Veeam Backup & Replication

Version 10
Veeam Agent Management Guide
February, 2020
© 2020 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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTENTS</td>
<td>3</td>
</tr>
<tr>
<td>CONTACTING VEEAM SOFTWARE</td>
<td>6</td>
</tr>
<tr>
<td>ABOUT THIS DOCUMENT</td>
<td>7</td>
</tr>
<tr>
<td>OVERVIEW</td>
<td>8</td>
</tr>
<tr>
<td>VEEAM AGENT MANAGEMENT INFRASTRUCTURE</td>
<td>9</td>
</tr>
<tr>
<td>PROTECTED COMPUTERS DISCOVERY AND VEEAM AGENT DEPLOYMENT</td>
<td>12</td>
</tr>
<tr>
<td>Protection Groups</td>
<td>12</td>
</tr>
<tr>
<td>Rescan Job</td>
<td>15</td>
</tr>
<tr>
<td>VEEAM AGENT BACKUP JOBS AND POLICIES</td>
<td>17</td>
</tr>
<tr>
<td>Backup Job</td>
<td>19</td>
</tr>
<tr>
<td>Backup Policy</td>
<td>21</td>
</tr>
<tr>
<td>VEEAM AGENT BACKUP JOBS AND POLICIES</td>
<td>17</td>
</tr>
<tr>
<td>Backup Job</td>
<td>19</td>
</tr>
<tr>
<td>Backup Policy</td>
<td>21</td>
</tr>
<tr>
<td>BACKUP OF MICROSOFT WINDOWS MACHINES</td>
<td>24</td>
</tr>
<tr>
<td>Backup Cache</td>
<td>24</td>
</tr>
<tr>
<td>BACKUP OF LINUX MACHINES</td>
<td>26</td>
</tr>
<tr>
<td>Backup Job Scripts</td>
<td>26</td>
</tr>
<tr>
<td>BACKUP TO VEEAM CLOUD CONNECT REPOSITORY</td>
<td>28</td>
</tr>
<tr>
<td>FAILOVER CLUSTER SUPPORT</td>
<td>30</td>
</tr>
<tr>
<td>PLANNING AND PREPARATION</td>
<td>32</td>
</tr>
<tr>
<td>CONSIDERATIONS AND LIMITATIONS</td>
<td>32</td>
</tr>
<tr>
<td>SYSTEM REQUIREMENTS</td>
<td>33</td>
</tr>
<tr>
<td>LICENSING REQUIREMENTS</td>
<td>39</td>
</tr>
<tr>
<td>SUPPORTED APPLICATIONS</td>
<td>40</td>
</tr>
<tr>
<td>USED PORTS</td>
<td>43</td>
</tr>
<tr>
<td>GETTING STARTED</td>
<td>46</td>
</tr>
<tr>
<td>CONFIGURING SECURITY SETTINGS</td>
<td>47</td>
</tr>
<tr>
<td>MANAGING TLS CERTIFICATES</td>
<td>49</td>
</tr>
<tr>
<td>Generating Self-Signed Certificates</td>
<td>49</td>
</tr>
<tr>
<td>Importing Certificates from Certificate Store</td>
<td>53</td>
</tr>
<tr>
<td>Importing Certificates from PFX Files</td>
<td>55</td>
</tr>
<tr>
<td>Using Certificate Signed by Internal CA</td>
<td>57</td>
</tr>
<tr>
<td>ADDING COMPUTERS TO TRUSTED HOSTS LIST</td>
<td>61</td>
</tr>
<tr>
<td>WORKING WITH PROTECTION GROUPS</td>
<td>63</td>
</tr>
<tr>
<td>CREATING PROTECTION GROUPS</td>
<td>63</td>
</tr>
<tr>
<td>ADDING PROTECTION GROUP TO BACKUP JOB</td>
<td>85</td>
</tr>
<tr>
<td>EDITING PROTECTION GROUP SETTINGS</td>
<td>86</td>
</tr>
<tr>
<td>RESCANNING PROTECTION GROUP</td>
<td>87</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>REPORTING</td>
<td>276</td>
</tr>
<tr>
<td>Viewing Rescan Job Statistics</td>
<td>276</td>
</tr>
<tr>
<td>Viewing Rescan Job Report</td>
<td>277</td>
</tr>
<tr>
<td>Viewing Veeam Agent Backup Job Statistics</td>
<td>278</td>
</tr>
<tr>
<td>Viewing Veeam Agent Backup Job Report</td>
<td>279</td>
</tr>
<tr>
<td>Viewing Backup Policy Statistics</td>
<td>280</td>
</tr>
<tr>
<td>Viewing Backup Policy Report</td>
<td>282</td>
</tr>
<tr>
<td>Enabling Email Reporting</td>
<td>283</td>
</tr>
<tr>
<td>APPENDIX A. DEPLOYING HOTFIX ON PROTECTED LINUX COMPUTERS</td>
<td>284</td>
</tr>
</tbody>
</table>
Contacting Veeam Software

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

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal 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 guide describes how to use Veeam Backup & Replication to remotely deploy and manage Veeam Agent for Microsoft Windows and Veeam Agent for Linux. It provides a general overview of the Veeam Agent management functionality, as well as description of data protection and disaster recovery tasks available within the Veeam Agent management scenario. The document applies to Veeam Backup & Replication 10 and all subsequent versions until it is replaced by a new document.

Intended Audience

The guide is designed for anyone who wants to use Veeam Backup & Replication to automate data protection tasks performed on Veeam Agent computers. It is primarily aimed at backup administrators and other IT professionals managing Veeam Backup & Replication, but can also be helpful for Veeam Agent computer users. The document assumes that you are familiar with basic concepts and operations that can be performed in Veeam Backup & Replication, Veeam Agent for Microsoft Windows and Veeam Agent for Linux.

Related Documentation

The document should be regarded as a supplement to existing technical documentation for Veeam Backup & Replication, Veeam Agent for Microsoft Windows and Veeam Agent for Linux. The complete set of documentation for Veeam products can be found at https://www.veeam.com/documentation-guides.datasheets.html.
Overview

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. You do not need to install, set up and operate Veeam Agent on every machine whose data you want to protect. Instead, you can perform the whole set of deployment, administration, data protection and disaster recovery tasks on Veeam Agent computers remotely from the Veeam Backup & Replication console.

Veeam Backup & Replication offers the following Veeam Agent management capabilities:

- **Automated deployment and management of Veeam Agents.** You can set up Veeam Backup & Replication to automatically discover computers that you want to protect with Veeam Agent for Microsoft Windows and/or Veeam Agent for Linux and install Veeam Agent on these computers. Once Veeam Agent is deployed on protected computers, you can use the Veeam Backup & Replication console to administrate Veeam Agent on multiple computers.

- **Centralized configuration and management of Veeam Agent backup jobs on protected computers.** You can use the Veeam Backup & Replication console to create and manage Veeam Agent backup jobs on computers in your infrastructure whose data you want to protect.

- **Centralized management of backups created by Veeam Agent backup jobs.** If you choose to create Veeam Agent backups on a backup repository managed by the Veeam backup server, you can use the Veeam Backup & Replication console to restore data from these backups.
Veeam Agent Management Infrastructure

The Veeam Agent management infrastructure comprises the following components:

- Veeam backup server
- Veeam Agent computers
- Distribution server

Veeam Backup Server

The Veeam backup server is the core component in the backup infrastructure that fills the role of the “configuration and control center”. To use the Veeam Agent management functionality offered by Veeam Backup & Replication, you can use the backup server that is already running in your backup infrastructure or deploy a separate backup server.

To learn more, see the Deployment section in the Veeam Backup & Replication User Guide.
Veeam Agent Computers

To deploy and manage Veeam Agent for Microsoft Windows and/or Veeam Agent for Linux on computers in your infrastructure, you must add computers that you want to protect with Veeam Agents to the inventory in the Veeam Backup & Replication console. In Veeam Backup & Replication, protected computers are organized into protection groups. To learn more, see Protection Groups.

Veeam Backup & Replication is set up to automatically discover computers added to the inventory and deploy Veeam Agents on these computers. To learn more, see Computers Discovery and Veeam Agent Deployment.

Veeam Backup & Replication lets you deploy and manage Veeam Agent on machines of the following types:

- **Workstations, servers and failover clusters running a Microsoft Windows OS** — on machines of this type Veeam Backup & Replication deploys Veeam Agent for Microsoft Windows 4.0.
- **Workstations and servers running a Linux OS** — on machines of this type Veeam Backup & Replication deploys Veeam Agent for Linux 4.0.

On every Windows machine added to the inventory, Veeam Backup & Replication installs the Veeam Installer Service. The service performs the following tasks:

- Collects information about the protected computer and sends it to the Veeam backup server. The collected data includes details on the computer type, platform, host name, guest OS, BIOS UUID, IP address, and information about Veeam Agent (its presence on the machine, product version and license installed).
- Downloads Veeam Agent setup files from the distribution server and installs Veeam Agent on the protected computer.

On Linux machines, Veeam Backup & Replication does not install additional components for Veeam Agent deployment. Veeam Backup & Replication connects to a Linux computer via SSH and performs necessary operations on the computer.

Veeam Agent for Microsoft Windows and Veeam Agent for Linux deployed on remote computers by Veeam Backup & Replication operate in the managed mode. In this mode, all data protection and administration tasks are performed by a backup administrator in Veeam Backup & Replication. In some scenarios, a user can also perform a limited set of backup and disaster recovery tasks directly on a protected computer.
Distribution Server

The distribution server is an architecture component in the Veeam Agent management infrastructure used for deployment of Veeam Agent setup files to protected computers. When you instruct Veeam Backup & Replication to install Veeam Agent on a protected computer, the Veeam backup server communicates to the distribution server, and Veeam Backup & Replication uploads Veeam Agent setup file from the distribution server to the target computer.

By default, the role of the distribution server is assigned to the backup server itself. However, you can deploy a dedicated distribution server to reduce workload on the backup server. To deploy a distribution server, you need to add a Windows-based server to Veeam Backup & Replication and select this server in the properties of a protection group. To learn more, see Specify Discovery and Deployment Options.

A machine performing the role of the distribution server must meet the following requirements:

- The role of the distribution server can be assigned to a physical or virtual machine.
- The machine must run a 64-bit Microsoft Windows OS.
- You must add the machine to the Veeam Backup & Replication console as a managed server.

The distribution server comprises the following services and components:

- Veeam Distribution Service
- Veeam Agent for Microsoft Windows Redistributable
- Veeam Agent for Linux Redistributable

TIP:

If you have several Veeam Agent for Linux installations managed by Veeam Backup & Replication, you can centrally deploy a hotfix on all managed Veeam Agent computers using the distribution server. To learn more, see Appendix A. Deploying Hotfix on Protected Linux Computers.
Protected Computers Discovery and Veeam Agent Deployment

Veeam Backup & Replication supports automatic deployment of Veeam Agent for Microsoft Windows and Veeam Agent for Linux on computers in your infrastructure. To deploy Veeam Agents, Veeam Backup & Replication needs to discover computers whose data you want to back up. To enable discovery, you organize your computers into one or more protection groups. Protection group settings define what Veeam Agent computers Veeam Backup & Replication will discover and how the discovery process will run.

Protection Groups

In Veeam Backup & Replication, computers that you want to protect with Veeam Agents are organized into protection groups. Technically, a protection group is a container in the Veeam Backup & Replication inventory aimed to combine protected computers of a specific type. For example, you can use a dedicated protection group for computers of the same type (for example, laptops, workstations or servers) or computers running the same OS type to simplify management of such computers. You can also use a separate protection group for a number of Veeam Agent computers that you want to manage in a different way from other machines in your infrastructure.

To start managing Veeam Agents in Veeam Backup & Replication, you need to create a protection group in the inventory and specify computers that you want to protect with Veeam Agents in the protection group settings. You can create one or more protection groups depending on the size and complexity of your infrastructure. Protection groups appear under the Physical Infrastructure node in the Inventory view of the Veeam Backup & Replication console.

NOTE:

Mind the following:

- The Physical Infrastructure node is not available if the Veeam Cloud Connect service provider license is installed on the backup server.
- If you want to manage only a small number of Veeam Agent computers in Veeam Backup & Replication and do not want to create protection groups, you can add the necessary computers directly to a Veeam Agent backup job. Veeam Backup & Replication will automatically include such computers to the Manually Added protection group. To learn more, see Predefined Protection Groups.

Protection groups allow you to automate deployment and management of Veeam Agents on computers in your infrastructure. When you configure a protection group, you can specify scheduling options for protected computers discovery and Veeam Agent deployment. You do not need to perform administrative tasks individually for every computer that you want to protect with Veeam Agent — Veeam Backup & Replication will perform the specified operations automatically upon the defined schedule.

Veeam Backup & Replication connects to discovered computers using credentials of the account specified in the protection group settings. You can specify a master account that Veeam Backup & Replication will use to connect to all computers added to the protection group or specify separate accounts to connect to specific computers in the protection group.

After you create a protection group, Veeam Backup & Replication starts the rescan job session to connect to computers added to the protection group and perform the required operations on these computers. To learn more, see Rescan Job.
Protection Group Types

Veeam Backup & Replication offers several methods to specify computers on which you want to install and manage Veeam Agent. You can create protection groups that include the following types of objects:

- **Individual computers**
  You can organize individual computers into a protection group by specifying the necessary computers in the protection group settings. This option is recommended for smaller environments that do not have Microsoft Active Directory deployed.

- **Microsoft Active Directory objects**
  You can create protection groups that include one or more Microsoft Active Directory objects: entire domain, container, organization unit, group, computer or cluster. This allows you to manage Veeam Agents on computers being part of an Active Directory domain. Protection groups that include Active Directory domain, containers, groups and/or organization units are dynamic in their nature. For example, if a new computer is added to a container, Veeam Backup & Replication will automatically discover this computer and start managing this computer as specified in the protection group settings.
  You can specify a protection scope based on Active Directory objects in one of the following ways:
  - You can select individual Active Directory objects that you want to include in a protection group, for example, selected organization units and/or computers.
  - You can include in the protection group an entire domain or other Active Directory object (such as a container or organization unit) and exclude specific child objects being part of this object, for example, selected organization units and/or computers.

- **Computers listed in a CSV file**
  You can add multiple computers to a protection group by importing a list of computers from a CSV file. Protection groups that include computers listed in a CSV file are also dynamic. If a new computer appears in a CSV file after the protection group is created, during the next protection group rescan session, Veeam Backup & Replication will automatically update the protection group settings to include the added computer.
Predefined Protection Groups

In addition to protection groups created by a user, the Veeam Backup & Replication inventory may contain one or more predefined protection groups.

Manually Added

The **Manually Added** protection group contains individual computers added to Veeam Agent backup jobs configured in Veeam Backup & Replication. This protection group is aimed for scenarios when you want to manage a single Veeam Agent computer or a small number of Veeam Agent computers and do not want to create additional protection groups. Veeam Backup & Replication automatically adds a computer to the **Manually Added** protection group when you add this computer to a Veeam Agent backup job. To learn more, see *Adding New Computers*.

The **Manually Added** protection group has the following limitations:

- For the **Manually Added** protection group, you can change only a limited number of settings:
  - You can change discovery and deployment options. (Except for changing the distribution server. For the **Manually Added** protection group, the role of the distribution server is always assigned to the backup server.)
  - You can remove computers from this protection group. For example, you may want to remove a computer from a **Manually Added** protection group if you do not want to back up data of this computer any longer, and you have removed this computer from a Veeam Agent backup job.
  - You cannot change other settings, such as the name and type of this protection group.
- You cannot add the entire **Manually Added** protection group to a Veeam Agent backup job.

Unmanaged

The **Unmanaged** protection group acts as a filter to display unmanaged Veeam Agent computers, that is, computers that meet the following conditions:

1. Have Veeam Agent deployed and configured directly from a Veeam Agent computer or with Veeam Availability Console.
2. Run a Veeam Agent backup job targeted at a backup repository managed by Veeam Backup & Replication.

You cannot perform any operations with the **Unmanaged** protection group, as well as add computers included in this group to a Veeam Agent backup job. However, you can move such computers to a protection group that you created. To learn more, see *Moving Unmanaged Computer to Protection Group*.

After you move an unmanaged computer to a protection group, Veeam Backup & Replication will start managing Veeam Agent running on this computer according to discovery settings specified in the properties of the protection group. If the protection group is added to a Veeam Agent backup job, Veeam Backup & Replication will add the new computer to the job, too. You will no longer be able to manage Veeam Agent directly on the Veeam Agent computer or from Veeam Availability Console.
Out of Date

The *Out of Date* protection group is displayed when Veeam Backup & Replication discovers protected computers on which an outdated version of Veeam Agent is installed. For example, this may happen in a situation where you configure a protection group with Veeam Agent deployment options disabled, and Veeam Backup & Replication detects a newer version of Veeam Agent on the distribution server during discovery.

The *Out of Date* protection group lets you update Veeam Agent on multiple computers at once. To learn more, see [Upgrading Veeam Agent on Multiple Computers](#).

Offline

The *Offline* protection group acts as a filter to display computers to which Veeam Backup & Replication could not connect during the latest rescan session.

Untrusted

The *Untrusted* protection group acts as a filter to display Linux-based computers whose fingerprints were not verified in Veeam Backup & Replication. For computers included in this protection group, you need to check and validate SSH fingerprints. To learn more, see [Validating SSH Fingerprints](#).

Rescan Job

For automated discovery of protected computers, Veeam Backup & Replication uses the rescan job that runs on the backup server. Veeam Backup & Replication automatically creates this job once you create the first protection group in the inventory. The rescan job runs upon schedule defined individually for every protection group in the protection group settings. By default, Veeam Backup & Replication is set up to perform discovery at 9:00 PM daily. You can adjust daily schedule in the protection group settings or define periodic schedule.

The rescan job itself is not displayed in the Veeam Backup & Replication console. However, you can start and stop rescan job sessions manually for a specific protection group or individual computer in the inventory. This may be helpful, for example, if new computers appeared in your infrastructure, and you want to discover these computers without waiting for the next scheduled rescan job session start. To learn more, see [Rescanning Protection Group](#) and [Rescanning Protected Computer](#).

You can view statistics for currently running and already performed rescan job sessions. To learn more, see [Viewing Rescan Job Statistics](#).
How It Works

When the rescan job is started — either automatically upon schedule or manually — Veeam Backup & Replication performs the following operations:

1. Obtains from the Veeam Backup & Replication database settings specified for the protection group. The settings include a list of computers to scan, an account for connecting to these computers, and so on.

2. Connects to each computer in the list under the specified account.

3. Deploys Veeam Installer Service on each newly discovered computer.

4. If the automatic Veeam Agent deployment option is enabled in the protection group settings, Veeam Backup & Replication also deploys Veeam Agent on discovered computers. As a part of this process, Veeam Backup & Replication performs the following operations:
   a. Veeam Installer Service running on the computer collects information about the computer and sends it to Veeam Backup & Replication. The collected data includes details on the computer type, platform, host name, guest OS, IP address, BIOS UUID, and information about Veeam Agent (its presence on the machine, product version and license installed).
   b. Veeam Backup & Replication uploads the Veeam Agent setup file from the distribution server to the discovered computer.
   c. Veeam Installer Service installs Veeam Agent on the target computer.
Veeam Agent Backup Jobs and Policies

To back up data of your protected computers, you must configure a Veeam Agent backup job. The Veeam Agent backup job defines what data to back up, how, where and when to back up data. In Veeam Backup & Replication, you can create Veeam Agent backup jobs of the following types:

- **Backup job**

  The backup job that processes Veeam Agent computers runs on the backup server in the similar way as a regular job for VM data backup. The backup job is intended for protected computers that have permanent connection to the backup server, such as standalone servers and failover clusters. You can use the backup job to create Veeam Agent backups in a backup repository or cloud repository.

  In Veeam Backup & Replication, the backup job of this type is also referred to as the *Veeam Agent backup job managed by the backup server*.

  To learn more, see Backup Job.

- **Backup policy**

  The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers. Veeam Backup & Replication uses the backup policy as a saved template and applies settings from the backup policy to Veeam Agents that run on computers specified in the backup policy. The backup policy is intended for protected computers that may have limited connection to the backup server, such as workstations, laptops and so on. You can choose to create Veeam Agent backups in a backup repository, cloud repository, network shared folder or on a local storage of a protected computer.

  In Veeam Backup & Replication, the backup policy is also referred to as the *Veeam Agent backup job managed by Veeam Agent*.

  To learn more, see Backup Policy.

Veeam Backup & Replication lets you create the following types of backup jobs and policies depending on the type of OS that runs on a protected computer:

- **Backup jobs and policies that process Microsoft Windows computers.** For such Veeam Agent backup jobs, Veeam Backup & Replication offers settings supported in Veeam Agent for Microsoft Windows.

- **Backup jobs and policies that process Linux computers.** For such Veeam Agent backup jobs, Veeam Backup & Replication offers settings supported in Veeam Agent for Linux.
If a protection group contains Microsoft Windows computers and Linux computers, you can add this protection group to a Veeam Agent backup job intended for any of these types of protected computers. Veeam Backup & Replication will automatically exclude computers of another type from the backup job and processes only those computers that run an OS of the same type.

For example, if you add a protection group that contains Microsoft Windows and Linux computers to a Veeam Agent backup job intended for Linux computers, Veeam Backup & Replication will exclude Microsoft Windows computers from this backup job and process only Linux computers within the job.

### Processing One Computer with Multiple Jobs and Policies

The number of backup jobs and policies that can process the same protected computer depends on the computer type. A protected computer can be processed by more than one Veeam Agent backup job according to the following rules:

- You can include a computer of the **Server** type in more than one backup job managed by the backup server or more than one backup policy.
- You can include a computer of the **Workstation** type in one backup job managed by the backup server or one backup policy.
- You cannot include the same computer in a backup job and backup policy simultaneously.
Backup Job

The backup job that processes Veeam Agent computers runs on the backup server in the similar way as a regular job for VM data backup. You can add one or more protection groups or individual computers to the job and instruct Veeam Backup & Replication to create Veeam Agent backups in a Veeam backup repository or cloud repository. In terms of the Veeam Agent management scenario, the backup job of this type is also referred to as the Veeam Agent backup job managed by the backup server.

For a Veeam Agent backup job managed by the backup server, all job management tasks are performed on the Veeam Backup & Replication side: Veeam Backup & Replication starts the job upon the defined schedule, allocates backup infrastructure resources, and so on. Veeam Agent running on a protected computer operates under control from Veeam Backup & Replication and performs data backup operations only, such as creating a volume snapshot, reading the backed-up data and transferring backed-up data to the target location. To learn more, see How Veeam Agent Backup Job Works.

To configure a backup job, you must launch the New Agent Backup Job wizard and select the Managed by backup server option at the Job mode step of the wizard. For backup jobs of this type, Veeam Backup & Replication offers settings similar to settings of a VM backup job, as well as settings specific for Veeam Agents. To learn more, see Creating Veeam Agent Backup Jobs.

NOTE:

To manage a Veeam Agent backup job managed by the backup server, you can use the Veeam Backup & Replication console only. On a computer added to a backup job of this type, the Veeam Agent user interface is not available, and you cannot perform operations with Veeam Agent directly on the protected computer.

How Veeam Agent Backup Job Works

In the scenario where you use the backup job to create Veeam Agent backups, Veeam Backup & Replication performs backup in the following way:

1. When you create a Veeam Agent backup job in Veeam Backup & Replication, Veeam Backup & Replication saves the backup job settings in its database.
2. 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 backup tasks to process. For every protected computer added to the job, Veeam Backup & Replication creates a new task.
3. 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 repository to process job tasks.
4. Veeam Backup Manager connects to Veeam Transport Service on the backup repository. The Veeam Transport Service, in its turn, starts Veeam Data Mover. A new instance of Veeam Data Mover is started for every job task.
5. Veeam Backup Manager establishes a connection with Veeam Agent service that runs on the protected computer and Veeam Data Mover that runs on the backup repository, and sets a number of rules for data transfer, such as network traffic throttling rules and so on.
6. Veeam Agent service that runs on the protected computer and Veeam Data Mover that runs on the backup repository establish a connection with each other for data transfer.
7. If application-aware processing is enabled for the job, Veeam Backup & Replication connects to protected computers, establishes a connection with Veeam Agents running on protected computers and performs in-guest processing tasks.

8. Veeam Backup & Replication requests Veeam Agent to create a VSS snapshot or volume snapshot, depending on the type of OS running on the Veeam Agent computer. For Windows-based computers, Veeam Agent for Microsoft Windows leverages Microsoft VSS technology to create a VSS snapshot. For Linux-based computers, Veeam Agent for Linux uses the Veeam driver to create a volume snapshot.

9. Veeam Agent service that runs on the protected computer reads the backed-up data from the volume snapshot and transfers the data to the backup repository. During incremental job sessions, the Veeam Agent service uses CBT to retrieve only those data blocks that have changed since the previous job session. If CBT is not available, the Veeam Agent service 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 backed-up data, Veeam Agent running on a protected computer performs additional processing. It filters out zero data blocks, blocks of swap files and blocks of excluded files and folders. Veeam Agent compresses backed-up data and transports it to the target Veeam Data Mover.

Veeam Backup & Replication stores backed-up data to the backup file in the backup repository.
Backup Policy

In some cases, the backup job managed by the backup server may be not suitable for data backup with Veeam Agents. For example, you may want use Veeam Agents to back up data of computers that reside in a remote location and have limited connection to the Veeam backup server and backup repository. For such scenarios, Veeam Backup & Replication offers the concept of the backup policy.

The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers. You can add one or more protection groups or individual computers to the backup policy and instruct Veeam Agent to create backups in a Veeam backup repository, in a Veeam Cloud Connect repository, in a network shared folder or on a local storage of a protected computer. In terms of the Veeam Agent management scenario, the backup policy is also referred to as the Veeam Agent backup job managed by the Veeam Agent.

Veeam Backup & Replication uses the backup policy as a saved template and applies settings from the backup policy to protected computers. The resulting Veeam Agent backup jobs run on protected computers in the similar way as a regular backup job configured directly in Veeam Agent. All backup job management and data processing tasks are performed by Veeam Agent itself. This allows Veeam Agent to create backups of your data even if a connection to the backup server is unavailable. To learn more, see How Backup Policy Works.

To configure a backup policy, you must launch the New Agent Backup Job wizard and select the Managed by agent option at the Job mode step of the wizard. For backup policies, Veeam Backup & Replication offers settings similar to settings of a Veeam Agent backup job configured directly in Veeam Agent. To learn more, see Creating Veeam Agent Backup Jobs.

NOTE:

For computers specified in the backup policy, in addition to managing backup settings and performing backup tasks from the Veeam backup console, you can also perform selected operations directly on a protected computer. In particular, you can use the Veeam Agent control panel to start the backup job manually and monitor backup statistics. This allows you to create ad-hoc backups of your data in addition to backups created upon schedule defined in the backup policy.

How Backup Policy Works

In the scenario where you use the backup policy to create Veeam Agent backups, Veeam Backup & Replication and Veeam Agents interact in the following way:

1. When you create a backup policy, Veeam Backup & Replication saves the backup policy settings in the following locations on the backup server:
   - In the Veeam Backup & Replication database.
   - In the configuration file of the XML format.

2. Once the backup policy is created, Veeam Backup & Replication immediately applies the backup policy to Veeam Agents that run on protected computers:
   a. Veeam Backup & Replication reads the list of computers and protection groups specified in the backup policy and starts the discovery process for these computers.
   b. During the discovery process, Veeam Backup & Replication connects to each computer in the backup policy and uploads the XML file with backup policy settings to the target computer.
c. Veeam Backup & Replication uses settings from the backup policy to configure the Veeam Agent backup job. This process differs depending on what OS and Veeam Agent the protected computer runs.

- On Microsoft Windows computers, Veeam Backup & Replication creates the Veeam Agent backup job using the Veeam Agent for Microsoft Windows Configurator.
- On Linux computers, Veeam Backup & Replication creates the Veeam Agent backup job using the Veeam Agent for Linux command line interface.

Settings of the created backup job are saved to the Veeam Agent database on the protected computer.

Veeam Backup & Replication regularly applies the backup policy to protected computers during rescan of protection groups added to the backup policy. To learn more, see Backup Policy Application Methods.

3. The created Veeam Agent backup job runs on the protected computer in the similar way as a regular Veeam Agent backup job configured directly on the Veeam Agent computer. To learn more, see the following sections:

- How Backup Works section in the Veeam Agent for Microsoft Windows User Guide
- How Backup Works section in the Veeam Agent for Linux User Guide

Veeam Agent regularly checks whether job settings obtained from the backup policy are up-to-date and do not differ from the current backup settings specified in the backup policy. If the settings differ, Veeam Agent updates backup job settings in its database. To learn more, see Backup Policy Application Methods.
Backup Policy Application Methods

To ensure that settings of Veeam Agent backup jobs on protected computers are up-to-date and do not differ from backup settings specified in the backup policy, Veeam Backup & Replication regularly applies the backup policy to protected computers. There are two methods to start the policy application process:

- **By Veeam Backup & Replication**
  Veeam Backup & Replication applies the backup policy to protected computers at the following events:
  - At the time when the backup policy is created.
  - At the time when you start or stop the backup process.
  - At the time when Veeam Backup & Replication performs scheduled rescan of protection groups added to the backup policy. Veeam Backup & Replication automatically rescans a protection group upon schedule specified in the protection group settings.

- **By Veeam Agent**
  The Veeam Agent service running on a protected computer regularly checks whether job settings obtained from the backup policy are up-to-date and updates backup job settings, if necessary. Veeam Agent performs the check operation according to the following rules:
  - In case 6 or more hours pass since the previous check, Veeam Agent performs the check operation at the time when the backup job starts upon schedule.
  - In case 24 hours pass since the previous check, Veeam Agent immediately starts the check operation.

  During the check, Veeam Agent performs the following operations:
  - Connects to Veeam Backup & Replication and obtains from the Veeam Backup & Replication database information about backup policies to which the Veeam Agent computer was added.
  - Compares obtained backup policy settings with backup job settings in the Veeam Agent database.
    - If the settings differ, Veeam Agent performs the following tasks:
      - If backup policy settings and Veeam Agent backup job settings do not match, Veeam Agent updates backup job settings in its database.
      - If the protected computer was added to a new backup policy, Veeam Agent creates a new backup job on the protected computer.
      - If the protected computer was removed from the backup policy, Veeam Agent removes the Veeam Agent backup job on the protected computer.

**TIP:**
You can also apply the backup policy to protected computers manually, if needed. To learn more, see Applying Backup Policy to Protected Computers.
Backup of Microsoft Windows Machines

To back up data of Microsoft Windows machines, you can use Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication. In this scenario, some Veeam Agent features differ from the same features in Veeam Agent operating the standalone mode. This section provides description for such features in the Veeam Agent management scenario.

Backup Cache

Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication supports creating restore points in the backup cache — a temporary local storage where Veeam Agent creates backup files in case a remote backup location is unavailable at the time of backup. This may be helpful in the scenario where you create Veeam Agent backups using the backup policy: if some computers in the backup policy cannot access the remote location during scheduled backup, Veeam Agent creates backup files in the backup cache on these computers. When the target location becomes available, Veeam Agent uploads backup files from the backup cache to the remote storage so that the backup chain contains a sequence of restore points that precisely complies with the backup schedule.

In the Veeam Agent management scenario, the backup cache works in the similar way as in Veeam Agent operating in the standalone mode. To learn more, see the Backup Cache section in the Veeam Agent for Microsoft Windows User Guide.

In addition to backup cache features and limitations listed in the Veeam Agent for Microsoft Windows User Guide, the following applies to Veeam Agent operating in the managed mode:

- You can specify backup cache settings in the properties of backup policies targeted at the following types of backup location:
  - Veeam backup repository
  - Cloud repository
- To facilitate backup cache configuration on multiple Veeam Agent computers added to the backup policy, you can instruct Veeam Agent to automatically select location for the backup cache on each computer. To learn more, see How Automatic Backup Cache Placement Works.

How Automatic Backup Cache Placement Works

You can instruct Veeam Agent to automatically select location for the backup cache on each computer added to the backup policy. To do this, select the Automatic selection option at the Backup Cache step of the New Agent Backup Job wizard. For details, see Specify Backup Cache Settings.

With the Automatic selection option enabled in the backup cache settings, Veeam Agent for Microsoft Windows creates the backup cache according to the following rules:

1. Veeam Agent selects for the backup cache a non-system volume that has enough free space for the specified backup cache quota (that is, maximum backup cache size) and has the largest amount of free space.
2. On the selected volume, Veeam Agent creates the backup cache in the Veeam Backup Cache folder.
Mind the following:

- If the volume with the largest amount of free space is a system volume, Veeam Agent selects the volume that has enough space for the backup cache quota and has the second largest amount of free space.
- If the system volume is the only volume that has enough space for the backup cache quota, Veeam Agent creates the backup cache on the system volume.
- If no volumes have enough space for the backup cache quota, Veeam Agent selects the volume that has the largest amount of free space.
- Once Veeam Agent creates the *Veeam Backup Cache* folder on a protected computer, Veeam Agent does not change the location of this folder.
  
  For example, the system volume is the only volume that has enough space for the backup cache quota at the time when you create the backup policy. In this case, Veeam Agent creates the *Veeam Backup Cache* folder on the system volume. After disk configuration changes on the computer, a non-system volume becomes able to fit the backup cache quota. However, Veeam Agent will not move the *Veeam Backup Cache* folder to the non-system volume.
- Veeam Agent does not create the backup cache on external, removable or virtual disks.

**Tasks with Backup Cache**

For Veeam Agent operating in the managed mode, you can perform the same operations with the backup cache as for the standalone version of the product: you can monitor backup cache activity, pause backup cache synchronization and delete restore points from the backup cache. To do this, you must use the Veeam Agent control panel directly on the protected computer. For details, see the Managing Backup Cache section in the Veeam Agent for Microsoft Windows User Guide.

Note that Veeam Backup & Replication automatically deletes restore points from the backup cache on all computers added to the backup policy after you perform one of the following operations:

- Change the target location for backup files in the backup policy settings.
- Change the backup mode for the backup policy to the *File-level backup*.
- Enable or disable data encryption settings for the backup policy.
- Change backup cache location for the backup policy (in case it was specified manually).
- Disable the backup cache for the backup policy.
- Delete the backup policy.

You can also delete restore points from the backup cache manually in the Veeam backup console. To learn more, see Clearing Backup Cache.
Backup of Linux Machines

To back up data of Linux machines, you can use Veeam Agent for Linux managed by Veeam Backup & Replication. In this scenario, some Veeam Agent features differ from the same features in Veeam Agent operating the standalone mode. This section provides description for such features in the Veeam Agent management scenario.

Backup Job Scripts

You can instruct Veeam Agent for Linux to run custom scripts within the backup job session. In contrast to the standalone version of the product that can run custom scripts on the Veeam Agent computer only, Veeam Agent for Linux operating in the managed mode supports the following types of scripts:

- Pre-freeze and post-thaw scripts (for backup jobs that process servers)
- Pre-job and post-job scripts executed on the Veeam Agent computer
- Pre-job and post-job scripts executed on the backup server (for backup jobs managed by the backup server)

Pre-Freeze and Post-Thaw Scripts

Veeam Agent runs these scripts before and after creating a snapshot of the backed-up volume. For example, the pre-freeze script may quiesce the file system and application data to bring the Linux OS to a consistent state before Veeam Agent for Linux creates a snapshot. After the snapshot is created, the post-thaw script brings the file system and applications to their initial state.

You can specify pre-freeze and post-thaw script settings at the Guest Processing step of the New Agent Backup Job wizard. For details, see Backup Job and Snapshot Scripts.

During the backup job session, Veeam Backup & Replication uploads the scripts to each Veeam Agent computer added to the backup job and executes them on these computers. The scripts run in the same way as in the standalone version of Veeam Agent. To learn more, see the Backup Job Scripts section in the Veeam Agent for Linux User Guide.

Pre-Job and Post-Job Scripts on Veeam Agent Computer

Veeam Agent runs these scripts before the backup job starts and after the backup job completes. You can use pre-job and post-job scripts, for example, to quiesce an application for the time when the backup job session runs on the Veeam Agent computer.

You can specify backup job script settings at the Guest Processing step of the New Agent Backup Job wizard. For details, see Backup Job and Snapshot Scripts.

During the backup job session, Veeam Backup & Replication uploads the scripts to each Veeam Agent computer added to the backup job and executes them on these computers. The scripts run in the same way as in the standalone version of Veeam Agent. To learn more, see the Backup Job Scripts section in the Veeam Agent for Linux User Guide.

Pre-Job and Post-Job Scripts on Backup Server

Veeam Agent runs these scripts before the backup job starts and after the backup job completes. You can use pre-job and post-job scripts, for example, to throttle activities of some resource-consuming services on the backup server during the backup process.
You can specify backup job script settings at the **Storage** step of the **New Agent Backup Job** wizard. For details, see **Script Settings**.

During the backup job session, Veeam Backup & Replication executes the scripts on the backup server. The scripts are executed on the backup server under the account under which the Veeam Backup Service runs (the local System account or account that has the local Administrator permissions on the backup server).

### Script Execution Order

If you specify both pre-job and post-job scripts that run on the backup server and pre-job and post-job scripts that run on the Veeam Agent computer, the scripts will be executed in the following order:

1. Pre-job script on the backup server.
2. Pre-job script on the Veeam Agent computer.
3. Pre-freeze script.
4. Post-thaw script.
5. Post-job script on the Veeam Agent computer.
6. Post-job script on the backup server.
Backup to Veeam Cloud Connect Repository

If you want to store your data in the cloud, you can connect to a Veeam Cloud Connect service provider (SP) and create Veeam Agent backups in a cloud repository.

Getting Started

To back up Veeam Agent computer data to a cloud repository, you must complete the following steps:

1. Add the SP in the Veeam backup console. To do this, you must provide credentials of the tenant account that you obtained from the SP. For details, see the Connecting to Service Providers section in the Veeam Cloud Connect Guide.

2. Create Veeam Agent backup job or policy and specify a cloud repository as a target location for backup files. For details, see Creating Veeam Agent Backup Jobs.

3. In case some Veeam Agent computer data becomes missing or corrupted, you can restore the necessary data from the cloud. To learn more, see Restore Tasks with Veeam Agent Backups in Cloud Repository.

NOTE:

Consider the following:

- In the Veeam Agent management scenario, you do not need to create subtenant accounts to connect Veeam Agent computers to the Veeam Cloud Connect infrastructure on the SP side. To learn more, see How It Works.

- If you plan to back up Veeam Agent computer data to the cloud using a backup policy, you must not connect to the SP using credentials of a vCloud Director tenant account. Veeam Backup & Replication does not support creating managed subtenant accounts for tenant accounts of this type.

How It Works

There are 2 scenarios for data backup to the cloud with Veeam Agent operating in the managed mode:

- **Scenario 1: backup to the cloud with a backup job managed by the backup server.** In this scenario, the backup process is similar to the same process for VM backup to a cloud repository.

- **Scenario 2: backup to the cloud with a backup policy.** In this scenario, the backup process is similar to the same process for Veeam Agent operating in the standalone mode.
Scenario 1. Backup to Cloud with Backup Job

In the scenario where you use a backup job managed by the backup server to back up Veeam Agent machine data to the cloud, backup is performed in the following way:

1. The tenant adds the SP in the Veeam backup console on the tenant backup server.
2. The tenant creates a Veeam Agent backup job managed by the backup server. The backup job is targeted at a cloud repository.
3. The backup job operates in the similar way as in the regular Veeam Cloud Connect Backup scenario. The difference is that Veeam Backup & Replication processes Veeam Agent computer data instead of VM data. To learn more about backup to a cloud repository, see the How Cloud Repository Works section in the Veeam Cloud Connect Guide.

Scenario 2. Backup to Cloud with Backup Policy

In the scenario where you use a backup policy to back up Veeam Agent machine data to the cloud, backup is performed in the following way:

1. The tenant adds the SP in the Veeam backup console on the tenant backup server.
2. The tenant creates a backup policy targeted at a cloud repository.
3. For each Veeam Agent computer added to the backup policy, Veeam Backup & Replication automatically creates a managed subtenant account. To learn more, see the Managed Subtenant Account section in the Veeam Cloud Connect Guide.
4. Backup jobs that run on Veeam Agent computers added to the backup policy operate in the similar way as in the standalone version of Veeam Agent. Veeam Agent connects to the SP under the managed subtenant account and transfers the backed-up data to the cloud repository.

Restore Tasks with Veeam Agent Backups in Cloud Repository

You can use the Veeam backup console to perform the following data restore tasks with Veeam Agent backups in a cloud repository:

- Restore computer volumes from a Veeam Agent backup (for backups of Microsoft Windows machines only).
- Restore individual files and folders from a Veeam Agent backup (for backups of Microsoft Windows machines only).
- Restore application items from a Veeam Agent backup with Veeam Explorers (for backups of Microsoft Windows machines only).
- Export computer disks as VMDK, VHD or VHDX disks.
- Export a specific restore point in a Veeam Agent backup to a full backup (VBK) file.

You cannot restore data from a Veeam Agent backup in the cloud repository to a VMware vSphere or Microsoft Hyper-V VM, Amazon EC2 and Microsoft Azure.

Limitations for Veeam Agent Backup to Cloud Repository

To learn about limitations for Veeam Cloud Connect Backup, see the Limitations for Cloud Repository section in the Veeam Cloud Connect Guide.
Failover Cluster Support

You can use Veeam Agent for Microsoft Windows operating in the managed mode (within the Veeam Agent management scenario) to protect data processed by a failover cluster. Veeam Agent for Microsoft Windows supports Windows Server Failover Clusters running Microsoft Windows Server 2008 R2 and later.

Veeam Agent for Microsoft Windows supports data backup and restore for the following types of clusters:

- Windows File Server Failover Clusters
- Windows Server Failover Clusters that run the following applications:
  - Microsoft SQL Server 2008 SP4 or newer (AlwaysOn Failover Cluster Instances and AlwaysOn Availability Groups are supported.)
  - Microsoft Exchange Server 2010 or newer

Failover Cluster Backup

To process a cluster with Veeam Agent for Microsoft Windows, you must complete the following tasks:

1. In Veeam Backup & Replication, create a protection group that includes Active Directory objects and add to this protection group one of the following types of objects:
   - Cluster account of the failover cluster whose data you want to back up
   - Active Directory container that includes this cluster account
   To learn more, see Creating Protection Groups.

2. In Veeam Backup & Replication, configure a Veeam Agent backup job for a failover cluster. To add a failover cluster to the backup job, do the following:
   a. At the Job Mode step of the New Agent Backup Job wizard, select Failover cluster.
   b. At the Computers step of the wizard, add to the job the cluster account that you added to a protection group at the step 1. Alternatively, you can add to the job a container or protection group that includes this cluster account.
   To learn more, see Creating Agent Backup Job for Windows Computers.

IMPORTANT!

In case a backup task within a Veeam Agent backup job that processes a cluster completes unsuccessfully, Veeam Agent for Microsoft Windows will create full backup of all shared disks of the cluster.

Backup of Microsoft Exchange Database Availability Groups

You can use Veeam Agent for Microsoft Windows to process Microsoft Exchange Database Availability Groups (DAGs). The procedure of adding a DAG to a Veeam Agent backup job differs depending on the type of the DAG that you want to process:

- For a regular DAG, the backup job configuration procedure is the same as for any failover cluster. To learn more, see Failover Cluster Backup.
- For an IP Less DAG (a DAG without an Administrative Access Point), the backup job configuration procedure is similar to the same procedure for standalone servers. To process an IP Less DAG, you must create a
Veeam Agent backup job for servers in the Veeam backup console and add to this job all nodes of the IP Less DAG. To learn more, see Creating Agent Backup Job for Windows Computers.

During the backup process, Veeam Backup & Replication will detect that servers in the backup job are part of a DAG, and create transactionally consistent backup of Microsoft Exchange databases running on these servers.

Limitations for Failover Cluster Support

Failover cluster support in Veeam Agent for Microsoft Windows has the following limitations:

- Backup of failover clusters is supported in Veeam Agent for Microsoft Windows managed by Veeam Backup & Replication only. You cannot process a failover cluster by Veeam Agent for Microsoft Windows operating in the standalone mode.

- Backup of CSV (Cluster Shared Volumes) is not supported. Cluster disks used as CSV are automatically excluded from backup.

- AlwaysOn Clusterless Availability Groups are not supported.

- Backup of Storage Replica log volumes is not supported. Such volumes are automatically excluded from backup because of Microsoft VSS limitations. To learn more, see Microsoft Docs.
Planning and Preparation

Before you start using the Veeam Agent management functionality in Veeam Backup & Replication, make sure that the Veeam backup server and computers that you plan to protect with Veeam Agent for Microsoft Windows and/or Veeam Agent for Linux meet the system requirements and all required ports are open.

Considerations and Limitations

Before you start using the Veeam Agent management functionality in Veeam Backup & Replication, consider the following:

1. If you have already been using Veeam Agent for Microsoft Windows and/or Veeam Agent for Linux with Veeam Backup & Replication, after you start managing this Veeam Agent with Veeam Backup & Replication, Veeam Agent will start a new backup chain on a target location. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.

2. You cannot map a Veeam Agent backup job or backup policy configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
System Requirements

Make sure that components in the Veeam Agent management infrastructure meet system requirements listed below.

Veeam Backup Server

To learn about system requirements for the Veeam backup server and other Veeam Backup & Replication components, see the System Requirements section in the Veeam Backup & Replication User Guide.

Veeam Agent Computer (Microsoft Windows)

A machine that you want to protect with Veeam Agent for Microsoft Windows must meet the following requirements:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CPU: x86-64 processor.</td>
</tr>
<tr>
<td></td>
<td>Memory: 2 GB RAM or more. Memory consumption varies depending on number and size of processed disks.</td>
</tr>
<tr>
<td></td>
<td>Disk Space: 200 MB for product installation.</td>
</tr>
<tr>
<td></td>
<td>Network: 1 Mbps or faster1.</td>
</tr>
<tr>
<td></td>
<td>System firmware: BIOS or UEFI.</td>
</tr>
<tr>
<td></td>
<td>Drive encryption: Microsoft BitLocker (optional)2.</td>
</tr>
<tr>
<td></td>
<td>1 High latency and reasonably unstable WAN links are supported.</td>
</tr>
<tr>
<td></td>
<td>2 BitLocker encrypted volumes must be unlocked at the moment when Veeam Agent for Microsoft Windows starts the backup or restore operation. Only Microsoft BitLocker is supported for drive encryption. Other drive encryption products are not supported.</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported1,2:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2019</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server Semi-Annual Channel (including version 1909)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2008 R2 SP13</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 10 (starting from version 1607 up to version 1909)4</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 8.1</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows 7 SP1</td>
</tr>
<tr>
<td></td>
<td>Each Veeam Agent computer that consumes a license installed in Veeam Backup &amp; Replication must have a unique BIOS UUID.</td>
</tr>
<tr>
<td></td>
<td>1 Running Veeam Agent on Insider versions of Microsoft Windows OS (both Client and Server) is not supported.</td>
</tr>
</tbody>
</table>
Server Core installations of Microsoft Windows Server OSes can be backed-up only by Veeam Agent backup jobs managed by the Veeam backup server.

Veeam CBT driver is supported only if Microsoft Windows update KB3033929 is installed on the Veeam Agent computer.

Microsoft Windows 10 Education is supported starting from build 10586 and later.

File System

Microsoft Windows FAT, NTFS, ReFS file systems are supported.

The supported file system must reside on a volume that is 64 TB or smaller, because Veeam Agent uses the Microsoft Software Shadow Copy Provider to create a volume shadow copy during the backup. To learn more about the limitation, see this Microsoft KB article.

Software

The following required 3rd party software is included in the Veeam Agent for Microsoft Windows Redistributable.

- Microsoft .NET Framework 4.7.2
- Microsoft SQL Server 2012 Management Objects
- Microsoft SQL Server System CLR Types

During the Veeam Agent deployment process, Veeam Backup & Replication checks whether all prerequisite software is available on the target computer. If some of the required software components are missing, Veeam Backup & Replication will install missing software automatically.

Microsoft SQL Database

Microsoft SQL Server 2012 SP4 Express LocalDB Edition (installed within the Veeam Agent deployment process).

Veeam Agent Computer (Linux)

A machine that you want to protect with Veeam Agent for Linux must meet the following requirements:

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>CPU: x86-64 processor (i386 or later).</td>
</tr>
<tr>
<td></td>
<td>Memory: 1 GB RAM or more. Memory consumption varies depending on the backup type and the total amount of backed-up data.</td>
</tr>
<tr>
<td></td>
<td>Disk Space: 100 MB free disk space for product installation.</td>
</tr>
<tr>
<td></td>
<td>Network: 10 Mbps or faster network connection to a backup target.</td>
</tr>
<tr>
<td></td>
<td>System firmware: BIOS or UEFI.</td>
</tr>
<tr>
<td></td>
<td>Disk layout: MBR or GPT.</td>
</tr>
<tr>
<td></td>
<td>For virtual machines: Only full virtualization type is supported. Containers and paravirtualized instances are not supported. OVM is supported with limitations.</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Linux kernel 2.6.32 or later is supported.</td>
</tr>
</tbody>
</table>
|               | Both 64-bit and 32-bit versions of the following distributions are supported:
|               | - Debian 6 - 10.3 |
• Ubuntu 10.04, 16.04, 18.04, 19.10
• RHEL 6.0 - 8.1³
• CentOS 6.0 - 8.1³
• Oracle Linux 6 (starting from UEK R1) - Oracle Linux 7 (up to UEK R5 U2)
• Oracle Linux 6 - 8.1 (RHCK)³
• Fedora 30 – 31
• openSUSE Tumbleweed
• openSUSE Leap 15.1
• SLES 11 SP4, 12 SP1 – 15 SP1
• SLES for SAP 11 SP4, 12 SP1 – 15 SP1

1 As long as you use kernels supplied by your distribution. Consider the following limitations:
   • Fedora is supported up to kernel 5.4.14, inclusive.
   • openSUSE Tumbleweed is supported up to kernel 5.1.7, inclusive.
   • Linux kernel 2.6.32-754.6.3 in CentOS / RHEL and Oracle Linux (RHCK) is not supported.

2 For Debian 6 – 7, CentOS / RHEL 6.0 – 6.3, Fedora and openSUSE 11.3 – 13.2, 42.0 – 42.1, Tumbleweed distributions, automatic Veeam Agent deployment from Veeam Backup & Replication is not supported. You need to install Veeam Agent for Linux directly on a target machine. For details, see the Installing Veeam Agent for Linux section in the Veeam Agent for Linux User Guide.

After that, you can add this machine to the Veeam Backup & Replication inventory and start managing Veeam Agent running on the machine.

3 RHEL and derivatives running kernel 3.10.0-1062 or later require Veeam Agent for Linux build 3.0.2.1190. RHEL / CentOS / Oracle Linux (RHCK) 6.10 and 7.6 are supported up to certain kernel versions. For details, see this Veeam KB article.

<table>
<thead>
<tr>
<th>File System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Agent for Linux supports consistent snapshot-based data backup for the following file systems¹:</td>
</tr>
<tr>
<td>• Btrfs (for OSes that run Linux kernel 3.16 or later)</td>
</tr>
<tr>
<td>• Ext 2/3/4</td>
</tr>
<tr>
<td>• F2FS</td>
</tr>
<tr>
<td>• FAT16</td>
</tr>
<tr>
<td>• FAT32</td>
</tr>
<tr>
<td>• HFS</td>
</tr>
<tr>
<td>• HFS+</td>
</tr>
<tr>
<td>• JFS</td>
</tr>
<tr>
<td>• NILFS2</td>
</tr>
<tr>
<td>• NTFS</td>
</tr>
<tr>
<td>• ReiserFS</td>
</tr>
<tr>
<td>• XFS</td>
</tr>
</tbody>
</table>

The supported file system (except for Btrfs) can reside on a simple volume or LVM2 volume. Btrfs is supported only if it resides directly on a physical device with no additional abstraction layers (such as LVM, software RAID, dm-crypt and so on) below or above it.
Data that reside in other file systems (including NFS and SMB shares) can be backed up using the snapshot-less mode. For details, see the Snapshot-Less File-Level Backup section in the Veeam Agent for Linux User Guide.

1 Consider the following:

- Veeam Agent for Linux does not back up volumes that reside on USB devices.
- The `veemsnap` module provides RAM-based changed block tracking (CBT) mechanism. Every time the module is unloaded or Veeam Agent for Linux computer is rebooted, CBT data is reset. As a result, Veeam Agent reads the entire data added to the backup scope to detect what blocks have changed since the last job session, and incremental backup requires greater time.
- Backup of machines used as cluster nodes is not supported (that includes backup of machines that use shared disks, clustered file systems or clustered LVM).
- Certain limitations for EMC PowerPath configuration apply. To learn more, see this Veeam KB article.
- BFQ I/O scheduler is not supported.

### Software

**Important!** Linux user account used to work with Veeam Agent for Linux must have the `/bin/bash` shell set as the default shell.

Protected computer must have the following components installed:

- `dkms`
- `gcc`
- `make`
- `perl`
- `kernel-headers`
- `kernel-devel`
- `libudev`
- `libacl`
- `libattr`
- `lvm`
- `libfuse`
- `libncurses`
- `dmidecode`
- `openssh-server`
- `openssh-clients`
- `libmysqlclient`
- `libpq`
- `python`
- `btrfs-progs` (for backup of Btrfs file system)
To install Veeam Agent for Linux packages on a target computer, Veeam Backup & Replication uses the default package manager of the Linux distribution running on this computer. During the installation process, the package manager checks whether all prerequisite software is available on the computer. If some of the required software components are missing, the package manager will attempt to install the missing packages from a software repository configured in the OS.

Does not apply to CentOS, RHEL, SLES distributions. For details, see the Installing Veeam Agent for Linux section in the Veeam Agent for Linux User Guide.

For openSUSE 15 and SLES 15 distributions, either of the following packages is required: libncurses5 or libncurses6.

Required for Veeam Agent management — a valid BIOS UUID must be obtainable either from dmidecode | grep -i uuid or from /sys/class/dmi/id/product_uuid. Each Veeam Agent that consumes a license installed in Veeam Backup & Replication must have a unique BIOS UUID. If a valid UUID cannot be obtained, Veeam will generate it automatically.

A package with the MySQL database client library is required to process MySQL database system located on the Veeam Agent server. Package version varies depending on the MySQL database system version that you use.

A package with the PostgreSQL database client library is required to process PostgreSQL database system located on the Veeam Agent server.

Required for CentOS, RHEL 7.0 and later if a pre-built binary kmod-veeamsnap package is to be installed.

Backup Target

Backup can be performed to the following types of storage:

For Veeam Agent backup jobs managed by the backup server
- Veeam Backup & Replication 10 backup repository
- Veeam Cloud Connect 10 cloud repository

For Veeam Agent backup jobs managed by Veeam Agent
- Local (internal) storage of the protected computer (not recommended)
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives, and raw device mapping (RDM) volumes
- Network Attached Storage (NAS) able to represent itself as an SMB (CIFS) share
- Network Attached Storage (NAS) able to represent itself as an NFS share (for backups of Linux machines only)
- Veeam Backup & Replication 10 backup repository
- Veeam Cloud Connect 10 cloud repository

Network

Consider the following:
- Veeam Agent should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Agent cannot work with Veeam Backup & Replication that is located behind the NAT gateway.

- Domain names of all managed servers added to the Veeam backup infrastructure and machines you want to back up must be resolvable into IPv4 addresses.
Licensing Requirements

The Veeam Agent management functionality is licensed by the number of instances. Instances are units (or tokens) that you can use to protect your machines (servers and workstations) with Veeam Agent for Microsoft Windows and Veeam Agent for Linux. The number of instances that you can use depends on the type of license installed in Veeam Backup & Replication:

- **Per-instance license.** If you use a per-instance license in Veeam Backup & Replication, the number of servers and workstations that you can process with Veeam Agents depends on the edition of Veeam Backup & Replication and the number of instances in the license. For more information, see Veeam Licensing Policy.

- **Per-socket license.** If you use a perpetual per-socket license in Veeam Backup & Replication, the product allows you to use up to 6 instances to process Veeam Agents. If the number of sockets in your license is less than 6, you can use the number of instances that equals the number of sockets in the license. For example, if the number of sockets in the license is 5, you can use 5 instances. If the number of sockets in the license is 7, you can use 6 instances.

  Note that you can use Veeam Agents to protect VMs residing on a virtualization host that consumes a per-socket license. In this scenario, Veeam Agents will not consume instances in the license.

- **Community edition.** If you do not install a license in Veeam Backup & Replication, you can use the Community edition of the product. The Community edition of Veeam Backup & Replication allows you to use 10 instances. Functionality available in the Community edition of Veeam Backup & Replication is the same as in the Standard edition of the product.

For more information on Veeam Backup & Replication licensing, see the Licensing section in the Veeam Backup & Replication User Guide.

**TIP:**

After Veeam Agent connects to the Veeam backup server, Veeam Agent starts using instances in the license. You can restrict license consumption for Veeam Agents, for example, if you want to use Veeam Backup & Replication to process VMs and do not want Veeam Agents to use instances in the license. To do this, in the **Instances** tab of the License Information window, clear the Allow unlicensed agents to consume instances check box.
## Supported Applications

**Veeam Agent for Microsoft Windows**

You can use Veeam Agent for Microsoft Windows operating in the managed mode to create transactionally consistent backups of servers running applications that support Microsoft VSS. System requirements for VSS-aware processing are listed in the following table.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Active Directory Domain Controllers</strong></td>
<td>The following versions of Microsoft Active Directory Domain Services servers (domain controllers) are supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2019</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2012 R2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Windows Server 2008 R2 SP1</td>
</tr>
<tr>
<td></td>
<td>Minimum supported domain and forest functional level is Windows 2003.</td>
</tr>
<tr>
<td><strong>Microsoft Exchange</strong></td>
<td>The following versions of Microsoft Exchange are supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Exchange 2019</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Exchange 2016</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Exchange 2013 SP1</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Exchange 2013</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Exchange 2010 SP1, SP2, or SP3</td>
</tr>
<tr>
<td><strong>Microsoft SharePoint</strong></td>
<td>The following versions of Microsoft SharePoint are supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SharePoint 2019</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SharePoint 2016</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SharePoint 2013</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SharePoint 2010</td>
</tr>
<tr>
<td></td>
<td>All editions are supported (Foundation, Standard, Enterprise).</td>
</tr>
<tr>
<td><strong>Microsoft SQL Server</strong></td>
<td>The following versions of Microsoft SQL Server are supported:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2019</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2017</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2014</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2012</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2008</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2005 SP4</td>
</tr>
<tr>
<td></td>
<td>All editions of Microsoft SQL Server except LocalDB are supported.</td>
</tr>
</tbody>
</table>
### Oracle

Oracle Database versions 11g – 19c are supported for the following operating systems (32-bit and 64-bit architecture):

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1

For information about OS requirements for particular Oracle Database versions, see Oracle documentation.

**Important notes:**

- Automatic Storage Management (ASM) is not supported.
- Oracle Real Application Clusters (RAC) are not supported.
- Oracle Database systems running on Microsoft Windows Failover Clusters are not supported.
- Oracle servers using Data Guard are not supported.
- Oracle Database Express Edition is supported.
- Current version does not support creating transactionally-consistent backups of a standby database in case you are using Oracle Active Data Guard; only crash-consistent backups can be created in this case. However, a primary database can be backed up in a transactionally-consistent way.
- Configurations with different versions of Oracle Database deployed on the same server are not supported.
- 32-bit Oracle running on 64-bit operating systems is not supported.

### Veeam Agent for Linux

You can use Veeam Agent for Linux operating in the managed mode to create transactionally consistent backups of servers running Oracle database systems. System requirements for Oracle database processing are listed in the following table.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Oracle        | - Oracle Database versions 11g – 19c are supported for all operating systems supported by Veeam Agent for Linux. To learn more, see System Requirements.  
- Automatic Storage Management (ASM) is not supported.  
- Oracle Real Application Clusters (RAC) are not supported.  
- Oracle Grid Infrastructure is not supported.  
- Oracle Database Express Edition is not supported.  
- SAP on Oracle is not supported.  
- Oracle Database architectures with Data Guard and passive instances are not supported.  
- Configurations with multiple installations of Oracle Database and/or multiple Oracle homes on the same server are not supported. |
<table>
<thead>
<tr>
<th>Database</th>
<th>Supported Versions</th>
<th>Supported Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>5.6 – 8.0</td>
<td>Configurations with multiple MySQL installations and/or instances on the same machine are not supported.</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>9.4 – 12.1</td>
<td>Configurations with multiple PostgreSQL installations and/or instances on the same server are not supported.</td>
</tr>
</tbody>
</table>
# Used Ports

The following tables describe network ports that must be opened to ensure proper communication of components in the Veeam Agent management infrastructure.

## Veeam Backup & Replication Connections

For information about network ports that must be opened to ensure proper communication of the backup server with backup infrastructure components, see the Used Ports section in the Veeam Backup & Replication User Guide.

For information about ports that must be opened to ensure communication of the backup server with Veeam Cloud Connect infrastructure components, see the Used Ports section in the Veeam Cloud Connect Guide.

In addition to general port requirements applicable to a Veeam backup server, the backup server used in the Veeam Agent management scenario must have the following ports opened:

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup Server</td>
<td>Veeam Agent Computer (Microsoft Windows)</td>
<td>TCP</td>
<td>6184</td>
<td>Default port used for communication with the Veeam Agent for Microsoft Windows Service. If the default port number is already in use, Veeam Agent for Microsoft Windows Service will try to use the next port number.</td>
</tr>
<tr>
<td></td>
<td>Veeam Agent Computer (Linux)</td>
<td>TCP</td>
<td>22</td>
<td>Default port used as a control channel from the Veeam Backup Server to the Veeam Agent computer.</td>
</tr>
<tr>
<td>Distribution Server</td>
<td>TCP</td>
<td>UDP</td>
<td>135, 137 to 139, 445</td>
<td>Ports on a Microsoft Windows server used for deploying the Distribution Server component.</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td></td>
<td>49152 to 65535 (for Microsoft Windows 2008 and newer)</td>
<td>Dynamic RPC port range. For more information, see this Microsoft KB article.</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td></td>
<td>9380</td>
<td>Default port used for communication with the Veeam Distribution Service.</td>
</tr>
<tr>
<td>Distribution Server</td>
<td>Veeam Agent Computer (Microsoft Windows)</td>
<td>TCP</td>
<td>49152 to 65535 (for Microsoft Windows 2008 and newer)</td>
<td>Dynamic RPC port range. For more information, see this Microsoft KB article. The port range is required for communication with the Veeam Installer Service.</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>UDP</td>
<td>135, 137 to 139, 445</td>
<td>Ports on the Veeam Agent computer used for deploying Veeam Agent.</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Protocol</td>
<td>Port</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------</td>
<td>----------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Veeam Agent Computer</td>
<td>Veeam Backup Server</td>
<td>TCP</td>
<td>10005</td>
<td>Default port used by Veeam Agent for Microsoft Windows operating in the managed mode for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.</td>
</tr>
<tr>
<td>(Microsoft Windows)</td>
<td></td>
<td></td>
<td></td>
<td>[For Microsoft SQL logs shipping] Ports used to collect Microsoft SQL logs from the Veeam Agent computer.</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td></td>
<td>2500 to 5000</td>
<td>[For Microsoft SQL logs shipping] Ports used to collect Microsoft SQL logs from the Veeam Agent computer operating as part of a failover cluster with SQL Server AlwaysOn Availability Groups.</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td></td>
<td>6167, 2500 to 5000</td>
<td>[For Microsoft SQL logs shipping] Ports used to collect Microsoft SQL logs from the Veeam Agent computer operating as part of a failover cluster with SQL Server AlwaysOn Availability Groups.</td>
</tr>
<tr>
<td>Veeam Agent Computer</td>
<td>Veeam Backup Server</td>
<td>TCP</td>
<td>9395, 6183</td>
<td>Ports used locally on the Veeam Agent computer for communication between Veeam Agent components and Veeam Agent for Microsoft Windows Service. If the default port number is already in use, Veeam Agent for Microsoft Windows Service will try to use the next port number.</td>
</tr>
<tr>
<td>(Linux)</td>
<td>TCP</td>
<td></td>
<td></td>
<td>Default port used for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers.</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td></td>
<td>2500 to 5000</td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
</tr>
<tr>
<td>Veeam Agent Computer</td>
<td>Linux server performing the role of a backup repository</td>
<td>TCP</td>
<td>49152 to 65535</td>
<td>Dynamic RPC port range. For more information, see this Microsoft KB article.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(for Microsoft Windows 2008 and newer)</td>
</tr>
<tr>
<td>Role of a backup repository</td>
<td>Protocol</td>
<td>Port Range</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
<td>------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>TCP 2500 to 5000</td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared folder CIFS (SMB) share</td>
<td>TCP</td>
<td>135, 137 to 139, 445</td>
<td>Ports used as a transmission channel from the Veeam Agent computer to the target CIFS (SMB) share.</td>
<td></td>
</tr>
<tr>
<td>Gateway Microsoft Windows server</td>
<td>TCP</td>
<td>135, 137 to 139, 445</td>
<td>If a CIFS (SMB) share is used as a backup repository and a Microsoft Windows server is selected as a gateway server for this CIFS share, these ports must be opened on the gateway Microsoft Windows server.</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>Dynamic RPC port range. For more information, see this Microsoft KB article.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>2500 to 5000</td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Getting Started

To start using the Veeam Agent management functionality in Veeam Backup & Replication, you must perform the following operations:

1. Deploy Veeam Backup & Replication.
   To learn more, see the Deployment section in the Veeam Backup & Replication User Guide.

2. Configure security settings.
   By default, Veeam Backup & Replication offers the following settings to establish a secure connection between the backup server and protected computers:
   - To establish a secure connection between parties, Veeam Backup & Replication uses the default self-signed certificate.
   - Veeam Backup & Replication allows all new Linux hosts to establish a connection to the backup server.
   You can use the default security settings or change them if needed. To learn more, see Configuring Security Settings.

3. Add computers that you want to protect with Veeam Agents to the Veeam Backup & Replication inventory.
   In Veeam Backup & Replication, computers that you want to protect with Veeam Agents are organized into protection groups. You can use the Veeam Backup & Replication console to create one or more protection groups that include individual computers, Microsoft Active Directory objects or list of computers imported from a CSV file. To learn more, see Creating Protection Groups.

4. Discover protected computers and deploy Veeam Agents.
   Veeam Backup & Replication is set up to automatically discover protected computers and install Veeam Agent on a discovered computer. By default, these operations are performed immediately after you create a protection group. You can change Veeam Agent discovery and deployment options in the protection group settings, if needed. You can also run discovery and deployment operations manually for an entire protection group, individual Active Directory object in a protection group or individual computer in a protection group. To learn more, see Specify Discovery and Deployment Options, Managing Protection Groups and Managing Protected Computers.

5. Configure Veeam Agent backup job settings.
   You can configure one or more Veeam Agent backup jobs and add to these jobs one or more protection groups, Active Directory objects and/or individual computers. In Veeam Backup & Replication, you can configure the following types of Veeam Agent backup jobs:
   - Veeam Agent backup job managed by the Veeam backup server
   - Veeam Agent backup job managed by Veeam Agent, or Veeam Agent backup policy
   To learn more, see Creating Veeam Agent Backup Jobs.

6. Manage Veeam Agent backup jobs.
   You can start, stop, enable and disable Veeam Agent backup jobs to administer data protection operations on protected computers. To learn more, see Managing Veeam Agent Backup Jobs.

7. In case of a disaster, you can restore data from a Veeam Agent backup.
   To learn more, see Restoring Data from Veeam Agent Backups.
Configuring Security Settings

When you configure the Veeam Agent management infrastructure in Veeam Backup & Replication, you can specify what TLS certificate Veeam Backup & Replication will use to establish a secure connection between the backup server and protected computers. By default, Veeam Backup & Replication offers the following security settings for testing and evaluation purposes:

- To establish a secure connection between parties, Veeam Backup & Replication uses the default self-signed certificate.
- Veeam Backup & Replication allows all computers that run a Linux OS to establish a connection to the backup server.

You can change security settings if needed, for example, in case security regulations of your organization require usage of a custom certificate and/or verification of Linux host fingerprints.

To specify the security settings, do the following:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Certificate** section, check information about the currently used certificate. By default, Veeam Backup & Replication uses a self-signed TLS certificate generated during the Veeam Backup & Replication installation process. If you want to use a custom certificate, click **Install** and specify a new certificate. To learn more, see **Managing TLS Certificates**.
4. In the **Linux hosts authentication** section, specify how Veeam Backup & Replication will add Linux-based protected computers to the list of trusted hosts. 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 discovered computers that run a Linux OS to connect to the backup server. This scenario is recommended for demo environments only.
   - **Add unknown hosts to the list manually** — with this option enabled, only the following Linux-based computers can connect to the backup server:
     - Protected computers 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 such computers in the **Trusted hosts** field. You can export the list of trusted Linux computers to a **known_hosts** file. To do this, click **Export** and specify a path to the folder to save the file.
     - Protected computers specified in the **known hosts** file imported to Veeam Backup & Replication. To import a **known hosts** file, click **Import** and specify a path to the folder where the file resides.
     - Protected computers added to the list of trusted hosts in the Veeam Backup & Replication console. To learn more, see **Adding Computers to Trusted Hosts List**.
5. Click **OK**.
Managing TLS Certificates

When you configure the Veeam Agent management infrastructure, you can specify what TLS certificate must be used to establish a secure connection between the backup server and protected computers. 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.
- 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 Certificate Authority (CA), make sure that the certificate meets the requirements. To learn more, see Using Certificate Signed by Internal CA.

Generating Self-Signed Certificates

You can use Veeam Backup & Replication to generate a self-signed certificate for authenticating parties in the Veeam Agent management 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
- Local 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 protected computer, 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**.

![Certificate Management Screen]

- **Certificate Type**
  - **Generate Certificate**
    - **Generate new certificate**
      - Generate a new self-signed certificate that is verifiable with the thumbprint.
  - **Select certificate from the Certificate Store**
    - Use an existing certificate already present in the local Certificate Store of this server.
  - **Import certificate from a file**
    - Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server.
5. At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.
6. 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 Agent management 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**.

![Certificate Management Interface](image)
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**.

![Manage Certificate](image)
5. At the **Import Certificate** step of the wizard, specify a path to the PXF file.

6. If the PFX file is protected with a password, specify the password in the field below.

   ![Image of Manage Certificate dialog box]

   - **Import Certificate**: Specify the PFX file to import certificate from. The certificate will be automatically imported into the local Certificate Store of this server.

   - **Certificate Type**
     - **Import Certificate**
     - **Summary**

   - **Certificate**: cert\NAME_cert.pfx
   - **Password**: ************

   Password is required only if this certificate was exported with the password protection enabled.

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.
Using Certificate Signed by Internal CA

To establish a secure connection between the backup server and protected computers, Veeam Backup & Replication uses a TLS certificate. By default, Veeam Backup & Replication uses a self-signed certificate. Veeam Backup & Replication generates this certificate when you install the product on the Veeam backup server.

In you want to use a certificate signed by your internal Certification Authority (CA), make sure that the following requirements are met:

- Veeam Agents and Veeam Backup & Replication must trust the CA. That is, the Certification Authority certificate must be added to the Trusted Root Certification Authority store on the Veeam backup server and Veeam Agent computers.
- Certificate Revocation List (CRL) must be accessible from the Veeam backup server and Veeam Agent computers.
- [For Linux-based Veeam Agent computers] OpenSSL version 1.0 or later must be installed on the Veeam Agent computer.

A certificate signed by a CA must meet the following requirements:

1. The certificate subject must be equal to the fully qualified domain name of the Veeam backup server. For example: \textit{vbrserver.domain.local}.
2. The following key usage extensions must be enabled in the certificate to sign and deploy child certificates for Veeam Agent computers:

- Digital Signature
- Certificate Signing
- Off-line CRL Signing
- CRL Signing (86)

If you use Windows Server Certification Authority, it is recommended that you issue a Veeam Backup & Replication certificate based on the built-in "Subordinate Certification Authority" template or templates similar to it.
3. The key type in the certificate must be set to Exchange.

If you create a certificate request using the Windows MMC console, to specify the key type, do the following:

a. At the Request Certificates step of the Certificate Enrollment wizard, select a check box next to the necessary certificate template and click Properties.
b. In the **Certificate Properties** window, click the **Private Key** tab.

c. In the **Key Type** section, select **Exchange**.

To start using the signed certificate, you must select it from the certificates store on the Veeam backup server. To learn more, see [Importing Certificates from Certificate Store](#).

After you specify the signed certificate in Veeam Backup & Replication, during the next backup job session Veeam Agents will receive child certificates from the Veeam backup server.
Adding Computers to Trusted Hosts List

After you enable the **Add unknown hosts to the list manually** option in Veeam Backup & Replication settings, Linux-based computers whose fingerprints are not stored in the Veeam Backup & Replication database 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 must add it to the list of trusted hosts manually in the Veeam Backup & Replication console.

To add a computer to the list of trusted hosts:
1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and click **Untrusted**.
3. In the working area, Veeam Backup & Replication will display discovered computers that you can add to the list of trusted hosts. Check fingerprints of the computers and add them to the list of trusted hosts in one of the following ways:
   - To add all computers at once to the list of trusted hosts, select the **Untrusted** node in the inventory pane and click **Trust All** on the ribbon or right-click the **Untrusted** node and select **Trust all**.
To add a specific computer to the list of trusted hosts, select the necessary computer in the working area and click **Trust** on the ribbon or right-click the computer and select **Trust**.
Working with Protection Groups

In Veeam Backup & Replication, Veeam Agent computers are organized into protection groups. You can perform the following operations with protection groups:

- Create a protection group.
- Add a protection group to a Veeam Agent backup job.
- Edit protection group settings.
- Rescan a protection group.
- Assign location to a protection group.
- Disable a protection group.
- Remove a protection group.

Creating Protection Groups

You must add computers that you plan to protect with Veeam Agents to the inventory in the Veeam Backup & Replication console. In Veeam Backup & Replication, protected computers are organized into protection groups. You can create one or more protection groups that contain computers of different types or offer different discovery and deployment options.

**TIP:**

If you do not want to create protection groups, for example, if you plan to manage only a small number of computers in your infrastructure, you can add the necessary computers directly to a Veeam Agent backup job. Veeam Backup & Replication will automatically add such computers to the *Manually Added* protection group. To learn more, see Adding Computers to Backup Job and Protection Groups.
Before You Begin

Before creating a protection group, consider the following prerequisites and limitations:

1. When Veeam Backup & Replication performs discovery of protected computers, Veeam Backup & Replication connects to every computer added to the protection group. If you instruct Veeam Backup & Replication to perform discovery immediately after the protection group is created, make sure that all computers added to the protection group are powered on and may be accessed over the network. Otherwise, Veeam Backup & Replication will be unable to connect to a protected computer and perform the required operations on this computer.

2. A protection group that includes Microsoft Active Directory objects can include objects from one domain only. To add to the inventory computers that reside in another domain, you need to create a separate protection group and include in this protection group the necessary objects from that domain.

3. Veeam Backup & Replication automatically excludes from the protection scope Active Directory objects of the Group type that exist in a parent Active Directory object (organization unit, container or entire domain) specified in the protection group settings. To instruct Veeam Backup & Replication to process a group, you must select this group explicitly in the protection group settings.

4. You cannot add and/or exclude universal and domain local groups to/from protection groups that include Microsoft Active Directory objects. Only global groups are supported.

5. It is recommended that you do not add a computer to a protection group by specifying a dynamic IP address assigned to this computer. If such computer receives another IP address from a DHCP server, Veeam Backup & Replication will be unable to discover the computer and perform on this computer operations defined in the protection group settings.

6. It is recommended that you do not add a computer to a protection group by specifying a public IP address assigned to this computer. If you add such computer to a backup policy targeted at a cloud repository, the name of the subtenant account created for the computer can contain the public IP address. This IP address will be visible to the Veeam Cloud Connect service provider who has access to subtenant account settings.

7. It is recommended that you include each computer in one protection group only. For example, if you have added an Active Directory container to a protection group, it is not recommended to add a computer that exists in this container to another protection group. Adding computers to multiple protection groups with different computer discovery and Veeam Agent deployment settings will result in additional load on the backup server.

8. You can add a cluster only to a protection group that includes Microsoft Active Directory objects. You cannot add clusters to protection groups that include individual computers or computers specified in a CSV file.

9. To deploy Veeam Installer Service and Veeam Agent for Microsoft Windows on a protected computer, Veeam Backup & Replication uses the administrative share (admin$) of the target computer. An account that you plan to use to connect to a computer included in the protection group must have access to the administrative share.

   Note that in client Microsoft Windows OSes access to the administrative share is forbidden by default for local accounts. You can enable this option with a registry key. For details, see this Microsoft KB article.

10. Veeam Backup & Replication does not support usage of a Linux account with the modified PS1 shell variable to connect to a computer included in the protection group.

Step 1. Launch New Protection Group Wizard

To launch the New Protection Group wizard, do one of the following:
- Open the **Inventory** view. Click the **Physical Infrastructure** node in the inventory pane and click **Add Group** on the ribbon.

- Open the **Inventory** view. Click the **Physical Infrastructure** node in the inventory pane and click **Create Protection Group** in the working area.

- Open the **Inventory** view. Right-click the **Physical Infrastructure** node in the inventory pane and select **Add protection group**.

```
CREATE PROTECTION GROUP
Protection group defines a set of computers (physical server, workstations or cloud instances) to be protected with agent-based backup jobs. Protection groups can be populated with individual computers, Active Directory containers or a dynamic CSV file exported from an management system.

CREATE JOB OR POLICY
Agent-based protection provides additional flexibility with two deployment approaches. For 24/7 workloads such as servers and fileserver, we recommend that you create backup jobs managed by the backup server, which controls scheduling and retains backup remotely. For any workloads which may remain offline or unreachable for extended and/or unpredictable time periods (such as virtualisations, laptops or remote office servers), we recommend that you create backup policy that configures backup agents to schedule and execute backup independently.

PERFORM RESTORE
To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other restore options include direct restore to Microsoft Azure, or install recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the backups tree of the home tab, and select one of many restore options provided.
```
Step 2. Specify Protection Group Name and Description

At the Name step of the wizard, specify a name and description for the protection group.

1. In the Name field, specify a name for the protection group.
2. In the Description field, provide a description for future reference. The default description contains information about the user who added the protection group, date and time when the protection group was created.

### New Protection Group

<table>
<thead>
<tr>
<th>Name</th>
<th>Windows Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Protection group for Windows based server</td>
</tr>
</tbody>
</table>

Step 3. Select Protection Group Type

At the Type step of the wizard, select the type of the protection group.

**NOTE:**

You can add a Microsoft failover cluster to a protection group based on Microsoft Active Directory objects only. To do this, you must select the Microsoft Active Directory objects option and then add a cluster account or an AD object containing this account at the Active Directory step of the wizard.
You can select one of the following types:

- **Individual computers** — select this option if you want to define a static protection scope by adding specific computers to the protection group. This option is recommended for smaller environments that do not have Microsoft Active Directory deployed. With this option selected, you will pass to the Computers step of the wizard.

- **Microsoft Active Directory objects** — select this option if you want to add to the protection group one or several Active Directory objects: entire domain, container, organization unit, group, computer or cluster. Protection groups that include Active Directory containers and/or organization units are dynamic in their nature. If a new computer is added to a container or organization unit that you have specified in the protection group settings, during the next rescan session, Veeam Backup & Replication will discover this computer and (optionally) deploy Veeam Agent on this computer. With this option selected, you will pass to the Active Directory step of the wizard.

- **Computers from CSV file** — select this option if you want to add to the protection scope computers listed in a CSV file that resides in a local folder on the backup server or in a network shared folder. As well as protection groups that include Active Directory containers, protection groups of this type are also dynamic. If a new computer appears in a CSV file after the protection job is created, within the next rescan session, Veeam Backup & Replication will automatically update the protection group settings to include the added computer. With this option selected, you will pass to the CSV File step of the wizard.
Step 4. Specify Protection Scope

Specify protection scope for the created protection group:

- **Specify computers** — if you have selected the *Individual computers* option at the Type step of the wizard.
- **Specify Microsoft Active Directory objects** — if you have selected the *Microsoft Active Directory objects* option at the Type step of the wizard.
- **Specify a CSV file** — if you have selected the *Computers from CSV file* option at the Type step of the wizard.

Specifying Computers

The **Computers** step of the wizard is available if you have chosen the *Individual computers* option at the Type step of the wizard.

At this step of the wizard, you can specify computers that you want to add to the protection group.

To add a computer to a protection group:

1. Click **Add**.
2. In the **Add Computer** window, in the **Host name or IP address** field, enter a full DNS name, NetBIOS name or IP address of the computer that you want to add to the protection group.
3. From the **Credentials** list, select a user account that has administrative permissions on the computer that you want to add to the protection group. Veeam Backup & Replication will use this account to connect to the protected computer and perform the necessary operations on the computer: upload and install Veeam Agent, and so on.
   
   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 the **Credentials Manager** section in the Veeam Backup & Replication User Guide.
4. Repeat steps 1–3 for every computer that you want to add to the protection group.
5. To check if Veeam Backup & Replication can communicate with computers added to the protection group, click **Test Now**. Veeam Backup & Replication will use the specified credentials to connect to all computers in the list.
NOTE:

If you chose to manually add Linux-based computers to the list of trusted hosts in Veeam Backup & Replication, when you test credentials for an unknown Linux-based computer in the protection group settings, the test operation will complete with the Failed status. This happens because Veeam Backup & Replication cannot connect to the untrusted computer before you add this computer to the list of trusted hosts. To learn more, see Adding Computers to Trusted Hosts List.

Specifying Active Directory Objects

The Active Directory step of the wizard is available if you have chosen the Microsoft Active Directory objects option at the Type step of the wizard.

At this step of the wizard, you can select Active Directory objects that you want to add to the protection group. You can add to a protection group the following types of Active Directory objects: domain, organization unit, container, computer, cluster, or group.

To add Active Directory objects to a protection group:

1. In the Search for objects in this domain field, click Change.
2. In the Specify Domain window, specify settings of the domain whose objects you want to include in the protection group:
   a. In the Domain controller or domain DNS name field, type a name of the domain controller or domain whose objects you want to include in the protection group.
   b. In the Port field, specify a port number over which Veeam Backup & Replication must communicate with the domain controller. By default, Veeam Backup & Replication uses port 389.
c. From the **Account** list, select a user account that is a member of the `DOMAIN\Administrators` group. 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 the **Credentials Manager** section in the Veeam Backup & Replication User Guide.

d. Click **OK** to close the **Specify Domain** window.

**NOTE:**

If you want to include a large number of computers in the protection group but do not want to use an account with domain administrator permissions in the protection group settings, consider configuring a protection group based on a list of computers imported from a CSV file. To learn more, see **Select Protection Group Type**.

3. In the **Selected objects** field, click **Add**.

4. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

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

   a. Click the button to the left of the search field and select the necessary type of object to search for: **Everything**, **Computer**, **Cluster**, **Organization Unit**, **Container** or **Group**.

   b. Enter the object name or a part of it in the search field.

   c. Click the **Start search** button on the right or press **[ENTER]**.
Specifying CSV File

The CSV File step of the wizard is available if you have chosen the Computers from CSV file option at the Type step of the wizard.

At this step of the wizard, you can specify a file that defines a list of computers that you want to add to the protection group. You must specify a list of computers in a file of the CSV or TXT format. The file must be created beforehand. To learn more, see Preparing CSV File.

To specify a CSV file:

1. In the Path to file field, click Browse and specify a path to a CSV file that contains a list of IP addresses or domain names of computers that you want to add to the protection group. The CSV file can reside in a folder on the local drive of the Veeam backup server or in a network shared folder accessible from the backup server.

2. In the Computers field, review the list of IP addresses or domain names imported from the CSV file.

**NOTE:**

After you finish configuring the protection group, Veeam Backup & Replication will perform discovery of computers listed in the CSV file upon schedule defined in the protection group settings. If Veeam Backup & Replication is unable to read the CSV file (for example, after the file was moved or deleted from the specified location), the rescan job will use the list of computers imported from the CSV file during the previous rescan job session.
Preparing CSV File

To define a dynamic protection scope based on a list of computers, you must create a CSV file with a list of IP addresses or domain names to scan during discovery. Veeam Backup & Replication supports IP addresses of the IPv4 format only.

Delimit IP addresses or domain names in the list with commas (','), or semicolons (';'). For example:

```
172.17.53.16,172.17.53.19,172.17.53.31,172.17.53.40
```

Alternatively, you can delimit IP addresses or domain names in the list with the newline character:

```
172.17.53.16
172.17.53.19
172.17.53.31
172.17.53.40
```

Step 5. Exclude Objects from Protection Group

The **Exclusions** step of the wizard is available if you have chosen to define a protection scope that includes Microsoft Active Directory objects.

At this step of the wizard, you can specify which objects you want to exclude from the protection group. You can exclude the following types of objects:

- All virtual machines — all VMs residing in the domain. You can select this option, for example, if you do not want to protect VMs with Veeam Agents and want to back up VM data with Veeam Backup & Replication instead.
- All computers that have been offline for over 30 days — all computers in the domain that have not logged on to Active Directory for more than 30 days.
- Individual Active Directory objects — specific Active Directory objects: computers, clusters, groups, organization units and/or containers. With this option selected, you must specify Active Directory objects that you want to exclude from the protection group.

To exclude Active Directory objects:

1. In the **Exclude** section, select the **The following objects** check box.
2. Click **Add**.
3. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK**. You can press and hold [CTRL] to select multiple objects at once.
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, Computer, Cluster, Group, Organization Unit or Container.

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 6. Specify Credentials

The Credentials step of the wizard is available if you have chosen to define a protection scope that includes Microsoft Active Directory objects or computers specified in a CSV file.

At this step of the wizard, specify credentials to connect to computers included in the protection group:

1. If you want to use the same credentials for all computers in the protection group, select the necessary user account from the Master account list. The account must have local administrator permissions on all computers that you have added to the protection group.

   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 the Credentials Manager section in the Veeam Backup & Replication User Guide.
2. By default, Veeam Backup & Replication uses credentials specified in the Master account field for all computers in the protection group. If some computer requires a different user account, do the following:

   a. Select the Use custom credentials for the following objects check box,

   b. Click Add next to the list of objects and select the necessary object in the Add Objects window:
      
      - If you configure a protection group that includes Active Directory objects, objects that you have added to the protection group at the Active Directory step or the wizard are already displayed in the Use custom credentials for the following objects list. In the Add Objects window, you can also select child objects for which you want to specify custom credentials. For example, you may want to specify separate credentials for different organization units, containers, groups or individual computers within the entire domain added to the protection group.

      - If you configure a protection group that includes computers specified in a CSV file, you can select in the Add Objects window one or more computers listed in a CSV file and add them to the Use custom credentials for the following objects list.

   c. In the Use custom credentials for the following objects list, select the necessary object, click Edit and select custom credentials for the object. Credentials must be specified in the following format:
      
      - For Active Directory accounts — DOMAIN\Username
      - For local accounts — Username or HOST\Username

**NOTE:**

Consider the following:

- If you configure a protection group that includes dynamic Active Directory objects, such as domain, organization unit, container or group, the master account or custom account specified for an object must be a member of the DOMAIN\Administrators group.

- If you plan to back up Oracle databases that run on Linux-based machines, the account used to connect to the machine must be a member of the oinstall group.
To check if Veeam Backup & Replication can connect to computers added to the protection group, click **Test Now**. Veeam Backup & Replication will form a list of computers to connect and use the specified credentials to connect to computers in the list.

Step 7. Specify Discovery and Deployment Options

At the **Options** step of the wizard, specify settings for protected computers discovery and Veeam Agent deployment.

Veeam Backup & Replication regularly connects to protected computers according to the schedule defined in the protection group settings. At this step of the wizard, you can define the discovery schedule and specify operations that Veeam Backup & Replication must perform on discovered computers. You can also select which server in your backup infrastructure should act as a distribution server for Veeam Agents.

To specify discovery and deployment options:

1. In the **Discovery** section, define schedule for automatic computer discovery within the scope of the protection group:

   o To run the rescan 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.

   o To run the rescan 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 rescan job. In the **Start time within an hour** field, specify the exact time when the job must start.

   o To run the rescan job continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new rescan job session will start as soon as the previous rescan job session finishes.
NOTE:
You cannot create a protection group without defining schedule for automatic discovery. However, you can disable automatic discovery for a specific protection group, if needed. To learn more, see Disabling Protection Group.

2. In the Deployment section, from the Distribution server list, select a Microsoft Windows server that you plan to use as a distribution server. Veeam Backup & Replication will use the distribution server to upload Veeam Agent setup archives to computers added to the protection group. By default, Veeam Backup & Replication assigns the distribution server role to the backup server. To learn more, see Distribution Server.

3. If you want to instruct Veeam Backup & Replication to automatically deploy Veeam Agents on all discovered computers in the protection group, in the Deployment section, make sure that the Install backup agent automatically check box is selected.
   
   You can also choose to disable automated Veeam Agent installation. In this case, you will need to install Veeam Agent on every computer included in the protection group and discovered by Veeam Backup & Replication. To learn more, see Installing Veeam Agent.

NOTE:
Veeam Backup & Replication installs the Veeam Installer Service on every computer added to the protection group even if the Install backup agent automatically check box is not selected in the protection group settings.

4. If you want to instruct Veeam Backup & Replication to automatically upgrade Veeam Agent on discovered computers when a new version of Veeam Agent appears on the distribution server, in the Deployment section, make sure that the Auto-update backup agent check box is selected.

5. [For protection groups that include Microsoft Windows servers] Select the Install changed block tracking driver on Windows Server OS check box if you want to install the advanced changed block tracking (CBT) driver on servers protected with Veeam Agent for Microsoft Windows. To learn more, see the Veeam Changed Block Tracking Driver section in the Veeam Agent for Microsoft Windows User Guide.

   If you included workstations and servers in the created protection group, Veeam Backup & Replication will install the Veeam CBT driver on servers only.
6. Select the **Perform reboot automatically if required** check box to allow Veeam Backup & Replication to reboot a protected computer. In particular, the reboot operation is required as part of the Veeam CBT driver installation process.

7. Click **Advanced** to specify advanced settings for the protection group. To learn more, see **Specify Advanced Protection Group Settings**.

---

**Step 8. Specify Advanced Protection Group Settings**

In the **Advanced Settings** window, specify advanced settings for the protection group:

- **Veeam Agent for Microsoft Windows settings**
- **Notification settings**

**TIP:**

After you specify necessary settings for the protection group, 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 protection group, Veeam Backup & Replication will automatically apply the default settings to the new protection group.
Veeam Agent for Microsoft Windows Settings

You can specify the following settings for Veeam Agent for Microsoft Windows that will be deployed on computers included in the protection group:

- **Network usage settings.** You can limit bandwidth consumption and restrict network connections usage for Veeam Agent for Microsoft Windows backup jobs. Limiting bandwidth consumption prevents jobs from utilizing the entire bandwidth available in your environment and makes sure that enough traffic is provided for other network operations. In addition to limiting bandwidth consumption, you can choose whether to allow backup over metered connections and VPN connections. For Microsoft Windows workstations that run Veeam Agent, you can also specify one or more wireless networks over which Veeam Agent is allowed to perform backup.

  To learn more, see the Restricting Network Connections Usage section in the Veeam Agent for Microsoft Windows User Guide.

- **Throttling settings.** You can instruct Veeam Agent for Microsoft Windows to throttle its activities during backup. The throttling option can help you avoid situations when backup tasks performed by Veeam Agent for Microsoft Windows consume all available hard disk resources and hinder work of other applications and services on a protected computer. With throttling enabled, Veeam Backup & Replication sets low priority for Veeam Agent components running on protected computers and engaged in the backup process. If this option is not enabled, Veeam Agent components have normal priority.

- **Security settings.** You can allow user accounts that do not have administrative privileges on a Veeam Agent computer to perform file-level restore on this computer.

Veeam Backup & Replication applies the specified settings to Veeam Agent that runs on a protected computer added to a backup policy. Veeam Backup & Replication applies the settings during the protection group rescan process. Settings are saved to the Veeam Agent for Microsoft Windows database on the protected computer.

These settings are not applied to protected computers added to a Veeam Agent backup job managed by the backup server.

To specify settings for Veeam Agent for Microsoft Windows:

1. At the **Options** step of the wizard, click **Advanced**.
2. If you want to limit bandwidth consumption for Veeam Agent backup jobs, on the **Agent for Windows** tab, in the **Network** section, select the **Limit bandwidth consumption to** check box. Then specify the maximum speed for transferring backed-up data from the Veeam Agent computer to the target location.
3. By default, backup over metered connections is disabled for Veeam Agent for Microsoft Windows. Veeam Agent automatically detects metered connections and does not perform backup when your computer is on such connection. To enable backup over metered connections, clear the **Restrict metered connections usage** check box.

**NOTE:**

Mind the following limitations and requirements:

- Veeam Agent for Microsoft Windows disables backup over metered Internet connections only on computers that run Microsoft Windows 8 and later. If the computer runs an earlier version of Microsoft Windows, this option is not applicable.
- You must specify which connections are metered in Microsoft Windows. To learn more, see this Microsoft webpage.
4. If you want to disable backup over VPN connections, select the **Restrict VPN connections usage** check box. Veeam Agent for Microsoft Windows will automatically detect VPN connections and will not perform backup when the Veeam Agent computer is on such connection.

5. If you want to restrict usage of wireless networks for Veeam Agent running on Microsoft Windows workstations, do the following:
   a. Select the **Restrict Wi-Fi usage to these networks only** check box and click **Add**.
   b. In the **Wi-Fi Network** window, specify the SSID of the Wi-Fi network over which Veeam Agent will be allowed to perform backup, and click **OK**.

   Veeam Backup & Replication will add the specified network to the list of allowed Wi-Fi networks. Backup over other wireless networks will be disabled for Veeam Agent.

6. If you want to throttle Veeam Agent activities during backup, in the **Backup I/O control** section, make sure that the **Throttle agent activity on** option is selected. Then select the type of computers on which to throttle Veeam Agent backup activities: **Workstations only**, **Servers only** or **All hosts**.

   If you do not want to throttle backup activities for Veeam Agent, select **Do not throttle agent**.

7. In the **Security** section, select the **Allow file level recovery without administrative account** check box. With this option enabled, you will be able to perform file-level restore under an account that does not have administrative privileges on the Veeam Agent computer. To learn more, see [Restoring Files and Folders](#).
Notification Settings

You can specify email notification settings for the protection group. If you enable notification settings, Veeam Backup & Replication will send a daily email report with protection group statistics to a specified email address. The report contains cumulative statistics for rescan job sessions performed for the protection group within the last 24-hour period.

NOTE:

Email reports with protection group statistics will be sent only if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.

After you enable notification settings for the protection group, in addition to reports sent according to the global email notification settings, Veeam Backup & Replication will send reports with the protection group statistics to email addresses specified in the protection group settings. This allows you to fine-tune email notifications in Veeam Backup & Replication: while one or more backup administrators receive email notifications according to the global settings, other backup administrators can receive reports for specific protection groups only.

If you do not enable global email notification settings in Veeam Backup & Replication, notification settings for the protection group will not be sent even if you enable them in the protection group settings.

To specify notification settings for the protection group:

1. At the Options step of the wizard, click Advanced.
2. Click the Notifications tab.
3. Select the Send daily agent status report e-mail to the following recipients check box and specify a recipient's email address. You can enter several addresses separated by a semicolon.
4. In the Send at field, specify the time when Veeam Backup & Replication must send the daily email report for the protection group.
5. You can choose to use global notification settings or specify custom notification settings.

To receive a typical notification for the protection group, select Use global notification settings. In this case, Veeam Backup & Replication will apply to the protection group global email notification settings specified for the backup server.

To configure a custom notification for the protection group, select Use custom notification settings specified below. You can specify the following notification settings:

- In the Subject field, specify a notification subject. You can use the following variables in the subject:
  - %JobResult% — rescan job result.
  - %PGName% — protection group name.
  - %FoundCount% — number of new computers discovered within the last 24-hour period.
  - %TotalCount% — total number of computers in the protection group.
  - %SeenCount% — number of computers in the protection group that were online for the last 24 hours. A computer is considered to be online if Veeam Backup & Replication successfully connected to this computer during the last rescan session.
Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.
Step 9. Review Components

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

1. Review the components.
2. Click **Apply** to add the configured protection group to the inventory.
Step 10. Assess Results

At the **Apply** step of the wizard, Veeam Backup & Replication will create the configured protection group. Wait for the operation to complete and click Next to continue.
Step 11. Finish Working with Wizard

At the **Summary** step of the wizard, complete the protection group configuration process.

1. Review information about the created protection group.

2. To start the rescan job after you close the wizard, make sure that the **Run discovery when I click Finish** option is selected.
   
   If you want to perform computer discovery later, you can clear the **Run discovery when I click Finish** check box. In this case, the rescan job will start automatically upon the defined schedule. You can also start the rescan job manually at any time you need. To learn more, see [Starting Protection Group Discovery](#).

3. Click **Finish** to close the wizard.
Adding Protection Group to Backup Job

You can quickly add an entire protection group to a Veeam Agent backup job configured in Veeam Backup & Replication.

**NOTE:**

If you add a protection group that contains both Microsoft Windows computers and Linux computers to a Veeam Agent backup job for Microsoft Windows computers, Veeam Backup & Replication will automatically exclude Linux computers from this backup job. In the same way, if you add such protection group to a Veeam Agent backup job for Linux computers, Veeam Backup & Replication will automatically exclude Microsoft Windows computers from this backup job.

To add a protection group to a Veeam Agent backup job:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and do one of the following:
   - **For Microsoft Windows computers**
     - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup > Windows > name of the job** on the ribbon.
     - In the inventory pane, right-click the protection group that you want to add to the backup job and select **Add to backup job > Windows > name of the job**.
   - **For Linux computers**
     - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup > Linux > name of the job** on the ribbon.
     - In the inventory pane, right-click the protection group that you want to add to the backup job and select **Add to backup job > Linux > name of the job**.
Editing Protection Group Settings

You can edit settings of a protection group. This operation may be required, for example, if you want to add/remove computers to/from a protection group or change settings for protected computers discovery and Veeam Agent deployment defined in the properties of the protection group.

NOTE:

Consider the following:

- You cannot change the type of a protection group when editing protection group settings.
- For the Manually Added protection group, you can change only a limited number of settings. In particular, you can edit protected computers discovery and Veeam Agent deployment options (except for changing the distribution server for the protection group). You can also remove from this protection group computers that are no longer included in a Veeam Agent backup job.
- You cannot edit settings of default protection groups that act as filters used to display protected computers of a specific type: Unmanaged, Out of Date, Offline and Untrusted.

To edit protection group settings:

1. Open the Inventory view.
2. In the inventory pane, expand the Physical Infrastructure node.
3. In the inventory pane, select the protection group that you want to edit and click Edit Group on the ribbon or right-click the protection group that you want to edit and select Properties.
4. Edit protection group settings as required.
Rescanning Protection Group

You can rescan a protection group configured in the inventory. When you perform protection group rescan, you manually start the discovery process for the protection group. This operation may be required, for example, if you want to discover new computers added to the protection group without waiting for the next scheduled start of the rescan job.

During the rescan operation, Veeam Backup & Replication starts the rescan job in the same way as in case of scheduled discovery. The rescan job connects to computers included in the protection group and performs on these computers operations specified in the protection group settings. For example, if Veeam Backup & Replication is set up to automatically install Veeam Agent on protected computers during discovery, you can use the rescan operation to deploy Veeam Agent to computers that have appeared in the protection group after the previous scheduled rescan job session finished.

To rescan a protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.
Assigning Location to Protection Group

You can assign a location to a protection group configured in Veeam Backup & Replication. To assign a location:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Location** > `<Location name>` on the ribbon or right-click the necessary protection group and select **Location** > `<Location name>`.

To learn more about locations, see the **Locations** section in the Veeam Backup & Replication User Guide.
Disabling Protection Group

You can temporarily disable a protection group configured in the inventory. When you disable a protection group, you disable scheduled discovery of protected computers added to this protection group. This may be required, for example, if a new version of Veeam Agent appears on a distribution server, and you do not want to deploy Veeam Agent to all protected computers at once. Instead, you can disable the protection group, test the deployment process on a specific computer in this group, and then enable the protection group to let Veeam Backup & Replication deploy Veeam Agent to remaining computers.

When you disable a protection group, Veeam Backup & Replication does not start the rescan job upon schedule defined in the protection group settings. However, you can start the discovery process manually if needed. To learn more, see Rescanning Protection Group.

Disabling a protection group does not affect processing of Veeam Agent computers included in this protection group. If a protected computer is added to a Veeam Agent backup job, and the backup job is scheduled to start at the time when the protection group is in the disabled state, the backup job will run as usual.

**NOTE:**

You cannot disable default protection groups that act as filters used to display protected computers of a specific type: Unmanaged, Out of Date, Offline and Untrusted.

To disable automatic discovery for the protection group:

1. Open the Inventory view.
2. In the inventory pane, expand the Physical Infrastructure node.
3. In the inventory pane, select the necessary protection group and click Disable on the ribbon or right-click the necessary protection group and select Disable.
To enable automatic discovery for the protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Disable** on the ribbon or right-click the necessary protection group and select **Disable**.
Removing Protection Group

You can remove a protection group that you configured.

When you remove a protection group, you can instruct Veeam Backup & Replication to remove Veeam Agents from all protected computers included in this protection group, too. The protection group is removed permanently. You cannot undo this operation.

Backups created for computers that were included in the removed protection group remain intact in the backup location. You can delete this backup data manually later if needed.

**NOTE:**

Consider the following:

- You cannot remove a protection group if the entire protection group or a separate computer included in this protection group is added to a Veeam Agent backup job.
- You cannot remove default protection groups, such as *Manually Added*, *Unmanaged*, and so on.

**TIP:**

You can also remove separate computers from protection groups. To learn more, see Removing Computer from Protection Group.
To remove a protection group:

1. Open the **Inventory** view.

2. In the inventory pane, expand the **Physical Infrastructure** node.

3. In the inventory pane, select the protection group that you want to remove and click **Remove Group** on the ribbon or right-click the protection group and select **Remove**.

4. If you want to remove Veeam Agent deployed on protected computers, in the displayed window, select the **Uninstall Agents** check box. With this option selected, Veeam Backup & Replication will remove the protection group from the configuration database and, in addition, uninstall Veeam Agent and Veeam Installer Service from every computer in the deleted protection group.

5. In the displayed window, click **Yes**.
Working with Veeam Agent Backup Jobs

You can perform the following operations with Veeam Agent backup jobs in Veeam Backup & Replication:

- Create Veeam Agent Backup jobs
- Manage Veeam Agent Backup jobs

Creating Veeam Agent Backup Jobs

To back up data of your protected computers, you must configure a Veeam Agent backup job in Veeam Backup & Replication. The Veeam Agent backup job defines what data to back up, how, where and when to back up data. One Veeam Agent backup job can be used to process one or more protected computers.

In Veeam Backup & Replication, you can create Veeam Agent backup jobs of the following types:

- The backup job that runs on the backup server in the similar way as a regular job for VM data backup. The backup job is intended for protected computers that have permanent connection to the backup server. To learn more, see Backup Job.
- The backup policy that describes configuration of individual Veeam Agent backup jobs that run on protected computers. Veeam Backup & Replication uses the backup policy as a saved template and applies settings from the backup policy to Veeam Agents that run on computers added to the backup policy. The backup policy is intended for protected computers that may have limited connection to the backup server. To learn more, see Backup Policy.

Veeam Backup & Replication lets you create backup jobs and policies for the following types of protected computers:

- Microsoft Windows computers — computers protected with Veeam Agent for Microsoft Windows
- Linux computers — computers protected with Veeam Agent for Linux

To learn more, see Veeam Agent Backup Jobs and Policies.

One protected computer may be processed with one or more Veeam Agent backup jobs. To learn more, see Processing One Computer with Multiple Jobs and Policies.
Creating Agent Backup Job for Windows Computers

To back up data of a computer protected with Veeam Agent for Microsoft Windows, you must configure a Veeam Agent backup job in Veeam Backup & Replication.

Before You Begin

Before you create a Veeam Agent backup job in the Veeam Backup & Replication console, check the following prerequisites:

- The Veeam Backup & Replication license must have a sufficient number of instances to process servers and/or workstations that you plan to add to the Veeam Agent backup job.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the job must be configured in advance.
- [For backup jobs targeted at the cloud repository] The Veeam Cloud Connect service provider must be added in the Veeam backup console.

Veeam Agent backup jobs have the following limitations:

- [For Veeam Agent backup job managed by backup server] You can create Veeam Agent backups on a Veeam backup repository only. Other types of target locations are not supported.
- [For Veeam Agent backup job managed by Veeam Agent] You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Agent for Microsoft Windows does not support file-level backup for backup jobs that include clusters.
- Veeam Agent for Microsoft Windows does not back up data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.
- After you start managing a Veeam Agent computer with Veeam Backup & Replication, data backup for this computer is performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer starts a new backup chain on a target location specified in the backup job settings. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.
- You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- The backup cache is supported only for Veeam Agent backup jobs managed by Veeam Agent.
- You cannot use a Microsoft OneDrive storage as a target for a Veeam Agent backup job configured in Veeam Backup & Replication.
- Veeam Agent does not support creating transaction log backups in a cloud repository. You cannot enable transaction log backup options in the properties of the backup job targeted at a cloud repository.
Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup job for protected computers that run a Microsoft Windows OS in one of the following ways:

- **Create a new backup job** — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard. You will be able to specify protection groups, individual Active Directory objects and/or Veeam Agent computers to which the backup job settings must apply at the **Computers** step of the wizard.

- **Add a protection group to a new backup job** — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected protection group to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the **Computers** step of the wizard.

- **Add individual computers to a new backup job** — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected computers to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the **Computers** step of the wizard.

Launching Backup Job Wizard

To launch the New Agent Backup Job wizard, do either of the following:

- On the **Home** tab, click **Backup Job > Windows computer**.

- Open the **Home** view. Select the **Jobs** node and click **Backup Job > Windows computer** on the ribbon.

- Open the **Home** view. Right-click the **Jobs** node and select **Backup > Windows computer**.

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, right-click the protection group that you want to add to the backup job and select **Add to backup job > Windows > New job**.

- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup job and click **Add to Backup > Windows > New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the protection group to the job. You can add other protection groups and (or) individual computers to the job later on, when you pass through the wizard steps.
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job, right-click the selected computer and select **Add to backup job > New job**.

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job and click **Add to Backup > New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the selected computers to the job. You can add other computers and (or) protection groups to the job later on, when you pass through the wizard steps.

**TIP:**

Consider the following:

- You can press and hold **[CTRL]** to select multiple computers at once.
- You can add an individual computer or protection group to a Veeam Agent backup job that is already configured in Veeam Backup & Replication. To learn more, see **Adding Computers to Backup Job** and **Adding Protection Group to Backup Job**.
Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify protection settings for the backup job:

1. **Select the type of protected computers whose data you want to back up with Veeam Agents.**
2. **If you choose to back up data pertaining to servers, select the job mode.**
   
   The job mode defines the type of the created Veeam Agent backup job: the backup job (backup job managed by the backup server) or backup policy (backup job managed by Veeam Agent).

Selecting Protected Computer Type

At the **Job Mode** step of the wizard, in the **Type** field, select the type of protected computers whose data you want to back up with Veeam Agents. The selected type defines what modes will be available for the configured backup job and what job settings will be available at subsequent steps of the wizard. You can select one of the following computer types:

- **Workstation** — select this option if you want to back up data pertaining to workstations or laptops. This option is suitable for computers that reside in a remote location and may have limited connection to the backup server.

  For backup jobs that process workstations, Veeam Backup & Replication offers settings similar to the settings of the backup job available in the **Workstation** edition of Veeam Agent for Microsoft Windows. To learn more, see Veeam Agent for Microsoft Windows User Guide.

  With this option selected, the backup job will be managed by Veeam Agent installed on the protected computer — you do not need to select the job mode.

- **Server** — select this option if you want to back up data pertaining to standalone servers. This option is suitable for computers that have permanent connection to the backup server.

  For backup jobs that process servers, Veeam Backup & Replication offers settings similar to the settings of the backup job available in the **Server** edition of Veeam Agent for Microsoft Windows. To learn more, see Veeam Agent for Microsoft Windows User Guide.

  With this option selected, you can also select the job mode. To learn more, see Selecting Job Mode.

- **Failover cluster** — select this option if you want to back up data pertaining to a failover cluster.

  For backup jobs that process failover clusters, Veeam Backup & Replication offers practically the same backup job settings as for servers.

  With this option selected, the backup job will be managed by the Veeam backup server — you do not need to select the job mode.
Selecting Job Mode

If you selected the Server computer type in the Type field, in the Mode field, select the job mode. You can select one of the following modes:

- **Managed by backup server** — select this option if you want to configure the Veeam Agent backup job. With this option selected, you will be able to add one or more individual computers and/or protection groups to the job and instruct Veeam Backup & Replication to create Veeam Agent backups in a Veeam backup repository or Veeam Cloud Connect repository. The Veeam Agent backup job will run on the backup server in the similar way as a regular job for VM data backup. To learn more, see Backup Job.

- **Managed by agent** — select this option if you want to configure the backup policy. The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers, and acts as a saved template. With this option selected, you will be able to add one or more individual computers and/or protection groups to the backup policy, and instruct Veeam Agent to create backups on a local disk of a protected computer, in a network shared folder, Veeam backup repository or Veeam Cloud Connect repository. To learn more, see Backup Policy.

**NOTE:**

Consider the following:

- The Managed by backup server option is available for servers and failover clusters. For failover clusters, this is the only available option. This option is not available for workstations.
- The Managed by agent option is available for workstations and servers. For workstations, this is the only available option. This option is not available for failover clusters.
Step 3. 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.

![New Agent Backup Job](image)

Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and/or individual computers whose data you want to back up.

You can add to the Veeam Agent backup job one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. You can also add to the job computers that are not added to inventory yet. Veeam Backup & Replication will add such computers to the job and also add them to the *Manually Added* protection group.

Jobs with protection groups are dynamic in their nature. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup job is created, Veeam Backup & Replication will automatically update the job settings to include the added computer.
NOTE:

If you used the Add to backup job > Windows > New job option to launch the New Agent Backup Job wizard, the Protected computers list will already contain computers that you have selected to add to the job. You can remove some computers from the job or add new computers to the job, if necessary.

Adding Protection Groups and Computers from Inventory

To add protection groups and/or individual computers to the Veeam Agent backup job:

1. Click Add > Protection group.
2. In the Select Objects window, select one or more protection groups and/or computers in the list and click OK. You can press and hold [CTRL] to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the Select Objects window.

1. Enter the object name or a part of it in the search field.
2. Click the Start search button on the right or press [ENTER].
Adding New Computers

To add to the Veeam Agent backup job new computers that do not exist in the inventory:

1. Click **Add > Individual computer**.

2. In the **Add Computer** window, in the **Host name or IP address** field, enter a full DNS name or IP address of the computer that you want to add to the job.

3. From the **Credentials** list, select a user account that has administrative permissions on the computer that you want to add to the job. 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 the **Credentials Manager** section in the Veeam Backup & Replication User Guide.
Step 5. Select Backup Mode

At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup.

1. In the **Backup mode** section, select the backup mode. You can select one of the following options:

   - **Entire computer** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, folders, application data and so on. With this option selected, you will pass to one of the following steps of the wizard:
     - **Storage** — if you have selected the **Managed by backup server** option at the **Job Mode** step of the wizard.
     - **Destination** — if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.

   - **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, all volumes except the system one. When you restore data from such backup, you will be able to recover data on these volumes only: files, folders, application data and so on. With this option selected, you will pass to the **Objects** step of the wizard.

   - **File level backup** — select this option if you want to create a backup of individual folders on your computer. With this option selected, you will pass to the **Objects** step of the wizard.

2. [For entire computer backup] If you want to include in the backup one or more external USB drives, select the **Include external USB drives** check box. With this option selected, Veeam Agent for Microsoft Windows will include in the backup all external USB drives that are connected to the Veeam Agent computer at the time when the backup job starts. To learn more, see the **Backup of External Drives** section in the Veeam Agent for Microsoft Windows User Guide.
NOTE:
Consider the following:

- The **File level backup** option is not available if you have selected the **Failover cluster** option at the **Job Mode** step of the wizard.

- File-level backup is typically slower than volume-level backup. Depending on the performance capabilities of your computer and backup environment, the difference between file-level and volume-level backup job performance may increase significantly. If you plan to back up all folders with files on a specific volume or back up large amount of data, it is recommended that you configure volume-level backup instead of file-level backup.

**Step 6. Specify Backup Scope Settings**

The **Objects** step of the wizard is available if you chose to create volume-level or file-level Veeam Agent backups. Specify backup scope for the Veeam Agent backup job:

- **Specify volumes to back up** — if you have selected the **Volume level backup** option at the **Backup Mode** step of the wizard.

- **Specify folders to back up** — if you have selected the **File level backup** option at the **Backup Mode** step of the wizard.

**Specifying Volumes to Back Up**

The **Objects** step of the wizard is available if you have selected the **Volume level backup** option at the **Backup Mode** step of the wizard.

At this step of the wizard, you must specify the backup scope — define what volumes you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified volume does not exist on one or more computers in the job, the job will skip such volume on those computers and back up only existing ones.

To specify the backup scope, in the **Volumes to backup** section, select check boxes next to necessary objects. You can include the following data in the backup:

- **Operating system** — data pertaining to the OS installed on a protected computer. With this option enabled, Veeam Agent for Microsoft Windows will include in the backup scope the Microsoft Windows system partition and boot partition of your computer. For GPT disks on Microsoft Windows 8, 8.1, 10, 2012, 2012 R2, 2016 and 2019, Veeam Agent will additionally back up the recovery partition. To learn more, see the **System State Data Backup** section in the Veeam Agent for Microsoft Windows User Guide.

- **Individual volumes**.

To specify individual volumes to back up:

1. In the **Volumes to backup** section, click **Add**.
2. In the **Add Object** window, type the drive letter of a volume that you want to back up, for example, C:\, and click **OK**.
3. Repeat steps 1–2 for all volumes that you want to back up.
NOTE:

Mind the following:

- If you include a system volume in the volume-level backup, Veeam Agent for Microsoft Windows automatically includes the System Reserved/UEFI or other system partitions in the backup too.
- Veeam Agent for Microsoft Windows automatically adds to the list of exclusions the following Microsoft Windows objects for all computer users: temporary files folder, Recycle Bin, Microsoft Windows pagefile, hibernate file and VSS snapshot files from the System Volume Information folder.

Specifying Folders to Back Up

The **Objects** step of the wizard is available if you have selected the **File level backup** option at the **Backup Mode** step of the wizard.

In the file-level backup mode, you can create two types of backups:

- File-level backup that includes individual folders on your computer.
- Hybrid backup that contains individual folders and specific volumes of your computer.

At this step of the wizard, you must specify the backup scope — define what folders with files or entire volumes you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified object does not exist on one or more computers in the job, the job will skip such object on those computers and back up existing ones.

To specify the backup scope, in the **Choose directories to backup** list, select check boxes next to necessary objects. You can include the following data in the backup:
- **Operating system** — data pertaining to the OS installed on a protected computer.

- **Personal files** — user profile folder including all user settings and data. Typically, the user profile data is located in the *Users* folder on the system disk, for example, `C:\Users`.

- **Individual file system objects** — folders or volumes of a protected computer.

To specify individual folders to back up:

1. Select the **The following file system objects** check box and click **Add**.

2. In the **Add Object** window, type the path to a folder or volume that you want to back up, for example, `D:\Reports` or `D:\`, and click **OK**.

   To specify the backup scope, you can use wildcards and system environment variables such as `%ProgramFiles%` or `%WinDir%`. This may be useful, for example, in case computers added to the backup job run different versions of Microsoft Windows OSes, and actual paths to directories that contain data of the same type differ on these computers.

   Consider the following:

   - You can use only system environment variables — variables defined for the Local System account on computers added to the backup job. User-dependent environment variables are not supported.
   - Environment variables that contain multiple values (such as the `%PATH%` variable) are not supported.
   - Environment variables that contain other environment variables are not supported.

3. Repeat steps 1–2 for all folders and volumes that you want to back up.
NOTE:

Mind the following:

- If you include a system volume in the file-level backup, Veeam Agent for Microsoft Windows does not automatically include the System Reserved/UEFI or other system partitions in the backup. These volumes are automatically included in the backup only if you select the *Operating system* option to specify the backup scope.

- Veeam Agent for Microsoft Windows automatically adds to the list of exclusions the following Microsoft Windows objects for all computer users: temporary files folder, Recycle Bin, Microsoft Windows pagefile, hibernate file and VSS snapshot files from the System Volume Information folder.
Configuring Filters

To include or exclude files of a specific type in/from the file-level backup, you can configure filters.

To configure a filter:

1. At the **Objects** step of the wizard, click **Advanced**.

2. Specify what files you want to back up:
   - If you include a specific folder in the file-level backup, in the **Include masks** field, specify file names and/or masks for file types that you want to back up, for example, `MyReport.pdf`, `*filename*`, `*.docx`. The resulting Veeam Agent backup will contain only selected files. Other files will not be backed up.

   You cannot specify include masks if you add an entire volume in the backup.

   - In the **Exclude masks** field, specify files that you do not want to back up in the following ways:
     - If you include an entire volume in the file-level backup, in the **Exclude masks** field, specify paths to folders that contain files that you do not want to back up. The resulting Veeam Agent backup will contain all folders that reside on the backed-up volume except the files in the specified folders.

       For example, you include the D:\ volume in the backup and specify the D:\Reports\OldReports folder in the **Exclude masks** field. The resulting backup will contain all folders and files that reside on the volume except files that reside in the D:\Reports\OldReports folder.

     - If you include a specific folder in the file-level backup, in the **Exclude masks** field, specify file names and/or masks for file types that you do not want to back up, for example, `OldReports.rar`, `*.temp`, `*.tmp`, `*.back`. The resulting Veeam Agent backup will contain all files except files whose names match the specified names or masks.

3. Click **Add**.

4. Repeat steps 2–3 for each mask that you want to add.

**NOTE:**

You can also use system environment variables to specify include and exclude masks. In this case, you must type the back slash (\) symbol in the beginning of the mask. For example: `\%appdata%`.

Consider the following:

- To specify include and exclude masks, you can use only system environment variables — variables defined for the Local System account on computers added to the backup job, and cannot use user environment variables. For example, if you specify the `%appdata%` exclude mask, Veeam Agent for Microsoft Windows will exclude the C:\Windows\system32\config\systemprofile\AppData\Roaming folder from the backup. Application data directories for other user accounts (for example, C:\Users\Administrator\AppData\Roaming) will not be excluded from the backup.

- You cannot use environment variables that contain multiple values or other environment variables to specify include and exclude masks.
You can use a combination of include and exclude masks. Note that exclude masks have a higher priority than include masks. For example, you can specify masks in the following way:

- **Include mask**: `*.pdf`
- **Exclude mask**: `*draft*`

The resulting Veeam Agent backup will contain all files of the PDF format that do not contain `draft` in their names.

---

**Step 7. Select Backup Destination**

The **Destination** step of the wizard is available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.

At this step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.
You can store backup files in one of the following locations:

- **Local storage** — select this option if you want to save a backup on a removable storage device attached to a protected computer or on a local drive of a protected computer. With this option selected, you will pass to the Local Storage step of the wizard.

**IMPORTANT!**

Consider the following:

- It is strongly recommended that you store backups in the external location like USB storage device or shared network folder. You can also keep your backup files on the separate non-system local drive.
- If you select to store the backup on a local folder included in the backup scope, Veeam Agent for Microsoft Windows will automatically exclude this folder from the backup.

- **Shared folder** — select this option if you want to save a backup in a network shared folder. With this option selected, you will pass to the Shared folder step of the wizard.

- **Veeam backup repository** — select this option if you want to save a backup on a backup repository managed by the Veeam backup server of which the Veeam Agent backup job is configured. With this option selected, you will pass to the Backup Server step of the wizard.

- **Veeam Cloud Connect repository** — select this option if you want to save a backup on a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the Storage step of the wizard.

---

**Step 8. Specify Backup Storage Settings**

Specify backup storage settings for the backup job:
• If you have selected the **Managed by backup server** mode at the **Job Mode** step of the wizard, you can create Veeam Agent backups only on a backup repository managed by this Veeam backup server or on a cloud repository exposed to you by a Veeam Cloud Connect service provider. Specify backup repository settings at the **Storage** of the wizard.

• If you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard, specify backup storage settings at one of the following steps of the wizard:
  
  o **Local storage settings** — if you have selected the **Local storage** option at the **Destination** step of the wizard.
  
  o **Shared folder settings** — if you have selected the **Shared folder** option at the **Destination** step of the wizard.
  
  o **Veeam backup repository settings** — if you have selected the **Veeam backup repository** option at the **Destination** step of the wizard.
  
  o **Cloud repository settings** — if you have selected the **Veeam Cloud Connect repository** option at the **Destination** step of the wizard.

**Backup Storage Settings**

The **Storage** step of the wizard is available if you have selected the **Managed by backup server** mode at the **Job Mode** step of the wizard.

Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store Veeam Agent backups. You can select from the following types of backup repositories:
  
  o Veeam backup repository configured on the backup server that will manage the created backup job.
  
  o Cloud repository allocated to your tenant account by a Veeam Cloud Connect service provider.

   When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. 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.

**NOTE:**

Mind the following:

• Backup job mapping is available only for a Veeam Agent backup job managed by the backup server.

• You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a backup chain that was created by Veeam Agent operating in the standalone mode.

3. Specify backup retention policy settings:
   
   o From the **Retention policy** list, select **restore points** and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup &
Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

- From the Retention policy list, select days and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

4. To use the GFS (Grandfather-Father-Son) retention scheme, select the Keep some periodic full backups longer for archival purposes check box and click Configure. In the Configure GFS window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

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 destinations for this job check box. With this option enabled, the New Agent 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.
6. Click **Advanced** to specify advanced settings for the backup job. To learn more, see **Specify Advanced Backup Settings**.

---

**Local Storage Settings**

The **Local Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard and chosen to save the backup on a local drive of your computer.

Specify local storage settings:

1. In the **Local folder** field, type a path to a folder on a protected computer where backup files must be saved. If the specified folder does not exist in the file system of a protected computer, Veeam Agent for Microsoft Windows will create this folder and save the resulting backup file to this folder. If the volume on which the specified folder must reside does not exist on a protected computer, Veeam Backup & Replication will not apply the backup job settings to this computer.

**IMPORTANT!**

USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.
2. Specify backup retention policy settings:
   - If you have selected the **Workstation** type at the **Job Mode** step of the wizard, in the **Keep backups for <N> days** field, specify the number of days for which you want to store backup files in the target location (excluding days when backups were not created). By default, Veeam Agent for Microsoft Windows keeps backup files for 7 days. After this period is over, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.
   - If you have selected the **Server** type at the **Job Mode** step of the wizard, in the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

**NOTE:**
Mind the following:
- For backups of workstations, the retention policy is the same as in the Workstation edition of Veeam Agent for Microsoft Windows operating in the standalone mode.
- For backups of servers, the retention policy is the same as in the Server edition of Veeam Agent for Microsoft Windows operating in the standalone mode.

To learn more, refer to the Veeam Agent for Microsoft Windows User Guide.

3. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.
Shared Folder Settings

The **Shared Folder** step of the wizard is available if you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard and chosen to save the backup in a network shared folder.

Specify shared folder settings:

1. In the **Shared folder** field, type a UNC name of the network shared folder in which you want to store backup files. Keep in mind that the UNC name always starts with two back slashes (\\).

2. If the network shared folder requires authentication, select the **This share requires access credentials** check box and select from the list a user account that has access permissions on this shared folder. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. The user name must be specified in the **DOMAIN\USERNAME** format.
   
   If you do not select the **This share requires access credentials** check box, Veeam Agent for Microsoft Windows will connect to the shared folder using the **NT AUTHORITY\SYSTEM** account of the computer where the product is installed. You can use this scenario if the Veeam Agent computer is joined to the Active Directory domain. In this case, you can simply grant **Full Control** access on the shared folder and underlying file system to the computer account (**DOMAIN\COMPUTERNAME$**).

3. Specify backup retention policy settings:
   
   o If you have selected the **Workstation** type at the **Job Mode** step of the wizard, in the **Keep backups for <N> days** field, specify the number of days for which you want to store backup files in the target location (excluding days when backups were not created). By default, Veeam Agent for Microsoft Windows keeps backup files for 7 days. After this period is over, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

   o If you have selected the **Server** type at the **Job Mode** step of the wizard, in the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

**NOTE:**

Mind the following:

- For backups of workstations, the retention policy is the same as in the **Workstation** edition of Veeam Agent for Microsoft Windows operating in the standalone mode.

- For backups of servers, the retention policy is the same as in the **Server** edition of Veeam Agent for Microsoft Windows operating in the standalone mode.

To learn more, refer to the [Veeam Agent for Microsoft Windows User Guide](https://docs.veeam.com).
4. Click **Advanced** to specify advanced settings for the backup job. To learn more, see **Specify Advanced Backup Settings**.

**Veeam Backup Repository Settings**

If you have selected the **Managed by agent** mode for the backup job and chosen to store backup files on a Veeam backup repository, specify settings to connect to the backup repository:

1. **At the Backup Server step of the wizard**, specify backup server settings.
2. **At the Backup Repository step of the wizard**, select the Veeam backup repository.
Specifying Backup Server Settings

The **Backup Server** step of the wizard is available if you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard and chosen to store backup files on a Veeam backup repository.

In the **DNS name or external IP address field**, review and change if necessary the name or IP address of the Veeam backup server on which you configure the Veeam Agent backup job. The specified DNS name or IP address must be accessible from Veeam Agent computers.

**NOTE:**

Veeam Backup & Replication does not automatically update information about the backup server in the backup policy settings after migration of the configuration database. After you migrate configuration data to a new location, you must specify the name or IP address of the new backup server in the properties of all backup policies configured in Veeam Backup & Replication.

![New Agent Backup Job](image)

**Backup Server**
Specify Veeam Backup & Replication management server connection parameters.

- **Job Mode**
- **Name**
- **Computers**
- **Backup Mode**
- **Objects**
- **Destination**

**Backup Server**
- **Storage**
- **Backup Cache**
- **Guest Processing**
- **Schedule**
- **Summary**

**DNS name or external IP address:**

The specified DNS name must resolve to the external IP address of your backup server, or remote backup agents need to be able to establish network connection to this endpoint.
Selecting Backup Repository

The Storage step of the wizard is available if you have selected the Managed by agent mode at the Job Mode step of the wizard and chosen to save backup files on a Veeam backup repository.

NOTE:
You cannot map a Veeam Agent backup job managed by Veeam Agent (backup policy).

Specify settings for the target backup repository:

1. From the Backup repository list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. Specify backup retention policy settings:
   - If you have selected the Workstation type at the Job Mode step of the wizard, in the Keep backups for <N> days field, specify the number of days for which you want to store backup files in the target location (excluding days when backups were not created). By default, Veeam Agent for Microsoft Windows keeps backup files for 7 days. After this period is over, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.
   - If you have selected the Server type at the Job Mode step of the wizard, in the Restore points to keep on disk field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

NOTE:
Mind the following:

- For backups of workstations, the retention policy is the same as in the Workstation edition of Veeam Agent for Microsoft Windows operating in the standalone mode.
- For backups of servers, the retention policy is the same as in the Server edition of Veeam Agent for Microsoft Windows operating in the standalone mode.

To learn more, refer to Veeam Agent for Microsoft Windows User Guide.

3. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the Configure secondary destinations for this job check box. With this option enabled, the New Agent 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.
4. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.

### Cloud Repository Settings

The **Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard and chosen to save backup files on a Veeam Cloud Connect repository.

**NOTE:**

Keep in mind that FQDN or IP addresses of Veeam Agent machines that you back up to the cloud repository will be visible to the Veeam Cloud Connect service provider. To learn more, see Creating Protection Groups: Before You Begin.

Specify settings for the cloud repository:

1. From the **Backup repository** list, select a cloud repository where you want to store created backups. The **Backup repository** list displays cloud repositories allocated to your tenant account by the Veeam Cloud Connect service provider. When you select a cloud repository, Veeam Backup & Replication automatically checks how much free space is available on the repository.

2. Specify backup retention policy settings:
   - If you have selected the **Workstation** type at the **Job Mode** step of the wizard, in the **Keep backups for <N> days** field, specify the number of days for which you want to store backup files in the target location (excluding days when backups were not created). By default, Veeam Agent for Microsoft Windows keeps backup files for 7 days. After this period is over, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.
If you have selected the **Server** type at the **Job Mode** step of the wizard, in the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Microsoft Windows keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Microsoft Windows will remove the earliest restore points from the backup chain.

**NOTE:**

Mind the following:

- For backups of workstations, the retention policy is the same as in the **Workstation** edition of Veeam Agent for Microsoft Windows operating in the standalone mode.
- For backups of servers, the retention policy is the same as in the **Server** edition of Veeam Agent for Microsoft Windows operating in the standalone mode.

To learn more, refer to **Veeam Agent for Microsoft Windows User Guide**.

3. Click **Advanced** to specify advanced settings for the backup job. To learn more, see **Specify Advanced Backup Settings**.
Step 9. Specify Advanced Backup Settings

In the Advanced Settings window, specify advanced settings for the Veeam Agent backup job:

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings
- [For Veeam Agent jobs managed by the backup server] Script settings

TIP:

After you specify necessary settings for the Veeam Agent 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. Click Advanced at one of the following steps of the wizard:
   - Storage — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - Local Storage — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - Shared Folder — if you have selected to save backup files in a network shared folder.

2. If you want to periodically create synthetic full backups, on the Backup tab, select the Create synthetic full backups periodically check box and click Days to schedule synthetic full backups on the necessary week days.

3. If you want to periodically create active full backups, select the Create active full backups periodically check box. Use the Monthly on or Weekly on selected days options to define scheduling settings.
NOTE:
Consider the following:

- Before scheduling periodic full backups, you must make sure that you have enough free space on the target location. For more information about periodic full backups, see the Active Full Backup and Synthetic Full Backup sections in the Veeam Agent for Microsoft Windows User Guide.
- If you schedule the active full backup and synthetic full backup on the same day, Veeam Agent for Microsoft Windows will perform only active full backup. Synthetic full backup will be skipped.

Maintenance Settings

You can specify maintenance settings for a backup chain created with the Veeam Agent backup job. Maintenance operations help make sure that the backup chain remains valid and consistent.

Maintenance settings are available for the following types of Veeam Agent backup jobs that process Microsoft Windows computers:

- Backup job managed by the backup server.
- Backup job managed by Veeam Agent (backup policy).
To specify maintenance settings for the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.

2. In the **Advanced Settings** window, 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 schedule for the health check.

   An automatic health check can help you avoid a situation where a restore point gets corrupted, making all dependent restore points corrupted, too. If during the health check Veeam Agent for Microsoft Windows or Veeam Backup & Replication detect corrupted data blocks in the latest restore point in the backup chain (or 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 Veeam Agent computer to the target location. 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 Veeam Agent backup jobs managed by the backup server, the health check process is similar to the one for backup jobs that process VMs. For more information, see the **Health Check for Backup Files** section in the Veeam Backup & Replication User Guide.

   For Veeam Agent backup jobs managed by Veeam Agent, the health check process is the same as for Veeam Agent backup jobs configured directly on a Veeam Agent computer. For more information, see the **Health Check for Backup Files** section in the Veeam Agent for Microsoft Windows User Guide.

4. [For backup jobs and policies targeted at a Veeam backup repository or cloud repository] Select the **Remove deleted items data after** check box and specify the number of days for which you want to keep the backup created with the backup job in the target location.

   - For backup jobs managed by the backup server, deleted items retention policy is similar to retention policy for deleted VMs. After you remove a protection group or individual computer from a Veeam Agent backup job, Veeam Backup & Replication will keep its data on the backup repository for the period that you have specified. When this period is over, backup data of this computer will be removed from the backup repository. For more information, see the **Retention Policy for Deleted VMs** section in the Veeam Backup & Replication User Guide.

   - For backup jobs managed by Veeam Agent, if Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location. For more information, see the **Retention Policy for Outdated Backups** section in the Veeam Agent for Microsoft Windows User Guide.

   By default, the deleted items data retention period is 30 days. Do not set the deleted items retention period to 1 day or a similar short interval. In the opposite case, the backup job may work not as expected and remove data that you still require.
NOTE:
The Remove deleted items data after option is not available if you configure a backup job managed by Veeam Agent (backup policy) and have selected the Local storage or Shared folder option at the Destination step of the wizard.

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, data blocks from the full backup file are copied to a new empty file. As a result, the full backup file gets defragmented, and the speed of reading from and writing to the backup file increases.

The compact operation differs depending on the type of the backup job.

- For Veeam Agent backup jobs managed by the backup server, the compact operation is similar to the compact operation performed for VM backup jobs. If the full backup file contains data blocks for deleted items (protection groups or individual computers that were removed from the backup job), Veeam Backup & Replication will remove these data blocks. For more information, see the Compact of Full Backup File section in the Veeam Backup & Replication User Guide.

- For Veeam Agent backup jobs managed by Veeam Agent, if the full backup file contains data blocks for deleted drives, Veeam Agent for Microsoft Windows will remove these data blocks. For more information, see the Compact of Full Backup File section in the Veeam Agent for Microsoft Windows User Guide.
NOTE:

Consider the following:

- If you want to periodically compact a full backup, you must make sure that you have enough free space in the target location. For the compact operation, the amount of free space must be equal to or more that the size of the full backup file.
- In contrast to the compact operation for a VM backup, during compact of a full Veeam Agent backup file, Veeam Backup & Replication does not perform the data take out 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, Veeam Backup & Replication will not extract data for this machine to a separate full backup file.

Storage Settings

To specify storage settings for the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.

2. Click the **Storage** tab.

3. [For a failover cluster backup job] By default, Veeam Backup & Replication deduplicates failover cluster 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. You can disable data deduplication if necessary, for example, if you use a deduplication storage appliance as a backup repository. To disable data deduplication, clear the **Enable inline data deduplication** check box.

NOTE:

The **Enable inline data deduplication** option is unavailable if you selected the **Workstation** or **Server** option at the **Job Mode** step of the wizard.

4. From the **Compression level** list, select a compression level for the backup: **None**, **Dedupe-friendly**, **Optimal**, **High** or **Extreme**.

5. 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 Agent for Microsoft Windows will use data blocks of different size to optimize the size of backup files and job performance.
6. 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 the **Password Manager** section in the Veeam Backup & Replication User Guide.

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 the **Decrypting Data Without Password** section in the Veeam Backup & Replication User Guide.
NOTE:

Consider the following:

- Data encryption settings for Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup jobs and policies targeted at a Veeam backup repository, all data encryption operations are performed in Veeam Backup & Replication, too. Encryption settings are passed to a Veeam Agent computer only in case this computer is added to a backup policy targeted at a local drive of a protected computer or at a network shared folder. Veeam Backup & Replication performs this operation when applying the backup policy to a protected computer.

- If you change a password for data encryption for an existing backup policy targeted at a Veeam backup repository without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.

- If you enable encryption for an existing Veeam Agent backup, during the next job session Veeam Agent for Microsoft Windows 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 backup job, Veeam Agent for Microsoft Windows will encrypt the backup chain starting from the next restore point created with this job.

- [For backup policies targeted at a local drive, network shared folder or cloud repository] When you enable data encryption for a backup policy, Veeam Backup & Replication uses the specified password to encrypt backups of all Veeam Agent computers added to the backup policy. A Veeam Agent computer user can restore data from the backup of this computer without providing a password to decrypt backup. To restore data from a backup of another computer in this backup policy, a user must provide a password specified in the backup policy settings.

This scenario differs from the same scenario in earlier versions of Veeam Backup & Replication where all backups created for Veeam Agent computers in the backup policy could be accessed from any computer in the backup policy without providing a password.

To learn more about data encryption in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.
Notification Settings

You can specify notification settings for Veeam Agent backup jobs configured in Veeam Backup & Replication. Notification options differ depending on the job mode that you have selected at the Job Mode step of the wizard:

- **Managed by backup server.** To learn more, see Notification Settings for Veeam Agent Backup Job.
- **Managed by agent.** To learn more, see Notification Settings for Backup Policy.

Notification Settings for Veeam Agent Backup Job

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 the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.

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 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 the Configuring Global Email Notification Settings section in Veeam Backup & Replication User Guide.

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.
   - To configure a custom notification for the job, select Use custom notification settings specified below. You can specify the following notification settings:
     - In the Subject field, specify a notification subject. You can use the following variables in the subject: %Time% (completion time), %JobName%, %JobResult%, %ObjectCount% (number of machines in the job) and %Issues% (number of machines in the job that have been processed with the Warning or Failed status).
- Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.

- 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.
Notification Settings for Backup Policy

You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup job sessions performed for the last 24-hour period on computers to which the backup policy is applied.

**NOTE:**

Email reports with backup policy statistics will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.

After you enable notification settings for the backup policy, Veeam Backup & Replication will send reports with the backup policy statistics to email addresses specified in global email notification settings and email addresses specified in the backup policy settings.

To specify notification settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. Click the **Notifications** tab.
3. Select the **Send daily e-mail report to the following recipients** check box and specify a recipient's email address in the field below. You can enter several addresses separated by a semicolon.
4. In the **Send at** field, specify the time when Veeam Backup & Replication must send the email notification for the backup policy. Veeam Backup & Replication will send the report daily at the specified time.
5. You can choose to use global notification settings or specify custom notification settings.
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server.
To configure a custom notification for the backup policy, select **Use custom notification settings specified below**. You can specify the following notification settings:

- In the **Subject** field, specify a notification subject. You can use the following variables in the subject: %Time% (completion time), %JobName%, %JobResult%, %ObjectCount% (number of machines in the backup policy) and %Issues% (number of machines in the backup policy that have been processed with the Warning or Failed status).

- Select the **Notify on success**, **Notify on warning** and/or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.

### Script Settings

You can specify script settings for the job if you have selected the **Managed by backup server** mode at the **Job Mode** step of the wizard.

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 **Before the job** and **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 OS quiescence process on protected computers. To add pre-freeze and post-thaw scripts for Veeam Agent computer OS quiescence, use the **Guest Processing** step of the wizard.
Step 10. Specify Secondary Target

The Secondary Target step of the wizard is available if you have enabled the Configure secondary destinations for this job option at the Storage step of the wizard.

At the Secondary Target step of the wizard, you can link the Veeam Agent 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 the Linking Backup Jobs to Backup Copy Jobs and Linking Backup Jobs to Backup to Tape Jobs sections in the Veeam Backup & Replication User Guide.

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 Veeam Agent backup job to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the Veeam Agent 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 Veeam Agent 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 11. Specify Backup Cache Settings

The Backup Cache step of the wizard is available if you selected the following options at the previous steps of the wizard:

1. Selected the Managed by agent mode at the Job Mode step of the wizard.
2. Selected the Veeam backup repository or Veeam Cloud Connect repository option at the Destination step of the wizard.

To specify backup cache settings:

1. Select the Enable backup cache check box.
2. In the Maximum size field, specify the size for the backup cache.
   When defining the size of the backup cache, assume the following:
   - Each full backup file may consume about 50% of the backed-up data size.
   - Each incremental backup file may consume about 10% of the backed-up data size.
3. In the Location section, specify where Veeam Agent for Microsoft Windows will create the backup cache. You can select from the following options:
   - Automatic selection — select this option if you want to let Veeam Agent pick a location for the backup cache automatically. On every computer added to the backup policy, Veeam Agent will detect a volume with the largest amount of free disk space and create the backup cache in the Veeam Backup Cache folder on this volume. To learn more, see Backup Cache.
   - Manual selection — select this option if you want to specify a location for the backup cache manually. If you select this option, in the Folder field, specify a path to the folder on a protected computer in which backup files must be stored.
Step 12. Specify Guest Processing Settings

The **Guest Processing** step of the wizard is available if you have selected the **Server** or **Failover cluster** option at the **Job Mode** step of the wizard.

For a Veeam Agent backup job that includes Windows-based computers, you can enable the following guest OS processing settings:

- Application-aware processing
- Transaction log handling for Microsoft SQL Server
- Archived log handling for Oracle databases
- SharePoint account settings
- Use of pre-freeze and post-thaw scripts
- File indexing
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 machines and applications... Applications...

Enable guest file system indexing
Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files.
Indexing is optional, and is not required to perform instant file level recoveries.
Customize advanced guest file system indexing options for individual machines... Indexing...
Application-Aware Processing

If your computer runs VSS-aware applications, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup guarantees proper recovery of applications without data loss.

To enable application-aware processing:

1. At the Guest Processing step of the wizard, make sure that the Enable application-aware processing check box is selected.
2. Click Applications.
3. In the displayed list, select a protection group or individual computer and click Edit.
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click Add and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the General tab, in the Applications section, make sure that the Enable application-aware processing check box is selected.
   You can clear this check box, for example, if you want to disable application-aware processing for a specific computer added to the backup job as a part of a protection group.
5. [For Microsoft Exchange, Microsoft SQL and Oracle] In the Transaction logs section, specify if Veeam Agent for Microsoft Windows running on a protected computer must process transaction logs or copy-only backups must be created.
   - Select Process transaction logs with this job if you want Veeam Agent for Microsoft Windows to process transaction logs.
     [For Microsoft Exchange] With this option selected, Veeam Agent for Microsoft Windows will wait for backup to complete successfully, and then trigger truncation of transaction logs. If the backup job fails, the logs will remain untouched until the next backup job session.
     [For Microsoft SQL Server and Oracle] You will have to specify settings for database log handling on the SQL and Oracle tabs of the Processing Settings window. For more information, see Microsoft SQL Server Transaction Log Settings and Oracle Archived Log Settings.
   - Select Perform copy only if you use another tool to maintain consistency of the database state. Veeam Agent for Microsoft Windows will create a copy-only backup. The copy-only backup preserves the chain of full/differential backup files and transaction logs. For more information, see Microsoft Docs.
IMPORTANT!

Consider the following:

- [For Microsoft Exchange] Veeam Agent for Microsoft Windows performs truncation of Microsoft Exchange transaction logs only if all disks that contain the Microsoft Exchange database are included in a volume-level backup job.
- [For Microsoft SQL Server and Oracle] If both Microsoft SQL Server and Oracle Server are installed on one guest OS, and log backup is enabled for both applications, Veeam Agent for Microsoft Windows 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 Microsoft SQL Server, you can specify how Veeam Agent for Microsoft Windows must process database transaction logs:

1. At the Guest Processing step of the wizard, make sure that the Enable application-aware processing check box is selected.
2. Click Applications.
3. In the displayed list, select a protection group or individual computer and click Edit.
4. In the Transaction logs section, select Process transaction logs with this job.
5. In the Processing Settings window, click the SQL tab.
6. To specify a user account that Veeam Agent for Microsoft Windows will use to connect to the Microsoft SQL Server, select from the **Specify Microsoft SQL Server account with database admin privileges** list a user account that has access permissions on the database. To connect to the Microsoft SQL Server, you must use a Microsoft Windows user account that has sysadmin privileges on the Microsoft SQL Server. You cannot use Microsoft SQL Server accounts (for example, the SA account) to connect to the database.

By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will connect to the Microsoft SQL Server under the account that you have specified for the protected computer in the protection group settings.

If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

7. Specify how transaction logs must be processed. You can select one of the following options:

   o **Select Truncate logs** to truncate transaction logs after successful backup. Veeam Agent for Microsoft Windows will wait for the backup to complete successfully and then truncate transaction logs. If the backup job fails, the logs will remain untouched until the next backup job session.

   o **Select Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Agent for Microsoft Windows will not truncate transaction logs.

   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 may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs him-/herself.

   o **Select Backup logs periodically** to back up transaction logs with Veeam Agent for Microsoft Windows. Veeam Agent for Microsoft Windows will periodically copy transaction logs to the backup location and store them together with the image-level backup. During the backup job session, transaction logs will be truncated.

   For more information, see the Microsoft SQL Server and Oracle Logs Backup section in the Veeam Agent for Microsoft Windows User Guide.

If you have selected to back up transaction logs with Veeam Agent for Microsoft Windows, 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 in the backup location.

   o **Select Until the corresponding image-level backup is deleted** to apply the same retention policy for image-level backups and transaction log backups.

   o **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 backup.

   For more information, see the Retention for Database Log Backups section in the Veeam Agent for Microsoft Windows User Guide.
IMPORTANT!

Veeam Agent for Microsoft Windows automatically excludes its configuration database from application-aware processing during backup. Transaction logs for the configuration database are not backed up.

Oracle Archived Log Settings

If you back up an Oracle database, you can specify how Veeam Agent for Microsoft Windows must process archived logs:

1. At the Guest Processing step of the wizard, make sure that the Enable application-aware processing check box is selected.
2. Click Applications.
3. In the displayed list, select a protection group or individual computer and click Edit.
4. In the Transaction logs section, select Process transaction logs with this job.
5. In the Processing Settings window, click the Oracle tab.
6. To specify a user account that Veeam Agent for Microsoft Windows will use to connect to the Oracle database, select from the Specify Oracle account with SYSDBA privileges list a user account that has SYSDBA rights on the database. If you have not set up credentials beforehand, click the Manage accounts link or click Add on the right to add credentials.

By default, the Use guest OS credentials option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will connect to the Oracle database under the account that you have specified for the protected computer in the protection group settings.

7. In the Archived logs section, specify if Veeam Agent for Microsoft Windows must delete archived logs on the Oracle database:

   o Select Do not delete archived logs if you want Veeam Agent for Microsoft Windows to preserve archived logs. When the backup job completes, Veeam Agent for Microsoft Windows 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 may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.

   o Select Delete logs older than <N> hours or Delete logs over <N> GB if you want Veeam Agent for Microsoft Windows to delete archived logs that are older than <N> hours or larger than <N> GB. Veeam Agent for Microsoft Windows will wait for the backup to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.

8. To back up Oracle archived logs with Veeam Agent for Microsoft Windows, 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 minimum log backup interval is 5 minutes. The maximum log backup interval is 480 minutes.
9. In the **Retain log backups** section, specify retention policy for archived logs stored in the backup location:

   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for Veeam Agent backups and archived log backups.
   - Select **Keep only last \( n \) days of log backups** 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 Veeam Agent backups. For more information, see the **Retention for Database Log Backups** section in the Veeam Agent for Microsoft Windows User Guide.

Microsoft SharePoint Account Settings

If you back up Microsoft SharePoint, you must specify a user account that has enough permissions on the application:

1. At the **Guest Processing** step of the wizard, make sure that the **Enable application-aware processing** check box is selected.

2. Click **Applications**.

3. In the displayed list, select a protection group or individual computer and click **Edit**.

4. In the **Processing Settings** window, click the **SharePoint** tab.

5. From the **Specify SharePoint admin account** list, select a user account that Veeam Agent for Microsoft Windows will use to connect to the SharePoint application. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.
By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will connect to the SharePoint application under the account that you have specified for the protected computer in the protection group settings.

---

**Pre-Freeze and Post-Thaw Scripts**

If you plan to back up data of applications that do not support VSS, you can specify what scripts Veeam Agent for Microsoft Windows must use to quiesce the OS on the protected computer. The pre-freeze script quiesces the file system and application data to bring the OS to a consistent state before Veeam Agent for Microsoft Windows creates a VSS snapshot. After the VSS snapshot is created, the post-thaw script brings the file system and applications to their initial state.

To specify pre-freeze and post-thaw scripts for the job:

1. At the **Guest Processing** step, make sure that the **Enable application-aware processing** check box is selected.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.
4. In the **Processing Settings** window, click the **Scripts** tab.
5. From the **Specify admin account for script execution** list, select a user account that Veeam Agent for Microsoft Windows will use to run pre-freeze and post-thaw scripts. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials.

By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will run pre-freeze and post-thaw scripts under the account that you have specified for the protected computer in the protection group settings.
6. In the **Script processing mode** section, specify the scenario for scripts execution:
   - Select **Require successful script execution** if you want Veeam Agent for Microsoft Windows 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.

7. In the **Pre-freeze script** and **Post-thaw script** fields, click **Browse** to choose executable files from a local folder on the backup server. During the backup job session, Veeam Backup & Replication will upload the scripts to Veeam Agent computers added to the job and execute them on these computers. Veeam Agent for Microsoft Windows supports scripts in the EXE, BAT and CMD format.

---

**File Indexing**

You can instruct the backup job to create an index of files and folders on the protected computer OS during backup. If you enable the file indexing option, you will be able to search for individual files inside Veeam Agent backups and perform 1-click restore in Veeam Backup Enterprise Manager.

**NOTE:**

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 Restore] section in the Veeam Backup Enterprise Manager User Guide.
To specify file indexing options:

1. At the **Guest Processing** step of the wizard, select the **Enable guest file system indexing** check box.
2. Click **Indexing**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.
4. In the **Windows indexing settings** window, specify the indexing scope:

   - Select **Index everything** if you want to index all files within the backup scope that you have specified at the **Backup mode** step of the wizard. Veeam Agent for Microsoft Windows will index all files that reside:
     - On the protected computer OS (for entire computer backup)
     - On the volumes that you have specified for backup (for volume-level backup)
     - In the folders that you have specified for backup (for file-level backup)
   
   - Select **Index everything except** if you want to index all files on the protected computer OS 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%`, `%Program Files%` 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%`, `%Program Files%` and `%Temp%`. 

![Image of Windows Servers Indexing Settings dialog box](image)
Step 13. Specify Backup Schedule

At the Schedule step of the wizard, specify the schedule according to which you want to perform backup. Backup job scheduling options differ depending on the platform and job mode that you have selected at the Job Mode step of the wizard:

- Scheduling Settings for Workstations
- Scheduling Settings for Servers and Failover Clusters

**NOTE:**

If you configure a backup policy, after you click Apply at the Schedule step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.

Scheduling Settings for Workstations

At the Schedule step of the wizard, specify the schedule according to which you want to perform backup.

To specify the job schedule:

1. Select the Daily at check box and use the fields on the right to specify time and days when the backup job must start:
   - Everyday — select this option to start the job at specific time daily.
   - On week-days — select this option to start the job at specific time on week-days.
   - On these days — select this option to start the job at specific time on selected days.
   
   You can leave the Daily at check box unchecked to configure the backup job without daily schedule. In this case, you will be able to use the backup job to perform backup automatically at specific events.

2. If you have selected the On these days option, click the Days button and clear check boxes for the days when the job must not start.

3. Select the action that Veeam Agent for Microsoft Windows must perform in case the protected computer is powered off at the time when the scheduled backup job must start.
   - Backup once powered on — select this option if you want Veeam Agent for Microsoft Windows to start the scheduled backup job when the protected computer is powered on.
   - Skip backup — select this option if you want Veeam Agent for Microsoft Windows not to start the scheduled backup job when the computer is powered on. Veeam Agent for Microsoft Windows will perform backup at the next scheduled time.

4. If you want Veeam Agent for Microsoft Windows to perform a finalizing action after the backup job completes successfully, select the necessary action:
   - Keep running — select this option if the computer must keep on working.
   - Sleep — select this option if you want Veeam Agent for Microsoft Windows to bring the computer to the standby mode.
   - Shutdown — select this option if you want Veeam Agent for Microsoft Windows to shut down the computer.
   - Hibernate — select this option if you want Veeam Agent for Microsoft Windows to bring the computer to the hibernate mode. This option is available if the hibernate mode is enabled on the protected computer. To learn more, see this Microsoft KB article.
When the backup job completes, Veeam Agent for Microsoft Windows will prompt a dialog with a countdown to the selected post-job action. You can select to proceed to the action immediately or to cancel the action. To learn more, see the Controlling Backup Post-Job Action section in the Veeam Agent for Microsoft Windows User Guide.

5. In the **At the following events** section, specify settings for events that trigger the backup job launch:

- Select the **Lock** check box if you want to start the backup job when the user locks the Veeam Agent computer.
- Select the **Log off** check box if you want to start the backup job when the user working with the computer performs a logout operation.
- Select the **When backup target is connected** check box if you want to start the backup job when the backup storage becomes available (for example, when the computer connects to a local network and the target shared folder is accessible).
- Select the **Eject removable storage once backup is completed** check box if you want Veeam Agent for Microsoft Windows to unmount the storage device after the backup job completes successfully. With this option selected, backup files on the removable storage will be protected from encrypting ransomware, such as CryptoLocker.
- Use the **Back up no more often than every <N> <time units>** field to restrict the frequency of backup job sessions. Specify a minutely, hourly or daily interval between the backup job sessions. The **Back up no more often than every <N> <time units>** option is applied only to job sessions started at specific events. Daily backups are performed according to defined schedule regardless of the time interval specified for this setting.
IMPORTANT!

If the power scheme on the Veeam Agent computer does not allow using wake up timers, Veeam Agent for Microsoft Windows will not be able to wake your computer from sleep for backup. You can manually change the power scheme settings on the Veeam Agent computer. To do this, navigate to Control Panel > All Control Panel Items > Power Options > Edit Plan Settings.

Scheduling Settings for Servers and Clusters

At the Schedule step of the wizard, specify the schedule according to which you want to perform backup.

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 backup job manually to create 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:

- The defined interval always starts at 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, the job will start immediately and then run 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.

- [For Managed by backup server mode only] 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.
NOTE:

Mind the following:

- The **After this job** option is not available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.
- 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.

3. In the **Automatic retry** section, define whether Veeam Backup & Replication or Veeam Agent for Microsoft Windows (depending on the selected job mode) must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Agent for Microsoft Windows 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 impact performance of your server. 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** window, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.
Step 14. Review Backup Job Settings

At the Summary step of the wizard, complete the backup job configuration process.

1. Review settings of the configured Veeam Agent backup job.

2. [For backup job managed by backup server] 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.
Creating Agent Backup Job for Linux Computers

To back up data of a computer protected with Veeam Agent for Linux, you must configure a Veeam Agent backup job in Veeam Backup & Replication.

Before You Begin

Before you create a Veeam Agent backup job in the Veeam Backup & Replication console, check the following prerequisites:

- The Veeam Backup & Replication license must have a sufficient number of instances to process servers and/or workstations that you plan to add to the Veeam Agent backup job.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the job must be configured in advance.
- [For backup jobs targeted at the cloud repository] The Veeam Cloud Connect service provider must be added in the Veeam backup console.

Veeam Agent backup jobs have the following limitations:

- [For Veeam Agent backup job managed by backup server] You can create Veeam Agent backups on a Veeam backup repository only. Other types of target locations are not supported.
- [For Veeam Agent backup job managed by Veeam Agent] You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- After you start managing a Veeam Agent computer with Veeam Backup & Replication, data backup for this computer is performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer starts a new backup chain on a target location specified in the backup job settings. You cannot continue the existing backup chain that was created by Veeam Agent operating in the standalone mode.
- You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- Veeam Agent does not support creating transaction log backups in the cloud repository. You cannot enable transaction log backup options in the properties of the backup job targeted at the cloud repository.
Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup job for protected computers that run a Linux OS in one of the following ways:

- **Create a new backup job** — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard. You will be able to specify protection groups, individual Active Directory objects and/or Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.

- **Add a protection group to a new backup job** — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected protection group to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.

- **Add individual computers to a new backup job** — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected computers to the backup job. You will also be able to change the list of Veeam Agent computers to which the backup job settings must apply at the Computers step of the wizard.

Launching Backup Job Wizard

To launch the New Agent Backup Job wizard, do either of the following:

- On the **Home** tab, click **Backup Job** > **Linux computer**.
- Open the **Home** view. Select the **Jobs** node and click **Backup Job** > **Linux computer** on the ribbon.
- Open the **Home** view. Right-click the **Jobs** node and select **Backup** > **Linux computer**.

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Linux** > **New job**.

- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup job and click **Add to Backup** > **Linux** > **New job** on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the protection group to the job. You can add other protection groups and (or) individual computers to the job later on, when you pass through the wizard steps.
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup job, do either of the following:

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job, right-click the selected computer and select *Add to backup job > New job*.

- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job and click *Add to Backup > New job* on the ribbon.

Veeam Backup & Replication will start the New Agent Backup Job wizard and add the selected computers to the job. You can add other computers and (or) protection groups to the job later on, when you pass through the wizard steps.

**TIP:**

Consider the following:

- You can press and hold `[CTRL]` to select multiple computers at once.
- You can add an individual computer or protection group to a Veeam Agent backup job that is already configured in Veeam Backup & Replication. To learn more, see Adding Computers to Backup Job and Adding Protection Group to Backup Job.
Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify protection settings for the backup job:

1. Select the type of protected computers whose data you want to back up with Veeam Agents.
2. If you choose to back up data pertaining to servers, select the job mode.

   The job mode defines the type of the created Veeam Agent backup job: the backup job (backup job managed by the backup server) or backup policy (backup job managed by Veeam Agent).

Selecting Protected Computer Type

At the **Job Mode** step of the wizard, in the **Type** field, select the type of protected computers whose data you want to back up with Veeam Agents. The selected type defines what settings will be available for the configured backup job and the job mode. You can select one of the following computer types:

- **Workstation** — select this option if you want to back up data pertaining to Linux-based workstations or laptops. This option is suitable for computers that reside in a remote location and may have limited connection to the backup server.

  For backup jobs that process workstations, Veeam Backup & Replication offers settings similar to the job settings available in Veeam Agent for Linux operating in the **Workstation** mode. To learn more, see Veeam Agent for Linux User Guide.

  With this option selected, the backup job will be managed by Veeam Agent installed on the protected computer — you do not need to select the job mode.

- **Server** — select this option if you want to back up data pertaining to Linux-based servers. This option is suitable for computers that have permanent connection to the backup server.

  For backup jobs that process servers, Veeam Backup & Replication offers settings similar to the job settings available in Veeam Agent for Linux operating in the **Server** mode. To learn more, see Veeam Agent for Linux User Guide.

  With this option selected, you can also select the job mode. To learn more, see Selecting Job Mode.
Selecting Job Mode

If you selected the **Servers** computer type in the **Type** field, in the **Mode** field, select the job mode. You can select one of the following modes:

- **Managed by backup server** — select this option if you want to configure the Veeam Agent backup job. With this option selected, you will be able to add one or more individual computers and/or protection groups to the job and instruct Veeam Backup & Replication to create Veeam Agent backups in a Veeam backup repository or Veeam Cloud Connect repository. The Veeam Agent backup job will run on the backup server in the similar way as a regular job for VM data backup. To learn more, see Backup Job.

- **Managed by agent** — select this option if you want to configure the backup policy. The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers, and acts as a saved template. With this option selected, you will be able to add one or more individual computers and/or protection groups to the backup policy, and instruct Veeam Agent to create backups on a local disk of a protected computer, in a network shared folder, Veeam backup repository or Veeam Cloud Connect repository. To learn more, see Backup Policy.
Step 3. 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.

---

Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and/or individual computers that you want to back up.

You can add to the Veeam Agent backup job one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. You can also add to the job computers that are not added to inventory yet. Veeam Backup & Replication will add such computers to the job and also add them to the **Manually Added** protection group.

Jobs with protection groups are dynamic in their nature. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup job is created, Veeam Backup & Replication will automatically update the job settings to include the added computer.
NOTE:
If you used the Add to backup job > Linux > New job option to launch the New Agent Backup Job wizard, the Protected computers list will already contain computers that you have selected to add to the job. You can remove some computers from the job or add new computers to the job, if necessary.

Adding Protection Groups and Computers from Inventory

To add protection groups and/or individual computers to the Veeam Agent backup job:

1. Click Add > Protection group.
2. In the Select Objects window, select one or more protection groups and/or computers in the list and click OK. You can press and hold [CTRL] to select multiple objects at once.

To quickly find the necessary object, use the search field at the bottom of the Select Objects window.

1. Enter the object name or a part of it in the search field.
2. Click the Start search button on the right or press [ENTER].
Adding New Computers

To add to the Veeam Agent backup job new computers that do not exist in the inventory:

1. Click Add > Individual computer.

2. In the Add Computer window, in the Host name or IP address field, enter a full DNS name or IP address of the computer that you want to add to the job.

3. From the Credentials list, select a user account that has administrative permissions on the computer that you want to add to the job. 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 the Credentials Manager section in the Veeam Backup & Replication User Guide.
Step 5. Select Backup Mode

At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup.

1. In the **Backup mode** section, select the backup mode. You can select one of the following options:

   - **Entire computer** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, directories, application data and so on. With this option selected, you will pass to one of the following steps:
     - **Storage** — if the Managed by backup server option was selected at the **Job Mode** step of the wizard.
     - **Destination** — if the Managed by agent option was selected at the **Job Mode** step of the wizard.

   - **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, the system volume. When you restore data from such backup, you will be able to recover data on these volumes only: files, directories, application data and so on. With this option selected, you will pass to the **Objects** step of the wizard.

   - **File level backup** — select this option if you want to create a backup of individual directories on your computer. With this option selected, you will pass to the **Objects** step of the wizard.

2. **[For file-level backup]** If you want to perform backup in the snapshot-less mode, select the **Backup directly from live file system** check box. With this option selected, Veeam Agent for Linux will not create a snapshot of a backed-up volume during backup. This allows Veeam Agent to back up data residing in file systems that are not supported for snapshot-based backup with Veeam Agent for Linux. To learn more, see the **Snapshot-Less File-Level Backup** section in the Veeam Agent for Linux User Guide.
Step 6. Specify Backup Scope Settings

The **Objects** step of the wizard is available if you chose to create volume-level or file-level Veeam Agent backups. Specify backup scope for the backup job:

- **Specify volumes to back up** — if you have selected the **Volume level backup** option at the **Backup Mode** step of the wizard.
- **Specify directories to back up** — if you have selected the **File level backup** option at the **Backup Mode** step of the wizard.

Specifying Volumes to Back Up

The **Objects** step of the wizard is available if you have chosen to create volume-level backup. At this step of the wizard, you must specify the backup scope — define what volumes you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified volume does not exist on one or more computers in the job, the job will skip such volumes on those computers and back up only existing ones. To specify the backup scope:

1. In the **Objects to backup** field, click **Add** and select the type of object that you want to include in the backup: **Device**, **Mount point**, **LVM** or **BTRFS**.
2. In the **Add Object** window, specify the object that you want to back up and click **OK**.

You can specify the following objects to back up:

- **Block devices**. You can include in the backup scope all volumes on a computer disk or individual volumes of a protected computer:
  - To include all volumes on a computer disk in the backup, type the path to a block device that represents the disk whose volumes you want to back up. For example: `/dev/sda`.
  - To include a specific volume of a protected computer in the backup, type the path to a block device that represents the volume that you want to back up. For example: `/dev/sda1`.

- **Mount points**. You can include in the backup scope individual volumes of a protected computer. Type the path to a mount point of the volume that you want to back up. For example: `/ or `/home`. 

**TIP:**

File-level backup is typically slower than volume-level backup. Depending on the performance capabilities of your computer and backup environment, the difference between file-level and volume-level backup job performance may increase significantly. If you plan to back up all folders with files on a specific volume or back up large amount of data, it is recommended that you configure volume-level backup instead of file-level backup.
1. LVM volumes. You can include in the backup scope entire LVM volume groups or individual LVM logical volumes of a protected computer. Type the path to a mount point or a block device that represents the volume group or logical volume that you want to back up. For example: `/dev/vg` or `/dev/vg/lv1`.

2. Btrfs subvolumes. You can include in the backup scope all Btrfs subvolumes of a Btrfs storage pool or specific Btrfs subvolumes.
   - To include all subvolumes of a Btrfs pool in the backup, type the path to a block device that represents the Btrfs pool. For example: `/dev/sda1`.
   - To include a specific Btrfs subvolume in the backup, type the path to a mount point of this subvolume. For example: `/sub1`.

3. Repeat steps 1–2 for all objects that you want to back up.

If you have created several system partitions, for example, a separate partition for the `/boot` directory, make sure that you include all of these partitions in the backup. Otherwise, Veeam Agent for Linux does not guarantee that the OS will boot properly when you attempt to recover from such backup.
Specifying Directories to Back Up

The **Objects** step of the wizard is available if you have chosen to create a file-level backup.

At this step of the wizard, you must specify the backup scope — define what directories with files you want to include in the backup. The specified backup scope settings will apply to all computers that are added to the backup job. If a specified directory does not exist on one or more computers in the job, the job will skip such folder on those computers and back up existing ones.

To specify directories to back up:

1. In the **Choose directories to backup** field, click **Add**.
2. In the **Add Object** window, type the path to a directory that you want to back up, for example, `/home/user01`, and click **OK**.
3. Repeat steps 1-2 for all directories that you want to back up.
Configuring Filters

To include or exclude files of a specific type in/from the file-level backup, you can configure filters.

To configure a filter:

1. At the Objects step of the wizard, click Advanced.
2. Specify what files you want to back up:
   - In the Include masks field, specify file names and/or masks for file types that you want to back up, for example, *Report.pdf* or *filename*. Veeam Agent for Linux will create a backup only for selected files. Other files will not be backed up.
   - In the Exclude masks field, specify file names and/or masks for file types that you do not want to back up, for example, *OldReports.tar.gz* or **.odt*. Veeam Agent for Linux will back up all files except files of the specified type.
3. Click Add.
4. Repeat steps 2–3 for each mask that you want to add.

You can use a combination of include and exclude masks. Note that exclude masks have a higher priority than include masks. For example, you can specify masks in the following way:

- Include mask: *pdf*
- Exclude mask: *draft*

Veeam Agent for Linux will include in the backup all files of the PDF format that do not contain draft in their names.
Step 7. Select Backup Destination

The **Destination** step of the wizard is available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.

At this step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

You can store backup files in one of the following locations:

- **Local storage** — select this option if you want to save a backup on a removable storage device attached to a protected computer or on a local drive of a protected computer. With this option selected, you will pass to the **Local Storage** step of the wizard.

**IMPORTANT!**

It is recommended that you store backups in the external location like USB storage device or shared network folder. You can also keep your backup files on the separate non-system local drive.

- **Shared folder** — select this option if you want to save a backup in a network shared folder. With this option selected, you will pass to the **Shared folder** step of the wizard.

- **Veeam backup repository** — select this option if you want to save a backup on a backup repository managed by a Veeam backup server. With this option selected, you will pass to the **Backup Server** step of the wizard.

- **Veeam Cloud Connect repository** — select this option if you want to save a backup on a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the **Storage** step of the wizard.
Step 8. Specify Backup Storage Settings

Specify backup storage settings for the backup job:

- If you have selected the Managed by backup server mode at the Job Mode step of the wizard, you can create Veeam Agent backups on a backup repository managed by this Veeam backup server. Specify Veeam backup repository settings at the Storage of the wizard.

- If you have selected the Managed by agent mode at the Job Mode step of the wizard, specify backup storage settings at one of the following steps of the wizard:
  - Local storage settings — if you have selected the Local storage option at the Destination step of the wizard.
  - Shared folder settings — if you have selected the Shared folder option at the Destination step of the wizard.
  - Veeam backup repository settings — if you have selected the Veeam backup repository option at the Destination step of the wizard.
  - Cloud repository settings — if you have selected the Veeam Cloud Connect repository option at the Destination step of the wizard.

Backup Storage Settings

The Storage step of the wizard is available if you have selected the Managed by backup server mode at the Job Mode step of the wizard.

Specify settings for the target backup repository managed by the same backup server that manages the Backup Job:

1. From the Backup repository list, select a backup repository where you want to store Veeam Agent backups. You can select from the following types of backup repositories:
   - Veeam backup repository configured on the backup server that will manage the created backup job.
   - Cloud repository allocated to your tenant account by a Veeam Cloud Connect service provider.

   When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. 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.
NOTE:
Mind the following:

- Backup job mapping is available only for a Veeam Agent backup job managed by the backup server.
- You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a backup chain that was created on a backup repository by Veeam Agent operating in the standalone mode.

3. Specify backup retention policy settings:
   - From the Retention policy list, select restore points and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication will remove the earliest restore points from the backup chain.
   - From the Retention policy list, select days and specify the number of days for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files for 7 days. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

4. To use the GFS (Grandfather-Father-Son) retention scheme, select the Keep some periodic full backups longer for archival purposes check box and click Configure. In the Configure GFS window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the GFS Retention Policy section in the Veeam Backup & Replication User Guide.

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 destinations for this job check box. With this option enabled, the New Agent 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.
6. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.

Local Storage Settings

The **Local Storage** step of the wizard is available if you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard and chosen to save the backup on a local drive of your computer.

Specify local storage settings:

1. In the **Local folder** field, type a path to a folder on a protected computer where backup files must be saved. If the specified folder does not exist in the file system of a protected computer, Veeam Agent for Linux will create this folder and save the resulting backup file to this folder. If the volume on which the specified folder must reside does not exist on a protected computer, Veeam Backup & Replication will not apply the backup job settings to this computer.

**IMPORTANT!**

USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.
2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

3. Click **Advanced** to specify advanced settings for the backup job. To learn more, see **Specify Advanced Backup Settings**.

---

**Shared Folder Settings**

The **Shared Folder** step of the wizard is available if you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard and chosen to save the backup in a network shared folder.

Specify shared folder settings:

1. In the **File share type** section, select the type of a network shared folder:
   - **NFS** – to connect to a network shared folder using the NFS protocol.
   - **SMB** – to connect to a network shared folder using the SMB (CIFS) protocol.

2. In the **Shared folder** field, type a name of the network shared folder in which you want to store backup files.
   - [For an NFS shared folder] Specify a name of the network shared folder in the `SERVER://DIRECTORY` format.
   - [For an SMB shared folder] Specify a UNC name of the network shared folder. Keep in mind that the UNC name always starts with two back slashes (`\`).
3. [For an SMB shared folder] If the network shared folder requires authentication, select the **This share requires access credentials** check box and select from the list a user account that has access permissions on this shared folder. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. The user name must be specified in the `DOMAIN\USERNAME` format.

4. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

5. Click **Advanced** to specify advanced settings for the backup job. To learn more, see **Specify Advanced Backup Settings**.

### Veeam Backup Repository Settings

If you have selected the **Managed by agent** mode for the backup job and chosen to store backup files on a Veeam backup repository, specify settings to connect to the backup repository:

1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Backup Repository step of the wizard, select the Veeam backup repository.
Specifying Backup Server Settings

The Backup Server step of the wizard is available if you have selected the Managed by agent mode at the Job Mode step of the wizard and chosen to store backup files on a Veeam backup repository.

In the DNS name or external IP address field, review and change if necessary the name or IP address of the Veeam backup server on which you configure the Veeam Agent backup job. The specified DNS name or IP address must be accessible from the network to which Veeam Agent computers are connected.

NOTE:
Veeam Backup & Replication does not automatically update information about the backup server in the backup policy settings after migration of the configuration database. After you migrate configuration data to a new location, you must specify the name or IP address of the new backup server in the properties of all backup policies configured in Veeam Backup & Replication.
Selecting Backup Repository

The **Backup Repository** step of the wizard is available if you have selected the **Managed by agent** mode at the **Job Mode** step of the wizard and chosen to save backup files on a Veeam backup repository.

Specify settings for the target backup repository:

1. From the **Backup repository** list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.

2. In the **Restore points to keep on disk** field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

3. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary destinations for this job** check box. With this option enabled, the **New Agent 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.

4. Click **Advanced** to specify advanced settings for the backup job. To learn more, see **Specify Advanced Backup Settings**.
Cloud Repository Settings

The Storage step of the wizard is available if you have selected the Managed by agent mode at the Job Mode step of the wizard and chosen to save backup files on a Veeam Cloud Connect repository.

NOTE:
Keep in mind that FQDN or IP addresses of Veeam Agent machines that you back up to the cloud repository will be visible to the Veeam Cloud Connect service provider. To learn more, see Creating Protection Groups: Before You Begin.

Specify settings for the cloud repository:

1. From the Backup repository list, select a cloud repository where you want to store created backups. The Backup repository list displays cloud repositories allocated to your tenant account by the Veeam Cloud Connect service provider. When you select a cloud repository, Veeam Backup & Replication automatically checks how much free space is available on the repository.

2. In the Restore points to keep on disk field, specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Agent for Linux keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent for Linux will remove the earliest restore points from the backup chain.

3. Click Advanced to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.
Step 9. Specify Advanced Backup Settings

In the Advanced Settings window, specify advanced settings for the Veeam Agent backup job:

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings
- [For Veeam Agent jobs managed by the backup server] Script settings

TIP:

After you specify necessary settings for the Veeam Agent 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. Click Advanced at one of the following steps of the wizard:
   - Storage — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - Local Storage — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - Shared Folder — if you have selected to save backup files in a network shared folder.

2. [For Veeam Agent jobs managed by the backup server] If you want to periodically create synthetic full backups, on the Backup tab, select the Create synthetic full backups periodically check box and click Days to schedule synthetic full backups on the necessary week days.

3. If you want to periodically create active full backups, select the Create active full backups periodically check box. Use the Monthly on or Weekly on selected days options to define scheduling settings.
NOTE:
Consider the following:

- Before scheduling periodic full backups, you must make sure that you have enough free space on the target location.
- If you schedule the active full backup and synthetic full backup on the same day, Veeam Backup & Replication will perform only active full backup. Synthetic full backup will be skipped.

Maintenance Settings

You can specify maintenance settings for a backup chain created with the Veeam Agent backup job. Maintenance operations help make sure that the backup chain remains valid and consistent.

Maintenance settings are available for the following types of Veeam Agent backup jobs that process Linux computers:

- Backup job managed by the backup server.
- Backup job managed by Veeam Agent (backup policy). For backup jobs of this type, maintenance settings are available only if the job is targeted at a Veeam backup repository.
To specify maintenance settings for the backup job:

1. At the Storage step of the wizard, click Advanced.

2. Click the Maintenance tab.

3. [For backup jobs managed by the backup server] 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 where 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 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 protected computer to the Veeam 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 the Health Check for Backup Files section in the Veeam Backup & Replication User Guide.

   **NOTE:**

   For a file-level Veeam Agent backup job, if Veeam Backup & Replication detects corrupted data blocks in the restore point during health check, Veeam Backup & Replication will always create a full backup file during the health check retry.

4. Select the Remove deleted items data after check box and specify the number of days for which you want to keep the backup created with the backup job in the target location.

   - For backup jobs managed by the backup server, deleted items retention policy is similar to retention policy for deleted VMs. After you remove a protection group or individual computer from a Veeam Agent backup job, Veeam Backup & Replication will keep its data on the backup repository for the period that you have specified. When this period is over, backup data of this computer will be removed from the backup repository. For more information, see the Retention Policy for Deleted VMs section in the Veeam Backup & Replication User Guide.

   - For backup jobs managed by Veeam Agent, if Veeam Agent does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location. For more information, see the Veeam Agent for Linux User Guide.

   By default, the deleted items data retention period is 30 days. Do not set the deleted items retention period to 1 day or a similar short interval. In the opposite case, the backup job may work not as expected and remove data that you still require.

5. [For backup jobs managed by the backup server] 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 items (protection groups or individual computers), Veeam Backup & Replication will remove these data blocks. For more information, see the Compact of Full Backup File section in the Veeam Backup & Replication User Guide.
NOTE:
Consider the following:

- If you want to periodically compact a full backup, you must make sure that you have enough free space in the target location. For the compact operation, the amount of free space must be equal to or more than the size of the full backup file.
- In contrast to the compact operation for a VM backup, during compact of a full Veeam Agent backup file, Veeam Backup & Replication does not perform the data take out 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, Veeam Backup & Replication will not extract data for this machine to a separate full backup file.

Storage Settings

To specify storage settings for the backup job:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.

2. Click the **Storage** tab.
3. From the Compression level list, select a compression level for the backup: None, Dedupe-friendly, Optimal, High or Extreme.

4. 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 Agent for Linux will use data blocks of different size to optimize the size of backup files and job performance.

5. 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 the Password Manager section in the Veeam Backup & Replication User Guide.

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 the Decrypting Data Without Password section in the Veeam Backup & Replication User Guide.
NOTE:

Consider the following:

- Data encryption settings for Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup jobs and policies targeted at a Veeam backup repository, all data encryption operations are performed in Veeam Backup & Replication, too. Encryption settings are passed to a Veeam Agent computer only in case this computer is added to a backup policy targeted at a local drive of a protected computer or at a network shared folder. Veeam Backup & Replication performs this operation when applying the backup policy to a protected computer.

- If you change a password for data encryption for an existing backup policy targeted at a Veeam backup repository without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.

- If you enable encryption for an existing Veeam Agent backup, during the next job session Veeam Agent for Linux 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 backup job, Veeam Agent for Microsoft Windows will encrypt the backup chain starting from the next restore point created with this job.

- [For backup policies targeted at a local drive, network shared folder or cloud repository] When you enable data encryption for a backup policy, Veeam Backup & Replication uses the specified password to encrypt backups of all Veeam Agent computers added to the backup policy. A Veeam Agent computer user can restore data from the backup of this computer without providing a password to decrypt backup. To restore data from a backup of another computer in this backup policy, a user must provide a password specified in the backup policy settings.

  This scenario differs from the same scenario in earlier versions of Veeam Backup & Replication where all backups created for Veeam Agent computers in the backup policy could be accessed from any computer in the backup policy without providing a password.

To learn more about data encryption in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.
Notification Settings

You can specify notification settings for Veeam Agent backup jobs configured in Veeam Backup & Replication. Notification options differ depending on the job mode that you have selected at the Job Mode step of the wizard:

- **Managed by backup server.** To learn more, see Notification Settings for Veeam Agent Backup Job.
- **Managed by agent.** To learn more, see Notification Settings for Backup Policy.

Notification Settings for Veeam Agent Backup Job

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 the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.

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 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 the Configuring Global Email Notification Settings section in Veeam Backup & Replication User Guide.
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.

- To configure a custom notification for the job, select **Use custom notification settings specified below**. You can specify the following notification settings:
  
  - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: `%Time%` (completion time), `%JobName%`, `%JobResult%`, `%ObjectCount%` (number of machines in the job) and `%Issues%` (number of machines in the job that have been processed with the Warning or Failed status).
  
  - 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.

  - 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.
Notification Settings for Backup Policy

You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup job sessions performed for the last 24-hour period on computers to which the backup policy is applied.

**NOTE:**

Email reports with backup policy statistics will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.

After you enable notification settings for the backup policy, Veeam Backup & Replication will send reports with the backup policy statistics to email addresses specified in global email notification settings and email addresses specified in the backup policy settings.

To specify notification settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Shared Folder** — if you have selected to save backup files in a network shared folder.
2. Click the **Notifications** tab.
3. Select the **Send daily e-mail report to the following recipients** check box and specify a recipient's email address in the field below. You can enter several addresses separated by a semicolon.
4. You can choose to use global notification settings or specify custom notification settings.
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server. Veeam Backup & Replication will send the email report containing backup policy statistics at 8:00 AM daily.
   - To configure a custom notification for the backup policy, select **Use custom notification settings specified below**. You can specify the following notification settings:
     - In the **Send report at** field, specify the time when Veeam Backup & Replication must send the email notification for the backup policy. Veeam Backup & Replication will sent the report daily at the specified time.
     - In the **Subject** field, specify a notification subject. You can use the following variables in the subject: %Time% (completion time), %JobName%, %JobResult%, %ObjectCount% (number of machines in the backup policy) and %Issues% (number of machines in the backup policy that have been processed with the **Warning or Failed** status).
- 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.

### Script Settings

You can specify what scripts Veeam Backup & Replication will execute on the backup server before and after the backup job session. This option is available if you have selected the **Managed by backup server** mode at the **Job Mode** step of the wizard.

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 **Before the job** and **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 under the account under which the Veeam Backup Service runs (the local System account or account that has the local Administrator permissions 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.

**TIP:**

Consider the following:

- Custom scripts that you define in the advanced job settings relate to the backup job itself, not the OS quiescence process on protected computers. To add pre-freeze and post-thaw scripts for Veeam Agent computer OS quiescence, use the **Guest Processing** step of the wizard.
- You can also specify what scripts will be executed on a Veeam Agent computer before and/or after the backup job session. To learn more, see **Backup Job and Snapshot Scripts**.
Step 10. Specify Secondary Target

The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent 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** in the Veeam Backup & Replication User Guide.

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 Veeam Agent backup job to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the Veeam Agent 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 Veeam Agent 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 11. Specify Guest Processing Settings

At the Guest Processing step of the wizard, you can enable the following guest OS processing settings for a Veeam Agent backup job that includes Linux-based computers:

- Application-aware processing
- Processing of Oracle databases
- Processing of MySQL databases
- Processing of PostgreSQL databases
- Use of backup job and snapshot scripts
- File indexing

NOTE:

Consider the following:

- Application-aware processing and database processing options are available if you have selected the Server option at the Job Mode step of the wizard.
- Application-aware processing and database processing options are available if you have selected the Entire computer or Volume level backup option at the Backup Mode step of the wizard.
- Available script settings depend on the options that you have selected at the Job Mode and Backup Mode steps of the wizard. To learn more, see Backup Job and Snapshot Scripts.
Application-Aware Processing

If a machine protected with Veeam Agent for Linux runs an Oracle, MySQL or PostgreSQL database system, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup guarantees proper recovery of databases 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 a protection group or individual computer and click Edit.
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click Add and choose the computer whose settings you want to customize. Then select the computer 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 Agent for Linux to process databases. With this option selected, if an error occurs when processing a database, Veeam Agent for Linux will stop the backup process.
     If you select this option, you will need to specify database processing settings. For more information, see Oracle Processing Settings, MySQL Processing Settings and PostgreSQL Processing Settings.
   - Select Try application processing, but ignore failures if you want Veeam Agent for Linux to process databases. With this option selected, if an error occurs when processing a database, Veeam Agent for Linux will not stop the backup process. Instead, Veeam Agent for Linux will skip this database and proceed to the next one. After the backup process completes, you will be able to restore data from the backup and restore databases that were successfully processed during backup.
     If you select this option, you will need to specify database processing settings. For more information, see Oracle Processing Settings, MySQL Processing Settings and PostgreSQL Processing Settings.
Select **Disable application processing** if you do not want Veeam Agent for Linux to process databases. If you select this option, the **Oracle**, **MySQL** and **PostgreSQL** tabs of the **Processing Settings** window will become unavailable. You will be able to specify script settings for the job on the **Scripts** tab of the window.

---

**Oracle Processing Settings**

If you back up an Oracle database, you can specify how Veeam Agent for Linux must process archived 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 a protection group or individual computer and click **Edit**.
   
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the **General** tab, in the **Applications** section, select **Require successful processing** or **Try application processing, but ignore failures**.
5. In the **Processing Settings** window, click the **Oracle** tab.
6. To specify a user account that Veeam Agent for Linux will use to connect to the Oracle database, select from the Specify Oracle account with SYSDBA privileges list a user account that has SYSDBA rights on the database. If you have not set up credentials beforehand, click the Manage accounts link or click Add on the right to add credentials.

By default, the Use guest credentials option is selected in the list. With this option selected, Veeam Agent for Linux will connect to the Oracle database under the account that you have specified for the protected computer in the protection group settings.

7. In the Archived logs section, specify if Veeam Agent for Linux must delete archived logs on the Oracle database:

   o Select Do not delete archived logs if you want Veeam Agent for Linux to preserve archived logs. When the backup job completes, Veeam Agent for Linux 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 may grow large and consume all disk space. In this case, the database administrator must take care of archived logs him-/herself.

   o Select Delete logs older than <N> hours or Delete logs over <N> GB if you want Veeam Agent for Linux to delete archived logs that are older than <N> hours or larger than <N> GB. Veeam Agent for Linux will wait for the backup job to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.

8. [For Veeam Agent jobs managed by the backup server] To back up Oracle archived logs with Veeam Agent for Linux, 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 minimum log backup interval is 5 minutes. The maximum log backup interval is 480 minutes.
9. [For Veeam Agent jobs managed by the backup server] In the **Retain log backups** section, specify retention policy for archived logs stored in the backup location:

   - Select **Until the corresponding image-level backup is deleted** to apply the same retention policy for Veeam Agent 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 Veeam Agent backups. The maximum time period to keep archived logs is 60 days.

### MySQL Processing Settings

You can specify how Veeam Agent for Linux must process a MySQL database:

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 a protection group or individual computer and click **Edit**.
   
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the **General** tab, in the **Applications** section, select **Require successful processing** or **Try application processing, but ignore failures**.
5. In the **Processing Settings** window, click the **MySQL** tab.
6. To specify a user account that Veeam Agent for Linux will use to connect to the MySQL database, from the Specify MySQL account with superuser privileges list, select a user account that has the following privileges on the database:

- SELECT for all tables. If the account does not have the SELECT privilege for the table, Veeam Agent will not process the table.
- LOCK TABLES. If the account does not have this privilege, Veeam Agent will not process MyISAM tables.

If you have not set up credentials beforehand, click the Manage accounts link or click Add on the right to add credentials.

By default, the User from password file option is selected in the list. With this option selected, Veeam Agent for Linux will connect to the MySQL database under the account specified in the password file on the Veeam Agent computer. The default location for the password file is /root/.my.cnf. For information about the password file format, see the Preparing Password File for MySQL Processing section in the Veeam Agent for Linux User Guide.

7. If you want to specify a custom path to the password file, type it in the Password file path field.

For information on how Veeam Agent for Linux processes the MySQL database system, see the MySQL Backup section in the Veeam Agent for Linux User Guide.
PostgreSQL Processing Settings

You can specify how Veeam Agent for Linux must process a PostgreSQL database:

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 a protection group or individual computer and click Edit.
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click Add and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. On the General tab, in the Applications section, select Require successful processing or Try application processing, but ignore failures.
5. In the Processing Settings window, click the PostgreSQL tab.
6. To specify a user account that Veeam Agent for Linux will use to connect to the PostgreSQL database, select the account from the Specify PostgreSQL account with superuser privileges list. If you have not set up credentials beforehand, click the Manage accounts link or click Add on the right to add credentials.
   Note that if you plan to select the peer authentication method at the step 7 of this procedure, you can add a user account in the Credentials Manager without specifying the password for the account.
   By default, the Use guest credentials option is selected in the list. With this option selected, Veeam Agent will connect to the PostgreSQL database under the account that you have specified for the protected computer in the protection group settings.
7. In the The specified user is field, specify how Veeam Agent for Linux will connect to the PostgreSQL database:
   - Select Database user with password if the account that you specified at the step 6 is a PostgreSQL account, and you entered the password for this account in the Credentials Manager.
   - Select Database user with password file if the password for the account that you specified at the step 6 is defined in the .pgpass configuration file on the Veeam Agent computer. For information about the .pgpass file format, see the Password File for PostgreSQL Processing section in the Veeam Agent for Linux User Guide.
   - Select System user without password if you want Veeam Agent to use the peer authentication method. In this case, Veeam Agent will apply the Veeam Agent computer OS account as the PostgreSQL account.
For more information on how Veeam Agent for Linux processes the PostgreSQL database system, see the PostgreSQL Backup section in the Veeam Agent for Linux User Guide.

Backup Job and Snapshot Scripts

You can specify custom scripts that will be executed within the backup job session on Linux computers. Veeam Agent for Linux supports the following types of scripts:

- **Backup job scripts** — pre-job and post-job scripts that run on the Veeam Agent computer before and after the backup job session.

- **Snapshot scripts** — pre-freeze and post-thaw scripts that run on the Veeam Agent computer before and after the volume snapshot is created.

To learn more, see Backup Job Scripts.

Veeam Backup & Replication offers 2 scenarios for specifying script settings:

- **Scenario 1. Specify backup job scripts and snapshot scripts.**

  You can specify both backup job scripts and snapshot scripts for the backup job if the following conditions are met:

  a. You selected the Server option at the Job Mode step of the wizard.

  b. You did not select the Backup directly from live file system option at the Backup Mode step of the wizard.
• **Scenario 2. Specify backup job scripts only.**

In one of the following conditions, you can specify only backup job scripts that will be executed on Linux computers:

- If you selected the **Server** option at the **Job Mode** step of the wizard and selected the **Backup directly from live file system** option at the **Backup Mode** step of the wizard.

- If you selected the **Workstation** option at the **Job Mode** step of the wizard.

**TIP:**

You can also specify custom scripts that will be executed on the backup server before and/or after the backup job session. To learn more, see **Script Settings**.

---

**Specifying Backup Job and Snapshot Scripts**

To specify custom scripts for the job:

1. At the **Guest Processing** step, select the **Enable application-aware processing** check box.

2. Click **Applications**.

3. In the displayed list, select a protection group or individual computer and click **Edit**.

   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.

4. [For an entire computer backup or volume-level backup job] In the **Processing Settings** window, click the **Scripts** tab.

**NOTE:**

For a file-level backup job, application-aware processing and database processing options are not available, and no tabs are displayed in the **Processing Settings** window.

5. Select the **Enable script execution** check box.

6. In the **Job scripts** section, specify custom scripts that you want to execute before and/or after the backup job session. To do this, in the **Pre-job script** and **Post-job script** fields, click **Browse** and choose executable files from a local folder on the backup server.

7. In the **Snapshot scripts** section, specify custom scripts that you want to execute before Veeam Agent for Linux creates a snapshot of the backed-up volume and/or after the snapshot is created. To do this, in the **Pre-freeze script** and **Post-thaw script** fields, click **Browse** and choose executable files from a local folder on the backup server.
Veeam Agent for Linux supports scripts in the SH file format. During the backup job session, Veeam Backup & Replication will upload the scripts to the `/var/lib/veeam/scripts` directory on each Veeam Agent computer added to the backup job and execute them on these computers.

### Specifying Backup Job Scripts

To specify custom scripts for the job:

1. At the **Guest Processing** step, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.
   - To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. In the **Processing Settings** window, select the **Enable script execution** check box.
5. In the **Pre-job script** and **Post-job script** fields, click **Browse** to choose executable files from a local folder on the backup server.
Veeam Agent for Linux supports scripts in the SH file format. During the backup job session, Veeam Backup & Replication will upload the scripts to the `/var/lib/veeam/scripts` directory on each Veeam Agent computer added to the job and execute them on these computers.

File Indexing

To specify file indexing options:

1. At the **Guest Processing** step of the wizard, select the **Enable guest file system indexing** check box.
2. Click **Indexing**.
3. In the displayed list, select the protection group or individual computer and click **Edit**.
   
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
4. In the **Indexing Settings** window, specify the indexing scope:
   
   - Select **Index everything** if you want to index all files within the backup scope that you have specified at the **Backup mode** step of the wizard. Veeam Agent for Linux will index all files that reside:
     - On the protected computer OS (for entire computer backup)
     - On the volumes that you have specified for backup (for volume-level backup)
     - In the directories that you have specified for backup (for file-level backup)
- [For volume-level backup only] Select **Index everything except** if you want to index all files on your computer OS except those defined in the list. By default, system directories `/cdrom`, `/dev`, `/media`, `/mnt`, `/proc`, `/tmp` and `/lost+found` are excluded from indexing. You can add or delete folders using the Add and Remove buttons on the right.

To reset the list of folders to its initial state, click Default.

- [For volume-level backup only] Select **Index only following folders** to define directories that you want to index. You can add or delete directories to index using the Add and Remove buttons on the right.

**NOTE:**

You can specify a custom indexing scope only in for a volume-level backup job. For a file-level backup job that processes Linux-based computers, only the Index everything option is available.
Step 12. Specify Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

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 backup job manually to create 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:
   - The defined interval always starts at 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, the job will start immediately and then run 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.

   - [For backup job managed by backup server] 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.

**NOTE:**

Mind the following:

- The **After this job** option is not available if you have selected the **Managed by agent** option at the **Job Mode** step of the wizard.

- 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.
3. In the **Automatic retry** section, define whether Veeam Backup & Replication or Veeam Agent for Linux (depending on the selected job mode) must attempt to run the backup job again if the job fails for some reason. Enter the number of attempts to run the job and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Agent for Linux will retry the job for the defined number of times without any time intervals between the job runs.

4. [For backup job managed by backup server] 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 impact performance of your server. 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** window, define the allowed hours and prohibited hours for backup. If the job exceeds the allowed window, it will be automatically terminated.

**NOTE:**

If you configure a backup policy, after you click **Apply** at the **Schedule** step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.
Step 13. Review Backup Job Settings

At the **Summary** step of the wizard, complete the Veeam Agent backup job configuration process.

1. Review settings of the configured backup job.
2. [For backup job managed by backup server] 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.

![Edit Agent Backup Job Linux Servers Backup](image)

### Summary
- **Name**: Linux Servers Backup
- **Description**: Backup job for Linux servers
- **Type**: Server
- **Mode managed by**: backup server
- **Protected computers**: Linux Servers
- **Backup mode**: File level backup
- **Destination**: Veeam backup repository
- **Target storage**: Default Backup Repository
- **Retention policy**: 14 restore points
- **Application-aware processing**: enabled
- **Guest file system indexing**: enabled
- **Backup is scheduled to run automatically**: Off
- **GS retention policy**: 1 yearly

- **Run the job when I click Finish**

![Wizard Controls](image)

- Previous
- Next
- Finish
- Cancel
Creating Veeam Agent Backup Policy

To create a Veeam Agent backup policy, you must create a Veeam Agent backup job in Veeam Backup & Replication with the Managed by agent option selected in the job settings. In contrast to a Veeam Agent backup job managed by the backup server that is similar to a regular backup job for VM backup, a backup policy acts as a template that describes settings of individual Veeam Agent backup jobs running on protected computers. When you select the Managed by agent option in the New Agent Backup Job wizard, the subsequent steps of the wizard will automatically change to offer backup settings available in Veeam Agent for Microsoft Windows or Veeam Agent for Linux. For details, see Creating Agent Backup Job for Windows Computers and Creating Agent Backup Job for Linux Computers.

After you create a backup policy, Veeam Backup & Replication immediately connects to protected computers added to the backup policy and applies settings specified in the policy to configure the Veeam Agent backup job on each computer.
Managing Veeam Agent Backup Jobs

You can manage Veeam Agent backup jobs configured in Veeam Backup & Replication. Operations available for a Veeam Agent backup job depend on the job mode specified in the job properties:

- For a Veeam Agent backup jobs managed by the backup server, Veeam Backup & Replication allows you to perform a set of operations similar to a regular backup job for VM data backup. To learn more, see Managing Veeam Agent Backup Jobs.

- For a Veeam Agent backup job managed by Veeam Agent, or backup policy, Veeam Backup & Replication allows you to perform a set of operations similar to a regular Veeam Agent backup job configured on a Veeam Agent computer. To learn more, see Managing Veeam Agent Backup Policies.

Managing Veeam Agent Backup Jobs

You can use the Veeam Backup & Replication console to perform the following operations with a Veeam Agent backup job managed by the backup server:

- Start and stop a Veeam Agent backup job.
- Retry a Veeam Agent backup job.
- Perform active full backup.
- Edit Veeam Agent backup job settings.
- Enable and disable a Veeam Agent backup job.
- Clone a Veeam Agent backup job.
- Remove a Veeam Agent backup job.
Starting and Stopping Veeam Agent Backup Job

You can start a Veeam Agent backup job manually, for example, if you want to create an additional restore point in the backup chain and do not want to change the job schedule. You can also stop a job, for example, if processing of a Veeam Agent computer 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 Veeam Agent backup job and click Start on the ribbon or right-click the job and select Start.

Stopping Jobs

You can stop a Veeam Agent backup 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 computers in the job that have already been processed by the time you stop the job.
- Stop job gracefully. In this case, Veeam Backup & Replication will produce a new restore point only for those computers in the job that have already been processed and for computers that are being processed at the moment.

To stop a job immediately:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the Veeam Agent backup job and click Stop on the ribbon or right-click the job and select Stop. In the displayed window, click Immediately.
To stop a job gracefully:

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**.
Retrying Veeam Agent Backup Job

You can manually retry a Veeam Agent backup job configured in Veeam Backup & Replication if the job failed during the previous job session. When you retry a Veeam Agent backup job, Veeam Backup & Replication processes only those computers in the job that were not processed successfully during the previous job session.

To retry a job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job and click **Retry** on the ribbon or right-click the job and select **Retry**.
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 Veeam Agent backup job and click **Active Full** on the ribbon or right-click the job and select **Active Full**.
Editing Veeam Agent Backup Job Settings

You can edit Veeam Agent backup jobs configured in Veeam Backup & Replication at any time. For example, you may want to edit a backup job to change the backup scope, target location or job scheduling settings.

**NOTE:**

Mind the following:

- You cannot change the type of protected computers added to the job and the job mode (that is, change a Veeam Agent backup job to a backup policy and vice versa).
- If you want to specify another backup repository as a target for backups created by the job, you must delete backups from the old repository or move backups to the new repository prior to changing a backup repository in the job settings.
- [For Veeam Agent backup jobs for Linux computers] You cannot change the backup mode from file-level to volume-level and vice versa.

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**.
4. Complete the steps of the **Edit Agent Backup Job** wizard to change the job settings as required.
Enabling and Disabling Veeam Agent Backup Job

You can temporarily disable Veeam Agent backup jobs configured in Veeam Backup & Replication. When you disable a job, Veeam Backup & Replication does not start the job by the specified schedule. You can start a disabled job manually at any time you need. You can also 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.
Cloning Veeam Agent Backup Job

You can clone Veeam Agent backup jobs configured in Veeam Backup & Replication. For example, you may want to configure a Veeam Agent backup job that will be used as a ‘job template’, and use this job to create multiple jobs with similar settings.

To clone a Veeam Agent backup 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.
Removing Veeam Agent Backup Job

You can permanently remove a Veeam Agent backup job from Veeam Backup & Replication. When you remove a job, Veeam Agent backups created by this job remain intact on the backup repository. In the Veeam Backup & Replication console, such backups are displayed in the Home view, under the Backups > Imported node in the inventory pane.

To remove a job:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the Veeam Agent backup job and click Delete on the ribbon or right-click the job and select Delete.
Managing Veeam Agent Backup Policies

You can use the Veeam Backup & Replication console to perform the following operations with a Veeam Agent backup policy, that is, a Veeam Agent backup job managed by Veeam Agent:

- Apply backup policy to Veeam Agent computers.
- Start and stop Veeam Agent backup jobs on computers added to the backup policy.
- Perform active full backup on computers added to the backup policy.
- Clear the backup cache on computers added to the backup policy.
- Edit backup policy settings.
- Enable and disable a backup policy.
- Clone a backup policy.
- Remove a backup policy.
Applying Backup Policy to Protected Computers

To configure individual Veeam Agent backup jobs on protected computers added to a backup policy, Veeam Backup & Replication applies settings of the backup policy to these computers. This operation is performed automatically at the time when the backup policy is created and at the process of automatic protection group rescan. You can also apply backup policy settings manually at any time. This may be required, for example, in case one or more protected computers could not be accessed over the network at the time when the backup policy was created.

To assign a backup policy to protected computers:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the backup policy and click Apply configuration on the ribbon or right-click the policy and select Apply configuration.
Starting and Stopping Backup

You can manually start backup on Veeam Agent computers added to the backup policy, for example, if you want to create an additional restore point in the backup chain and do not want to change the backup schedule. You can also stop the backup process, for example, if processing of a Veeam Agent computer is about to take long, and you do not want the backup process to produce workload on the production environment during business hours.

When you start or stop the backup process for a backup policy, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to perform the start or stop backup jobs on these computers. Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time when the command is sent. Keep in mind that the selected operation will be performed only on those computers that received the command from the backup server.

Starting Backup

To start backup on Veeam Agent computers added to the backup policy:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the backup policy and click Start backup on the ribbon or right-click the job and select Start backup.

**TIP:**
You can also start a Veeam Agent backup job directly on a protected computer from the Veeam Agent user interface.
Stopping Backup

To stop backup on Veeam Agent computers added to the backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Stop backup** on the ribbon or right-click the job and select **Stop backup**. In the displayed window, click **Yes**.
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.

When you start active full backup for a backup policy, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to perform active full backup on these computers. Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time when the command is sent. Keep in mind that the active full backup operation will be performed only on those computers that received the command from the backup server.

To perform active full backup on Veeam Agent computers added to the backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Active Full** on the ribbon or right-click the job and select **Active Full**.
Clearing Backup Cache

You can use the Veeam backup console to delete restore points from the backup cache on computers added to the backup policy. This operation may be required, for example, if the backup cache contains one or more restore points, and the backup chain in the target location has changed prior to the time when Veeam Agent starts uploading restore points to the target location.

When you perform the clear cache operation, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to delete restore points from the backup cache on these computers. Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time when the command is sent. Keep in mind that the operation will be performed only on those computers that received the command from the backup server.

To clear the backup cache on Veeam Agent computers added to the backup policy:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, press and hold the [CTRL] key, right-click the backup policy and select Clear cache.
Editing Backup Policy Settings

You can edit settings of a Veeam Agent backup policy at any time. For example, you may want to change the backup scope, target location or scheduling settings for Veeam Agent backup jobs running on protected computers. After you change settings of the backup policy, Veeam Backup & Replication applies the specified settings to Veeam Agent backup jobs configured on protected computers added to the policy.

**NOTE:**

Mind the following:

- You cannot change the type of protected computers added to the job and the job mode (that is, change a Veeam Agent backup job to a backup policy and vice versa).
- [For Veeam Agent backup jobs for Linux computers] You cannot change the backup mode from file-level to volume-level and vice versa.
- If you change a password for data encryption without changing other backup policy settings, the process of applying the backup policy to a protected computer completes with a notification informing that the backup policy was not modified. This happens because data encryption settings for managed Veeam Agents are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.

To edit backup policy settings:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Edit** on the ribbon or right-click the policy and select **Edit**.
4. Complete the steps of the **Edit Agent Backup Job** wizard to change the job settings as required.
Enabling and Disabling Backup Policy

You can temporarily disable Veeam Agent backup policies configured in Veeam Backup & Replication. While a backup policy is in the disabled state, the following operations are not performed in the Veeam Agent management infrastructure:

- Veeam Backup & Replication does not apply backup policy settings to Veeam Agent computers.
- Veeam Agent running on a protected computer does not create backups on the backup repository.

If a user of a protected computer starts the Veeam Agent backup job manually or if the job starts by schedule, the job session will fail and report the "The job has been disabled by the Veeam Backup & Replication administrator" error. To let Veeam Agent for Microsoft Windows store backups to the backup repository again, you must enable the disabled policy and apply it to protected computers. To learn more, see Applying Backup Policy to Protected Computers.

NOTE:
Disabling a backup policy does not affect performance of Veeam Agent backup jobs if a local drive or network shared folder is specified as a target location for backups in the policy settings.

To disable a Veeam Agent backup policy:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the Veeam Agent backup policy and click Disable on the ribbon or right-click the policy and select Disable.

To enable a disabled policy, select it in the list and click Disable on the ribbon once again.
Cloning Backup Policy

You can clone backup policies configured in Veeam Backup & Replication. For example, you may want to configure a backup policy that will be used as a ‘policy template’, and use this policy to create multiple policies with similar settings.

To clone a backup policy:

1. Open the Home view.
2. In the inventory pane, select Jobs.
3. In the working area, select the backup policy and click Clone on the ribbon or right-click the backup policy and select Clone.
4. After a backup policy is cloned, you can edit all its settings, including the job name.

**NOTE:**

The backup policy cloning functionality is available only in the Enterprise and Enterprise Plus editions of Veeam Backup & Replication.
Removing Backup Policy

You can permanently remove a Veeam Agent backup policy from Veeam Backup & Replication. When you remove a backup policy, Veeam Backup & Replication also removes child backup jobs configured on Veeam Agent computers. Backups created by these jobs remain on the target location.

To remove a Veeam Agent backup policy:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup policy and click **Delete** on the ribbon or right-click the policy and select **Delete**.
Managing Protected Computers

You can perform the following operations with computers added to the inventory in Veeam Backup & Replication:

- Move an unmanaged computer to a protection group.
- Add a protected computer to a Veeam Agent backup job.
- Perform quick backup for a protected computer.
- View properties of a protected computer.
- Rescan a protected computer.
- Manage Veeam Agent installed on a protected computer:
  - Create Veeam Recovery Media for a protected computer.
  - Install Veeam Agent on a protected computer.
  - Upgrade Veeam Agent on a protected computer.
  - Install Veeam CBT driver on a protected computer.
  - Reboot a protected computer.
  - Uninstall Veeam Agent on a protected computer.
Moving Unmanaged Computer to Protection Group

You can quickly move an unmanaged Veeam Agent computer to a protection group in the Veeam Backup & Replication inventory. This allows you to start using Veeam Backup & Replication to manage Veeam Agent that is already set up to create backups in the Veeam backup repository.

You can move a computer from the Unmanaged protection group to a new protection group or protection group that you have already created.

- When you move an unmanaged computer to a new protection group, Veeam Backup & Replication creates the protection group and adds the computer to this group. In the protection group settings, you can define discovery and deployment options according to which Veeam Backup & Replication will process the added computer.
- When you move an unmanaged computer to an already existing protection group, Veeam Backup & Replication adds this computer to the protection group and starts processing the computer according to discovery and deployment settings defined in the properties of the protection group. Veeam Backup & Replication discovers the added computer, checks whether Veeam Agent running on the computer needs upgrade and upgrades Veeam Agent if needed.

NOTE:

Mind the following:

- You can move an unmanaged computer only to a protection group that includes individual computers.
- After you move a computer to a protection group, data backup for this computer will be performed by a backup job configured in Veeam Backup & Replication. Veeam Agent running on the computer will start a new backup chain on a target location specified in the backup job settings. The original backup job configured on the Veeam Agent computer will be removed in Veeam Agent, and you will not be able to continue the backup chain created with this job.
- You cannot map a Veeam Agent backup job configured in Veeam Backup & Replication to a backup chain that was created on a backup repository by Veeam Agent operating in the standalone mode.

To move an unmanaged computer to a new protection group:

1. Open the Inventory view.
2. In the inventory pane, expand the Physical Infrastructure node and select the Unmanaged node.
3. In the working area, select the necessary computer and click Move to > New protection group on the ribbon or right click the computer and select Move to > New protection group.
To move an unmanaged computer to a protection group that is already created in the inventory:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the **Unmanaged** node.
3. In the working area, select the necessary computer and click **Move to > name of the protection group** on the ribbon or right click the computer and select **Move to > name of the protection group**.
Adding Computer to Backup Job

You can quickly add a specific protected computer to a Veeam Agent backup job that you have configured in Veeam Backup & Replication. To do this, do the following:

1. Open the **Inventory** view.
2. In the inventory pane, in the **Physical Infrastructure** node, select a protection group whose computers you want to add to a Veeam Agent backup job and do one of the following:
   - In the working area, select the computer that you want to add to the job and click **Add to Backup > name of the job** on the ribbon.
   - In the working area, right-click the computer that you want to add to the job and select **Add to backup job > name of the job**.

**NOTE:**

Consider the following:

- You can add a computer to a Veeam Agent backup job configured for computers of the same platform. For example, you can add a Linux computer only to a Veeam Agent backup job for Linux computers.
- You can also add a specific protected computer to a new backup job. To learn more, see [Creating Veeam Agent Backup Jobs](#).
Performing Quick Backup

You can create an ad-hoc incremental backup for one or more protected computers — 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 computers in the Veeam Agent backup job and do not want to configure a new job or modify the existing one.

Quick backup can be performed for computers that meet the following requirements:

- A protected computer is added to a Veeam Agent backup job managed by the backup server.
- A full backup file for the protected computer exists on the backup repository configured in the backup infrastructure.

To perform quick backup:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the protected computer that you want to back up.
3. In the working area, select one or more computers and click **Quick Backup** on the ribbon or right-click the computers and select **Quick backup**.

Veeam Backup & Replication will trigger a Veeam Agent backup job to create a new incremental restore point for selected computers. Details of a running quick backup task are displayed in the job session window.

**NOTE:**

If a computer for which you want to perform quick backup is added to more than one Veeam Agent backup job, Veeam Backup & Replication will trigger only the job that created the latest restore point for this computer.
Viewing Properties

You can view detailed information about protected computers. The detailed information provides the following data:

- Host name
- IP address
- Fingerprint (for computers running a Linux OS)
- Key algorithm (for computers running a Linux OS)
- Operating system
- Veeam Agent version
- CBT driver version (for computers running a Microsoft Windows Server OS)

To view detailed information about a protected computer:

1. Open the Inventory view.
2. In the inventory pane, expand the Physical Infrastructure node.
3. In the working area, select the computer and click Details on the ribbon or right-click the computer and select Details.
Rescanning Protected Computer

You can rescan protected computers added to the inventory. The rescan operation may be required, for example, if you want to refresh information about the protected computer in the Veeam Backup & Replication database. During the rescan operation, Veeam Backup & Replication communicates to Veeam Installer Service running on the protected computer, retrieves information about the computer and stores this information to the configuration database.

To rescan a protected computer:

1. Open the Inventory view.
2. In the inventory pane, expand the Physical Infrastructure node and select the necessary protection group.
3. In the working area, select the computer and click Rescan on the ribbon or right-click the computer and select Rescan.
Creating Veeam Recovery Media

You can use the backup console to create a Veeam Recovery Media for a Veeam Agent computer that you manage in Veeam Backup & Replication. The process of creating a Veeam Recovery Media in Veeam Backup & Replication practically does not differ from the same procedure performed on a Veeam Agent computer.

To learn more about the Veeam Recovery Media, see the Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.

Before You Begin

You can create a Veeam Recovery Media for a protected computer in Veeam Backup & Replication if the following conditions are met:

- A protected computer runs a Microsoft Windows OS.
- A full backup file of one of the following backup types was created for the protected computer on the target location by a Veeam Agent backup job:
  - Entire computer backup
  - Volume-level backup of the computer OS data (created with the Operating system option selected in the backup job settings) or computer system volume
  - File-level backup of the computer OS data created with the Operating system option selected in the backup job settings

NOTE:

By default, you cannot create a Veeam Recovery Media for a failover cluster with Cluster Shared Volumes (CSV). You can enable creation of a Veeam Recovery Media for such clusters with a registry key. For more information, contact Veeam Customer Support.

Removable Storage Device Scenario (USB, SD Card and Other)

- The removable storage device must be inserted into a corresponding slot on the computer or connected to the computer.
- The removable storage device must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- During the recovery image creation, Veeam Agent for Microsoft Windows formats the removable storage device. If you have important information on the device, create a copy of this data in some other location.

CD/DVD/BD Scenario

- An empty or re-writable CD/DVD/BD must be inserted into a CD/DVD/BD drive on the computer.
- The CD/DVD/BD must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- [For RW CD/DVD/BD] During the recovery image creation, Veeam Agent for Microsoft Windows erases information on the CD/DVD/BD. If you have important information on the CD/DVD/BD, create a copy of this data in some other location.
Step 1. Launch Create Recovery Media Wizard

To launch the **Create Recovery Media** wizard:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the necessary protected computer.
3. In the working area, select the computer and click **Recovery Media** on the ribbon or right-click the computer and select **Agent > Create recovery media**.

**TIP:**

You can also launch the **Create Recovery Media** wizard from the **Backups** node in the **Home** view of the Veeam backup console. To learn more, see **Creating Recovery Media from Backup**.
Step 2. Specify Recovery Media Options

At the **Recovery Media** step of the wizard, in the **Available bootable media types** list, specify on which type of media you want to create a recovery image. You can create the following types of recovery images:

- Recovery image on a removable storage device. You can create a recovery image on a USB drive, SD card and so on. Veeam Backup & Replication displays all removable storage devices currently attached to the backup server. Select the necessary one in the list.

- Recovery image on an optical disk. You can create a recovery image on a CD, DVD or BD. Veeam Backup & Replication displays all CD, DVD and BD drives available on the backup server. Select the necessary one in the list.

- ISO file with the recovery image. You can create a recovery image in the ISO file format and save the resulting file locally on the backup server.

**NOTE:**

When you create a recovery image from the Veeam backup console, you cannot specify additional recovery media options in the same way as when you create a recovery image on the Veeam Agent computer. In this scenario, the recovery image is created with default settings: Veeam Backup & Replication includes network connection settings and hardware drivers installed on the Veeam Agent computer in the recovery image.
Step 3. Specify Path to ISO

The **Image Path** step of the wizard is available if you have selected to create an ISO file with the recovery image.

In the **Specify folder to create recovery media image in** field, specify a real path to the folder where you want to save the created recovery image, and the ISO file name. When you create Veeam Recovery Media using the Veeam Backup & Replication console, you can save the ISO file on the local drive of the Veeam backup server only. Thus, the recovery image will always be available should Veeam Agent computer volumes get corrupted or the computer fail to start.

![Create Recovery Media dialog](image)
Step 4. Review Recovery Image Settings

At the **Ready to Apply** step of the wizard, review settings of the recovery image that you plan to create and click **Create**.

Veeam Backup & Replication will collect data necessary for recovery image creation and write the resulting recovery image to the specified target.
Step 5. Finish Working with Wizard

The process of recovery image creation may take some time. Wait for the process to complete and click **Finish** to exit the wizard.

If you want to interrupt the process of recovery image creation, click **Cancel** or close the wizard window.

![Create Recovery Media](image)

What You Do Next

[For ISO file] After the recovery image is created, you can burn the created ISO file to a CD/DVD/BD. To do this, you can use native Microsoft Windows tools or third-party software.
Installing Veeam Agent

You can install Veeam Agent on a specific protected computer in the inventory. This operation may be required, for example, if you want to test the installation process before allowing Veeam Backup & Replication to deploy Veeam Agent to all computers included in the protection group.

Before you install Veeam Agent, check the following prerequisites:

- The protected computer must be powered on and able to be connected over the network.
- The required version of Veeam Agent must be available on the distribution server.

To install Veeam Agent on a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Install Agent** on the ribbon or right-click the computer and select **Agent > Install backup agent**.
Upgrading Veeam Agent

You can upgrade Veeam Agent running on a specific protected computer. This operation may be required, for example, if you did not allow Veeam Backup & Replication to automatically upgrade Veeam Agent on computers included in the protection group and want to test the upgrade process on a selected computer first.

Before you upgrade Veeam Agent, check the following prerequisites:

- The protected computer must be powered on and able to be connected over the network.
- The required version of Veeam Agent must be available on the distribution server.

**TIP:**

During the protected computers discovery process, Veeam Backup & Replication checks the version of Veeam Agent running on a protected computer and the version of Veeam Agent available on the distribution server. If a newer version of Veeam Agent becomes available on the distribution server, and automatic upgrade of Veeam Agent is disabled for a protection group, Veeam Backup & Replication puts a computer to the *Upgrade required* state.

In addition, Veeam Backup & Replication includes computers that require upgrade of Veeam Agent in the *Out of Date* protection group. You can upgrade Veeam Agent on all computers that require upgrade at once. To learn more, see Upgrading Veeam Agent on Multiple Computers.

To upgrade Veeam Agent on a protected computer:

1. Open the *Inventory* view.
2. In the inventory pane, expand the *Physical Infrastructure* node and select the necessary protection group.
3. In the working area, select the necessary computer and click *Upgrade* on the ribbon or right-click the computer and select *Agent* > *Upgrade*. 
Upgrading Veeam Agent on Multiple Computers

You can upgrade Veeam Agent on all computers that require upgrade at once. To upgrade Veeam Agent on protected computers:

1. Open the **Inventory** view.

2. In the inventory pane, in the **Physical Infrastructure** node, select the **Out of Date** protection group and click **Upgrade** on the ribbon or right-click the **Out of Date** protection group and select **Upgrade**.
Installing Veeam CBT Driver

You can use the Veeam Backup & Replication console to quickly install the Veeam changed block tracking (CBT) driver on a protected computer. This operation may be required, for example, if you want to evaluate driver performance on a selected computer rather than deploy driver to all computers in the protection group at once.

Before you install the Veeam CBT driver, check the following prerequisites:

- The protected computer on which you want to install the driver must run a Microsoft Windows Server OS.
- The protected computer on which you want to install the driver must be powered on and able to be connected over the network.

**IMPORTANT!**

Prior to installing the Veeam CBT driver on a computer that runs Microsoft Windows Server 2008 R2, make sure that update KB3033929 is installed in the OS. To learn more, see this Microsoft KB article.

The update adds SHA-2 code signing support for Microsoft Windows 7 and Microsoft Windows Server 2008 R2 that is required for verification of the Veeam CBT driver signature. Without this update installed, the OS running on a protected computer will fail to boot after you install the Veeam CBT driver.

To install the Veeam CBT driver on a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the computer on which you want to install the driver.
3. In the working area, select the necessary computer and click **Install Driver** on the ribbon or right-click the computer and select **Agent > Install driver**.
NOTE:
To enable the CBT driver after installation, you need to reboot the computer. To learn more, see Rebooting Protected Computer.

Uninstalling Veeam CBT Driver

You can uninstall the Veeam CBT driver at any time you need. To uninstall the driver:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the computer on which you want to uninstall the driver.
3. In the working area, select the necessary computer and click **Uninstall Driver** on the ribbon or right-click the computer and select **Agent > Uninstall driver**.

NOTE:
To complete the driver uninstallation process, you need to reboot the computer. To learn more, see Rebooting Protected Computer.
Rebooting Protected Computer

You can use the Veeam Backup & Replication console to reboot a protected computer. This operation may be required, for example, if you have installed the CBT driver on a selected computer and need to reboot this computer to finish the installation process and enable the driver.

To reboot a protected computer:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select a protection group that contains the computer that requires reboot. The computer that requires reboot is displayed in the Reboot required status in the Veeam Backup & Replication console.
3. In the working area, select the necessary computer and click **Reboot** on the ribbon or right-click the computer and select **Agent > Reboot**.
4. In the displayed window, click **Yes**.

**TIP:**

You can also reboot a computer with a different status than the Reboot required status. To do this, press and hold the [CTRL] key, right-click the necessary computer and select **Agent > Reboot**.
Uninstalling Veeam Agent

You can remove Veeam Agent from a specific protected computer, for example, if you want to reinstall Veeam Agent running on the protected computer. When you remove Veeam Agent from a protected computer, Veeam Backup & Replication also removes the Veeam Installer Service from this computer.

To uninstall Veeam Agent:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the necessary protection group.
3. In the working area, select the necessary computer and click **Uninstall All Components** on the ribbon or right-click the computer and select **Agent > Uninstall all components**.
4. In the displayed notification window, click **Yes**.

**NOTE:**

Mind the following:

- If automatic installation of Veeam Agent is enabled in the protection group settings, after you remove Veeam Agent from a selected computer, Veeam Backup & Replication will install Veeam Agent on this computer during the next rescan job session started by schedule.
- Prerequisite components installed and used by Veeam Agent are not removed during the uninstall process. To remove the remaining components, use the Microsoft Windows Control Panel on the computer from which you uninstalled Veeam Agent.
Removing Computer from Protection Group

You can remove one or more computers from a protection group, for example, if you do not want to protect these computers with Veeam Agent any longer but want to back up data of other computers in the protection group.

When you remove a computer from a protection group, Veeam Backup & Replication removes records about the computer from the Veeam backup console and configuration database but does not uninstall Veeam Agent from the computer. You can remove Veeam Agent from the computer in advance, before you remove the computer from the protection group. To learn more, see Uninstalling Veeam Agent.

Alternatively, you can remove a computer from a protection group, and then uninstall Veeam Agent from this computer. Note that in this case you will have to uninstall Veeam Agent using the Microsoft Windows control panel directly on the Veeam Agent computer.

**TIP:**

You can also remove entire protection groups from the Veeam Backup & Replication inventory. When you remove a protection group, you can instruct Veeam Backup & Replication to uninstall Veeam Agents from all protected computers included in this protection group. To learn more, see Removing Protection Group.

The process of removing a computer from a protection group differs depending on the type of the protection group that contains the computer you want to remove.

- For a protection group that contains individual computers, edit the protection group and remove the necessary computer at the Computers step of the Edit Protection Group wizard. To learn more, see Editing Protection Group Settings.
  
  You can also use this option to remove a computer from the Manually Added protection group. This protection group contains computers that you add directly to a Veeam Agent backup job. To learn more, see Removing Computer from "Manually Added" Protection Group.

- For a protection group that contains Active Directory objects, edit the protection group and remove the necessary computer account at the Active Directory step of the Edit Protection Group wizard.
  
  Alternatively, if the protection group contains a container, organization unit, group or entire domain, you can exclude the computer at the Exclusions step of the wizard. To learn more, see Exclude Objects from Protection Group.

- For a protection group that contains computers listed in a CSV file, remove the record about the necessary computer from the CSV file. During subsequent rescan of the protection group, Veeam Backup & Replication will remove the computer from the protection group.

Backups created for computers that were removed from a protection group remain intact in the backup location. You can delete this backup data manually later if needed.
Removing Computer from "Manually Added" Protection Group

Individual computers that you add directly to a Veeam Agent backup job are included in the Manually Added protection group. When you remove such a computer from the backup job, Veeam Backup & Replication does not remove the computer from the Manually Added protection group as well. The computer remains in the Manually Added protection group until you remove the computer from this protection group.

To remove a computer from the Manually Added protection group, you must edit this protection group and remove the computer at the Computers step of the Edit Protection Group wizard. To learn more, see Editing Protection Group Settings.

**NOTE:**

You cannot remove a computer from the Manually Added protection group if this computer is added to a Veeam Agent backup job.
Restoring Data from Veeam Agent Backups

You can recover data from backups created by Veeam Agent backup jobs configured in Veeam Backup & Replication. For data restore with the Veeam backup console, you can use Veeam Agent backups created on a Veeam backup repository. If you specified a local drive or network shared folder as a target for Veeam Agent backups, you need to restore data from such backups using Veeam Agent UI on a protected computer.

You can perform the following data restore tasks with Veeam Agent backups in Veeam Backup & Replication:

- Restore a Veeam Agent backup to a vSphere VM.
- Restore a Veeam Agent backup to a Hyper-V VM (for backups of Microsoft Windows machines only).
- Restore data from a Veeam Agent backup to Microsoft Azure.
- Restore data from a Veeam Agent backup to Amazon EC2.
- Restore computer volumes from a Veeam Agent backup.
- Restore individual files and folders from a Veeam Agent backup.
- Restore application items from a Veeam Agent backup with Veeam Explorers.
- Export computer disks as VMDK, VHD or VHDX disks.
- Export a specific restore point in a Veeam Agent backup to a full backup (VBK) file.

Restoring Data with Veeam Recovery Media

In addition to data restore tasks available in the Veeam backup console, you can also recover data on a Veeam Agent computer using the Veeam Recovery Media. To do this, you must have a backup of the computer whose data you want to restore and the Veeam Recovery media created for this computer.

- For a Microsoft Windows computer, you can create the Veeam Recovery Media with the Veeam backup console. To learn more, see Creating Veeam Recovery Media.
- For a Linux computer, you can download the Veeam Recovery Media from the Veeam website or create a custom Veeam Recovery Media. To learn more, see the Veeam Recovery Media section in the Veeam Agent for Linux User Guide.

The process of data restore with the Veeam Recovery Media in the Veeam Agent management scenario does not differ from the same process on a computer that runs Veeam Agent operating in the standalone mode.

- For information on data restore with the Veeam Recovery Media on a Microsoft Windows computer, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.
- For information on data restore with the Veeam Recovery Media on a Linux computer, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Linux User Guide.
Restoring Veeam Agent Backup to vSphere VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a VMware vSphere VM in your virtualization environment. For instant recovery to a vSphere VM, you can use backups of Microsoft Windows and Linux machines created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

The procedure of instant recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more about instant VM recovery, see the Instant VM Recovery section in the Veeam Backup & Replication User Guide.
Restoring Veeam Agent Backup to Hyper-V VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment. For instant recovery to a Hyper-V VM, you can use backups of Microsoft Windows machines created on the Veeam backup repository. You cannot use backups of Linux machines and backups created on the Veeam Cloud Connect repository for this operation.

The procedure of instant recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from instant VM recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more about instant VM recovery, see the Instant VM Recovery section in the Veeam Backup & Replication User Guide.
Restoring to Microsoft Azure

You can restore machines from Veeam Agent backups to Microsoft Azure. For restore to Microsoft Azure, you can use backups of Microsoft Windows and Linux machines created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

The procedure of restore to Microsoft Azure from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Microsoft Azure, see the Restore to Microsoft Azure section in the Veeam Backup & Replication User Guide.
Restoring to Amazon EC2

You can restore machines from Veeam Agent backups to Amazon EC2. For restore to Amazon EC2, you can use backups of Microsoft Windows and Linux machines created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

The procedure of restore to Amazon EC2 from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Amazon EC2, see the Restore to Amazon EC2 section in the Veeam Backup & Replication User Guide.
Restoring Volumes

You can use Veeam Backup & Replication to restore a specific computer volume or all volumes from a volume-level backup created with Veeam Agent for Microsoft Windows.

If data on a computer volume gets corrupted, you can restore this volume from the backup. For volume-level restore, you can use backups that were created at the volume level. File-level backups cannot be used for volume restore.

When you perform volume-level restore, Veeam Backup & Replication restores the entire content of the volume. It retrieves from the backup data blocks pertaining to a specific volume and copies them to the necessary location.

Note that you cannot browse the volume in the backup and select individual application items, files and folders for restore. For granular file-level restore, you can use the File-Level Restore option.

A volume can be restored to its original location or new location. If you restore the volume to its original location, Veeam Backup & Replication overwrites data on the original volume. If you restore the volume to a new location, and the target disk contains any data, Veeam Backup & Replication overwrites data in the target location with data retrieved from the backup.

A volume can be restored to a new location that has greater or less space than the size of the volume in the backup. Depending on the amount of free disk space on target location, you can select either to shrink or to extend the volume during restore. To learn more, see the Volume Resize section in the Veeam Agent for Microsoft Windows User Guide.

Before You Begin

Before you begin the volume-level restore process, check the following prerequisites:

- The volume-level backup from which you plan to restore data must be successfully created at least once.
- A computer on which you want to restore a volume must be added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows operating in the managed mode.

Volume-level restore has the following limitations:

- You can restore volumes only from backups created with Veeam Agent for Microsoft Windows.
- You cannot restore a system volume to a system volume of the original Veeam Agent computer or another computer.
- You cannot restore a volume to a volume on which the Microsoft Windows swap file is hosted.
Step 1. Launch Volume Level Restore Wizard

To launch the **Volume Level Restore** wizard, do either of the following:

- Open the **Home** tab and click **Restore > Agent > Volume restore > Volume restore**. In this case, you will be able to select a backup of the necessary Veeam Agent computer at the **Backup** step of the wizard.

- Open the **Home** view. In the inventory pane, click the **Backups** node. In the working area, expand the necessary Veeam Agent backup, select the necessary computer in the backup and click **Restore Volumes** on the ribbon or right-click the computer and select **Volume restore**.

  In this case, you will pass immediately to the **Restore Point** step of the wizard.
Step 2. Select Backup

At the **Backup** step of the wizard, select a backup from which you want to recover data.

To quickly find the necessary backup, use the search field at the bottom of the window: enter a backup name or a part of it in the search field and click the **Start search** button on the right or press **[ENTER]**.

In the list of backups, Veeam Backup & Replication displays only volume-level backups created with Veeam Agent for Microsoft Windows. File-level backups and backup created with Veeam Agent for Linux are not displayed.
Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

By default, Veeam Backup & Replication uses the latest restore point. However, you can select any valid restore point to recover volumes to a specific point in time.

Veeam Backup & Replication displays restore points for volume-level backups only. For example, if you have run 3 job sessions to create a backup of all computer volumes and then changed the backup scope to file-level backup, Veeam Backup & Replication will display only 3 restore points in the list.

Veeam Backup & Replication displays restore points for volume-level backups only. For example, if you have run 3 job sessions to create a backup of all computer volumes and then changed the backup scope to file-level backup, Veeam Backup & Replication will display only 3 restore points in the list.

Step 4. Map Restored Disks

At the **Disk Mapping** step of the wizard, select what volumes you want to restore and map volumes from the backup to volumes on the target computer.

**IMPORTANT!**

It is strongly recommended that you change disk mapping settings only if you have experience in working with Microsoft Windows disks and partitions. If you make a mistake, your computer data may get corrupted.
To select volumes for restore:

1. In the **Destination hosts** field, specify the target computer where you want to restore volumes. By default, Veeam Backup & Replication restores volumes to their original location. If you want to restore volumes from the backup to another computer, click **Choose** and select the necessary computer. You can restore volumes only to computers that are added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows.

2. In the **Disk mapping** section, select check boxes next to volumes that you want to restore from the backup. By default, Veeam Backup & Replication restores volumes to their initial location and maps the restored volumes automatically. If the initial location is unavailable, a volume is restored to a disk of the same or larger size. If you want to map the restored volume to another computer disk, at the bottom of the wizard click **Customize disk mapping**.

**NOTE:**

If Veeam Backup & Replication cannot map a volume automatically, Veeam Backup & Replication will prompt you to perform disk mapping manually. To proceed to the **Disk Mapping** window, click **Yes**.

3. At the **Disk Mapping** window, specify how volumes must be restored:
   - Right-click the target disk on the left and select the necessary disk layout:
     - **Apply Backup Layout** — select this option if you want to apply to disk the settings that were used on your computer at the moment when you performed backup.
     - **Apply Disk Layout** — select this option if you want to apply to the current disk settings of another disk.
     - **Erase** — select this option if you want to discard the current disk settings.
- Right-click unallocated disk space in the disk area on the right and select what volume from the backup you want to place on this computer disk.

If you want to change disk layout configured by Veeam Backup & Replication, right-click an automatically mapped volume and select **Remove**. You will be able to use the released space for mapping volumes in your own order.

4. **[For restore with volume resize]** You can resize a volume mapped by Veeam Backup & Replication to a target computer disk. To resize a volume, right-click it in the **Disk Mapping** window and select **Resize**. With this option selected, you will pass to the **Volume Resize** window.

**NOTE:**

If you map a backup volume that is larger than the amount of available space on the target disk, Veeam Backup & Replication will prompt you to shrink the restored volume. After you agree and click **OK**, Veeam Backup & Replication will prepare to shrink the volume to the size of available disk space.
Step 5. Resize Restored Volumes

At the Disk Mapping step of the wizard you can set the necessary size for the restored volumes. You can resize a volume if you have chosen to restore data in the Manual mode and customize disk layout. A volume will be shrunk or extended to the specified size during the process of data restore.

NOTE:

By default, Veeam Agent for Microsoft Windows displays volume size in megabytes (MB). This allows you to specify the desired size for the volume precisely. You can also choose to display volume size in gigabytes (GB). This may be helpful when you need to resize volumes on larger computer disks and want to simplify disk size calculations.

When you use GB as a volume size unit, you can specify volume size with integral numbers, for example, 1 GB, 60 GB or 200 GB, but not 0,8 GB, 60,5 GB or 200,7 GB. However, if the maximum volume size is in fact greater than the displayed value for less than 1 GB, Veeam Agent for Microsoft Windows will automatically add the exceeding amount of disk space to the extended volume. For example, if the maximum volume size is 60,2 GB, Veeam Agent for Microsoft Windows will display this size as 60 GB. When you specify 60 GB as a desired volume size, Veeam Agent for Microsoft Windows will extend the volume to 60,2 GB.

To resize a volume:

1. Specify a volume you want to resize:
   a. Right-click a restored volume mapped to a target disk and select Resize.
   b. [For volume shrink] Right-click unallocated disk space and select what volume from the backup you want to place on the computer disk. If the selected volume is larger than the amount of unallocated disk space, Veeam Backup & Replication will prompt you to shrink the restored volume.

2. In the Volume Resize window, select the volume size unit and specify the desired size for the restored volume.

![Volume Resize window]

- Size in: MB
- Current volume size: 61437 MB
- Maximum volume size: 61438 MB
- Minimum volume size: 3122 MB
- Desired volume size: 51200 MB

⚠️ You cannot shrink a volume beyond the point where any unmovable files are.

OK | Cancel
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 volume data with antivirus software before restoring the volume. To learn more about secure restore, see the **Secure Restore** section in the Veeam Backup & Replication User Guide.

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 the entire image** check box if you want the antivirus software to continue volume scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the **Viewing Antivirus Scan Results** section in the Veeam Backup & Replication User Guide.

![Volume Restore](image_url)
Step 7. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the computer volume.

**TIP:**

If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.
Step 8. Complete Restore Process

At the **Summary** step of the wizard, complete the procedure of volume-level restore.

1. Review settings of the restore process.

2. Click **Finish** to start the recovery process. Veeam Backup & Replication will perform partition re-allocation operations if necessary, restore the necessary volume data from the backup and overwrite volume data on the target computer with the restored data.

![Volume Restore Wizard](image_url)
Restoring Files and Folders

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups. The procedure of file-level restore from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. The difference is that you select a Veeam Agent backup instead of a VM backup in the File Level Restore wizard. To learn more, see the Guest OS File Recovery section in the Veeam Backup & Replication User Guide.

**NOTE:**

To restore files and folders from a backup of a Linux machine, you must have a VMware vSphere or Microsoft Hyper-V virtualization host added to the Veeam backup infrastructure. When you start the file-level restore procedure, Veeam Backup & Replication will use this host to deploy a helper appliance — a helper VM required to mount Linux machine disks from the backup. To learn more about adding a virtualization server, see Adding VMware vSphere Servers and Adding Microsoft Hyper-V Servers.

It is recommended that you add a vCenter Server and not a standalone ESXi host in the Veeam backup console. If Veeam Backup & Replication is set up to deploy a helper appliance on a standalone ESXi host, after Veeam Backup & Replication removes the helper appliance, the helper VM will be displayed in vCenter as orphaned.
Restoring Application Items

You can use Veeam Explorers to restore application items from Veeam Agent backups. Veeam Backup & Replication lets you restore items and objects from the following applications:

**From backups created with Veeam Agent for Microsoft Windows**

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Oracle

**From backups created with Veeam Agent for Linux**

- Oracle

The procedure of application-item restore from a Veeam Agent backup does not differ from the same procedure for a VM backup. To learn more, see the Restoring Application Items section in the Veeam Backup & Replication User Guide.
Exporting Disks

You can restore computer disks from volume-level backups and convert them to disks of the VMDK, VHD or VHDX format.

During disks 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 ESXi 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 computer disks, Veeam Backup & Replication will convert them to 2 virtual disks and store these disks in the specified location.

To restore disks 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 either of the following:

- Open the Home tab and click Restore > Agent > Volume restore > Export disk. In this case, you will be able to select a backup of the necessary Veeam Agent computer at the Backup step of the wizard.

- Open the Home view. In the inventory pane, click the Backups node. In the working area, expand the necessary Veeam Agent backup, select the necessary computer in the backup and click Export Disks on the ribbon or right-click a computer in the backup and select Export disk content as virtual disks.

In this case, you will pass immediately to the Restore Point step of the wizard.
**Step 2. Select Backup**

At the **Backup** step of the wizard, select a backup from which you want to restore disks. In the list of backups, Veeam Backup & Replication displays all backups that are currently hosted on the Veeam backup repository.

Make sure that you select a volume-level backup in the list.

<table>
<thead>
<tr>
<th>Job name</th>
<th>Last restore point</th>
<th>Objects</th>
<th>Restore points</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB Backup</td>
<td>10/15/2019 10:00:54 Pm</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>MySQL DB Backup</td>
<td>10/15/2019 10:01:22 Pm</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL DB Bac</td>
<td>10/16/2019 12:23:16 Am</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Server Backup</td>
<td>10/14/2019 5:00:01 PM</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Servers Backup to</td>
<td>10/15/2019 10:00:56 Pm</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Windows Servers B</td>
<td>10/15/2019 10:00:39 Pm</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>appsrv01.techloc</td>
<td>less than a day ago</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>filesrv03.techloc</td>
<td>less than a day ago</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Workstations Bac</td>
<td>10/15/2019 11:00:27 Pm</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select the necessary restore point from which you want to restore disks. In the list of points, Veeam Backup & Replication displays all restore points that have been created. Make sure that you select a restore point that relates to a volume-level backup.
**Step 4. Select Disks**

At the **Disks** step of the wizard, select check boxes next to those disks that you want to export.

**Step 5. Select Destination and Disk Format**

At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk.

1. From the **Server** list, select a server on which the resulting virtual disks must be saved. If you plan to save the disks in the VMDK format on a datastore, select an ESXi host to which this datastore is connected.

2. In the **Path** to folder field, specify a folder on the server or datastore where the virtual disks must be placed.

3. Select the export format for disks:
   - **VMDK** — select this option if you want to save the resulting virtual disk in the VMware VMDK format.
   - **VHD** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHD format.
   - **VHDX** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHDX format (supported by Microsoft Windows Server 2012 and later).
NOTE:
If you have selected to store the resulting virtual disk to a datastore, you will be able to save the virtual disk in the VMDK format only. Other options will be disabled.
Step 6. Specify Secure Restore Settings

The **Secure Restore** step of the wizard is available if you export disks from a Veeam Agent backup of a Microsoft Windows machine.

At this 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. To learn more about secure restore, see the **Secure Restore** section in the Veeam Backup & Replication User Guide.

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 the entire image** check box if you want the antivirus software to continue disk scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the **Viewing Antivirus Scan Results** section in the Veeam Backup & Replication User Guide.
Step 7. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the computer volume.

**TIP:**

If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.
Step 8. Complete Restore Process

At the Summary step of the wizard, complete the disk restore procedure.

1. Review details for the disk to be restored.
2. Click Finish to start the restore procedure and exit the wizard.
Exporting Restore Point to Full Backup File

You can restore data from a specific restore point in a Veeam Agent backup and export this data to a standalone full backup file. The procedure of Veeam Agent backup export does not differ from the same procedure for a VM. To learn more, see the Exporting Backups section in the Veeam Backup & Replication User Guide.
Managing Veeam Agent Backups

You can perform administration tasks with backups created on a Veeam backup repository by Veeam Agent backup jobs configured in Veeam Backup & Replication. For such Veeam Agent backups, Veeam Backup & Replication allows you to perform the same set of operations as for backups created with Veeam Agent backup jobs configured directly on a Veeam Agent computer. You can perform the following tasks:

- Create the Veeam Recovery Media for a computer in backup.
- Remove a Veeam Agent backup from configuration.
- Delete a Veeam Agent backup from disk.
- View properties of a Veeam Agent backup.
Creating Veeam Recovery Media from Backup

You can create the Veeam Recovery Media for a computer whose Veeam Agent backup resides on a Veeam backup repository. For this operation, you can use a backup created by any type of a Veeam Agent backup job: a backup job managed by the backup server or backup job managed by Veeam Agent (backup policy).

Creating the Veeam Recovery Media for a computer in a backup does not differ from creating the Veeam Recovery Media for a protected computer in the Veeam Backup & Replication inventory. To learn more, see Creating Veeam Recovery Media.

To create Veeam Recovery Media:

1. Open the Home view.
2. In the inventory pane, click Backups.
3. In the working area, expand the Veeam Agent backup, select the necessary computer in the backup and click Recovery Media on the ribbon or right-click the computer and select Create recovery media.
4. Complete the steps of the Create Recovery Media wizard.
Removing Backup from Configuration

If you want to remove records about Veeam Agent backups from the Veeam Backup & Replication console and configuration database, you can use the Remove from configuration operation. When you remove a Veeam Agent backup from configuration, the actual backup files remain on the backup repository. You can import the backup to the Veeam Backup & Replication at any time later and restore data from it.

NOTE:

Mind the following:

- You can use the Veeam Backup & Replication console to remove backups created by Veeam Agent backup jobs on the Veeam backup repository. Backups created on a local drive of a protected computer or in a network shared folder are not displayed in the Veeam backup console.
- The Remove from configuration operation is not available for backups created on the Veeam Cloud Connect repository.
- The Remove from configuration operation is not available for backups of failover clusters.

You can remove an entire backup related to a Veeam Agent backup job or remove specific child backups — backups related to individual computers in the backup.
To remove a Veeam Agent backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area select and remove the necessary backup:
   - To remove the entire backup related to the Veeam Agent backup job or policy, select the backup and click **Remove from > Configuration** on the ribbon or right-click the backup and select **Remove from configuration**.
   - To remove a backup of a specific computer in the Veeam Agent backup job or policy, expand the parent backup, select the necessary computer and click **Remove from > Configuration** on the ribbon or right-click the computer and select **Remove from configuration**.
Deleting Backup 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.

**NOTE:**

You can use the Veeam Backup & Replication console to remove backups created by Veeam Agent backup jobs on the Veeam backup repository. Backups created on a local drive of a protected computer or in a network shared folder are not displayed in the Veeam Backup & Replication console.

You can remove an entire backup related to a Veeam Agent backup job or remove specific child backups — backups related to individual computers in the backup.

To remove a Veeam Agent backup from the backup repository:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area select and remove the necessary backup:
   - To remove the entire backup related to the Veeam Agent backup job or policy, select the backup and click **Remove from > Disk** on the ribbon or right-click the backup and select **Delete from disk**.
   - To remove a backup of a specific computer in the Veeam Agent backup job or policy, expand the parent backup, select the necessary computer and click **Remove from > Disk** on the ribbon or right-click the computer and select **Delete from disk**.
Viewing Backup Properties

You can view summary information about backups created by Veeam Agent backup jobs on the backup repository. The summary information provides the following data:

- Backup location
- Available restore points
- Date of restore points creation
- Compression and deduplication ratios
- Data size and backup size

You can view summary information for the following types of Veeam Agent backups:

- Entire backup related to a Veeam Agent backup job (parent backup)
- Backup of a separate protected computer in the Veeam Agent backup job (child backup)

To view summary information for a parent backup:

1. Open the Home view.
2. In the inventory pane, select Backups.
3. In the working area, select the backup and click Properties on the ribbon or right-click the backup and select Properties.
To view summary information for a child backup (backup of a specific Veeam Agent computer):

1. Open the **Home** view.

2. In the inventory pane, select **Backups**.

3. In the working area, expand the parent backup, select the necessary child backup and click **Properties** on the ribbon or right-click the child backup and select **Properties**.

![Agent Backup Properties](image)
Reporting

You can view real-time statistics for rescan jobs, as well as Veeam Agent backup jobs and backup policies configured in Veeam Backup & Replication. You can also generate reports with statistics data for performed rescan job or backup job sessions. You can generate reports manually in the Veeam Backup & Replication console or set up Veeam Backup & Replication to send reports automatically by email.

Viewing Rescan Job Statistics

You can view statistics about performed rescan job sessions. When you create a protection group or manually start the discovery process for a protection group or individual protected computer, Veeam Backup & Replication displays statistics for the currently running rescan job session. In the statistics window, Veeam Backup & Replication displays session duration details and a list of operations performed during the job.

In addition to overall rescan job statistics, the statistics window provides information on each protected computer processed within the rescan job session. To view the processing progress for a specific computer, select it in the list on the left.

You can also view statistics for any performed rescan job session. To view rescan job statistics, do one of the following:

- Open the **Inventory** view. In the inventory pane, select the necessary protection group and click **Statistics** on the ribbon or right-click the protection group and select **Statistics**.

- Open the **History** view. In the inventory pane, select the **System** node. In the working area, select the necessary rescan job session and click **Statistics** on the ribbon or right-click the rescan job session and select **Statistics**.
Viewing Rescan Job Report

You can generate reports with details about rescan job sessions performed for a specific protection group. The report contains data on the latest rescan job session initiated for the job upon schedule. To generate a report:

1. Open the **Inventory** view.
2. In the inventory pane, select the necessary protection group and click **Report** on the ribbon or right-click the protection group and select **Report**.

The report contains the following data:

- Cumulative session statistics: details of the session performance, including the number of protected computers in the protection group and the number of newly discovered computers.
- Detailed statistics for every protected computer processed within the session: DNS name, IP address and operating system of the protected computer, list of warnings and errors (if any).

**TIP:**
You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see **Enabling Email Reporting**.

<table>
<thead>
<tr>
<th>Windows Servers</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned 2</td>
<td>2</td>
</tr>
<tr>
<td>Seen 2</td>
<td>0</td>
</tr>
<tr>
<td>Updated 2</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>IP address</th>
<th>Status</th>
<th>Operating System</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>appsv01.tech.local</td>
<td>172.24.30.120</td>
<td>Success</td>
<td>Microsoft Windows Server 2012 R2 (64-bit)</td>
<td>Backup agent has been installed.</td>
</tr>
<tr>
<td>filesv03.tech.local</td>
<td>172.24.30.121</td>
<td>Success</td>
<td>Microsoft Windows Server 2012 R2 (64-bit)</td>
<td>Backup agent has been installed.</td>
</tr>
</tbody>
</table>
Viewing Veeam Agent Backup Job Statistics

You can view statistics about Veeam Agent backup jobs configured in Veeam Backup & Replication. For Veeam Agent backup jobs managed by the backup server, Veeam Backup & Replication displays statistics in the similar way as for backup jobs for VM data backup. To learn more, see the Reporting section in the Veeam Backup & Replication User Guide.

To view Veeam Agent backup job statistics:

1. Open the Home view.
2. In the inventory pane, click the Jobs node.
3. In the working area, double-click the necessary Veeam Agent backup job. Alternatively, you can select the necessary Veeam Agent backup job and click Statistics on the ribbon or right-click the job and select Statistics.
Viewing Veeam Agent Backup Job Report

You can generate a report with details about Veeam Agent backup job session performance. The report contains data on the latest backup job session initiated for the job. To generate a report:

1. Open the Home view.
2. In the inventory pane, click the Jobs node.
3. In the working area, select the necessary job and click Report on the ribbon or right-click the job and select Report.

The report contains data on the latest 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 protected computer processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).

**TIP:**

You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.

### Agent Backup Job: Windows Servers Backup

<table>
<thead>
<tr>
<th>Success</th>
<th>Start Time</th>
<th>End Time</th>
<th>Total Size</th>
<th>Backup Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>12:04:39 AM</td>
<td>12:04:39 AM</td>
<td>89.2 GB</td>
<td>30.8 GB</td>
</tr>
<tr>
<td>Warning</td>
<td>12:40:42 AM</td>
<td>12:40:42 AM</td>
<td>43.6 GB</td>
<td>Dedupe 1.8x</td>
</tr>
<tr>
<td>Error</td>
<td>0:30:02</td>
<td>Transferred</td>
<td>30.8 GB</td>
<td>Compression 1.9x</td>
</tr>
</tbody>
</table>

#### Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Start Time</th>
<th>End Time</th>
<th>Size</th>
<th>Read</th>
<th>Transferred</th>
<th>Duration</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>appsvr01.technocal</td>
<td>Success</td>
<td>12:04:35 AM</td>
<td>12:04:24 AM</td>
<td>40.0 GB</td>
<td>20.5 GB</td>
<td>14.7 GB</td>
<td>00:35:28</td>
<td></td>
</tr>
<tr>
<td>Filesvr03.technocal</td>
<td>Success</td>
<td>12:05:01 AM</td>
<td>12:06:20 AM</td>
<td>40.0 GB</td>
<td>23.0 GB</td>
<td>15.2 GB</td>
<td>00:35:19</td>
<td></td>
</tr>
</tbody>
</table>
Viewing Backup Policy Statistics

You can view statistics about Veeam Agent backup jobs configured in Veeam Backup & Replication. For Veeam Agent backup jobs managed by Veeam Agent, or backup policies, Veeam Backup & Replication displays statistics in the following way:

- After you create a backup policy, Veeam Backup & Replication applies the backup policy to protected computers. In the policy statistics window, Veeam Backup & Replication displays information about policy application process and results. This information remains in the policy statistics window until the first Veeam Agent backup job session is performed on computers included in the backup policy.

- After the Veeam Agent backup job session statistics becomes available in Veeam Backup & Replication, this statistics appears in the policy statistics window. The job session statistics becomes available in Veeam Backup & Replication at a different time depending on what target for backup files is selected in the backup policy settings:
  - If a Veeam Agent backup job whose settings are defined by the backup policy creates backup files on a Veeam backup repository, backup job session statistics is available in Veeam Backup & Replication on real-time basis.
  - If a Veeam Agent backup job creates backup files on a local drive of a Veeam Agent computer, in a network shared folder or in a Veeam Cloud Connect repository, backup job session results are not passed to Veeam Backup & Replication in real time. Statistics for such backup sessions becomes available in Veeam Backup & Replication later, after rescan of a protection group that contains computers added to the backup policy. This process happens regularly upon the discovery schedule defined in the protection group settings.

- Veeam Backup & Replication regularly applies the backup policy to protected computers. This operation is performed during automatic rescan of a protection group that contains computers added to the backup policy. If the application process completes with a warning or an error, Veeam Backup & Replication displays information about the application process results in the policy statistics window. Information about successful application of the backup policy is not displayed in the statistics window between two backup sessions.

Veeam Backup & Replication displays statistics for backup policies in a different way than for Veeam Agent backup jobs managed by the backup server. The main differences are the following:

- For backup policies, Veeam Backup & Replication does not display the job progress bar. You can monitor backup progress only for individual machines in the backup policy.

- Detailed statistics include the number of Veeam Agent computers specified in the backup policy settings, the number of computers to which settings of the backup policy are applied, and the number of computers that have no connection to the backup server at the time when the Veeam Agent backup job is performed.

- You can use the Errors, Warnings and/or Success buttons at the bottom of the job statistics window to view details on operations that failed, completed with a warning or completed successfully during a Veeam Agent job session performance.

TIP:

In addition to backup policy statistics, Veeam Backup & Replication displays individual backup session statistics for each computer in the backup policy. You can view these statistics in the Last 24 Hours node of the Home view and in the History view of the Veeam backup console.
To view Veeam Agent backup policy statistics:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, double-click the necessary Veeam Agent backup policy. Alternatively, you can select the necessary Veeam Agent backup policy and click **Statistics** on the ribbon or right-click the backup policy and select **Statistics**.
Viewing Backup Policy Report

You can generate a report with details about Veeam Agent backup job sessions performed on protected computers added to a backup policy. The report contains data on the latest backup job session initiated for the backup policy. To generate a report:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary backup policy and click **Report** on the ribbon or right-click the backup policy and select **Report**.

The report contains data on the latest job session:

- Cumulative session statistics: details on the number of protected computers specified in the backup policy settings, the number of computers to which settings of the backup policy are applied, and the number of disconnected computers, details of the session performance, amount of read, processed and transferred data.
- Detailed statistics for every protected computer processed within the session: processing duration details, backup data size, amount of read and transferred data, list of warnings and errors (if any).

**TIP:**

You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see **Enabling Email Reporting.**

<table>
<thead>
<tr>
<th>Workstations Backup to Cloud</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 of 2 hosts processed</td>
<td>2</td>
</tr>
</tbody>
</table>

| Assigned | Processed | 62 GB | Success | 2 |
| Configured | Read | 3.5 GB | Warnings | 0 |
| Disconnected | Transferred | 2 GB | Errors | 0 |

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>desktop03.local</td>
</tr>
<tr>
<td>win01.local</td>
</tr>
</tbody>
</table>
Enabling Email Reporting

You can set up Veeam Backup & Replication to send reports automatically by email. To do this, you must enable and configure global email notification settings in Veeam Backup & Replication. To learn more, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.

In addition, you can enable and configure custom notification settings for a specific protection group, Veeam Agent backup job or backup policy. This may be useful if you want to change subject, notification rules or list of recipients for some reports.

Rescan Job Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends rescan job reports at 10:00 PM daily. Veeam Backup & Replication sends a separate report for every protection group that you configured. The report contains cumulative statistics for rescan job sessions performed within the last 24-hour period.

You can specify custom notification settings for a specific protection group. To learn more, see Notification Settings.

Veeam Agent Backup Job Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends an email notification after every backup job session completes.

You can specify custom notification settings for a specific Veeam Agent backup job. To learn more, see the following sections:

- Notification Settings for Veeam Agent Backup Job (for Microsoft Windows computers)
- Notification Settings for Veeam Agent Backup Job (for Linux computers)

Backup Policy Report

By default, after you enable and configure global email notification settings in Veeam Backup & Replication, Veeam Backup & Replication sends backup policy reports at 10:00 AM daily. Veeam Backup & Replication sends a separate report for every backup policy that you configured. The report contains cumulative statistics for backup job sessions performed for the last 24-hour period on computers to which the backup policy is applied.

You can specify custom notification settings for a specific backup policy. To learn more, see the following sections:

- Notification Settings for Backup Policy (for Microsoft Windows computers)
- Notification Settings for Backup Policy (for Linux computers)
Appendix A. Deploying Hotfix on Protected Linux Computers

This scenario describes how to deploy a hotfix on protected computers with installed Veeam Agent for Linux. A hotfix for Veeam Agent for Linux is a set of updated Veeam Agent packages that addresses a certain issue in the product. Veeam Software issues a hotfix in one of the following cases:

- To mitigate an existing issue in the product. In this case, a hotfix is provided by Veeam Customer Support.
- To add support of a new distribution version to the product. In this case, a hotfix is available in the Veeam software repository.

If you have several Veeam Agent for Linux installations managed by Veeam Backup & Replication, you can centrally deploy a hotfix on all managed agents using the distribution server.
Prerequisites

Before you deploy a Veeam Agent hotfix on protected Linux computers:

- Check that protected computers are powered on and can be connected over the network.
- Check the dedicated distribution server settings. Distribution server is used for deployment Veeam Agent setup files to protected computers. To learn more, see Distribution Server.

Each protection group can have a different distribution server. To check the distribution server settings of the protection group:

a. Open the **Inventory** view.

b. In the inventory pane, expand the **Physical Infrastructure** node.

c. In the inventory pane, select the protection group that contains computers with an outdated Veeam Agent installed and click **Edit Group** on the ribbon or right-click the protection group that you want to edit and select **Properties**.
d. At the **Options** step of the wizard, in the **Deployment** section, check what distribution server is selected for the protection group.

To automatically deploy hotfix on all Veeam Agent computers, make sure that the **Install backup agent automatically** and **Auto-update backup agent** check boxes are selected.

### Deployment Procedure

To deploy a hotfix on protected Linux computers included in the protection group, perform the following steps:

1. Obtain Veeam Agent for Linux packages from Veeam Customer Support or download packages from the Veeam software repository.

2. Save Veeam Agent for Linux packages to the following folder on the distribution server:
   - **For 32-bit CentOS / RHEL / Fedora / openSUSE / SLES**
     
     C:\Program Files\Veeam\Veeam Distribution Service\Fixes\val\x86\rpm
   
   - **For 64-bit CentOS / RHEL / Fedora / openSUSE / SLES**
     
     C:\Program Files\Veeam\Veeam Distribution Service\Fixes\val\x64\rpm
3. Rescan the protection group:
   a. Open the **Inventory** view.
   b. In the inventory pane, expand the **Physical Infrastructure** node.
   c. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.