Veeam Backup & Replication

Version 12

Veeam Agent Management Guide

March, 2023

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

Contents

Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

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

About This Document

This guide describes how to use Veeam Backup & Replication to deploy and manage Veeam Agents. 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 12 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 and Veeam Agents you need.

Related Documentation

The document should be regarded as a supplement to existing technical documentation for the following products:

- Veeam Backup & Replication
- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for IBM AIX
- Veeam Agent for Oracle Solaris
- Veeam Agent for Mac

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 the following Veeam Agents on computers in your infrastructure:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for IBM AIX
- Veeam Agent for Oracle Solaris
- Veeam Agent for Mac

You do not need to install, set up and operate Veeam Agent on every computer 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.

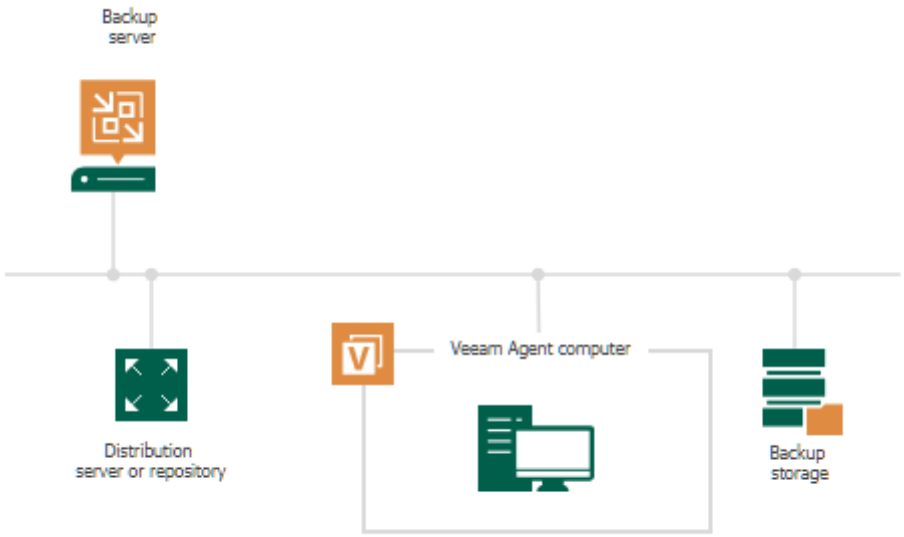
Veeam Backup & Replication offers the following Veeam Agent management capabilities:

- **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 Veeam Agent for Linux. You can also manually deploy all supported Veeam Agents on computers you want to protect. 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
- Distribution repository



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

Veeam Backup & Replication lets you manage Veeam Agent on computers of the following types:

- Workstations, servers, failover clusters, and cloud machines running a Microsoft Windows OS
- Workstations, servers, and cloud machines running a Linux OS
- Servers running a Unix OS
- Workstations and servers running a macOS

If you want to manage Veeam Agents installed on protected computers in Veeam Backup & Replication, you must set Veeam Agents 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.

The following Veeam Agent configurations operate in the managed mode:

- Veeam Agent for Microsoft Windows and Veeam Agent for Linux deployed on remote computers and cloud machines by Veeam Backup & Replication automatically
- Veeam Agents deployed on remote computers by user manually

Veeam Agent for Microsoft Windows and Veeam Agent for Linux Deployed on Remote Computers and Cloud Machines by Veeam Backup & Replication Automatically

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

- On Microsoft Windows computers, Veeam Backup & Replication installs Veeam Transport Service. Veeam Transport Service deploys Veeam installer Service that performs the necessary operations on the computer.
- On Linux computers, Veeam Backup & Replication connects to a Linux computer via SSH and installs Veeam Transport Service. Veeam Transport Service deploys Veeam Deployer Service that performs necessary operations on the computer.

  Keep in mind that Veeam Backup & Replication requires a SSH connection with the Linux computer in the following cases:

  - To communicate with the Linux computer for the first time.

    After Veeam Backup & Replication computer is discovered and Veeam Agent is deployed, Veeam Backup & Replication uses Veeam Deployer Service to connect to the Veeam Agent computer instead of the SSH connection.

  - To communicate with the Linux computer after Veeam Deployer Service failed to establish a connection. In this case Veeam Backup & Replication fails over to the SSH connection.

  - To communicate with the Linux computer running a 32-bit OS. Veeam Backup & Replication does not deploy Veeam Deployer Service is on Linux computers with 32-bit OSes as a connection with Veeam Deployer Service is not supported for these OSes.

  To establish the SSH connection, the Linux computer must be added to the list of trusted hosts. To learn more, see Configuring Security Settings.
- On Amazon EC2 instances or Microsoft Azure virtual machines (both objects can be also referred to as cloud machines), Veeam Backup & Replication installs Veeam Transport Service and Veeam Cloud Message Service that perform necessary operations on the computer.

Veeam Agents Deployed on Remote Computers by User Manually.

On Unix and macOS computers, you must deploy Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris, or Veeam Agent for Mac on a computer you want to protect and set a connection to Veeam Backup & Replication. You can manually deploy Veeam Agent for Microsoft Windows and Veeam Agent for Linux as well. After that, you can use Veeam Backup & Replication to perform necessary operations on the computers. To learn more, see Protected Computers Discovery and Veeam Agent Deployment.

Distribution Server

The distribution server is an architecture component in the Veeam Agent management infrastructure used for automated 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. To learn more, see the Adding Microsoft Windows Servers section in the Veeam Backup & Replication User Guide. After you assigned the role of distribution server, you need to 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:

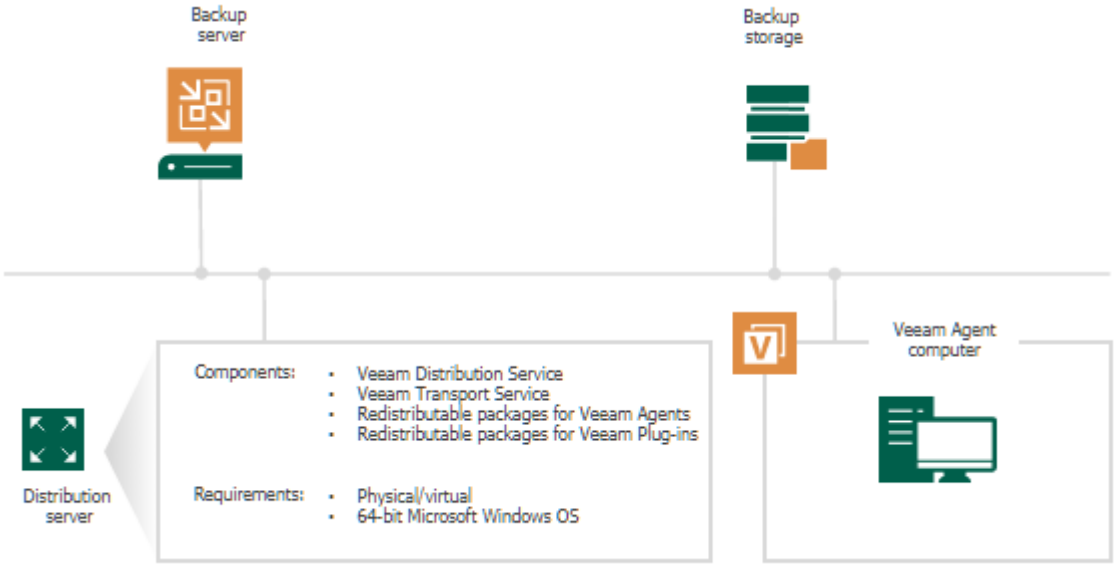
- The role of the distribution server can be assigned to a physical or virtual machine.
- The machine must run a 64-bit Microsoft Windows OS.
- You must add the machine to the Veeam Backup & Replication console as a managed server.

The distribution server comprises the following services and components:

- Veeam Distribution Service
- Veeam Cloud Message Service (for cloud machines only)
- Veeam Transport Service
- Redistributable packages for Veeam Agents and Veeam Plug-ins

> **TIP**
>
> To learn how to use protection groups to automatically deploy Veeam plug-ins for enterprise applications, see Veeam Plug-ins for Enterprise Applications Guide.

Keep in mind that Veeam Backup & Replication does not support automated deployment of Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris and Veeam Agent for Mac. You must deploy these Veeam Agent on computers using setup files generated by Veeam Backup & Replication. To learn more, see Deploying Veeam Agents Using Generated Setup Files.



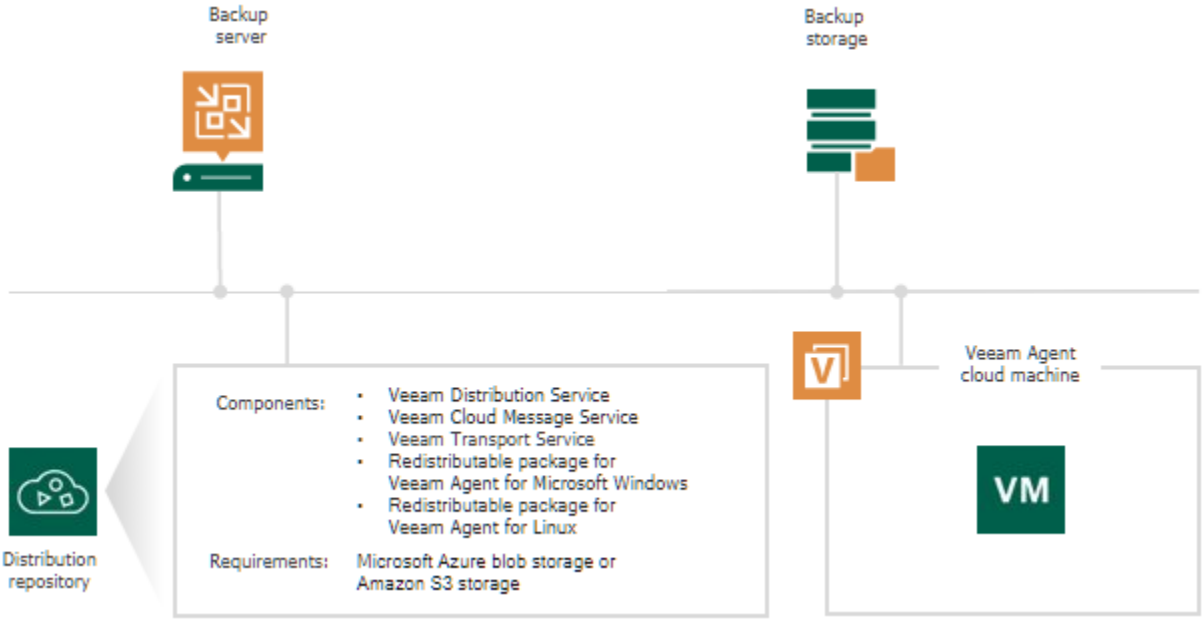
y

> **TIP**
>
> If you have several Microsoft Windows and Linux computers with Veeam Agent installations managed by Veeam Backup & Replication, you can centrally deploy a hotfix on all managed Veeam Agent computers. To learn more, see Appendix A. Deploying Hotfix on Protected Computers.

Distribution Repository

The distribution repository is an architecture component in the Veeam Agent management infrastructure used for automated deployment of Veeam Agent setup files to cloud machines. When you instruct Veeam Backup & Replication to deploy Veeam Agent on a cloud machine, the Veeam backup server communicates to the distribution repository, and Veeam Backup & Replication uploads Veeam Agent setup file from the distribution repository to the target cloud machine.

The role of the distribution repository must be assigned to a dedicated object storage repository. To do this, you need to add a Microsoft Azure blob storage or Amazon S3 storage to your infrastructure depending on the type of cloud machines you plan to protect. To learn more, see Adding Azure Blob Storage or Adding Amazon S3 Storage in the Veeam Backup & Replication User Guide.



Protected Computers Discovery and Veeam Agent Deployment

Veeam Backup & Replication supports automated and manual deployment of Veeam Agents on computers in your infrastructure:

- Automated and manual deployment using the Veeam backup console
- Manual deployment using external tools

Automated and Manual Deployment Using Veeam Backup Console

You can deploy Veeam Agent for Microsoft Windows and Veeam Agent for Linux from the Veeam Backup & Replication console. To learn more about supported scenarios, see Supported Veeam Agents.

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. To learn more, see Protection Groups.

You can also disable automated Veeam Agent installation when configuring a protection group. In this case, you will need to use the Veeam Backup & Replication console to install Veeam Agent on every computer included in the protection group. To learn more, see Installing Veeam Agent.

Manual Deployment Using External Tools

You can manually deploy all supported Veeam Agents using external tools. To learn more about supported scenarios, see Supported Veeam Agents.

To deploy Veeam Agents using external tools, you need to perform the following operations:

1. Create a protection group for pre-installed Veeam Agents using Veeam Backup & Replication. To learn more about this type of protection groups, see Protection Group Types.

   After a new protection group is created, Veeam Backup & Replication generates a set of setup files required for the Veeam Agent deployment. This set of setup files includes an XML configuration file with a TLS certificate. This certificate is used to secure the first communication between Veeam Backup & Replication and Veeam Agents. It helps Veeam Agents identify themselves and make sure that computers connecting to the Veeam backup server are really the ones that they claim to be.

   To learn how to check information about the currently used certificate, see Configuring Security Settings.

   > **IMPORTANT**
   >
   > Veeam Backup & Replication generates the same TLS certificate for the first communication between Veeam Backup & Replication and all computers you want to include in protection groups for pre-installed Veeam Agents. So, it is strongly recommended that you securely store and share Veeam Agent setup files. Otherwise, any computer that has this certificate can connect to the Veeam backup server.

2. Using external tools, transfer Veeam Agent setup files to the computer you want to protect. Then, deploy Veeam Agent and connect it to Veeam backup server with an XML configuration file. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

   Once you connect Veeam Agent to the Veeam backup server, Veeam Backup & Replication discoveries the computer and replaces the TLS certificate for all Veeam Agent computers with another TLS certificate that is unique for each computer. After that, you can find the connected computer in the Veeam Backup & Replication console displayed as a member of the protection group.

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.

> **IMPORTANT**
>
> Keep in mind that protection groups for pre-installed Veeam Agents do not allow you to perform deployment and management tasks. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

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, organizational unit, group, computer, or failover 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 organizational 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 organizational units and/or computers.
  - You can include in the protection group an entire domain or other Active Directory object (such as a container or organizational unit) and exclude specific child objects being part of this object, for example, selected organizational 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.

- **Computers with pre-installed agents**

  You can create protection groups for pre-installed Veeam Agents. Protection groups for pre-installed Veeam Agents are empty just after they are created. You must deploy Veeam Agents on computers and configure Veeam Agents to connect to the Veeam backup server. After deployment and configuration, computers become members of the protection group.

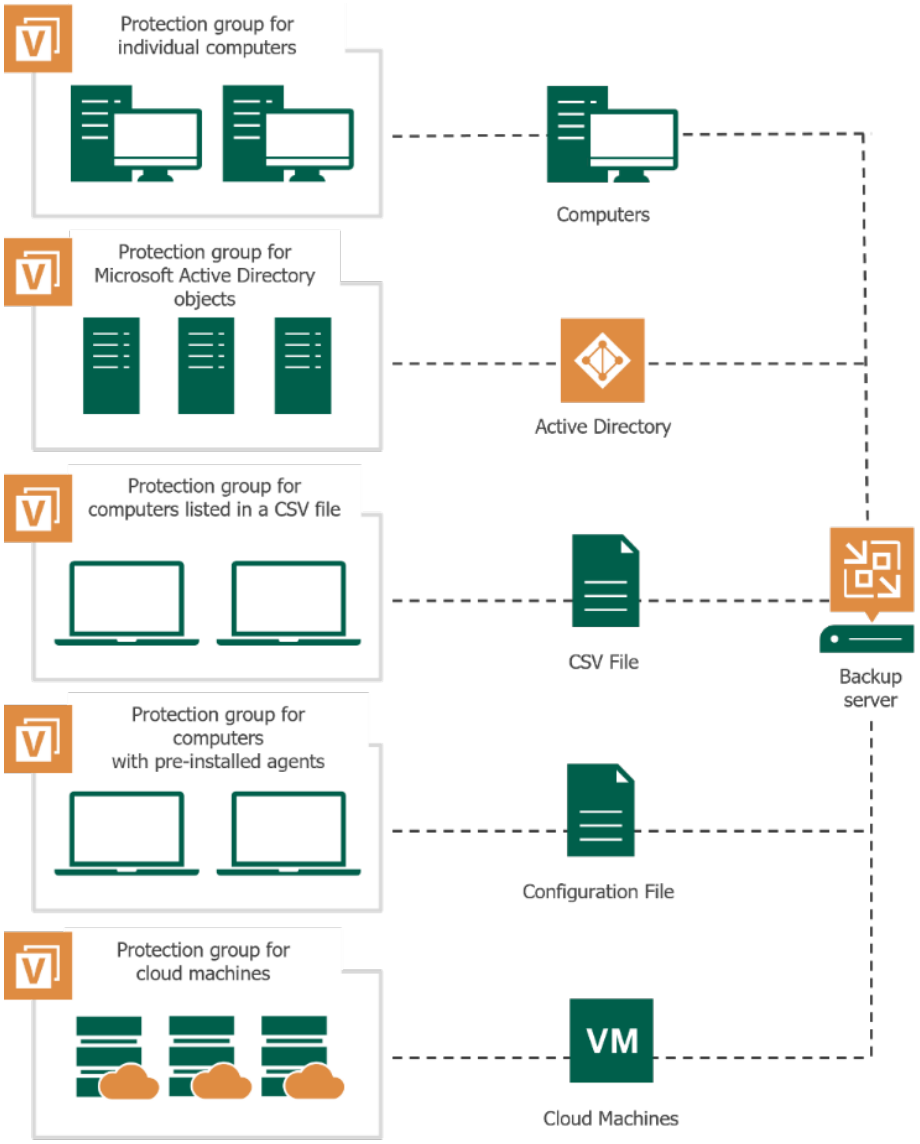
  This option is recommended if you do not have the full list of computers that you want to protect when you create the protection group. This option also provides a convenient way to install agents using third-party software distribution solutions, when deploying them from the Veeam backup server is not possible due to security and network connectivity restrictions.

  Keep in mind that the **Computers with pre-installed agents** option is the only applicable option for Unix and macOS computers that you plan to protect with Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris, and Veeam Agent for Mac.

- **Cloud machines**

  You can create protection groups to manage Veeam Agents installed on Amazon EC2 instances or Microsoft Azure virtual machines (both objects can be also referred to as cloud machines). This protection group allows you to discover cloud machines and deploy Veeam Agents using cloud native API instead of the connection over network. Cloud machines that run Microsoft Windows or Linux OSes are supported.

  This option is useful if you have cloud machines that run VSS-aware applications in your infrastructure and you want to create transactionally consistent backups of applications on these cloud machines.



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 Service Provider 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 Service Provider 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 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.

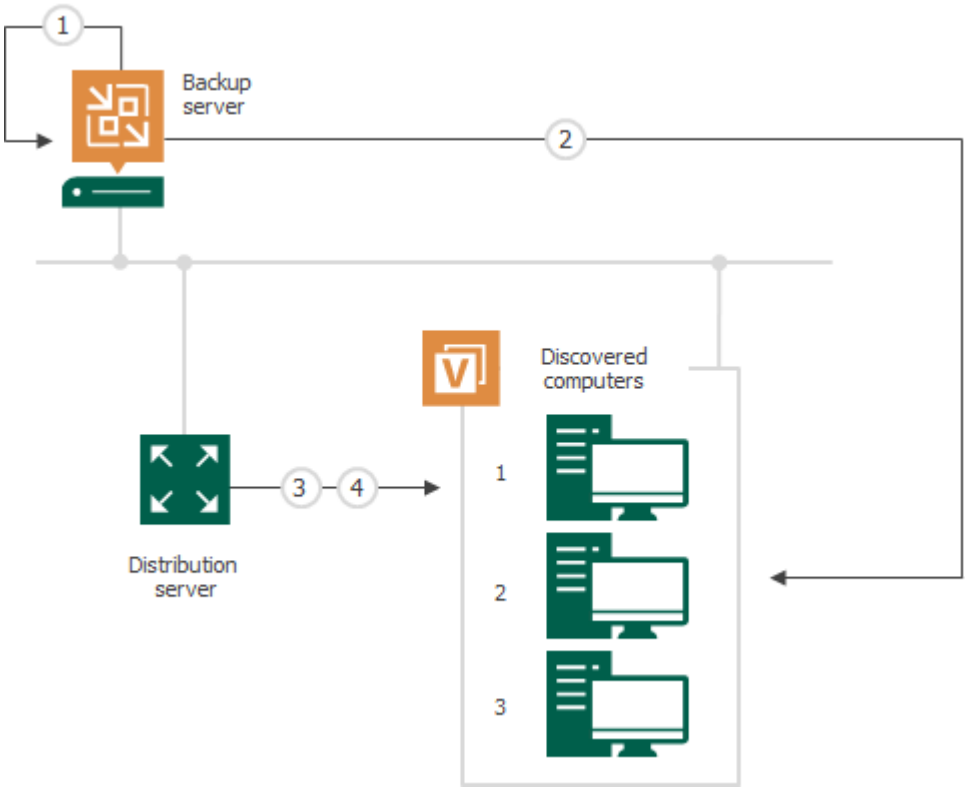
You can view statistics for currently running and already performed rescan job sessions. To learn more, see Viewing Rescan Job Statistics.

Keep in mind that rescan is not available for protection groups for pre-installed Veeam Agents and their members. Veeam Agents installed on computers included in such protection groups synchronize with Veeam Backup & Replication every 6 hours and provide information about the Veeam Agent computer.

How It Works

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

1. Obtains settings specified for the protection group from the configuration database. 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 components on each newly discovered computer:
    - On Windows-based computers, Veeam Backup & Replication deploys Veeam Transport Service that deploys Veeam Installer Service.
    - On Linux-based computers, Veeam Backup & Replication deploys Veeam Transport Service that deploys Veeam Deployer Service.
    - On Amazon EC2 instances or Microsoft Azure virtual machines (both objects can be also referred to as cloud machines), Veeam Backup & Replication deploys Veeam Transport Service and Veeam Cloud Message Service.
4. If the automatic Veeam Agent deployment option is enabled in the protection group settings, Veeam components also deploy Veeam Agent on discovered computers. As a part of this process, Veeam Backup & Replication performs the following operations:
    a. Veeam components 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 computer, product version and license installed).
    b. Veeam Backup & Replication uploads the Veeam Agent setup files:
        - On Windows-based and Linux-based computers, Veeam Backup & Replication uploads files from the distribution server to the discovered computers.
        - On Amazon EC2 instances or Microsoft Azure virtual machines, Veeam Backup & Replication uploads files from the distribution repository to the discovered instances and virtual machines.
    c. Veeam services deploy Veeam Agent:
        - On Windows-based computers, Veeam Installer Service installs Veeam Agent on the target computer.
        - On Linux-based computers, Veeam Deployer Service installs Veeam Agent on the target computer.
        - On Amazon EC2 instances or Microsoft Azure virtual machines, Veeam Cloud Message Service installs Veeam Agent on the target cloud machine.


1
Backup
server
2
Discovered
computers
1
2
3
3
4
Distribution
server

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.

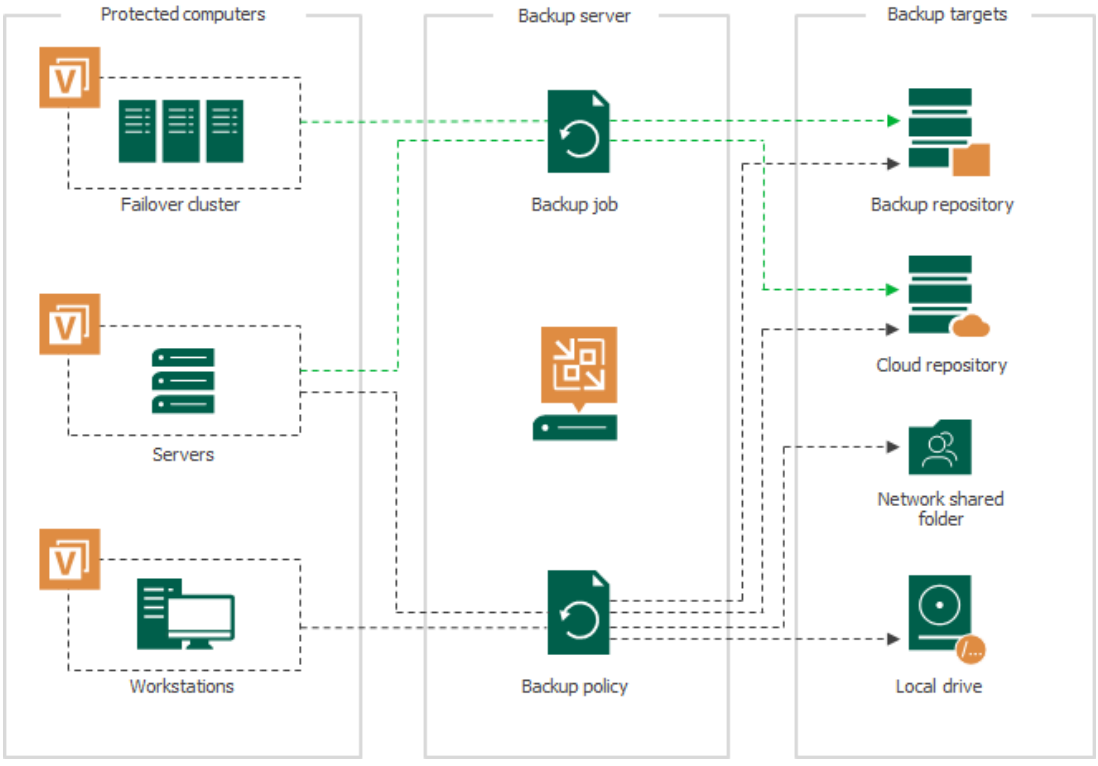
- **Backup policy**

  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.

  Veeam Agent computers that are members of a protection group for pre-installed Veeam Agents can be processed only by backup policies. To learn more about protection group for pre-installed Veeam Agents, see Protection Group Types.

  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.
- Backup policies that process Unix computers. For such Veeam Agent backup policies, Veeam Backup & Replication offers settings supported in Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris.
- Backup policies that process Mac computers. For such Veeam Agent backup policies, Veeam Backup & Replication offers settings supported in Veeam Agent for Mac.

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 policy targeted at a local drive, network shared folder or Veeam backup repository plus unlimited number of backup policies targeted at a Veeam Cloud Connect repository.
- 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.
- The Veeam Agent backup job is the only approach to protect members of a protection group for cloud machines. To learn more, see Protection Group Types.

How Veeam Agent Backup Job Works

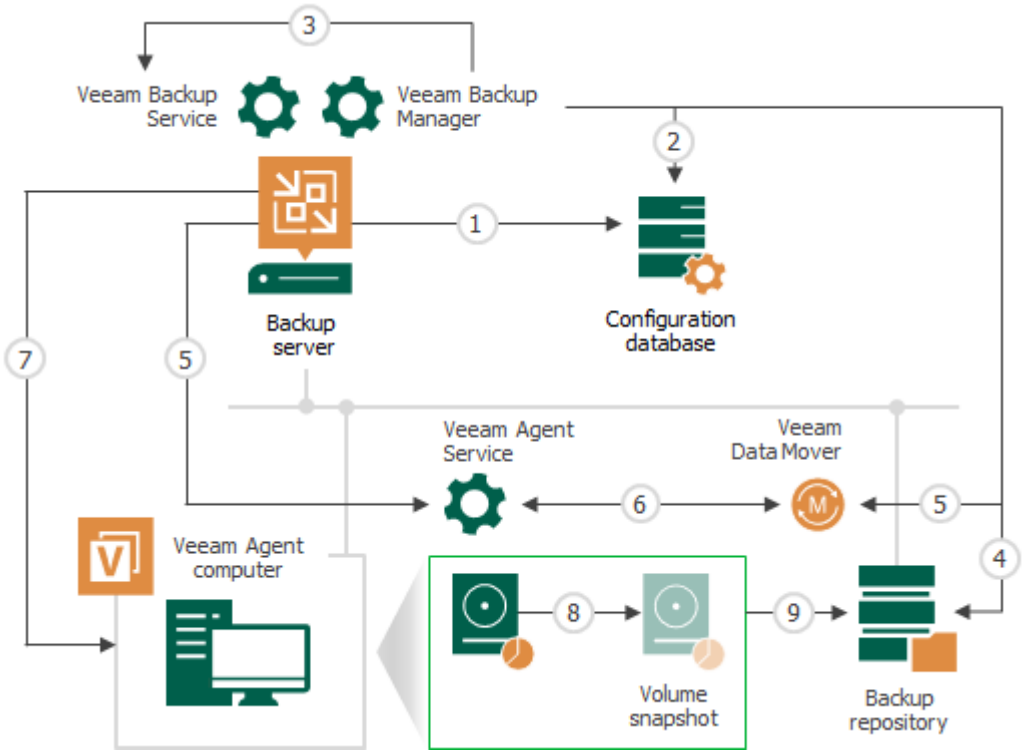
In the scenario where you use the backup job to create Veeam Agent backups, Veeam Backup & Replication performs backup in the following way:

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.

   For Windows-based computers, if the Microsoft VSS technology fails to create a VSS snapshot for some reason, Veeam Agent for Microsoft Windows retries the operation up to 3 times.
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.


3
Veeam Backup Service
Veeam Backup Manager
2
1
Backup server
Configuration database
7
5
Veeam Agent Service
Veeam Data Mover
6
5
4
Veeam Agent computer
8
9
Volume snapshot
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. To learn more, see Creating Veeam Agent Backup Policies.

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. You can use the Veeam Agent control panel to start the backup job manually. This allows you to create ad-hoc backups of your data in addition to backups created upon schedule defined in the backup policy.
- The backup policy is the only approach to protect Mac and Unix computers as Veeam Agent for Mac, Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris do not support backup jobs managed by backup server.
- The backup policy is the only approach to protect members of a protection group for pre-installed Veeam Agents. To learn more, see Protection Group Types.

How Backup Policy Works

> **IMPORTANT**
>
> Mind that the way how backup policy works for computers included in protection groups for pre-installed Veeam Agents differs from the standard scenario. To learn more, see How Backup Policy Works With Computer Included In Protection Group for Pre-Installed Veeam Agents.

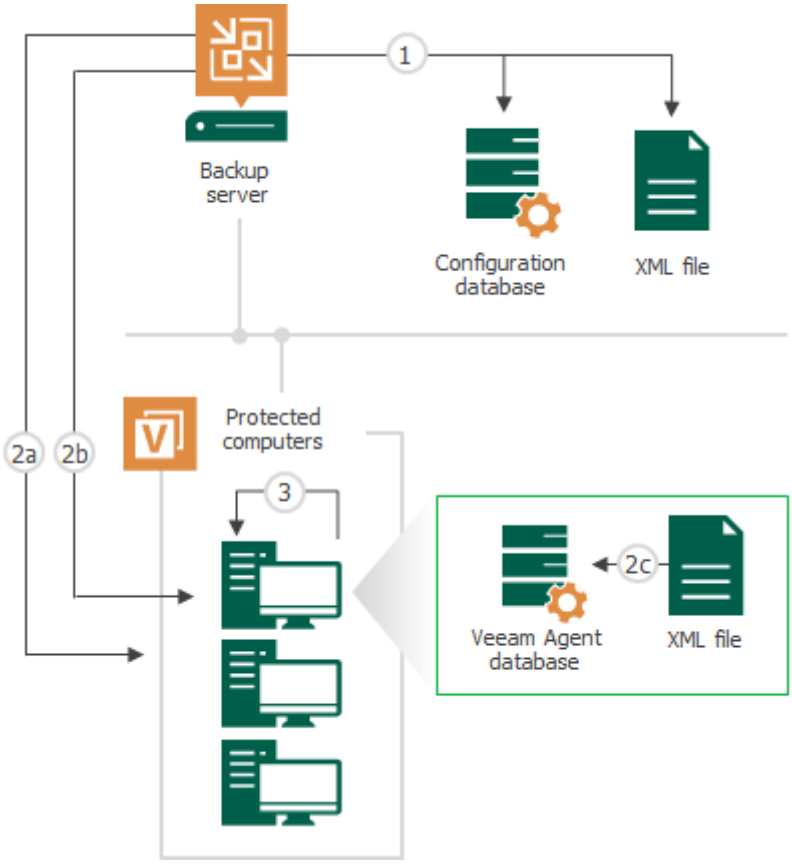
In the scenario where you use the backup policy to create Veeam Agent backups, Veeam Backup & Replication and Veeam Agents interact in the following way:

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.

   Every 6 hours, Veeam Agent 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.


1
Backup server
Configuration database
XML file
2a
2b
Protected computers
3
2c
Veeam Agent database
XML file

How Backup Policy Works with Computer Included in Protection Group for Pre-Installed Veeam Agents

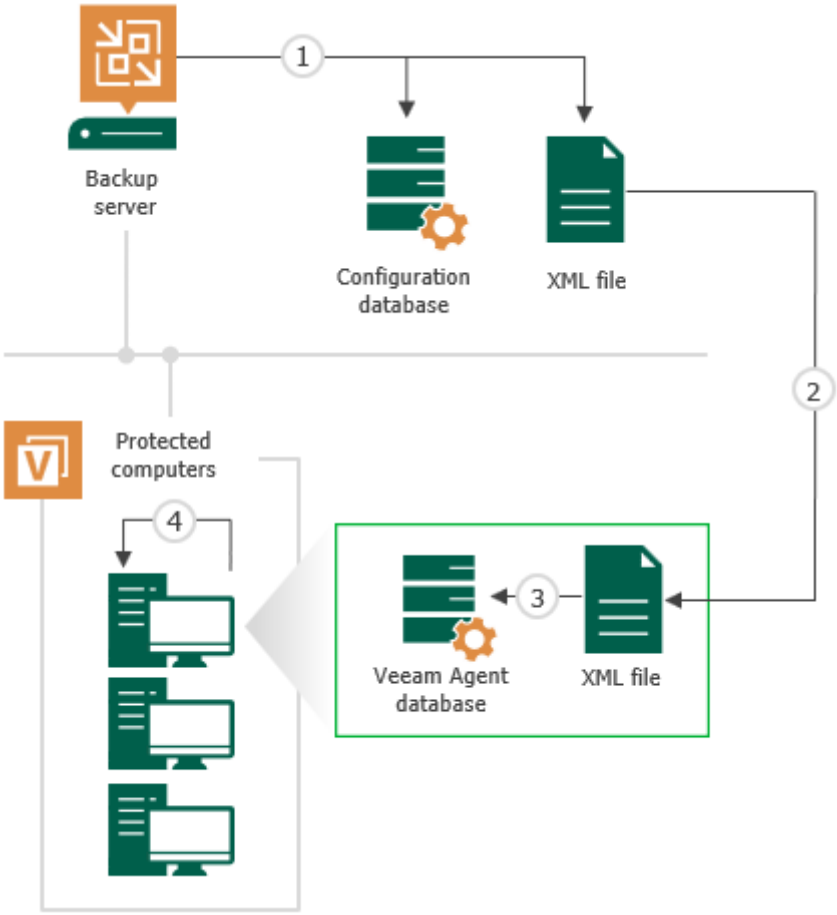
In the scenario where you use the backup policy to create Veeam Agent backups on Veeam Agent computer included in a protection group for pre-installed Veeam Agents, Veeam Backup & Replication and Veeam Agents interact in the following way:

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. Veeam Agent connects to Veeam Backup & Replication and gets the configuration file.

   > **IMPORTANT**
   >
   > Veeam Agent does not connect to Veeam Backup & Replication immediately after updated backup policy settings are saved. Veeam Agent checks whether Veeam Backup & Replication has any updates in the backup policy settings periodically. As a result, a time period between scenario steps 1 and 2 may take up to 6 hours.

3. Veeam Agent uses the backup policy settings from the configuration file to create a Veeam Agent backup job. Settings of the created backup job are saved to the Veeam Agent database on protected computer.
4. 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.
   - How Backup Works section in the Veeam Agent for Oracle Solaris User Guide.
   - How Backup Works section in the Veeam Agent for IBM AIX User Guide.
   - How Backup Works section in the Veeam Agent for Mac User Guide.

   Every 6 hours, Veeam Agent 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.


1
Backup server
Configuration database
XML file
2
Protected computers
4
3
Veeam Agent database
XML file

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.

> **TIP**
>
> You can also apply the backup policy to protected computers manually, if needed. To learn more, see Applying 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 the backup process manually in the Veeam Backup & Replication console.
  - 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.

  Keep in mind that Veeam Backup & Replication cannot apply backup policy to protection groups for pre-installed Veeam Agents and their members. For members of such protection groups, the policy application process can be started only by Veeam Agent.

- **By Veeam Agent**

  The Veeam Agent service running on a protected computer regularly synchronizes with Veeam Backup & Replication and checks whether job settings obtained from the backup policy are up-to-date and updates backup job settings, if necessary. Veeam Agent performs the synchronization every 6 hours.

  During the synchronization session, Veeam Agent performs the following operations:

  a. 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.

  b. 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.

Backup of Microsoft Windows Computers

To back up data of Microsoft Windows computers, 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
- The backup cache is supported only for backup policies (backup jobs managed by Veeam Agent).
- 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.

Storage Snapshots Support

You can use Veeam Backup & Replication and Veeam Agent for Microsoft Windows operating in the managed mode (within the Veeam Agent management scenario) to create backups from native storage snapshots.

Native storage snapshots allow the following:

- Veeam Backup & Replication to use backup proxy servers to process storage systems.
- Veeam Agent to use hardware Volume Shadow Copy Service (VSS) provider and capabilities of native snapshots that are created on production storage systems to create backups.

This approach results in much less load on protected servers compared to the regular backup scenario that uses software VSS provider.

For general information about backup jobs that use storage snapshots as a data source, see the Integration with Storage Systems section in the Veeam Backup & Replication User Guide.

Getting Started

Before you configure a Veeam Agent backup job that will use a storage system snapshot as a data source, you must complete the following steps:

1. Configure the backup infrastructure to create backups from native storage snapshots. For details, see the Backup Infrastructure for Storage Integration section in the Veeam Backup & Replication User Guide.

   Keep in mind that you must allow your storage to process Veeam Agent backups. To do this, select the **Block storage for Microsoft Windows servers** check box at the **Name** step of the **New Storage** wizard, then specify options for accessing the storage system at the **Agent Access** step of the wizard. For details, see the Adding Storage Systems section in the Veeam Backup & Replication User Guide.

   Veeam Agent for Microsoft Windows allows you to create backups from native snapshots with hardware VSS provider only. For the list of supported storage systems, see the Veeam Agent Integration section in the Veeam Backup & Replication User Guide.

2. Add a Microsoft Windows computer to the inventory and deploy Veeam Agent for Microsoft Windows on this computer using the Veeam Backup & Replication console. To learn more, see Creating Protection Groups.

Considerations and Limitations

Before you create a Veeam Agent backup from a storage system snapshot, check the following prerequisites:

- The backup proxy and the Veeam Agent computer must run Microsoft Windows Server OS versions. The backup proxy cannot run the OS version that is earlier than the Veeam Agent computer OS version.
- You must use the following product editions:
  - The Standard, Enterprise, or Enterprise Plus edition of Veeam Backup & Replication on the backup server with the backup proxy role.
  - The Server edition of Veeam Agent for Microsoft Windows on the Veeam Agent computer.

  You can check product editions in the **License Information** window of the Veeam Backup & Replication backup console. For details, see the Viewing License Information section in the Veeam Backup & Replication User Guide and the Assigning License to Veeam Agent section in the Veeam Agent for Microsoft Windows User Guide.
- At least one storage logical unit number (LUN) must be mapped to the Veeam Agent computer.
- At least one backup proxy must have access to all LUNs.
- You must use iSCSI or Fibre Channel protocol for your storage system:
  - You must use iSCSI or Fibre Channel protocol to connect LUNs to Veeam Agent computer and backup proxy to your storage system.
  - If you plan to use the iSCSI Protocol, the backup proxy and the Veeam Agent computer must have a Microsoft iSCSI Software initiator enabled.
  - If you plan to use the Fibre Channel Protocol, the backup proxy and the Veeam Agent computer must have a Fibre channel adapter installed and must have access to the storage system over Fibre Channel fabric.
- If a Veeam Agent computer has a storage system with disks that use the GUID Partition Table (GPT) as a partitioning scheme, each disk must contain a Microsoft Reserved (MSR) partition.

In addition to general limitations listed in the in the Veeam Backup & Replication User Guide, consider the following limitations for Veeam Agent backups from storage snapshots:

- If the Storage Replica feature is installed on the Veeam Agent computer, you cannot back up this computer using the hardware VSS provider. If you want to add this computer to the backup scope, you must allow Veeam Backup & Replication to fail over to the regular backup scenario that uses software VSS provider. To learn more, see Integration Settings. To learn more about Storage Replica, see this Microsoft article.
- The backup proxy and the Veeam Agent computer you want to back up cannot be the same computer.
- You cannot back up the following objects using the hardware VSS provider:
  - Volumes allocated to the RDM disk
  - Storage spaces

  With volumes allocated to RDM disks or storage spaces in the backup scope, Veeam Backup & Replication will fail over to the regular backup scenario even if failover is not allowed in storage integration settings.
- If your Veeam Agent computer has a disk that contains the storage spaces protective partition, you cannot back up volumes allocated to this disk using the hardware VSS provider. To back up such volumes, you must allow Veeam Backup & Replication to fail over to the regular backup scenario that uses software VSS provider. To learn more about failover, see Integration Settings.

- Volumes greater than 64 TB are supported with limitations. For details, see Storage Snapshots on Volumes Greater than 64 TB.
- BitLocker encrypted volumes are supported with limitations. For details, see Storage Snapshots on BitLocker Encrypted Volumes.

Backup from Storage Snapshots

To create a backup from a storage snapshot, Veeam Backup & Replication and Veeam Agent do the following:

1. Veeam Backup & Replication checks that the hardware VSS provider is installed on the Veeam Agent computer.

   If the hardware VSS provider is not installed, Veeam Backup & Replication rescans the Veeam Agent computer and installs the hardware VSS provider.

2. Veeam Backup & Replication starts a backup job session and sends a request to the storage system to create a native snapshot as a new LUN.

   If storage system fails to create a native snapshot within the time period allowed by VSS, Veeam Backup & Replication will behave according to the storage integration settings. Veeam Backup & Replication will complete the backup job with the *Failed* status or fail over to the regular backup scenario that uses software VSS provider.

   To learn more about VSS and its limitations, see this Microsoft article.

3. After a snapshot LUN is created, this LUN connects to Veeam Agent computer to finish VSS operations and record storage metadata.

4. Veeam Backup & Replication moves the snapshot LUN to the backup proxy.

5. Veeam Backup & Replication reads the snapshot LUN and transfers data from the backup proxy to the target repository.

   Keep in mind that if the snapshot LUN contains a dynamic volume, Veeam Backup & Replication reads all extents of this volume.

6. Veeam Backup & Replication completes the backup job session and deletes snapshot metadata from the storage and backup proxy.

After that, you can use backups created from storage snapshots for restore and administration tasks. For such Veeam Agent backups, Veeam Backup & Replication allows you to perform the same set of operations as for backups created with regular backup scenario that uses software VSS provider. To learn more, see Restoring Data from Veeam Agent Backups and Managing Veeam Agent Backups.

Storage Snapshots on Volumes Greater than 64 TB

By default, Veeam Agent can back up file systems that 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. But if you use Veeam Backup & Replication and Veeam Agent operating in the managed mode and you create backups from storage snapshots, you can back up volumes greater than 64 TB.

In addition to considerations and limitations listed in the Storage Snapshots Support, consider the following:

- You can back up volumes that are greater than 64 TB using only hardware VSS provider installed by Veeam Agent. In case of fail over to the regular backup scenario that uses software VSS provider, the backup job will fail.
- Your production system storage must support backup of the volume with the size that you plan to back up.
- We strongly do not recommend to back up Veeam Agent computer volumes (for example, system volume) together with volumes greater than 64 TB. Otherwise, the software VSS provider may locate the shadow copy storage area for Veeam Agent computer volumes on the volume greater than 64 TB. In this case, the backup job will fail and the OS running on the Veeam Agent computer may get a blue screen error.

Storage Snapshots on BitLocker Encrypted Volumes

You can use Veeam Backup & Replication and Veeam Agent for Microsoft Windows operating in the managed mode to create backups from storage snapshots located on volumes encrypted with Microsoft Windows BitLocker.

If volumes you want to back up are protected by Microsoft Windows BitLocker, do the following:

1. On the Veeam Agent computer, set BitLocker to automatically unlock volumes to which LUNs are mapped. For details, see this Veeam KB article.
2. On the backup proxy, perform the following operations:
    a. Connect volumes to which LUNs are mapped to the backup proxy.
    b. Set BitLocker to automatically unlock connected volumes on the backup proxy. For details, see this Veeam KB article.
    c. Disconnect volumes to which LUNs are mapped from the backup proxy.

If you plan to use several backup proxies, repeat step 2 for each backup proxy.

Consider the following:

- Automatic unlocking requires encryption of the system drive.
- If automatic unlocking is not set on the Veeam Agent computer, file indexing will not work during the backup process.
- If automatic unlocking is not set on the backup proxy, only volume-level restore to a new location is available. File-level restore and volume-level restore to the original location will fail.

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 supports Windows Server Failover Clusters running on any of the supported Microsoft Windows Server OS versions. To learn the full list of versions, see System Requirements.

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

- Windows File Server Failover Clusters
- Windows Server Failover Clusters that run the following applications:
  - Microsoft SQL Server 2008 SP4 or later

    Keep in mind that SQL Server Failover Cluster Instances and AlwaysOn Availability Groups are supported only for Microsoft SQL Server 2012 or later. For details about AlwaysOn Availability Groups, see Backup of AlwaysOn Availability Groups.
  - Microsoft Exchange Server 2013 or later

    Microsoft Exchange Database Availability Groups (DAGs) are supported. For details, see Backup of Database Availability Groups.

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 managed by Veeam Backup & Replication only. You cannot process a failover cluster by Veeam Agent operating in the standalone mode.
- Backup of CSV (Cluster Shared Volumes) is not supported. Cluster disks used as CSV are automatically excluded from backup.
- Active Directory-Detached Clusters 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 this Microsoft article.
- AlwaysOn Availability Groups based on SQL Server Failover Cluster Instances are not supported.
- AlwaysOn Clusterless Availability Groups are not supported.
- Distributed AlwaysOn Groups are not supported.
- SureBackup of failover clusters is not supported.

NOTE

Veeam Backup & Replication does not support simultaneous processing of Microsoft SQL Server transaction logs on SQL Server clustered instances with identical names. The limitation applies to clustered instances of different failover clusters as well.

For example, you configure two backup jobs that process transaction logs of different failover clusters whose SQL clustered instances have identical names. In case these backup jobs run simultaneously, transaction logs will be processed only by the backup job that started first. The second backup job will not process transaction logs.

Backup and Restore of Failover Clusters

To process a failover 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:
   - Failover cluster account of the failover cluster whose data you want to back up
   - Active Directory container that includes this failover 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 failover 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 failover cluster account.

   To learn more, see Creating Agent Backup Job for Windows Computers.

IMPORTANT

- If a backup task within a Veeam Agent backup job that processes a failover cluster completes unsuccessfully or a new node is added to a failover cluster, Veeam Agent will create a full backup of all shared disks of the failover cluster during the next backup job run.
- You cannot create per-machine backup files with a Veeam Agent backup job that processes failover clusters because of failover cluster limitations. The backup job with failover clusters in the backup scope creates a separate backup file for each failover cluster.

Data Restore from Failover Cluster Backups

You can perform data restore tasks with failover cluster backups created by Veeam Agent. For example, you can restore entire volumes or individual folders and files from such backups.

Consider the following:

- When you restore data of a failover cluster, make sure that the failover cluster is added to the Veeam Backup & Replication inventory as part of a protection group.
- When you restore data of a failover cluster with shared disks, Veeam Agent does not restore data of a disk witness. During volume restore for shared disks of a failover cluster, the disk witness is not displayed at the **Disk Mapping** step of the **Volume Restore** wizard.

Backup Copy from Failover Cluster Backups

You can perform data copy tasks with failover cluster backups created by Veeam Agent to a secondary location.

When you copy failover cluster backups, consider the following:

- The network traffic will be higher compared to the traffic sent during the Veeam Agent backup job run.
- If you copy a failover cluster backup, the job ignores the **Use per-machine backup files** option enabled for the backup repository and creates a single backup copy file for each failover cluster.

  To learn more, see the Per-Machine Backup Files section in the Veeam Backup & Replication User Guide.

To learn more about backup copy, see the Backup Copy section in the Veeam Backup & Replication User Guide.

Backup of Database Availability Groups

The procedure of adding a Microsoft Exchange Database Availability Group (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 process a regular DAG, you must configure a Veeam Agent backup job for a failover cluster. To learn more, see Backup and Restore of Failover Clusters.
- 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 protection group with all nodes of the IP Less DAG and add this protection group to the Veeam Agent backup job managed by the backup server. To learn more, see Creating Agent Backup Job for Windows Computers.

How It Works

During backup, Veeam Agent performs the following operations:

1. Veeam Agent detects Microsoft Exchange Server.

   Keep in mind that Veeam Agent performs the backup, but all pre-/post-backup operations are performed by the Exchange VSS Writer that is available on any Microsoft Exchange Server. To learn more about Exchange VSS Writer, see this Microsoft article.

   To learn more about Exchange data backups, see this Microsoft article.

2. Veeam Agent detects that server added to the backup scope is a part of a DAG.

   - For a regular DAG, Veeam Agent gets the list of all DAG servers and adds these servers to the backup job.

     If a set of servers included in regular DAG changes between the job runs, Veeam Agent changes the backup scope accordingly.

   - For an IP less DAG, you must add all servers of an IP less DAG to the backup job manually.

     > **IMPORTANT**
     >
     > An IP less DAG does not have an Administrative Access Point. As a result, you must add all servers of an IP less DAG to the protection group manually. If a set of servers included in an IP less DAG changes between the job runs, you must update the backup scope manually as well. Otherwise, Veeam Agent will still back up all database files from all servers included into backup scope, but Microsoft Exchange Server will detect data inconsistency and skip the database processing.

3. Veeam Agent processes databases to prepare them for backup: Veeam Agent freezes databases, creates database snapshots, and returns databases to the initial state.

   DAG servers contain active and passive copies of each database. By default, the Exchange VSS Writer issues VSS freeze commands to passive database copies only. If all passive copies of the database are not available for some reason, the Exchange VSS Writer issues the VSS freeze command to the active copy of the database. This approach helps to ensure data consistency.

4. After the database processing is finished, Veeam Agent creates a transactionally consistent backup of all databases running on DAG servers. The backup will include all database files from all servers included into backup scope regardless of the database processing success.

   > **NOTE**
   >
   > Consider the following:
   >
   > - The Exchange VSS Writer cannot create a VSS snapshot of all databases at once. That is why Veeam Agent backs up DAG servers one by one.
   > - Veeam Agent backs up all active and passive copies of the database on all DAG servers. Otherwise, Veeam Agent will not be able to ensure data consistency as Microsoft Exchange transfers data from active copy to passive copies after some time.

5. Veeam Agent notifies the Exchange VSS Writer about successful backup. If required, the Exchange VSS Writer truncates logs on DAG servers.

   Log truncation is applied to all passive and active database copies. Veeam Agent uses the Exchange VSS Writer to truncate logs. However, you can set Veeam Agent to disable transaction logs or backup transaction logs with Veeam Agent in the backup job settings. To learn more, see Guest Processing Settings.

Backup of AlwaysOn Availability Groups

To process AlwaysOn Availability Group, you must complete the following tasks:

1. In Veeam Backup & Replication, create a protection group that includes Active Directory objects. Add to this protection group the failover cluster account of the failover cluster whose data you want to back up.
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 failover 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 failover cluster account.
   c. At the **Guest Processing** step of the wizard, select the **Enable application-aware processing** option. Then click **Applications**. In the **Processing Settings** window, define processing settings. To learn more, see Application-Aware Processing.

   To learn more about the backup job configuration, see Creating Agent Backup Job for Windows Computers.

If you select to process transaction logs with the backup job in the **Processing Settings** window, Veeam Backup & Replication performs the following operations during an image-level backup:

1. Requests and analyzes information about databases that are included in the AlwaysOn Availability Groups.
2. Depending on the retrieved information, selects the VSS backup type for each computer: full backup (VSS_BT_FULL) or copy-only backup (VSS_BT_COPY). The copy-only backup is created if the computer represents a secondary node for at least one AlwaysOn Availability Group.

   To learn more about VSS backup types, see this Microsoft article.

Transaction Log Backup

You can enable transaction log backup in the **Processing Settings** window. To learn more, see Microsoft SQL Server Transaction Log Settings.

Transaction log backup can be performed only for those databases that were successfully backed up, on the primary or on the secondary node of AlwaysOn Availability Group. At each log processing interval, Veeam Backup & Replication chooses the AlwaysOn Availability Group node for which transaction logs will be backed up. Logs are backed up from one node of the AlwaysOn Availability Group.

To become a subject for a log backup, the node must meet the following criteria:

- The node is not subject to the limitations listed in Failover Cluster Support.
- The necessary Veeam Backup & Replication components must be installed on this node and the computer included in AlwaysOn Availability Group must be running. For more information on the necessary components, see the How Microsoft SQL Server Log Backup Works section in the Veeam Backup & Replication User Guide.
- The database backup preferences settings must allow a backup of the node that you want to process. For example, if you want to back up the primary node, you must not exclude this node from a backup, or select the **Secondary only** option in the database backup preferences settings.
- Databases in the AlwaysOn Availability Groups for this node were successfully backed up for the last two processing intervals.

Backup of Linux Computers

To back up data of Linux computers, 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 and Snapshot 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 executed on the Veeam Agent computer (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.

Keep in mind that scripts of this type are supported for computers that run Veeam Agent for Linux 4.0 and later only. Earlier versions of Veeam Agent for Linux do not run pre-job and post-job scripts obtained from the backup server.

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 of Database Systems

You can instruct Veeam Agent for Linux to create consistent backups of Veeam Agent computers that run one of the following database systems:

- Oracle database system
- MySQL database system
- PostgreSQL database system

> **TIP**
>
> If you back up the Oracle or PostgreSQL database system using a backup job managed by Veeam backup server, Veeam Agent can also back up archived logs. You can use archived logs to restore the database system to the necessary state up to the certain operation. Veeam Agent backups archived logs in the similar way as in a backup job for VMs. To learn more, see Oracle Log Backup or PostgreSQL Log Backup section in the Veeam Backup & Replication User Guide.

To learn how backup of database systems works, see the Backup of Database Systems section in the Veeam Agent for Linux User Guide.

Backup of Unix Computers

To back up data of Unix servers, you can use Veeam Agent for Oracle Solaris or Veeam Agent for IBM AIX together with 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.

Veeam Backup & Replication is required for the following tasks that are critical for the Unix computers protection:

- Configuration of the protection group for pre-installed Veeam Agents that is the only applicable group for Unix computers.
- Configuration of the backup policy for Veeam Agent for Unix.

Keep in mind that you must deploy Veeam Agent for Unix on the Unix computer using setup files generated by Veeam Backup & Replication. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

Backup Job Scripts

You can instruct Veeam Agent for Unix to run custom scripts within the backup job session.

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 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 following sections:

- The Backup Job Scripts section in the Veeam Agent for IBM AIX User Guide.
- The Backup Job Scripts section in the Veeam Agent for Oracle Solaris User Guide.

Backup of macOS Computers

To back up data of macOS computers, you can use Veeam Agent for Mac together with 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.

Veeam Backup & Replication is required for the following tasks that are critical for the macOS computer protection:

- Configuration of the protection group for pre-installed Veeam Agents that is the only applicable group for macOS computer.
- Configuration of the backup policy for Veeam Agent for Mac.

Keep in mind that you must deploy Veeam Agent for Mac on the macOS computer using setup files generated by Veeam Backup & Replication. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

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.
- Veeam Agents must trust the TLS certificate obtained from the SP in the same way as Veeam Backup & Replication. If you accept the certificate as trusted in Veeam Backup & Replication, Veeam Agents will trust it automatically as well. If you set up the trust relationship on the Veeam backup server, you must also do this on all Veeam Agent computers that you plan to back up to the cloud repository.

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 computer 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 computer 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 computers only).
- Restore individual files and folders from a Veeam Agent backup (for backups of Microsoft Windows computers only).
- Restore application items from a Veeam Agent backup with Veeam Explorers (for backups of Microsoft Windows computers 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.

Backup to Object Storage

If you want to store your data in a cloud-based or on-premises object storage, you can create Veeam Agent backups in repositories provided by the object storage.

The following Veeam Agents support the object storage as a primary repository for backup jobs, backup policies, and backup copy jobs:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for Mac

You can store Veeam Agent backups on the following types of the object storage:

- Amazon S3
- S3 compatible storage
- Google Cloud
- Microsoft Azure Blob
- IBM Cloud
- Wasabi Cloud

Veeam Agents communicate with the object storage using one of the following connection modes:

- Connection through a gateway server. With this connection mode, Veeam Agents access object storage through Veeam Backup & Replication. As a result, Veeam Agent access to object storage is managed by a proxy component — a gateway server assigned in the Veeam Backup & Replication console. Backup data is sent from Veeam Agent computer to the gateway server, then it is sent from gateway server to the object storage.
- Direct connection. With this connection mode, Veeam Agents access object storage directly. Backup data is sent from Veeam Agent computer to the object storage. Veeam Agent access to object storage is managed by Application Programming Interface (API) provided by an external cloud service provider. To learn more, see Access Permissions for Direct Connection to Object Storage.

  If you plan to back up to the repository in the object storage using a direct connection and a backup job managed by Veeam Agent, mind that Veeam Agents will still connect to Veeam Backup & Replication periodically. Using these connections, Veeam Agent will update license and backup job settings. These connections are not necessary for backup job sessions.

  > **IMPORTANT**
  > - After you switch your repository from one connection mode to another, Veeam Agent will need to connect to Veeam Backup & Replication to update repository settings. Until this connection is made, all backup operations by Veeam Agents will fail.
  > - If you plan to back up data to the S3 compatible storage using the direct connection, you must perform an extra step: manually set access to the object storage for Veeam Agents. To learn more, see the Managing Permissions for S3 Compatible Object Storage section in the Veeam Backup & Replication User Guide.

Getting Started

To back up Veeam Agent computer data to an object storage, you must complete the following steps:

1. Add repository in the Veeam backup console. For details, see the Adding Object Storage Repositories section in the Veeam Backup & Replication User Guide.

   You can use an object storage in Veeam Backup & Replication as one of the following repositories:

   - Backup repository. To learn more, see Backup Repository section in the Veeam Backup & Replication User Guide.
   - Scale-out backup repository added as a Veeam backup repository. To learn more, see Scale-Out Backup Repository section in the Veeam Backup & Replication User Guide.
   - Cloud repository. Both simple cloud repository and scale-out backup repository added as a cloud repository are supported. To learn more, see Backup to Object Storage section in the Veeam Cloud Connect Guide.

2. [For S3 compatible object storage] Set access to the added S3 compatible object storage. To learn more see the Managing Permissions for S3 Compatible Object Storage section in the Veeam Backup & Replication User Guide.
3. Create a Veeam Agent backup job or policy and specify the following repository as a target location for backup files:

   - If the object storage is configured as a backup repository or a scale-out backup repository in your infrastructure, specify a Veeam backup repository as a target location for backup files, then select the repository from the list of available repositories.
   - If the object storage is provided to you by Service Provider, specify a Veeam Cloud Connect repository as a target location for backup files, then select the repository from the list of available repositories.

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

Limitations

Before you configure your backup infrastructure to back up to the object storage, consider the following limitations:

- You cannot back up data using Veeam Agent backup job or policy to the following storage devices:
  - AWS SnowBall
  - Azure Databox
- If you plan to add a repository in the object storage as a performance tier of a scale-out backup repository and you plan to back up this repository using direct connection, you can use only backup jobs managed by the backup server. Veeam Agent backup policies are not supported.
- If you plan to back up data to the Microsoft Azure Blob object storage using direct connection, the following limitations apply:
  - Cold Tier is not supported for the following configurations:
    - Backup policies targeted at the object storage added as the Veeam backup repository.
    - Backup jobs and policies targeted at the object storage added as cloud repository.

    To learn more about access tiers for blob data, see this Microsoft article.
  - Immutability is not supported for the following configurations:
    - Backup policies targeted at the object storage added as the Veeam backup repository.
    - Backup jobs and policies targeted at the object storage added as cloud repository.

    To learn more about immutability, see Immutability.
  - Veeam Agents does not support direct backup under the general-purpose V1 storage account type.

Access Permissions for Direct Connection to Object Storage

If you back up data using a direct connection between the Veeam Agent computer and the object storage, access to the object storage will be managed by an API provided by this object storage. Depending on the selected object storage, access permissions are distributed differently. As a result, you must consider different limitations. To learn more, see the following subsections:

- Amazon S3
- Google Cloud
- Microsoft Azure
- IBM Cloud, Wasabi Cloud or other S3 compatible storage

Amazon S3 Storage

On the Amazon S3 storage side, Veeam Agent backup is performed with the following steps:

1. Depending on the backup job mode and the way you added the object storage to your infrastructure, Veeam Backup & Replication performs a certain operation to grant access to the repository in the object storage:

   For backup jobs targeted at the Veeam backup repository

   - For the following job configurations, Veeam Backup & Replication provides Veeam Agents an access to the repository in the object storage using credentials that were specified during the repository configuration in the following job configurations:
     - backup job managed by the backup server
     - backup policy targeted at the object storage though a gateway
   - For the backup policy targeted at the object storage directly, Veeam Backup & Replication creates a user in AWS for each Veeam Agent that backs up to AWS.

   For backup jobs targeted at the Cloud Connect repository

   - For the following job configurations, Veeam Backup & Replication creates a user in AWS for each tenant:
     - backup job managed by the backup server
     - backup policy targeted at the object storage though a gateway
   - For the backup policy targeted at the object storage directly, Veeam Backup & Replication creates a user in AWS for each subtenant.

     To learn more about tenants and subtenants, see Veeam Cloud Connect Guide.

2. If applicable, Veeam Backup & Replication assigns a policy to each created user. This policy contains access permissions and allows Veeam Agent access only those backups that were made only by this Veeam Agent.

Keep in mind the following limitations and prerequisites:

- By default, Veeam Backup & Replication assigns an inline policy to the user. All inline policies combined cannot be greater than 2048 symbols. If you reach this limit, Veeam Backup & Replication starts assigning managed policies. All managed policies combined cannot be greater than 6144 symbols. If you reach this limit, refer to the AWS customer support.
- AWS allows to create 1500 managed policies per the AWS account. If you need more policies, refer to the AWS customer support.
- AWS allows to create 5000 users per the AWS account. If you need more users, use another AWS account.
- Consider that user accounts that you use to connect to the Amazon S3 storage have the required permissions. To learn more, see Permissions.

Google Cloud Storage

On the Google storage side, Veeam Agent backup is performed with the following steps:

1. Depending on the backup job mode and the way you added the object storage to your infrastructure, Veeam Backup & Replication performs a certain operation to grant access to the repository in the object storage:

   For backup jobs targeted at the Veeam backup repository

   - For the following job configurations, Veeam Backup & Replication provides Veeam Agents an access to the repository in the object storage using credentials that were specified during the repository configuration:
     - backup job managed by the backup server
     - backup policy targeted at the object storage though a gateway
   - For the backup policy targeted at the object storage directly, Veeam Backup & Replication creates a user for each Veeam Agent that backs up to Google storage.

   For backup jobs targeted at the Cloud Connect repository

   - For the following job configurations, Veeam Backup & Replication creates a user in Google Cloud for each tenant:
     - backup job managed by backup server
     - backup policy targeted at the object storage though a gateway
   - For the backup policy targeted at the object storage directly, Veeam Backup & Replication creates a user in Google Cloud for each subtenant.

     To learn more about tenants and subtenants, see Veeam Cloud Connect Guide.

2. If applicable, Veeam Backup & Replication assigns a policy to each bucket. This policy contains access permissions and allows Veeam Agent access only those backups that were made only by this Veeam Agent.

Keep in mind the following limitations and prerequisites:

- Policies for buckets have a size limit. If you need to increase the limit, refer to the Google customer support.
- Keep in mind that Google allows to create 100 users per the Google account. If you need more users, refer to the Google customer support.
- If you plan to target Veeam Agent backups at the Google Cloud storage using a backup policy, you must configure a Helper Appliance. To learn more, see the Configuring Helper Appliance section in the Veeam Backup & Replication User Guide.
- Consider that user accounts that you use to connect to the Google Cloud storage have the required permissions. To learn more, see Permissions.

Microsoft Azure Storage

Access permissions are granted to Veeam Agents using shared access signatures (SAS).

IBM Cloud, Wasabi Cloud or Other S3 Compatible Storage

Keep in mind the following limitations and prerequisites:

- After you added the S3 compatible object storage, you must configure access permissions manually in the Veeam Backup & Replication console. To learn more see the Managing Permissions for S3 Compatible Object Storage section in the Veeam Backup & Replication User Guide.
- User accounts that you use to connect to the S3 compatible storage have the required permissions. To learn more, see Permissions.

Backup Immutability

If you store your backup files in an object storage repository, Veeam Agent allows you to protect backup data from deletion or modification by making that data temporarily immutable. It is done for increased security: immutability protects data in your recent backups from loss as a result of attacks, malware activity or any other injurious actions.

> **IMPORTANT**
>
> Backup immutability uses native object storage capabilities. You may incur additional API and storage charges from the storage provider.

Supported Object Storage Types

Veeam Agent supports backup immutability for the following object storage types:

- Amazon S3 storage.
- S3 compatible storage that supports S3 Object Lock (including Wasabi).
- Microsoft Azure Blob storage.

> **NOTE**
>
> Veeam Agent does not support backup immutability for the Google Cloud storage.

Before You Begin

Before you configure immutability for Veeam Agent backups, you must prepare the target storage account. Depending on the selected object storage type, perform the following actions:

- [S3 Compatible and Amazon S3 storage] When you create the S3 bucket, you must enable versioning and the S3 Object Lock feature for the bucket. For more information, see AWS documentation.
- [S3 Compatible and Amazon S3 storage] After you create the S3 bucket with Object Lock enabled, make sure that the default retention is disabled to avoid unpredictable system behavior and data loss. To disable the default retention, edit the Object Lock retention settings as described in AWS documentation.
- [Microsoft Azure Blob storage] You must enable blob versioning and version-level immutability support in the storage account. For more information, see Microsoft Azure documentation.

Consider the following about backup immutability:

- The effective immutability period consists of the user-defined immutability period and the block generation period automatically appended by Veeam Agent. For more information, see How Backup Immutability Works and Block Generation.
- [S3 Compatible and Amazon S3 storage] Veeam Agent will use the *compliance* retention mode for each uploaded object. For more information on retention modes of S3 Object Lock, see AWS documentation.

Configuring Backup Immutability

When you create the backup job that is targeted at an object storage, the immutability period must be specified in the settings of the object storage repository. For details, see Adding Object Storage Repositories in Veeam Backup & Replication User Guide.

Backup Immutability and Retention Policy

Backup immutability operates with backup data and related metadata (checkpoints) on the object storage side. Retention policy operates with logical representation of the stored data, or restore points, on the Veeam Agent side. These two mechanisms act independently from each other.

Veeam Agent will remove the irrelevant restore points per the defined backup retention policy. If the data associated with the removed restore point is still immutable, such data will remain in the repository until expiration of the immutability period. After that it will be automatically removed from the storage.

Limitation of Backup Immutability

You can restore the immutable data that is associated with a restore point removed by retention policy only in Veeam Backup & Replication console. In Veeam Backup & Replication, you must perform the following actions:

- Add the object storage repository that contains the necessary data to Veeam Backup & Replication. For details, see Adding Object Storage Repositories in Veeam Backup & Replication User Guide.
- Roll back to the necessary checkpoint. For details, see Immutability in Veeam Backup & Replication PowerShell Reference.
- Remove the repository from the Veeam Backup & Replication infrastructure. For details, see Removing Backup Repositories in Veeam Backup & Replication User Guide.

After that, you will be able to use Veeam Agent to restore data from the object repository in a regular manner.

How Backup Immutability Works

After you specify the immutability period for a backup and run the backup job for the first time, Veeam Agent will append an additional period of 10 days to the specified immutability period. This additional period of 10 days is called *block generation*. The resulting effective immutability period is the sum of the user-defined immutability period and the block generation period. All data blocks transferred to the target repository within the block generation period will have the same immutability expiration date. For example, data block *a* added on day 1 of the block generation period will have the same immutability expiration date as block *b* added on day 9. For more information, see Block Generation.

During the effective immutability period, the following operations with backup data in the object storage repository will be prohibited:

- Manual removal of data from the backup repository.
- Removal of data by backup retention policy.
- Removal of data using any object storage provider tools.
- Removal of data by the technical support department of the object storage provider.

Extension of Effective Immutability Period

During each transfer of data to the object storage repository, Veeam Agent creates a new checkpoint file with metadata that describes the latest state of the backup in the storage. The immutable blocks of data from a previous checkpoint may be reused in the newly created checkpoint. Veeam Agent keeps reused, or dependent, blocks of data locked by continuously assigning them to new generations and extending their effective immutability period. This guarantees that the effective immutability period is no less than the immutability period defined by user.

During data transfer, the effective immutability period for the backup is set as follows:

- [For new data blocks in the checkpoint] Immutability is set anew. The user-defined immutability period is appended with a 10-day block generation period.
- [For data blocks reused from the previous checkpoint] Immutability is extended to the immutability expiration date set for the new blocks.
- [For data blocks that are not reused in the checkpoint] Immutability is not extended. Such data blocks will remain in the repository until their immutability period is over. After that Veeam Agent will automatically remove them from the repository.

Block Generation

When you specify an immutability period for the recent backups, Veeam Agent will automatically add 10 days to the immutability expiration date. This period is called *block generation*. The block generation period serves to reduce the number of requests to the object storage repository, which results in lower traffic and reduced storage costs. You do not have to configure it, the block generation period is applied automatically.

When the block generation period is appended to the user-defined immutability period, it means there is no need to extend the immutability period for old data blocks when adding new data blocks to the backup during that block generation period.

Consider this example. When you create a full backup to start a backup chain, all data blocks transferred to the object storage repository are new. For these new blocks of data, Veeam Agent will add the block generation period of 10 days to the specified immutability period. If the immutability period is set by user to the default period of 30 days, the effective immutability period with the added block generation period will become 40 days. The first full backup starts its generation that will last for 10 days. All new and reused data blocks within this block generation period will have the same immutability expiration date. For instance, a data block that was transferred to the target repository on day 9 will have the same immutability expiration date as a data block transferred on day 1. This mechanism guarantees that the effective immutability period for all the data blocks within a generation is no less than 30 days.

If a block generation period is over but data blocks from that generation are reused in the newly created checkpoint, their effective immutability period is automatically extended to ensure that the effective immutability period for all the data blocks in the new checkpoint is no less than the user-defined immutability period. For more information, see How Backup Immutability Works.

Recovery Verification for Veeam Agent Backups

Veeam Backup & Replication offers the SureBackup technology to test backups and check if you can recover data from them. You can verify any restore point of a backed-up computer protected with Veeam Agent for Microsoft Windows and Veeam Agent for Linux.

During a SureBackup job, Veeam Backup & Replication performs "live" verification: creates a virtual machine using the backup of a physical machine, scans backed-up data for malware, boots VM from the backup in the isolated environment, runs tests for the VM, powers the VM off and creates a report on recovery verification results. To learn more about the logic behind SureBackup, see the How SureBackup Works section in the Veeam Backup & Replication User Guide.

Before creating the SureBackup job, check limitations for Veeam Agent backups below. Then learn how to prepare your backup infrastructure and create a SureBackup job in Creating SureBackup Job.

General Limitations

For backups created with Veeam Agent for Microsoft Windows or Veeam Agent for Linux, SureBackup has the following limitations:

- SureBackup is not supported for backup files created by backup copy jobs.
- SureBackup is not supported for backups containing drives greater than 64 TB.
- SureBackup is not supported if the Microsoft Windows system partition and boot partition of the backed-up computer are located on different drives.
- SureBackup is not supported for backups stored on the Veeam Cloud Connect repository.
- If you plan to verify computer recovery with VMware vSphere, consider the following:
  - SureBackup is not supported for backups of 4 KB sector drives.
  - SureBackup is not supported for backups of storage spaces.
  - SureBackup is not supported for backups containing more than 54 drives.

Limitations for backups created with Veeam Agent for Microsoft Windows

For backups created with Veeam Agent for Microsoft Windows, SureBackup has the following limitations:

- You must use volume-level backup of the protected computer. File-level backups are not supported. To learn more about backup types, see the Backup Types section in the Veeam Agent for Microsoft Windows User Guide.
- SureBackup is not supported for failover clusters.
- If you plan to verify computer recovery with Microsoft Hyper-V, SureBackup is not supported for application groups with computers connected to different networks.

Limitations for backups created with Veeam Agent for Linux

For backups created with Veeam Agent for Linux, SureBackup has the following limitations:

- The backed-up computer must run one of the following OSes:
  - Debian 10.13 – 11.6
  - Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10
  - RHEL 6.3 – 9.1
  - CentOS 7

  For other Linux distributions, the successful recovery verification is not guaranteed.
- If you want Veeam Backup & Replication to connect the recovered VM to the virtual network, the protected computer must run one of the following OSes:
  - Ubuntu 16.04, 18.04, 20.04, 22.04
  - RHEL 6.3 – 9.1

  Besides the OS, one of the following configuration utilities must be installed on the protected computer:
  - Netplan
  - NetworkManager
  - sysconfig
- You must use volume-level backup of the protected computer. File-level backups are not supported. To learn more about backup types, see the Backup Types section in the Veeam Agent for Linux User Guide.

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

Specification	Requirement
Hardware	CPU: x86-64 processor. Memory: 2 GB RAM or more. Memory consumption varies depending on number and size of processed disks. Disk Space: 200 MB for product installation. Network: 1 Mbps or faster. High latency and reasonably unstable WAN links are supported. System firmware: BIOS or UEFI. Drive encryption: Microsoft BitLocker (optional). 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.
OS	Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported[1]: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server Semi-Annual Channel (from version 1803 to version 20H2) • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1[2] • Microsoft Windows 11 (version 22H2) • Microsoft Windows 10 Semi-Annual Channel (from version 1803 to version 22H2)[3] • Microsoft Windows 10 Long-Term Servicing Channel (versions 2015, 2016 and 2019) • Microsoft Windows 8.1 • Microsoft Windows 7 SP1 Each Veeam Agent computer that consumes a license installed in Veeam Backup & Replication must have a unique BIOS UUID. [1] Consider the following: • Running Veeam Agent on Insider versions of Microsoft Windows Client and Server OSes is not supported.

Specification	Requirement
	• Server Core installations of Microsoft Windows Server OSes can be backed-up only by Veeam Agent backup jobs managed by the Veeam backup server. • Windows Embedded / Windows IoT OSes are supported (except for custom builds by certain vendors that do not have components required for Veeam Agent operation). [2] Veeam CBT driver is supported only if Microsoft Windows update KB3033929 is installed on the Veeam Agent computer. [3] 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 article.
Database	SQLite database engine (installed with the product).
Software	The following required 3rd party software is included in the Veeam Agent for Microsoft Windows Redistributable. 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 .NET Framework 4.5.2 • Windows Universal C Runtime Library

Veeam Agent for Microsoft Windows works with only those hard drive types that are supported by the Microsoft Windows OS. Thus, Veeam Agent supports the 512 bytes and 4 KB sector hard drives only. Other hard drive types are not supported. To learn more, see this Microsoft article.

Veeam Agent Computer (Linux)

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

Specification	Requirement
Hardware	CPU: x86-64 processor (i386 or later). Memory: 1 GB RAM or more. Memory consumption varies depending on the backup type and the total amount of backed-up data. Disk Space: 100 MB free disk space for product installation. Network: 10 Mbps or faster network connection to a backup target. System firmware: BIOS or UEFI. Disk layout: MBR or GPT. For virtual machines: Only full virtualization type is supported. Oracle VM virtual machines are supported with limitations. Virtual I/O (VirtIO) devices have experimental support status. Other containers and paravirtualized instances are not supported.
OS	**IMPORTANT!** Check considerations and limitations that apply to the list of supported OSes. Linux kernel version 2.6.32 to version 6.1 is supported. Veeam Agent supports 64-bit versions of the following distributions: • Debian 10.13 - 11.6 • Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 • RHEL 6.4 - 9.1 • CentOS 7 • Oracle Linux 6 - 9.1 (RHCK) • Oracle Linux 6 (starting from UEK R2) - Oracle Linux 8 (up to UEK R6) • Oracle Linux 8 (UEK R7) — for information on installation, see this Veeam KB article. • Oracle Linux 9 (up to 5.15.0-6.80.3.1.el9uek) • SLES 12 SP4, 12 SP5, 15 SP1 - 15 SP4 • SLES for SAP 12 SP4, 12 SP5, 15 SP1 - 15 SP4 • Fedora 36, 37 • openSUSE Leap 15.3, 15.4 • openSUSE Tumbleweed has an experimental support status. For details about experimental support, see this Veeam KB article. Veeam Agent supports 32-bit versions of RHEL 6 and Oracle Linux 6 distributions only.

Specification	Requirement
File System	**IMPORTANT!** Check considerations and limitations that apply to the list of supported file systems. Veeam Agent for Linux supports consistent snapshot-based data backup for the following file systems[1]: • Btrfs (for OSes that run Linux kernel 3.16 or later) • Ext 2/3/4 • F2FS • FAT16 • FAT32 • HFS • HFS+ • JFS • NILFS2 • NTFS • ReiserFS • XFS The supported file system (except for Btrfs) can reside on a simple volume or LVM2 volume; volumes protected with encryption software such as dm-crypt are supported. 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 resides on other file systems and volumes (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.
Software	**IMPORTANT!** Check considerations and limitations that apply to the list of supported components. Protected computer must have the following components installed: • dkms • gcc • make • perl • linux-headers (for Debian-based systems) • kernel-headers (for RedHat-based systems) • kernel-devel (for RedHat-based systems) • libudev • libacl • libattr • lvm2 • libfuse • libncurses5

Specification	Requirement
	• dmidecode • libmysqlclient • libpq5 • python3 • efibootmgr (for UEFI-based systems) • isolinux (for Debian-based systems) • syslinux (for RedHat-based systems) • btrfs-progs (for backup of Btrfs file system) • mksquashfs (for custom Veeam Recovery Media) • unsquashfs (for custom Veeam Recovery Media) • wget (for custom Veeam Recovery Media) • xorriso (for custom Veeam Recovery Media with EFI support) For file system indexing, the following utilities are required: `tar` and `gzip`.

Considerations and Limitations (Linux)

OS

- Linux kernel version 2.6.32 to version 6.1 is supported as long as you use kernels supplied by your distribution. Consider the following limitations:
  - Fedora and openSUSE Tumbleweed are supported up to kernel 6.1.
  - Linux kernel 2.6.32-754.6.3 in CentOS / RHEL and Oracle Linux (RHCK) is not supported.
- Only GA versions of the supported distributions that have been released before the current version of Veeam Agent for Linux are supported.
- The Linux OS must be set up to receive software updates from the default repositories enabled in the OS after installation.
- For cloud-based installations that use customized kernels (such as Linux distributions deployed from AWS Marketplace or Azure Marketplace), the `veeamsnap` kernel module has experimental support status. For details about experimental support, see this Veeam KB article.
- Automatic Veeam Agent deployment from the Veeam backup console is not supported for the following distributions:
  - Fedora
  - openSUSE Tumbleweed

  You need to install Veeam Agent for Linux directly on a target computer. For details, see the Installing Veeam Agent for Linux section in the Veeam Agent for Linux User Guide.
- RHEL, CentOS, and Oracle Linux (RHCK) are supported up to certain kernel versions. For details, see this Veeam KB article.

File System

- Veeam Agent for Linux does not back up volumes that reside on USB devices and SD cards.
- Veeam Agent for Linux does not back up LVM snapshots.
- File-level backup has the following limitations:
  - Total size of all file systems must not exceed 218 TB. This limitation applies to all file systems where files you plan to back up are located.
  - Size of a file included in a file-level backup must not exceed 16 TB.
  - Name of a file must not be larger than 254 bytes.

    Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more.
- Veeam Agent for Linux supports backup of extended attributes with the following limitations:
  - Veeam Agent for Linux backs up extended attributes only with the following public namespaces: system, security, trusted, and user.
  - All extended attribute names and values of a file must not exceed 4096 bytes (size of a default ext4 file system block). Veeam Agent does not back up attributes exceeding the limit.

    For the kernel version 4.13 or later, if a value of extended attribute exceeds the limit, Veeam Agent uses the *ea_inodes* feature. Backups created using the *ea_inodes* feature cannot be mounted on kernel versions up to 4.12.
- Backup of file and directory attributes (for example, a — append only, c — compressed, and so on) is not supported.
- Each volume included in a backup must have a unique UUID.
- The `veeamsnap` 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.
- You cannot back up an entire system image or specific volumes of computers used as cluster nodes. Only snapshot-less file-level backup of cluster nodes is supported. That includes backup of computers that use shared disks, clustered file systems, or clustered LVM.
- Certain limitations for Dell PowerPath configuration apply. To learn more, see this Veeam KB article.
- BFQ I/O scheduler is not supported.
- Sparse files are not supported. Veeam Agent for Linux backs up and restores sparse files as regular files.

Software

> **IMPORTANT**
>
> Linux user account used to work with Veeam Agent for Linux installed on the protected computer must have the `/bin/bash` shell set as the default shell.

- 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.
- The following packages are not required for CentOS, RHEL and SLES distributions if a pre-built binary `veeamsnap` package is to be installed.
  - dkms
  - gcc
  - make
  - perl
  - kernel-headers (for RedHat-based systems)
  - kernel-devel (for RedHat-based systems)

  For details, see the Installing Veeam Agent for Linux section in the Veeam Agent for Linux User Guide.
- Version of the following packages varies according to the Linux kernel version that you use:
  - linux-headers (for Debian-based systems)
  - kernel-headers (for RedHat-based systems)
  - kernel-devel (for RedHat-based systems)
- For openSUSE and SLES distributions, either of the following packages is required: `libncurses5` or `libncurses6`.
- The `dmidecode` package is 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.
- The `libmysqlclient` package is required to process MySQL database system located on the Veeam Agent server. Package version varies according to the MySQL database system version that you use.
- The `libpq5` package is required to process PostgreSQL database system located on the Veeam Agent server.
- The `python3` package or another RPM package providing a `/usr/bin/python3` binary is required for CentOS, RHEL 7.0 and later distributions if a pre-built binary `kmod-veeamsnap` package is to be installed.
- The `btrfs-progs` package version 3.16 or later is required.

Veeam Agent Computer (IBM AIX)

A computer that you want to protect with Veeam Agent for IBM AIX must meet the following requirements:

Specification	Requirement
Hardware	Memory: 1 GB RAM. For information about RAM requirements for backup of a great number of files, see the RAM Requirements for Large-Scale Environments section in the Veeam Agent for IBM AIX User Guide. Disk space: 1.5 GB free disk space for product installation. Network: 10 Mbps or faster network connection to a backup target.
OS	IBM AIX versions starting from version 7.1 up to the latest update of version 7.3 are supported. **Note:** • IBM AIX 6.1 is supported starting from Technology Level 5 (TL 5). • Backup of a Virtual I/O Server (VIOS) is not supported. • Only GA versions of the IBM AIX operating system that have been released before the Veeam Agent for IBM AIX 4.0 are are supported.
File System	All file systems supported by the supported operating systems. **Note:** • Total size of all file systems included in a file-level backup must not exceed 218 TB. • The maximum number of files in one backup job is 20,000,000. To back up a greater number of files, use multiple jobs. • Size of a file in a backup must not exceed 16 TB. • Name of a file in a backup must not be larger than 254 bytes. Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more. • Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files. • JFS external snapshots are not supported.
Software	The following utilities must be installed on the machine: • `mlocate` (version 0.26-1) — required for file system indexing. It is provided along with the product in the product installation media. • `tar` — required for file system indexing, exporting and rotating logs. It is installed with the product. • `gzip` — required for file system indexing, exporting and rotating logs. It must be installed separately. • `mkisofs` — required for creating Veeam recovery Media.

Specification	Requirement
	[For IBM AIX 7.3, 7.2 and 7.1 TL1 or higher] This utility is pre-installed in the OS and does not require separate installation. [For IBM AIX 7.1 TL0 and 6.1] You must install version 1.13 of the mkisofs utility.

AIX Environment

The `LIBPATH` AIX environment variable on the Veeam Agent computer must be set to blank (default value). If a different value is specified for this variable, you must make adjustments to the AIX environment for proper operation of Veeam Agent. For details, see this Veeam KB article.

Veeam Agent Computer (Oracle Solaris)

A computer that you want to protect with Veeam Agent for Oracle Solaris must meet the following requirements:

Specification	Requirement
Hardware	CPU: Oracle SPARC or Intel x86 processor. Memory: 1 GB RAM. For information about RAM requirements for backup of a great number of files, see the RAM Requirements for Large-Scale Environments section in the Veeam Agent for Oracle Solaris User Guide. Disk space: 250 MB free disk space for product installation. Network: 10 Mbps or faster network connection to a backup target.
OS	Oracle Solaris 10 – 11.4 operating systems on machines based on the SPARC and Intel x86 architecture are supported. **Note:** Only GA versions of the Oracle Solaris OS that have been released before the Veeam Agent for Oracle Solaris version 4.0 are supported.
File System	All file systems supported by the supported operating systems. **Note:** • Total size of all file systems included in a file-level backup must not exceed 218 TB. • The maximum number of files in one backup job is 20,000,000. To back up a greater number of files, use multiple jobs. • Size of a file in a backup must not exceed 16 TB. • Name of a file in a backup must not be larger than 254 bytes. Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more. • Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files.

Specification	Requirement
Software	For file system indexing, the following utilities are required: `tar`, `mlocate` and `gzip`. • `mlocate` (version 0.26-1 or later) – required for file system indexing. If your system does not have the mlocate utility, you can install it from the product installation media. • `tar` - required for file system indexing, exporting and rotating logs. It is installed with the product. • `gzip` – required for file system indexing, exporting and rotating logs. It must be installed separately. • `xorriso` – required for creating Veeam Recovery Media. Oracle Solaris minimal install (Core System Support Software Group) requires adding the following packages: `SUMWtoo`, `SUNWzoneu` and `SUNWzoner`.

Veeam Agent Computer (macOS)

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

Specification	Requirement
Hardware	The protected macOS computer must meet the following hardware requirements: • CPU: x64 or ARM Apple-branded hardware* • Disk Space: 450 MB free disk space for product installation • Network: 10 Mbps or faster network connection to a backup target * On a macOS computer with the ARM Apple-branded hardware, the product is running using the Rosetta Translation Environment.
OS	Veeam Agent supports the following macOS versions: • 13 Ventura • 12 Monterey • 11 Big Sur • 10.15 Catalina • 10.14 Mojave • 10.13.6 High Sierra
File System	Veeam Agent supports consistent data backup with snapshot for the APFS file system. The following file systems can be backed up in the snapshot-less mode: • HFS+ • MS-DOS (FAT) • exFAT • NTFS • FAT32 • SMB Consider the following: • Sortware RAID is not supported. • Total size of all file systems included in a backup must not exceed 218 TB. • Size of a file in a backup must not exceed 16 TB. • Name of a file in a backup must not be larger than 254 bytes. Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more.

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 12 or later backup repository
- Veeam Cloud Connect 12 or later 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

  > **IMPORTANT**
  >
  > [For Veeam Agent for Microsoft Windows] We do not recommend targeting a backup job at the storage device with the exFAT file system. If the protected computer runs Microsoft Windows 10 or Microsoft Windows Server 2019 and later, this configuration may lead to the backup data corruption caused by the exFAT file system issue.

- 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 and Unix computers only)
- On-premises and cloud-based object storage
- Veeam Backup & Replication 12 backup repository
- Veeam Cloud Connect 12 cloud repository (excluding backups of Unix computers)

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.
- For communication between Veeam backup infrastructure and computers you want to back up, one of the following authentication protocols is required:
  - Windows New Technology LAN Manager (NTLM)
  - Kerberos
- Domain names of all managed servers added to the Veeam backup infrastructure and computers you want to back up must be resolvable into IPv4 or IPv6 addresses.

  Keep in mind that for Veeam Agent computers that are included in a protection group for pre-installed Veeam Agents, only Veeam Backup & Replication server must be resolvable into IPv4 or IPv6 address.

IMPORTANT

Veeam products support the Kerberos authentication protocol and IPv6 addresses starting from the following versions:

- Veeam Backup & Replication 12
- Veeam Agent for Microsoft Windows 6.0
- Veeam Agent for Linux 6.0
- Veeam Agent for Mac 2.0
- Veeam Agent for IBM AIX 4.0
- Veeam Agent for Oracle Solaris 4.0

Veeam Backup & Replication 12 will not be able to use the Kerberos autentication protocol and IPv6 addresses to communicate with earlier versions of Veeam Agents. To start using these features, upgrade Veeam Agents. To learn more, see Upgrading Veeam Agent.

To learn more about new features see the following sections of the Veeam Backup & Replication User Guide:

- Kerberos Authentication
- IPv6 Support

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 computers (servers and workstations) with Veeam Agents. 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.

  Keep in mind that you cannot use Veeam Agent for Unix to protect Unix computers with the Community edition of the product. To protect such computers, you must use Enterprise Plus edition of the product.

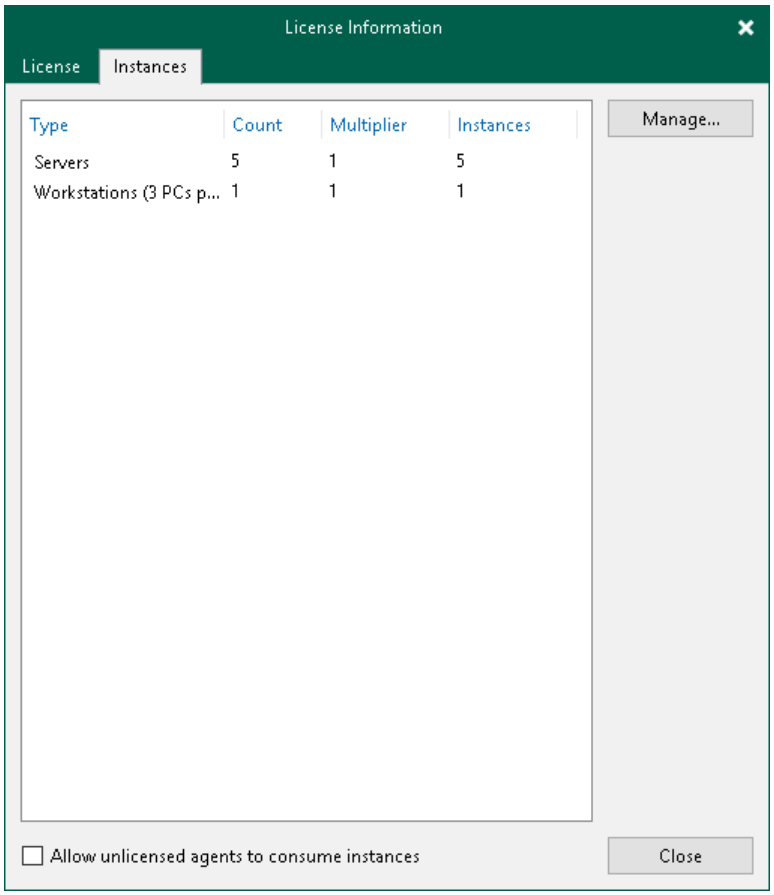
For more information on Veeam Backup & Replication licensing, see the Licensing section in the Veeam Backup & Replication User Guide.

Managing Instance Consumption by Veeam Agents

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 restrict instance consumption by Veeam Agents:

1. From the main menu, select **License**.
2. In the **License Information** window, click the **Instances** tab.
3. On the **Instances** tab, clear the **Allow unlicensed agents to consume instances** check box.
4. Click **Close**.



Permissions

If you plan to use object storage in the Veeam Agent management infrastructure, make sure user accounts that you plan to use have the required permissions. Keep in mind that depending on the functionality that you use, the list of required permissions differ. Make sure user accounts have permissions described in the following subsections:

- Back Up Cloud Machines
- Back Up to Object Storage

Backing Up Cloud Machines

The list of permissions differs depending on the type of the cloud machine you plan to back up:

- Microsoft Azure virtual machines

  If you plan to back up Microsoft Azure virtual machines, all required permissions are assigned when you add a Microsoft Azure Compute account to Veeam Backup & Replication. To learn more, see the Creating New Azure AD Application section in the Veeam Backup & Replication User Guide.

- Amazon EC2 instances

  If you plan to back up Amazon EC2 instances, make sure the user account that you plan to use have the following permissions:

```
{
 "ssm:SendCommand",
 "ssm:DescribeInstanceInformation",
 "ssm:UpdateManagedInstanceRole",
 "ssm:GetCommandInvocation",
 "iam:GetRole",
 "iam:PassRole",
 "iam:AddRoleToInstanceProfile",
 "iam:CreateRole",
 "iam:CreateInstanceProfile",
 "iam:AttachRolePolicy",
 "iam:SimulatePrincipalPolicy",
 "ec2:DescribeInstances",
 "ec2:AssociateIamInstanceProfile",
 "ec2:DescribeIamInstanceProfileAssociations",
 "sqs:*"
}
```

Backing Up to Object Storage

Besides the general permissions listed in the Using Object Storage Repositories section in the Veeam Backup & Replication User Guide, some additional permissions are required for object storage in the Veeam Agent management infrastructure. The list of required permissions differs depending on the selected object storage and the way you set your backup infrastructure. To learn more, see the following subsections:

- Amazon S3 or S3 compatible storage (including IBM Cloud and Wasabi Cloud)
- Google Cloud

Amazon S3 or S3 Compatible Storage (Including IBM Cloud, Wasabi Cloud)

Consider the following:

- Make sure the account you are using has access to Amazon buckets and folders.
- The *ListAllMyBuckets* permission is not required if you specify the bucket name explicitly at the Bucket step of the New Object Repository wizard.
- If you plan to use Amazon S3 storage with immutability enabled, see permissions required for immutability in the Using Object Storage Repositories section in the Veeam Backup & Replication User Guide. To learn more about immutability, see Backup Immutability.

The list of permissions below is required for the following configurations:

- You plan to back up data to the Amazon S3 storage.
- You selected direct connection in the object storage settings. To learn more, see the Adding Amazon S3 Object Storage section in the Veeam Backup & Replication User Guide.

or

- You plan to back up data to the S3 compatible storage.
- Direct connection is selected in the object storage settings. To learn more, see the Specify Object Storage Account section in the Veeam Backup & Replication User Guide.
- The **Provided by IAM/STS object storage capabilities** option is selected for the object storage. To learn more, see the Managing Permissions for S3 Compatible Object Storage section in the Veeam Backup & Replication User Guide.

If you plan to back up data using one of the configurations above, make sure the user account that you plan to use have the following permissions:

```
{
 "iam:GetPolicyVersion",
 "iam:DeleteAccessKey",
 "iam:GetPolicy",
 "iam:AttachUserPolicy",
 "iam:DeleteUserPolicy",
 "iam:DeletePolicy",
 "iam:DeleteUser",
 "iam:ListUserPolicies",
 "iam:CreateUser",
 "iam:TagUser",
 "iam:CreateAccessKey",
 "iam:CreatePolicy",
 "iam:ListPolicyVersions",
 "iam:GetUserPolicy",
 "iam:PutUserPolicy",
 "iam:ListAttachedUserPolicies",
 "iam:GetUser",
 "iam:CreatePolicyVersion",
 "iam:DetachUserPolicy",
 "iam:DeletePolicyVersion",
 "iam:ListAccessKeys",
 "iam:SetDefaultPolicyVersion"
}
```

Google Cloud

The list of permissions below is required for the following configurations:

- You plan to back up data to the Google Cloud storage.
- You configured Helper Appliance in the object storage settings. To learn more, see the Configuring Helper Appliance section in the Veeam Backup & Replication User Guide.
- You selected direct connection in the object storage settings. To learn more, see the Specify Object Storage Account section in the Veeam Backup & Replication User Guide.

If you plan to back up data using the configuration above, make sure the user account that you specify in the Helper Appliance settings have the following permissions:

```
(
 "iam.serviceAccounts.create",
 "iam.serviceAccounts.delete",
 "iam.serviceAccounts.get",
 "storage.buckets.get",
 "storage.buckets.getIamPolicy",
 "storage.buckets.list",
 "storage.buckets.setIamPolicy",
 "storage.hmacKeys.create",
 "storage.objects.create",
 "storage.objects.delete",
 "storage.objects.get",
 "storage.objects.list",
 "iam.serviceAccounts.list",
 "storage.buckets.update",
 "storage.hmacKeys.delete",
 "storage.hmacKeys.list"
}
```

Ports

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

Communication Between Veeam Backup & Replication Components

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

For general requirements for ports that must be opened to ensure proper communication of the backup server with Veeam Cloud Connect infrastructure components, see the Ports section in the Veeam Cloud Connect Guide.

In addition to general port requirements applicable to a backup server, the following network ports that must be opened to enable proper communication between Veeam Backup & Replication components .

From	To	Protocol	Port	Notes
Veeam Backup Server	Veeam Agent Computer (Microsoft Windows)	TCP	6184+	Default port used for communication with the Veeam Agent for Microsoft Windows Service. If port 6184 is already in use, Veeam Agent for Microsoft Windows Service tries to use the next port number in the allocated range (6184 to 6194). Once the service takes the next available port, it makes it the default port for all subsequent connections.
		TCP UDP	135, 137 to 139, 445, 6160, 11731	Default ports used for communication with the Veeam Installer Service. Port 135 is used for WMI queries. WMI queries are mandatory to back up failover clusters and perform file-level restore and optional to provide faster Veeam Agent deployment. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS. Ports 137 to 139 and 445 are used during restore started from the Veeam Backup & Replication console. Ports 6160 and 11731 are used to deploy Veeam Agent on the computer and to provide faster restore. If the backup repository server role and the mount server role are assigned to different servers in your infrastructure, you must open ports described in the Mount Server Connections subsection of the Veeam Backup & Replication User Guide.

From	To	Protocol	Port	Notes
		TCP	2500 to 3300	[For Microsoft SQL logs shipping] Ports used to collect Microsoft SQL logs from the Veeam Agent computer.
		TCP	6167, 2500 to 3300	[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.
		TCP	6211	[For storage snapshots support] Port used for communication with the hardware VSS provider. For more information, see Storage Snapshots Support.
		TCP	6160, 11731	Port used for the volume-level restore.
	Veeam Agent Computer (Linux)	TCP	22, 6160, 6162	Port 22 is used to establish an SSH connection from the Veeam Backup Server to the Veeam Agent computer. Ports 6160 and 6162 are used for default connection to the Veeam Agent computer using Veeam Transport Service and Veeam Deployer Service.
		TCP	6162	Default port used by the Veeam Data Mover.
		TCP	2500 to 3300	Default range of ports used for communication between Veeam Agent components during data transmission. For every TCP connection that a backup job uses, one port from this range is assigned.
	Distribution Server	TCP UDP	135, 137 to 139, 445, 6160, 11731	Ports on a Microsoft Windows server used for deploying the Distribution Server component. Port 135 is optional. This port is used to provide faster Veeam Agent deployment. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.

From	To	Protocol	Port	Notes
				Ports 6160 and 11731 are used by the Veeam Installer Service. These ports together with port 445 are mandatory to deploy the Distribution Server component.
		TCP	49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article.
		TCP	9380	Default port used for communication with the Veeam Distribution Service.
	Backup Proxy	TCP	6211	[For storage snapshots support] Port used for communication with the hardware VSS provider. For more information, see Storage Snapshots Support.
Distribution Server	Veeam Agent Computer (Microsoft Windows)	TCP	49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article. The port range is required for communication with the Veeam Installer Service.
		TCP UDP	6160, 11731	Ports on the Veeam Agent computer used for deploying Veeam Agent.
	Veeam Agent Computer (Linux)	TCP	22, 6160, 6162	Port 22 is used to establish an SSH connection for the purpose of Veeam Agent packages transmission and deployment control. After Veeam Agent is deployed, ports 6160 and 6162 are used for default connection to Veeam Agent computer using Veeam Transport Service and Veeam Deployer Service.
Veeam Agent Computer (Microsoft Windows)	Veeam Backup Server	TCP	10005	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.

From	To	Protocol	Port	Notes
Veeam Agent Computer (Linux, Unix, macOS)		TCP	10006	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.

Communication Between Veeam Agent Components

The following table describes network ports that must be opened to enable proper communication between Veeam Agent components.

From	To	Protocol	Port	Notes
Veeam Agent Computer (Microsoft Windows)	Veeam Agent Computer (Microsoft Windows)	TCP	9395+, 6183+	Ports used locally on the Veeam Agent computer for communication between Veeam Agent components and Veeam Agent for Microsoft Windows Service. If port 9395 or 6183 is already in use, Veeam Agent for Microsoft Windows Service will try to use the next port number.
Veeam Agent Computer (Linux, Unix, macOS)	Veeam Agent Computer (Linux, Unix, macOS)	TCP	2500 to 3300	Default range of ports used locally for communication between Veeam Agent components during data transmission. For every TCP connection that a backup job uses, one port from this range is assigned.

Communication with Veeam Backup Repositories

The following table describes network ports that must be opened to ensure proper communication between Veeam Agent and Veeam backup repositories.

From	To	Protocol	Port	Notes
Veeam Agent Computer	Linux server performing the role of a backup repository	TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
	Microsoft Windows server performing the role of a backup repository	TCP	49152 to 65535 (for Microsoft Windows 2008 and newer)	Dynamic RPC port range. For more information, see this Microsoft KB article.
		TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
	Shared folder CIFS (SMB) share	TCP UDP	137 to 139, 445	Ports used as a transmission channel from the Veeam Agent computer to the target CIFS (SMB) share. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.
	Gateway Microsoft Windows server	TCP UDP	137 to 139, 445	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. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.
		TCP	49152 to 65535	Dynamic RPC port range. For more information, see this Microsoft KB article.

From	To	Protocol	Port	Notes
		TCP	2500 to 3300	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.

Communication with Veeam Cloud Connect Repositories

The following table describes network ports that must be opened to ensure proper communication between Veeam Agents and Veeam Cloud Connect repositories.

From	To	Protocol	Port	Notes
Veeam Agent Computer (Microsoft Windows, Linux, macOS)	Cloud gateway	TCP	6180	Port on the cloud gateway used to transport Veeam Agent data to the Veeam Cloud Connect repository.
	Certificate Revocation Lists	TCP	80 or 443 (most popular)	Veeam Agent computer needs access to CRLs (Certificate Revocation Lists) of the CA (Certification Authority) who issued a certificate to the Veeam Cloud Connect service provider. Generally, information about CRL locations can be found on the CA website.

Communication with Object Storage

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

From	To	Protocol	Port/Endpoint	Notes
Gateway server	Amazon S3 object storage	TCP	443	Port and endpoints used for communication with Amazon S3 object storage.
		HTTPS	**AWS service endpoints:** • *.amazonaws.com (for both *Global* and Government regions) • *.amazonaws.com.cn (for *China* region) A complete list of connection endpoints can be found in AWS Documentation.	
		TCP	80	Port and endpoints used to verify the certificate status. Keep in mind that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself.
		HTTP	**Certificate verification endpoints:** • *.amazontrust.com	
	Microsoft Azure object storage	TCP	443	Port and endpoints used for communication with Microsoft Azure object storage. Keep in mind that the <xxx> part of the address must be replaced with your actual storage account URL, which can be found in the Azure management portal.
		HTTPS	**Cloud endpoints:** • xxx.blob.core.windows.net (for *Global* region) • xxx.blob.core.chinacloudapi.cn (for *China* region) • xxx.blob.core.cloudapi.de (for *Germany* region) • xxx.blob.core.usgovcloudapi.net (for *Government* region)	
		TCP	80	Port and endpoints used to verify the certificate status.

From	To	Protocol	Port/Endpoint	Notes
		HTTP	**Certificate verification endpoints:** • ocsp.digicert.com • ocsp.msocsp.com • *.d-trust.net	Consider the following: • Certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself. • The **.d-trust.net* endpoint is used for the *Germany* region only.
	Google Cloud storage	TCP	443	Port and endpoints used for communication with Google Cloud storage.
		HTTPS	**Cloud endpoints:** • storage.googleapis.com A complete list of connection endpoints can be found in this Google article.	
		TCP	80	Port and endpoints used to verify the certificate status. Keep in mind that certificate verification endpoints (CRL URLs and OCSP servers) are subject to change. The actual list of addresses can be found in the certificate itself.
		HTTP	**Certificate verification endpoints:** • ocsp.pki.goog • pki.goog • crl.pki.goog	
	IBM Cloud object storage	TCP/HTTPS	Customizable and depends on device configuration	Port and endpoints used for communication with IBM Cloud object storage.

From	To	Protocol	Port/Endpoint	Notes
	S3 compatible object storage	TCP/HTTPS	Customizable and depends on device configuration	Port and endpoints used for communication with S3 compatible object storage.

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.

Specification	Requirement
Microsoft Active Directory Domain Controllers	The following versions of Microsoft Active Directory Domain Services servers (domain controllers) are supported: • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 SP1 Minimum supported domain and forest functional level is Microsoft Windows Server 2003.
Microsoft Exchange	The following versions of Microsoft Exchange are supported: • Microsoft Exchange 2019 • Microsoft Exchange 2016 • Microsoft Exchange 2013 SP1 • Microsoft Exchange 2013
Microsoft SharePoint	The following versions of Microsoft SharePoint Server are supported: • Microsoft SharePoint Server Subscription Edition • Microsoft SharePoint Server 2019 • Microsoft SharePoint Server 2016 • Microsoft SharePoint Server 2013 All editions are supported (Foundation, Standard, Enterprise).

Specification	Requirement
Microsoft SQL Server	The following versions of Microsoft SQL Server are supported: • Microsoft SQL Server 2022 • Microsoft SQL Server 2019 • Microsoft SQL Server 2017 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2014 SP3 • Microsoft SQL Server 2012 SP4 • Microsoft SQL Server 2008 R2 SP3 • Microsoft SQL Server 2008 SP4 All editions of Microsoft SQL Server except LocalDB are supported.
Oracle	Oracle Database versions 11g to 21c are supported for the following operating systems (32-bit and 64-bit architecture): • Microsoft Windows Server 2022 • 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!** • 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. • 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, MySQL, and PostgreSQL database systems. System requirements for database processing are listed in the following table.

Specification	Requirement
Oracle	• Oracle Database versions 11g to 21c 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.
MySQL	• MySQL database system versions 5.6 to 8.0 are supported. • Configurations with multiple MySQL installations and/or instances on the same machine are not supported. • MySQL Cluster versions are not supported.
PostgreSQL	• PostgreSQL database system versions 12.0 to 15.2 are supported. • Configurations with multiple PostgreSQL installations and/or instances on the same server are not supported.

Supported Veeam Agents

The following tables describe what Veeam Agents are supported by the Veeam Backup & Replication depending on the product usage scenario.

Veeam Backup & Replication 12 (build 12.0.0.1420) supports the following Veeam Agents:

Scenario	Veeam Agent for Microsoft Windows Version	Veeam Agent for Linux Version	Veeam Agent for IBM AIX Version	Veeam Agent for Oracle Solaris Version	Veeam Agent for Mac Version	Description
Veeam Agent upgrade	4.0 - 4.0.2	4.0 - 4.0.1	N/A	N/A	N/A	Veeam Backup & Replication 12 can detect these versions of Veeam Agent, but does not support backup operations for them. To start working with Veeam Backup & Replication 12, you must upgrade Veeam Agents. To learn more, see Upgrading Veeam Agents.
Veeam Agent backup	5.0 - 6.0	5.0 - 6.0	3.0 - 4.0	3.0 - 4.0	1.0 - 2.0	Veeam Backup & Replication 12 supports backup operations for these Veeam Agent versions.
Automated Veeam Agent deployment from the Veeam backup console	6.0	6.0	N/A	N/A	N/A	If you set up Veeam Backup & Replication 12 to deploy or upgrade Veeam Agents on protected computers included in a protection group, these Veeam Agent versions are deployed. To learn more, see Protected Computers Discovery and Veeam Agent Deployment.
Manual Veeam Agent deployment using external tools	6.0	6.0	4.0	4.0	2.0	If you set up Veeam Backup & Replication 12 to generate Veeam Agent setup files for a manual installation, setup files for these Veeam Agent versions are generated. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

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, Working with 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 and policies.

   You can start, stop, enable and disable Veeam Agent backup jobs and policies to administer data protection operations on protected computers. To learn more, see Working with Veeam Agent Backup Jobs and Policies.

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 security settings 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:

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

Keep in mind that default security settings are only for testing and evaluation purposes. To prevent potential security issues, you can change security settings. For example, you can use a custom TLS certificate and verification of Linux host SSH fingerprints.

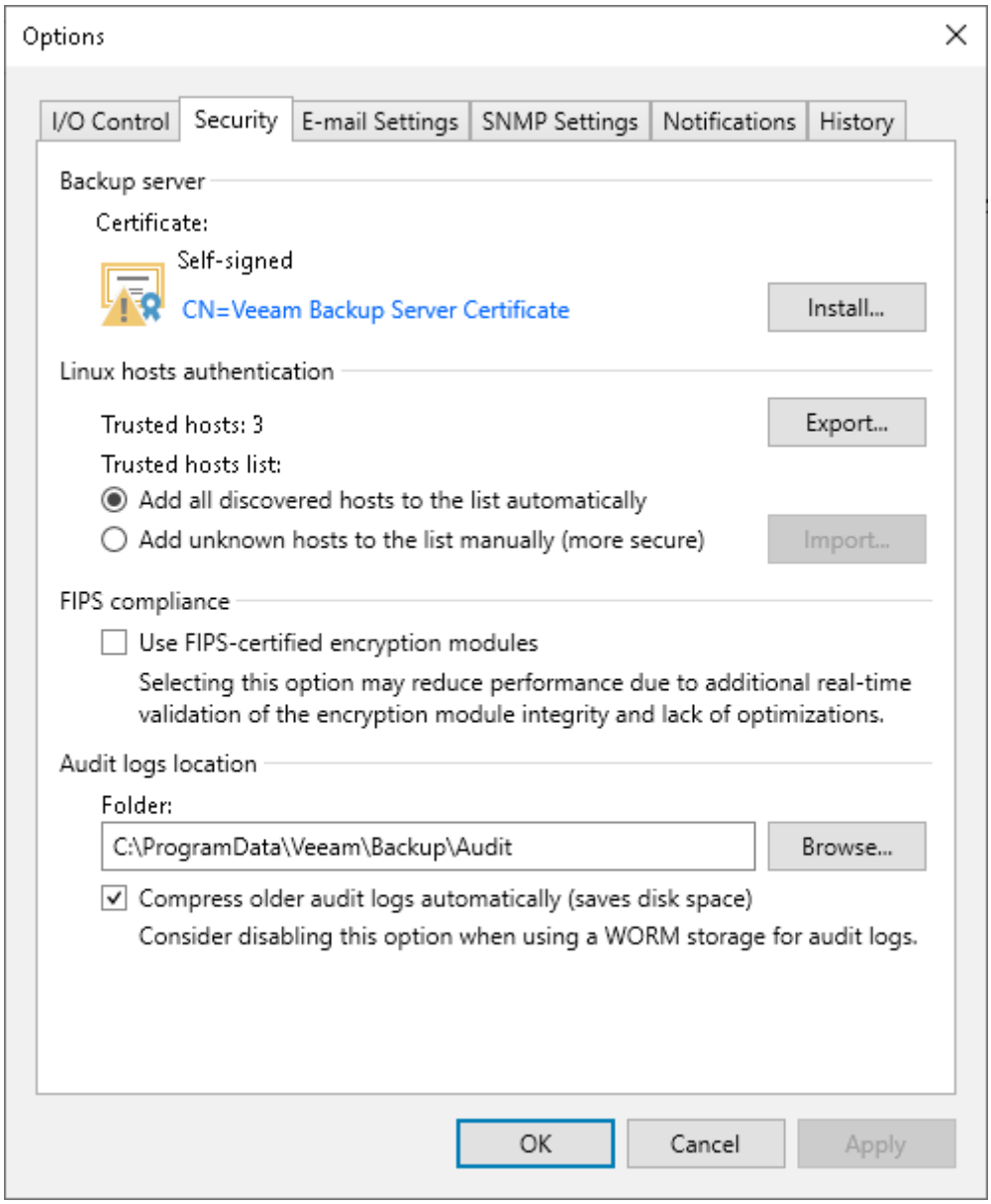
To specify the security settings, do the following:

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 (more secure)** — 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.

   Computers that are not in the list of trusted hosts cannot connect to the Veeam backup server and download Veeam Agent for Linux installation packages during discovery.
5. Click **OK**.

TIP

To learn more about other security settings available on the **Security** tab, see the Configuring Security Settings section in the Veeam Backup & Replication User Guide.



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

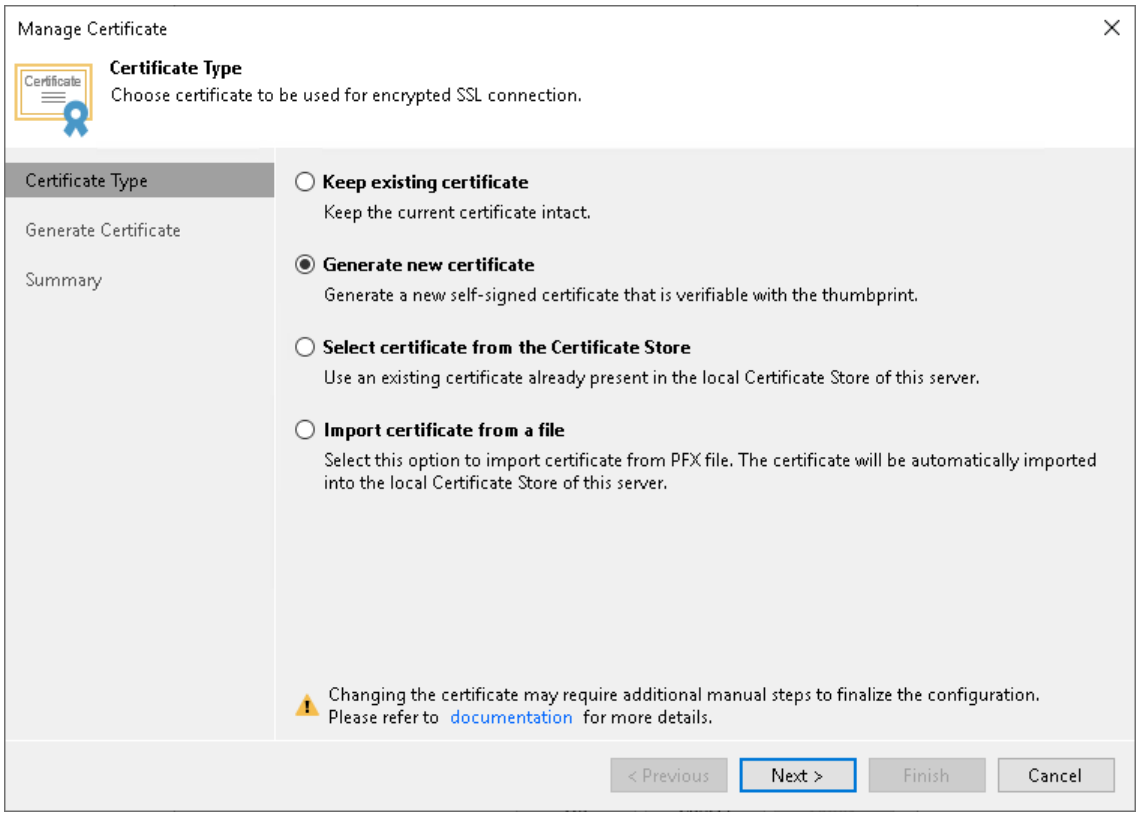
If you use a self-signed TLS certificate generated by Veeam Backup & Replication, you do not need to take any additional actions to deploy the TLS certificate on a protected computer. When Veeam Backup & Replication discovers a protected computer, a matching TLS certificate with a public key is installed 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.

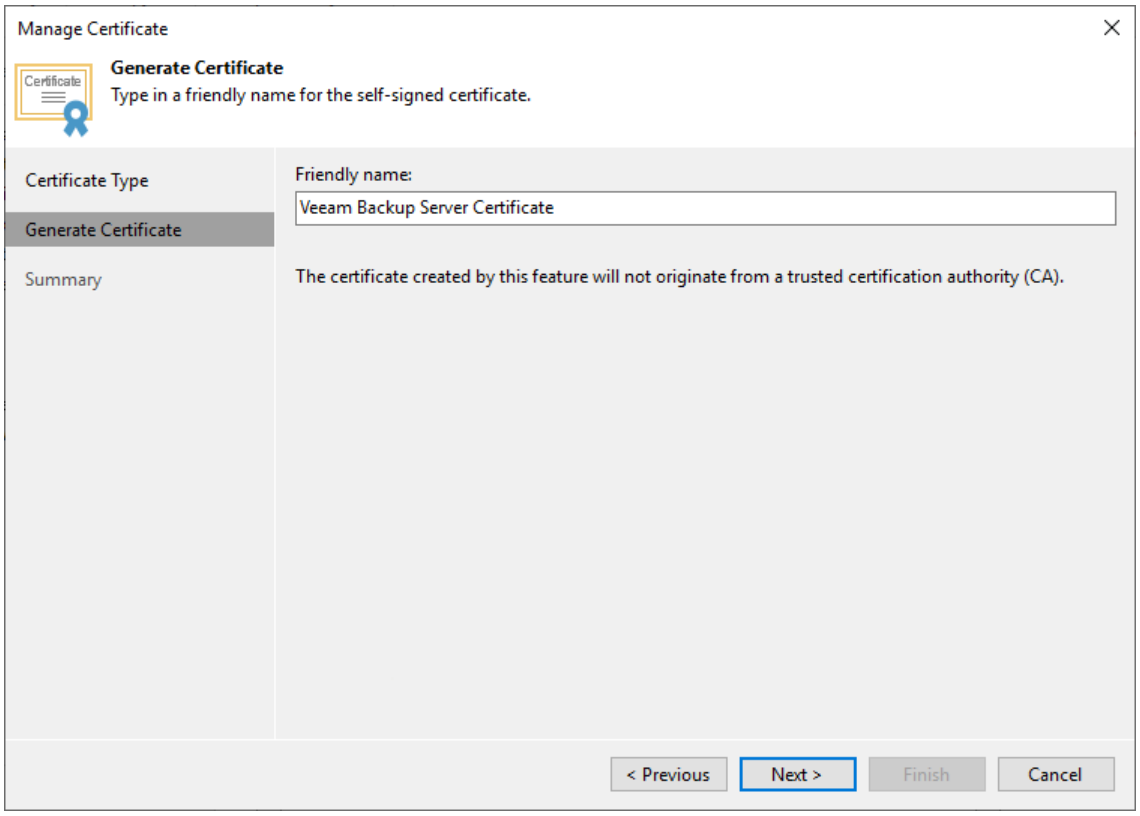
To generate a self-signed TLS certificate:

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**.

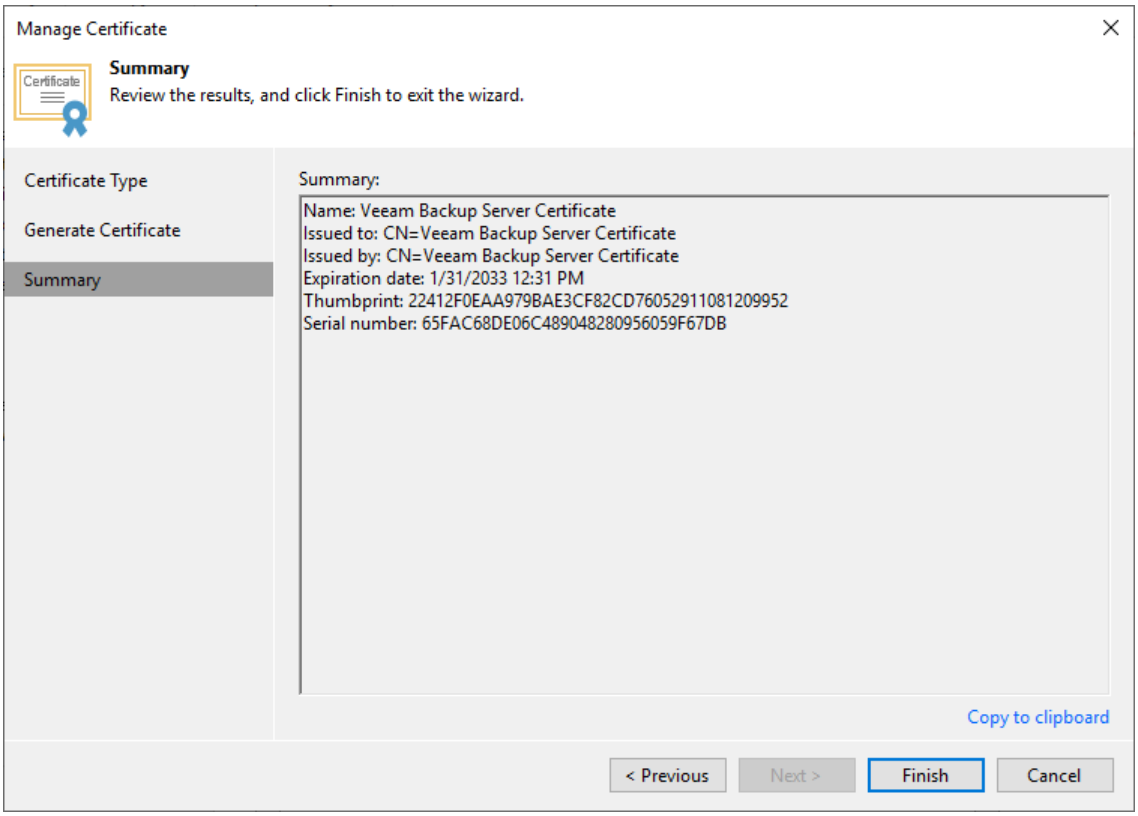


5. At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.



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.

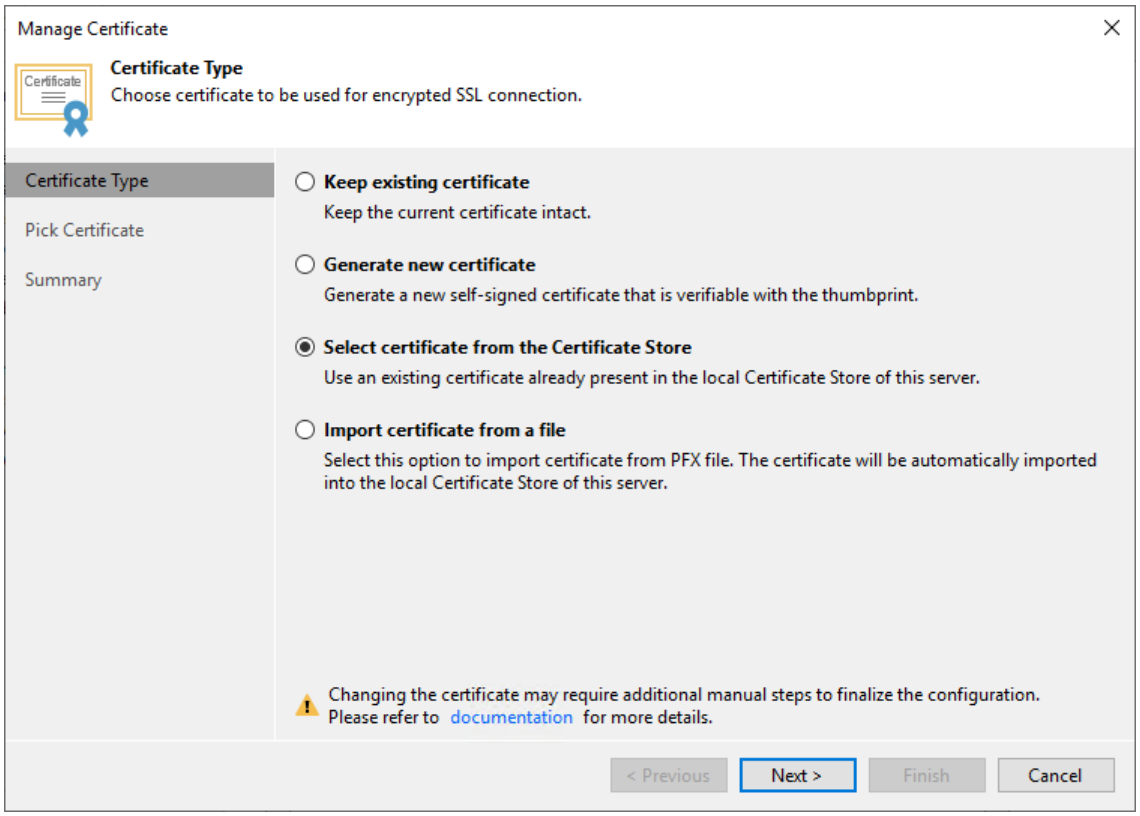


Importing Certificates from Certificate Store

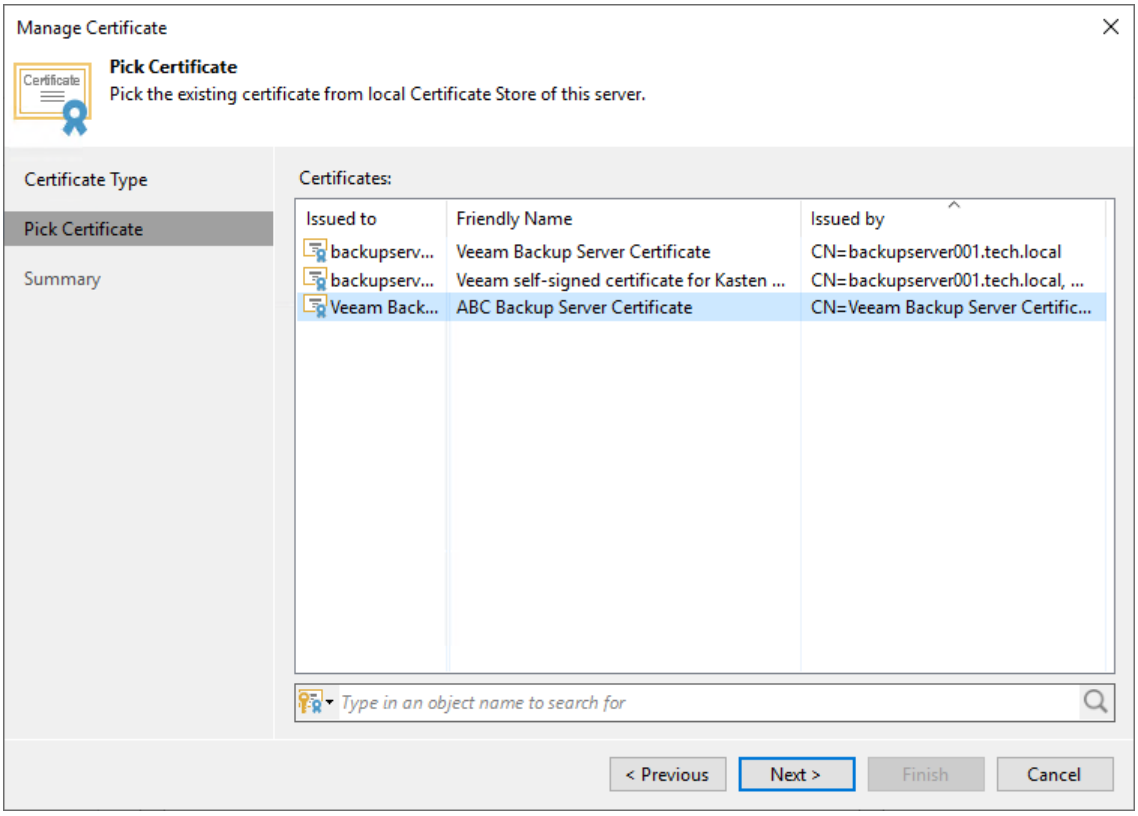
If your organization has a TLS certificate signed by a CA and the TLS certificate is located in the Microsoft Windows Certificate store, you can use this certificate for authenticating parties in the Veeam Agent management infrastructure.

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**.



5. At the **Pick Certificate** step of the wizard, select a TLS certificate that you want to use. You can select only certificates that contain both a public key and a private key. Certificates without private keys are not displayed in the list.



6. At the **Summary** step of the wizard, review the certificate properties.
7. Click **Finish** to apply the certificate.

Importing Certificates from PFX Files

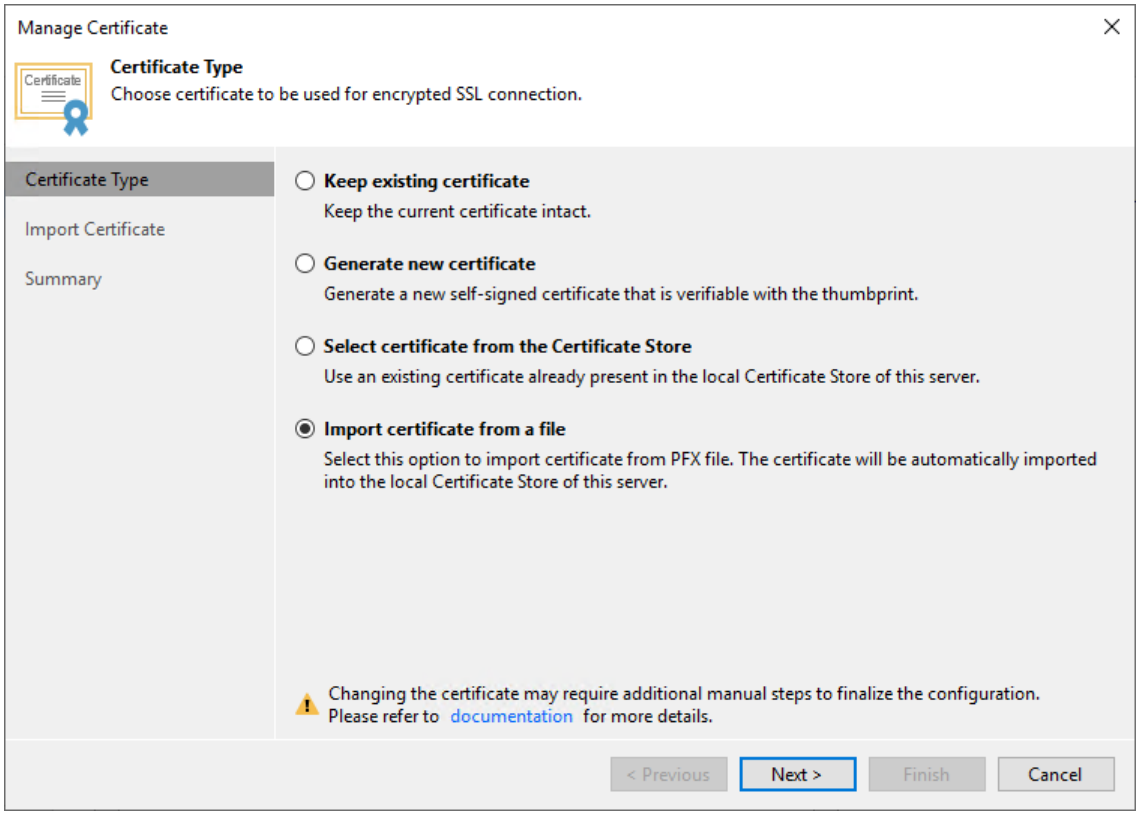
You can import a TLS certificate in the following situations:

- Your organization uses a TLS certificate signed by a CA and you have a copy of this certificate in a file of PFX format.
- You have generated a self-signed TLS certificate in the PFX format with a third-party tool and you want to import it to Veeam Backup & Replication.

> **IMPORTANT**
>
> The TLS certificate must pass validation on the Veeam backup server. In the opposite case, you will not be able to import the TLS certificate.

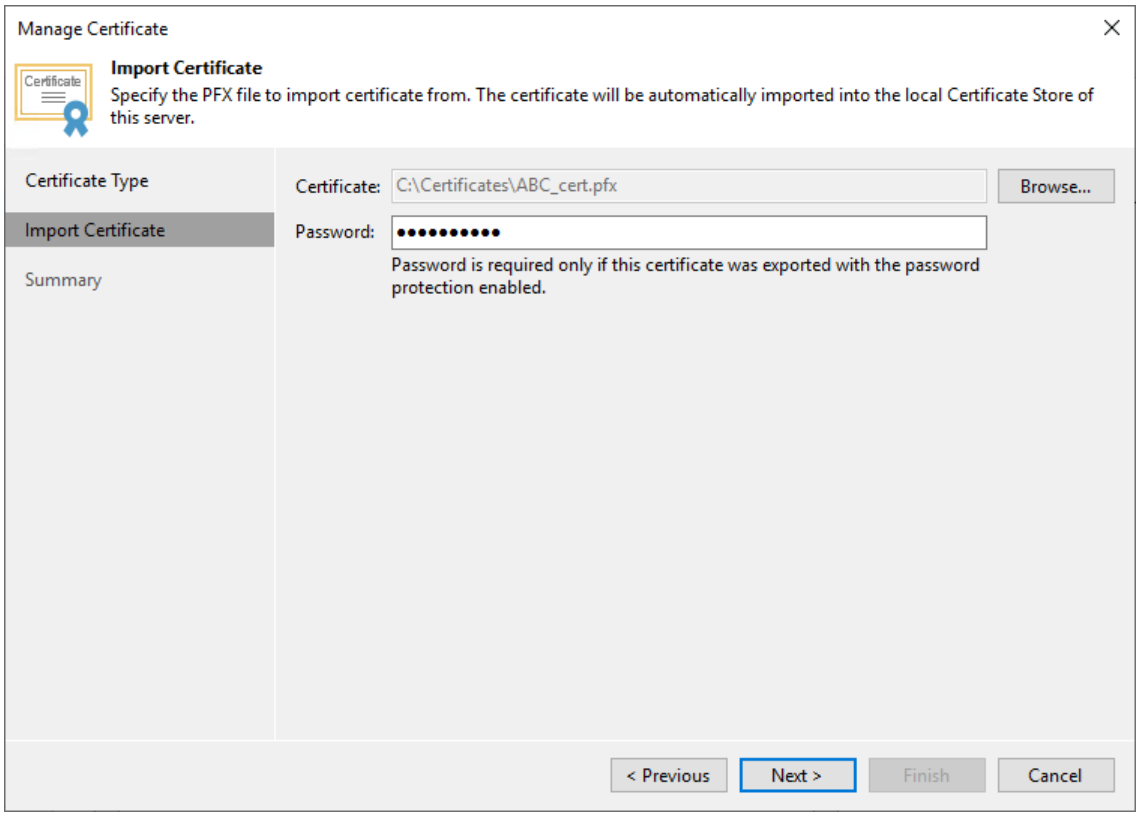
To import a TLS certificate from a PFX file:

1. From the main menu, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, choose **Import certificate from a file**.



5. At the **Import Certificate** step of the wizard, specify a path to the PXF file.

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



7. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the TLS certificate. You can use the copied information on a protected computer to verify the TLS certificate with the certificate thumbprint.

8. Click **Finish** to apply the certificate.

Using Certificate Signed by Internal CA

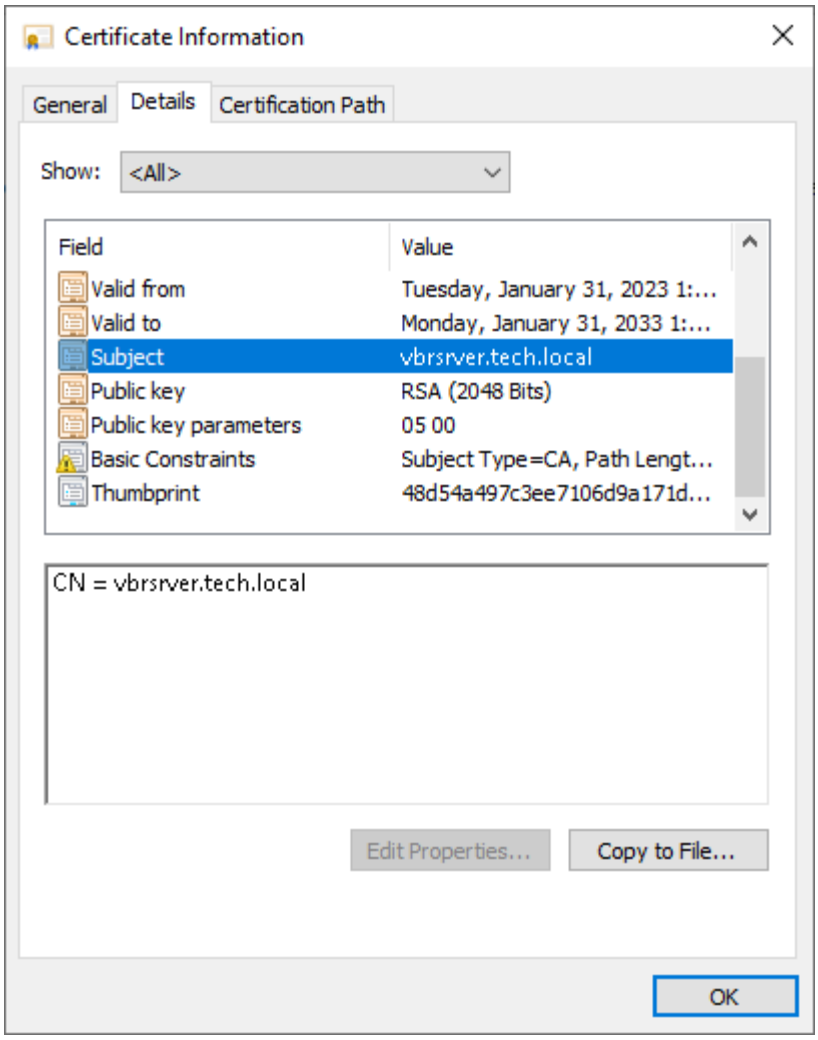
To establish a secure connection between the backup server and protected computers, Veeam Backup & Replication uses a TLS certificate. By default, Veeam Backup & Replication uses a self-signed certificate. Veeam Backup & Replication generates this certificate when you install the product on the Veeam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

If 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: *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. It is highly recommended to add "pathLen:0" to Basic Constraints.

   If you use Windows Server Certification Authority, to do this, enable the **Do not allow subject to issue certificates to other CAs** option in the certificate template.

4. 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.

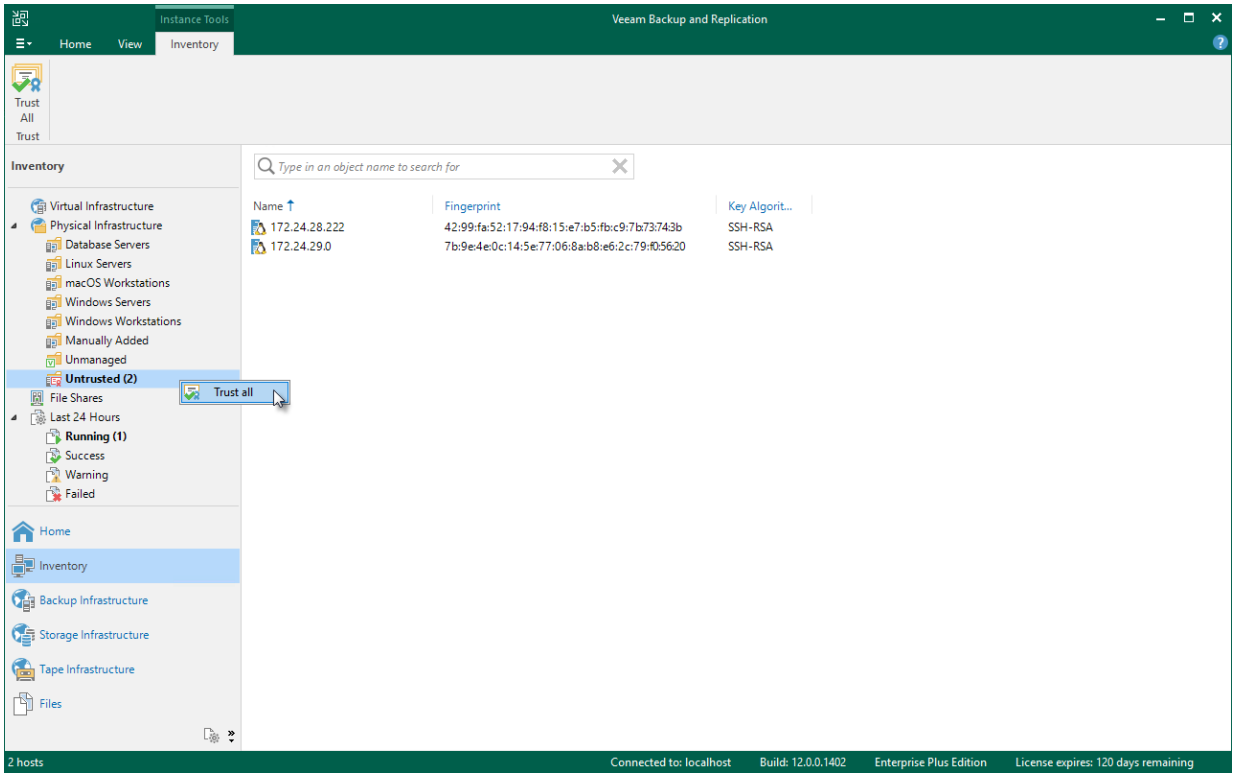
After you specify the signed certificate in Veeam Backup & Replication, during the next backup job session Veeam Agents will receive child certificates from the Veeam backup server.

Adding Computers to Trusted Hosts List

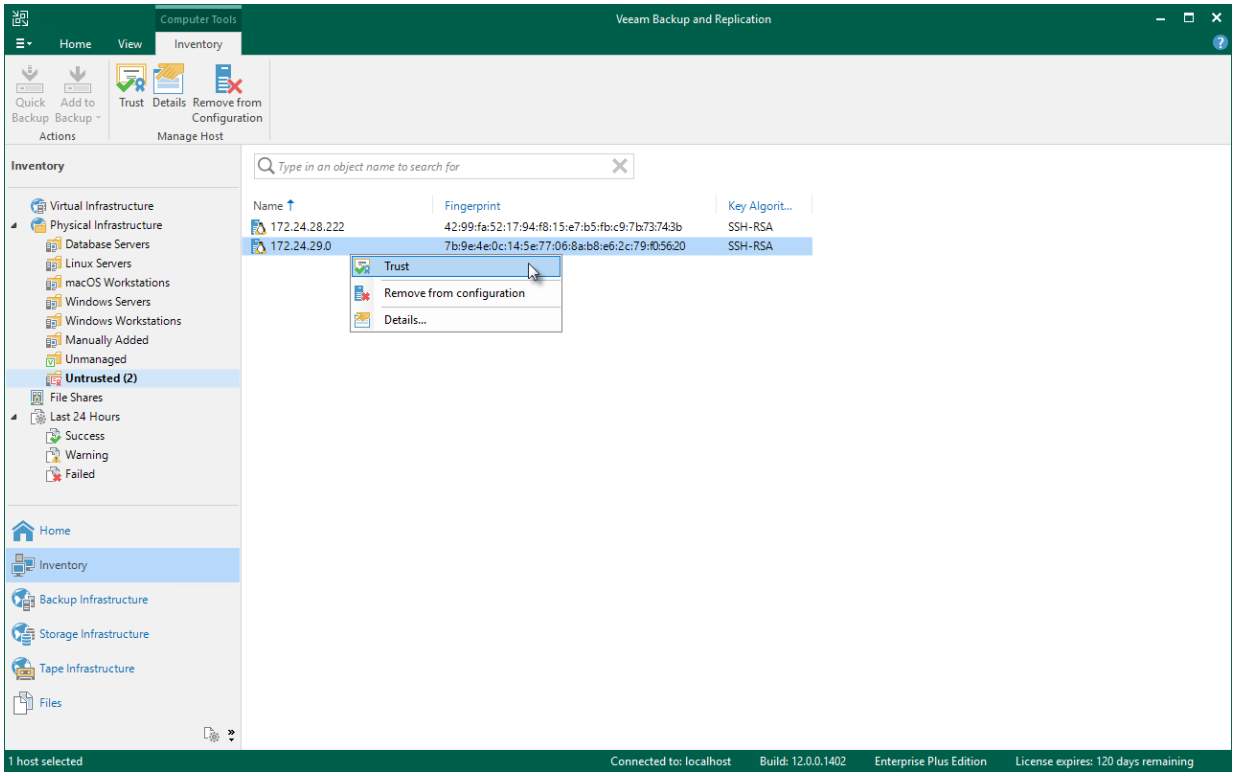
After you enable the **Add unknown hosts to the list manually (more secure)** option in Veeam Backup & Replication settings, Linux-based computers whose SSH fingerprints are not stored in the Veeam Backup & Replication database become unable to communicate to the Veeam backup server. During discovery, Veeam Backup & Replication puts such computers to the *Untrusted* protection group. To start managing an untrusted computer, you must manually validate the SSH fingerprint and add the to the list of trusted hosts 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 SSH 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

> **IMPORTANT**
>
> Protection groups for pre-installed Veeam Agents offer a limited set of operations. To learn more, see Working with Protection Groups for Pre-Installed Veeam Agents.

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.

Working with Protection Groups for Pre-Installed Veeam Agents

A protection group for pre-installed Veeam Agents offers a limited set of operations. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

For protection groups for pre-installed Veeam Agents, you can perform the following operations:

- Create a protection group.
- Add a protection group to a Veeam Agent backup job.
- Edit protection group settings.
- 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 Predefined Protection Groups.

Before You Begin

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

1. [Not applicable to protection groups for pre-installed Veeam Agents] 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 for pre-installed Veeam Agents is the only protection group that allows to protect the following computers:
   - Unix computers with Veeam Agent for IBM AIX or Veeam Agent for Oracle Solaris installed
   - macOS computers with Veeam Agent for Mac installed
3. A protection group for pre-installed Veeam Agents offers a limited set of deployment and management operations. To learn more, see Working with Protection Groups for Pre-Installed Veeam Agents and Managing Protected Computers Added to Protection Group for Pre-Installed Veeam Agents.
4. 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.
5. Veeam Backup & Replication automatically excludes from the protection scope Active Directory objects of the Group type that exist in a parent Active Directory object (organizational 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.
6. 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.
7. A protection group for cloud machines can include only the following objects:
   - Amazon EC2 instances
   - Microsoft Azure virtual machines
8. A protection group for cloud machines can include objects running only supported Microsoft Windows and Linux OSes.
9. Amazon EC2 instances included in the protection group for cloud machines must meet the following requirements:
   - Instances must have SSM Agent installed and running. To learn more, see this Amazon article.
   - Instances must have access to CRL lists and certificates of the AWS internal services necessary to connect to these internal services.
10. Microsoft Azure virtual machines included in the protection group for cloud machines must meet the following requirements:
    - Virtual machines must have Microsoft Azure Virtual Machine Agent (Azure VM Agent) installed and running. To learn more, see this Microsoft article.
    - Virtual machines must have access to CRL lists and certificates of the Microsoft Azure internal services necessary to connect to these internal services.

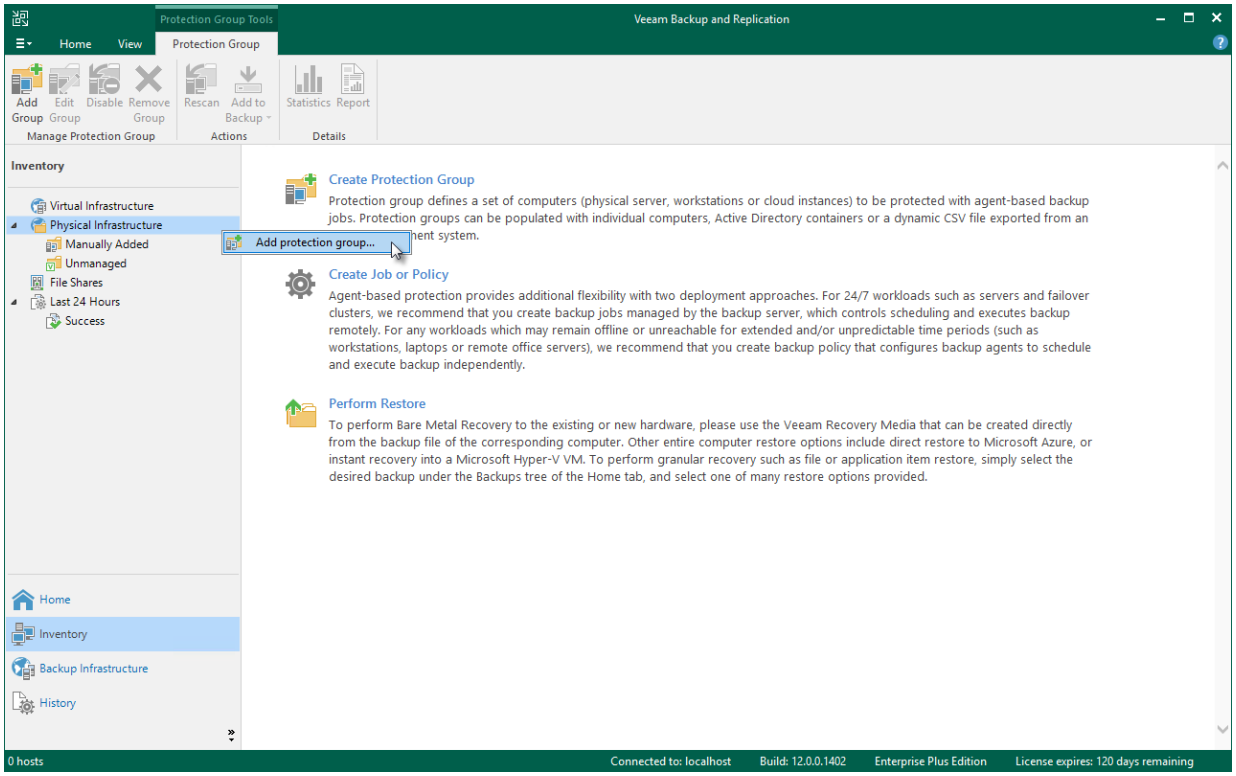
11. [Not applicable to protection groups for pre-installed Veeam Agents] It is recommended that you do not add a computer to a protection group by specifying a dynamic IP address assigned to this computer. If such computer receives another IP address from a DHCP server, Veeam Backup & Replication will be unable to discover the computer and perform on this computer operations defined in the protection group settings.
12. [Not applicable to protection groups for pre-installed Veeam Agents] 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.
13. We recommend 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.
14. You can add a failover cluster only to a protection group that includes Microsoft Active Directory objects. You cannot add failover clusters to protection groups that include individual computers or computers specified in a CSV file.
15. When you configure a protection group for a failover cluster, do not exclude nodes of this cluster from a protection scope. Otherwise, Veeam Backup & Replication will not have complete information about all clustered servers.
16. [Not applicable to protection groups for pre-installed Veeam Agents and protection group for cloud machines] 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.
17. Veeam Backup & Replication does not support usage of a Linux account for which system settings modify shell output results to connect to a computer included in the protection group. For example, this includes Linux accounts with the modified *PS1* shell variable.
18. Each time you add a Veeam Agent computer to the protection group, Veeam Backup & Replication considers this Veeam Agent computer as a new object. For example, if you add a Veeam Agent computer to the protection group, then remove this Veeam Agent computer from the protection group and add to the same protection group again, Veeam Backup & Replication will consider this Veeam Agent computer as two different objects. As a result, Veeam Agent will start a new backup chain each time you add the Veeam Agent computer to the protection group.
19. To connect to the Linux-based computer where you want to install Veeam Agent for Linux, you must specify the user account that have a home directory. Users without home directories are not supported.

Step 1. Launch New Protection Group Wizard

To launch the **New Protection Group** wizard, do one of the following:

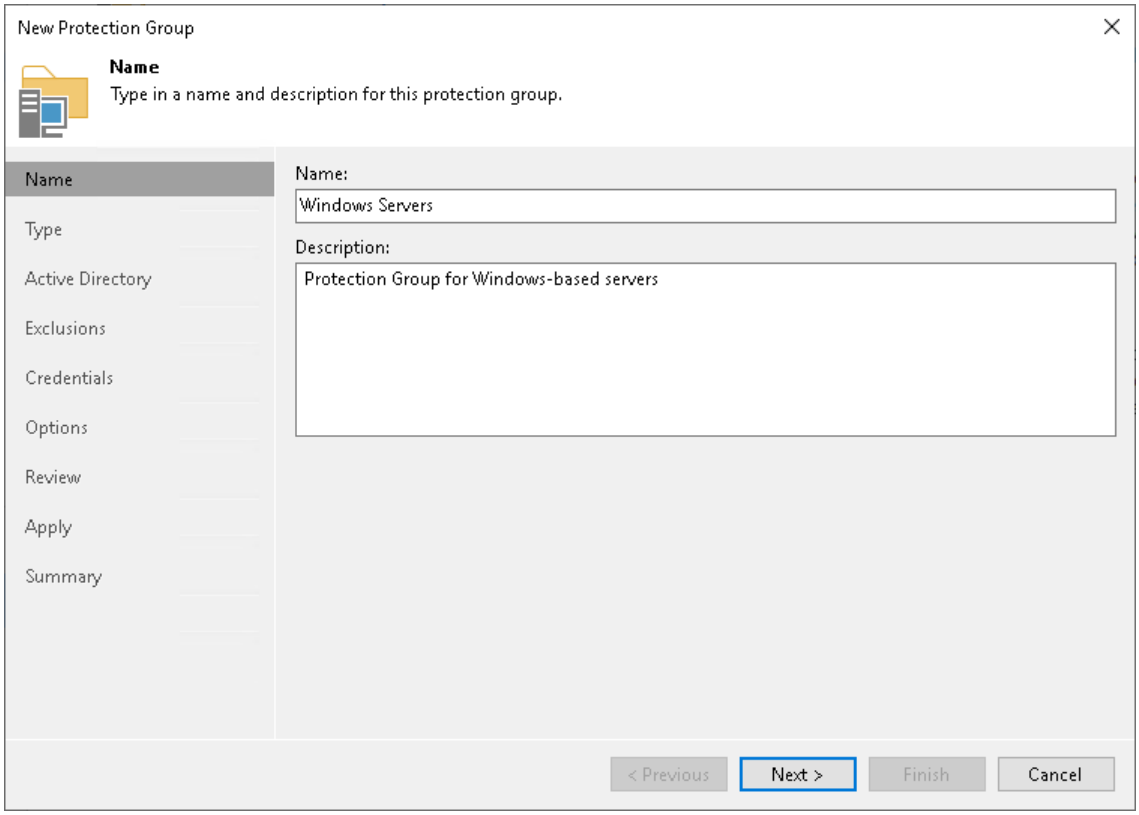
- Open the **Inventory** view. Click the **Physical Infrastructure** node in the inventory pane and click **Add Group** on the ribbon.
- Open the **Inventory** view. Click the **Physical Infrastructure** node in the inventory pane and click **Create Protection Group** in the working area.
- Open the **Inventory** view. Right-click the **Physical Infrastructure** node in the inventory pane and select **Add protection group**.



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.



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 failover 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, organizational unit, group, computer or failover cluster. Protection groups that include Active Directory containers and/or organizational units are dynamic in their nature. If a new computer is added to a container or organizational 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.

- **Computers with pre-installed agents** — select this option if you want to create a protection group for pre-installed Veeam Agents. This protection group will include any number of computers that use a certain certificate ID to connect to the Veeam backup server. Certificate ID is a unique identification number generated for each protection group that is available among other connection settings in a configuration file. You will obtain the configuration file along with Veeam Agent setup files after the protection group is created. Using these setup files, you must deploy Veeam Agent and apply connection settings from the configuration file on the Veeam Agent computer. After that, Veeam Agent connects to the Veeam backup and Veeam Backup & Replication includes the Veeam Agent computer in the protection group.

  With this option selected, you will pass to the Package step of the wizard.

  To learn more about Veeam Agents deployment, see Deploying Veeam Agents Using Generated Setup Files.

NOTE

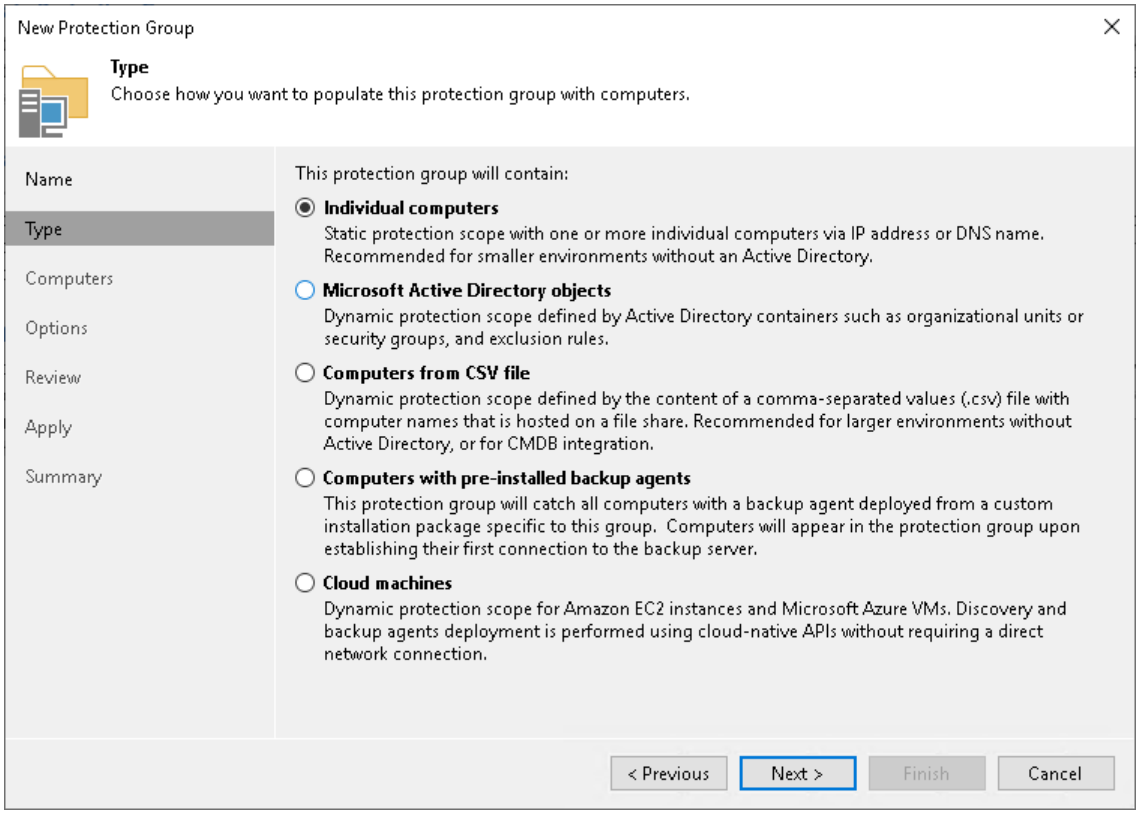
- The **Computers with pre-installed agents** option is the only applicable option for Unix computers that you plan to protect with Veeam Agent for Oracle Solaris or Veeam Agent for IBM AIX and Mac computers that you plan to protect with Veeam Agent for Mac.
- You can add a protection group of the Computers with pre-installed agents type only to a Veeam Agent backup job managed by Veeam Agent. Veeam Agent backup jobs managed by the backup server are not supported by this type of protection groups. To learn more about backup job types, see Working with Veeam Agent Backup Jobs and Policies.

- **Cloud machines** – select this option if you want to add to the protection group one or several Amazon EC2 instances or Microsoft Azure virtual machines (both objects can be also referred to as cloud machines). Using this protection group, Veeam Backup & Replication will discover such cloud machines and deploy Veeam Agent for Microsoft Windows or Veeam Agent for Linux on them without connection over network. After that, you will be able to create transactionally consistent backups of cloud machines included in the protection group.

  With this option selected, you will pass to the Cloud Account step of the wizard.

  NOTE

  - You can add a protection group of the Cloud machines type only to a Veeam Agent backup job managed by the backup server. Veeam Agent backup jobs managed by Veeam Agent are not supported by this type of protection groups. To learn more about backup job types, see Working with Veeam Agent Backup Jobs and Policies.
  - You can store backups of cloud machines only in the object repository located on the same external cloud storage as the cloud machines you want to back up.
  - Scale-out backup repositories and Veeam Cloud Connect repositories are not supported as a backup destination for cloud machines.



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.
- Specify packages — if you have selected the **Computers with pre-installed agents** option at the Type step of the wizard.
- Specify cloud machines — if you have selected the **Cloud machines** 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, 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.

   Veeam Backup & Replication allows to add the following types of credentials:

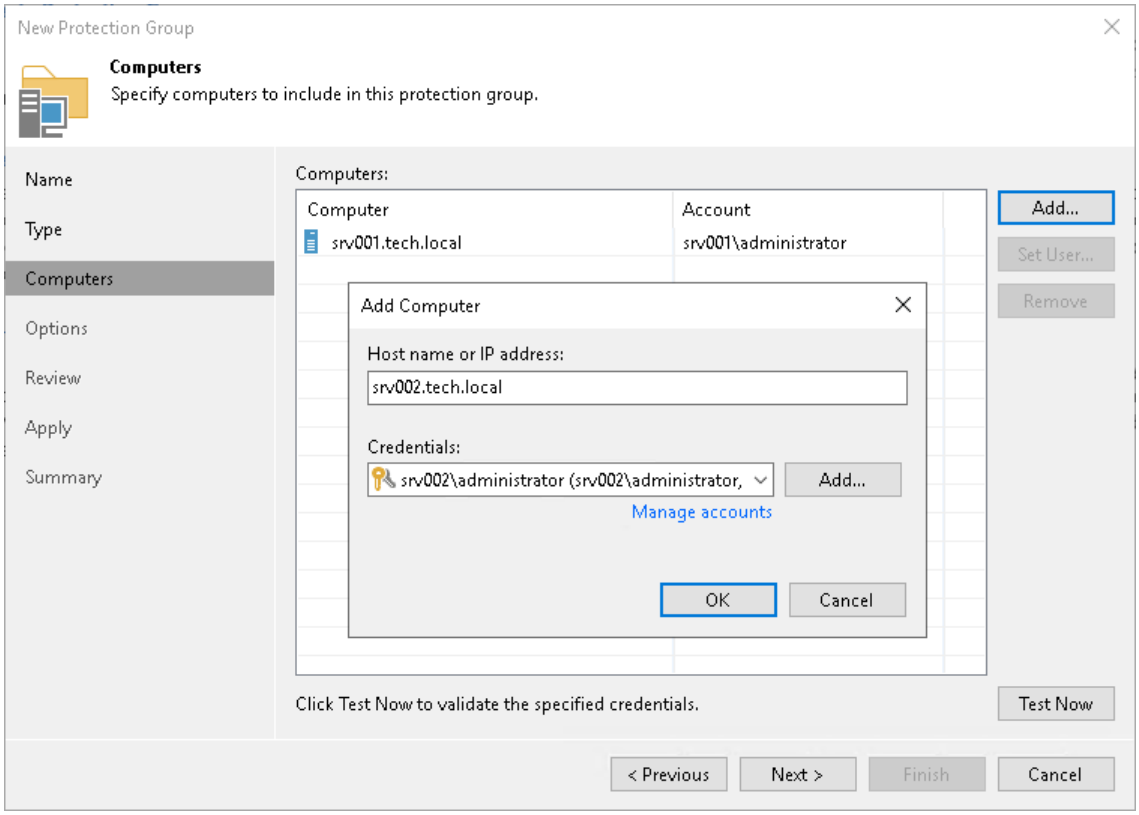
   - Stored credentials. Select stored credentials if you want Veeam Backup & Replication to use the specified user name and password for each connection to Veeam Agent.
   - [For Linux computers] Single-use credentials. Select single-use credentials if you do not want Veeam Backup & Replication to store credentials in the configuration database. With this option selected, Veeam Backup & Replication will use the specified user name and password only for the first connection to Veeam Agent. After that, Veeam Backup & Replication will use Veeam Transport Service to communicate with the Veeam Agent computer.

   Keep in mind that the username must be specified in the down-level logon name format. For example, DOMAIN\UserName or HOSTNAME\UserName. Use the full domain or hostname name. Do not replace them with a dot.

   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, 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, organizational unit, container, computer, failover 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.

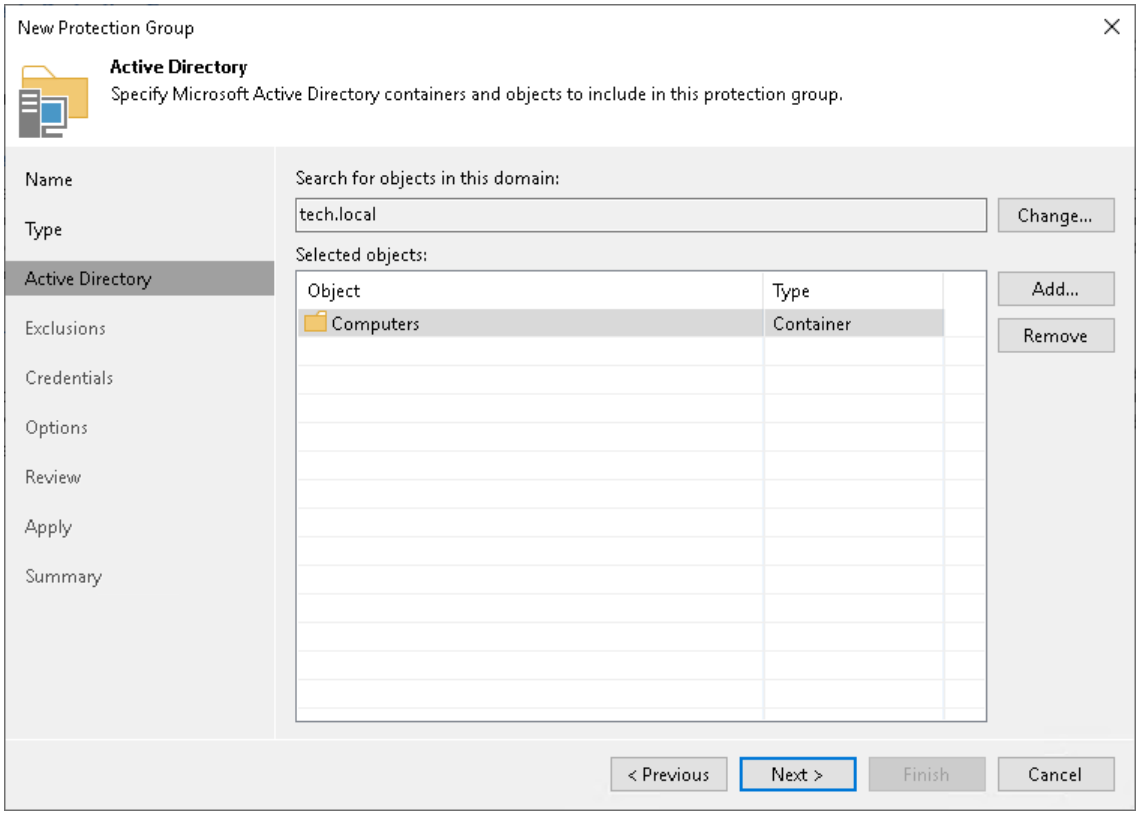
3. In the **Selected objects** field, click **Add**.
4. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK**. You can press and hold **[CTRL]** to select multiple objects at once.

   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*, *Failover Cluster*, *Organizational 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

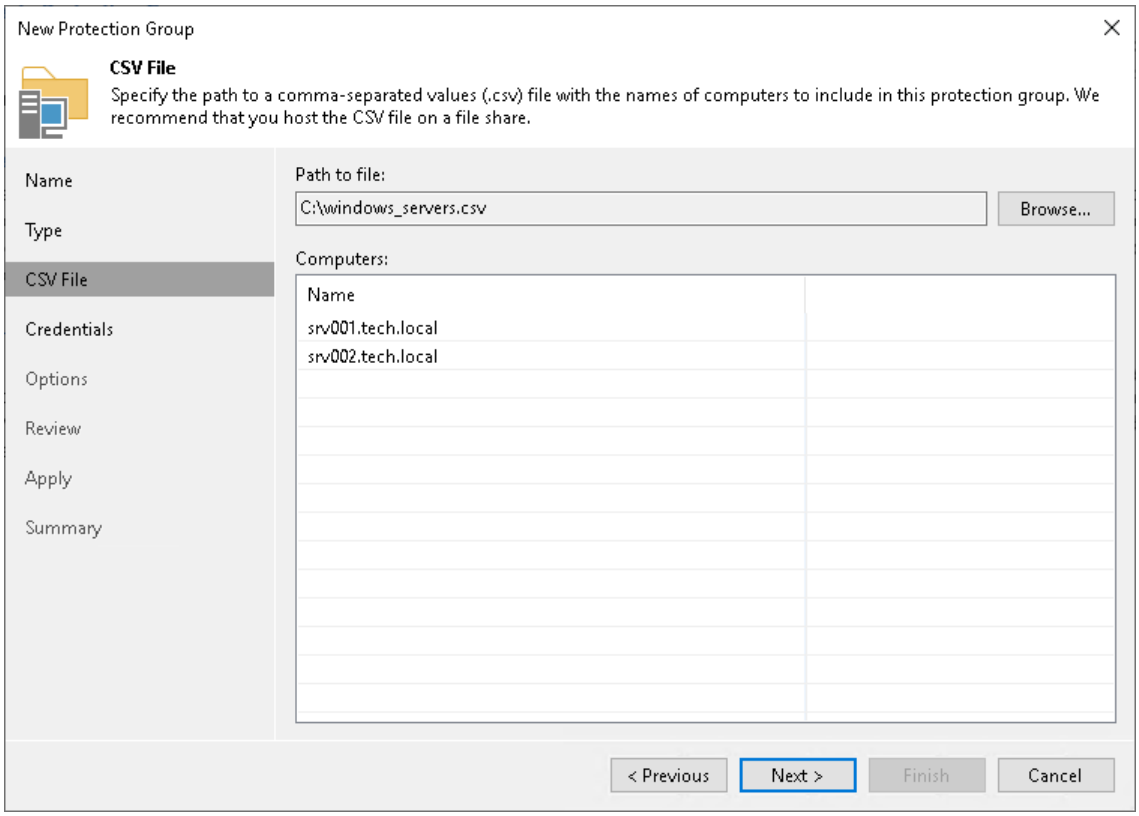
The **CSV File** step of the wizard is available if you have chosen the **Computers from CSV file** option at the Type step of the wizard.

At this step of the wizard, 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 and IPv6 formats.

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. For example:

```
172.17.53.16
172.17.53.19
172.17.53.31
172.17.53.40
```

Specifying Packages

The **Package** step of the wizard is available if you have chosen the **Computers with pre-installed agents** option at the Type step of the wizard.

At this step of the wizard, specify what setup files you want to obtain to deploy Veeam Agents. Veeam Backup & Replication will export the specified setup files to the specified folder. Then, you must use these setup files to deploy Veeam Agents on computers you plan to protect. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

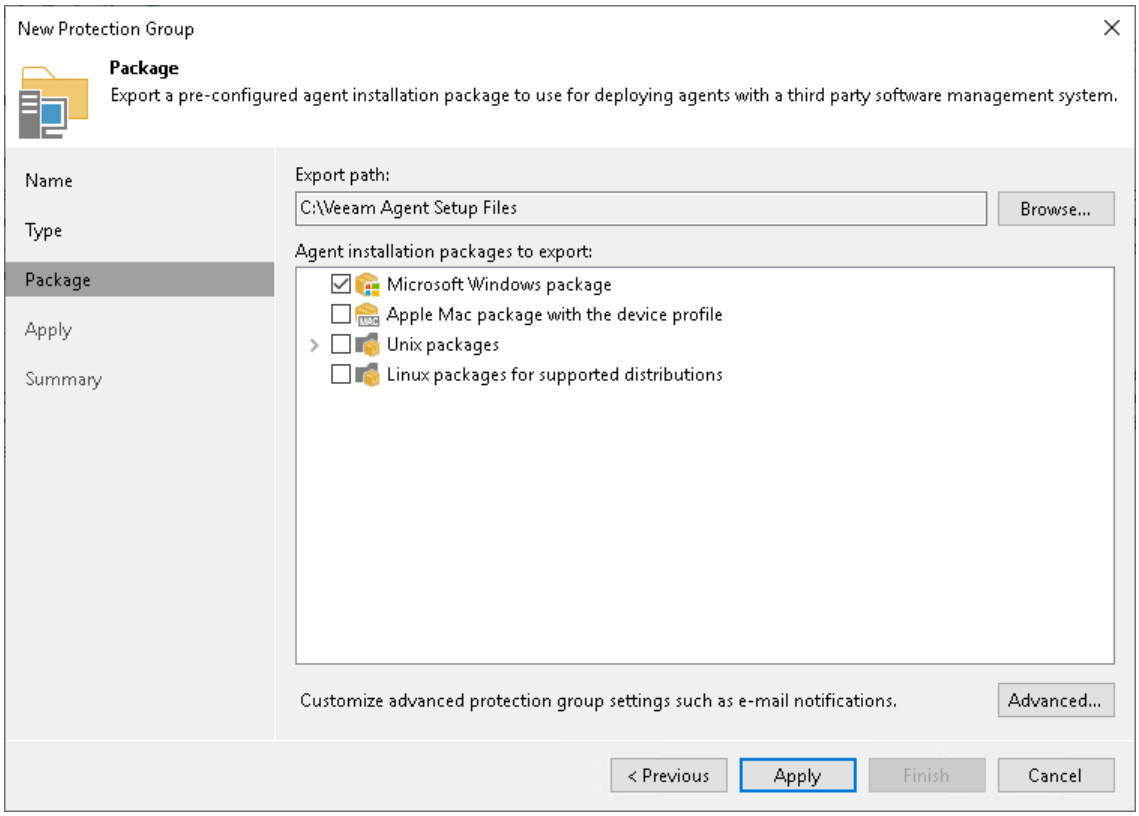
To specify setup files to export:

1. In the **Export path** field, click **Browse**.
2. In the **Select Folder** window, specify a path to the folder to which Veeam Backup & Replication will export Veeam Agent setup files. Setup files can be exported to a folder on the local drive of the Veeam backup server or to a network shared folder accessible from the backup server.
3. In the **Agent installation packages to export** field, select setup files depending on the type of the OS that runs on computers you plan to add to the protection group.
   a. If you plan to protect Windows computers, select the **Microsoft Windows package** option
   b. If you plan to protect Mac computers, select the **Apple Mac package with the device profile** option
   c. If you plan to protect Unix computers, expand the **Unix Packages** option and select options depending on the distributions you need.

      If you select the **Unix Packages** option, Veeam Backup & Replication will export setup files for all Unix distributions supported by Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris.
   d. If you plan to protect Linux computers, expand the **Linux packages for supported distributions** option and select options depending on the distributions you need.

      If you select the **Linux packages for supported distributions** option, Veeam Backup & Replication will export setup files for all Linux distributions supported by Veeam Agent for Linux.

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



Specifying Cloud Machines

If you have chosen the **Cloud machines** option at the Type step of the wizard, specify settings to connect to the cloud storage:

1. At the Account step of the wizard, specify cloud storage settings.
2. At the Cloud Machines step of the wizard, specify cloud machines to deploy Veeam Agents.

Specifying External Cloud Settings

The **Cloud Account** step of the wizard is available if you have chosen the **Cloud Machines** option at the Type step of the wizard.

At this step of the wizard, specify settings for Amazon or Microsoft Azure cloud that you want to use to deploy Veeam Agents on cloud machines.

> **NOTE**
>
> AWS user that you use to connect to Amazon cloud must have the required permissions. To learn more, see Permissions.

To specify settings that Veeam Backup & Replication will use to connect to the external cloud:

1. Select the account from the **Credentials** list. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials using Cloud Credentials Manager.

   Keep in mind that to deploy Veeam Agents on cloud machines, you can specify only access keys for AWS User or Microsoft Azure Compute Account. To learn more, see Access Keys for AWS Users and Microsoft Azure Compute Accounts in the Veeam Backup & Replication User Guide.

   > **NOTE**
   >
   > Azure Stack Hub accounts are not supported.

2. Specify additional information required to connect to the cloud:

For AWS User

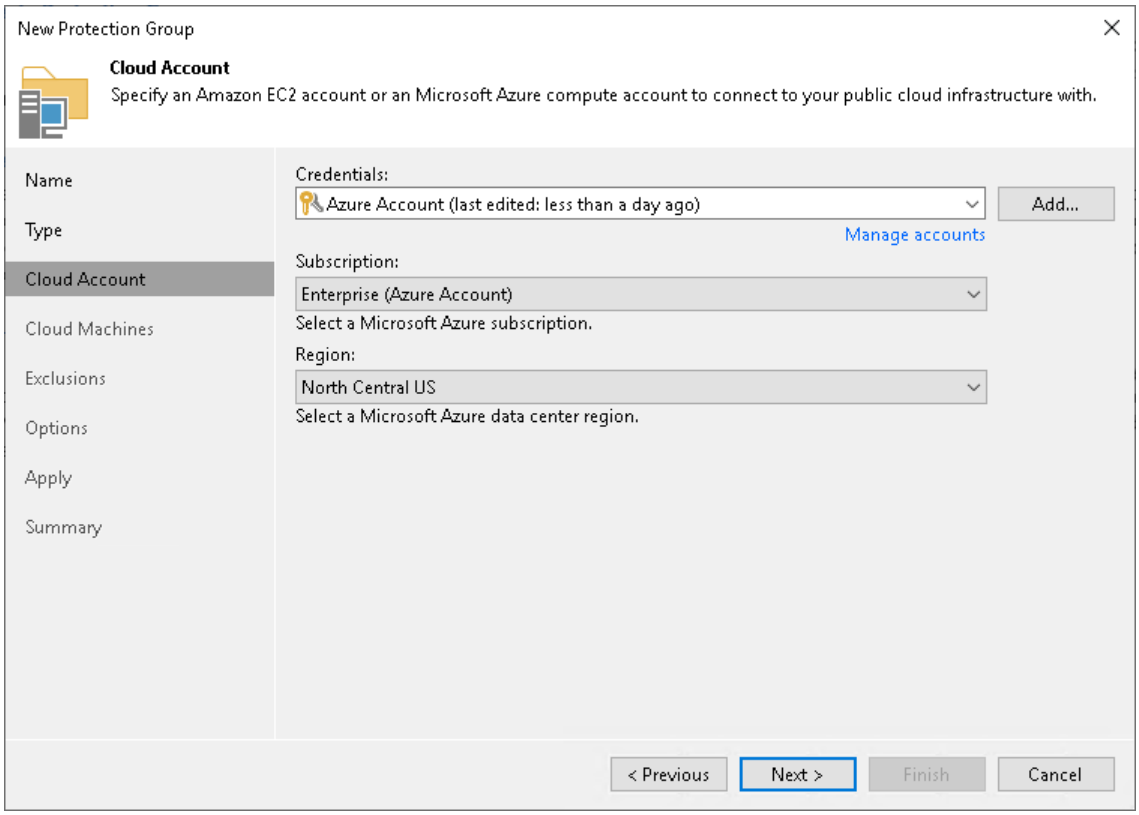
a. From the **AWS region** list, select the AWS region in which Veeam Backup & Replication will deploy Veeam Agents on cloud machines.

b. From the **Data center** list, select the geographic region where Veeam Backup & Replication will deploy Veeam Agents on cloud machines.

For Microsoft Azure Compute Account

a. From the **Subscription** list, select a subscription which resources you want to use. The subscription list contains all subscriptions associated with the Azure compute or Azure Stack Hub compute accounts that you have added to Veeam Backup & Replication.

b. From the **Region** list, select a geographic region where you want to deploy Veeam Agents on cloud machines. Make sure that you select a geographic region with that at least one storage account of the subscriptions is associated.



Specifying Cloud Machines

The **Cloud Machines** step of the wizard is available if you have chosen the **Cloud machines** option at the Type step of the wizard and specified settings for Amazon or Microsoft Azure cloud at the Cloud Account step of the wizard.

At this step of the wizard, specify cloud machines that you want to add to the protection group. To do this, you can select individual cloud machines, whole datacenters, or specify metadata tags.

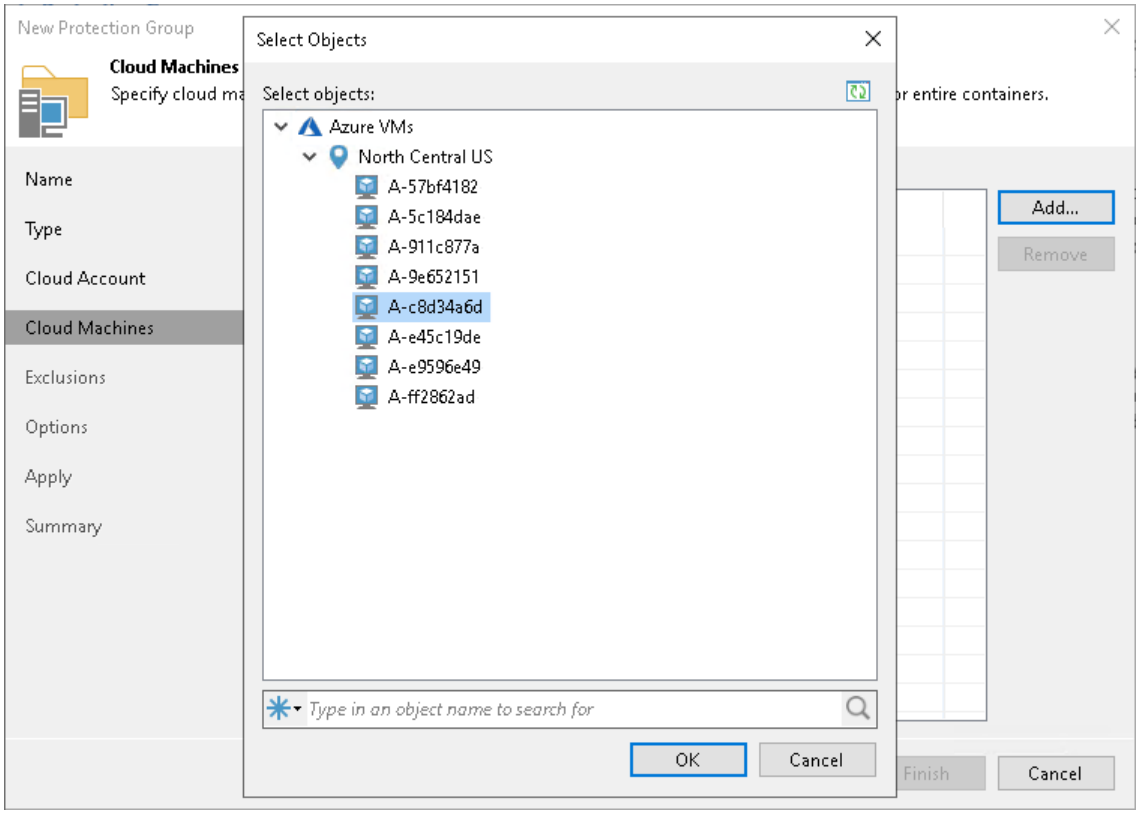
Adding Individual Cloud Machine or Datacenter

To add an individual cloud machine or datacenter to a protection group:

1. Click **Add** > **Machines**.
2. In the **Select Objects** window, select the necessary object 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.

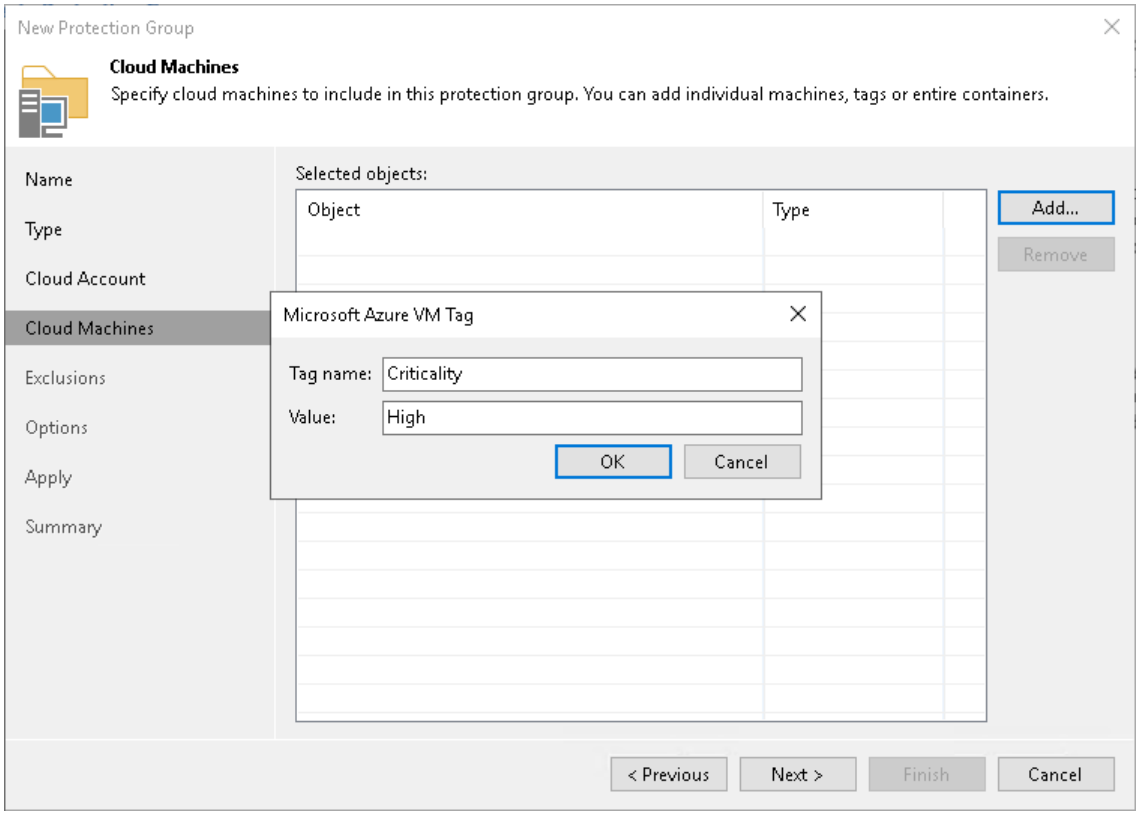
1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Adding Cloud Machines Using Metadata Tag

To add a tag:

1. Click **Add** > **Tags**.
2. In the **Tag** window:
   a. In the **Key** field, specify a key for the tag.
   b. In the **Value** field, specify a value for the tag and click **OK**.



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 or cloud machines.

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:

- [For protection groups that include Microsoft Active Directory 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.
- [For protection groups that include Microsoft Active Directory objects] 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 objects:

  For protection groups that include Microsoft Active Directory objects

  - Specific Active Directory objects: computers, failover clusters, groups, organizational units and containers.

  For protection groups that include cloud machines

  - Specific cloud machines.
  - Cloud machines with specific metadata tags.

  With this option selected, you must specify Active Directory objects, cloud machines, or metadata tags that you want to exclude from the protection group.

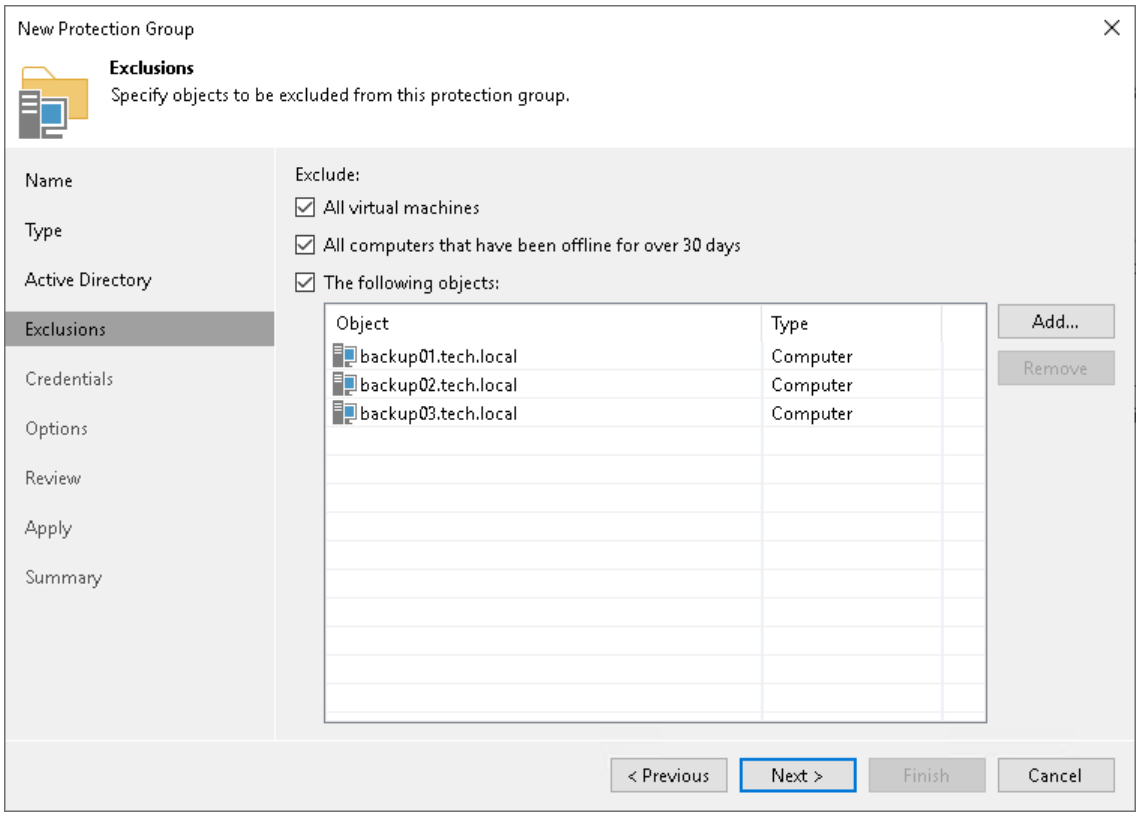
Excluding Individual Active Directory Objects

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 Active Directory 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*, *Failover cluster*, *Group*, *Organizational 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]**.



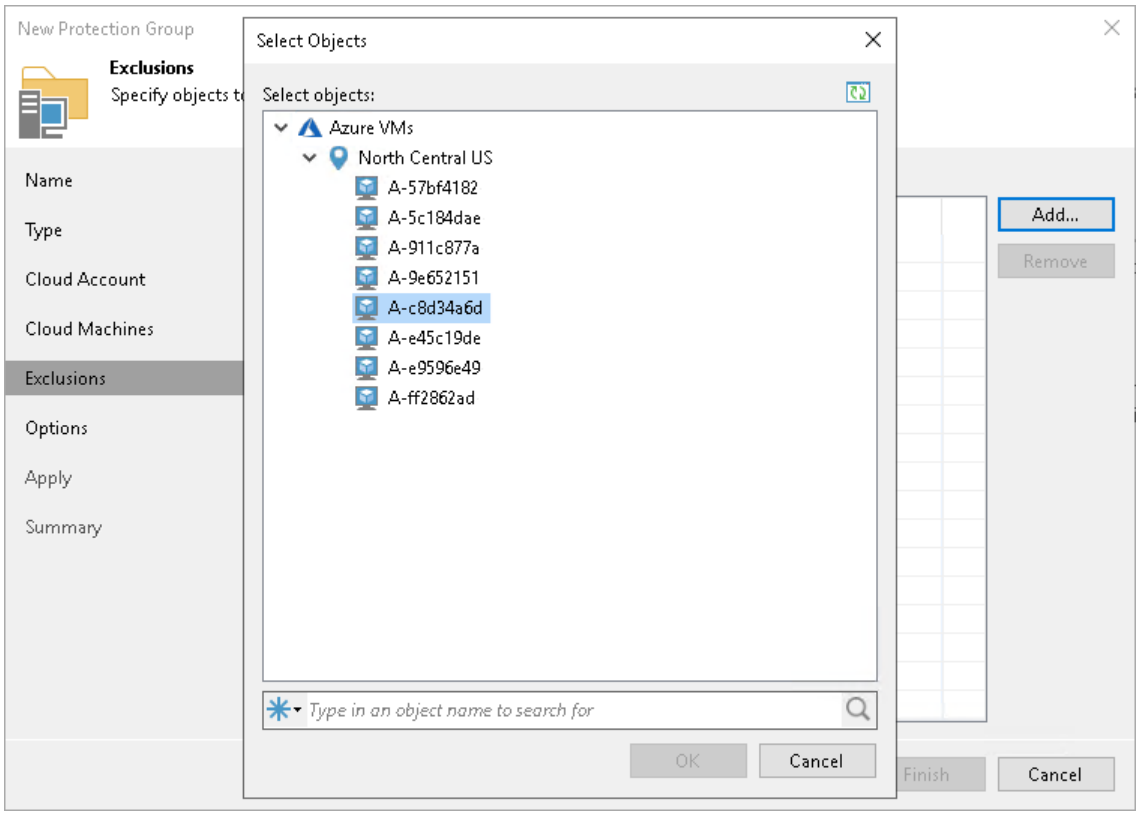
Excluding Individual Cloud Machines

To exclude an individual cloud machine:

1. Click **Add** > **Machines**.
2. In the **Select Objects** window, select the necessary cloud machine in the list and click **OK**. You can press and hold **[CTRL]** to select multiple machines at once.

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

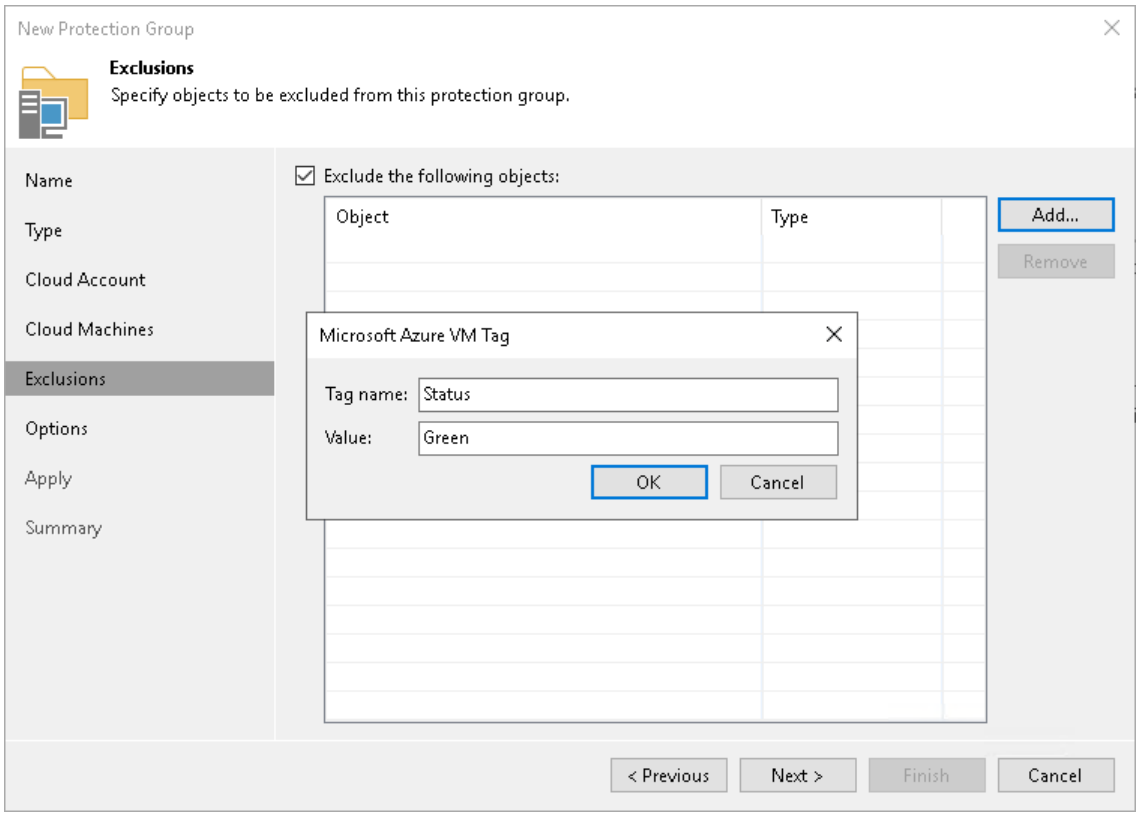
1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



Excluding Cloud Machines Using Tags

To exclude cloud machines using a metadata tag:

1. Click **Add** > **Tags**.
2. In the **Tag** window:
   a. In the **Key** field, specify a key for the tag.
   b. In the **Value** field, specify a value for the tag.



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 organizational 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:

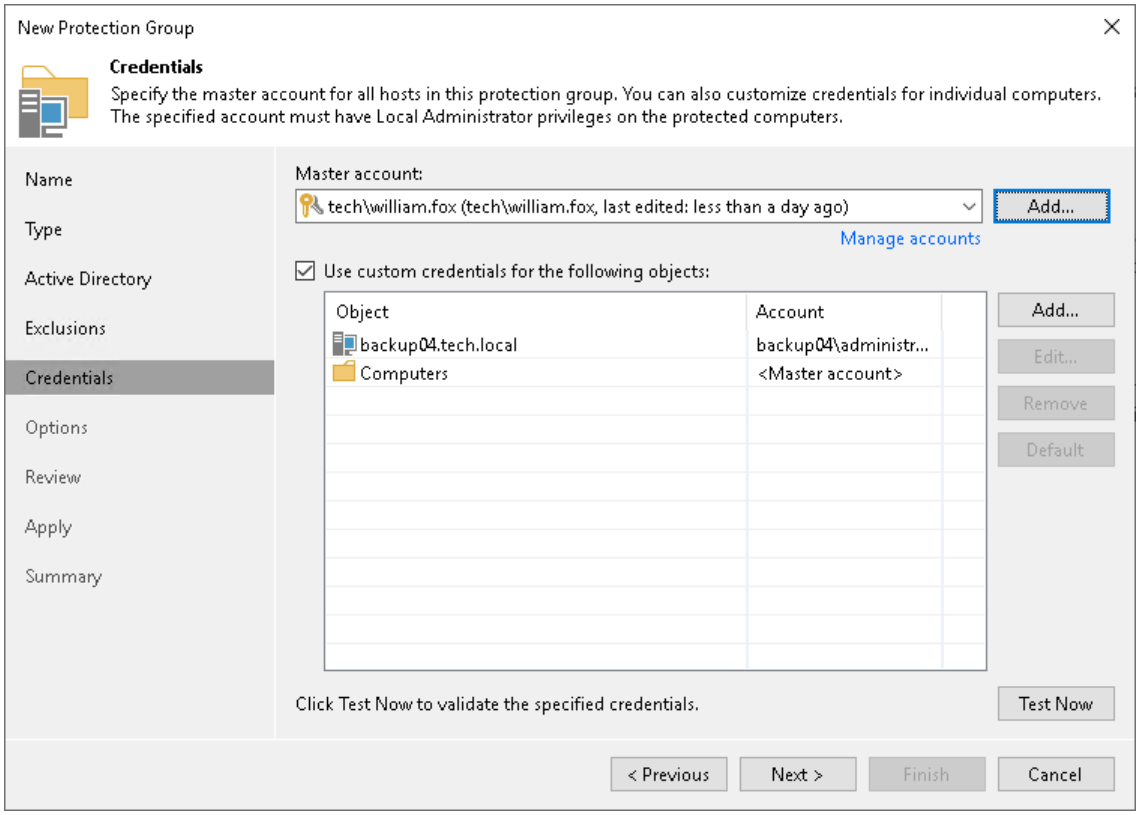
      - For Active Directory accounts — *DOMAIN\Username*
      - For local accounts — *Username* or *HOST\Username*

NOTE

Consider the following:

- Veeam Backup & Replication supports user account names in the SAM-Account-Name format (*DOMAIN\Username*). The User-Principal-Name (UPN) format (*username@domain*) is not supported. If you specify credentials in the UPN format, Veeam Backup & Replication will successfully connect to computers added to the protection group during the *Test Now* operation. However, the subsequent protection group rescan operations will fail.
- The user account that you use to connect to a Linux computer must have a home directory, users without home directories are not supported.
- If you configure a protection group that includes dynamic Active Directory objects, such as domain, organizational 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 computers, the OS account used to connect to the computer must be a member of the group that owns configuration files of the Oracle database (for example, 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 Permissions

The **Cloud Permissions** step of the wizard is available if you have chosen to define a protection scope that includes Amazon EC2 virtual machines.

To communicate with Amazon EC2 virtual machines included in the protection group, you need to perform the following operations:

1. Set the IAM role with the *AmazonSSMManagedInstanceCore* policy. To learn more, see this Amazon article.
2. Assign the IAM role to the cloud machine you want to back up.

Veeam Backup & Replication allows you to automate these operations.

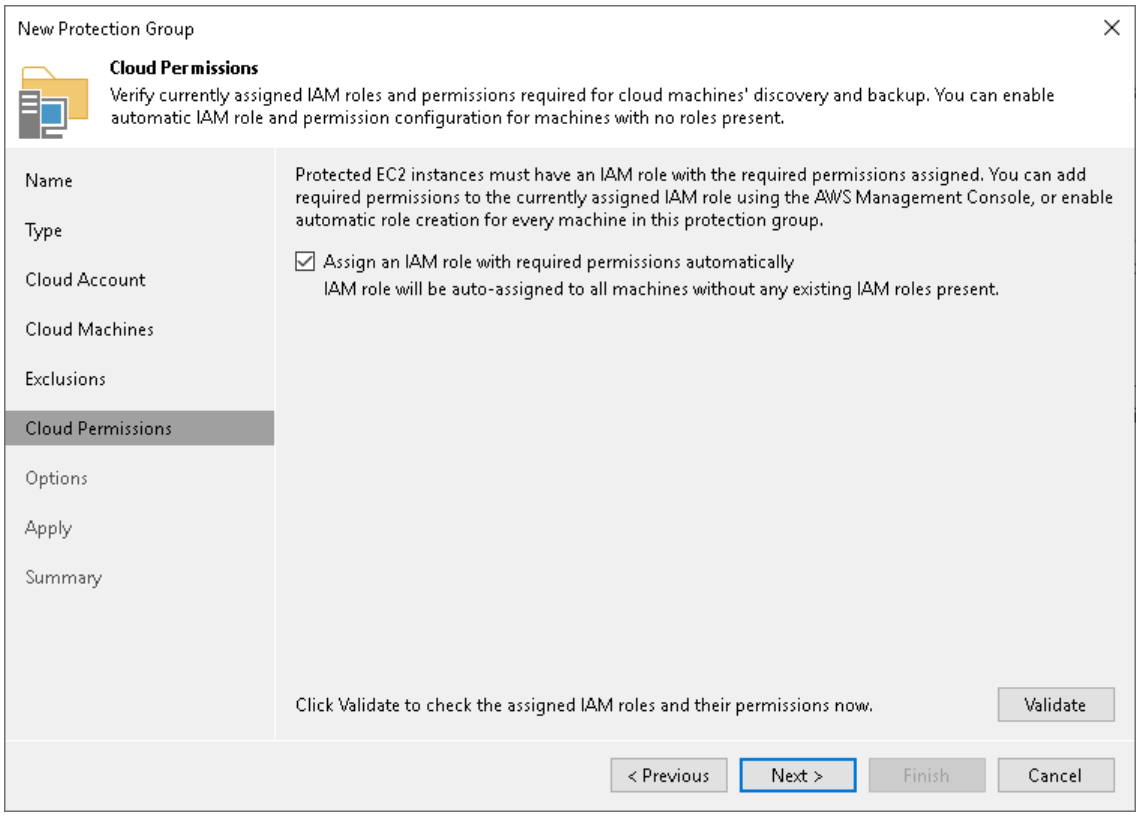
At this step of the wizard, set roles for Amazon EC2 virtual machines included in the protection group:

1. If you want to instruct Veeam Backup & Replication to automatically set the required role and policy, select the **Assign an IAM role with required permissions automatically** check box. If necessary, Veeam Backup & Replication will set the IAM role with the *AmazonSSMManagedInstanceCore* policy to all virtual machines included in the protection group.

   Keep in mind that Veeam Backup & Replication will set the IAM role with the *AmazonSSMManagedInstanceCore* policy to the virtual machine only if the following conditions are met:

   - The user account specified at the **Cloud Account** step of the wizard has enough access rights to set the IAM role.
   - The virtual machine does not have the IAM role already assigned.

2. To check if Veeam Backup & Replication can communicate with virtual machines added to the protection group, click **Validate**. Veeam Backup & Replication will try to connect to all virtual machines included in the protection group.



Step 7. Specify Discovery and Deployment Options

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

At this 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:
   - 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.
   - 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.
   - 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, select the object that will be responsible for the Veeam Agents distribution:
   - If you plan to create any protection group excluding protection group for cloud machines, 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 files 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.
   - If you plan to create a protection group for cloud machines, from the **Distribution repository** list, select a Microsoft Azure blob storage or Amazon S3 storage repository that you plan to use as a distribution repository. Veeam Backup & Replication will use the distribution repository to upload Veeam Agent setup files to cloud machines added to the protection group.

     If you have not added the necessary repository to your infrastructure before, click **Add** to add a new repository. For details, see Adding Azure Blob Storage or Adding Amazon S3 Storage in the Veeam Backup & Replication User Guide.

> **IMPORTANT**
>
> If you plan to use the Azure blob storage repository as a distribution repository, you must add this repository using a general-purpose v2 storage account. Other account types are not supported.

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** 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.

   Keep in mind that Veeam Backup & Replication installs the Veeam Installer Service or Veeam Deployer Service on every computer added to the protection group even if the **Install backup agent** check box is not selected in the protection group settings.

   > **TIP**
   >
   > To learn how to use protection groups to automatically deploy Veeam plug-ins for enterprise applications, see Veeam Plug-ins for Enterprise Applications Guide.

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 agents and plug-ins** check box is selected.

5. [For protection groups that include Microsoft Windows computers] Select the **Install changed block tracking driver** check box if you want to install the advanced changed block tracking (CBT) driver on computers protected with Veeam Agent for Microsoft Windows.

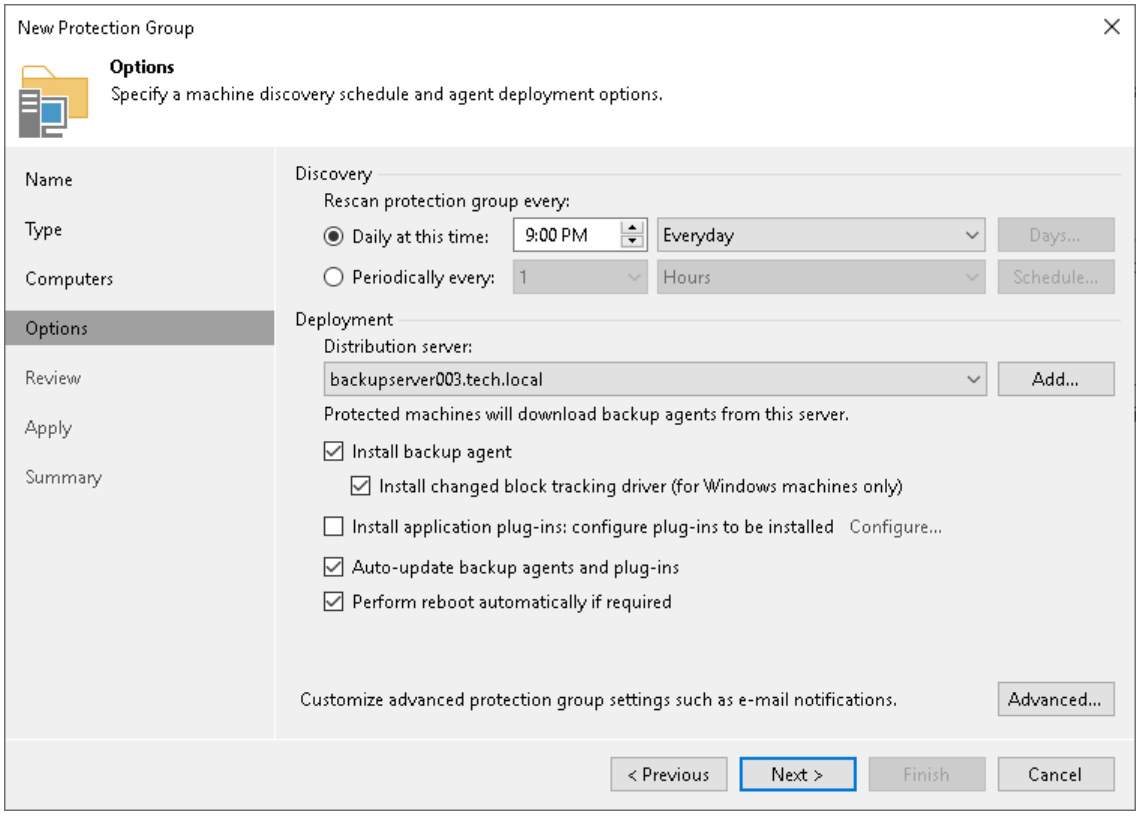
   Keep in mind that Veeam Backup & Replication will install the CBT driver only on those computers that run supported Microsoft Windows OS versions.

   To learn more, see the Veeam Changed Block Tracking Driver section in the Veeam Agent for Microsoft Windows User Guide.

   > **TIP**
   >
   > Veeam Backup & Replication 12 can install the CBT driver on a wider range of Microsoft Windows OS versions, but Veeam Backup & Replication will not install drivers automatically after upgrade. To install drivers in the existing protection group on the computers running OS versions that got support only in Veeam Backup & Replication 12, open the **Edit Protection Group** wizard, make sure that the **Install changed block tracking driver** check box is selected and re-save the protection group.

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 or restrict usage over any wireless networks.

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

> **IMPORTANT**
>
> Network usage settings are not applied to protected computers added to a Veeam Agent backup job managed by the backup server.

- **Backup I/O settings**. You can instruct Veeam Agent for Microsoft Windows to throttle its activities during backup. This 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.

> **IMPORTANT**
>
> Security settings are not applied to protected computers added to a Veeam Agent backup job managed by the backup server.

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.

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.

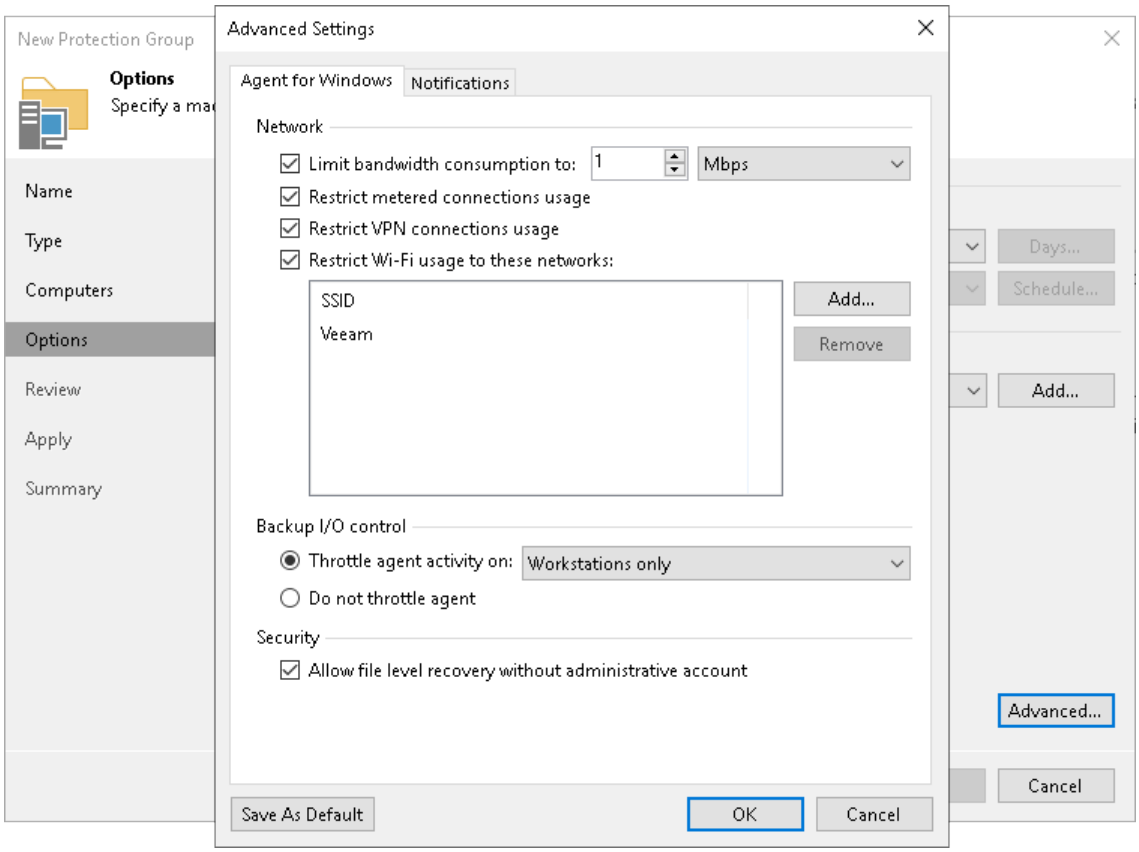
   > **TIP**
   >
   > If you want to restrict usage over any wireless networks, select the **Restrict Wi-Fi usage to these networks only** check box and do not add any networks to the list.

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, Veeam Agent computer users who work under accounts that do not have administrative privileges will be able to perform file-level restore on the Veeam Agent computer.

   In this case, access rights to files and folders are managed by Veeam Agent computer OS. If user cannot access the folder in the original location, this user cannot browse or restore the content of this folder as well.

To learn more, see Appendix B. Restore Files from Backup without Administrator Privileges.



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:

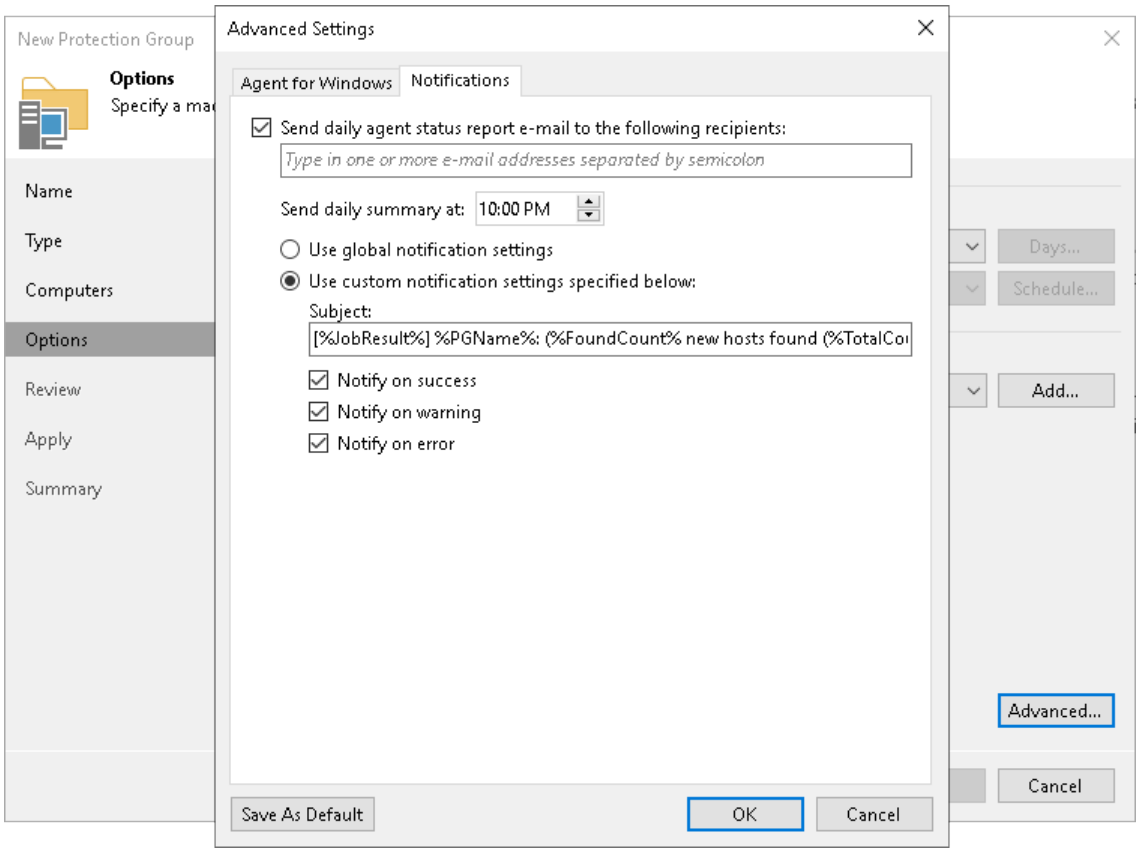
1. At the **Options** step of the wizard, click **Advanced**.
2. Click the **Notifications** tab.
3. Select the **Send daily agent status report e-mail to the following recipients** check box and specify a recipient's email address. You can enter several addresses separated by a semicolon.
4. In the **Send daily summary 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.



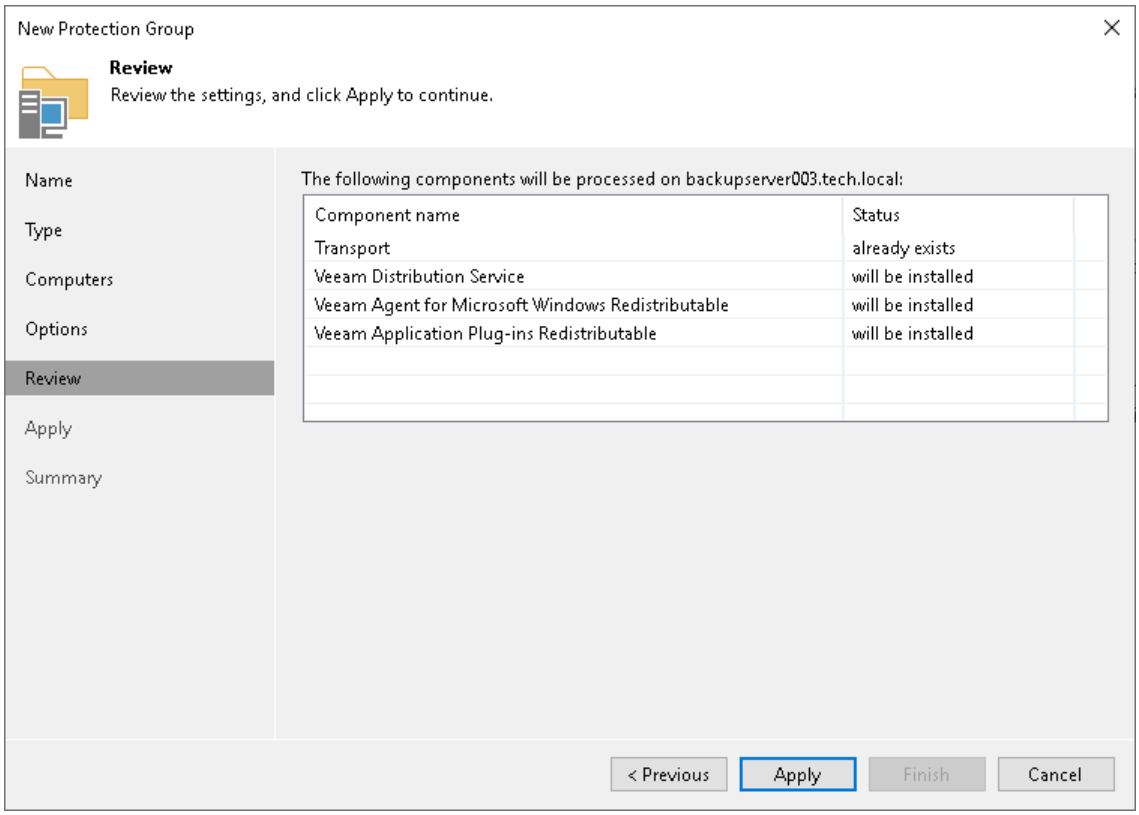
Step 9. Review Components

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

At this 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.

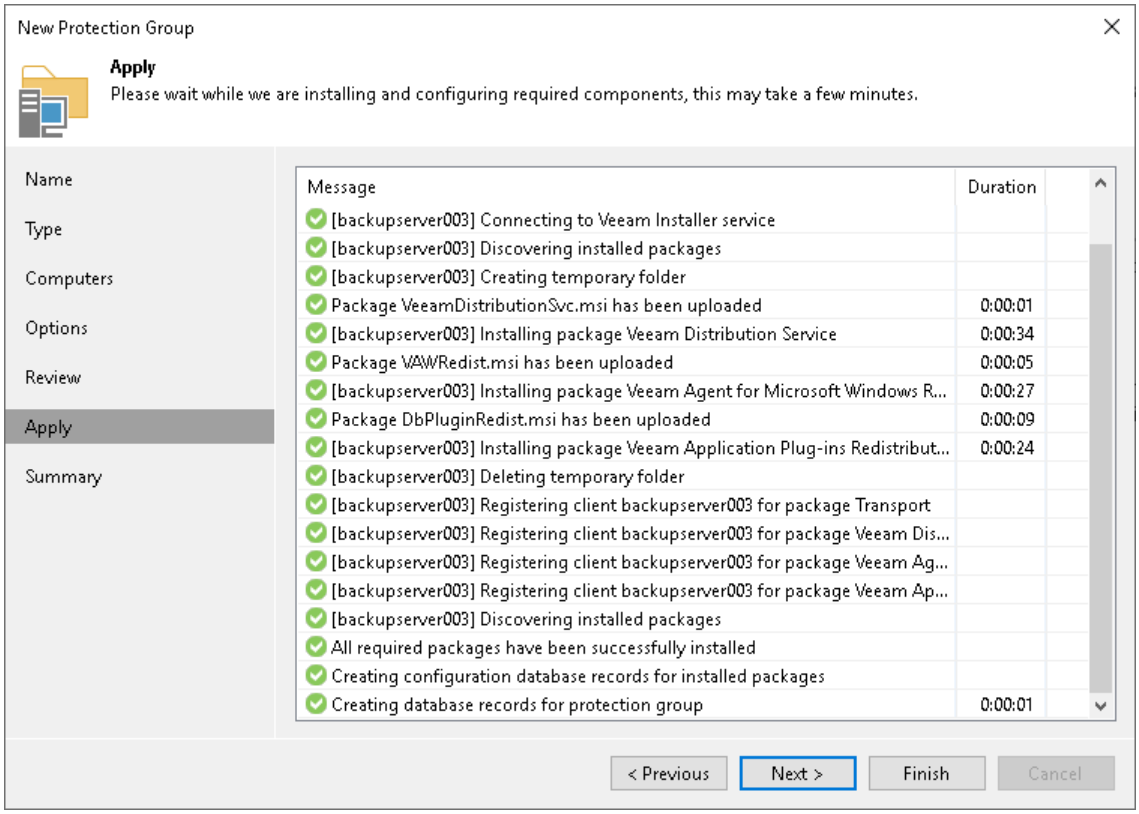
1. Review the components.
2. Click **Apply** to add the configured protection group to the inventory.

> **NOTE**
>
> Veeam Agent and Veeam Plug-in components are installed on the distribution server even if the **Install application plug-ins** and **Install backup agent** check boxes are clear at the Options step of the wizard.



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.

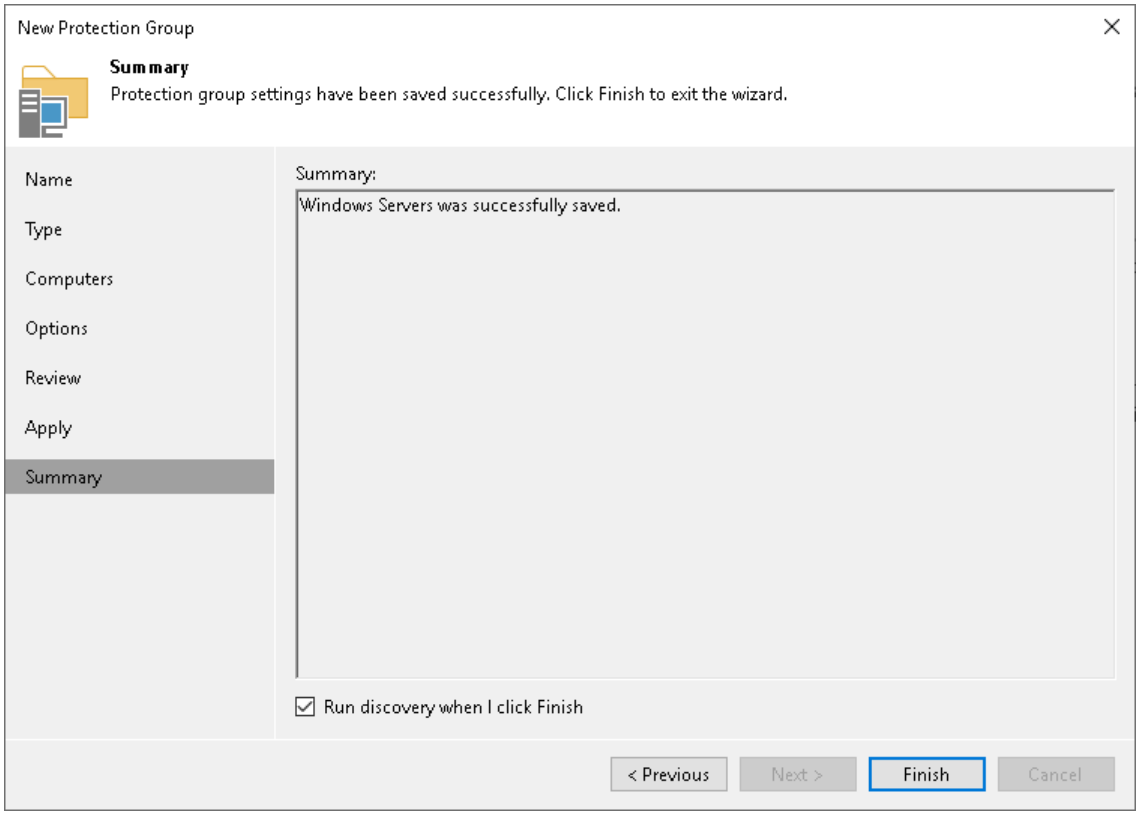


Step 11. Finish Working with Wizard

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**.



Deploying Veeam Agents Using Generated Setup Files

When you configure the Veeam Agent management infrastructure in Veeam Backup & Replication, you can create protection groups of the Computers with pre-installed agents type. If you selected this protection group type, you must deploy Veeam Agents on the computers that you plan to protect.

> **IMPORTANT**
>
> Mind the following:
>
> - The deployment operation must take place on the Veeam Agent computer side.
> - You must use only those Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.
> - If any other version of Veeam Agent is already installed on the computer you plan to protect, you must uninstall it first.
> - If you uninstall Veeam Agent for Microsoft Windows added to the protection group of the Computers with pre-installed agents type and then re-install it on the same computer, Veeam Agent will not connect to the Veeam backup server automatically. To connect Veeam Agent, you must repeat the configuration step of the Veeam Agent deployment scenario.

Deployment scenario depends on the Veeam Agent you work with:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for Unix
- Veeam Agent for Mac

Deploying Veeam Agent for Microsoft Windows

To deploy Veeam Agent for Microsoft Windows using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Microsoft Windows and all the required components, do the following:

1. Upload Veeam Agent setup files on the computer you want to protect. Then navigate to the folder where you have saved setup files.

   Keep in mind that you must use Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. To install the .NET Framework 4.5.2, double-click the `NDP452-KB2901907-x86-x64-AllOS-ENU.exe` file located in the `<path_to_setup_files>/Windows/6.0.0.960` folder.

   If a later version of the .NET Framework is already installed on the computer, you can skip this step.

3. To install Windows Universal C Runtime (CRT), find and double-click the file depending on your computer OS architecture and version:

OS Architecture	OS Version	File Location	File Name
32-bit	Windows 7 or Windows Server 2008 R2	`<path_to_setup_files>/Windows/6.0.0.960/VAW/x86/CRT`	`Windows6.1-KB2999226-x86.msu`
	Windows 8 or Windows Server 2012		`Windows6.1-KB2999226-x64.msu`
	Windows 8.1 or Windows Server 2012 R2		`Windows8-RT-KB2999226-x86.msu`
64-bit	Windows 7 or Windows Server 2008 R2	`<path_to_setup_files>/Windows/6.0.0.960/VAW/x64/CRT`	`Windows8-RT-KB2999226-x64.msu`
	Windows 8 or Window		`Windows8.1-KB2999226-x86.msu`

OS Architecture	OS Version	File Location	File Name
	s Server 2012		
	Windows 8.1 or Windows Server 2012 R2		`Windows8.1-KB2999226-x64.msu`

4. To install Veeam Agent for Microsoft Windows, use one of the following files depending on the architecture of your computer OS:

   For 32-bit Windows

   - Double-click the `Veeam_B&R_Endpoint_x86.msi` file located in the `<path_to_setup_files>/Windows/6.0.0.960/VAW` folder

   For 64-bit Windows

   - Double-click the `Veeam_B&R_Endpoint_x64.msi` file located in the `<path_to_setup_files>/Windows/6.0.0.960/VAW` folder

6. To install the Veeam Installer Service, double-click the `VeeamInstallerSvc` file located in the `<path_to_setup_files>/Windows/6.0.0.960` folder.

   If an earlier version of the Veeam Installer Service is already installed on the computer, uninstall it first.

Configuration

To configure Veeam Agent for Microsoft Windows, you must apply connection settings from the configuration file. You obtained this file together with other setup files when the protection group for pre-installed Veeam Agents was created. To do configure Veeam Agent, execute the following command from the folder where Veeam Agent setup files are located:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.Agent.Configurator.exe" -setVBRse
ttings /p:"<protection_group_name>.xml"
```

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents. Alternatively, you can specify the full path to the configuration file passed with the `/p` option.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. After you apply new backup policy settings in the Veeam Backup & Replication console, Veeam Agent will get these settings during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.Agent.Configurator.exe" -syncnow
```

Deploying Veeam Agent for Linux

To deploy Veeam Agent for Linux using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Linux and all the required components, do the following:

1. Upload Veeam Agent setup files on the computer you want to protect.

   Keep in mind that you must use Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the installation of the Veeam Agent for Linux in the offline mode. For details, see the Installing Veeam Agent for Linux in Offline Mode section in the Veeam Agent for Linux User Guide.

   Keep in mind that if you use the APT package manager and the installation command reports that some dependencies for package not installed, run the following command instead:

   ```
   apt-get install -f
   ```

   After that, repeat the Veeam Agent installation procedure.

Configuration

To configure Veeam Agent for Linux, you must apply connection settings from the configuration file that you obtained when the protection group for pre-installed Veeam Agents was created. To do this, run the following command from the directory where Veeam Agent setup files are located:

```
veeamconfig mode setVBRsettings --cfg <protection_group_name>.xml
```

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents. Alternatively, you can specify the full path to the configuration file passed with the `--cfg` option.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. After you apply new backup policy settings in the Veeam Backup & Replication console, Veeam Agent will get these settings during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
veeamconfig mode syncnow
```

Deploying Veeam Agent for Unix

To deploy Veeam Agent for IBM AIX or Veeam Agent for Oracle Solaris using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Unix and all the required components, do the following:

1. Upload the installation archive to a directory that can be accessed from the computer where you want to install the product and extract setup files from this archive.

   Keep in mind that you must use the Veeam Agent installation archive that is generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. Navigate to the directory where you have extracted setup files and install Veeam Agent. This procedure is similar to the default installation of the Veeam Agent for Unix. For details, see the following sections:

   - For Veeam Agent for Oracle Solaris, see the Installing Veeam Agent section in the Veeam Agent for Oracle Solaris User Guide.
   - For Veeam Agent for IBM AIX, see the Installing Veeam Agent section in the Veeam Agent for IBM AIX User Guide.

Configuration

To configure Veeam Agent for Unix, you must apply connection settings from the configuration file that you obtained when the protection group for pre-installed Veeam Agents was created. To do this, run the following command from the folder where Veeam Agent setup files are located:

```
veeamconfig mode setVBRsettings --cfg <protection_group_name>.xml
```

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents. Alternatively, you can specify the full path to the configuration file passed with the `--cfg` option.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with the Veeam backup server every 6 hours. After you apply the connection settings, Veeam Agent will use them to connect to backup server during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
veeamconfig mode syncnow
```

Deploying Veeam Agent for Mac

To deploy Veeam Agent for Mac using setup files generated by Veeam Backup & Replication, perform the following operations:

1. Installation
2. Configuration

> **TIP**
>
> You can also find detailed instructions on the Veeam Agent deployment in the `readme.txt` file that is available among the setup files generated by Veeam Backup & Replication.

Installation

To install Veeam Agent for Mac and all the required components, do the following:

1. Upload Veeam Agent setup files on the computer you want to protect.

   Keep in mind that you must use Veeam Agent setup files that are generated by Veeam Backup & Replication after the protection group for pre-installed Veeam Agents is created. To learn more, see Specifying Packages.

2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the default installation of the Veeam Agent for Mac. For details, see the Installing Veeam Agent section in the Veeam Agent for Mac User Guide.

3. Grant full disk access to Veeam Agent for Mac. For details, see the Granting Full Disk Access section in the Veeam Agent for Mac User Guide.

Alternatively, you use install Veeam Agent and grant full disk access using a Mobile Device Management (MDM) solution. For details, see the Installation and Configuration with MDM Solution section in the Veeam Agent for Mac User Guide.

Configuration

To configure Veeam Agent for Mac, you must import connection settings from the configuration file that you obtained when the protection group for pre-installed Veeam Agents was created. For details, see the Importing Configuration Database section in the Veeam Agent for Mac User Guide.

If you use the MDM solution to install Veeam Agent, you must deploy the configuration file as a device profile. For details, see Installation and Configuration with MDM Solution in the Veeam Agent for Mac Use Guide.

Keep in mind that you may need one of the following configuration files depending on the solution that you use:

- `<protection_group_name>.xml`
- `<protection_group_name>_escaped.xml`

where `<protection_group_name>` is a name of the protection group for pre-installed Veeam Agents.

Mind that the connection between Veeam Backup & Replication and Veeam Agent is not persistent. Veeam Agent synchronizes with the Veeam backup server every 6 hours. After you apply the connection settings, Veeam Agent will use them to connect to backup server during the next synchronization.

To synchronize Veeam Agent immediately, run the following command on the Veeam Agent computer:

```
veeamconfig mode syncnow
```

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.

Before working with protection groups, consider the following limitations:

- You can add a protection group for pre-installed Veeam Agents only to a backup policy (Veeam Agent backup job managed by Veeam Agent). Veeam Agent backup jobs managed by the backup server are not supported by this type of protection groups. To learn more about backup job types, see Working with Veeam Agent Backup Jobs and Policies.
- You can add only a protection group for pre-installed Veeam Agents to a backup job for Unix and macOS computers. Other protection groups are not supported for computers running these OSes. To learn more, see Protection Group Types.
- You can add a protection group for cloud machines only to a Veeam Agent backup job managed by the backup server. Backup policies are not supported by this type of protection groups. To learn more about backup job types, see Working with Veeam Agent Backup Jobs and Policies.
- You cannot add both cloud machines and physical computers to the same backup job.
- If you add a protection group that contains computers running different OSes to a Veeam Agent backup job for computers running a certain OS, Veeam Backup & Replication will automatically exclude computers running other OSes from this backup job.

  For example, if you add protection group that contains Microsoft Windows, Linux, and Mac computers to a Veeam Agent backup job for Linux computers, Veeam Backup & Replication will automatically exclude Microsoft Windows and Mac 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

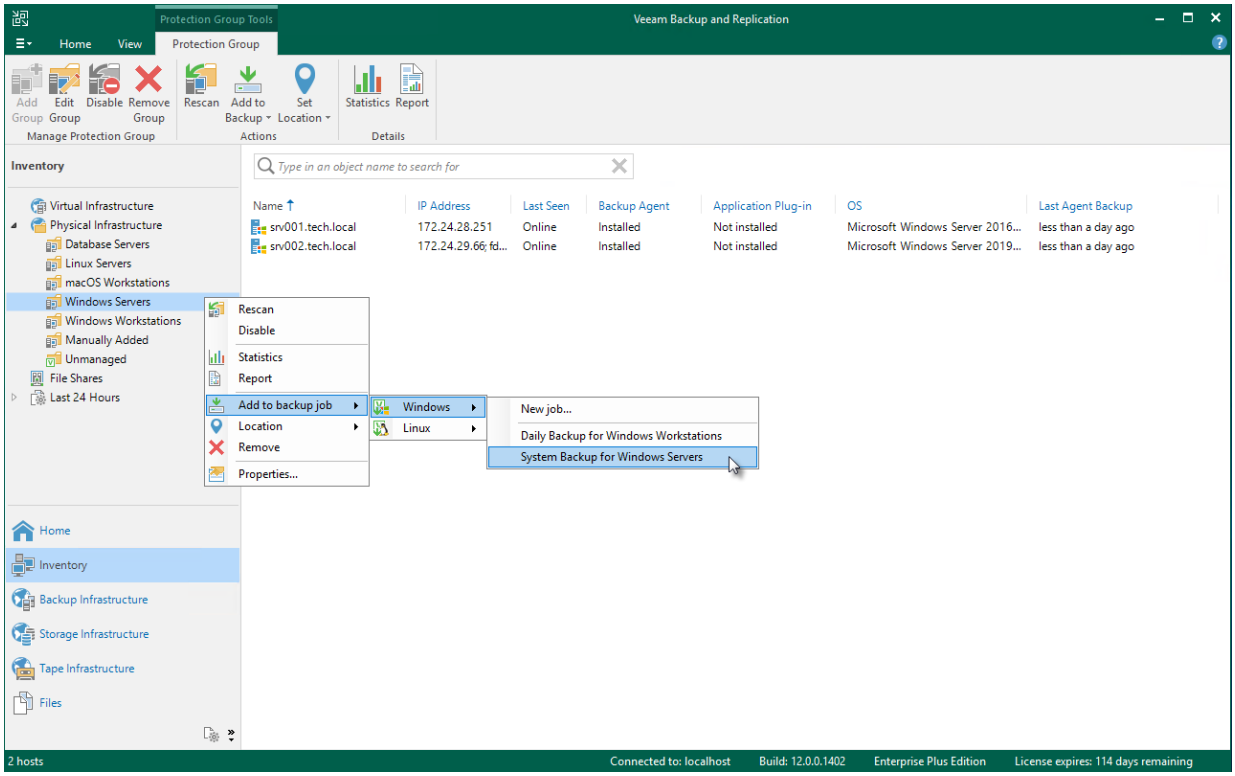
   - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup** > **Linux** > *name of the job* on the ribbon.
   - In the inventory pane, right-click the protection group that you want to add to the backup job and select **Add to backup job** > **Linux** > *name of the job*.

   [For protection groups for pre-installed Veeam Agents] For Unix computers

   - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup** > **Unix** > *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** > **Unix** > *name of the job*.

   [For protection groups for pre-installed Veeam Agents] For Mac computers

   - In the inventory pane, select the protection group that you want to add to the backup job and click **Add to Backup** > **Mac** > *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** > **Mac** > *name of the job*.



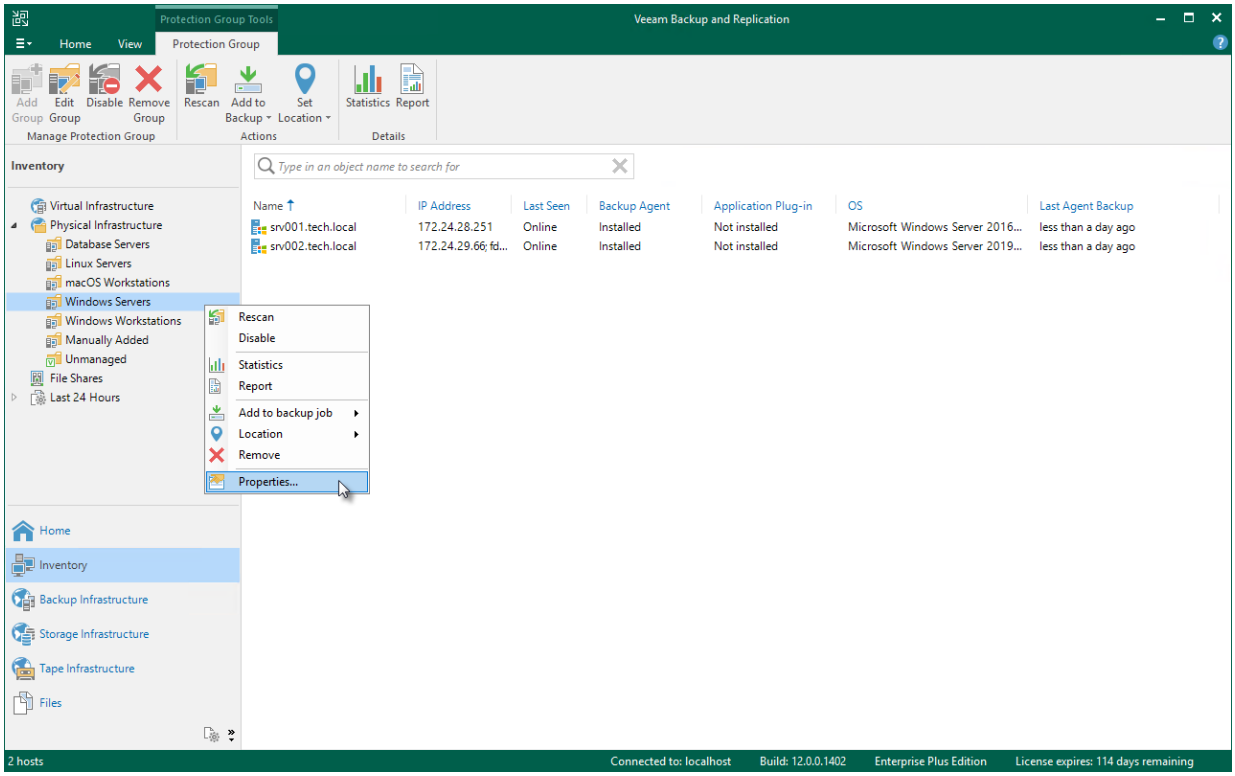
Editing Protection Group Settings

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

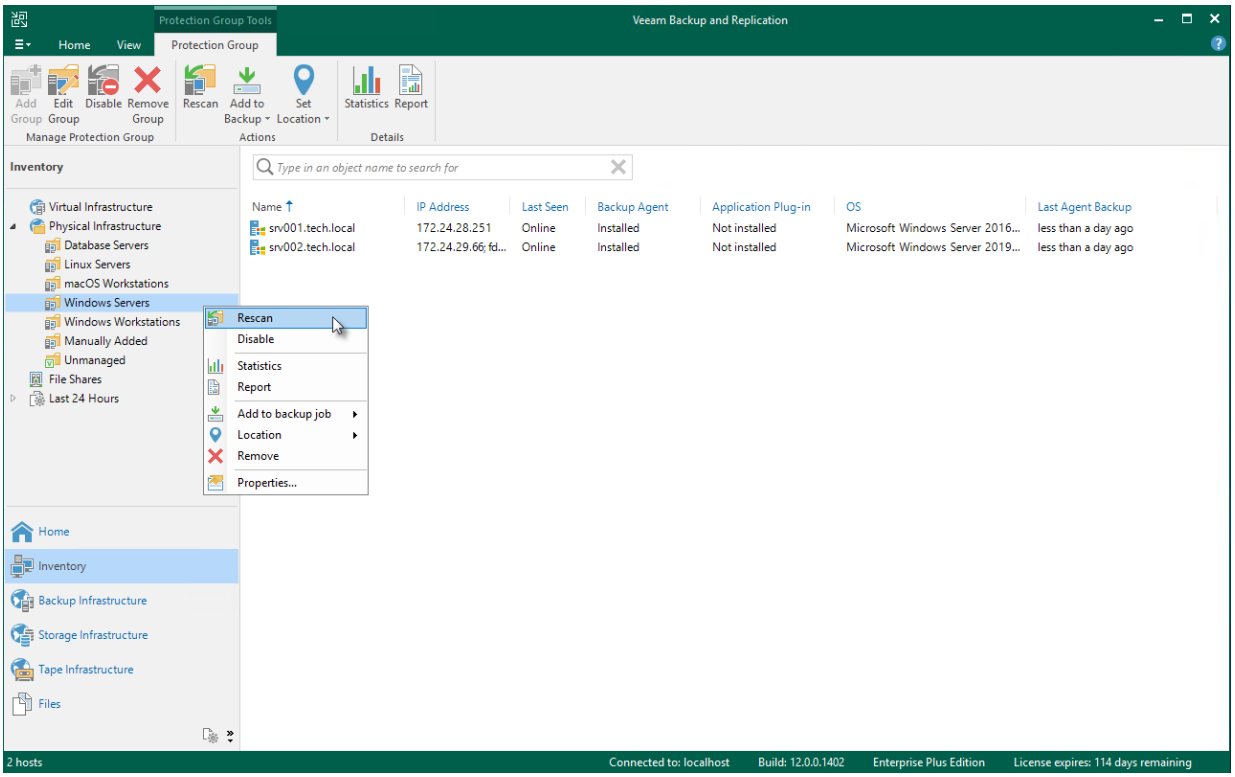
You can rescan a protection group configured in the inventory. When you perform protection group rescan, you manually start the discovery process for the protection group. This operation may be required, for example, if you want to discover new computers added to the protection group without waiting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

> **NOTE**
>
> You cannot rescan a protection group for pre-installed Veeam Agents. To learn more, see Protection Group Types.

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**.

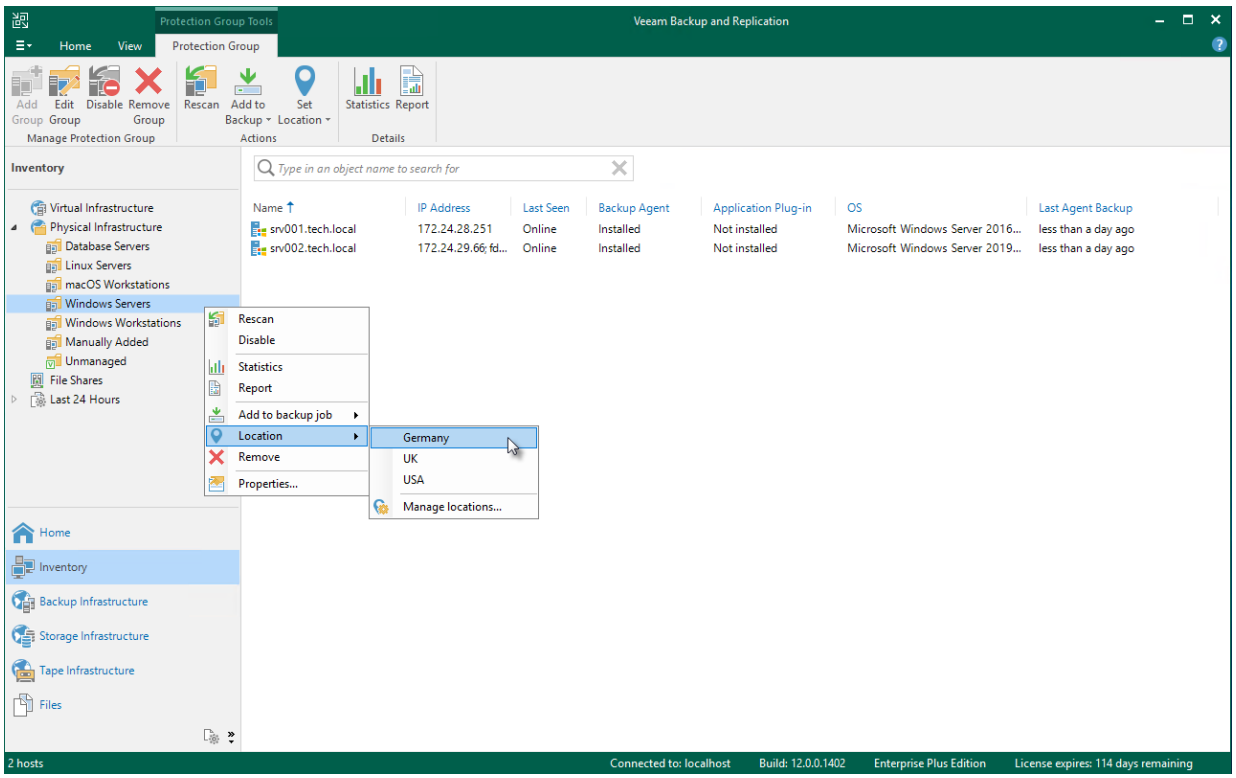


Assigning Location to Protection Group

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 temporary 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:

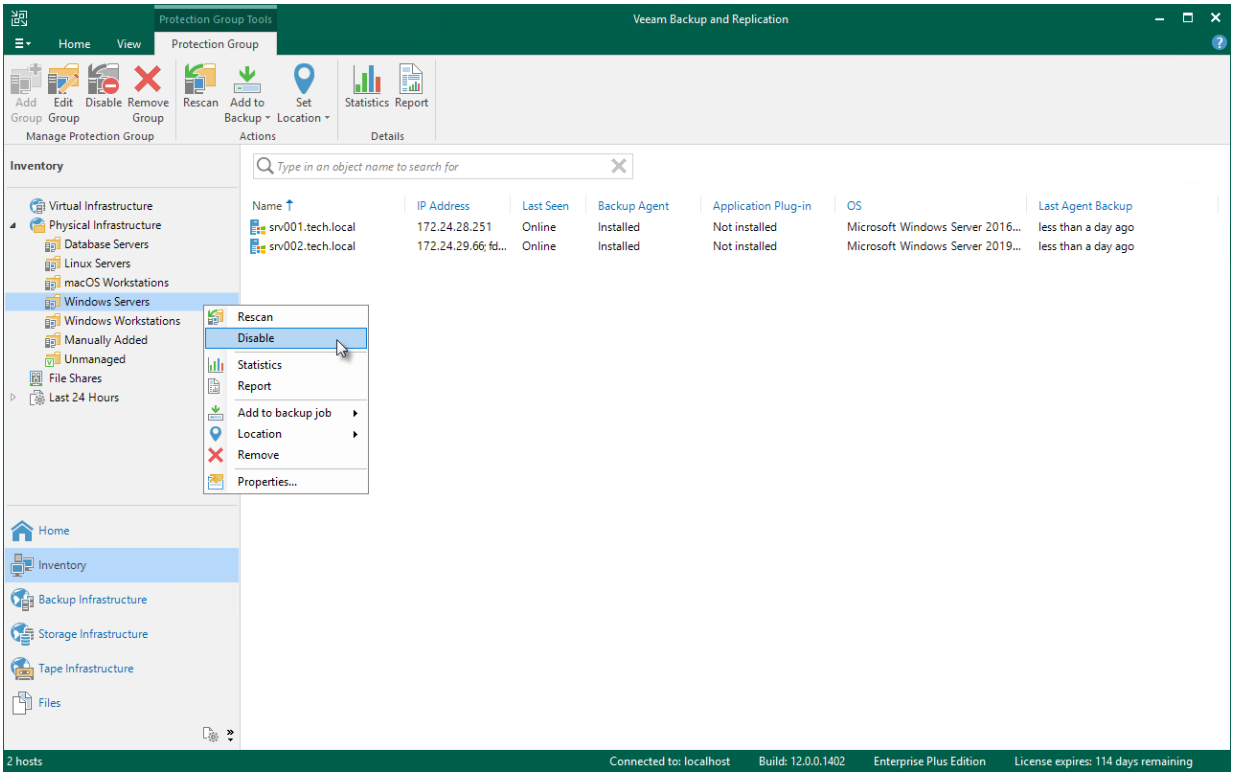
1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Disable** on the ribbon or right-click the necessary protection group and select **Disable**.

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**.

TIP

After you disable a protection group for pre-installed Veeam Agents, Veeam Backup & Replication does not add new members to this protection group. If the Veeam Agent computer user tries to connect to the Veeam backup server with the configuration file, the user will get an error message. To learn more about protection group types, see Protection Group Types.



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.

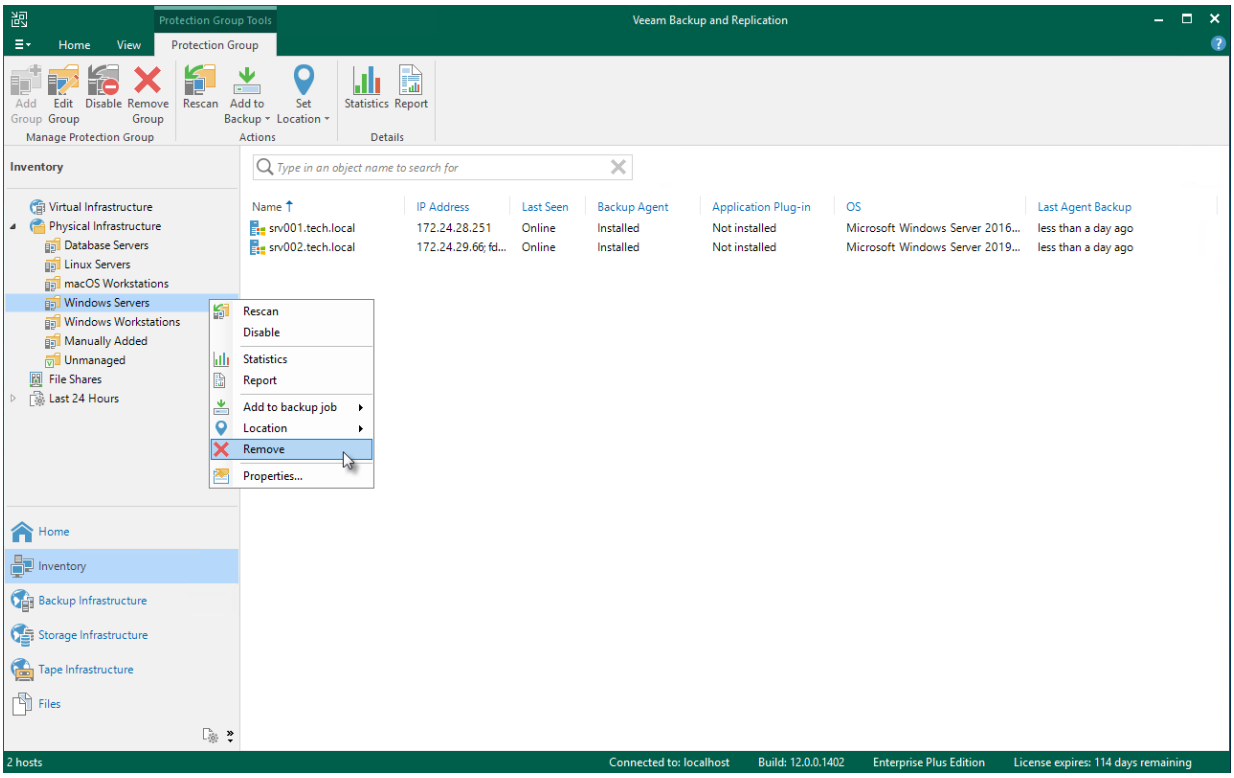
TIP

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 and Policies

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.

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

After you configured a Veeam Agent backup job in Veeam Backup & Replication, you can manage it in Veeam Backup & Replication as well. 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.

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 Veeam Agent Backup Jobs

To create a Veeam Agent backup job, you must create a Veeam Agent backup job in Veeam Backup & Replication with the **Managed by backup server** option selected in the job settings.

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

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

If you want to protect a computer running Unix or macOS, you must create a Veeam Agent backup policy. For details, see Creating Policy for Unix Computers and Creating Agent Backup Policy for Mac Computers.

Creating 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 in a Veeam backup repository and Veeam Cloud Connect repository. If you want to save backups in other target locations, you must configure a Veeam Agent backup job managed by Veeam Agent (backup policy). To learn more, see Veeam Agent Backup Jobs and Policies.
- [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 failover 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 in 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 in a backup repository.
- The backup cache is supported only for Veeam Agent backup jobs managed by Veeam Agent.
- 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.

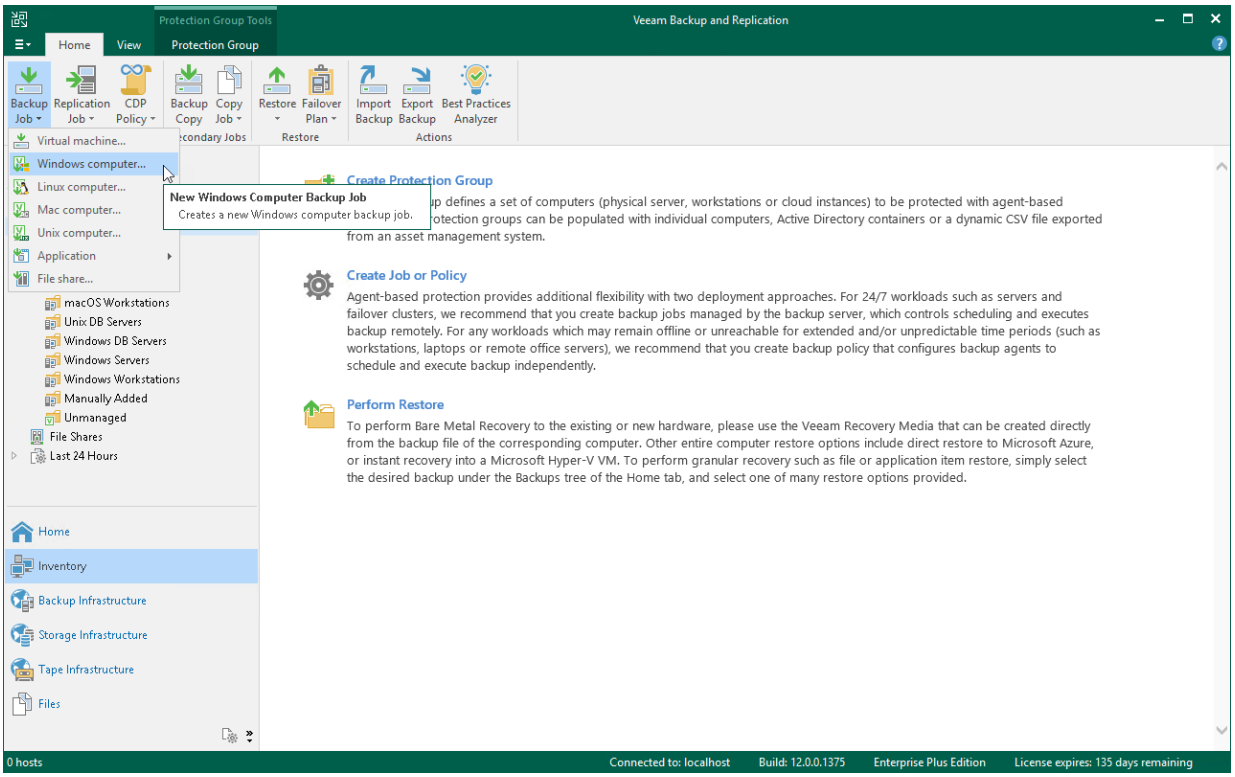
Adding Computers to New Backup Job

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:

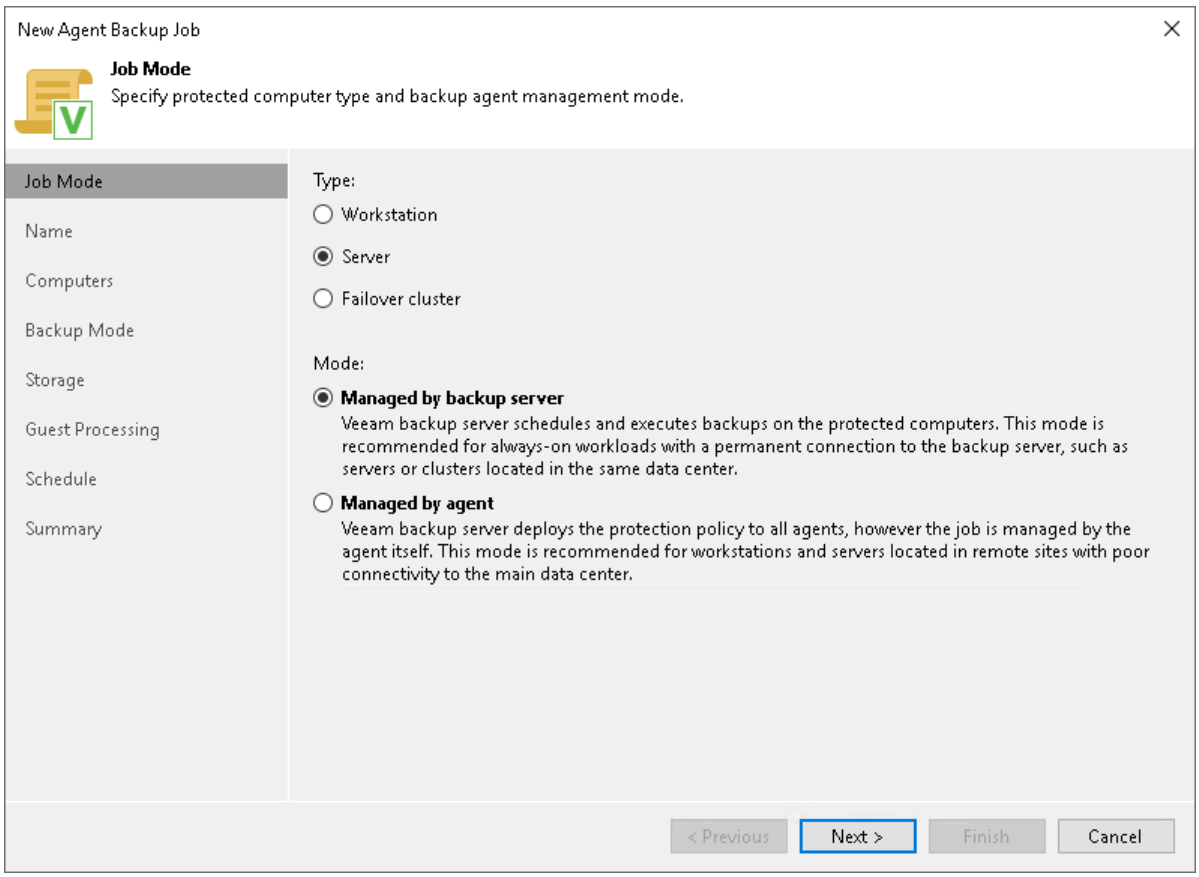
- **Managed by backup server** — select this option if you want to configure the Veeam Agent backup job. With this option selected, you will be able to add one or more individual computers and/or protection groups to the job and instruct Veeam Backup & Replication to create Veeam Agent backups in a Veeam 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.

  > NOTE
  > - The **Managed by backup server** option is available for the **Server** and **Failover cluster** computer types. For **Failover cluster**, this is the only available option. This option is not available for the **Workstation** computer type.
  > - You must select the **Managed by backup server** option if you want to use the backup job to protect cloud machines. To learn more, see Select Protection Group Type.

- **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, in a Veeam backup repository or in a Veeam Cloud Connect repository. To learn more, see Backup Policy.

NOTE

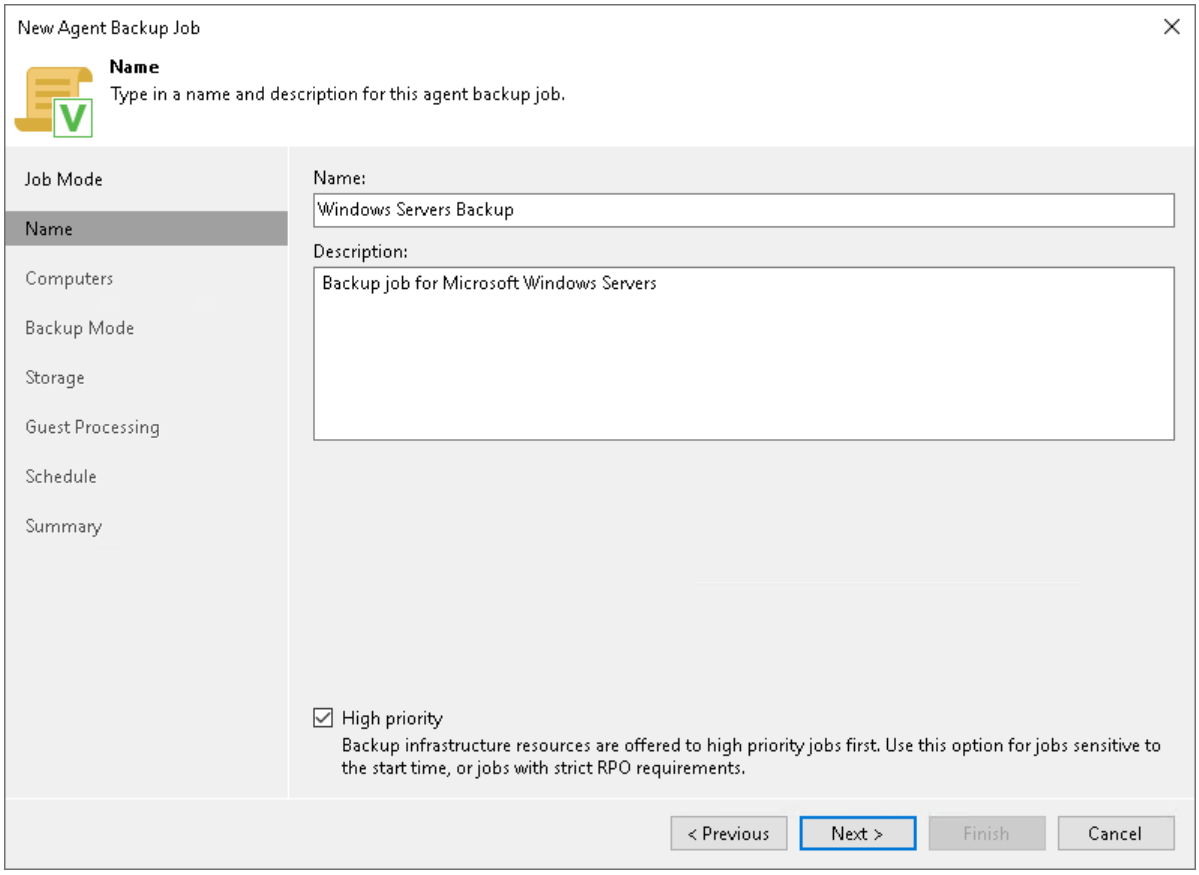
- The **Managed by agent** option is available for the **Workstation** and **Server** computer types. For **Workstation**, this is the only available option. This option is not available for the **Failover cluster** computer type.
- You must select the **Managed by agent** option if you want to use the backup job to protect computers with pre-installed Veeam Agents. To learn more, see Select Protection Group Type.



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.
3. [For backup job managed by backup server] Select the **High priority** check box if you want the resource scheduler of Veeam Backup & Replication to prioritize this job higher than other similar jobs and to allocate resources to it in the first place. To learn more, see the Job Priorities section in the Veeam Backup & Replication User Guide.



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.
- Veeam Backup & Replication displays protection groups for pre-installed Veeam Agents and their members only if you selected the **Managed by agent** option at the **Job Mode** step of the wizard. You cannot add protection groups for pre-installed Veeam Agents to backup jobs managed by backup server. To learn more, see Selecting Job Mode.
- Veeam Backup & Replication displays protection groups for cloud machines and their members only if you selected the **Managed by backup server** option at the **Job Mode** step of the wizard. You cannot add protection groups for cloud machines to backup policies (backup jobs managed by backup Veeam Agent). To learn more, see Selecting Job Mode.

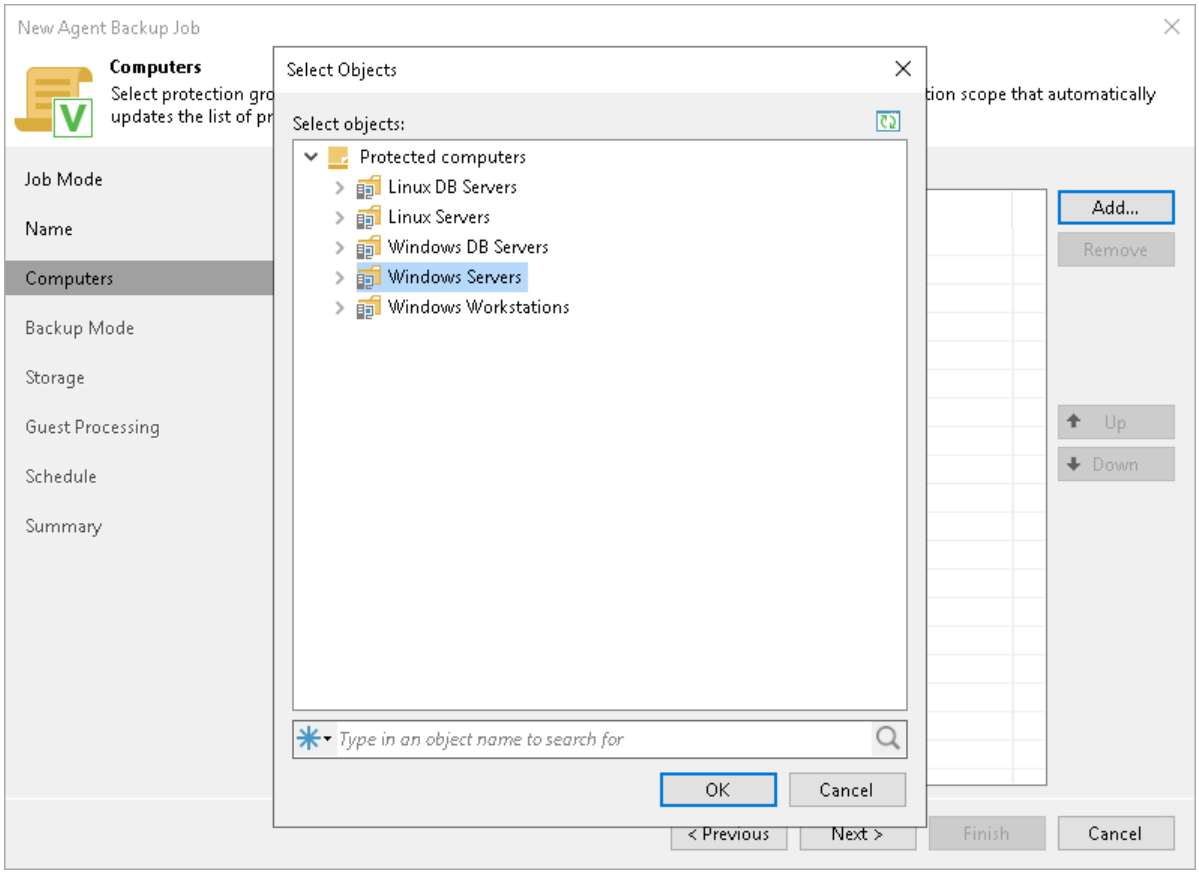
Adding Protection Groups and Computers from Inventory

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.

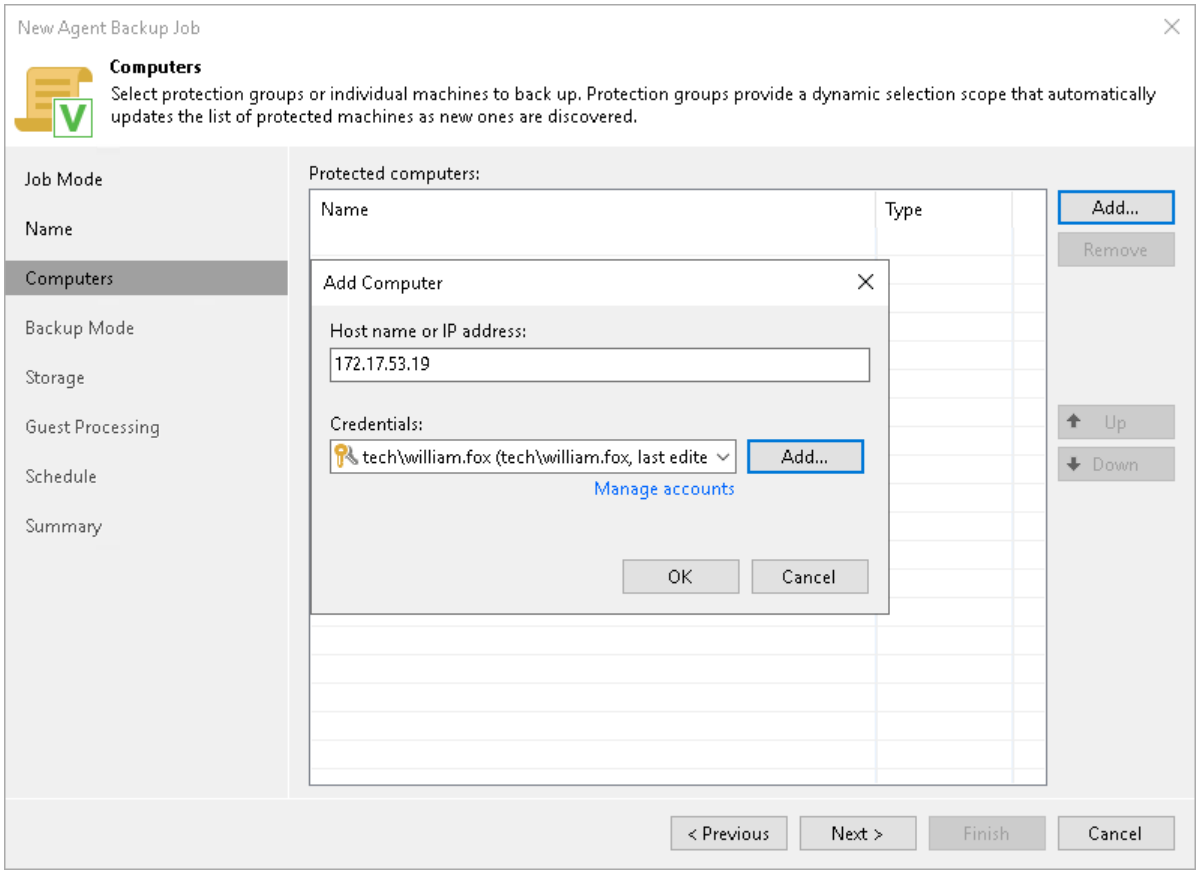
1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



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.



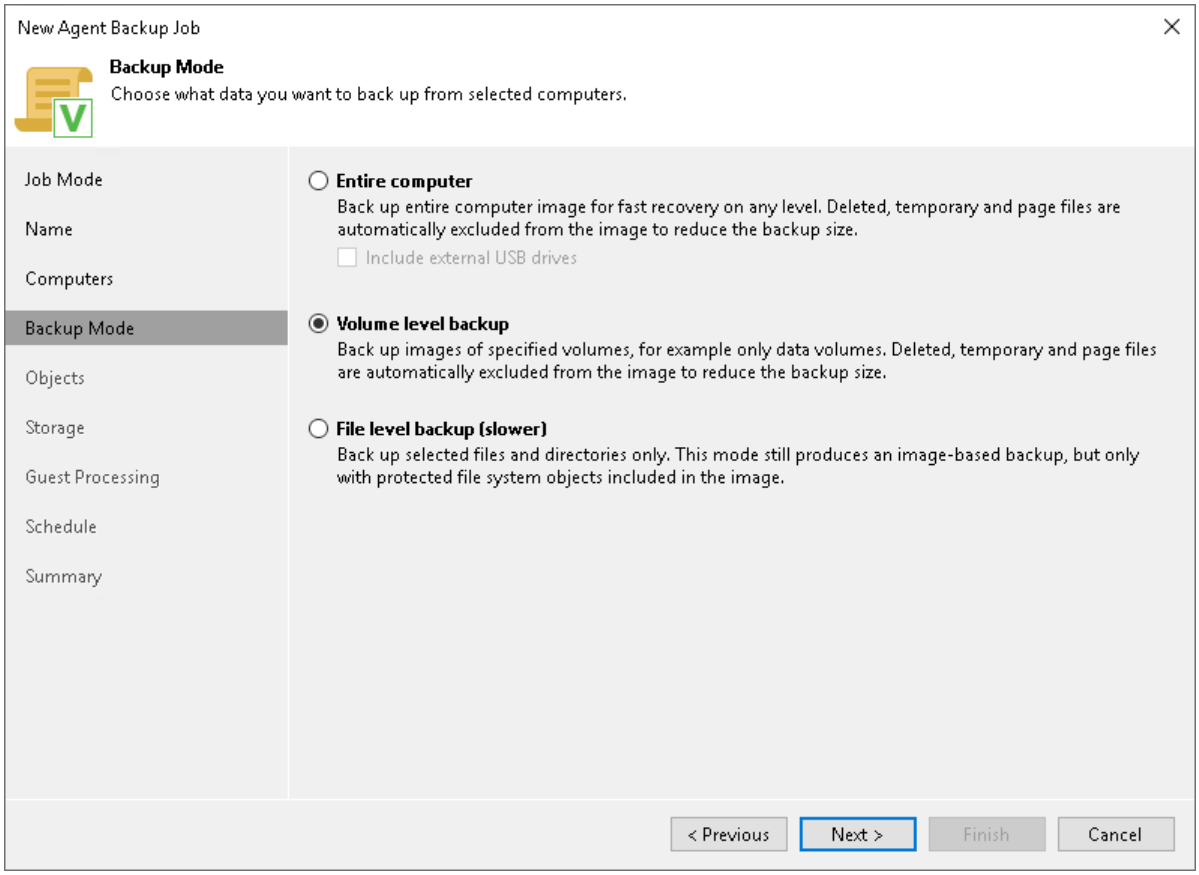
Step 5. Select Backup Mode

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 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

- 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, you can select the **Backup the following volumes only** option and add necessary objects.

Alternatively, you can back up the whole Veeam Agent computer. To do this, select the **Backup all volumes except the following** option. With this option selected, you can exclude objects that you do not need from the backup scope.

You can include or exclude the following objects:

- *OS volume* — data pertaining to the OS installed on a protected computer. This object includes the Microsoft Windows system partition and boot partition of your computer. For GPT disks on Microsoft Windows 8.1, 10, 11, 2012, 2012 R2, 2016, 2019, and 2022, the object additionally includes the recovery partition. To learn more, see the System State Data Backup section in the Veeam Agent for Microsoft Windows User Guide.

  To include or exclude the OS volume, in the necessary wizard section, click **Add** and select the **OS volume** option.

- *Individual volumes.*

  To include or exclude individual volumes:

  a. In the necessary wizard section, click **Add** and select the **Volume name** option.

  b. In the **Add Object** window, type the drive letter of a volume that you want to back up, for example, `C:\`, and click **OK**.

  c. Repeat steps a-b for all volumes that you want to back up.

- *Individual mount points.*

  To include or exclude individual mount points:

  a. In the necessary wizard section, click **Add** and select the **Volume name** option.

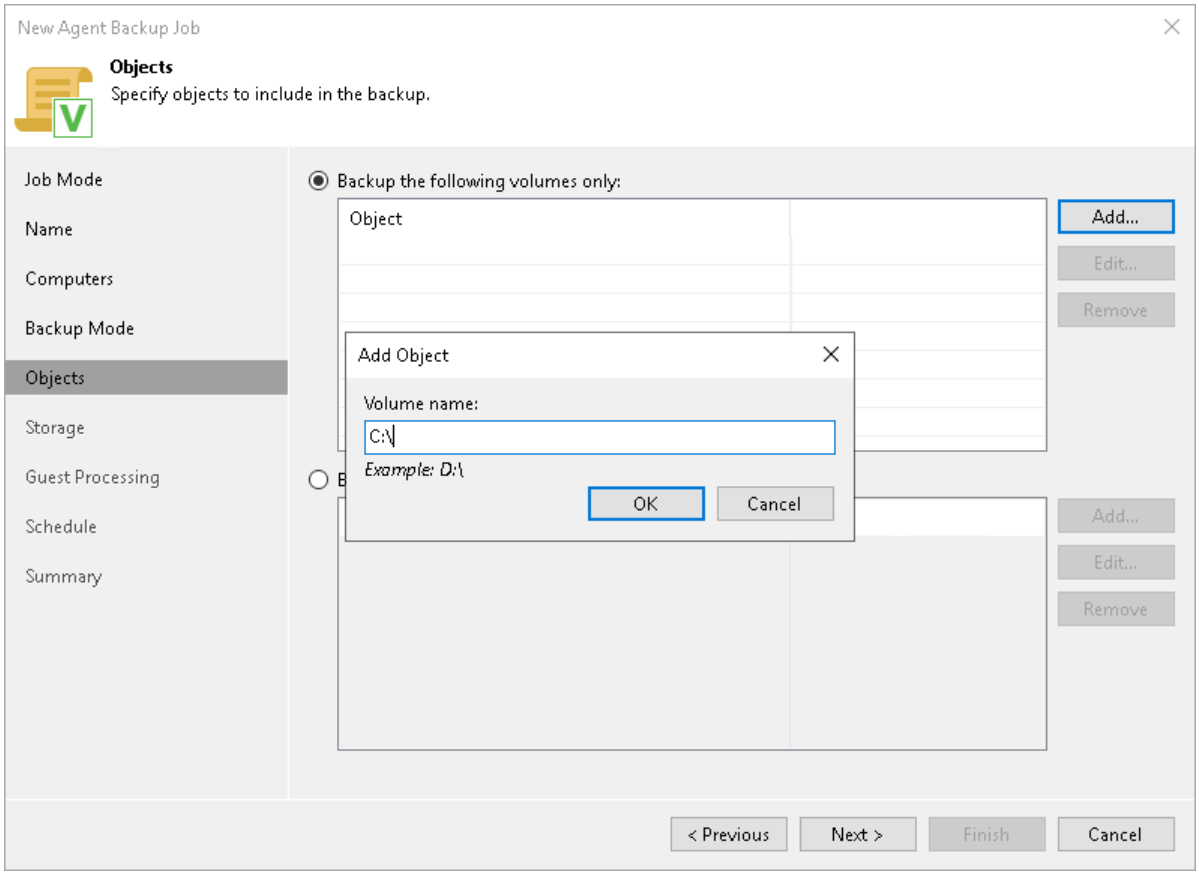
  b. In the **Add Object** window, type the path to a folder that is an entry point to the mounted volume you want to back up, for example, `C:\Data`, and click **OK**.

  c. Repeat steps a-b for all mount points 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.
- You cannot include volumes located on virtual hard disks (VHD or VHDX) in the volume-level backup.
- 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 **Objects to backup** list, select check boxes next to necessary objects. You can include the following data in the backup:

- *Operating system* — data related to the OS installed on a protected computer. To learn more, see the System State Data Backup section in the Veeam Agent for Microsoft Windows User Guide.
- *Personal files* — data related to user profiles. With this option enabled, Veeam Backup & Replication will include in the backup scope settings and data related to Veeam Agent computer user profiles. To learn more, see the Personal Data Backup section in the Veeam Agent for Microsoft Windows User Guide.
- *Individual file system objects* — folders, mount points, and 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, mount point 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 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.

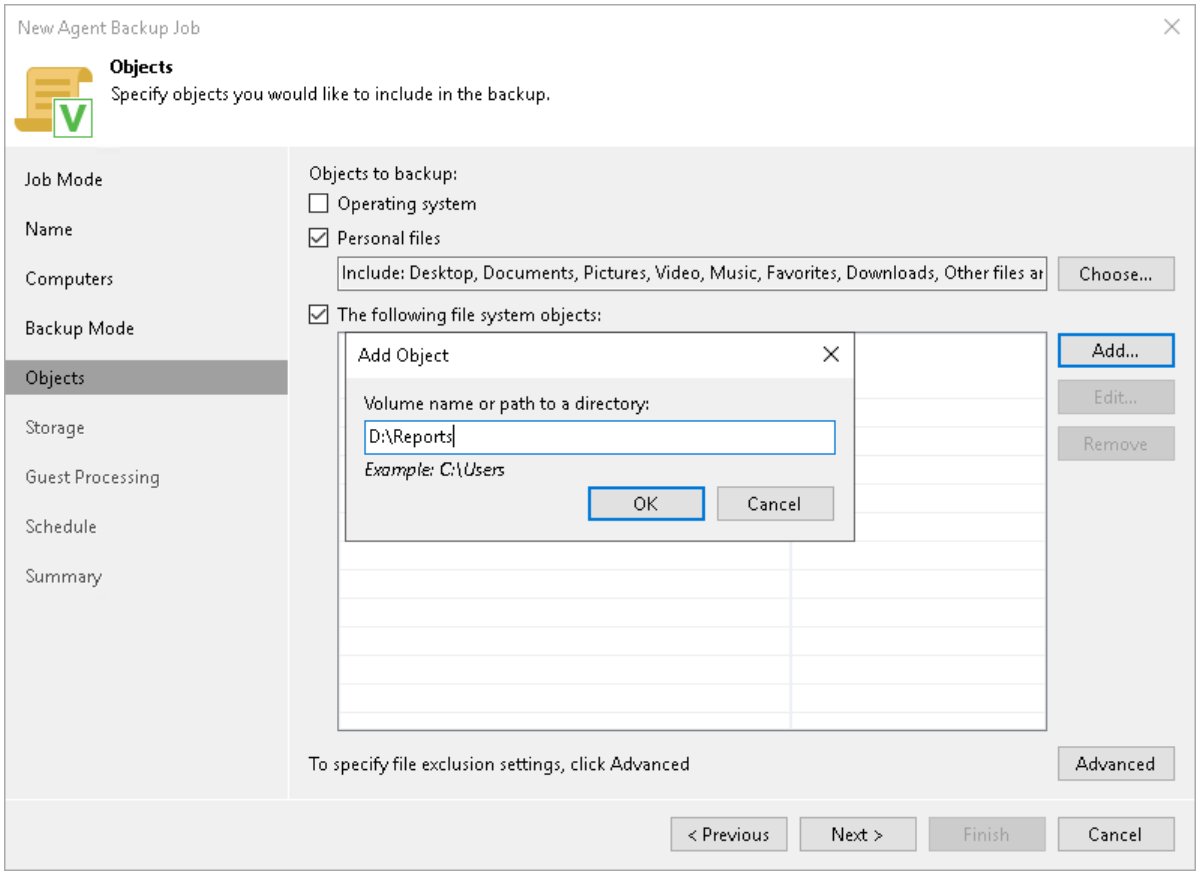
   Consider the following:

   - 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 items that you want to back up.

NOTE

Mind the following:

- If you include a system volume in the file-level backup, Veeam Agent 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 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.
- You can exclude Microsoft OneDrive folders from the backup scope in the File Filters window.



Configuring Filters

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

> **NOTE**
>
> Consider the following:
>
> - If you include a specific folder in the file-level backup, Veeam Agent applies filters to files in specific folders that you include in the backup. Filters are not applied to computer volumes, mount points, and folders selected for backup. If you plan to create a hybrid backup that will contain volumes, mount points, and folders, filters will be applied to files in folders only.
> - If you include a whole volume in the file-level backup, you cannot apply filters to include or exclude files of a specific type in/from the backup. You can only exclude specific folders that reside on the volume.
> - You cannot apply filters to files and folders that reside on the mount point.

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.

     Keep in mind that depending on the backup type, Veeam Agent excludes files and folders from the backup scope differently:

     - For the volume-level backup, content of folders you do not want to back up is excluded from the VSS snapshot with the FilesNotToSnapshot registry key.

- For the file-level backup, folders and files are excluded by Veeam Agent after the VSS snapshot is created.

As a result, some objects may be excluded or not excluded from the backup scope depending on the type of the created backup. For example, if you configure a volume-level backup, the objects that you excluded may stay in the backup scope due to the FilesNotToSnapshot registry key limitations. To learn more, see this Microsoft article.

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

> **TIP**
>
> 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 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:

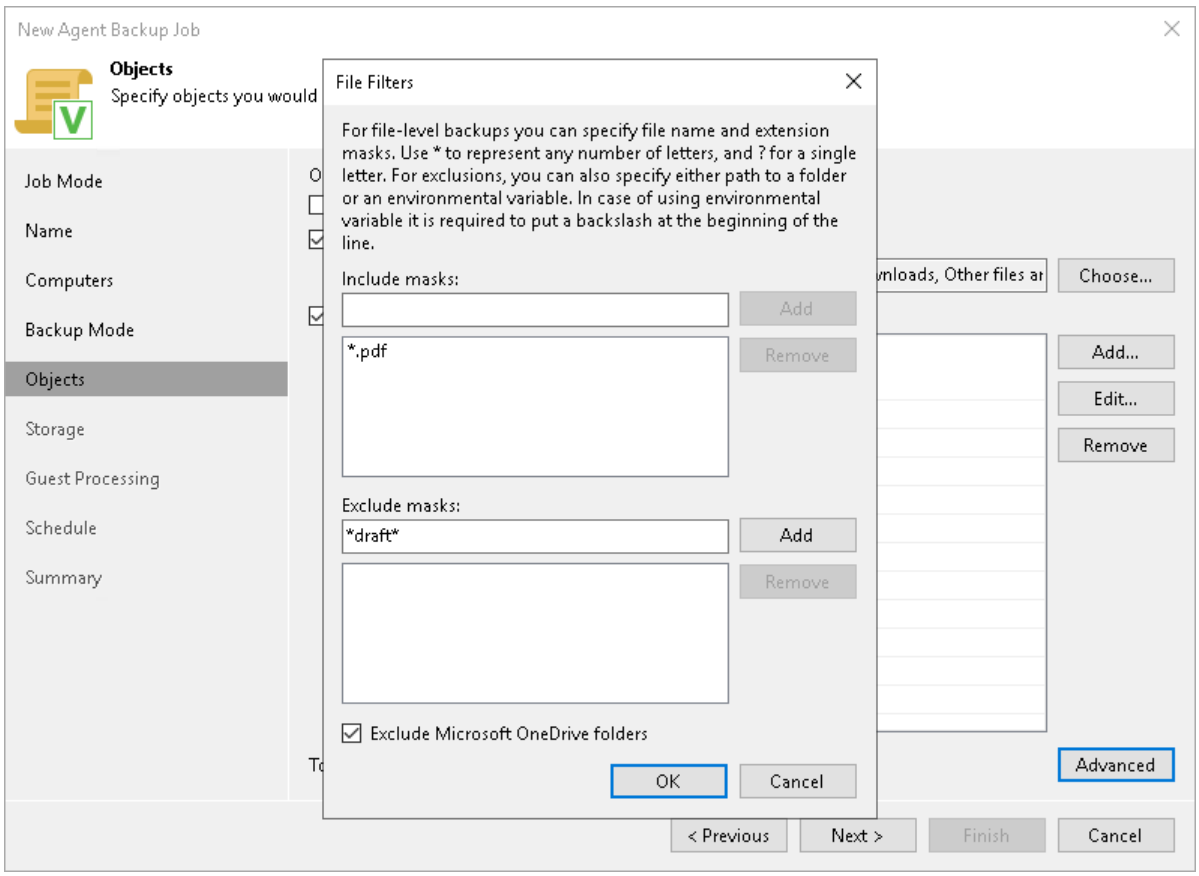
- Include mask: `*.pdf`
- Exclude mask: `*draft*`

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

Additionally, you can specify how Veeam Agent for Microsoft Windows will process Microsoft OneDrive folders. Select the **Exclude Microsoft OneDrive folders** option to exclude Microsoft OneDrive folders and their content from the backup scope.

Consider the following limitation:

- Veeam Agent excludes Microsoft OneDrive folders only in file-level backups. If you include an entire volume in the backup, Veeam Agent will not exclude Microsoft Onedrive folders from this volume.
- Due to the OS limitations, the **Exclude Microsoft OneDrive folders** option behaves properly only on Veeam Agent computers running Microsoft Windows 10. If your Veeam Agent computers run other OS versions, we recommend to exclude Microsoft OneDrive folders manually.



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.

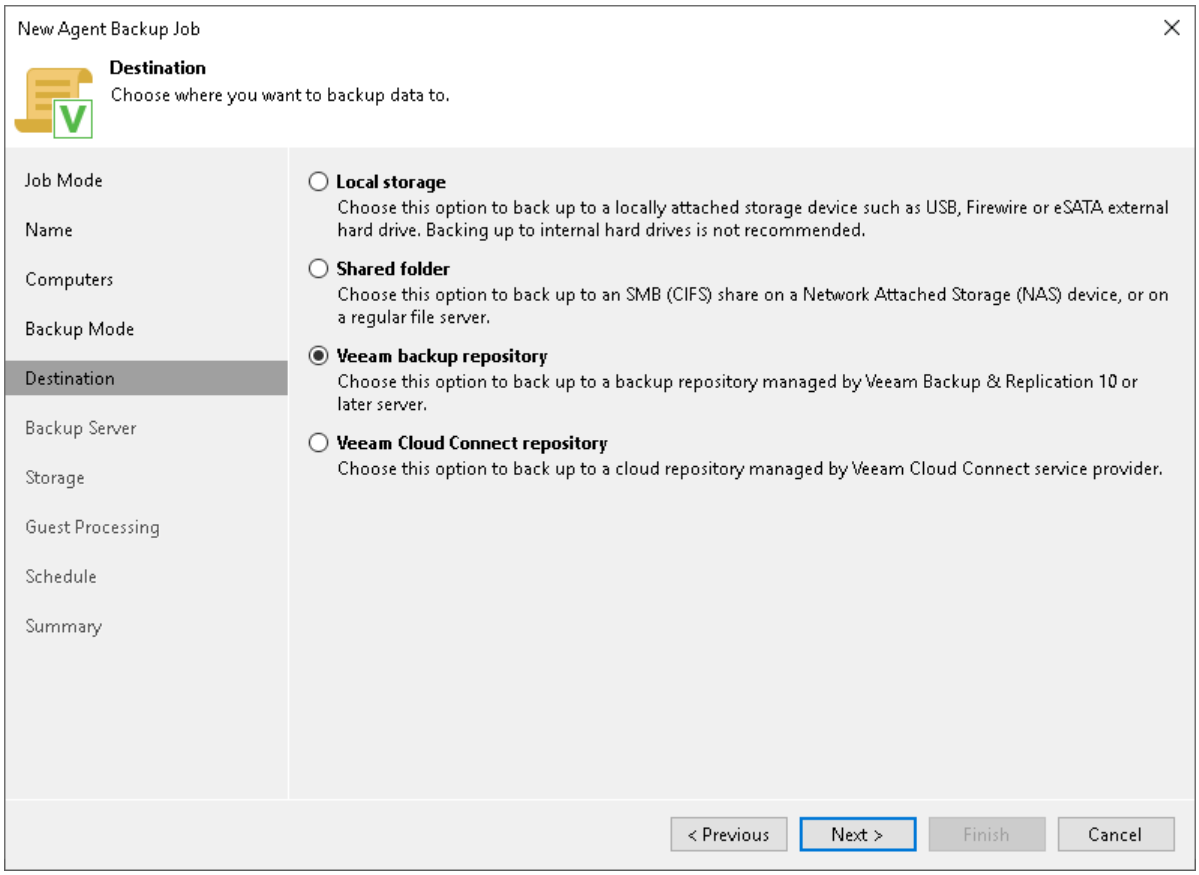
You can store backup files in one of the following locations:

- **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 in 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 in 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 in 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 in a backup repository managed by this Veeam backup server or in 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:
  - 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:

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.

   > **NOTE**
   >
   > Keep in mind when you work with cloud machines, Veeam Backup & Replication displays only AWS or Azure object storage repositories depending on the type of cloud machine you selected to back up.

2. You can map the job to a specific backup stored in 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 in 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 in 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:
   >
   > - The **Map backup** link is available only for a Veeam Agent backup job managed by the backup server. If you want to map a backup job managed by Veeam Agent, see Backup Job Mapping.
   > - 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.

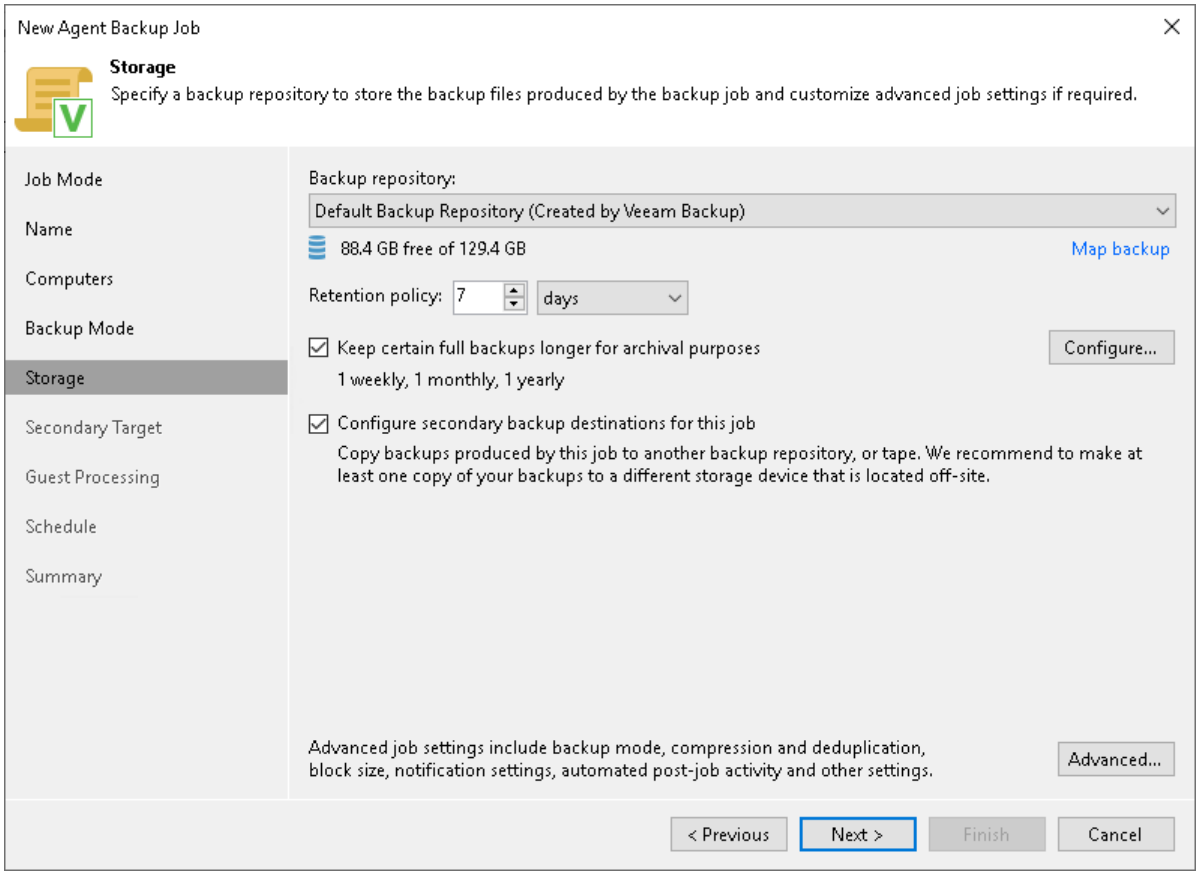
3. Specify short-term backup retention policy settings in one of the following ways:
   - From the **Retention policy** list, select *restore points* and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps 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 certain 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 Long-Term Retention Policy (GFS) 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.
   > - We do not recommend targeting a backup job at the storage device with the exFAT file system. If the protected computer runs Microsoft Windows 10 or Microsoft Windows Server 2019 and later, this configuration may lead to the backup data corruption caused by the exFAT file system issue.

2. Specify short-term backup retention policy settings in one of the following ways:

   - 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.

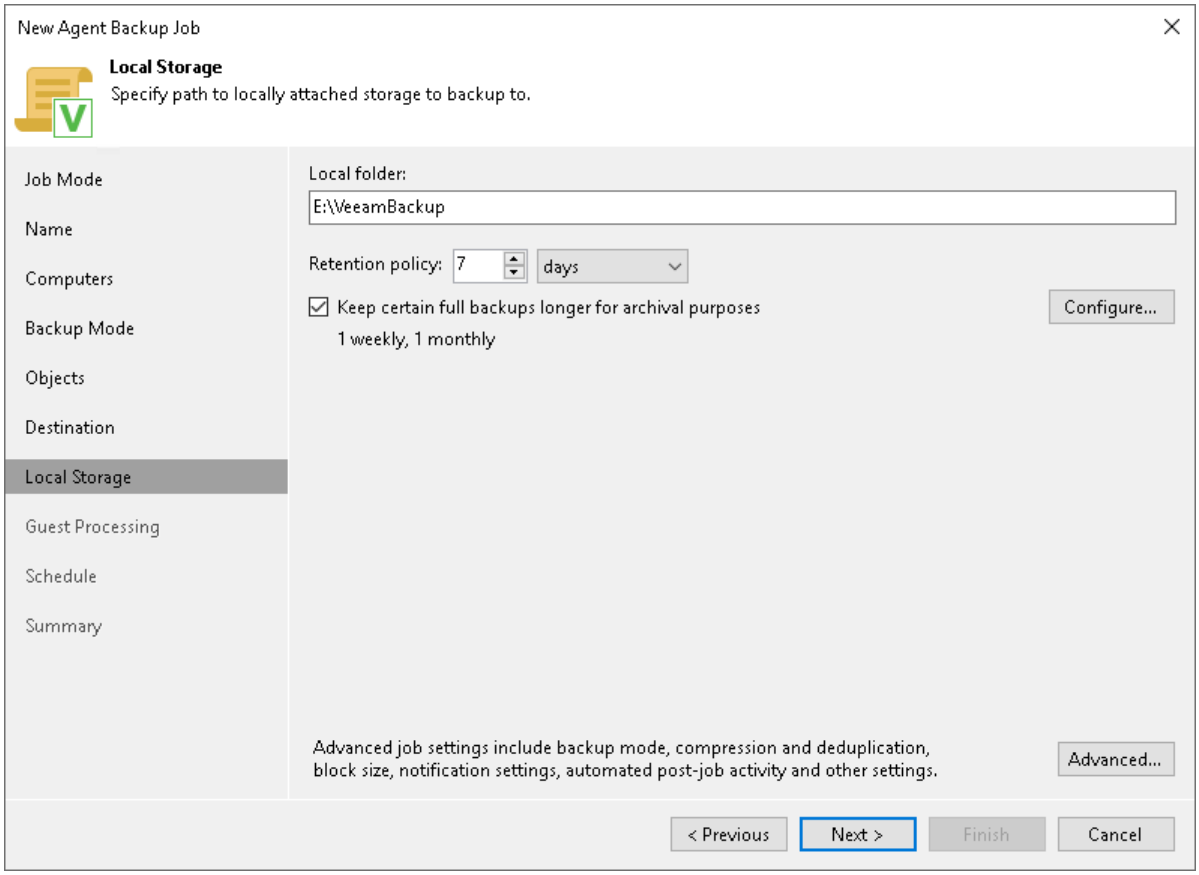
     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

   > **NOTE**
   > The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
   > - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
   > - The Retention Policy in Server Edition section about retention policy using that Veeam Agent retains restore points for a certain number of days or retains the number of latest restore points.

3. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

4. 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.

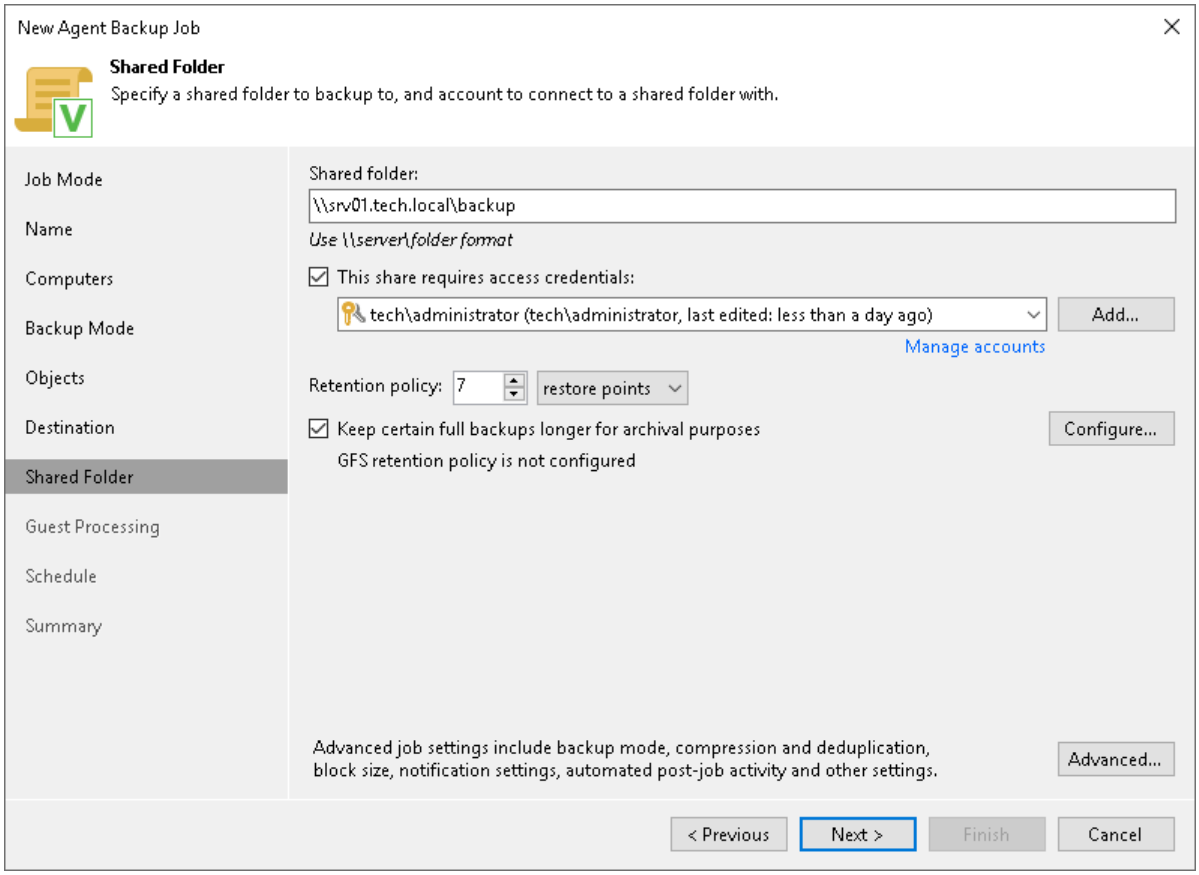
   If you do not select the **This share requires access credentials** check box, Veeam Agent for Microsoft Windows will connect to the shared folder using the *NT AUTHORITY\SYSTEM* account of the computer where the product is installed. You can use this scenario if the Veeam Agent computer is joined to 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 short-term backup retention policy settings in one of the following ways:
   - 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.

     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

   > **NOTE**
   > The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
   > - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
   > - The Retention Policy in Server Edition section about retention policy using that Veeam Agent retains restore points for a certain number of days or retains the number of latest restore points.
4. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

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 in a Veeam backup repository, specify settings to connect to the backup repository:

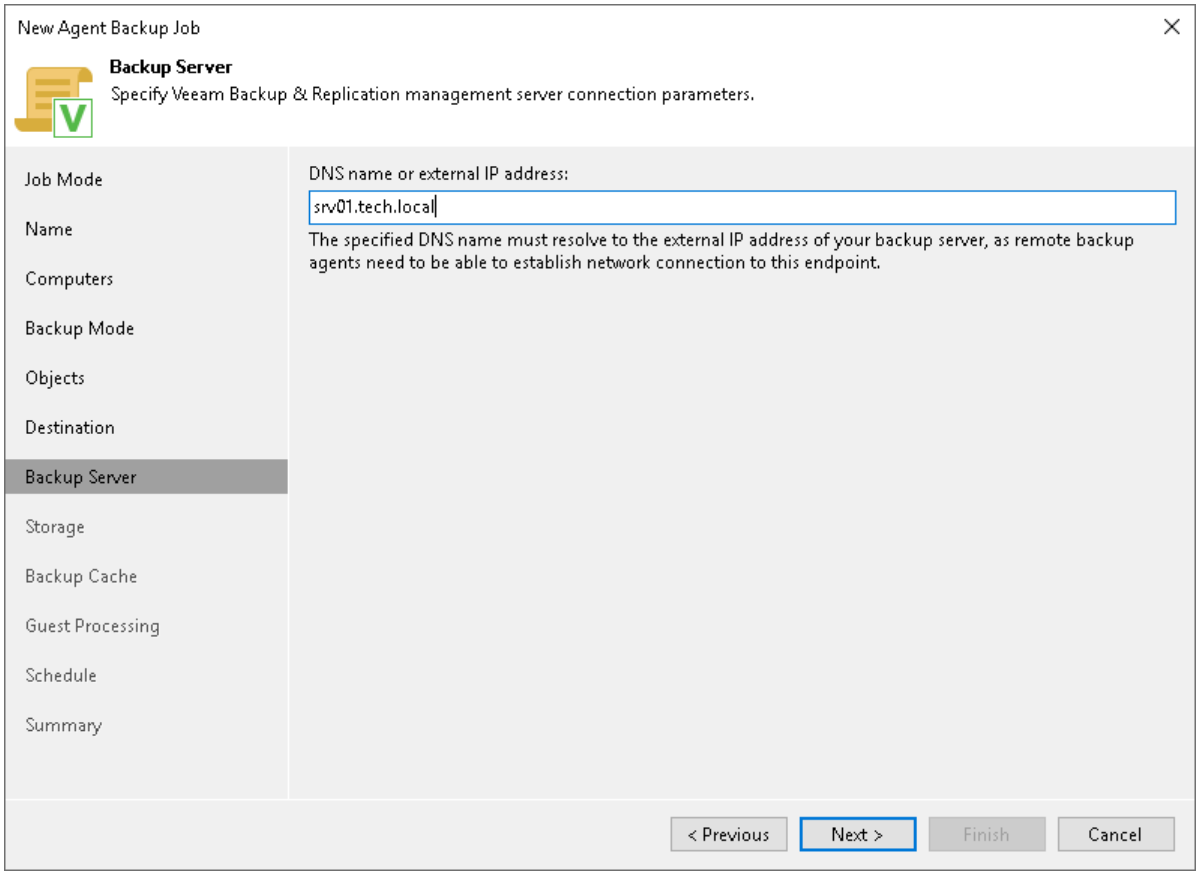
1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Storage step of the wizard, select the Veeam backup repository.

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 in 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.



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 in 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. Specify short-term backup retention policy settings in one of the following ways:
   - 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.

     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

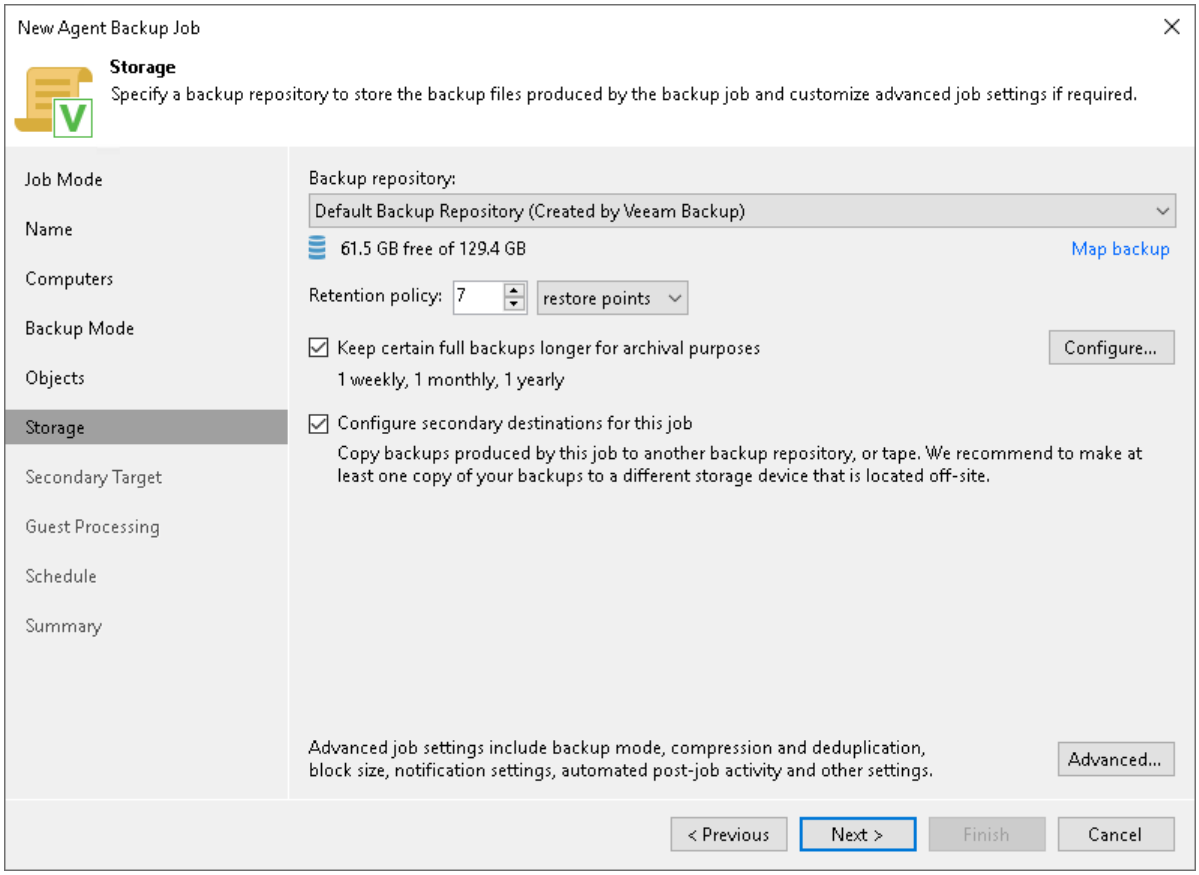
   > **NOTE**
   > The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
   > - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
   > - The Retention Policy in Server Edition section about retention policy using that Veeam Agent restore points for a certain number of days or retains the number of latest restore points.

3. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.
4. 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.
5. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.

TIP

You can map the job to a specific backup stored in the Veeam 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 in this new backup repository. To learn more, see Backup Job Mapping.



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 in a Veeam Cloud Connect repository.

> **NOTE**
>
> Keep in mind that FQDN or IP addresses of Veeam Agent computers 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.

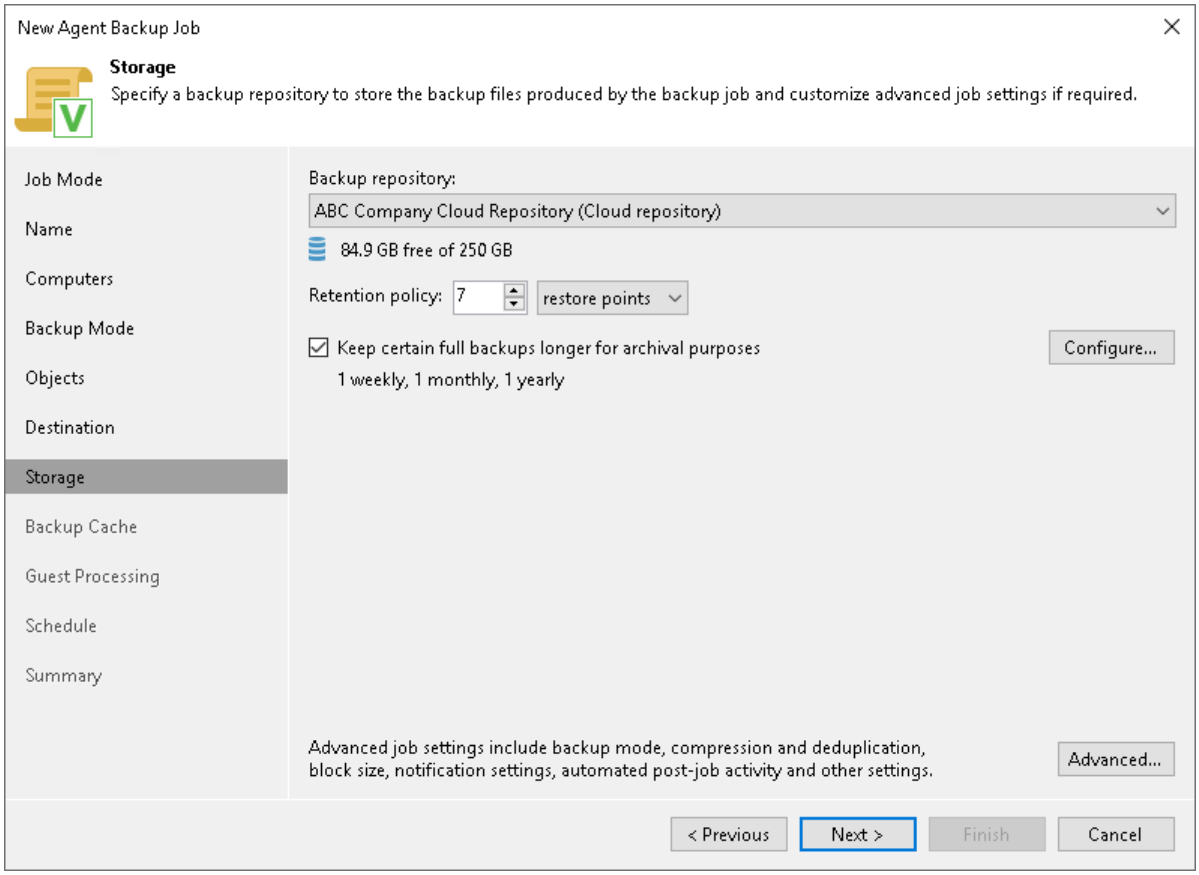
Specify settings for the cloud repository:

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 in the repository.
2. Specify short-term backup retention policy settings in one of the following ways:
   - 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.

     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

     > **NOTE**
     >
     > The short-term retention policies for backups of workstations and servers are the same as in Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more about retention policies, see the following sections in the Veeam Agent for Microsoft Windows User Guide:
     > - The Retention Policy in Free and Workstation Editions section about retention policy using that Veeam Agent retains restore points for a certain number of days.
     > - The Retention Policy in Server Edition section about retention policy using that Veeam Agent restore points for a certain number of days or retains the number of latest restore points.
3. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

4. 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] Integration 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 in 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.

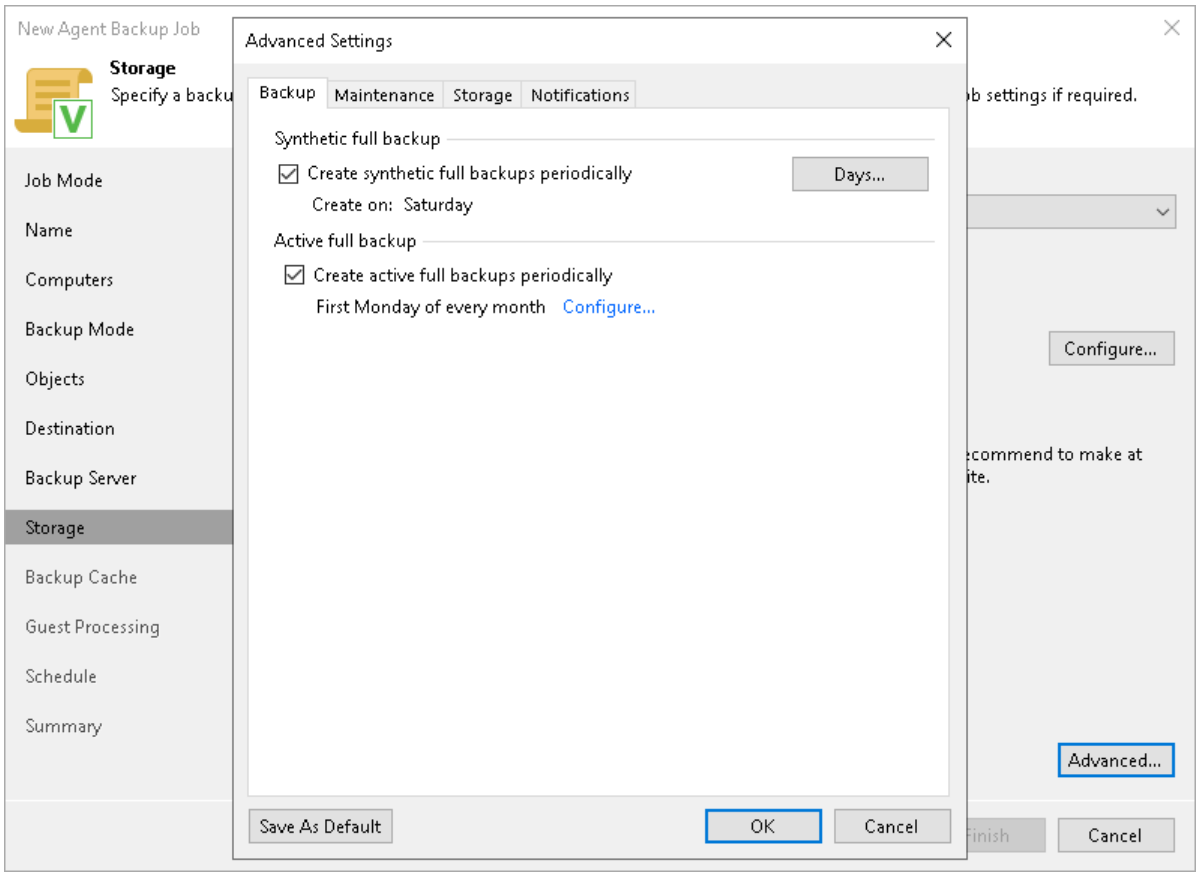
   > **NOTE**
   >
   > Synthetic full backup is not available for backup jobs targeted at an object storage repository.

3. If you want to periodically create active full backups, select the **Create active full backups periodically** check box. To define scheduling settings, click **Configure**.

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 in 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. To specify the schedule for the health check, click **Configure**.

   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.

   > **NOTE**
   >
   > For object storage, Veeam Agent offers a special health check mechanism as default. To run the health check for object storage, enable the **Perform backup files health check** option in the **Storage-level corruption guard** section and specify the health check schedule.
   >
   > You can also switch from the health check for object storage to the standard health check. To do so, select the **Verify content of each object in backup** check box in the backup job settings. Keep in mind that enabling this setting may result in additional charges from your object storage provider.

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. To specify the schedule for the compact operation, click **Configure**. 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.

   > **NOTE**
   >
   > The **Defragment and compact full backup file** option is not available for backup jobs targeted at object storage.

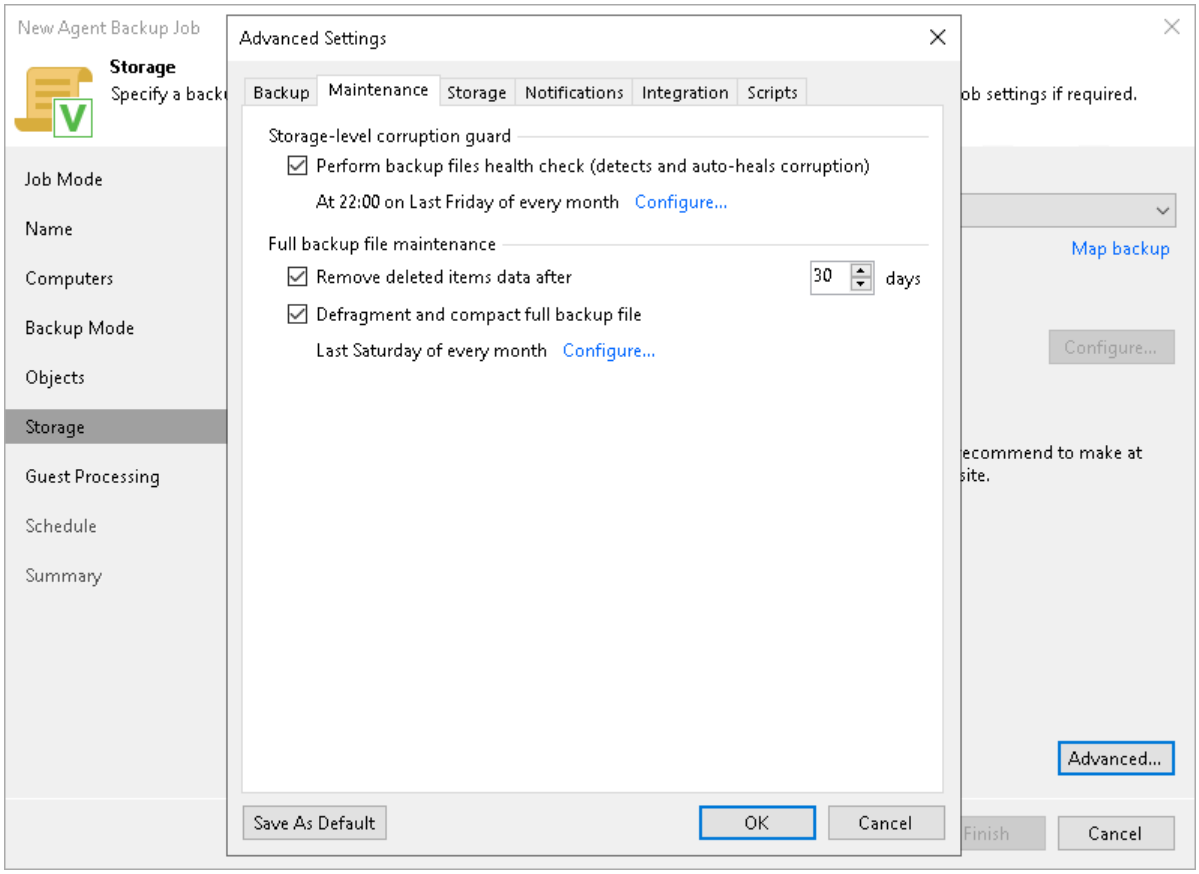
   The compact operation differs depending on the type of the backup job.

   - 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 computer that has only one restore point and this restore point is older than 7 days, Veeam Backup & Replication will not extract data for this computer 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 in 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 in 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 size of data blocks you plan to use: *4 MB, 1 MB, 512 KB, 256 KB*. Veeam Agent for Microsoft Windows will use data blocks of the chosen 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.

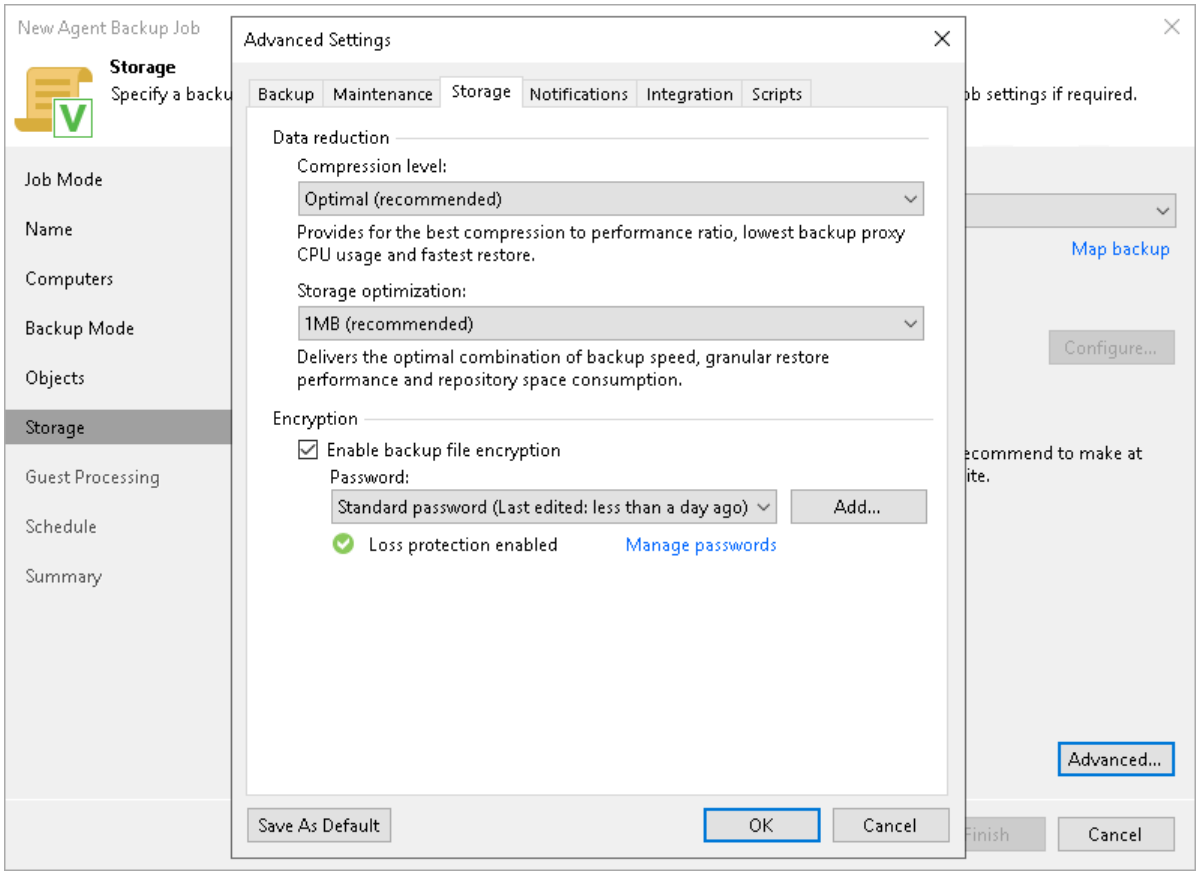
NOTE

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, at a network shared folder, or at a cloud repository. 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.


New Agent Backup Job
Storage
Specify a backu
Job Mode
Name
Computers
Backup Mode
Objects
Storage
Guest Processing
Schedule
Summary
Advanced Settings
Backup
Maintenance
Storage
Notifications
Integration
Scripts
Data reduction
Compression level:
Optimal (recommended)
Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.
Storage optimization:
1MB (recommended)
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.
Encryption
Enable backup file encryption
Password:
Standard password (Last edited: less than a day ago)
Add...
Loss protection enabled
Manage passwords
Save As Default
OK
Cancel
ob settings if required.
Map backup
Configure...
ecommend to make at
ite.
Advanced...
Finish
Cancel

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

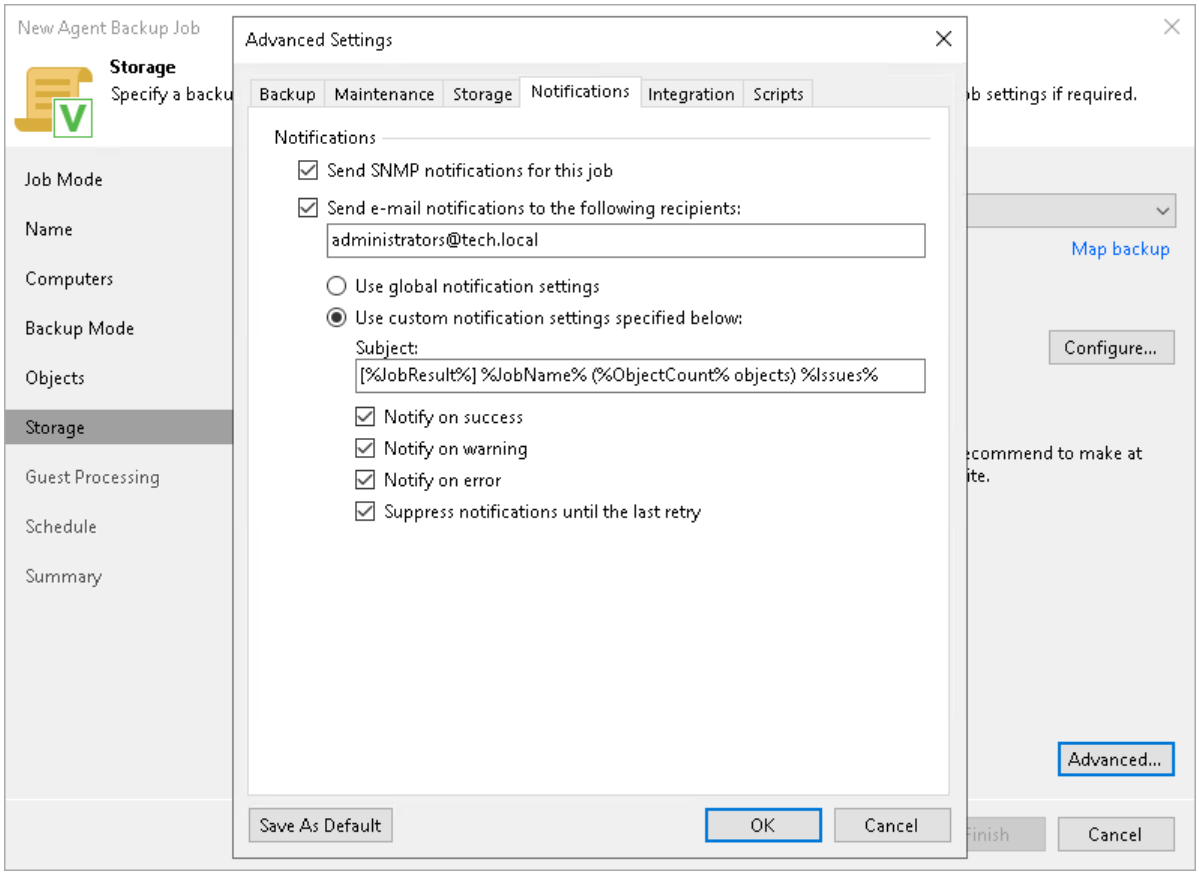
To specify notification settings for the backup job:

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 e-mail 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** 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

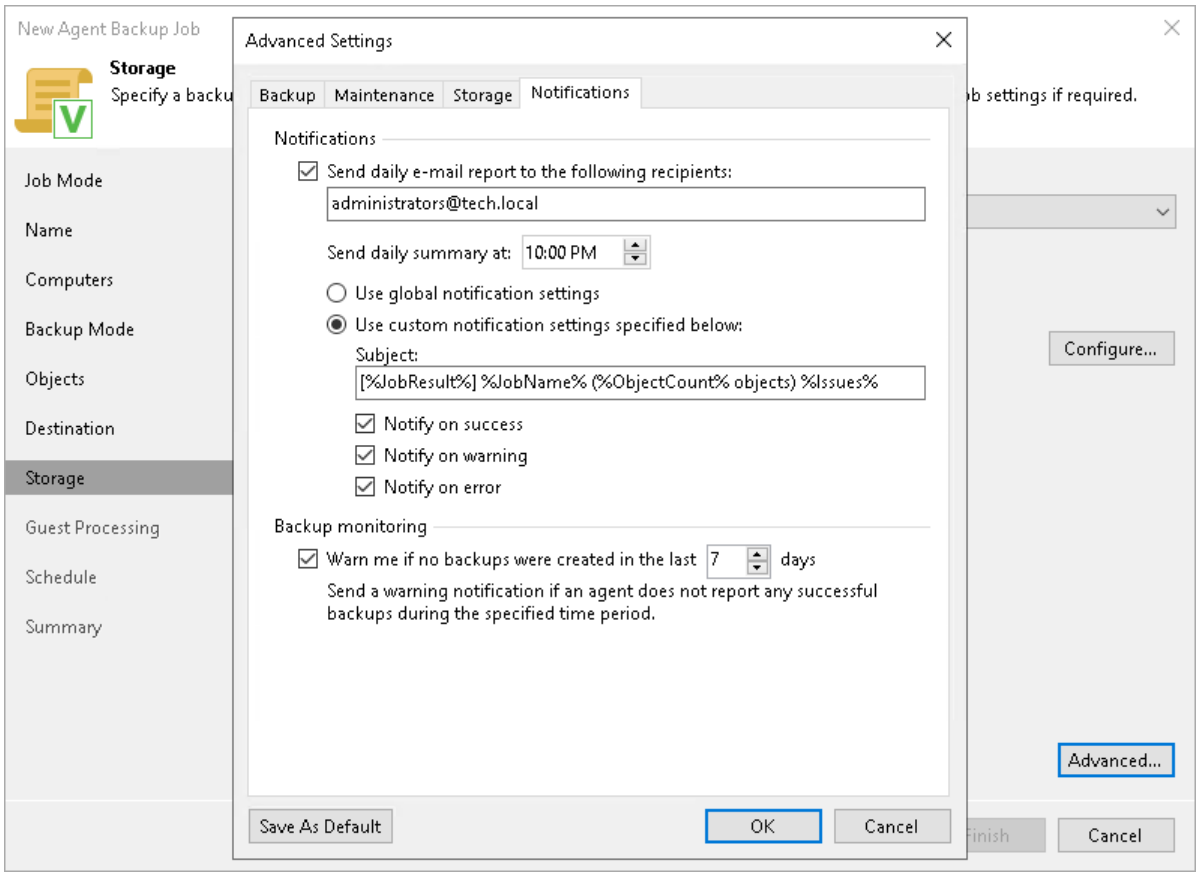
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup job sessions performed for 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 in 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 daily summary 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** or **Notify on error** check boxes to receive email notification if the job completes successfully, completes with a warning or fails.

6. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



Integration Settings

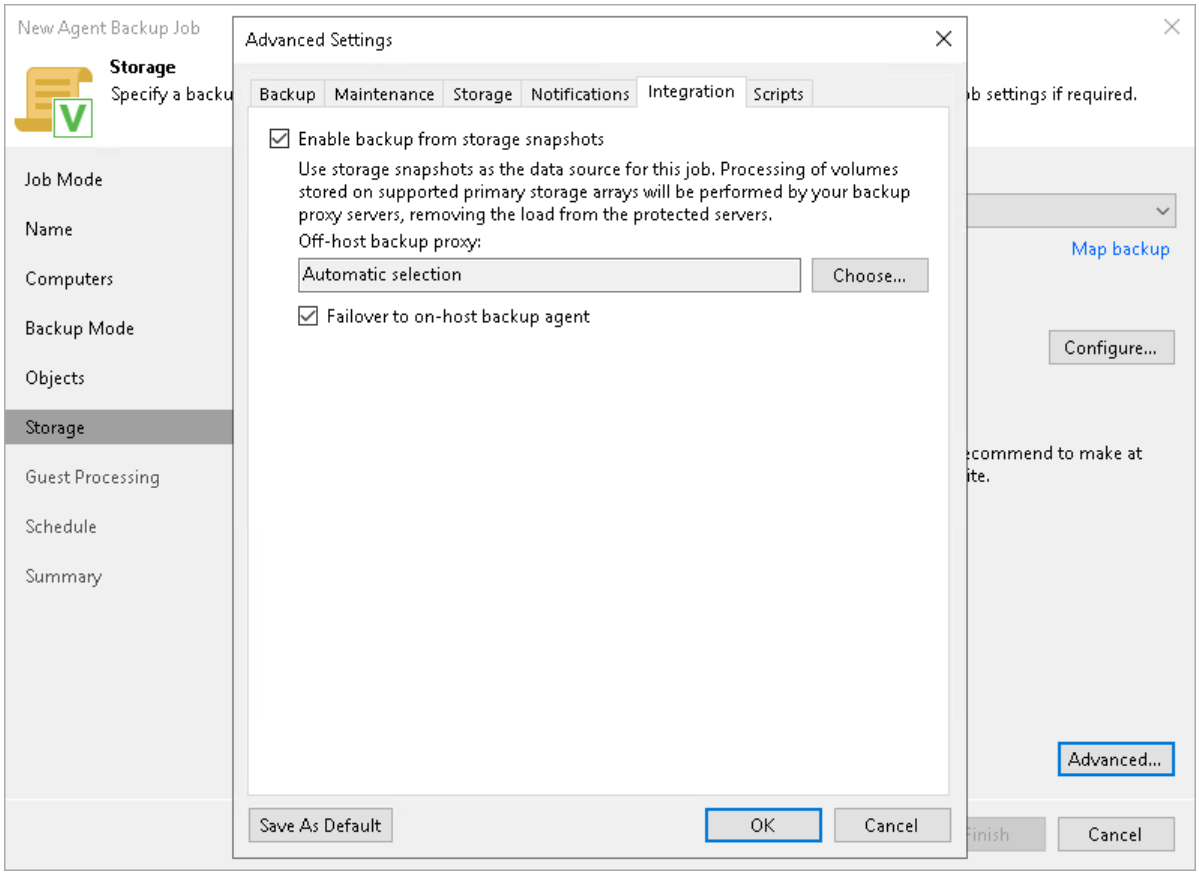
You can specify storage integration settings for the job if you have selected the **Managed by backup server** mode at the Job Mode step of the wizard.

Keep in mind that storage integration settings are unavailable if you work with protection group for cloud machines.

To specify storage integration settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Integration** tab.
3. If you select the **Enable backup from storage snapshots** check box, Veeam Backup & Replication will use native storage snapshots to create Veeam Agent backups. To learn more about storage snapshots support, see Storage Snapshots Support.
4. To transfer a snapshot from storage to the target repository, Veeam Backup & Replication uses off-host backup proxies. You can allow Veeam Backup & Replication to use any suitable backup proxies or you can select specific backup proxies. To learn more, see Selecting Off-Host Backup Proxy.
5. If Veeam Backup & Replication fails to create a storage snapshot or backup proxy is unavailable, you can fail over to the regular backup scenario that uses the software VSS provider. To do this, select the **Failover to on-host backup agent** check box.

   To learn more about regular backup scenario, see the How Backup Works section in the Veeam Agent for Microsoft Windows User Guide.



Selecting Off-Host Backup Proxy

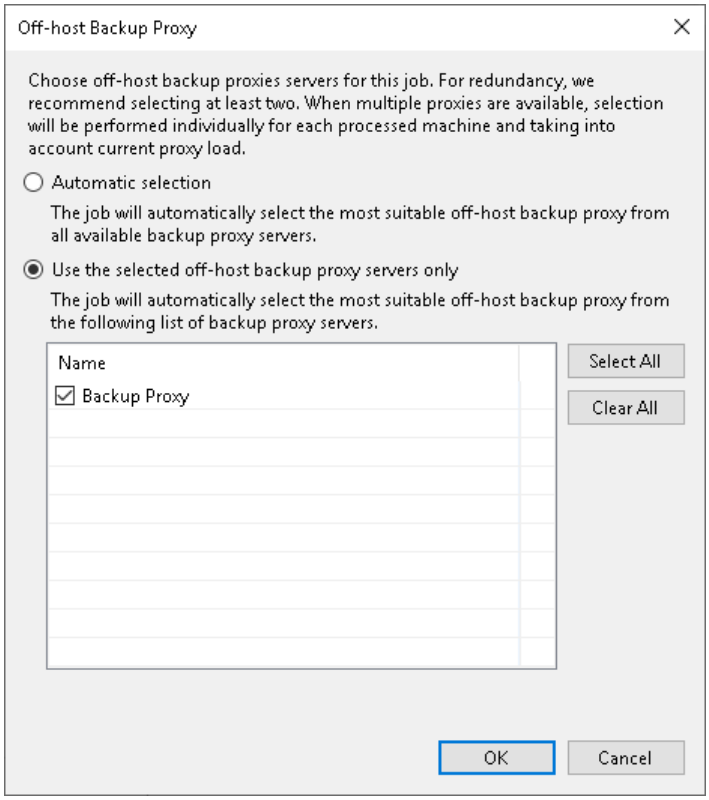
To specify what backup proxies Veeam Backup & Replication will use during the backup process, click **Choose** and select one of the following options in the **Off-host Backup Proxy** window:

- If you want Veeam Backup & Replication to use any suitable backup proxies, select the **Automatic selection** option. In this case, the number of backup proxies that Veeam Backup & Replication uses for data transfer depends on the backup scope.

  > **IMPORTANT**
  >
  > If you use the NetApp Element storage system and you have 4 or more backup proxies set in your Veeam Backup & Replication infrastructure, you cannot use automatic selection. You must manually select up to 3 backup proxies.

- If you want to select backup proxies manually, select the **Use the selected off-host backup proxy servers only** option and select check boxes near backup proxies you plan to use.

Keep in mind that Veeam Backup & Replication displays only those backup proxies that run Microsoft Windows Server OS. For more information about backup proxy requirements, see Storage Snapshots Support.



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.

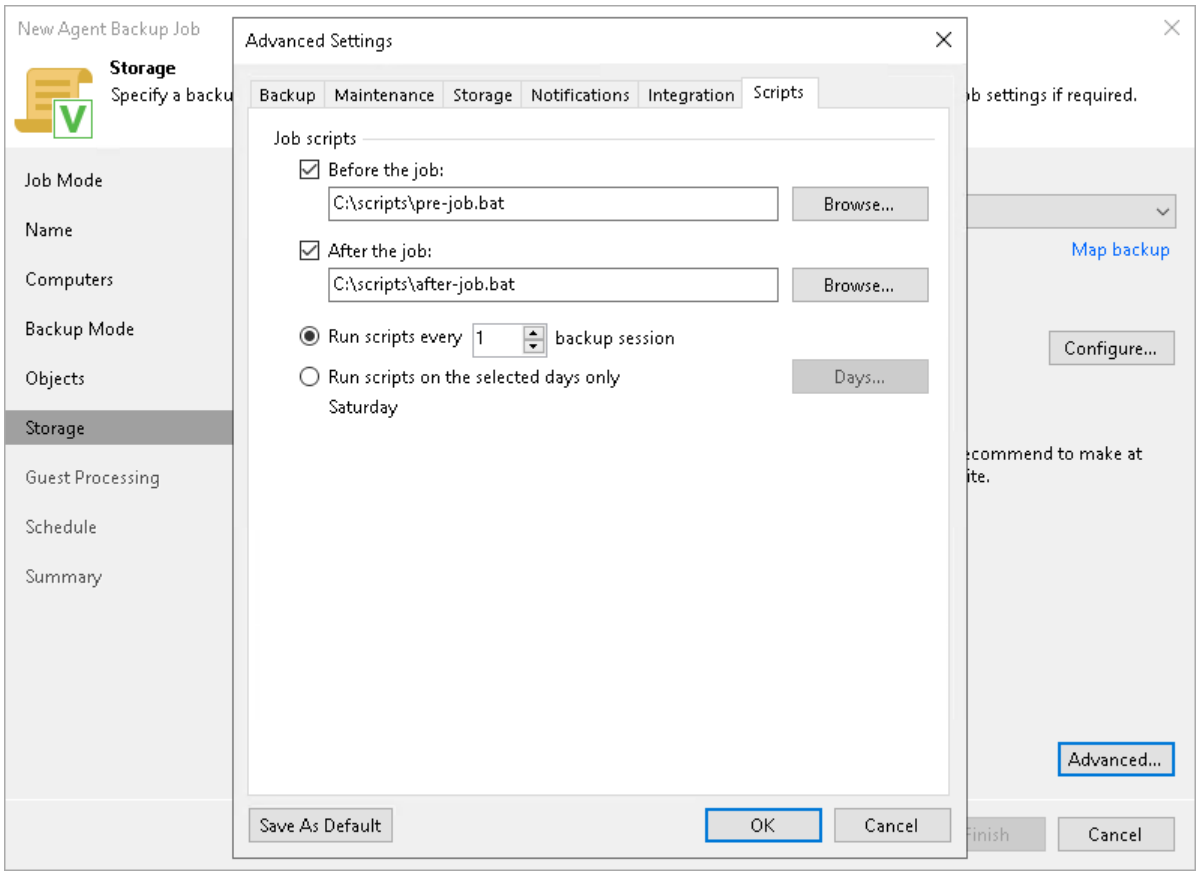
To specify script settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Scripts** tab.
3. If you want to execute custom scripts before or after the backup job, select the **Before the job** or **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

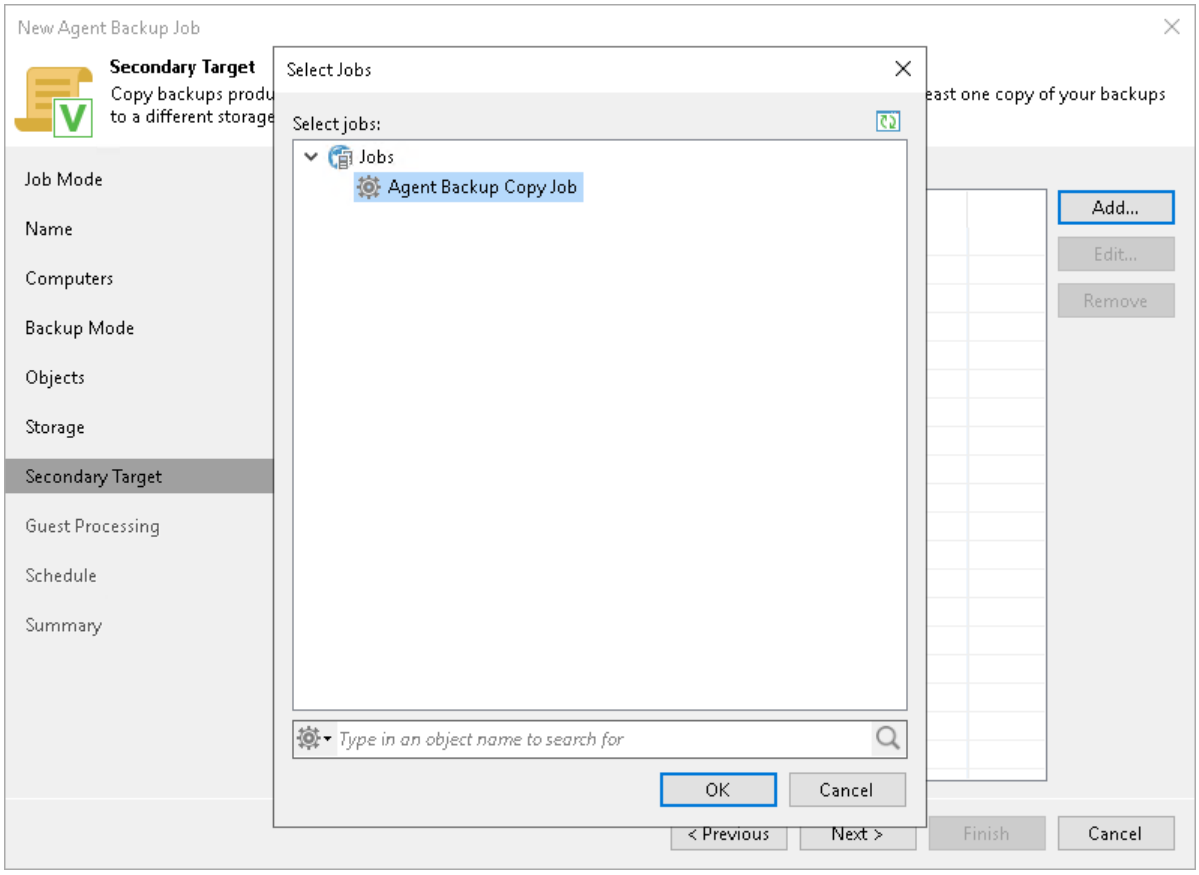
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

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:

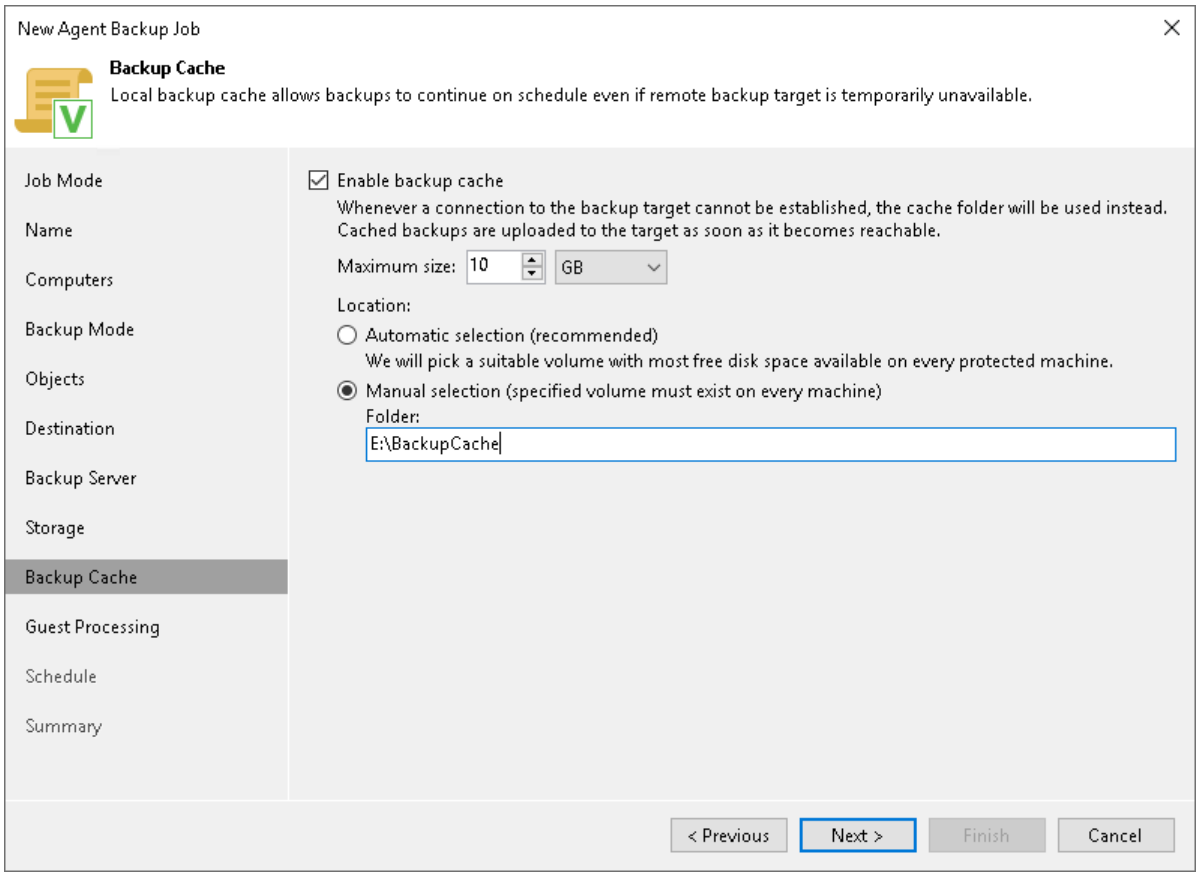
1. Select the **Enable backup cache** check box.
2. In the **Maximum size** field, specify the size for the backup cache.

   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.

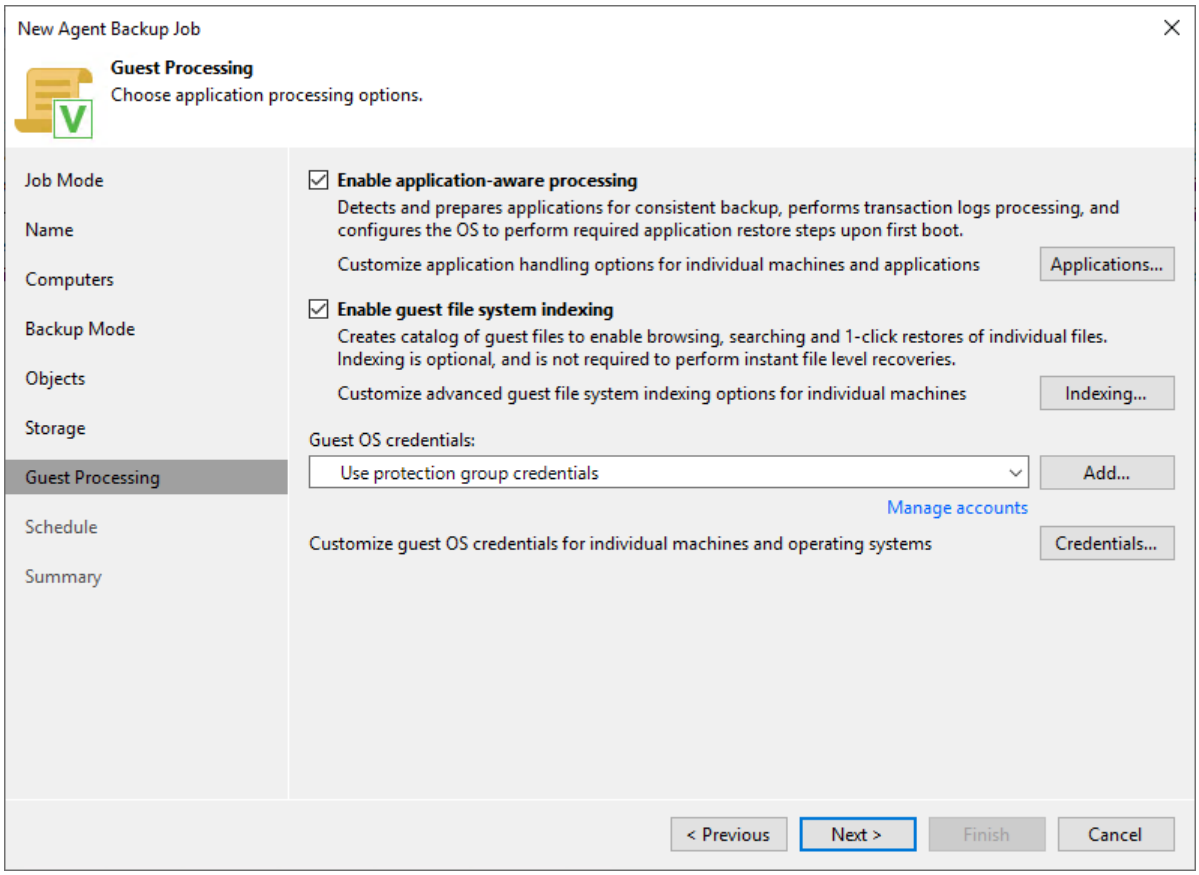


Step 12. Specify Guest Processing Settings

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



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.

   [For Microsoft SQL Server] If you disable application-aware processing, Veeam Agent will not include information about databases in the backup. However, you can use Veeam Explorer for Microsoft SQL to locate a database file in the backup and restore the database.
5. [For Microsoft Exchange, Microsoft SQL Server and other applications that rely on VSS] In the **Microsoft VSS settings** 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.

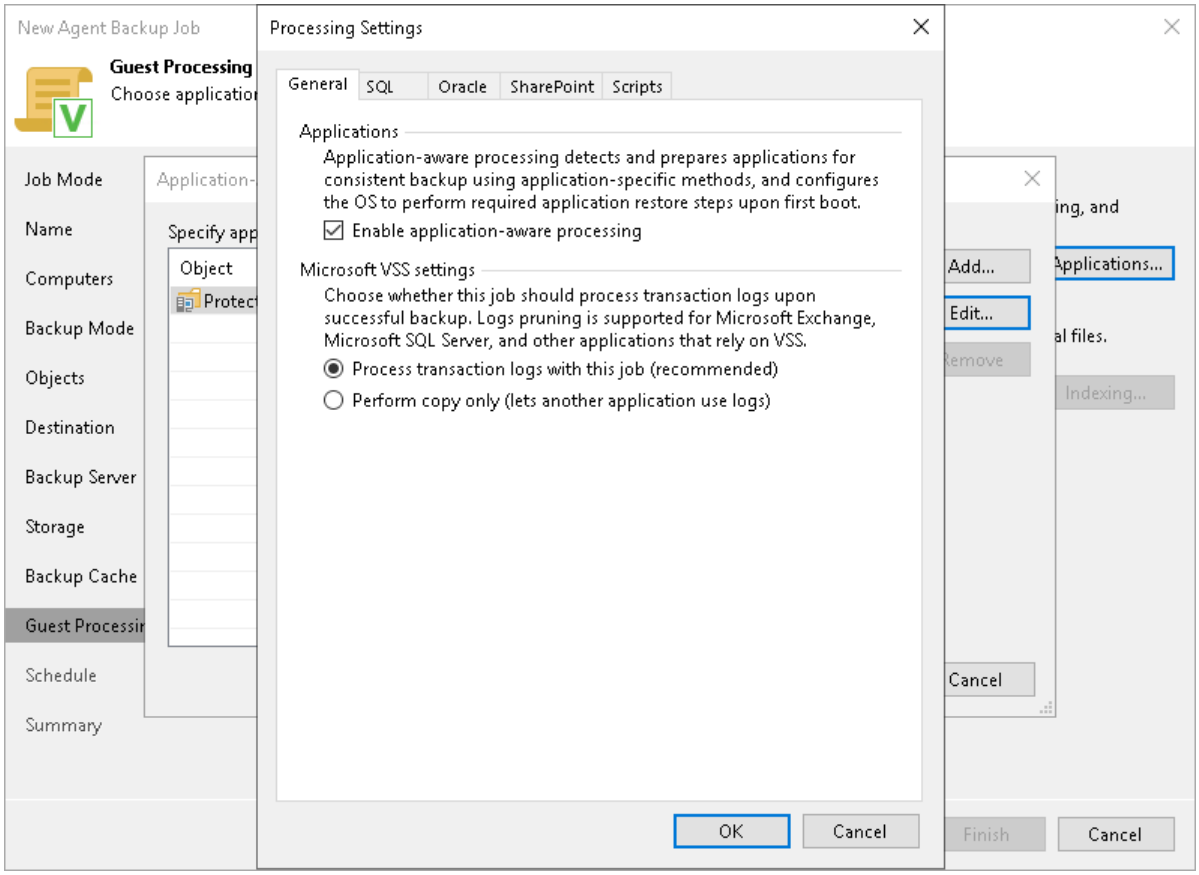
     [For Microsoft Exchange] With this option selected, Veeam Agent for Microsoft Windows will wait for backup to complete successfully, and then trigger truncation of transaction logs. If the backup job fails, the logs will remain untouched until the next backup job session.

     [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. After a copy-only backup, Veeam Agent does not trigger truncation of transaction logs. For more information, see this Microsoft article.

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 **Microsoft VSS settings** 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 will use to connect to the Microsoft SQL Server, select from the **Specify Windows account with sysadmin role on SQL Server** list a user account that has access permissions on the database. This account must be a Microsoft Windows user account with roles and permissions as specified in the Performing Guest Processing section of the Veeam Backup & Replication User Guide. Keep in mind that 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 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:
   - Select **Truncate logs** to truncate transaction logs after successful backup. Veeam Agent 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.
   - Select **Do not truncate logs** to preserve transaction logs. When the backup job completes, Veeam Agent 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.
   - Select **Backup logs periodically** to back up transaction logs with Veeam Agent. Veeam Agent 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 User Guide.

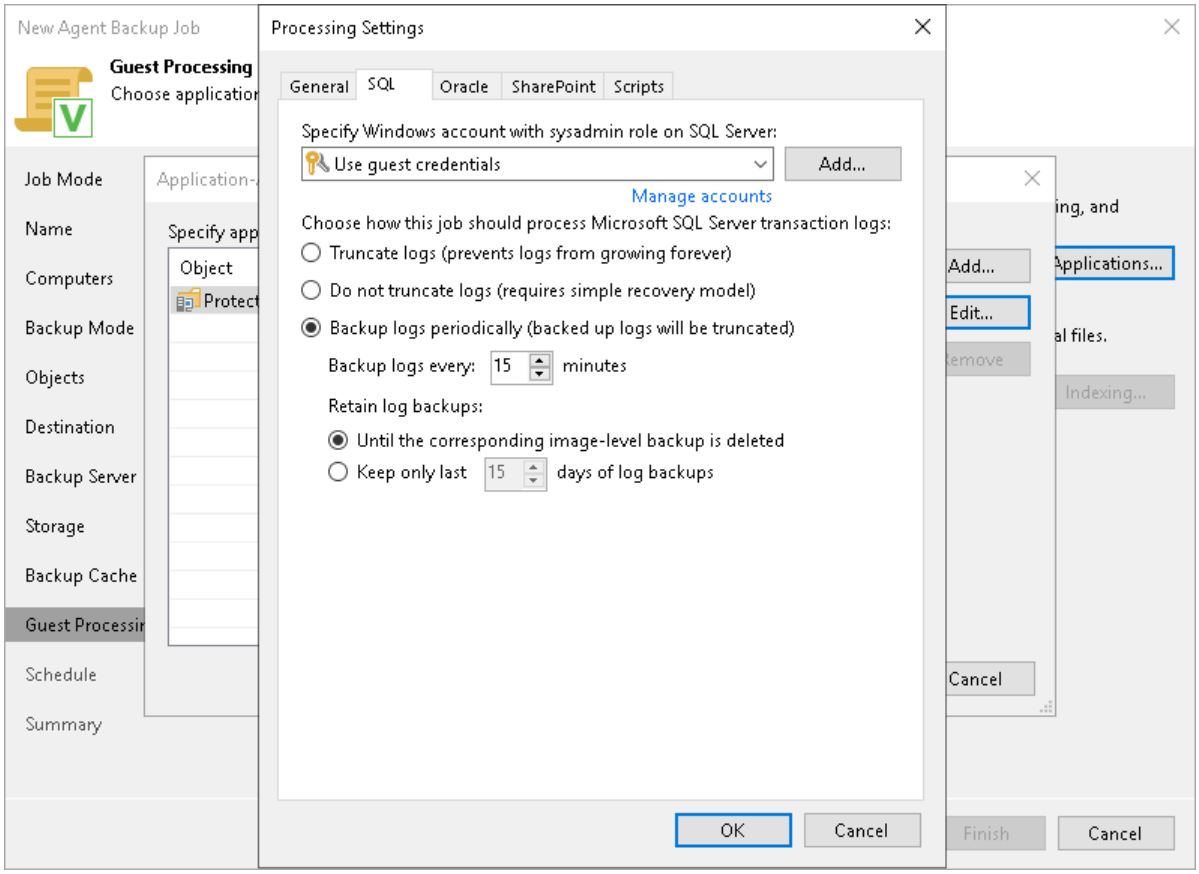
If you have selected to back up transaction logs with Veeam Agent for Microsoft Windows, you must specify settings for transaction logs backup:

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

- Select **Keep only last <N> days of log backups** to keep transaction logs for a specific number of days. By default, transaction logs are kept for 15 days. If you select this option, you must make sure that retention for transaction logs is not greater than retention for the image-level 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

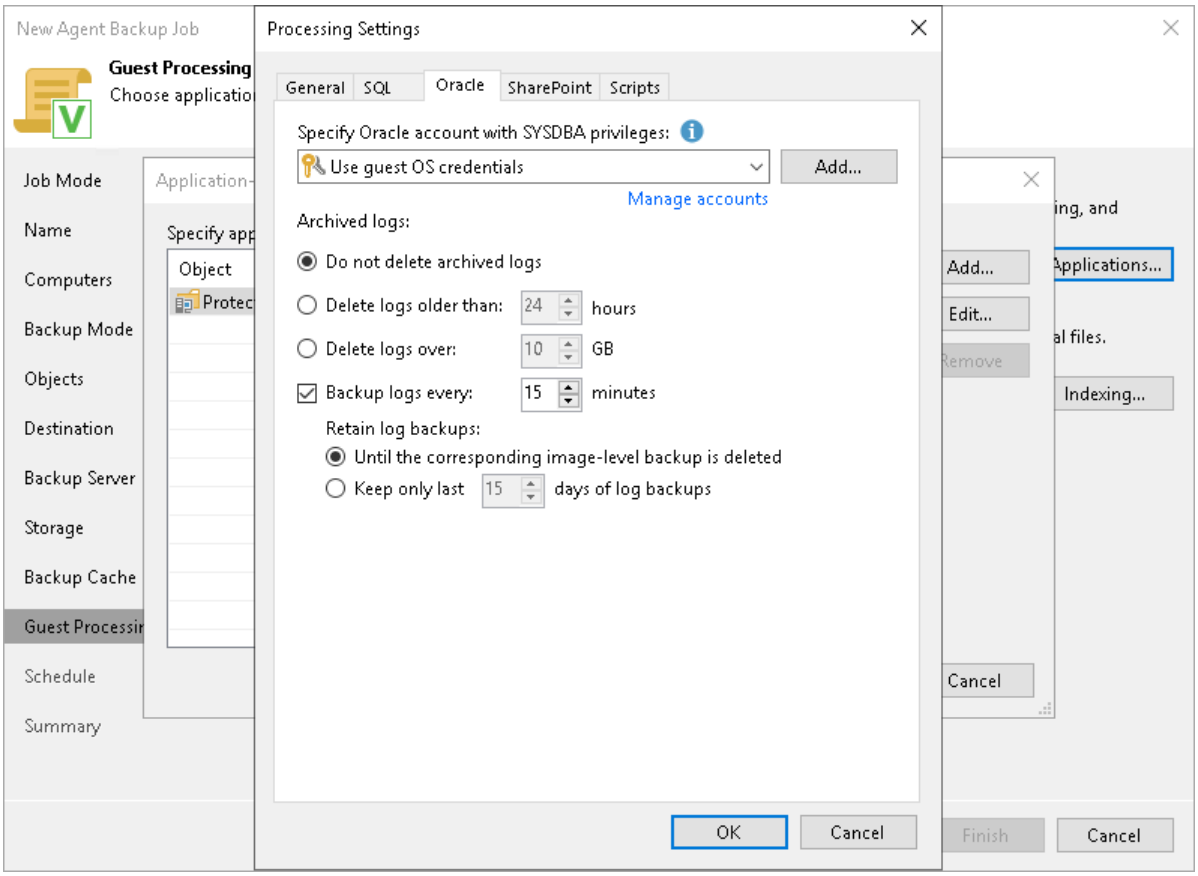
If you back up an Oracle database, you can specify how Veeam Agent for Microsoft Windows must process archived logs:

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 **Microsoft VSS settings** 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:
   - 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.
   - 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 logs 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.

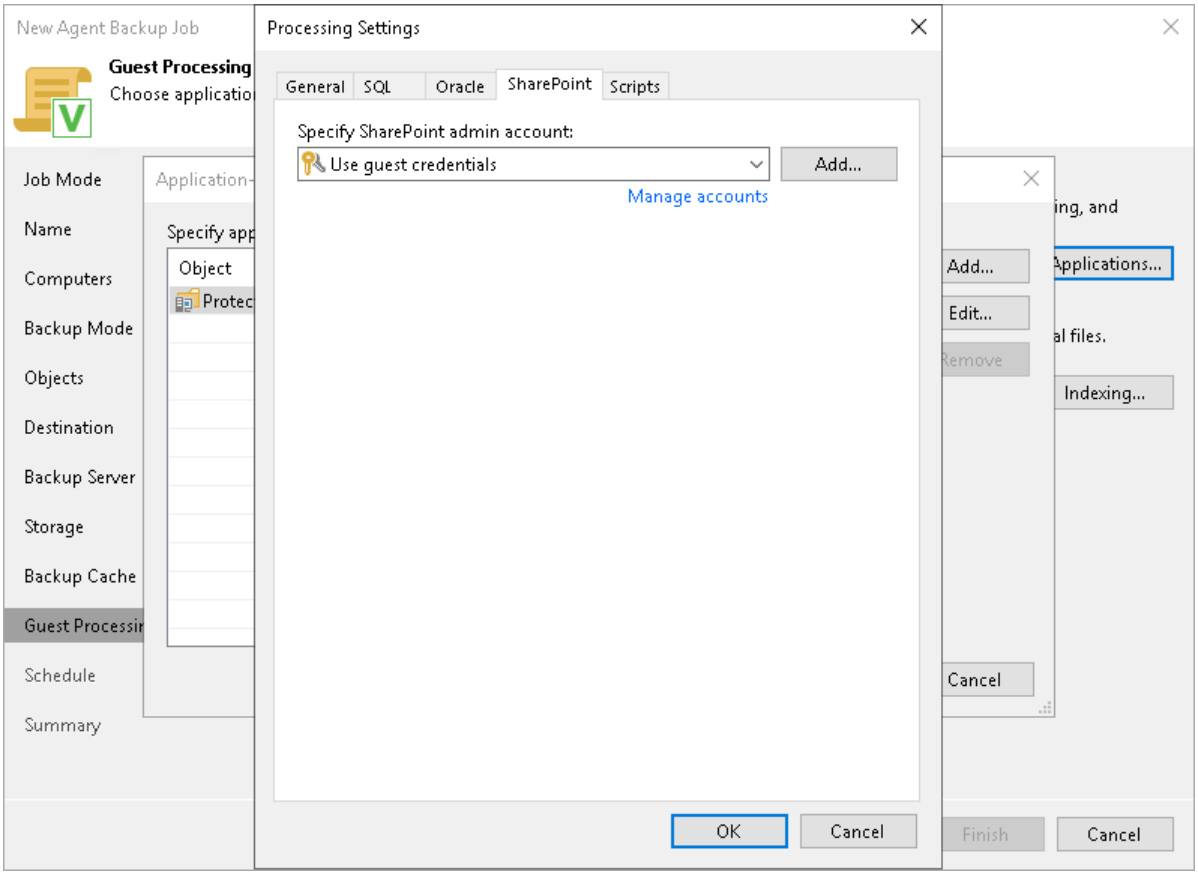


Microsoft SharePoint Account Settings

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.

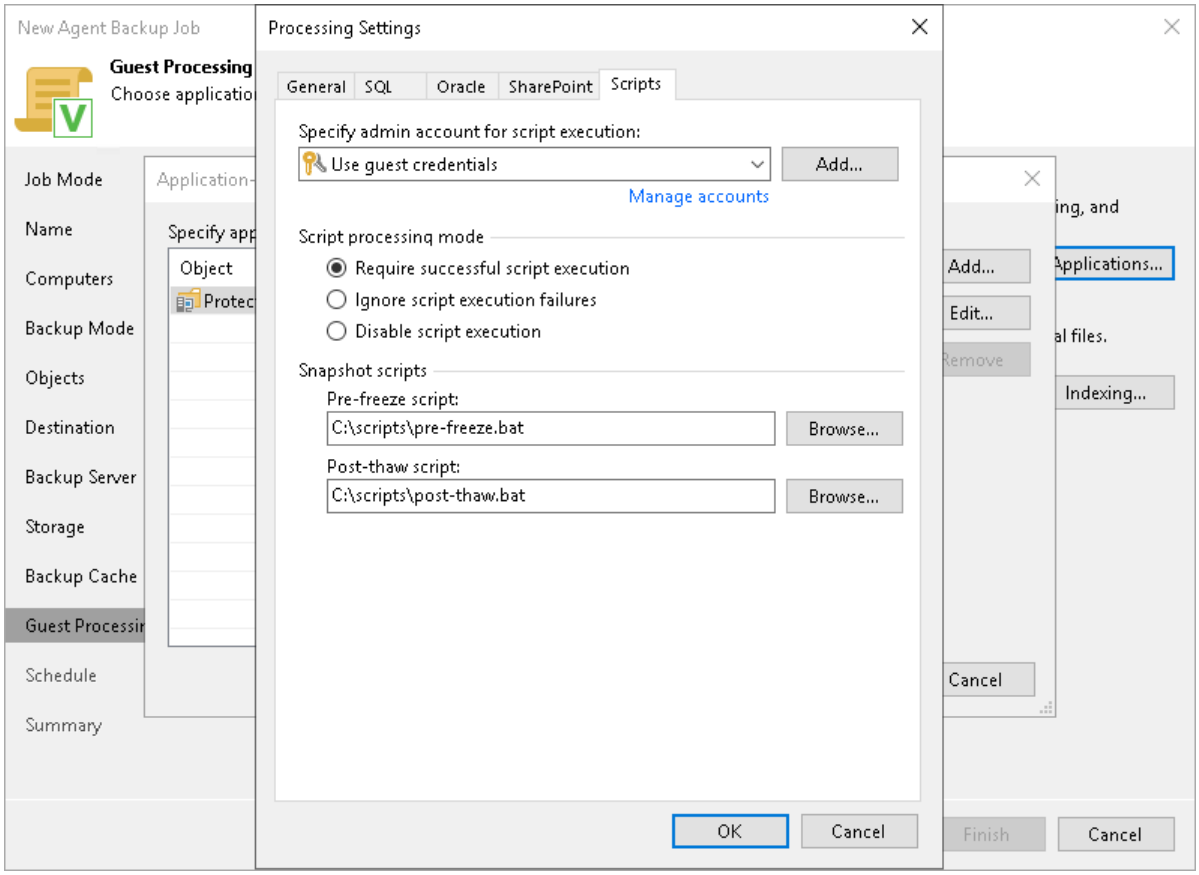
   By default, the **Use guest credentials** option is selected in the list. With this option selected, Veeam Agent for Microsoft Windows will run pre-freeze and post-thaw scripts under the account that you have specified for the protected computer in the protection group settings.
6. In the **Script processing 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 **Snapshot scripts** section, 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 the following types of scripts:

   - Program files in the EXE, BAT and CMD format
   - Windows script files in the JS, VBS and WSF format
   - PowerShell script files in the PS1 format

   You can use scripts of other formats as well, but we cannot guarantee correct processing of such scripts.



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.

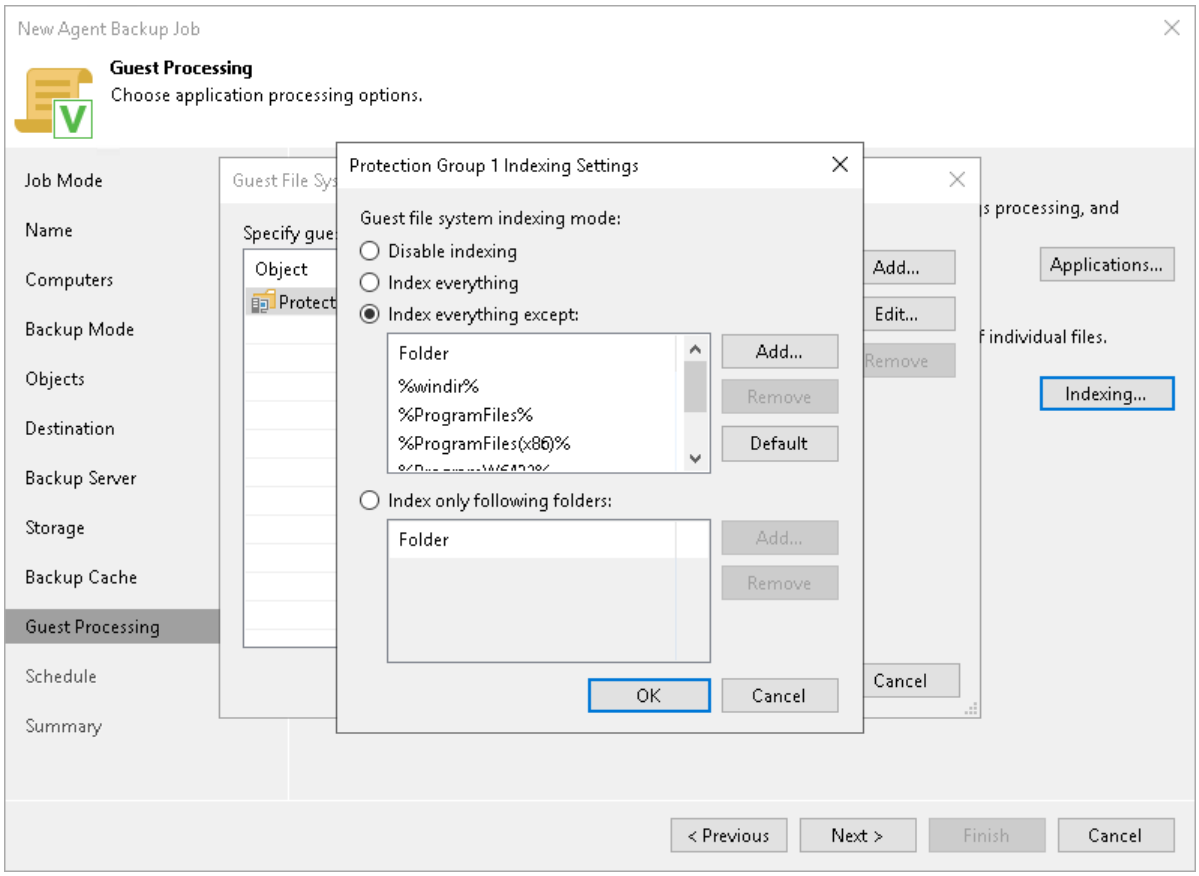
> **NOTE**
>
> File system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the backup created with such backup job. For more information, see the Preparing for File Browsing and Restore section in the Veeam Backup 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%*.



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.

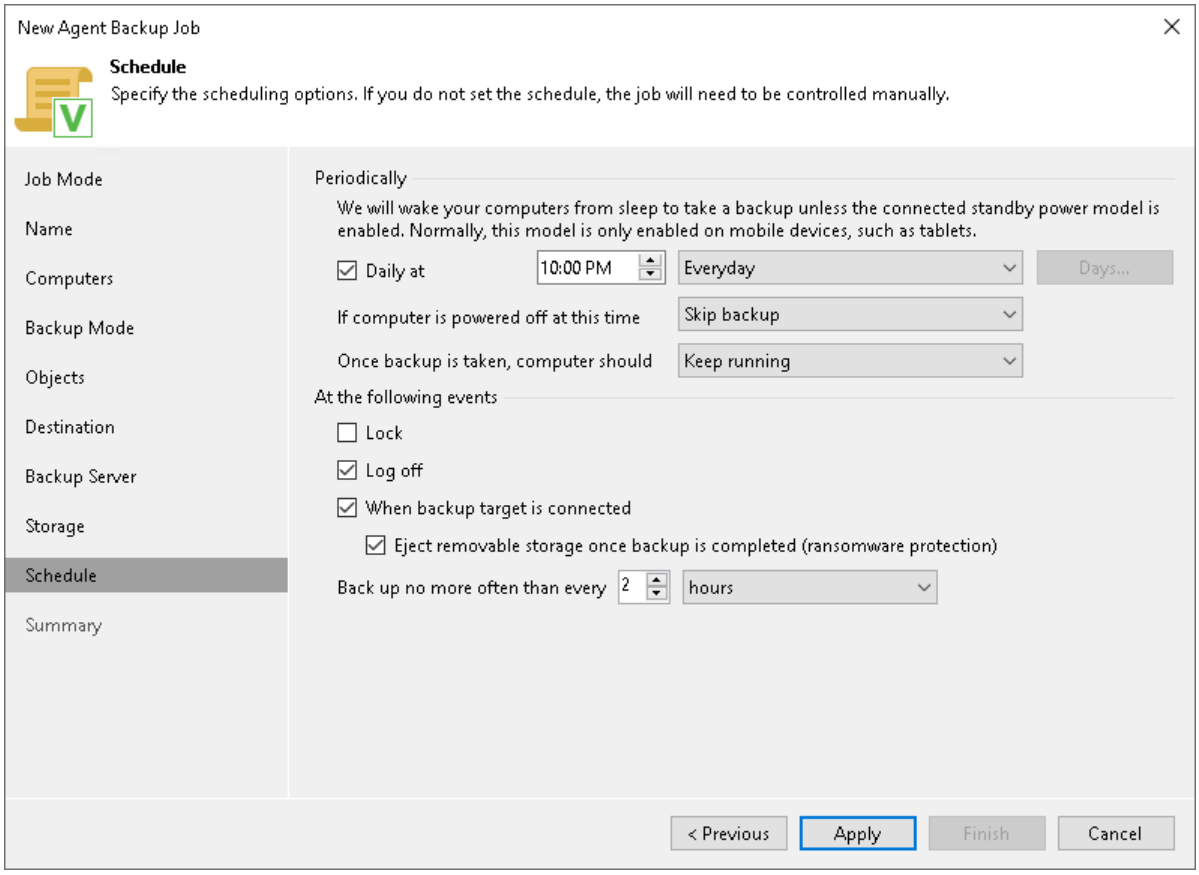
  Veeam Agent applies this setting only to backup jobs triggered by the *When backup target is connected* event. In case of backup jobs triggered by other computer events or started periodically at specific time, Veeam Agent will ignore this setting, and the storage device will not be unmounted after the backup job completes successfully.

  > **IMPORTANT**
  >
  > The *Eject removable storage once backup is completed* option does not guarantee a bulletproof protection against ransomware. To ensure your backups are safe, keep the OS up to date and regularly scan your backup repository for virus threats using modern antivirus software.

- 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 Failover 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 retries the job for the defined number of times without any time intervals between the job runs.

   [For Managed by agent mode only] If a backup policy fails and Veeam Agent retries the session, Veeam Agent does not transfer all the data again. Instead, Veeam Agent continues data transfer that was started before the backup policy fail. To do so, Veeam Agent compares hash values for data blocks on source and target. After the hash comparison, Veeam Agent also transfers only those data blocks that were not transferred before the policy fail. If data blocks on source were changed before the retry, Veeam Agent transfers these data blocks as well.

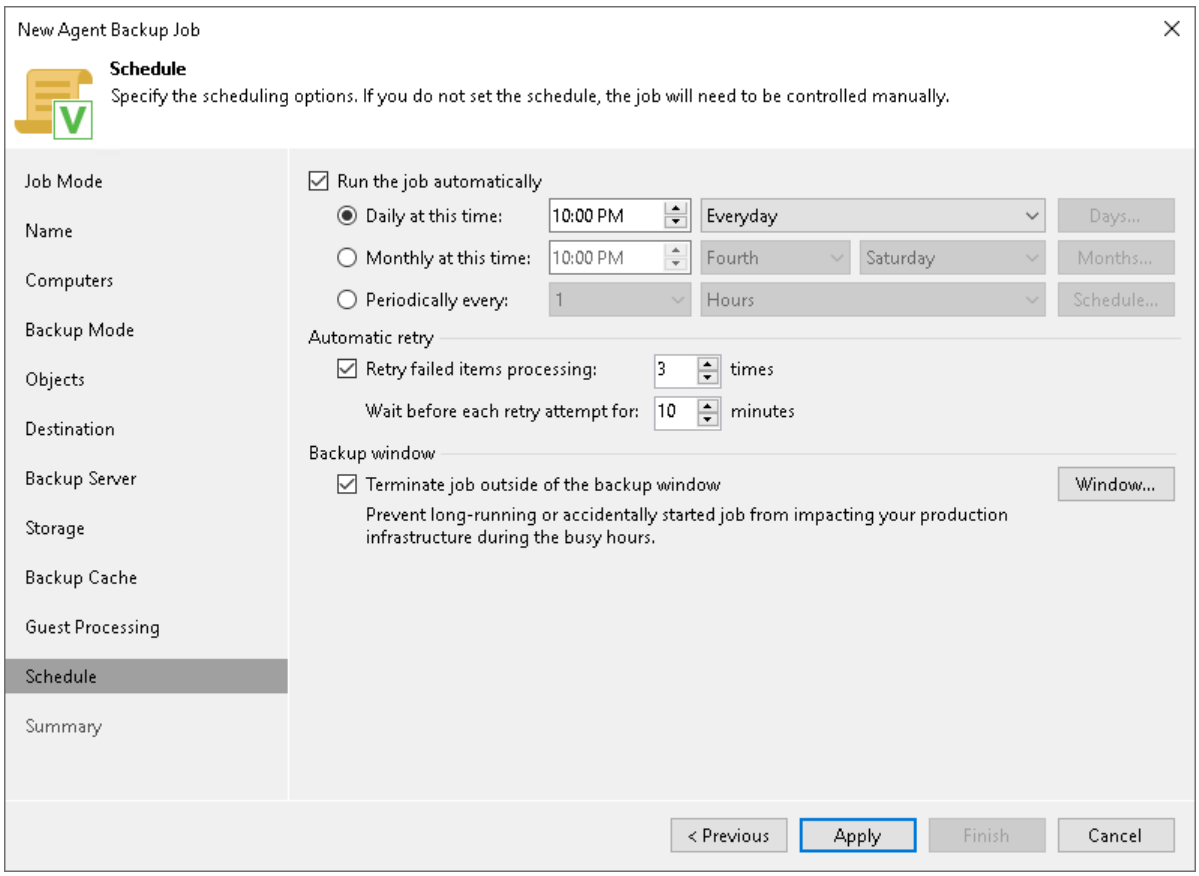
4. In the **Backup window** section, define the time interval within which the backup job must complete. The backup window prevents the job from overlapping with production hours and ensures that the job does not impact performance of your server. To set up a backup window for the job:

   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. In this case, data transport and backup chain transformation processes are stopped. Keep in mind that this behavior differs from a VM backup job where backup window affects data transport process and health check operations only.

> **IMPORTANT**
>
> [For backup policy] The backup window does not affect the process of uploading backup files from the backup cache to the target storage. If Veeam Agent creates one or more backup files in the backup cache, and then the backup target becomes available, Veeam Agent uploads backup files to the target location immediately, regardless of the specified backup window.



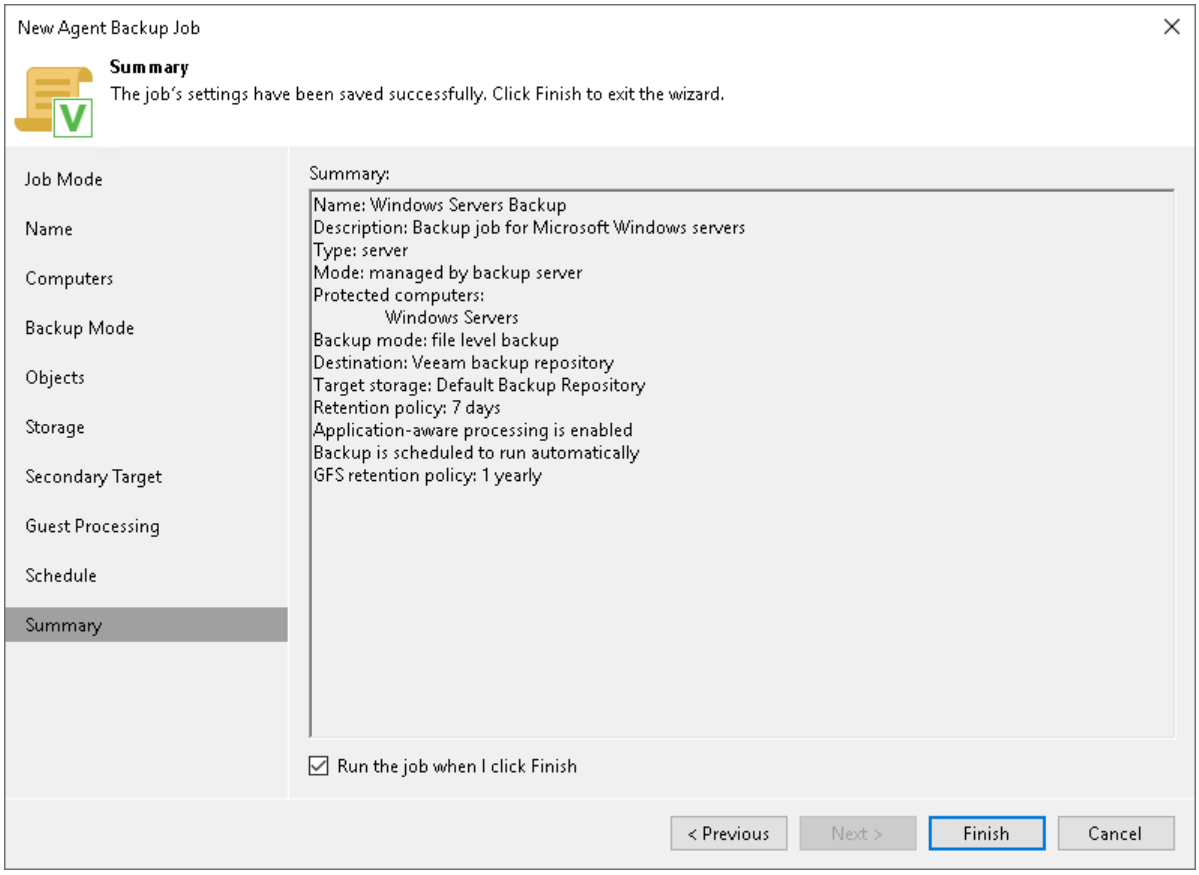
Step 14. Review Backup Job Settings

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.

[For backup job managed by Veeam Agent] Keep in mind that Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Microsoft Windows Configuration.



Creating 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 in a Veeam backup repository and Veeam Cloud Connect repository. If you want to save backups in other target locations, you must configure a Veeam Agent backup job managed by Veeam Agent (backup policy). To learn more, see Veeam Agent Backup Jobs and Policies.
- [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 in 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 in 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.
- If you plan to create a Veeam Agent backup job for computers with Veeam Agents installed using the `veeam-nosnap` package, consider the limitations and system requirements in the Appendix A. Requirements for veeam-nosnap section of the Veeam Agent for Linux User Guide.

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.

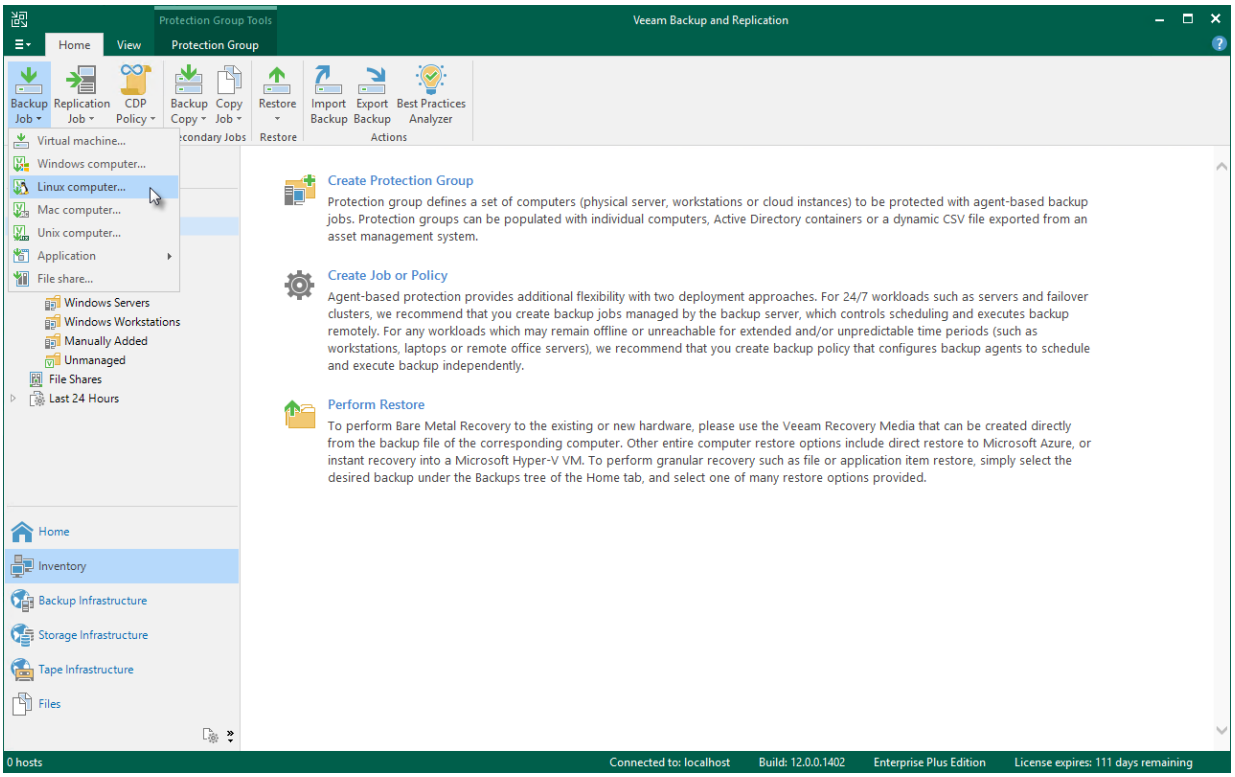
Adding Computers to New Backup Job

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 the Product Editions section in the 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

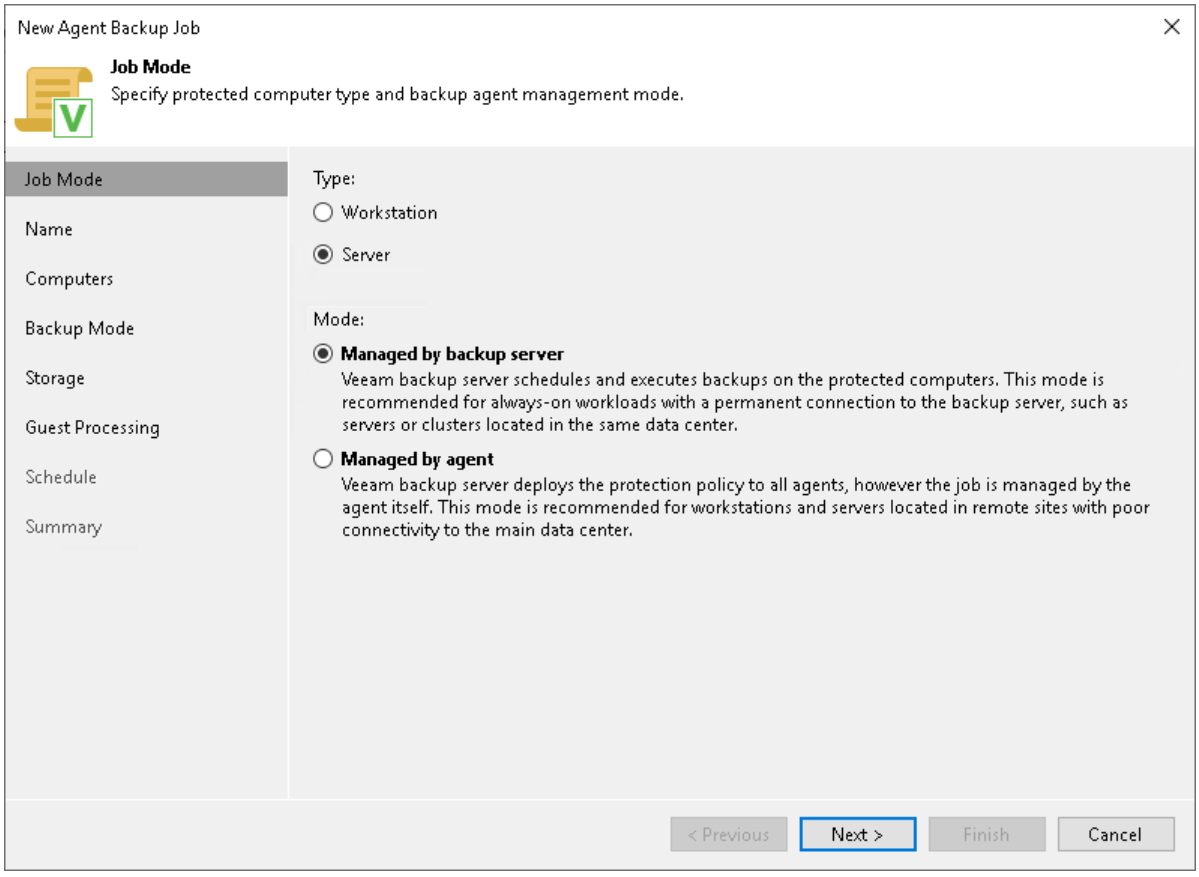
If you selected the **Servers** computer type in the Type field, in the **Mode** field, select the job mode. You can select one of the following modes:

- **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.

  > **NOTE**
  >
  > You must select the **Managed by backup server** option if you want to use the backup job to protect cloud machines. To learn more, see Select Protection Group Type.

- **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.

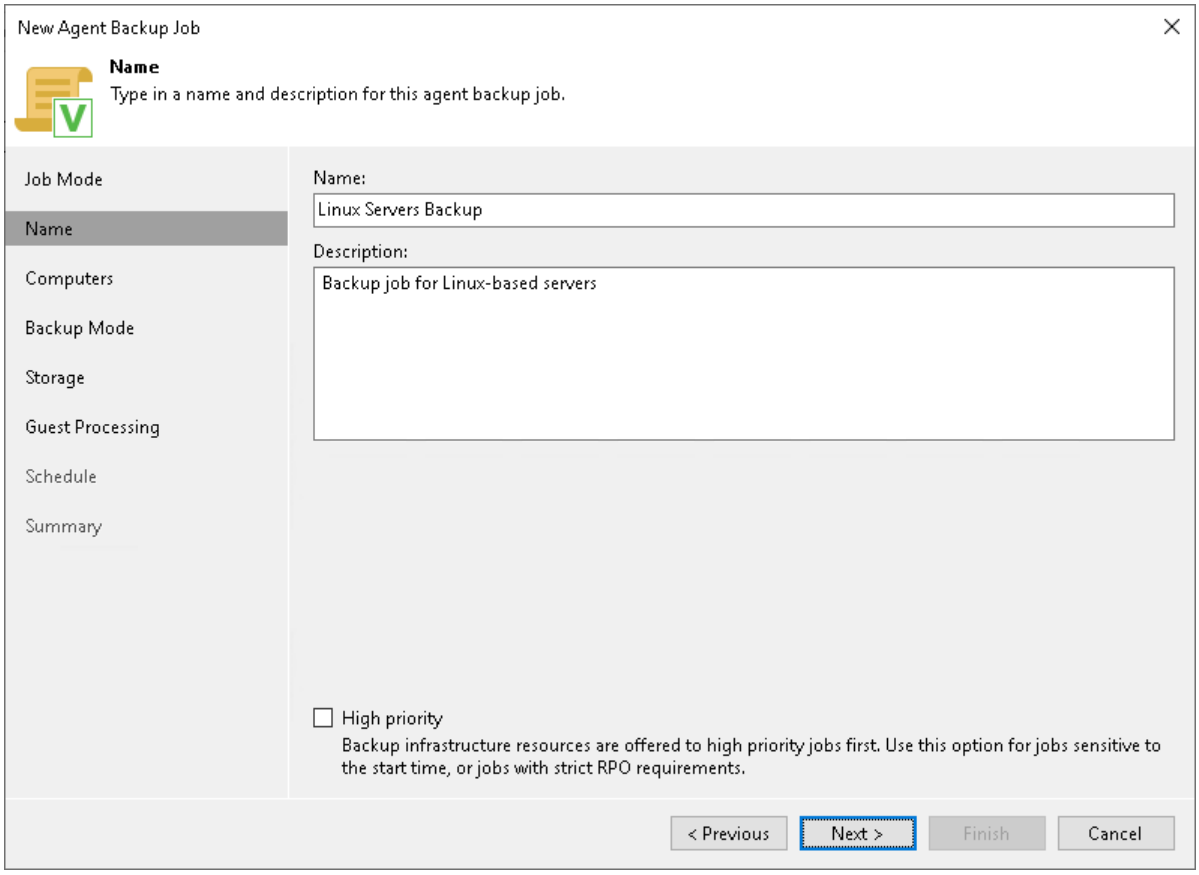
  > **NOTE**
  >
  > You must select the **Managed by agent** option if you want to use the backup job to protect computers included in protection groups for pre-installed Veeam Agents. To learn more, see Select Protection Group Type.



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.
3. [For backup job managed by backup server] Select the **High priority** check box if you want the resource scheduler of Veeam Backup & Replication to prioritize this job higher than other similar jobs and to allocate resources to it in the first place. To learn more, see the Job Priorities section in the Veeam Backup & Replication User Guide.



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.
- Veeam Backup & Replication displays protection groups for pre-installed Veeam Agents and their members only if you selected the **Managed by Agent** option at the **Job Mode** step of the wizard. You cannot add protection groups for pre-installed Veeam Agents to backup jobs managed by backup server. To learn more, see Selecting Job Mode.

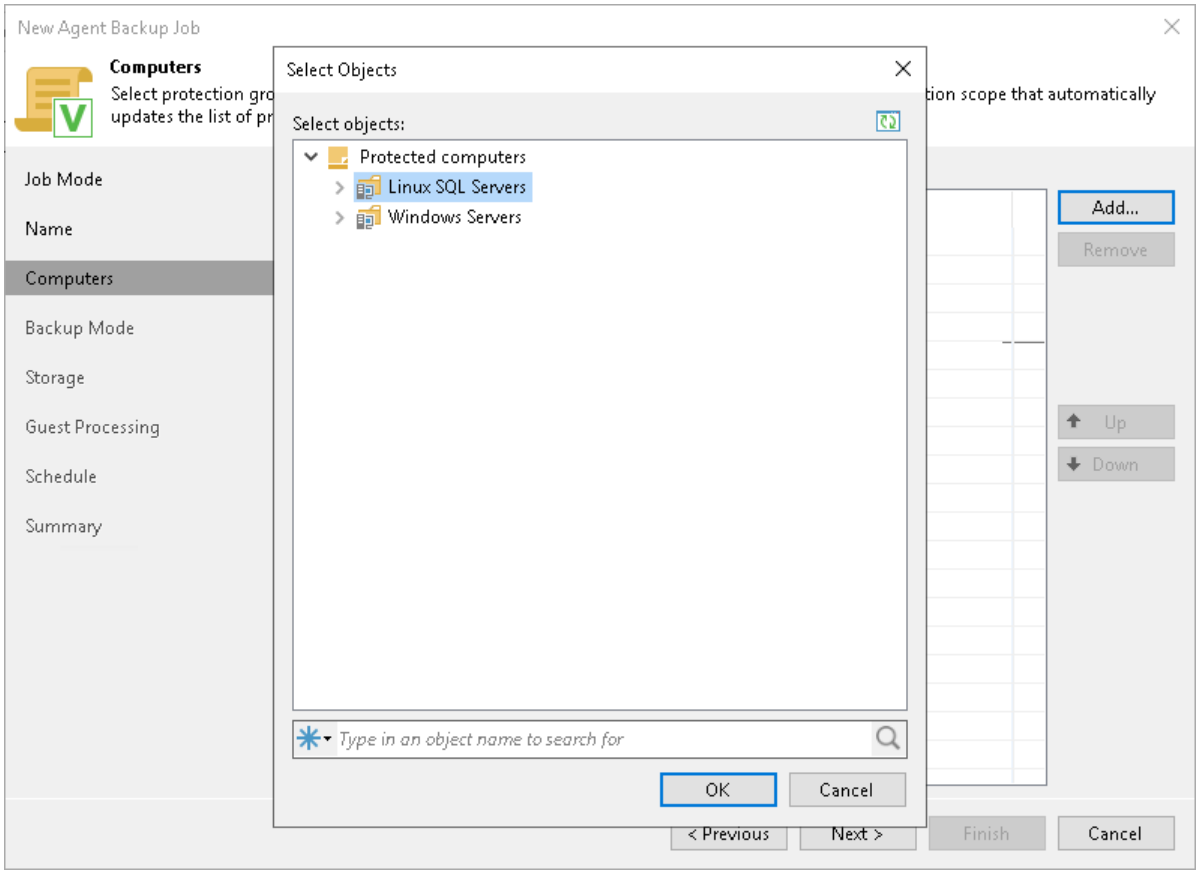
Adding Protection Groups and Computers from Inventory

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.

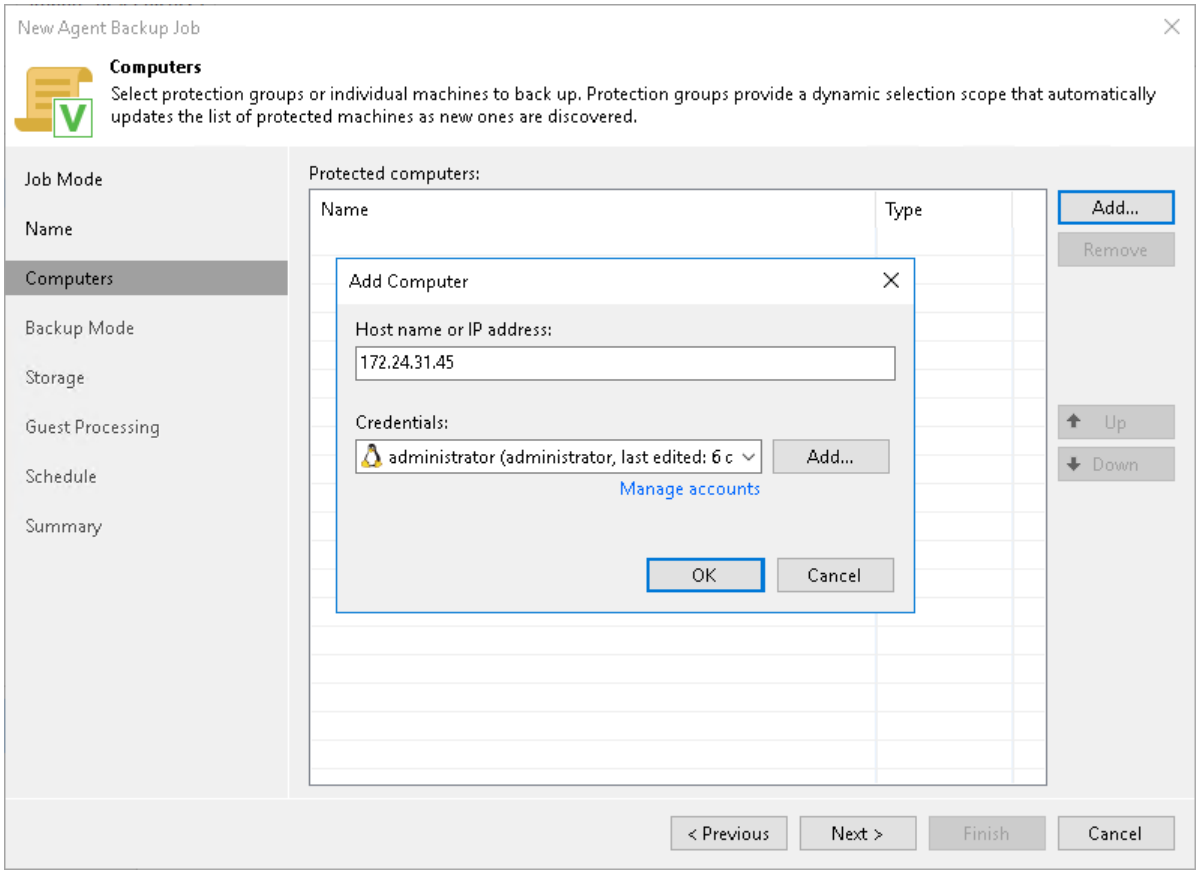
1. Enter the object name or a part of it in the search field.
2. Click the **Start search** button on the right or press **[ENTER]**.



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.



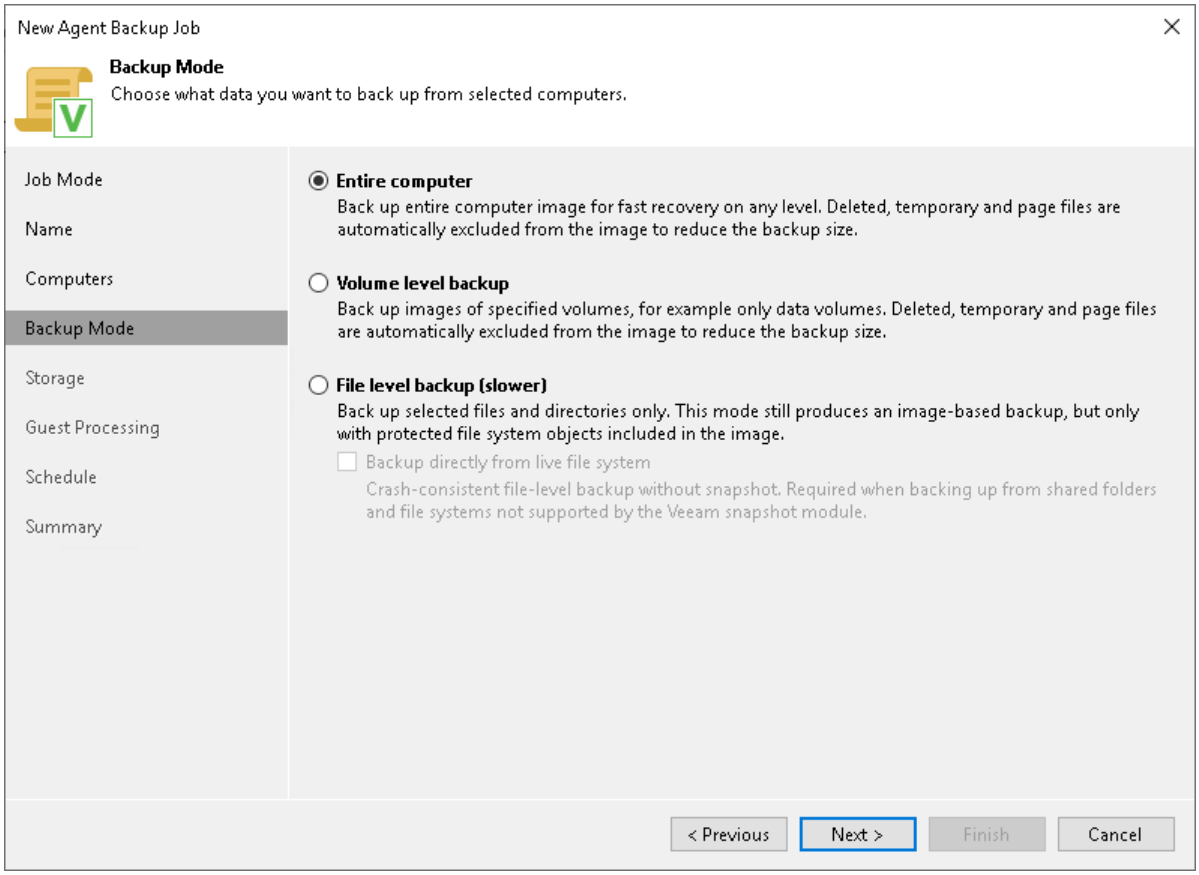
Step 5. Select Backup Mode

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 of the wizard:
     - 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.

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.



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**.

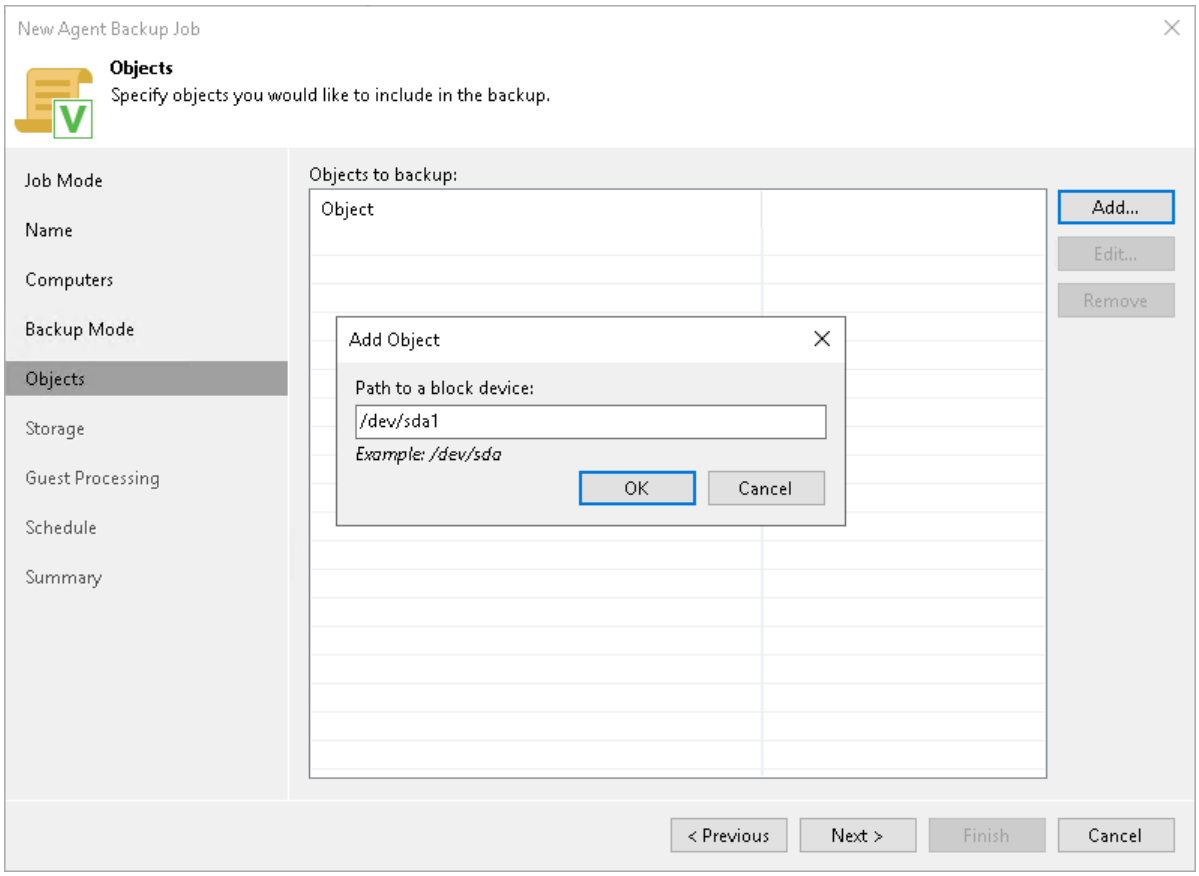
   You can specify the following objects to back up:

   - *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*.

     > **NOTE**
     >
     > If you include a block device in the backup, and this block device is a physical volume assigned to an LVM volume group, Veeam Agent will include the whole LVM volume group in the backup.

   - *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.
   - *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*.
   - *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

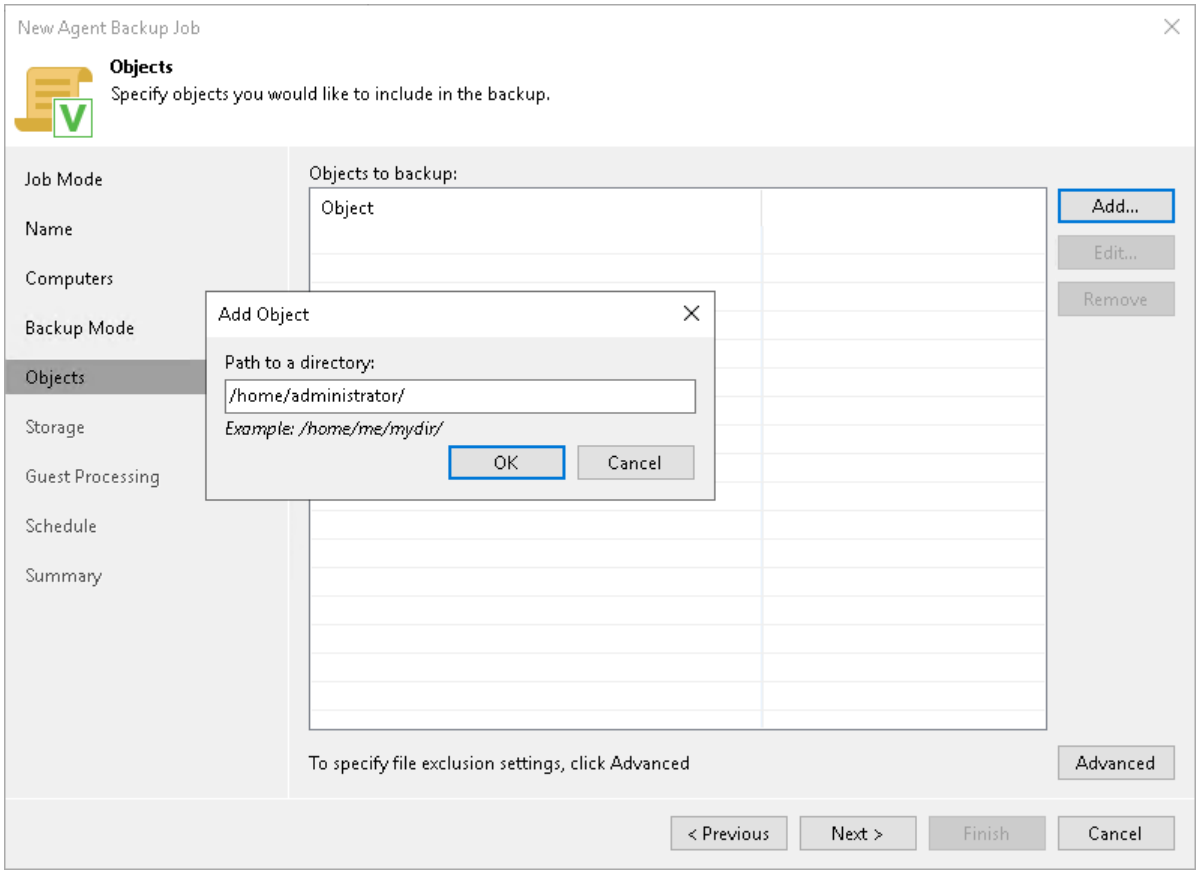
The **Objects** step of the wizard is available if you have chosen to create a file-level backup.

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.

> **TIP**
>
> If you want to back up the root directory and specify `/` in the **Path to a directory** field, Veeam Agent does not automatically include remote mount points in the backup scope. To include remote mount points, you need to specify paths to these mount points manually.
>
> For example, you have a file system mounted to the `/home/media` directory. If you add `/` as an object to the backup scope, Veeam Agent will not back up the mounted file system. To back up the root directory and the mounted file system, add the following objects to the backup scope:
>
> - `/`
> - `/home/media`



Configuring Filters

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

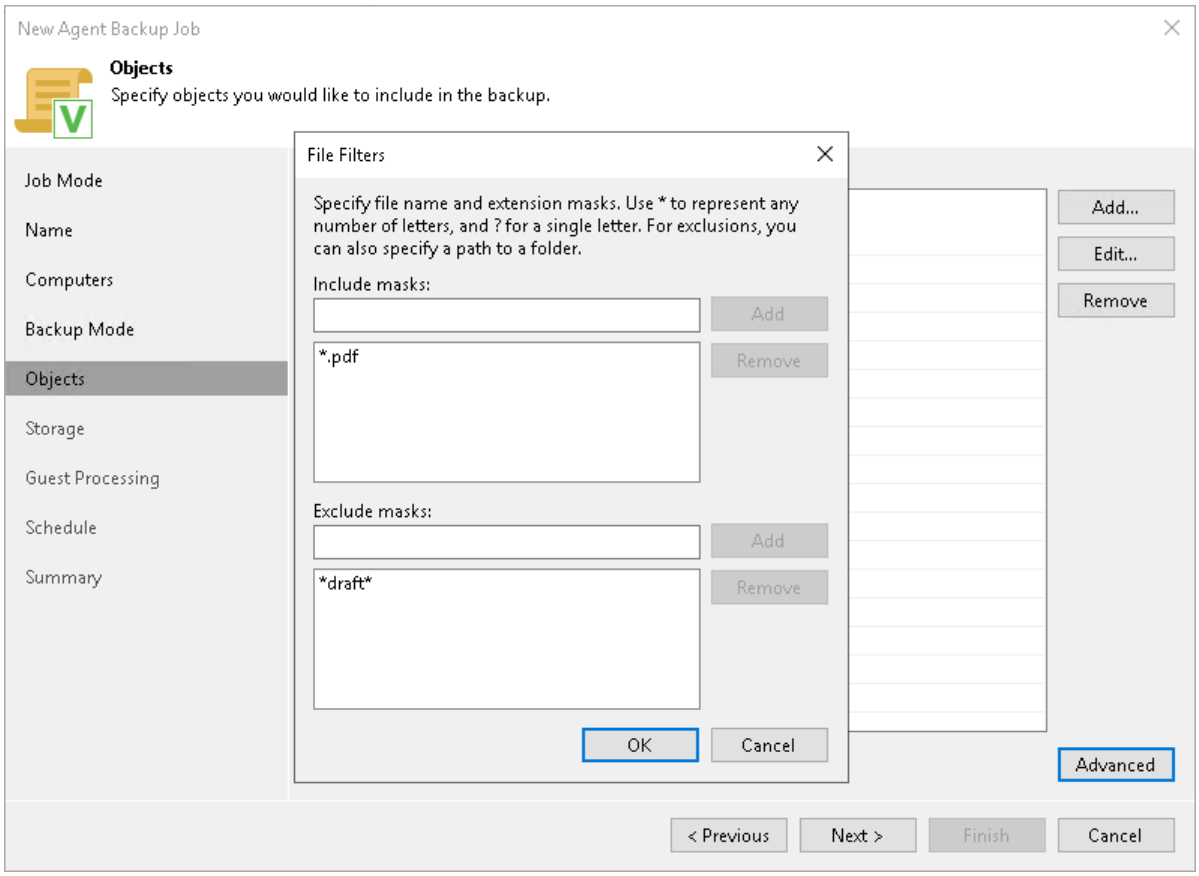
To configure a filter:

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.

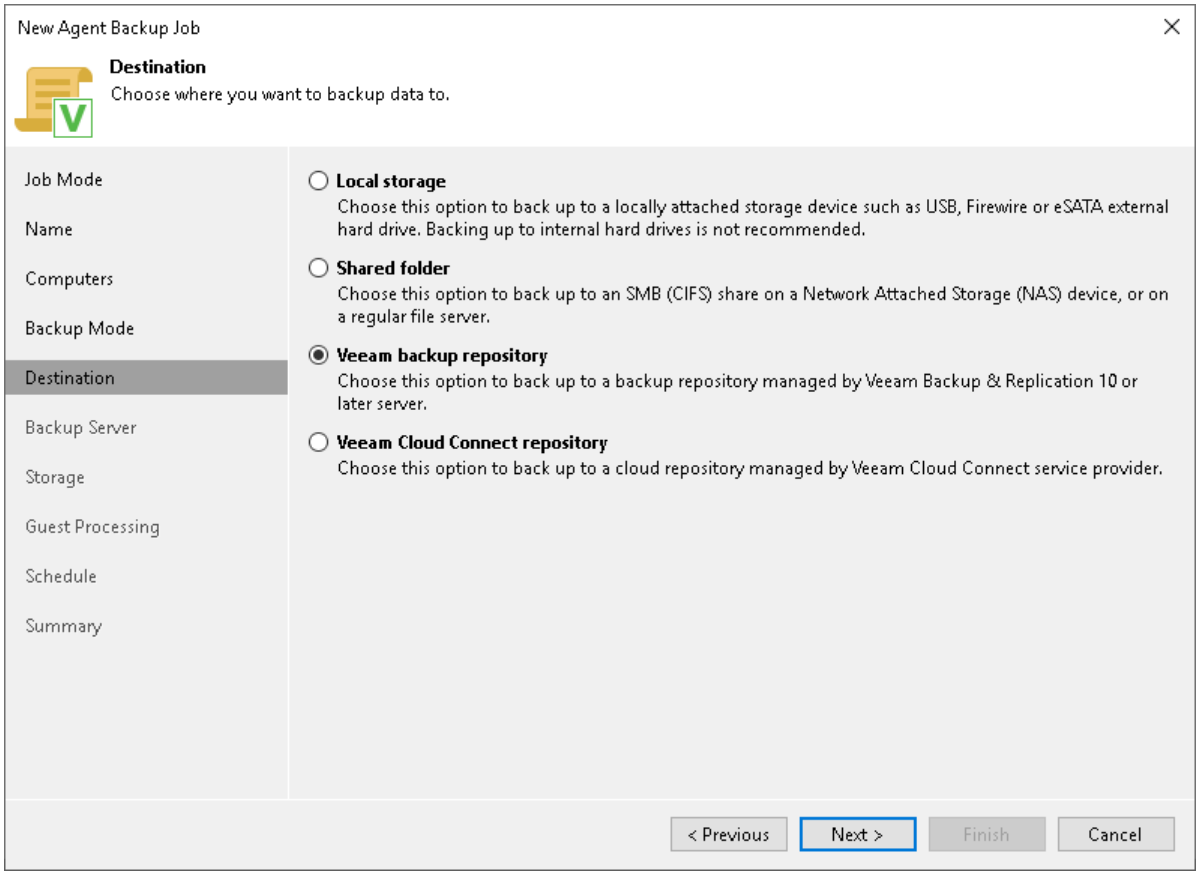
At this step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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.

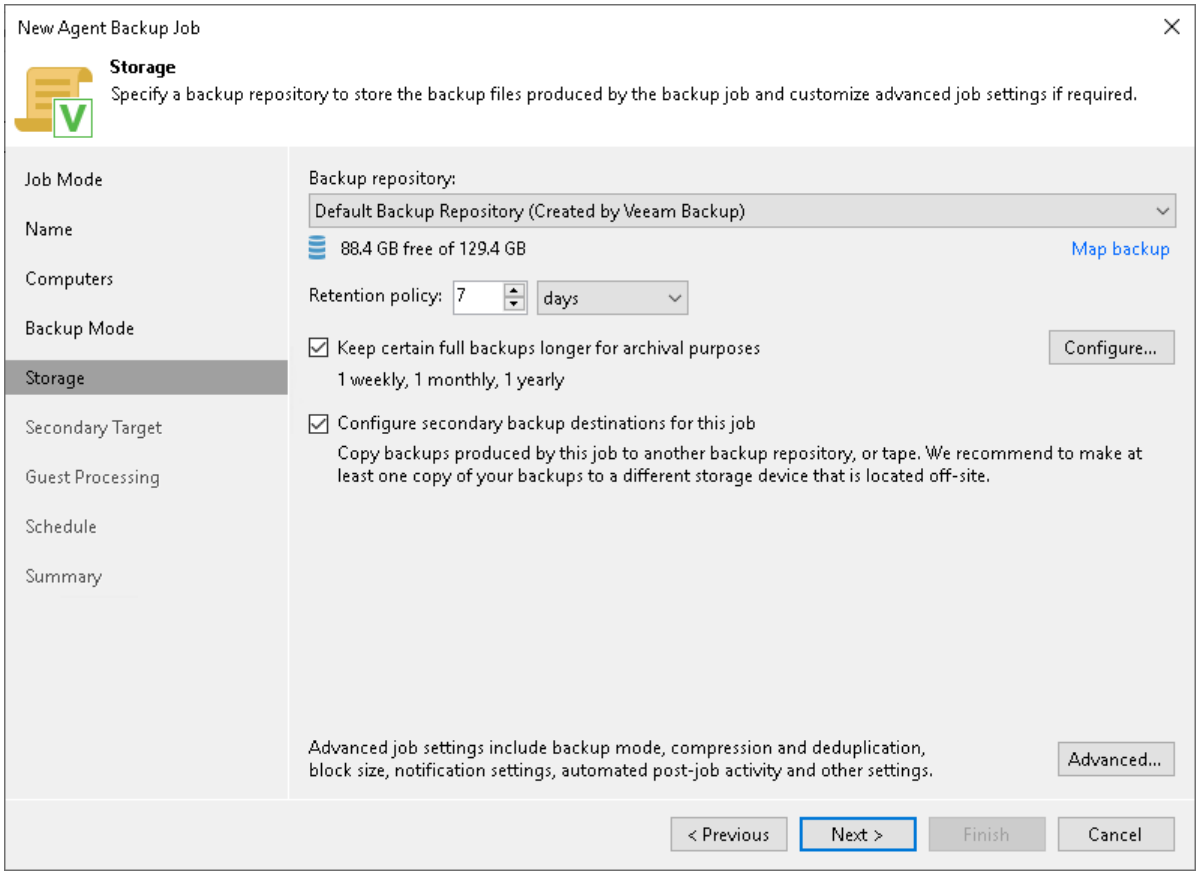
   > **NOTE**
   >
   > Mind the following:
   >
   > - The **Map backup** link is available only for a Veeam Agent backup job managed by the backup server. If you want to map a backup job managed by Veeam Agent, see Backup Job Mapping.
   > - You cannot map a Veeam Agent backup job configured in Veeam 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 certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

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 backup 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 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.

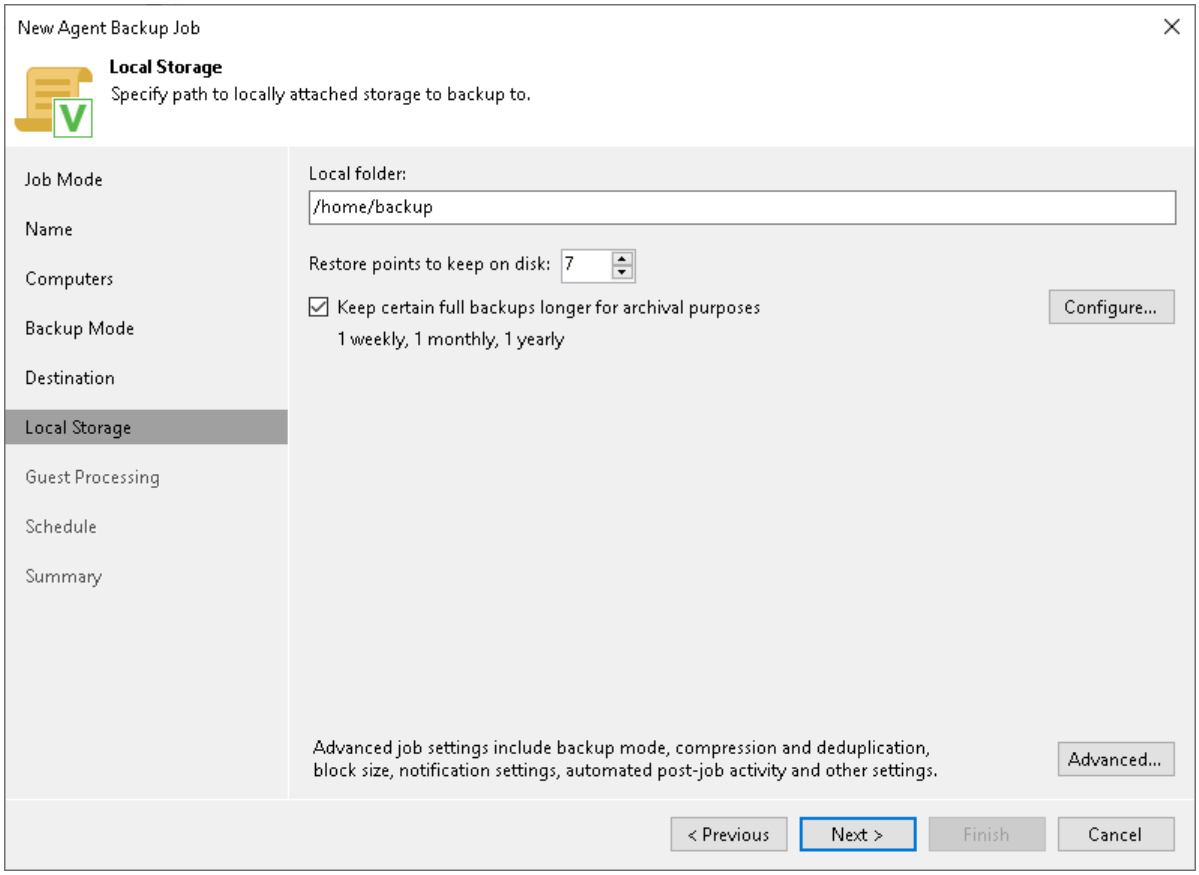
   > **IMPORTANT**
   >
   > USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.

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. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

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



Shared Folder Settings

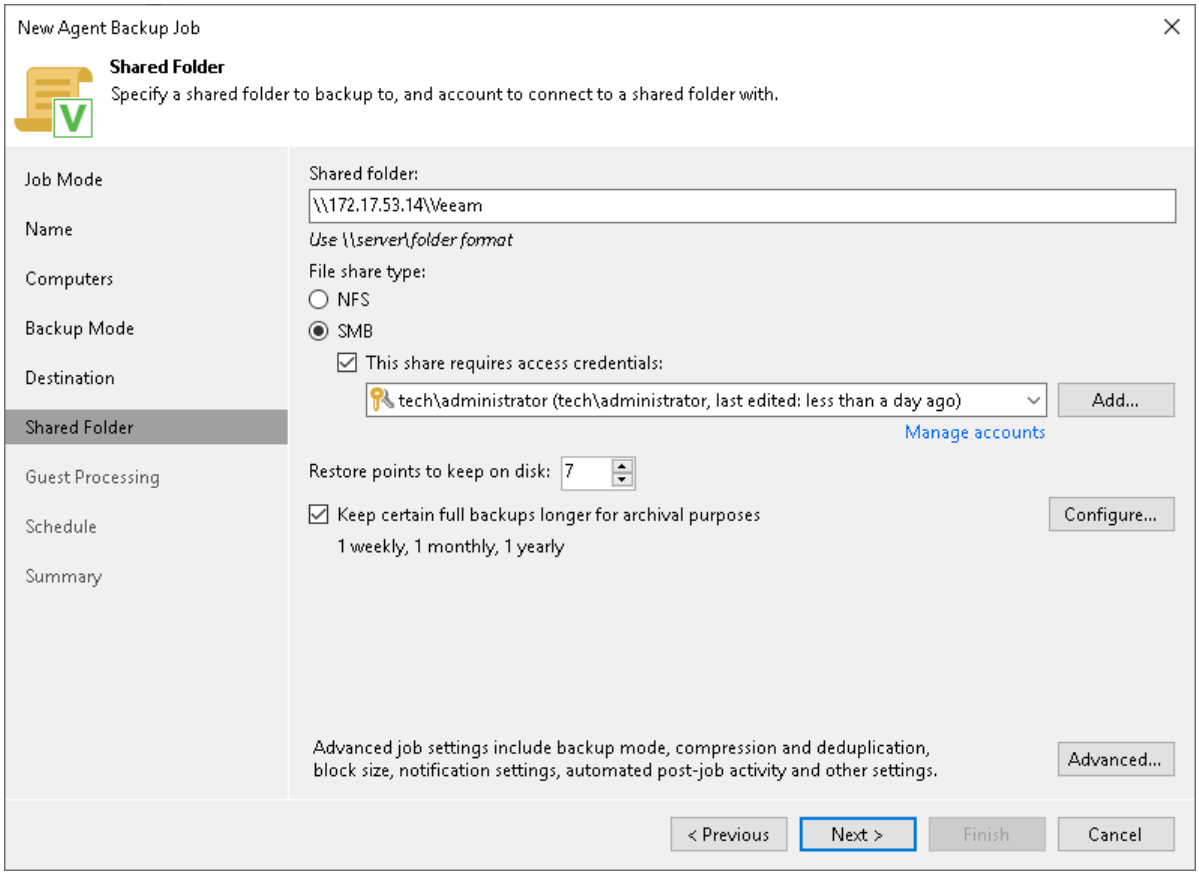
The **Shared Folder** step of the wizard is available if you have selected the **Managed by agent** mode at the Job Mode step of the wizard and chosen to save the backup in a network shared folder.

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. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

6. 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:

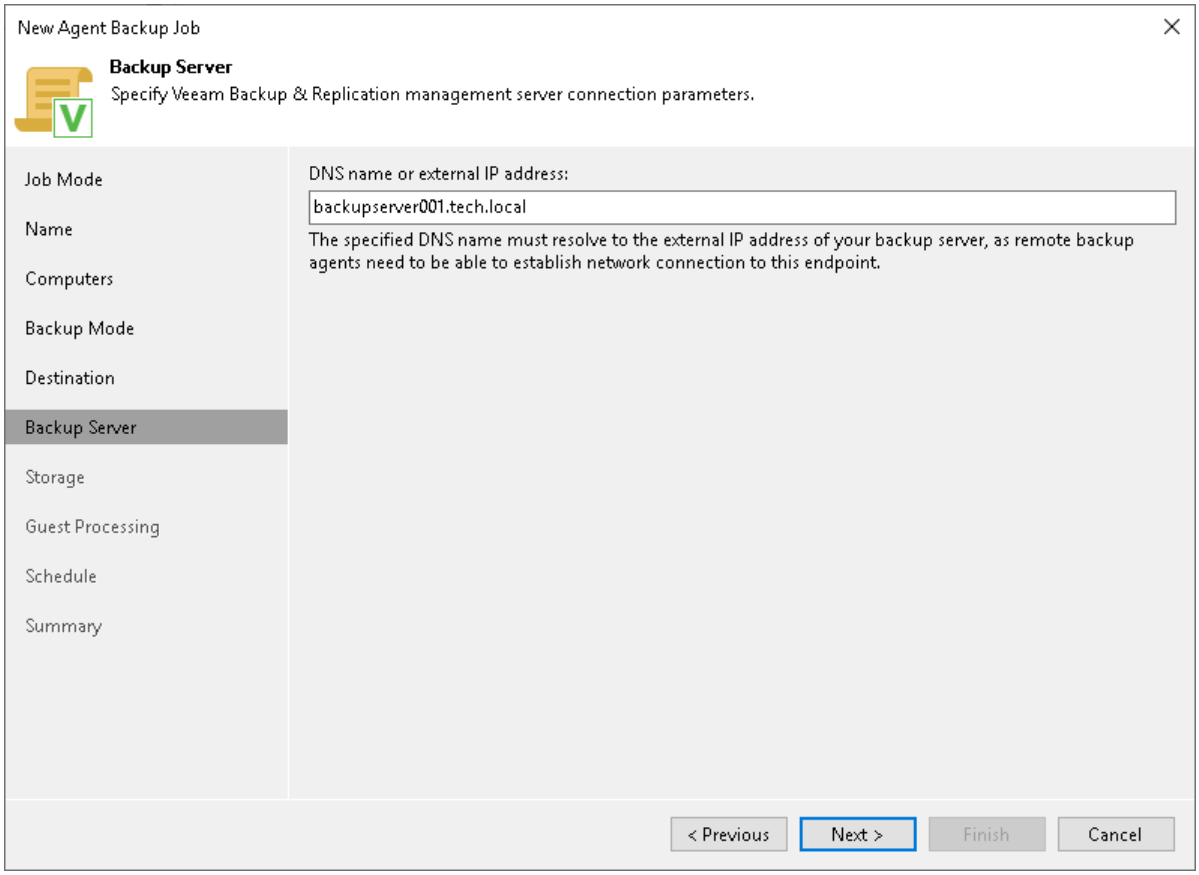
1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Backup Repository step of the wizard, select the Veeam backup repository.

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:

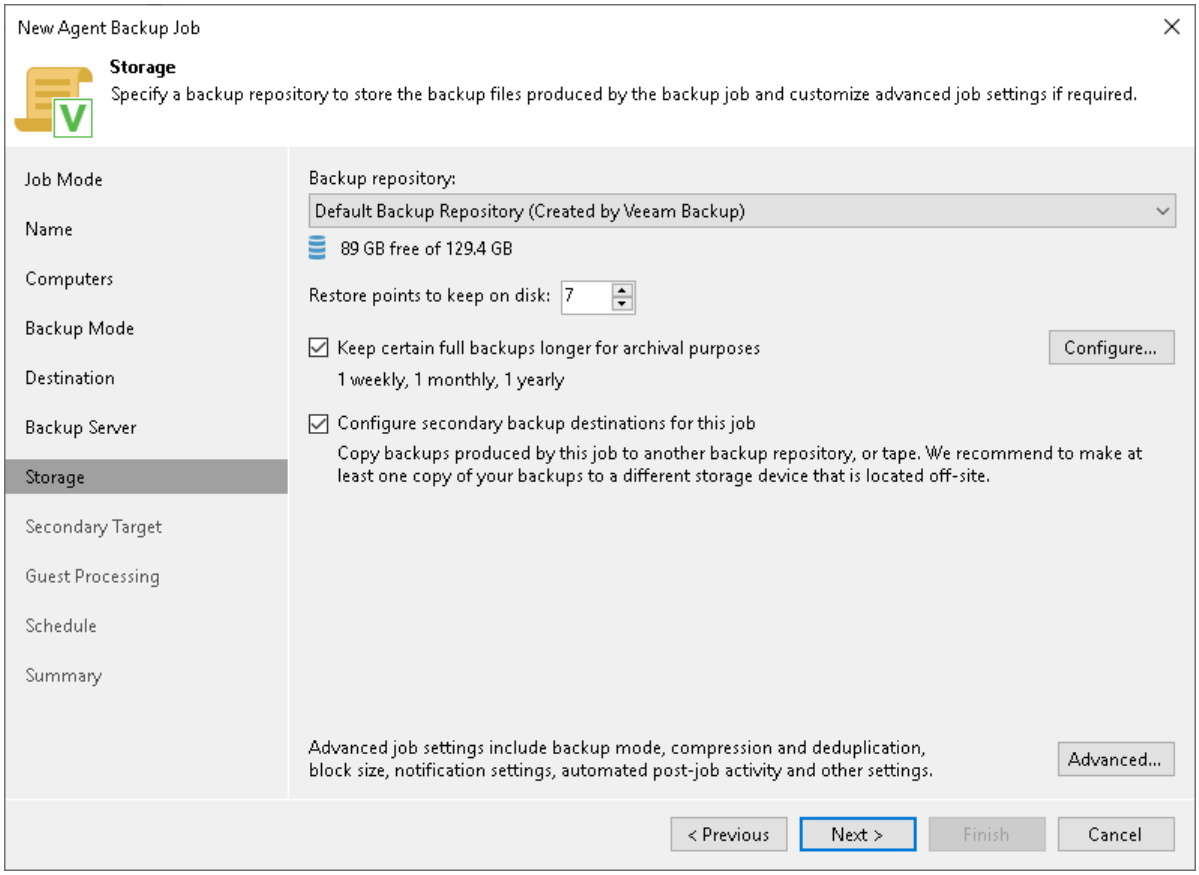
1. From the **Backup repository** list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.
2. In the **Restore points to keep on disk** field, 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. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.
4. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary backup 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.
5. Click **Advanced** to specify advanced settings for the backup job. To learn more, see Specify Advanced Backup Settings.

TIP

You can map the job to a specific backup stored on the Veeam 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. To learn more, see Backup Job Mapping.



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.

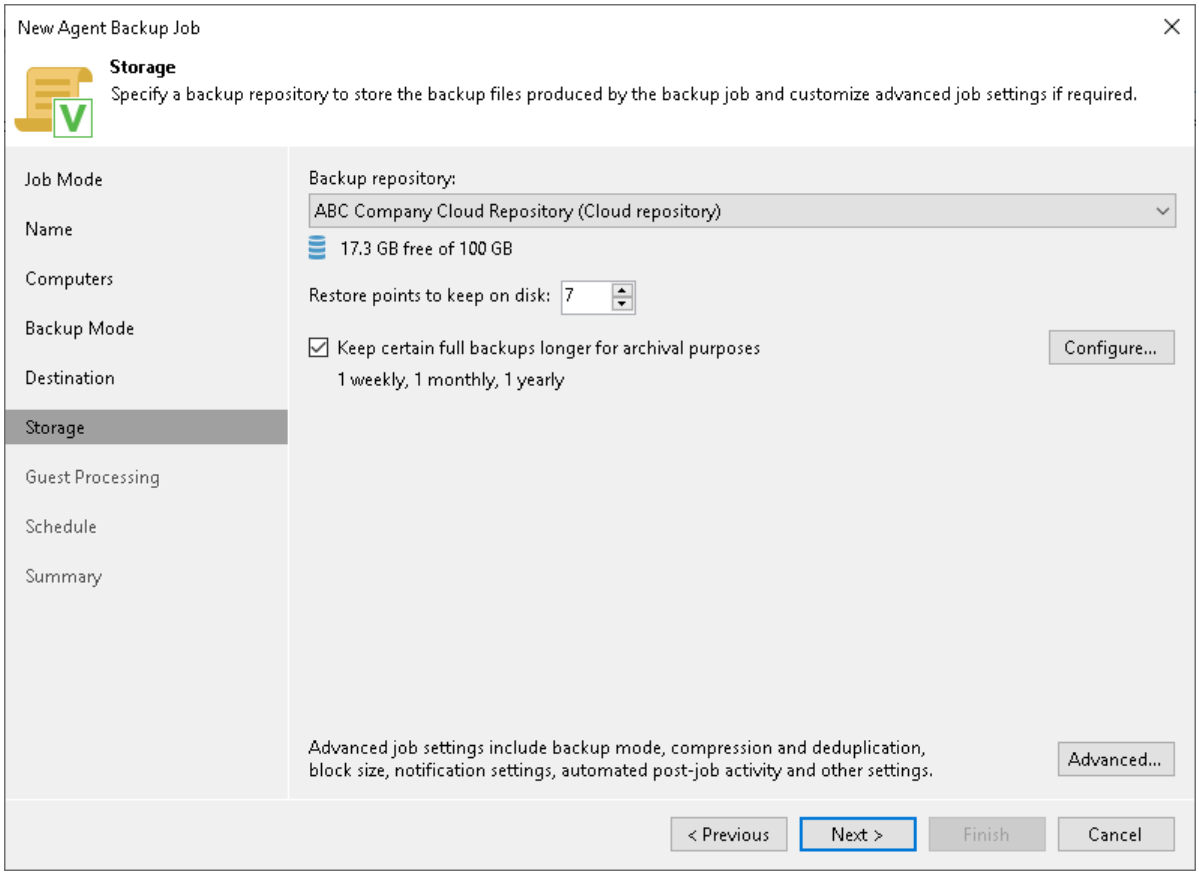
> **NOTE**
>
> Keep in mind that FQDN or IP addresses of Veeam Agent computers that you back up to the cloud repository will be visible to the Veeam Cloud Connect service provider. To learn more, see Creating Protection Groups: Before You Begin.

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. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain 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 Long-Term Retention Policy (GFS) section in the Veeam Backup & Replication User Guide.

   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

4. 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

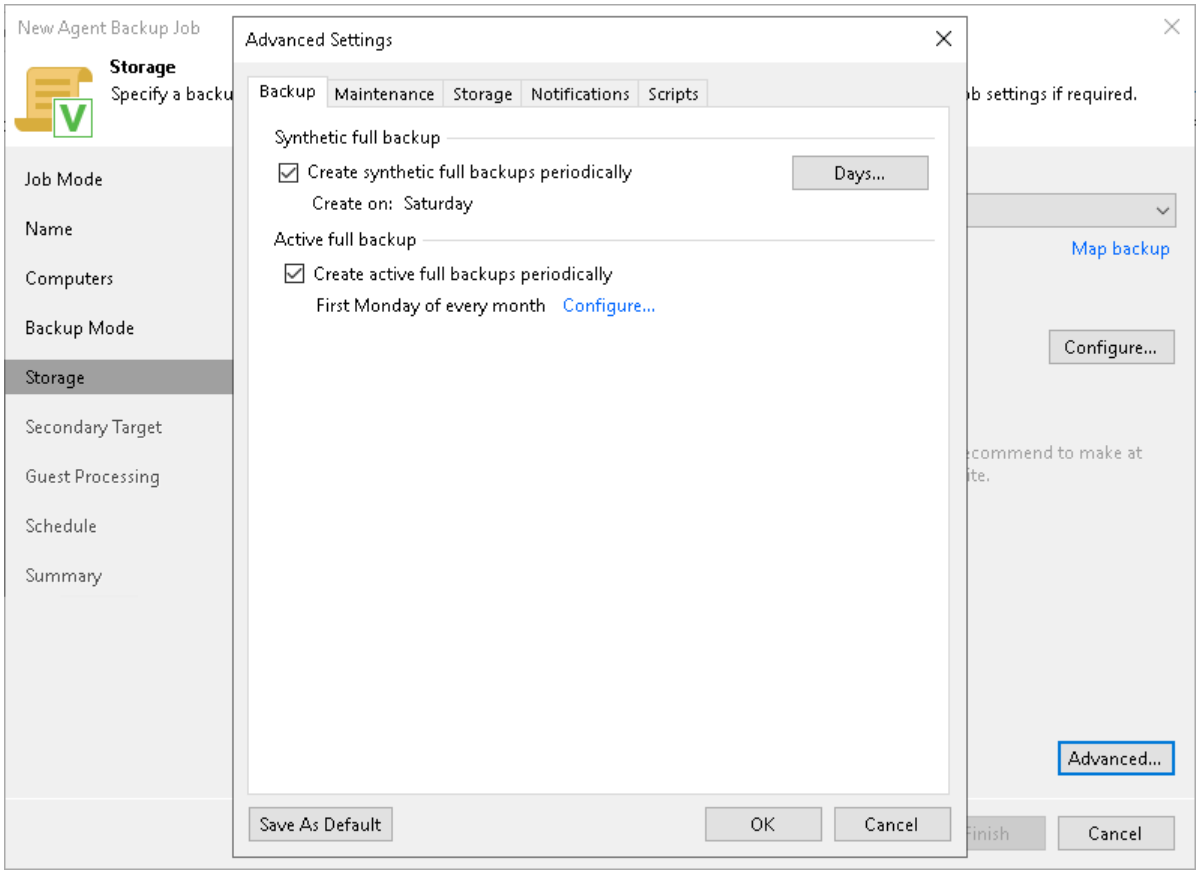
To specify settings for a backup chain created with the backup job:

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 and click **Configure** 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 click **Configure** to 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**
   >
   > The **Defragment and compact full backup file** option is not available for backup jobs targeted at object storage. For object storage, Veeam Agent offers a special health check mechanism as default. To run the health check for object storage, enable the **Perform backup files health check** option in the **Storage-level corruption guard** section and specify the health check schedule.
   >
   > You can also switch from the health check for object storage to the standard health check. To do so, select the **Verify content of each object in backup** check box in the backup job settings. Keep in mind that enabling this setting may result in additional charges from your object storage provider.
   >
   > For more information, see the Health Check for Object Storage section in the Veeam Agent for Linux User Guide.

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 click **Configure** to specify the schedule for the compact operation.

> **NOTE**
>
> The **Defragment and compact full backup file** option is not available for backup jobs targeted at object storage.

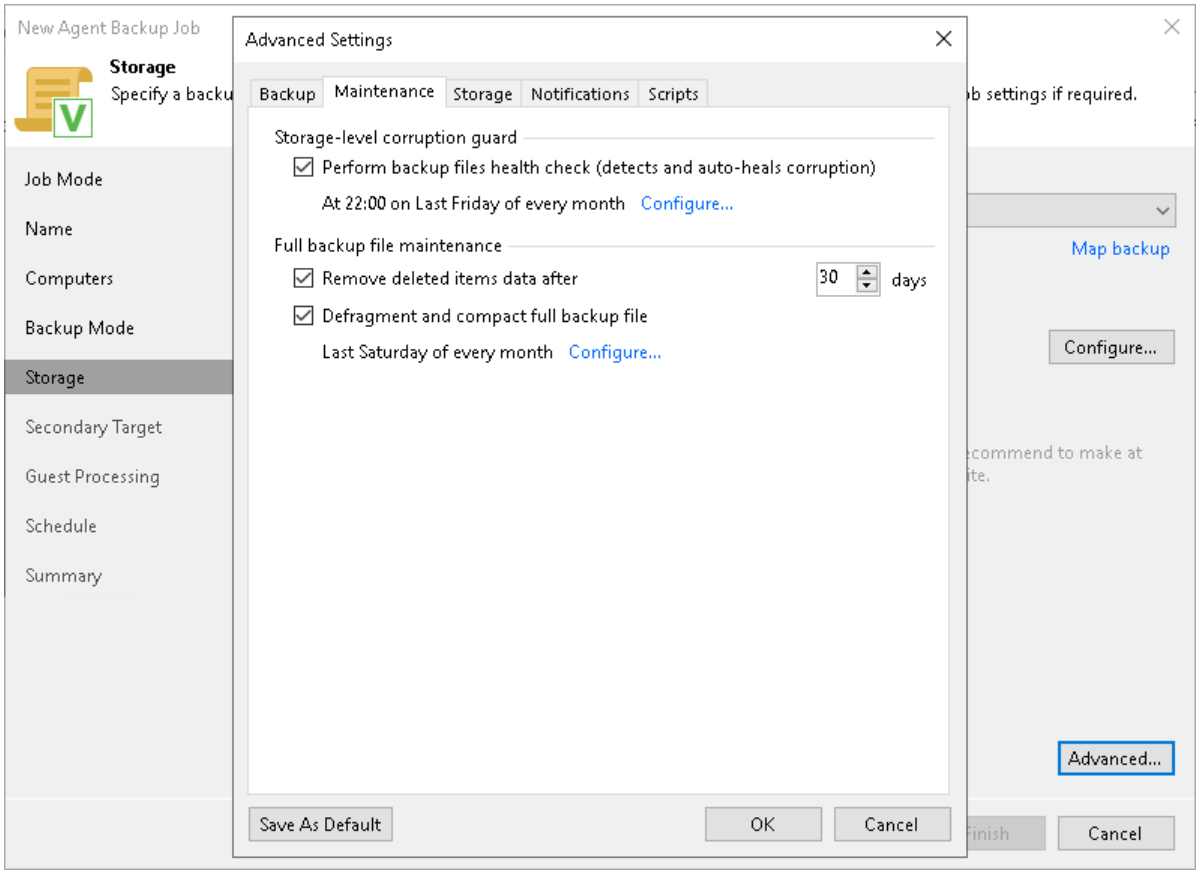
During the compact operation, Veeam Backup & Replication creates a new empty file and copies to it data blocks from the full backup file. As a result, the full backup file gets defragmented and the speed of reading and writing from/to the backup file increases.

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 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. 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. 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: *4 MB*, *1 MB*, *512 KB* or *256 KB*.
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.

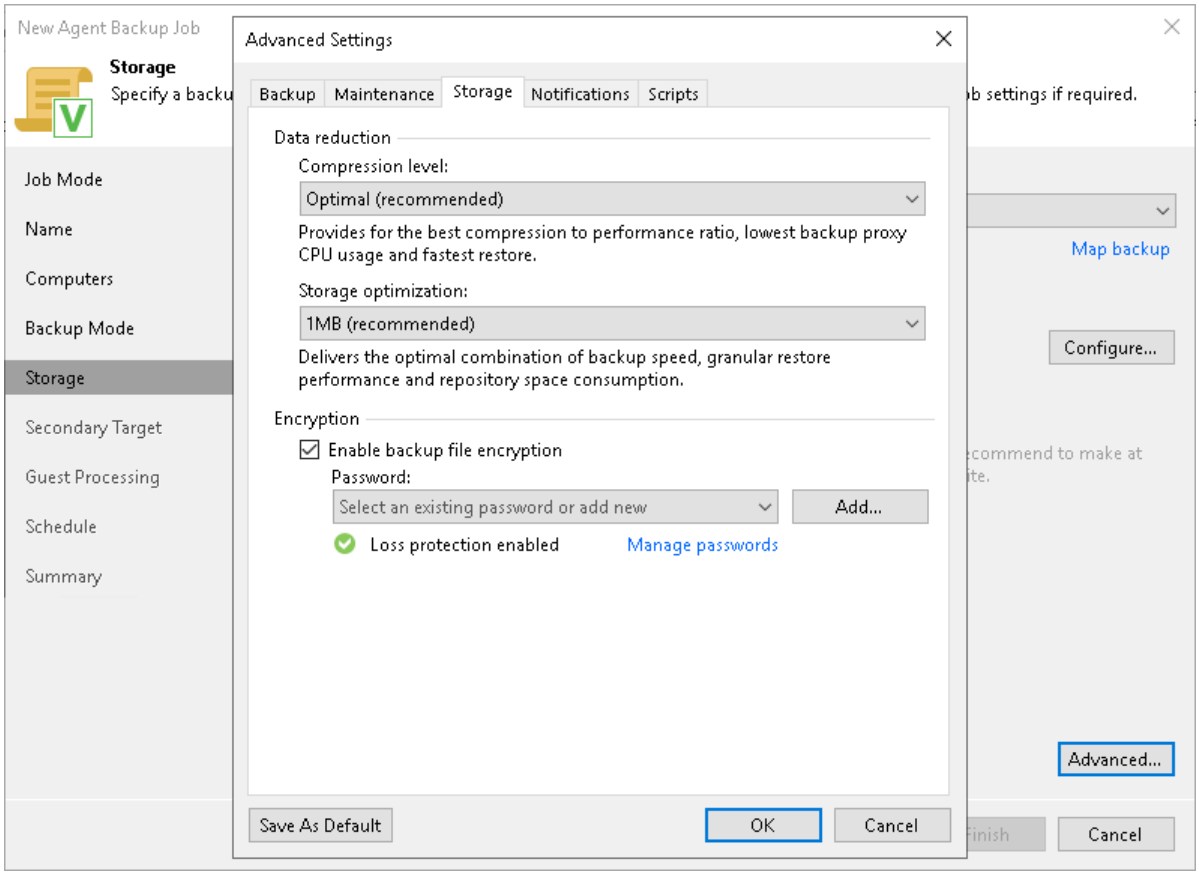
   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it: *Loss protection disabled*. For more information, see the Decrypting Data Without Password section in the Veeam Backup & Replication User Guide.

NOTE

Consider the following:

- 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 Linux 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.

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 Backup Job

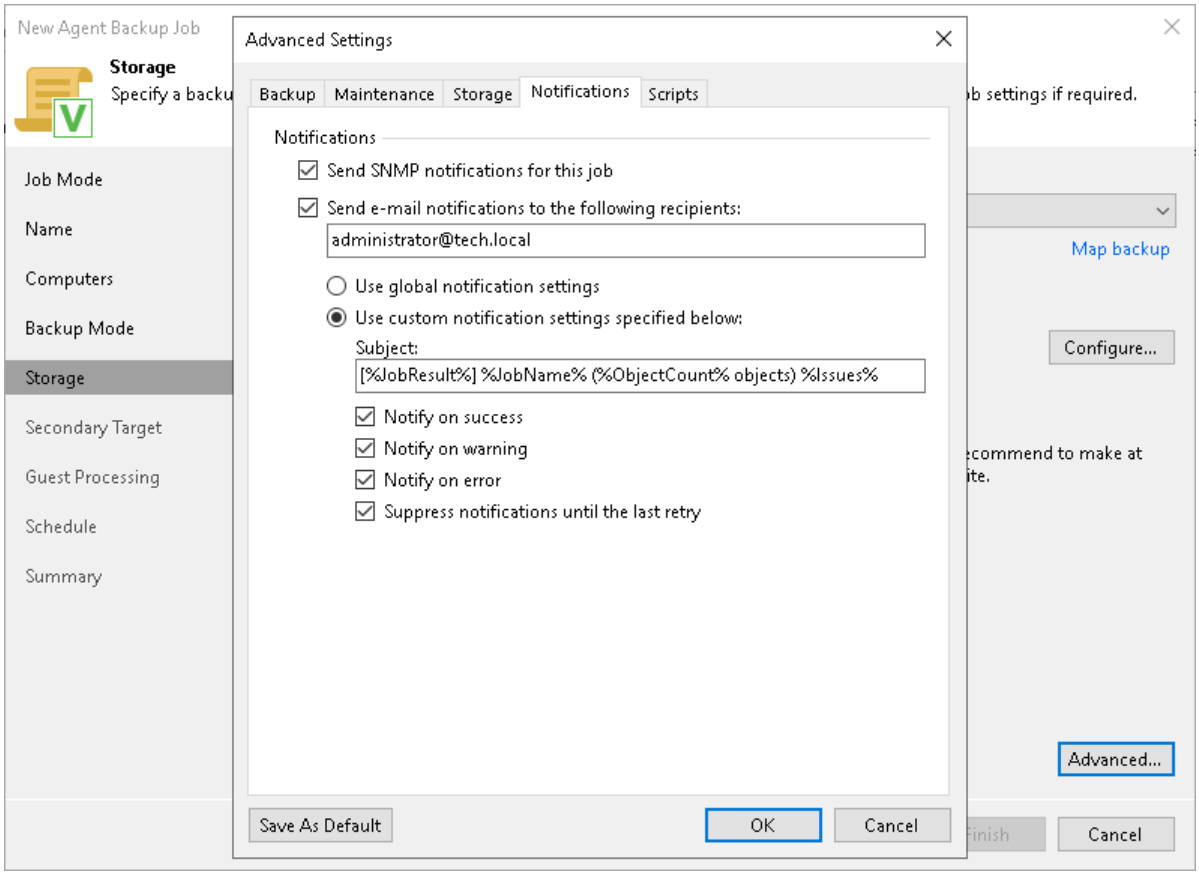
To specify notification settings for the backup job:

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

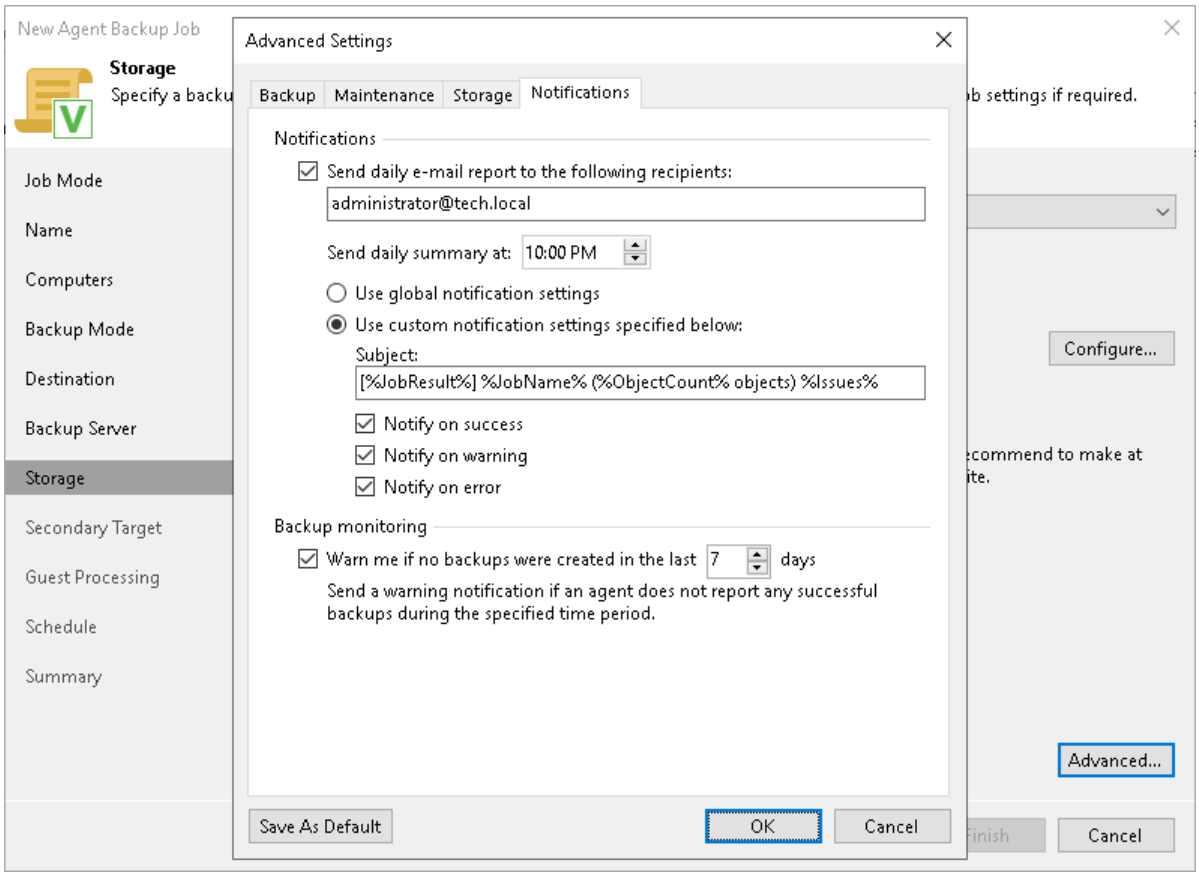
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup job sessions performed for 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 daily summary 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.
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. 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 **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.

5. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



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).

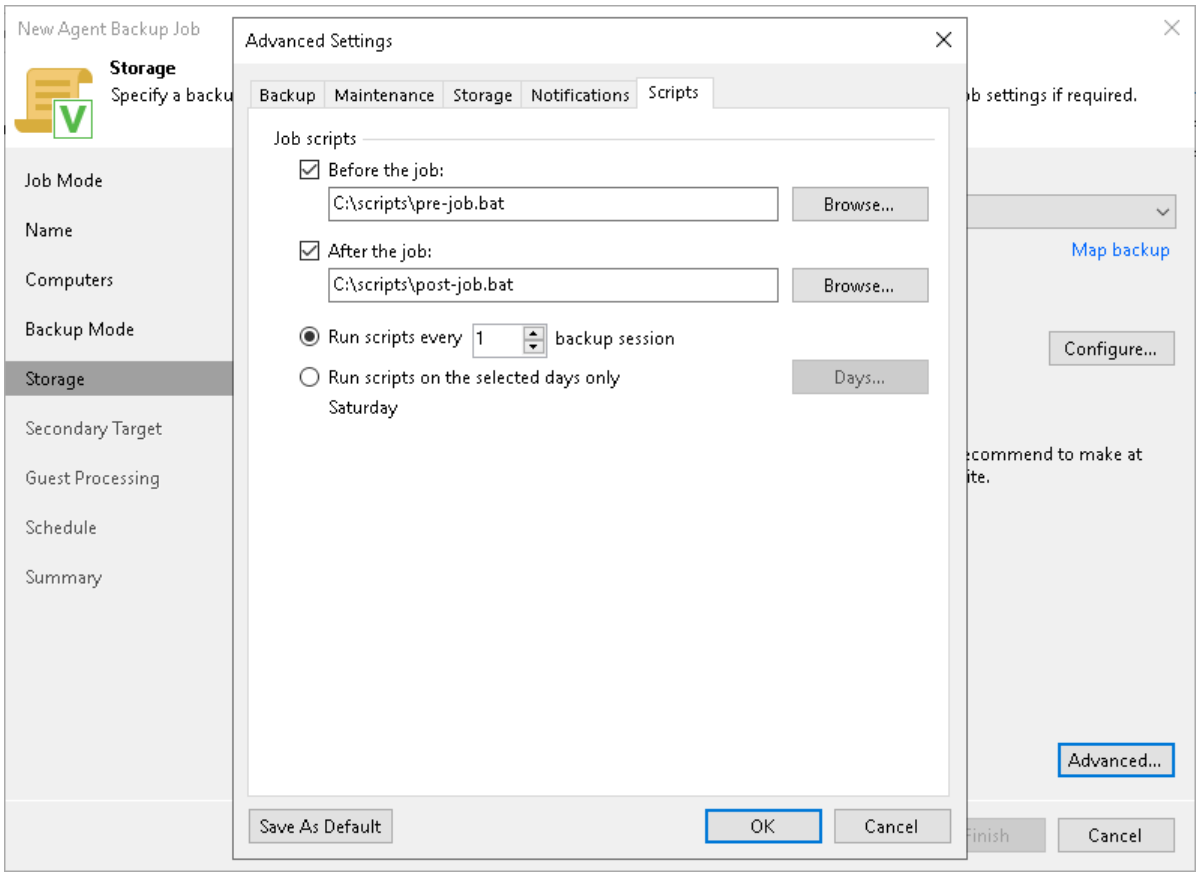
   You can select to execute pre- and post-backup actions after a number of backup sessions or on specific week days.

   - 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

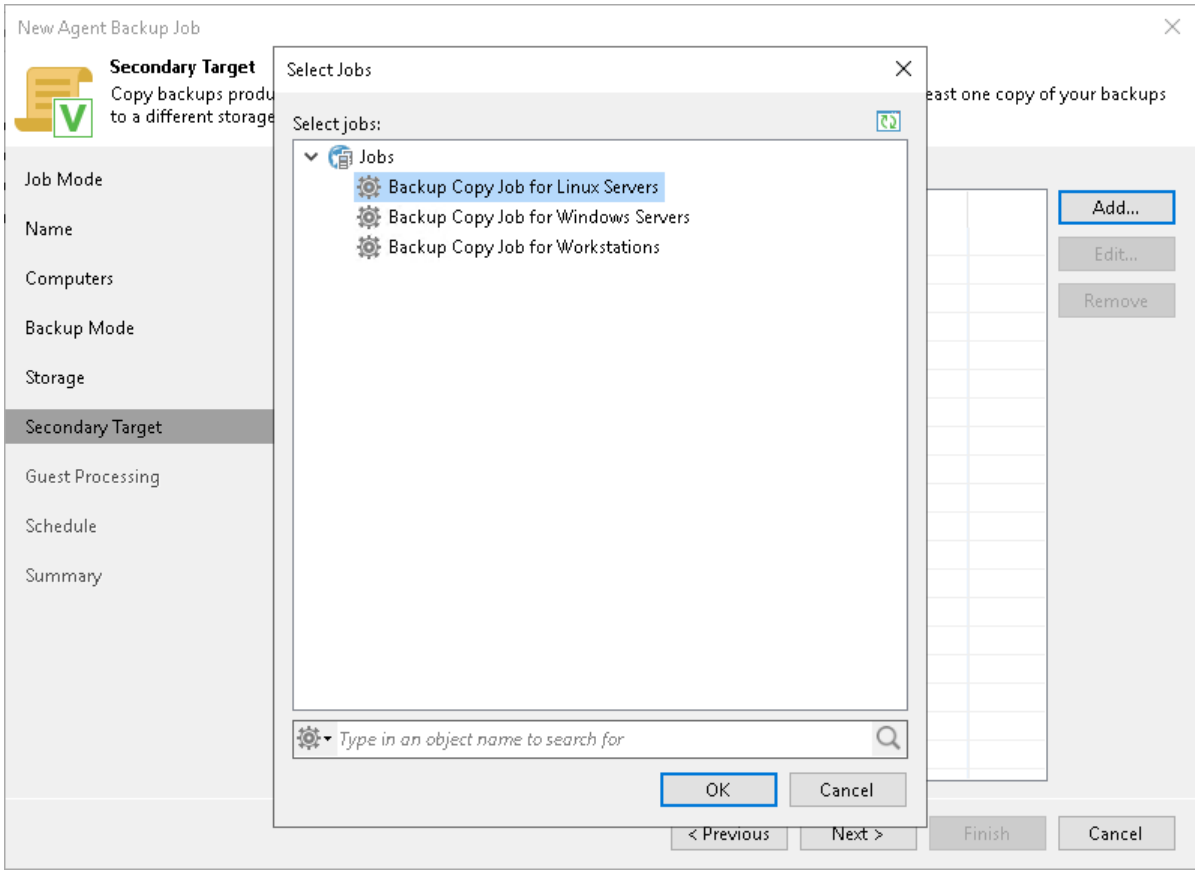
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

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
- File indexing

Application-Aware Processing

To configure application-aware processing:

1. Select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the **Application-Aware Processing Options** window, 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 backup job managed by Veeam backup server] In the **Guest OS credentials** list, select a user account that Veeam Agent will use for the processing of applications on the protected computer.

   By default, the **Use protection group credentials** option is selected in the list. With this option selected, Veeam Agent will do one of the following:

   - If you specified stored credential for this computer in the protection group settings, Veeam Agent will process applications using the specified account.
   - If you specified single-use credentials for this computer in the protection group settings, Veeam Agent will use the `root` user.

   To learn more stored and single-use credentials, see Specifying Computers.

   If you want to use account that is not available in the **Guest OS credentials** list, click the **Manage accounts** link or click **Add** on the right to add credentials.

   To specify credentials for a particular computer or a protection group, click **Credentials** on the right to set up credentials. In the displayed list, select a protection group or individual computer and click **Set User**.

   Keep in mind that to specify credentials for a particular computer, you must include this computer to the backup job as a standalone object at the **Computers** step of the wizard. To do this, click **Add** and choose the computer whose credentials you want to add. Then select the computer in the list and specify the necessary credentials.

   > **NOTE**
   >
   > Veeam Agent uses credentials selected in the **Guest OS credentials** list for Veeam Transport Service and database systems processing.
   >
   > For file system indexing and scripts execution, Veeam Agent always uses the `root` user.
4. Configure the necessary settings for the selected protection group or individual computer:
   - General Settings
   - Processing settings for Oracle database system
   - Processing settings for MySQL database system
   - Processing settings for PostgreSQL database system
   - Backup job and snapshot scripts

NOTE

Consider the following:

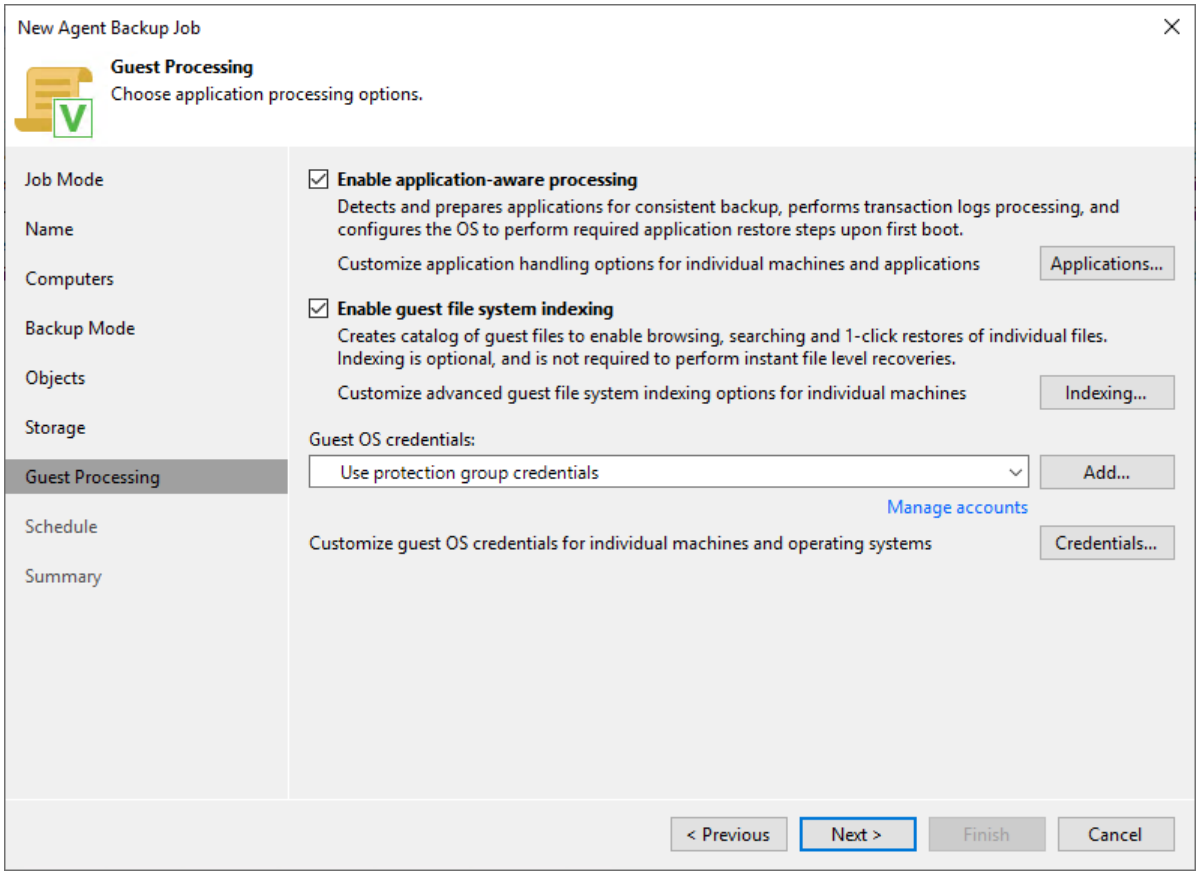
- Application-aware processing and database processing options are available if you have selected the **Server** option at the Job Mode step of the wizard.
- Application-aware processing and database processing options are available if you have selected the **Entire computer** or **Volume level backup** option at the Backup Mode step of the wizard.
- Veeam Agent does not support processing of multiple database systems on one Veeam Agent computer.
- 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.

File Indexing

To configure file indexing setiings:

1. 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. Configure file indexing settings for the selected protection group or individual computer. To learn more, see File Indexing.



Application-Aware Processing

If a computer 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.

Before you start working on the General tab, check the following at the **Guest Processing** step of the wizard:

1. The **Enable application-aware processing** check box is selected.
2. In the **Application-Aware Processing Options** window, a necessary protection group or individual computer is added to the list.

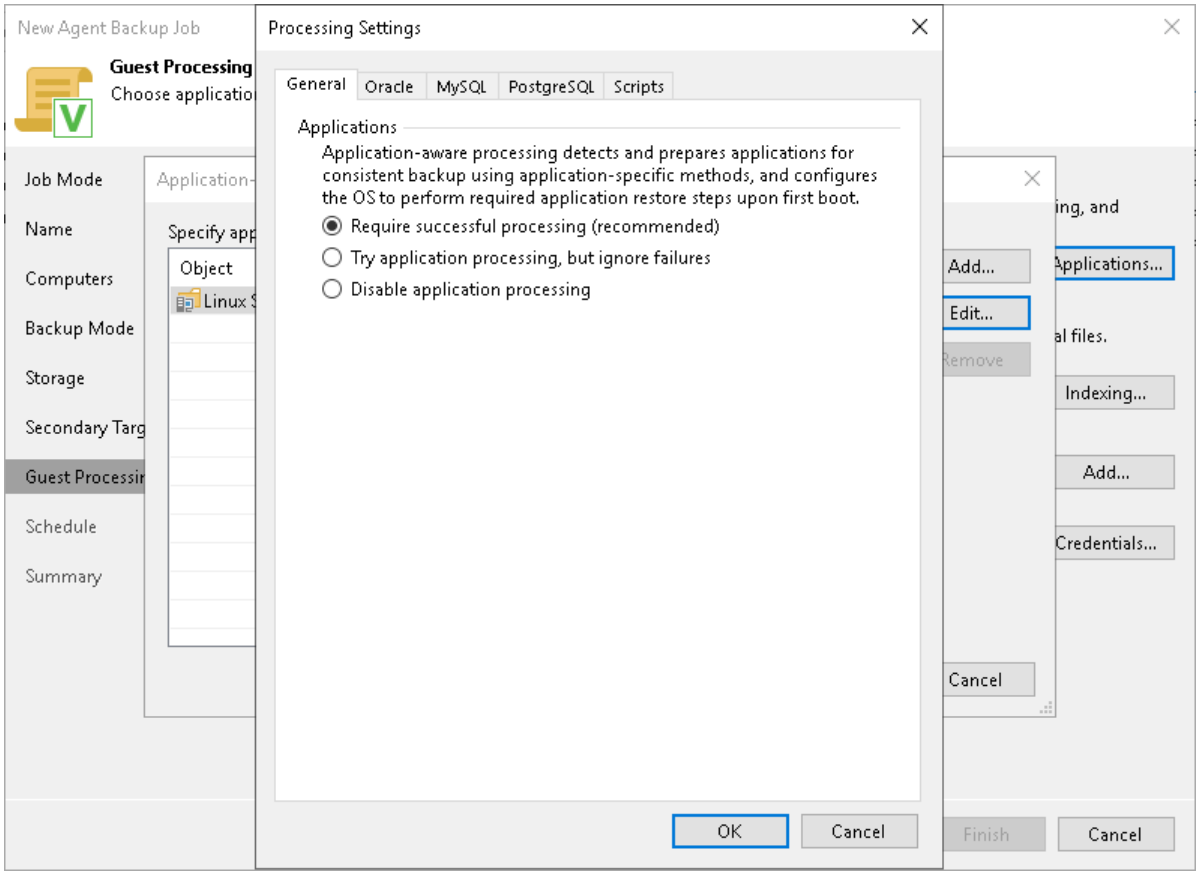
For details, see Guest Processing Settings.

Application Processing Settings

1. At the **Guest Processing** step of the wizard, click **Applications**.
2. In the **Application-Aware Processing Options** window, select the necessary object, click **Edit**.
3. 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. Information about the skipped database will be displayed in a warning message in the job session statistics. 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 still will be able to specify script settings for the job on the **Scripts** tab of the window.



Oracle Processing Settings

You can specify how Veeam Agent for Linux must process Oracle archived logs.

Before you start working with Oracle archived logs, check the following:

1. At the **Guest Processing** step of the wizard, the **Enable application-aware processing** check box is selected.
2. At the **Guest Processing** step of the wizard, in the **Application-Aware Processing Options** window, a necessary protection group or individual computer is added to the list.
3. At the **Guest Processing** step of the wizard, in the **Guest OS credentials** list, a necessary user account is selected.

For details, see Guest Processing Settings.

4. On the **General** tab, in the **Applications** section, **Require successful processing** or **Try application processing, but ignore failures option is selected**.

For details, see Application-Aware Processing.

Oracle Processing

To specify how Veeam Agent for Linux must process Oracle archived logs, perform the following:

1. At the **Guest Processing** step of the wizard, click **Applications**.
2. In the **Application-Aware Processing Options** window, select the necessary object, click **Edit**, then click the **Oracle** tab.
3. On the **Oracle** tab, 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.

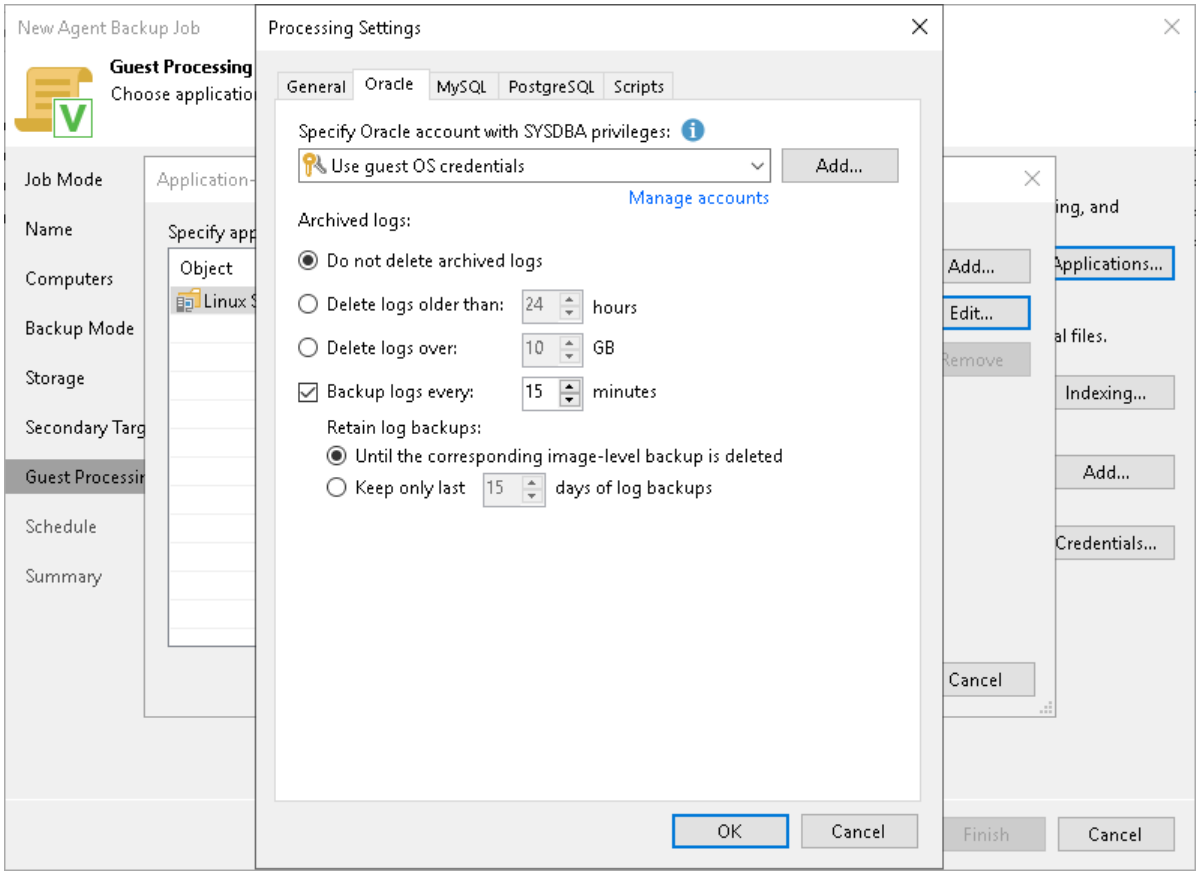
   By default, the **Use guest OS credentials** option is selected in the list. With this option selected, Veeam Agent for Linux will connect to the Oracle database under the account that you have specified for the protected computer at the **Guest Processing** step of the wizard.

   > **NOTE**
   >
   > Veeam Agent for Linux always uses the root account to connect to the Oracle database. This includes the following cases:
   >
   > - An Oracle account with the SYSDBA rights is selected in the **Specify Oracle account with SYSDBA privileges** list, and the database is set to use database authentication.
   > - A non-root OS account added to the group that owns configuration files for the Oracle database (for example, the oinstall group) is selected in the **Specify Oracle account with SYSDBA privileges** list, and the database is set to use authentication by the operating system.

4. In the **Archived logs** section, specify if Veeam Agent for Linux must delete archived logs on the Oracle database:
   - 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.
   - 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.
5. [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.
6. [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.

Before you start working on the **MySQL** tab, check the following:

1. At the **Guest Processing** step of the wizard, the **Enable application-aware processing** check box is selected.
2. At the **Guest Processing** step of the wizard, in the **Application-Aware Processing Options** window, a necessary protection group or individual computer is added to the list.

For details, see Guest Processing Settings.

3. On the **General** tab, in the **Applications** section, **Require successful processing** or **Try application processing, but ignore failures option is selected**.

For details, see Application-Aware Processing.

MySQL Processing

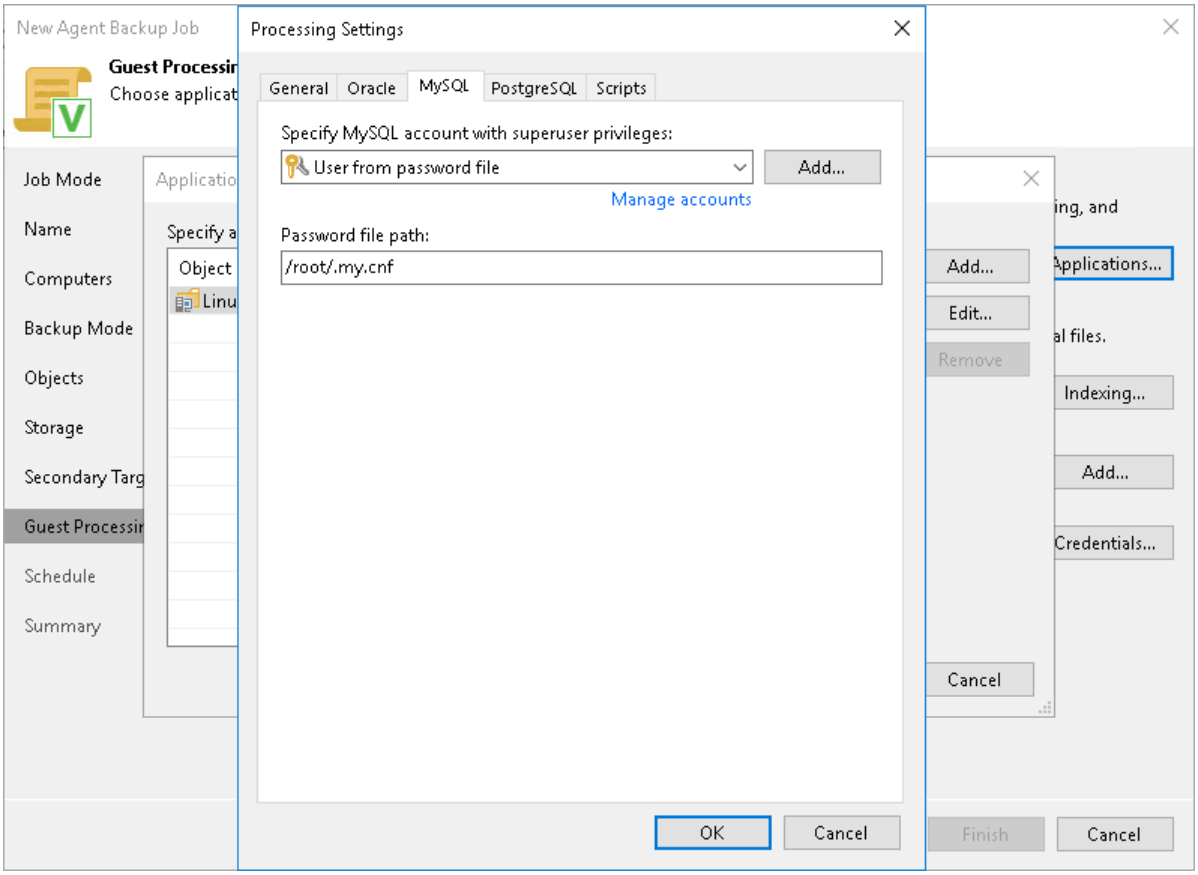
To specify how Veeam Agent for Linux must process a MySQL database, perform the following:

1. At the **Guest Processing** step of the wizard, click **Applications**.
2. In the **Application-Aware Processing Options** window, select the necessary object, click **Edit** and switch to the **MySQL** tab.
3. On the **MySQL** tab, 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 be able to access the table metadata. Thus, Veeam Agent will not process the table. To learn more, see MySQL documentation.
   - LOCK TABLES. If the account does not have this privilege, Veeam Agent will not process tables based on the MyISAM storage engine.

   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.
4. If you want to specify a custom path to the password file, specify a full path in the **Password file path** field. Specifying relative paths is not supported.

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:

Before you start working with a PostgreSQL archived logs, check the following:

1. At the **Guest Processing** step of the wizard, the **Enable application-aware processing** check box is selected.
2. At the **Guest Processing** step of the wizard, in the **Application-Aware Processing Options** window, a necessary protection group or individual computer is added to the list.
3. At the **Guest Processing** step of the wizard, in the **Guest OS credentials** list, a necessary user account is selected.

For details, see Guest Processing Settings.

4. On the **General** tab, in the **Applications** section, **Require successful processing** or **Try application processing, but ignore failures option is selected**.

For details, see Application-Aware Processing.

PostgreSQL Processing

To specify how Veeam Agent for Linux must process PostgreSQL archived logs, perform the following:

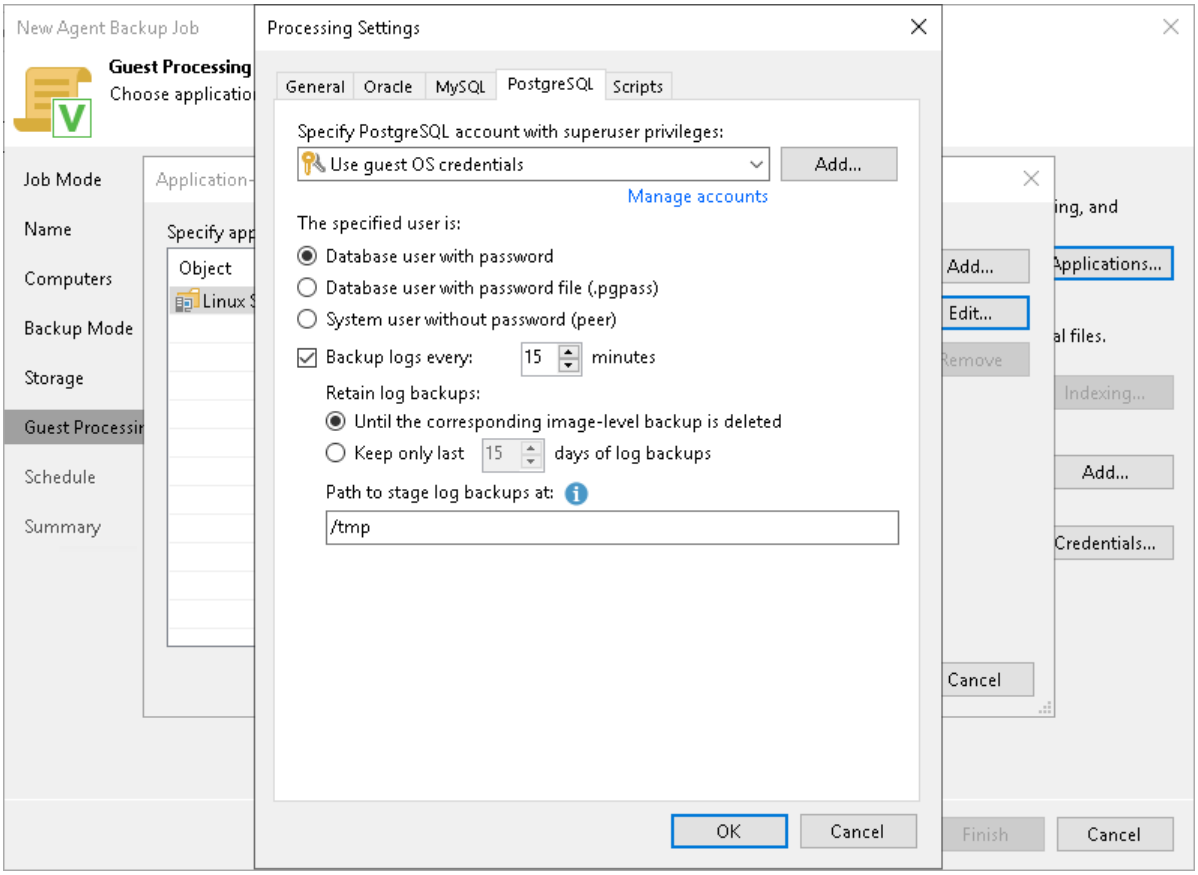
1. At the **Guest Processing** step of the wizard, click **Applications**.
2. In the **Application-Aware Processing Options** window, select the necessary object, click **Edit, then** click the **PostgreSQL** tab.
3. To specify a user account that Veeam Agent will use to connect to the PostgreSQL database, 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 8 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 OS 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 at the step 2.
4. In the **The specified user is** field, specify how Veeam Agent 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 7 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.
5. [For Veeam Agent jobs managed by the backup server] To back up PostgreSQL archived logs with Veeam Agent, 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.
6. [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.
7. [For Veeam Agent jobs managed by the backup server] In the **Path to stage log backups at** field, specify temporary storage location for the archive logs.

   During backup, Veeam Agent saves archive logs to a temporary storage, move logs to a Veeam backup repository and deletes logs from a temporary storage. Keep in mind the following:
   - Directory set as a temporary storage location must be locally accessible by the guest OS and have enough free space.
   - If temporary storage location for the archive logs is not specified or Veeam Agent cannot save logs in the specified directory for some reason, Veeam Agent will not be able to back up logs.

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:

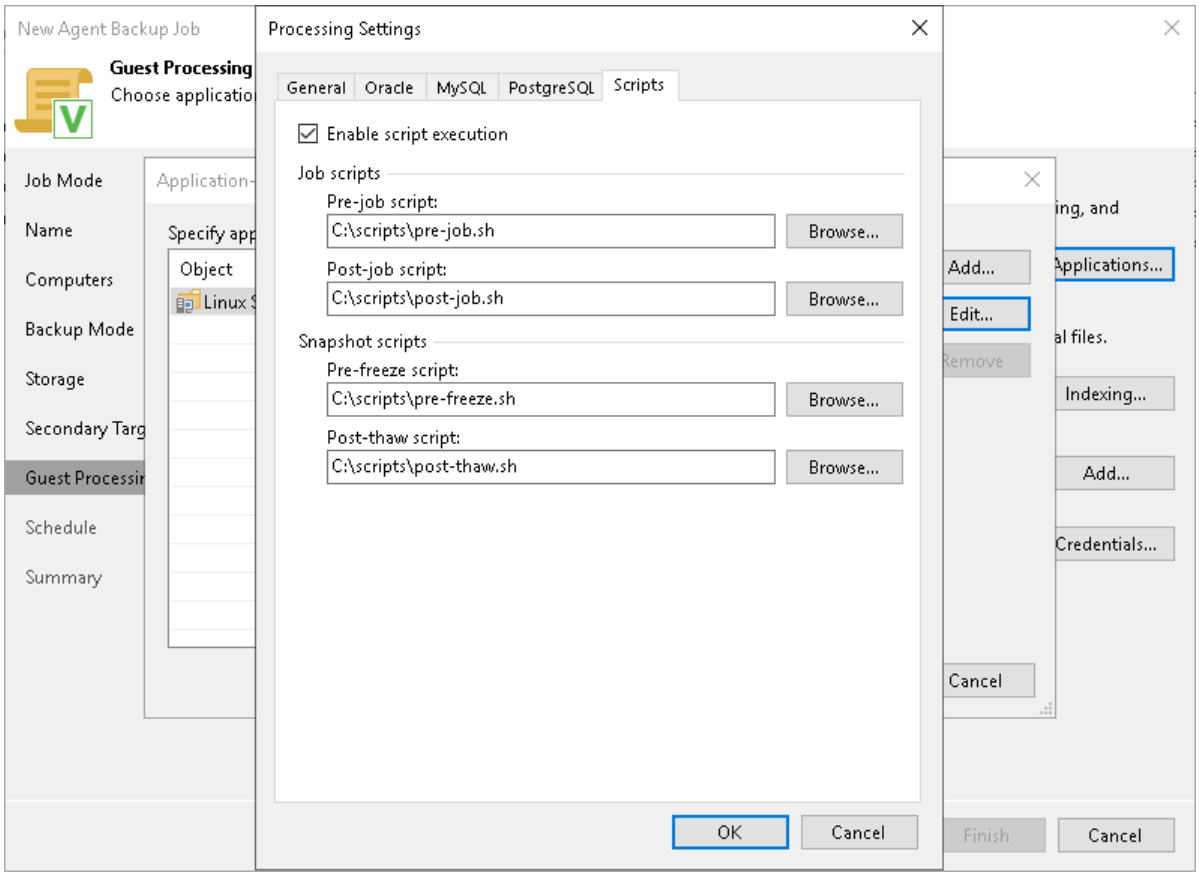
1. At the **Guest Processing** step, select the **Enable application-aware processing** check box.
2. Click **Applications**.
3. In the displayed list, select a protection group or individual computer and click **Edit**.

   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.



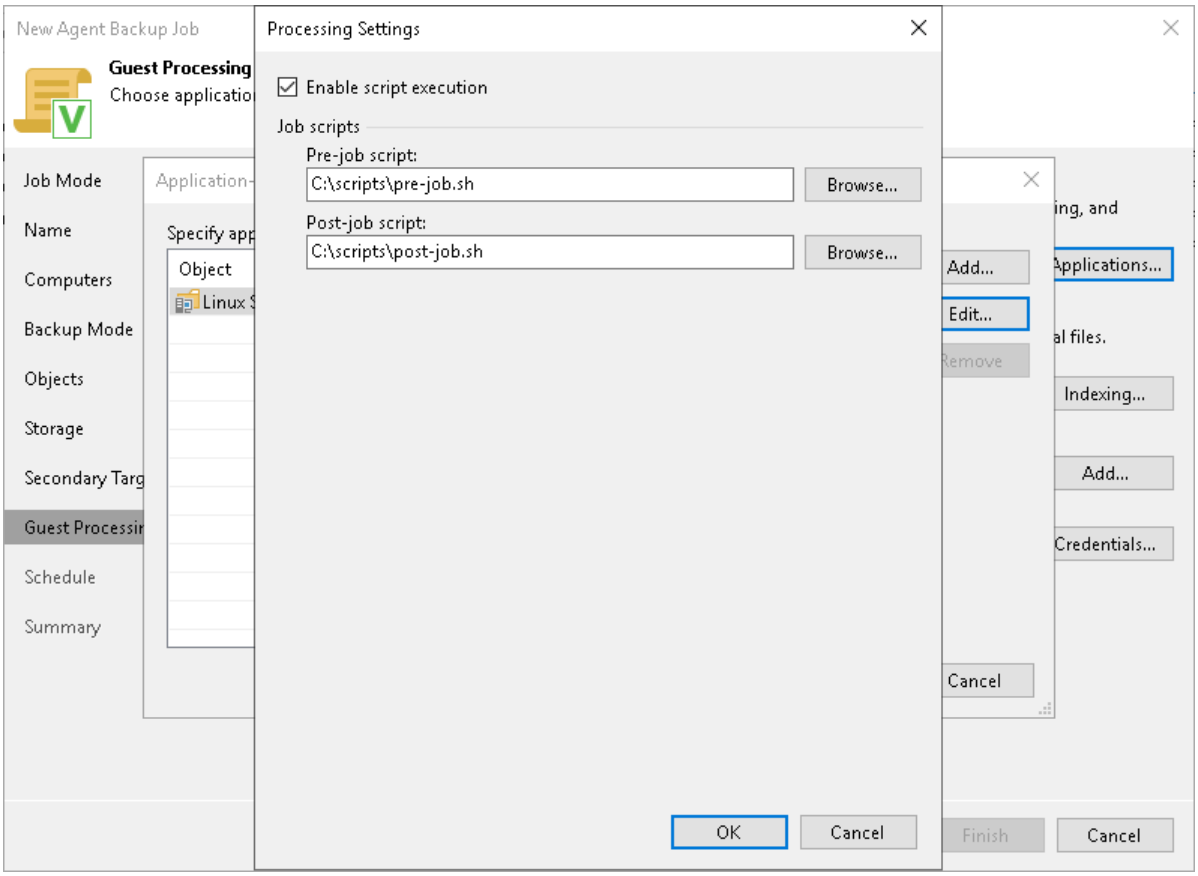
Specifying Backup Job Scripts

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:

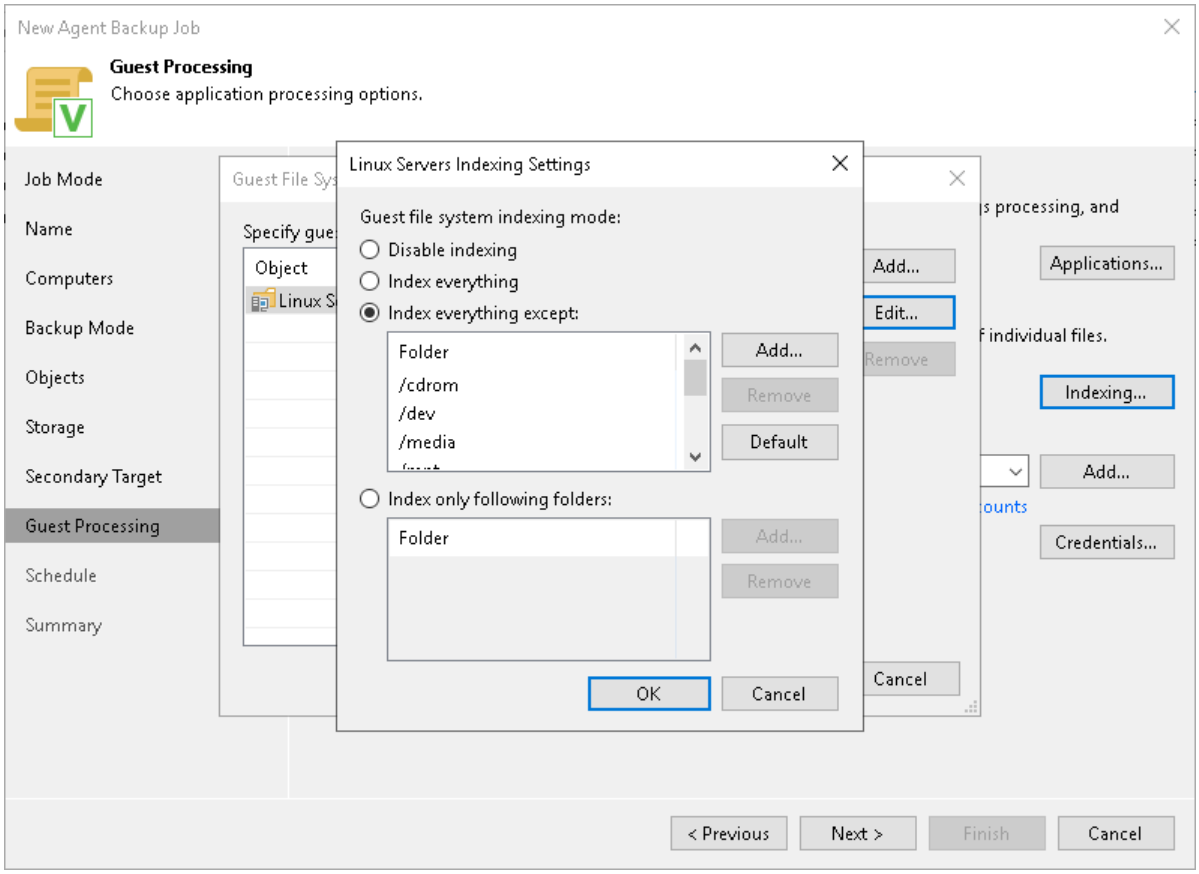
1. At the **Guest Processing** step of the wizard, select the **Enable guest file system indexing** check box.
2. Click **Indexing**.
3. In the displayed list, select the protection group or individual computer and click **Edit**.

   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*.
     - [For backup job managed by backup server] To define the permitted time window for the job, click **Schedule** and use the time table. 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

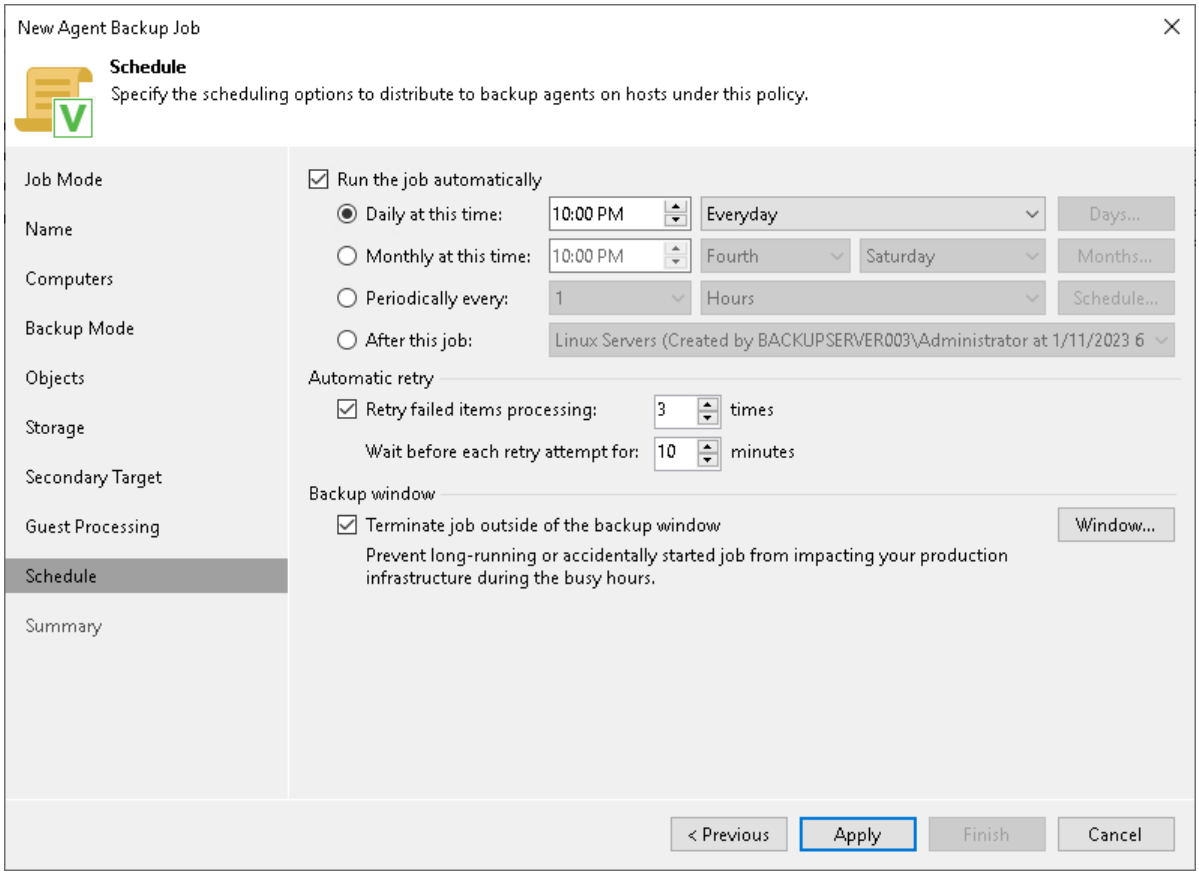
Mind the following:

- 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.



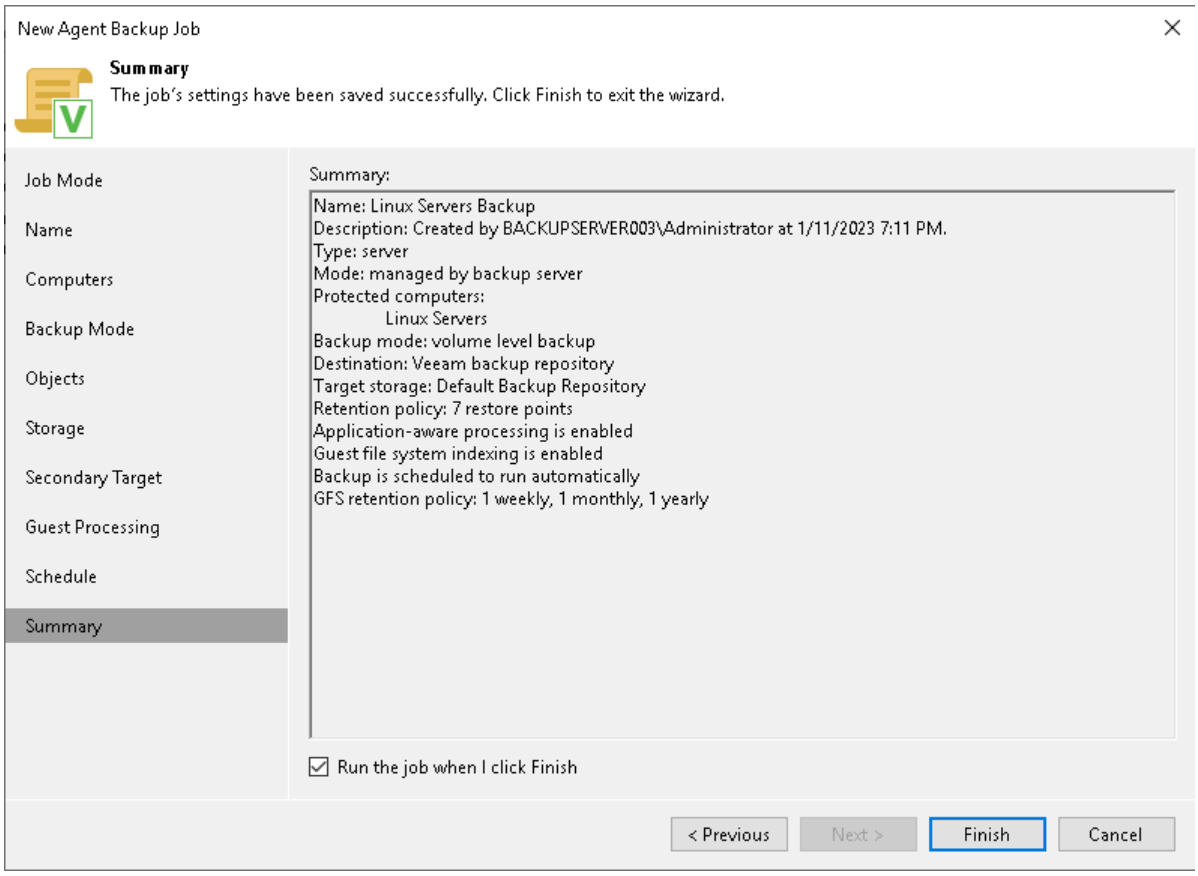
Step 13. Review Backup Job Settings

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.

[For backup job managed by Veeam Agent] Keep in mind that Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Linux Configuration.



Creating Veeam Agent Backup Policies

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.

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

- Microsoft Windows computers protected with Veeam Agent for Microsoft Windows
- Linux computers protected with Veeam Agent for Linux
- Unix computers protected with Veeam Agent for Unix
- macOS computers protected with Veeam Agent for Mac

After you create a backup policy, Veeam Backup & Replication 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.

Keep in mind that Veeam Backup & Replication does not connect to the protected computers added to the protection group for pre-installed Veeam Agents. In case of this protection group, computers connect to the Veeam backup server and become members of the protection group after Veeam Agent deployment. To learn more, see Protection Group Types.

Creating Policy for Windows Computers

Backup jobs and policies for Microsoft Windows computers protected with Veeam Agent for Microsoft Windows are configured in the same **New Agent Backup Job** wizard. When you select the **Managed by agent** option in the wizard, the subsequent steps of the wizard will automatically change to offer backup settings available in Veeam Agent for Microsoft Windows. For details, see Creating Agent Backup Job for Windows Computers.

Creating Policy for Linux Computers

Backup jobs and policies for Linux computers protected with Veeam Agent for Linux are configured in the same **New Agent Backup Job** wizard. When you select the **Managed by agent** option in the wizard, the subsequent steps of the wizard will automatically change to offer backup settings available in Veeam Agent for Linux. For details, see Creating Agent Backup Job for Linux.

Creating Policy for Unix Computers

To back up data of a computer protected with Veeam Agent for Oracle Solaris or Veeam Agent for IBM AIX, you must configure a Veeam Agent backup policy in Veeam Backup & Replication. This backup policy will be applied to Veeam Agent computers to create individual backup jobs. Using these jobs, Veeam Agents will perform backup operations.

Before configuring a backup policy, check prerequisites. Then use the **New Agent Backup Job** wizard to define settings for the backup policy.

1. Launch the New Agent Backup Job wizard.
2. Select the type of protected computers.
3. Specify policy name and description.
4. Select computers to back up.
5. Select backup mode.
6. Specify backup scope.
7. Select backup destination.
8. Specify backup storage settings.
9. Specify advanced backup settings.
10. Specify secondary backup target.
11. Specify guest processing settings.
12. Specify the backup schedule.
13. Review backup policy settings.

Before You Begin

Before you create a Veeam Agent backup policy 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 policy.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the policy must be configured in advance.
- Protection groups that you want to add to the job must be of the **Computer with pre-installed agents** type. To learn more, see Protection Group Types.

Veeam Agent backup policies have the following limitations:

- 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 policy 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 policy configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will be updated on the Veeam Agent computer at the next start of the backup session. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

  Keep in mind, that you can immediately update settings of the backup policy from the Veeam Agent computer. To learn more, see Deploying Veeam Agent for Unix.

Step 1. Launch New Agent Backup Job Wizard

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

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

Launching Backup Job Wizard

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

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

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup policy, do one 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 policy and select **Add to backup job** > **Unix** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup policy and click **Add to Backup** > **Unix** > **New job** on the ribbon.

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

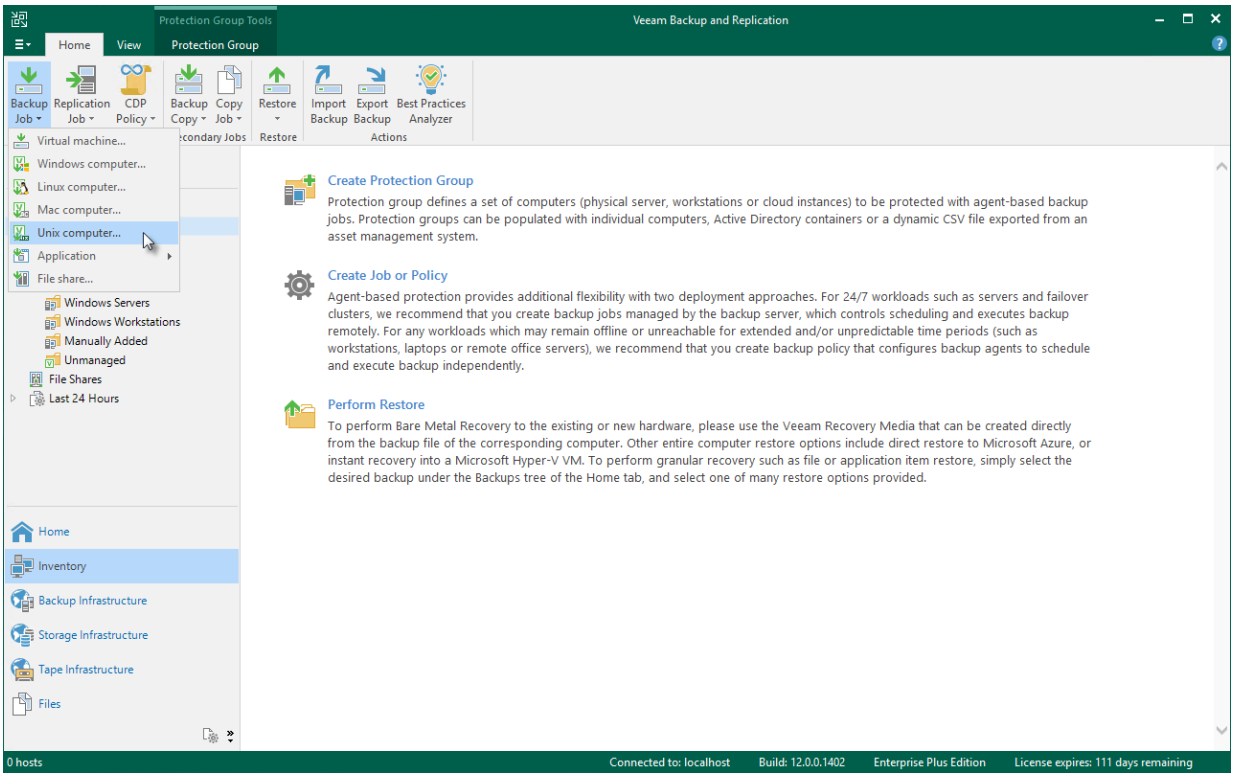
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup policy, 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 policy. In the working area, select one or more computers that you want to add to the policy, 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 policy. In the working area, select one or more computers that you want to add to the policy 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 policy. You can add other computers and (or) protection groups to the policy later on, when you pass through the wizard steps.

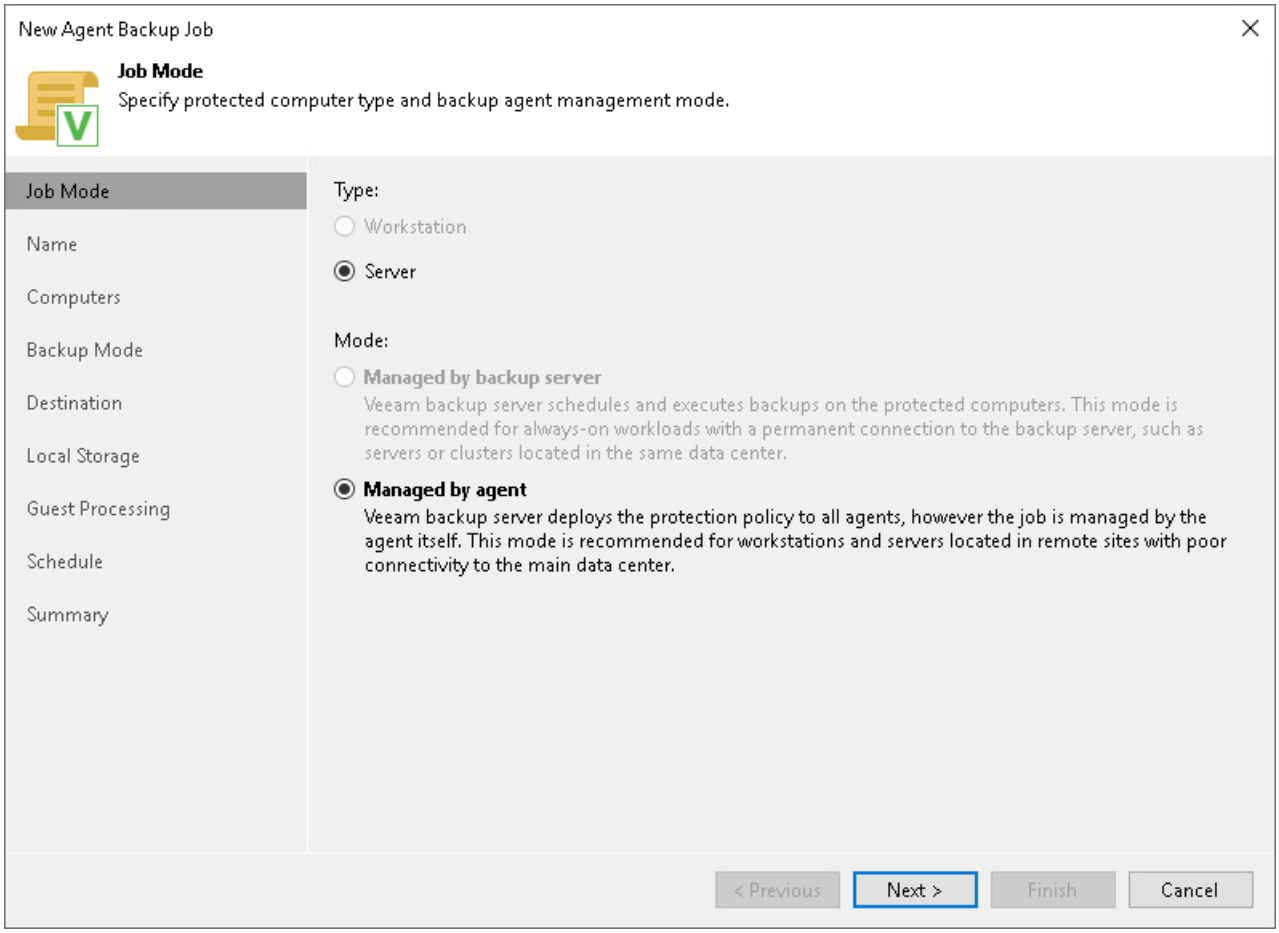
> **TIP**
>
> Consider the following:
>
> - You can press and hold **[CTRL]** to select multiple computers at once.
> - You can add an individual computer or protection group to a Veeam Agent backup policy that is already configured in Veeam Backup & Replication. To learn more, see Adding Computers to Backup Job and Adding Protection Group to Backup Job.



Step 2. Select Job Mode

At the **Job Mode** step of the wizard, click **Next**.

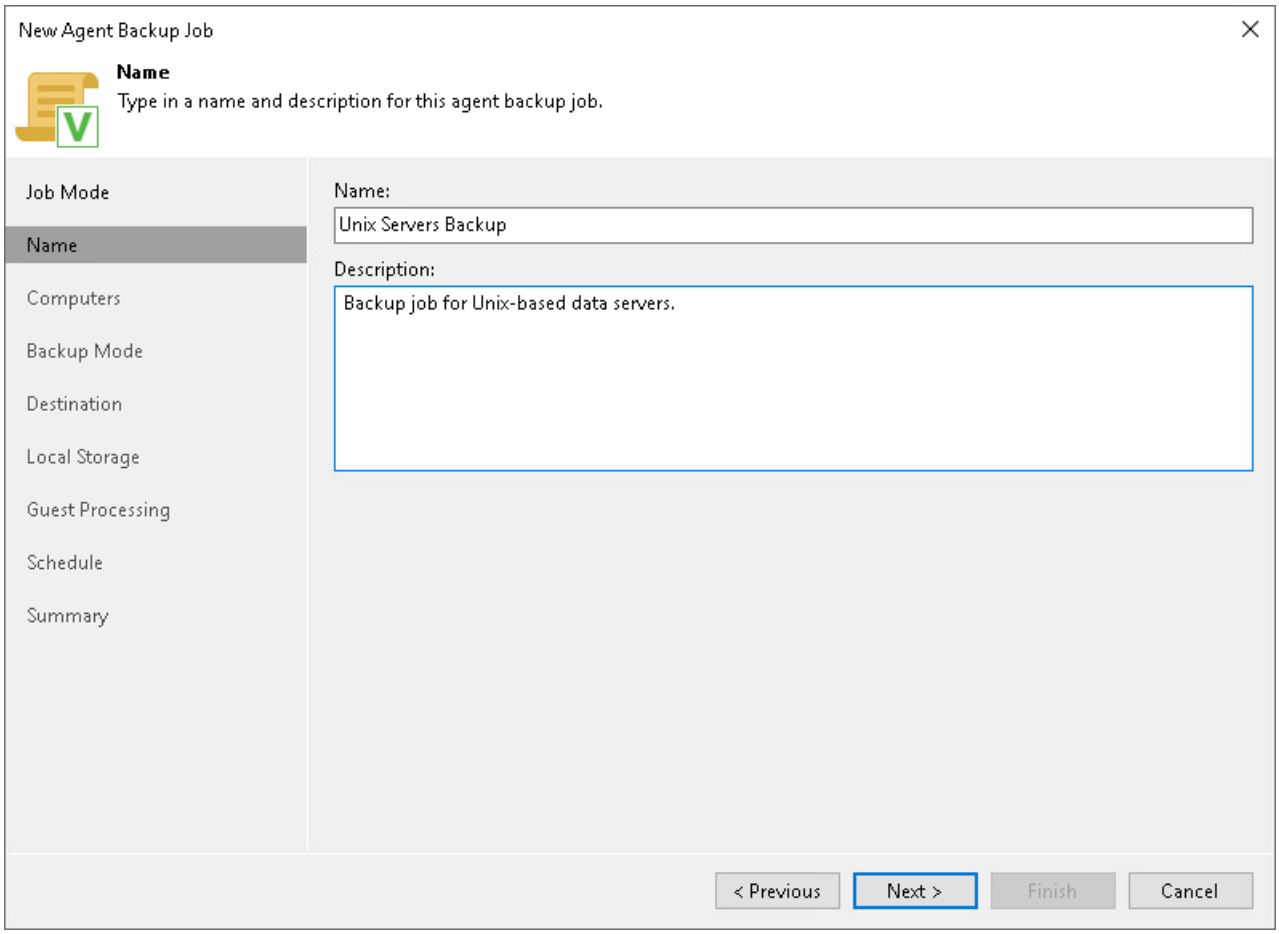
You do not need to select the job type and mode. Unix computers can be added only as servers and only to Veeam Agent backup jobs managed by Veeam Agent.



Step 3. Specify Policy Name and Description

At the **Name** step of the wizard, specify a name and description for the backup policy.

1. In the **Name** field, enter a name for the backup policy.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the policy, date and time when the policy 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 policy one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup policy is created, Veeam Backup & Replication will automatically update the policy settings to include the added computer.

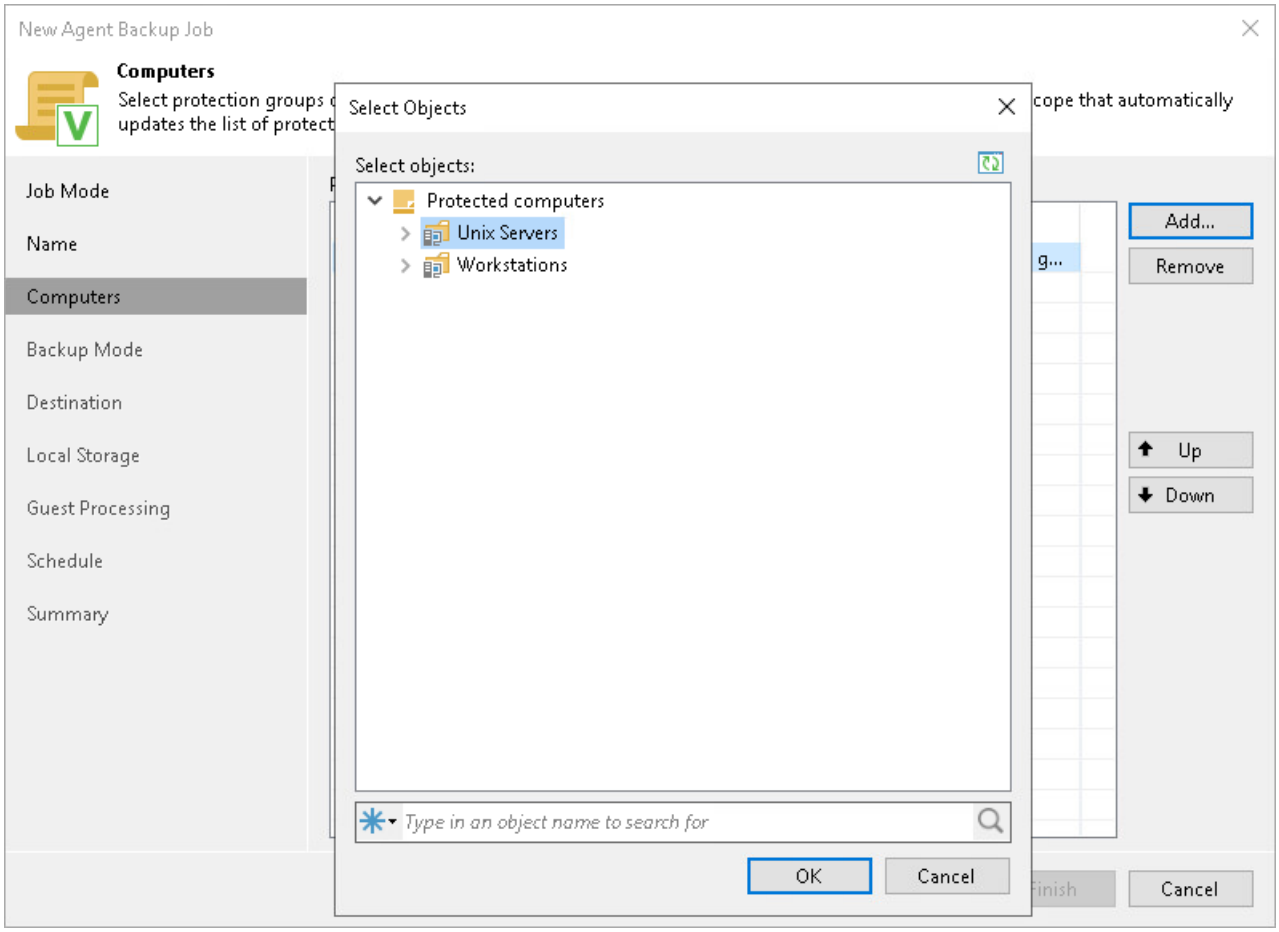
> **NOTE**
>
> If you used the **Add to backup job** > **Unix** > **New job** option to launch the New Agent Backup Job wizard, the **Protected computers** list will already contain computers that you have selected to add to the policy. You can remove some computers from the policy or add new computers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

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

1. Click **Add**.
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]**.



Step 5. Select Backup Mode

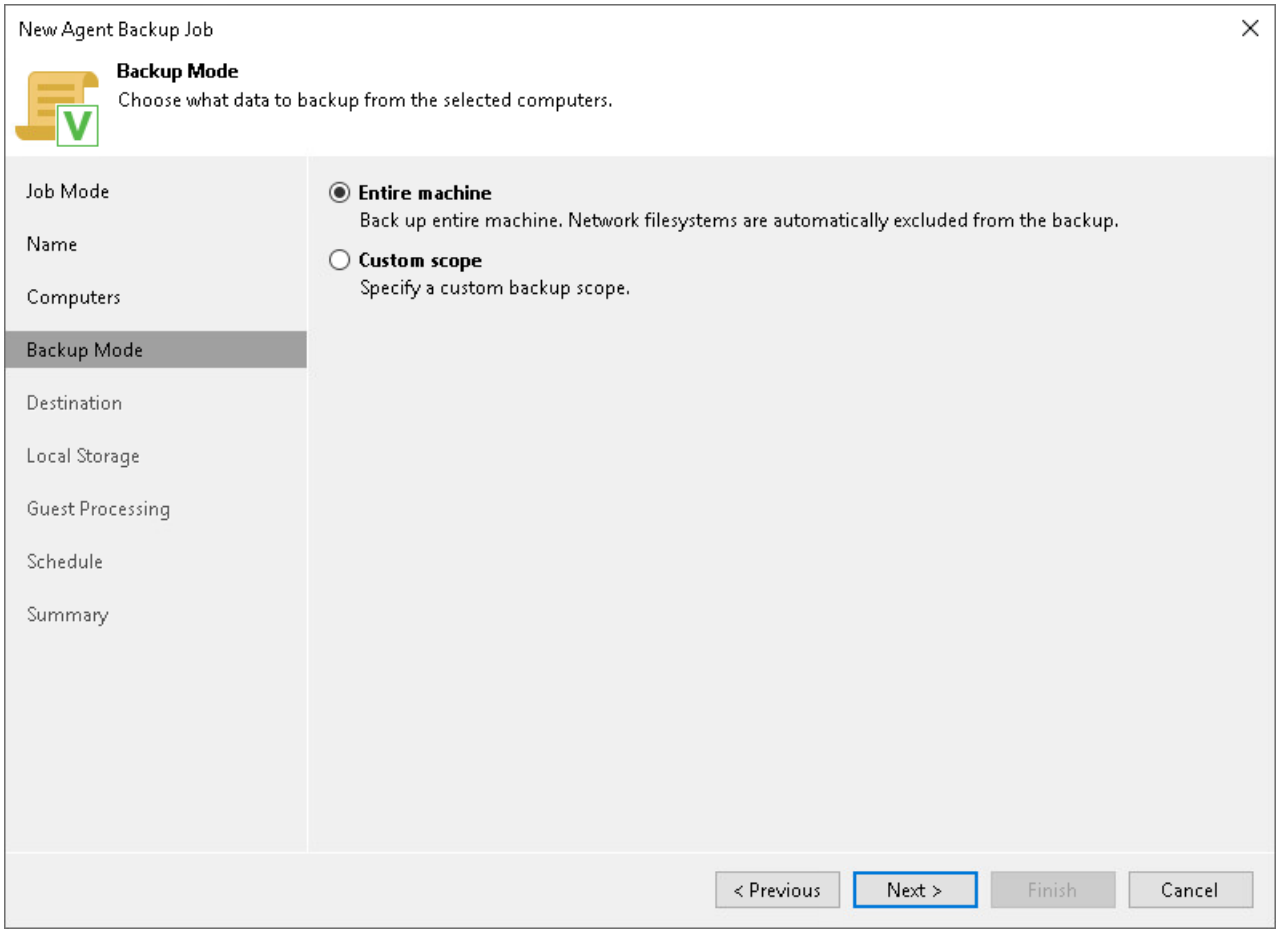
At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup. You can select one of the following options:

- **Entire machine** — select this option if you want to create a backup of all files and directories available on the protected Unix computer.

  Mind that in the Entire machine mode, Veeam Agent excludes network shared folders from the backup scope. To back up network shared folders, use the Custom scope mode.

- **Custom scope** — 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.

  > **TIP**
  >
  > If you plan to back up a network shared folder, you must select the **Custom scope** option and add this network shared folder as an individual object to the backup scope at the **Objects** step of the wizard.



Step 6. Specify Backup Scope Settings

The **Objects** step of the wizard is available if you have chosen the **Custom scope** mode at the Backup Mode step of the wizard.

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 policy. If a specified directory does not exist on one or more computers in the policy, the policy will skip such directory on those computers and back up existing ones.

To specify directories to back up:

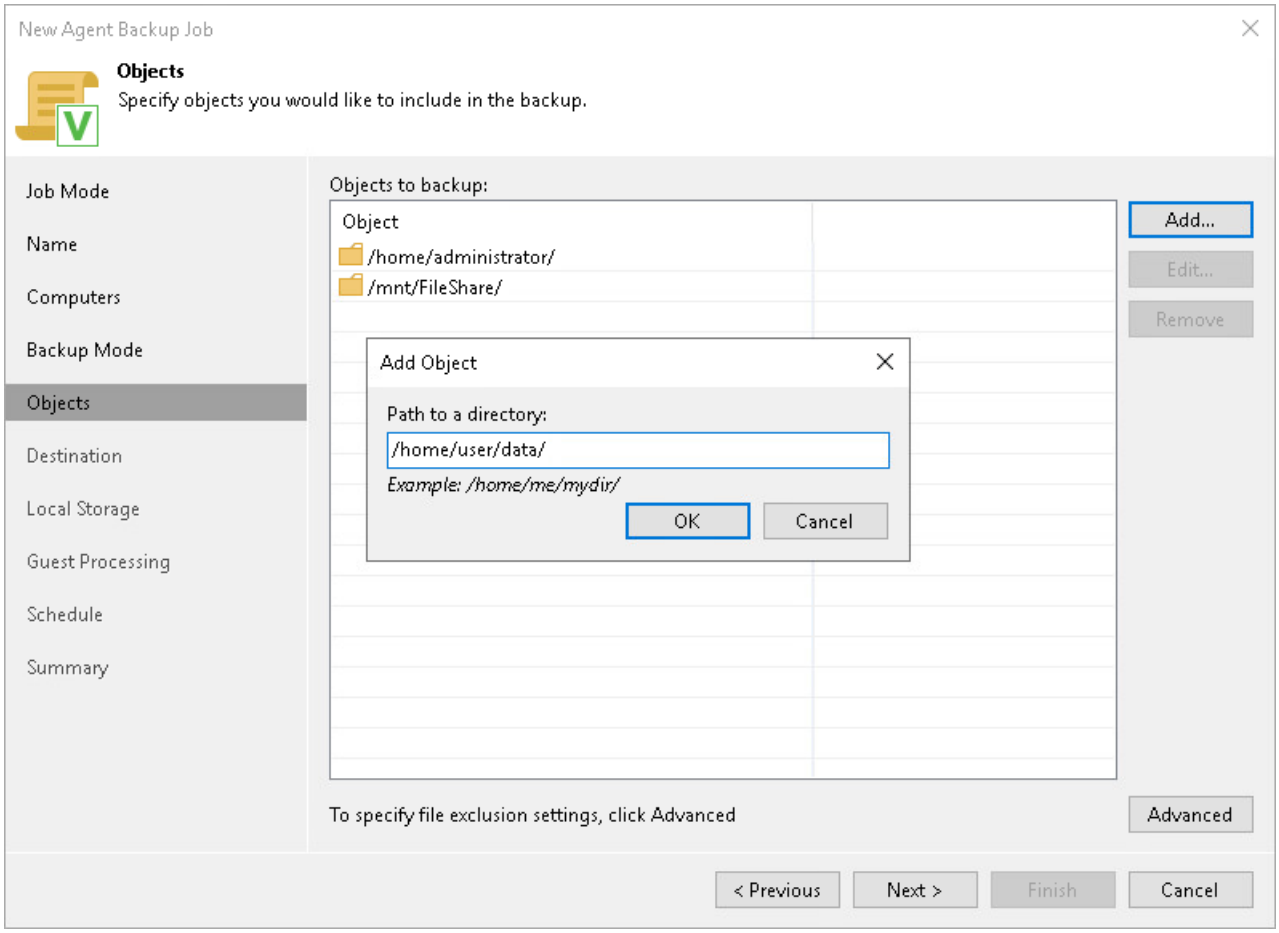
1. In the **Choose directories to backup** field, click **Add**.
2. In the **Add Object** window, type the path to a directory that you want to back up, for example, `/home/user01`, and click **OK**.
3. Repeat steps 1–2 for all directories that you want to back up.

TIP

If you want to back up the root directory and specify `/` in the **Path to a directory** field, Veeam Agent does not automatically include remote mount points in the backup scope. To include remote mount points, you need to specify paths to these mount points manually.

For example, you have a file system mounted to the `/Library/Media` directory. If you add `/` as an object to the backup scope, Veeam Agent will not back up the mounted file system. To back up the root directory and the mounted file system, add the following objects to the backup scope:

- `/`
- `/Library/Media`



Configuring Filters

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

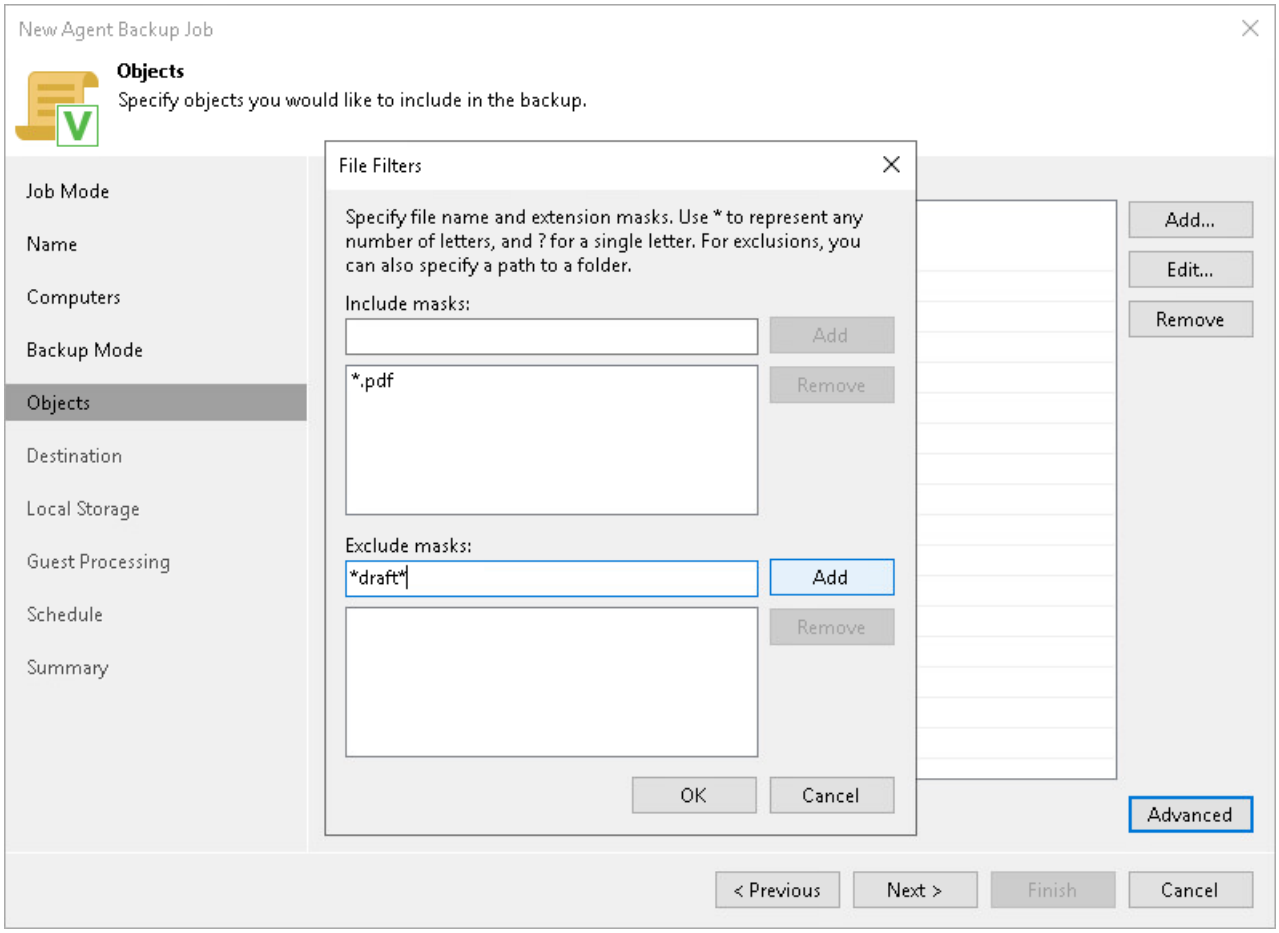
To configure a filter:

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 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 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 will include in the backup all files of the PDF format that do not contain *draft* in their names.



Step 7. Select Backup Destination

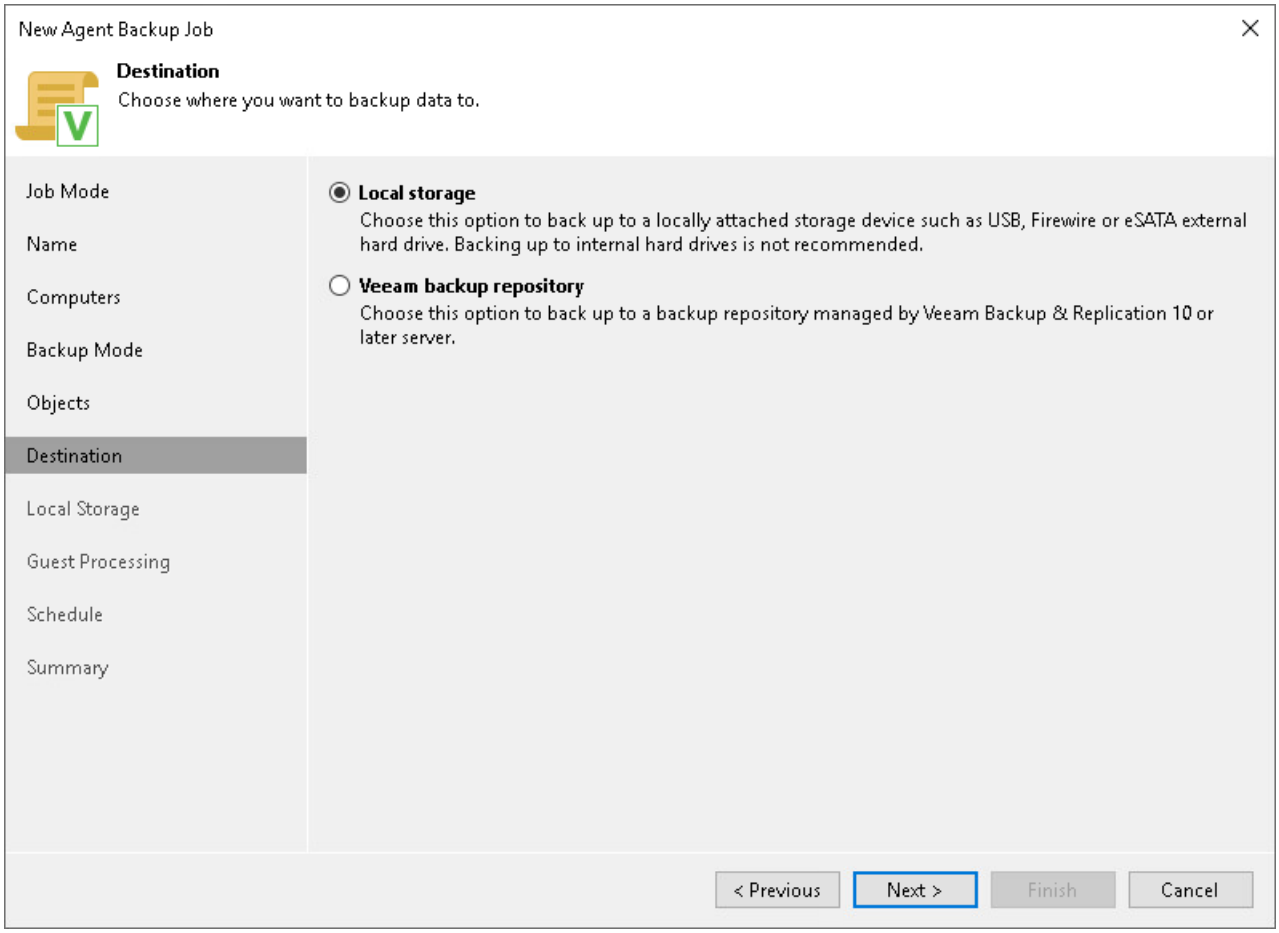
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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.

- **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.



Step 8. Specify Backup Storage Settings

Specify backup storage settings for the backup policy 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.
- Veeam backup repository settings — if you have selected the **Veeam backup repository** option at the Destination step of the wizard.

Local Storage Settings

The **Local Storage** step of the wizard is available if you have chosen to save the backup on a local drive of your computer.

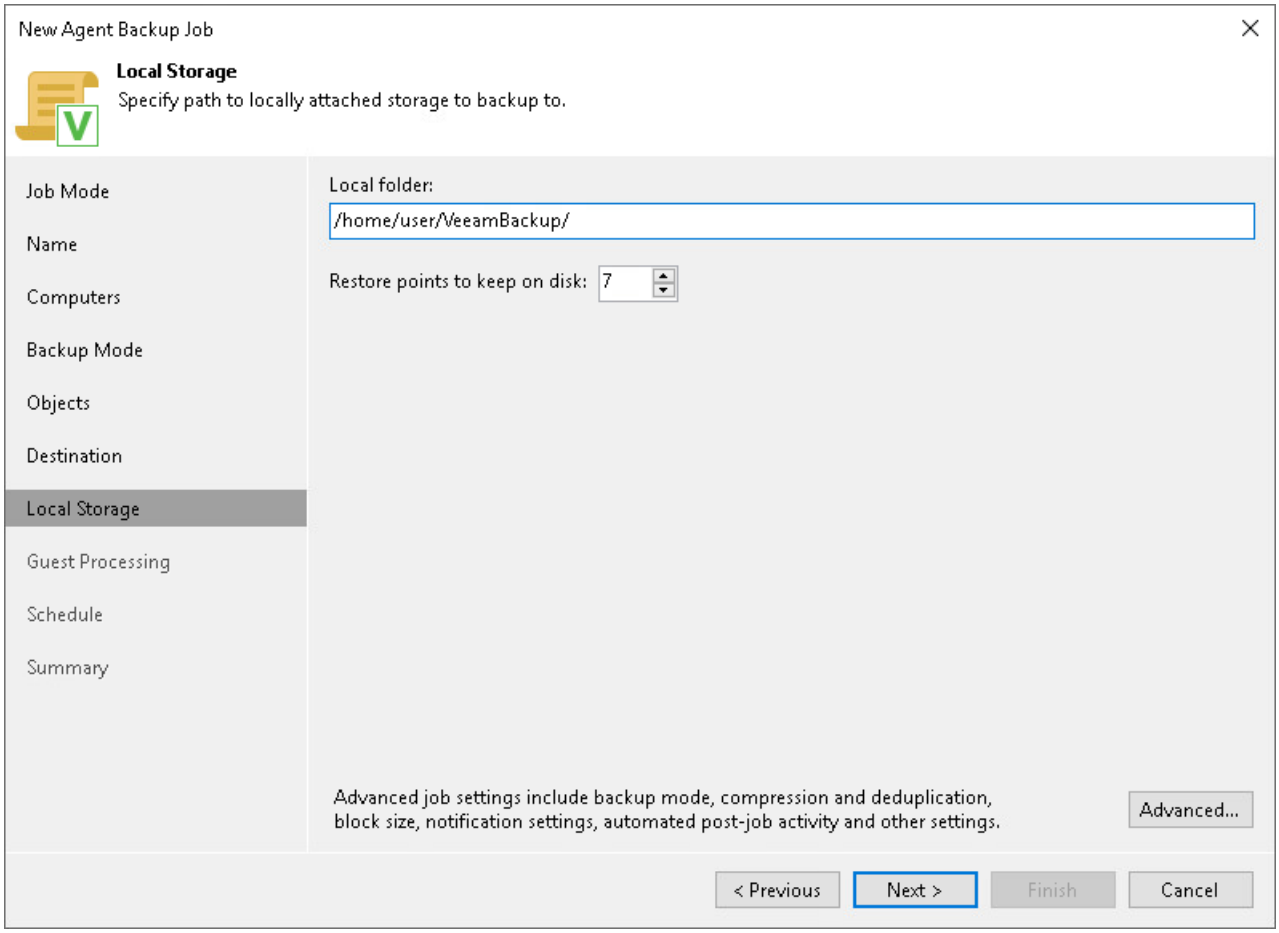
Specify local storage settings:

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 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 policy 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 keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

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



Veeam Backup Repository Settings

If you have chosen to store backup files on a Veeam backup repository, specify settings to connect to the backup repository:

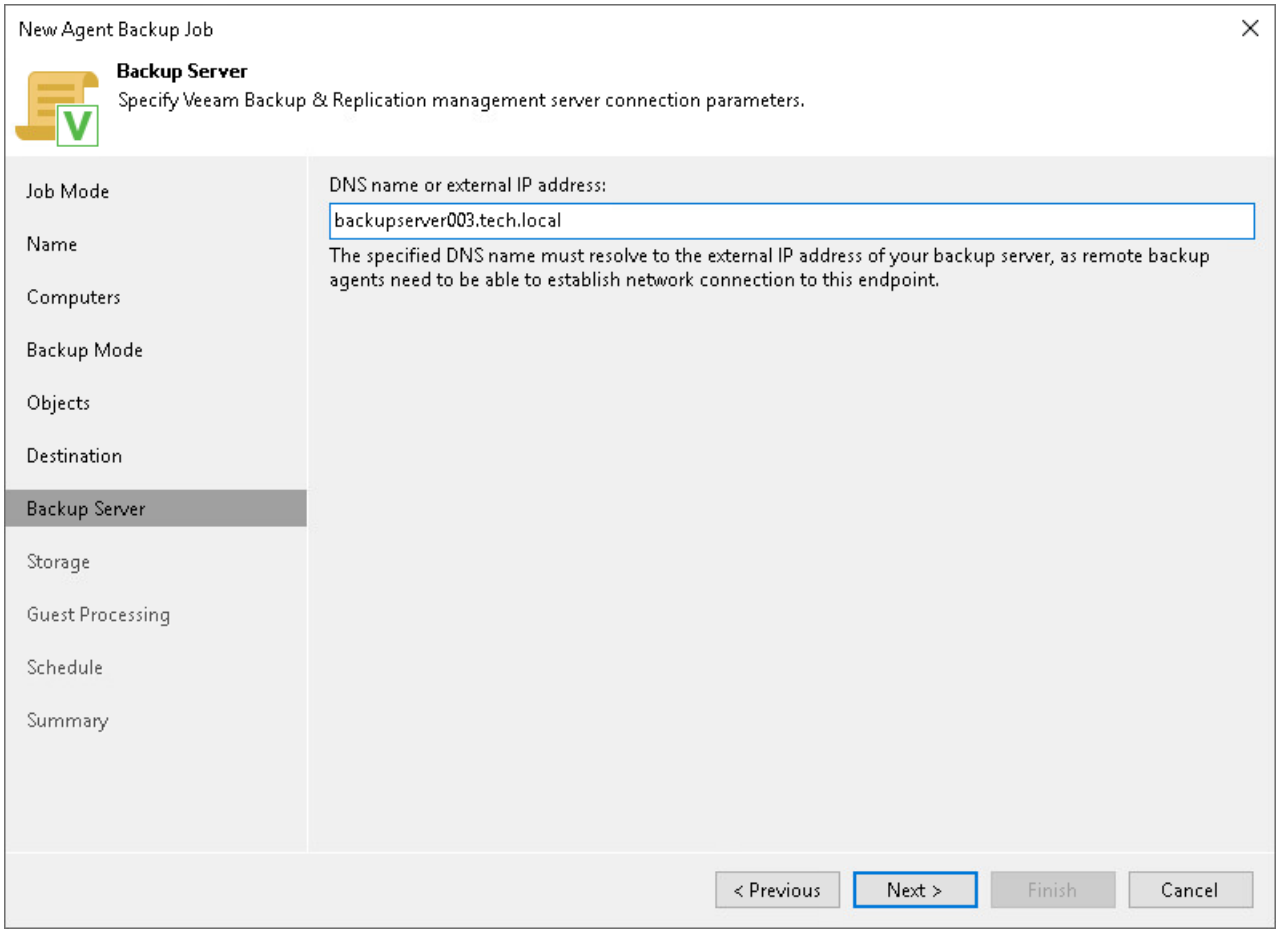
1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Storage step of the wizard, select the Veeam backup repository.

Specifying Backup Server Settings

The **Backup Server** step of the wizard is available if you have 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 policy. 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.



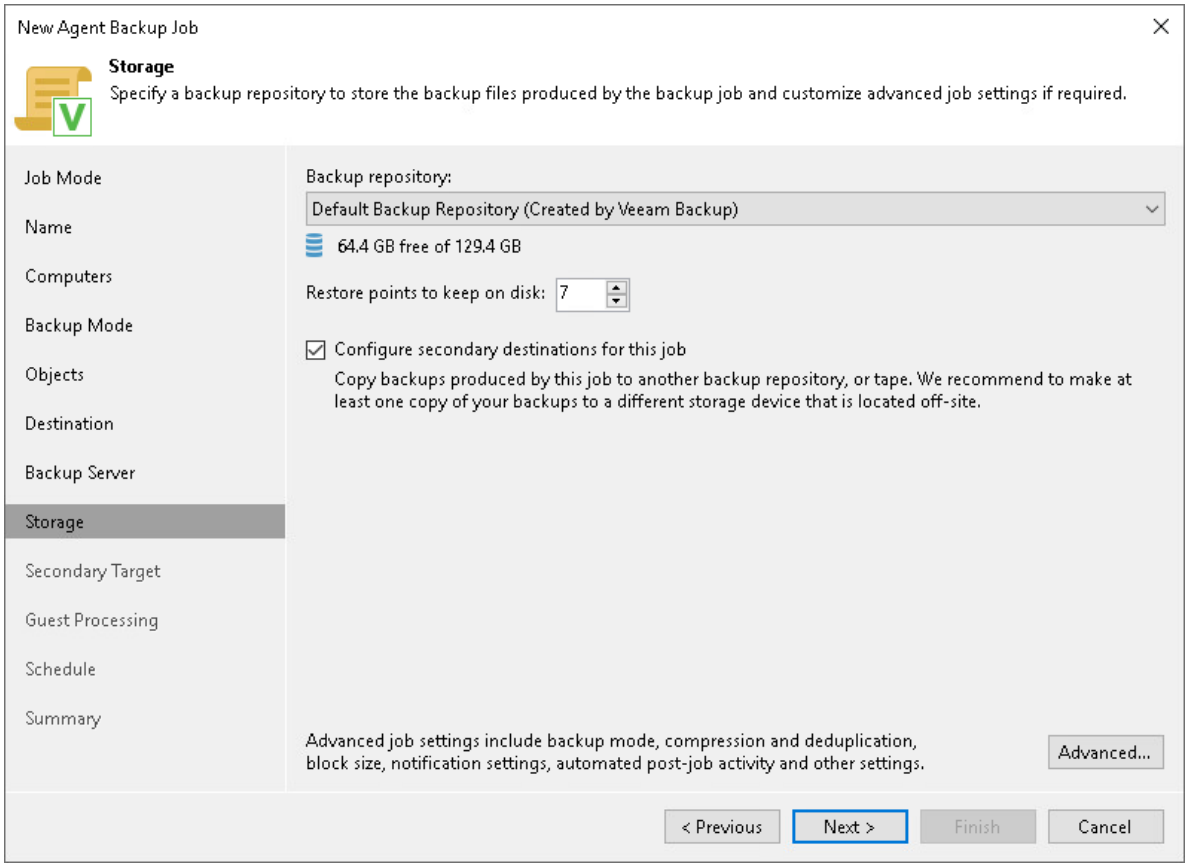
Selecting Backup Repository

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 keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent 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 backup 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 policy 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 policy. To learn more, see Specify Advanced Backup Settings.

> **TIP**
>
> You can map the job to a specific backup stored on the Veeam 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. To learn more, see Backup Job Mapping.



Step 9. Specify Advanced Backup Settings

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

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings

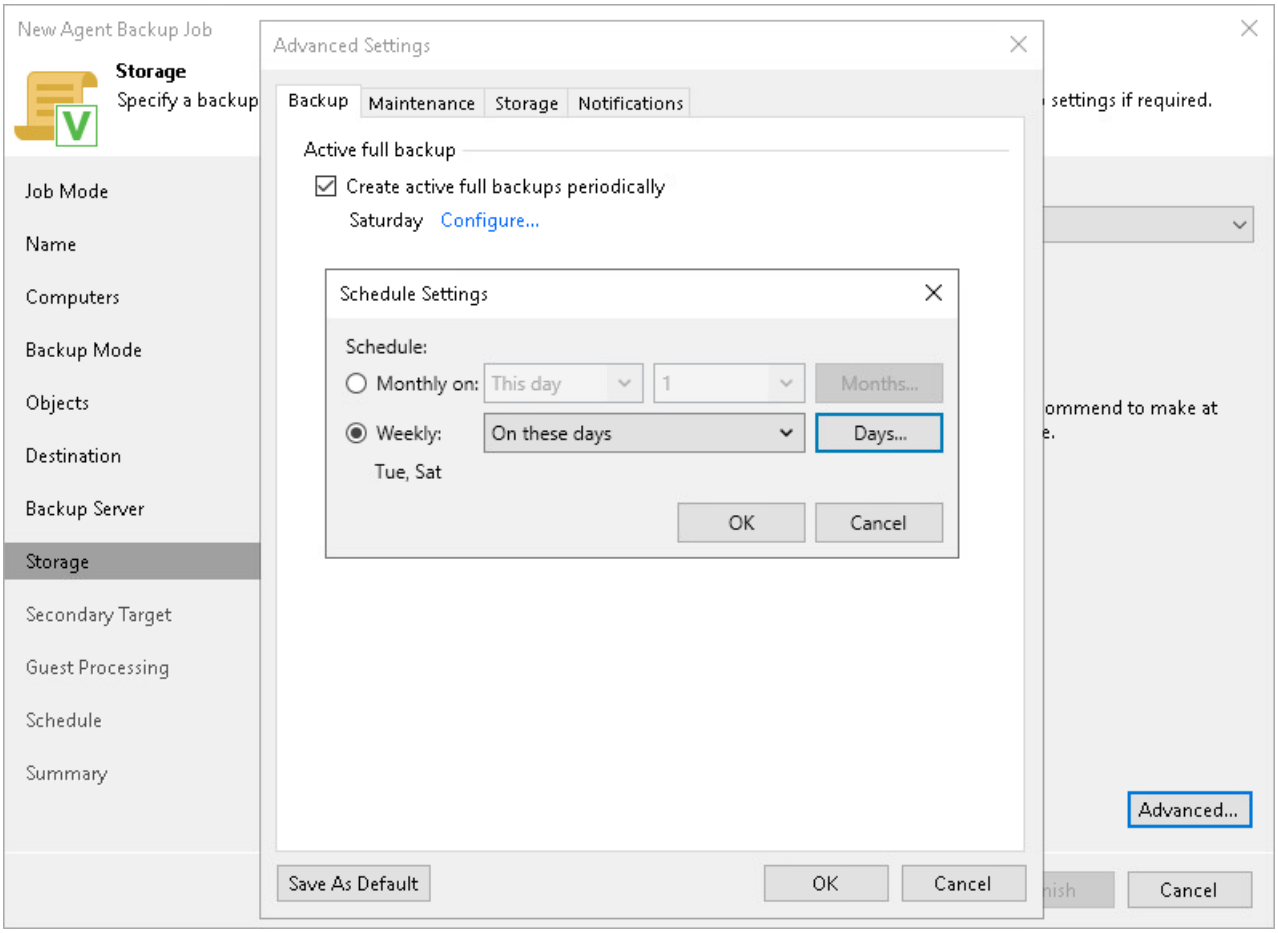
> **TIP**
>
> After you specify necessary settings for the Veeam Agent backup policy, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup policy, Veeam Backup & Replication will automatically apply the default settings to the new policy.

Backup Settings

To specify settings for a backup chain created with the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository.
2. If you want to periodically create active full backups, select the **Create active full backups periodically** check box.
3. Click **Configure**.
4. In the **Schedule Settings** window, use the **Monthly on** or **Weekly** options to define the schedule.

> **NOTE**
>
> Before scheduling periodic full backups, you must make sure that you have enough free space on the target location.



Maintenance Settings

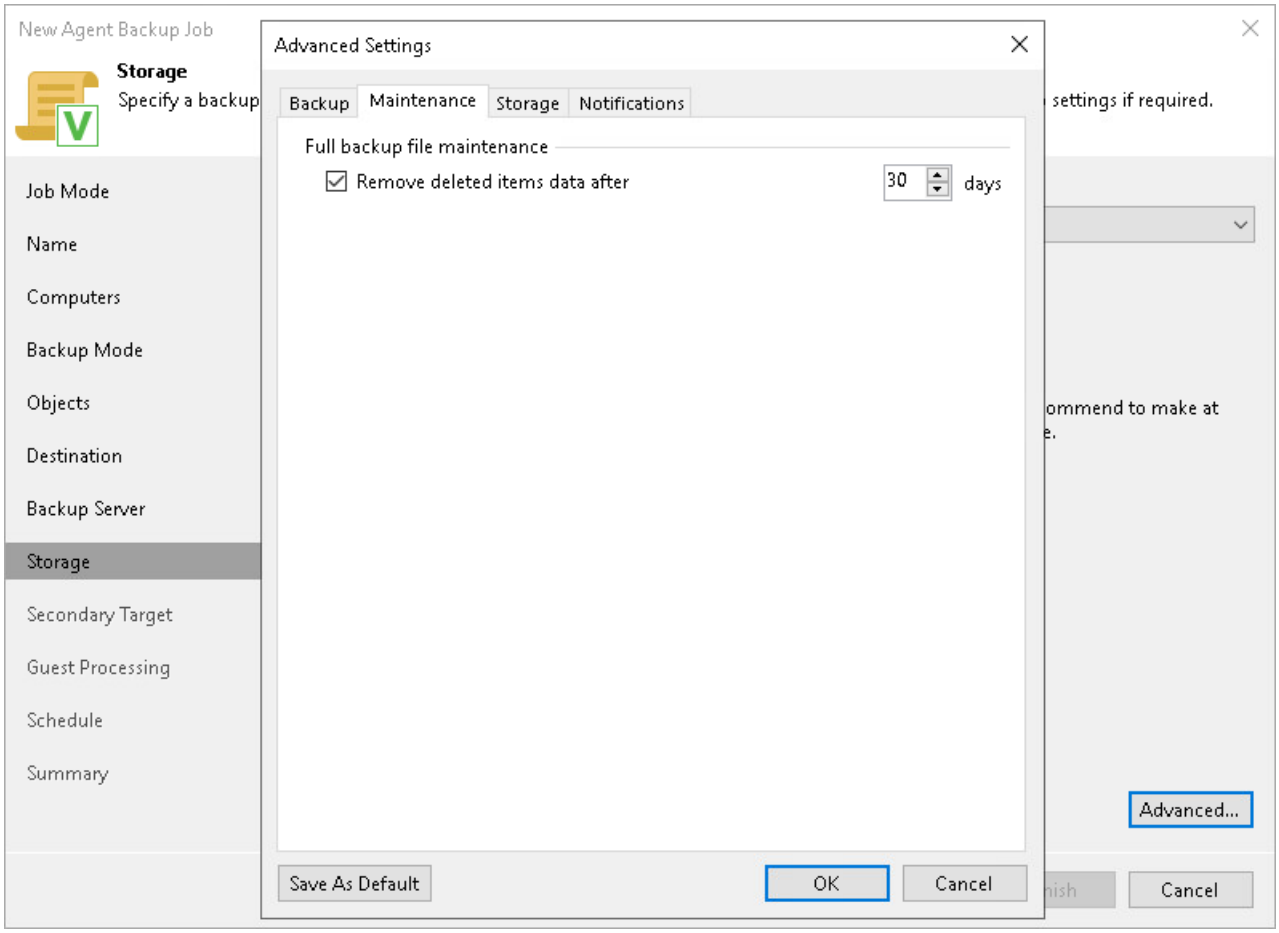
You can specify maintenance settings for a backup policy targeted at a Veeam backup repository. Maintenance operations help make sure that the backup chain remains valid and consistent.

To specify maintenance settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Maintenance** tab.
3. 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 policy in the target location.

   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.

   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. Otherwise, the backup policy may not work as expected and remove data that you still require.



Storage Settings

To specify storage settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository.
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 size of data blocks you plan to use: *4 MB, 1 MB, 512 KB, 256 KB*. Veeam Agent will use data blocks of the chosen 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.

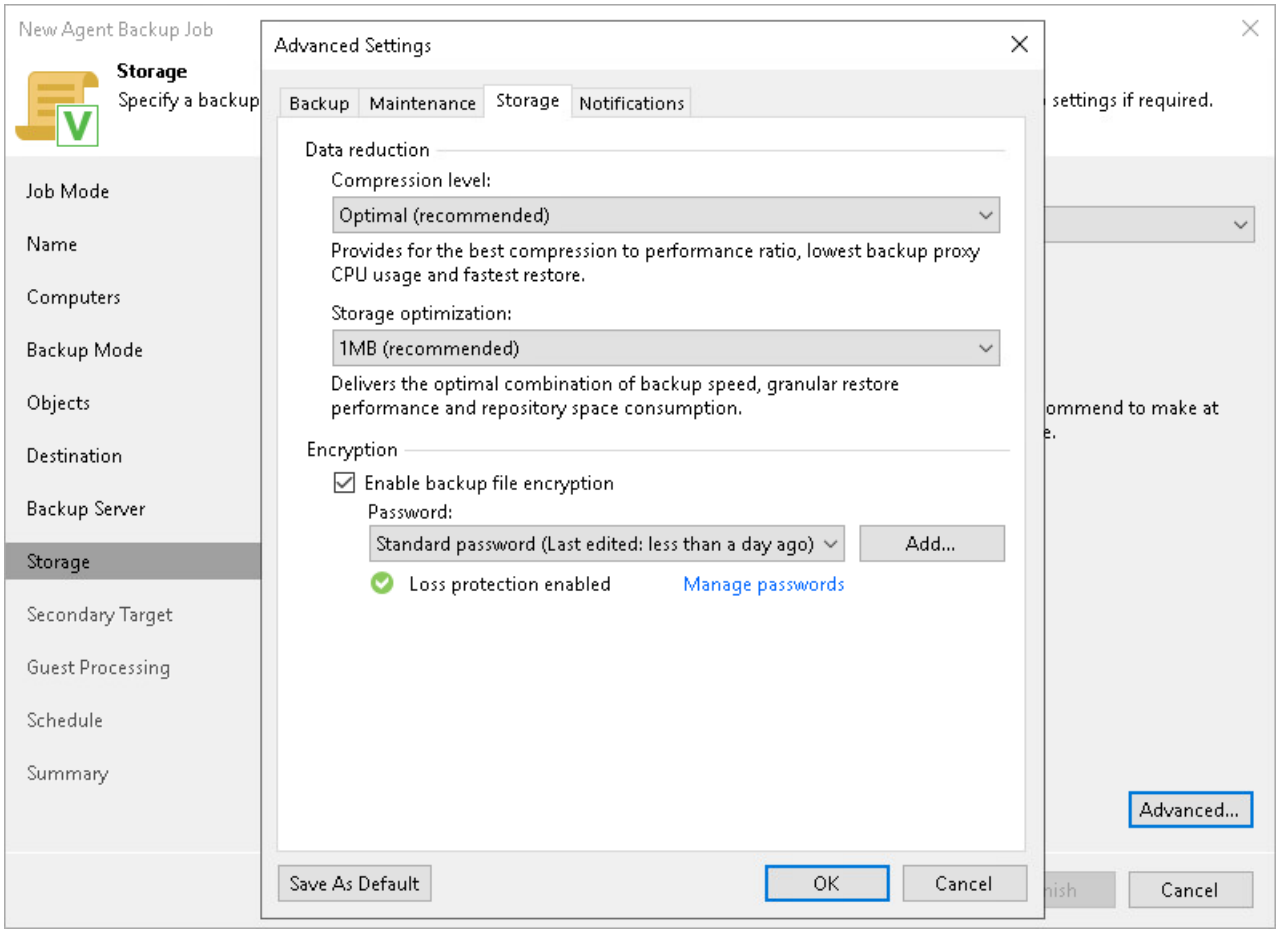
NOTE

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 job or policy, during the next session Veeam Agent 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 or policy, Veeam Agent will encrypt the backup chain starting from the next restore point created with this job.
- 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.


New Agent Backup Job
Storage
Specify a backup
settings if required.
Job Mode
Name
Computers
Backup Mode
Objects
Destination
Backup Server
Storage
Secondary Target
Guest Processing
Schedule
Summary
ommend to make at
e.
Advanced...
Cancel
Advanced Settings
Backup
Maintenance
Storage
Notifications
Data reduction
Compression level:
Optimal (recommended)
Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.
Storage optimization:
1MB (recommended)
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.
Encryption
Enable backup file encryption
Password:
Standard password (Last edited: less than a day ago)
Add...
Loss protection enabled
Manage passwords
Save As Default
OK
Cancel

Notification Settings

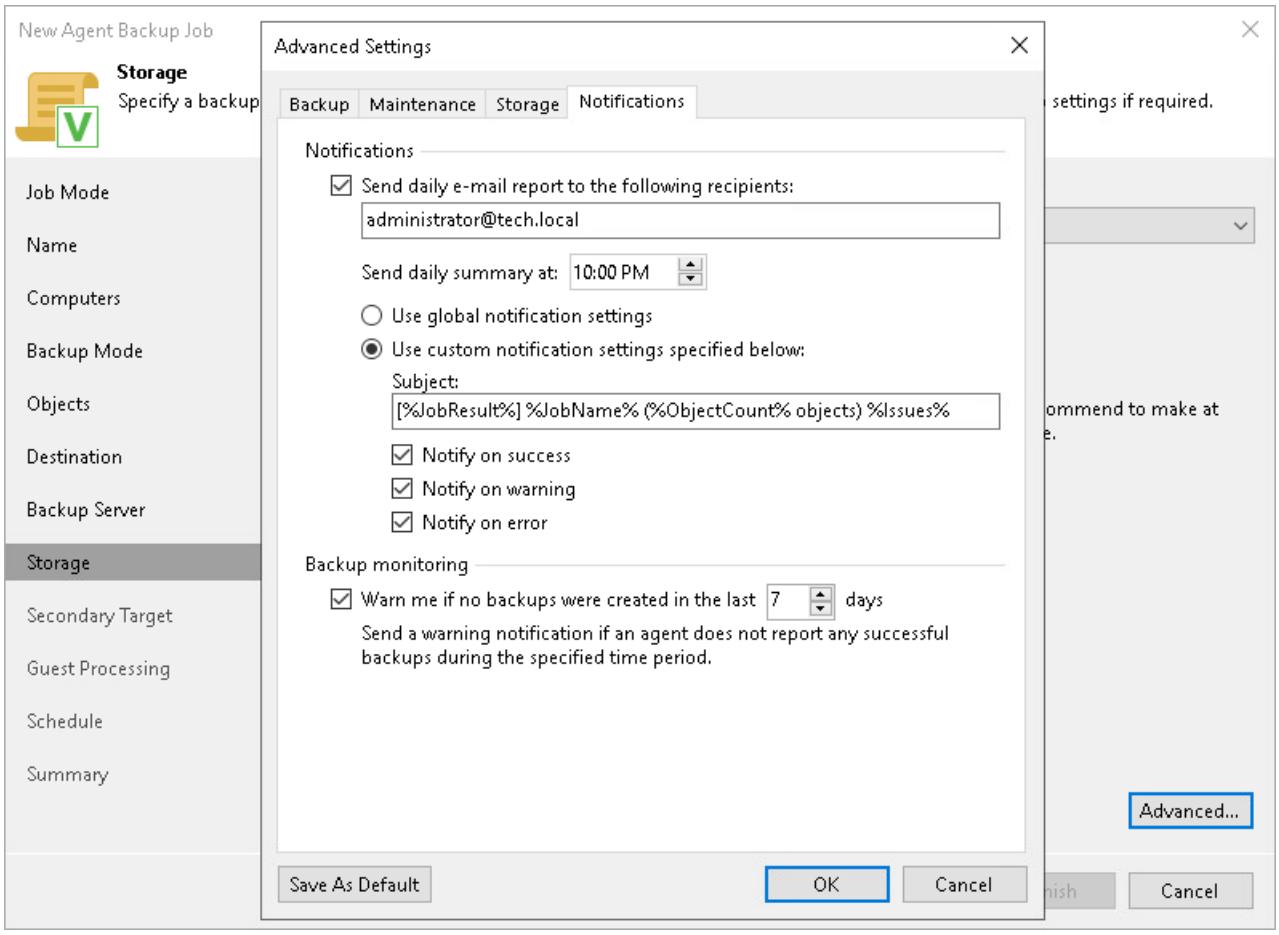
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup policy sessions performed 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:
   - **Local Storage** – if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Storage** – if you have selected to save backup files in a Veeam backup repository.
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 daily summary 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. 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 **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 policy completes successfully, completes with a warning or fails.

5. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



Step 10. Specify Secondary Target

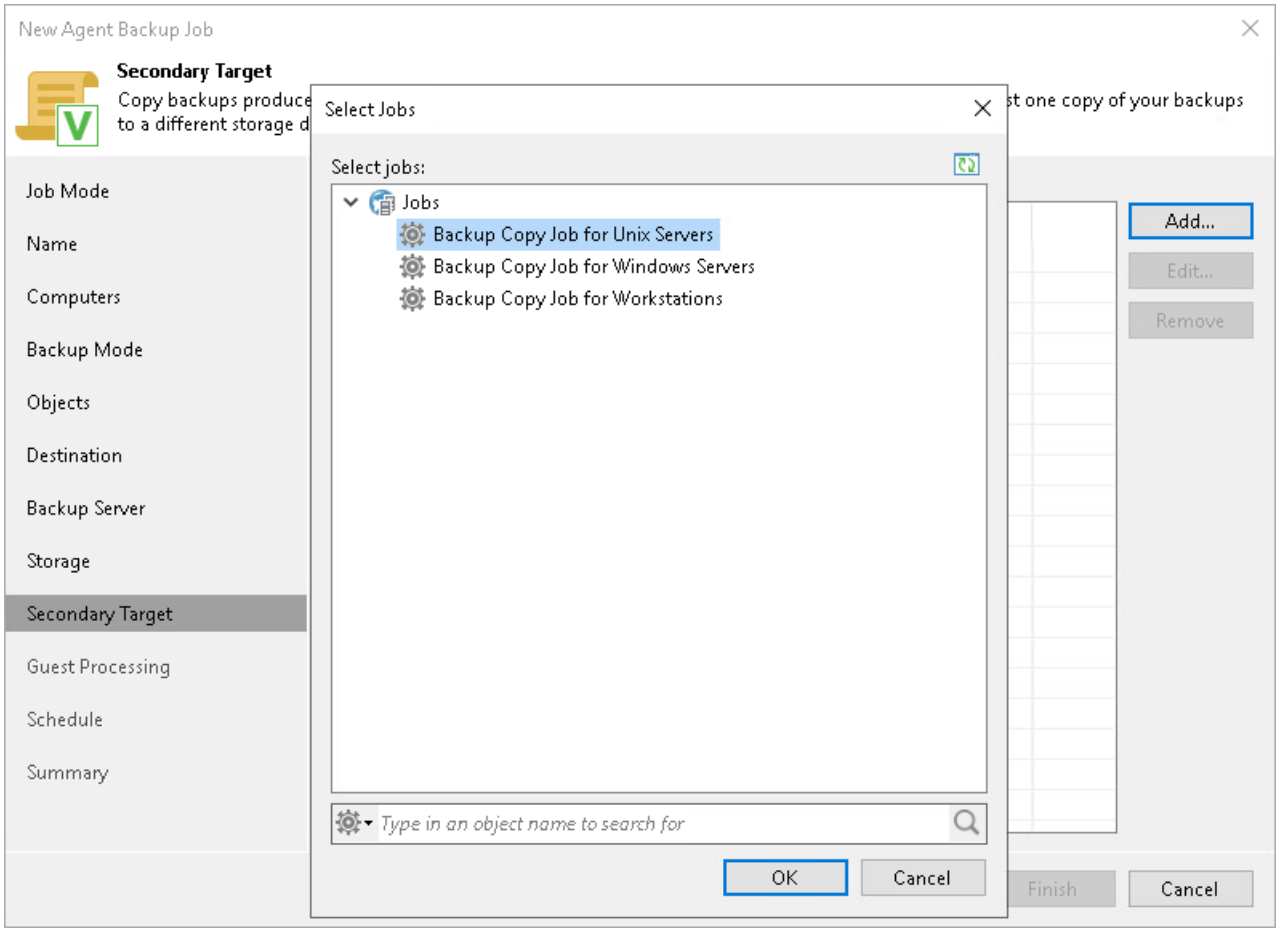
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

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:

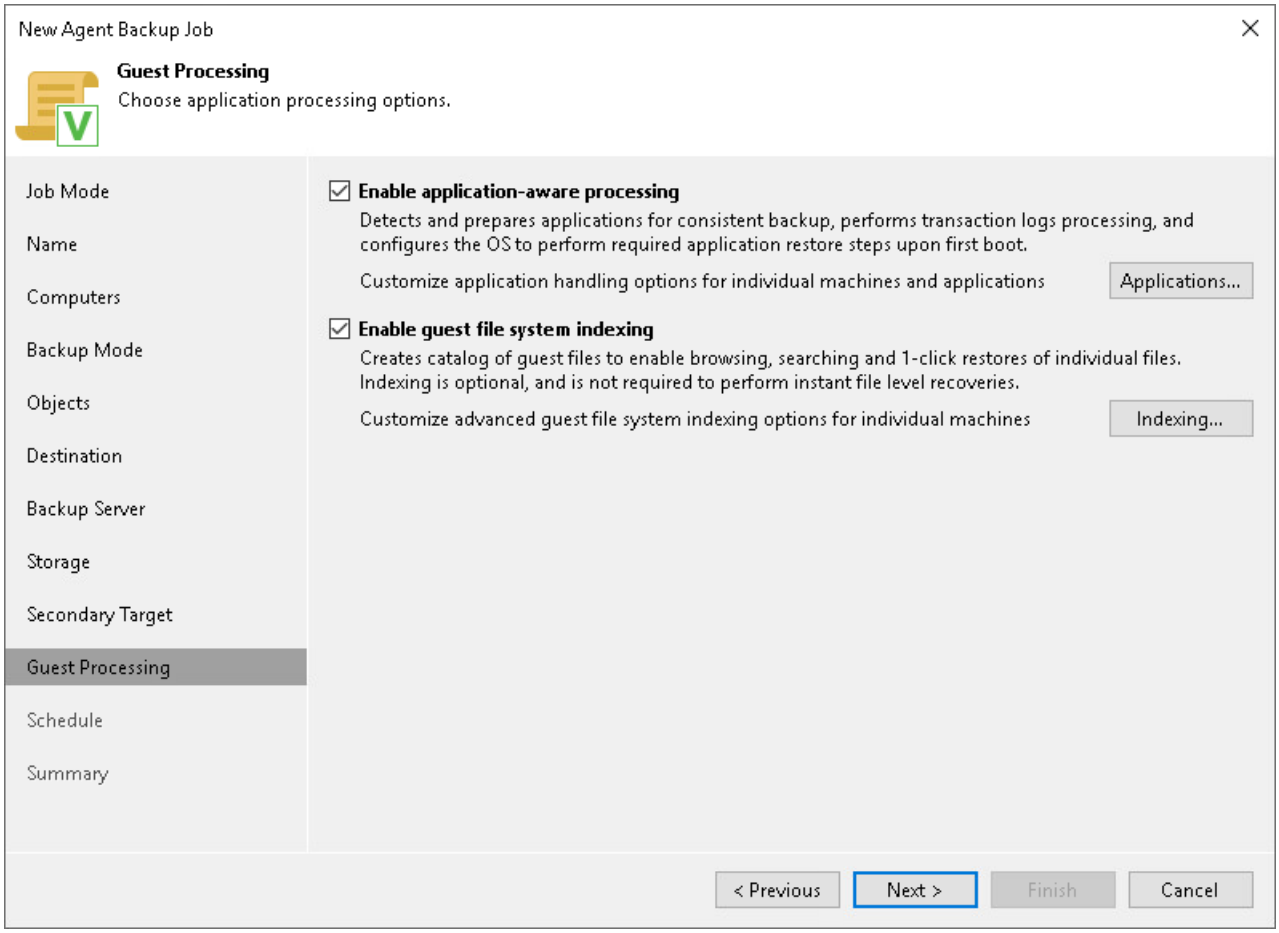
1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the Veeam Agent backup job. You can link several jobs to the backup job, for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom 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 Unix-based computers:

- Use of backup job and snapshot scripts
- File indexing



Backup Job Scripts

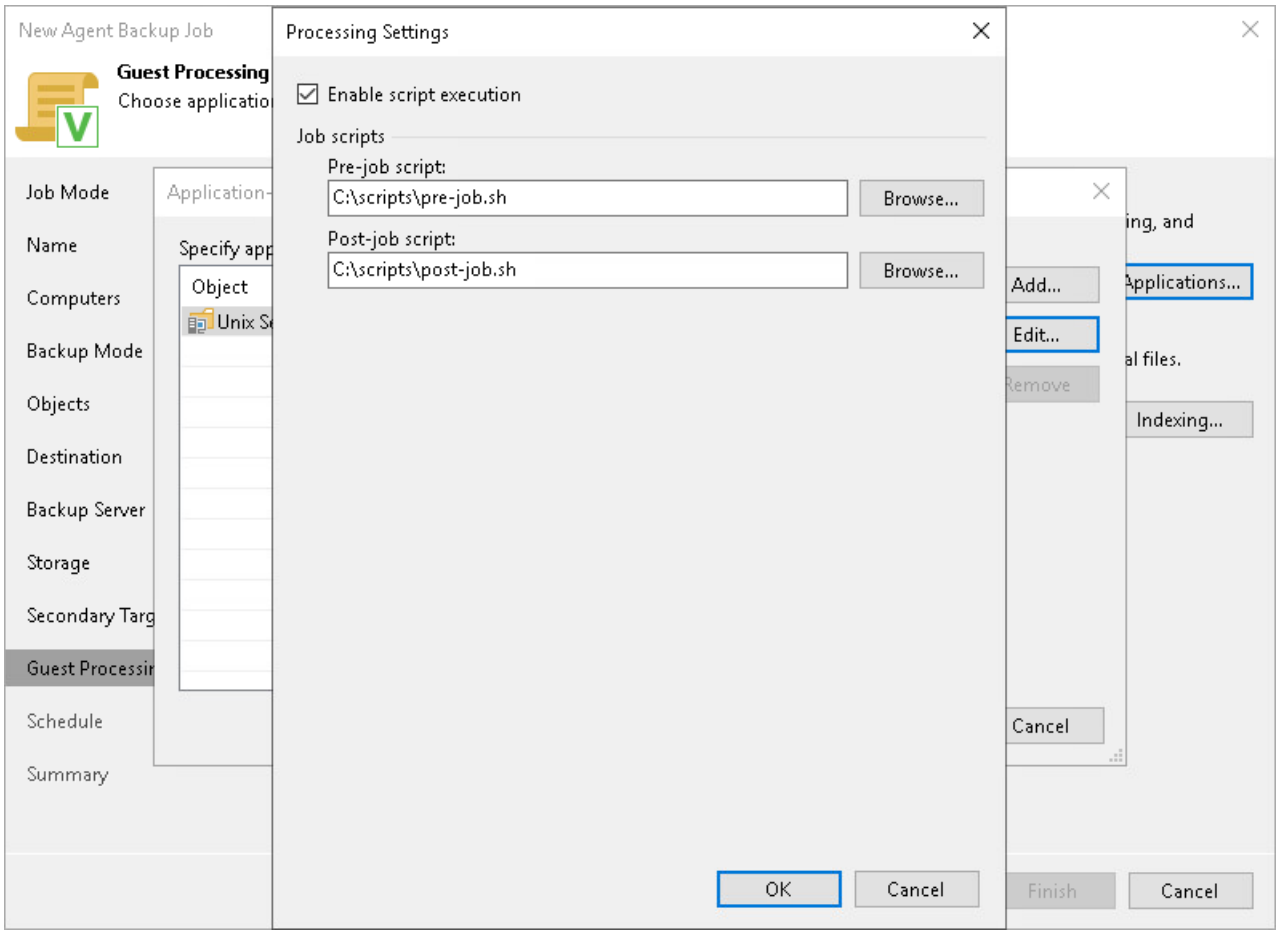
You can specify custom backup job scripts that will be executed within the backup job session on Unix computers. Veeam Agent supports pre-job and post-job scripts that run on the Veeam Agent computer before and after the backup job session. To learn more, see Backup Job Scripts.

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 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.



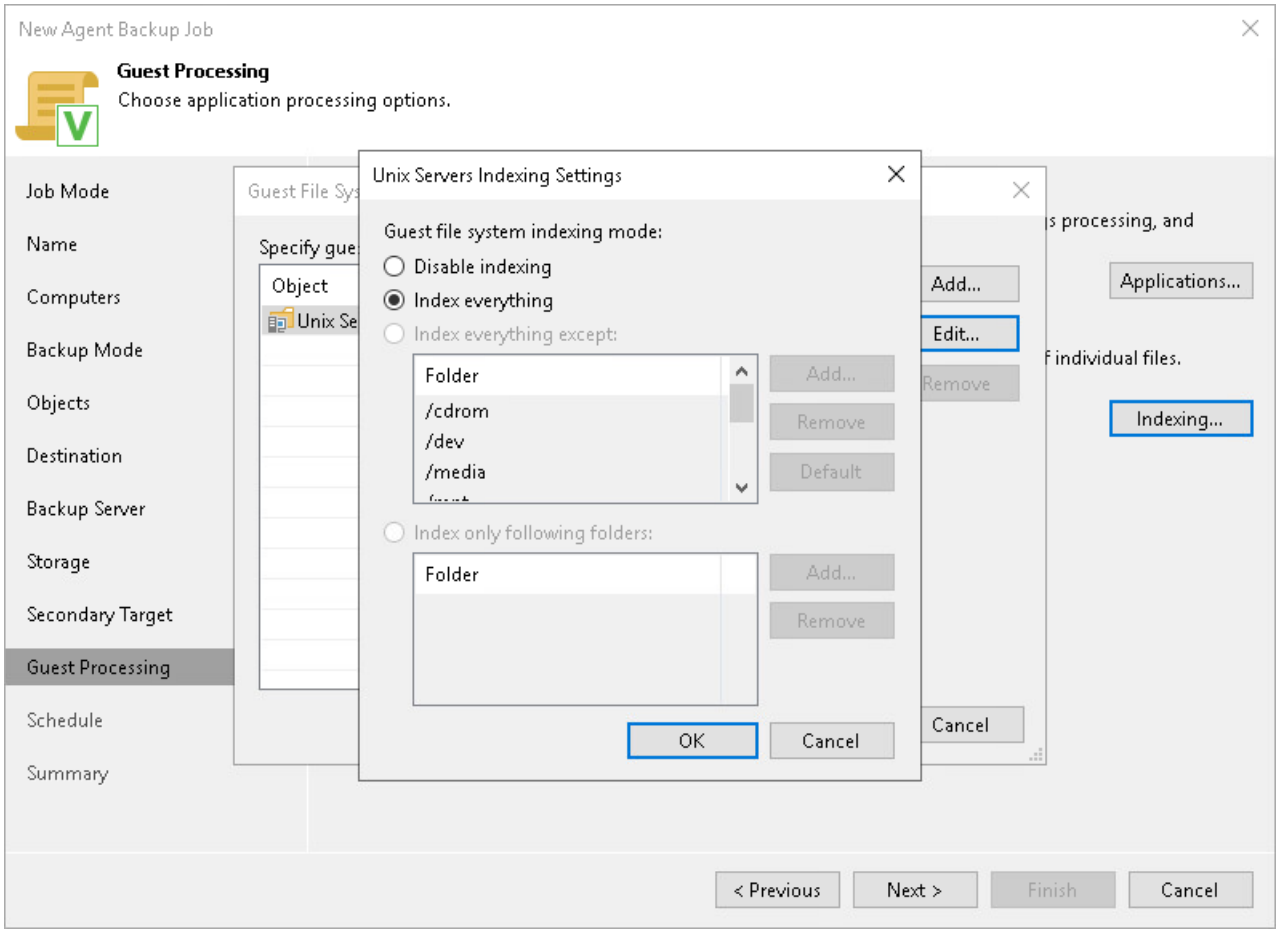
File Indexing

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, select **Index everything** if you want to index all files within the backup scope that you have specified at the [TBD} Unix Source step of the wizard.

> **NOTE**
>
> You cannot specify a custom indexing scope for Unix computers. For a file-level backup job that processes Unix 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.

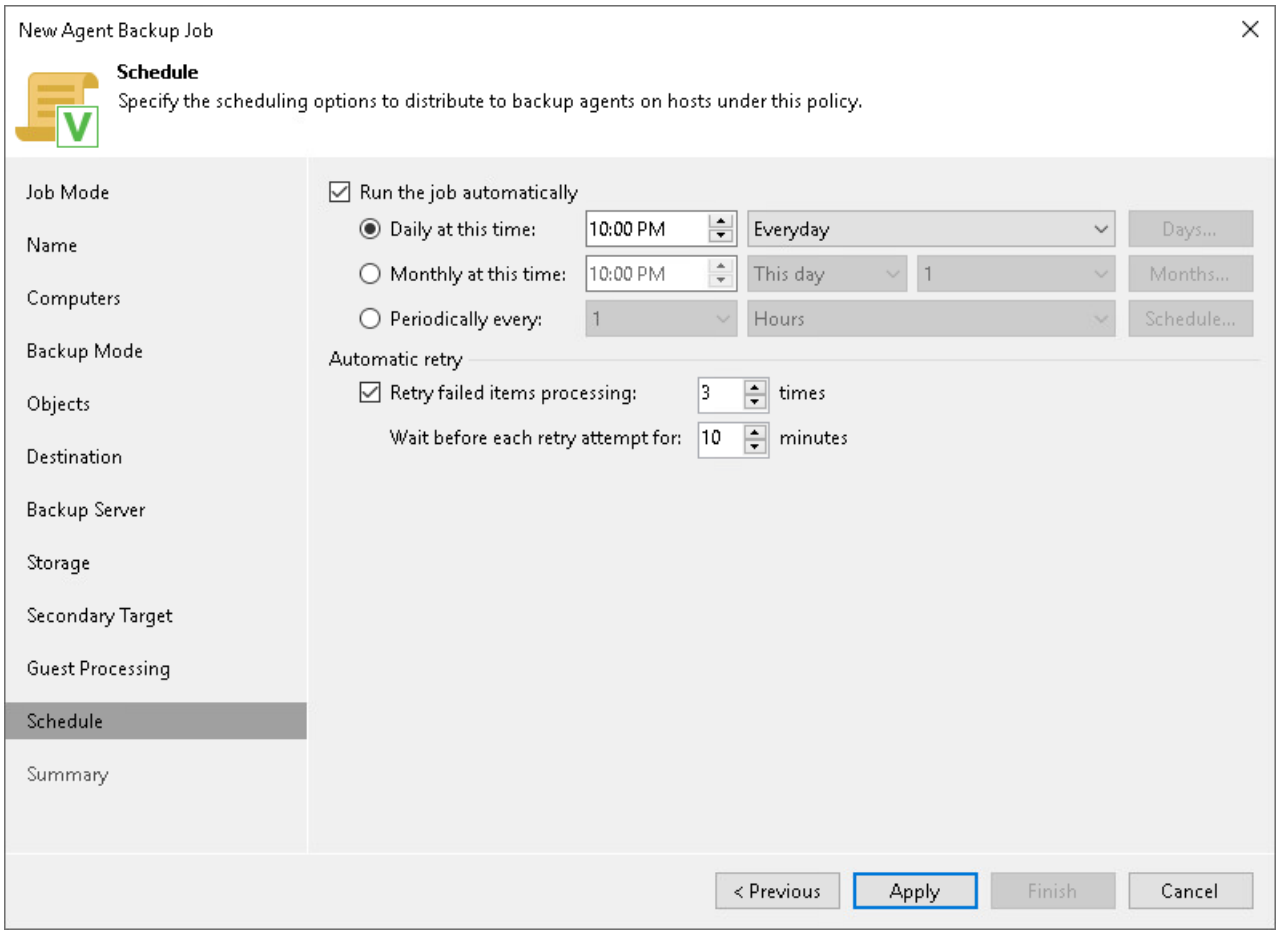
     A repeatedly run job is started by the following rules:

     - 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.

3. In the **Automatic retry** section, define whether Veeam Agent 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 Agent for Unix will retry the job for the defined number of times without any time intervals between the job runs.



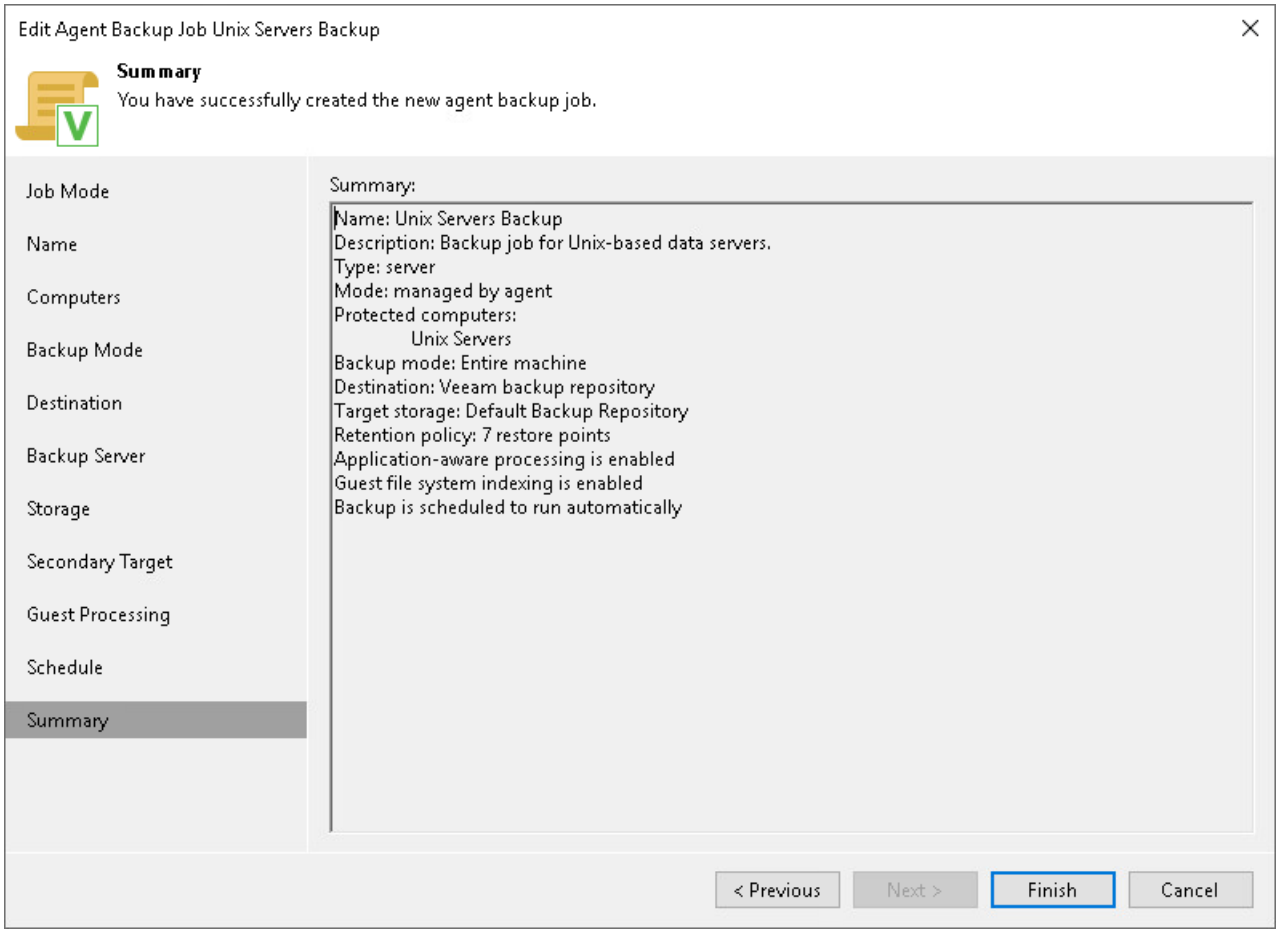
Step 13. Review Backup Job Settings

At the **Summary** step of the wizard, complete the Veeam Agent backup policy configuration process.

1. Review settings of the configured backup policy.
2. Click **Finish** to close the wizard.

Keep in mind that Veeam Backup & Replication does not apply backup policy to Unix computers immediately. Veeam Agents installed on Unix computers connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Unix Configuration.



Creating Policy for Mac Computers

To back up data of a computer protected with Veeam Agent for Mac, you must configure a Veeam Agent backup policy in Veeam Backup & Replication. This backup policy will be applied to Veeam Agent computers to create individual backup jobs. Using these jobs, Veeam Agents will perform backup operations.

Before configuring a backup policy, check prerequisites. Then use the **New Agent Backup Job** wizard to define settings for the backup policy.

1. Launch the New Agent Backup Job wizard.
2. Select the type of protected computers.
3. Specify policy name and description.
4. Select computers to back up.
5. Select backup mode.
6. Specify backup scope.
7. Select backup destination.
8. Specify backup storage settings.
9. Specify advanced backup settings.
10. Specify secondary backup target.
11. Specify the backup schedule.
12. Review backup policy settings.

Before You Begin

Before you create a Veeam Agent backup policy 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 policy.
- The target location where you plan to store backup files must have enough free space.
- Protection groups that you want to add to the policy must be configured in advance.
- Protection groups that you want to add to the job must be of the **Computer with pre-installed agents** type. To learn more, see Protection Group Types.
- [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 policies have the following limitations:

- 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 policy 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 policy configured in Veeam Backup & Replication to a Veeam Agent backup chain created by a standalone Veeam Agent on a backup repository.
- Veeam Backup & Replication does not immediately apply backup policy to computers included in protection groups for pre-installed Veeam Agents. Veeam Agents installed on computers that are included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will be updated on the Veeam Agent computer at the next start of the backup session. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

  Keep in mind, that you can immediately update settings of the backup policy from the Veeam Agent computer. To learn more, see Deploying Veeam Agent for Mac.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup policy for protected computers that run a macOS in one of the following ways:

- Create a new backup policy — 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 policy settings must apply at the Computers step of the wizard.
- Add a protection group to a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected protection group to the backup policy. You will also be able to change the list of Veeam Agent computers to which the backup policy settings must apply at the Computers step of the wizard.
- Add individual computers to a new backup policy — in this case, Veeam Backup & Replication will launch the New Agent Backup Job wizard and add the selected computers to the backup policy. You will also be able to change the list of Veeam Agent computers to which the backup policy 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** > **Mac computer**.
- Open the **Home** view. Select the **Jobs** node and click **Backup Job** > **Mac computer** on the ribbon.
- Open the **Home** view. Right-click the **Jobs** node and select **Backup** > **Mac computer**.

Adding Protection Group to New Backup Job

To add a protection group to a new Veeam Agent backup policy, 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 policy and select **Add to backup job** > **Mac** > **New job**.
- Open the **Inventory** view. In the **Physical Infrastructure** node, select the protection group that you want to add to the backup policy and click **Add to Backup** > **Mac** > **New job** on the ribbon.

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

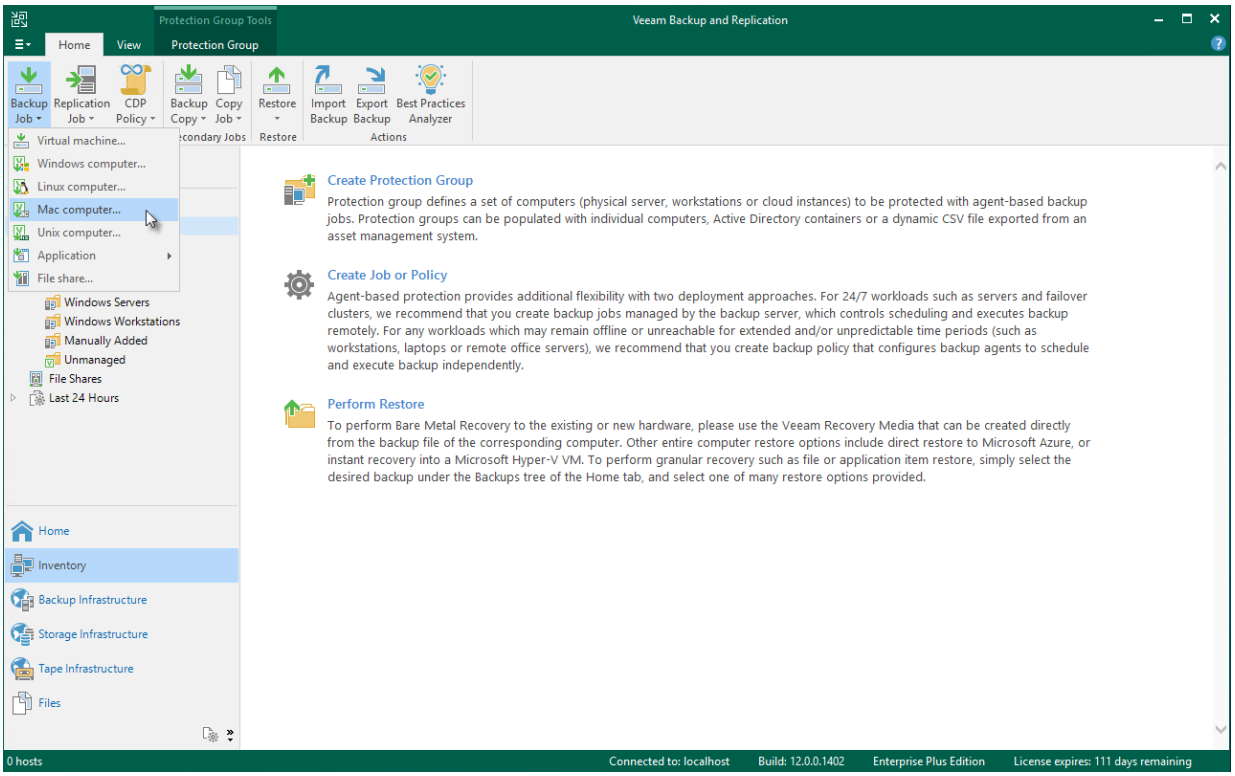
Adding Computers to New Backup Job

To add specific computers to a new Veeam Agent backup policy, 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 policy. In the working area, select one or more computers that you want to add to the policy, 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 policy. In the working area, select one or more computers that you want to add to the policy 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 policy. You can add other computers and (or) protection groups to the policy 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 policy 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, 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 policy. You can select one of the following computer types:

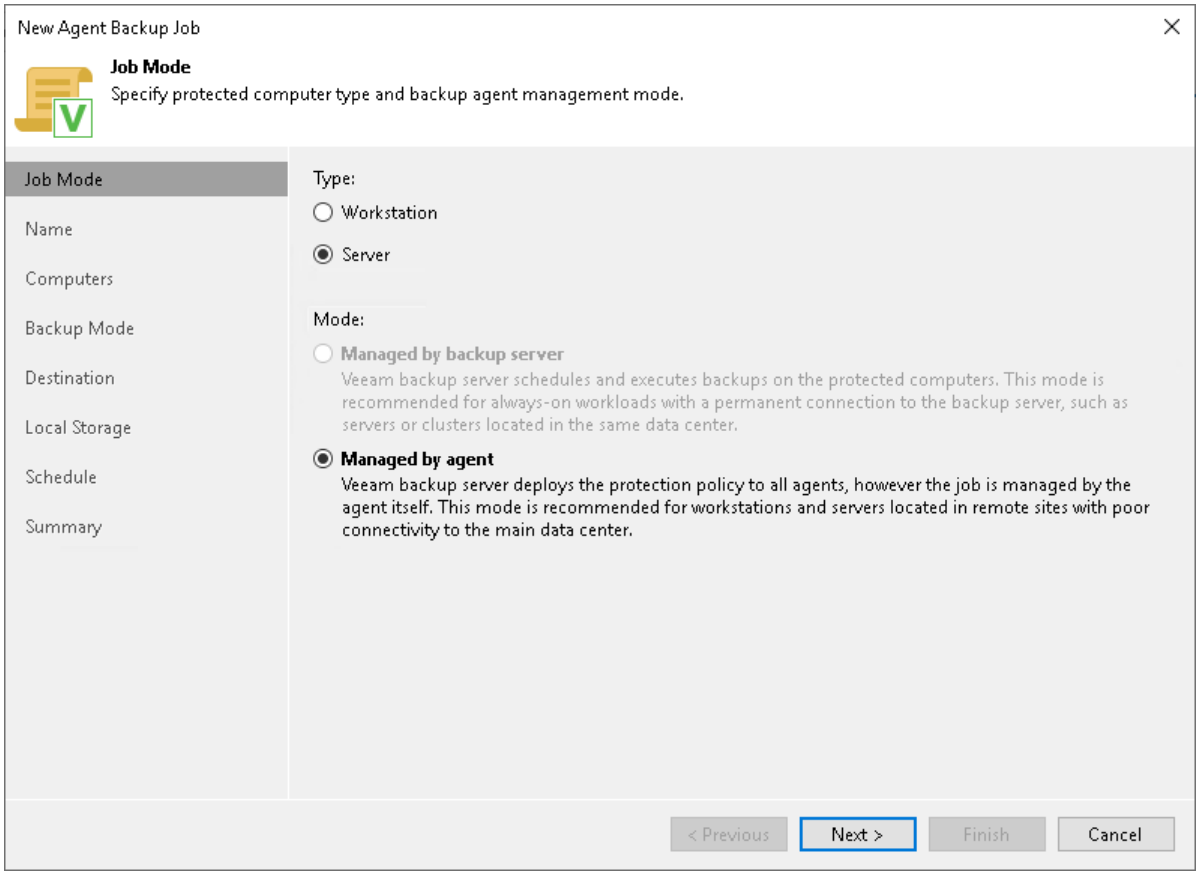
- **Workstation** — select this option if you want to back up data pertaining to macOS workstations or laptops. This option is suitable for computers that reside in a remote location and may have limited connection to the backup server.

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

- **Server** — select this option if you want to back up data pertaining to macOS 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 operating in the Server mode. To learn more, see the Product Editions section in the Veeam Agent for Mac User Guide.

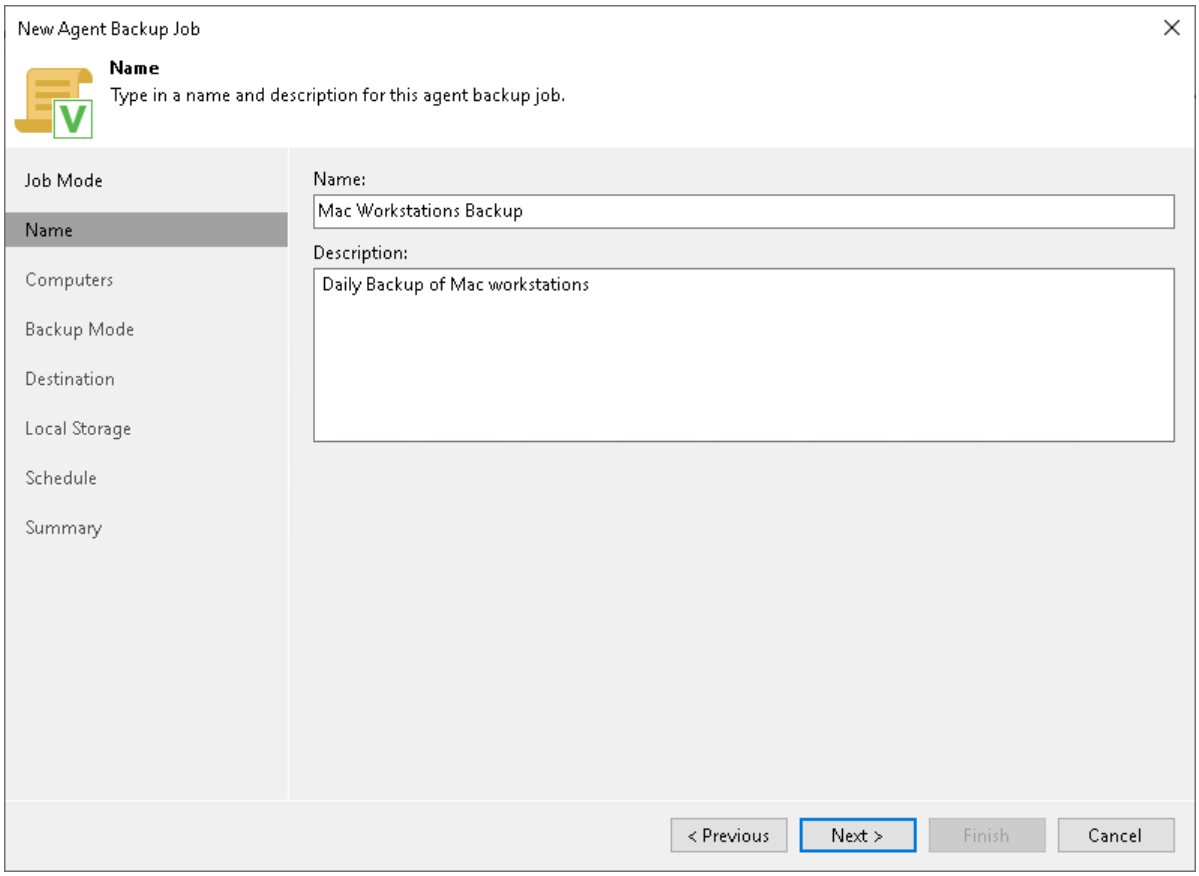
You do not need to select the job mode. Mac computers can be added only to Veeam Agent backup jobs managed by Veeam Agent.



Step 3. Specify Policy Name and Description

At the **Name** step of the wizard, specify a name and description for the backup policy.

1. In the **Name** field, enter a name for the backup policy.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who created the policy, date and time when the policy 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 policy one or more protection groups and/or individual computers added to inventory in the Veeam Backup & Replication console. If Veeam Backup & Replication discovers a new computer in a protection group after the Veeam Agent backup policy is created, Veeam Backup & Replication will automatically update the policy settings to include the added computer.

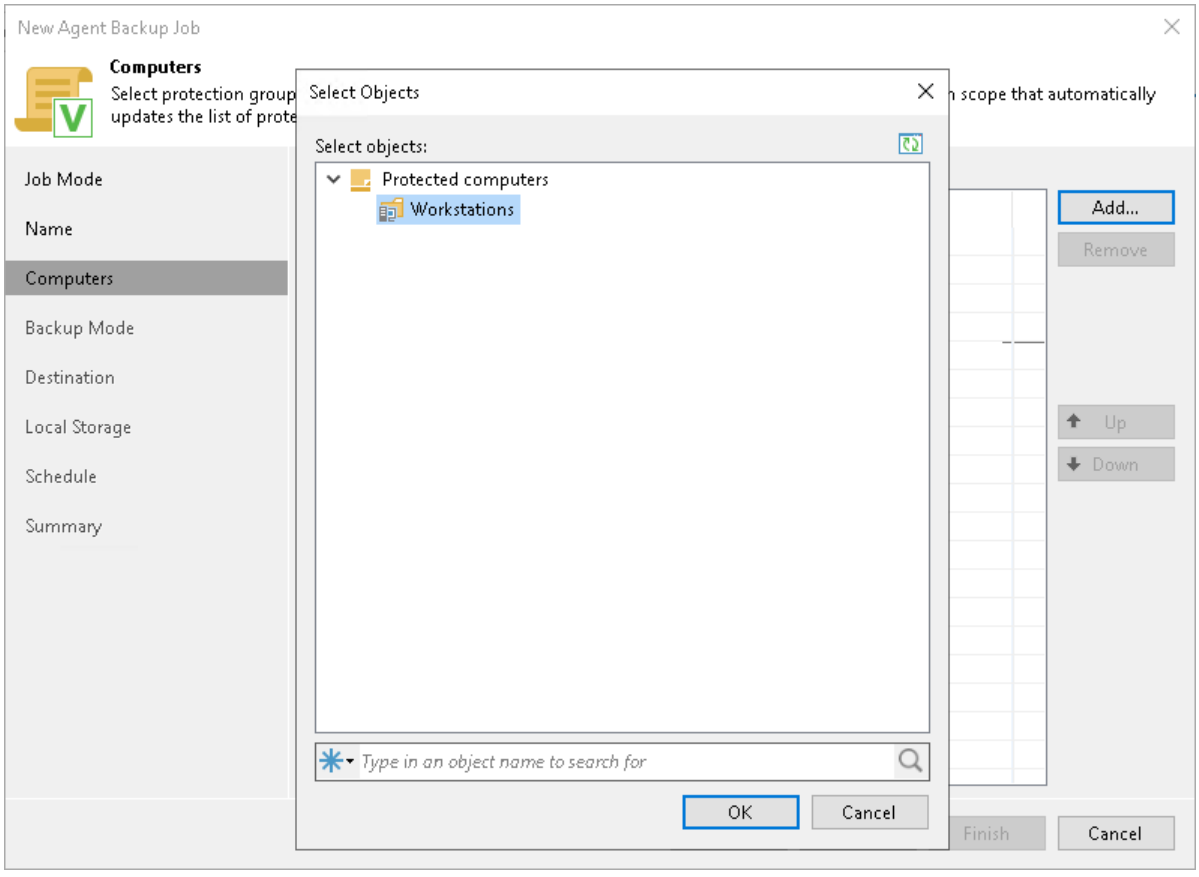
> **NOTE**
>
> If you used the **Add to backup job** > **Mac** > **New job** option to launch the New Agent Backup Job wizard, the **Protected computers** list will already contain computers that you have selected to add to the policy. You can remove some computers from the policy or add new computers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

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

1. Click **Add**.
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]**.



Step 5. Select Backup Mode

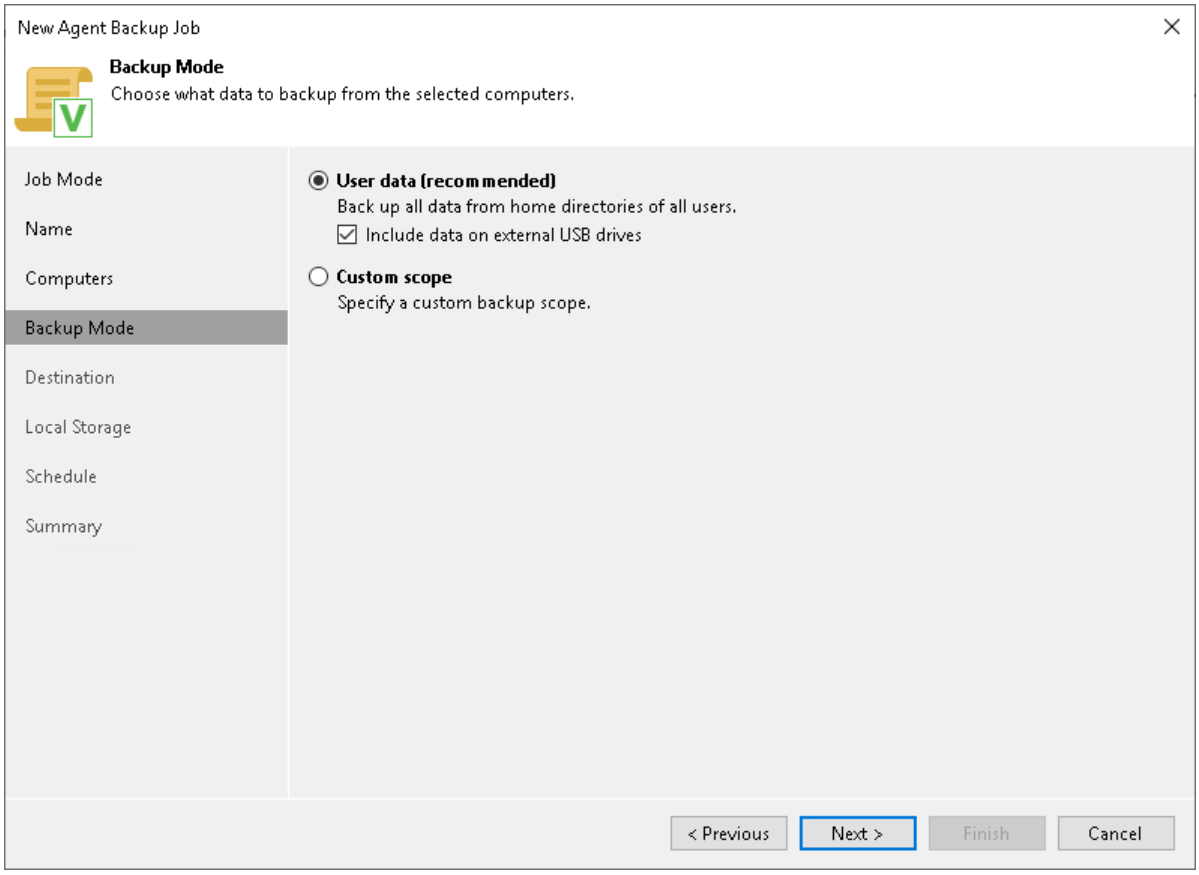
At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup. You can select one of the following options:

- **User data** – select this option if you want to create a backup of the `Users` folder that contains the `Home` folders of all users. With this option selected, you will pass to the Destination step of the wizard.

  To include user data residing on an external USB drive, select the **Include external USB drives** check box. The USB drive must be mounted to a location within the `Users` folder. You can include user data from one or more USB drives connected to the Veeam Agent computer at the time when the backup job starts on the protected computer.

  > **NOTE**
  >
  > When you select **User data** mode, Veeam Agent excludes network shared folders from the backup scope. To back up a network shared folder, you must select the **Custom scope** option and add this network shared folder as an individual object to the backup scope at the **Objects** step of the wizard.

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



Step 6. Specify Backup Scope Settings

The **Objects** step of the wizard is available if you have chosen the **Custom scope** mode at the Backup Mode step of the wizard.

At this step of the wizard, you must specify the backup scope — define what folders 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 policy. If a specified folder does not exist on one or more computers in the policy, the policy will skip such folder on those computers and back up existing ones.

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

- *Include data on external USB drives* — data residing on an external USB drive. The USB drive must be mounted to a location within the `Users` folder. You can include user data from one or more USB drives connected to the Veeam Agent computer at the time when the backup job starts on the protected computer.
- *Personal files* — data related to user profiles. With this option enabled, Veeam Backup & Replication will include in the backup scope settings and data related to Veeam Agent computer user profiles. To learn more, see the Protecting User Profiles section in the Veeam Agent for Mac User Guide.
- *Individual file system objects* — directories, mount points, and volumes of a protected computer.

To specify individual folders to back up:

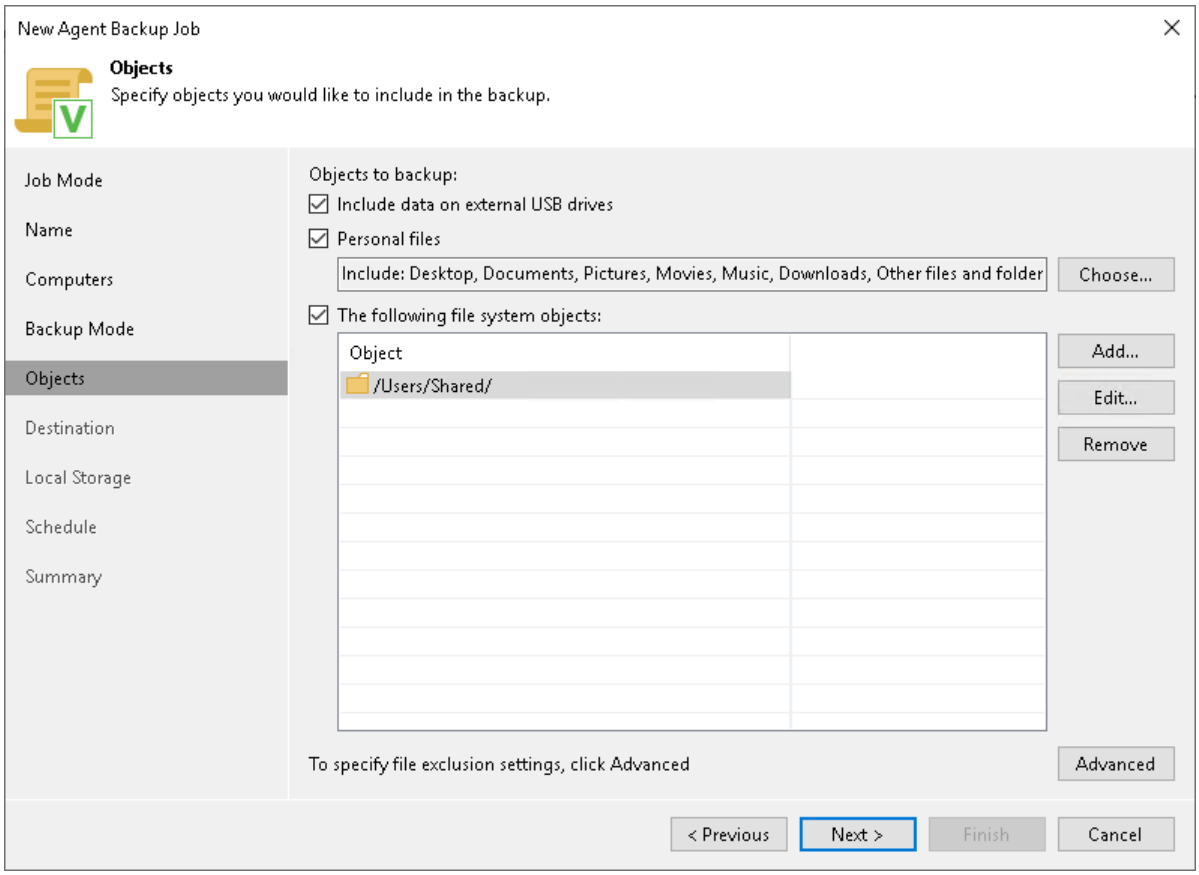
1. Select the **The following file system objects** check box and click **Add**.
2. In the **Add Object** window, type the path to a folder, mount point folder, or volume that you want to back up, for example, */Users/Shared/* or */Users/Administrator/Documents/*, and click **OK**.
3. Repeat steps 1-2 for all items that you want to back up.

TIP

If you want to back up the root folder and specify `/` in the **Path to a directory** field, Veeam Agent does not automatically include remote mount points in the backup scope. To include remote mount points, you need to specify paths to these mount points manually.

For example, you have a file system mounted to the `/Library/Media` folder. If you add `/` as an object to the backup scope, Veeam Agent will not back up the mounted file system. To back up the root folder and the mounted file system, add the following objects to the backup scope:

- `/`
- `/Library/Media`



Configuring Filters

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

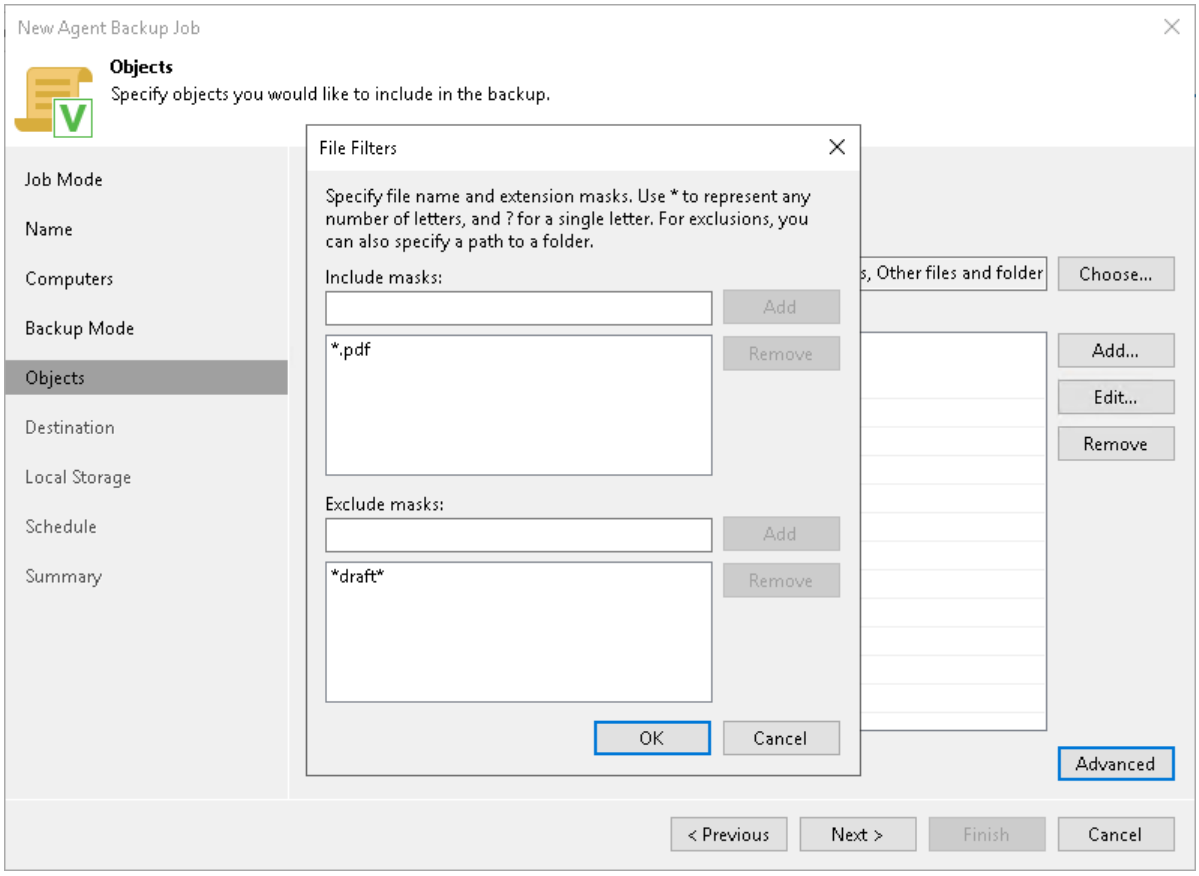
To configure a filter:

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 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 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 will include in the backup all files of the PDF format that do not contain *draft* in their names.



Step 7. Select Backup Destination

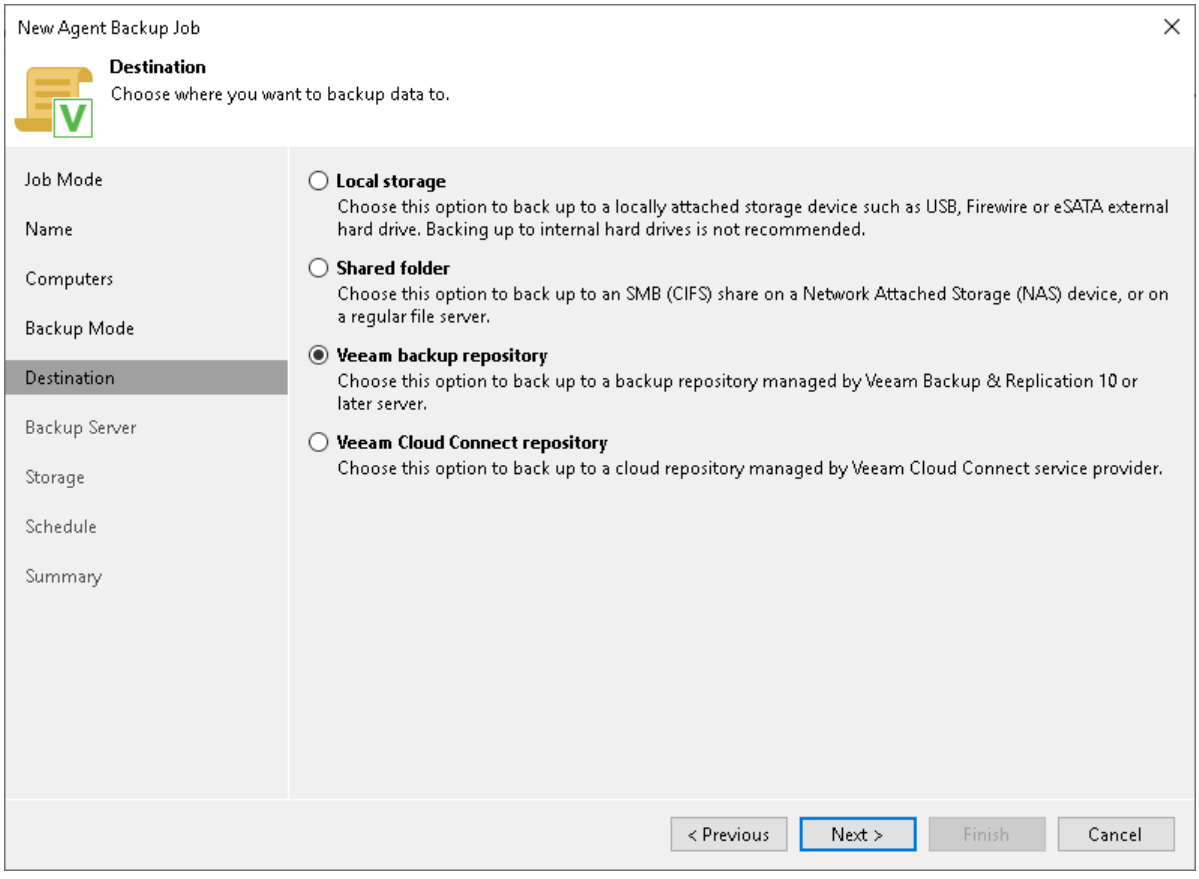
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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 policy 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.

Local Storage Settings

The **Local Storage** step of the wizard is available if you have chosen to save the backup on a local drive of your computer.

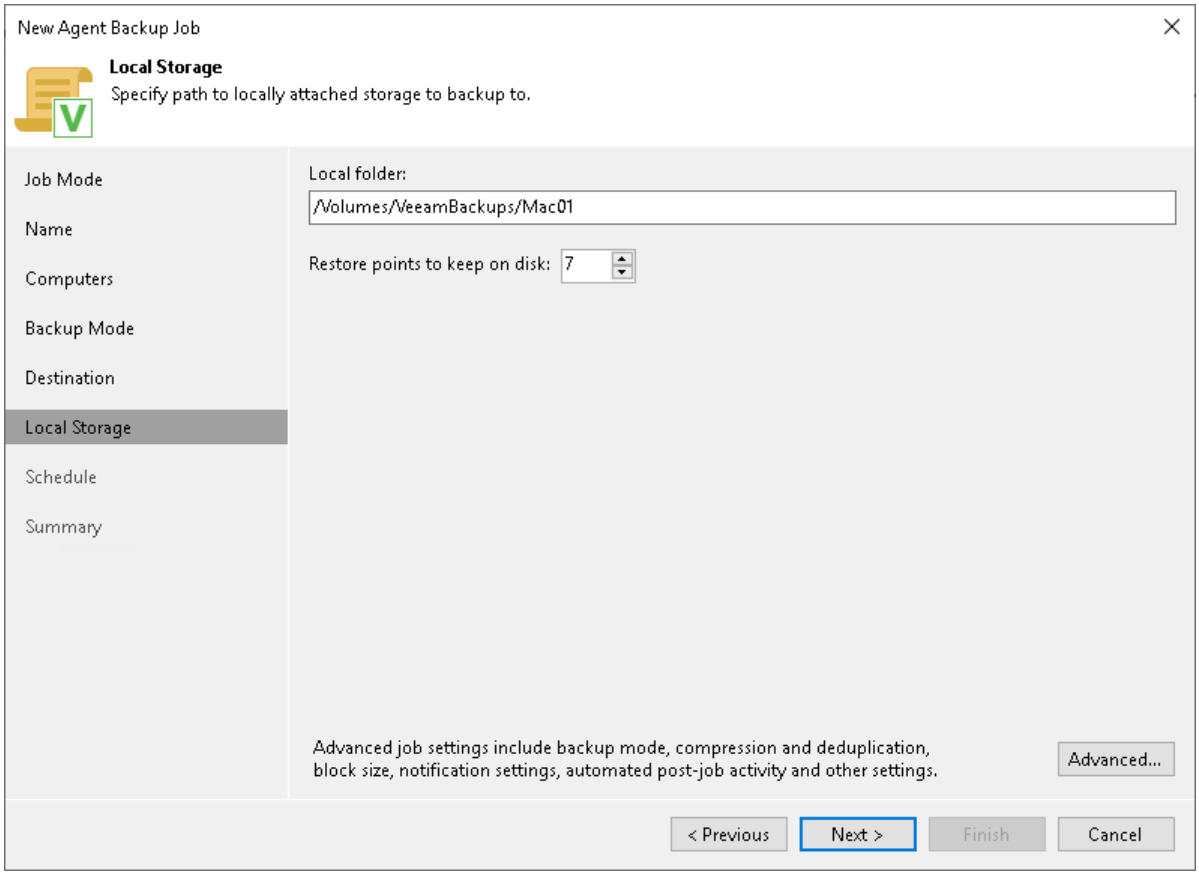
Specify local storage settings:

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 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 policy 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 keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

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



Shared Folder Settings

The **Shared Folder** step of the wizard is available if you have chosen to save the backup in a network shared folder.

Specify shared folder settings:

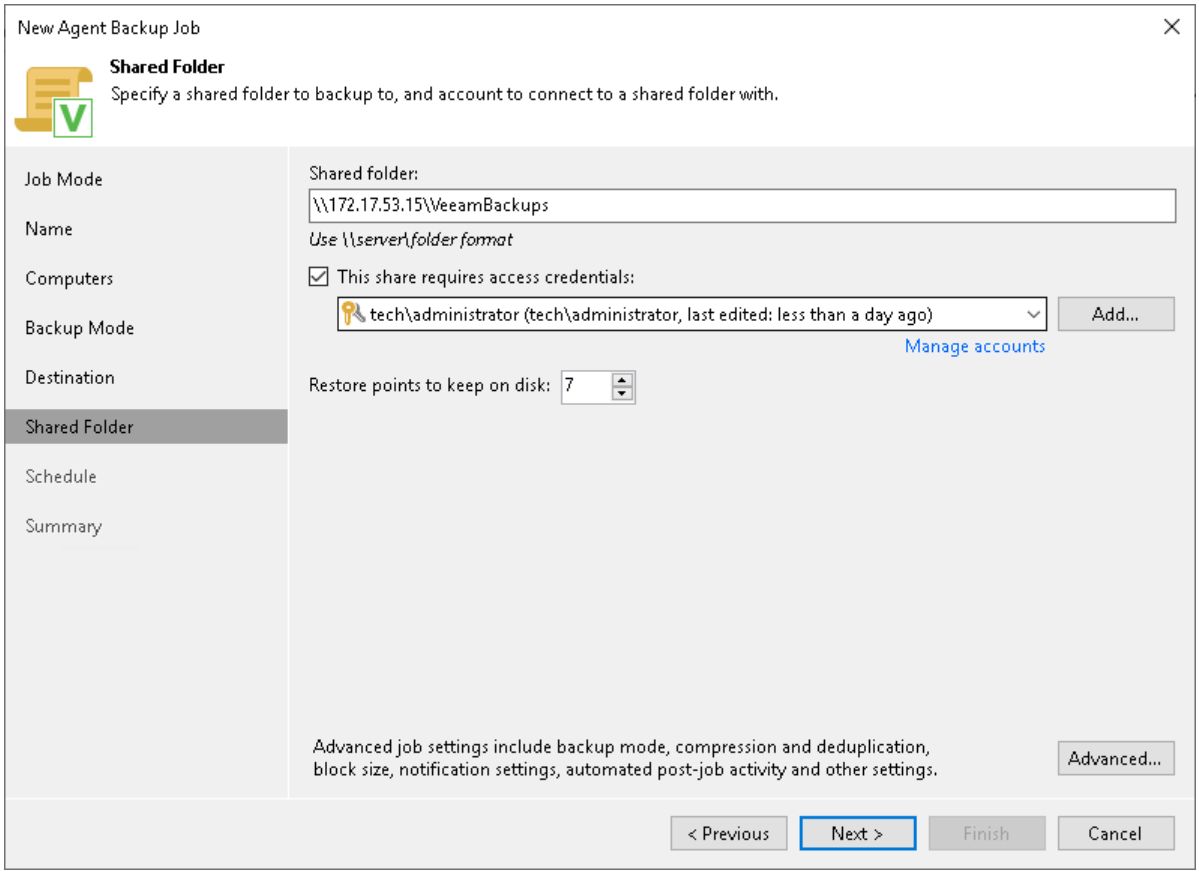
1. In the **Shared folder** field, specify a UNC name of the SMB network shared folder. The UNC name always starts with two back slashes (\\).

   Mind that Veeam Backup & Replication does not support the NFS shares for Mac computers.

2. If the SMB 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.

3. 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 keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

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



Veeam Backup Repository Settings

If you have chosen to store backup files on a Veeam backup repository, specify settings to connect to the backup repository:

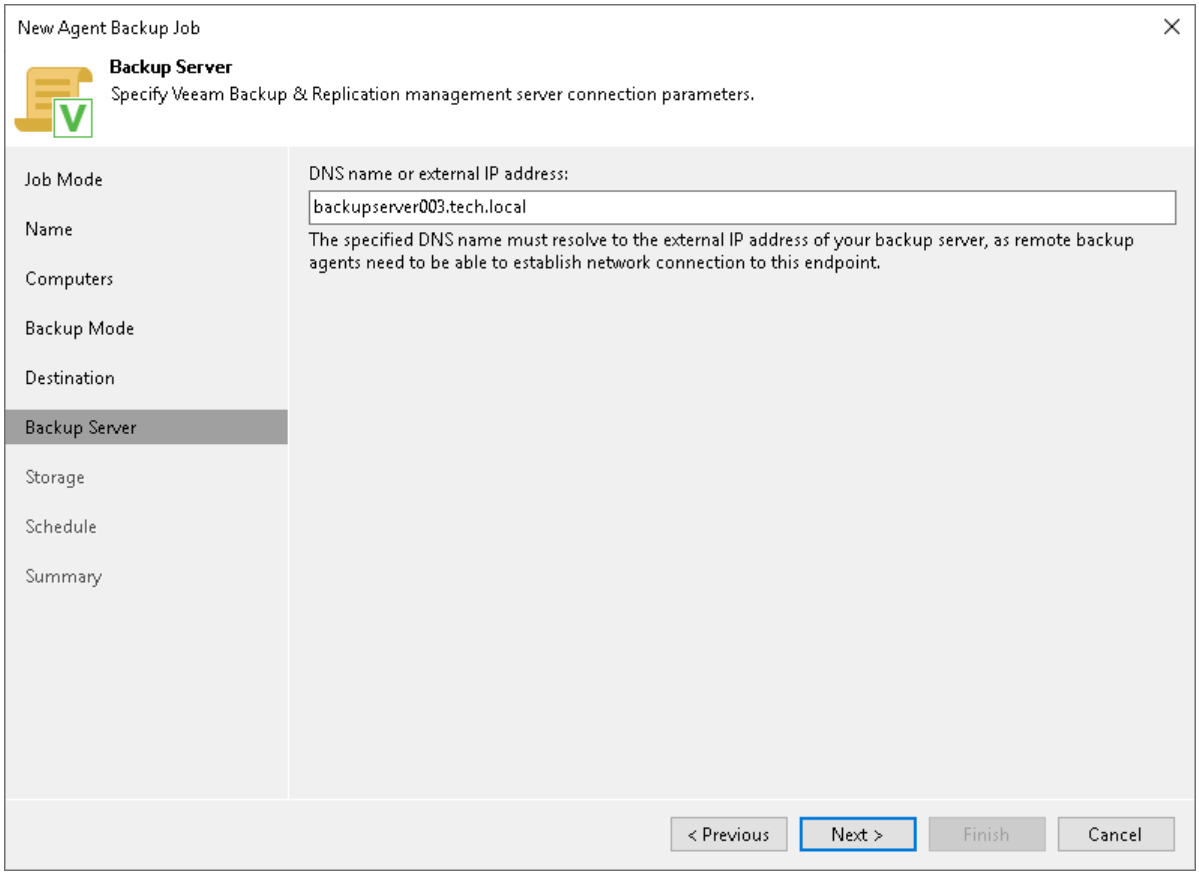
1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Storage step of the wizard, select the Veeam backup repository.

Specifying Backup Server Settings

The **Backup Server** step of the wizard is available if you have 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 policy. 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.



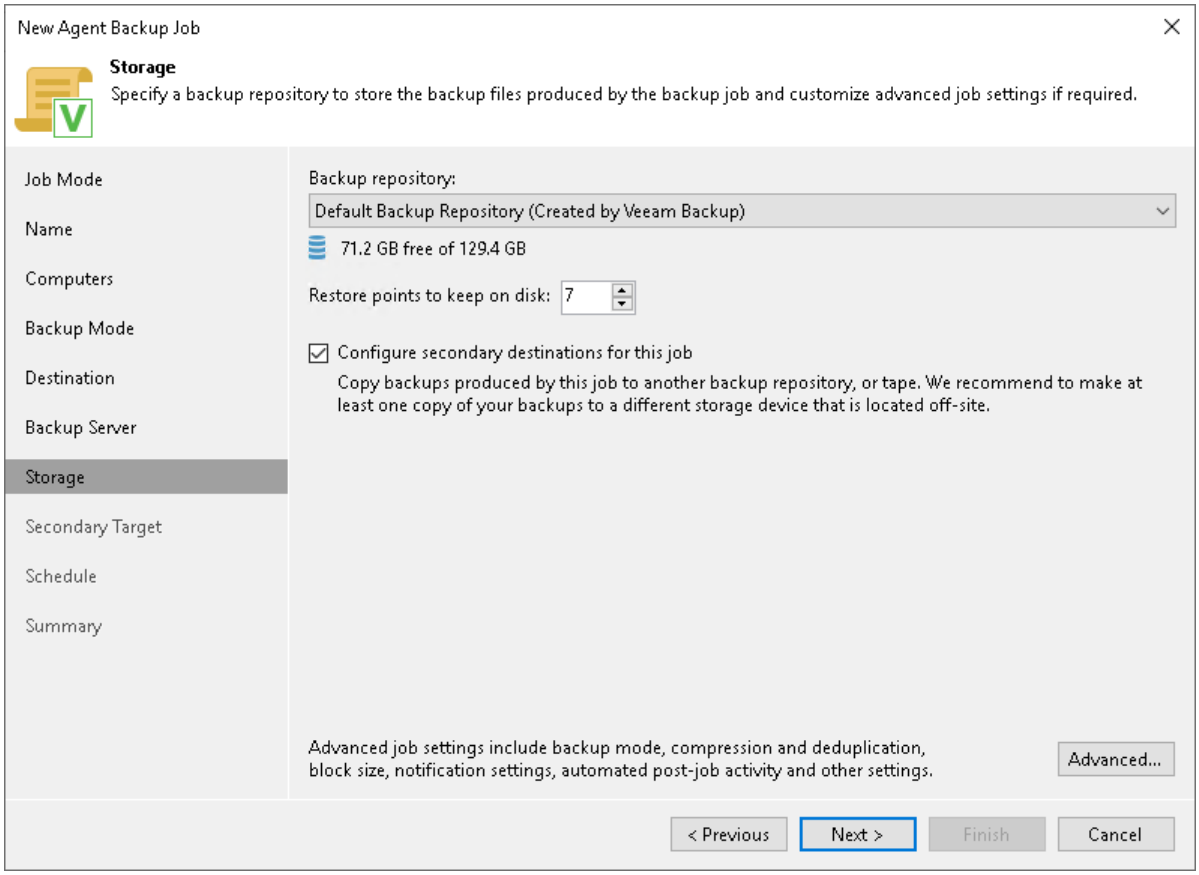
Selecting Backup Repository

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 keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent 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 backup 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 policy 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 policy. To learn more, see Specify Advanced Backup Settings.

> **TIP**
>
> You can map the job to a specific backup stored on the Veeam 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. To learn more, see Backup Job Mapping.



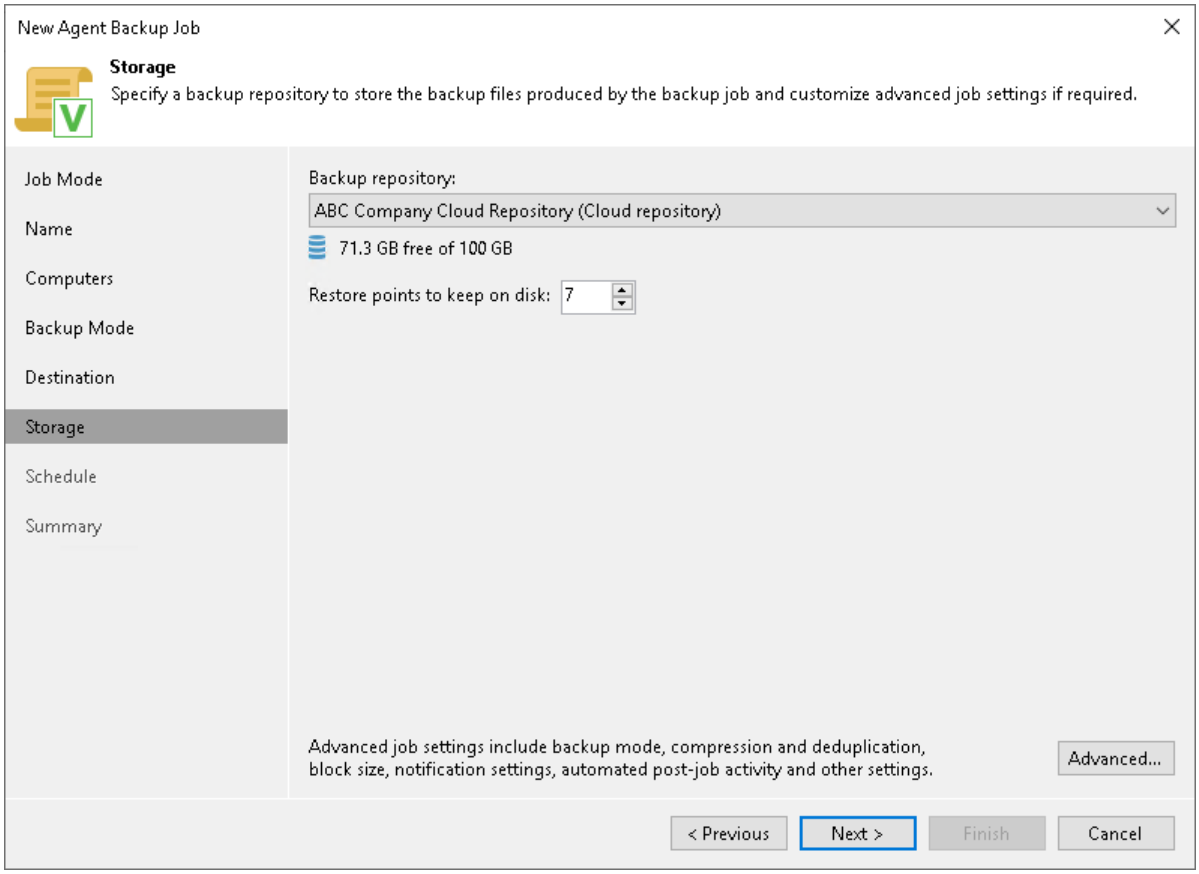
Cloud Repository Settings

The **Storage** step of the wizard is available if you have chosen to save backup files on a Veeam Cloud Connect repository.

> **NOTE**
>
> Keep in mind that FQDN or IP addresses of Veeam Agent computers 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 keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.
3. Click **Advanced** to specify advanced settings for the backup policy. 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 policy:

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings

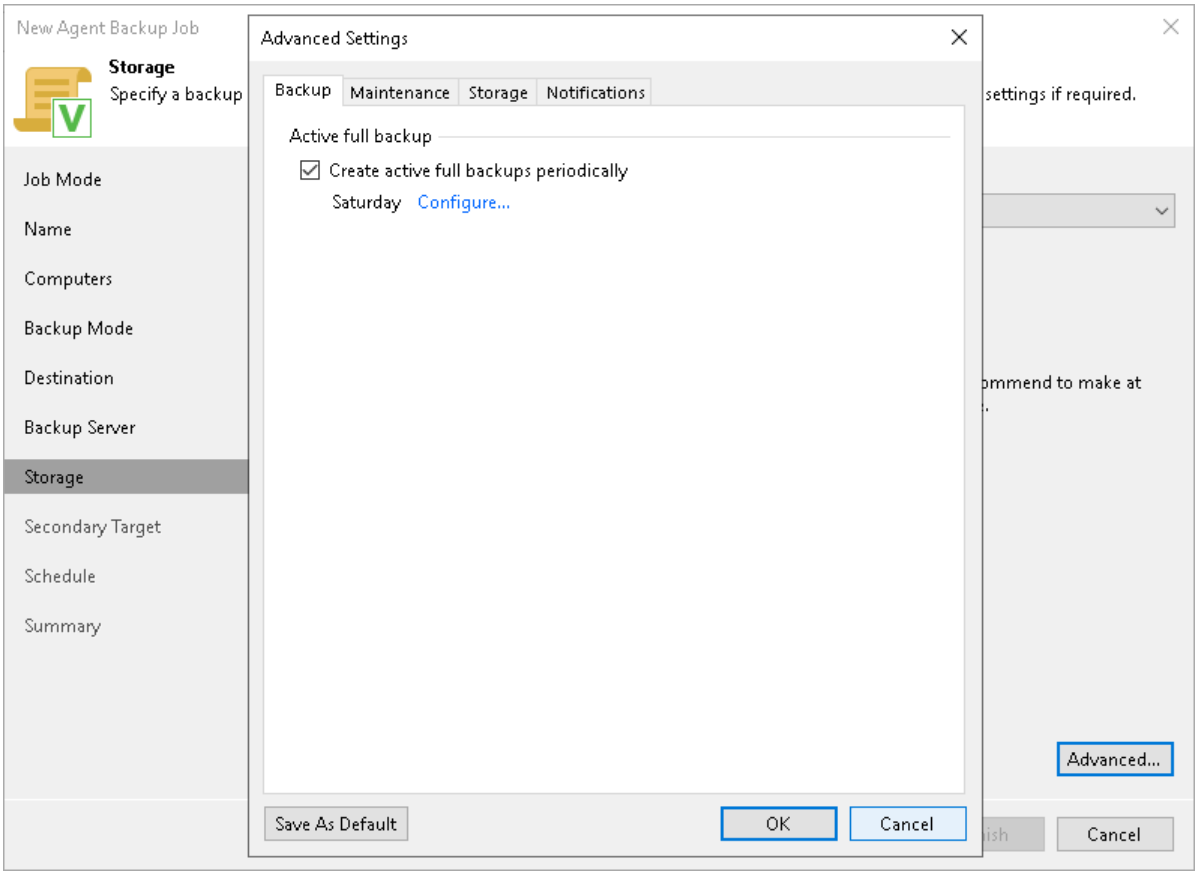
> **TIP**
>
> After you specify necessary settings for the Veeam Agent backup policy, you can save them as default settings. To do this, click **Save as Default** at the bottom left corner of the **Advanced Settings** window. When you create a new backup policy, Veeam Backup & Replication will automatically apply the default settings to the new policy.

Backup Settings

To specify settings for a backup chain created with the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **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.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
2. If you want to periodically create active full backups, select the **Create active full backups periodically** check box and click **Configure** to define scheduling settings.

> **NOTE**
>
> Before scheduling periodic full backups, you must make sure that you have enough free space on the target location.



Maintenance Settings

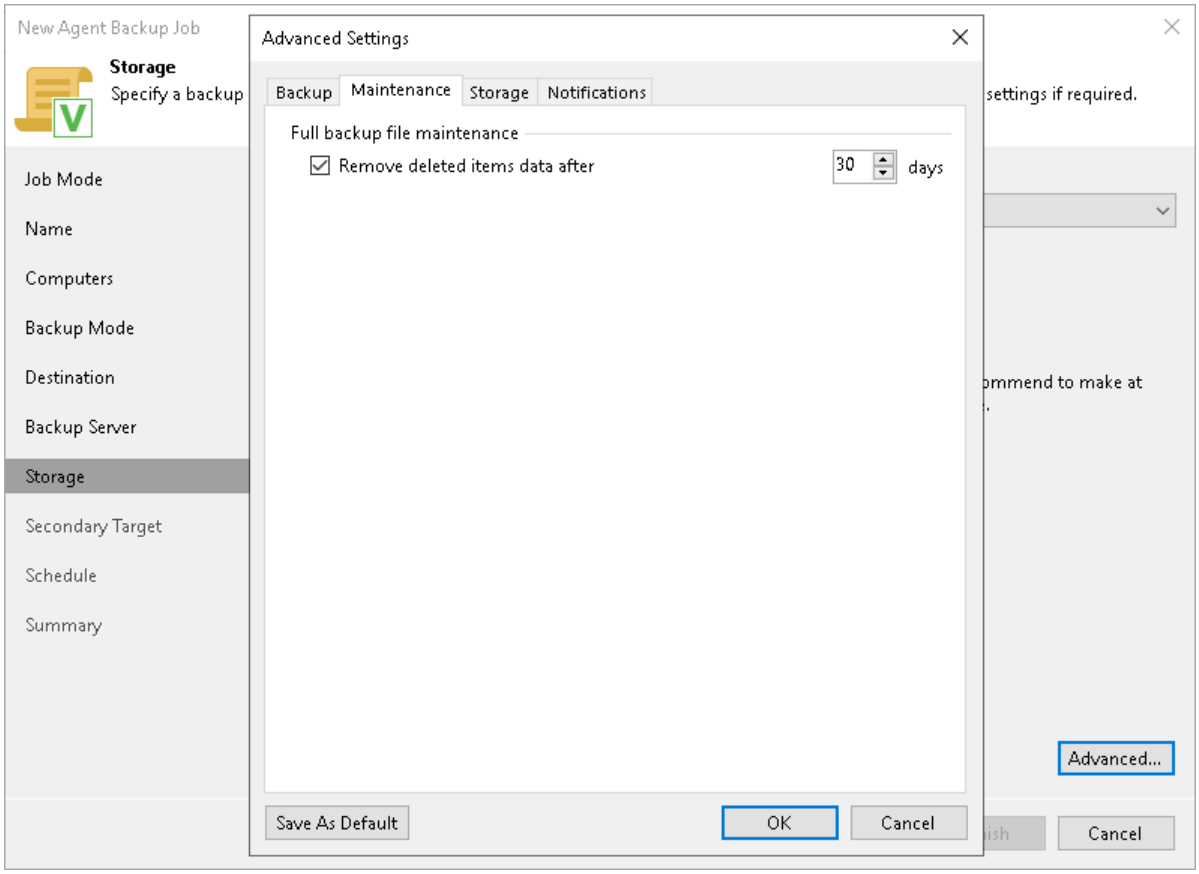
You can specify maintenance settings for a backup policy targeted at a Veeam backup repository. Maintenance operations help make sure that the backup chain remains valid and consistent.

To specify maintenance settings for the backup policy:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Maintenance** tab.
3. 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 policy in the target location.

   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.

   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. Otherwise, the backup policy may not work as expected and remove data that you still require.
4. If you selected object storage as a target for your backup, Veeam Backup & Replication will display the setting that allows you to schedule a regular backup health check. For details, see Scheduling Health Check.



Scheduling Health Check

When you store backup files in object storage, an automatic health check can help you avoid a situation when a restore point gets corrupted, making all dependent restore points corrupted, too. For more information, see Health Check for Object Storage.

To periodically perform a health check of the backup, do the following:

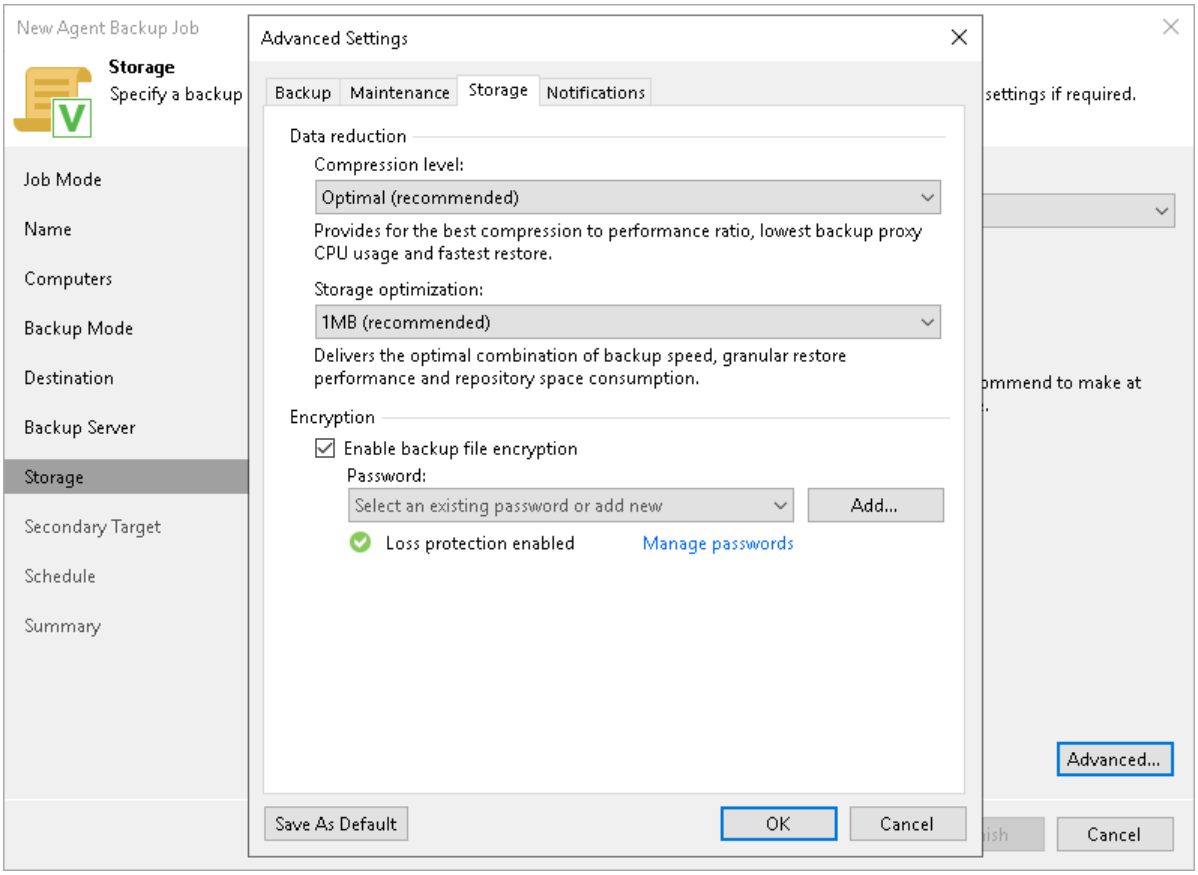
1. In the Advanced Settings window, select the Maintenance tab.
2. Select the **Perform backup files health check** check box.
3. Use the **Monthly** on or **Weekly** on selected days options to define the schedule for the health check of the backup in the repository.

Storage Settings

To specify storage settings for the backup policy:

1. Click **Advanced** at one of the following steps of the wizard:
   - **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.
   - **Storage** – if you have selected to save backup files in a Veeam backup repository or cloud repository.
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 size of data blocks you plan to use: *4 MB, 1 MB, 512 KB, 256 KB*. Veeam Agent will use data blocks of the chosen 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 job or policy, during the next session Veeam Agent 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 or policy, Veeam Agent will encrypt the backup chain starting from the next restore point created with this job.
- 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

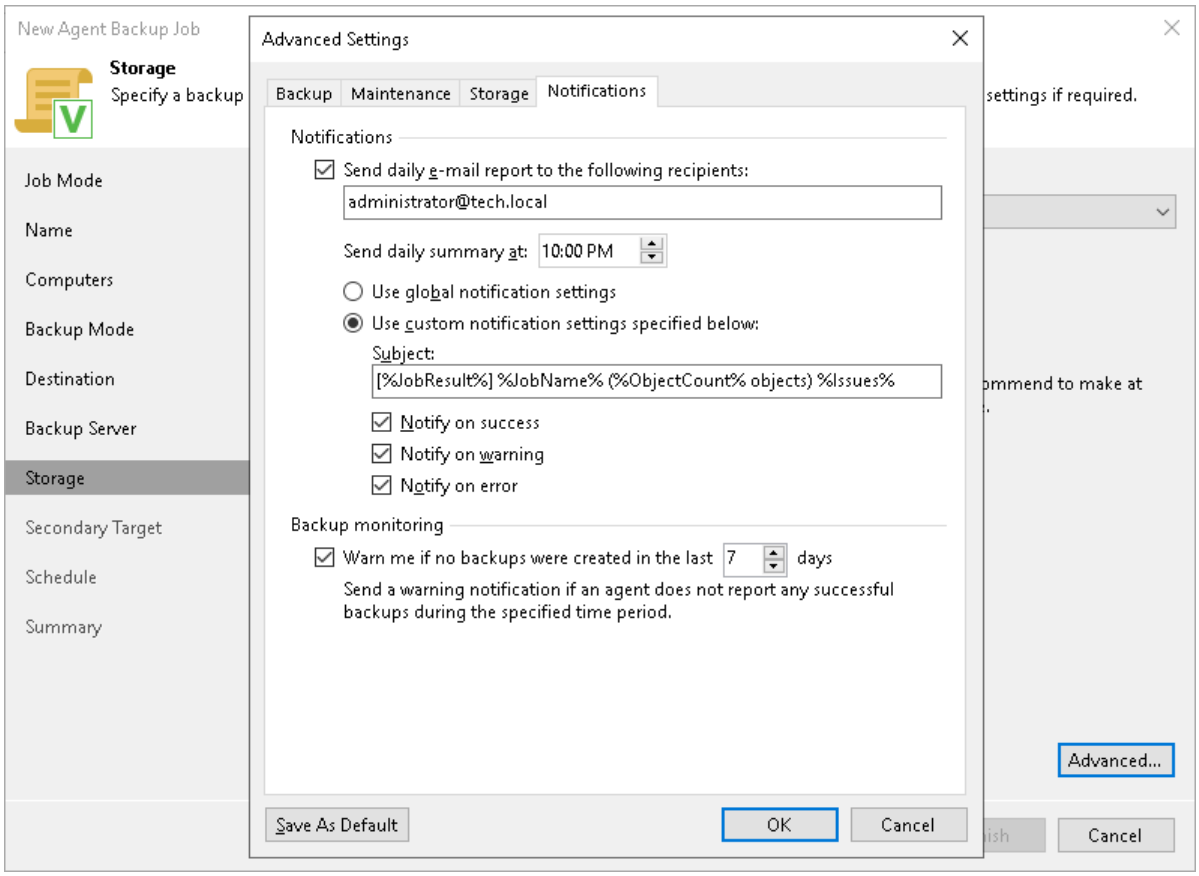
You can specify email notification settings for the backup policy. If you enable notification settings, Veeam Backup & Replication will send a daily email report with backup policy statistics to a specified email address. The report contains cumulative statistics for backup policy sessions performed 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 & Replicationwill 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:
   - **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.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository or cloud repository.
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 daily summary 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.
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. 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 **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 policy completes successfully, completes with a warning or fails.

5. In the **Backup monitoring** section, select the **Warn me if no backups were created in the last N days** check box and specify a number of days. In this case, Veeam Backup & Replication will display a warning message in a backup policy session statistics in case successful backups are not created for a specified number of days.



Step 10. Specify Secondary Target

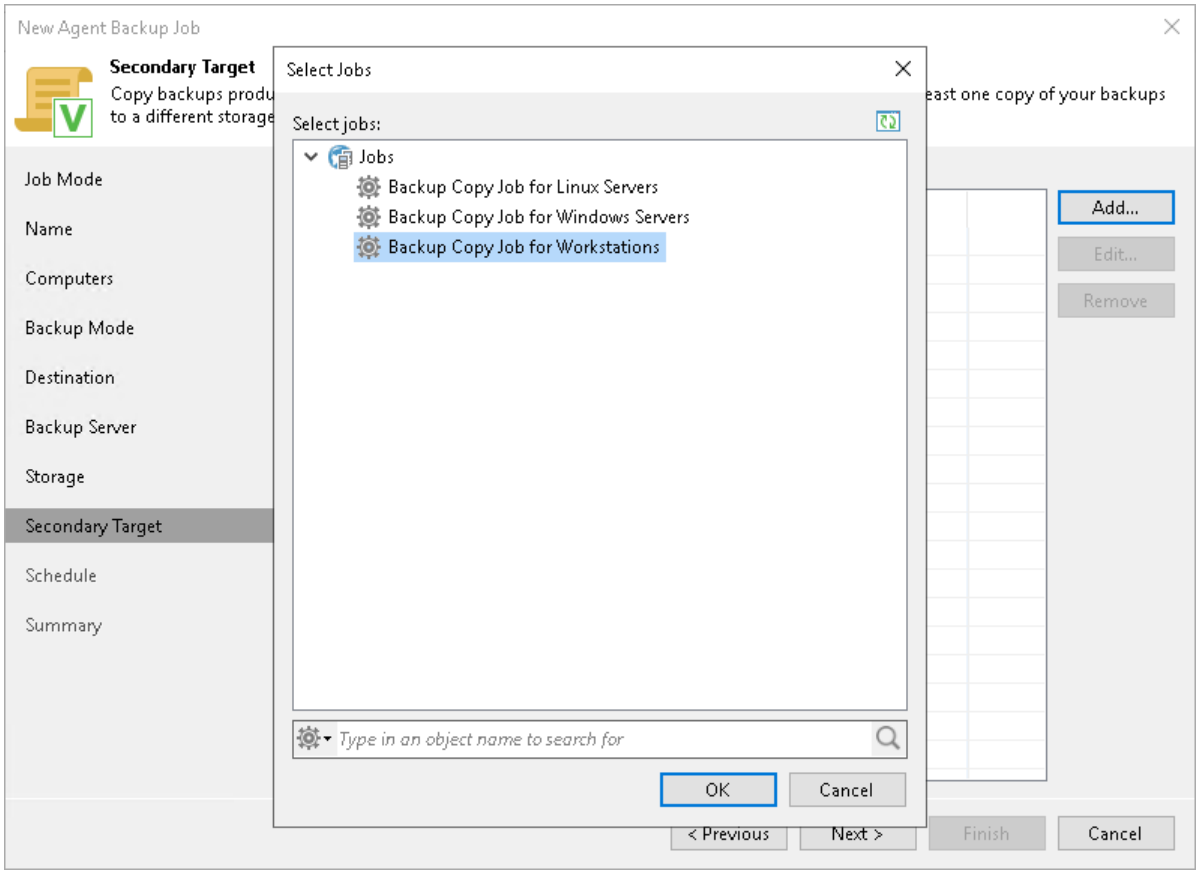
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

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 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 job mode that you have selected at the Job Mode step of the wizard:

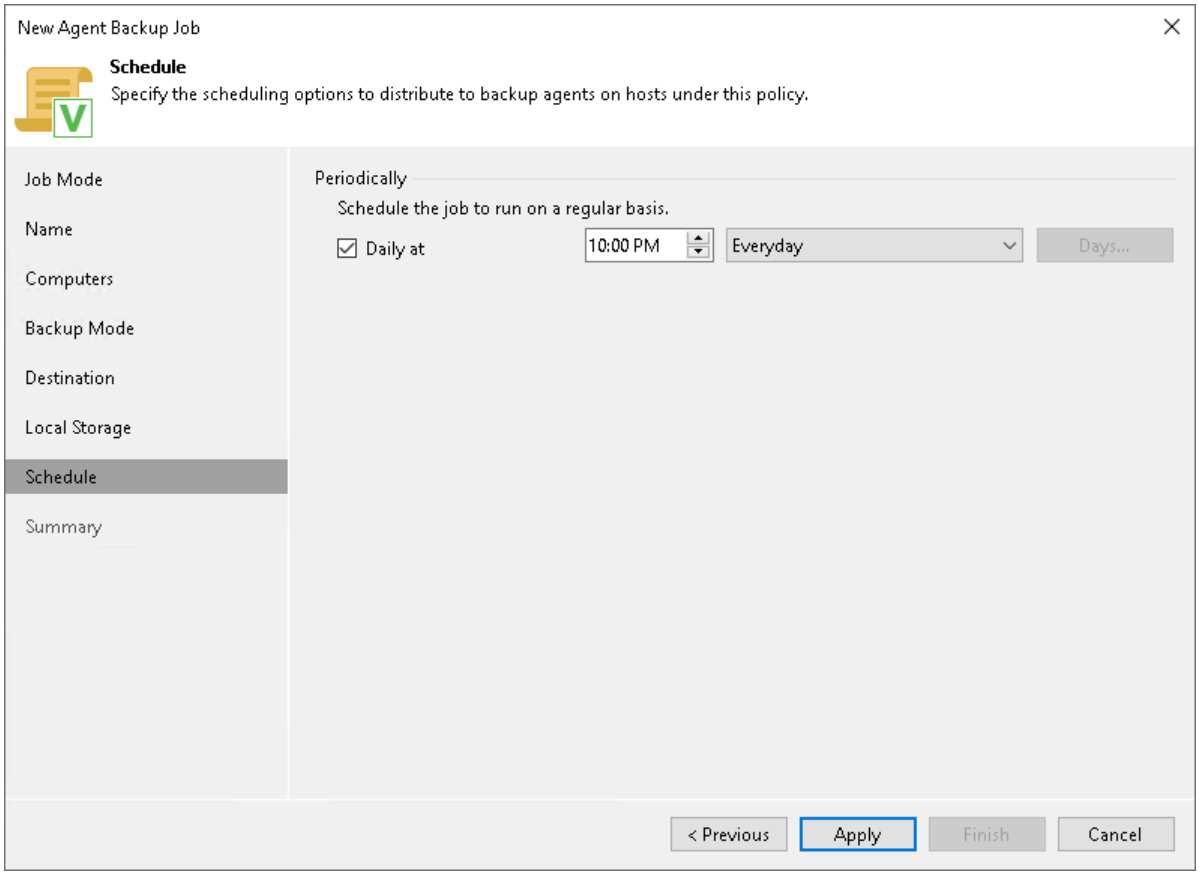
- Scheduling Settings for Workstations
- Scheduling Settings for Servers

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.

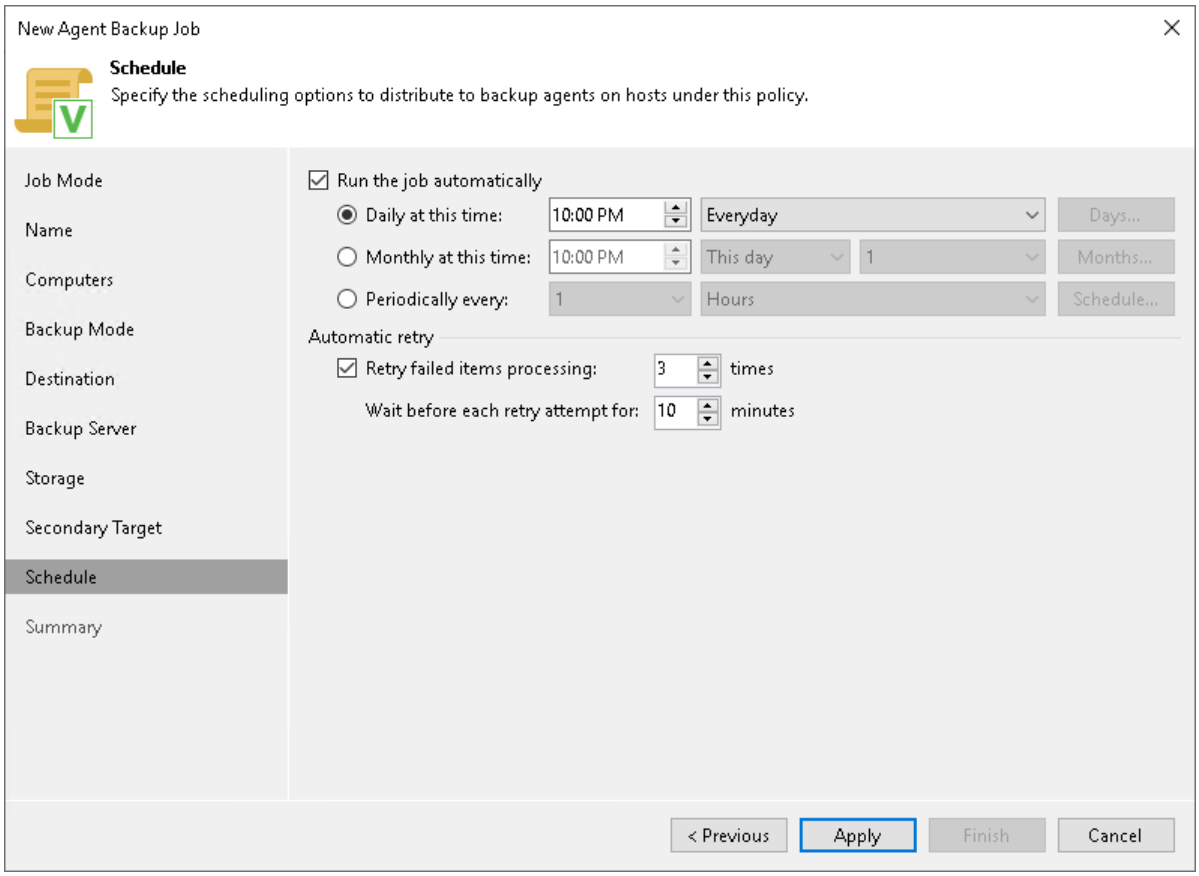


Scheduling Settings for Servers

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*.
3. In the **Automatic retry** section, define whether Veeam Agent 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 Agent for Mac will retry the job for the defined number of times without any time intervals between the job runs.



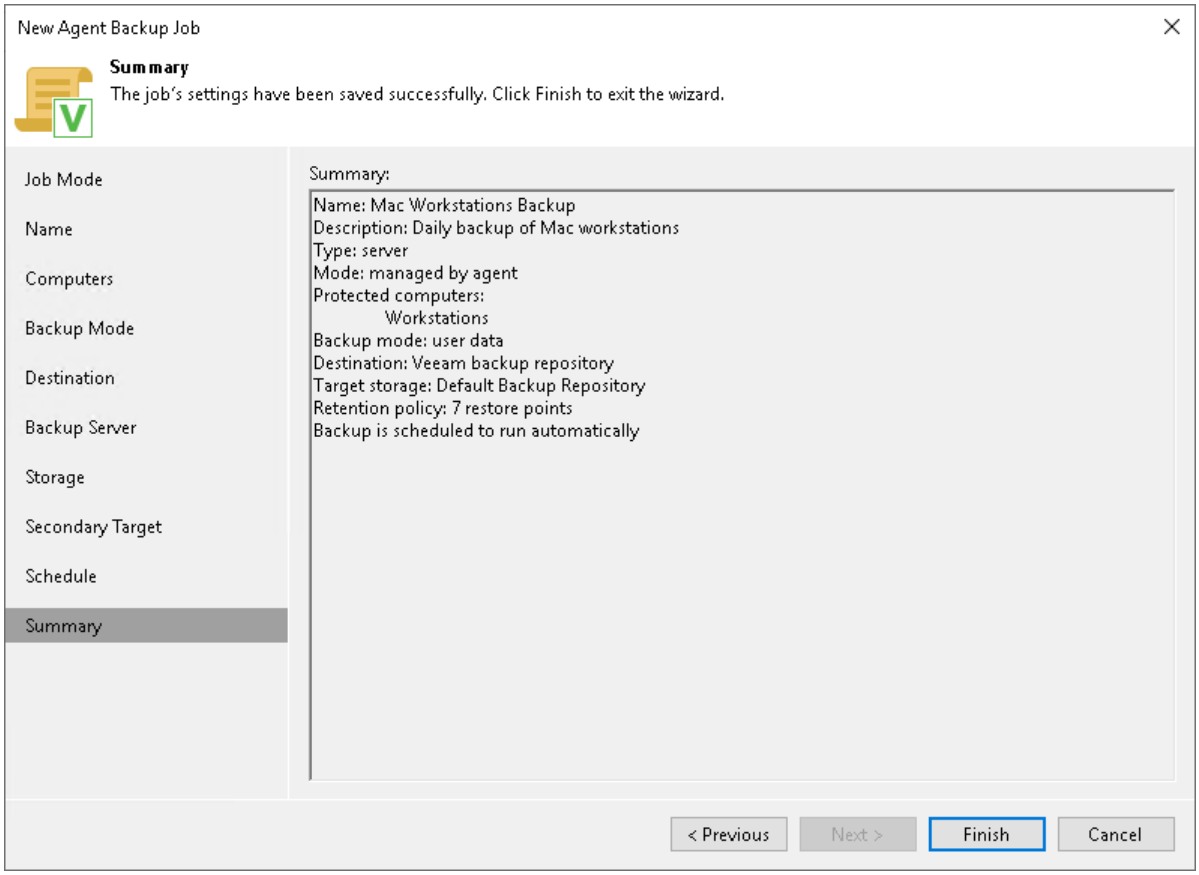
Step 12. Review Backup Job Settings

At the **Summary** step of the wizard, complete the Veeam Agent backup policy configuration process.

1. Review settings of the configured backup policy.
2. Click **Finish** to close the wizard.

Keep in mind that Veeam Backup & Replication does not apply backup policy to Mac computers immediately. Veeam Agents installed on Mac computers connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If you targeted a backup policy at the Veeam backup server and scheduled it earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next backup policy session start.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Mac Configuration.



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:

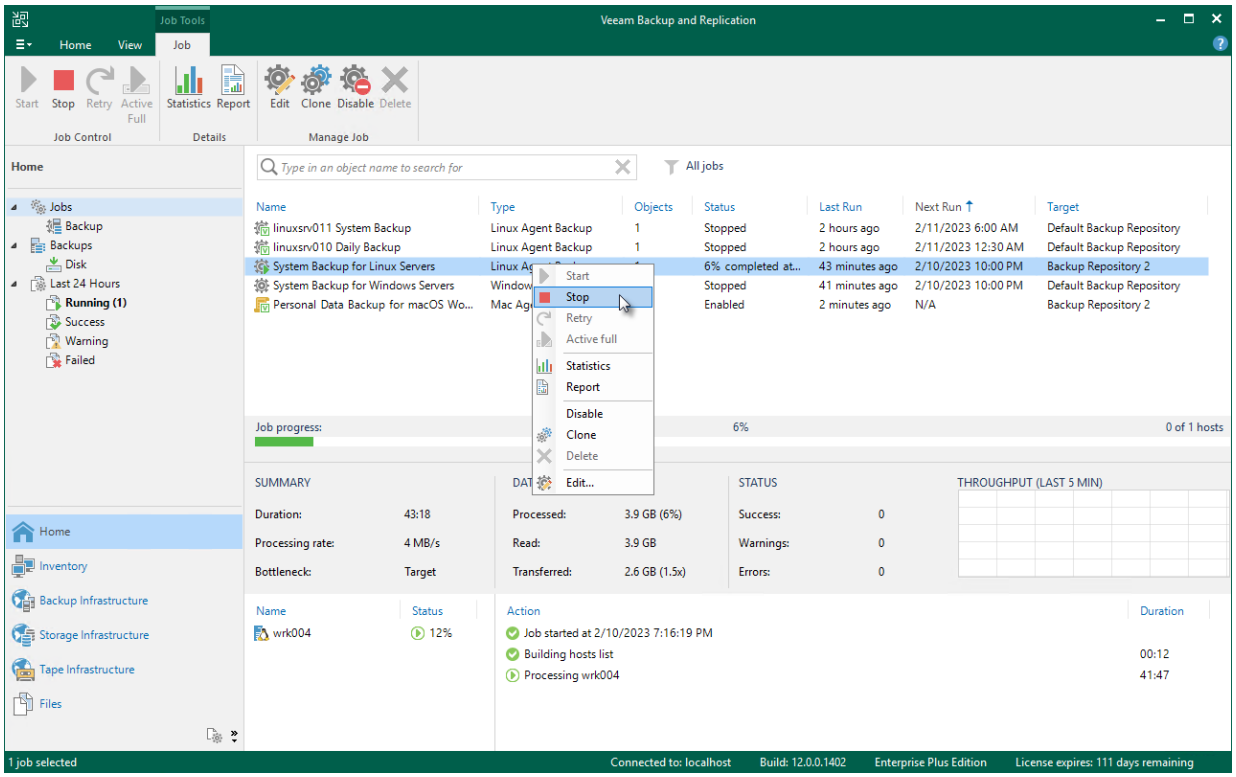
- Stop job immediately. In this case, Veeam Backup & Replication will produce a new restore point only for those computers in the job that have already been processed by the time you stop the job.
- Stop job gracefully. In this case, Veeam Backup & Replication will produce a new restore point only for 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**.



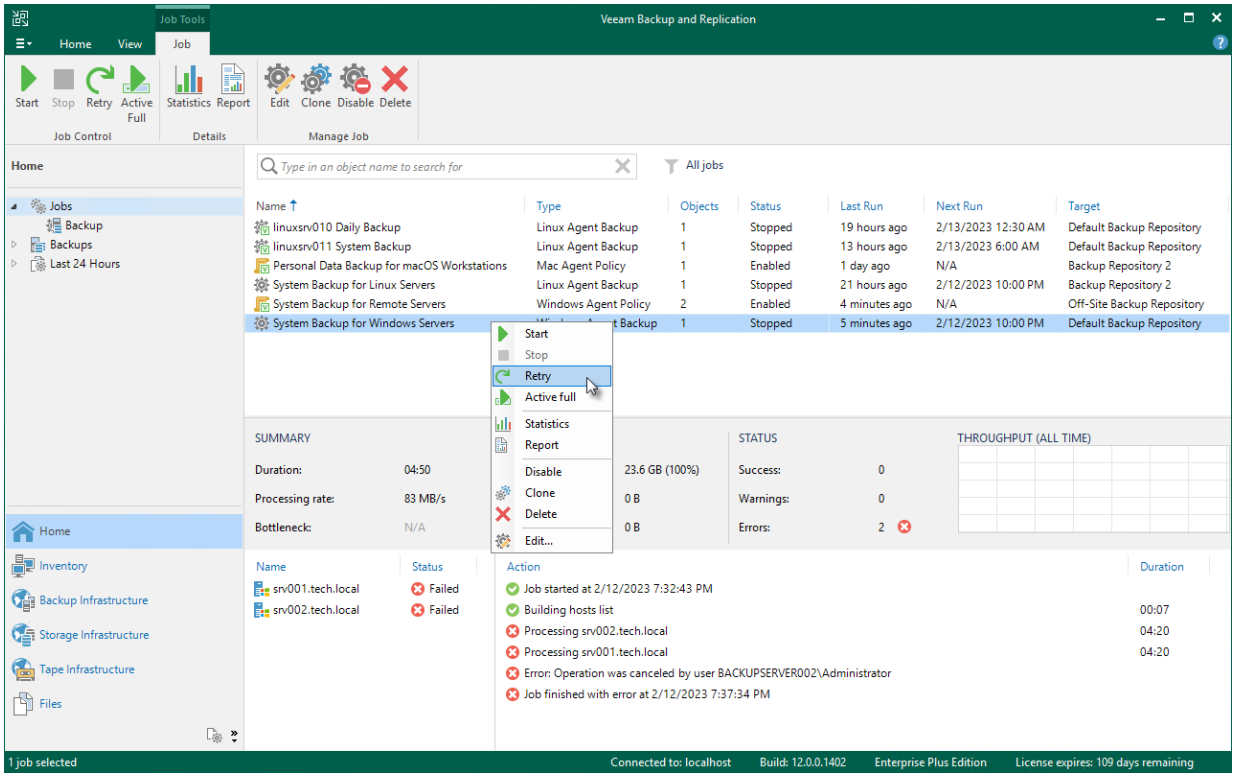
Retrying Veeam Agent Backup Job

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**.

> **TIP**
>
> You can also retry a backup job for an individual computer added to this job. To learn more, see Retrying Job for Individual Computer.

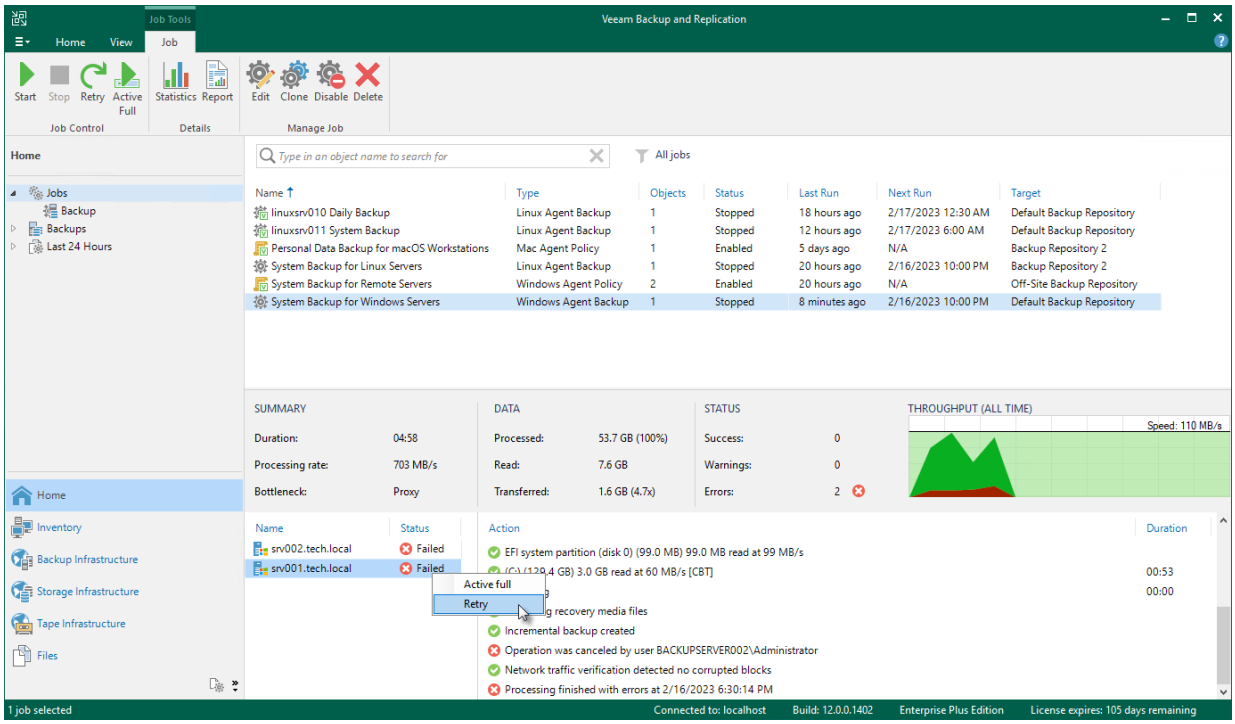


Retrying Job for Individual Computer

To retry a backup job for an individual computer:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job
4. In the bottom part of Veeam Backup & Replication, find the list of computers that are processed by the selected backup job. In the list, right-click the computer with the *Failed* status and click **Retry**.

   Keep in mind that you will be able to launch retry for another computer in the same job only after retry finishes for the selected computer.



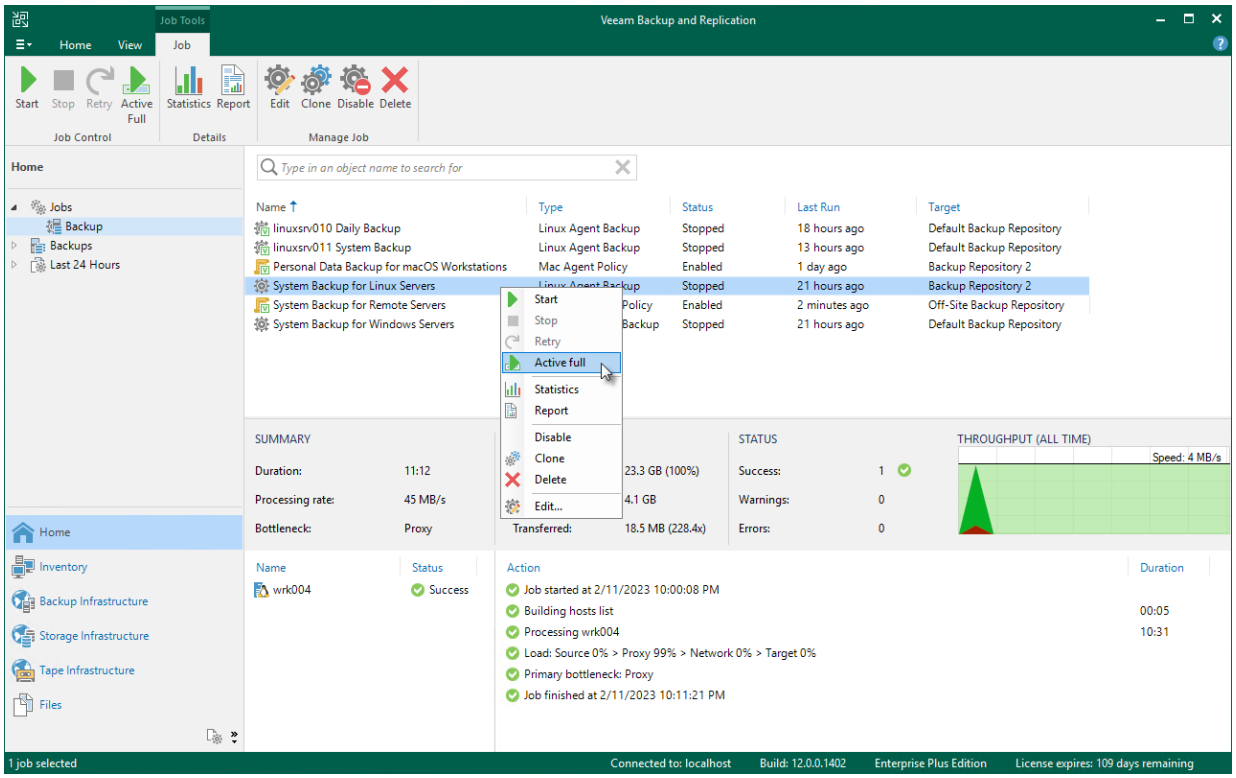
Performing Active Full Backup

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 create an 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**.

> **TIP**
>
> You can also create a full backup of an individual computer added to the backup job. To learn more, see Performing Active Full Backup for Individual Computer.



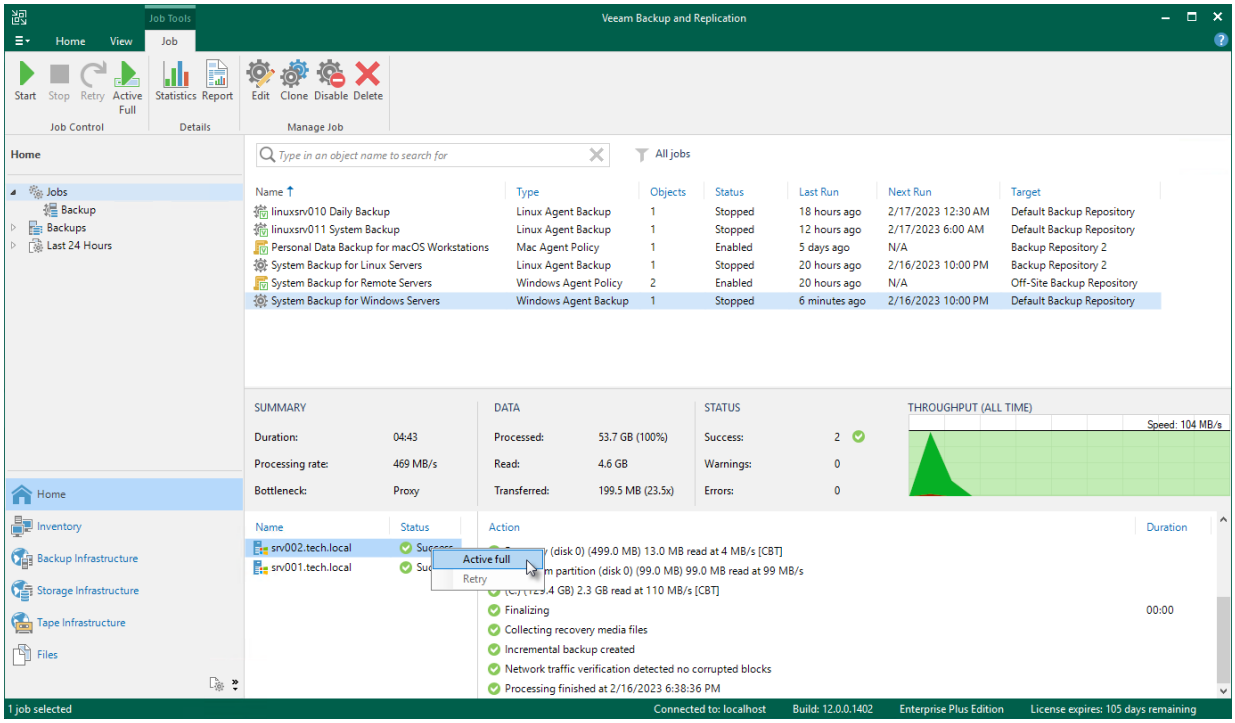
Performing Active Full Backup for Individual Computer

To create an active full backup for an individual computer:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup job
4. In the bottom part of Veeam Backup & Replication, find the list of computers that are processed by the selected backup job. In the list, right-click the computer and click **Active full**.

   Keep in mind the following:

   - You will be able to create an active full backup for another computer in the same job only after active full backup is created for the selected computer.
   - You cannot create an active full backup of a failover cluster node.



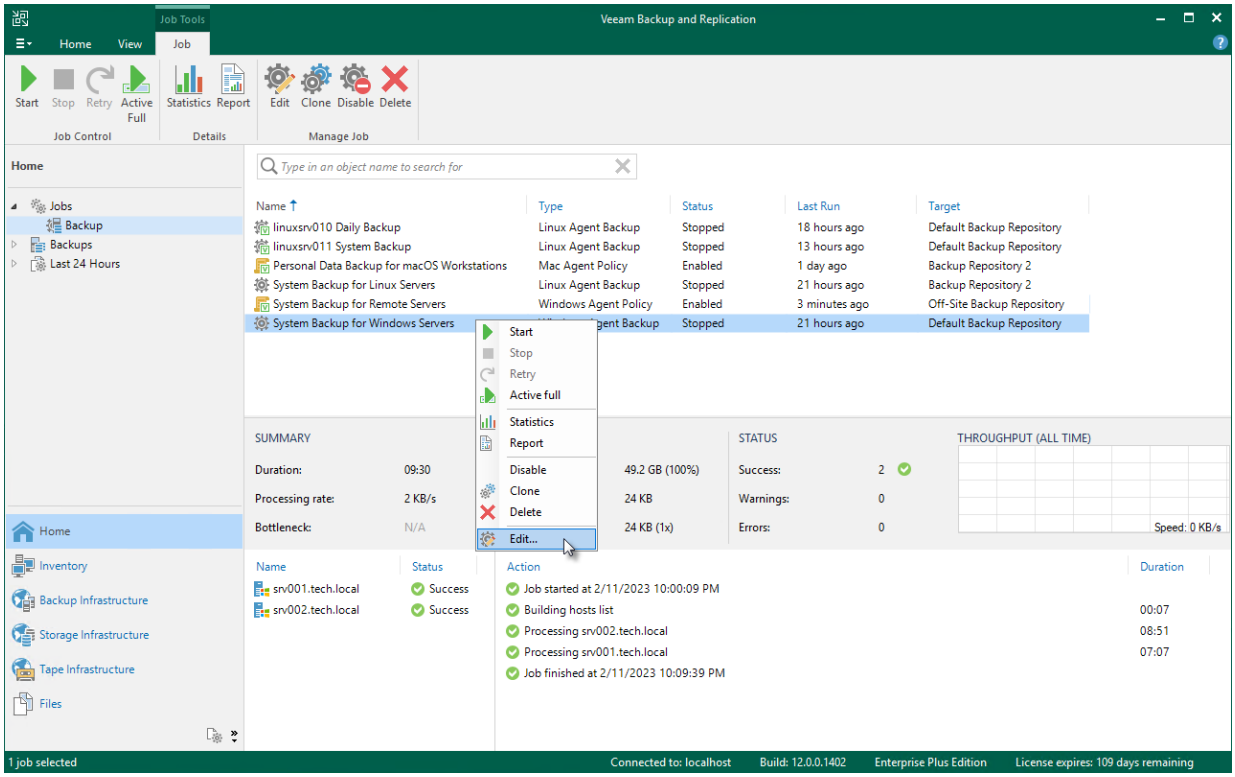
Editing Veeam Agent Backup Job Settings

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).
> - [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.



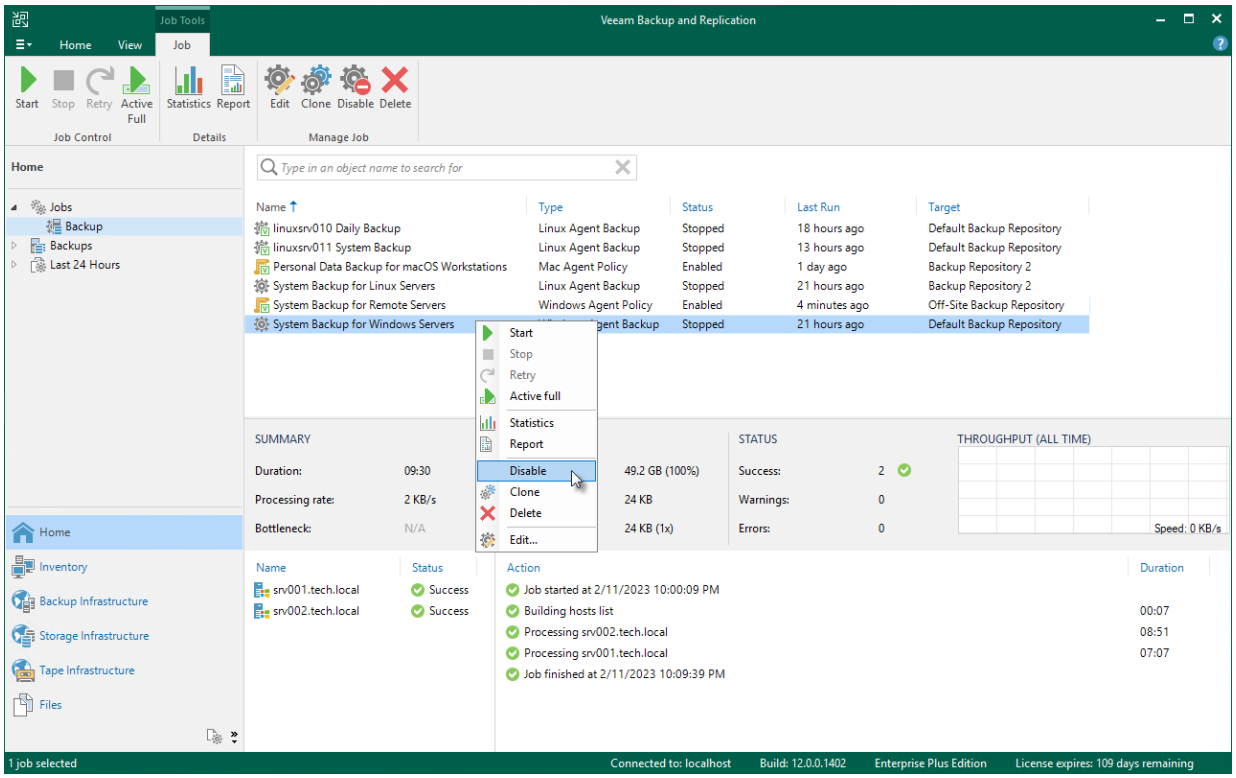
Enabling and Disabling Veeam Agent Backup Job

You can temporary 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.



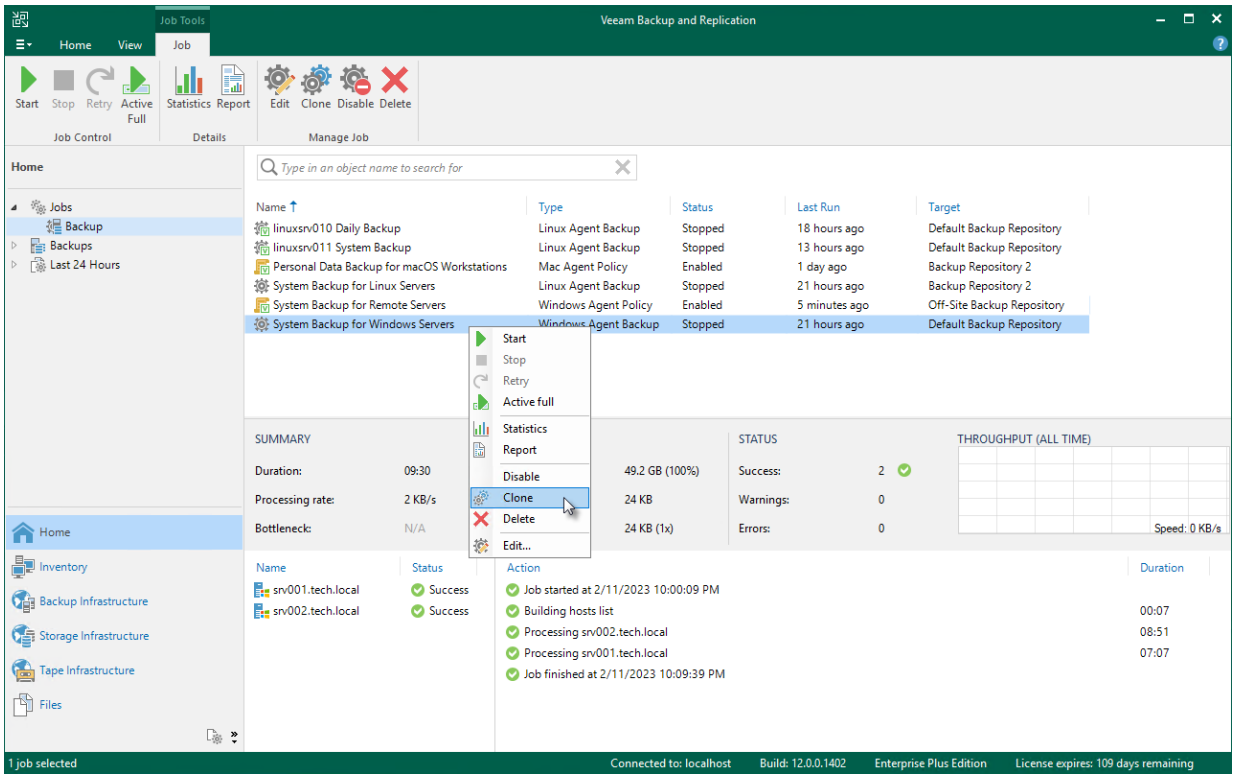
Cloning Veeam Agent Backup Job

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.

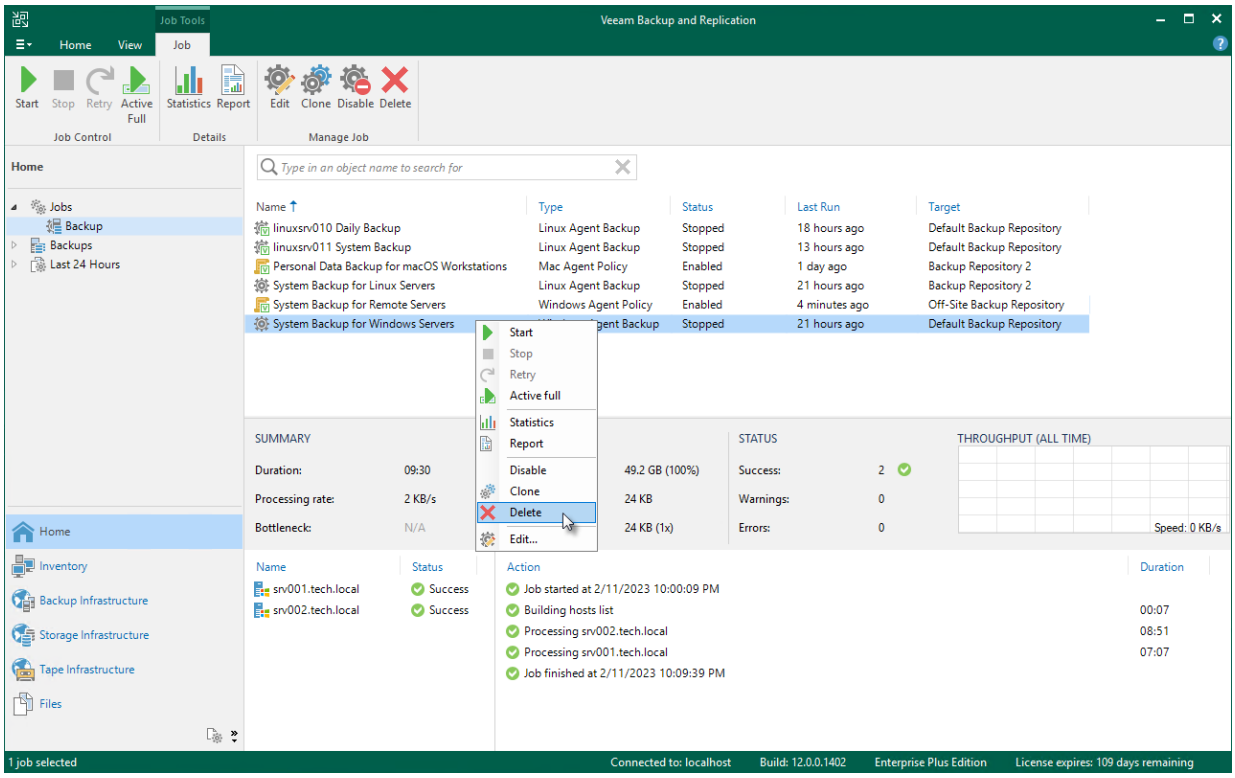


Removing Veeam Agent Backup Job

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** > **Orphaned** 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 job managed by Veeam Agent (a Veeam Agent backup policy):

- 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.

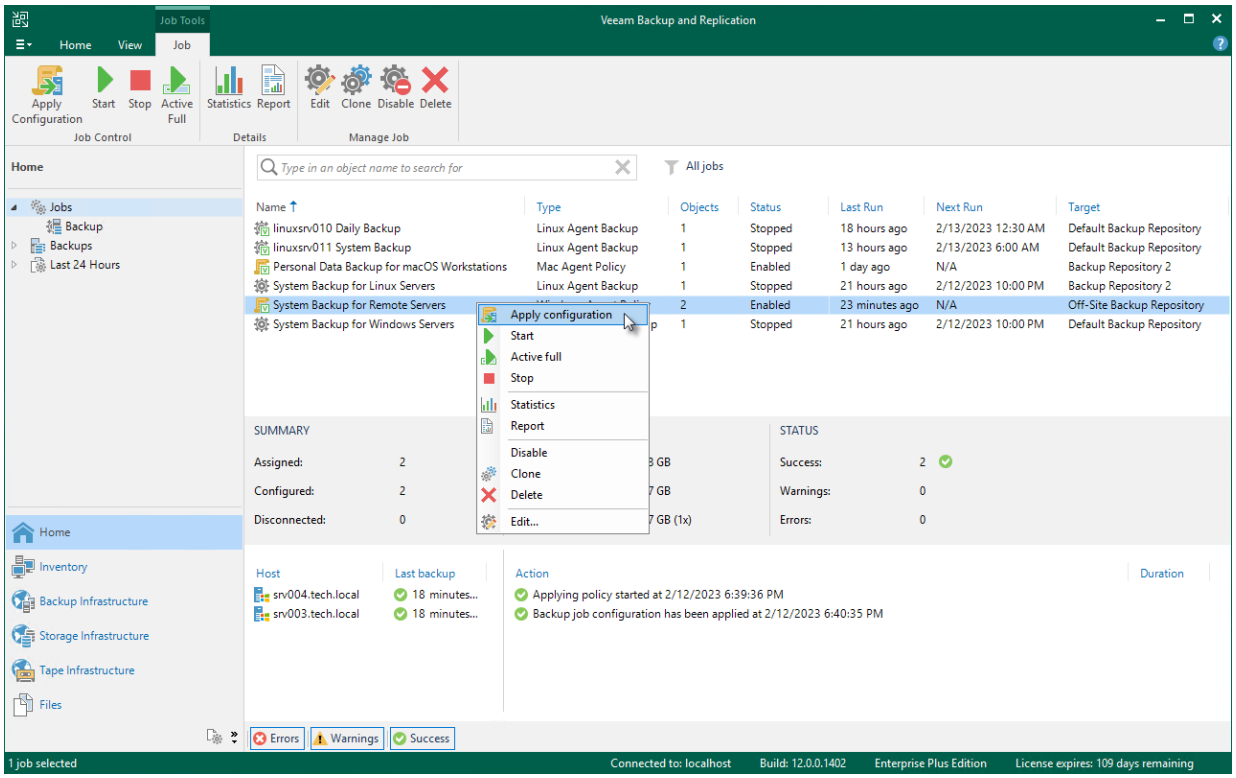
To assign a backup policy to protected computers:

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**.

   Keep in mind that Veeam Backup & Replication does not apply backup policy to protection groups for pre-installed Veeam Agents and their members immediately. Veeam Agents installed on computers included in such protection groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If a backup policy is targeted at the Veeam backup server and the backup policy session is scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next session start.

If you want to apply backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see one of the following sections depending on the Veeam Agent you use:

- Veeam Agent for Microsoft Windows Configuration
- Veeam Agent for Linux Configuration
- Veeam Agent for Unix Configuration
- Veeam Agent for Mac 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 the backup process for a backup policy, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to start backup jobs on these computers.

When you stop the backup process for a backup policy, Veeam Backup & Replication does not apply the policy to Veeam Agent computers and immediately sends a command to 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 start or stop operation will be performed only on those computers that received the command from the backup server.

Keep in mind that you cannot start or stop the backup process for protection groups for pre-installed Veeam Agents and their members. Veeam Agent computers included in such protection groups will be skipped and Veeam Backup & Replication will display a warning message in a backup policy session statistics.

Starting Backup

To start backup on Veeam Agent computers added to the backup policy:

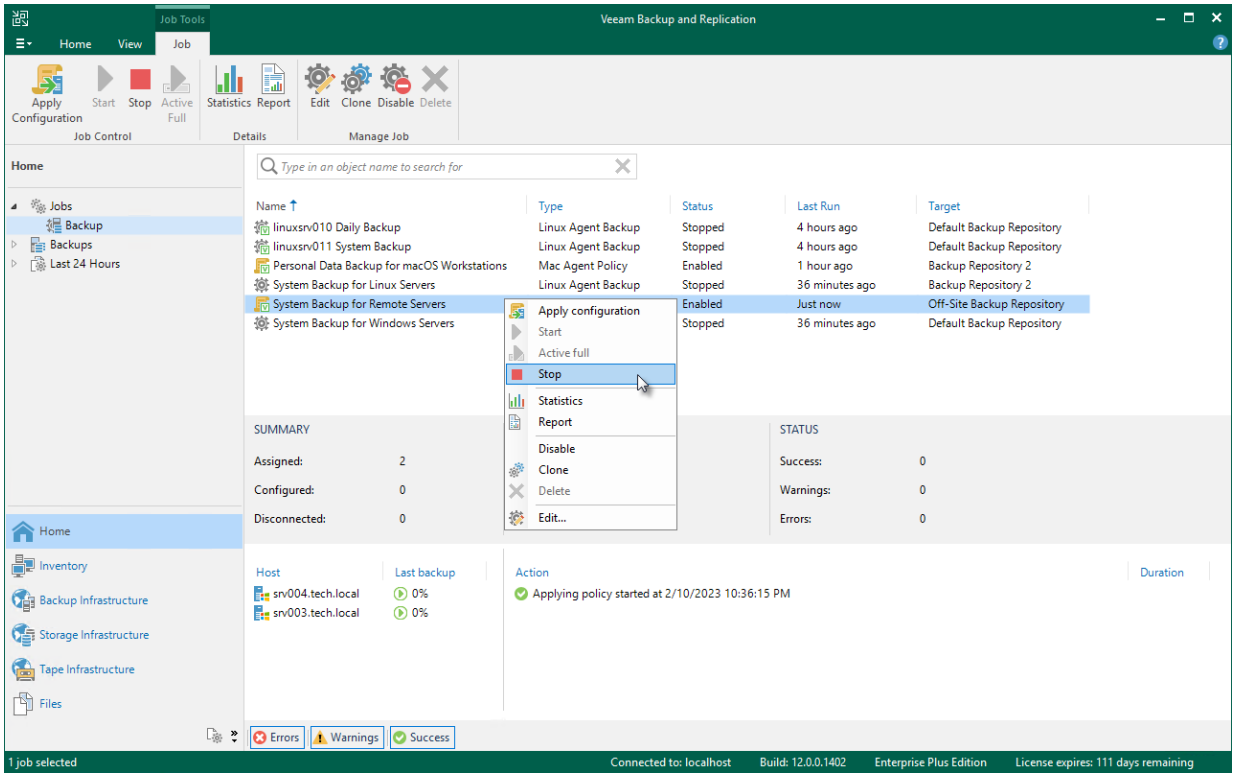
1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the backup policy and click **Start** on the ribbon or right-click the job and select **Start**.

> **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** on the ribbon or right-click the job and select **Stop**. 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.

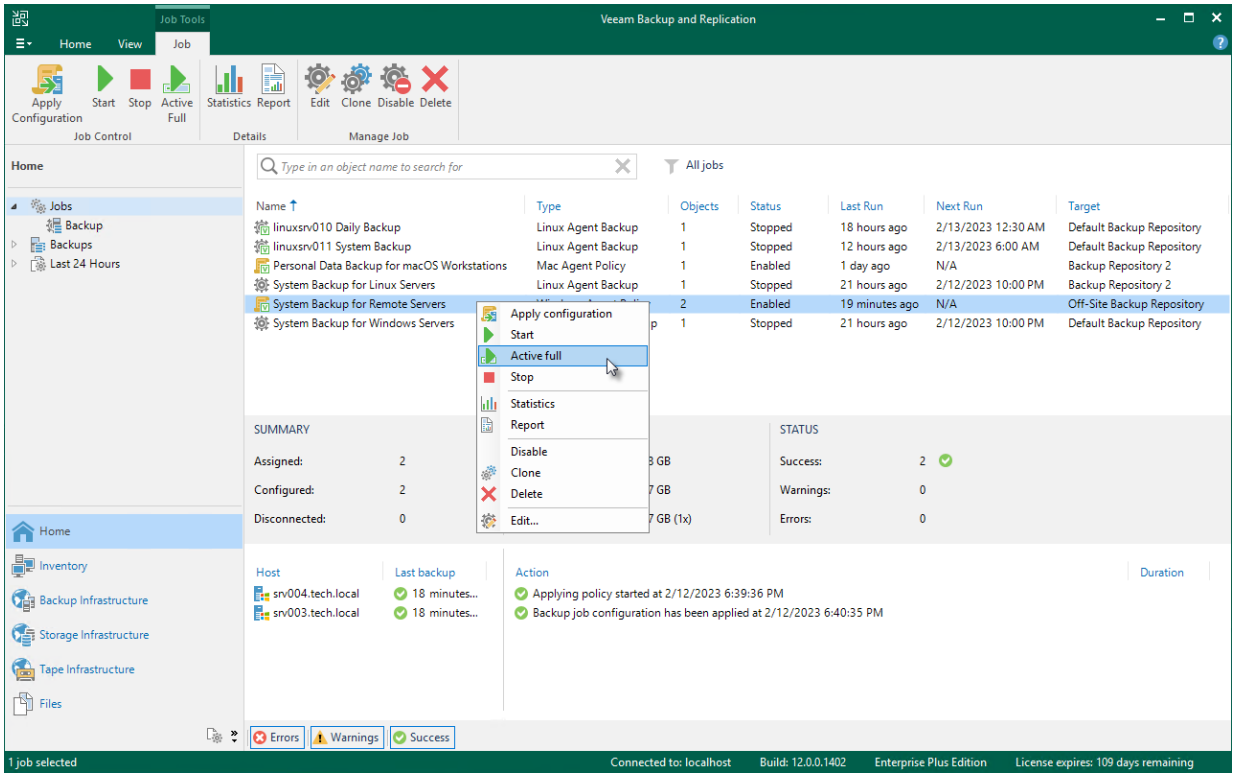
When you start active full backup for a backup policy, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to perform active full backup on these computers. Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time 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.

Keep in mind that you cannot start active full backup for protection groups for pre-installed Veeam Agents and their members. Veeam Agent computers included in such protection groups will be skipped and Veeam Backup & Replication will display a warning message in a backup policy session statistics.

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 policy and select **Active full**.

> **TIP**
>
> You can also create a full backup of an individual computer added to the backup policy. To learn more, see Performing Active Full Backup for Individual Computer.

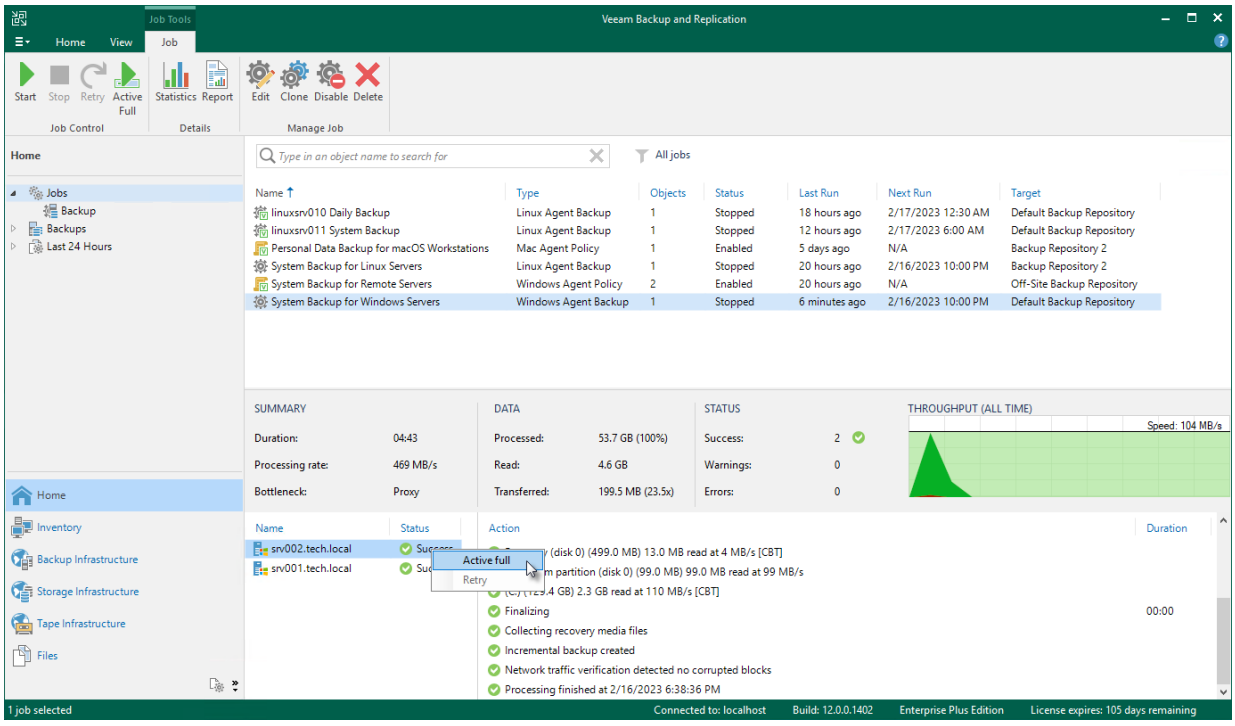


Performing Active Full Backup for Individual Computer

To create an active full backup for an individual computer:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup policy
4. In the bottom part of Veeam Backup & Replication, find the list of computers that are processed by the selected backup policy. In the list, right-click the computer and click **Active full**.

   Keep in mind the following you will be able to create an active full backup for another computer in the same job only after active full backup is created for the selected computer.



Clearing Backup Cache

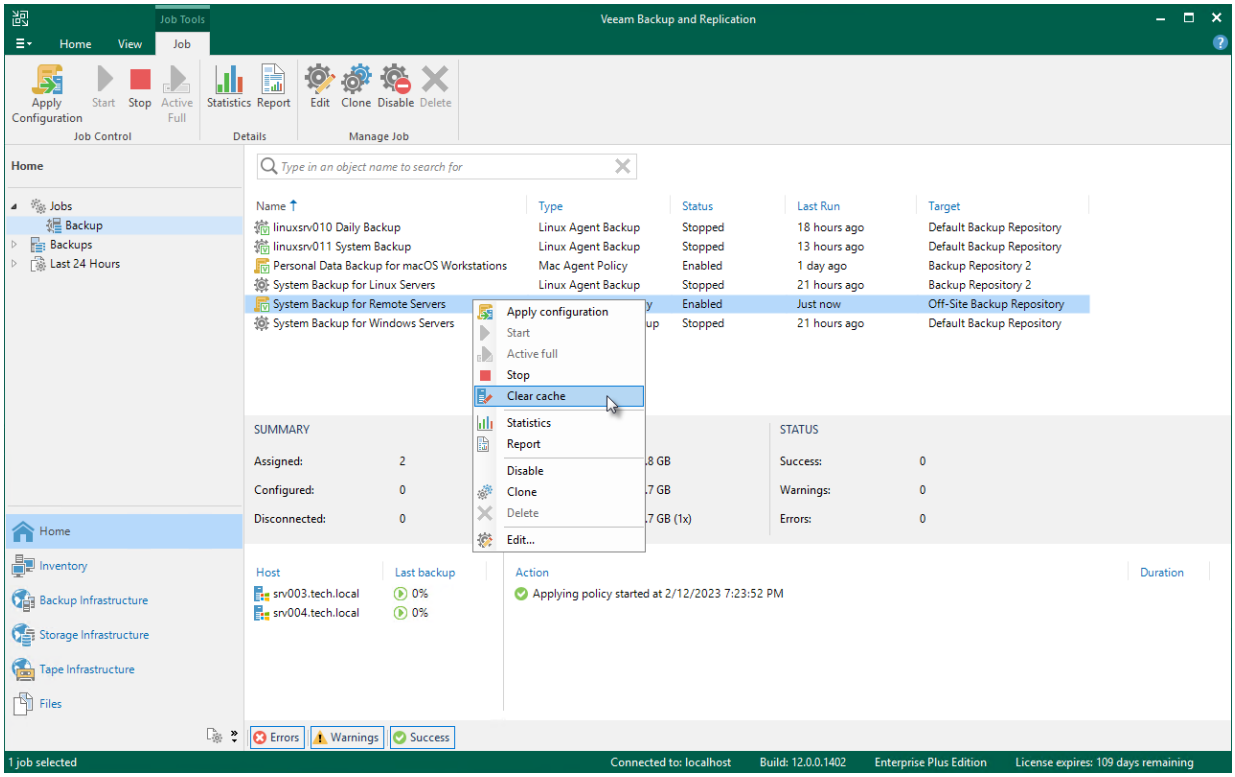
You can use the Veeam backup console to delete restore points from the backup cache on computers added to the backup policy. This operation may be required, for example, if the backup cache contains one or more restore points, and the backup chain in the target location has changed prior to the time when Veeam Agent for Microsoft Windows starts uploading restore points to the target location.

Keep in mind that the clear cache operation is available only for computers that are protected with Veeam Agent for Microsoft Windows and are members of any protection group excluding protection group for pre-installed Veeam Agents.

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**.



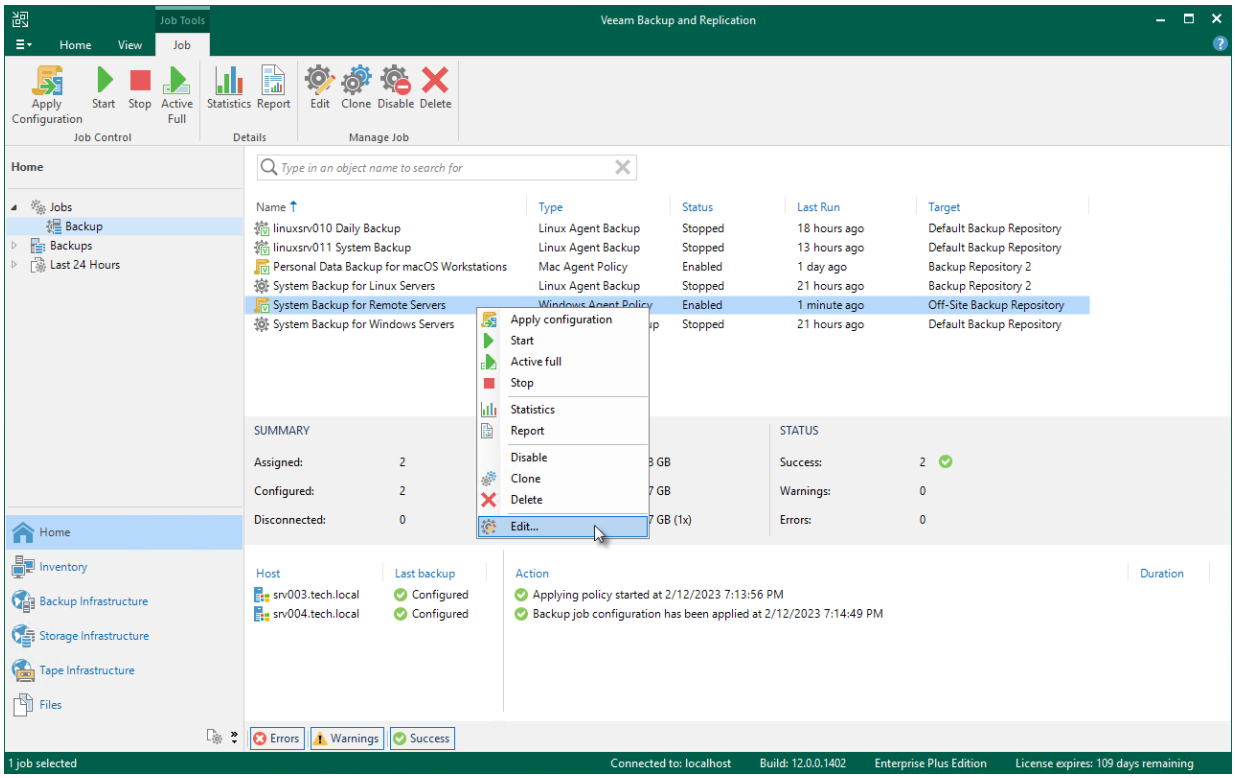
Editing Backup Policy Settings

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 temporary 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.

To disable a Veeam Agent backup policy:

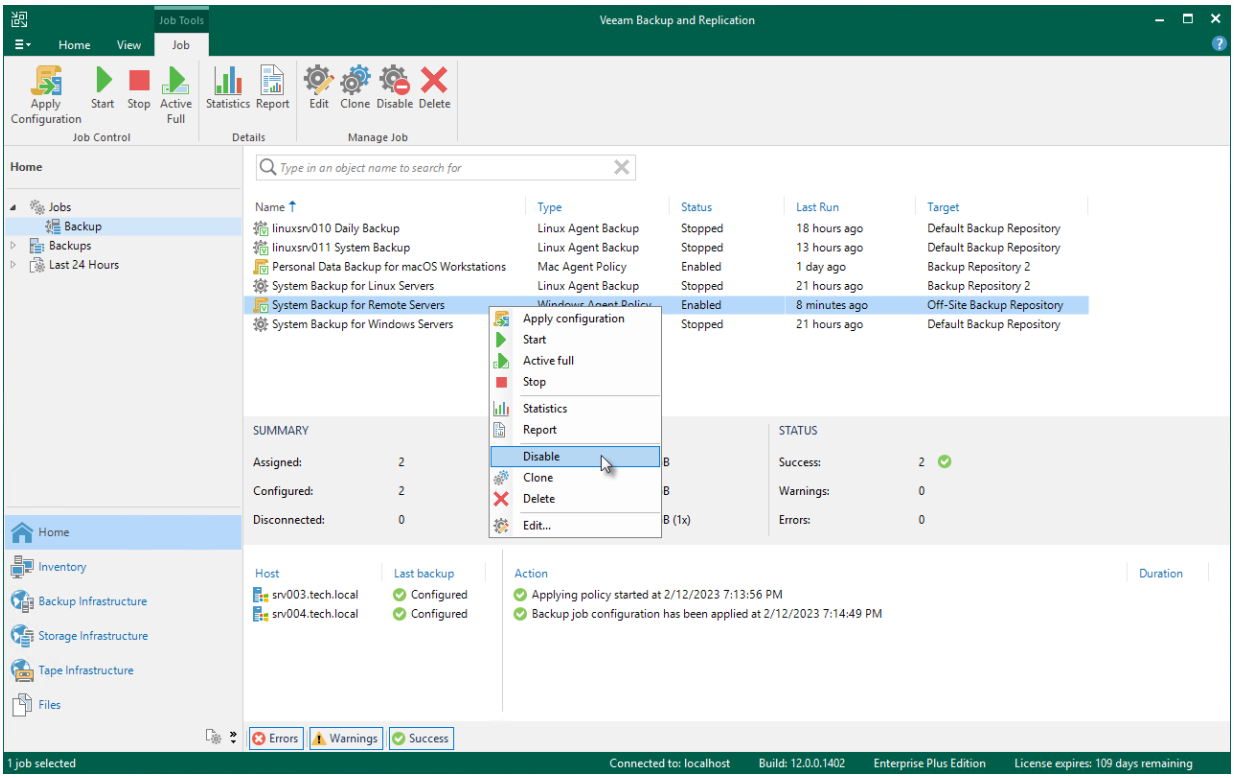
1. Open the **Home** view.
2. In the inventory pane, select **Jobs**.
3. In the working area, select the Veeam Agent backup policy and click **Disable** on the ribbon or right-click the policy and select **Disable**.

   Keep in mind that Veeam Backup & Replication does not immediately disable a backup policy for protection groups for pre-installed Veeam Agents and their members. Veeam Agents installed on computers included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy settings. If a backup policy is targeted at the Veeam backup server and the next backup policy session is scheduled earlier than the next connection to Veeam Backup & Replication, this backup policy will get updated backup policy settings at the next session start.

   If you disabled a backup policy in the Veeam Backup & Replication console and this backup policy starts a new backup session targeted at the Veeam backup server before the next connection to Veeam Backup & Replication, this backup session and all automatic retries of this session will fail.

   If you want to disable backup policy immediately, you must synchronize Veeam Agent with Veeam Backup & Replication from the Veeam Agent computer side manually. To learn more, see Veeam Agent for Microsoft Windows Configuration, Veeam Agent for Linux Configuration, or Veeam Agent for Mac Configuration.

To enable a disabled policy, select it in the list and click **Disable** on the ribbon once again.



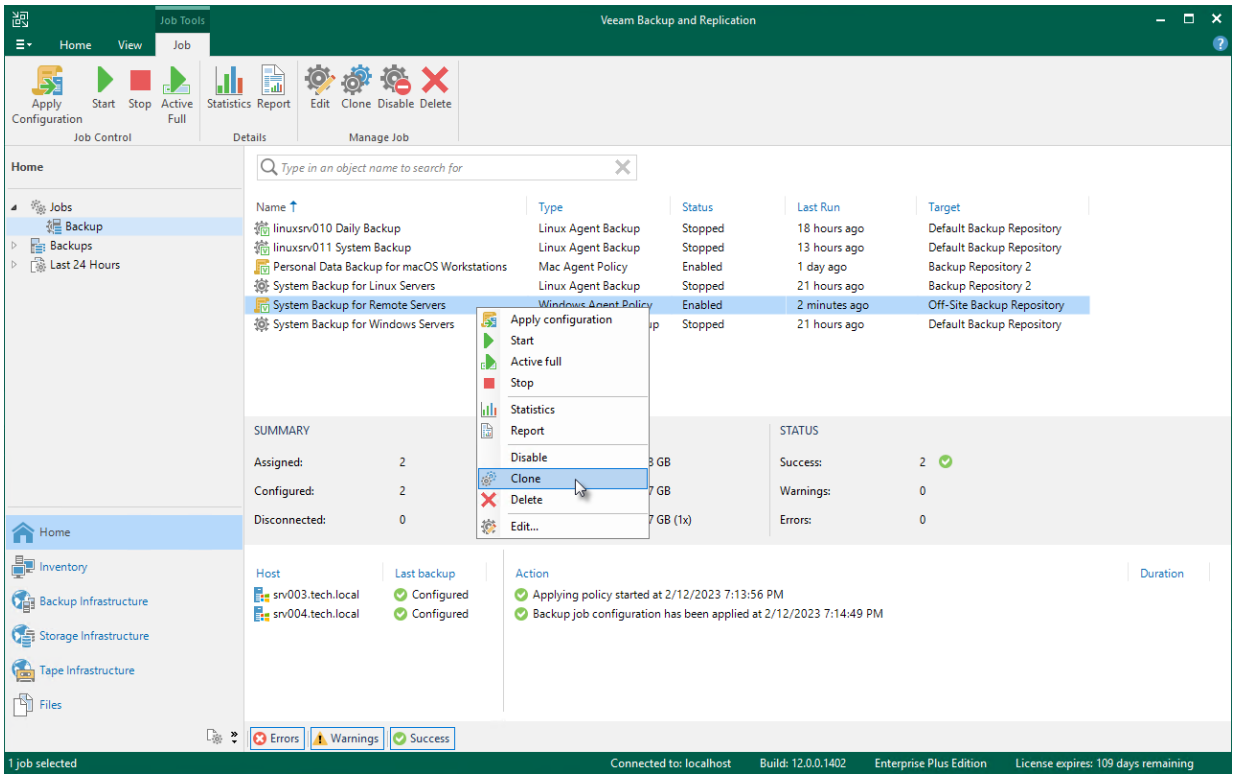
Cloning Backup Policy

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.

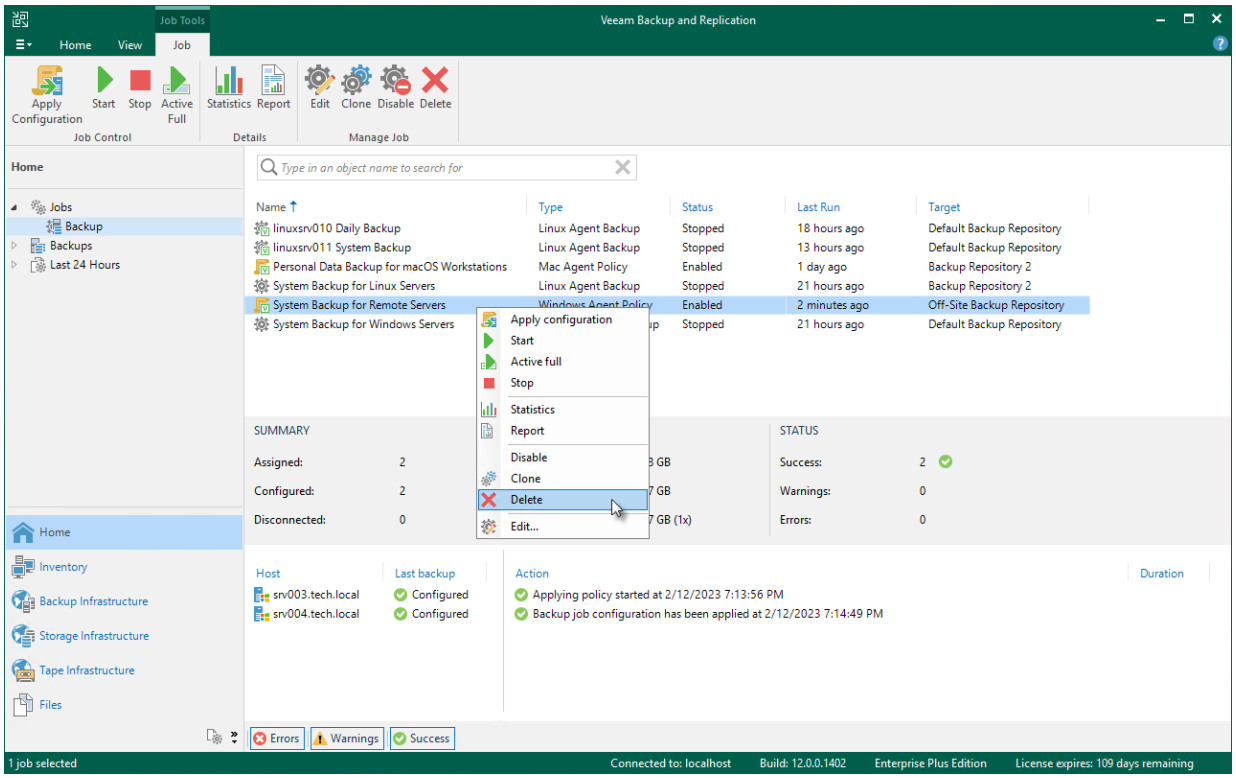


Removing Backup Policy

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

> **IMPORTANT**
>
> A protection group for pre-installed Veeam Agents offers a limited set of operations to manage protected computers. To learn more, see Managing Protected Computers With Pre-Installed Veeam Agents.

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.
- Remove a computer from a protection group.
- 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.

Managing Protected Computers with Pre-Installed Veeam Agents

A protection group for pre-installed Veeam Agents offers a limited set of operations to manage protected computers. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

For Veeam Agent computers added to the protection group for pre-installed Veeam Agents, you can perform the following operations:

- Move an unmanaged computer to a protection group.
- Add a protected computer to a Veeam Agent backup job.
- View properties of 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.

Keep in mind, that you can move an unmanaged Veeam Agent computer only to a protection group that includes individual computers and a protection group for pre-installed Veeam Agents:

- In case of the protection group that includes individual computers, you can move unmanaged computer using the Veeam Backup & Replication console.
- In case of the protection group for pre-installed Veeam Agents, you can move unmanaged computer only from the Veeam Agent side. This operation is similar to the initial Veeam Agent configuration. To learn more, see one of the following sections depending on the Veeam Agent that is installed on the computer you plan to move:
  - Veeam Agent for Microsoft Windows Configuration
  - Veeam Agent for Linux Configuration
  - Veeam Agent for Unix Configuration
  - Veeam Agent for Mac Configuration

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

- 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.

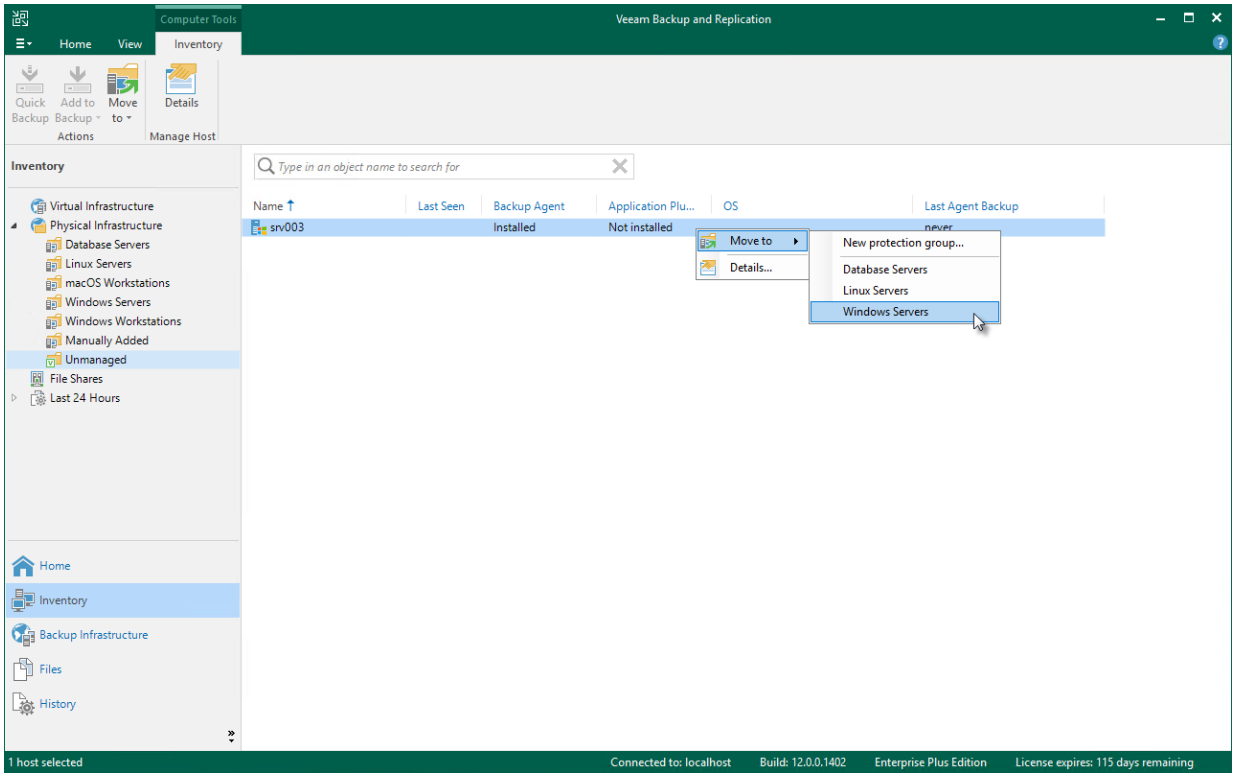
To move an unmanaged computer to a new protection group:

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*.

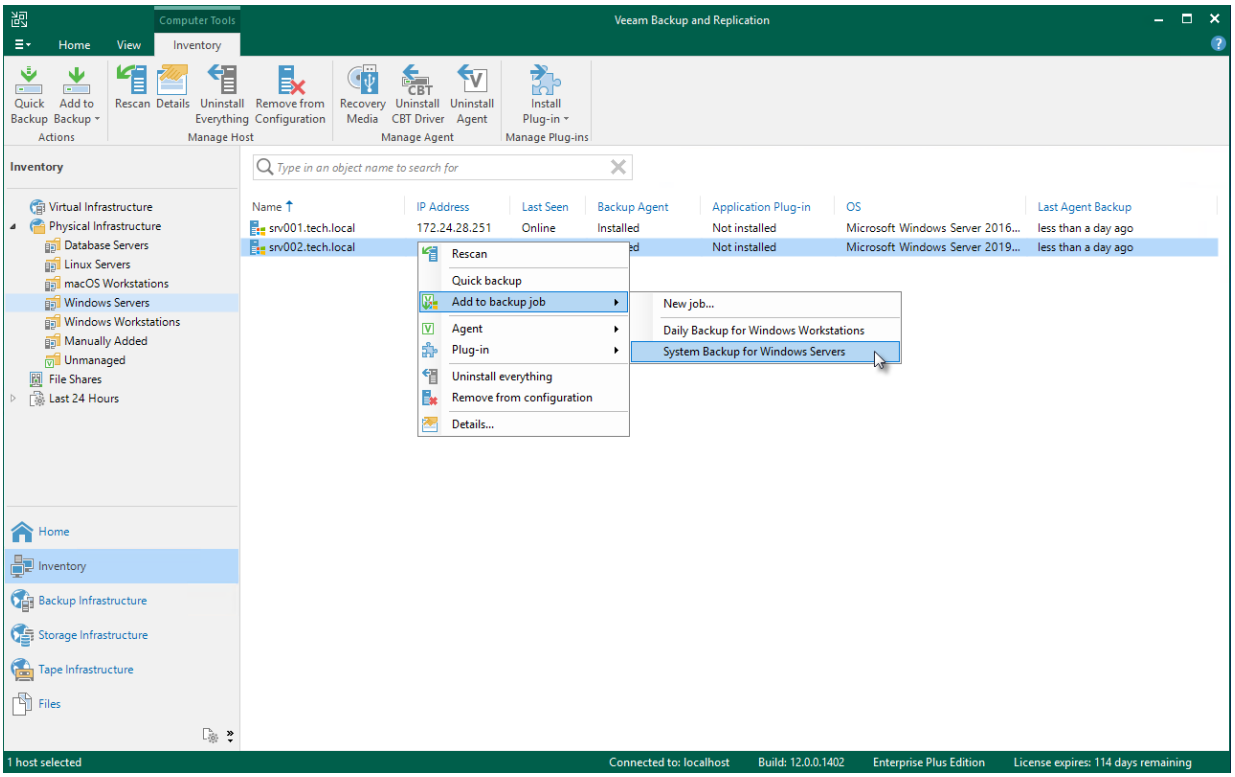


Adding Computer to Backup Job

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:

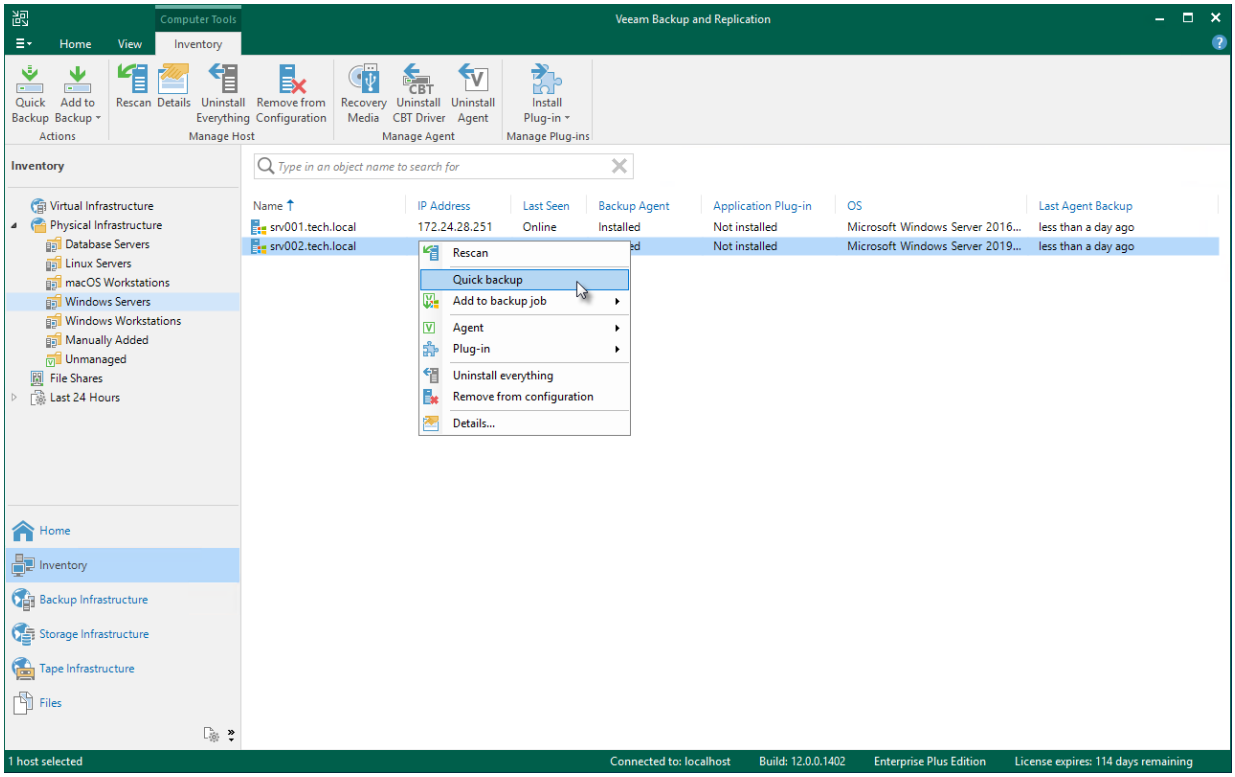
- A protected computer is added to a Veeam Agent backup job managed by the backup server.
- A full backup file for the protected computer exists on the backup repository configured in the backup infrastructure.

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

  Keep in mind that IP address is not available for members of a protection group for pre-installed Veeam Agents and a protection group for cloud machines.
- Fingerprint (for computers running a Linux OS)

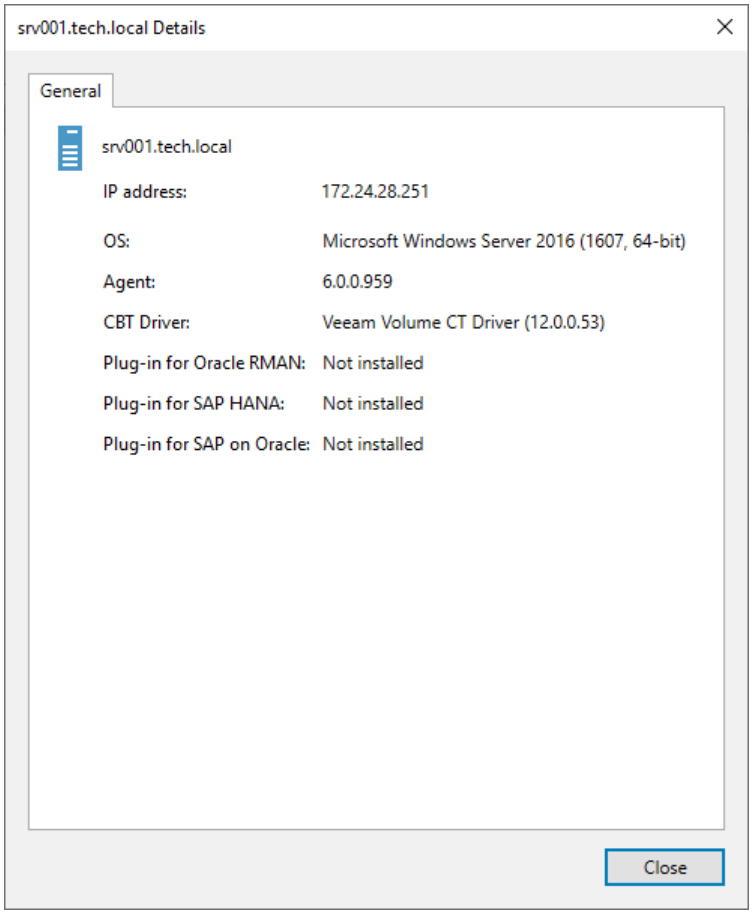
  Keep in mind that IP address is not available for members of a protection group for cloud machines.
- Key algorithm (for computers running a Linux OS)

  Keep in mind that IP address is not available for members of a protection group for cloud machines.
- 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**.



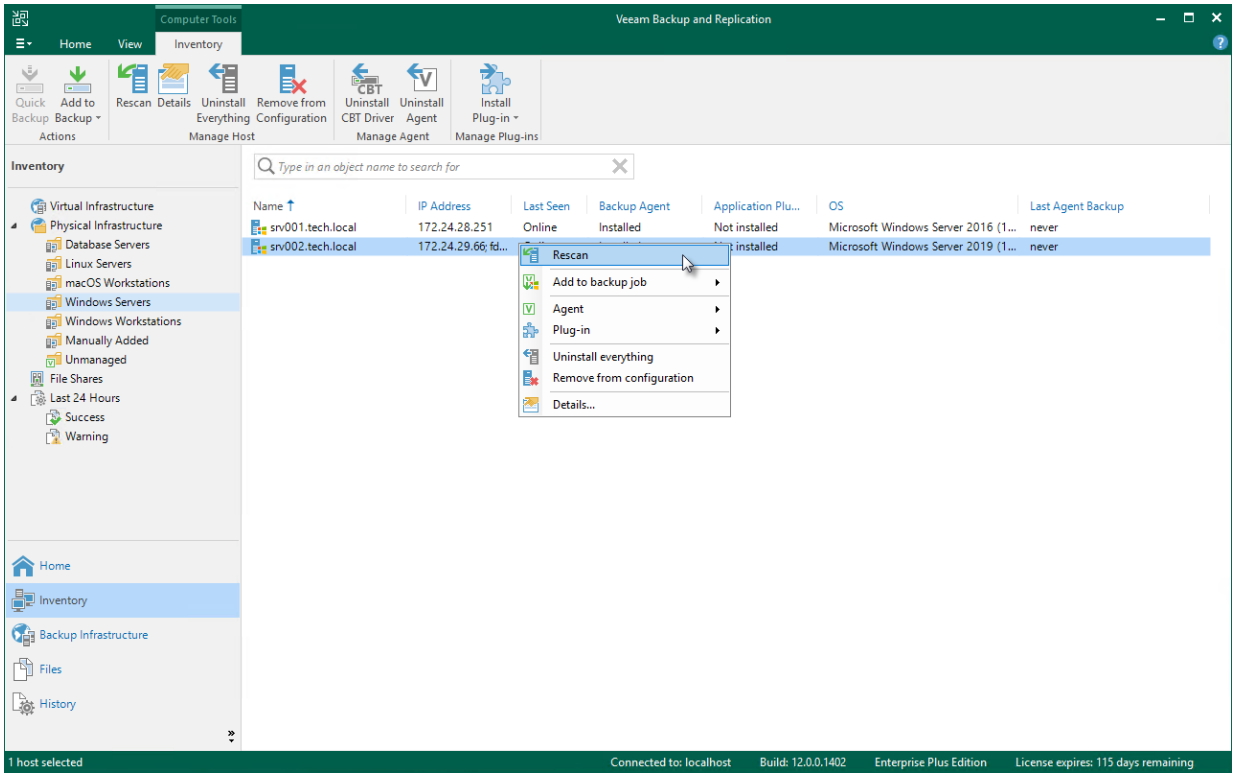
Rescanning Protected Computer

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.

Keep in mind that rescan is not available for protection groups for pre-installed Veeam Agents and their members. Veeam Agents installed on computers included in such protection groups connect to Veeam Backup & Replication every 6 hours and provide information about the Veeam Agent computer.

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**.



Managing Veeam Agent

You can use the backup console to manage the following Veeam Agents on a specific computer in the inventory:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux

Keep in mind that Veeam Agents for computers that you plan to add to a protection group for pre-installed Veeam Agents require a different installation approach. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

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.

Keep in mind that Veeam Agents for computers that you plan to add to a protection group for pre-installed Veeam Agents require a different installation approach. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

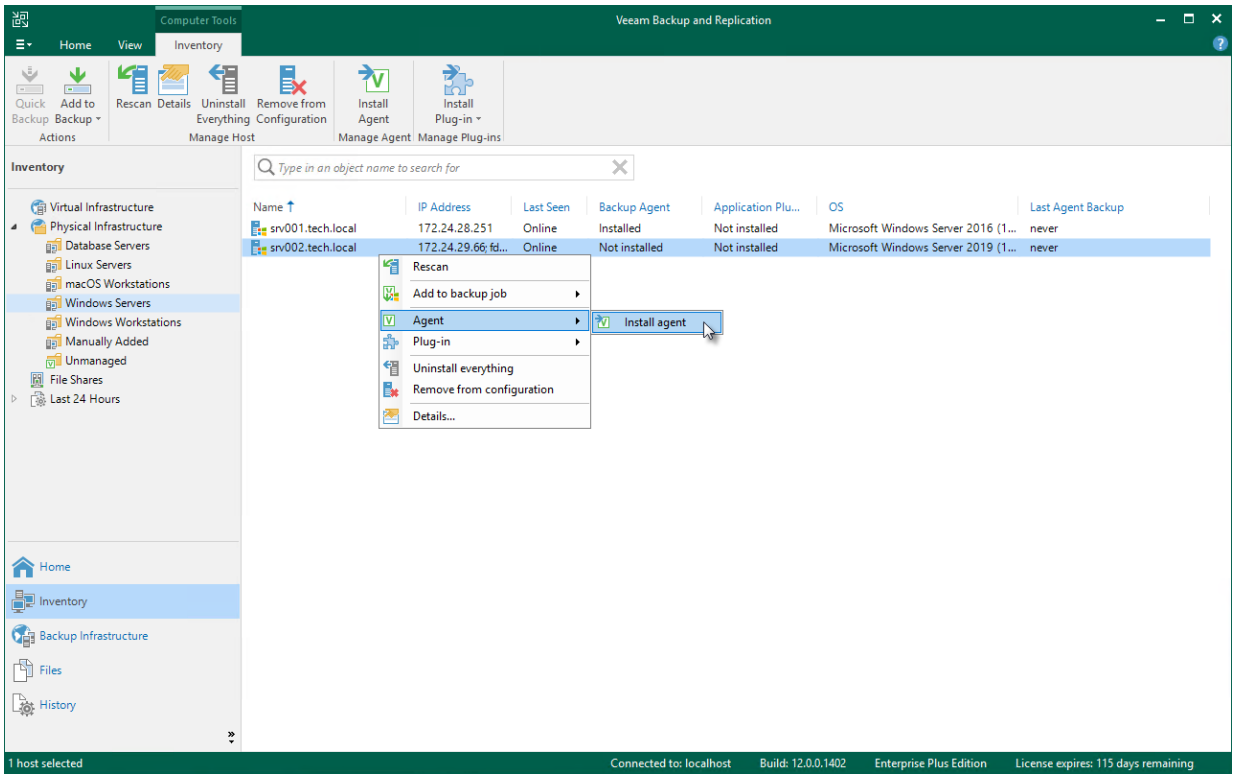
Before you install Veeam Agent, check the following prerequisites:

- 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 agent**.

> **NOTE**
>
> In some cases, installation of Veeam Agent for Microsoft Windows may require computer reboot. This can happen, for example, if you have an earlier version of Microsoft .NET Framework installed on the computer and during the installation process the framework is used by third-party software.



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.

Keep in mind that you can upgrade Veeam Agent on a computer added to a protection group for pre-installed Veeam Agents only from the Veeam Agent computer side. To learn more, see Upgrading from Veeam Agent Side.

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.
- There are no running jobs.

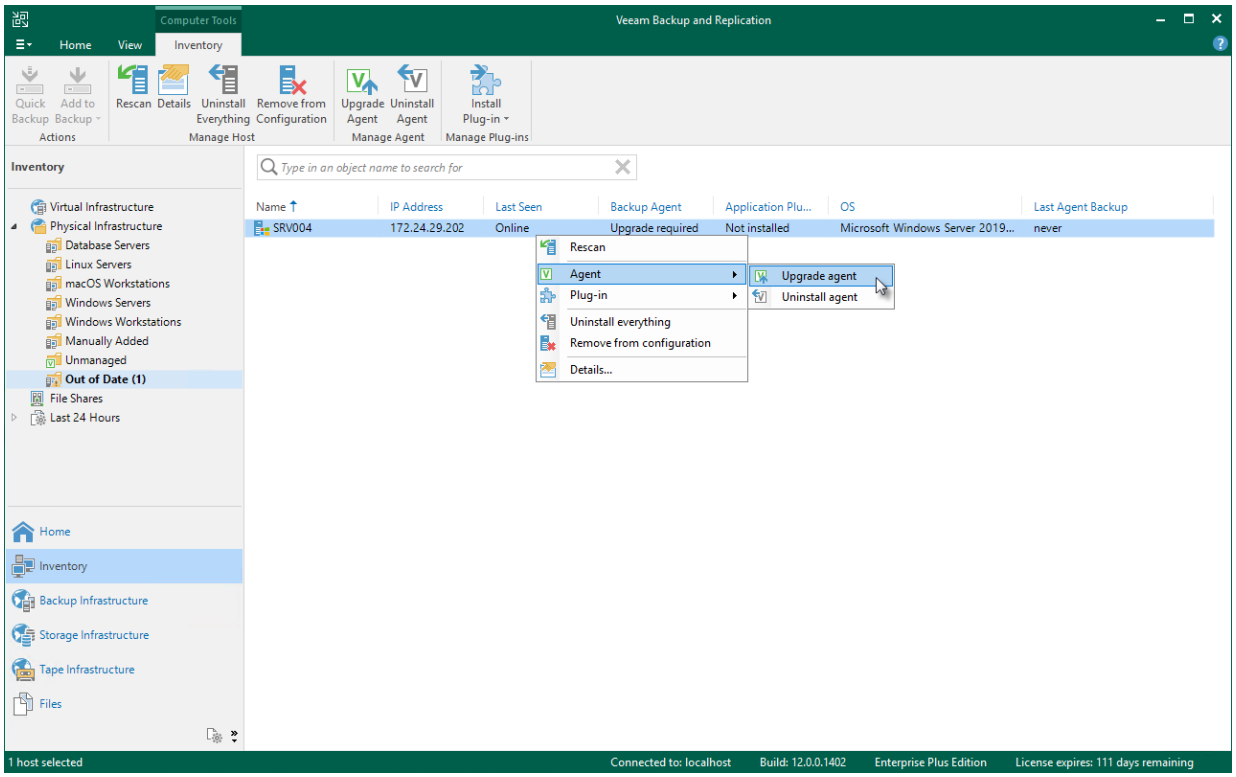
  We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic jobs temporarily to prevent them from starting during the upgrade. If the protected computer runs VSS-aware applications and backup of database logs (Microsoft SQL Server transaction logs or Oracle archived logs) is enabled in the backup job for the computer, disable this backup job too.

> **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 Agent** on the ribbon or right-click the computer and select **Agent** > **Upgrade agent**.

> **NOTE**
>
> In some cases, upgrade to the new version of Veeam Agent for Microsoft Windows may require computer reboot.

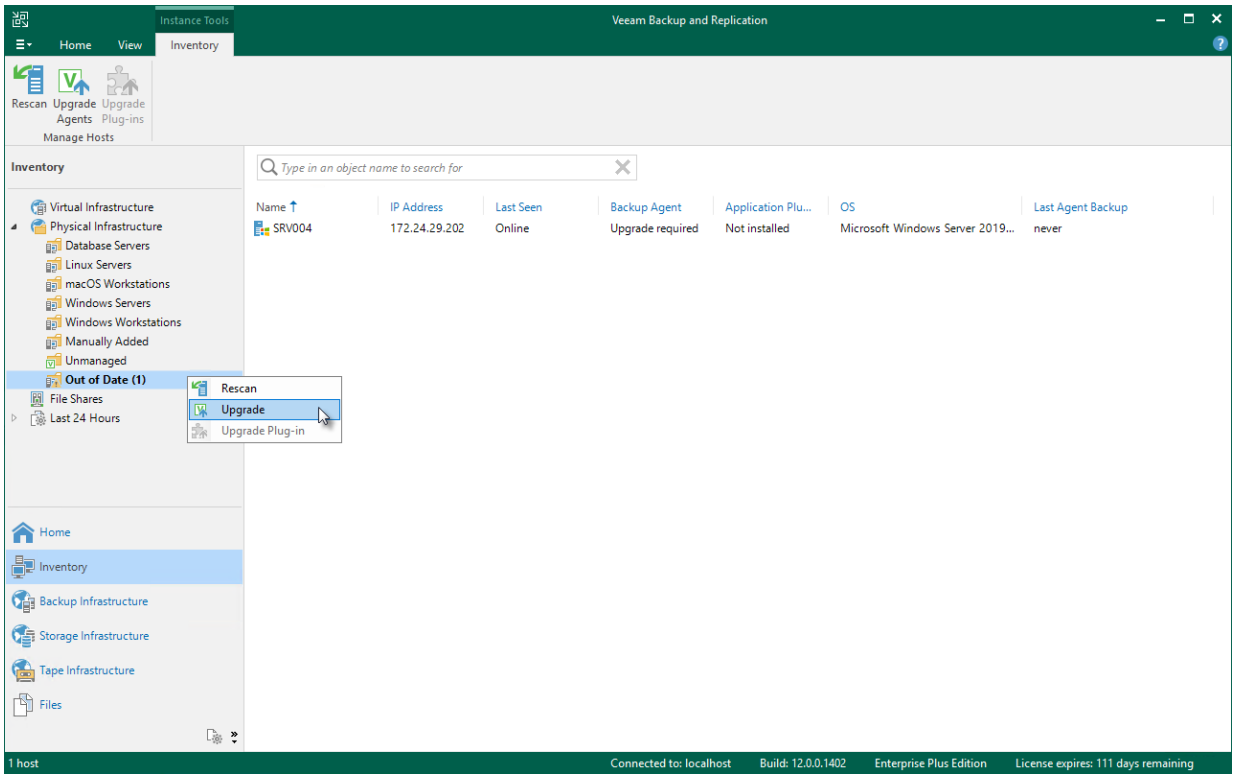


Upgrading Veeam Agent on Multiple Computers

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 Agents** on the ribbon or right-click the **Out of Date** protection group and select **Upgrade**.

> **NOTE**
>
> In some cases, upgrade to the new version of Veeam Agent for Microsoft Windows may require computer reboot.



Upgrading from Veeam Agent Side

You can also upgrade Veeam Agent from the Veeam Agent computer side. This approach is required, for example, for Veeam Agent computers that are added to a protection group for pre-installed Veeam Agents. The process of upgrading differs depending on the Veeam Agent computer OS:

- For Windows-based Veeam Agent computers, see the Upgrading Veeam Agent section in the Veeam Agent for Microsoft Windows User Guide.
- For Linux-based Veeam Agent computers, see the Upgrading Veeam Agent section in the Veeam Agent for Linux User Guide.
- For Unix-based Veeam Agent computers running the IBM AIX operating system, see the Upgrading Product section in the Veeam Agent for IBM AIX User Guide.
- For Unix-based Veeam Agent computers running the Oracle Solaris operating system, see the Upgrading Product section in the Veeam Agent for Oracle Solaris User Guide.
- For macOS-based Veeam Agent computers, see the Upgrading Veeam Agent section in the Veeam Agent for Mac User Guide.

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.

If you work with computer included in a protection group for pre-installed Veeam Agents, you can install and uninstall Veeam CBT driver only from the Veeam Agent computer side. To learn more, see the InstallCBTDriver and UninstallCBTDriver sections in the Veeam Agent Configurator Reference.

Before you install the Veeam CBT driver, check the following prerequisites:

- The protected computer on which you want to install the driver must run one of the following OSes:
  - Microsoft Windows 11 (versions 21H2, 22H2)
  - Microsoft Windows 10 (from version 1803 to version 22H2)
  - Microsoft Windows Server OS that is supported by Veeam Agent. For more information, see System Requirements
- 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 running Microsoft Windows Server 2008 R2 SP1, make sure that update KB3033929 is installed in the OS.

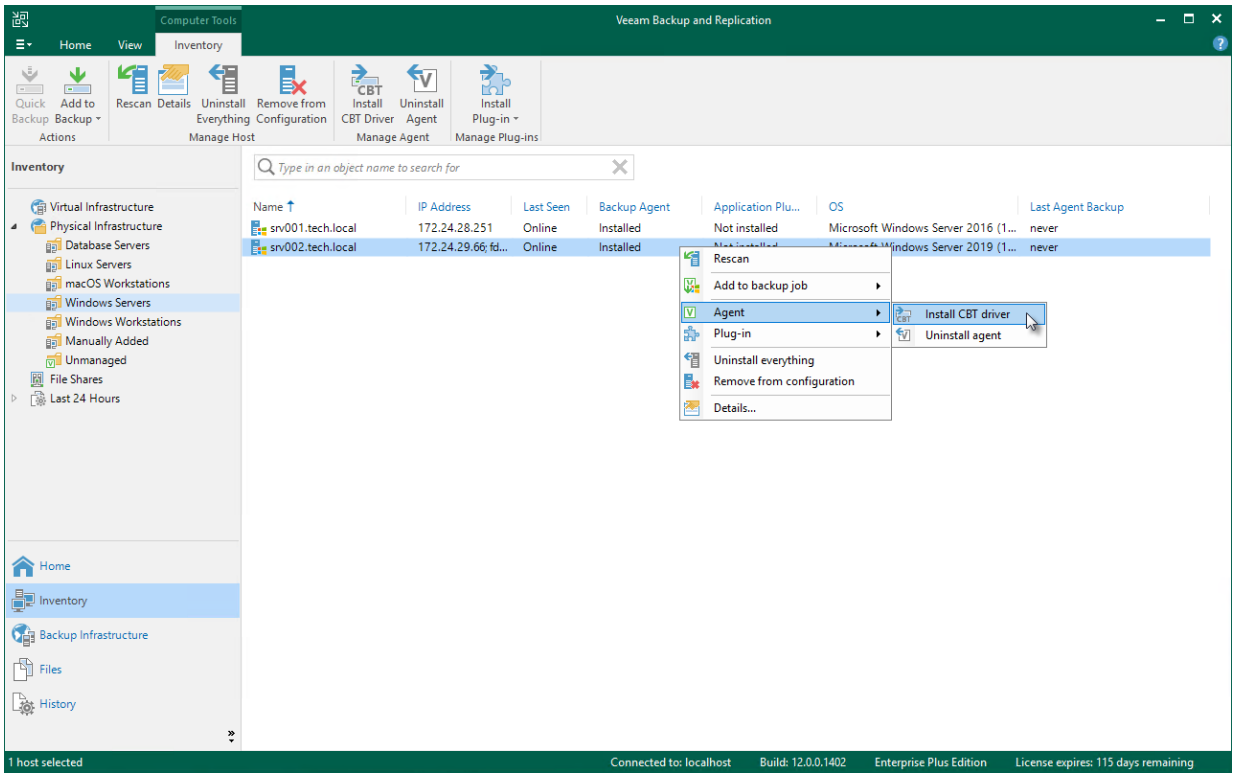
  The update adds the SHA-2 code signing support that is required for verification of the Veeam CBT driver signature. Without this update installed, the OS running on a protected computer will fail to boot after you install the Veeam CBT driver. To learn more, see this Microsoft KB article.
- Do not install the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, 2012 or 2012 R2 if one or more volumes on this computer are encrypted with Microsoft BitLocker (or other encryption tool), or if you plan to use Microsoft BitLocker to encrypt volumes on this computer. Concurrent operation of Microsoft BitLocker and Veeam CBT driver may result in driver failures and may prevent the OS from starting.

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 CBT Driver** on the ribbon or right-click the computer and select **Agent** > **Install CBT driver**.

NOTE

To enable the CBT driver after installation, you need to reboot the computer. To learn more, see Rebooting Protected Computer.

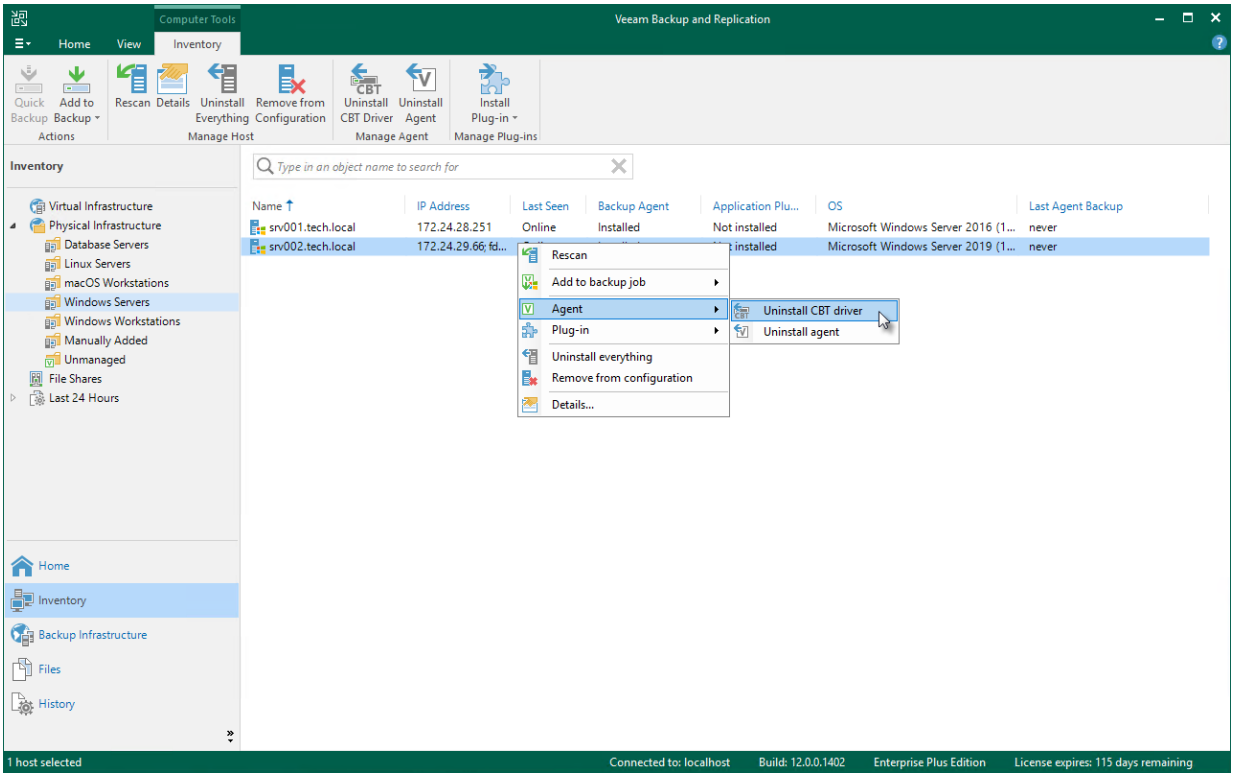


Uninstalling Veeam CBT Driver

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 CBT Driver** on the ribbon or right-click the computer and select **Agent** > **Uninstall CBT driver**.

> **NOTE**
>
> To complete the driver uninstallation process, you need to reboot the computer. To learn more, see Rebooting Protected Computer.



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.

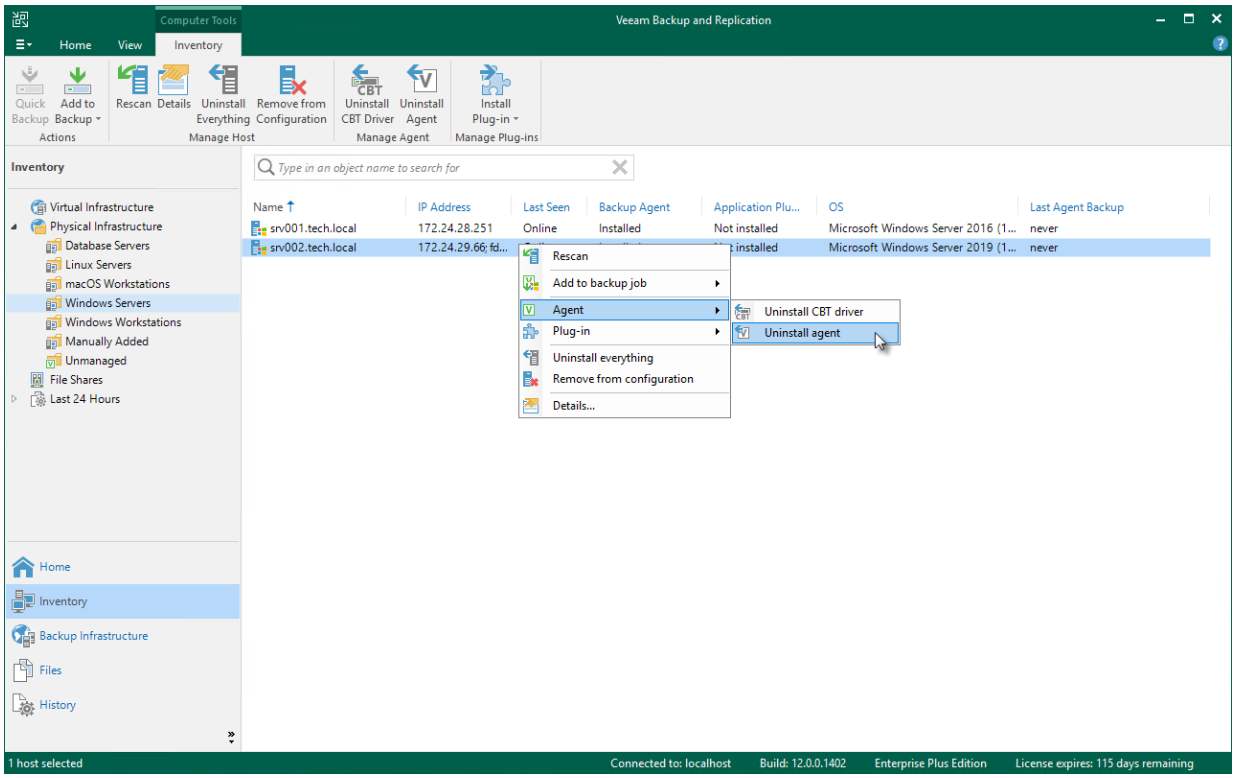
To uninstall Veeam Agent:

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 Agent** on the ribbon or right-click the computer and select **Agent** > **Uninstall agent**.
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.
- If you uninstall Veeam Agent for Microsoft Windows added to the protection group for pre-installed Veeam Agents and then re-install on the same computer, Veeam Agent will not connect to Veeam backup server automatically. To connect Veeam Agent, you must repeat the configuration step of the Veeam Agent deployment scenario. To learn more, see Deploying Veeam Agents Using Generated Setup Files.



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.

Keep in mind that you can create Veeam Recovery Media in Veeam Backup & Replication only for computers that are protected with Veeam Agent for Microsoft Windows.

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

- You can create a Veeam Recovery Media for a protected computer using a copy of a full backup file that meets all the conditions. The copy must be created by a backup copy job. To learn more, see the Backup Copy section in the Veeam Backup & Replication User Guide.
- 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 failover clusters with a registry value. 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

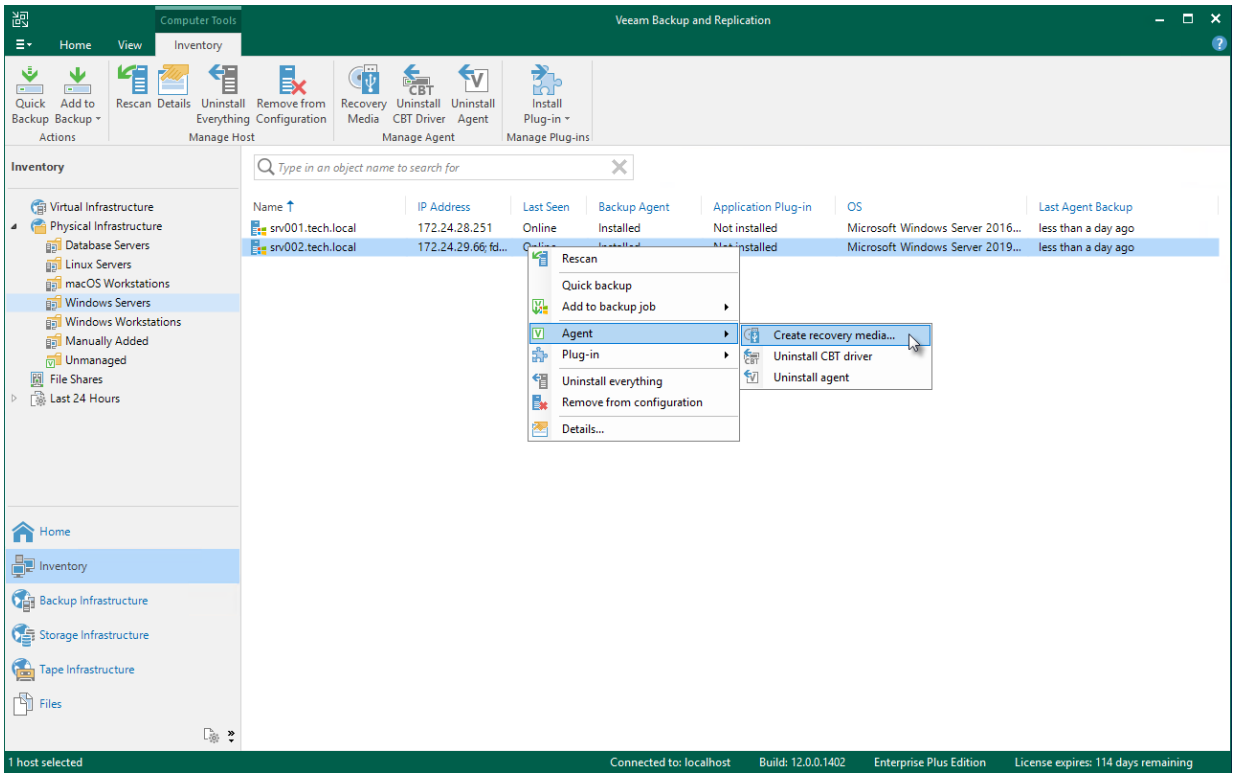
- An empty or re-writable CD/DVD/BD must be inserted into a CD/DVD/BD drive on the computer.
- The CD/DVD/BD must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- [For RW CD/DVD/BD] During the recovery 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.

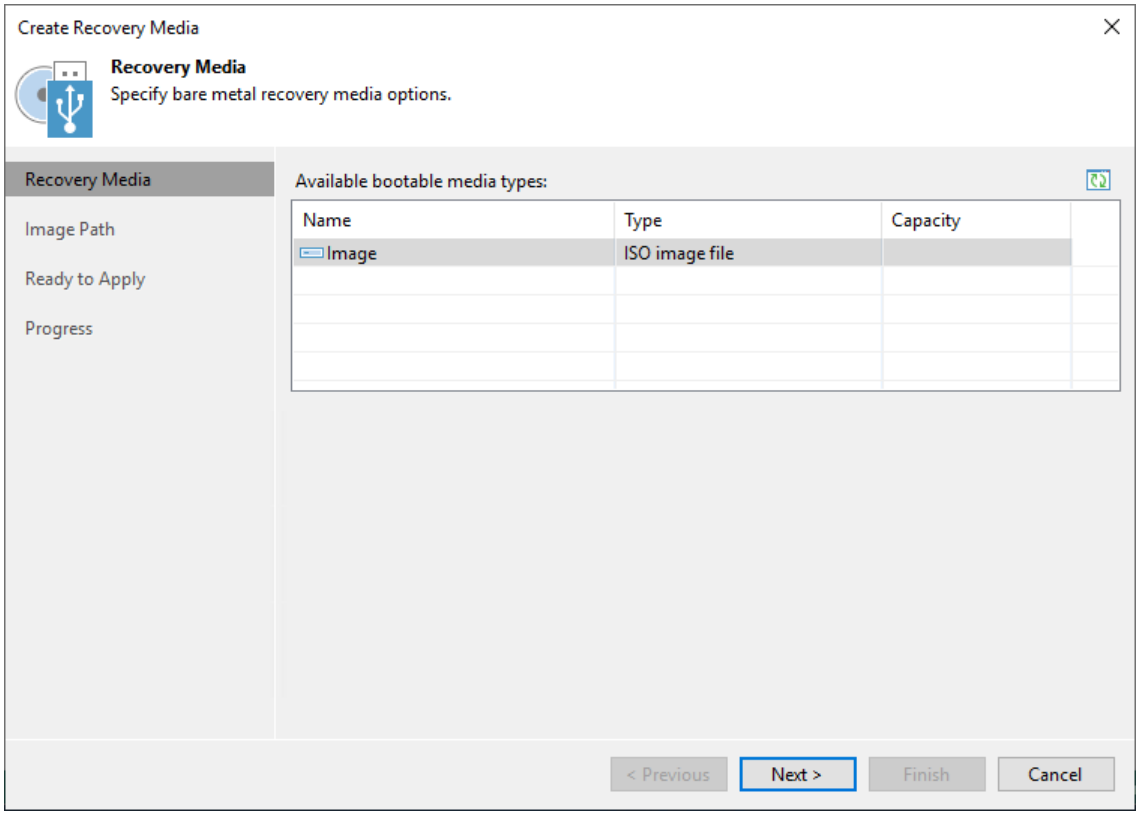


Step 2. Specify Recovery Media Options

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.

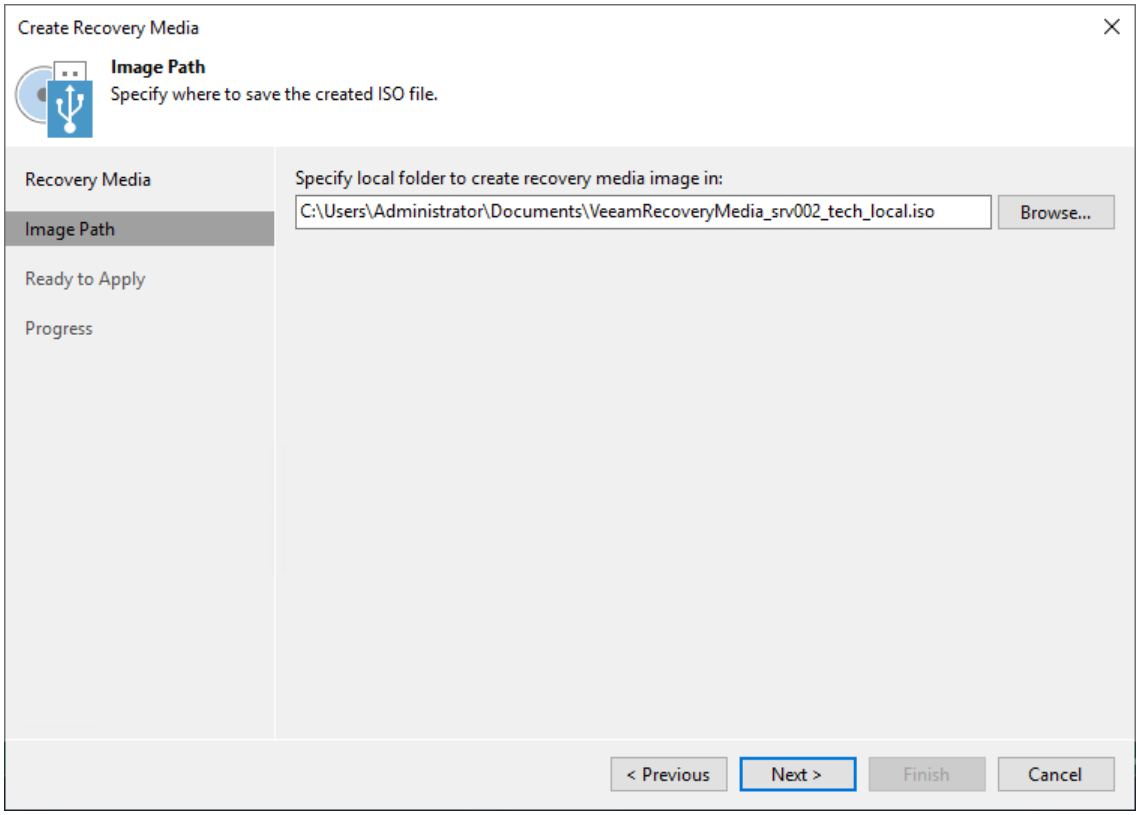
> **NOTE**
>
> When you create a recovery image from the Veeam backup console, you cannot specify additional recovery media options in the same way as when you create a recovery image on the Veeam Agent computer. In this scenario, the recovery image is created with default settings: Veeam Backup & Replication 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.

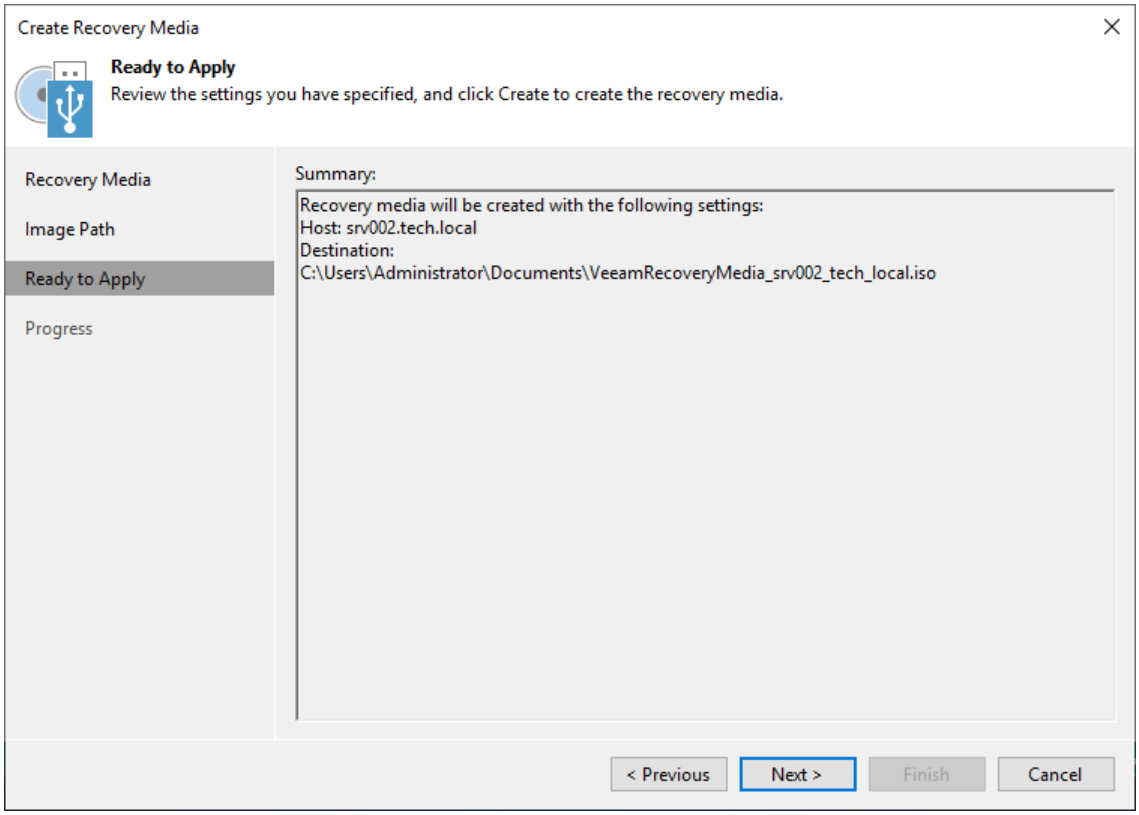
In the **Specify folder to create recovery media image in** field, specify a real path to the folder where you want to save the created recovery image, and the ISO file name. When you create Veeam Recovery Media using the Veeam Backup & Replication console, you can save the ISO file on the local drive 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.



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**.

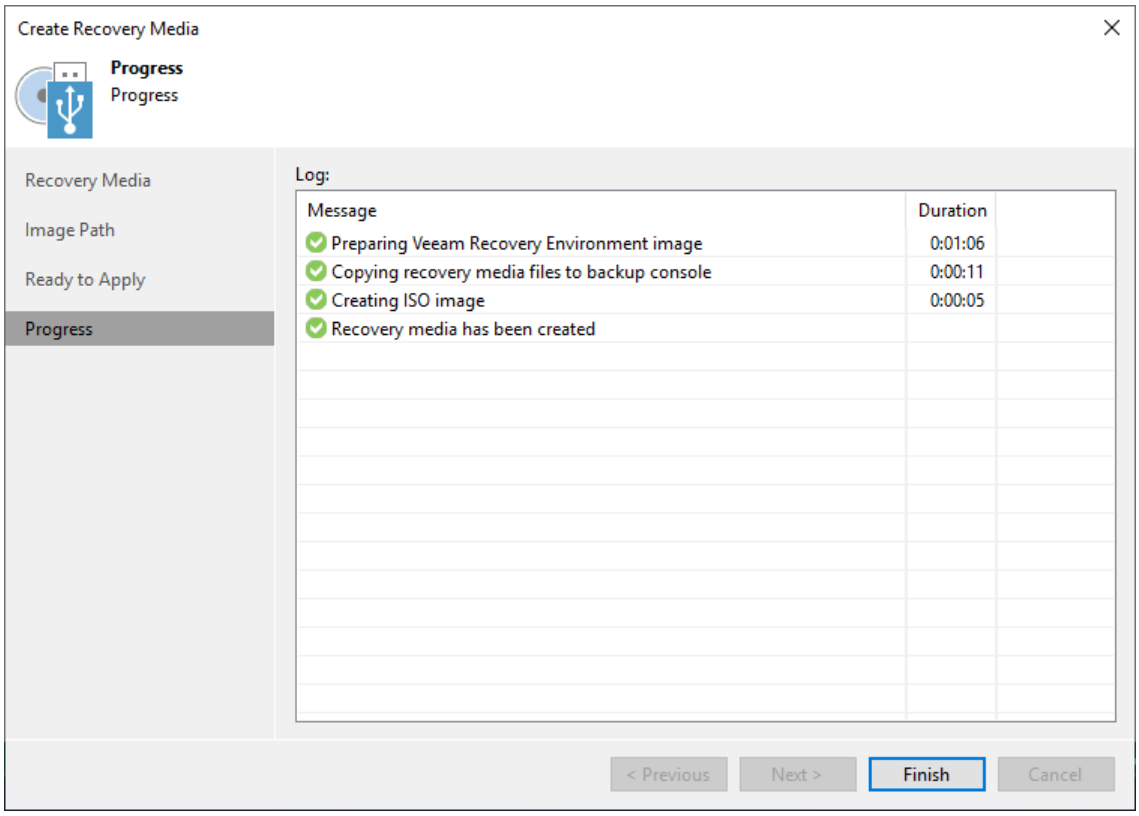
Veeam Backup & Replication will collect data necessary for recovery image creation and write the resulting recovery image to the specified target.



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.



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.

Rebooting Protected Computer

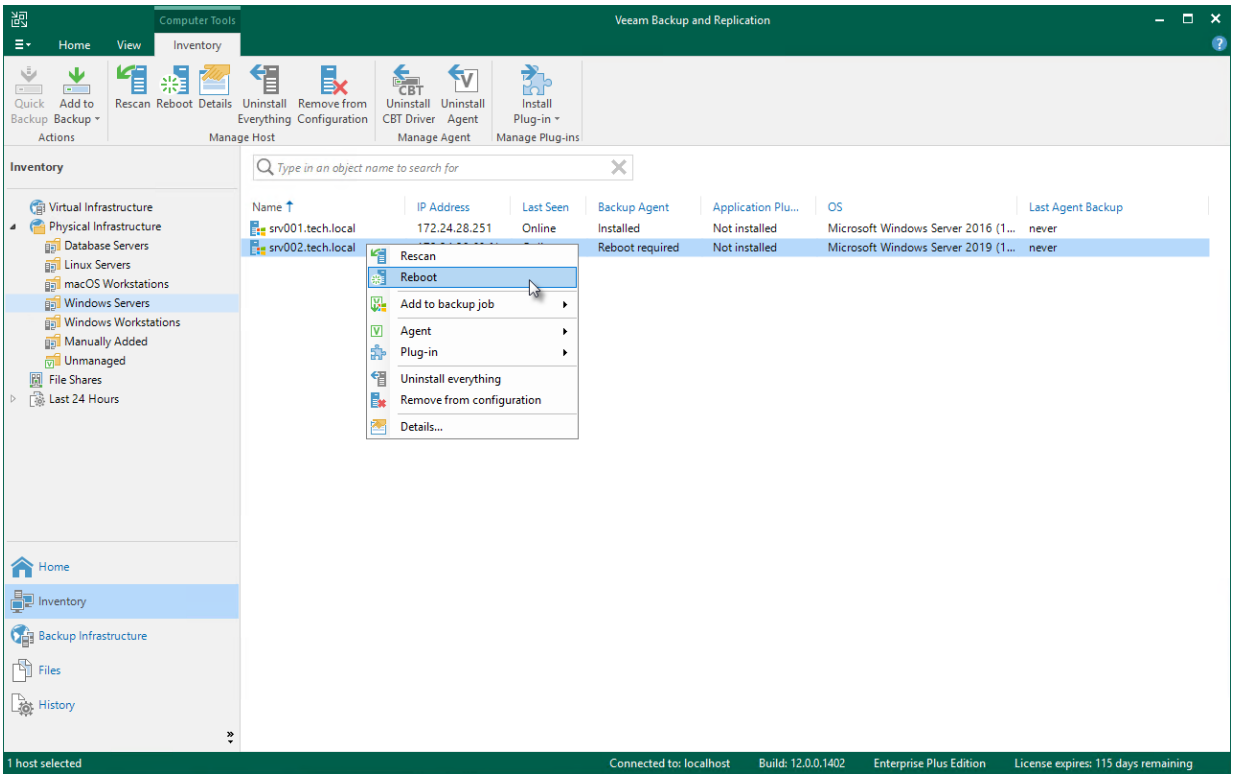
You can use the Veeam Backup & Replication console to reboot a protected computer. This operation may be required, for example, if you have installed the CBT driver on a selected computer and need to reboot this computer to finish the installation process and enable the driver.

Keep in mind that you cannot reboot a protected computer that is added to a protection group for pre-installed Veeam Agents. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

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 **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 Agents and Veeam Plug-ins

You can remove all Veeam Agents and Veeam Plug-ins installed on a specific protected computer as one operation. This may be useful is both Veeam Agent and Veeam Plug-in are installed on the computer and you do not want to uninstall them one by one.

> **TIP**
>
> To learn about Veeam plug-ins for enterprise applications, see Veeam Plug-ins for Enterprise Applications Guide.

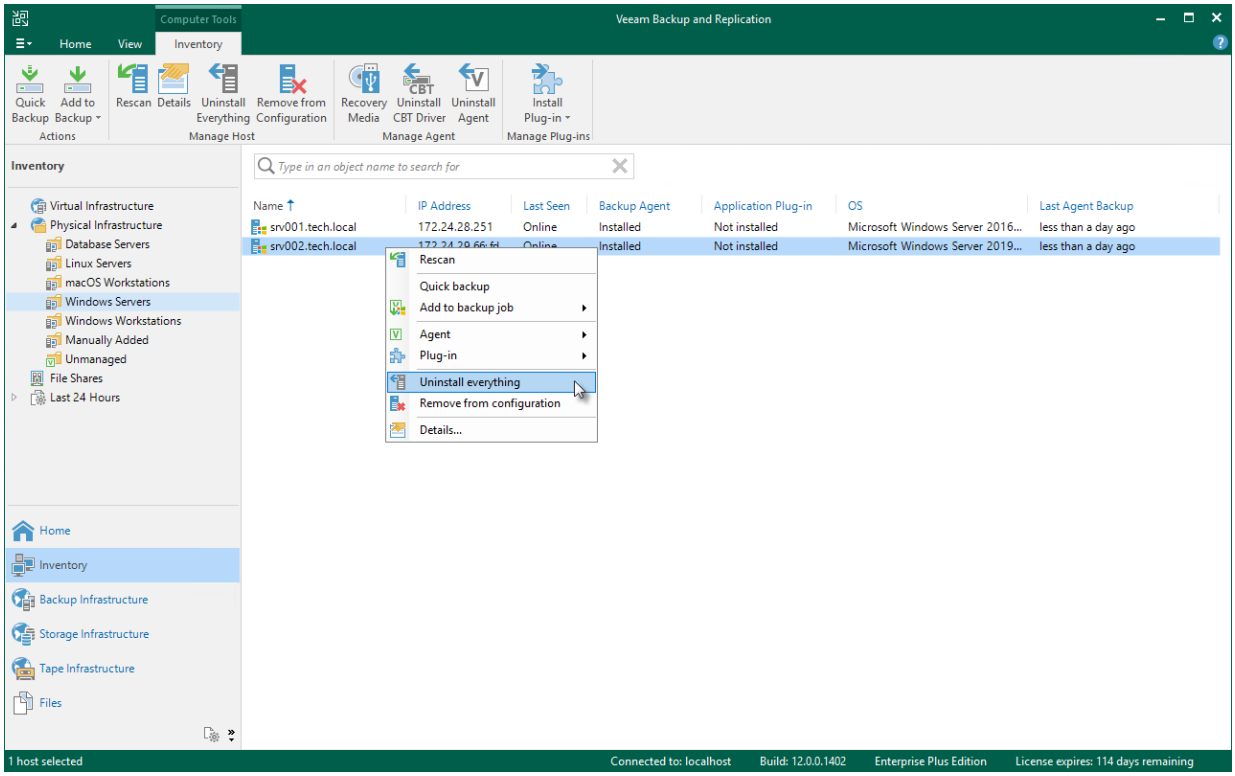
To uninstall all Veeam Agents and Veeam Plug-ins:

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 Everything** on the ribbon or right-click the computer and select **Uninstall everything**.
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.
- If you uninstall Veeam Agent for Microsoft Windows added to the protection group for pre-installed Veeam Agents and then re-install on the same computer, Veeam Agent will not connect to Veeam backup server automatically. To connect Veeam Agent, you must repeat the configuration step of the Veeam Agent deployment scenario. To learn more, see Deploying Veeam Agents Using Generated Setup Files.



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. Keep in mind 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 group 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.

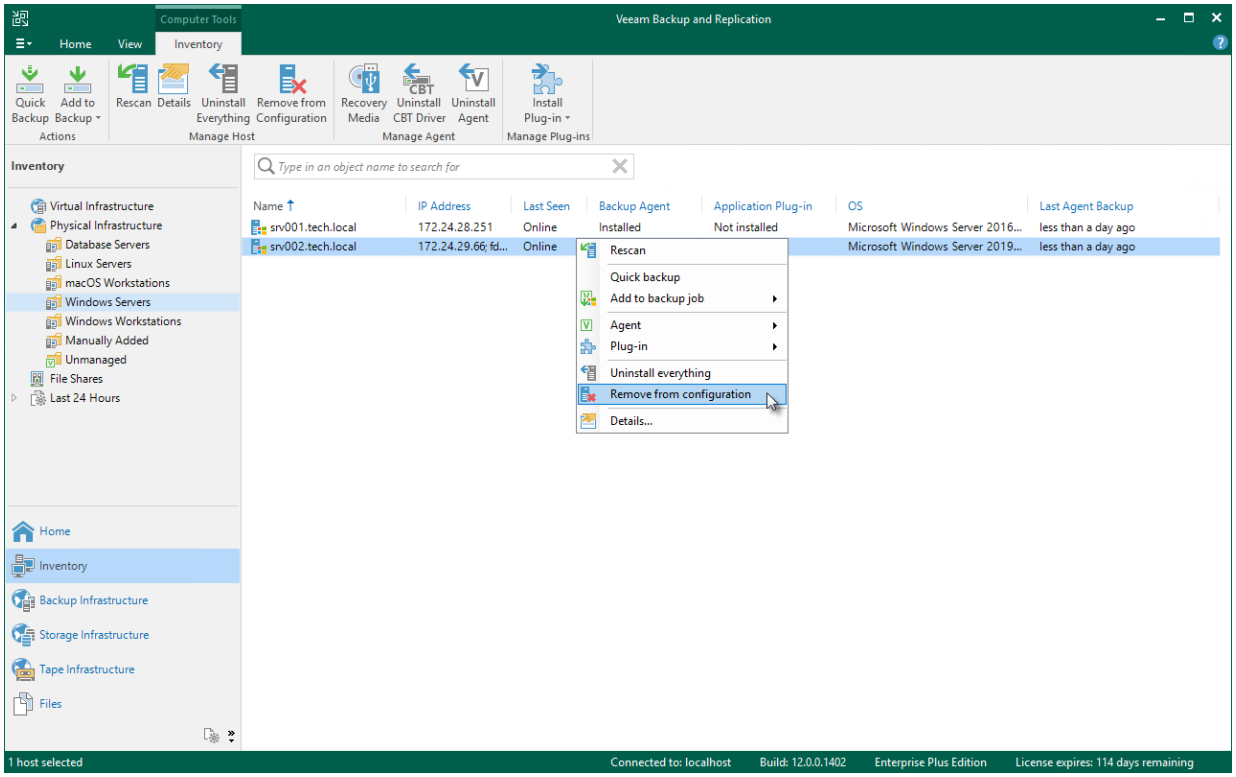
To remove a computer from a protection group:

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 **Remove from Configuration** on the ribbon or right-click the computer and select **Remove from configuration**.

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.

NOTE

You cannot remove a computer from the protection group if this computer is a failover cluster node.



Alternative Ways to Remove Computer from Protection Group

There are alternative ways to remove computer from protection group that may be suitable for specific situations. For example, you want to remove a Mac computer from a protection group from the Veeam Agent computer side.

Alternative ways of removing computer from protection group differ 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, organizational 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.

- For a protection group for pre-installed Veeam Agents, you can remove the computer from the Veeam Agent computer side. The process of removing a computer from a protection group for pre-installed Veeam Agents differs depending on the Veeam Agent computer OS:

  - For Windows-based Veeam Agent computers, see the RemoveOwner section in the Veeam Agent Configurator Reference.
  - For Linux-based Veeam Agent computers, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for Linux User Guide.
  - For Unix-based Veeam Agent computers running the IBM AIX operating system, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for IBM AIX User Guide.
  - For Unix-based Veeam Agent computers running the Oracle Solaris operating system, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for Oracle Solaris User Guide.
  - For macOS-based Veeam Agent computers, see the Deleting Connection to Veeam Backup Server section in the Veeam Agent for Mac User Guide.

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 or cloud 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 restore operations:

- Restore individual files and folders from Veeam Agent backups
- Export computer disks as VMDK, VHD or VHDX disks
  - Export restore points of Veeam Agent backups to standalone full backup files

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 computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

A restored VMware vSphere VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM. These settings include:

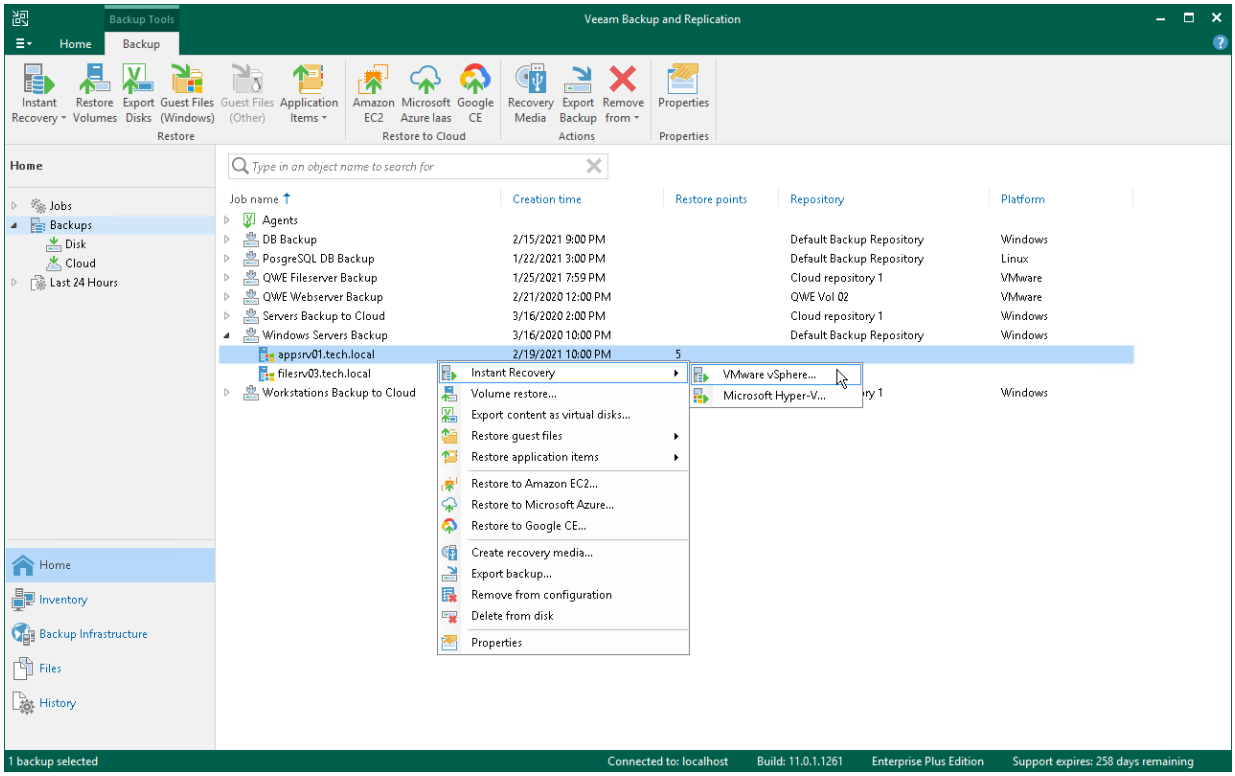
- Amount of RAM
- Number of CPU cores
- Number of network adapters
- Network adapter settings
- BIOS UUID

  If you do not want to preserve the backed-up machine UUID for a VMware vSphere VM, you can create a new UUID during the Instant Recovery configuration process.
- Number of disks and volumes
- Size of volumes

If you restore a Veeam Agent computer to a VMware vSphere VM, consider the following:

- Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
- If you restore a workload to the production network, make sure that the original workload is powered off.
- [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

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 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, see the Performing Instant Recovery of Workloads to VMware vSphere VMs 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 and Linux computers created on the Veeam backup repository. You cannot use backups created on the Veeam Cloud Connect repository for this operation.

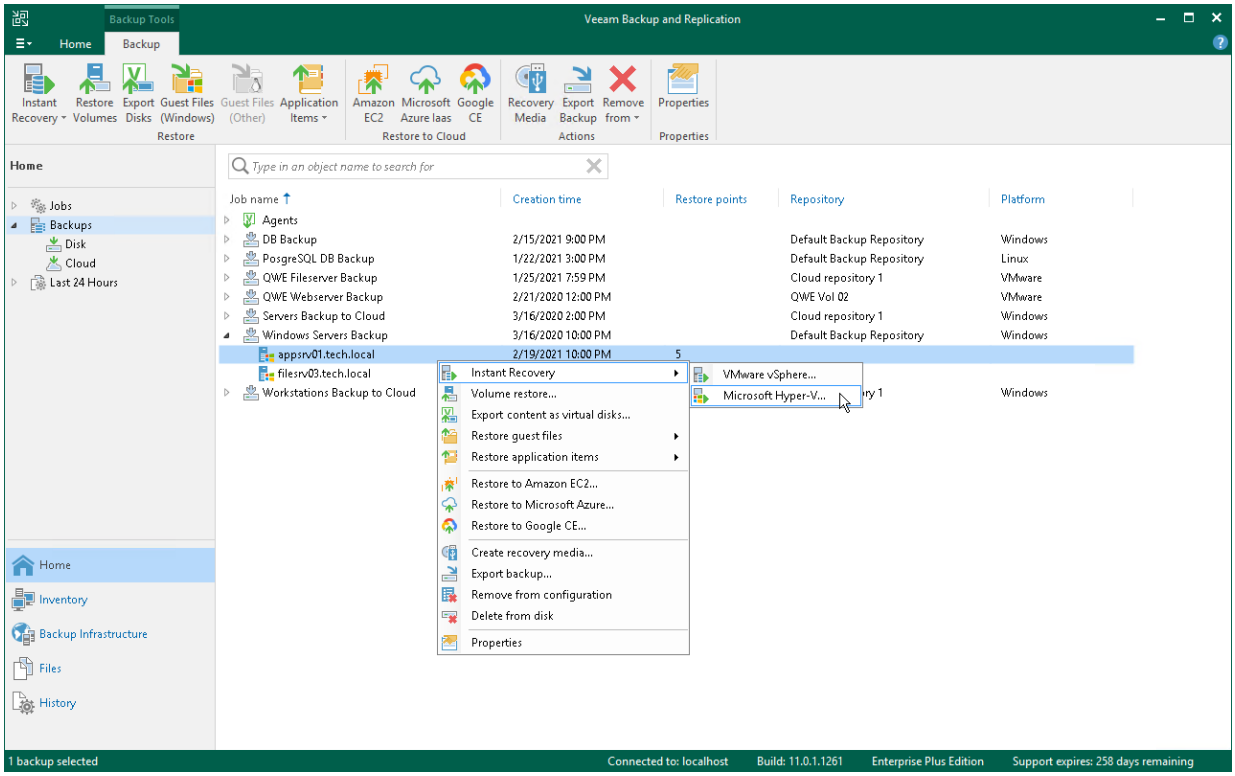
Mind that to restore to a Hyper-V VM using a backup of a Linux computer, you must consider the Hyper-V limitations. To learn more, see this Microsoft article.

A restored Hyper-V VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM.

If you restore a Veeam Agent computer to a Hyper-V VM, consider the following:

- [For backups of Microsoft Windows computers] You cannot recover an EFI-based Veeam Agent computer that runs Windows 7, Windows Server 2008 or Windows Server 2008 R2 to a Hyper-V VM. These OSes can be restored only to a Generation 1 VM that does not support EFI. To learn more, see this Microsoft article.
- Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.
- Veeam Agent computer disks are recovered as dynamically expanding virtual disks.
- By default, Veeam Backup & Replication automatically powers on a VM after restore. If you do not want to power on a VM after restore, you can change this setting during the Instant Recovery configuration process.
- [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

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 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, see the Performing Instant Recovery of Workloads to Hyper-V VMs section in the Veeam Backup & Replication User Guide.



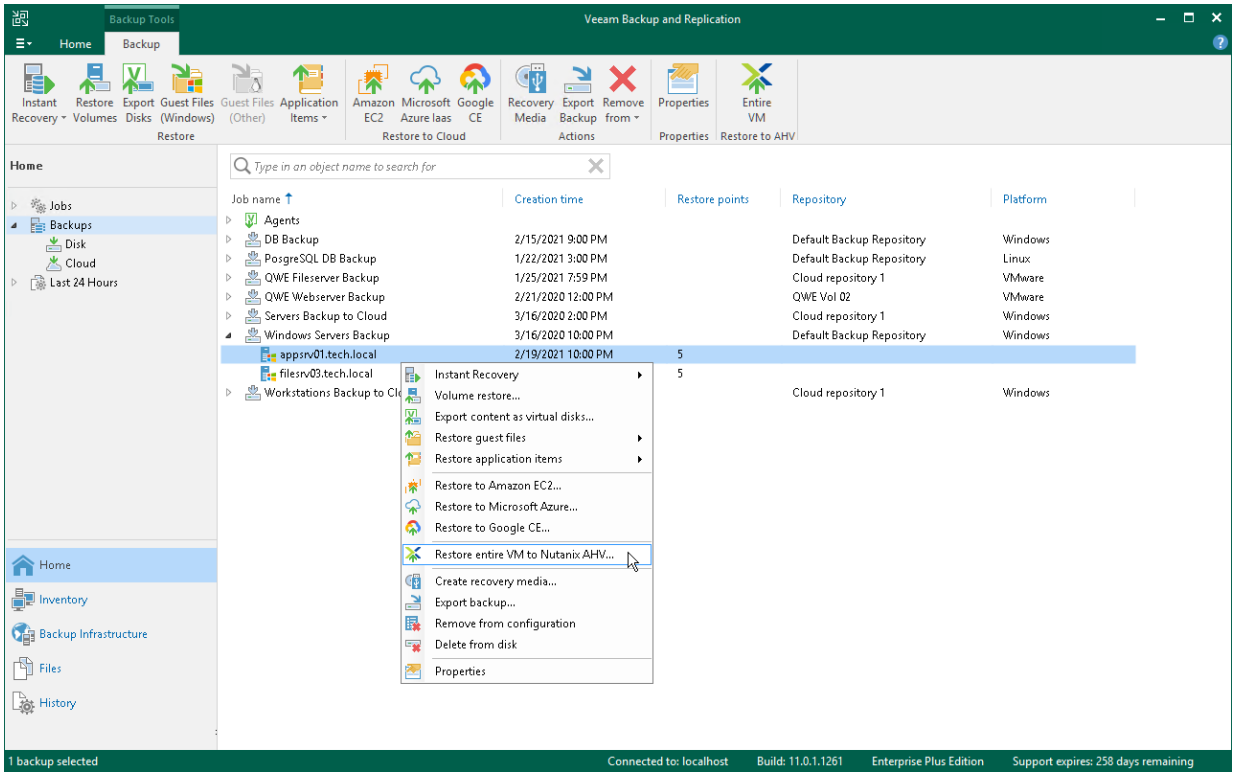
Restoring Veeam Agent Backup to Nutanix VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Nutanix AHV VM in your virtualization environment. For restore to Nutanix AHV, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

Mind that to restore to Nutanix AHV, you must install Nutanix AHV Plug-in on the Veeam Backup & Replication server. To learn more, see the Installation section in the Veeam Backup for Nutanix AHV User Guide.

> **IMPORTANT**
>
> [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Nutanix AHV for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more about restore to Nutanix AHV, see the Restoring VMs Using Veeam Backup & Replication Console section in the Veeam Backup for Nutanix AHV User Guide.



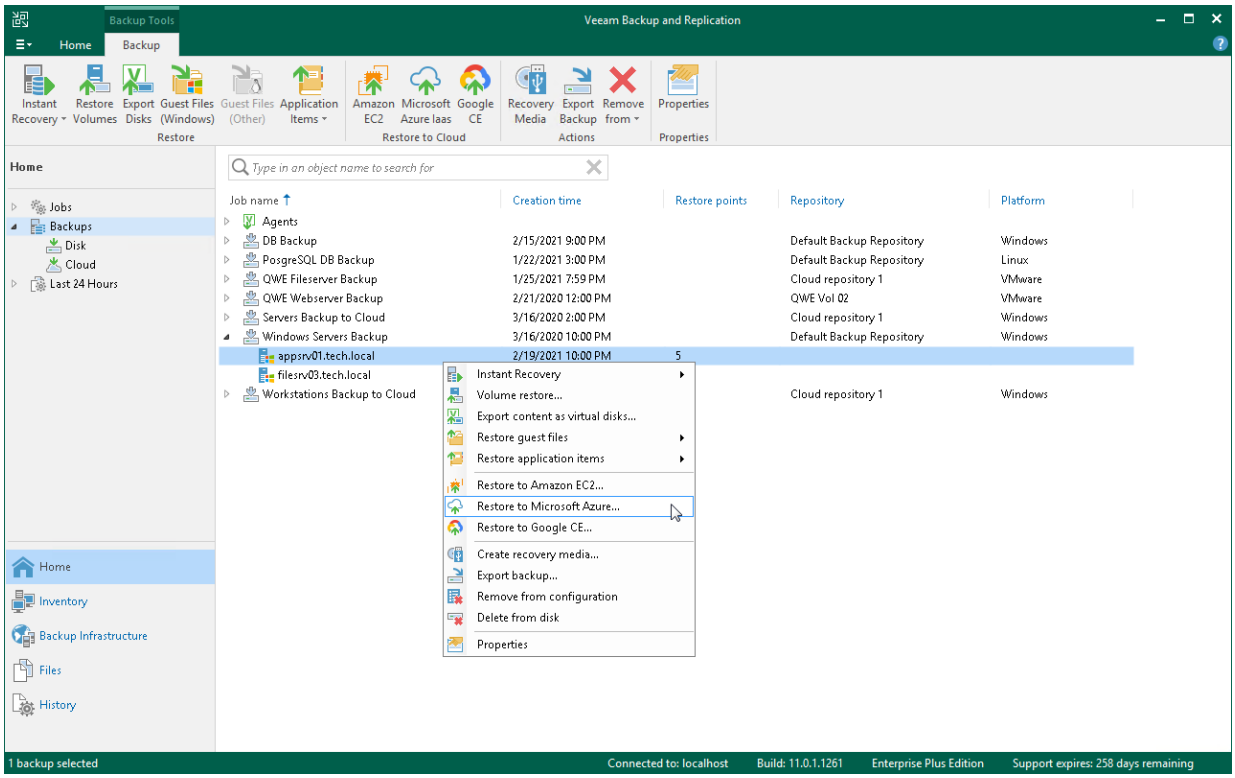
Restoring to Microsoft Azure

You can restore computers from Veeam Agent backups to Microsoft Azure. For restore to Microsoft Azure, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository. Backups must be created at the entire machine level or volume level.

If you restore a Veeam Agent machine to Microsoft Azure, consider the following:

- If you recover a EFI-based system to Microsoft Azure, Veeam Agent will restore a BIOS-based Generation 1 VM.
- Veeam Backup & Replication offers experimental support for generation 2 VMs within restore to Microsoft Azure feature. To learn more, see the Generation 2 VM Support section in the Veeam Backup & Replication User Guide.
- [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

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.

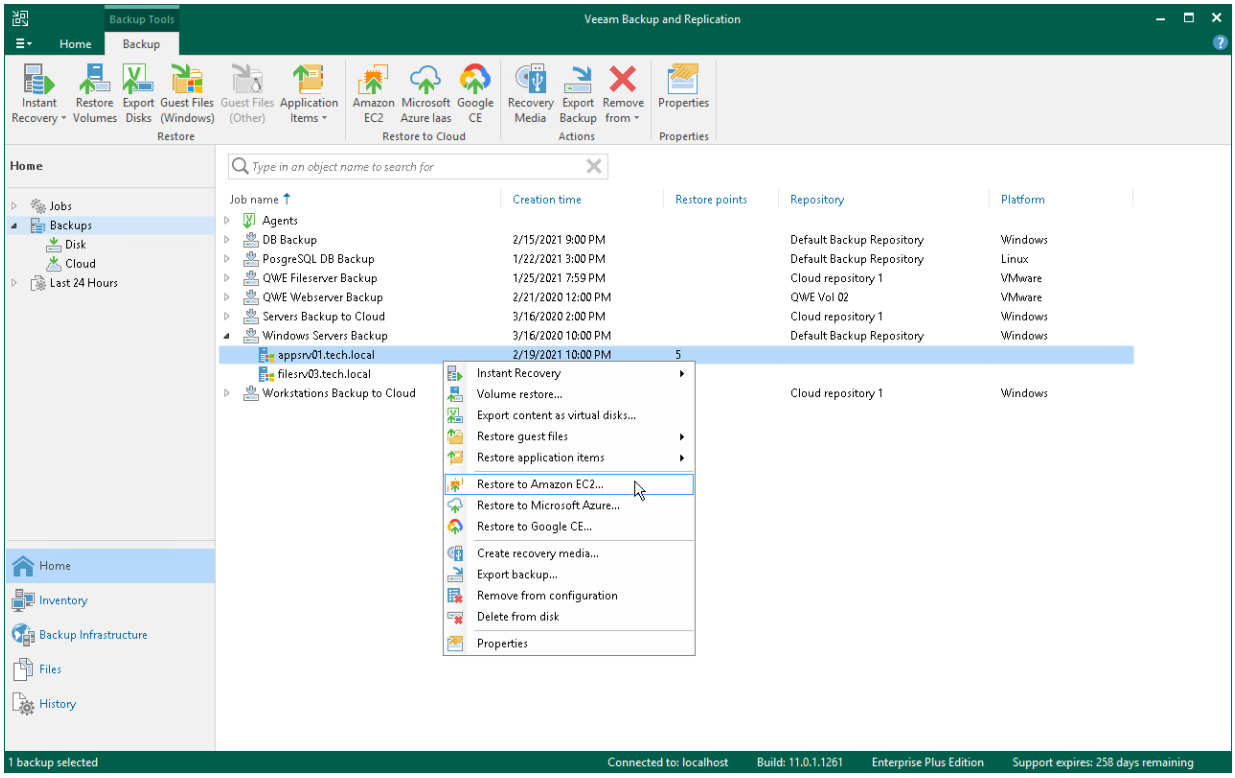


Restoring to Amazon EC2

You can restore computers from Veeam Agent backups to Amazon EC2. For restore to Amazon EC2, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository. Backups must be created at the entire machine level or volume level.

> **IMPORTANT**
>
> [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

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.

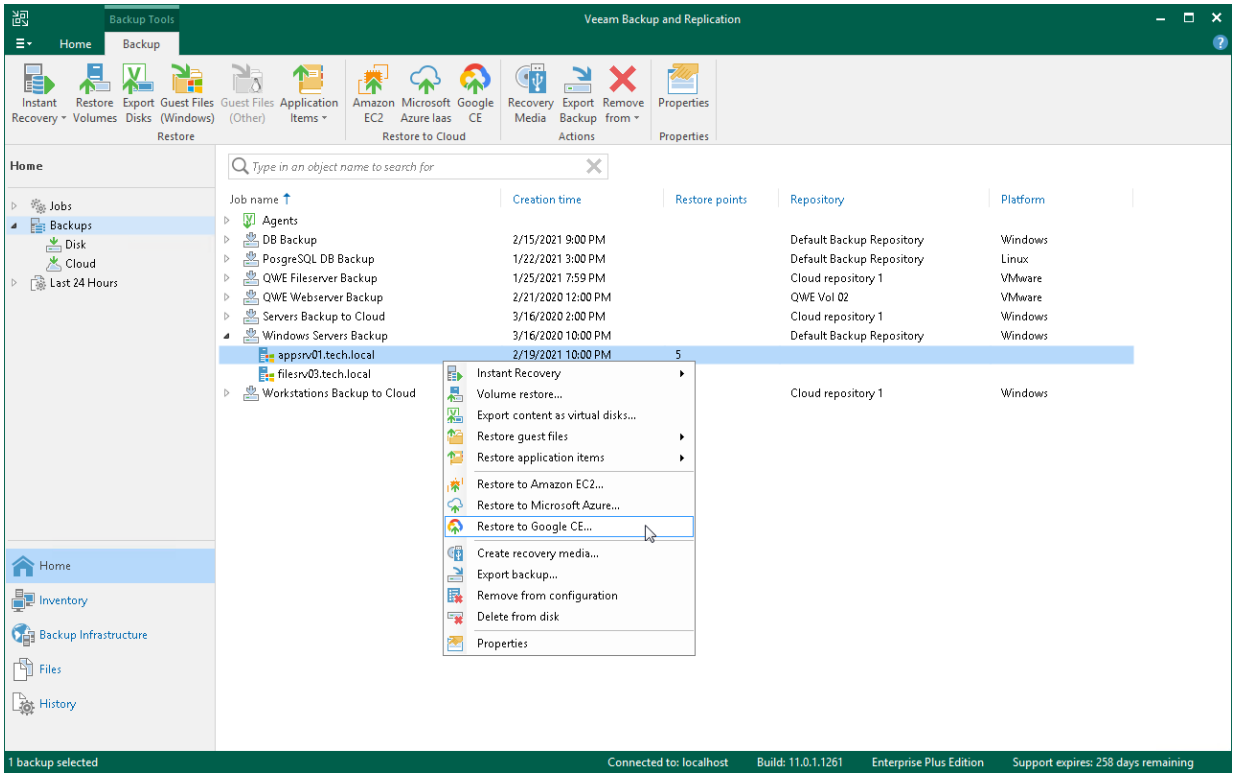


Restoring to Google Compute Engine

You can restore computers from Veeam Agent backups to Google Compute Engine. For restore to Google Compute Engine, you can use backups of Microsoft Windows and Linux computers created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository. Backups must be created at the entire computer level or volume level.

> **IMPORTANT**
>
> [For backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Google Compute Engine from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about restore to Google Compute Engine, see the Restore to Google Compute Engine 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. Keep in mind 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 Restore guest files option.

A volume can be restored to its original location or a 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:

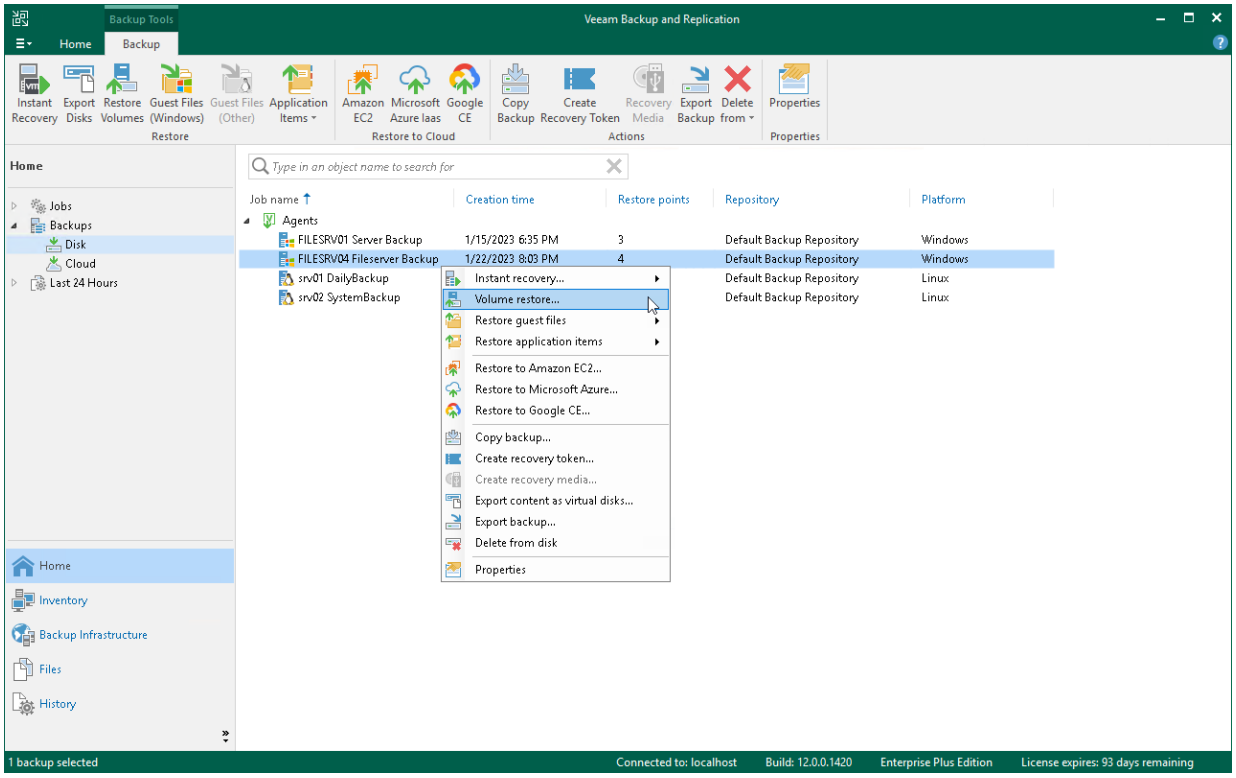
- You can restore volumes only from backups created with Veeam Agent for Microsoft Windows.
- You cannot restore a system volume to a system volume of the original Veeam Agent computer or another computer with the running OS. To perform such restore, you need to boot the OS from the recovery image. For details, see Restoring Data with Veeam Recovery Media. You can also restore a system volume to a non-system volume that has enough free space.
- 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** > **Disk 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 proceed immediately to the Restore Point step of the wizard.

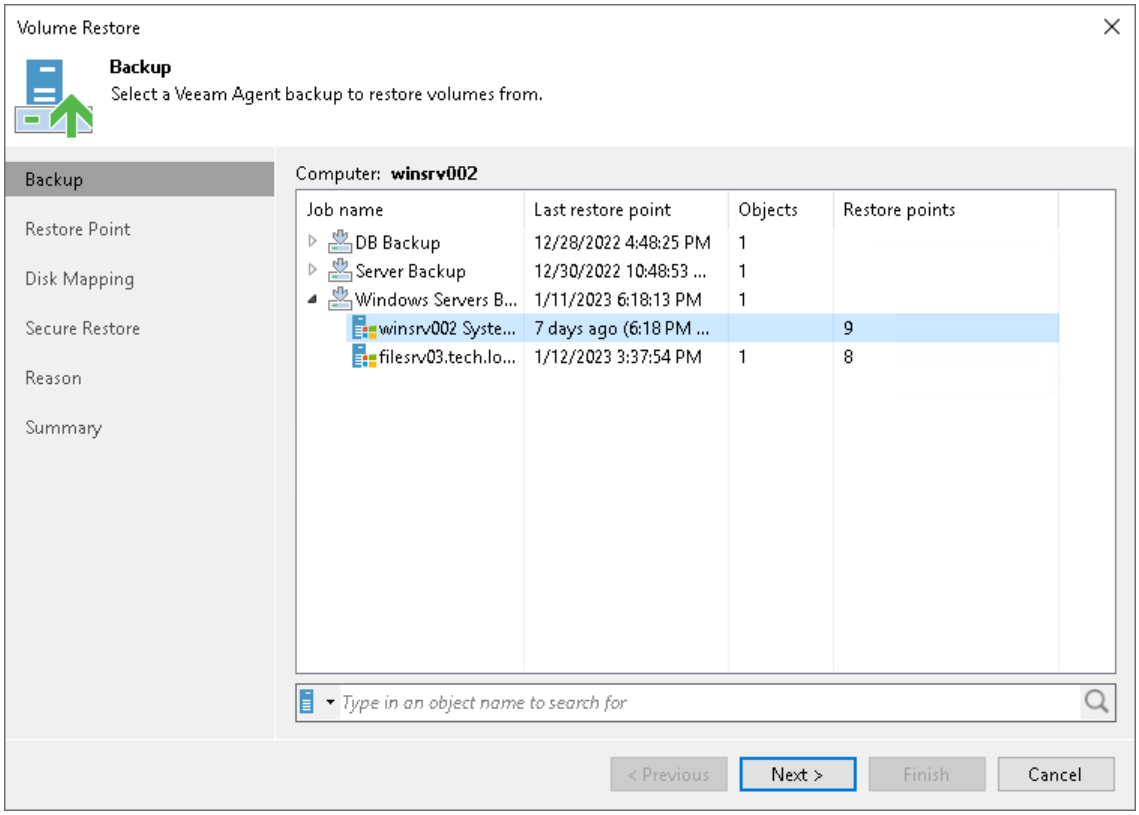


Step 2. Select Backup

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 backups created with Veeam Agent for Linux are not displayed.

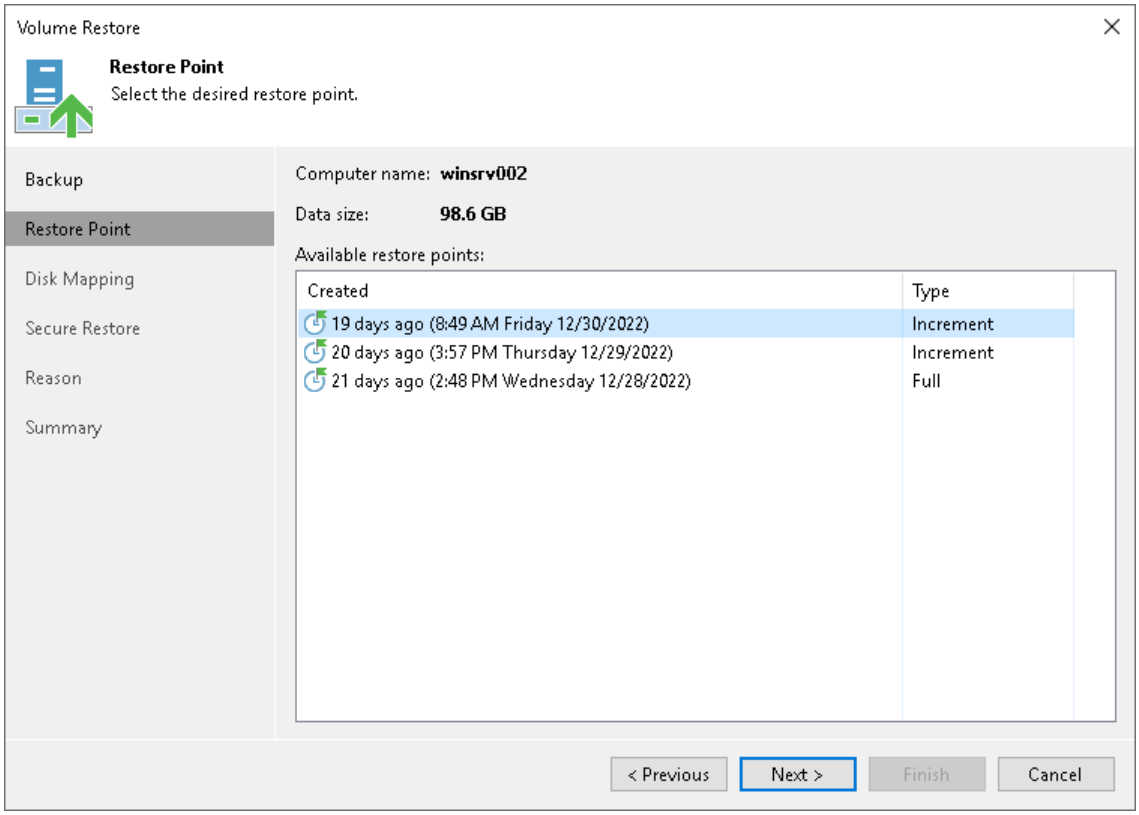


Step 3. Select Restore Point

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.



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 host** 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.

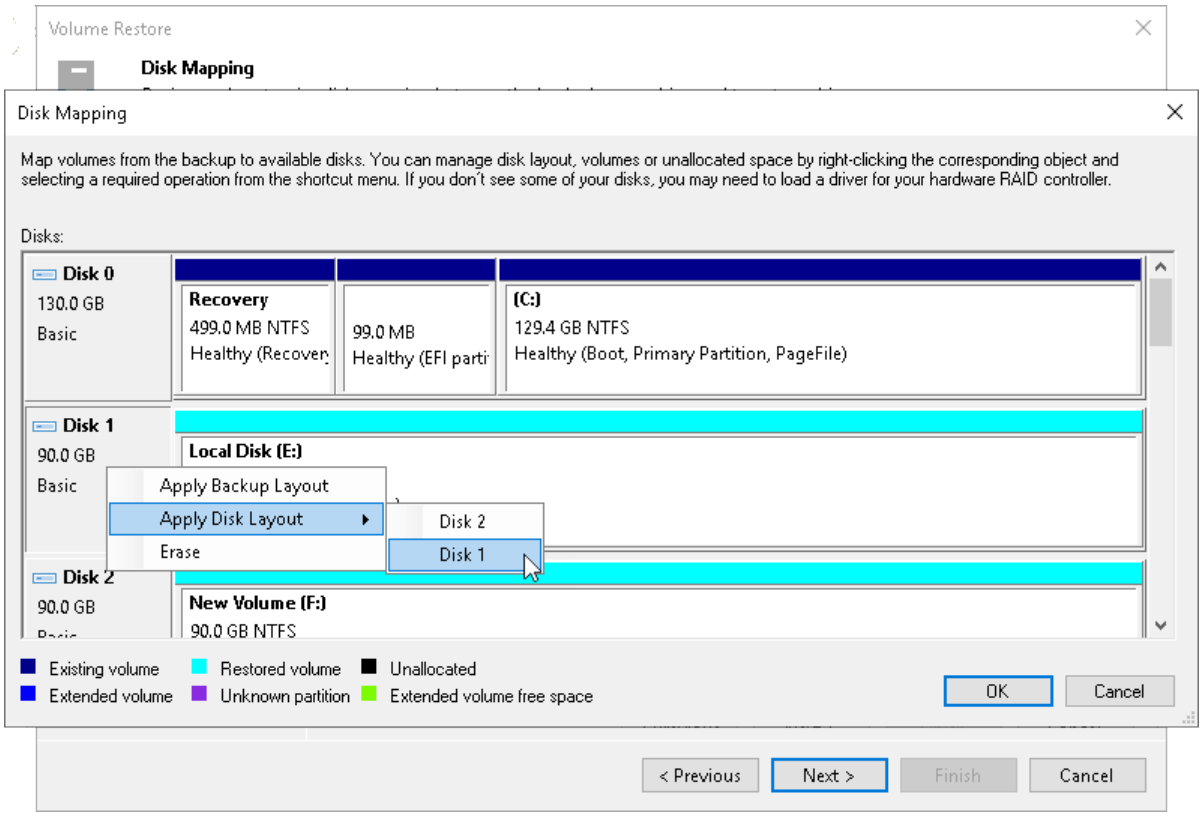
   If you select a computer included in a protection group for pre-installed Veeam Agents, you must provide credentials of the account that has administrator permissions on the target computer. Keep in mind that Veeam Backup & Replication will keep these credentials only during the restore process and delete them after the restore process completion. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.

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**.

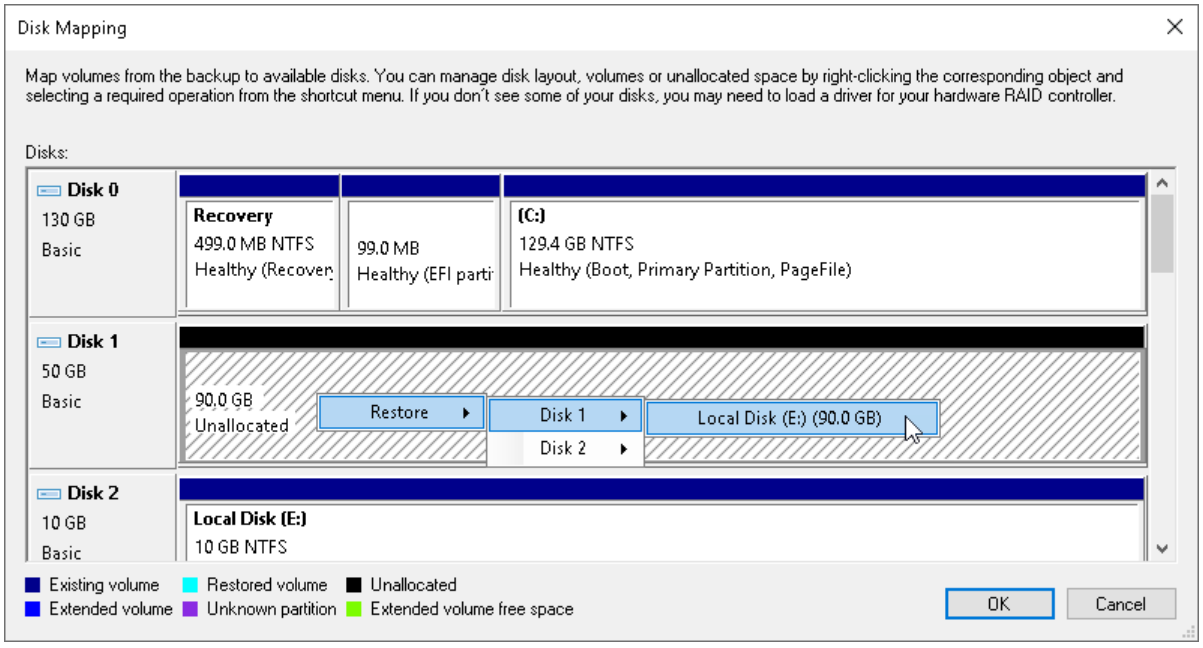
3. In the **Disk Mapping** window, specify how volumes must be restored:
   - Right-click the target disk on the left and select the necessary disk layout:
     - **Apply Backup Layout** — select this option if you want to apply to disk the settings that were used on your computer at the moment when 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.



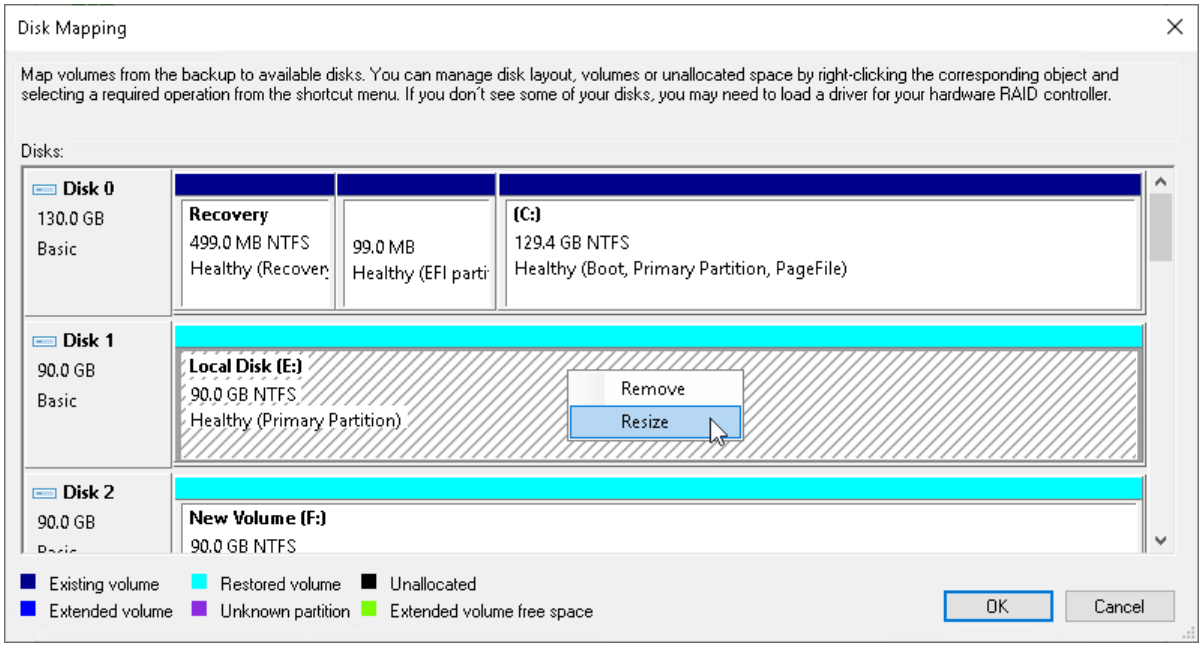
- Right-click unallocated disk space in the disk area on the right and select what volume from the backup you want to place on this computer disk.

  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.



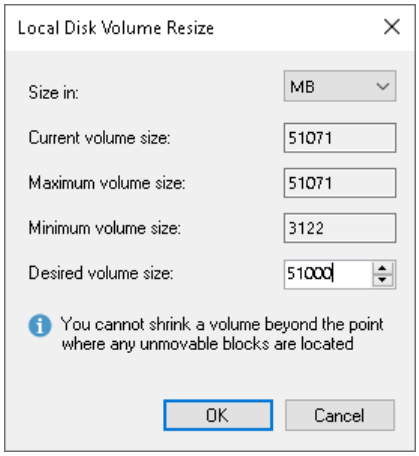
Step 5. Resize Restored Volumes

At the **Disk Mapping** step of the wizard you can set the necessary size for the restored volumes. 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.

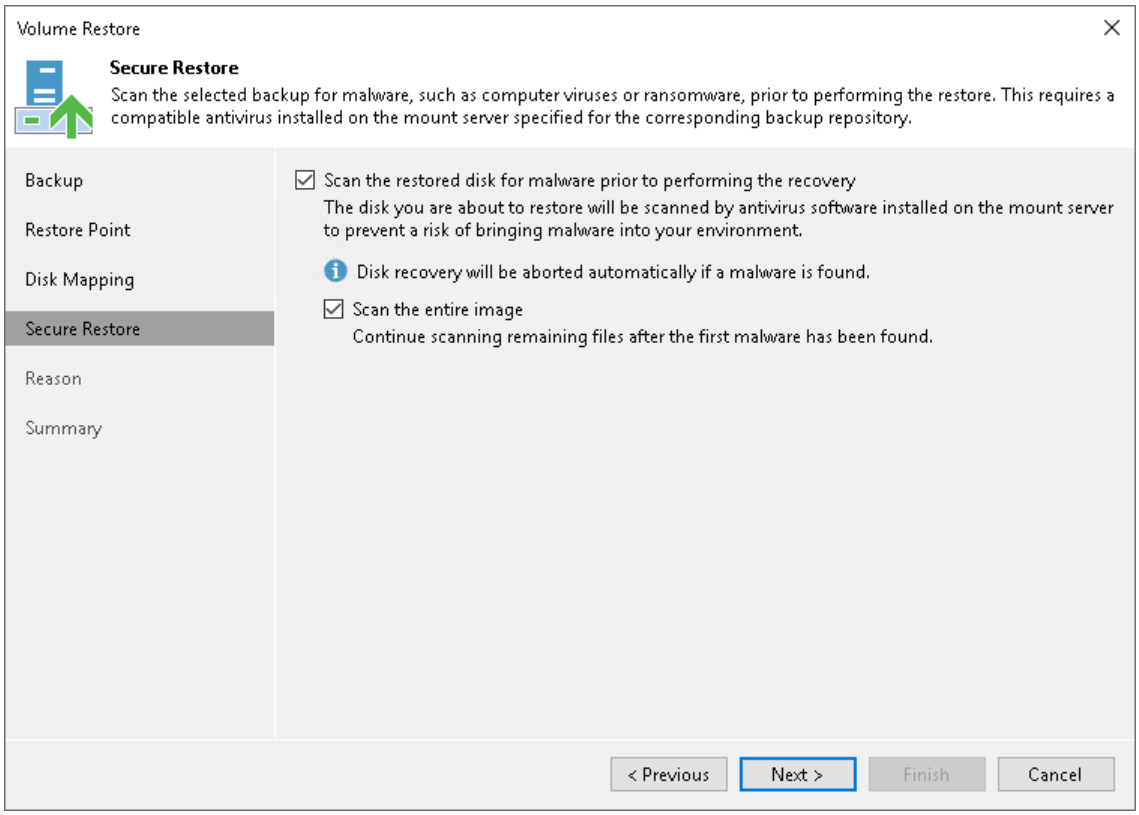


Step 6. Specify Secure Restore Settings

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:

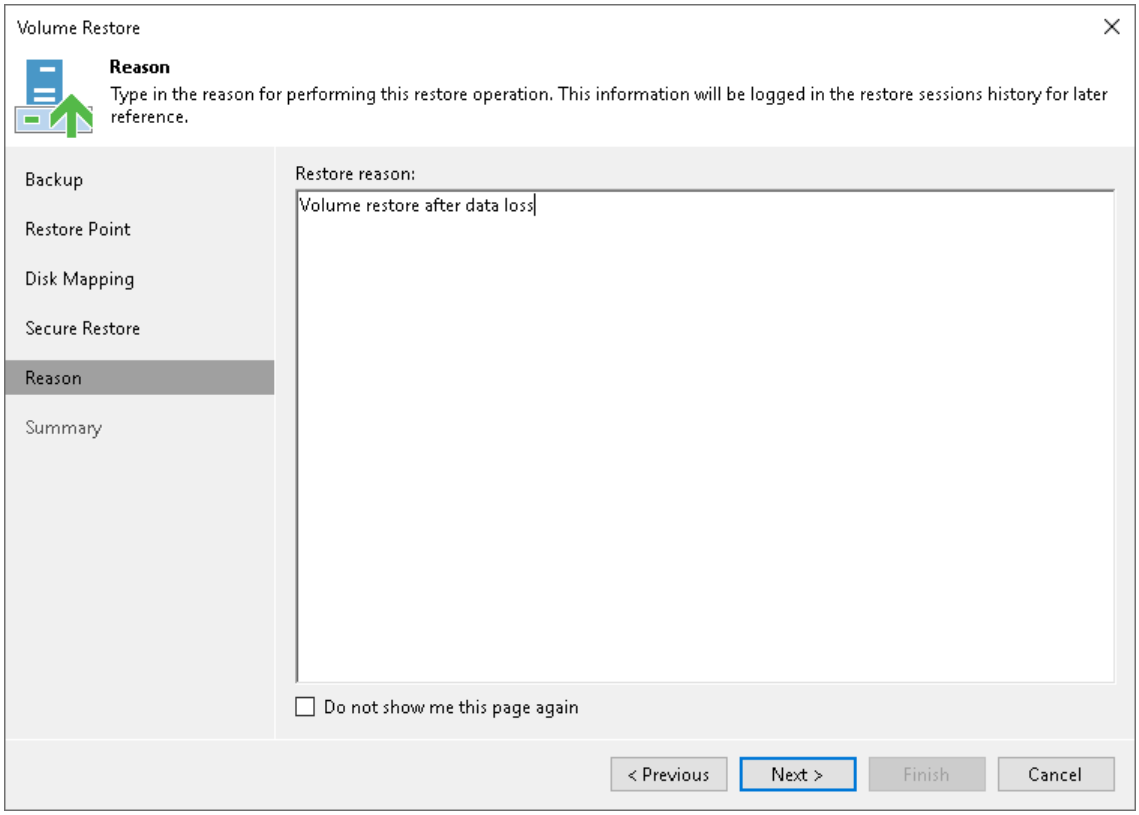
1. At the **Secure Restore** step of the wizard, select the **Scan the restored disk for malware prior to performing the recovery** check box.
2. Select the **Scan the entire image** check box if you want the antivirus software to continue volume scan after the first malware threat is found. For information on how to view results of the antivirus scan, see the Viewing Antivirus Scan Results section in the Veeam Backup & Replication User Guide.



Step 7. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring the computer volume.

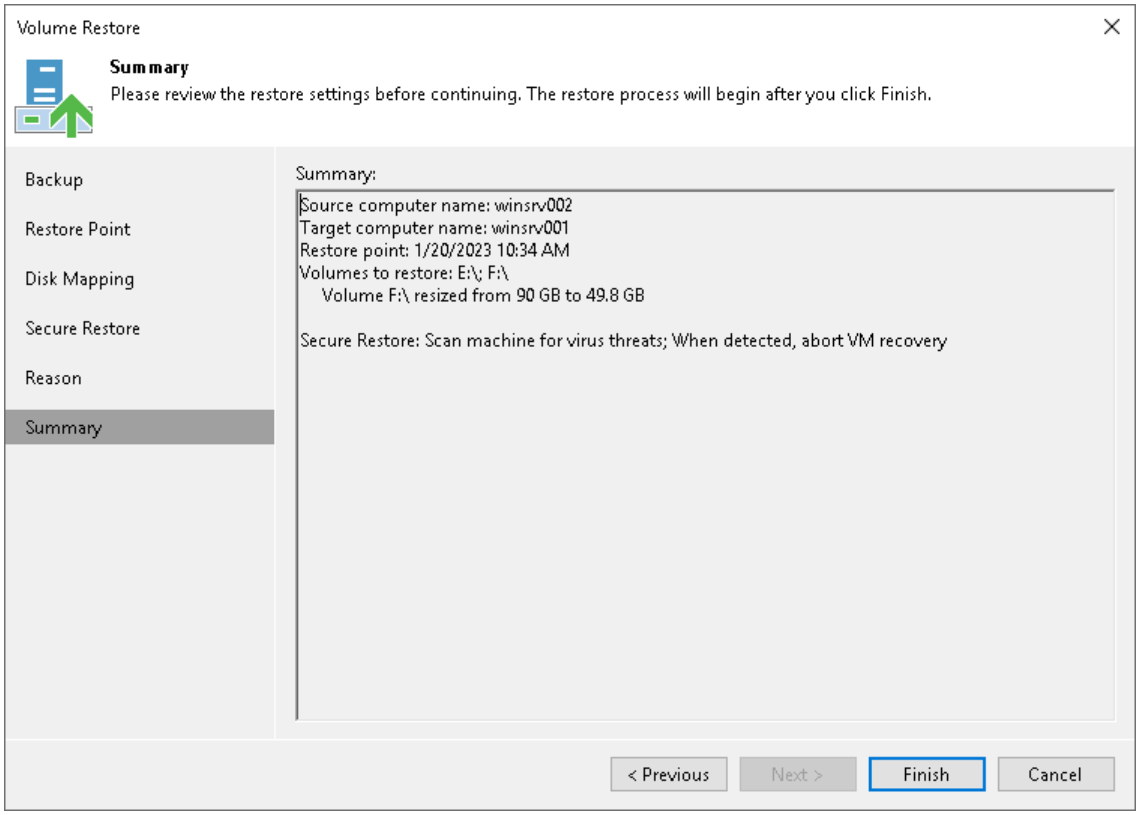
> **TIP**
>
> If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.



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.



Restoring Files and Folders

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups.

For file-level restore, you can use Veeam Agent backups created in the Veeam backup repository or Veeam Cloud Connect repository. For Veeam Agent backups created in the cloud repository, you can perform restore tasks in Veeam Backup & Replication deployed on the tenant backup server. The service provider cannot perform restore tasks with Veeam Agent backups.

Consider the following:

- [For backups of Linux computers] When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of a Linux computer from the backup or replica:
  - Mounting disks to a helper host — a target host where you want to restore files from the backup or any other Linux host.
  - Mounting disks to a helper appliance — a helper VM required to mount Linux computer disks from the backup.

    If you have selected to mount disks to a helper appliance, 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*.

  To learn more about these options, see the Restore from Linux, Unix and Other File Systems section in the Veeam Backup & Replication User Guide.
- [For backups of Microsoft Windows computers] Before you start file-level restore from a backup of a failover cluster, make sure that the cluster is added to a protection group in the Veeam Backup & Replication inventory. The failover cluster may be not present in the inventory, for example, in the following cases:
  - The original protection group that contained the cluster was removed from Veeam Backup & Replication.
  - You want to restore cluster data from a backup created on another backup server and imported in the Veeam backup console.

  In this case, add the failover cluster whose data you want to restore to a protection group.

NOTE

When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of a Linux, Unix or Mac endpoint from the backup or replica:

- Mounting disks to a helper host — a target host where you want to restore files from the backup or any other Linux host.
- Mounting disks to a helper appliance — a helper VM required to mount Veeam Agent computer disks from the backup.

  If you have selected to mount disks to a helper appliance, 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.

To learn more about these options, see the Restore from Linux, Unix and Other File Systems section in the Veeam Backup & Replication User Guide.

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.

Restoring Application Items

You can use Veeam Explorers to restore application items from backups created using Veeam Agent for Microsoft Windows and Veeam Agent for Linux. Veeam Backup & Replication lets you restore items and objects from the following applications:

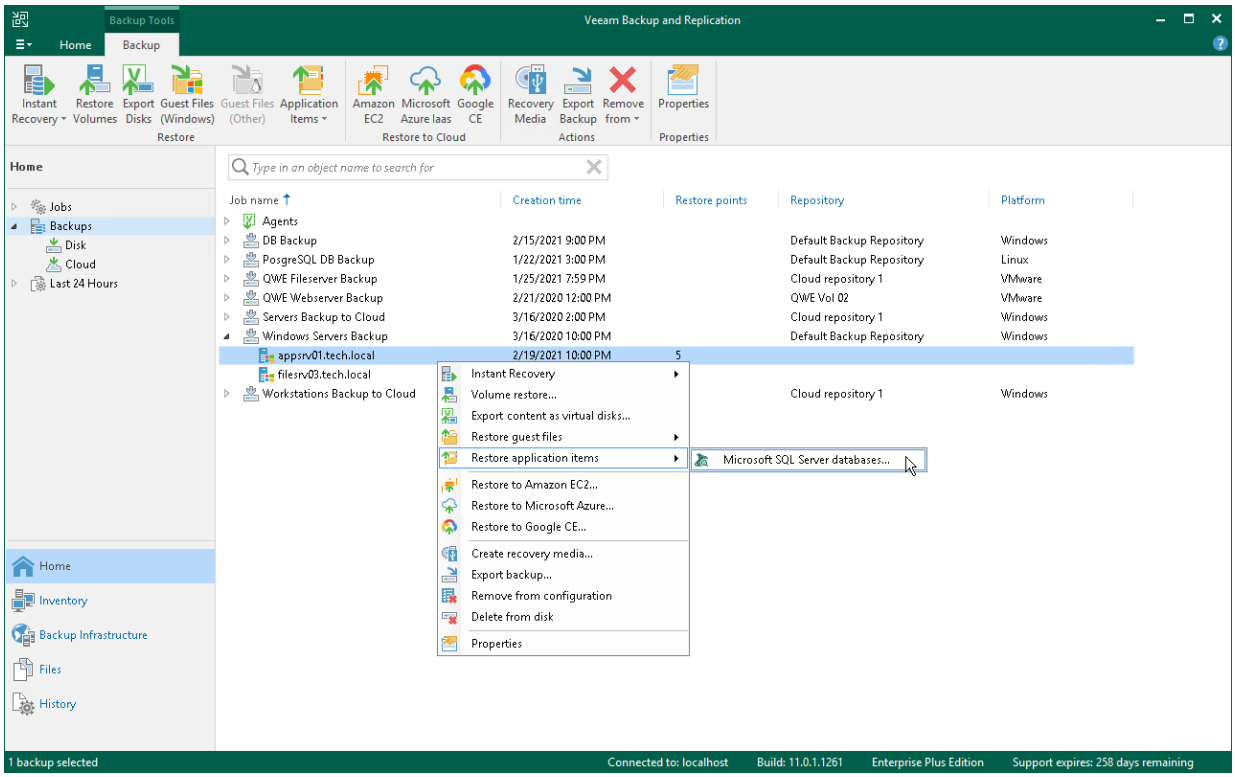
From backups created with Veeam Agent for Microsoft Windows

- Microsoft Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- Oracle

From backups created with Veeam Agent for Linux

- Oracle
- PostgreSQL

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 Veeam Agent backups created using Veeam Agent for Microsoft Windows and Veeam Agent for Linux 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 provisioned format.

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.

> **IMPORTANT**
>
> Consider the following:
>
> - If the backup from which you restore disks contains a Btrfs storage pool, during the disk restore process Veeam Backup & Replication will create a separate disk and restore the Btrfs pool to this disk.
> - If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks..

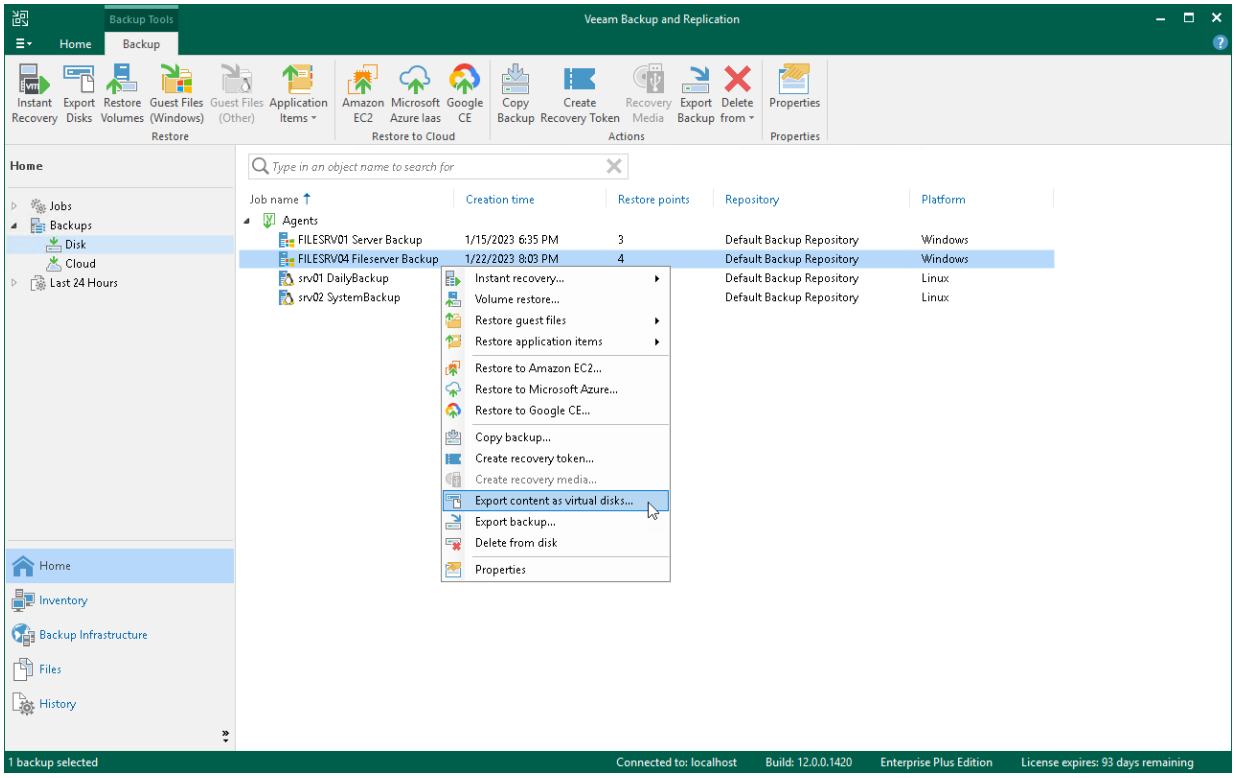
To restore disks and convert them to the VMDK, VHD or VHDX format, use the **Export Disk** wizard.

Step 1. Launch Export Disk Wizard

To launch the **Export Disk** wizard, do either of the following:

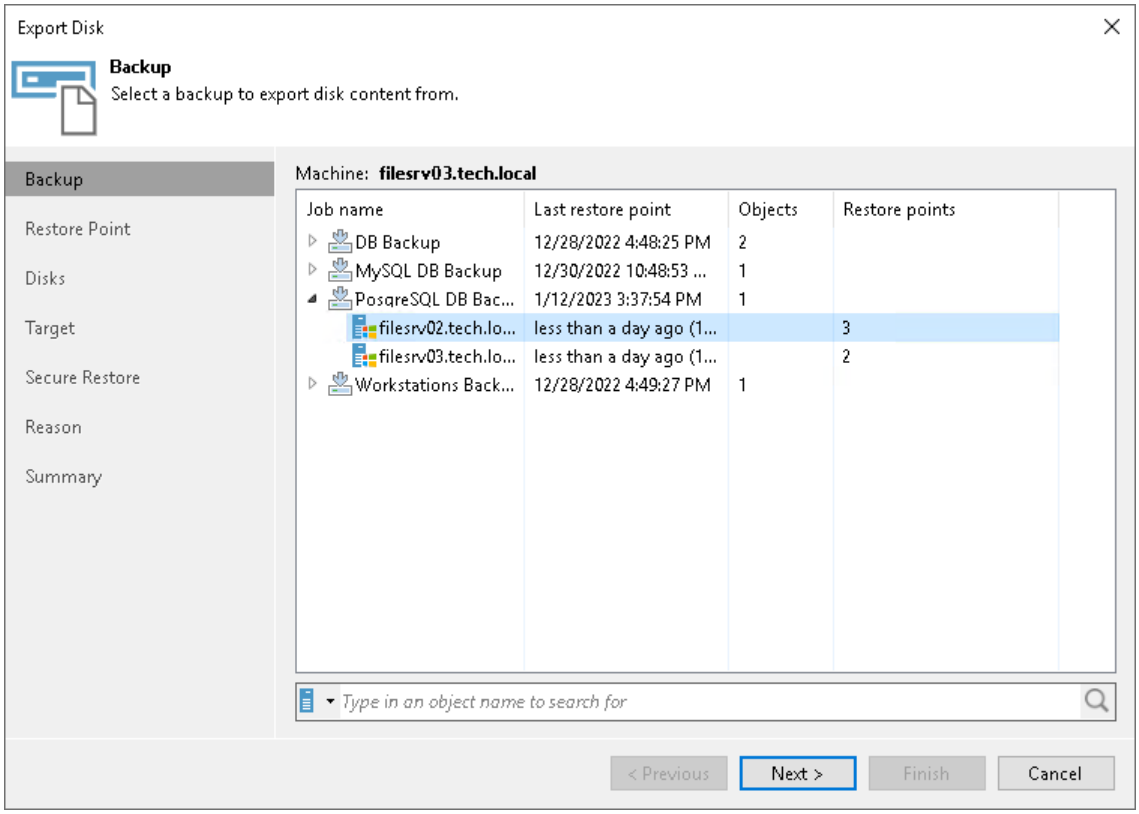
- Open the **Home** tab and click **Restore** > **Agent** > **Disk restore** > **Export disk**. In this case, you will be able to select a backup of the necessary Veeam Agent computer at the Backup step of the wizard.
- Open the **Home** view. In the inventory pane, click the **Backups** node. In the 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 content as virtual disks**.

  In this case, you will pass immediately to the Restore Point step of the wizard.



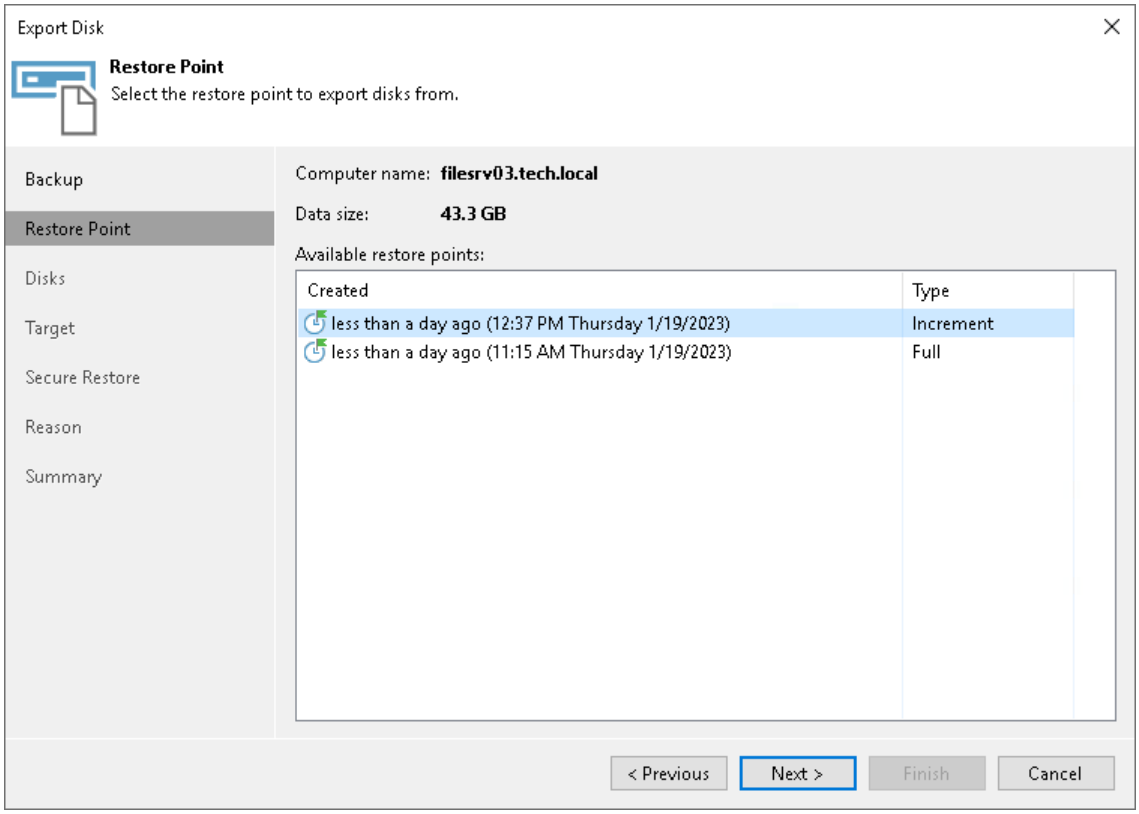
Step 2. Select Backup

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 and Veeam Cloud Connect repository.



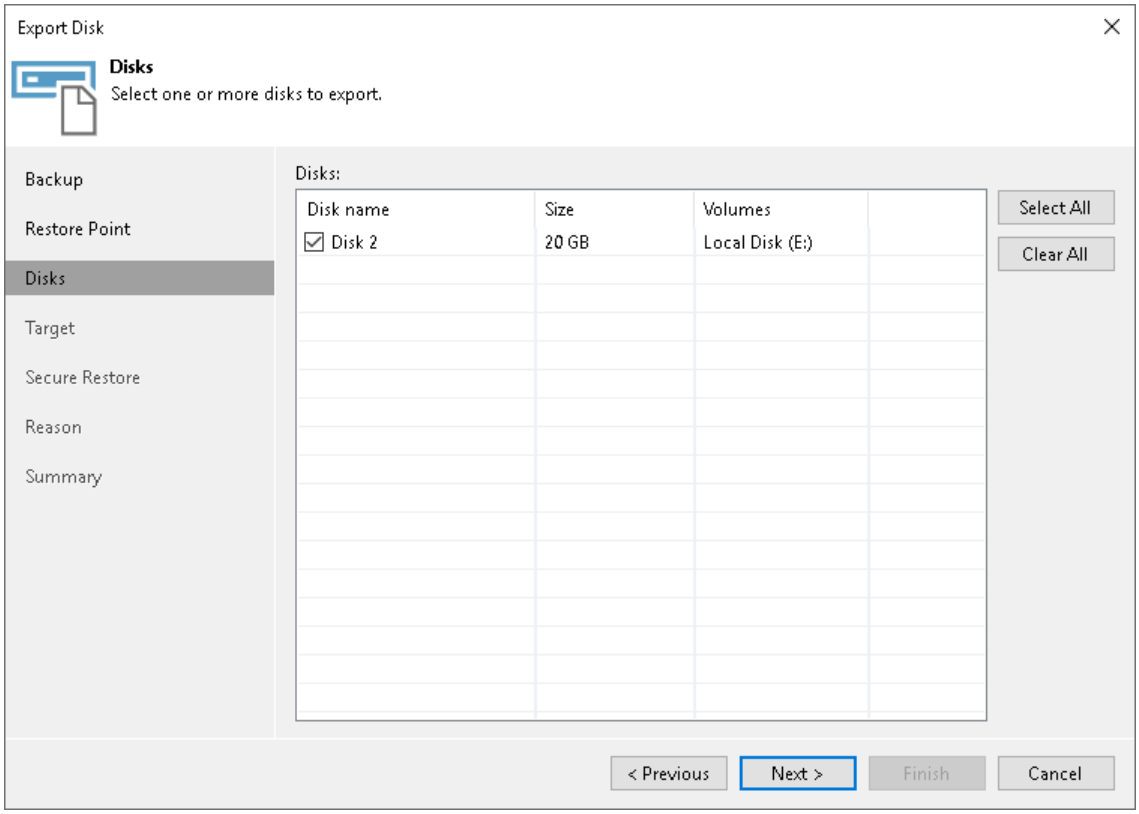
Step 3. Select Restore Point

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 the selected 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

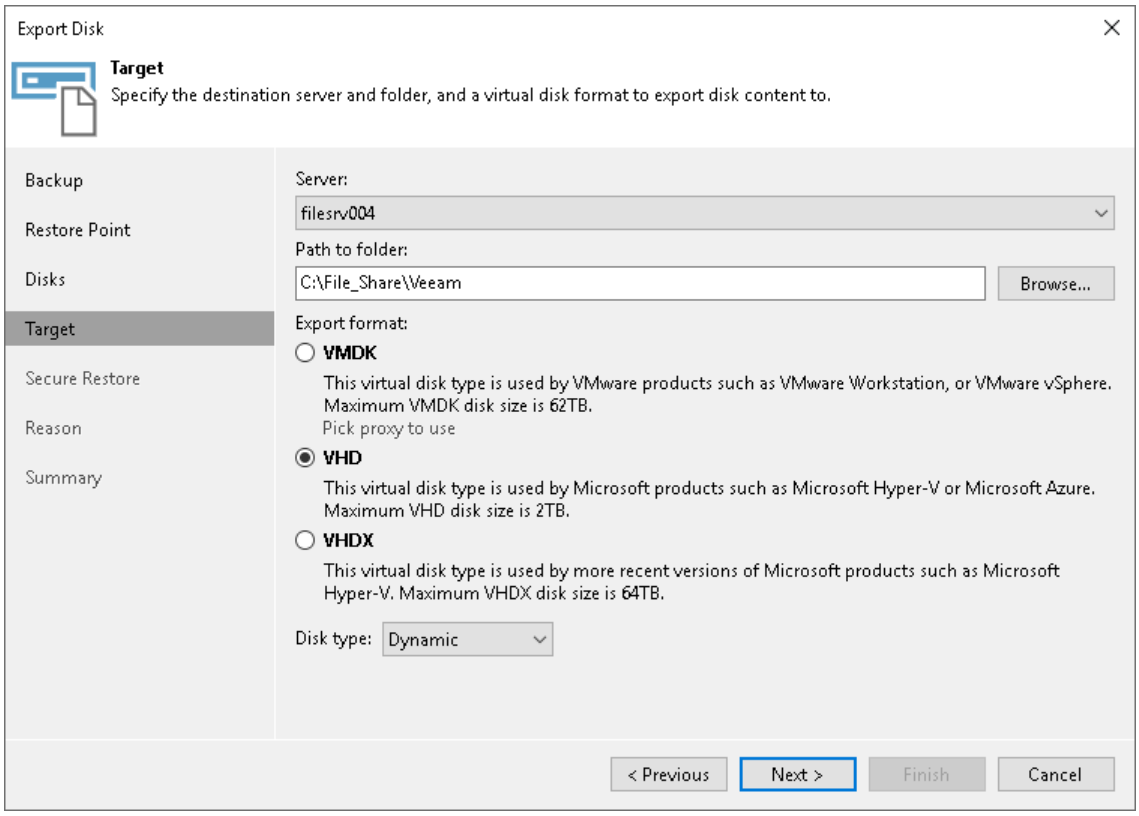
At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk.

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).
4. Click **Disk type** to specify how the resulting disk must be saved:
   - [For VMDK disk format] in the thin provisioned, lazy zeroed thick provisioned, or eagerly zeroed thick provisioned format
   - [For VHD and VMDX disk formats] in the dynamic or fixed format
5. [For export of a VMDK disk to an ESXi host] Click the **Pick proxy to use** link to select backup proxies over which backup data must be transported to the target datastore.

NOTE

Consider the following:

- 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.
- If you have selected to store the resulting virtual disk on the server running Microsoft Windows Server OS and in the VMDK format, you will be able to save the virtual disk in the lazy zeroed thick provisioned format only.


Export Disk
Target
Specify the destination server and folder, and a virtual disk format to export disk content to.
Backup
Restore Point
Disks
Target
Secure Restore
Reason
Summary
Server:
filesrv004
Path to folder:
C:\File_Share\Veeam
Browse...
Export format:
VMDK
This virtual disk type is used by VMware products such as VMware Workstation, or VMware vSphere. Maximum VMDK disk size is 62TB.
Pick proxy to use
VHD
This virtual disk type is used by Microsoft products such as Microsoft Hyper-V or Microsoft Azure. Maximum VHD disk size is 2TB.
VHDX
This virtual disk type is used by more recent versions of Microsoft products such as Microsoft Hyper-V. Maximum VHDX disk size is 64TB.
Disk type:
Dynamic
< Previous
Next >
Finish
Cancel

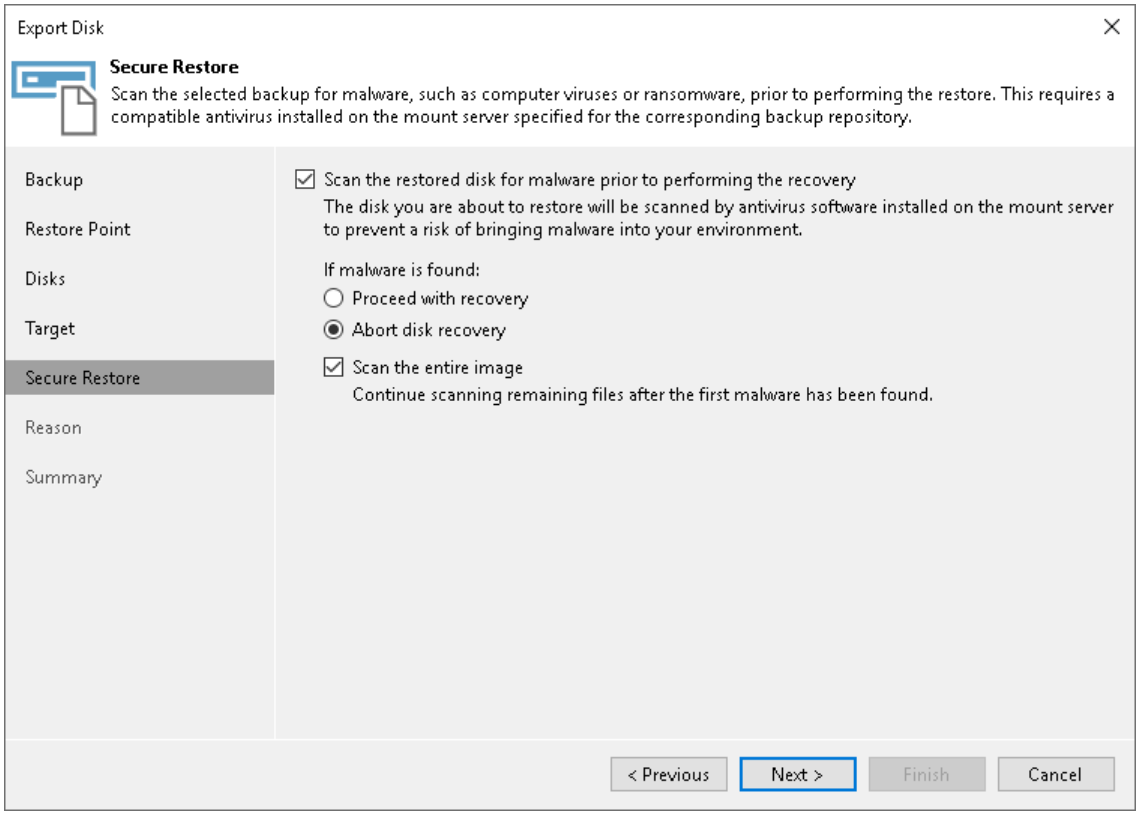
Step 6. Specify Secure Restore Settings

> **IMPORTANT**
>
> The **Secure Restore** step of the wizard is available if you export disks from a Veeam Agent backup of a Microsoft Windows computer.

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:

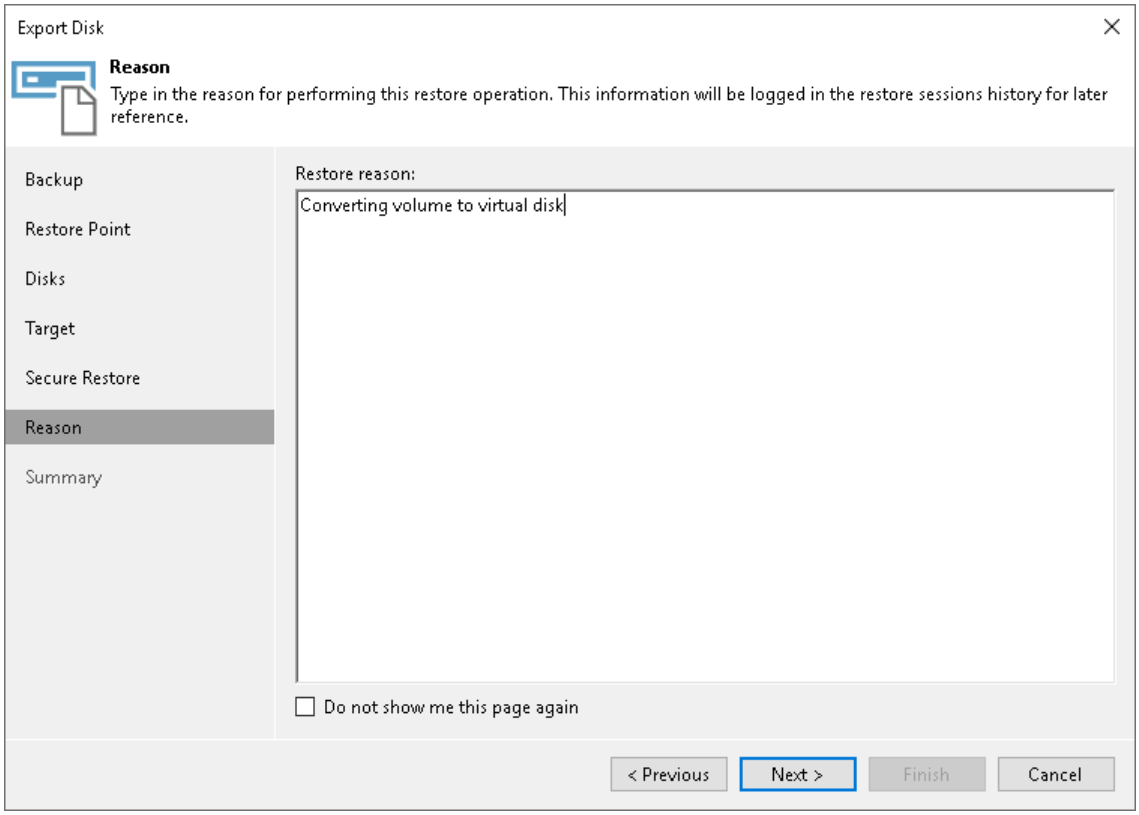
1. At the **Secure Restore** step of the wizard, select the **Scan the restored disk for malware prior to performing the recovery** check box.
2. Instruct Veeam Backup & Replication what to perform in case malware is found:
   - Select **Proceed with recovery** if you want to continue the recover process, despite the found malware threat.
   - Select **Abort disk recovery** if you want to stop the recovery process after the first malware threat is found.
3. 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.

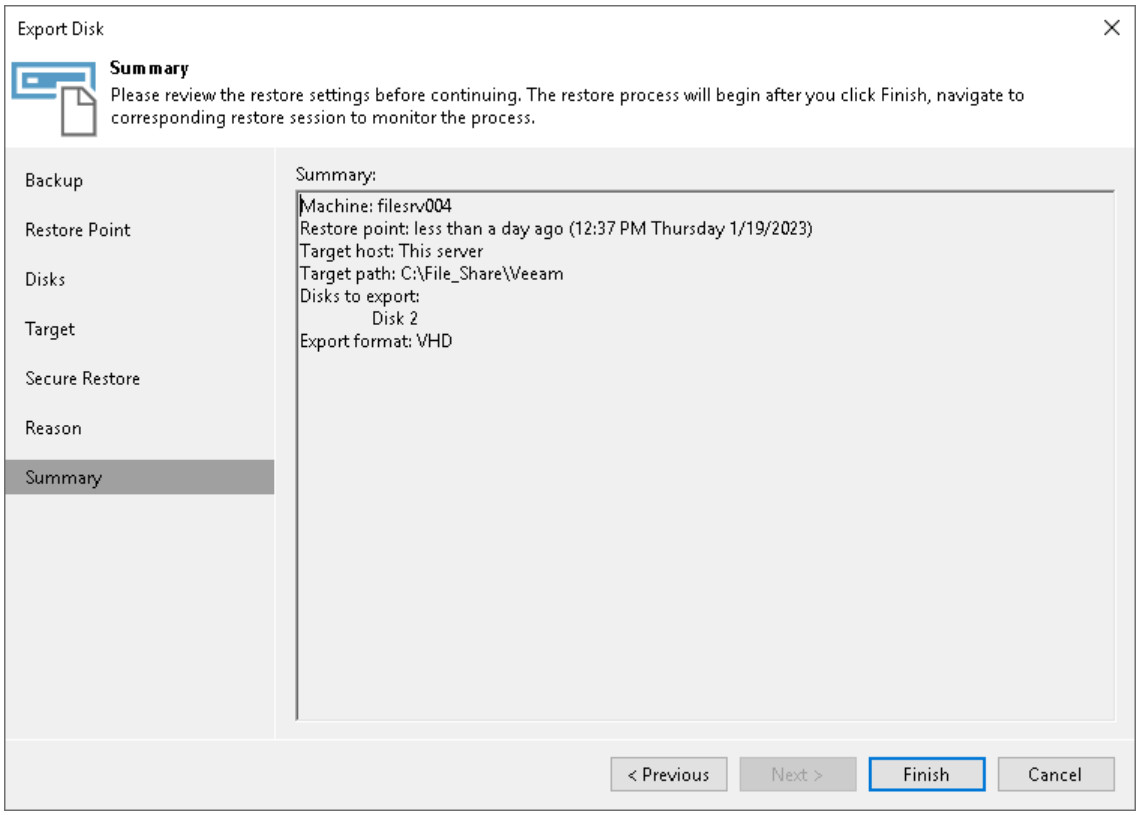
> **TIP**
>
> If you do not want to display the **Restore Reason** step of the wizard in future, select the **Do not show me this page again** check box.



Step 8. Complete Restore Process

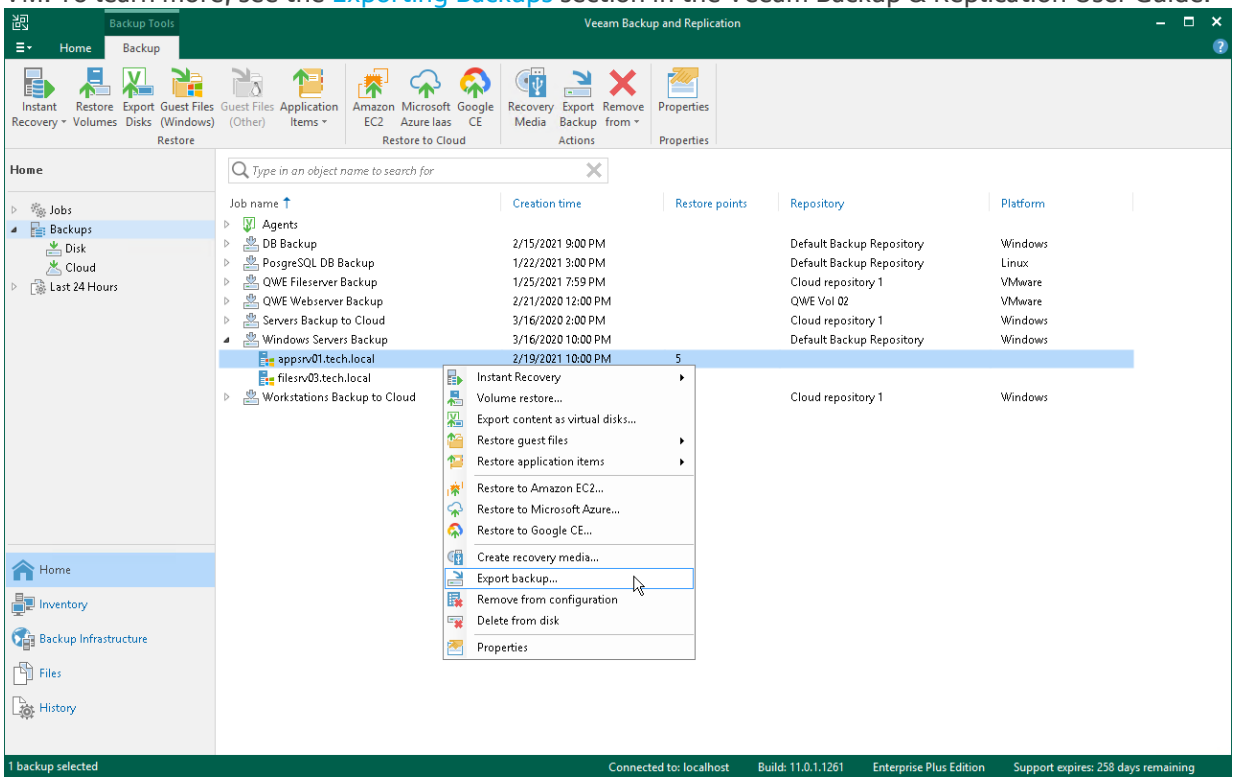
At the **Summary** step of the wizard, complete the disk restore procedure.

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 a SureBackup job
- Move a Veeam Agent backup to another backup job
- Create a backup copy job
- Create a recovery token
- Create Veeam Recovery Media for a computer.
- Remove a Veeam Agent backup from configuration.
- Delete a Veeam Agent backup from disk.
- View properties of a Veeam Agent backup.

Creating SureBackup

A SureBackup job is a task for recovery verification. The SureBackup job aggregates all settings and policies of the recovery verification task, such as application group and virtual lab to be used, Veeam Agent backups that must be verified in the virtual lab and so on. You can run the SureBackup job manually or schedule it to run automatically.

Getting Started

Before you configure a SureBackup job that will test your backup, you must complete the following steps:

1. Consider limitations listed in Recovery Verification for Veeam Agent Backups.
2. Prepare a backup that you will test using the SureBackup job:
   a. Add a computer to the inventory and deploy Veeam Agent on this computer using the Veeam Backup & Replication console. To learn more, see Creating Protection Groups.
   b. Create a backup job with the **Entire machine** or **Volume level backup** mode selected in the job settings. To learn more, Creating Veeam Agent Backup Jobs.
   c. Run the backup job to create a backup.
3. Configure the backup infrastructure to create the SureBackup job:
   a. Add a virtual lab. The virtual lab is an isolated virtual environment in which Veeam Backup & Replication will test your backups. VMware vSphere and Microsoft Hyper-V servers are supported. To learn more, see the Creating Virtual Lab section in the Veeam Backup & Replication User Guide.
   b. Add an application group. The application group provides a fully functional work for a host or a group of hosts that is created by Veeam Agent to test your backup. To learn more, see the Creating Application Groups section in the Veeam Backup & Replication User Guide.

      When you configure the application group, you must add the backup you want to test to this group.

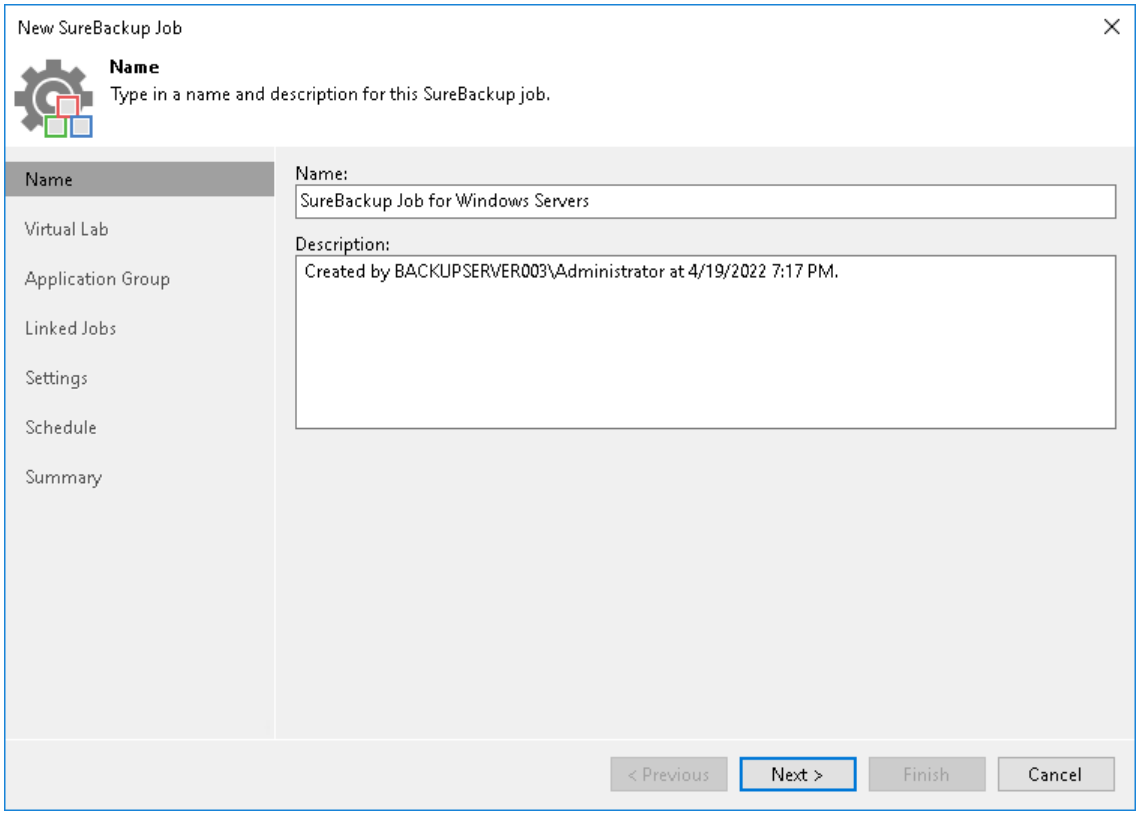
      > **TIP**
      >
      > Keep in mind that the application group is optional for the SureBackup job. If you do not create an application group, you can still use the backup job as a source of backups for the SureBackup job. In this case the SureBackup job will test all Veeam Agent backups created by this backup job. To learn more, see the Link Backup or Replication Job section in the Veeam Backup & Replication User Guide.

After all preparations are done, you can create the SureBackup job.

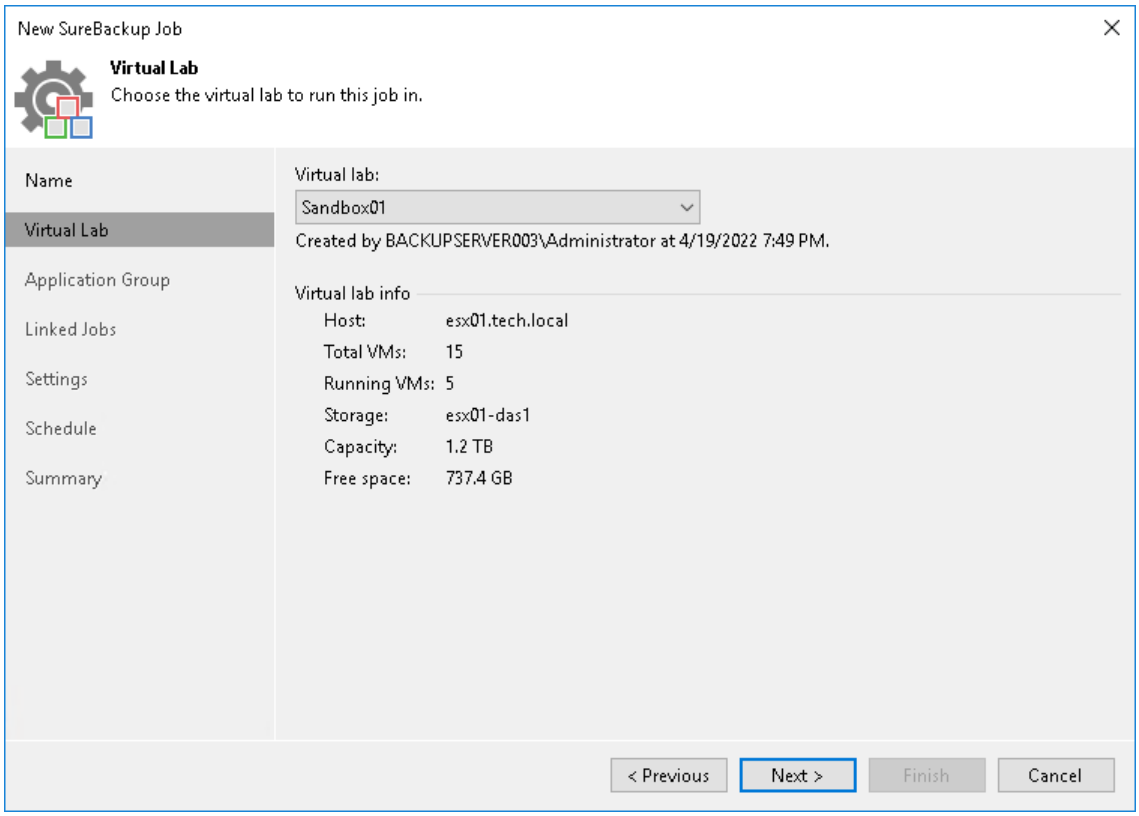
Creating SureBackup Job

To create a new SureBackup job, use the **New SureBackup Job** wizard.

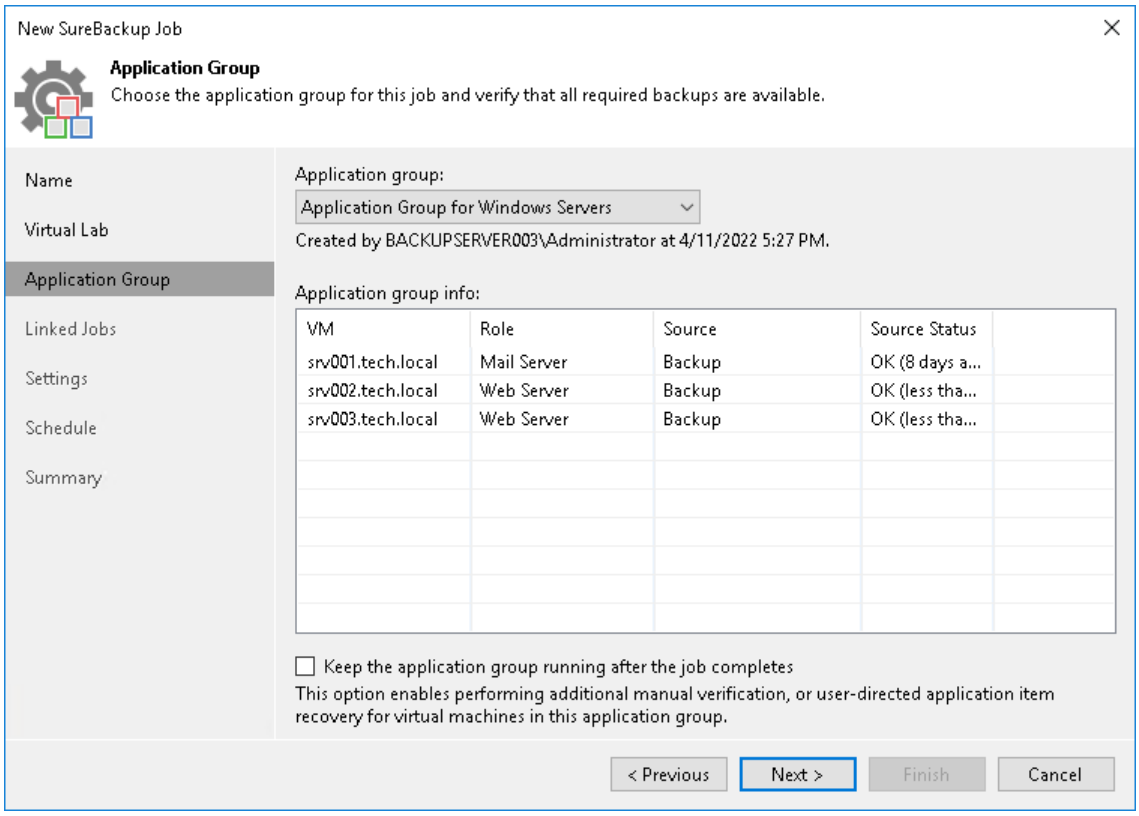
1. On the **Home** tab, click the **SureBackup** to launch the SureBackup Job wizard.
2. At the **Name** step of the wizard, specify a name and description for the SureBackup job.



3. At the **Virtual Lab** step of the wizard, select the virtual lab that Veeam Backup & Replication will use to recover your computer as a VM.



4. At the **Application Group** step of the wizard, select the application group with backups you want to test.



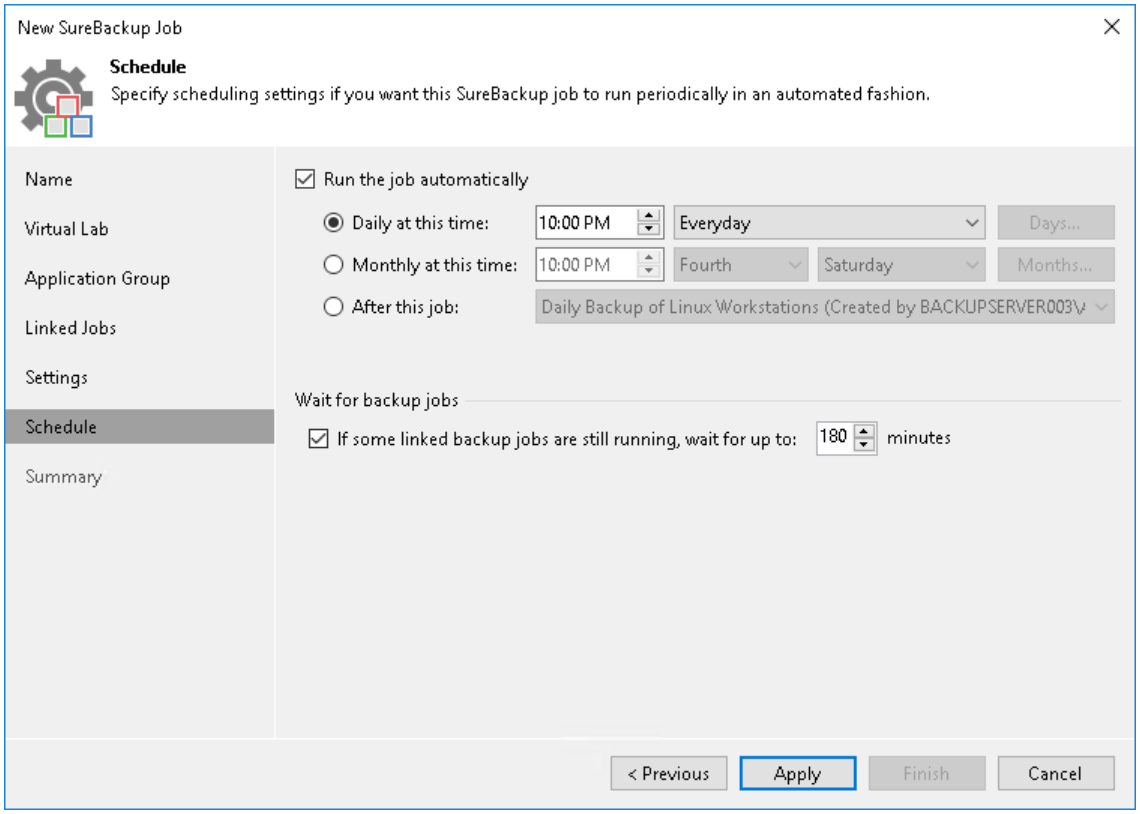
5. At the **Linked Jobs** step of the wizard, click **Next**.

> **TIP**
>
> You can link a backup job to the SureBackup job and use this backup job as a source of backups instead of the application group. To learn more, see the Link Backup or Replication Job section in the Veeam Backup & Replication User Guide. Consider that backup copy jobs cannot be sources for Veeam Agent backups.

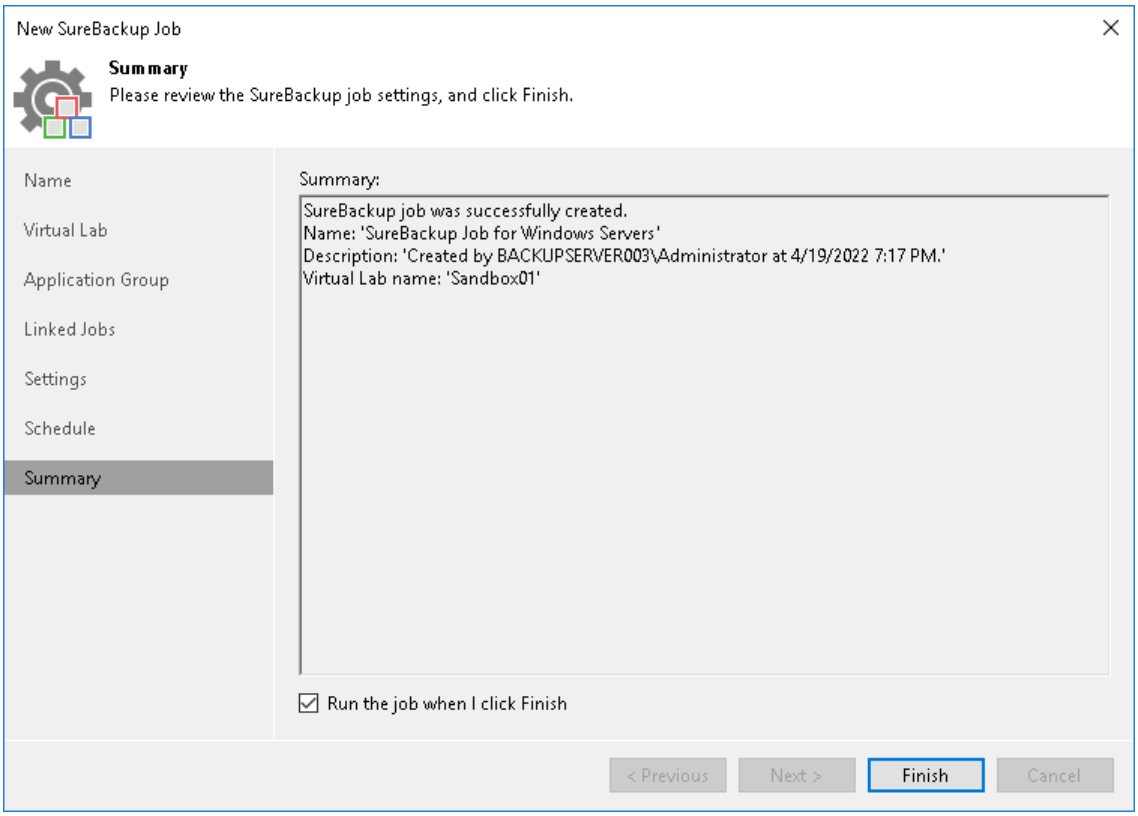
6. At the **Settings** step of the wizard, click **Next**. In this case Veeam Backup & Replication will perform a heartbeat test and a ping test. Using these tests, Veeam Backup & Replication will check that the VM is booted successfully: the guest OS is running and the VM responds to ping requests.

   If you want to perform more predefined or custom tests, see details in the Specify Additional Job Settings section in the Veeam Backup & Replication User Guide.

7. At the **Schedule** step of the wizard, select the **Run the job automatically** check box and specify time and days the job must start. By default, the SureBackup job starts daily at 10:00 PM.



8. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box if you want to start the SureBackup job right after you complete working with the wizard.



9. Click **Finish**.

Moving Backup

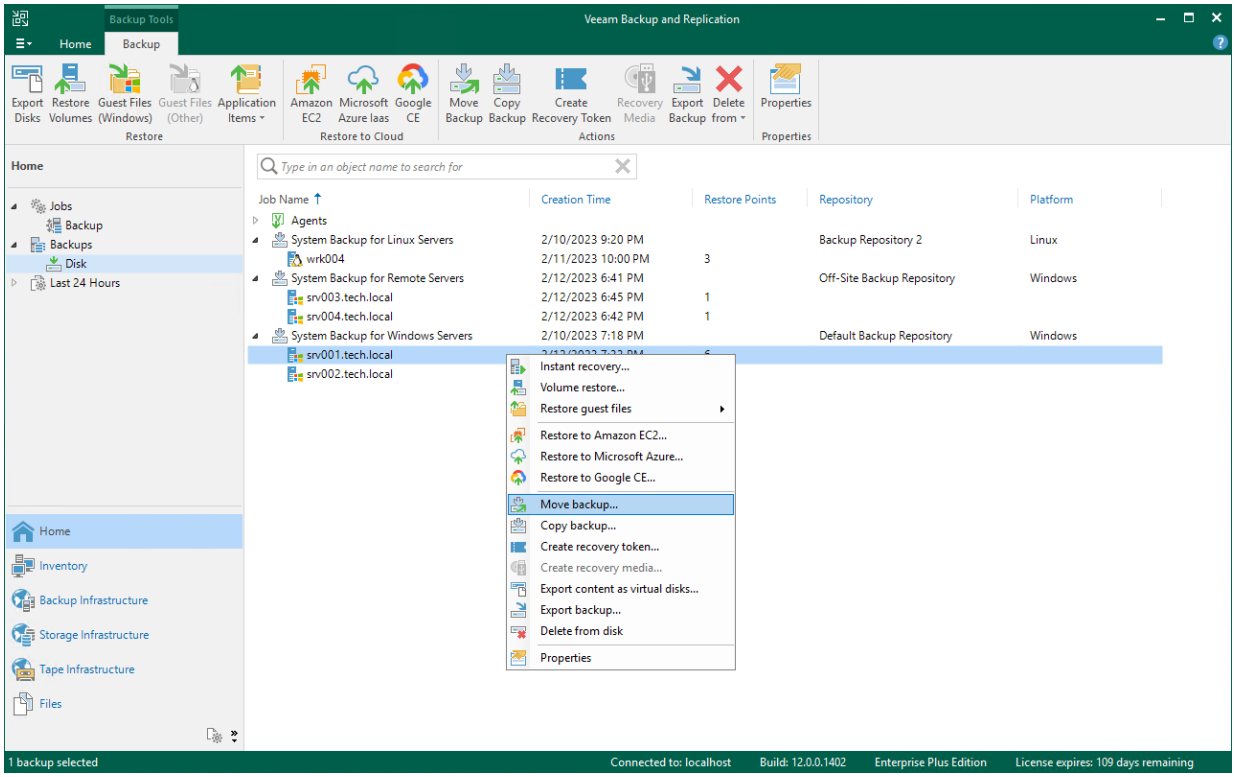
You can move backups created with Veeam Agent from one backup job to another.

To move a backup to another backup job:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, right-click the backup and select **Move backup**.
4. In the **Move Backup to Another Job** window, select the target backup job to which you want to move your backup.

   Keep in mind that Veeam Backup & Replication displays only those backup jobs in the list that have the same backup mode and backed-up computer type as the source backup job. For example, if your source job is a backup job managed by Veeam backup server for Windows-based computers, Veeam Backup & Replication will display in the list only backup jobs managed by Veeam backup server for Windows-based computers.

After the move operation is completed, all restore points of the backup will be displayed in the node of the target backup job.



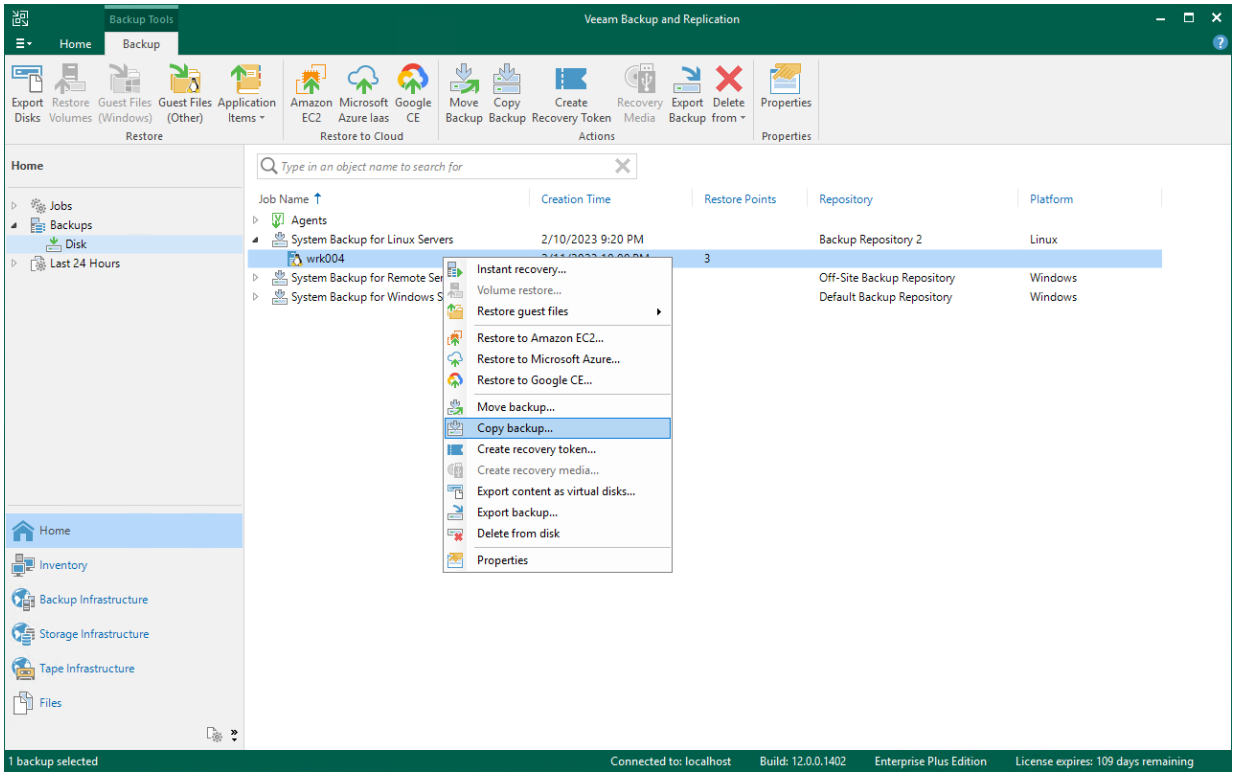
Copying Backup

Veeam Backup & Replication offers the backup copy functionality that allows you to create several instances of the same backup in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes. For more details, see the Copying Backups section of the Veeam Backup & Replication User Guide.

To create a backup copy:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, right-click the backup and select **Copy backup**.



Creating Recovery Token

If you want to recover volumes or an entire computer protected with Veeam Agent for Microsoft Windows or Veeam Agent for Linux, you can use the **Create recovery token** operation.

You can generate the recovery token on the Veeam Backup & Replication side. Then, on the computer side, with this recovery token get access to the backup and recover data that are stored in the backup.

> **TIP**
>
> Alternatively, you can get access to the backup using user credentials. To learn more, see one of the following sections depending on Veeam Agent you work with:
>
> - Veeam Agent for Microsoft Windows
> - Veeam Agent for Linux

Before creating a recovery token, consider the following prerequisites and limitations:

- Recovery tokens stay valid for 24 hours.
- You can recover files and folders from the selected backup only.
- During recovery, Veeam Backup & Replication does not stop backup operations.
- You cannot create a recovery token for backups stored in Veeam Cloud Connect repository.
- You cannot create a recovery token for a whole backup copy job, but you can create a recovery token for individual objects included in a backup copy job.
- If you work with scale-out backup repositories (SOBR), you cannot create a recovery token for backups displayed in **Capacity** and **Archive** nodes in the inventory pane. To create a recovery token for such backups, select the backup in the **Backups** node in the inventory pane.

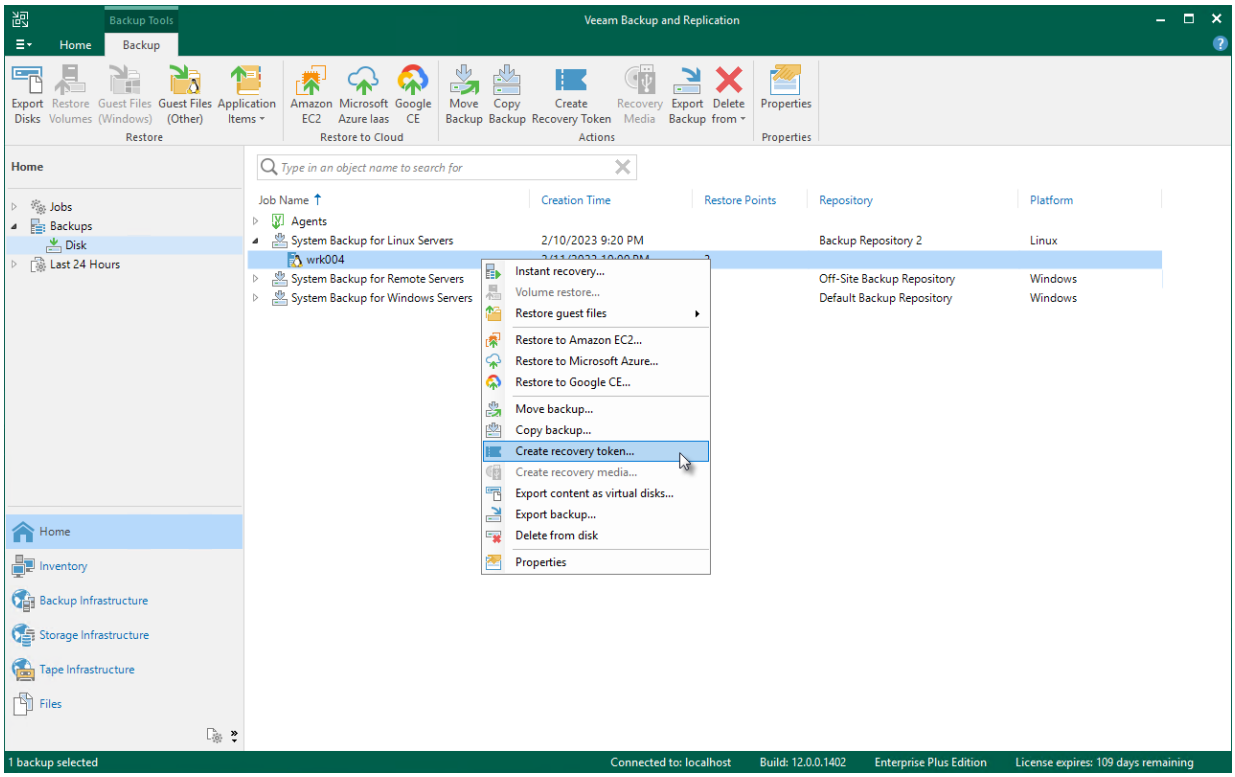
Generating Recovery Token

To create a recovery token on the Veeam Backup & Replication side:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, right-click the backup and select **Create recovery token**.

You can modify the existing recovery token using the PowerShell console. To learn more, see the Working with Tokens section in Veeam PowerShell Reference.

To learn how to access the backup with the recovery token on the Veeam Agent computer side, see Accessing Backup.



Accessing Backup

To access the backup using recovery token on the Veeam Agent computer side:

1. Use the Veeam Recovery Media to recover your computer.
2. Select to restore data from a backup file located in a Veeam backup repository.
3. Specify recovery token to gain access to the backup file.

To learn more, see one of the following sections depending on Veeam Agent you work with:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux

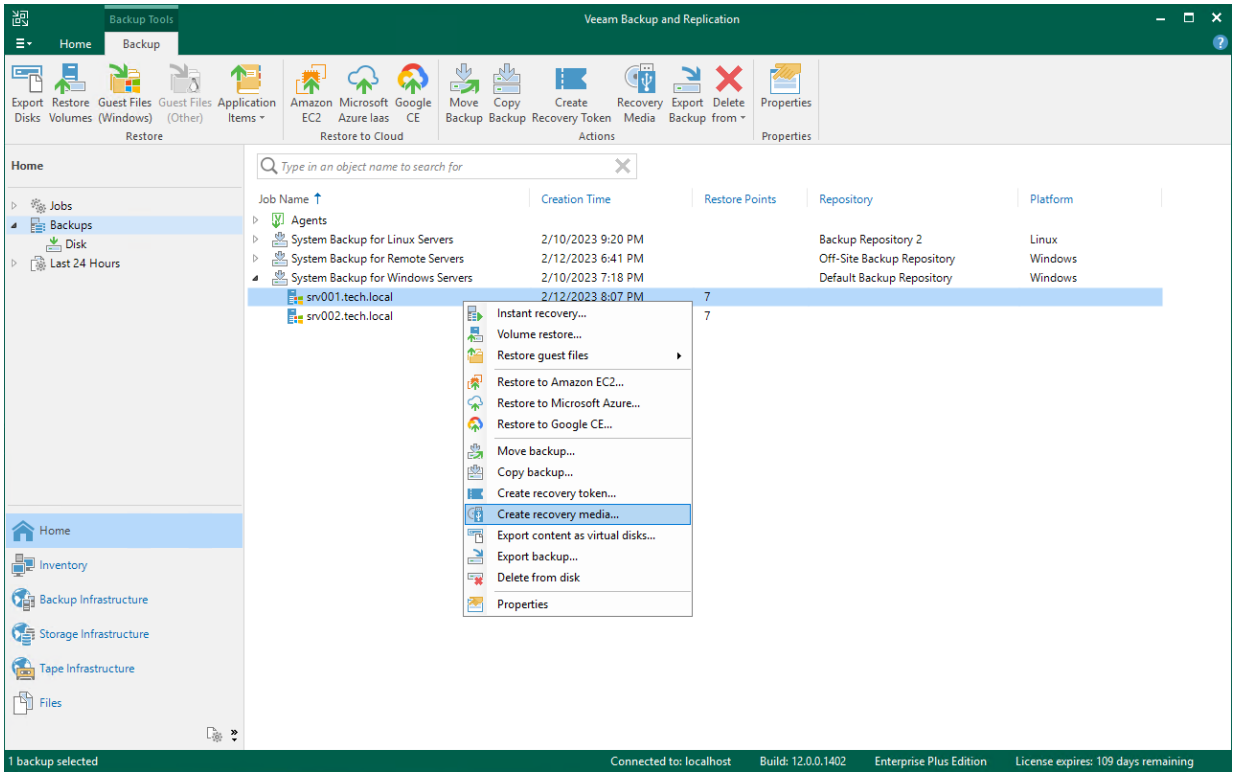
Creating Veeam Recovery Media from Backup

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.

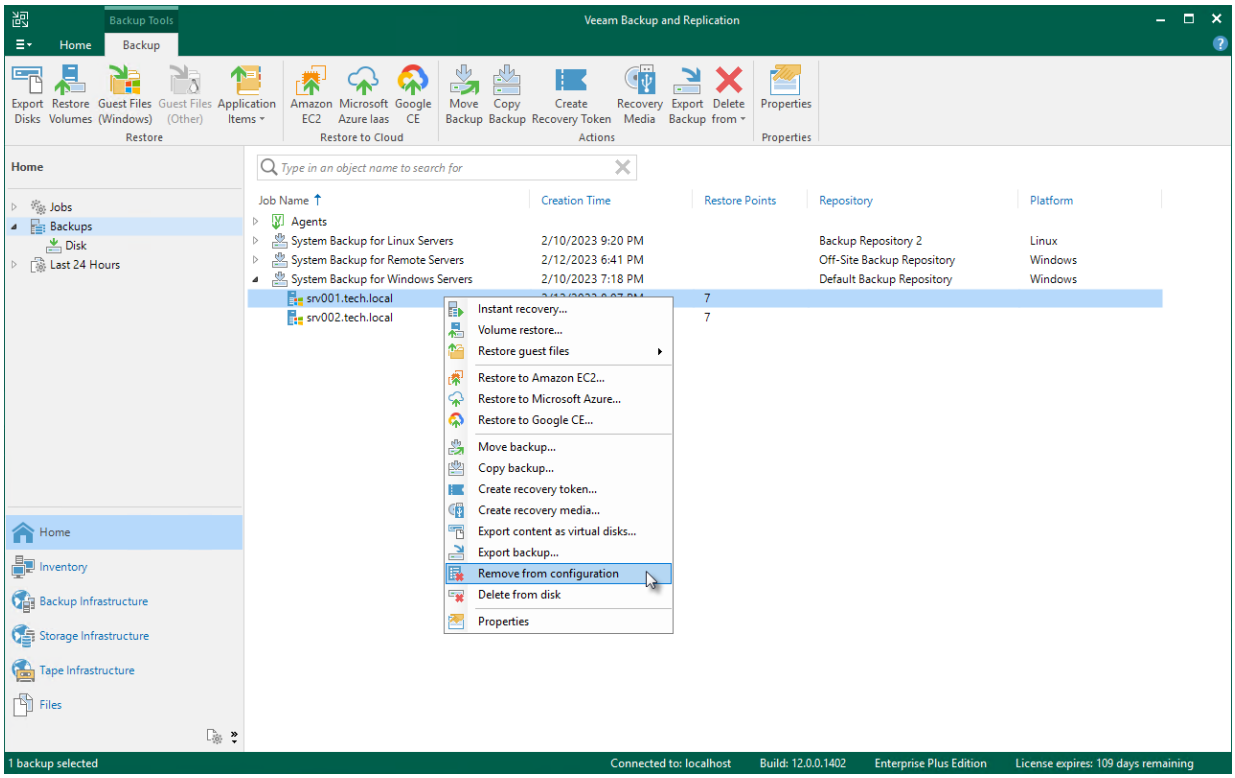
> **NOTE**
>
> Mind the following:
>
> - You can use the Veeam Backup & Replication console to remove backups created by Veeam Agent backup jobs on the Veeam backup repository. Backups created on a local drive of a protected computer or in a network shared folder are not displayed in the Veeam backup console.
> - If you remove from configuration a backup of a failover cluster node, backup of all nodes of this failover cluster will be removed.

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, press and hold the [CTRL] key, 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, press and hold the [CTRL] key, 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

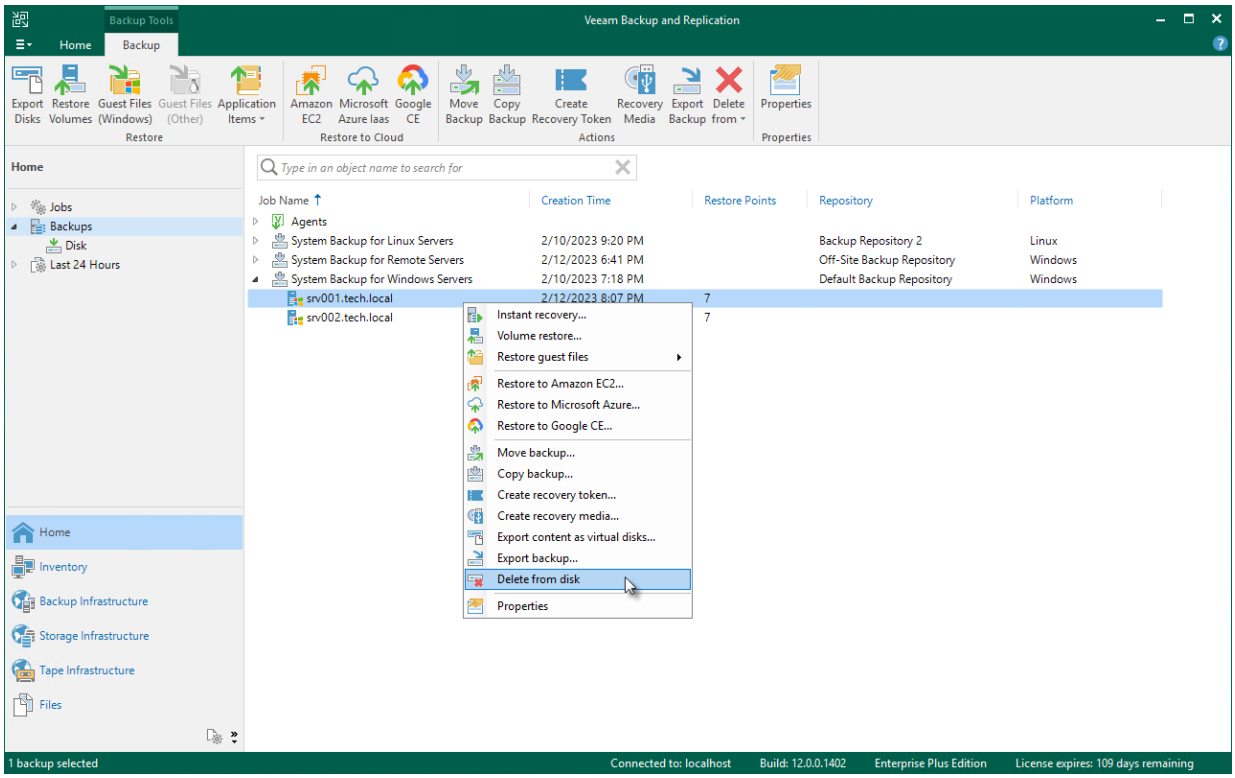
If you want to delete records about backups from the Veeam Backup & Replication console and configuration database and, additionally, delete backup files from the backup repository, you can use the **Delete from disk** operation.

> **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.
> - If you delete a backup of a failover cluster node, backup of all nodes of this cluster will be deleted.

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 **Delete 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 **Delete 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:

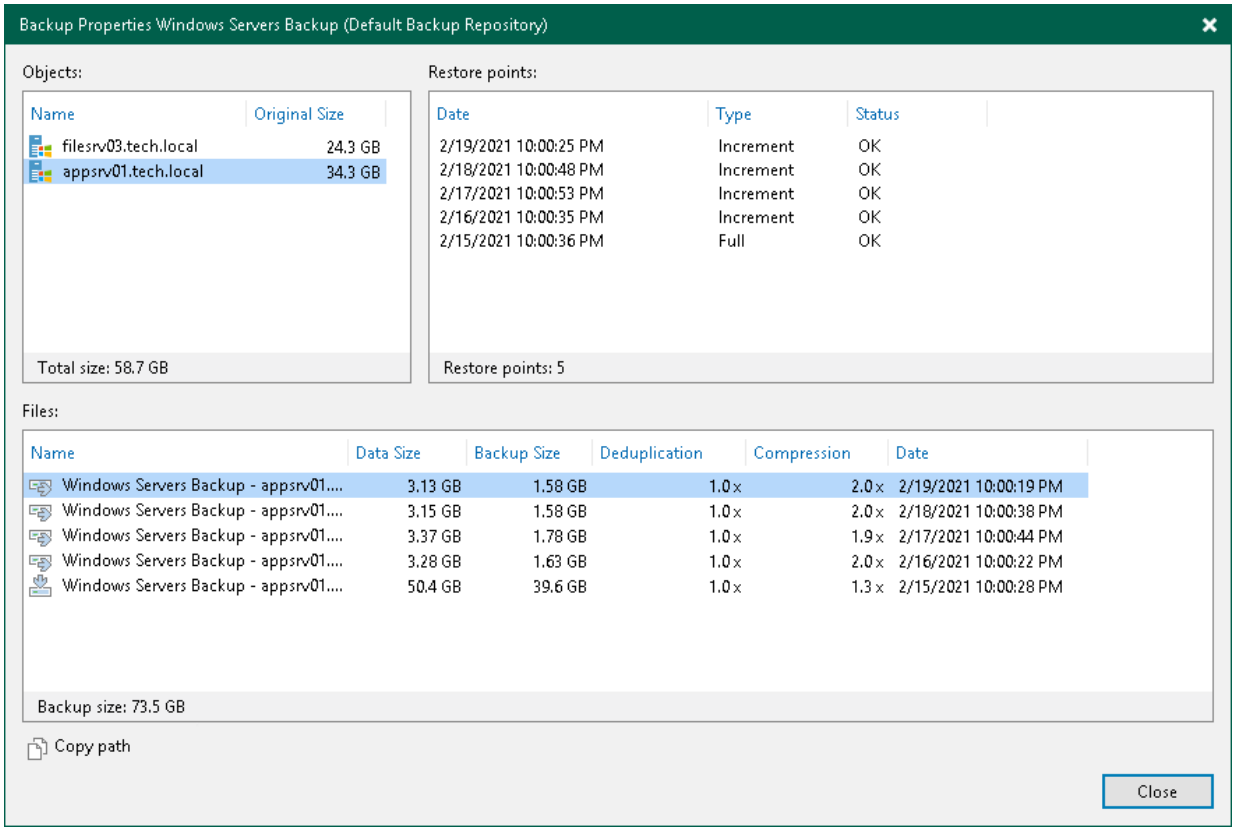
- Backup location
- Available restore points
- Date of restore points creation
- Compression and deduplication ratios
- Data size and backup size

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)

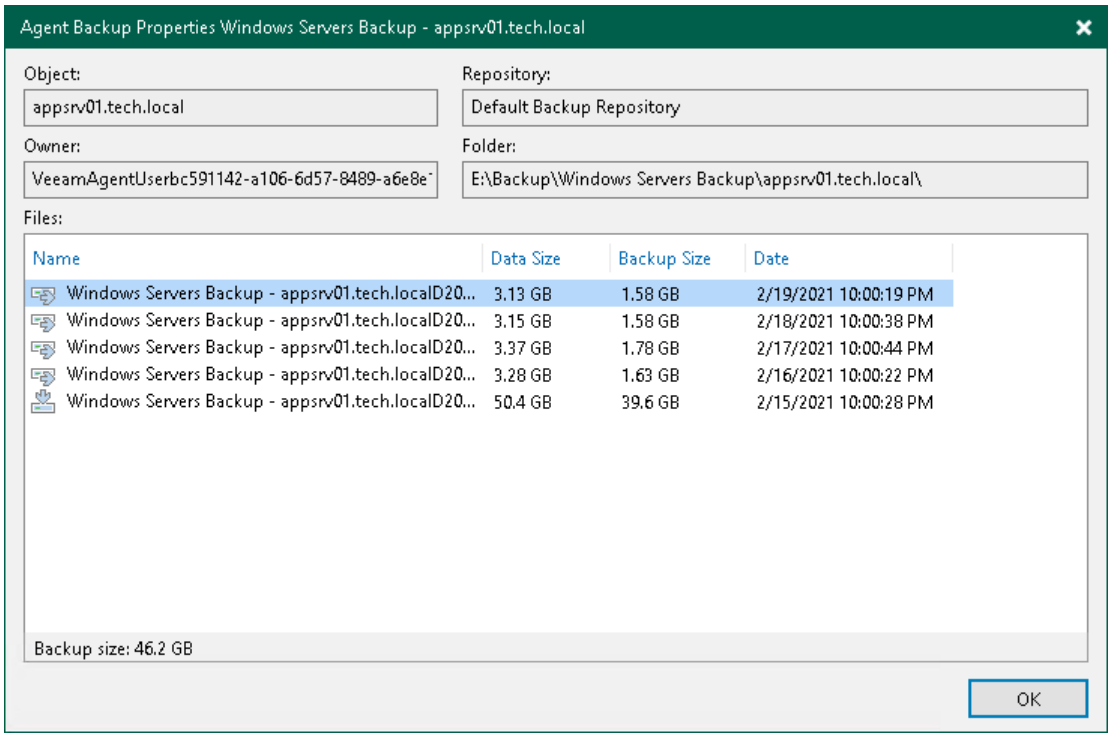
To view summary information for a parent backup:

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**.



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.

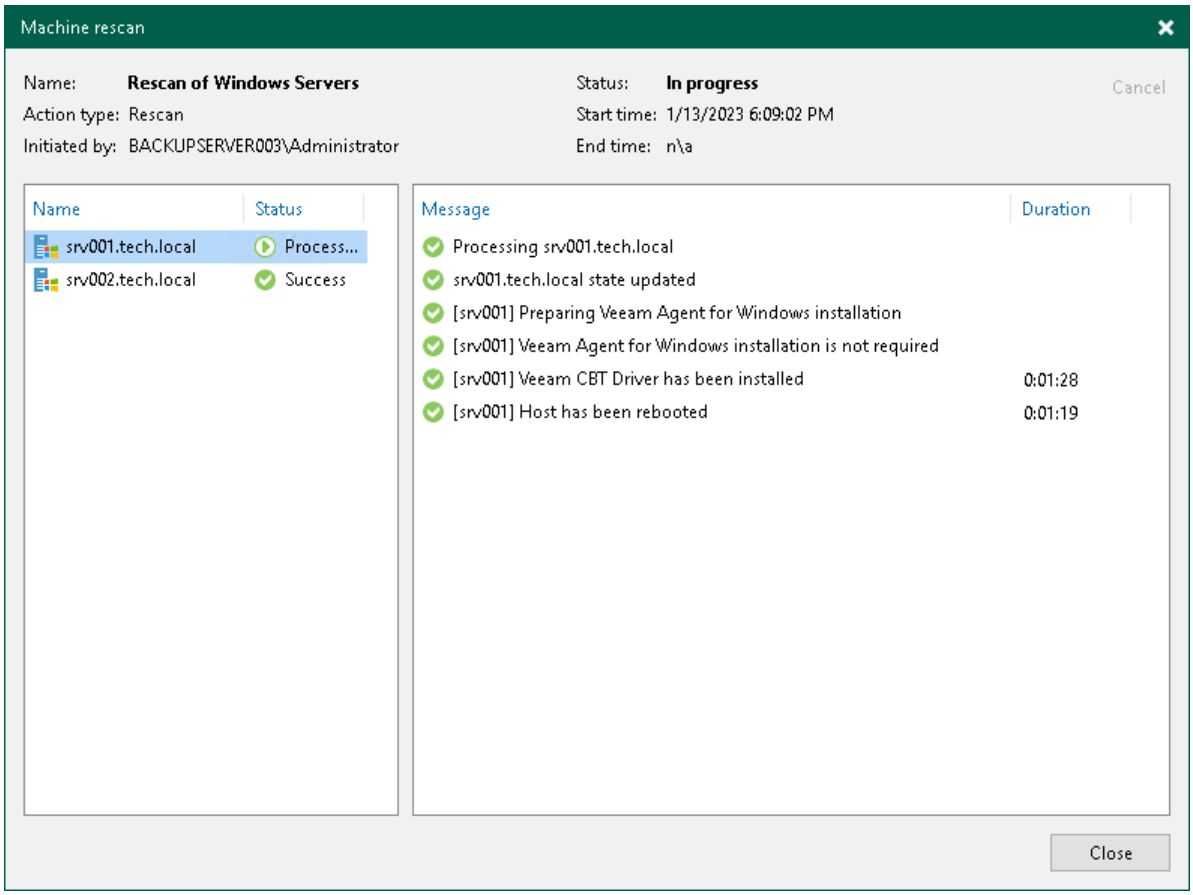
Viewing Rescan Job Statistics

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.

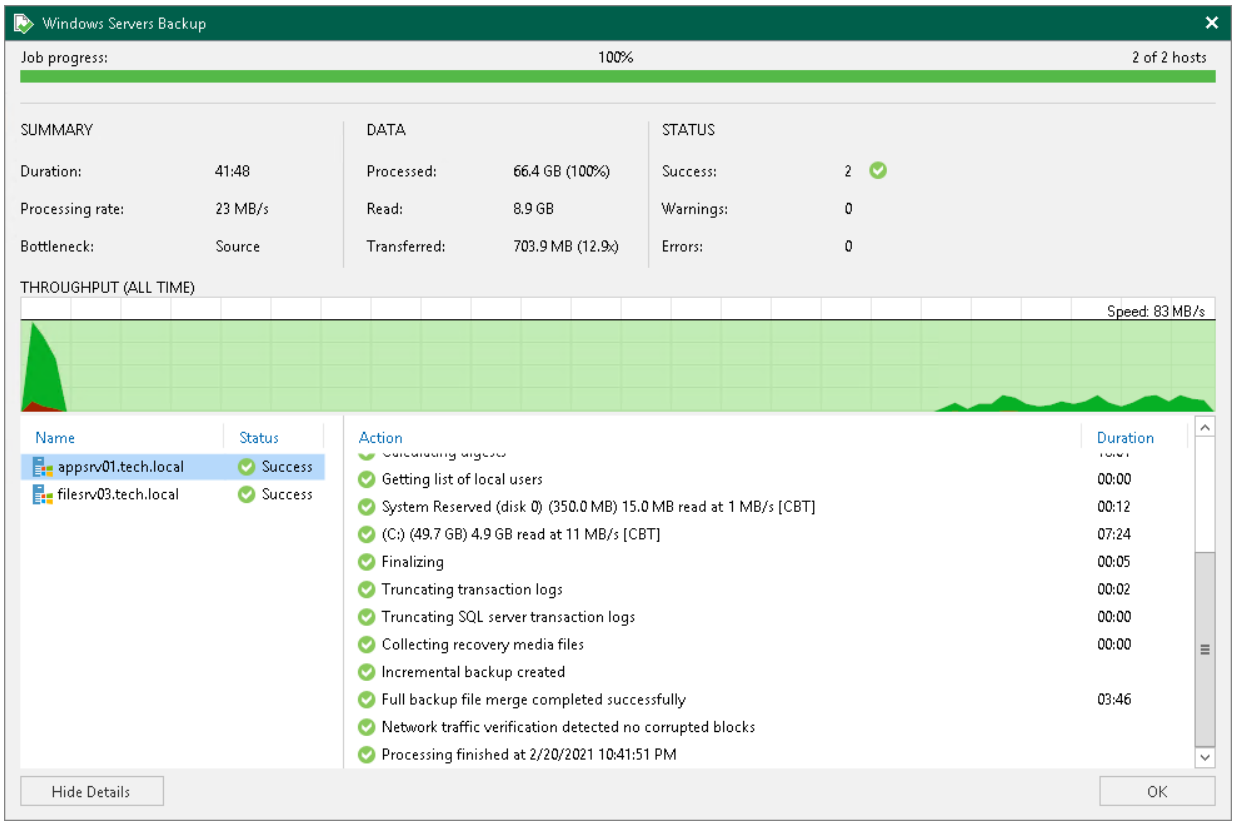
Windows Servers				Success
Assigned	2	**Success**	2	
Seen	2	**Warnings**	0	
Updated	2	**Errors**	0	
Name	**IP address**	**Status**	**Operating System**	**Details**
appsrv01.tech.local	172.24.30.120	Success	Microsoft Windows Server 2012 R2 (64-bit)	Backup agent has been installed.
filesrv03.tech.local	172.24.30.121	Success	Microsoft Windows Server 2012 R2 (64-bit)	Backup agent has been installed.

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 — **Success** — 2 of 2 hosts processed

Saturday, February 20, 2021 10:00:08 PM

Success	2	**Start time**	10:00:08 PM	**Total size**	90.2 GB	**Backup size**	703.9 MB	
Warning	0	**End time**	10:41:57 PM	**Data read**	8.9 GB	**Dedupe**	1.0x	
Error	0	**Duration**	0:41:48	**Transferred**	703.9 MB	**Compression**	2.7x	

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
filesrv03.tech.local	Success	10:00:28 PM	10:11:51 PM	40.2 GB	4 GB	420.2 MB	0:11:23	
appsrv01.tech.local	Success	10:00:33 PM	10:41:51 PM	50 GB	4.9 GB	283.7 MB	0:41:18	

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, in a Veeam Cloud Connect repository, or in object storage using the direct connection mode, 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:

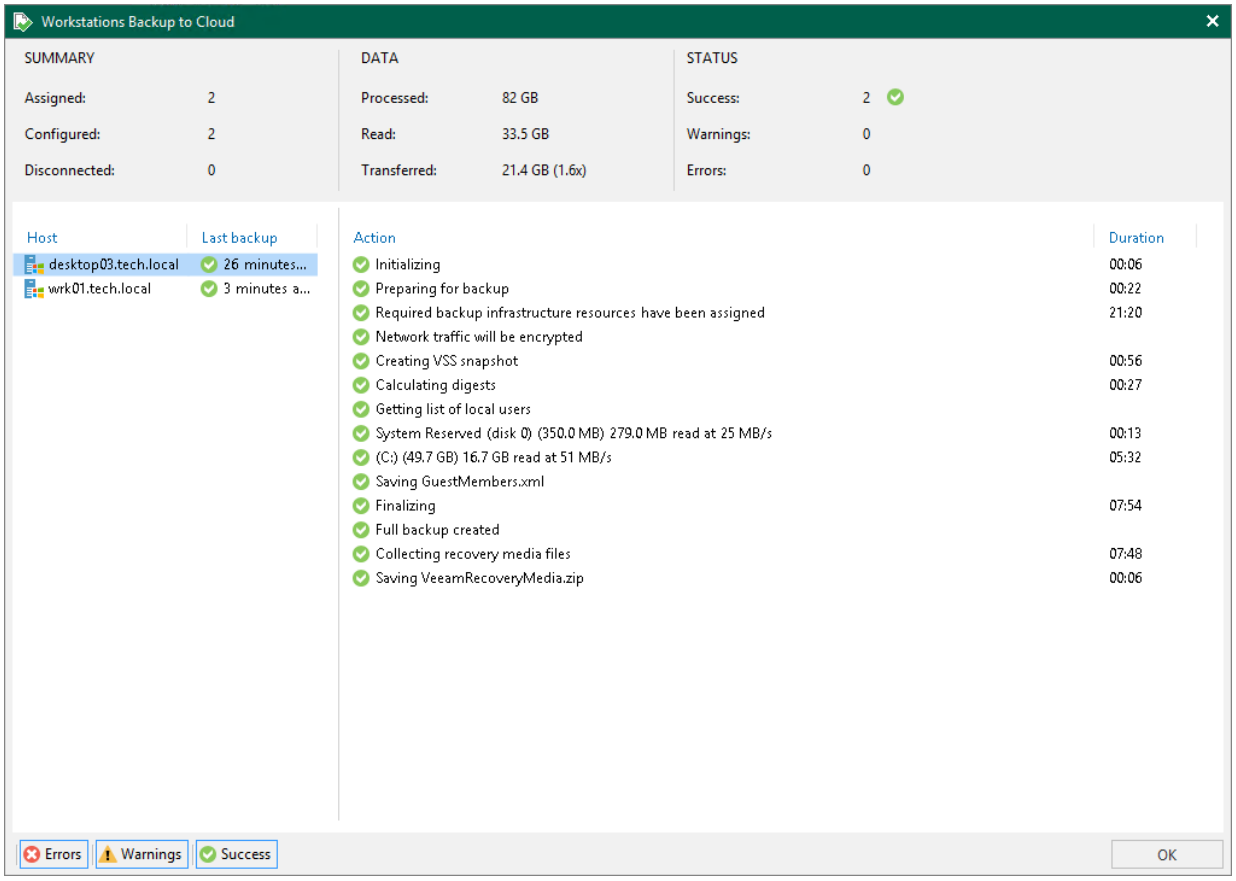
- For backup policies, Veeam Backup & Replication does not display the job progress bar. You can monitor backup progress only for individual computers in the backup policy.
- Detailed statistics include the number of Veeam Agent computers specified in the backup policy settings, the number of computers to which settings of the backup policy are applied, and the number of computes 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 **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 computes, 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).
- Detailed statistics for the application process if you edit the backup policy. In this case Veeam Backup & Replication applies the backup policy to protected computers and includes information about this process in the next job session report.

> **TIP**
>
> You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.

Workstations Backup to Cloud — **Success** — 2 of 2 hosts processed

Assigned	2	**Processed**	82 GB	**Success**	2
Configured	2	**Read**	5.5 GB	**Warnings**	0
Disconnected	0	**Transferred**	2 GB	**Errors**	0

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
desktop03.tech.local	Success	10/15/2020 11:00:00 PM	10/15/2020 11:05:23 PM	50 GB	3.5 GB	1.2 GB	00:05:23	
wrk01.tech.local	Success	10/15/2020 11:00:00 PM	10/15/2020 11:09:21 PM	32 GB	2 GB	754 MB	00:09:21	

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)
- Notification Settings for Backup Policy (for Unix computers)
- Notification Settings for Backup Policy (for macOS computers)

Appendix A. Deploying Hotfix on Protected Computers

This scenario describes how to deploy a hotfix on protected computers with installed Veeam Agent for Microsoft Windows or Veeam Agent for Linux:

- A Veeam Agent for Microsoft Windows hotfix is an updated Veeam Agent setup archive that addresses a certain issue in the product.
- A Veeam Agent for Linux hotfix 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.
- [For Veeam Agent for Linux hotfix] To add support of a new Linux distribution version to the product. In this case, a hotfix is available in the Veeam software repository.

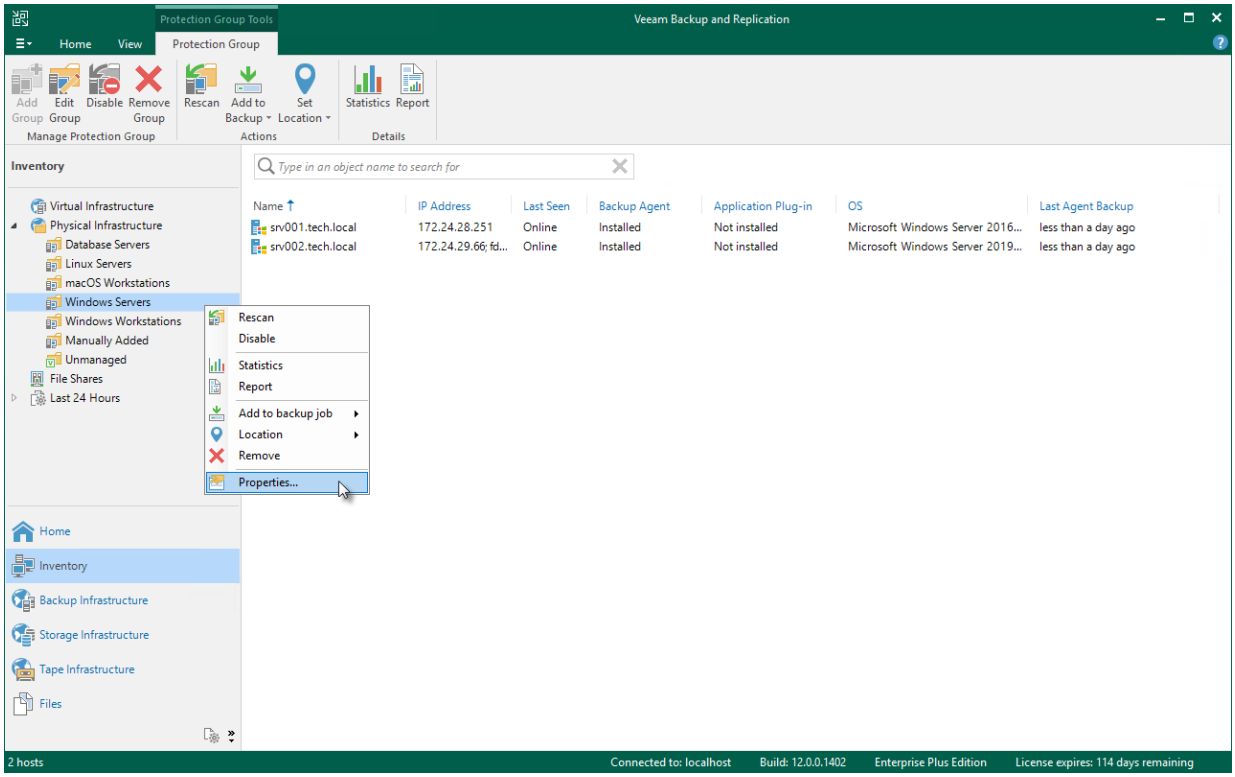
If you have several Microsoft Windows and Linux computers with Veeam Agent installations managed by Veeam Backup & Replication, you can centrally deploy a hotfix on all managed agents. Keep in mind that this scenario is not available for Veeam Agent computers add

Prerequisites

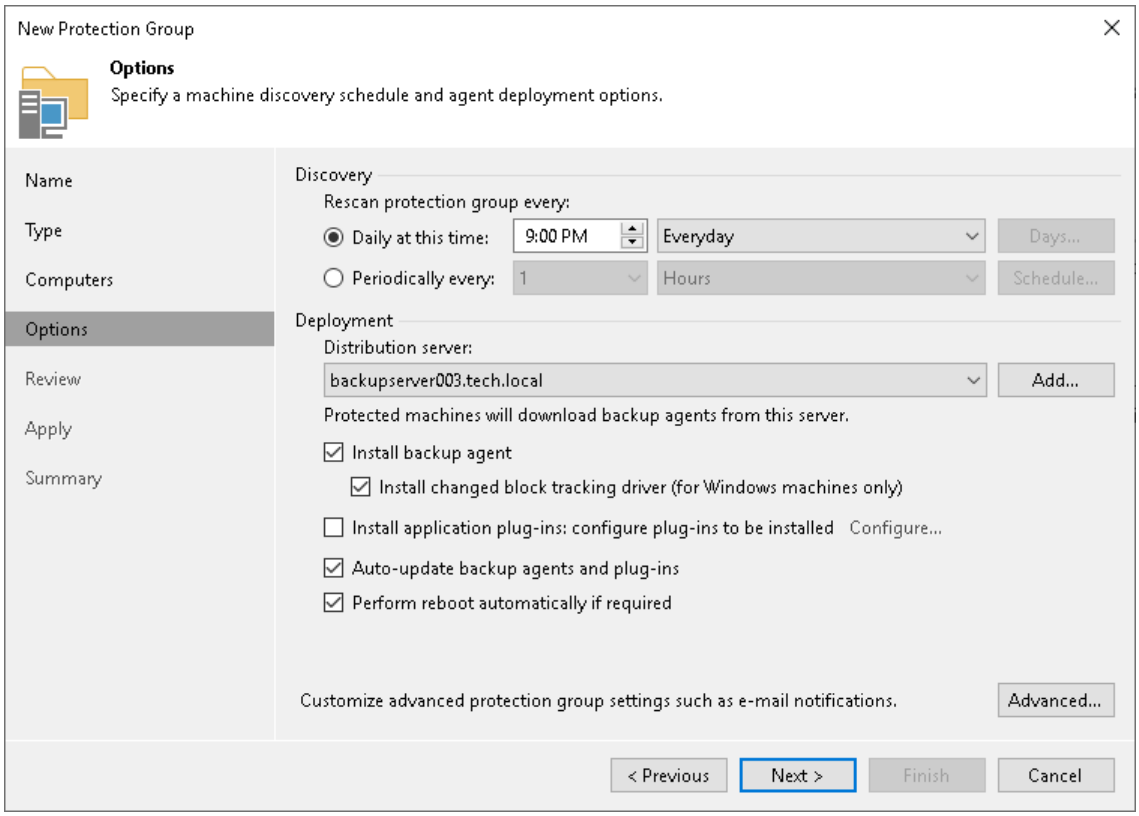
Before you deploy a Veeam Agent hotfix on protected computers:

1. Check that protected computers are powered on and can be connected over the network.
2. Check that there are no running jobs.

   We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic jobs temporarily to prevent them from starting during the upgrade. If protected computers run VSS-aware applications and backup of database logs (Microsoft SQL Server transaction logs or Oracle archived logs) is enabled in the backup job for these computers, disable this backup job too.
3. Check that automatic Veeam Agent deployment options are enabled in the protection group settings:
   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, make sure that the **Install backup agent automatically** and **Auto-update backup agent** check boxes are selected.



4. Determine a location for the hotfix distribution:

   a. If you plan to deploy a Veeam Agent for Microsoft Windows hotfix, you will need to place the hotfix to a folder on the backup server.

   b. If you plan to deploy a Veeam Agent for Linux hotfix, you will need to place the hotfix to a folder on the distribution server specified for the protection group.

      Each protection group can have a different distribution server, so you need to place the hotfix on the distribution server of each protection group that contains Veeam Agent computers on which you need to deploy a hotfix.

Deployment Procedure for Protected Computers

The hotfix deployment procedure differs depending on the OS running on the protected computers:

- Deployment procedure for Microsoft Windows computers
- Deployment procedure for Linux computers

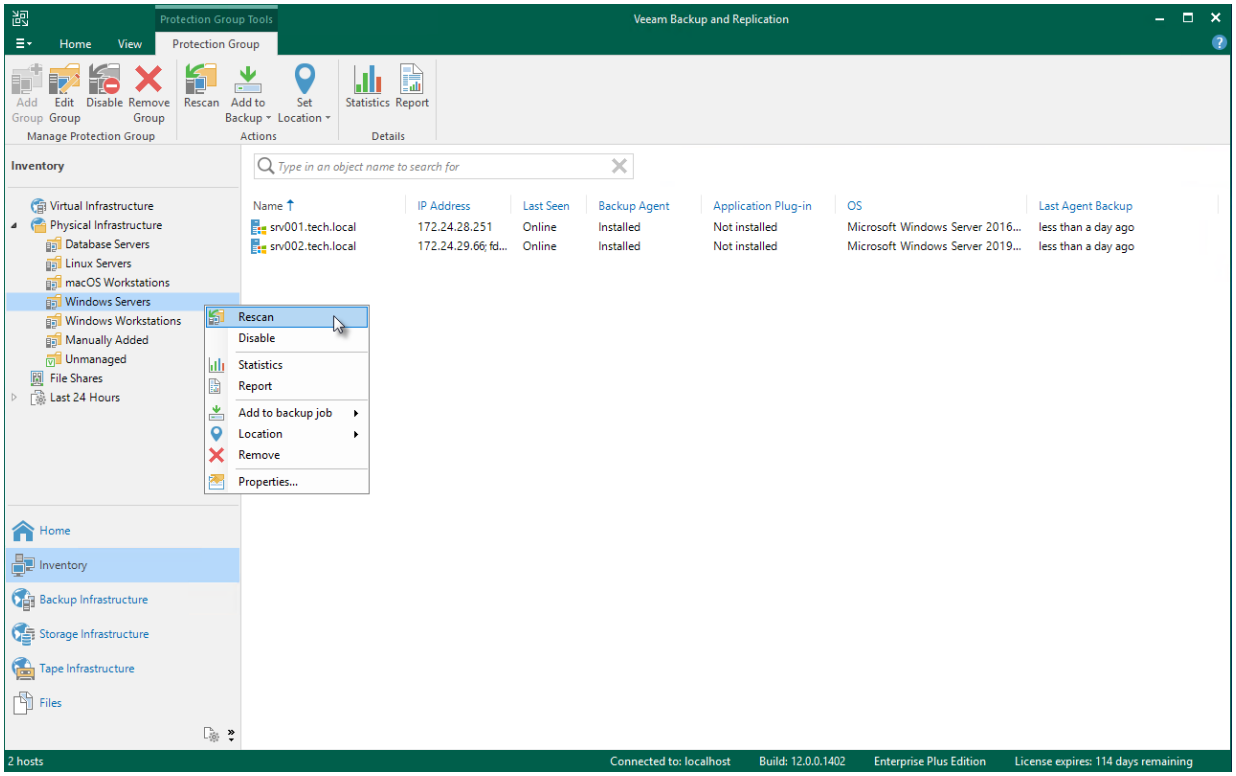
Deployment Procedure for Windows Computers

To deploy a hotfix on Microsoft Windows computers included in the protection group, perform the following steps:

1. Obtain a hotfix from Veeam Customer Support.
2. Save the Veeam Agent for Microsoft Windows setup archive to the following folder on the backup server:

   ```
   C:\Program Files\Veeam\Veeam Distribution Service\Fixes\vaw
   ```

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**.



Deployment Procedure for Linux Computers

To deploy a hotfix on Linux computers included in the protection group, perform the following steps:

1. Obtain a hotfix from Veeam Customer Support or download it from the Veeam software repository.
2. Save Veeam Agent for Linux packages to the following folder on the distribution server specified in the protection group settings:

   For 32-bit CentOS / RHEL / Oracle Linux / Fedora / openSUSE / SLES

   ```
   C:\ProgramData\Veeam\Agents\val\x86\rpm
   ```

   For 64-bit CentOS / RHEL / Oracle Linux / Fedora / openSUSE / SLES

   ```
   C:\ProgramData\Veeam\Agents\val\x64\rpm
   ```

   For 32-bit Debian / Ubuntu

   ```
   C:\ProgramData\Veeam\Agents\val\x86\deb
   ```

   For 64-bit Debian / Ubuntu

   ```
   C:\ProgramData\Veeam\Agents\val\x64\deb
   ```

3. Replace names of Veeam Agent for Linux package in the index file.

   a. Open the `ValPackageIndex.xml` file that is located in the following folder on the distribution server specified in the protection group settings:

   ```
   C:\ProgramData\Veeam\Agents\val
   ```

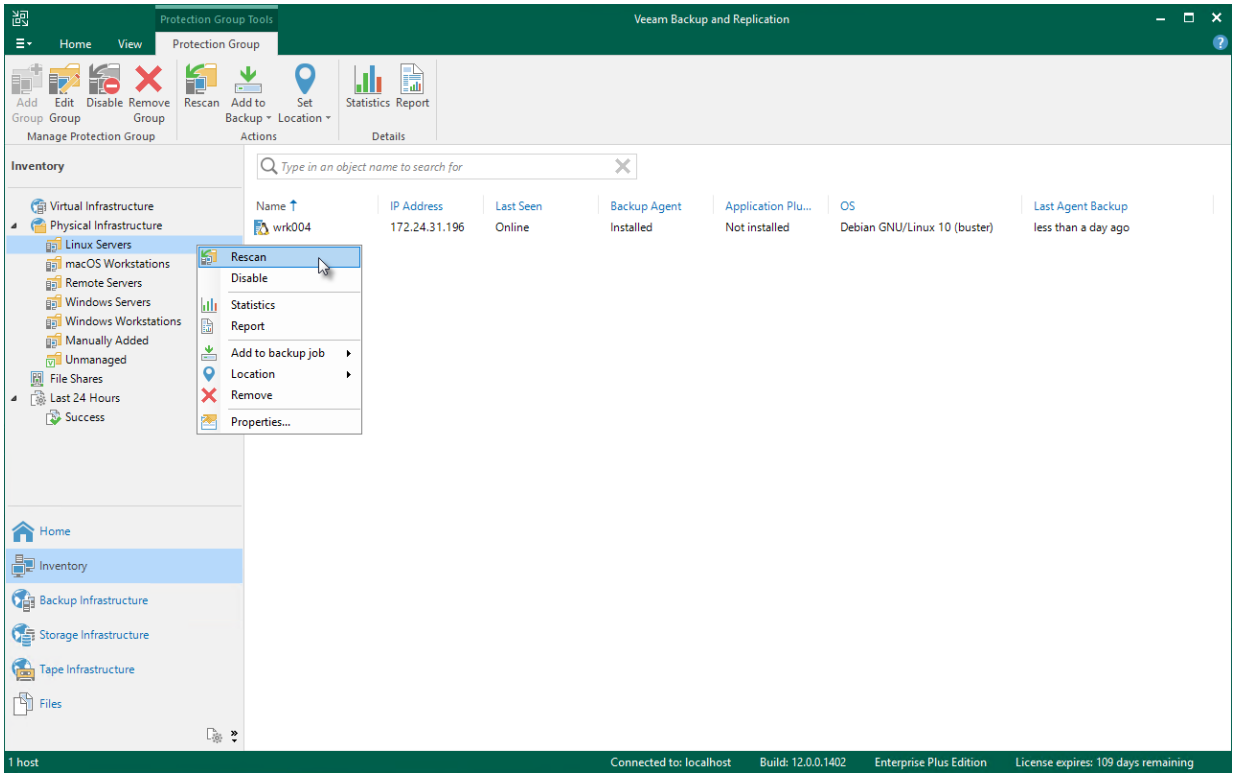
   b. In the `ValPackageIndex.xml` file, locate packages that you want to update. Replace their names with names of Veeam Agent for Linux packages you saved in step 2. After that, save changes and close the index file. For more detailed explanation, see Example.

4. 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**.



Example

For example, Veeam Software issued a hotfix for Veeam Agent for Linux 6.0 for 64-bit RHEL 8 and you want to deploy it on your Veeam Agent computers.

In this scenario, the hotfix consists of the following Veeam Agent packages:

- `veeamsnap-6.0.0.XXXX-1.noarch.rpm`
- `veeam-6.0.0.XXXX-1.el8.x86_64.rpm`
- `kmod-veeamsnap-6.0.0.XXXX-1.el8.x86_64.rpm`

To deploy the hotfix, you need to do the following:

1. Obtain all three updated Veeam Agent for Linux packages from Veeam Customer Support or download them from the Veeam software repository.
2. Save the packages to the following folder on the distribution server specified in the protection group settings:

   ```
   C:\ProgramData\Veeam\Agents\val\x64\rpm
   ```

   You do not need to delete obsolete Veeam Agent for Linux packages you want to update.
3. Edit the index file located in the following folder on the distribution server specified in the protection group settings:

   ```
   C:\ProgramData\Veeam\Agents\val
   ```

   a. Open the `ValPackageIndex.xml` file.

   b. Locate the packages that you want to update and replace their version and names with version and names of the packages you saved is step 2.

   Usually, the packages that are available as a hotfix have a build version that is different from the obsolete packages. In this scenario, obsolete packages have the 6.0.0.1060 build version and the updated packages have the 6.0.0.XXXX build version.

In the example below, replaced package version and names are highlighted in green:

```
...
<Distribution id="RHEL" displayName="Red Hat">
  <Version majorVersions="6">
     <Packages version="6.0.0.1060" arch="x64">
        <driver_noarch value="veeamsnap-6.0.0.1060-1.noarch.rpm"/>
        <driver_uefi_cert value="veeamsnap-ueficert-6.0.0.1060-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-6.0.0.1060-
2.6.32_131.0.15.el6.x86_64.rpm"/>
        <veeam value="veeam-6.0.0.1060-1.el6.x86_64.rpm" />
     </Packages>
     <Packages version="6.0.0.1060" arch="x86">
        <driver_noarch value="veeamsnap-6.0.0.1060-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-6.0.0.1060-
2.6.32_131.0.15.el6.i386.rpm"/>
        <veeam value="veeam-6.0.0.1060-1.el6.i386.rpm"/>
     </Packages>
  </Version>
  <Version majorVersions="7">
     <Packages version="6.0.0.1060" arch="x64">
        <driver_noarch value="veeamsnap-6.0.0.1060-1.noarch.rpm"/>
        <driver_uefi_cert value="veeamsnap-ueficert-6.0.0.1060-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-6.0.0.1060-1.el7.x86_64.rpm"/>
        <veeam value="veeam-6.0.0.1060-1.el7.x86_64.rpm"/>
     </Packages>
  </Version>
  <Version majorVersions="8">
     <Packages version="6.0.0.XXXX" arch="x64">
        <driver_noarch value="veeamsnap-6.0.0.XXXX-1.noarch.rpm"/>
        <driver_uefi_cert value="veeamsnap-ueficert-6.0.0.1060-1.noarch.rpm"/>
        <driver_bin value="kmod-veeamsnap-6.0.0.XXXX-1.el8.x86_64.rpm"/>
        <veeam value="veeam-6.0.0.XXXX-1.el8.x86_64.rpm"/>
     </Packages>
  </Version>
</Distribution>
....
```

c. Save changes and close the index file.

4. Rescan the protection group:

   a. Open the **Inventory** view.

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

   e. In the inventory pane, select the necessary protection group and click **Rescan** on the ribbon or right-click the protection group and select **Rescan**.

During the rescan, Veeam Backup & Replication will use updated packages specified in the index file to install Veeam Agent for Linux version with the hotfix on protected computers.

Appendix B. Restoring Files from Backup without Administrator Privileges

If you have Veeam Agent for Microsoft Windows installed on your computer and you work on this computer under an account that does not have Administrator privileges, you can still restore files from the file-level backup.

This scenario describes how to restore a file from the backup under an account that does not have local administrator permissions to its original location.

Before restoring, check the following prerequisites:

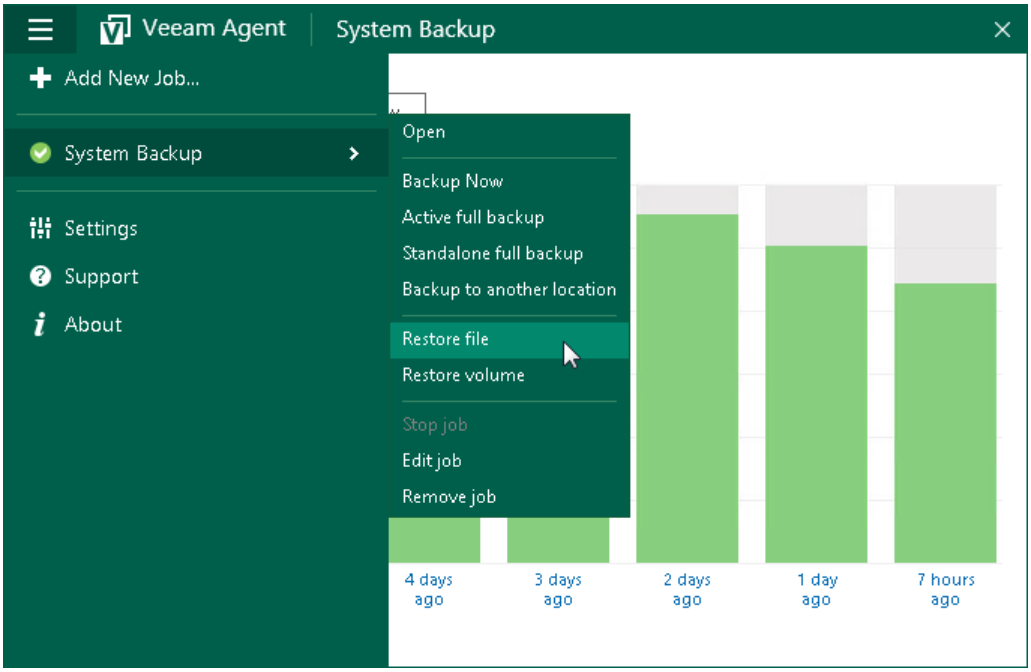
- Your Veeam Agent computer must be a member of a protection group for which file-level restore without Administrator privileges is allowed. To learn more, see Veeam Agent for Microsoft Windows Settings.
- You must restore from the backup created by a backup job managed by Veeam Agent. To learn more, see Selecting Job Mode.
- You must restore from the backup stored on Veeam backup repository or Veeam Cloud Connect repository.
- You must restore from the backup of the same Veeam Agent computer.
- You must open the restore wizard from the Veeam Agent for Microsoft Windows control panel.

To restore files, perform the following operations.

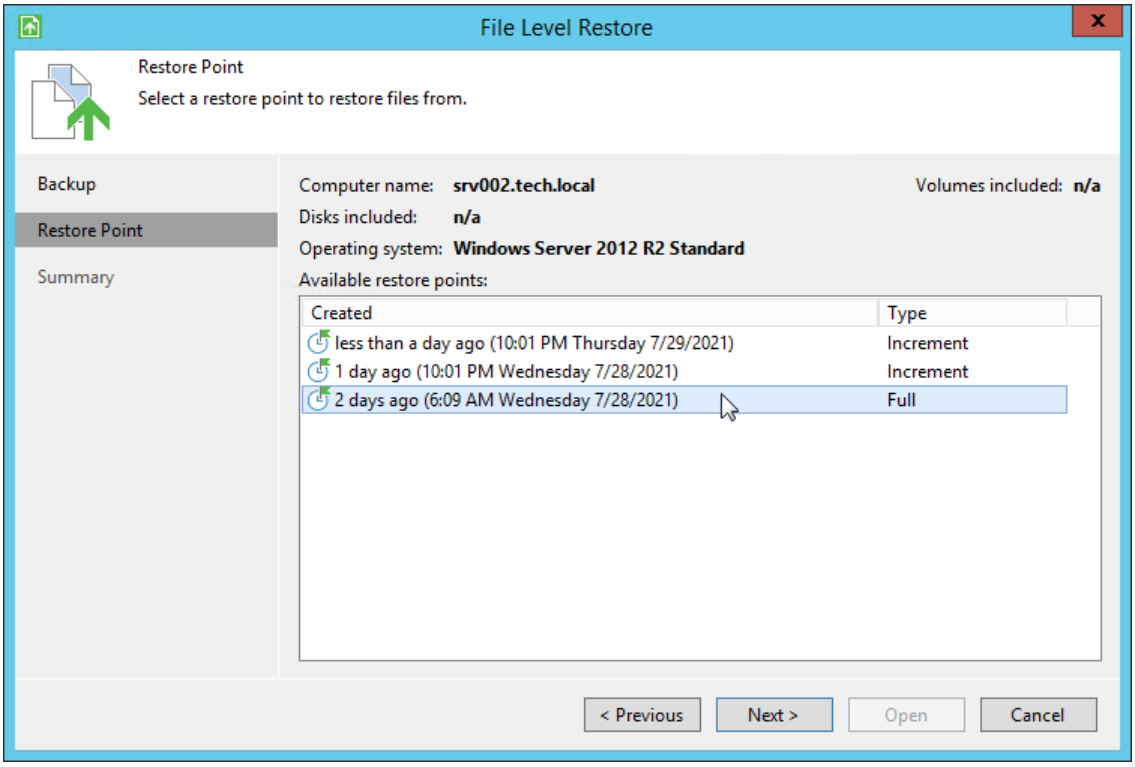
1. On the Veeam Agent computer, double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the icon in the system tray and select **Control Panel**.

2. From the main menu in the upper left corner, hover over the name of the necessary job and select **Restore file** to open the **File Level Restore** wizard.

   Mind that when you work on the Veeam Agent computer under an account that does not have Administrator privileges, you can open the **File Level Restore** wizard only from the Veeam Agent for Microsoft Windows control panel. If you try to open the wizard from the system tray, Veeam Agent will ask you to enter Administrator credentials.



3. In the **File Level Restore** wizard, select a restore point from which you want to restore the file.

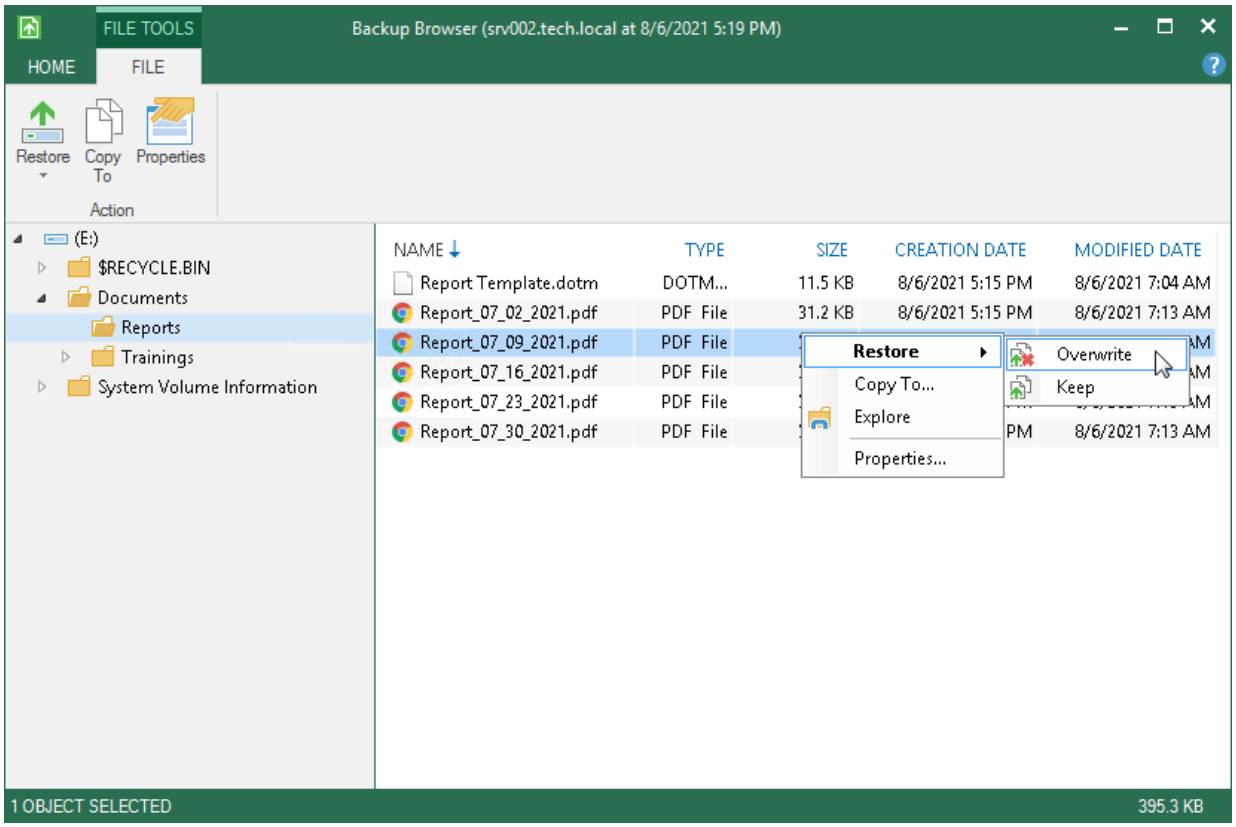


4. At the **Summary** step, click **Open**. Veeam Agent will display the backup file content in the Veeam Backup browser.

5. Locate the file you want to restore, right-click it and select **Restore** > **Overwrite**. The file will be restored to its original location.

   Mind that access rights to files and folders are managed by Veeam Agent computer OS. When you cannot access the folder in the original location, you cannot view the content of this folder in the Veeam Backup browser as well. If you select file to restore, but do not have enough access rights to restore it, Veeam Agent will not restore the file and will display an error message in the restore job session.

   To get the access rights you need, you can switch to another system user with the Veeam Backup browser. To learn more, see the Elevating Access Rights section in the Veeam Agent for Microsoft Windows User Guide.



Appendix C. Updating Pre-Installed Veeam Agents

This scenario describes how to update Veeam Agents on the computers added to protection groups for pre-installed Veeam Agents.

> **TIP**
>
> During each rescan job and synchronization session, Veeam Backup & Replication checks the version of Veeam Agents installed on the protected computers. If the Veeam Agent version does not coincide with the version of Veeam Backup & Replication, Veeam Agent computer will be moved to the *Out of Date* protection group.

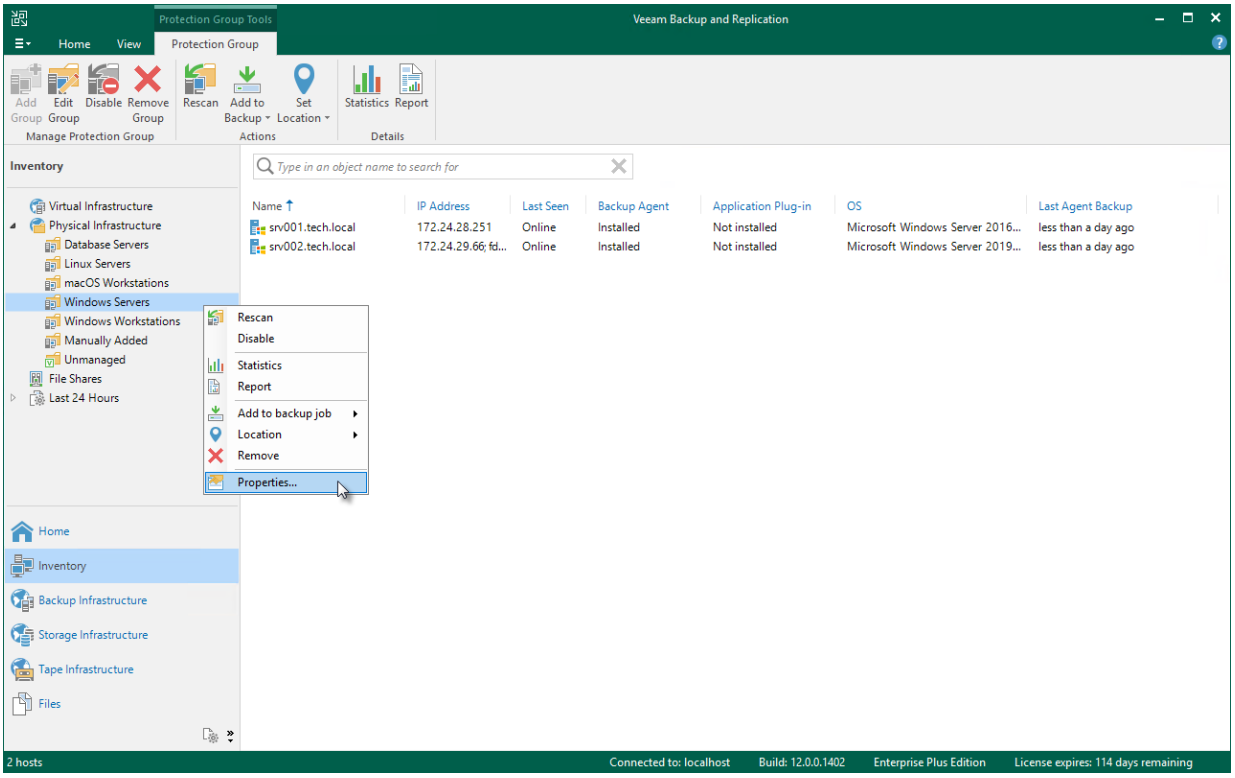
Before you update pre-installed Veeam Agents:

- Check that the latest update for Veeam Backup & Replication is installed on your backup server. For details, see Upgrading to Veeam Backup & Replication 12 section in the Veeam Backup & Replication Guide.
- Make sure that Veeam Backup & Replication remote components, such as the distribution server, are updated.
- Make sure that a user account that you plan to use for installation on the Veeam Agent computer side has Local Administator privileges.

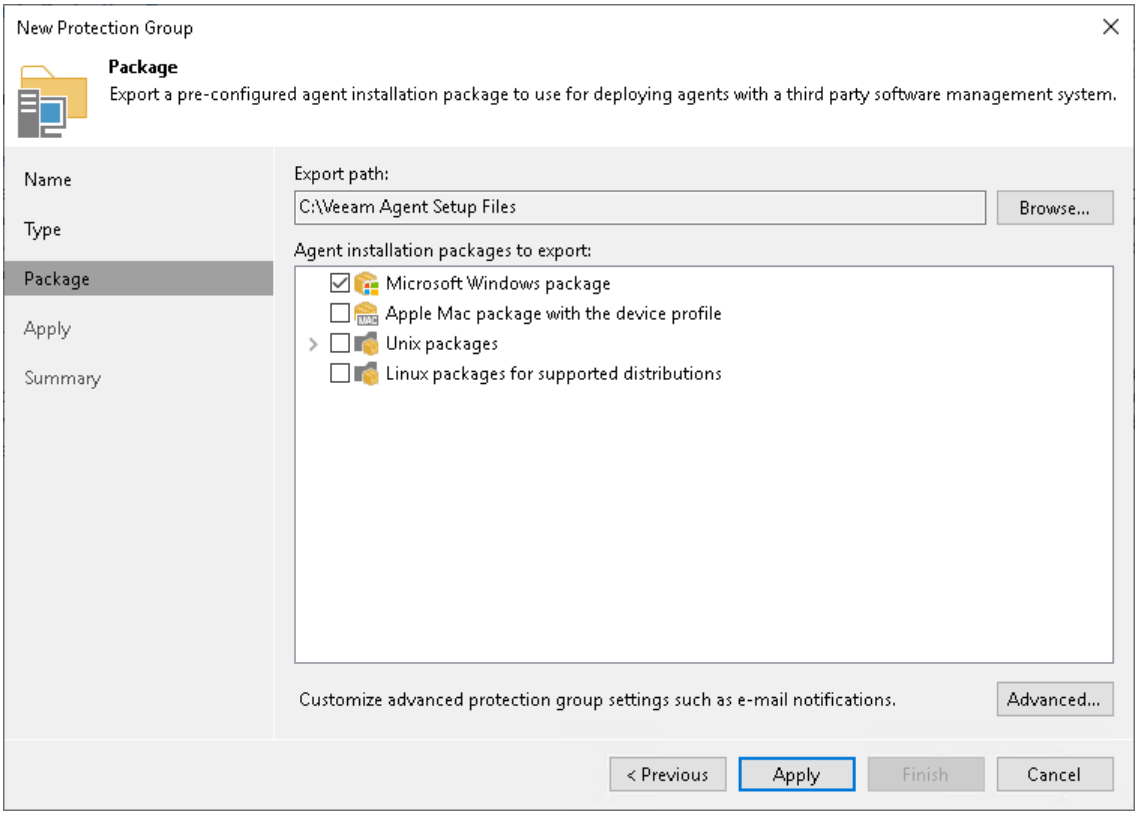
To update pre-installed Veeam Agents, you must generate new Veeam Agent setup files on the Veeam Backup & Replication side, To do so, edit protection group settings:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.

3. In the inventory pane, select the protection group for pre-installed Veeam Agents that you want to update and click **Edit Group** on the ribbon or right-click the protection group for pre-installed Veeam Agents that you want to update and select **Properties**.



4. At the **Package** step, check that the export path and setup files for OSes that runs on computers with Veeam Agents you want to update are specified correctly.



5. Click **Apply** to generate setup files. Then click **Finish** to close the wizard.

On the Veeam Agent computer side, the update procedure differs depending on the OS running on the protected computers:

- Update procedure for Microsoft Windows computers
- Update procedure for Linux computers
- Update procedure for Mac computers

Update Procedure for Windows Computers

To update pre-installed Veeam Agent on the Microsoft Windows computer, perform the following operations:

1. Upload Veeam Agent setup files on the computer you want to protect.
2. Update the Veeam Installer Service. To do this:
   a. Uninstall obsolete version of the Veeam Installer Service. To do this, navigate to Control Panel > Programs > Programs and Features, find the Veeam Installer Service in the list of programs and uninstall it.
   b. Install the updated version of the Veeam Installer Service. Double-click the `VeeamInstallerSvc` file located in the `<path_to_setup_files>/Windows/6.0.0.960/VAW` folder.
3. Install updated version of Veeam Agent. Use one of the following files depending on the architecture of your computer OS:

For 32-bit Windows

- Double-click the `Veeam_B&R_Endpoint_x86.msi` file located in the `<path_to_setup_files>/Windows/6.0.0.960/VAW` folder

For 64-bit Windows

- Double-click the `Veeam_B&R_Endpoint_x64.msi` file located in the `<path_to_setup_files>/Windows/6.0.0.960/VAW` folder

4. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
"C:\Program Files\Veeam\Endpoint Backup\Veeam.Agent.Configurator.exe" -syncnow
```

Update Procedure for Linux Computers

To update pre-installed Veeam Agent on the Linux computer, perform the following operations:

1. Upload Veeam Agent setup files on the computer you want to protect.
2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the installation of the Veeam Agent for Linux in the offline mode. For details, see the Installing Veeam Agent for Linux in Offline Mode section in the Veeam Agent for Linux User Guide.

   Keep in mind that if you use the APT package manager and the installation command reports that some dependencies for package not installed, run the following command instead:

   ```
   apt-get install -f
   ```

   After that, repeat the Veeam Agent installation procedure.
3. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
veeamconfig mode syncnow
```

Update Procedure for Mac Computers

To update pre-installed Veeam Agent on the Linux computer, perform the following operations:

1. Upload Veeam Agent setup files on the computer you want to protect.
2. Navigate to the directory where you have saved setup files and install Veeam Agent. This procedure is similar to the default installation of the Veeam Agent for Mac. For details, see the Installing Veeam Agent section in the Veeam Agent for Mac User Guide.
3. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
veeamconfig mode syncnow
```

Appendix D. Using Filters in Backup Jobs for Windows Computers

When you create or edit a Veeam Agent backup job for a Microsoft Windows computer in the Veeam Backup & Replication console, you can include and exclude files and folders from the backup job scope by using include and exclude masks as described in Specifying Folders to Back Up. This topic demonstrates several basic scenarios you may want to implement in your infrastructure.

Before You Begin

Before you configure filters, consider the following:

- This topic covers the file filtering functionality available for a backup job created by Veeam Agent operating in the managed mode.

  The settings of a backup job created by Veeam Agent operating in the managed mode provide additional file filtering capabilities compared to the settings available for a backup job created by Veeam Agent operating in the standalone mode. For example, when you create a backup job in the Veeam Backup & Replication console, you can specify paths and system environment variables in exclude masks. To learn more about setting up file filters for backup jobs when Veeam Agent operates in the standalone mode, see How to Use Filters to Define File-Level Backup Scope in the Veeam Agent for Windows User Guide.

- All backup scenarios in this topic are performed in the file-level backup mode.

  A file-level backup job may contain entire volumes and individual folders or files from the other volumes (this is referred to as *hybrid backup job*). In this case, entire volumes are processed using volume-level backup mode while specific folders from other volumes are processed using file-level backup mode. In the hybrid backup job, filters work in the following way:

  - File name and file type masks are applied only to the folders specified in the backup scope and not the entire volumes.
  - Masks that contain paths are applied to the selected folders and entire volumes.

- Depending on the type of the object in the backup scope, during job execution Veeam Agent behaves differently:

  - When you select an entire volume as an object of a file-level backup, Veeam Agent adds backup exclusions to the FilesNotToSnapshot registry key, triggers creation of the volume shadow copy (VSS snapshot), reads data from the VSS snapshot and saves the data to a backup repository. During backup, Veeam Agent will ignore any filters configured for this volume.

    > **NOTE**
    >
    > By default, Microsoft Windows does not include some files into the VSS snapshot — for example, temporary files, Microsoft Outlook .ost files and so on. As a result, these files are not included into Veeam Agent backups too. To learn how you can override this default behavior, see this Veeam KB article.

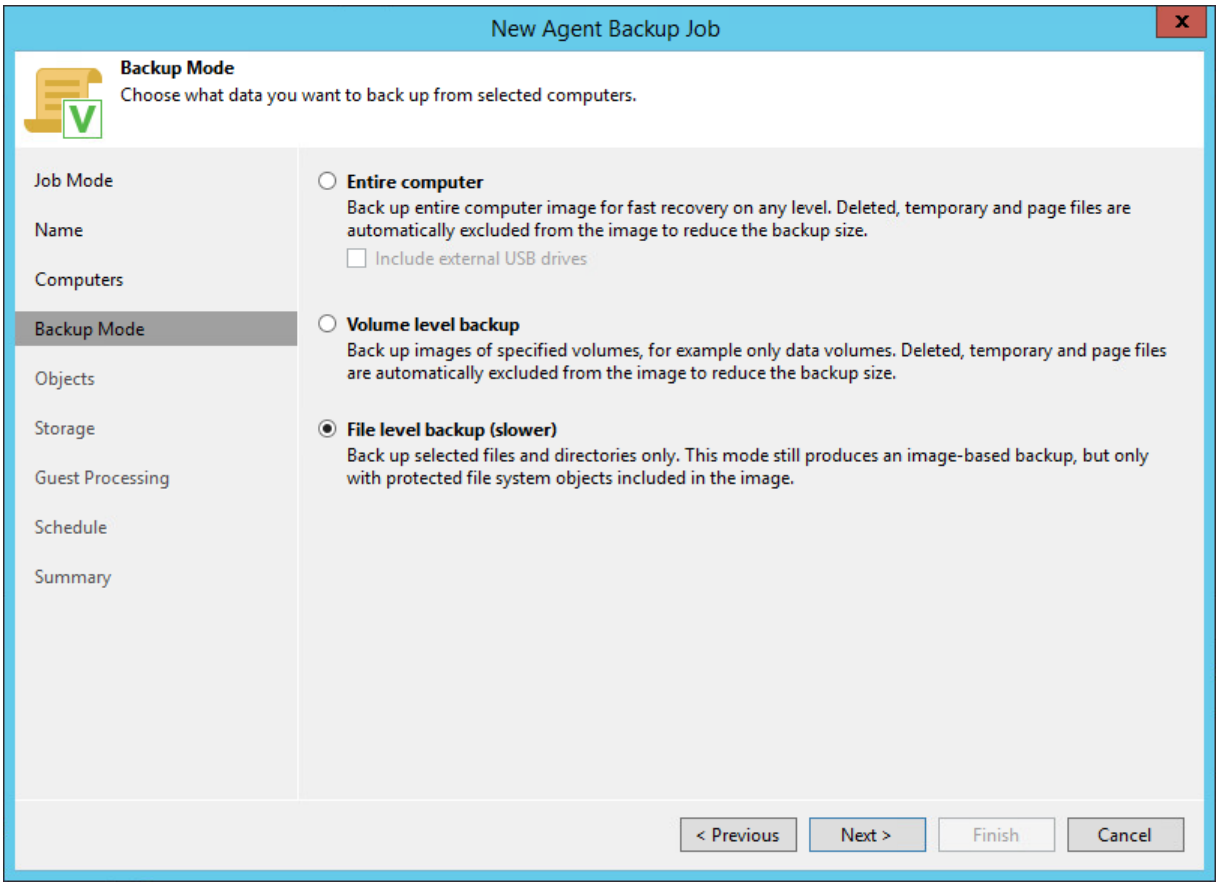
  - When you select an individual folder as an object of a file-level backup, Veeam Agent reads all data from the VSS snapshot first, then applies filters defined in the job configuration to save the data.

- When you specify include masks, the backup will contain only the data that matches these masking criteria within the backup scope. When you specify exclude masks, the backup will contain all data from the backup scope except the data that matches these masking criteria.

Setting Up File Filters for Backup Scope

To specify file filters when you create a new backup job, do the following:

1. At the **Backup Mode** step of the Backup Job wizard, select the **File level backup** option.



2. At the **Objects** step, select the directories to back up.

   You can apply filters only to the folders included in the backup scope.

3. Click **Advanced**; then in the **File Filters** window, use masks to include or exclude specific files and folders.

> **NOTE**
>
> You cannot apply filters to **Operating system** folders.

Common Filter Configurations

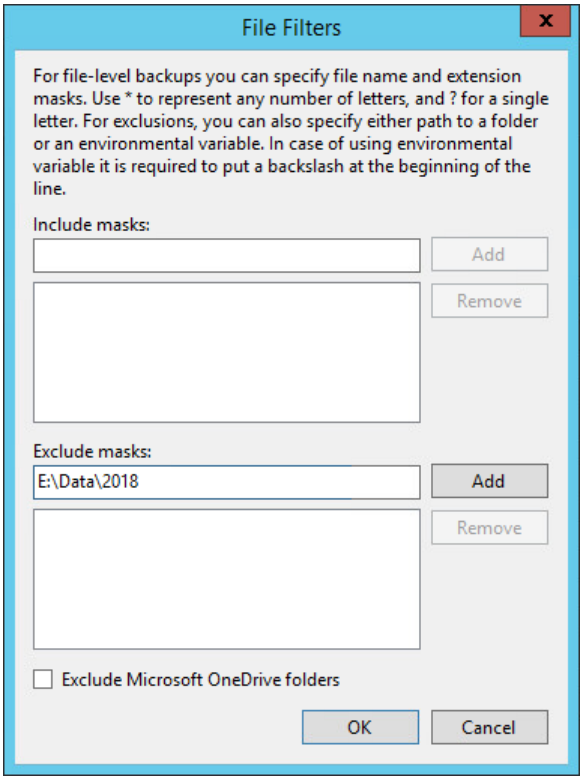
To learn how to use filters for a more granular definition of a backup scope, see the following scenarios:

- Excluding a Folder Using Full Path.
- Excluding a Folder Using an Environment Variable in the Path.
- Excluding a Folder Using a Wildcard Character in the Path.
- Including or Excluding Specific Files.
- Including or Excluding Files by File Type.
- Including or Excluding Files Whose Names Contain a Specific Sequence of Characters.
- Including or Excluding Files Named According to a Convention.

Excluding a Folder Using Full Path

You can exclude a folder from the backup by specifying a full path to it. In this example, we will exclude the `E:\Data\2018` folder from the backup scope.

1. In the **Exclude masks** field, enter the full path to the folder — *E:|Data|2018*.



2. Click **Add**.
3. Click **OK** to complete the configuration.

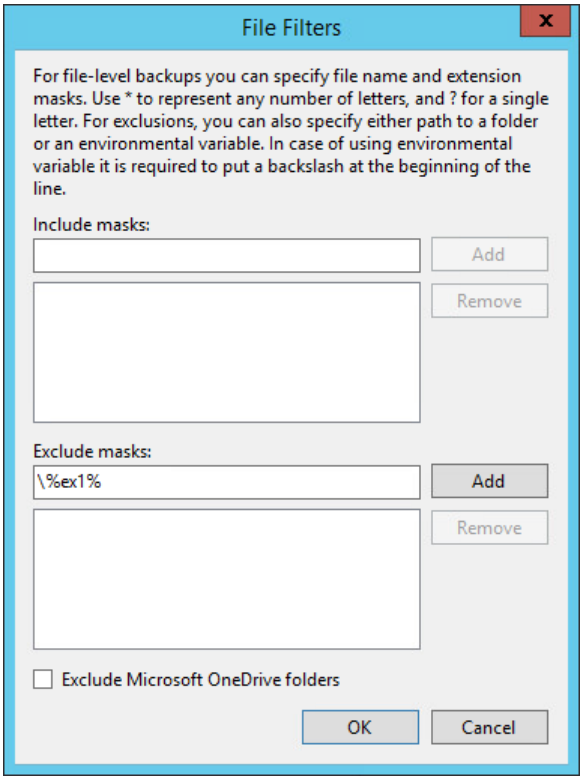
As a result, the backup will contain all data from the backup scope except the `E:\Data\2018` folder.

Excluding a Folder Using an Environment Variable in the Path

You can exclude a folder by specifying a system environment variable in its path. In this example, we will exclude the `E:\Data\2021\Drafts` folder that is defined as the `ex1` variable. To do this:

1. In the **Exclude masks** field, enter *|%ex1%*.

   > **IMPORTANT**
   >
   > When you specify a system environment variable in a mask, you must precede such variable with a backslash.

2. Click **Add.**
3. Click **OK** to complete the configuration.

As a result, the backup will contain all data from the backup scope except the `E:\Data\2021\Drafts` folder.

> **NOTE**
>
> If you use a system environment variable in the file filter for the backup, consider the following:
>
> - You can use only system environment variables defined for the Local System account on computers added to the backup job. You cannot use user environment variables (Veeam Agent works under the NT AUTHORITY\SYSTEM account, so all exclusions are treated accordingly).
> - You cannot use environment variables that contain multiple values or other environment variables.

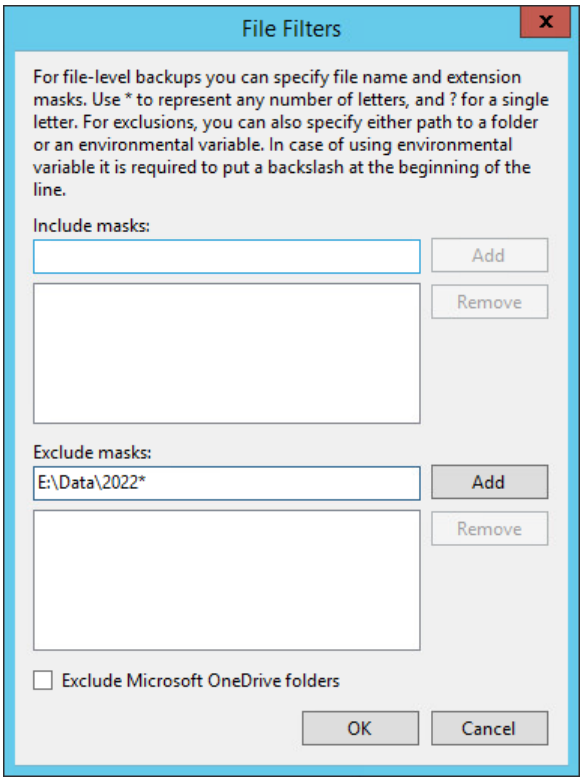
Excluding a Folder Using a Wildcard Character in the Path

To exclude a folder from the backup, you can specify a partial path with a wildcard at the end.

> **NOTE**
>
> Note that you cannot use a wildcard in the middle of the path. For example, specifying *E:|*|2020* will cause an error during backup. To recursively exclude files from specific subfolders of the selected root folder, you can use the standard OS mechanism for exclusions. To learn more, see this Veeam KB article.

In this example, we will exclude all subfolders of the `E:\Data` folder whose names begin with `2022`. To do this:

1. In the **Exclude masks** field, enter *E:|Data|2022**.



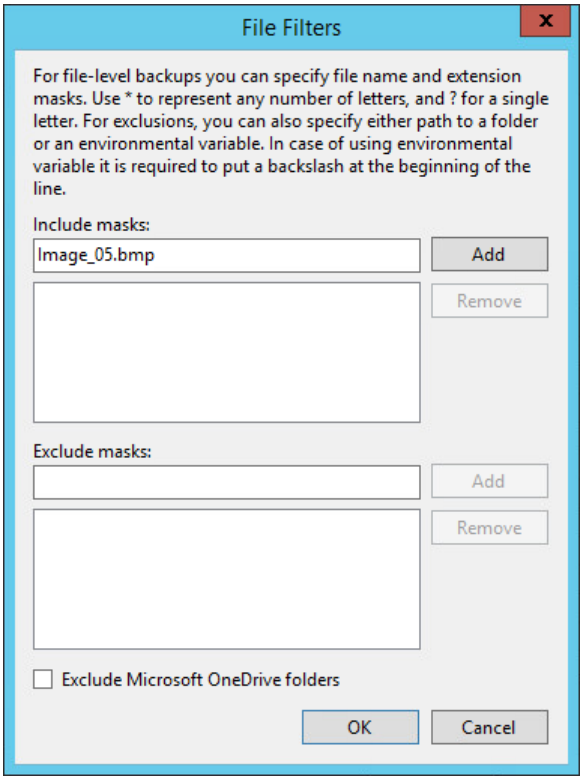
2. Click **Add**.
3. Click **OK** to complete the configuration.

As a result, the backup will contain all data from the backup scope except the folders whose names start with `2022` — for example `2022_Jan` or `2022_Reports`.

Including or Excluding Specific Files

You can select specific files for inclusion or exclusion. In this example, we will include only the `Image_05.bmp` file into the backup. To do this:

1. In the **Include masks** field, enter *Image_05.bmp*:



2. Click **Add**.
3. Click **OK** to complete the configuration.

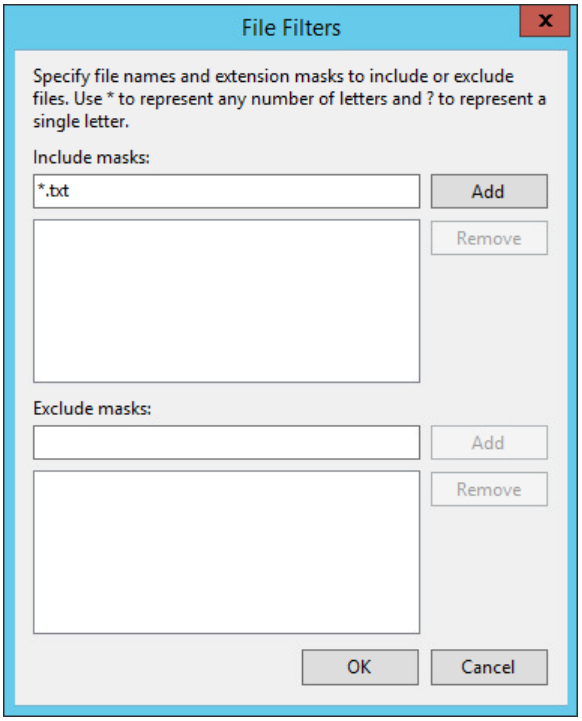
As a result, the backup will contain only the `Image_05.bmp` file from the specified backup scope.

Including or Excluding Files by File Type

You can include or exclude files by their type using a wildcard character instead of the file name — for example, `*.docx` will select all Microsoft Word files with such extension in the backup scope.

In this example, we will back up all text files in the .txt format. To do this:

1. In the **Include masks** field, enter **.txt* to select all files with the .txt extension.



2. Click **Add**.
3. Click **OK** to complete the configuration.

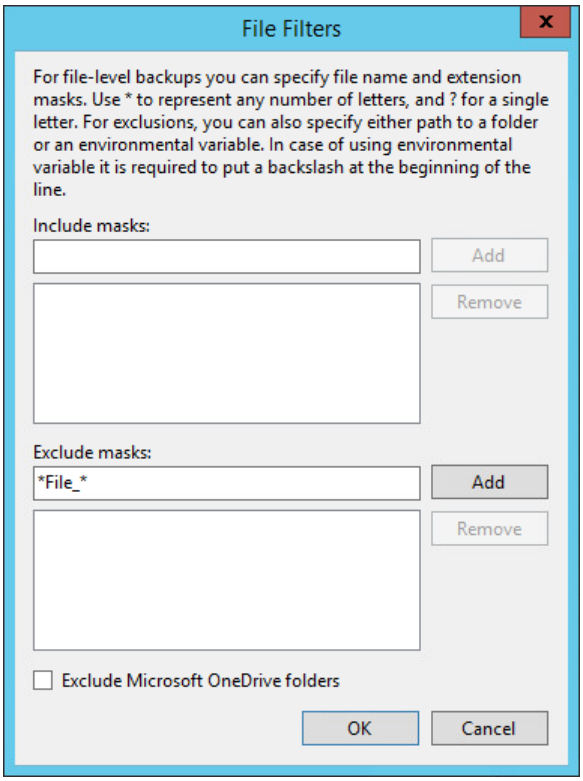
As a result, the backup will contain all the text files in the .txt format from the backup scope except the files that contain `draft` in the name.

> **NOTE**
>
> You can combine include and exclude masks as needed. For example, you can include all .pdf files into the backup scope and exclude the ones that contain the word `draft` in their name by specifying **.pdf* in the include mask and **draft** in the exclude mask.

Including or Excluding Files Whose Names Contain a Specific Sequence of Characters

You can include or exclude files whose names contain a specific sequence of characters. In this example, we will exclude files of any type that have `File_` in the name. To do this:

4. In the **Exclude masks** field, enter **File_**.



   This will select all files that contain this sequence of characters in any position in the file name.

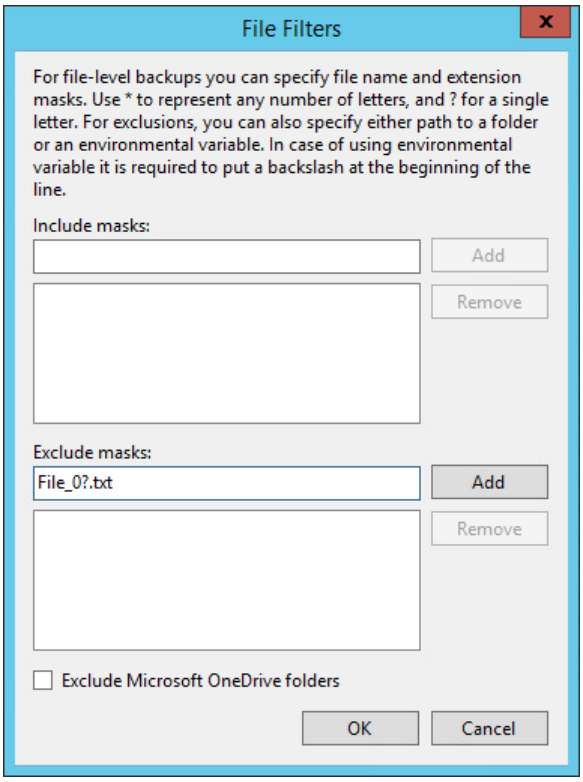
5. Click **Add**.
6. Click **OK** to complete the configuration.

As a result, the backup will contain all data from the backup scope except the files that contain `File_` in the name — for example, `File_01.txt` or `Draft_File_05.pdf`.

Including or Excluding Files Named According to a Convention

You may have a set of files named according to a convention — for example, `File_XX.txt` where `XX` is a two-digit number. You can use a single-character wildcard to select specific files for inclusion or exclusion. In this example, we will exclude files named according to the `File_XX.txt` convention with numbers ranging from `01` to `09`:

1. In the **Exclude masks** field, enter *File_0?.txt*.



2. Click **Add**.
3. Click **OK** to complete the configuration.

As a result, the backup will contain all data from the backup scope except the text files whose names contain a digit ranging from 1 to 9 in the position of the wildcard character specified in the mask — for example, `File_01.txt`, `File_07.txt` and so on. Keep in mind that this filter will also exclude files whose names contain any other character in the wildcard position — for example, `File_0A.txt`.