
5. After that, Veeam Backup & Replication will run the job by the defined schedule: at 8:15 PM, 12:15 AM and so on.

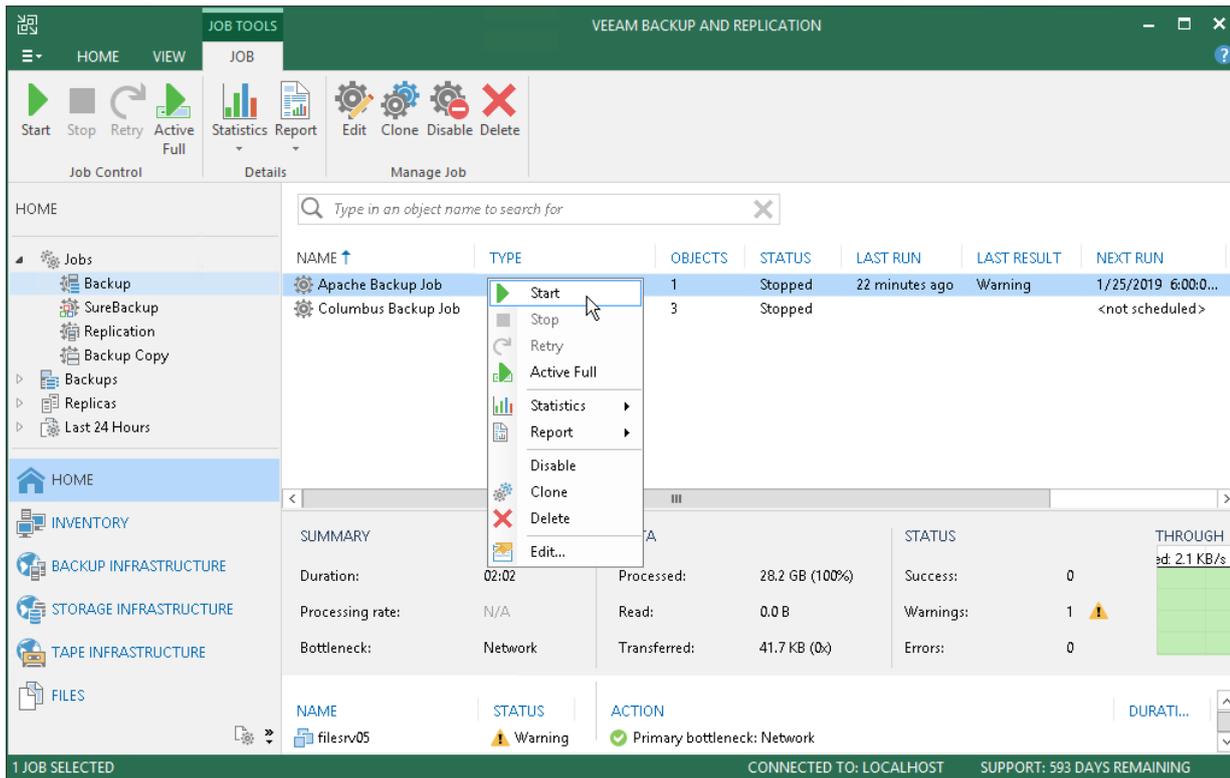


Manual Start of Backup Jobs

You can start jobs manually if you need to capture VM data at a specific point in time and do not want to re-configure job scheduling settings. For example, you can start a job to create a VM backup before you install new software on a VM or enable a new feature.

When you start the job manually, Veeam Backup & Replication runs a regular job session that produces a new restore point in the backup chain on the backup repository.

To start and stop jobs configured on the backup server, you can use the **Start** and **Stop** buttons on the ribbon or corresponding commands in the shortcut menu.



Manual Stop of Backup Jobs

You can stop job execution at any moment of time. For example, you can stop a job if the job processes several VMs but the workload appears to be greater than you expected. Or you can stop the job if there is not enough time to finish the job session.

You can stop a job in 2 ways:

- [You can stop the job immediately](#). In this scenario, Veeam Backup & Replication terminates the job session and does not create a new restore point for VMs that are currently processed.
- [You can stop the job gracefully](#). In this scenario, Veeam Backup & Replication creates a restore point for the VMs that are currently processed and then terminates the job session.

Immediate Stop of Jobs

Immediate job stop terminates the job session instantly. The job finishes with the following results:

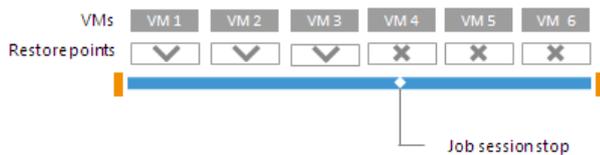
- VMs that Veeam Backup & Replication has succeeded to process by the time you stop the job will have new restore points.

- VMs that Veeam Backup & Replication is currently processing and VMs that Veeam Backup & Replication has not started to process will not have new restore points.

When you stop a job session immediately, Veeam Backup & Replication performs the following operations:

1. If a snapshot for a VM has already been created, Veeam Backup & Replication instructs VMware vSphere to remove the snapshot.
2. Veeam Backup & Replication terminates all job processes and tasks. The job is finished with the *Failed* error.

All restore points created with the previous job sessions remain untouched. You can use them for restore operations.



Graceful Stop of Jobs

Graceful job stop instructs Veeam Backup & Replication that it must create restore points for VMs that are currently being processed, and then terminate the job. The job finishes with the following results:

- VMs that Veeam Backup & Replication has succeeded to process and VMs that are being processed will have new restore points.
- VMs that Veeam Backup & Replication has not started to process will not have new restore points.

You can use graceful job stop for the following types of jobs:

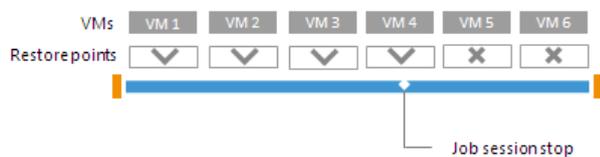
- Backup jobs
- VM copy jobs
- Replication jobs

You cannot use graceful job stop for the following types of jobs:

- File copy jobs
- Backup copy jobs
- Quick migration job (during quick migration, Veeam Backup & Replication processes all VMs in one task)
- Restore operations

VMs added to the job are processed in the order defined in job settings. Information about VMs that have already been processed and VMs that are being processed is displayed in job details.

If you stop the job gracefully before Veeam Backup & Replication starts processing the first VM in the job, the job will be finished with the *Failed* error. You will see the message *Operation was canceled by user* in job details.



Health Check for Backup Files

You can instruct Veeam Backup & Replication to periodically perform a health check for the latest restore point in the backup chain. During the health check, Veeam Backup & Replication performs a CRC check for metadata and a hash check for VM data blocks in the backup file to verify their integrity. The health check helps make sure that the restore point is consistent, and you will be able to restore data from this restore point.

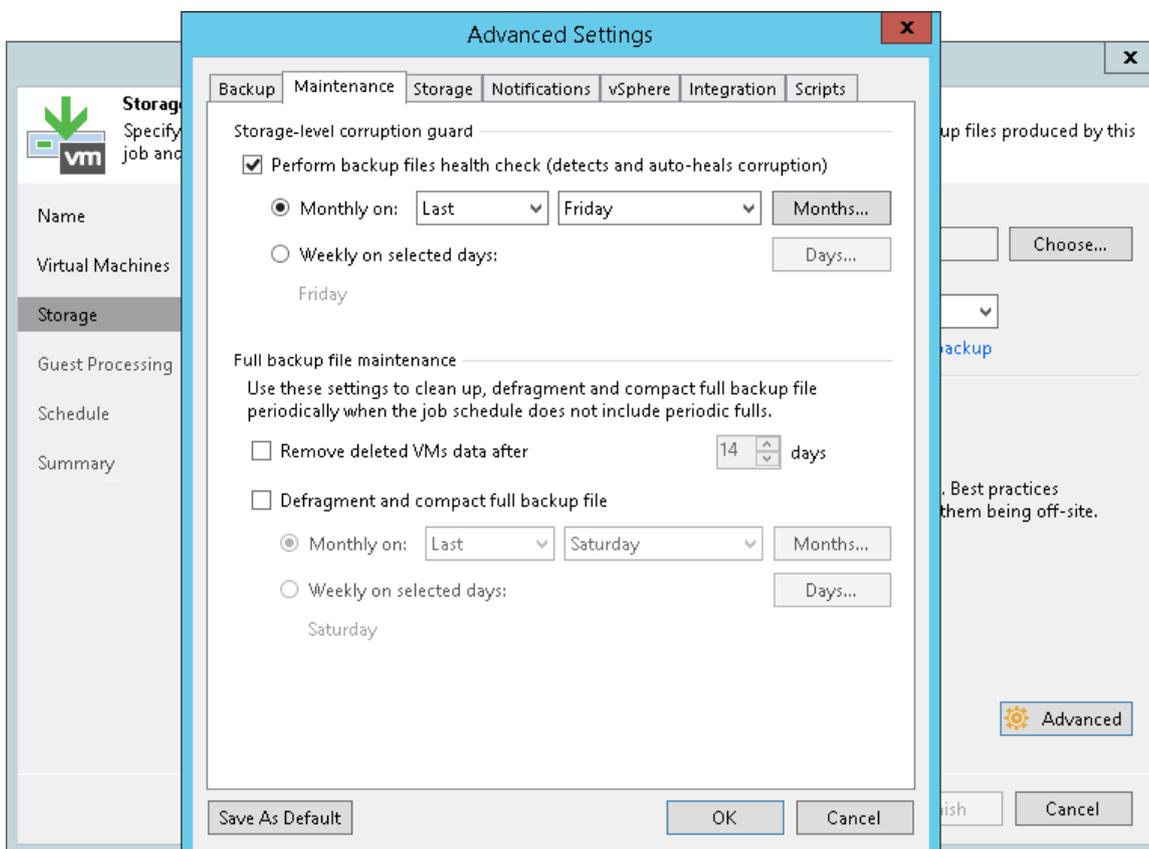
The health check can be performed for all types of backup chains:

- Forever forward incremental
- Forward incremental
- Reverse incremental backup chains

To run the health check periodically, you must enable the **Perform backup files health check** option in the backup job settings and define the health check schedule. By default, the health check is performed on the last Friday of every month. You can change the schedule and run the health check weekly or monthly on specific days.

NOTE:

Veeam Backup & Replication performs the health check during the first job session on the day when the health check is scheduled. If another job session runs on the same day, Veeam Backup & Replication will not perform the health check during this job session. For example, if the job is scheduled to run several times on Saturday, and the health check is scheduled on Saturday, the health check will only be performed during the first backup job session on Saturday.



Verification Content

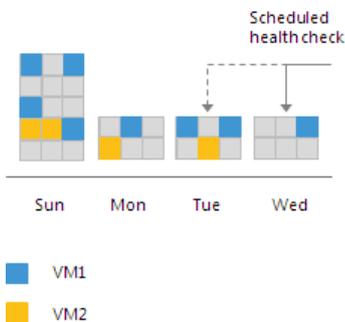
The health check always verifies only the latest restore point in the backup chain. In case of forever forward incremental and forward incremental backup chains, if the latest restore point is incomplete, the health check verifies the restore point preceding the latest one.

Bear in mind that the health check procedure verifies not the latest backup file in the backup chain, but the latest restore point for a VM. The latest restore point corresponds to the state of the VM at the date and time when the latest backup file for this VM was created. Data blocks that are required to "compose" the VM latest state are typically spread out across several backup files in the backup chain. Therefore, to verify the latest state of the VM, Veeam Backup & Replication must open several backup files in the backup chain and read data blocks from these backup files. For this reason, the health check procedure may take long.



The health check verifies only those virtual disks of a VM that are available in the latest restore point. For example, you added a VM with 3 virtual disks to a backup job. The VM was backed up Sunday through Tuesday. On Wednesday, you removed 1 virtual disk, and Veeam Backup & Replication run the health check for the VM. During the health check, Veeam Backup & Replication will verify only the 2 remaining virtual disks.

The health check verifies only those VMs that are available in the latest restore point. For example, you added 2 VMs to a backup job and run the job for some time. The health check verified 2 VMs. If you remove 1 VM from the backup job, the next scheduled health check run will verify the latest unverified restore point for the removed VM, and the latest restore point for the remaining VM. In future, the health check will verify only the restore point for the remaining VM in the job.



Limitations for Health Check

- The health check is not performed during an active full backup job session started manually or automatically by schedule.
- The health check is not performed for offloaded restore points. For more information, see [Capacity Tier](#).
- [For per-VM backup chains] If you add a new VM to an existing backup job that has been run for some time, Veeam Backup & Replication will perform the health check for it during the next incremental backup job session for the added VM.

How Health Check Works

When Veeam Backup & Replication saves a new restore point to the backup repository, it calculates CRC values for backup metadata and hash values for data blocks of VM disk in the backup file, and saves these values in the metadata of the backup file, together with VM data. During the health check session, Veeam Backup & Replication uses these values to make sure that a verified restore point is consistent.

NOTE:

If you perform health check for encrypted backup files, Veeam Backup & Replication will pass encryption keys to the regular backup repository or cloud repository. For more information on encryption, see [Data Encryption](#).

Veeam Backup & Replication uses different mechanisms of health check for different types of backup chains:

- [Forever forward incremental and forward incremental backup chains](#)
- [Reverse incremental backup chains](#)
- [Mixed backup chains \(chains containing forward incremental and reverse incremental restore points\)](#)

Forever Forward Incremental and Forward Incremental Backup Chains

The health check for forward incremental backup chains is performed in the following way:

1. At the end of the backup job session, Veeam Backup & Replication performs the health check. It calculates CRC values for backup metadata and hash values for VM disks data blocks in the backup file and compares them with the CRC and hash values that are already stored in the backup file.

During the health check, Veeam Backup & Replication verifies the latest restore point in the backup chain (restore point created with the current backup job session – the session during which the health check is performed). If the latest restore point in the backup chain is incomplete, Veeam Backup & Replication checks the restore point preceding the latest one.

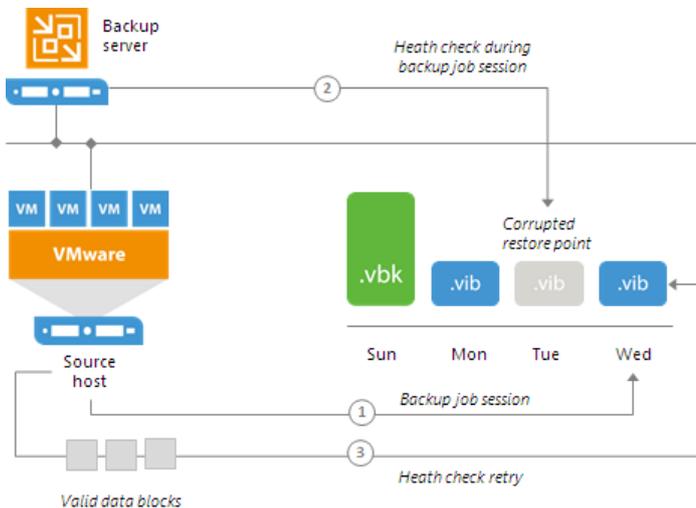
2. If the health check does not detect data corruption, the backup job session completes in a regular way.

If the health check detects corrupted data, Veeam Backup & Replication completes the backup job with the *Error* status and starts the health check retry process. The health check retry starts as a separate backup job session.

Depending on the revealed data corruption, Veeam Backup & Replication performs the following actions:

- If the health check has detected corrupted backup metadata in the full backup file, Veeam Backup & Replication marks the backup chain starting from this full restore point as corrupted in the configuration database. During the health check retry, Veeam Backup & Replication transports data blocks of the whole VM image from the source datastore, creates a new full backup file on the backup repository and saves transported data blocks to it.
- If the health check has detected corrupted backup metadata in the incremental backup file, Veeam Backup & Replication removes information about this incremental restore point and subsequent incremental restore points from the configuration database. During the health check retry, Veeam Backup & Replication transports incremental data relatively the latest valid restore point in the backup chain from the source datastore, creates a new incremental backup file on the backup repository and saves transported data blocks to it.

- If the health check has detected corrupted VM disk blocks in the full or incremental backup file, Veeam Backup & Replication marks the restore point that includes the corrupted data blocks and subsequent incremental restore points as corrupted in the configuration database. During the health check, Veeam Backup & Replication transports data blocks from the source datastore. In addition, Veeam Backup & Replication transports data blocks that have changed since the backup job session that has triggered the health check. Veeam Backup & Replication stores these data blocks to the latest restore point that has been created with the current backup job session (session that has triggered the health check retry).



Reverse Incremental Backup Chains

In case of reverse incremental backup chains, the health check always verifies only the latest restore point in the backup chain, which is always a full backup file.

The health check is performed in the following way:

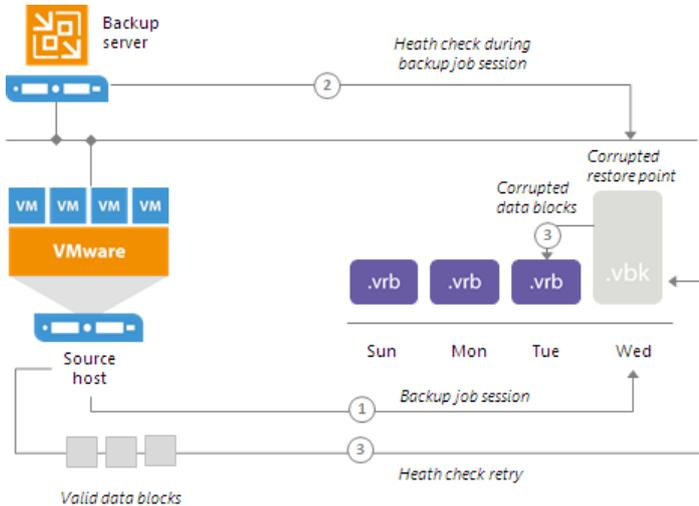
1. At the end of the backup job session, Veeam Backup & Replication verifies the full backup file. Veeam Backup & Replication calculates CRC values for backup metadata and hash values for VM disks data blocks in the full backup file, and compares them with the CRC and hash values that are already stored in the full backup file.
2. If the health check does not detect data corruption, the backup job session completes in a regular way.

If the health check detects corrupted data, Veeam Backup & Replication completes the backup job with the *Error* status and starts the health check retry process. The health check retry starts as a separate backup job session.

Depending on the revealed data corruption, Veeam Backup & Replication performs the following actions:

- If the health check has detected corrupted backup metadata in the full backup file, Veeam Backup & Replication marks the whole backup chain (full backup file and preceding reverse incremental backup files) as corrupted in the configuration database. During the health check retry, Veeam Backup & Replication transports data blocks of the whole VM image from the source datastore, creates a new full backup file on the backup repository and saves transported data blocks to it.

- If the health check has detected corrupted VM disk blocks in the full backup file, Veeam Backup & Replication marks the full backup file and preceding reverse incremental backup files as corrupted in the configuration database. During the health check retry, Veeam Backup & Replication transports data blocks from the source datastore. In addition, Veeam Backup & Replication transports data blocks that have changed since the backup job session that has triggered the health check. Veeam Backup & Replication stores these data blocks to the existing full backup file on the backup repository. Corrupted data blocks that have been replaced with data blocks from the source datastore are stored to an existing reverse incremental backup file preceding the full backup file.



Mixed Backup Chains

If you enable the **Transform previous backup chains into rollback** option in the job settings, Veeam Backup & Replication creates a mixed backup chain that contains two types of incremental backup files – reverse incremental backup files (VRB) and forward incremental backup files (VIB). In case of mixed backup chains, Veeam Backup & Replication performs a health check only the forward incremental part of the backup chain. The reverse incremental part of the backup chain is not verified. However, if Veeam Backup & Replication detects corrupted data blocks metadata or VM disk data blocks in the full backup file, it marks preceding reverse incremental backup files as corrupted in the configuration database.

Health Check Retries

The health check itself is started during the backup job session or the job retry session if the backup job session has failed. If attempts are not successful, Veeam Backup & Replication performs the health check during the last job retry in any case.

If the health check detects corrupted data, Veeam Backup & Replication completes the backup job with the *Error* status and starts the health check retry process. The health check retry starts as a separate backup job session. During the health check retry, Veeam Backup & Replication attempts to transport data blocks for the corrupted restore point from the source datastore.

For scheduled jobs, the number of health check retries is equal to the number of job retries specified in the job settings. For jobs started manually, Veeam Backup & Replication performs 1 health check retry.

NOTE:

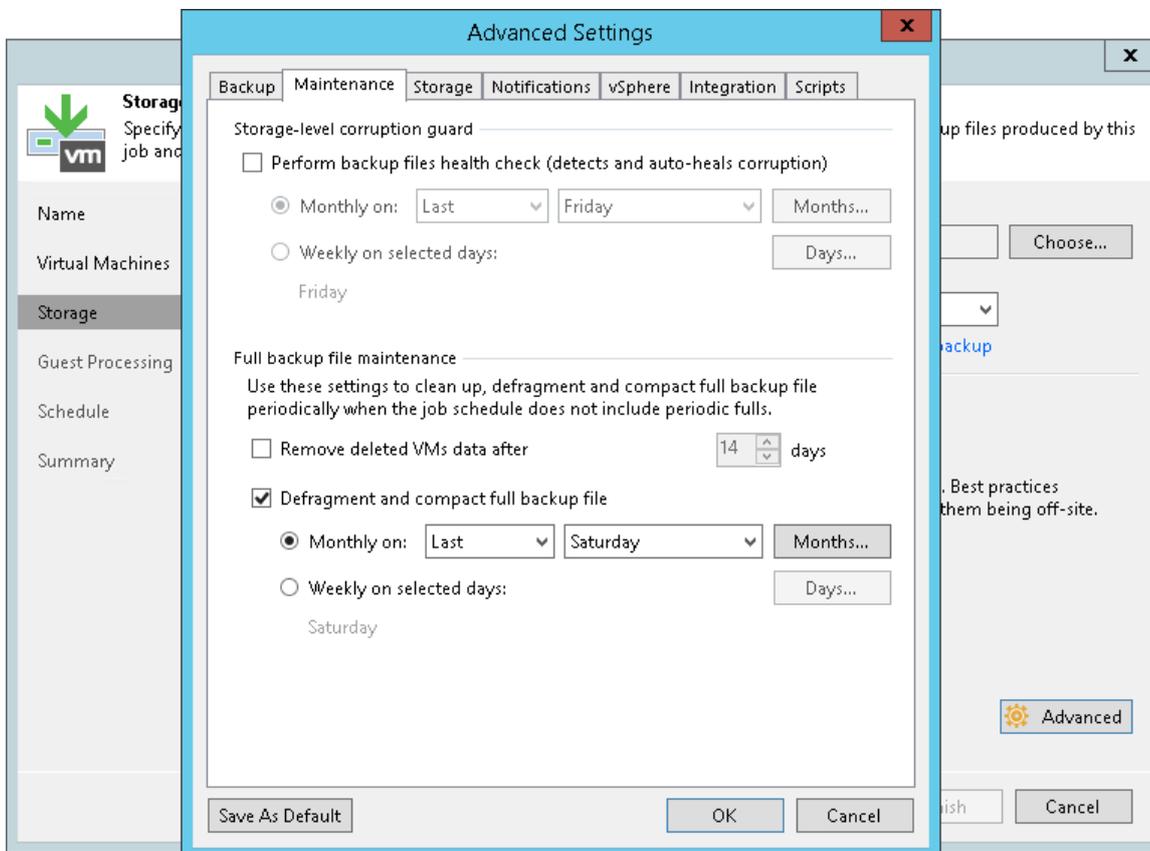
If Veeam Backup & Replication fails to fix the corrupted data during all health check retries, you must retry the job manually. In this case, Veeam Backup & Replication will transport the required data blocks from the source datastore to fix the latest restore point. If the latest restore point in the backup chain is incomplete, Veeam Backup & Replication will attempt to fix the restore point preceding the latest one.

Compact of Full Backup File

If you use a forever forward incremental or reverse incremental backup method, the backup job constantly transforms the full backup file in the backup chain to meet retention policy settings. The transformation process, however, has a side effect. In the long run, the full backup file grows large and gets badly fragmented. The file data occurs to be written to non-contiguous clusters on disk, and operations of reading and writing data from and to the backup file slow down.

To resolve the fragmentation problem, you can instruct Veeam Backup & Replication to compact the full backup file periodically. During the file compact operation, Veeam Backup & Replication creates a new empty file and copies to it data blocks from the full backup file. As a result, the full backup file gets defragmented and the speed of reading and writing from and to the file increases.

To compact the full backup file periodically, you must enable the **Defragment and compact full backup file** option in the backup job settings and define the compact operation schedule. By default, the compact operation is performed on the last Saturday of every month. You can change the compact operation schedule and instruct Veeam Backup & Replication to perform it weekly or monthly on specific days.



Limitations for Full Backup File Compact

The full backup file compact has the following limitations:

- The **Defragment and compact full backup file** option can be enabled only for backup jobs for which active full and synthetic full backups are not scheduled.
- The compact full backup file operation is not performed during backup job sessions that produce active full backups. If the backup job starts again on the same day when the active full backup was created, Veeam Backup & Replication does not perform the compact full backup operation. This limitation helps reduce the number of backup operations – Veeam Backup & Replication considers that the full backup is recent and does not need to be rebuilt.

If such situation occurs, Veeam Backup & Replication triggers the full backup file compact operation during the next backup job session that produces an incremental backup file on another day.

- The compact full backup file operation is not performed for offloaded full backup files. For more information, see [Capacity Tier](#).
- The backup repository must have enough space to store a file of the full backup size. During the compact process, Veeam Backup & Replication creates auxiliary files that exist on the backup repository until the end of the compact operation.
- [For per-VM backup chains] If you add a new VM to an existing backup job that has been run for some time, Veeam Backup & Replication will perform the compact full operation for it during the next incremental backup job session for the added VM.
- If you change the block size in backup job settings, Veeam Backup & Replication does not change the block size in the compacted backup file till the next full backup. However, if you change compression settings in backup job settings, during the next compact file operation Veeam Backup & Replication changes the compression level for the compacted backup file.

Removal of Deleted VMs Data

During the compact operation, Veeam Backup & Replication does not copy all data blocks from the VBK file to the newly created file. It copies only data blocks of VMs whose information is stored in the configuration database. For example, if the VM is removed from the backup job, its data is not copied to the new full backup file. This approach helps reduce the size of the full backup file and remove unnecessary data from it.

VM Data Take Out

If the full backup file contains data for a VM that has only one restore point and this restore point is older than 7 days, during the compact operation Veeam Backup & Replication will extract data for this VM from the full backup file and write this data to a separate full backup file. Such backup will be displayed under the **Backups > Disk** (imported) node in the **Home** view.

The mechanism works if the following conditions are met:

- The **Remove deleted VMs data** option is not enabled in the backup job settings.
- The **Use per-VM backup files** option is not enabled in backup repository settings.

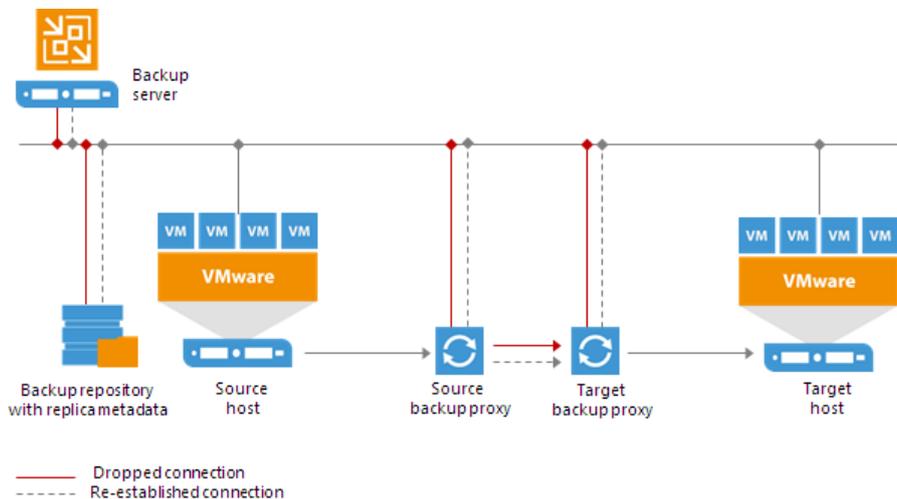
Resume on Disconnect

Veeam Backup & Replication can handle a situation of an unstable network during backup, backup copy and replication jobs. If a network connection drops for a short period of time during the data transport process, Veeam Backup & Replication automatically resumes the dropped network connection. The data transfer process starts from the point when the connection was lost. The resume on disconnect capability improves the reliability of remote data transfer, reduces the backup window and minimizes the network load.

Veeam Backup & Replication automatically re-establishes a connection between the following backup infrastructure components engaged in the data transfer process:

- Backup server
- Backup proxies
- Backup repository

Resume on disconnect works only for dropped network connections. Veeam Backup & Replication attempts to resume the connection with an interval of 15 seconds during 30 minutes. If the problem has any other nature, Veeam Backup & Replication retries the job in a regular manner.



Veeam Backup & Replication does not create a new restore point on resume: VM data is written to the same restore point that was created for the current job session. When resuming the data transfer process, Veeam Backup & Replication regards VM disks, not the whole VM.

For example, a VM has two disks: *disk A* and *disk B*. Before the connection dropped, Veeam Backup & Replication managed to transfer 20 GB of *disk A* and did not start transferring *disk B*. After the connection is re-established, Veeam Backup & Replication will start transferring the data for *disk A* from the 20 GB point; data of the whole *disk B* will be transferred anew.

Snapshot Hunter

The Snapshot Hunter is a Veeam technology used to detect and remove orphaned snapshots that may remain after backup or replication job sessions.

The Snapshot Hunter addresses the problem of “phantom” snapshots. Under some circumstances, VMware vSphere can report a successful removal of a snapshot but the snapshot actually remains on the datastore.

Phantom snapshots can take substantial space on the datastore or impact VM performance. They can even cause the production VMs to stop if the datastore runs out of free space.

To solve the problem of phantom snapshots, Veeam Backup & Replication starts the Snapshot Hunter during each backup or replication job session. The Snapshot Hunter looks for snapshot files not registered in vSphere. If there are no orphaned files, the Snapshot Hunter stops. If orphaned snapshot files are detected, the Snapshot Hunter removes them in the background mode.

The Snapshot Hunter runs in jobs that use VMware VM snapshots:

- Backup jobs: regular backup and backup from storage snapshots
- Replication jobs (the source VM snapshot): regular replication, replication from storage snapshots
- VeeamZIP

NOTE:

During Snapshot Hunter analysis, Veeam Backup & Replication skips VMware vCloud Director VMs.

How Snapshot Hunter Works

A temporary snapshot of the VM is taken and then removed during every backup or replication job session. To remove the snapshot, Veeam Backup & Replication triggers the VMware snapshot consolidation mechanism that includes two steps:

1. VMware vSphere removes the snapshot from the VM snapshots list.
2. VMware vSphere consolidates the data written to the delta file with the VM disks.

The problem occurs when the snapshot was removed successfully but the consolidation failed. This may happen, for example, if the files appear to be locked when VMware vSphere attempts to consolidate the snapshot files. In this case, the files remain on datastore.

The Snapshot Hunter is started as a separate process scheduled within every job session. The discovery of the phantom snapshots does not affect the job: if the phantom snapshots are discovered, the Veeam Backup Service schedules the snapshot consolidation, and the job runs in normal way.

Veeam Backup & Replication checks the datastore to discover orphaned snapshot files. To consolidate these files with the VM disks, Veeam Backup & Replication calls a consolidation algorithm. The algorithm consists of three steps, each representing a VMware method.

1. VMware Consolidate method

As a first attempt, Veeam Backup & Replication calls the VMware Snapshot Consolidate method. This method is the same mechanism that VMware vSphere uses for VMs with the *Needs Consolidation* status.

2. Hard consolidation without quiesce

If the first attempt fails, Veeam Backup & Replication creates a new snapshot and calls the VMware

Delete all snapshots method. As a result, all VM snapshots and associated files are deleted. The snapshot is taken without quiescing the VM.

3. Hard consolidation with quiesce

If the snapshot deletion still fails, Veeam Backup & Replication implies another VMware method that creates a quiesced snapshot and then removes all VM snapshots.

NOTE:

Hard consolidation without quiesce and hard consolidation with quiesce are performed only if the VM does not have any user snapshots. In case there are one or more user snapshots, these steps will not be performed.

The 3-steps consolidation procedure is launched up to 4 times with a 4-hour interval.

In case all four attempts fail, Veeam Backup & Replication sends an e-mail notification informing that the user needs to manually troubleshoot the problem. Note that you need to have the global email notifications option enabled. For more information, see [Specifying Email Notification Settings](#).

The Snapshot Hunter considers the backup window set for the job. If any of the attempts does not fit the backup window, Veeam Backup & Replication will not perform the consolidation and send the e-mail notification.

You can view information on the Snapshot Hunter sessions on the **History > System** view in the Veeam Backup & Replication console.

In case no consolidation attempt could fit the backup window, the warning appears in the job statistics.

Creating Backup Jobs

To back up VMs, you must configure a backup job. The backup job defines how, where and when to back up VM data. One job can be used to process one or more VMs.

You can configure a backup job and start it immediately or save the job and run it later. Jobs can be started manually or scheduled to run automatically at specific time.

Before creating a backup job, [check prerequisites](#). Then use the **New Backup Job** wizard to configure the backup job.

Before You Begin

Before you create a backup job, check the following prerequisites:

- Backup infrastructure components that will take part in the backup process must be added to the backup infrastructure and properly configured. These include ESX(i) hosts on which VMs are registered, backup proxy and backup repository.
- The backup repository must have enough free space to store created backup files. To receive alerts about low space on the backup repository, configure global notification settings. For more information, see [Specifying Other Notification Settings](#).
- For VM guest OS indexing on Linux-based VMs, a user account with root privileges on the VM is required. It is recommended that you create a separate user account for work with Veeam Backup & Replication on the Linux-based VM, grant root privileges to this account and specify settings of this account at the **Guest Processing** step of the **New Backup Job** wizard.
- If you plan to map a backup job to a backup file that already exists on the backup repository, you must perform the rescan operations for this backup repository. Otherwise, Veeam Backup & Replication will not be able to recognize backup files on the backup repository. For more information, see [Rescanning Backup Repositories](#).
- If you plan to configure a secondary destination for the backup job, you can create a backup copy job or backup to tape job beforehand. The backup copy job or backup to tape job can have an empty source, that is, can be not linked to any backup job. For more information, see [Creating Backup Copy Jobs](#) and [Creating Backup to Tape Jobs](#).
- If you plan to use pre-job and post-job scripts and/or pre-freeze and post-thaw scripts, you must create scripts before you configure the backup job.
- To back up Microsoft SQL transaction logs with Veeam Backup & Replication, you must make sure that the recovery model is set to *Full* or *Bulk-logged* recovery model for required databases on Microsoft SQL Server VMs. If the recovery model is set to *Simple*, Veeam Backup & Replication will not detect and process transaction logs on Microsoft SQL Server VMs.
- Veeam Backup & Replication excludes from application-aware processing Microsoft SQL databases that are mounted to the Microsoft SQL Server using a remote UNC path. If at least one file of the database is located on a network shared folder, this database will be backed up in the crash-consistent state. Other databases on this server will be backed up in the transactionally consistent state. For more information, see <https://www.veeam.com/kb1879>.
- By default, system databases (master, model, msdb) are skipped from transaction log processing and are not a part of the Veeam Explorer for Microsoft SQL Server restore workflow. To recover these databases, you can use file-level restore.

If you want to exclude other databases from the transaction log processing workflow, refer to this Veeam Knowledge Base article: <https://www.veeam.com/kb2104>. (Consider that exclusion configured this way will be treated as a global setting.)
- To back up Oracle transaction logs with Veeam Backup & Replication, you must make sure that ARCHIVELOG is turned on for required databases on Oracle VMs. If ARCHIVELOG is turned off, Veeam Backup & Replication will not detect and process transaction logs on Oracle VMs.

Mind the following:

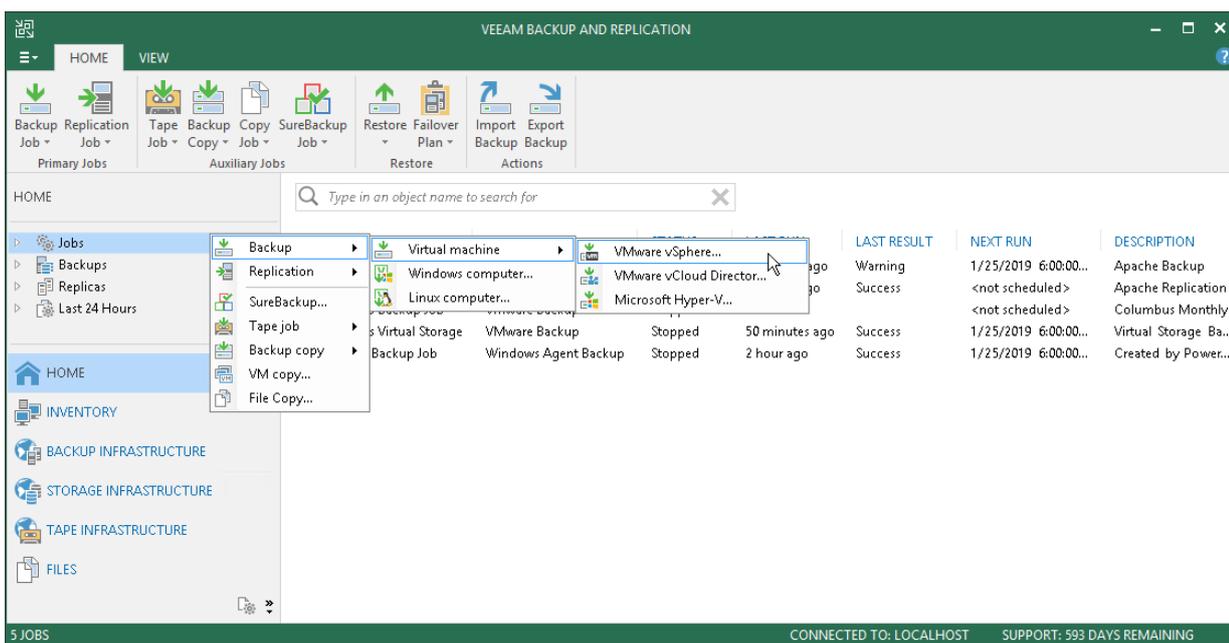
- If you plan to periodically perform maintenance operations with backup files, mind the following limitations: [Health Check for Backup Files](#), [Retention Policy for Deleted VMs](#), [Compact of Full Backup File](#).
- Due to Microsoft limitations, you cannot use Microsoft Azure Active Directory credentials to perform guest processing on VMs running Microsoft Windows 10.

- [For Dell EMC Data Domain backup repository] The length of forward incremental and forever forward incremental backup chains that contain one full backup and a set of subsequent incremental backups cannot be greater than 60 restore points. To overcome this limitation, schedule full backups (active or synthetic) to split the backup chain into shorter series. For example, to perform backups at 30-minute intervals, 24 hours a day, you must schedule synthetic fulls every day. In this scenario, intervals immediately after midnight may be skipped due to the duration of synthetic processing. For more information, see [How Synthetic Full Backup Works](#).
- If you assign the role of a backup proxy to a VM, you should not add this VM to the list of processed VMs in a job that uses this backup proxy. Such configuration may result in degraded job performance. Veeam Backup & Replication will assign this backup proxy to process other VMs in the job first, and processing of this VM itself will be put on hold. Veeam Backup & Replication will report the following message in the job statistics: *VM is a backup proxy, waiting for it to stop processing tasks*. The job will start processing this VM only after the backup proxy deployed on the VM finishes its tasks.
- If you use tags to categorize virtual infrastructure objects, check limitations for VM tags. For more information, see [VM Tags](#).
- Veeam Backup & Replication supports backup of Microsoft Exchange, SharePoint and SQL Server databases existing in mount point volumes.

Step 1. Launch New Backup Job Wizard

To launch the **New Backup Job** wizard, do one of the following:

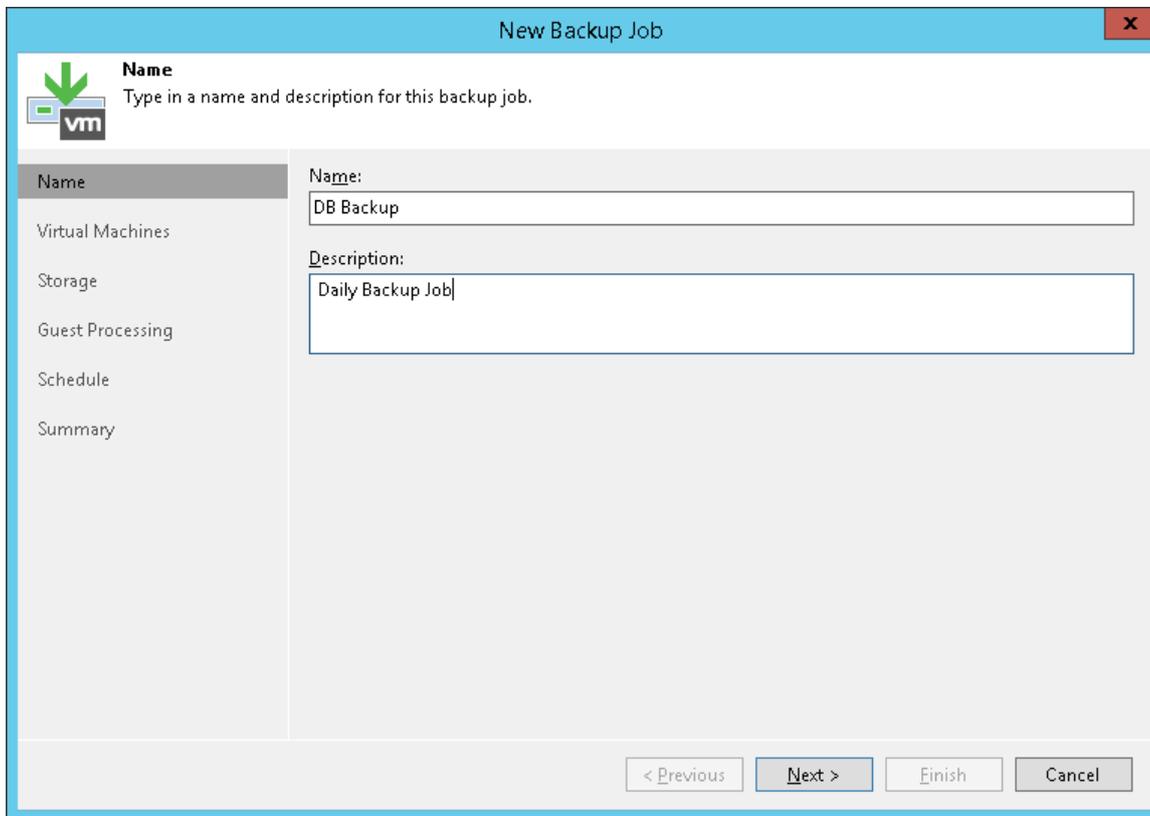
1. On the **Home** tab, click **Backup Job > Virtual machine > VMware vSphere**.
2. Open the **Home** view. In the inventory pane right-click **Jobs** and select **Backup > Virtual machine > VMware vSphere**.
3. Open the **Inventory** view. In the working area select the VMs, click **Add to Backup** on the ribbon and select **New job** or right-click the VMs and select **Add to backup job > New job**. Veeam Backup & Replication will start the **New Backup Job** wizard and add the VMs to this job. You can add other VMs to the job later on, when you pass through the wizard steps.
4. You can quickly add the VMs to an already existing job. To do this, open the **Inventory** view, in the working area select the VMs and click **Add to Backup > name of the job** on the ribbon or right-click the VMs and select **Add to backup job > name of the job**.



Step 2. Specify Job Name and Description

At the **Name** step of the wizard, specify a name and description for the backup job.

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



The screenshot shows the 'New Backup Job' wizard window. The title bar reads 'New Backup Job'. The main area is titled 'Name' and contains the instruction 'Type in a name and description for this backup job.' Below this, there is a 'Name' field with the text 'DB Backup' and a 'Description' field with the text 'Daily Backup Job'. On the left side, there is a navigation pane with the following items: 'Name' (selected), 'Virtual Machines', 'Storage', 'Guest Processing', 'Schedule', and 'Summary'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 3. Select VMs to Back Up

At the **Virtual Machines** step of the wizard, select VMs and VM containers that you want to back up.

Jobs with VM containers are dynamic in their nature. If a new VM is added to the container in the virtual infrastructure after the backup job is created, Veeam Backup & Replication will automatically update the job settings to include the added VM.

NOTE:

You can use a regular backup job to process VMs that are part of vApps created in vCenter Server. To back up vCloud Director vApps, you must use specifically developed vCD backup jobs. For more information, see [Backup and Restore of vApps](#).

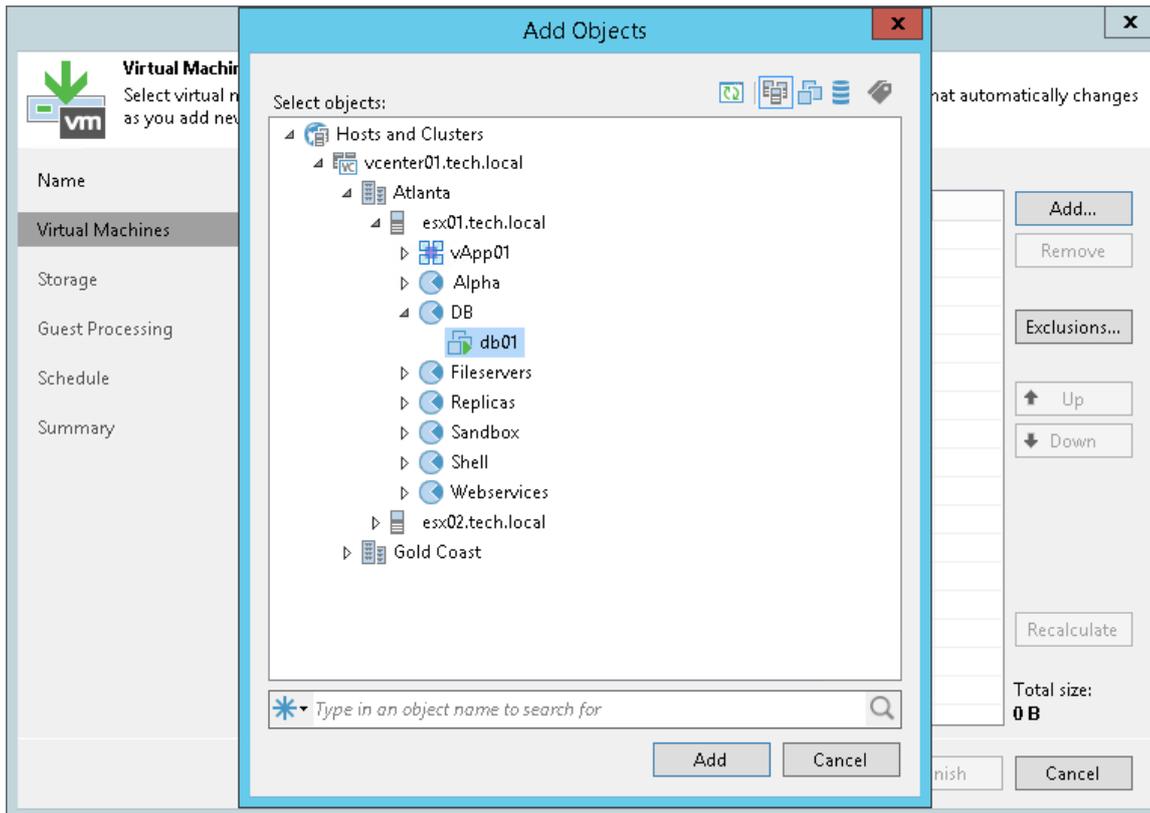
To add VMs to the job:

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**, **VMs and Tags**. Depending on the view you select, some objects may not be available. For example, if you switch to the **VMs and Templates** view, no resource pools, hosts or clusters will be displayed in the tree.
3. Select the VM or VM container in the list and click **Add**.

To quickly find the necessary object, 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 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]**.

The initial size of VMs and VM containers added to the backup job is displayed in the **Size** column in the list. The total size of objects is displayed in the **Total size** field. Use the **Recalculate** button to refresh the total size value after you add a new object to the job.



Step 4. Exclude Objects from Backup Job

After you have added VMs and VM containers to the job, you can specify which objects you want to exclude from the backup. You can exclude the following types of objects:

- [VMs from VM containers](#)
- [Specific VM disks](#)
- [VM templates](#)

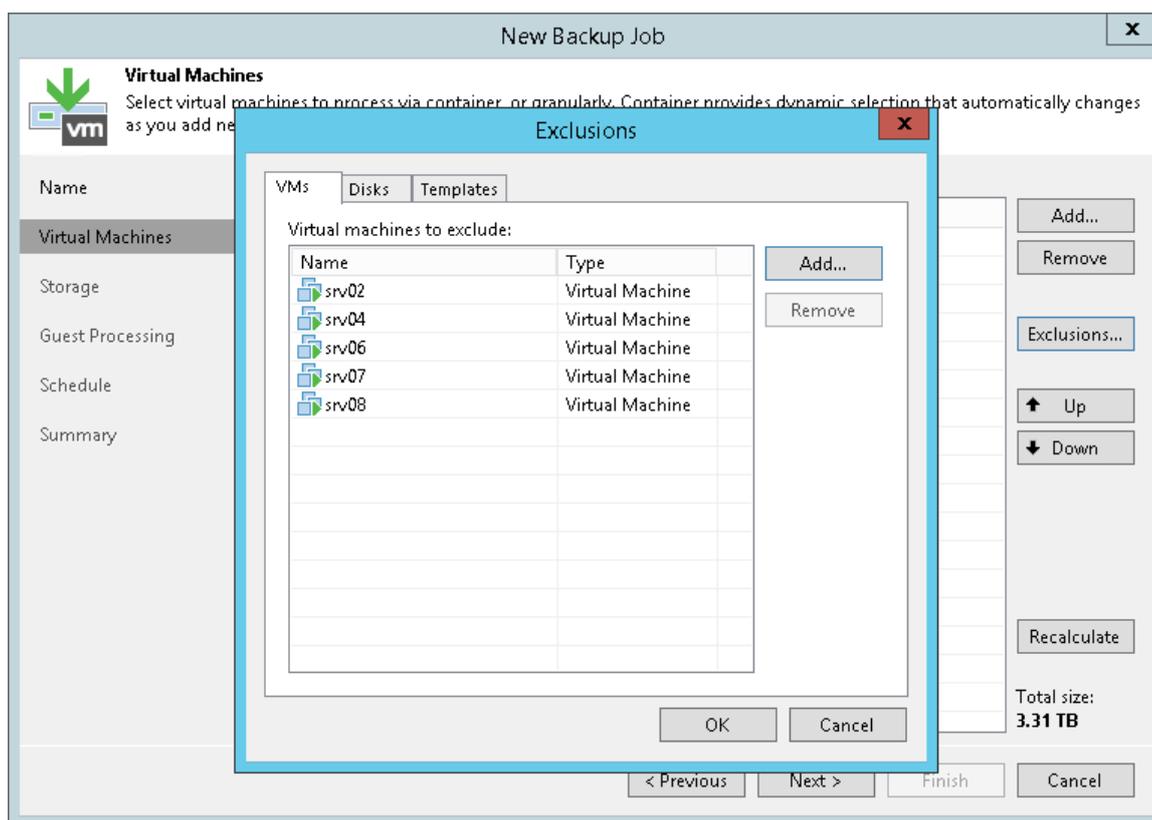
NOTE:

Veeam Backup & Replication automatically excludes VM log files from backup to make the backup process faster and reduce the size of the backup file.

To exclude VMs from a VM container:

1. At the **Virtual Machines** step of the wizard, click **Exclusions**.
2. Click the **VMs** tab.

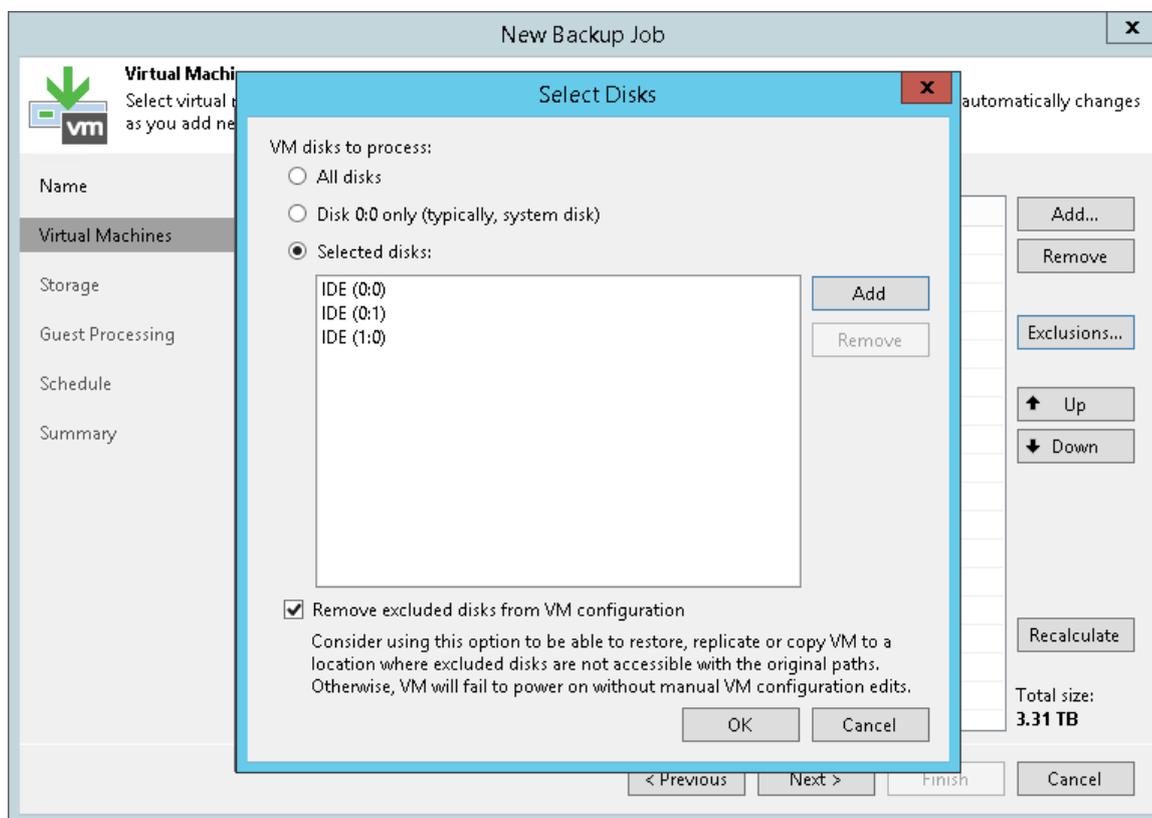
3. Click **Add**.
4. Use the toolbar at the top right corner of the window to switch between views: **Hosts and Clusters, VMs and Templates, Datastores and VMs** and **Tags**. Depending on the view you select, some objects may not be available. For example, if you select the **VMs and Templates** view, no resource pools, hosts or clusters will be displayed in the tree.
5. In the displayed tree, select the necessary object and click **Add**. Use the **Show full hierarchy** check box to display the hierarchy of all VMware Servers added to the backup infrastructure.
6. Click **OK**.



To exclude VM disks:

1. At the **Virtual Machines** step of the wizard, click **Exclusions**.
2. Click the **Disks** tab.
3. Select the VM in the list and click **Edit**. If you want to exclude disks of a VM added as part of the container, click **Add** to include the VM in the list as a standalone object.
4. Choose disks that you want to back up. You can choose to process all disks, 0:0 disks (typically, system disks) or add to the list custom IDE, SCSI or SATA disks.

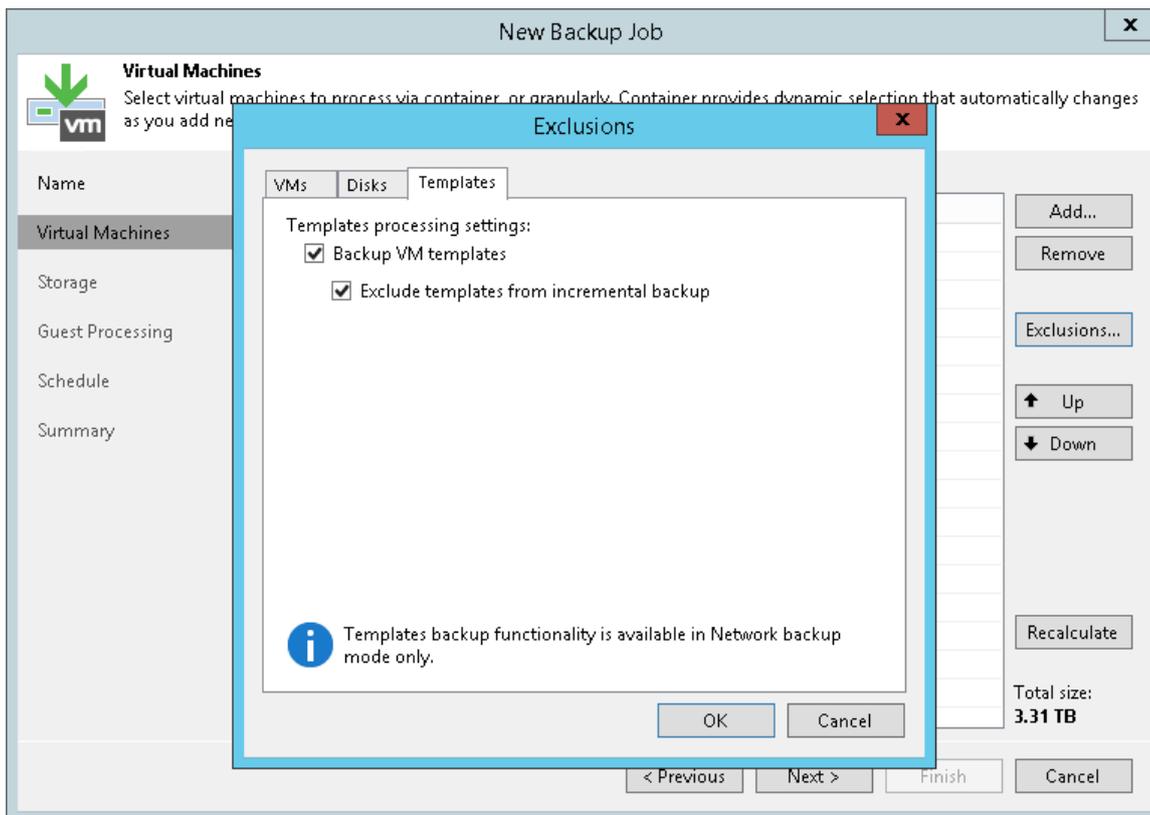
5. Select the **Remove excluded disks from VM configuration** check box. Veeam Backup & Replication will modify the VMX file of a backed up VM to remove excluded disks from the VM configuration. If you restore this VM from the backup file to a location where excluded disks are not accessible with the original paths, you will not have to manually edit the VM configuration file to be able to power on the VM.



To exclude VM templates:

1. At the **Virtual Machines** step of the wizard, select a VM container and click **Exclusions**.
2. Click the **Templates** tab.
3. Clear the **Backup VM templates** check box.

4. If you want to include VM templates into the full backup only, leave the **Backup VM templates** check box selected and select the **Exclude templates from incremental backup** check box.



Step 5. Define VM Backup Order

You can define the order in which the backup job must process VMs. Setting VM order can be helpful, for example, if you add some mission-critical VMs to the job and want the job to process them first. You can set these VMs first in list to ensure that their processing fits the backup window.

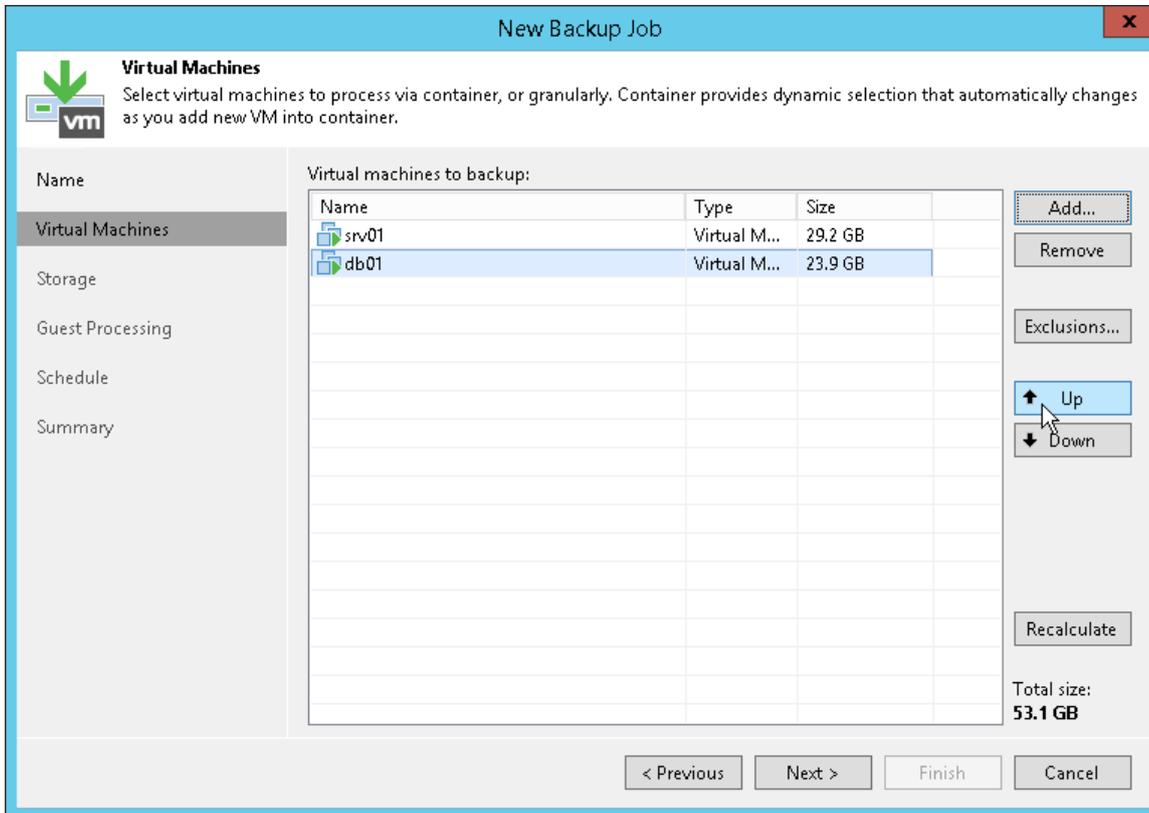
VMs inside a VM container are processed at random. To ensure that VMs are processed in the defined order, you must add them as standalone VMs, not as a part of the VM container.

To define the VM backup order:

1. At the **Virtual Machines** step of the wizard, select a VM or VM container.
2. Use the **Up** and **Down** buttons on the right to move the VM or VM container up or down in the list.

NOTE:

VMs may be processed in a different order. For example, if backup infrastructure resources for a VM that is higher on the priority list are not available, and resources for a VM that is lower on the list are available, Veeam Backup & Replication will start processing the VM that is lower on the list first.



Step 6. Specify Backup Storage Settings

At the **Storage** step of the wizard, select backup infrastructure components for the job – backup proxy and backup repository, and specify backup storage settings.

1. Click **Choose** next to the **Backup proxy** field to select a backup proxy.
 - If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that have access to the source datastore and automatically assign an optimal backup proxy to process VMs in the job.

Veeam Backup & Replication assigns backup proxies to VMs included in the backup job one by one. Before processing a new VM in the VM list, Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use to retrieve VM data and the current workload on the backup proxies to select the most appropriate one for VM processing.
 - If you choose **Use the selected backup proxy servers specified below**, you can explicitly select backup proxies that the job must use. It is recommended that you select at least two backup proxies to ensure that the backup job starts if one of the proxies fails or loses its connectivity to the source datastore.
2. From the **Backup repository** list, select a backup repository where the created backup files must be stored. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

3. You can map the job to a specific backup stored on the backup repository. Backup job mapping can be helpful if you have moved backup files to a new backup repository and want to point the job to existing backups on this new backup repository. You can also use backup job mapping if the configuration database got corrupted and you need to reconfigure backup jobs.

To map the job to a backup, click the **Map backup** link and select the backup on the backup repository. Backups can be easily identified by job names. To find the backup, you can also use the search field at the bottom of the window.

4. In the **Retention policy** section, specify the number of restore points that you want to store on the backup repository. When this number is exceeded, the earliest restore point will be removed from the backup chain. The number of restore points doesn't correspond to the number of days to store restore points. For more information, see [Retention Policy](#).
5. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary destination for this job** check box. With this option enabled, the **New Backup Job** wizard will include an additional step – **Secondary Target**. At the **Secondary Target** step of the wizard, you can link the backup job to the backup copy job or backup to tape backup job.

You can enable this option only if a backup copy job or backup to tape job is already configured on the backup server.

The screenshot shows the 'New Backup Job' wizard window with the 'Storage' step selected. The window title is 'New Backup Job'. On the left is a navigation pane with options: Name, Virtual Machines, Storage (selected), Guest Processing, Schedule, and Summary. The main area contains the following settings:

- Storage:** Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.
- Backup proxy:** Automatic selection (with a 'Choose...' button).
- Backup repository:** Scale-out Backup Repository (Extensible Backup Repository) (with a 'Map backup' link).
- Retention policy:** Restore points to keep on disk: 14 (with an information icon).
- Configure secondary destinations for this job**
Copy backups produced by this job to another backup repository, or to tape. Best practices recommend maintaining at least 2 backups of production data, with one of them being off-site.
- Advanced job settings** include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings. (with an 'Advanced' button).

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

Step 7. Specify Advanced Backup Settings

At the **Storage** step of the wizard, specify advanced settings for the backup job:

- [Backup settings](#)
- [Maintenance settings](#)
- [Storage settings](#)
- [Notification settings](#)

- [vSphere settings](#)
- [Integration settings](#)
- [Script settings](#)

TIP:

After you specify necessary settings for the backup 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 backup job, Veeam Backup & Replication will automatically apply the default settings to the new job.

Backup Settings

To specify settings for a backup chain created with the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. On the **Backup** tab, select the backup method that you want to use to create the backup chain on the backup repository:
 - To create a reverse incremental backup chain, select **Reverse Incremental**.
Dell EMC Data Domain and HPE StoreOnce do not support the reverse incremental backup method. Do not select this option for backup jobs targeted at these types of backup repositories.
 - To create an incremental backup chain, select **Incremental** and enable synthetic full and/or active full backups (see items 3-4).
 - To create a forever forward incremental backup chain, select **Incremental** and do not enable synthetic full and/or active full backups (see items 3-4).

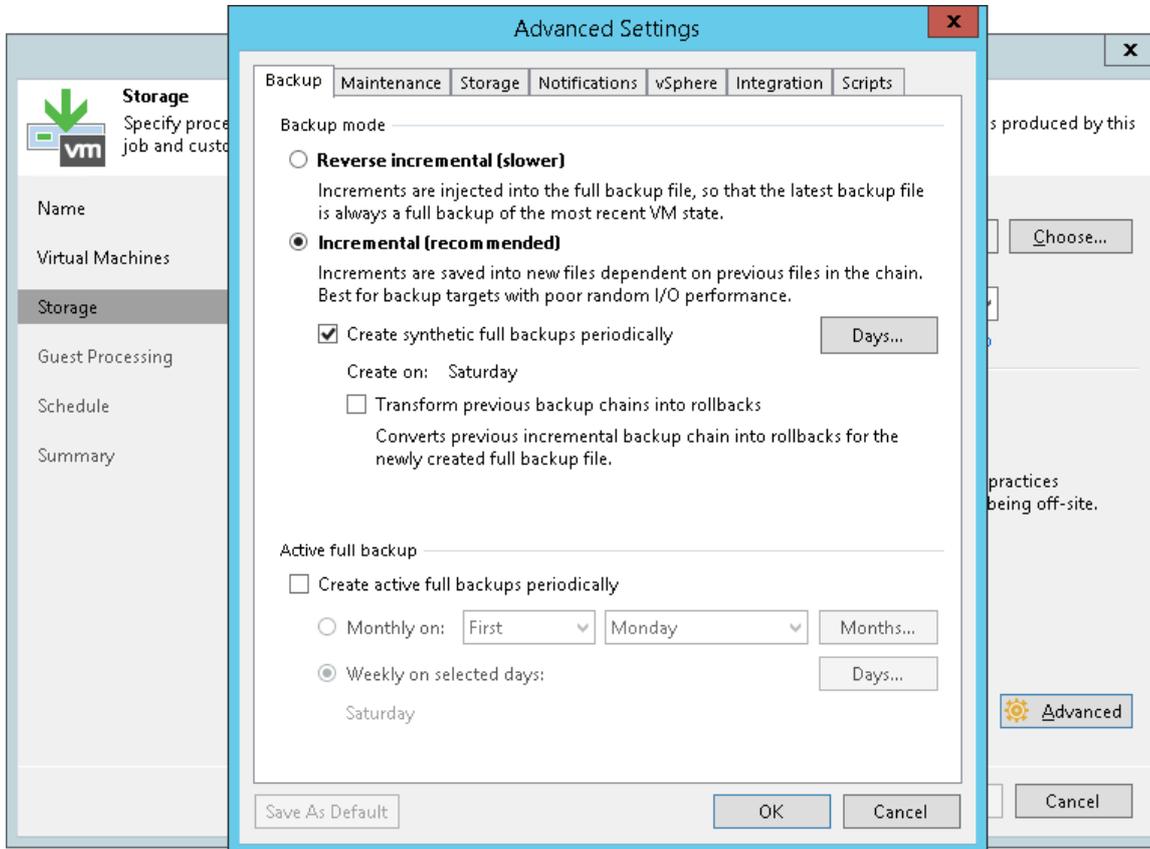
For more information, see [Backup Methods](#).

3. If you choose the incremental backup method, you can select to periodically create synthetic full backups and/or active full backups.
 - To create a synthetic full backup, select the **Create synthetic full backups periodically** check box and click **Days** to schedule synthetic full backups on the necessary week days.
You can additionally choose to transform the previous full backup chain into the reverse incremental backup chain. To do this, select the **Transform previous full backup chains into rollbacks** check box.
 - To create full backups regularly, select the **Create active full backups periodically** check box. Use the **Monthly on** or **Weekly on selected days** options to define scheduling settings.

Before scheduling periodic full backups, you must make sure that you have enough free space on the backup repository. As an alternative, you can create active full backups manually when needed. For more information, see [Active Full Backup](#).

NOTE:

If you schedule the active full backup and synthetic full backup with or without the transform task on the same day, Veeam Backup & Replication will perform only active full backup. Synthetic full backup and transform task will be skipped.



Maintenance Settings

You can instruct Veeam Backup & Replication to periodically perform maintenance operations – service actions that will help make sure that the backup chain remains valid and consistent.

To specify maintenance settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Maintenance** tab.
3. To periodically perform a health check for the latest restore point in the backup chain, in the **Storage-level corruption guard** section select the **Perform backup files health check** check box and specify the time schedule for the health check.

An automatic health check can help you avoid a situation when a restore point gets corrupted, making all dependent restore points corrupted, too. If during the health check Veeam Backup & Replication detects corrupted data blocks in the latest restore point in the backup chain (or, in case of forever forward incremental and forward incremental chains, the restore point before the latest one if the latest restore point is incomplete), it will start the health check retry and transport valid data blocks from the source datastore to the backup repository. The transported data blocks are stored to a new backup file or the latest backup file in the backup chain, depending on the data corruption scenario. For more information, see [Health Check for Backup Files](#).

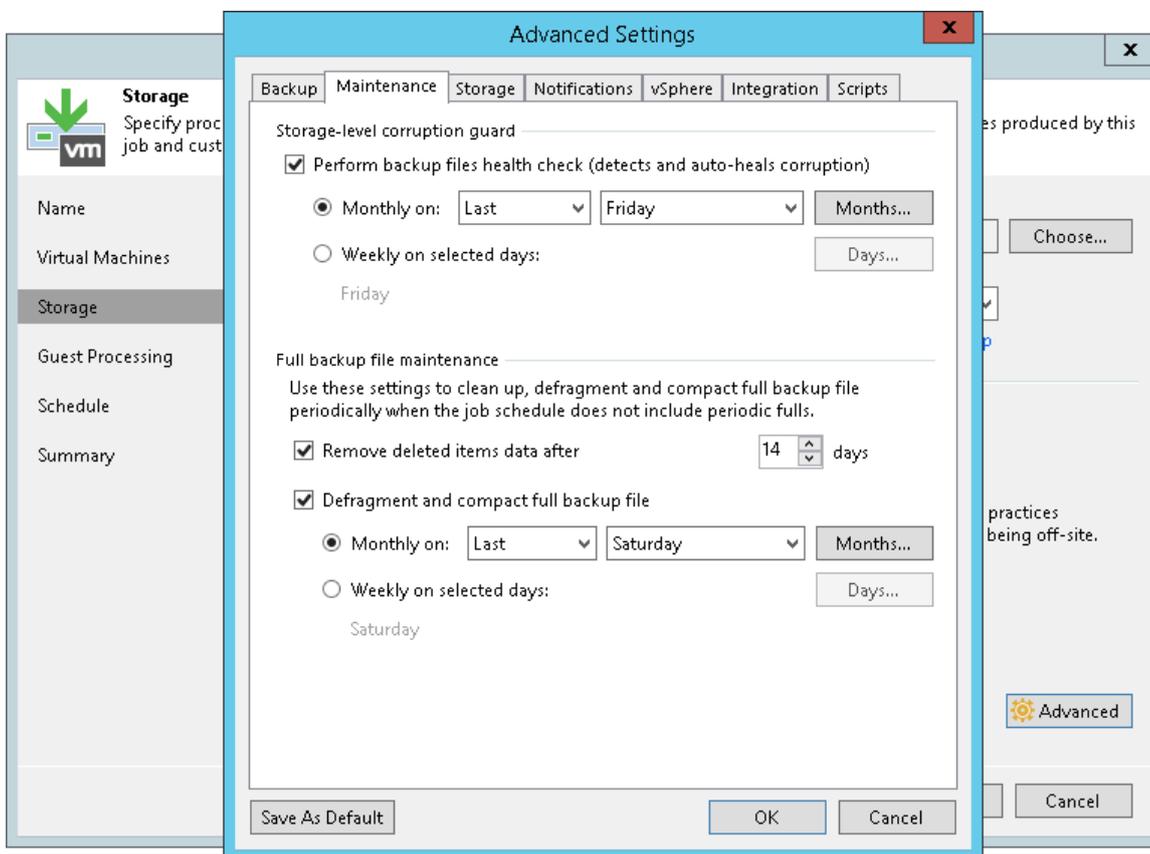
4. Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep backup data for deleted VMs. If a VM is no longer available (for example, it was deleted or excluded from the job), Veeam Backup & Replication will keep its data on the backup repository for the period that you have specified. When this period is over, data of the deleted VM will be removed from the backup repository.

By default, the retention period for deleted VM data is 14 days. It is strongly recommended that you set the retention period to 3 days or more to prevent unwanted data loss. For more information, see [Retention Policy for Deleted VMs](#).

5. To periodically compact a full backup, select the **Defragment and compact full backup file** check box and specify the schedule for the compact operation.

During the compact operation, Veeam Backup & Replication creates a new empty file and copies to it data blocks from the full backup file. As a result, the full backup file gets defragmented and the speed of reading and writing from/to the backup file increases.

If the full backup file contains data blocks for deleted VMs, Veeam Backup & Replication will remove these data blocks. If the full backup file contains data for a VM that has only one restore point, and this restore point is older than 7 days, Veeam Backup & Replication will perform the take out operation. For more information, see [Compact of Full Backup File](#).



Storage Settings

To specify storage settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Storage** tab.

3. By default, Veeam Backup & Replication deduplicates VM data before storing it on the backup repository. Data deduplication provides a smaller size of the backup file but may reduce the backup job performance. To disable data deduplication, clear the **Enable inline data deduplication** check box.

If you disable this option, you also change the workflow of incremental backup. If Changed Block Tracking is enabled for the job, Veeam Backup & Replication will save all data blocks marked by CBT as new to the destination storage without performing an additional check or using Veeam's filtering mechanism. This will result in faster incremental backup. For more information, see [Changed Block Tracking](#).

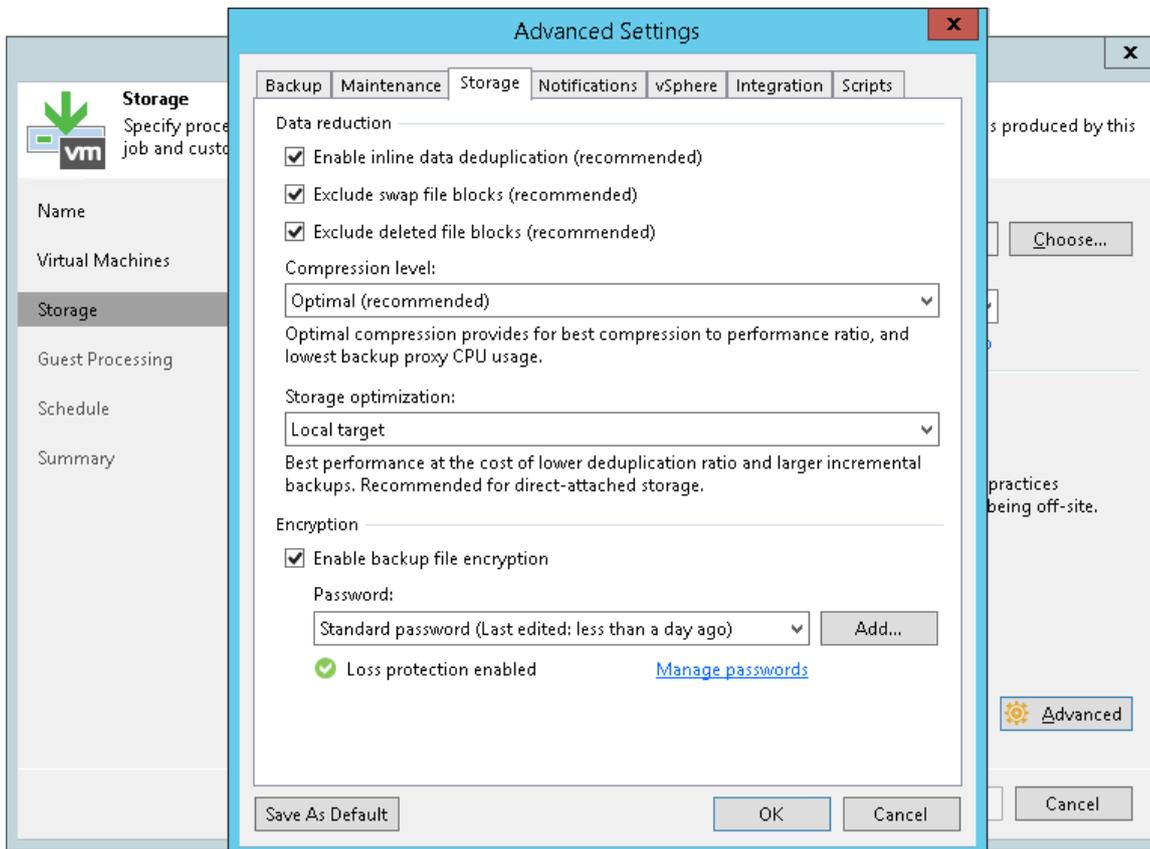
4. By default, Veeam Backup & Replication checks the NTFS MFT file on VMs with Microsoft Windows OS to identify data blocks of the `hiberfil.sys` file (file used for the hibernate mode) and `pagefile.sys` file (swap file), and excludes these data blocks from processing. The swap file is dynamic in nature and changes intensively between backup job sessions, even if the VM itself does not change much. Processing of service files reduces the job performance and increases the size of incremental backup files.
5. If you want to include data blocks of the `hiberfil.sys` file and `pagefile.sys` file to the backup, clear the **Exclude swap file blocks** check box. For more information, see [Swap Files](#).
6. By default, Veeam Backup & Replication does not copy deleted file blocks ("dirty" blocks on the VM guest OS) to the target location. This option lets you reduce the size of backup files and increase the job performance. If you want to include dirty data blocks to the backup, clear the Exclude deleted file blocks check box. For more information, see [Deleted File Blocks](#).
7. From the **Compression level list**, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*.
8. In the **Storage optimization** section, select what type of backup target you plan to use: *Local target (large blocks)*, *Local target*, *LAN target* or *WAN target*. Depending on the chosen storage type, Veeam Backup & Replication will use data blocks of different size to optimize the size of backup files and job performance. For more information, see [Compression and Deduplication](#).
9. To encrypt the content of backup files, select the **Enable backup file encryption** check box. In the **Password** field, select a password that you want to use for encryption. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. For more information, see [Managing Passwords for Data Encryption](#).

If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it. For more information, see [Decrypting Data Without Password](#).

NOTE:

If you enable encryption for an existing backup job, during the next job session Veeam Backup & Replication will create a full backup file. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.

Encryption is not retroactive. If you enable encryption for an existing job, Veeam Backup & Replication does not encrypt the previous backup chain created with this job. If you want to start a new chain so that the unencrypted previous chain can be separated from the encrypted new chain, follow this scenario: <https://www.veeam.com/kb1885>.



Notification Settings

To specify notification settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully.

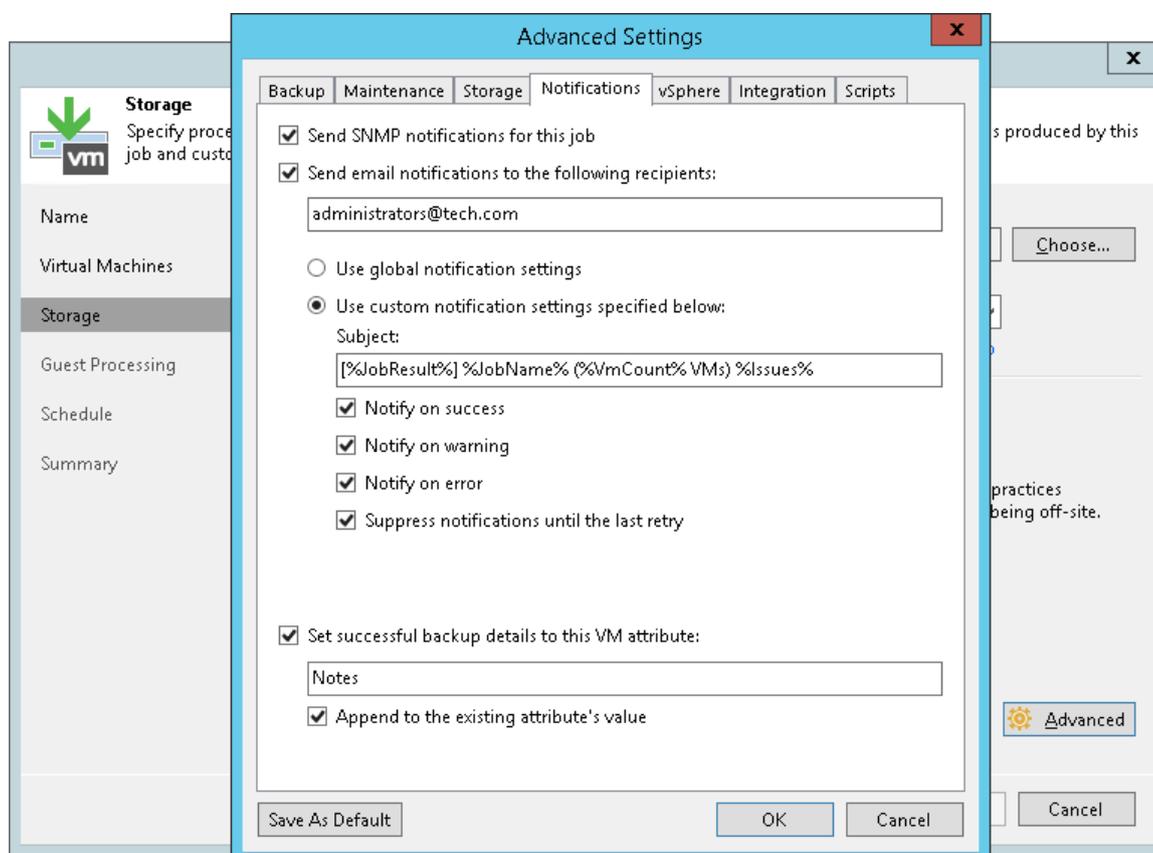
SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see [Specifying SNMP Settings](#).

4. Select the **Send email notifications to the following recipients** check box if you want to receive notifications about the job completion status by email. In the field below, specify recipient's email address. You can enter several addresses separated by a semicolon.

Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see [Configuring Global Email Notification Settings](#).

5. 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 & Replication will apply to the job global email notification settings specified for the backup server. For more information, see [Configuring Global Email Notification Settings](#).
 - To configure a custom notification for the job, select **Use custom notification settings specified below** check box. You can specify the following notification settings:
 - a. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of VMs in the job) and *%Issues%* (number of VMs in the job that have finished with the *Warning* or *Failed* status).
 - b. 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.
 - c. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.
6. Select the **Set successful backup details to this VM attribute** check box to write information about successfully performed backup and backup results (backup date and time, backup server name and path to the backup file) to a VM attribute. In the field below, enter a name of the attribute. If the specified attribute does not exist, Veeam Backup & Replication will create it.

7. Select the **Append to the existing attribute's value** check box to append information about successfully performed backup to an existing value of the attribute. In this case, Veeam Backup & Replication will keep values added by the user in the attribute, and will overwrite only the value added by the backup job. If you do not select this option, Veeam Backup & Replication will overwrite the existing attribute values (made both by the user and backup job).



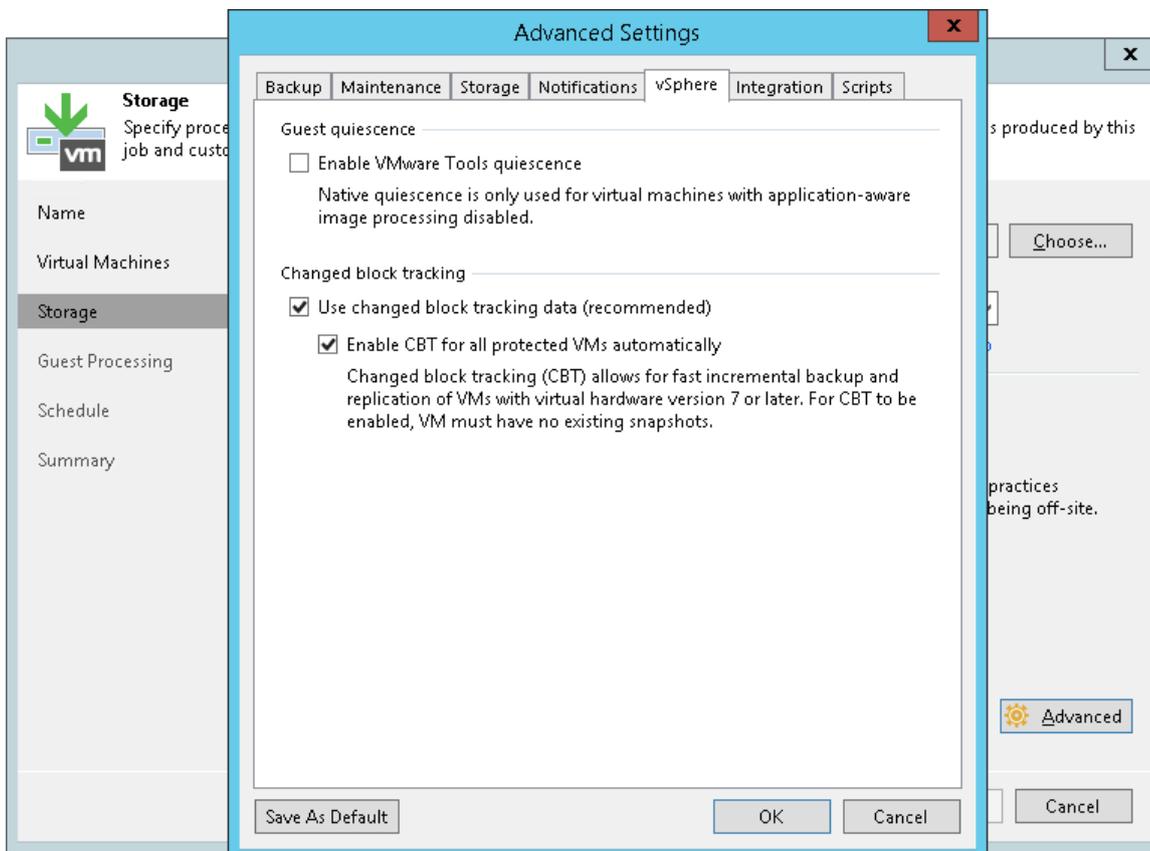
vSphere Settings

To specify VMware vSphere settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **vSphere** tab.
3. Select the **Enable VMware tools quiescence** check box to freeze the file system of processed VMs during backup. Depending on the VM version, Veeam Backup & Replication will use the VMware FileSystem Sync Driver (vmsync) driver or VMware VSS component in VMware Tools for VM snapshot creation. These tools are responsible for quiescing the VM file system and bringing the VM to a consistent state suitable for backup.
For more information, see [VMware Tools Quiescence](#).
4. In the **Changed block tracking** section, specify if VMware vSphere CBT must be used for VM backup. By default, this option is enabled. If you want to force using CBT even if CBT is disabled at the level of the ESX(i) host, select the **Enable CBT for all processed VMs automatically** check box.
For more information, see [Changed Block Tracking](#).

IMPORTANT!

You can use CBT for VMs with virtual hardware version 7 or later.



Integration Settings

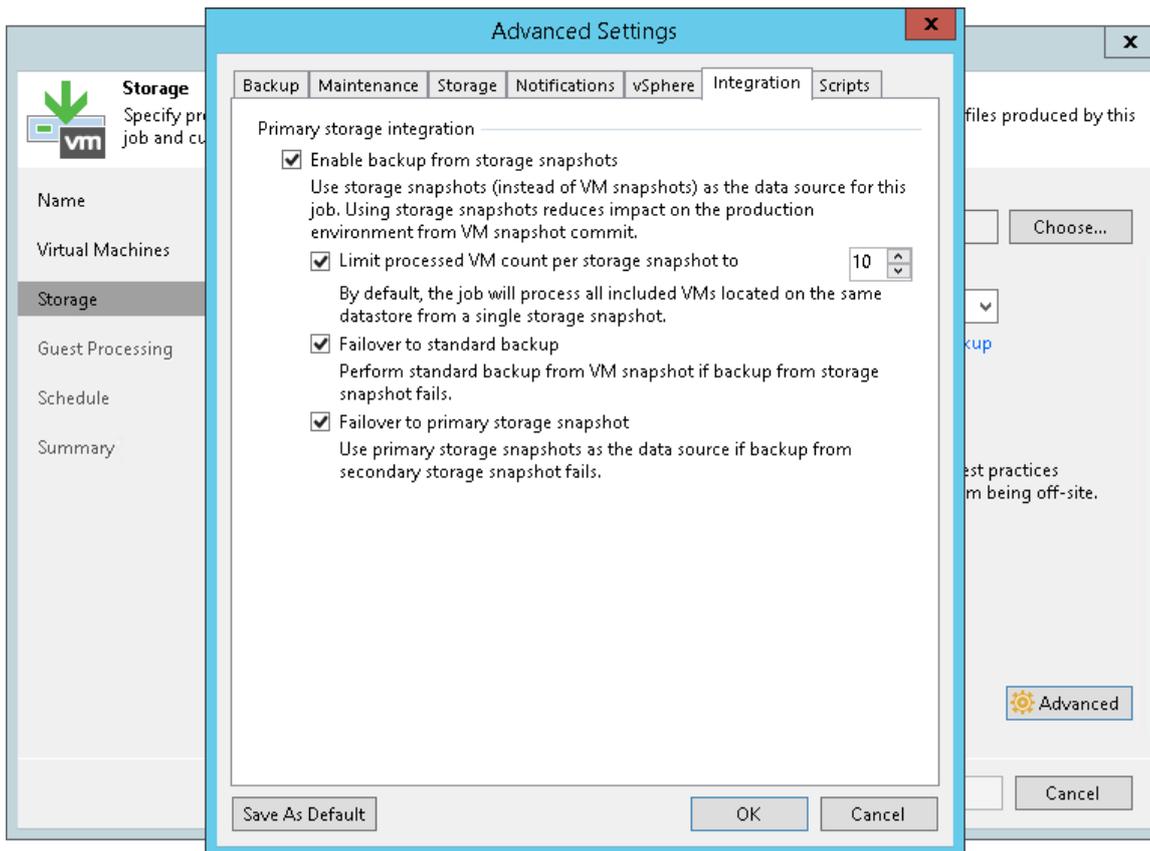
On the **Integration** tab, you can define whether you want to use the Backup from Storage Snapshots technology to create the backup. Backup from Storage Snapshots lets you leverage storage snapshots for VM data processing. The technology improves RPOs and reduces the impact of backup activities on the production environment.

To specify storage integration settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Integration** tab.
3. By default, the **Enable backup from storage snapshots** option is enabled. If you do not want to use Backup from Storage Snapshots, clear this check box. For more information, see [Performing Backup from Storage Snapshots](#).
4. If you add to the job many VMs whose disks are located on the same volume or LUN, select the **Limit processed VM count per storage snapshot to <N>** check box and specify the number of VMs for which one storage snapshot must be created. Veeam Backup & Replication will divide VMs into several groups and trigger a separate storage snapshot for every VM group. As a result, the job performance will increase.

For more information, see [Limitation on Number of VMs per Snapshot](#).

5. If Veeam Backup & Replication fails to create a storage snapshot, VMs whose disks are located to the storage system will not be processed by the job. To fail over to the regular VM processing mode and back up or replicate such VMs in the regular processing mode, select the **Failover to standard backup** check box.
6. [For secondary NetApp storage systems] If Veeam Backup & Replication cannot create a storage snapshot on NetApp SnapMirror or SnapVault, the job will not back up VMs whose disks are located to the storage system. To fail over to Backup from Storage Snapshots on the production storage, select the **Failover to primary storage snapshot** check box. If Veeam Backup & Replication fails to create a storage snapshot on NetApp SnapMirror or SnapVault, it will trigger the storage snapshot on the primary NetApp storage and use it as a source for backup. Note, however, that Backup from Storage Snapshots on the primary NetApp storage will put additional load on the production environment.



Script Settings

To specify script settings for the backup job:

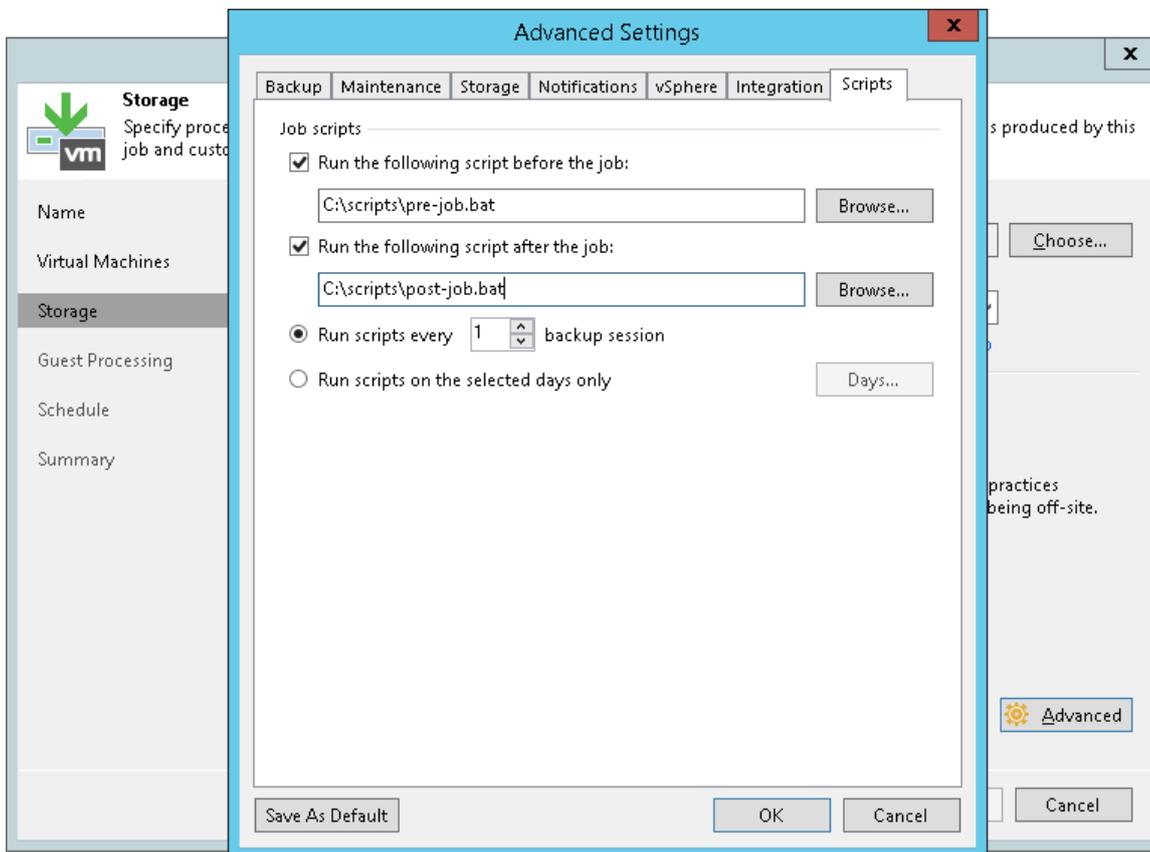
1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Scripts** tab.
3. If you want to execute custom scripts before and/or after the backup job, select the **Run the following script before the job** and **Run the following script after the job** check boxes and click **Browse** to choose executable files from a local folder on the backup server. The scripts are executed on the backup server.

You can select to execute pre- and post-backup actions after a number of backup sessions or on specific week days.

- If you select the **Run scripts every <N> backup session** option, specify the number of the backup job sessions after which the scripts must be executed.
- If you select the **Run scripts on the selected days only** option, click **Days** and specify week days on which the scripts must be executed.

NOTE:

- Custom scripts that you define in the advanced job settings relate to the backup job itself, not the VM quiescence process. To add pre-freeze and post-thaw scripts for VM image quiescence, use the **Guest Processing** step of the wizard.
- To run the script, Veeam Backup & Replication uses the [Service Account](#) under which the Veeam Backup Service is running.



Step 8. Specify Secondary Target

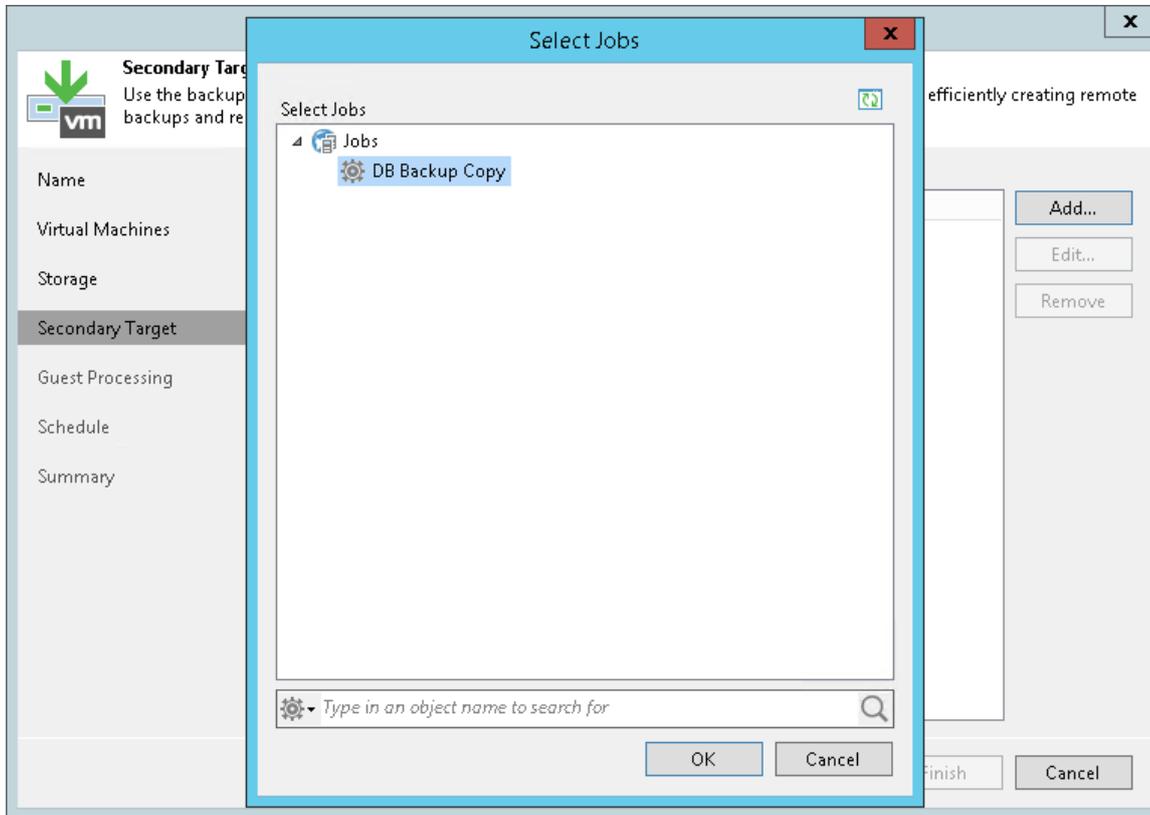
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destination for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the backup job to a backup to tape or backup copy job. As a result, the backup job will be added as a source to the backup to tape or backup copy job. Backup files created with the backup job will be archived to tape or copied to the secondary backup repository according to the secondary jobs schedule. For more information, see [Linking Backup Jobs to Backup Copy Jobs](#) and [Linking Backup Jobs to Backup to Tape Jobs](#).

The backup to tape job or backup copy job must be configured beforehand. You can create these jobs with an empty source. When you link the backup job to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the backup job as a source for these jobs.

To link jobs:

1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the backup job. You can link several jobs to the backup job, for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom of the wizard.



Step 9. Specify Guest Processing Settings

At the **Guest Processing** step of the wizard, you can enable the following settings for VM guest OS processing:

- [Application-aware processing](#)
- [Transaction log handling for Microsoft SQL VMs](#)
- [Archived log handling for Oracle VM](#)
- [VM guest OS file exclusion](#)
- [Use of pre-freeze and post-thaw scripts](#)
- [VM guest OS file indexing](#)

To coordinate guest processing activities, Veeam Backup & Replication deploys a runtime process on the VM guest OS. The process runs only during guest processing and is stopped immediately after the processing is finished (depending on the selected option, during the backup job session or after the backup job completes).

You must specify a user account that will be used to connect to the VM guest OS and deploy the runtime process:

1. From the **Guest OS credentials** list, select a user account with local administrator privileges on the VM guest OS. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see [Guest Processing](#).

Note that for Veeam Backup & Replication version 9.5 Update 3a and later, the account used for guest OS processing must have the following user rights assigned:

- **Logon as a batch job** granted
- **Deny logon as a batch job** not set

Local accounts do not support Kerberos authentication. To authenticate with Microsoft Windows guest OS using Kerberos, specify an Active Directory account.

By default, Veeam Backup & Replication uses the **Log on as a batch job** policy to connect to guest OS. If the connection fails, Veeam Backup & Replication switches to **Interactive Logon**.

NOTE:

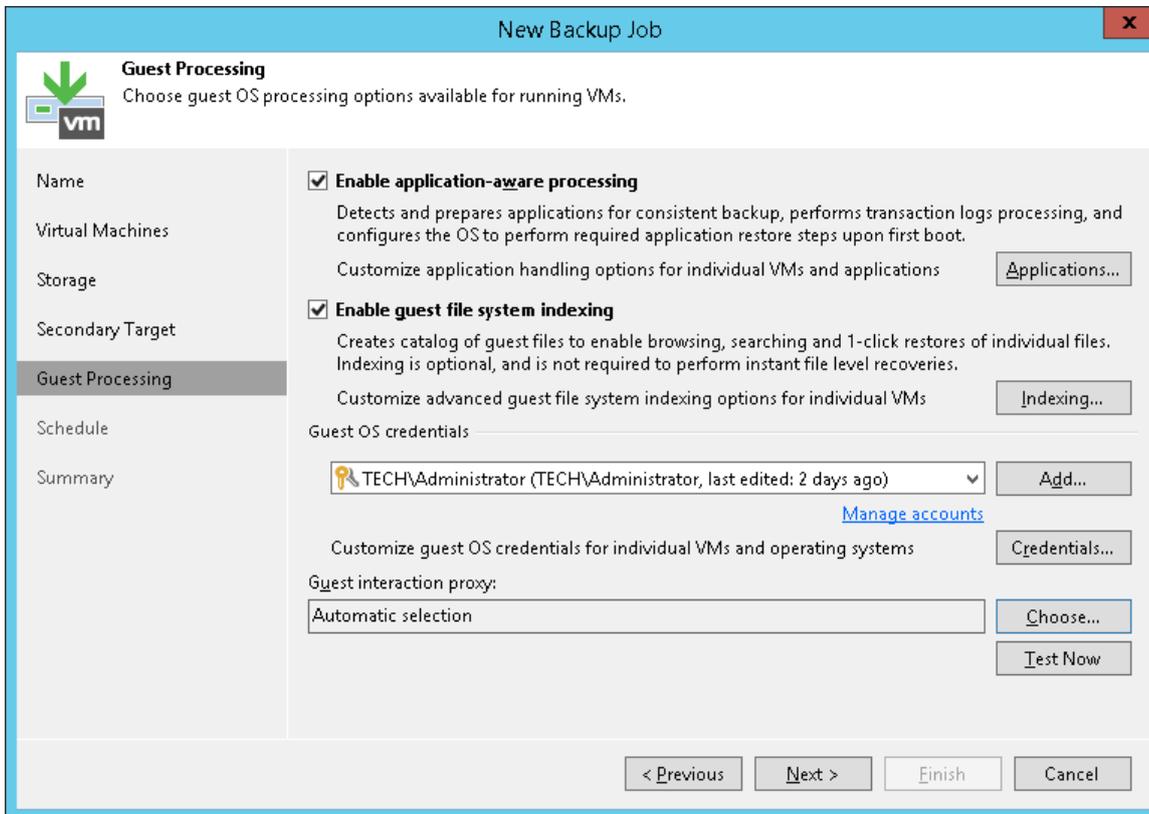
[For Kerberos authentication] Mind the following:

- Networkless application-aware guest processing through VMware VIX/vSphere Web Services is not supported for VMs with guest OS where NTLM is restricted.
 - Veeam backup infrastructure machines (backup server, repositories, backup proxies, guest interaction proxies, etc.) must correctly resolve FQDNs of guest operating systems.
 - To back up VMs where Kerberos is used, NTLM must be allowed in the Veeam backup infrastructure machines. For details, see [Kerberos Authentication for Guest OS Processing](#).
2. By default, Veeam Backup & Replication uses the same credentials for all VMs in the job. If some VM requires a different user account, click **Credentials** and enter custom credentials for the VM.
 3. If you have added Microsoft Windows VMs to the job, specify which guest interaction proxy Veeam Backup & Replication can use to deploy the runtime process on the VM guest OS. On the right of the **Guest interaction proxy** field, click **Choose**.
 - Leave **Automatic selection** to let Veeam Backup & Replication automatically select the guest interaction proxy.
 - Select **Use the selected guest interaction proxy servers only** to explicitly define which servers will perform the guest interaction proxy role. The list of servers contains Microsoft Windows servers added to the backup infrastructure.

To check if Veeam Backup & Replication can communicate with VMs added to the job and deploy the runtime process on their guest OSes, click **Test Now**. Veeam Backup & Replication will use the specified credentials to connect to all VMs in the list.

NOTE:

The guest interaction proxy functionality is available in the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication.



Application-Aware Processing

If you add to the backup job VMs running VSS-aware applications, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup guarantees proper recovery of applications on VMs without data loss.

To enable application-aware processing:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the VM and click **Edit**.

To define custom settings for a VM added as a part of a VM container, you must include the VM to the list as a standalone object. To do this, click **Add** and choose the VM whose settings you want to customize. Then select the VM in the list and define the necessary settings.

4. On the **General** tab, in the **Applications** section specify the behavior scenario for application-aware processing:
 - Select **Require successful processing** if you want Veeam Backup & Replication to stop the backup process if any error occurs during application-aware processing.

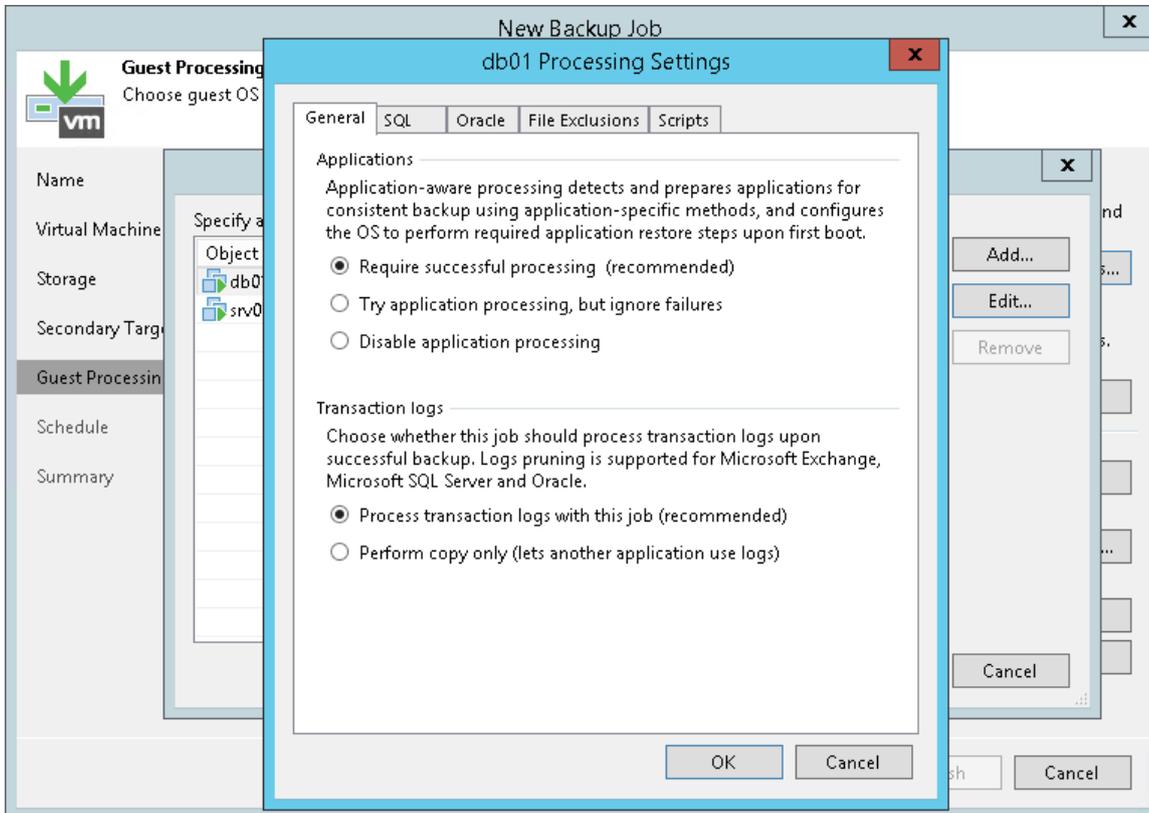
- Select **Try application processing, but ignore failures** if you want to continue the backup process even if an error occurs during application-aware processing. This option guarantees completion of the backup job. However, the resulting backup will not be transactionally consistent but crash consistent.
 - Select **Disable application processing** if you do not want to enable application-aware processing for the VM.
5. [For Microsoft Exchange, Microsoft SQL and Oracle VMs] In the **Transaction logs** section, specify if Veeam Backup & Replication must process transaction logs or copy-only backups must be created.
- a. Select **Process transaction logs with this job** if you want Veeam Backup & Replication to process transaction logs.

[For Microsoft Exchange VMs] With this option selected, the runtime process running on the VM guest OS will wait for backup to complete successfully and then trigger truncation of transaction logs. If the backup job fails, the logs will remain untouched on the VM guest OS until the next start of the runtime process.

[For Microsoft SQL Server VMs and Oracle VMs] You will have to specify settings for transaction log handling on the **SQL** and **Oracle** tabs of the **VM Processing Settings** window. For more information, see [Transaction Log Settings: Microsoft SQL](#) and [Transaction Log Settings: Oracle](#).
 - b. Select **Perform copy only** if you use another backup tool to perform VM guest level backup, and this tool maintains consistency of the database state. Veeam Backup & Replication will create a copy-only backup for the selected VM. The copy only backup preserves the chain of full/differential backup files and transaction logs on the VM. For more information, see <http://msdn.microsoft.com/en-us/library/ms191495.aspx>.

IMPORTANT!

If both Microsoft SQL Server and Oracle Server are installed on one VM, and this VM is processed by a job with log backup enabled for both applications, Veeam Backup & Replication will back up only Oracle transaction logs. Microsoft SQL Server transaction logs will not be processed.



Microsoft SQL Server Transaction Log Settings

If you back up a Microsoft SQL VM, you can specify how Veeam Backup & Replication must process transaction logs on this VM:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the Microsoft SQL Server VM and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.
5. In the **VM Processing Settings** window, click the **SQL** tab.
6. Specify how transaction logs must be processed. You can select one of the following options:
 - Select **Truncate logs** to truncate transaction logs after successful backup. The runtime process running on the VM guest OS will wait for the backup to complete successfully and then truncate transaction logs. If the job does not manage to back up the Microsoft SQL Server VM, the logs will remain untouched on the VM guest OS until the next start of the runtime process.
 - Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Backup & Replication will not truncate transaction logs on the Microsoft SQL Server VM.

It is recommended that you enable this option for databases that use the *Simple* recovery model. If you enable this option for databases that use the *Full* or *Bulk-logged* recovery model, transaction logs on the VM guest OS may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs him-/herself.

- Select **Backup logs periodically** to back up transaction logs with Veeam Backup & Replication. Veeam Backup & Replication will periodically copy transaction logs to the backup repository and store them together with the image-level backup of the Microsoft SQL Server VM. During the backup job session, transaction logs on the VM guest OS will be truncated.

For more information, see [Microsoft SQL Server Logs Backup and Restore](#).

If you have selected to back up transaction logs with Veeam Backup & Replication, you must specify settings for transaction logs backup:

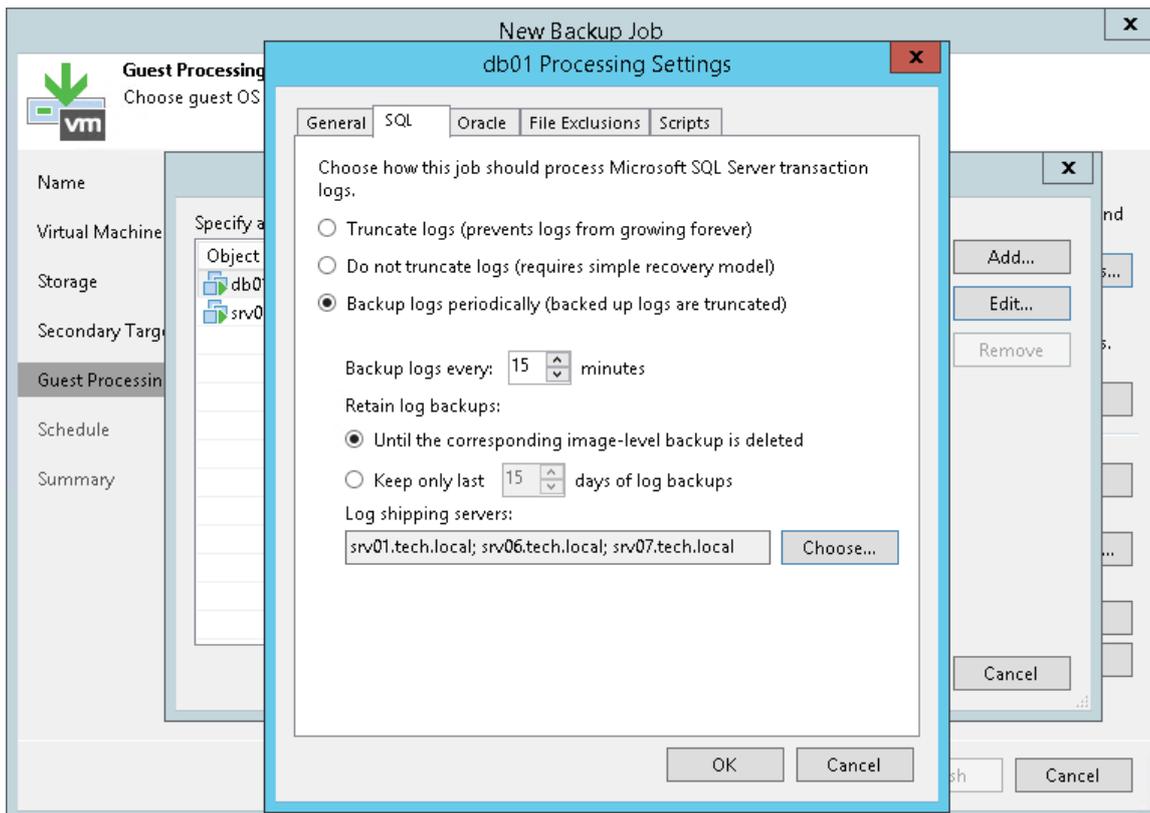
1. In the **Backup logs every <N> minutes** field, specify the frequency for transaction logs backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
2. In the **Retain log backups** section, specify retention policy for transaction logs stored on the backup repository.
 - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and transaction log backups.
 - Select **Keep only last <N> days of log backups** to keep transaction logs for a specific number of days. By default, transaction logs are kept for 15 days. If you select this option, you must make sure that retention for transaction logs is not greater than retention for the image-level backups. For more information, see [Retention for Transaction Log Backups](#).
3. In the **Log shipping servers** section, click **Choose** to select what log shipping server you want to use to transport transaction logs:
 - Select **Automatic selection** if you want Veeam Backup & Replication to choose an optimal log shipping server automatically. If the optimal shipping server is busy, Veeam Backup & Replication will direct the data flow to another shipping server not to lose data and to comply with RPO. The process of transaction logs shipment does not require a dedicated server – Veeam Backup & Replication can use any Microsoft Windows server added to the backup infrastructure.
 - To define a log shipping server explicitly, select **Use the specified servers only** and select check boxes next to servers that you want to use as log shipping servers. The server list includes all Microsoft Windows servers added to the backup infrastructure.

Make sure that you select a server that is not engaged in other resource-consuming tasks. For example, you may want not to use a server that performs the WAN accelerator role as a log shipping server. For load balance and high availability purposes, it is recommended that you select at least 2 log shipping servers.

IMPORTANT!

Veeam Backup & Replication automatically excludes its configuration database from application-aware processing during backup if the database is hosted without using SQL Server AlwaysOn Availability Group. Transaction logs for the configuration database are not backed up.

If the Veeam Backup & Replication configuration database is hosted using SQL Server AlwaysOn Availability Group, you should manually exclude this database from application-aware processing during backup as described in <https://www.veeam.com/kb2110>. Otherwise, job processing will fail with the following error: Failed to freeze guest over network, wait timeout.



Oracle Archived Log Settings

If you back up an Oracle VM, you can specify how Veeam Backup & Replication must process archived logs on this VM:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select an Oracle VM and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.
5. In the **VM Processing Settings** window, click the **Oracle** tab.
6. In the **Specify Oracle account with SYSDBA privileges** section, specify a user account that Veeam Backup & Replication will use to connect to the Oracle database. The account must have SYSDBA rights on the Oracle database.

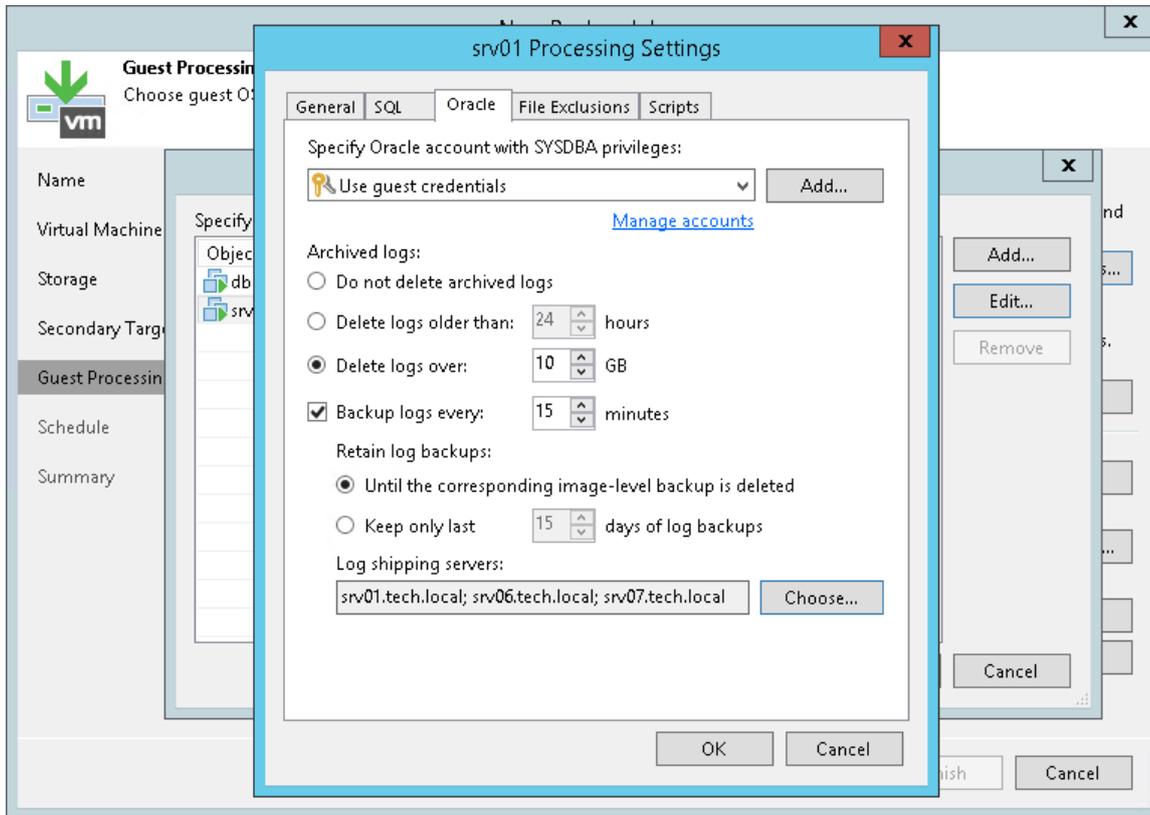
You can select **Use guest credentials** in the list of user accounts. In this case, Veeam Backup & Replication will use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.

7. In the **Archived logs** section, specify how Veeam Backup & Replication must process archived logs on the Oracle VM:
 - Select **Do not delete archived logs** if you want Veeam Backup & Replication to preserve archived logs on the VM guest OS. When the backup job completes, the runtime process will not delete archived logs.

It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, archived logs on the VM guest OS may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.
 - Select **Delete logs older than <N> hours** or **Delete logs over <N> GB** if you want Veeam Backup & Replication to delete archived logs that are older than <N> hours or larger than <N> GB. The log size threshold refers not to the total size of all logs for all databases, but to the log size of each database on the selected Oracle server.

When the parent backup job (job creating an image-level backup) runs, Veeam Backup & Replication will wait for the backup to complete successfully, and then trigger archived logs deletion on the Oracle VM over Oracle Call Interface (OCI). If the primary job does not manage to back up the Oracle VM, the logs will remain untouched on the VM guest OS until the next start of the runtime process.
8. To back up Oracle archived logs with Veeam Backup & Replication, select the **Backup log every <N> minutes** check box and specify the frequency for archived logs backup. By default, archived logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
9. In the **Retain log backups** section, specify retention policy for archived logs stored on the backup repository:
 - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and archived log backups.
 - Select **Keep only last <n> days** to keep archived logs for a specific number of days. By default, archived logs are kept for 15 days. If you select this option, you must make sure that retention for archived logs is not greater than retention for the image-level backups. For more information, see [Retention for Archived Log Backups](#).
10. In the **Log shipping servers** section, click **Choose** to select what log shipping server you want to use to transport archived logs:
 - Select **Automatic selection** if you want Veeam Backup & Replication to select an optimal log shipping server automatically. The process of archived logs shipment does not require a dedicated server – Veeam Backup & Replication can use any Microsoft Windows or Linux server added to the backup infrastructure.
 - Select **Use the specified servers only** to define a log shipping server explicitly. In the **Log Shipping Servers** window, select check boxes next to servers that you want to use as log shipping servers. The server list includes all Microsoft Windows servers added to the backup infrastructure.

Make sure that you select a server that is not engaged in other resource-consuming tasks. For example, you may want not to use a server that performs the WAN accelerator role as a log shipping server. For load balance and high availability purposes, it is recommended that you select at least 2 log shipping servers.



VM Guest OS File Exclusion

If you do not want to back up specific files and folders on the VM guest OS, you can exclude them from the backup. Note that this option is available only for Enterprise and Enterprise Plus Editions.

To define what files and folders must be excluded:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the VM and click **Edit**.

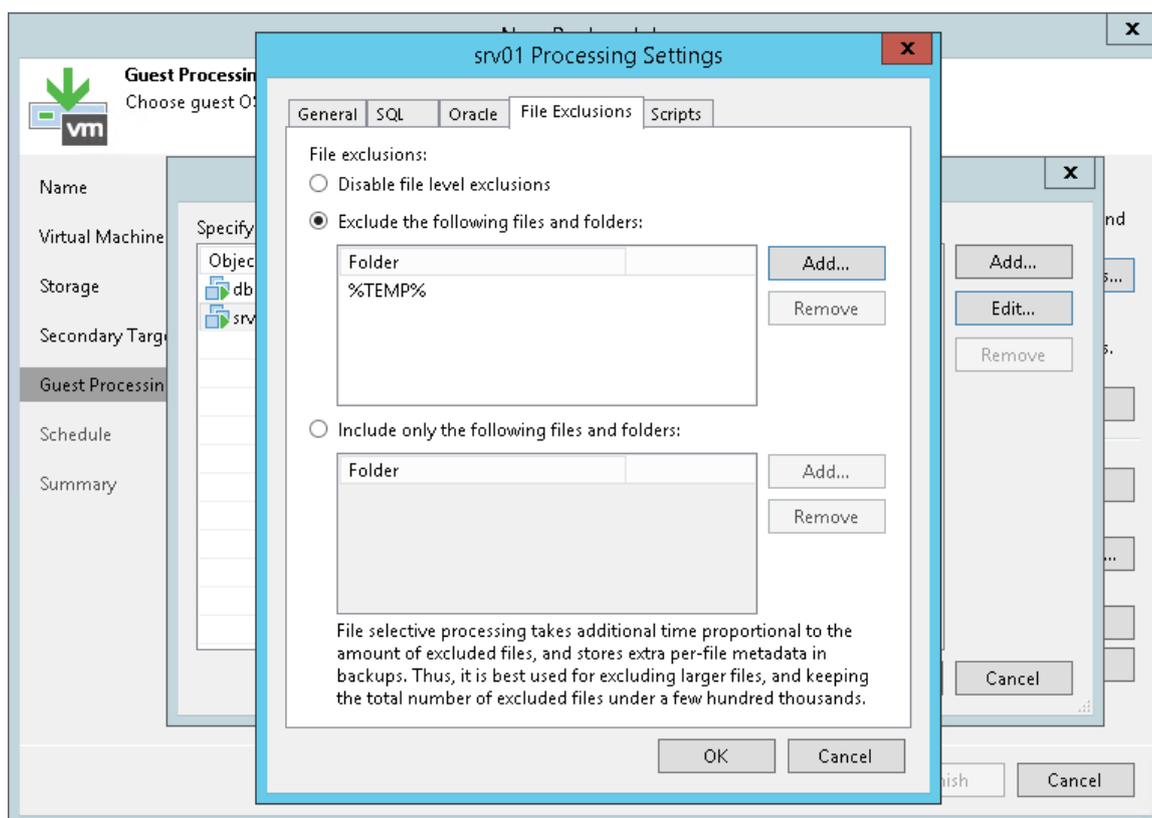
To define custom settings for a VM added as part of a VM container, you must include the VM in the list as a standalone object. To do this, click **Add** and choose a VM whose settings you want to customize. Then select the VM in the list and define the necessary settings.

4. Click the **File Exclusions** tab and specify what files must be excluded from the backup:
 - o Select **Exclude the following files and folders** to remove the individual files and folders from the backup.
 - o Select **Include only the following files and folders** to leave only the specified files and folders in the backup.

5. Click **Add** and specify what files and folders you want to include or exclude. To form the list of exclusions or inclusions, you can use full paths to files and folders, environmental variables and file masks with the asterisk (*) and question mark (?) characters. For more information, see [VM Guest OS Files](#).
6. Click **OK**.
7. Repeat steps 5-6 for every file or folder that you want to exclude or include.

NOTE:

Volumes on the dynamic disks must not be split. Spanned, striped and other types of split volumes cannot be excluded.



Pre-Freeze and Post-Thaw Scripts

If you plan to back up VMs running applications that do not support VSS, you can specify what scripts Veeam Backup & Replication must use to quiesce the VM. The pre-freeze script quiesces the VM file system and application data to bring the VM to a consistent state before Veeam Backup & Replication triggers a VM snapshot. After the VM snapshot is created, the post-thaw script brings the VM and applications to their initial state.

To specify pre-freeze and post-thaw scripts for the job:

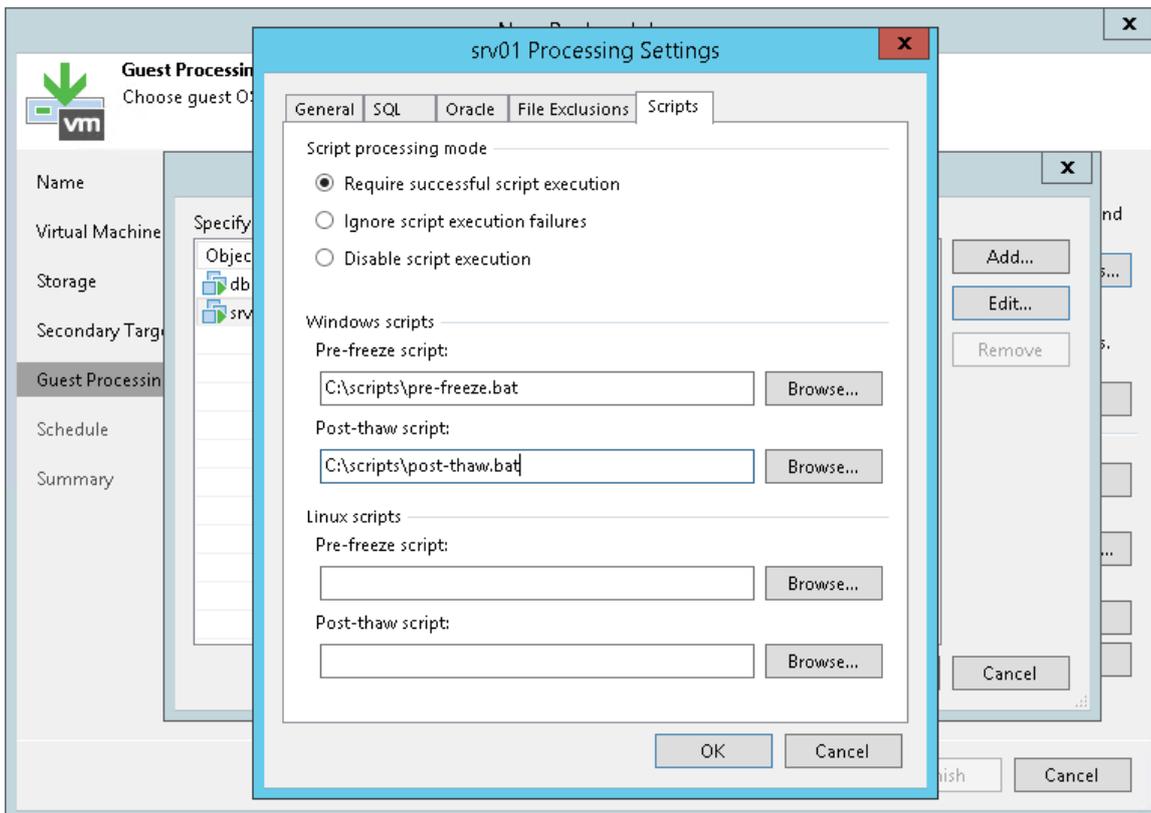
1. At the **Guest Processing** step, click **Applications**.
2. In the displayed list, select the VM and click **Edit**.
3. Click the **Scripts** tab.

4. In the **Script processing mode** section, specify the scenario for scripts execution:
 - Select **Require successful script execution** if you want Veeam Backup & Replication to stop the backup process if the script fails.
 - Select **Ignore script execution failures** if you want to continue the backup process even if script errors occur.
 - Select **Disable script execution** if you do not want to run scripts for the VM.
5. In the **Windows scripts** section, specify paths to pre-freeze and post-thaw scripts for Microsoft Windows VMs. Veeam Backup & Replication supports scripts in the EXE, BAT, CMD, WSF, JS, and PS1 file format.
6. In the **Linux scripts** section, specify paths to pre-freeze and/or post-thaw scripts for Linux VMs. Veeam Backup & Replication supports scripts of the SH file type.

If you have added to the job a VM container with Microsoft Windows and Linux VMs, you can select to execute both Microsoft Windows and Linux scripts for the VM container. When the job starts, Veeam Backup & Replication will automatically determine what OS type is installed on the VM and use corresponding scripts to quiesce this VM.

TIP:

Beside pre-freeze and post-thaw scripts for VM quiescence, you can instruct Veeam Backup & Replication to run custom scripts before the job starts and after the job completes. For more information, see [Script Settings](#).



VM Guest OS File Indexing

To specify VM guest OS indexing options for a VM:

1. At the **Guest Processing** step of the wizard, click **Indexing**.

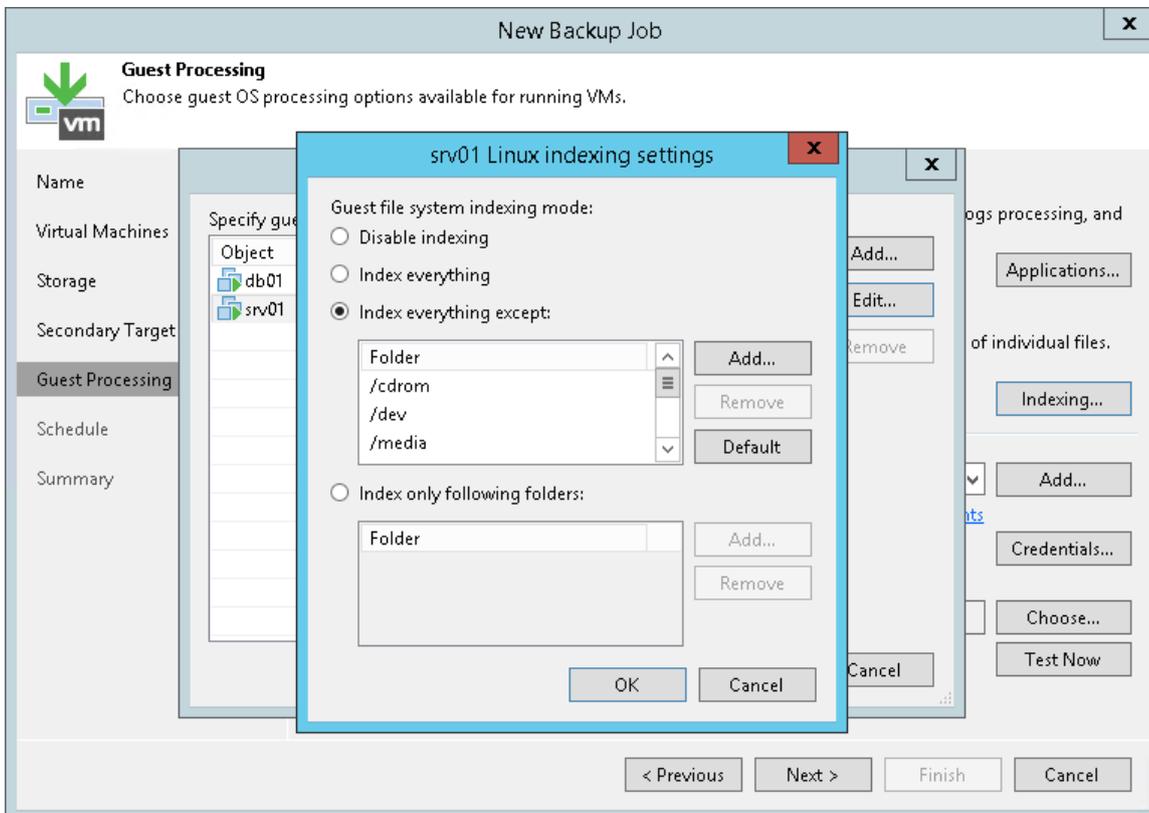
2. Select a VM in the list and click **Edit > Windows indexing** or **Linux indexing**.
3. Specify the indexing scope:
 - Select **Disable indexing** if you do not want to index guest OS files of the VM.
 - Select **Index everything** if you want to index all VM guest OS files.
 - Select **Index everything except** if you want to index all VM guest OS files except those defined in the list. By default, system folders are excluded from indexing. You can add or delete folders using the **Add** and **Remove** buttons on the right. You can also use system environment variables to form the list, for example: *%windir%*, *%ProgramFiles%* and *%Temp%*.
 - To reset the list of folders to its initial state, click **Default**.
 - Select **Index only following folders** to define folders that you want to index. You can add or delete folders to index using the **Add** and **Remove** buttons on the right. You can also use system environment variables to form the list, for example: *%windir%*, *%ProgramFiles%* and *%Temp%*.

NOTE:

For Linux system indexing, Veeam Backup & Replication requires several utilities to be installed on the Linux VM: openssh, mlocate, gzip and tar. If these utilities are not found, Veeam Backup & Replication will prompt you to deploy them on the VM guest OS.

IMPORTANT!

Guest OS file indexing over VIX API is not supported.



Step 10. Define Job Schedule

At the **Schedule** step of the wizard, select to run the backup 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 create the VM backup.
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 specific 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.

A repeatedly run job is started by the following rules:

- Veeam Backup & Replication 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 & Replication 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. A new backup job session will start as soon as the previous backup job session finishes.
 - 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 must define the time schedule for the first job in the chain. For the rest of the jobs in the chain, select the **After this job option** and choose the preceding job from the list.
3. In the **Automatic retry** section, define whether Veeam Backup & Replication must attempt to run the backup job again if the job fails for some reason. During a job retry, Veeam Backup & Replication processes failed VMs only. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication will retry the job for the defined number of times without any time intervals between the job runs.
 4. In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not provide unwanted overhead on the production environment. To set up a backup window for the job:
 - a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.
 - b. In the **Time Periods** section, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.

NOTE:

The **After this job** function will automatically start a job if the first job in the chain is started automatically by schedule. If you start the first job manually, Veeam Backup & Replication will display a notification. You will be able to choose whether Veeam Backup & Replication must start the chained job as well.

Schedule
Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Run the job automatically

Daily at this time: 10:00 PM Everyday Days...

Monthly at this time: 10:00 PM Fourth Saturday Months...

Periodically every: 1 Hours Schedule...

After this job: Apache Backup (Apache Backup Job)

Automatic retry

Retry failed VMs processing: 3 times
Wait before each retry attempt for: 10 minutes

Backup window

Terminate job if it exceeds allowed backup window Window...

If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

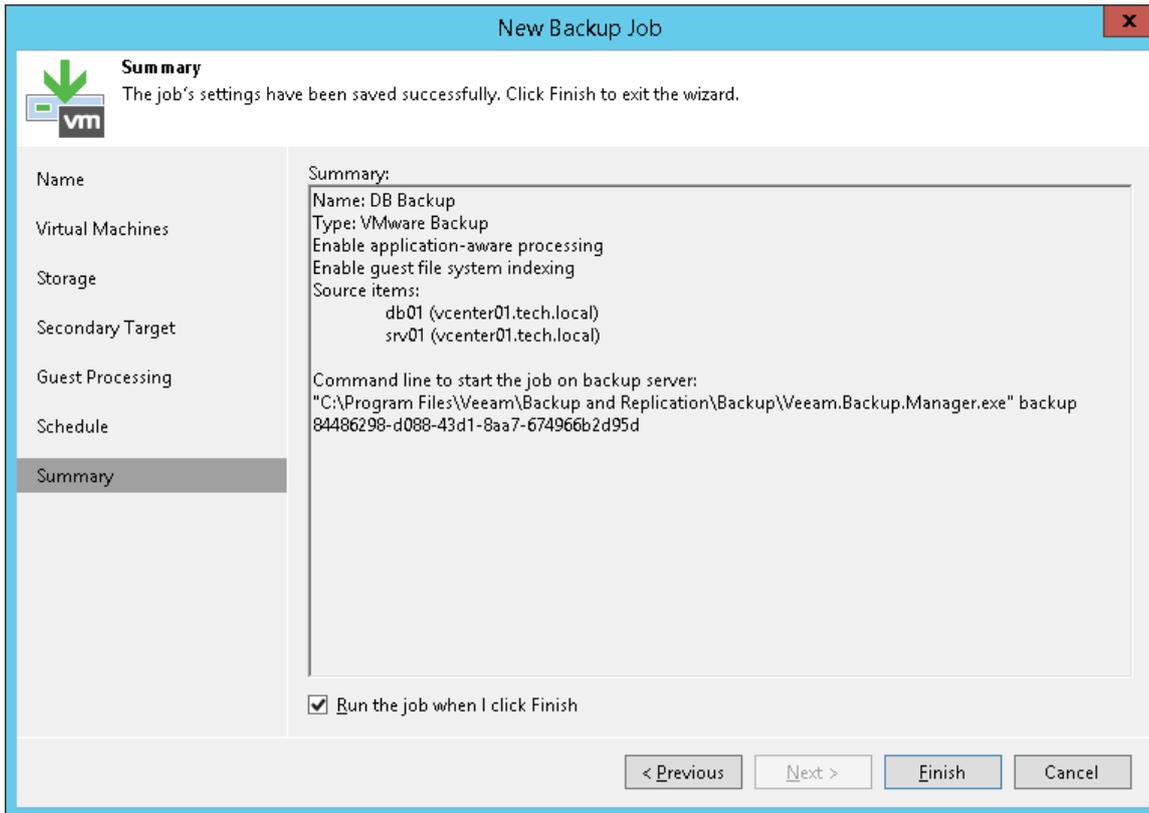
< Previous Apply Finish Cancel

Step 11. Finish Working with Wizard

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

1. Review details of the backup 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.

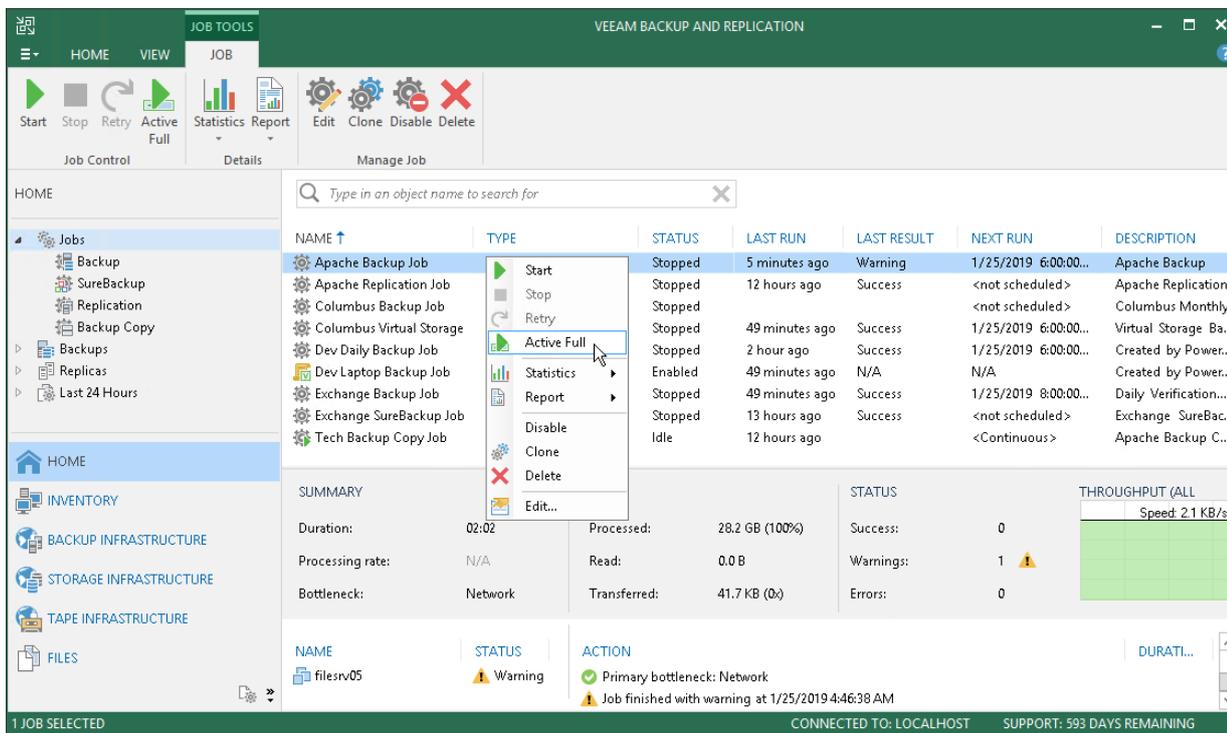


Performing Active Full Backup

You can create an ad-hoc full backup – active full backup, and add it to the backup chain on the backup repository. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain on the backup repository until it is removed from the backup chain according to the retention policy.

To perform active full backup:

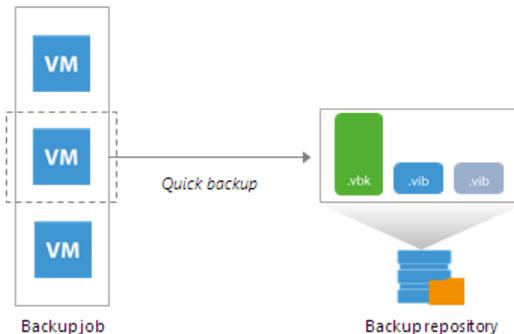
1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Active Full** on the ribbon or right-click the job and select **Active Full**.



Quick Backup

Quick backup lets you perform on-demand incremental backup for VMs. You can use quick backup if you want to produce an additional restore point for one or more VMs in a backup job and do not want to configure a new job or modify the existing one. Quick backup can be run for both incremental and reverse incremental backup chains.

Quick backup is an incremental backup task: Veeam Backup & Replication copies only changed data for selected VMs and saves this data to a new restore point in the backup chain. Similar to incremental backup, quick backup can only be run for VMs that have been successfully backed up at least once and has a full restore point. If there is no full restore point for a VM, quick backup cannot be performed.



To perform quick backup, Veeam Backup & Replication uses an existing backup job. When you start a quick backup task for a VM, Veeam Backup & Replication verifies that a backup job processing this VM exists on the backup server. If such job is detected, Veeam Backup & Replication triggers a job and creates an incremental restore point for the VM. If a backup job for the VM does not exist, quick backup is terminated.

You can run quick backup for one VM or more VMs at once. If you start quick backup for several VMs and these VMs are processed by different backup jobs, Veeam Backup & Replication triggers a set of backup jobs. Each triggered job creates a separate restore point and stores this restore point in a corresponding backup chain.

In some cases, a VM may be processed by several backup jobs on the backup server. In this case, Veeam Backup & Replication starts the job that has created the most recent restore point for the VM.

For example, *VM01* is processed by 2 jobs:

- *Backup job 1* created the most recent restore point on Monday
- *Backup job 2* created the most recent restore point on Tuesday

When you start quick backup for *VM01*, Veeam Backup & Replication will trigger *Backup job 2* to create a new incremental restore point.

NOTE:

If the quick backup task overlaps the scheduled backup job, the backup job waits for the quick backup task to complete.

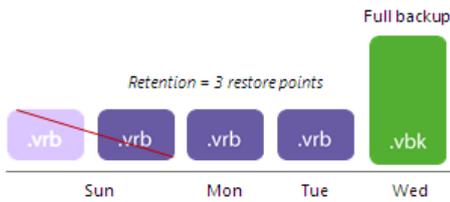
Limitations for Quick Backup

You cannot perform quick backup for vCloud Director VMs processed with vCloud Director jobs. However, if you process a vCloud Director VM with a regular backup job, you can switch to the **Computer** view and start the quick backup operation for this VM.

Retention Policy for Quick Backups

When you perform quick backup, Veeam Backup & Replication creates a single VM incremental restore point. Unlike a regular incremental restore point that contains data for all VMs in a job, single VM incremental restore point contains data only for a specific VM.

A single VM restore point is not regarded as full-fledged restore point in the backup chain. From the retention policy perspective, single VM restore point is grouped with a regular restore point following it. When Veeam Backup & Replication needs to delete a single VM restore point by retention, it waits for the next regular restore point to expire, and deletes two restore points at once.



Performing Quick Backup

You can create an ad-hoc incremental backup for one or more VMs – quick backup, and add it to the backup chain on the backup repository. Quick backup can be helpful if you want to produce an additional restore point for one or more VMs in the backup job and do not want to configure a new job or modify the existing one.

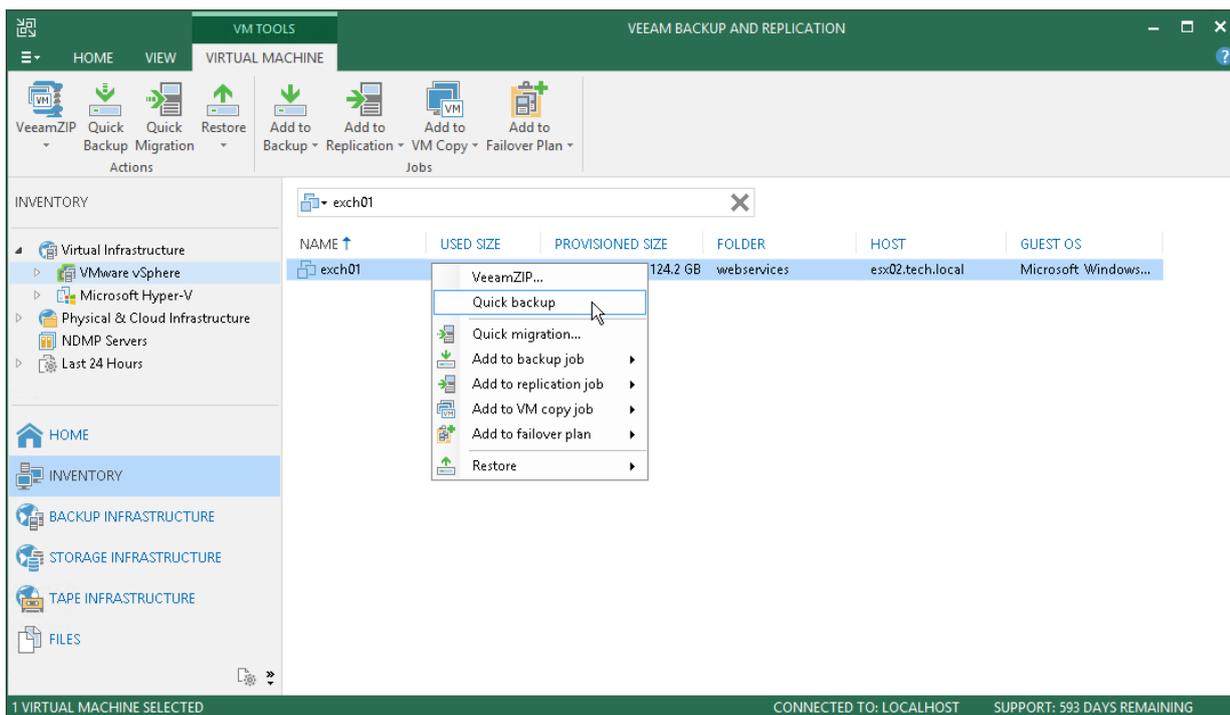
Quick backup can be performed for VMs that meet the following requirements:

1. A backup job processing the VM exists on the backup server.
2. A full backup file for the VM exists on the backup repository configured in the backup infrastructure.

To perform quick backup:

1. Open the **Inventory** view.
2. In the infrastructure tree, select a host or VM container in which the VMs that you want to back up reside.
3. In the working area, select the VMs and click **Quick Backup** on the ribbon. You can also right-click the VMs and select **Quick Backup**.

Veeam Backup & Replication will trigger a backup job to create a new incremental restore point for selected VMs. Details of a running quick backup task are displayed in the job session window.



Importing Backups

You may need to import backups to Veeam Backup & Replication in the following situations:

- The backup server has failed and you have restored it in a new location. You want to restore VM data from backups created by the backup server that has failed.
- You want to restore VM data from backups created on another backup server.
- You want to restore VM data from backups on the backup repository that is not added to the backup infrastructure (for example, if you removed it earlier).
- You want to restore VM data from VeeamZIP files created on your backup server or another backup server.

The imported backup becomes available in the Veeam Backup & Replication console. You can use any restore operation to recover VM data from this backup.

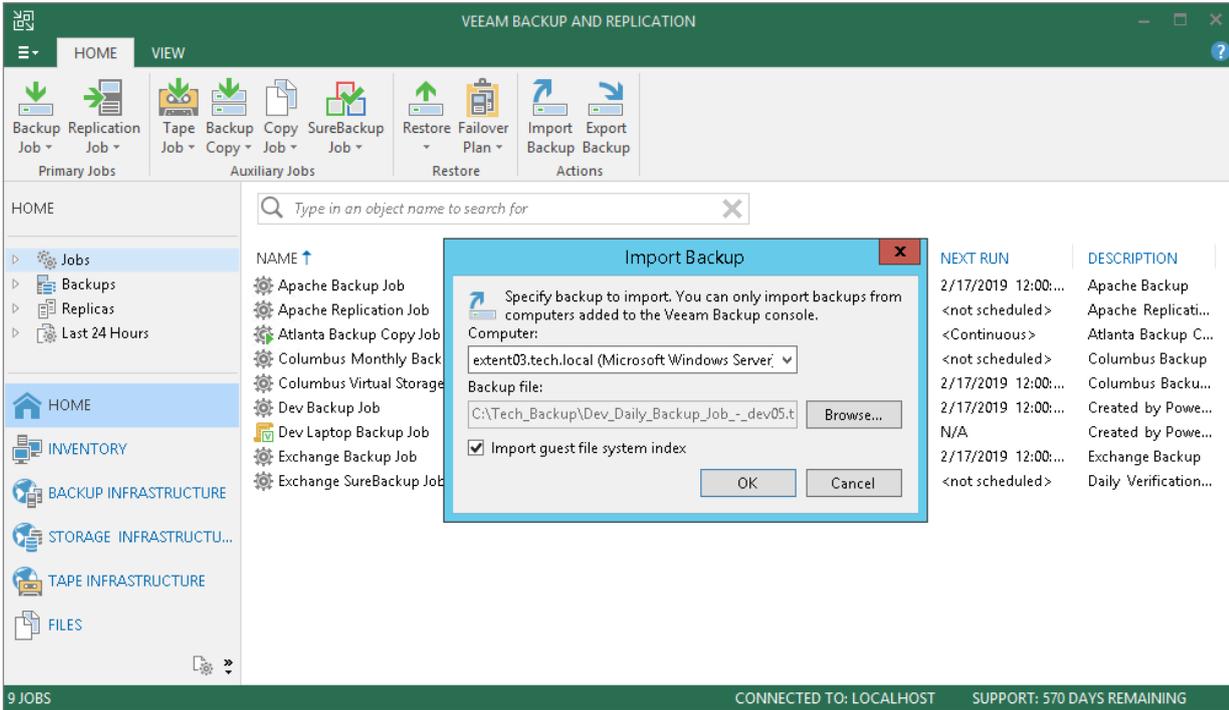
Before importing a backup, check the following prerequisites:

- The server from which you plan to import backups must be added to the backup infrastructure. Otherwise you will not be able to access backup files.
- To be able to restore VM data from previous backup restore points, make sure that you have all required incremental backup files (forward or reverse) in the same folder where the full backup file resides.

To import a backup to the Veeam Backup & Replication console:

1. On the **Home** tab, click **Import Backup**.
2. From the **Computer** list, select the server on which the backup you want to import is stored.
3. Click **Browse** and select the necessary VBM or VBK file. If you select the VBM file, the import process will be notably faster. It is recommended that you select the VBK file only if the VBM file is not available.
4. By default, index data of the VM guest OS file system is not imported with the backup to speed up the import process. If you want to import index data, select the **Import guest file system index** check box.

- Click **OK** to import the backup. The imported backup will be displayed in the **Home** view, under the **Backups > Imported** node in the inventory pane. Backups are imported using the original name of the backup job with the `_imported` suffix appended.



Importing Encrypted Backups

You can import backups that were encrypted on this backup server or on another backup server.

To import an encrypted backup file:

1. On the **Home** tab, click **Import Backup**.
2. From the **Computer** list, select the host on which the backup you want to import is stored.
3. Click **Browse** and select the VBM or VBK file.
4. Click **OK**. The encrypted backup will appear under the **Backups > Disk (encrypted)** node in the inventory pane.
5. In the working area, select the imported backup and click **Specify Password** on the ribbon or right-click the backup and select **Specify password**.
6. In the **Password** field, enter the password for the backup file.

If you changed the password one or several times while the backup chain was created, you must enter passwords in the following manner:

- If you select a VBM file for import, you must specify the latest password that was used to encrypt files in the backup chain.
- If you select a VBK file for import, you must specify the whole set of passwords that were used to encrypt files in the backup chain.

If you enter correct passwords, Veeam Backup & Replication will decrypt the backup file. The backup will be moved under the **Backups > Disk (imported)** node in the inventory pane.

NOTE:

If you use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication and your backup servers are connected to Veeam Backup Enterprise Manager, you can recover data from encrypted backups even if the password is lost. For more information, see [Decrypting Data Without Password](#).



Importing Transaction Logs

You cannot import transaction log backups without VM backups (as there will be no restore point to which the transaction logs can be applied).

To import a VM backup with transaction log backups, do either of the following:

- Import a backup metadata file (VBM). In this case, Veeam Backup & Replication will automatically import the database backup and log backups.
- Import a full backup file (VBK). In this case, Veeam Backup & Replication will browse to corresponding log backups and import them, too.

Importing Backup Files from Scale-Out Backup Repositories

You cannot import a backup directly from the scale-out backup repository. When you perform backup import, you cannot browse through all extent of the scale-out backup repository. Veeam Backup & Replication lets you browse only through individual extents.

To import a backup from the scale-out backup repository, you must place backup files from all extents to one staging folder. The staging folder can reside on any server added to the backup infrastructure. After that, you can import the backup as usual.

Exporting Backups

Exporting backups allows you to synthesize a complete and independent full backup file out of selected restore points that are located in your backup repositories. That is, you can transform any incremental or reverse-incremental backup chain (i.e all dependent *.vbk*, *.vib* or *.vrb* files) into a standalone *.vbk* file.

Export applies to *Full*, *Incremental* and *Reverse-incremental* restore points located in:

- Backup repositories.
- Object storage repositories.
- Backup repositories of cloud service providers and their tenants.

Consider the following:

- The restore point that is being exported as a new full backup file is saved to the same repository, wherein the source selected restore points reside.
- Once export is complete, the exported backup files will be attached under the **Backups > Disk (Imported)** node.
- If a restore point that is being exported resides on the tenant side, a new full backup file will also be exported to the same repository (on the tenant side) from which the source restore point is being taken.
- If a tenant initiates export of a restore point that resides in the *subtenant* directory, a new full backup file will be exported to the *tenant* directory.
- If you select a backup job consisting of multiple virtual machines, Veeam will synthesize a separate full backup file per each machine.
- When exporting VMs from vCloud Director (vCD) backups, all the VMs will be exported without vApps, that is, a new full backup file will be exported as a simple VMWare backup, not vCD backup. For more information about vCD backups, see [Backup of vCloud Director VMs](#).
- Export session results are saved to the configuration database and available for viewing, as described in [Viewing Session Statistics](#).

Performing Export

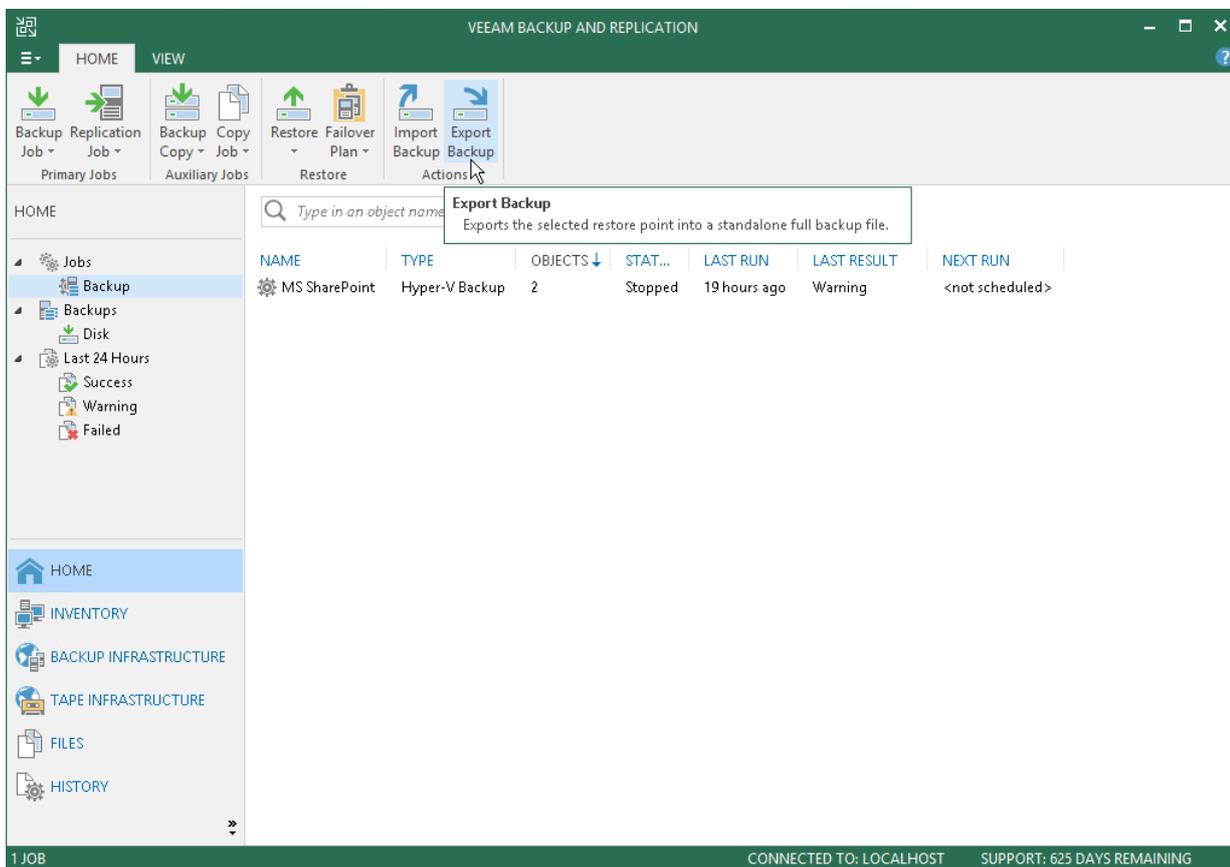
To export data, do the following:

1. [Launch New Export Wizard](#)
2. [Select Restore Points to Export](#)
3. [Specify Export Reason](#)
4. [Finish Working with Wizard](#)

Step 1. Launch New Export Wizard

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

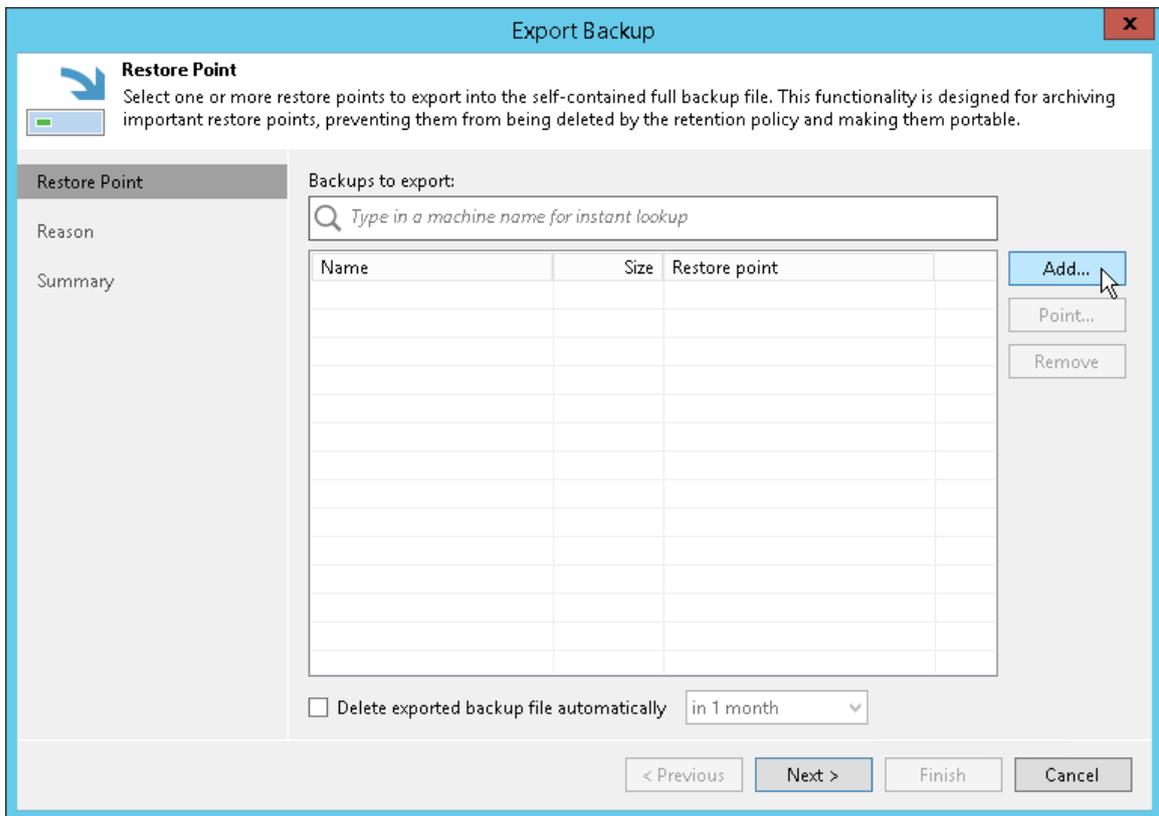
- On the **Home** tab, click **Export Backup**.
- In the **Home** view, under the **Backups > Disks** node, select a VM you want to transform into a full backup file and click **Export backup**.



Step 2. Select Restore Points to Export

At the **Restore Point** step of the wizard, do the following:

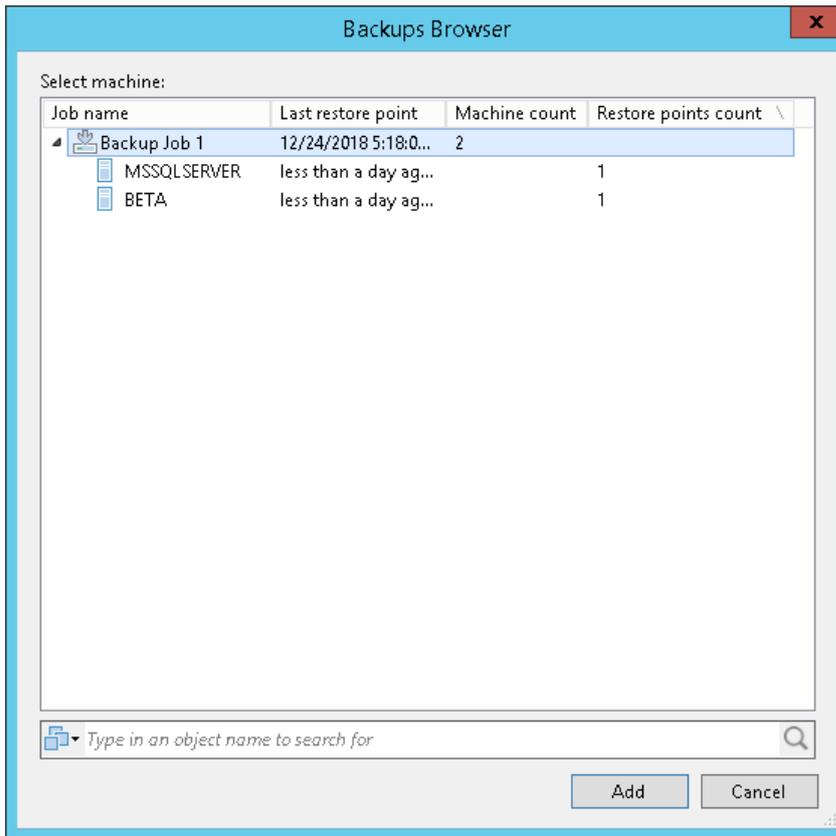
1. Click **Add** to select a VM, the restore points of which you want to transform into full backup files.



2. In the **Backups Browser** dialog, select a backup job or virtual machine.

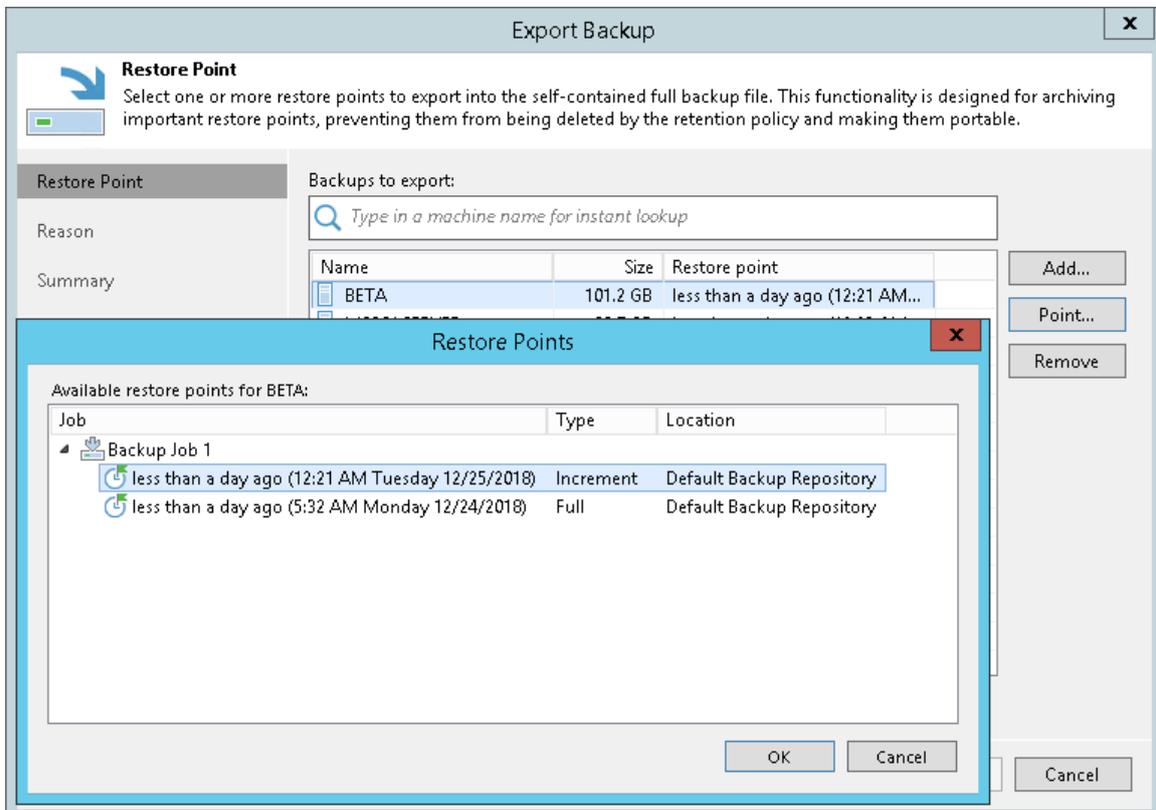
When selecting a backup job consisting of multiple machines, then each machine will be exported as an independent full backup file.

Use the search field at the bottom of the dialog to find particular VMs in the list.

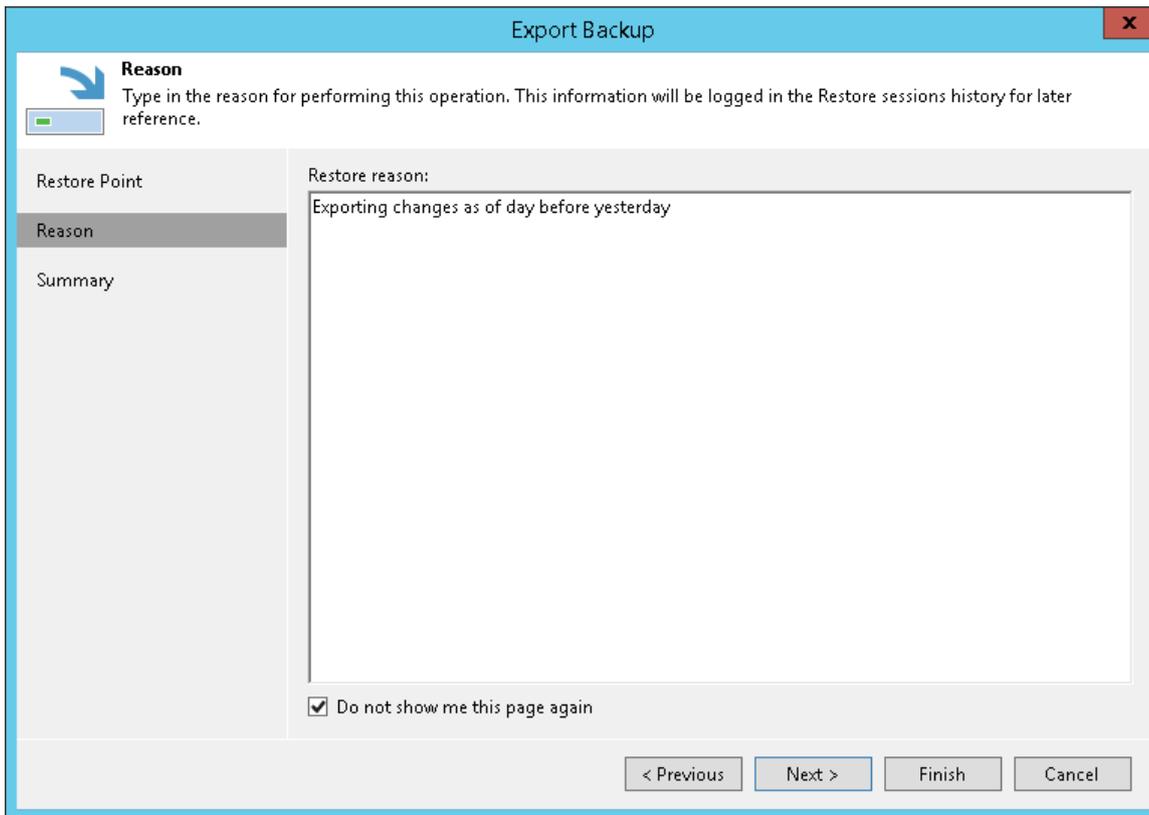


3. Select a VM from the table and click **Point** to select a restore point that you want to transform into a full backup file.

By default, the latest available restore point is selected.

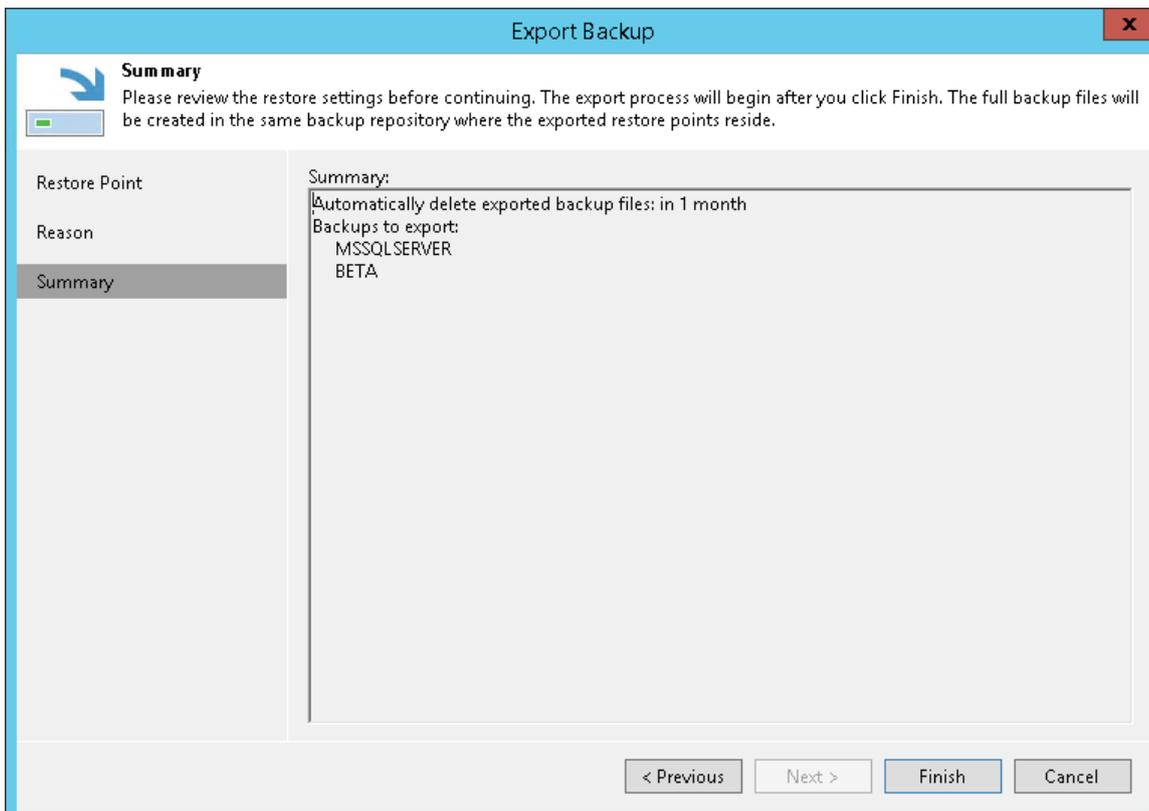


If you do not want to see this step in future, select the **Do not show me this page again** checkbox at the bottom of the dialog.



Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information, click **Finish** and wait until the restore session, which is described in [Viewing Session Statistics](#), is complete.



Viewing Session Statistics

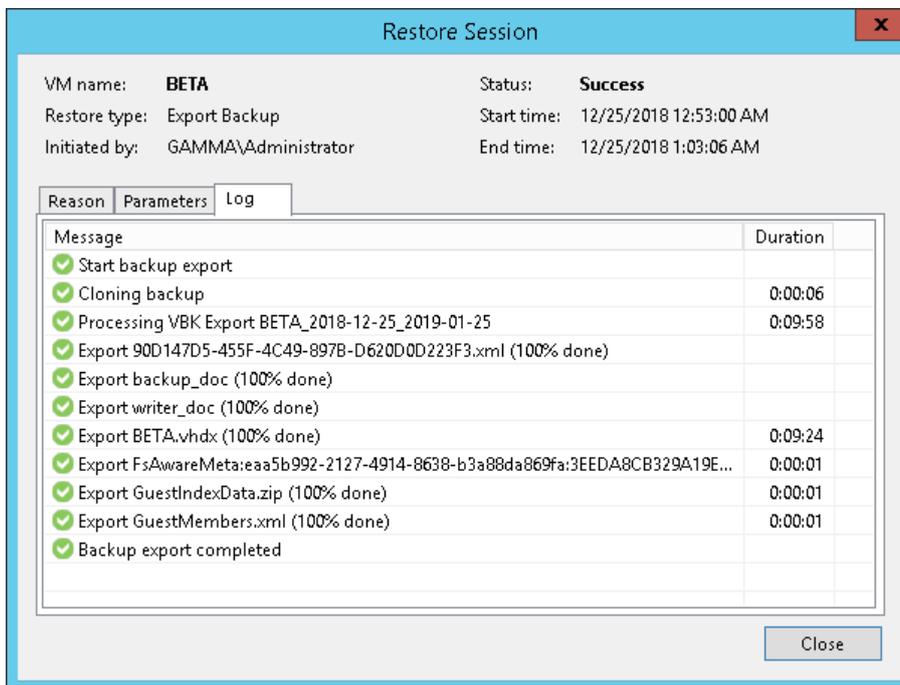
Once you invoke the export procedure, Veeam shows the **Restore Session** progress dialog that informs you of the current export status.

You can close the dialog by clicking the **Close** button in the lower-right corner and let Veeam perform export in the background.

As each export session saves its results to the configuration database, you can review them at any time.

To review the export session results, do the following:

1. In the inventory pane, go to the **History** view and select the **Restore > Export** node.
2. In the working area, double-click a machine for which you want to review the session results or right-click a machine and select **Statistics**.

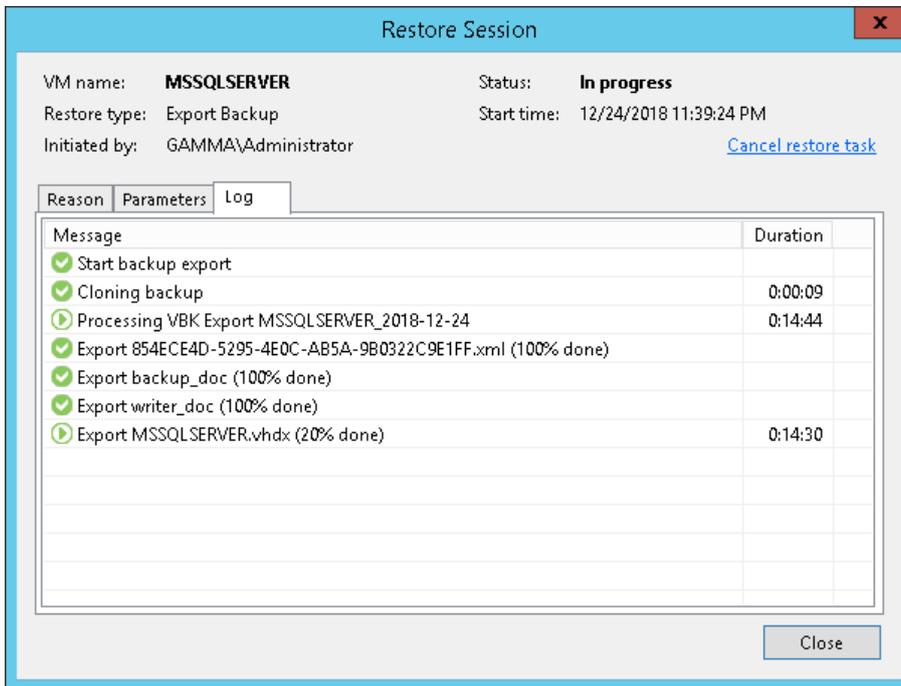


The **Restore Session** dialog contains the following tabs:

- The **Reason** tab – shows you the reason of export you may have provided at the [Specify Export Reason](#) step of the wizard.
- The **Parameters** tab – shows you the date when the exported backup files will be removed due to the retention policy you may have configured at the [Select Restore Points to Export](#) step of the wizard. In this tab you can also find a backup name and Date/time of a restore point that was synthesized into a full backup file.
- The **Log** tab – shows you the actual export progress.

Canceling Session

To cancel a session, open the **Restore Session** dialog, as described above, and click **Cancel restore task** in the upper-right corner of the dialog.



Managing Backups

You can perform the following operations with backups:

- [View backup properties](#)
- [Remove a backup from configuration](#)
- [Delete a backup from disks](#)
- [Remove missing restore points](#)

Viewing Properties

You can view summary information about created backups. The summary information provides the following data:

- Available restore points
- Date of restore points creation
- Compression and deduplication ratios
- Data size and backup size

To view summary information for backups:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click the backup and select **Properties**.
4. To see the list of available restore points, select the required object from the **Objects** list.

Backup Properties Exchange Backup Job

Repository: Storage 01 Folder: C:\Backup Repository\Exchange Backup Job\

Files:

NAME	DATA SIZE	BACKUP SIZE	DEDUPLICATION	COMPRESSION	DATE
Exchange Backup Job_D457D2019-01...	407 MB	239 MB	1.0x	1.8x	1/25/2019 3:06:08 AM
Exchange Backup Job_2AD9D2019-01...	113 KB	21.1 MB	1.0x	1.0x	1/25/2019 12:00:30 AM
Exchange Backup Job_EA7AD2019-01...	113 KB	21.1 MB	1.0x	1.0x	1/24/2019 8:00:35 PM
Exchange Backup Job_1B1ED2019-01-...	220 GB	24.7 GB	5.8x	1.5x	1/24/2019 3:56:27 PM

Objects:

NAME	ORIGINAL SIZE
dc03	20.1 GB
dns01	17.0 GB
exch01	27.5 GB

Restore points:

DATE	TYPE	STATUS
1/25/2019 3:06:30 AM	Increment	OK
1/25/2019 12:00:54 AM	Increment	OK
1/24/2019 8:00:56 PM	Increment	OK
1/24/2019 3:56:56 PM	Full	OK

OK

Removing from Configuration

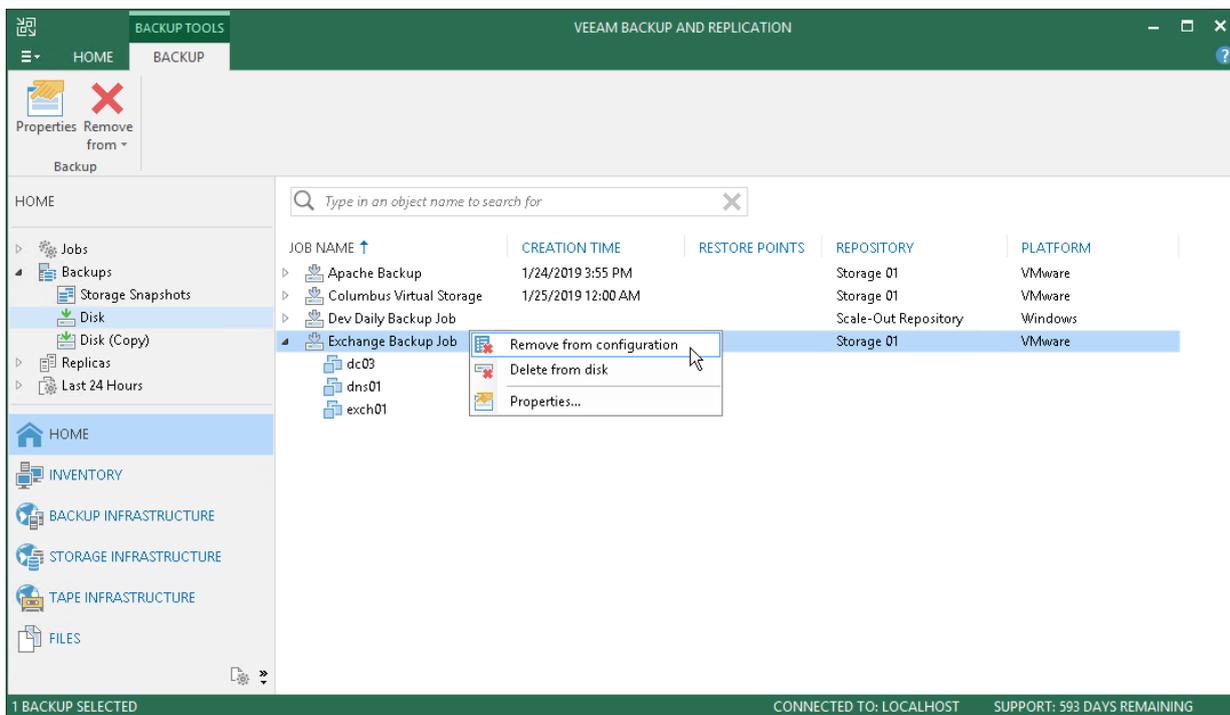
If you want to remove records about backups from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation.

When you remove a backup from the configuration, backup files (VBK, VIB, VRB, VBM) remain on the backup repository. You can import the backup later and restore VM data from it.

When you remove an encrypted backup from configuration, Veeam Backup & Replication removes encryption keys from the configuration database. If you import such backup on the same backup server or another backup server, you will have to specify the password or unlock the backup with Veeam Backup Enterprise Manager. For more information, see [Importing Encrypted Backups](#).

To remove a backup from the configuration:

1. Open the **Home** view.
2. In the inventory pane, select **Backups** or **Replicas**.
3. In the working area, select the backup and click **Remove from > Configuration** on the ribbon. You can also right-click the backup and select **Remove from configuration**.



Deleting from Disk

If you want to delete records about backups from the Veeam Backup & Replication console and configuration database and, additionally, delete backup files from the backup repository, you can use the **Delete from disk** operation. When you delete backup files from a disk, Veeam Backup & Replication deletes the whole chain from the backup repository. Thus, on the next run of the backup job, Veeam Backup & Replication will create full backups for VMs included in the job.

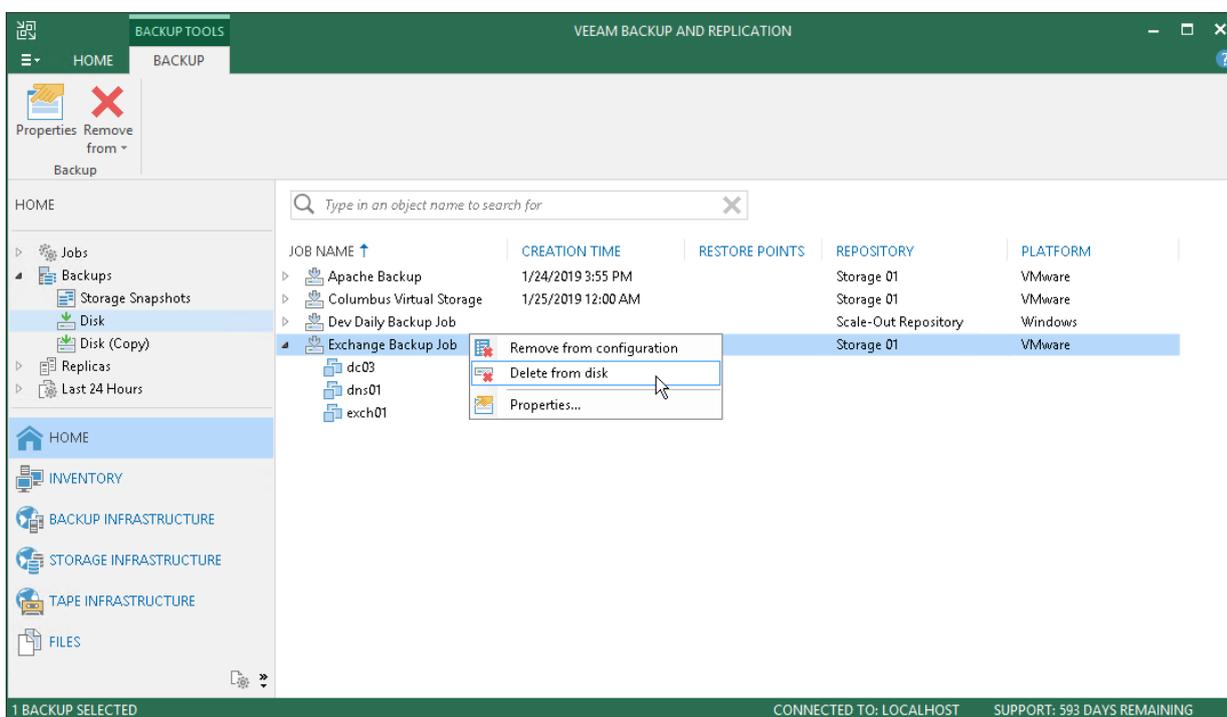
Mind the following:

- Do not delete backup files from the backup repository manually. Use the **Delete from disk** option instead. If you delete backup files manually, subsequent backup or replication job sessions will fail.
- If the per-VM functionality is enabled, you can perform the **Delete from disk** operation for separate VMs in the backup. If you delete backup files for one VM, on the next run of the backup job Veeam Backup & Replication will create a full backup for VMs whose backup files are deleted. For all other VMs, Veeam Backup & Replication will create increments.

To learn more about per-VM backup files, see [Per-VM Backup Files](#)

To delete backup files from the backup repository, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Backups** or **Replicas**.
3. In the working area, select the backup or separate VM in the backup and click **Remove from > Disk** on the ribbon. You can also right-click the backup and select **Delete from disk**.



Removing Missing Restore Points

In some cases, one or more restore points in the backup chain may be not accessible. This can happen, for example, if the backup repository is put to the maintenance mode (for scale-out backup repositories), the backup repository is not available or some backup file is missing in the backup chain. Backup chains that contain missing restore points get corrupted – you cannot perform backup or restore VM data from the missing restore point, and restore points that depend on the missing restore point.

You can perform two operations with missing restore points:

- **Forget** – you can remove records about missing restore points from the configuration database. Veeam Backup & Replication will “forget” about missing restore points and will not display them in the console. The backup files themselves will remain on disk (if backup files are still available).
- **Delete** – you can remove records about missing restore points from the configuration database and delete backup files from disk (if backup files are still available).

NOTE:

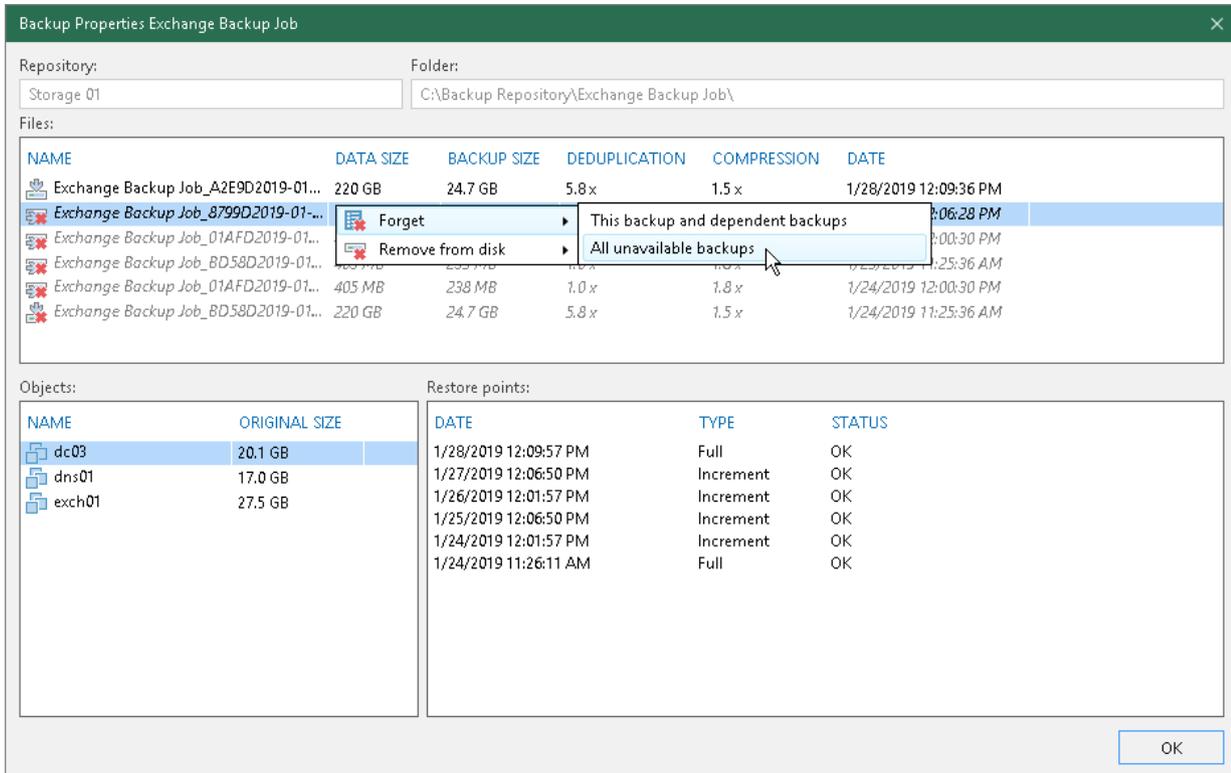
Consider the following:

- The **Forget** and **Delete from disk** options are available only for restore points that are missing from the backup chain or points that depend on missing ones. If the restore point is available in the backup chain and does not depend on a missing restore point, you will not be able to use the **Forget** and **Delete from disk** options for it.
- Veeam Backup & Replication may require some time to update information in the configuration database for restore points that were removed from a backup chain or became inaccessible. Therefore, such restore points may not be displayed in the console as missing restore points. To overcome this situation and reveal missing restore points, you can update information in the configuration database manually. To do that, disable the associated backup job and rescan a backup repository that is configured as a target for this job.

To remove records about missing restore points from the configuration database:

1. Open the **Home** view.
2. In the inventory pane, select **Disk** under **Backups**.
3. In the working area, select the backup and click **Properties** on the ribbon or right-click the backup and select **Properties**.

4. In the **Backup Properties** window, right-click the missing restore point and select **Forget**.
 - To remove only the selected restore point and restore points that depend on it (that is, a part of the backup chain starting from this restore point), select **This and dependent backups**.
 - To remove all missing restore points, select **All unavailable backups**.

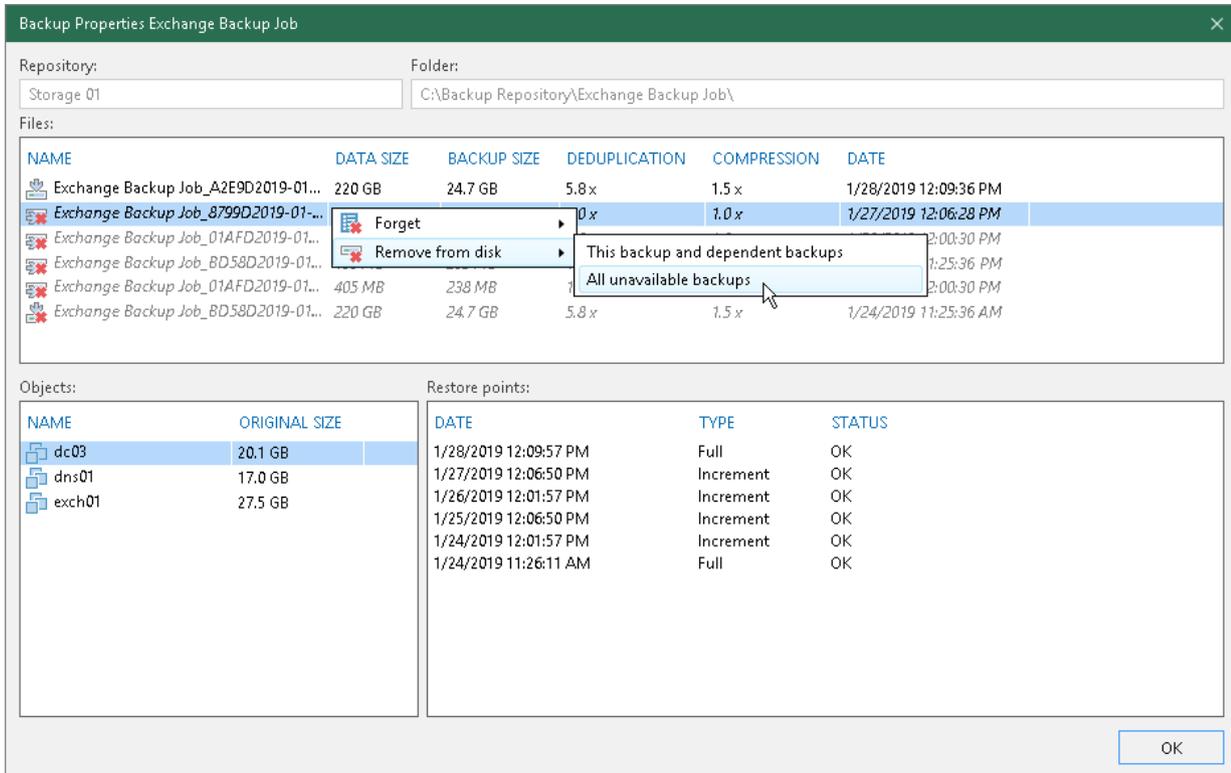


To remove missing restore points from the configuration database and disk:

1. Open the **Home** view.
2. In the inventory pane, click **Disk** under **Backups**.
3. In the working area, select the backup and click **Properties** on the ribbon or right-click the backup and select **Properties**.

4. In the **Backup Properties** window, right-click the missing restore point and select **Delete from disk**.

- To remove only the selected restore point and restore points that depend on it (that is, a part of the backup chain starting from this restore point), select **This and dependent backups**.
- To remove all missing restore points, select **All unavailable backups**.



Managing Capacity Tier Data

Continue with this section to learn more about:

- [Moving Backups to Capacity Tier](#)
- [Copying Backups to Performance Tier](#)
- [Viewing Capacity Tier Sessions Statistic](#)

Moving to Capacity Tier

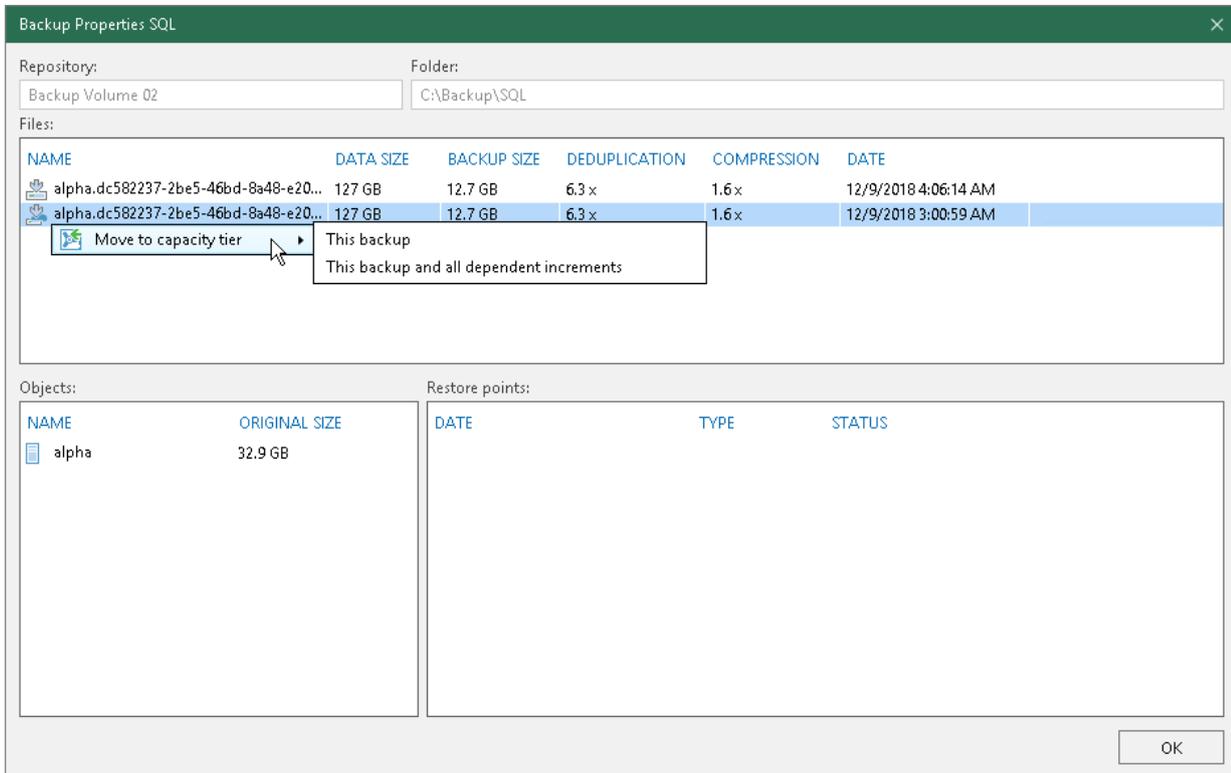
The **Move to capacity tier** option allows you to:

- Manually offload selected backup files to object storage repositories.
Consider that backup files you want to offload must belong to an inactive backup chain. For more information, see [Backup Chain Legitimacy](#).
- Remove blocks of data that were copied, as described in [Copying to Performance Tier](#).
Mind that such copied blocks will only be removed from the extents, not from object storage.

To move your backup data to capacity tier, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click a backup job and select **Properties**.
4. In the **Properties** window, right-click a backup file that either:
 - Belongs to an inactive backup chain.
When moving such a backup, Veeam initiates a new session of the **SOBR Offload** job. For more information, see [SOBR Offload Job](#).
 - Was replenished by copying offloaded data from object storage. For more information, see [SOBR Download Job](#).
When moving such a backup, Veeam simply removes all the copied blocks of data from the selected backup file, leaving it only with metadata. Nothing is going to be offloaded in such a scenario.
5. Select **Move to capacity tier** and click:
 - For *.vib/.vbk* backup files:
 - **This backup and all dependent increments** – to offload the selected backup along with its associated increments or to remove all the copied blocks of data from the selected backup and its associated increments.

- For *.vbk* backup files:
 - **This backup** – to offload a full backup only or to remove all the copied blocks of data from such a full backup.
 - **This backup and all dependent increments** – to offload the selected backup along with its associated increments or to remove all the copied blocks of data from the selected backup and its associated increments.



Copying to Performance Tier

The **Copy to performance tier** option allows you to download offloaded data from object storage repositories back to the source extents. For more information about how Veeam downloads the backup data, see [SOBR Download Job](#).

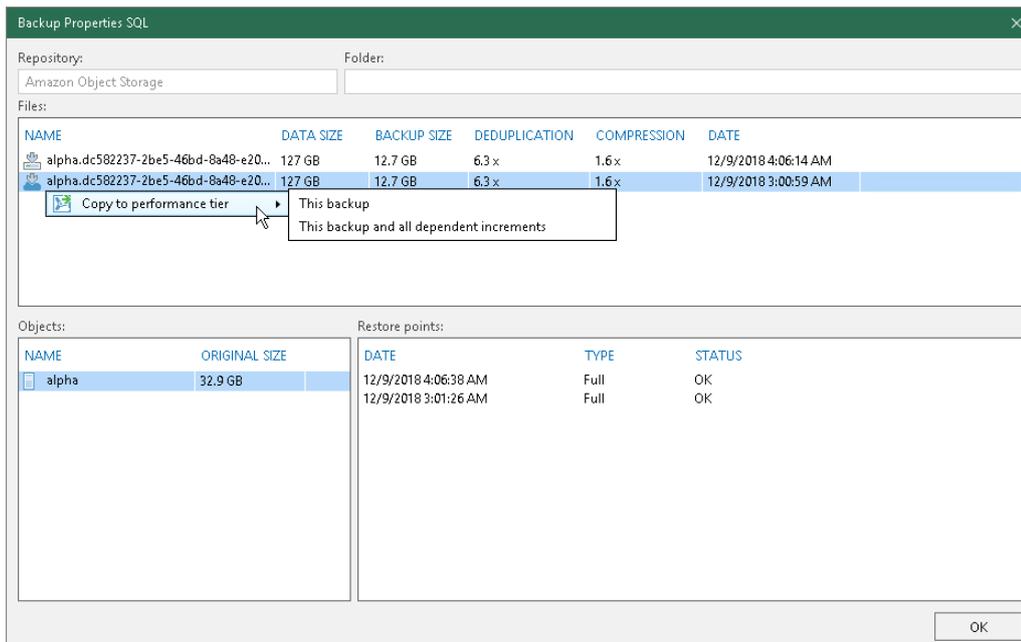
Copying offloaded data may be useful in certain situations. For example, you may want to transfer this data to any other storage device or perform certain operations with the VMs in a backup file and then offload it back to the cloud once you have done working with it.

To copy offloaded backup data back to the source extents, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click a backup job and select **Properties**.
4. In the **Properties** window, right-click an offloaded backup file, select **Copy to performance tier** and click:
 - For **.vib/.vbk** backup files:
 - **This backup and all dependent increments** – to copy the selected backup along with its associated increments.
 - For **.vbk** backup files:
 - **This backup** – to copy a full backup only.
 - **This backup and all dependent increments** – to copy the selected backup along with its associated increments.

NOTE:

To remove copied blocks from the extents, use the **Move to capacity tier** option, as described in [Moving to Capacity Tier](#).



Viewing Capacity Tier Sessions Statistic

Continue with this section to learn more about:

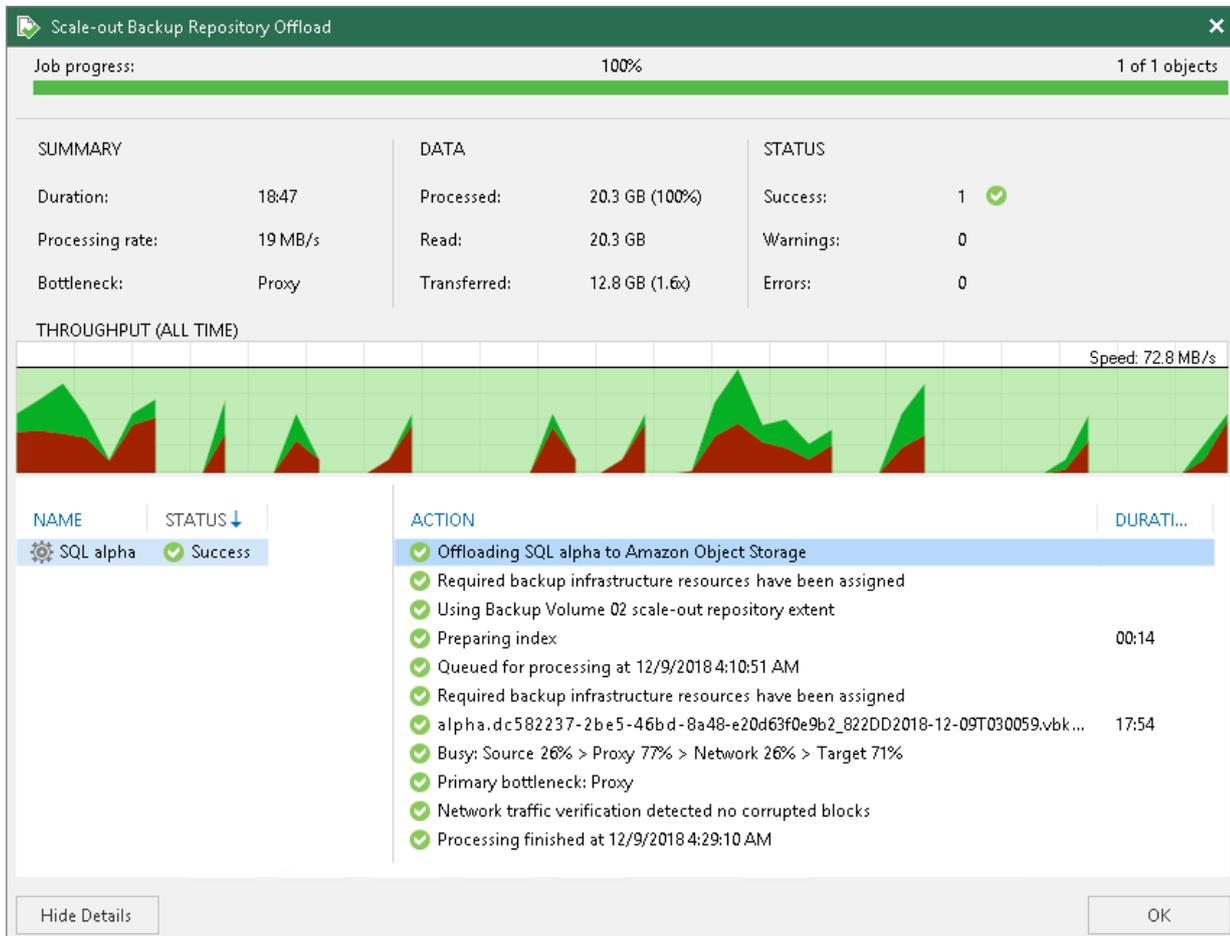
- [Viewing Offload Job Session Results](#)
- [Viewing Download Job Session Results](#)

Viewing Offload Job Session Results

To review the offload session results, do the following:

1. Switch to the **History** view.
2. In the inventory pane, select the **System** node.
3. In the preview pane, right-click the offload session and select **Statistics**.

For more information about the offload job, see [Data Transfer](#).



Veeam Backup & Replication displays the offload job session statistics for the following counters:

- The **Job progress** bar shows percentage of the offload session completion.
- The **Summary** box shows general information about the offload session:
 - **Duration** – duration of the offload session.

- **Processing rate** – average speed of VM data processing. This counter is a ratio between the amount of data that has actually been read and the offload session duration.
- **Bottleneck** – bottleneck in the data transmission process. To learn more about bottlenecks, see [Detecting Performance Bottlenecks](#).
- The **Data** box shows information about processed data:
 - **Processed** – total size of all VM disks processed by the offload session.
 - **Read** – the amount of data read from the extents.
 - **Transferred** – the amount of data transferred from the extents to object storage.
- The **Status** box shows information about the job results. This box informs how many tasks have completed with the *Success*, *Warning* and *Error* statuses (1 task per 1 VM).
- The pane in the lower-left corner shows a list of objects processed by the offload session.
- The pane in the lower-right corner shows a list of operations performed during the session. To see a list of operations for a specific object, click the object in the pane on the left. To see a list of operations for the whole offload session, click anywhere on the blank area in the left pane.

Viewing Download Job Session Results

To review the **SOBR Download** job session results, do the following:

1. Switch to the **History** view.
2. In the inventory pane, select the **System** node.
3. In the preview pane, right-click a **SOBR Download** session and select **Statistics**.

For more information about the **SOBR Download** job, see [Data Transfer](#).

The screenshot displays the 'SOBR Download' job progress window. At the top, the job progress is shown as 100% complete for 1 of 1 VMs. Below this, a summary table provides key metrics: Duration (03:39), Processing rate (179 MB/s), Bottleneck (Network), Processed (20.1 GB (100%)), Read (20.1 GB), Transferred (25.3 MB (815.4x)), Success (1), Warnings (0), and Errors (0). A throughput graph shows a peak speed of 238.0 MB/s. The lower section lists actions for the 'SQL alpha' object, including downloading from Amazon Object Storage, preparing files, and processing completion at 12/11/2018 11:48:08 PM.

Veeam Backup & Replication displays the **SOBR Download** job session statistics for the following counters:

- The **Job progress** bar shows percentage of the job completion.
- The **Summary** box shows general information about the job session:
 - **Duration** – duration of the job session.
 - **Processing rate** – average speed of data processing. This counter is a ratio between the amount of data that has actually been read and the job session duration.
 - **Bottleneck** – bottleneck in the data transmission process. To learn more about bottlenecks, see [Detecting Performance Bottlenecks](#).
- The **Data** box shows information about processed data:
 - **Processed** – total size of data blocks being downloaded from object storage repository plus blocks (if any) being taken from the extents of your scale-out backup repository.
 - **Read** – the amount of data read from both the object storage repository and extents of your scale-out backup repository.
 - **Transferred** – the amount of data downloaded from object storage.
- The **Status** box shows information about the job results. This box informs how many tasks have completed with the *Success*, *Warning* and *Error* statuses.
- The pane in the lower-left corner shows a list of objects processed by the job.

- The pane in the lower-right corner shows a list of operations performed during the session. To see a list of operations for a specific object, click the object in the pane on the left. To see a list of operations for the whole job session, click anywhere on the blank area in the left pane.

Managing Jobs

To view all jobs configured on the backup server, open the **Home** view and select the **Jobs** node in the inventory pane. The list of available jobs is displayed in the working area. You can edit job properties, start and stop jobs, restart failed jobs, clone jobs, view job statistics and delete unnecessary jobs.

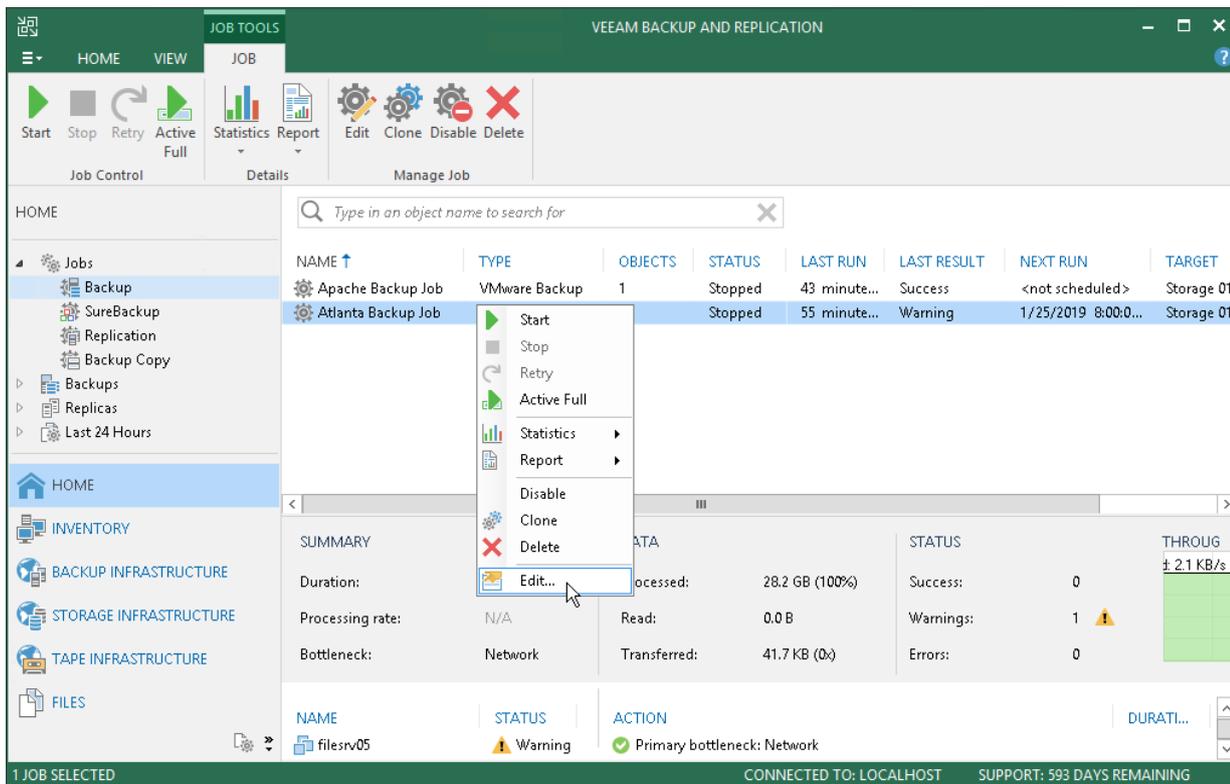
Editing Job Settings

You can edit configured jobs at any moment. For example, you may want to change scheduling settings for the job or add some VMs to the job.

To edit job settings:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Edit** on the ribbon or right-click the job and select **Edit**.

You will follow the same steps as you have followed when creating the job and can change job settings as required.



Cloning Jobs

You can create new jobs by means of job cloning. Job cloning allows you to create an exact copy of any job with the same job settings. Configuration information of the created job copy are written to the configuration database that stores information of the original job.

To create multiple jobs with similar settings, you can configure a set of jobs that will be used as 'job templates'. You can then clone these 'job templates' and edit settings of cloned jobs as required.

The name of the cloned job is formed by the following rule: *<job_name_clone1>*, where *job_name* is the name of the original job and *clone1* is a suffix added to the original job name. If you clone the same job again, the number in the name will be incremented, for example, *job_name_clone2*, *job_name_clone3* and so on.

When cloning job, Veeam Backup & Replication can change some job settings so that cloned jobs do not hinder original jobs.

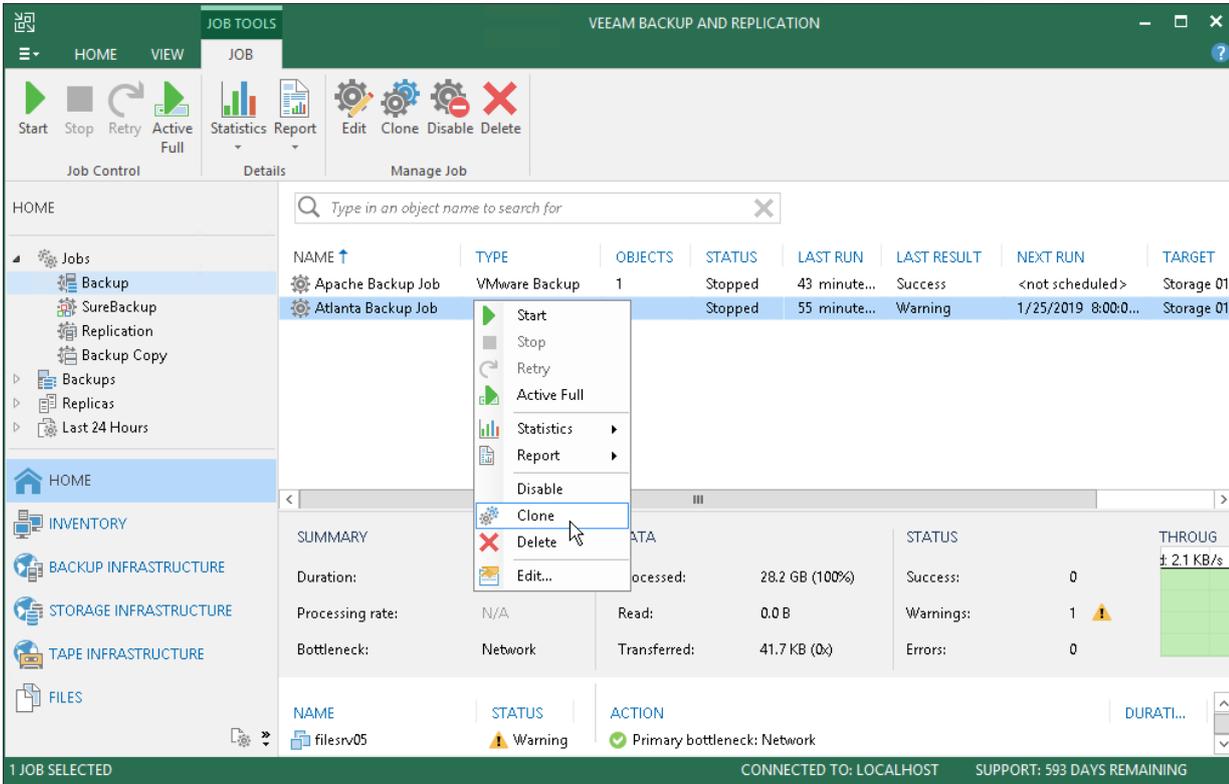
- If the original job is scheduled to run automatically, Veeam Backup & Replication disables the cloned job. To enable the cloned job, select it in the job list and click **Disable** on the ribbon or right-click the job and select **Disable**.
- If the original job is configured to use a secondary target, the cloned job is created without the secondary target settings.

To clone a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Clone** on the ribbon or right-click the job and select **Clone**.
4. After a job is cloned, you can edit all its settings, including the job name.

NOTE:

The job cloning functionality is available only in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.



Disabling and Removing Jobs

You can temporarily disable scheduled jobs. The disabled job is not deleted from Veeam Backup & Replication, it is paused for some period of time and is not run by the specified schedule. You can enable a disabled job at any time.

To disable a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Disable** on the ribbon or right-click the job and select **Disable**.

To enable a disabled job, select it in the list and click **Disable** on the ribbon once again.

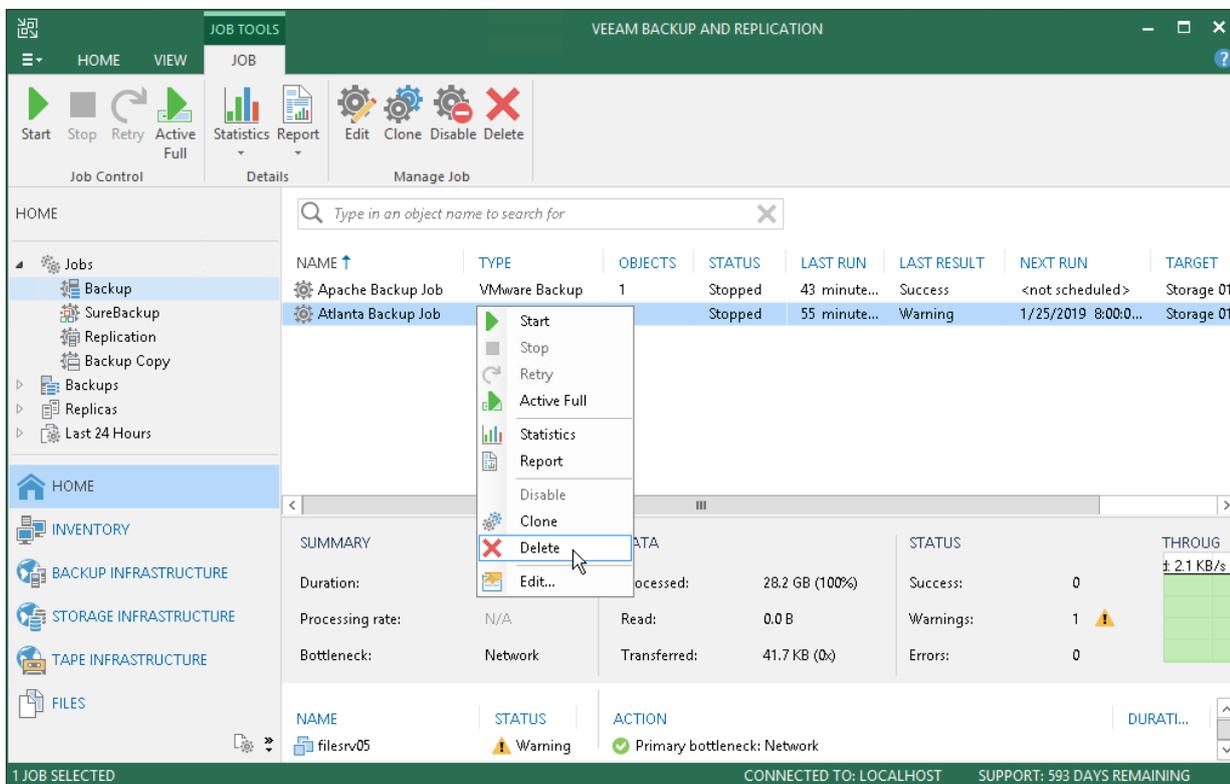
You can permanently remove a job from Veeam Backup & Replication and from the configuration database.

To remove a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the job and click **Delete** on the ribbon or right-click the job and select **Delete**.

NOTE:

If you want to permanently remove a backup copy job, you must first stop the synchronization process. To do this, disable the backup job. After the job is disabled, you can delete it.



Starting and Stopping Jobs

You can start job manually, for example, if you want to create an additional restore point for a VM backup or replica and do not want to change the job schedule. You can also stop a job, for example, if VM processing is about to take long, and you do not want the job to produce workload on the production environment during business hours.

Starting Jobs

To start a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup job and click **Start** on the ribbon or right-click the job and select **Start**.

Stopping Jobs

You can stop a job in one of the following ways:

- Stop job immediately. In this case, Veeam Backup & Replication will produce a new restore point only for those VMs that have already been processed by the time you stop the job.
- Stop job after current VM. In this case, Veeam Backup & Replication will produce a new restore point only for those VMs that have already been processed and for VMs that are being processed at the moment.

To stop a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup job and click **Stop** on the ribbon or right-click the job and select **Stop**. In the displayed window, click **Immediately**.

To stop the job after the current VM:

1. Open the **Home** view.
2. In the inventory pane, click **Jobs**.
3. In the working area, right-click the job and select **Stop**. In the displayed window, click **Gracefully**.

The screenshot shows the Veeam Backup and Replication console. The 'JOB TOOLS' tab is active, displaying a toolbar with 'Start', 'Stop', 'Retry', 'Active Full', 'Statistics', 'Report', 'Edit', 'Clone', 'Disable', and 'Delete'. The 'HOME' view is selected in the left-hand navigation pane. The main area shows a table of backup jobs:

NAME	TYPE	OBJECTS	STATUS	LAST RUN	LAST RESULT	NEXT RUN	TARGET
Apache Backup Job	Hyper-V Backup	1	Stopped	6 minutes...	Success	<not schedul...	Storage 01
Atlanta Backup Job	VMware Backup	1	6% comp...	2 minutes...		1/25/2019 8:0...	Storage 01

A dialog box titled 'Veeam Backup and Replication' is overlaid on the job table. It contains the following text: 'We can stop this job gracefully as soon as we are done with all VMs already being processed. Alternatively, we can kill the job immediately, leaving unusable restore points for such VMs. How would you like us to stop this job?'. The dialog has three buttons: 'Gracefully', 'Immediately', and 'Cancel'. A mouse cursor is pointing at the 'Immediately' button.

Below the dialog, the 'Job progress' bar shows 6% completion for 0 of 1 VMs. A summary table is also visible:

SUMMARY	DATA	STATUS	THROU
Duration: 02:23	Processed: 7.3 GB (6%)	Success: 0	5.5 MB/s
Processing rate: 124 MB/s	Read: 7.3 GB	Warnings: 0	
Bottleneck: Network	Transferred: 4.4 GB (1.7x)	Errors: 0	

The bottom status bar indicates '1 JOB SELECTED', 'CONNECTED TO: LOCALHOST', and 'SUPPORT: 593 DAYS REMAINING'.

Starting and Stopping Transaction Log Backup Jobs

If you create a backup job and instruct it to ship transaction logs, the backup job comprises 2 jobs:

1. A parent backup job creating an image-level backup of the VM on which the database runs. This job is named as a regular backup job, for example: *Daily Job*.
2. A transaction log backup job responsible for shipping transaction logs to the backup repository. This job is named by the following pattern:
 - For MS SQL: *<job_name> SQL Server Transaction Log Backup*. For example, *Daily Job SQL Server Transaction Log Backup*.
 - For Oracle: *<job_name> Oracle Redo Log Backup*. For example, *Daily Job Oracle Redo Log Backup*.

The transaction log backup job is created automatically by Veeam Backup & Replication if it detects that you have added to the backup job at least one Microsoft SQL Server or Oracle VM, enabled application-aware processing and instructed Veeam Backup & Replication to back up transaction logs periodically.

Starting Transaction Log Backup Jobs

A parent backup job is started manually when you click **Start** on the toolbar, or automatically by schedule. The transaction log backup job is initially started when you enable schedule for the parent backup job. The transaction log backup works continuously in the background. A new session of the transaction log backup job starts every time the parent backup job is launched.

Stopping Transaction Log Backup Jobs

You can stop transaction log processing in one of the following ways:

- [Disable transaction log shipping](#)
- [Disable the parent backup job](#)

If you want the backup job to create image-level backups of the VM but do not want it to ship transaction logs anymore, you can disable transaction log backup in the backup job settings.

To disable transaction log shipping:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup job and click **Edit** on the ribbon or right-click the backup job and select **Edit**.
4. Pass to the **Guest Processing** step of the wizard and click **Applications**.
5. In the **Application-Aware Processing Options** window, select the VM and click **Edit**.
6. On the **SQL** or **Oracle** tab of the **VM Processing Settings** window, disable transaction log backup.
7. Click **Finish** to save the job settings.

If you do not want to create image-level backups of the VM and back up database transaction logs, you can disable scheduling for the parent backup job. Veeam Backup & Replication will instruct the transaction log backup job to complete log processing for all VMs added to the parent backup job, and will switch the parent backup job to the non-scheduled mode. The parent backup job will no longer be started automatically by schedule – you will have to run it manually.

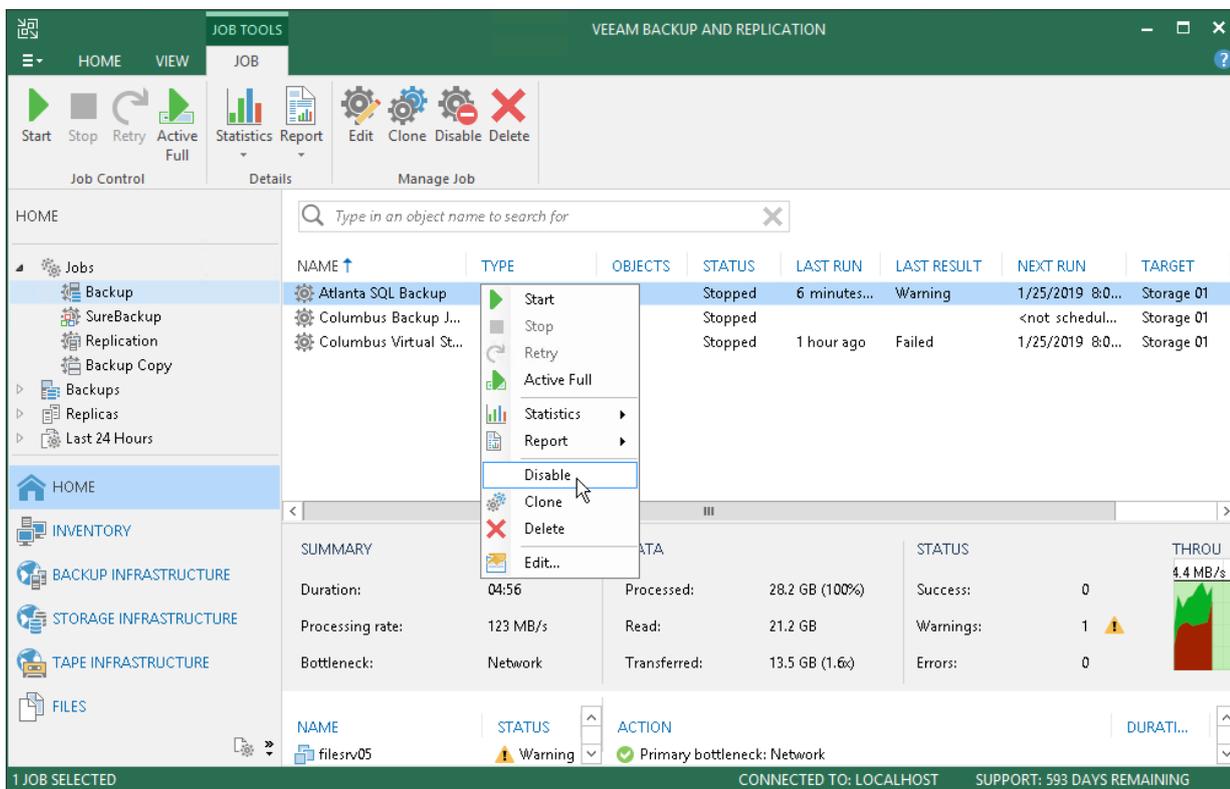
To disable scheduling for the parent backup job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup job and click **Edit** on the ribbon. Alternatively, you can right-click the the backup job and select **Edit**.
4. Pass to the **Schedule** step of the wizard and clear the **Run the job automatically** check box.
5. Click **Finish** to save the job settings.

Alternatively, you can disable the parent backup job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup job and click **Disable** on the ribbon or right-click the job and select **Disable**.

To re-activate transaction log processing for all VMs in the parent backup job, select the job in the list and click **Disable** on the ribbon once again.



Reconfiguring Jobs with Microsoft SQL Server VMs

In some situations, you may need to reconfigure a backup job that processes a Microsoft SQL Server VMs and ships transaction logs. For example, you may want to create a separate backup job to process the virtualized database, and delete the VM running the database from the previously created job.

When you configure a new job, mind the restriction on transaction logs shipping. By default, the new backup job that processes the VM will not ship transaction logs if transaction logs for this VM have been shipped for the last 7 days by another backup job on the same backup server.

You can overcome this restriction with registry keys. For more information, contact [Veeam Support Team](#).

Reporting

When you run a job, Veeam Backup & Replication saves the jobs statistics and operation data to the configuration database. You can view realtime statistics for any performed job and generate reports with statistics data for any job or separate job session.

Viewing Real-Time Statistics

To view real-time statistics for a job, do one of the following:

- Open the **Home** view, in the inventory pane select **Jobs, Last 24 hours** or **Running**. In the working area, double-click the job.
- Open the **Home** view, in the inventory pane select **Jobs, Last 24 hours** or **Running**. In the working area, right-click the job and select **Statistics**.

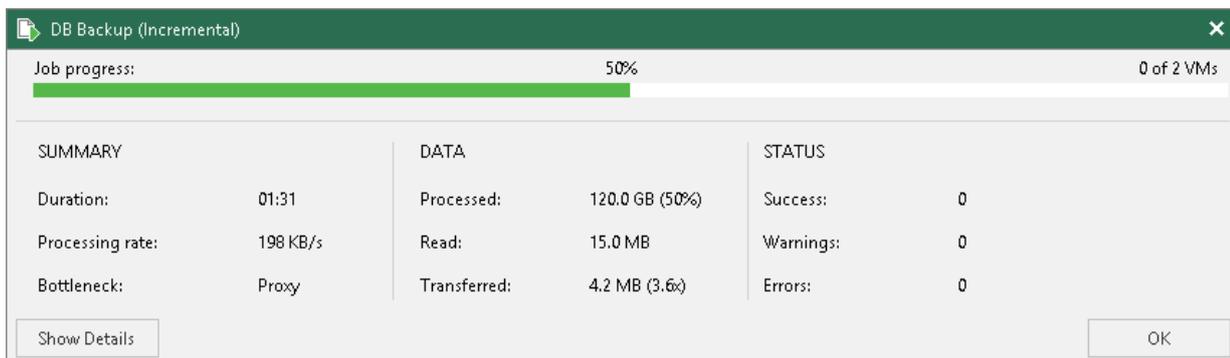
The real-time statistics provides detailed data on job sessions: job progress, duration, processing rate, performance bottlenecks, amount of processed data, read and transferred data and details of the session performance, for example, warnings and errors that have occurred in the process of operation.

In addition to overall job statistics, the real-time statistics provides information on each object processed with the job. To view the processing progress for a specific object, select it in the list on the left.

TIP:

Mind the following:

- To collapse and expand the real-time statistics window, use **Hide Details** and **Show Details** buttons at the bottom left corner of the window.
- To switch between the job sessions backward and forward, use left and right arrow keys on the keyboard.



Statistics Counters

Veeam Backup & Replication displays jobs statistics for the following counters:

- The **Job progress** bar shows percentage of the job completion.
- The **Summary** box shows general information about the job:
 - **Duration** – time from the job start till the current moment or job end.
 - **Processing rate** – average speed of VM data processing. This counter is a ratio between the amount of data that has actually been read and job duration.
 - **Bottleneck** – bottleneck in the data transmission process. To learn about job bottlenecks, see [Detecting Performance Bottlenecks](#).
- The **Data** box shows information about processed VM data:
 - **Processed** – total size of all VM disks processed by the job.

- **Read** – amount of data read from the datastore by the source-side Data Mover Service prior to applying compression and deduplication. For incremental job runs, the value of this counter is typically lower than the value of the **Processed** counter. Veeam Backup & Replication reads only data blocks that have changed since the last job session, processes and copies these data blocks to the target.
- **Transferred** – amount of data transferred from the source-side Data Mover Service to the target-side Data Mover Service after applying compression and deduplication. This counter does not directly indicate the size of the resulting files. Depending on the backup infrastructure and job settings, Veeam Backup & Replication can perform additional activities with data: deduplicate data, decompress data prior to writing the file to disk and so on. The activities can impact the size of the resulting file.
- The **Status** box shows information about the job results. This box informs how many tasks have completed with the *Success*, *Warning* and *Error* statuses (1 task per 1 VM).
- The pane at the lower left corner shows a list of objects included in the job.
- The pane at the lower right corner shows a list of operations performed during the job. To see a list of operations for a specific object included in the job, click the object in the pane on the left. To see a list of operations for the whole job, click anywhere on the blank area in the left pane.

Colored Graph

To visualize the data transfer process, Veeam Backup & Replication displays a colored graph in the real-time statistics window:

- The green area defines the amount of data read from source.
- The brown area defines the amount of data transported to target.
- The horizontal line defines the current data processing speed.

If the job session is still being performed, you can click the graph to view data rate for the last 5 minutes or the whole processing period. If the job session has already ended, the graph will display information for the whole processing period only.

The colored graph is displayed only for the currently running job session or the latest job session. If you open real-time statistics for past sessions other than the latest one, the colored graph will not be displayed.

DB Backup (Incremental) [Close]

Job progress: 32% 0 of 2 VMs

SUMMARY		DATA		STATUS	
Duration:	04:55	Processed:	17.3 GB (32%)	Success:	0
Processing rate:	32 MB/s	Read:	5.1 GB	Warnings:	0
Bottleneck:	Source	Transferred:	2.9 GB (1.8x)	Errors:	0

THROUGHPUT (LAST 5 MIN)

Speed: 29.5 MB/s

Read speed: 34 MB/s
Transfer speed: 13 MB/s
Time: Wednesday, February 20, 2019 7:26:45 AM
Click to switch to all time view

NAME	STATUS	ACTION	DURATION
db01	63%	✓ VM size: 150.0 GB (20.8 GB used)	
srv01	0%	✓ Getting VM info from vSphere	00:08
		✓ Creating VM snapshot	00:52
		✓ Saving [esx01-das1] crm_db_restored/crm_db_restored.vmx	00:00
		✓ Saving [esx01-das1] crm_db_restored/crm_db_restored.vmx	00:00
		✓ Saving [esx01-das1] crm_db_restored/crm_db_restored.nvram	00:00
		✓ Using backup proxy VMware Backup Proxy for disk Hard disk 2 [nbd]	00:00
		✓ Using backup proxy VMware Backup Proxy for disk Hard disk 1 [nbd]	00:00
		▶ Hard disk 1 (60.0 GB) 4.9 GB read at 29 MB/s [CBT]	03:06
		✓ Hard disk 2 (60.0 GB) 82.0 MB read at 49 MB/s [CBT]	00:08
		✓ Using backup proxy VMware Backup Proxy for disk Hard disk 3 [nbd]	00:00
		✓ Hard disk 3 (30.0 GB) 207.0 MB read at 37 MB/s [CBT]	00:18

Hide Details [OK]

Viewing Job Session Results

You can view detailed statistics on every job session.

To view statistics for a selected job session, do either of the following:

- Open the **History** view. In the inventory pane select **Jobs**. In the working area, double-click the necessary job session.
- Open the **History** view. In the inventory pane select **Jobs**. In the working area, right-click the necessary job session and select **Statistics**.

TIP:

To switch between past job sessions, use left and right arrow keys on the keyboard.

Job progress: 10% 0 of 1 VMs

SUMMARY		DATA		STATUS	
Duration:	17:27	Processed:	10.8 GB (10%)	Success:	0
Processing rate:	18 MB/s	Read:	10.8 GB	Warnings:	0
Bottleneck:	Source	Transferred:	6.9 GB (1.6x)	Errors:	0

THROUGHPUT (LAST 5 MIN)

Speed: 15.4 MB/s

NAME	STATUS	ACTION	DURATI...
pearl	▶ 10%	<ul style="list-style-type: none"> Queued for processing at 10/24/2017 3:39:12 AM Required backup infrastructure resources have been assigned VM processing started at 10/24/2017 3:39:19 AM VM size: 120.0 GB (50.7 GB used) Getting VM info from vSphere Creating VM snapshot Potential data sovereignty violation: target Backup Volume 01 location (Undefi... Saving [esx02-ds1] pearl/pearl.vmx Saving [esx02-ds1] pearl/pearl.nvram Using backup proxy VMware Backup Proxy for disk Hard disk 1 [nbd] Hard disk 1 (120.0 GB) 10.8 GB read at 18 MB/s [CBT] 	00:53 04:30 00:00 00:01 00:00 11:06

Hide Details OK

Viewing Job and Job Session Reports

You can generate reports with details about job and job session performance.

Job Report

The job report contains data on all sessions initiated for a specific job. To generate a job report:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary job and click **Report** on the ribbon. You can also right-click the job and select **Report**.

The session report contains data on a single job session:

- Cumulative session statistics: session duration details, details of the session performance, amount of read, processed and transferred data, backup size, compression and deduplication ratios.
- Detailed statistics for every VM processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).

TIP:

Generated reports are stored at the `C:\Users\\AppData\Local\Temp` folder.

Session Report

To generate a session report:

1. Open the **History** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the necessary session and click **Report** on the ribbon. You can also right-click the necessary session and select **Report**.

Backup job: DB Backup				Success				
Daily Backup Job				2 of 2 VMs processed				
Monday, January 9, 2017 12:59:59 AM								
Success	2	Start time	12:59:59 AM	Total size	290.0 GB	Backup size	1.5 GB	
Warning	0	End time	1:12:37 AM	Data read	16.2 GB	Dedupe	1.1x	
Error	0	Duration	0:12:38	Transferred	1.4 GB	Compression	2.1x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
db01	Success	1:00:56 AM	1:07:13 AM	150.0 GB	1.6 GB	692.0 MB	0:06:16	
srv01	Success	1:05:34 AM	1:12:28 AM	140.0 GB	14.6 GB	784.9 MB	0:06:54	

Replication

In addition to VM backups, you can create VM replicas with Veeam Backup & Replication. When you replicate a VM, Veeam Backup & Replication creates an exact copy of the VM in the native VMware vSphere format on a spare host, and maintains this copy in sync with the original VM.

Replication provides the best recovery time objective (RTO) values, as you actually have a copy of your VM in a ready-to-start state. That is why replication is commonly recommended for the most critical VMs that need minimum RTOs.

About Replication

Veeam Backup & Replication is built for virtual environments. It operates at the virtualization layer and uses an image-based approach for VM replication.

Veeam Backup & Replication does not install agent software inside the VM guest OS to retrieve VM data. To replicate VMs, it leverages VMware vSphere snapshot capabilities. When you replicate a VM, Veeam Backup & Replication requests VMware vSphere to create a VM snapshot. The VM snapshot can be thought of as a cohesive point-in-time copy of a VM including its configuration, OS, applications, associated data, system state and so on. Veeam Backup & Replication uses this point-in-time copy as a source of data for replication.

In many respects, replication works similarly to forward incremental backup. During the first replication cycle, Veeam Backup & Replication copies data of the original VM running on the source host, and creates its full replica on the target host. Unlike backup files, replica virtual disks are stored decompressed in their native format. All subsequent replication cycles are incremental. Veeam Backup & Replication copies only those data blocks that have changed since the last replication job session. To keep track of changed data blocks, Veeam Backup & Replication uses different approaches. For more information, see [Changed Block Tracking](#)

Veeam Backup & Replication lets you perform onsite replication for high availability (HA) scenarios and remote (offsite) replication for disaster recovery (DR) scenarios. To facilitate replication over the WAN or slow connections, Veeam Backup & Replication optimizes traffic transmission. It filters out unnecessary data blocks such as duplicate data blocks, zero data blocks, blocks of swap files and blocks of excluded VM guest OS files, and compresses replica traffic. Veeam Backup & Replication also allows you to use WAN accelerators and apply network throttling rules to prevent replication jobs from consuming the entire network bandwidth.

In Veeam Backup & Replication, replication is a job-driven process. To perform replication, you need to configure replication jobs. A replication job is a configuration unit of the replication activity. The replication job defines when, what, how and where to replicate. One replication job can be used to process one or several VMs. You can instruct Veeam Backup & Replication to run jobs automatically by schedule or start them manually.

Limitations for Replication

Replication has the following limitations:

- Due to VMware vSphere limitations, if you change the size of VM disks on the source VM, Veeam Backup & Replication deletes all available restore points (represented as VM snapshots) on the VM replica during the next replication job session. For more information, see https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004047.
- If you assign the role of a backup proxy to a VM, you should not add this VM to the list of processed VMs in a job that uses this backup proxy. Such configuration may result in degraded job performance. Veeam Backup & Replication will assign this backup proxy to process other VMs in the job first, and processing of this VM itself will be put on hold. Veeam Backup & Replication will report the following message in the job statistics: *VM is a backup proxy, waiting for it to stop processing tasks*. The job will start processing this VM only after the backup proxy deployed on the VM finishes its tasks.
- If you use tags to categorize virtual infrastructure objects, check limitations for VM tags. For more information, see [VM Tags](#).
- Due to Microsoft limitations, you cannot use Microsoft Azure Active Directory credentials to perform application-aware processing on VMs running Microsoft Windows 10.

How Replication Works

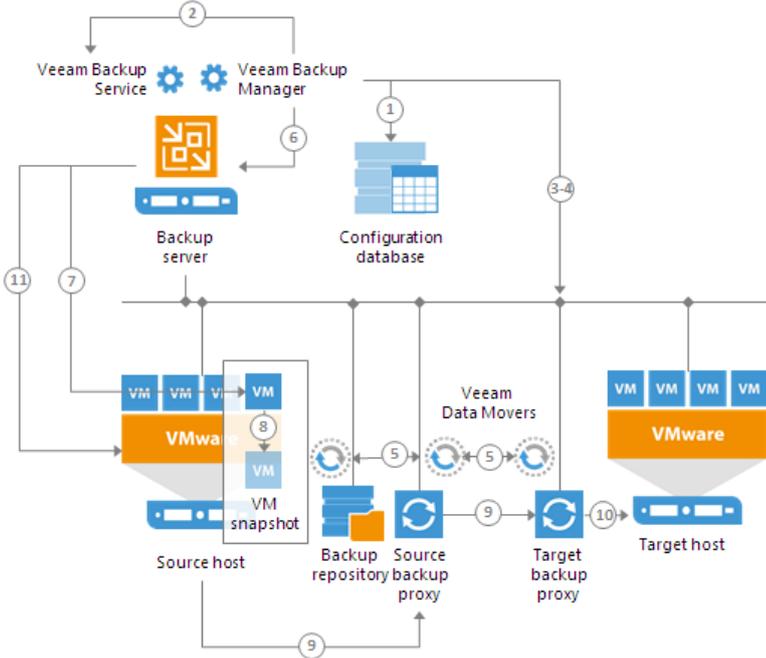
Veeam Backup & Replication performs VM replication in the following way:

1. When a new replication job session starts, Veeam Backup & Replication starts the Veeam Backup Manager process on the backup server. Veeam Backup Manager reads job settings from the configuration database and creates a list of VM tasks to process. For every disk of VMs added to the job, Veeam Backup & Replication creates a new task.
2. Veeam Backup Manager connects to the Veeam Backup Service. The Veeam Backup Service includes a resource scheduling component that manages all tasks and resources in the backup infrastructure. The resource scheduler checks what backup infrastructure resources are available, and assigns backup proxies and backup repositories to process job tasks.
3. Veeam Backup Manager connects to Veeam Transport Services on source and target backup proxies and on the backup repository. The Veeam Transport Services, in their turn, start Veeam Data Movers. A new instance of Veeam Data Mover is started for every task that the backup proxy is processing.
4. Veeam Backup Manager establishes a connection with Veeam Data Movers on backup proxies and the backup repository, and sets a number of rules for data transfer, such as network traffic throttling rules and so on.
5. The source Veeam Data Mover establishes a connection with the target Veeam Data Mover, and Veeam Data Mover on the backup repository.
6. Veeam Backup Manager queries information about VMs and virtualization hosts from the Veeam Broker Service.
7. If application-aware image processing is enabled for the job, Veeam Backup & Replication connects to VM guest OSes, deploys runtime processes on VM guest OSes and performs in-guest processing tasks.
8. Veeam Backup & Replication requests vCenter Server or ESXi host to create a VM snapshot. VM disks are put to the read-only state, and every virtual disk receives a delta file. All changes that the user makes to the VM during replication are written to delta files.
9. The source Veeam Data Mover reads the VM data from the read-only VM disk and copies it. During incremental job sessions, the source Veeam Data Mover uses CBT to retrieve only those data blocks that have changed since the previous job session. If CBT is not available, the source Veeam Data Mover interacts with the Veeam Data Mover on the backup repository to obtain replica metadata, and uses this metadata to detect blocks that have changed since the previous job session.

While copying VM data, the source Veeam Data Mover performs additional processing. It filters out zero data blocks, blocks of swap files and blocks of excluded VM guest OS files. The source Veeam Data Mover compresses VM data and transports it to the target Veeam Data Mover.

10. The target Veeam Data Mover decompresses VM data and writes the result to the destination datastore.

11. After the backup proxy finishes reading VM data, Veeam Backup & Replication requests the vCenter Server or ESXi host to commit the VM snapshot.



Replication Architecture

Veeam Backup & Replication uses the following components for the replication process:

- [Backup server](#)
- [Source host and target host with associated datastores](#)
- [One or two backup proxies hosting Veeam Data Movers](#)
- [Backup repository](#)
- [Optional] [WAN accelerators](#)

All backup infrastructure components engaged in the job make up a data pipe. The source and target hosts produce two terminal points for the data flow. Veeam Backup & Replication processes VM data in multiple cycles, moving VM data over the data pipe block by block.

Backup Server

The backup server is the configuration, administration and management core of the backup infrastructure. During the replication process, the backup server coordinates replication tasks, controls resource allocation and replica job scheduling.

Source and Target Hosts

The source host and the target host produce two terminal points between which replicated VM data is moved. The role of a target host can be assigned to a single ESX(i) host or ESX(i) cluster. Assigning a cluster as a target ensures uninterrupted replication in case one of the cluster hosts fails.

Backup Proxies

To collect, transform and transport VM data during the VM replication process, Veeam Backup & Replication uses Veeam Data Movers. Veeam Data Movers communicate with each other and maintain a stable connection.

For every replication job, Veeam Backup & Replication requires three Veeam Data Movers:

- Source Veeam Data Mover hosted on the source backup proxy
- Target Veeam Data Mover hosted on the target backup proxy
- Veeam Data Mover hosted on the backup repository

During replication, the source Veeam Data Mover interacts with the source host and the target Veeam Data Mover interacts with the target host. The Veeam Data Mover hosted on the backup repository works with replica metadata files.

To streamline the replication process, you can deploy a backup proxy on a VM. The virtual backup proxy must be registered on an ESX(i) host that has a direct connection to the target datastore. In this case, the backup proxy will be able to use the Virtual appliance transport mode for writing replica data to target.

During the first run of a replication job, Veeam Backup & Replication creates a replica with empty virtual disks on the target datastore. If the Virtual appliance mode can be used, replica virtual disks are mounted to the backup proxy and populated through the ESX host I/O stack. This results in increased writing speed and fail-safe replication to ESX targets. For more information, see [Transport Modes](#).

If the backup proxy is deployed on a physical machine or the Virtual appliance mode cannot be used for other reasons, Veeam Backup & Replication uses the Network transport mode to populate replica disk files.

Backup Repository

The backup repository stores replica metadata. The backup repository must be deployed in the source site, as close to the source host as possible. When you perform incremental replication, the source Veeam Data Mover communicates with the Veeam Data Mover Service on the backup repository to obtain replica metadata and quickly detect changed blocks of data between 2 replica states.

WAN Accelerators

WAN accelerators are optional components in the backup infrastructure. You can use WAN accelerators if you replicate VMs over a slow connection or over WAN.

In the replication process, WAN accelerators are responsible for global data caching and deduplication. To use WAN acceleration, you must deploy 2 WAN accelerators in the following way:

- The source WAN accelerator must be deployed in the source side, close to the backup proxy running the source Veeam Data Mover.
- The target WAN accelerator must be deployed in the target side, close to the backup proxy running the target Veeam Data Mover.

Replication Scenarios

Veeam Backup & Replication supports a number of replication scenarios that depend on the location of the target host and the data transport path.

- [Onsite replication](#)
- [Offsite replication](#)

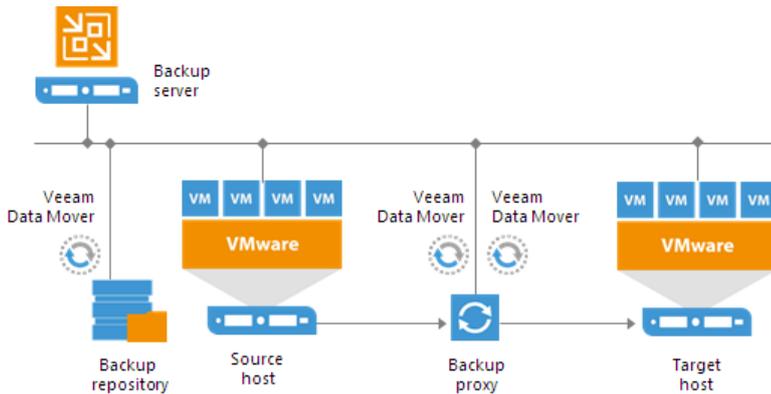
Onsite Replication

If the source host and target host are located in the same site, you can perform onsite replication.

Onsite replication requires the following replication infrastructure components:

- Source and target hosts
- Backup proxy. In the onsite replication scenario, the source Veeam Data Mover and target Veeam Data Mover are started on the same backup proxy. The backup proxy must have access to the backup server, source host, target host and backup repository holding replica metadata.
- Backup repository for storing replica metadata.

In the onsite replication scenario, Veeam Backup & Replication does not perform data compression. Replication traffic is transferred decompressed between the two Veeam Data Mover started on the same backup proxy.



Offsite Replication

If the source host is located in the primary site, and the target host is located in the DR site, you can perform offsite replication.

Offsite replication can run over two data paths:

- Direct data path
- Via a pair of WAN accelerators

NOTE:

When planning for offsite replication, consider advanced possibilities to reduce the amount of replication traffic and streamline replica configuration: [replica seeding](#), [replica mapping](#), [network mapping](#) and [Re-IP](#).

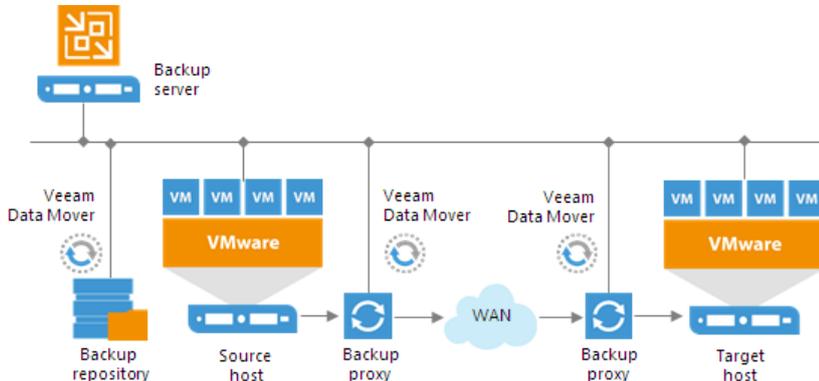
Replication Over Direct Data Path

The common requirement for offsite replication is that one Veeam Data Mover runs in the production site, closer to the source host, and the other Veeam Data Mover runs in the remote DR site, closer to the target host. During backup, the Veeam Data Movers maintain a stable connection, which allows for uninterrupted operation over WAN or slow links.

Offsite replication over a direct path requires the following backup infrastructure components:

- Source and target hosts
- At least one backup proxy in the source site. The backup proxy must have access to the backup server, source host, backup proxy in the target site and backup repository holding replica metadata.
- At least one backup proxy in the target site. The backup proxy must have access to the backup server, target host and backup proxy in the source site.
- Backup repository for storing replica metadata. The backup repository must be located in the source site, closer to the backup proxy, and must have access to it.

In the offsite replication scenario, Veeam Backup & Replication uses data compression. The Veeam Data Mover on the source backup proxy compresses VM data blocks and sends them to the target backup proxy in the compressed format. The Veeam Data Mover on the target backup proxy decompresses VM data and stores it to a datastore in a native VMware vSphere format.



Replication via WAN Accelerators

If you have a weak WAN link, you can replicate VM data over a pair of WAN accelerators. WAN accelerators provide advanced technologies to optimize VM data transfer:

- Global data caching and deduplication
- Resume on disconnect for uninterrupted data transfer

WAN accelerators add a new layer in the backup infrastructure – a layer between the source Veeam Data Mover and target Veeam Data Mover. The data flow goes from the source backup proxy over a pair of WAN accelerators to the target backup proxy that, finally, destines VM data to the target host.

Offsite replication over WAN accelerators requires the following backup infrastructure components:

- Source and target hosts
- A pair of WAN accelerators at each end of the WAN link:
 - Source WAN accelerator in the source site. The source WAN accelerator must have access to the backup server, source backup proxy and target WAN accelerator.
 - Target WAN accelerator in the target site. The target WAN accelerator must have access to the backup server, source WAN accelerator and target backup proxy.
- At least one backup proxy in the source site. The backup proxy must have access to the backup server, source host, source WAN accelerator and backup repository holding replica metadata.
- At least one backup proxy in the target site. The backup proxy must have access to the backup server, target host and target WAN accelerator.
- Backup repository for storing replica metadata. The backup repository must be located in the source site, closer to the backup proxy, and must have access to it.

In the offsite replication scenario via WAN accelerators, Veeam Backup & Replication compresses VM data. VM data blocks are compressed on the source WAN accelerator, transported to the target site in the compressed format and decompressed on the target WAN accelerator.

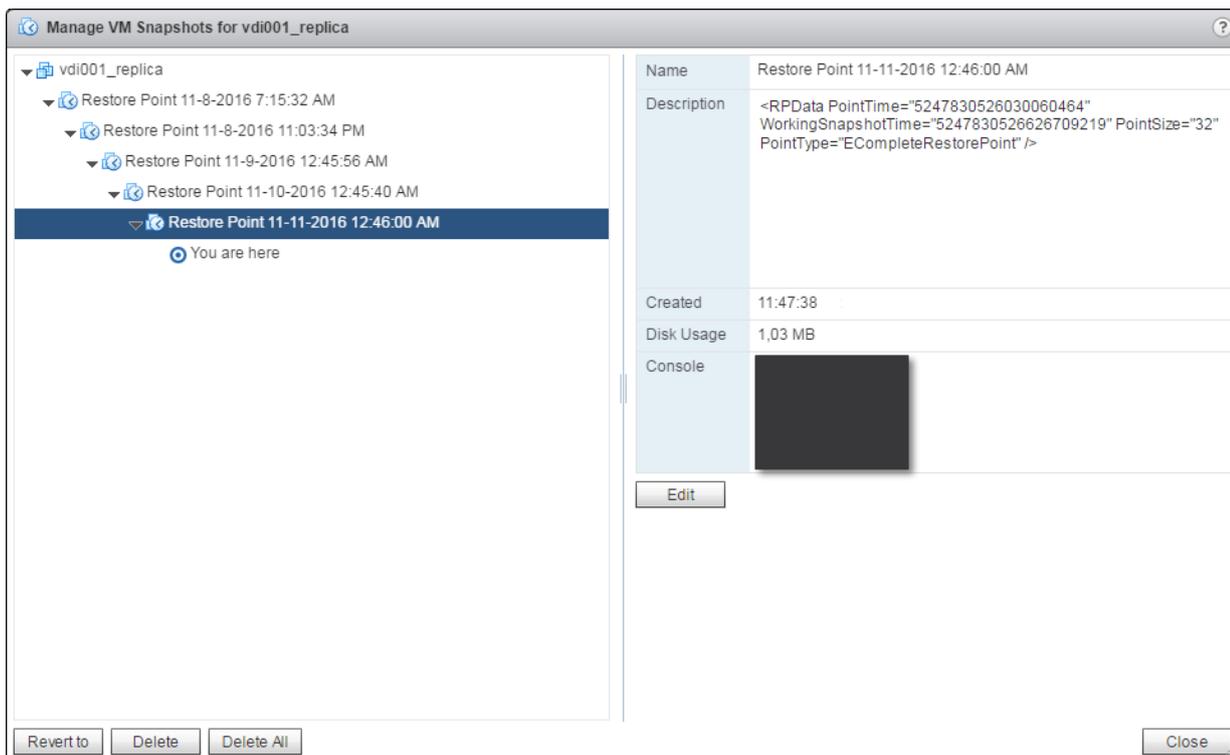
Replication Chain

For every VM replica, Veeam Backup & Replication creates and maintains a number of restore points. If the original VM fails for any reason, you can temporary or permanently fail over to a VM replica and restore critical services with minimum downtime. If you cannot fail over to the latest VM replica state (for example, in case corrupted data was replicated from source to target), you can select a previous restore point and fail over to it.

Veeam Backup & Replication utilizes VMware ESX snapshot capabilities to create and manage replica restore points. During the first replication job session, Veeam Backup & Replication creates a copy of the source VM on the target host. During every subsequent replication job session, it adds a new snapshot to the snapshot chain for the VM replica. Blocks of data that have changed since the last job run are written to the snapshot delta file, and the snapshot delta file acts as a restore point.

VM replica restore points are stored in a native VMware vSphere format next to replica virtual disk files, which allows Veeam Backup & Replication to accelerate failover operations. To fail over to the necessary point of the VM replica, Veeam Backup & Replication does not need to apply rollback files. Instead, it uses a native VMware vSphere mechanism of reverting to a snapshot.

You can specify retention policy settings for replication jobs – define how many retention points you want to keep for every VM replica. Veeam Backup & Replication will keep only the specified number of points and remove outdated snapshots.



Changed Block Tracking

To perform incremental replication, Veeam Backup & Replication needs to know what data blocks have changed since the previous job session. For this purpose, it uses [Changed Block Tracking](#).

Advanced Replication Technologies

To minimize the workload on the production infrastructure and reduce data traffic, you can use the following advanced replication technologies:

- [Remote replica from backup](#) can help you minimize use of compute, storage and network resources of the production infrastructure.
- [Replica seeding](#) and [replica mapping](#) can help you minimize the amount of traffic going to the DR site over WAN or slow links.

Remote Replica from Backup

Disaster recovery plans often require that you back up and replicate the same VM for DR and HA purposes. Normally, this doubles the workload on the virtual infrastructure. You need to create two VM snapshots, independently from one another, and transfer VM data from the production site twice.

You can reduce the workload on the production environment by using the remote replica from backup option. This option can be used for onsite and offsite replication scenarios.

When you perform remote replication from backup, Veeam Backup & Replication does not address hosts and storage in the production environment to read VM data. As a source of data, it uses a backup chain that already exists on the backup repository. As a result, you do not need to create a VM snapshot for replication and transport the same data twice. You retrieve VM data only during the backup job. The replication job re-uses retrieved data to build VM replica restore points.

Although replica from backup might resemble replica seeding, there is difference between these options:

- Replica seeding uses the backup file only during the first run of a replication job. To further build VM replica restore points, the replication job addresses the production environment and reads VM data from the source storage.
- Remote replica from backup uses a backup chain on the backup repository as the only source of data. When building a new VM replica restore point, Veeam Backup & Replication always reads data from the latest restore point in the backup chain, either full or incremental. The backup chain on the backup repository may be created with a backup job or a backup copy job.

Limitations for Remote Replica from Backup

- You cannot perform remote replication from vCloud Director backups.
- A backup that you plan to use for remote replication must be mapped to a backup job on the backup server where you configure the replication job.

If you want to use a backup created on another backup server, perform the following steps:

- a. Import the backup to the Veeam Backup & Replication console.
- b. Create a new backup job and map the imported backup to it.
- c. Create a replication job, enable the **Get seed from the following backup repository** option and point to the backup repository where the imported backup resides.

Mind the following:

- The backup job to which you map the imported backup file on another backup server must run periodically and produce new restore points. You cannot create a job, map the imported backup to it and never run this job.

- No other job on any other backup server must use the imported backup.

How Remote Replica from Backup Works

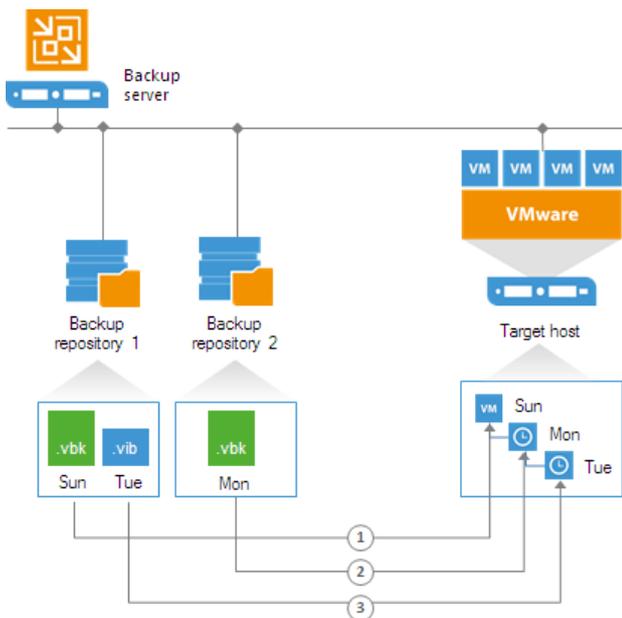
Remote replica from backup is performed with a regular replication job. When you set up a replication job, you define a backup repository with VM backups as a source of data. If the backups for this VM are available in different backup repositories, you can select several backup repositories as a source. In this case, Veeam Backup & Replication will look for the latest VM restore point across these backup repositories.

For example, you have configured two backup jobs that process the same VM, and targeted these jobs at two different backup repositories. The backup jobs have created the following backup files:

- *Backup job 1* has created 2 restore points in *Backup repository 1*: full backup file on Sunday and incremental backup file on Tuesday.
- *Backup Job 2* has created 1 restore point in *Backup repository 2*: full backup file on Monday.

The replication job is configured to retrieve VM data from backups and scheduled to run daily. In this case, the replication job will retrieve VM data from backups in the following way:

1. On Sunday, the replication job will retrieve VM data from the full backup file in *Backup repository 1*.
2. On Monday, the replication job will retrieve VM data from the full backup file in *Backup repository 2*.
3. On Tuesday, the replication job will retrieve VM data from the incremental backup file in *Backup repository 1*.



In some situations, a new restore point on the backup repository may not be created by the time a replication job starts. In this case, Veeam Backup & Replication displays a warning notifying that the latest restore point has already been replicated. The replication job session finishes with the *Warning* status.

NOTE:

When you replicate a VM over a production network, Veeam Backup & Replication retrieves VM data as of the latest VM state. When you replicate a VM from backup, Veeam Backup & Replication retrieves VM data as of the point in time when the backup was created. The VM replica restore point has the same timestamp as a corresponding VM backup restore point, not the time when the replica job session is run.

Replica Seeding

If you replicate a VM to a remote DR site, you can use replica seeding. Replica seeding helps significantly minimize the amount of traffic going from the production site to the DR site over WAN or slow LAN links.

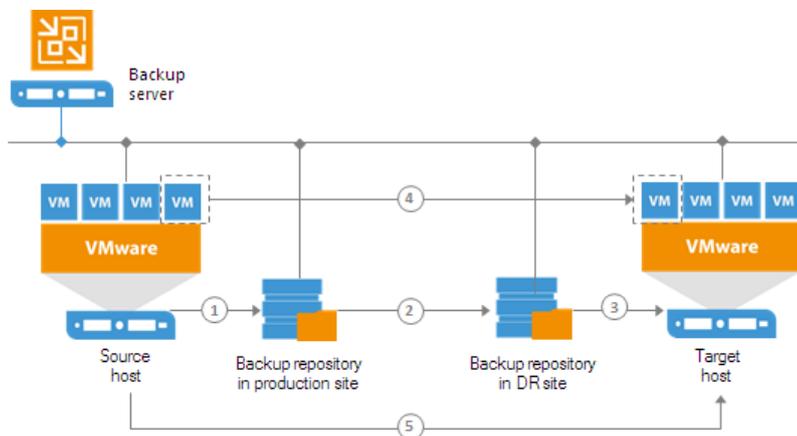
With replica seeding, you do not have to transfer all of VM data from the source host to the target host across the sites when you perform initial replication. Instead, you can use a VM backup created with Veeam Backup & Replication as a replica "seed". When the replication job starts, Veeam Backup & Replication will use the seed to build a VM replica.

Replica seeding includes the following steps:

1. As a preparatory step for replica seeding, you need to create a backup of a VM that you plan to replicate.
2. The created backup should then be copied from the backup repository in the production site to the backup repository in the DR site. After the backup is copied to the backup repository in the DR site, you will need to perform rescan of this repository as described in the [Managing Backup Repositories](#) section.
3. When you create a replication job, you should point it to the backup repository in the DR site. During the first run of a replication job, Veeam Backup & Replication accesses the backup repository where the replica seed is located, and restores the VM from the backup. The restored VM is registered on the replication target host in the DR site. Files of the restored VM are placed to the location you specify as the replica destination datastore.

Virtual disks of a replica restored from the backup preserve their format (that is, if the original VM used thin provisioned disks, virtual disks of the VM replica are restored as thin provisioned).

4. Next, Veeam Backup & Replication synchronizes the restored VM with the latest state of the original VM. After successful synchronization, in the **Home** view of Veeam Backup & Replication, under **Replicas** node you will see a VM replica with two restore points. One point will contain the state of the VM from the backup file; the other point will contain the latest state of the original VM you want to replicate.
5. During all subsequent runs of the replication job, Veeam Backup & Replication transfers only incremental changes in a regular manner.



Replica seeding dramatically reduces traffic sent over WAN or slow connections because

Veeam Backup & Replication does not send the full contents of the VM image. Instead, it transmits only differential data blocks.

TIP:

If you add new VMs to an already existing replication job, you can enable replica seeding settings for these VMs. In this case, the newly added VMs will be seeded from the selected backups at the next pass of the replication job. VMs that have already been processed by the job by the time you add new VMs will be processed in a regular manner.

Replica Mapping

If a replica for the VM that you plan to replicate already exists in the DR site, you can map the original VM in the production site to this VM. For example, you can map the original VM to a VM replica created with another replication job or restore a VM from the backup on the target host in the DR site and map the original VM to it. You can also use replica mapping if you need to reconfigure or recreate replication jobs, for example, split one replication job into several jobs.

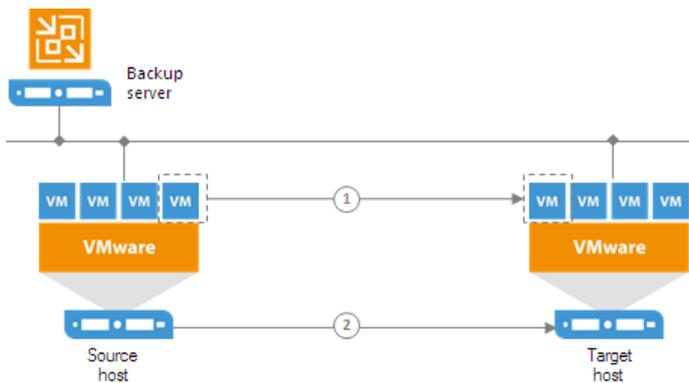
Replication to a mapped VM is performed in the following way:

1. During the first run, the replication job calculates the differences between the original and mapped VM. Instead of copying and transferring all data of the original VM, the replication job transfers only incremental changes to synchronize the state of the mapped VM with the state of the original VM.

After successful synchronization, in the **Home** view of Veeam Backup & Replication, under **Replicas** node you will see a VM replica with 2 restore points:

- One restore point will contain the latest state of the mapped VM.
- The other restore point will contain the latest state of the original VM on the source host.

2. All subsequent runs of the replication job will be performed in a regular manner: Veeam Backup & Replication will transfer only incremental changes to the target host.



NOTE:

If a VM replica to which the original VM is mapped has any snapshots, these snapshots will be removed during the run of the replication job.

Network Mapping and Re-IP

If you use different network and IP schemes in production and DR sites, in the common case you would need to change the network configuration of a VM replica before you fail over to it. To eliminate the need for manual replica reconfiguration and ensure minimum failover downtime, Veeam Backup & Replication offers possibilities of network mapping and automatic IP address transformation.

Network Mapping

By default, a replicated VM uses the same network configuration as the original VM. If the network in the DR site does not match the production network, you can create a network mapping table for the replication job. The table maps source networks to target networks.

During every job run, Veeam Backup & Replication checks the network configuration of the original VM against the mapping table. If the original VM network matches a source network in the table, Veeam Backup & Replication updates the replica configuration file to replace the source network with the target one. Thus, network settings of a VM replica are always kept up to date with the DR site requirements. In case you choose to fail over to the VM replica, it will be connected to the correct network.

Re-IP Rules

For Microsoft VMs, Veeam Backup & Replication also automates reconfiguration of VM IP addresses. If the IP addressing scheme in the production site differs from the DR site scheme, you can create a number of Re-IP rules for the replication job.

When you fail over to the replica, Veeam Backup & Replication checks if any of the specified Re-IP rules apply to the replica. If a rule applies, Veeam Backup & Replication mounts VM disks of the replica to the backup server and changes its IP address configuration via the Microsoft Windows registry. The whole operation takes less than a second. If failover is undone for any reason or if you fail back to the original location, replica IP address is changed back to the pre-failover state.

IMPORTANT!

- Replica Re-IP works only if you perform replica failover using Veeam Backup & Replication. If you power on a VM replica in some other way, for example, manually using vSphere Client, Re-IP rules will not be applied to it.
- The backup server OS must support mounting of the system disk of processed machine.

Creating Replication Jobs

To create VM replicas, you must configure a replication job. The replication job defines how, where and when to replicate VM data. One job can be used to process one VM or more VMs.

You can configure a job and start it immediately or save the job to start it later. Jobs can be started manually or scheduled to run automatically at specific time.

Before creating a replication job, [check prerequisites](#). Then use the **New Replication Job** wizard to configure a replication job.

Before You Begin

Before you create a replication job, check the following prerequisites:

- Backup infrastructure components that will take part in the replication process must be added to the backup infrastructure and properly configured. These include source and target ESX(i) hosts, one backup proxy for onsite replication scenario or two backup proxies for offsite replication scenario and backup repository for storing replica metadata.

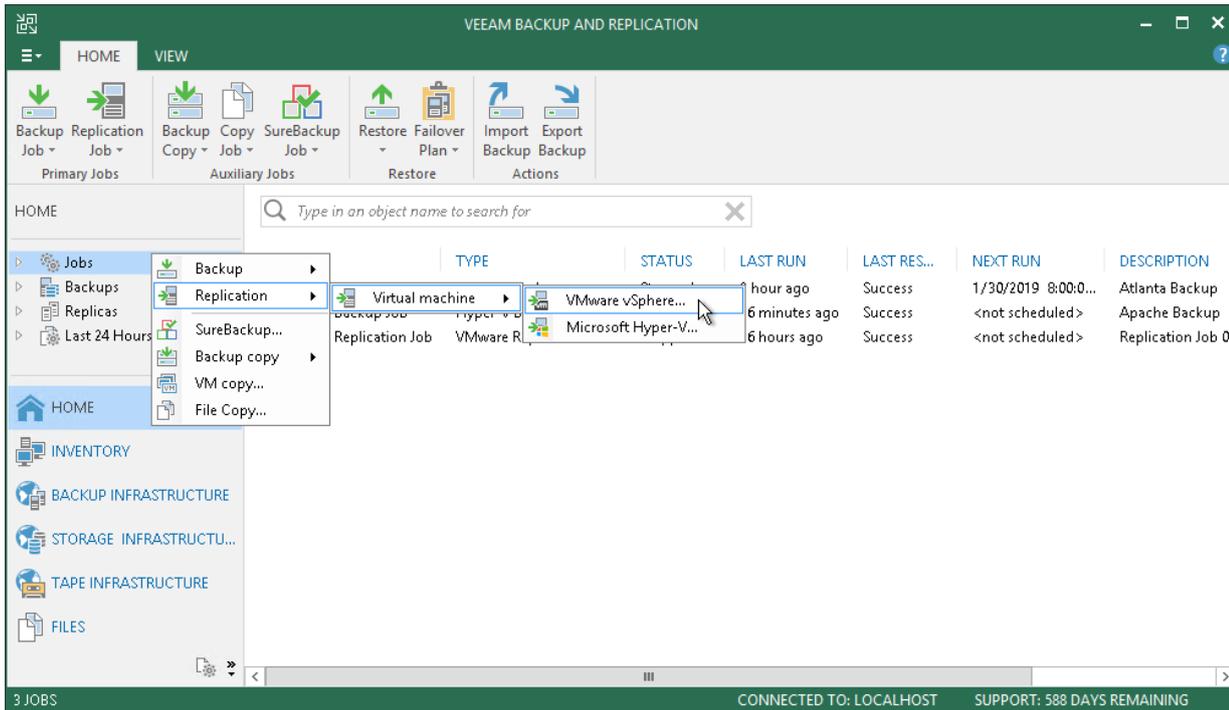
The backup server must be able to resolve short names and connect to source and target virtualization hosts.
- The target datastore must have enough free space to store disks of replicated VMs. To receive alerts about low space on the target datastore, configure global notification settings. For more information, see [Specifying Other Notification Settings](#).
- If you plan to replicate VMs via WAN accelerators, source and target WAN accelerators must be added to the backup infrastructure and properly configured. For more information, see [Adding WAN Accelerators](#).
- If you plan to replicate VMs via WAN accelerators, it is recommended that you pre-populate global cache on the target WAN accelerator before you start the replication job. Global cache population helps reduce the amount of traffic transferred over WAN. For more information, see [Populating Global Cache](#).
- If you plan to replicate VMs from the backup, the backup job that you plan to use as the source must be configured beforehand. For more information, see [Remote Replica from Backup](#).
- If you plan to use pre-job and post-job scripts and/or pre-freeze and post-thaw scripts, you must create scripts before you configure the replication job. Veeam Backup & Replication supports script files in the following formats: EXE, BAT, CMD, JS, VBS, WSF, PS1, SH.
- You must check limitations for replication. For more information, see [About Replication](#).

Step 1. Launch New Replication Job Wizard

To run the **New Replication Job** wizard, do one of the following:

- On the **Home** tab, click **Replication Job > Virtual machine > VMware vSphere**.
- Open the **Home** view, in the inventory pane right-click **Jobs** and select **Replication > Virtual machine > VMware vSphere**.
- Open the **Inventory** view. In the working area, select the VMs, click **Add to Replication** on the ribbon and select **New job** or right-click the VMs and select **Add to replication job > New job**. In this case, the VMs will be automatically added to the replication job. You can add other VMs to the job when passing through the wizard steps.

- You can quickly include the VMs to already existing jobs. To do this, open the **Inventory** view. In the working area, select the VMs and click **Add to Replication** > *name of the job* on the ribbon or right-click VMs and select **Add to replication job** > *name of the job*.



Step 2. Specify Job Name and Description

At the **Name** step of the wizard, specify the job name and description and define advanced settings of for the replication job.

- In the **Name** field, enter a name for the replication job.
- 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.
- If you plan to replicate VMs to a DR site, you can use a number of advanced settings for the job:
 - Select the **Low connection bandwidth** check box to enable the **Seeding step** in the wizard. Replica seeding can be used if you plan to replicate VMs to a remote site and want to reduce the amount of traffic sent over the network during the first run of the replication job.
 - Select the **Separate virtual networks** check box to enable the **Network step** in the wizard. If the network in the DR site does not match the production network, you can resolve this mismatch by creating a network mapping table.

- Select the **Different IP addressing scheme** check box to enable the [Re-IP step](#) in the wizard. Re-IP possibilities can be used to automate reconfiguration of replica IP addresses for Microsoft Windows VMs if IP schemes in the DR and production sites do not match.

Step 3. Select VMs to Replicate

At the **Virtual Machines** step of the wizard, select VMs and VM containers that you want to replicate.

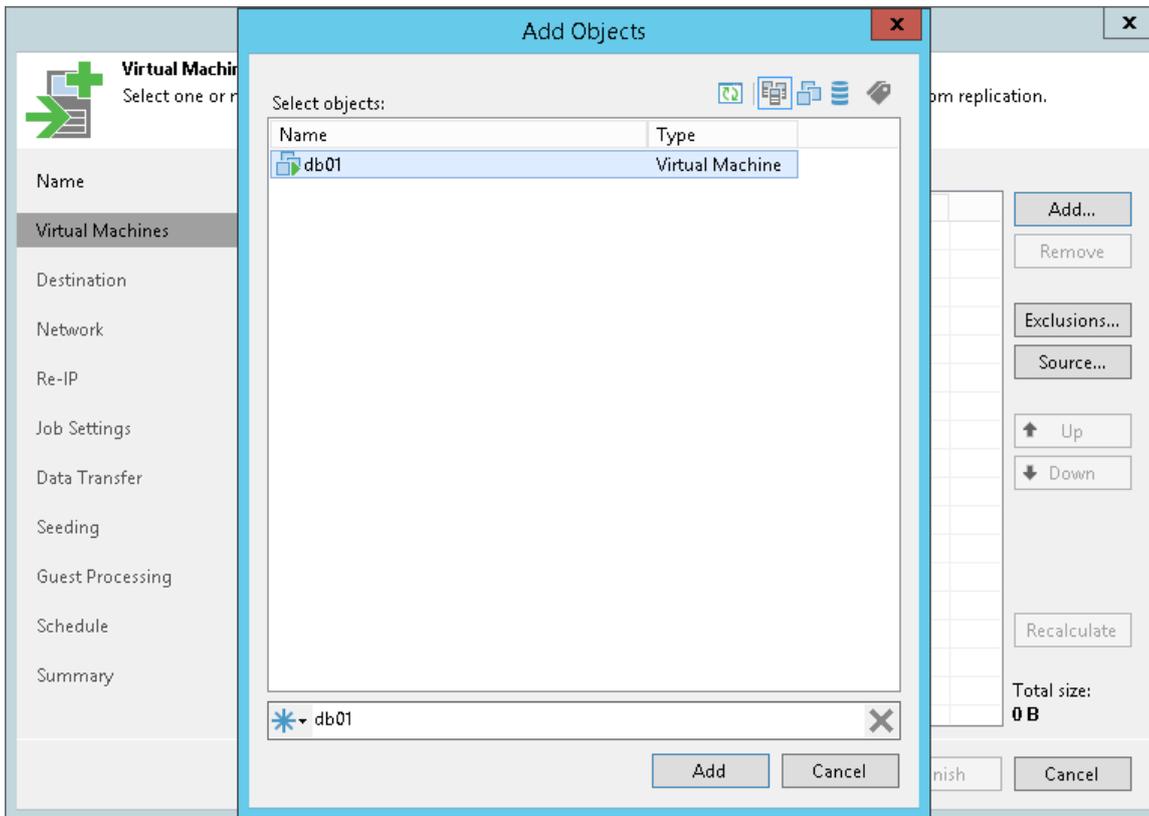
Jobs with VM containers are dynamic in their nature. If a new VM is added to the container in the virtual infrastructure after the replication job is created, Veeam Backup & Replication will automatically update the job settings to include the added VM.

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 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]**.

The initial size of VMs and VM containers added to the replication job is displayed in the **Size** column in the list. The total size of objects is displayed in the **Total size** field. Use the **Recalculate** button to refresh the total size value after you add a new object to the job.

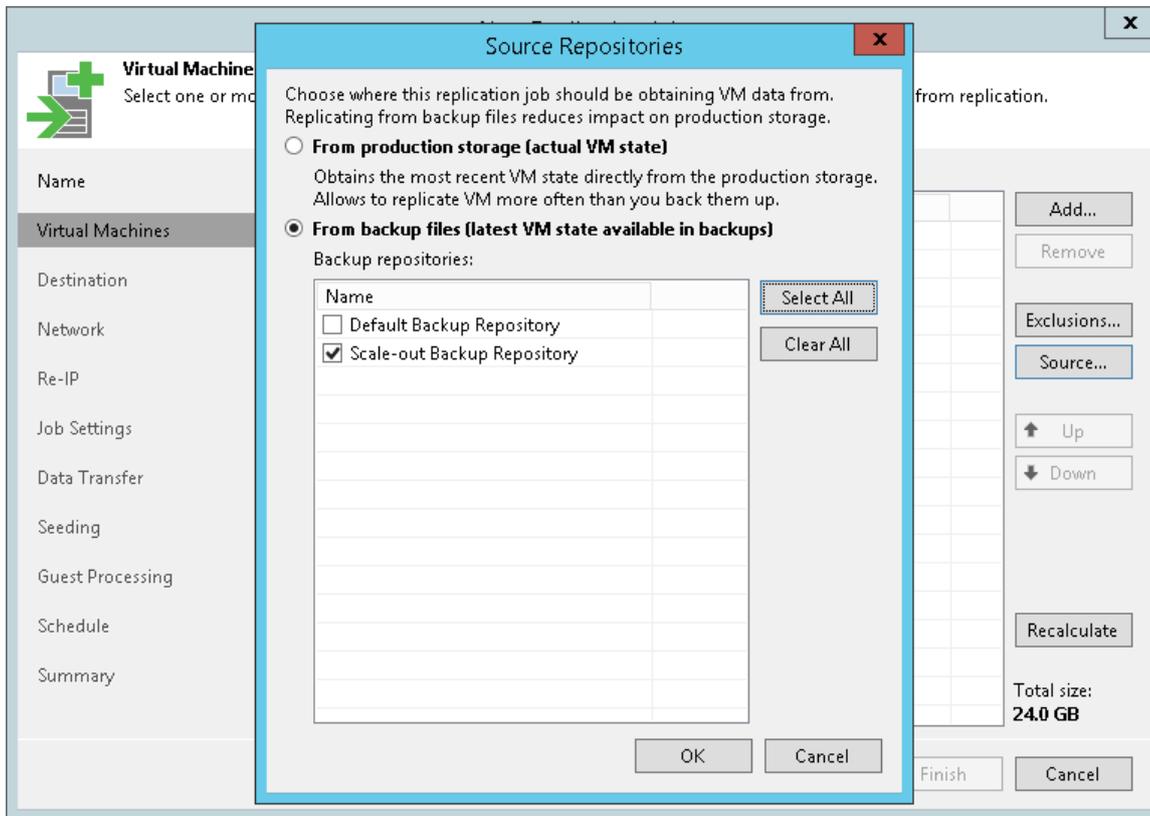


Step 4. Specify Data Source

You can select a data source from which VM data must be read.

1. At the **Virtual Machines** step of the wizard, click **Source** on the right of the VMs list.
2. In the displayed window, select one of the following options:
 - o **From production storage.** In this case, Veeam Backup & Replication will retrieve VM data from datastores connected to the source ESX(i) host.

- **From backup files.** In this case, Veeam Backup & Replication will read VM data from the backup chain already existing on the backup repository. This option can be used in the replica from backup scenario. For more information, see [Remote Replica from Backup](#).



Step 5. Exclude Objects from Replication Job

After you have added VMs and VM containers to the job, you can specify which objects you want to exclude from replicas. You can exclude the following types of objects:

- [VMs from VM containers](#)
- [Specific VM disks](#)

NOTE:

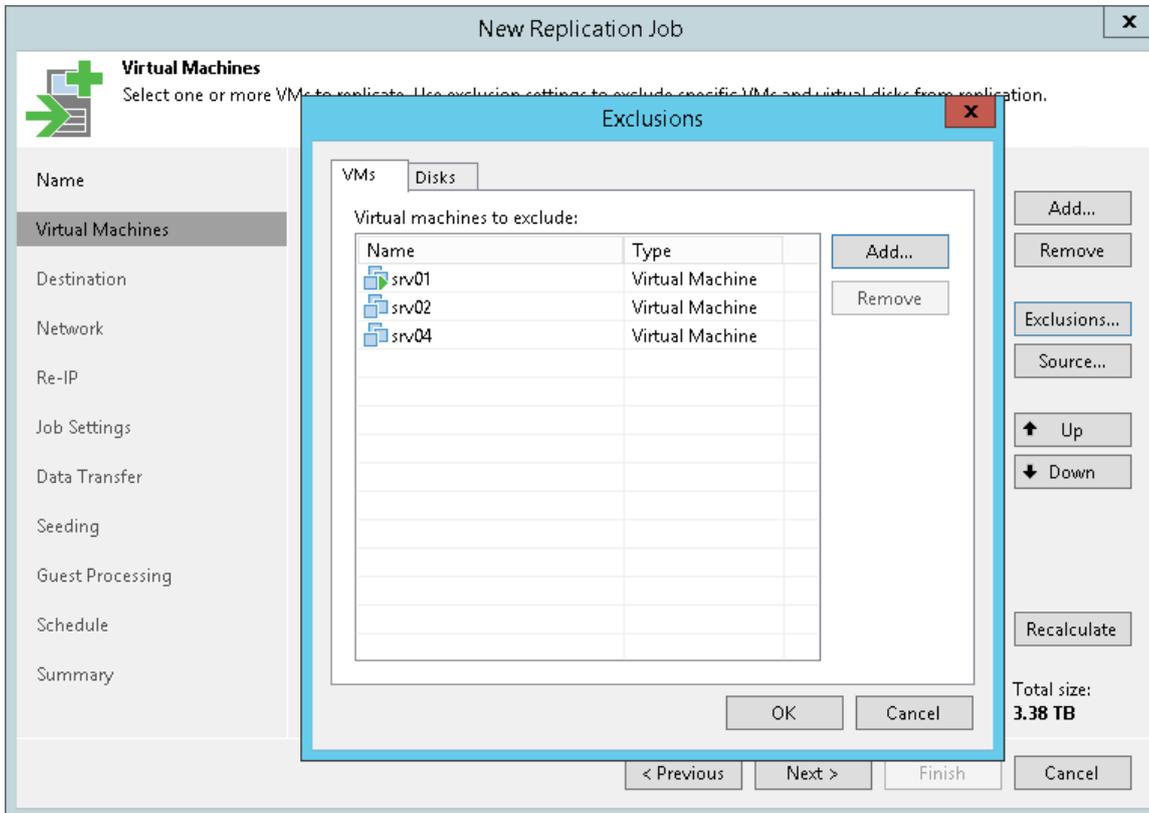
To make the replication process faster and reduce the size of created replicas, Veeam Backup & Replication automatically excludes the following objects from replication:

- VM log files
- VM templates from VM containers

To exclude VMs from a VM container:

1. At the **Virtual Machines** step of the wizard, click **Exclusions**.
2. Click the **VMs** tab.
3. Click **Add**.
4. 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.

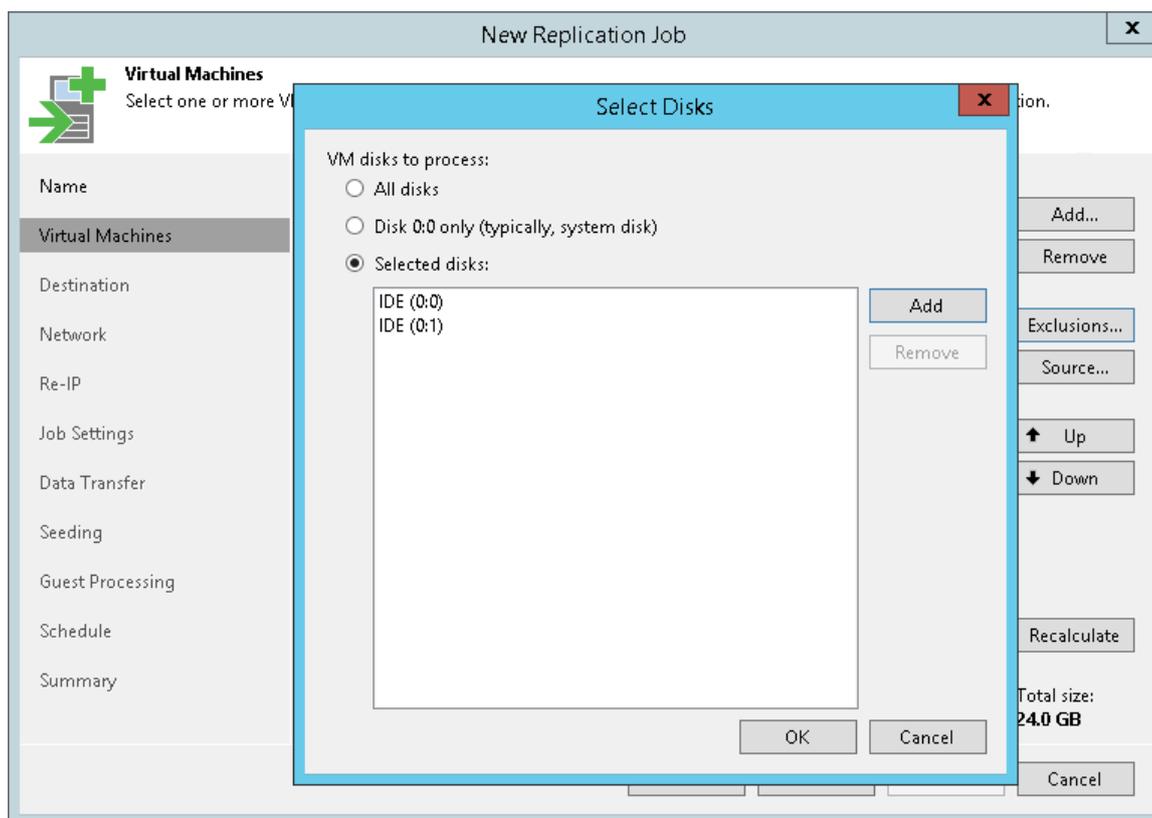
5. Select the object and click **Add**. Use the **Show full hierarchy** check box to display the hierarchy of all VMware Servers added to Veeam Backup & Replication.
6. Click **OK**.



To exclude VM disks:

1. At the **Virtual Machines** step of the wizard, click **Exclusions**.
2. Click the **Disks** tab.
3. Select the VM in the list and click **Edit**. If you want to exclude disks of a VM added as a part of the container, click **Add** to include the VM in the list as a standalone object.

4. Choose disks that you want to replicate. You can choose to process all disks, 0:0 disks (typically, system disks) or add to the list custom IDE, SCSI or SATA disks.



Step 6. Define VM Replication Order

You can define the order in which the replication job must process VMs. Setting VM order can be helpful, for example, if you have added some mission-critical VMs to the job and want the job to process them first. You can set these VMs first in list to ensure that their processing fits the backup window.

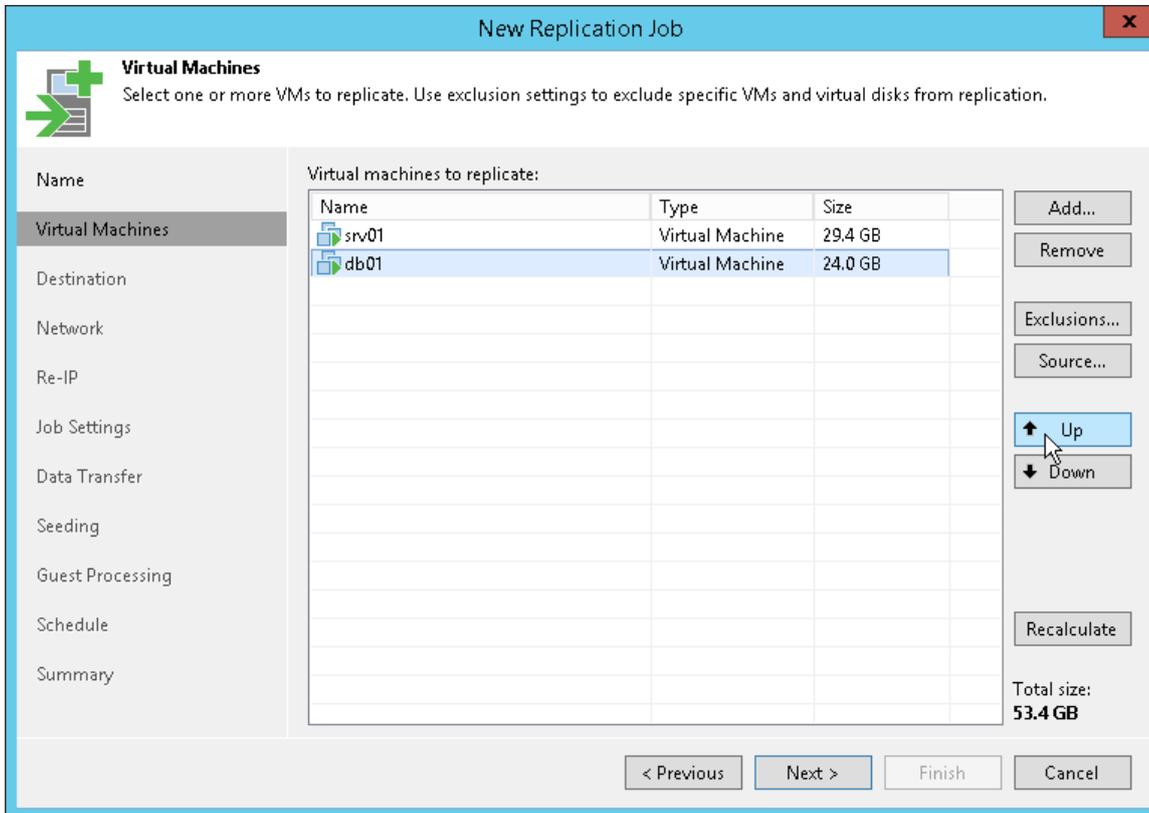
VMs inside a VM container are processed at random. To ensure that VMs are processed in the defined order, you must add them as standalone VMs, not as a part of the VM container.

To define VM replication order:

1. At the **Virtual Machines** step of the wizard, select a VM or VM container.
2. Use the **Up** and **Down** buttons on the right to move the VM or VM container up or down in the list.

NOTE:

VMs may be processed in a different order. For example, if backup infrastructure resources for a VM that is higher on the priority list are not available, and resources for a VM that is lower on the list are available, Veeam Backup & Replication will start processing the VM that is lower on the list first.



Step 7. Specify Replica Destination

At the **Destination** step of the wizard, select a destination for the VM replicas.

1. Click **Choose** next to the **Host or cluster** field and select an ESX(i) host or cluster where VM replicas must be registered.

If an ESX(i) host is a part of a cluster or is managed by a vCenter Server, it is recommended that you select a cluster or a server rather than a standalone host. This way, the replication process will be more sustainable and accurate. The replication job will be performed until there is at least one available host in the cluster.

2. If all or majority of VM replicas 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 VM replicas to different resource pools:

- a. Click the **Pick resource pool for selected replicas** link.
- b. In the **Choose Resource Pool** window, click **Add VM** on the right and select the VMs and click **Add**.
- c. Select the added VM in the **Replica VM resource pool** list and click **Resource Pool** at the bottom of the window.
- d. From the list of available resource pools, choose the target resource pool for the VM.

3. If all or majority of VM replicas must be placed in the same folder, click **Choose** next to the **VM folder** field and choose the target folder.

If you want to place VM replicas to different folders:

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

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

4. If files for all or majority of VM replicas must be stored on the same datastore, click **Choose** next to the **Datastore** field and select the target datastore. Veeam Backup & Replication displays only those datastores that are accessible by the selected replication target. If you have chosen to replicate VMs to a cluster, Veeam Backup & Replication will display only shared datastores.

If you want to place VM replicas 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 VMs 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 replica configuration files and disk files in different locations.

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

NOTE:

After the first run of the replication job, you can change the target location for replicated files. However, the target will be changed only for new files that were created on the source VM after the first run. The target for old files will not be changed.

5. By default, Veeam Backup & Replication saves disks of a VM replica in the thin format. If necessary, you can configure the job to change the disk format. For example, if the original VM uses thick disks, you can change the format of replica disks to thin provisioned and save on disk space required to store VM replica data.

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

To change replica 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 VMs whose disk format you want to change and click **Add**.
- c. Select the added VM 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 replica disk files: same as source, thin, thick lazy zeroed or thick eager zeroed. For more information about disk types, see <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.html.hostclient.doc/GUID-4COF4D73-82F2-4B81-8AA7-1DD752A8A5AC.html>.

TIP:

When selecting the necessary object in the virtual infrastructure, you can use the search field at the bottom of the corresponding window. Click the button on the left of the field to select the necessary type of object, enter an object's name or a part of it and click the **Start search** button on the right or press [ENTER].

The screenshot shows the 'New Replication Job' wizard in the 'Destination' step. The window title is 'New Replication Job'. The main heading is 'Destination' with a sub-heading 'Specify where replicas should be created in the DR site.' On the left is a navigation pane with options: Name, Virtual Machines, Destination (selected), Network, Re-IP, Job Settings, Data Transfer, Seeding, Guest Processing, Schedule, and Summary. The main area contains the following fields and options:

- Host or cluster:** esx01.tech.local (Choose...)
- Resource pool:** Replicas (Choose...)
Pick resource pool for selected replicas
- VM folder:** vm (Choose...)
Pick VM folder for selected replicas
- Datastore:** esx01-das3 [752.3 GB free] (Choose...)
Pick datastore for selected virtual disks

At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 8. Create Network Map Table

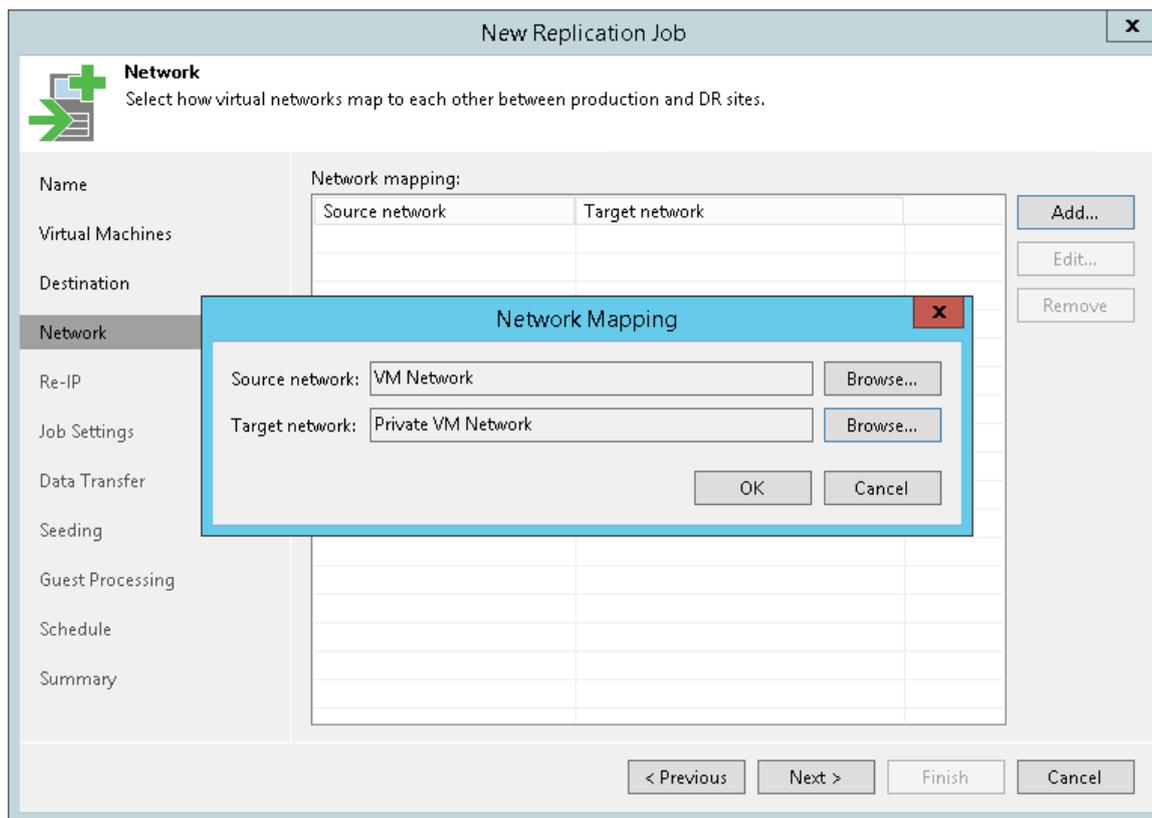
The **Network** step of the wizard is available if you have selected the **Separate virtual networks** option at the **Name step** of the wizard. You can use this step to configure network mapping settings for the VM replicas.

Network mapping can be helpful if you use different networks in the production site and DR site. In this situation, you can configure a table that maps production networks to networks in the DR site. During every replication job session, Veeam Backup & Replication will check the network mapping table and update the VM replica configuration file to replace the production network with the specified network in the DR site. As a result, when you perform failover, the VM replica will be connected to the necessary networks in the DR site, and you will not have to re-configure network settings for the VM replica manually.

To configure a network mapping table:

1. Click **Add**.
2. Click **Browse** next to the **Source network** field and select the production network to which VMs added to the job are connected.
3. Click **Browse** next to the **Target network** field and select the network in the DR site to which VM replicas must be connected.

4. Repeat steps 1-3 for all networks to which VM replicas must be connected.



Step 9. Configure Re-IP Rules

The **Re-IP** step of the wizard is available if you have selected the **Different IP addressing scheme** option at the **Name** step of the wizard. You can use this step to configure Re-IP rules for Microsoft Windows VMs.

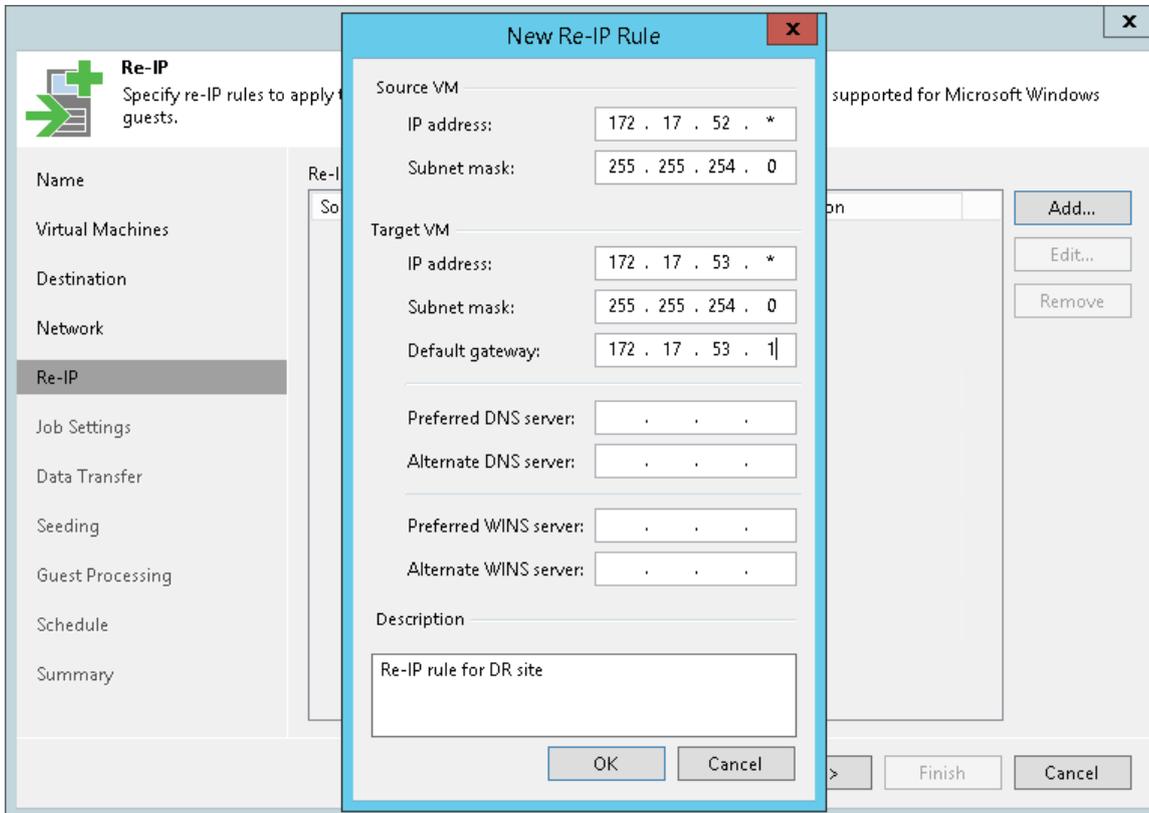
Re-IP rules can be helpful if the IP addressing scheme in the production site differs from the addressing scheme in the DR site. In this situation, you can configure a number of re-IP rules for the replication job. When you perform failover, Veeam Backup & Replication will check if configured Re-IP rules apply for the VM replica. If a Re-IP rule applies to the VM replica, the VM replica will get a new IP address according to the new network mask, and you will be able to reach this VM replica in the DR site.

To configure a Re-IP rule:

1. Click **Add**.
2. In the **Source VM** section, describe an IP numbering scheme adopted in the source site. To facilitate configuration, Veeam Backup & Replication detects an IP address and subnet mask for the backup server and pre-populates values in the **Source VM** section.
3. In the **Target VM** section, describe an IP numbering scheme adopted in the DR site. Specify an IP address, subnet mask and default gateway that will be used for VM replicas. If necessary, define the DNS and WINS server addresses.
4. In the **Description** field, specify a brief outline of the rule or any related comments.

NOTE:

You can use the asterisk character (*) to specify a range of IP addresses, for example, 172.16.17.*. Do not use 0 to specify a range of IP addresses. In Veeam Backup & Replication, value 172.16.17.0 means a regular IP address 172.16.17.0, not an IP address range.



Step 10. Specify Replication Job Settings

At the **Job Settings** step of the wizard, define replication job settings.

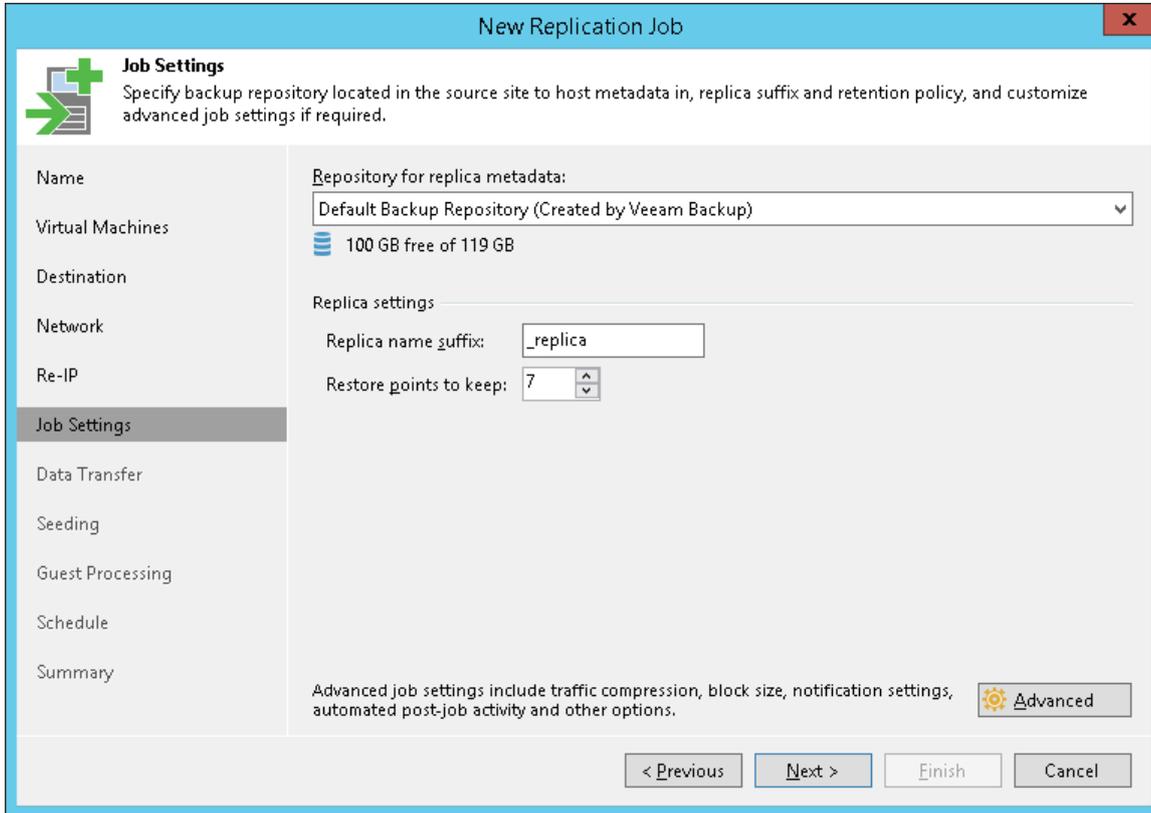
1. From the **Repository for replica metadata** list, select a backup repository that is located in the source site. This backup repository will be used to store metadata for VM replicas – checksums of read data blocks required to streamline incremental sessions of the replication job.
2. In the **Replica name suffix** field, enter a suffix for the name of VM replicas. To register a VM replica on the target host, Veeam Backup & Replication appends the specified suffix to the name of the source VMs. Files of the VM replica are placed to the *VMname_suffix* folder on the selected datastore.
3. In the **Restore points to keep** field, specify the number of restore points that must be maintained by the replication job. If this number is exceeded, the earliest restore point will be removed.

Due to VMware restrictions on the number of VM snapshots, the maximum number of restore points for VM replicas is limited to 28.

When you specify the retention policy settings for the replication job, consider available space on the target datastore. A great number of restore points (snapshots) may fill the target datastore.

IMPORTANT!

- You cannot store VM replica metadata on deduplicating storage appliances. During replication jobs, Veeam Backup & Replication frequently reads and writes small portions of metadata from/to the backup repository. Frequent access to metadata causes low performance of deduplicating storage appliances, which may result in low performance of replication jobs.
- You cannot store replica metadata on a scale-out backup repository.



The screenshot shows the 'New Replication Job' wizard in the 'Job Settings' step. The window title is 'New Replication Job'. The 'Job Settings' section is active, with a sub-header 'Job Settings' and a description: 'Specify backup repository located in the source site to host metadata in, replica suffix and retention policy, and customize advanced job settings if required.' The left sidebar contains a list of steps: Name, Virtual Machines, Destination, Network, Re-IP, Job Settings (selected), Data Transfer, Seeding, Guest Processing, Schedule, and Summary. The main area shows the following settings:

- Repository for replica metadata:** A dropdown menu showing 'Default Backup Repository (Created by Veeam Backup)' with a status indicator '100 GB free of 119 GB'.
- Replica settings:**
 - Replica name suffix:
 - Restore points to keep:

At the bottom, there is a note: 'Advanced job settings include traffic compression, block size, notification settings, automated post-job activity and other options.' Next to it is an 'Advanced' button with a gear icon. At the very bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 11. Specify Advanced Replica Settings

At the **Job settings** step of the wizard, you can specify the following settings for the replication job:

- [Traffic settings](#)
- [Notification settings](#)
- [vSphere settings](#)
- [Integration settings](#)
- [Script settings](#)

TIP:

After you specify necessary settings for the replication 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 replication job, Veeam Backup & Replication will automatically apply the default settings to the new job.

Traffic Settings

To specify traffic settings for the replication job:

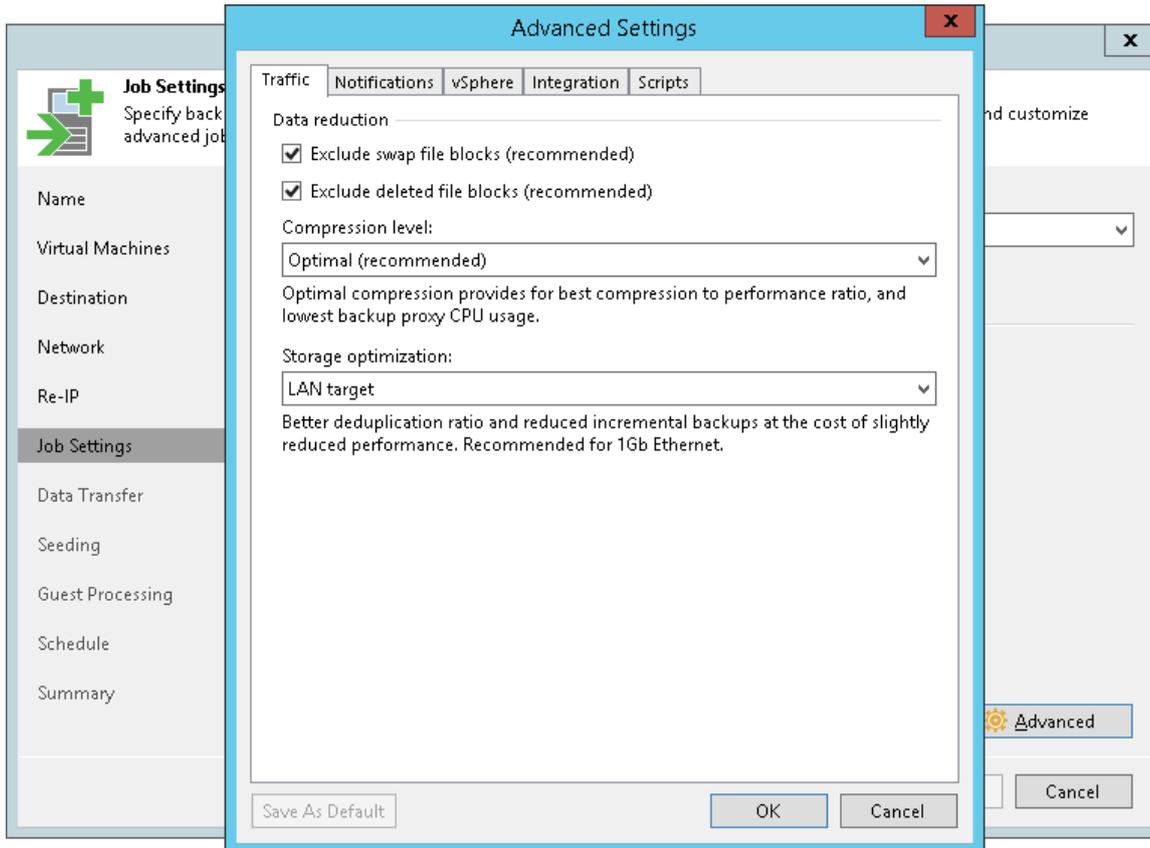
1. At the **Job Settings** step of the wizard, click **Advanced**.
2. Click the **Traffic** tab.
3. By default, Veeam Backup & Replication checks the NTFS MFT file on VMs with Microsoft Windows OS to identify data blocks of the `hiberfil.sys` file (file used for the hibernate mode) and `pagefile.sys` file (swap file), and excludes these data blocks from processing. The swap file is dynamic in nature and changes intensively between replication job sessions, even if the VM itself does not change much. Processing of service files reduces the job performance and increases the size of incremental data.

If you want to include data blocks of the `hiberfil.sys` file and `pagefile.sys` file to the replica, clear the **Exclude swap file blocks** check box. For more information, see [Swap Files](#).
4. By default, Veeam Backup & Replication does not copy deleted file blocks ("dirty" blocks on the VM guest OS) to the target location. This option lets you reduce the size of the VM replica and increase the job performance. If you want to include dirty data blocks to the VM replica, clear the **Exclude deleted file blocks** check box. For more information, see [Deleted File Blocks](#).
5. From the **Compression level** list, select a compression level for the created VM replica: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*. Compression is applicable only if VM data is transferred between two backup proxies. If one backup proxy acts as the source and target backup proxy, VM data is not compressed at all.
6. In the **Storage optimization** section, select what type of backup target you plan to use: *Local target (large blocks)*, *Local target*, *LAN target* or *WAN target*. Depending on the chosen storage type, Veeam Backup & Replication will use data blocks of different size to optimize the size of backup files and job performance.

When selecting the data block size, consider the following aspects:

- When reading the VM image, Veeam Backup & Replication "splits" the VM image into blocks of the selected size. The more data blocks there are, the more time is required to process the VM image.
- Veeam Backup & Replication writes information about every data block to the VM replica metadata stored on the backup repository. The more data blocks there are, the more metadata is written to the backup repository.
- During incremental job runs, Veeam Backup & Replication uses CBT to define changed data blocks in the VM. The larger is the size of the found changed data block, the greater amount of data needs to be transferred to the target site.

For more information, see [Compression and Deduplication](#).



Notification Settings

To specify notification settings for the replication job:

1. At the **Job Settings** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully.

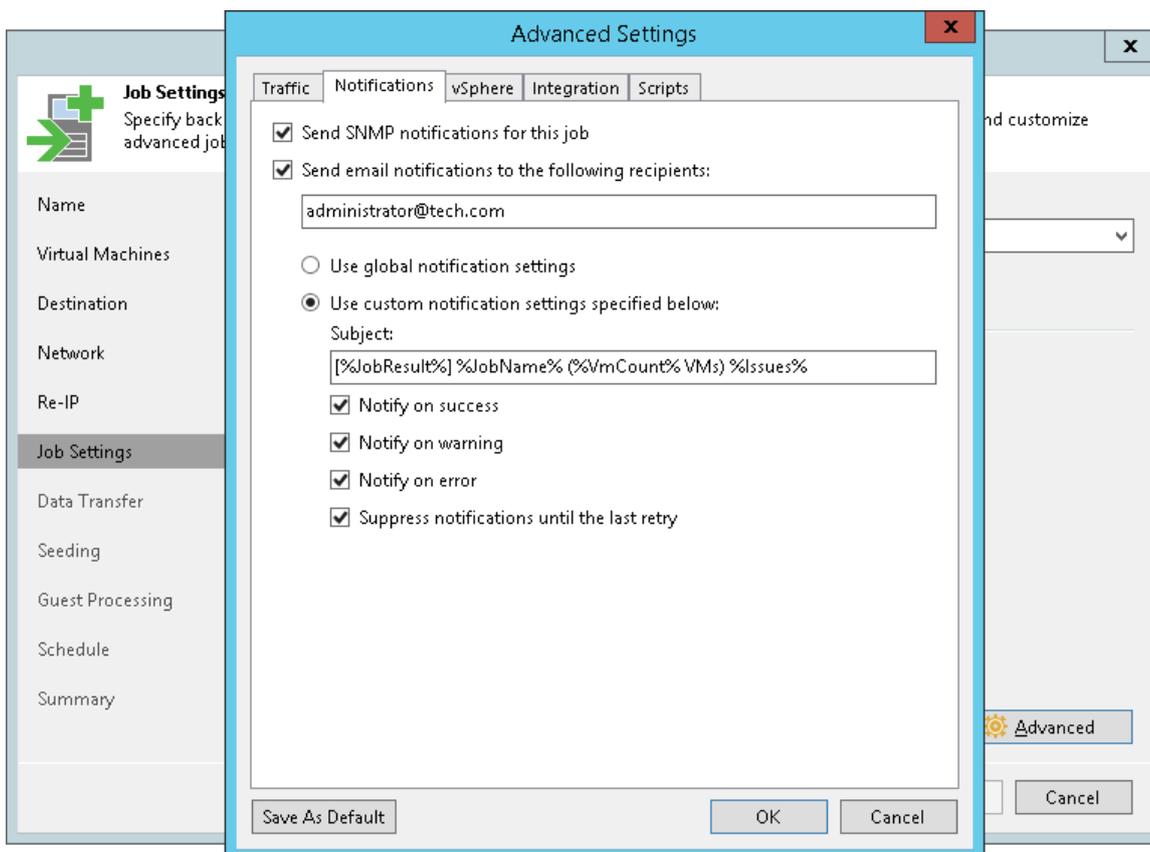
SNMP traps will be sent if you configure global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see [Specifying SNMP Settings](#).

4. 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 global email notification settings in Veeam Backup & Replication. For more information, see [Configuring Global Email Notification Settings](#).

5. You can choose to use global notification settings or specify custom notification settings.
 - o To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see [Configuring Global Email Notification Settings](#).

- o To configure a custom notification for a job, select **Use custom notification settings specified below**. You can specify the following notification settings:
 - a. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of VMs in the job) and *%Issues%* (number of VMs in the job that have been processed with the *Warning* or *Failed* status).
 - b. 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.
 - c. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, Veeam Backup & Replication will send one notification per every job retry.



vSphere Settings

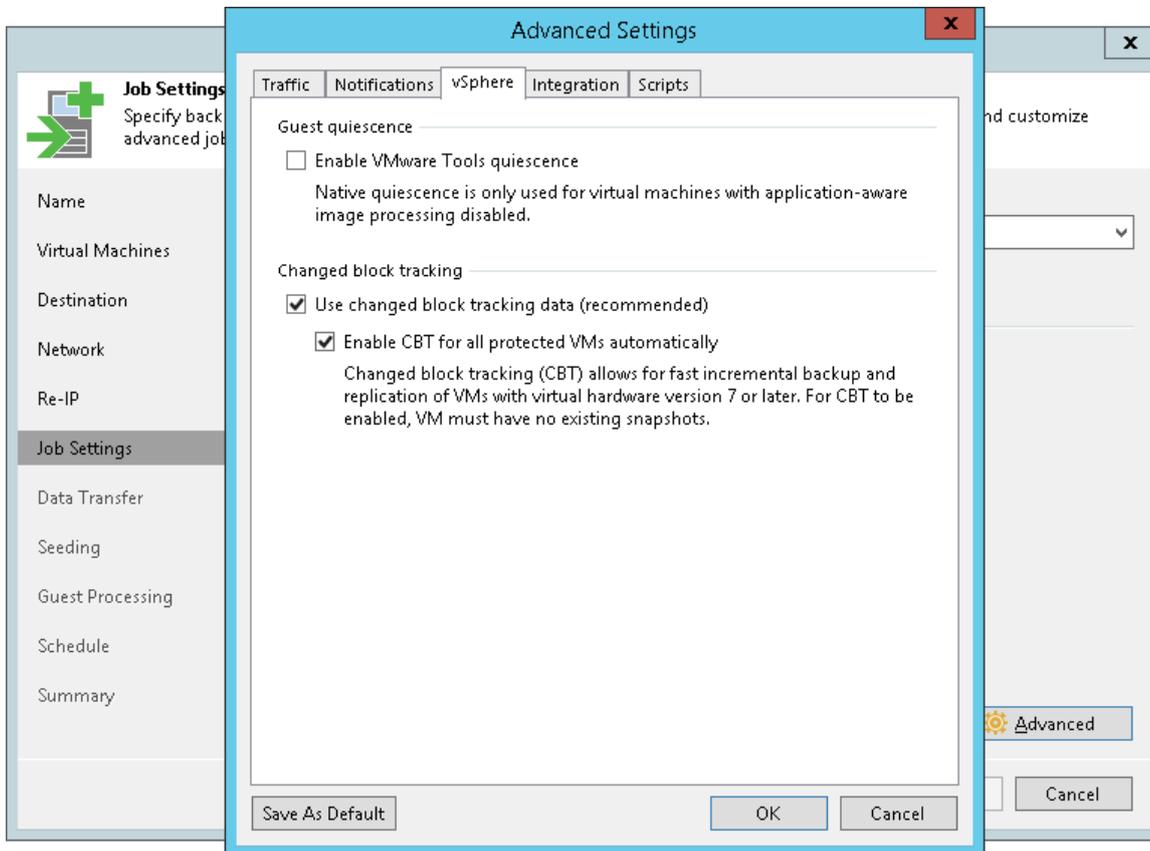
To specify vSphere settings for the replication job:

1. At the **Job Settings** step of the wizard, click **Advanced**.
2. Click the **vSphere** tab.
3. Select the **Enable VMware tools quiescence** check box to freeze the file system of processed VMs during replication. Depending on the VM version, Veeam Backup & Replication will use the VMware Filesystem Sync Driver (vmsync) driver or VMware VSS component in VMware Tools for VM snapshot creation. These tools are responsible for quiescing the VM file system and bringing the VM to a consistent state suitable for replication.

4. In the **Changed block tracking** section, specify if VMware vSphere CBT must be used for replication. By default, this option is enabled. If you want to force using CBT even if CBT is disabled at the level of the ESX(i) host, select the **Enable changed block tracking for all processed VMs** check box.

IMPORTANT!

You can use CBT only for VMs with virtual hardware version 7 or later.



Integration Settings

On the **Integration** tab, define whether you want to use the Backup from Storage Snapshots technology to create a VM replica. Backup from Storage Snapshots lets you leverage storage snapshots for VM data processing. The technology improves RPOs and reduces the impact of replication activities on the production environment.

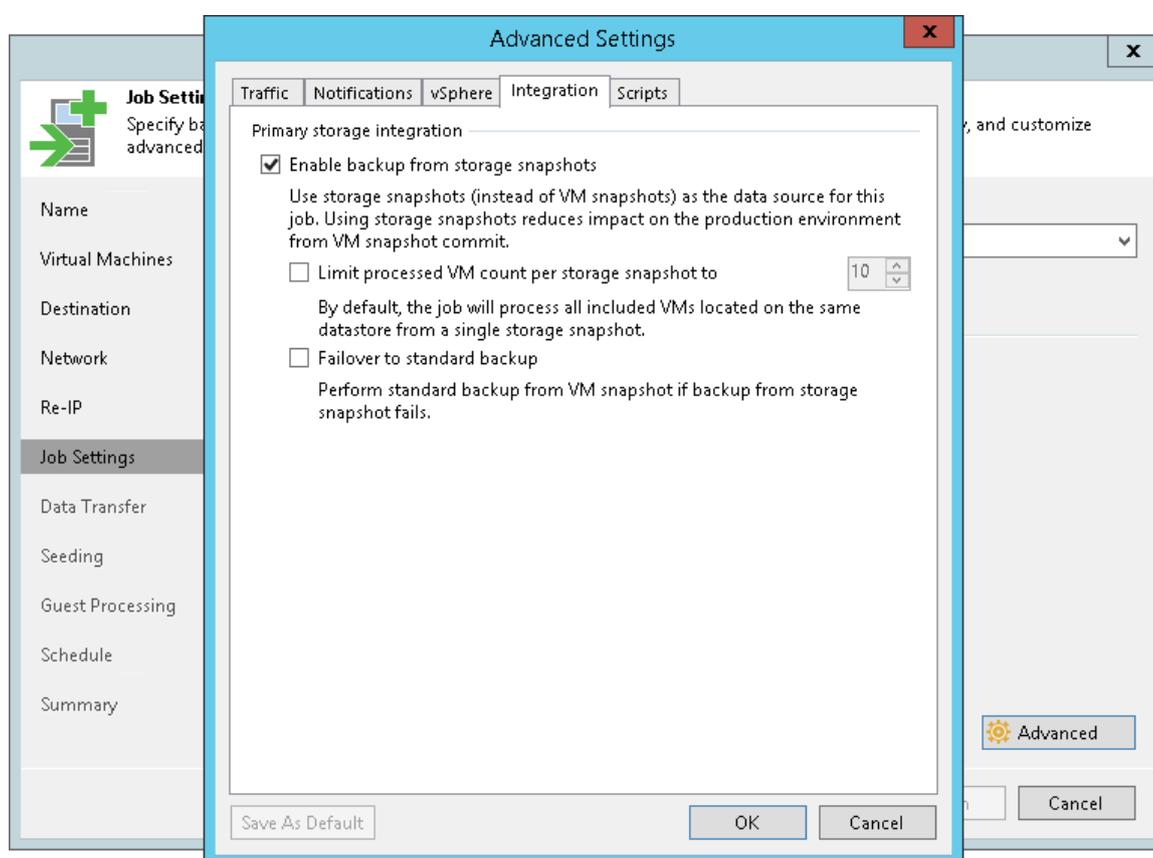
To specify storage integration settings for the replication job:

1. At the **Job Settings** step of the wizard, click **Advanced**.
2. Click the **Integration** tab.
3. By default, the **Enable backup from storage snapshots** option is enabled. If you do not want to use Backup from Storage Snapshots, clear this check box. For more information, see [Performing Backup from Storage Snapshots](#).

4. If you add to the job many VMs whose disks are located on the same volume or LUN, select the **Limit processed VM count per storage snapshot to** check box and specify the number of VMs for which one storage snapshot must be created. In a regular job processing course, Veeam Backup & Replication creates a VMware snapshot for every VM added to the job and then triggers one storage snapshot for all VMs. In some situations, creating VMware snapshots for all VMs may require a lot of time. If you limit the number of VMs per storage snapshot, Veeam Backup & Replication will divide VMs into several groups, trigger a separate storage snapshot for every VM group and read VM data from these snapshots. As a result, the job performance will increase.

For example, you add to the job 30 VMs whose disks are located on the same volume and set the **Limit processed VM count per storage snapshot to** option to 10. Veeam Backup & Replication will divide all VMs into 3 groups and create 3 storage snapshots from which it will read VM data.

5. If the backup infrastructure is configured incorrectly, for example, the backup proxy does not meet the necessary requirements, Backup from Storage Snapshots will fail and VMs residing on the storage systems will not be processed by the job at all. To fail over to the regular VM processing mode and process such VMs in any case, select the **Failover to standard backup** check box.



Script Settings

To specify script settings for the replication job:

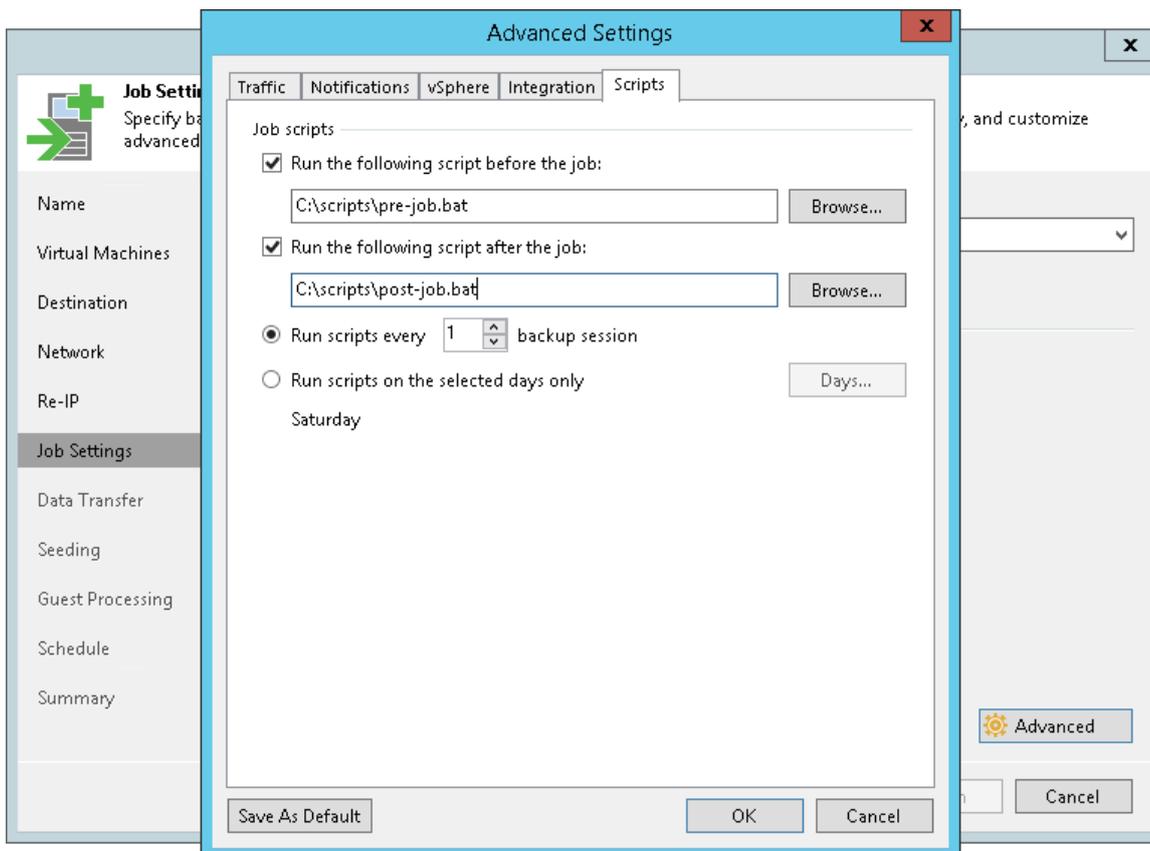
1. At the **Job Settings** step of the wizard, click **Advanced**.
2. Click the **Scripts** tab.
3. If you want to execute custom scripts before and/or after the replication job, select the **Run the following script before the job** and **Run the following script after the job** check boxes and click **Browse** to choose executable files from a local folder on the backup server. The scripts are executed on the backup server.

You can select to execute pre- and post-replication actions after a number of job sessions or on specific week days.

- If you select the **Run scripts every... backup session** option, specify the number of the replication job sessions after which scripts must be executed.
- If you select the **Run scripts on selected days only** option, click **Days** and specify week days on which scripts must be executed.

NOTE:

Custom scripts that you define in the advanced job settings relate to the replication job itself, not the VM quiescence process. To add pre-freeze and post-thaw scripts for VM image quiescence, use the **Guest Processing** step of the wizard.



Step 12. Specify Data Transfer Settings

At the **Data Transfer** step of the wizard, select backup infrastructure components that must be used for the replication process and choose a path for VM data transfer.

1. If you plan to replicate VM data within one site, the same backup proxy can act as the source and target backup proxy. For offsite replication, you must deploy at least one backup proxy in each site to establish a stable connection for VM data transfer across sites.

Click **Choose** next to the **Source proxy** and **Target proxy** fields to select backup proxies for the job. In the **Backup Proxy** window, you can choose automatic backup proxy selection or assign backup proxies explicitly.

- If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that have access to the source and target datastores and automatically assign optimal backup proxy resources for processing VM data.

Veeam Backup & Replication assigns resources to VMs included in the replication job one by one. Before processing a new VM from the list, Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use and the current workload on the backup proxies to select the most appropriate backup proxy for VM processing.

- If you choose **Use the selected backup proxy servers only**, you can explicitly select backup proxies that the job can use. It is recommended that you select at least two backup proxies to ensure that the job will be performed if one of backup proxies fails or loses its connectivity to the source datastore.

2. Select a path for VM data transfer:

- To transport VM data directly via backup proxies to the target datastore, select **Direct**.
- To transport VM data via WAN accelerators, select **Through built-in WAN accelerators**. From the **Source WAN accelerator** list, select the WAN accelerator configured in the source site. From the **Target WAN accelerator** list, select the WAN accelerator configured in the target site.

You should not assign one source WAN accelerator to several replication jobs that you plan to run simultaneously. The source WAN accelerator requires a lot of CPU and RAM resources, and does not process multiple replication tasks in parallel. As an alternative, you can create one replication job for all VMs you plan to process over one source WAN accelerator.

The target WAN accelerator, however, can be assigned to several replication jobs. For more information, see [Adding WAN Accelerators](#).

New Replication Job

Data Transfer
Choose how VM data should be transferred to the target site.

Name
Virtual Machines
Destination
Network
Re-IP
Job Settings
Data Transfer
Seeding
Guest Processing
Schedule
Summary

When replicating between remote sites, we highly recommend that you deploy at least one backup proxy server locally in both sites to allow for direct access to storage.
Source proxy:
Automatic selection

Target proxy:
Automatic selection

Direct
Best for local and off-site replication over fast links.

Through built-in WAN accelerators
Best for off-site replication over slow links due to significant bandwidth savings.
Source WAN accelerator:
srv01.tech.local (Source WAN Accelerator)
Target WAN accelerator:
srv07.tech.local (Target WAN Accelerator)

< Previous Next > Finish Cancel

Step 13. Define Seeding and Mapping Settings

The **Seeding** step is available if you have selected the **Low connection bandwidth** option at the [Name step](#) of the wizard. You can use this step to configure replica seeding and mapping for the replication job.

If you use replica seeding or mapping, make sure that you select correct backup infrastructure components for the job: source-side backup repository for metadata and backup proxies. It is recommended that you explicitly assign backup proxies in the production site and DR site. For more information, see [Step 12. Specify Data Transfer Settings](#).

Configuring Replica Seeding

If you plan to replicate to a remote DR site over WAN or low-bandwidth network, you can use replica seeding. Replica seeding helps reduce the amount of VM data transferred over the network.

Replica seeding can be used if you have a backup for the replicated VM on the backup repository located in the DR site. In this case, you can point the replication copy job to this backup. During the first session of the replication job, Veeam Backup & Replication will use this backup file as a "seed". Veeam Backup & Replication will restore the VM image from the backup and register the VM replica on the target host. After that, Veeam Backup & Replication will synchronize the VM replica with the source VM. All subsequent incremental replication runs will be performed in the regular manner.

Before you start a replication job that uses replica seeding, you must perform a number of preparatory tasks:

1. Create a backup (seed) of the VM that you plan to replicate. To do this, configure a backup job that points to an onsite backup repository. Run the job to create a full backup.

If you have previously created a backup containing all necessary VMs, there is no need to configure and run a new backup job.

For seeding, you can use any existing backup created with Veeam Backup & Replication. The backup must include VBK and VBM files. If you have a full backup and a chain of forward increments, you can use VIB files together with the VBK and VBM files. In this case, Veeam Backup & Replication will restore VMs from the seed to the latest available restore point.

2. Copy the backup from the backup repository in the production site to a backup repository in the DR site. If you do not have a backup repository in the DR site, you will need to create one.

You can move the backup using a file copy job or any other appropriate method, for example, copy the backup to a removable storage device, ship the device to the DR site and copy backups to the backup repository in the DR site.

3. After the backup is copied to the backup repository in the DR site, perform rescan of this backup repository. Otherwise, Veeam Backup & Replication will not be able to detect the copied backup.

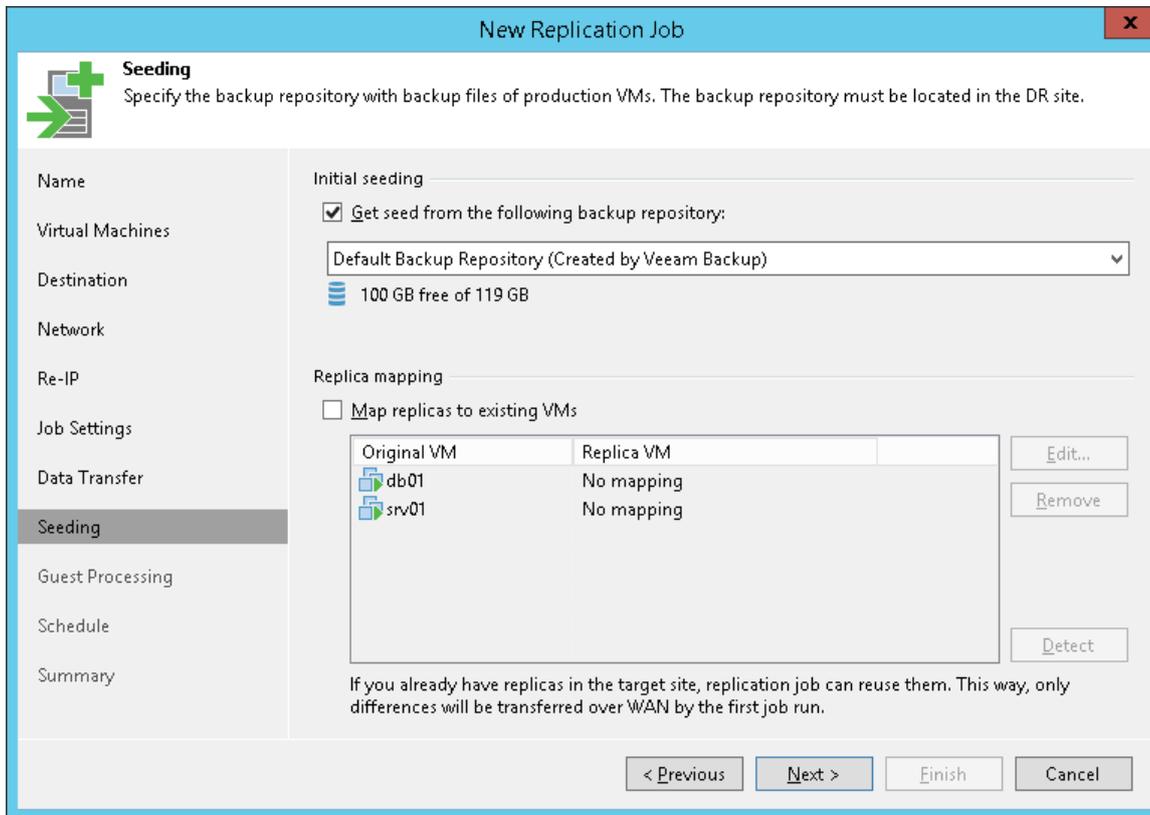
When you complete the preliminary steps, you can configure replica seeding settings for the job.

1. In the **Initial seeding** section, select the **Get seed from the following backup repository** check box.
2. From the list of backup repositories, select the backup repository in the DR site to where the seed (the full backup) resides.

When you start the replication job, Veeam Backup & Replication will attempt to restore all VMs added to the job from the seed that you have specified. If a VM is not found in the seed, the VM will be skipped from replication.

IMPORTANT!

You cannot use a backup located on the scale-out backup repository as a seed for a replication job.



Configuring Replica Mapping

If a replica for the VM that you plan to replicate already exists on the target host in the DR site, you can use replica mapping. Replica mapping helps reduce the amount of VM data transferred over the network.

To use replica mapping, you must point the replication job to a VM replica on the host in the DR site. During the first session of the replication job, Veeam Backup & Replication will calculate the difference between the source VM and VM replica and copy necessary data blocks to synchronize the VM replica to the latest state of the source VM. All subsequent incremental replication sessions will be performed in the regular manner.

TIP:

If there is no existing VM replica in the DR site, you can restore a VM from the backup and map it to the original VM.

To set up replica mapping:

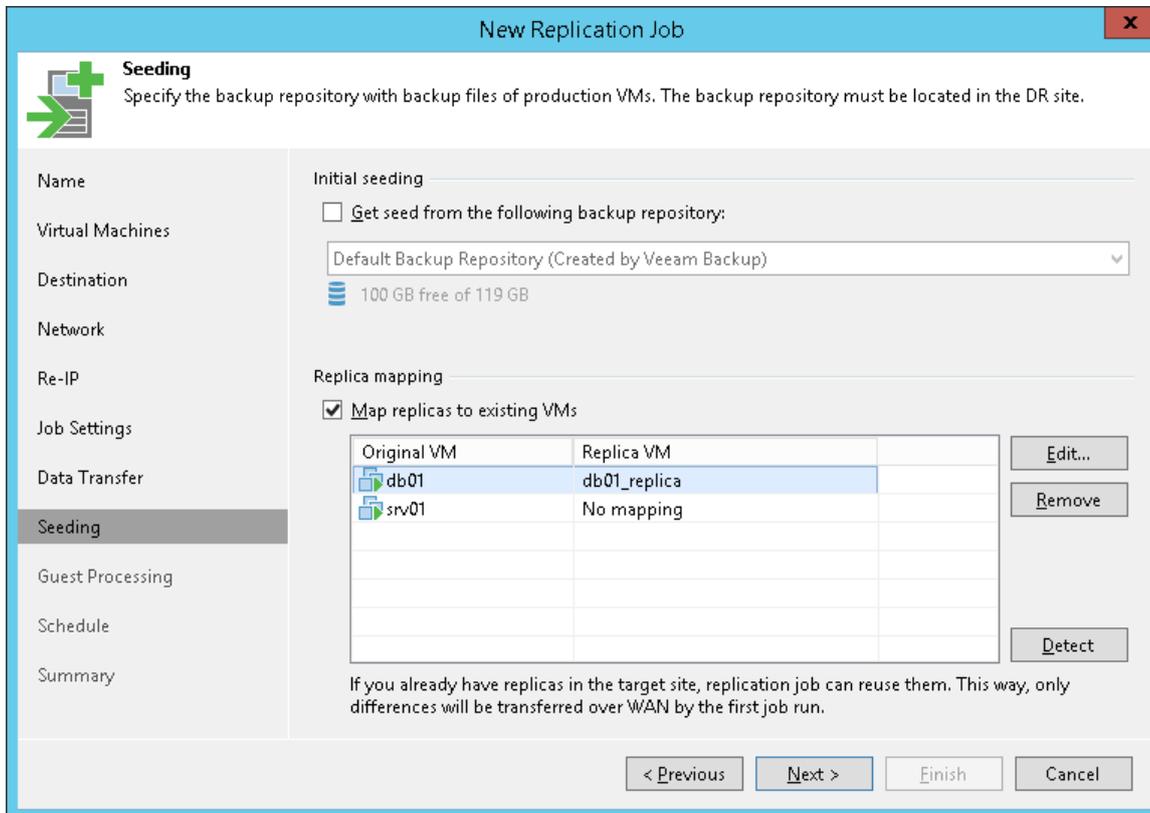
1. Select the **Map replicas to existing VMs** check box.
2. Click **Detect**. Veeam Backup & Replication will scan the destination location to detect existing VM replicas. If any matches are found, Veeam Backup & Replication will populate the mapping table.

If Veeam Backup & Replication does not find a match, you can map a VM to its VM replica manually. To do this, select a production VM from the list, click **Edit** and choose an existing VM replica. To facilitate selection, use the search field at the bottom of the window.

To break a mapping association, select the VM in the list and click **Remove**.

IMPORTANT!

The mapping list does not display VMs added to the list of exclusions. For more information, see [Step 5. Exclude Objects from Replication Job](#).



Configuring Replica Seeding and Replica Mapping

You configure both replica seeding and replica mapping in the same replication job. For example, if a job includes 2 VMs, you can use seeding for one VM and map the other VM to an existing VM replica.

If replica seeding is enabled in the job settings, all VMs in the job must be covered with seeding or mapping. If a VM is neither available in the seed, nor mapped to an existing VM replica, it will be skipped from processing. And, on the contrary, if the same VM is available in the seed and mapped to an existing replica, replication will be performed using replica mapping as mapping has precedence over seeding.

Step 14. Specify Guest Processing Settings

At the **Guest Processing** step of the wizard, you can enable the following settings for VM guest OS processing:

- [Application-aware processing](#)
- [Transaction log handling for Microsoft SQL Server](#)
- [Transaction log handling for Oracle](#)
- [VM guest OS file exclusion](#)
- [Use of pre-freeze and post-thaw scripts](#)

To coordinate guest processing activities, Veeam Backup & Replication deploys a runtime process on the VM guest OS. The process runs only during guest processing and is stopped immediately after the processing is finished (depending on the selected option, during the replication job session or after the replication job completes).

You must specify a user account that will be used to connect to the VM guest OS and deploy the runtime process:

1. From the **Guest OS credentials** list, select a user account with local administrator privileges on the VM guest OS. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see [Guest Processing](#).

Local accounts do not support Kerberos authentication. To authenticate with Microsoft Windows guest OS using Kerberos, specify an Active Directory account.

NOTE:

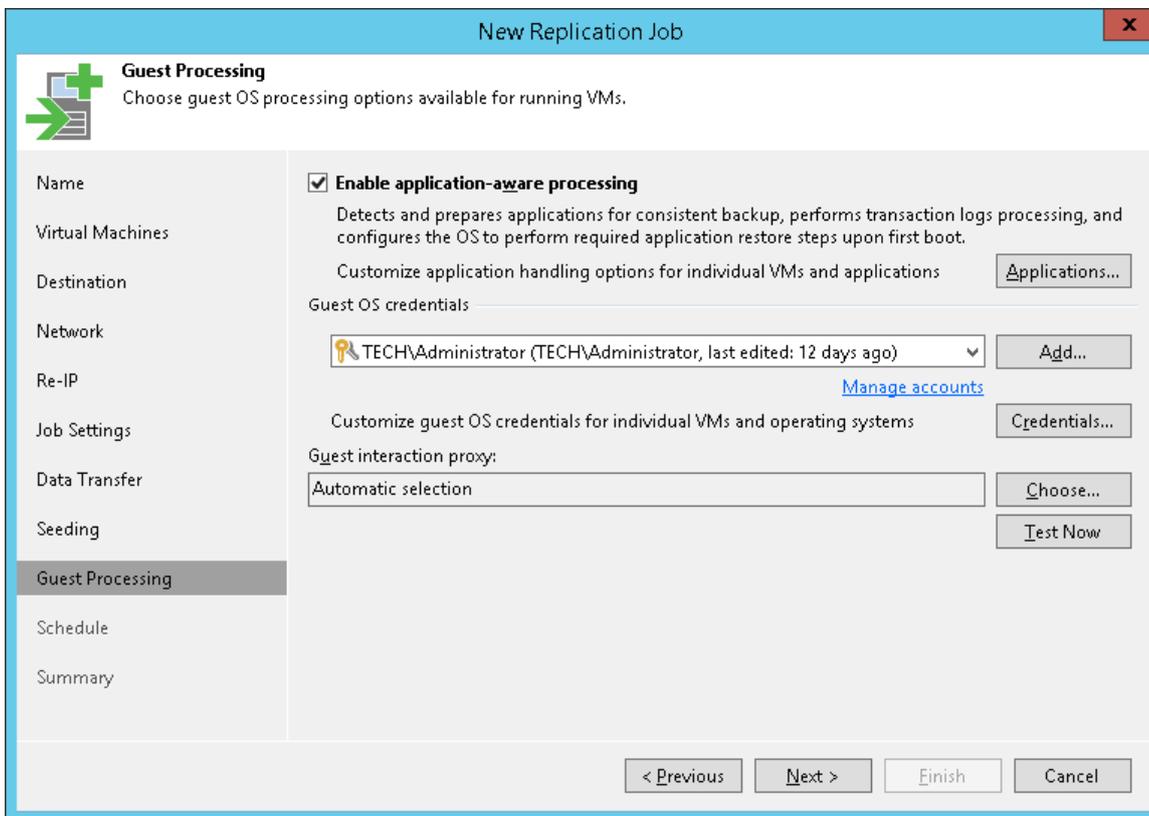
[For Kerberos authentication] Mind the following:

- Networkless application-aware guest processing through VMware VIX/vSphere Web Services is not supported for VMs with guest OS where NTLM is restricted.
 - Veeam backup infrastructure machines (backup server, repositories, backup proxies, guest interaction proxies, etc.) must correctly resolve FQDNs of guest operating systems.
 - To back up VMs where Kerberos is used, NTLM must be allowed in the Veeam backup infrastructure machines. For details, see [Kerberos Authentication for Guest OS Processing](#).
2. By default, Veeam Backup & Replication uses the same credentials for all VMs in the job. If some VM requires a different user account, click **Credentials** and enter custom credentials for the VM.
 3. If you have added Microsoft Windows VMs to the job, specify which guest interaction proxy Veeam Backup & Replication can use to deploy the runtime process on the VM guest OS. On the right of the **Guest interaction proxy** field, click **Choose**.
 - Leave **Automatic selection** to let Veeam Backup & Replication automatically select the guest interaction proxy.
 - Select **Use the selected guest interaction proxy servers only** to explicitly define which servers will perform the guest interaction proxy role. The list of servers contains Microsoft Windows servers added to the backup infrastructure.

To check if Veeam Backup & Replication can communicate with VMs added to the job and deploy the runtime process on their guest OSes, click **Test Now**. Veeam Backup & Replication will use the specified credentials to connect to all VMs in the list.

NOTE:

The guest interaction proxy functionality is available in the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication.



Application-Aware Processing

If you add to the replication job VMs running VSS-aware applications, you can enable application-aware processing to create transactionally consistent replicas. The transactionally consistent replica guarantees proper recovery of applications on VMs without data loss.

To enable application-aware processing:

1. Select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the VM and click **Edit**.

To define custom settings for a VM added as a part of the VM container, you must include the VM in the list as a standalone object. To do this, click **Add** and choose a VM whose settings you want to customize. Then select the VM in the list and define the necessary settings.

4. On the **General** tab, in the **Applications** section specify the VSS behavior scenario:
 - Select **Require successful processing** if you want Veeam Backup & Replication to stop the replication process if any VSS errors occur.
 - Select **Try application processing, but ignore failures** if you want to continue the replication process even if VSS errors occur. This option is recommended to guarantee completion of the job. The created VM replica image will not be transactionally consistent but crash consistent.
 - Select **Disable application processing** if you do not want to enable quiescence for the VM at all.

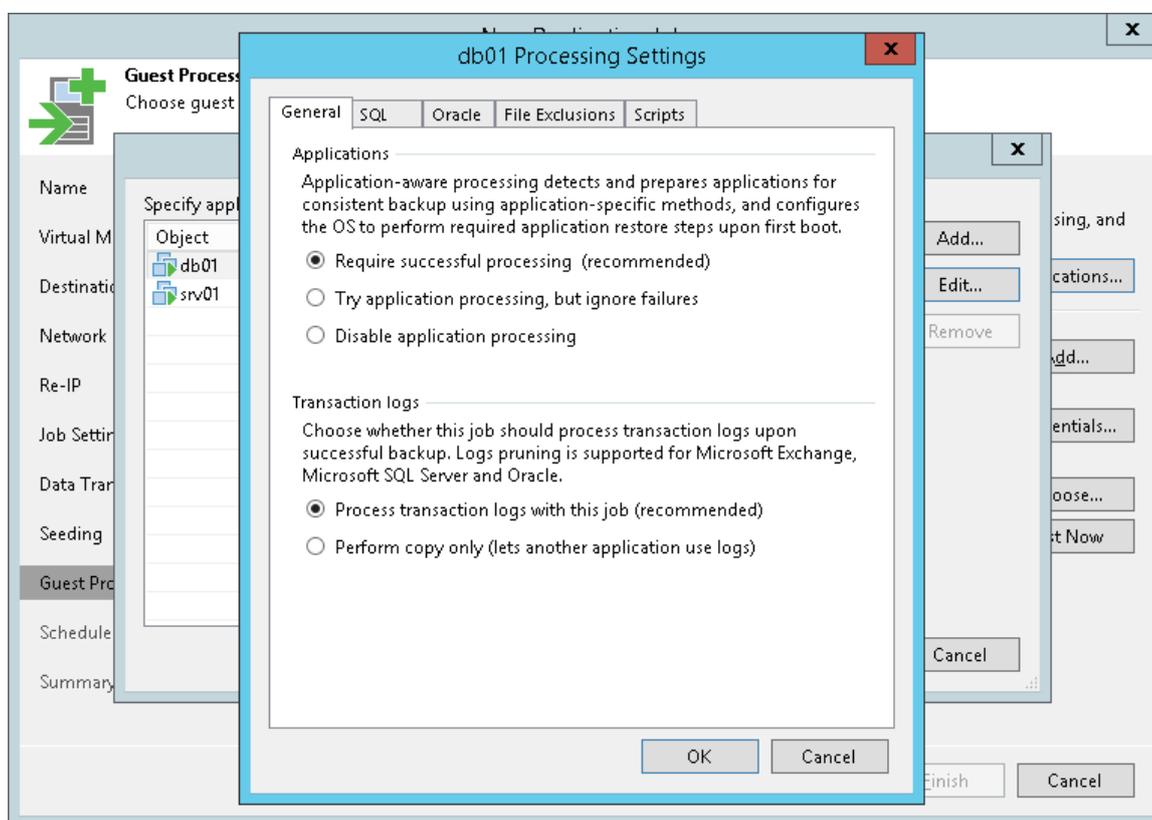
5. [For Microsoft Exchange, Microsoft SQL and Oracle VMs] In the **Transaction logs** section, specify if Veeam Backup & Replication must process transaction logs or copy-only backups must be created.

- a. Select **Process transaction logs with this job** if you want Veeam Backup & Replication to process transaction logs.

[For Microsoft Exchange VMs] With this option selected, the runtime process running on the VM guest OS will wait for replication to complete successfully and then trigger truncation of transaction logs. If the replication job fails, the logs will remain untouched on the VM guest OS until the next start of the runtime process.

[For Microsoft SQL Server VMs and Oracle VMs] You will have to specify settings for transaction log handling on the **SQL** and **Oracle** tabs of the **VM Processing Settings** window. For more information, see [Transaction Log Settings: Microsoft SQL](#) and [Transaction Log Settings: Oracle](#).

- b. Select **Perform copy only** if you use another backup tool to perform VM guest level backup or replication, and this tool maintains consistency of the database state. Veeam Backup & Replication will create a copy-only replica for the selected VM. The copy only replica preserves the chain of full/differential backup files and transaction logs on the VM. For more information, see <http://msdn.microsoft.com/en-us/library/ms191495.aspx>.

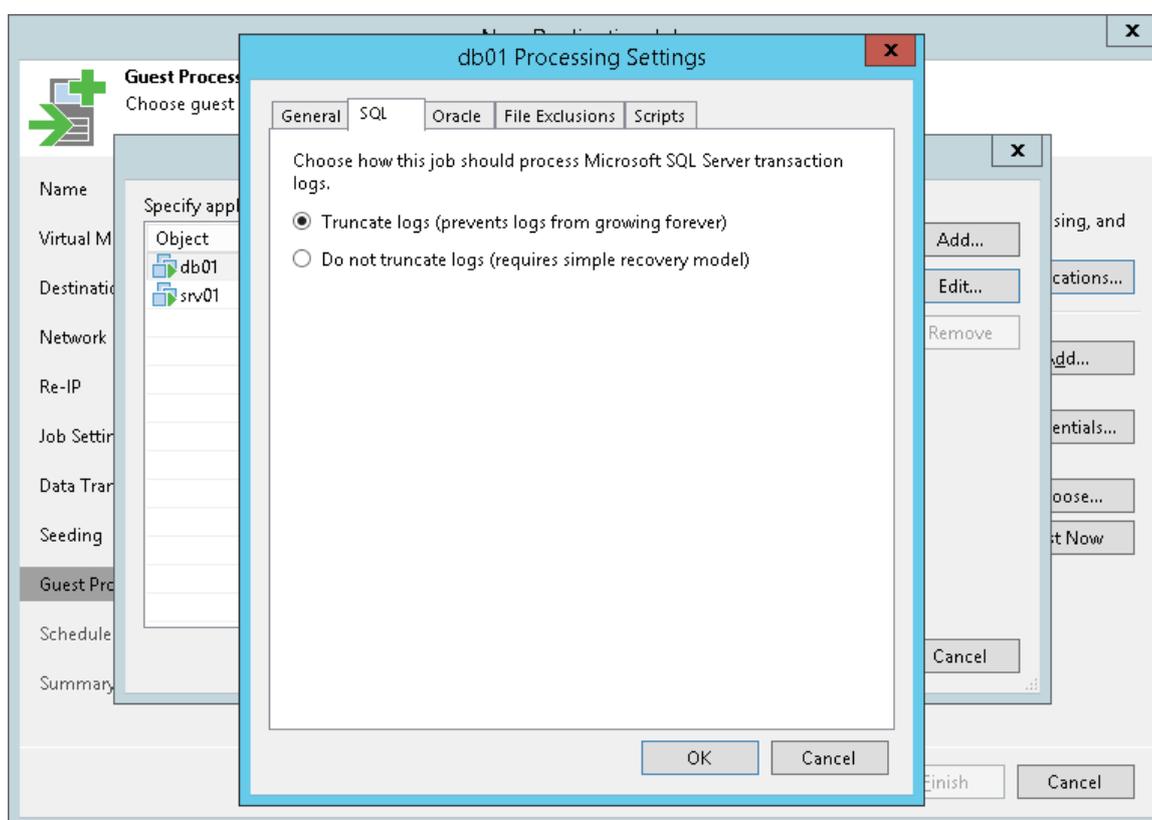


Transaction Log Settings: Microsoft SQL Server

If you replicate a Microsoft SQL VM, you can specify how Veeam Backup & Replication must process transaction logs:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the Microsoft SQL Server VM and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.

5. In the **VM Processing Settings** window, click the **SQL** tab.
6. Specify how transaction logs must be processed:
 - Select **Truncate logs** if you want Veeam Backup & Replication to trigger truncation of transaction logs only after the job completes successfully. In this case, the runtime process will wait for VM replication to complete and then trigger truncation of transaction logs. If the replication job fails, the logs will remain untouched on the VM guest OS until the next start of the runtime process.
 - Select **Do not truncate logs** if you do not want Veeam Backup & Replication to truncate logs at all. This option is recommended if you are using another backup tool to perform VM guest-level backup or replication, and this tool maintains consistency of the database state. In such scenario, Veeam Backup & Replication will not trigger transaction log truncation. After you fail over to the necessary restore point of the VM replica, you will be able to apply transaction logs to get the database system to the necessary point in time between replication job sessions.



Transaction Log Settings: Oracle

If you replicate an Oracle VM, you can specify how Veeam Backup & Replication must process transaction logs:

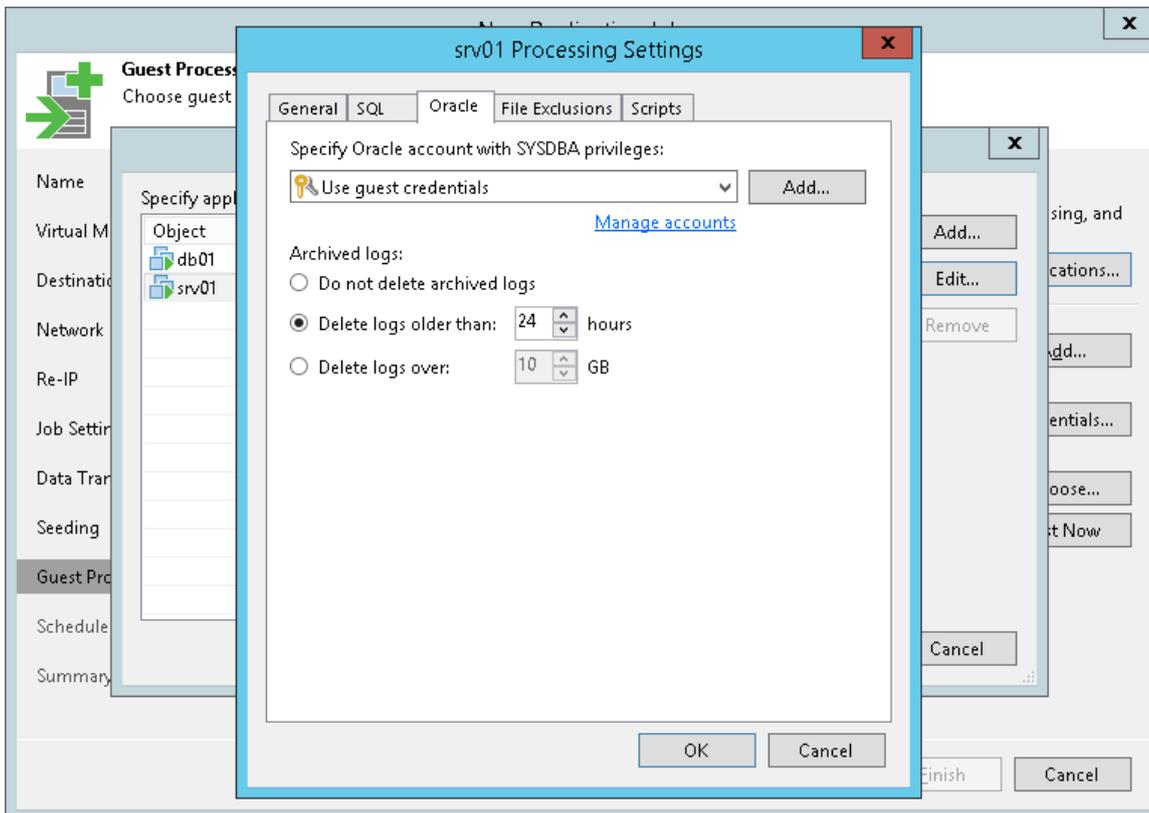
1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the Oracle VM and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.
5. In the **VM Processing Settings** window, click the **Oracle** tab.
6. In the **Specify Oracle account with SYSDBA privileges** section, specify a user account that Veeam Backup & Replication will use to connect to the Oracle database. The account must have SYSDBA rights on the Oracle database.

You can select **Use guest credentials** in the list of user accounts. In this case, Veeam Backup & Replication will use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.

7. In the **Archived logs** section, specify if Veeam Backup & Replication must truncate transaction logs on the Oracle VM:
 - Select **Do not truncate archived logs** if you want Veeam Backup & Replication to preserve archived logs on the VM guest OS. When the replication job completes, the runtime process will not truncate transaction logs.

It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, transaction logs on the VM guest OS may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs him-/herself.

- Select **Truncate logs older than <N> hours** or **Truncate logs over <N> GB** if you want Veeam Backup & Replication to truncate archived logs that are older than <N> hours or larger than <N> GB. The runtime process running on the VM guest OS will wait for the replication job to complete successfully and then trigger transaction logs truncation via Oracle Call Interface (OCI). If the job does not manage to replicate the Oracle VM, the logs will remain untouched on the VM guest OS until the next start of the runtime process.



VM Guest OS File Exclusion

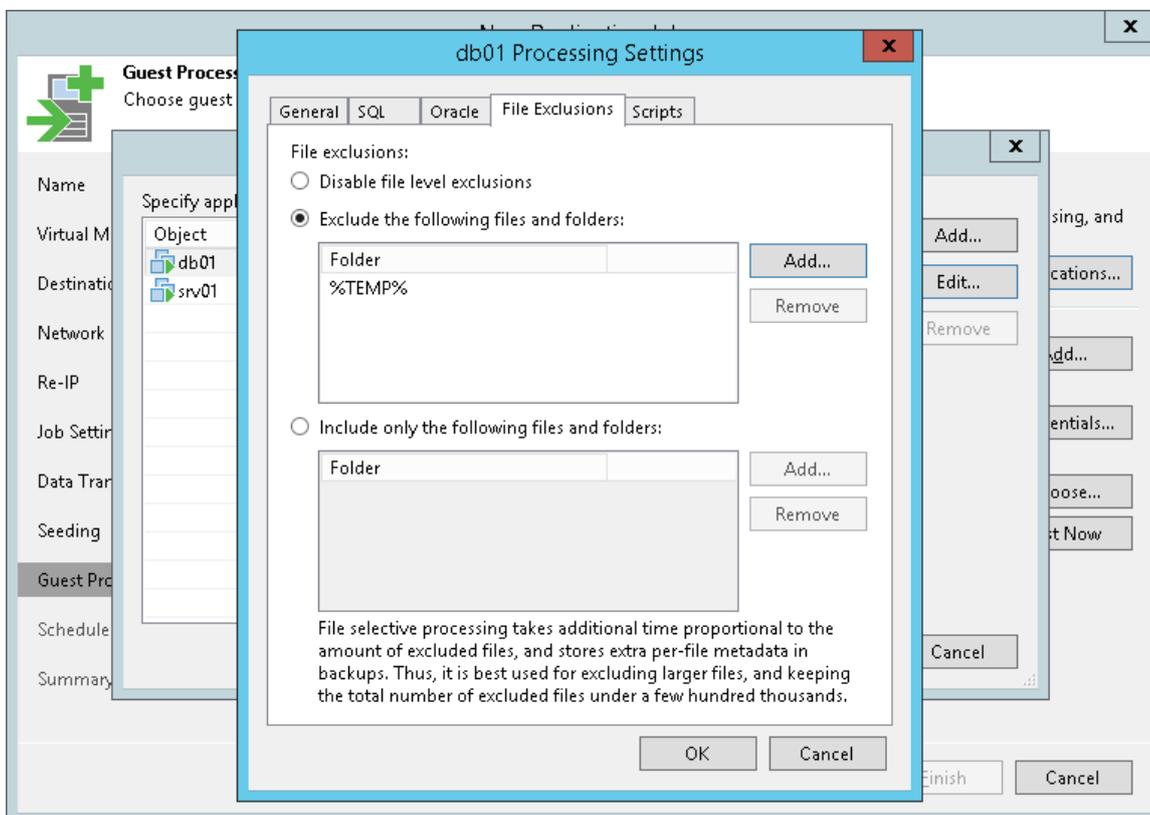
If you do not want to replicate specific files and folders on the VM guest OS Windows, you can exclude them from the VM replica.

To define what files and folders must be excluded:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the VM and click **Edit**.

To define custom settings for a VM added as part of a VM container, you must include the VM in the list as a standalone object. To do this, click **Add** and choose a VM whose settings you want to customize. Then select the VM in the list and define the necessary settings.

4. Click the **File Exclusions** tab and specify what files must be excluded from the VM replica:
 - Select **Exclude the following files and folders** to remove the individual files and folders from the VM replica.
 - Select **Include only the following files and folders** to leave only the specified files and folders in the VM replica.
5. Click **Add** and specify what files and folders you want to include or exclude. To form the list of exclusions or inclusions, you can use full paths to files and folders, environmental variables and file masks with the asterisk (*) and question mark (?) characters. For more information, see [VM Guest OS Files](#).
6. Click **OK**.
7. Repeat steps 5-6 for every object that you want to exclude or include.



Pre-Freeze and Post-Thaw Scripts

If you plan to replicate VMs running applications that do not support VSS, you can instruct Veeam Backup & Replication to run custom pre-freeze and post-thaw scripts for these VMs. The pre-freeze script quiesces the VM file system and application data to bring the VM to a consistent state before Veeam Backup & Replication triggers a VM snapshot. After the VM snapshot is created, the post-thaw script brings the VM and applications to their initial state.

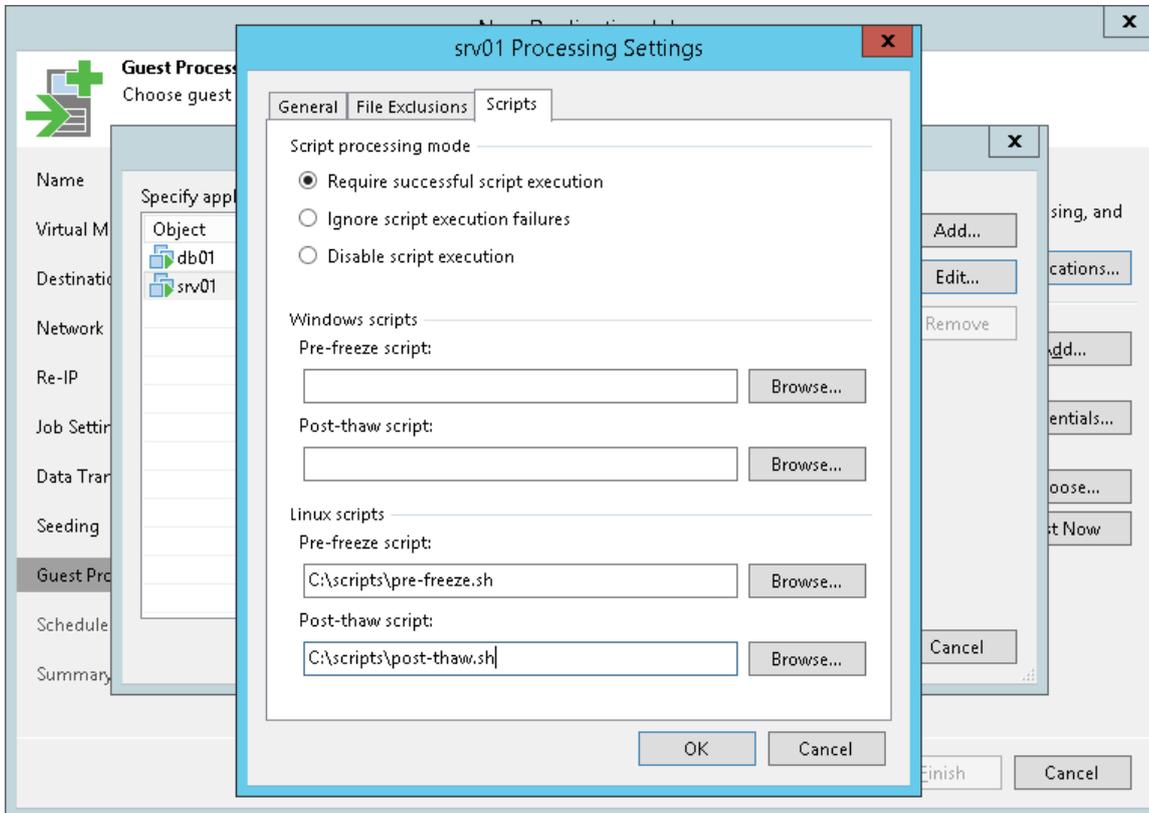
To specify pre-freeze and post-thaw scripts for the job:

1. At the **Guest Processing** step, click **Applications**.
2. In the displayed list, select the VM and click **Edit**.
3. Click the **Scripts** tab.
4. In the **Script processing mode** section, specify the scenario for scripts execution:
 - Select **Require successful script execution** if you want Veeam Backup & Replication to stop the replication process if the script fails.
 - Select **Ignore script execution failures** if you want to continue the replication process even if script errors occur.
 - Select **Disable script execution** if you do not want to run scripts for the VM.
5. In the **Windows scripts** section, specify paths to pre-freeze and post-thaw scripts for Microsoft Windows VMs. Veeam Backup & Replication supports scripts in the EXE, BAT and CMD format.
6. In the **Linux scripts** section, specify paths to pre-freeze and/or post-thaw scripts for Linux VMs. Veeam Backup & Replication supports scripts of the SH file type.

If you have added to the job a VM container with Microsoft Windows and Linux VMs, you can select to execute both Microsoft Windows and Linux scripts for the VM container. When the job starts, Veeam Backup & Replication will automatically determine what OS type is installed on the VM and apply corresponding scripts to quiesce this VM.

TIP:

Beside pre-freeze and post-thaw scripts for VM quiescence, you can instruct Veeam Backup & Replication to run custom scripts before the job starts and after the job completes. For more information, see [Advanced Settings](#).



Step 15. Define Job Schedule

At the **Schedule** step of the wizard, select to run the replication 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 perform VM replication.
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.

A repeatedly run job is started by the following rules:

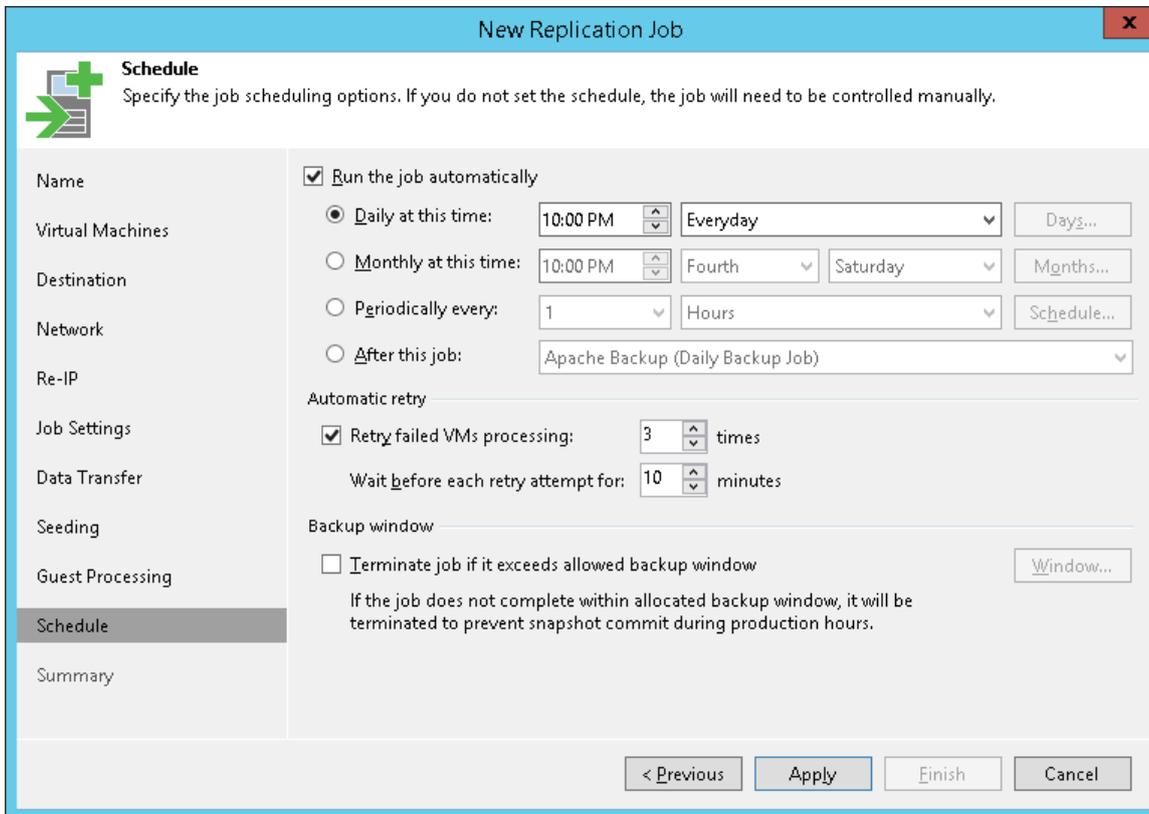
- Veeam Backup & Replication always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
- If you define permitted hours for the job, after the denied interval is over, Veeam Backup & Replication 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, select the **After this job option** and choose the preceding job from the list.
3. In the **Automatic retry** section, define whether Veeam Backup & Replication should attempt to run the job again if the job fails for some reason. During a job retry, Veeam Backup & Replication processes failed VMs only. Enter the number of attempts to run the job and define time spans between them. If you select continuous schedule for the job, Veeam Backup & Replication will retry the job for the defined number of times without any time intervals between the job sessions.
 4. In the **Backup window** section, determine a time interval within which the job must be completed. The backup window prevents the job from overlapping with production hours and ensures it does not provide unwanted overhead on your production environment. To set up a backup window for the job:
 - a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.
 - b. In the **Time Periods** section, define the allowed hours and prohibited hours for VM replication. If the job exceeds the allowed window, it will be automatically terminated.

NOTE:

The **After this job** function will only start a job if the first job in the chain is started automatically by schedule. If the first job is started manually, jobs chained to it will not be started.



The screenshot shows the 'New Replication Job' wizard, specifically the 'Schedule' step. The window title is 'New Replication Job' and it has a close button (X) in the top right corner. The 'Schedule' step is highlighted in the left-hand navigation pane. The main area contains the following options:

- Run the job automatically**
 - Daily at this time:** 10:00 PM, Everyday, Days...
 - Monthly at this time:** 10:00 PM, Fourth, Saturday, Months...
 - Periodically every:** 1, Hours, Schedule...
 - After this job:** Apache Backup (Daily Backup Job)
- Automatic retry**
 - Retry failed VMs processing:** 3 times
 - Wait before each retry attempt for: 10 minutes
- Backup window**
 - Terminate job if it exceeds allowed backup window** Window...
 - If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

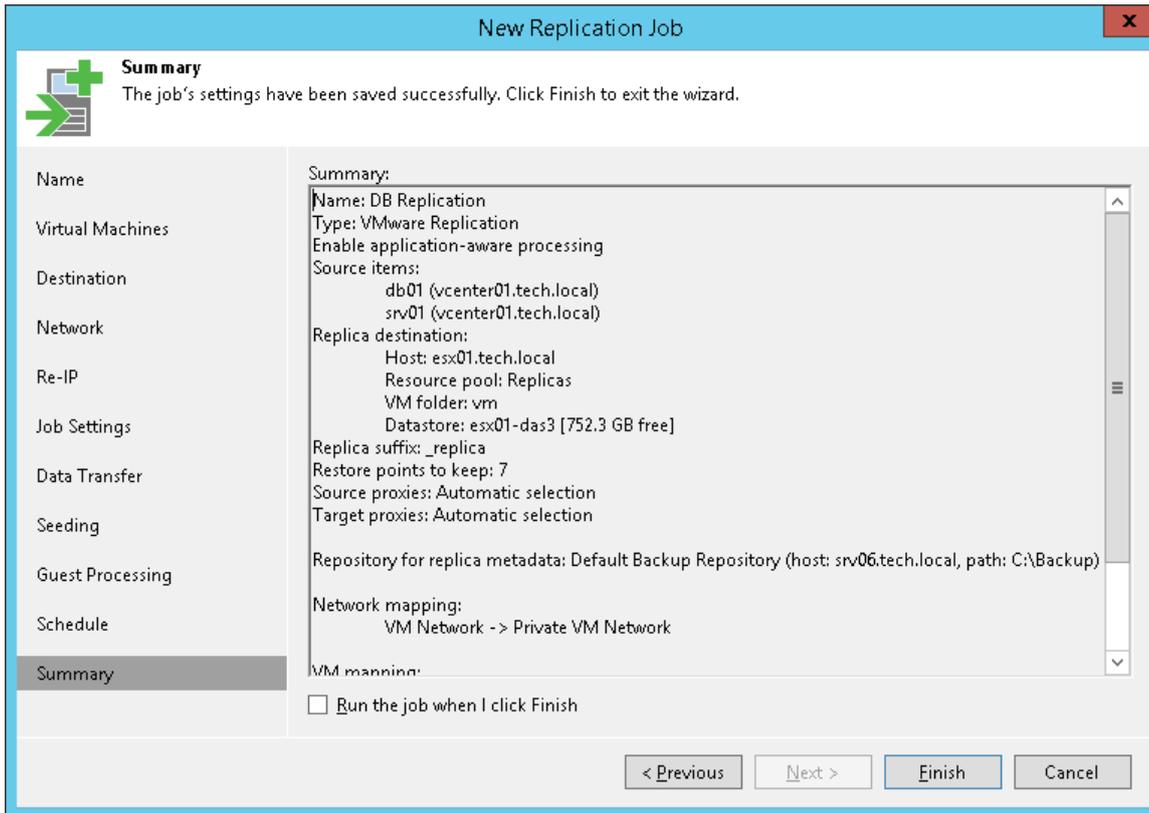
At the bottom of the window, there are four buttons: '< Previous', 'Apply', 'Finish', and 'Cancel'.

Step 16. Finish Working with Wizard

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

1. Review details of the replication 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 Replicas

You can perform the following operations with replicas:

- [View replica properties](#)
- [Remove a replica from configuration](#)
- [Delete a replica from disks](#)

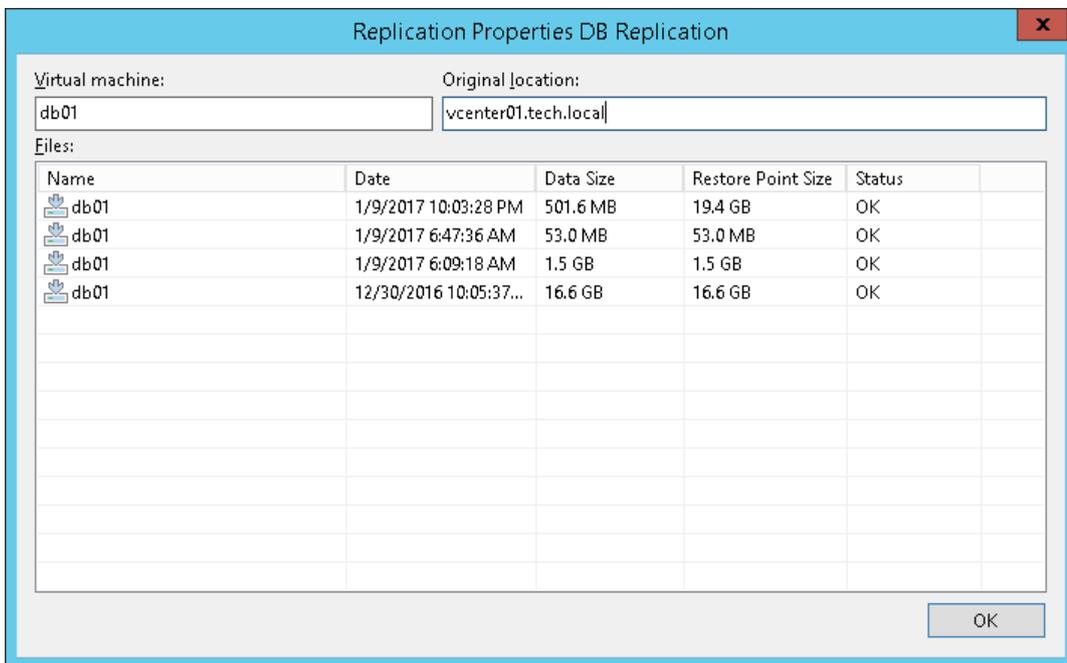
Viewing Replica Properties

You can view summary information about created replicas. The summary information provides the following data:

- Available restore points
- Date of restore points creation
- Data size and replica status

To view summary information for replicas:

1. Open the **Home** view.
2. In the inventory pane, select **Replicas**.
3. In the working area, right-click the replica and select **Properties**.



Removing from Configuration

If you want to remove records about replicas from the Veeam Backup & Replication console and configuration database, you can use the **Remove from configuration** operation.

Replicated VMs remain on target hosts. If necessary, you can start them manually after the **Remove from configuration** operation is performed.

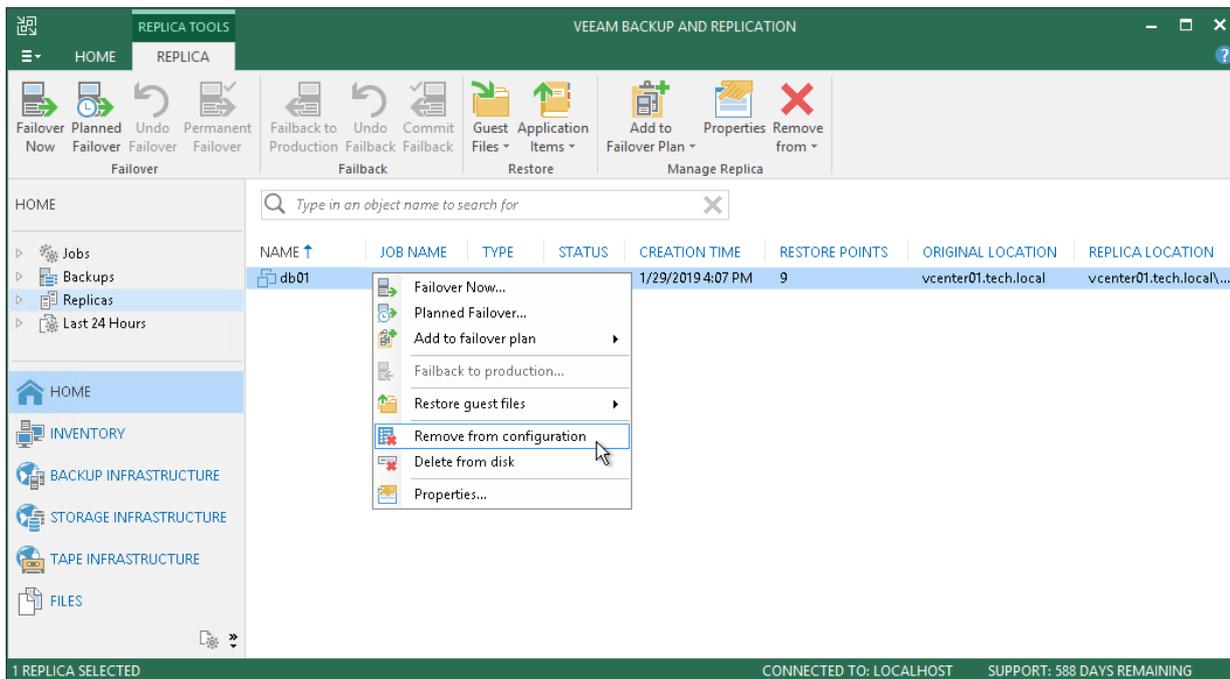
Mind the following:

- The **Remove from configuration** operation can be performed only for VM replicas in the *Ready* state. If the VM replica is in the *Failover* or *Failback* state, this option is disabled.

When you perform the **Remove from configuration** operation for a VM that is replicated as a standalone object, Veeam Backup & Replication removes this VM from the initial replication job. When you perform the **Remove from configuration** operation for a VM that is replicated as part of a VM container, Veeam Backup & Replication adds this VM to the list of exclusions in the initial replication job. For more information, see [Step 5. Exclude Objects from Replication Job](#).

To remove records about VM replicas from the Veeam Backup & Replication console and configuration database:

1. Open the **Home** view.
2. In the inventory pane, select **Replicas**.
3. In the working area, select the replica and click **Remove from > Configuration** on the ribbon. You can also right-click the replica and select **Remove from configuration**.



Deleting from Disk

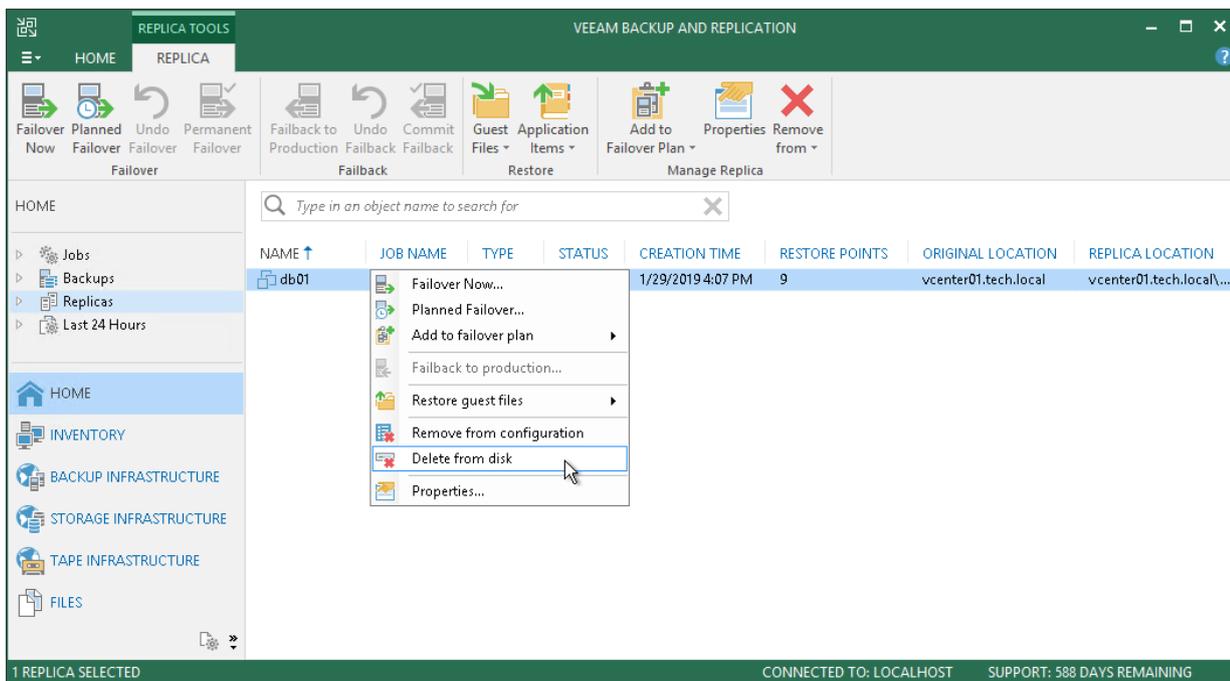
If you want to delete records about replicas from the Veeam Backup & Replication console and configuration database and, additionally, delete replica files from the destination storage, you can use the **Delete from disk** operation.

Mind the following:

- Do not delete replica files from the destination storage manually. Use the **Delete from disk** option instead. If you delete replica files manually, subsequent replication job sessions will fail.
- The **Delete from disk** operation can be performed only for VM replicas in the *Ready* state. If the VM replica is in the *Failover* or *Failback* state, this option is disabled.

To delete replica files from disk:

1. Open the **Home** view.
2. In the inventory pane, select **Replicas**.
3. In the working area, select the VM replica and click **Remove from > Disk** on the ribbon. You can also right-click the VM replica and select **Delete from disk**.



Replica Failover and Failback

In case of software or hardware malfunction, you can quickly recover a corrupted VM by failing over to its replica. When you perform failover, a replicated VM takes over the role of the original VM. You can fail over to the latest state of a replica or to any of its good known restore points.

In Veeam Backup & Replication, failover is a temporary intermediate step that should be further finalized. Veeam Backup & Replication offers the following options for different disaster recovery scenarios:

- You can perform permanent failover to leave the workload on the target host and let the replica VM act as the original VM. Permanent failover is suitable if the source and target hosts are nearly equal in terms of resources and are located on the same HA site.
- You can perform failback to recover the original VM on the source host or in a new location. Failback is used in case you failed over to a DR site that is not intended for continuous operations and would like to move the operations back to the production site when the consequences of a disaster are eliminated.

Veeam Backup & Replication supports failover and failback operations for one VM and for several VMs. In case one or several hosts fail, you can use batch processing to restore operations with minimum downtime.

Replica Failover

Failover is a process of switching from the original VM on the source host to its VM replica on the target host.

During failover, Veeam Backup & Replication recovers a fully functional VM to the required restore point on the target host. As a result, you have a VM up and running within a couple of seconds, and your users can access services and applications they need with minimum disruption.

When you perform failover, the state of the original VM on the source host is not affected in any way. If you need to test the VM replica and its restore points for recoverability, you can perform failover while the original VM is running. After all necessary tests, you can undo failover and get back to the normal mode of operation.

NOTE:

If the original VM and VM replica are located in the same network and you plan to perform replica failover while the original VM is running, consider temporarily disconnecting the original VM from the network to avoid IP addresses and/or machine names conflicts.

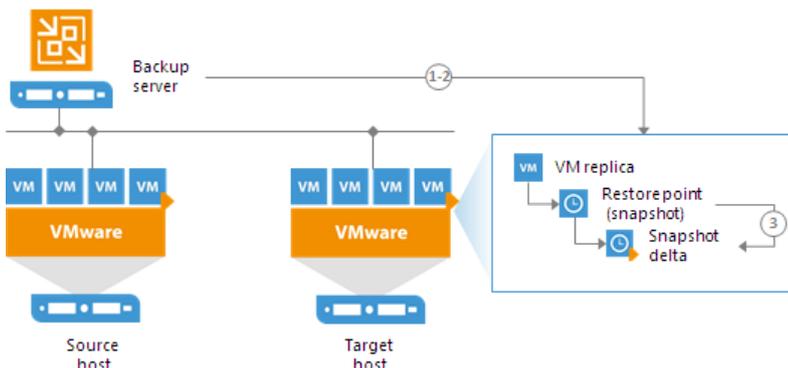
It is recommended that you always use Veeam Backup & Replication to perform failover operations. Avoid powering on a replica manually – this may disrupt further replication operations or cause loss of important data.

The failover operation is performed in the following way:

1. Veeam Backup & Replication rolls back the VM replica to the required restore point. To do this, it reverts the VM replica to the necessary snapshot in the replica chain.
2. Veeam Backup & Replication powers on the VM replica. The state of the VM replica is changed from *Normal* to *Failover*. If you perform failover for testing or DR simulation purposes, and the original VM still exists and is running, the original VM remains powered on.

Note that any replication activities for the original VM will fail until the VM replica is returned to the *Normal* state.

3. All changes made to the VM replica while it is running in the *Failover* state are written to the delta file of the snapshot, or restore point, to which you have selected to roll back.



In Veeam Backup & Replication, the actual failover is considered a temporary stage that should be further finalized. While the replica is in the *Failover* state, you can undo failover, perform failback or perform permanent failover. In a disaster recovery scenario, after you test the VM replica and make sure the VM runs stable, you should take another step to perform permanent failover.

Performing Failover

If a VM becomes unavailable or fails in case of a disaster, you can fail over to a VM replica and quickly restore services in the production environment. When you perform failover, the VM replica takes over the role of the original VM. As a result, you have your VM up and running within a couple of minutes, and your users can access services and applications they need with minimal disruption.

Before performing failover, [check prerequisites](#). Then use the **VMware Failover** wizard to fail over the VM replica.

Before You Begin

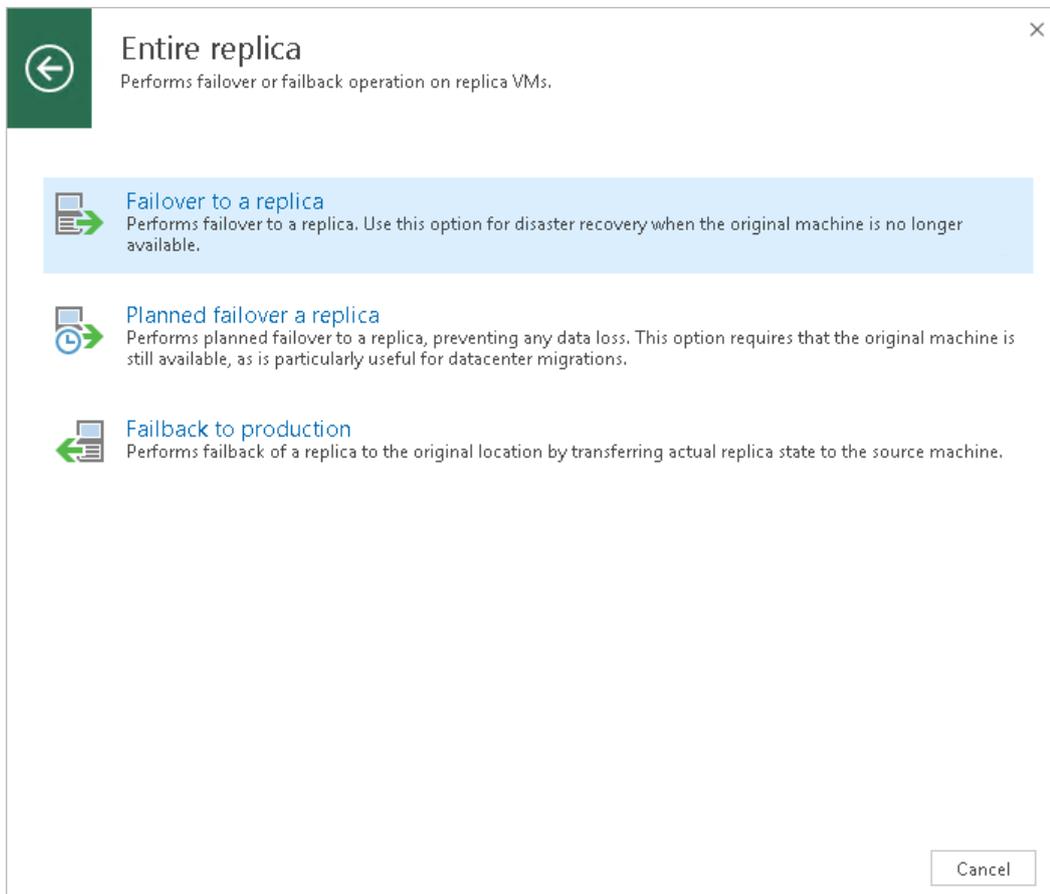
Before you fail over to a VM replica, check the following prerequisites:

- The failover operation can be performed for VMs that have been successfully replicated at least once.
- VM replicas must be in the *Ready* state.

Step 1. Launch Failover Wizard

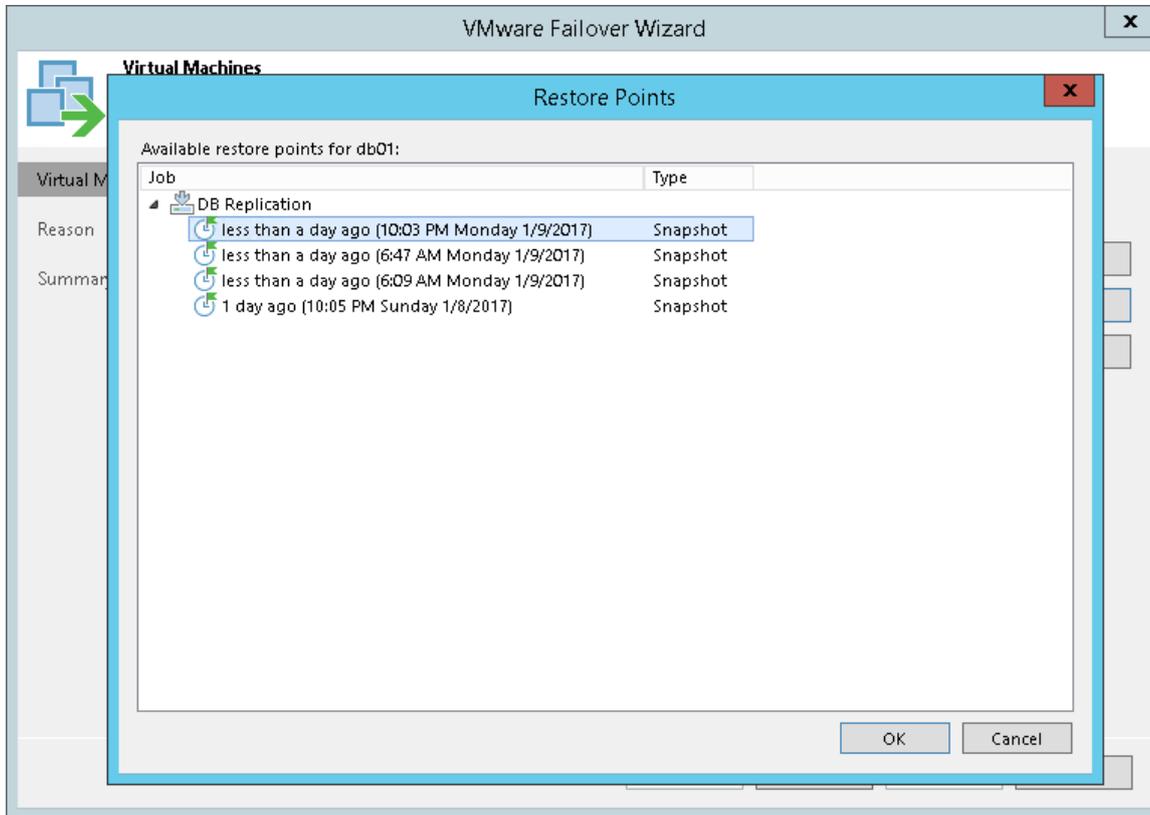
To launch the **Failover** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from replica > Entire replica > Failover to a replica**.
- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, select the necessary replica and click **Failover Now** on the ribbon.
- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary replica and select **Failover Now**.



To select a restore point for a VM:

1. In the **Virtual machines to failover** list, select a VM.
2. Click **Point** on the right.
3. In the **Restore Points** window, select a restore point that must be used.

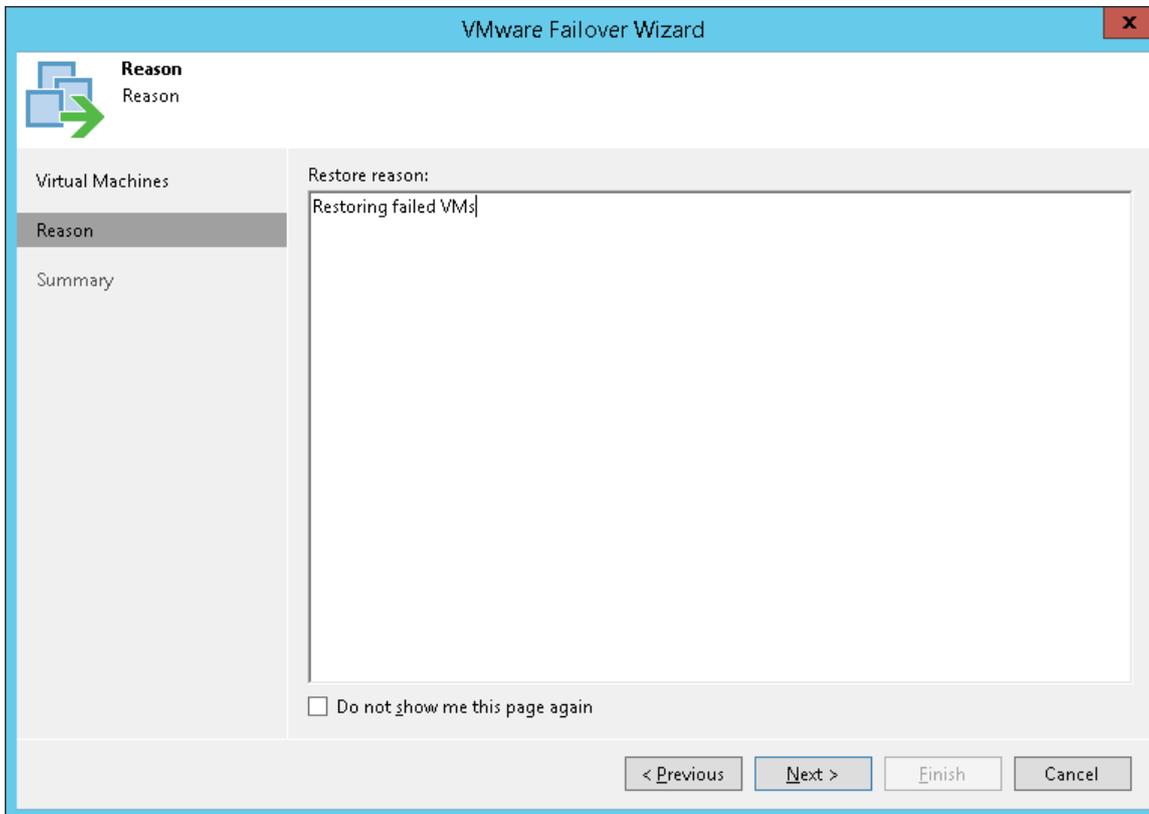


Step 4. Specify Failover Reason

At the **Reason** step of the wizard, enter a reason for failing over to the VM replicas. 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.

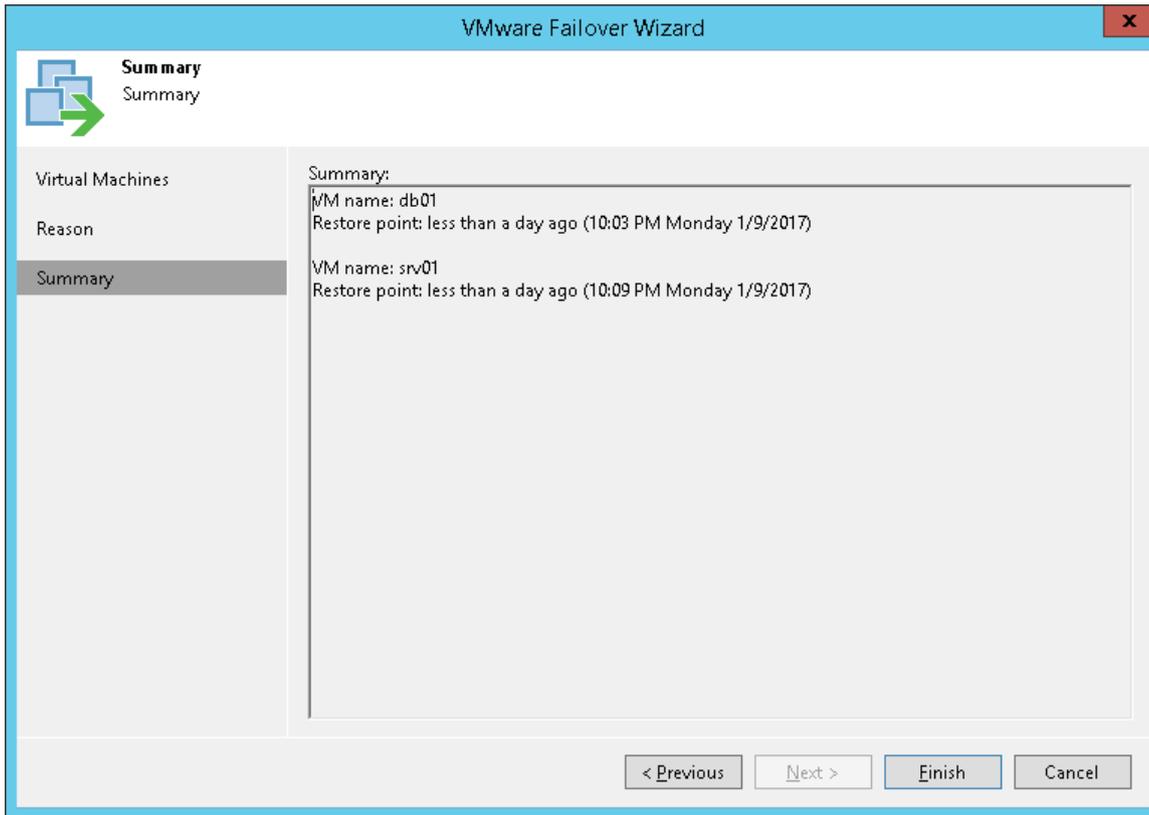


Step 5. Review Summary and Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of failover.

1. Review details of the failover task.
2. Click **Finish** to start the failover process.

When the failover process is complete, the VM replicas will be started on the target hosts.



Permanent Failover

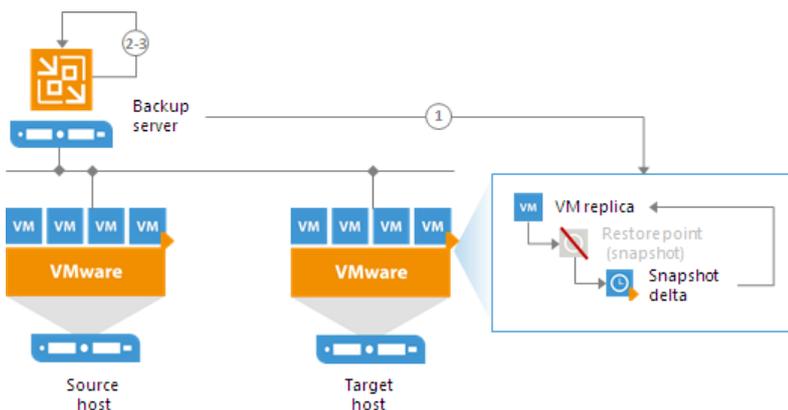
To finalize the failover process, you can permanently fail over to the VM replica.

When you perform permanent failover, you "commit" failover. You can perform this operation if you want to permanently switch from the original VM to a VM replica and use this replica as the original VM. As a result of permanent failover, the VM replica ceases to exist as a replica and takes on the role of the original VM.

The permanent failover scenario is acceptable if the original VM and VM replica are located in the same site and are nearly equal in terms of resources. In this case, users will not experience any latency in ongoing operations.

The permanent failover operation is performed in the following way:

1. Veeam Backup & Replication removes snapshots (restore points) of the VM replica from the snapshot chain and deletes associated files from the datastore. Changes that were written to the snapshot delta file are committed to the VM replica disk files to bring the VM replica to the most recent state.
2. Veeam Backup & Replication removes the VM replica from the list of replicas in the Veeam Backup & Replication console.
3. To protect the VM replica from corruption after permanent failover is complete, Veeam Backup & Replication reconfigures the replication job and adds the original VM to the list of exclusions. When the replication job starts, the original VM is skipped from processing. As a result, no data is written to the working VM replica.



Performing Permanent Failover

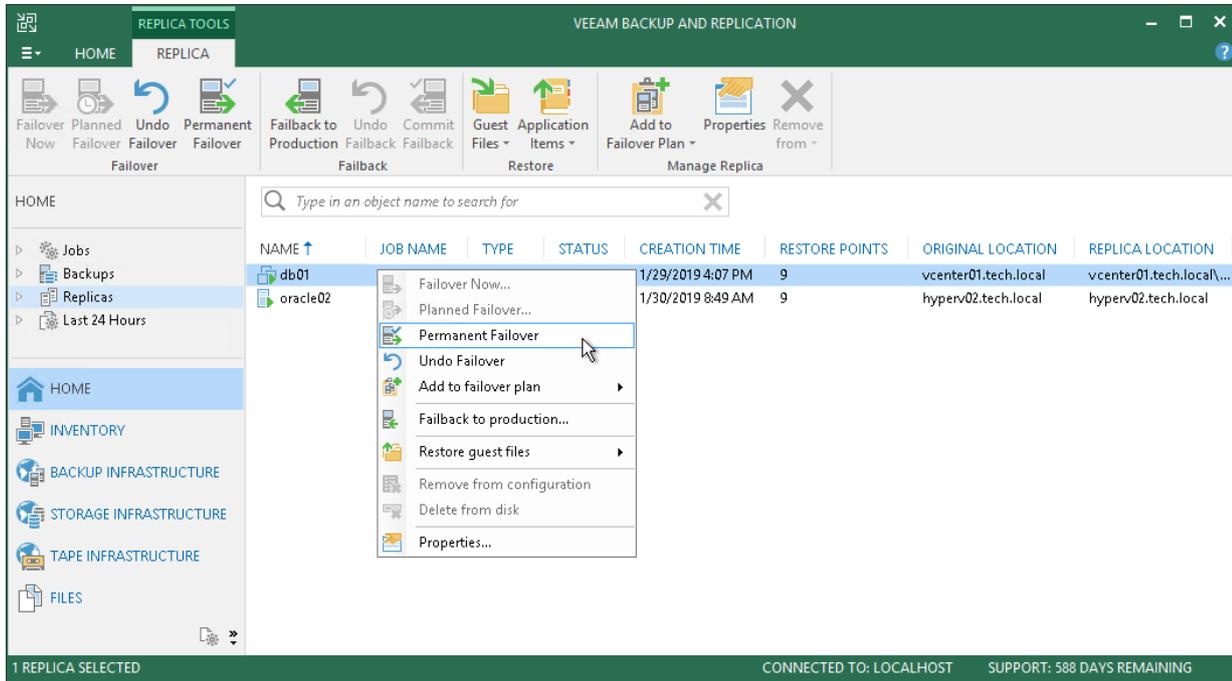
With permanent failover, you can finalize failover to a VM replica. As a result of permanent failover, the VM replica on the target host ceases to exist as a replica and takes on the role of the original VM.

To perform permanent failover, do either of the following:

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, select the necessary replica and click **Permanent Failover** on the ribbon.
- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary replica and select **Permanent Failover**.

In the displayed window, click **Yes** to confirm the operation.

To protect the VM replica from corruption after performing a permanent failover, Veeam Backup & Replication removes the VM replica from the **Replicas** list. Additionally, Veeam Backup & Replication reconfigures the replication job and adds the original VM to the list of exclusions. When the replication job that processes the original VM starts, the VM will be skipped from processing, and no data will be written to the working VM replica.



Failover Plan

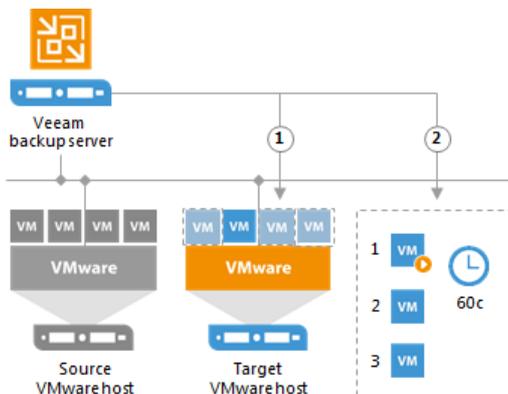
If you have a number of VMs running interdependent applications, you need to failover them one by one, as a group. To do this automatically, you can prepare a failover plan.

In a failover plan, you set the order in which VMs must be processed and time delays for VMs. The time delay is an interval of time for which Veeam Backup & Replication must wait before starting the failover operation for the next VM in the list. It helps to ensure that some VMs, such as a DNS server, are already running at the time the dependent VMs start. The time delay is set for every VM in the failover plan except the last VM in the list.

The failover plan must be created in advance. In case the primary VM group goes offline, you can start the corresponding failover plan manually. When you start the procedure, you can choose to fail over to the latest state or select the point in time to which VM replicas must be started. Veeam Backup & Replication will look for the closest restore points to this point in time and use them to start VM replicas.

The failover process is performed in the following way:

1. For each VM, Veeam Backup & Replication detects its replica. The VMs whose replicas are already in *Failover* or *Failback* state are skipped from processing.
2. The replica VMs are started in the order they appear in the failover plan within the set time intervals.



Limitations for Failover Plans

The maximum number of VMs that can be started simultaneously when you run a failover plan is 10. If you have added more VMs to the failover plan and scheduled them to start simultaneously, Veeam Backup & Replication will wait for the first VMs in the list to fail over and then start the failover operation for subsequent VMs. This limitation helps reduce the workload on the production infrastructure and backup server.

For example, if you have added 14 VMs to the failover plan and scheduled them to start at the same time, Veeam Backup & Replication will start the failover operation for the first 10 VMs in the list. After the 1st VM is processed, Veeam Backup & Replication will start the failover operation for the 11th VM in the list, then for the 12th VM and so on.

Finalizing Failover Plans

Failover is a temporary intermediate step that needs to be finalized. The finalizing options for a group failover are similar to a regular failover: undoing failover, permanent failover or failback.

If you decide to commit failover or failback, you need to process every VM individually. Although you can undo failover for the whole group using the undo failover plan option.

Undoing the failover switches the replica back to the primary VM discarding all changes that were made to the replica while it was running. When you undo group failover, Veeam Backup & Replication uses the list of VMs that were failed over during the last failover plan session and switches them back to the primary VMs. If some of the VMs were already failed back, for example manually by the user, they are skipped from processing.

Veeam Backup & Replication starts the undo failover operation for a group of 5 VMs at the same time. The time interval between the operation starts is 10 seconds. For example, if you have added 10 VMs to the failover plan, Veeam Backup & Replication will undo failover for the first 5 VMs in the list, then will wait for 10 seconds and undo failover for the remaining 5 VMs in the list. Time intervals between the operation starts help Veeam Backup & Replication reduce the workload on the production environment and backup server.

Creating Failover Plans

If you have a number of VMs running dependent applications, you need to failover them one by one, as a group. To do this automatically, you can prepare a failover plan.

Before creating a failover plan, [check prerequisites](#). Then use the **New Failover Plan** wizard to create a failover plan.

Before You Begin

Before you create a failover plan, check the following prerequisites:

- VMs that you plan to include in the failover plan must be successfully replicated at least once.
- VM replicas must be in the *Ready* state.
- If you plan to use pre-failover and/or post-failover scripts for the failover plan, you must create scripts before you configure the failover plan.

Step 1. Launch New Failover Plan Wizard

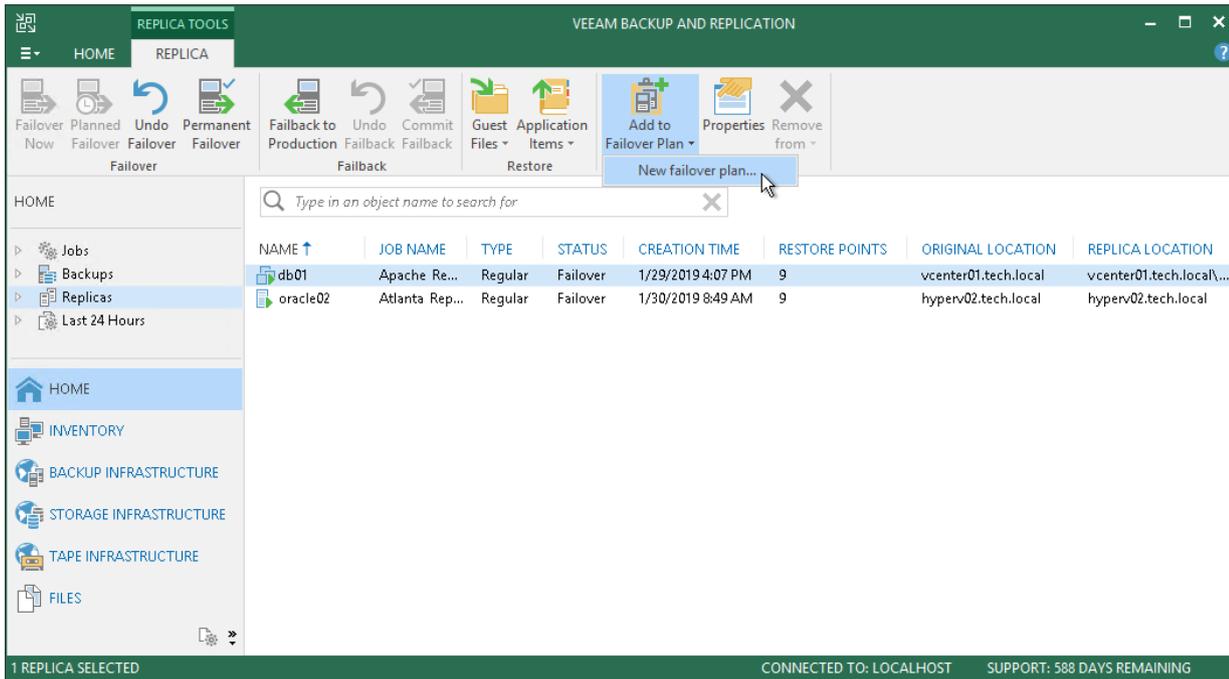
To launch the **New Failover Plan** wizard, do one of the following:

- On the **Home** tab, click **Failover Plan** and select **VMware vSphere**.
- Open the **Home** view, in the inventory pane select **Replicas**. In the working area select one or more VMs, click **Add to Failover Plan > New Failover Plan** on the ribbon or right-click one or more VMs and select **Add to failover plan > New Failover Plan**.

In this case, the VMs will be automatically added to the failover plan. You can add other VMs to the failover plan when passing through the wizard steps.

- Open the **Inventory** view, in the working area select one or more VMs, click **Add to Failover Plan > New Failover Plan** on the ribbon or right-click one or more VMs and select **Add to failover plan > New Failover Plan**.

In this case, the selected VMs will be automatically added to the failover plan. You can add other VMs to the failover plan when passing through the wizard steps.



Step 2. Specify Failover Plan Name and Description

At the **General** step of the wizard, specify a name and description for the failover plan and define script settings for the plan if necessary.

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

3. If you want to execute custom scripts before and/or after the failover plan, select the **Pre-failover script** and **Post-failover script** check boxes and click **Browse** to choose executable files. Veeam Backup & Replication supports script files in the following formats: BAT, CMD, EXE and PS1. For example, you may want stop some applications on production VMs before the failover plan starts or send an email to backup administrators after the failover plan finishes.

New Failover Plan

General
Type in name and description for this failover plan, and optionally specify scripts to trigger before and after the failover.

General
Virtual Machines
Summary

Name:
DB Failover Plan

Description:
Failover Plan for Microsoft SQL Servers

Pre-failover script:
C:\scripts\pre-failover.bat

Post-failover script:
C:\scripts\post-failover.bat

< Previous Next > Finish Cancel

Step 3. Select VMs

At the **Virtual Machines** step of the wizard, select VMs that you want to add to the failover plan. You can add separate VMs and whole VM containers.

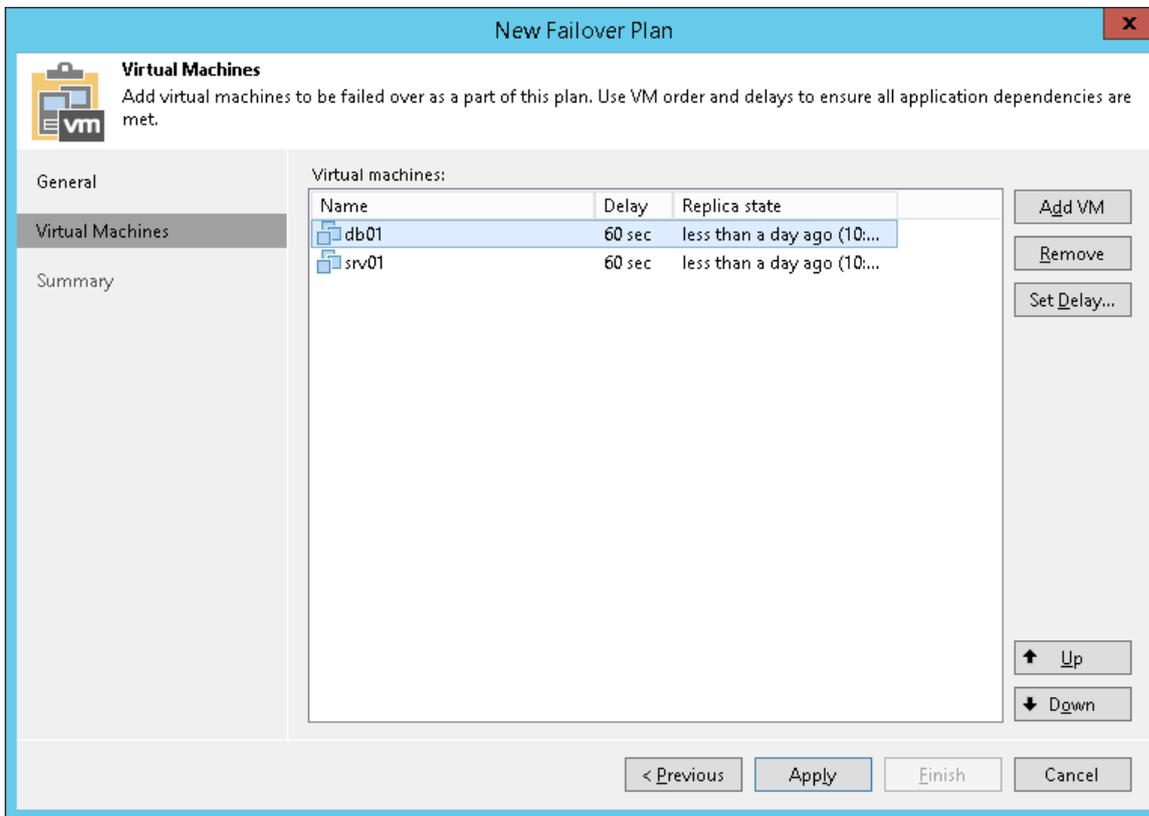
To add VMs and VM containers:

1. Click **Add VM**.
2. Select where to browse for VMs and VM containers:
 - **From infrastructure** – browse the virtual environment and select VMs or VM containers. If you choose a VM container, Veeam Backup & Replication will expand it to a plain VM list.
To quickly find VMs or VM containers, you can use the search field at the bottom of the **Add Object** window. Enter a VM or VM container name or a part of it in the search field and click **Start search** or press **[ENTER]**.
 - **From replicas** – browse existing replication jobs and select all VMs or specific VMs from replication jobs.
To quickly find VMs, you can use the search field at the bottom of the **Select Replica** window. Enter a VM name or a part of it in the search field and click **Start search** or press **[ENTER]**.

Make sure that VMs you select from the virtual environment have been successfully replicated at least once.

IMPORTANT!

A source from which you add a VM to a failover plan does not matter. When you run the failover plan, Veeam Backup & Replication always fails over to the latest restore point of VM replicas. To fail over to a specific restore point of VM replicas, use the **Start to** command. For more information, see [Running Failover Plans](#).

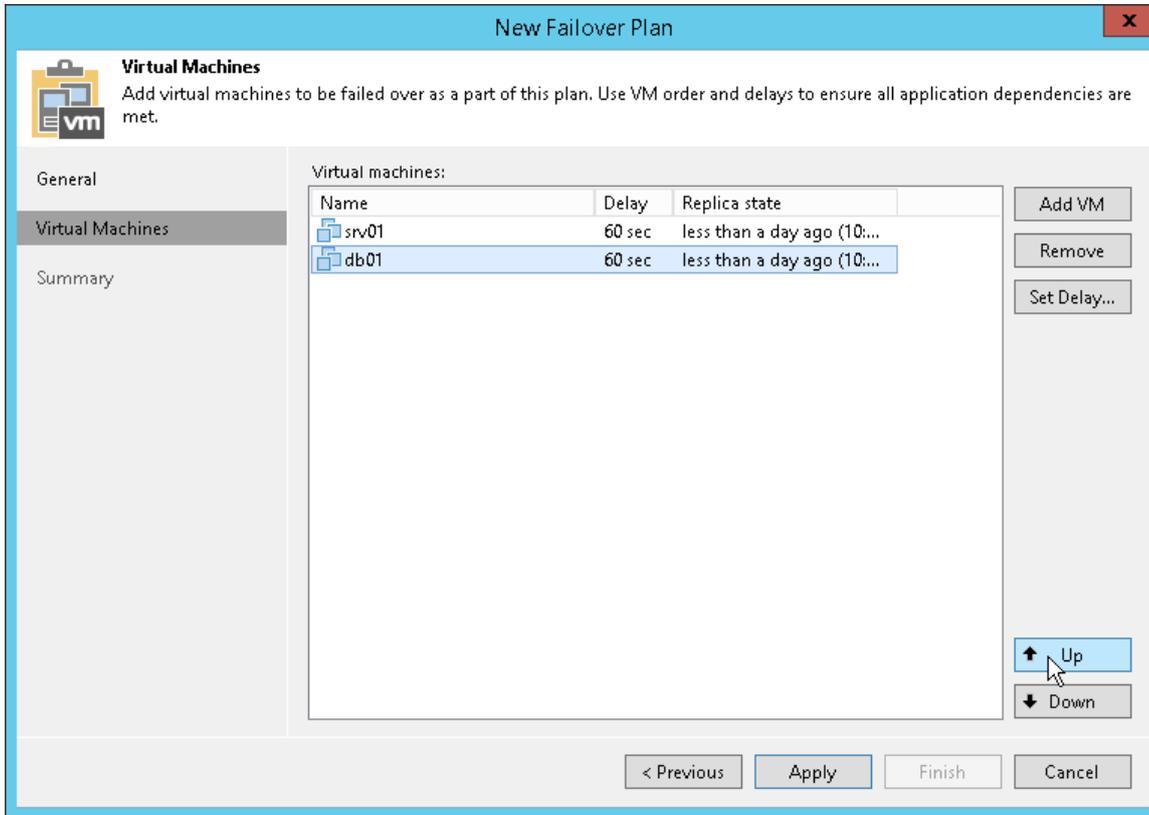


Step 4. Define VM Failover Order

The VM replicas in the failover plan are started in the order they appear in the VM list. If some VMs provide environment for other dependent VMs, make sure that they are started first.

To set VM start order:

1. Select the VM in the list
2. Move the VM up or down the list using the **Up** and **Down** buttons on the right.



Step 5. Set Time Delay

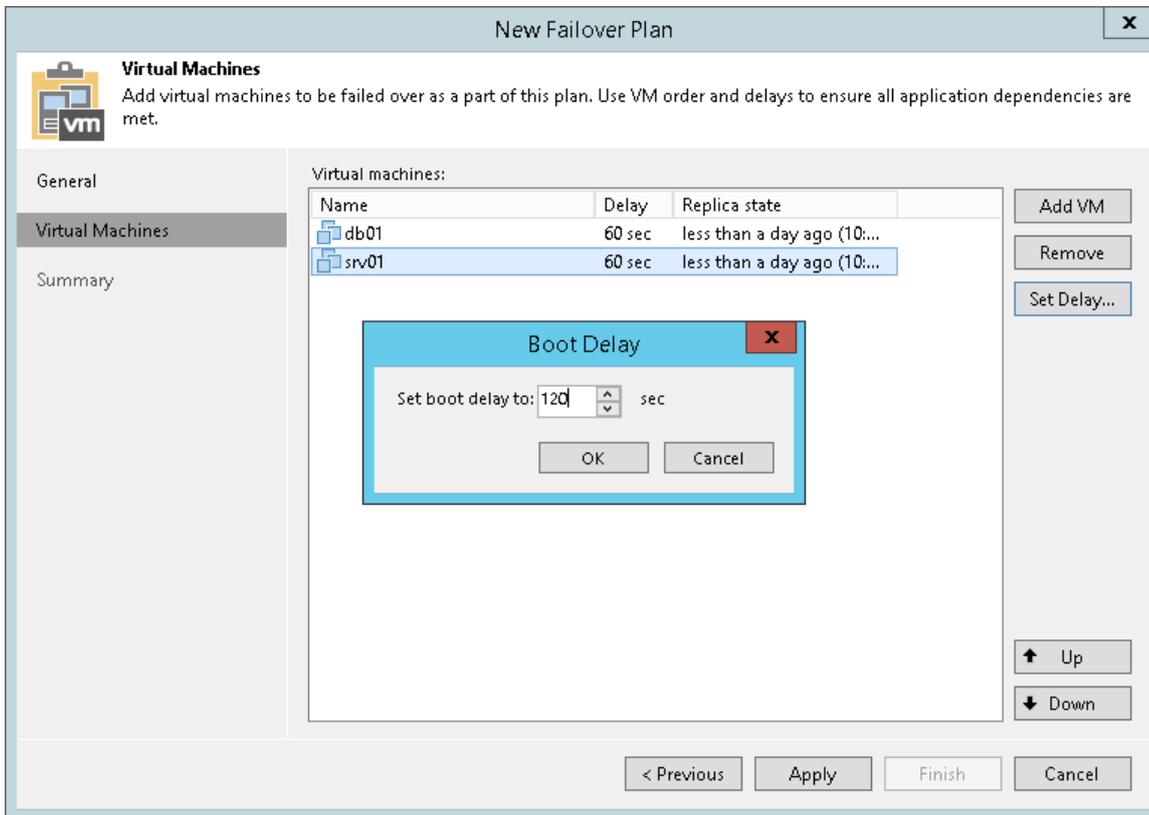
After you have set the order for VMs in the failover plan, you need to set a time delay for VMs. The delay time defines for how long Veeam Backup & Replication must wait before starting the failover operation for the next VM in the list. You can use time delays to make sure that some VMs are already running at the moment dependent VMs start.

Time delays can be specified for all VMs in the list except the last one. If you do not specify time delays, VMs will be started simultaneously.

For example, you have added 2 VMs to the failover plan and set a time delay to 60 seconds for the first VM in the list. Veeam Backup & Replication will perform failover in the following manner: Veeam Backup & Replication will start the failover operation for the first VM in the list, then wait for 60 seconds and start the failover operation for the second VM in the list.

To set the time delay for a VM:

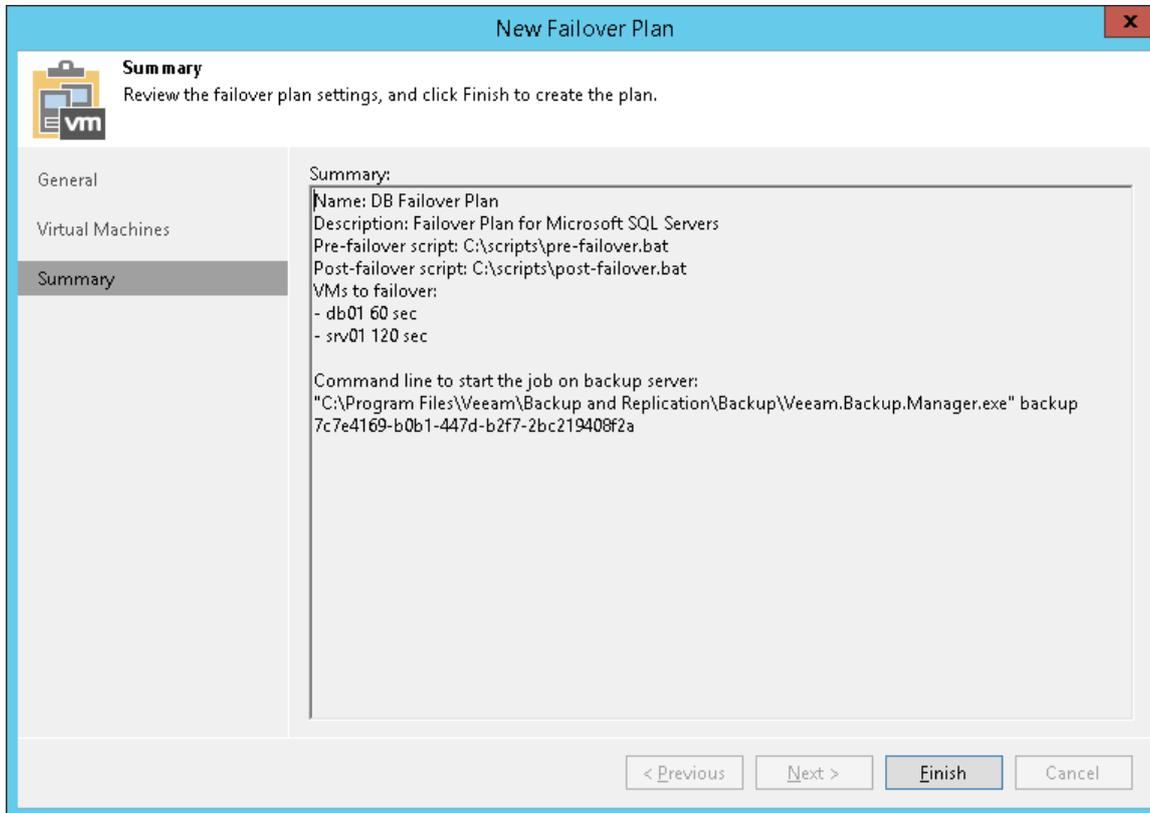
1. Select it and click **Set Delay** on the right or double-click the VM in the list.
2. Enter the time interval that you consider sufficient for this VM to boot.



Step 6. Review Summary and Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of the failover plan configuration.

1. Review details for the configured failover plan.
2. Click **Finish** to create the failover plan.



Running Failover Plans

You have the following options to run the failover plan:

- You can fail over to latest restore point of VM replicas. To use this option, you must run the failover plan with the **Start** command.

Veeam Backup & Replication searches for the latest restore point of VM replicas across all replication jobs configured on the backup server. For example, you have 2 jobs that replicate the same VM: *Job 1* has created the most recent point at 2:00 AM and *Job 2* has created the most recent restore point at 3:00 AM. When you run the failover plan using the **Start** command, Veeam Backup & Replication will pick the restore point created at 3:00 AM with *Job 2*.

- You can fail over to a specific restore point of VM replicas. To use this option, you must run the failover plan with the **Start to** command and select the necessary date when restore points for VM replicas were created.

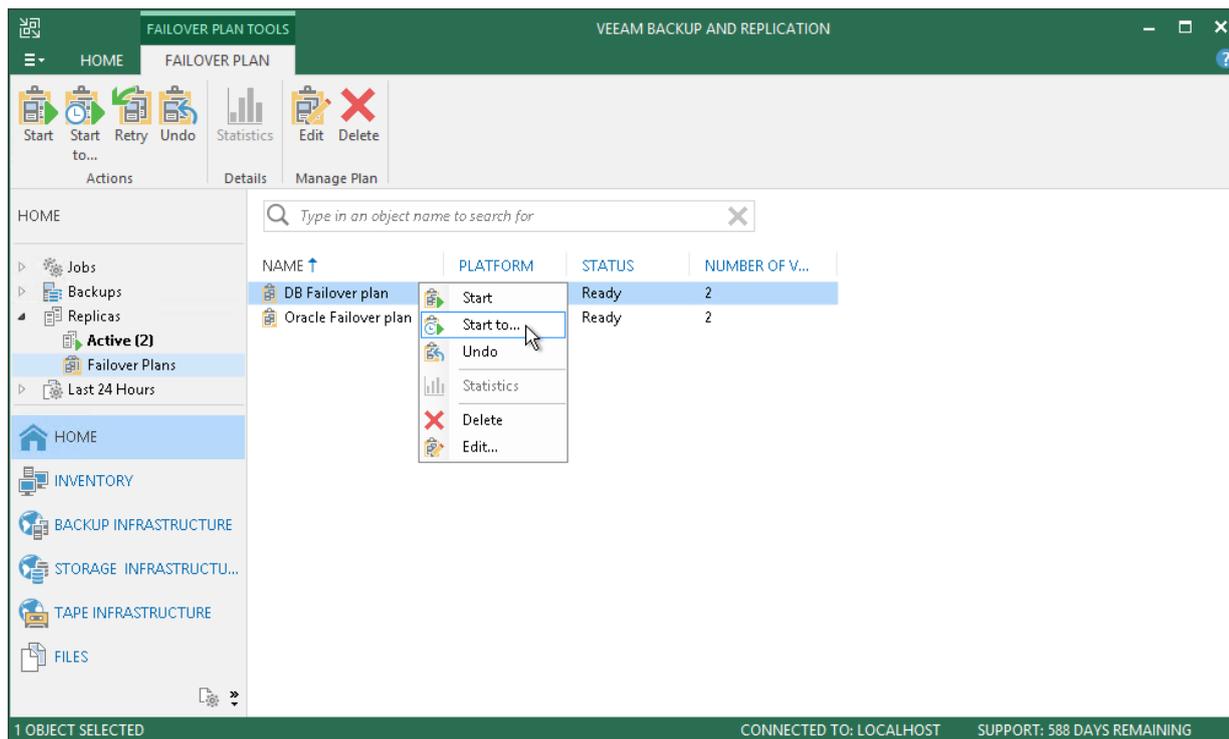
To fail over to the latest restore point of VM replicas:

1. Open the **Home** view.
2. Expand the **Replicas** node.
3. Select **Failover Plans**.

4. In the working area, right-click the failover plan and select **Start**.

To fail over to a specific restore point of VM replicas:

1. Open the **Home** view.
2. Expand the **Replicas** node.
3. Select **Failover Plans**.
4. In the working area, right-click the failover plan and select **Start to**.
5. In the displayed window, select the backup date and time. Veeam Backup & Replication will find the closest restore point prior to the entered value for each VM and fail over to it.



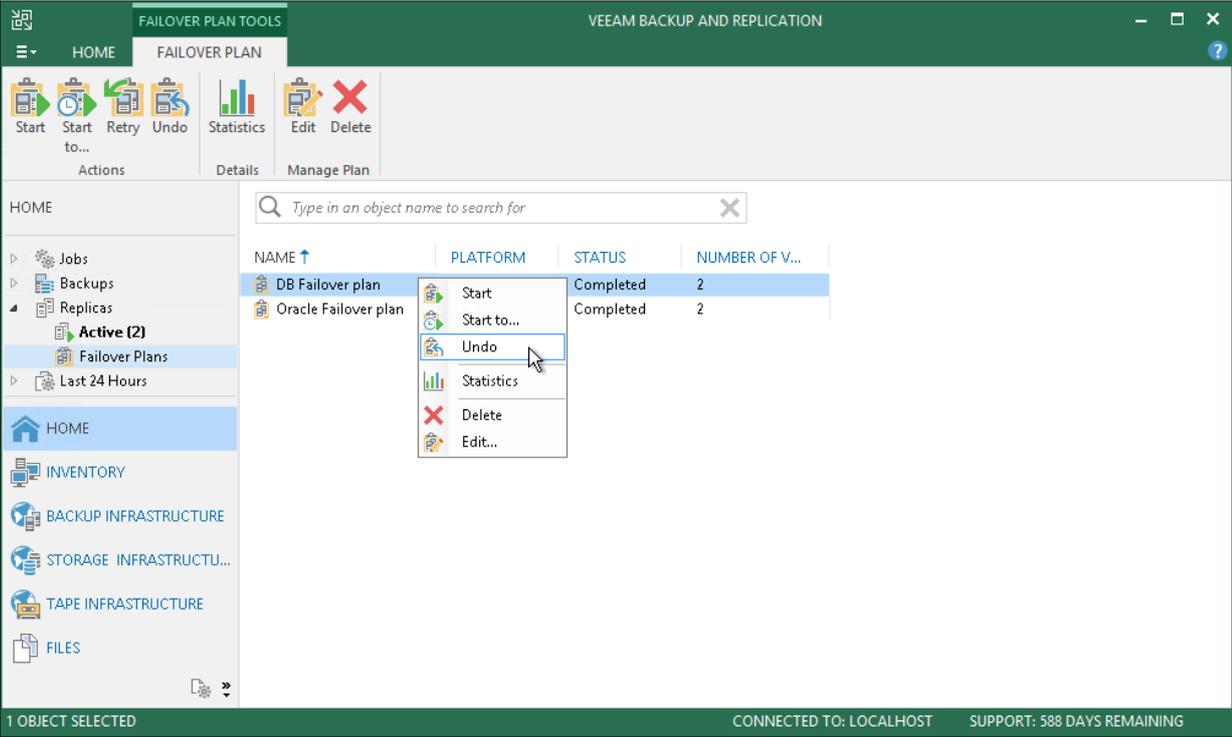
Undoing Failover by Failover Plans

You can undo failover for all VMs added to the failover plan at once. When you undo failover, you switch the workload back to original VMs and discard all changes that were made to VM replicas during failover.

To undo failover by a failover plan:

1. Open the **Home** view.
2. Expand the **Replicas** node.
3. Select **Failover Plans**.
4. In the working area, right-click the failover plan and select **Undo**.

5. In the displayed dialog box, click **Yes** to confirm the operation.

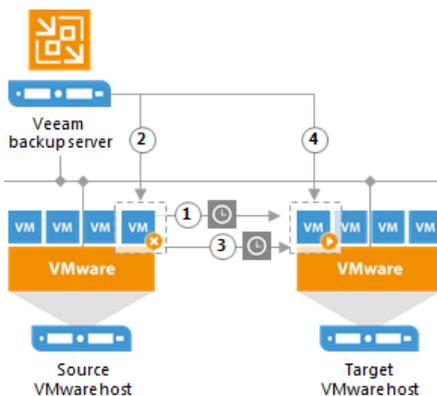


Planned Failover

If you know that your primary VMs are about to go offline, you can proactively switch the workload to their replicas. A planned failover is smooth manual switching from a primary VM to its replica with minimum interrupting in operation. You can use the planned failover, for example, if you plan to perform datacenter migration, maintenance or software upgrade of the primary VMs. You can also perform planned failover if you have an advance notice of a disaster approaching that will require taking the primary servers offline.

When you start the planned failover, Veeam Backup & Replication performs the following steps:

1. The failover process triggers the replication job to perform an incremental replication run and copy the un-replicated changes to the replica.
2. The VM is powered off.
3. The failover process triggers the replication job to perform another incremental replication run and copy the portion of last-minute changes to the replica. The replica becomes fully synchronized with the source VM.
4. The VM is failed over to its replica.
5. The VM replica is powered on.



As the procedure is designed to transfer the current workload to the replica, it does not suggest selecting a restore point to switch.

During the planned failover, Veeam Backup & Replication creates 2 helper restore points that are not deleted afterwards. These restore points will appear in the list of restore points for this VM; you can use them later to roll back to the necessary VM replica state.

When your primary host is online again, you can switch back to it. The finalizing options for a planned failover are similar to those of an unplanned failover: undoing failover, permanent failover or failback.

NOTE:

During planned failover, Veeam Backup & Replication always retrieves VM data from the production infrastructure, even if the replication job uses the backup as a data source. This approach helps Veeam Backup & Replication synchronize the VM replica to the latest state of the production VM.

Limitations for Planned Failover

Planned failover has the following limitations:

- If you start planned failover for several VMs that are replicated with one replication job, these VMs will be processed one by one, not in parallel.
- Each planned failover task for each VM is processed as a separate replica job session. If a backup proxy is not available and the session has to wait for resources, job sessions for other VMs in the same task cannot be started before the current session is finished.
- The user account under which you launch the planned failover operation must have the *Veeam Backup Administrator* role or *Veeam Backup Operator* and *Veeam Restore Operator* roles in Veeam Backup & Replication. For more information, see [Roles and Users](#).

Performing Planned Failover

Planned failover is the operation of switching from a running VM to its replica. Planned failover is performed to transfer the workload to the replica in advance in case the original VM is scheduled to go offline for some time.

Before performing planned failover, [check prerequisites](#). Then use the **Planned Failover** wizard to perform planned failover.

Before You Begin

Before you perform planned failover, check the following prerequisites:

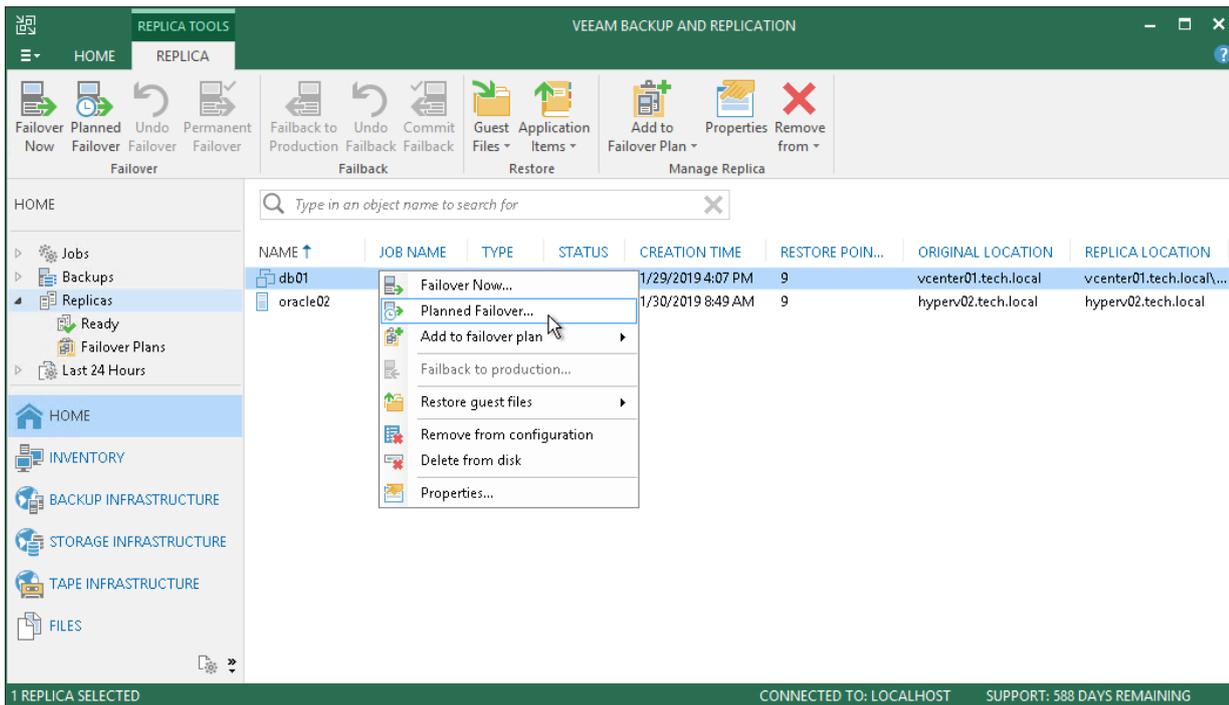
- VMs for which you plan to perform planned failover must be successfully replicated at least once.
- VM replicas must be in the *Ready* state.

Step 1. Launch Planned Failover Wizard

To launch the **Planned Failover** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware vSphere > Restore from replica > Entire replica > Planned failover a replica**.
- Open the **Home** view, expand the **Replicas** node. In the working area, select one or more VMs and click **Planned Failover** on the ribbon. You can also right-click one or more VMs and select **Planned Failover**.
- Open the **Inventory** view, in the working right-click one or more VMs area and select **Restore > Planned Failover**.

In this case, the selected VMs will be automatically included into the planned failover task. You can add other VMs to the task when passing through the wizard steps.



Step 2. Select VMs

At the **Virtual Machines** step of the wizard, select one or more VMs for which you want to perform failover. You can perform failover for separate VMs and whole VM containers.

To select VMs and VM containers:

1. Click **Add VM**.
2. Select where to browse for VMs and VM containers:
 - **From infrastructure** – browse the virtual environment and select VMs or VM containers. If you choose a VM container, Veeam Backup & Replication will expand it to a plain VM list.
To quickly find VMs or VM containers, you can use the search field at the bottom of the **Add Object** window. Enter a VM or VM container name or a part of it in the search field and click **Start search** or press **[ENTER]**.
 - **From replicas** – browse existing replication jobs and select all VMs or specific VMs from replication jobs.
To quickly find VMs, you can use the search field at the bottom of the **Backup Browser** window. Enter a VM name or a part of it in the search field and click **Start search** or press **[ENTER]**.

You can also use the search field at the top of the wizard:

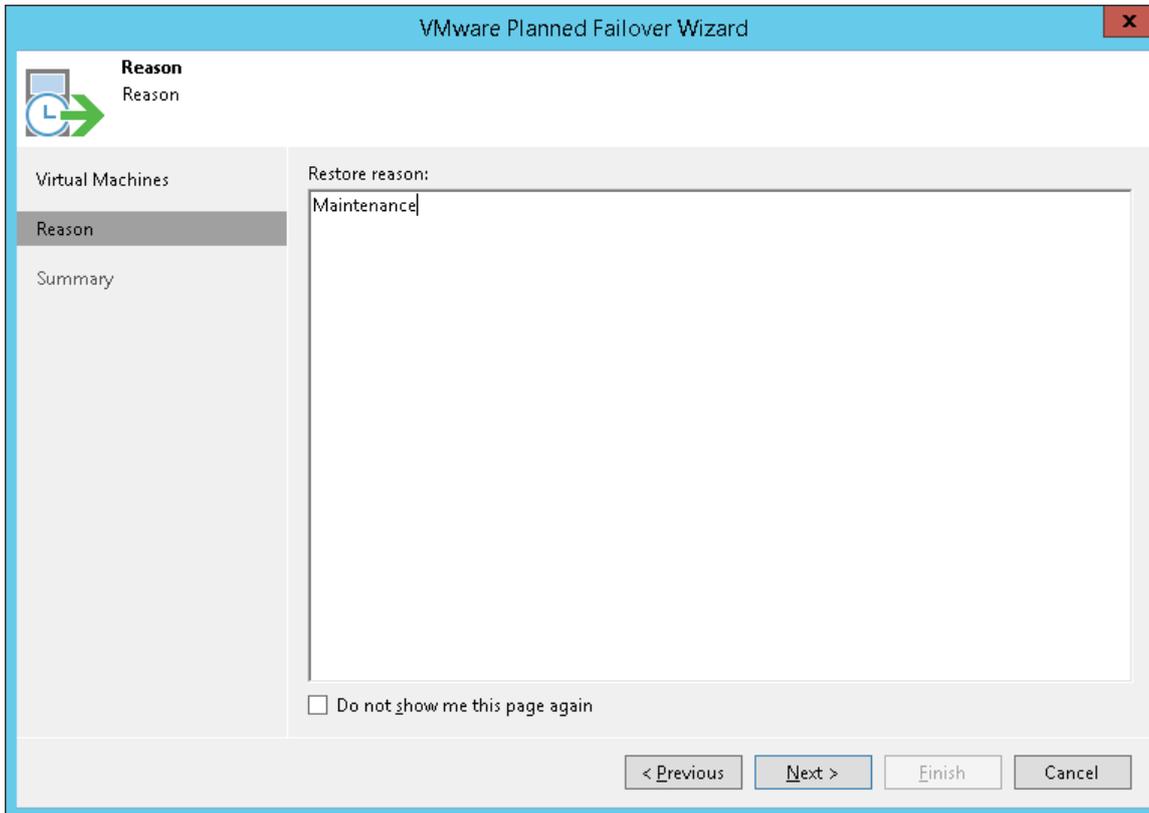
1. Enter a VM name or a part of it in the search field. Veeam Backup & Replication will display possible matches.
2. If the VM is not in the list, click the **Show more** link to browse existing VM replicas. Veeam Backup & Replication will open the **Backup Browser** window, and you can select the necessary VM replica there.

Step 3. Specify Failover Reason

At the **Reason** step of the wizard, enter a reason for failing over to VM replicas. 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.

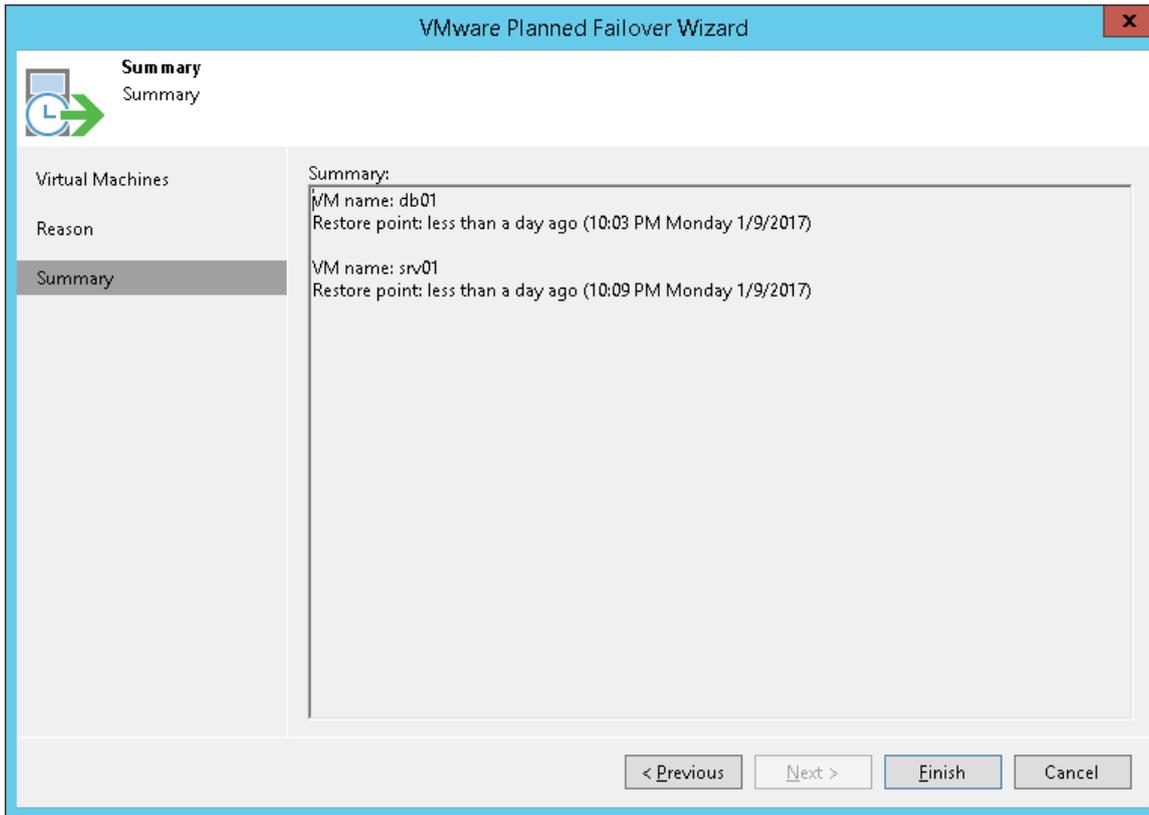


Step 4. Review Summary and Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of planned failover.

1. Review details of the failover task.
2. Click **Finish** to start the failover process.

Once planned failover is complete, VM replicas will be started on the target hosts.



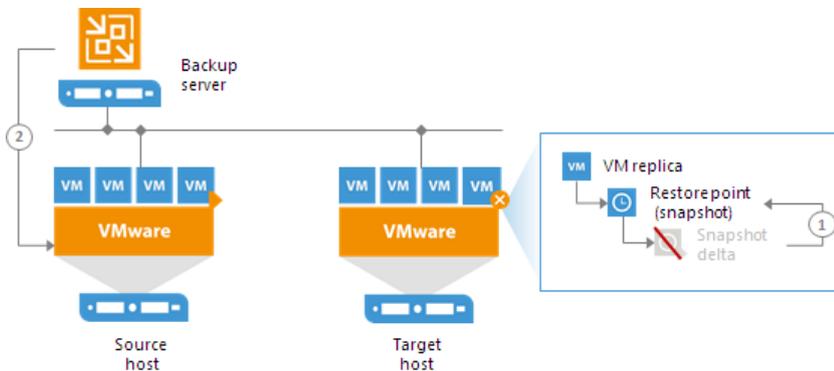
Undo Failover

To revert a VM replica to its pre-failover state, you can undo failover.

When you undo failover, you switch back from the VM replica to the original VM. Veeam Backup & Replication discards all changes made to the VM replica while it was in the *Failover* state. You can use the undo failover scenario if you have failed over to the VM replica for testing and troubleshooting purposes and want to get back to the normal operation mode.

The undo failover operation is performed in the following way:

1. Veeam Backup & Replication reverts the VM replica to its pre-failover state. To do this, Veeam Backup & Replication powers off the VM replica and gets it back to the state of the latest snapshot in the snapshot chain. Changes that were written to the snapshot delta file while the VM replica was in the *Failover* state are discarded.
2. The state of the VM replica gets back to *Normal*, and Veeam Backup & Replication resumes replication activities for the original VM on the source host.



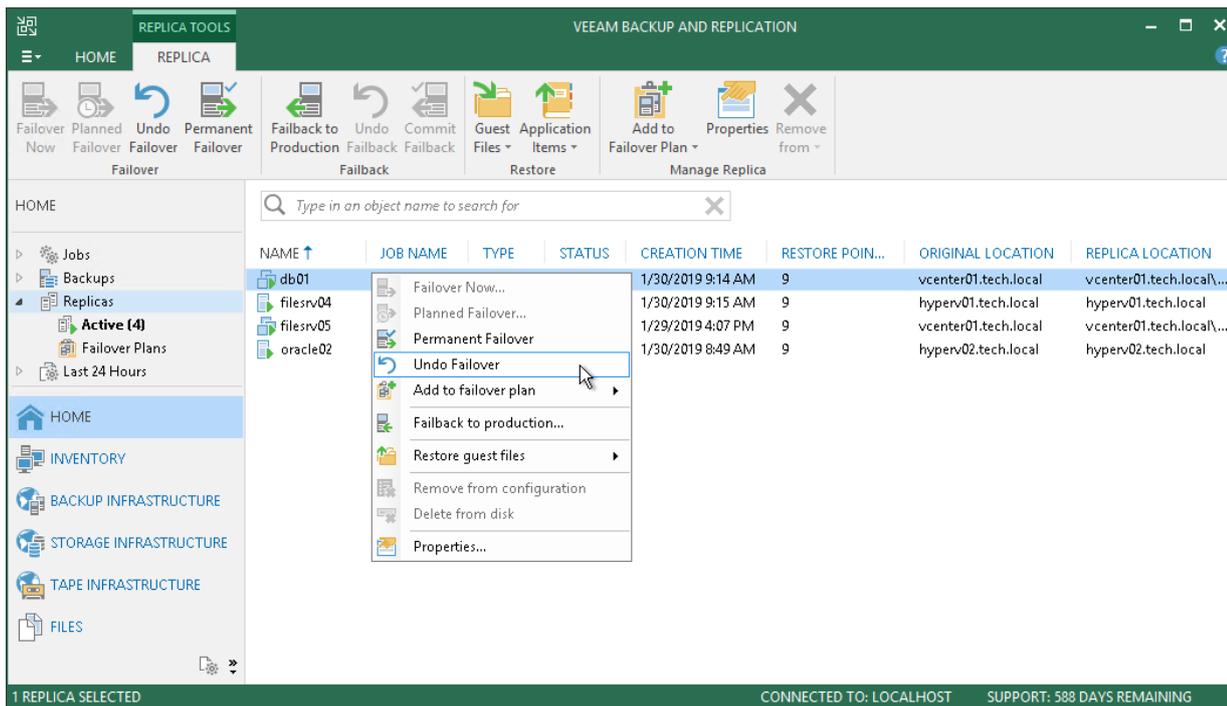
Undoing Failover

With the undo failover operation, you can power off running VM replicas on target hosts and roll back to initial state of VM replicas.

To undo failover:

1. Open the **Home** view.
2. In the inventory pane, select **Replicas**.
3. In the working area, select the necessary replica and click **Undo Failover** on the ribbon. You can also right-click the necessary replica and select **Undo Failover**.

4. In the displayed window, click **Yes** to confirm the operation.



Forcing Undo Failover

In some cases, Veeam Backup & Replication may fail to perform the undo failover operation. This can happen, for example, if the host on which the VM replica resides is unavailable. To overcome this situation, you can force undo failover.

When you force failover, Veeam Backup & Replication attempts to perform the undo failover operation in a regular way. If the host is unavailable, Veeam Backup & Replication changes the VM replica state to *Ready* in the configuration database and console.

To force undo failover:

1. Open the **Home** view.
2. In the inventory pane, select **Replicas**.
3. In the working area, select the necessary replica and click **Undo Failover** on the ribbon. You can also right-click the necessary replica and select **Undo Failover**.

4. In the displayed window, select the **Force undo failover** check box and click **Yes**.

The screenshot shows the Veeam Backup & Replication console. The main window displays a list of replicas under the 'Replicas' section. A dialog box is overlaid on the screen, asking for confirmation to 'Force undo failover'.

NAME	JOB NAME	TYPE	STATUS	CREATION TIME	RESTORE POIN...	ORIGINAL LOCATION	REPLICA LOCATION
fileserv03	Replication...	Regular	Failover	1/30/2019 9:14 AM	9	vcenter01.tech.local	vcenter01.tech.local\...
fileserv04	Replication...	Regular	Processi...	1/30/2019 9:15 AM	9	hyperv01.tech.local	hyperv01.tech.local
filesrv05	Apache Re...	Regular	Failover	1/29/2019 4:07 PM	9	vcenter01.tech.local	vcenter01.tech.local\...
windows001	Atlanta Rep...	Regular	Failover	1/30/2019 8:49 AM	9	hyperv02.tech.local	hyperv02.tech.local

Veeam Backup & Replication

Undo failover resets replica VM to the latest state so that you can continue replication. Any disk changes happened after failover will be lost. Would you like to continue?

Force undo failover

Yes No

1 REPLICA SELECTED CONNECTED TO: LOCALHOST SUPPORT: 588 DAYS REMAINING

Replica Failback

If you want to resume operation of a production VM, you can fail back to it from a VM replica. When you perform failback, you get back from the VM replica to the original VM, shift your I/O and processes from the target host to the production host and return to the normal operation mode.

If you managed to restore operation of the source host, you can switch from the VM replica to the original VM on the source host. If the source host is not available, you can restore the original VM to a new location and switch back to it. Veeam Backup & Replication offers three failback options:

- You can fail back to a VM in the original location on the source host.
- You can fail back to a VM that has been restored up-front from the backup in a new location.
- You can fail back to an entirely new location by transferring all VM replica files to the selected destination.

The first two options help you decrease recovery time and use of the network traffic:

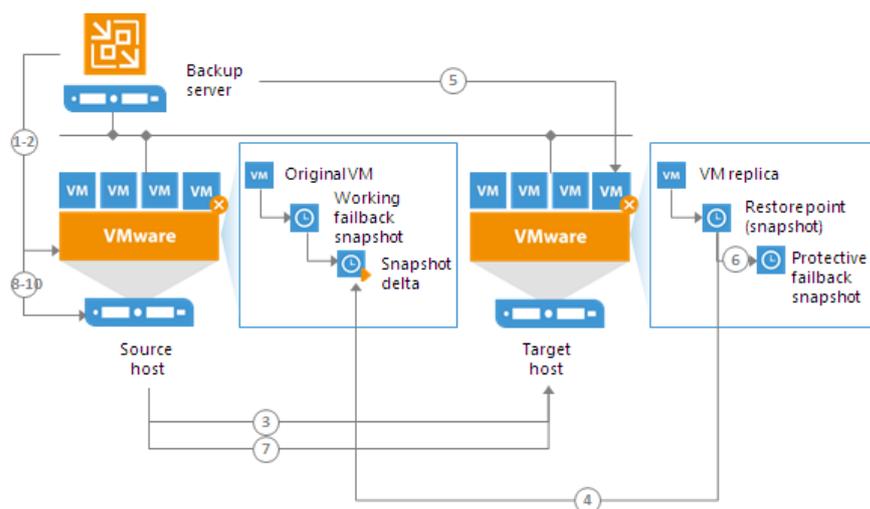
Veeam Backup & Replication needs to transfer only differences between the original VM and VM replica. The third option can be used if there is no way to use the original VM or restore the VM from the backup before performing failback.

How Failback Works

If you fail back to an existing original VM, Veeam Backup & Replication performs the following operations:

1. If the original VM is running, Veeam Backup & Replication powers it off.
2. Veeam Backup & Replication creates a working failback snapshot on the original VM.
3. Veeam Backup & Replication calculates the difference between disks of the original VM and disks of the VM replica in the *Failover* state. Difference calculation helps Veeam Backup & Replication understand what data needs to be transported to the original VM to synchronize it with the VM replica.
4. Veeam Backup & Replication transports changed data to the original VM. Transported data is written to the delta file of the working failback snapshot on the original VM.
5. Veeam Backup & Replication powers off the VM replica. The VM replica remains powered off until you commit failback or undo failback.
6. Veeam Backup & Replication creates a failback protective snapshot for the VM replica. The snapshot acts as a new restore point and saves the pre-failback state of the VM replica. You can use this snapshot to return to the pre-failback state of the VM replica afterwards.
7. Veeam Backup & Replication calculates the difference between the VM replica and the original VM once again and transports changed data to the original VM. A new synchronization cycle lets Veeam Backup & Replication copy a portion of last-minute changes made on the VM replica while the failback process was being performed.
8. Veeam Backup & Replication removes the working failback snapshot on the original VM. Changes written to the snapshot delta file are committed to the original VM disks.
9. The state of the VM replica is changed from *Failover* to *Failback*. Veeam Backup & Replication temporarily puts replication activities for the original VM on hold.

- If you have selected to power on the original VM after failback, Veeam Backup & Replication powers on the restored original VM on the target host.



If you fail back to an entirely new location, Veeam Backup & Replication performs the following operations:

- Veeam Backup & Replication transports all VM replica files and stores them on the target datastore.
- Veeam Backup & Replication registers a new VM on the target host.
- If you have selected to power on the original VM after failback, Veeam Backup & Replication powers on the restored original VM on the target host.

In Veeam Backup & Replication, failback is considered a temporary stage that should be further finalized. After you test the recovered original VM and make sure it is working without problems, you should commit failback. You can also undo failback and return the VM replica back to the *Failover* state.

Failback on VSAN

Due to specifics of VSAN data storage organization, Veeam Backup & Replication cannot get the difference between disks of a VM replica located on VSAN and disks of the original VM in a regular manner. Veeam Backup & Replication needs to read VM disks data anew in every failback process phase. As a result, failback for VMs replicas on VSAN slightly differs from the regular failback course.

Before Veeam Backup & Replication starts the failback process, it checks the location of VM replica disks. If at least one disk is located on VSAN, Veeam Backup & Replication performs failback in the following way:

- Veeam Backup & Replication creates a working failback snapshot for the original VM.
- For every VM disk, Veeam Backup & Replication performs the following actions:
 - If you fail back to the original VM location, Veeam Backup & Replication calculates the difference between the VM replica disk and the original VM disk. To do this, Veeam Backup & Replication reads the whole amount of disk data from VSAN, and transfers only changed data to the original VM side.
 - If you fail back to a new location, Veeam Backup & Replication transfers the whole disk without calculating the difference.
- The VM replica is powered off.

4. Veeam Backup & Replication creates a protective failback snapshot for the VM replica. Using the protective failback snapshot, Veeam Backup & Replication detects what changes took place on the VM replica while VM disk data was being transported. As well as before, Veeam Backup & Replication reads the whole amount of VM disks data but transports only those data blocks that have changed since the VM disks transfer.

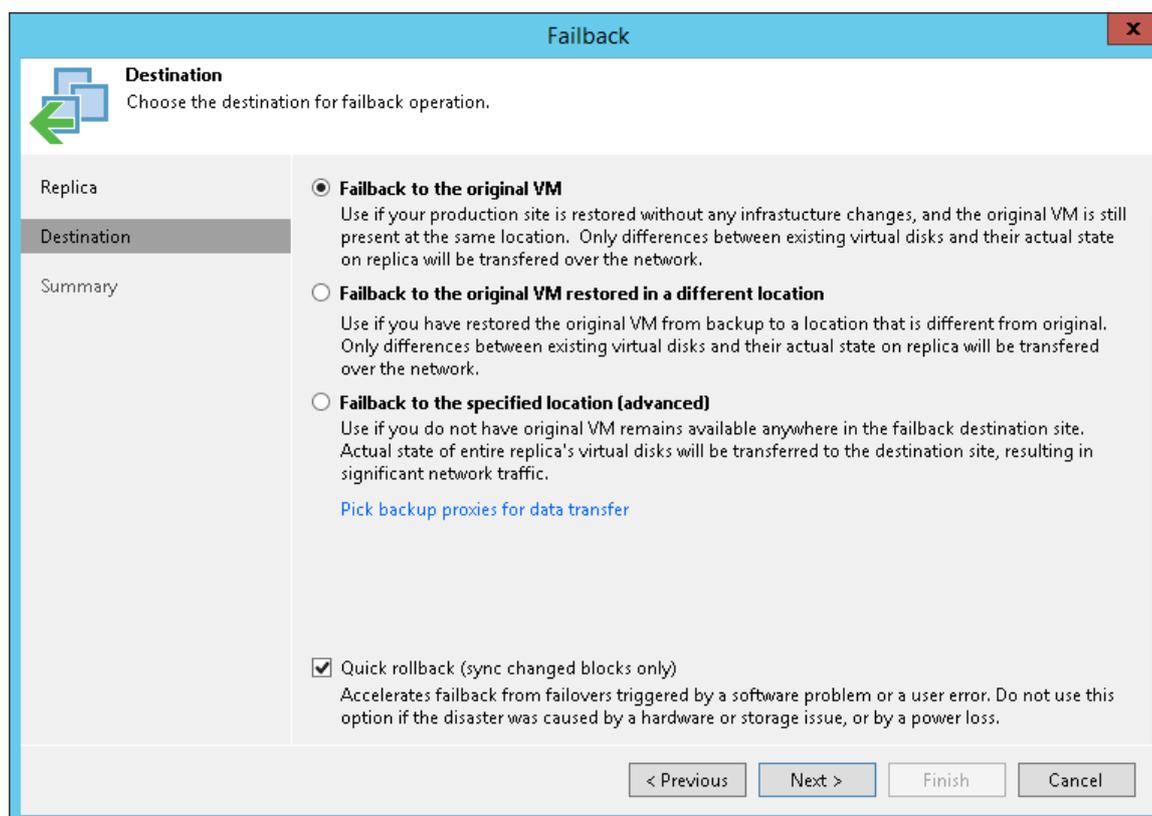
The rest of the failback process does not differ from the regular failback process.

Quick Rollback

If you fail back from a VM replica to the VM in the original location, you can instruct Veeam Backup & Replication to perform quick rollback. Quick rollback significantly reduces the failback time and has little impact on the production environment.

During failback with the quick rollback option enabled, Veeam Backup & Replication does not calculate digests for entire VM replica disks to get the difference between the original VM and VM replica. Instead, it queries CBT to get information about disk sectors that have changed, and calculates digests only for these disk sectors. As a result, digest calculation is performed much faster. After that, Veeam Backup & Replication performs failback in a regular way: transport changed blocks to the original VM, powers off the VM replica and synchronizes the original VM with the VM replica once again.

It is recommended that you use quick rollback if you fail back to the original VM after a problem that has occurred at the level of the guest OS of the VM replica – for example, there has been an application error or a user has accidentally deleted a file on the VM replica guest OS. Do not use quick rollback if the problem has occurred at the VM hardware level, storage level or due to a power loss.



Requirements for Quick Rollback

To perform quick rollback, make sure that the following requirements are met:

- You must perform failback to the VM in the original location.

- CBT must be enabled for the original VM.
- The VM replica must be created with the **Use changed block tracking data** option enabled.

Limitations for Quick Rollback

- During the first replication job session after failback with quick rollback, the CBT on the original VM is reset. Due to that Veeam Backup & Replication will read data of the entire VM.
- Quick rollback can be performed in the Direct NFS access, Virtual appliance, Network transport mode. The Direct SAN access transport mode cannot be used for quick rollback due to [VMware limitations](#).

Performing Failback

With the **Failback** option, you can switch from a VM replica back to the original VM or restore a VM from a VM replica in a new location.

Before starting failback, [check prerequisites](#). Then use the **Failback** wizard to switch back to the original VM.

Before You Begin

Before you perform failback, check the following prerequisites:

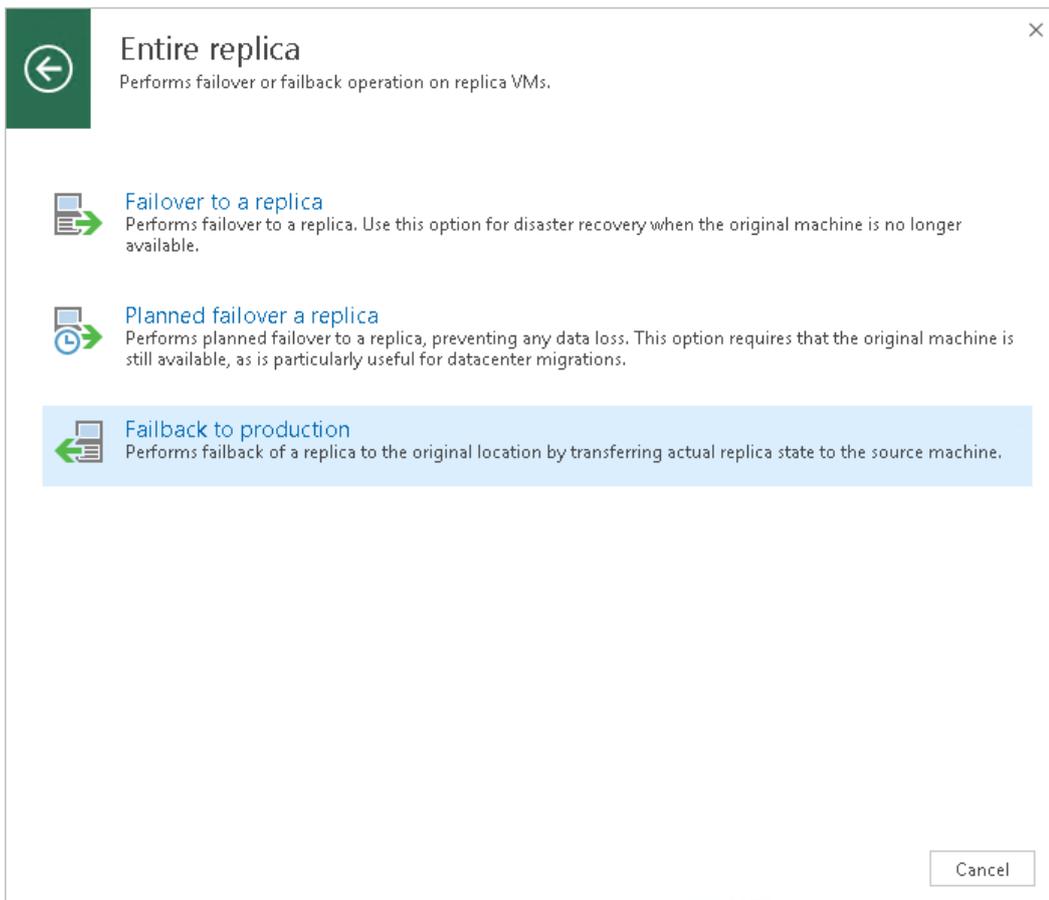
- VMs for which you plan to perform failback must be successfully replicated at least once.
- VM replicas must be in the *Failover* state.

Step 1. Launch Failback Wizard

To launch the **Failback** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from replica > Entire replica > Failback to production**.
- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, select the necessary replica and click **Failback to Production** on the ribbon.

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary replica and select **Failback to production**.

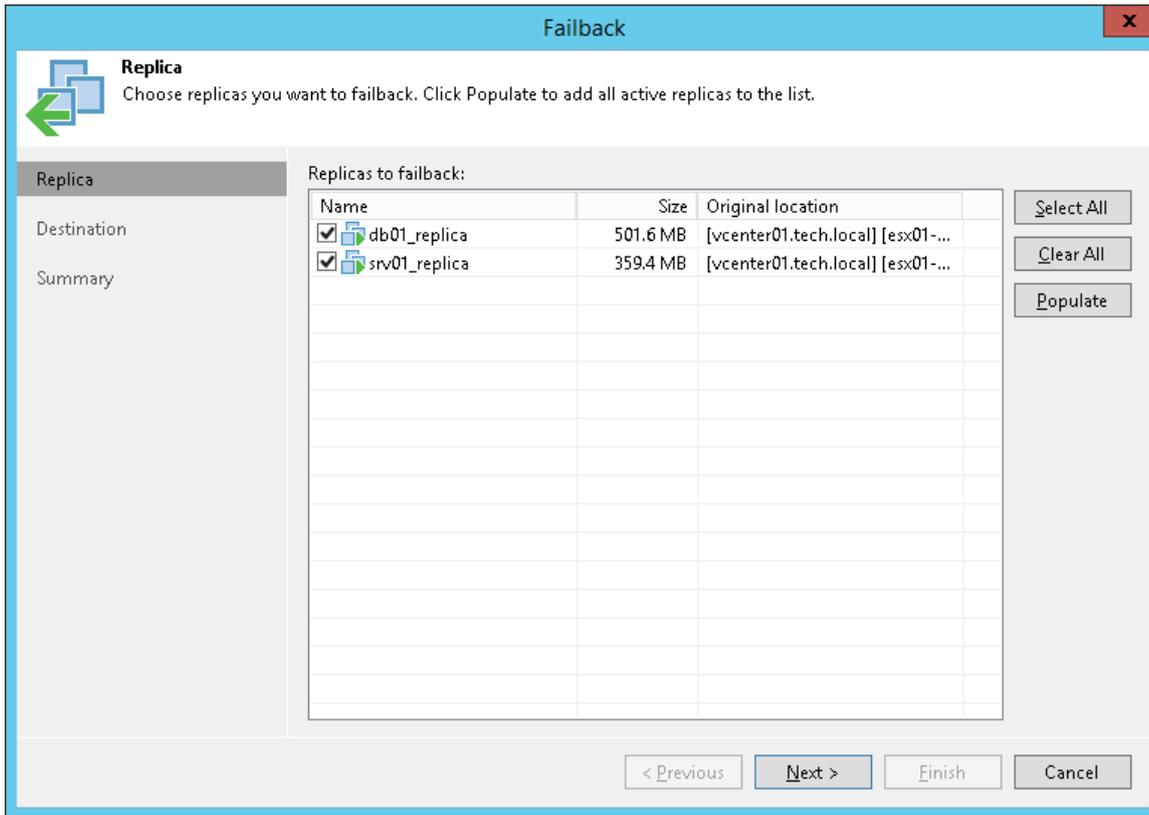


Step 2. Select VM Replicas to Fail Back

At the **Replica** step of the wizard, select one or more VM replicas from which you want to fail back.

1. Click **Populate** to display all existing replicas in the *Failover* state.

2. Leave check boxes selected for those VM replicas from which you want to fail back.



Step 3. Select Failback Destination

At the **Destination** step of the wizard, select the failback destination and backup proxies for VM data transport during failback.

1. Veeam Backup & Replication supports three possible failback destination variants. Note that the **Failback** wizard displays a different set of steps for every failback variant.
 - Select **Failback to the original VM** if you want to fail back to the original VM residing on the source host. Veeam Backup & Replication will restore the original VM to the current state of its replica.
If this option is selected, you will pass to the [Summary step](#) of the wizard.
 - Select **Failback to the original VM restored in a different location** if you have recovered the original VM from a backup in a new location, and you want to switch to it from the replica. In this case, Veeam Backup & Replication will synchronize the recovered VM with the current state of the replica.
If this option is selected, you will pass to the [Target VM step](#) of the wizard.
 - Select **Failback to the specified location** if you want to restore the original VM from a replica – in a new location and/or with different settings (such as VM location, network settings, virtual disk and configuration files path and so on).
If this option is selected, you will need to complete all further steps of the wizard.

If you fail back to the original VM or the original VM is restored in a new location, only differences between the existing virtual disks and their state will be transferred to the original VM. Veeam Backup & Replication will not transfer replica configuration changes such as a different IP address or network settings (if replica Re-IP and network mapping were applied), new hardware or virtual disks added while the replica was in the *Failover* state.

If you choose to perform advanced failback, the entire VM replica, including its configuration and virtual

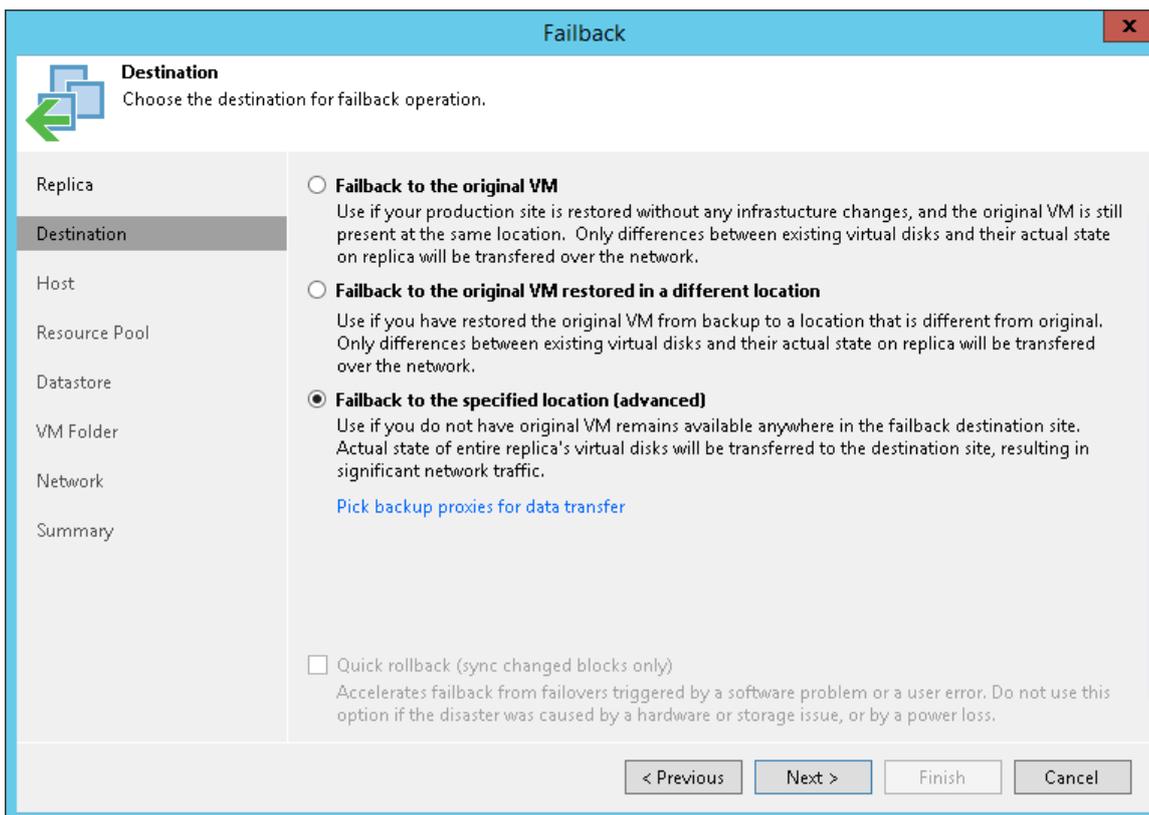
disks content, will be restored in the selected location.

2. Click the **Pick backup proxies for data transfer** link to select backup proxies for data transfer during failback. In the offsite replication scenario, you must select one backup proxy in the production site and one proxy in the DR site. In the onsite replication scenario, you can use the same backup proxy as a source and target one.
3. In the **Choose backup Proxy** section, click **Choose** to assign a backup proxy. You can assign backup proxies explicitly or instruct Veeam Backup & Replication to select backup proxies automatically.

- If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that are connected to the source datastore and will automatically assign optimal proxy resources for processing VM data.

VMs selected for failback are processed one by one. Before processing a new VM in the VM list, Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use, the current workload on the backup proxies to select the most appropriate resource for VM processing.

- If you choose **Use the selected backup proxy servers only**, you can explicitly define backup proxies that must be used for data transfer. It is recommended that you select at least two backup proxies to ensure that failover is performed should one of backup proxies fail or lose its connectivity to the source or target datastore.



Restoring Storage Policies

If the replicated VM was associated with the storage policy, in the failback to original location scenario, Veeam Backup & Replication will associate the restored VM with this storage policy.

When you click **Next**, Veeam Backup & Replication will check storage policies in the virtual environment and compare this information with the information about the replica storage policy. If the original storage policy has been changed or deleted, Veeam Backup & Replication will display a warning. You can select one of the following options:

- **Current** – the restored VM will be associated with the profile with which the original VM in the production environment is currently associated.
- **Default** – the restored VM will be associated with the profile that is set as default for the target datastore.
- **Stored** – the restored VM will be associated with the profile that was assigned to the original VM at the moment of replication.

For more information, see [Storage Policy Restore](#).

Step 4. Select Target Host

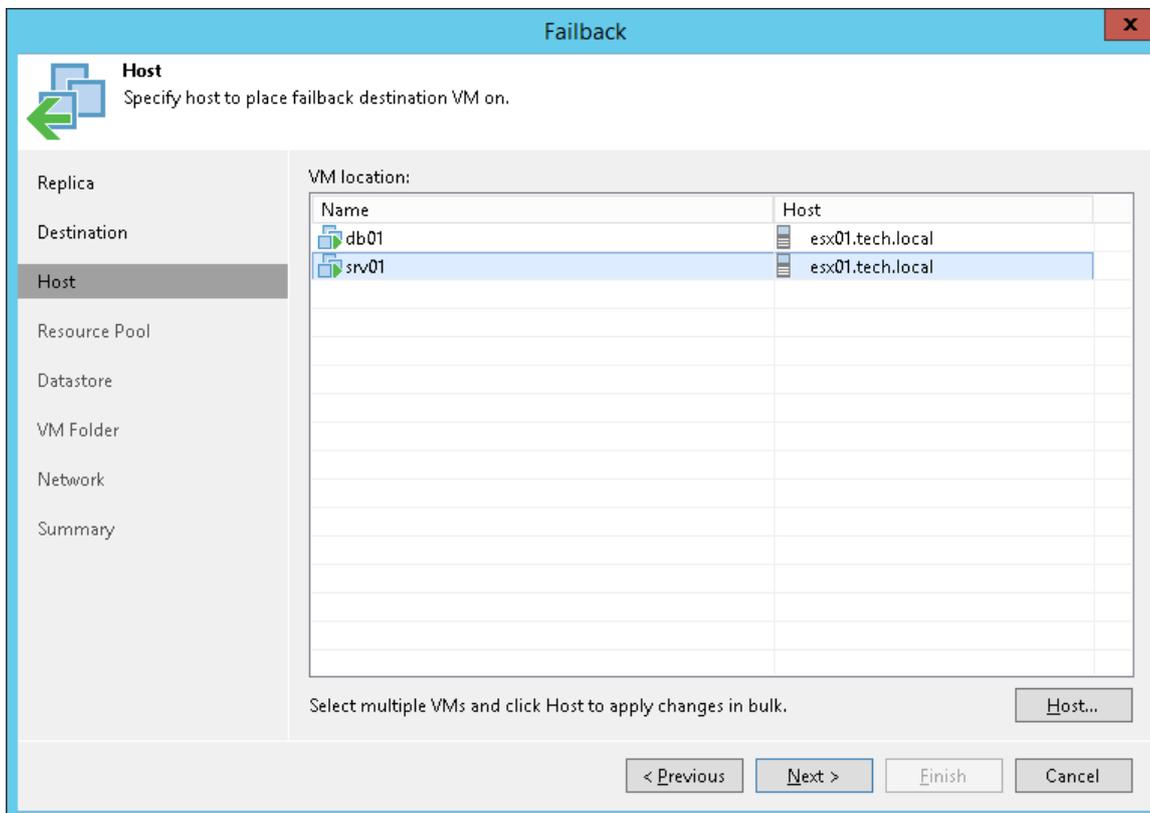
The **Host** step of the wizard is only available if you have chosen to perform advanced failback.

To specify a target host:

1. Select one or more VMs in the list and click **Host**.
2. Choose a host or cluster where the VMs 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: *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]**.



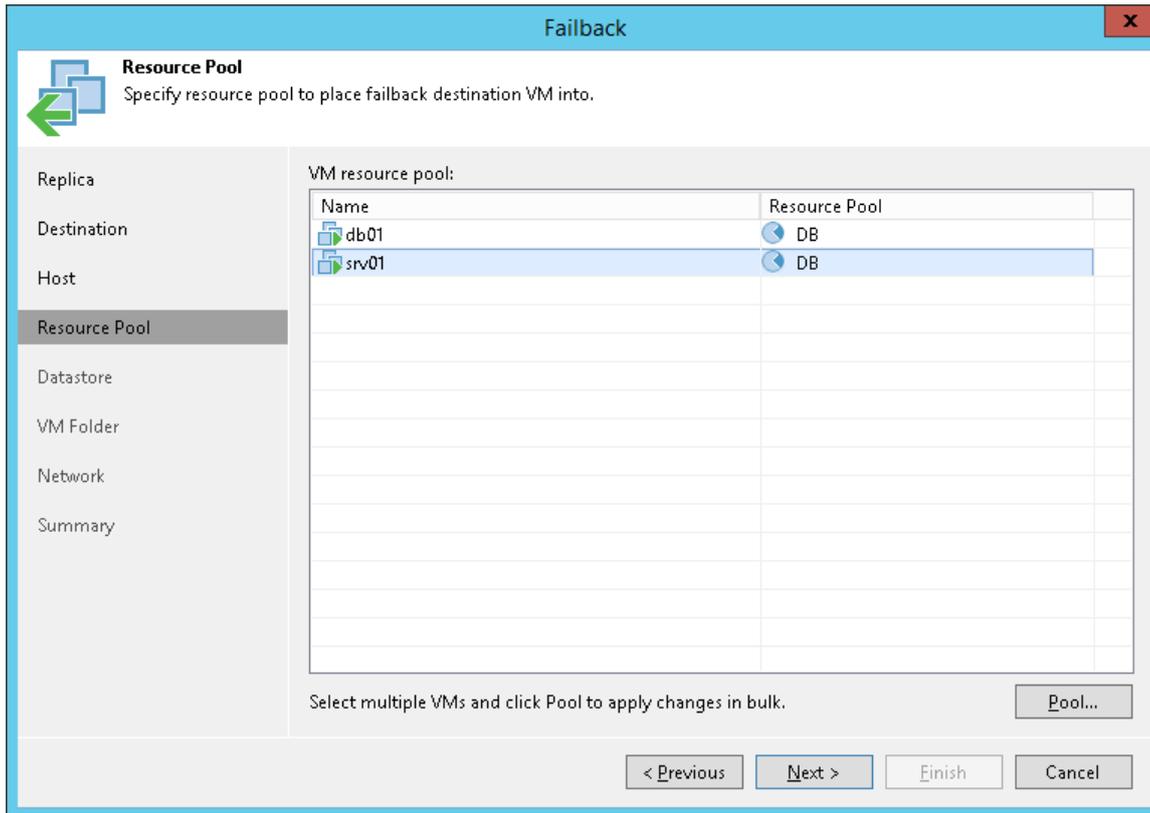
Step 5. Select Target Resource Pool

The **Resource Pool** step of the wizard is only available if you have chosen to perform advanced failback.

To specify a destination resource pool:

1. Select one or more VMs in the list and click **Pool**.
2. Choose a resource pool to which the selected VMs will belong.
3. If necessary, you can also select a vApp to which the restored VM will be included.

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



Step 6. Select Target Datastore

The **Datastore** step of the wizard is only available if you have chosen to perform advanced failback.

When restoring a VM from a replica, you can place an entire VM to a particular datastore or choose to store configuration files and disk files of a restored VM in different locations.

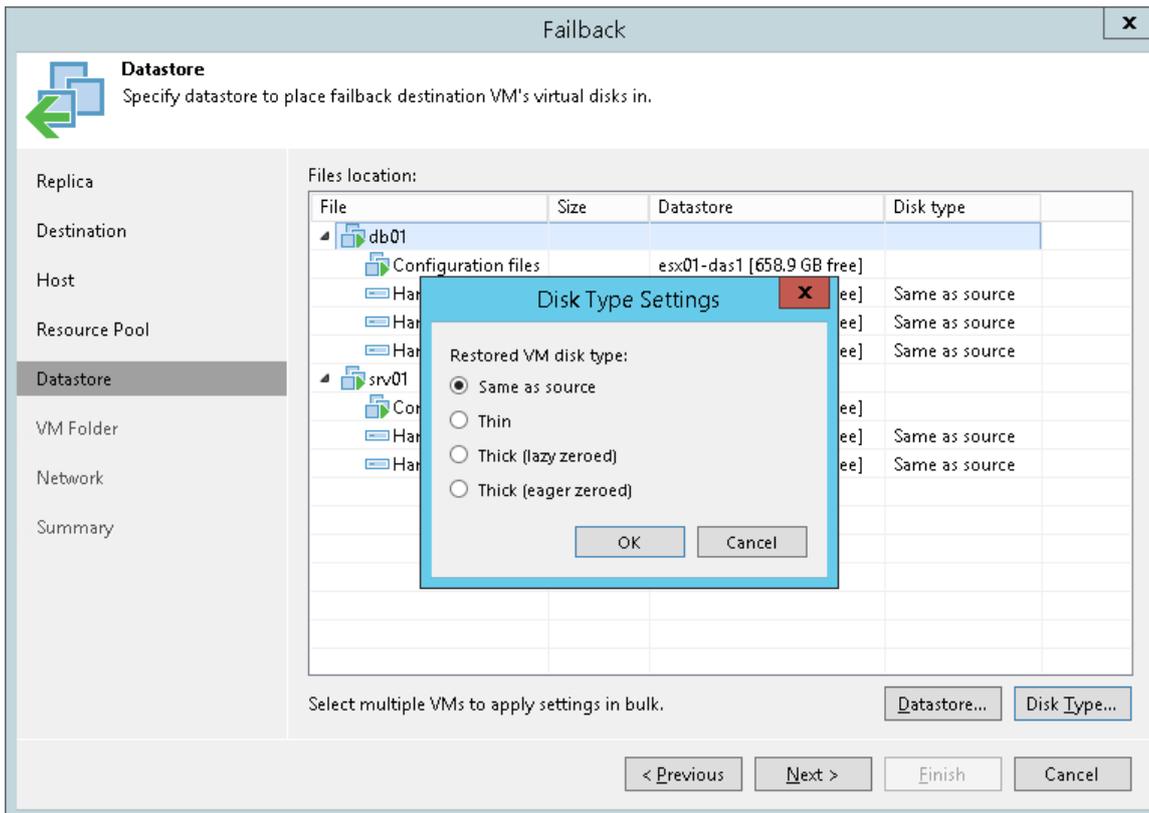
To specify a destination datastore:

1. Select one or more VMs in the list and click **Datastore**.
2. If configuration and disk files of a VM should be placed to different datastores, expand the VM in the list, select the necessary file type and click **Datastore**. From the virtual environment, choose a datastore to which the selected objects will be stored. To facilitate selection, use the search field at the bottom of the window: enter a datastore name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

- By default, Veeam Backup & Replication preserves the format of restored VM disks, so that if disks of the VM replica were provisioned as thick, Veeam Backup & Replication will restore the VM with thick disks. If necessary, you can change the disk format of a restored VM. To do so, expand a VM in the list, select the necessary disk and click **Disk Type**. In the **Disk Type Settings** section, choose the format that will be used to restore virtual disks of the VM: same as original, thin, thick lazy zeroed or thick eager zeroed. For more information about disk types, see <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.html.hostclient.doc/GUID-4COF4D73-82F2-4B81-8AA7-1DD752A8A5AC.html>.

NOTE:

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



Step 7. Select Target Folder

The **VM Folder** step of the wizard is only available if you have chosen to perform advanced failback.

Specifying Destination VM Folder

To specify a destination VM folder, do the following:

- Select one or more VMs in the list and click Folder.
- Choose a folder to which the selected VMs must be placed.

To facilitate selection, you can 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]**.

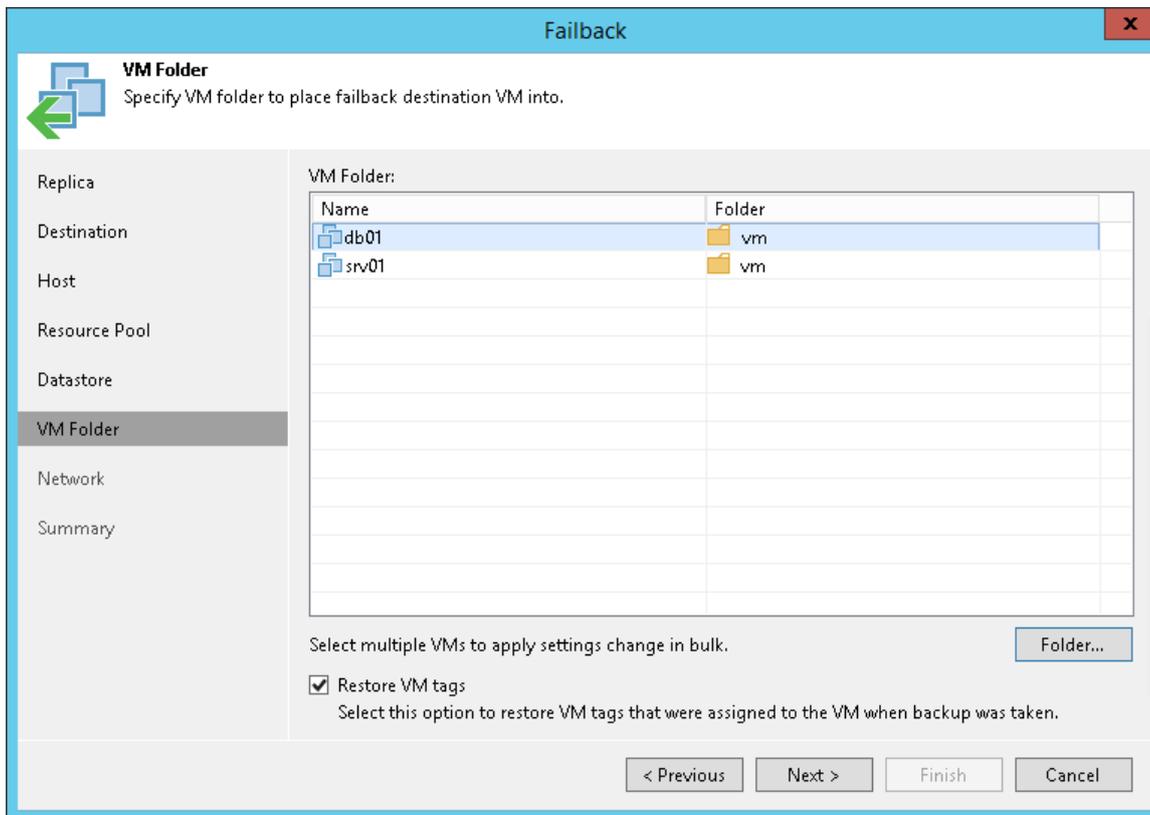
NOTE:

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

Restoring VM Tags

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. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:

- The VM is restored to its original location.
- The original VM tag is still available on the source vCenter Server.



Step 8. Select Target Network

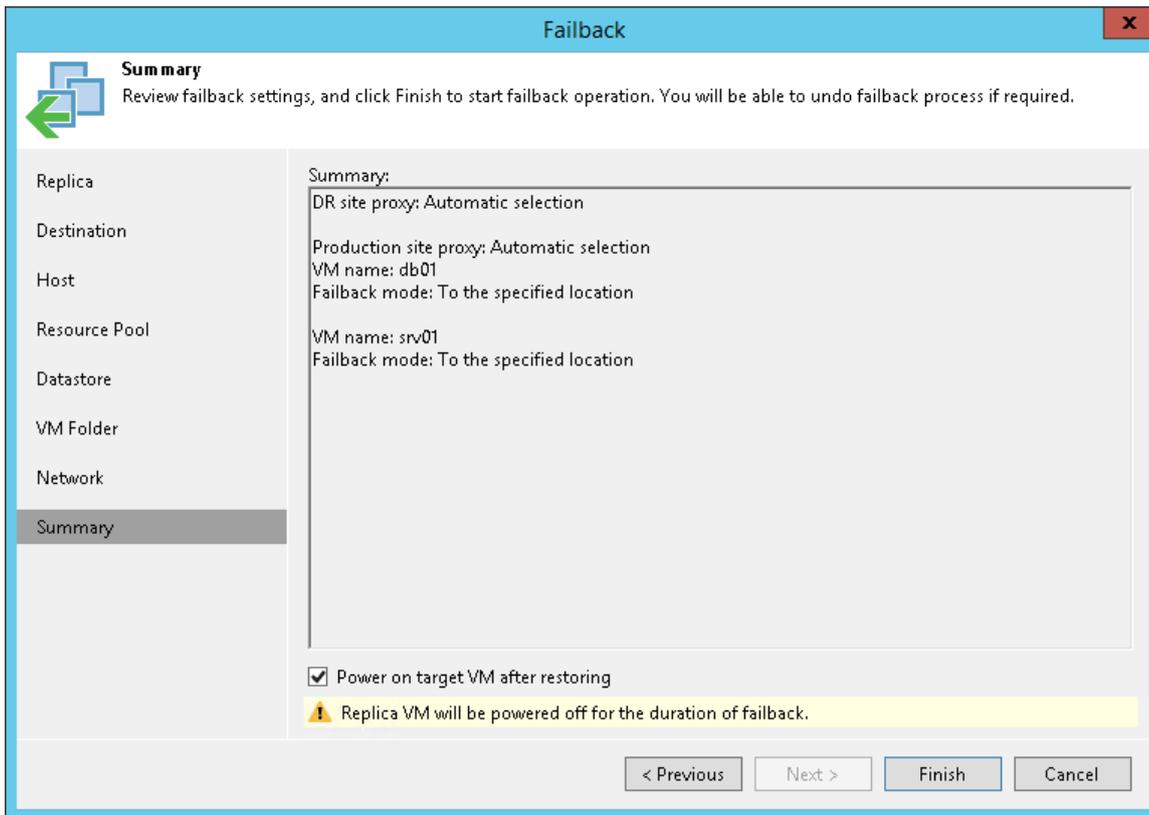
The **Network** step of the wizard is only available if you have chosen to perform advanced failback.

If you plan to fail back to VMs in a new location (for example, another site with a different set of networks), you can map DR site networks to production site networks. Veeam Backup & Replication will use the network mapping table to update configuration files of VMs on the fly, during the failback process.

To change networks to which restored VMs will be connected:

1. Select one or more VMs in the list and click **Network**.
2. If a VM is connected to multiple networks, expand the VM, select the network to map and click **Network**.

2. Check the specified settings and click **Finish**. Veeam Backup & Replication will restore the original VMs to the state of corresponding VM replicas.



Commit Failback

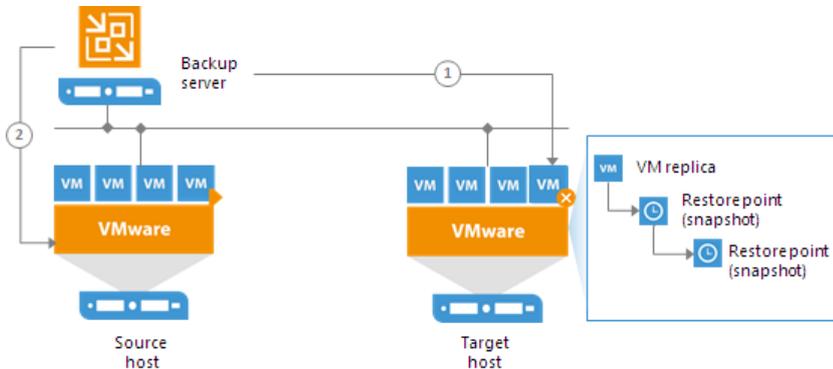
To confirm failback and finalize recovery of the original VM, you need to commit failback.

When you commit failback, you confirm that you want to get back to the original VM. Veeam Backup & Replication gets back to the normal operation mode and resumes replication activities for the original VM to which you failed back.

The commit failback operation is performed in the following way:

1. Veeam Backup & Replication changes the state of the replica from *Failback* to *Normal*.
2. Further operations depend on the location to which the VM is failed back:
 - If the VM replica is failed back to a new location, Veeam Backup & Replication additionally reconfigures the replication job and adds the former original VM to the list of exclusions. The VM restored in the new location takes the role of the original VM and is included into the replication job instead of the excluded VM. When the replication job starts, Veeam Backup & Replication will process the newly restored VM instead of the former original VM.
 - If the VM replica is failed back to the original location, the replication job is not reconfigured. When the replication job starts, Veeam Backup & Replication will process the original VM in the normal operation mode.

During failback commit, the failback protective snapshot that saves the pre-failback state of a VM replica is not deleted. Veeam Backup & Replication uses this snapshot as an additional restore point for VM replica. With the pre-failback snapshot, Veeam Backup & Replication needs to transfer fewer changes and therefore puts less load on the network when replication activities are resumed.



Committing Failback

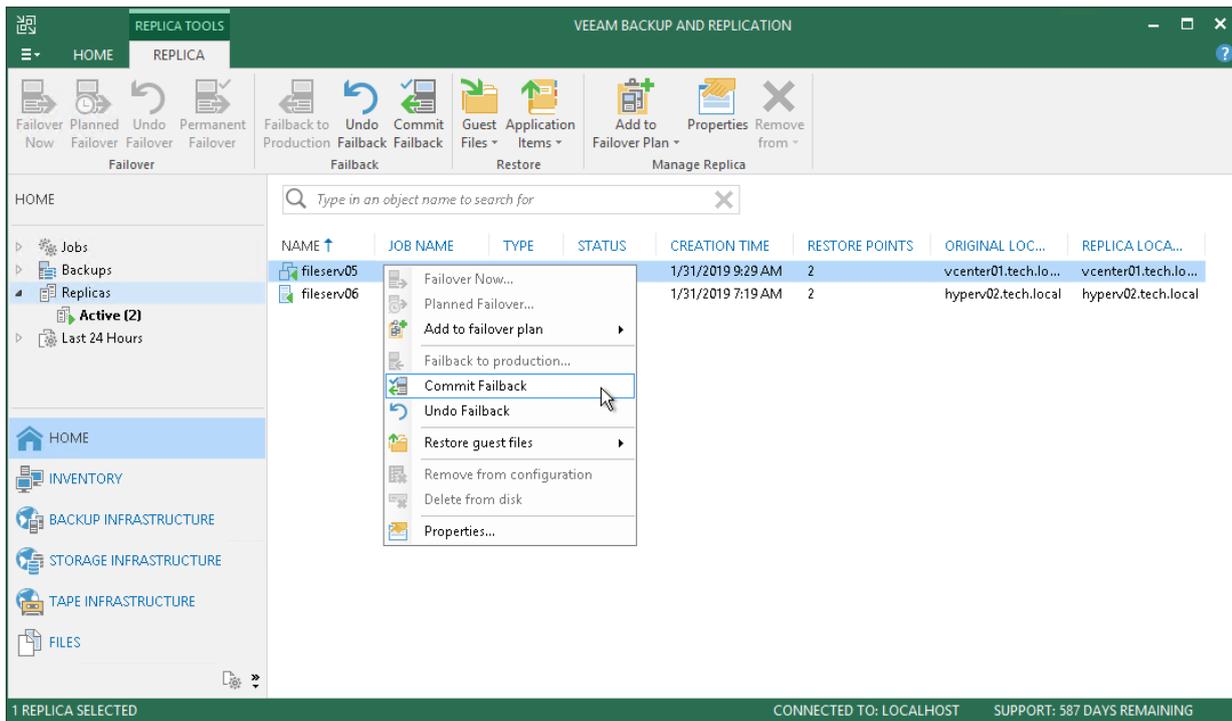
The **Commit failback** operation finalizes failback from the VM replica to the original VM.

To commit failback, do one of the following:

- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, select the necessary replica and click **Commit Failback** on the ribbon. In the displayed window, click **Yes** to confirm the operation.
- Open the **Home** view, in the inventory pane select **Replicas**. In the working area, right-click the necessary replica and select **Commit Failback**. In the displayed window, click **Yes** to confirm the operation.

Depending on the location to which the VM is failed back, Veeam Backup & Replication performs the following finalizing operations after failback is committed:

- If the VM replica is failed back to a new location, Veeam Backup & Replication additionally reconfigures the replication job and adds the former original VM to the list of exclusions. The VM restored in the new location takes the role of the original VM, and is included into the replication job instead of the excluded VM. When the replication job starts, Veeam Backup & Replication will exclude the former original VM from processing, and will replicate the newly restored VM instead.
- If the VM replica is failed back to the original location, the replication job is not reconfigured. When the replication job starts, Veeam Backup & Replication will process the original VM in the normal mode.

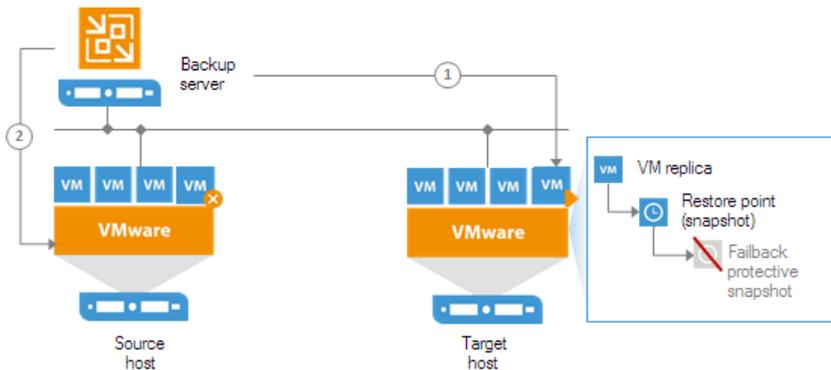


Undo Failback

If the original VM is not working as expected after the failback operation, you can undo failback and get back to the VM replica.

The undo failback operation is performed in the following way:

1. Veeam Backup & Replication deletes the protective failback snapshot on the VM replica.
2. Veeam Backup & Replication powers on the VM replica and changes the VM replica state from *Failback* to *Failover*.



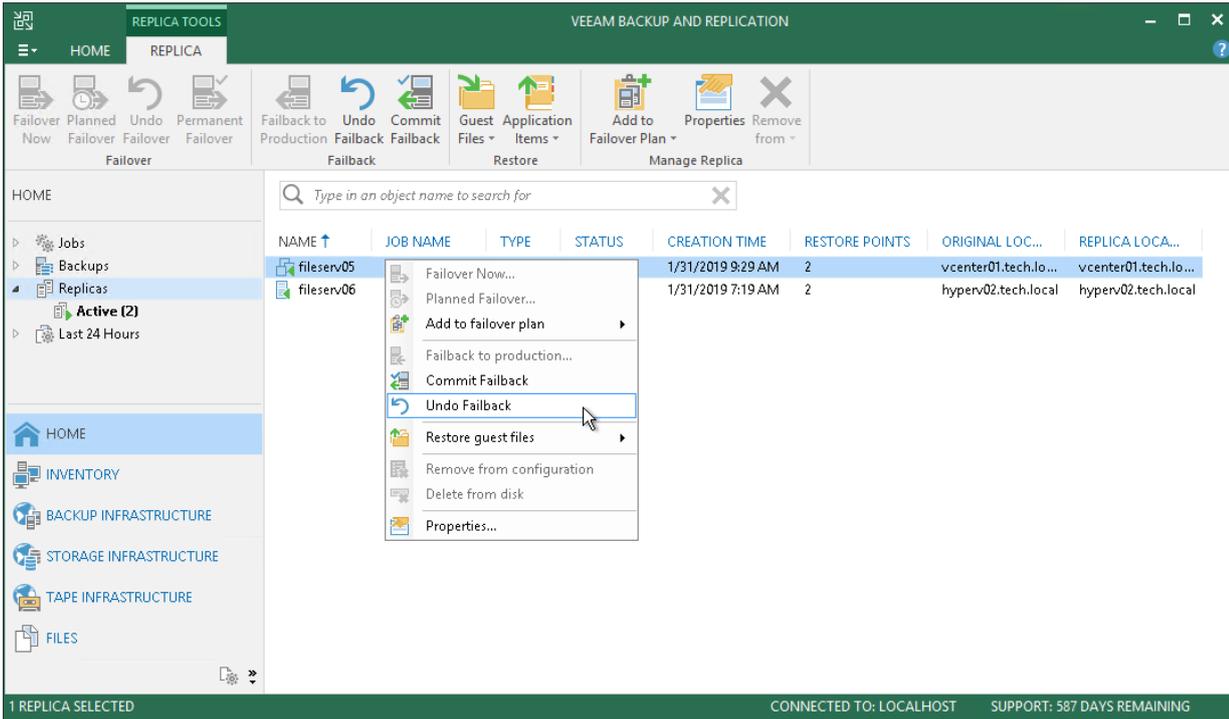
Undoing Failback

The **Undo failback** option allows you to switch from the original VM back to the VM replica and roll back the replica to the failover state.

To undo failback, do one of the following:

- Open the **Home** view and select the **Replicas** node. In the working area, select the necessary replica and click **Undo Failback** on the ribbon.
- Open the **Home** view and select the **Replicas** node. In the working area, right-click the necessary replica and select **Undo Failback**.

In the displayed dialog box, click **Yes** to confirm the operation.



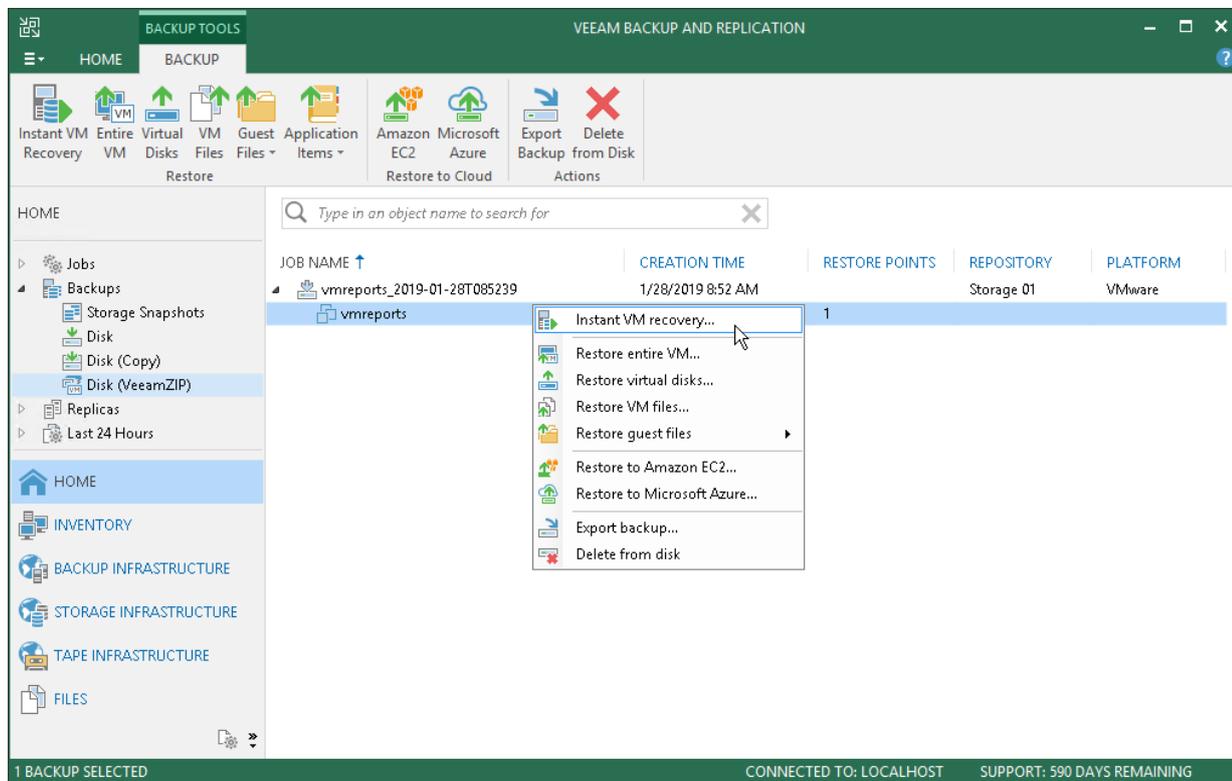
VeeamZIP

With Veeam Backup & Replication, you can quickly perform backup of one or several VMs with VeeamZIP.

VeeamZIP is similar to a full VM backup. The VeeamZIP job always produces a full backup file (VBK) that acts as an independent restore point. You can store the backup file to a backup repository, to a local folder on the backup server or to a network share.

When you perform backup with VeeamZIP, you do not have to configure a backup job and schedule it. Instead, you can start the backup process for selected VMs immediately. This type of backup requires minimum settings – you should only select the backup destination, choose the necessary compression level and enable or disable encryption and application-aware processing if necessary.

Backup files produced with VeeamZIP jobs are displayed in the **Home** view, under the **Backups > Disk (VeeamZIP)** node. To restore VM data from VeeamZIP backups, you can right-click it in the **Home** view and select the necessary restore option. You can also double-click the necessary VeeamZIP backup file on the machine where Veeam Backup & Replication is installed.



To view the progress or results of the VeeamZIP job session, you can use the **History** view. For more information, see [Viewing Real-Time Statistics](#).

IMPORTANT!

Veeam Backup & Replication does not enforce backup repository throttling rules during VeeamZIP jobs.

Creating VeeamZIP Backups

You can quickly back up running and powered off VMs with VeeamZIP. VeeamZIP can be helpful if you want to create an ad-hoc backup for VMs, archive VMs before decommissioning and so on. You can create VeeamZIP backups for one or more VMs.

To create VeeamZIP backups:

1. Open the **Inventory** view.
2. In the infrastructure tree, select a host or VM container in which the VMs that you want to back up reside.
3. In the working area, select the VMs and click **VeeamZIP > VeeamZIP** on the ribbon or right-click the VMs and select **VeeamZIP**.

To quickly find the necessary VMs, 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 of the **VeeamZIP <N> VM** window, specify a location in which you want to store VeeamZIP backups.
 - To store VeeamZIP backups in a backup repository, select **Backup repository** and choose the necessary backup repository from the list.
 - To store VeeamZIP backups in a local folder on the backup server, select **Local or shared folder**, click **Browse** on the right and select a folder in which VeeamZIP backups must be stored.
 - To store VeeamZIP backups 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 (\\).

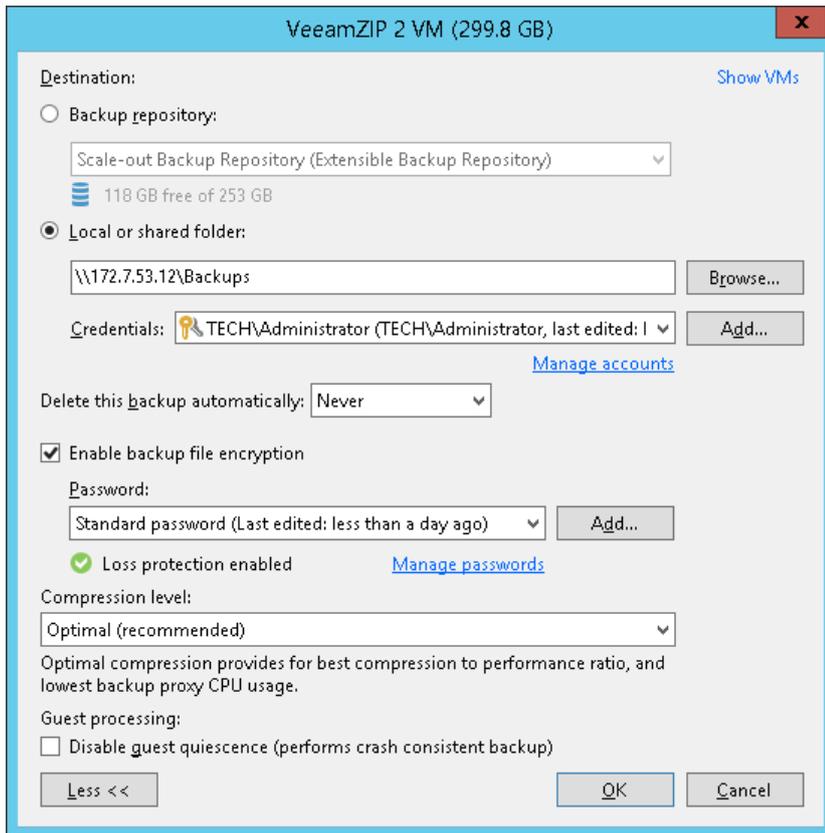
If the shared folder requires authentication, select the necessary credentials from the **Credentials** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add necessary credentials. For more information, see [Managing Credentials](#).

5. Use the **Delete this backup automatically** list to specify retention settings for the created VeeamZIP backups. By default, VeeamZIP backups are not removed and kept in the specified location for an indefinite period of time.
6. To encrypt VeeamZIP backups, select the **Enable backup file encryption** check box. From the **Password** list, select a password that 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](#).
7. From the **Compression level** list, select a compression level for created backups: *None, Dedupe-friendly, Optimal, High or Extreme*.
8. By default, Veeam Backup & Replication uses VMware Tools quiescence to create a transactionally consistent image of VMs. You can disable VM quiescence. To do this, select the **Disable guest quiescence** check box. In this case, Veeam Backup & Replication will create a crash-consistent VM backup.
9. Click **OK**. The VeeamZIP task will start immediately. Veeam Backup & Replication 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 backups afterwards.

- 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 & Replication keeps settings of the latest VeeamZIP task. To quickly create VeeamZIP backups with the same settings and store backups in the same location, right-click the necessary VM and select **VeeamZIP to**.



Backup Copy

The main backup purpose is to protect your data against disasters and virtual or physical machine failures. However, having just one backup does not provide the necessary level of safety. The primary backup may get destroyed together with production data, and you will have no backups from which you can restore data.

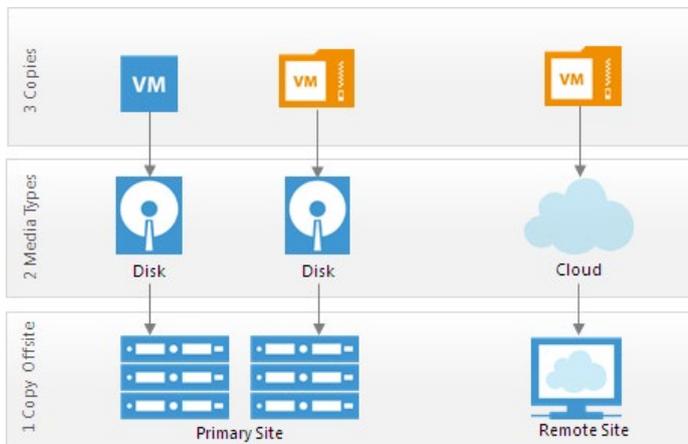
Backup experts advise that to build a successful data protection and disaster recovery plan, you must follow the 3-2-1 rule:

- 3: You must have at least three copies of your data: the original production data and two backups.
- 2: You must use at least two different types of media to store the copies of your data, for example, local disk and cloud.
- 1: You must keep at least one backup offsite, for example, in the cloud or in a remote site.

Thus, you must have at least two backups and they must be in different locations. If a disaster takes out your production data and local backup, you can still recover from your offsite backup.

To help you adopt the 3-2-1 rule, Veeam Backup & Replication offers backup copy capabilities. Backup copy allows you to create several instances of the same backup data in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Backup copy is a job-driven process. Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes.



About Backup Copy

With backup copy, you can create several instances of the same backup file and copy them to secondary (target) backup repositories for long-term storage. Target backup repositories can be located in the same site as the source backup repository, or can be deployed offsite. The backup copy file has the same format as the primary backup, so you can restore necessary data directly from it in case of a disaster.

Veeam Backup & Replication supports backup copy for the following types of backups:

- VM backups created with Veeam Backup & Replication
- Backups of physical and virtual machines created with Veeam Agent for Microsoft Windows
- Backups of physical and virtual machines created with Veeam Agent for Linux
- Backups of Amazon EC2 instances created with [N2WS Backup & Recovery](#)

With backup copy jobs, you can transport backups of EC2 instances to on-premises repositories.

Veeam Backup & Replication copies backup data per machine at the block level. That is, it does not copy the whole VBK, VIB or VRB files from the source to target backup repository. Instead, it works with data of separate machines stored in these files.

When the backup copying process starts, Veeam Backup & Replication accesses backup files on the source backup repository, retrieves data blocks for a specific machine from the backup file, copies them to the target backup repository, and composes copied blocks into a backup file on the target backup repository. The backup copying process does not affect virtual and physical infrastructure resources, does not require creation of additional VM snapshots or VSS snapshots and does not produce load on machines whose backups are copied.

In Veeam Backup & Replication, backup copy is a job-driven process. To copy backups, you need to configure backup copy jobs. The backup copy job defines when, what, how and where to copy.

One backup copy job can be used to process one or multiple VMs. VMs included in the job are processed in parallel. If a VM included in the backup copy job has multiple disks, disks are processed sequentially, one after another.

On the target backup repository, the backup copy job creates a forever forward incremental backup chain. The target backup repository always contains only one active incremental backup chain. Restore points in the chain are rotated according to the retention policy. For more information, see [Retention Policy for Backup Copy Jobs](#).

How Backup Copy Works

Veeam Backup & Replication performs backup copy in the following way:

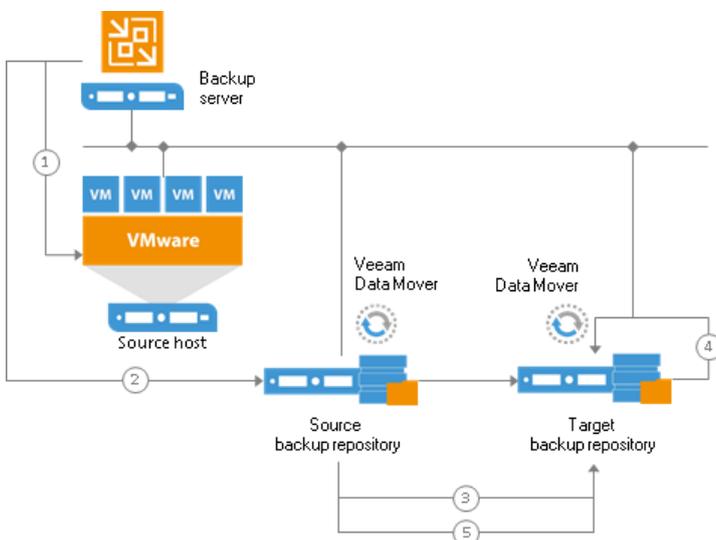
1. [For VM backup copy jobs only] Veeam Backup & Replication connects to vCenter Servers and ESX(i) hosts to gather information about VMs whose restore points you want to copy.
2. For backup copying process, Veeam Backup & Replication starts two Veeam Data Movers – source Veeam Data Mover and target Veeam Data Mover. Veeam Data Movers location depends on the backup repository type and data transport path. For more information, see [Backup Copy Architecture](#).
3. The first backup copy interval of the backup copy job always produces a full backup file. Veeam Backup & Replication copies data blocks that are necessary to build a full backup of a machine as of the most recent state.

Veeam Backup & Replication can copy data blocks from one or more backup files in the backup chain on the source backup repository.

- If the backup chain is created in the reverse incremental backup method, Veeam Backup & Replication copies data blocks of the latest full backup.
- If the backup chain is created in the forward or forever forward incremental backup method, Veeam Backup & Replication copies data blocks from the first full backup and a set of incremental backups.

To minimize the amount of traffic going over the network, Veeam Backup & Replication uses the data compression and deduplication technologies.

4. Veeam Backup & Replication transports copied data to the target backup repository and writes all copied data blocks to the full backup file.
 - If you do not enable the **Use per-VM backup files** option for the target backup repository, Veeam Backup & Replication creates one backup file on the target backup repository and stores to it data for all machines processed by the job.
 - If you enable the **Use per-VM backup files** option, data of every machine in the job is stored to separate backup files on the target backup repository.
5. During every next backup copy interval, when a new restore point appears on the source backup repository, Veeam Backup & Replication copies incremental changes from this most recent restore point and transfers them to the target backup repository. Veeam Backup & Replication writes the copied data blocks to the incremental backup file on the target backup repository.



Backup Copy Architecture

To transport data from the source backup repository to the target backup repository, the backup copy job uses one of the following paths:

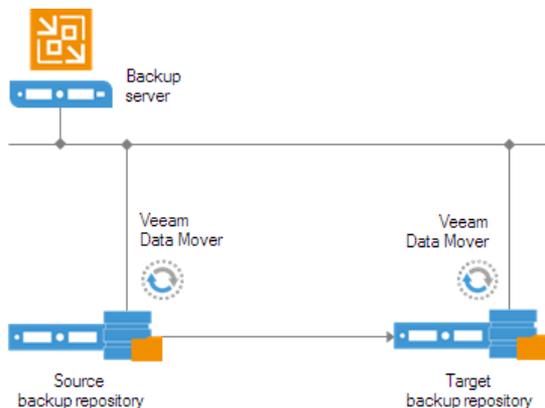
- [Direct transport path](#)
- [Transport path over WAN accelerators](#)

Direct Transport Path

Veeam Backup & Replication transports data directly from the source backup repository to the target backup repository. This type of data transport is recommended for copying backups to onsite backup repositories or offsite backup repositories over fast connections.

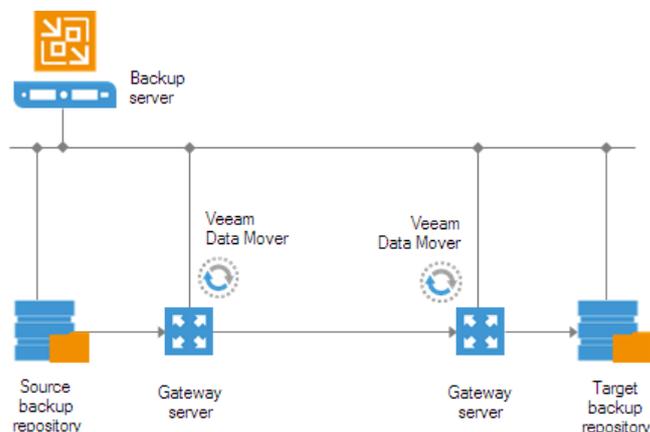
When Veeam Backup & Replication transports data over the direct data path, it uses Veeam Data Movers on the following backup infrastructure components:

- **Microsoft Windows and Linux repositories.** Veeam Backup & Replication uses the source Veeam Data Mover on the source backup repository and target Veeam Data Mover on the target backup repository.



- **Shared folder backup repository.** If you have instructed Veeam Backup & Replication to automatically select the gateway server, Veeam Backup & Replication will use Veeam Data Movers deployed on mount servers associated with backup repositories. In case mount servers cannot be used for some reason, Veeam Backup & Replication will fail over to the backup server.

If you have explicitly defined the gateway server, Veeam Backup & Replication will use the source Veeam Data Mover on the gateway server in the source site and target Veeam Data Mover on the gateway server on the target site.



Transport Path over WAN Accelerators

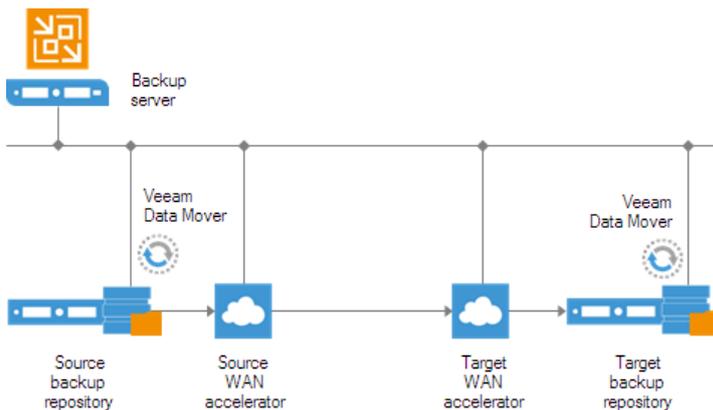
Veeam Backup & Replication transports data through a pair of WAN accelerators: one deployed on the source side and the other one deployed on the target side. WAN accelerators remove redundant blocks before transferring data and thus significantly reduce the amount of traffic going over the network. This type of data transport is recommended for copying backups offsite over slow connections or WAN.

IMPORTANT!

The WAN acceleration technology is available in the Enterprise Plus Edition of Veeam Backup & Replication. For more information, see [WAN Acceleration](#).

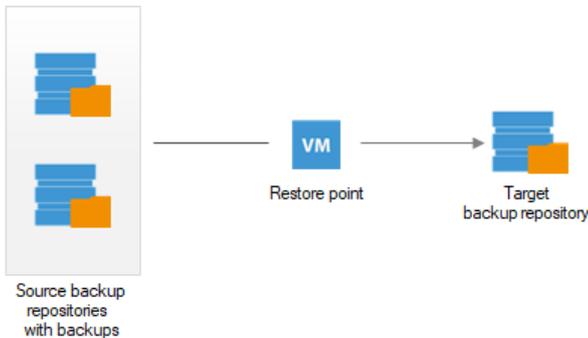
When Veeam Backup & Replication transports data via WAN accelerators, it uses Veeam Data Movers on the following backup infrastructure components:

- **Microsoft Windows and Linux repositories.** Veeam Backup & Replication uses the source Veeam Data Mover on the source backup repository and target Veeam Data Mover on the target backup repository.
- **Shared folder backup repository.** If you have instructed Veeam Backup & Replication to automatically select the gateway server, Veeam Backup & Replication will use the Data Mover Services deployed on the source and/or target WAN accelerator. If you have explicitly defined the gateway server, Veeam Backup & Replication will use the source Veeam Data Mover on the gateway server in the source site and target Veeam Data Mover on the gateway server on the target site.



Restore Point Selection

Veeam Backup & Replication does not necessarily use a backup created by one job and one backup repository as a source of data. It can copy data from backups created by different jobs and even from different backup repositories. When you set up a backup copy job, you only define what machines you want to process. During the backup copy job, Veeam Backup & Replication searches for the most recent restore point in all available backup repositories, copies data blocks from it and saves them to a backup file on the target backup repository.



You can specify a search scope for the backup copy job: that is, define in which backup repositories Veeam Backup & Replication should search for restore points. In this case, Veeam Backup & Replication will skip all other backup repositories from searching.

Veeam Backup & Replication always copies the most recent restore point from the source backup repository. Even when backup copying is performed for the first time and the source backup repository already contains a chain of restore points, Veeam Backup & Replication will only copy a restore point containing data as of the most recent machine state. For more information, see [How Backup Copy Works](#).

Veeam Backup & Replication identifies new restore points using the following rule:

```
Time of restore point creation >= current time - backup copy interval
```

For example, you have set the backup copy interval to 24 hours. Today's date and time are 7/1/2013, 12:00 PM and the restore point was created 23 hours ago, on 6/30/2013 at 1:00 PM. In this case, Veeam Backup & Replication will copy this new restore point:

```
6/30/2013, 1:00 PM >= 7/1/2013, 12:00 PM - 24 hours
```

The rule above is applied to all backup copy intervals, both the first one, copying a full backup file, and subsequent ones, copying incremental restore points. After you create a backup copy job and the first backup copy interval starts, Veeam Backup & Replication checks if there is some restore point falling into the necessary search scope on the source backup repository. If there is no restore point matching this condition, Veeam Backup & Replication will not copy data from the source backup repository. Instead, it will wait for the new restore point to appear on the source backup repository. Only after that Veeam Backup & Replication will copy the first, full restore point, to the target repository. This mechanism helps ensure that the backup chain produced by the backup copy job contains only the most recent machine data.

Limitations for Restore Points Selection

The backup copy job has the following limitations:

- Veeam Backup & Replication does not copy restore points from the target backup repository.
- Veeam Backup & Replication does not copy restore points from imported backups.

- Veeam Backup & Replication does not copy restore points that have already been copied by the same backup copy job to the target backup repository.
- Veeam Backup & Replication does not copy incomplete restore points.
- Veeam Backup & Replication does not copy restore points that are locked by the backup transformation process (merge, transform).
- [For target backup repositories with the **Use per-VM backup files** option disabled]
Veeam Backup & Replication does not copy restore points if the block size of the restore point on the source backup repository differs from the block size of restore points on the target backup repository.

The data block size for restore points on the target backup repository is set at the first backup copy interval of the backup copy job. This size is taken from the [corresponding settings](#) of the primary backup job – the backup job that creates the backup chain on the source backup repository. If after the first backup copy interval you add to the backup copy job new sources that use a different data block size, Veeam Backup & Replication will detect such restore points and display the *Restore point is located in backup file with different block size* message.

- [For target backup repositories with the **Use per-VM backup files** option enabled] One backup copy job can process machines with different block sizes. However, the block size for one machine must always stay the same.

For example, you have 2 source backups: *Backup1* contains *VM1* and *Backup2* contains *VM2*. The block size for *Backup1* is 1024 KB and block size for *Backup2* is 512 KB. The **Use-per VM backup files** option is enabled for the target backup repository. In this case, one backup copy job will successfully process VMs from *Backup1* and *Backup2*. However, if you change the block size for *VM1* to 256 KB and create *Backup3*, the backup copy job will not be able to copy VM data from such backup.

- If you select a backup job as a source for the backup copy job, Veeam Backup & Replication will only copy restore points created by this very backup job. Veeam Backup & Replication will not perform search in other backup repositories.

TIP:

You can configure several backup copy jobs to copy one restore point from the source backup repository to different target locations.

Backup Copy Job

The backup copy job is a separate task that needs to be set apart from the backup job.

The aim of the backup copy job is to copy a restore point from the source backup repository to the target backup repository. Every backup copy job creates its own folder on the target backup repository and stores to it all copied restore points. The folder has the same name as the backup copy job.

The backup copy job runs continuously and has several phases:

- [Idle state](#)
- [Synchronization process](#)
- [Transform operations](#)
- [Post-job activities](#)

Idle State

For the most time, the backup copy job remains in the idle state, waiting for a new restore point to appear on the source backup repository.

Synchronization Process

The synchronization process starts at backup copy intervals. You can define backup copy intervals needed in minutes, in hours or days.

At the beginning of a new interval, Veeam Backup & Replication checks if a new restore point is available on the source backup repository:

- If a new restore point is found, the backup copy job starts the synchronization process and copies the latest restore point from the source backup repository to the target backup repository.
- If a new restore point is not found or is locked by the source backup job, the backup copy job gets back to the idle state.

Transform Operations

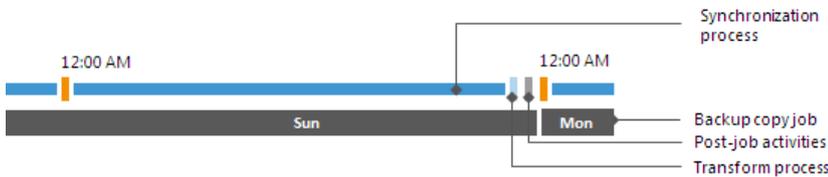
Veeam Backup & Replication can perform a number of additional transform operations on the target backup repository after the backup copying task or at the end of the backup copy interval. Transform operations include 3 tasks:

- **Backup chain transform.** When a new restore point is copied to the target backup repository, Veeam Backup & Replication checks the retention policy settings for the backup copy job. If the limit in restore points is exceeded, Veeam Backup & Replication transforms the backup chain to make room for a new restore point. For more information, see [Retention Policy for Backup Copy Jobs](#). After the transform process, Veeam Backup & Replication can perform additional operations: remove data for deleted machines from the backup chain and compact a full backup file.
- **Removal of deleted items.** In the backup copy job settings, you can select to maintain retention policy for deleted machines. In this case, Veeam Backup & Replication will check the list of machines included in the job and remove data for deleted machines from the backup chain on the target backup repository. For more information, see [Specifying Advanced Settings](#).
- **Full backup file compact.** In the backup copy job settings, you can select to periodically compact a full backup file to reduce its size and increase the speed of read and write operations. For more information, see [Compacting Full Backup File](#).

Post-Job Activities

In the backup copy job settings, you can instruct Veeam Backup & Replication to perform post-job activities, such as execution of custom scripts or sending job results by email. Post-job activities are performed after all transform operations are completed.

The synchronization process and transform operations make up a separate session of the backup copy job.



Backup Copy Intervals

When creating a backup copy job, you should specify its backup copy interval.

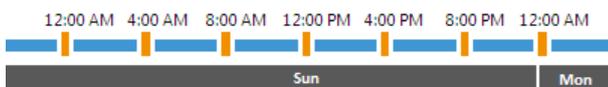
The backup copy interval is a time span in which the backup copy job must copy a restore point from the source backup repository to the target backup repository. When a new backup copy interval starts, Veeam Backup & Replication checks if a new restore point is available on the source backup repository. In case a new restore point is found, Veeam Backup & Replication copies it from the source backup repository to the target backup repository. Note that the duration of the backup copy interval affects the restore point selection process. For more information, see [Restore Point Selection](#).

You can specify the backup copy interval in minutes, hours or days.

Minutely and Hourly Backup Copy Intervals

If you set the backup copy interval in minutes or hours, Veeam Backup & Replication runs the backup copy process in cycles, one following another. When one backup copy interval is over, Veeam Backup & Replication starts a new backup copy interval.

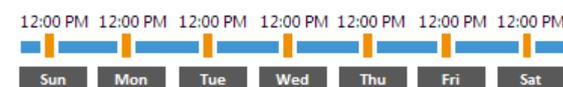
For example, if you set the backup copy interval to 4 hours and start the backup copy job at 12:00 AM, Veeam Backup & Replication will create new backup copy intervals at 12:00 AM, 4:00 AM, 8:00 AM and so on.



Daily Backup Copy Intervals

If you set the backup copy interval to 1 or more days, Veeam Backup & Replication requires that you define the start time for the backup copy interval. This start time acts as a milestone, or control point for the backup copy process. When the specified point in time occurs, Veeam Backup & Replication starts a new backup copy interval.

For example, if you set the backup copy interval to 1 day and instruct Veeam Backup & Replication to start a new interval at 12:00 PM, Veeam Backup & Replication will force a new backup copy interval at 12:00 PM daily.



In some cases, the start time of the backup copy job and the start time of the backup copy interval start may be different. For example, when configuring a backup copy job, you may set the start time of the backup copy interval to 12:00 PM and launch the backup copy job itself at 12:00 AM. In this case, the first backup copy interval will be started immediately after you launch the backup copy job, and will be run for a shorter period of time. In the example above, for 12 hours only instead of one day. All subsequent backup copy intervals will be started as defined by backup copy job schedule.

Backup Copy Window

If necessary, you can specify a window for the backup copy job. The backup copy window is a period of time when the backup copy job is allowed to transport data between source and target backup repositories. The backup copy window can be helpful if you do not want the backup copy job to produce unwanted overhead for the production environment or do not want the job to overlap the production hours. In this case, you can define the time interval in which the job must not transfer backup data.

The backup copy window affects only the data transport process; transform operations performed on the target repository are not affected by the backup copy window. The backup copy job behavior during the 'prohibited' period of time depends on the length of the backup copy interval:

- If the backup copy interval is greater than the 'prohibited period', the backup copy job will put on hold the backup copying operations and wait for allowed hours. The backup copy job is put to the *Idle* state and remains in this state for the whole "prohibited period".
- If the backup copy interval is smaller than the 'prohibited period', Veeam Backup & Replication will finish all backup copy job sessions that must run during the 'prohibited period' with the *Failed* status. During the first backup copy interval on allowed hours, Veeam Backup & Replication will copy the restore point to the target backup repository. The copied restore point will contain all data for the 'prohibited period'. That is, it will aggregate all data that has changed between the latest restore point on the target backup repository and latest restore point on the source backup repository.



For example, you have set the backup copy interval to 2 hours and defined the backup copy window from 8 PM to 8 AM. Without the backup copy window, Veeam Backup & Replication would transport 6 restore points to the target backup repository between 8 AM and 8 PM. With the backup window, the backup copy job will not copy data from 8 AM to 8 PM. At 8 PM, however, a new backup copy interval will start. Veeam Backup & Replication will transport one restore points from the source backup repository. This restore point will contain data for those 6 restore points that might have been copied during the 'prohibited period' plus one that must be created within this new backup copy interval.

Automatic Job Retries

Veeam Backup & Replication automatically retries several operations that are performed within a backup copy job sessions.

Job Tasks Retry

By default, Veeam Backup & Replication automatically retries a failed backup copy task 5 times within one backup copy job session. A new task is started immediately after the previous one, without any interval.

The backup copy task is retried only if the previous task has failed and a restore point has not been copied to the target backup repository. Veeam Backup & Replication does not perform a retry if a task has finished with the *Success* or the *Warning* status.

The backup copy task is retried during the same backup copy interval only. If a restore point fails to be copied during all retries in the current backup copy interval, Veeam Backup & Replication marks the synchronization task as failed and waits for the expiration of the backup copy interval. After that, Veeam Backup & Replication performs the necessary transform operations and starts a new backup copy interval.

A backup copy job can process several machines. If only some machines are successfully processed by the backup copy task, Veeam Backup & Replication creates a restore point holding data for these machines on the target backup repository. Veeam Backup & Replication will attempt to process restore points for all machines during the next backup copy interval.

NOTE:

Some errors from WAN accelerators can block backup copy job retries. For example, if there is no space in the global cache on the target WAN accelerator, Veeam Backup & Replication put backup copying operations on hold and wait for the expiration of the backup copy interval.

Transform Retry

After the backup copying task, Veeam Backup & Replication performs a number of additional transform operations on the target backup repository if necessary. These operations include the backup chain transform, removing of deleted machines from restore points and compacting a full backup file. For more information, see [Backup Copy Job](#).

Veeam Backup & Replication may fail to perform transform operations for some reason: for example, if the backup file on the target backup repository is locked by the file-level restore session. By default, Veeam Backup & Replication automatically retries transform operations for 5 times. The first interval between retries is 1 minute; the interval doubles with every new attempt. If Veeam Backup & Replication fails to perform transform operations during all retries in this backup copy interval, the job is put to the idle state, waiting for the new backup copy interval to begin.

Virtual Infrastructure Access Retry

At the beginning of every backup copy interval, Veeam Backup & Replication accesses the virtual infrastructure to make up a list of machines processed by the job.

Veeam Backup & Replication may fail to access the virtual infrastructure for some reason: for example, in case the vCenter Server is not responding. By default, Veeam Backup & Replication automatically retries access operations for 5 times with a 5 minute interval.

Backup Copy Job Issues

Being a scheduled activity, the backup copy job may fail to run as expected. Veeam Backup & Replication automatically handles some issues that can occur with the backup copy job.

Short Backup Copy Intervals

In some cases, Veeam Backup & Replication may fail to transport the restore point within the backup copy interval of the backup copy job. This can happen, for example, if the backup copy interval is too short and is not sufficient for the amount of data to be copied.

Veeam Backup & Replication handles this situation differently for the first and subsequent backup copy intervals.

- The first backup copy interval always produces a full backup file — the starting point in the backup chain. If Veeam Backup & Replication fails to copy data for the full backup file during the first backup copy interval, it marks the job session as finished with the *Warning* status. During the next backup copy interval, Veeam Backup & Replication attempts to copy data for the full backup file in the following manner:
 - a. When a new backup copy interval begins, the restore point that was previously copied no longer corresponds to the [restore point selection rules](#). That is, the time of the restore point creation falls out of the search scope. For this reason, Veeam Backup & Replication waits for a new restore point to appear on the source backup repository.
 - b. When a new restore point appears on the source backup repository, Veeam Backup & Replication detects what data blocks still need to be copied to make up a full backup file on the target backup repository, and copies these data blocks.

This process continues until there is a full backup file on the target backup repository.

- At subsequent backup copy intervals, Veeam Backup & Replication copies incremental restore points. If Veeam Backup & Replication fails to transport an incremental restore point, it marks the synchronization task as failed. Veeam Backup & Replication waits for the expiration of the backup copy interval; after that, Veeam Backup & Replication marks the job session as finished with the *Error* status.

Veeam Backup & Replication does not mark the backup copy job session with the *Error* status in the following cases:

- The source backup job has not started during the backup copy interval of the backup copy job (that is, the backup copy job has nothing to copy to the target backup repository).
- A task in the backup copy job processes a VM template, and the source backup job is set to exclude the VM template during incremental backup jobs sessions.

Simultaneous Use of Backup Files

In some cases, the source backup job and backup copy job may overlap. Such situation can occur, for example, if the source backup job needs to transform the source backup chain.

If a specific task in the backup copy job locks the source backup chain to read data from it, and the source backup job that needs to write data to this backup chain starts at this moment (for example, for reverse incremental backup), the task in the backup copy job is put on hold. The backup copy job can continue processing other tasks that use other sources (for example, backup files created by other backup jobs). After the source backup job releases the backup chain, the backup copy job resumes processing machines in this backup chain.

Change of the Backup Copy Interval Start Time

If you have selected to run a backup copy job with a daily backup copy interval, you must define the start time of the backup copy interval. However, you may want to change the start time afterwards. After the start time change, Veeam Backup & Replication behaves in the following manner:

1. Veeam Backup & Replication finishes the current backup copy interval running according to the 'old' start time value as usual.
2. After the current backup copy interval is over, Veeam Backup & Replication immediately starts the backup copy interval, not waiting for the 'new' start time point to come. At that, Veeam Backup & Replication "stretches" the started interval: the interval lasts for the time remaining till the new start time plus the time of the backup copy interval itself.

3. All subsequent backup copy intervals are created and started in a regular manner by the new schedule.

For example, when you first created a backup copy job, you set a daily backup copy interval with the start time at 8 AM. After that, you changed the start time to 10 AM. In this case, Veeam Backup & Replication will first finish the backup copy interval that is currently running – that is, the backup copy interval that was started at 8 AM – as usual. After that, it will immediately start a new backup copy interval. This interval will run for 26 hours – from 8 AM of the current day until 10 AM of the next day. All subsequent backup copy intervals will be started at 10 AM every day.

The first backup copy interval that is run after the start time change is typically longer than a regular one. This happens because of the backup copy interval “stretch” mentioned above. To start the synchronization process right away, you can use the **Sync Now** option after you change the start time value. In this case, Veeam Backup & Replication will behave in the following manner:

1. When you start the synchronization process manually, Veeam Backup & Replication forcibly finishes the current backup copy interval and begins a new backup copy interval according to the new start time value. This backup copy interval lasts until a new backup copy interval by the new schedule must be started.
2. All subsequent backup copy intervals are created and started in a regular manner.

As a result, the first backup copy interval after the start time change will begin immediately.

For example, when you first created a backup copy job, you set a daily backup copy interval with the start time at 8 AM. After that, you changed the start time to 10 AM. On the start time change, you started the manual synchronization process at 1 PM. In this case, Veeam Backup & Replication will finish the current backup copy interval – that is, the backup copy interval that was started at 8 AM – immediately at 1 PM. After that, it will start a new backup copy interval. This interval will run for 21 hours – from 1 PM of the current day until 10 AM of the next day. All subsequent backup copy intervals will be started at 10 AM every day.

Retention Policy for Backup Copy Jobs

The retention policy of a backup copy job does not depend on retention policy settings of the source backup job. The backup copy job has its own retention policy settings. The retention policy of a backup copy job defines for how long Veeam Backup & Replication must retain copied restore points on the target backup repository.

Veeam Backup & Replication offers two retention policy schemes for backup copy jobs:

- [Simple Retention Policy](#)
- [GFS Retention Policy](#)

Simple Retention Policy

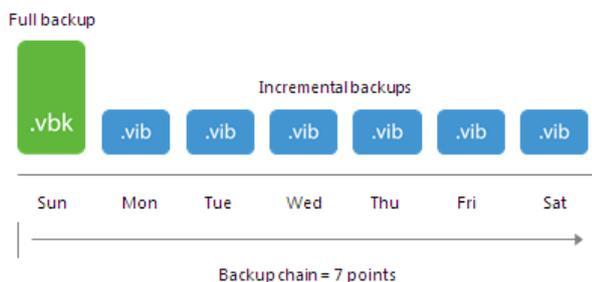
A simple retention policy scheme is intended for short-time archiving. When you specify retention policy settings for a simple scheme, you define how many restore points you want to retain on the target backup repository.

With the simple retention policy scheme, Veeam Backup & Replication creates a chain of restore points that subsequently follow one another. The first restore point in the chain is always a full backup (also known as a recent full backup). All other restore points in the chain are incremental backups.

By default, Veeam Backup & Replication keeps 7 restore points on the target backup repository.

NOTE:

The minimum number of restore points that you can keep with the simple retention policy scheme is 2.

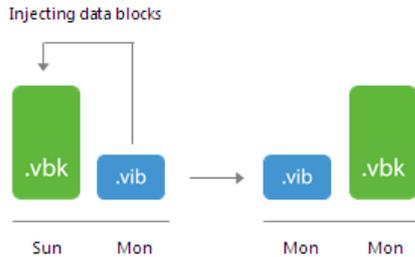


To maintain a desired number of restore points in the backup chain, Veeam Backup & Replication uses the forever forward incremental scheme.

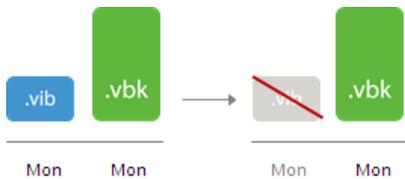
1. During the first backup copy interval, Veeam Backup & Replication creates the first restore point (full backup) on the target backup repository.
2. During every subsequent backup copy interval, Veeam Backup & Replication adds a new restore point (incremental backup) to the backup chain on the target backup repository. This happens until the number of restore points in the backup chain reaches the number specified in the retention policy settings.
3. After the new restore point is added, the allowed number of restore point is exceeded. Veeam Backup & Replication transforms the backup chain to make room for the most recent restore point.

The backup chain transformation is performed in the following way:

1. Veeam Backup & Replication re-builds the full backup file to include changes from the incremental backup following the full backup. More specifically, Veeam Backup & Replication injects data blocks from the first incremental backup in the chain into the full backup. This way, the full backup 'moves' one step forward in the backup chain.

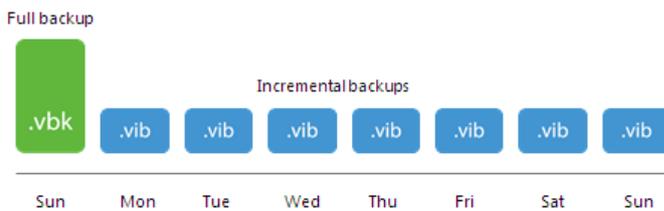


2. Veeam Backup & Replication removes the first incremental backup from the chain as redundant. Data of the redundant incremental backup file has already been injected into the full backup, and so the full backup file contains the same data as this incremental backup.



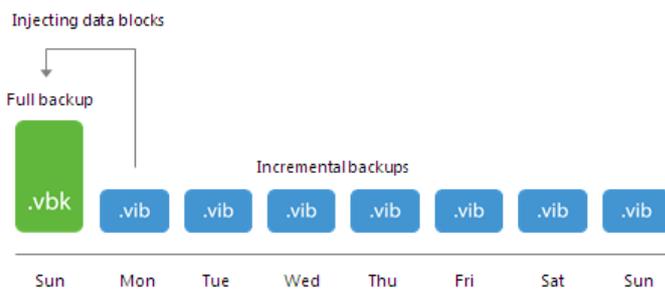
For example, you want a backup copy job to keep 7 restore points. The backup copy interval is 1 day; the backup copy job starts on Sunday.

1. During the first backup copy interval on Sunday, Veeam Backup & Replication creates the first restore point – a full backup. Monday through Saturday Veeam Backup & Replication adds six incremental backups to the backup chain.
2. The next Sunday, Veeam Backup & Replication adds a new incremental backup to the backup chain. The number of allowed restore point in the backup chain is exceeded.

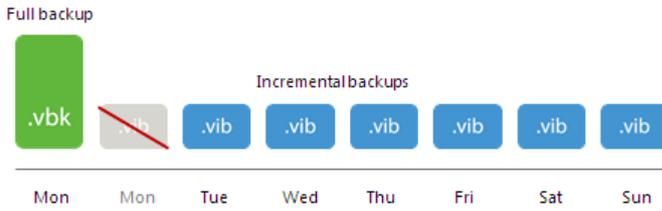


For this reason, Veeam Backup & Replication transforms the backup chain in the following way:

1. Veeam Backup & Replication merges data blocks from the incremental backup copied on Monday into the full backup copied on Sunday. This way, the full backup file 'moves' one step forward – from Sunday to Monday.



- The incremental backup copied on Monday becomes redundant, and Veeam Backup & Replication removes it from the backup chain. As a result, you have a chain of a full backup as of Monday and six incremental backups Tuesday through Sunday.



GFS Retention Policy

In most cases, simple backup retention policy is not enough. You cannot store an unlimited number of restore points on the target backup repository forever – it is not rational and is resource consuming. If you want to retain copied data for longer periods of time, you can enable the GFS retention policy scheme for backup copy jobs.

The GFS, or Grandfather-Father-Son retention policy is a backup rotation scheme intended for long-term archiving. It lets you keep backups of machines for an entire year and requires minimum amount of storage space. GFS backups are always full backup files that contain data of the whole machine image as of specific date.

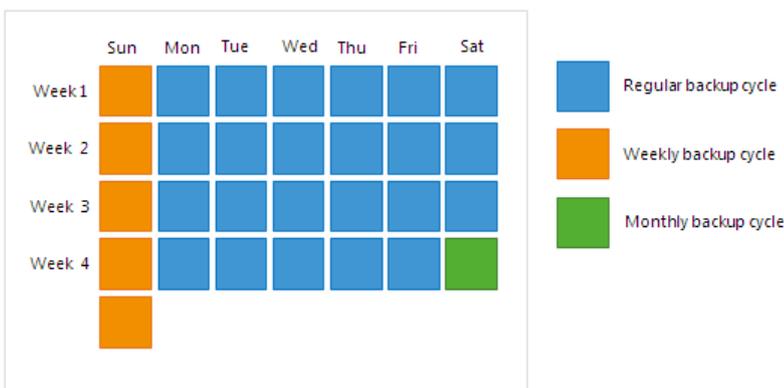
GFS is a tiered retention policy scheme. It uses a number of cycles to retain backups for different periods of time:

- Regular backup cycle
- Weekly backup cycle
- Monthly backup cycle
- Quarterly backup cycle
- Yearly backup cycle

In the GFS retention policy scheme, weekly backups are known as 'sons', monthly backups are known as 'fathers' and yearly backup are known as 'grandfathers'. Additionally, Veeam Backup & Replication maintains quarterly backups. Weekly, monthly, quarterly and yearly backups are also called archive backups.

IMPORTANT!

You cannot enable GFS retention settings if you use a backup repository with rotated drives as the target backup repository.



Methods for Archive Backups Creation

You can instruct Veeam Backup & Replication to create archive full backups with the following methods:

- [Synthetic full method](#) – Veeam Backup & Replication synthesizes archive full backups using restore points on the target backup repository.
- [Active full method](#) – Veeam Backup & Replication copies data for archive full backups from the source backup repository.

Synthetic Full Method for Archive Backups

The synthetic full backup is the default method to create archive full backups. Veeam Backup & Replication does not copy data for archive full backups from the source backup repository. It synthesizes archive full backups from backup files that are already stored on the target backup repository. This approach helps reduce load on the network and production environment.

To use the synthetic full method, you must leave the **Read the entire restore point from source instead of synthesizing it from increments** check box not selected in backup copy job settings.

NOTE:

The synthetic full method is not recommended if you use a deduplication storage appliance as a target backup repository. Performing a synthetic full backup on such repositories requires additional time and resources to download and decompress backup data blocks.

This recommendation does not apply to HPE StoreOnce, Dell EMC Data Domain and ExaGrid:

- HPE StoreOnce and Dell EMC Data Domain use virtual synthetics. Veeam Backup & Replication creates archive full backups by virtually synthesizing data blocks from existing backup files.
- ExaGrid uses adaptive deduplication. Veeam Backup & Replication creates archive full backups from existing backup files that are stored in complete form in ExaGrid high-speed cache.

The screenshot shows the 'New Backup Copy Job' dialog box with the 'Target' tab selected. The 'Target' section includes a description: 'Specify the target backup repository, amount of most recent restore points to keep, and retention policy for full backups. You can use map backup functionality to seed the backup files.' The 'Backup repository' is set to 'Scale-out Backup Repository (Extensible Backup Repository)' with 109 GB free of 399 GB. The 'Restore points to keep' is set to 7. There is a checked option 'Keep the following restore points as full backups for archival purposes' with a 'Schedule...' button. The backup schedule is configured as follows: Weekly backup: 4, Sunday; Monthly backup: 0, First Sunday of the month; Quarterly backup: 0, First Sunday of the quarter; Yearly backup: 0, First Sunday of the year. There is an unchecked option 'Read the entire restore point from source backup instead of synthesizing it from increments'. At the bottom, there is an 'Advanced' button and navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Active Full Method for Archive Backups

You can instruct Veeam Backup & Replication to create archive full backups (backups retained by the GFS scheme) with the active full backup method. The active full backup method is recommended if you use a deduplicating storage appliance as the target backup repository. Active full backup helps improve the backup job performance and reduce the load on the target backup repository.

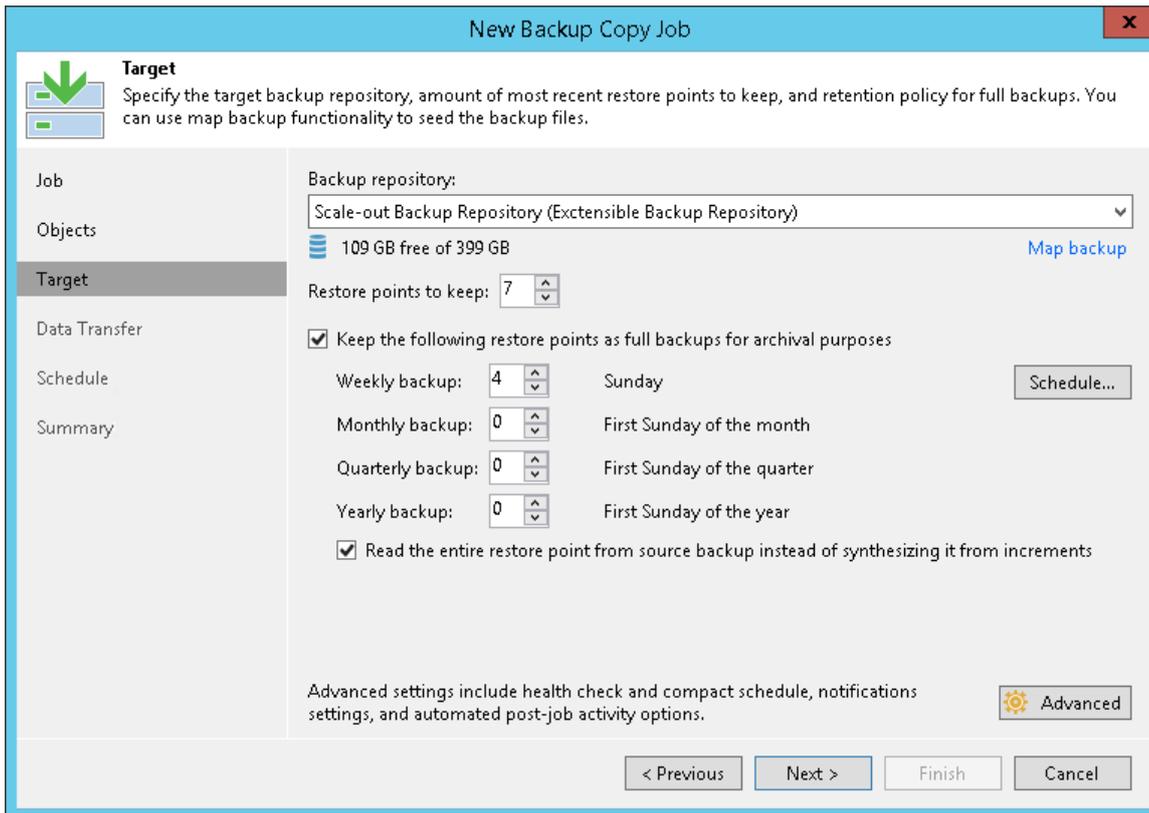
By default, Veeam Backup & Replication uses the synthetic backup method to create archive full backups. However, synthesizing archive full backups can cause problems with storage performance on deduplicating storage appliances. Deduplicating storage appliances are optimized for sequential data access. The synthetic backup creation, however, takes random I/O operations — Veeam Backup & Replication reads data from existing backup files and writes data to the synthesized archive full backup file. As a result, the storage performance can degrade.

In addition, backups reside on the target backup repository in the deduplicated and compressed state. Before creating synthetic full backups, Veeam Backup & Replication needs to download and decompress data blocks of backups, which requires additional time and resources.

To optimize the backup copy job performance on deduplicating storage appliances, you can enable the **Read the entire restore point from source instead of synthesizing it from increments** option in the backup copy job settings. Veeam Backup & Replication will copy data for the archive full backup from restore points on the source backup repository, transport it to the target backup repository over the network and write it to the archive full backup file. The load on the network will be higher but the performance of the deduplicating storage appliance will increase.

NOTE:

If data transfer does not fit the backup copy interval, the backup copy interval is extended.



Retention Policy for Active Full Archive Backups

If you enable the **Read the entire restore point from source instead of synthesizing it from increments** option, Veeam Backup & Replication stops transforming the backup chain with every backup copy interval, and no longer uses the forever forward incremental backup method to maintain the desired number of restore points in the backup chain. Instead, it applies retention rules of the forward incremental backup method to the backup chain. For more information, see [Forward Incremental Backup Retention Policy](#).

Veeam Backup & Replication waits until the number of restore points in the new backup chain is greater than the retention policy setting, and then removes restore points from the previous backup chain. Archive full backups remain on disk because Veeam Backup & Replication applies a separate retention policy scheme to archive full backups.

For example, you have configured a backup copy job in the following way:

- The backup copy job starts on Sunday; the backup copy interval is equal to 1 day and starts at 12:00 AM.
- Simple retention policy is set to 4.
- Weekly full backups are enabled, Thursday is selected in the [full backup schedule settings](#).

- The **Read the entire restore point from source instead of synthesizing it from increments** option is enabled.

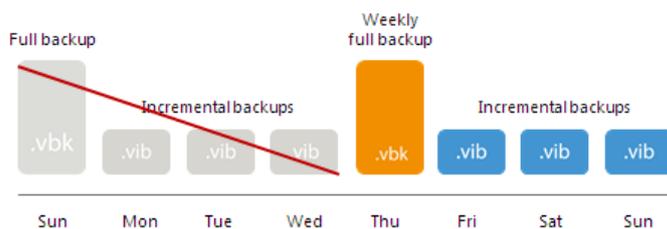
Veeam Backup & Replication will run the backup copy job in the following way:

1. During the first 4 backup copy intervals, Sunday through Wednesday, Veeam Backup & Replication will create a full backup and 3 incremental backups.
2. On Thursday, Veeam Backup & Replication will add a weekly full backup to the backup chain.

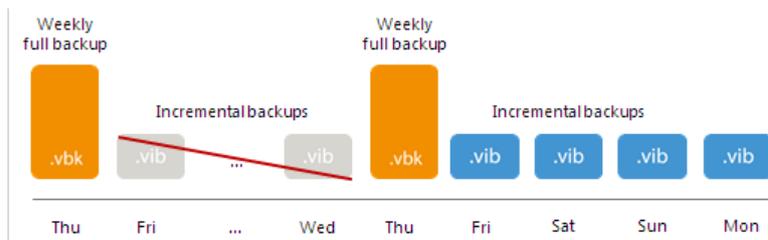
IMPORTANT!

If the daily interval start time is different from 12:00 AM, Veeam Backup & Replication will create a weekly full backup 1 day prior to the day selected in the full backup schedule settings. For more information, see [Active Weekly Full Backups](#).

3. Friday through Sunday, Veeam Backup & Replication will add incremental backups to the new backup chain. On Sunday, Veeam Backup & Replication will remove the whole previous backup chain.



4. Veeam Backup & Replication will keep on adding incremental backups to the backup chain until the next Thursday. On Thursday, Veeam Backup & Replication will create a new weekly full backup.
5. Friday through Sunday, Veeam Backup & Replication will add incremental backups to the new backup chain.
6. On Monday, Veeam Backup & Replication will add a new incremental backup to the new backup chain, and remove incremental backups from the previous backup chain. The weekly full backup will remain on disk.



Switching Between Synthetic and Active Full Modes

In some cases, you may want to change the algorithm of archive full backup creation. You can perform the following operations:

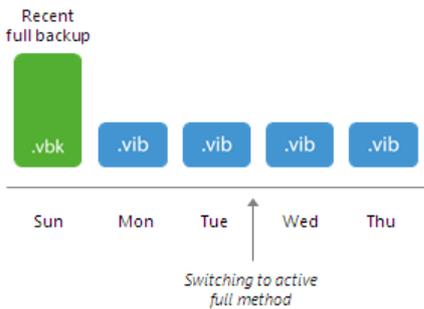
- [Switch from the synthetic to the active full mode](#)
- [Switch from the active full to the synthetic mode](#)

Switching from Synthetic to Active Full Method

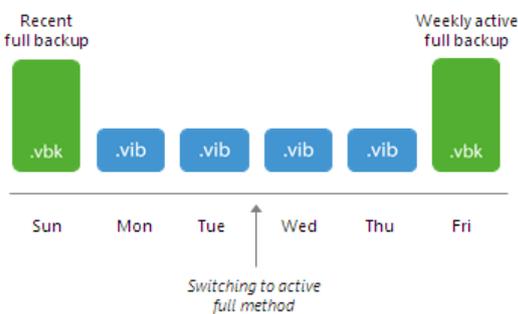
After you switch from the synthetic to the active full method of archive backup creation, Veeam Backup & Replication does not perform synthetic transform operations for some time.

Veeam Backup & Replication works in the following way:

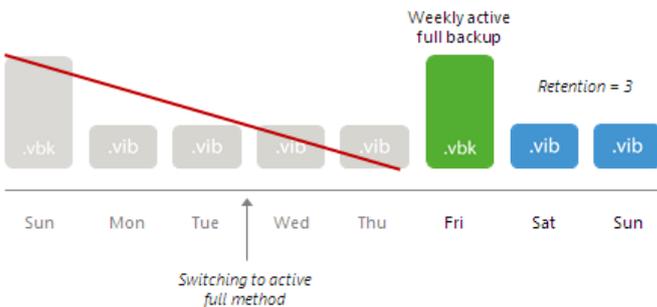
1. Veeam Backup & Replication will add new incremental restore points to the backup chain and keeps existing restore points until a new active full backup is created.



2. Veeam Backup & Replication will add a new active full backup to the backup chain.



3. Veeam Backup & Replication will keep adding new incremental restore points to the backup chain. When the number of restore points in the new backup chain is equal to the number allowed by retention, Veeam Backup & Replication will remove incremental restore points that precede the new active full backup.



After this, Veeam Backup & Replication will use the new method to create the backup chain in a regular manner.

Switching from Active Full to Synthetic Method

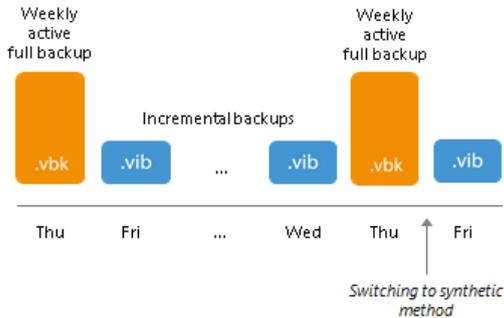
Scenario 1. The backup chain does not contain archive full backup files

In this case, Veeam Backup & Replication will work by the standard archive full backup scheme. For more information, see [Weekly Backup Cycle](#).

Scenario 2. The backup chain contains full backups (recent or archive)

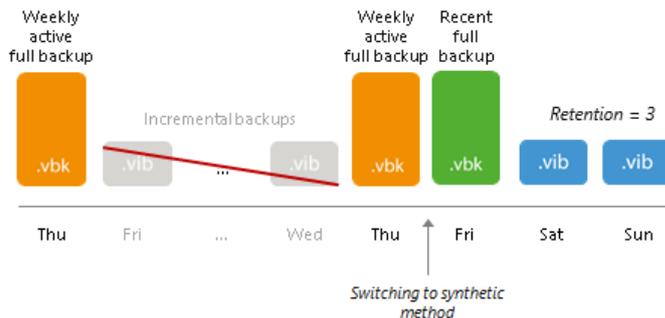
After you switch from the active full to the synthetic method of archive backup creation, Veeam Backup & Replication works in the following way:

1. During the first backup copy interval after the switch, Veeam Backup & Replication will add a new incremental restore point to the recent backup chain.



2. Veeam Backup & Replication will keep adding new incremental restore points to the recent backup chain. When the number of restore points in the recent backup chain is equal to the number allowed by retention, Veeam Backup & Replication will build a recent full backup out of the latest archive full and the first incremental restore point in the new backup chain.

After that, Veeam Backup & Replication will remove all incremental restore points from preceding backup chains. If there are any outdated archive full backups, Veeam Backup & Replication will remove them, too.



Subsequent backup copy intervals work according to the standard retention scheme for the synthetic full method of archive backups. For more information, see [Weekly Backup Cycle](#).

NOTE:

Veeam Backup & Replication normally creates one archive full backup per GFS cycle. However, when you switch from active to synthetic backup method or change scheduling settings for synthetic full backups, Veeam Backup & Replication will create and keep in the backup chain two archive full backups marked with the same flag. For details, see [Archive Full Backups per GFS Cycle](#).

GFS Cycles

Veeam Backup & Replication uses a number of cycles to retain backups for different periods of time according to the GFS retention scheme:

- [Regular backup cycle](#)
- [Weekly backup cycle](#)
- [Monthly backup cycle](#)

- [Quarterly backup cycle](#)
- [Yearly backup cycle](#)

IMPORTANT!

The full backup can be marked as weekly, monthly, quarterly and/or yearly. When transforming weekly, monthly, quarterly and yearly backup chains, Veeam Backup & Replication checks flags set for the full backup file. If the full backup file belongs to some other retention policy tier and must be retained on the target backup repository, such backup file will not be removed.

Regular Backup Cycle

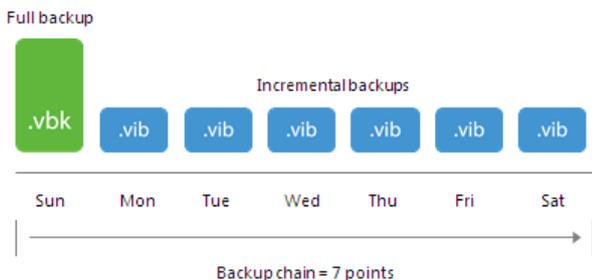
The regular backup cycle is based on the simple retention policy scheme. When you specify retention policy settings, you define how many restore points you want to retain in the backup chain on the target backup repository.

Veeam Backup & Replication runs the regular backup cycle in the following way:

1. During the first backup copy interval, Veeam Backup & Replication creates the first restore point – a full backup.
2. The next backup copy intervals add incremental backups to the backup chain.

As a result, the regular backup cycle produces a chain of a full backup and set of incremental backups on the target backup repository.

For example, you have selected to retain 7 restore points. The backup copy interval is 1 day, the backup copy job starts on Sunday. Veeam Backup & Replication will create a full backup on Sunday and add 6 incremental backups Monday through Saturday.



Weekly Backup Cycle

In the GFS scheme, the weekly backup is created during the weekly backup cycle.

Weekly backup cycles always produce full backup files that contain data of the whole machine image as of specific date. When you define retention policy settings for the weekly backup cycle, you specify how many weekly backups you want to retain and define the week day on which the weekly full backup must be created.

Veeam Backup & Replication creates weekly full backups for synthetic and active full backup methods in different ways:

- [Synthetic weekly full backups](#)
- [Active weekly full backups](#)

Synthetic Weekly Full Backups

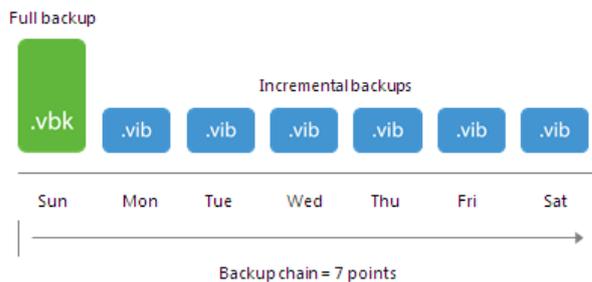
Veeam Backup & Replication does not use a separate task to create weekly full backups.

Veeam Backup & Replication re-uses a full backup created in the regular backup cycle and propagates this full backup to the weekly tier.

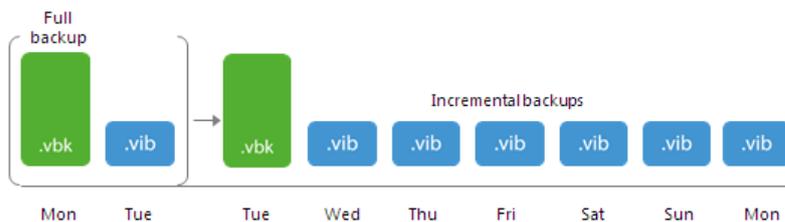
Veeam Backup & Replication creates a weekly full backup in the following way:

1. Veeam Backup & Replication creates a chain of backups in the regular backup cycle. The chain consists of a full backup and set of subsequent incremental backups.

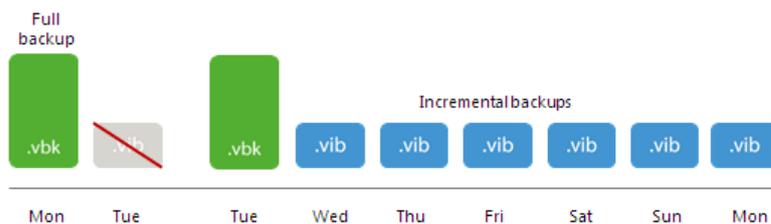
For example, you have selected to keep 7 restore points. The backup copy interval is 1 day, the backup copy job starts on Sunday. During the week, Veeam Backup & Replication creates a backup chain on the target backup repository. The backup chain consists of a full backup copied on Sunday and a set of incremental backups copied Monday through Saturday.



2. With every new backup copy interval, Veeam Backup & Replication transforms the backup chain and moves the full backup forward. This procedure repeats until the full backup file reaches the day when the weekly backup is scheduled.
3. During the backup copy interval on this day, Veeam Backup & Replication transforms the backup chain and creates a weekly full backup at the same time. This process is performed in the following way:
 - a. Veeam Backup & Replication adds a new restore point to the backup chain.
 - b. As the allowed number of restore points is exceeded, Veeam Backup & Replication transforms the backup chain. The transformation process slightly differs from a regular one. Veeam Backup & Replication does not inject data from the incremental backup to the full backup. Instead, it copies data from full and incremental backups and stores them to a new full backup file, next to the primary backup file.

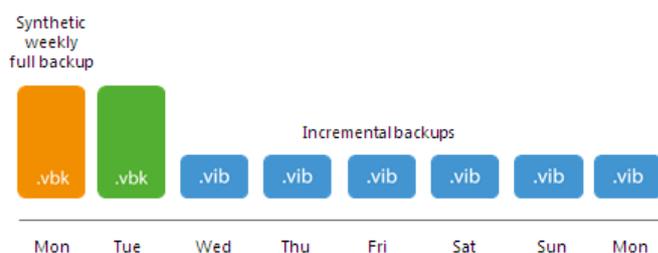


4. The incremental backup from which data was copied is removed as obsolete.



5. The primary full backup file remains on the target backup repository. Veeam Backup & Replication sets it aside and marks it as a weekly full backup. The weekly backup is no longer used in the backup chain.

- The newly created full backup file remains in the backup chain and is used as a starting point for incremental backups created by the regular backup cycle.



For example, weekly backup is scheduled on Monday. Veeam Backup & Replication will keep transforming the backup chain until the full backup file reaches Monday. During the next backup copy interval, Veeam Backup & Replication will transform the backup chain. To do that, it will copy data from the Monday full backup and Tuesday incremental backup to a new full backup file and store it next to the primary full backup file.

As a result, on the target backup repository you will have a full backup created on Monday and a backup chain that includes a full backup as of Tuesday and a chain of increments Wednesday through Monday. The full backup as of Monday will be marked as a weekly backup and set aside. The full backup as of Tuesday will be used as a new starting point in the backup chain.

NOTE:

Veeam Backup & Replication normally creates one archive full backup per GFS cycle. However, when you switch from active to synthetic backup method or change scheduling settings for synthetic full backups, Veeam Backup & Replication will create and keep in the backup chain two archive full backups marked with the same flag. For details, see [Archive Full Backups per GFS Cycle](#).

Active Weekly Full Backups

Veeam Backup & Replication copies data from the source backup repository and saves it to the full backup file on the target backup repository. The created full backup file is marked as a weekly full backup.

Weekly Full Backup Creation

To let Veeam Backup & Replication create active weekly full backups, you must configure the full backup schedule settings for the backup copy job. For more information, see [Step 7. Define Backup Copy Target](#).

When you select the day in the full backup schedule settings, Veeam Backup & Replication understands 12:00 AM on this day as a reference point for creating full backups. For example, you selected Thursday. The reference point for Thursday is "Thursday, 12:00 AM".

For backup copy jobs with backup copy intervals of 1 day, Veeam Backup & Replication creates weekly full backups by the following rules:

- If the backup copy interval start time is different from 12:00 AM, the full backup is created 1 day prior to the selected day.
- If the backup copy interval start time is 12:00 AM, the full backup is created on the selected day.

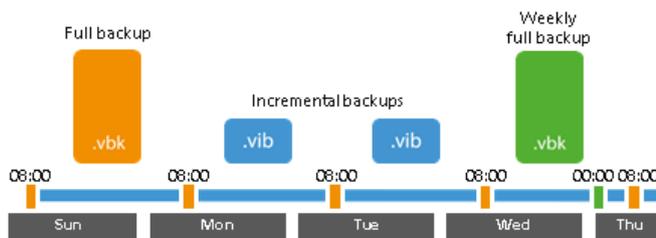
Scenario A

You have configured the backup copy job schedule settings in the following way:

- The backup copy job starts on Sunday; the backup copy interval is equal to 1 day and starts at 8:00 AM.
- You selected Thursday as the day when weekly full backups must be created.

Veeam Backup & Replication will perform the backup copy job in the following way:

1. The backup copy job will create a full backup on its first run.
2. Veeam Backup & Replication will check if "Thursday, 12:00 AM" reference point lies within the backup copy interval:
 - a. Backup copy intervals that start on Monday and Tuesday do not include the reference point. Veeam Backup & Replication adds incremental backups to the backup chain on these days.
 - b. Veeam Backup & Replication extends the interval from "Wednesday 08:00 AM - Thursday 08:00 AM" to "Wednesday 00:00 AM - Thursday 08:00 AM".
Veeam Backup & Replication detects that "Thursday, 00:00 AM" reference point lies within the backup copy interval "Wednesday 00:00 AM - Thursday 08:00 AM" and creates a weekly full backup on Wednesday.
 - c. On Thursday Veeam Backup & Replication adds an incremental backup.



Scenario B

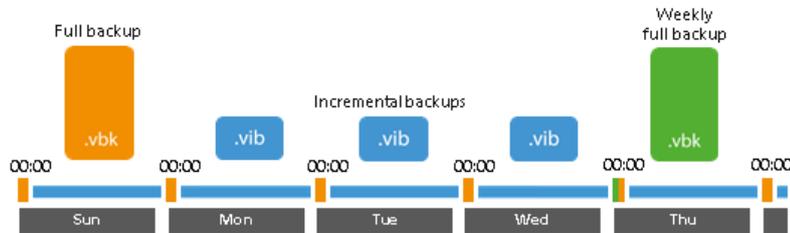
You have configured the backup copy job schedule settings in the following way:

- The backup copy job starts on Sunday; the backup copy interval is equal to 1 day and starts at 12:00 AM.
- You selected Thursday as the day when weekly full backups must be created.

Veeam Backup & Replication will perform the backup copy job in the following way:

1. The backup copy job will create a full backup on its first run.
2. Veeam Backup & Replication will check if "Thursday, 12:00 AM" reference point lies within the backup copy interval:
 - a. Backup copy intervals that start on Monday, Tuesday and Wednesday do not include the reference point. Veeam Backup & Replication adds incremental backups to the backup chain on these days.

- b. Veeam Backup & Replication detects that "Thursday, 12:00 AM" reference point is the same as the "Thursday 00:00 AM - Friday 00:00 AM" interval start time and creates a weekly full backup on Thursday.



Veeam Backup & Replication applies the described weekly full backup creation rules to jobs with minutely and hourly backup copy intervals.

Weekly Full Backup Retention

Veeam Backup & Replication repeats the weekly backup cycle until the number of weekly backups allowed by the retention policy is exceeded. After that, Veeam Backup & Replication removes the earliest active weekly full backup from the target backup repository to make room for the most recent active weekly full backup.

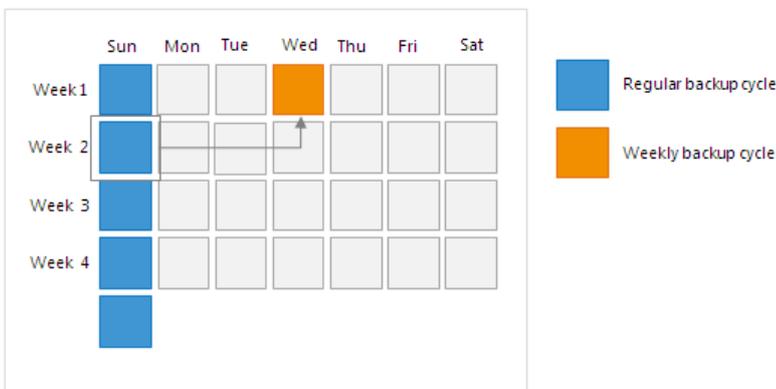
Veeam Backup & Replication treats active weekly full backups as regular full backups, and applies regular retention policy rules to maintain the necessary number of restore points in the backup chain. For more information, see [Retention Policy for Active Full Archive Backups](#).

Restore Point Selection for Weekly Backup (Synthetic Method)

Typically, when a weekly full backup is created, Veeam Backup & Replication takes a full backup as of this day and marks it as a weekly backup. In some cases, however, Veeam Backup & Replication may fail to find a full backup on the day when the weekly backup is scheduled. In this situation, Veeam Backup & Replication will use the nearest full backup file created within the next backup copy interval.

For example, you have set the backup copy interval to 1 week and started the backup copy job on Sunday. As a result, a new restore point is created every Sunday. When Veeam Backup & Replication transforms the backup chain, the full backup moves from the previous Sunday to the next Sunday.

Imagine the weekly backup is scheduled on Wednesday. As all backups are created on Sunday, Veeam Backup & Replication will not find a full backup as of Wednesday. For this reason, it will use the full backup from the next backup copy interval – a full backup as of Sunday.



Monthly, Quarterly and Yearly Backup Cycles

Monthly, quarterly and yearly backup cycles use the same algorithms as the [weekly backup cycle](#). When you define retention policy settings for these backup cycles, you specify how many backups you want to retain and define the week day on which the monthly, quarterly or yearly backup must be created.

Veeam Backup & Replication repeats the monthly, quarterly or yearly backup cycle until the number of backups allowed by the retention policy is exceeded. After that, Veeam Backup & Replication removes the earliest full backup from the target backup repository to make room for the most recent monthly, quarterly or yearly backup.

Concurrent Archive Full Schedule

If you schedule a monthly, quarterly or yearly full backup on the same day when the weekly full backup is scheduled, Veeam Backup & Replication will create only one archive full backup – the weekly backup. The created weekly backup will be marked at the same time as monthly, quarterly or yearly GFS backup. In the Veeam Backup & Replication console, you will see all GFS flags assigned to the backup. In the file system, however, the file will be visible as having only one GFS flag – the flag of the highest GFS tier. For example, if you schedule weekly and yearly backup on the same day, the backup file will be marked as yearly in the file system.

Minutely and Hourly Backup Copy Intervals

If the backup copy interval is less than 1 day, Veeam Backup & Replication creates the archive full backup during the backup copy interval when the weekly full backup is scheduled. In the Veeam Backup & Replication console, the created archive backup is marked with all necessary GFS flags.

For example, you have scheduled both weekly and monthly full backups on Sunday. The backup copy interval is set to 3 hours and starts at 5:00 PM on Saturday. That is, backup copy intervals take place on Saturday at 5:00 PM, 8:00 PM, 11:00 PM, on Sunday at 2:00 AM, 5:00 AM and so on.

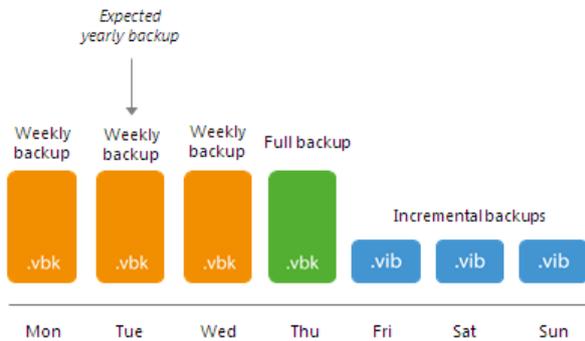
Before creating an archive full backup, Veeam Backup & Replication checks if the "Sunday, 12:00 AM" point in time lies within a current backup copy interval. If so, Veeam Backup & Replication creates an archive full backup. In this example, Veeam Backup & Replication will create an archive full backup during the backup copy interval "Saturday, 11:00 PM - Sunday, 2:00 AM". The created archive full backup will be marked with weekly and monthly flags.

Expected GFS Schedule for Active Full Method

If you use the active full method, mind that archive backups may not be created as you expect. For example, you configure the GFS schedule for a backup copy job in the following way:

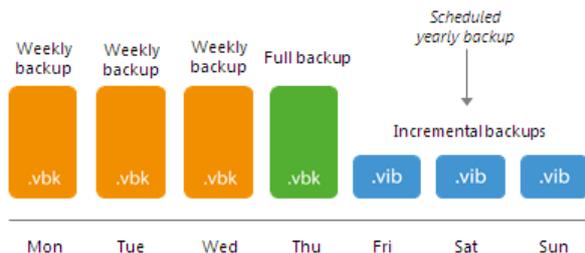
- Weekly backups are created regularly, for example, on Sundays.
- Yearly backups are not created.

After some time passes, you change the GFS schedule and enable yearly backups for the backup copy job. You may expect that Veeam Backup & Replication marks a weekly backup, that has already been created, as a yearly one. That is, the existing archive backup will have weekly and yearly GFS flags.



However, with the active full method, Veeam Backup & Replication never marks full backups, that have already been set aside as archive backups, with additional GFS flags. In the described situation, Veeam Backup & Replication will not mark an existing archive backup as yearly. Veeam Backup & Replication will create a yearly backup only during the next yearly cycle – in the next year.

To overcome this behavior and create a yearly backup during the current yearly cycle, you must schedule a yearly backup so that it coincides with the active backup copy chain (backup chain created during a regular backup copy cycle). In this case, Veeam Backup & Replication will assign the yearly flag when it sets a full backup aside as a yearly one. After a full backup is marked as yearly and set aside, you can change the yearly GFS schedule as required.



The described behavior is specific only for archived backups created with the active full method, and is applicable to all GFS cycles – monthly, quarterly and yearly.

NOTE:

Veeam Backup & Replication normally creates one archive full backup per GFS cycle. However, when you switch from active to synthetic backup method or change scheduling settings for synthetic full backups, Veeam Backup & Replication will create and keep in the backup chain two archive full backups marked with the same flag. For details, see [Archive Full Backups per GFS Cycle](#).

Related Topics

[Weekly Backup Cycle](#)

Archive Full Backups per GFS Cycle

Veeam Backup & Replication normally creates one archive full backup per GFS cycle.

However, Veeam Backup & Replication will create and keep in the backup chain two archive full backups marked with the same flag in the following cases:

- If you switch from active to synthetic backup method
- If you change scheduling settings for synthetic full backups

Two archive full backups will be created only for one GFS cycle – the GFS cycle when you switched the backup method or changed scheduling settings. In terms of retention policy, these backups are regarded as one. When the allowed number of archive full backups is exceeded, Veeam Backup & Replication removes both backups at the same time from the backup chain.

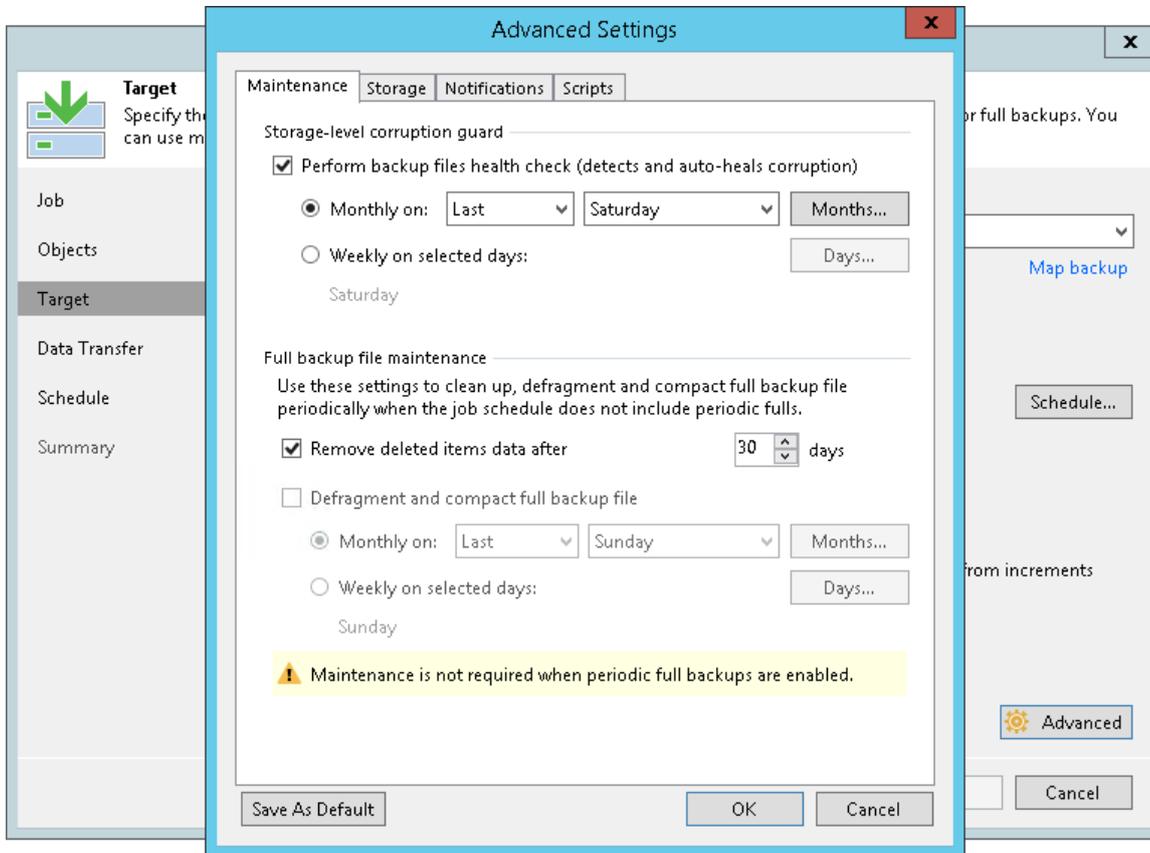
For example, you instruct a backup copy job to create weekly full backups on Monday. After a weekly full backup is created, you change scheduling settings for weekly full backups to Thursday. In this case, Veeam Backup & Replication will create a new weekly full backup on Thursday. During subsequent weeks, the backup copy job will produce weekly full backups only on Thursday. When the allowed number of weekly full backups is exceeded, Veeam Backup & Replication will remove two weekly full backups created for the week when you changed scheduling settings.

The described behavior is applicable to all GFS cycles – weekly, monthly, quarterly and yearly.

Deleted Items Retention

After you configure a backup copy job, you may want to change something in the virtual infrastructure. For example, you may decommission some virtual or physical machines or move VMs to another location. You may also exclude VMs from the backup copy job that has already run for some time.

By default, when you remove a machine protected by Veeam Backup & Replication from the virtual infrastructure, exclude a machine from the backup copy job or stop protecting a machine with Veeam Agent, the copied data still remains in backup files on the target backup repository. To avoid keeping redundant data on disk, you can enable the **Remove deleted items data after** option in the backup copy job settings. With this option enabled, at the end of every synchronization cycle Veeam Backup & Replication will remove data for deleted machines from backup files on the target backup repository.



Veeam Backup & Replication removes data for deleted machine only if two conditions are met:

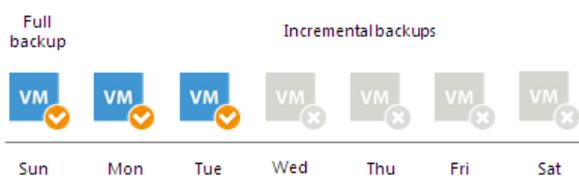
1. Veeam Backup & Replication has not created a valid restore points for the deleted machine for the number of days specified in the **Remove deleted items data after** field.
2. The backup chain on the target backup repository does not contain any successful incremental restore points for the deleted machine.

This approach helps ensure that data for deleted machines can be saved by the GFS retention.

For example:

- The retention for the backup copy job is set to 7.
- The retention period for deleted machine is set to 3 days.

The backup copy job has created 3 successful restore points – a full backup and two incremental backups. During the next 4 days, no successful restore points were created. At the next synchronization cycle, Veeam Backup & Replication will not remove data for the deleted machine from the target backup repository as the backup chain contains successful incremental restore points for this machine.



IMPORTANT!

Mind the following:

- When Veeam Backup & Replication removes data for deleted machines from regular backup chains, it does not free up space on the backup repository. It marks the space as available to be overwritten, and this space is overwritten during subsequent job sessions or the backup file compact operation.
- When Veeam Backup & Replication removes data for deleted machines from per-VM backup chains, it does not mark the space as available but deletes backup files since they contain data for 1 machine only.

Veeam Backup & Replication does not analyze the reason for which the machine has not been processed during the backup copy interval. For example, a VM may be regarded as deleted if Veeam Backup & Replication has failed to obtain data for the VM from the virtual infrastructure, the VM has failed to be processed in time during the backup copy interval and so on.

For this reason, you must be careful when specifying the retention period for deleted machines. If the retention period is too short, Veeam Backup & Replication may remove from the backup chain restore points that you still require.

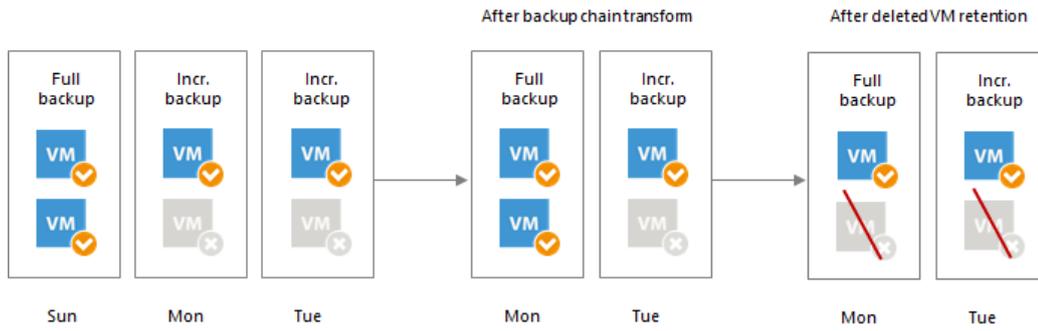
For example, a backup copy job is configured to process 2 VMs and has the following settings:

- The backup copy interval is set to 1 day.
- The retention for the backup copy job is set to 2.
- The retention period for deleted VMs is set to 1 day.

The backup copy job runs in the following way:

1. On Sunday, the backup copy job creates a full backup for 2 VMs – VM1 and VM2.
2. On Monday, the backup copy job creates an incremental backup for VM1. The backup copy job does not manage to process VM2 in time.
3. On Tuesday, the backup copy job creates an incremental backup for VM1. The backup copy job does not manage to process VM2 in time.
4. At the end of the backup copy job session on Tuesday, Veeam Backup & Replication transforms the backup chain and detects deleted VMs. Veeam Backup & Replication regards VM2 as a deleted VM – the deleted VMs retention is set to 1 day, and after transform, there are no valid restore points for this VM in the backup chain.

As a result, after the backup copy interval on Tuesday backup files on the target backup repository will not contain data for VM2.



Health Check for Backup Files

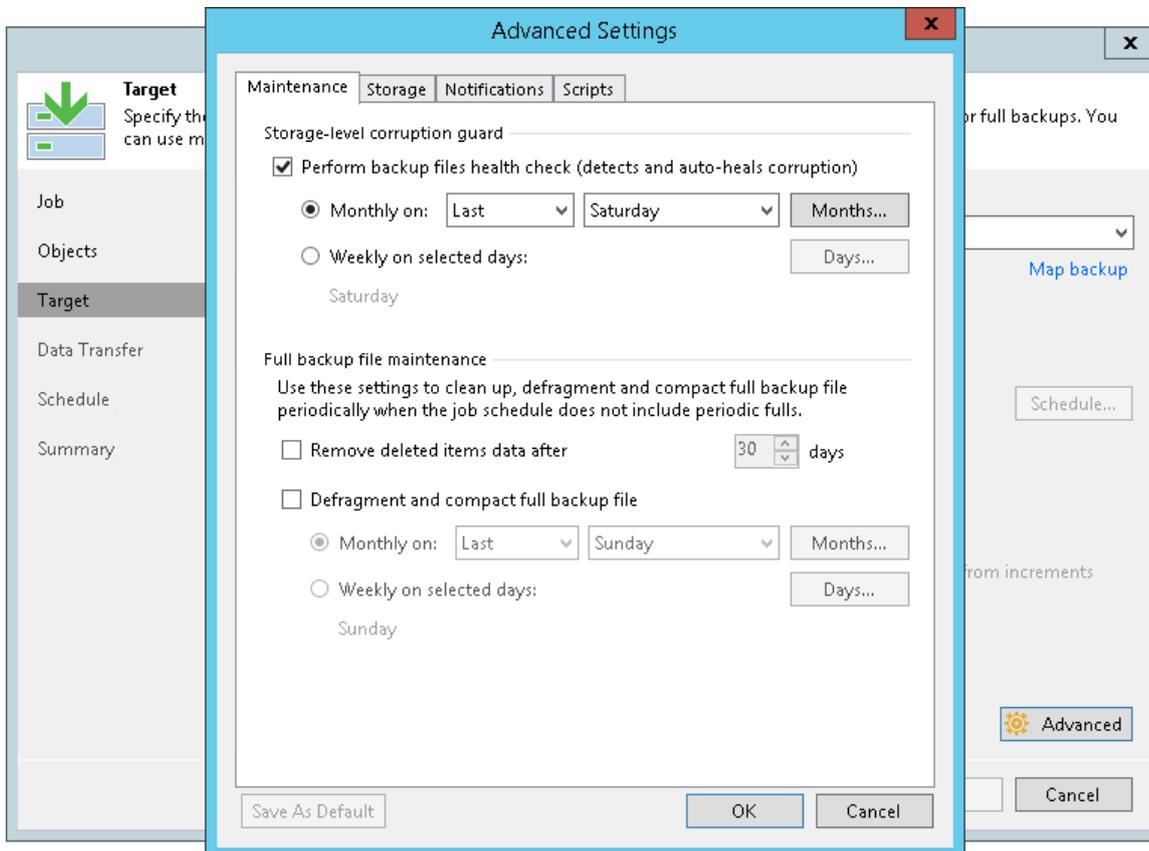
You can instruct Veeam Backup & Replication to periodically perform a health check for the latest restore point in the backup chain. During the health check, Veeam Backup & Replication performs a CRC check for metadata and a hash check for data blocks in the backup file to verify their integrity. The health check helps Veeam Backup & Replication make sure that the restore point is consistent, and you will be able to restore data from this restore point and subsequent restore points.

NOTE:

If you perform health check for the encrypted backup files, Veeam Backup & Replication will pass encryption keys to the regular backup repository or cloud repository. For more information on encryption, see [Data Encryption](#).

The health check is performed at the beginning of the backup copy interval. Veeam Backup & Replication always verifies only the latest point of the backup chain (or the restore point preceding the latest one if the latest restore point is incomplete). Veeam Backup & Replication performs the health check during the first backup copy interval on the day when the health check operation is scheduled. If another backup copy interval runs on the same day, Veeam Backup & Replication will not perform the health check during this backup copy interval. For example, if several backup copy intervals are scheduled to run on Saturday, and the health check is scheduled on Saturday, the health check will only be performed during the first backup copy interval on Saturday.

To run the health check periodically, you must enable the **Perform backup files health check** option in the backup copy job settings and define the health check schedule. By default, the health check is performed on the last Sunday of every month. You can change the health check schedule and instruct Veeam Backup & Replication to perform it weekly or monthly on specific days.



How Health Check Works

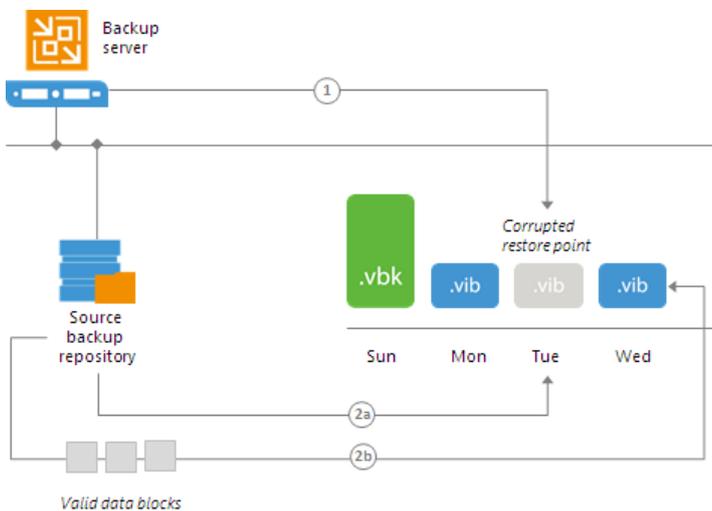
Veeam Backup & Replication performs the health check in the following way:

1. When Veeam Backup & Replication saves a restore point to the backup repository, it calculates CRC values for backup metadata and hash values for data blocks of a disk in the backup file and saves these values in the metadata of the backup file, together with copied data.
2. On the day when the health check is scheduled, Veeam Backup & Replication performs the following actions:
 - a. At the beginning of the backup copy interval, Veeam Backup & Replication performs the health check for the latest restore point in the backup chain. If the latest restore point in the backup chain is incomplete, Veeam Backup & Replication checks the restore point preceding the latest one.

Veeam Backup & Replication calculates CRC values for backup metadata and hash values for disks data blocks in the backup file, and compares them with the CRC and hash values that are already stored in the backup file.
 - b. If the health check detects corrupted data blocks, together with data blocks for the new restore point, Veeam Backup & Replication transports valid data blocks for the corrupted restore point. The valid data blocks are stored to the new incremental restore point created with this backup copy interval. As a result, the backup chain gets "fixed", and you get a possibility to restore data from restore points following the corrupted restore point.

NOTE:

If the backup copy job uses WAN accelerators, Veeam Backup & Replication attempts to find data blocks in the global cache not to transfer data over the network. For more information, see [WAN Acceleration](#).

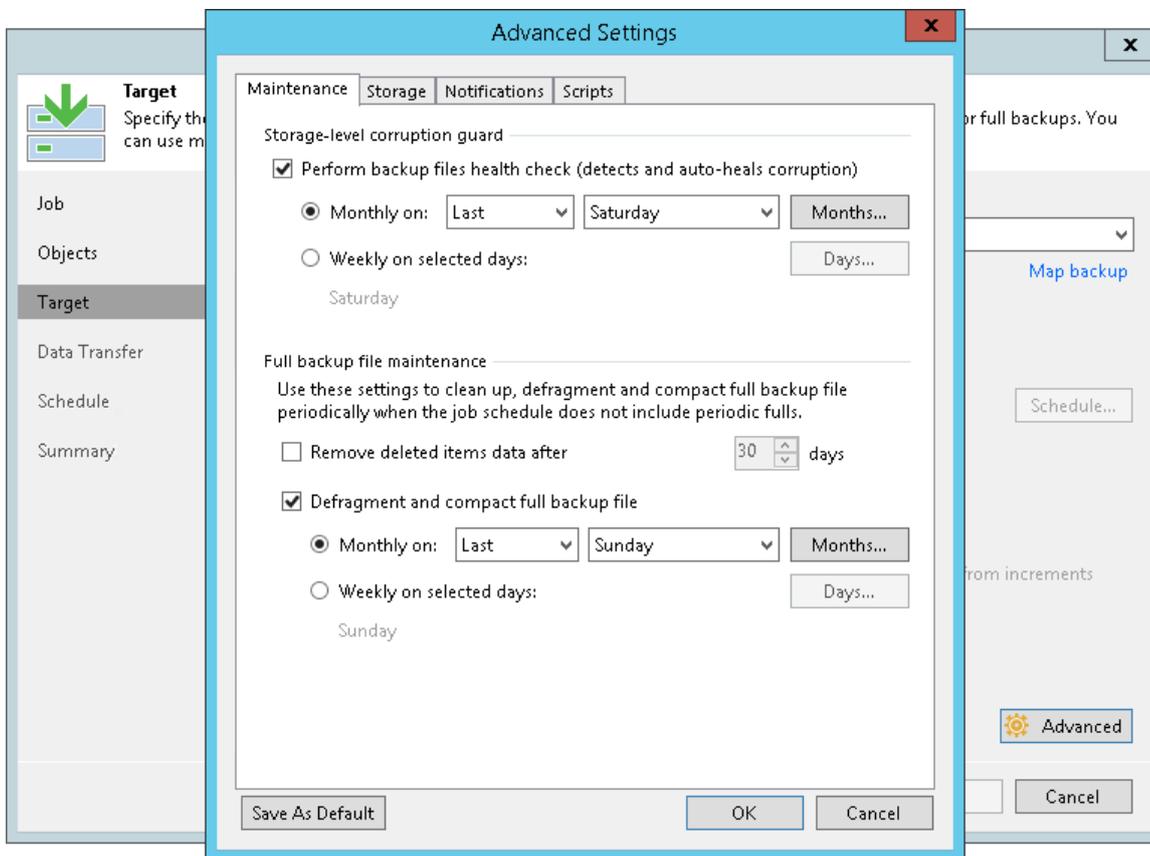


Compact of Full Backup File

The backup copy job constantly transforms the full backup file in the backup chain to meet retention policy settings. The transformation process, however, has a side effect. In the long run, the full backup file grows large and gets badly fragmented. The file data occurs to be written to non-contiguous clusters on disk, and operations of reading and writing data from and to the backup file slow down.

To resolve the fragmentation problem, you can instruct Veeam Backup & Replication to compact the full backup file periodically. During the file compact operation, Veeam Backup & Replication creates a new full backup file on the target repository: it copies existing data blocks from the old backup file, rearranges and stores them close to each other. As a result, the full backup file gets defragmented, its size reduces and the speed of reading and writing from and to the file increases.

To compact the full backup file periodically, you must enable the **Defragment and compact full backup file** option in the backup copy job settings and define the compact operation schedule. By default, the compact operation is performed on the last Sunday of every month. You can change the compact operation schedule and instruct Veeam Backup & Replication to perform it weekly or monthly on specific days.



Limitations for Full Backup File Compact

The full backup file compact has the following limitations:

- The **Defragment and compact full backup file** option can be enabled only for the simple retention policy scheme.
- The target backup repository must have enough space to store a file of the full backup size. During the compact process, Veeam Backup & Replication creates an auxiliary VBK file that exists on the backup repository until the end of the compact operation.

- If the full backup file contains data for a machine that has only one restore point and this restore point is older than 7 days, during the compact operation Veeam Backup & Replication will not copy data for such machine to the newly created full backup file. Veeam Backup & Replication will extract data for this machine from the full backup file and write this data to a separate backup file. The file will be displayed under the **Backups > Disk (imported)** node in the **Home** view. This mechanism helps remove data for machines that are no longer processed with the backup copy job from the full backup file and reduce the size of the full backup file.

The mechanism works if the following conditions are met:

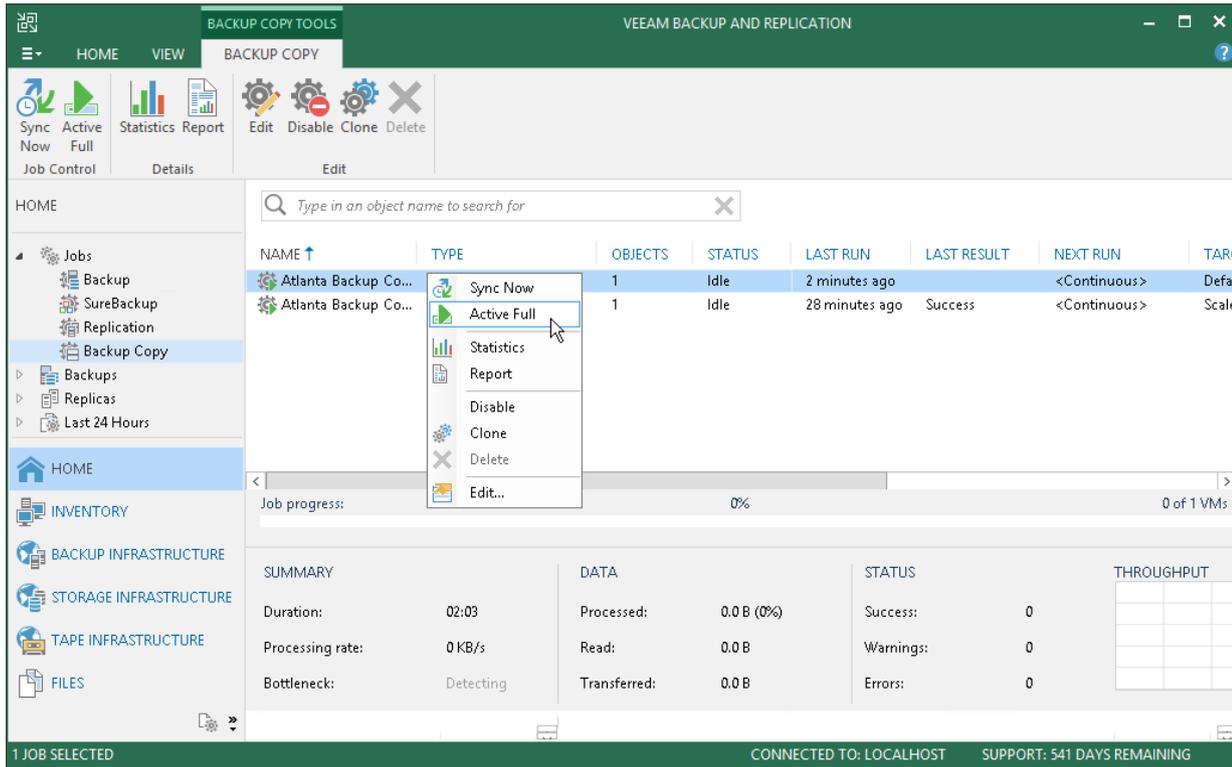
- The **Remove deleted items data** option is not enabled in the backup copy job settings.
- The **Use per-VM backup files** option is not enabled in the settings of the target backup repository.

Active Full Backup Copies

You can manually create an ad-hoc full backup for the backup copy job – active full backup copy, and add it to the backup chain on the target backup repository. To do this, you can use the **Active Full** button on the ribbon or the **Active Full** command from the shortcut menu.

Active full backup copy can be helpful if you want to change backup copy job settings, for example, enable or disable encryption. Veeam Backup & Replication will apply new settings starting from this full backup.

Veeam Backup & Replication treats archive full backups created with the active full backup method as regular backups and applies regular retention policy rules to maintain the necessary number of restore points.



Retention Policy for Active Full Backups

If you create active full backups for backup copy jobs, Veeam Backup & Replication applies to the backup chain retention rules of the forward incremental backup method. Veeam Backup & Replication waits until the number of restore points in the new backup chain is equal to the retention policy setting, and then removes the previous backup chain on the whole. For more information, see [Retention for Forward Incremental Backup](#).

If you additionally use the GFS retention scheme for the backup copy job, Veeam Backup & Replication behaves in a different way. After the number of restore points in the new backup chain is equal to the retention policy setting, Veeam Backup & Replication merges restore points in the previous backup chain to the restore point that must be marked as an archive backup. When the archive restore point is set aside, Veeam Backup & Replication uses the standard scheme described above.

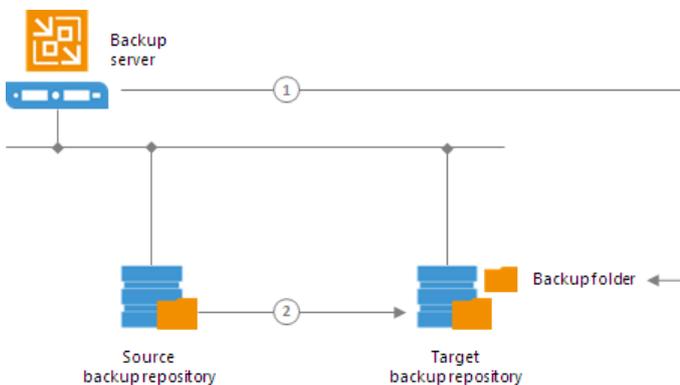
Backup Copy Jobs Mapping

If you already have a backup of machines whose restore points you want to copy in the target backup repository, you can map a backup copy job to this backup. Backup copy job mapping can be helpful if you plan to copy backups over the WAN or slow connections. Mapping will help you transfer a smaller amount of data and reduce the load on the WAN or network.

A backup copy job mapped to a backup is performed in the following way:

1. Veeam Backup & Replication accesses a backup to which you map the backup copy job. The backup may have any number of restore points in the chain. This backup chain will be used as a seed for the further backup copying process.
2. During subsequent backup copy intervals, Veeam Backup & Replication copies restore points in a regular manner. It copies only incremental changes and stores them as new restore points next to the seed backup chain.

A mapped backup copy job does not store copied restore points in a dedicated folder in the target backup repository. Instead, it stores restore points to the same folder where the "seed" backup chain resides.



Limitations for Backup Copy Job Mapping

- [For VM backup copy jobs] A backup copy job can be mapped only to a backup created with the incremental backup method. You cannot map a backup copy job to a backup created with the reverse incremental backup method, or to a backup whose chain contains both incremental and reverse incremental restore points (for example, if the backup chain has been transformed). To overcome this limitation, you can use a workaround scenario. For more information, see [Creating Seed for Backup Copy Job](#).

- If the initial backup that you plan to use as a seed is encrypted, you must enable encryption for the backup copy job, too. In terms of Veeam Backup & Replication, the encryption setting applies to the whole backup chain. If the full backup is encrypted, subsequent incremental backups must also be encrypted.

The password that you use for the backup copy job can differ from the password used for the initial backup job.

- [For backup copy jobs processing Veeam Agent backups] You can map a Veeam Agent backup copy job only to backups created by the following types of jobs:
 - Veeam Agent backup copy job that processes backups created by Veeam Agent operating in the standalone mode
 - Veeam Agent backup job configured directly on a Veeam Agent Computer

You cannot map a backup copy job to a backup created by a Veeam Agent backup job configured in Veeam Backup & Replication.

Creating Seed for Backup Copy Job

You can map backup copy jobs only to backups created with the incremental backup method. If the backup is created with the reverse incremental backup method or the backup chain contains both incremental and reverse incremental restore points, Veeam Backup & Replication will display a warning, and you will not be able to map a backup copy job to such backup.

To overcome this limitation, you can use a workaround scenario. You can configure a backup copy job to produce a full backup file out of the reverse incremental backup chain, transfer this full backup file to the target backup repository, and remap the backup copy job to the transferred full backup file.

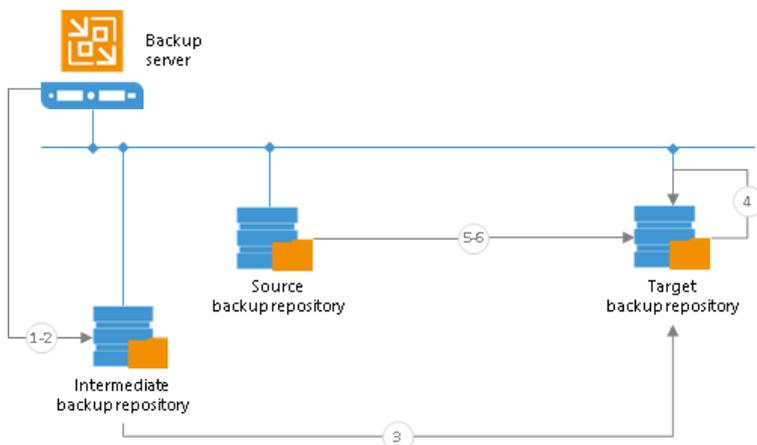
To create a seed for the primary backup copy job, do the following:

1. Create a backup copy job. Add machines whose restore points you want to copy to this backup copy job. Target the backup copy job to some backup repository on the source side. This backup repository will be used as an intermediate one.
2. Run the backup copy job to create a full backup file (VBK) in the intermediate backup repository.
3. Transfer the created VBK file and VBM file from the intermediate backup repository to the target backup repository.
4. Perform [repository rescan](#) to populate the target backup repository.

If the initial backup file was encrypted, you will need to enter a password to unlock the full backup file. Otherwise, Veeam Backup & Replication will not display the full backup file in the list of backups on the backup repository. For more information, see [Importing Encrypted Backups](#).

5. Remap the backup copy job to the full backup file that you have created and transferred to the target backup repository.
6. Click **Sync Now** to start a new backup copy interval.

As a result, Veeam Backup & Replication will use the full backup file as a seed. When a new restore point for the machine is available in the source backup repository, Veeam Backup & Replication will copy it to the target backup repository and store it next to the full backup seed.



When you configure a backup copy job, make sure that its backup copy interval covers the whole chain of restore points on the backup repository from which you plan to copy backups. The length of the backup copy interval has an impact on the algorithm of restore point selection. Veeam Backup & Replication copies only restore points that match the following criterion:

```
Time of restore point creation >= current time - backup copy interval
```

That is, if you have a backup chain whose earliest restore point is 1 week old, you need to set the backup copy interval to 1 week. If you set the backup copy interval to a smaller time interval, for example, 1 day, all restore points that are older than 1 day will fall out of the search scope, and Veeam Backup & Replication will not transfer such restore points. For more information, see [Restore Point Selection](#).

Creating Backup Copy Jobs

To copy a backup to a secondary location, you must configure a backup copy job. The backup copy job defines how, where and when to copy backups. One job can be used to process backups of one or more machines.

You can configure a job and start it immediately or save the job to start it later. Jobs can be started manually or scheduled to run automatically at specific time.

Before creating a job, check prerequisites. Then use the **New Backup Copy Job** wizard to configure a backup copy job.

Before You Begin

Before you create a backup copy job, check the following prerequisites:

- Backup infrastructure components that will take part in the backup copy process must be added to the backup infrastructure and properly configured. These include source and target backup repositories between which backups must be copied.
- The target backup repository must have enough free space to store copied backups. To receive alerts about low space on the backup repository, configure global notification settings. For more information, see [Specifying Other Notification Settings](#).
- If you plan to use pre-job and/or post-job scripts, you must create scripts before you configure the backup copy job.
- [For backup mapping] The backup copy job can be mapped to a backup if the backup chain is created with the incremental backup method. You cannot map the backup copy job to a backup if the backup chain is created with the reverse incremental backup method or contains both incremental and reverse incremental restore points (for example, if the backup chain was transformed).

If you plan to use WAN accelerators for backup copying, check the following prerequisites and limitations:

- Source and target WAN accelerators must be added to the backup infrastructure and properly configured. For more information, see [Adding WAN Accelerators](#).
- A license for Enterprise Plus Edition for Veeam Backup & Replication must be installed on the backup server.
- It is recommended that you pre-populate the global cache on the target WAN accelerator before you start the backup copy job. Global cache population helps reduce the amount of traffic transferred over WAN. For more information, see [Populating Global Cache](#).
- You cannot use WAN accelerators for backup copy jobs that copy backups of Amazon EC2 instances

NOTE:

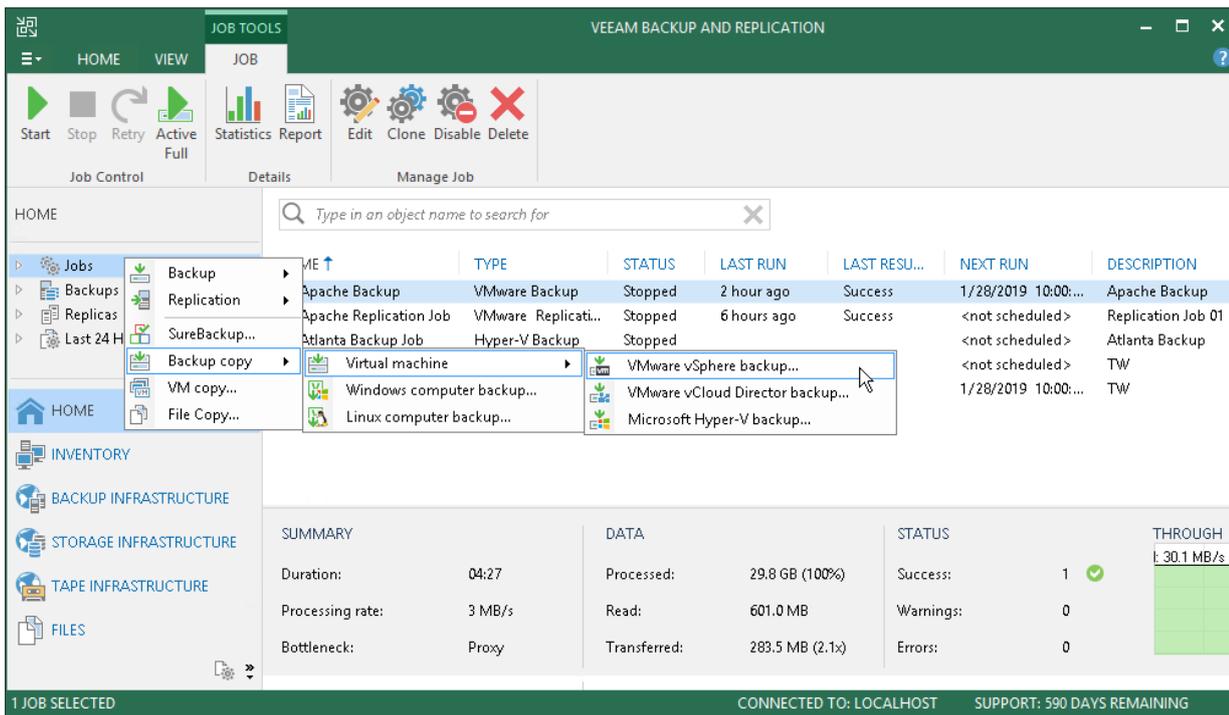
If you use tags to categorize virtual infrastructure objects, check limitations for VM tags. For more information, see [VM Tags](#).

Step 1. Launch New Backup Copy Job Wizard

To run the **New Backup Copy Job** wizard, do one of the following:

- On the **Home** tab, click **Backup Copy** and select the necessary platform:
 - Virtual Machine
 - Windows computer backup
 - Linux computer backup
 - Amazon EC2

- Open the **Home** view, in the inventory pane right-click **Jobs** or right-click anywhere in the working area, and select the necessary option:
 - **Backup Copy** > *Virtual machine* > *VMware vSphere backup* – if you want to create a copy of a VM backup.
 - **Backup Copy** > *Windows computer backup* – if you want to create a copy of a Veeam Agent backup created for Microsoft Windows machines.
 - **Backup Copy** > *Linux computer backup* – if you want to create a copy of a Veeam Agent backup created for Linux machines.
 - **Backup Copy** > *Amazon EC2 backup* – if you want to create a copy of an EC2 instance backup created with N2WS Backup & Recovery.



Step 2. Specify Job Name and Description

At the **Job** step of the wizard, specify basic settings for the backup copy job.

1. In the **Name** field, enter a name for the job.
2. In the **Description** field, enter a description for the job. The default description contains information about the user who created the job, date and time when the job was created.
3. The backup copy job runs continuously. The synchronization process starts at specific time intervals. During this backup copy interval, Veeam Backup & Replication copies new restore points from the source backup repository to the target backup repository.

In the **Copy every** field, specify the time interval according to which the synchronization process must start. By default, the backup copy interval is set to 1 day. This means that the backup copy job will create a new backup copy interval once a day. Veeam Backup & Replication will check if new restore points are available on the source backup repository. If a new restore point is found, it will be copied to the target backup repository within the backup copy interval. For more information, see [Backup Copy Interval](#).

4. If you have selected a daily backup copy interval, specify the start time for it. By default, the daily backup copy interval starts at 12:00 AM.

NOTE:

In some situations, the backup copy synchronization process may not manage to complete from the time the copy interval begins to the time the copy interval finishes due to a new copy interval beginning. This can happen if the defined backup copy interval is not enough to copy a restore point. If such situation occurs, Veeam Backup & Replication will display a warning in the job session results. It is recommended that you increase the backup copy interval time.

Job
Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data. Type in a name and description for the job, and specify backup copy interval.

Job
Objects
Target
Data Transfer
Schedule
Summary

Name:
DB Backup Copy Job

Description:
Daily Backup Copy Job

Copy every:
1 Day starting at 12:00 AM

Controls how often backup copies are created. Backup Copy job creates a new backup file for each copy interval, and starts copying the most recent restore point of each processed object into this backup file immediately, or as soon as the new restore point appears in the source backup repository.

< Previous Next > Finish Cancel

Step 3. Select Machines to Process

At the **Objects** step of the wizard, select machines whose restore points you want to copy to the target backup repository.

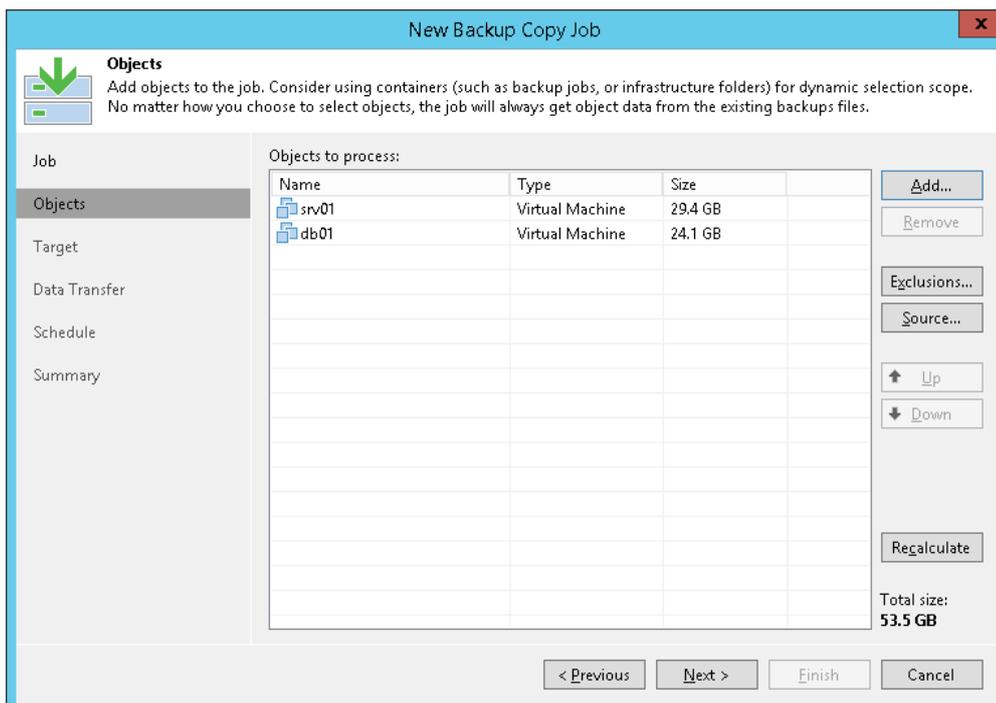
1. Click **Add**.
2. Select machines that you want to process with the job. You can use the following source to browse to machines:
 - **From infrastructure.** You can browse the virtual infrastructure to add single VMs or VM containers to the job. When a backup copy job runs, Veeam Backup & Replication will search for restore points of selected VMs on all backup repositories in the backup infrastructure. You can limit the search scope by [selecting only specific backup repositories](#) for the backup copy job.
This option is available only for backup copy jobs that process VMware or Hyper-V VMs.
 - **From backups.** You can select virtual or physical machines from backups. When a backup copy job runs, Veeam Backup & Replication will search for restore points of selected machines in all backups created on the backup server. You can limit the search scope by [selecting only specific backup repositories](#) for the backup copy job.
This option is the only available option for backup copy jobs that process backups of EC2 instances. You can select instances only from backups that are stored on external repositories.

- **From jobs.** You can select virtual or physical machines from backup jobs. When a backup copy job runs, Veeam Backup & Replication will search for restore points of selected machines in backups created for selected jobs.

Mind the following:

- Within one backup copy job, Veeam Backup & Replication processes machines of one platform only. For example, if you configure a backup copy job that processes VM backups, you cannot add a Veeam Agent backup as an additional source for this job.
- You can create a backup copy job with an empty source – that is, not add any machines or jobs at this step of the wizard. In this case, you will need to configure a secondary destination for the source backup job and link it to the created backup copy job. When you save the backup job settings, Veeam Backup & Replication will automatically update the backup copy job and link it to the source backup job. For more information, see [Linking Backup Jobs to Backup Copy Jobs](#).
- If a machine that you add to the backup copy job is processed by multiple source backup jobs that use different block sizes, you must not add this machine with the **From infrastructure** and **From backups** options. When you add a machine with these options, Veeam Backup & Replication picks the most recent backup as a data source. If Veeam Backup & Replication picks source backups with different block sizes during different backup copy intervals, the backup copy job will fail. To avoid this situation, you must add such a machine with the **From jobs** option. Alternatively, you can use the **Source** option to specify from which backup repository Veeam Backup & Replication must retrieve data.
- [For backup copy jobs processing Veeam Agent backups] The following limitation applies to backup copy jobs only if you upgrade to Veeam Backup & Replication 9.5 Update 4 from earlier versions of the product.

If a Microsoft Windows machine that you add to the backup copy job is processed by multiple source Veeam Agent backup jobs configured in Veeam Backup & Replication, you must not add this machine with the **From backups** option. In case Veeam Backup & Replication detects restore points of such a machine, the backup copy job will fail, and the following message will be displayed: *Unable to determine source backup: multiple backup files with the same instance ID exist in the source backup repository. Please reconfigure this Backup Copy job to use the specific backup job as the source.* To avoid this situation, you must add such a machine with the **From jobs** option. Alternatively, you can use the **Source** option to specify from which backup repository Veeam Backup & Replication must retrieve data.



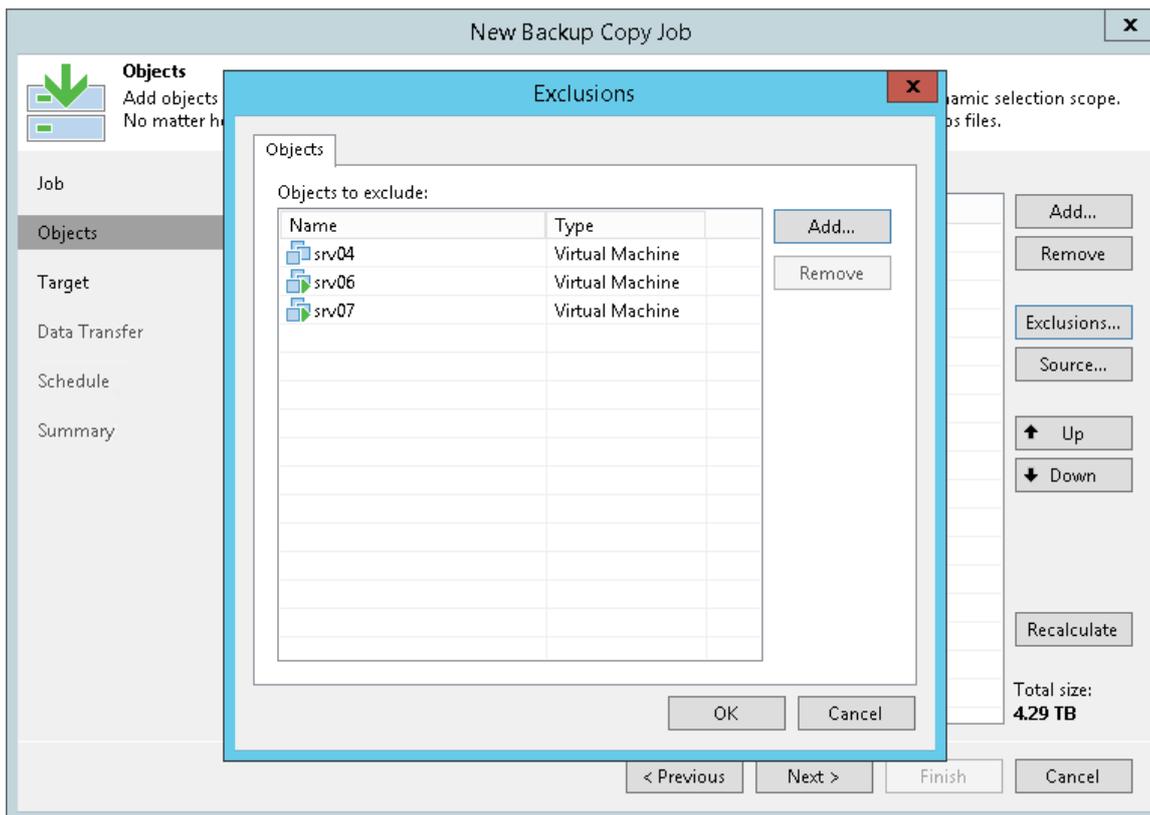
Step 4. Exclude Objects from Backup Copy Job

If you have added VM containers to the list of processed machines, you can specify which objects you want to exclude from the backup copy job.

NOTE:

The **Exclude** option is available for VM backup copy jobs only. This option is not available for Veeam Agent backup copy jobs.

1. At the **Objects** step of the wizard, select a VM container added to the job and click **Exclusions**.
2. Click the **Objects** tab.
3. Click **Add**.
4. Use the toolbar at the top right corner of the window to switch between views. 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.
5. In the displayed tree, select the necessary object and click **Add**. Use the **Show full hierarchy** check box to display the hierarchy of all hosts added to Veeam Backup & Replication.
6. Click **OK**.



Step 5. Select Source Backup Repositories

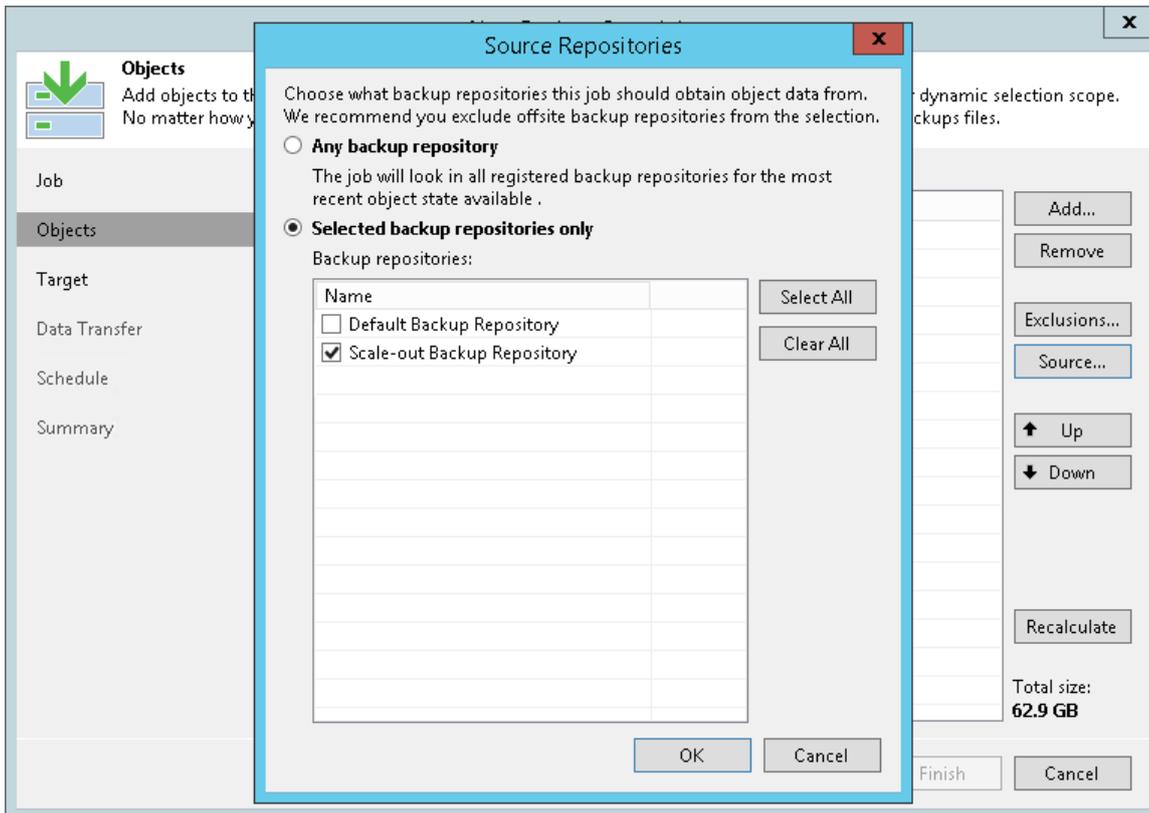
By default, Veeam Backup & Replication searches for restore points on all backup repositories configured in the backup infrastructure. However, you can select backup repositories in which Veeam Backup & Replication must search for restore points of selected machines.

1. At the **Objects** step of the wizard, click **Source**.

2. Choose backup repositories on which restore points must be searched for. You can select all backup repositories configured in the backup infrastructure or define specific backup repositories.

IMPORTANT!

You can limit the search scope to backup repositories if you have added machines to the backup copy job using the **From infrastructure** and **From backups** options. If you have used the **From jobs** option, the **Selected backup repositories only** option will not be applied, and Veeam Backup & Replication will retrieve data from the backup repository where the backup created with the source backup job resides.



Step 6. Define Machines Processing Order

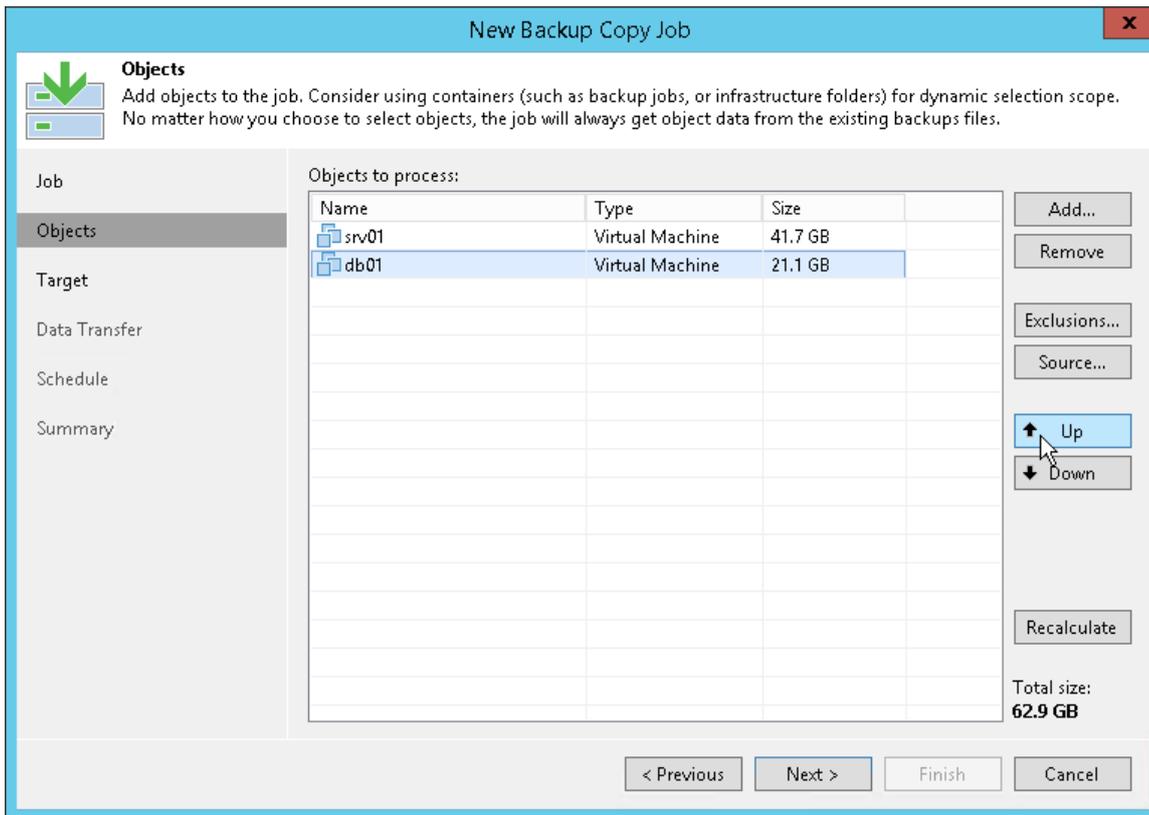
You can define the order in which the backup copy job must process machines. Setting machines order can be helpful, for example, if you have added some mission-critical machines to the job and want the job to process them first. You can set these machines first in the list to ensure that their processing fits the backup window.

VMs inside a VM container are processed at random. To ensure that VMs are processed in the defined order, you must add them as standalone VMs, not as part of the VM container.

To define machine processing order:

1. At the **Objects** step of the wizard, select a virtual or physical machine, or VM container added to the job.

- Use the **Up** and **Down** buttons on the right to move the virtual or physical machine, or VM container up or down in the list.



Step 7. Define Backup Copy Target

At the **Target** step of the wizard, define the target backup repository for the backup copy job and retention policy settings.

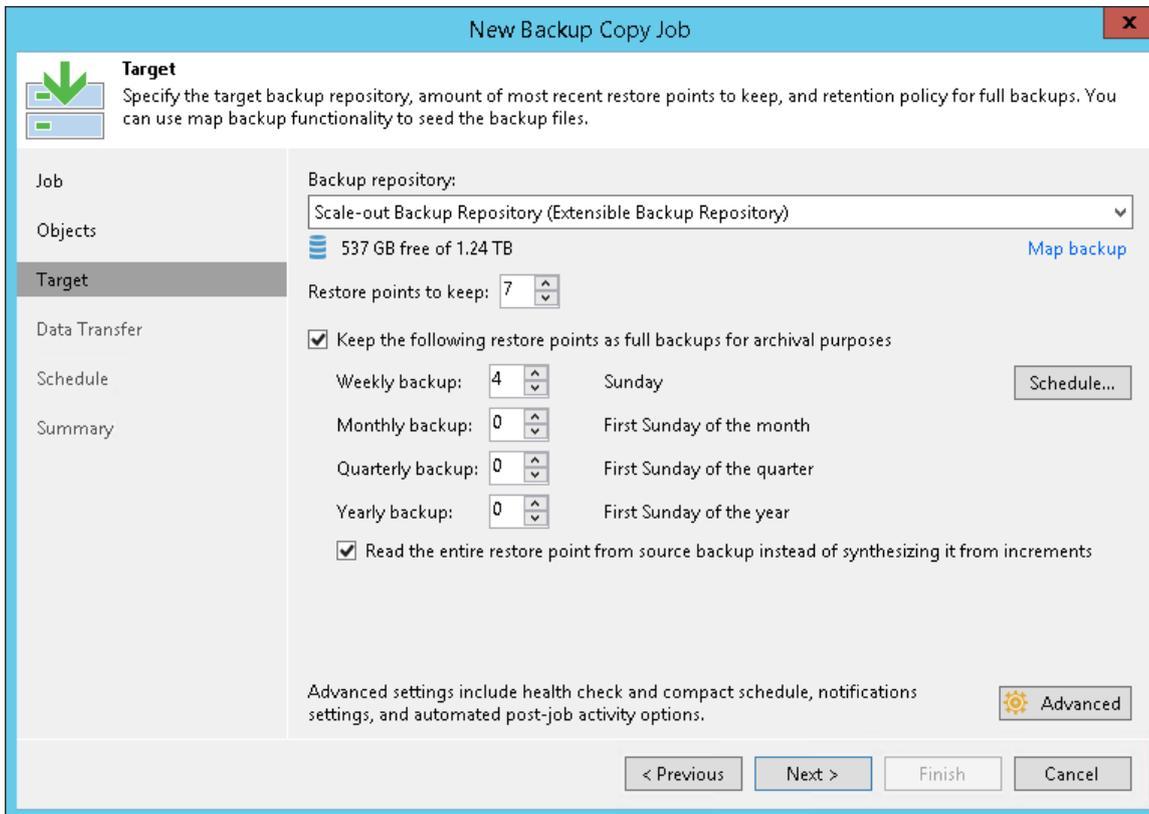
- From the **Backup repository** list, select a backup repository in the target site where copied backups must be stored. When you select a target backup repository, Veeam Backup & Replication automatically checks how much free space is available on it. Make sure that you have enough free space to store copied backups.
- In the **Restore points to keep** field, specify the number of restore points that must be retained on the target backup repository. When this number is exceeded, Veeam Backup & Replication will remove the earliest restore point from the backup chain.

The maximum number of restore points for the backup copy job is 999. For more information, see [Simple Retention Policy](#).

- To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep the following restore points as full backups for archival purposes** check box. In the fields below, specify the number of daily, weekly, monthly, quarterly and yearly full intervals for which backups must be retained. Use the **Schedule** button to define the schedule by which GFS full backups must be created. For more information, see [GFS Retention Policy](#).
- If you do not want Veeam Backup & Replication to synthesize archive backup files on the target backup repository, select the **Read the entire restore point from source backup instead of synthesizing it from increments** check box. Veeam Backup & Replication will transport data for archive full backups from restore points from the source backup repository to the target backup repository over the network. The load on the network will be higher but the performance of the target backup repository will increase. For more information, see [Methods for Archive Backups Creation](#).

IMPORTANT!

You cannot enable GFS retention settings if you use a backup repository with rotated drives as the target backup repository.



The screenshot shows the 'New Backup Copy Job' dialog box with the 'Target' tab selected. The dialog has a sidebar on the left with options: Job, Objects, Target (selected), Data Transfer, Schedule, and Summary. The main area is titled 'Target' and contains the following information:

- Backup repository:** Scale-out Backup Repository (Extensible Backup Repository) (dropdown menu)
- Storage:** 537 GB free of 1.24 TB (with a 'Map backup' link)
- Restore points to keep:** 7 (spinners)
- Keep the following restore points as full backups for archival purposes
- Weekly backup:** 4 (spinners) on Sunday (with a 'Schedule...' button)
- Monthly backup:** 0 (spinners) on First Sunday of the month
- Quarterly backup:** 0 (spinners) on First Sunday of the quarter
- Yearly backup:** 0 (spinners) on First Sunday of the year
- Read the entire restore point from source backup instead of synthesizing it from increments
- Advanced settings:** A link to 'Advanced' settings (gear icon) with the text: 'Advanced settings include health check and compact schedule, notifications settings, and automated post-job activity options.'

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

Step 8. Map Backup File

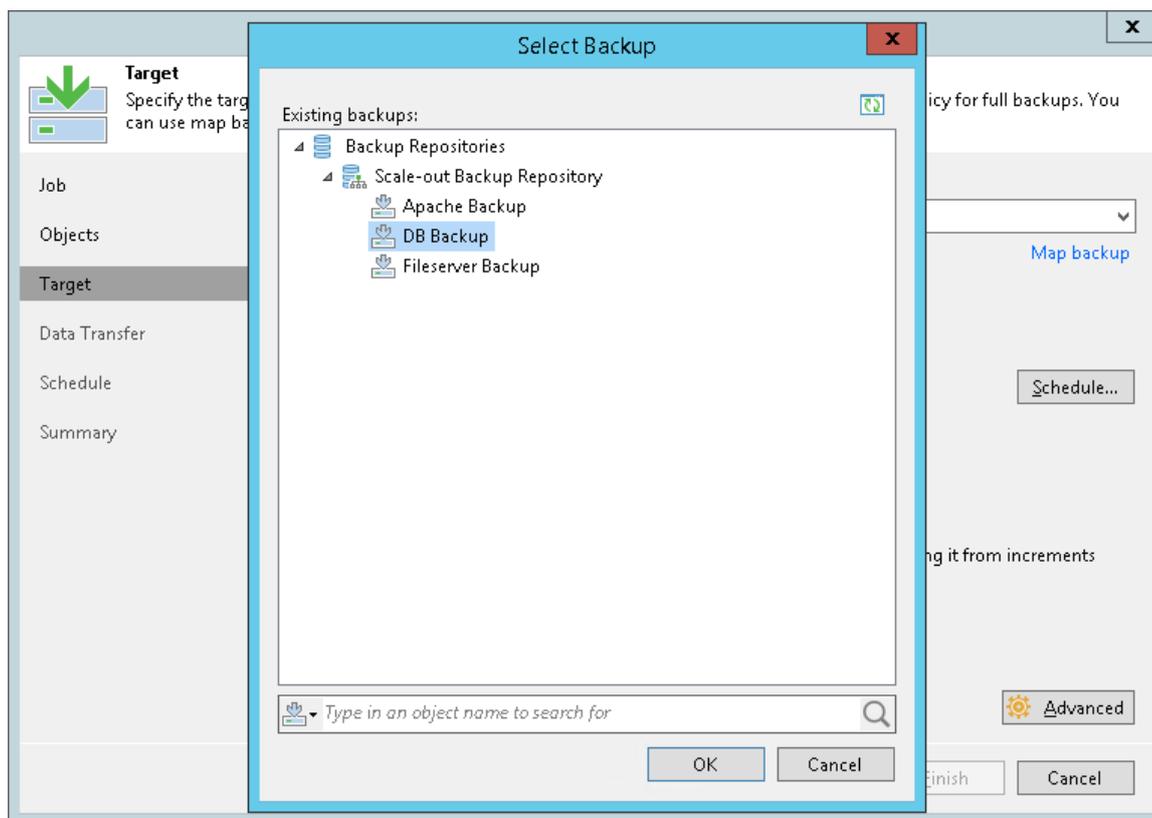
If you plan to copy backups over WAN or slow connections, you can use backup mapping.

Backup mapping can only be used if you already have a backup for the necessary machine in the target backup repository. In this case, you can point the backup copy job to this backup. The backup will be used as a "seed" by the backup copy job, and you will need to transfer only small amount of incremental changes over the network. For more information, see [Mapping Backup Copy Jobs](#).

To map a backup copy job to the backup:

1. Click the **Map backup** link.

- Point the backup copy job to the backup in the target backup repository. Backups in the target backup repository can be easily identified by backup job names. To facilitate search, you can use the search field at the bottom of the window.



Step 9. Specify Advanced Settings

At the **Target** step of the wizard, you can specify the following settings for the backup copy job:

- [Maintenance settings](#)
- [Storage settings](#)
- [Notification settings](#)
- [Script settings](#)

TIP:

After you specify necessary settings for the backup copy 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 backup copy job, Veeam Backup & Replication will automatically apply the default settings to the new job.

Maintenance Settings

To specify settings for backup files stored in the target backup repository:

- At the **Target** step of the wizard, click **Advanced**.
- If you want to periodically perform a health check of the most recent restore point in the backup chain, select the **Perform backup files health check** check box and specify the time schedule for the health check. By default, the health check is performed on the last Saturday of every month.

An automatic health check allows you to avoid a situation when a restore point gets corrupted, making all further increments corrupted, too. If Veeam Backup & Replication detects corrupted data blocks in the restore point during the health check, it will transfer these data blocks to the target backup repository during the next backup copy interval and store them in the newly copied restore point. For more information, see [Health Check for Copied Backups](#).

3. Select the **Remove deleted items data after** check box and specify the retention policy settings for deleted machines. If a machine is no longer processed by a job for some reason (for example, it was excluded from the job, removed from the infrastructure and so on), its data may still be kept in backups on the target backup repository. To avoid this situation, you can define the number of days for which data for deleted machines must be retained.

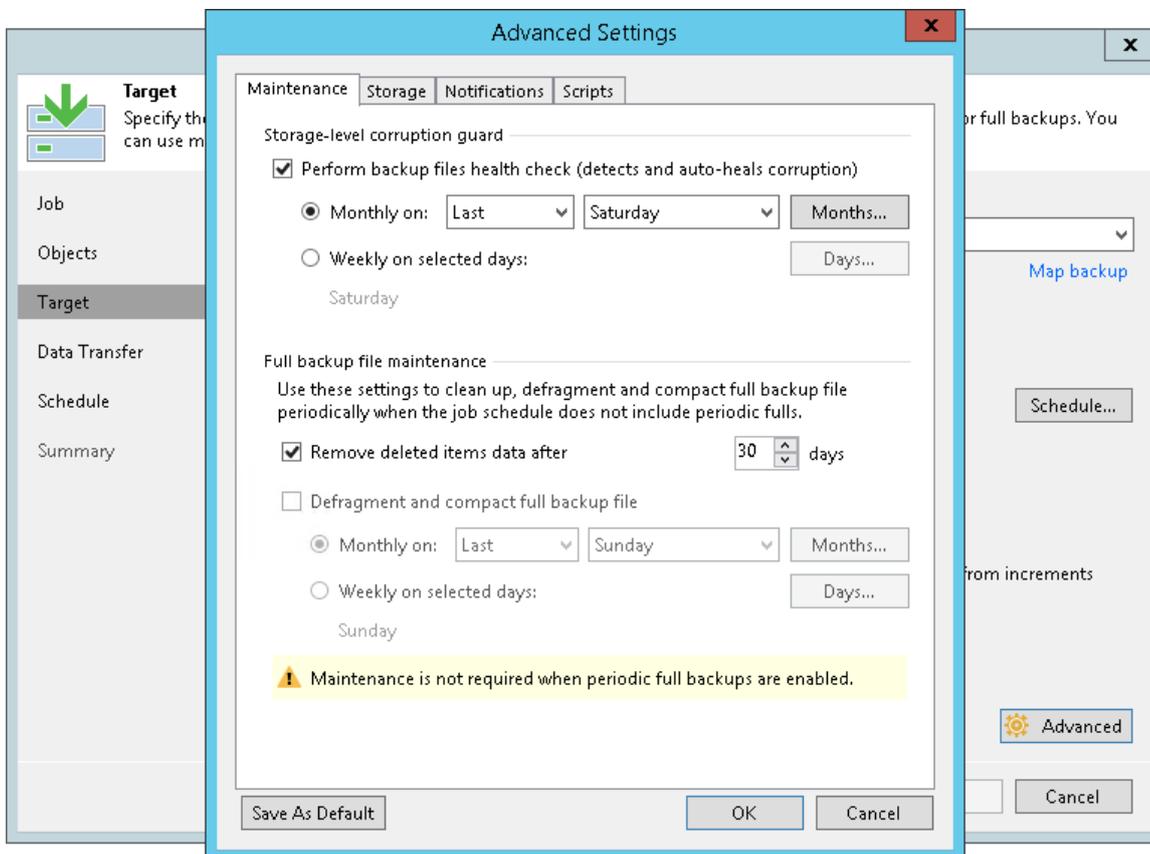
By default, the deleted items retention period is 30 days. It is strongly recommended that you set the retention period to 3 days or more to prevent unwanted data loss. For more information, see [Deleted Items Retention](#).

4. To periodically compact a full backup, select the **Defragment and compact full backup file** check box and specify the schedule for the compacting operation. By default, the compact operation is disabled.

The compact option can be enabled only if you have not specified the GFS settings. During the compacting operation, Veeam Backup & Replication creates a new empty VBK file and copies to it all data blocks from the full backup file. As a result, the full backup file gets defragmented, its size reduces and the speed of writing and reading to/from the file increases. For more information, see [Compacting a Full Backup File](#).

NOTE:

The **Remove deleted items data after** option applies only to regular backup chains. Veeam Backup & Replication does not remove data for deleted machines from weekly, monthly, quarterly and yearly backups.



Storage Settings

To specify compression, deduplication and encryption settings for backup files stored on target backup repository:

1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Storage** tab.
3. By default, Veeam Backup & Replication performs deduplication before storing copied data on the target backup repository. Deduplication provides a smaller size of the resulting backup file but may reduce the job performance.

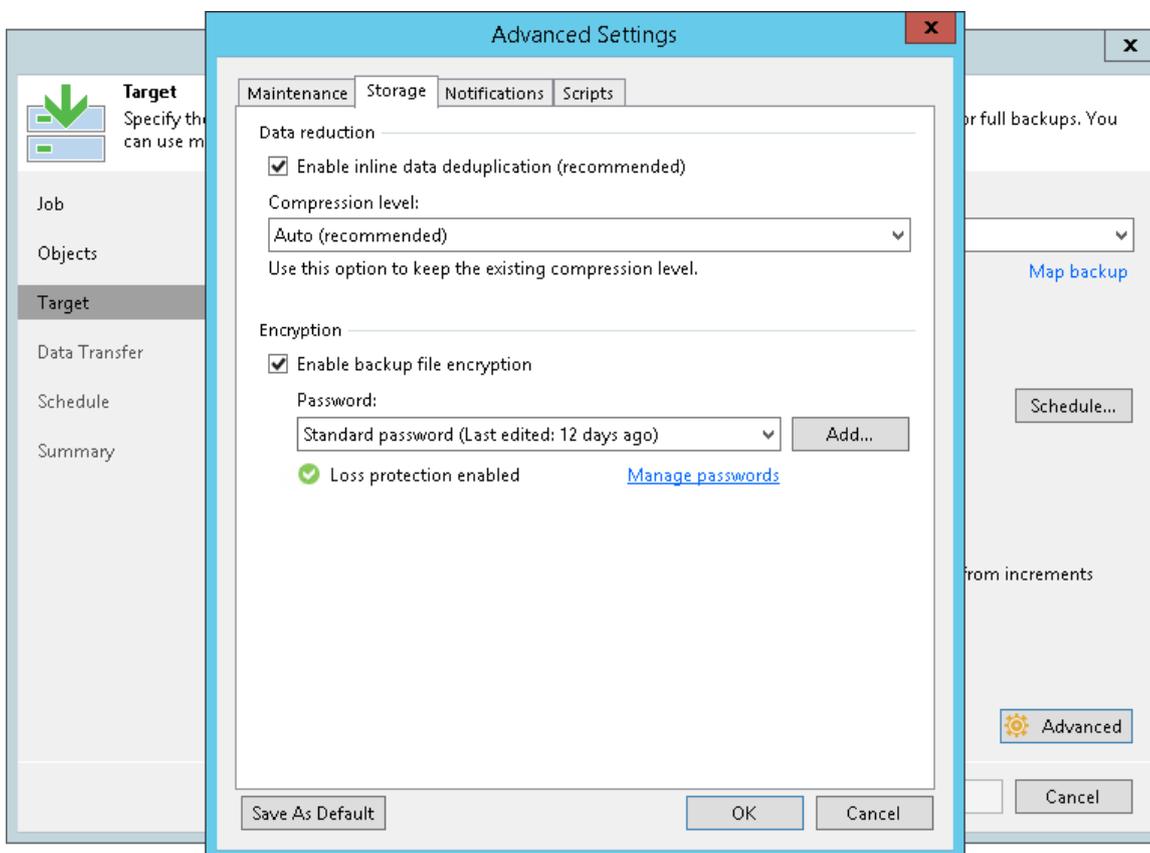
You can disable data deduplication. To do this, clear the **Enable inline data deduplication** check box.

4. From the **Compression level** list, choose a compression level to be used: *Auto*, *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*. The recommended level of compression for backup copy jobs is *Auto*. In this case, Veeam Backup & Replication uses compression settings of the copied backup files. For more information, see [Compression and Deduplication](#).
5. To encrypt the backup file created with the backup copy job, select the **Enable backup file encryption** check box. From the **Password** field, select a password that you want to use to encrypt the backup 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](#).

NOTE:

Consider the following:

- If you enable encryption for an existing backup copy job, Veeam Backup & Replication applies new settings only starting from the next active full backup (created manually or by the GFS schedule). The active full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password. Note that if you disable the **Read the entire restore point from source backup instead of synthesizing it from increments** option in the backup copy job, you will have synthetic full backups, not active full backups. For details, see [Defining Backup Copy Target](#).
- Encryption is not retroactive. If you enable encryption for an existing job, Veeam Backup & Replication does not encrypt the previous backup chain created with this job. If you want to start a new chain so that the unencrypted previous chain can be separated from the encrypted new chain, follow the scenario described in [this Veeam KB article](#).



Notification Settings

To specify notification settings for the backup copy job:

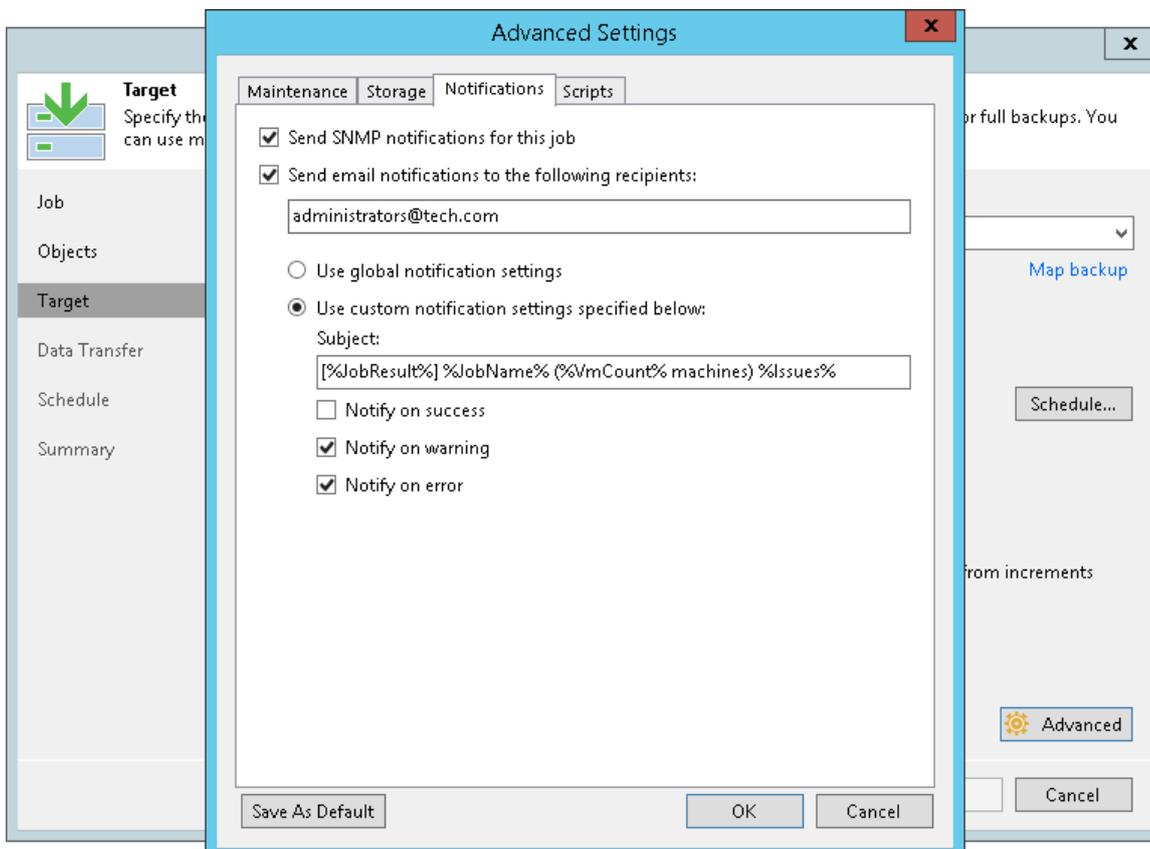
1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send SNMP notifications for this job** check box if you want to receive SNMP traps when the job completes successfully. SNMP traps will be sent if you specify global SNMP settings in Veeam Backup & Replication and configure software on recipient's machine to receive SNMP traps. For more information, see [Specifying SNMP Settings](#).

4. 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.

Veeam Backup & Replication sends a consolidated email notification once for the specified backup copy interval. Even if the synchronization process is started several times within the interval, for example, due to job retries, only one email notification will be sent.

Email notifications will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see [Configuring Global Email Notification Settings](#).

5. You can choose to use global notification settings or specify custom notification settings.
 - o To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server. For more information, see [Configuring Global Email Notification Settings](#).
 - o To configure a custom notification for a job, select **Use custom notification settings specified below**. You can specify the following notification settings:
 - a. In the **Subject** field, specify a notification subject. You can use the following variables in the subject: *%Time%* (completion time), *%JobName%*, *%JobResult%*, *%VmCount%* (number of machines in the job) and *%Issues%* (number of machines in the job that have been processed with the *Warning* or *Failed* status).
 - b. Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if data processing within the backup copy interval completes successfully, fails or completes with a warning.



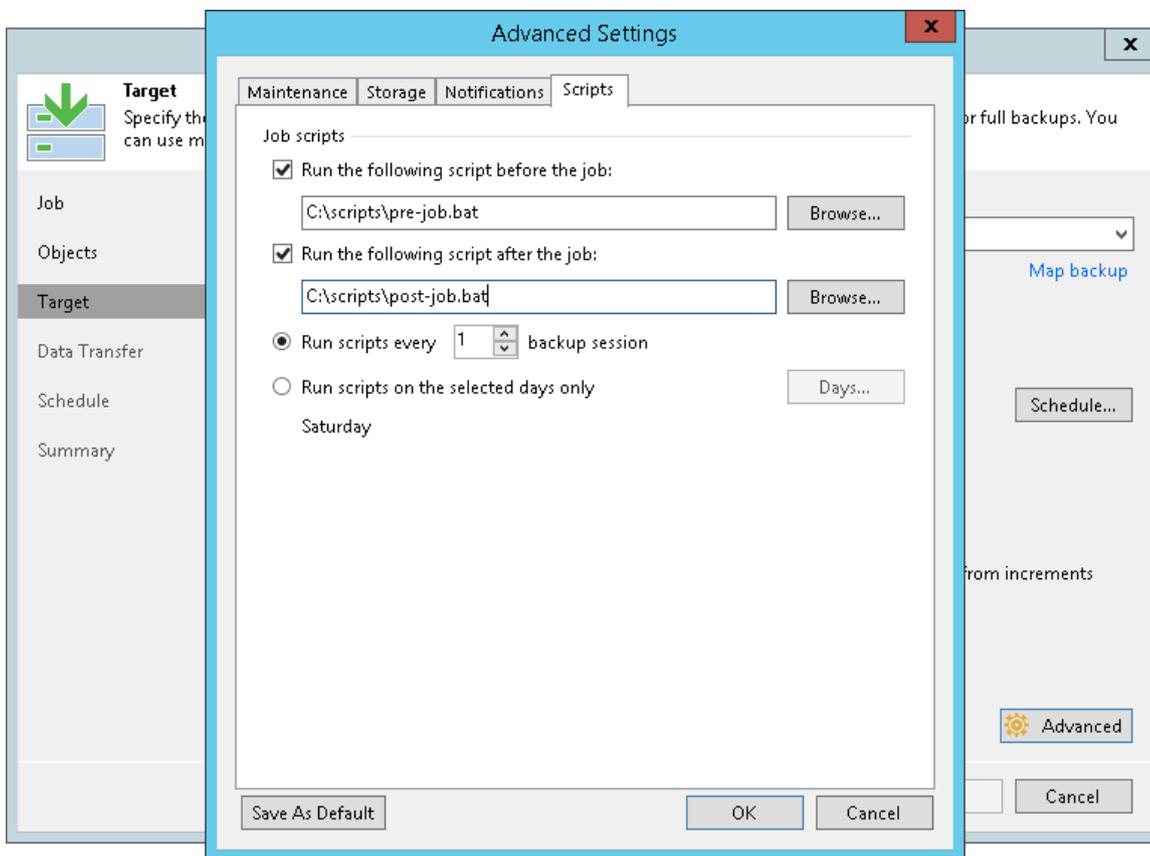
Scripts Settings

To specify script settings for the backup copy job:

1. At the **Target** step of the wizard, click **Advanced**.
2. Click the **Scripts** tab.
3. If you want to execute custom scripts before and/or after the backup copy job, select the **Run the following script before the job** and **Run the following script after the job** check boxes and click **Browse** to choose executable files from a local folder on the backup server. The scripts are executed on the backup server.

You can select to execute pre- and post-replication actions after a number of backup copy intervals or on specific week days.

- If you select the **Run scripts every... backup session** option, specify the number of backup copy intervals after which scripts must be executed.
- If you select the **Run scripts on selected days only** option, click **Days** and specify week days on which scripts must be executed.



Step 10. Specify Data Path Settings

The **Data Transfer** step of the wizard is available only if you copy backups of virtual or physical machines created with Veeam Backup & Replication or Veeam Agents.

At this step of the wizard, you can select how Veeam Backup & Replication will transport backed up data – directly or through a pair of WAN accelerators. By default, during the backup copy job Veeam Backup & Replication transports data directly from the source backup repository to target backup repository. This type of transport is recommended if you plan to copy backup files over high-speed connections.

If you plan to copy backup files over WAN or slow connections, it is recommended that you configure a pair of WAN accelerators in the backup infrastructure and copy backups via these WAN accelerators. WAN accelerators perform global data deduplication, eliminate the need to transport redundant blocks of data and reduce the load on the WAN. For more information, see [WAN Acceleration](#).

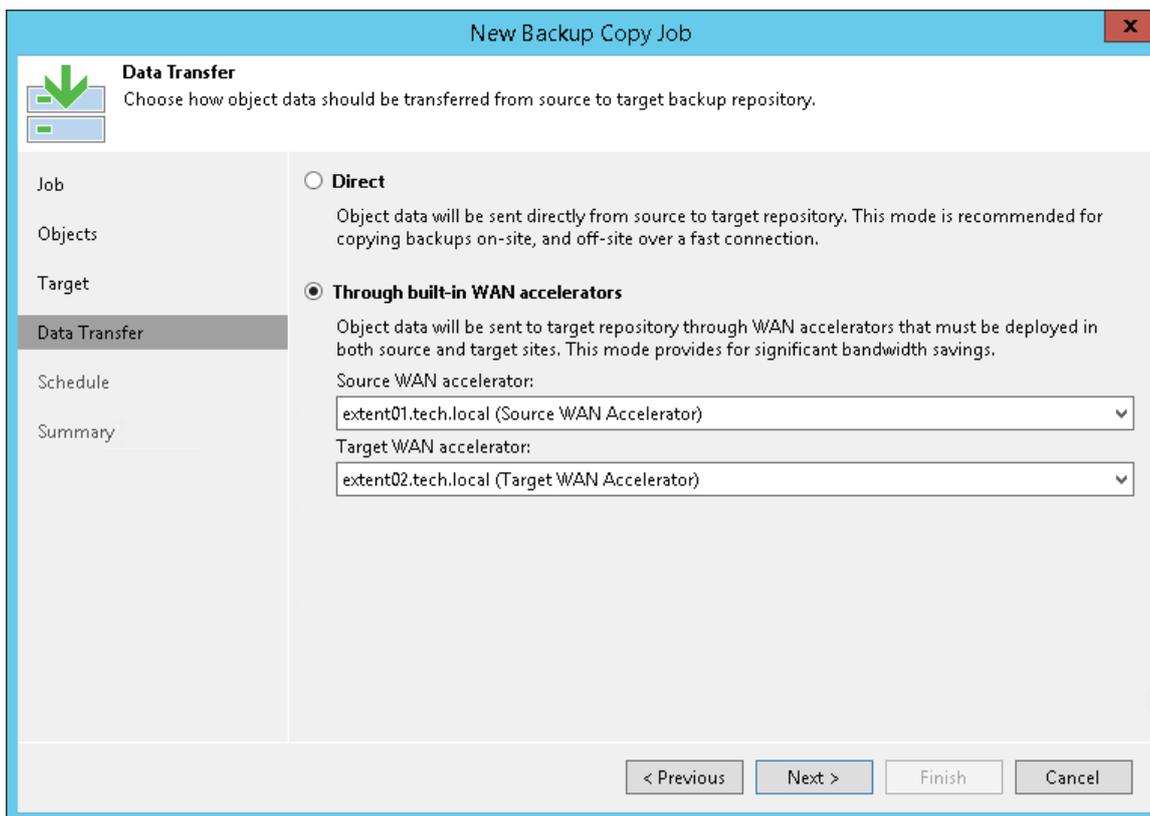
To use WAN acceleration for the backup copy job:

1. At the **Data Transfer** step of the wizard, select the **Through built-in WAN accelerators** option.
2. From the **Source WAN accelerator** list, select a WAN accelerator configured in the source site.
3. From the **Target WAN accelerator** list, select a WAN accelerator configured in the target site.

Be extremely careful when assigning WAN accelerators to the backup copy job. If you make a mistake and assign the WAN accelerator in the target site to be used as the source WAN accelerator, data will go in the backward direction and workload on the WAN will increase.

You should not assign one source WAN accelerator to several backup copy jobs that you plan to run simultaneously. The source WAN accelerator requires a lot of CPU and RAM resources, and does not process multiple backup copy tasks in parallel. As an alternative, you can create one backup copy job for all machines you plan to process over one source WAN accelerator.

The target WAN accelerator, however, can be assigned to several backup copy jobs. For more information, see [Adding WAN Accelerators](#).



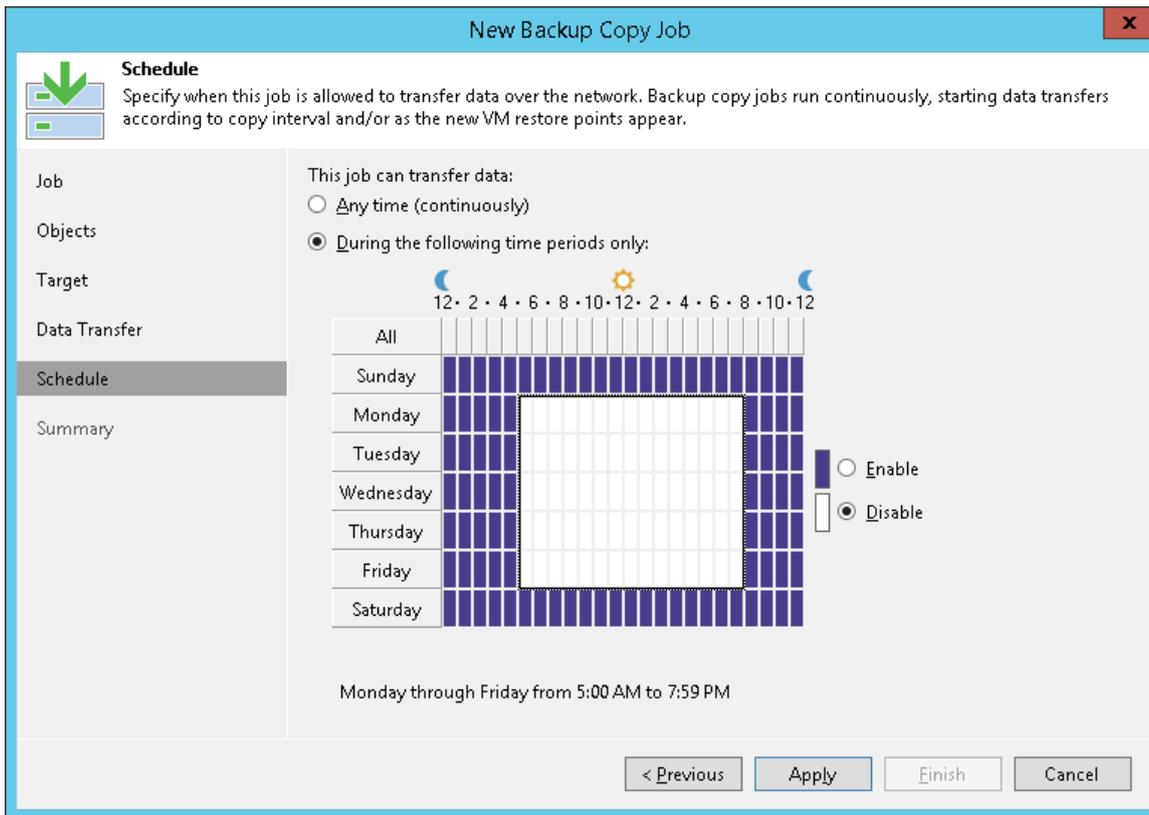
Step 11. Define Backup Copy Window

At the **Schedule** step of the wizard, define the time span in which the backup copy job must not transport data between source and target backup repositories. For more information, see [Backup Copy Window](#).

To define a backup window for the backup copy job:

1. Select the **During the following time periods only** option.
2. In the schedule box, select the desired time area.

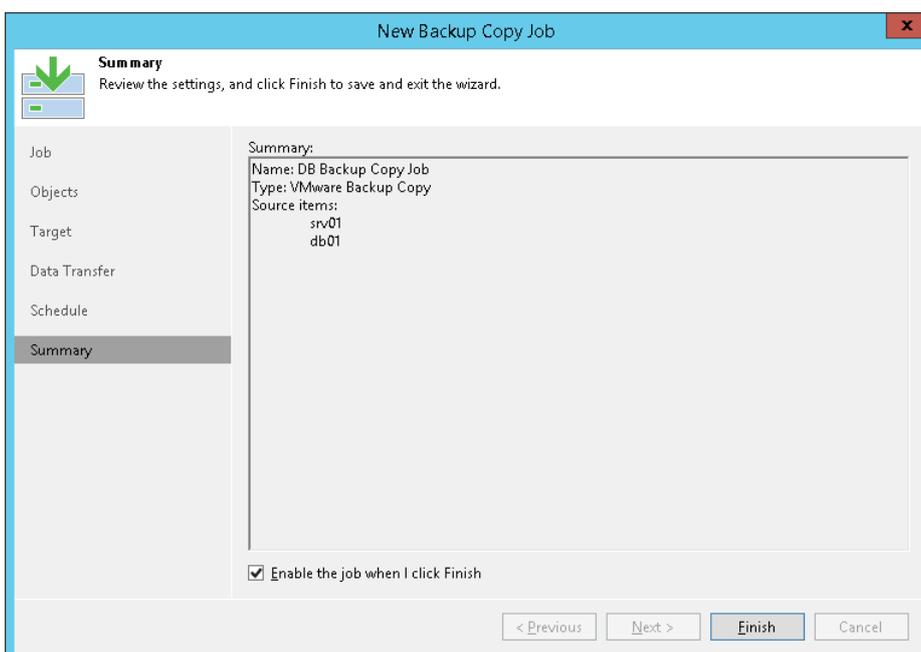
- Use the **Enable** and **Disable** options to mark the selected area as allowed or prohibited for the backup copy job.



Step 12. Finish Working with Wizard

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

- Review details of the backup copy job.
- Select the **Enable the job when I click Finish** check box if you want to start the job right after you finish working with the wizard.
- Click **Finish** to close the wizard.



Editing Backup Copy Jobs

You can edit backup copy job settings at any moment. For example, you may want to change scheduling settings for the job or add some machines to the job.

To edit job settings:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs > Backup Copy**.
3. In the working area, select the job and click **Edit** on the ribbon or right-click the job and select **Edit**.

You will follow the same steps as you have followed when creating the job and can change job settings as required.

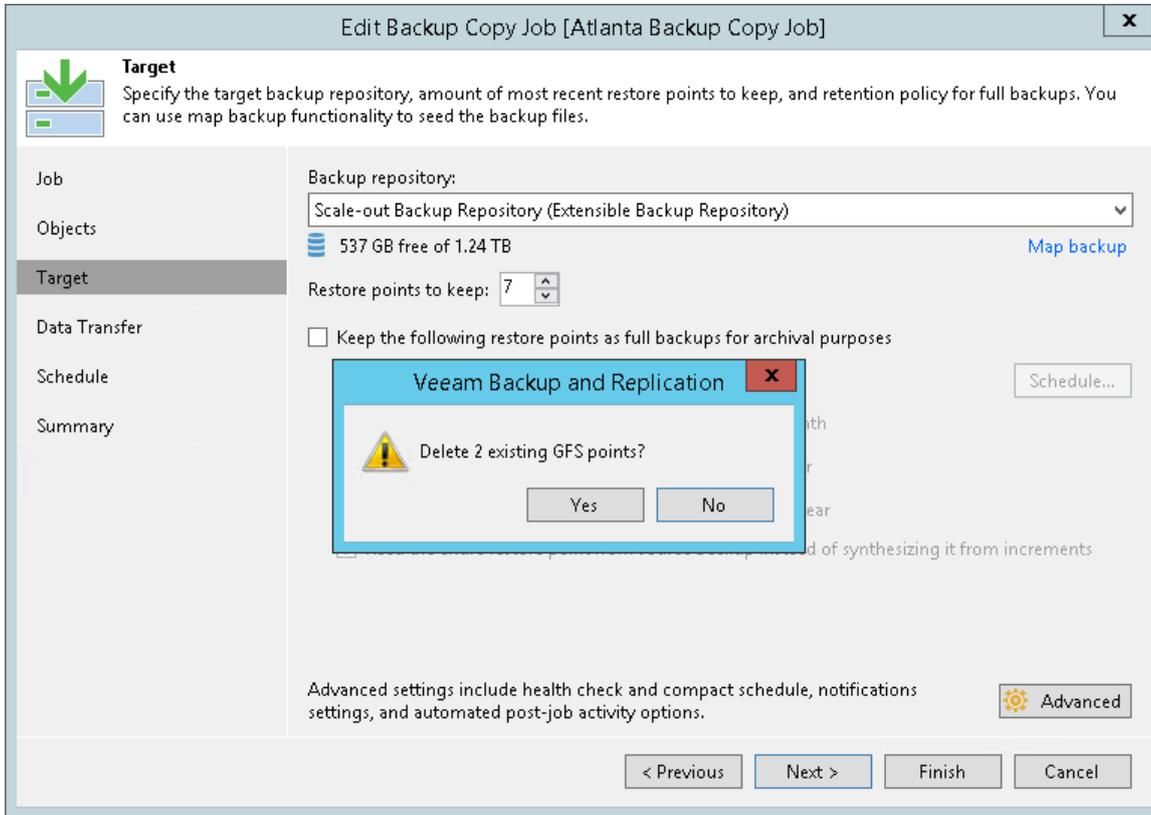
Disabling GFS Scheme

If you disable the **Keep the following restore points as full backups for archival purposes** option, and you already have archive full backups on the target backup repository, Veeam Backup & Replication will offer you to remove existing archive full backups.

- Click **Yes** to remove archive full backups from the target backup repository. Archive full backups will be removed during the next retention cycle (next backup copy interval). The backup copy job will not create archive full backups.
- Click **No** to keep archive full backups on the target backup repository. Archive full backups will be displayed under the **Backups > Disk (imported)** node in the Veeam Backup & Replication console. The backup copy job will not create archive full backups.

NOTE:

If you disable the **Keep the following restore points as full backups for archival purposes** option and enable it again after some time, archive full backups that remained on disk will not be linked to the backup copy job. They will still be displayed under the **Backups > Disk (imported)** node in the Veeam Backup & Replication console.



Viewing Backup Copy Properties

You can view summary information about created backup copies. The summary information provides the following data: available restore points, date of restore points creation, compression and deduplication ratios, data size and backup size.

In the summary information, Veeam Backup & Replication displays data about restore points created by the simple retention scheme and archive restore points created by the GFS retention scheme (if GFS retention is enabled). Archive restore points are marked with the following letters:

- R – full backups created with the simple retention scheme or active full backups
- W – weekly backups
- M – monthly backups
- Q – quarterly backups
- Y – yearly backups

To view summary information for a backup copy:

1. Open the **Home** view.
2. In the inventory pane, select **Backups > Disk (copy)**.
3. In the working area, right-click the backup copy and select **Properties**.

Backup Properties: Atlanta Backup Copy Job

Repository: Scale-out Backup Repository Folder: C:\Backup\Atlanta_Backup_Copy_Job

Files:

NAME	DATA SIZE	BACKUP SIZE	DEDUPLICATION	COMPRESSION	DATE	RETENTION
fileserv05.vm-51086_1A16D2019-03-1...	1.91 GB	1.05 GB	1.0x	1.7x	3/17/2019 8:10:25 AM	
fileserv05.vm-51086_2585D2019-03-1...	297 MB	126 MB	1.0x	2.4x	3/16/2019 8:08:40 AM	
fileserv05.vm-51086_FC65D2019-03-1...	296 MB	120 MB	1.0x	2.5x	3/15/2019 8:09:58 AM	
fileserv05.vm-51086_D8ABD2019-03-1...	160 GB	15.9 GB	6.6x	1.5x	3/14/2019 7:33:12 AM	M
fileserv05.vm-51086_36D1D2019-03-1...	161 MB	76.1 MB	1.0x	2.2x	3/13/2019 7:35:43 AM	
fileserv05.vm-51086_F4FED2019-03-1...	904 MB	530 MB	1.0x	1.7x	3/12/2019 7:31:35 AM	
fileserv05.vm-51086_AE2BD2019-03-1...	2.06 GB	998 MB	1.4x	1.5x	3/11/2019 6:03:23 AM	
fileserv05.vm-51086_007DD2019-03-1...	160 GB	15.9 GB	6.6x	1.5x	3/10/2019 6:01:37 AM	W

Objects:

NAME	ORIGINAL SIZE	DATE	TYPE	STATUS
fileserv05	37.8 GB	3/17/2019 8:10:25 AM	Increment	OK
		3/16/2019 8:08:40 AM	Increment	OK
		3/15/2019 8:09:58 AM	Increment	OK
		3/14/2019 7:33:12 AM	Full	OK
		3/13/2019 7:35:43 AM	Increment	OK
		3/12/2019 7:31:35 AM	Increment	OK
		3/11/2019 6:03:23 AM	Increment	OK
		3/10/2019 6:01:37 AM	Full	OK

OK

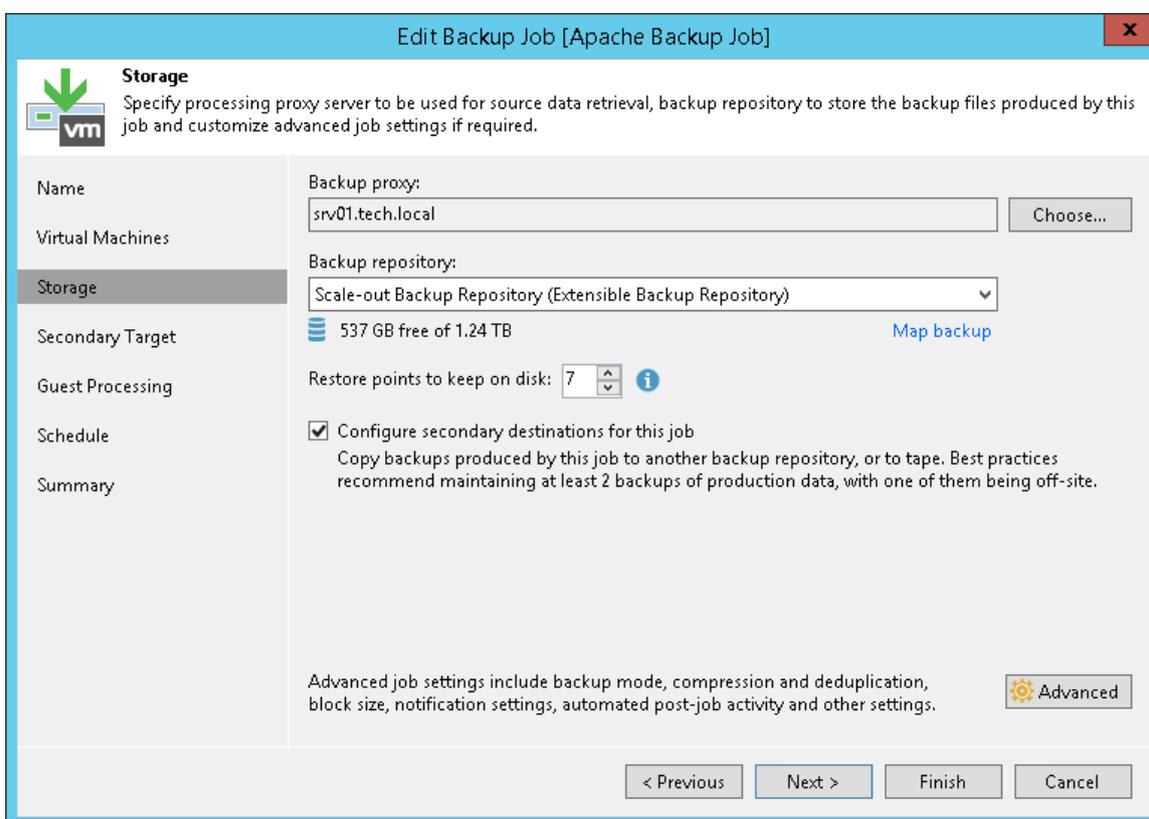
Linking Backup Jobs to Backup Copy Jobs

You can link backup jobs to backup copy jobs. This option lets you create a secondary target for the backup job and store backups created with the backup job on the secondary backup repository.

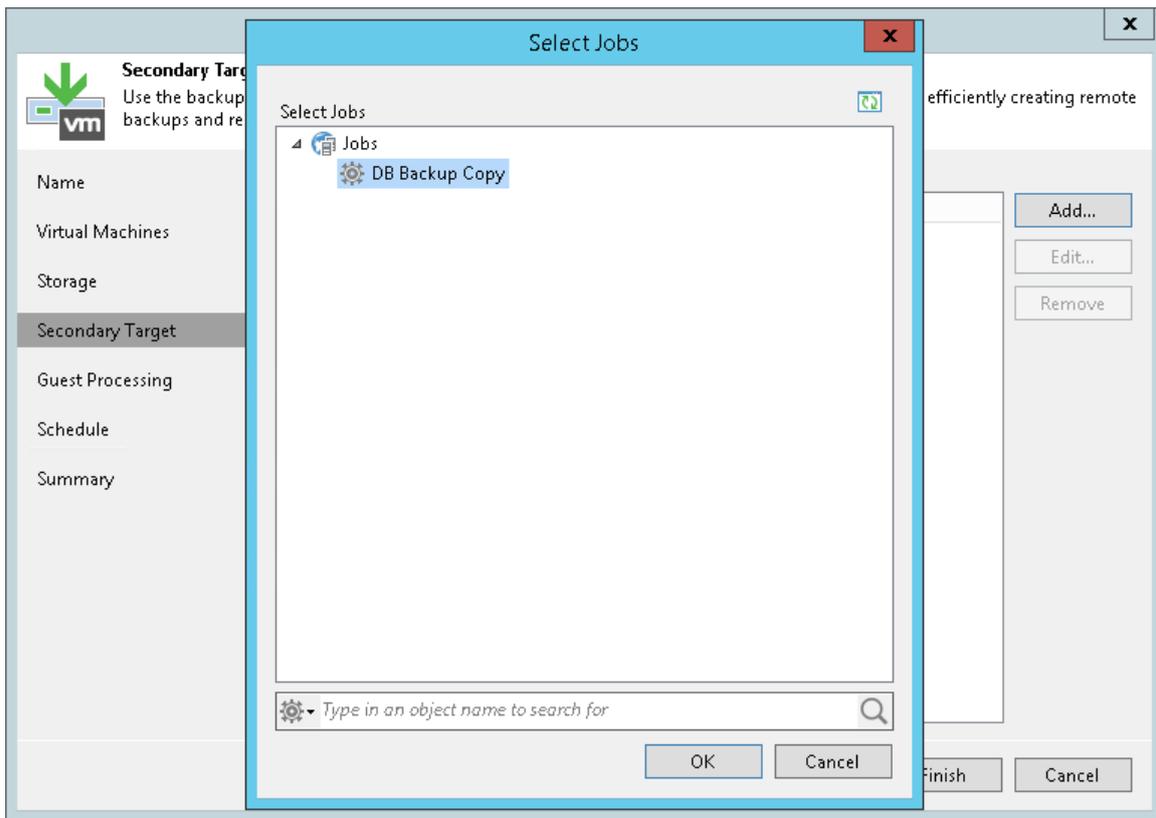
When you link a backup job to the backup copy job, Veeam Backup & Replication automatically updates properties of the backup copy job and adds to it the backup job as a source of data. The backup copy job starts monitoring the backup job linked to it. During every backup copy interval, the backup copy job checks the source backup repository for new restore points. As soon as a backup job session is finished and a new restore point appears on the source backup repository, the backup copy job automatically copies this restore point to the target backup repository.

You can point a backup job to an existing backup copy job using the **Backup Job** wizard. To link jobs:

1. Open the backup job settings and navigate to the **Storage** step. Select the **Configure secondary destination for this job** check box.



- At the **Secondary Target** step of the wizard, click **Add** and choose a backup copy job to which the backup job must be linked. The backup copy job must be already configured on the backup server.



Starting Backup Copy Intervals Manually

As soon as you create a backup copy job and start it, Veeam Backup & Replication automatically enables the job. Backups are copied between backup repositories automatically according to the specified backup copy interval. For more information, see [Backup Copy Intervals](#).

You can start the synchronization process manually. Manual start of the backup copy interval can be helpful, for example, if a new restore point has already appeared on the source backup repository but the previous backup copy interval has not finished yet.

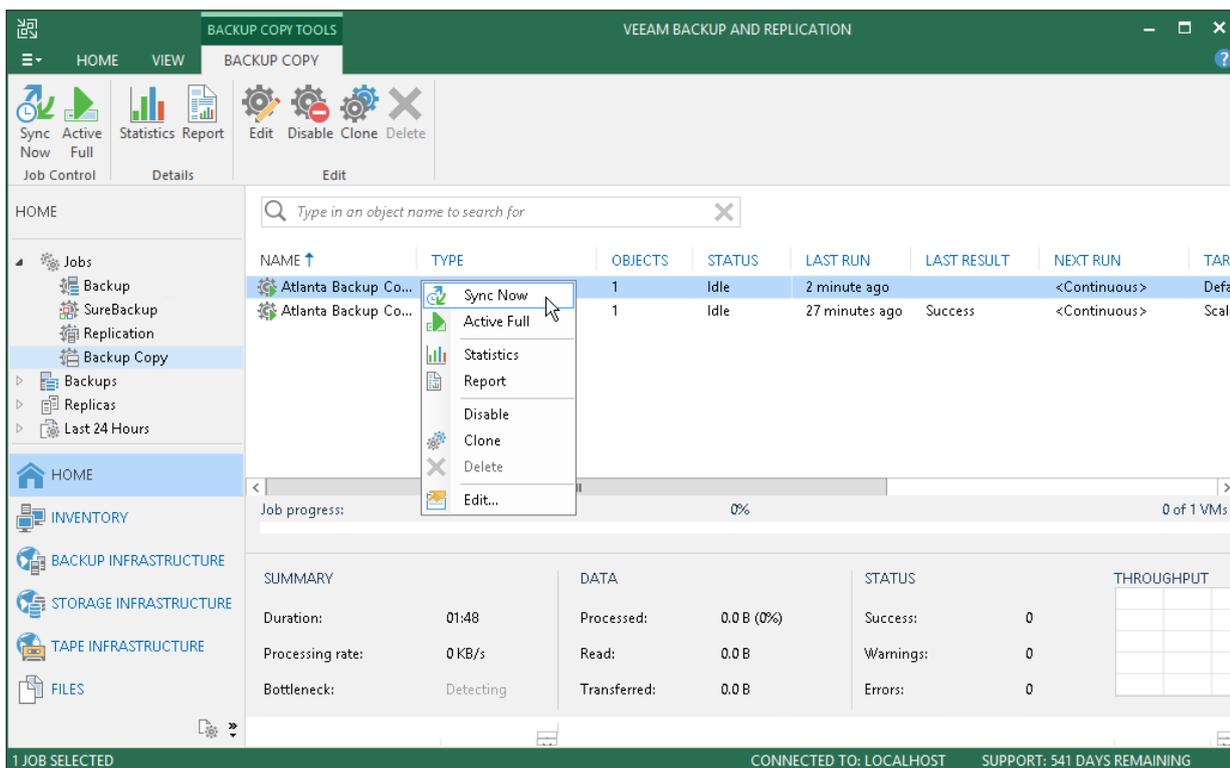
When you manually start the synchronization process, Veeam Backup & Replication creates a new backup copy interval.

- In case of backup copy jobs with minutely and hourly intervals, the backup copy interval is equal to those that are created automatically by the schedule. As a result, the start time of backup copy processing shifts forward.
- In case of backup copy jobs with intervals equal to one or several days, the day of the next backup copy interval shifts forward for the number of days equal to the interval. The start time of the backup copy interval, however, remains the same.

For example, you configure a backup copy job to copy data every 30 days. The backup copy interval starts at 2:00 AM. The manual backup copy interval starts on May 1 at 1:00 PM. The manual backup copy interval will work from 1:00 PM on May 1 till 2:00 AM on May 31. On May 31 at 2:00 AM Veeam Backup & Replication will automatically start a new 30-day backup copy interval.

To start a new data backup copy interval manually:

1. Open the **Home** view.
2. In the inventory pane, select the **Backup Copy** node under **Jobs**.
3. In the working area, select the backup copy job and click **Sync Now** on the ribbon or right-click the backup copy job and select **Sync Now**.

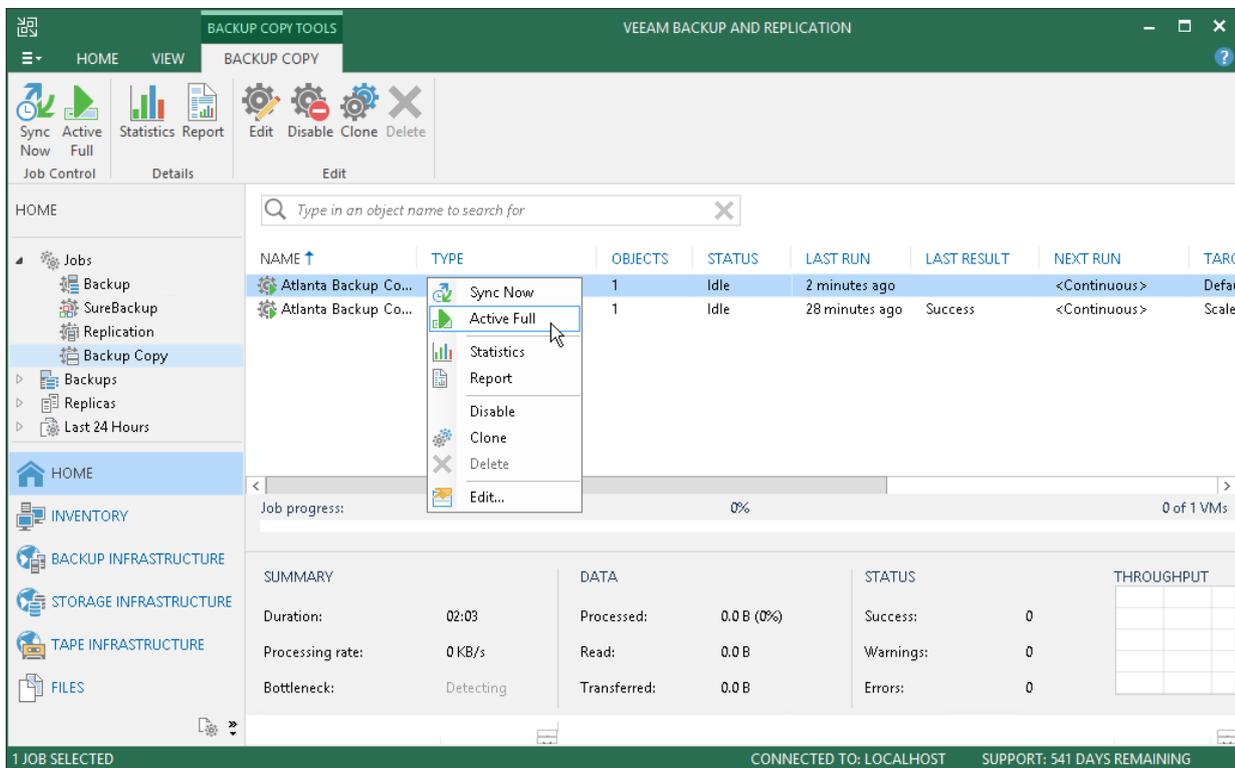


Creating Active Full Backups

You can manually create an ad-hoc full backup – active full backup, and add it to the backup chain on the target backup repository. Active full backup can be helpful if you want to change backup copy job settings, for example, enable or disable encryption. Veeam Backup & Replication will apply new settings starting from this full backup.

To create an active full backup manually:

1. Open the **Home** view.
2. In the inventory pane, select the **Backup Copy** node under **Jobs**.
3. In the working area, select the backup copy job and click **Active Full** on the ribbon or right-click the backup copy job and select **Active Full**. Veeam Backup & Replication will start a new backup copy interval, copy data from the source backup repository and save it in a full backup file on the target backup repository.



Removing Backups from Target Repositories

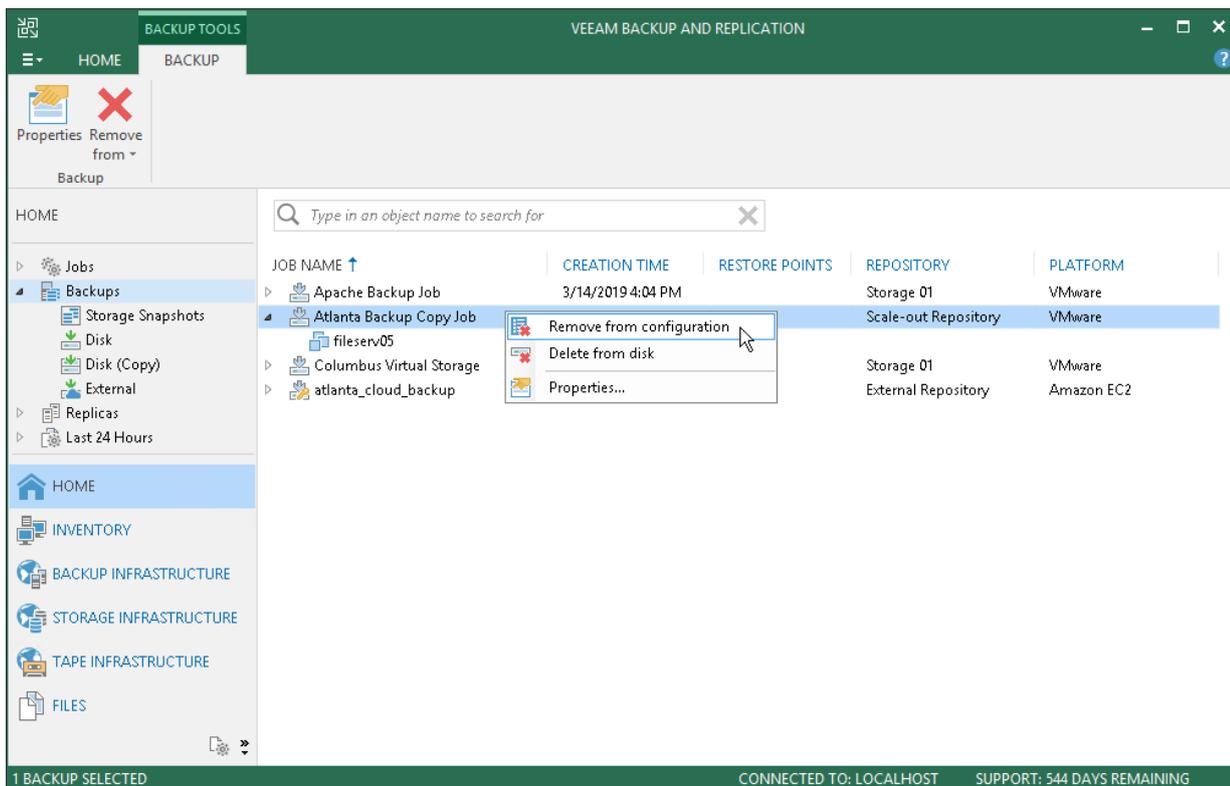
You can remove backups created by backup copy jobs from Veeam Backup & Replication configuration or permanently delete backup chains from the target backup repository.

Removing from Configuration

When you use the **Remove from configuration** option, you delete records about backup copies from the Veeam Backup & Replication console and configuration database. The backup copy job remains in the list of jobs and all backup files remain on the target backup repository. You can easily import backups to the Veeam Backup & Replication console for restore operations at any moment.

To remove from backups:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click the backup copy and select **Remove from configuration**.
4. To remove all weekly, monthly, quarterly and yearly backups created by the job, select the **Include archived full backups** check box and click **Yes**.

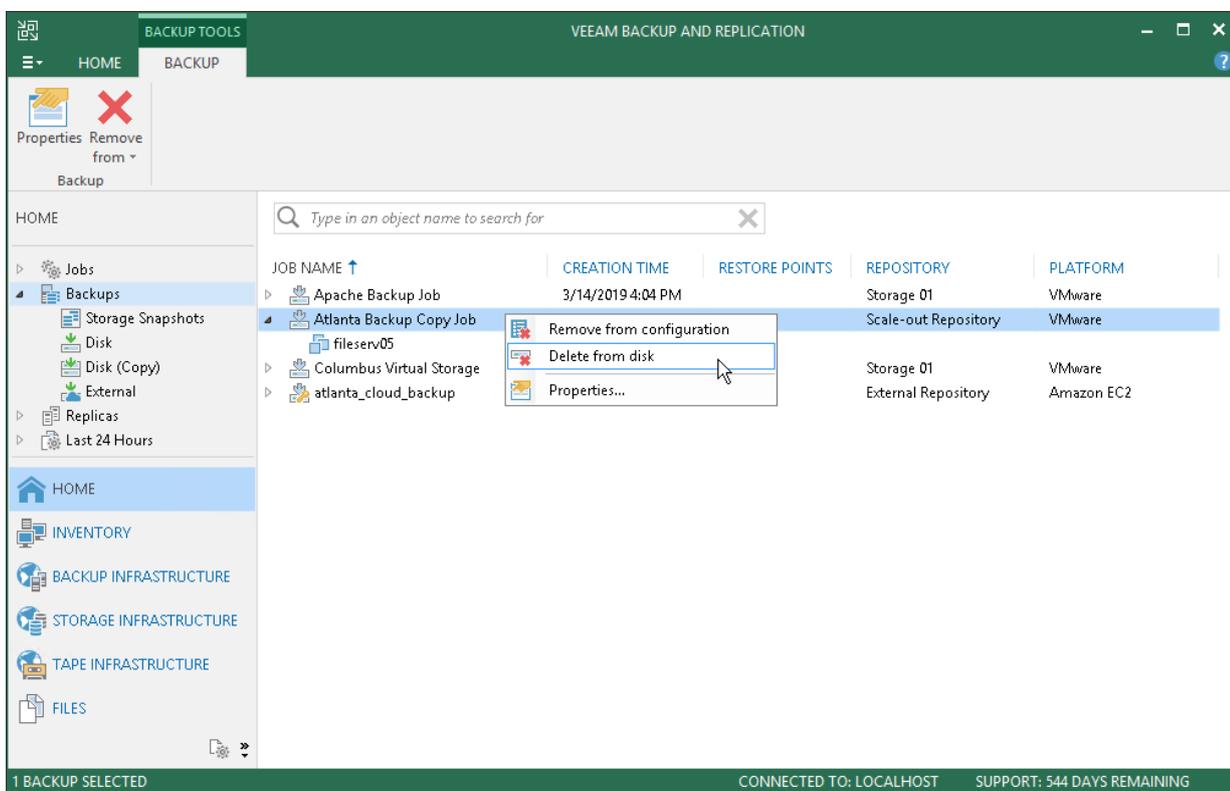


Deleting from Disk

When you use the **Delete from disk** option, you delete records about backup copies from the Veeam Backup & Replication console and configuration database and, additionally, delete backup files themselves from the target backup repository. This option can be used for the whole backup copy or for some machines in the backup copy.

To permanently remove backup copies from the target backup repository:

1. Open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click the backup copy or a machine in the backup copy and select **Delete from disk**.
4. To remove all weekly, monthly, quarterly and yearly backups from disk, select the **Include archived full backups** check box and click **Yes**.



Removing Missing Restore Points

In some cases, one or more restore points in the backup chain may be not accessible. This can happen, for example, if the backup repository is put to the maintenance mode (for scale-out backup repositories), the backup repository is not available or some backup file is missing in the backup chain. Backup chains that contain missing restore points get corrupted – you cannot perform backup copy or restore data from the missing restore point, and restore points that depend on the missing restore point.

You can perform two operations with missing restore points:

- **Forget** – you can remove records about missing restore points from the configuration database. Veeam Backup & Replication will “forget” about missing restore points and will not display them in the console. The backup files themselves will remain on disk (if backup files are still available).
- **Delete** – you can remove records about missing restore points from the configuration database and delete backup files from disk (if backup files are still available).

NOTE:

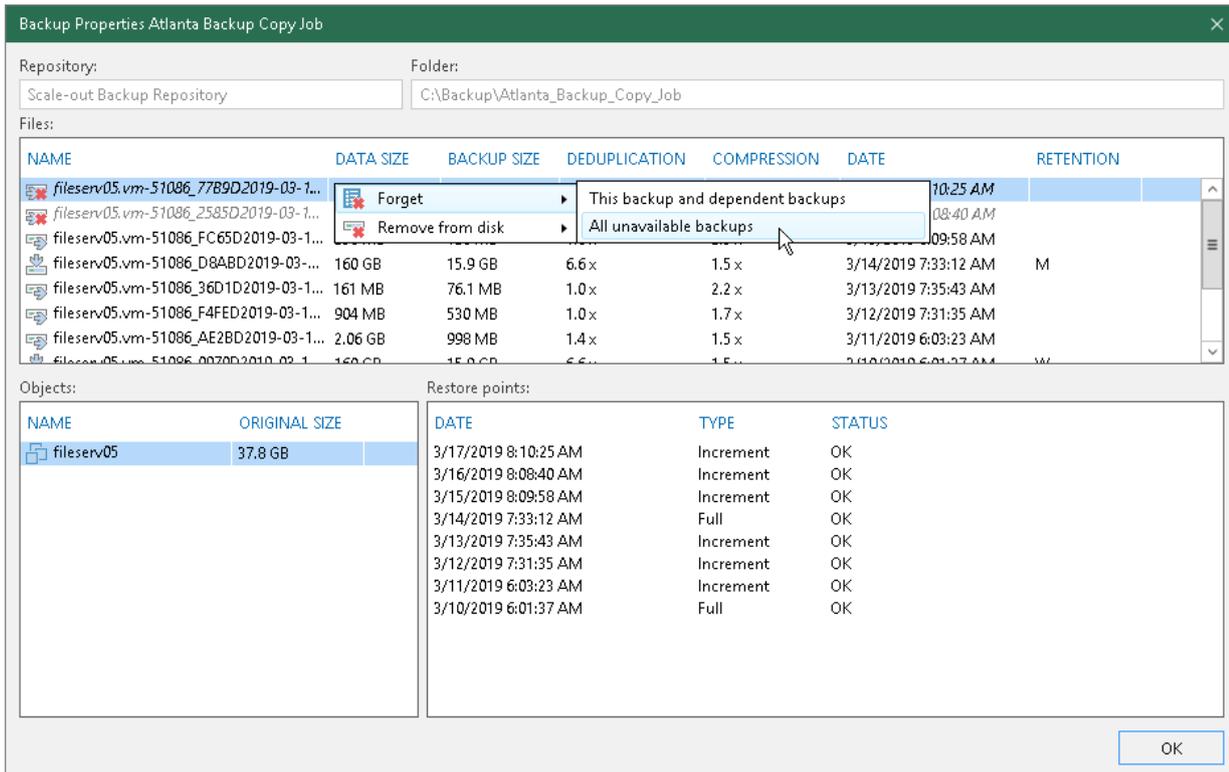
Consider the following:

- The **Forget** and **Delete from disk** options are available only for restore points that are missing from the backup chain or points that depend on missing ones. If the restore point is available in the backup chain and does not depend on a missing restore point, you will not be able to use the **Forget** and **Delete from disk** options for it.
- Veeam Backup & Replication may require some time to update information in the configuration database for restore points that were removed from a backup chain or became inaccessible. Therefore, such restore points may not be displayed in the console as missing restore points. To overcome this situation and reveal missing restore points, you can update information in the configuration database manually. To do that, disable the associated backup copy job and rescan a backup repository that is configured as a target for this job.

To remove records about missing restore points from the configuration database:

1. Open the **Home** view.
2. In the inventory pane, select **Disk (copy)** under **Backups**.
3. In the working area, select the backup and click **Properties** on the ribbon or right-click the backup and select **Properties**.
4. In the **Backup Properties** window, right-click the missing restore point and select **Forget**.
 - To remove only the selected restore point and restore points that depend on it (that is, a part of the backup chain starting from this restore point), select **This and dependent backups**.

- To remove all missing restore points, select **All unavailable backups**.



To remove missing restore points from the configuration database and disk:

1. Open the **Home** view.
2. In the inventory pane, click **Disk (copy)** under **Backups**.
3. In the working area, select the backup and click **Properties** on the ribbon or right-click the backup and select **Properties**.
4. In the **Backup Properties** window, right-click the missing restore point and select **Delete from disk**.
 - To remove only the selected restore point and restore points that depend on it (that is, a part of the backup chain starting from this restore point), select **This and dependent backups**.

- To remove all missing restore points, select **All unavailable backups**.

Backup Properties: Atlanta Backup Copy Job

Repository: Scale-out Backup Repository Folder: C:\Backup\Atlanta_Backup_Copy_Job

Files:

NAME	DATA SIZE	BACKUP SIZE	DEDUPLICATION	COMPRESSION	DATE	RETENTION
fileserv05.vm-51086_77B9D2019-03-1...				1.7x	3/17/2019 8:10:25 AM	
fileserv05.vm-51086_2585D2019-03-1...					3/16/2019 8:08:40 AM	
fileserv05.vm-51086_FC65D2019-03-1...					3/15/2019 8:09:58 AM	
fileserv05.vm-51086_D8ABD2019-03-1...	160 GB	15.9 GB	6.0x	2.2x	3/14/2019 7:33:12 AM	M
fileserv05.vm-51086_36D1D2019-03-1...	161 MB	76.1 MB	1.0x	2.2x	3/13/2019 7:35:43 AM	
fileserv05.vm-51086_F4FED2019-03-1...	904 MB	530 MB	1.0x	1.7x	3/12/2019 7:31:35 AM	
fileserv05.vm-51086_AE2BD2019-03-1...	2.06 GB	998 MB	1.4x	1.5x	3/11/2019 6:03:23 AM	
fileserv05.vm-51086_0070D2019-03-1...	160 GB	15.9 GB	6.0x	1.5x	3/10/2019 6:01:37 AM	W

Objects:

NAME	ORIGINAL SIZE
fileserv05	37.8 GB

Restore points:

DATE	TYPE	STATUS
3/17/2019 8:10:25 AM	Increment	OK
3/16/2019 8:08:40 AM	Increment	OK
3/15/2019 8:09:58 AM	Increment	OK
3/14/2019 7:33:12 AM	Full	OK
3/13/2019 7:35:43 AM	Increment	OK
3/12/2019 7:31:35 AM	Increment	OK
3/11/2019 6:03:23 AM	Increment	OK
3/10/2019 6:01:37 AM	Full	OK

OK

VM Copy

With Veeam Backup & Replication, you can run a VM copy job to create an independent fully-functioning copy of a VM or VM container on the selected storage. VM copying can be helpful if you want to move your datacenter, create a test lab and so on.

The produced copy of a VM is stored decompressed, in a native VMware vSphere format, so it can be started right away. Although VM copy is similar to replication in many respects, there are several important differences.

- VM copy is a single-use process (that is, every run of a VM copy job mirrors a VM in its latest state). Due to their nature, VM copy jobs do not support incremental runs.
- Veeam Backup & Replication does not create and maintain restore points for VM copies. If you schedule to run a VM copy job periodically, every new run will overwrite the existing copy.
- With the VM copy job, all VM disks are copied as thick, while replication allows you to preserve the format of disks or convert the disk format on the fly.
- There are no failover or failback possibilities for a VM copy.

VM copy jobs use the same infrastructure components as backup jobs (for details, see [Backup Architecture](#)). In addition to available scenarios, you can also copy VMs to a target folder on any server or host connected to the backup server.

Copying VMs

With VM copy jobs you can create a fully-functional copy of a VM and store this copy on the backup repository or storage device. VM copying may be helpful if you want to move your datacenter to another location, archive a VM before decommissioning and so on.

To create a VM copy, you must configure a VM copy job. One job can be used to process one VM or more VMs.

You can configure a job and start it immediately or save the job to start it later. Jobs can be started manually or scheduled to run automatically at specific time.

Before creating a VM copy job, [check prerequisites](#). Then use the **New VM Copy Job** wizard to configure a VM copy job.

Before You Begin

Before you create a VM copy job, check the following prerequisites:

- Backup infrastructure components that will take part in the VM copying process must be added to the backup infrastructure and properly configured. These include the source ESX(i) host and server or backup repository on which you plan to store the VM copy.
- The target storage device must have enough free space to store created VM copies. To receive alerts about low space on the storage device, configure global notification settings. For more information, see [Specifying Other Notification Settings](#).
- If you plan to use pre-freeze and/or post-thaw scripts, you must create scripts before you configure the VM copy job.

Mind the following limitations:

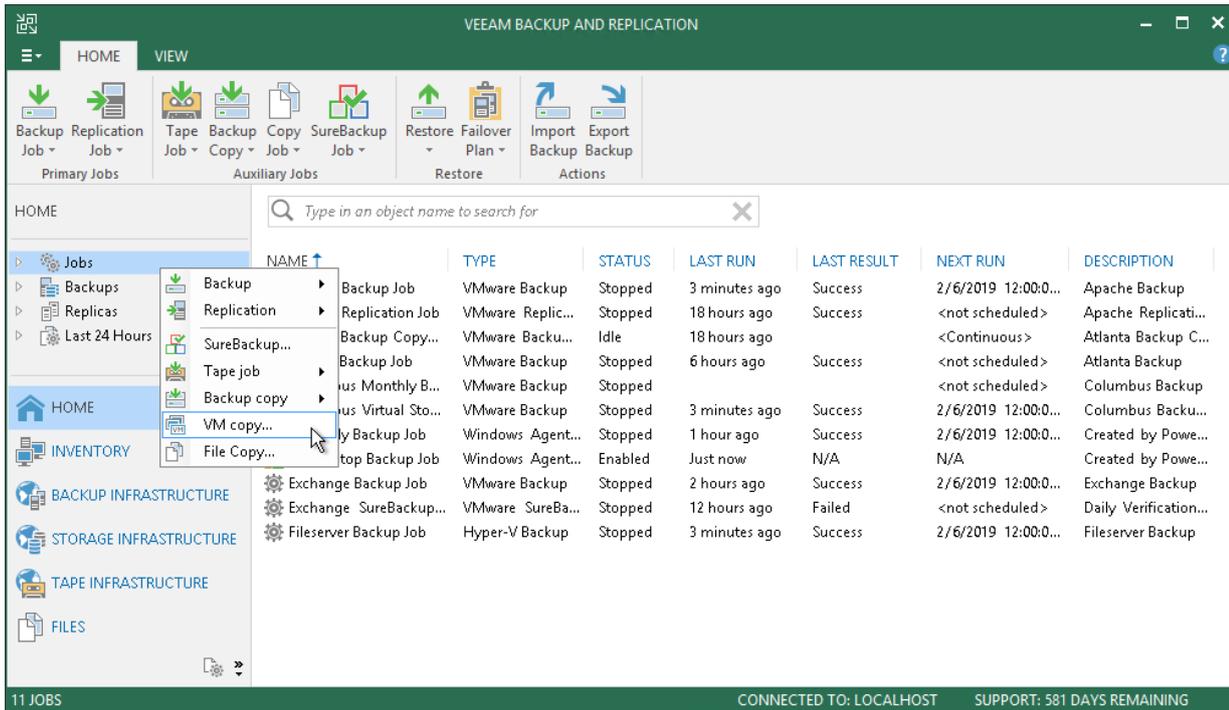
- Due to Microsoft limitations, you cannot use Microsoft Azure Active Directory credentials to perform application-aware processing on VMs running Microsoft Windows 10.
- If you use tags to categorize virtual infrastructure objects, check limitations for VM tags. For more information, see [VM Tags](#).

Step 1. Launch VM Copy Job Wizard

To run the **VM Copy Job** wizard, do either of the following:

- On the **Home** tab, click **Copy Job > Virtual machine**.
- Open the **Home** view. In the inventory pane, right-click **Jobs** and select **VM Copy**.
- Open the **Inventory** view, in the working area select the VMs, click **Add to VM Copy** on the ribbon and select **New job** or right-click the VMs area and select **Add to VM copy job > New job**. In this case, the selected VMs will be automatically added to the VM copy job. You can add other VMs to the job when passing through the wizard steps.

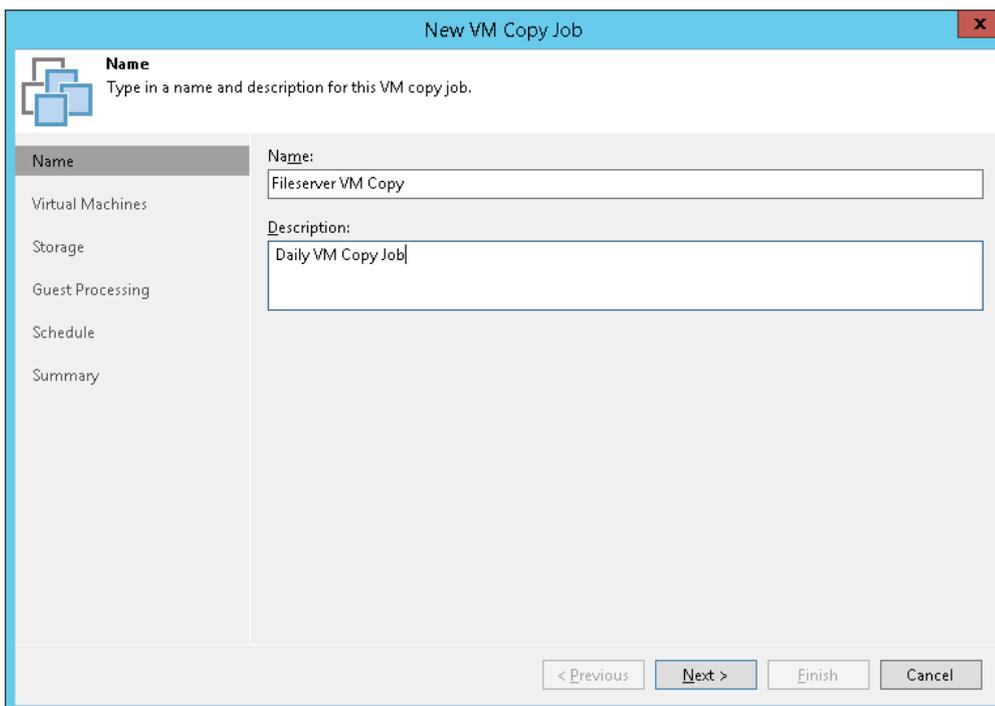
- You can quickly add the VMs to an already existing job. To do this, open the **Inventory** view, in the working area select the VMs and click **Add to VM Copy > name of the job** on the ribbon or right-click the VMs and select **Add to VM copy job > name of the job**.



Step 2. Specify Job Name and Description

At the **Name** step of the wizard, specify a name and description for the VM copy job.

- In the **Name** field, enter a name for the VM copy job.
- 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.



Step 3. Select VMs to Copy

At the **Virtual Machines** step of the wizard, select VMs and VM containers that you want to copy.

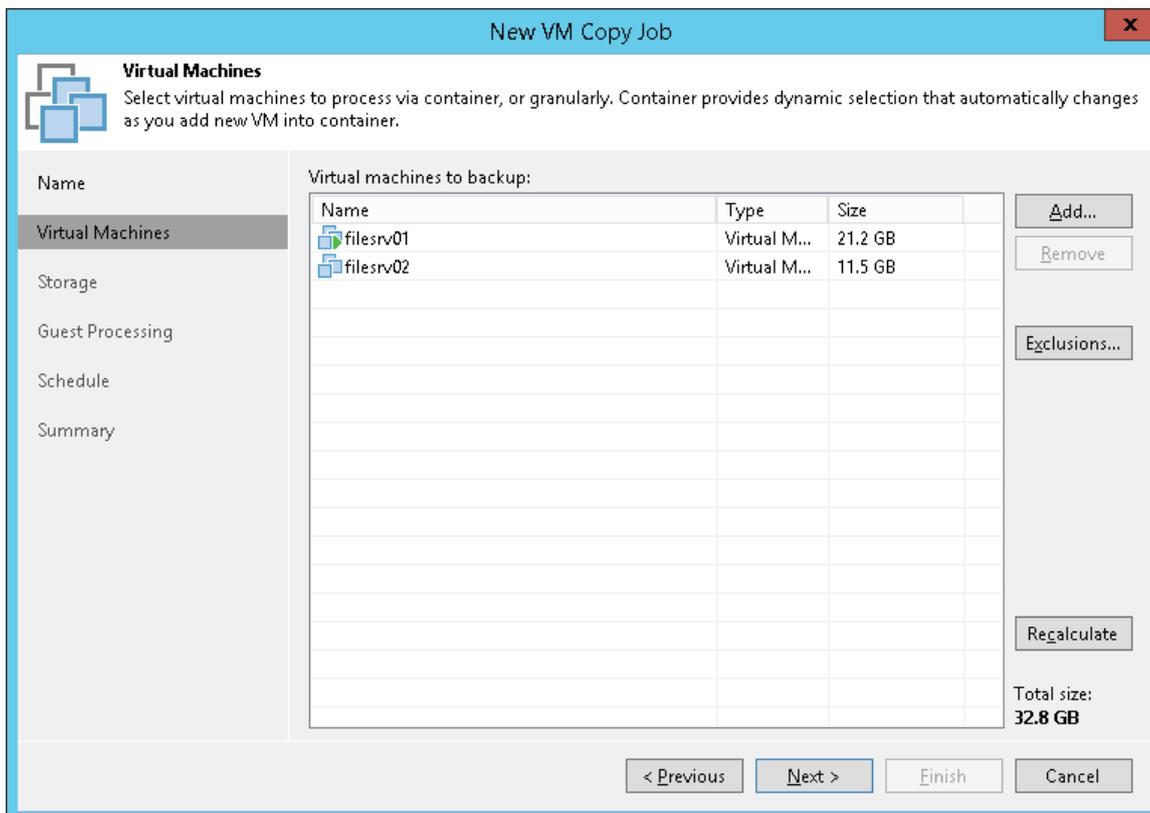
Jobs with VM containers are dynamic in their nature. If a new VM is added to the container in the virtual infrastructure after the VM copy job is created, Veeam Backup & Replication will automatically update the job settings to include the added VM.

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 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]**.

The initial size of VMs and VM containers added to the VM copy job is displayed in the **Size** column in the list. The total size of objects is displayed in the **Total size** field. Use the **Recalculate** button to refresh the total size value after you add a new object to the job.



Step 4. Exclude Objects from VM Copy Job

After you have added VMs and VM containers to the job, you can specify which objects you want to exclude from the VM copy. You can exclude the following types of objects:

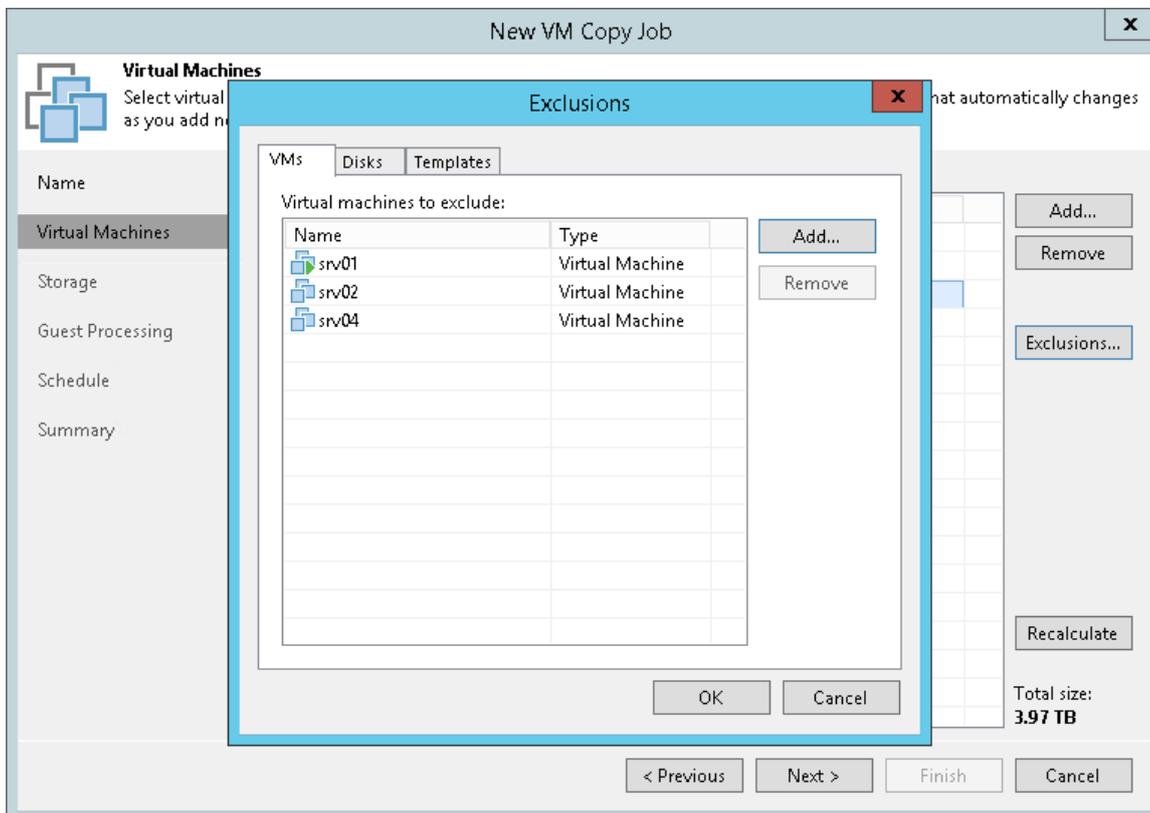
- [VMs from VM containers](#)
- [Specific VM disks](#)
- [VM templates](#)

NOTE:

Veeam Backup & Replication automatically excludes VM log files from VM copies to make copying process faster and reduce the size of the resulting file.

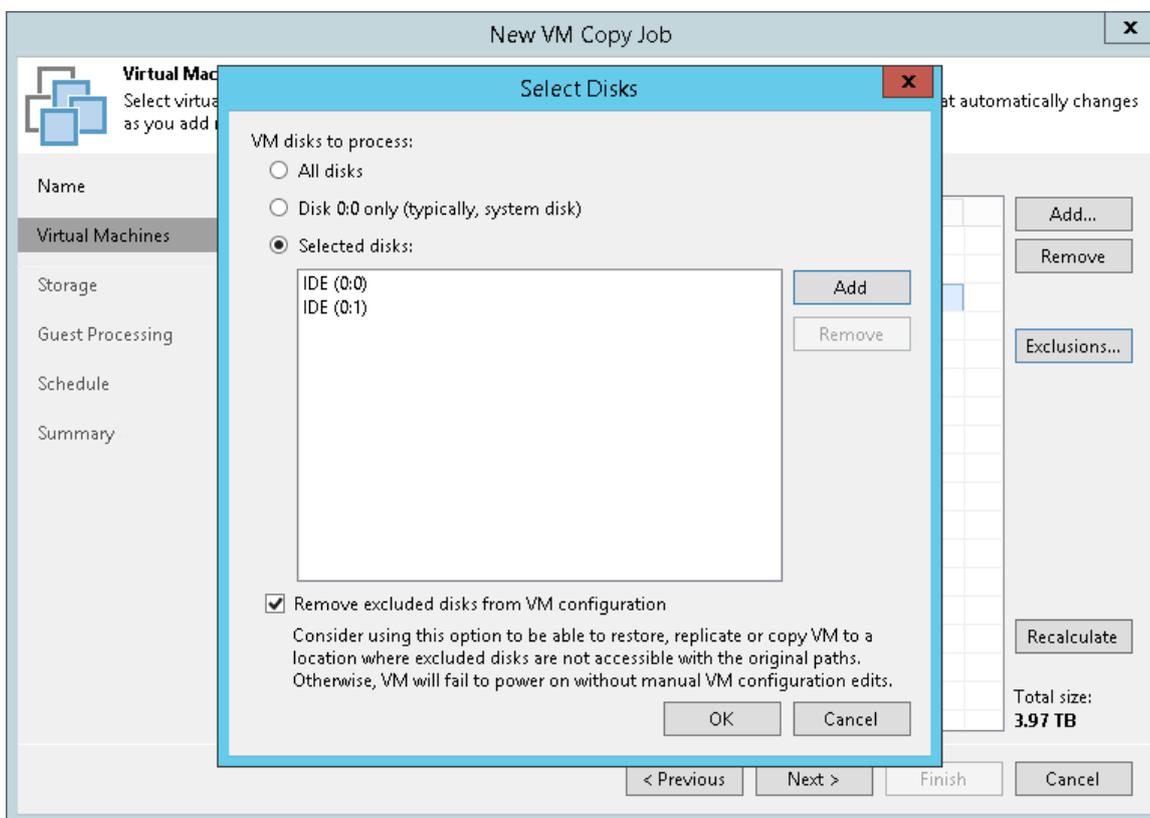
To exclude VMs from a VM container:

1. At the **Virtual Machines** step of the wizard, select a VM container added to the job and click **Exclusions**.
2. Click the **VMs** tab.
3. Click **Add**.
4. 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.
5. In the displayed tree, select the necessary object and click **Add**. Use the **Show full hierarchy** check box to display the hierarchy of all VMware Servers added to Veeam Backup & Replication.
6. Click **OK**.



To exclude VM disks:

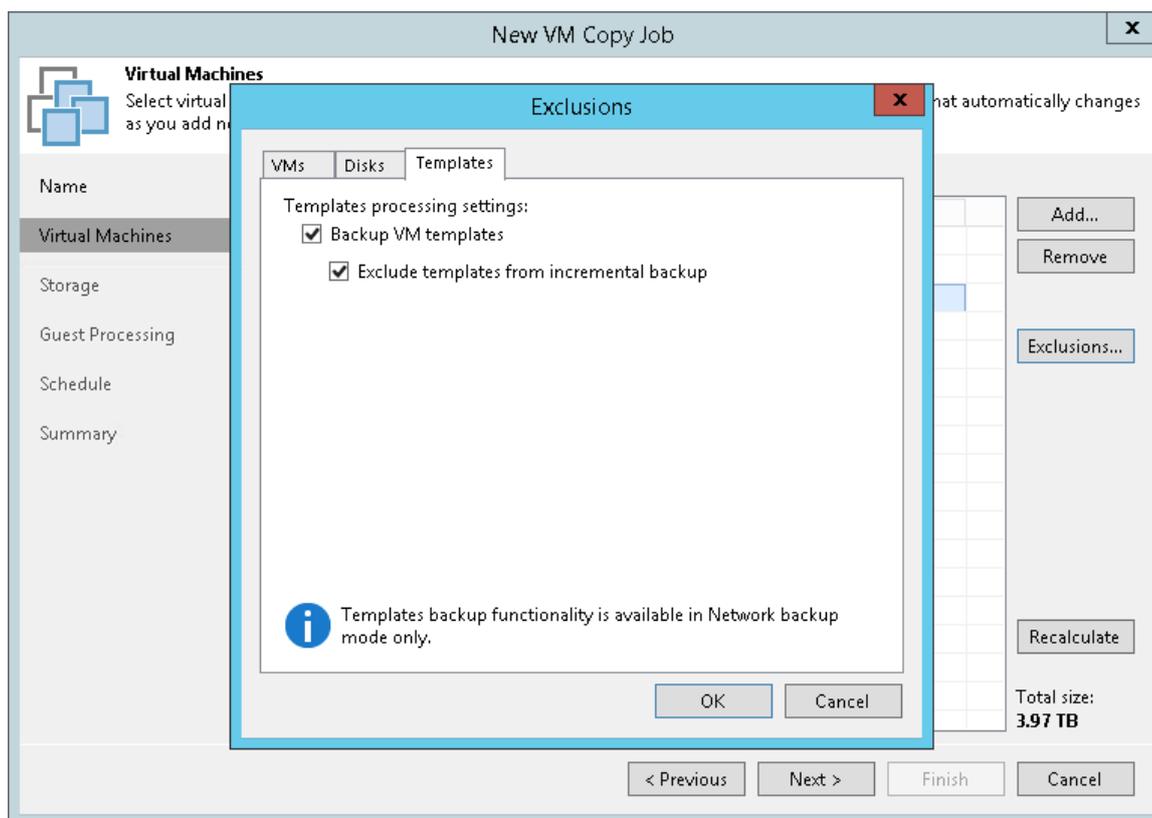
1. At the **Virtual Machines** step of the wizard, select a VM or VM container added to the job and click **Exclusions**.
2. Click the **Disks** tab.
3. Select the VM in the list and click **Edit**. If you want to exclude disks of a VM added as a part of the container, click **Add** to include the VM in the list as a standalone object.
4. Choose disks that you want to copy. You can choose to process all disks, 0:0 disks (typically, the system disks) or add to the list custom IDE, SCSI or SATA disks.
5. Select the **Remove excluded disks from VM configuration** check box. Veeam Backup & Replication will modify the VMX file of a copied VM to remove excluded disks from the VM configuration. If you use the VM copy to register the VM in a location where excluded disks are not accessible with the original paths, you will not have to manually edit the VM configuration file to be able to power on the VM.



To exclude VM templates:

1. At the **Virtual Machines** step of the wizard, select a VM or VM container added to the job and click **Exclusions**.
2. Click the **Templates** tab.
3. Clear the **Backup VM templates** check box.

4. If you want to include VM templates into the full VM copy only, leave the **Backup VM templates** check box selected and select the **Exclude templates from incremental backup** check box.



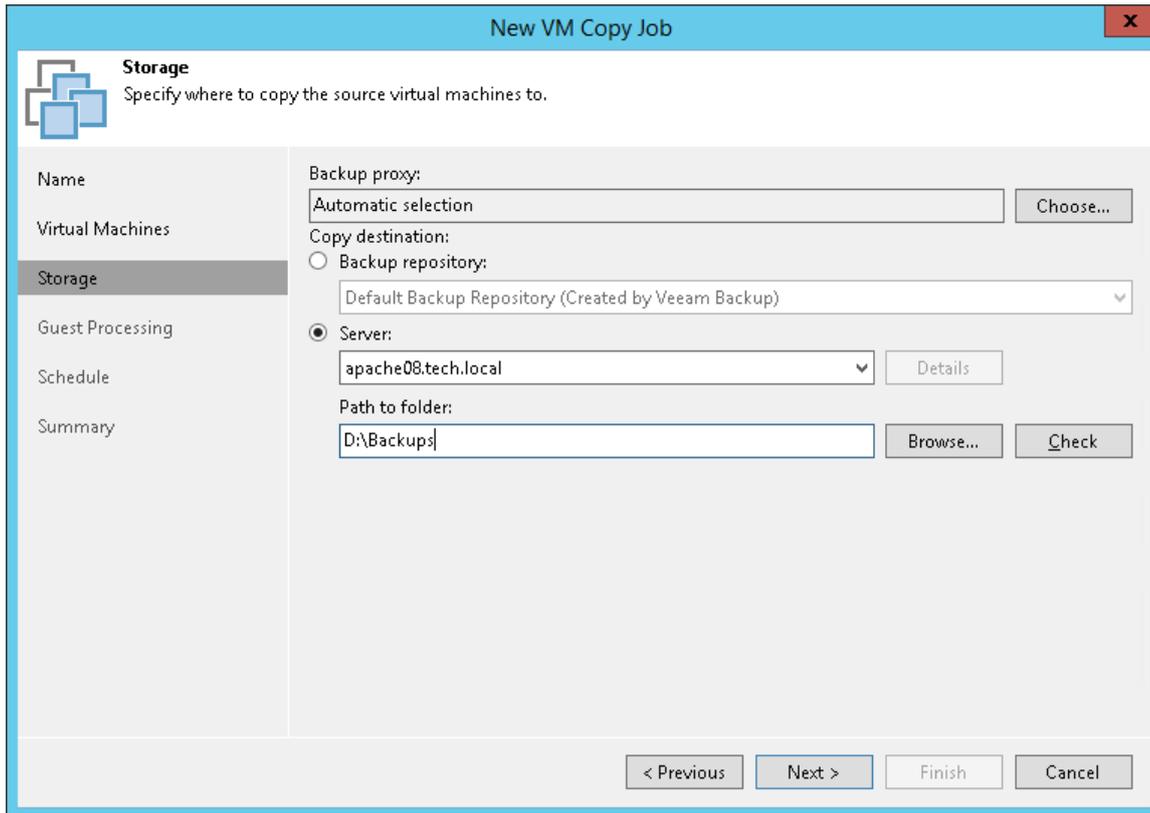
Step 5. Specify Copy Destination

At the **Storage** step of the wizard, select which backup proxy must be used for VM data transporting and specify the destination for the VM copy.

1. Click **Choose** next to the **Backup proxy** field to select a backup proxy.
 - If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that have access to the source datastore and automatically assign an optimal backup proxy for processing VM data.

Veeam Backup & Replication assigns backup proxies to VMs included in the VM copy job one by one. Before processing a new VM in the VM list, Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use for data retrieval and the current workload on the backup proxies to select the most appropriate one for VM processing.
 - If you choose **Use the selected backup proxy servers only**, you can explicitly select backup proxies that the job must use. It is recommended that you select at least two backup proxies to ensure that the VM copy job starts if one of the proxies fails or loses its connectivity to the source datastore.
2. In the **Copy destination** section, select a location where the created VM copy must be stored.
 - Select a backup repository from the list if you want to create a VM copy on the backup repository configured in the backup infrastructure. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on it.
 - Select **Server** if you want to store the VM copy on a disk or storage device attached to the server. From the **Server** list, select a server added to the backup infrastructure. In the **Path to folder** field, specify a folder on the server where the created VM copy must be stored.

Use the **Check** button to see how much free space is available in the target location.



Step 6. Specify Guest Processing Settings

At the **Guest Processing** step of the wizard, you can enable the following settings for VM guest OS processing:

- [Application-aware processing](#)
- [Transaction log handling for Microsoft SQL Server](#)
- [Transaction log handling for Oracle](#)
- [Use of pre-freeze and post-thaw scripts](#)

To coordinate guest processing activities, Veeam Backup & Replication deploys a runtime process on the VM guest OS. The process runs only during guest processing and is stopped immediately after the processing is finished (depending on the selected option, during the VM copy job session or after the replication job completes).

You must specify a user account that will be used to connect to the VM guest OS and deploy the runtime process:

1. From the **Guest OS credentials** list, select a user account with local administrator privileges on the VM guest OS. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. For more information, see [Managing Credentials](#).
2. By default, Veeam Backup & Replication uses the same credentials for all VMs in the job. If some VM requires a different user account, click **Credentials** and enter custom credentials for the VM.

IMPORTANT!

Credentials for application-aware processing and guest OS file indexing for Microsoft Windows VMs must be specified in the following format:

- For Active Directory accounts – *DOMAIN\Username*
- For local accounts – *Username* or *HOST\Username*

3. If you have added Microsoft Windows VMs to the job, specify which guest interaction proxy Veeam Backup & Replication can use to deploy the runtime process on the VM guest OS. On the right of the **Guest interaction proxy** field, click **Choose**.
 - Leave **Automatic selection** to let Veeam Backup & Replication automatically select the guest interaction proxy.
 - Select **Use the selected guest interaction proxy servers only** to explicitly define which servers will perform the guest interaction proxy role. The list of servers contains Microsoft Windows servers added to the backup infrastructure.

To check if Veeam Backup & Replication can communicate with VMs added to the job and deploy the runtime process on their guest OSes, click **Test Now**. Veeam Backup & Replication will use the specified credentials to connect to all VMs in the list.

NOTE:

The guest interaction proxy functionality is available in the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication.

New VM Copy Job

Guest Processing
Choose guest OS processing options available for running VMs.

Name

Virtual Machines

Storage

Guest Processing

Schedule

Summary

Enable application-aware processing
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual VMs and applications **Applications...**

Guest OS credentials

TECH\Administrator (TECH\Administrator, last edited: 14 days ago) **Add...**

[Manage accounts](#)

Customize guest OS credentials for individual VMs and operating systems **Credentials...**

Guest interaction proxy:
Automatic selection **Choose...**

Test Now

< Previous Next > Finish Cancel

Application-Aware Processing

If you add to the VM copy job VMs running VSS-aware applications, you can enable application-aware processing to create a transactionally consistent VM copy. The transactionally consistent VM copy guarantees proper recovery of applications on VMs without data loss.

To enable application-aware processing:

1. Select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the VM and click **Edit**.

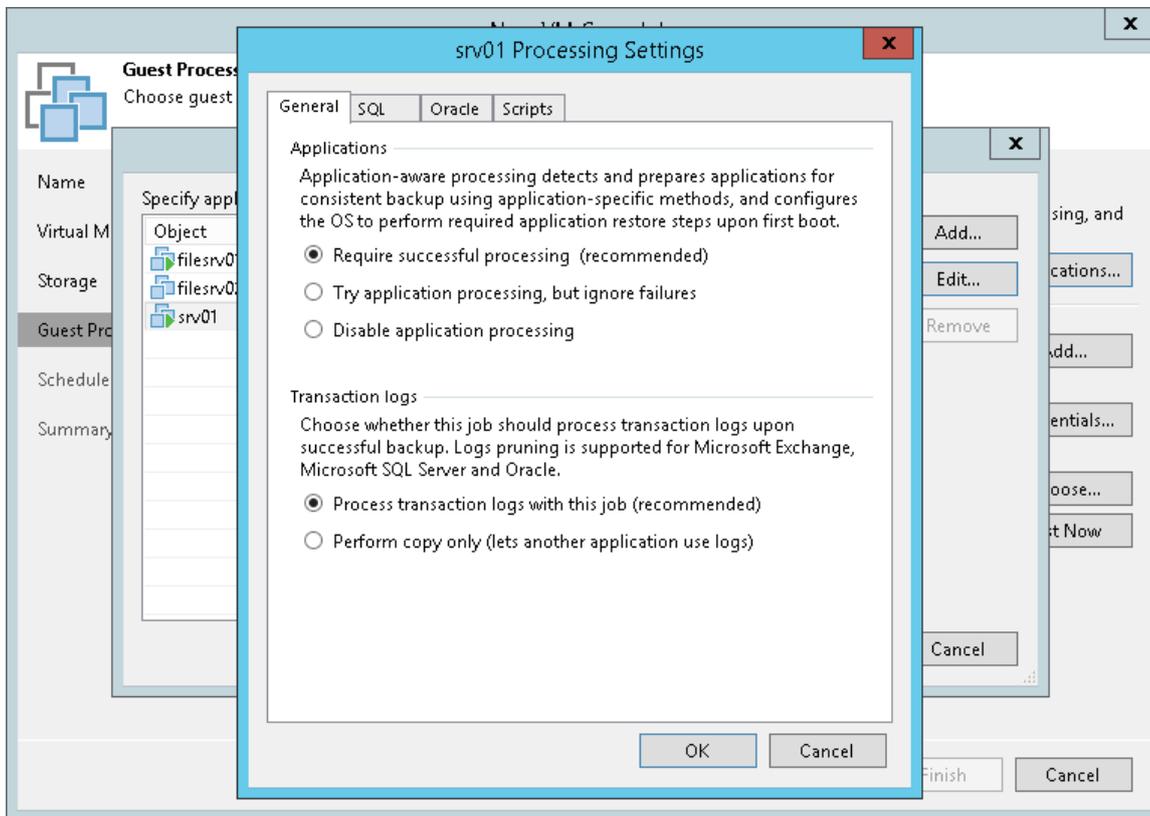
To define custom settings for a VM added as a part of the VM container, you must include the VM in the list as a standalone object. To do this, click **Add** and choose a VM whose settings you want to customize. Then select the VM in the list and define the necessary settings.

4. On the **General** tab, in the **Applications** section specify the VSS behavior scenario:
 - o Select **Require successful processing** if you want Veeam Backup & Replication to stop the VM copy process if any VSS errors occur.
 - o Select **Try application processing, but ignore failures** if you want to continue the VM copy process even if VSS errors occur. This option is recommended to guarantee completion of the job. The created VM image will not be transactionally consistent but crash consistent.
 - o Select **Disable application processing** if you do not want to enable quiescence for the VM.
5. [For Microsoft Exchange, Microsoft SQL and Oracle VMs] In the **Transaction logs** section, specify if Veeam Backup & Replication must process transaction logs or copy-only VM copies must be created.
 - a. Select **Process transaction logs with this job** if you want Veeam Backup & Replication to process transaction logs.

[For Microsoft Exchange VMs] With this option selected, the runtime process running on the VM guest OS will wait for the VM copy job to complete successfully and then trigger truncation of transaction logs. If the VM copy job fails, the logs will remain untouched on the VM guest OS until the next start of the runtime process.

[For Microsoft SQL Server VMs and Oracle VMs] You will have to specify settings for transaction log handling on the **SQL** and **Oracle** tabs of the **VM Processing Settings** window. For more information, see [Transaction Log Settings: Microsoft SQL](#) and [Transaction Log Settings: Oracle](#).

- b. Select **Perform copy only** if you use another backup tool to perform VM guest level backup or replication, and this tool maintains consistency of the database state. Veeam Backup & Replication will create a copy-only VM image for the selected VMs. The copy-only VM image preserves the chain of full/differential backup files and transaction logs on the VM. For more information, see <http://msdn.microsoft.com/en-us/library/ms191495.aspx>.

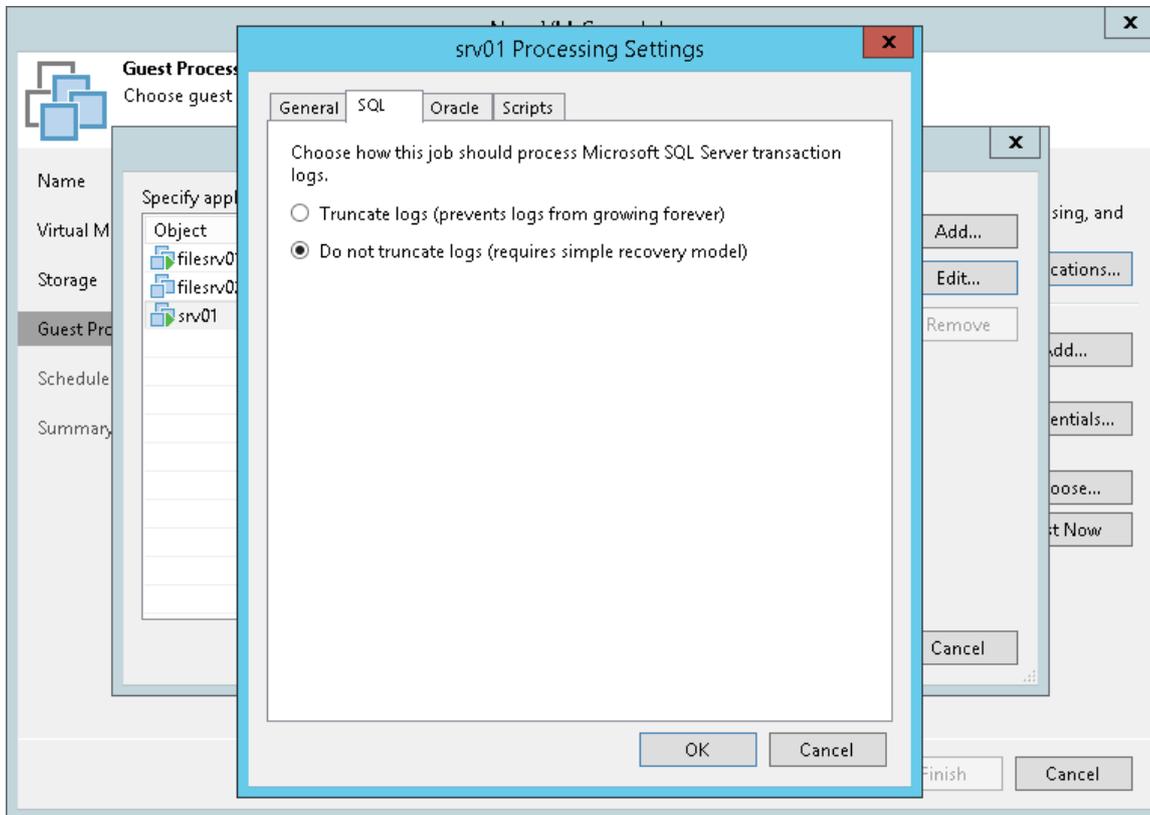


Transaction Log Handling: Microsoft SQL Server

If you copy a Microsoft SQL VM, you can specify how Veeam Backup & Replication must process transaction logs:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the Microsoft SQL Server VM and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.
5. In the **VM Processing Settings** window, click the **SQL** tab.
6. Specify how transaction logs must be processed:
 - Select **Truncate logs** if you want Veeam Backup & Replication to trigger truncation of transaction logs only after the job completes successfully. In this case, the runtime process will wait for the job to complete and then trigger truncation of transaction logs. If the VM copy job fails, the logs will remain untouched on the VM guest OS until the next start of the runtime process.

- Select **Do not truncate logs** if you do not want Veeam Backup & Replication to truncate logs at all. This option is recommended if you are using another backup tool to perform VM guest-level backup or replication, and this tool maintains consistency of the database state. In such scenario, Veeam Backup & Replication will not trigger transaction log truncation. After you fail over to the necessary restore point of the VM copy, you will be able to apply transaction logs to get the database system to the necessary point in time between VM copy job sessions.



Transaction Log Handling: Oracle

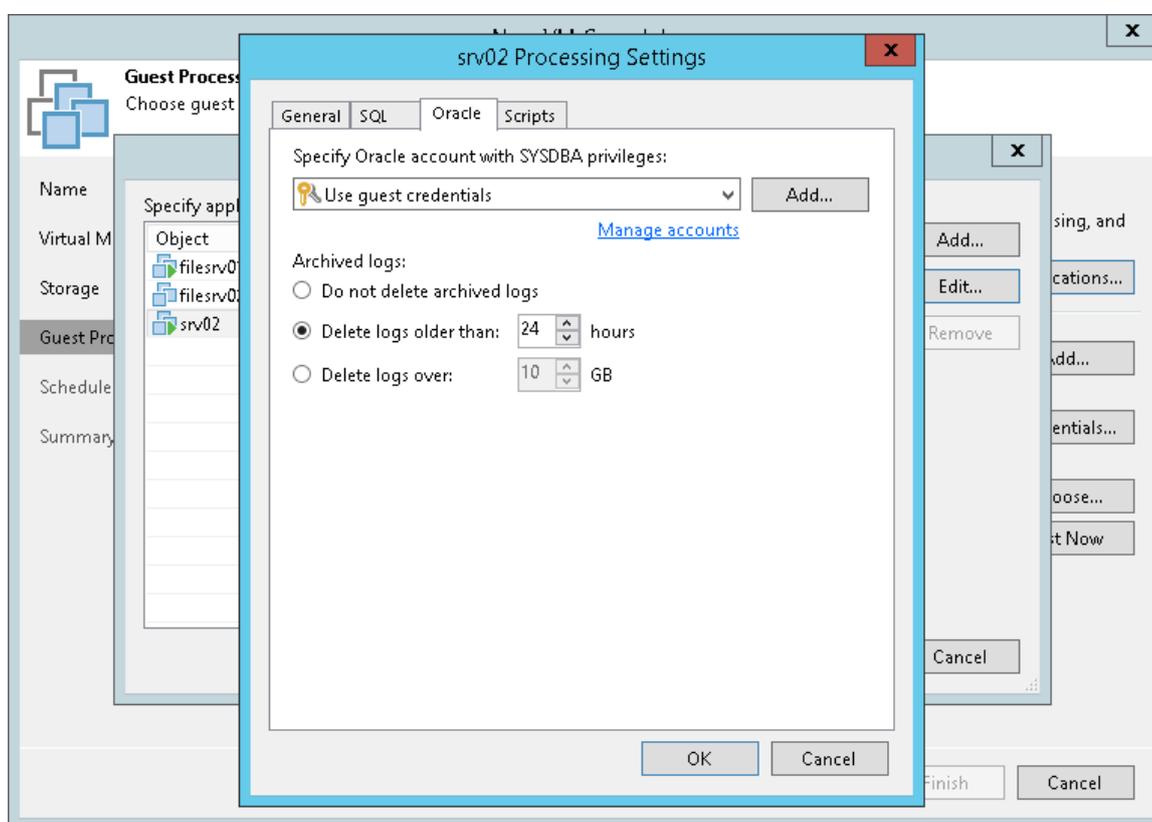
If you copy an Oracle VM, you can specify how Veeam Backup & Replication must process transaction logs:

1. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select the Oracle VM and click **Edit**.
4. In the **Transaction logs** section, select **Process transaction logs with this job**.
5. In the **VM Processing Settings** window, click the **Oracle** tab.
6. In the **Specify Oracle account with SYSDBA privileges** section, specify a user account that Veeam Backup & Replication will use to connect to the Oracle database. The account must have SYSDBA rights on the Oracle database.

You can select **Use guest credentials** in the list of user accounts. In this case, Veeam Backup & Replication will use the account specified at the **Guest Processing** step of the wizard to access the VM guest OS and connect to the Oracle database.

7. In the **Archived logs** section, specify if Veeam Backup & Replication must truncate transaction logs on the Oracle VM:
- Select **Do not truncate archived logs** if you want Veeam Backup & Replication to preserve archived logs on the VM guest OS. When the Vm copy job completes, the runtime process will not truncate transaction logs.

It is recommended that you select this option for databases for which the ARCHIVELOG mode is turned off. If the ARCHIVELOG mode is turned on, transaction logs on the VM guest OS may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs him-/herself.
 - Select **Truncate logs older than <N> hours** or **Truncate logs over <N> GB** if you want Veeam Backup & Replication to truncate archived logs that are older than <N> hours or larger than <N> GB. The runtime process running on the VM guest OS will wait for the VM copy job to complete successfully and then trigger transaction logs truncation via Oracle Call Interface (OCI). If the job does not manage to copy the Oracle VM, the logs will remain untouched on the VM guest OS until the next start of the runtime process.



Pre-Freeze and Post-Thaw Scripts

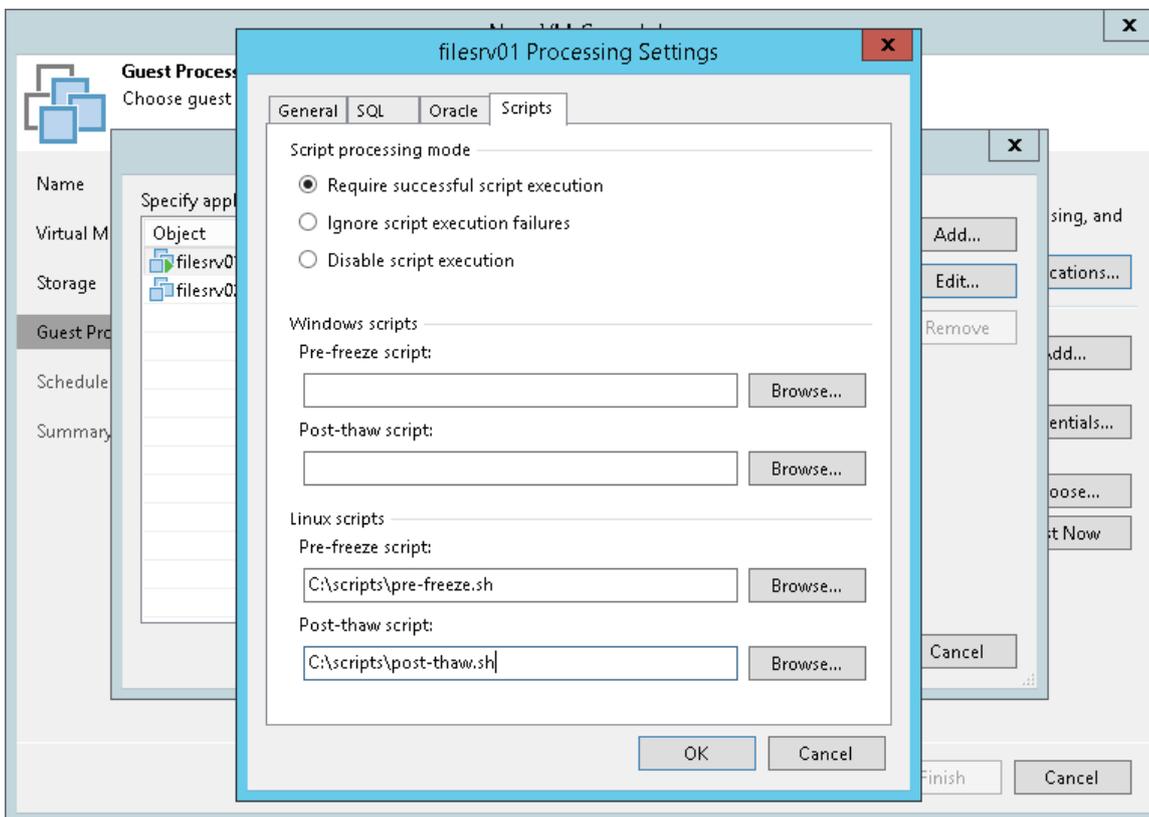
If you plan to copy VMs running applications that do not support VSS, you can instruct Veeam Backup & Replication to run custom pre-freeze and post-thaw scripts for these VMs. The pre-freeze script quiesces the VM file system and application data to bring the VM to a consistent state before Veeam Backup & Replication triggers a VM snapshot. After the VM snapshot is created, the post-thaw script brings the VM and applications to their initial state.

To specify pre-freeze and post-thaw scripts for the job:

1. At the **Guest Processing** step, click **Applications**.
2. In the displayed list, select the VM and click **Edit**.

3. Click the **Scripts** tab.
4. In the **Script processing mode** section, specify the scenario for scripts execution:
 - Select **Require successful script execution** if you want Veeam Backup & Replication to stop the VM copy process if the script fails.
 - Select **Ignore script execution failures** if you want to continue the VM copy process even if script errors occur.
 - Select **Disable script execution** if you do not want to run scripts for the VM.
5. In the **Windows scripts** section, specify paths to pre-freeze and post-thaw scripts for Microsoft Windows VMs. Veeam Backup & Replication supports scripts in the EXE, BAT and CMD format.
6. In the **Linux scripts** section, specify paths to pre-freeze and/or post-thaw scripts for Linux VMs. Veeam Backup & Replication supports scripts of the SH file type.

If you have added to the job a VM container with Microsoft Windows and Linux VMs, you can select to execute both Microsoft Windows and Linux scripts for the VM container. When the job starts, Veeam Backup & Replication will automatically determine what OS type is installed on the VM and apply corresponding scripts to quiesce this VM.



Step 7. Define the Job Schedule

At the **Schedule** step of the wizard, select to run the VM 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 perform VM replication.

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.

A repeatedly run job is started by the following rules:

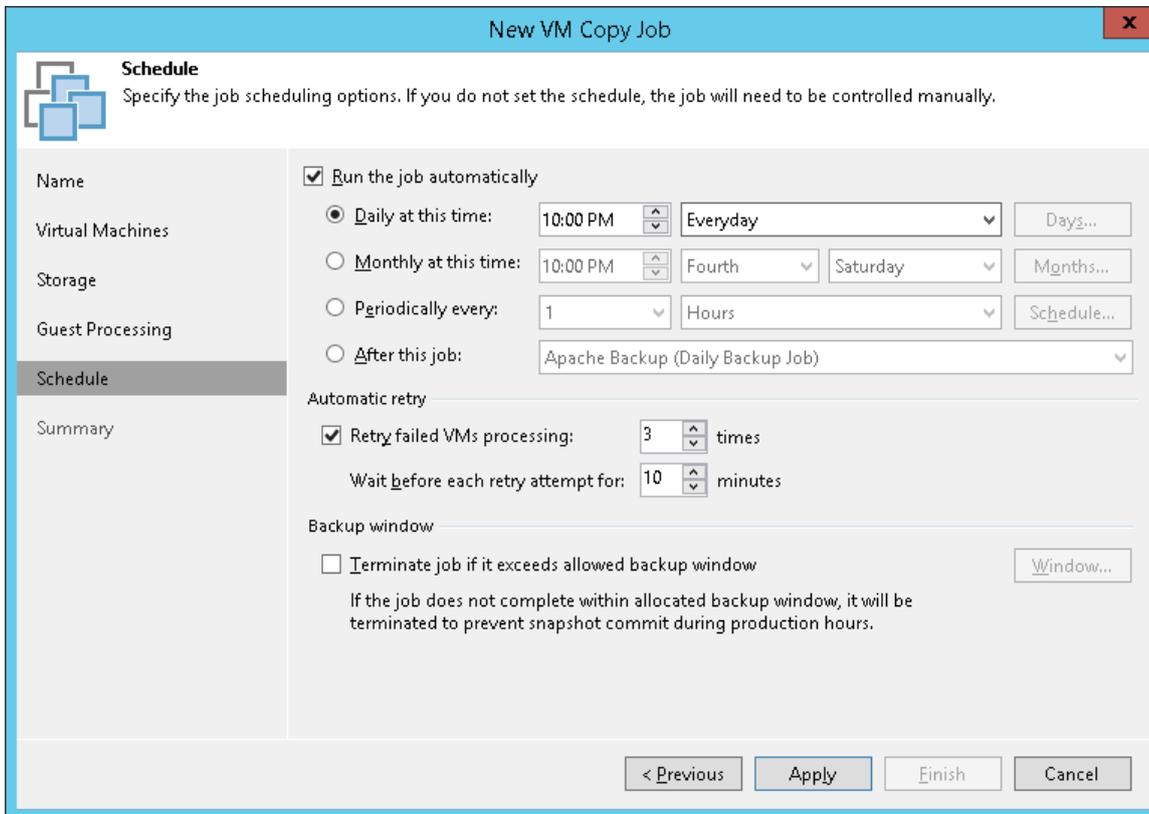
- Veeam Backup & Replication always starts counting defined intervals from 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.
- If you define permitted hours for the job, after the denied interval is over, Veeam Backup & Replication 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, select the **After this job option** and choose the preceding job from the list.
3. In the **Automatic retry** section, define whether Veeam Backup & Replication must attempt to run the job again if the job fails for some reason. During a job retry, Veeam Backup & Replication processes failed VMs only. Enter the number of attempts to run the job and define time spans between them. If you select continuous schedule for the job, Veeam Backup & Replication will retry the job for the defined number of times without any time intervals between the job sessions.
4. In the **Backup window** section, determine a time interval within which the job must be completed. The backup window prevents the job from overlapping with production hours and ensures it does not provide unwanted overhead on your production environment. To set up a backup window for the job:
- a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.
 - b. In the **Time Periods** section, define the allowed hours and prohibited hours for VM copying. If the job exceeds the allowed window, it will be automatically terminated.

NOTE:

The **After this job** function will only start a job if the first job in the chain is started automatically by schedule. If the first job is started manually, jobs chained to it will not be started.

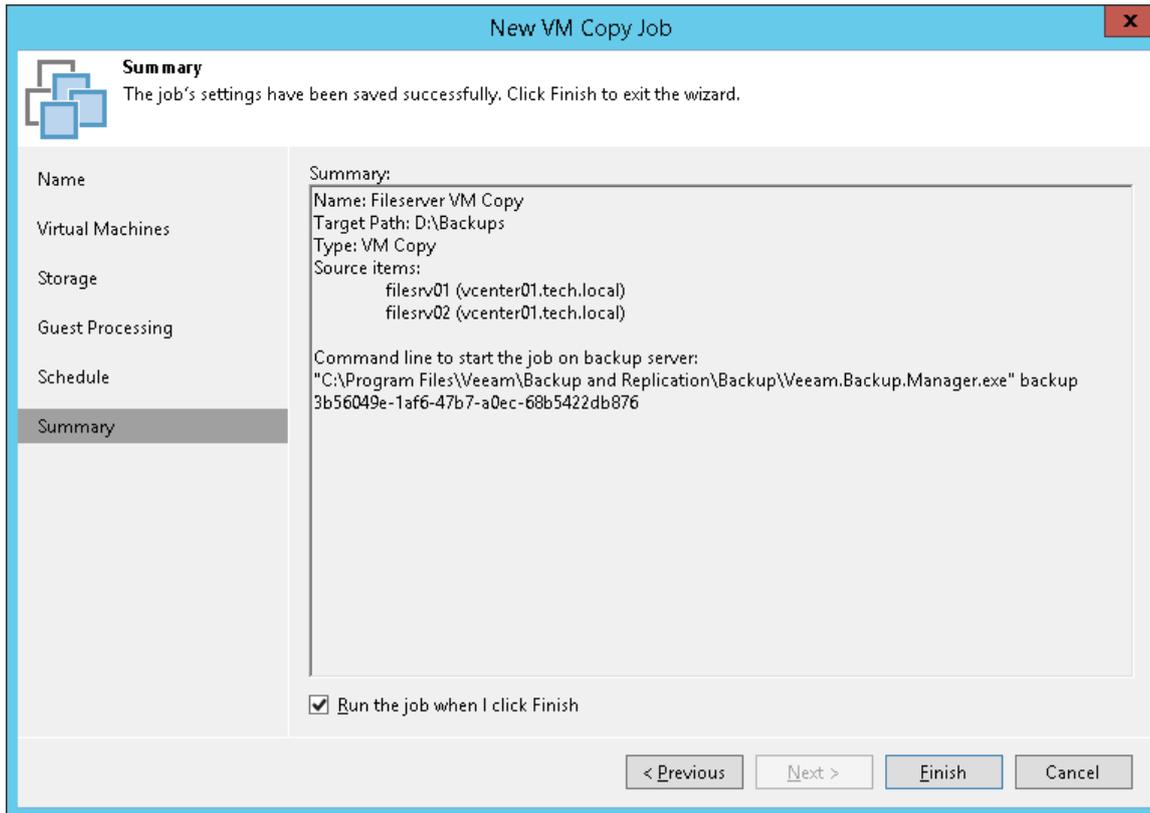


Step 8. Finish Working with Wizard

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

1. Review details of the VM 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.



File Copy

You can copy and move files and folders between servers and hosts added to the backup infrastructure. For file copying operations, Veeam Backup & Replication offers a Windows Explorer-like user interface familiar to a Microsoft Windows user. You can copy files manually or schedule file copy jobs to run automatically by the defined schedule.

The file copy functionality is not intended for creating backups of VM guest OS files. Use backup jobs to create VM image-level backups instead.

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.

File copy jobs let you copy files between the following backup infrastructure objects:

- Virtualization hosts
- Microsoft Windows servers
- Linux servers
- ExaGrid storage appliances used as backup repositories

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.

Mind the following limitations:

- File copy is not supported for Unix systems, for example, Solaris, FreeBSD and AIX.
- Veeam Backup & Replication does not preserve the Access Control List (ACL) settings for copied guest OS folders. The ACL settings are preserved for files only.

TIP:

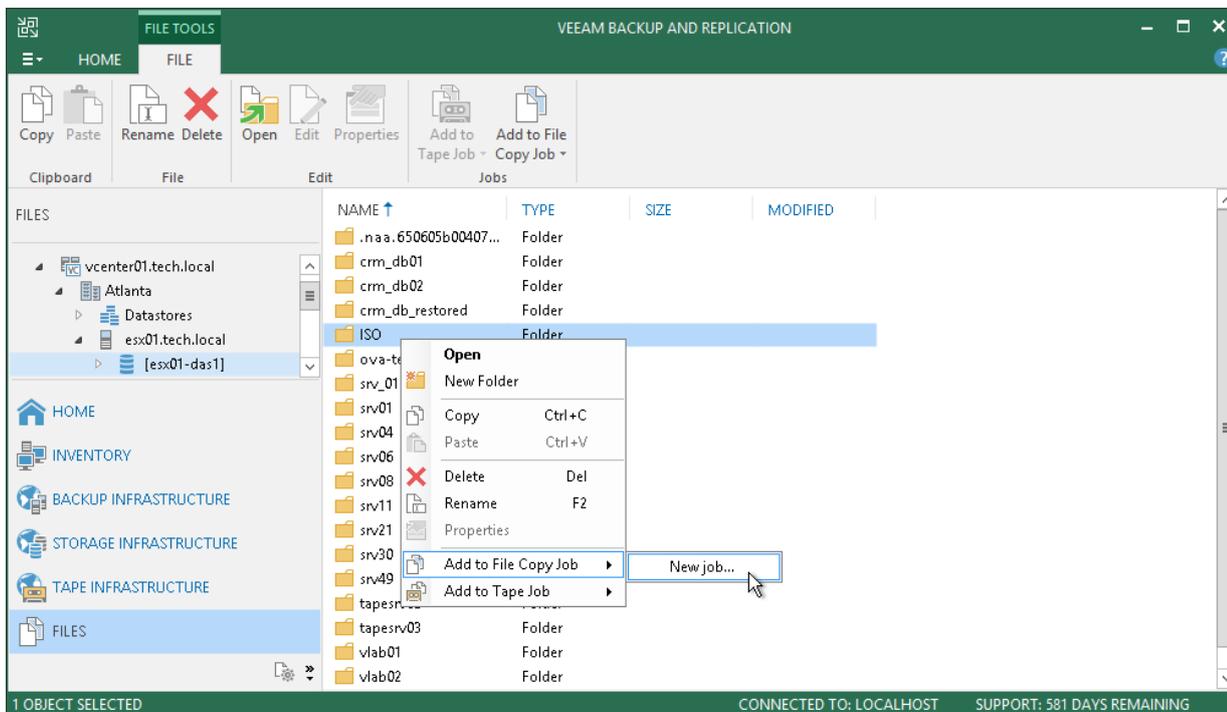
You can restore the ACL settings for recovered guest OS files and folders using [Instant File-Level Restore](#).

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 **Copy Job > File**.
- 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 & Replication 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.

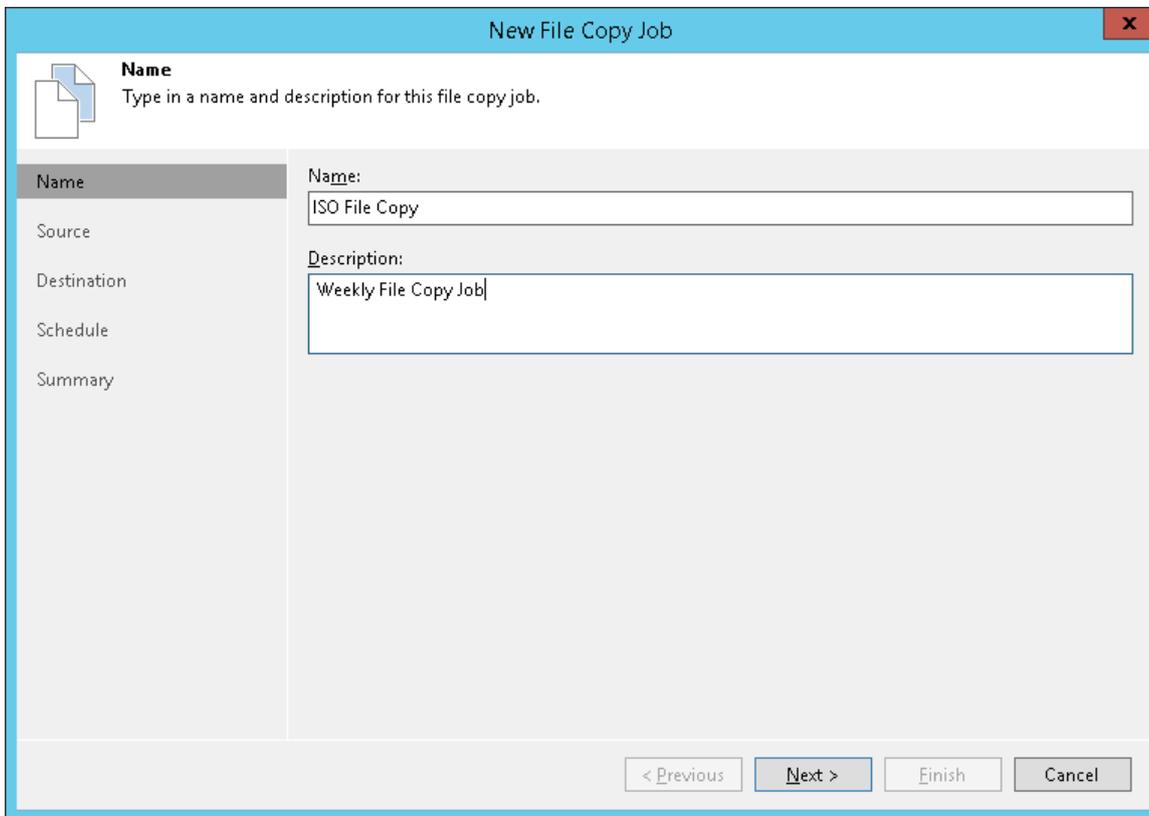
You can add files and folders to already existing jobs. To do this, open the **Files** view, in the working area right-click necessary objects and select **Add to file copy job > name of the job**.



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.



The screenshot shows a window titled "New File Copy Job" with a close button (X) in the top right corner. The window contains a wizard interface with a left-hand navigation pane and a main content area. The navigation pane has five items: "Name" (selected and highlighted), "Source", "Destination", "Schedule", and "Summary". The main content area has a sub-header "Name" with a document icon and the instruction "Type in a name and description for this file copy job." Below this, there are two text input fields. The first is labeled "Name:" and contains the text "ISO File Copy". The second is labeled "Description:" and contains the text "Weekly File Copy Job". At the bottom of the window, there are four buttons: "< Previous", "Next >", "Finish", and "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.

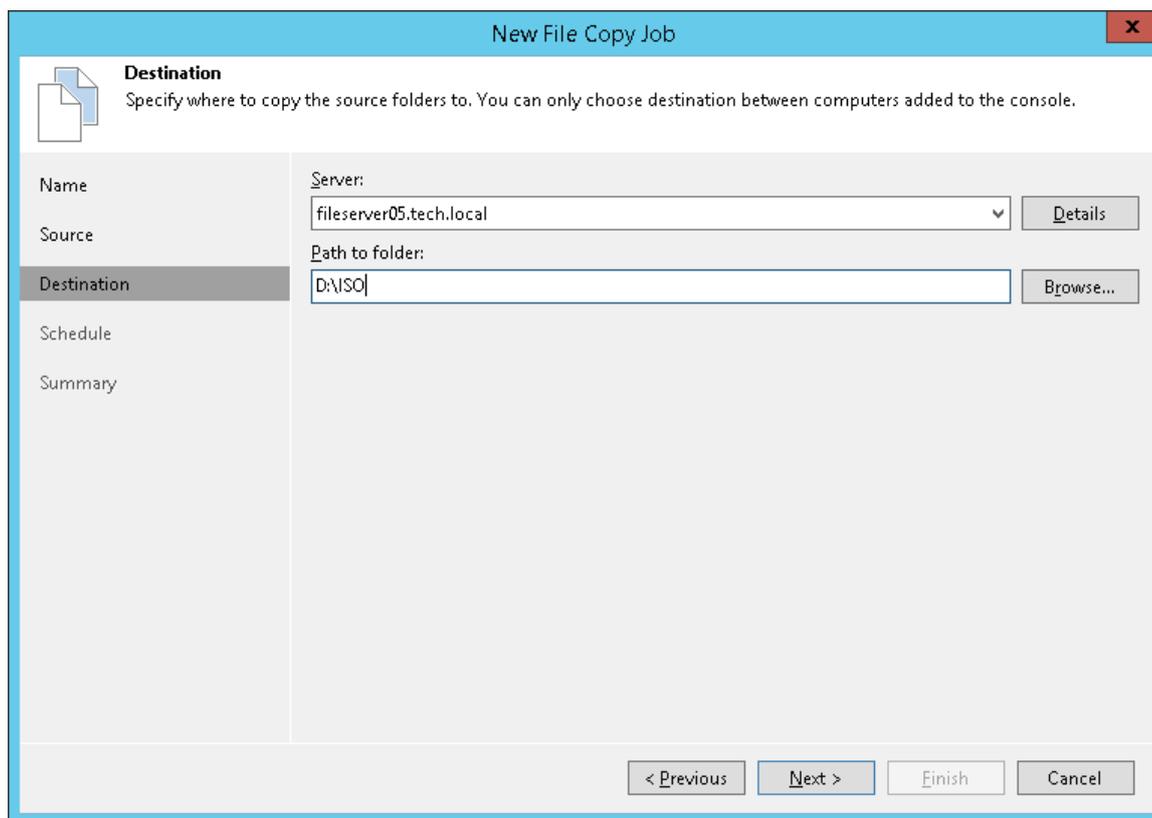
You can use the following sources for the file copy job:

- Virtualization hosts
- Microsoft Windows servers
- Linux servers
- ExaGrid storage appliances used as backup repositories

To 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.

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 in the 'Destination' step. The window title is 'New File Copy Job'. Below the title bar, there is a document icon and the heading 'Destination' with the instruction: 'Specify where to copy the source folders to. You can only choose destination between computers added to the console.' On the left side, there is a vertical navigation pane with the following items: 'Name', 'Source', 'Destination' (which is highlighted), 'Schedule', and 'Summary'. The main area contains two input fields: 'Server:' with a dropdown menu showing 'fileserver05.tech.local' and a 'Details' button; and 'Path to folder:' with a text box containing 'D:\ISO\|' and a 'Browse...' button. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 5. Define 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.

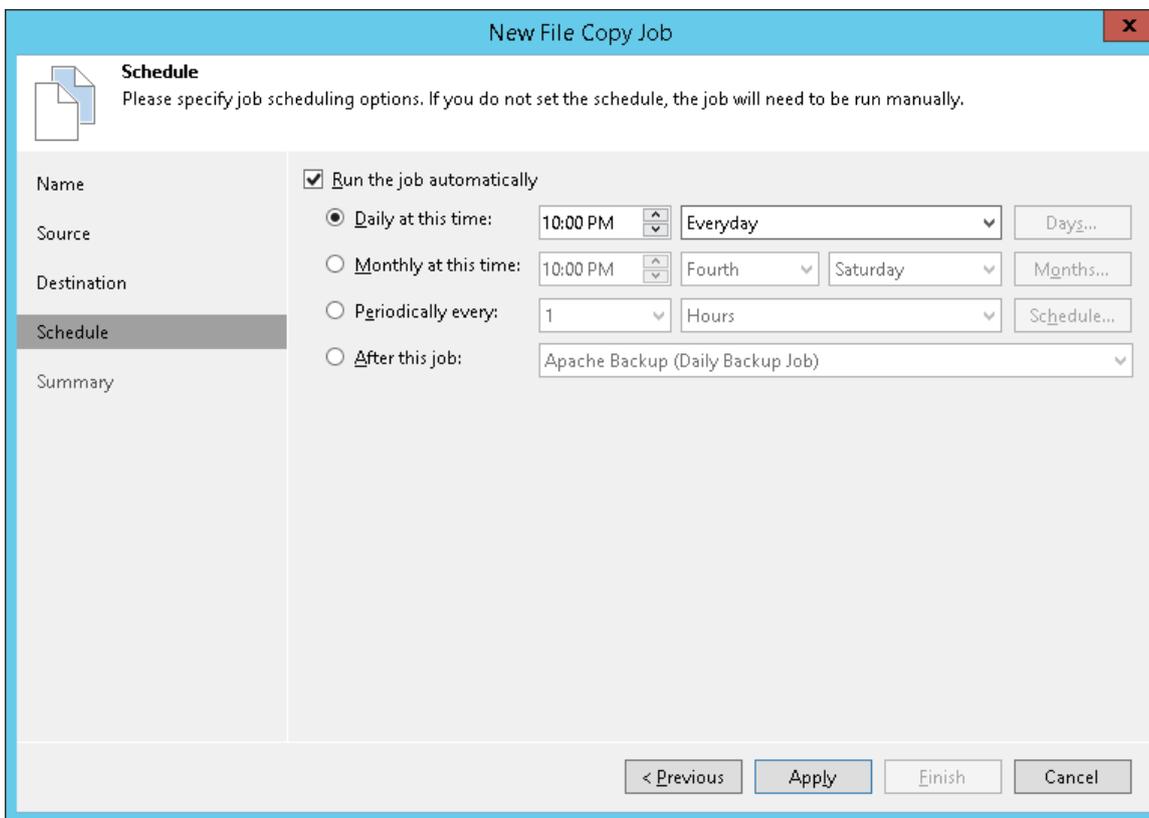
To specify the job schedule:

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.
A repeatedly run job is started by the following rules:
 - Veeam Backup & Replication 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 & Replication 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.

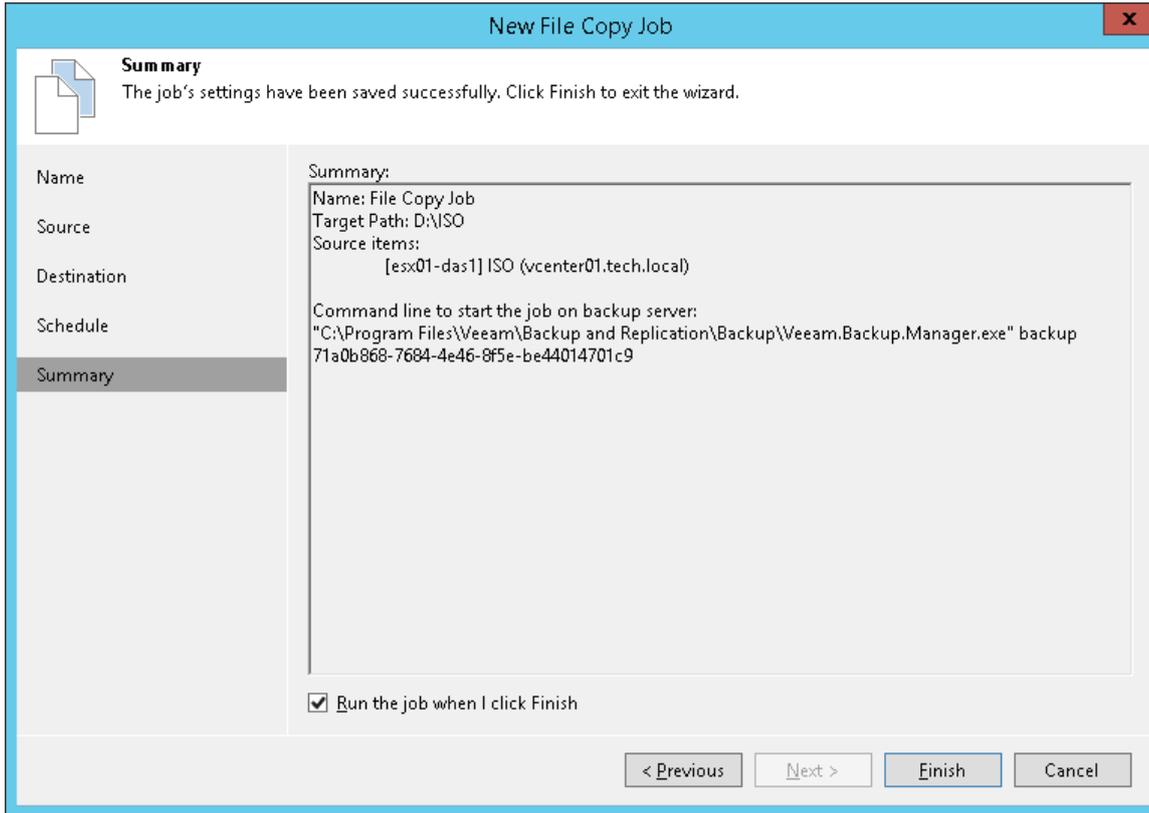


Step 6. Finish Working with Wizard

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.



Copying Files and Folders Manually

You can manually copy and move files and folders between servers and hosts added to the backup infrastructure.

Veeam Backup & Replication lets you copy files manually between the following backup infrastructure objects:

- Virtualization hosts
- Microsoft Windows servers
- Linux servers
- Deduplicating storage appliances used as backup repositories

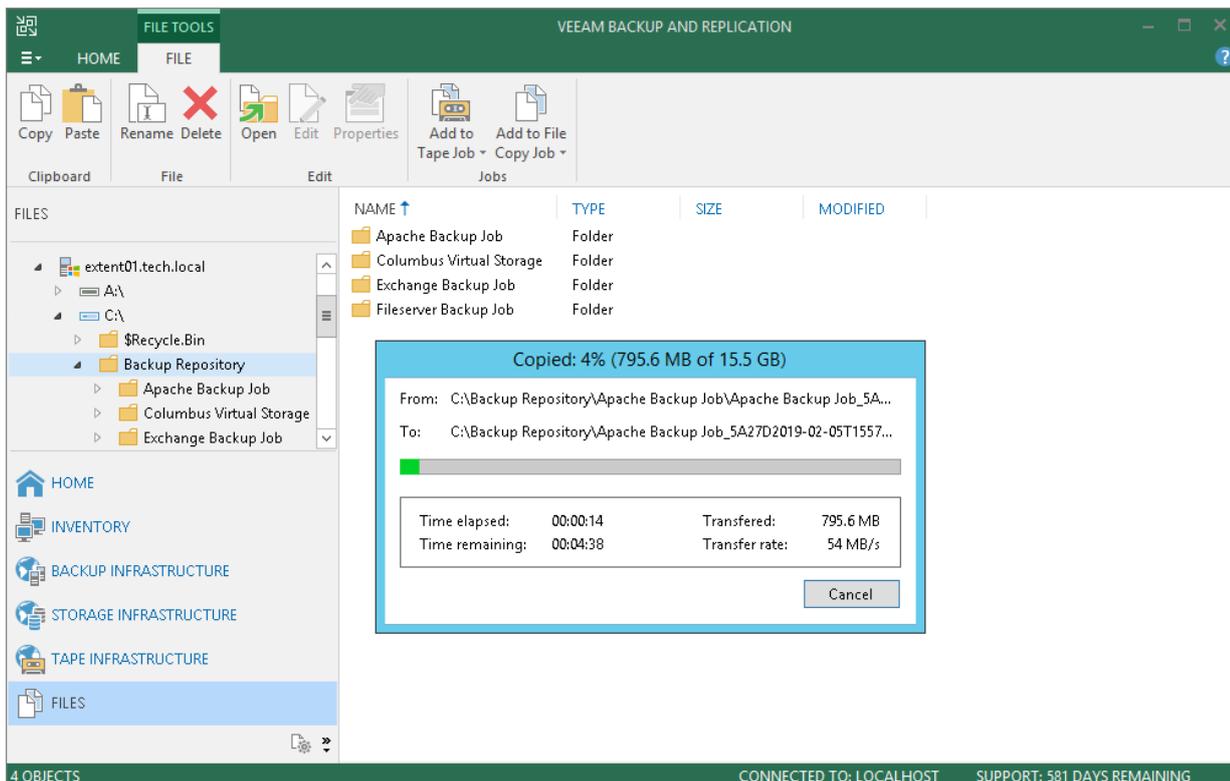
IMPORTANT!

You cannot copy backup files (VBK, VIB and VRB) to HPE StoreOnce storage appliances used as backup repositories. To copy such files, use backup copy jobs.

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.



Managing Folders

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

To create a folder:

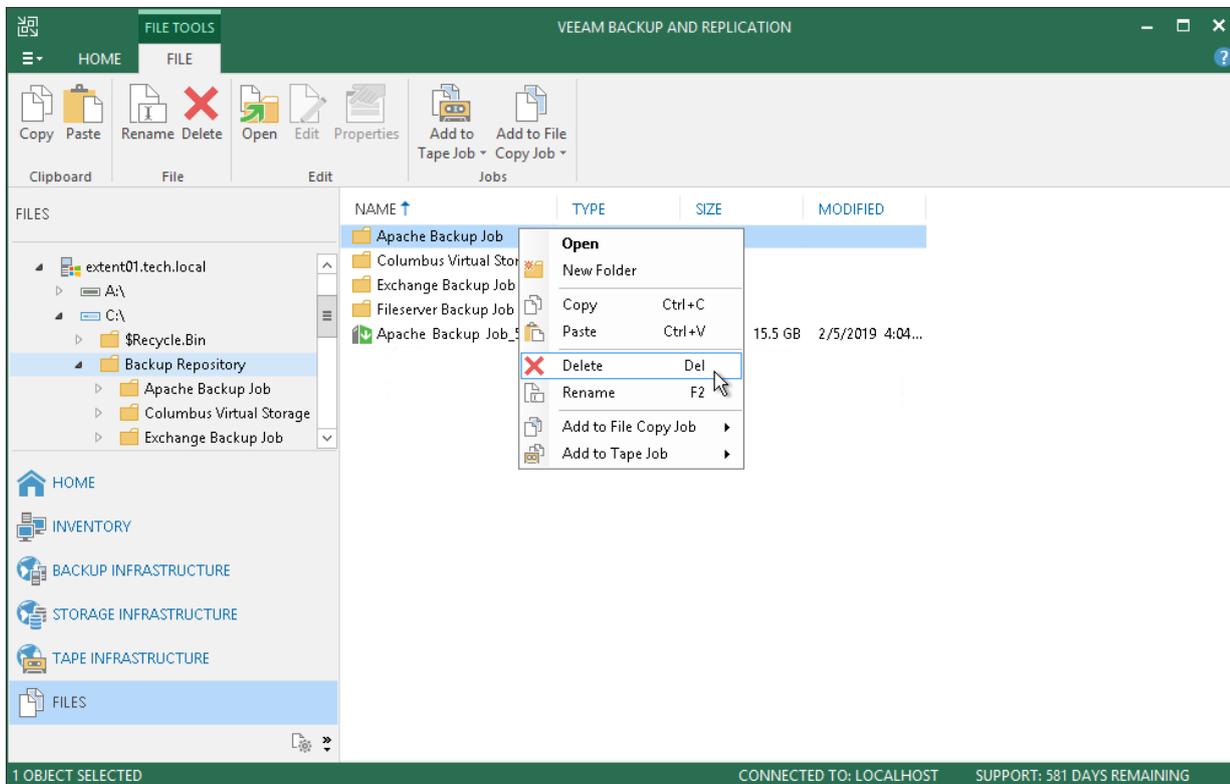
1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the necessary server or host.
3. In the working area, right-click anywhere on the blank area and select **New Folder**.

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 & Replication. 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:

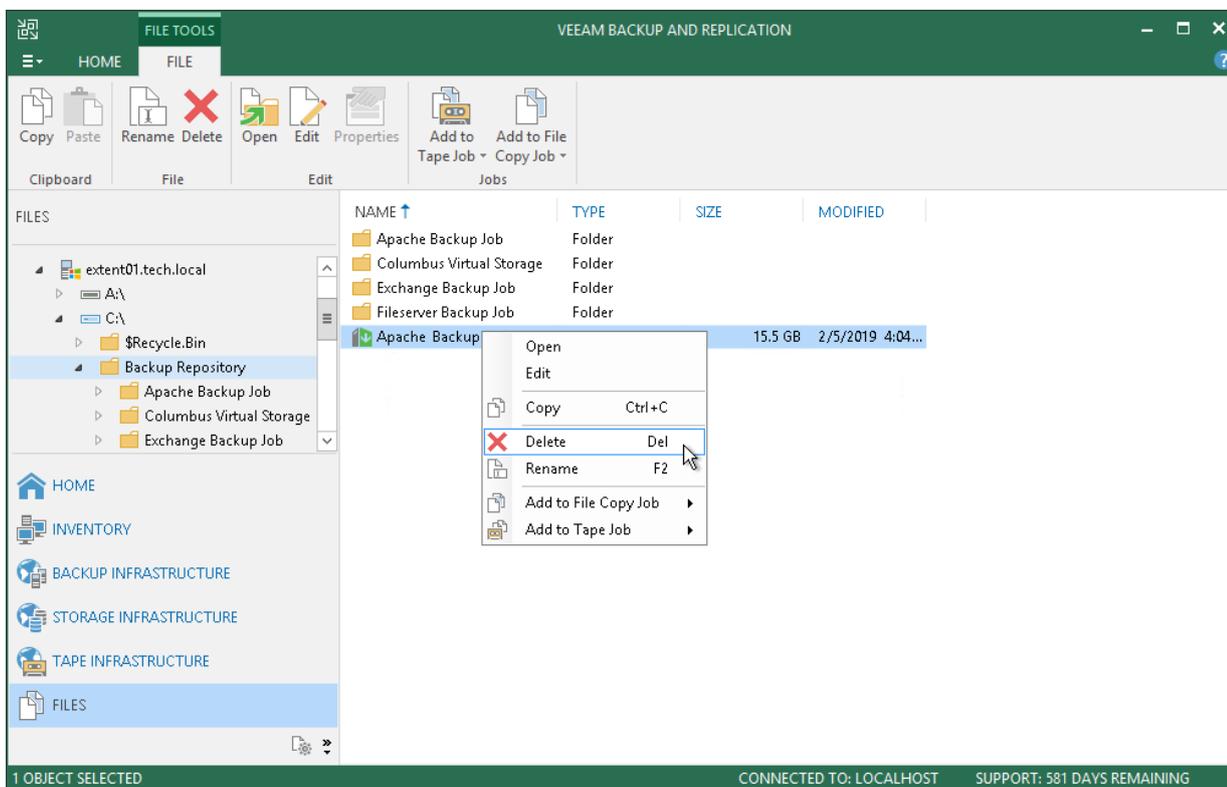
1. Open the **Files** view.
2. In the inventory pane, expand the file tree of the necessary server or host.
3. In the working area, select the file and click **Edit** on the ribbon or right-click the folder and select **Edit**.
4. Veeam Backup & Replication will open the selected file in the editor. 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.



Quick Migration

Veeam Quick Migration enables you to promptly migrate one or more VMs between ESX(i) hosts and datastores. Veeam Backup & Replication allows migration of VMs in any state with minimum disruption to business operations and end user access to services. You can use Quick Migration as a self-contained capability, solely for VM migration, or combine it with Instant VM Recovery.

Veeam Backup & Replication analyzes your virtual environment, its configuration, the state of VMs and selects the most appropriate relocation method. Whenever possible, Veeam Backup & Replication coordinates its operations with vCenter Server and uses native VMware vCenter migration mechanisms: vMotion and Storage vMotion. When VMware vCenter migration methods cannot be used (for example, if 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 & Replication uses 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). Both methods provide for no data loss during migration.

Migration of a VM is performed in several stages:

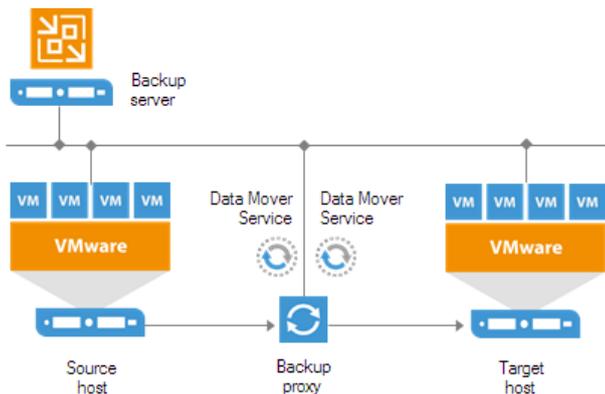
1. Veeam Backup & Replication copies VM configuration (.vmx) to the target host and registers the VM.
2. Veeam Backup & Replication triggers a VM snapshot and copies VM disk content to the new destination.
3. VM state and changes made after snapshot creation are moved to the new location. Veeam Backup & Replication 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 & Replication uses SmartSwitch. Veeam Backup & Replication suspends the VM to move its state file and changes made after snapshot creation. The VM is then resumed on the new host. This method ensures minimum possible VM downtime during migration.
 - If you move a VM between two hosts with non-compatible CPUs, Veeam Backup & Replication stops the VM, moves changes made after snapshot creation, and then starts the VM on the new host.

Quick Migration Architecture

Quick Migration architecture in a VMware vSphere environment comprises the following components:

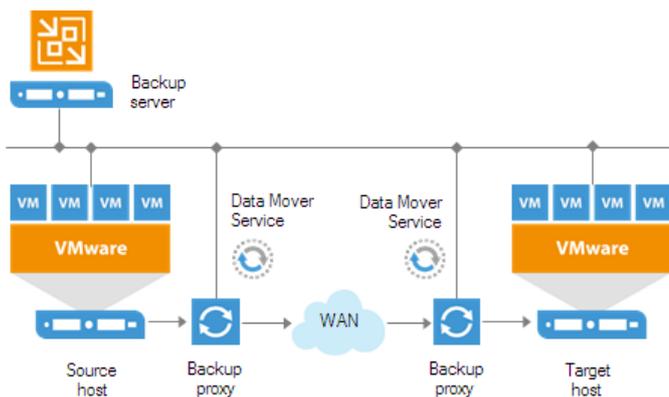
- Source host and target host with associated datastores
- One or two backup proxy servers

Similar to backup, Quick Migration uses two-service architecture: the source-side Veeam Data Mover interacts with the source host, and the target-side Veeam Data Mover interacts with the target host. To perform onsite migration, you can deploy one backup proxy for data processing and transfer. This backup proxy must have access to the source host and to the target host at the same time. In this scenario, the source-side Data Mover Service and the target-side Data Mover Service are started on the same backup proxy.



The common requirement for offsite migration is that one Data Mover Service runs in the production site (closer to the source host and datastore), and the other Data Mover Service runs in the remote target site (closer to the target host and datastore). During backup, the Data Mover Services maintain a stable connection, which allows for uninterrupted operation over WAN or slow links.

For offsite migration, you need to deploy at least one local backup proxy in each site: a source backup proxy in the production site, and a target backup proxy in the remote target site.



Migrating VMs

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 & Replication 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 and limitations.

- 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 VMs. To receive alerts about low space on the target datastore, configure global notification settings. For more information, see [Specifying Other Notification Settings](#).
- If you want to 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.
- If you use tags to categorize virtual infrastructure objects, check limitations for VM tags. For more information, see [VM Tags](#).

Encryption

Veeam Backup & Replication does not keep encryption settings if a VM is migrated with VMware vMotion. After the migration process is finished, you will need to enable encryption for the migrated VM manually.

Integration with Instant VM Recovery

When you restore a VM using Instant VM Recovery, Veeam Backup & Replication starts the VM directly from a compressed and deduplicated backup file. To finalize recovery of a VM, you still need to move it to a new location. Moving the VM with VMware Storage vMotion or hot replication may require a lot of time and resources, or it may cause loss of valuable data.

Veeam Quick Migration was designed to complement Instant VM Recovery. Instead of pulling data from vPower NFS datastore, Quick Migration registers the VM on the target host, restores the VM contents from the backup file located on the backup repository and synchronizes the VM restored from backup with the running VM.

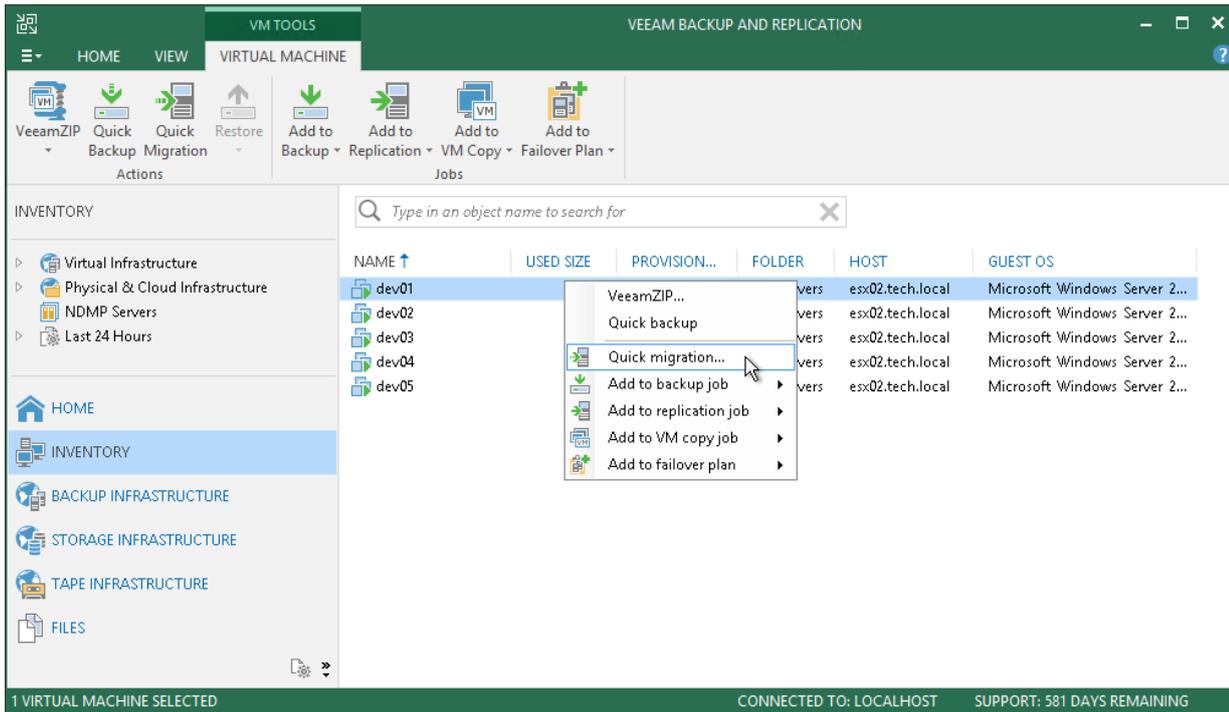
For more information, see [Instant VM Recovery](#).

Step 1. Launch Quick Migration Wizard

To run the **Quick Migration** wizard:

1. Open the **Inventory** view
2. In the infrastructure tree, select a host or VM container in which the VMs that you want to relocate reside.

3. In the working area, select the VM and click **Quick Migration** on the ribbon or right-click the VMs and select **Quick Migration**.



Step 2. Select VMs to Relocate

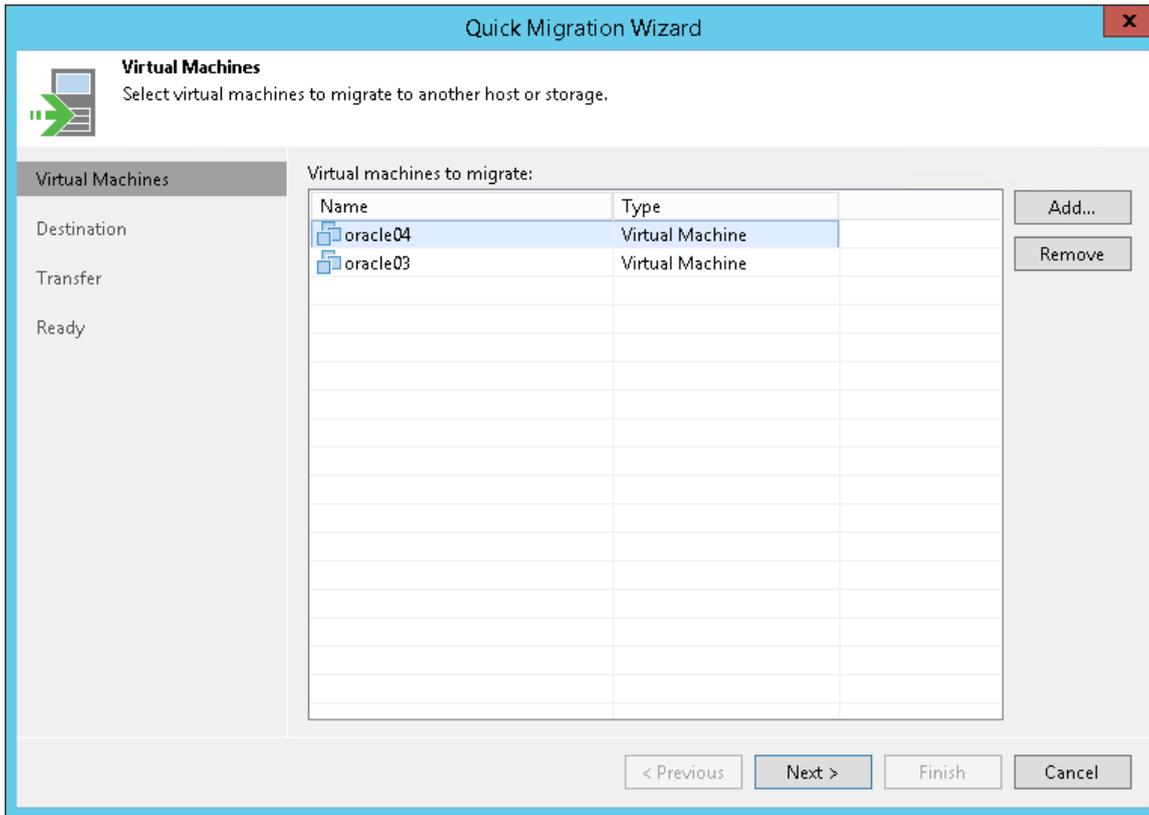
At the **Virtual Machines** step of the wizard, select the VMs and VM containers that you want to relocate.

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 VMs 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 & Replication displays only those datastores that are accessible by the selected ESX(i) host. If you have chosen relocate VMs to a cluster, Veeam Backup & Replication 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 & Replication 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.

Quick Migration Wizard

Destination
Choose destination host, resource pool, VM folder and datastore.

Virtual Machines
Destination
Transfer
Ready

Host or cluster:
esx02.tech.local Choose...

Resource pool:
Resources Choose...
[Pick resource pool](#) for selected VMs

VM folder:
vm Choose...
[Pick VM folder](#) for selected VMs

Datastore:
esx02-ds1 [1.4 TB free] Choose...
[Pick datastore](#) for selected virtual disks

< Previous Next > Finish Cancel

Step 4. Select Infrastructure Components for Data Transfer

At the **Transfer** step of the wizard, assign infrastructure components to relocate the VMs.

1. In the **Data transfer** section, select backup proxies that must be used to transfer VM data from source to target.

If you plan to migrate VMs within one site, the same backup proxy can act as the source backup proxy and target backup proxy. For offsite migration, you must deploy at least one backup proxy in each site to establish a stable connection across the sites for data transfer.

Click **Choose** next to the **Source proxy** and **Target proxy** fields to select backup proxies for migration. In the **Backup Proxy** window, you can choose automatic proxy selection or assign proxies explicitly.

- If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that have access to the source datastore and will automatically assign optimal proxy resources for processing VM data.

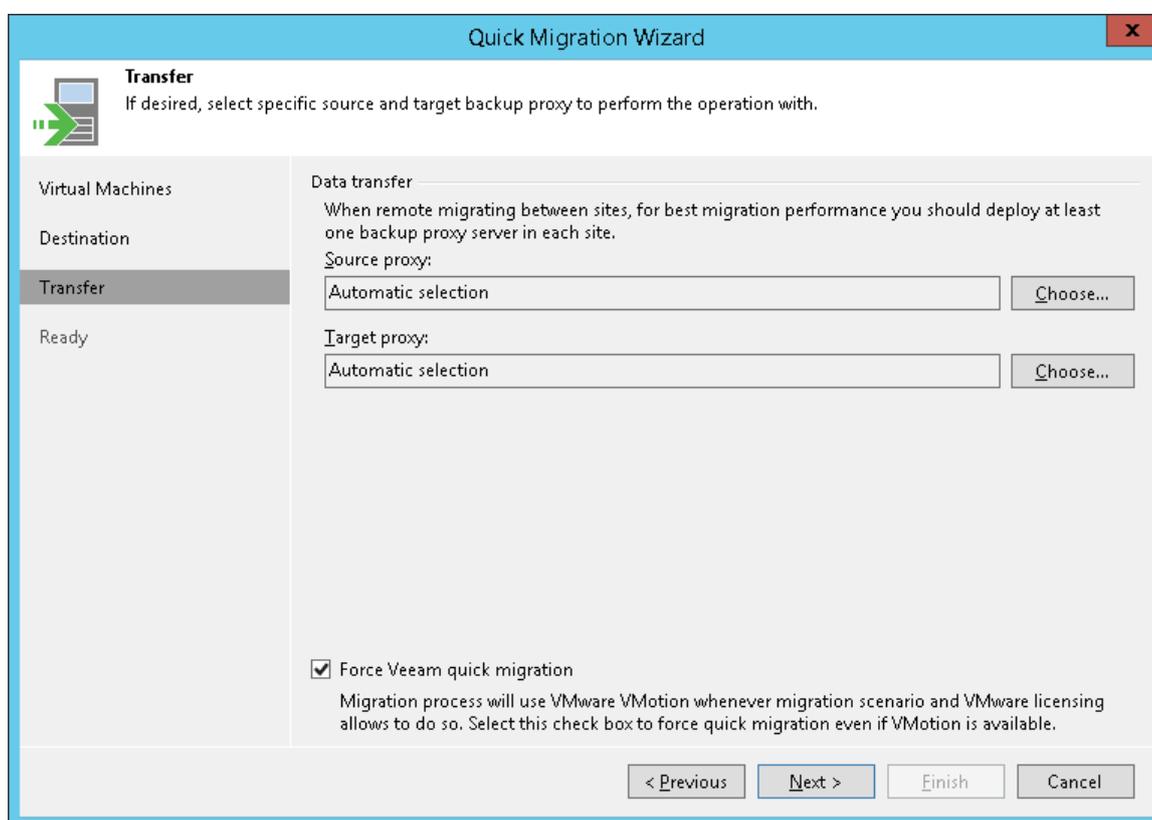
Migrated VMs are processed one by one. Before processing a new VM in the VM list, Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use for data retrieval and the current workload on the backup proxies to select the most appropriate resource for VM processing.

- If you choose **Use the selected backup proxy servers only**, you can explicitly select backup proxies that must be used to perform migration.

2. Select which migration mechanism to use: VMware vMotion or Veeam Quick Migration. Veeam Backup & Replication can use VMware vMotion only if your VMware license covers this functionality.
 - If you want to use VMware vMotion to relocate the VMs, leave the **Force Veeam quick migration** check box not selected. Veeam Backup & Replication will attempt to use the VMware vMotion mechanism to migrate the selected VMs. If VMware vMotion cannot be used for some reason (for example, if using it can cause data loss or if you do not have a VMware vSphere license for this functionality), Veeam Backup & Replication will fail over to its native migration mechanism.
 - If you do not want to use VMware vMotion, select the **Force Veeam quick migration** check box. Veeam Backup & Replication will use its native migration mechanism.

IMPORTANT!

If you use a native Veeam mechanism to relocate a VM, Veeam Backup & Replication suspends the initial VM on the source ESX(i) host (SmartSwitch) or powers off the initial VM (cold switch) for a short period of time during quick migration. For more information, see [Quick Migration](#).



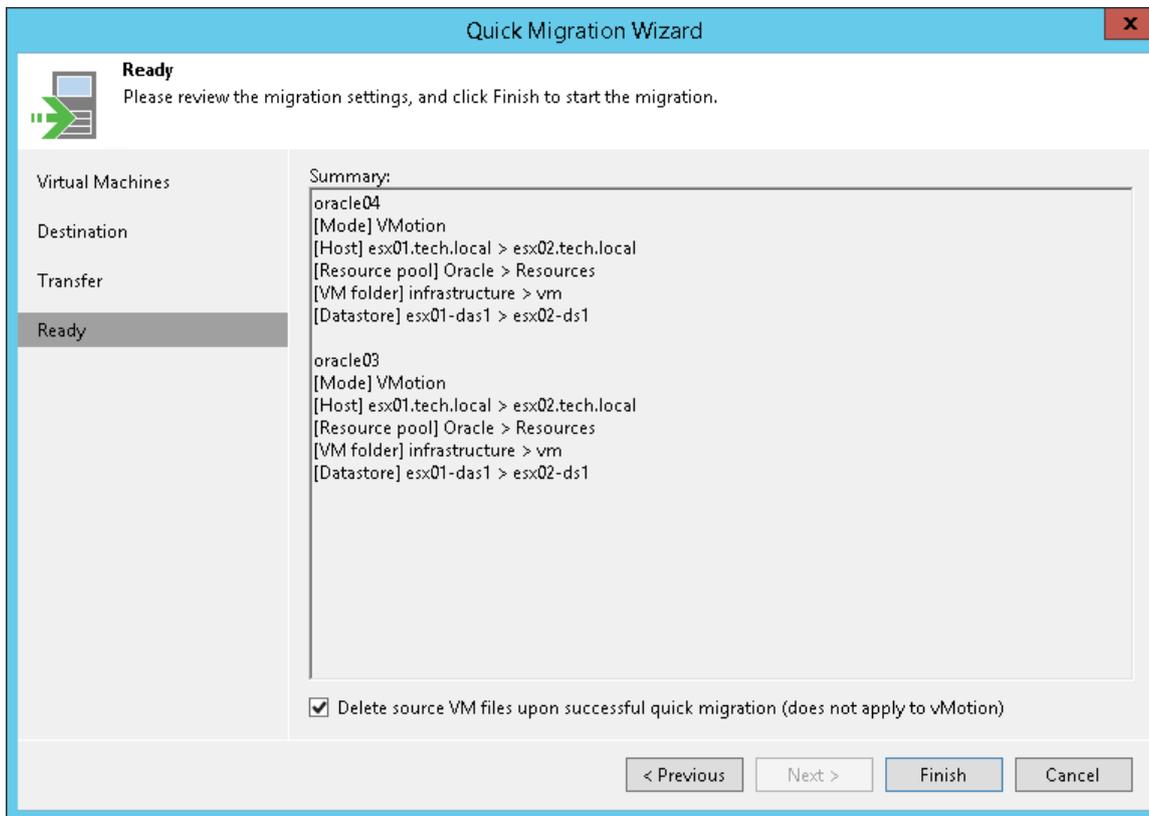
Step 5. Finish Working with Wizard

At the **Ready** step of the wizard, Veeam Backup & Replication will check if the selected VMs can be relocated.

1. Review details of the quick migration task.
2. By default, when VM migration completes successfully, Veeam Backup & Replication 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. Note that you cannot use this option if you have selected to relocate the VMs using VMware vMotion.
 - If you disable the **Delete source VM files upon successful migration** option, the source VM will not be deleted. All jobs to which the VM is added will continue to process the source VM.

- If you enable the **Delete source VM files upon successful migration** option, the source VM will be deleted. All jobs to which the VM is added will switch to the migrated VM. The backup chain will be continued, thus, the next job session for the VM will be incremental.

3. Click **Finish** to close the wizard and start the migration process.



Recovery Verification

Veeam Backup & Replication offers two technologies to verify recoverability of VM backups and replicas:

- [SureBackup](#)
- [SureReplica](#)

SureBackup

SureBackup is the Veeam technology that lets you test VM backups and check if you can recover data from them. You can verify any restore point of a backed-up VM.

During a SureBackup job, Veeam Backup & Replication performs "live" verification: scans the backed-up data for malware, boots the VM from the backup in the isolated environment, runs tests for the VM, powers the VM off and creates a report on recovery verification results.

IMPORTANT!

The recovery verification functionality is available in the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication. If you use the Standard Edition, you can manually verify VM backups with Instant VM Recovery. For more information, see [Manual Recovery Verification](#).

How SureBackup Works

For SureBackup, Veeam Backup & Replication uses a regular image-based backup. During recovery verification, Veeam Backup & Replication performs the following actions:

1. If the SureBackup job is configured to perform malware scan, Veeam Backup & Replication scans data of VMs from the application group and the verified VM with antivirus software.
2. Veeam Backup & Replication publishes VMs from the application group and the verified VM in the isolated environment – virtual lab. VMs are started directly from compressed and deduplicated backup files that reside on the backup repository. To achieve this, Veeam Backup & Replication utilizes the [Veeam vPower NFS Service](#).
3. If the SureBackup job is configured to perform malware scan, Veeam Backup & Replication scans VM data with antivirus software.
4. Veeam Backup & Replication performs a number of tests against VMs in the application group and verified VM: heartbeat test, ping test and application test.
5. If the SureBackup job is configured to validate backup files, Veeam Backup & Replication performs a CRC check for the backup file from which the verified VM is started and, optionally, for backup files from which VMs in the application group are started. The backup file validation is performed after all verification tests are complete.
6. When the recovery verification process is over, Veeam Backup & Replication unpublishes VMs and creates a report on their state. The report is sent to the backup administrator by email.

During verification, a backed up VM image remains in read-only state. All changes that take place when the VM is running are written to redo log files that are stored on the datastore selected in the virtual lab settings. When the recovery process is complete, the redo logs are removed.

To perform recovery verification, you need to create the following objects:

1. [Application group](#). During recovery verification, the verified VM may need to be started with a group of VMs on which it is dependent. The application group enables full functionality of applications running inside the VM and lets you run these applications just like in the production environment.
2. [Virtual lab](#). The virtual lab is the isolated virtual environment in which the verified VM and VMs from the application group are started and tested.
3. [SureBackup job](#). The SureBackup job is a task to perform recovery verification. You can run the SureBackup job manually or schedule it to run automatically by schedule.

Backup Recovery Verification Tests

To verify VMs with a SureBackup job, you can instruct Veeam Backup & Replication to run predefined tests for VMs or use custom verification scripts.

- [Predefined tests](#)
- [Microsoft SQL Server Checker script](#)
- [Backup file validation](#)

Predefined Tests

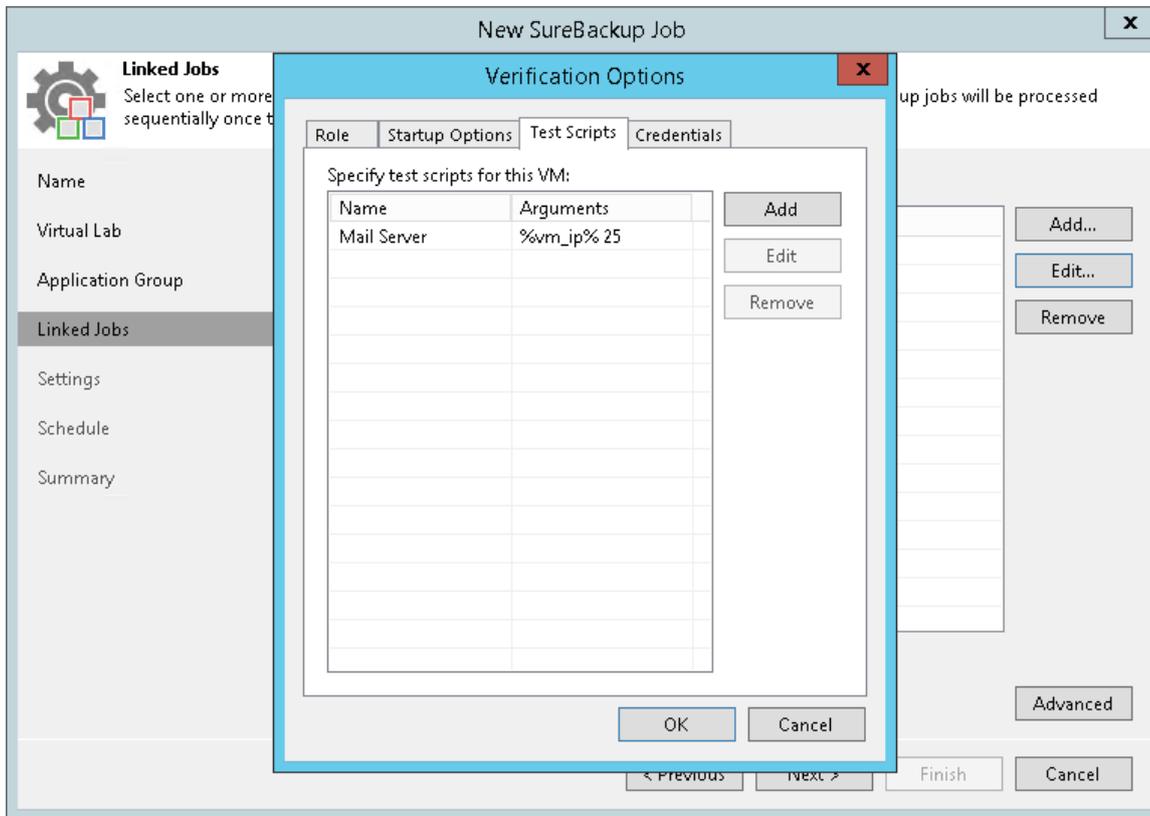
Veeam Backup & Replication can verify VMs with the following predefined tests:

- **Heartbeat test.** When the VM starts, Veeam Backup & Replication performs a heartbeat test. It waits for a heartbeat signal from VMware Tools installed inside the VM to determine that the VM guest OS is running. If the signal comes regularly at specific time intervals, the test is passed.
- **Ping test.** Veeam Backup & Replication sends ping requests to the VM from the backup server and checks if the VM can respond to them. If the VM responds to ping requests, the test is passed.
- **Application test.** Veeam Backup & Replication waits for applications inside the VM to start and runs a script against these applications. Veeam Backup & Replication uses two types of predefined scripts:
 - For DNS servers, domain controllers, Global Catalog servers, mail servers and web servers, Veeam Backup & Replication uses a script that probes an application-specific port. For example, to verify a domain controller, Veeam Backup & Replication probes port 389 for a response. If the response is received, the test is passed.
 - For Microsoft SQL Server, Veeam Backup & Replication uses a script that attempts to connect to instances and databases on the Microsoft SQL Server. For more information, see Microsoft SQL Server Checker Script.

NOTE:

To run the heartbeat and ping tests, you must have VMware Tools installed inside the VM. If VMware Tools are not installed, these tests will be skipped.

You can run verification tests for VMs added to the application group or processed with a linked SureBackup job. Settings for verification tests can be specified and customized in the application group or SureBackup job settings.



Microsoft SQL Server Checker Script

If you need to verify a virtualized Microsoft SQL Server, you can instruct Veeam Backup & Replication to run the Microsoft SQL Server Checker script against it during the SureBackup job. The script sequentially performs the following operations:

1. Connects to Microsoft SQL Server instances.
2. Enumerates databases on these instances.
3. Employs the USE SQL statement to connect to databases and check their availability.

The script is located on the backup server in the Veeam Backup & Replication product folder, by default, `C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.SqlChecker.vbs`.

The script runs on the backup server side, not from inside of a Microsoft SQL Server VM. For this reason, Named Pipes or TCP/IP connections must be enabled for the Microsoft SQL Server running in the virtual lab. For more information, see [https://msdn.microsoft.com/en-us/library/dd983822\(v=nav.71\).aspx](https://msdn.microsoft.com/en-us/library/dd983822(v=nav.71).aspx).

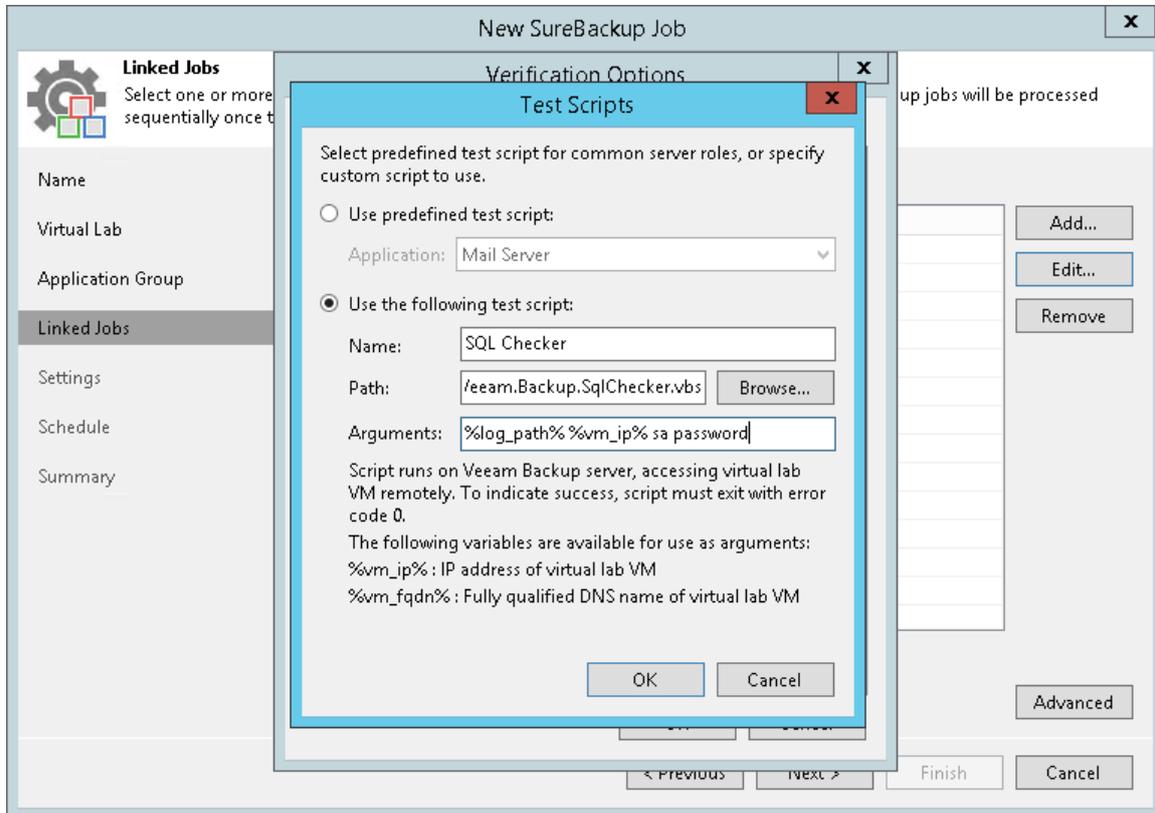
Credentials for Script Execution

To execute the script, Veeam Backup & Replication connects to Microsoft SQL Server. By default, Veeam Backup & Replication uses the account under which the Veeam Backup Service is running. If you need to run the script under another account, you can specify credentials for this account. The script supports Microsoft Windows and SQL Server authentication methods.

- For the Microsoft Windows authentication mode, you can specify credentials for the account on the **Credentials** tab in the application group or SureBackup job settings.

- For the SQL Server authentication mode, you must pass credentials of the account as arguments to the script. You can do it via the UI or command line interface.

To pass credentials via the UI, in the application group or SureBackup job settings, select to use a custom script, specify a path to the Microsoft SQL Server Checker script (by default, `C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.SqlChecker.vbs`) and specify the user name and password in the **Arguments** field.



To pass credentials via the command line, run the script from the command line in with the following parameters:

```
cscript Veeam.Backup.SqlChecker.vbs [logs folder] <sql server[\instance]>
<username> <password>
```

IMPORTANT!

Even if you use the Microsoft SQL Server authentication mode, in some cases, you may need to specify credentials of the account to connect to the machine on which Microsoft SQL Server is installed. To do this, use the **Credentials** tab in the application group or SureBackup job settings.

Database Exclusion

By default, Veeam Backup & Replication verifies all databases on all instances of Microsoft SQL Server. However, you can exclude specific databases from verification – for example, vCenter Server database. To exclude an instance or a database, you must open the script in the text editor and edit the **Settings** section in the following way:

- To exclude specific databases, uncomment the `'gDBsToExclude.Push "dbname"` line in the script and specify names of databases that you want to exclude. To exclude several databases, use a comma.
- To exclude specific instances, uncomment the `'gInstancesToExclude.Push "instancename"` line in the script and specify names of instances that you want to exclude. To exclude several instances, use a comma.

- To exclude the default instance, uncomment the 'gInstancesToExclude.Push "MSSQLSERVER" line.

IMPORTANT!

Instance and database names are case sensitive.

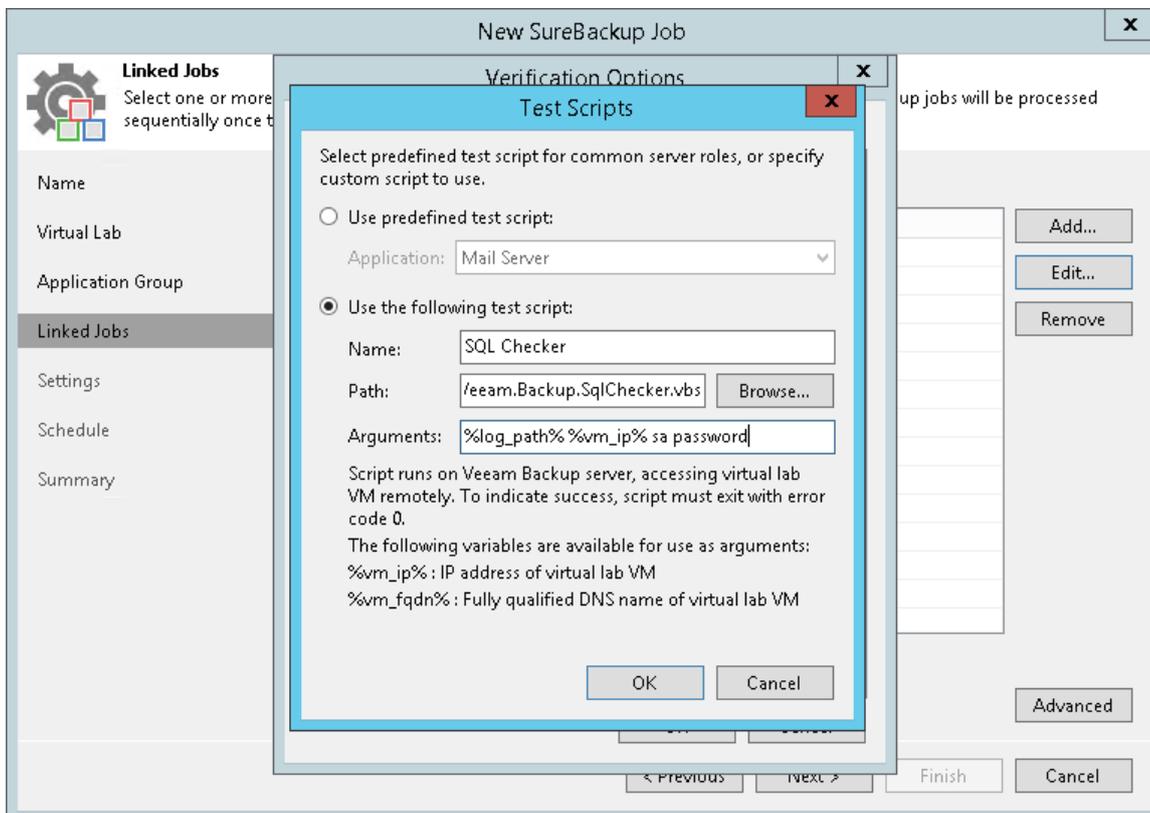
Logging

To define whether the script has completed successfully or not, Veeam Backup & Replication publishes the following return codes in the SureBackup job session statistics:

- 0 – test is passed successfully.
- 1 – you use a wrong syntax for the script command.
- 2 – Veeam Backup & Replication is unable to connect to Microsoft SQL Server.
- 3 – all instances are excluded from the check.
- 4 – error occurred while Veeam Backup & Replication was getting the list of databases.
- 5 – unknown error
- 6 – one or more databases are not accessible.

Results of script execution are written to the log file located by the following path:

`%programdata%\Veeam\Backup\<<name of the job>\<VM name>_SQLChecker.log`. If necessary, you can change the log file location. To do this, you must pass a new path to the log file in the `%log_path%` argument in the application group or SureBackup job settings.



Backup File Validation

In addition to recovery verification tests, Veeam Backup & Replication allows you to perform backup file validation. For backup file validation, Veeam Backup & Replication performs a CRC check for backup files of VMs verified by the SureBackup job. You can also validate backup files for VMs from the application group with this test.

To validate the backup file, Veeam Backup & Replication uses the checksum algorithm. When Veeam Backup & Replication creates a backup file for a VM, it calculates a checksum for every data block in the backup file and stores this data in the backup file, together with VM data. During the backup file validation test, Veeam Backup & Replication de-compresses the backup file, re-calculates checksums for data blocks in the decompressed backup file and compares them with initial checksum values. If the results match, the test is passed.

The backup file validation test is started after recovery verification tests. As soon as Veeam Backup & Replication completes all "live" verification for all VMs in the SureBackup job, it unpublishes VMs and starts the backup file validation test.

The result of the backup file validation test impacts the state of the SureBackup job session. If the validation tests are completed successfully but the backup validation is not passed, Veeam Backup & Replication marks the SureBackup job session with the *Warning* or *Error* status.

The screenshot displays the 'Exchange SureBackup Job Session 10/11/2018 8:25:48 AM' window. It features a 'VM status:' table and a 'dns01 log:' section.

Name	Status	Heartbeat	Ping	Script	Verification	Antivirus scan
dns01	Success	Success	Success	Disabled	Disabled	Disabled
dc03	Success	Success	Success	Success	Success	Disabled
exch01	Success	Success	Success	Success	Success	Disabled
apache02	Starting	Pending	Pending	Disabled	Pending	In progress

The 'dns01 log:' section shows a list of messages with durations:

- Running ping test(s) - 0:00:15
 - Network adapter 1: name VM Network, usable
 - Network adapter 1: IP address fe80::5fa:130f:b61c:7929, skipped - IPv4 supported only
 - Network adapter 1: IP address 172.17.0.1, OK
 - Results: 1/2 test(s) passed, 0 failed, 1 skipped
 - Summary: 50% total pass rate
- Application initialization - 0:02:00
 - Waiting for 120 more seconds...
 - Note: operation will be continued at 10/11/2018 8:34:59 AM
 - Summary: application is initialized

Buttons for 'Stop Session' and 'Close' are visible at the bottom.

Application Group

In most cases, a VM works not alone but in cooperation with other services and components. To verify such VM, you first need to start all services and components on which this VM is dependent. To this aim, Veeam Backup & Replication uses the application group.

The application group creates the “surroundings” for the verified VM. The application group contains one or several VMs on which the verified VM is dependent. These VMs run applications and services that must be started to enable fully functional work of the verified VM. Typically, the application group contains at least a domain controller, DNS server and DHCP server.

When you set up an application group, you specify a role of every VM, its boot priority and boot delay. Additionally, you can specify what tests must be performed to verify VMs in the application group.

When a SureBackup job is launched, Veeam Backup & Replication first starts in the virtual lab VMs from the application group in the required order and performs necessary tests against them. This way, Veeam Backup & Replication creates the necessary environment for the verified VM. Only after all VMs from the application group are started and tested, Veeam Backup & Replication starts the verified VM in the virtual lab.

For example, if you want to verify a Microsoft Exchange Server, you need to test its functionality in cooperation with the domain controller and DNS server. Subsequently, you must add to the application group a virtualized domain controller and DNS server. When Veeam Backup & Replication runs a SureBackup job, it will first start and verify the domain controller and DNS server in the virtual lab to make verification of the Microsoft Exchange Server possible.

NOTE:

All VMs added to the application group must belong to the same platform – VMware or Hyper-V. Mixed application groups are not supported.

Creating Application Groups

Before you create an application group, [check prerequisites](#). Then use the **New Application Group** wizard to create an application group.

Before You Begin

Before you create an application group, check the following prerequisites:

- A valid license for Enterprise Edition of Veeam Backup & Replication must be installed on the backup server.
- All applications and services on which verified VMs are dependent must be virtualized in your environment.
- If you plan to scan VM data for malware, [check requirements and limitations](#).
- If you plan to verify VMs with a ping test, the firewall on tested VMs must allow ping requests.
- If you plan to verify VMs with a heartbeat test, VMware Tools must be installed in tested VMs.
- [For storage snapshots] The storage system must be added to the backup infrastructure.

Mind the following limitations:

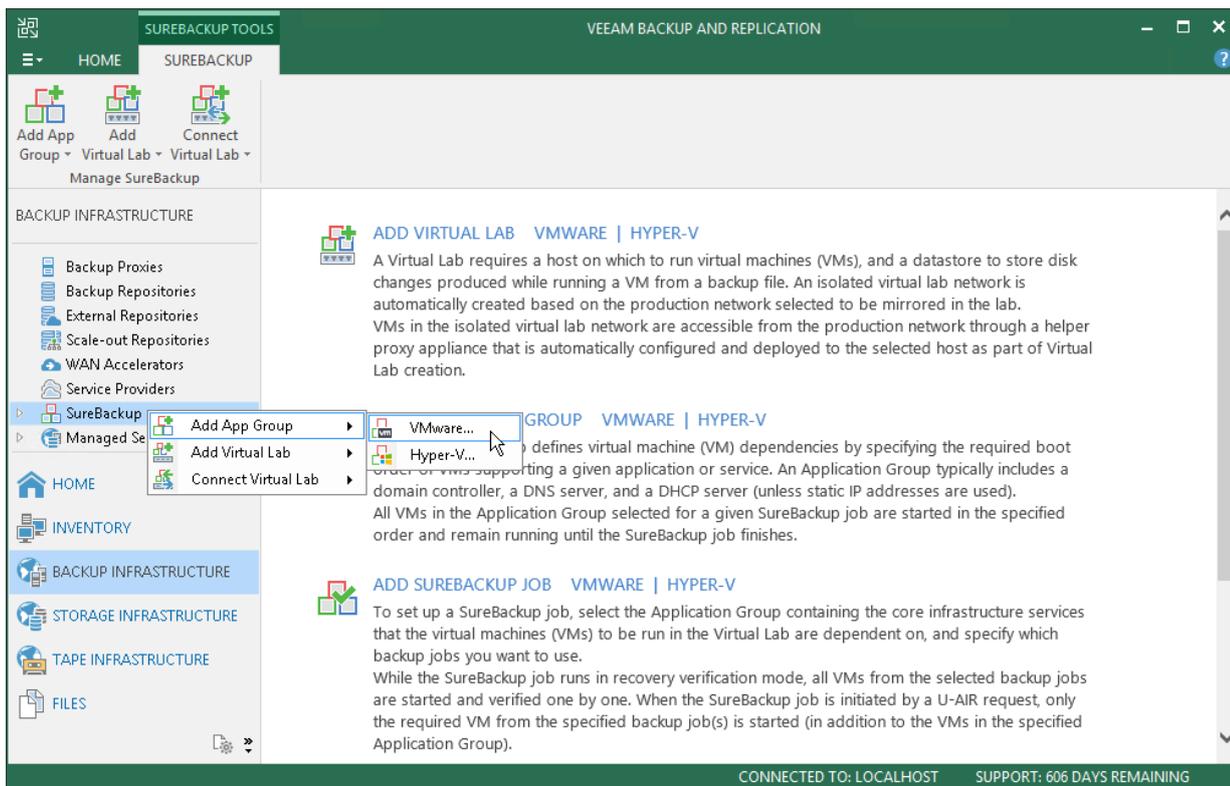
- VM replicas must be in the *Normal* state. If a VM replica is in the *Failover* or *Failback* state, you will not be able to add it to the application group.

- You cannot add to application groups VMs from backups of vCloud Director VMs, backups created with backup copy jobs and backups stored on cloud backup repositories.

Step 1. Launch New Application Group Wizard

To launch the **New Application Group** wizard, do one of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select **SureBackup**. In the working area, click **Add Application Group > VMware**.
- Open the **Backup Infrastructure** view, in the inventory pane select **Application Groups** under **SureBackup** and click **Add Group > VMware** on the ribbon.
- Open the **Backup Infrastructure** view, in the inventory pane right-click **Application Groups** under **SureBackup** and select **Add App Group > VMware**.



Step 2. Specify Application Group Name and Description

At the **Name** step of the wizard, specify a name and description for the application group.

- In the **Name** field, enter a name for the application group.

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

The screenshot shows a 'New Application Group' wizard window. The window title is 'New Application Group'. On the left, there is a sidebar with three items: 'Name' (selected), 'Virtual Machines', and 'Summary'. The main area of the wizard is divided into two sections. The top section is labeled 'Name' and contains a text box with the text 'Exchange Application Group'. Below this is a section labeled 'Description' with a text box containing the text 'VM Group for Microsoft Exchange Verification'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 3. Add VMs to Application Group

At the **Virtual Machines** step of the wizard, add VMs to the created application group. You can add VMs from different sources:

- VM backups
- VM replicas
- Storage snapshots

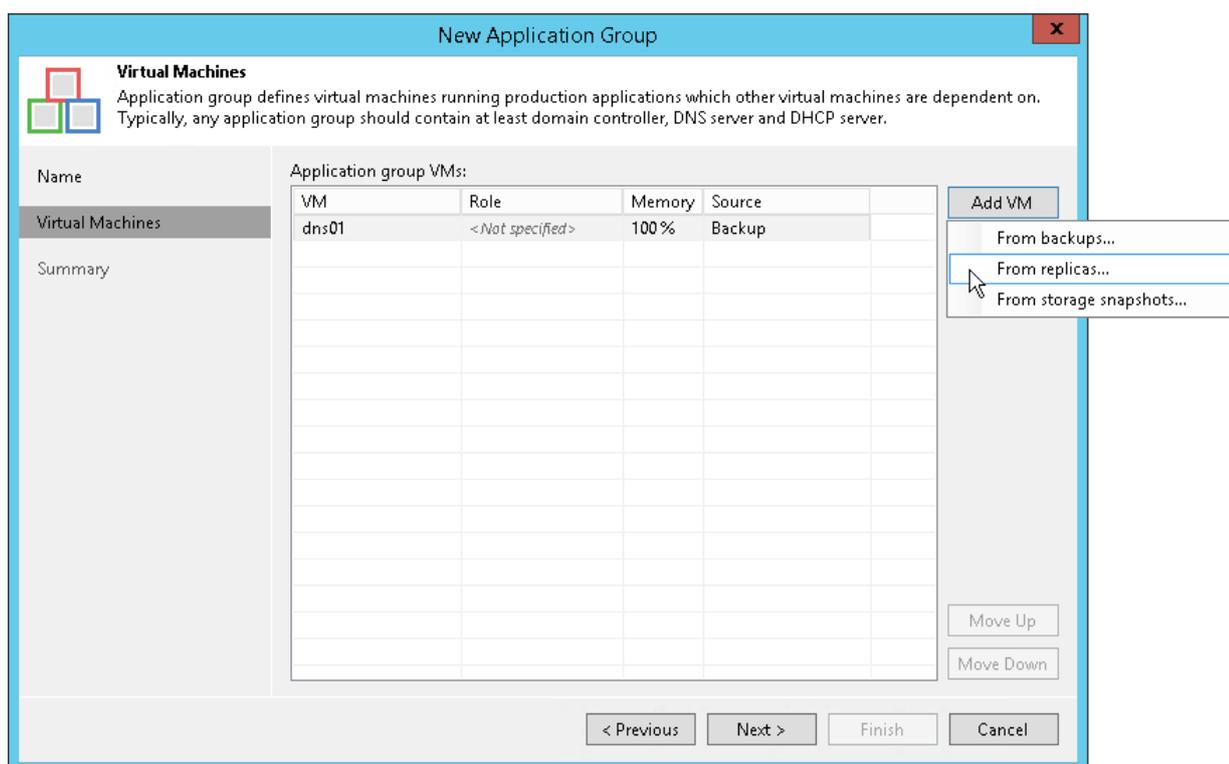
You can add VMs from backups, storage snapshots and VM replicas to the same application groups. Keep in mind the following limitations:

- VMs must belong to the same platform – VMware vSphere or Microsoft Hyper-V.
- VMs must have at least one valid restore point or must reside on a storage snapshot.
- You cannot add the same VM twice. For example, if you add a VM from the storage snapshot, you will not be able to add the same VM from the backup.

To add VMs to the application group:

1. Click **Add VM** and select **From backups**, **From replicas** or **From storage snapshots**.
2. In the displayed window, expand the job or storage snapshot, select the VM and click **Add**.

- VMs in the list are specified in the order of their boot priority. To move a VM up and down in the list, select it and click **Move Up** or **Move Down**.



Step 4. Specify Recovery Verification Options and Tests

You must specify verification options for every VM in the application group:

- [Select a role that the VM performs](#)
- [Configure startup settings](#)
- [Select tests that must be performed for the VM](#)
- [Specify credentials for running the verification script](#)

To specify recovery verification options:

1. At the **Virtual Machines** step of the wizard, select the VM in the list.
2. Click **Edit** on the right.
3. Use the **Verification Options** window to specify verification options.

Role Settings

On the **Role** tab, select a role that the VM performs. Veeam Backup & Replication offers the following predefined roles for VMs:

- DNS Server
- Domain Controller (Authoritative Restore). In the Authoritative Restore mode, Veeam Backup & Replication starts a domain controller in the virtual lab and marks it as being authoritative to its replication partners. When other domain controllers (replication partners) are started in the virtual lab, they replicate data from the domain controller started in the Authoritative Restore mode.

- Domain Controller (Non-Authoritative Restore). In the Non-Authoritative Restore mode, Veeam Backup & Replication restores a domain controller in the virtual lab and marks it as being non-authoritative to its replication partners. Non-authoritative domain controllers then replicate data from a domain controller started in the Authoritative Restore mode.
- Global Catalog
- Mail Server
- SQL Server
- Veeam Backup for Microsoft Office 365 (machine on which Veeam Backup for Microsoft Office 365 is installed)
- Web Server

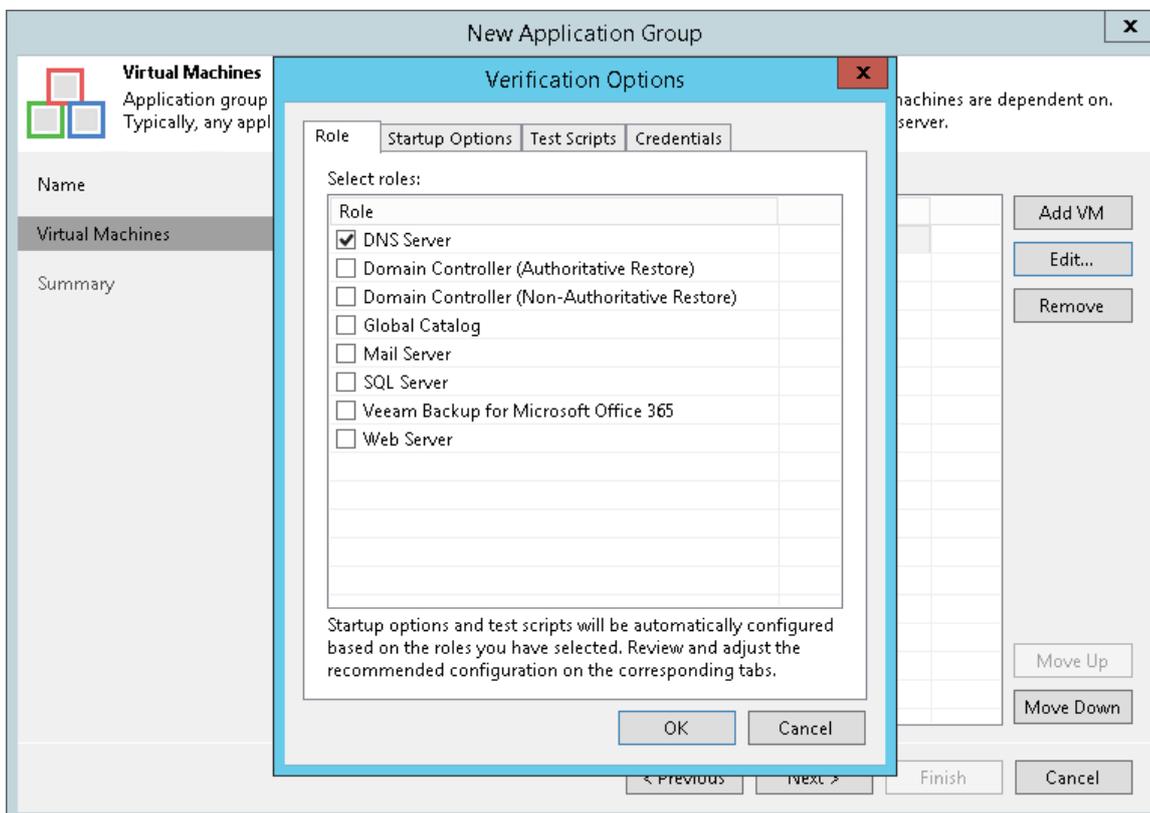
VM roles are described in XML files stored in the *%ProgramFiles%\Veeam\Backup and Replication\Backup\SbRoles* folder on the backup server. You can create your own roles. To do this, you must create a new XML file and specify role and test scripts settings in it. For more information, see [Creating XML files with VM Roles Description](#).

After you select a role for the VM, Veeam Backup & Replication will automatically configure startup options and assign predefined test scripts for the chosen role. You can use these settings or specify custom settings on the **Startup Options** and **Test Scripts** tabs.

To verify VMs that perform roles other than those specified in the list, you will have to manually configure startup options and specify test scripts that must be run for these VMs.

IMPORTANT!

If you want to add several domain controllers to the application group, you must assign the **Domain Controller (Authoritative Restore)** role to the first domain controller started in the virtual lab. Other domain controllers must have the **Domain Controller (Non-Authoritative Restore)** role.



Startup Settings

To configure VM startup settings:

1. In the **Verification Options** window, click the **Startup Options** tab.
2. In the **Memory** section, specify the amount of memory that you want to pre-allocate to the VM when this VM starts. The amount of pre-allocated memory is defined in percent. The percentage rate is calculated based on the system memory level available for the production VM. For example, if 1024 MB of RAM is allocated to the VM in the production environment and you specify 80% as a memory rate, 820 MB of RAM will be allocated to the verified VM on startup.
3. In the **Startup time** section, specify the allowed boot time for the VM and timeout to initialize applications on the VM.

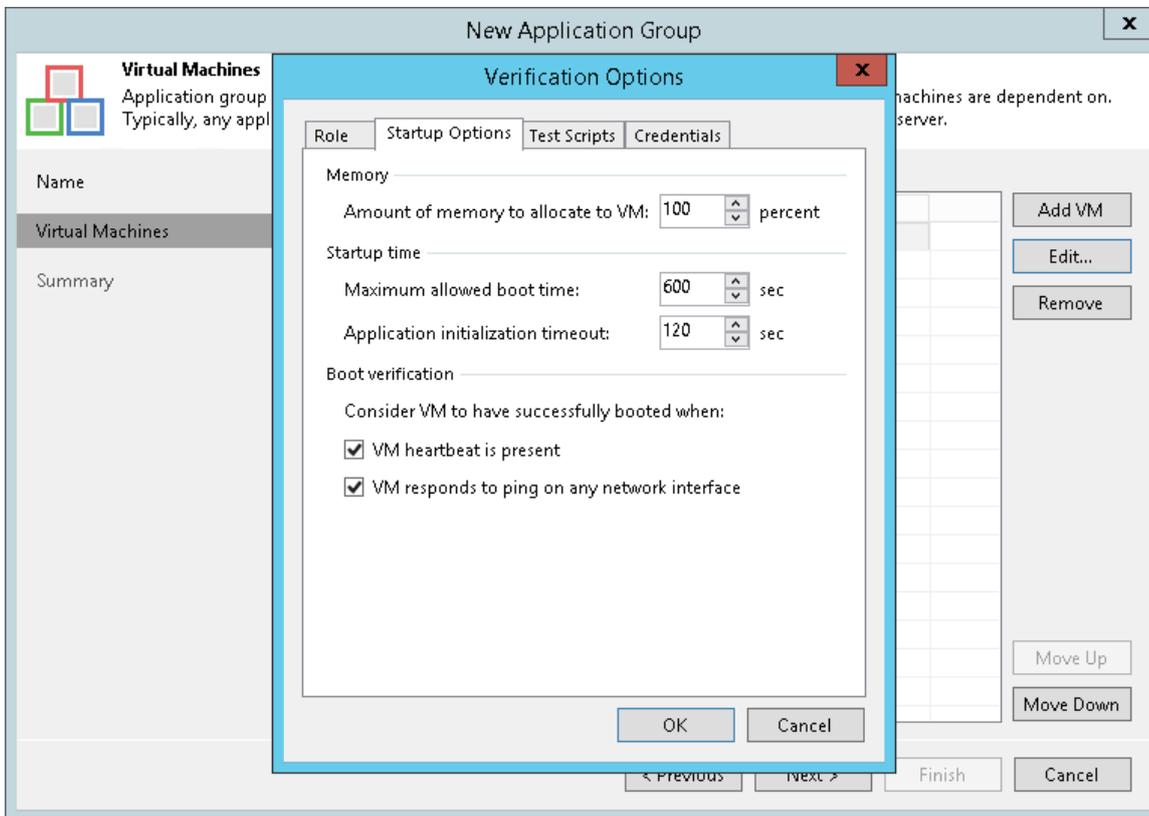
Be careful when specifying the **Maximum allowed boot time** value. Typically, a VM started by the SureBackup job requires more time to boot than a VM started in the production environment. If an application is not initialized within the specified interval of time, the recovery verification process fails with the timeout error. If such error occurs, you need to increase the **Maximum allowed boot time** value and run the SureBackup job again.

4. In the **Boot verification** section, specify when the VM must be considered to have been booted successfully:
 - **VM heartbeat is present.** If you enable this option, Veeam Backup & Replication will perform a heartbeat test for the verified VM.
 - **VM responds to ping on any network interface.** If you enable this option, Veeam Backup & Replication will perform a ping test for the verified VM.

If you enable both options, Veeam Backup & Replication will require that both tests are completed successfully: heartbeat test and ping test.

NOTE:

Veeam Backup & Replication performs a heartbeat test only if a VM has VMware Tools installed. If VMware Tools are not installed, the VM will be started but the test will not be performed. VMs without VMware Tools can still be used as auxiliary VMs: they can be started to enable proper work of other VMs. In this case, you do not need to select any role for such VMs.



Test Script Settings

When you select a VM role, Veeam Backup & Replication automatically assigns a predefined script that must be run to verify applications inside this VM. If you want to verify a VM that has some other role not listed on the **Role** tab:

1. In the **Verification Options** window, click the **Test Scripts** tab.
2. Click **Add**.
3. In the **Test Scripts** window, select **Use the following test script**.
4. In the **Name** field, specify a name for the script.
5. In the **Path** field, define a path to an executable script file that must be run to verify the VM. You can do one of the following:
 - If you have your own custom script, define a path to it in the **Path** field.
 - If you do not have a custom script, you can use a standard utility by Veeam, *Veeam.Backup.ConnectionTester.exe*, that probes application communication ports. The utility is located in the installation folder of Veeam Backup & Replication:
`%ProgramFiles%\Veeam\Backup and Replication\Backup\Veeam.Backup.ConnectionTester.exe`. Specify this path in the **Path** field.

- In the **Arguments** field, specify an IP address of the verified VM and the port that you want to probe (if the selected test probes the port). You can use the `%vm_ip%` variable to define the VM IP address or the `%vm_fqdn%` variable to define the VM fully qualified domain name.

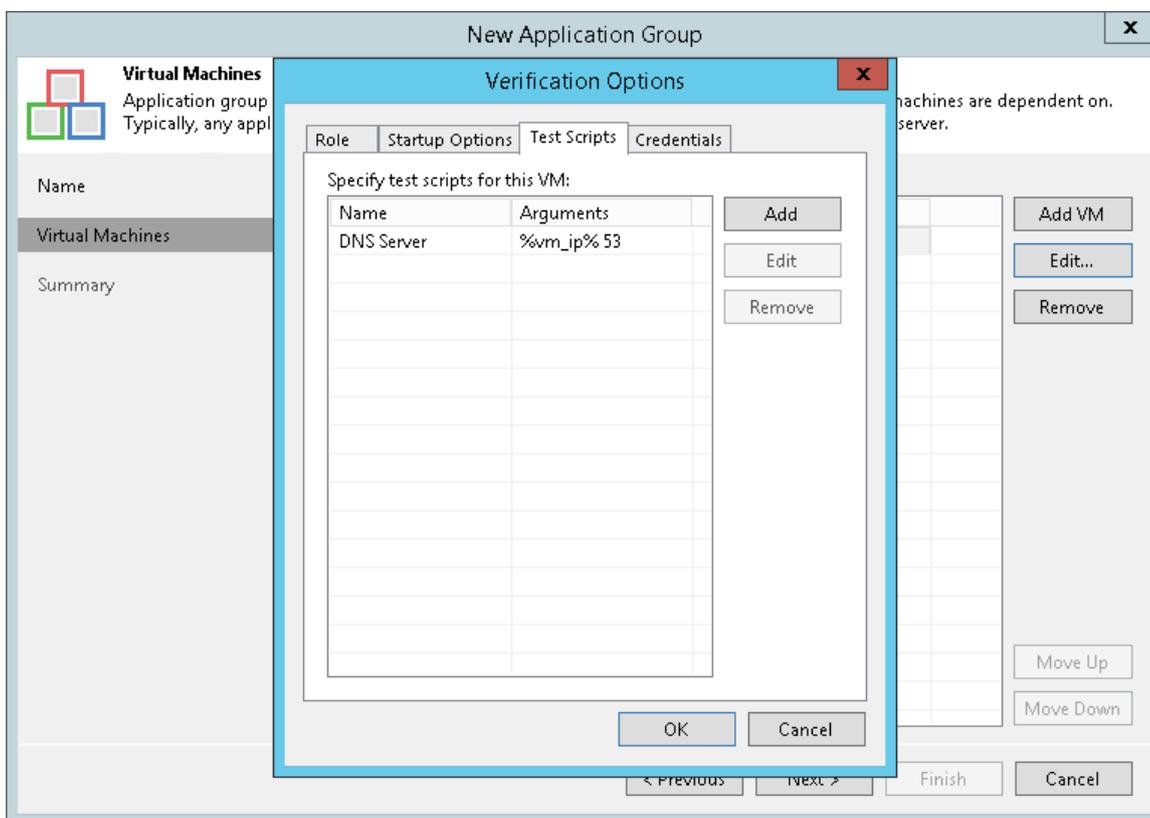
For Microsoft SQL Server, you can also specify a path to the log file in the `%log_path%` argument. For more information, see [Backup Recovery Verification Tests](#).

- Click **OK** to add the configured test.

To edit test settings, select the test in the list and click **Edit**. To delete a test, select the test in the list and click **Remove**.

NOTE:

If a VM performs several roles and runs a number of applications, you can add several verification scripts to verify work of these applications. It is recommended that you specify the maximum startup timeout value and allocate the greatest amount of memory for such VMs.

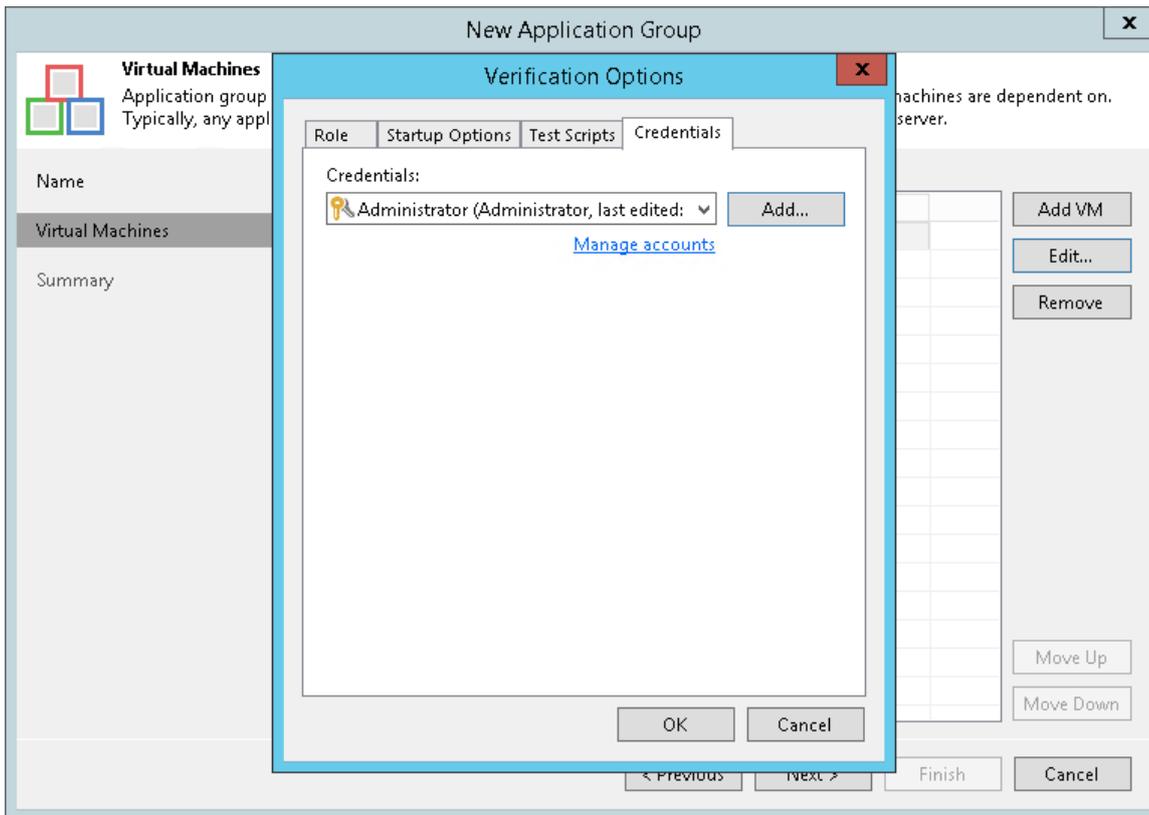


Credentials Settings

By default, to run the verification script Veeam Backup & Replication uses the account under which the Veeam Backup Service is running. If you need to run the script under some other account, you can specify credentials for this account in the application group settings.

- Click the **Credentials** tab.
- From the **Credentials** list, select credentials for the account under which you want to run the script.

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](#).

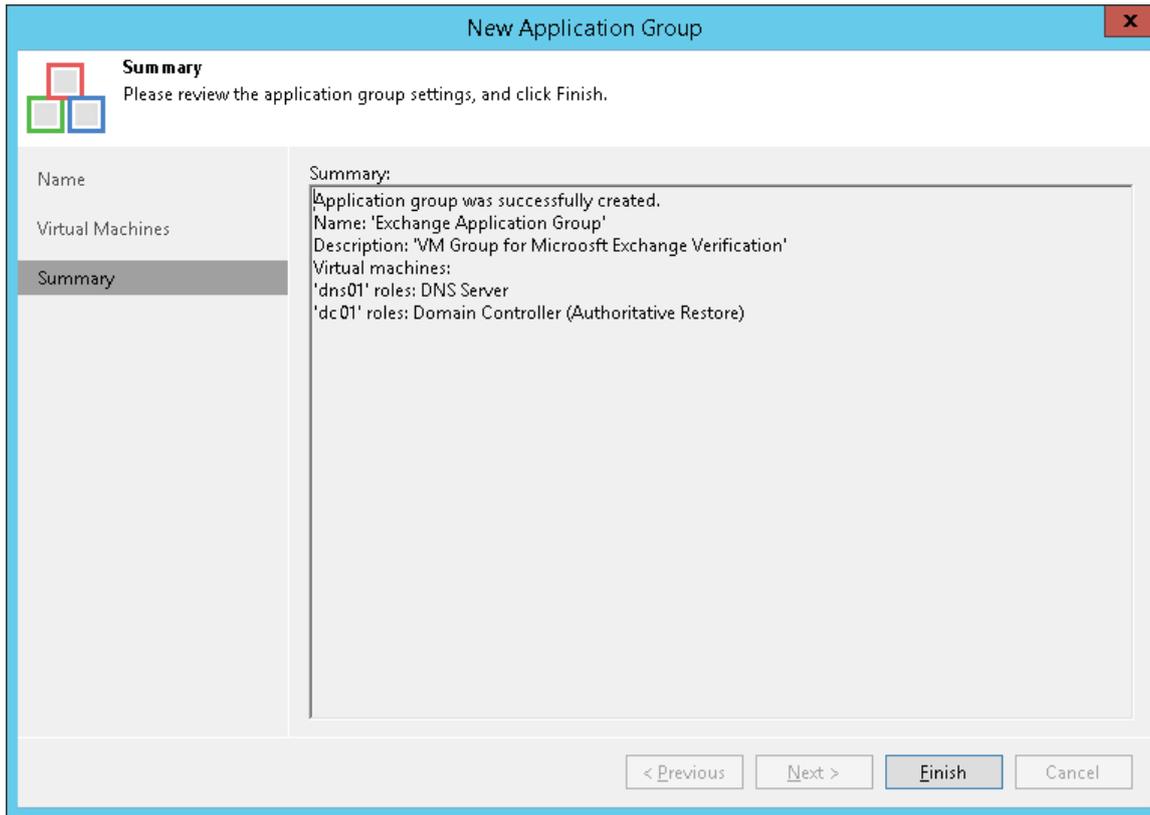


Step 5. Review Application Group Settings and Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of application group configuration.

1. Review details of the application group.

2. Click **Finish** to save the application group settings and close the wizard.



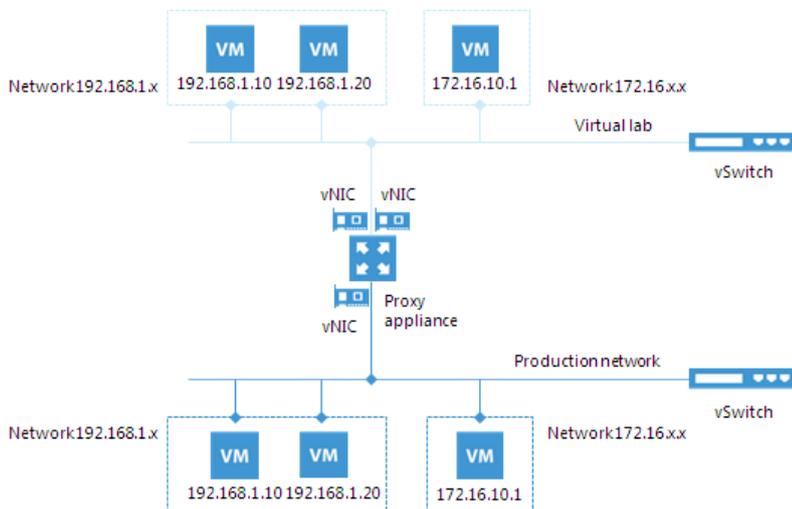
Virtual Lab

The virtual lab is an isolated virtual environment in which Veeam Backup & Replication verifies VMs. In the virtual lab, Veeam Backup & Replication starts VMs from the application group and the verified VM. The virtual lab is used not only for the SureBackup verification procedure, but also for U-AIR, On-Demand Sandbox and staged restore.

The virtual lab itself does not require that you provision extra resources for it. However, VMs running in the virtual lab consume CPU and memory resources of the ESX(i) host where the virtual lab is deployed. All VM changes that take place during recovery verification are written to redo log files. By default, Veeam Backup & Replication stores redo logs on the datastore selected in the virtual lab settings and removes redo logs after the recovery process is complete.

The virtual lab is fully fenced off from the production environment. The network configuration of the virtual lab mirrors the network configuration of the production environment. For example, if verified VMs and VMs from the application group are located in two logical networks in the production environment, the virtual lab will also have two networks. The networks in the virtual lab will be mapped to corresponding production networks.

VMs in isolated networks have the same IP addresses as in the production network. This lets VMs in the virtual lab function just as if they function in the production environment.



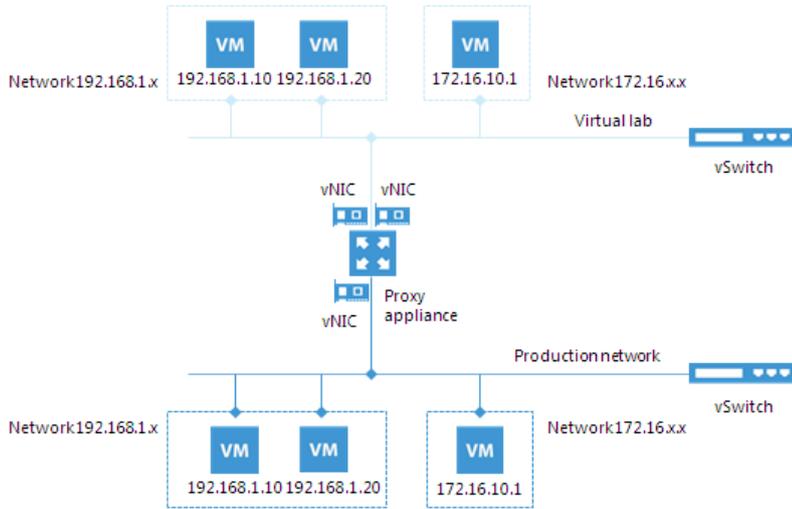
Proxy Appliance

To enable communication between the production environment and isolated networks in the virtual lab, Veeam Backup & Replication uses a proxy appliance. The proxy appliance is an auxiliary Linux-based VM that is deployed on the ESX(i) host where the virtual lab is created. The proxy appliance VM is assigned an IP address from the production network and placed to the dedicated virtual lab folder and resource pool on the ESX(i) host.

The proxy appliance is connected to the production network and to the isolated network and so has visibility of the production environment and virtual lab. In essence, the proxy appliance acts as a gateway between the two networks – it routes requests from the production environment to VMs in the virtual lab.

To connect to isolated networks, the proxy appliance uses network adapters. Veeam Backup & Replication adds to the proxy appliance one network adapter per every isolated network. For example, if there are two networks in the virtual lab, Veeam Backup & Replication will add two network adapters to the proxy appliance. The network adapter gets an IP address from the isolated network. Typically, this IP address is the same as the IP address of the default gateway in the corresponding production network.

The proxy appliance is an optional component for recovery verification. Technically, you can create a virtual lab without the proxy appliance. However, in this case, you will not be able to perform automatic recovery verification of VMs. VMs will be started from backups in the virtual lab; you will have to access them using the VM console and perform necessary tests manually.

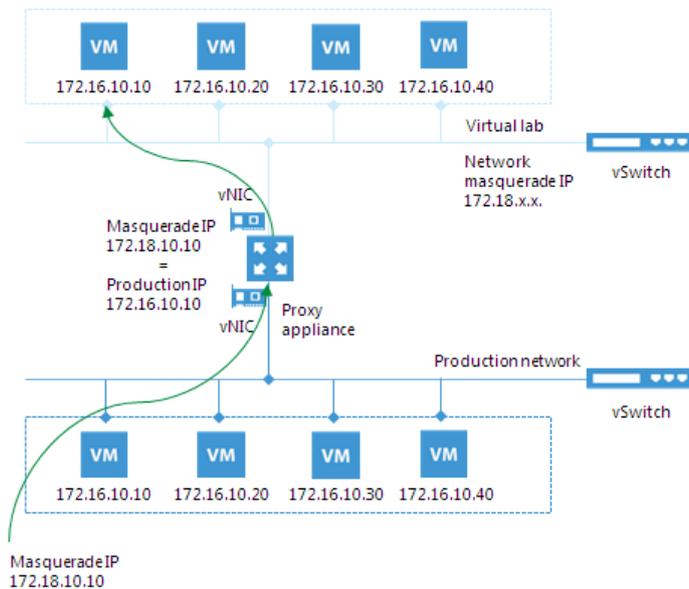


IP Masquerading

To let the traffic into the virtual lab, Veeam Backup & Replication uses masquerade IP addressing.

Every VM in the virtual lab has a masquerade IP address, along with the IP address from the production network. The masquerade IP address resembles the IP address in the production network. For example, if the IP address of a VM is 172.16.1.13, the masquerade IP address may be 172.18.1.13.

The masquerade IP address is an "entry point" to the VM in the virtual lab from the production environment. When you want to access a specific VM in the virtual lab, Veeam Backup & Replication addresses it by its masquerade IP address.



The rules that route requests to VMs in the virtual lab are specified in the routing table on the server from which you want to access VMs in the virtual lab. The routing table can be updated on the following servers:

- **Backup server.** Veeam Backup & Replication automatically creates the necessary static routes in the routing table on the backup server at the moment you launch a SureBackup job and Veeam Backup & Replication starts the virtual lab.
- **Client machine.** If you want to provide your users with access to VMs in the virtual lab, you need to manually update routing tables on their machines and add new static routes. For more information, see [Static IP Mapping](#).

The added static route destines the masquerade network traffic to the proxy appliance. The proxy appliance acts as a NAT device: it resolves the masquerade IP address, replaces it with "real" IP address of the VM from the production network and then directs the request to the necessary VM in the virtual lab. The static route is non-persistent: when you power off the virtual lab, the route is removed from the routing table on the backup server or client machine.

For example, when trying to access a VM with IP address 172.16.10.10 in the isolated network, Veeam Backup & Replication sends a request to the masquerade IP address 172.18.10.10. According to the routing rule added to the IP routing table, all requests are first sent to the next hop – the proxy appliance. The proxy appliance performs address translation, substitutes the masquerade IP address with the IP address in the isolated network, and forwards the request to the necessary VM in the isolated network – in this example, to 172.16.10.10.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>route print

=====
Interface List
12...00 50 56 89 1b 9a .....Intel(R) PRO/1000 MT Network Connection
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

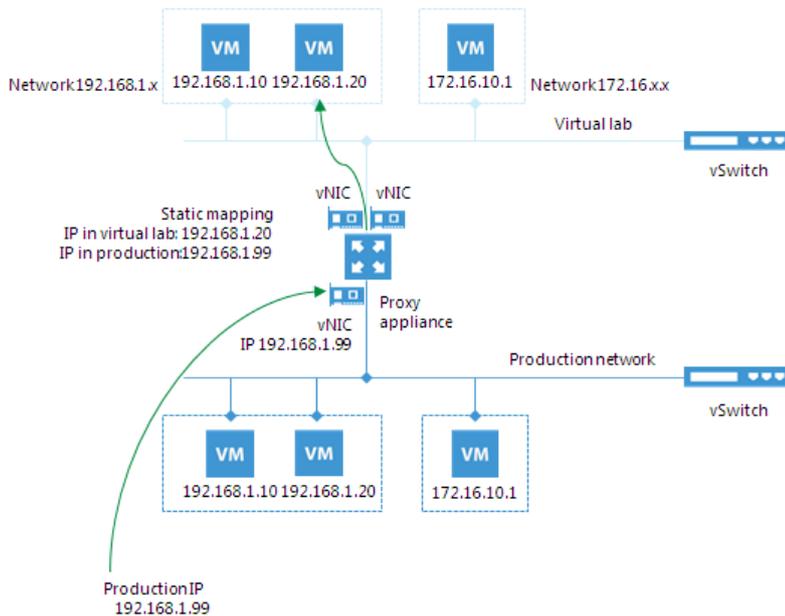
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          172.16.0.1       172.16.11.38     10
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255 On-link          127.0.0.1        306
127.255.255.255           255.255.255.255 On-link          127.0.0.1        306
172.16.0.0                 255.252.0.0      172.16.0.1       172.16.11.38     11
172.16.0.0                 255.255.0.0      On-link          172.16.11.38     266
172.16.11.38              255.255.255.255 On-link          172.16.11.38     266
172.16.255.255            255.255.255.255 On-link          172.16.11.38     266
172.17.0.0                 255.255.0.0      172.16.0.1       172.16.11.38     11
172.18.0.0                 255.255.0.0      172.16.11.142    172.16.11.38     11
192.168.169.0             255.255.255.0    172.16.0.1       172.16.11.38     11
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          172.16.11.38     266
255.255.255.255           255.255.255.255 On-link          127.0.0.1        306
255.255.255.255           255.255.255.255 On-link          172.16.11.38     266
=====
  
```

Static IP Mapping

Sometimes it is necessary to provide many clients with access to a restored VM, which is especially the case for user-directed application item-level recovery. For example, you may want to provide users with access to the Microsoft Exchange Server started in the virtual lab via web-based access (like Outlook Web Access). Technically, you may update the routing table on every client machine; however, this will demand a lot of administrative effort.

For such situations, Veeam Backup & Replication lets you get access to a VM in the virtual lab directly from the production environment. To access to a VM in the virtual lab, you must reserve a static IP address in the pool of production IP addresses and map this IP address to the IP address of a VM in the virtual lab.

The static IP address is assigned to the proxy appliance network adapter connected to the production network. IP traffic directed to the specified static IP address is routed by the proxy appliance to the VM in the isolated network.



For example, for a VM with IP address 192.168.1.20 in the isolated network, you can reserve IP address 192.168.1.99 (a free IP address from the production network). As a result, you will be able to use IP address 192.168.1.99 to access the VM in the virtual lab from the production side.

You can also register an alias record in the production DNS server for the reserved IP address. For example, you can register backup.exchange.local as an alias for the IP address 192.168.1.99, and users will be able to access Microsoft Exchange Server by this alias.

Virtual Lab Configuration

For SureBackup recovery verification, Veeam Backup & Replication offers two types of the virtual lab configuration:

- [Basic single-host virtual lab](#)
- [Advanced single-host virtual lab](#)

NOTE:

You can also verify VM backups in Advanced Multi-Host virtual labs with DVS. This scenario can be helpful if you want to test VM backups and VM replicas in the same virtual lab or want to add verified VM backups and replicas to the same SureBackup job.

For more information, see [Advanced Multi-Host Virtual Labs](#).

Basic Single-Host Virtual Labs

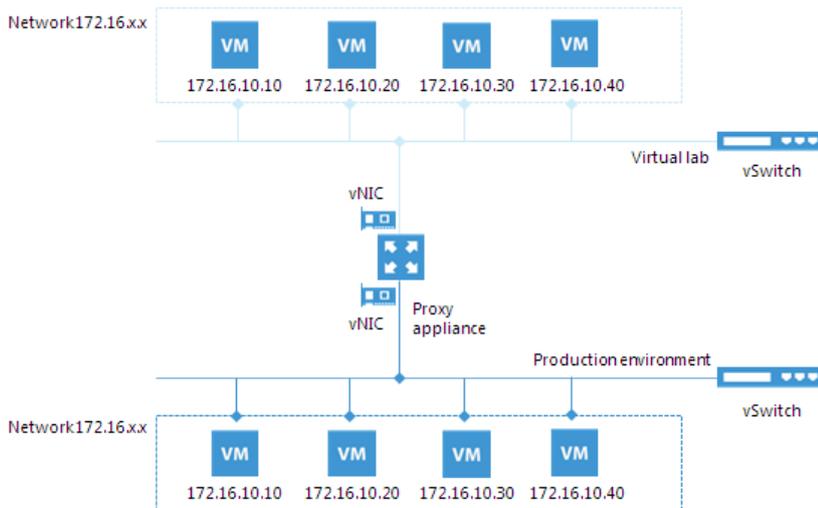
The basic single-host virtual lab can be used if all VMs that you want to verify, VMs from the application group and the backup server are connected to the same network.

For the basic single-host virtual lab, Veeam Backup & Replication creates one virtual network that is mapped to the corresponding production network. Veeam Backup & Replication automatically adds a number of new objects on the ESX(i) host where the virtual lab is created:

- A resource pool
- A VM folder
- A standard vSwitch

The vSwitch is only used by the VMs started in the virtual lab. There is no routing outside the virtual lab to other networks.

Veeam Backup & Replication automatically configures all settings for the basic single-host virtual lab. The proxy appliance is also created and configured automatically on the ESX(i) host where the virtual lab is created.



Advanced Single-Host Virtual Labs

The advanced single-host virtual lab can be used if VMs that you want to verify and/or VMs from the application group are connected to different networks.

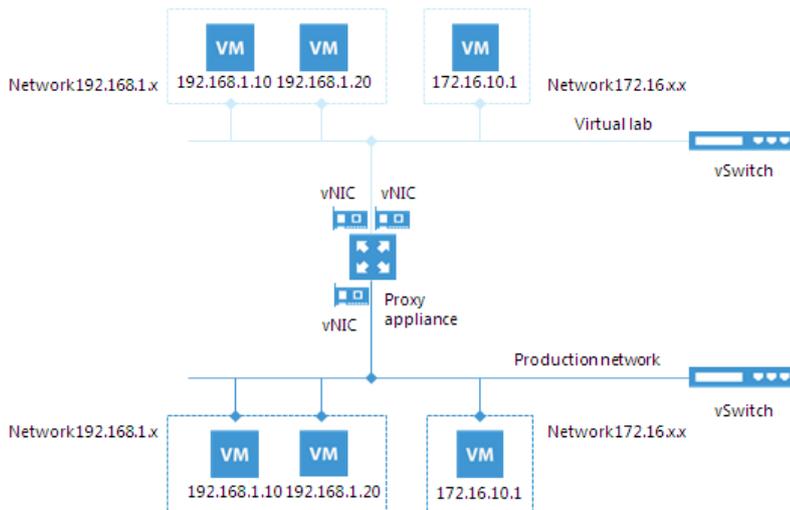
In the advanced single-host virtual lab, Veeam Backup & Replication creates several virtual networks for the virtual lab. The number of virtual networks corresponds to the number of production networks to which verified VMs are connected. Networks in the virtual lab are mapped to production networks.

Veeam Backup & Replication automatically adds a number of new VMware objects on the ESX(i) host where the virtual lab is created:

- A resource pool
- A VM folder
- A standard vSwitch

The vSwitch is only used by the VMs started in the virtual lab. There is no routing outside the virtual lab to other networks.

When you create an advanced single-host virtual lab, Veeam Backup & Replication configures basic settings for networks that are created in the virtual lab. You need to review these settings and manually adjust them.



Creating Virtual Lab

Before you create a new virtual lab, [check prerequisites](#). Then use the **New Virtual Lab** wizard to create a virtual lab.

Before You Begin

Before you create a virtual lab, check the following prerequisites:

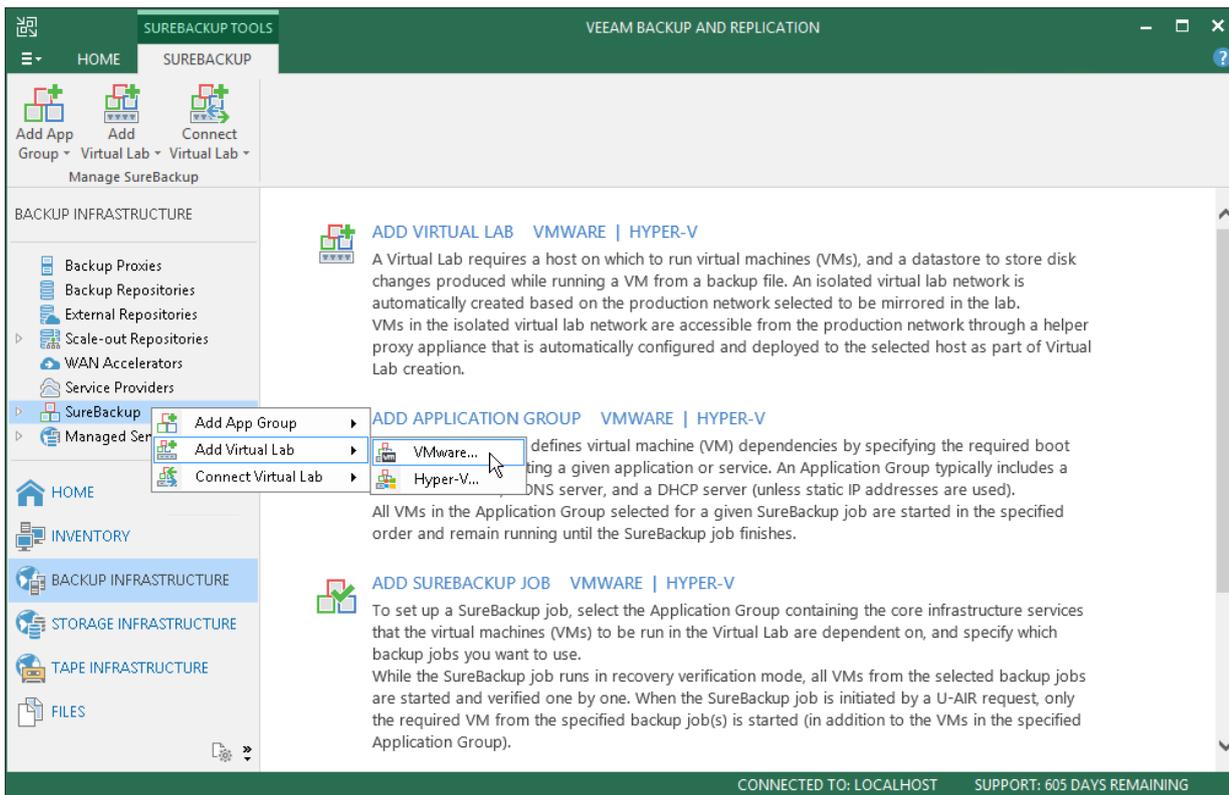
- A valid license for Enterprise Edition of Veeam Backup & Replication must be installed on the backup server.
- The ESX(i) host on which you plan to deploy a virtual lab must have a VMkernel interface. Otherwise the vPower NFS datastore will not be mounted on the ESX(i) host. For more information, see [Veeam vPower NFS Service](#).
- If you plan to use the advanced multi-host networking mode for VM replicas verification, you must configure a DVS beforehand. For more information, see [Advanced Multi-Host Virtual Labs](#).

Step 1. Launch New Virtual Lab Wizard

To launch the **New Virtual Lab** wizard, do one of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select **SureBackup**. In the working area, click **Add Virtual Lab > VMware**.
- Open the **Backup Infrastructure** view, in the inventory pane select **Virtual Labs** node under **SureBackup** and click **Add Virtual Lab > VMware** on the ribbon.

- Open the **Backup Infrastructure** view, in the inventory pane right-click **Virtual Labs** under **SureBackup** and select **Add Virtual Lab > VMware**.



Step 2. Specify Virtual Lab Name and Description

At the **Name** step of the wizard, specify a name and description for the virtual lab.

1. In the **Name** field, enter a name for the virtual lab.

2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the virtual lab, date and time when the lab was created.

The screenshot shows a 'New Virtual Lab' wizard window. The window title is 'New Virtual Lab'. On the left, there is a sidebar with a list of steps: Name, Host, Datastore, Proxy, Networking, Ready to Apply, and Applying Configuration. The 'Name' step is currently selected and highlighted. The main area of the wizard is divided into two sections. The top section is labeled 'Name' and contains a text input field with the text 'Sandbox01'. Below this is a section labeled 'Description' with a larger text area containing the text 'Virtual Lab'. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The 'Next >' button is highlighted, indicating the next step in the wizard.

Step 3. Select Host

At the **Host** step of the wizard, select an ESX(i) host on which the virtual lab must be created.

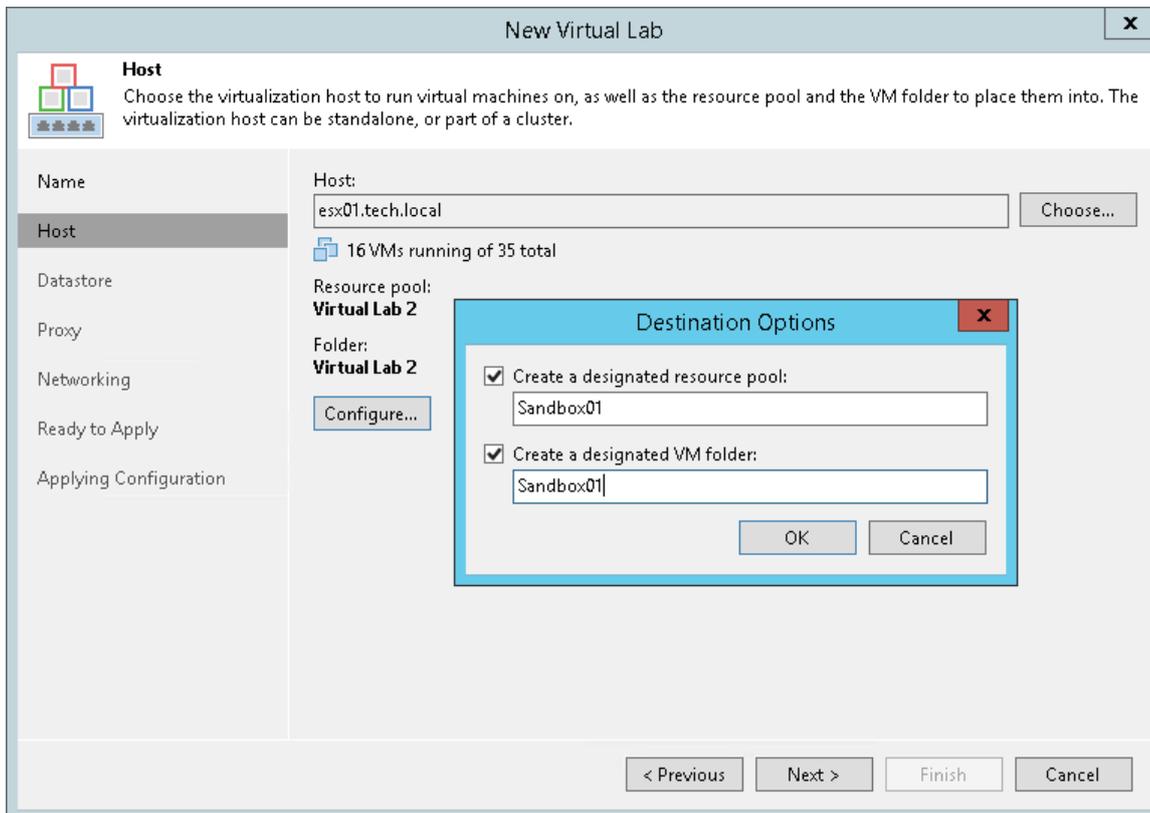
To select an ESX(i) host:

1. Click **Choose**.
2. Select an ESX(i) host on which the new virtual lab must be created. You can select a standalone ESX(i) host or an ESX(i) host being part of a cluster or vCenter Server hierarchy.
3. For every new virtual lab, Veeam Backup & Replication creates a dedicated folder and resource pool on the ESX(i) host. By default, the folder and pool have the same name as the virtual lab. To change the name of the folder and/or resource pool, click **Configure**. In the **Destination Options** window, enter the necessary names.

IMPORTANT!

You cannot create resource pools in clusters with disabled DRS. If the target host is a part of such a cluster, the **Create a designated resource pool** option will be disabled in the **Destination Options** window. For more information, see <http://kb.vmware.com/kb/1004098>.

You cannot create folders on standalone ESX(i) hosts or ESX(i) hosts that are managed by the vCenter Servers but are added to Veeam Backup & Replication as standalone hosts. To overcome this situation, add the corresponding vCenter Server to Veeam Backup & Replication.



Selecting an ESX(i) Host for VM Replicas Verification

When you select an ESX(i) host for the virtual lab where VM replicas will be verified, mind the location of verified VM replicas and VM replicas added to the application group:

- If verified VM replicas and VM replicas from the application group are located on the same ESX(i) host, you must select the ESX(i) host on which these VM replicas are registered. Verified VM replicas and VMs from the application group will be started on the selected ESX(i) host. If the application group contains VMs added from VM backups or storage snapshots, these VMs will also be started on the selected ESX(i) host.

For this type of virtual lab configuration, you need to choose one of single-host networking modes: Basic single-host or Advanced single-host. For more information, see [Selecting a Networking Mode](#).

- If verified VM replicas and/or VM replicas from the application group are located on different ESX(i) hosts, you can select any ESX(i) host in your virtual environment. Veeam Backup & Replication will create the virtual lab on the selected ESX(i) host. Verified VM replicas and VM replicas from the application group will be started on ESX(i) hosts where they are registered and connected to the virtual lab with the help of VMware DVS technology.

The ESX(i) host on which the virtual lab is created must meet the following requirements:

- The ESX(i) host must be located in the same datacenter where VM replicas are registered.
- The ESX(i) host must have enough CPU and RAM resources. If the application group contains VMs that are started from backups or storage snapshots, these VMs will be started on the same ESX(i) host where the virtual lab is located, which will require a lot of resources.
- For this type of virtual lab configuration, you must use the Advanced multi-host networking mode. For more information, see [Selecting a Networking Mode](#).

Step 4. Select Datastore

At the **Datastore** step of the wizard, you can select where redo logs for verified VMs must be stored. Redo logs are auxiliary files used to keep changes that take place when VMs run in the virtual lab. By default, redo logs are stored on the [vPower NFS server](#). However, you can store redo logs on any datastore in the virtual environment. Redirecting redo logs improves verification performance. As soon as a recovery verification job completes, Veeam Backup & Replication deletes redo logs.

To redirect redo logs:

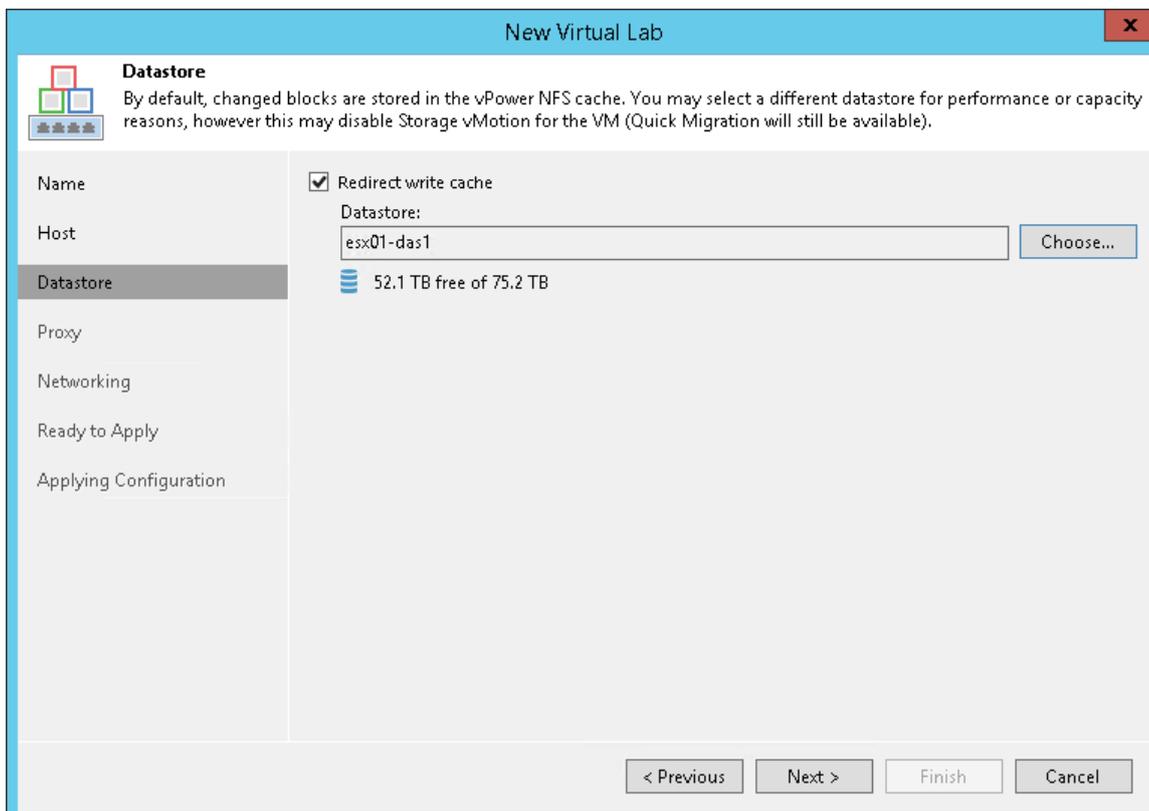
1. Select the **Redirect virtual disk updates** check box.

If you perform staged restore, the **Redirect virtual disk updates** option allows you to select a datastore where VM delta files will be stored. Delta files are auxiliary files that keep changes made to a VM during script execution. For more information, see [Staged Restore](#).

2. Click **Choose** and select a datastore from the list.

IMPORTANT!

If disks of verified VMs are greater than 2 TB, you must not place redo logs on a VSAN datastore. Otherwise, Veeam Backup & Replication will fail to create snapshots for verified VMs. For more information, see [VMware Docs](#).



Step 5. Set Up Proxy Appliance

At the **Proxy** step of the wizard, configure proxy appliance settings.

1. Select the **Use proxy appliance in this virtual lab** check box to enable automatic recovery verification of VMs. The proxy appliance acts as a gateway that provides access from the backup server to VMs in the virtual lab. If you do not select this check box, during recovery verification Veeam Backup & Replication will only start VMs in the virtual lab and perform the heartbeat test for VMs. You will have to manually test VMs or perform manual item-level restore over the VM console.
2. By default, the proxy appliance is placed on a datastore with the maximum amount of free space. The default name of the proxy appliance is the virtual lab name that you have specified at the **Name** step of the wizard. To change a name or a datastore for the proxy appliance, click **Edit** and specify a new name or choose a different datastore.
3. Click **Configure** and select a production network in which the proxy appliance will be created. Specify an IP address for the proxy appliance in the production network and settings of the DNS server to be used. You can choose to automatically obtain an IP address for the backup proxy and DNS server settings or set them manually.

IMPORTANT!

If you assign to the proxy appliance an IP address from the same network where the backup server is located, Veeam Backup & Replication will automatically add a new route to the routing table on the backup server. If you assign to the proxy appliance an IP address from a different network, you will have to manually add a new route to the routing table on the router in the production network. If you do not add a new route, tests and application scripts will fail and you will not be able to access VMs in isolated networks.

When Veeam Backup & Replication starts a virtual lab, it verifies if the proxy appliance is available by sending a ping request to it. If the corresponding route is not added to the routing table, the SureBackup job will fail.

4. By default, VMs in the virtual lab work in the isolated environment and do not have access to the Internet. If you want to let VMs in the virtual lab access the Internet, select the **Allow proxy appliance to act as internet proxy for virtual machines in this lab** check box. In the **Port** field, specify a port for HTTP traffic. By default, port 8080 is used. In the **Production proxy** field, you can optionally specify an IP address or a fully qualified domain name of an Internet-facing proxy server that VMs must use to access the Internet.

5. On every VM that you plan to start in the virtual lab, adjust proxy settings in the Internet options. To do this, on the VM open **Internet Options > Connections > LAN Settings > Proxy server** and specify an IP address of the proxy appliance on the isolated network and port number.

NOTE:

When you allow the proxy appliance to act as an Internet proxy, you enable the HTTP(S) Internet access for VMs in the virtual lab. The proxy appliance does not proxy other protocols (such as ICMP protocol used for ping tests) for VMs in the virtual lab.

The screenshot shows the 'New Virtual Lab' wizard window with the 'Proxy' step selected. The window title is 'New Virtual Lab'. The 'Proxy' section is active, showing a list of steps on the left: Name, Host, Datastore, Proxy, Networking, Ready to Apply, and Applying Configuration. The main area contains the following configuration options:

- Name:** The proxy appliance provides Veeam Backup server with access to virtual machines running in the isolated virtual lab. Without proxy appliance, recovery verification and item restore operations can only be performed manually, through the VM console.
- Use proxy appliance in this virtual lab (recommended)
- Name:** Sandbox01 (with an 'Edit...' button)
- Datastore:** esx01-das3
- Production network:** VM Network
- IP address:** Obtain automatically
- DNS server:** Obtain automatically (with a 'Configure...' button)
- Allow proxy appliance to act as internet proxy for virtual machines in this lab
- HTTP port:** 8080 (with a spin box)
- Production proxy:** 172.17.53.2

At the bottom of the window are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 6. Select Networking Mode

At the **Networking** step of the wizard, select the type of network settings configuration. The virtual lab configuration depends on objects that you plan to verify in the virtual lab:

- [Backups](#)
- [Replicas](#)
- [VMs from storage snapshots](#)

Selecting Networking Mode for Verifying Backups

Veeam Backup & Replication offers two networking modes for the virtual lab in which VMs from backups can be verified:

- **Basic single-host.** This networking mode is recommended if all VMs that you plan to verify, VMs from the application group and the backup server are located in the same production network. In this case, Veeam Backup & Replication will automatically define all networking settings for the virtual lab.

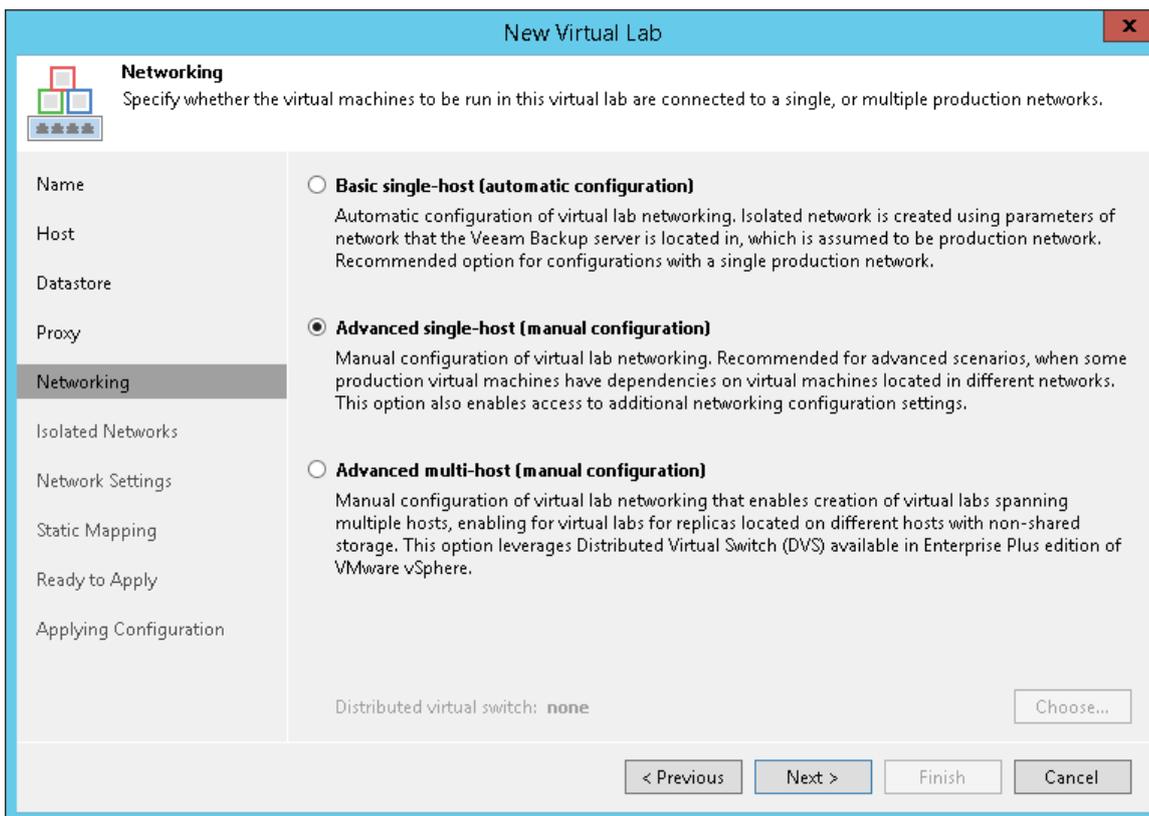
- **Advanced single-host.** This networking mode is recommended if VMs that you plan to verify and/or VMs from the application group are located in different networks. In this case, you will have to manually define settings for isolated networks in the virtual lab.

If you select the **Advanced single-host** option, the **New Virtual Lab** wizard will include additional steps for customizing network settings.

NOTE:

You can also verify VM backups in Advanced Multi-Host virtual labs with DVS. This scenario can be helpful if you want to test VM backups and replicas in the same virtual lab or want to add verified VM backups and replicas to the same SureBackup job.

For more information, see [Advanced Multi-Host Virtual Labs](#).



Selecting Networking Mode for Verifying Replicas

Veeam Backup & Replication offers three networking modes for the virtual lab in which VM replicas are verified:

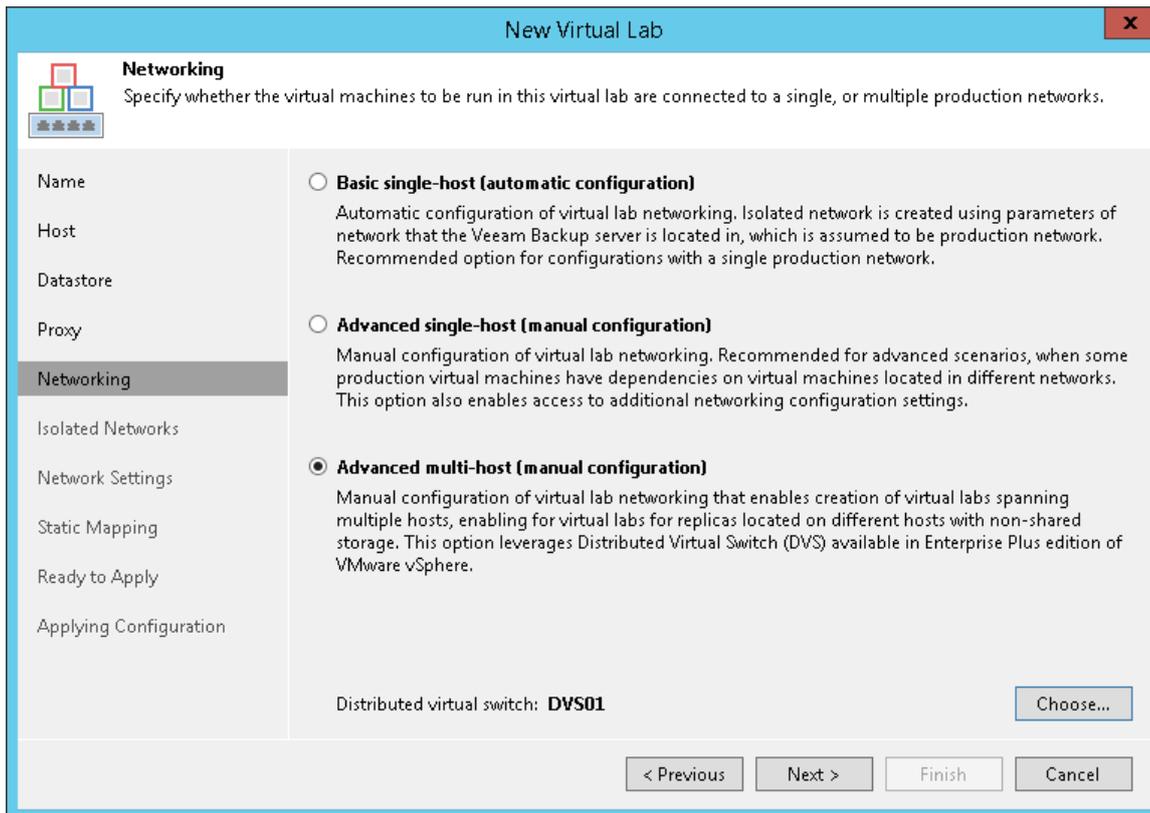
- **Basic single-host.** This type of networking is recommended if VM replicas that you plan to verify are located on the same ESX(i) host and are connected to the same production network. The backup server must also be located in this network. In this case, Veeam Backup & Replication will automatically define all networking settings for the virtual lab.
- **Advanced single-host.** This type of networking is recommended if VM replicas that you plan to verify are located on the same ESX(i) host but connected to different networks. In this case, you will have to manually define settings for isolated networks in the virtual lab.
- **Advanced multi-host.** This type of networking is recommended if VM replicas that you plan to verify are located on the different ESX(i) hosts. For multi-host configuration of the virtual lab, Veeam Backup & Replication uses VMware DVS technology.

If you select the **Advanced multi-host** option, click **Choose** and select the necessary DVS in your virtual environment. Note that Veeam Backup & Replication does not configure a DVS automatically: you must configure it beforehand.

If the **Advanced single-host** or **Advanced multi-host** option is selected, the **New Virtual Lab** wizard will include additional steps for customizing network settings.

IMPORTANT!

For every isolated network in the virtual lab, Veeam Backup & Replication adds a new port group to the DVS. If you use a production DVS, you must isolate port groups created with Veeam Backup & Replication from the production environment. For more information, see [Isolated Networks on DVS](#).



Selecting Network Mode for Verifying VMs on Storage Snapshots

For verifying VMs from storage snapshots, you can select any networking mode.

Step 7. Create Isolated Networks

The **Isolated Networks** step of the wizard is available if you have selected the advanced networking option at the **Networking** step of the wizard.

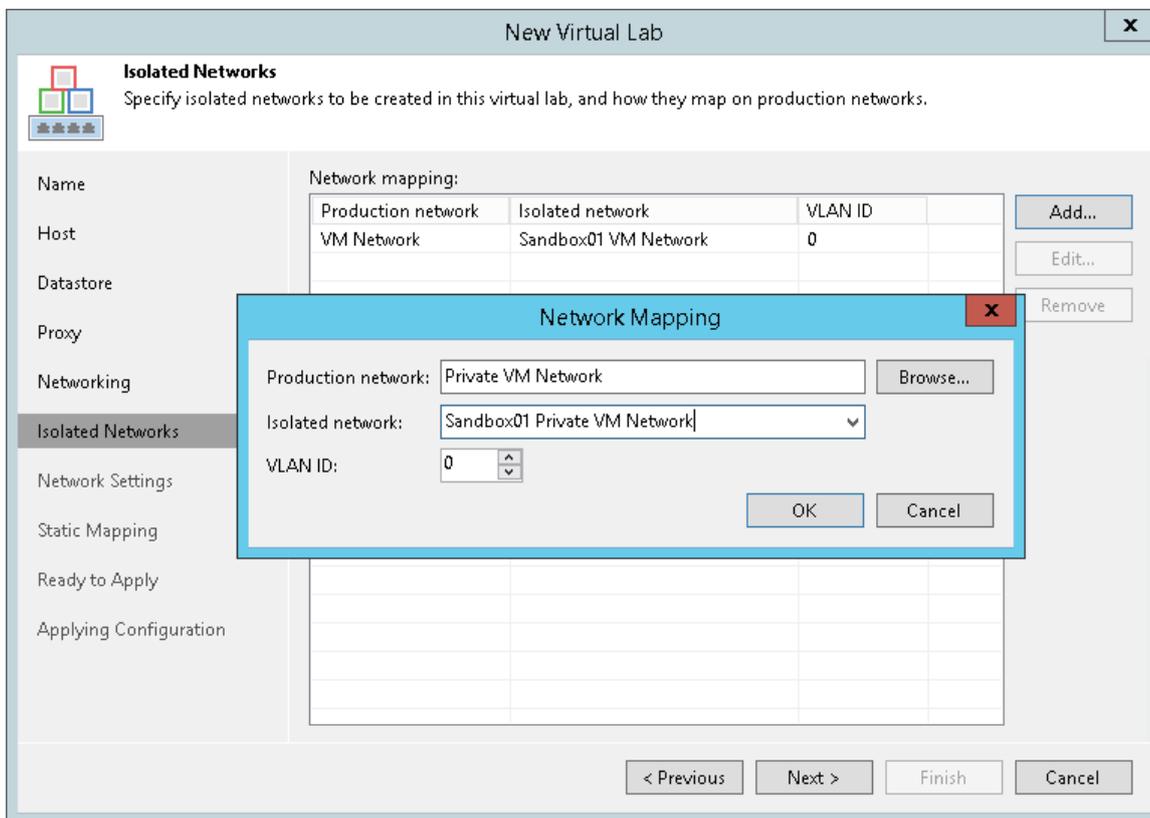
At the **Isolated Networks** step of the wizard, you must configure isolated networks to which verified VMs and VMs from the application group will be connected and map these networks to production networks where original VMs are located.

To add a network:

1. Click **Add**.
2. From the **Production network** list, select a production network in which a VM from the application group or verified VM resides.
3. In the **Isolated network** field, specify a name for the isolated network that must be mapped to the selected production network.
4. In the **VLAN ID** field, enter an ID for the created network. In the advanced multi-host virtual lab, VLAN IDs help ensure that the created network is isolated from the production environment. Alternatively, you can manually connect the DVS that you plan to use to the isolated network. For more information, see [Advanced Multi-Host Virtual Lab](#).

NOTE:

You can map several production networks to the same isolated network. The production networks that you plan to map must have the same network masks and pools of IP addresses. You cannot map one production network to several isolated networks.



Step 8. Specify Network Settings

The **Network Settings** step of the wizard is available if you have selected the advanced networking option at the [Networking](#) step of the wizard.

At the **Network Settings** step of the wizard, you must specify settings for every created isolated network and define how production networks map to isolated networks in the virtual lab.

Communication between production networks and isolated networks is carried out through vNIC adapters on the proxy appliance. A new vNIC adapter must be added for every isolated network.

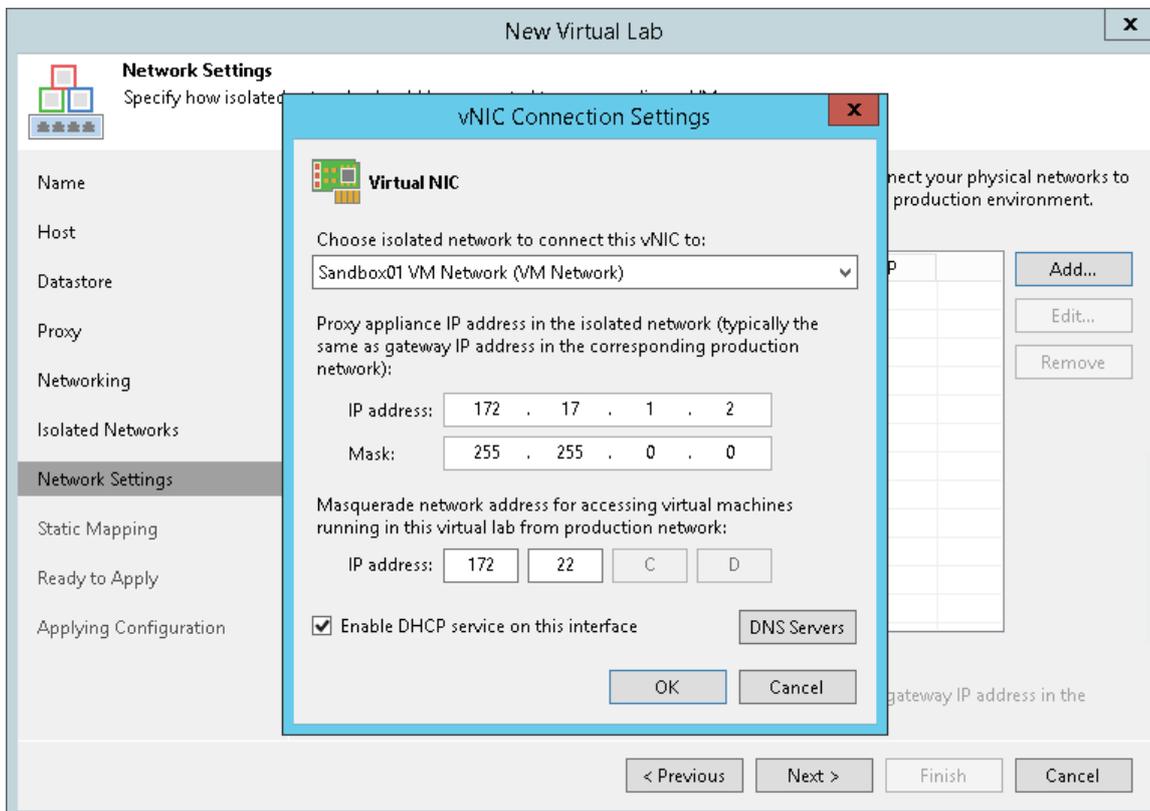
To add a vNIC adapter for an isolated network:

1. At the **Network Settings** step of the wizard, click **Add**.
2. Select a network to which the vNIC adapter must be connected. Specify an IP address that the proxy appliance must have in the isolated network and subnet mask for this isolated network. Typically, the IP address set for the proxy appliance coincides with the IP address of the gateway in the corresponding production network.
3. After you specify the IP address, Veeam Backup & Replication will automatically configure a masquerade IP address for accessing VMs in the virtual lab from the production network. You can change the masquerade network IP address if necessary.
4. Select the **Enable DHCP service on this interface** check box and specify settings of a virtualized DNS server if necessary.
5. Click **OK**.
6. To enable communication between isolated networks, select the **Route network traffic between vNICs** check box. Make sure that the IP address of the proxy appliance in the isolated network matches the IP address of the gateway in the production network.

IMPORTANT!

Mind the following:

- You cannot assign more than one vNIC to a single isolated network.
- Network addresses specified for different vNIC adapters must belong to different networks. For example, if the first network adapter has address 192.168.0.1 and the network mask is 255.255.255.0, and the second one – 192.168.0.2 and the network mask is 255.255.255.0, such configuration will not work. In this situation, you need to assign to the second adapter an IP address from a different network, for example, 172.16.0.1.



Step 9. Specify Static IP Mapping Rules

The **Static Mapping** step of the wizard is available if you have selected the advanced networking option at the [Networking](#) step of the wizard.

At the **Static Mapping** step of the wizard, you can specify static IP address mapping rules to make VMs in the virtual lab accessible from any machine in the production network.

To add a new rule:

1. Select the **Define static IP address mapping** check box.
2. Click **Add**.
3. In the **IP Address Mapping** window, specify settings of a new rule:
 - a. In the **Isolated IP** field, specify an IP address of the VM in the production network.
 - b. In the **Access IP** field, specify an IP address in the production network that you want to use to access the VM in the virtual lab. You must use an IP address that is not allocated to any machine yet.

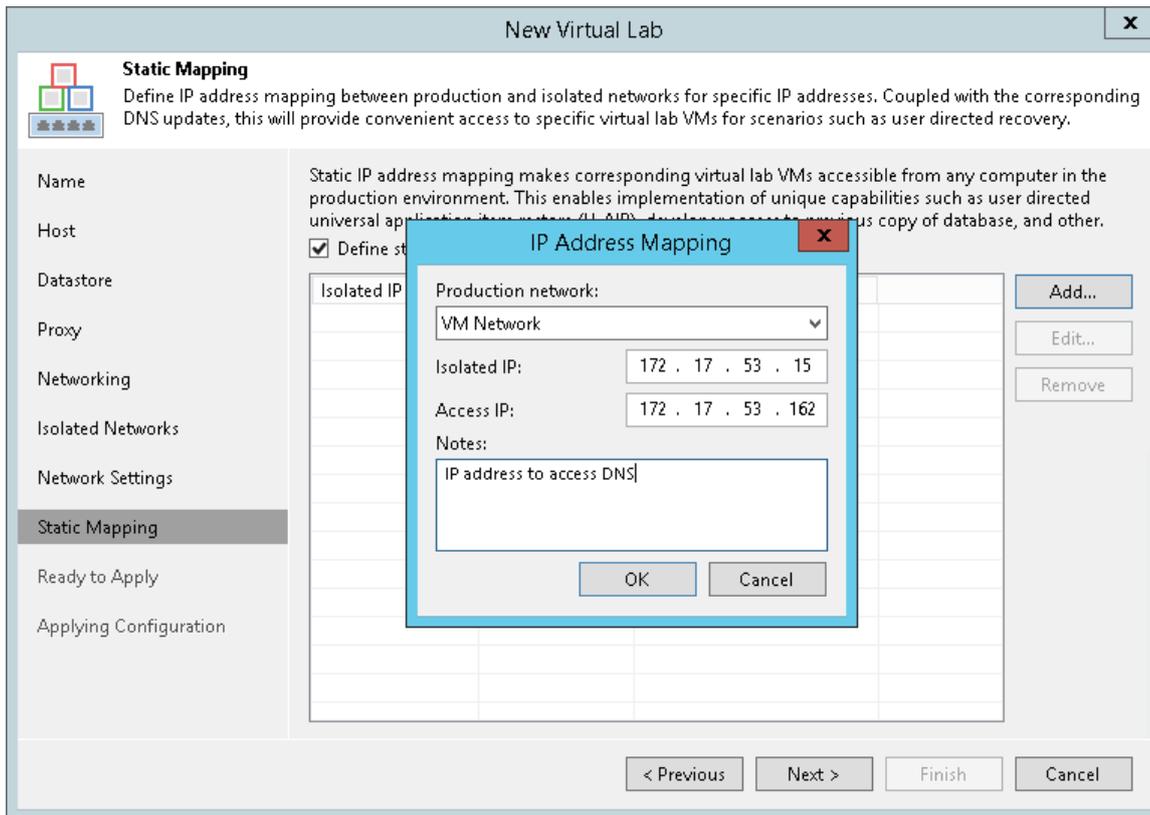
NOTE:

It is recommended that you assign an access IP from the same subnet where the proxy appliance resides. In the opposite case, you will have to configure routing rules for the access IP manually.

For example, a DNS server that you plan to start in the virtual lab has IP address 172.17.53.15 in the production network. To set static mapping for the DNS server:

1. In the **Isolated IP** field, you must define its production IP address – 172.17.53.15.
2. In the **Access IP** field, you must define any free IP address from the production network, for example, 172.17.53.162.

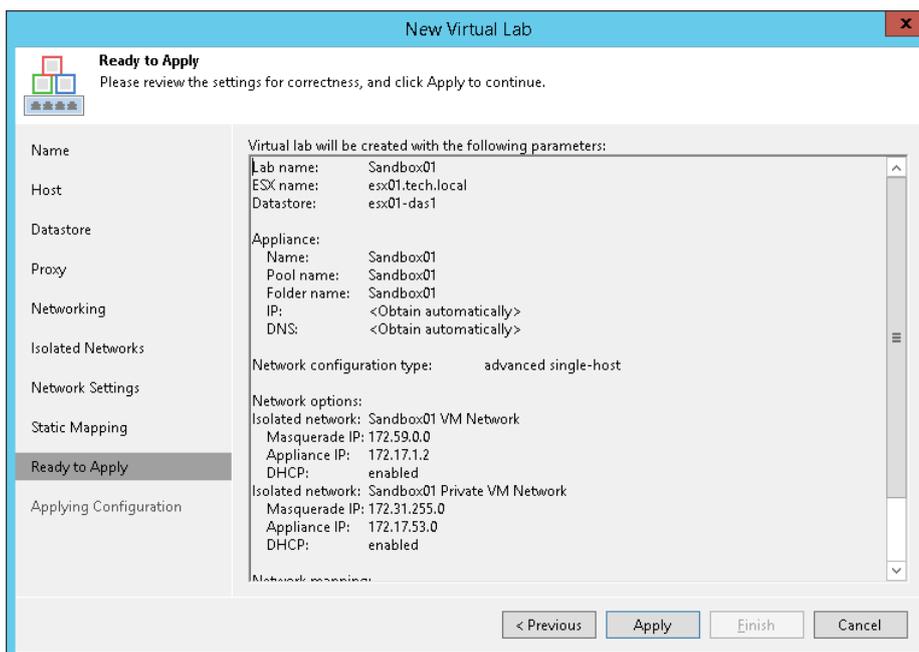
After a virtual lab is created and VMs are started in the virtual lab, you will be able to access the DNS server in the virtual lab from the production environment by IP address 172.17.53.162.



Step 10. Apply Parameters

At the **Ready to Apply** step of the wizard, complete the procedure of virtual lab configuration.

1. Review details of the virtual lab.
2. Click **Apply** to create the virtual lab.
3. At the last step of the wizard, click **Finish** to exit the wizard.

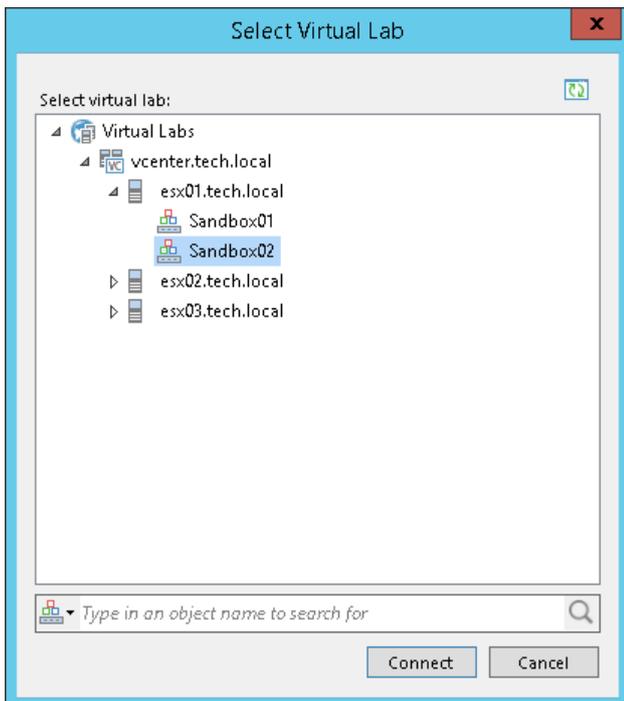


Connecting to Existing Virtual Lab

You can connect an existing virtual lab and use this virtual lab for recovery verification. For example, you can connect to a virtual lab that has been created on another backup server.

To connect to a virtual lab:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Virtual Labs** under **SureBackup** and click **Connect Virtual Lab > VMware** on the ribbon or right-click **Virtual Labs** and select **Connect Virtual Lab > VMware**.
3. Select the virtual lab and click **Connect**. To quickly find a virtual lab, use the search field at the bottom of the **Select Virtual Lab** window: enter a virtual lab name or a part of it in the field below and press **[ENTER]**.



Editing and Deleting Virtual Labs

You can edit settings of a virtual lab or delete the virtual lab.

Always use Veeam Backup & Replication to modify or delete a virtual lab. If you edit virtual lab settings or delete any of its components from outside, for example, in vSphere Client, the lab will be corrupted and its component such as the created vSwitch, resource pool will remain in the virtual infrastructure.

Editing Virtual Labs

To edit settings of a virtual lab:

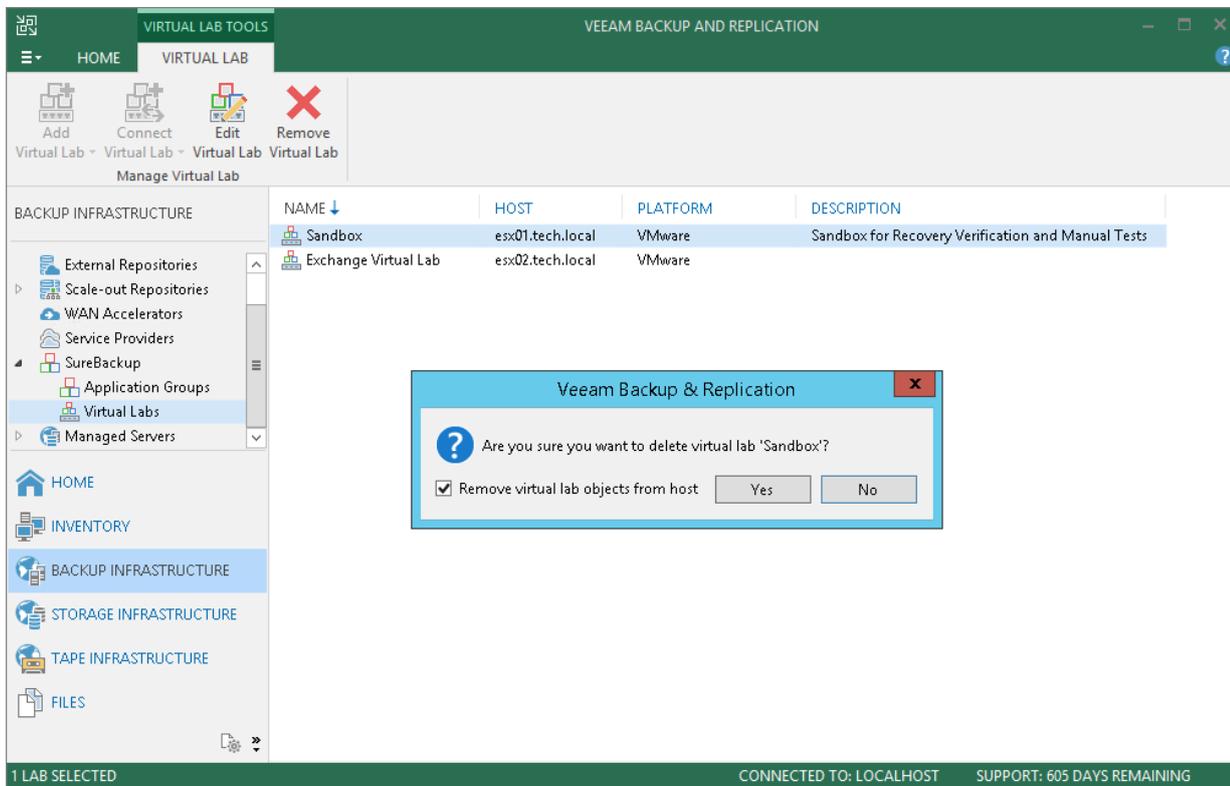
1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Virtual Labs** under **SureBackup**.
3. In the working area, select a virtual lab and click **Edit Virtual Lab** on the ribbon or right-click the virtual lab and select **Properties**.

4. Edit virtual lab settings as required.

Removing Virtual Labs

To remove a virtual lab:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Virtual Labs** under **SureBackup**.
3. In the working area, select a virtual lab and click **Remove Virtual Lab** on the ribbon or right-click the virtual lab and select **Delete**.
4. If you want to remove virtual lab object from the virtual infrastructure, in the displayed window select the **Remove virtual lab objects from host** check box. If you do not enable this option, Veeam Backup & Replication will disconnect the virtual lab from the backup server. You will be able to connect to this virtual lab later.



SureBackup Job

A SureBackup job is a task for recovery verification. The SureBackup job aggregates all settings and policies of the recovery verification task, such as application group and virtual lab to be used, VM backups that must be verified in the virtual lab and so on. You can run the SureBackup job manually or schedule it to run automatically.

When a SureBackup job runs, Veeam Backup & Replication first creates an environment for recovery verification:

1. Veeam Backup & Replication starts the virtual lab.
2. In the virtual lab, Veeam Backup & Replication starts VMs from the application group in the required order. VMs from the application group remain running until the verified VMs (VMs from the linked job) are booted from backups and tested.

If Veeam Backup & Replication does not find a valid restore point for any of VMs from the application group, the SureBackup job fails.
3. When the virtual lab is ready, Veeam Backup & Replication starts verified VMs (VMs from the linked job) to the necessary restore point and, depending on the job settings, verifies them one by one or creates several streams and verifies a number of VMs simultaneously.

If Veeam Backup & Replication does not find a valid restore point for any of verified VMs, verification of this VM fails, but the job continues to run.

By default, you can start and test up to three VMs at the same time. You can also increase the number of VMs to be started and tested simultaneously. Keep in mind that if these VMs are resource demanding, performance of the SureBackup job as well as performance of the ESX(i) host on which the virtual lab resides may decrease.

Once the verification process is complete, VMs from the application group are powered off. Optionally, you can leave the VMs from the application group running to perform manual testing or enable user-directed application item-level recovery.

In some cases, the SureBackup job schedule may overlap the schedule of the backup job linked to it. The backup file may be locked by the backup job and the SureBackup job will be unable to verify such backup. In this situation, Veeam Backup & Replication will not start the SureBackup job until the corresponding backup job is over.

To overcome the situation of job overlapping, you may chain the backup and SureBackup jobs or define the timeout period for the SureBackup job. For more information, see [Specifying Job Schedule](#).

NOTE:

VMs from the application group and verified VMs must belong to the same platform – VMware or Hyper-V. Mixed scenarios are not supported.

SureBackup Job Processing

The recovery verification process includes the following steps:

1. **Getting virtual lab configuration.** Veeam Backup & Replication gets information about configuration of the virtual lab where verified VMs must be started.
2. **Starting virtual lab routing engine.** Veeam Backup & Replication starts a proxy appliance used as a gateway to provide access to the virtual lab.
3. **Performing malware scan.** If the recovery verification process includes malware scan, Veeam Backup & Replication scans VM data with antivirus software.

After the malware scan is complete, Veeam Backup & Replication registers the VM on the selected ESX(i) host, powers it on, and runs recovery verification tests for this VM.

Veeam Backup & Replication verifies VMs sequentially – one after another. For example, when the malware scan and recovery verification tests for VM *A* complete, Veeam Backup & Replication verifies VM *B*, and so on.

4. **Publishing.** Veeam Backup & Replication creates a vPower NFS datastore with a VM backup and registers it on the selected ESX server. Veeam Backup & Replication does not deploy the whole VM from the backup file, it deploys VM configuration files only. Virtual disks are deployed per force and per required data blocks.
5. **Reconfiguring.** Veeam Backup & Replication updates configuration files for VMs that must be started in the isolated network.
6. **Registering.** Veeam Backup & Replication registers the verified VM on the selected ESX(i) host.
7. **Configuring DC.** If a verified VM has the Domain Controller or Global Catalog role, the VM is reconfigured.
8. **Powering on.** Veeam Backup & Replication powers on the verified VM in the isolated network.
9. **Performing heartbeat test.** Veeam Backup & Replication checks whether the VMware Tools heartbeat signal (green or yellow) is coming from the VM or not. If the VM has no VMware Tools, the test is not performed, and a notification is written to the session details.
10. **Running ping tests.** Veeam Backup & Replication checks if the VM responds to the ping requests or not. If the VM has no NICs and mapped networks for them and/or has no VMware Tools installed, the ping test is not performed, and a notification is written to the session details.
11. **Application initialization.** Veeam Backup & Replication waits for the applications installed in the VM, for example, Microsoft SQL Server, to start. The application initialization period is defined in settings of the SureBackup job and by default equals to 120 sec. Depending on the software installed in a VM, the application initialization process may require more time than specified in the job settings. If applications installed in a VM are not initialized within the specified period of time, test scripts can be completed with errors. If such an error situation occurs, you need to increase the **Application initialization timeout** value and start the job once again.
12. **Running test scripts.** Veeam Backup & Replication runs scripts to test whether the application installed in the VM is working correctly or not. If the VM has no VMware Tools installed and/or there are no NICs and mapped networks for them, Veeam Backup & Replication skips tests that use the `%vm_ip%` and `%vm_fqdn%` variables as the IP address and fully qualified domain name of the VM cannot be determined.

Test results are written to the job session details. To define whether the script has completed successfully or not, Veeam Backup & Replication uses return codes. If the return code is equal to 0, the script is considered to complete successfully. Other values in the return code mean that the script has failed.

13. **Powering off.** After all tests have been performed, Veeam Backup & Replication powers off the verified VM.
14. **Unregistering.** Veeam Backup & Replication unregisters the verified VM on the selected ESX(i) host.
15. **Clearing redo logs.** Veeam Backup & Replication deletes redo logs from the datastore in the production environment. Redo logs store changes made to the VM while it is running from the backup file.
16. **Unpublishing.** Veeam Backup & Replication unpublishes the content of the backup file on the ESX(i) host.

17. **Running backup validation test.** After a VM has been verified, powered off and unpublished, Veeam Backup & Replication runs a CRC check to verify the VM backup at the file level and make sure that this file is not corrupted.
18. **Stopping virtual lab engine.** Veeam Backup & Replication powers off the proxy appliance in the virtual lab.
19. **Deleting network routes.** Veeam Backup & Replication deletes added network routes from the routing table on the backup server.

Stabilization Algorithm

To be able to perform tests for a verified VM without errors, Veeam Backup & Replication needs to know that the VM is ready for testing. To determine this, Veeam Backup & Replication waits for the VM to reach a stabilization point: that is, waits for the VM to boot completely and report it is ready for tests. After the stabilization point has been established, Veeam Backup & Replication can start performing heartbeat tests, ping tests and running test scripts against the VM.

Veeam Backup & Replication establishes the stabilization point with the help of VMware parameters that it gets from the VM. Depending on the VM configuration, it uses one of three algorithms to do that:

- **Stabilization by IP.** This algorithm is used if the VM has VMware Tools installed, there are NICs and mapped networks for these NICs. In this case, Veeam Backup & Replication waits for an IP address of the VM for mapped networks that is sent by VMware Tools running in the VM. The sent IP address must be valid and must not change for a specific period of time. For more information, see [Recovery Verification Tests](#).
- **Stabilization by heartbeat.** This algorithm is used if the VM has VMware Tools installed but there are no vNICs and mapped networks for them. In this case, Veeam Backup & Replication waits for a green or yellow heartbeat signal from the VM. The signal is sent by VMware Tools running in the VM.
- **Stabilization by Maximum allowed boot time.** This algorithm is used if the VM has neither VMware Tools installed, nor NICs and mapped networks for them. In this case, Veeam Backup & Replication waits for the time specified in the **Maximum allowed boot time** field, which is considered to be a stabilization period for the VM. Once this time interval is exceeded, Veeam Backup & Replication considers that the VM is successfully booted and is ready for testing.

When the stabilization point has been established, Veeam Backup & Replication runs ping, heartbeat tests and performs test scripts against the verified VM.

The stabilization process cannot exceed the time specified in the **Maximum allowed boot** time field. For this reason, you should be careful when specifying this value. Typically, a VM started by a SureBackup job requires more time to boot than a VM started in the production environment. If the stabilization point cannot be determined within the **Maximum allowed boot time**, the recovery verification process is finished with the timeout error. When such an error occurs, you need to increase the **Maximum allowed boot time** value and start the job again.

Creating SureBackup Job

To create a new SureBackup job, use the **New SureBackup Job** wizard.

Before You Begin

Before you create and start a SureBackup job, check the following prerequisites:

- A valid license for Enterprise Edition of Veeam Backup & Replication must be installed on the backup server.

- All applications and services on which verified VMs are dependent must be virtualized in your environment.
- You must create or connect a virtual lab. For more information, see sections [Creating Virtual Lab](#) and [Connecting to Existing Virtual Lab](#).
- If you plan to scan VM data for malware, [check requirements and limitations](#).
- If you plan to verify VMs with a ping test, the firewall on tested VMs must allow ping requests.
- If you plan to verify VMs with a heartbeat test, VMware Tools must be installed in tested VMs.
- [For storage snapshots] The storage system must be added to the backup infrastructure.

Mind the following limitations:

- Verified VM replicas must be in the *Normal* state. If a VM replica is in the *Failover* or *Failback* state, you will not be able to verify it with the SureBackup job.
- You cannot link to SureBackup jobs VMs from backups of vCloud Director VMs, backups created with backup copy jobs and backups stored on cloud backup repositories.
- The source backup or replication job has a higher priority than the SureBackup job. If the source backup or replication job starts when the SureBackup job is running, and this job is about to modify the restore point from which the VM is started, Veeam Backup & Replication automatically powers off VMs in the virtual lab and completes the SureBackup job.

Step 1. Launch New Sure Backup Job Wizard

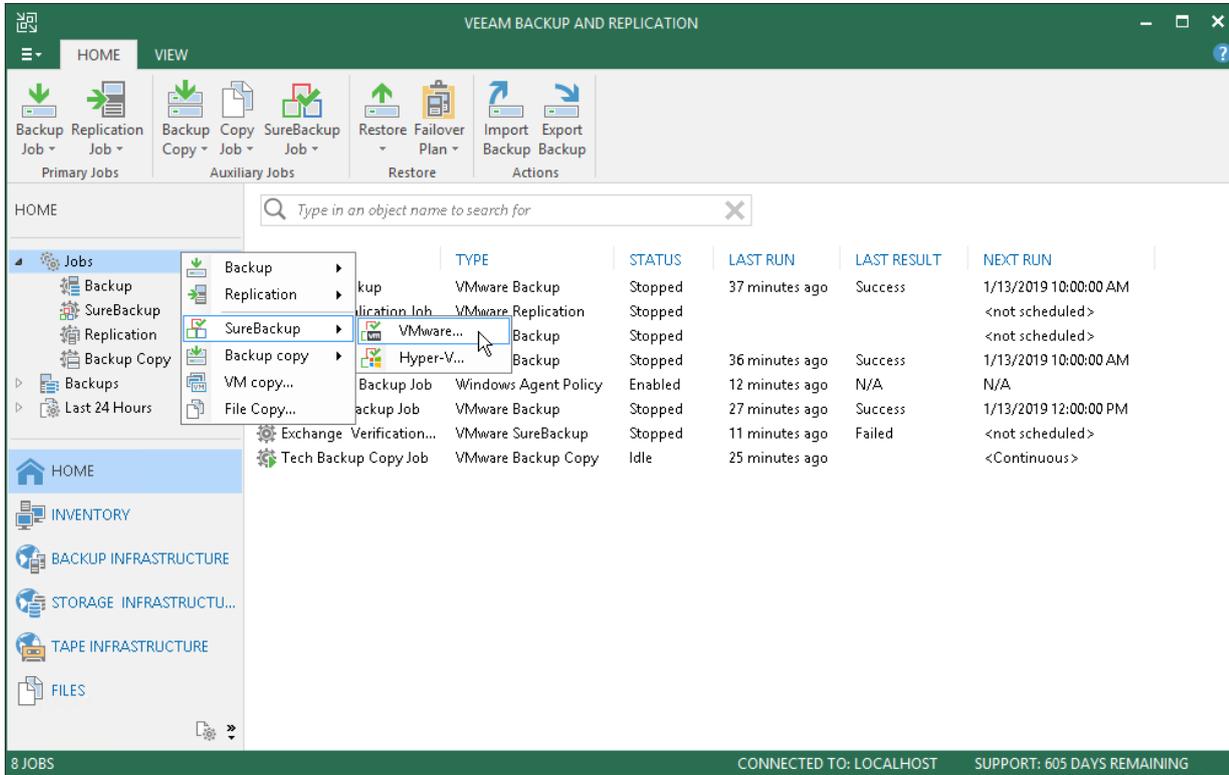
To launch the **New SureBackup Job** wizard, do either of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select **SureBackup**. In the working area, click **Add SureBackup Job > VMware**.
- Open the **Home** view. On the **Home** tab, click **SureBackup Job > VMware** on the ribbon.
- Open the **Home** view. In the inventory pane, right-click **SureBackup** under **Jobs** and select **SureBackup > VMware**.

You can use this method if you already have at least one SureBackup job. If there are no SureBackup jobs, the **SureBackup** node will not be displayed in the inventory pane. In this case, you can right-click **Jobs** in the inventory pane and select **SureBackup > VMware**.

NOTE:

SureBackup UI elements become available in the Veeam Backup & Replication console only after you create or connect a virtual lab. For more information, see sections [Creating Virtual Lab](#) and [Connecting to Existing Virtual Lab](#).



Step 2. Specify Job Name and Description

At the **Name** step of the wizard, specify a name and description for the SureBackup job.

1. In the **Name** field, enter a name for the SureBackup job.

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

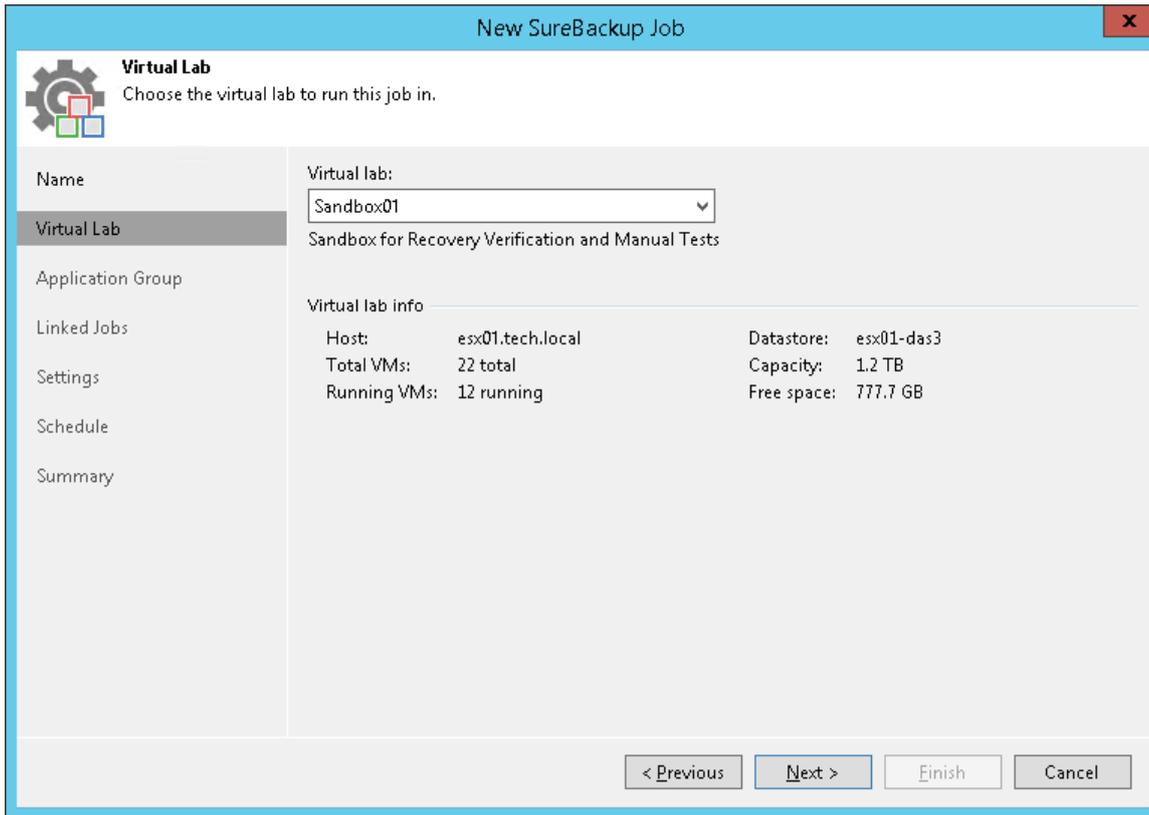
The screenshot shows a 'New SureBackup Job' wizard window. The window title is 'New SureBackup Job'. On the left side, there is a navigation pane with a gear icon and a 'Name' section. The 'Name' section contains a list of options: 'Virtual Lab', 'Application Group', 'Linked Jobs', 'Settings', 'Schedule', and 'Summary'. The main area of the wizard has two input fields: 'Name' and 'Description'. The 'Name' field contains the text 'Exchange SureBackup Job' and the 'Description' field contains the text 'Daily Verification Job'. At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 3. Select Virtual Lab

At the **Virtual Lab** step of the wizard, select a virtual lab that you want to use for recovery verification.

1. From the **Virtual Lab** list, select a virtual lab. The list contains all virtual labs that are created or connected to the backup server.

2. In the **Virtual lab info** section, review information about the selected virtual lab.



Step 4. Select Application Group

At the **Application Group** step of the wizard, select an application group that you want to use for recovery verification.

You can select an application group or skip this step. If the application group is not selected, you must link at least one backup or replication job to the SureBackup job at the [Linked Jobs](#) step of the wizard. In this case, when the SureBackup job starts, Veeam Backup & Replication will only run VMs from the linked job in the virtual lab and verify these VMs.

To select an application group:

1. From the **Application group** list, select an application group. The list contains all application groups that are created on the backup server.
2. In the **Application group info** list, refer to the **Source Status** column to make sure that backups and replicas for VMs in the application group are created.

- To leave VMs from the application group running after the SureBackup job finishes, select the **Keep the application group running after the job completes** check box. With this option enabled, the lab will not be powered off when the SureBackup job completes, and you will be able to perform application item-level restore (U-AIR) and manually test VMs started in the virtual lab.

Step 5. Link Backup or Replication Job

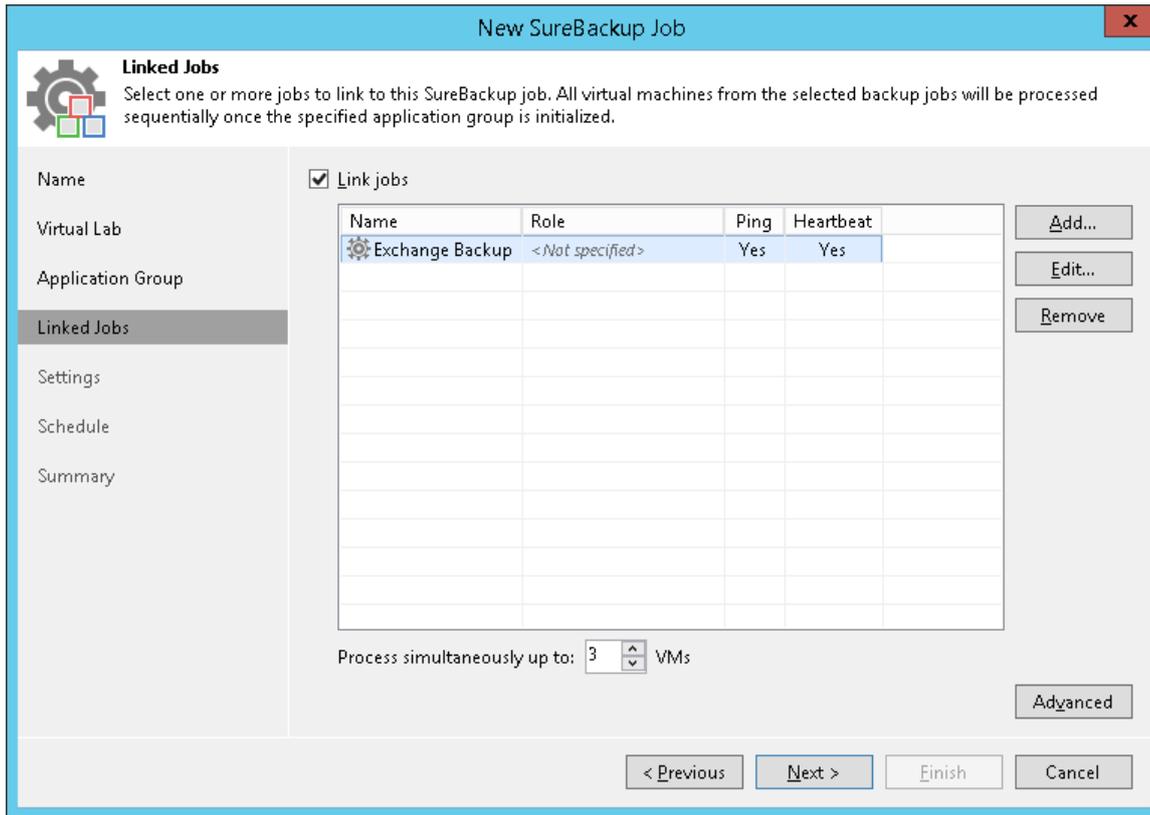
At the **Linked Jobs** step of the wizard, select backup or replication jobs with VMs that you want to verify with the SureBackup job.

You can link a backup or replication job to the SureBackup job or skip this step. If you do not link a backup or replication job, Veeam Backup & Replication will only start VMs from the application group in the virtual lab and verify them. You have an option not to link a backup or replication job to the SureBackup job only if you have selected an application group at the [Application Group](#) step of the wizard.

To link a backup or replication job to the SureBackup job:

- Select the **Link jobs** check box.
- Click **Add**.
- In the **Select Jobs** window, select backup and/or replication jobs.
- In the **Process simultaneously up to ... VMs** field, specify the maximum number of VMs that can be started at the same time. For example, if you select to start 3 VMs at the same time, Veeam Backup & Replication will create 3 streams – 1 stream per every verified VM. When one VM has been tested and powered off, the next VM will be started in the available stream. After all VMs are verified, VMs from the application group will be powered off or will be left running (if the **Keep the application group running after the job completes** option has been enabled at the [Application Group](#) step of the wizard).

To remove a backup or replication job from the list, select it and click **Remove**.



Step 6. Specify Recovery Verification Options and Tests

You must specify verification options for every VM from the jobs linked to the SureBackup job:

- [Select a role that a VM performs](#)
- [Configure VM startup settings](#)
- [Select tests that must be performed for the VM](#)
- [Specify credentials for running the verification script](#)

If all VMs in the linked job perform the same role, you can specify startup options and test settings for the whole job in bulk. If VMs have different roles, you can granularly specify startup options and test settings for every VM in the job.

- To specify startup options and select tests for the whole job, select a job in the list and click **Edit** on the right.
- To specify startup options and select tests for every VM in the job separately, select a job in the list and click **Advanced** on the right. Click **Add**; in the **Add Objects** window select a VM. Select the added VM in the list, click **Edit** and specify settings as described below.

If you use tags to categorize virtual infrastructure objects, check limitations for VM tags. For more information, see [VM Tags](#).

IMPORTANT!

If you specify startup options and tests individually for every VM, Veeam Backup & Replication will apply these options and tests only. Options and tests specified at the level of the SureBackup job will be ignored for this VM.

Role Settings

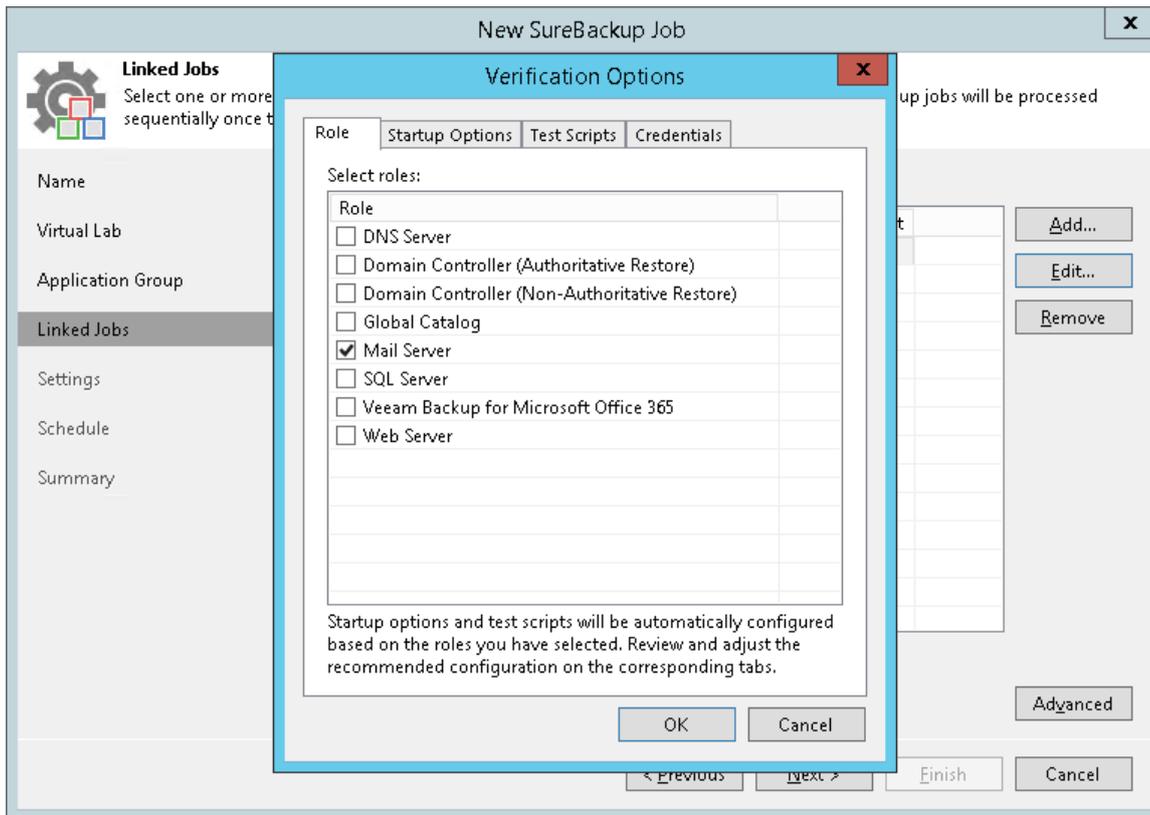
On the **Role** tab, select the role that the VM performs. Veeam Backup & Replication offers the following predefined roles for VMs:

- DNS Server
- Domain Controller (Authoritative Restore). In the Authoritative Restore mode, Veeam Backup & Replication starts a domain controller in the virtual lab and marks it as being authoritative to its replication partners. When other domain controllers (replication partners) are started in the virtual lab, they replicate data from the domain controller started in the Authoritative Restore mode.
- Domain Controller (Non-Authoritative Restore). In the Non-Authoritative Restore mode, Veeam Backup & Replication restores a domain controller in the virtual lab and marks it as being non-authoritative to its replication partners. Non-authoritative domain controllers then replicate data from a domain controller started in the Authoritative Restore mode.
- Global Catalog
- Mail Server
- SQL Server
- Veeam Backup for Microsoft Office 365 (machine on which Veeam Backup for Microsoft Office 365 is installed)
- Web Server

VM roles are described in XML files stored in the *%ProgramFiles%\Veeam\Backup and Replication\Backup\SbRoles* folder. You can add your own roles. To do this, you need to create a new XML file and specify role and test scripts settings in it. For more information, see [Creating XML files with VM Roles Description](#).

After you select the necessary role, Veeam Backup & Replication will automatically configure startup options and assign predefined test scripts for the chosen role. You can use these settings or specify custom settings on the **Startup Options** and **Test Scripts** tabs.

To verify VMs that perform roles other than those specified in the list, you will have to manually configure startup options and specify test scripts that must be run for these VMs.



VM Startup Settings

To configure VM startup settings:

1. In the **Verification Options** window, click the **Startup Options** tab.
2. In the **Memory** section, specify the amount of memory that you want to pre-allocate to the VM when this VM starts. The amount of pre-allocated memory is defined in percent. The percentage rate is calculated based on the system memory level available for the production VM. For example, if 1024 MB of RAM is allocated to the VM in the production environment and you specify 80% as a memory rate, 820 MB of RAM will be allocated to the verified VM on startup.
3. In the **Startup time** section, specify the allowed boot time for the VM and timeout to initialize applications on the VM.

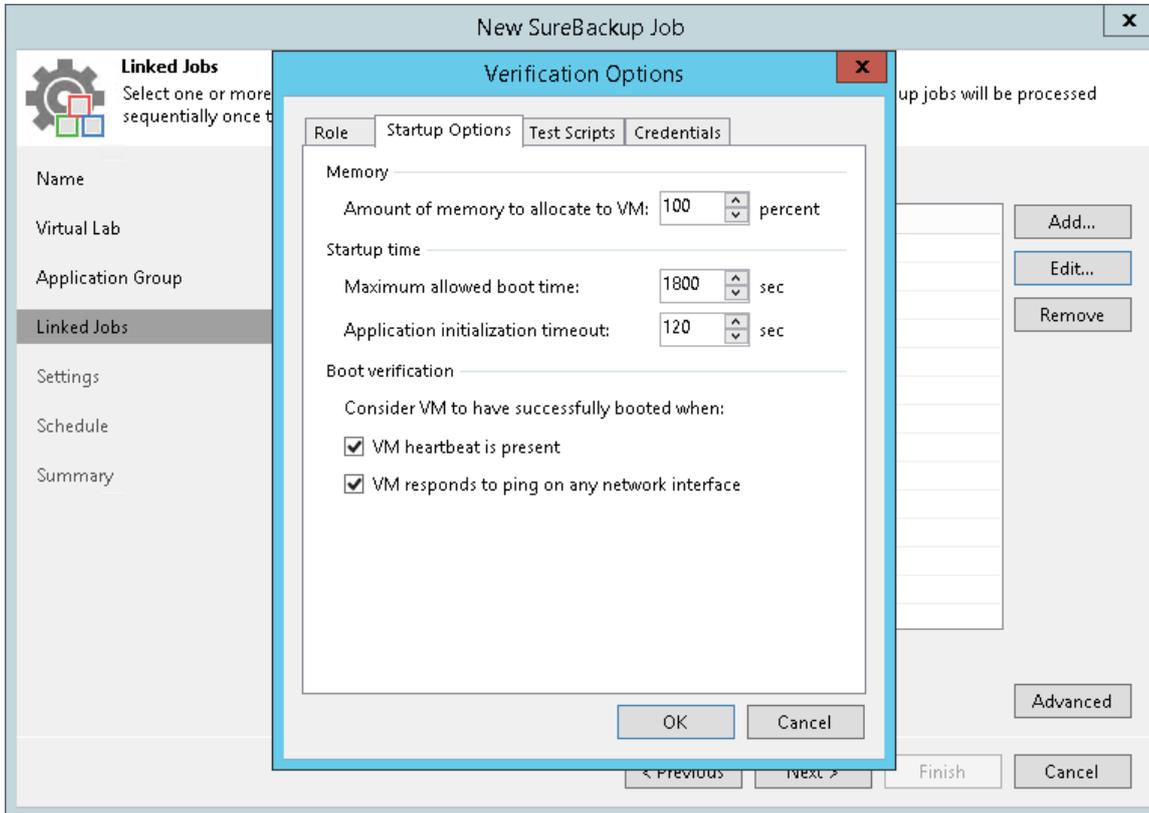
Be careful when specifying the **Maximum allowed boot time** value. Typically, a VM started by a SureBackup job requires more time to boot than a VM started in the production environment. If an application fails to be initialized within the specified interval of time, the recovery verification process fails with the timeout error. If such error occurs, you need to increase the **Maximum allowed boot time** value and run the SureBackup job again.

4. In the **Boot verification** section, specify when the VM must be considered to have been booted successfully:
 - **VM heartbeat is present.** If you enable this option, Veeam Backup & Replication will perform a heartbeat test for the verified VM.
 - **VM responds to ping on any network interface.** If you enable this option, Veeam Backup & Replication will perform a ping test for the verified VM.

If you enable both options, Veeam Backup & Replication will require that both tests are completed successfully: heartbeat test and ping test.

NOTE:

Veeam Backup & Replication performs a heartbeat test only if a VM has VMware Tools are installed. If VMware Tools are not installed, the VM will be started but the test will not be performed.



Test Script Settings

When you select a VM role, Veeam Backup & Replication automatically assigns a predefined script that must be run to verify applications inside the VM. If you want to verify a VM that has some other role not listed on the **Role** tab, do the following:

1. In the **Verification Options** window, click the **Test Scripts** tab.
2. Click **Add**.
3. In the **Test Scripts** window, select **Use the following test script**.
4. In the **Name** field, specify a name for the script.
5. In the **Path** field, define a path to an executable script file that must be run to verify the VM. You can do one of the following:
 - o If you have your own custom script, define a path to it in the **Path** field.
 - o If you do not have a custom script, you can use Veeam standard utility, `Veeam.Backup.ConnectionTester.exe`, that probes application communication ports. The utility is located in the installation folder of Veeam Backup & Replication: `%ProgramFiles%\Veeam\Backup and Replication\Backup\Veeam.Backup.ConnectionTester.exe`. Specify this path in the **Path** field.

- In the **Arguments** field, specify an IP address of the verified VM and the port that you want to probe (if the selected test probes the port). You can use the `%vm_ip%` variable to define the VM IP address or the `%vm_fqdn%` variable to define the VM fully qualified domain name.

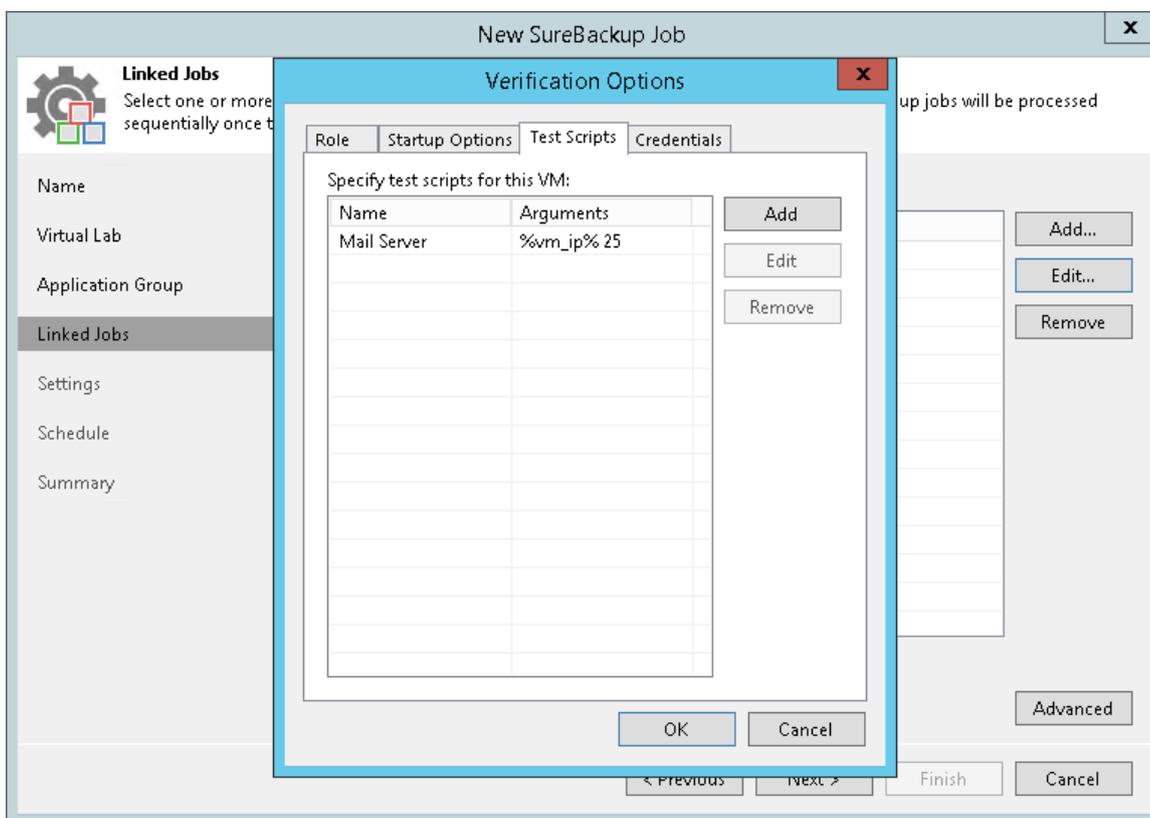
For Microsoft SQL Server, you can also specify a path to the log file in the `%log_path%` argument. For more information, see [Backup Recovery Verification Tests](#).

- Click **OK** to add the configured test.

To edit test settings, select the test in the list and click **Edit**. To delete a test, select it in the list and click **Remove**.

NOTE:

If a VM performs several roles and runs a number of applications, you can add several verification scripts to verify work of these applications. It is recommended that you specify the maximum startup timeout value and allocate the greatest amount of memory for such VMs.

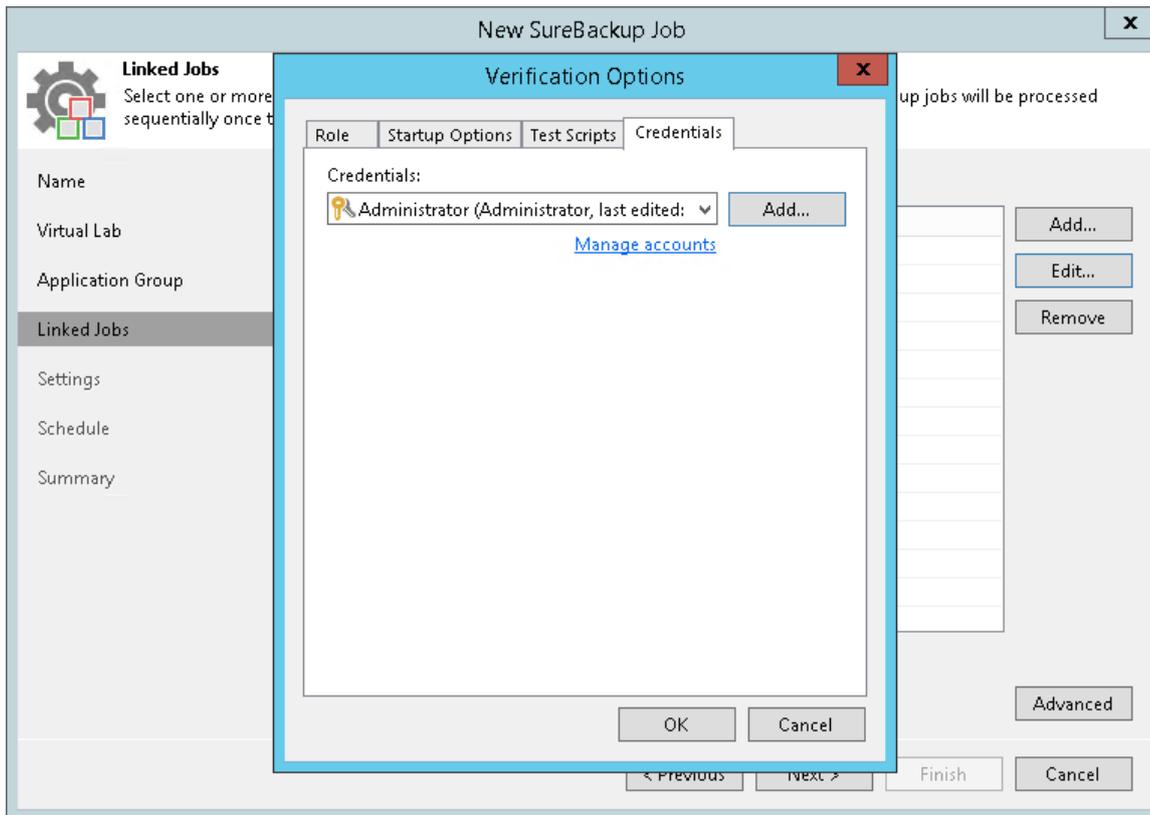


Credentials Settings

In the **Credentials** tab, specify credentials to authenticate in the VM where you need to run the script.

- Click the **Credentials** tab.
- From the **Credentials** list, select credentials for the account under which you want to run the script.

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](#).



Step 7. Specify Additional Job Settings

On the **Settings** step of the wizard, specify additional settings for the SureBackup job:

1. [For VM backups only] If you want to validate the backup file with a CRC check and make sure that the file is not corrupted, select the **Validate entire virtual disk contents** check box. You can optionally exclude VMs being a part of the application group from this test. To do this, select the **Skip validation for application group VMs** check box. For more information, see [Recovery Verification Tests](#).
2. If you want Veeam Backup & Replication to scan VM data with antivirus software, select the **Scan the selected restore point for malware** check box. For more information, see [Secure Restore](#).
 - If you want the antivirus to continue scanning VM data after the first malware is found, select the **Scan the entire image** check box. For information on how to view results of the malware scan, see [Viewing Recovery Verification Job Statistics](#).
 - If you do not want to scan VMs from the application group, select the **Skip application group machines from malware scan** check box. In this case, the antivirus will only scan VMs from linked jobs.

Veeam Backup & Replication scans VM data with antivirus before running verification tests. Mind that the SureBackup job may take considerable time to complete if you are verifying backups of large sized VMs.

3. If you want to receive SNMP traps, select the **Send SNMP trap** check box.

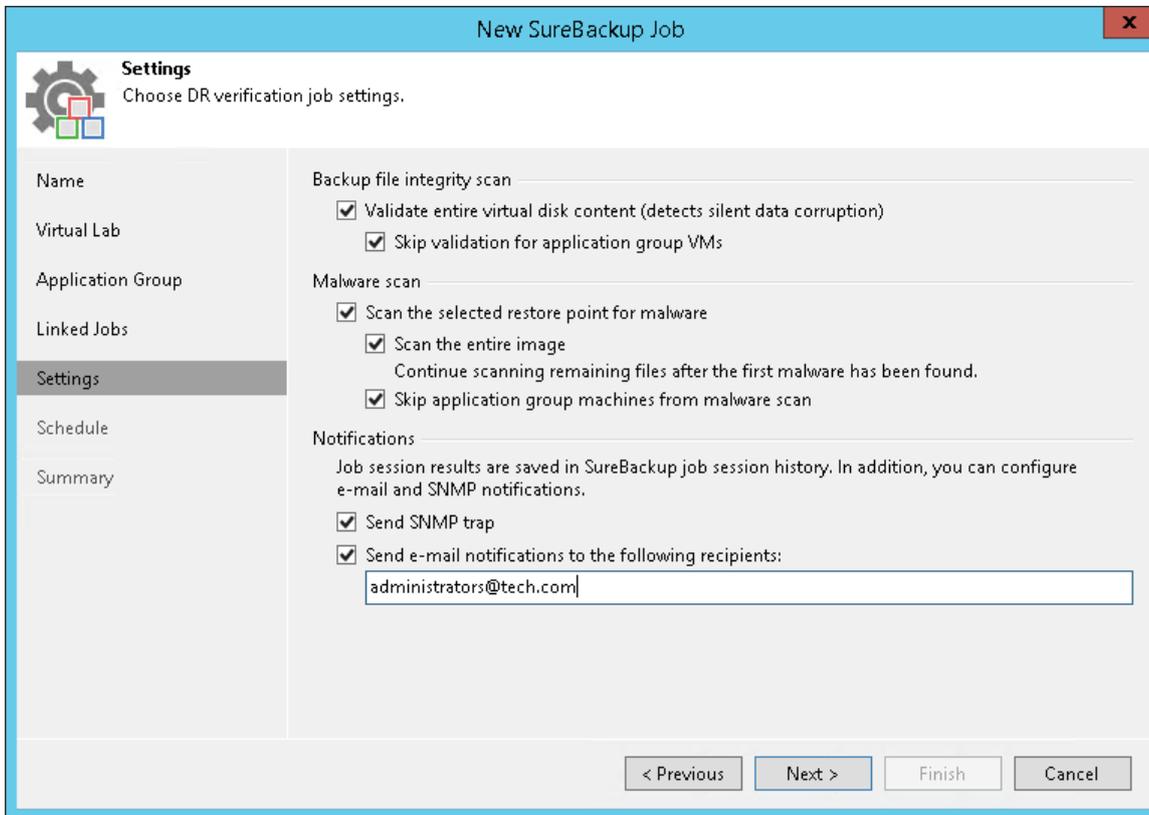
SNMP traps will be sent only if you configure global SNMP settings in Veeam Backup & Replication and on recipient's computer. For more information, see [Specifying SNMP Settings](#).

4. If you want to receive notifications by email, select the **Send email notifications to the following recipients** check box. In the field below, specify recipient's email address. You can enter several addresses separated by a semicolon.

Email notifications will be sent only if you configure global email notification settings in Veeam Backup & Replication. For more information, see [Specifying Email Notification Settings](#).

NOTE:

If you enable the **Keep the application group running after the job completes** option at the **Application Group** step of the wizard, the **Skip validation for application group VMs** option will be automatically enabled.



Step 8. Specify Job Schedule

At the **Schedule** step of the wizard, select to manually run the SureBackup job or schedule the job at specific time, for example, after the corresponding backup or replication job completes.

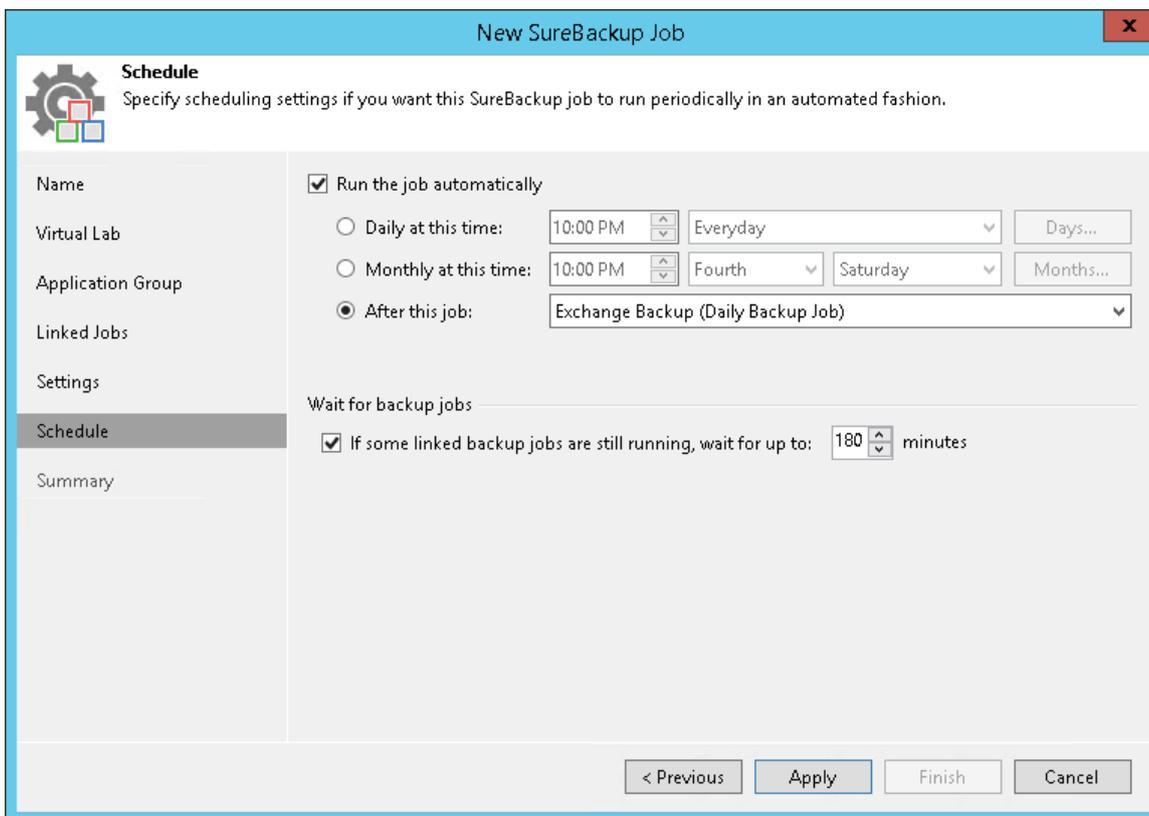
1. To specify the job schedule, select the **Run the job automatically** check box. If this check box is not selected, you will have to manually start the job to perform recovery verification.
2. Choose the necessary schedule option for the job:
 - **Daily at** to start the job at specific time every day, on week days or on specific days.
 - **Monthly at** to start the job once a month on the specified day.
 - **After this job** to chain the job. Typically, a SureBackup job should run after the linked backup or replication job completes. In this case, the SureBackup job will verify the VM backup or VM replica created by the source backup or replication job.

To create a chain of jobs, you must 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.

3. In some cases, the linked backup or replication job may not complete until the SureBackup job starts. If Veeam Backup & Replication finds out that the linked job is still running, the SureBackup job will fail to start. To overcome this situation, select the **If some linked backup jobs are still running, wait up to <N> minutes** check box and specify the necessary time period in the field on the right. If the linked job is still running, Veeam Backup & Replication will wait for the defined period of time and check the linked job after this period elapses.
 - If the linked job is finished within the specified period, the SureBackup job will start.
 - If the linked job is still running, the SureBackup job will not start.

NOTE:

The **After this job** function will only start a job if the first job in the chain is started automatically by schedule. If the first job is started manually, jobs chained to it will not be started.

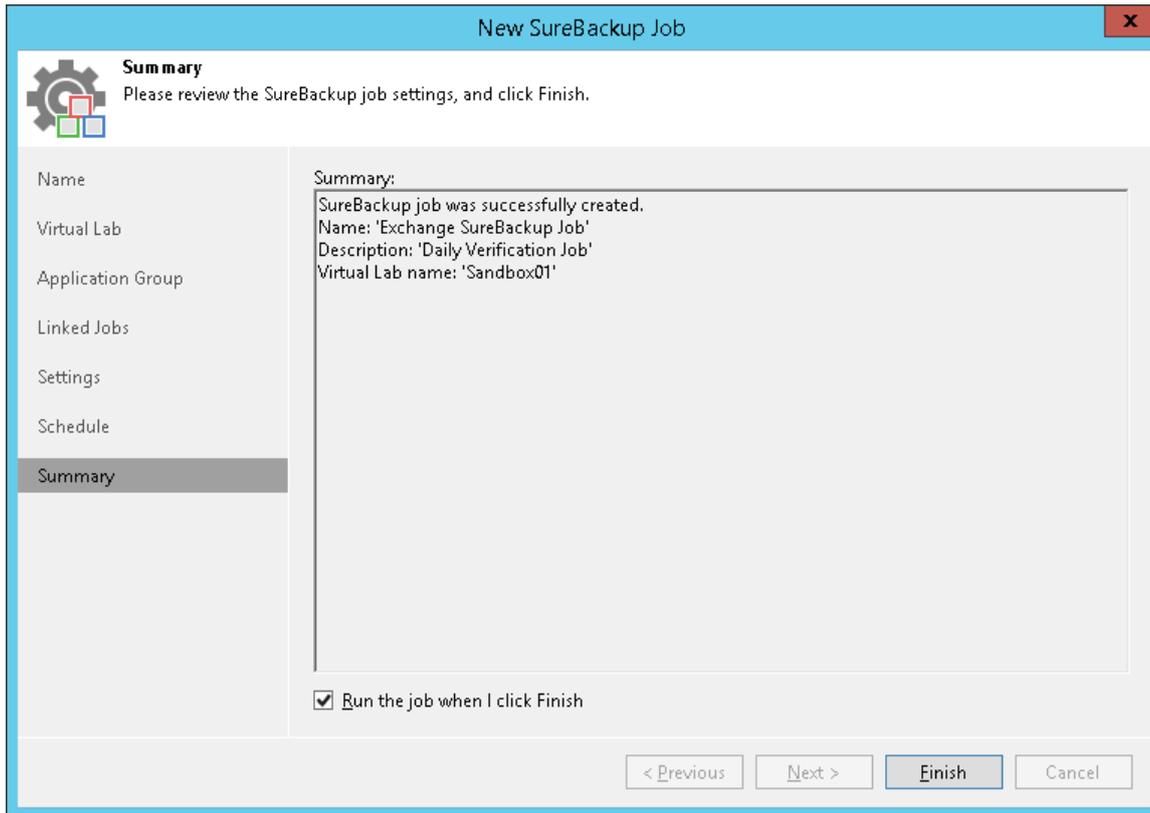


Step 9. Review Job Summary and Finish Working with Wizard

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

1. Review details of the SureBackup job.
2. If you want to start the job right after you finish working with the wizard, select the **Run the job when I click Finish** check box.

3. Click **Finish** to save the job settings and close the wizard.



Starting and Stopping SureBackup Job

You can instruct the SureBackup job to verify the latest restore point of a VM backup or VM replica or select a specific restore point to which the VM from the backup or VM replica must be started.

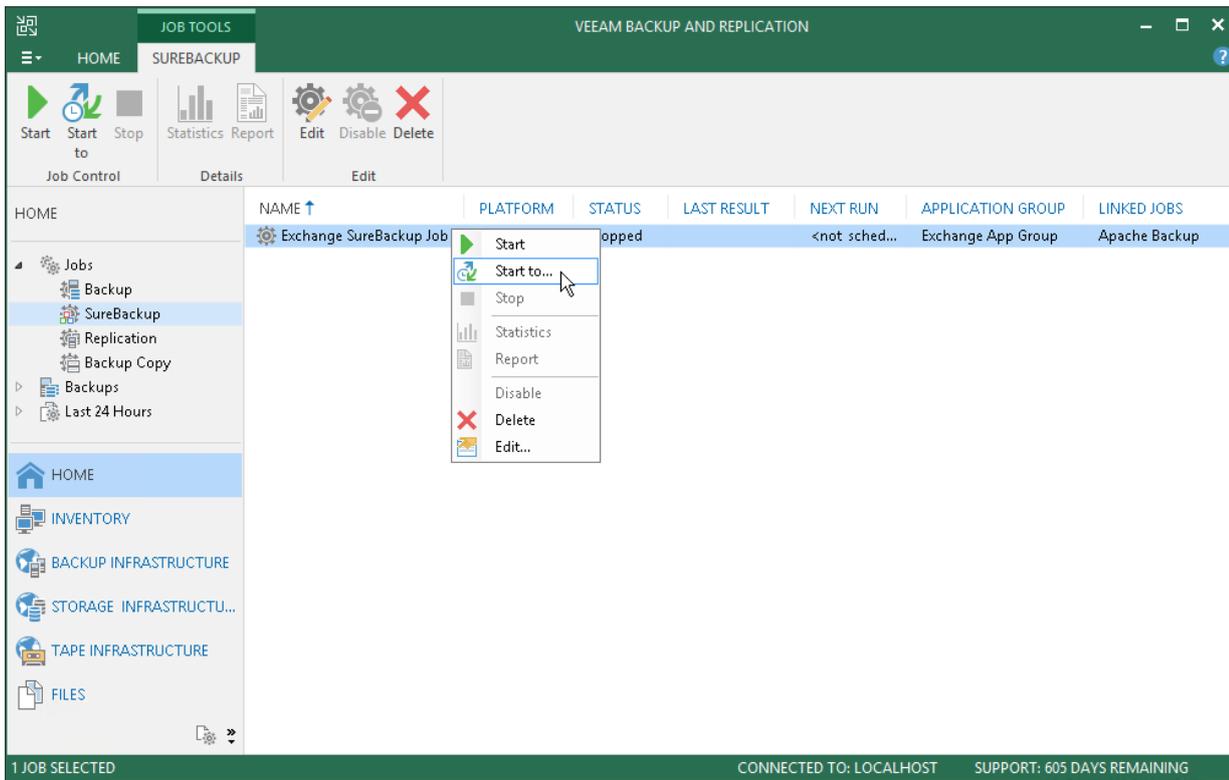
To start a VM from the latest restore point:

1. Open the **Home** view.
2. In the inventory pane, click **SureBackup** under **Jobs**.
3. In the working area, select the SureBackup job and click **Start** on the ribbon. You can also right-click the SureBackup job and select **Start**. Veeam Backup & Replication will start VMs in the application group and verified VMs from the latest restore point and perform necessary tests for them.

To start VMs from a specific point in time:

1. Open the **Home** view.
2. In the inventory pane, select **SureBackup** under **Jobs**.
3. In the working area, select the SureBackup job and click **Start to** on the ribbon. You can also right-click the SureBackup job and select **Start to**.

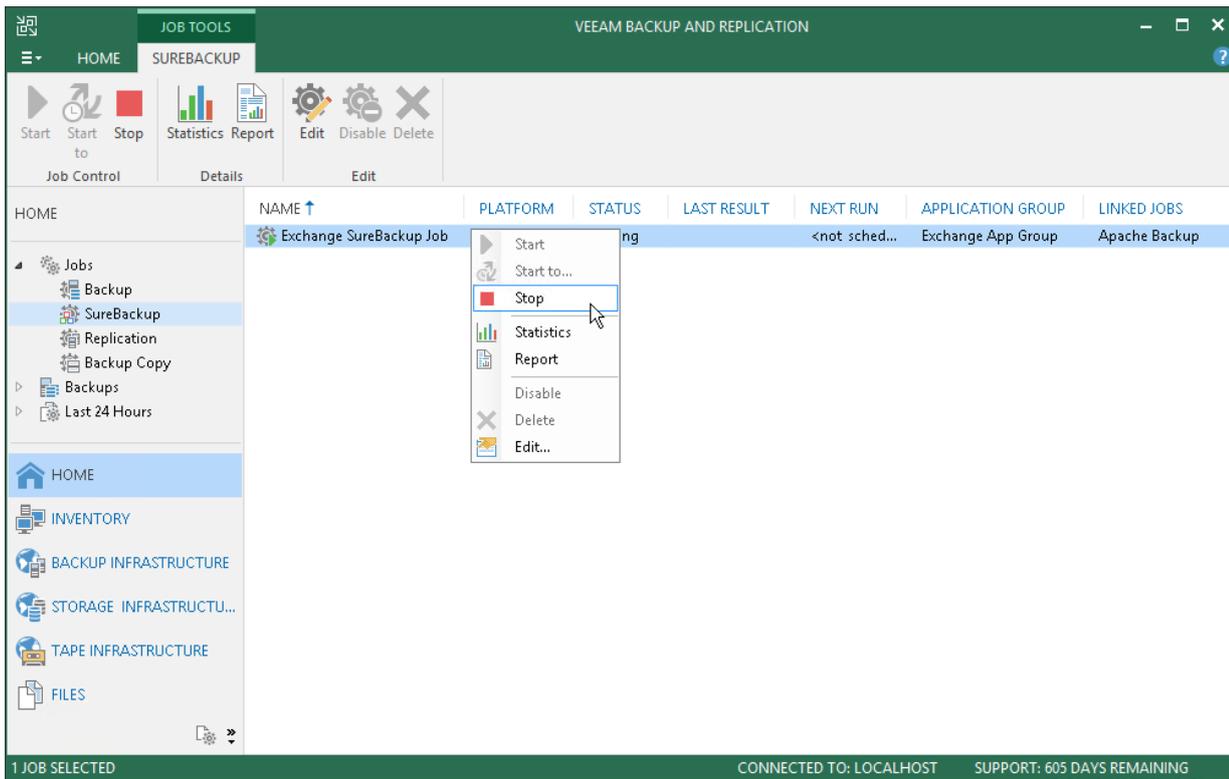
4. In the **Restore Point** window, select an approximate date of the restore point creation. Veeam Backup & Replication will pick the most recent restore point prior to the selected day and start VMs from the application group and verified VMs from this restore point.



To stop a running SureBackup job session:

1. Open the **Home** view.
2. In the inventory pane, select **SureBackup** under **Jobs**.

3. In the working area, select the SureBackup job and click **Stop** on the ribbon. You can also right-click the SureBackup job and select **Stop**.



Viewing Recovery Verification Job Statistics

You can monitor how tests for verified VMs are performed while a recovery verification job is running.

To see the status of VM tests:

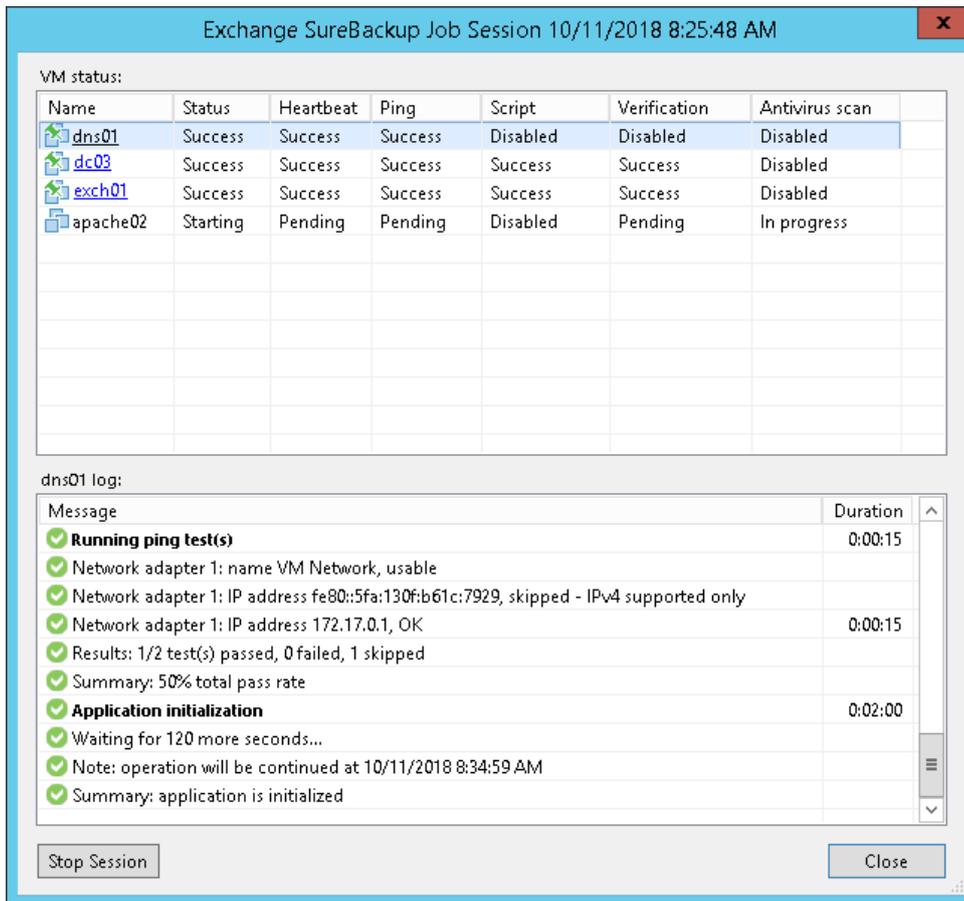
1. Open the **Home** view.
2. In the inventory pane, select **SureBackup** under **Jobs**.
3. In the working area, right-click a recovery verification job and select **Statistics**. You can also double-click the job in the list.

The job session window displays statistics for all VMs that are started during the SureBackup job: VMs from the application group in the specified order and VMs from linked jobs. For your convenience, these VMs are marked with different icons.

After the verified VM is powered on, its name is displayed as a hyperlink. You can click the link to open the VM console to see what is happening inside the VM or perform manual testing.

If some VM fails to be verified automatically, you can start it manually when this VM is powered off. To start a VM, right-click the VM in the list and select **Start**. If the application group has already been powered off by that time, it will be started again. After that, you can open the VM console and perform verification and testing manually.

If you enabled malware scan at the [Settings step](#) of the SureBackup job wizard, you can view the detailed logging of the scan process. To view logs, click the **Scan Log** button that will appear at the bottom of the job session window after the scan is complete.



Creating SureBackup Session Reports

You can generate HTML reports with statistics on the SureBackup job. A report contains detailed data on job sessions: job status, start and end time, details of the session performance, status of verified VMs and test results. You can generate a report for the whole SureBackup job or a specific job session/sessions.

The SureBackup job report contains data on all sessions initiated for a specific job. To generate a SureBackup job report:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the SureBackup job and click **Report** on the ribbon. You can also right-click the SureBackup job and select **Report**.

The session report contains data on a single job session. To generate a session report:

1. Open the **History** view.
2. In the inventory pane, select **Jobs**.

- In the working area, select the session and click **Report** on the ribbon. You can also right-click the session and select **Report**.

SureBackup: Exchange SureBackup Job										
Session Details										
Status	Success	Start time	12/29/2018 2:03:30 PM	Details						
Total tasks	4	End time	12/29/2018 3:21:05 PM							
Processed tasks	4	Duration	1:17:34							
Successful tasks	4	Warning tasks	0							
Failed tasks	0	Skipped tasks	0							
Progress	100 %									
Virtual machines status										
VM name	Status	Start time	End time	Heartbeat test	Ping test	Custom script test	Validation test	Malware scan test		
dns01	Success	12/29/2018 2:03:31 PM	12/29/2018 3:19:48 PM	Success	Success	Disabled	Disabled	Disabled		
dc03	Success	12/29/2018 2:03:31 PM	12/29/2018 3:19:39 PM	Success	Success	Disabled	Disabled	Disabled		
exch01	Success	12/29/2018 2:03:31 PM	12/29/2018 3:19:28 PM	Success	Success	Disabled	Disabled	Disabled		
fileserv03	Success	12/29/2018 2:03:31 PM	12/29/2018 3:20:55 PM	Success	Success	Disabled	Success	Success		

XML Files with VM Roles Description

VM roles that you can assign to verified VMs and VMs from the application group are described in XML files. These XML files are stored in the %ProgramFiles%\Veeam\Backup and Replication\Backup\SbRoles folder on the backup server.

To add a new role, you must create a new XML file and save it to the SbRoles subfolder on the backup server. Do not save the XML file on the machine where the Veeam Backup & Replication console is installed – this will not affect the list of roles in Veeam Backup & Replication.

XML files describing VM roles have the following structure:

```
<SbRoleOptions>
  <Role>
    <SbRole>
      <Id>4CDC7CC4-A906-4de2-979B-E5F74C44832F</Id>
      <Name>Web Server</Name>
    </SbRole>
  </Role>
  <Options>
    <SbVerificationOptions>
      <ActualMemoryPercent>100</ActualMemoryPercent>
      <MaxBootTimeoutSec>300</MaxBootTimeoutSec>
      <AppInitDelaySec>120</AppInitDelaySec>
      <TestScripts>
        <TestScript>
          <Name>Web Server</Name>
          <Type>Predefined</Type>
          <TestScriptFilePath>Veeam.Backup.ConnectionTester.exe</TestScriptFilePath>
          <Arguments>%vm_ip% 80</Arguments>
        </TestScript>
      </TestScripts>
      <HeartbeatEnabled>True</HeartbeatEnabled>
      <PingEnabled>True</PingEnabled>
    </SbVerificationOptions>
  </Options>
</SbRoleOptions>
```

The XML file with the role description contains the following tags and parameters:

Tag	Required/Optional	Description
<SbRoleOptions>	Required	Encapsulates the VM role file.
<Role>	Required	Parent tag for a role assigned to a VM. <SbRole>, <Id> and <Name> are children of this tag.
<SbRole>	Required	Encapsulates basic information for a VM role: ID and name.
<Id>	Required	Unique identifier of a VM role.
<Name>	Required	Name of a VM role. The VM role name is displayed in the roles list on the Role tab.

<Options>	Required	Parent tag for startup and test script options to be used for the defined role. <SbVerificationOptions>, <ActualMemoryPercent>, <MaxBootTimeoutSec>, <AppInitDelaySec>, <TestScripts>, <Name>, <Type>, <TestScriptFilePath>, <Arguments>, <HeartbeatEnabled>, <PingEnabled> are children of this tag.
<SbVerificationOptions>	Required	Encapsulates options data for a VM role.
<ActualMemoryPercent>	Optional	Percent of the original memory level that must be pre-allocated to a verified VM on the system boot.
<MaxBootTimeoutSec>	Optional	Maximum allowed time to boot a VM.
<AppInitDelaySec>	Optional	Duration of time for which Veeam Backup & Replication must wait after the VM is successfully booted in the virtual lab. After this time elapses, Veeam Backup & Replication will run test scripts. Time is specified in seconds.
<TestScripts>	Optional	Encapsulates test script data for a VM role.
<Name>	Optional	Name of a VM role. The VM role name is displayed on the Test Scripts tab.
<Type>	Optional	Type of the test script: <i>Predefined</i> or <i>Custom</i> .
<TestScriptFilePath>	Optional	Path to an executable file of the test script to be performed. The path can be absolute or relative.
<Arguments>	Optional	Arguments to be passed to the script. You can use two variables: <ul style="list-style-type: none"> ▪ <i>%vm_ip%</i> - IP address of a verified VM. ▪ <i>%vm_fqdn%</i> - a fully qualified domain name of a verified VM. ▪ <i>%log_path%</i> - path to a log file to which verification results are stored.
<HeartbeatEnabled>	Required	Must a heartbeat test be enabled for this VM role: <i>True</i> or <i>False</i> .
<PingEnabled>	Required	Must a ping test be enabled for this VM role: <i>True</i> or <i>False</i> .

Manual Recovery Verification

Beside automatic recovery verification, you can perform manual verification of VM backups. Manual verification can be performed with all editions of Veeam Backup & Replication.

Boot Test

To perform a VM boot test, perform Instant VM Recovery for the verified VM. Power on the VM but do not connect the VM to the production network to avoid conflicts with the original VM.

Application Test

To perform an application test:

1. Create an isolated network.
2. Use the **Instant VM Recovery** wizard to restore the verified VM. At the **Ready to Apply** step of the wizard, clear the **Connect VM to network** check box.
3. When the VM is started, connect it to the isolated network.

The same procedure must be performed for all VMs that run applications on which the verified VM is dependent such as domain controller and DNS. All VMs must be connected to the same isolated network and started in the correct order: for example, DNS > domain controller > verified VM.

SureReplica

To guarantee recoverability of your data, Veeam Backup & Replication complements the SureBackup recovery verification technology with SureReplica.

SureReplica is in many respects similar to the SureBackup recovery verification. It lets you validate your DR environment without impacting the production infrastructure. You can automatically verify every created restore point of every VM replica and ensure that they are functioning as expected.

The SureReplica technology is not limited only to VM replica verification. Just like SureBackup, it provides the following capabilities:

- SureReplica: automated VM replica verification
- On-Demand Sandbox: an isolated environment for testing VM replicas, training and troubleshooting
- U-AIR: recovery of individual items from applications running on VM replicas

IMPORTANT!

The recovery verification functionality is available in the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication. If you use the Standard Edition, you can manually verify VM backups with Instant VM Recovery. For more information, see [Manual Recovery Verification](#).

How SureReplica Works

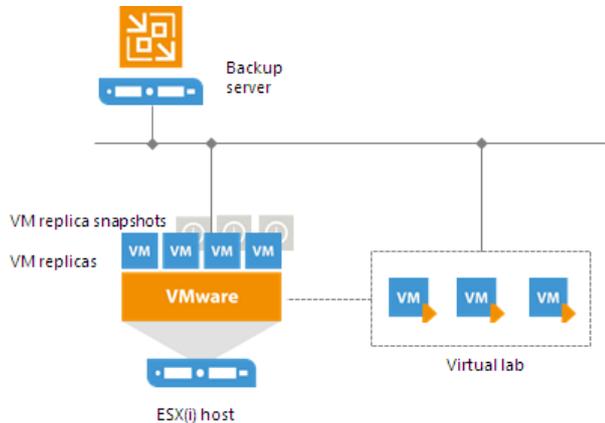
SureReplica is Veeam's technology that lets you test a VM replica for recoverability. To ensure that the VM replica is functioning properly, Veeam Backup & Replication performs its "live" verification. Veeam Backup & Replication automatically boots the VM replica from the necessary restore point in the isolated environment, performs tests against the VM replica, powers it off and creates a report on the VM replica state.

The SureReplica technology does not require the vPower engine. A VM replica is essentially an exact copy of a VM with a set of restore points. The VM replica data is stored in the raw decompressed format native to VMware. Therefore, to start a VM replica in the virtual lab, you do not need to present its data via the vPower NFS datastore to the ESX(i) host. Veeam Backup & Replication re-configures the VM replica settings for recovery verification, connects the VM replica to the isolated virtual lab and powers it on.

As there is no need to publish the VM from the backup file, the SureReplica processing is typically faster than SureBackup. Subsequently, the U-AIR and On-Demand Sandbox operations are faster, too.

During VM replica verification, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication triggers a VMware snapshot for a VM replica. The snapshot protects the VM replica from changes while it is running. All changes made to the VM replica are written to the delta file.
2. Veeam Backup & Replication starts the VM replica in the virtual lab.
3. Veeam Backup & Replication performs tests against the verified VM replica.
4. When the verification process is over, Veeam Backup & Replication removes the delta file of the VM replica snapshot, powers off the VM replica and creates a report on its state. The report is sent to the backup administrator by email.



NOTE:

Veeam Backup & Replication verifies only VM replicas in the *Normal* state. If a VM replica is in the *Failover* or *Failback* state, the verification process fails.

When Veeam Backup & Replication verifies the VM replica, it puts the VM replica to the *SureBackup* state. You cannot perform failback and failover operations for a VM replica in the *SureBackup* state until recovery verification or the U-AIR process is over and the VM replica returns to the *Normal* state.

To perform VM replica verification, you need to create the following objects:

1. **Application group.** During recovery verification, the VM replica is not started alone: it is started together with VMs on which the VM replica is dependent. Starting a VM replica in conjunction with other VMs enables full functionality of applications running inside the VM replica and lets you run these applications just like in the production environment.

2. [Virtual lab](#). The virtual lab is the isolated virtual environment in which the VM replica and VMs from the application group are started and tested.
3. [SureBackup job](#). The SureBackup job is a task for VM replica verification process. You can run the SureBackup job manually or schedule it to run automatically by schedule.

Replica Recovery Verification Tests

To verify a VM replica, Veeam Backup & Replication performs the same tests as for VM backup verification, except the backup validation test. You can run predefined tests or perform your own tests against VMs. The predefined tests include the following ones:

- Heartbeat test
- Ping test
- Application test

For more information, see [Backup Recovery Verification Tests](#).

Application Group

You can add to the same application groups both VMs from backups and VMs from replicas. Keep in mind that all VMs from the application group must have at least one valid restore point created by the time the SureBackup job starts.

For more information, see [Application Group](#).

Virtual Lab Configuration

Veeam Backup & Replication offers three types of the virtual lab configuration for VM replica verification:

- [Basic single-host virtual lab](#)
- [Advanced single-host virtual lab](#)
- [Advanced multi-host virtual lab](#)

Basic Single-Host Virtual Labs

The basic single-host virtual lab configuration can be used if your DR site is configured in the following way:

- All VM replicas that you want to verify are registered on the same ESX(i) host.
- All VM replicas that you want to verify are connected to the same network.

IMPORTANT!

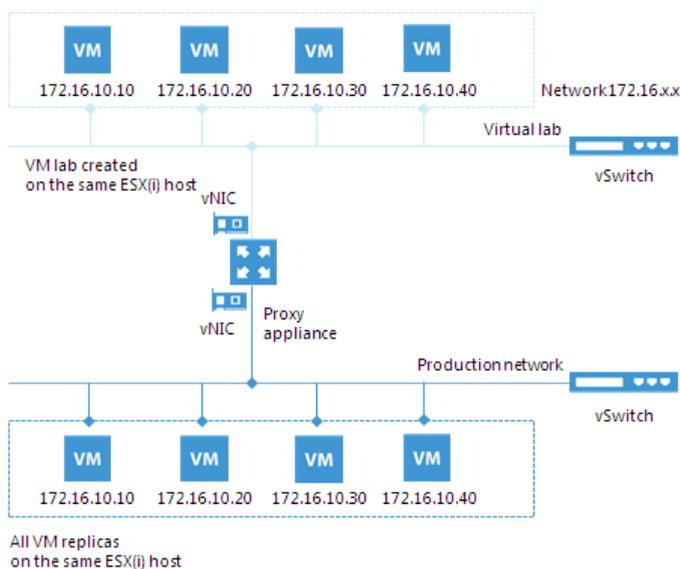
For this configuration type, the virtual lab must be created on the same ESX(i) host where VMs replicas are located. If you create the virtual lab on some other ESX(i) host, the SureBackup job will fail.

For the basic single-host virtual lab, Veeam Backup & Replication creates one virtual network that is mapped to the production network. Additionally, Veeam Backup & Replication automatically adds a number of new VMware objects on the ESX(i) host where the virtual lab is created:

- A resource pool
- A VM folder
- A standard vSwitch

The vSwitch is only used by the VMs started in the virtual lab. There is no routing outside the virtual lab to other networks.

Veeam Backup & Replication automatically configures all settings for the basic single-host virtual lab. The proxy appliance is also created and configured automatically and placed to the virtual lab folder and resource pool on the ESX(i) host.



Advanced Single-Host Virtual Labs

The advanced single-host virtual lab configuration can be used if your virtual environment is configured in the following way:

- All VM replicas that you want to verify are located on the same ESX(i) host.
- VM replicas you want to verify are connected to different networks.

IMPORTANT!

For this configuration type, the virtual lab must be created on the same ESX(i) host where VMs replicas are located. If you create the virtual lab on some other ESX(i) host, the SureBackup job will fail.

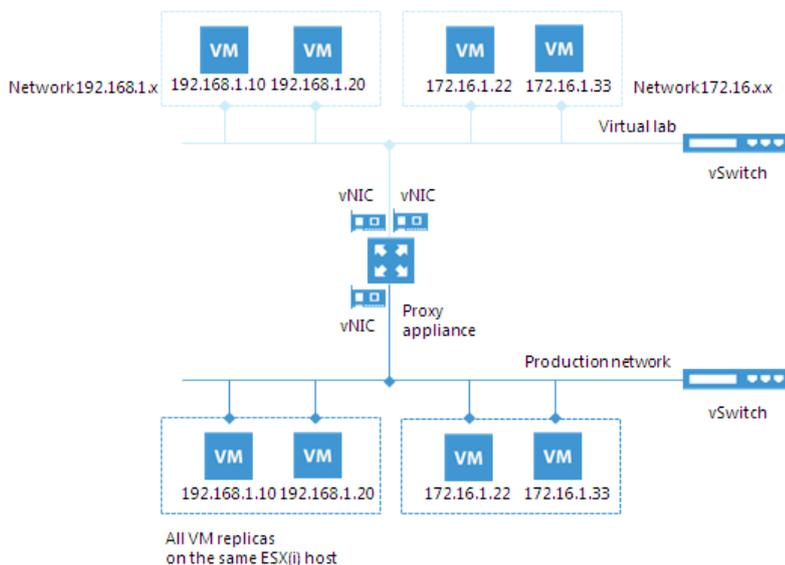
In the advanced single-host virtual lab, Veeam Backup & Replication creates several virtual networks. The number of virtual networks corresponds to the number of production networks to which verified VM replicas are connected. Networks in the virtual lab are mapped to corresponding production networks.

Veeam Backup & Replication automatically adds a number of new VMware objects on the ESX(i) host where the virtual lab is created:

- A resource pool
- A VM folder
- A standard vSwitch

The vSwitch is only used by the VMs started in the virtual lab. There is no routing outside the virtual lab to other networks.

When you create an advanced single-host virtual lab, Veeam Backup & Replication configures basic settings for networks that are created in the virtual lab. You need to review these settings and manually adjust them.

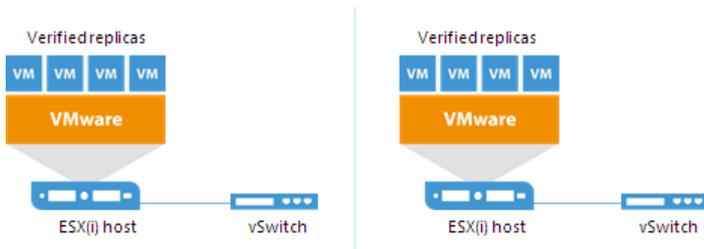


Limitations of Single-Host Virtual Labs

If VM replicas are located on different hosts, you cannot use the single-host virtual lab configuration (basic or advanced). A single-host virtual lab uses standard vSwitches that have specific configuration limitations.

When you create or edit a virtual lab, Veeam Backup & Replication creates a new port group for each isolated network in the virtual lab. All VMs in the isolated network are added to this port group. Such configuration helps differentiate the traffic passing through the standard vSwitch to the isolated network in the virtual lab.

However, the standard vSwitch has a restriction: it is “limited” to one ESX(i) host. A standard vSwitch is configured on a specific ESX(i) host. The configuration of the standard vSwitch, such as information about port groups, resides on the ESX(i) host where the vSwitch is configured. Other ESX(i) hosts in the virtual environment do not have access to this information.



For this reason, the single-host configuration can only be used if all VM replicas are registered on the same ESX(i) host. If attempt to verify VM replicas registered on different ESX(i) hosts in the single-host virtual lab, VMs from different port groups will not be able to “see” each other and communicate with each other.

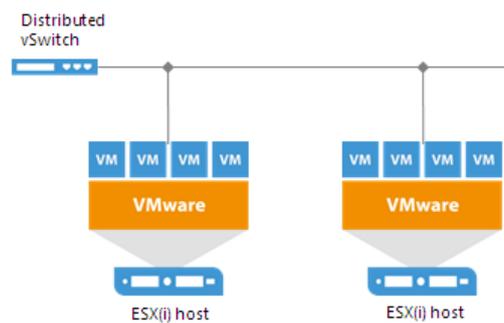
To overcome this limitation and verify VM replicas that are registered on different ESX(i) hosts, you can use [advanced multi-host virtual labs](#).

Advanced Multi-Host Virtual Labs

The advanced multi-host virtual lab configuration can be used if your DR site is configured in the following way:

- VM replicas that you want to verify are located on different ESX(i) hosts.
- VM replicas that you want to verify are connected to one or several networks.

The advanced multi-host virtual lab leverages the VMware Distributed vSwitch (DVS) technology. For more information, see <https://www.vmware.com/products/vsphere/distributed-switch.html>.



When you configure an advanced multi-host virtual lab, you must select an ESX(i) host on which the proxy server will be created and DVS on which Veeam Backup & Replication will create isolated networks.

Veeam Backup & Replication does not offer an option to automatically configure the DVS. The DVS must be preconfigured in your virtual environment.

IMPORTANT!

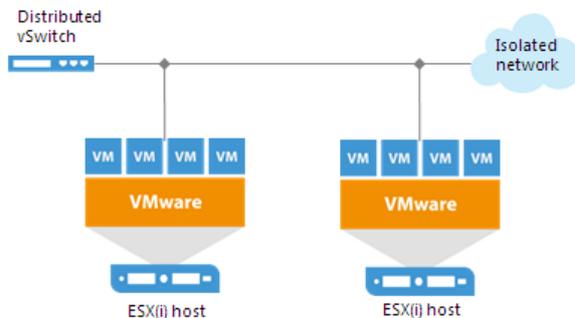
DVS is limited to one datacenter. For this reason, all verified VM replicas and VM replicas from the application group must belong to the same datacenter. If VM replicas belong to different datacenters, you will be able to start them in the virtual lab but Veeam Backup & Replication will not be able to automatically verify them.

Isolated Networks on DVS

For every isolated network in the virtual lab, Veeam Backup & Replication adds a new DVS port group to the DVS. The added port group is named after the isolated network.

The port groups created on the DVS must be isolated from the production environment. To isolate port groups, you can use one of the following methods:

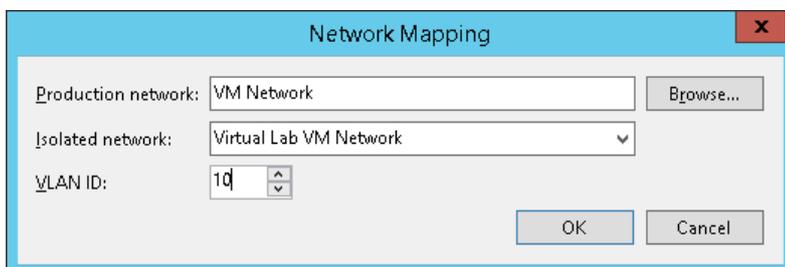
1. **Connect DVS uplinks to the isolated network.** You can link the DVS that you plan to use for recovery verification to an external isolated network using uplink adapters. This operation must be performed manually by the backup administrator.



2. **Use VLAN tagging.** This method can be used only if your router supports VLAN ID tagging. When you specify settings for isolated networks in the **New Virtual Lab** wizard, you can define different VLAN IDs for different isolated networks. Setting VLAN IDs restricts communication of VM replicas in the isolated network from the production environment.

IMPORTANT!

If your network does not support VLAN ID tagging or the virtual lab is configured incorrectly, VM replicas will be started in the virtual lab but Veeam Backup & Replication will not be able to automatically verify them.



Port Groups and VLAN IDs

You need to be extremely careful when specifying port group and VLAN ID settings for the advanced multi-host virtual lab.

Port Groups in Advanced Multi-Host Virtual Labs

For the advanced multi-host virtual lab, Veeam Backup & Replication uses an existing DVS that was configured by the backup administrator beforehand. Veeam Backup & Replication creates a number of new port groups on the DVS, one per isolated network in the virtual lab.

When Veeam Backup & Replication creates a new port group, it performs a check for the DVS selected for the virtual lab:

- If a port group with the specified name already exists, Veeam Backup & Replication starts using it for the virtual lab. However, in this case, Veeam Backup & Replication will not be the owner of this port group.
- If a port group with the specified name does not exist, Veeam Backup & Replication creates it and becomes the owner of the created port group.

When a virtual lab is removed, Veeam Backup & Replication checks the ownership of the port group:

- If Veeam Backup & Replication is not the owner of the port group, the port group remains on the DVS. Veeam Backup & Replication stops using it.
- If Veeam Backup & Replication is the owner of the port group, Veeam Backup & Replication removes this port group from the DVS.

Several virtual labs can use the same port group. For this reason, you should be extremely careful when removing virtual labs. If Veeam Backup & Replication is the owner of the virtual lab and the port group is removed, other virtual labs using this port group may fail to start.

VLAN IDs in Advanced Multi-Host Virtual Labs

A DVS port group has VLAN ID settings. If you select an existing port group for the virtual lab, you must specify its VLAN ID in the virtual lab settings.

- If VLAN ID settings are specified correctly, Veeam Backup & Replication will be able to configure the virtual lab and verify VM replicas in it.
- If VLAN ID settings are specified not correctly, Veeam Backup & Replication will report an error informing that the selected port group exists but cannot be used due to incorrect VLAN ID settings.

SureBackup Job for VM Replicas

You can verify VM replicas with the SureBackup job. The SureBackup job aggregates all settings and policies of a recovery verification task, such as application group and virtual lab to be used, VM replicas that must be verified in the virtual lab and so on. The SureBackup job can be run manually or scheduled to be performed automatically.

When a SureBackup job runs, Veeam Backup & Replication first creates an environment for VM replica verification:

1. Veeam Backup & Replication starts the virtual lab.
2. In the virtual lab, it starts VMs from the application group in the required order. VMs from the application group remain running until the verified VM replicas are booted and tested. If Veeam Backup & Replication does not find a successful VM replica or backup for any of VMs from the application group, the SureBackup job will fail.

When the virtual lab is ready, Veeam Backup & Replication starts VM replicas from the necessary restore point, tests and, depending on the specified settings, verifies them one by one or creates several streams and tests VM replicas simultaneously. If Veeam Backup & Replication does not find a successful restore point for any of verified VM replicas, verification of this VM replica fails, but the job continues to run.

By default, you can start and test up to three VM replicas at the same time. You can also increase the number of VMs to be started and tested simultaneously. Keep in mind that if these VMs are resource demanding, performance of the SureBackup job may decrease.

When the verification process is complete, VMs from the application group are powered off. Optionally, you can leave the VMs from the application group running to perform manual testing or enable user-directed application item-level recovery.

In some cases, the SureBackup job schedule may overlap the schedule of the replication job linked to it. The VM replica files may be locked by the replication job and the SureBackup job will be unable to verify such replica. In this situation, Veeam Backup & Replication will not start the SureBackup job until the replication job is over.

To overcome the situation of job overlapping, you may chain the replication and SureBackup jobs or define the timeout period for the SureBackup job. For more information, see [Specifying Job Schedule](#).

NOTE:

You can mix VM backups and replicas in the recovery verification job. For example, the application group may contain VMs that will be started from backup files and the job linked to the recovery verification job may be a replication job. Veeam Backup & Replication supports any type of a mixed scenario. Note that VMs that you verify with a SureBackup job must belong to the same platform – VMware or Hyper-V.

SureBackup Job for VM Replicas Processing

The recovery verification process for VM replicas includes the following steps:

1. **Getting virtual lab configuration.** Veeam Backup & Replication gets information about configuration of the virtual lab where verified VM replicas must be started.
2. **Starting virtual lab routing engine.** Veeam Backup & Replication starts a proxy appliance. The proxy appliance is used as a gateway that provides access to VM replicas the virtual lab.
3. **Publishing.** Veeam Backup & Replication triggers a protective VMware snapshot for the verified VM replica.

4. **Reconfiguring.** Veeam Backup & Replication updates configuration files of the VM replica to connect the VM replica to the isolated network in the virtual lab.
5. **Configuring DC.** If the VM replica has the Domain Controller or Global Catalog role, the VM replica is reconfigured.
6. **Powering on.** Veeam Backup & Replication powers on the VM replica in the isolated network.
7. **Heartbeat test.** Veeam Backup & Replication checks whether the green or yellow VMware Tools heartbeat signal is coming from the VM replica or not. If the VM replica has no VMware Tools, the test is not performed and a notification is written to the session details.
8. **Running ping tests.** Veeam Backup & Replication checks if the VM replica responds to the ping requests or not. If the VM replica has no NICs and mapped networks for them and/or has no VMware Tools installed, the ping test is not performed and a notification is written to the session details.
9. **Application initialization.** Veeam Backup & Replication waits for applications installed in the VM replica, for example, Microsoft SQL Server, to start. The application initialization period is defined in the properties of the SureBackup job and by default is equal to 120 sec. Depending on the software installed in a VM, the application initialization process may require more time than specified in the SureBackup job settings. If applications installed in a VM are not initialized within the specified period of time, test scripts can be completed with errors. If such error situation occurs, you need to increase the Application initialization timeout value and start the job once again.
10. **Running test scripts.** Veeam Backup & Replication runs scripts to test whether the application installed in the VM replica is working correctly or not. If the VM replica has no VMware Tools installed and/or there are no NICs and mapped networks for them, Veeam Backup & Replication skips tests that use variables %vm_ip% and %vm_fqdn%, as the IP address of the VM cannot be determined. Test results are written to the session details. To define whether the script has completed successfully or not, Veeam Backup & Replication uses return codes. If the return code is equal to 0, the script is considered to complete successfully. Other values in the return code mean that the script has failed.
11. **Powering off.** After all tests have been performed, Veeam Backup & Replication powers off the verified VM replica.
12. **Unpublishing.** Veeam Backup & Replication deletes the protective VMware snapshot and rolls back all changes made to the VM replica while it was running in the virtual lab.
13. **Stopping virtual lab engine.** Veeam Backup & Replication powers off the proxy appliance in the virtual lab.

Stabilization Algorithm

To perform tests for a VM replica without errors, Veeam Backup & Replication needs to know that the VM replica is ready for testing. To determine this, Veeam Backup & Replication waits for the VM replica to reach a "stabilization point": – the moment when the VM replica booted and reports it is ready for tests. After the stabilization point has been reached, Veeam Backup & Replication can start heartbeat tests, ping tests and test scripts against the VM replica.

Veeam Backup & Replication establishes the stabilization point with the help of VMware parameters that it gets from the VM replica. Depending on the VM replica configuration, it uses one of the three algorithms:

- **Stabilization by IP.** This algorithm is used if the VM replica has VMware Tools installed, there are NICs and mapped networks for these NICs. In this case, Veeam Backup & Replication waits for an IP address of the VM replica for mapped networks that is sent by VMware Tools running in the VM replica. The sent IP address must be valid and must not change for a specific period of time.
- **Stabilization by heartbeat.** This algorithm is used if the VM replica has VMware Tools installed but there are no NICs and mapped networks for them. In this case, Veeam Backup & Replication waits for the green or yellow heartbeat signal from VMware Tools installed inside the VM replica.

- Stabilization by Maximum allowed boot time. This algorithm is used if the VM replica has neither VMware Tools installed, nor NICs and mapped networks for them. In this case, Veeam Backup & Replication will wait for the time specified in the **Maximum allowed boot time** field, which is considered to be a stabilization period for the VM replica. Once this time interval is exceeded, Veeam Backup & Replication considers that the VM replica is successfully booted and is ready for testing.

Once the stabilization point has been established, Veeam Backup & Replication runs ping, heartbeat tests and test scripts against the verified VM replica.

The stabilization process cannot exceed the value specified in the **Maximum allowed boot time** field. If the stabilization point cannot be determined within the **Maximum allowed boot time**, the recovery verification process will be finished with the timeout error. For this reason, you should be careful when specifying this value. Typically, a VM replica started by a recovery verification job requires more time to boot than a VM started regularly. When such error situation occurs, you need to increase the **Maximum allowed boot time** value and start the job again.

On-Demand Sandbox

If you need to perform tests for production VMs, you can use an On-Demand Sandbox™. The On-Demand Sandbox is an isolated virtual environment where you can start one or more VMs from backups, VM replicas or VMs from storage snapshots. You can use the On-Demand Sandbox to perform the following tasks:

- Troubleshoot problems with VMs
- Test software patches and upgrades
- Install new software and so on

The On-Demand Sandbox uses a virtual lab – an isolated environment that is fully fenced off from the production environment. VMs started in the virtual lab remain in the read-only state. All changes made to VMs are written to redo logs (for VM backups and storage snapshots) or saved to delta files (for VM replicas). Redo logs and delta files are deleted after you finish working with the On-Demand Sandbox and power it off.

To create the On-Demand Sandbox, you must configure the following objects:

- Virtual lab in which VMs will be started. For more information, see [Virtual Lab](#).
- Application group. The application group must include all VMs and/or VM replicas that you want to start in the On-Demand Sandbox. This can be one VM or a group of VMs that work together. For more information, see [Application Group](#).
- SureBackup job. The virtual lab and application group must be linked to this job. For more information, see [SureBackup Job](#).

On-Demand Sandbox for Storage Snapshots

In the On-Demand Sandbox, you can start VMs from snapshots existing on the production storage array. You can use the On-Demand Sandbox to test VMs, troubleshoot issues, perform training and so on.

Veeam Backup & Replication offers the On-Demand Sandbox functionality for the following storage systems:

- Dell EMC VNX(e)\Unity
- HPE 3PAR StoreServ, including secondary volumes – HPE 3PAR Peer Persistence
- HPE StoreVirtual P4000 series and HPE StoreVirtual VSA (Virtual Storage Appliance)
- IBM Spectrum Virtualize, including secondary IBM volumes – IBM Spectrum Virtualize HyperSwap
- NetApp, including secondary arrays – NetApp SnapMirror and NetApp SnapVault
- HPE Nimble storage, including secondary arrays – Nimble Snapshot Replicated Copy
- Universal Storage API Integrated Systems

Configuration of the On-Demand Sandbox in which VMs from storage snapshots are started is similar to configuration of the regular On-Demand Sandbox. To start a VM from the storage snapshot in the isolated environment, you must configure the following objects:

- **Virtual lab.** The virtual lab must mirror the networking scheme of the production environment. You can configure a new virtual lab or use an existing virtual lab. Any type of the virtual lab configuration is supported: basic single-host, advanced single-host or advanced multi-host. For more information, see [Virtual Lab](#).
- **Application group.** The application group must contain one or several VMs that you want to start in the On-Demand Sandbox. You can select VMs from volumes or LUNs on the storage system. During the SureBackup job, Veeam Backup & Replication will detect the latest snapshot for this volume or LUN and start the VM from this snapshot. For more information, see [Application Group](#).
- **SureBackup job.** You must link the application group with VMs and virtual lab to the SureBackup job. For more information, see [SureBackup Job](#).

How On-Demand Sandbox for Storage Snapshots Works

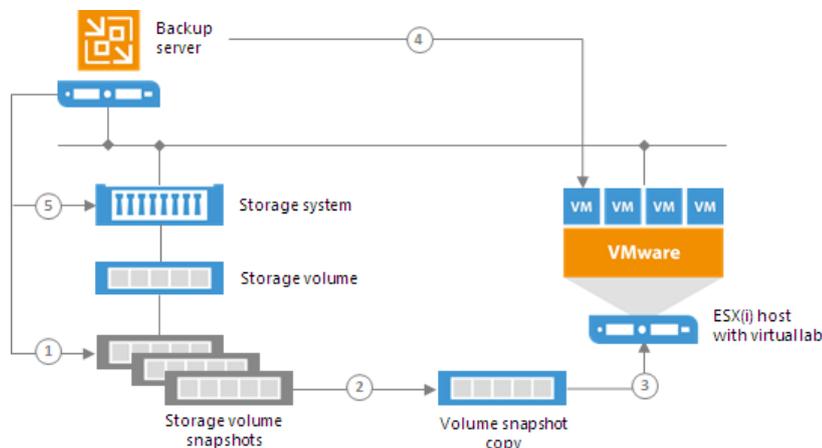
To start a VM from the storage snapshot in the On-Demand Sandbox, Veeam Backup & Replication needs to present this storage snapshot to an ESX(i) host as a datastore. To do this, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication detects the latest storage snapshot for the VM whose disks are located on the storage system.
2. Veeam Backup & Replication triggers the storage system to create a copy of the storage snapshot. The snapshot copy helps protect the storage snapshot from changes.

To create a snapshot copy, Veeam Backup & Replication uses the same technology as for Veeam Explorer from Storage Snapshots. The technology choice depends on licenses installed on the storage system. For more information, see [Veeam Explorer for Storage Snapshots](#).

3. The snapshot copy is presented as a new datastore to the ESX(i) host on which the virtual lab is registered.

4. Veeam Backup & Replication performs regular operations required for On-Demand Sandbox: reconfigures the VMX file, starts the VM, performs necessary tests for it and so on.
5. After you finish working with VMs and power off the On-Demand Sandbox, Veeam Backup & Replication performs cleanup operations: powers off the VM and the proxy appliance in the virtual lab, unmounts the datastore from the ESX(i) host and triggers the storage system to remove the snapshot copy.



Number of Mounted NFS Datastores

You can add to the application group several VMs that reside on different storage snapshots. In this case, Veeam Backup & Replication will trigger several snapshot copies (one per each storage snapshot) and present the equal number of datastores to the ESX(i) host.

The number of NFS datastores that can be mounted to the ESX(i) host is limited by VMware vSphere. If number of snapshot copies is great, Veeam Backup & Replication may fail to present all of them as datastores to the ESX(i) host. In this case, VMs in the application group will not be started and the SureBackup job will fail. For more information about limitations, see

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2239.

To overcome this situation, Veeam Backup & Replication offers the mechanism of the snapshot copy re-mounting:

1. If Veeam Backup & Replication detects that there are not enough resources to mount a datastore, it displays a warning and offers you to free up resources on the ESX(i) host.
2. During the next 20 minutes, Veeam Backup & Replication attempts to mount the datastore with the time interval of 2 minutes.
3. If resources are freed and Veeam Backup & Replication manages to mount the datastore, VMs in the application group are started and the SureBackup job continues to run. If resources on the ESX(i) hosts are not freed within 20 minutes, the SureBackup job fails.

Limitations for On-Demand Sandbox for Storage Snapshots

Before you start using On-Demand Sandbox for storage snapshots, check limitations for Veeam Explorer for Storage Snapshots. For more information, see [General Limitations](#).

Mixed Scenarios

You can start VMs from different sources in the On-Demand Sandbox:

- VM backups
- VM replicas
- VMs from storage snapshots

For example, you can add VMs from backups and VMs from storage snapshots to the same application group and link a replication job to the SureBackup job.

You cannot link jobs that trigger snapshots on storage arrays to the SureBackup job. This option is not supported.

Type of Job/Object	SureBackup	SureReplica	SureSnap
Application group			
Linked job			

Configuring On-Demand Sandbox

To configure the On-Demand Sandbox, perform the following steps:

1. Configure a virtual lab in which you plan to start VMs. For more information, see [Creating Virtual Lab](#).
2. Configure an application group. The application group must contain all VMs that you plan to start in the On-Demand Sandbox and all VMs on which these VMs are dependent. For more information, see [Creating Application Group](#).
3. Configure a SureBackup job:
 - a. Launch the **New SureBackup Job** wizard.
 - b. At the **Virtual Lab** step of the wizard, select the configured virtual lab.
 - c. At the **Application Group** step of the wizard, select the configured application group.
 - d. Select the **Keep the application group running after the job completes** check box.
 - e. Configure other job settings as required and save the job settings.

New SureBackup Job

Application Group
Choose the application group for this job and verify that all required backups are available.

Name
Virtual Lab
Application Group
Linked Jobs
Settings
Schedule
Summary

Application group:
Exchange Application Group
VM Group for Microsoft Exchange Verification

Application group info:

VM	Role	Source	Source Status
dns01	DNS Server	Backup	OK (less tha...
dc03	Domain Controller...	Backup	OK (less tha...

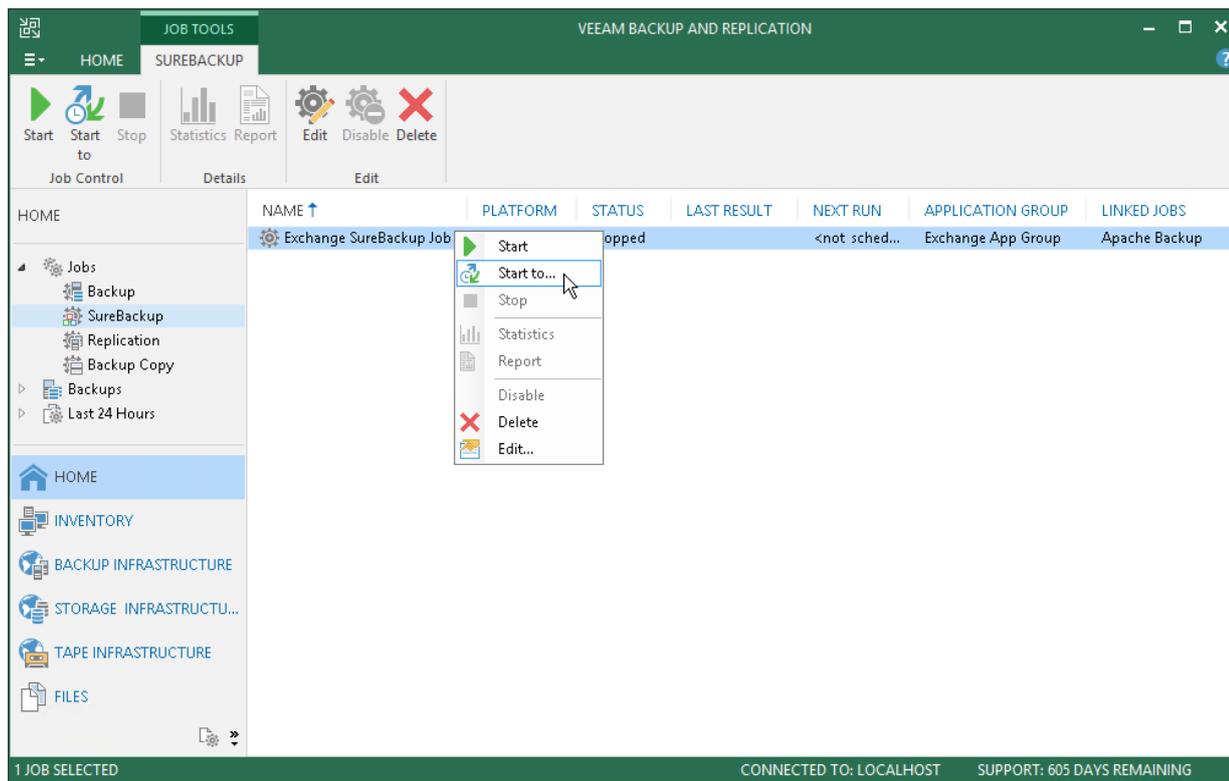
Keep the application group running after the job completes
This option enables performing additional manual verification, or user-directed application item recovery for virtual machines in this application group.

< Previous Next > Finish Cancel

To start VMs in the On-Demand Sandbox, run the SureBackup job:

1. Open the **Home** view.
2. In the inventory pane, select **SureBackup**.
3. In the working area, right-click the configured SureBackup job and select **Start** or **Start to**.

Veeam Backup & Replication will start the virtual lab and power on VMs from the application group in the virtual lab. You will be able to connect to VMs and perform tests for them.



Data Recovery

Veeam Backup & Replication offers a number of recovery options for various disaster recovery scenarios:

- [Instant VM Recovery](#) enables you to instantly start a VM directly from a backup file.
- [Entire VM recovery](#) enables you to recover a VM from a backup file to its original or another location.
- [VM files restore](#) enables you to recover separate VM files (virtual disks, configuration files and so on).
- [Virtual disks restore](#) enables you to recover a specific hard drive of a VM from the backup file, and attach it to the original VM or to a new VM.
- [Guest OS File Recovery](#) enables you to recover individual guest OS files from Windows, Linux, Mac and other guest OS file systems.

Veeam Backup & Replication uses the same image-level backup for all data recovery operations. You can restore VMs, VM files and drives, application items and individual guest OS files to the most recent state or to any available restore point.

To view and recover Microsoft Active Directory, Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange or Oracle application items, you can use the capabilities of Veeam Backup Explorers. For more information, see [Veeam Backup Explorers User Guide](#).

To restore VMware VM data directly from storage snapshots, you can use the capabilities of Veeam Explorer for Storage Snapshots. For more information, see [Veeam Explorer for Storage Snapshots](#).

NOTE:

Veeam Backup & Replication provides backward compatibility: backups created with previous product versions can be restored with later product versions.

Instant VM Recovery

With Instant VM Recovery, you can immediately restore a VM into your production environment by running it directly from the backup file. Instant VM recovery helps improve recovery time objectives (RTO), minimize disruption and downtime of production VMs. It is like having a "temporary spare" for a VM: users remain productive while you can troubleshoot an issue with the failed VM.

When Instant VM Recovery is performed, Veeam Backup & Replication uses the Veeam vPower technology to mount a VM image to an ESX(i) host directly from a compressed and deduplicated backup file. Since there is no need to extract the VM from the backup file and copy it to production storage, you can restore a VM from any restore point (incremental or full) in a matter of minutes.

The archived image of the VM remains in read-only state to avoid unexpected modifications. By default, all changes to virtual disks that take place while the VM is running are logged to auxiliary redo log files residing on the NFS server (backup server or backup repository). These changes are discarded as soon as a restored VM is removed, or merged with the original VM data when VM recovery is finalized.

To improve I/O performance for a restored VM, you can redirect VM changes to a specific datastore. In this case, instead of using redo logs, Veeam Backup & Replication will trigger a snapshot and put it to the *Veeam IR* directory on the selected datastore, together with metadata files holding changes to the VM image. Redirecting VM changes improves recovery performance but makes Storage vMotion not possible for ESX 4.x and earlier. As a result, you will not be able to use Storage vMotion to finalize Instant VM Recovery.

To finalize Instant VM Recovery, you can do one of the following:

- Use Storage vMotion to quickly migrate the restored VM to the production storage without any downtime. In this case, original VM data will be pulled from the NFS datastore to the production storage and consolidated with VM changes while the VM is still running. Storage vMotion, however, can only be used if you select to keep VM changes on the NFS datastore without redirecting them. Note that Storage vMotion is only available with select VMware licenses.
- Use replication or VM copy functionality of Veeam Backup & Replication. In this case, you can create a copy of a VM and fail over to it during the next maintenance window. In contrast to Storage vMotion, this approach requires you to schedule some downtime while you clone or replicate the VM, power it off and then power the cloned copy or replica on.
- Use Quick Migration. In this case, Veeam Backup & Replication will perform a two-stage migration procedure – instead of pulling data from the vPower NFS datastore, it will restore the VM from the backup file on the production server, then move all changes and consolidate them with the VM data. For details, see [Quick Migration](#).

In many respects, Instant VM Recovery gives results similar to failover of a VM replica. Both features can be used for tier-1 applications with little tolerance for business interruption and downtime. However, when you perform replica failover, you do not have dependencies on the backup server. And, unlike Instant VM Recovery that provides only limited I/O throughput, replication guarantees full I/O performance.

Beside disaster recovery matters, Instant VM Recovery can also be used for testing purposes. Instead of extracting VM images to production storage to perform regular DR testing, you can run a VM directly from the backup file, boot it and make sure the VM guest OS and applications are functioning properly.

Performing Instant VM Recovery

With Instant VM Recovery, you can immediately start a VM from a backup file stored on the backup repository. Instant VM Recovery accelerates the restore process, allows you to improve RTOs and decrease downtime of production VMs.

Before starting Instant VM Recovery, [check prerequisites](#). Then use the **Instant VM Recovery** wizard to recover the necessary VM.

Before You Begin

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

- You can restore a machine from a backup that has at least one successfully created restore point.
- If you restore a machine to the production network, make sure that the original machine is powered off to avoid conflicts.
- If you want to scan machine data for viruses, check the [secure restore requirements and limitations](#).
- You must have at least 10 GB of free disk space on the vPower NFS datastore to store virtual disk updates for the restored VM.

By default, Veeam Backup & Replication writes virtual disk updates to the *NfsDatastore* folder on a volume with the maximum amount of free space, for example, `C:\ProgramData\Veeam\Backup\NfsDatastore`. The vPower cache is not used when you choose to redirect virtual disk updates to a VMware vSphere datastore in the **Instant VM Recovery** wizard.

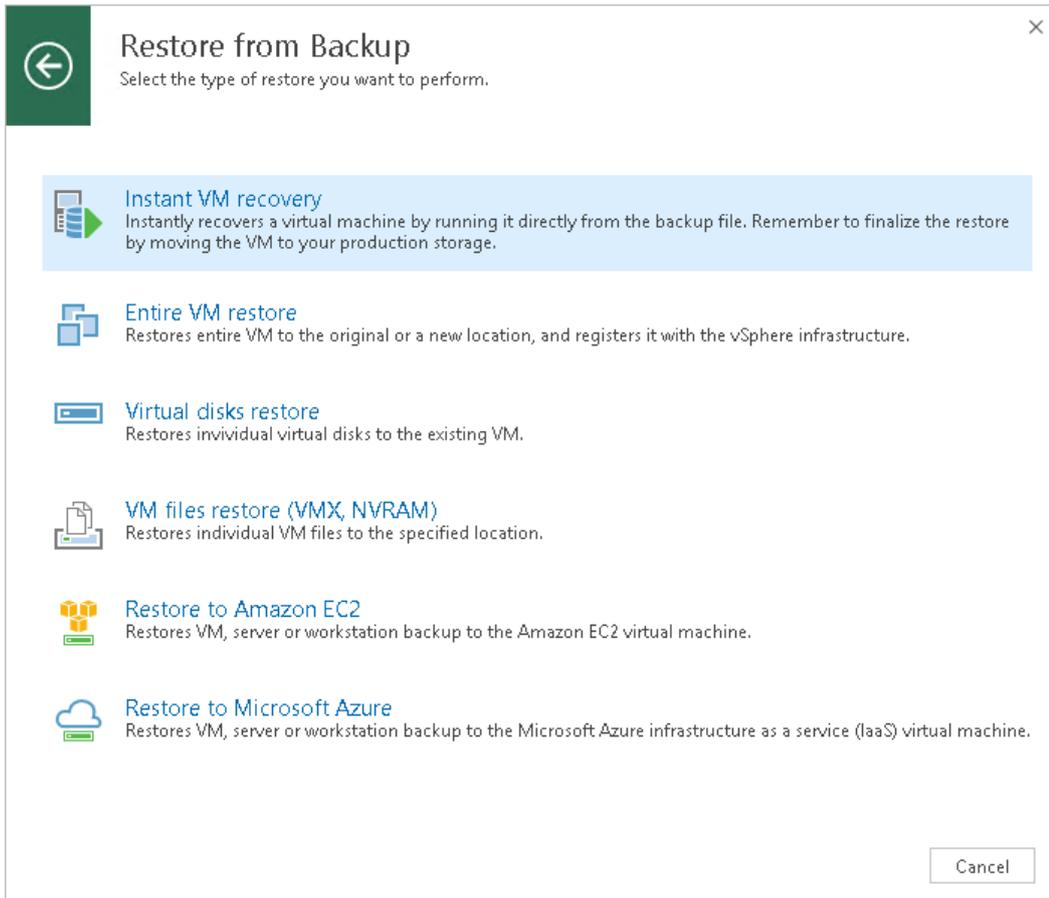
- Finalizing Instant VM Recovery using Veeam Quick Migration with Smart Switch requires at least the amount of instantly recovered VM RAM settings plus 200 MB of free disk space in vPower NFS cache location to suspend the VM state to disk. For example, if the restored VM has 32 GB of virtual RAM, 32.2 GB of free space is required. This is not a requirement when you are using vSphere Storage vMotion instead.

Step 1. Launch Instant VM Recovery Wizard

To launch the **Instant VM Recovery** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from backup > Entire VM restore > Instant VM recovery**.
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Select the VM that you want to restore and click **Instant VM Recovery** on the ribbon.

- o Right-click the VM that you want to restore and select **Instant VM recovery**.



Step 2. Select VMs

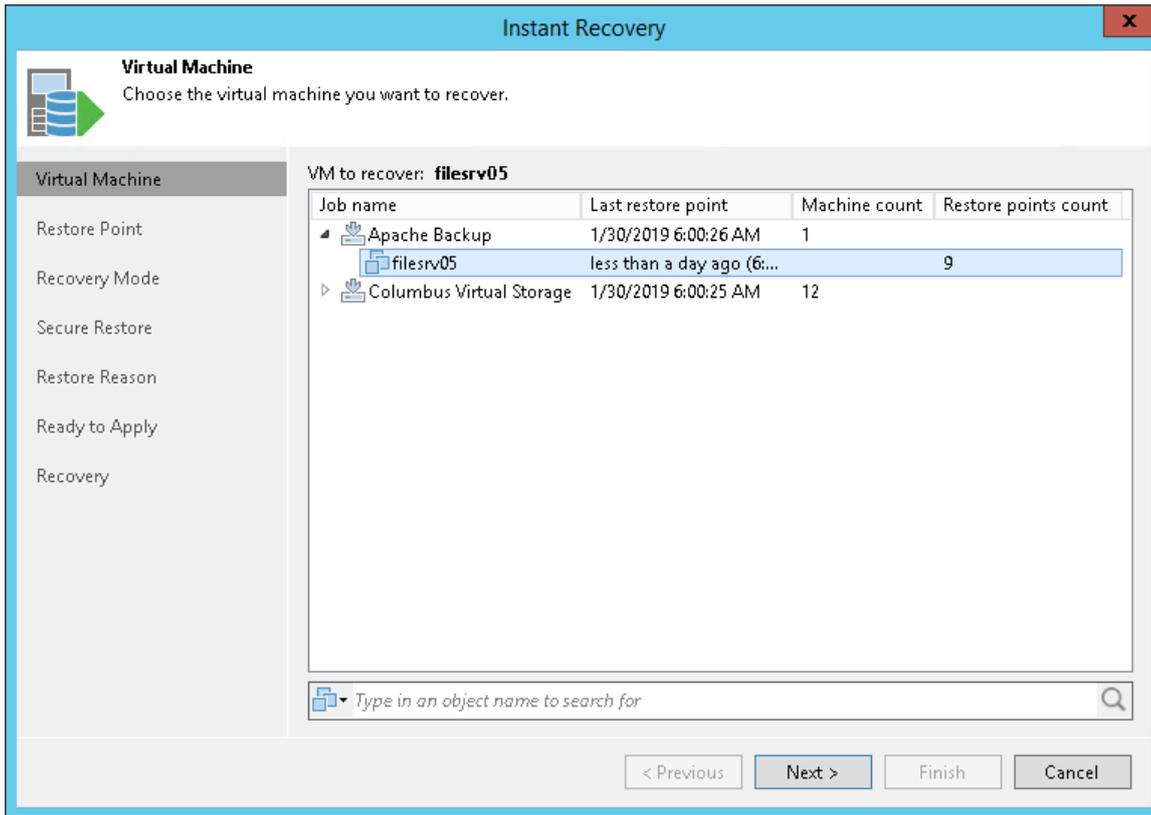
At the **Virtual Machine** step of the wizard, select the VM that you want to recover:

1. In the **VM to recover** list, expand the backup job.
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.

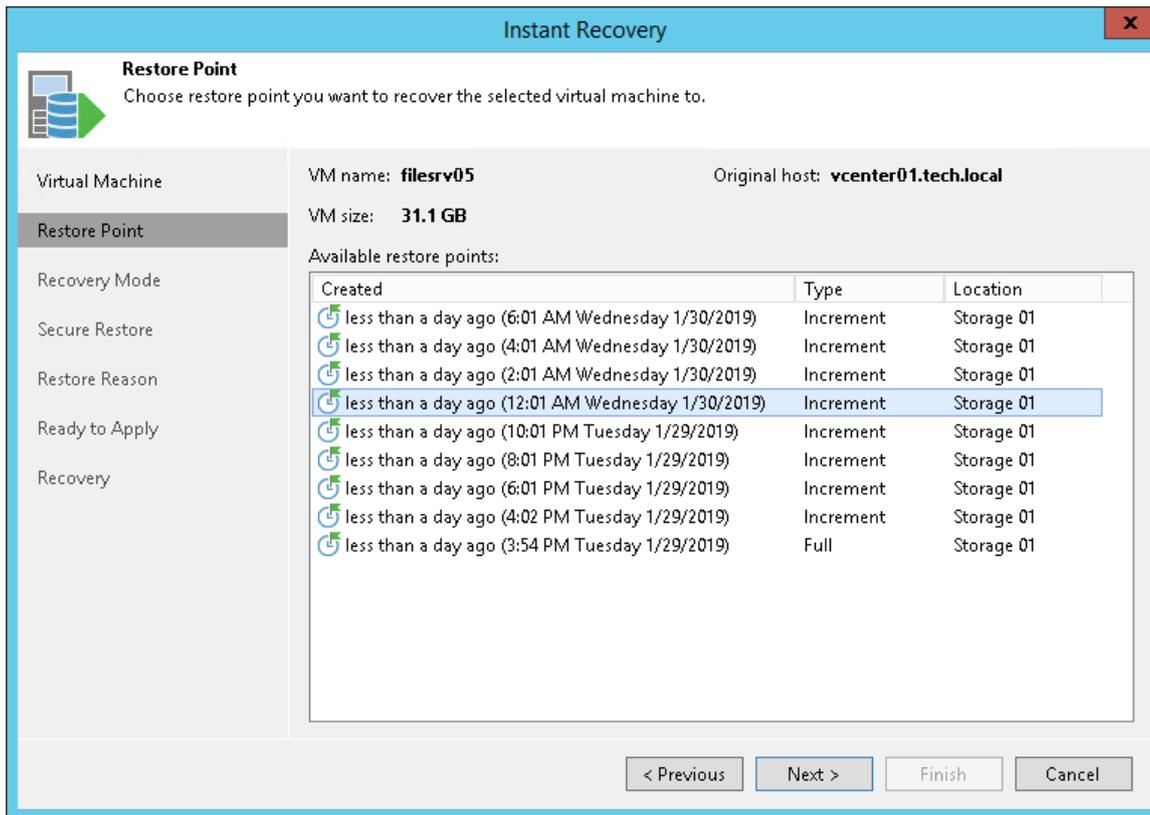
2. Click the **Start search** button on the right or press [ENTER].



Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point for the VM.

In the **Location** column, you can view a name of a backup repository or object storage repository where a restore point resides.



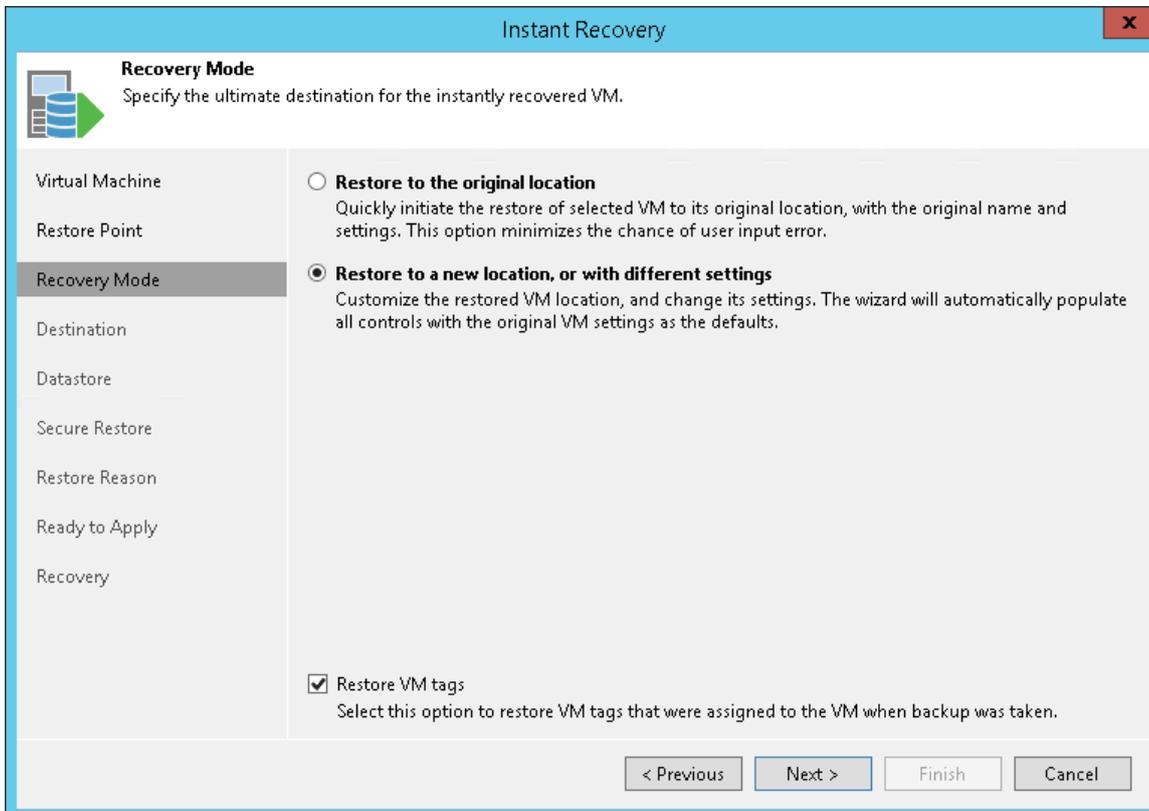
Step 4. Select Recovery Mode

At the **Recovery Mode** of the wizard, choose the necessary restore mode.

1. Choose a restore mode:
 - o 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 [Reason step](#) of the wizard.
 - o 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, format of restored virtual disks and so on). If this option is selected, the **Instant Recovery** 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. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:
 - o The VM is restored to its original location.
 - o The original VM tag is still available on the source vCenter Server.

IMPORTANT!

If you recover a VM with original settings, and the original VM still exists in the virtual infrastructure, the original VM will be removed.



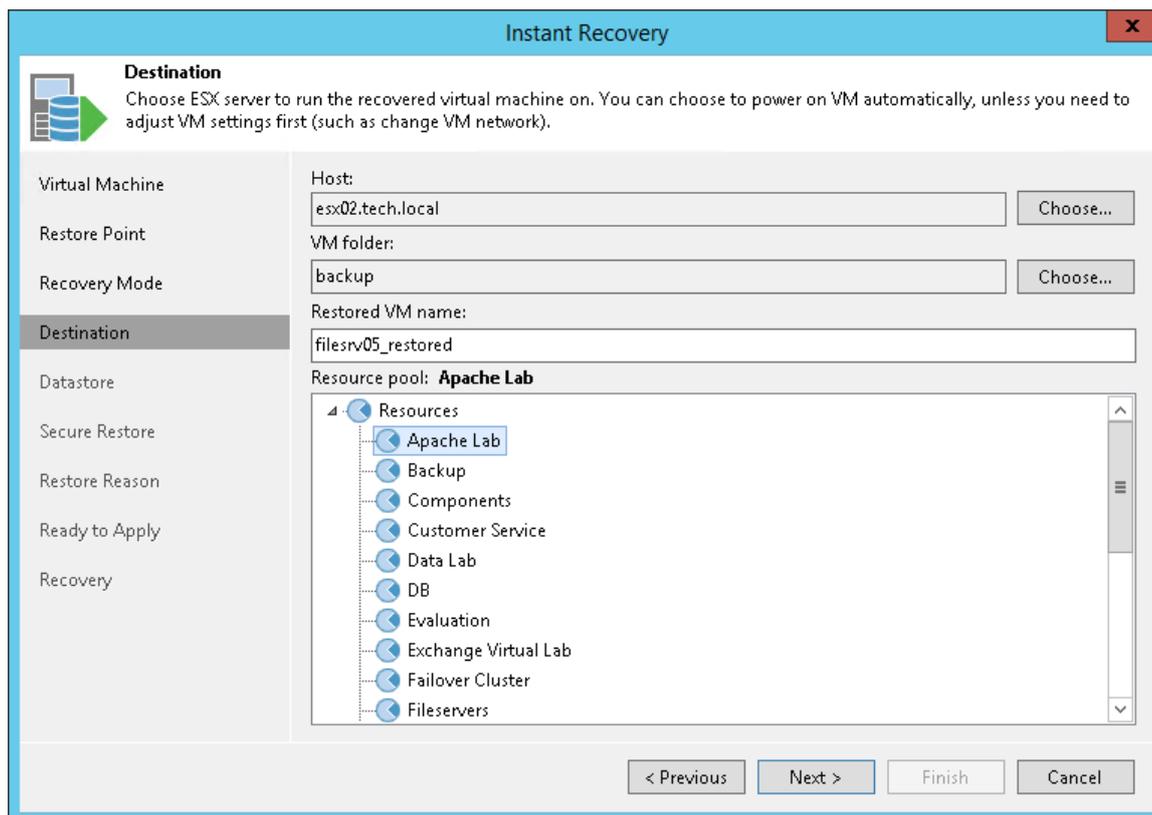
Step 5. Select Destination for Restored VM

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 restored VM:

1. In the **Host** field, specify a host on which the VM must run.
2. In the **VM folder** field, specify a folder to which the restored VM must be placed.
3. In the **Restored VM name** field, enter a name under which the VM must be restored and registered. By default, the restored VM has the name of the original 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 VM must be placed.



Step 6. Select Destination for Virtual Disk Updates

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

At the **Datastore** step of the wizard, you can select where redo logs must be written when the VM is running from the backup. By default, redo logs are stored directly on the backup server. However, you can store redo logs on any datastore in the virtual environment. Redirecting redo logs improves recovery performance but makes Storage vMotion not possible for ESX(i) 5.x and earlier.

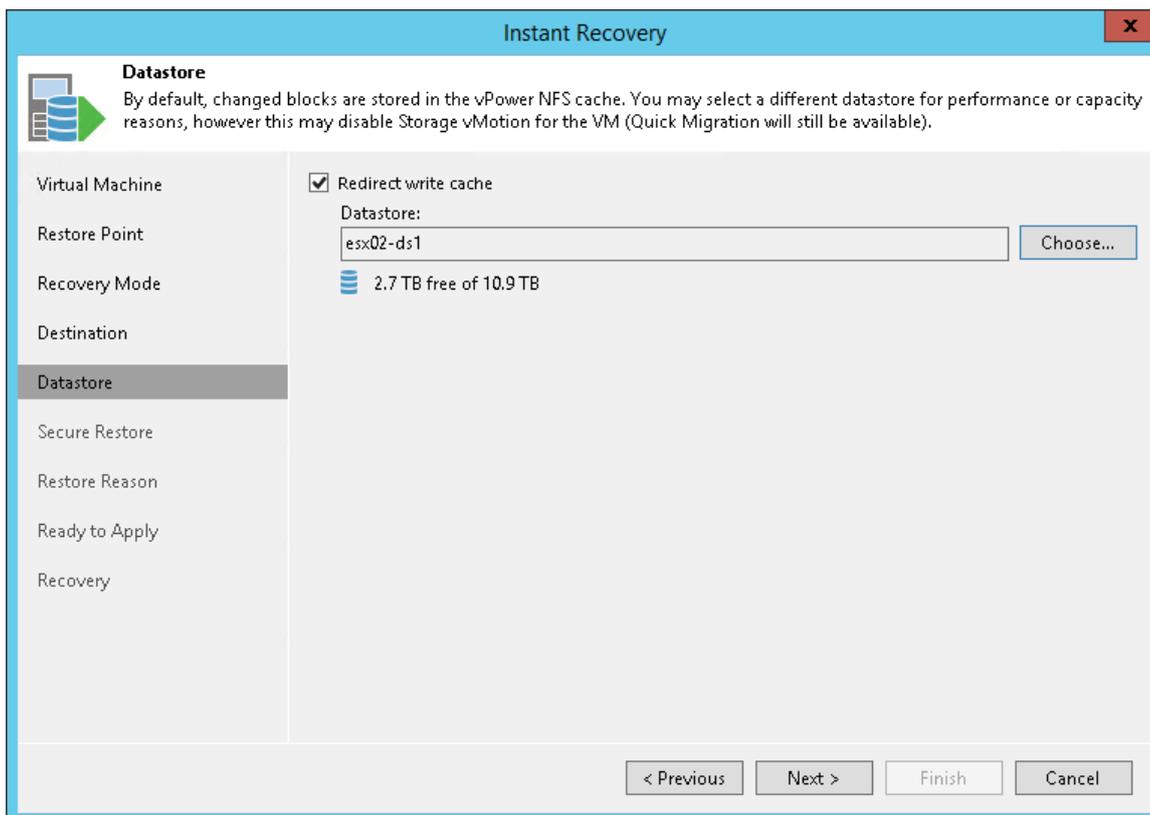
To redirect redo logs:

1. Select the **Redirect virtual disk updates** check box.
2. Select a datastore from the list.

IMPORTANT!

Consider the following:

- If you plan to migrate the recovered VM to the same datastore which is used as the destination for redirecting virtual disk updates, Veeam Backup & Replication will automatically switch to Veeam Quick Migration instead of using Storage vMotion. The described behavior is implemented to prevent data loss due to a bug in VMware Storage vMotion. Note that using Veeam Quick Migration will cause minimal VM downtime.
- If disks of a restored VM are greater than 2 TB, you must not place redo logs on a VSAN datastore. Otherwise, Veeam Backup & Replication will fail to create a snapshot for the restored VM. For more information, see [VMware Docs](#).



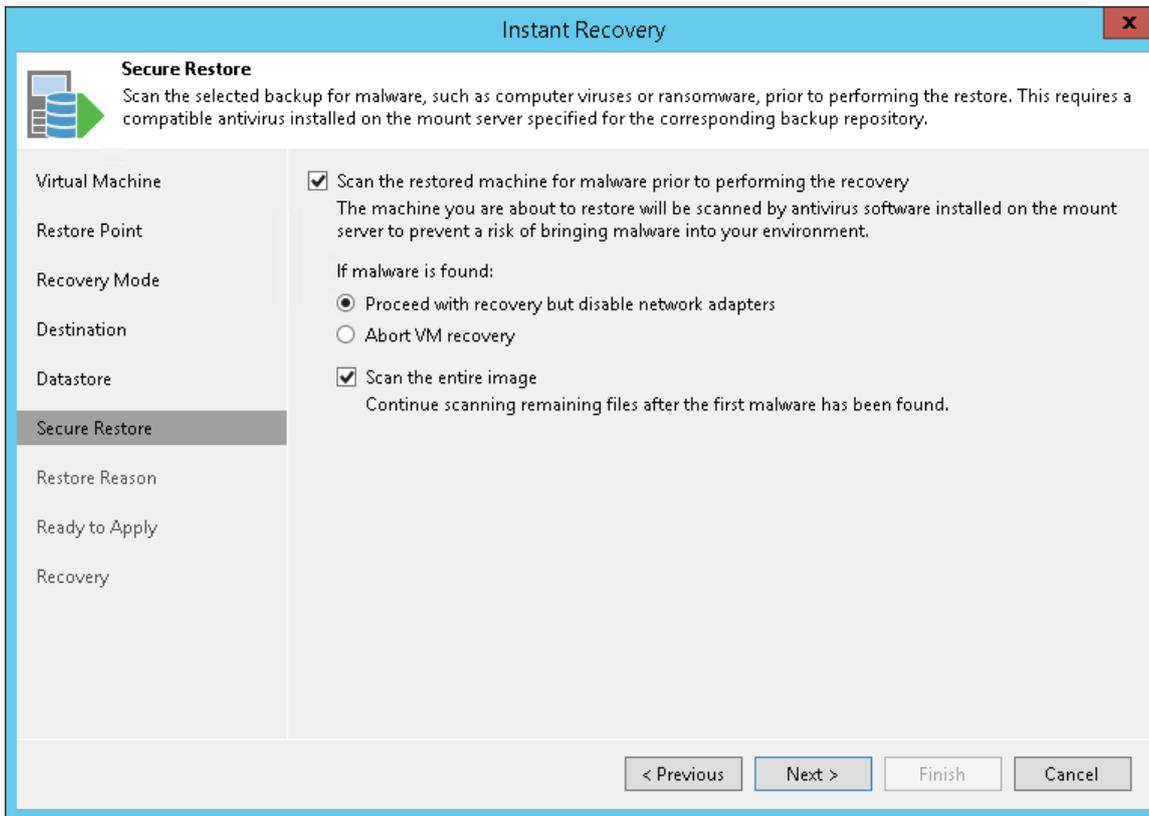
Step 7. Specify Secure Restore Settings

You can instruct Veeam Backup & Replication to perform secure restore – scan machine data with antivirus software before restoring the machine to the production environment. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

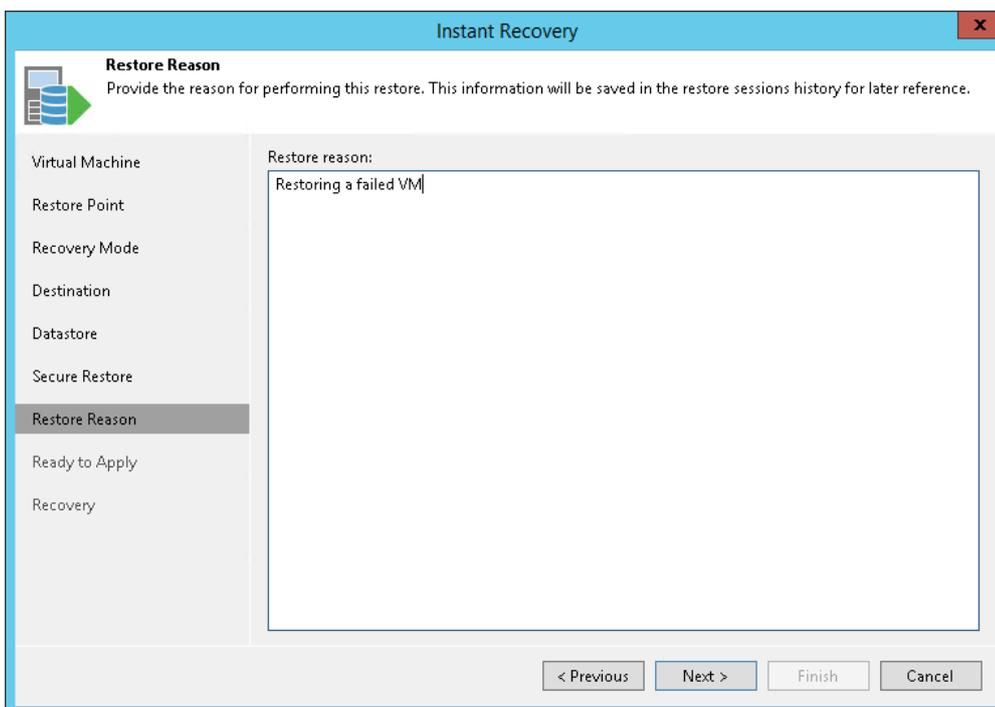
1. At the **Secure Restore** step of the wizard, select the **Scan the restored machine for malware prior to performing the recovery** check box.
2. Select which action Veeam Backup & Replication will take if the antivirus finds a virus threat:
 - **Proceed with recovery but disable network adapters.** Select this action if you want to restore the machine with disabled network adapters (NICs).
 - **Abort VM recovery.** Select this action if you want to cancel the restore session.

3. Select the **Scan the entire image** check box if you want the antivirus to continue the machine data scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).



Step 8. Specify Restore Reason

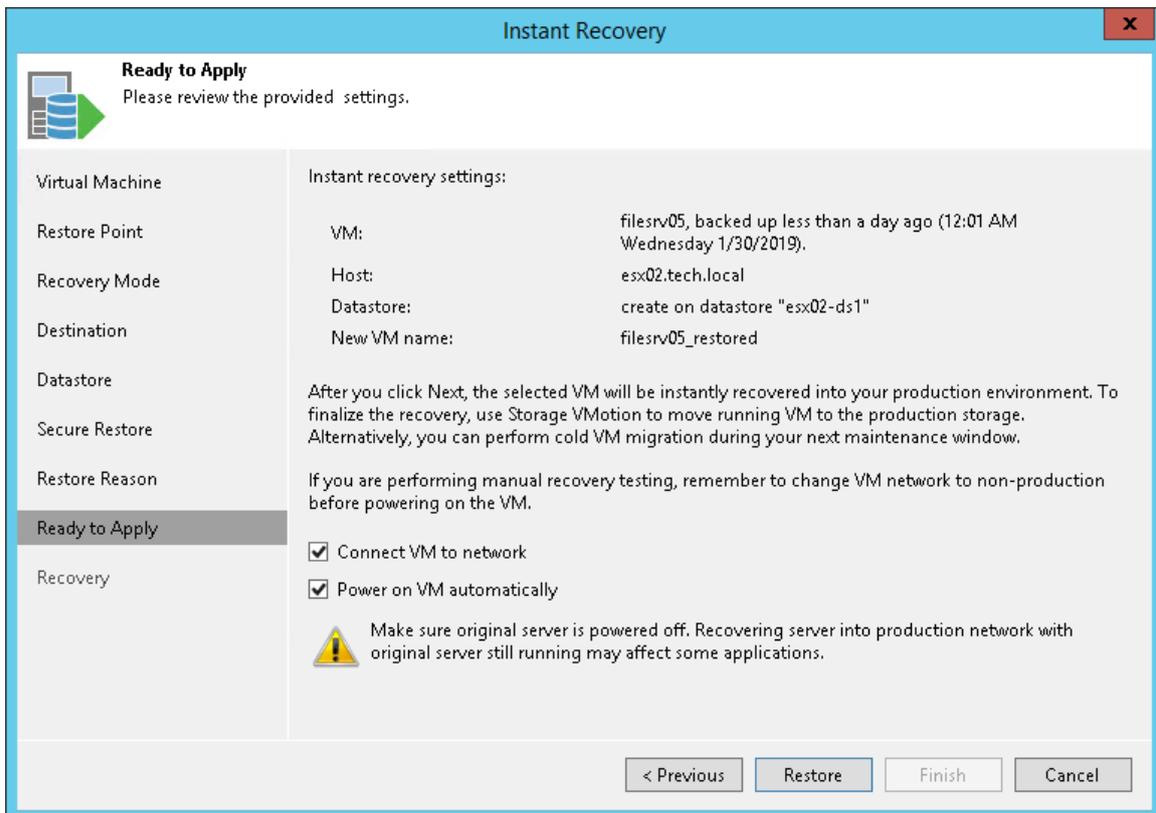
At the **Restore Reason** step of the wizard, enter a reason for performing Instant VM Recovery for the VM. The information you provide will be saved in the session history and you can reference it later.



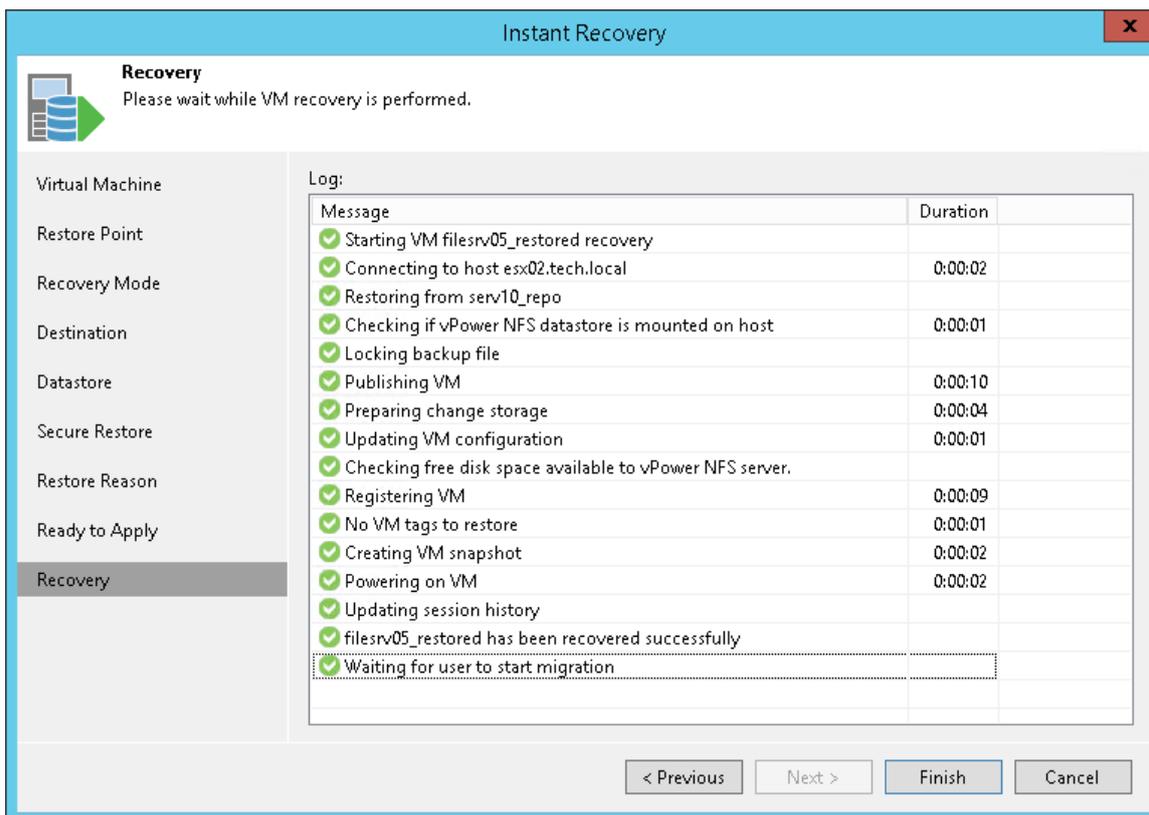
Step 9. Verify Instant VM Recovery Settings

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 while the initial VM is still running, leave this check box not selected. Before you power on such VM, you will have to manually change VM network settings: disconnect the VM from the production network and connect it to an isolated non-production network to avoid conflicts.
2. To start a 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 settings you have specified for Instant VM Recovery and click **Restore**. Veeam Backup & Replication will recover the VM on the selected ESX(i) host.



4. Wait for Veeam Backup & Replication to publish the VM on the host and click **Finish**.



Step 10. Finalize Instant VM Recovery

After the VM has been successfully published, you can test the VM and migrate it to production. After the migration, if you don't need the recovery source files anymore, you can unpublish the recovered VM.

- [Test the recovered VM before migrating to production](#)
- [Migrate the recovered VM to the production environment](#)
- [Unpublish the recovered VM](#)

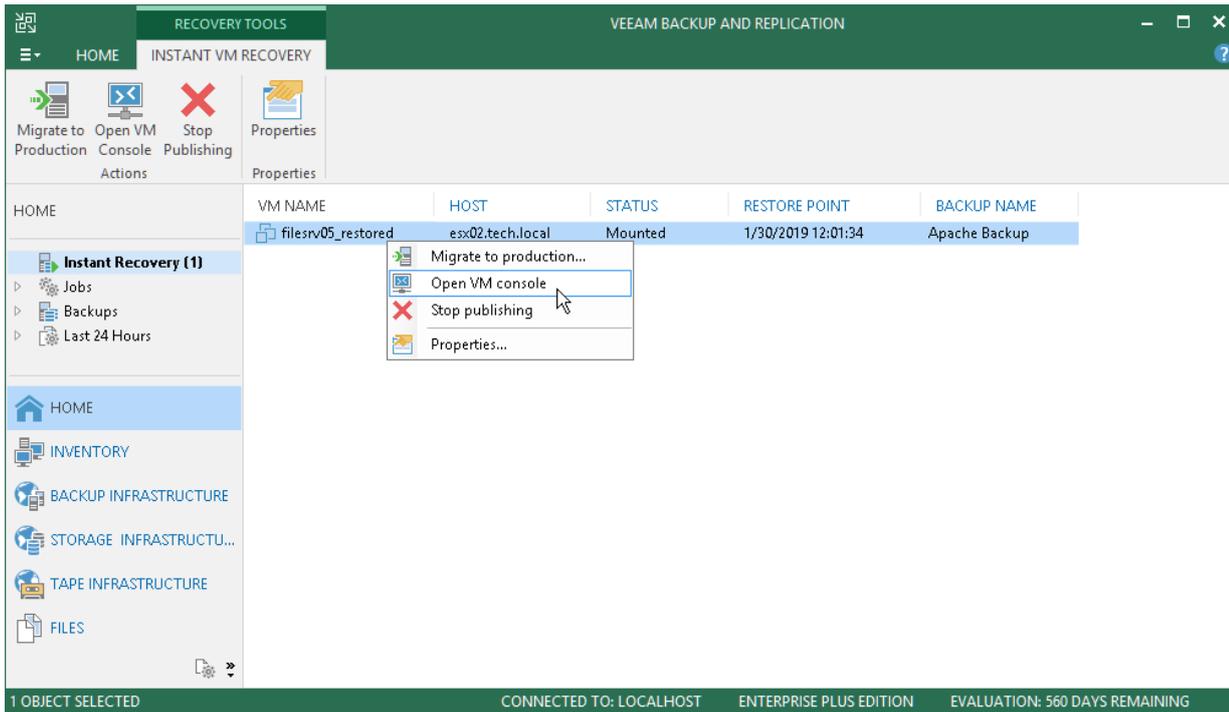
Testing Recovered VM

Before migrating the recovered VM to production, you can open the VM console in Veeam Backup & Replication. You can also test the recovered VM in the VMware vSphere client.

To open a VM console in Veeam Backup & Replication:

1. Open the **Home** view.
2. In the inventory pane, select the **Instant Recovery** node.

3. In the working area, right-click the VM and select **Open VM console**.

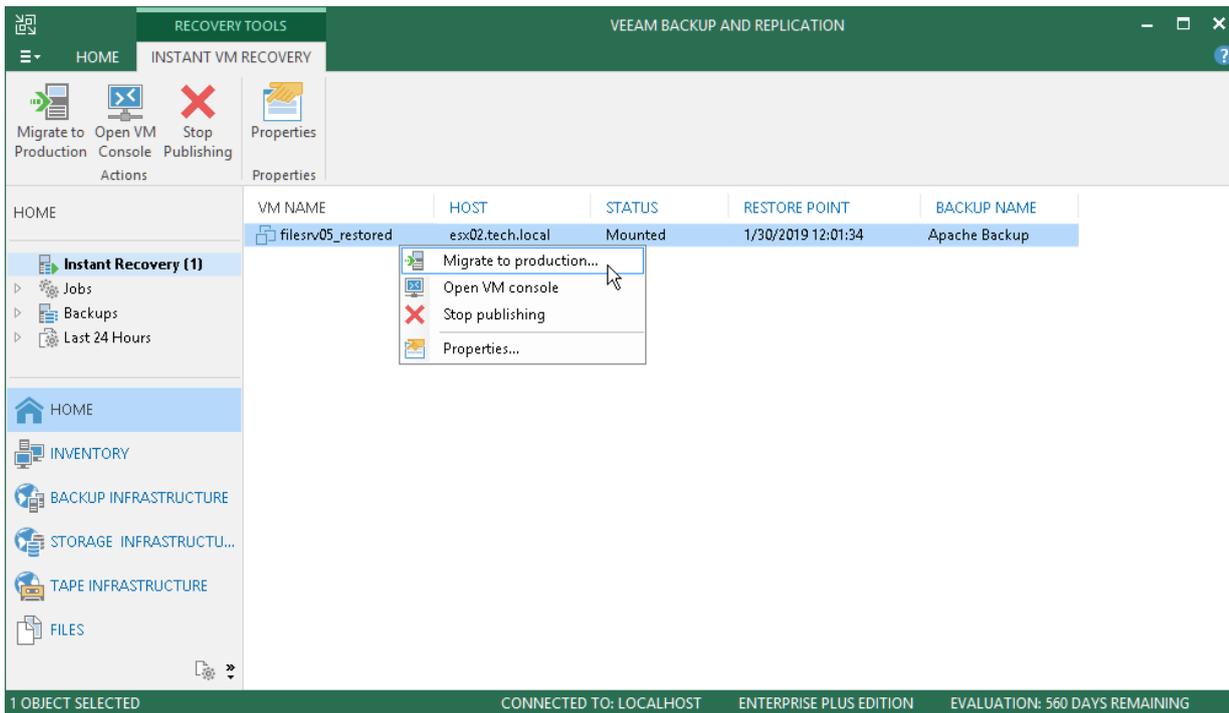


Migrating Recovered VM

To migrate a recovered VM to the production environment:

1. Open the **Home** view.
2. In the inventory pane, select the **Instant Recovery** node.
3. In the working area, right-click the VM and select **Migrate to production**. Veeam Backup & Replication will launch the [Quick Migration](#) wizard.

During migration, Veeam Backup & Replication will restore the VM from the backup file and additionally move all changes that were made while the VM was running from the backup in the Instant Recovery mode.



TIP:

When you pass through the **Quick Migration** wizard, if you don't need the recovery source files anymore, you can enable the **Delete source VM files upon successful migration** option. Veeam Backup & Replication will restore the VM to production and automatically stop the Instant VM recovery session. If you do not enable this option, the Instant VM recovery session will still be running, and you will need to unpublish the recovered VM manually.

Unpublishing Recovered VM

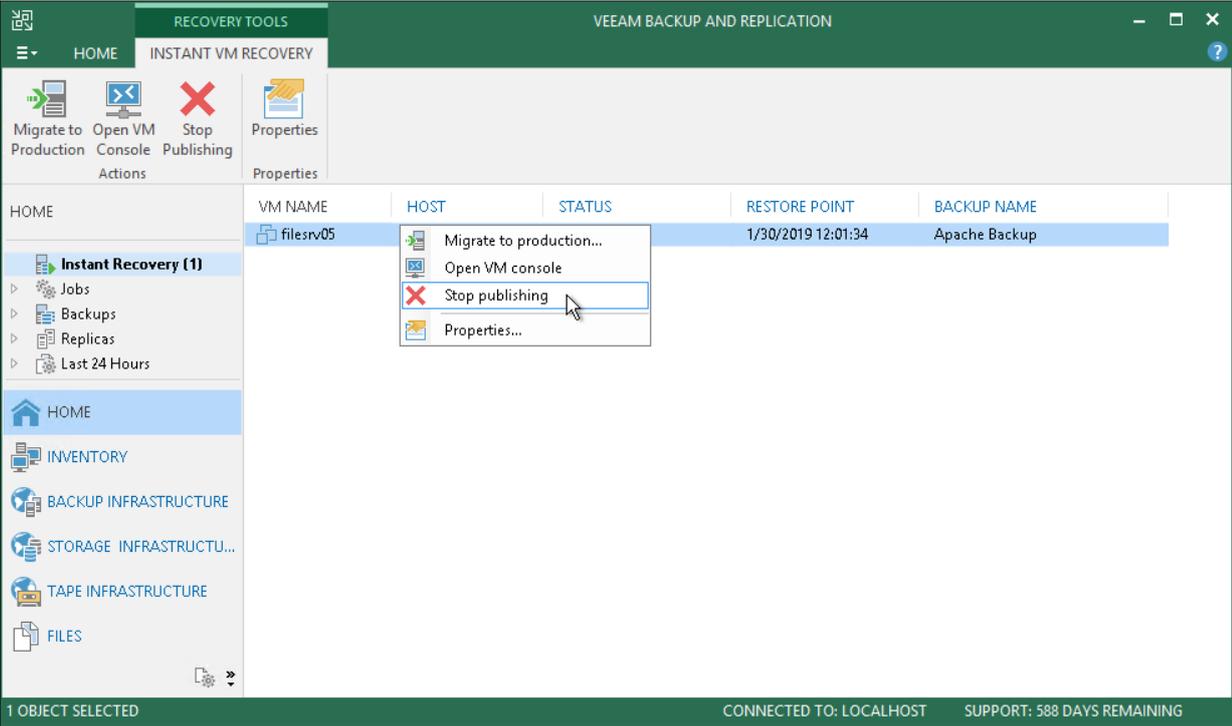
After migration, if you don't need the recovery source files anymore, you can unpublish the recovered VM. If you have enabled the **Delete source VM files upon successful migration** option in the Quick Migration settings, the VM will be unpublished automatically.

After you unpublish the VM, the Instant Recovery session will end and the recovered VM will be unmounted from the vPower NFS server. The migrated VM will remain on the production environment. Note that all changes made in the recovered VM after migration will be lost.

To unpublish a recovered VM:

1. Open the **Home** view.
2. In the inventory pane, select the **Instant Recovery** node.

3. In the working area, right-click the VM and select **Stop publishing**.



Entire VM Restore

If the primary VM fails, you can restore an entire VM from a backup file to the latest state or a previous point in time.

When you restore an entire VM, you extract the VM image from the backup to the production storage. Though entire VM restore takes more resources and time to complete than Instant VM Recovery, you do not need to perform extra steps to finalize the recovery process. Veeam Backup & Replication pulls the VM data from the backup repository to the selected storage, registers the VM on the chosen ESX host and, if necessary, powers it on. Entire VM restore enables full disk I/O performance while Instant VM recovery provides a “temporary spare” for a VM as the vPower NFS throughput is limited.

To perform entire VM restore, Veeam Backup & Replication uses one of the following transport modes:

- If the backup proxy is connected directly into the SAN fabric or has access to NFS datastores, Veeam Backup & Replication uses the Direct storage access transport mode. Veeam Data Movers deployed on the backup repository and backup proxy retrieve VM data from the backup file and put it directly to the necessary datastore.

Veeam Backup & Replication can restore only thick VM disks using the Direct storage access transport mode. For thin VM disks restore, Veeam Backup & Replication will use the Virtual appliance or Network transport modes. Alternatively, you can instruct Veeam Backup & Replication to restore VM disks as thick.

- If the backup proxy is virtualized and resides on the ESX(i) host to which the VM must be restored, Veeam Backup & Replication uses the Virtual appliance transport mode. The Virtual appliance mode utilizes VMware ESX(i) capabilities of HotAdding disks to the VM and thus eliminates the need to transfer the backup data across the network. Veeam Data Movers deployed on the backup repository and backup proxy retrieve VM data from the backup file and put it directly to the necessary datastore via the ESX(i) I/O stack.
- If the Direct storage access and Virtual appliance transport modes cannot be used, Veeam Backup & Replication uses the Network transport mode.

A VM can be restored to its original location or to a new location. When you restore a VM to its original location, 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 which can be potentially caused by changes in VM settings.

When you restore a VM to a new location, you need to specify new VM settings such as the new VM name, the host and datastore where the VM will reside, disk format (thin or thick provisioned) and network properties. Veeam Backup & Replication will change the VM configuration file and store the VM data to the location of your choice.

NOTE:

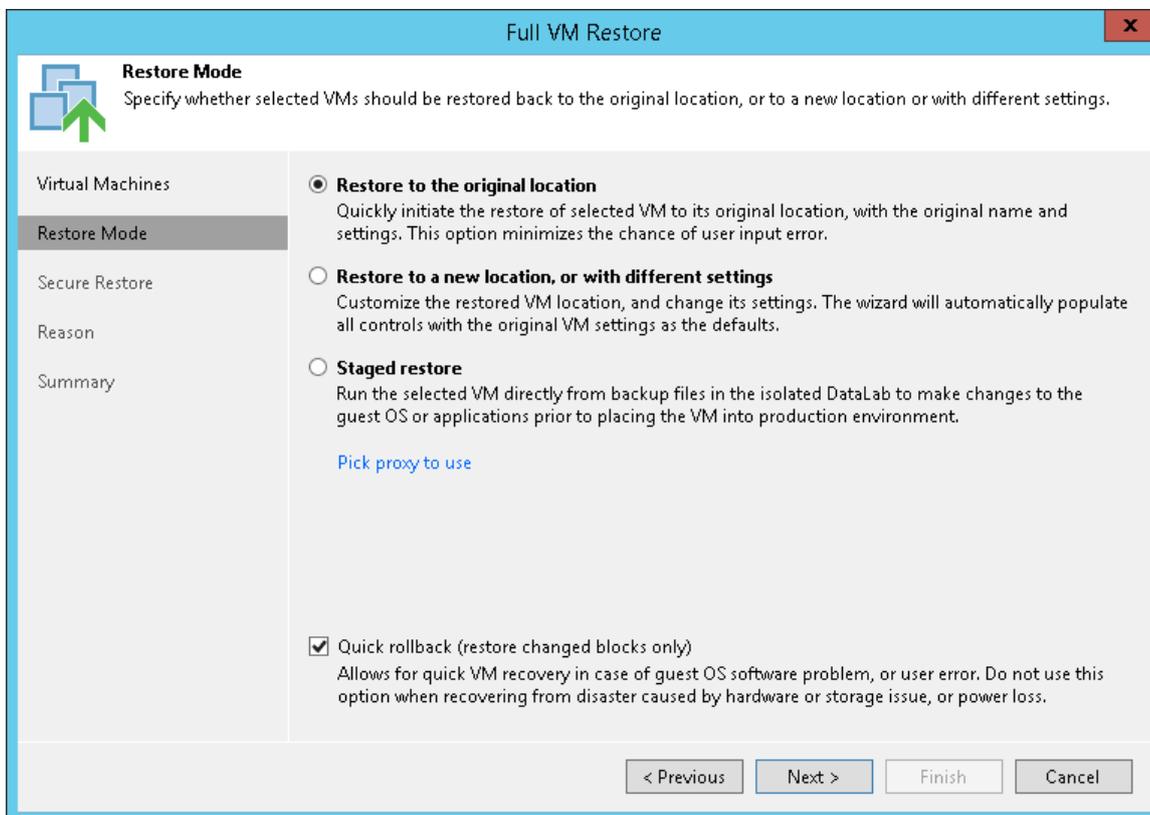
If a VM has several VM disks, Veeam Backup & Replication restores VM disks in parallel.

Quick Rollback

When you restore a full VM or VM hard disk to the original location, you can instruct Veeam Backup & Replication to perform quick rollback – incremental data restore. Instead of restoring an entire VM or VM disk from a backup file, Veeam Backup & Replication will recover only those data blocks that are necessary to revert the VM or VM disk to an earlier point in time. Quick rollback significantly reduces the recovery time and has little impact on the production environment.

For quick rollback, Veeam Backup & Replication uses the Changed Block Tracking technology. Veeam Backup & Replication gets information about the current VM state and compares it with the CBT information in the backup file. This way, Veeam Backup & Replication detects what data blocks must be transported back to the production datastore to rebuild the VM or VM disk to the necessary point in time.

It is recommended that you use quick rollback if you restore a VM or VM disk after a problem that has 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 use quick rollback if the problem has occurred at the VM hardware level, storage level or due to a power loss.



Requirements for Quick Rollback

To perform quick rollback, make sure that the following requirements are met:

- VM or VM disk must be restored to its original location.
- CBT must be enabled for the VM disk or all disks of a VM that you plan to restore.
- The backup file from which you plan to restore a VM or a VM disk must be created with the **Use changed block tracking data** option enabled.

Limitations for Quick Rollback

- [For Microsoft Hyper-V 2016 and later] You cannot run two restore sessions with quick rollback subsequently. After you restore a VM with quick rollback, the CBT on the original VM is reset. You must run at least one incremental backup job session to be able to perform quick rollback again.
- Quick rollback can be performed in the Direct NFS access, Virtual appliance, Network transport mode. The Direct SAN access transport mode cannot be used for quick rollback due to [VMware limitations](#).
- Use quick rollback and VM guest OS file exclusion wisely. If you exclude specific files and folders from the VM guest OS during backup and use quick rollback to restore the VM or VM disk from such backup, Veeam Backup & Replication will restore only the content of the backup file. The excluded data will not be restored. For example, if you exclude C:\Folder from the backup, data in this folder will not be backed up and will not be available in the resulting backup file. After some time, data in C:\Folder may change but the folder will still not be backed up (since the job excludes this folder). For this reason, when you perform quick rollback, Veeam Backup & Replication will restore all data that have changed except the excluded C:\Folder.

Restoring Entire VM

If a VM has failed, you can recover it from the backup with entire VM restore. You can restore one or more VMs at once, to the original location or new location.

The entire VM restore operation recovers an entire VM from the backup file and registers the VM on the target host. Full VM recovery takes more time than Instant VM Recovery as you have to extract the VM image from the backup to the production storage. However, you do not need to take any additional steps to finalize entire VM restore: entire VM restore actually recovers a failed VM on the production storage and provides full disk I/O performance.

Before restoring a VM from the backup, [check prerequisites](#). Then use the **Full VM Restore** wizard to restore the necessary VM.

Before You Begin

Before you restore a VM from a backup, check the following prerequisites:

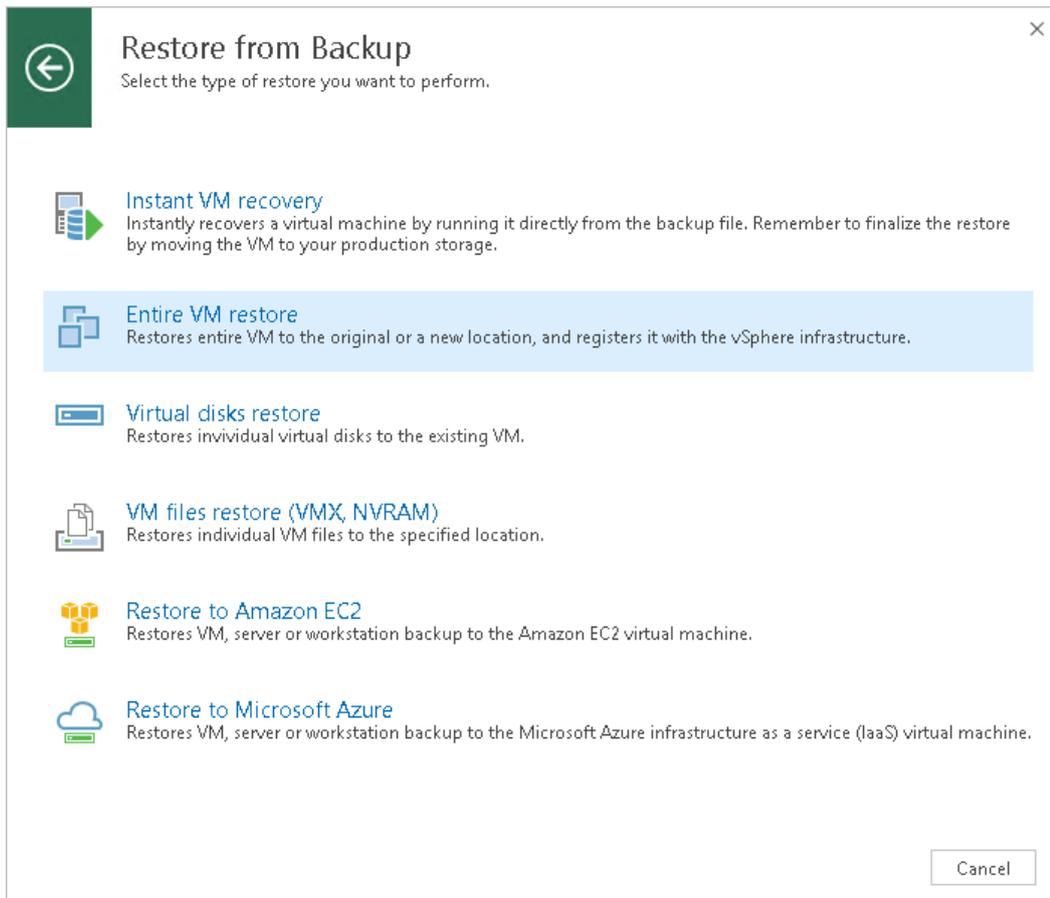
- You can restore a VM from a backup that has at least one successfully created restore point.
- When you restore a VM to its initial location and the original VM is still running, Veeam Backup & Replication will power off the original VM and restore only the disks included in the backup file. All other disks and VM configuration will not be changed.
- If you want to scan VM data for viruses, check the [secure restore requirements and limitations](#).
- If you want to run an executable script for a VM, check the [staged restore requirements and limitations](#).
- When you restore a VM, mind the Virtual Hardware version compatibility. For more information, see <https://kb.vmware.com/s/article/2007240>.

Step 1. Launch Restore Wizard

To launch the **Full VM Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from backup > Entire VM restore > Entire VM restore**.
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Select the machine that you want to restore and click **Entire VM** on the ribbon.
 - Right-click the machine that you want to restore and select **Restore entire VM**.
- Double-click the VBK or VBM file (for example, in Microsoft Windows Explorer). In the displayed window, select the VM and click **Restore > Entire VM**.

You can use this option if you perform restore on the backup server. You cannot use this option if you perform restore remotely over the Veeam Backup & Replication console.



Step 2. Select VMs

At the **Virtual Machines** step of the wizard, select one or more VMs that you want to restore.

To select VMs:

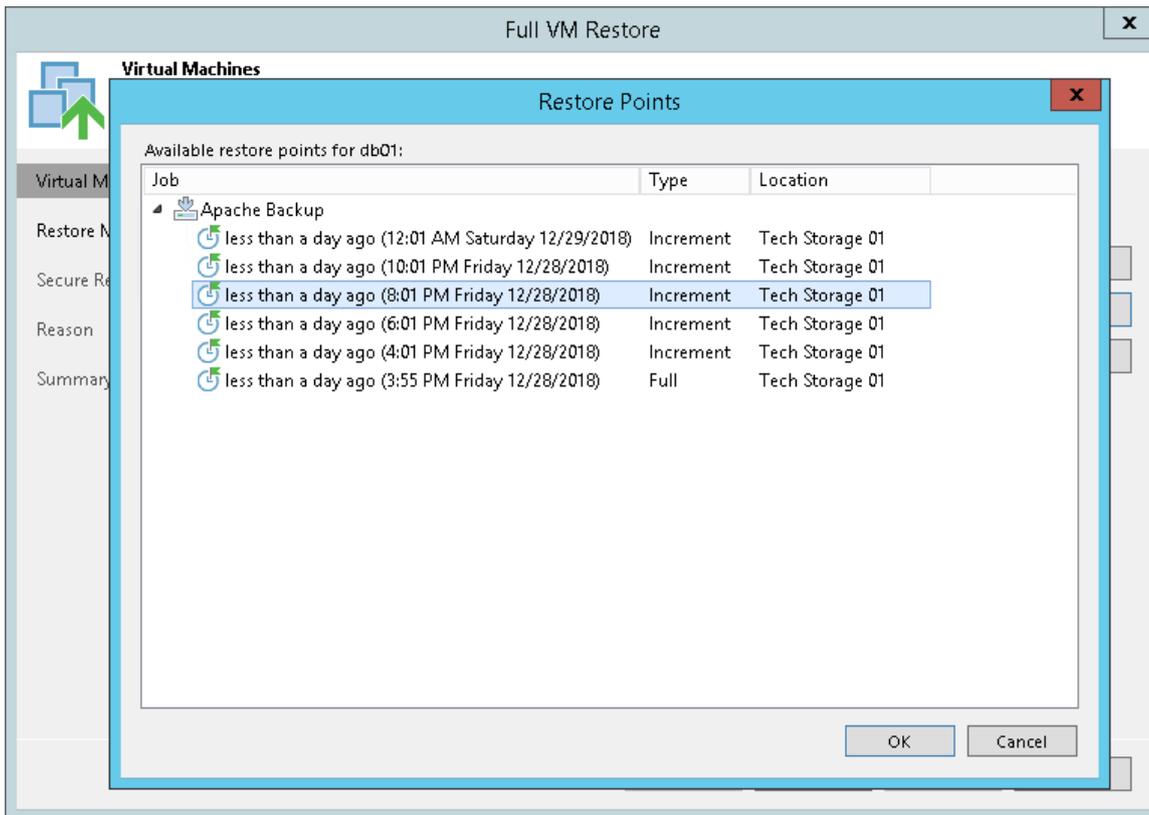
1. Click **Add VM**.
2. Select where to browse for VMs:
 - **From infrastructure** – browse the virtual environment and select VMs or VM containers to restore. If you choose a VM container, Veeam Backup & Replication will expand it to a plain VM list.

When you add a VM to the list, Veeam Backup & Replication displays information about the most recent restore point in the **Restore point** column. If no restore point is available for the added VM, Veeam Backup & Replication will display a warning next to this VM.
 - **From backup** – browse existing backups and select VMs under backup jobs.

To quickly find VMs, you can use the search field at the top of the wizard.

1. Enter a VM name or a part of it in the search field. Veeam Backup & Replication will display possible matches.

In the **Location** column, you can view a name of a backup repository or object storage repository where a restore point resides.



Step 4. 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 VMs with their initial settings and to their original location. If this option is selected, you will immediately pass to the [Reason step](#) of the wizard.
 - 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, format of restored virtual disks and so on). If this option is selected, the **Full VM Restore** wizard will include additional steps for customizing VMs settings.
 - Select **Staged restore** if you want to run an executable script for VMs before restoring them to the production environment. If this option is selected, the **Full VM Restore** wizard will include an additional step for customizing staged restore 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 & Replication will query CBT 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.

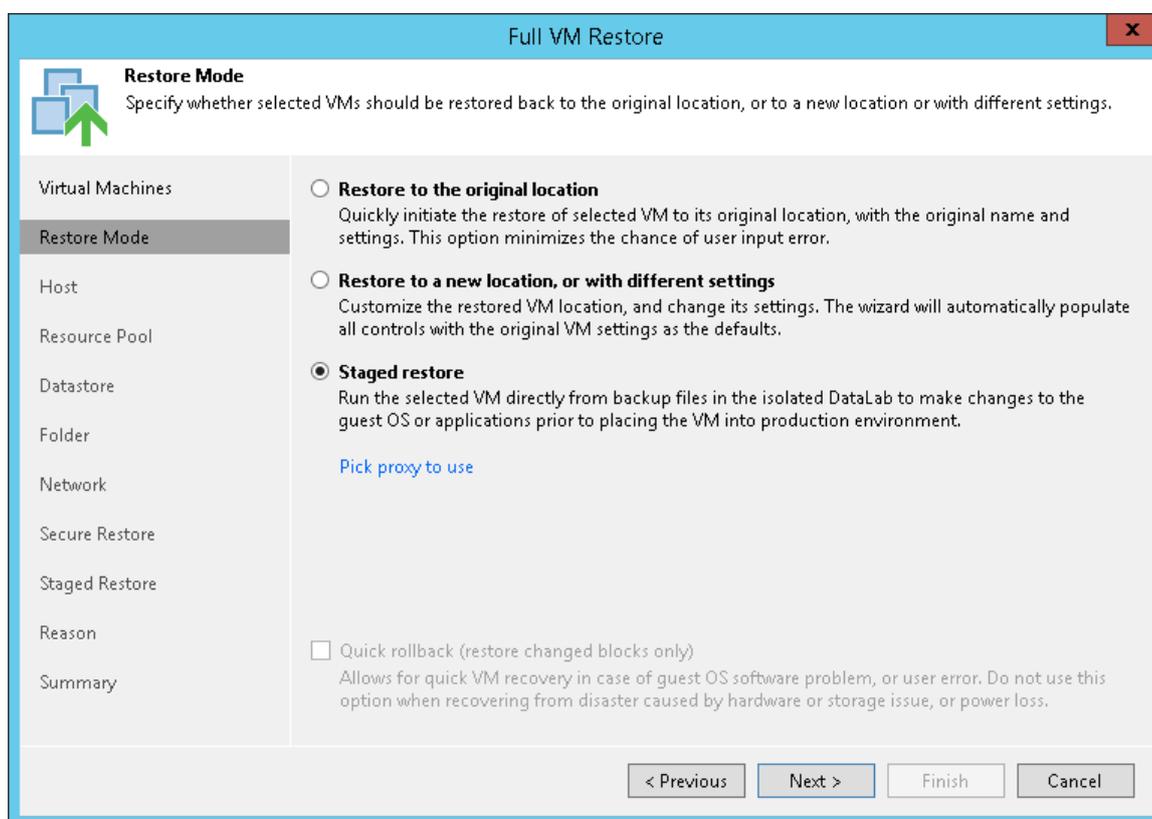
It is recommended that you enable this option if you restore a VM after a problem that occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not enable this option if the problem has occurred at the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

3. Click the **Pick proxy to use** link to select backup proxies over which VM data must be transported to the source datastore. You can assign backup proxies explicitly or instruct Veeam Backup & Replication to automatically select backup proxies.

- If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that are connected to the source datastore and will automatically assign optimal proxy resources for processing VM data.

During the restore process, VMs are processed simultaneously. Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use for writing data to target, current workload on these backup proxies, and selects the most appropriate resources for VMs processing.

- If you choose **Use the selected backup proxy servers only**, you can explicitly select backup proxies that will be used for restore. It is recommended that you select at least two proxies to ensure that VMs are recovered should one of backup proxies fail or lose its connectivity to the source datastore during restore.



Restoring Storage Policies

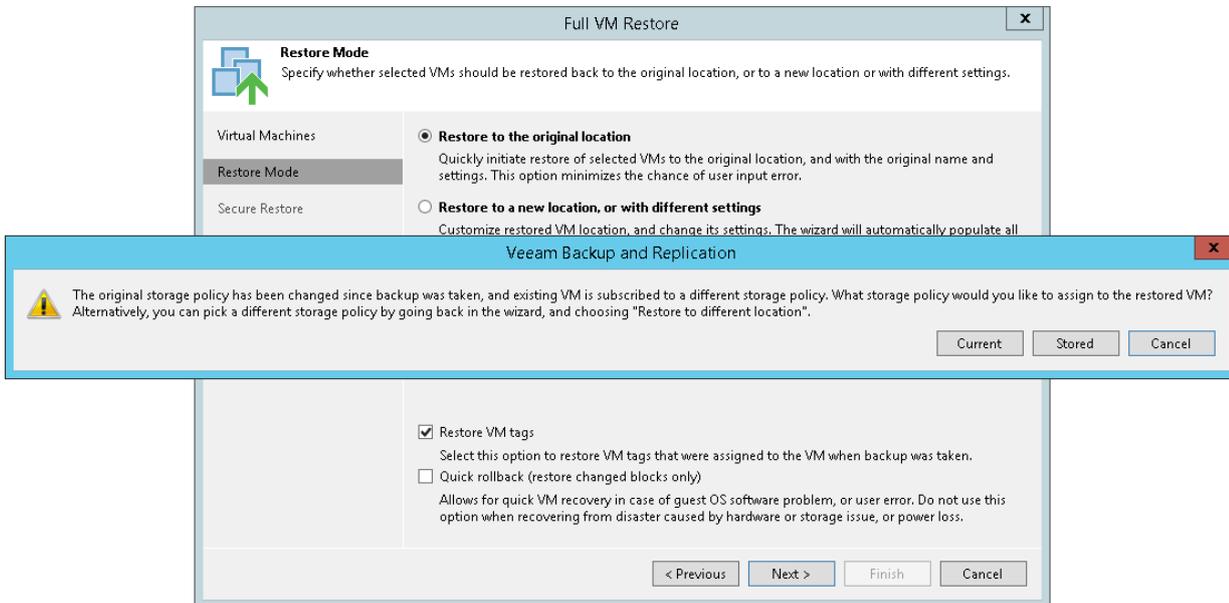
If the backed up VM was associated with the storage policy, in the restore to original location scenario, Veeam Backup & Replication will associate the restored VM with this storage policy.

When you click **Next**, Veeam Backup & Replication will check storage policies in the virtual environment and compare this information with the information about the storage policy in the backup file. If the original storage policy has been changed or deleted, Veeam Backup & Replication will display a warning. You can select one of the following options:

- **Current** – the restored VM will be associated with the profile with which the original VM in the production environment is currently associated.
- **Default** – the restored VM will be associated with the profile that is set as default for the target datastore.

- **Stored** – the restored VM will be associated with the profile that was assigned to the original VM at the moment of backup, and whose information is stored in the backup file.

For more information, see [Storage Policies](#).



Step 5. Select Target Host

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

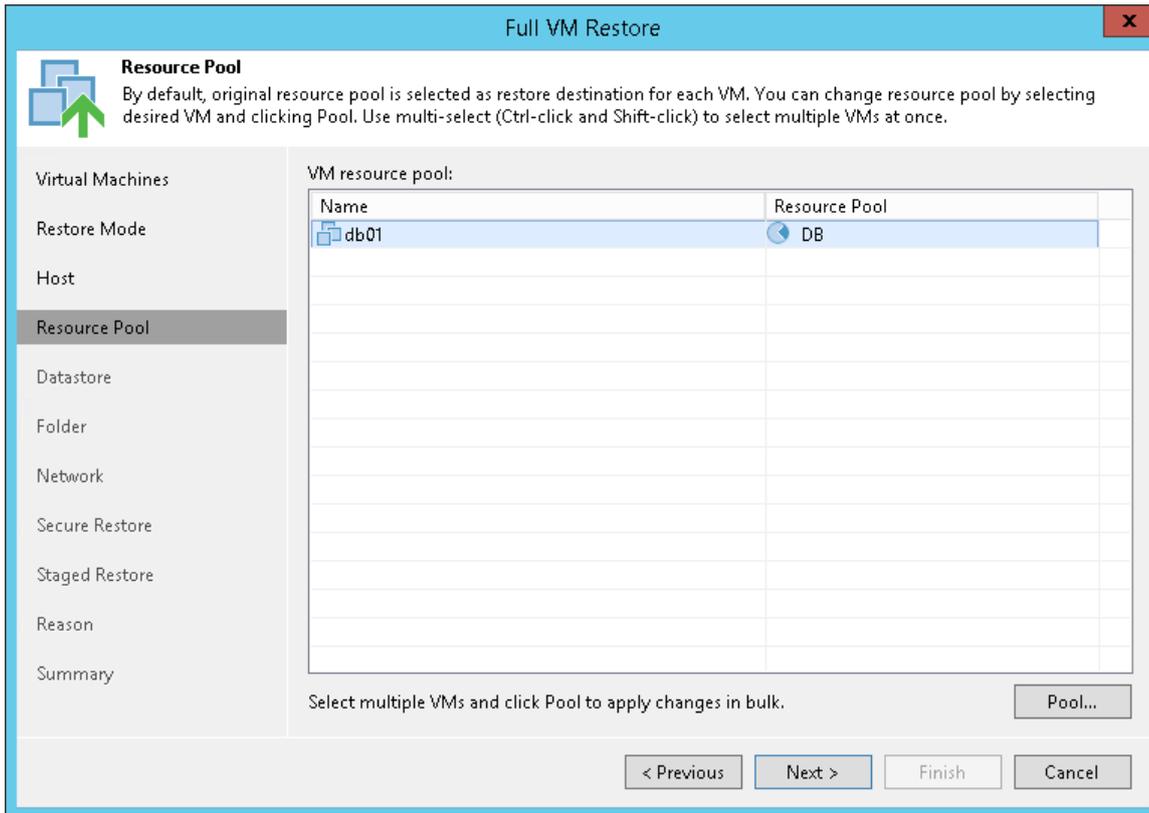
To specify a target host:

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. Click the **Start search** button on the right or press **[ENTER]**.



Step 7. Select Target 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]**.

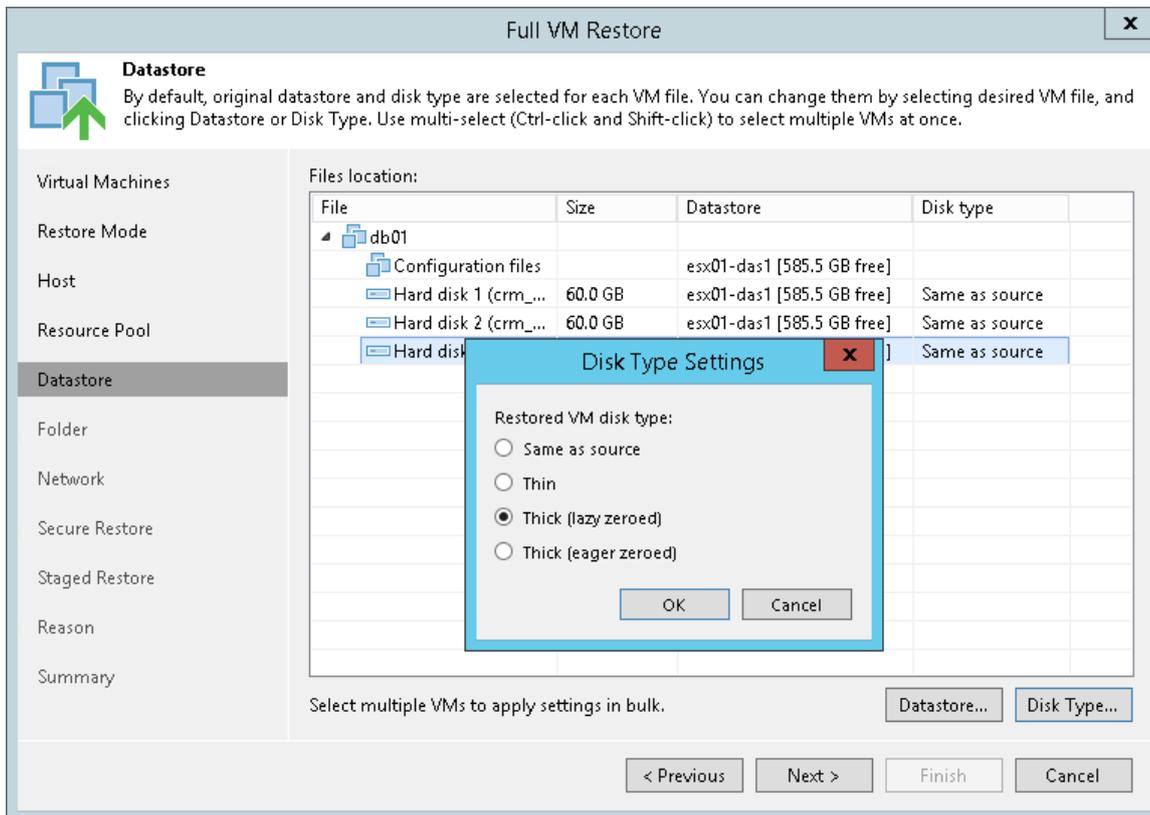
By default, Veeam Backup & Replication preserves the format of restored VM disks. If disks of the original VM are provisioned as thick, Veeam Backup & Replication will restore the VM from the backup with thick disks. If necessary, you can change the disk format of a restored VM.

1. Expand a VM in the list.
2. Select the disk and click **Disk Type**.

- In the **Disk Type Settings** section, choose the format that will be used to restore virtual disks of the VM: same as source, thin, thick lazy zeroed or thick eager zeroed. For more information about disk types, see <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.html.hostclient.doc/GUID-4COF4D73-82F2-4B81-8AA7-1DD752A8A5AC.html>.

NOTE:

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



Step 8. Select Target Folder and Change VM Settings

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

At this step of the wizard, you can do the following:

- Specify a destination VM folder
- Change VM settings

Specifying Destination VM Folder

To specify a destination VM folder:

- Select a VM in the list and click **Folder**.
- 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]**.

By default, Veeam Backup & Replication 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.

Changing VM Settings

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 also change the VM name directly in the list:

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

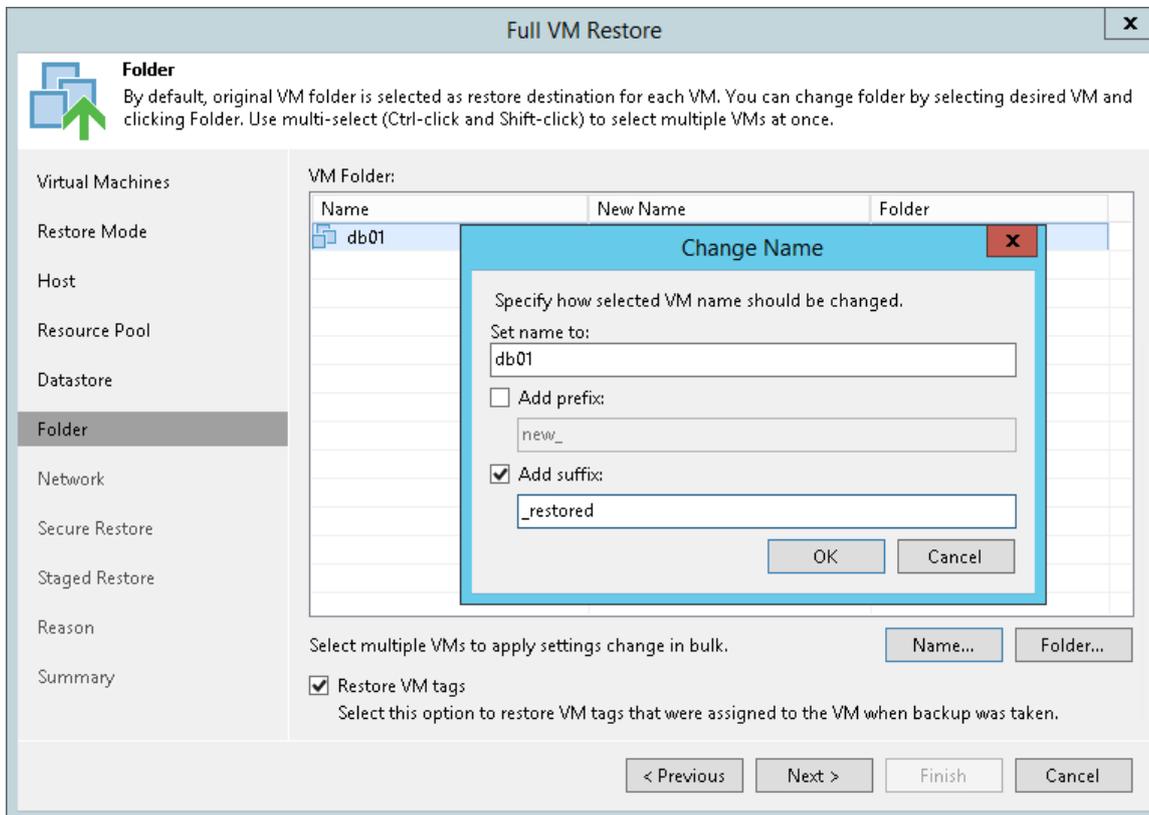
Select the **Restore VM tags** check box if you want to restore tags that were assigned to the original VM, and assign them to the restored VM. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:

- The VM is restored to its original location.
- The original VM tag is still available on the source vCenter Server.

NOTE:

Mind the following:

- If you restore a VM to a standalone ESX(i) host that is not managed by the vCenter Server, you cannot select a destination folder: this option will be disabled.
- During entire VM restore, Veeam Backup & Replication preserves the UUID of the original VM.



Step 9. Specify Network Mapping

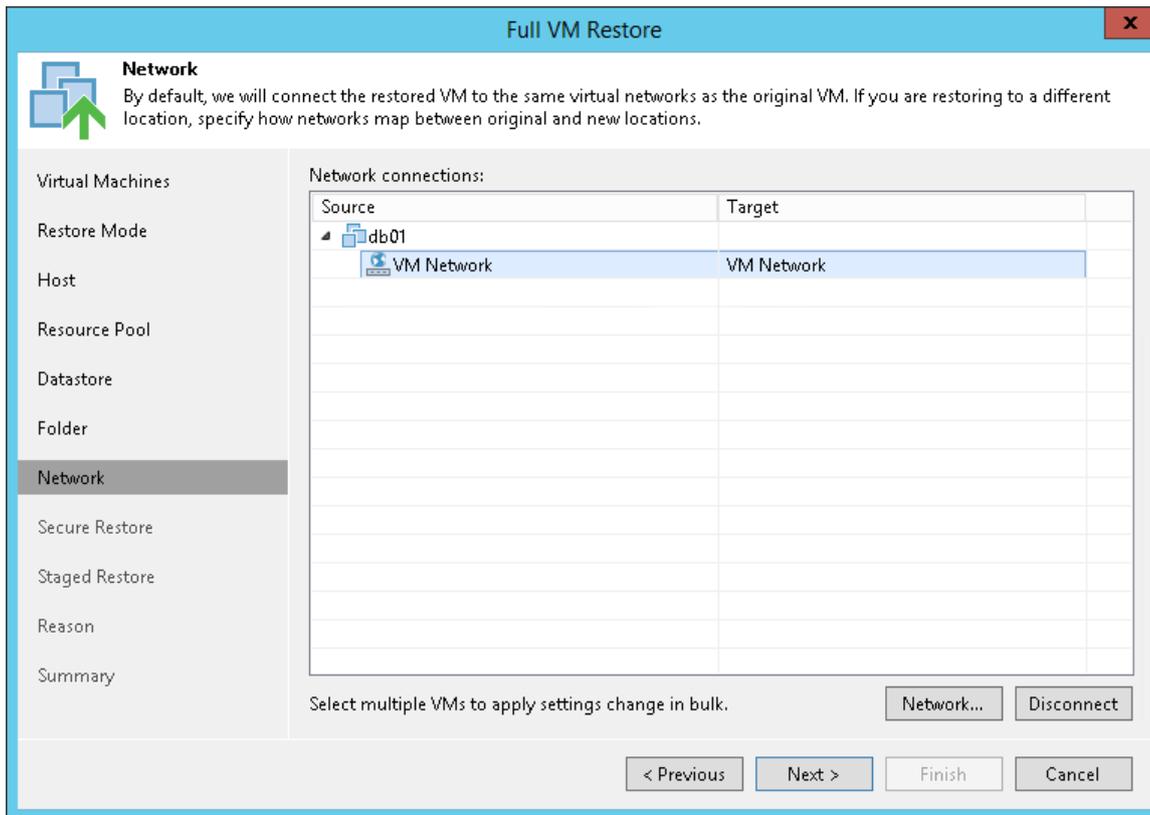
The **Network** step of the wizard is available if you have chosen to change the location and settings for the restored VM.

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 & Replication 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 target 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**.



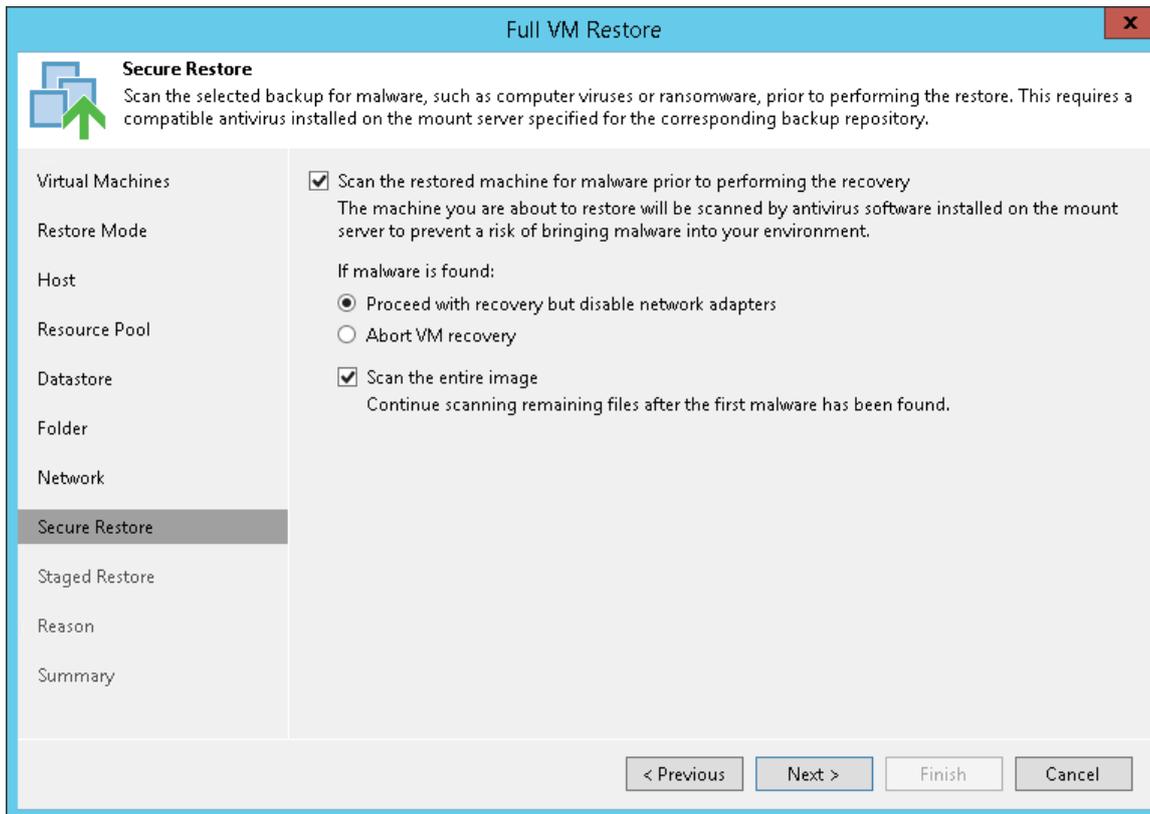
Step 10. Specify Secure Restore Settings

You can instruct Veeam Backup & Replication to perform secure restore – scan machine data with antivirus software before restoring the machine to the production environment. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

1. At the **Secure Restore** step of the wizard, select the **Scan the restored machine for malware prior to performing the recovery** check box.
2. Select which action Veeam Backup & Replication will take if the antivirus finds a virus threat:
 - **Proceed with recovery but disable network adapters.** Select this action if you want to restore the machine with disabled network adapters (NICs).
 - **Abort VM recovery.** Select this action if you want to cancel the restore session.

3. Select the **Scan the entire image** check box if you want the antivirus to continue machine scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).



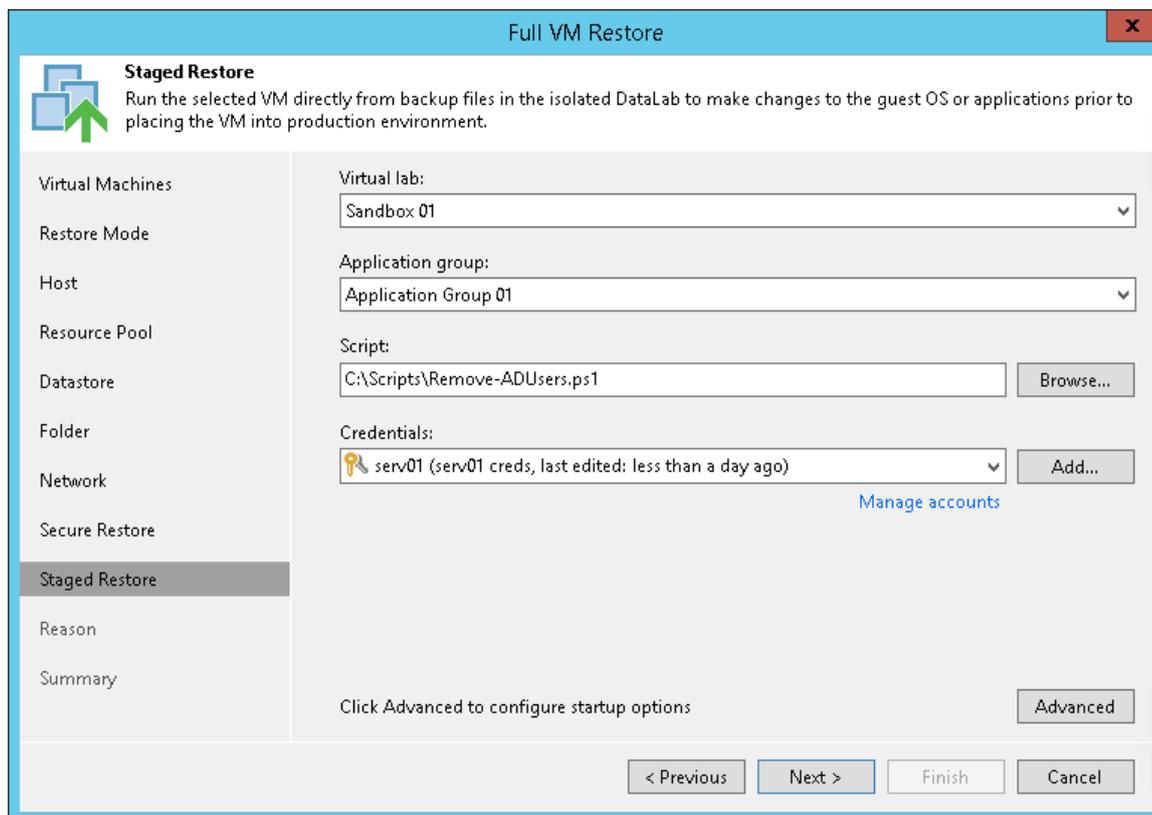
Step 11. Specify Staged Restore Settings

The **Staged Restore** step of the wizard is available if you have chosen to run an executable script for VMs before recovering them to the production environment. For more information on staged restore, see [Staged Restore](#).

To specify staged restore settings:

1. From the **Virtual lab** list, select a virtual lab that will be used to start VMs. The list contains all virtual labs that are created or connected to the backup server.
2. From the **Application group** list, select an application group if script execution requires other VMs to be powered on. In the virtual lab during staged restore, Veeam Backup & Replication will start VMs from the selected application group in the required order. The **Application group** list contains all application groups that are created on the backup server. For more information, see [Application Group](#).
3. On the right of the **Script** field, click **Browse** to choose the script from a local folder on the backup server.

- From the **Credentials** list, select credentials for the account that has administrator privileges on VMs for which you want to run the script. 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](#).

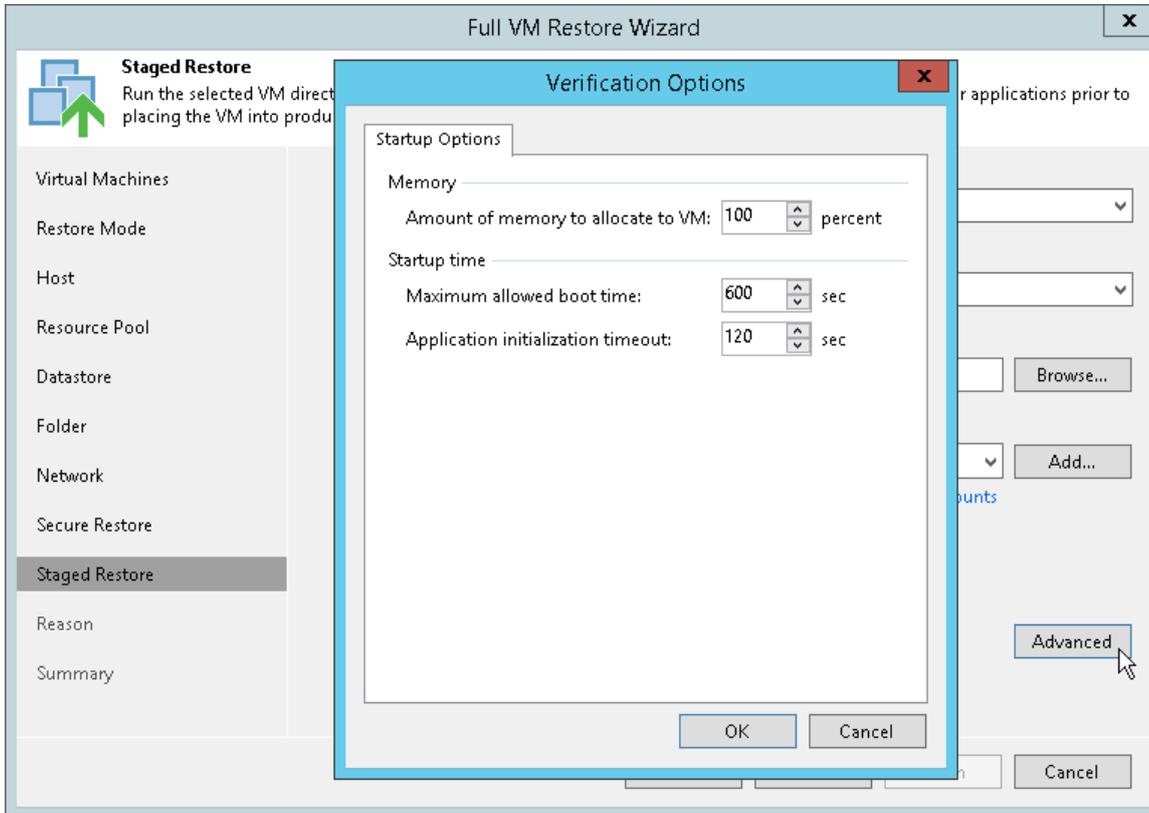


VM Startup Settings

If you want to start VMs after recovery, perform the following steps:

- Click **Advanced**.
- In the **Memory** section, specify the amount of memory that you want to pre-allocate to a VM when it starts. The amount of pre-allocated memory is defined in percent. The percentage rate is calculated based on the system memory level available for the production VM. For example, if 4096 MB of RAM is allocated to the VM in the production environment and you specify 50% as a memory rate, 2048 MB of RAM will be allocated to the VM on startup.
- In the **Startup time** section, specify the allowed boot time for the VM and timeout to initialize applications on the VM.

Be careful when specifying the **Maximum allowed boot time** value. Typically, a VM started in a virtual lab requires more time to boot than a VM started in the production environment. If an application fails to be initialized within the specified interval of time, the recovery process fails with the timeout error. If such error occurs, you need to increase the **Maximum allowed boot time** value and perform VM restore again.

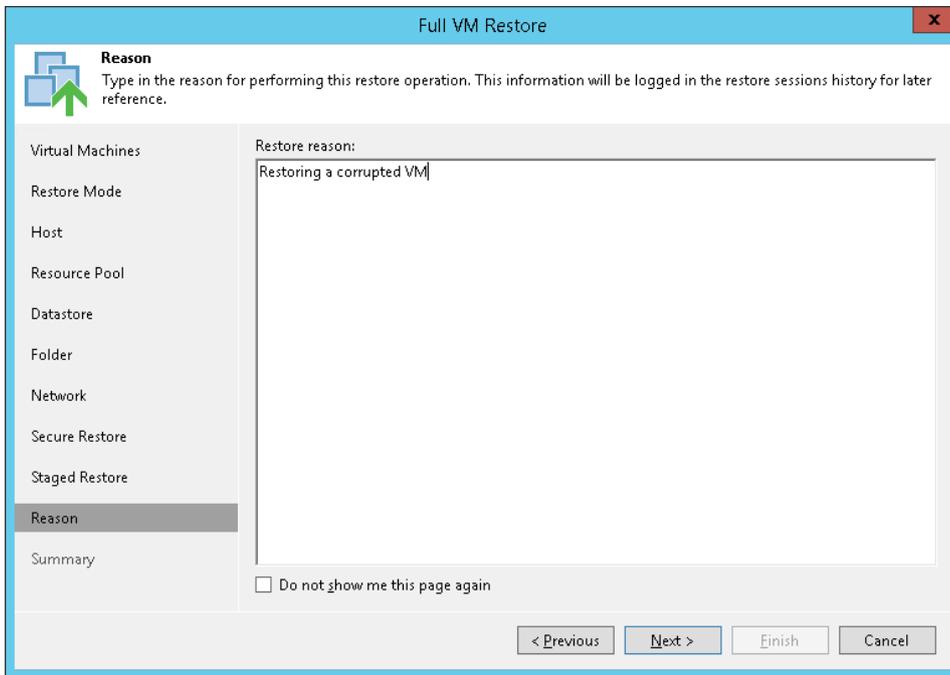


Step 12. Specify Restore Reason

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:

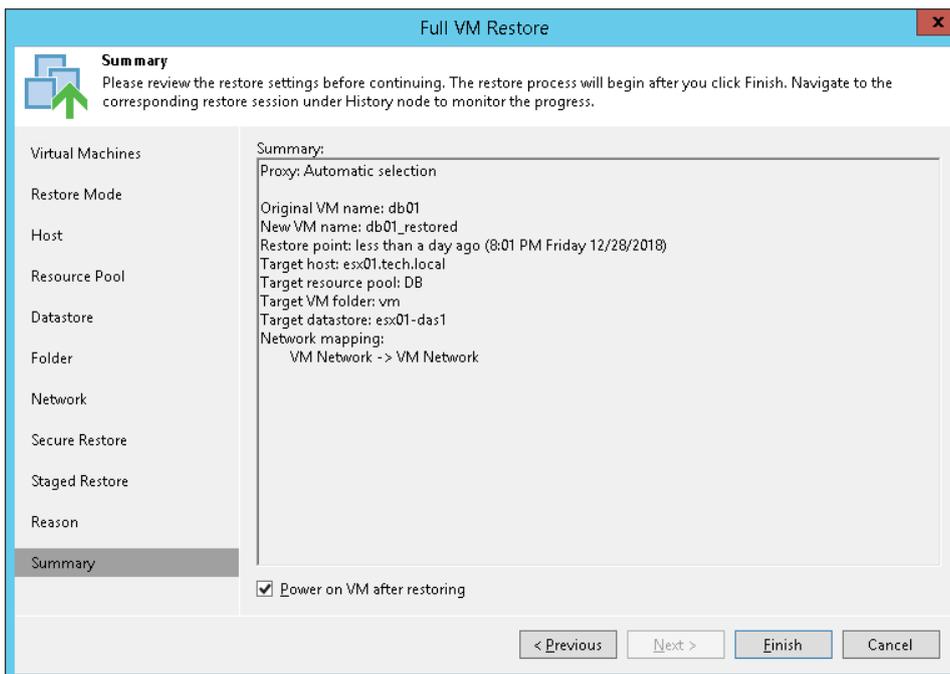
If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 13. Verify Restore 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 & Replication will restore selected VMs in the specified destination.



VM Files Restore

Veeam Backup & Replication can help you to restore specific VM files (.vmdk, .vmx and others) if any of these files are deleted or the datastore is corrupted. This option provides a great alternative to entire VM restore, for example, when your VM configuration file is missing and you need to restore it. Instead of restoring the whole VM image to the production storage, you can restore the specific VM file only.

When you perform VM file restore, VM files are restored from regular image-level backups. Veeam Data Movers deployed on the backup repository and the backup proxy retrieve VM data from the backup file and send it to the original VM location, or to a new location specified by the user.

Restoring VM Files

You can restore specific VM files from the backup: VMDK, VMX and others. VM file restore can be helpful, for example, if one or several VM files have been deleted or corrupted and you need to replace them on the production storage. Veeam Backup & Replication lets you restore the necessary VM file directly from the image-level backup, without prior de-staging of the VM image from the backup file.

Before restoring VM files from the backup, [check prerequisites](#). Then use the **Virtual Machine Files Restore** wizard to restore VM files.

Before You Begin

Before you restore VM files, check the following prerequisites:

- You can restore VM files from a backup that has at least one successfully created restore point.
- The server on which you plan to save restored VM files must be added to the backup infrastructure.

Step 1. Launch Restore Wizard

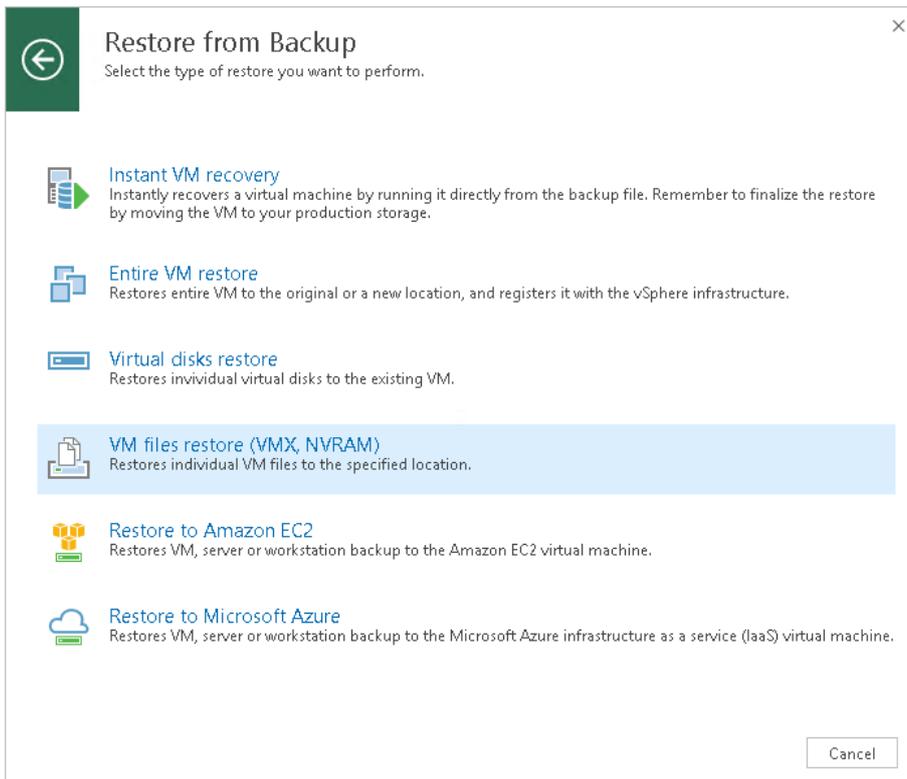
To launch the **Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from backup > Entire VM restore > VM files restore (VMX, NVRAM)**.
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Click the VM whose files you want to restore and click **VM Files** on the ribbon.
 - Right-click the VM whose files you want to restore and select **Restore VM files**.

In this case, you will pass to the [Restore Point](#) step of the wizard.

- Double-click the VBK or VBM file (for example, in Microsoft Windows Explorer). In the displayed window, select the VM and click **Restore > VM files**. In this case, you will pass to the [Restore Point](#) step of the wizard.

You can use this option if you perform restore on the backup server. You cannot use this option if you perform restore remotely over the Veeam Backup & Replication console.



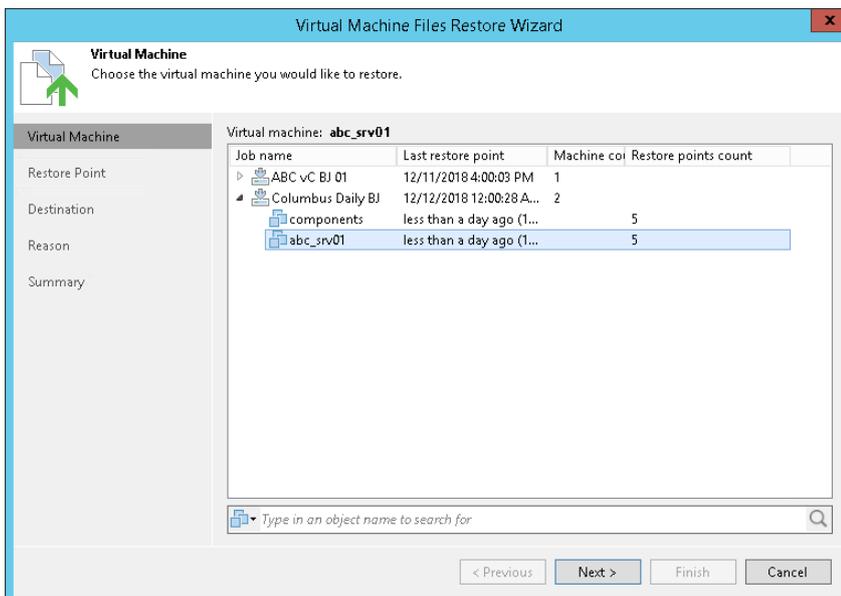
Step 2. Select VM

At the **Virtual Machine** step of the wizard, select the VM whose 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.

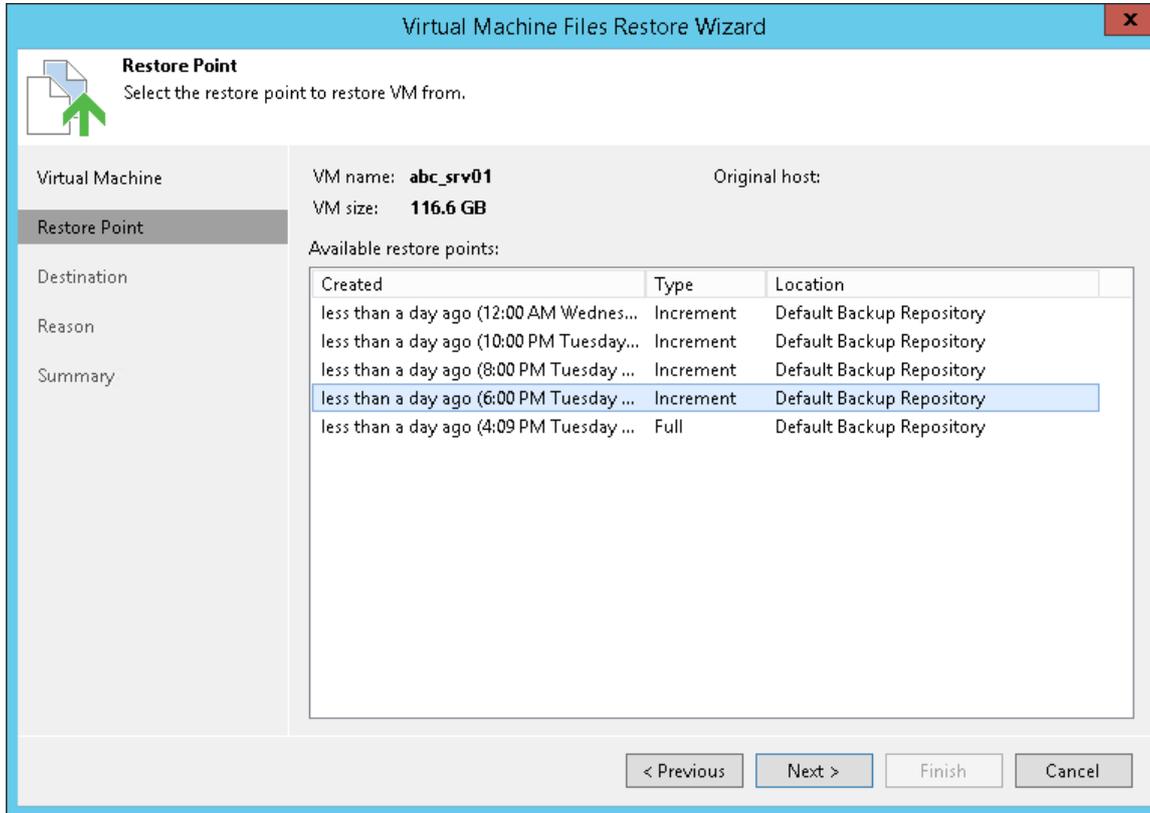
1. Enter a VM name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Step 3. Select Restore Point

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

In the **Location** column, you can view a name of a backup repository or object storage repository where a restore point resides.



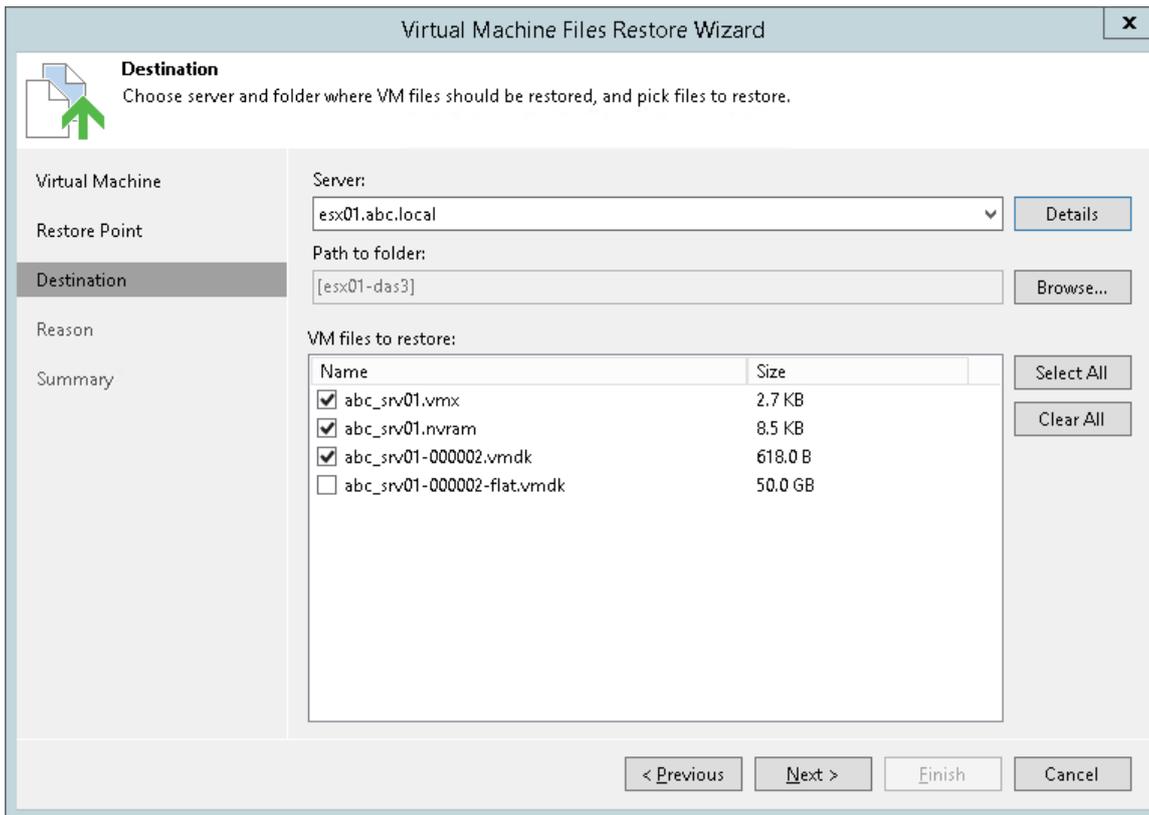
Step 4. Select VM Files and Destination

At the **Destination** step of the wizard, select VM files that 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 an ESX(i) 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 target 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.

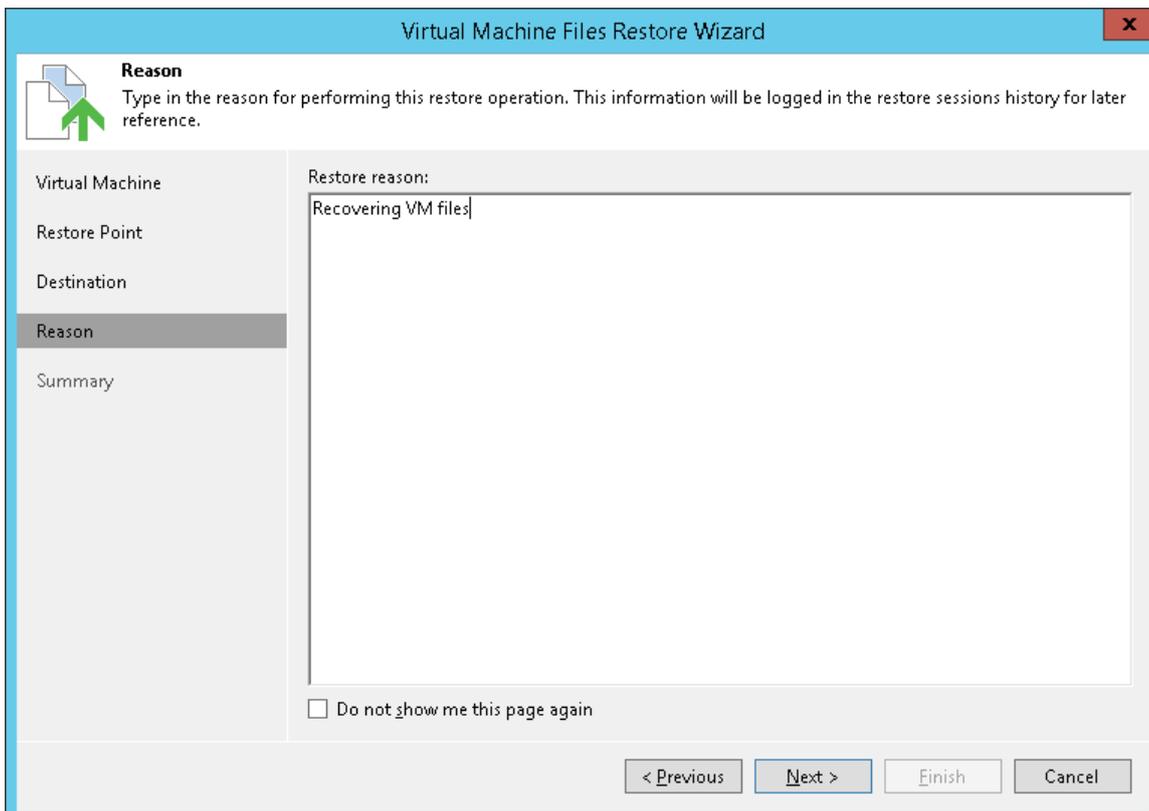
To create a dedicated folder for restored files, click **Browse**. In the **Select Folder** window, select the target location for VM files and click **Make New Folder** at the bottom of the window.

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.



Step 5. Specify Restore Reason

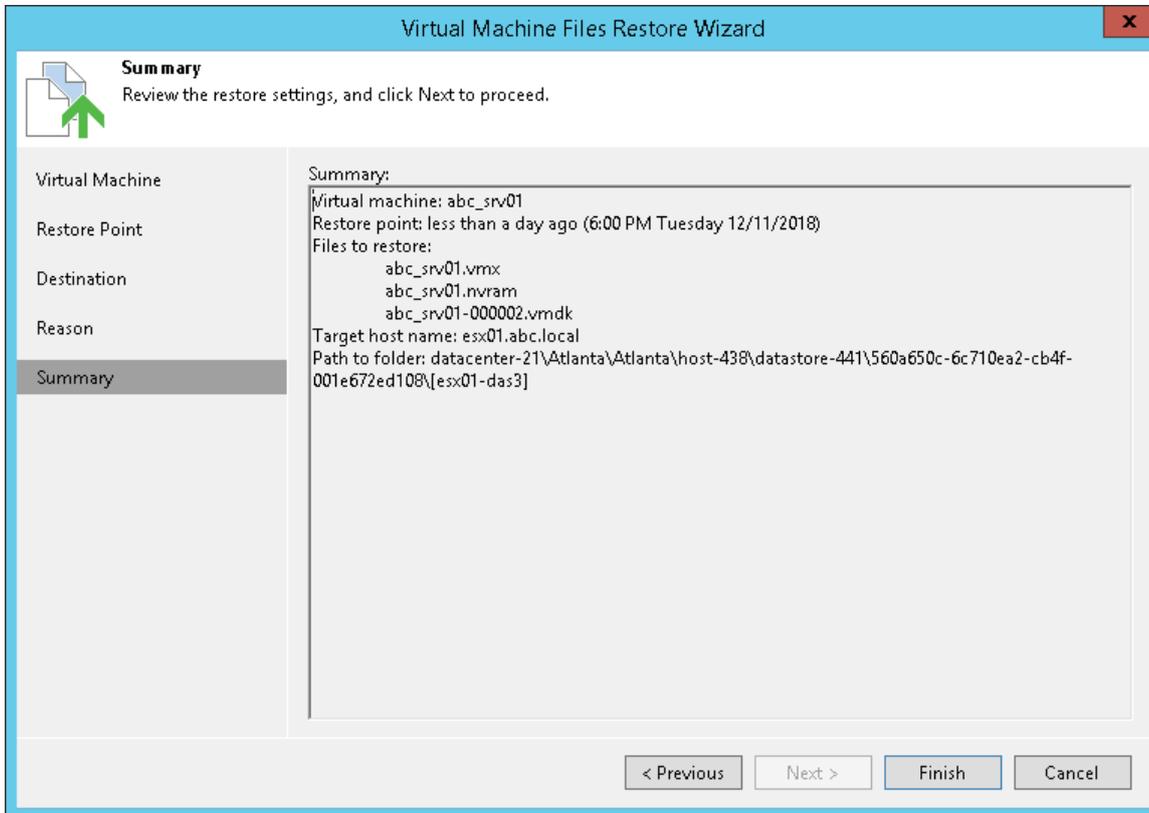
At the **Reason** step of the wizard, enter a reason for restoring VM files. The information you provide will be saved in the session history and you can reference it later.



Step 6. Finish Working with Wizard

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

1. Review details for the restore task.
2. Click **Finish** to start VM files restore.



Virtual Disks Restore

If a VM virtual disk becomes corrupted for some reason, for example, with a virus, you can restore it from the image-based backup to any point in time. The restored virtual disk can be attached to the original VM to replace a corrupted drive, or connected 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 on the fly.

NOTE:

If a VM has several VM disks, Veeam Backup & Replication restores VM disks in parallel.

Restoring Virtual Disks

You can restore virtual disks of a VM from backups. The restored disks can be attached to the original VM (for example, if you need to replace a corrupted disk) or mapped to any other VM in the virtual infrastructure.

Before restoring virtual disks from the backup, [check prerequisites](#). Then use the **Virtual Disk Restore** wizard to restore the necessary VM disks.

Before You Begin

Before you restore virtual disks, check the following prerequisites:

- You can restore virtual disks from a backup that has at least one successfully created restore point.
- During the virtual disk restore, Veeam Backup & Replication turns off the target VM to reconfigure its settings and attach restored disks. It is recommended that you stop all activities on the target VM for the restore period.
- You cannot mount restored disks to a VM that has one or more snapshots.
- If you want to scan virtual disk data for viruses, check the [secure restore requirements and limitations](#).

NOTE:

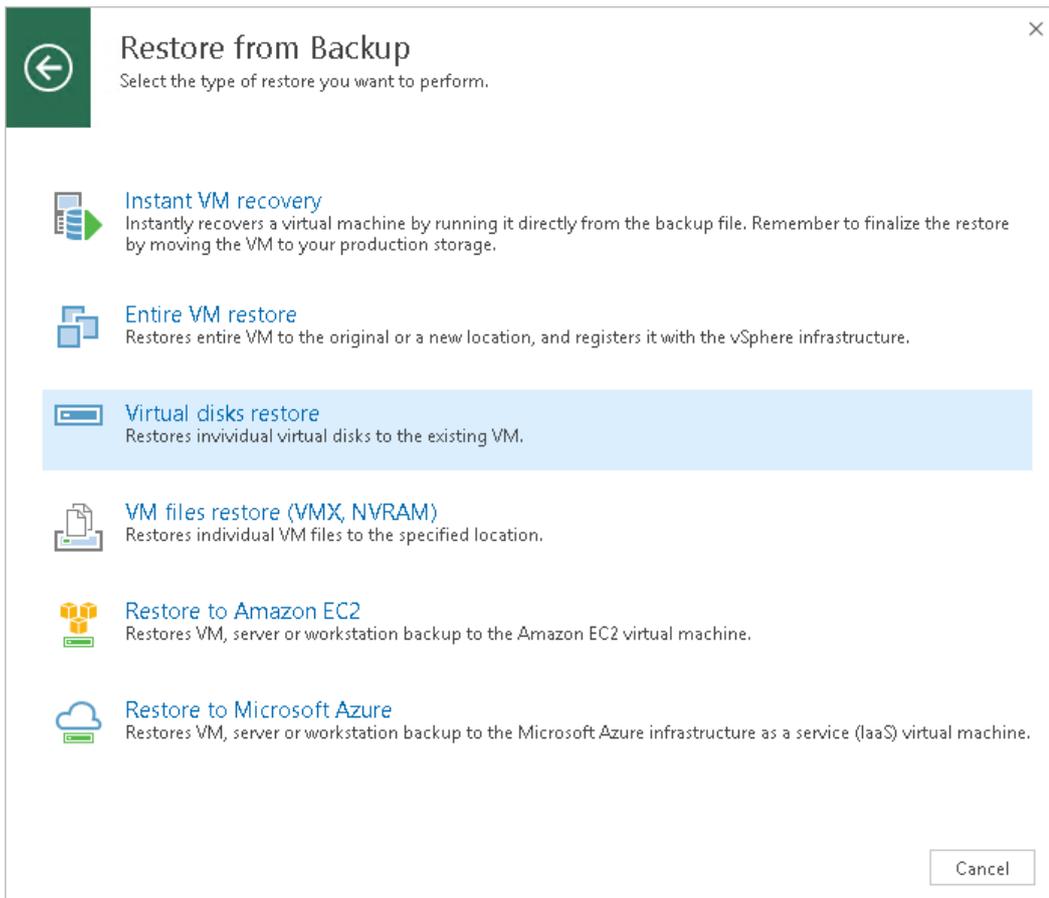
If you back up a VM with vRDM disks, Veeam Backup & Replication converts them into VMDK files. Thus, when you restore a vRDM disk, Veeam Backup & Replication will restore it as a VMDK file. If you want to preserve the vRDM format for restored disks, use Quick Rollback. For more information, see [Quick Rollback](#).

Step 1. Launch Virtual Disk Restore Wizard

To launch the **Virtual Disk Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from backup > Entire VM restore > VM disks restore**.
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Click the VM whose files you want to restore and click **Virtual Disks** on the ribbon.
 - Right-click the VM whose files you want to restore and select **Restore virtual disks**.
- Double-click the VBK or VBM file (for example, in Microsoft Windows Explorer). In the displayed window, select the VM and click **Restore > Virtual disks**.

You can use this option if you perform restore on the backup server. You cannot use this option if you perform restore remotely over the Veeam Backup & Replication console.



Step 2. Select VM

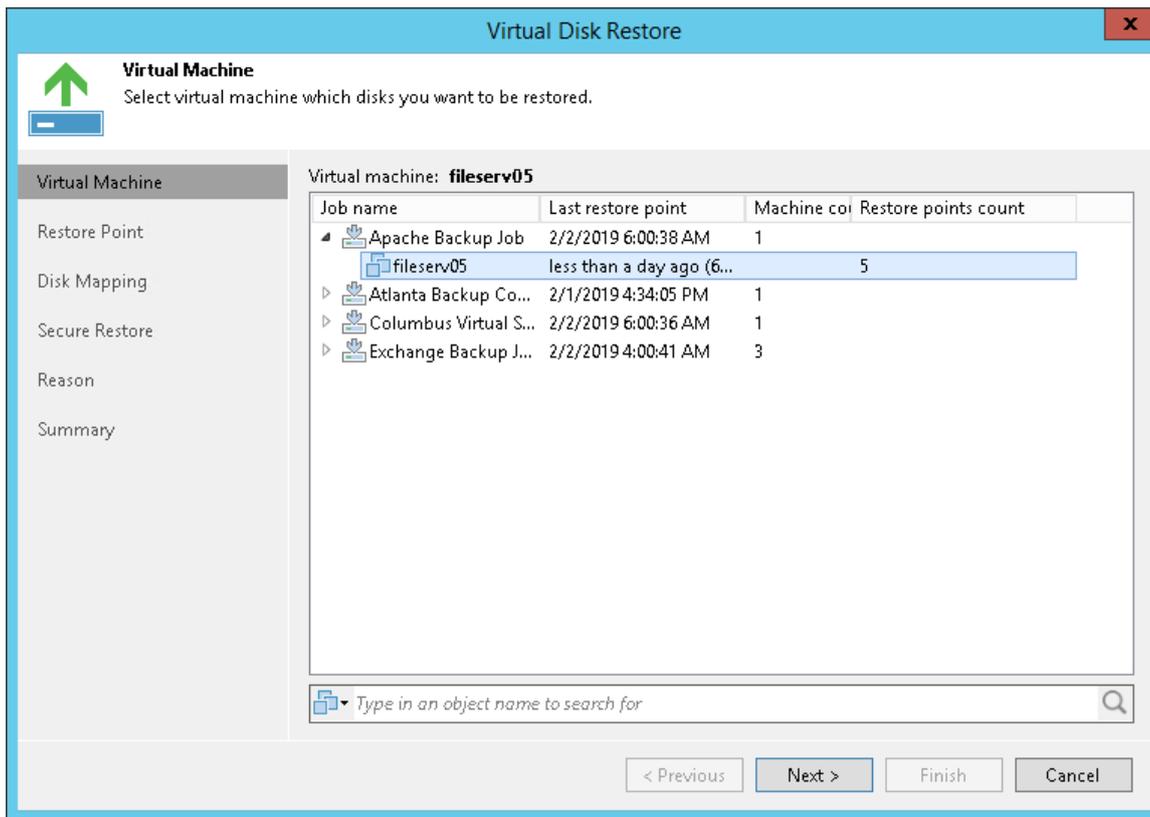
At the **Virtual Machine** step of the wizard, select the VM whose disks you want to restore:

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.

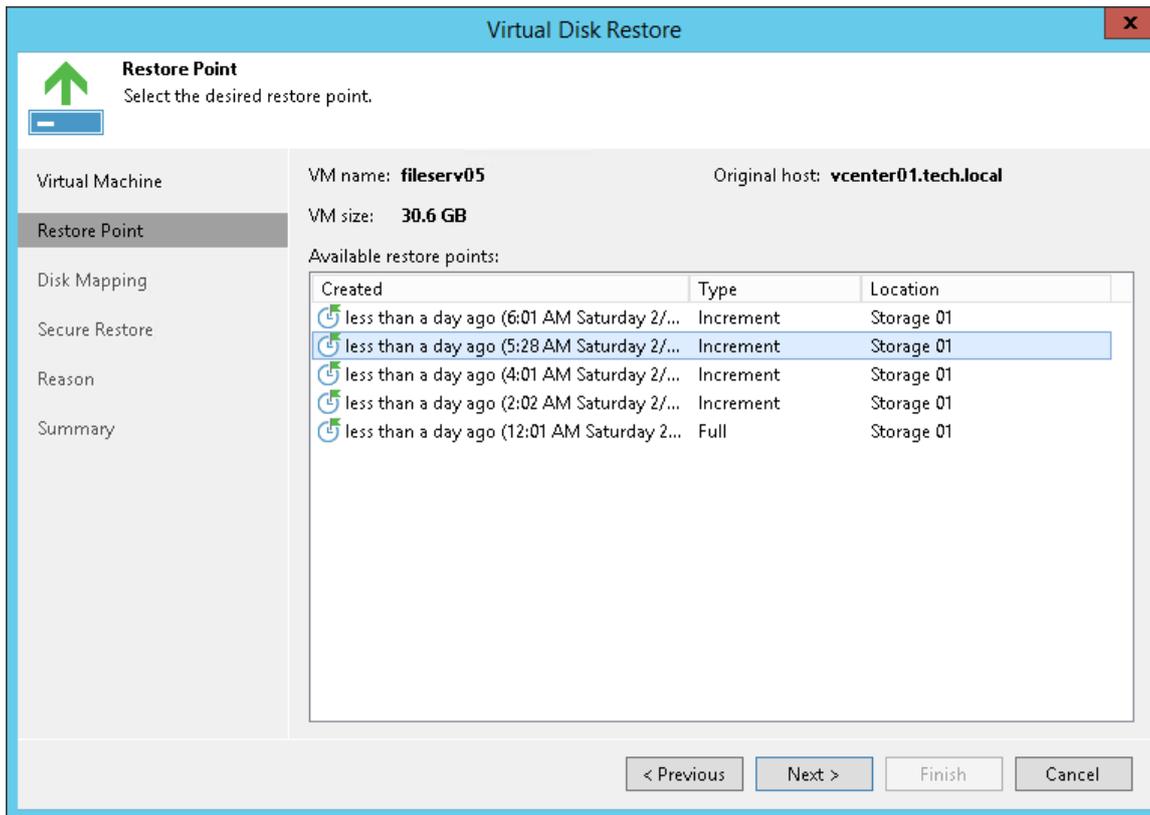
2. Click the **Start search** button on the right or press [ENTER].



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 disks.

In the **Location** column, you can view a name of a backup repository or object storage repository where a restore point resides.



Step 4. 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 settings.

1. By default, Veeam Backup & Replication 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 placed.

NOTE:

If you use storage policies in the virtual environment, Veeam Backup & Replication will display information about storage policies in the **Select Datastore** window. You can select a datastore associated with the necessary storage policy.

4. In the **Virtual Disk Properties** section, select a virtual device node.
 - o If you want to replace an existing virtual disk, select an occupied virtual node.
 - o If you want to attach the restored disk to the VM as a new drive, select a node that is not occupied yet.

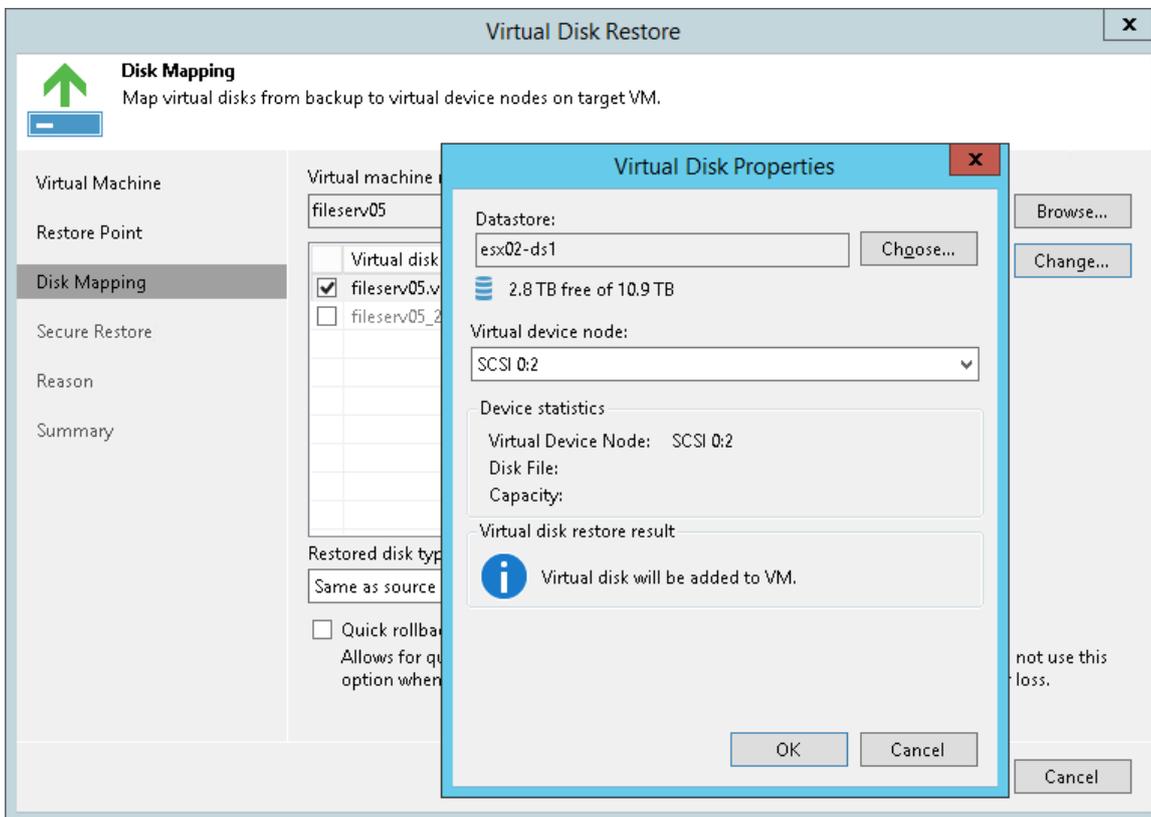
5. Veeam Backup & Replication preserves the format of the restored virtual hard disks. To change disk format, select the required option from the Restore disks list – same as original, thin, thick lazy zeroed or thick eager zeroed. For more information about disk types, see [VMware Docs](#).

NOTE:

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

6. [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 & Replication will query CBT to get 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 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 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.



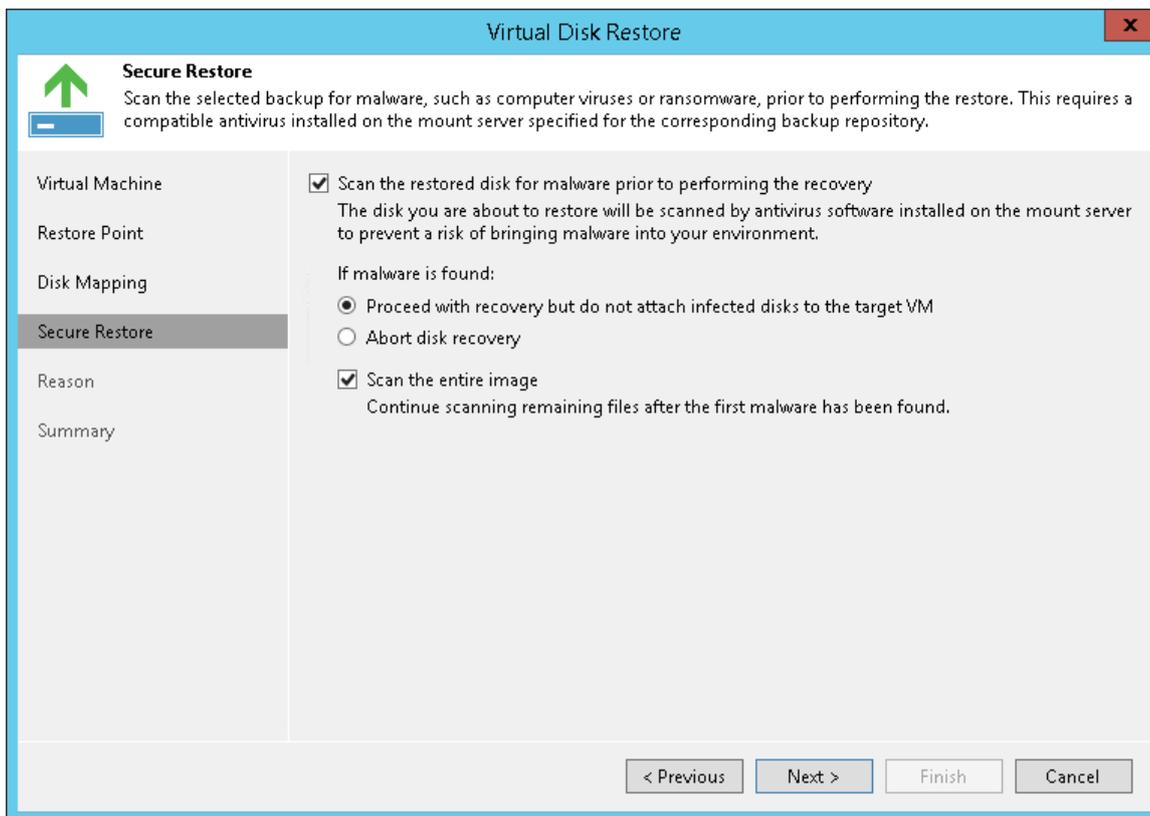
Step 5. Specify Secure Restore Settings

At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore – scan virtual disk data with antivirus software before restoring the disk. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

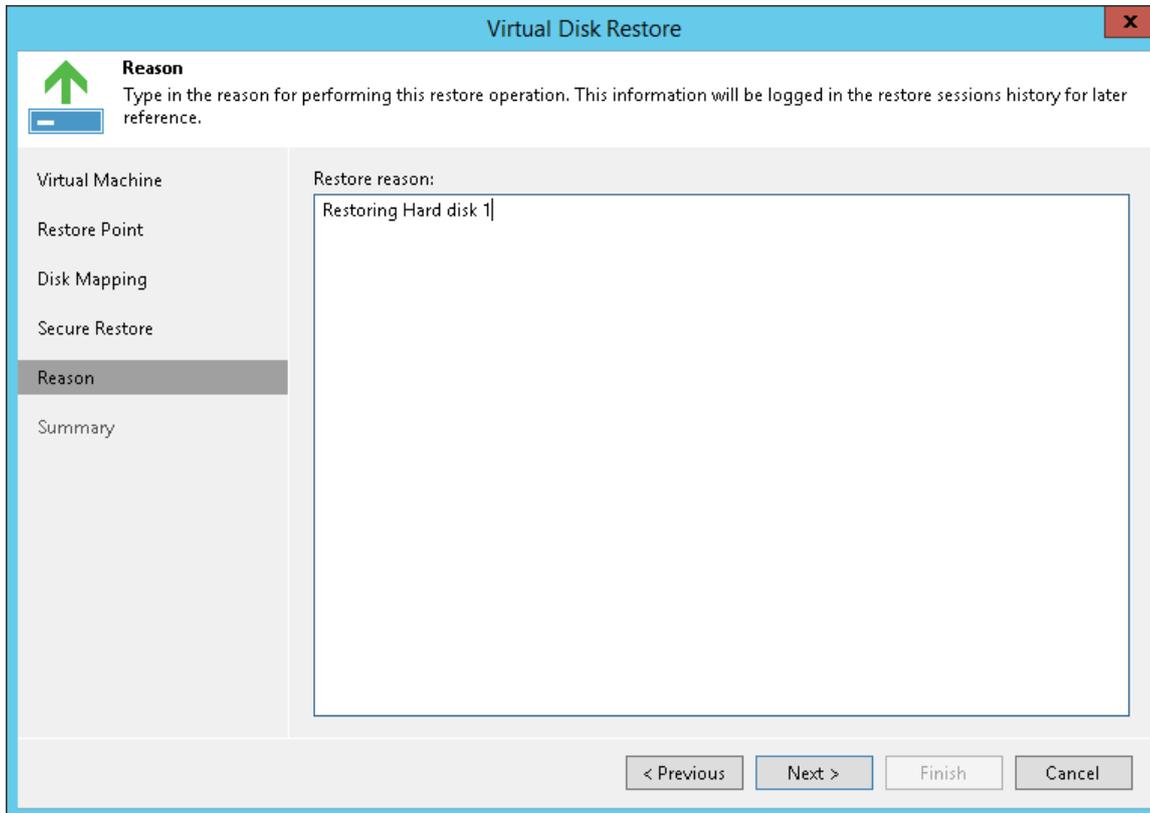
1. At the **Secure Restore** step of the wizard, select the **Scan the restored disk for malware prior to performing the recovery** check box.

2. Select which action Veeam Backup & Replication will take if the antivirus detects a virus threat:
 - **Proceed with recovery but do not attach infected disks to the target VM.** Select this action if you want to continue the virtual disk restore. In this case, the restored disk will not be attached to the target VM.
 - **Abort disk recovery.** Select this action if you want to cancel the restore session.
3. Select the **Scan the entire image** check box if you want the antivirus to continue the virtual disk scan after the first virus threat is detected. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).



Step 6. Specify Restore Reason

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



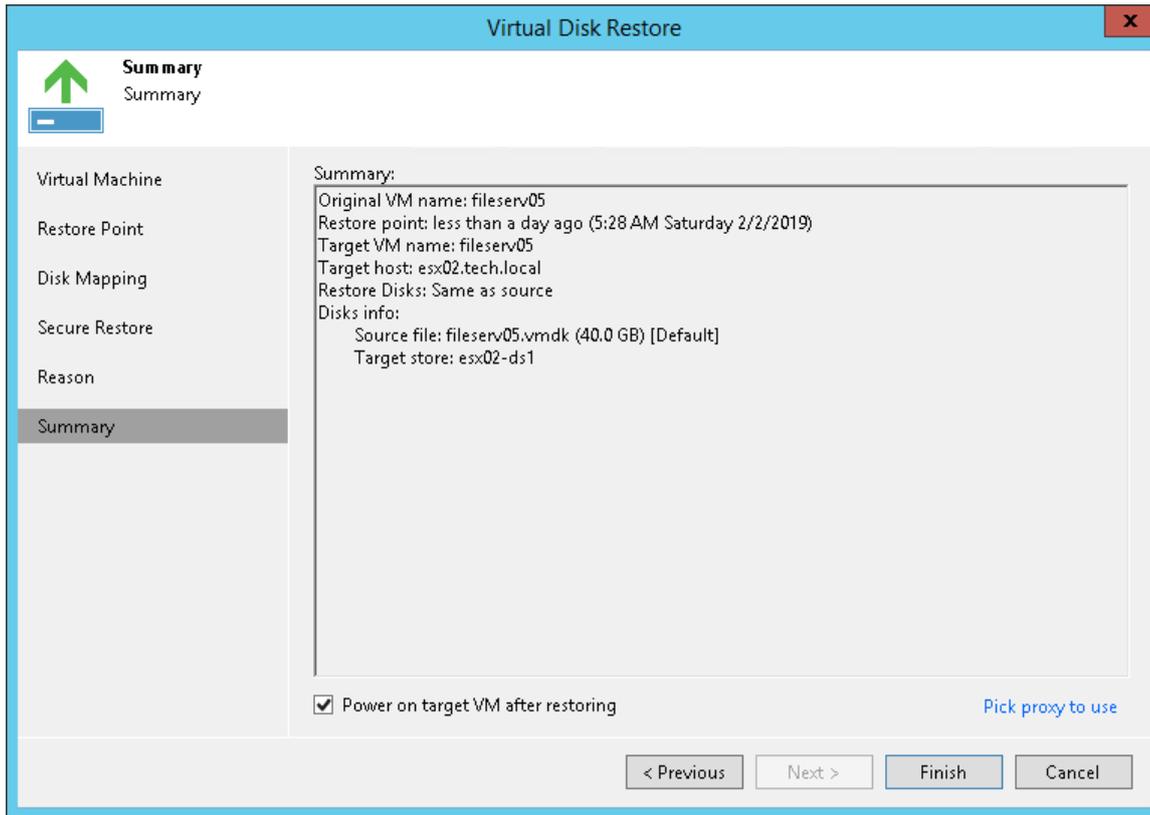
Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, complete the procedure of VM disks restore.

1. Review details for the restore task.
2. To start a VM immediately after the restore process, select the **Power on VM after restoring** check box.
3. Click the **Pick proxy to use** link to select backup proxies over which VM data must be transported to the target datastore. You can assign backup proxies explicitly or instruct Veeam Backup & Replication to automatically select backup proxies.
 - If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that have access to the source datastore and will automatically assign optimal proxy resources for processing VM data.

During the restore process, VM hard disks are processed simultaneously. Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use for writing data to target, current workload on these backup proxies, and selects the most appropriate resources for VM hard disk processing.
 - If you choose **Use the selected backup proxy servers only**, you can explicitly select backup proxies that must be used for restore. It is recommended that you select at least two backup proxies to ensure that VM hard disks are recovered if one of backup proxies fails or loses its connectivity to the target datastore during restore.

4. Click **Finish** to start VM disks restore.



EC2 Instance Disks Export

Veeam Backup & Replication allows you to restore disks of Amazon EC2 instances from backups created with [N2WS Backup & Recovery](#). You can restore disks in the VMDK, VHD or VHDX format.

During disk restore, Veeam Backup & Replication creates standard virtual disks that can be used by VMware vSphere and Microsoft Hyper-V VMs.

- When you restore a disk in the VMDK format, Veeam Backup & Replication creates a pair of files that make up the VM virtual disk: a descriptor file and file with the virtual disk content.
- When you restore a disk in the VHD/VHDX format, Veeam Backup & Replication creates a file of the VHD or VHDX format.

You can save converted disks locally on any server added to the backup infrastructure or place disks on a datastore connected to an ESX(i) host (for VMDK disk format only). VMDK disks can be restored as thin provision and thick disks:

- Disks restored to a datastore are saved in the thin provisioned format.
- Disks restored to a server are saved in the thick format.

VHD/VHDX disks are always restored as dynamically expanding.

Veeam Backup & Replication supports batch disk restore. For example, if you choose to restore 2 instance disks, Veeam Backup & Replication will convert them to 2 virtual disks and store these disks in the specified location.

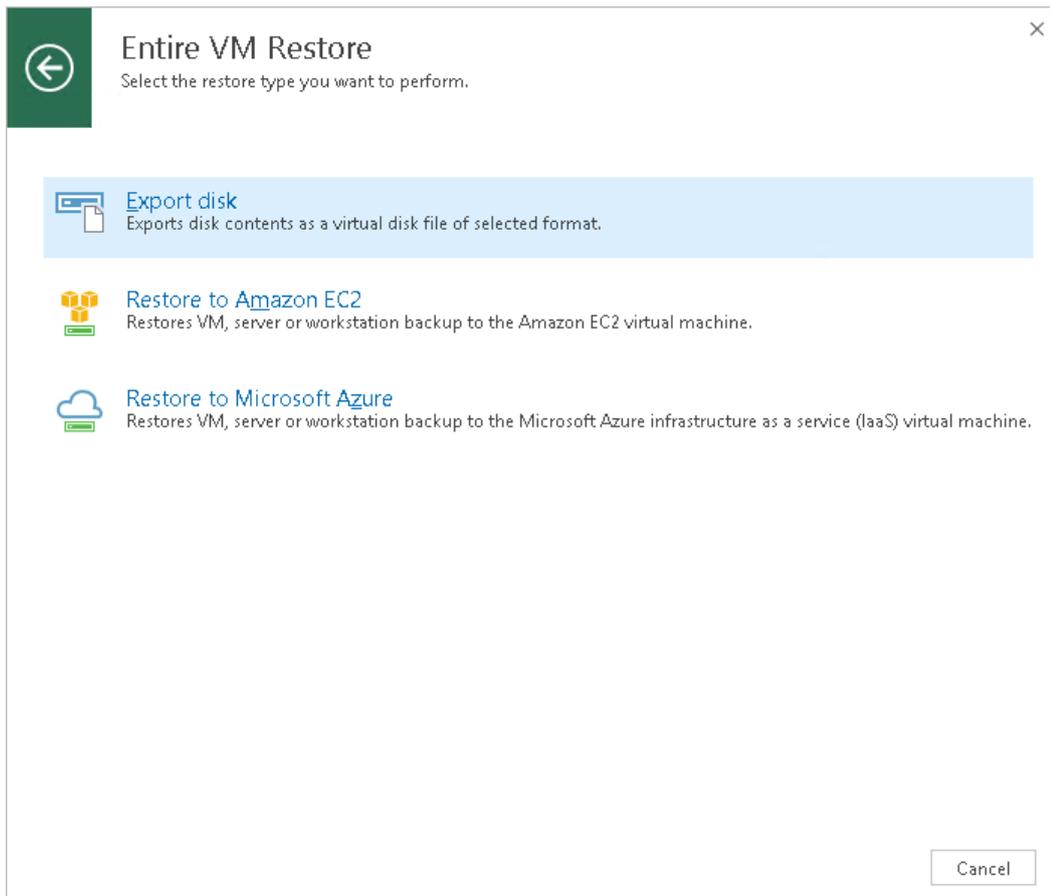
Exporting Disks

To restore disks of Amazon EC2 instances and convert them to the VMDK, VHD or VHDX format, use the **Export Disk** wizard.

Step 1. Launch Export Disk Wizard

To launch the **Export Disk** wizard, do the following:

- Open the **Home** tab.
- Click **Restore > Amazon EC2 > Entire machine restore > Export disk**.



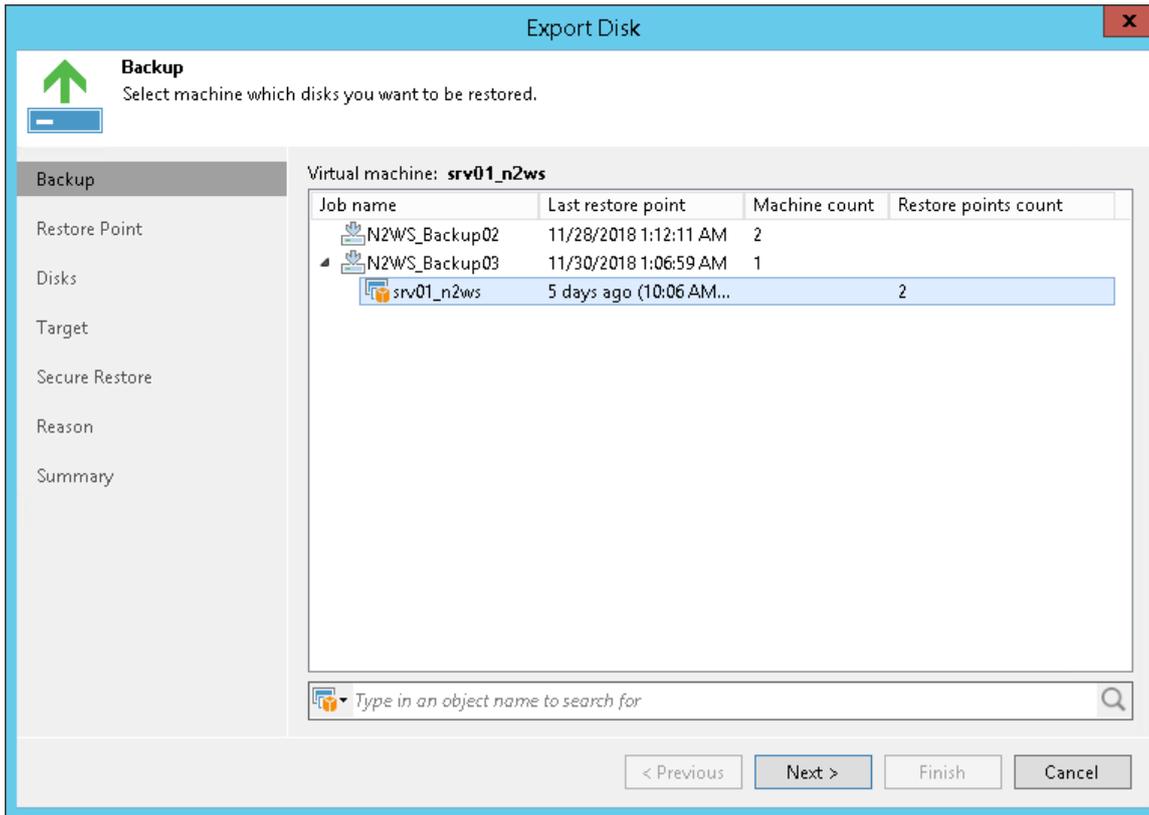
Step 2. Select Backup

At the **Backup** step of the wizard, select an Amazon EC2 instance whose disks you want to restore.

To quickly find an instance, you can use the search field at the bottom of the window.

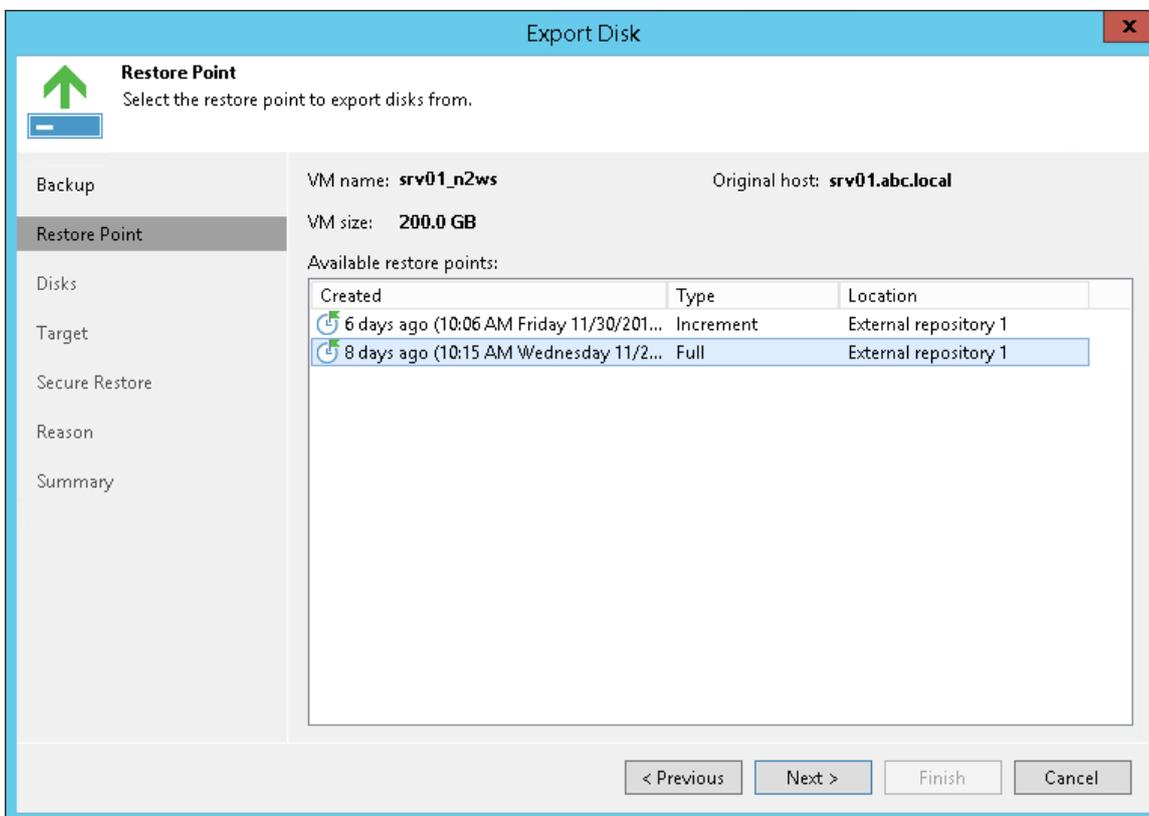
1. Enter an instance name or a part of it in the search field.

2. Click the **Start search** button on the right or press **[ENTER]**.

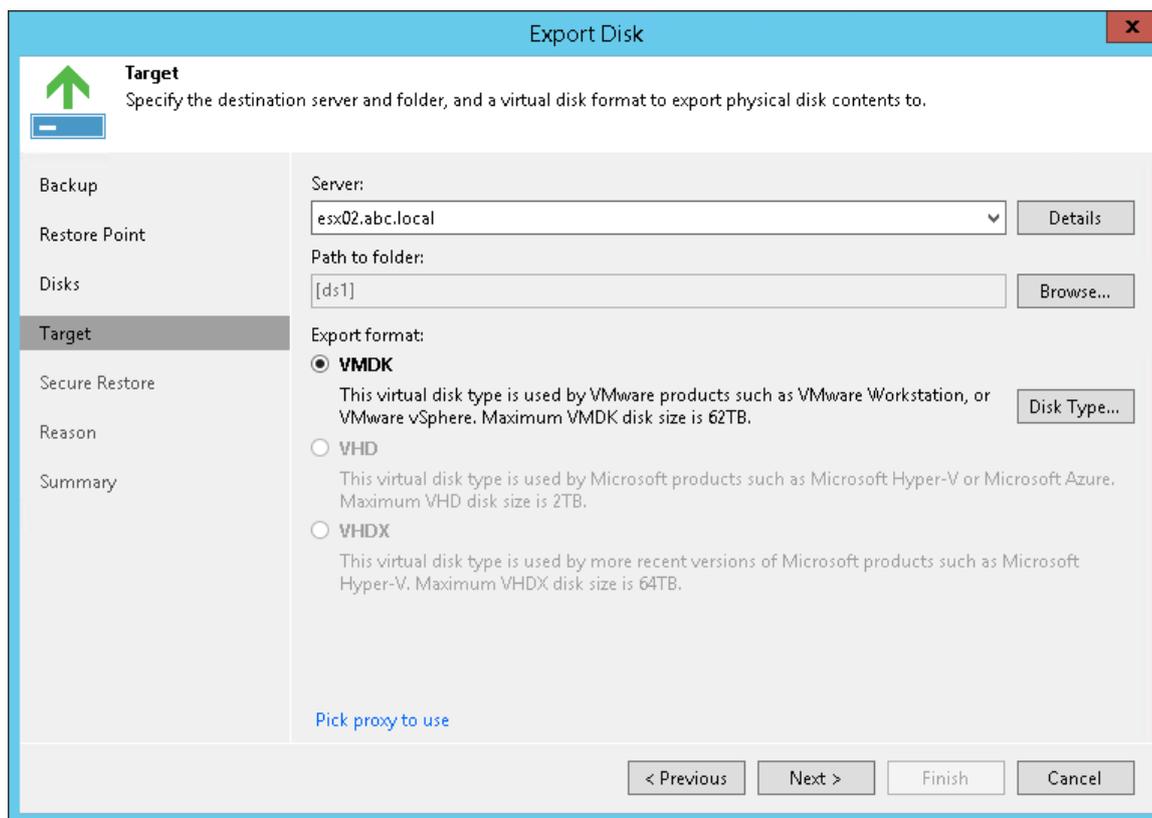


Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point from which you want to restore disks.



4. [For VMDK virtual disks] Click the **Pick proxy to use** link to select backup proxies over which disk data must be transported to the target datastore. You can assign backup proxies explicitly or instruct Veeam Backup & Replication to automatically select backup proxies.



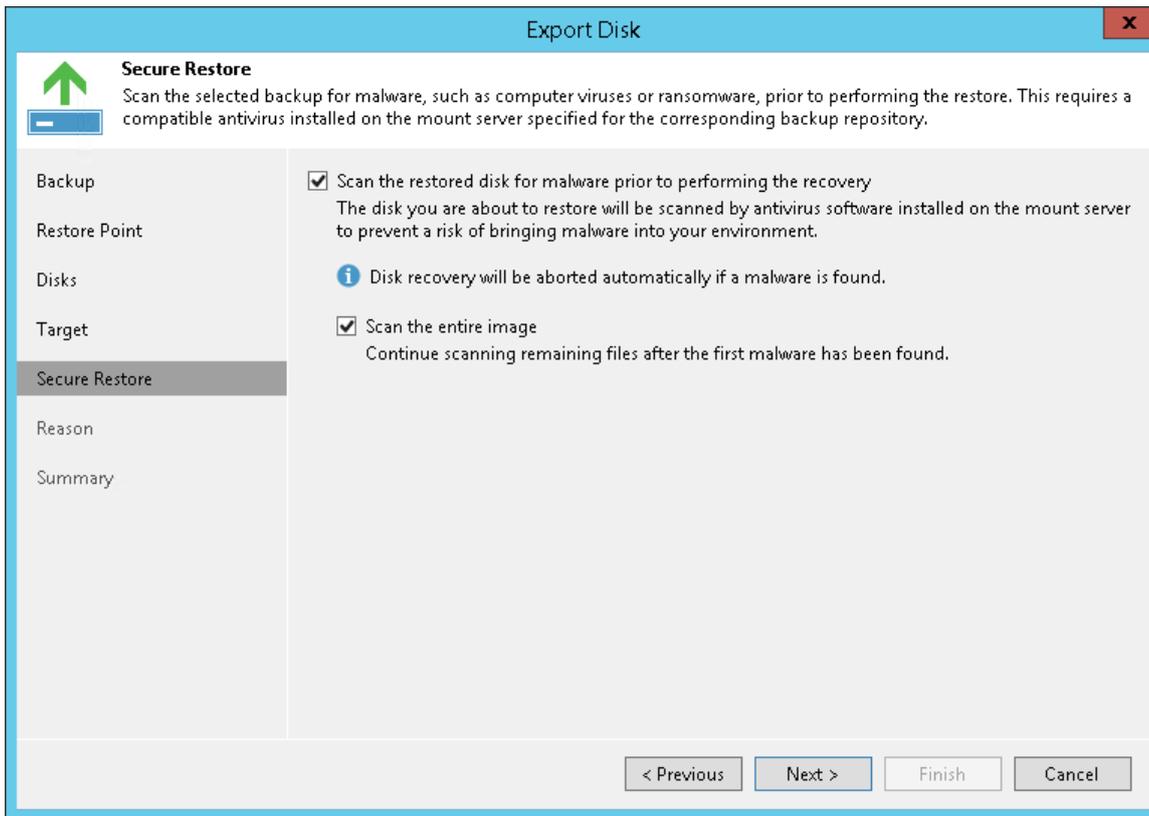
Step 6. Specify Secure Restore Settings

At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore – scan restored disk data with antivirus software before restoring the disk. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

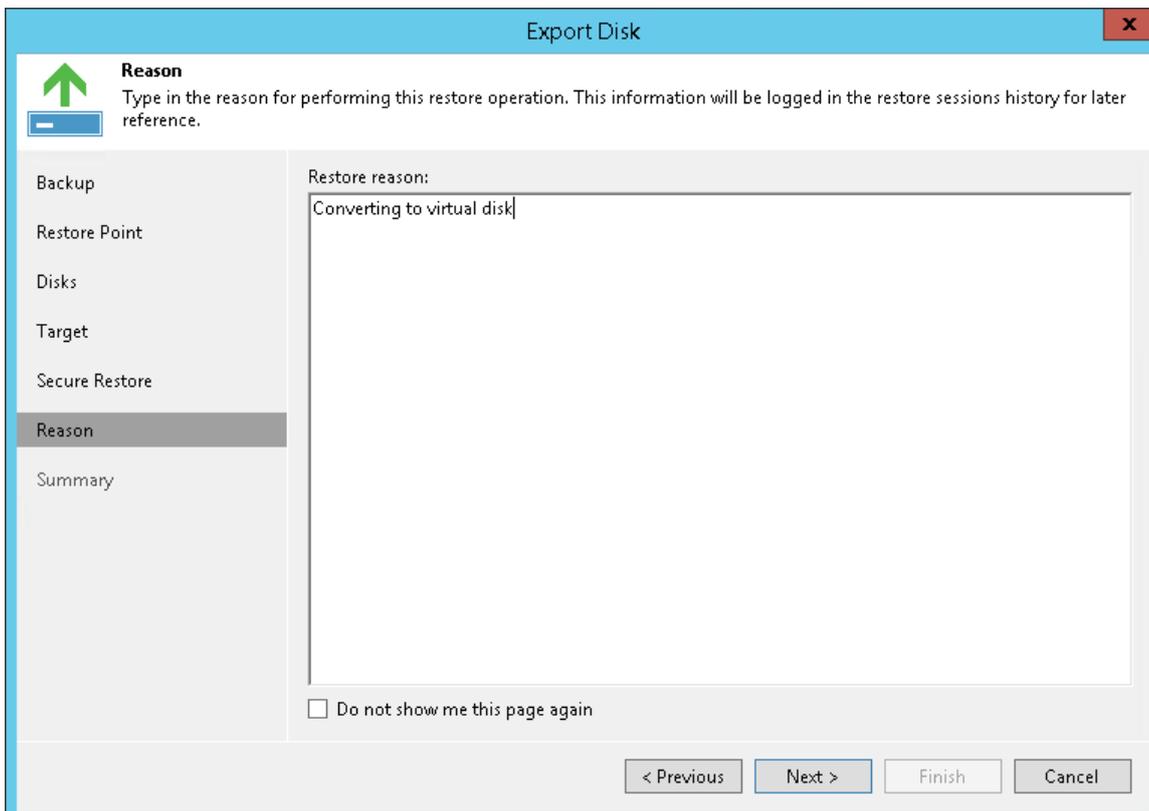
1. At the **Secure Restore** step of the wizard, select the **Scan the restored disk for malware prior to performing the recovery** check box.

2. Select the **Scan entire image** check box if you want the antivirus software to continue disk scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).



Step 7. Specify Restore Reason

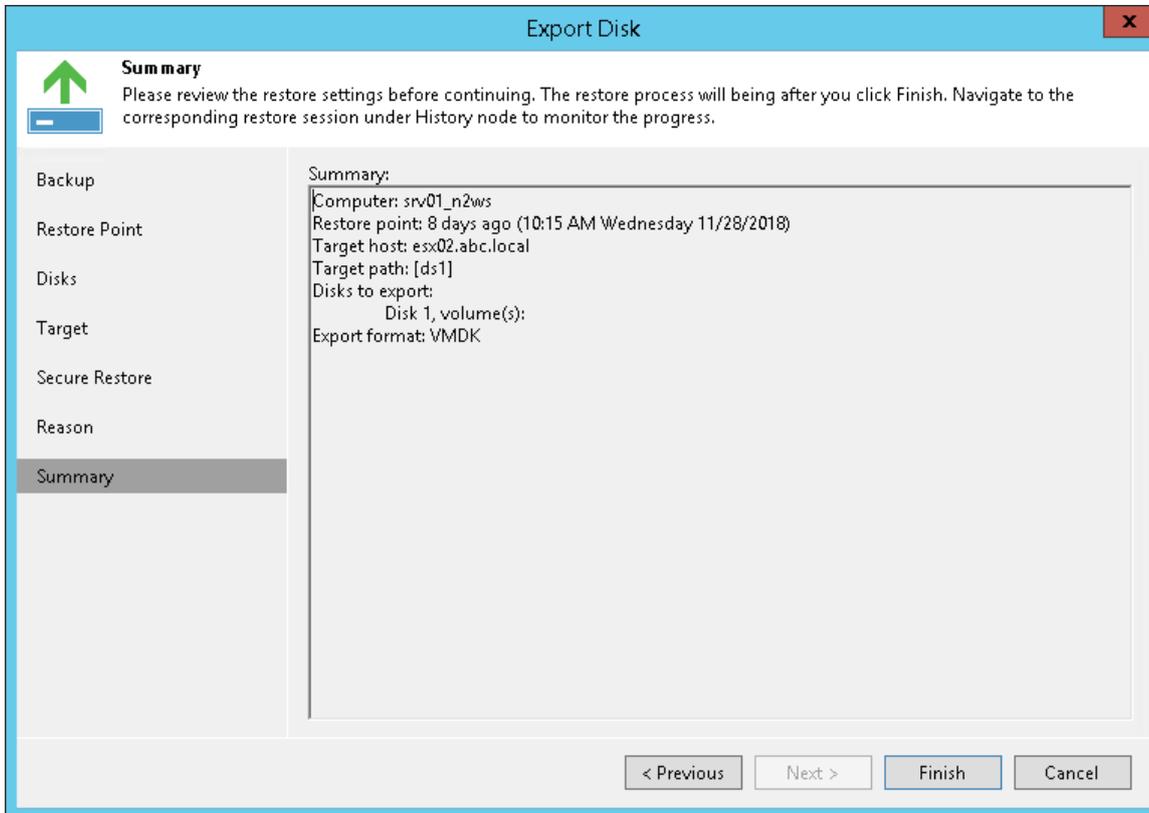
At the **Reason** step of the wizard, enter a reason for disk restore.



Step 8. Complete Restore Process

At the **Summary** step of the wizard, complete the disk restore procedure.

1. Review details for disks that will be restored.
2. Click **Finish** to start the restore procedure and exit the wizard.



Guest OS File Recovery

You can use IFLR (Instant File-Level Restore) to recover individual VM guest OS files and folders from VM backups and replicas. IFLR does not require you to extract the VM image to a staging location or start the VM prior to restore. You can restore files and folders directly from a regular image-level backup or replica to the necessary point in time.

IFLR works with any VM guest OS file system. Veeam Backup & Replication offers different tools and methods for different file systems:

- [Restore from FAT, NTFS or ReFS](#): for file-level restore from Microsoft Windows VMs with NTFS, FAT and ReFS file systems, you can use the **File-Level Restore** wizard.
- [Restore from Linux, Unix and Other File Systems](#): for file-level restore from Linux, Solaris, BSD, Novell Storage Services, Unix, Mac and other file systems, you can use the multi-OS **File-Level Restore** wizard.

Note that multi-OS file-level restore supports recovery of files and folders only. Recovery of other file system objects such as pipes is not supported.

- [Restore from Other File Systems](#): for file-level restore from file systems not supported by file-level restore wizards, you can leverage the Instant VM Recovery functionality.

Restore from FAT, NTFS or ReFS

To restore individual files and folders from FAT, NTFS and ReFS file systems, you can use the **File-Level Restore** wizard.

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

1. Veeam Backup & Replication mounts VM disks from the backup or replica to the mount server under the `C:\VeeamFLR\ folder. For more information on the mount server, see Mount Server.`

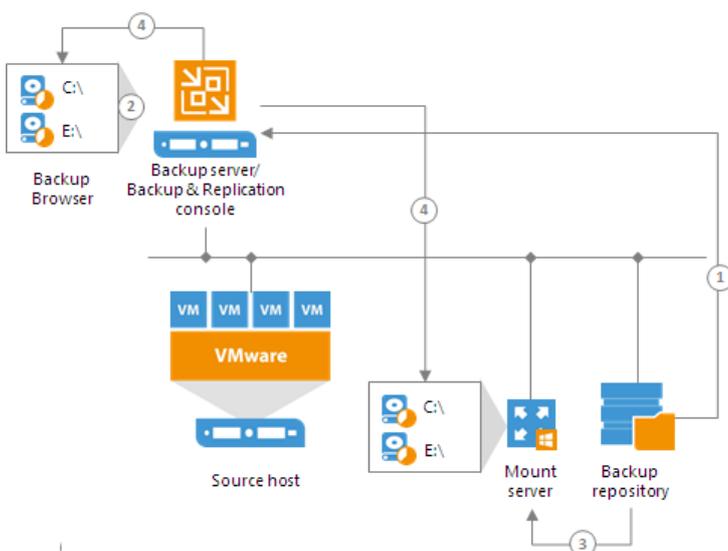
For accessing VM disks content, Veeam Backup & Replication uses a separate program – Virtual Disk Driver (VDK) that is provided with the product. VM disks are not physically extracted from the backup file or VM replica. Veeam Backup & Replication emulates their presence on the backup server or Veeam Backup & Replication console. The backup file or VM replica itself remains in the read-only state.

2. Veeam Backup & Replication launches the Veeam Backup browser where mounted VM disks are displayed. You can browse the VM guest file system in the Veeam Backup browser.
3. If you restore files to the original location, Veeam Backup & Replication creates an additional mount point on the mount server associated with the backup repository on which the backup file resides. The mount server is typically located close to the backup repository. The second mount point lets Veeam Backup & Replication route for VM data in an optimal way and reduce load on the network.

As a result, restored files data travels in the following way:

- In the restore to original scenario – from the mount server to the original location. The first mount point here is used only for browsing the VM guest file system.
 - In the restore to new location scenario – from the backup server or Veeam Backup & Replication console to the specified new location.
4. When the restore process is finished or the Veeam Backup browser is closed by timeout, Veeam Backup & Replication removes mount points from the backup server or machine on which the Veeam Backup & Replication console is installed and from the mount server (if the second mount was used).

Depending on the restore scenario, Veeam Backup & Replication may create mount points on different backup infrastructure components. For more information, see [File-Level Restore Scenarios](#).



File-Level Restore Scenarios

You can use different scenarios for file-level restore:

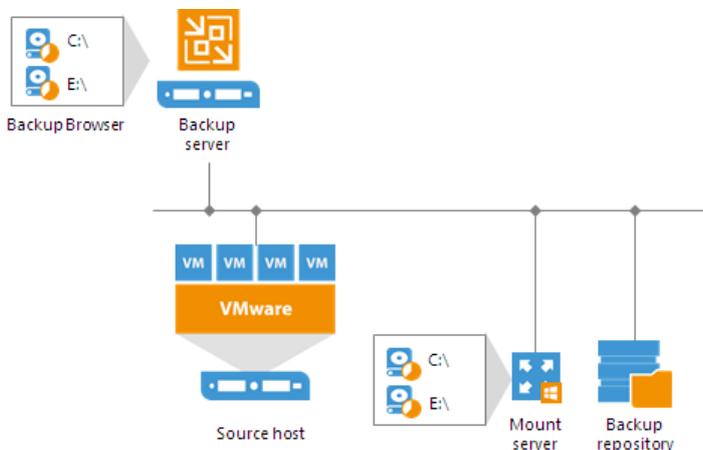
- [Restore files from backups](#)
- [Restore files from replicas](#)
- [Restore files from storage snapshots](#)
- [Restore files for work with Veeam Explorers](#)
- [Restore files from Veeam Backup Enterprise Manager](#)

In different restore scenarios, Veeam Backup & Replication uses different servers as mount points.

Restoring Files from Backups

When you restore files from backups that reside on the backup repository, Veeam Backup & Replication uses the following mount points:

1. Veeam Backup & Replication mounts disks of the VM from the backup file to the machine where the restore process is launched. This can be the backup server or machine on which the Veeam Backup & Replication console is installed. This mount point allows you to browse the VM file system.
2. If you restore files to the original location, Veeam Backup & Replication creates an additional mount point on the mount server associated with the backup repository on which the backup file resides. The second mount lets you keep the VM traffic in one site and reduce load on the network.



If you restore files to a new location (perform the **Copy to** operation), Veeam Backup & Replication does not create the second mount point. It copies files to the destination from the backup server or Veeam Backup & Replication console machine.

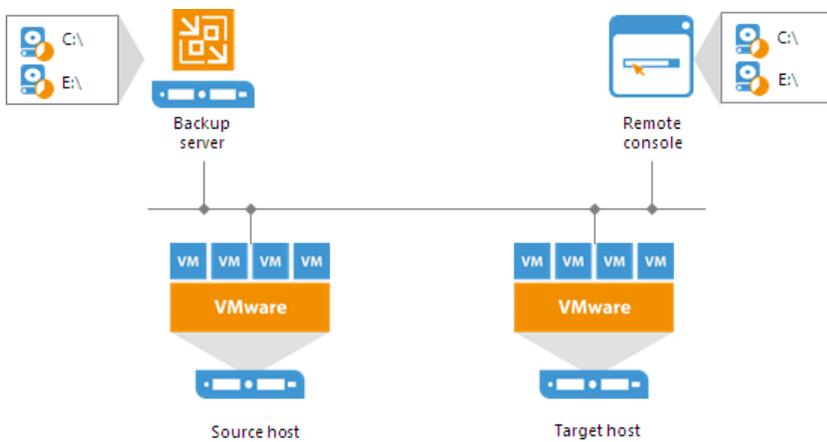
NOTE:

Backup files on HPE StoreOnce are locked exclusively by a restore task. For this reason, Veeam Backup & Replication uses only one mount point on the backup server or Veeam Backup & Replication console machine for backups on HPE StoreOnce.

Restoring Files from Replicas

When you restore files from a VM replica, Veeam Backup & Replication uses the following mount points:

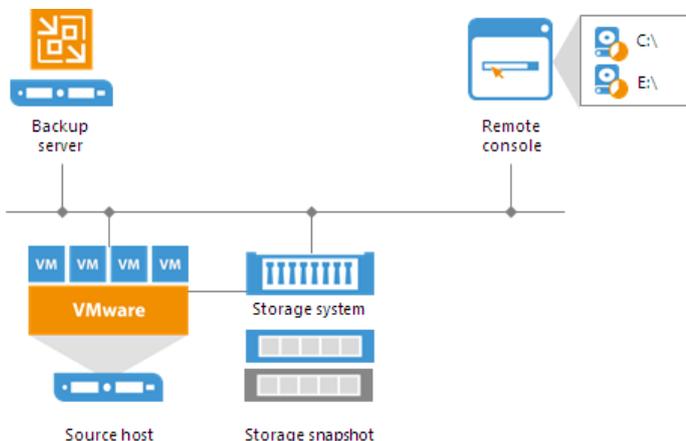
1. Veeam Backup & Replication mounts disks of the VM replica to the machine where the restore process is launched. This can be the backup server or machine on which the Veeam Backup & Replication console is installed. This mount point allows you to browse the VM file system.
2. If you start the restore process from the Veeam Backup & Replication console and restore files to the original location, Veeam Backup & Replication creates an additional mount point on the backup server.



If you start the restore process on the backup server or restore files to a new location (perform the **Copy to** operation), Veeam Backup & Replication does not create the second mount point. It copies files to the destination from the backup server or Veeam Backup & Replication console machine.

Restoring Files from Storage Snapshots

When you restore files from storage snapshots, Veeam Backup & Replication uses one mount point on the backup server or Veeam Backup & Replication console machine.

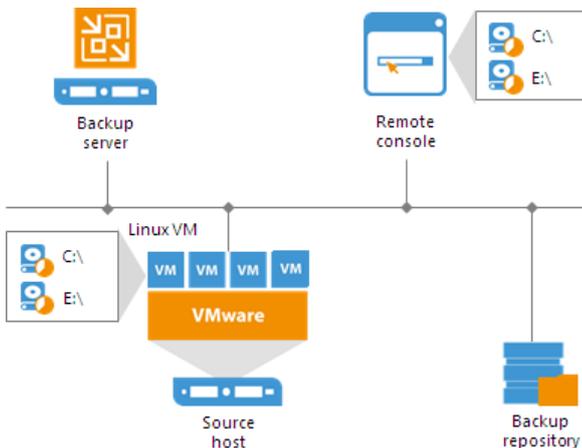


Restoring Files for Veeam Explorers

Veeam Backup & Replication can perform file-level restore as a preparatory step for application items restore. However, the database files may be huge and require a lot of network resources. For this reason, if you restore application items from Microsoft SQL and Oracle VMs, Veeam Backup & Replication can mount the content of the backup file directly to the original VM.

For restore from backups of Microsoft SQL Server VMs or Oracle VMs, Veeam Backup & Replication creates an additional mount point on the original VM. In some cases, Veeam Backup & Replication may create an additional mount point on a staging Microsoft SQL Server or Oracle server. This may be required if Veeam Backup & Replication does not have information about databases (for example, if you initiate restore from storage snapshots) or you restore Microsoft SQL Server or Oracle databases or Microsoft SQL Server database schema objects and table data up to a specific transaction.

- To create a mount point on Microsoft Windows machines, Veeam Backup & Replication uses the iSCSI protocol. The remote machine or staging server acts as an iSCSI initiator. The machine on which the Veeam Explorer runs acts as an iSCSI target. The iSCSI mount point is non-persistent – it is created only for duration of the restore process.
- To create a mount point on Linux VMs (for Oracle running on Linux), Veeam Backup & Replication uses fuse.

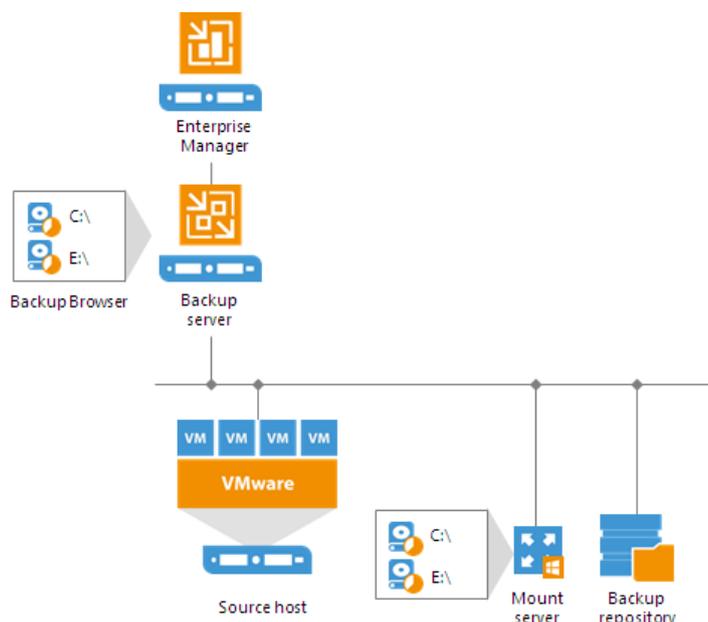


Restoring Files from Veeam Backup Enterprise Manager

When you restore files from the backup file that was created without VM guest OS file indexing, Veeam Backup & Replication uses the following mount points:

1. Veeam Backup & Replication mounts disks of the VM from the backup file to the backup server.

- If you restore files to the original location, Veeam Backup & Replication creates an additional mount point on the mount server associated with the backup repository on which the backup file resides. The second mount lets you keep the VM traffic in one site and reduce load on the network.



If you select to download files, Veeam Backup & Replication does not create the second mount point. It copies files to the destination from the backup server.

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

You can restore individual Microsoft Windows guest OS files from the backup or replica of a Microsoft Windows VM.

Before restoring VM guest OS files, [check prerequisites](#). Then use the **File Level Restore** wizard to restore the necessary VM guest OS files and folders.

Before You Begin

Requirements

- You can restore VM guest OS files from a backup or replica that has at least one successfully created restore point.
- The mount server must have access to the VM guest OS (if file-level restore is performed over the network) or vCenter Server (if file-level restore is performed over VIX).
- [Restore to original location] VM guest OS must be accessible from the backup server over the network.
- [Restore to initial location] VMware Tools must be installed on the target VM.

ReFS

If you plan to restore files from a VM running Microsoft Windows ReFS, for the restore process you must use Veeam Backup & Replication components running the following OSes:

- [For VM file system browsing and file copy to another location] The Veeam Backup & Replication console must be installed on a machine running Microsoft Windows Server 2012 or later.

- [For restore to the original location] The Veeam Backup & Replication console and the mount server associated with the backup repository where backup files reside must be installed on a machine running Microsoft Windows Server 2012 or later.
- The version of the Windows Server on the mount host and machine with Veeam Backup & Replication console must be the same as the version of guest OS or later.
- [ReFS 3.x] If you plan to restore files from a VM running Microsoft Windows ReFS 3.x, the Veeam Backup & Replication console and mount server must be installed on machines running Microsoft Windows Server 2016 or later and specific ReFS version must be supported.

Data Deduplication

If you plan to restore files from a VM running Microsoft Windows Server 2012 or later and Data Deduplication is enabled for some VM volumes, for the restore process you must use Veeam Backup & Replication components running the following OSes:

- [For copy to another location operations] The Veeam Backup & Replication console must be installed on a machine running Microsoft Windows Server 2012 or later. Data Deduplication must be enabled on this machine.
- [For restore to the original location] The Veeam Backup & Replication console and mount server associated with the backup repository where backup files reside must be installed on a machine running Microsoft Windows Server 2012 or later. Data Deduplication must be enabled on the mount server.
- The version of the Windows Server on the mount host and machine with Veeam Backup & Replication console must be the same as the version of guest OS or later.

Limitations

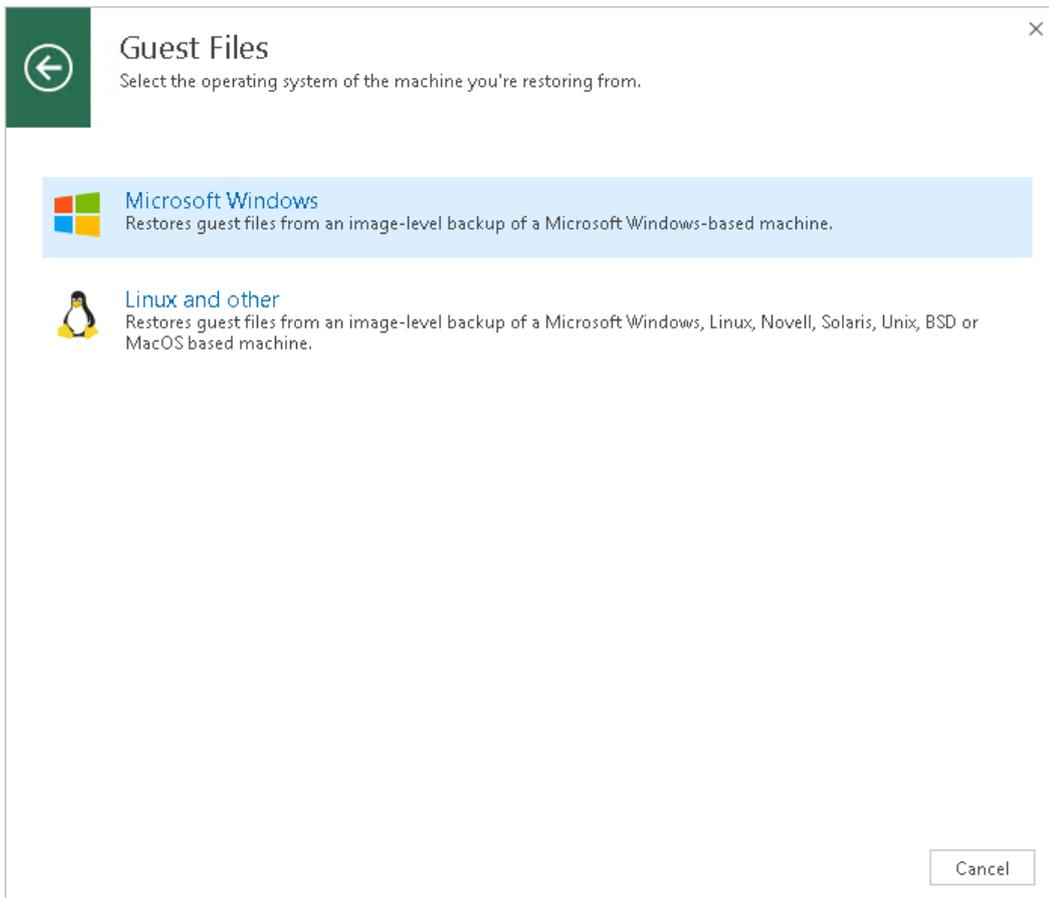
- Processing of reparse points is supported only for NTFS.
- You cannot restore files from a backup created in the reverse incremental mode if the backup job is being performed. If the backup is created in the incremental backup mode and the backup job is being performed, you can restore files from any available restore point.
- You cannot restore VM guest OS files from a running replica or if the replication job with the necessary VM is being performed.

Step 1. Launch Restore Wizard

To launch the **File Level Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from backup** or **Restore from replica > Guest files restore > Microsoft Windows**.
- Open the **Home** view. In the inventory pane, select **Backups** or **Replicas**. In the working area, expand the necessary backup and do one of the following:
 - Click the VM whose files you want to restore and click **Guest files > Microsoft Windows** on the ribbon.
 - Right-click the VM whose files you want to restore and select **Restore guest files > Microsoft Windows**.
- Double-click the VBK or VBM file (for example, in Microsoft Windows Explorer). In the displayed window, select the VM and click **Restore > Guest files (Microsoft Windows)**.

You can use this option if you perform restore on the backup server. You cannot use this option if you perform restore remotely over the Veeam Backup & Replication console.



Step 2. Select VM

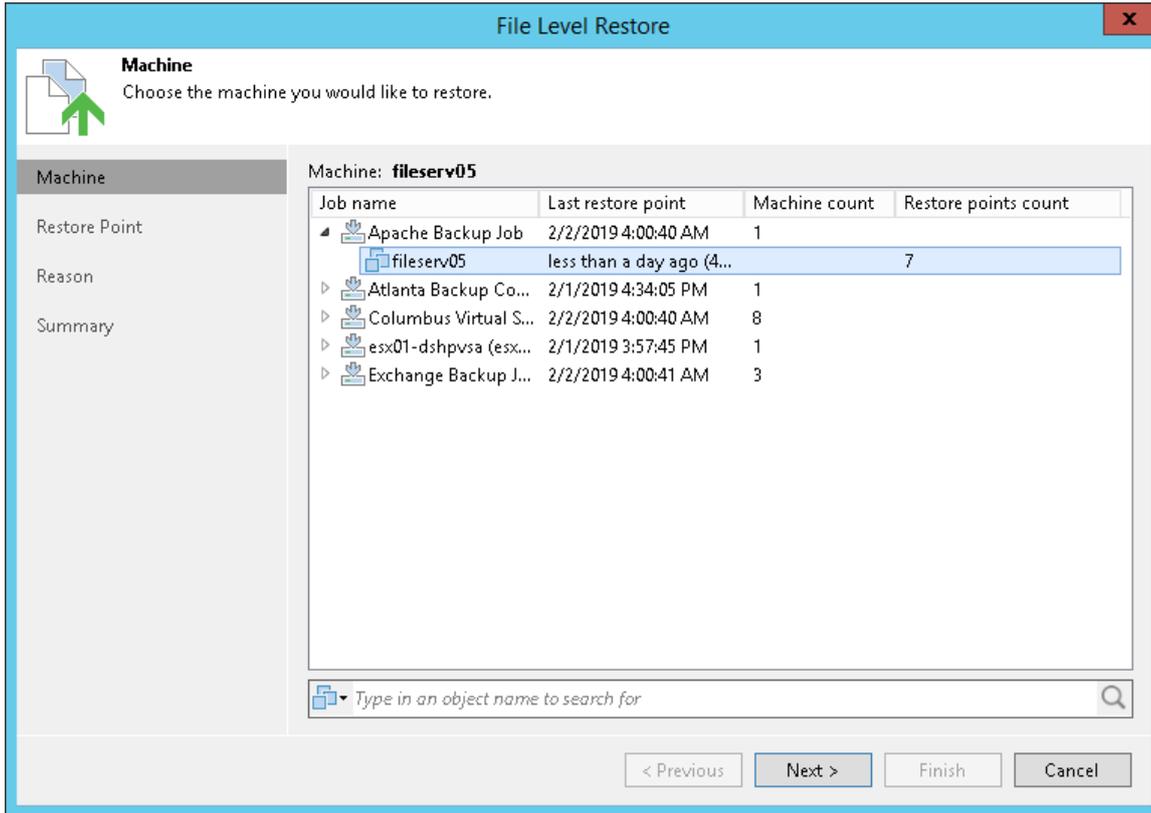
At the **Machine** step of the wizard, select the VM whose guest OS files you want to restore:

1. In the **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 the VM name or a part of it in the search field.

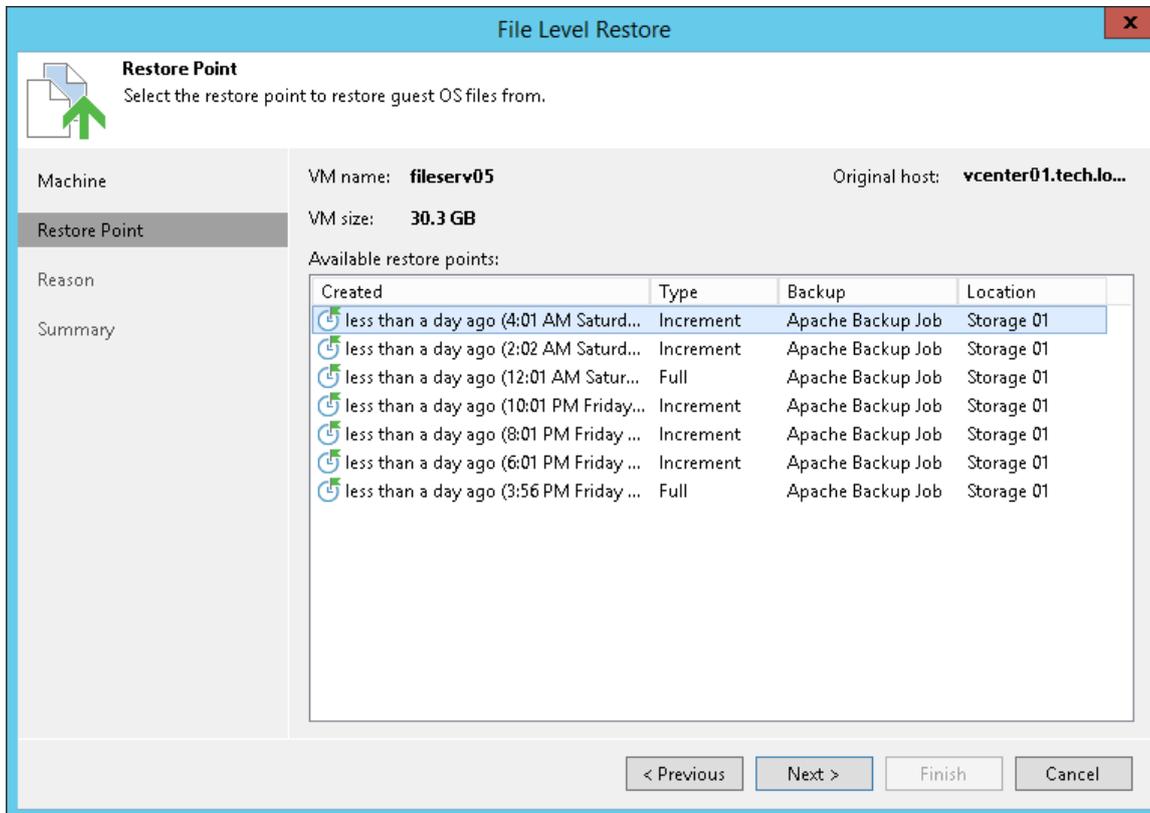
2. Click the **Start search** button on the right or press [ENTER].



Step 3. Select Restore Point

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

In the **Location** column, you can view a name of a regular backup repository or cloud repository where a restore point resides.

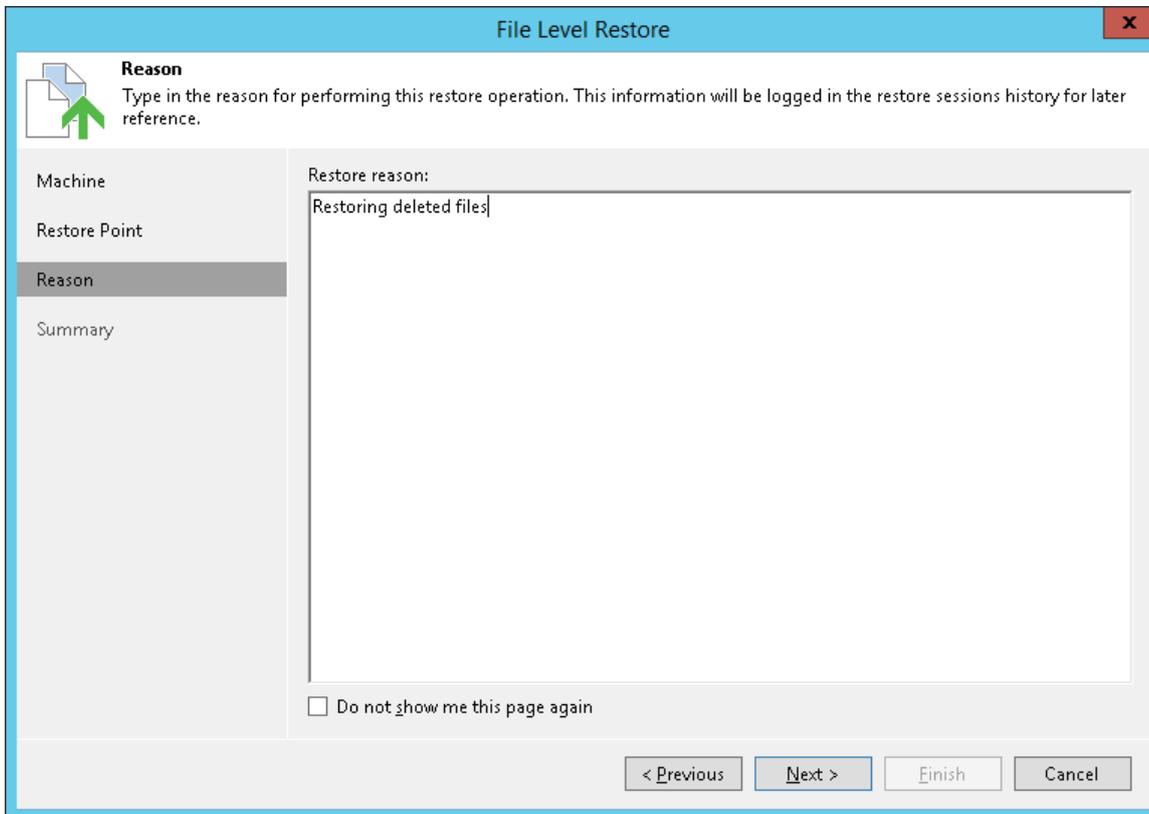


Step 4. Specify Restore Reason

At the **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 **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

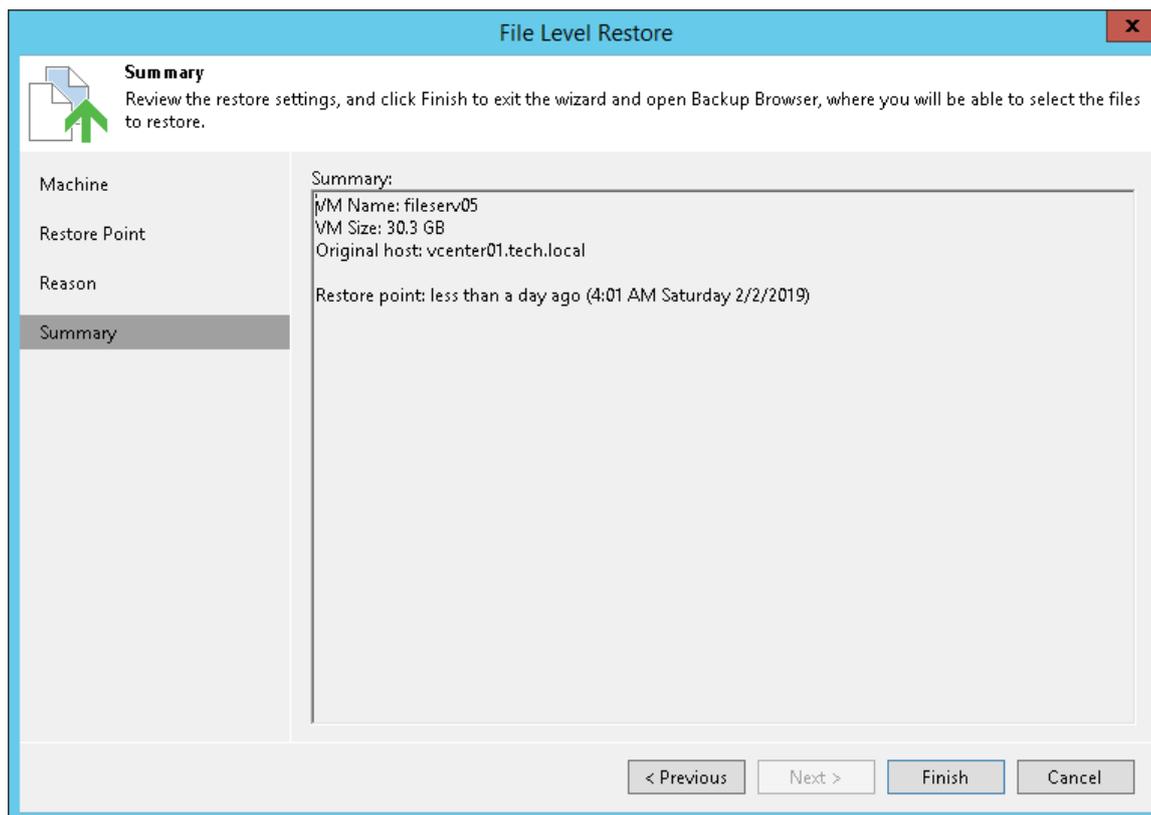


Step 5. Finish Working with Wizard

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 or replica.



Step 6. Save Restored Files

When the restore process is complete, Veeam Backup & Replication 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:

- [Restore 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](#).

Restoring Files to Original Location

To restore a file or folder to its original location, in the Veeam Backup browser right-click the file or folder 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 & Replication will add the *RESTORED-* prefix to the original file name and store the restored file in the same folder where the original file resides.

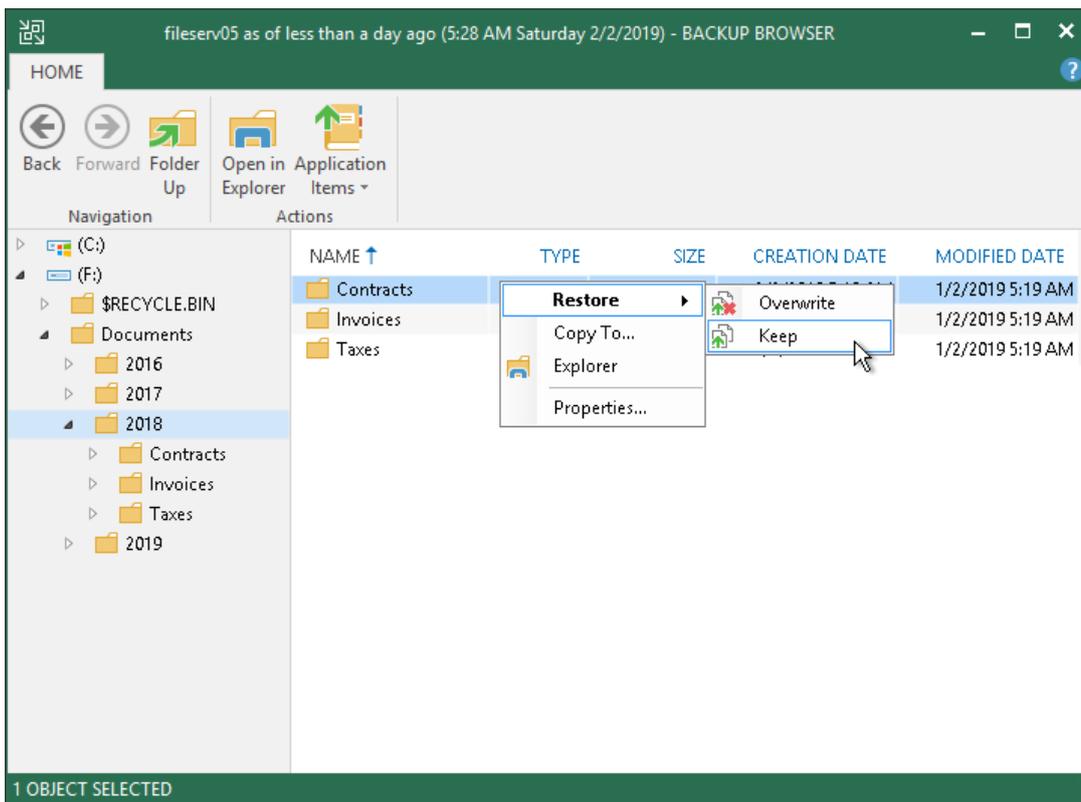
If the file with the *RESTORED-* prefix already exists in the original location, Veeam Backup & Replication will name the restored file in the following format: *RESTORED-
<filename>_YYYYMMDD_HHMMSS*.

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.
- Application-aware processing is not supported for the Microsoft Windows OS of the initial VM.

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.

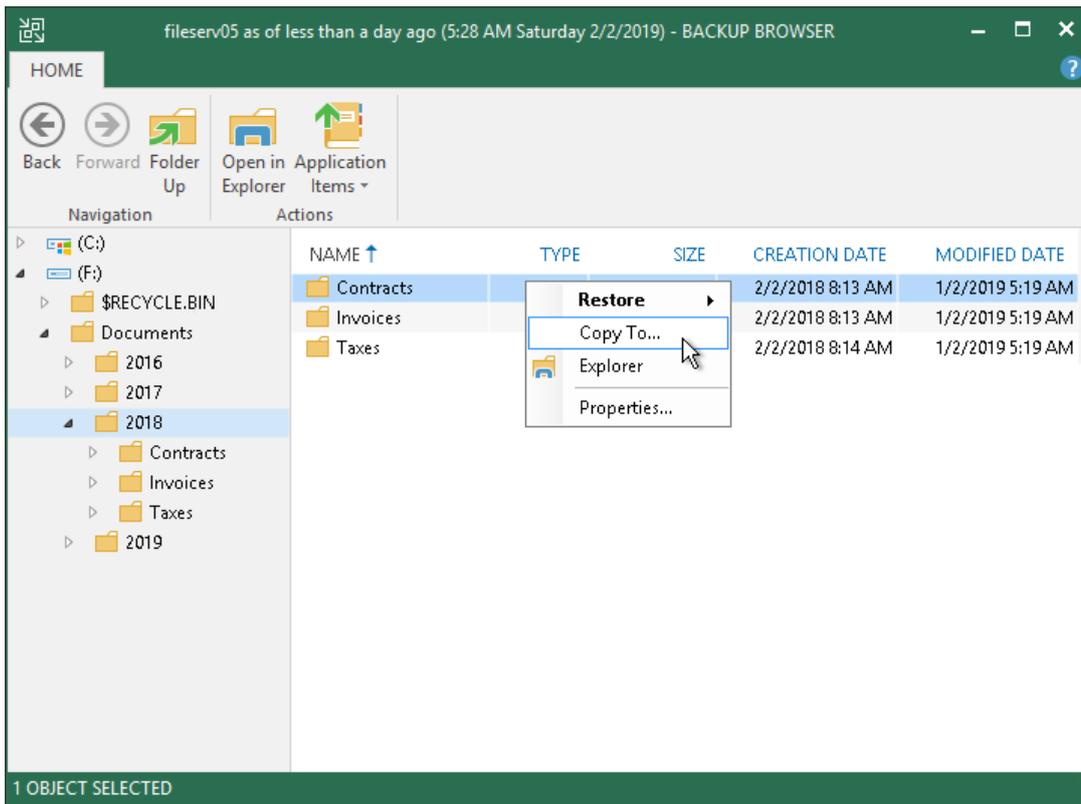


Saving Files to a New Location

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 & Replication 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 & Replication will change security settings: the user who launched the Veeam Backup & Replication 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.

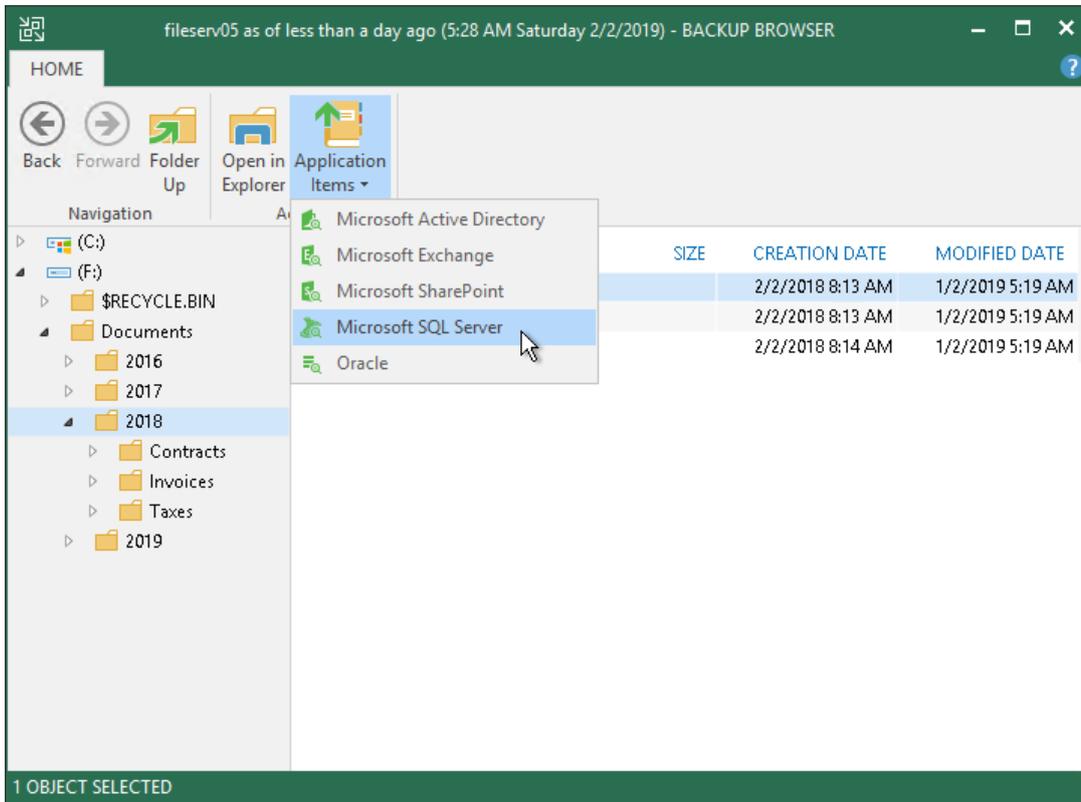


Launching Veeam Explorers

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 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 [Microsoft Docs](#).



Working with Windows Explorer

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

- Click **Open in Explorer** on the ribbon in the Veeam Backup browser or right-click the necessary folder and select **Explorer**.
- Veeam Backup & Replication 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\ folder of the machine where the Veeam Backup & Replication console is installed.`

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:

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

If you open the VM file system in the Microsoft Windows Explorer, these capabilities will not be available. For more information, see [Microsoft Docs](#).

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 & Replication unmounts VM disks from the machine where the Veeam Backup & Replication console is installed and mount server (if you have restored VM guest OS files to the original location).

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

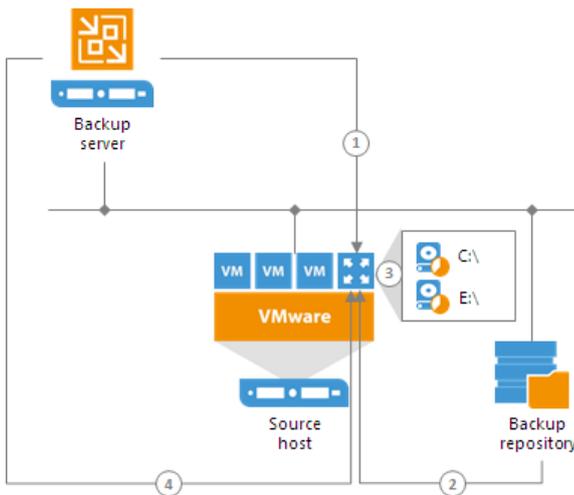
Restore from Linux, Unix and Other File Systems

To restore individual files and folders from file systems other than Microsoft Windows, you can use the multi-OS **File-Level Restore** wizard.

To restore files from VM guest OS, Veeam Backup & Replication uses a helper appliance. The helper appliance is a helper VM running a stripped down Linux kernel that has a minimal set of components. The appliance is quite small – around 50 MB. It requires 1024 MB RAM and takes around 10 seconds to boot.

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

1. Veeam Backup & Replication deploys a helper appliance on the ESX(i) host in the virtual infrastructure.
2. Veeam Backup & Replication mounts disks of the VM from the backup or replica to the helper appliance. The backup file or VM replica itself remains in the read-only state on the backup repository or datastore.
3. Veeam Backup & Replication launches the Veeam Backup browser where mounted VM disks are displayed. You can browse the VM guest file system in the Veeam Backup Browser and restore files or folders to the original VM or to another location. Alternatively, you can enable an FTP server on the virtual appliance and allow VM owners to restore files themselves.
4. When the restore process is finished or the Veeam Backup browser is closed by timeout, Veeam Backup & Replication unmounts the content of the backup file or replica from the helper appliance and unregisters the helper appliance on the ESX(i) host.



Restoring VM Guest OS Files (Multi-OS)

With the multi-OS restore wizard, you can restore VM guest OS files from 15 file systems such as Linux, Unix, BSD, MacOS and many others.

Before restoring VM guest OS files, [check prerequisites](#). Then use the **Guest File Restore** wizard to restore the necessary VM guest OS files and folders.

Before You Begin

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

- You can restore VM guest OS files from a backup or replica that has at least one successfully created restore point.

- You cannot restore files from a backup created in the reverse incremental mode if the backup job is being performed. If the backup is created in the incremental backup mode and the backup job is being performed, you can restore files from any available restore point.
- You cannot restore VM guest OS files from a running replica or if the replication job with the necessary VM is being performed.
- If you plan to restore VM guest OS files to their initial location, VMware Tools must be installed on the target VM.
- Veeam Backup & Replication 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 target VM, mind the following:
 - Veeam Backup & Replication uses the SSH protocol to communicate with the target Linux 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.
 - SELinux must be disabled on the target VM.
 - A range of ports that are used for data transfer must be open on the target VM.

For more information on configuring connection settings for Linux servers, see the [SSH Connection](#) step of the **New Linux Server** wizard.
- Veeam Backup & Replication can restore ACL for recovered VM guest OS files. To let Veeam Backup & Replication detect the target Linux system architecture and kernel version, the following utilities must be present in the minimal configuration of the system: *arch* and *uname*.

Mind the following limitations:

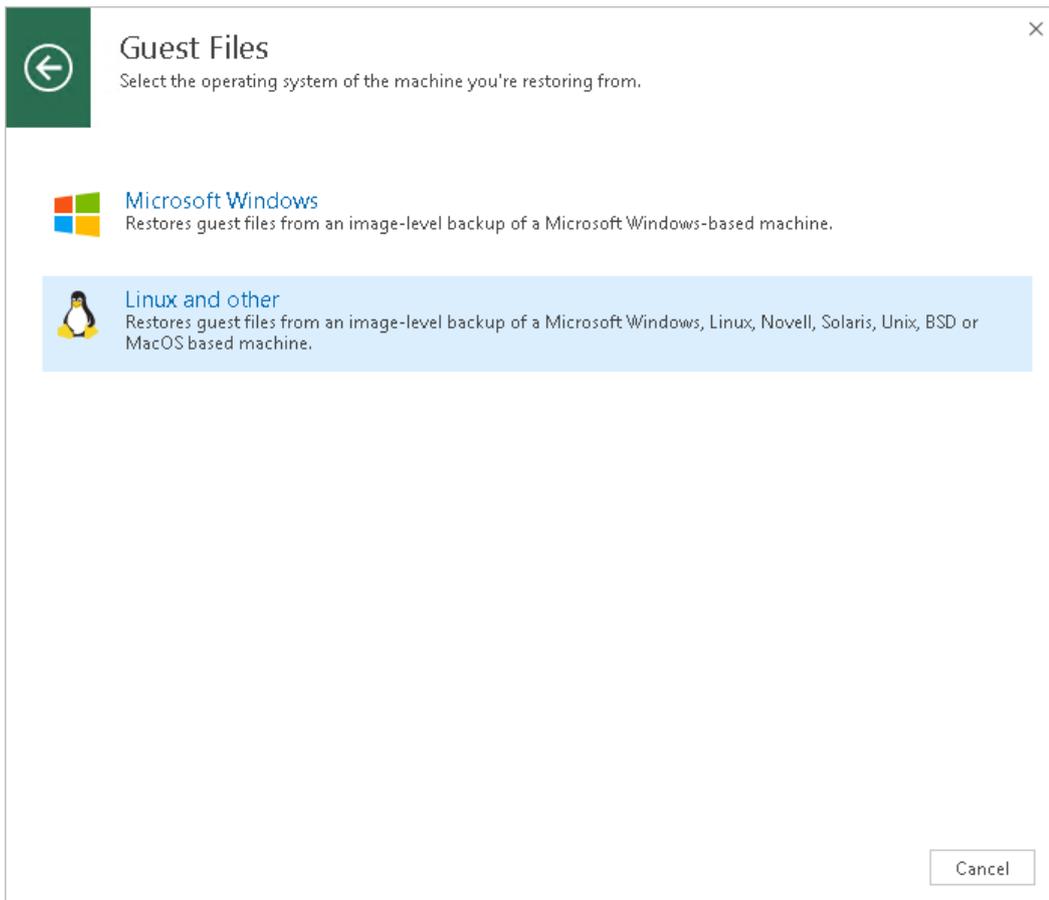
- You cannot restore pipes and other file system objects. File-level restore supports recovery of files and folders only.
- You cannot restore files directly to the original location from backups of BSD, Mac and Solaris VMs. Use the **Copy to** option instead.
- The multi-OS file-level restore wizard does not support restore of deduplicated volumes (for example, Microsoft Windows volumes with Data Deduplication enabled).

Step 1. Launch Veeam File Level Restore Wizard

To launch the **Guest File Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore > VMware vSphere > Restore from backup > Guest files restore > Linux and other**.
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Click the VM whose files you want to restore and click **Guest files > Linux and other** on the ribbon.
 - Right-click the VM whose files you want to restore and select **Restore guest files > Linux and other**.
- Double-click the VBK or VBM file (for example, in Microsoft Windows Explorer). In the displayed window, select the VM and click **Restore > Guest files (Linux and other)**.

You can use this option if you perform restore on the backup server. You cannot use this option if you perform restore remotely over the Veeam Backup & Replication console.



Step 2. Select VM

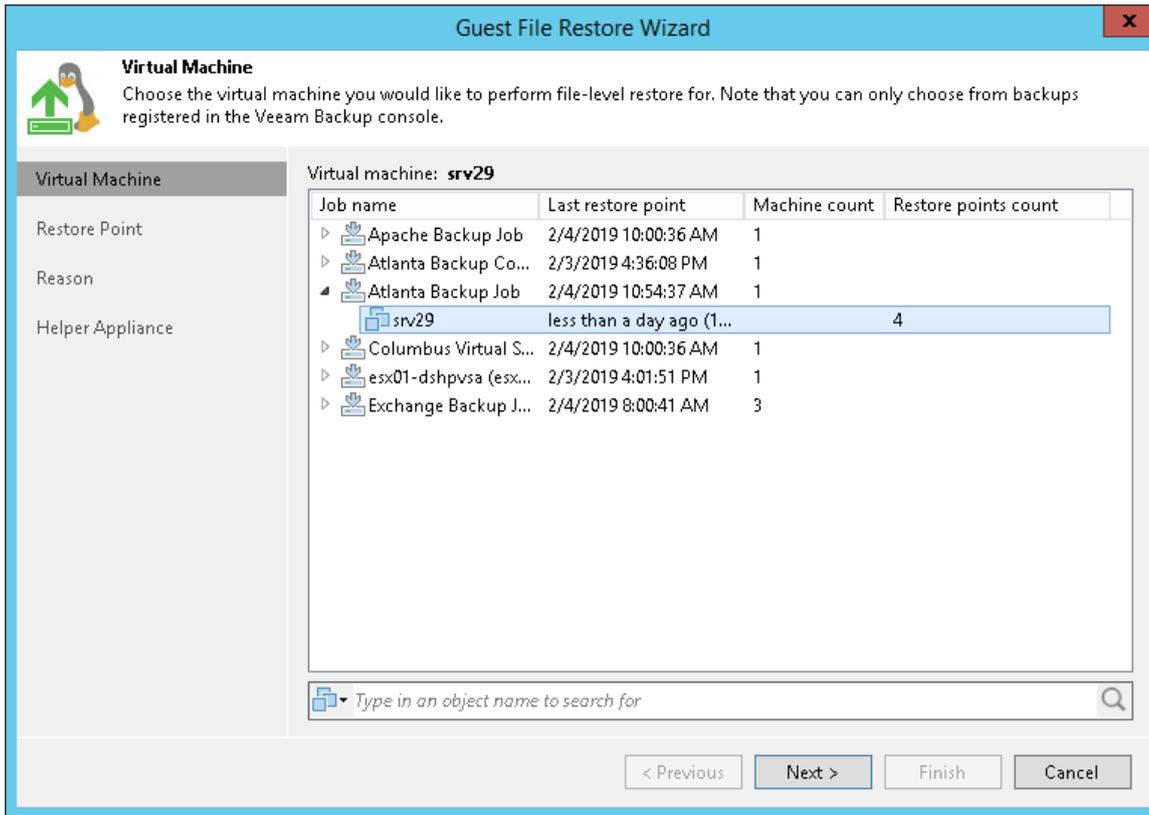
At the **Virtual Machine** step of the wizard, select the VM whose guest OS files you want to restore:

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.

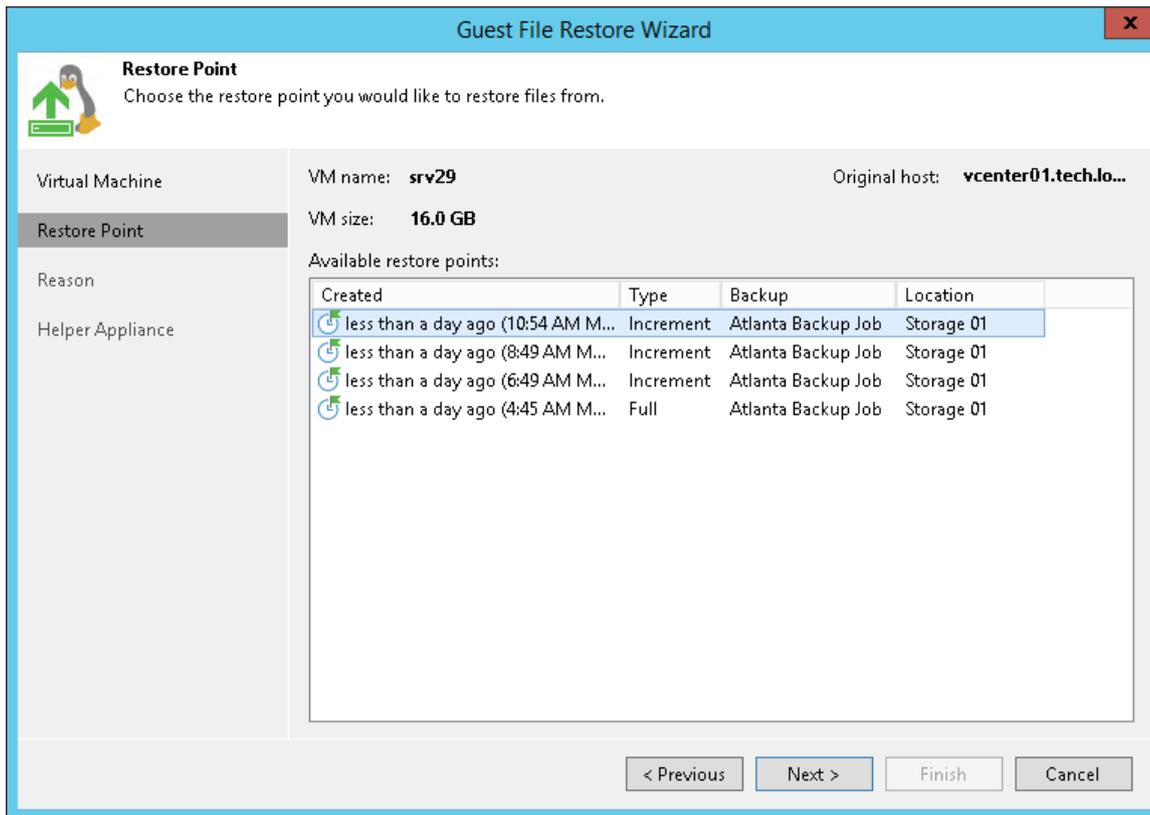
2. Click the **Start search** button on the right or press **[ENTER]**.



Step 3. Select Restore Point

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

In the **Location** column, you can view a name of a regular backup repository or cloud repository where a restore point resides.

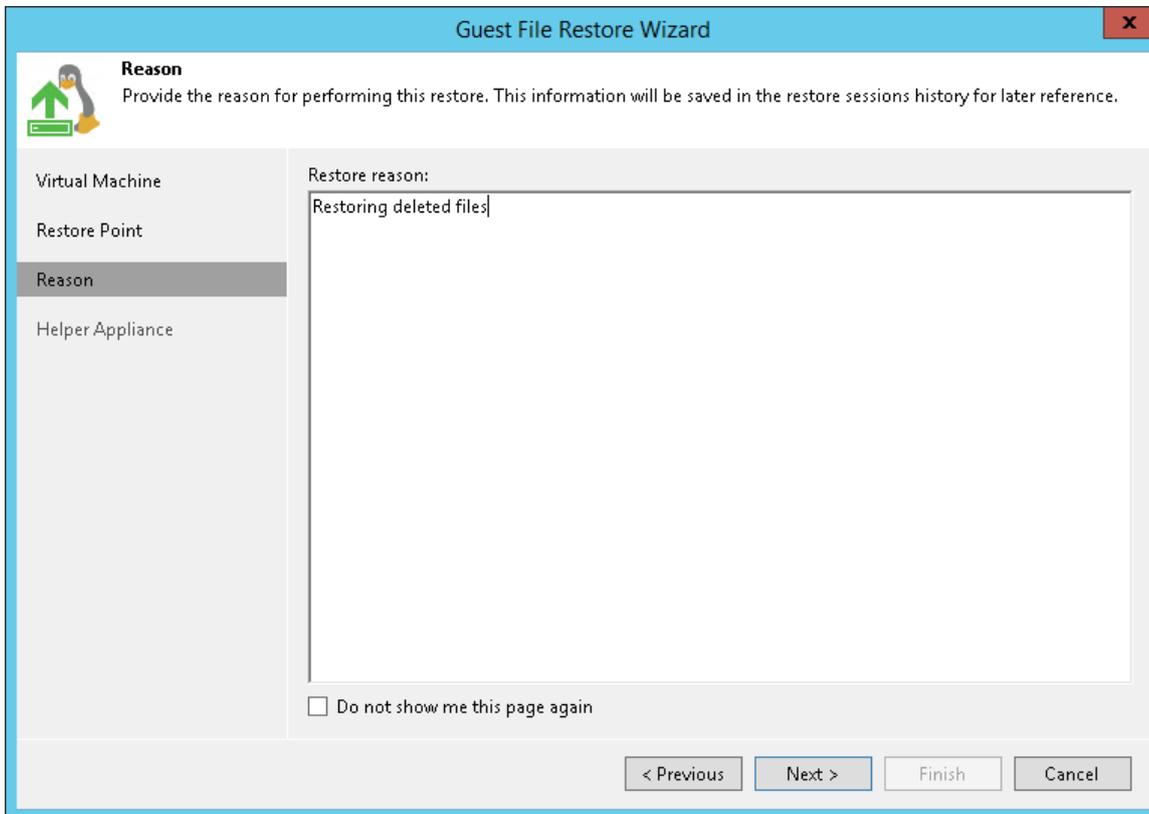


Step 4. Specify Restore Reason

At the **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 **Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 5. Specify Location for Helper Appliance

At the **Helper Appliance** step of the wizard, select an ESX(i) host on which you want to place the helper appliance.

To locate the appliance:

1. At the bottom of the window, click **Customize**.
2. In the **Host** field, specify an ESX(i) host on which the helper appliance must be registered.
3. In the **Resource pool** field, specify a resource pool to which the helper appliance must be placed.
4. Select a network for the helper appliance:

- a. On the right of the **Network** field, click **Choose**.

In the **Select Network** window, Veeam Backup & Replication will display a list of networks to which the specified host is connected.

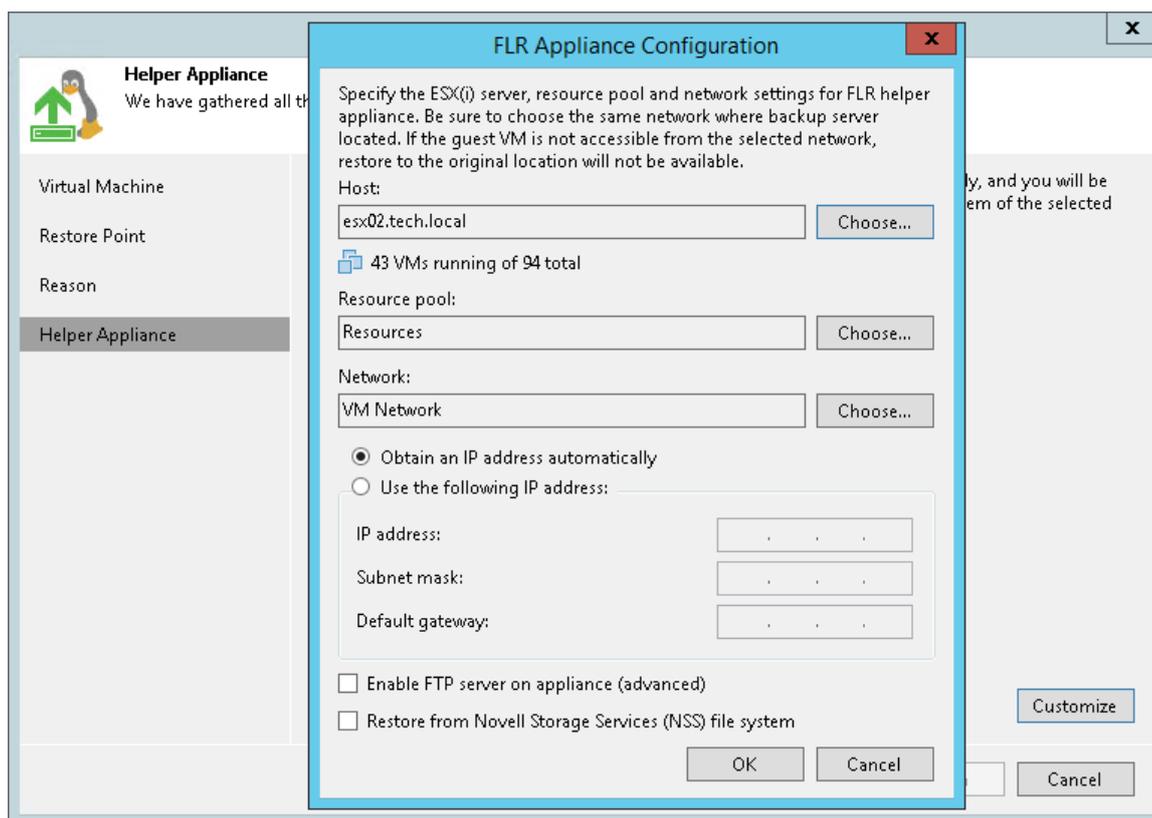
- b. From the **Networks** list, select a network to which the helper appliance must be connected and click **OK**.

Mind that the backup server and the mount server must have access to the helper appliance over the network.

5. Specify IP addressing settings for the helper appliance:
 - If you use a DHCP server in the network, leave the **Obtain an IP address automatically** option selected.
 - To manually assign the specific IP address to the helper appliance, select the **Use the following IP address** option and specify the IP address, subnet mask and default gateway address.
6. To enable FTP access to the restored file system, select the **Enable FTP server on appliance (advanced)** check box. As a result, users will be able to access the helper appliance over FTP, browse the file system of the restored VM and download necessary files on their own.
7. 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 & Replication will deploy a specific appliance that supports the Novell Storage Services file system.
8. Click **OK**.

IMPORTANT!

When choosing an ESX(i) host for the helper appliance used for file-level restore from the Novell Storage Services file system, make sure that it allows running VMs with 64-bit guest OSes.



Step 6. Save Restored Files

At the **Helper Appliance** 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.

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

You can restore 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, Veeam Backup & Replication unmounts the VM disks from the helper appliance and removes helper appliance from the ESX(i) host.

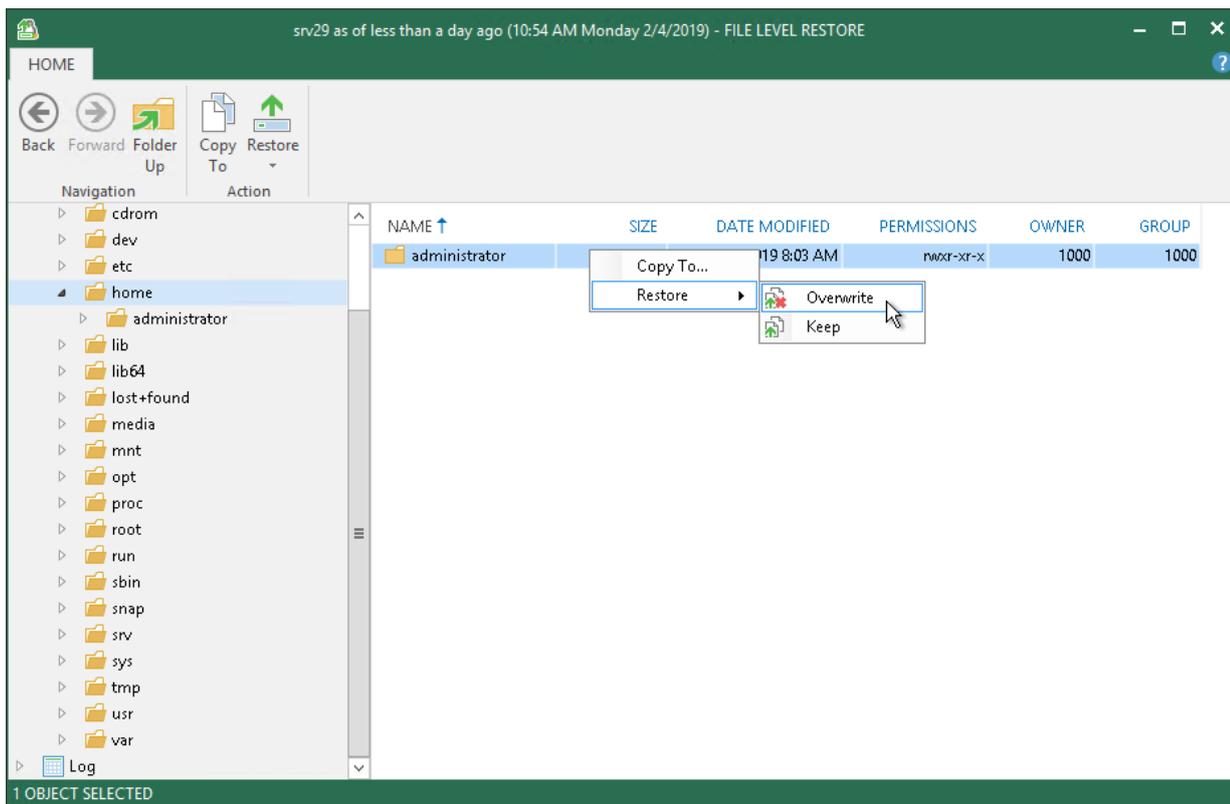
Restoring Files to Original Location

To restore 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 & Replication will add the `.RESTORED-YYYYMMDDHHMMSS` suffix 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 & Replication 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).



In some cases, you may remove the original VM and restore it from the backup by the time of file-level restore. If you then attempt to restore VM guest OS files to the original location, Veeam Backup & Replication will not be able to find the original VM by its reference ID, and display a warning. Click **OK** and browse to the target VM in the virtual infrastructure to which you want to restore VM guest OS files.

Saving Files to New Location

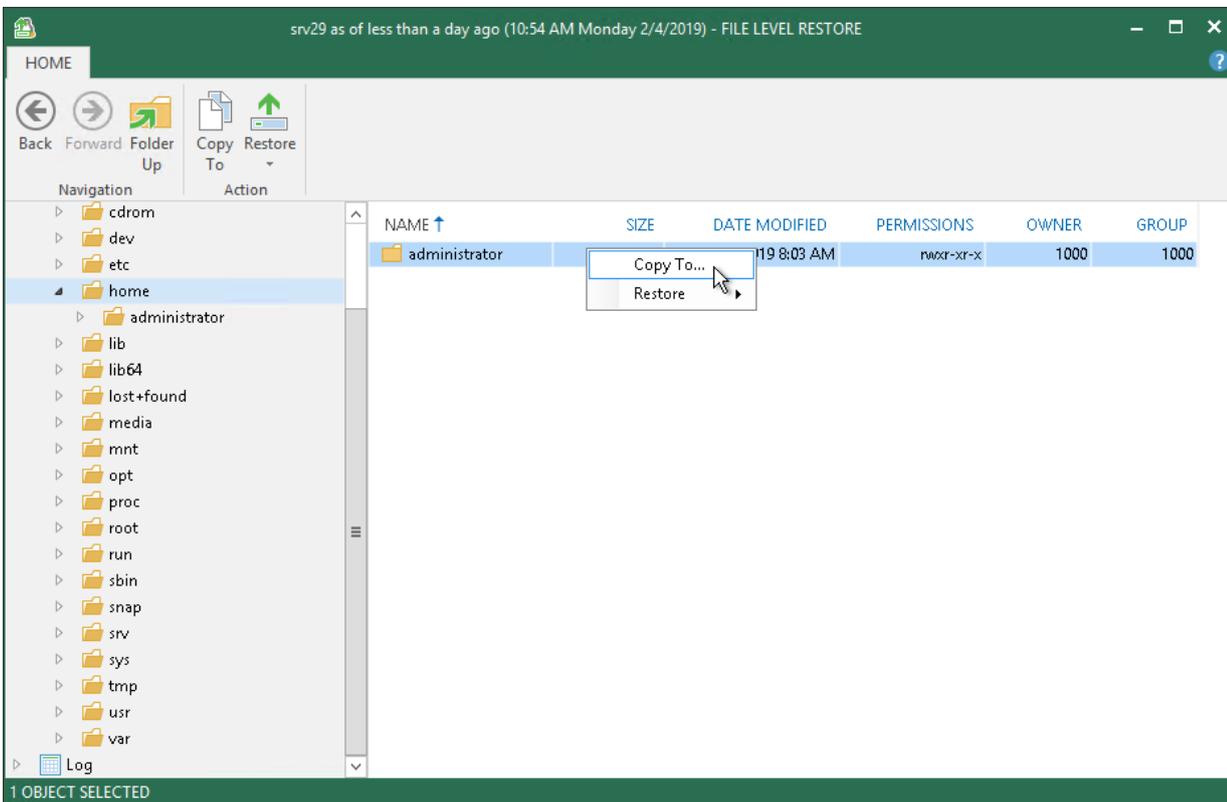
To save files and folders to a new location:

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 target host.

The server you add ad-hoc will not appear in the list of managed hosts in Veeam Backup & Replication: 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 user account you have specified must 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.

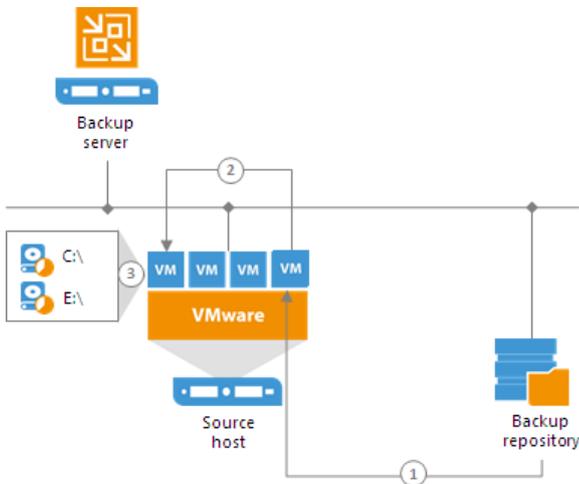
Accessing the appliance over FTP requires credentials. Use the Guest OS helper appliance credentials specified in managed credentials. If the password has not been updated, refer to the following knowledge base article: <https://www.veeam.com/kb1447>.

Restore from Other File Systems

With the vPower technology, Veeam extends IFLR to any file system, not just Microsoft Windows FAT, NTFS, ReFS and file systems supported by the multi-OS File-Level Restore wizard.

To restore files and folders from file systems not supported by file-level restore wizards, you must perform the following actions:

1. Use Instant VM Recovery to publish the VM from the backup file on the ESX(i) host in the virtual infrastructure. Do not start the recovered VM.
2. Mount the disks of the restored VM to any VM that can read the file system of the original VM.
3. Restore files or folders using native file management tools. Alternatively, you can mount the VM disks to a Microsoft Windows VM and use file management tools such as Portlock Explorer.



Viewing File Restore Session Statistics

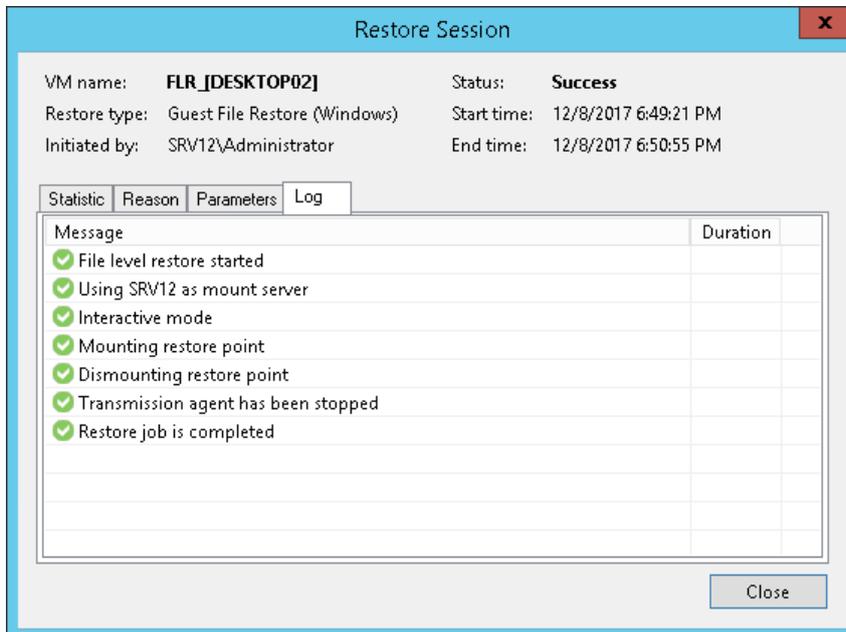
You can view statistics about performed guest OS file restore sessions.

To view the restore session statistics, do one of the following:

- Open the **Home** view, in the inventory pane select **Last 24 hours**. In the working area, double-click the necessary restore session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.
- Open the **History** view, in the inventory pane select **Restore**. In the working area, double-click the necessary restore session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.

The file restore statistics provides detailed data on file restore sessions:

- At the top of the **Restore Session** window, Veeam Backup & Replication shows general session statistics: a name of the machine whose guest OS files are restored during the session, a user name of the account under which the session was started, session status and duration details.
- The **Statistics** tab shows detailed information about the files restored during the session.
- The **Reason** tab shows the reason for the guest OS file restore that was specified at the **Reason** step of the **File Level Restore** wizard.
- The **Parameters** tab shows information about the restore point selected for the guest OS file restore at the **Restore Point** step of the **File Level Restore** wizard.
- The **Log** tab shows a list of operations performed during the session.



Application Items Restore

You can use Veeam Explorers to restore application items directly from VM backups and replicas.

Using Veeam Explorer for Microsoft Active Directory

You can use Veeam Explorer for Microsoft Active Directory to restore Microsoft Active Directory objects from any successfully created backup or replica of a virtualized Microsoft Active Directory Server. The backup or replica must be created with application-aware processing enabled and the corresponding options turned on.

To launch Veeam Explorer for Microsoft Active Directory from Veeam Backup & Replication:

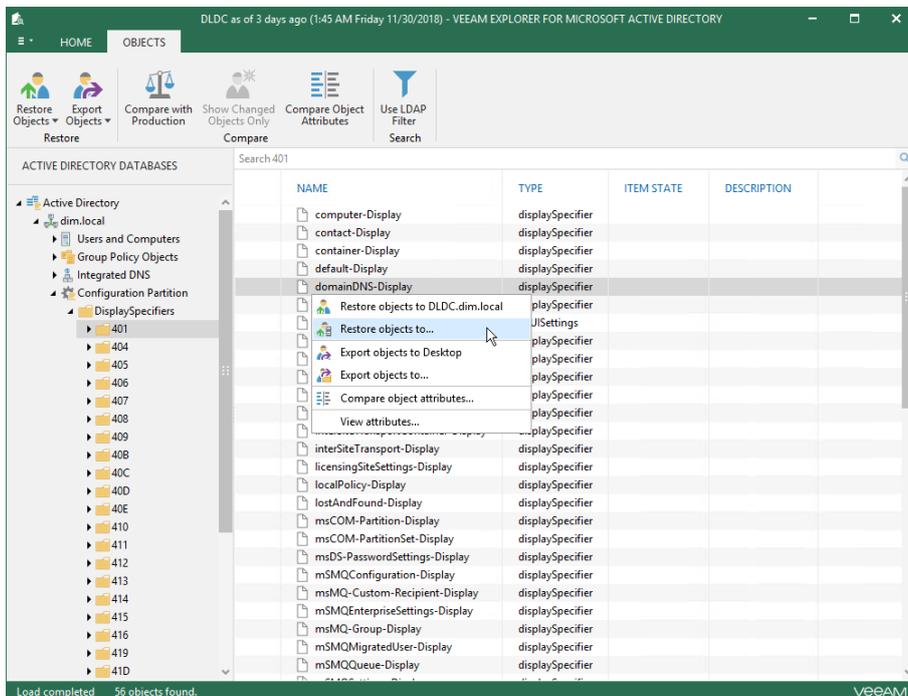
1. Open the **Home** view.
2. In the inventory pane, select the **Backups** or **Replicas** node.
3. In the working area, select the necessary machine in the backup or VM replica and click **Application Items > Microsoft Active Directory** on the ribbon.

You can also right-click the machine or VM replica and select **Restore application items > Microsoft Active Directory objects**.

4. Veeam Backup & Replication will open the **Microsoft Active Directory Object Restore** wizard. You can use this wizard to automatically extract the Microsoft Active Directory database from the backup or replica and open it in Veeam Explorer for Microsoft Active Directory.

Detailed information about preparing your applications for item-level recovery and using with Veeam Explorer for Microsoft Active Directory is provided in the Veeam Backup Explorers User Guide. To view the guide, do one of the following:

- Open Veeam Explorer for Microsoft Active Directory and press **[F1]**.
- Select **Help > Online Help** from the main menu of Veeam Explorer for Microsoft Active Directory.
- See [Veeam Explorers User Guide](#).



Using Veeam Explorer for Microsoft Exchange

You can use Veeam Explorer for Microsoft Exchange to restore Microsoft Exchange items from any successfully created backup or replica of a virtualized Microsoft Exchange Server. The backup or replica must be created with application-aware processing enabled and the corresponding options turned on.

To launch Veeam Explorer for Microsoft Exchange from Veeam Backup & Replication:

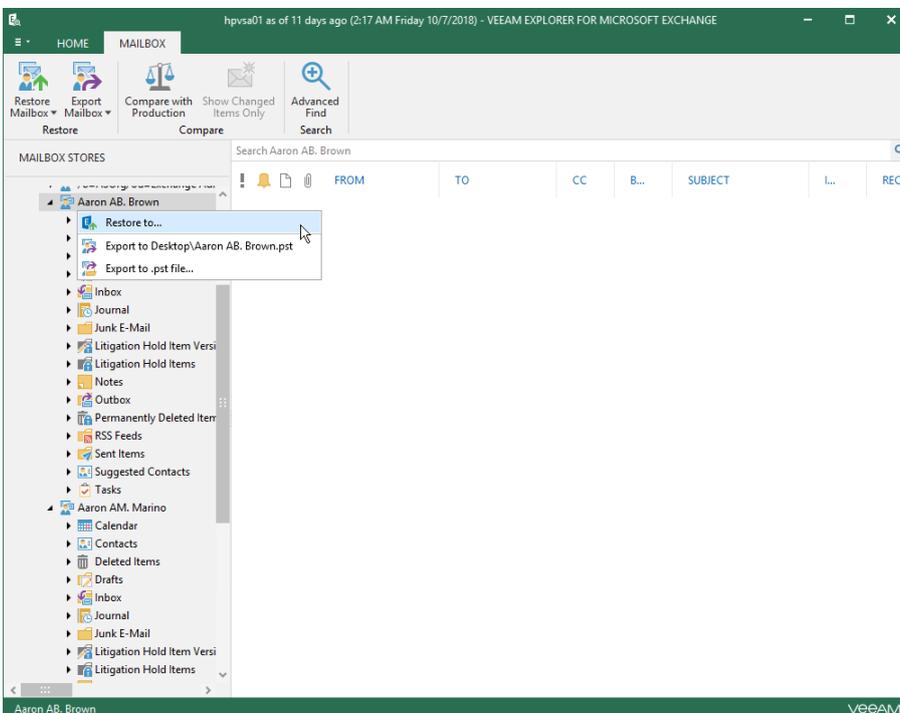
1. Open the **Home** view.
2. In the inventory pane, select the **Backups** or **Replicas** node.
3. In the working area, select the necessary machine in the backup or VM replica and click **Application Items > Microsoft Exchange** on the ribbon.

You can also right-click the machine or VM replica and select **Restore application items > Microsoft Exchange mailbox items**.

4. Veeam Backup & Replication will open the **Microsoft Exchange Item Level Restore** wizard. You can use this wizard to automatically extract the Microsoft Exchange database from the backup or replica and open it in Veeam Explorer for Microsoft Exchange.

Detailed information about preparing your applications for item-level recovery and using with Veeam Explorer for Microsoft Exchange is provided in the Veeam Backup Explorers User Guide. To view the guide, do one of the following:

- Open Veeam Explorer for Microsoft Exchange and press **[F1]**.
- Select **Help > Online Help** from the main menu of Veeam Explorer for Microsoft Exchange.
- See [Veeam Explorers User Guide](#).



Using Veeam Explorer for Microsoft SharePoint

You can use Veeam Explorer for Microsoft SharePoint to restore Microsoft SharePoint items from any successfully created backup or replica of a virtualized Microsoft SharePoint Server. The backup or replica must be created with application-aware processing enabled and the corresponding options turned on.

To launch Veeam Explorer for Microsoft SharePoint from Veeam Backup & Replication:

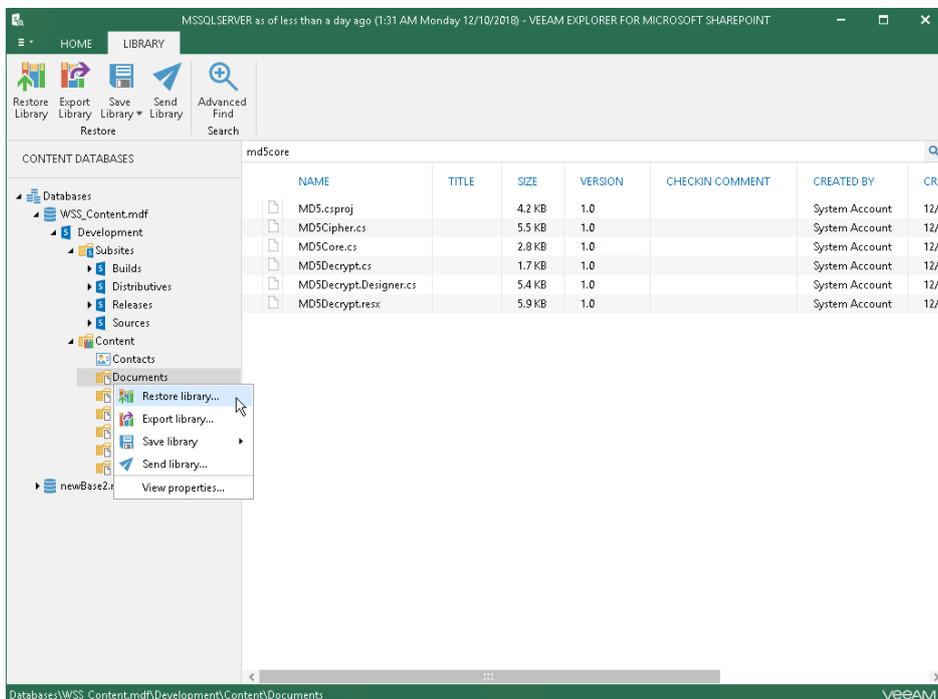
1. Open the **Home** view.
2. In the inventory pane, select the **Backups** or **Replicas** node.
3. In the working area, select the necessary machine in the backup or VM replica and click **Application Items > Microsoft SharePoint** on the ribbon.

You can also right-click the machine or VM replica and select **Restore application items > Microsoft SharePoint content**.

4. Veeam Backup & Replication will open the **Microsoft SharePoint Item Restore** wizard. You can use this wizard to automatically extract the Microsoft SharePoint content database from the backup or replica and open it in Veeam Explorer for Microsoft SharePoint.

Detailed information about preparing your applications for item-level recovery and using with Veeam Explorer for Microsoft SharePoint is provided in the Veeam Backup Explorers User Guide. To view the guide, do one of the following:

- Open Veeam Explorer for Microsoft SharePoint and press **[F1]**.
- Select **Help > Online Help** from the main menu of Veeam Explorer for Microsoft SharePoint.
- See [Veeam Explorers User Guide](#).



Using Veeam Explorer for Microsoft OneDrive for Business

You can use Veeam Explorer for Microsoft OneDrive for Business to restore Microsoft OneDrive for Business data from any successfully created backup or replica of a Veeam Backup for Microsoft Office 365 server. The backup or replica must be created with application-aware processing enabled.

To launch Veeam Explorer for Microsoft OneDrive for Business from Veeam Backup & Replication:

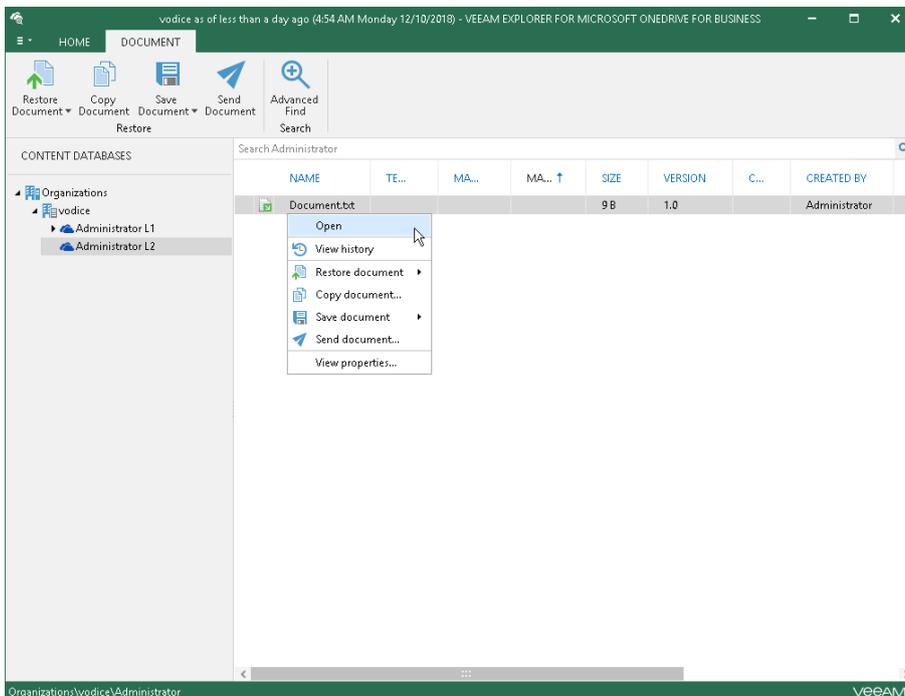
1. Open the **Home** view.
2. In the inventory pane, select the **Backups** or **Replicas** node.
3. In the working area, select the necessary machine in the backup or VM replica and click **Application Items > Microsoft OneDrive for Business** on the ribbon.

You can also right-click the machine or VM replica and select **Restore application items > Microsoft OneDrive for Business files**.

4. Veeam Backup & Replication will open the **Microsoft OneDrive for Business Files** wizard. You can use this wizard to extract Microsoft OneDrive for Business data from the backup or replica and open it in Veeam Explorer for Microsoft OneDrive for Business.

Detailed information about preparing your applications for item-level recovery and using with Veeam Explorer for Microsoft OneDrive for Business is provided in the Veeam Backup Explorers User Guide. To view the guide, do one of the following:

- Open Veeam Explorer for Microsoft OneDrive for Business and press **[F1]**.
- Select **Help > Online Help** from the main menu of Veeam Explorer for Microsoft OneDrive for Business.
- See [Veeam Explorers User Guide](#).



Using Veeam Explorer for Microsoft SQL Server

You can use Veeam Explorer for Microsoft SQL to restore databases from any successfully created backup or replica of a virtualized Microsoft SQL Server. The backup or replica must be created with application-aware processing enabled and the corresponding options turned on.

To launch Veeam Explorer for Microsoft SQL from Veeam Backup & Replication:

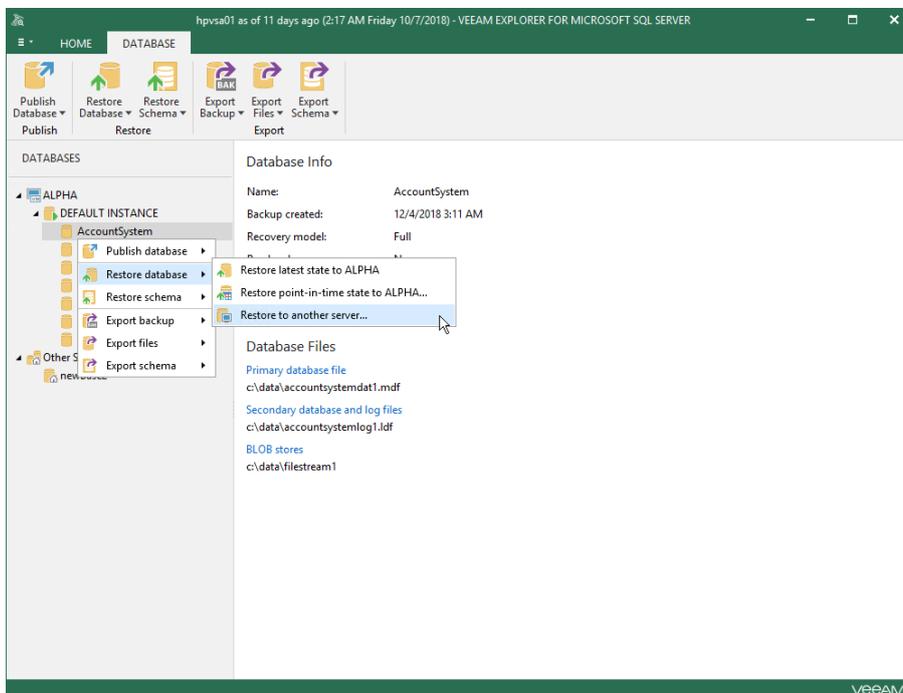
1. Open the **Home** view.
2. In the inventory pane, select the **Backups** or **Replicas** node.
3. In the working area, select the necessary machine in the backup or VM replica and click **Application Items > Microsoft SQL Server** on the ribbon.

You can also right-click the machine or VM replica and select **Restore application items > Microsoft SQL Server databases**.

4. Veeam Backup & Replication will open the **Microsoft SQL Server Database Restore** wizard. You can use this wizard to automatically extract the Microsoft SQL database from the backup or replica and open it in Veeam Explorer for Microsoft SQL.

Detailed information about preparing your applications for item-level recovery and using with Veeam Explorer for Microsoft SQL is provided in the Veeam Backup Explorers User Guide. To view the guide, do one of the following:

- Open Veeam Explorer for Microsoft SQL Server and press **[F1]**.
- Select **Help > Online Help** from the main menu of Veeam Explorer for Microsoft SQL.
- See [Veeam Explorers User Guide](#).



Using Veeam Explorer for Oracle

You can use Veeam Explorer for Oracle to restore databases from any successfully created backup or replica of a virtualized Oracle system. The backup or replica must be created with application-aware processing enabled and the corresponding options turned on.

To launch Veeam Explorer for Oracle from Veeam Backup & Replication:

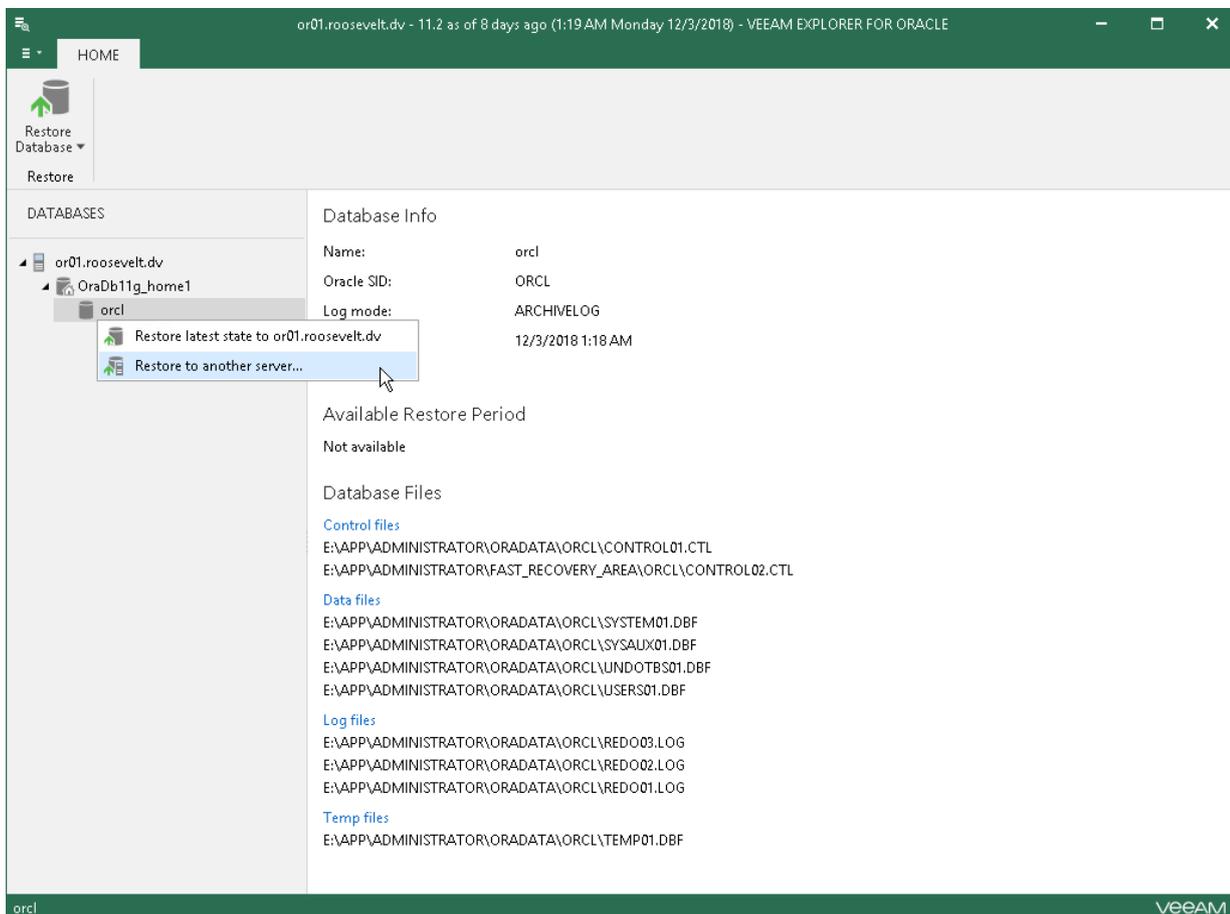
1. Open the **Home** view.
2. In the inventory pane, select the **Backups** or **Replicas** node.
3. In the working area, select the necessary machine in the backup or VM replica and click **Application Items > Oracle** on the ribbon.

You can also right-click the machine or VM replica and select **Restore application items > Oracle databases**.

4. Veeam Backup & Replication will open the **Oracle Database Restore** wizard. You can use this wizard to automatically extract the Oracle database from the backup or replica and open it in Veeam Explorer for Oracle.

Detailed information about preparing your applications for item-level recovery and using with Veeam Explorer for Oracle is provided in the Veeam Backup Explorers User Guide. To view the guide, do one of the following:

- Open Veeam Explorer for Oracle and press **[F1]**.
- Select **Help > Online Help** from the main menu of Veeam Explorer for Oracle.
- See [Veeam Explorers User Guide](#).



Restore to Microsoft Azure

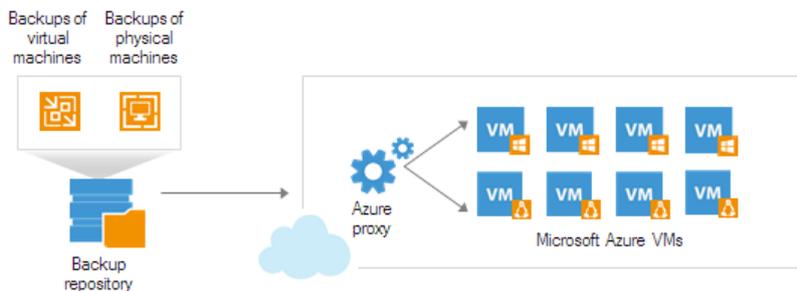
Veeam Backup & Replication allows you to restore machines from Veeam backups to Microsoft Azure. You can use Veeam Backup & Replication to complete the following tasks:

- Restore machines from Veeam backups to Microsoft Azure.
- Migrate machines from the on-premises infrastructure to the cloud.
- Create a test environment in the cloud for troubleshooting, testing patches and updates and so on.

You can restore machines from the following types of backups:

- Backups files of Microsoft Windows and Linux VMs created with Veeam Backup & Replication. You can use backups of VMware vSphere VMs and VMware vCloud Director VMs.
- Backups of Microsoft Windows machines created with Veeam Agent for Windows. Backups must be created at the entire machine level or volume level.
- Backups of Linux machines created with Veeam Agent for Linux. Backups must be created at the entire machine level or volume level.
- Backups of EC2 instances created with [N2WS Backup & Recovery](#).
- Backups of Nutanix AHV VMs created with [Veeam Availability for Nutanix AHV](#).

For restore to Microsoft Azure, Veeam Backup & Replication can employ the Microsoft Azure Resource Manager or Classic deployment model. Veeam Backup & Replication supports batch restore – you can launch the restore process for several VMs at a time.



IMPORTANT!

Starting from Veeam Backup & Replication version 9.5 Update 4, the Classic deployment model is deprecated. Thus, you cannot add Classic Azure accounts. You can restore VMs in the Classic model only if you have added the Classic Azure account before upgrading to Veeam Backup & Replication 9.5 Update 4.

How Restore to Microsoft Azure Works

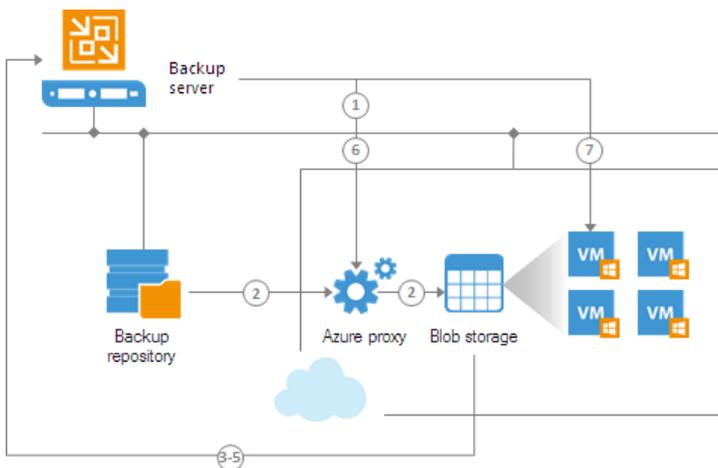
Veeam Backup & Replication lets you restore physical and virtual machines from VeeamZIP files and backups residing in the on-premises environment to Microsoft Azure. The restore process differs for Microsoft Windows and Linux machines.

- [Restore of Microsoft Windows machines](#)
- [Restore of Linux machines](#)

Restore of Microsoft Windows Machines

To restore a Microsoft Windows machine, Veeam Backup & Replication performs the following steps:

1. If you use an Azure proxy for restore, Veeam Backup & Replication powers on the Azure proxy. For more information about the Azure proxy, see [Configuring Azure Proxies](#).
2. Veeam Backup & Replication converts disks of a backed up machine to the VHD format and uploads converted disks to blob storage in Microsoft Azure.
3. Veeam Backup & Replication mounts uploaded disks to the backup server.
4. Veeam Backup & Replication prepares disks for VM restore. As part of this process, it enables Remote Desktop rules, configures firewall rules, prepares disks for Microsoft Azure agent installation and so on.
5. Veeam Backup & Replication unmounts prepared disks from the backup server.
6. If you use an Azure proxy for restore, Veeam Backup & Replication powers off the Azure proxy after a timeout.
7. Veeam Backup & Replication registers a Microsoft Azure VM with the prepared machine disks. After the registration process is complete, the Microsoft Azure VM is powered on immediately, and the Microsoft Azure agent is installed on the machine.



Restore of Linux Machines

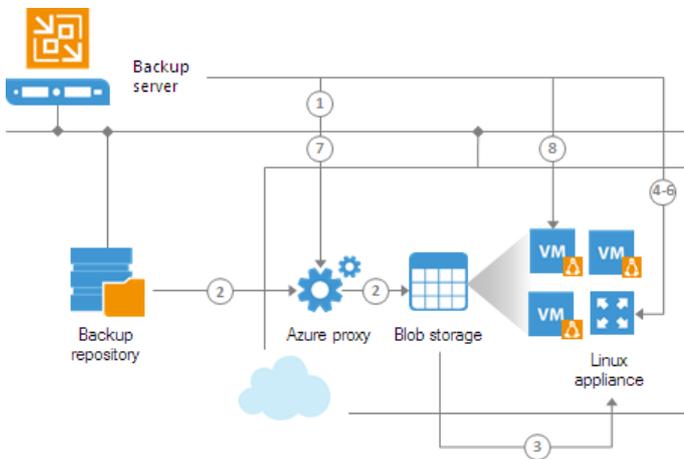
For restore of Linux machines, Veeam Backup & Replication uses a helper appliance. The helper appliance is a small auxiliary Linux-based VM in Microsoft Azure registered by Veeam Backup & Replication. During the restore process, Veeam Backup & Replication mounts disks of a backed up machine to the helper appliance to prepare disks for restore.

You can set up a helper appliance when you configure initial settings for restore to Microsoft Azure. If you plan to restore Linux machines to different locations, you must set up several appliances – one appliance in every location.

The helper appliance is persistent. After you set up the appliance, it remains in Microsoft Azure in the powered off state. Veeam Backup & Replication starts the helper appliance for a short period of time during the restore process and powers the appliance off when the restore process is complete.

To restore a Linux machine, Veeam Backup & Replication performs the following steps:

1. If you use an Azure proxy for restore, Veeam Backup & Replication powers on the Azure proxy. For more information about the Azure proxy, see [Configuring Azure Proxies](#).
2. Veeam Backup & Replication converts disks of a backed up machine to the VHD format and uploads converted disks to blob storage in Microsoft Azure.
3. Veeam Backup & Replication mounts uploaded disks to the helper appliance that resides in the location to which you restore the Linux machine.
4. Veeam Backup & Replication starts the helper appliance with mounted disks.
5. Veeam Backup & Replication prepares disks for VM restore. As part of this process, it enables remote connection rules, configures firewall rules and so on.
6. Veeam Backup & Replication unmounts prepared disks from the helper appliance and powers off the helper appliance.
7. If you use an Azure proxy for restore, Veeam Backup & Replication powers off the Azure proxy after a timeout.
8. Veeam Backup & Replication registers a Microsoft Azure VM with the prepared machine disks. After the registration process is complete, the VM is powered on immediately.



Restore Workflow

To restore a machine from backup or VeeamZIP file to Microsoft Azure, you must perform the following steps:

1. [Configure initial settings for restore to Microsoft Azure.](#)

You must add information about Microsoft Azure accounts to Veeam Backup & Replication, configure helper appliances and Azure proxies.

2. [Create a backup file.](#)

You must create a backup of a machine that you want to restore to Microsoft Azure.

3. [Restore a machine from the backup.](#)

You must restore a machine from the backup to Microsoft Azure.

Configuring Initial Settings

Before you restore machines from backups, you must configure initial settings for Microsoft Azure in Veeam Backup & Replication. As part of this process, you must perform the following tasks:

- [Add an Azure account](#) or [add an Azure Stack account](#).
- [For restore of Linux machines] [Configure helper appliances in Microsoft Azure](#).
- [For restore process speed-up] [Configure an Azure proxy](#).

Adding Microsoft Azure Accounts

To restore machines to Microsoft Azure, you must add a Microsoft Azure account to Veeam Backup & Replication. When you add a Microsoft Azure account, Veeam Backup & Replication imports information about subscriptions and resources associated with the Microsoft Azure account. During the restore process, Veeam Backup & Replication accesses these resources and uses them to register new VMs in Microsoft Azure.

If necessary, you can add different user accounts to Veeam Backup & Replication. In this case, Veeam Backup & Replication will import information about all subscriptions and resources associated with provided accounts, and you will be able to use these resources for restore.

Information about subscriptions and resources is saved to the Veeam Backup & Replication configuration database. You can re-import this information at any time.

Before You Begin

Before you add a Microsoft Azure account to Veeam Backup & Replication, check the following prerequisites:

- Make sure that you have a user account in Microsoft Azure. You will not be able to create a new user account when passing through the **Initial Configuration** wizard.
- [For Microsoft Server OS] The Protected Mode must be switched off in the Internet Explorer settings. Otherwise, you will not be able to log on to Microsoft Azure when passing through the **Initial Configuration** wizard.

If you do not want to switch off the Protected Mode for security reasons, you can add the following sites to the list of trusted hosts in **Internet Options > Secure** settings in Internet Explorer or in **Control Panel > Network and Internet**:

- <https://login.live.com>
- <https://login.microsoftonline.com>
- <https://secure.aadcdn.microsoftonline-p.com>
- <https://auth.gfx.ms>
- about:security_veeam.backup.shell.exe

You may need to additionally disable the Internet Explorer Enhanced Security Configuration in Server Manager.

- On the backup server, you must set the correct time according to the timezone where the backup server is located. Otherwise, you may not be able to add a Microsoft Azure user account to Veeam Backup & Replication.
- We recommend having Microsoft Azure PowerShell version 5.1.1 installed on the machine running the Veeam Backup & Replication console. If the version is different from 5.1.1 you may not be able to add a Microsoft Azure account to Veeam Backup & Replication.

If you do not have Microsoft Azure PowerShell on the machine, Veeam Backup & Replication will prompt you to install it. For more information, see the [Deployment Model](#) step of the **Initial Configuration** wizard.

- When the Internet access is possible only through HTTP/HTTPS proxy, you must configure the proxy settings for the Local System account or account under which the Veeam Backup Service is running. For more information, see [MSDN Blogs](#).

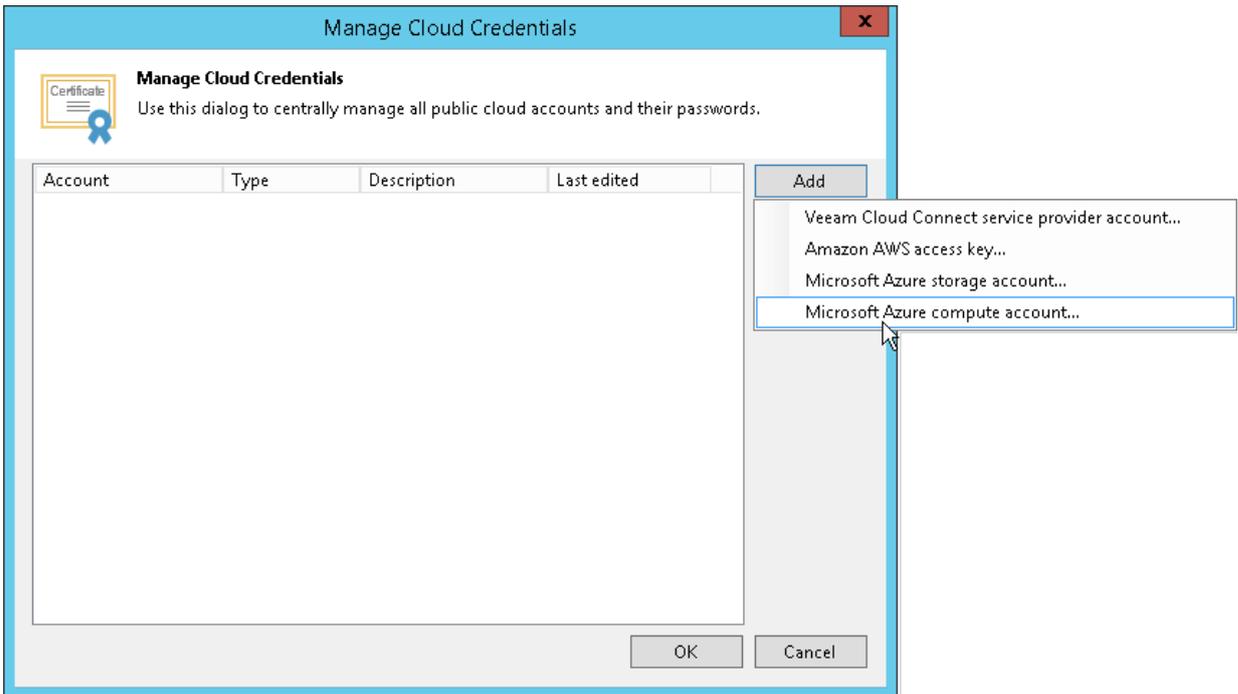
NOTE:

When you add a Microsoft Azure account to Veeam Backup & Replication, Veeam Backup & Replication creates an Azure AD application in the added account. For more information, see [Microsoft Azure documentation](#).

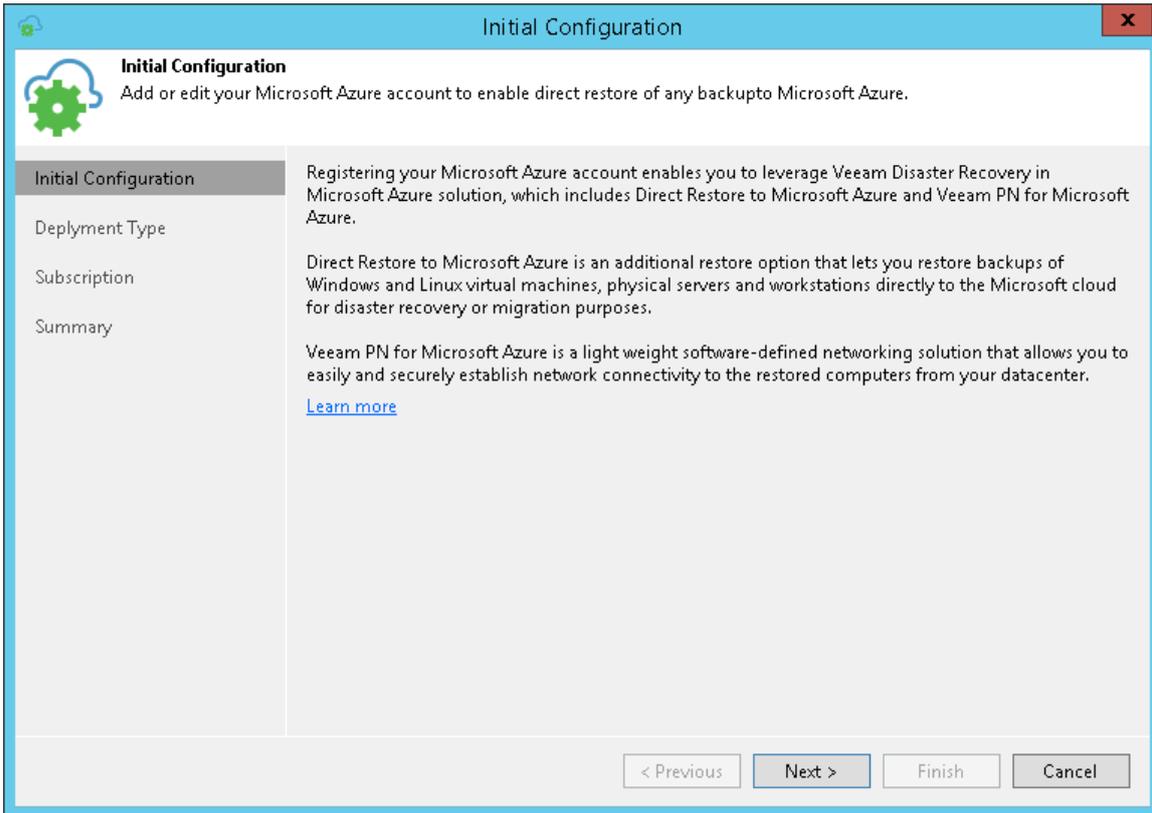
Procedure

To add a Microsoft Azure account using the Resource Manager deployment model, do the following:

1. From the main menu, select **Manage Cloud Credentials**.
2. In the **Manage Cloud Credentials** window, click **Add** and select **Microsoft Azure compute account**.

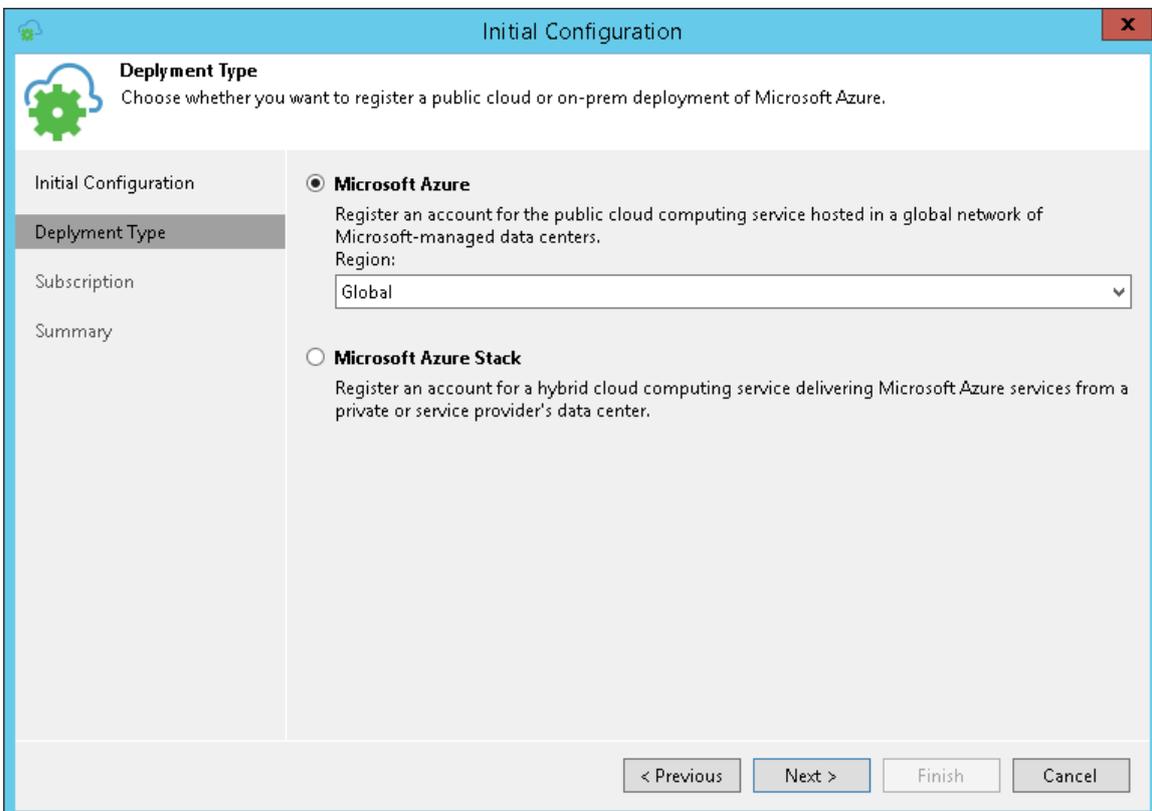


- At the **Initial Configuration** step of the wizard, click **Next**.



- At the **Deployment Type** step of the wizard, select **Microsoft Azure**.

From the **Region** list, select a Microsoft Azure region: *Global*, *Germany*, *China* or *Government*, and click **Next**.



5. At the **Subscription** step of the wizard, select the method of importing your Azure Resource Manager subscription. You have two options:

- **Use the existing account:** Select this option, if you want to use Azure Active Directory Account.

The Azure account must have the *Owner* role privileges for the required subscription. If the *Owner* role cannot be used, you can create a custom role with minimal permissions. To learn how to create a custom role, see [Creating Custom Role for Azure Account](#).

Note that only subscriptions that belong to selected account's directory will be added.

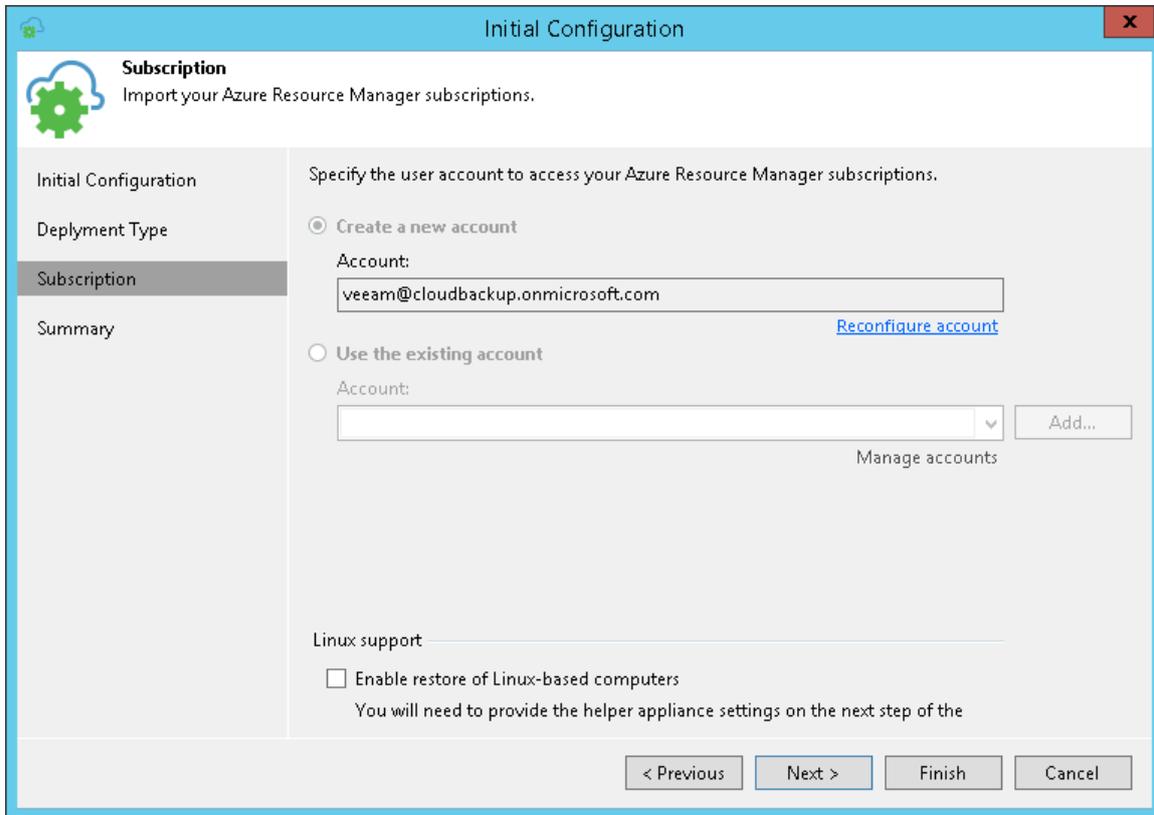
- **Create a new account:** If you select this option, Veeam Backup & Replication will register a special application on Azure. Veeam Backup & Replication will use this application to communicate with Azure. Mind the following prerequisites:
 - A Microsoft Azure account that you plan to add to Veeam Backup & Replication must have the *Owner* role privileges for the subscription that will be used for restore to Microsoft Azure. Owner role privileges are required to provide access to subscription for the created application. For details, see [Microsoft Azure documentation](#).
 - The user must have privileges to register applications: Global Administrator privileges or the enabled **Users can register applications** option in Azure portal. For details, see [Microsoft Azure documentation](#).

To create a new account, do the following:

- a. Click the **Configure account** link.

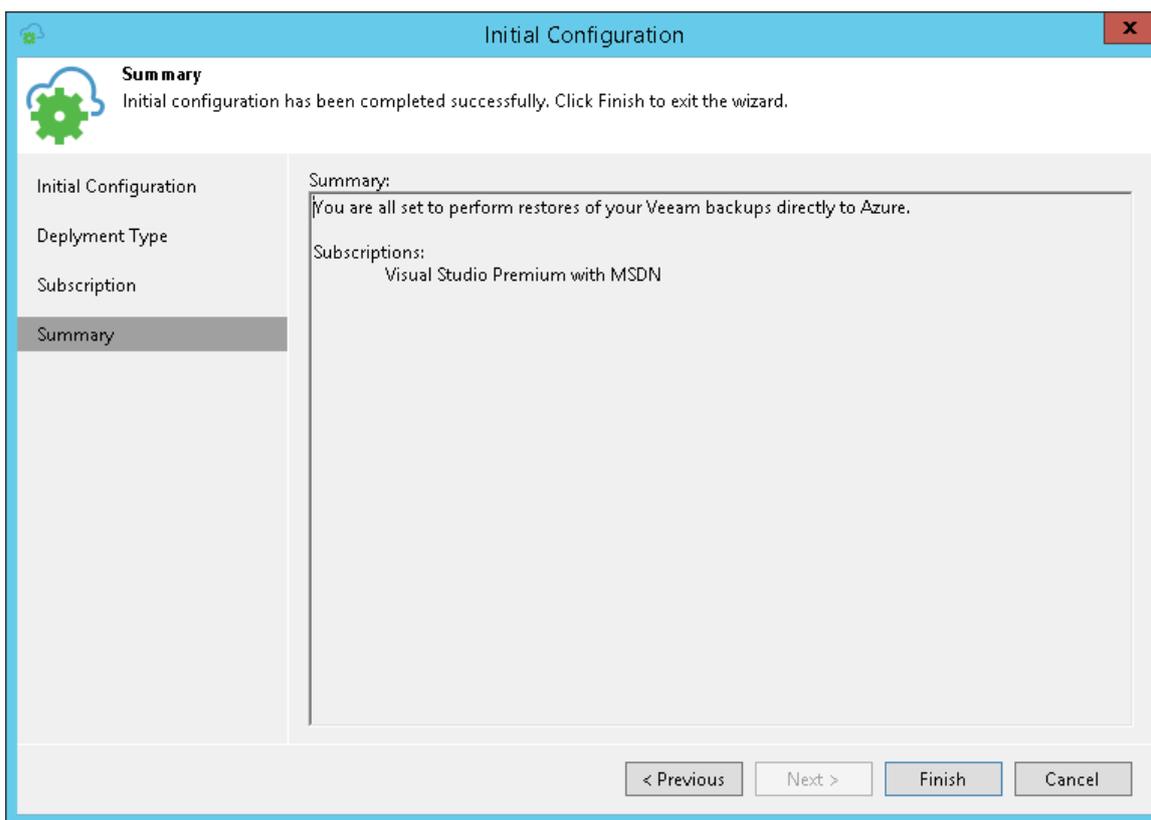
Veeam Backup & Replication will check if Microsoft Azure PowerShell is installed on the machine that runs the Veeam Backup & Replication console. If Microsoft Azure PowerShell is not installed, Veeam Backup & Replication will display a warning.
- b. In the warning window, click **this link**. Veeam Backup & Replication will launch the Microsoft Azure Powershell installation wizard. Follow steps of the installation wizard to set up the Microsoft Azure PowerShell 5.1.1 on the machine.
- c. After the installation process is complete, close the Veeam Backup & Replication console. In some cases, Microsoft PowerShell Azure requires you to restart the machine.
- d. Open the Veeam Backup & Replication console and pass through the **Initial Configuration** wizard once again.

- e. Click the **Configure account** link. You will be prompted to log in to the Microsoft Azure portal. Enter credentials of an existing Microsoft Azure account in the browser window. Veeam Backup & Replication will retrieve information about subscriptions and resources associated with this account.



6. If you plan to restore Linux machines to Microsoft Azure, select the **Enable restore of Linux-based computers** check box. Veeam Backup & Replication will deploy a helper appliance in Microsoft Azure and use it for restore of Linux machines. For more information about helper appliance setup, see [Configuring Helper Appliances](#).

7. At the **Summary** step of the wizard, review details of configured settings and click **Finish** to close the wizard.



Adding Microsoft Azure Stack Accounts

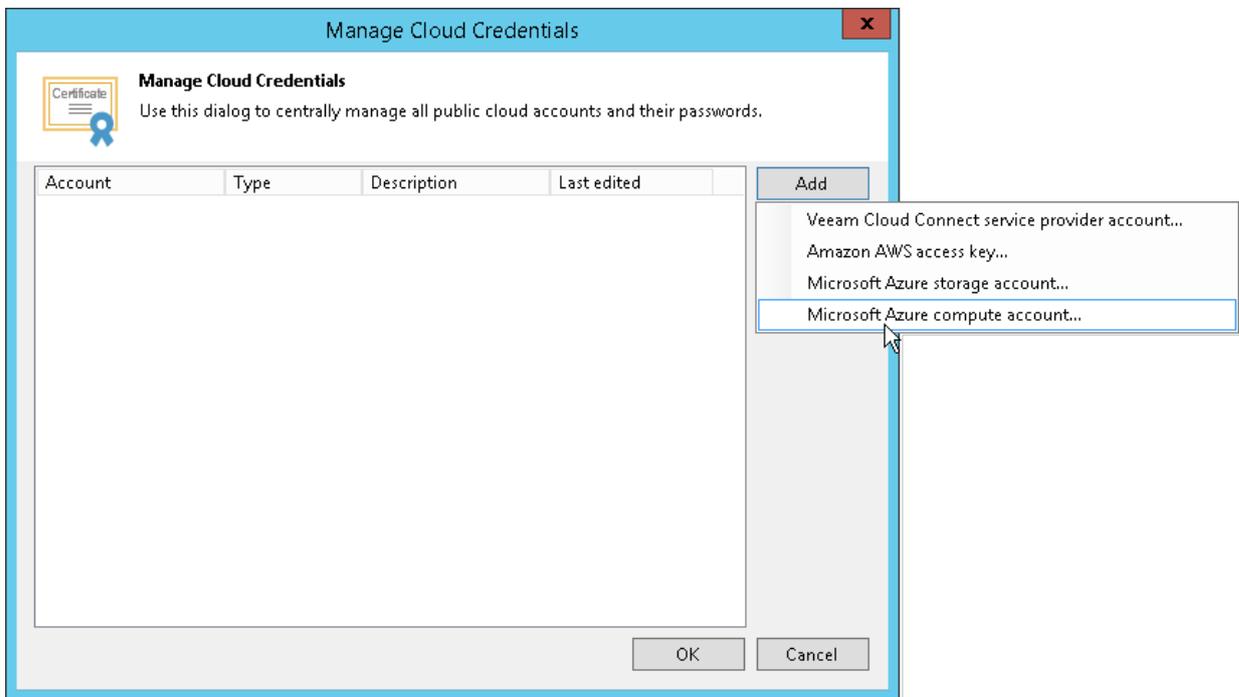
To restore machines to Microsoft Azure Stack, you must add an Azure Stack account to Veeam Backup & Replication. When you add an Azure Stack account, Veeam Backup & Replication imports information about subscriptions and resources associated with the Azure Stack account. During the restore process, Veeam Backup & Replication accesses these resources and uses them to register new VMs in Azure Stack.

If necessary, you can add different user accounts to Veeam Backup & Replication. In this case, Veeam Backup & Replication will import information about all subscriptions and resources associated with provided accounts, and you will be able to use these resources for restore.

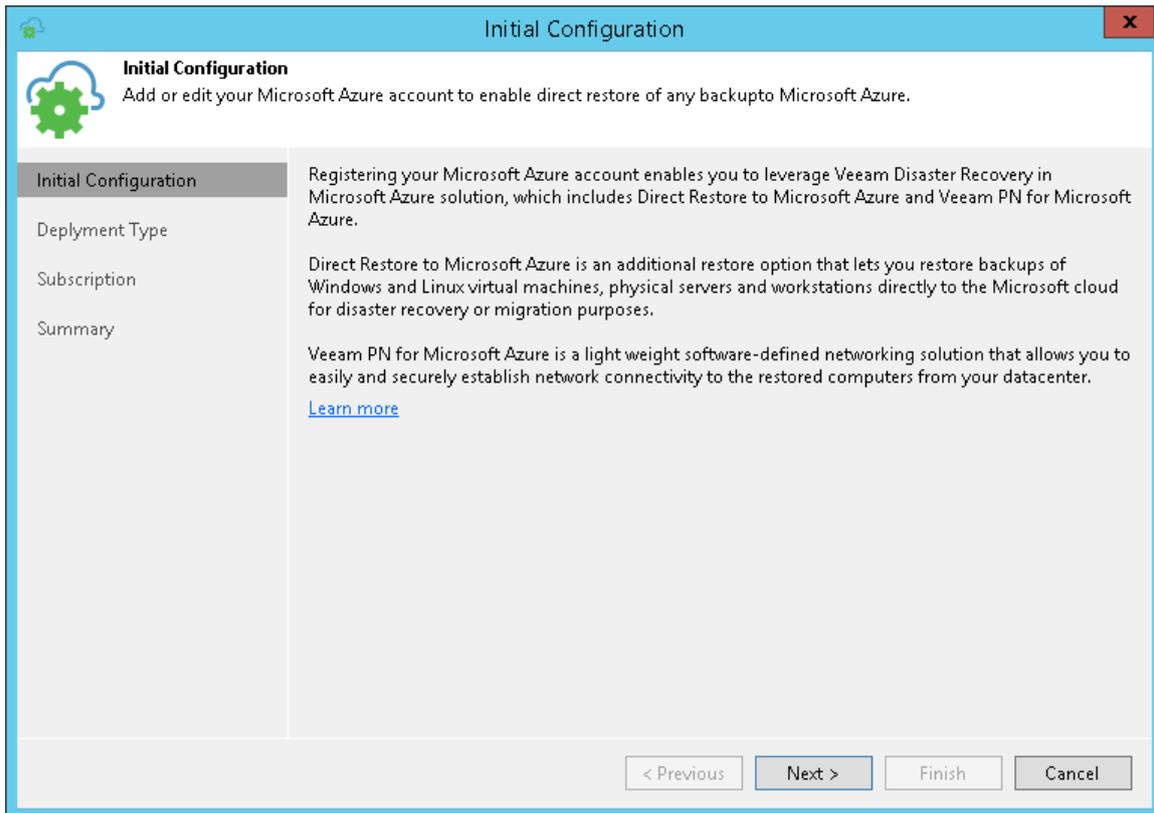
Information about subscriptions and resources is saved to the Veeam Backup & Replication configuration database. You can re-import this information at any time.

To add a Microsoft Azure Stack account, do the following.

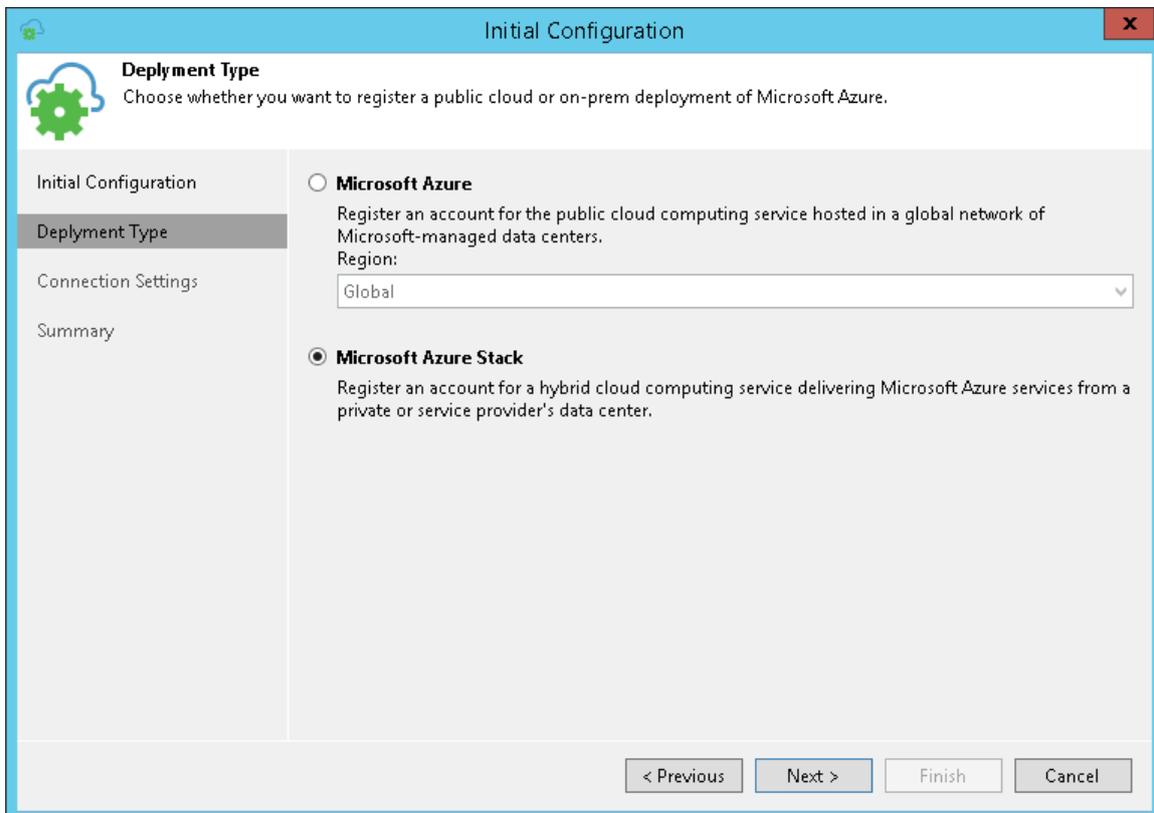
1. From the main menu, select **Manage Cloud Credentials**.
2. In the **Manage Cloud Credentials** window, click **Add** and select **Microsoft Azure compute account**.



- At the **Initial Configuration** screen of the wizard, click **Next**.



- At the **Deployment Type** step of the wizard, select **Microsoft Azure Stack** and click **Next**.



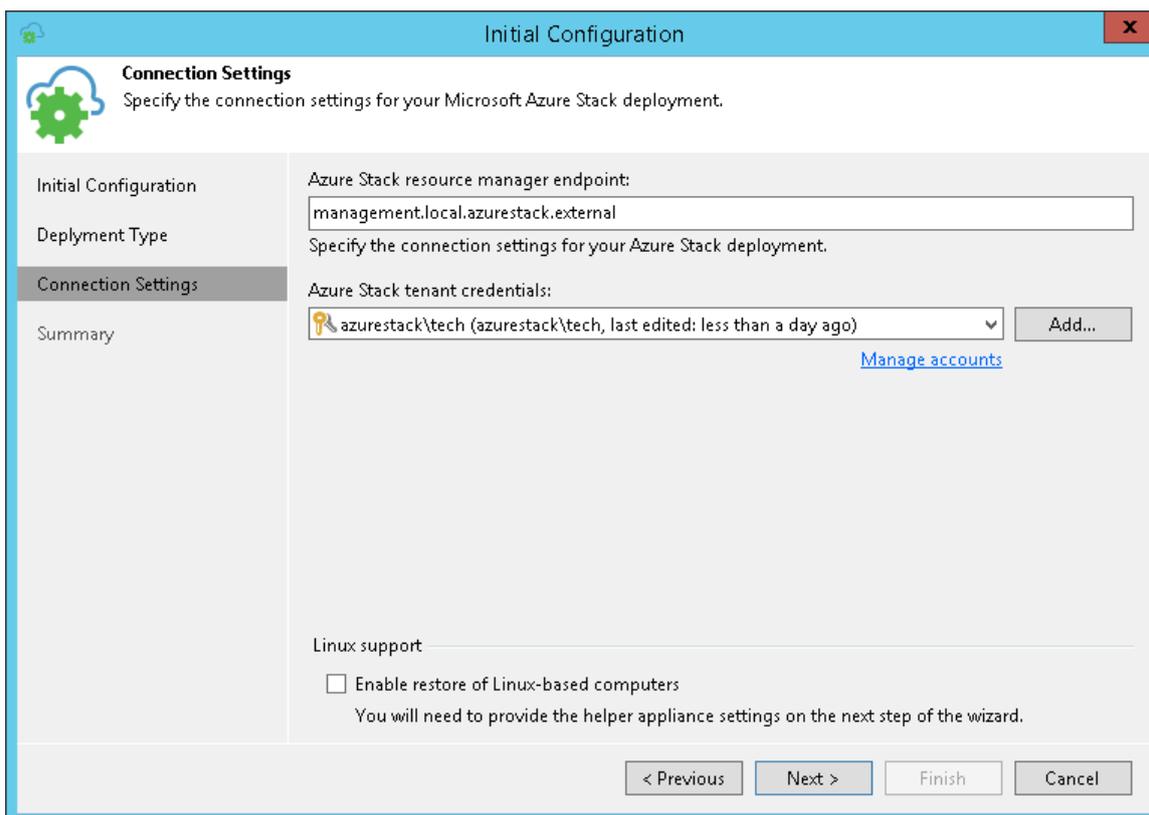
5. At the **Name** step of the wizard, do the following:

- a. In the **Azure Stack resource manager endpoint** field, specify the virtual IP address of Azure Resource Manager in the following format: *management.<region>.<FQDN>*.

To learn about Azure Stack virtual IP addresses, see <https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-integrate-endpoints>.

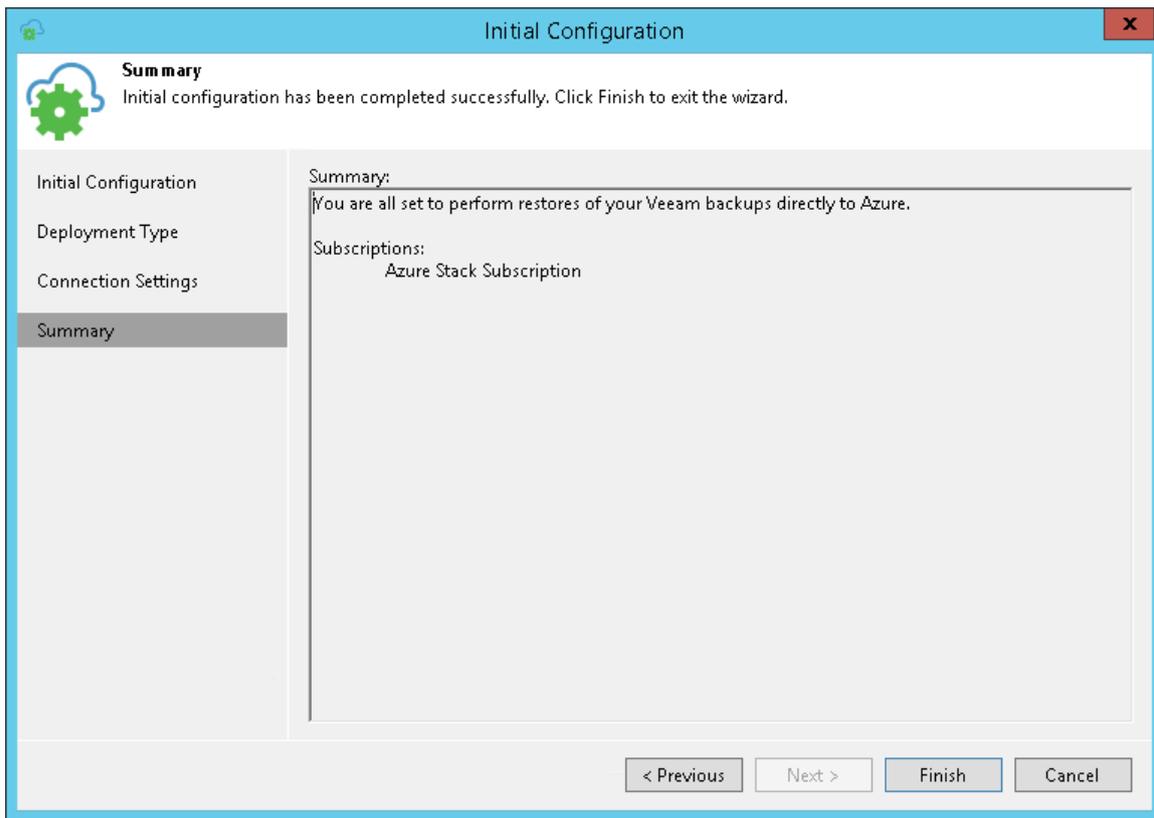
- b. If you have added the Azure Stack tenant user account beforehand, select the Azure Stack tenant user account from the list.

If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add an Azure Stack tenant user credentials.



- 6. If you want to restore Linux-based computers, select the **Enable restore of Linux-based computers** check box. Veeam Backup & Replication will deploy a helper appliance in Microsoft Azure. The helper appliance will be used to restore Linux machines. For more information about helper appliance setup, see [Configuring Helper Appliances](#).

- At the **Summary** step of the wizard, review details of configured settings and click **Finish** to close the wizard.



Creating Custom Role for Azure Account

If you do not want to use built-in Azure roles, you can create a custom role with minimal permissions.

To create a custom role, do the following:

1. Run the following script in Azure PowerShell:

```
$role =
[Microsoft.Azure.Commands.Resources.Models.Authorization.PSRoleDefinition]::new
()
$role.Name = 'Veeam Restore Operator'
$role.Description = 'Permissions for Veeam Direct Restore to Microsoft Azure'
$role.IsCustom = $true
$permissions = @(
'Microsoft.Storage/storageAccounts/listkeys/action',
'Microsoft.Storage/storageAccounts/read',
'Microsoft.Network/locations/checkDnsNameAvailability/read',
'Microsoft.Network/virtualNetworks/read',
'Microsoft.Network/virtualNetworks/subnets/join/action',
'Microsoft.Network/publicIPAddresses/read',
'Microsoft.Network/publicIPAddresses/write',
'Microsoft.Network/publicIPAddresses/delete',
'Microsoft.Network/publicIPAddresses/join/action',
'Microsoft.Network/networkInterfaces/read',
'Microsoft.Network/networkInterfaces/write',
'Microsoft.Network/networkInterfaces/delete',
'Microsoft.Network/networkInterfaces/join/action',
'Microsoft.Network/networkSecurityGroups/read',
'Microsoft.Network/networkSecurityGroups/write',
'Microsoft.Network/networkSecurityGroups/delete',
'Microsoft.Network/networkSecurityGroups/join/action',
'Microsoft.Compute/locations/vmSizes/read',
'Microsoft.Compute/locations/usages/read',
'Microsoft.Compute/virtualMachines/read',
'Microsoft.Compute/virtualMachines/write',
'Microsoft.Compute/virtualMachines/delete',
'Microsoft.Compute/virtualMachines/start/action',
'Microsoft.Compute/virtualMachines/deallocate/action',
'Microsoft.Compute/virtualMachines/instanceView/read',
'Microsoft.Compute/virtualMachines/extensions/read',
'Microsoft.Compute/virtualMachines/extensions/write',
'Microsoft.Resources/checkResourceName/action',
'Microsoft.Resources/subscriptions/resourceGroups/read',
'Microsoft.Resources/subscriptions/resourceGroups/write',
'Microsoft.Resources/subscriptions/locations/read'
)
$role.Actions = $permissions
$role.NotActions = (Get-AzureRmRoleDefinition -Name 'Virtual Machine
Contributor').NotActions
$subs = '/subscriptions/00000000-0000-0000-0000-000000000000'
$role.AssignableScopes = $subs
New-AzureRmRoleDefinition -Role $role
```

2. Assign the created role to the required Azure User. For details, see the [Assign Roles to Users](#) section in the Azure Active Directory Fundamentals.
3. In the **Subscription** step of the **Initial Configuration** wizard, select **Use existing account** and select the Azure user with the assigned role. For details, see [Adding Microsoft Azure Account](#).

Reference

[Create Custom Roles Using Azure PowerShell](#)

Configuring Helper Appliances

Veeam Backup & Replication requires a helper appliance to restore Linux machines to Microsoft Azure. The helper appliance is a small auxiliary VM in Microsoft Azure registered by Veeam Backup & Replication. During the restore process, Veeam Backup & Replication mounts disks of the restored machine to the helper appliance to prepare these disks for restore.

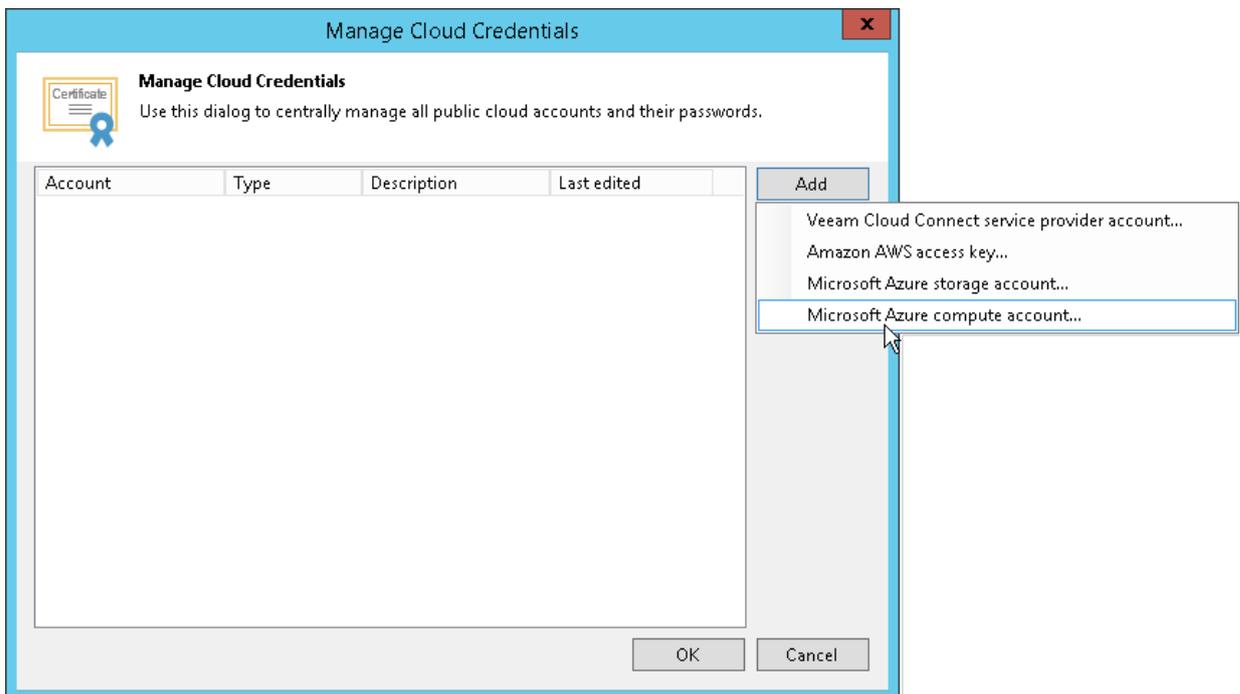
You must configure a helper appliance in the location to which you plan to restore Linux machines. If you plan to restore Linux machines to different locations, you must configure several appliances – one appliance in every location.

Mind the following:

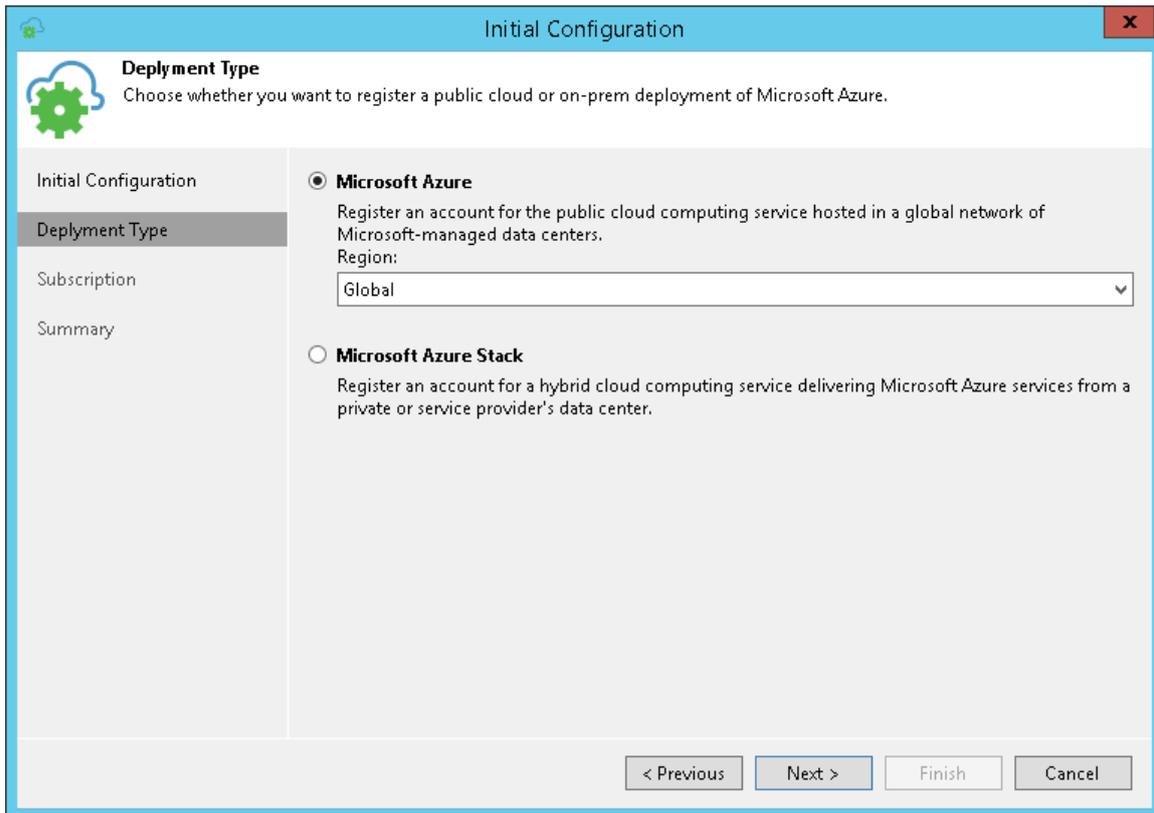
- Helper appliances are persistent. After you set up appliances, they remain in Microsoft Azure in the powered off state until you start the restore process. Microsoft Azure will bill you for storing helper appliances disks in the storage account.
- Veeam Backup & Replication uses a built-in credentials record to work with all helper appliances. For security reasons, it is recommended that you change a password for this account before you set up the helper appliances. For more information, see [Changing Credentials for Helper Appliances](#).

To configure a helper appliance:

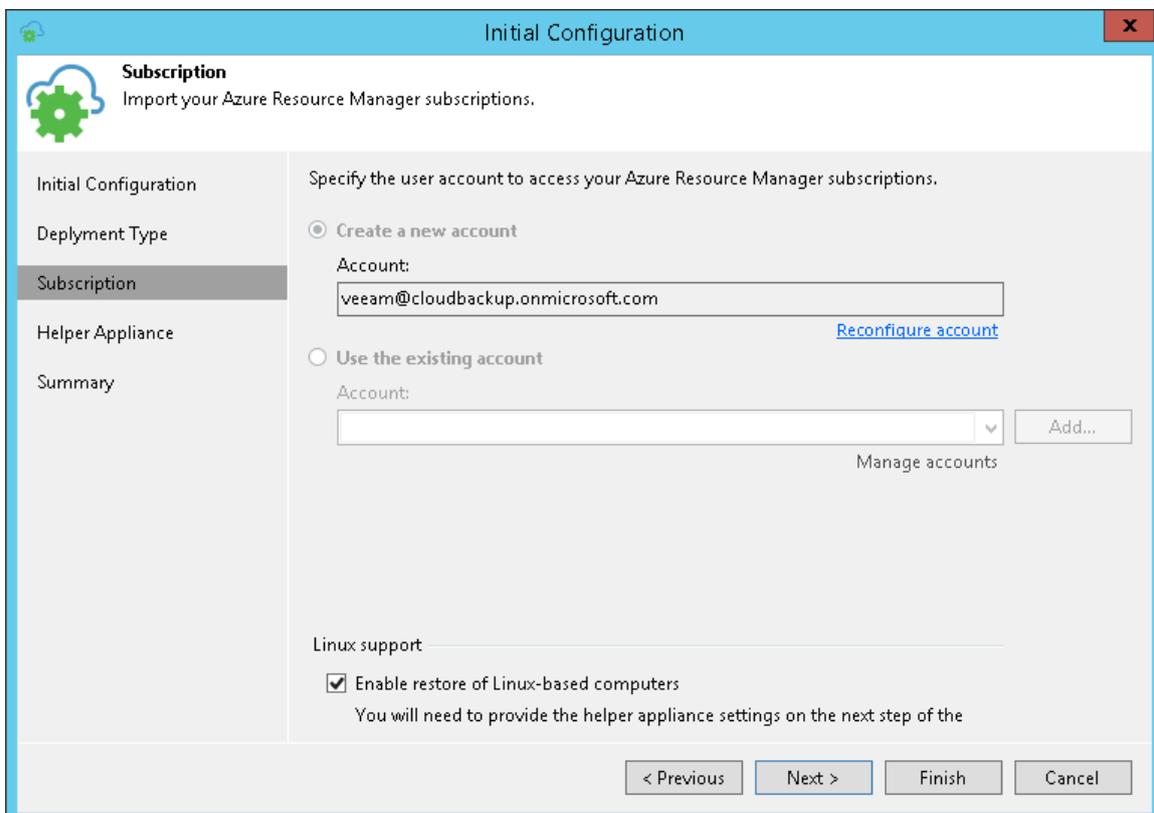
1. From the main menu, select **Manage Cloud Credentials**.
2. In the **Manage Cloud Credentials** window, click **Add**. If you edit an existing account, select it in the list and click **Edit**.



- At the **Deployment Model** step of the wizard, select the necessary deployment model.

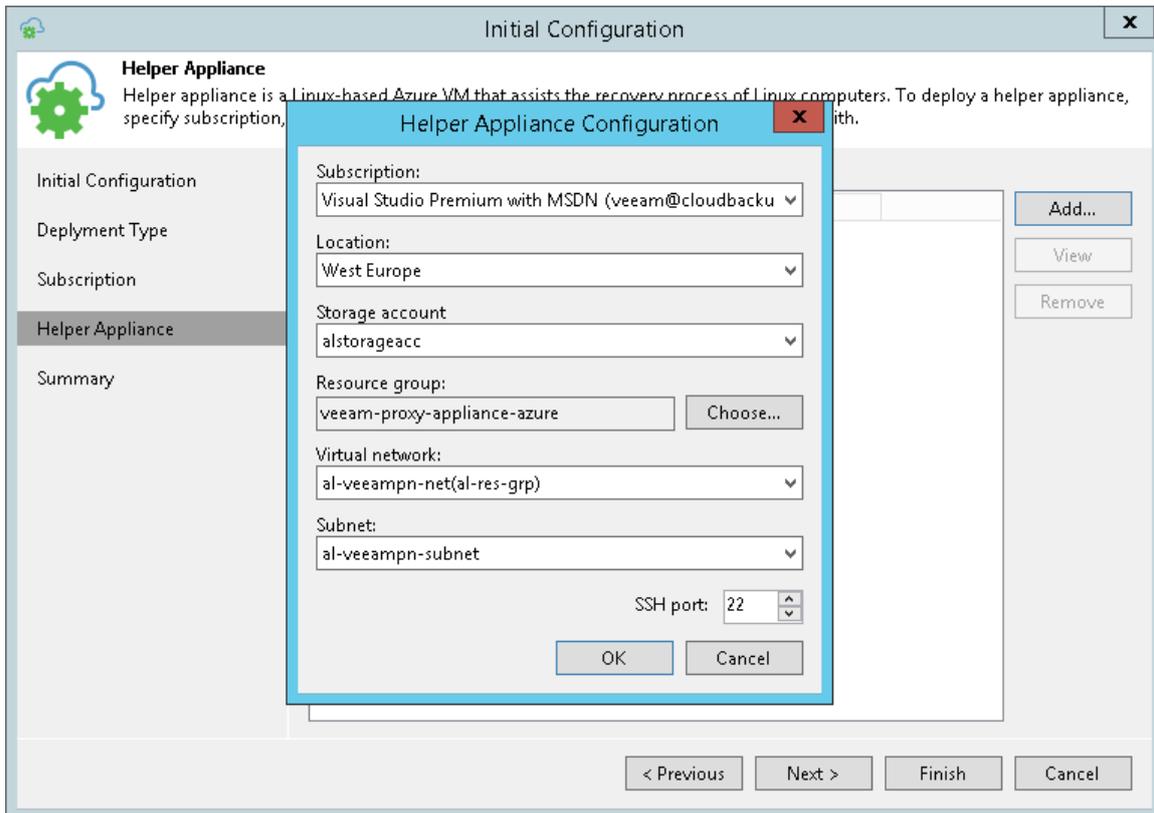


- At the **Subscription** step of the wizard, select the **Enable restore of Linux-based computers** check box.



- At the **Helper Appliance** step of the wizard, configure settings of the helper appliance.
 - On the right of the **Helper appliances** list, click **Add**.

- b. From the **Subscription** list, select a subscription whose resources you want to use to configure the helper appliance. The subscription list contains all subscriptions that are associated with the Microsoft Azure user account.
- c. From the **Location** list, select a location in which you want to configure the helper appliance. Make sure that you select a geographic region with which at least one storage account of the subscription is associated.
- d. From the **Storage account** list, select a storage account whose resources you want to use to store disks of the helper appliance.
- e. [Optional] Click **Choose** if you don't want Veeam Backup & Replication to create a new resource group.
- f. From the **Virtual network** list, select a network to which the helper appliance must be connected.
- g. From the **Subnet** list, select a subnet for the helper appliance.
- h. At the **SSH port** field, specify a port over which Veeam Backup & Replication will communicate with the helper appliance. By default, port 22 is used.
- i. Click **OK**.



6. Repeat steps from *a* to *i* for all locations to which you plan to restore Linux machines and click **Next**.

Changing Credentials for Helper Appliances

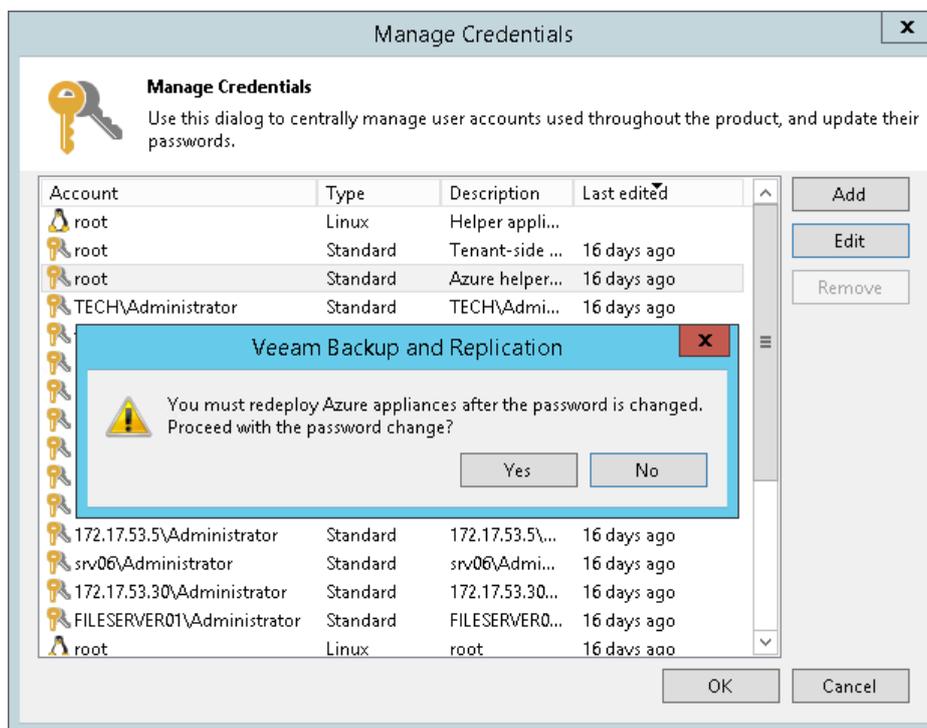
By default, Veeam Backup & Replication uses built-in credentials record to work with all helper appliances in Microsoft Azure and Azure Stack. For security reasons, it is recommended that you change a password for this credentials record before you set up helper appliances.

IMPORTANT!

When you change a password in the built-in credentials record, you must re-deploy existing helper appliances in Microsoft Azure and Azure Stack.

To change the password in a credentials record for helper appliances:

1. From the main menu, select **Manage Credentials**.
2. In the **Manage Credentials** window, click the Azure helper appliance credentials record.
3. Click **Edit**.
4. In the **Password** field, specify a new password.
5. Click **OK** to save changes.



Removing Helper Appliances

You can remove helper appliances from Microsoft Azure and Azure Stack, for example, if you no longer need to restore Linux machines to Azure or Azure Stack.

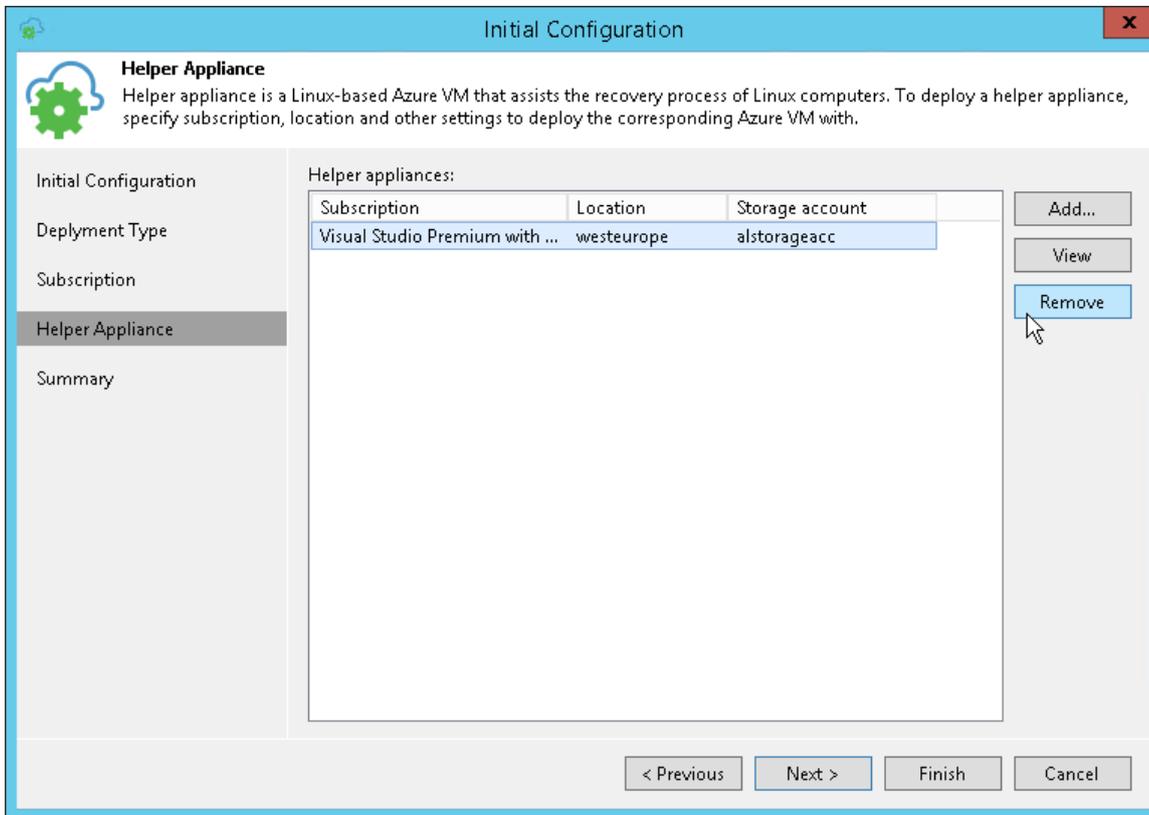
To remove a helper appliance, do the following:

1. From the main menu, select **Manage Cloud Credentials**.
2. In the accounts list, select the Azure account and click **Edit**.
3. Pass to the **Helper Appliance** step of the **Initial Configuration** wizard.

4. In the **Helper appliances** list, select the helper appliance and click **Remove**.

IMPORTANT!

Do not clear the **Enable restore of Linux-based computers** check box at the **Subscription** step of the wizard to remove helper appliances. In this case, the **Initial Configuration** wizard will not display the **Helper Appliance** step. Helper appliances themselves will remain in Microsoft Azure.



Configuring Azure Proxies

In some cases, upload of machine disks to Microsoft Azure may take a long time. This can happen if you restore machines to a distant location and the network connection is slow. To speed up the restore process, it is recommended that you deploy an Azure proxy in the backup infrastructure.

The Azure proxy is a small auxiliary machine in Microsoft Azure over which Veeam Backup & Replication transports VM disk data to blob storage. Veeam components installed on the Azure proxy compress and deduplicate disk data, which helps reduce network traffic and increase the speed of the restore process.

To configure an Azure proxy, you must pass through the **Azure Proxy** wizard. Veeam Backup & Replication will deploy a Microsoft Windows Server 2012 R2 machine in Microsoft Azure and assign the role of the Azure proxy to this machine. You can then instruct Veeam Backup & Replication to use the Azure proxy for restore tasks.

It is strongly recommended that you configure Azure proxies in the backup infrastructure. Azure proxies do not require a lot of resources and can speed up the restore process significantly. You should configure an Azure proxy in a location to which you plan to restore machines, or close to this location. If you plan to restore machines to different locations, you should configure at least one Azure proxy in each location.

The process of Azure proxy deployment takes some time. It is recommended that you configure the Azure proxy in advance, before you start the restore process.

Before you configure an Azure proxy, [check prerequisites](#). Then follow the Azure Proxy wizard steps to deploy the proxy.

Before You Begin

Before you configure an Azure proxy, check the following prerequisites:

- You must import information about your Microsoft Azure user account to Veeam Backup & Replication. For more information, see [Adding Azure Accounts](#) or [Adding Azure Stack Accounts](#).
- You must configure the following objects in Microsoft Azure beforehand:
 - Storage account whose resources you plan to use to store disks of the Azure proxy.
 - Networks to which you plan to connect the Azure proxy.

For storage accounts and network configuration, you must use the same deployment model that you plan to use for Azure proxy creation.

IMPORTANT!

When you deploy Azure proxy for Azure Stack, make sure that Windows Server 2012 R2 is available in Azure marketplace.

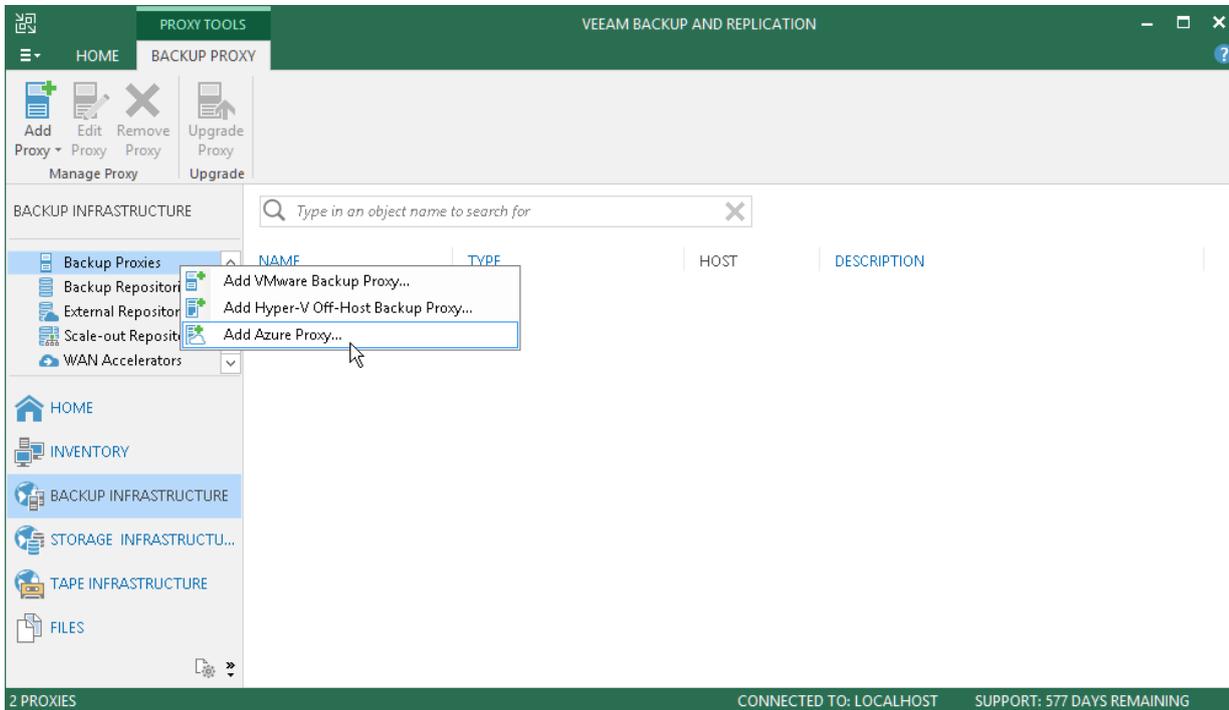
Step 1. Launch Azure Proxy Wizard

To launch the **Azure Proxy** wizard, do one of the following:

- Open the **Backup Infrastructure** view. In the inventory pane, select **Backup Proxies**, click the **Backup Proxy** node, and click **Add Proxy > Azure** on the ribbon.
- Open the **Backup Infrastructure** view. In the inventory pane, right-click **Backup Proxies** and select **Add Azure Proxy**.

IMPORTANT!

Before you start to configure an Azure proxy, you must import information about the Microsoft Azure user account. In the opposite case, the **Add Azure Proxy** option will not be available. For more information, see [Adding Azure Accounts](#) or [Adding Azure Stack Accounts](#).



Step 2. Specify Azure Proxy Name

At the **Name** step of the wizard, specify a name and description for the Azure proxy.

1. In the **Name** field, specify a name for the Azure proxy. The name must meet the following requirements:
 - The name must not be longer than 15 characters.
 - The name must contain only alphanumeric characters and hyphens.
 - The name must start with a letter and end with a letter or number.
 - The name must not contain only numeric characters.
 - The name must not contain special characters: `!@#\$%^&*()+=[{}|;:.",<>/?`.
2. In the **Description** field, provide a description for the Azure proxy. The default description contains information about the user who added the proxy, date and time when the proxy was added.
3. At the **Max concurrent tasks** field, specify the number of tasks that the Azure proxy must handle in parallel. If the **Max concurrent tasks** value is exceeded, the Azure proxy will not start a new task until one of current tasks finishes.

Veeam Backup & Replication creates one task per one machine disk. By default, Azure proxy handles 4 concurrent tasks.

The screenshot shows the 'Add Azure Proxy' wizard window. The 'Name' step is selected in the left-hand navigation pane. The main area contains the following fields:

- Name:** proxy001
- Description:** Microsoft Azure Proxy in North Europe
- Max concurrent tasks:** 4

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

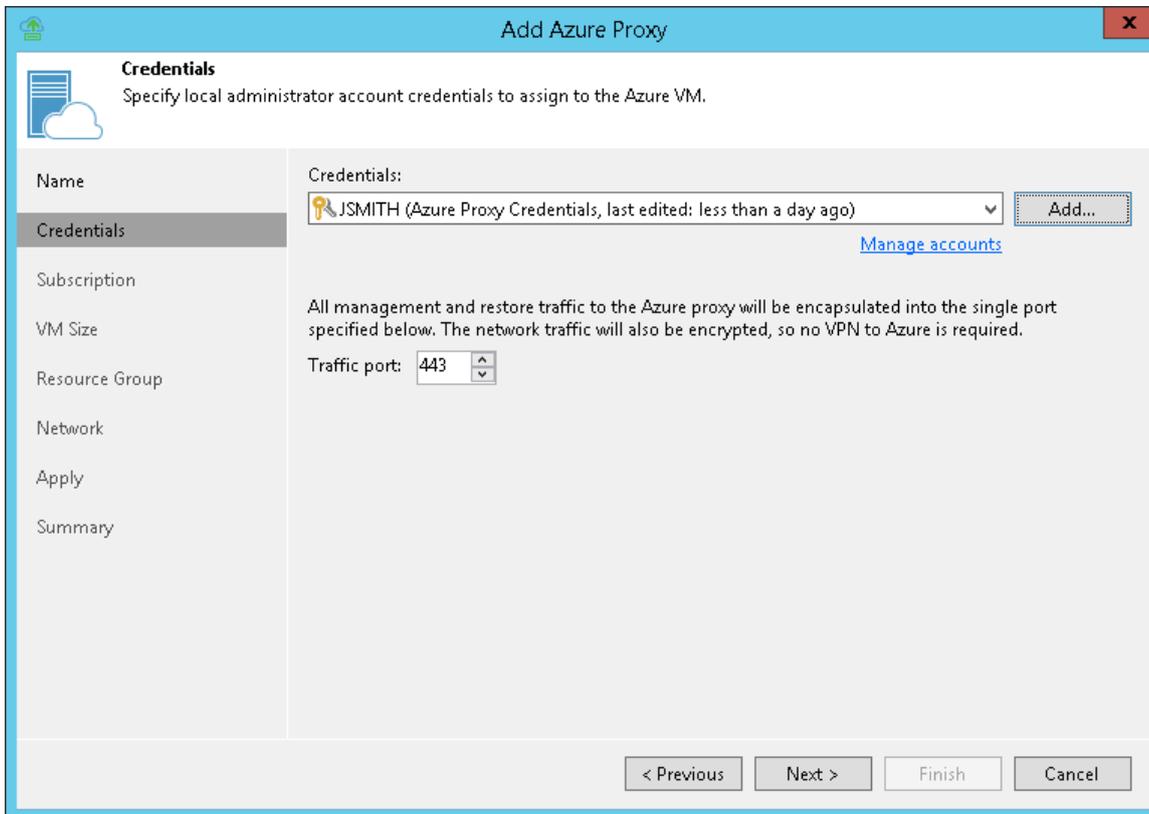
Step 3. Specify Credentials and Transport Port

At the **Credentials** step of the wizard, specify credentials of the local administrator account on the Azure proxy and define the transport port.

1. When you configure an Azure proxy, Veeam Backup & Replication creates an account with the Local Administrator permissions on this proxy. To specify a user name and password for this account, do the following:
 - a. On the right of the **Credentials** list, click the **Manage accounts** link or click **Add**.
 - b. In the **Credentials** window, enter a user name, password and description for the account.
You must specify the user name without a domain or Microsoft Azure machine name. The password must be at least 8 characters long, and must contain at least 1 uppercase character, 1 lowercase character, 1 numeric character and 1 special character.
 - c. Click **OK**.
2. In the **Traffic port** field, specify a port over which Veeam Backup & Replication will control components installed on the Azure proxy and transport VM disks data to blob storage. By default, port 443 is used. The port must be opened on the backup server and backup repository that stores VM backups.

IMPORTANT!

You cannot use reserved names such as 'administrator', 'admin', 'user', 'abc@123', 'P@\$\$wOrd' and so on as a user name and password of the local administrator account.



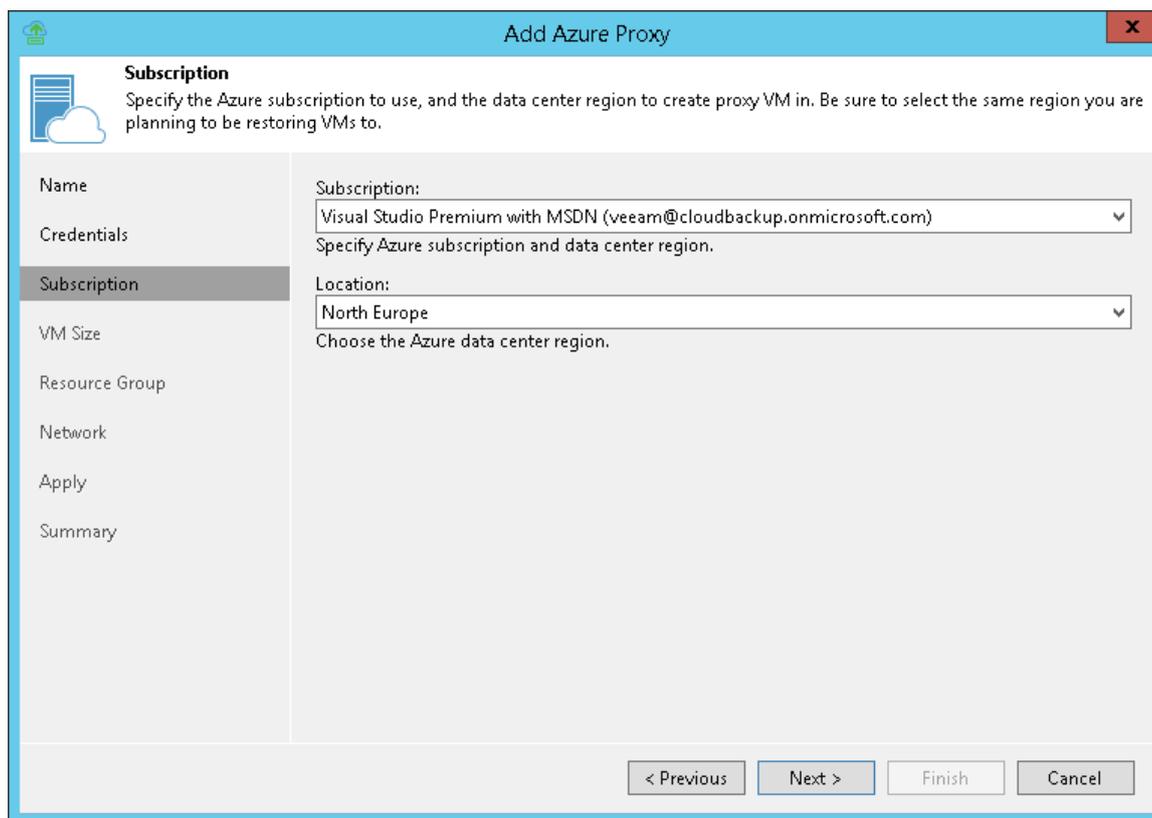
The screenshot shows the 'Add Azure Proxy' wizard in the 'Credentials' step. The window title is 'Add Azure Proxy'. The main heading is 'Credentials' with the instruction 'Specify local administrator account credentials to assign to the Azure VM.' On the left, a navigation pane lists 'Name', 'Credentials', 'Subscription', 'VM Size', 'Resource Group', 'Network', 'Apply', and 'Summary'. The 'Credentials' section is active, showing a dropdown menu with 'JSMITH (Azure Proxy Credentials, last edited: less than a day ago)' and an 'Add...' button. Below this is a 'Manage accounts' link. A text block states: 'All management and restore traffic to the Azure proxy will be encapsulated into the single port specified below. The network traffic will also be encrypted, so no VPN to Azure is required.' The 'Traffic port' is set to '443' with up and down arrows. At the bottom, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 4. Select Subscription and Location

At the **Subscription** step of the wizard, select a subscription and location for the Azure proxy.

1. From the **Subscription** list, select a subscription whose resources you want to use to deploy the Azure proxy. The subscription list contains all subscriptions associated with the user accounts that you have added to Veeam Backup & Replication.

2. From the **Locations** list, select a geographic region to which you want to place the Azure proxy. Make sure that you select a geographic region with which at least one storage account of the subscription is associated.



The screenshot shows the 'Add Azure Proxy' wizard in the 'Subscription' step. The window title is 'Add Azure Proxy'. The main heading is 'Subscription' with a sub-heading: 'Specify the Azure subscription to use, and the data center region to create proxy VM in. Be sure to select the same region you are planning to be restoring VMs to.' On the left, there is a navigation pane with the following items: Name, Credentials, Subscription (highlighted), VM Size, Resource Group, Network, Apply, and Summary. The main area contains two dropdown menus: 'Subscription:' with the value 'Visual Studio Premium with MSDN (veeam@cloudbackup.onmicrosoft.com)' and 'Location:' with the value 'North Europe'. Below the dropdowns, there is a note: 'Specify Azure subscription and data center region.' and 'Choose the Azure data center region.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 5. Select VM Size

At the **VM size** step of the wizard, you can select the size for the Azure proxy VM and specify what storage account you want to use to deploy the Azure proxy VM.

1. From the **Size** list, select the size for the Azure proxy.

By default, Veeam Backup & Replication selects *Basic_A2*. This size is typically sufficient to transport VM disks data to blob storage. If necessary, you can select a greater size for the Azure proxy.

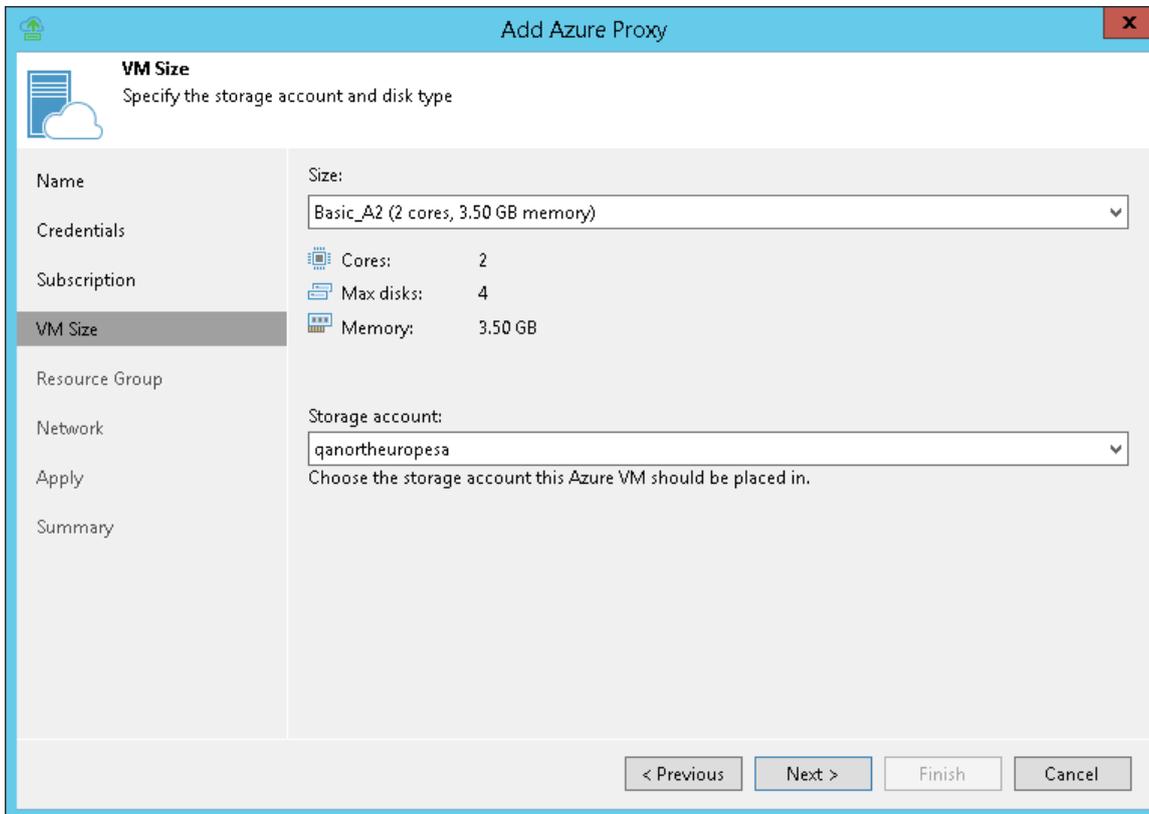
If you select a premium storage account, make sure that the VM size is compatible with the selected account.

2. From the **Storage account** list, select a storage account whose resources you want to use to store disks of the Azure proxy. The storage account must be compatible with the VM size you select.

The list of storage accounts will contain only general purpose storage accounts. Blob storage accounts will not be displayed in the list of subscriptions. For more information about account types, see <https://azure.microsoft.com/en-us/documentation/articles/storage-create-storage-account/>.

TIP:

Microsoft Azure subscriptions have default limits on the number of CPU cores. Make sure that the VM size you select does not exceed limits of the subscription.



The screenshot shows the 'Add Azure Proxy' wizard window, specifically the 'VM Size' step. The window title is 'Add Azure Proxy' and the subtitle is 'VM Size Specify the storage account and disk type'. On the left, there is a navigation pane with options: Name, Credentials, Subscription, VM Size (selected), Resource Group, Network, Apply, and Summary. The main area contains a 'Size:' dropdown menu set to 'Basic_A2 (2 cores, 3.50 GB memory)'. Below this, the specifications are listed: Cores: 2, Max disks: 4, and Memory: 3.50 GB. There is also a 'Storage account:' dropdown menu set to 'qanortheuropesa'. Below the storage account dropdown, there is a note: 'Choose the storage account this Azure VM should be placed in.' At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 6. Select Resource Group

At the **Resource Group** step of the wizard, you can specify settings of the resource group to which the Azure proxy must be placed.

By default, Veeam Backup & Replication creates a new resource group for the Azure proxy and places the proxy to it. If necessary, you can place the proxy to an existing resource group.

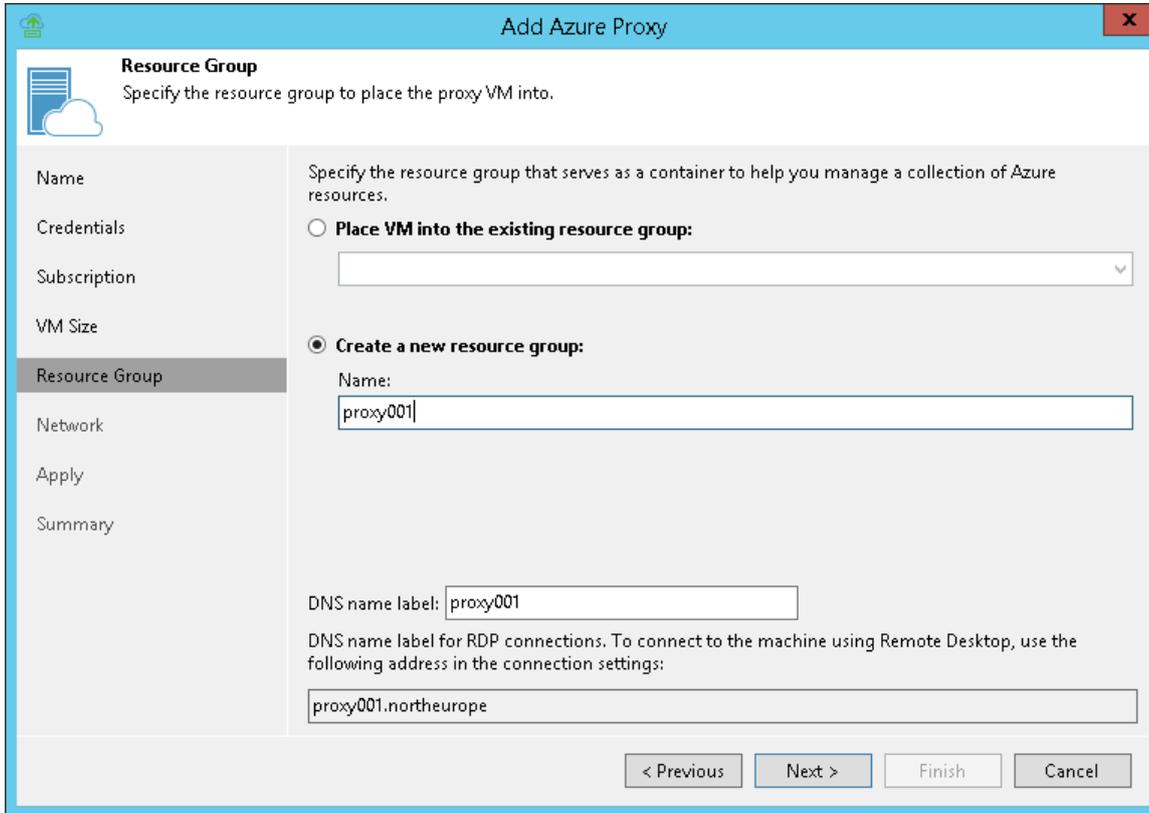
Select the necessary option for the Azure proxy:

- If you want to place the Azure proxy to an existing resource group, select **Place VM into the existing resource group**. From the list below, select the necessary resource group.
- If you want to create a dedicated resource group for the Azure proxy, select **Create a new resource group**. In the **Name** field, enter a name for the new resource group. The resource group name can be up to 64 characters long, and can contain only alphanumeric, underscore and hyphen characters.

In the new resource group, Veeam Backup & Replication automatically creates a Network Security Group, dynamic public IP and network interface. In the DNS name label field, enter a name of for the new dynamic public IP created with Veeam Backup & Replication. The DNS name label can be up to 80 characters long, and can contain only alphanumeric, dash and underscore characters. For more information, see <https://docs.microsoft.com/en-us/azure/architecture/best-practices/naming-conventions>.

TIP:

Microsoft Azure subscriptions have default limits on the number of resource groups. If you decide to create a new resource group, make sure that you do not exceed limits of the subscription.

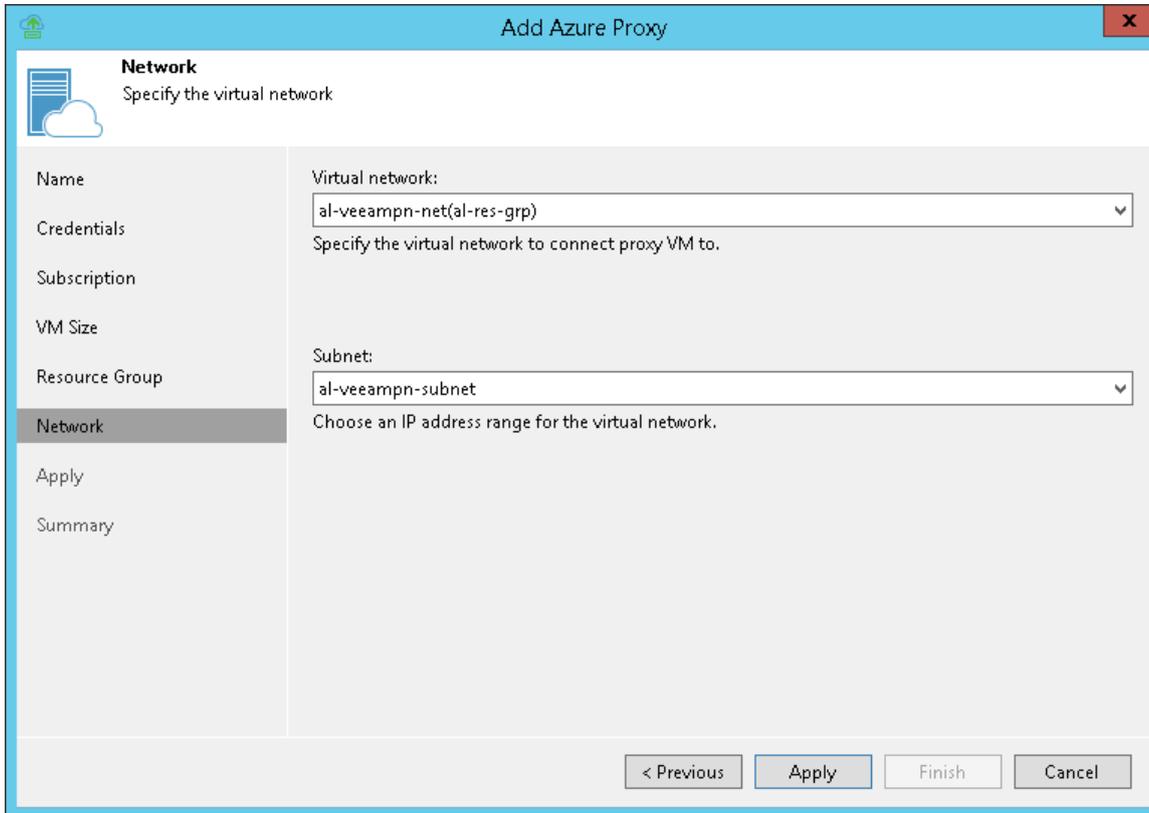


Step 7. Select Virtual Network

At the **Network** step of the wizard, you can select to which network and subnet the Azure proxy must be connected.

To define network settings for the Azure proxy:

1. From the **Virtual network** list, select a network to which the Azure proxy must be connected.
2. From the **Subnet** list, select a subnet for the Azure proxy.



The screenshot shows a wizard window titled "Add Azure Proxy" with a close button in the top right corner. The main area is titled "Network" with the instruction "Specify the virtual network". On the left, there is a navigation pane with the following items: Name, Credentials, Subscription, VM Size, Resource Group, Network (highlighted), Apply, and Summary. The main content area contains two dropdown menus. The first is labeled "Virtual network:" and has the value "al-veeamprn-net(al-res-grp)". Below it is the text "Specify the virtual network to connect proxy VM to.". The second dropdown is labeled "Subnet:" and has the value "al-veeamprn-subnet". Below it is the text "Choose an IP address range for the virtual network.". At the bottom of the window, there are four buttons: "< Previous", "Apply", "Finish", and "Cancel".

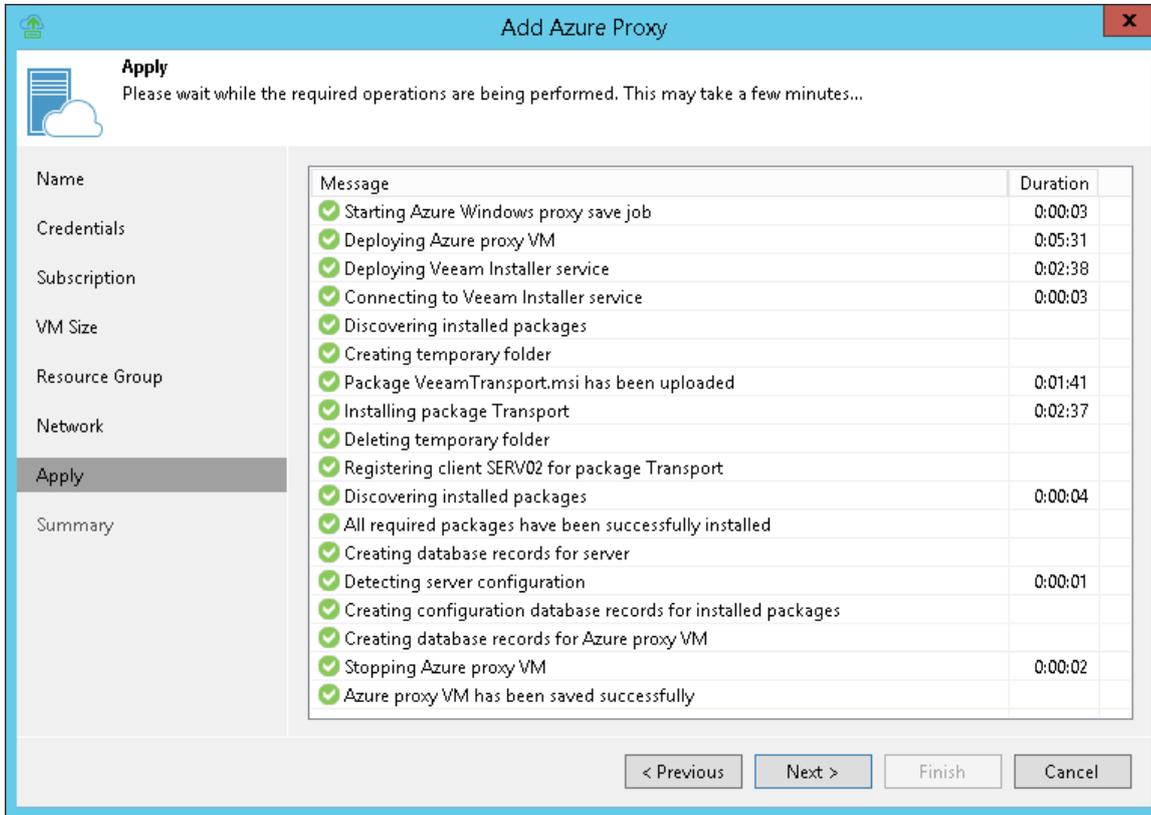
Step 8. Start Azure Proxy Configuration

At the **Apply** step of the wizard, Veeam Backup & Replication deploys the Azure proxy with specified settings. You can view the deployment progress in the real-time mode.

When the configuration process is over, click **Next**. At the **Summary** step of the wizard, click **Finish** to close the wizard.

TIP:

The Azure proxy deployment may take several minutes. You can close the **Azure Proxy** wizard and continue working with Veeam Backup & Replication while the proxy is being deployed. To view the deployment progress, open the **History** view, in the inventory pane select **System**, and double-click the task of the proxy deployment in the working area.



Removing Azure Proxies

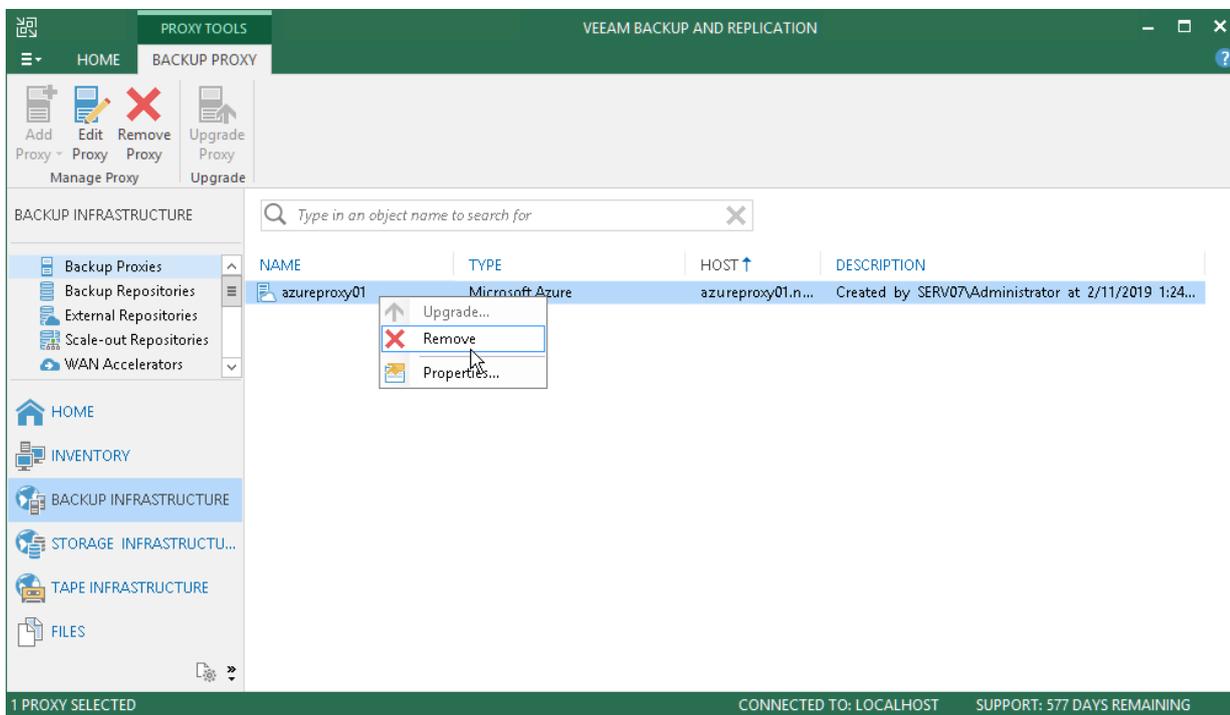
Veeam Backup & Replication does not provide a possibility to edit settings of deployed Azure proxies. If you want to change Azure proxy configuration, remove the Azure proxy and create a new proxy.

To remove an Azure proxy, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Backup Proxies**.
3. In the working area, right-click the Azure proxy and select **Remove**.

IMPORTANT!

If you want to remove an Azure or an Azure Stack account from Veeam Backup & Replication, you must remove all Azure proxies first.



Creating Backup Files

You can restore machines to Microsoft Azure from the following types of backups:

- Backup files of Microsoft Windows and Linux VMs created with Veeam Backup & Replication. VeeamZIP files and backups created with Veeam Backup & Replication and Veeam Backup & Replication. You can use backups of VMware vSphere VMs and VMware vCloud Director VMs.
- Backups of Microsoft Windows machines created with Veeam Agent for Windows. Backups must be created at the entire machine level or volume level.
- Backups of Linux machines created with Veeam Agent for Linux. Backups must be created at the entire machine level or volume level.
- Backups of EC2 instances created with [N2WS Backup & Recovery](#).
- Backups of Nutanix AHV VMs created with [Veeam Availability for Nutanix AHV](#).

You can restore a machine to the latest restore point or any previous restore point in the backup chain. A backup chain from which you plan to restore a machine must reside on a backup repository added to the backup infrastructure.

You can also import a backup to the Veeam Backup & Replication console. For more information, see [Importing Backups](#).

Restoring Machines

You can restore machines from backups to Microsoft Azure or Azure Stack. The restored machine appears in the Microsoft Azure portal, and you can use it as a regular Microsoft Azure VM.

IMPORTANT!

After the restore process is finished, Veeam Backup & Replication immediately powers on the restored VM.

Before you restore a machine to Microsoft Azure, [check prerequisites](#). Then use the **Restore to Azure** wizard to restore the machine.

Before You Begin

Before you restore a machine to Microsoft Azure, mind the following prerequisites and limitations.

Prerequisites

- You must add a Microsoft Azure account to Veeam Backup & Replication. For more information, see [Adding Microsoft Azure Accounts](#).
- You must configure the following objects in Microsoft Azure beforehand:
 - Storage account whose resources you plan to use to store disks of the restored machine.
 - Networks to which you plan to connect the restored machine.

For storage accounts and network configuration, you must use the same deployment model that you plan to use for machine restore.

- [For restore of Linux machines] You must configure a helper appliance in the location to which you plan to restore a machine. For more information, see [Configuring Helper Appliances](#).
- [For speeding up the restore] If you plan to restore machines to a distant location, you can configure Azure proxies through which machine disks will be transported to blob storage. For more information, see [Configuring Microsoft Azure Proxies](#).

[For speeding up restore from Capacity Tier] It is strongly recommended to use Azure proxy when you restore from backups residing on a Capacity Tier. For more information, see [Configuring Microsoft Azure Proxies](#).

- You must create a backup of the machine that you want to restore in Microsoft Azure. For more information, see [Creating Backup Files](#).
- You must check limitations for restoring machines to Microsoft Azure. For more information, see [Restore to Microsoft Azure](#).
- You must set up correct time on the backup server. Otherwise you may not be able to add a Microsoft Azure account to Veeam Backup & Replication, or the restore process may fail.

Limitations

- Veeam Backup & Replication supports restore to Microsoft Azure for the following machines:
 - Microsoft Windows machines running Windows Server 2008/Windows Vista and later
 - Linux machines (see the Supported Distributions & Versions section: <https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-linux-endorsed-distros>).
- Mind the following limitations of disk sizes for Azure VMs and Azure stack VMs:
 - **[Azure VMs]** At the release date of Veeam Backup & Replication 9.5 Update 4, the maximum size for unmanaged virtual machine disks for Azure VM is 4095 GB. For details, see <https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits#virtual-machines-limits>.

When you restore a VM to Azure, VM disks can increase in size because of conversion. Thus, Veeam Backup & Replication does not allow to restore disks larger than 4093 GB.

Support of bigger-sized unmanaged disks is in public preview and will be supported in one of the following updates of Microsoft Azure. When the bigger-sized unmanaged disks become generally available, you will be able to restore VMs with disks larger than 4093 GB. To restore VMs with such disks, you must create a registry key with the following parameters:

Registry key location: *HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication*

Registry key name: *AzureMaxDiskSizeGB*

Type: *REG_DWORD*

Value: *8189* (For example, for 8191 GB disks, it is recommended to set 2 GB less)

After you set the registry key, restart the Veeam Backup service and the Veeam Backup & Replication console.

- **[Azure Stack VMs]** At the release date of Veeam Backup & Replication 9.5 Update 4, the maximum size for unmanaged virtual machine disks for Azure Stack VM is 1023 GB.

When you restore a VM to Azure Stack, VM disks increase in size because of conversion. Thus, Veeam Backup & Replication does not allow to restore disks larger than 1021 GB. You can regulate the maximum size of VM disks by creating the *AzureStackMaxDiskSizeGB* registry key as shown above for the Azure VMs.

- If the system disk of an initial machine uses the GPT partitioning scheme, the number of partitions on the disk cannot exceed 4. During restore such disk will be converted to a disk with the MBR partitioning scheme.
- The restore to Microsoft Azure functionality does not support the Azure Hybrid Use Benefit program.

Step 1. Launch Restore to Azure Wizard

To begin the restore process, do the following:

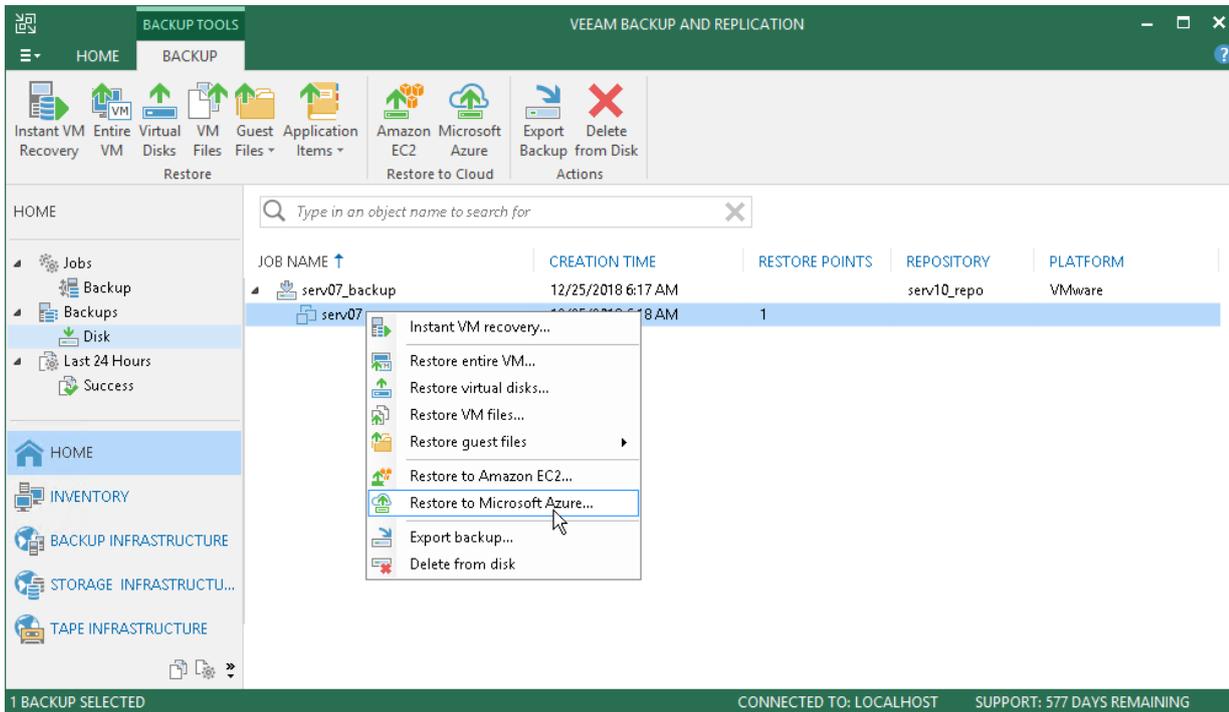
1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, expand the necessary backup, right-click the machine that you want to restore and select **Restore to Microsoft Azure**.

In this case, you will pass to the [Subscription](#) step of the wizard.

Alternatively, you can do one of the following:

- [VMware vSphere] On the **Home** tab, click **Restore > VMware vSphere > Restore from backup > Entire VM restore > Restore to Microsoft Azure**.
- [Amazon EC2] On the **Home** tab, click **Restore > Amazon EC2 > Entire machine restore > Restore to Microsoft Azure**.
- [Nutanix AHV] On the **Home** tab, click **Restore > Nutanix AHV > Entire machine restore > Restore to Microsoft Azure**.
- [Agents] On the **Home** tab, click **Restore > Agents > Entire machine restore > Restore to Microsoft Azure**.

- Double-click a full backup file (VBK) or backup metadata file (VBM) in a file browser. Veeam Backup & Replication will start its console. In the **Backup Properties** window, select the necessary machine and click **Restore > Restore to Microsoft Azure**. In this case, you will pass to the [Subscription](#) step of the wizard.

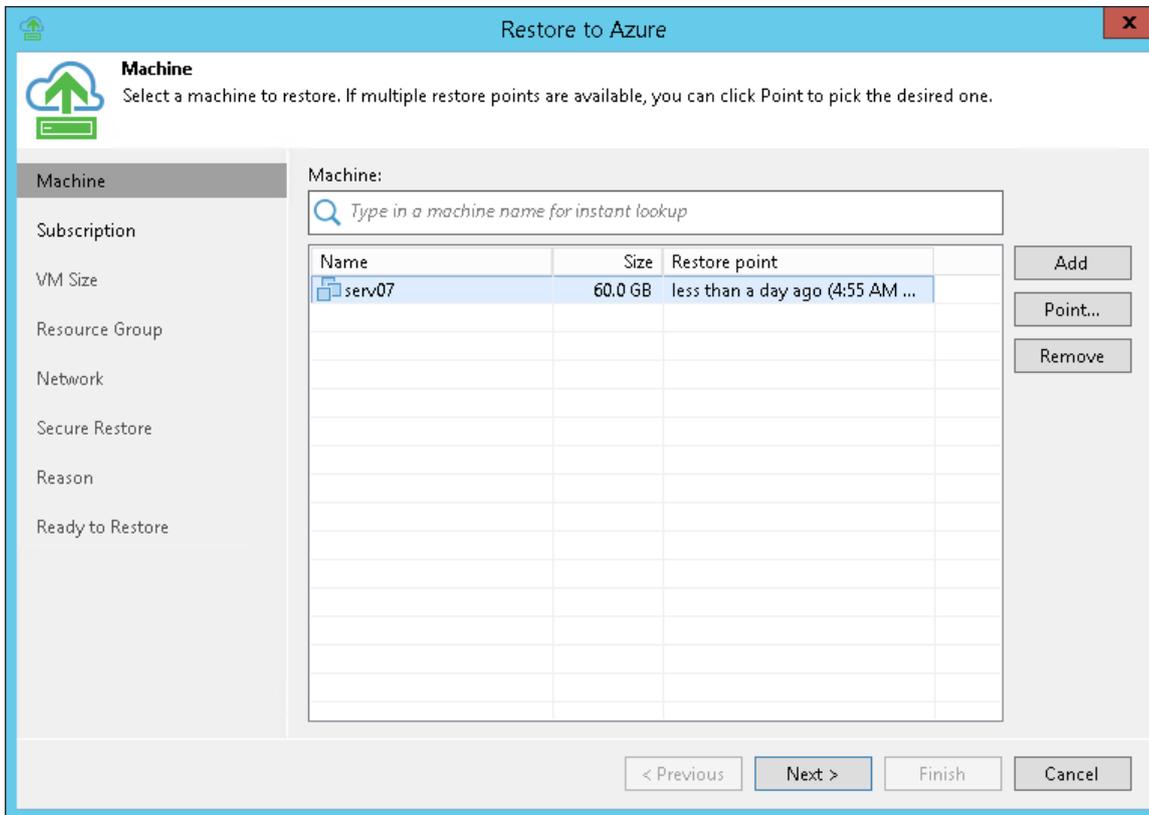


Step 2. Select Machine and Restore Point

At the **Machine** step of the wizard, specify the machine that you want to restore and specify restore points to which you want to restore the machine.

To select a machine to restore:

1. On the right of the **Machine** list, click **Add**.
2. In the **Backup Browser** window, expand the required backup, select the machine and click **Add**. You can add several machines to the list to perform batch restore.

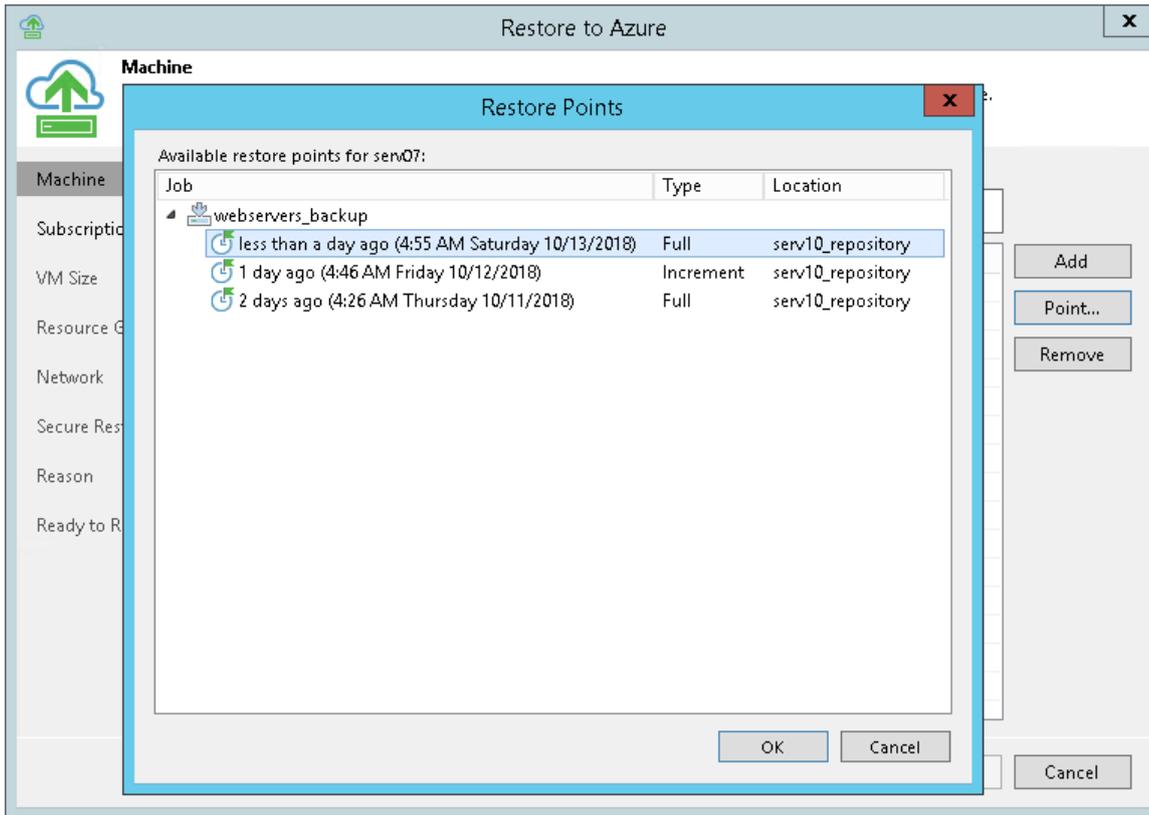


By default, Veeam Backup & Replication restores a machine to latest valid restore point in the backup chain. However, you can restore the machine to an earlier restore point.

To select a restore point, do the following:

1. In the **Machine** list, select the machine.
2. Click **Point** on the right.

3. In the **Restore Points** window, select a restore point to which you want to restore the machine.



Step 3. Select Subscription and Location

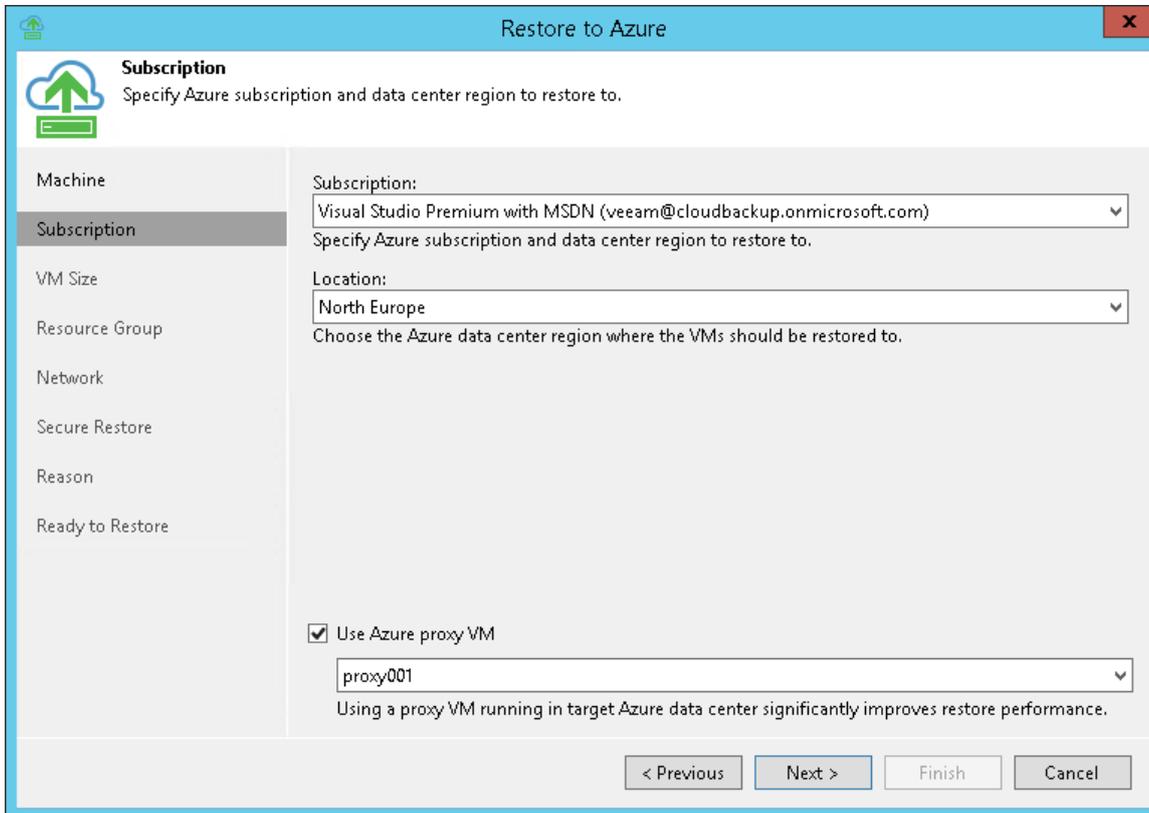
At the **Subscription** step of the wizard, you must select a subscription, location for the restored machine and define how machine data must be transported to Microsoft Azure or Azure Stack.

1. From the **Subscription** list, select a subscription whose resources you want to use. The subscription list contains all subscriptions associated with the user accounts that you have added to Veeam Backup & Replication.
2. From the **Locations** list, select a geographic region to which you want to place the restored machine. Make sure that you select a geographic region with which at least one storage account of the subscriptions is associated.
3. If you are restoring the machine to a distant location and want to speed up the restore process, select the **Use Azure proxy VM** check box. From the **Proxy VM** list, select a Microsoft Azure proxy.

It is recommended that you configure the Azure proxy in the same location to which you plan to restore the machine. For more information, see [Configuring Azure Proxies](#).

IMPORTANT!

[For restore of Linux machines] You must have a preconfigured helper appliance in the location to which you are restoring a Linux machine. If the appliance is not configured, Veeam Backup & Replication will display the **Initial Configuration** wizard so that you can configure the appliance in the selected location.



The screenshot shows the 'Restore to Azure' wizard window. The title bar reads 'Restore to Azure'. The main window has a blue header with a home icon and a close button. Below the header, there is a 'Subscription' section with a green cloud icon and a plus sign. The text says 'Specify Azure subscription and data center region to restore to.' On the left, there is a navigation pane with the following items: Machine, Subscription (selected), VM Size, Resource Group, Network, Secure Restore, Reason, and Ready to Restore. The main area contains two dropdown menus: 'Subscription:' with the value 'Visual Studio Premium with MSDN (veeam@cloudbackup.onmicrosoft.com)' and 'Location:' with the value 'North Europe'. Below these, there is a checkbox labeled 'Use Azure proxy VM' which is checked, and a dropdown menu with the value 'proxy001'. A note below the checkbox says 'Using a proxy VM running in target Azure data center significantly improves restore performance.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 4. Specify VM Size

At the **VM Size** step of the wizard, you can:

- [Select a size and storage account for the restored machine](#)
- [Exclude specific disks from the restored machine](#)

Selecting VM Size and Storage Account

To select a size and storage account for the machine:

1. In the **Azure VM Configuration** list, select the machine and click **Edit**.
2. From the **Size** list, select a size for the restored VM. By default, Veeam Backup & Replication selects the smallest VM size that can support the number of disks for the restored machine.

Make sure that you select the right VM size that corresponds to the initial machine configuration. The VM size affects the number of CPU cores, memory and disk resources that will be allocated to the restored machine. For more information, see <https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-size-specs/>.

3. From the **Storage account** list, select a storage account whose resources you want to use to store disks of the restored machine. The storage account must be compatible with the VM size you select.

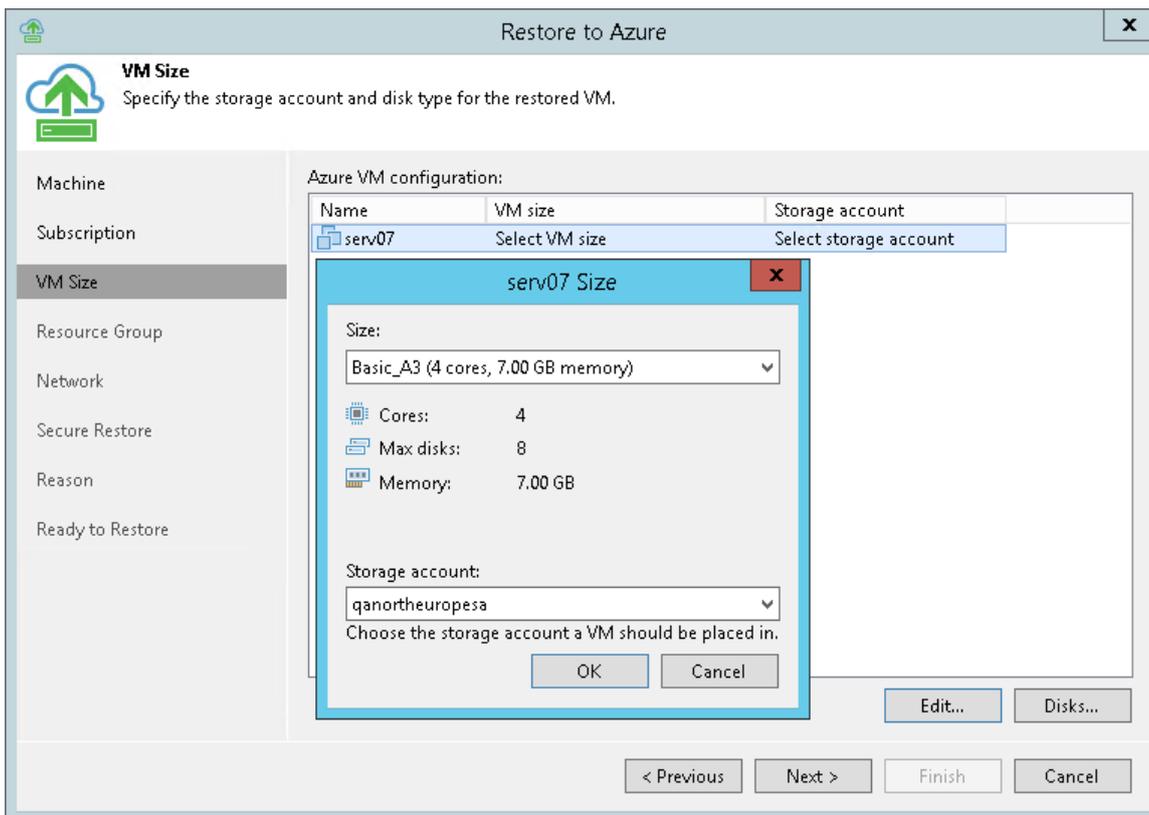
The list of storage accounts contains only general purpose storage accounts. Blob storage accounts are not be displayed in the list of subscriptions. For more information about account types, see <https://azure.microsoft.com/en-us/documentation/articles/storage-create-storage-account/>.

If you select a premium storage account, make sure that the VM size is compatible with the selected account.

4. Click **OK**.

TIP:

Microsoft Azure subscriptions have default limits on the number of CPU cores. Make sure that the VM size you select does not exceed limits of the subscription.



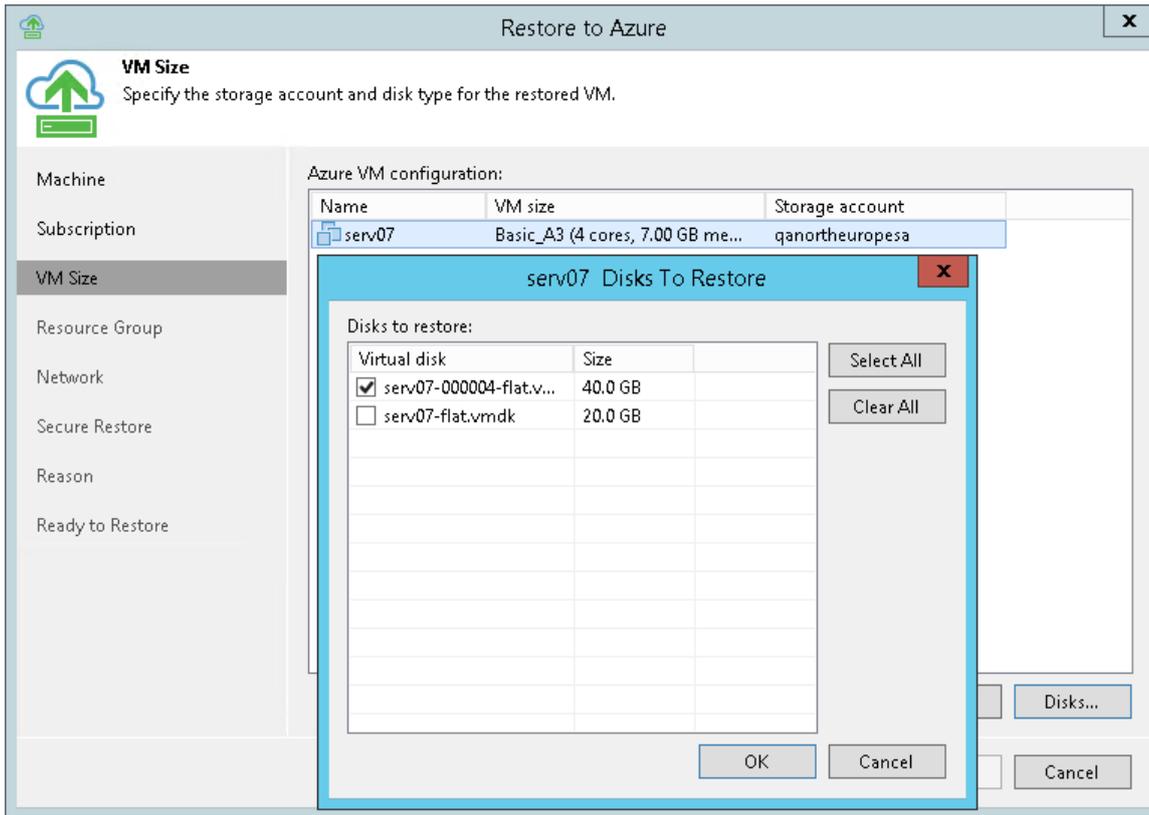
Excluding Machine Disks

If necessary, you can restore only specific disks of the machine.

To exclude specific disks of a machine:

1. In the **Azure VM Configuration** list, select the machine and click **Exclusions**.

2. In the **Disks to restore** window, select check boxes next to disks that you want to restore.



Step 5. Specify VM Name and Resource Group

At the **Resource Group** step of the wizard, you can:

- [Specify a new name for the restored machine](#)
- [Select a resource group for the restored machine](#)

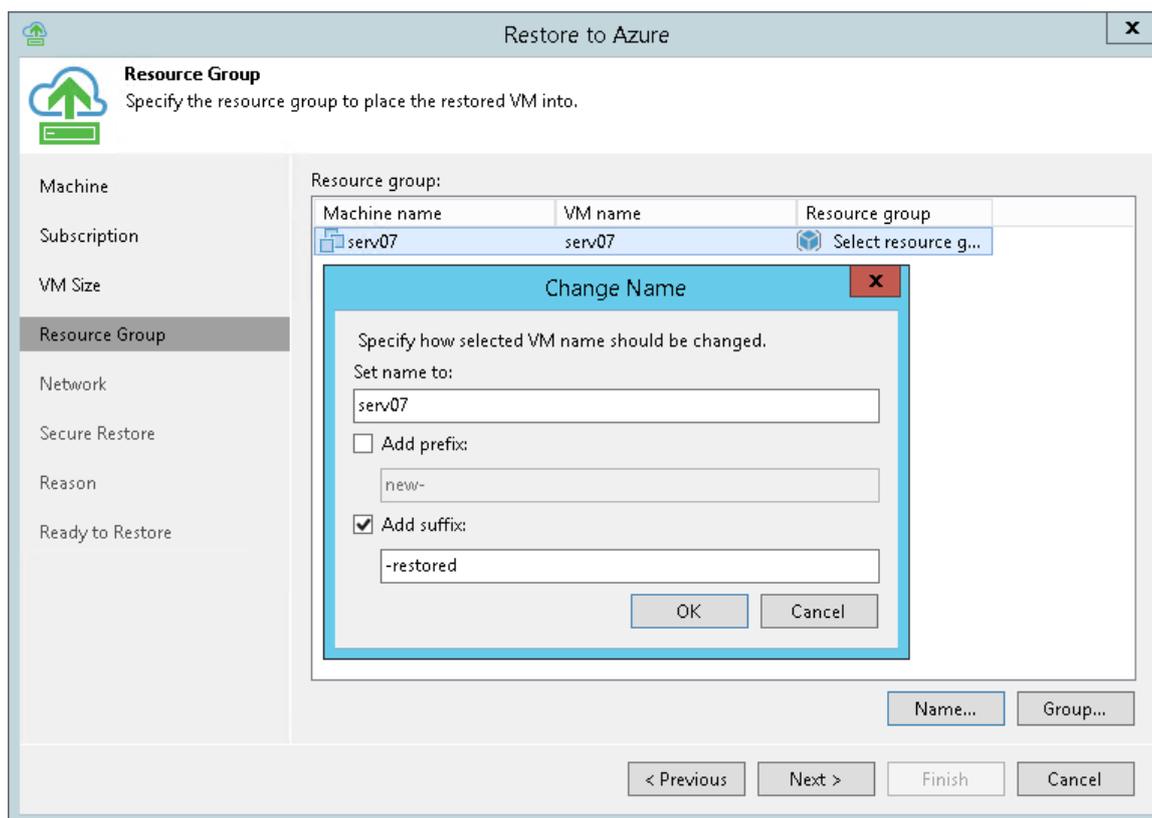
Specifying Name for Machine

By default, Veeam Backup & Replication restores a machine with its original name. However, you can define a new name for the restored machine if necessary.

To define a new name for the machine:

1. In the **Resource group** list, select the machine and click **Name**.

2. In the **Change Name** window, enter a new name explicitly or specify a change name rule – add a prefix and/or suffix to the original machine name.



Selecting Resource Group

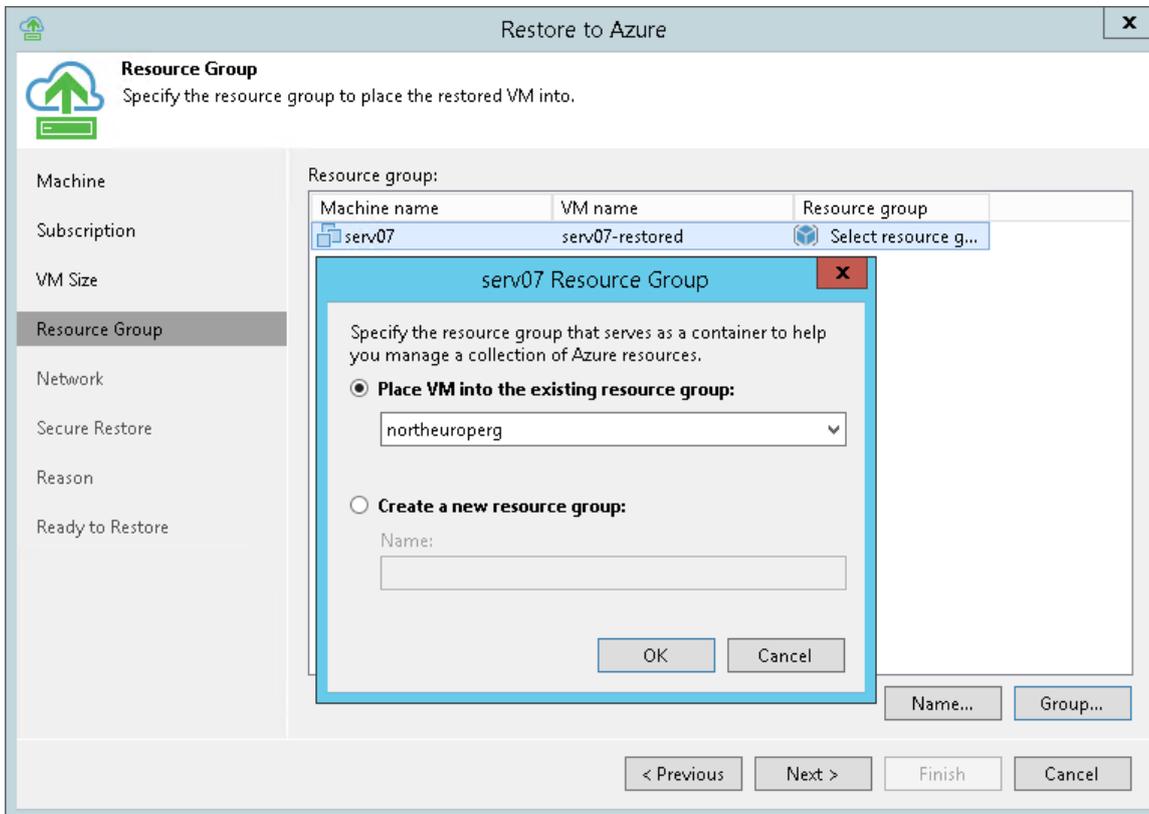
By default, Veeam Backup & Replication creates a new resource group for the restored machine and places the machine to it. If necessary, you can place the machine to an existing resource group.

1. In the **Resource group** list, select the machine and click **Group**.
2. In the **VM Resource Group** window, select the necessary option for the machine:
 - Select **Place VM into the existing resource group** if you want to place the machine to an existing resource group. From the list below, select the necessary resource group.
 - Select **Create a new resource group** if you want to create a dedicated resource group for the restored machine. In the **Name** field, enter a name for the new resource group.

In the new resource group, Veeam Backup & Replication automatically creates a Network Security Group, a dynamic public IP and network interface.

TIP:

Microsoft Azure subscriptions have default limits on the number of resource groups. If you decide to create a new resource group, make sure that you do not exceed limits of the subscription.



Step 6. Select Virtual Network

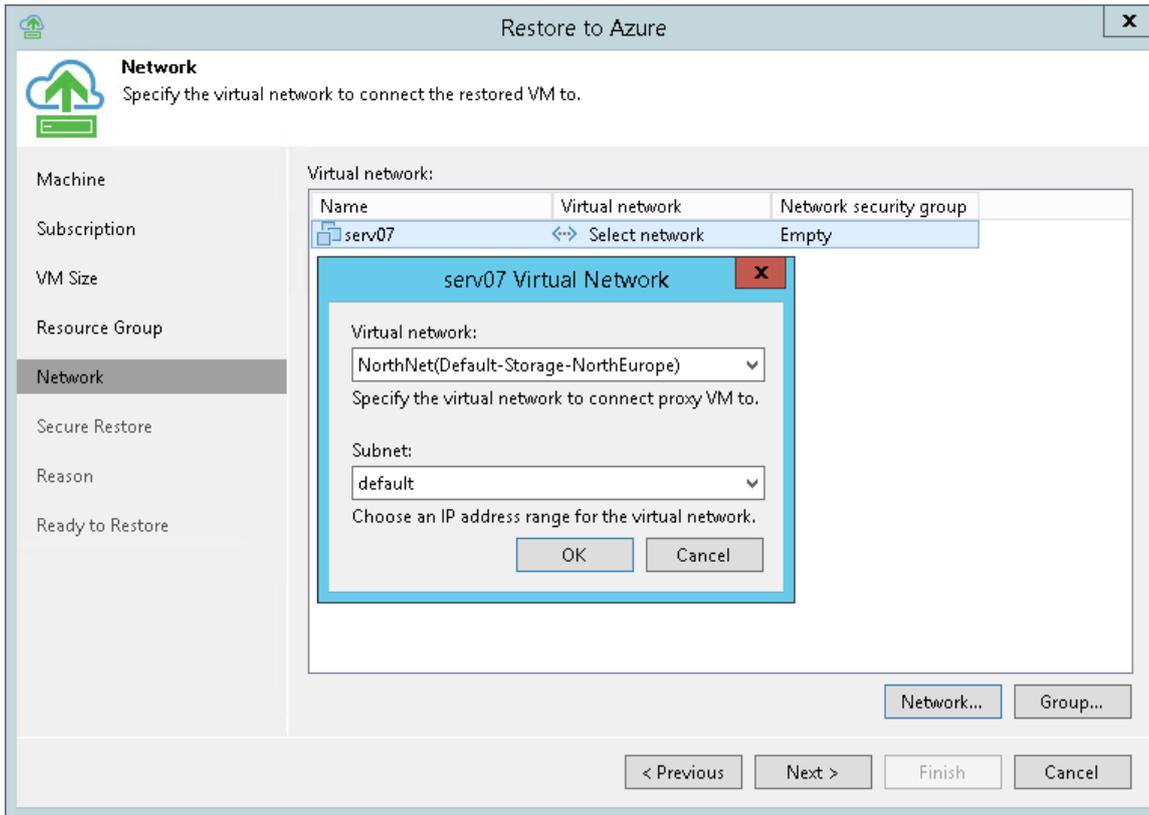
At the **Network** step of the wizard, you can select to which network and subnet the restored machine must be connected.

Veeam Backup & Replication can connect the machine only to one virtual network. If necessary, you can manually configure additional network connections in Microsoft Azure after the machine is restored.

To define network settings for the machine, do the following:

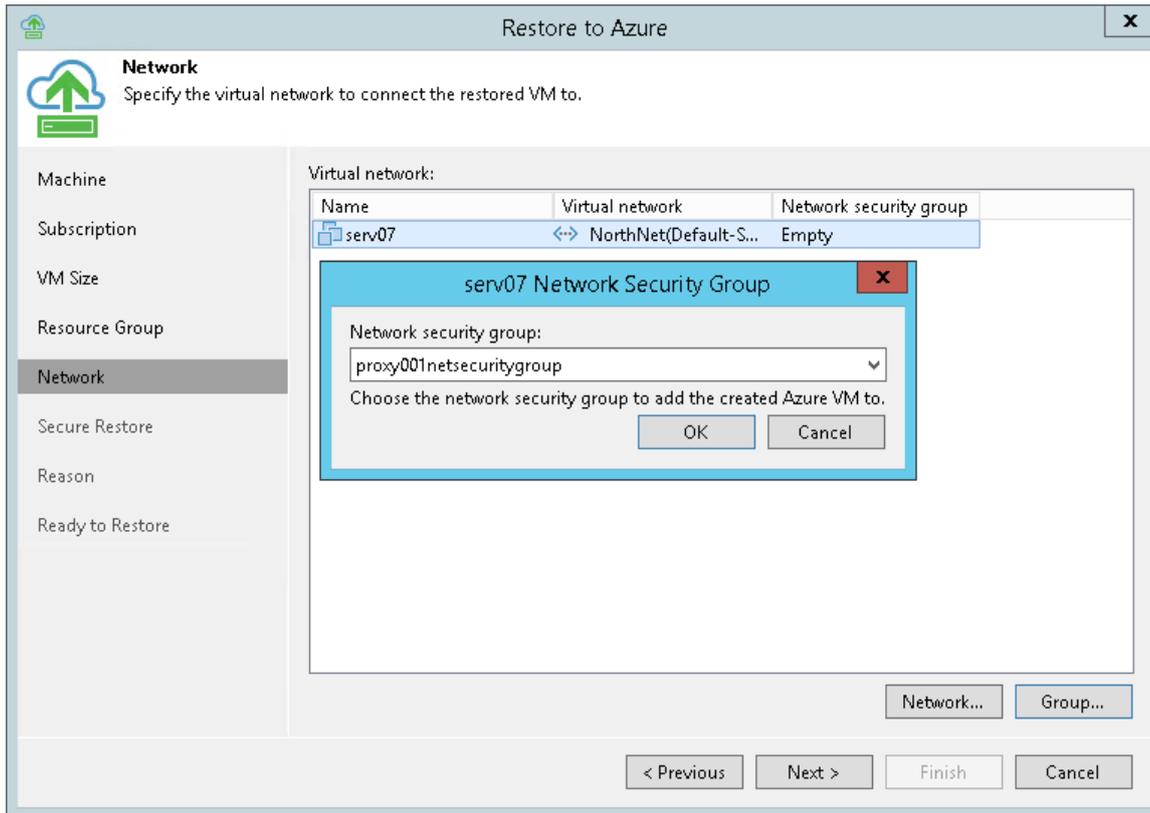
1. In the **Virtual network** list, select the machine and click **Network**.
2. From the **Virtual network** list, select a network to which the machine must be connected.

3. From the **Subnet** list, select a subnet for the machine and click **OK**.



4. From the **Virtual network** list, select the machine and click **Group**.
5. [Optional] Select the network security group from the list and click **OK**. The restored machine will be added to the selected network security group.

If you leave the field empty, Veeam Backup & Replication will create a new network security group.



Step 7. Specify Malware Scan Options

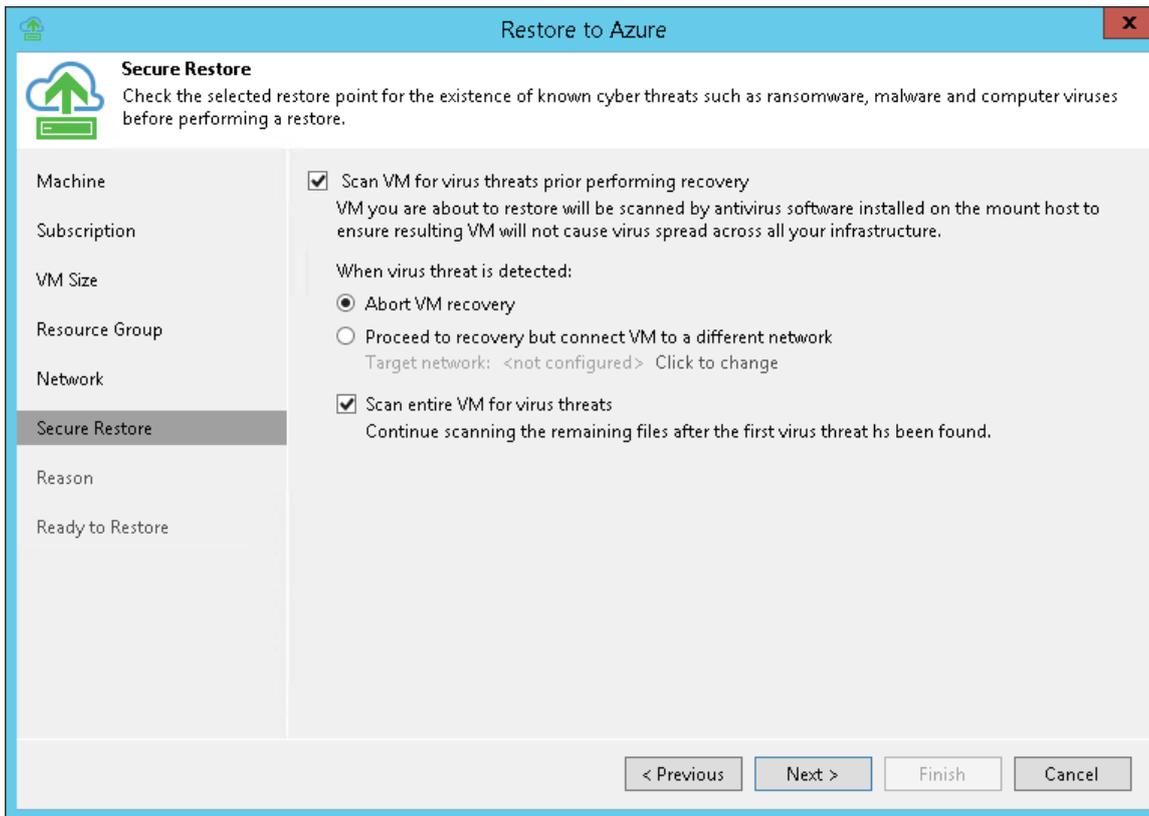
You can instruct Veeam Backup & Replication to perform secure restore – scan machine data with antivirus software before restoring the machine to Microsoft Azure or Azure Stack. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

1. At the **Secure Restore** step of the wizard, select the **Scan VM for virus threats prior performing recovery** check box.
2. Select which action Veeam Backup & Replication will take if the antivirus finds a virus threat:
 - **Abort VM recovery.** Select this action if you want Veeam Backup & Replication to cancel the restore session.
 - **Proceed recovery but connect VM to a different network.** Select this action if you want to restore the machine to a different Microsoft Azure virtual network.

Click the **Click to change** link to select the virtual network.

3. Select the **Scan entire VM for virus threats** check box if you want the antivirus to continue machine scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).

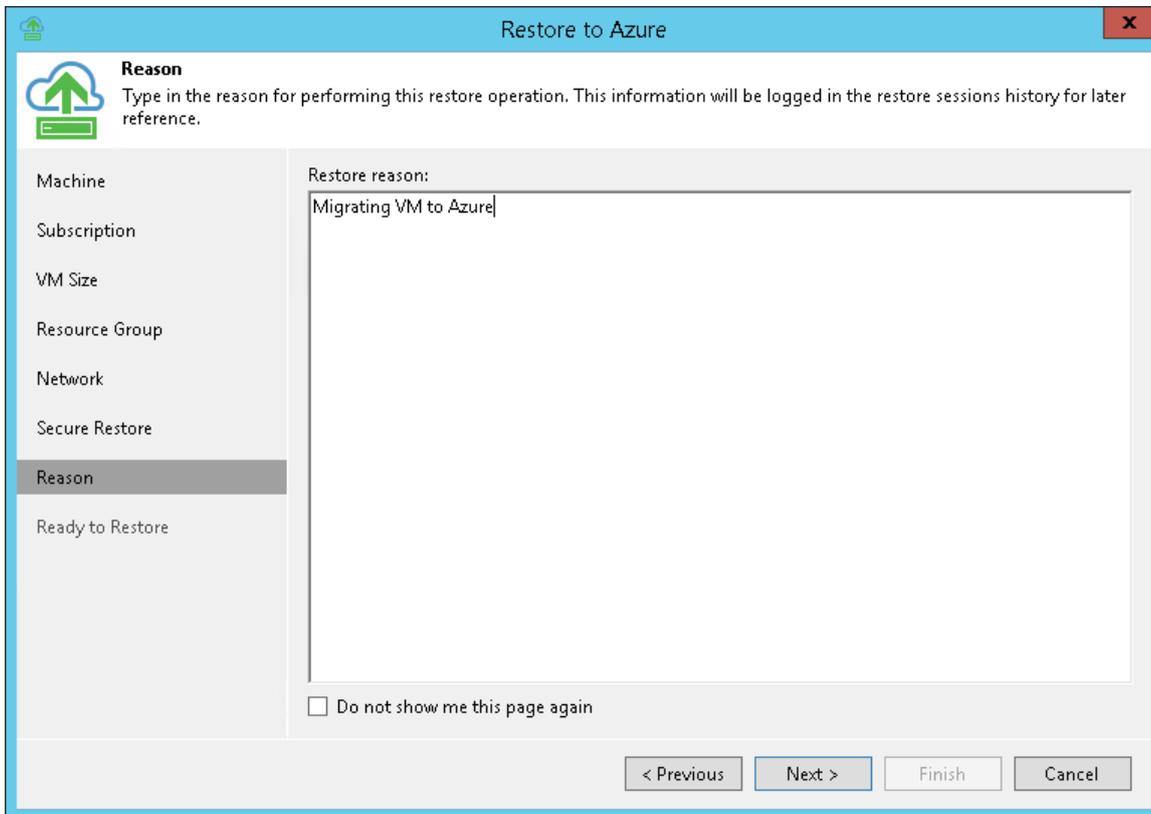


Step 8. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the machine. The information you provide will be saved in the session history in Veeam Backup & Replication, and you can view it later.

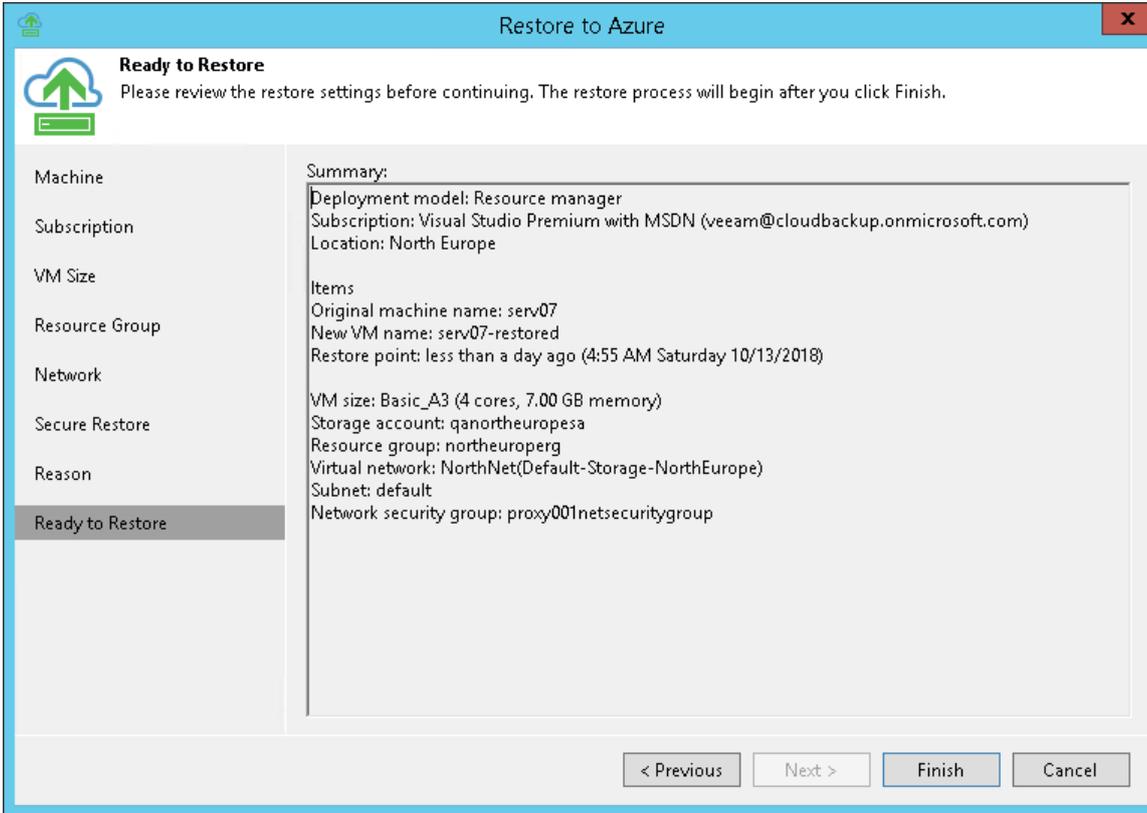
TIP:

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.



Step 9. Start Restore Process

At the **Ready to Restore** step of the wizard, check the specified settings and click **Finish**. Veeam Backup & Replication will start the restore process.



You can trace the restore process in the **Restore Session** window. If you need to cancel the machine restore, click the **Cancel** restore task link.

Restore to Amazon EC2

Veeam Backup & Replication allows you to restore physical or virtual machines to Amazon Elastic Compute Cloud (Amazon EC2) as instances.

You can use Veeam Backup & Replication to perform the following operations:

- Restore machines to Amazon EC2 from backups.
- Migrate machines from the on-premises infrastructure to the cloud.
- Create a test environment in the cloud for troubleshooting, testing patches and updates, and so on.

You can restore machines from the following types of backups:

- Backups of VMware vSphere or VMware vCloud Director VMs created with Veeam Backup & Replication.
- Backups of Microsoft Hyper-V VMs created with Veeam Backup & Replication.
- Backups of Microsoft Windows or Linux machines created with Veeam Agent for Windows or Veeam Agent for Linux. Backups must be created at the entire machine level or volume level.
- Backups of EC2 instances created with [N2WS Backup & Recovery](#).
- Backups of Nutanix AHV VMs created with [Veeam Availability for Nutanix AHV](#).

How Restore to Amazon EC2 Works

The workflow of the restore process depends on the location of machine backups:

- [Restore from repositories in Amazon S3](#)
- [Restore from backup repositories](#)

Restore from Repositories in Amazon S3

To restore a machine from backups located in [external repositories](#) or [object storage repositories](#), Veeam Backup & Replication requires a proxy appliance. A proxy appliance is an auxiliary Linux-based instance. During the restore process, Veeam Backup & Replication uses the proxy appliance to upload disks of a backed up machine to AWS.

The restore process includes the following steps:

1. Veeam Backup & Replication creates a proxy appliance in Amazon EC2.
During the restore process, the Veeam backup server communicates with the proxy appliance over the SSH protocol. A network redirector routes requests between Veeam Backup & Replication components and the proxy appliance.
2. Veeam Backup & Replication hot-adds disks of the backed up machine to the proxy appliance.
3. Veeam Backup & Replication creates a target instance in Amazon EC2.
4. Veeam Backup & Replication removes machine disks from the proxy appliance and attaches them to the target instance.
5. When the restore process is complete, Veeam Backup & Replication removes the proxy appliance from Amazon EC2.

Restore from Backup Repositories

To restore a machine from backups located in backup repositories, Veeam Backup & Replication performs the following steps:

1. Veeam Backup & Replication uploads disks of a backed-up machine to Amazon S3:
 - If you use the proxy appliance for restore, Veeam Backup & Replication hot-adds disks of a backed up machine to the appliance, takes snapshots of added disks, and transports disk data from snapshots to Amazon S3. After the data transport is complete, the proxy appliance is removed from Amazon EC2.
 - If you do not use the proxy appliance for restore, Veeam Backup & Replication uploads disks of a backed up machine directly to Amazon S3. In Amazon S3, the uploaded disks are stored in the RAW format.
2. Veeam Backup & Replication creates a target instance in Amazon EC2.
3. Veeam Backup & Replication uses AWS CLI to import disk data from Amazon S3 to the target instance.
As part of the import process, AWS installs the needed storage and network drivers and services to make the restored machine accessible in Amazon EC2.
4. [For Microsoft Windows machines] AWS installs or updates the Microsoft software licenses if you selected to obtain licenses from Amazon AWS.

AWS Account Permissions

To restore to Amazon EC2, it is recommended that the account used to connect to AWS has administrative permissions – access to all AWS actions and resources.

If you do not want to provide full access to AWS, you can grant to the account a minimal set of permissions. This set of permissions will be sufficient for restore. To grant minimal permissions, create the following policy in the JSON format and attach it to the AWS user:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "ec2:DescribeInstances",
      "ec2:RunInstances",
      "ec2:TerminateInstances",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeImages",
      "ec2:ImportImage",
      "ec2:DeregisterImage",
      "ec2:DescribeVolumes",
      "ec2:CreateVolume",
      "ec2:ModifyVolume",
      "ec2:ImportVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:DetachVolume",
      "ec2:CreateSnapshot",
      "ec2:DescribeSnapshots",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSubnets",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeKeyPairs",
      "ec2:CreateKeyPair",
      "ec2>DeleteKeyPair",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeVpcs",
      "ec2:DescribeConversionTasks",
      "ec2:DescribeImportImageTasks",
      "ec2:DescribeVolumesModifications",
      "ec2:CancelImportTask",
      "ec2:CancelConversionTask",
      "ec2:CreateTags",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeVpcAttribute",
      "iam:GetRole",
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam>DeleteRolePolicy",
      "s3:CreateBucket",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3>DeleteBucket",
      "s3:PutObject",
      "s3>DeleteObject",
      "s3:GetBucketLocation",
      "s3:PutLifecycleConfiguration",
    ]
  }]
}
```

```
        "s3:GetObject",
        "s3:RestoreObject",
        "s3:AbortMultiPartUpload",
        "s3:ListBucketMultiPartUploads",
        "s3:ListMultipartUploadParts"
    ],
    "Effect": "Allow",
    "Resource": "*"
}]
}
```

For information on how to create and attach a policy to an AWS user, see the [Creating IAM Policies](#) and [Adding and Removing IAM Identity Permissions](#) sections in the IAM User Guide.

Restoring Machines

You can restore physical or virtual machines from backups to Amazon EC2. The restored machine appears in the Amazon EC2 console, and you can use it as a regular EC2 instance.

Before you restore a machine to Amazon EC2, [check prerequisites](#). Then use the **Restore to Amazon EC2** wizard to restore the machine.

Before You Begin

Before you restore a machine to Amazon EC2, mind the following requirements and limitations:

- The Veeam backup server and repositories with machine backup files must have access to the Internet. If backup files are located on deduplicating storage appliances or shared folder repositories, the Internet connection is required for gateway servers that communicate with these repositories.
- You must have a backup of the machine that you plan to restore to Amazon EC2.
- Make sure that the account used to connect to AWS has permissions to restore to Amazon EC2. For more information, see [AWS Account Permissions](#).
- If you restore machines from backups created with Veeam Backup & Replication, check the supported OS and EC2 instance types in the [Amazon EC2 documentation](#).
- If you plan to assign AWS tags to the restored machine, check limitations for tags in the [Amazon EC2 documentation](#).

Step 1. Launch Restore to Amazon EC2 Wizard

To begin the restore process, do one of the following.

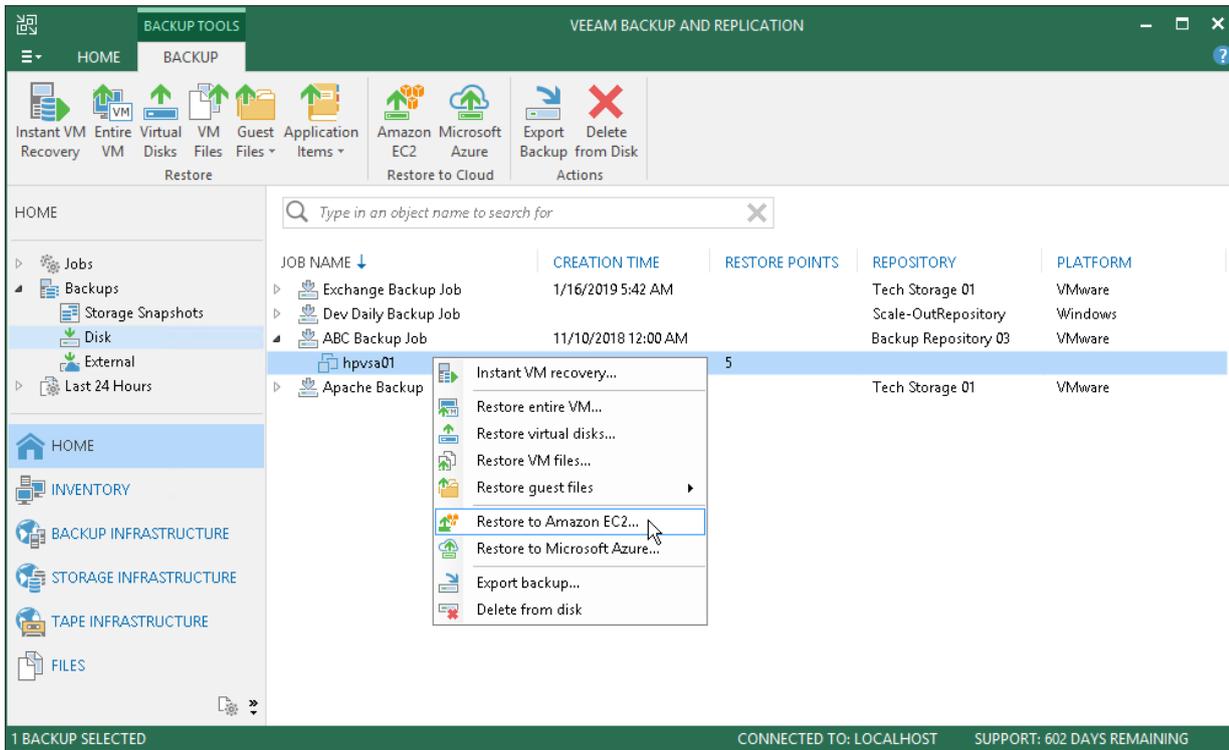
- On the **Home** tab, click **Restore** and select the type of backups from which you want to restore:
 - VMware vSphere or VMware vCloud Director
 - Microsoft Hyper-V
 - Agent
 - Amazon EC2
 - Nutanix AHV

In the displayed window, click **Entire machine restore > Restore to Amazon EC2**.

- Open the **Home** view. In the inventory pane, click **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Select the machine that you want to restore and click **Restore to Amazon EC2** on the ribbon.
 - Right-click the machine that you want to restore and select **Restore to Amazon EC2**.

In this case, you will pass to the [Account](#) step of the wizard.

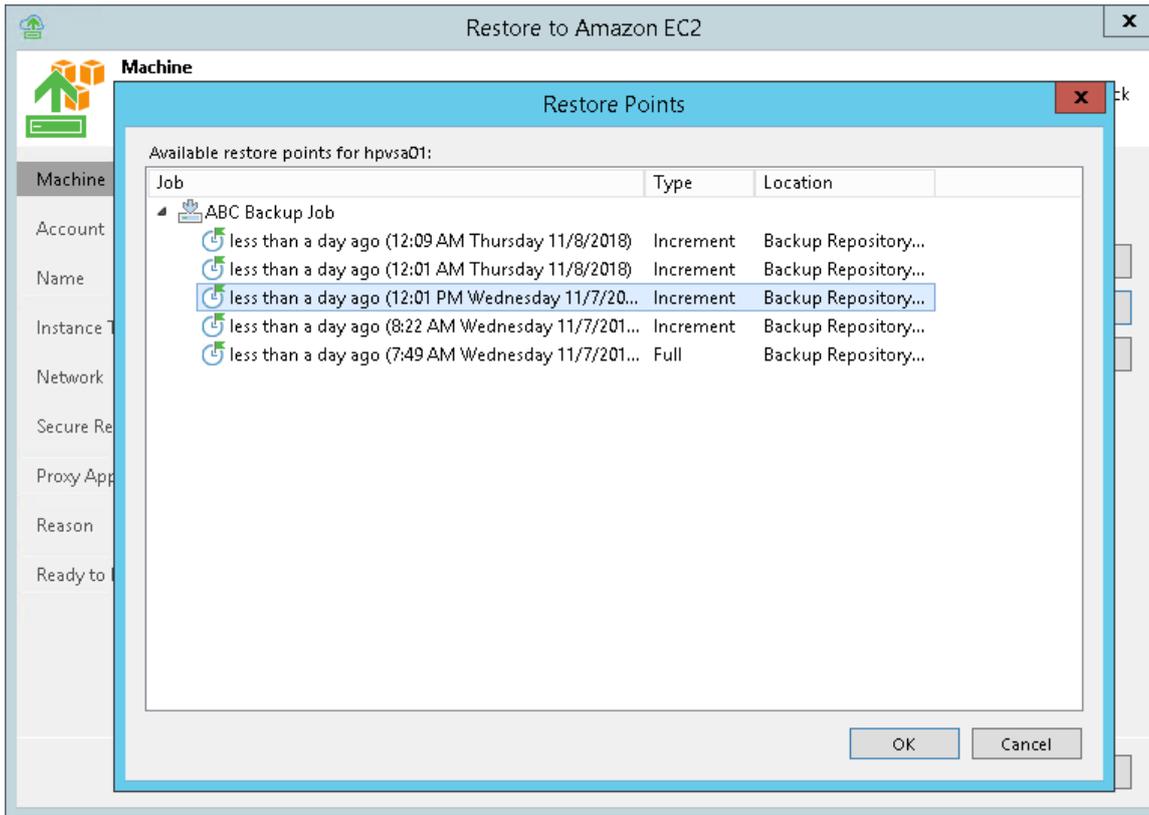
- Double-click a full backup file (VBK) or backup metadata file (VBM) in a file browser. Veeam Backup & Replication will start its console. In the **Backup Properties** window, select the necessary machine and click **Restore > Restore to Amazon EC2**. In this case, you will pass to the [Account](#) step of the wizard.



Step 2. Select Machine and Restore Point

At the **Machine** step of the wizard, specify the machine that you plan to restore and specify a restore point to which you want to restore the machine.

3. In the **Restore Points** window, select a restore point to which you want to restore the machine.



Step 3. Specify Account and Region Settings

At the **Account** step of the wizard, you can specify an AWS account and region settings.

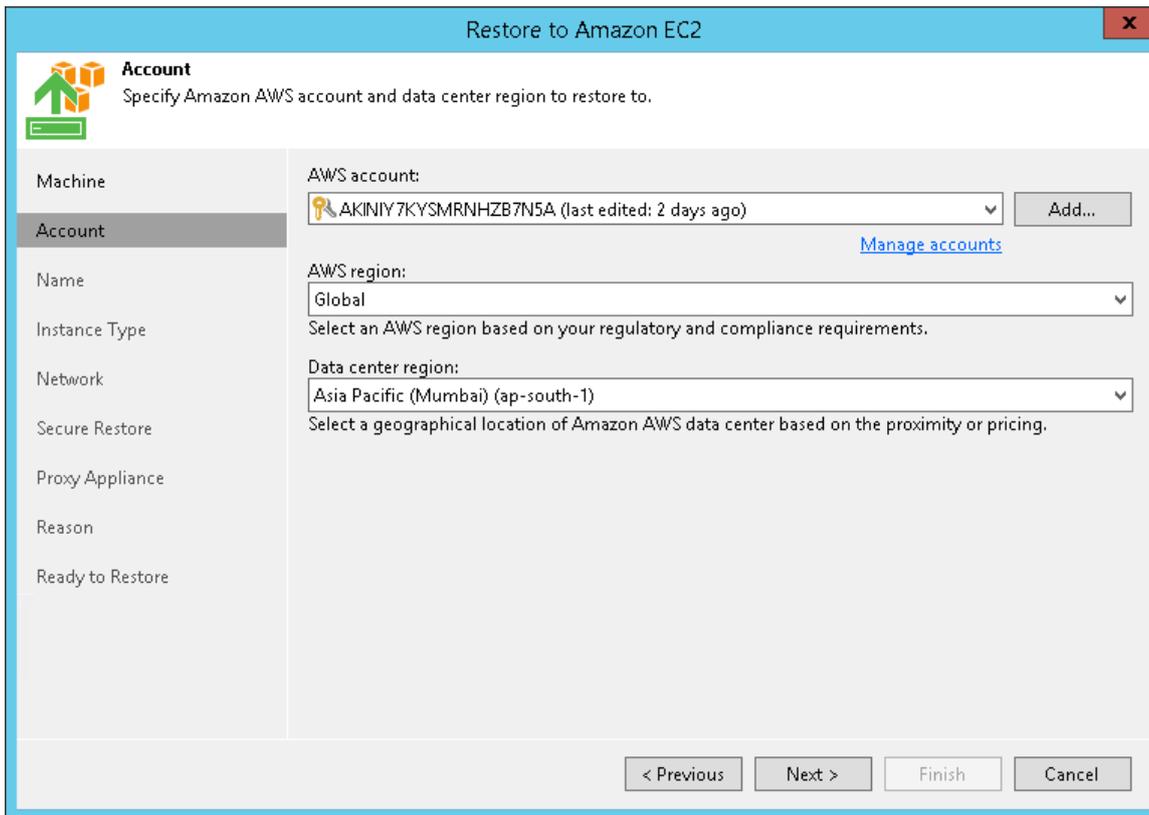
To specify an AWS account and region settings:

1. From the **AWS account** list, select the account to connect to AWS. If you have not set up the account beforehand in the [Cloud Credentials Manager](#), click the **Manage accounts** link or click **Add** on the right to add necessary account credentials.

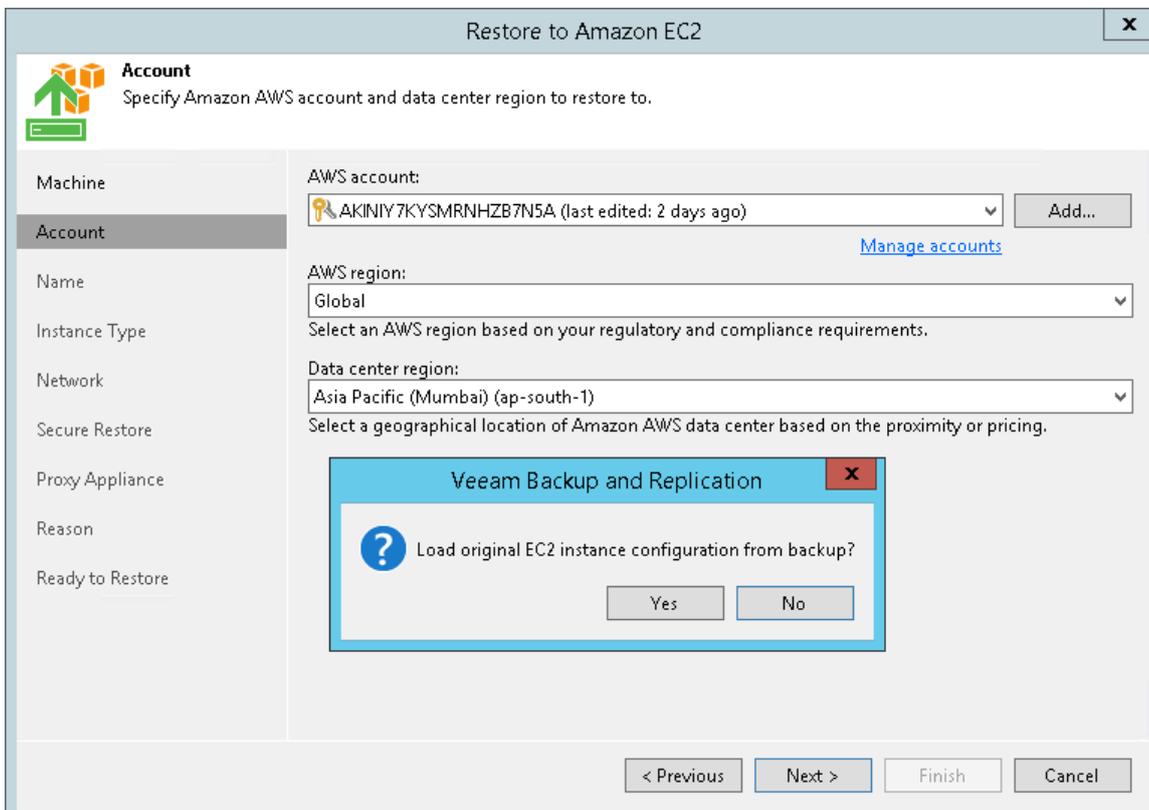
When you add an AWS account, Veeam Backup & Replication imports information about resources associated with this account. During the restore process, Veeam Backup & Replication accesses these resources and uses them to create a target instance in Amazon EC2.

2. From the **AWS region** list, select the AWS region type: *Global*, *GovCloud (US)*, or *China*.

- From the **Data center region** list, select the geographic region where Veeam Backup & Replication will create an EC2 instance for your restored machine.



If you restore an EC2 instance from backups created with N2WS Backup & Recovery to the same AWS region where the instance is placed, after you click **Next**, the wizard will offer you to use region settings associated with this instance.



Step 4. Specify Instance Name

At the **Name** step of the wizard, you can:

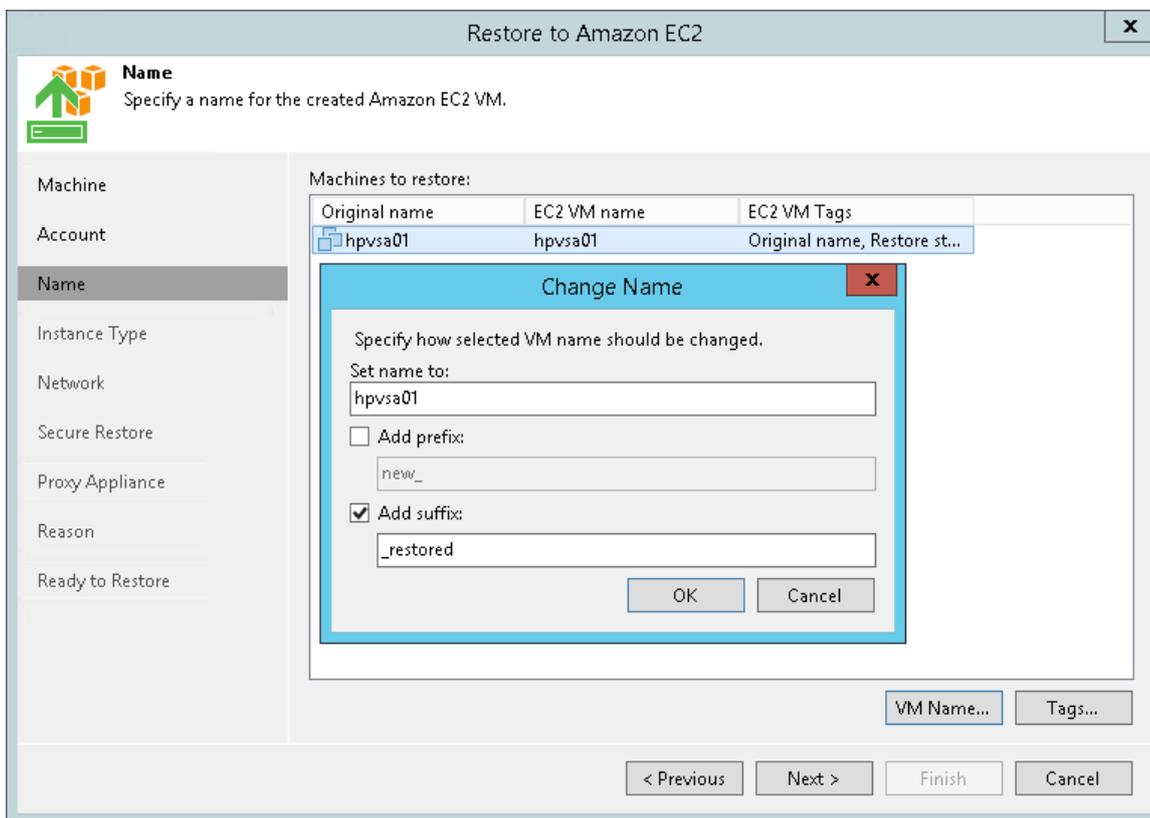
- [Specify the name for the target instance](#)
- [Manage AWS tags for the target instance](#)

Specifying Instance Name

Veeam Backup & Replication restores the machine to Amazon EC2 as an instance. An instance is a virtual machine in Amazon EC2 with a preconfigured combination of computing resources. By default, Veeam Backup & Replication uses the original machine name for the target instance. However, you can define a new name for the instance if necessary.

To define a new name for the instance:

1. In the **Machines to restore** list, select the machine and click **VM name**.
2. In the **Change Name** window, enter a new name explicitly or specify a change name rule – add a prefix and/or suffix to the original machine name.



Managing AWS Tags for Machine

You can use AWS tags to categorize instances in Amazon EC2. A tag is a label with metadata that includes two properties: a key and a value. For more information on AWS tags, see the [Amazon AWS documentation](#).

By default, Veeam Backup & Replication adds the **Original name** and **Restore start time** tags for the target instance. However, you can modify or delete these tags, or add new ones.

To add a new tag:

1. In the **Machines to restore** list, select the machine and click **Tags**.
2. In the **Tags** window, click **Add**.
3. In the **EC2 VM Tag** window, specify the **Key** and **Value** properties.

Note that you cannot add the tag with the *Name* key. Veeam Backup & Replication uses the *Name* tag to set the name for the target instance in Amazon EC2.

To modify a tag:

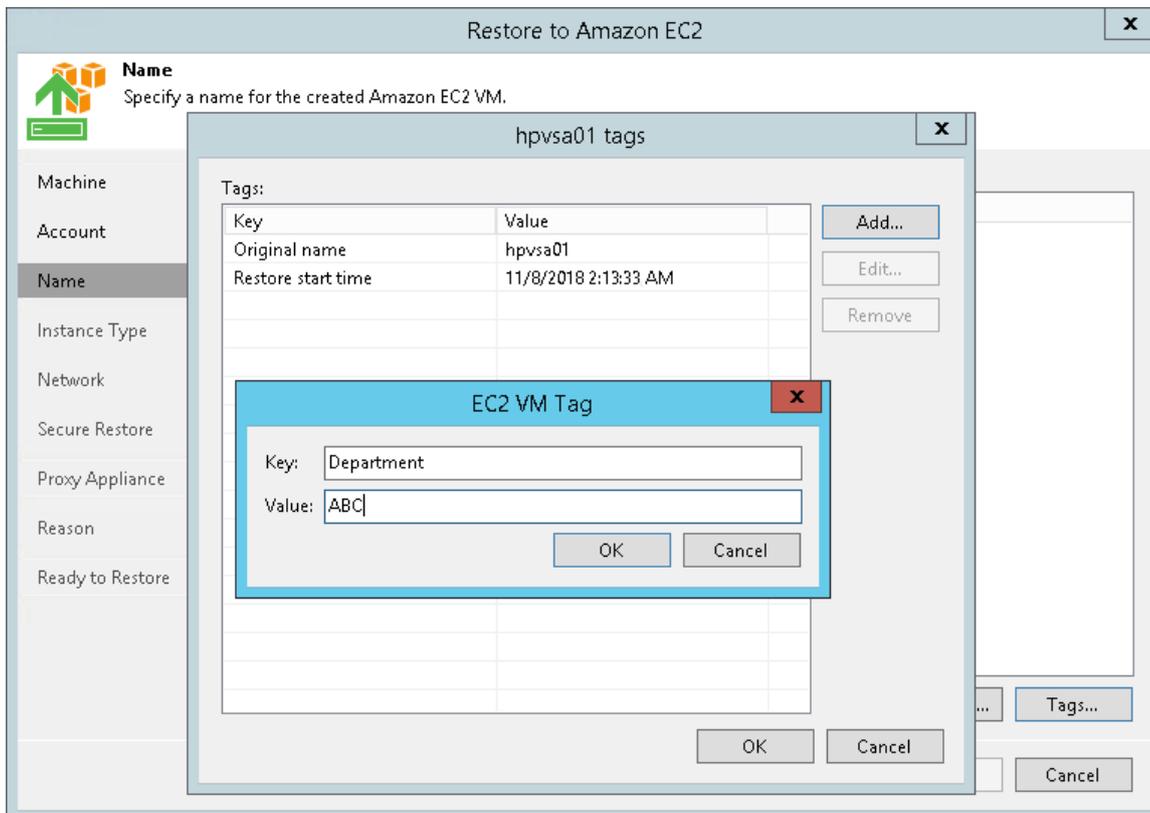
1. In the **Machines to restore** list, select the machine and click **Tags**.
2. In the **Tags** window, select the needed tag and click **Edit**.
3. In the **EC2 VM Tag** window, edit the **Key** or **Value** properties.

To delete a tag:

1. In the **Machines to restore** list, select the machine and click **Tags**.
2. In the **Tags** window, select the needed tag and click **Remove**.

NOTE:

If you restore a machine from backups of an EC2 instance, Veeam Backup & Replication displays tags that were assigned to this instance. You can modify or delete these tags as well.



Step 5. Specify Instance Type

At the **Instance Type** step of the wizard, you can:

- [Select the instance type for the restored machine](#)
- [Select disks for the restored machine](#)

Selecting Instance Type

You can select the amount of computing resources that AWS will provision for your restored machine – an EC2 instance type. Each instance type offers a unique combination of CPU, memory, storage, and networking resources.

To select an instance type for the machine:

1. In the **Virtual machines** list, select the machine and click **Edit**.
2. From the **EC2 instance type** list, select the instance type for the restored machine.

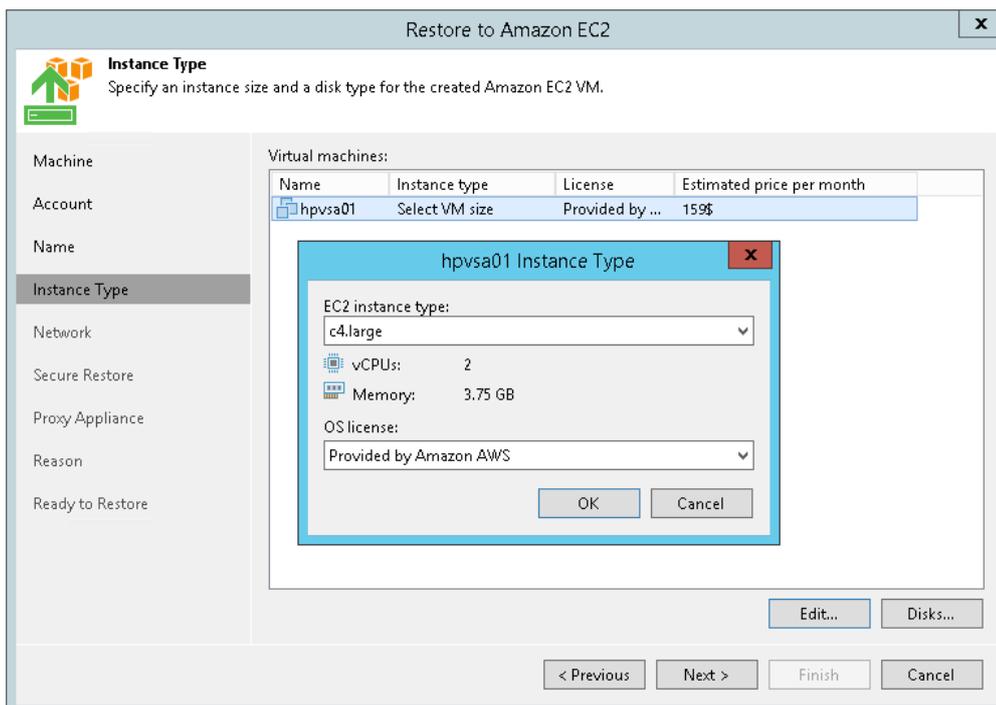
Make sure that you select the right instance type that corresponds to the initial machine configuration. For information on instance types, see the [Amazon EC2 documentation](#).

Note that if you restore an EC2 instance from backups created with N2WS Backup & Recovery, Veeam Backup & Replication will identify the type of a backed up instance and select it by default.

3. [For Microsoft Windows machines] From the **OS license** list, select the license policy that AWS will apply for Microsoft software on the target instance:
 - **Provided by Amazon AWS**. Select this option if you want to obtain licenses for Microsoft software from AWS.
 - **Bring Your Own License (BYOL)**. Select this option if you want to use your existing licenses for Microsoft software.

For more information on Microsoft software licensing in AWS, see the [Amazon AWS documentation](#).

4. Click **OK**.



Selecting Machine Disks

If necessary, you can restore only specific machine disks.

To select machine disks for restore:

1. In the **Virtual machines** list, select the machine and click **Disks**.
2. In the **Disks To Restore** window, select check boxes next to disks that you want to restore.

In Amazon EC2, Veeam Backup & Replication saves disks of the restored machine as Amazon Elastic Block Store (EBS) volumes. By default, Veeam Backup & Replication creates EBS volumes of the General Purpose SSD type. For information on types of EBS volumes, see [Amazon EC2 documentation](#).

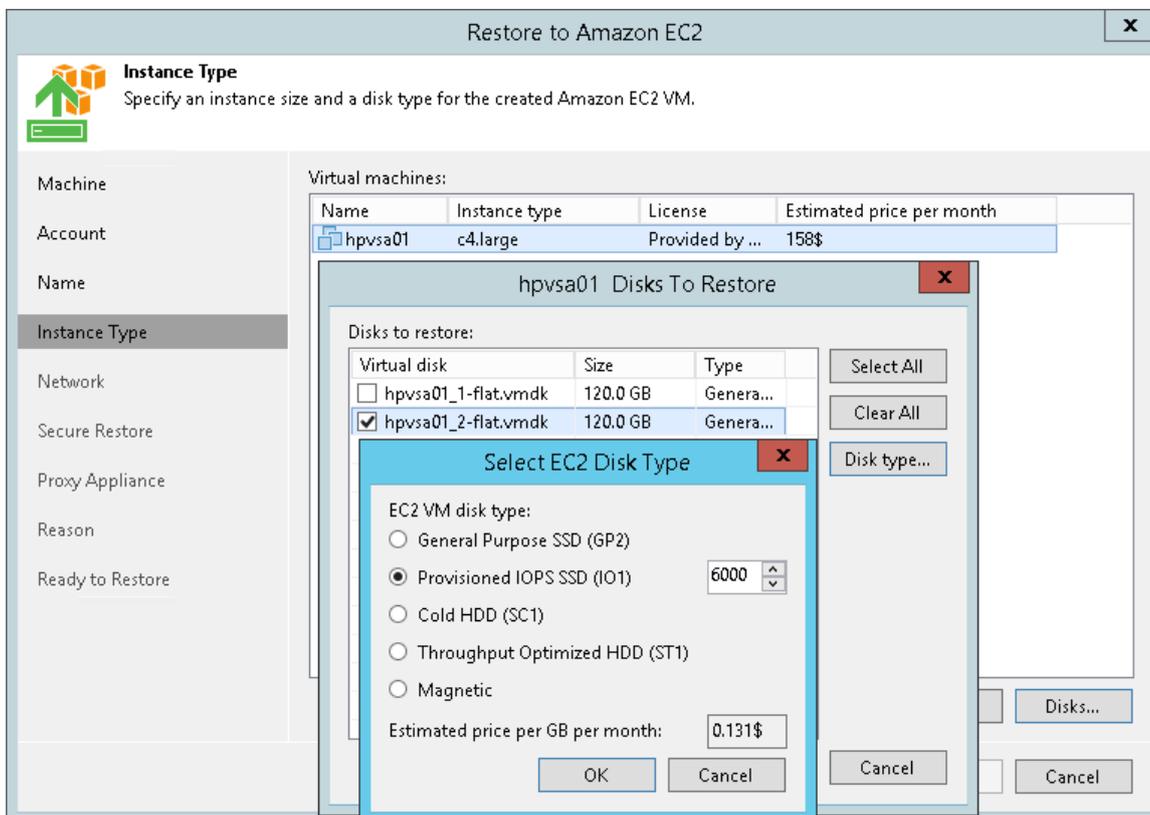
If necessary, you can change the EBS volume type. To do that, perform the following steps:

1. In the **Virtual machines** list, select the machine and click **Disks**.
2. In the **Disks To Restore** window, select the machine disk and click **Disk type**.
3. In the **Select EC2 Disk Type** window, choose the volume type.

If you selected the **Provisioned IOPS SSD (IO1)** type, you can also specify the maximum number of input/output operations per second (IOPS) for the volume. For more information on IOPS, see [Amazon EC2 documentation](#).

TIP:

For your convenience, Veeam Backup & Replication uses the AWS Simple Monthly Calculator tools to estimate an approximate price per month for using a selected instance. The estimated price is calculated based on the instance type, license policy and disk configuration.

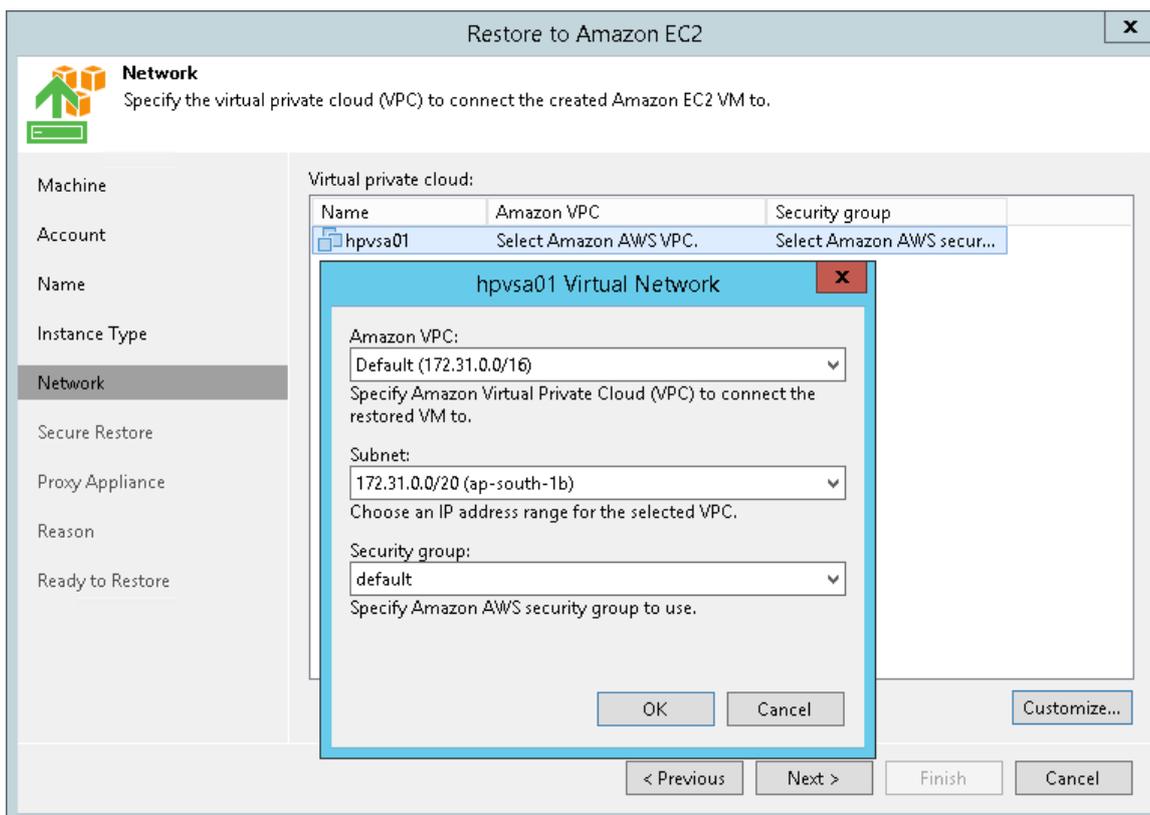


Step 6. Select Amazon VPC

At the **Network** step of the wizard, you can select to which Amazon Virtual Private Cloud (Amazon VPC) the target EC2 instance must be connected. You can also specify a subnet, and a security group – a virtual firewall for the target instance. For more information on Amazon VPC, see the [Amazon AWS documentation](#).

To define network settings for the target instance, do the following:

1. In the **Amazon VPC** list, select the Amazon VPC where the target instance will be launched.
2. From the **Subnet** list, select the subnet for the target instance.
3. From the **Security group** list, select a security group that will be associated with your target instance.
4. Click **OK**.



Step 7. Specify Secure Restore Settings

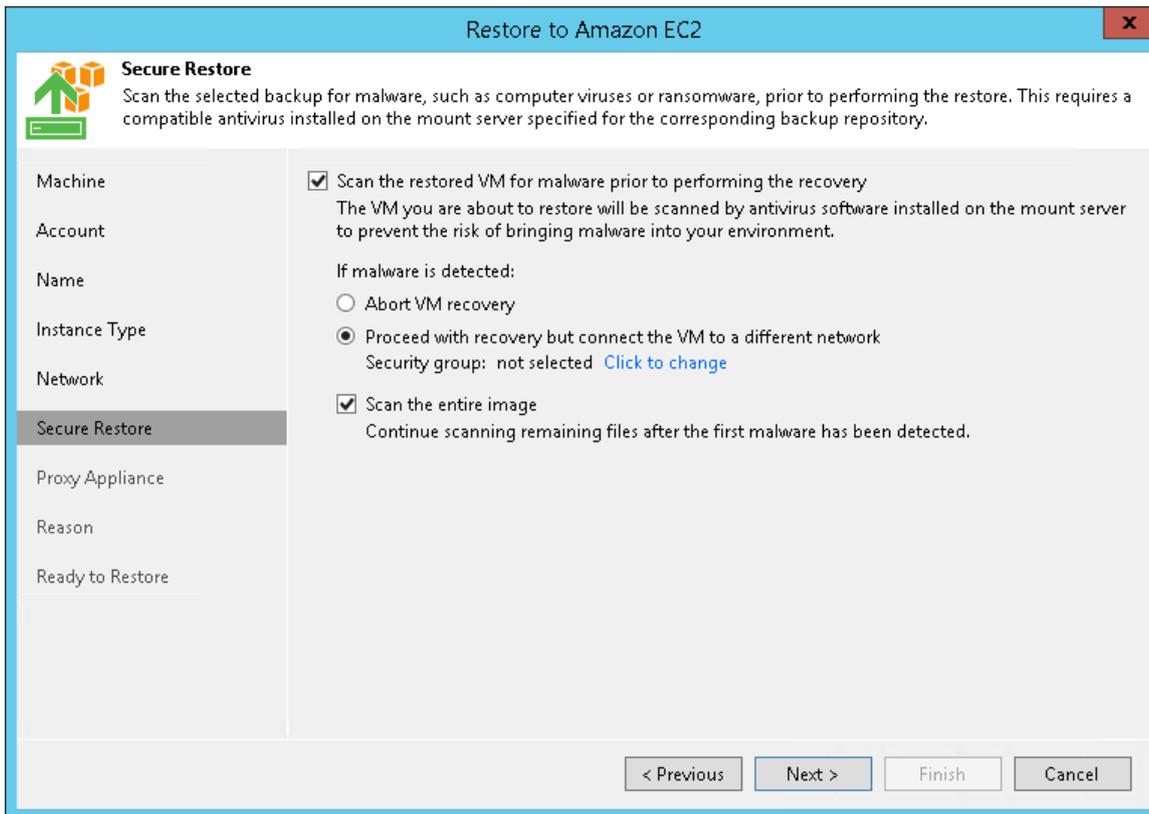
You can instruct Veeam Backup & Replication to perform secure restore – scan machine data with antivirus software before restoring the machine to Amazon EC2. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

1. At the **Secure Restore** step of the wizard, select the **Scan the restored VM for malware prior to performing the recovery** check box.
2. Select which action Veeam Backup & Replication will take if the antivirus finds a virus threat:
 - **Abort VM recovery.** Select this action if you want to cancel the restore session.
 - **Proceed with recovery but connect the VM to a different network.** Select this action if you want to restore the machine to a different AWS security group.

Click the **Click to change** link to select the security group.

3. Select the **Scan the entire image** check box if you want the antivirus to continue machine scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).



Step 8. Specify Proxy Appliance

At the **Proxy Appliance** step of the wizard, you can specify the proxy appliance settings. A proxy appliance is an auxiliary Linux-based instance. During the restore process, Veeam Backup & Replication uses the proxy appliance to upload disks of a backed up machine to AWS.

The proxy appliance is non-persistent. Veeam Backup & Replication automatically deploys the appliance in AWS only for the duration of the restore process and removes it immediately after that.

NOTE:

The proxy appliance is required if you restore machines from backups located in [external repositories](#) or [object storage repositories](#), and is recommended to use if you restore machines from backup repositories.

To specify proxy appliance settings, do the following:

1. Select the **Use the proxy appliance** check box.
2. Click **Customize**.
3. From the **EC2 instance type** list, select the instance type for the proxy appliance.

IMPORTANT!

To upload one machine disk to AWS, the proxy appliance requires 1 GB RAM.

Make sure that the selected instance type offers enough memory resources to upload all machine disks. Otherwise, the restore process may fail.

4. From the **Subnet** list, select the subnet for the proxy appliance.
5. From the **Security group** list, select a security group that will be associated with the proxy appliance.
6. In the **Redirector port** field, specify the port for routing requests between Veeam Backup & Replication components and the proxy appliance.
7. Click **OK**.

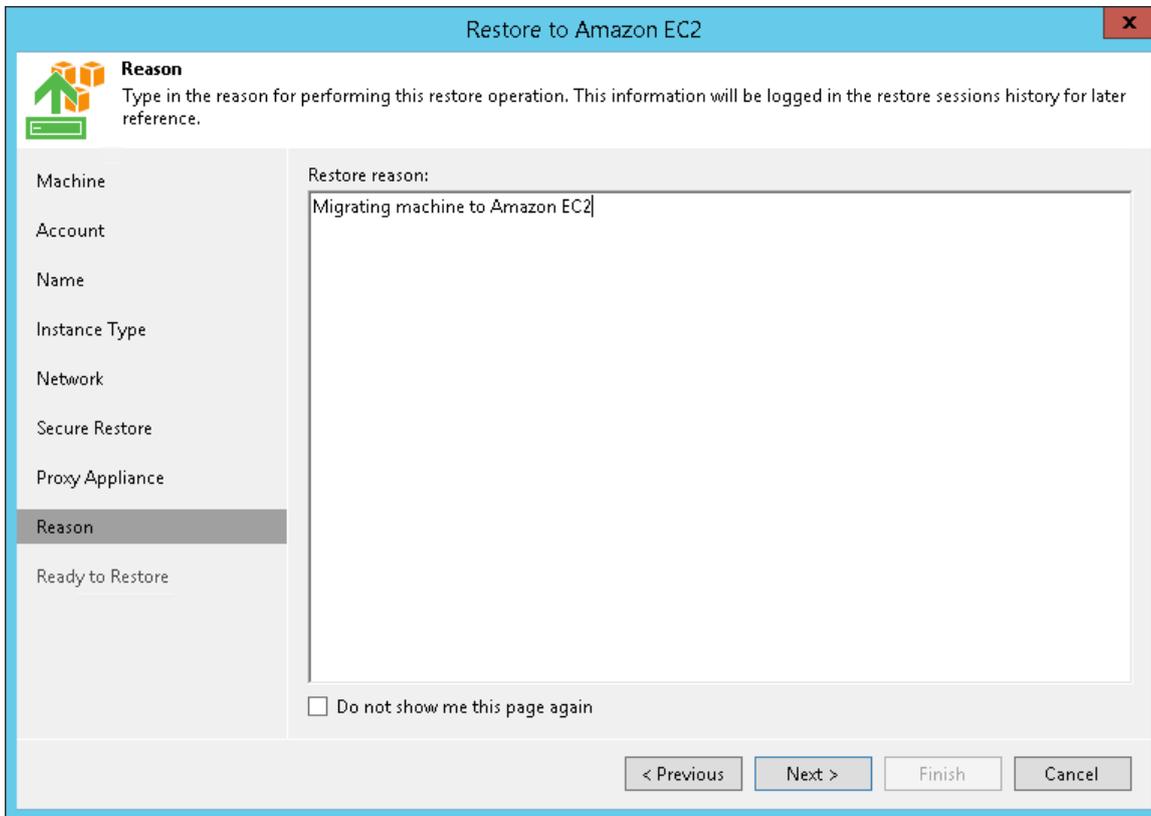
The screenshot shows the 'Restore to Amazon EC2' wizard at the 'Proxy Appliance' step. The main window has a sidebar with options: Machine, Account, Name, Instance Type, Network, Secure Restore, Proxy Appliance (selected), Reason, and Ready to Restore. The main area contains text explaining the proxy appliance and a 'Proxy Appliance Settings' dialog box. The dialog box has the following fields: EC2 instance type (c4.large), vCPUs (2), Memory (3.75 GB), Subnet (172.31.0.0/20 (ap-south-1b)), Security group (default), and Redirector port (443). There are 'OK' and 'Cancel' buttons at the bottom of the dialog. Below the dialog, there is a checkbox 'Use the proxy appliance (recommended)' which is checked, and a 'Customize...' button. At the bottom of the main window, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 9. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the machine. The information you provide will be saved in the session history in Veeam Backup & Replication, and you can view it later.

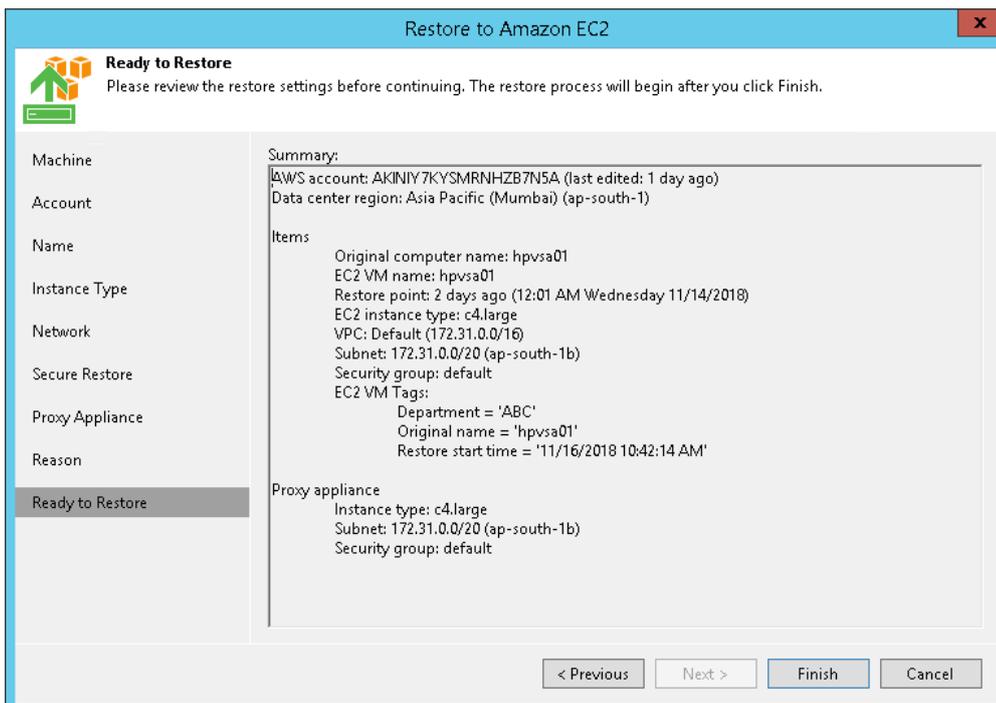
TIP:

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.



Step 10. Start Restore Process

At the **Ready to Restore** step of the wizard, check the specified settings and click **Finish**. Veeam Backup & Replication will start the restore process.



You can trace the restore process in the **Restore Session** window. If you need to cancel the machine restore, click the **Cancel** restore task link.

Secure Restore

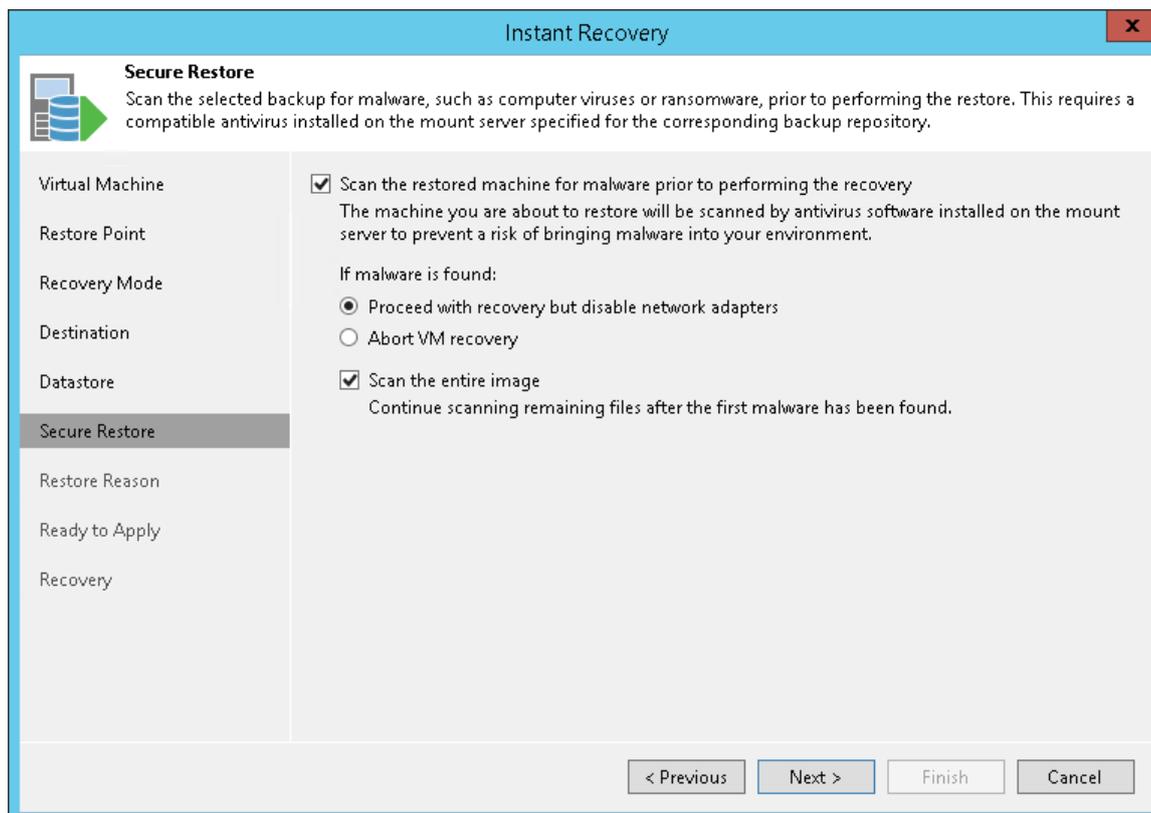
Veeam Backup & Replication allows you to perform secure restore – scan machine data with antivirus software before restoring the machine to the production environment.

During secure restore, Veeam Backup & Replication mounts disks of the machine that you plan to restore to the mount server. On the mount server, Veeam Backup & Replication triggers an antivirus to scan files from the mounted disks. If during the scan the antivirus detects malware, Veeam Backup & Replication will either abort the restore process, or restore the machine or its disks with restrictions depending on secure restore settings.

Secure restore is available for the following restore operations:

- Instant VM Recovery
- Entire VM Restore
- Virtual Disks Restore
- Restore to Microsoft Azure
- Restore to Amazon EC2
- EC2 Instance Disks Export

To perform secure restore, you must enable the **Scan the restored machine for malware prior to performing the recovery** option at the **Secure Restore** step of the restore wizard.



TIP:

You can also scan machine data for malware regularly within a SureBackup job. For information on how to enable the malware scan for a SureBackup job, see the [Settings step](#) of the SureBackup job wizard.

Requirements and Limitations for Secure Restore

Before you perform secure restore, check the following prerequisites:

- You can perform secure restore only for machines that run Microsoft Windows.
- The antivirus software must be installed on the mount server and support the command line interface (CLI).
- The antivirus configuration file must be located on the mount server and must be properly configured. For details, see [Antivirus XML Configuration File](#).
- Veeam Backup & Replication does not perform malware scan for disks or volumes that cannot be mounted to the mount server.

For example, Storage Spaces disks or ReFS volumes (if ReFS is not supported by the mount server OS) are skipped from the scan and restored in a regular way.

How Secure Restore Works

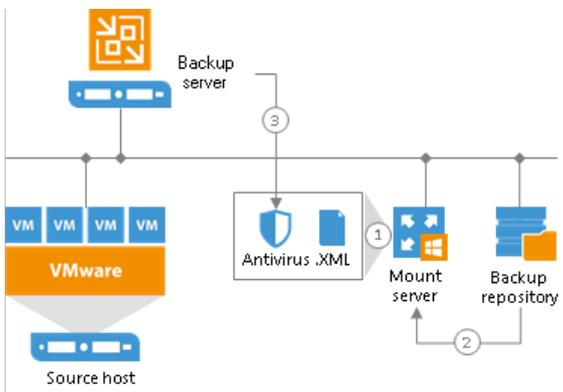
Veeam Backup & Replication uses the mount server as a staging server for scanning machine data with antivirus software. By default, the mount server role is assigned to one of the following machines: the Veeam backup server or a repository that stores machine backups. However, you can assign the mount server role to any 64-bit Microsoft Windows machine in your backup infrastructure. For example, you may want to run the malware scan process on a different server for security reasons. For details on mount server deployment and requirements, see [Mount Server](#).

To run the malware scan, Veeam Backup & Replication performs the following actions:

1. On the mount server, Veeam Backup & Replication runs Veeam Mount Service to check the [antivirus configuration file](#) and antivirus software:
 - a. Veeam Mount Service verifies if the `AntivirusInfos.xml` configuration file is located in the `%ProgramFiles%\Common Files\Veeam\Backup and Replication\Mount Service` folder.
 - b. Veeam Mount Service checks the scan settings in the configuration file and verifies if the antivirus is installed on the mount server.

Note that if the antivirus is not installed or the configuration file is improperly configured, Veeam Backup & Replication will not start the restore process. In the restore wizard, you will not be able to pass the step with secure restore settings.

2. Veeam Backup & Replication mounts machine disks from backups to the mount server under the `C:\VeeamFLR\<machinename>` folder.
3. Veeam Backup & Replication triggers the antivirus to scan files in the `C:\VeeamFLR\<machinename>` folder.



If during the scan the antivirus does not detect malware, Veeam Backup & Replication restores the machine or its disks to the target location.

If the antivirus detects malware, Veeam Backup & Replication will either abort the restore process, or restore the machine or its disks with restrictions depending on the following secure restore settings:

- Disable the network adapter (NIC) on the restored machine.
- Connect the restored machine to a different Microsoft Azure virtual network.
- Change the AWS security group for the restored machine.
- Disconnect restored virtual disks from the target VM.

You can further access the restored machine or its disks in the isolated environment and clean the infection.

Antivirus XML Configuration File

The antivirus software that you plan to use for scanning backups is described in the `AntivirusInfos.xml` file. Veeam Backup & Replication creates this configuration file on every machine with the mount server role and stores the file in the `%ProgramFiles%\Common Files\Veeam\Backup and Replication\Mount Service` folder.

During secure restore, Veeam Backup & Replication reads settings from the configuration file and triggers the antivirus to scan backup files. The settings in the file are already predefined for the following antivirus software vendors:

- [Symantec](#)
- [ESET](#)
- [Windows Defender](#)

If you want to scan machine data with antivirus software of other vendors, you must add settings for this software to the antivirus configuration file. Mind that the antivirus software must support the command line interface (CLI).

NOTE:

If you made changes to the antivirus configuration file, you do not need to restart Veeam services on the backup server – Veeam Backup & Replication will perform the next malware scan with new settings.

XML File Structure

The XML file describing antivirus settings has the following structure:

```
<Antiviruses>
  <AntivirusInfo Name='Symantec' IsPortableSoftware='false'
ExecutableFilePath='Veeam.Backup.Antivirus.Scan.exe' CommandLineParameters='/p:%Path%'
RegPath='HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\symcscan' ServiceName='symcscan'
ThreatExistsRegEx='Threat\s+found' IsParallelScanAvailable='false'>
  <ExitCodes>
    <ExitCode Type='Success' Description='No threats detected'>0</ExitCode>
    <ExitCode Type='Error' Description='Invalid command line argument'>1</ExitCode>
    <ExitCode Type='Error' Description='Antivirus scan was completed with
errors'>2</ExitCode>
    <ExitCode Type='Error' Description='Antivirus scan was canceled'>4</ExitCode>
    <ExitCode Type='Infected' Description='Virus threat was detected'>3</ExitCode>
  </ExitCodes>
</AntivirusInfo>
  <AntivirusInfo Name='Eset File Security' IsPortableSoftware='true'
ExecutableFilePath='%ProgramFiles%\ESET\ESET File Security\ecsl.exe'
CommandLineParameters='%Path% /clean-mode=None /no-symlink' RegPath='' ServiceName=''
ThreatExistsRegEx='threat\s*=\s*["&apos;](?!is OK["&apos;])[^"&apos;]+["&apos;]'
IsParallelScanAvailable='false'>
  <ExitCode Type='Success' Description='No threats detected'>0</ExitCode>
  <ExitCode Type='Infected' Description='Virus threat was detected'>1</ExitCode>
  <ExitCode Type='Warning' Description='Some files were not scanned'>10</ExitCode>
  <ExitCode Type='Infected' Description='Virus threat was detected'>50</ExitCode>
  <ExitCode Type='Error' Description='Antivirus scan was completed with
errors'>100</ExitCode>
  </ExitCodes>
</AntivirusInfo>
  <AntivirusInfo Name='ESET Antivirus' IsPortableSoftware='true'
ExecutableFilePath='%ProgramFiles%\ESET\ESET Security\ecsl.exe' CommandLineParameters='%Path%
/clean-mode=None /no-symlink' RegPath='' ServiceName=''
ThreatExistsRegEx='threat\s*=\s*["&apos;](?!is OK["&apos;])[^"&apos;]+["&apos;]'
IsParallelScanAvailable='false'>
  <ExitCodes>
    <ExitCode Type='Success' Description='No threats detected'>0</ExitCode>
    <ExitCode Type='Infected' Description='Virus threat was detected'>1</ExitCode>
    <ExitCode Type='Warning' Description='Some files were not scanned'>10</ExitCode>
    <ExitCode Type='Infected' Description='Virus threat was detected'>50</ExitCode>
    <ExitCode Type='Error' Description='Antivirus scan was completed with
errors'>100</ExitCode>
  </ExitCodes>
</AntivirusInfo>
  <AntivirusInfo Name='Windows Defender' IsPortableSoftware='false'
ExecutableFilePath='%ProgramFiles%\Windows Defender\mpcmdrun.exe' CommandLineParameters='-Scan -
ScanType 3 -File %Path% -DisableRemediation -BootSectorScan'
RegPath='HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDefend' ServiceName='WinDefend'
ThreatExistsRegEx='Threat\s+information' IsParallelScanAvailable='false'>
  <ExitCodes>
    <ExitCode Type='Success' Description='No threats detected'>0</ExitCode>
    <ExitCode Type='Error' Description='Antivirus scan was completed with
errors'>2</ExitCode>
    <ExitCode Type='Infected' Description='Virus threat was detected'>2</ExitCode>
  </ExitCodes>
</AntivirusInfo>
</Antiviruses>
```

The XML file contains the following elements:

- **Antiviruses**. The element encapsulates the file with antivirus settings.
- **AntivirusInfo**. The element describes the antivirus software.
- **ExitCodes**. The element encapsulates messages that Veeam Backup & Replication displays on scan results.
- **ExitCode**. The element describes the subject and the body of the message that Veeam Backup & Replication displays on scan results.

AntivirusInfo

The element has the following attributes:

Attribute	Description
Name	Specifies the antivirus name. Veeam Backup & Replication will display this name in restore session logs.
IsPortableSoftware	Indicates if antivirus software is portable: <ul style="list-style-type: none">• If you set this attribute to <code>True</code>, Veeam Backup & Replication will treat the antivirus software as portable. Before performing secure restore, Veeam Backup & Replication will verify if the antivirus executable file exists. The path to the file is specified by the ExecutableFilePath attribute.• If you set this attribute to <code>False</code>, Veeam Backup & Replication will treat the antivirus software as non-portable. Before performing secure restore, Veeam Backup & Replication will verify if the antivirus registry key exists and if the antivirus service is running. The key is specified by the RegPath attribute. The service name is specified by the ServiceName attribute.
ExecutableFilePath	Specifies the path to the antivirus executable file.
CommandLineParameters	Specifies antivirus commands that you want to execute during the scan. Make sure that the antivirus supports the specified commands. For example, the list of commands for ESET is available in this ESET KB article . Note: The <code>%Path%</code> variable is required for this attribute. During secure restore, Veeam Backup & Replication substitutes this variable for the path to the folder with mounted disks (<code>C:\VeeamFLR\<machinename></code>).
RegPath	Specifies the antivirus registry key.
ServiceName	Specifies the name of the antivirus service.
ThreatExistsRegEx	Specifies regular expressions. A regular expression is a sequence of characters that form a search pattern. Veeam Backup & Replication will search the antivirus output messages for the specified regular expression. If any of the output messages match the expression, Veeam Backup & Replication will notify you on detected threat. Note: You must have a good understanding of the regular expression language to specify this attribute properly. For more information on the regular expression language, see Microsoft Docs .

IsParallelScanAvailable	<p>Indicates if the antivirus will run multiple jobs to scan files on mounted disks simultaneously.</p> <p>If you set this attribute to <code>True</code>, Veeam Backup & Replication will lock the antivirus to perform the scan for the current restore session. The antivirus will not be available for other sessions with enabled secure restore until the scan completes.</p> <p>The default value for antivirus lock time-out is 24 hours. If the scan does not complete after this period, Veeam Backup & Replication will finish other restore sessions as specified in the restore wizard: abort restore sessions or restore machines (or its disks) with restrictions.</p> <p>Note: You can change the lock time-out using registry keys. For more information, contact Veeam Support.</p> <p>If the antivirus CLI does not support multiple scan jobs, set this attribute to <code>False</code>.</p>
--------------------------------	---

ExitCode

The element has the following attributes:

Attribute	Description
Type	<p>Specifies the subject of the message that Veeam Backup & Replication will display on scan results:</p> <ul style="list-style-type: none"> • Success • Infected • Warning • Error
Description	<p>Specifies the body of the message that Veeam Backup & Replication will display on scan results.</p>

TIP:

You can distribute the XML configuration file among other mount servers in your backup infrastructure using Veeam PowerShell. For more information, see the [Copy-VBRAntivirusConfigurationFile](#) section in the Veeam PowerShell Reference.

Related Topics

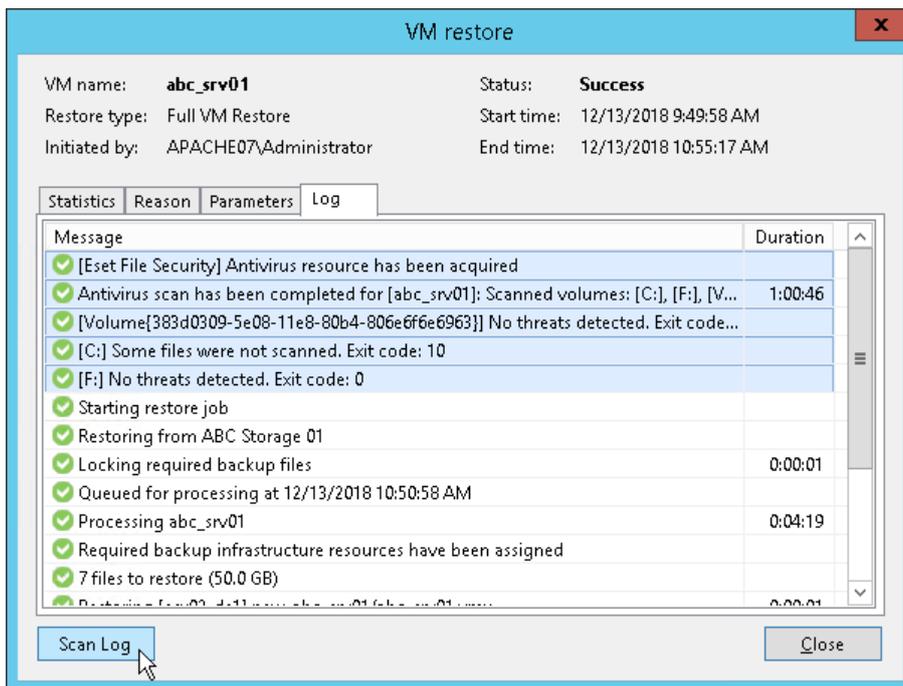
[How Secure Restore Works](#)

Viewing Malware Scan Results

Results of the malware scan are available in restore session statistics.

To view restore session statistics, do one of the following:

- Open the **Home** view, in the inventory pane select **Last 24 hours**. In the working area, double-click the necessary restore session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.
- Open the **History** view, in the inventory pane select **Restore**. In the working area, double-click the necessary restore session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.



To view the detailed logging of the malware scan, click the **Scan Log** button at the bottom of the window with restore session statistics. Veeam Backup & Replication will display the most recent logs in a file of 1 MB in size.

Full logs of the scan are stored on the mount server in the following folder:

C:\ProgramData\Veeam\Backup\FLRSessions\Windows\FLR__<machinename>_\Antivirus.

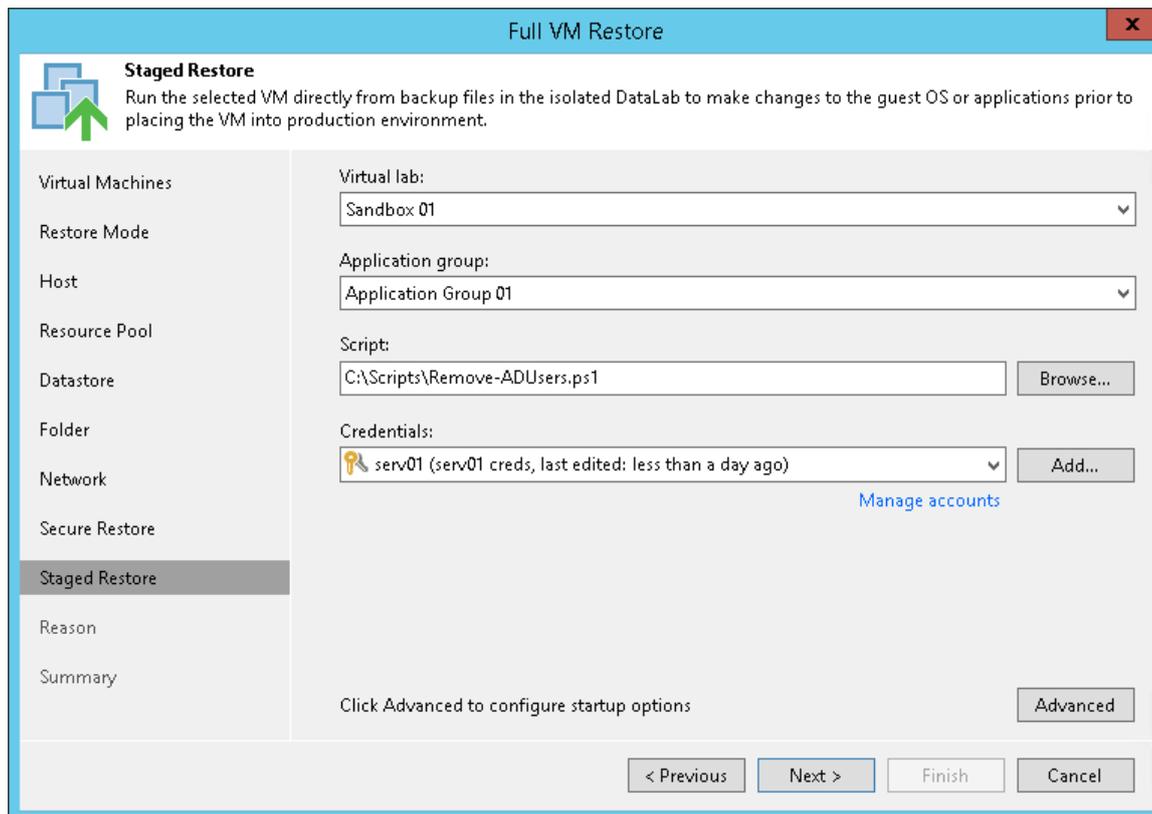
Staged Restore

Veeam Backup & Replication allows you to perform staged restore – run an executable script for VMs before recovering them to the production environment.

Staged restore can help you ensure that recovered VMs do not contain any personal or sensitive data. For example, you can instruct Veeam Backup & Replication to run a [Windows PowerShell script](#) that removes Active Directory users:

```
$UserName = "John.Smith"
$ADUser = Get-ADUser -Filter 'Name -like $UserName'
if (!$ADUser)
{
    [Environment]::Exit(1)
}
Remove-ADUser -Identity $UserName -Confirm:$false
```

Stage restore is available only for entire VM restore operations. To perform staged restore, you must select the **Staged Restore** mode in the **Full VM Restore** wizard and specify staged restore settings.



The screenshot shows the 'Full VM Restore' wizard window. The 'Staged Restore' tab is selected in the left-hand navigation pane. The main area contains the following configuration options:

- Virtual lab:** A dropdown menu set to 'Sandbox 01'.
- Application group:** A dropdown menu set to 'Application Group 01'.
- Script:** A text box containing 'C:\Scripts\Remove-ADUsers.ps1' with a 'Browse...' button to its right.
- Credentials:** A dropdown menu showing 'serv01 (serv01 creds, last edited: less than a day ago)' with an 'Add...' button to its right. A 'Manage accounts' link is located below the dropdown.
- Advanced:** A button labeled 'Advanced' with the text 'Click Advanced to configure startup options' above it.

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

Requirements and Limitations for Staged Restore

Before you perform staged restore, check the following prerequisites:

- The staged restore functionality is available in Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
- You must have a preconfigured virtual lab in your backup infrastructure. For more information, see [Virtual Lab](#).

- Scripts that you plan to run must reside in a local folder on a backup server.
- If you plan to perform staged restore for several VMs within one restore session, make sure these VMs run OS of the same type: either Microsoft Windows or Linux. In the current version of Veeam Backup & Replication, you cannot specify credentials and scripts for each VM individually.

How Staged Restore Works

For staged restore, Veeam Backup & Replication uses a preconfigured virtual lab, an executable script located on the backup server, and credentials to connect to VMs and run the script. Veeam Backup & Replication performs staged restore in the following way:

1. In the virtual lab, Veeam Backup & Replication starts VMs directly from compressed and deduplicated backup files that reside on the backup repository. To achieve this, Veeam Backup & Replication uses the [Veeam vPower NFS Service](#).

If you selected to use an application group to run a script, Veeam Backup & Replication first starts VMs from the application group in the required order.

2. Veeam Backup & Replication copies the script from the backup server to VMs that you plan to restore. To connect to VMs, Veeam Backup & Replication uses credentials specified in staged restore settings.
3. Veeam Backup & Replication runs the copied script on every VM.

To run the script, Veeam Backup & Replication uses the same technology as for pre-freeze and post-thaw scripts. For more information, see [Pre-Freeze and Post-Thaw Scripts](#).

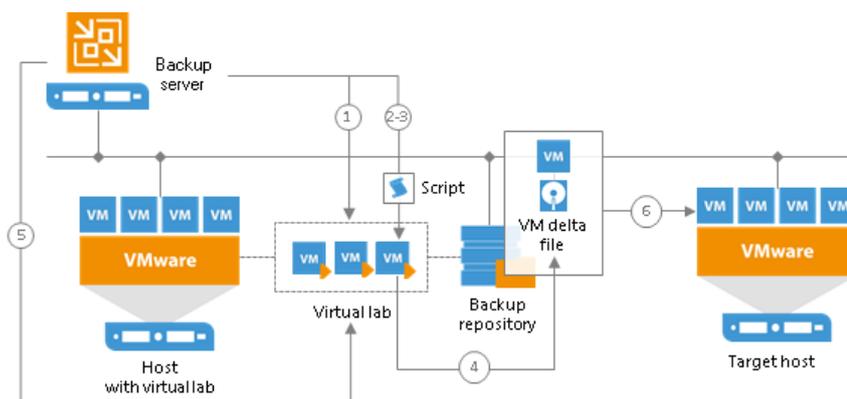
4. All VM changes that take place during script execution are written to VM delta files.

By default, Veeam Backup & Replication stores delta files on the [vPower NFS server](#). You can change the destination for VM delta files in virtual lab settings.

5. After the script execution is complete, Veeam Backup & Replication powers off VMs in the virtual lab.

6. Veeam Backup & Replication restores VMs in a changed state to the production environment.

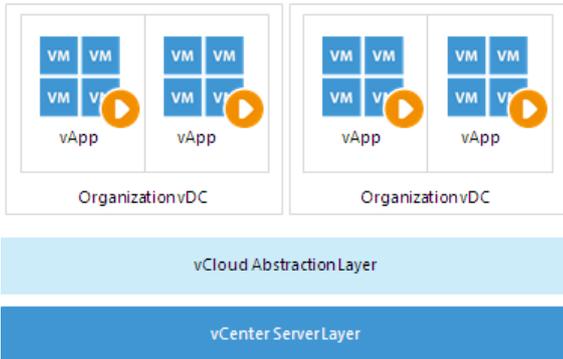
To achieve that, Veeam Backup & Replication copies VM data from the backup repository and delta files to the target host using [Quick Migration](#).



vCloud Director Support

Veeam Backup & Replication provides support for vCloud Director. It uses vCloud Director API to help you back up vApps and VMs and restore them directly to the vCloud Director hierarchy.

The main entity with which Veeam Backup & Replication works during backup is a vApp. A vApp is a virtual system that contains one or more individual VMs along with parameters that define operational details – vApp metadata. When Veeam Backup & Replication performs backup of 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 objects back to the vCloud Director hierarchy and do not need to perform any additional actions on import and VM configuration.



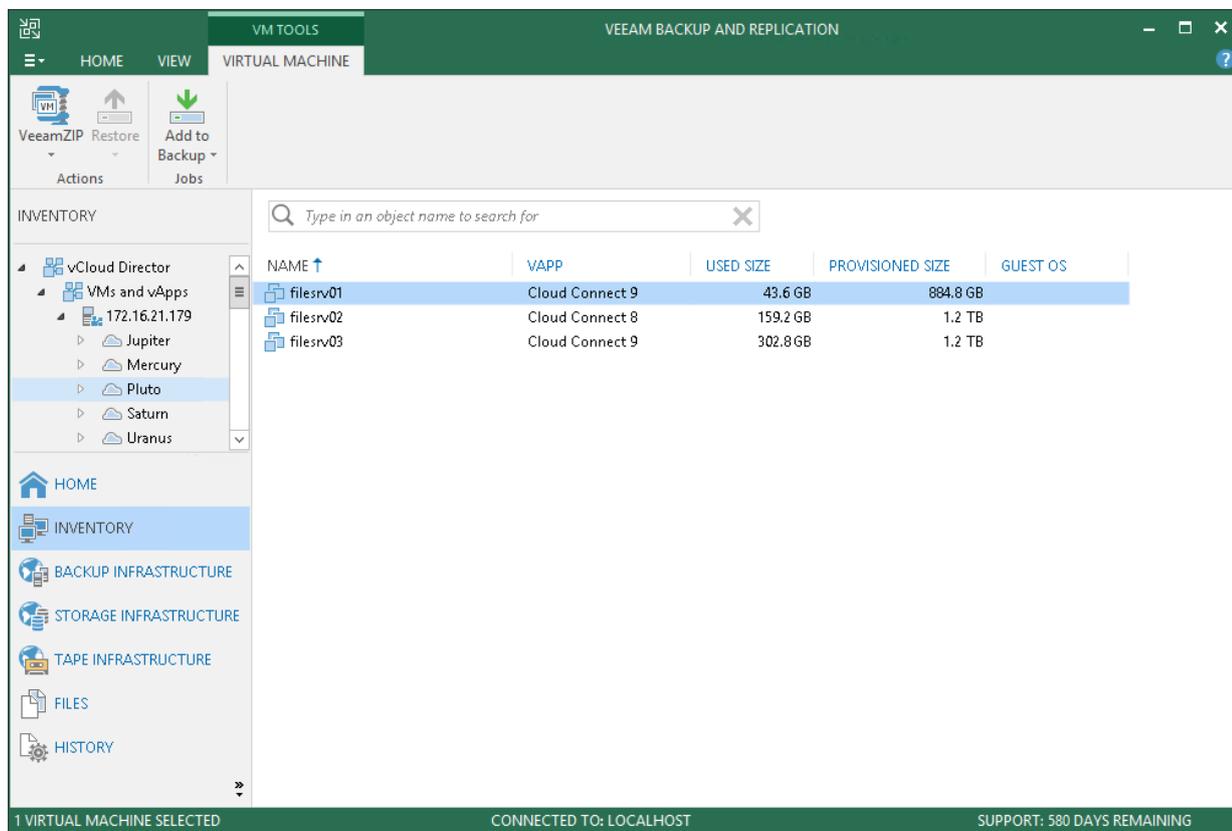
Viewing VMware vCloud Director VMs

After you add the VMware vCloud Director server to the backup infrastructure, you can view the VMware vCloud Director hierarchy in Veeam Backup & Replication and work with VMs managed with VMware vCloud Director.

To open the VMware vCloud Director hierarchy:

1. Open the **Inventory** view.
2. Click the **View** tab on the ribbon.
3. On the **View** tab, click **vCloud View**.

The hierarchy of the VMware vCloud Director server will become available in the inventory pane. VMs managed by VMware vCloud Director will be displayed in the working area. You can work with these VMs just as if you work with VMs managed by vCenter Servers or registered on ESX(i) hosts added to the backup infrastructure.



Backup and Restore of vApps

Veeam Backup & Replication provides you with an option to back up vCloud Director vApps and restore them back to the vCloud Director hierarchy.

In terms of vCloud Director, a vApp is a coherent system that includes one or more VMs. Every vApp is described with a set of operational details – vApp metadata. vApp metadata contains the following information:

- vApp owner settings
- Access rights settings
- vApp network settings: information about organization networks to which the vApp is connected
- Lease settings and so on

When Veeam Backup & Replication performs backup of a vApp, it backs up all VMs being a part of this vApp along with the vApp metadata. Backup of the vApp is performed with the [vCD backup job](#). The vCD backup job may contain one or several vApps. If necessary, you can exclude specific VMs and VM disks from the backup when configuring a vCD backup job.

Veeam Backup & Replication offers the following restore options for backed up vApps:

- [Restoring vApps to vCloud Director](#)
- [Restore of separate VMs being a part of the vApp to vCloud Director](#)

NOTE:

Just like vCloud Director, Veeam Backup & Replication treats a vApp as a coherent system. For this reason, it is recommended that you add entire vApps, not separate VMs from the vApp, to the vCD backup job. If you do not want to back up specific VMs in the vApp, you can use exclusion settings in the vCD job.

Backup of vCloud Director VMs

Veeam Backup & Replication lets you perform backup for vApps and VMs, as well as VM containers in vCloud Director such as Organization vDC, Organization and even the vCloud Director instance.

When Veeam Backup & Replication performs backup of vApps and VMs, it additionally captures vApp metadata.

vApp metadata includes:

- General information about the vApp where VMs reside, such as: vApp name, description, VMs 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. Capturing vApp metadata is extremely important for restore: without it, you will not be able to restore vApps and VMs back to vCloud Director.

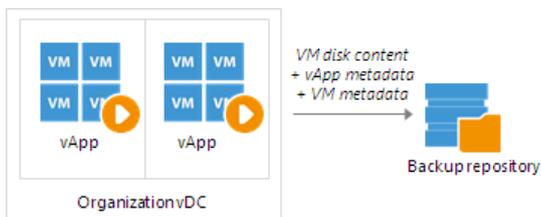
Data to Back Up

With Veeam Backup & Replication, you can back up regular VMs and linked clone VMs.

Backup of Regular VMs

When you perform backup of regular VMs, Veeam Backup & Replication captures and stores to the backup file the following data:

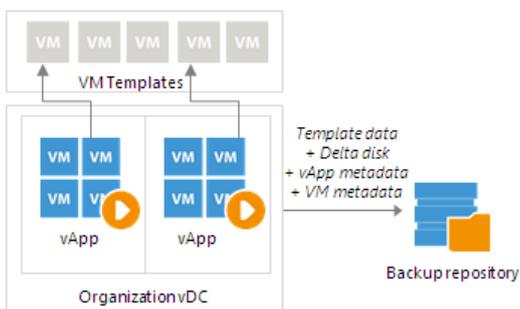
- VM disk content
- vApp metadata
- VM metadata



Backup of Linked Clone VMs

When you perform backup of linked clone VMs, Veeam Backup & Replication captures and stores to the backup 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



During full backup of linked clone VMs, Veeam Backup & Replication consolidates data of the VM template and delta disk and saves it as a regular VM disk in the backup 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 backup.

During incremental backup, Veeam Backup & Replication saves only changed data of the delta file.

Limitations for Backup of Linked Clone VMs

Before you perform backup of linked clone VMs, consider the following:

- [For vCenter 6.5 or later] If you perform backup of a linked clone VM that has snapshots, Veeam Backup & Replication may fail to produce a valid restore point. To overcome this issue, do one of the following:
 - Disable CBT (Change Block Tracking) in the backup job settings.
 - Ensure that CBT is enabled on the VM template to which the VM is linked.

For details on how to enable CBT on the VM template, contact Veeam Customer Support.

- Performing backup of linked clone VMs created with services other than vCloud Director may cause snapshot-related problems. To overcome this issue, disable Veeam Snapshot Hunter. For details, see [this Veeam KB article](#).

vCD Backup Jobs

For VMs managed by vCloud Director, Veeam Backup & Replication offers a special type of the backup job – vCD backup job. vCD backup jobs have been specifically developed to process vCloud Director objects, ensure their proper restore and support of vCloud-specific features.

It is recommended that you use vCD backup jobs to back up VMs managed by vCloud Director. If you back up VMs managed by vCloud Director using a regular backup job, Veeam Backup & Replication will perform backup at the level of the underlying vCenter Server and will not capture vApp metadata. As a result, you will not be able to restore a fully-functioning VM to vCloud Director.

Performing Backup of VMware vCloud Director VMs

The vCD backup is practically the same as a regular VM backup. The vCD backup job aggregates main settings for the backup task and defines when, what, how and where to back up vCD VMs.

You can perform the vCD backup job for single VMs and for VM containers:

- vApp
- Organization vDC
- Organization
- VMware vCloud Director instance

Just like a regular backup job, the vCD backup job can be scheduled or run manually. To create a vCD backup job, do one of the following:

- On the **Home** tab, click **Backup Job** and select **vCloud**.
- Open the **Home** view, in the inventory pane right-click **Jobs** and select **Backup > vCloud**.
- Open the **Inventory** view, click the **View** tab and click **vCloud View** on the ribbon. In the inventory pane expand the **vCloud Director** hierarchy, in the working area select one or more VMs, click **Add to Backup** on the ribbon and select **New job**. Alternatively, you can right-click one or several VMs and select **Add to backup job > New job**. In this case, the selected VMs will be automatically added to the new vCD backup job. You can add other VMs to the job when passing through the wizard steps.

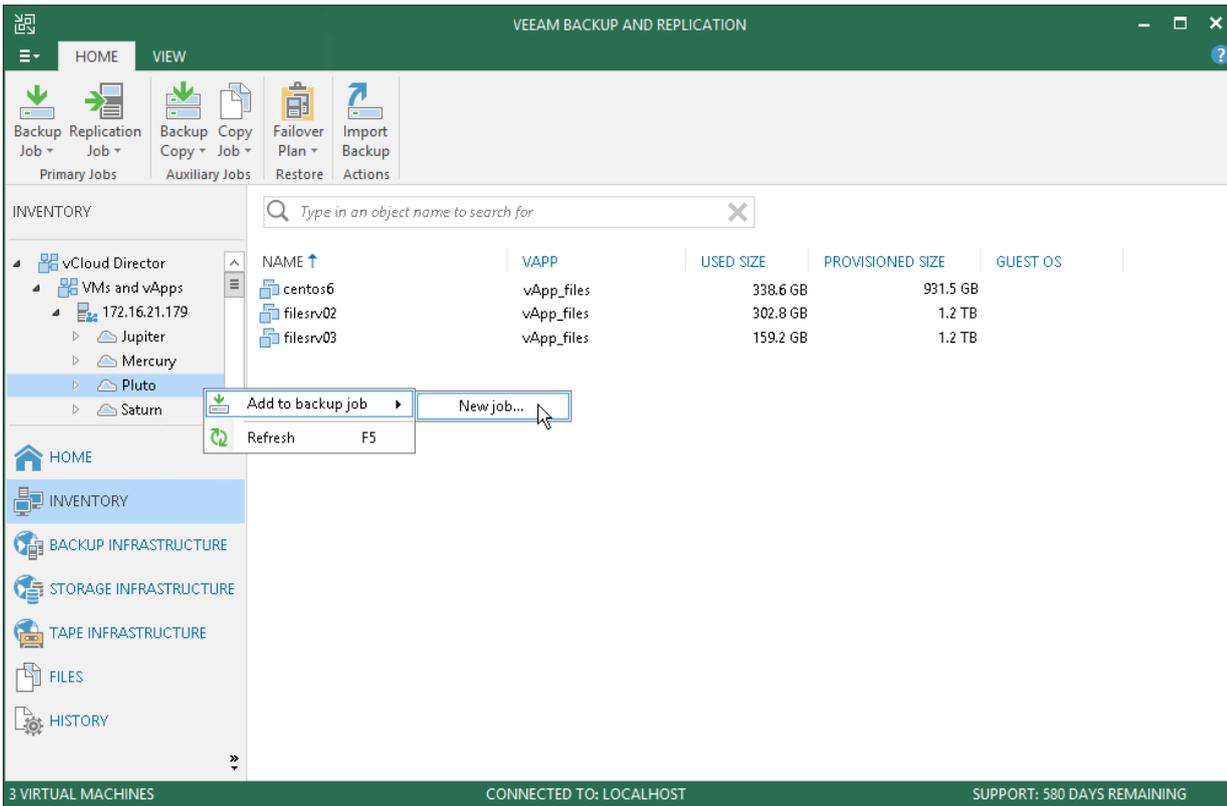
You can quickly include VMs to already existing vCD backup jobs. To do this, in the **Inventory** view, in the working area right-click necessary VMs and select **Add to backup job > name of the job**.

The **New vCD Backup Job** wizard offers the same options as a **New Backup Job** wizard. For more information, see [Creating Backup Jobs](#).

IMPORTANT!

If you run a vCD backup job for the vApp, the job is considered to finish with the *Success* status and the complete restore point for the vApp is created only if all VMs in the vApp are successfully backed up. If any VM in the job fails, the restore point for the vApp will be in the incomplete status, and you will not be able to restore the whole vApp from such restore point.

However, you will be able to perform restore to the original vApp for VMs that were partially or successfully backed up and whose data is available in the incomplete restore point. Veeam Backup & Replication will restore all data that is available for such VMs in the backup.

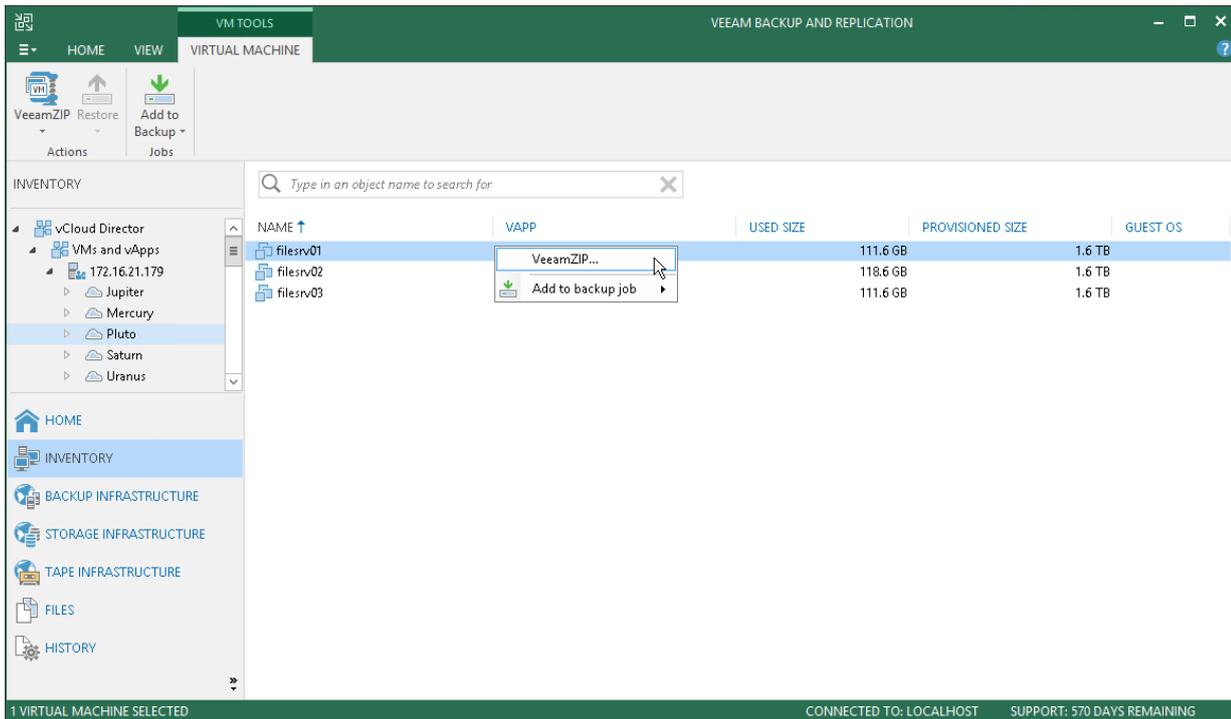


Creating VeeamZIP Files for VMware vCloud Director VMs

You can create a VeeamZIP file for one or more vCD VMs.

When Veeam Backup & Replication creates a VeeamZIP file for a vCD VM, it backs up a VM as separate object. Veeam Backup & Replication does not capture metadata of the vApp to which the VM belongs. When you restore a vCD VM from the VeeamZIP file, Veeam Backup & Replication registers the VM on the underlying ESX(i) host and does not register the VM in vCloud Director.

The process of VeeamZIP files creation for vCD VMs does not differ from that for regular VMware VMs. For more information, see [Creating VeeamZIP Files](#).



Restore of vCloud Director VMs

Veeam Backup & Replication enables full-fledged restore of VMs to vCloud Director. You can restore separate VMs to vApps, as well as VM data.

For restore, Veeam Backup & Replication uses VM metadata saved to a backup 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 settings manually.

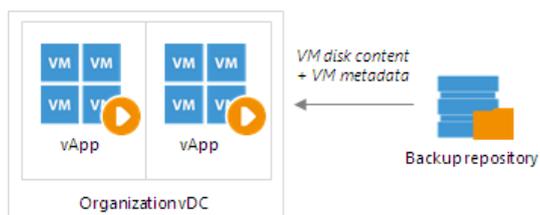
Backed up objects can be restored to the same vCloud Director hierarchy or to a different vCloud Director environment. Restore options include:

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

Restoring Regular VMs to vCloud Director

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

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



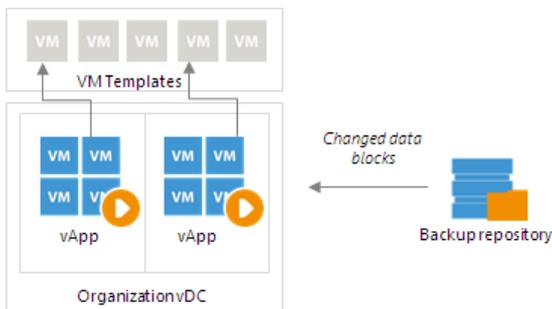
Restoring Linked Clone VMs to vCloud Director

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

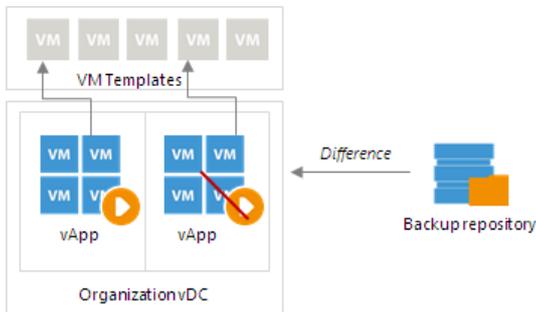


Restore of Deleted VMs

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

1. Veeam Backup & Replication 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 & Replication calculates a signature for the consolidated VM disk in the backup file (containing the VM template data and data of the delta file) and the signature for the created VM in vCloud Director. Veeam Backup & Replication then compares the disk signatures to define what data blocks need to be restored.
3. Veeam Backup & Replication restores only those data blocks that need to be restored from the backup file and writes them to the blank user delta file.

By default, Veeam Backup & Replication links the VM to the same VM template that was used by the initial VM. During restore, Veeam Backup & Replication 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.

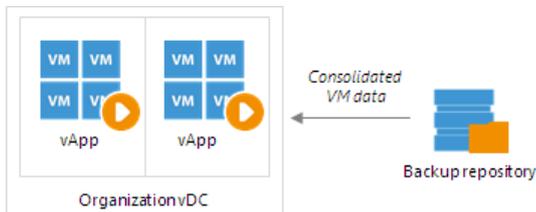


Restore of Linked Clone VMs as Regular VMs

In some cases, Veeam Backup & Replication can restore a VM from a backup 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 & Replication 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 backup file and restores the VM in the vCloud Director hierarchy.



Performing Instant VM Recovery for VMs

Veeam Backup & Replication provides two options for Instant VM Recovery of vCD VMs:

- You can instantly recover a VM to a vApp in vCloud Director.
- You can instantly recover a VM to the virtual infrastructure. In this case, the VM will be restored at the level of the underlying vCenter Server, and the Instant VM Recovery process will be the same as for regular VMware VMs.

When you instantly recover a VM to VMware vCloud Director, Veeam Backup & Replication uses the vPower NFS datastore, just as with other VMware VMs. To import the VM to the vApp, Veeam Backup & Replication needs to associate the vPower NFS datastore with some storage policy. To do this, Veeam Backup & Replication creates for the underlying vCenter Server an auxiliary storage policy – *Veeam-InstantVMRecovery*, and displays it in VMware vCloud Director.

The created storage policy is added to the Provider vDC and Organization vCD hosting the vApp to which the VM is restored. When the vPower NFS datastore is mounted to the ESX(i) host, the vPower NFS datastore is associated with the *Veeam-InstantVMRecovery* storage policy. After that, the VM is instantly restored in a regular manner and imported to the selected vApp.

When an Instant VM Recovery session is finished, the storage policy is not deleted from the Provider vDC, it remains on vCenter Server. This helps speed up all subsequent Instant VM Recovery operations. However, the storage policy is deleted from the Organization vDC as Organization vDC settings can be accessed only by Organization administrators.

Restoring VMs with Instant VM Recovery into vCloud vApp

With Instant VM Recovery, you can immediately start a VM from a backup file stored on the backup repository. Instant VM Recovery accelerates the restore process, allows you to improve RTOs and decrease downtime of production VMs.

Before starting Instant VM Recovery, [check prerequisites](#). Then use the **vCloud Instant VM Recovery** wizard to recover the necessary VM.

Before You Begin

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

- You can perform Instant VM Recovery for a VM that has been successfully backed up at least once.
- You must have at least 10 GB of free disk space on the vPower NFS datastore to store virtual disk updates for the restored VM.

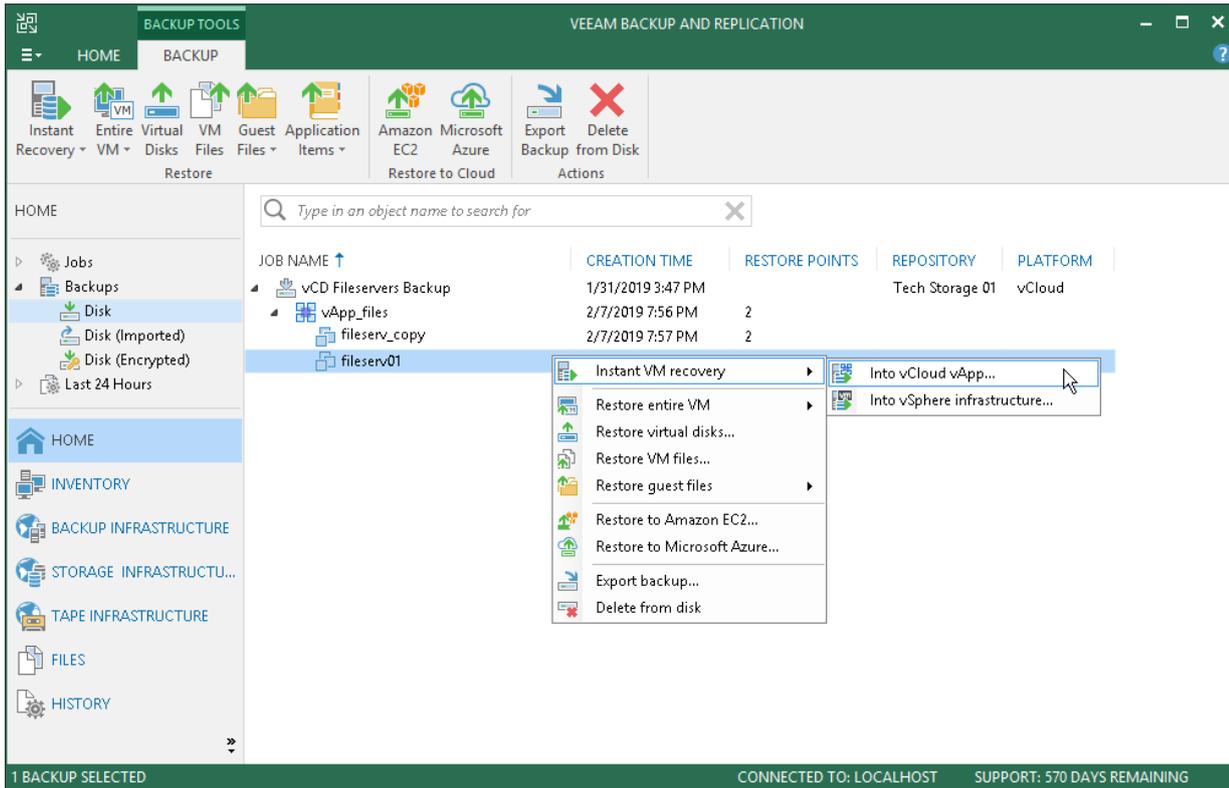
By default, Veeam Backup & Replication writes virtual disk updates to the *NfsDatastore* folder on a volume with the maximum amount of free space, for example, `C:\ProgramData\Veeam\Backup\NfsDatastore`. The vPower cache is not used when you choose to redirect virtual disk updates to a VMware vSphere datastore in the **vCloud Instant VM Recovery** wizard.

- If you are recovering a VM to the production network, make sure that the initial VM is powered off to avoid conflicts.
- If you want to scan VM data for viruses, check the [secure restore requirements and limitations](#).

Step 1. Launch vCloud Instant VM Recovery Wizard

To launch the **vCloud Instant VM Recovery** wizard, do one of the following:

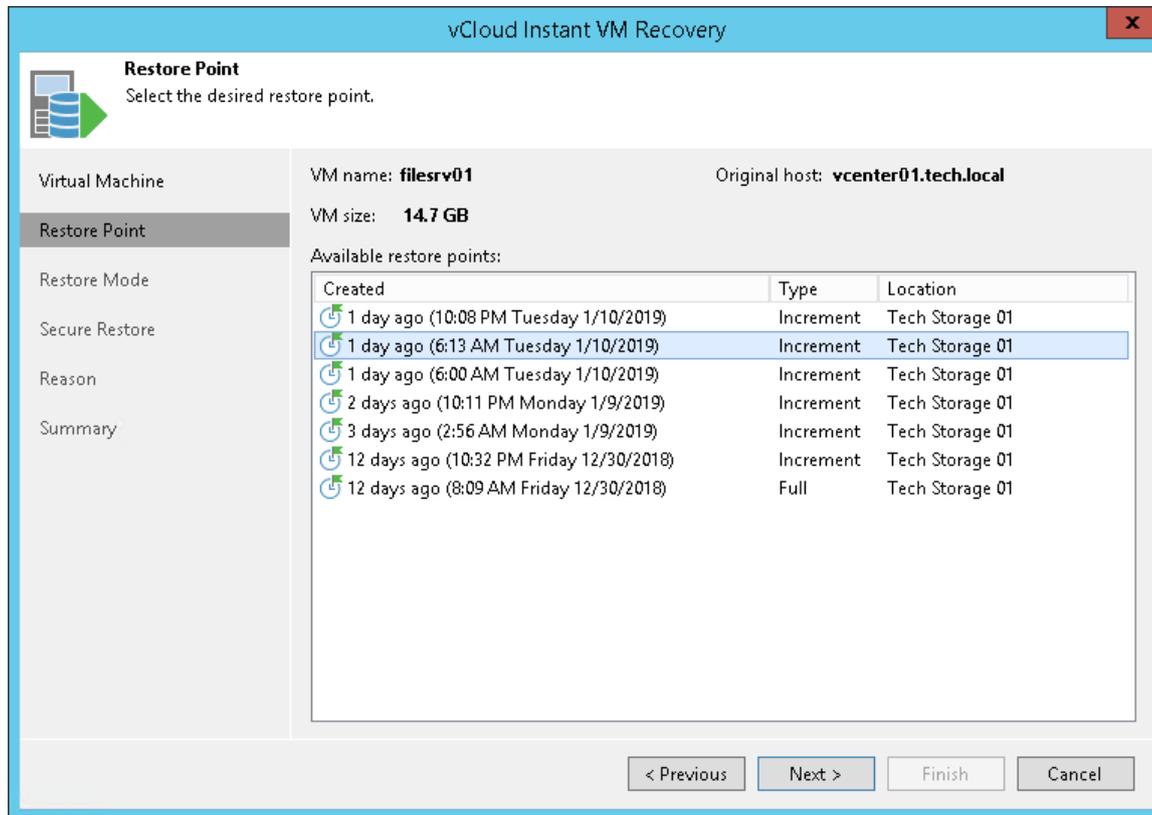
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Select the machine that you want to restore and click **Instant VM Recovery > Into vCloud vApp** on the ribbon.
 - Right-click the machine that you want to restore and select **Instant VM recovery > Into vCloud vApp**.
- Open the **Inventory** view. On the **View** tab, click **vCloud View**. In the inventory pane, expand the **vCloud Director** hierarchy. In the working area, right-click the VM you want to restore and select **Restore > Instant VM recovery > Into vCloud vApp**.



Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the restore point for the VM.

In the **Location** column, you can view a name of a backup repository where a restore point resides.

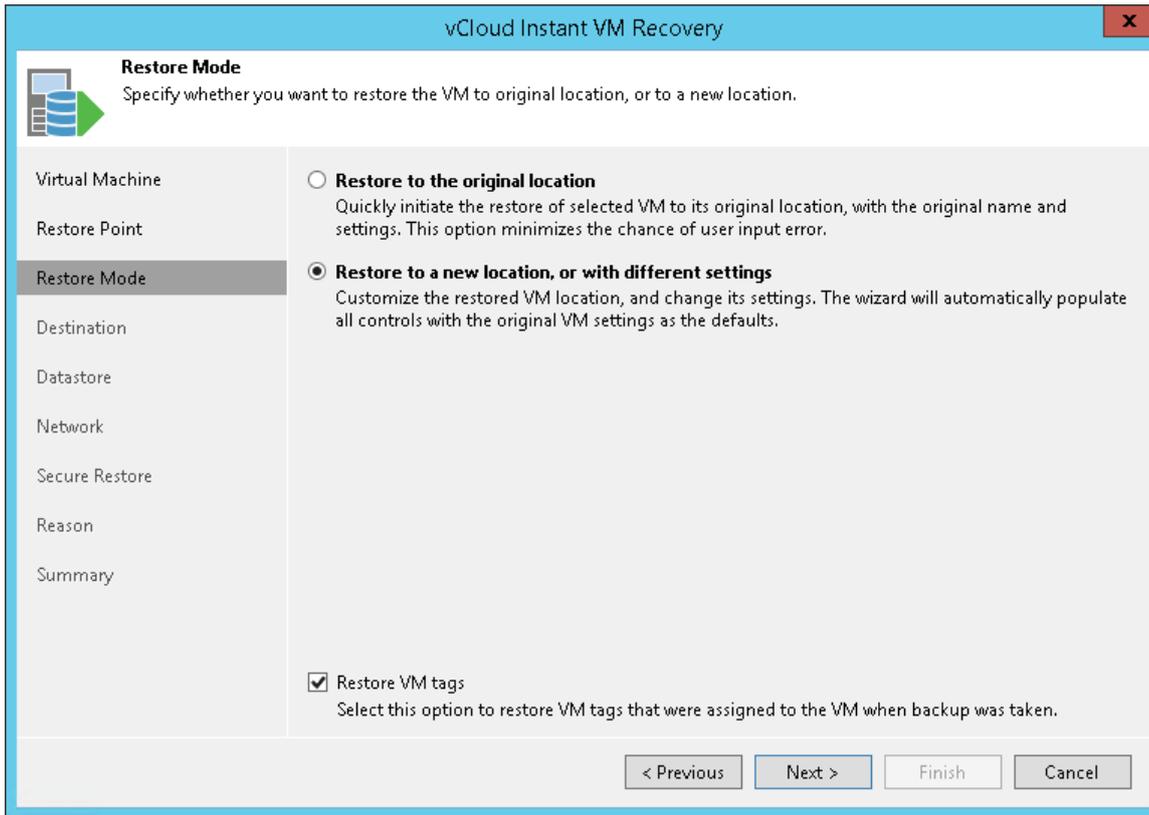


Step 3. Select Restore Mode

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

1. Choose a 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 **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 (such as vApp, VM name, network settings and so on). If this option is selected, the **Instant Recovery** 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. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:
 - The VM is restored to its original location.

- The original VM tag is still available on the source vCenter Server.



Step 4. Select Destination for Restored VM

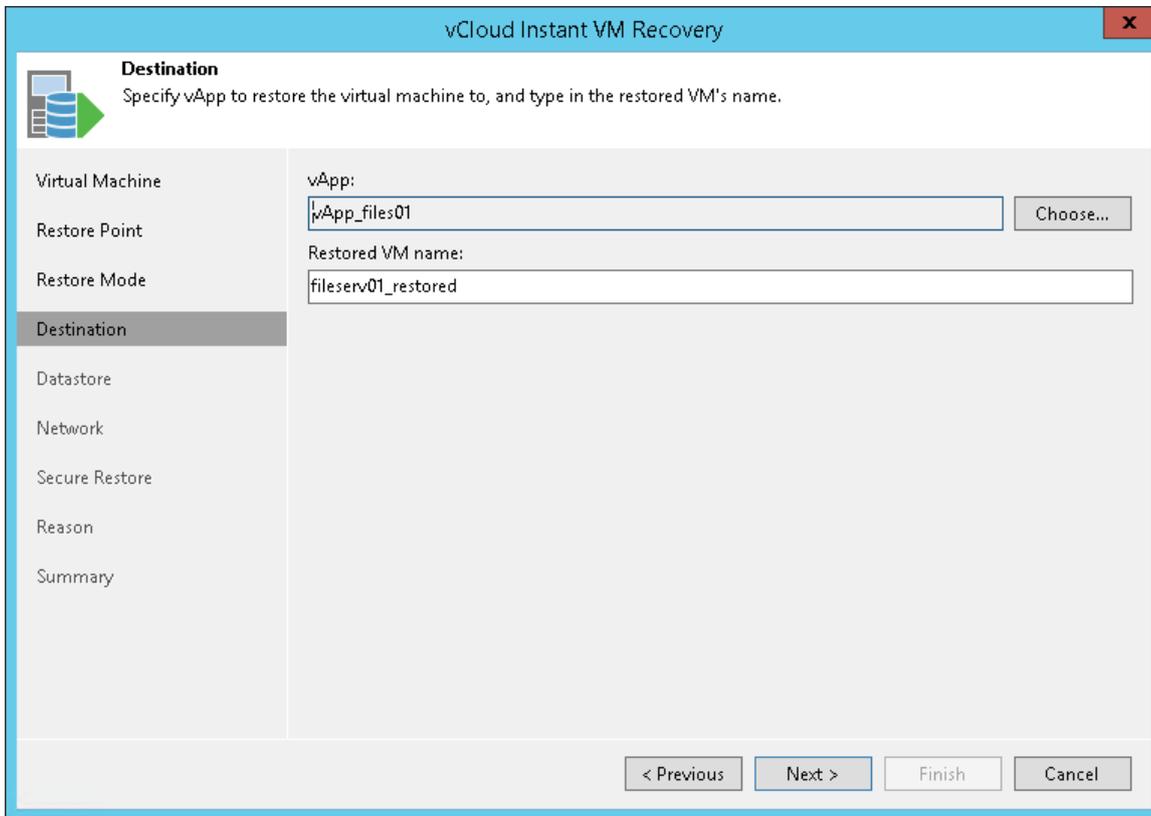
The **Destination** step of the wizard is available if you have chosen to change the location and settings of the restored VM.

Select a destination and specify a name for the restored VM:

1. In the **vApp** field, specify a vApp to which the VM must be restored. By default, Veeam Backup & Replication restores the VM to its initial vApp.
2. In the **Restored VM name** field, enter a name under which the VM must be restored and registered. By default, Veeam Backup & Replication uses the original name of the VM. If you are restoring the VM to the same vApp 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.

NOTE:

Veeam Backup & Replication checks the lease term for the vApp to which the VM is restored. In case the lease period has expired, the lease will be automatically updated.



Step 5. Select Destination for Virtual Disk Updates

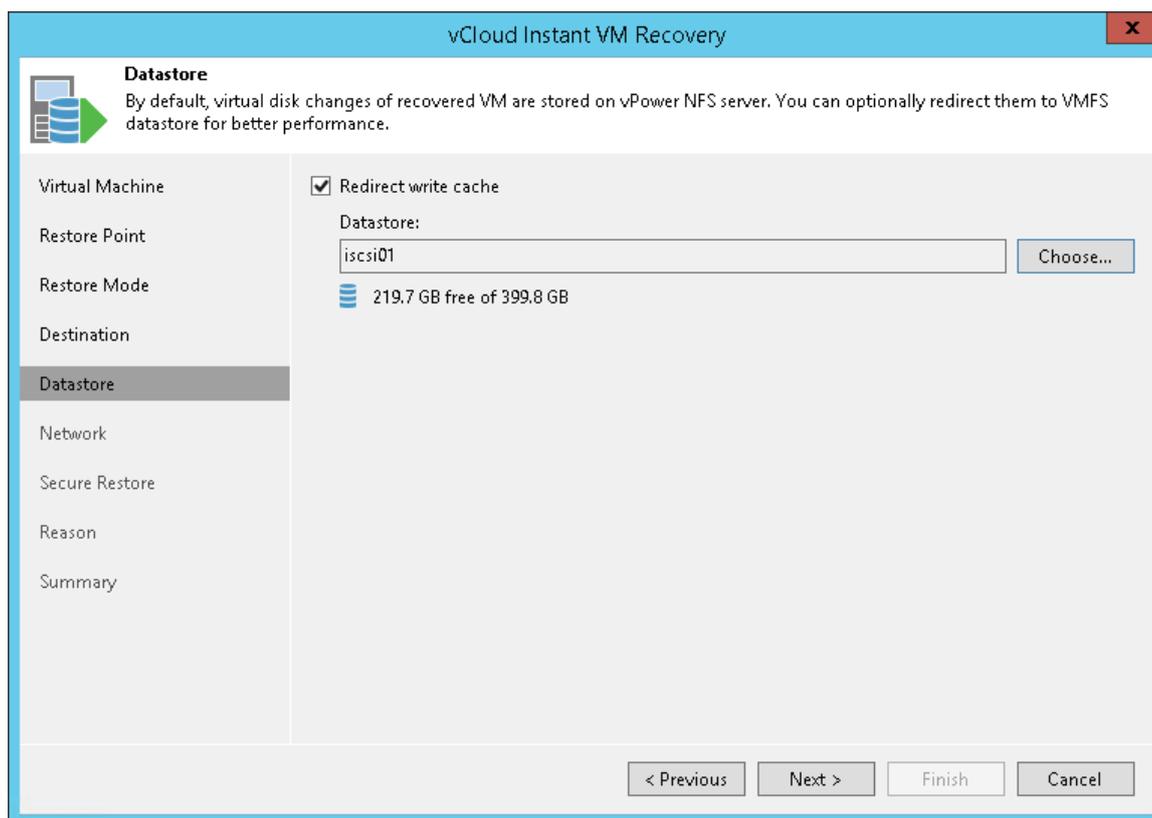
The **Datastore** step of the wizard is available if you have chosen to change the location and settings of the restored VM.

Select the location for holding the VM disk changes when the VM is restored. By default, disk changes are stored directly on the vPower NFS server. However, you can store disk changes on any datastore in your virtual environment. Redirecting disk changes improves recovery performance but makes Storage vMotion not possible for ESX 4.x and earlier.

To select a datastore:

1. Select the **Redirect virtual disk updates** check box.

2. From the **Datastore** list, choose the necessary datastore. You can select only a datastore that is available in the Organization vCD hosting the vApp to which the VM is restored.



Step 6. Select Destination Network

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

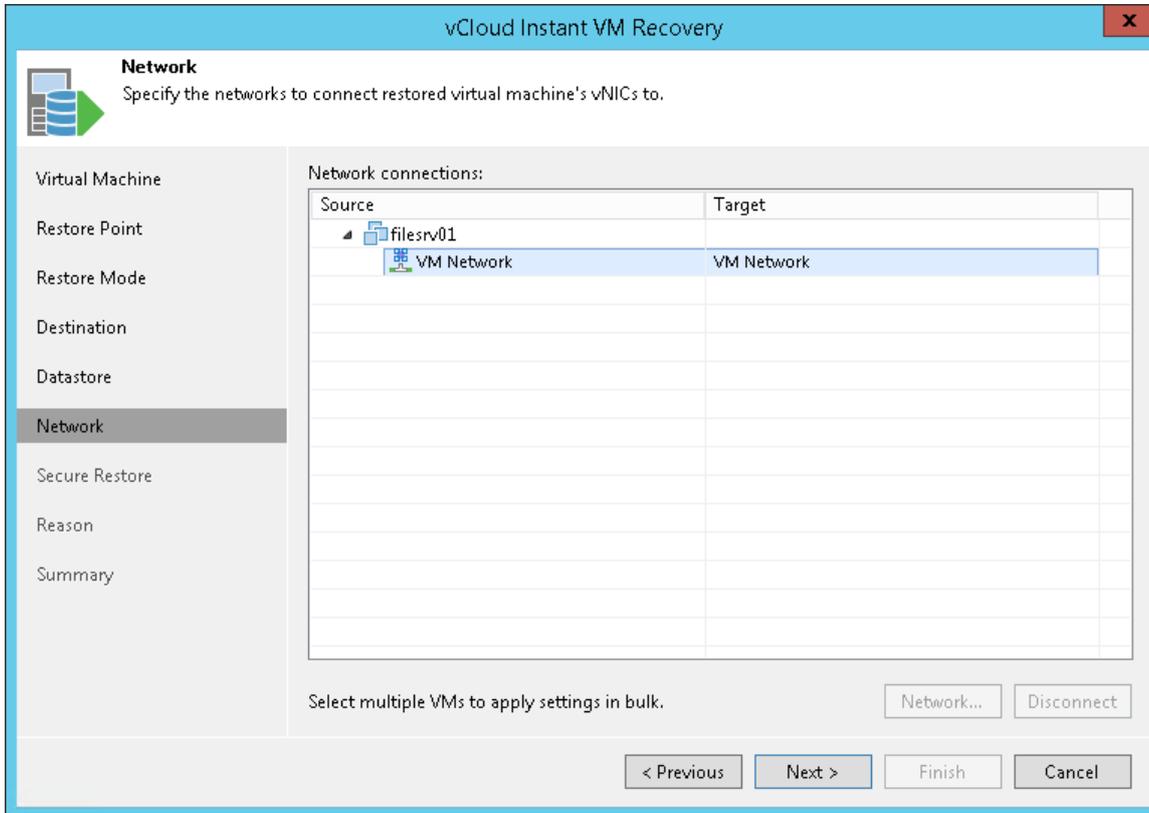
To select networks to which restored VMs must be connected:

1. Select a VM in the list and click **Network**.
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 selected VM should 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]**.

3. To prevent the restored VM from accessing any network, select it in the list and click **Disconnect**.

Veeam Backup & Replication maps the network settings you define and network settings of the initial VM. If necessary, Veeam Backup & Replication makes changes to the network settings of the recovered VM. For example, if the initial VM was connected to the network using the static IP mode and you have selected to connect a recovered VM to a network using the dynamic IP mode, Veeam Backup & Replication will change the network settings to the dynamic mode.



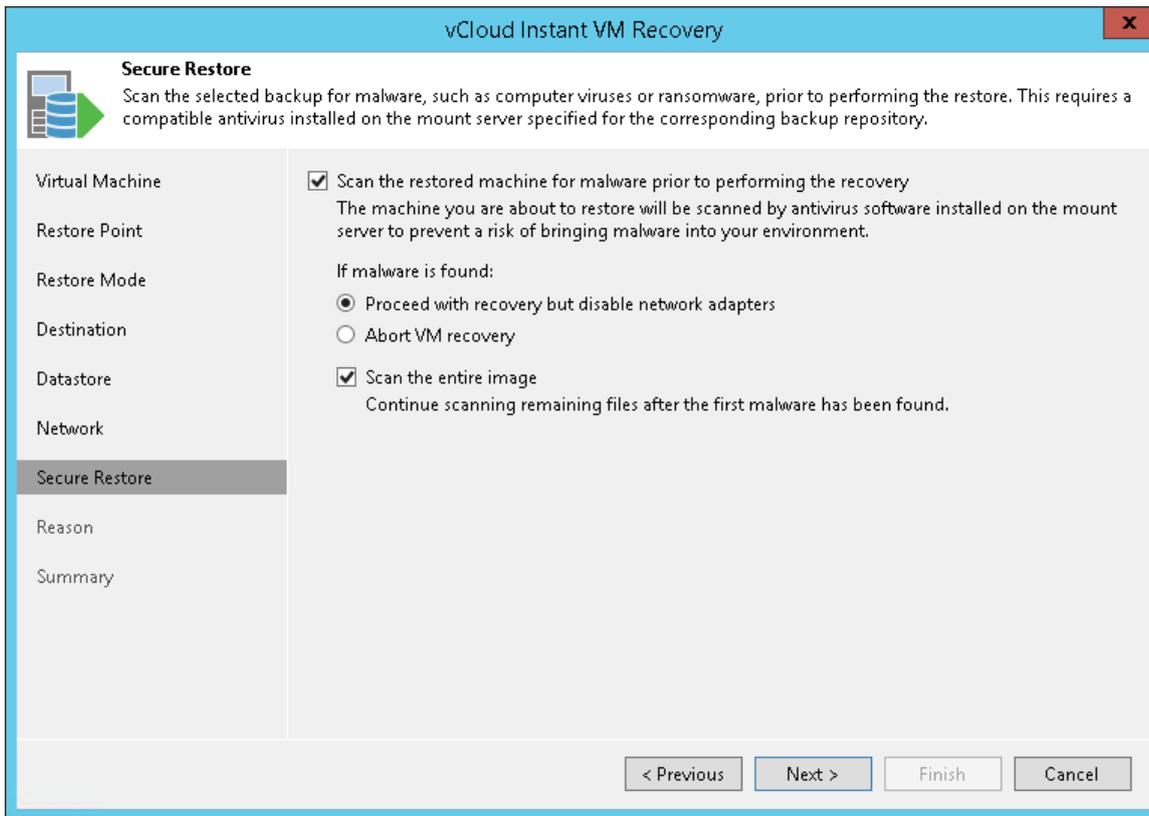
Step 7. Specify Secure Restore Settings

You can instruct Veeam Backup & Replication to perform secure restore – scan VM data with antivirus software before restoring the VM to the production environment. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

1. At the **Secure Restore** step of the wizard, select the **Scan the restored machine for malware prior to performing the recovery** check box.
2. Select which action Veeam Backup & Replication will take if the antivirus finds a virus threat:
 - **Proceed with recovery but disable network adapters.** Select this action if you want to restore the VM with disabled network adapters (NICs).
 - **Abort VM recovery.** Select this action if you want to cancel the restore session.

3. Select the **Scan the entire image** check box if you want the antivirus to continue the VM data scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).

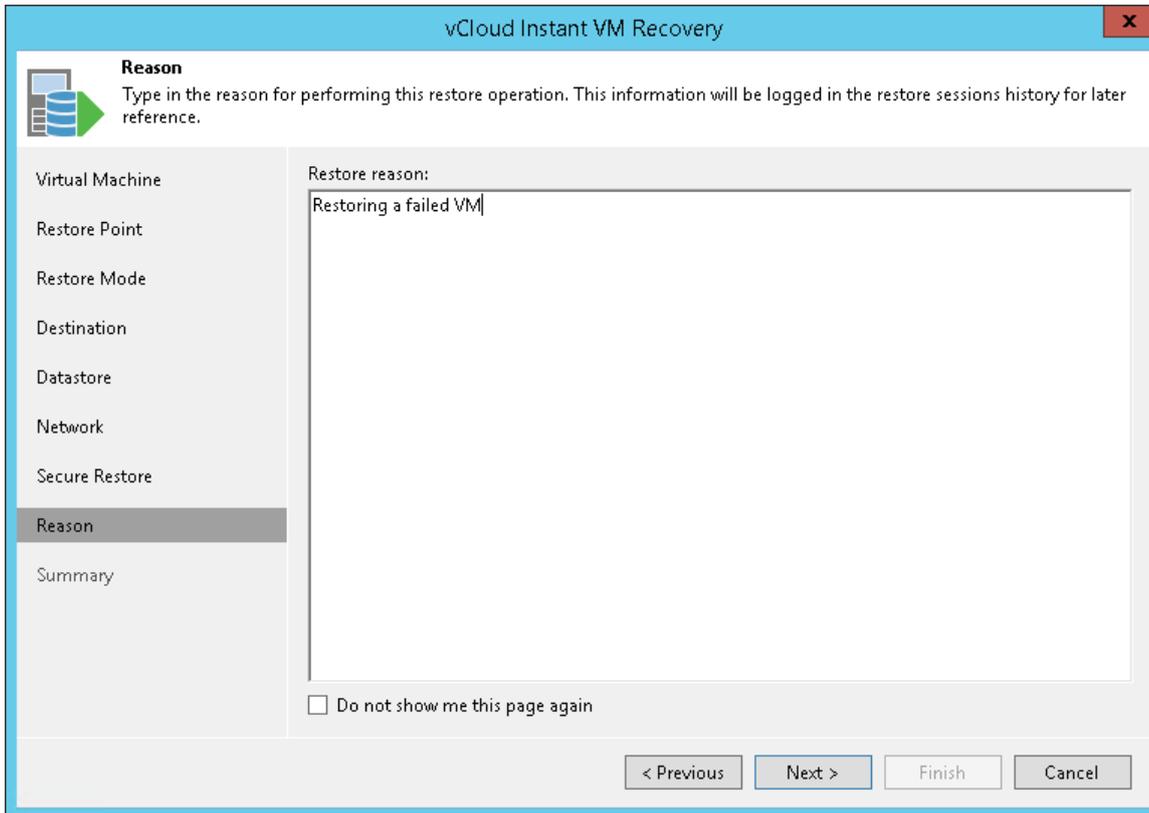


Step 8. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for performing Instant VM Recovery of the VM. 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.



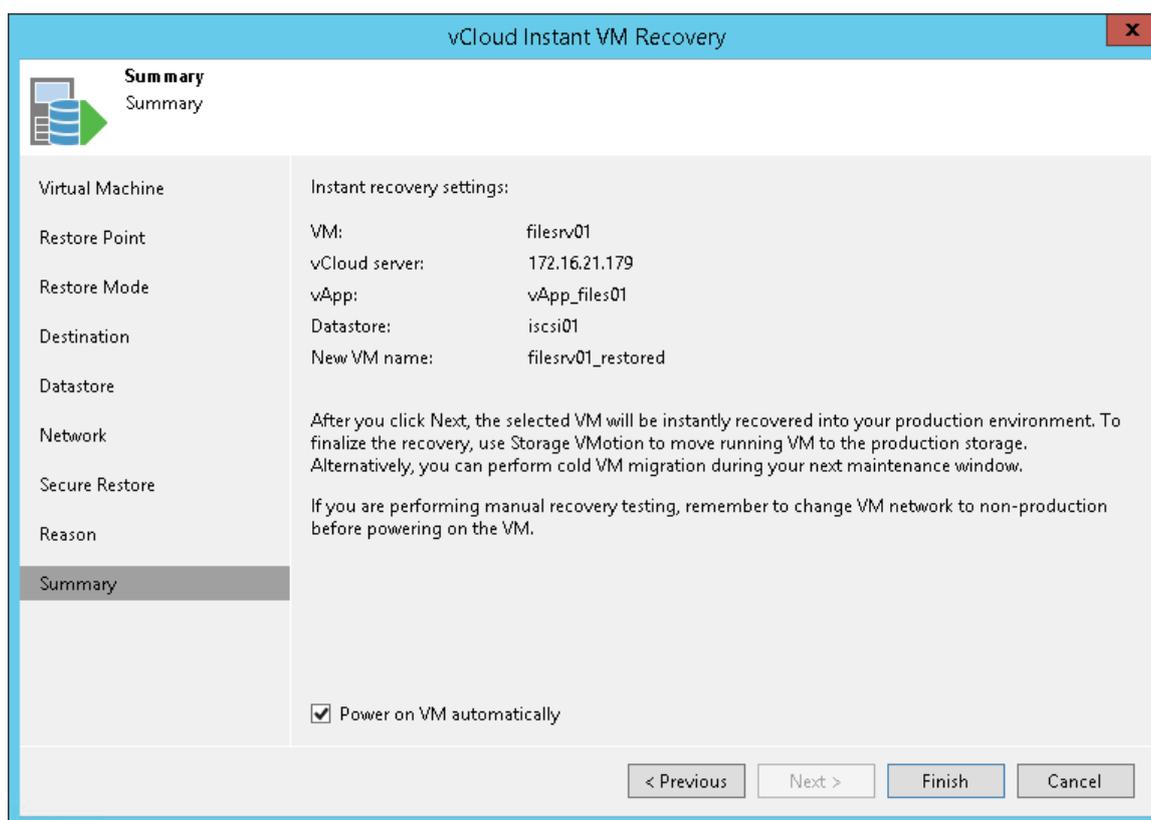
The screenshot shows the 'vCloud Instant VM Recovery' wizard window. The title bar is blue with the text 'vCloud Instant VM Recovery' and a close button. The main area is divided into a left sidebar and a main content area. The sidebar contains a list of steps: Virtual Machine, Restore Point, Restore Mode, Destination, Datastore, Network, Secure Restore, Reason (highlighted), and Summary. The main content area has a header 'Reason' with a sub-header 'Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.' Below this is a large text input field with the text 'Restoring a failed VM'. At the bottom of the main content area is a checkbox labeled 'Do not show me this page again'. The bottom of the window contains four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 9. Verify Instant VM Recovery Settings

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

1. If you want to start the recovered VM, select the **Power on VM automatically** check box.

2. Check the specified settings of Instant VM Recovery and click **Finish**. Veeam Backup & Replication will recover the selected VM in the specified destination.



Step 10. Finalize Instant VM Recovery

All VMs restored with Instant VM Recovery are displayed in the **Home** view, under the **Instant Recovery** node.

To check the progress of Instant VM Recovery and view session details:

1. Open the **Home** view.
2. In the inventory pane, click the **Instant Recovery** node.
3. Right-click the VM in the working area and select **Properties**.

Alternatively, you can open the **History** view, select the **Instant Recovery** node under **Restore** in the inventory pane and double-click the necessary instant VM restore session.

After the VM has been successfully recovered, you can finalize Instant VM Recovery in one of two ways:

- [Migrate the recovered VM to the production environment](#)
- [Unpublish the recovered VM](#)

Migrating Recovered VM

To migrate the restored VM to production:

1. Open the **Home** view.
2. In the inventory pane, select the **Instant Recovery** node.
3. In the working area, right-click the VM and select **Migrate to production**. Veeam Backup & Replication will launch the [Quick Migration](#) wizard.

During migration, Veeam Backup & Replication will restore the VM from the backup file and additionally move all changes that were made while the VM was running from the backup in the Instant Recovery mode.

TIP:

When you pass through the **Quick Migration** wizard, enable the **Delete source VM files upon successful migration** option. Veeam Backup & Replication will restore the VM to production and automatically stop the Instant VM recovery session. If you do not enable this option, the Instant VM recovery session will still be running, and you will need to unpublish the recovered VM manually.

Unpublish Recovered VM

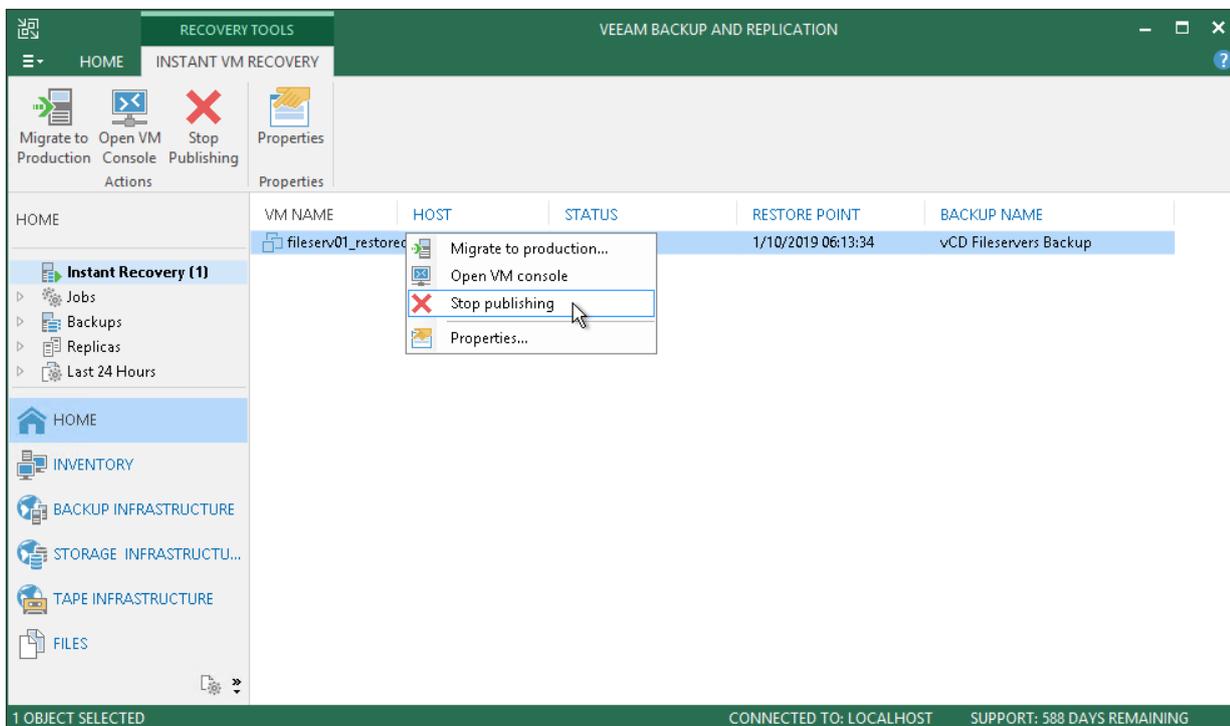
If you have disabled the **Delete source VM files upon successful migration** option in the Quick Migration settings, you must unpublish the VM manually. After you unpublish the VM, the Instant Recovery session will end and the recovered VM will be unmounted from the vPower NFS server. The migrated VM will remain on the production environment.

To unpublish a recovered VM:

1. Open the **Home** view.
2. In the inventory pane, select the **Instant Recovery** node.
3. In the working area, right-click the VM and select **Stop publishing**.

TIP:

After the VM has been published from the backup, you can open the VM console directly from Veeam Backup & Replication. To do this, in the working area right-click the VM and select **Open VM Console**.

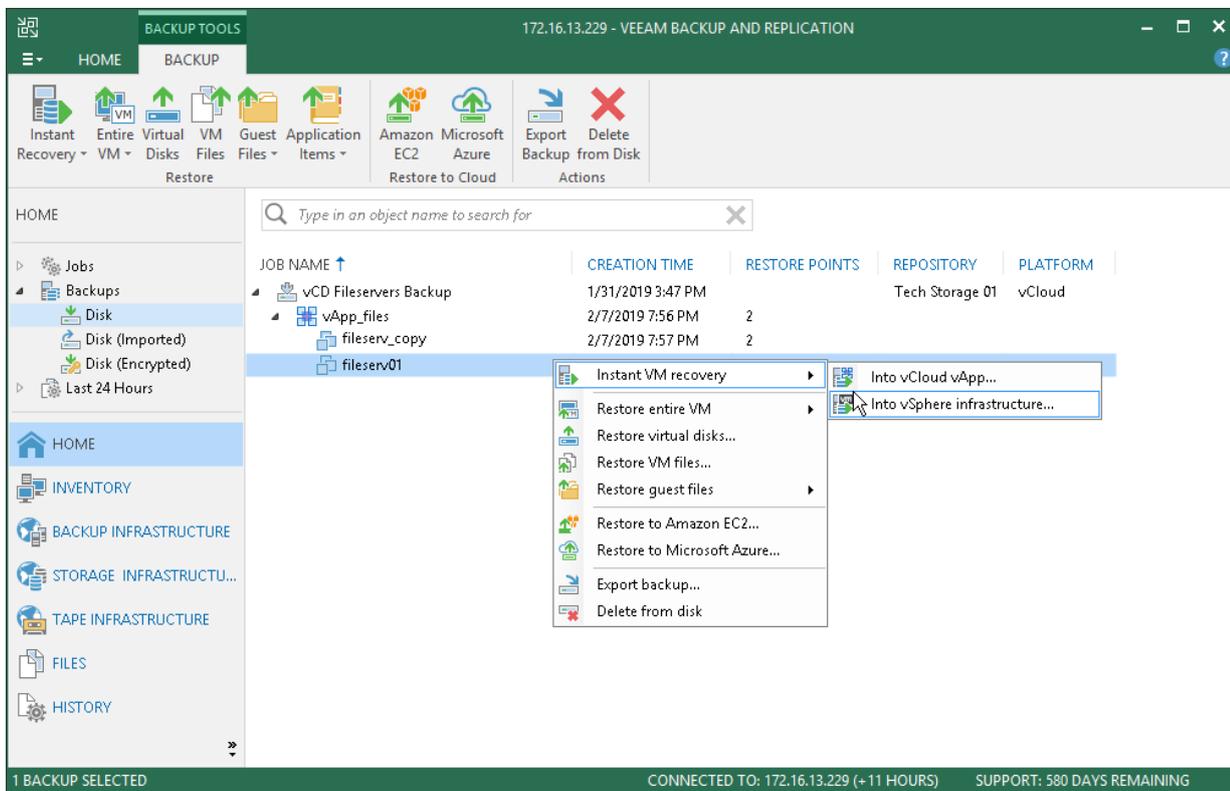


Restoring VMs with Instant VM Recovery into vSphere infrastructure

To launch the **Instant Recovery** wizard, do one of the following:

- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Select the machine that you want to restore and click **Instant VM Recovery > Into vSphere infrastructure** on the ribbon.
 - Right-click the machine that you want to restore and select **Instant recovery > Into vSphere infrastructure**.
- Open the **Inventory** view. On the **View** tab, click **vCloud Director View**. In the inventory pane, expand the vCloud Director hierarchy. In the working area, right-click the VM you want to restore and select **Restore > Instant VM Recovery > Into vSphere infrastructure**.

The process of Instant VM Recovery for vCD VMs does not differ from the regular Instant VM Recovery process. For more information, see [Performing Instant VM Recovery](#).



Restoring vCloud vApps

You can restore the whole vApp from the backup to VMware vCloud Director.

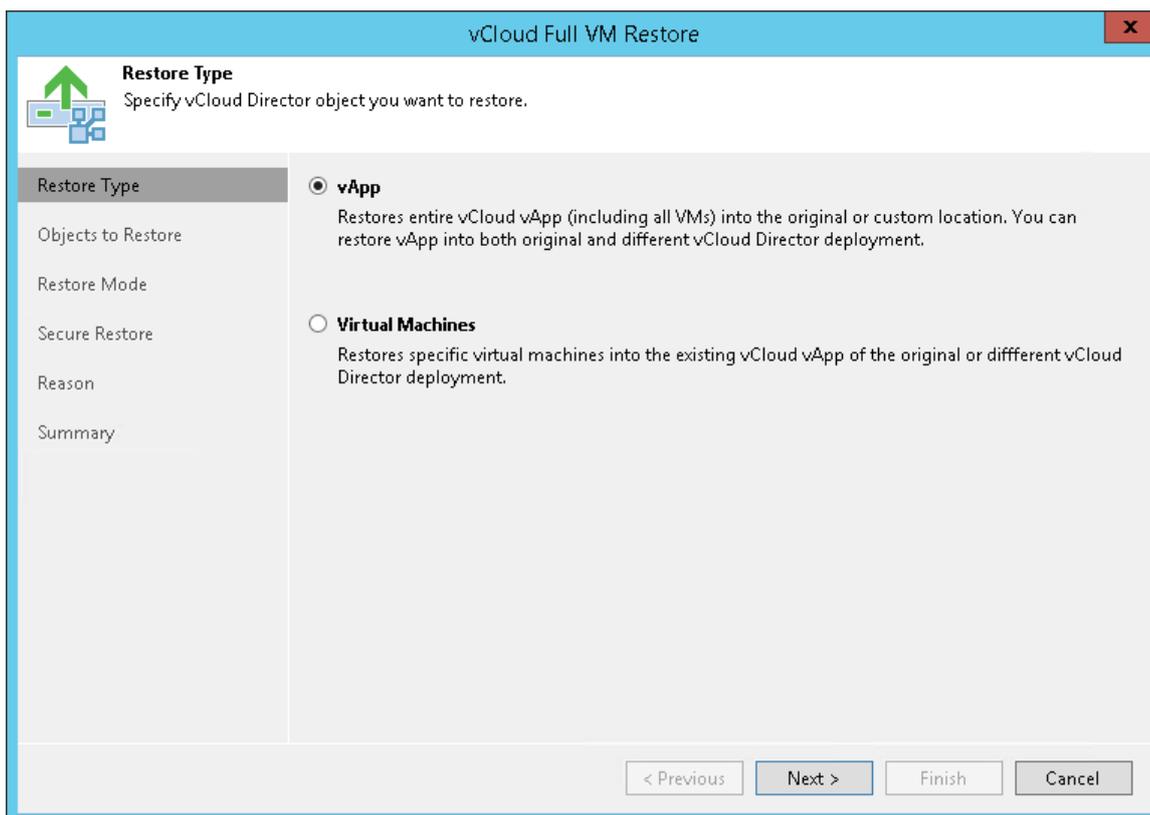
vApps can be restored to their Organization vDC or to any other Organization vDC. You can restore the vApp that already exists, for example, in case the initial vApp is corrupted or you want to revert to an earlier state of the vApp, or the vApp that no longer exists, for example, if it was deleted by mistake. If you restore a vApp that already exists, the vApp is overwritten with that from the vCD backup.

To restore a vApp to vCloud Director, use the **vCloud Full vApp Restore** wizard.

Step 1. Launch Full vApp Restore Wizard

To launch the **Full vApp Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware vCloud Director**. At the **Restore Type** step of the wizard, select the object you would like to restore: *vApp*.
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Select the vApp and click **Restore vCloud vApp** on the ribbon.
 - Right-click the vApp and select **Restore vCloud vApp**.



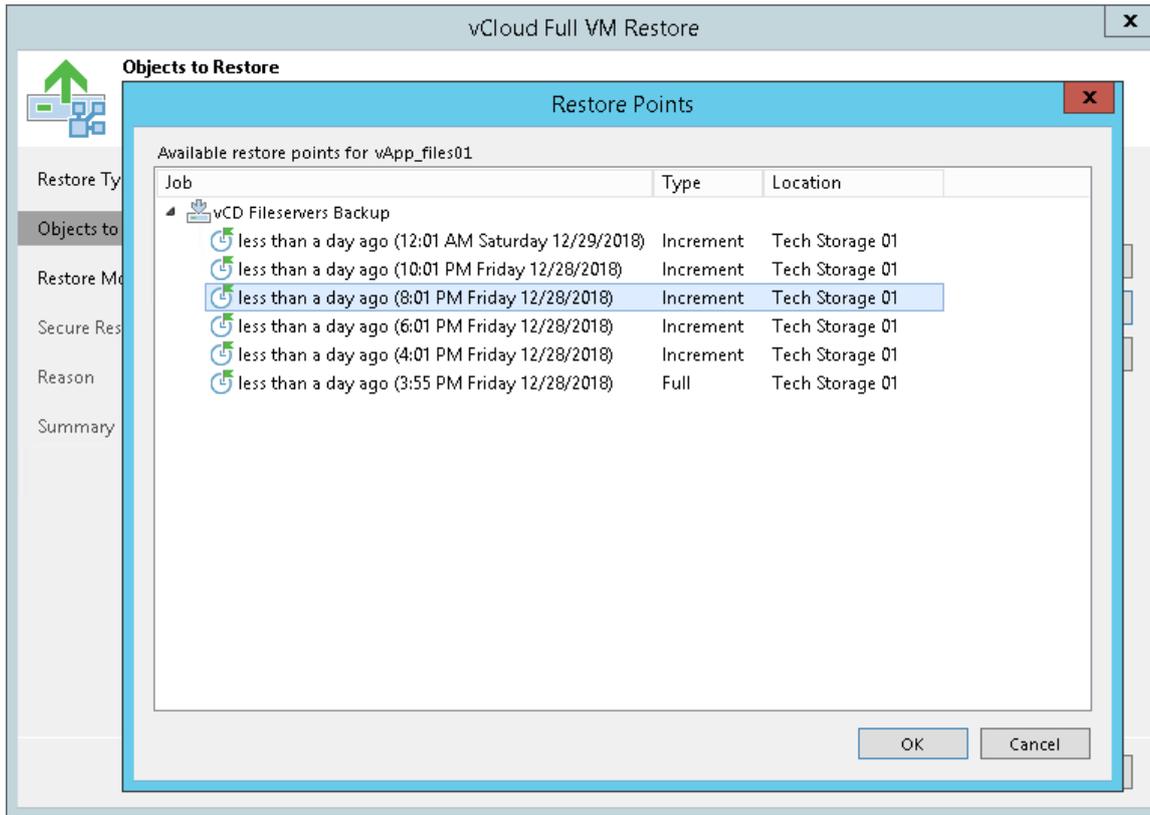
Step 2. Select vApp to Restore

At the **Objects to Restore** step of the wizard, select the vApp you want to restore.

To add a vApp, click **Add vApp** and select where to browse for vApps:

- **From infrastructure** – browse the vCloud Director hierarchy and select a vApp to restore. Note that the vApp you select from the vCloud Director hierarchy must be successfully backed up at least once.

In the **Location** column, you can view a name of a backup repository where a restore point resides.



Step 4. 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 vApp with its initial settings and to its 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 vApp to a different location and/or with different settings (such as Organization vDC, network settings, fast provisioning settings and so on). If this option is selected, the **vCloud Full vApp Restore** wizard will include additional steps for customizing vApp settings.
2. [For vApp restore to the original location] Select the **Quick rollback** check box if you want to use incremental restore for the vApp. Veeam Backup & Replication will query CBT to get data blocks that are necessary to revert the vApp 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 VMs in the vApp 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.

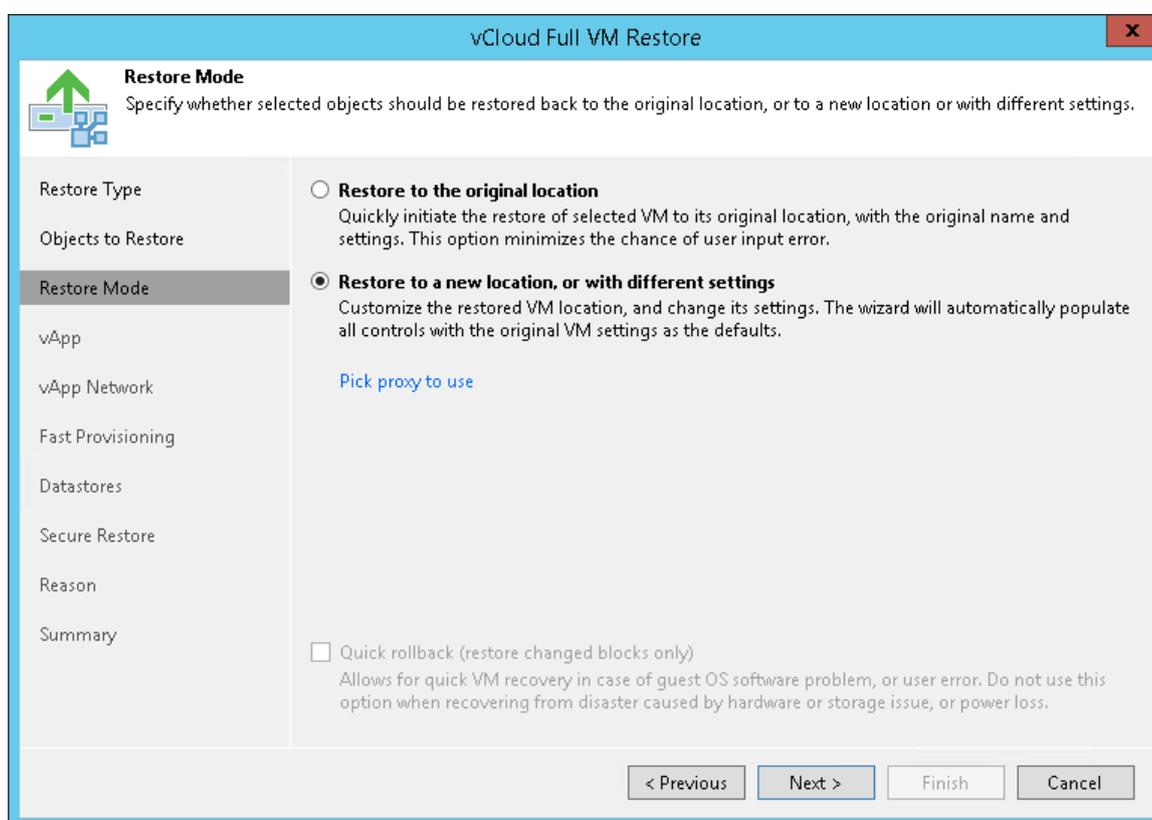
3. Click the **Pick proxy to use** link to select backup proxies over which vApp data must be transported to the source datastore. You can assign backup proxies explicitly or instruct Veeam Backup & Replication to automatically select backup proxies.

- If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that are connected to the source datastore and will automatically assign optimal proxy resources for processing vApp data.

During the restore process, VMs in the vApp are processed simultaneously.

Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use for writing data to target, current workload on these backup proxies, and selects the most appropriate resources for VMs processing.

- If you choose **Use the selected backup proxy serves only**, you can explicitly select backup proxies that will be used for restore. It is recommended that you select at least two proxies to ensure that VMs are recovered should one of backup proxies fail or lose its connectivity to the source datastore during restore.



Step 5. Select vApp Location

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

By default, Veeam Backup & Replication restores the vApp to its initial location with its initial name.

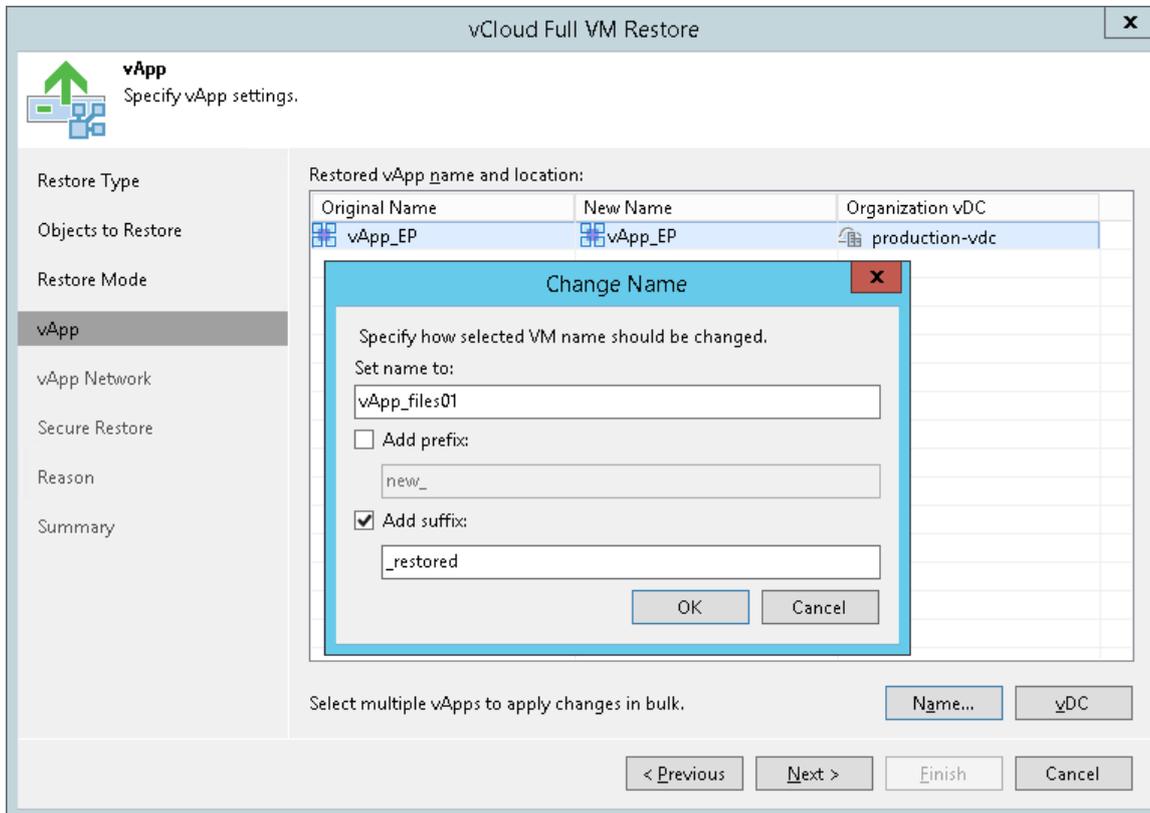
To restore the vApp to a different location:

1. Select the App in the list and click **vDC**.
2. From the vCloud Director hierarchy, choose an Organization vDC where the selected vApp must be registered.

To facilitate selection, use the search field at the bottom of the window: enter an object's name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

To change the vApp name:

1. Select the vApp 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 vApp name.
3. You can also change the vApp name directly in the list: select a vApp, click the **New Name** field and enter the name to be assigned to the recovered vApp.



Step 6. Select Destination Network

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

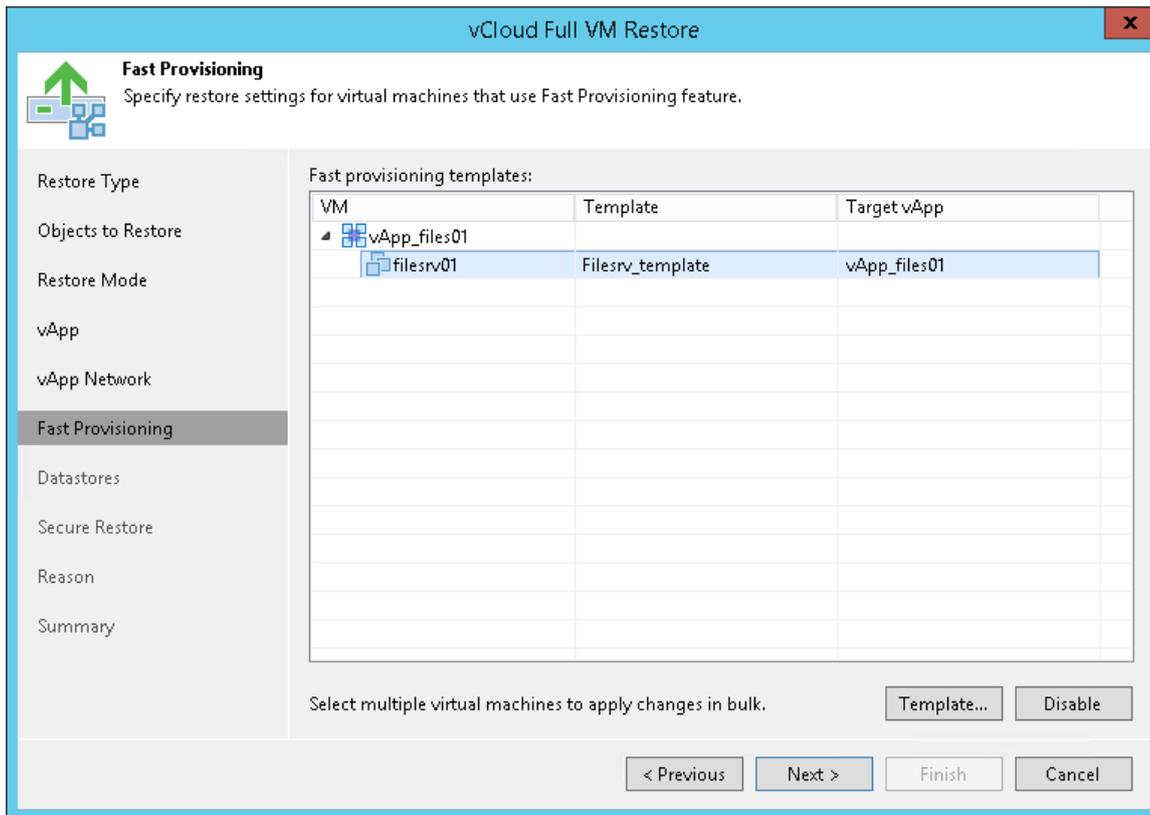
To select networks to which the restored vApp must be connected:

1. Select the vApp in the list and click **Network**.
2. The **Select Network** window displays all networks that are configured for the destination Organization vDC. From the list of available networks, choose a network to which selected vApp 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 vApp from accessing any network, select it in the list and click **Disconnect**.

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**.



Step 8. Select Storage Policy and Datastores

The **Datastores** step of the wizard is available if you have chosen to change settings of the restored vApp, for example, its name or location.

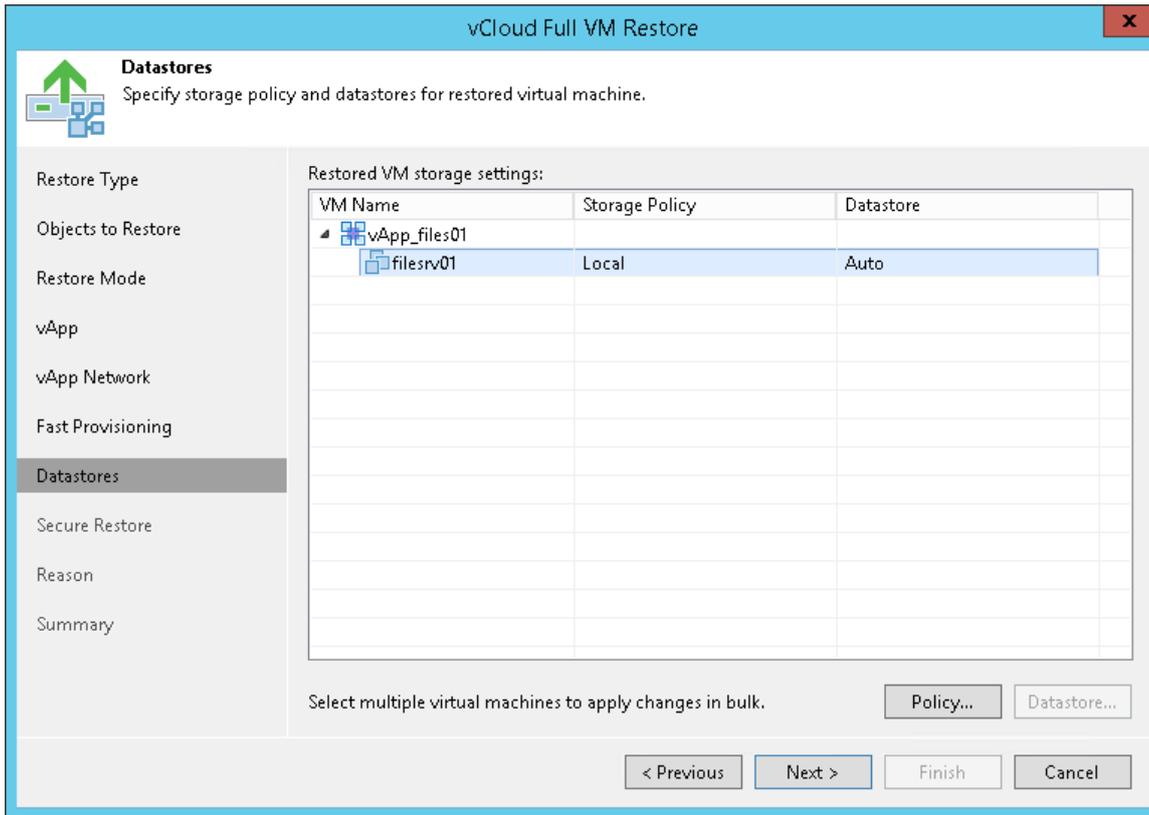
To select a storage policy for the vApp:

1. Select the vApp in the list and click **Policy**.
2. In the displayed window, select the necessary policy for the vApp.

If you have selected to disable fast provisioning at the previous step of the wizard, you must select a datastore on which the disks of restored VMs will be placed. To do this:

1. Select VM or vApp in the list and click **Datastore**.

2. In the displayed window, select the datastore on which the disks of the VM must be placed.



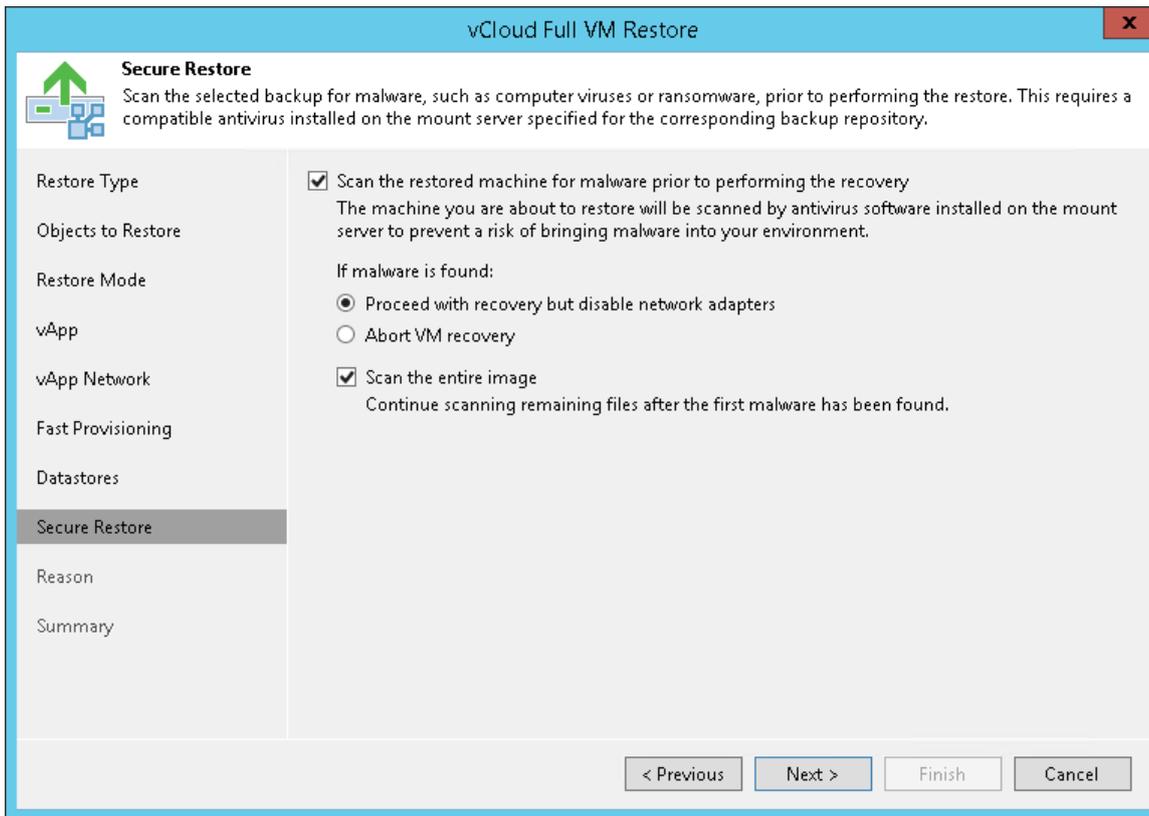
Step 9. Specify Secure Restore Settings

You can instruct Veeam Backup & Replication to perform secure restore – scan vApp data with antivirus software before restoring the vApp. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

1. At the **Secure Restore** step of the wizard, select the **Scan the restored machine for malware prior to performing the recovery** check box.
2. Select which action Veeam Backup & Replication will take if the antivirus finds a virus threat:
 - **Proceed with recovery but disable network adapters.** Select this action if you want to restore the vApp VMs with disabled network adapters (NICs).
 - **Abort VM recovery.** Select this action if you want to cancel the restore session.

3. Select the **Scan the entire image** check box if you want the antivirus to continue the vApp data scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).

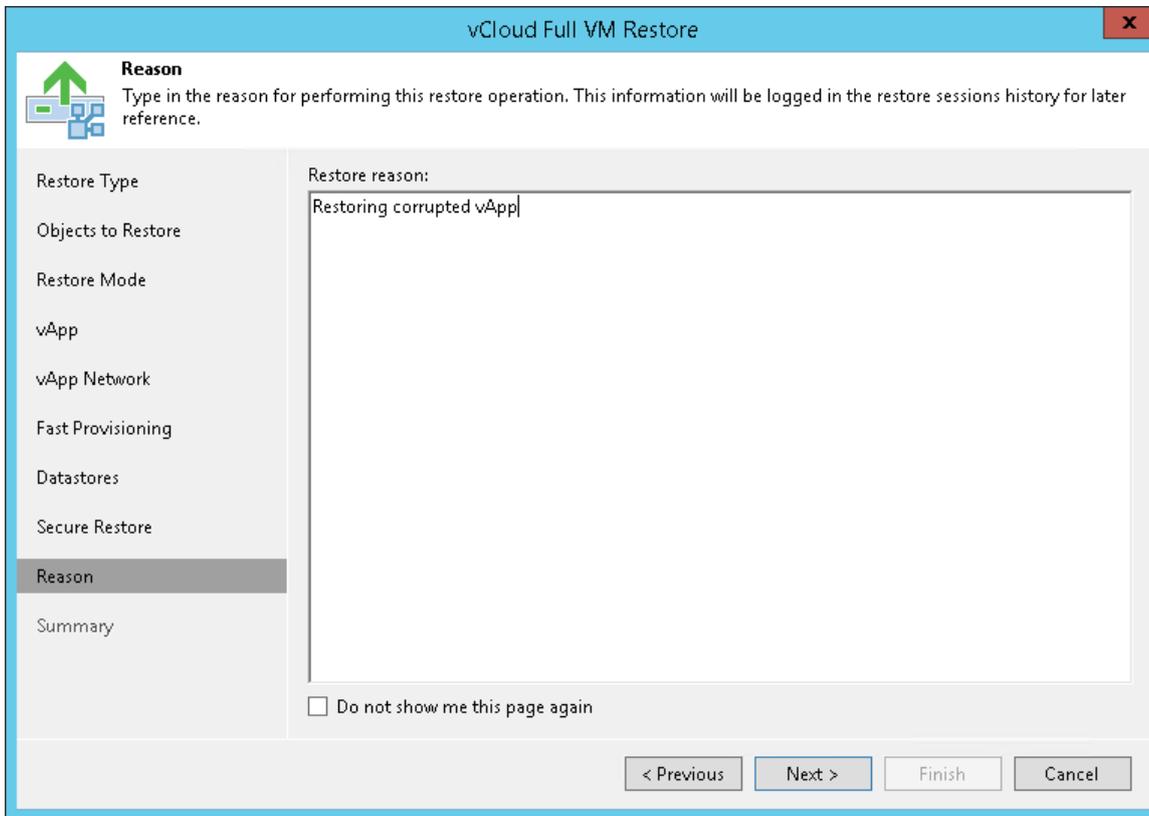


Step 10. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the selected vApp. 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.



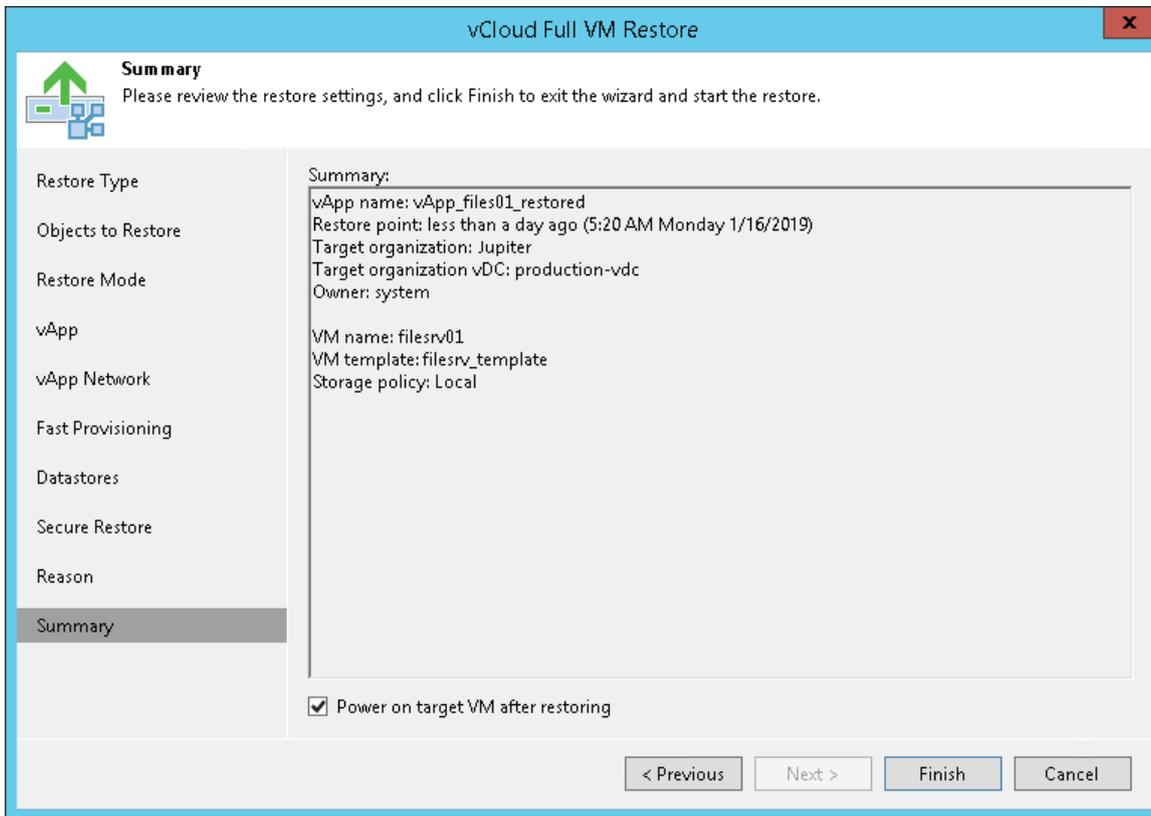
Step 11. Verify Recovery Settings and Finish Working with Wizard

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

1. If you want to start VMs in the restored vApp, select the **Power on VM after restoring** check box.
2. Check the settings for vApp restore and click **Finish**. Veeam Backup & Replication will recover the vApp in the specified destination.

NOTE:

Veeam Backup & Replication checks the lease term for the restored vApp. If the lease period has expired, the lease will be automatically updated.



Restoring VMs into vCloud vApp

You can restore one or several VMs from vCD backups back to VMware vCloud Director.

The vCD VM can be restored to its initial location or to any other location. You can restore a VM that already exists, for example, if 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 the VM was deleted by mistake. If you restore a VM that already exists, the initial VM is overwritten with that from the vCD backup.

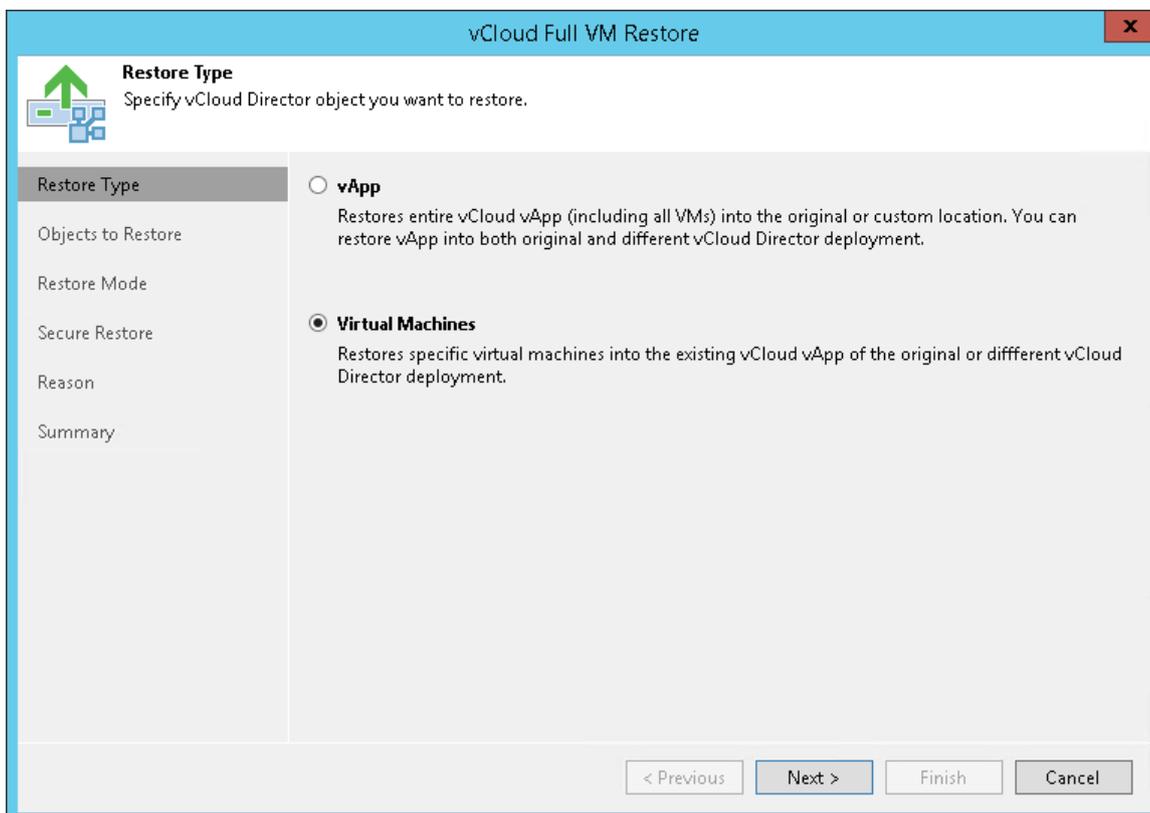
When restoring VMs to the vCloud Director hierarchy, make sure that you select the **Restore into vCloud vApp** option. If you select the **Restore into vSphere infrastructure** option, the VM will be restored at the level of the underlying vCenter Server. To get a fully functional VM managed by vCloud Director, you will need to manually import the restored VM to the vCloud Director hierarchy.

To restore a VM to the vCloud Director hierarchy, use the **vCloud Full VM Restore** wizard.

Step 1. Launch vCloud Full VM Restore Wizard

To launch the **vCloud Full VM Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware vCloud Director**. At the **Restore Type** step of the wizard, select the object you would like to restore: *Virtual Machines*.
- Open the **Home** view. In the inventory pane, select **Backups**. In the working area, expand the necessary backup and do one of the following:
 - Select the VM you want to restore and click **Entire VM > Into vCloud vApp** on the ribbon.
 - Right-click the VM you want to restore and select **Restore entire VM > Into vCloud vApp**.
- Open the **Inventory** view. On the **View** tab, click **vCloud View**. In the inventory pane, expand the vCloud Director hierarchy. In the working area, right-click the VM you want to restore and select **Restore > Restore Entire VM > Into vCloud vApp**.



Step 2. Select VMs to Restore

At the **Objects to Restore** step of the wizard, select one or several VMs to restore.

To add a VM, click **Add VM** and select where to browse for VMs:

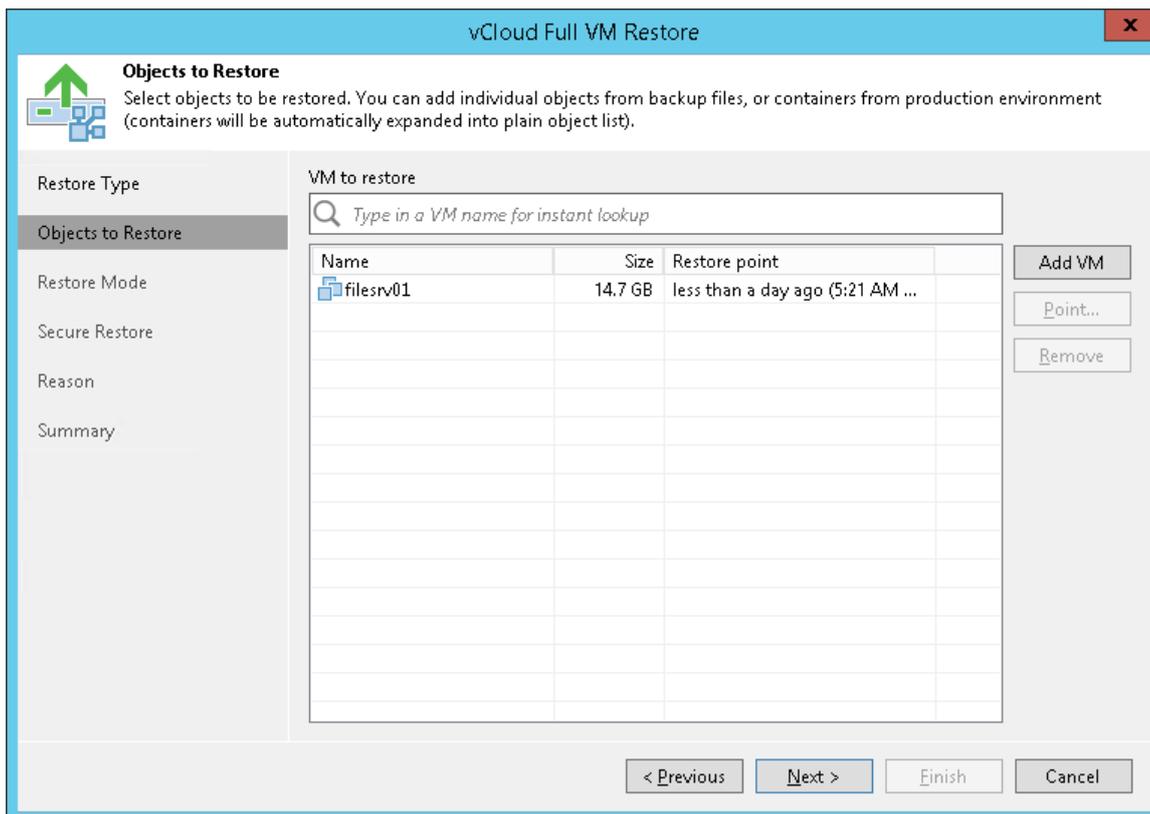
- **From infrastructure** – browse the vCloud Director hierarchy and select VMs to restore. Note that the VM you select from the vCloud Director hierarchy must be successfully backed up at least once.
- **From backup** – browse existing backups and select VMs under backup jobs.

To facilitate selection, use the search field at the bottom of the **Select VMs** window: enter an object's name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

To add VMs to the list, you can also use the search field at the top of the window:

1. Enter a VM name or a part of it in the search field and Veeam Backup & Replication will search existing backups for the specified VM and display matching results.
2. To add the VM to the list, double-click it in the list of search results.
3. If the necessary VM is not found, click the **Show more** link to browse existing backups and choose the necessary VM.

To remove a VM from the list, select it and click **Remove** on the right.



Step 3. Select Restore Point

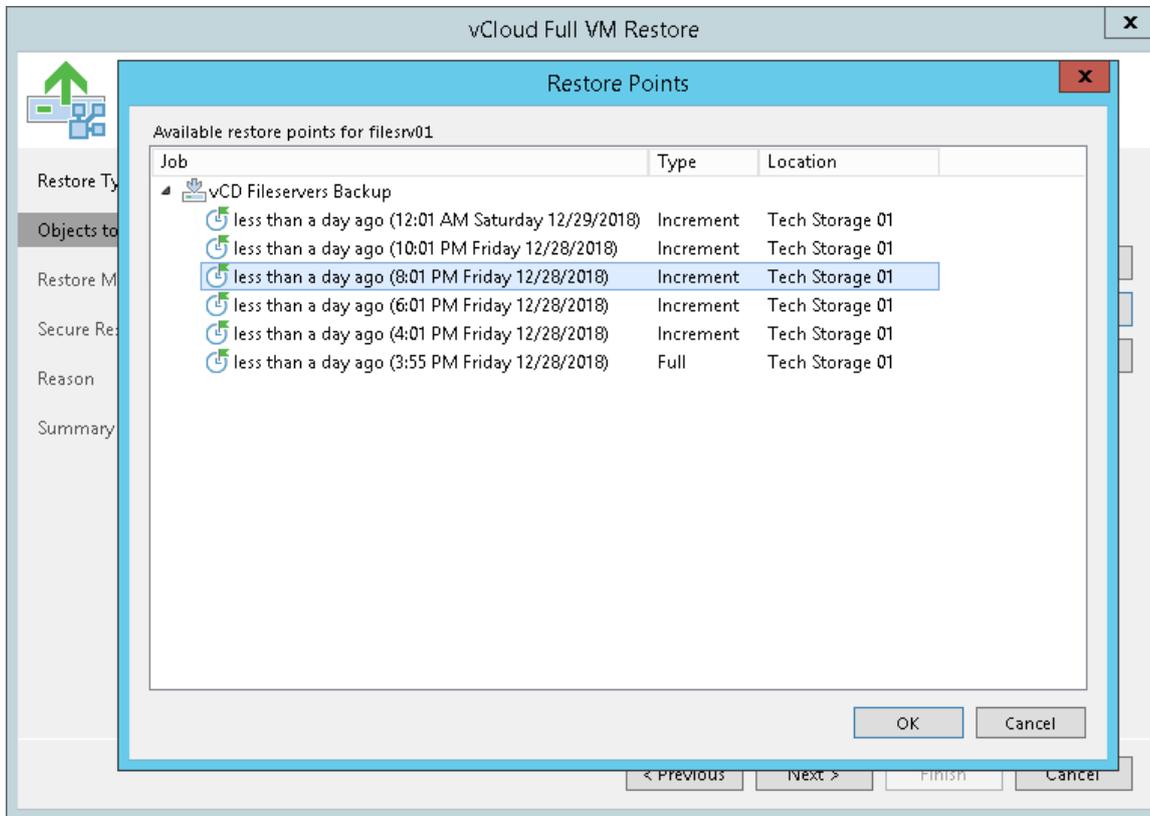
You can select the restore point for the VM.

By default, Veeam Backup & Replication uses the latest valid restore point to recover a VM. However, you can restore a VM to an earlier state. If you have chosen to restore multiple VMs, you can select a different restore point for every VM specifically.

To select a restore point for a VM:

1. Select a VM in the list and click **Point** on the right.
2. In the **Restore Points** window, select the restore point that must be used to recover the VM.

In the **Location** column, you can view a name of a backup repository where a restore point resides.



Step 4. Select Restore Mode

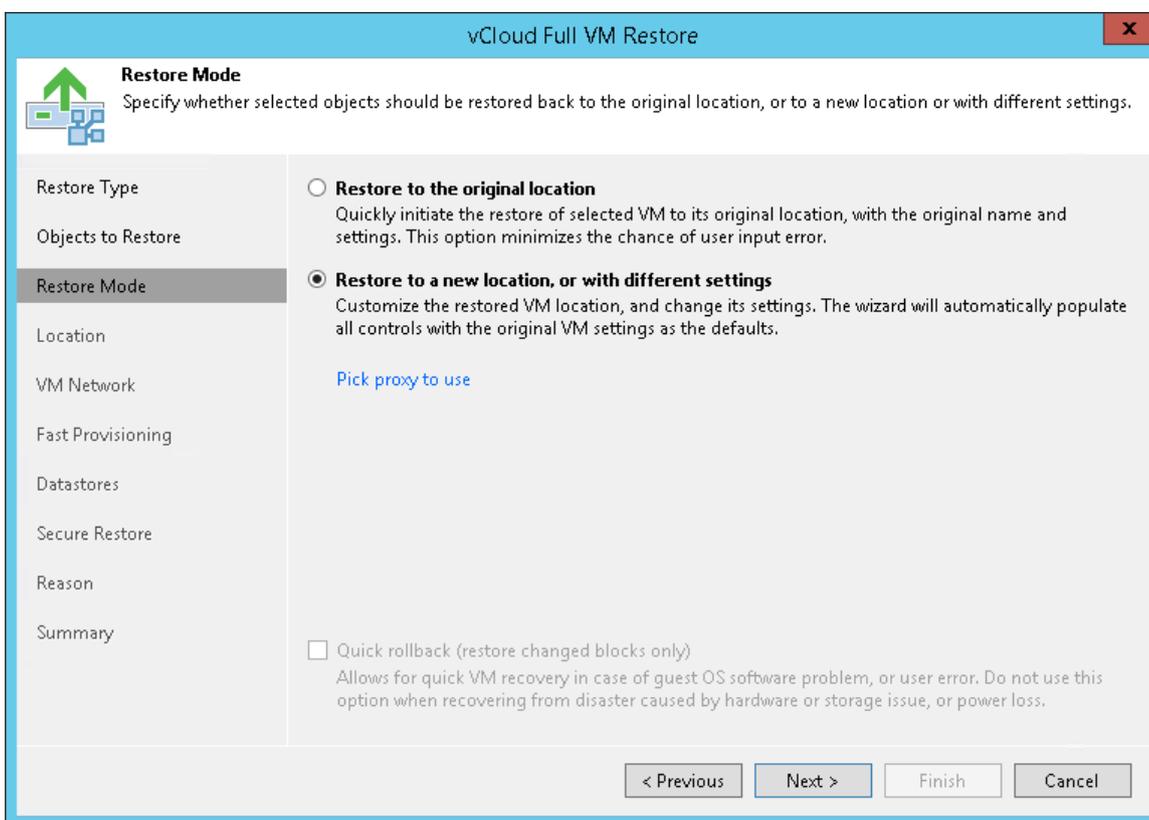
At the **Restore Mode** step of the wizard, choose the necessary restore mode and backup proxy for VM data transport:

1. Choose a restore mode:
 - Select **Restore to original location** if you want to restore the VMs 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 VMs 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 VMs. Veeam Backup & Replication will use CBT to get data blocks that are necessary to revert the VMs 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 VMs 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.

3. Click the **Pick proxy to use** link to select backup proxies over which VM data must be transported to the source datastore. You can assign backup proxies explicitly or instruct Veeam Backup & Replication to automatically select backup proxies.
 - If you choose **Automatic selection**, Veeam Backup & Replication will detect backup proxies that are connected to the source datastore and will automatically assign optimal proxy resources for processing VM data.

During the restore process, VMs are processed simultaneously. Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use for writing data to target, current workload on these backup proxies, and selects the most appropriate resources for VMs processing.
 - If you choose **Use the selected backup proxy servers only**, you can explicitly select backup proxies that will be used for restore. It is recommended that you select at least two proxies to ensure that VMs are recovered should one of backup proxies fail or lose its connectivity to the source datastore during restore.



Step 5. Select VM Location

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

By default, Veeam Backup & Replication 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.

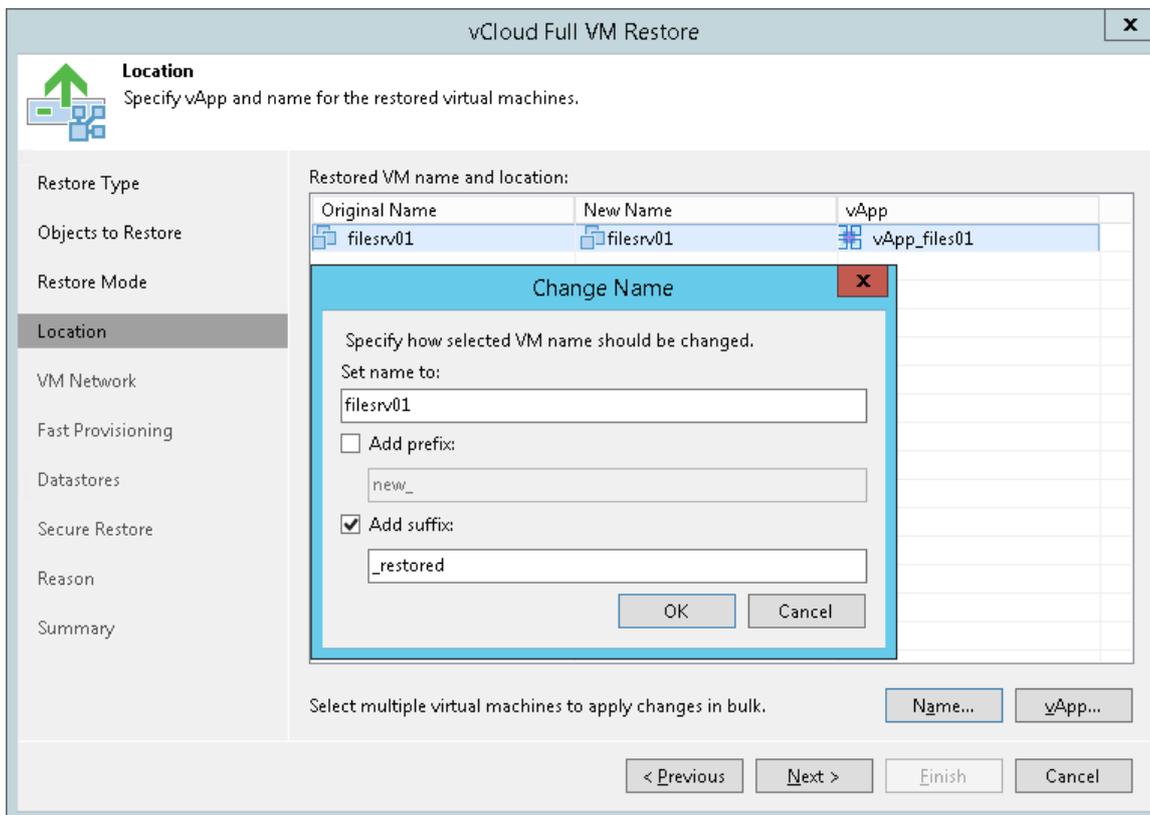
To facilitate selection, use the search field at the bottom of the window: enter the vApp name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

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 & Replication will restore the VM as a regular VM.



Step 6. Select Destination Network

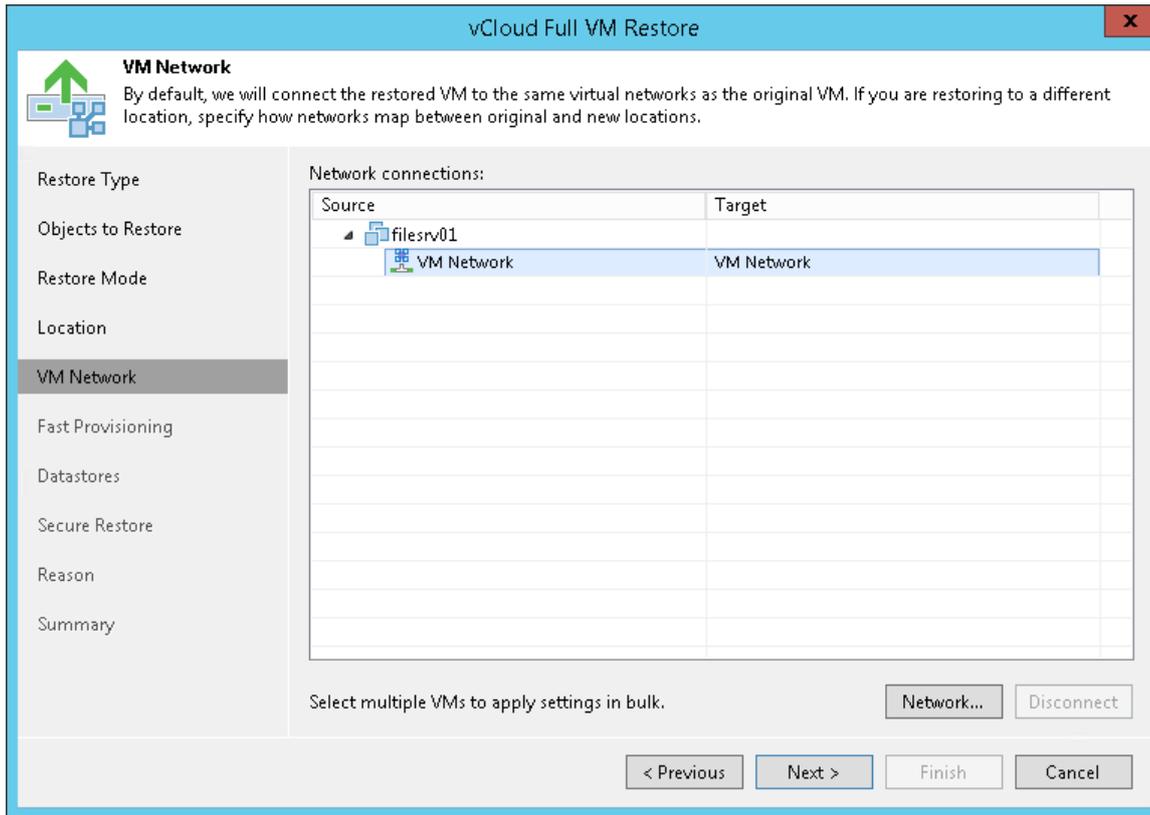
The **VM Network** step of the wizard is available if you have chosen to change the location and settings of the restored VMs.

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 7. Select Template to Link

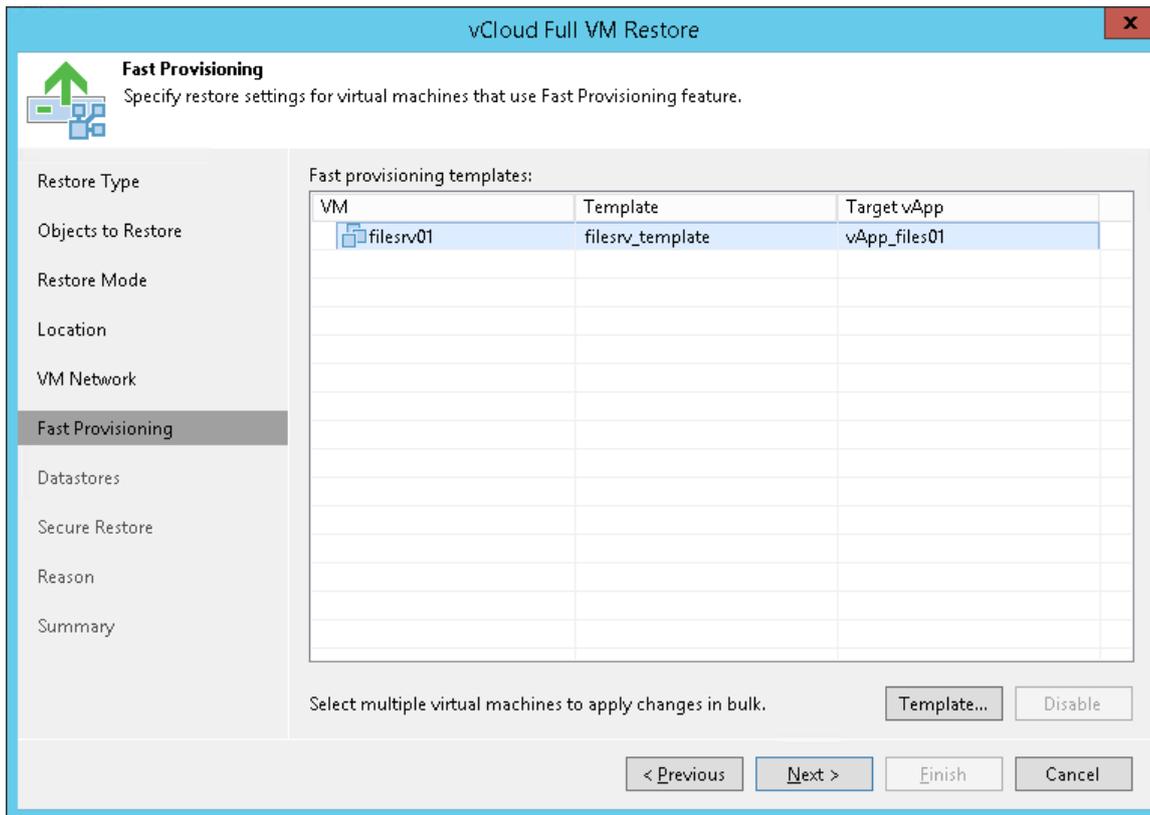
The **Fast Provisioning** step of the wizard is available if you have chosen to change the settings of the restored VMs.

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**.



Step 8. Select Storage Policy and Datastores

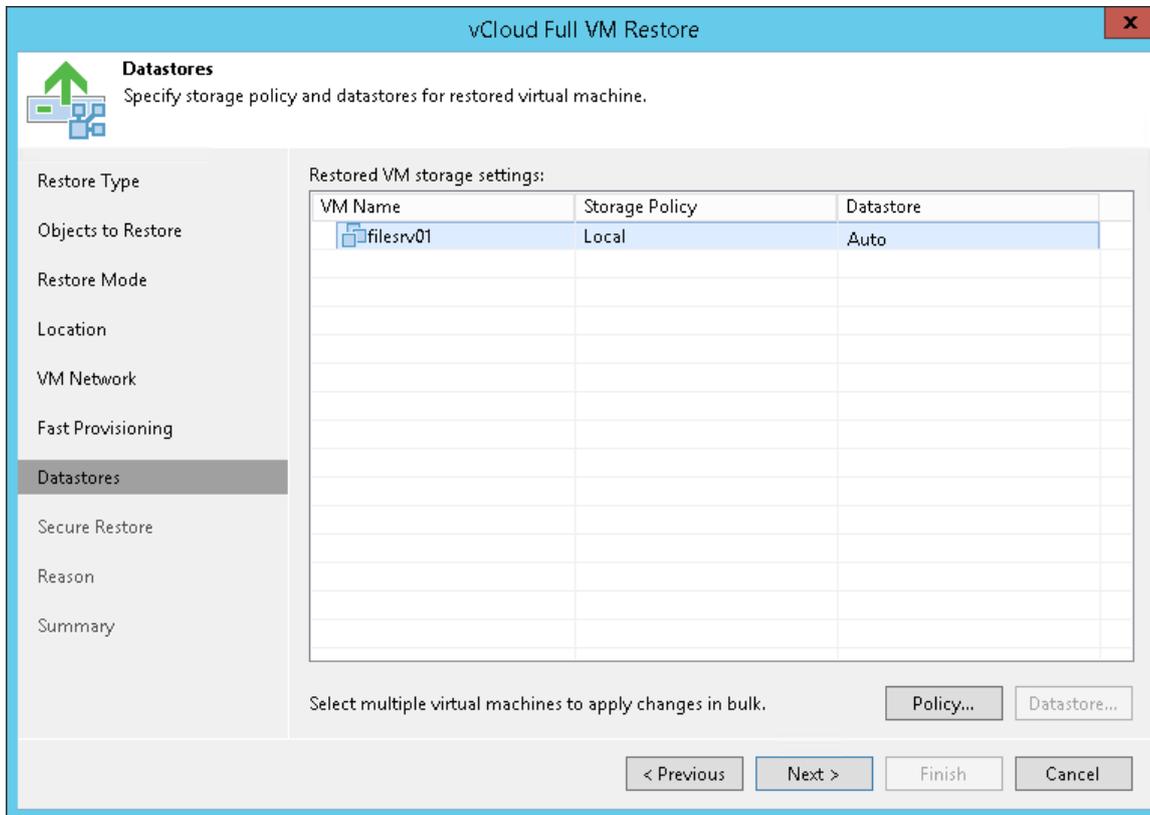
The **Datastores** step of the wizard is available if you have chosen to change the settings of the restored VMs.

To select a storage policy for the restored VM:

1. Select a VM in the list and click **Policy**.
2. In the displayed window, select the necessary policy 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.



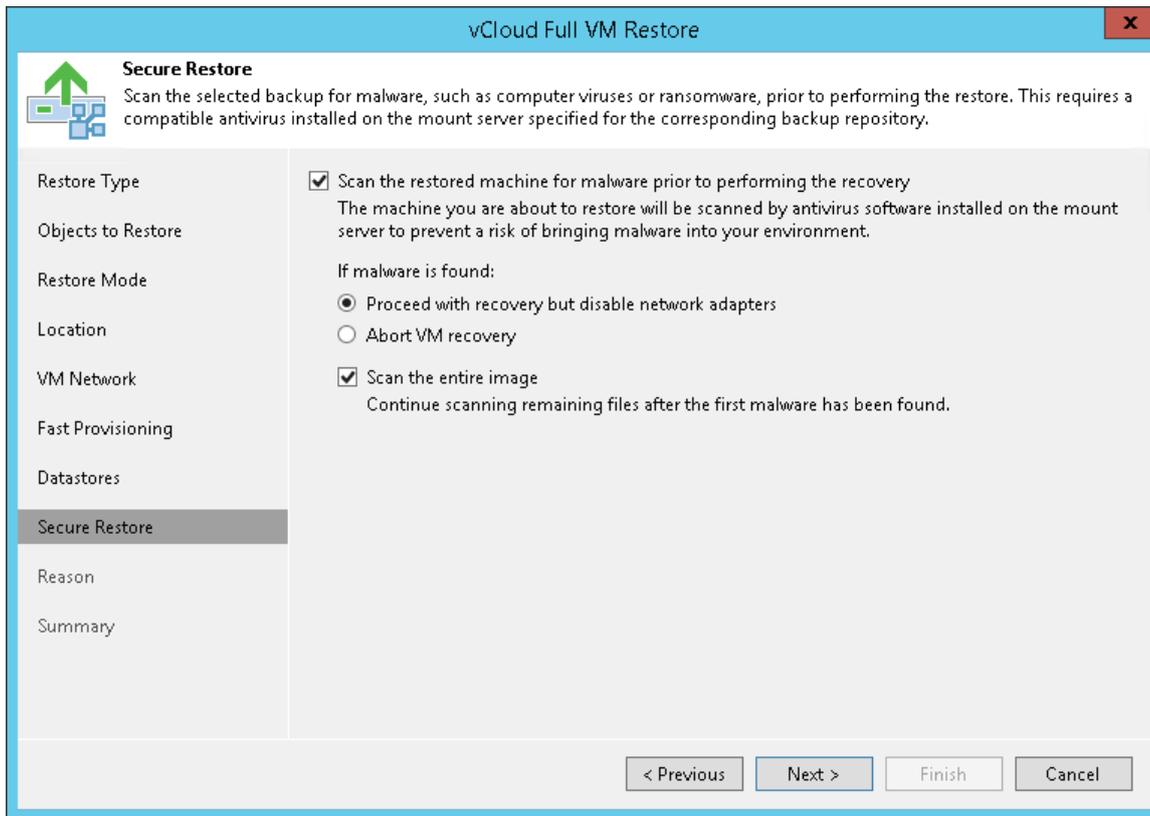
Step 9. Specify Secure Restore Settings

You can instruct Veeam Backup & Replication to perform secure restore – scan VM data with antivirus software before restoring the VM into a vApp. For more information on secure restore, see [Secure Restore](#).

To specify secure restore settings:

1. At the **Secure Restore** step of the wizard, select the **Scan the restored machine for malware prior to performing the recovery** check box.
2. Select which action Veeam Backup & Replication will take if the antivirus finds a virus threat:
 - **Proceed with recovery but disable network adapters.** Select this action if you want to restore the VM with disabled network adapters (NICs).
 - **Abort VM recovery.** Select this action if you want to cancel the restore session.

3. Select the **Scan the entire image** check box if you want the antivirus to continue the VM data scan after the first malware is found. For information on how to view results of the malware scan, see [Viewing Malware Scan Results](#).

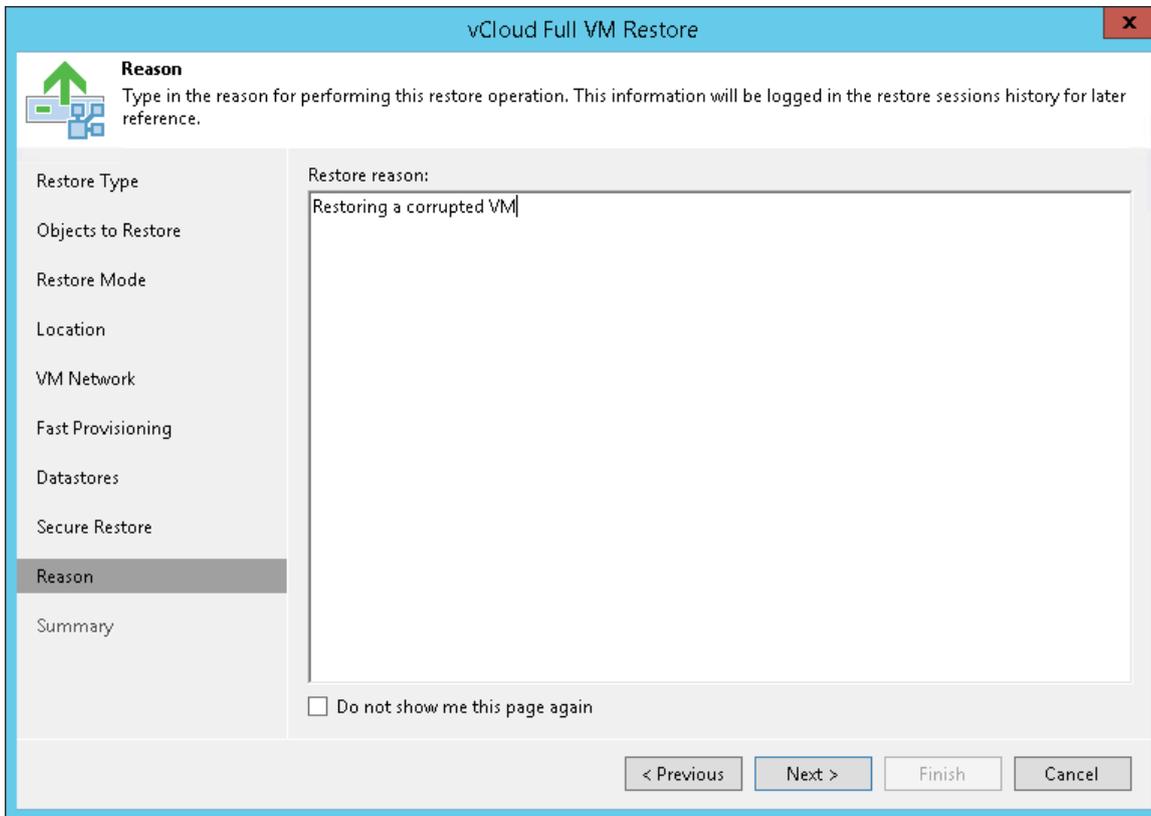


Step 10. Specify Restore Reason

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.



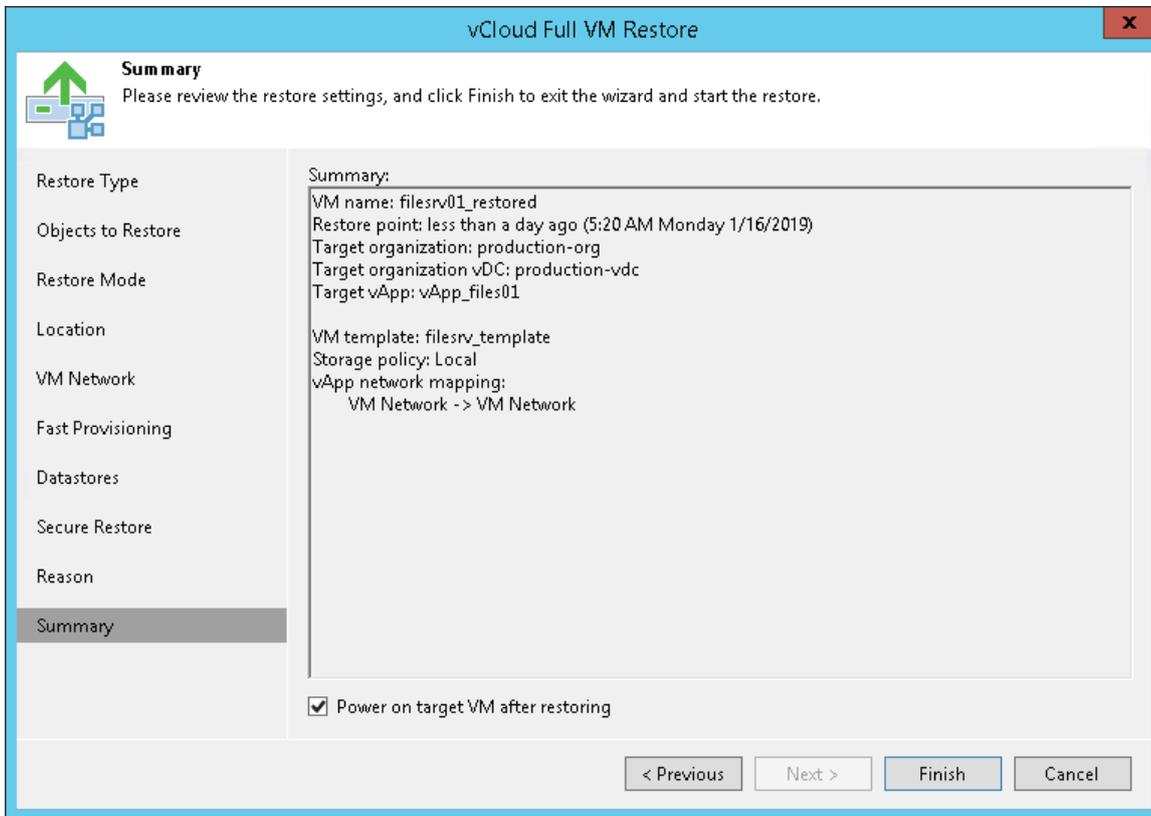
Step 11. Verify Recovery Settings and Finish Working with Wizard

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

1. If you want to start the restored VMs, select the **Power on VM after restoring** check box.
2. Check the settings for VMs restore and click **Finish**. Veeam Backup & Replication will recover the VMs in the specified destination.

NOTE:

Veeam Backup & Replication checks the lease term for the restored VMs. In case the lease period has expired, the lease will be automatically updated.



Restoring Entire VMs into vSphere Infrastructure

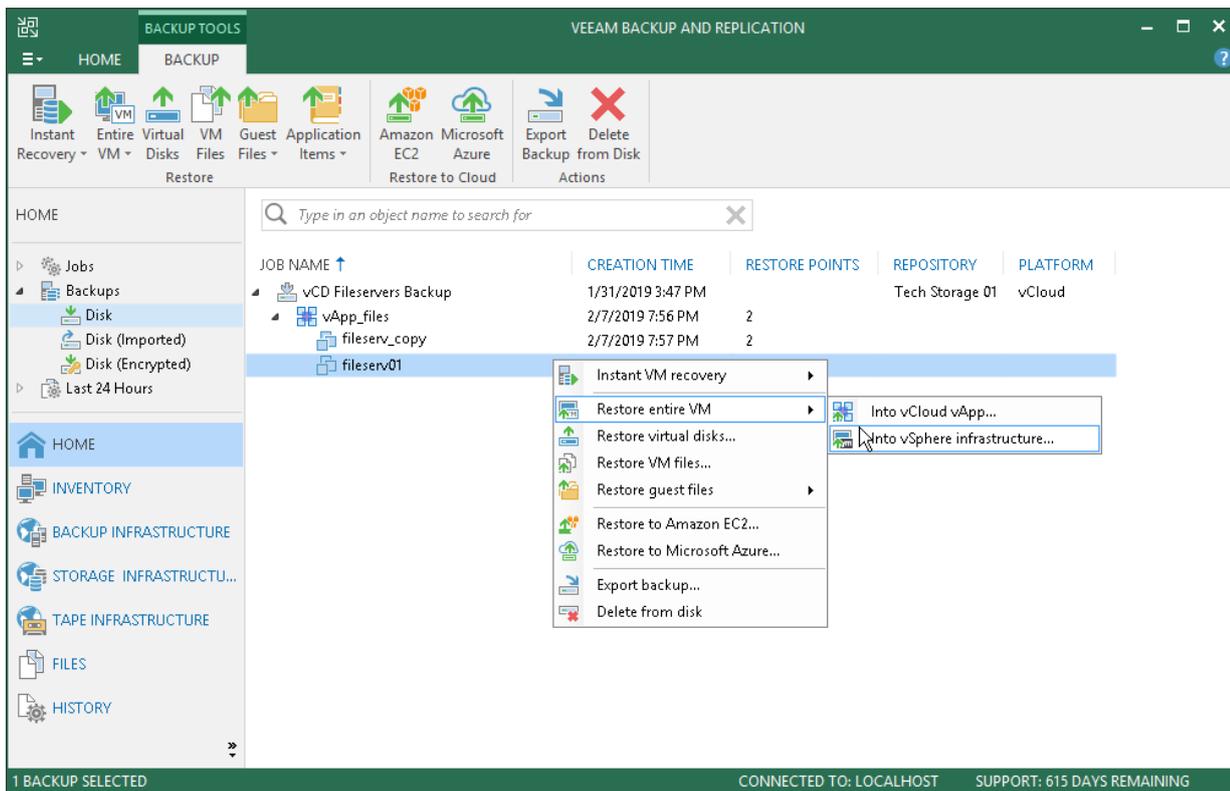
You can restore vCD VMs from the backup to the VMware vSphere infrastructure.

During restore, Veeam Backup & Replication neglects the vApp metadata saved to the backup file and performs a regular entire VM restore process. The VM is restored to the vCenter Server or ESX(i) host and is not registered in VMware vCloud Director. vCloud-specific features such as fast provisioning are not supported for such type of restore.

To launch the **Full VM Restore** wizard, do one of the following:

- Open the **Home** view, in the inventory pane select **Backups**. In the working area, expand the necessary backup, select the VMs you want to restore and click **Entire VM > Into vSphere infrastructure** on the ribbon.
- Open the **Inventory** view. In the inventory pane, expand the VMware vCloud Director hierarchy and select the vCenter Server. In the working area, right-click the VM you want to restore and select **Restore entire VM > Into vSphere infrastructure**.

Entire VM restore of vCD VMs does not differ from entire VM restore of regular VMware VMs. For more information, see [Performing Entire 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 Virtual Disks](#).

Restoring VM Guest OS Files

The process of VM guest files restore for vCD VMs does not differ from that for regular VMware VMs. For more information, see [Restoring VM Guest OS Files \(FAT, NTFS or ReFS\)](#) and [Restoring VM Guest OS Files \(Multi-OS\)](#).

VMware Cloud on AWS Support

Veeam provides support for VMware Cloud on AWS. With Veeam Backup & Replication, you can administrate backup, replication and restore operations in VMware Cloud on AWS environments.

Deployment

To perform data protection and disaster recovery tasks in VMware Cloud on AWS, consider the following recommendations and requirements on the backup infrastructure deployment:

- **Backup Server:** it is recommended to deploy Veeam backup server in the VMware Cloud on AWS environment. The machine must run Microsoft Windows.
- **Backup Proxy:** you must deploy a backup proxy in the VMware Cloud on AWS environment. The machine must run Microsoft Windows. You can assign the role of the backup proxy to a dedicated VM or to the backup server.

To provide sufficient resources, deploy at least one backup proxy per each SDDC cluster in the VMware Cloud on AWS. This is required for VMware Cloud on AWS specific Hot-Add processing.

- **Backup Repository:** it is recommended to use a backup repository created outside of the VMware Cloud on AWS environment, for example, on the Amazon EC2 server. This type of deployment allows for efficient data transfer over the fast ENI connection used by VMware to communicate with Amazon AWS.

Alternatively, you can store backups on a Veeam backup repository in the on-premises VMware environment or use Veeam Cloud Connect to transfer backups to the cloud. Note that in this scenario you may be charged additional fee for the traffic from VMware Cloud on AWS to the internet.

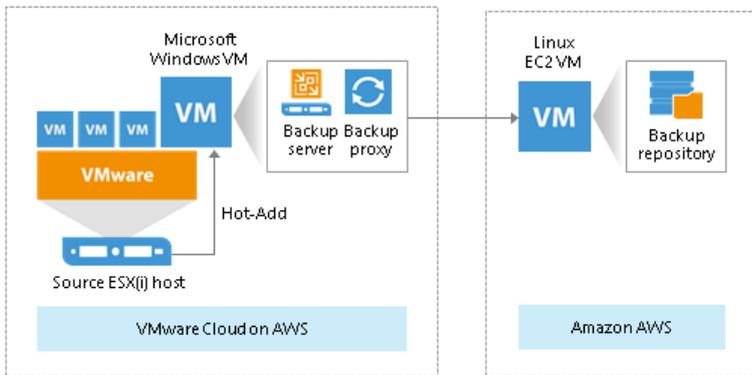
To add VMware Cloud on AWS to the backup infrastructure, follow the same steps as described in the [Adding VMware vSphere Servers](#) section.

Simple Deployment

Simple deployment is preferable for VMware Cloud on AWS environments with low traffic load. Per this deployment type, you can install the backup server and the backup proxy on the same VM.

In a simple VMware Cloud on AWS deployment the backup infrastructure includes the following components:

- Source ESX(i) host
- Veeam backup server
- Veeam backup proxy
- Veeam backup repository: a Linux-based EC2 VM in Amazon AWS

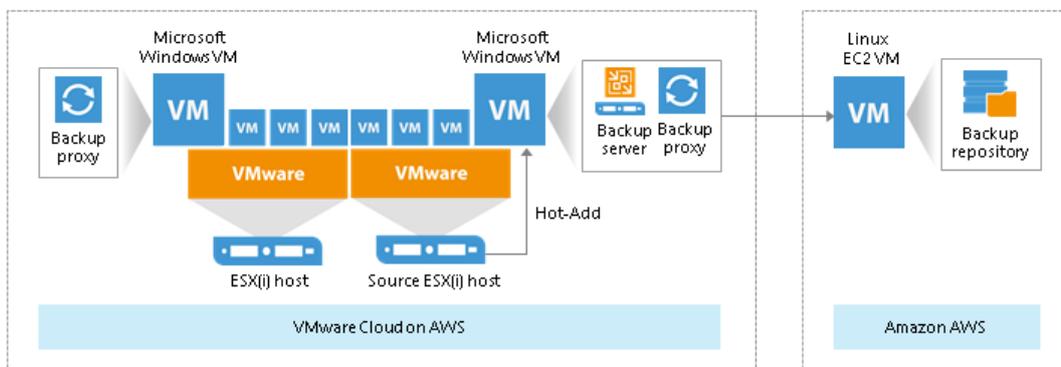


Advanced Deployment

Advanced deployment is intended for large-scale VMware Cloud on AWS environments with a large number of backup and replication jobs. Per this deployment type, it is recommended to install several backup proxies on dedicated VMs to move the workload from the backup server.

In an advanced VMware Cloud on AWS deployment the backup infrastructure includes the following components:

- Source ESX(i) host
- Veeam backup server
- Several Veeam backup proxies for better performance and workload distribution
- Veeam backup repository: a Linux-based EC2 VM in Amazon AWS



To increase scalability and optimize performance in an advanced deployment, follow the recommendations below:

- Deploy additional backup proxies.
- Scale accordingly CPU and RAM resources of the EC2 VM used as a backup repository. Make sure it has enough free space for storing backups.

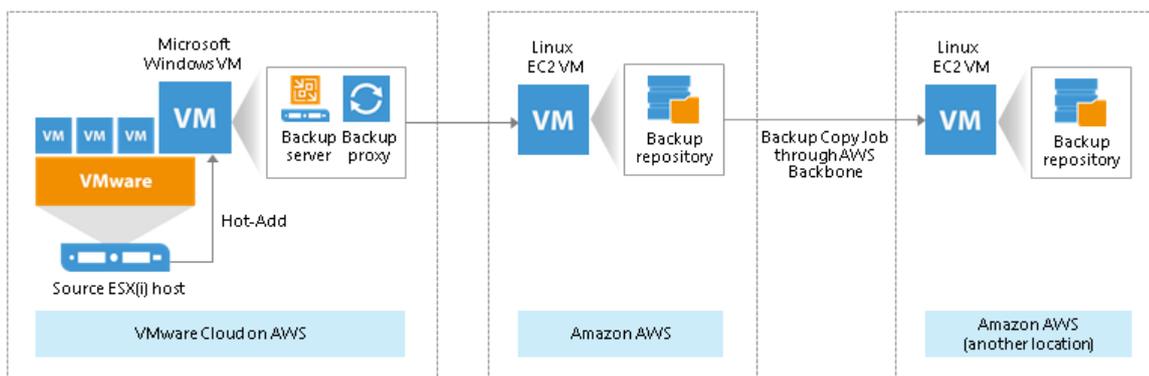
Deployment Scenarios for Offsite Backup

To keep up with the 3-2-1 backup rule, it is recommended that you have a copy of your backups in an offsite location. To transfer your backups offsite, you can leverage Veeam backup copy.

Mind that transferring backups over the Internet may require paying additional fees. As a cost-effective alternative, you can store backups in a different Amazon AWS geographical location. In this case, backup copies are transferred through the AWS backbone. Using such AWS network solution provides data transfer at lower latency and cost when compared to the public Internet.

To perform backup copy to a different Amazon AWS location, the backup infrastructure must contain the following components:

- Source ESX(i) host
- Veeam backup server
- Veeam backup proxy
- Veeam backup repository: a Linux-based EC2 VM in Amazon AWS
- Veeam backup repository for backup copy: a Linux-based EC2 VM in another Amazon AWS location



TIP:

As an offsite backup solution, you can copy backups to virtual tapes and store them in Amazon S3/Glacier cloud storage. In this case, AWS Storage Gateway performs the role of a Virtual Tape Library (VTL).

Considerations, Limitations and Troubleshooting

Some of VMware features and permissions are not granted by default at the start of VMware Cloud on AWS. For details, see <https://www.veeam.com/kb2414>.

WAN Acceleration

Offsite backup and replication always involves moving large volumes of data between remote sites. The most common problems that backup administrators encounter during offsite backup and replication are:

- Insufficient network bandwidth to support VM data traffic
- Transmission of redundant data

To solve these problems, Veeam Backup & Replication offers the WAN acceleration technology that helps optimize data transfer over WAN. Veeam WAN acceleration is a built-in feature and does not add complexity and cost to the backup infrastructure.

The WAN acceleration technology is specific for remote jobs: backup copy jobs and replication jobs.

NOTE:

WAN acceleration is available in specific editions of Veeam Backup & Replication. For more information, see [Editions Comparison](#).

Global Data Deduplication

The goal of WAN acceleration is to send less data over the network. To reduce the amount of data going over WAN, Veeam Backup & Replication uses the global data deduplication mechanism.

1. When you first run a remote job, Veeam Backup & Replication analyzes data blocks going over WAN.
2. With every new cycle of a remote job, Veeam Backup & Replication uses the data redundancy algorithm to find duplicate data blocks in copied files. Veeam Backup & Replication analyzes data blocks in files on the source side and compares them with those that have been previously transferred over WAN. If an identical data block is found, Veeam Backup & Replication deduplicates it.

Veeam Backup & Replication uses three sources for data deduplication:

- VM disks. Veeam Backup & Replication analyses data blocks within the same VM disk. If identical blocks are found, duplicates are eliminated.
For example, in case of a virtualized Microsoft Exchange server, the same email is typically stored in sender's Outbox folder and recipient's Inbox folder, which results in duplicate data blocks. When a remote job runs, Veeam Backup & Replication detects such VM data blocks and performs deduplication.
- Previous restore points for the processed VM on the target repository. Veeam Backup & Replication analyses data in the restore point that is about to be copied and the restore points that are already stored on the target side. If an identical block is found on the target side, Veeam Backup & Replication eliminates the redundant data block in the copied restore point.
- Global cache. Veeam Backup & Replication creates a global cache holding data blocks that repeatedly go over WAN. In a new job session, Veeam Backup & Replication analyzes data blocks to be sent and compares them with data blocks stored in the global cache. If an identical data block is already available in the global cache, its duplicate on the source side is eliminated and not sent over WAN.

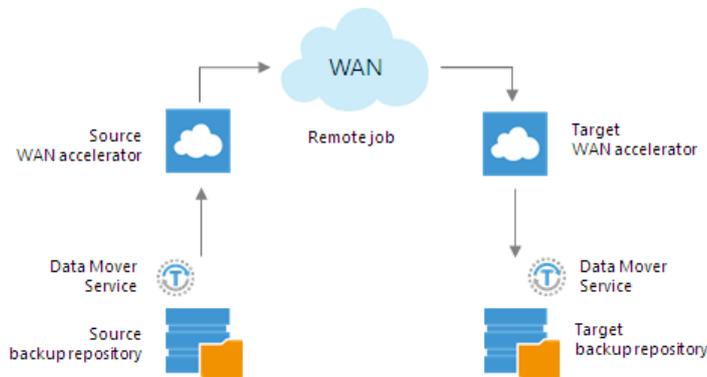
As a result, only unique data blocks go over WAN. Data blocks that have already been sent are not sent. This way, Veeam Backup & Replication eliminates transfer of redundant data over WAN.

NOTE:

Veeam Backup & Replication deduplicates data blocks within one VM disk and in restore points for one VM only. Deduplication between VM disks and restore points of different VMs is performed indirectly, via the global cache. For more information, see [WAN Global Cache](#).

WAN Accelerators

For WAN acceleration, Veeam Backup & Replication uses dedicated components – WAN accelerators. WAN accelerators are responsible for global data caching and data deduplication. Technically, WAN accelerators add a new layer in the backup infrastructure – between the Veeam Data Movers on the source side and the Veeam Data Mover on the target side.



WAN Accelerators Deployment

To enable WAN acceleration and data deduplication technologies, you must deploy a pair of WAN accelerators in your backup infrastructure.

- One WAN accelerator is deployed on the source site, closer to the source backup repository or source host.
- The other WAN accelerator is deployed on the target site, closer to the target backup repository or target host.

On each WAN accelerator Veeam Backup & Replication creates the `VeeamWAN` folder containing the following data:

- The `VeeamWAN` folder on the source WAN accelerator stores files with digests required for global deduplication. For more information, see [How WAN Acceleration Works](#).
- The `VeeamWAN` folder on the target WAN accelerator stores global cache data.

To create a WAN accelerator, you need to assign the WAN accelerator role to a specific machine. You can even assign the WAN accelerator role to the existing backup proxies and backup repositories.

WAN Accelerators Services

On each WAN accelerator, Veeam Backup & Replication installs the Veeam WAN Accelerator Service responsible for WAN acceleration tasks.

Requirements for WAN Accelerators

A machine performing the role of a WAN accelerator must meet the following requirements:

- The machine must meet the system requirements. For more information, see [System Requirements](#).
- The WAN accelerator can run on a physical or virtual machine.
- The WAN accelerator can run on a 64-bit Windows-based machine.

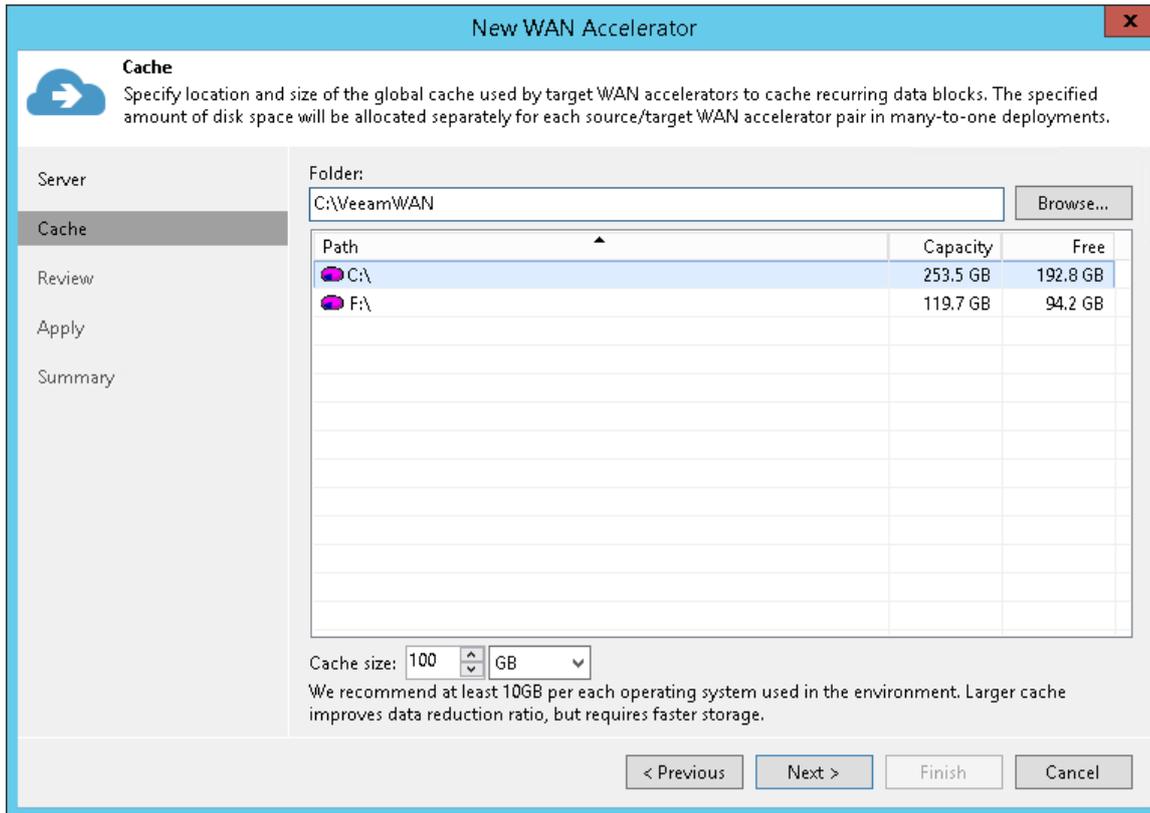
- You must add the machine to the Veeam Backup & Replication console as a managed server.
- The machine must have enough free disk space to store digests or global cache data. For more information, see [WAN Accelerator Sizing](#).

WAN Accelerator Sizing

To ensure correct work of remote jobs over WAN accelerators, you must provide enough free space for service data on source and target WAN accelerators.

Source WAN Accelerator

When you run a remote job over WAN accelerators, Veeam Backup & Replication analyses data blocks going to target and calculates digests for these data blocks. Digests data is stored on the source WAN accelerator, in the VeeamWAN folder on the disk that you select when you configure the WAN accelerator.



You must make sure that there is enough disk space on the source WAN accelerator to store digest data. The amount of required space is calculated by the following formula:

$$\text{Digest Size} = 5\% \text{ of Provisioned VM Size}$$

For example, if you plan to process 10 VMs whose provisioned size is 2 TB, you must allocate 100 GB of disk space for digest data on the source WAN accelerator.

Target WAN Accelerator

You must make sure that you provide enough free space to store the following data on the target WAN accelerator:

- [Global cache data](#)
- [Digest data](#)

Digest Data

In some cases, Veeam Backup & Replication may require more space on the target WAN accelerator than specified in the WAN accelerator properties. This can happen if digest data on the source WAN accelerator are missing or cannot be used. For example:

- You have performed the **Clear Cache** operation on the source WAN accelerator and it no longer contains digest data. For more information, see [Clearing Global Cache](#).
- Veeam Backup & Replication has attempted to resume operation of backup data transfer but the backup file was not prepared for the operation in a proper way. The digest data must be re-calculated.

In such situations, the target WAN accelerator will have to calculate digest data on its own, which will require additional space.

For safety reasons, it is recommended that you provide the following amount of space for digest data on the target WAN accelerator:

```
Digest Size = 2% of Provisioned VM Size
```

This amount of space is required for digest data recalculation. If you do not provide this amount of space and a situation when Veeam Backup & Replication needs to recalculate digest data occurs, the remote job will work in the limited mode. Veeam Backup & Replication will not deduplicate data against the previous restore points copied to target. For more information, see [Global Data Deduplication](#).

IMPORTANT!

When you specify the global cache size for a target WAN accelerator, you do not allocate any space for storing digest data. To let Veeam Backup & Replication recalculate digest data, you must make sure that necessary amount of free space is available on the target WAN accelerator (in addition to the space allocated for the global cache).

For example:

- You have allocated 100 GB for global cache on the target WAN accelerator.
- Provisioned size of VMs to be processed is 2 TB.

In this case, the needed amount of free disk space for the global cache on the target WAN accelerator is:

```
100 GB + 40 GB = 140 GB
```

Many-to-One WAN Acceleration Scenario

Global cache size is calculated per 1 source WAN accelerator working with the target WAN accelerator. If you plan to use several source WAN accelerators with 1 target WAN accelerator, you must increase the size of the global cache proportionally. The cache data for every source WAN accelerator will be stored in a dedicated subfolder in the global cache folder of the target WAN accelerator. The global cache size is calculated by the following formula:

```
Total Global Cache Size = (# of Source WAN Accelerators) * (Size of Global Cache Configured in Target WAN Accelerator Properties) + Digest Size
```

For example:

- You have 4 source WAN accelerators in the source side working with 1 target WAN accelerator in the DR site.
- The global cache size configured in properties of the target WAN accelerator is 100 GB.
- The size of VMs to be processed is 2 TB.

In this case, the needed amount of free disk space for the global cache on the target WAN accelerator is:

$$4 * 100 \text{ GB} + 40 \text{ GB} = 440 \text{ GB}$$

NOTE:

For more information and recommendations on WAN accelerator cache sizing, see the [Veeam KB1877](#) article.

Adding WAN Accelerators

To add a WAN accelerator, you must assign the WAN accelerator role to a Microsoft Windows server added to the backup infrastructure.

You must deploy a pair of WAN accelerators: one WAN accelerator on each side of the WAN link.

Before adding a WAN accelerator, [check prerequisites](#). Then use the **New WAN Accelerator** wizard to add a WAN accelerator.

Before You Begin

Before you add a WAN accelerator, check the following prerequisites:

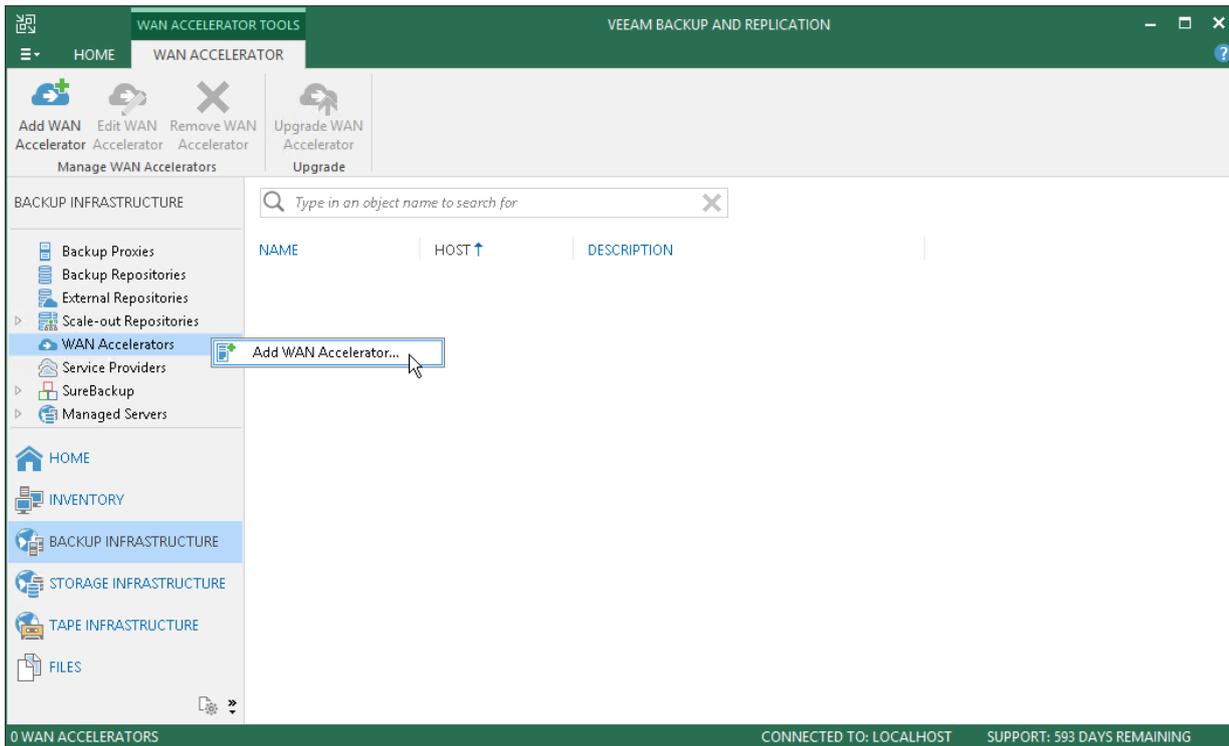
- You must assign the WAN accelerator role to a Microsoft Windows server (physical or virtual). The WAN accelerator role can be assigned to backup proxies and Microsoft Windows backup repositories configured in the backup infrastructure.
- You must use 64-bit Microsoft Windows machines as WAN accelerators. Veeam Backup & Replication does not support 32-bit versions of Microsoft Windows used as WAN accelerators.
- WAN acceleration operations are resource-consuming. When assigning the WAN accelerator role, mind available CPU and memory resources of the Microsoft Windows server. It is recommended that you assign the WAN accelerator role to servers with 8 GB RAM and more. Otherwise, the WAN acceleration process may fail.

Step 1. Launch New WAN Accelerator Wizard

To launch the **New WAN Accelerator** wizard, either one of the following:

- Open the **Backup Infrastructure** view, in the inventory pane select **WAN Accelerators** and click **Add WAN Accelerator** on the ribbon.

- Open the **Backup Infrastructure** view, in the inventory pane right-click **WAN Accelerators** and select **Add WAN Accelerator**.



Step 2. Choose Server

At the **Server** step of the wizard, select a Microsoft Windows server that you plan to use as a WAN accelerator and define port and connection settings for this server.

1. From the **Choose server** list, select a Microsoft Windows server added to the backup infrastructure. If the server is not added to the backup infrastructure yet, you can click **Add New** to open the **New Windows Server** wizard. For more information, see [Adding Microsoft Windows Servers](#).
2. In the **Description** field, provide a description for future reference.
It is recommended that you describe the added WAN accelerator as the source or target one. When you create a remote job, this hint will be displayed in brackets next to the WAN accelerator name, which will help you choose the necessary WAN accelerator to be used on the source or target side.
3. In the **Traffic port** field, specify the number of the port over which WAN accelerators must communicate with each other. By default, port 6165 is used.
4. In the **Streams** field, specify the number of connections that must be used to transmit data between WAN accelerators. By default, 5 connections are used.

This setting applies only to the source WAN accelerator. The greater is the number of streams, the more bandwidth resources Veeam Backup & Replication will use. A great number of streams engage more CPU and memory resources of the source WAN accelerator.

The screenshot shows the 'New WAN Accelerator' wizard window. The title bar reads 'New WAN Accelerator'. The main heading is 'Server'. Below the heading, there is a sub-heading 'Server' and a description: 'Choose a server to install WAN accelerator components on. You can only select between 64-bit Microsoft Windows servers added to the managed servers tree in the console.' On the left side, there is a navigation pane with the following items: 'Server' (selected), 'Cache', 'Review', 'Apply', and 'Summary'. The main area contains the following fields and controls:

- 'Choose server:' dropdown menu with 'apache08.tech.local' selected and an 'Add New...' button.
- 'Description:' text box containing 'Source WAN Accelerator'.
- 'Traffic port:' spinner box set to '6165' with a note: 'TCP/IP port to use for data transfer. Ensure this port is open in any firewall between sites.'
- 'Streams:' spinner box set to '5' with a note: 'Using multiple upload streams helps to fully saturate WAN links.'

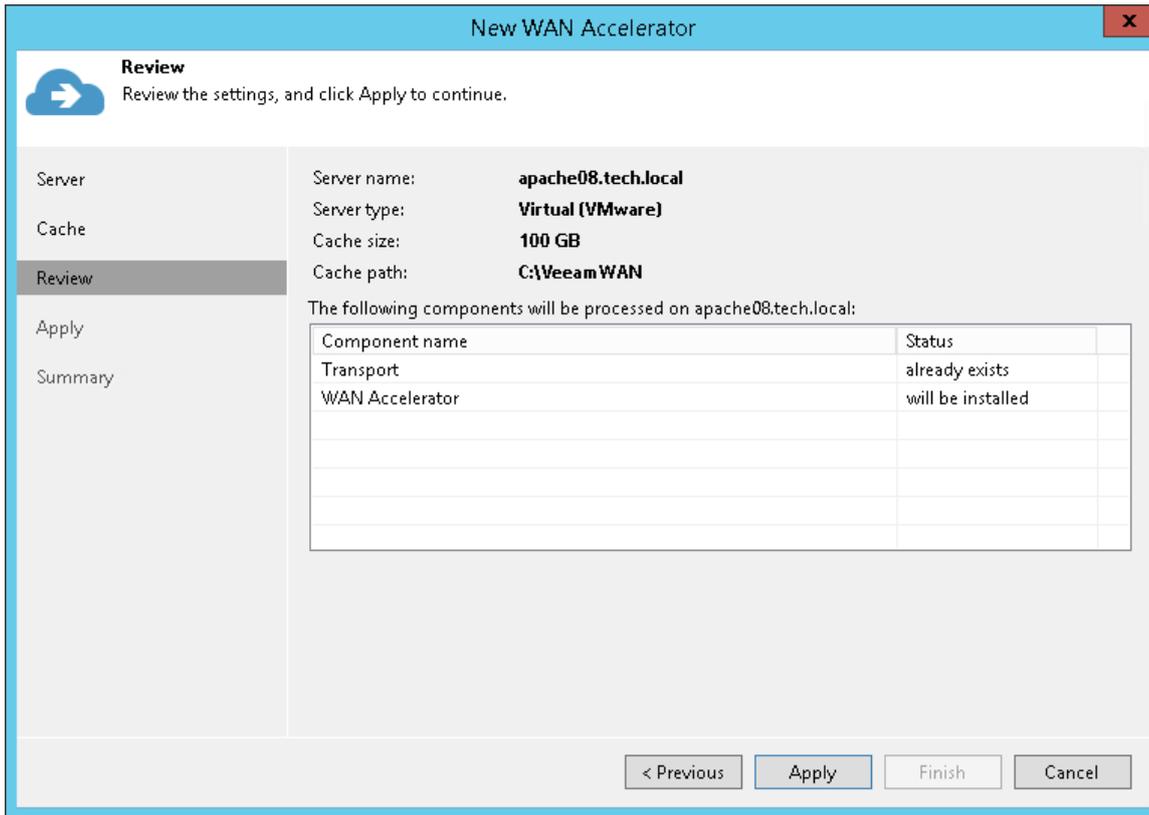
At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

Step 3. Define Cache Location and Size

At the **Cache** step of the wizard, define settings for the folder where service files and global cache data will be stored.

1. In the **Folder** field, specify a path to the folder in which service files (for source and target WAN accelerators) and global cache data (for target WAN accelerator) must be stored. When selecting a folder on the target WAN accelerator, make sure that there is enough space for storing global cache data.
2. [For target WAN accelerator] In the **Cache size** field, specify the size for the global cache. The global cache size is specified per source WAN accelerator. If you plan to use one target WAN accelerator with several source WAN accelerators, the specified amount of space will be allocated to every source WAN accelerator and the size of the global cache will increase proportionally. For more information, see [WAN Accelerator Sizing](#).

2. Click **Next** to install the components on the server.

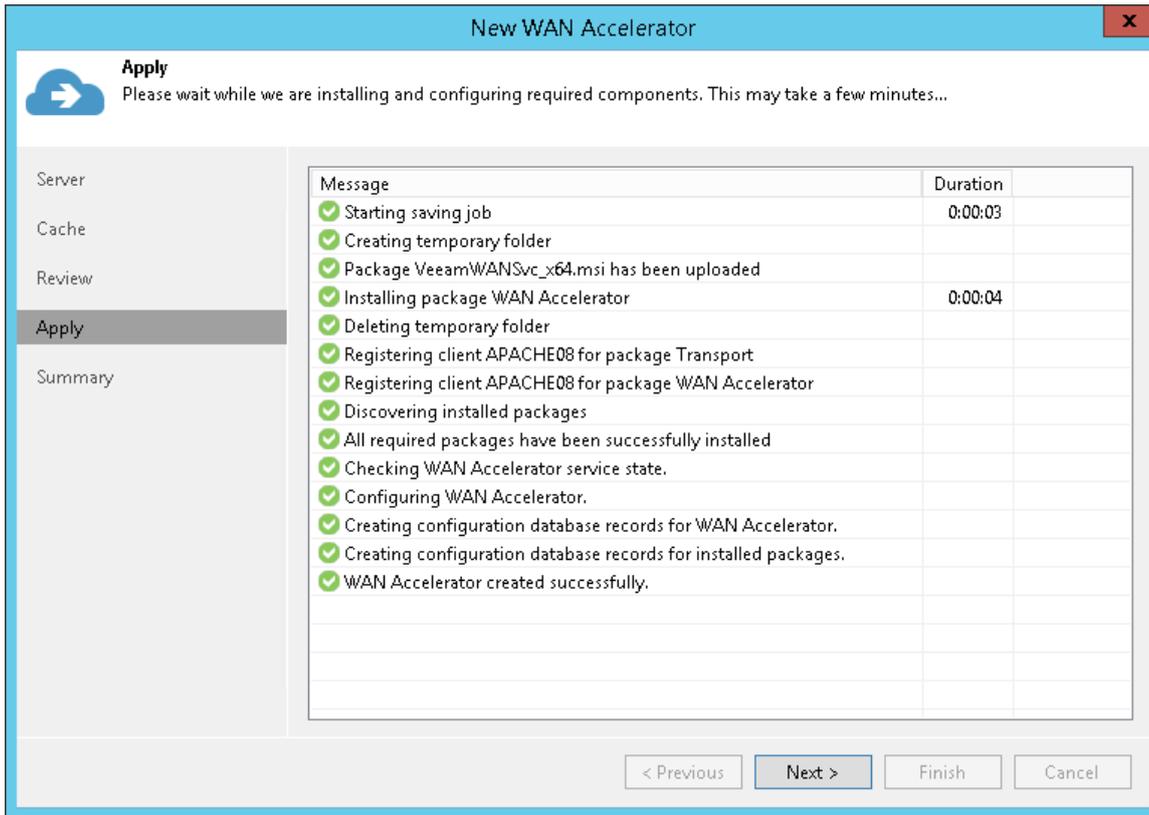


Step 5. Finish Working with Wizard

At the **Apply** step of the wizard, complete the procedure of WAN accelerator configuration.

1. Wait for the WAN accelerator to be added to the backup infrastructure.

2. Click **Next**, then click **Finish** to exit the wizard.

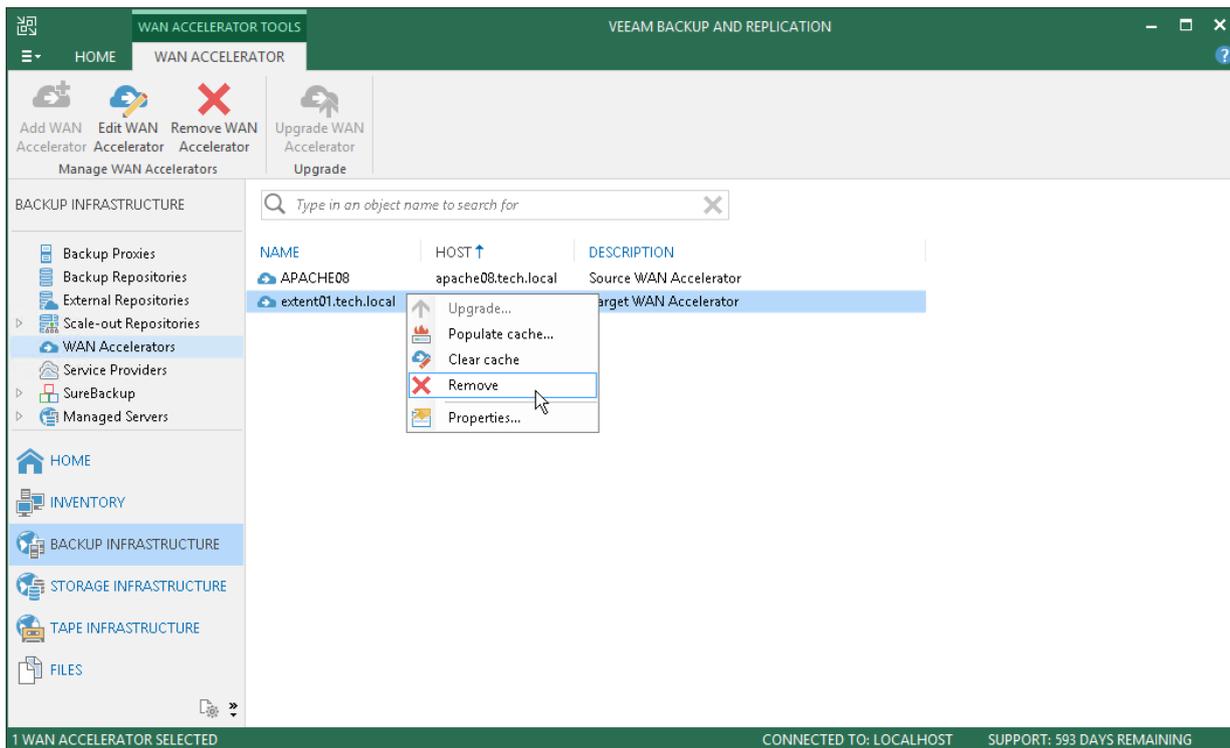


Removing WAN Accelerators

You can permanently remove a WAN accelerator from the backup infrastructure. When you remove a WAN accelerator, Veeam Backup & Replication unassigns the WAN accelerator role from the server, and this server is no longer used as a WAN accelerator. The server itself remains in the backup infrastructure.

To remove a WAN accelerator:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **WAN accelerators**.
3. In the working area, select the WAN accelerator and click **Remove WAN Accelerator** on the ribbon or right-click the WAN accelerator and select **Remove**.



WAN Global Cache

From the technical point of view, the global cache is a folder on the target WAN accelerator. By default, global cache data is stored in the `VeeamWAN` folder on the disk with the most amount of space available. However, you can define any folder of your choice when you configure the target WAN accelerator.

By default, the size of the global cache is 100 GB. You can increase the size or decrease it if necessary. The more space you allocate, the more repeating data blocks will be written to the global cache and the more efficient WAN acceleration will be. It is recommended that you allocate at least 40 GB to the global cache storage.

The global cache size is specified per source WAN accelerator. That is, if you plan to use one target WAN accelerator with several source WAN accelerators, the specified amount of space will be allocated for every source WAN accelerator that will be working with the target WAN accelerator and the size of the global cache will increase proportionally. For more information, see [WAN Accelerator Sizing](#).

The WAN global cache is a "library" that holds data blocks repeatedly going from the source side to the target side. The global cache is populated at the first cycle of a remote job. The priority is given to data blocks of Windows-based OSes, other OSes like Linux/Unix and standard applications such as Microsoft Exchange Server.

Veeam Backup & Replication constantly maintains the global cache in the actual state. To do that, it continuously monitors data blocks going over WAN and data blocks in the global cache.

- If some new data block is constantly sent over WAN, it is added to the global cache.
- If some data block in the global cache is not sent over WAN and are not re-used for some period of time, it is removed from the global cache to make room for new data blocks.

Veeam Backup & Replication also performs periodic consistency checks. If some data block in the global cache gets corrupted, Veeam Backup & Replication removes it from the global cache.

The efficiency of the WAN acceleration increases with every new backup copy interval in the backup copy job. During the first backup copy interval in the backup copy job, the WAN acceleration level is minimal. Veeam Backup & Replication populates the global cache. With every new job cycle, Veeam Backup & Replication updates the global cache to include the most "popular" data blocks and the WAN acceleration efficiency increases.

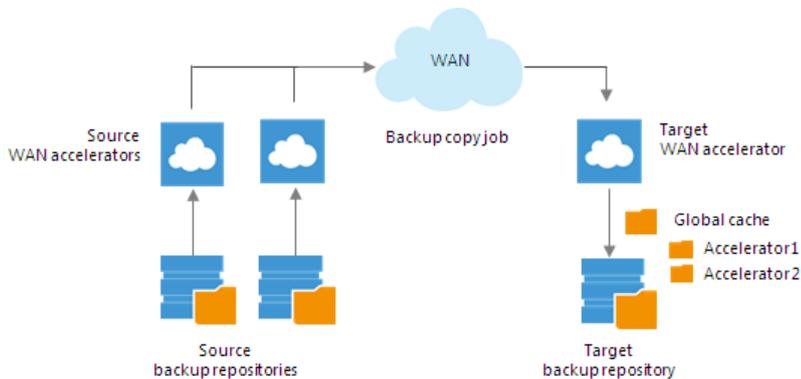
NOTE:

You can populate the global cache before you run the remote job for the first time. In this case, Veeam Backup & Replication will use the global cache starting from the first session of the remote job, and the WAN traffic will be minimal. For more information, see [Population of Global Cache](#).

Many to One WAN Acceleration

The WAN global cache can be used by several source WAN accelerators simultaneously. For example, if you have several remote/branch offices, you can configure several source WAN accelerators in remote sites and one target WAN accelerator in the head office.

In this case, the global cache will hold cache data for separate source WAN accelerators. The cache data for every source WAN accelerator will be stored in a dedicated subfolder in the global cache folder.



When one target WAN accelerator is used by several source WAN accelerators, Veeam Backup & Replication can copy data blocks between global cache of these WAN accelerators. This mechanism works if there are no matching backups of VMs on the target backup repository, but matching data is available in cache of other WAN accelerators.

For example, you have two backup copy jobs: *Job 1* and *Job 2*. The *Job 1* uses the source WAN accelerator *Source 1* and the target WAN accelerator *Target 3*. The *Job 2* uses the source WAN accelerator *Source 2* and the same target WAN accelerator *Target 3*. In the global cache folder, Veeam Backup & Replication will store data for 2 WAN accelerators: *Source 1* and *Source 2*.

- *Job 1* processes a VM running Microsoft Windows Server 2008 R2, and it has been running for some time. In the global cache, there is already data for this type of OS.
- *Job 2* also processes a VM running Microsoft Windows Server 2008 R2. When you start *Job 2* for the first time, there is no data for this type of OS in the global cache for *Source 2* WAN accelerator. In such situation, Veeam Backup & Replication will copy the necessary data block from the *Source 1* cache to the *Source 2* cache and will not transport this data block over WAN.

NOTE:

Beside using global cache of other WAN accelerator, Veeam Backup & Replication also utilizes backup files residing on the backup repository. For example, if the backup repository contains a backup file created with a backup job and the backup copy job starts copying a backup of a VM of the same type, Veeam Backup & Replication will populate global cache on the WAN accelerator from the backup file not to transfer redundant data over WAN.

Population of Global Cache

You can manually pre-populate the global cache to avoid the situation when the cache remains empty. As a result, by the time a remote job starts, the global cache will contain data blocks that can be used for data deduplication.

Population of the global cache can be helpful in the following scenarios:

- First run of a remote job. When you run a first session of a remote job, the global cache is empty, and the whole amount of VM data needs to be transferred over WAN. It is recommended that you populate the global cache before you start a remote job for the first time.
- Global cache corruption. If the global cache gets corrupted for some reason, Veeam Backup & Replication needs to perform at least one remote job session to replace corrupted data blocks with valid data blocks. In this situation, you can clean the global cache and populate it with valid data before a remote job begins.

Limitations for Population of Global Cache

The global cache population task has the following limitations:

- Veeam Backup & Replication does not use encrypted backups for global cache population.
- You can start the global cache population task for the target WAN accelerator that is not currently used by any remote job.
- If the global cache population task is currently running, the corresponding target WAN accelerator is locked. You cannot start any remote job using this target WAN accelerator.
- [For global cache corruption scenario] You must clean the global cache before you populate it with valid data. If the global cache contains data blocks, Veeam Backup & Replication will fail to perform the population task.
- [Veeam Cloud Connect] Veeam Backup & Replication does not use tenant backups to populate global cache on the service provider side.

How Population of Global Cache Works

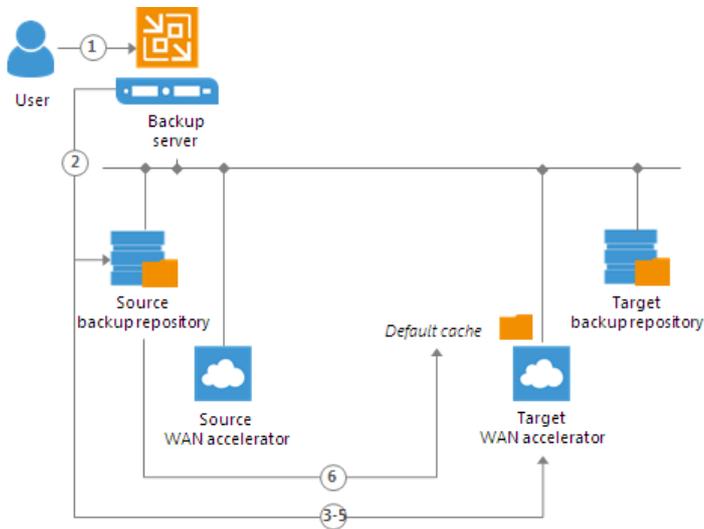
Global cache population is a manual operation performed by the user. When you run the global cache population task, Veeam Backup & Replication creates a 'default cache' on the target WAN accelerator. The default cache is used as a basic, universal cache for every new remote job.

To populate the default cache, Veeam Backup & Replication uses backup files stored on backup repositories as a source of data. Veeam Backup & Replication writes only data blocks for OSes to the default cache. Application data blocks are not written to the cache.

The procedure of global cache population includes the following steps:

1. The user starts the global cache population tasks and selects backup repositories from which data blocks should be retrieved.
2. Veeam Backup & Replication scans backup repositories and makes up a list of OSes whose data blocks are available in backup files.
3. Veeam Backup & Replication copies data blocks from backup repositories and populates the default cache with these data blocks.

- Veeam Backup & Replication copies data blocks only for missing OSEs from backup repositories and populates the default cache with these blocks. Data blocks for OSEs available in folders for other source WAN accelerators are not copied to the default cache during the population task. Veeam Backup & Replication copies these data blocks on the fly, when a remote job runs. For more information, see [Many to One WAN Acceleration](#).



Populating Global Cache

You can populate the global cache on the target WAN accelerator to reduce the amount of data transferred over WAN. It is recommended that you populate the global cache in the following situations:

- Global cache is empty before you start a remote job using WAN accelerators for the first time.
- Global cache is corrupted and you want to populate it with valid data. In this case, you must clear the global cache first and populate it with new data before a remote job starts. For more information, see [Clearing Global Cache](#).

IMPORTANT!

Veeam Backup & Replication does not use encrypted backups for global cache population.

To populate the global cache:

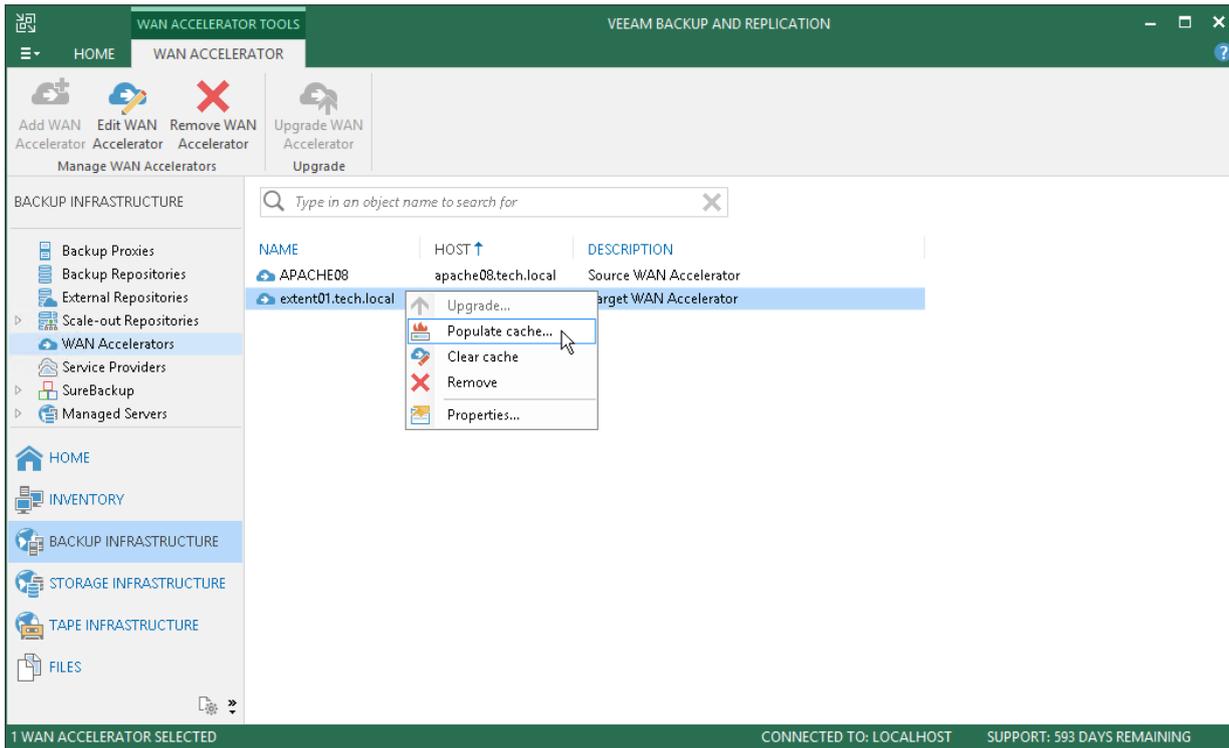
- Open the **Backup Infrastructure** view.
- In the inventory pane, select the **WAN Accelerators** node.
- In the working area, right-click the target WAN accelerator and select **Populate cache**.

If the selected WAN accelerator is not assigned as a target WAN accelerator to any remote job, Veeam Backup & Replication will display a warning.

- In the **Source Backup Repositories** window, select backup repositories from which OS data blocks must be retrieved.

It is strongly recommended that you select backup repositories on the same site where the target WAN accelerator is located. In the opposite case, the traffic will travel between sites, which will increase load on the network.

5. Click **OK**.



Clearing Global Cache

You can clear the global cache on the target WAN accelerator. It is recommended that you clear the global cache in the following situations:

- Global cache is corrupted.
- Global cache contains data that is no longer needed. This situation may occur, for example, if you have processed VMs running one OS and do not plan to process VMs with such OS in future. The global cache will contain data blocks that may be of no use for VMs running other OS.

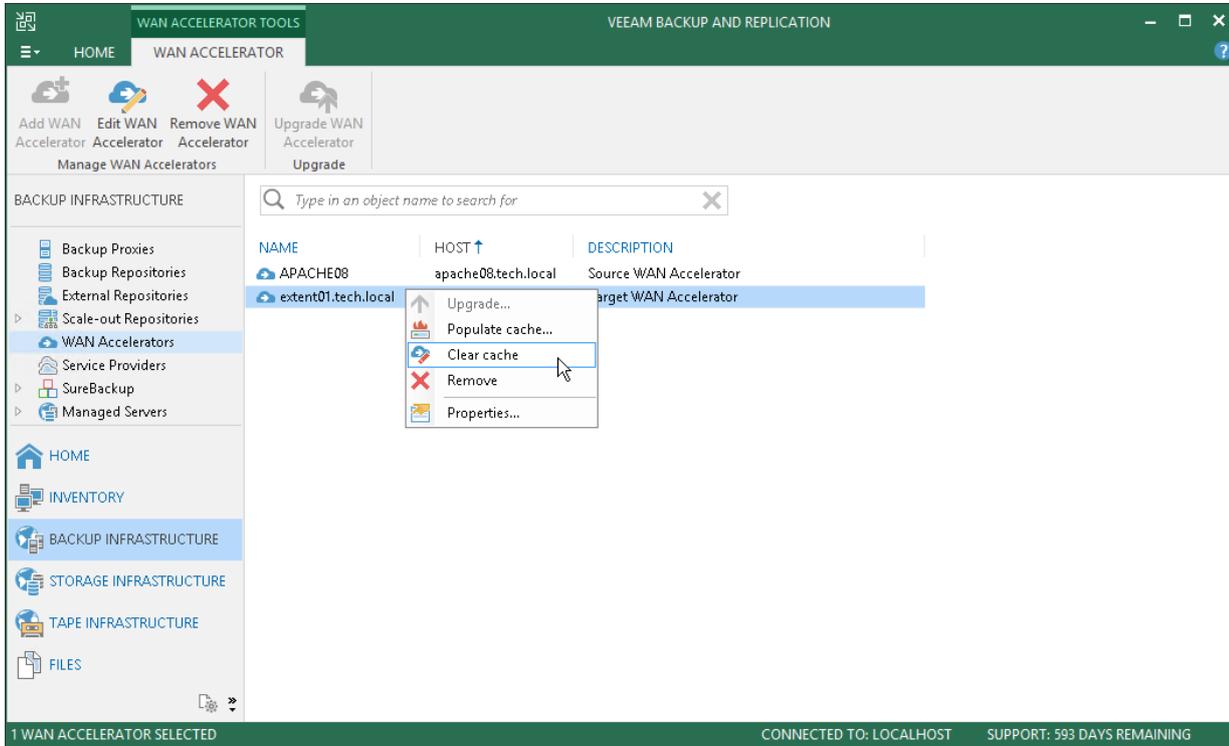
In such cases, it is recommended that you clear the global cache and **populate it anew** before you start remote jobs processing new types of VMs.

To clear the global cache:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, click **WAN Accelerators**.
3. In the working area, right-click the target WAN accelerator and select **Clear cache**.

IMPORTANT!

Before you clear the global cache, make sure that you do not have any running jobs that use this target WAN accelerator. When the global cache is cleared, Veeam Backup & Replication will restart the Veeam WAN Accelerator Service, and running jobs will complete with the *Failed* status.



Data Block Verification

During the VM copy process, Veeam Backup & Replication performs a CRC check for the VM traffic going between the source and target WAN accelerators. The CRC check helps ensure that the correct VM data goes to the target side and no corrupted data blocks are written to the global cache or to backup files in the target backup repository.

The check is performed in the following way:

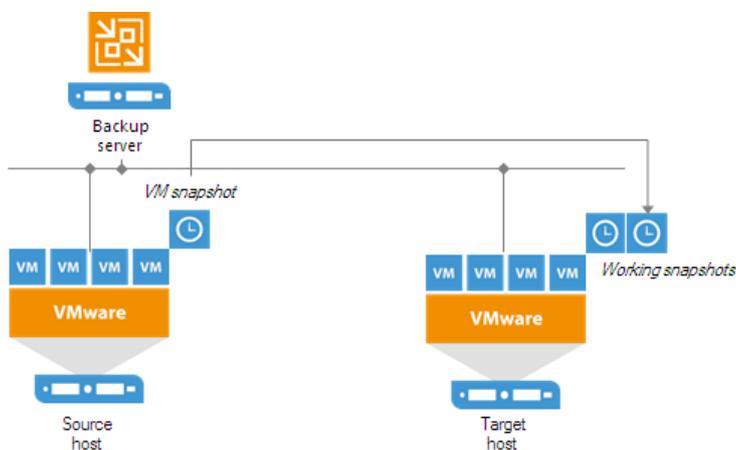
1. Before sending a data block to the target side, Veeam Backup & Replication calculates a checksum for the copied data block.
2. Once the data block is copied over WAN and before it is written to the global cache or to the target backup repository, Veeam Backup & Replication re-calculates the checksum for this data block on the target side.
3. The source and target checksums are compared. If the checksums do not coincide, the target WAN accelerator sends a request to the source WAN accelerator for the correct data block. The source WAN accelerator re-sends the necessary data blocks to the target WAN accelerator as is and the re-sent data block is written to the global cache or to the backup file on the target backup repository on the fly.

Data Transport on WAN Disconnect

If you replicate VMs over WAN accelerators, and a WAN connection drops for short periods of time (less than 30 minutes), Veeam Backup & Replication transparently handles disconnect issues. It automatically resumes the data transport process from the point when the connection was lost. The resume on disconnect capability improves the reliability of offsite replication, reduces the backup window and minimizes the load on the WAN link.

If a WAN connection is lost for more than 30 minutes, Veeam Backup & Replication still does not finish the job with a failed status. After a WAN connection is resumed, Veeam Backup & Replication starts a new data transfer cycle. Data transported with every new transport cycle is written to a new working snapshot of a VM replica. As the WAN connection may drop several times, Veeam Backup & Replication can create a number of working snapshots.

Not to keep long snapshot chains, Veeam Backup & Replication merges earlier snapshots and maintains only two working snapshots for the VM replica. When all VM data is transferred to the target host, the two working snapshots are also merged to create one fully functional VM restore point.



If the WAN link is weak and drops constantly, Veeam Backup & Replication may fail to transport VM data by the time a new replication job session starts. In this case, during a new replication job session Veeam Backup & Replication attempts to transfer VM data that have changed since the last replication job session and VM data that were not transferred during the previous replication job session.

Data Encryption

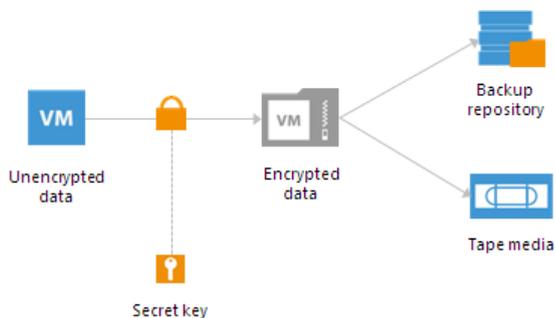
Data security is an important part of the backup strategy. You must protect your information from unauthorized access, especially if you back up sensitive VM data to offsite locations or archive it to tape. To keep your data safe, you can use data encryption.

Data encryption transforms data to an unreadable, scrambled format with the help of a cryptographic algorithm and a secret key. If encrypted data is intercepted, it cannot be unlocked and read by the eavesdropper. Only intended recipients who know the secret key can reverse encrypted information back to a readable format.

In Veeam Backup & Replication, encryption works at the following levels:

- Backup job
- Transaction log backup job
- Backup copy job
- VeeamZIP
- Tapes in media pools

Veeam Backup & Replication uses the block cypher encryption algorithm. Encryption works at the source side. Veeam Backup & Replication reads VM or file data, encodes data blocks, transfers them to the target side in the encrypted format and stores the data to a file on the backup repository or archives the data to tape. Data decryption is also performed on the source side: Veeam Backup & Replication transfers encrypted data back to the source side and decrypts it there.



NOTE:

Veeam Backup & Replication will pass encryption keys to the target backup repository or cloud repository in the following cases:

- If you run a backup copy job over WAN accelerators
- If you perform health check for the encrypted backup files

Beside the job-level encryption, Veeam Backup & Replication allows you to encrypt network traffic going between the primary site and the disaster recovery site. Network traffic encryption is configured as part of global network traffic rules that are set for backup infrastructure components. For network traffic encryption, Veeam Backup & Replication uses the 256-bit Advanced Encryption Standard (AES).

IMPORTANT!

Data encryption has a negative effect on the deduplication ratio if you use a deduplicating storage appliance as a target. Veeam Backup & Replication uses different encryption keys for every job session. For this reason, encrypted data blocks sent to the deduplicating storage appliances appear as different though they may contain duplicate data. If you want to achieve a higher deduplication ratio, you can disable data encryption.

Encryption Standards

Veeam Backup & Replication uses the following industry-standard data encryption algorithms:

Data Encryption

- To encrypt data blocks in backup files and files archived to tape, Veeam Backup & Replication uses the 256-bit AES with a 256-bit key length in the CBC-mode. For more information, see [Advanced Encryption Standard \(AES\)](#).
- To generate a key based on a password, Veeam Backup & Replication uses the Password-Based Key Derivation Function, PKCS #5 version 2.0. Veeam Backup & Replication uses 10,000 HMAC-SHA1 iterations and a 512-bit salt. For more information, see [Recommendation for Password-Based Key Derivation](#).

Enterprise Manager Keys

- To generate Enterprise Manager keys required for data restore without a password, Veeam Backup & Replication uses the RSA algorithm with a 4096-bit key length.
- To generate a request for data restore from a backup server, Veeam Backup & Replication uses the RSA algorithm with a 2048-bit key length.

For more information, see [RSA Cryptography Standard](#).

Hashing Algorithms

Veeam Backup & Replication uses the following hashing algorithms:

- For digital signature generation: SHA-1, SHA-256
- For HMAC generation: HMAC_SHA-1
- For random number generation: SHA-1

Encryption Libraries

For Microsoft Windows-based repositories and software-based encryption for tapes, Veeam Backup & Replication uses the Windows Crypto API complying with the Federal Information Processing Standards (FIPS 140). For more information, see [Cryptographic Module Validation Program](#).

Veeam Backup & Replication uses the following cryptographic service providers:

- Microsoft Base Cryptographic Provider. For more information, see [Microsoft Docs](#).
- Microsoft Enhanced RSA and AES Cryptographic Provider. For more information, see [Microsoft Docs](#).
- Microsoft Enhanced Cryptographic Provider. For more information, see [Microsoft Docs](#).

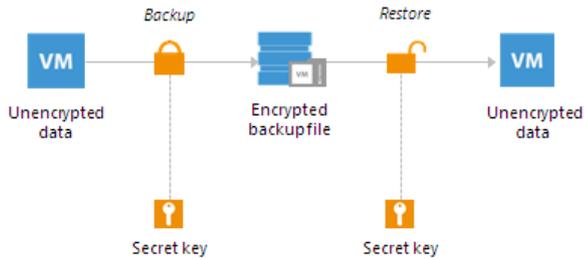
For Linux-based repositories, Veeam Backup & Replication uses a statically linked OpenSSL encryption library, without the FIPS 140 support. For more information, see [OpenSSL](#).

Veeam Backup & Replication encrypts stored credentials using the Data Protection API (DPAPI) mechanisms. For more information, see [Microsoft Docs](#).

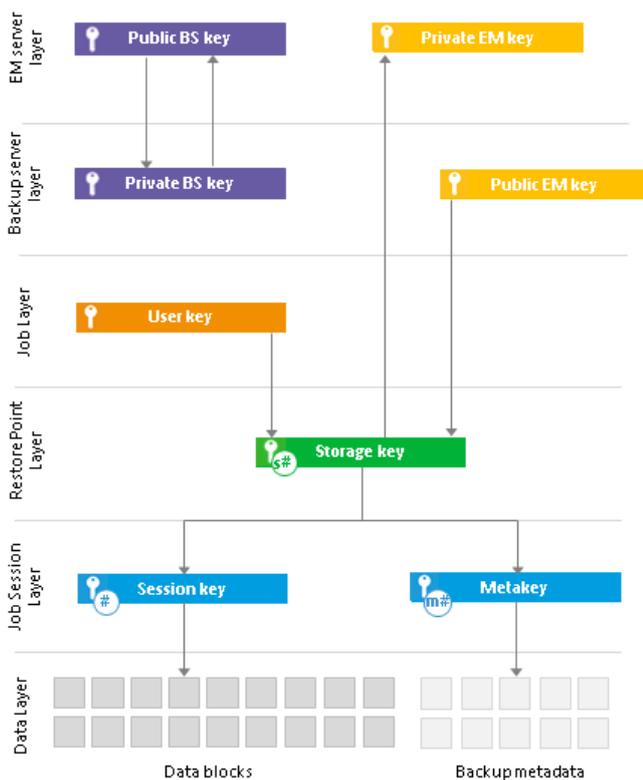
Encryption Algorithms

To encrypt data in backups and files, Veeam Backup & Replication employs a symmetric key encryption algorithm.

The symmetric, or single-key encryption algorithm, uses a single, common secret key to encrypt and decrypt data. Before data is sent to target side, it is encoded with a secret key. To restore encrypted data, you must have the same secret key. Users who do not have the secret key cannot decrypt data and get access to it.



Veeam Backup & Replication relies on a hierarchical encryption scheme. Each layer in the hierarchy encrypts the layer below with a key of specific type.



Encryption Keys

An encryption key is a string of random characters that is used to bring data to a scrambled format and back to unscrambled. Encryption keys encode and decode initial data blocks or underlying keys in the key hierarchy.

Veeam Backup & Replication uses 8 types of keys:

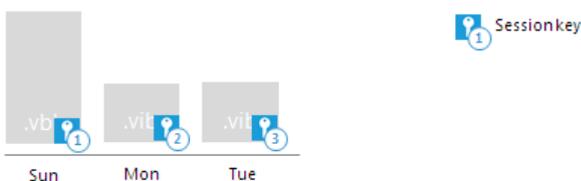
- 3 service keys generated by Veeam Backup & Replication:
 - [Session key](#)
 - [Metakey](#)
 - [Storage key](#)
- 1 key generated based on a user password: a [user key](#).
- A pair of keys used for data recovery without a password – [Enterprise Manager keys](#).
- A pair of keys used for identity verification of the backup server – [backup server keys](#).

Session Keys and Metakeys

The session key is the lowest layer in the encryption key hierarchy. When Veeam Backup & Replication encrypts data, it first encodes every data block in a file with a session key. For session keys, Veeam Backup & Replication uses the AES algorithm with a 256-bit key length in the CBC-mode.

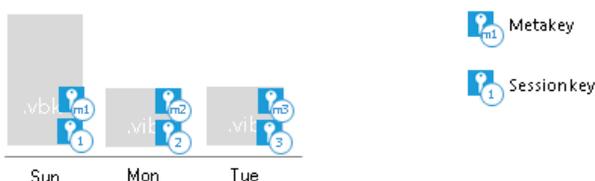
Veeam Backup & Replication generates a new session key for every job session. For example, if you have created an encrypted backup job and run 3 job sessions, Veeam Backup & Replication will produce 3 backup files that will be encrypted with 3 different session keys:

- Full backup file encrypted with session key 1
- Incremental backup file encrypted with session key 2
- Incremental backup file encrypted with session key 3



The session key is used to encrypt only data blocks in backup files or files archived to tape. To encrypt backup metadata, Veeam Backup & Replication applies a separate key – metakey. Use of a metakey for metadata raises the security level of encrypted backups.

For every job session, Veeam Backup & Replication generates a new metakey. For example, if you have run 3 job sessions, Veeam Backup & Replication will encrypt metadata with 3 metakeys.



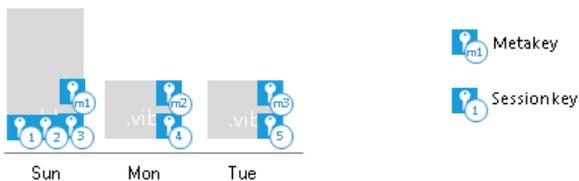
In the encryption process, session keys and metakeys are encrypted with keys of a higher layer – storage keys. Cryptograms of session keys and metakeys are stored to the resulting file next to encrypted data blocks.

Metakeys are additionally kept in the configuration database.

Storage Keys

Backup files in the backup chain often need to be transformed, for example, in case you create a reverse incremental backup chain. When Veeam Backup & Replication transforms a full backup file, it writes data blocks from several restore points to the full backup file. As a result, the full backup file contains data blocks that are encrypted in different job sessions with different session keys.

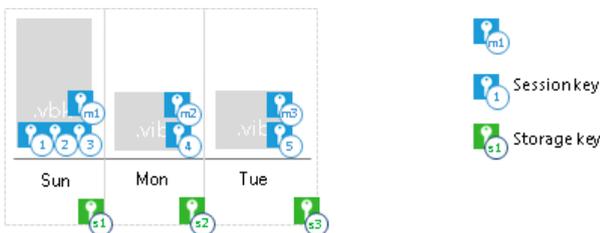
To restore data from such “composed” backup file, Veeam Backup & Replication would require a bunch of session keys. For example, if the backup chain contains restore points for 2 months, Veeam Backup & Replication would have to keep session keys for a 2-month period.



In such situation, storing and handling session keys would be resource consuming and complicated. To facilitate the encryption process, Veeam Backup & Replication introduces another type of service key – a storage key.

For storage keys, Veeam Backup & Replication uses the AES algorithm. A storage key is directly associated with one restore point in the backup chain. The storage key is used to encrypt the following keys in the encryption hierarchy:

- All session keys for all data blocks in one restore point
- Metakey encrypting backup metadata



During the restore process, Veeam Backup & Replication uses one storage key to decrypt all session keys for one restore point, no matter how many session keys were used to encrypt data blocks in this restore point. As a result, Veeam Backup & Replication does not need to keep the session keys history in the configuration database. Instead, it requires only one storage key to restore data from one file.

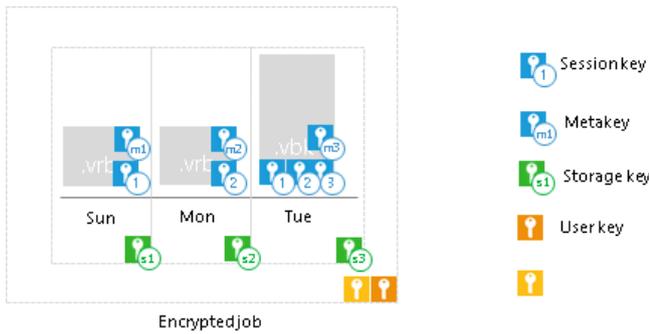
In the encryption process, storage keys are encrypted with keys of a higher layer – user keys and optionally a public Enterprise Manager key. Cryptograms of storage keys are stored to the resulting file next to encrypted data blocks, and cryptograms of session keys and metakeys.

Storage keys are also kept in the configuration database. To maintain a set of valid storage keys in the database, Veeam Backup & Replication uses retention policy settings specified for the job. When some restore point is removed from the backup chain by retention, the storage key corresponding to this restore point is also removed from the configuration database.

User Keys

When you enable encryption for a job, you must define a password to protect data processed by this job, and define a hint for the password. The password and the hint are saved in the job settings. Based on this password, Veeam Backup & Replication generates a user key.

The user key protects data at the job level. In the encryption hierarchy, the user key encrypts storage keys for all restore points in the backup chain.



During the encryption process, Veeam Backup & Replication saves a hint for the password to the encrypted file. When you decrypt a file, Veeam Backup & Replication displays a hint for the password that you must provide. After you enter a password, Veeam Backup & Replication derives a user key from the password and uses it to unlock the storage key for the encrypted file.

According to the security best practices, you must change passwords for encrypted jobs regularly. When you change a password for the job, Veeam Backup & Replication creates a new user key and uses it to encrypt new restore points in the backup chain.

IMPORTANT!

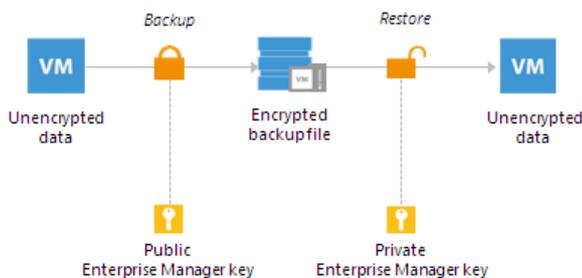
You must always remember passwords set for jobs or save these passwords in a safe place. If you lose or forget the password, you can restore data from a backup file by issuing a request to Veeam Backup Enterprise Manager. For more information, see [How Decryption Without Password Works](#).

Enterprise Manager Keys

In some cases, a password required for data decryption may be lost or forgotten, or a user who knows the password may leave your organization. As a result, you cannot recover data from backups or tapes encrypted with this password, and encrypted data becomes unusable.

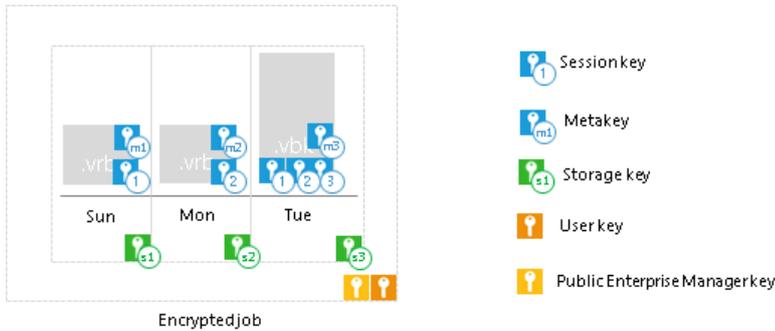
Veeam Backup & Replication offers you a way to restore encrypted data even if you do not have a password. For this purpose, Veeam Backup & Replication employs an additional pair of keys in the encryption process – Enterprise Manager keys.

Enterprise Manager keys is a pair of matching RSA keys: a public key and a private key. The public Enterprise Manager key is used to encrypt data, while the private Enterprise Manager key is used to decrypt data encrypted with the public key.



In the encryption process, Enterprise Manager keys perform a role similar to the user key: the public Enterprise Manager key encrypts storage keys and the private Enterprise Manager key decrypts them. Technically, Enterprise Manager keys offer an alternative to the user key. When you create an encrypted backup file or archive encrypted data to tape, Veeam Backup & Replication encrypts storage keys with two types of keys simultaneously:

- User key
- Public Enterprise Manager key



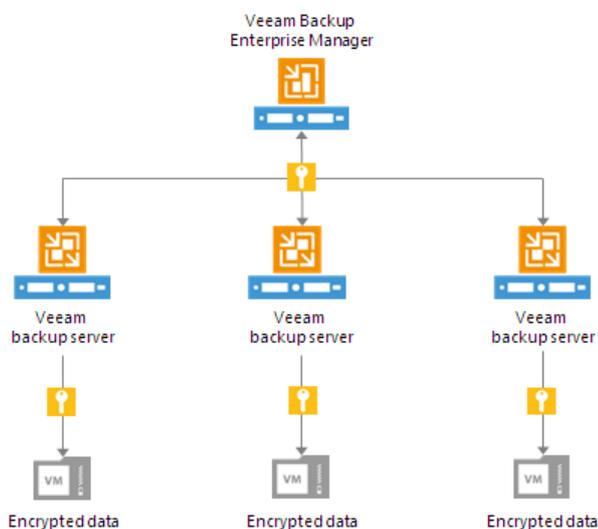
When you decrypt a file and the password is lost, Veeam Backup & Replication cannot derive the user key from the password. In this situation, you can send a request to Veeam Backup Enterprise Manager. Veeam Backup Enterprise Manager will employ the private Enterprise Manager key instead of the user key to unlock storage keys and decrypt the file content. For more information, see [How Decryption Without Password Works](#).

Enterprise Manager keys take part in the encryption process if the following two conditions are met:

1. You have Enterprise or Enterprise Plus Edition of Veeam Backup & Replication.
2. You have Veeam Backup Enterprise Manager installed and your backup servers are connected to Veeam Backup Enterprise Manager.

Enterprise Manager keys make up a pair of matching keys – a keyset. Enterprise Manager keysets are created and managed on the Veeam Backup Enterprise Manager server. During installation of Veeam Backup Enterprise Manager, the setup automatically generates a new keyset containing a public Enterprise Manager key and a private Enterprise Manager key. You can use Veeam Backup Enterprise Manager to create new Enterprise Manager keysets, activate them, import and export keysets and specify retention for their lifetime.

The public Enterprise Manager key is made publicly available to backup servers. When you connect backup servers to Veeam Backup Enterprise Manager, the public Enterprise Manager key is automatically propagated to these backup servers.



Veeam Backup Enterprise Manager acts as a manager for public Enterprise Manager keys but does not store these keys. After the public Enterprise Manager key is propagated to the backup server, it is kept in the configuration database.

Private Enterprise Manager keys, on the contrary, are not distributed anywhere: they are kept only on Veeam Backup Enterprise Manager.

Backup Server Keys

Eavesdroppers may potentially use Veeam Backup Enterprise Manager to unlock files encrypted with Veeam Backup & Replication. If the eavesdropper intercepts an encrypted file, s/he may generate a request for file unlocking and send such request to Veeam Backup Enterprise Manager Administrators. Having received a response from Veeam Backup Enterprise Manager, the eavesdropper will be able to unlock the encrypted file without a password.

To protect you against the "man-in-the-middle" attack, Veeam Backup & Replication uses backup server keys. Backup server keys are a pair of RSA keys, public and private, that are generated on the backup server.

- The public backup server key is sent to Veeam Backup Enterprise Manager to which the backup server is connected, and saved in the Veeam Backup Enterprise Manager configuration database.
- The private backup server key is kept on the backup server in the Veeam Backup & Replication configuration database.

Backup server keys are used to authenticate the identity of the request sender. When the backup server generates a request to unlock a file, it adds a signature encrypted with the private backup server key to this request.

When Veeam Backup Enterprise Manager processes the request, it uses the public backup server key to decrypt the signature and identify the request sender. If the backup server used for request generation is not added to Veeam Backup Enterprise Manager, Veeam Backup Enterprise Manager will not find a matching public key in its database. As a result, Veeam Backup Enterprise Manager will not be able to identify the sender and the storage key decryption process will fail.

How Data Encryption Works

Data encryption is performed as part of backup, backup copy or archiving to tape processes. Encryption works at the source side, before data is transported to the target. Encryption keys are not passed to the target side, unless you run a backup copy job over WAN accelerators or perform health check for the encrypted backup files.

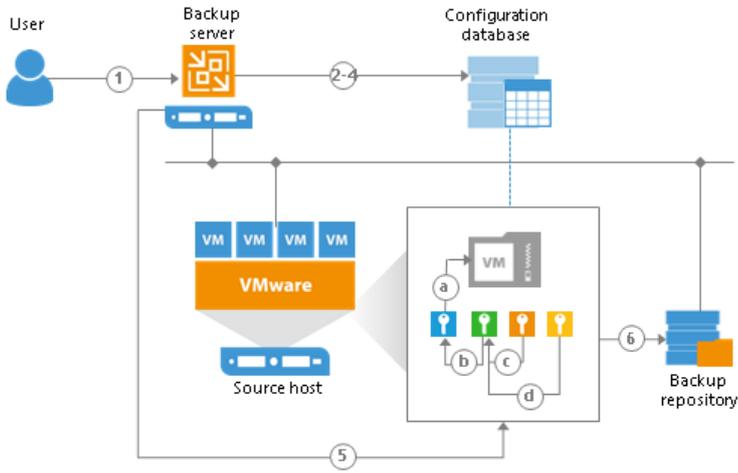
NOTE:

The procedure below describes the encryption process for backup, backup copy jobs and VeeamZIP tasks. For more information about encrypting data on tapes, see [Tape Encryption](#).

The encryption process includes the following steps:

1. When you create a new job, you enable the encryption option for the job and enter a password to protect data at the job level.
2. Veeam Backup & Replication generates a user key based on the entered password.
3. When you start an encrypted job, Veeam Backup & Replication creates a storage key and stores this key to the configuration database.
4. Veeam Backup & Replication creates a session key and a metakey. The metakey is stored to the configuration database.
5. Veeam Backup & Replication processes job data in the following way:
 - a. The session key encrypts data blocks in the backup file. The metakey encrypts backup metadata.
 - b. The storage key encrypts the session key and the metakey.
 - c. The user key encrypts the storage key.
 - d. If you use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication and the backup server is connected to Veeam Backup Enterprise Manager, the Enterprise Manager key also encrypts the storage key.
6. Encrypted data blocks are passed to the target. The cryptograms of the public Enterprise Manager key (if used), user key, storage key, session key and metakey are stored to the resulting file next to encrypted data blocks.

If you use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication and the backup server is connected to Veeam Backup Enterprise Manager, Veeam Backup & Replication saves two cryptograms of the storage key to the resulting file: one encrypted with the user key (c) and one encrypted with the Enterprise Manager key (d). Saving the cryptogram twice helps Veeam Backup & Replication decrypt the file even if a password is lost or forgotten. For more information, see [How Decryption Without Password Works](#).



Legend

-  Session key
-  User key
-  Storage key
-  Public Enterprise Manager key

How Data Decryption Works

When you restore data from an encrypted backup file, Veeam Backup & Replication performs data decryption automatically in the background or requires you to provide a password.

- If encryption keys required to unlock the backup file are available in the Veeam Backup & Replication configuration database, you do not need to enter the password. Veeam Backup & Replication uses keys from the database to unlock the backup file. Data decryption is performed in the background, and data restore does not differ from that from an unencrypted one.

Automatic data decryption is performed if the following conditions are met:

- a. You encrypt and decrypt the backup file on the same backup server using the same Veeam Backup & Replication configuration database.
 - b. [For backup file] The backup is not removed from the Veeam Backup & Replication console.
- If encryption keys are not available in the Veeam Backup & Replication configuration database, you need to provide a password to unlock the encrypted file.

Data decryption is performed at the source side, after data is transported back from the target side. As a result, encryption keys are not passed to the target side, which helps avoid data interception.

NOTE:

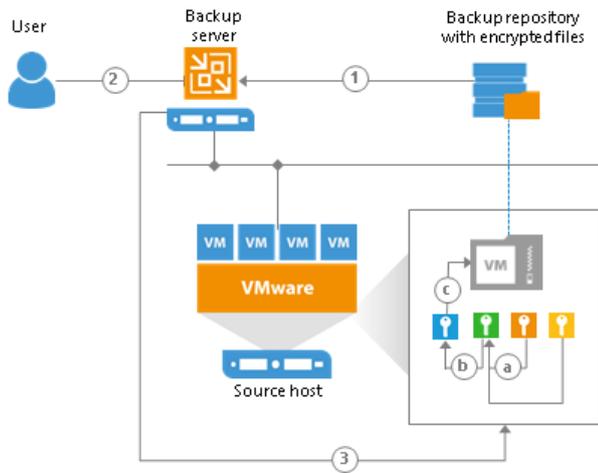
The procedure below describes the decryption process for backup, backup copy jobs and VeeamZIP tasks. For more information about decrypting tape data, see [Tape Encryption](#).

The decryption process includes the following steps. Note that steps 1 and 2 are required only if you decrypt the file on the backup server other than the backup server where the file was encrypted.

1. You import the file to the backup server. Veeam Backup & Replication notifies you that the imported file is encrypted and requires a password.
2. You specify a password for the imported file. If the password has changed once or several times, you need to specify the password in the following manner:
 - If you select a .vbm file for import, you must specify the latest password that was used to encrypt files in the backup chain.
 - If you select a full backup file for import, you must specify the whole set of passwords that were used to encrypt files in the backup chain.
3. Veeam Backup & Replication reads the entered password and generates the user key based on this password. With the user key available, Veeam Backup & Replication performs decryption in the following way:
 - a. Veeam Backup & Replication applies the user key to decrypt the storage key.
 - b. The storage key, in its turn, unlocks underlying session keys and a metakey.
 - c. Session keys decrypt data blocks in the encrypted file.

After the encrypted file is unlocked, you can work with it as usual.

If you have lost or forgotten a password for an encrypted file, you can issue a request to Veeam Backup Enterprise Manager and restore data from an encrypted file using Enterprise Manager keys. For more information, see [Enterprise Manager Keys](#) and [How Decryption Without Password Works](#).



Legend

-  Session key
-  User key
-  Storage key
-  Private Enterprise Manager key

How Decryption Without Password Works

When you import an encrypted backup file or tape media to the backup server, you need to enter a password to decrypt data. In some cases, however, a password can be lost or forgotten. Veeam Backup & Replication offers a way to restore data from encrypted backups or tapes even if a password is not available.

You can restore of data from encrypted backups or tapes without a password only if your backup infrastructure meets the following conditions:

1. You use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication.
2. The backup servers on which you encrypted data is added to Veeam Backup Enterprise Manager.
3. The backup server on which you generate a request for data decryption is added to Veeam Backup Enterprise Manager.

If the backup server on which you encrypt data is added to Veeam Backup Enterprise Manager, Veeam Backup & Replication employs the public Enterprise Manager key in the encryption process. To decrypt backups or tapes encrypted with the public Enterprise Manager key, you can apply a matching private Enterprise Manager key, instead of a password. The private Enterprise Manager key unlocks the underlying storage keys and lets you access the content of an encrypted file.

The restore process is accomplished with the help of two wizards that run on two servers:

1. The **Encryption Key Restore** wizard on the backup server.
2. The **Password Recovery** wizard on the Veeam Backup Enterprise Manager server.

The restore process includes the next steps:

1. You start the **Encryption Key Restore** wizard on the backup server to issue a request for data recovery.
2. The **Encryption Key Restore** wizard generates a request to Veeam Backup Enterprise Manager. The request has the format of a text document and contains cryptograms of storage keys that must be decrypted, together with information about the public Enterprise Manager key that was used to encrypt data. At the end of the request, the backup server adds a signature encrypted with a private backup server key.
3. You send the request to the Veeam Backup Enterprise Manager Administrator, for example, via email.
4. The Veeam Backup Enterprise Manager Administrator starts the **Password Recovery** wizard on Veeam Backup Enterprise Manager and inserts the text of the request to the wizard.
5. Veeam Backup Enterprise Manager finds a matching public backup server key in Veeam Backup Enterprise Manager configuration database and decrypts the signature with this key.
6. Veeam Backup Enterprise Manager decrypts storage keys with the private Enterprise Manager key available on Veeam Backup Enterprise Manager, and generates a response in the **Password Recovery** wizard. The response has the format of a text document and contains decrypted storage keys.
7. The Veeam Backup Enterprise Manager Administrator sends the response to you, for example, via email.
8. You input the request to the **Encryption Key Restore** wizard. Veeam Backup & Replication processes the response, retrieves the decrypted storage keys and uses them to unlock encrypted backups or tapes and retrieve their content.

IMPORTANT!

You can recover data only if Veeam Backup Enterprise Manager has a private Enterprise Manager key matching the public Enterprise Manager key that was used for data encryption. If a matching private Enterprise Manager key is not found in the Veeam Backup Enterprise Manager configuration database, the **Password Recovery** wizard will fail. In such situation, you can import a necessary private Enterprise Manager key via the import procedure. For more information, see *Exporting and Importing Enterprise Manager Keys* in Veeam Backup Enterprise Manager User Guide.



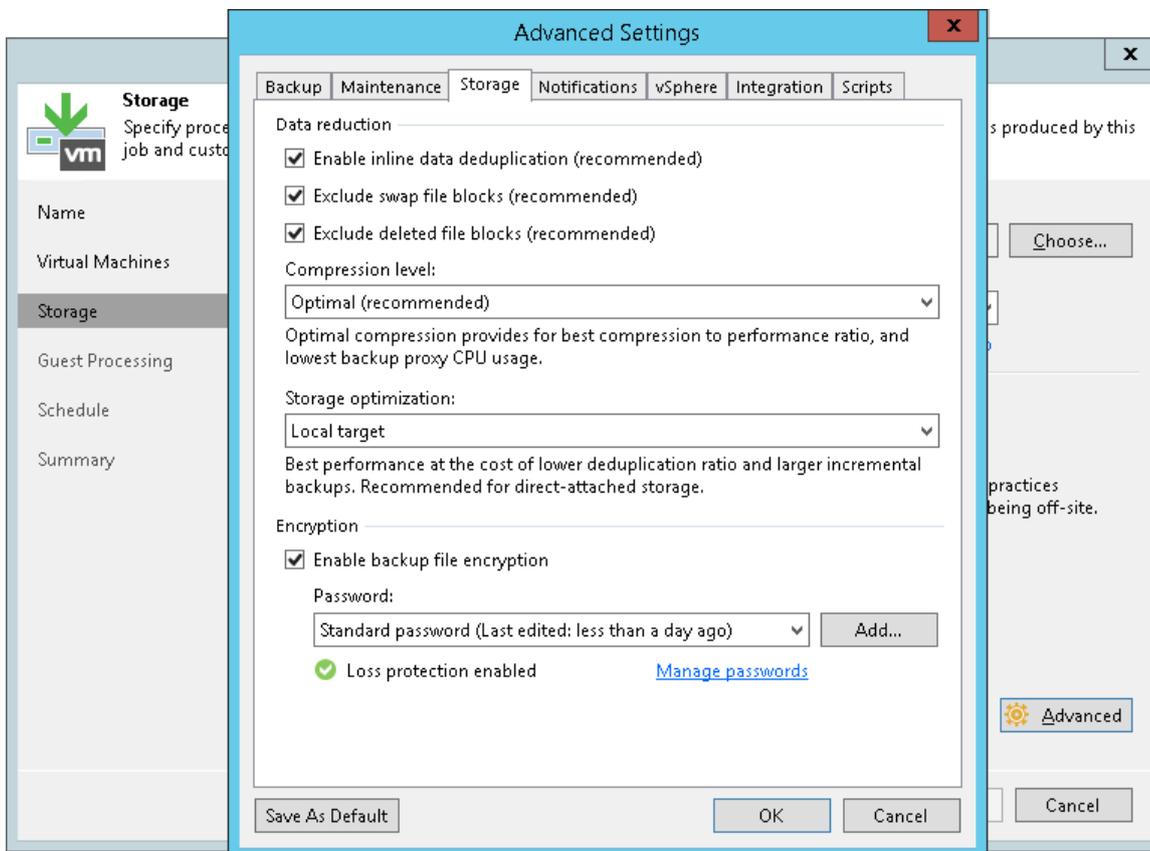
Encrypted Objects

The encryption algorithm works at the job level and media pool level. You can enable encryption for the following types of jobs:

- [Backup job](#)
- [Backup copy job](#)
- [Backup to tape job](#)
- [VeeamZIP](#)
- [Tape encryption](#)

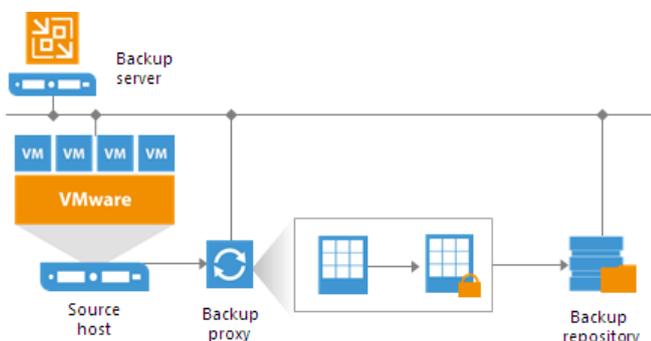
Backup Job Encryption

Encryption for a backup job is configured in the advanced job settings. You should enable the encryption option and specify a password to protect data in backup files produced by the backup job.



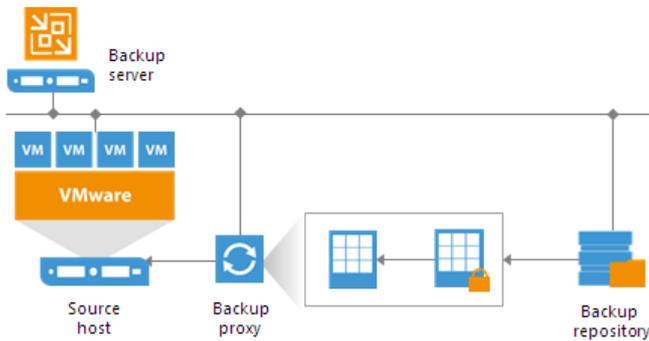
The backup job processing with encryption enabled includes the following steps:

1. You enable encryption for a backup job and specify a password.
2. Veeam Backup & Replication generates the necessary keys to protect backup data.
3. Veeam Backup & Replication encrypts data blocks on the backup proxy, either the dedicated or default one, and transfers them to the backup repository already encrypted.
4. On the backup repository, encrypted data blocks are stored to a resulting backup file.



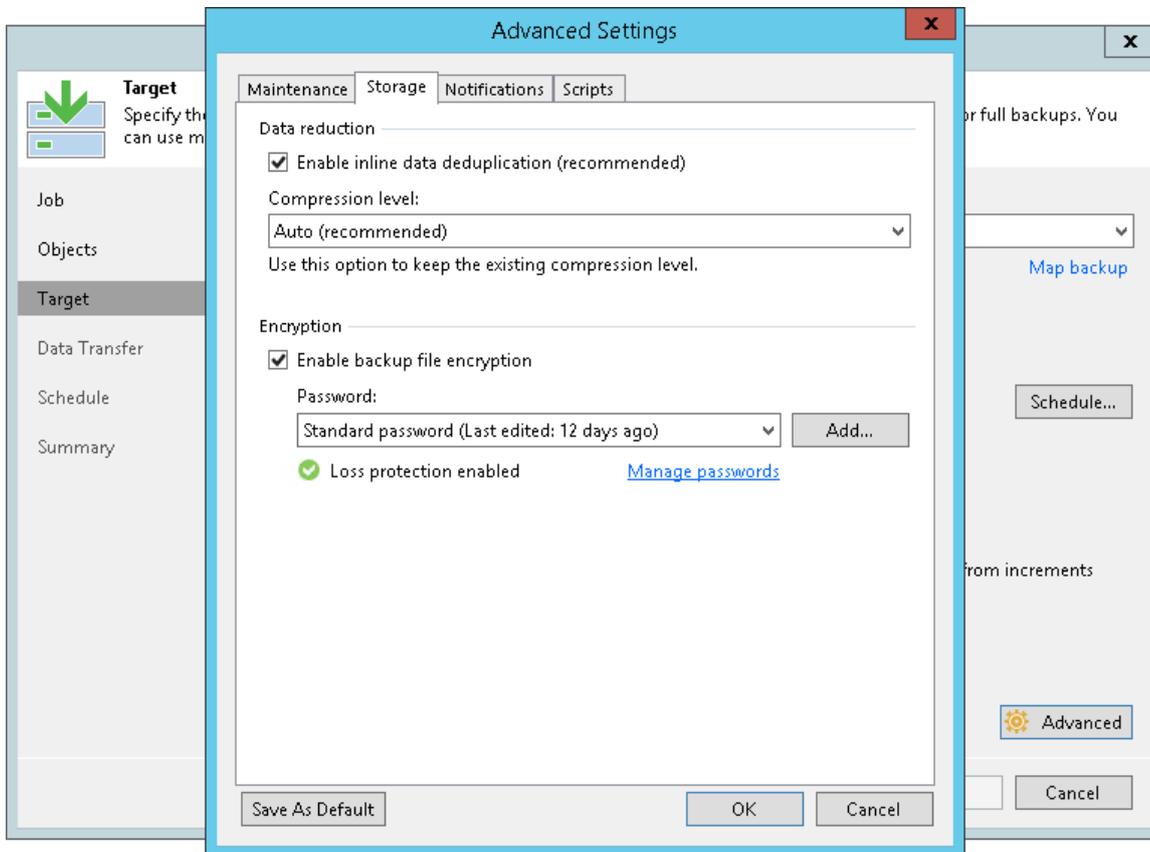
Restore of an encrypted backup file includes the following steps:

1. You import a backup file and define a password to decrypt the backup file. If the password has changed once or several times, you need to specify the password in the following manner:
 - If you select a metadata file (VBM) for import, you must specify the latest password that was used to encrypt files in the backup chain.
 - If you select a full backup file (VBK) for import, you must specify the whole set of passwords that were used to encrypt files in the backup chain.
2. Veeam Backup & Replication uses the provided passwords to generate user keys and unlock the subsequent keys for backup file decryption.
3. Veeam Backup & Replication retrieves data blocks from the backup file, sends them to the source side and decrypts them on the backup proxy, either the dedicated or default one.



Backup Copy Job Encryption

Encryption for a backup copy job is configured in the advanced job settings. You should enable the encryption option and specify a password to protect data in backup files produced by the backup copy job.



The workflow of the encrypted backup copy job depends on the path for data transfer:

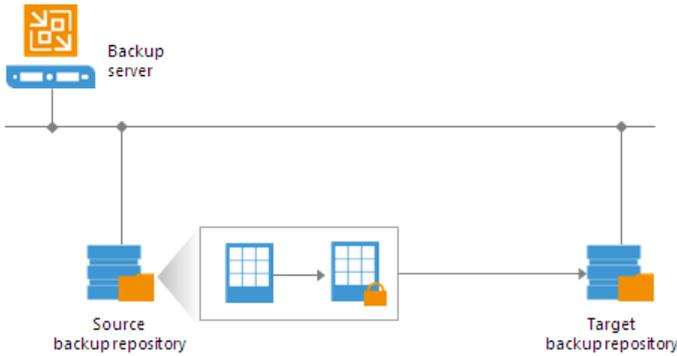
- [Direct data path](#)
- [Over WAN accelerators](#)

Direct Data Path

If you use a direct data path to transfer backups to the target backup repository, the encrypted backup copy job includes the following steps:

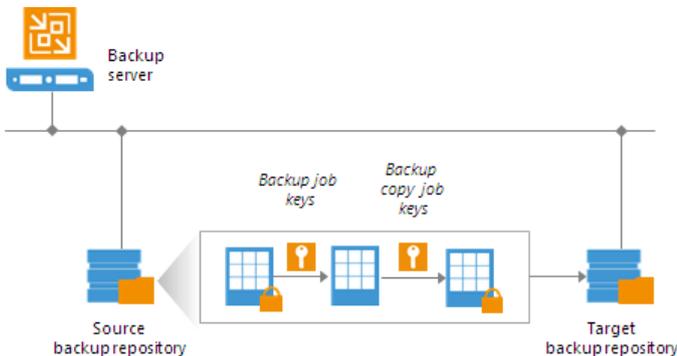
1. You enable encryption for a backup copy job and specify a password.
2. Veeam Backup & Replication generates the necessary keys to protect backup files produced by the backup copy job.
3. Veeam Backup & Replication encrypts data blocks on the source side and transfers them to the target backup repository.

4. On the target backup repository, encrypted data blocks are stored to a resulting backup file.



An encrypted backup copy job may use an encrypted backup file as a source. In this situation, Veeam Backup & Replication does not perform double encryption. The backup copy job includes the following steps:

1. Veeam Backup & Replication decrypts data blocks of the encrypted source backup file. For the decryption process, it uses the storage key and metakeys stored in the configuration database.
2. Veeam Backup & Replication generates the necessary keys to protect backup files produced by the backup copy job.
3. Veeam Backup & Replication encrypts data blocks on the source side using these keys and transfers encrypted data blocks to the target backup repository.
4. On the target backup repository, encrypted data blocks are stored to a resulting backup file.



The restore process for backups produced by backup copy jobs does not differ from that for backup jobs.

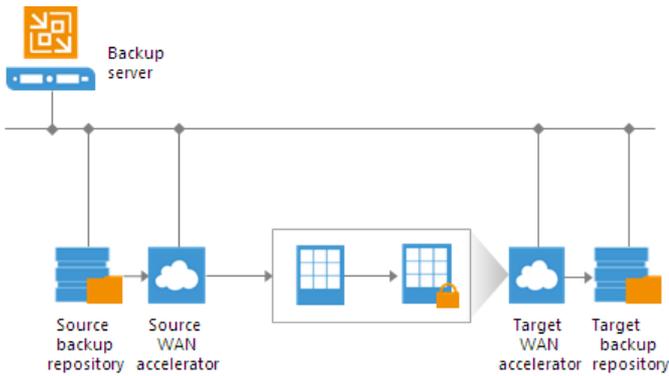
Over WAN Accelerators

WAN accelerators require reading data on the target side to perform such operations as global data deduplication, backup health check and so on. For this reason, if you use WAN accelerators for backup copy jobs, the encryption process is performed on the target side.

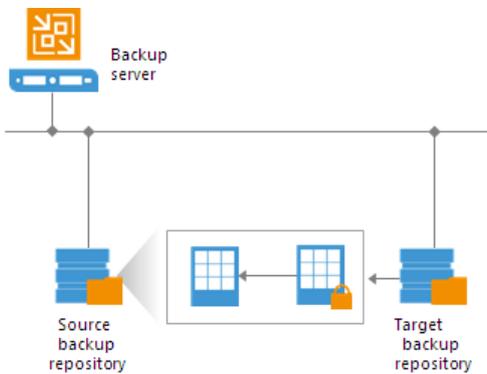
The backup copy job processing over WAN accelerators includes the following steps:

1. You enable encryption for a backup copy job and specify a password.
2. Veeam Backup & Replication generates necessary keys to protect backup files produced by the backup copy job.
3. Data blocks are passed to the target backup repository in the unencrypted format.

- Received data blocks are encrypted on the target site and stored to a resulting backup file on the target backup repository.



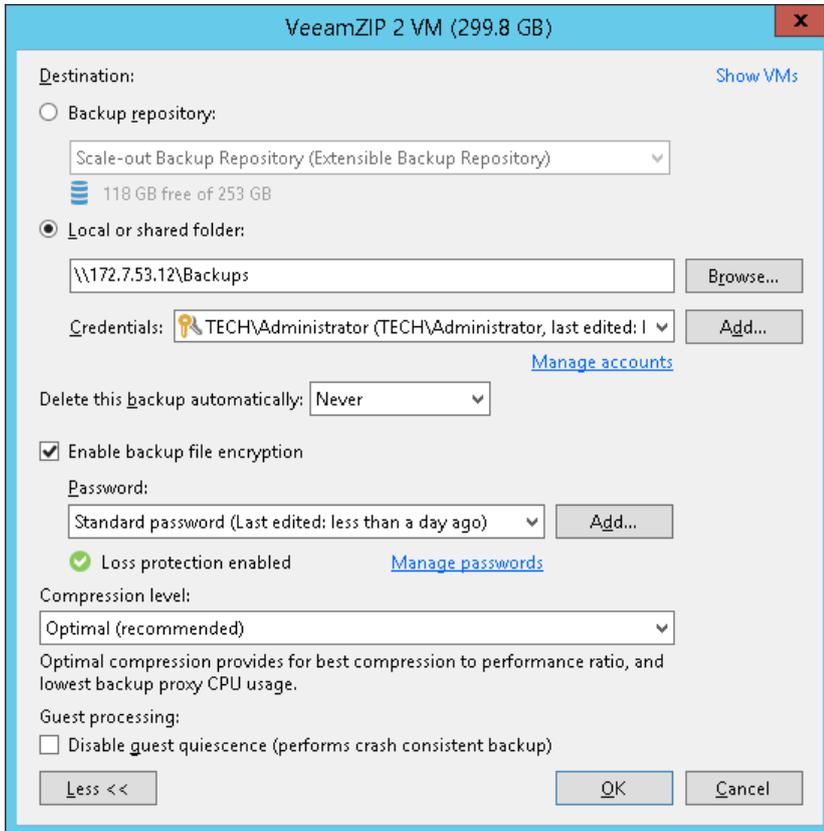
The restore process in this case does not differ from that for backup jobs. Veeam Backup & Replication retrieves data blocks from the backup file on the target backup repository, sends them to the source side and decrypts them on the source side.



When transporting data between WAN accelerators that face external networks, Veeam Backup & Replication encrypts the network traffic by default. For network traffic encryption, Veeam Backup & Replication uses the 256-bit Advanced Encryption Standard (AES). For more information, see [Enabling Network Data Encryption](#).

VeeamZIP Encryption

If you want to create an encrypted VeeamZIP file, you should enable the encryption option and specify a password in VeeamZIP task options.



Data processing during VeeamZIP file creation and restore from a VeeamZIP file does not differ from that of a backup job.

Tape Encryption

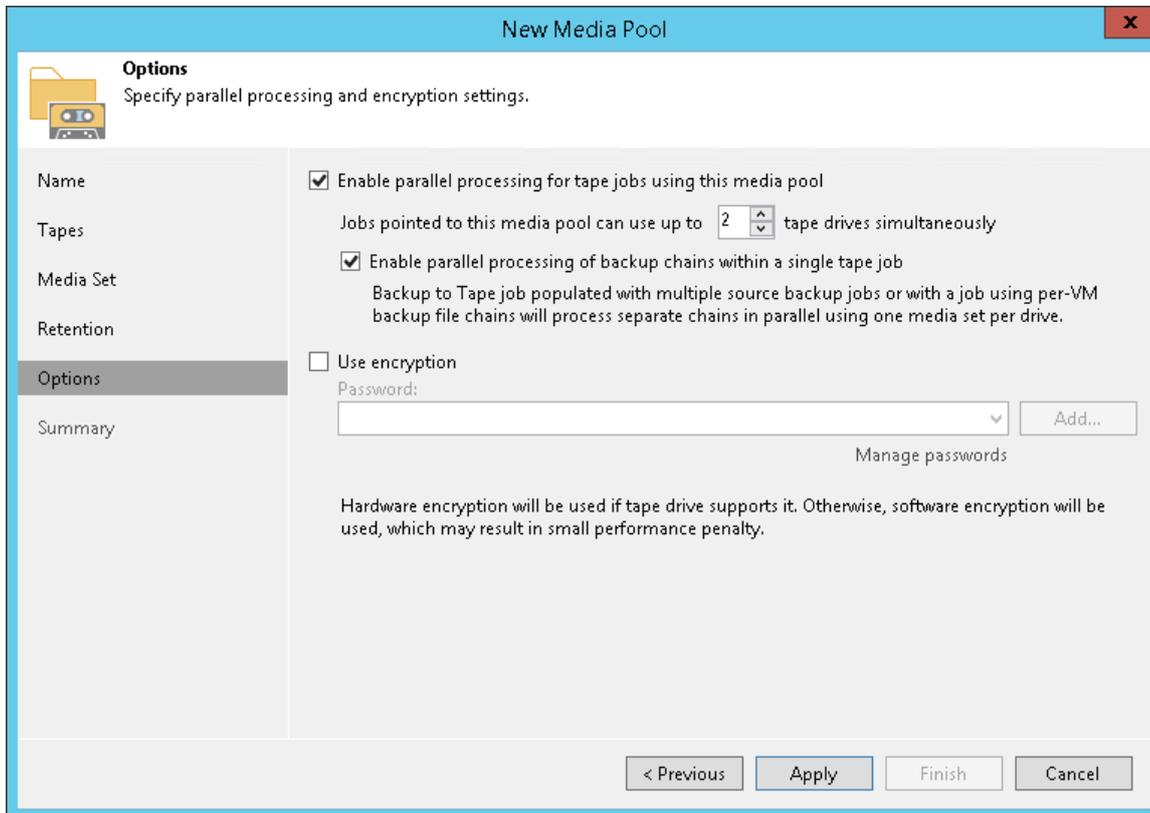
Veeam Backup & Replication supports two types of encryption for tape media:

- Hardware level: library- and driver-managed encryption mechanisms provided by the tape vendor
- Software level: the encryption mechanism provided by Veeam Backup & Replication

Hardware encryption has a higher priority. If hardware encryption is enabled for the tape media, Veeam Backup & Replication automatically disables its software encryption mechanism for such tape libraries. The Veeam encryption mechanism can only be used if hardware encryption is disabled at the tape device level or not supported.

To use the Veeam encryption mechanism, you need to enable encryption at the level of media pool. In this case, Veeam Backup & Replication will encrypt data for all jobs that use tapes from this media pool. Encryption is supported for both types of tape jobs:

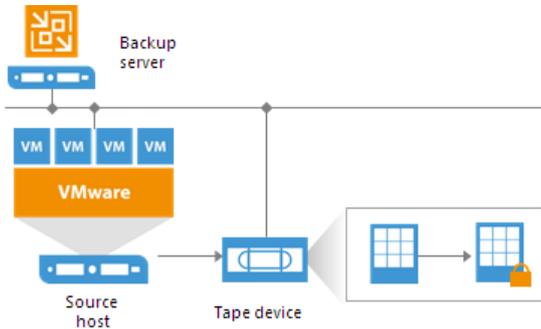
- Backup to tape jobs
- File to tape jobs



Encryption of data on tapes includes the following steps:

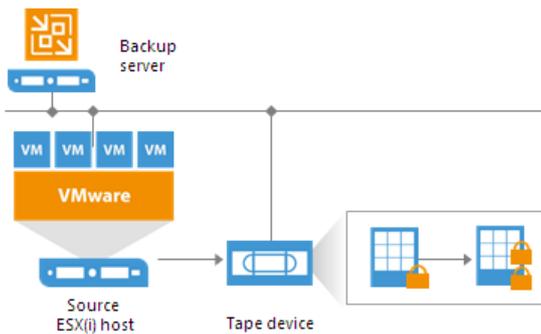
1. You enable encryption for a media pool and specify a password.
2. You select the media pool as a target for a backup to tape or file to tape job.
3. Veeam Backup & Replication generates the necessary keys to protect data archived to tape.

- During the backup to tape or file to tape job, the key is passed to the target side. In case of hardware encryption, Veeam Backup & Replication passes the key to the tape device, and the tape device uses its mechanism to encrypt data on tapes. In case of software encryption, Veeam Backup & Replication passes the keys to the tape server, and encrypts data when it is archived to tape.



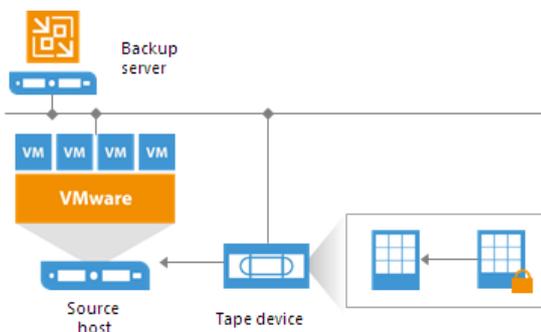
Backup to tape jobs allow double encryption. The backup to tape job uses a backup file as a source of data. If the backup file is encrypted with the initial backup job and the encryption option is enabled for the backup to tape job, too, the resulting backup file will be encrypted twice. To decrypt such backup file, you will need to subsequently enter two passwords:

- Password for the initial backup job
- Password for the media pool



Restore of encrypted data from tape includes the following steps:

1. You insert tape with encrypted data into the tape drive and perform tape catalogization. The catalogization operations lets Veeam Backup & Replication understand what data is written to tape.
2. You provide a password to decrypt data archived to tape.
3. Veeam Backup & Replication uses the provided password to generate a user key and unlock the subsequent keys for data Veeam Backup & Replication retrieves data blocks from encrypted files on tapes and decrypts them.



Encryption Best Practices

To guarantee the flawless process of data encryption and decryption, consider the following recommendations.

Password

1. Use strong passwords that are hard to crack or guess:
 - The password must be at least 8 characters long.
 - The password must contain uppercase and lowercase characters.
 - The password must be a mixture of alphabetic, numeric and punctuation characters.
 - The password must significantly differ from the password you used previously.
 - The password must not contain any real information related to you, for example, date of birth, your pet's name, your logon name and so on.
2. Provide a meaningful hint for the password that will help you recall the password. The hint for the password is displayed when you import an encrypted file or tape to the backup server and attempt to unlock it.
3. Keep passwords in the safe place. If you lose or forget your password, you will not be able to recover data from backups or tapes encrypted with this password, unless you use Enterprise Manager keys in the encryption process.
4. Change passwords for encrypted jobs regularly. Use of different passwords helps increase the encryption security level.

Data recovery without a password and Enterprise Manager keys

1. If you use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication, connect backup servers to Veeam Backup Enterprise Manager. In this case, Veeam Backup & Replication will employ Enterprise Manager keys in the encryption process, which will let you to recover data from encrypted backups and tapes even if the password is lost or forgotten. For more information, see [Decrypting Data Without Password](#).
2. Create and activate new Enterprise Manager keysets regularly. When you activate a keyset, the public Enterprise Manager key is automatically propagated to backup servers connected to Veeam Backup Enterprise Manager and used for encrypted jobs on these servers.
3. Create backup copies of Enterprise Manager keysets and keep them in a safe place. If your installation of Veeam Backup Enterprise Manager goes down for some reason, you will lose private Enterprise Manager keys. As a result, you will not be able to use the Veeam Backup Enterprise Manager functionality to recover data from backups and tapes without a password. For more information, see [Decrypting Data Without Password](#).

Encryption for Existing Jobs

If you enable encryption for an existing job, during the next job session Veeam Backup & Replication will create a full backup file. The created full backup file and subsequent incremental backup files in the backup chain will be encrypted with the specified password.

NOTE:

After enabling or disabling encryption for an existing backup copy job you will need to create an active full backup manually. For more information, see [Creating Active Full Backups](#).

Encryption is not retroactive. If you enable encryption for an existing job, Veeam Backup & Replication does not encrypt the previous backup chain created with this job. If you want to start a new chain so that the unencrypted previous chain can be separated from the encrypted new chain, follow this scenario: <https://www.veeam.com/kb1885>.

If you change the password for the already encrypted job, during the next job session Veeam Backup & Replication will create a new incremental backup file. The created backup file and subsequent backup files in the backup chain will be encrypted with the new password.

NOTE:

To unlock a backup encrypted with several passwords, you must decrypt it in the following manner:

- If you import a metadata file (VBM), provide the latest password that was used to encrypt files in the backup chain.
- If you import a full backup file (VBK), provide the whole set of passwords that were used to encrypt files in the backup chain.

For more information, see [Decrypting Data with Password](#).

Restoring Data from Encrypted Backups

When you restore data from an encrypted backup, Veeam Backup & Replication performs data decryption automatically in the background or requires you to specify a password.

- If encryption keys required to unlock the backup file are available in the configuration database, you do not need to specify the password. Veeam Backup & Replication uses keys from the database to unlock the backup file. Data decryption is performed in the background, and data restore from the encrypted backup does not differ from that from an unencrypted one.

Automatic backup file decryption is performed if the following conditions are met:

1. You encrypt and decrypt the backup file on the same backup server that uses the same configuration database.
 2. The backup is not removed from the Veeam Backup & Replication console.
- If encryption keys are not available in the configuration database, you can restore data from the encrypted backup with the following methods:
 - You can provide a password or a set of passwords to unlock an encrypted file. For more information, see [Decrypting Data with Password](#).
 - You can use Veeam Backup Enterprise Manager to unlock an encrypted file without a password. For more information, see [Decrypting Data Without Password](#).

Decrypting Data with Password

To unlock an encrypted file, you must specify a password. The password must be the same as the password that was used to encrypt the backup file.

To decrypt a backup file:

1. Import an encrypted backup file to the Veeam Backup & Replication console. After the import, the encrypted backup will appear under the **Backups > Disk (encrypted)** node in the inventory pane.
2. In the inventory pane, select **Disk (encrypted)**.
3. In the working area, select the imported backup and click **Specify Password** on the ribbon or right-click the backup and select **Specify password**.
4. In the **Description** field of the **Specify Password** window, Veeam Backup & Replication displays a hint for the password that was used to encrypt the backup file. Use the hint to recall the password.
5. In the **Password** field, enter the password for the backup file.

If you changed the password one or several times while the backup chain was created, you must enter passwords in the following manner:

- If you select a metadata file (VBM) for import, you must specify the latest password that was used to encrypt files in the backup chain.
- If you select a full backup file (VBK) for import, you must specify the whole set of passwords that were used to encrypt files in the backup chain.

If you enter correct passwords, Veeam Backup & Replication will decrypt the backup file. The backup will be moved under the **Backups > Disk (imported)** node in the inventory pane. You can perform restore operations with the backup file in a regular manner.

NOTE:

If you use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication and the backup servers are connected to Veeam Backup Enterprise Manager, you can recover data from an encrypted backup even if the password is lost. For more information, see [Decrypting Data Without Password](#).



Decrypting Data Without Password

If you have lost or forgotten a password, you can unlock an encrypted file with the help of Veeam Backup Enterprise Manager.

You can restore data without a password only if your backup infrastructure meets the following conditions:

1. You use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication.
2. The backup server on which you encrypted data is connected to Veeam Backup Enterprise Manager.
3. The backup server on which you generate a request for data decryption is connected to Veeam Backup Enterprise Manager.

IMPORTANT!

Backup servers that you use for data decryption must be connected to the same instance of Veeam Backup Enterprise Manager. If you connect a backup server to several instances of Veeam Backup Enterprise Manager, this may cause unexpected behavior, and the decryption process may fail.

The restore process is accomplished with the help of two wizards that run on two servers:

1. The **Encryption Key Restore** wizard on the backup server.
2. The **Password Recovery** wizard on the Veeam Backup Enterprise Manager server.

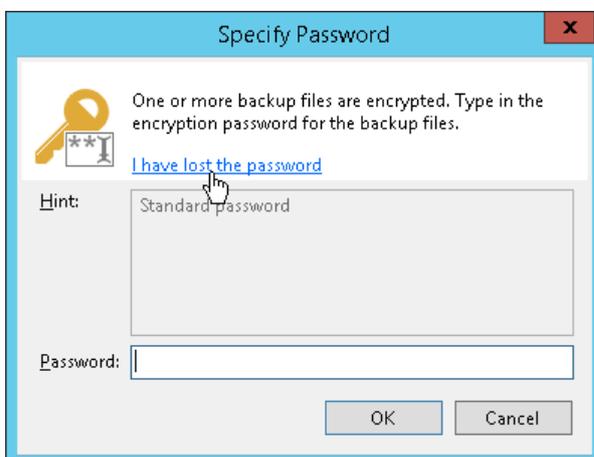
To restore encrypted data without a password:

1. [Create a request for data restore](#)
2. [Process the request in Veeam Backup Enterprise Manager](#)
3. [Complete the key restore process](#)

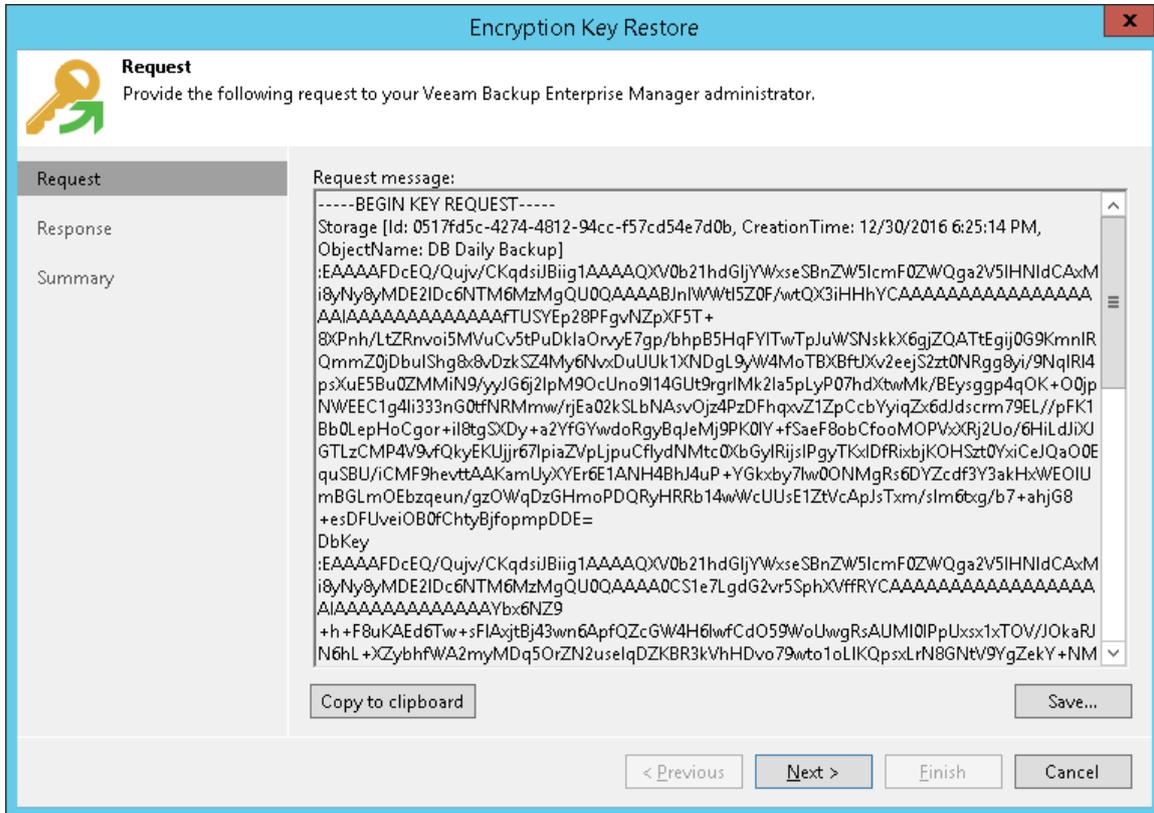
Step 1. Create Request for Data Restore

This procedure is performed by the Veeam Backup Administrator on the backup server.

1. Import encrypted backup to the Veeam Backup & Replication console.
2. Select the imported backup and click **Specify Password** on the ribbon or right-click the backup and select **Specify password**.
3. In the **Specify Password** window, click the **I have lost the password** link.



4. Veeam Backup & Replication will launch the **Encryption Key Restore** wizard. At the **Request** step of the wizard, review the generated request for data recovery. Use buttons at the bottom of the wizard to copy the request to the Clipboard or save the request to a text file.
5. Send the copied request by email or pass it in any other way to the Veeam Backup Enterprise Manager Administrator.



TIP:

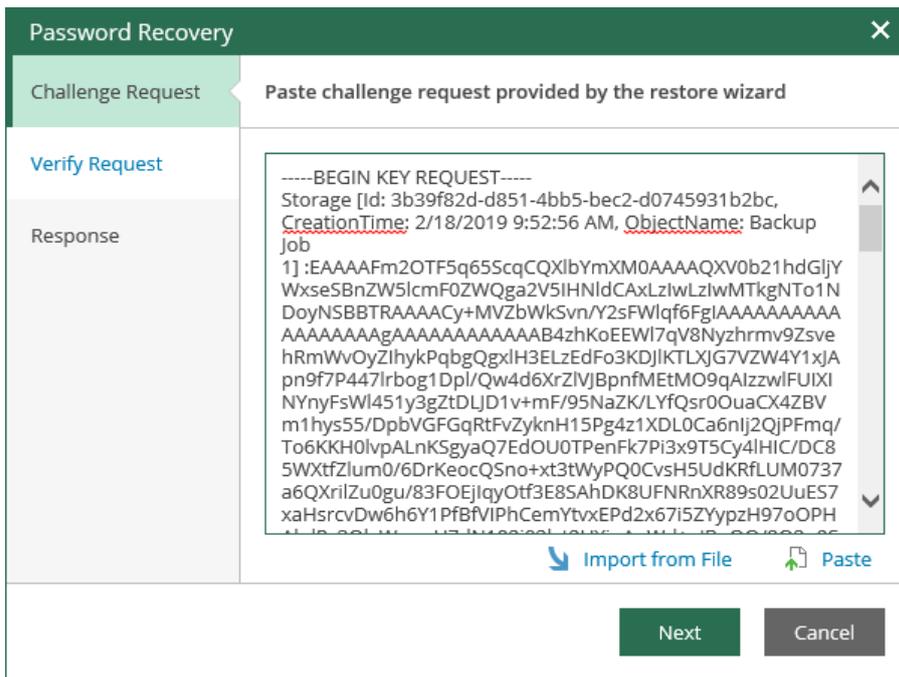
You can close the **Encryption Key Restore** wizard on the backup server and start it anew when you receive a response from the Veeam Backup Enterprise Manager Administrator.

Step 2. Process Request in Veeam Backup Enterprise Manager

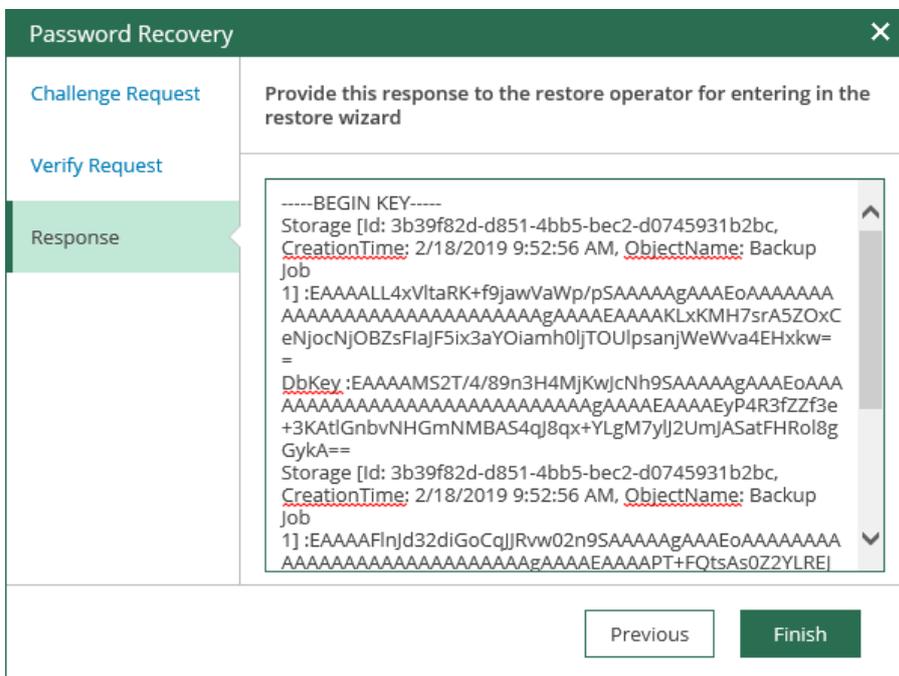
This procedure is performed by the Veeam Backup Enterprise Manager Administrator on the Veeam Backup Enterprise Manager server.

1. Copy the obtained request to the Clipboard.
2. In Veeam Backup Enterprise Manager, go to the **Configuration > Key Management** section.
3. Click **Password Recovery** at the top of the section to open the **Password Recovery** wizard.

- Paste the request that you have received from the Veeam Backup Administrator. You can use the **[CTRL+V]** key combination or click **Paste** at the bottom of the wizard.



- Follow the next steps of the wizard. At the **Response** step of the wizard, copy the text displayed in the wizard to the Clipboard.
- Send the copied response by email or pass it in any other way to the Veeam Backup Administrator working on the backup server.

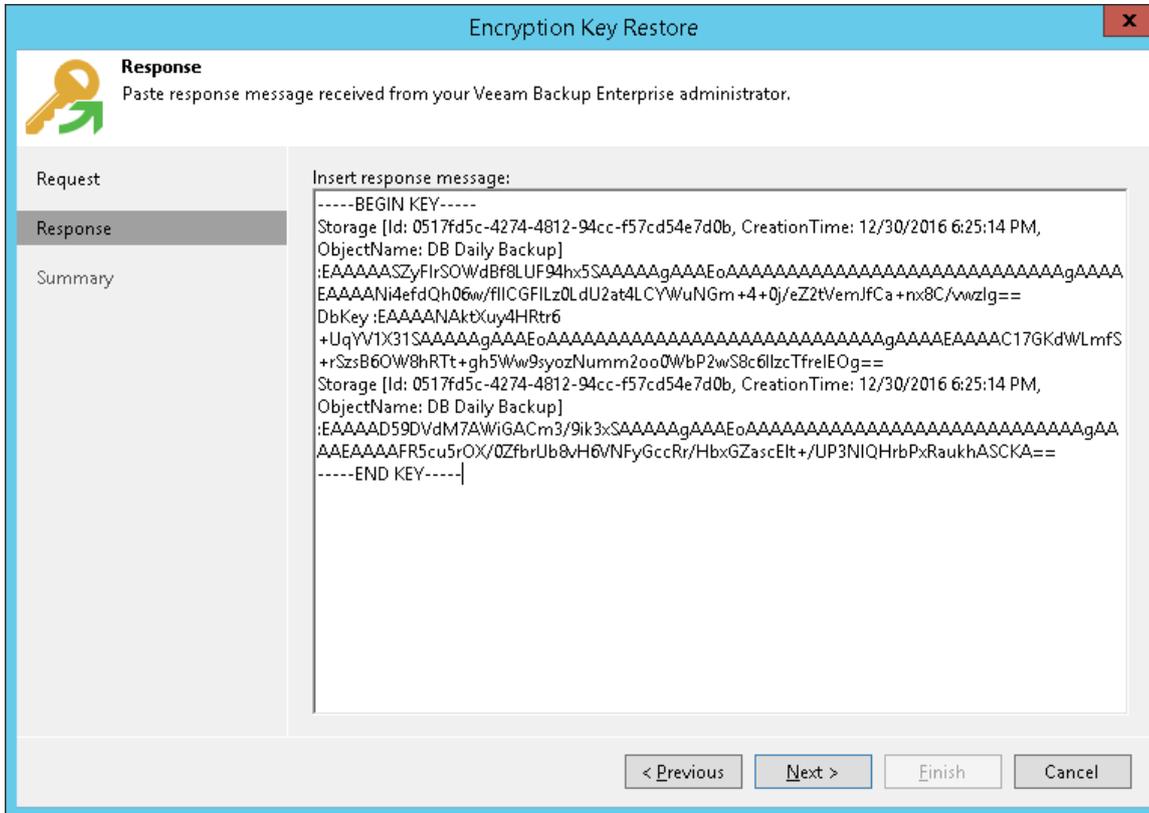


Step 3. Complete Key Restore Process

This procedure is performed by the Veeam Backup Administrator on the backup server.

- In Veeam Backup & Replication, get back to the **Encryption Key Restore** wizard.

2. Enter the copied response to the text window at the **Response** step of the **Encryption Key Restore** wizard.
3. Follow the next steps of the wizard. At the last step, click **Finish**. Veeam Backup & Replication will retrieve the decrypted storage keys from the response, apply them to the encrypted file and unlock the file content.



Restoring Encrypted Data from Tapes

When you restore data from encrypted tapes, Veeam Backup & Replication 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 & Replication database, you do not need to enter the password to decrypt the tape. Veeam Backup & Replication 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:

- You encrypt and decrypt tapes on the same Veeam backup server.
 - The tape is loaded to the tape library and information about this tape is available in the catalog.
 - 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 & Replication database, you can restore data from encrypted tapes with the following methods:
 - You can provide a password or a set of passwords to unlock the encrypted tape. For more information, see [Decrypting Tapes with Password](#).
 - You can use Veeam Backup Enterprise Manager to unlock the encrypted tape without a password. For more information, see [Decrypting Data Without 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 & Replication 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 & Replication 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 & Replication 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 & Replication 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 & Replication 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 & Replication needs to additionally catalog files on imported tapes.

If you enter a correct password, Veeam Backup & Replication 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.

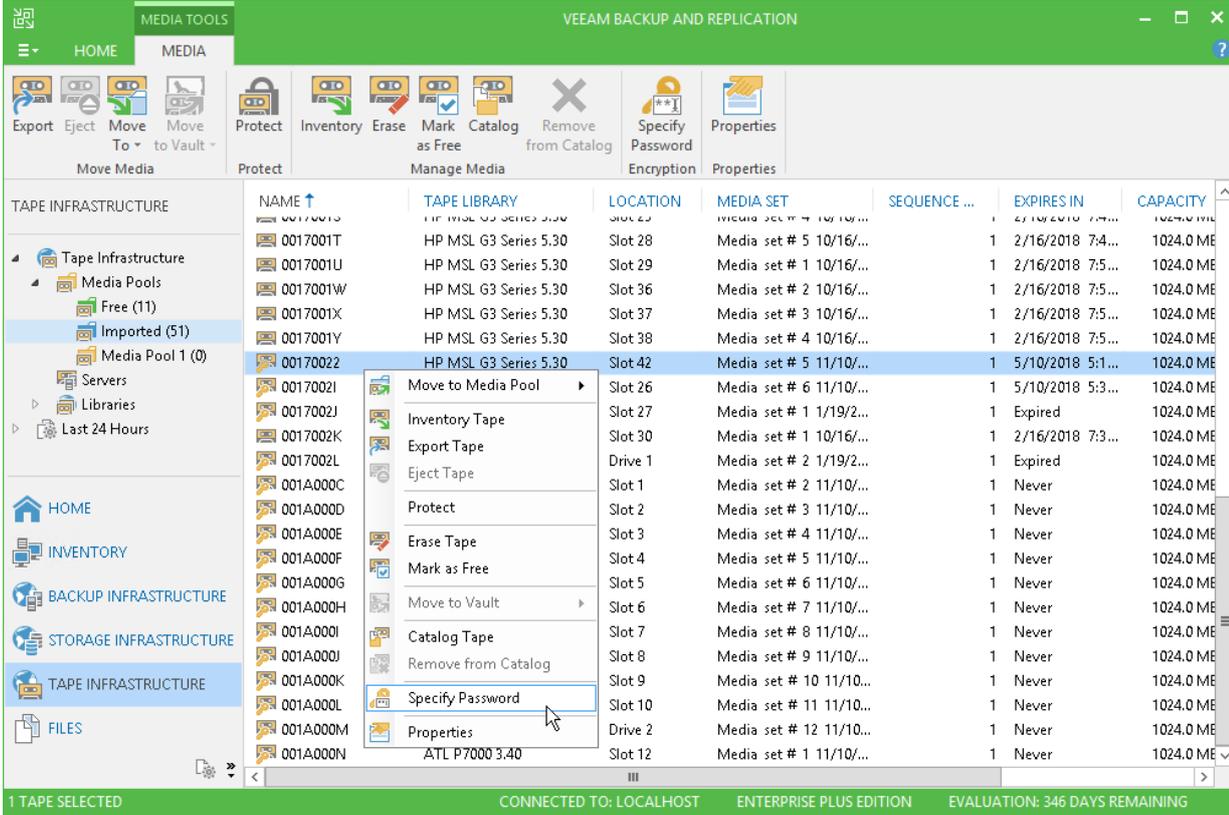
If you import a backup file from tape and the backup file was encrypted twice, with the initial backup job and with the backup to tape job, you must sequentially specify two passwords:

1. Password that was used to encrypt tapes in the media pool.
2. Password for the primary backup job.

After you enter the first password, backups from the tape will be moved under the **Backup > Encrypted** node in the inventory pane. You must then enter the second password to decrypt the backup and get access to its content.

NOTE:

If you use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication and your Veeam backup servers are connected to Veeam Backup Enterprise Manager, you can recover data from encrypted tapes even if the password is lost. For more information, see [Decrypting Data Without Password](#).



Decrypting Tapes Without Password

If you have lost or forgotten a password, you can unlock encrypted tapes with the help of Veeam Backup Enterprise Manager.

You can restore data from tapes without a password only if your backup infrastructure meets the following conditions:

1. You use Enterprise or Enterprise Plus Edition of Veeam Backup & Replication.
2. Veeam backup server on which you encrypted tapes is added to Veeam Backup Enterprise Manager.
3. Veeam backup server on which you generate a request for data decryption is added to Veeam Backup Enterprise Manager.

The restore process is accomplished with the help of two wizards that run on two servers:

1. The **Encryption Key Restore** wizard on the Veeam backup server.
2. The **Password Recovery** wizard on the Veeam Backup Enterprise Manager server.

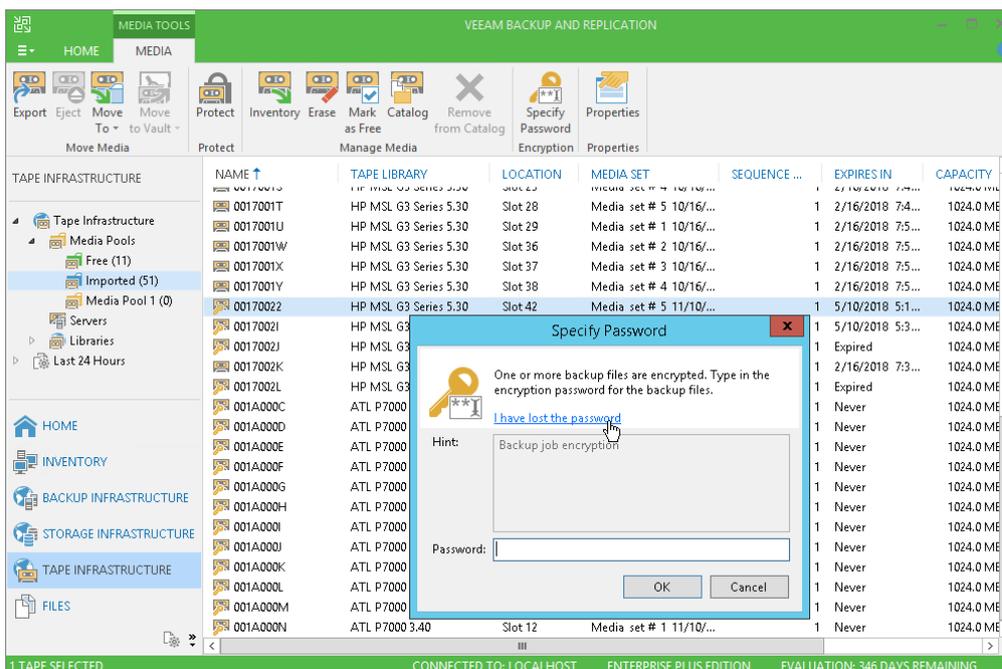
To restore encrypted data from tapes without a password:

1. [Create a request for data restore.](#)
2. [Process the request in Veeam Backup Enterprise Manager.](#)
3. [Complete the key restore process.](#)

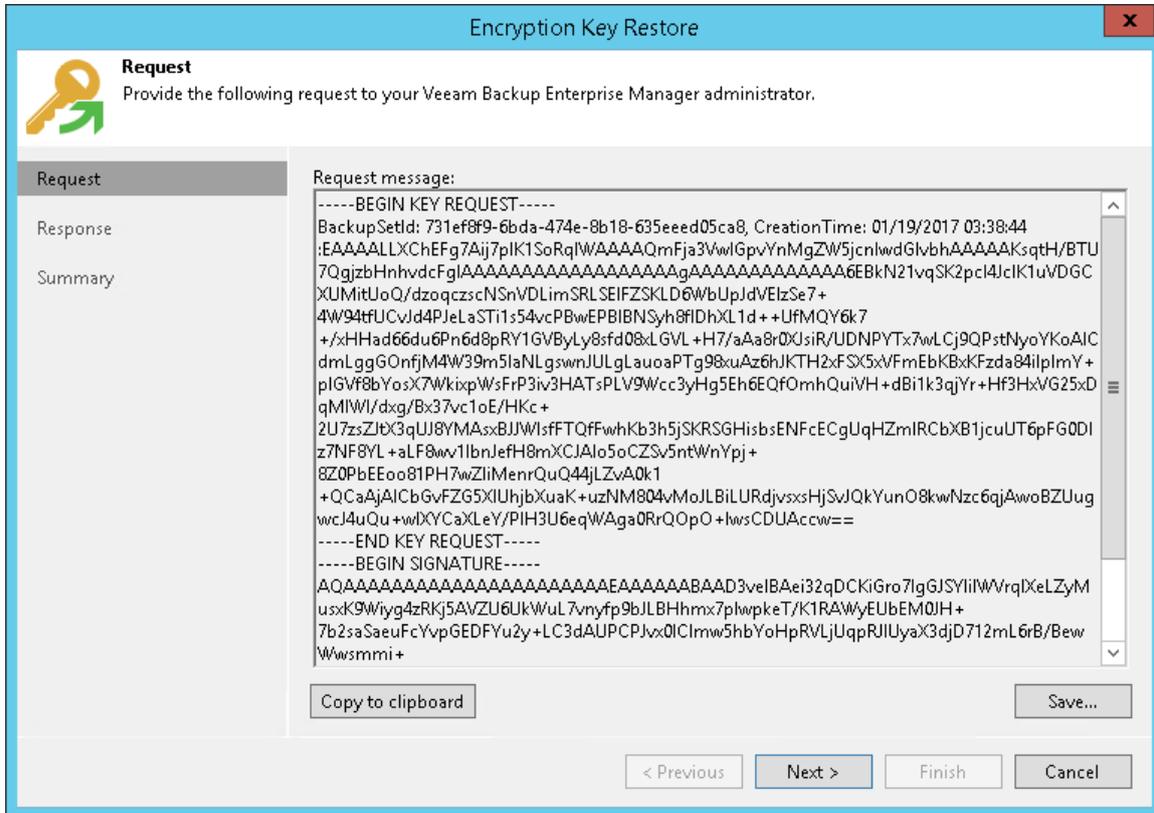
Step 1. Create Request for Data Restore

This procedure is performed by the Veeam Backup Administrator on the Veeam backup server.

1. Import encrypted tapes to the Veeam backup server.
2. Select the imported tape and click **Specify Password** on the ribbon or right-click the tape and select **Specify password**.
3. In the **Specify Password** window, click the **I have lost the password** link.



- Veeam Backup & Replication will launch the **Encryption Key Restore** wizard. At the **Request** step of the wizard, review the generated request for data recovery. Use buttons at the bottom of the wizard to copy the request to the Clipboard or save the request to a text file.
- Send the copied request by email or pass it in any other way to the Veeam Backup Enterprise Manager Administrator.



TIP:

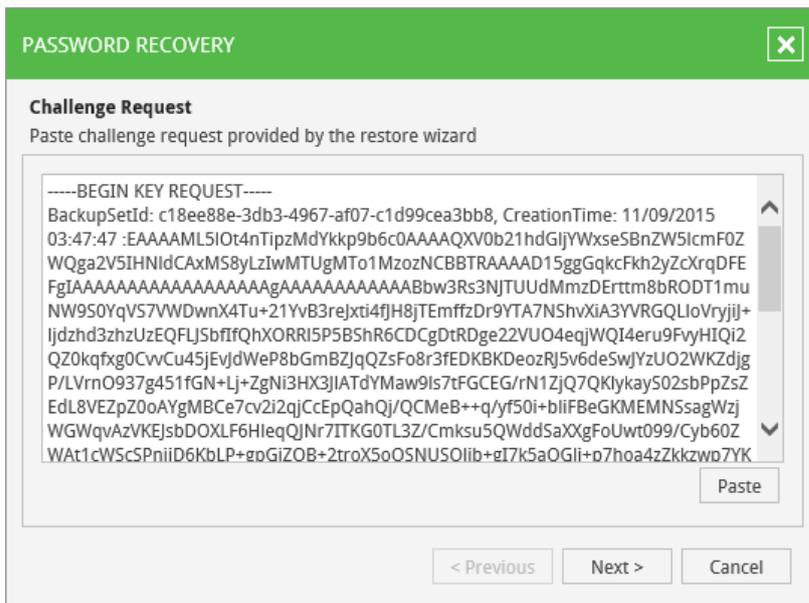
You can close the **Encryption Key Restore** wizard on the Veeam backup server and start it anew when you receive a response from the Veeam Backup Enterprise Manager Administrator.

Step 2. Process Request in Veeam Backup Enterprise Manager

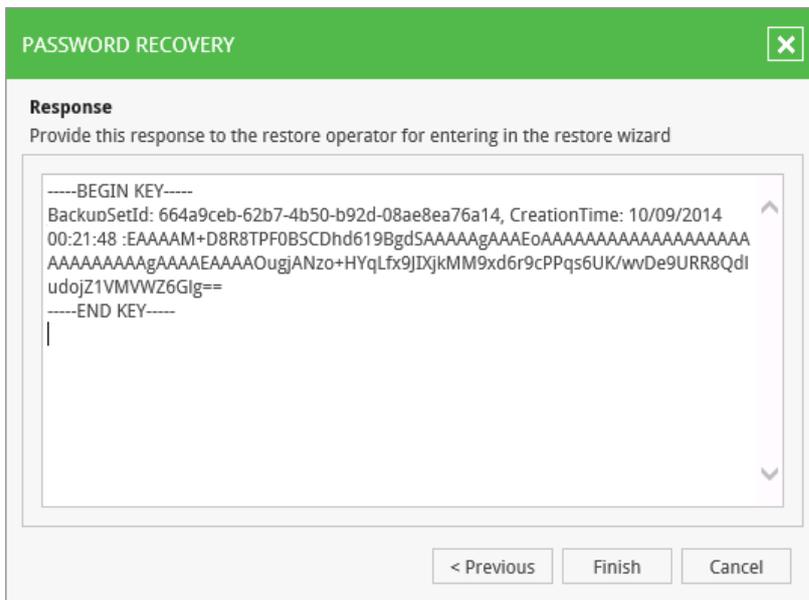
This procedure is performed by the Veeam Backup Enterprise Manager Administrator on the Veeam Backup Enterprise Manager server.

- Copy the obtained request to the Clipboard.
- In Veeam Backup Enterprise Manager, go to the **Configuration > Key Management** section.
- Click **Password Recovery** at the top of the section to open the **Password Recovery** wizard.

- Paste the request that you have received from the Veeam Backup Administrator. You can use the **[CTRL+V]** key combination or click **Paste** at the bottom of the wizard.



- Follow the next steps of the wizard. At the **Response** step, copy the text displayed in the wizard to the Clipboard.
- Send the copied response by email or pass it in any other way to the Veeam Backup Administrator working on the Veeam backup server.

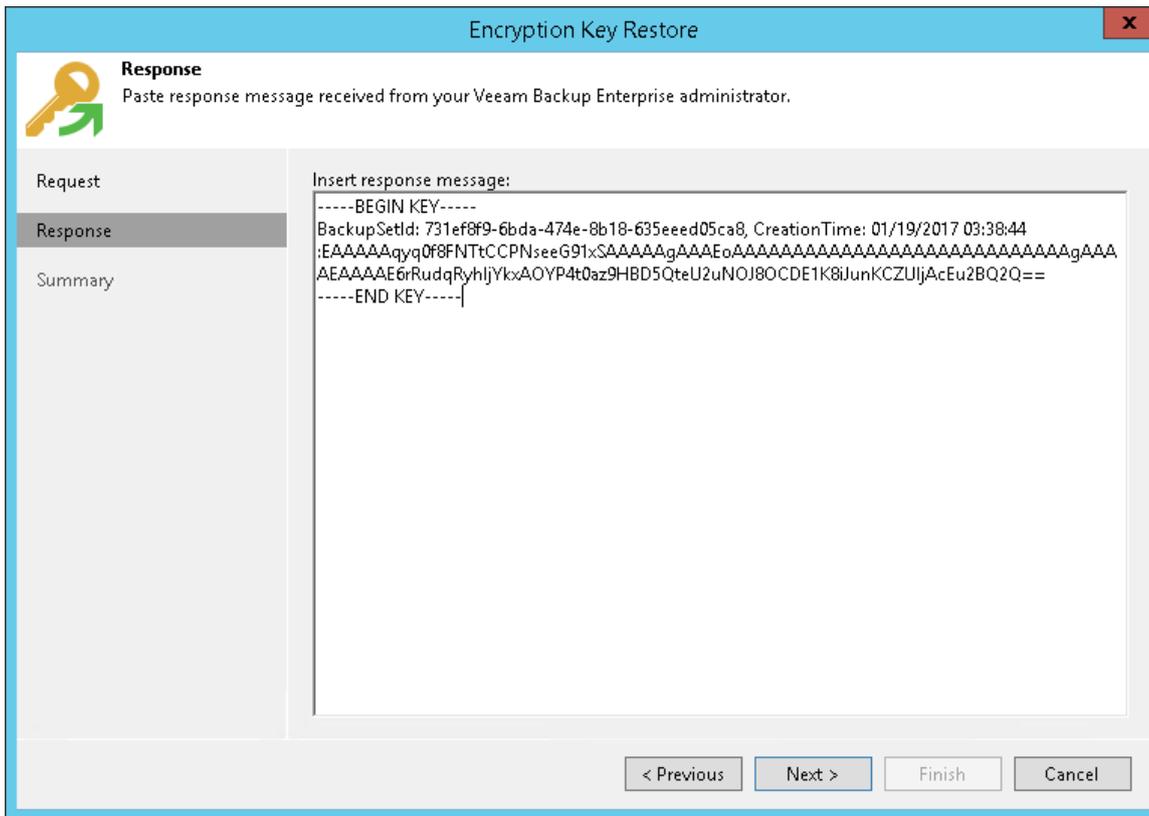


Step 3. Complete Key Restore Process

This procedure is performed by the Veeam Backup Administrator on the Veeam backup server.

- In Veeam Backup & Replication, get back to the **Encryption Key Restore** wizard.
- Enter the copied response to the text window at the **Response** step of the **Encryption Key Restore** wizard.

3. Follow the next steps of the wizard. At the last step, click **Finish**. Veeam Backup & Replication will retrieve the decrypted storage keys from the response, apply them to the encrypted tape and unlock the tape content.



Integration with Storage Systems

To build the data protection and disaster recovery strategy, you can use capabilities of storage systems that host VM disks. Veeam Backup & Replication integrates with storage systems and offers advanced functionality that helps you decrease impact from backup and replication operations on the production environment and significantly improve RPOs.

For more information, see the [Integration with Storage Systems Guide](#).

Tape Devices Support

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

For more information, see the [Tape Devices Support Guide](#).

Veeam Agent Management

Veeam Backup & Replication lets you deploy and manage Veeam Agent for Microsoft Windows and Veeam Agent for Linux (Veeam Agents) on computers in your infrastructure.

For more information about Veeam Agents, see the [Veeam Agent Management Guide](#).

Veeam Cloud Connect

If you want to store your data in the cloud, you can connect to the service provider and write VM backups to cloud repositories or create VM replicas on cloud hosts.

For more information about Veeam Cloud Connect, see the [Veeam Cloud Connect Guide](#).

Advanced VMware vSphere Features

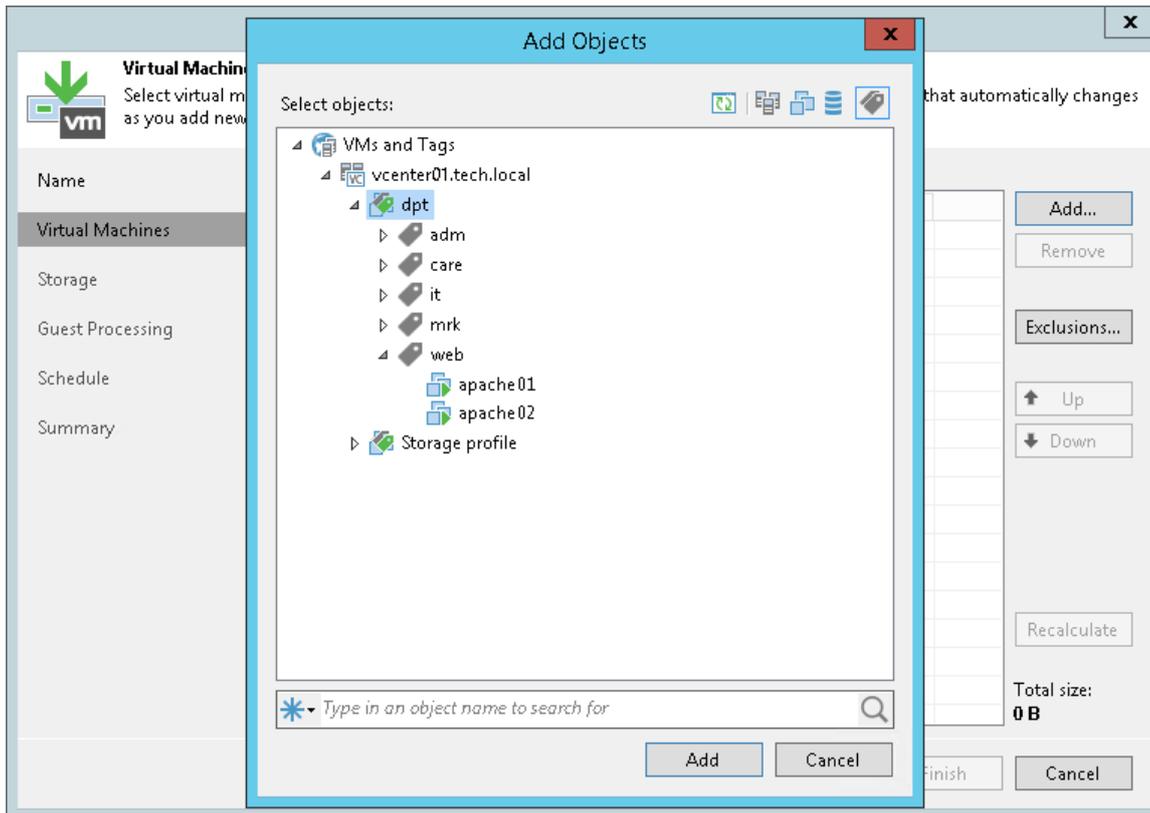
Veeam Backup & Replication lets you leverage the following VMware vSphere features and functionality during data protection and disaster recovery operations:

- [VM tags](#)
- [Encrypted VMs](#)
- [Storage policies](#)

VM Tags

If you use vCenter Server tags to categorize objects in the virtual infrastructure, you can filter objects that you add to data protection and disaster recovery jobs and tasks by these tags. Use of tags facilitates object management. You can quickly configure jobs and tasks for VMs that belong to a specific category, for example, a certain department or SLA level.

To add objects by tags, you must switch to the **VMs and Tags** view in the **Add Objects** window. Veeam Backup & Replication will display objects categorized by tags.



Requirements and Recommendations for VM Tags

When you work with tags in Veeam Backup & Replication, mind the following requirements and recommendations:

- The *VirtualCenter.FQDN* parameter in the **Advanced Settings** of vCenter Server must contain the real fully qualified domain name of the vCenter Server host.
- A certificate installed on vCenter Server must contain the real fully qualified domain name of the vCenter Server host.
- The fully qualified domain name of the vCenter Server host must be accessible and resolved to its IP (and vice versa) from machines on which Veeam Backup & Replication services are installed (at least the Veeam Backup Service and Veeam Broker Service).
- A user account used for specific data protection and disaster recovery operations must have sufficient permissions on the vCenter Server. For more information, see [Full VM Restore](#), [Replica Failback](#) and [Cumulative Permissions](#) sections in the Required Permissions guide.

- If VM tags are not displayed in the Veeam Backup & Replication console for some reason, try restarting VMware vSphere services that are responsible for the tags functionality. In VMware vSphere earlier than 6.5, you must restart the vCenter Inventory Service. Starting from VMware vSphere 6.5, vCenter Inventory Services functionality is replaced by the vCenter Content Library and other services that are part of vCenter Server 6.5.

When you upgrade to VMware vSphere 6.5, data from vCenter Inventory Service is migrated to the new database support services in vCenter Server 6.5. The vCenter Inventory Service may remain in the list of services, however, it is no longer used.

Limitations for VM Tags

The VM tags support functionality has the following limitation:

Veeam Backup & Replication ignores the cardinality setting for VM tag categories. For example, you create a tag category *Priority* and set cardinality to **One tag per object**. In the tag category, you create two tags: *Normal* and *High*. You assign the Normal tag to a VM folder and the *High* tag to a VM in this folder. If you now configure a job that will process objects with the *Normal* tag, the VM with the *High* tag will also be added to this job (since Veeam Backup & Replication regards that VMs and templates in the VM container inherit the tag assigned to the container).

To overcome this situation, you can add to the list of exclusions the tag assigned to objects that you do not want to process.

Encrypted VMs

Veeam Backup & Replication provides support for encrypted VMware vSphere VMs.

- [Backup of encrypted VMs](#)
- [Replication of encrypted VMs](#)
- [Restore of encrypted VMs](#)
- [Failback of encrypted VMs](#)

Backup of Encrypted VMs

Veeam Backup & Replication lets you back up encrypted VMs. The backup infrastructure must meet the following requirements:

- VM encryption instances must be preconfigured in the virtual infrastructure: you must set up the key management server, create the VM encryption policy and assign it to VMs in advance.
- The backup proxy used for backup must be working in the *Virtual appliance* transport mode or *Network* transport mode with SSL encryption enabled.
- The backup proxy working in the *Virtual appliance* transport mode must be deployed on an encrypted VM.

Replication of Encrypted VMs

Veeam Backup & Replication lets you replicate encrypted VMs. The backup infrastructure must meet the following requirements:

- VM encryption instances must be preconfigured in the virtual infrastructure: you must set up the key management server, create the VM encryption policy and assign it to VMs in advance.
- The backup proxy used for backup must be working in the *Virtual appliance* transport mode or *Network* transport mode with SSL encryption enabled.
- The backup proxy working in the *Virtual appliance* transport mode must be deployed on an encrypted VM.
- You must place disks and the configuration file of the VM replica on datastores to which the VM Encryption policy is assigned. To do this, at the **Destination** step of the wizard, click **Datastore** and select a datastore under the VM Encryption Policy.

NOTE:

Multi-OS file-level restore for encrypted VM replicas is not supported.

Restore of Encrypted VMs

Veeam Backup & Replication supports restore of encrypted VMs. You have the following restore options:

- You can back up an encrypted VM and restore it as encrypted.
- You can back up an encrypted VM and restore it as unencrypted.

- You can back up an unencrypted VM and restore it as encrypted.

To let Veeam Backup & Replication successfully restore an encrypted VMs, the backup infrastructure must meet the following requirements:

- VM encryption instances must be preconfigured in the virtual infrastructure: you must set up the key management server, create the VM encryption policy and assign it to VMs in advance.
- The backup proxy used for restore must be working in the *Virtual appliance* transport mode or *Network* transport mode with SSL encryption enabled.
- The backup proxy working in the *Virtual appliance* transport mode must be deployed on an encrypted VM.
- You must place VM disks on datastores to which the VM Encryption policy is assigned. To do this, at the **Datastore** step of the wizard, select a VM disk, click **Datastore** and select a datastore under the VM Encryption policy.

If a VM has several disks, you can optionally restore some disks as encrypted and some disks as unencrypted. Keep in mind, however, that the VM configuration file must always be placed on a datastore to which the VM Encryption policy is assigned.

Failback of Encrypted VMs

During failback, Veeam Backup & Replication lets you restore a VM as encrypted. To let Veeam Backup & Replication successfully restore an encrypted VMs, the backup infrastructure must meet the following requirements:

- VM encryption instances must be preconfigured in the virtual infrastructure: you must set up the key management server, create the VM encryption policy and assign it to VMs in advance.
- The backup proxy used for failback must be working in the *Virtual appliance* transport mode or *Network* transport mode with SSL encryption enabled.
- The backup proxy working in the *Virtual appliance* transport mode must be deployed on an encrypted VM.
- You must place VM disks on datastores to which the VM Encryption policy is assigned. To do this, at the **Datastore** step of the wizard, select a VM disk, click **Datastore** and select a datastore under the VM Encryption policy.

If a VM has several disks, you can optionally restore some disks as encrypted and some disks as unencrypted. Keep in mind, however, that the VM configuration file must always be placed on a datastore to which the VM Encryption policy is assigned.

Storage Profiles

During backup, Veeam Backup & Replication preserves information about the storage policy associated with the VM, and stores this information to the backup file or replica metadata. When you restore the VM to its original location, Veeam Backup & Replication also restores information about the VM storage policy. The restored VM gets automatically associated with the original storage policy.

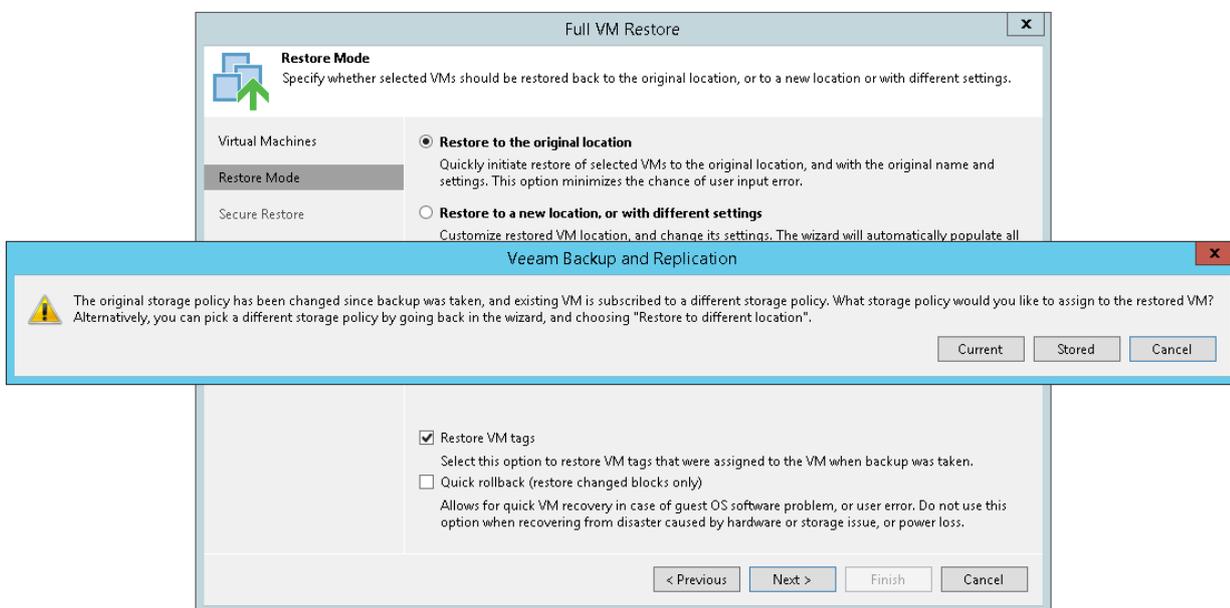
Veeam Backup & Replication restores the storage policy when you perform the following operations:

- Entire VM restore
- VM failback

Veeam Backup & Replication restores the storage policy only if you restore the VM to the original location. If you restore the VM to a new location, Veeam Backup & Replication does not preserve the storage policy for the VM.

In some cases, the original storage policy may be changed or missing by the time when you restore the VM. For example, the storage policy may be deleted, the original VM in the production environment may be associated with another storage policy and so on. In such situation, Veeam Backup & Replication displays a warning and lets you choose one of the following scenarios:

- Associate the VM with the current storage policy – the restored VM will be associated with the profile with which the original VM in the production environment is currently associated.
- Associate the VM with the default storage policy – the restored VM will be associated with the profile that is set as default for the target datastore.
- Associate the VM with the profile stored in the backup file – the restored VM will be associated with the profile that was assigned to the original VM at the moment of backup, and whose information is stored in the backup file.



Veeam Backup & Replication Utilities

You can use the following Veeam Backup & Replication utilities to perform advanced administration tasks in your backup infrastructure:

- [Extract.exe utility](#)
- [Veeam.Backup.DBConfig.exe utility](#)
- [Veeam backup validator](#)

Extract Utility

Veeam Backup & Replication comes with an extract utility that can be used to recover machines from backup files. The extract utility does not require any interaction with Veeam Backup & Replication and can be used as an independent tool on Linux and Microsoft Windows machines.

The extract utility can be helpful, for example, if it is written to the tape next to machine backup files. In this case, you get a possibility to recover machines from backups at any moment of time even if backups are removed from Veeam Backup & Replication or Veeam Backup & Replication is uninstalled at all.

IMPORTANT!

The extract utility does not work with backups that are stored on scale-out backup repositories.

The extract utility can be used in two interfaces:

- Graphic user interface (GUI)
- Command-line interface working in the [interactive](#) and [regular mode](#)

The extract utility is located in the installation folder of Veeam Backup & Replication, by default: `%PROGRAMFILES%\Veeam\Backup and Replication\Backup`. The folder contains three files for the extract utility:

- `Veeam.Backup.Extractor.exe` – utility working in GUI (can be used on Microsoft Windows machines only)
- `extract.exe` – utility working in the command-line interface, a version for Microsoft Windows
- `extract` – utility working in the command-line interface, a version for Linux

Using Extract Utility in GUI

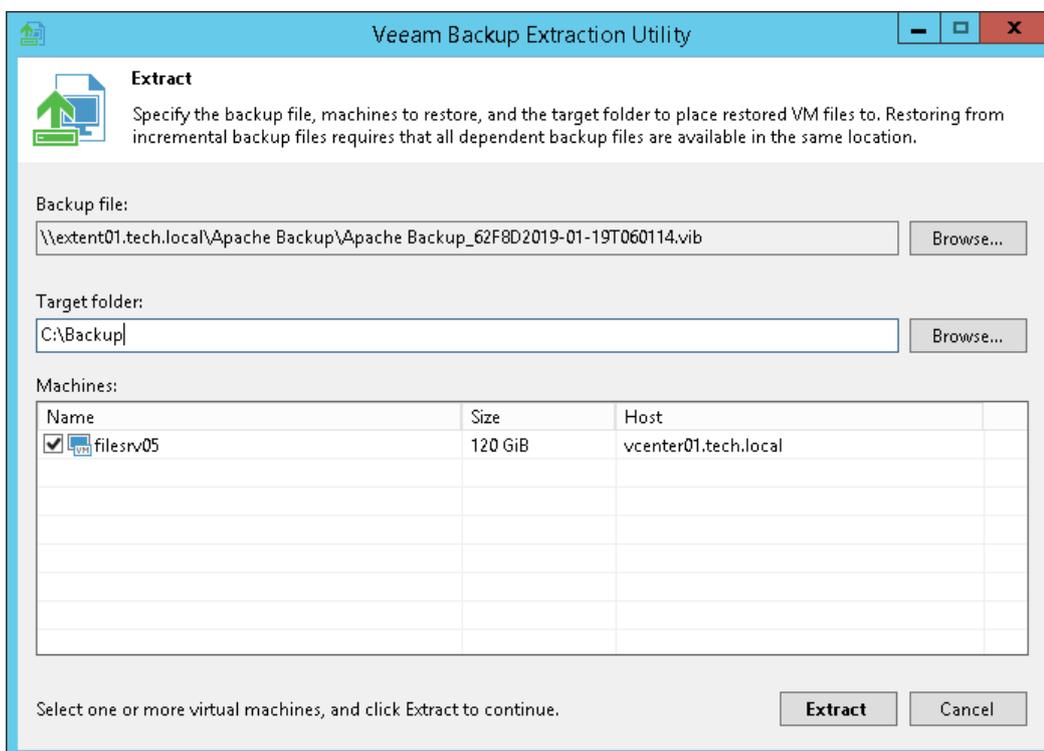
To restore machine data in the extract utility GUI:

1. Run the `Veeam.Backup.Extractor.exe` file from the installation folder of Veeam Backup & Replication.
2. In the **Backup file** field, specify a path to the backup file from which you want to restore machine data.
3. If the backup file is encrypted, the extract utility will require you to provide a password to unlock the backup file. Enter the password that was used for backup file encryption.
4. In the **Target folder** field, specify a path to the destination folder where machine data must be restored.
5. From the **Machines** list, select machines whose data you want to restore.
6. Click **Extract**. Machine data will be restored to the specified folder.

IMPORTANT!

If you restore machine data in the extract utility GUI, consider the following:

- The extract utility can be started on Microsoft Windows machines only.
- If you plan to start the extract utility on the machine other than the backup server, make sure that you copy the `Veeam.Backup.Extractor.exe` file together with the `extract.exe` file from the product installation folder and store these files to the same folder on the destination machine. In the opposite case, the extract utility will fail to start.



Using Extract Utility in Interactive Mode

To start the extract utility in the interactive mode, run the `extract.exe` file from the product installation folder(in case of a Linux machine, run the `extract` file).

You will have to sequentially enter the following arguments:

1. A path to the backup file from which the machine must be restored. After you enter the path, the extract utility will display a list of all machines included in the backup and their description.
2. A name of the machine that you want to restore. If there is more than one machine with the specified name in the backup, you will be asked to specify the host on which the backed up machine resides. If you want to restore all machines from the backup, press **[ENTER]**.
3. If the backup was encrypted, password that was used to encrypt the backup file.
4. An output directory to which machines must be restored. If you want to restore machines to the current directory, press **[ENTER]**.
5. The operation confirmation. Press **[Y]** on the keyboard to restore a machine to the directory you specified. If you want to abort the operation, press **[ENTER]**.

Using Extract Utility from Command Line

If you run the extract utility from the command line, you can perform the following actions:

- [Run the extract utility in the interactive mode](#)
- [Display help information for the utility usage](#)
- [Display the list of all VMs in the backup file](#)
- [Getting encryption status of a backup file](#)
- [Restore all or selected VMs from the backup](#)

Running Extract Utility in Interactive Mode

This command runs the extract utility in the interactive mode.

Syntax

```
extract.exe [-password backupkey] [pathtobackup]
```

Parameters

Parameter	Description	Required/Optional
password	Password for the encrypted backup file.	Required for encrypted backup files
pathtobackup	Path to the backup file from which machines must be restored.	Optional

Displaying Help Information for Utility Usage

This command prints all variants of the extract utility usage along with required and optional parameters.

Syntax

```
extract.exe -help
```

Displaying List of Machines in Backup

This command displays the list of all machines in the backup file from which you want to perform restore.

Syntax

```
extract.exe -dir [-vm vmname] [-host hostname] [-password backupkey] pathtobackup
```

Parameters

Parameter	Description	Required/Optional
vm	Name of the machine that you want to restore. Use this parameter to filter machines in the backup.	Optional
host	Name of the host on which the initial machine resides. Specify this parameter to filter machines that have the same name but reside on different hosts. Note: This parameter must be specified if the <code>vm</code> parameter is used.	Optional
password	Password for the encrypted backup file.	Required for encrypted backup files
pathtobackup	Path to the backup file from which the machine must be restored.	Required

Getting Encryption Status of Backup File

This command gets the encryption status of the backup file: encrypted or not encrypted.

Syntax

```
extract.exe -getEncryptionStatus pathtobackup
```

Parameters

Parameter	Description	Required/Optional
pathtobackup	Path to the backup file from which the machine must be restored.	Required

Restoring VMs from Backup

This command restores data for all machines or for the selected machine from the backup file.

Syntax

```
extract.exe -restore [-vm vmname] [-host hostname] [-password backupkey] pathtobackup  
[outputdir]
```

Parameters

Parameter	Description	Required/Optional
vm	Name of the machine that you want to restore. Use this parameter to filter machines in the backup. If you want to restore all machines from the backup file, do not specify this parameter.	Optional
host	Name of the host on which the initial machine resides. Specify this parameter to filter machines that have the same name but reside on different hosts. Note: This parameter must be specified if the <code>vm</code> parameter is used.	Optional
pathtobackup	Path to the backup file from which the machine must be restored.	Required
password	Password for the encrypted backup file.	Required for encrypted backup files
outputdir	Path to the directory to which machine data must be restored. If this parameter is not specified, the machine will be restored to the current directory.	Optional

Veeam.Backup.DBConfig.exe Utility

Veeam Backup & Replication comes with the `Veeam.Backup.DBConfig.exe` utility that allows you to manage connection settings for Veeam Backup & Replication and/or Veeam Backup Enterprise Manager configuration database. Using this utility, you can:

- Connect to a different database on the same or another Microsoft SQL Server instance. If you specify a database that does not exist yet, it will be created on the selected server.
- Change authentication method for database connection. Possible methods are Microsoft Windows authentication and Microsoft SQL server authentication.

NOTE:

The `Veeam.Backup.DBConfig.exe` utility supports only connection to configuration databases of the current version.

Using Veeam.Backup.DBConfig.exe Utility

You can launch the `Veeam.Backup.DBConfig.exe` utility from the **Start** menu by clicking **Configuration Database Connection Settings**.

Alternatively, you can use the `Veeam.Backup.DBConfig.exe` file located in the installation folders for Veeam Backup & Replication or Veeam Backup Enterprise Manager. By default, the installation folders have the following paths:

- `%PROGRAMFILES%\Veeam\Backup and Replication\Backup` – for Veeam Backup & Replication
- `%PROGRAMFILES%\Veeam\Backup and Replication\Enterprise Manager` – for Veeam Backup Enterprise Manager

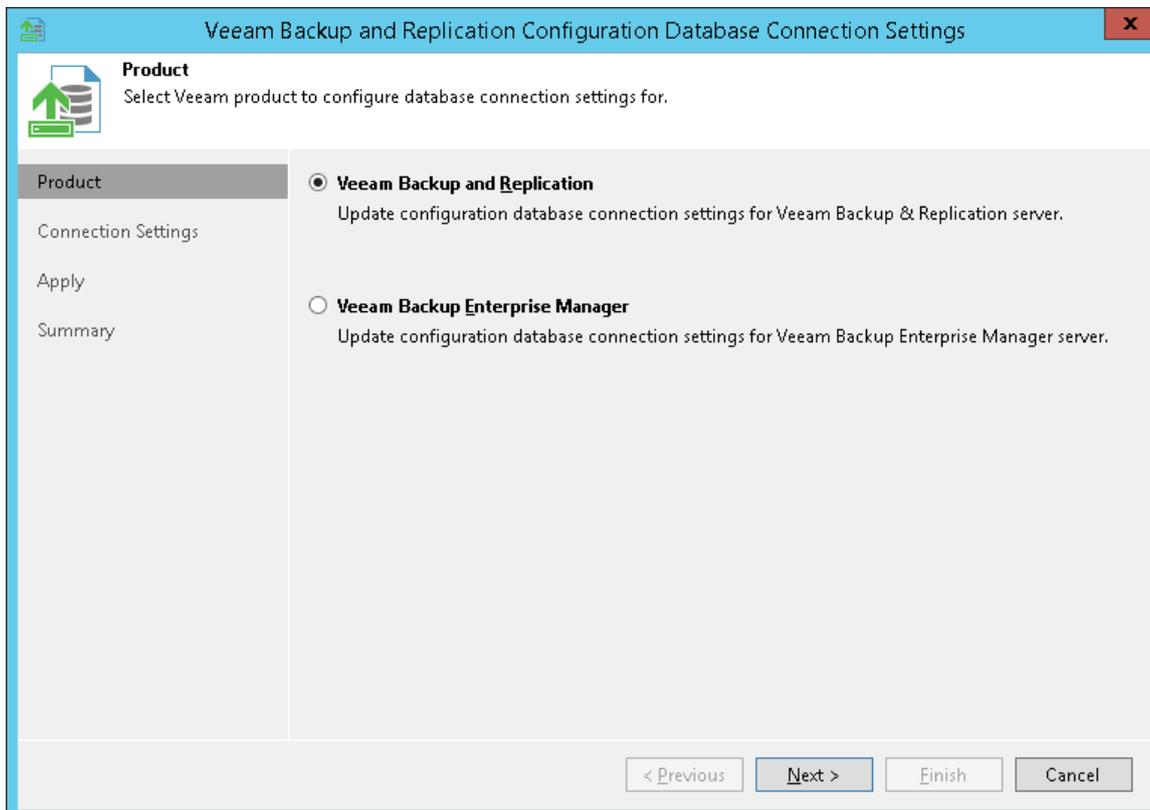
To run the utility, you must have administrative rights on the local machine, as long as the utility makes changes to the registry. If prompted at the launch, choose **Run as administrator**.

To manage connection settings for Veeam Backup & Replication and/or Veeam Backup Enterprise Manager configuration database, use the launched **Veeam Backup & Replication Configuration Database Connection Settings** wizard.

Step 1. Select Product

At the **Product** step of the wizard, select the database whose settings you want to configure.

The utility detects what server is installed on the local machine (backup server, Veeam Backup Enterprise Manager server or both) and displays available products for your choice. If Veeam Backup Enterprise Manager is not installed on the local machine, you will only have an opportunity to change Veeam Backup & Replication database settings (and vice versa). In this case, the **Product** step of the wizard will be skipped.



Step 2. Specify Connection Settings

At the **Connection Settings** step of the wizard, provide the connection settings for the selected database.

1. Specify the Microsoft SQL Server\instance and database name to which you want the Veeam Backup & Replication installation to connect. Both local and remote Microsoft SQL server instances are supported. Microsoft SQL server instances available on the network are shown in the **Server name** list. If necessary, click **Refresh** to get the latest information.

If a database with the specified name does not exist on the selected Microsoft SQL Server (instance), it will be created anew.

2. Select the authentication method that will be used for database connection:
 - If you plan to use the Microsoft Windows authentication, consider that the current service account will be used (that is, the account under which the Veeam Backup Service is running).
 - If you plan to use the Microsoft SQL authentication, provide a login name and password. To view the entered password, click and hold the eye icon on the right of the **Password** field.

The screenshot shows the 'Veeam Backup and Replication Configuration Database Connection Settings' dialog box. The title bar includes a close button (X). The main window has a sidebar on the left with 'Product', 'Connection Settings' (selected), 'Apply', and 'Summary'. The main area is titled 'Connection Settings' and contains the following fields and options:

- Connection** section:
 - Database name: VeeamBackup
 - Server name: SRV\VEEAMSQL2012 (with a Refresh button)
- Authentication** section:
 - Windows authentication
 - SQL authentication
 - Login name: SRV\Administrator
 - Password: (empty field)

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

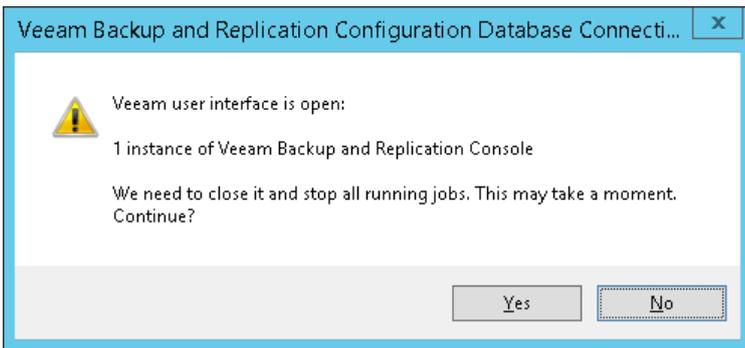
Step 3. Apply Connection Settings

Before proceeding, the utility validates the specified settings to make sure that the user account has enough privileges to access the database.

- If you have selected the Microsoft Windows authentication method, the utility will check the privileges of the current user account (that is, the account under which the utility is running) to connect to specified Microsoft SQL server.
- If you have selected the Microsoft SQL authentication method, the utility will check the privileges of the account you have specified.

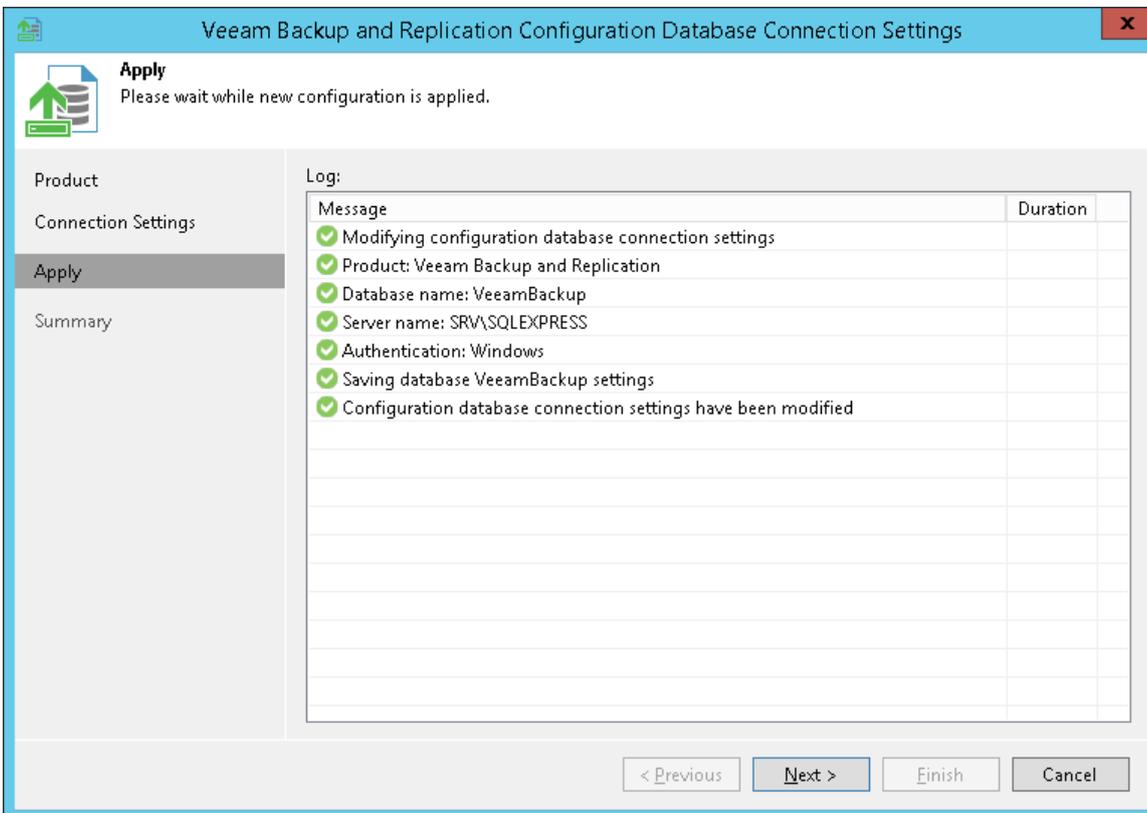
To ensure that these accounts (as well as the account under which the Veeam Backup Service is running) have sufficient privileges for database access, you can contact your database administrator. Refer to the list of system requirements for Veeam Backup & Replication for detailed information about required permission.

For the new settings to be applied, the utility needs to stop Veeam Backup & Replication services and jobs that are currently running. Before proceeding to the **Apply** step, you must confirm the operation. For example, if you are configuring Veeam Backup & Replication database settings, the following prompt will be displayed.



Confirm the operation by clicking **Yes** and wait for the services to be stopped. Then database connection settings will be applied, and you can view the operation progress in the log.

Wait for the operation to complete and click **Next** to proceed to the **Summary** step of the wizard. Previously stopped services will be started again at this moment.

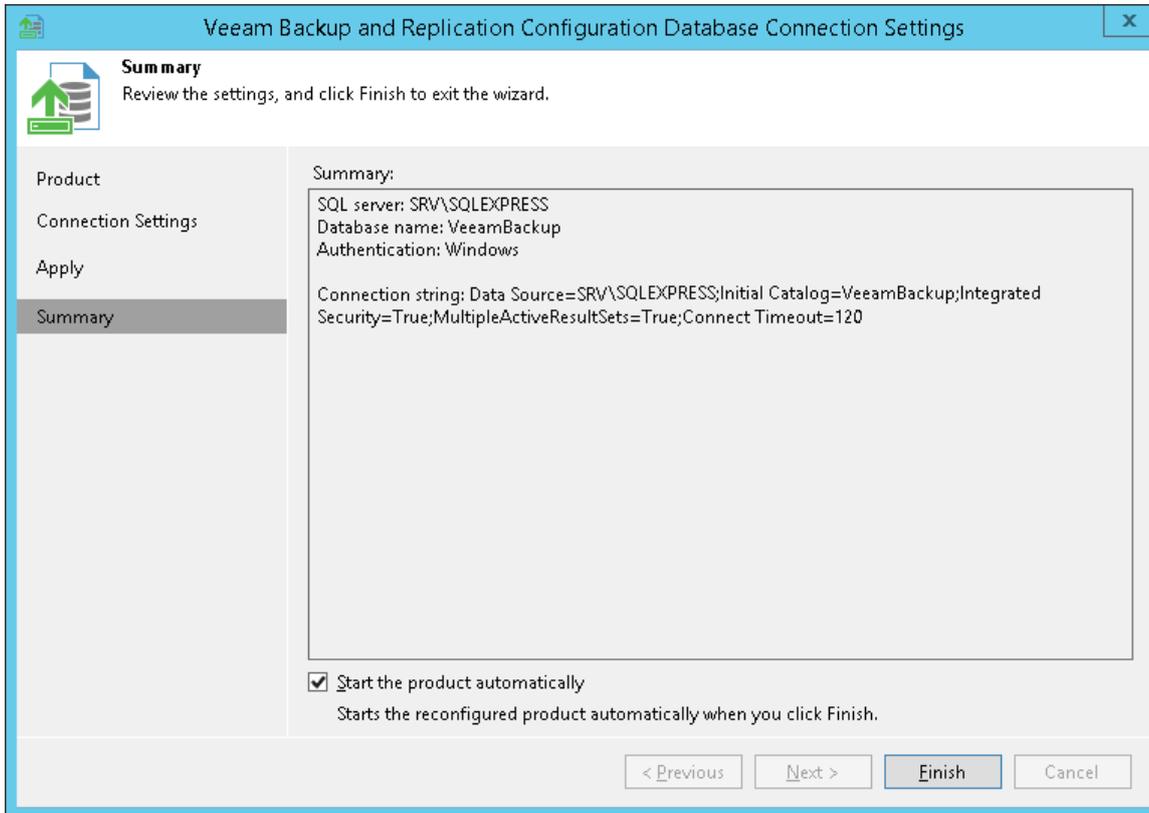


Step 4. Finish Working with Wizard

At the **Summary** step of the wizard, view the information about the changes in database connection settings. If you were configuring Veeam Backup & Replication database settings and you want the Veeam backup management console to be open automatically after you finish working with the wizard, select the **Start the product automatically** check box.

NOTE:

The **Start the product automatically** option is not available for Veeam Backup Enterprise Manager.



Veeam Backup Validator

In some cases, a backup can get corrupted due to accidental changes in the backup file data. For example, the file can be damaged after transfer over the network or from hardware failures on the backup storage side. With Veeam Backup Validator, you can quickly verify the integrity of any backup file, without extracting the VM data from the archive.

Veeam Backup Validator is a command-prompt CRC check utility that tests a backup at the file level. For integrity validation, it uses the checksum algorithm. When Veeam Backup & Replication creates a backup of a VM, it calculates a checksum for every data block in the backup file and attaches these checksums to the data blocks. Veeam Backup Validator re-calculates checksums for data blocks and compares them against the initial checksum values. If the results match, the backup file is viable. This works similarly to the backup file integrity check performed at [SureBackup](#).

Veeam Backup Validator is located in the installation folder of Veeam Backup & Replication – by default, %ProgramFiles%\Veeam\Backup and Replication\Backup\Veeam.Backup.Validator.exe.

If the default path was changed, you can find the actual path in the registry value:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication] CorePath.
```

Working with Veeam Backup Validator

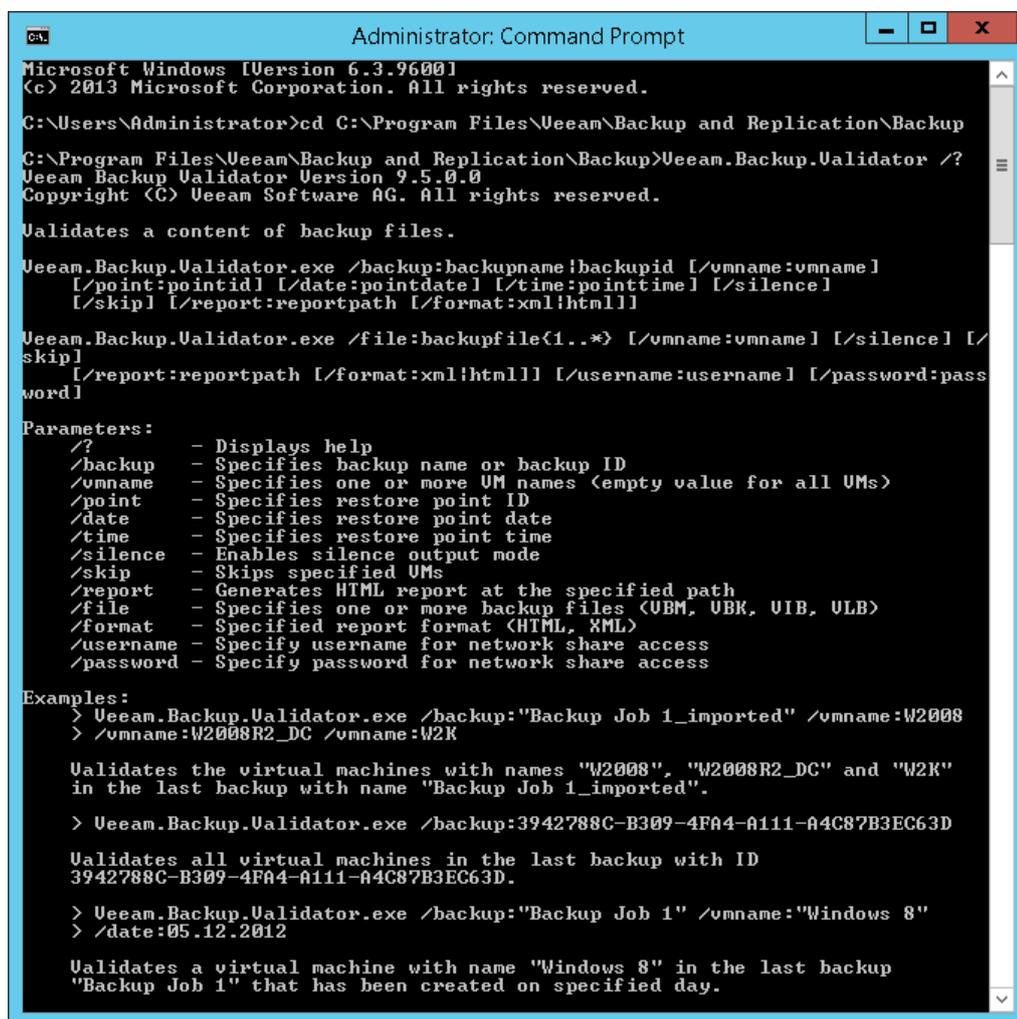
You can run the utility from the command prompt on the backup server, the machine on which Veeam Backup & Replication is installed.

To run Veeam Backup Validator, an account with administrative rights is required.

To display Veeam Backup Validator help information, run the following command:

```
Veeam.Backup.Validator /?
```

- In the *Parameters* section, you will see the list of all possible parameters and their descriptions
- In the *Examples* section, you will see the usage examples for each of these parameters:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files\Veeam\Backup and Replication\Backup
C:\Program Files\Veeam\Backup and Replication\Backup>Veeam.Backup.Validator /?
Veeam Backup Validator Version 9.5.0.0
Copyright (C) Veeam Software AG. All rights reserved.

Validates a content of backup files.

Veeam.Backup.Validator.exe /backup:backupname!backupid [/vmname:vmname]
  [/point:pointid] [/date:pointdate] [/time:pointtime] [/silence]
  [/skip] [/report:reportpath [/format:xml|html]]

Veeam.Backup.Validator.exe /file:backupfile(1..*) [/vmname:vmname] [/silence] [/
skip]
  [/report:reportpath [/format:xml|html]] [/username:username] [/password:pass
word]

Parameters:
/? - Displays help
/backup - Specifies backup name or backup ID
/vmname - Specifies one or more UM names (empty value for all UMs)
/point - Specifies restore point ID
/date - Specifies restore point date
/time - Specifies restore point time
/silence - Enables silence output mode
/skip - Skips specified UMs
/report - Generates HTML report at the specified path
/file - Specifies one or more backup files (UBM, UBK, UIB, ULB)
/format - Specified report format (HTML, XML)
/username - Specify username for network share access
/password - Specify password for network share access

Examples:
> Veeam.Backup.Validator.exe /backup:"Backup Job 1_imported" /vmname:W2008
> /vmname:W2008R2_DC /vmname:W2K

Validates the virtual machines with names "W2008", "W2008R2_DC" and "W2K"
in the last backup with name "Backup Job 1_imported".

> Veeam.Backup.Validator.exe /backup:3942788C-B309-4FA4-A111-A4C87B3EC63D

Validates all virtual machines in the last backup with ID
3942788C-B309-4FA4-A111-A4C87B3EC63D.

> Veeam.Backup.Validator.exe /backup:"Backup Job 1" /vmname:"Windows 8"
> /date:05.12.2012

Validates a virtual machine with name "Windows 8" in the last backup
"Backup Job 1" that has been created on specified day.
```

Validating Content of Backup File

Syntax

The following command validates for integrity the content of all VMs or selected VMs in the specified backup:

```
Veeam.Backup.Validator.exe /backup:backupname|backupid [/vmname:vmname]
[/point:pointid] [/date:pointdate] [/time:pointtime] [/silence]
[/skip] [/report:reportpath [/format:xml|html]]
```

The following command validates for integrity the content of VMs in the specified backup file:

```
Veeam.Backup.Validator.exe /file:backupfile{1..*} [/username:username
/password:password] [/vmname:vmname]
[/silence] [/skip] [/report:reportpath [/format:xml|html]]
```

IMPORTANT!

Veeam Backup Validator utility does not work with backups stored on scale-out backup repositories.

Parameters

Parameter	Description	Required/Optional	Parameter Type	Notes
/backup:backupname backupid	Specify a name or an ID* of the backup file that you want to validate.	Required	String	—
/file:backupfile{1..*}	Specify one or more backup files (VBM, VBK, VIB, VLB).	Required	String	<ul style="list-style-type: none">▪ If the file is located on a network share, make sure you specify a full path, for example: \\172.16.16.198\TestShare\Empty VM encryptedD2017-09-22T172639.vbk▪ Mapped network drives (like net use z: \\172.16.16.198\TestShare) are not supported.
/username:username /password:password	To access files on a network share, specify account credentials.	Required for network share	String	If you want to validate files located on different shares, make sure this account has access rights to all these shares.

/vmname:vmname	Specify a name of the VM in the backup file that you want to validate.	Optional	String	If not specified, Veeam Backup Validator will check all VMs in the backup file.
/point:pointID	Specify an ID* of the restore point that you want to validate	Optional	String	If not specified, Veeam Backup Validator will verify the latest restore point.
/date:pointdate	Specify the date when the restore point that you want to validate was created.	Optional	Date	Make sure to specify the date in the same format as used on the Veeam Backup server. For example: <ul style="list-style-type: none"> For the <code>mm/dd/yyyy</code> format, specify <code>08.30.2012</code>. For the <code>dd/mm/yyyy</code> format, specify <code>30.08.2012</code>.
/time:pointtime	Specify approximate time when the restore point you want to validate was created.	Optional	Time	—
/silence	Specify this parameter if you want to run validation in the silence mode.	Optional	Boolean	—
/skip	Specify this parameter if you want to skip VMs listed in the <code>vmname</code> parameter.	Optional	Boolean	In the <code>vmname</code> parameter, list all VMs that you want to skip
/report:reportpath [format:xml html]	Specify this parameter if you want to generate a report on validation results and store it at the specified path.	Optional	String	Supported report formats are HTML and XML.

* You can get IDs of backup jobs and restore points from the Veeam Backup & Replication database, for example, using scripts or using Management Studio.

Example 1

This command validates the exch01 VM in the Exchange Backup Job file.

```
Veeam.Backup.Validator /backup:"Exchange Backup Job"
```



```
Administrator: Command Prompt
C:\Program Files\Veeam\Backup and Replication\Backup> Veeam.Backup.Validator.exe
/backup:"Exchange Backup Job" /vmname:exch01
Veeam Backup Validator Version 9.5.0.0
Copyright (C) Veeam Software AG. All rights reserved.

Parameters:
  Backup ID:          <4CD9999F-33B4-4E0E-BBE9-2F9F692C5778>
  Backup name:       Exchange Backup Job
  Format:            Html
  Restore point date: Tuesday, December 18, 2018
  Restore point ID:  <7C94A4F3-532F-432A-B4CF-4AA96B435733>
  Restore point time: 12:00:31 AM
  Report:
  Silence:          no
  Skip:             no
  UM name:          exch01

Validating...

Validating UM...
  UM name:          exch01
  Creation time:    12/18/2018 12:00:54 AM
  Backup type:     increment
  Platform:        VMware
  OS name:         Microsoft Windows Server 2012 (64-bit)

Reading UM summary...
  Storage path:    C:\Backup Repository\Exchange Backup Job_1\Exchange Backup Job
_5D05D2018-12-18T000031.vib

  exch01.vmx (2.9 KB)
  exch01.nvram (8.5 KB)
  exch01-000002.vmdk (612.0 B)
  exch01-000002-flat.vmdk (50.0 GB)
  FsAwareMeta:df988d5b-6f4b-459c-b97c-0afe7f30fca4:2000 (0.0 B)

  Validating exch01.vmx
  _____

  Validating exch01.nvram
  _____

  Validating exch01-000002.vmdk
  _____

  Validating exch01-000002-flat.vmdk
  _____

  Validating FsAwareMeta:df988d5b-6f4b-459c-b97c-0afe7f30fca4:2000
  _____

Statistic:
  UM count:         1
  Incomplete UM count: 0
  Failed UM count:  0
  Files count:      5
  Total size:       50.0 GB

Validation completed successfully.
```

Example 2

This command validates all VMs in the Exchange Backup Job file created on December 18, 2018 around 12:00 AM.

```
Veeam.Backup.Validator /backup:"Exchange Backup Job"/date:12.18.2018 /time:12:00
```



```
Administrator: Command Prompt
C:\Program Files\Veeam\Backup and Replication\Backup>Veeam.Backup.Validator /bac
kup:"Exchange Backup Job" /date:12.18.2018 /time:12:00
Veeam Backup Validator Version 9.5.0.0
Copyright (C) Veeam Software AG. All rights reserved.

Parameters:
  Backup ID:          <4CD9999F-33B4-4E0E-BBE9-2F9F692C5778>
  Backup name:       Exchange Backup Job
  Format:            Html
  Restore point date: Tuesday, December 18, 2018
  Restore point ID:  <7C94A4F3-532F-432A-B4CF-4AA96B435733>
  Restore point time: 12:00:31 AM
  Report:
  Silence:          no
  Skip:             no

Validating...

Validating VM...
  VM name:          dns01
  Creation time:    12/18/2018 12:02:51 AM
  Backup type:      increment
  Platform:         VMware
  OS name:          Microsoft Windows Server 2012 (64-bit)

Reading VM summary...
  Storage path: C:\Backup Repository\Exchange Backup Job_1\Exchange Backup Job
_5D05D2018-12-18T000031.vib

  dns01.vmx (2.9 KB)
  dns01.nvram (8.5 KB)
  dns01-000002.vmdk (610.0 B)
  dns01-000002-flat.vmdk (50.0 GB)
  FsAwareMeta:29caab6e-1d10-4363-9ae5-c18c5e5ab3f2:2000 (0.0 B)

  Validating dns01.vmx
  _____

  Validating dns01.nvram
  _____

  Validating dns01-000002.vmdk
  _____

  Validating dns01-000002-flat.vmdk
  _____

  Validating FsAwareMeta:29caab6e-1d10-4363-9ae5-c18c5e5ab3f2:2000
  _____

Validating VM...
  VM name:          exch01
  Creation time:    12/18/2018 12:00:54 AM
  Backup type:      increment
  Platform:         VMware
  OS name:          Microsoft Windows Server 2012 (64-bit)

Reading VM summary...
  Storage path: C:\Backup Repository\Exchange Backup Job_1\Exchange Backup Job
```