Veeam Backup & Replication

Version 12

Veeam Agent Management Guide

January, 2025

> 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 12.3 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.

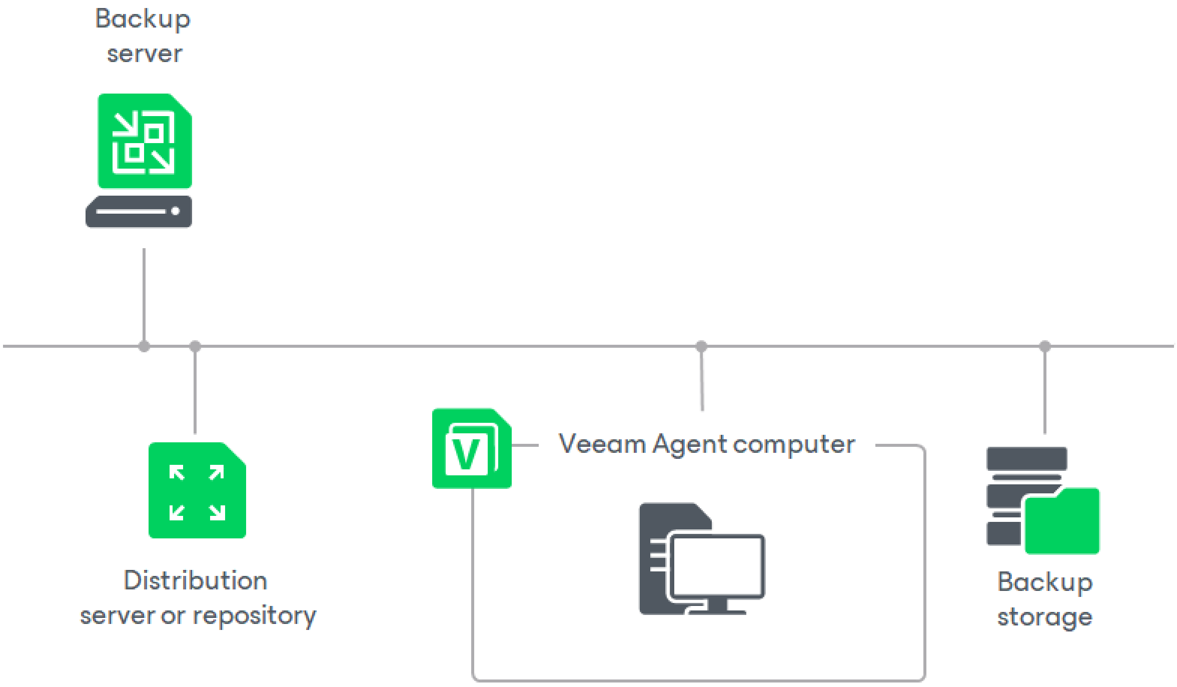
Veeam Backup & Replication offers the following Veeam Agent management capabilities:

- **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 and Unix machines that you want to protect with Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX. 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 manage Veeam Agents 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 Agents deployed on remote computers and cloud machines by Veeam Backup & Replication automatically
- Veeam Agents deployed on remote computers by user manually

Veeam Agents Deployed on Remote Computers and Cloud Machines by Veeam Backup & Replication Automatically

Veeam Backup & Replication can automatically discover computers added to the inventory and deploy Veeam Agents on these computers. Veeam Agent for Mac can be deployed manually only. To learn more about automatic deployment of Veeam Agents, see Protected Computers Discovery and Veeam Agent Deployment.

- On Microsoft Windows computers, Veeam Backup & Replication deploys Veeam Installer Service. Veeam Installer Service, in turn, deploys Veeam Transport Service that performs the necessary operations on the computer.
- On Linux computers, Veeam Backup & Replication connects to the Linux computer using SSH credentials and installs Veeam Deployer Service. After that, Veeam Deployer Service installs Veeam Transport Service that performs necessary operations on the computer.

  > NOTE
  >
  > You can manually pre-install Veeam Deployer Service on a Linux computer. In this case, Veeam Backup & Replication will make the initial connection to the Linux computer using a single-use certificate. For more information on this deployment option, see Deploying Veeam Agent for Linux Using Pre-Installed Veeam Deployer Service.

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

  - To communicate with the Linux computer for the first time if you use credentials to connect to the Linux computer. To learn more, see Specifying Computers.

    After Veeam Backup & Replication computer is discovered and Veeam Agent is deployed, Veeam Backup & Replication uses Veeam Deployer and Transport Services to connect to the Veeam Agent computer instead of the SSH connection.
  - To communicate with the Linux computer after Veeam Deployer and Transport Services 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 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 Unix computers, Veeam Backup & Replication connects to the Unix computer using SSH credentials and deploys Veeam Installer Service. After that, Veeam Installer Service installs Veeam Agent packages on the machine. The same rules for failover to SSH on Linux computers apply to Unix computers.

- 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 machine.

Veeam Agents Deployed on Remote Computers by User Manually

You must manually deploy Veeam Agent for Mac on the computer you want to protect and set connection to Veeam Backup & Replication. You can also manually deploy Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX. After you deploy Veeam Agent, you can use Veeam Backup & Replication to perform necessary operations on the computers. To learn more about manual deployment of Veeam Agents, 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 Step 4. 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 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 the Veeam Plug-ins for Enterprise Applications Guide.

Keep in mind that Veeam Backup & Replication does not support automated deployment of Veeam Agent for Mac and nosnap Veeam Agent for Linux (including Veeam Agent for Linux on Power). You must deploy Veeam Agent for Mac on protected computers using setup files generated by Veeam Backup & Replication. To learn more, see Deploying Veeam Agents Using Generated Setup Files.

TIP

If you have several Microsoft Windows and Linux computers and Unix machines 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 Deploying Hotfix on Protected Computers.

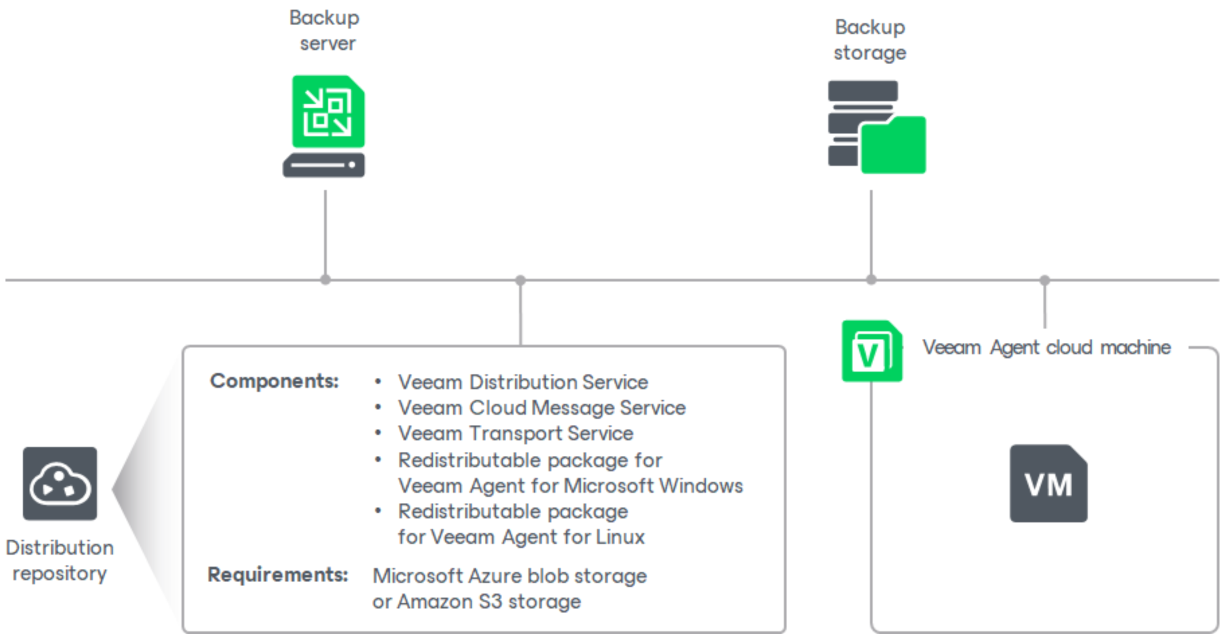
Distribution Repository

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 using signed URLs. To learn how Veeam Backup & Replication communicates with Veeam Agents installed on cloud machines, see Backup of Cloud Machines.

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 the Adding Azure Blob Storage or Adding Amazon S3 Storage sections in the Veeam Backup & Replication User Guide.

Consider the following:

- 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.
- [For Azure Blob Storage] 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.
- [For Azure Blob Storage] You cannot add a repository using the Microsoft Entra ID account.
- [For Amazon S3 Storage] If you plan to use the Amazon S3 repository in the China region as a distribution repository, make sure that you have the ICP license. This license is required to create signed URLs for Amazon S3 repositories in the China region. For more information, see AWS Documentation.


Backup server
Backup storage
Veeam Agent cloud machine
VM
Distribution repository
Components:
• Veeam Distribution Service
• Veeam Cloud Message Service
• Veeam Transport Service
• Redistributable package for Veeam Agent for Microsoft Windows
• Redistributable package for Veeam Agent for Linux
Requirements: Microsoft Azure blob storage or Amazon S3 storage

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, Veeam Agent for Linux, Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX 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
>
> Consider 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 a connection method specified in the protection group settings. If you use credentials to connect to discovered computers, 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. Veeam Backup & Replication connects to discovered computers with credentials or a single-use certificate.

- **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 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 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 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 or TXT file. Protection groups that include computers listed in a CSV file are also dynamic. If a new computer appears in the 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 backup 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.

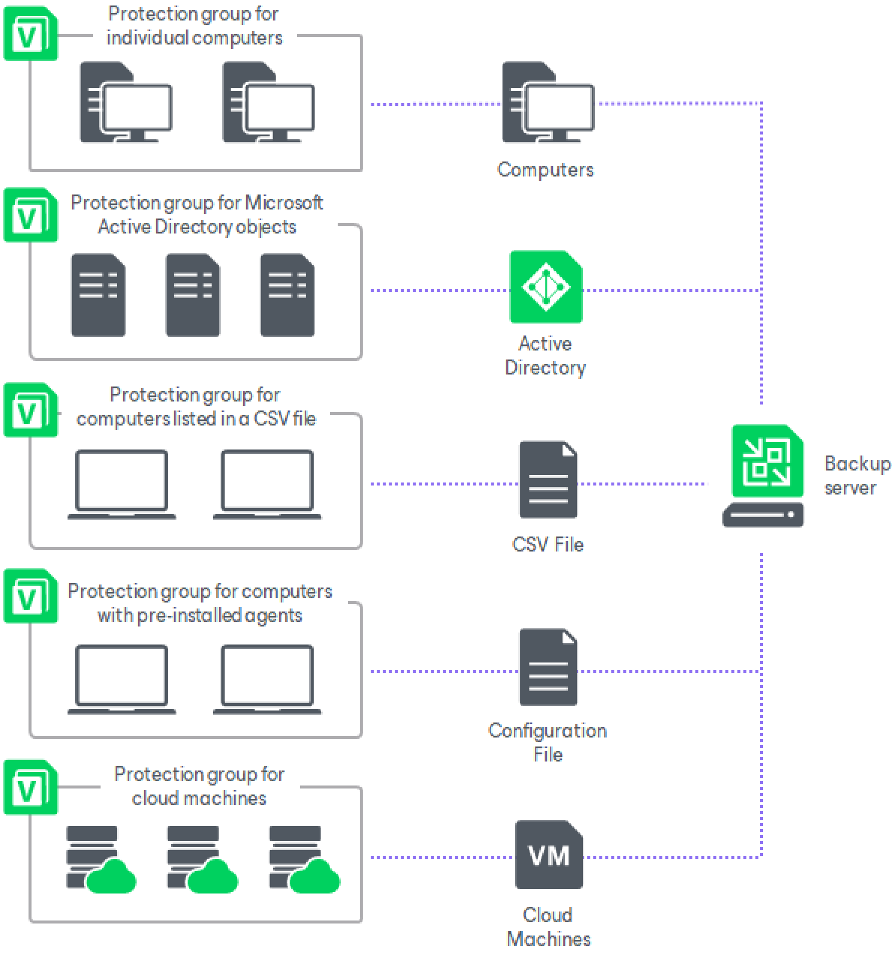
- **Cloud machines**

  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.

IMPORTANT

The current guide does not cover subjects related to protection groups that include applications. To learn about this protection group type, see the Protection Group Types section in the Veeam Plug-ins for Enterprise Applications Guide.


Protection group for individual computers
Protection group for Microsoft Active Directory objects
Protection group for computers listed in a CSV file
Protection group for computers with pre-installed agents
Protection group for cloud machines
Computers
Active Directory
CSV File
Configuration File
VM
Cloud Machines
Backup server

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 Working with Veeam Agent Backup Jobs and Policies.

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 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.

Considerations and Limitations

Consider the following about rescan of protection group and computer discovery:

- Automatic installation of nonsnap Veeam Agent for Linux during rescan is not available. If you want to add a computer with nonsnap Veeam Agent for Linux to a protection group, you must deploy Veeam Agent on the protected computer first. For more information on standalone installation of nonsnap Veeam Agent for Linux, see the Installation and Configuration section of the Veeam Agent for Linux User Guide.
- Automatic upgrade of nosnap Veeam Agent for Linux during rescan is not available. You must upgrade such Veeam Agents on the protected computer side, manually or using third-party tools.
- Rescan is available for all protection groups except protection groups for pre-installed Veeam Agents and their individual members. Veeam Agents installed on computers included in protection groups for pre-installed Veeam Agents synchronize with Veeam Backup & Replication every 6 hours and provide information about the Veeam Agent computer. If necessary, you can synchronize Veeam Agent with Veeam Backup & Replication running a command from the Veeam Agent computer. To learn more, see Backup Policy Application Methods.

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, a method for connecting to these computers, and so on.
2. Connects to each computer in the list using a connection method specified in the protection group settings.
3. Deploys Veeam components on each newly discovered computer: On Windows-based computers, Veeam Backup & Replication deploys Veeam Installer Service. After that, Veeam Installer Service deploys Veeam Transport Service.
   - On Windows-based computers, Veeam Backup & Replication deploys Veeam Installer Service. After that, Veeam Installer Service deploys Veeam Transport Service.
   - On Linux-based computers, Veeam Backup & Replication deploys Veeam Deployer Service. After that, Veeam Deployer Service deploys Veeam Transport Service.

> NOTE
>
> You can manually pre-install Veeam Deployer Service on a Linux computer. In this case, Veeam Backup & Replication will make the initial connection to the Linux computer using a single-use certificate. For more information on this deployment option, see Deploying Veeam Agent for Linux Using Pre-Installed Veeam Deployer Service.

- On Unix-based computers, Veeam Backup & Replication deploys Veeam Installer 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.

> NOTE
>
> On computers where Veeam Transport Service is already installed, Veeam Backup & Replication checks the Veeam Transport Service version. If a later version is available, Veeam Backup & Replication upgrades Veeam Transport 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).

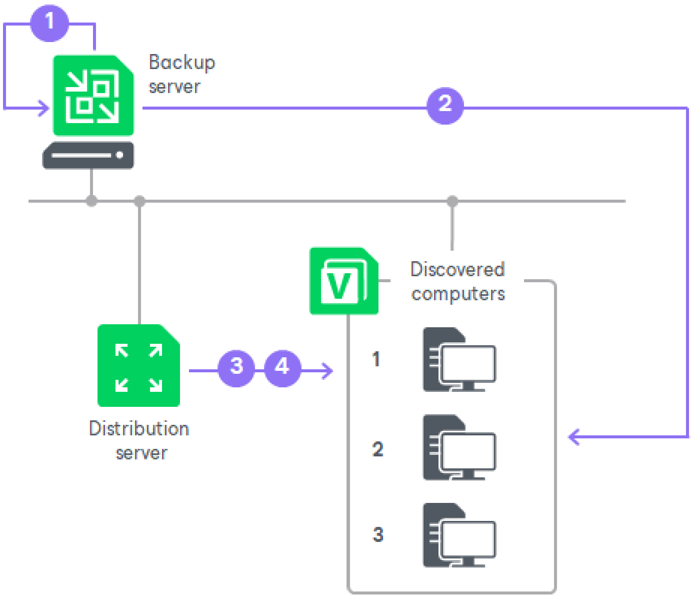
   b. Veeam Backup & Replication uploads the Veeam Agent setup files:

      - On Windows-based, Linux-based computers and Unix-based machines, 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 Unix-based computers, Veeam Installer 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.



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.

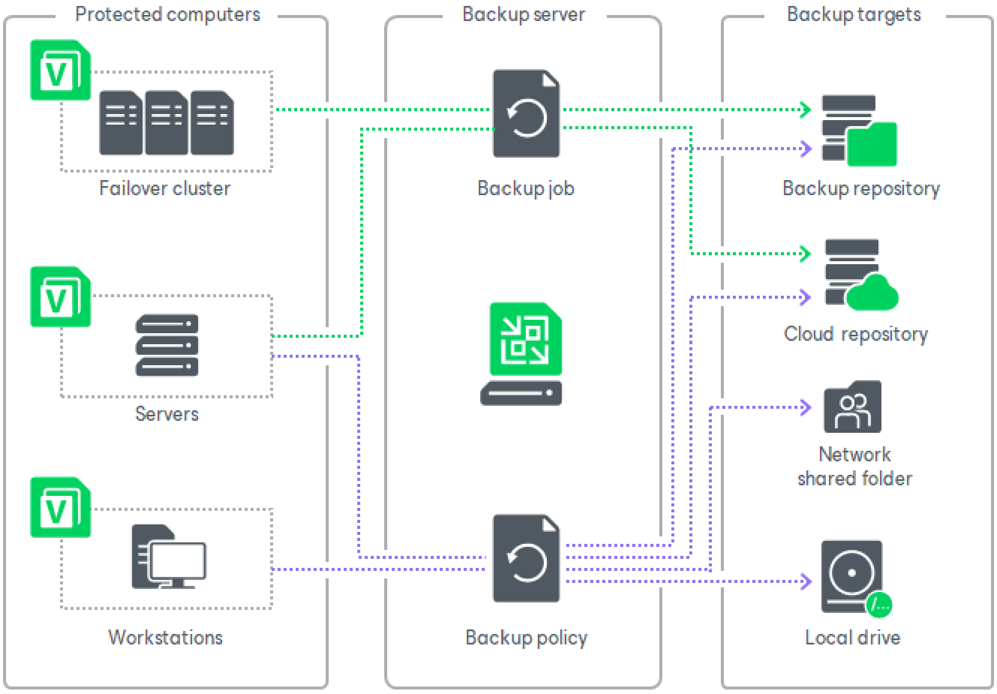
- **Backup policy**

  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
>
> - [For Microsoft Windows computers] 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.

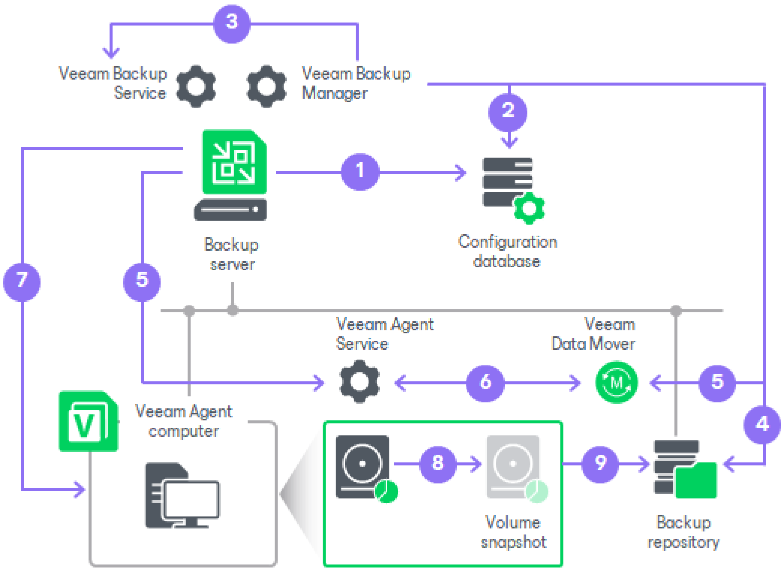
8. Veeam Backup & Replication requests Veeam Agent to trigger a VSS snapshot or volume snapshot, depending on the type of OS running on the Veeam Agent computer. For Windows-based computers, Veeam Agent for Microsoft Windows leverages Microsoft VSS technology to create a VSS snapshot. For Linux-based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



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, including file-level and volume-level restore, directly on a protected computer. In particular, 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
>
> Consider 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.

      - On Unix computers, Veeam Backup & Replication creates the Veeam Agent backup job using the Veeam Agent 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:

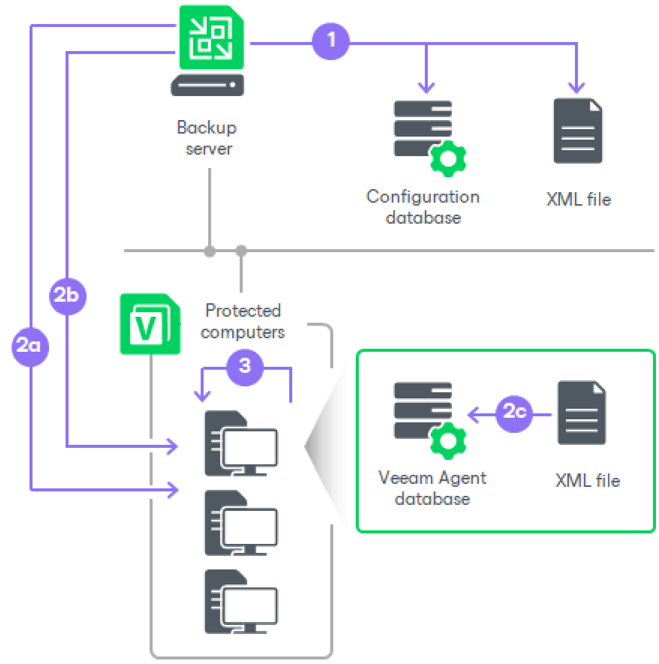
   - How Backup Works section in the Veeam Agent for Microsoft Windows User Guide.

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

   - How Backup Works section in the Veeam Agent for IBM AIX User Guide.

- How Backup Works section in the Veeam Agent for Oracle Solaris 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.



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.

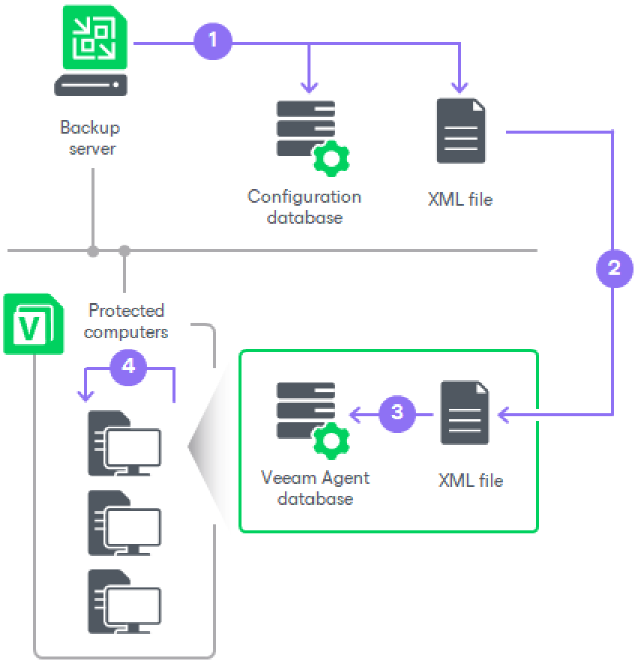
   > **IMPORTANT**
   >
   > Veeam Agent does not connect to Veeam Backup & Replication immediately after updated backup policy settings are saved. Veeam Agent checks whether Veeam Backup & Replication has any updates in the backup policy settings periodically. As a result, a time period between scenario steps 1 and 2 may take up to 6 hours. If necessary, you can synchronize Veeam Agent with Veeam Backup & Replication running a command from the Veeam Agent computer. To learn more, see Backup Policy Application Methods.

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.



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.

> NOTE
>
> 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.

  You can also synchronize Veeam Agent with Veeam Backup & Replication immediately running the following command from the Veeam Agent computer:

    - For Veeam Agent for Microsoft Windows computers:

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

    - For Veeam Agent for Linux, Veeam Agent for Oracle Solaris, Veeam Agent for IBM AIX and Veeam Agent for Mac computers:

      ```
      veeamconfig mode syncnow
      ```

  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 Chain

Backup chain is a sequence of backup files created by Veeam Agent backup jobs. The backup chain provides the ability to recover data.

The backup chain consists of the first full backup file, incremental backup files, metadata files and some additional files. Full and incremental backup files correspond to restore points of the backed-up Veeam Agent computers. Restore points let you roll back Veeam Agent computers to the necessary state.

To learn about types of backup files, see the Backup Files section in the Veeam Backup & Replication User Guide.

In This Section

Short-Term Retention Policy

Restore points in the backup chain are not kept forever. The short-term retention policy defines when a restore point is obsolete and must be removed from the backup chain so that backup files do not consume too much disk space.

Depending on the selected job mode, restore points are handled by Veeam Backup & Replication or Veeam Agent. To learn more, see Veeam Agent Backup Jobs and Policies.

To define the short-term retention policy for a backup job, you can select the following units:

- Days. In this case, Veeam Backup & Replication or Veeam Agent retains restore points in the following way:
  - [For Veeam Agent backup jobs managed by the backup server] Veeam Backup & Replication keeps backup files for the *<N>+1* days, where *<N>* is the number of days that you specified in the backup job settings.

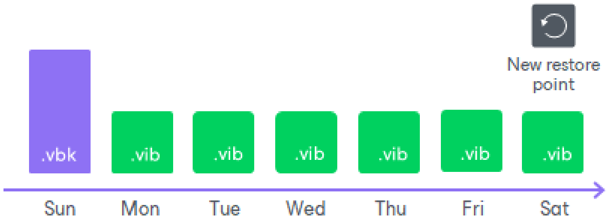
    > NOTE
    >
    > The minimum number of retained restore points is 3, and this number does not depend on the number of days set in the backup job settings. You can change the minimum number of retained restore points with a registry value. To learn more, contact Veeam Customer Support.

  - [For Veeam Agent backup jobs managed by Veeam Agent] Veeam Agent takes into account only days on which backup files were successfully created. Veeam Agent ignores restore points created on the day when the retention policy is applied and keeps restore points for the *<N> + 1* days, where *<N>* is the number of days that you specified in the backup job settings.
- Restore points. In this case, Veeam Backup & Replication or Veeam Agent retains the specified number of the latest restore points.

Removing Backups by Retention

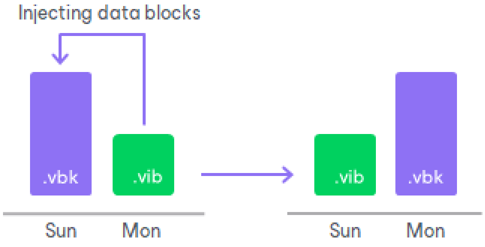
When the obsolete restore points are removed by retention, Veeam Backup & Replication or Veeam Agent transforms the backup chain so it always contains a full backup file on which subsequent incremental backup files are dependent. To do so, Veeam Backup & Replication or Veeam Agent uses the following rotation scheme:

1. During every backup job session Veeam Backup & Replication or Veeam Agent adds a backup file to the backup chain and checks if there is an obsolete restore point.

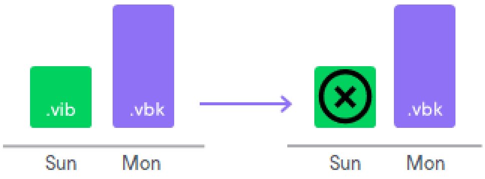


2. If an obsolete restore point exists, Veeam Backup & Replication or Veeam Agent transforms the backup chain. As part of this process, it performs the following operations:

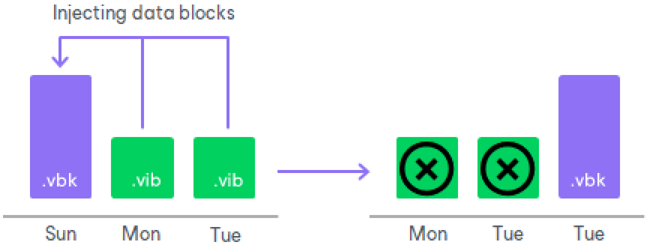
   a. Rebuilds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do this, Veeam Backup & Replication or Veeam Agent injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup 'moves' forward in the backup chain.



   b. Removes the earliest incremental backup file from the chain as redundant: its data has already been injected into the full backup file, and the full backup file includes data of this incremental backup file.



If the backup chain contains several obsolete restore points, the rebuild procedure is similar. Data from several restore points is injected to the rebuilt full backup file. This way, Veeam Backup & Replication or Veeam Agent makes sure that the backup chain is not broken, and you will be able to recover your data to any restore point.



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.To learn more, 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.

Consider 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. To learn more, 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 Storage System Snapshot Integration 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. To learn more, 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. To learn more, 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. To learn more, see the Viewing License Information section in the Veeam Backup & Replication 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 ha ve 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:

- You cannot create file-level backup from a storage snapshot.
- 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 Microsoft documentation.
- 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. To learn more, see Storage Snapshots on Volumes Greater than 64 TB.
- BitLocker encrypted volumes are supported with limitations. To learn more, 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.

   The hardware VSS provider aborts the shadow copy creation if the whole process takes longer than 60 seconds or if the provider takes longer than 10 seconds to commit the shadow copy. To meet these time limits, Veeam Agent expects the storage system to create a snapshot within 9 seconds. In case of a standalone server, Veeam Agent can extend this period up to 59 seconds. In case of a failover cluster, Veeam Agent cannot extend the 9-second period. To learn more on how the hardware VSS provider creates shadow copies, see Microsoft documentation.

   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.

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 mounts the snapshot LUN to the backup proxy.

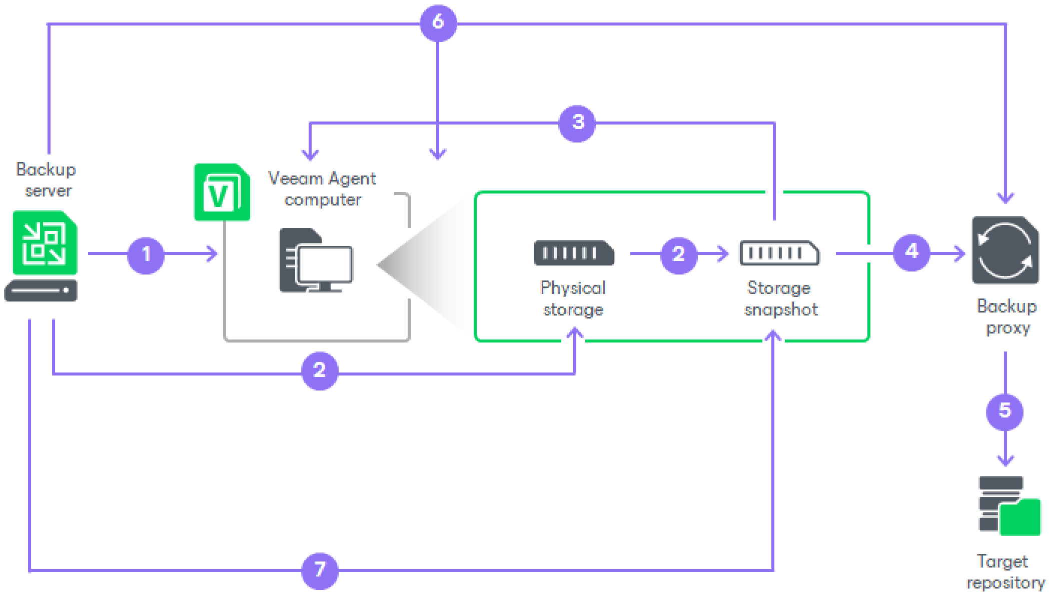
5. Veeam Backup & Replication reads the snapshot LUN and transfers data from the backup proxy to the target repository.

   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 backup operations on the Veeam Agent computer and the backup proxy.

7. Veeam Backup & Replication removes the snapshot LUN from storage.

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 section 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. To learn more, see Microsoft documentation.

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. To learn more, see Microsoft documentation.

   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 Always On Availability Groups are supported only for Microsoft SQL Server 2012 or later. To learn about Always On Availability Groups, see Backup of Always On Availability Groups.
  - Microsoft Exchange Server 2013 or later

    Microsoft Exchange Database Availability Groups (DAGs) are supported. To learn more, 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 Microsoft documentation.
- Backup of environments consisting of several failover clusters is not supported. For example:
  - Always On Availability Groups based on SQL Server Failover Cluster Instances (FCIs). To learn more, see Microsoft documentation.
  - Distributed Always On Groups. To learn more, see Microsoft documentation.
- Always On Availability Groups with no underlying failover cluster (Clusterless Availability Groups) are not supported.
- Backup of SQL Server failover clusters that store databases on a cluster disk is not supported if at least one of the cluster nodes hosts a local disk with the same mount point.
- SureBackup full recoverability testing mode is not supported for failover clusters.

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 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:

- 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 Backup Chain Formats section in the Veeam Backup & Replication User Guide.

- When you copy Veeam Agent backup jobs that process failover clusters with shared disks, the network traffic is higher compared to the traffic sent when Veeam Agent backup jobs run. This happens because Veeam Agent backup copy jobs send data as it is stored in the storage — each node with the cloned data — unlike Veeam Agent backup jobs that send data of shared disks only with the owner node and then, within the target storage, clone this data to other nodes.

- Data deduplication is not available when you copy Veeam Agent backup jobs that process failover clusters with shared disks to an object storage repository.

  > **IMPORTANT**
  >
  > In this case, you may require additional free space on the target location, because Veeam Backup & Replication creates in the target location as many copies of the cluster shared disks as there are nodes in the cluster.

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 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 Microsoft documentation.

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, that are included in a 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 Always On Availability Groups

To process Always On 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 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 Always On 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 Always On Availability Group.

   To learn more about VSS backup types, see Microsoft documentation.

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 Always On Availability Group. At each log processing interval, Veeam Backup & Replication chooses the Always On Availability Group node for which transaction logs will be backed up. Logs are backed up from one node of the Always On 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 section Failover Cluster Support.

- The necessary Veeam Backup & Replication components must be installed on this node and the computer included in Always On 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 Always On Availability Groups for this node were successfully backed up for the last two processing intervals.

Malware Detection

You can use built-in or third-party malware detection methods to scan data of backups created by Veeam Agent for Microsoft Windows and get information about suspicious activity or infected objects. To learn more about the feature, see the Malware Detection section in the Veeam Backup & Replication User Guide.

> NOTE
>
> Consider the following:
>
> - You cannot check data of backups created by Veeam Agent for Linux, Veeam Agent for Mac, Veeam Agent for IBM AIX or Veeam Agent for Oracle Solaris.
> - [For backups of failover clusters] You can exclude only the whole cluster from the malware detection scan, you cannot exclude a single cluster node.

To learn how to scan restore points of a specific backup, see Scanning Backup.

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)

Considerations and Limitations

- Scripts must be created before you configure the backup job. You must specify paths to them in the backup job settings.
- Veeam Agent supports scripts in the .SH file format only.
- Scripts must have UNIX line endings (LF).
- Script settings are enabled at the backup job level. If you want to configure multiple backup jobs, you can specify individual scripts for each job.
- If you use relative paths in your scripts, during script execution such paths will refer to the root directory. For example, the script may have an output that must be saved to a new file. If you specify a relative path to that file or only a file name, the file will be created in the root directory. To specify a different location for a file, use a full absolute path.

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. To learn more, 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. To learn more, 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. To learn more, 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 supported database systems using application-aware processing..

Supported Database Systems

- MySQL
- Oracle

  Veeam Agent processes the Oracle database system using an internal component: *oralib*.
- PostgreSQL

  Veeam Agent processes the PostgreSQL database system using an internal component: *pgsqlagent*.

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

Backup of Database Archived Logs

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, with the same requirements and limitations.

To learn more about backup of Oracle database archived logs, see the Oracle Log Backup section in the Veeam Backup & Replication User Guide.

To learn more about backup of PostgreSQL database archived logs, see the PostgreSQL Log Backup section in the Veeam Backup & Replication User Guide.

Considerations and Limitations

Consider the following about application-aware and database processing:

- Nosnap Veeam Agent for Linux and nosnap Veeam Agent for Linux on Power do not support application-aware processing and cannot be used to back up database systems.
- 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.
- If there are multiple database systems on the Veeam Agent computer, consider the following:
  - Veeam Agent supports processing of multiple PostgreSQL or Oracle database systems on one Veeam Agent computer.
  - Veeam Agent does not support processing of multiple MySQL database systems on one Veeam Agent computer.
  - Veeam Agent does not support processing of multiple database systems of different types on one Veeam Agent computer.

- Veeam Agent does not support 32-bit database systems installed on a 64-bit Linux OS.
- 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.

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 in the standalone mode. This section provides description for such features in the Veeam Agent management scenario.

Backup Job Scripts

You can instruct Veeam Agent for 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. To learn more, 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.

Considerations and Limitations

- Scripts must be created before you configure the backup job. You must specify paths to them in the backup job settings.
- Veeam Agent supports scripts in the .SH file format only.
- Scripts must have UNIX line endings (LF).
- Script settings are enabled at the backup job level. If you want to configure multiple backup jobs, you can specify individual scripts for each job.
- If you use relative paths in your scripts, during script execution such paths will refer to the root directory. For example, the script may have an output that must be saved to a new file. If you specify a relative path to that file or only a file name, the file will be created in the root directory. To specify a different location for a file, use a full absolute path.

Backup of Mac Computers

To back up data of Mac 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.

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

Backup of Cloud Machines

To back up data of Amazon EC2 instances or Microsoft Azure virtual machines (both objects can be also referred to as cloud machines), you can use Veeam Agent for Microsoft Windows or Veeam Agent for Linux together with Veeam Backup & Replication. Veeam Backup & Replication allows you to discover cloud machines and deploy Veeam Agents using cloud native API instead of the connection over network.

Veeam Backup & Replication supports backup of the following cloud machines:

- Amazon EC2 instances
- Microsoft Azure virtual machines

You can back up cloud machines running Microsoft Windows or Linux OSes that are supported by Veeam Agent and by cloud service provider.

- To learn lists of OSes supported by Veeam Agent, see system requirements for Veeam Agent for Microsoft Windows or for Veeam Agent for Linux depending on the type of Veeam Agent you plan to use.
- To learn lists of OSes supported by cloud service provider, see AWS documentation or Microsoft documentation depending on the type of cloud machines you plan to protect.

> IMPORTANT
>
> In case of cloud machines running Microsoft Windows, Windows PowerShell 5.1 must be installed on the cloud machine.

Getting Started

To back up cloud machine data, you must complete the following steps:

1. 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 the Adding Azure Blob Storage or Adding Amazon S3 Storage section in the Veeam Backup & Replication User Guide.

   > NOTE
   >
   > Regardless of the connection mode specified in the backup repository settings, Veeam Agent always performs backup of cloud machines directly to the cloud. Backup data is not sent to Veeam Backup & Replication. For information about the connection modes, see Backup to Object Storage.

2. Get the cloud user with the required permissions. With this user, Veeam Backup & Replication connects to the bucket or container on the cloud. To learn more, see Permissions.
3. Configure a protection group for cloud machines. Keep in mind that the protection group of the cloud machines type is the only applicable protection group to back up data of cloud machines. To learn more, see Creating Protection Groups.

   When you finish configuring a protection group and perform the rescan operation, Veeam Backup & Replication installs the Veeam components on the cloud machine. For more information, see Setup of Veeam Components.

4. Configure a backup job. Depending on the OS running on your cloud machine, see one of the following sections:

   - Creating Job for Windows Computers

- Creating Job for Linux Computers

Setup of Veeam Components

Veeam Backup & Replication installs the following Veeam components on the cloud machine:

- Veeam Cloud Message Service
- Veeam Agent
- Veeam Transport Service

When you add a cloud machine to a protection group, it is managed by Amazon EC2 Simple Systems Manager (SSM) or Azure Run Command depending on the cloud that you use. Unlike working with physical machines, Veeam Backup & Replication does not send commands to cloud machines directly, but through these services. For more information about Amazon SSM and Azure Run Command, see AWS documentation and Microsoft documentation.

To accelerate the communication speed between Veeam Backup & Replication and a cloud machine, Veeam Backup & Replication installs the Veeam Cloud Message Service on the machine during the rescan operation. After the Veeam Cloud Message Service is installed, all communication between Veeam Backup & Replication and the machine is switched from Amazon SSM or Azure Run Command to the Veeam Cloud Message Service. The Veeam Cloud Message Service uses queue services to send commands to the machine: Amazon Simple Queue Service (SQS) or Azure Queue Storage. To learn more about these queue services, see AWS documentation and Microsoft documentation.

To install the Veeam components on the cloud machine, Veeam Backup & Replication uses a distribution repository. Veeam Backup & Replication uploads installation files to the distribution repository using signed URLs, and from there the files are downloaded to the cloud machine. The distribution repository is only used to interchange files between the Veeam Backup & Replication and the machine, not to store backups. For more information, see Distribution Repository.

> IMPORTANT
>
> If you use the Amazon S3 repository in the China region as a distribution repository, make sure that you have the ICP license. This license is required to create signed URLs for Amazon S3 repositories in the China region. For more information, see AWS Documentation.

Veeam Backup & Replication installs the Veeam components on the cloud machine in the following way:

1. Veeam Backup & Replication starts the rescan operation and checks that Amazon SSM or Azure Run Command can receive and execute commands.

   > NOTE
   >
   > Keep in mind that Amazon SSM and Azure Run Command use scripts to execute commands. In some cases, script execution can be blocked — for example, by a PowerShell execution policy. If this happens, the Veeam components installation will fail.

2. Veeam Backup & Replication checks that the cloud machine is not managed by another Veeam backup server.

3. Veeam Backup & Replication creates two queues. Veeam Backup & Replication listens to its queue where a managed Veeam Agent sends messages. Veeam Agent listens to its queue and Veeam Backup & Replication sends messages to it.

   All managed by Veeam Backup & Replication Veeam Agents send messages to one Veeam Backup & Replication queue.

4. Veeam Backup & Replication installs the Veeam Cloud Message Service on the cloud machine and starts it.

5. Veeam Backup & Replication installs Veeam Agent and Veeam Transport Service on the cloud machine.

Communication Scheme

After the installation of Veeam components is completed, Veeam Backup & Replication communicates with the cloud machine and Veeam Agent in the following way:

1. Veeam Cloud Message Service on Veeam backup server sends a message to the queue service on the cloud.

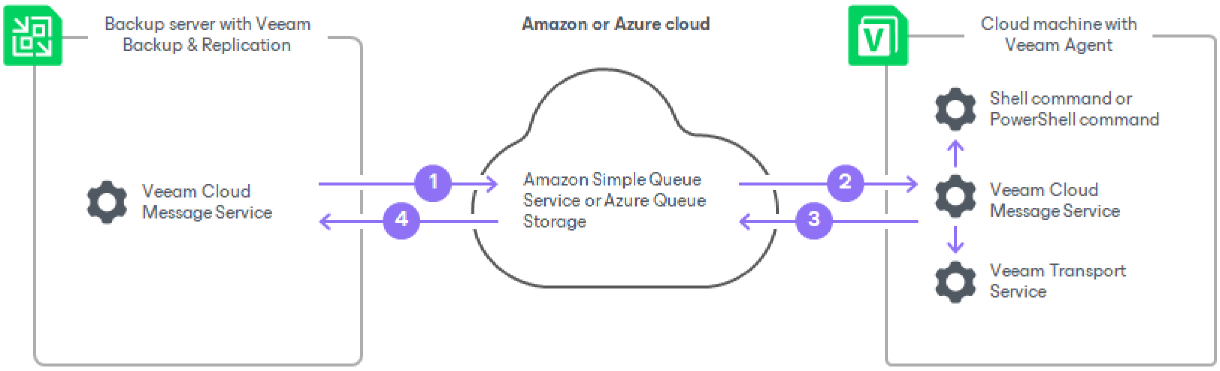
2. Veeam Cloud Message Service on the cloud machine with Veeam Agent checks the queue, reads the message, and performs one of the following operations depending on the message content:

   - Runs the command. For example, if your cloud machine runs the Microsoft Windows OS, Veeam Agent can run the Windows PowerShell command.

   - Re-sends the command to another Veeam component. For example, Veeam Agent or Veeam Transport Service.

3. Veeam Cloud Message Service sends the command result to the queue service.

4. Veeam Backup & Replication reads the queue and receives the command result.


Backup server with Veeam Backup & Replication
Veeam Cloud Message Service
Amazon or Azure cloud
Amazon Simple Queue Service or Azure Queue Storage
Cloud machine with Veeam Agent
Shell command or PowerShell command
Veeam Cloud Message Service
Veeam Transport Service
1
2
3
4

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

> NOTE
>
> Information about the latest Veeam Agent policy run appears in Veeam Backup & Replication only after synchronization with Veeam Agent.

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 and Linux computers only).
- Publish disks from a Veeam Agent backup (for backups of Microsoft Windows computers only).
- Create Veeam Recovery Media from Backup (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
- Google Cloud Storage
- Microsoft Azure Blob Storage
- IBM Cloud Object Storage
- Wasabi Cloud Storage
- Veeam Data Cloud Vault
- 11:11 Cloud Object Storage

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 in the direct connection mode and a backup job managed by Veeam Agent, keep in 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 in the direct connection mode, 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.
- Veeam Agent always performs backup of cloud machines directly to the cloud regardless of the connection mode specified in the backup repository settings.

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. To learn more, 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 the Backup Repositories section in the Veeam Backup & Replication User Guide.
   - Scale-out backup repository added as a Veeam backup repository. To learn more, see the Scale-Out Backup Repositories section in the Veeam Backup & Replication User Guide.
   - Cloud repository. To learn more, see the 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

- Data in object storage repositories must be managed solely by Veeam Backup & Replication, including retention and data management. Lifecycle rules are not supported, and their enabling may result in backup and restore failures.

- For backups located in object storage repositories, synthetic full backup method is not supported.

- For backups located in object storage repositories, compact full backup file option is not supported.

- For backups located in object storage repositories, data recovery options are not available if you access the object storage repository using credentials with the read-only access permissions.

- If you plan to add more than one repository in the object storage as a performance tier of a scale-out backup repository and you plan to back up to these repositories using a direct connection, you can use only managed by backup server backup jobs. If you want to back up data to a scale-out backup repository with backup jobs managed by Veeam Agent, you can use only scale-out backup repositories that have only one repository in the object storage in the direct connection mode as a performance tier.

- [For backup jobs managed by Veeam Agent] If you have a backup job targeted at an object storage added as an extent of a scale-out backup repository in the direct connection mode and you put this extent to the Maintenance or Seal mode during the backup job session while there is no connection between Veeam Backup & Replication and the object storage, the current and subsequent backup job sessions will end successfully.

  To learn about modes you can put extents of scale-out backup repositories to, see the Service Actions with Scale-Out Backup Repositories section in the Veeam Backup & Replication User Guide.

- [For backup jobs managed by Veeam Agent] You cannot back up data to the Veeam Data Cloud Vault storage added in the direct connection mode.

- [For backup jobs managed by Veeam Agent] If you back up data to the S3 compatible object storage with multiple buckets, Veeam Agent will ignore the number of workloads set for one bucket and will store all backups in a single child bucket. To learn more about multiple buckets, see the Multiple Buckets for S3 Compatible Object Storage Repositories section in the Veeam Backup & Replication User Guide.

- [For backup jobs managed by Veeam Agent for Microsoft Windows or Veeam Agent for Linux] If you back up data to an object storage added as a Veeam backup repository in the direct connection mode and you apply backup policy settings after you completed restore to another database from an unencrypted configuration backup, the application of the settings will fail because in this case temporary credentials to access the object storage are not stored in the database.

  To learn about the configuration backup, see the Veeam Backup & Replication Configuration Database section in the Veeam Backup & Replication User Guide.

- [For backup jobs managed by backup server] If you back up data to the S3 compatible object storage added as a Veeam Cloud Connect repository in the direct connection mode, Veeam Agent first transfers data to Veeam Backup & Replication, and then from Veeam Backup & Replication to the object storage.

- For Microsoft Azure Blob storage, Veeam Agents do not support soft delete for blobs.

- If you plan to back up data to the Microsoft Azure Blob storage using a direct connection, the following limitations apply:

  - Cool 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 Microsoft documentation.

- 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 the Immutability for Object Storage Repositories section in the Veeam Backup & Replication User Guide.

- Veeam Agents do 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 Storage
- Microsoft Azure Blob Storage
- IBM Cloud, Wasabi Cloud or other S3 compatible storage

Amazon S3

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 the 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 the 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 Blob 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. If you selected the **Provided by IAM/STS object storage capabilities** option for the object storage, Veeam Backup & Replication will perform the backup operation in the same way as for the Amazon S3 storage.

  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
- S3 compatible storage that supports S3 Object Lock (including Wasabi)
- Microsoft Azure Blob Storage
- Veeam Data Cloud Vault
- 11:11 Cloud Object 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 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.

- [Microsoft Azure Blob storage] Do not enable immutability for already existing containers in the Microsoft Azure Portal. Otherwise, Veeam Agent will not be able to process these containers properly and it may result in data loss.

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 more information, see the Adding Object Storage Repositories section in the 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:

1. Add the object storage repository that contains the necessary data to Veeam Backup & Replication. For more information, see the Adding Object Storage Repositories section in the Veeam Backup & Replication User Guide.
2. Roll back to the necessary checkpoint. For more information, see the Immutability section in the Veeam PowerShell Reference.
3. Remove the repository from the Veeam Backup & Replication infrastructure. For more information, see the Removing Backup Repositories section in the 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 to the specified immutability period depending on the type of the object storage repository:

- 30 days — for Amazon S3 object storage and IBM Cloud object storage.
- 10 days — for other types of object storage repositories.

This additional period 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 or 30-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 extend the immutability expiration date by 10 or 30 days depending on the type of the object storage repository:

- 30 days — for Amazon S3 object storage and IBM Cloud object storage.
- 10 days — for other types of object storage repositories.

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 to the specified immutability period. For example, 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.

Backup to Deduplicating Storage Appliances

You can store backups in the deduplicating storage appliances added as backup repositories. To learn the full lists of supported appliances and their requirements and limitations, see the Deduplicating Storage Appliances section in the Veeam Backup & Replication User Guide.

If you want to use immutability with the deduplicating storage appliances, consider the limitations listed in the following subsections:

- HPE StoreOnce Immutability and Veeam Agents.
- Dell Data Domain Immutability and Veeam Agents.

HPE StoreOnce Immutability and Veeam Agents

If you want to use immutability with HPE StoreOnce Catalyst repositories, make sure that the values of the following settings configured in Veeam Backup & Replication do not exceed the Maximum ISV Controlled Data Retention setting in HPE StoreOnce:

- The immutability period specified in the backup repository settings.
- The long-term retention period configured in backup job settings.

If the value of at least one of these periods exceeds the maximum value set for immutability in HPE StoreOnce Catalyst Store, consider the following:

- If the immutability period specified in the backup repository settings exceeds the maximum value set for immutability in HPE StoreOnce Catalyst Store, Veeam Backup & Replication applies immutability to the created backups according to the maximum value set for immutability in HPE StoreOnce Catalyst Store.
- If the long-term retention period configured in backup job settings exceeds the maximum value set for immutability in HPE StoreOnce Catalyst Store, the immutability period for backups with GFS flags is set according to the maximum value set for immutability in HPE StoreOnce Catalyst Store. For example, if the backup is stored for 1 year, but the maximum value for immutability in HPE StoreOnce Catalyst Store is set to 6 months, the backups will be immutable for 6 months.

To learn more about immutability for the HPE StoreOnce Catalyst repositories, see the HPE StoreOnce and Immutability section in the Veeam Backup & Replication User Guide.

Dell Data Domain Immutability and Veeam Agents

If you want to use immutability with the Dell Data Domain backup repository, make sure that the values of the following settings configured in Veeam Backup & Replication lie in the range between the minimum and maximum retention periods configured in Dell Data Domain:

- The immutability period specified in the backup repository settings.
- The long-term retention period configured in backup job settings.

The minimum and maximum values are included into the range.

If the value of at least one of these periods lies outside the established range, consider the following:

- If the immutability period specified in the backup repository settings lies outside the range between the minimum and maximum retention periods configured in Dell Data Domain, the immutability for backups is set equal to the nearest range value.
- If the long-term retention period configured in backup job settings lies outside the range between the minimum and maximum retention periods configured in Dell Data Domain, the immutability period for backups with GFS flags is set equal to the nearest range value. For example, if the backup is stored for 1 year, but the range for immutability in Dell Data Domain is set to from 2 to 6 months, the backups will be immutable for 6 months.

To learn more about immutability for the Dell Data Domain backup repositories, see the Retention Lock section in the Veeam Backup & Replication User Guide.

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.

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 Using SureBackup Job.

General Limitations

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

- SureBackup is not supported for backup files created by backup copy jobs.
- SureBackup is not supported for backups stored in the Veeam Cloud Connect repository.
- SureBackup is not supported for backups stored in the archive tier of the the scale-out backup repository.
- [For full recoverability testing mode] SureBackup is not supported for backups containing drives greater than 64 TB.
- [For full recoverability testing mode] 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.
- [For full recoverability testing mode] When Veeam Backup & Replication publishes virtual machines based on backed-up Veeam Agent computers in the isolated virtual environment, all these virtual machines are included in the first isolated network added during the virtual lab configuration. To learn more, see the Create Isolated Networks section in the Veeam Backup & Replication User Guide.

Limitations for Backups Created with Veeam Agent for Microsoft Windows

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

- [For full recoverability testing mode] SureBackup is not supported for file-level backups. You must use entire machine or volume-level backup of the protected computer. The backup must include the computer system volume. To learn more about backup types, see the Backup Types section in the Veeam Agent for Microsoft Windows User Guide.
- [For full recoverability testing mode] SureBackup is not supported if the Microsoft Windows system partition and boot partition of the backed-up computer are located on different drives.

- [For full recoverability testing mode] SureBackup is not supported for failover clusters.
- [For full recoverability testing mode] If you plan to verify computer recovery with Microsoft Hyper-V, SureBackup is not supported for application groups with computers connected to different networks.
- [For full recoverability testing mode] If you plan to verify computer recovery with Microsoft Hyper-V, SureBackup is not supported for EFI-based Veeam Agent computers that run Windows 7, Windows Server 2008 or Windows Server 2008 R2.

Limitations for Backups Created with Veeam Agent for Linux

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

- You cannot use SureBackup with backup files created with Veeam Agent for Linux on Power.
- SureBackup job in the **Backup verification and content scan only** mode is not supported.
- The successful recovery verification is not guaranteed for the following Linux distributions:
  - Amazon Linux 2
  - Amazon Linux 2023
  - openSUSE Tumbleweed
- The successful recovery verification is not guaranteed for backups of Linux-based systems that contain encrypted devices.
- If you want Veeam Backup & Replication to connect the recovered VM to the virtual network, one of the following configuration utilities must be installed on the protected computer:
  - Netplan
  - NetworkManager
  - sysconfig
  - systemd-networkd
  - ifupdown/ifupdown2
- SureBackup is not supported for file-level backups. You must use volume-level backup of the protected computer. The backup must include the `root` file system (/) and all partitions specified in the `/etc/fstab` file. 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:

- If you have already been using Veeam Agents with Veeam Backup & Replication in the standalone mode, 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.
- 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 in the topics below.

> NOTE
>
> 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.

System Requirements for Microsoft Windows Computers

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

Specification	Requirement
Hardware	CPU: x86 or x64. Memory: 2 GB RAM or more. Memory consumption varies depending on the number and size of processed disks. Disk Space: 200-700 MB for product installation. Required disk space varies depending on the Veeam Agent usage scenario. 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.

Specification	Requirement
OS	Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported[1]: • Microsoft Windows Server 2025 • 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 (from version 21H2 to version 24H2) • Microsoft Windows 10 Semi-Annual Channel (from version 1803 to version 22H2)[3] • Microsoft Windows 10 Long-Term Servicing Channel (versions 2015, 2016, 2019, 2021) • Microsoft Windows 8.1[4] • Microsoft Windows 7 SP1[4] 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. • Microsoft Windows OSes installed on ReFS boot partitions are not supported. • Server Core installations of Microsoft Windows Server OSes can be backed-up only by Veeam Agent backup jobs managed by the Veeam backup server. Note: to ensure proper work of Veeam Agent, do not uninstall the WoW64 feature. • 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. [4] OS is not supported for cloud machines.
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, see Microsoft documentation.

Specification	Requirement
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

Considerations and Limitations

Consider the following:

- 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.
- Devices managed by Veritas Volume Manager are not supported.
- Supported culture settings depend on the version of Microsoft Windows OS installed on your computer. To learn more, see this Microsoft article.

System Requirements for Linux Computers

You can use Veeam Backup & Replication to manage Veeam Agent for Linux that was installed using a package with the Veeam kernel module dependency or using a nosnap package without dependency on the Veeam kernel module. On IBM Power Systems, Veeam Agent for Linux can be installed using a special nosnap package — Veeam Agent for Linux on Power.

Veeam kernel module is used for creating system snapshots. The nosnap version of Veeam Agent for Linux leverages the native snapshot capabilities of the supported file systems. For information on system requirements for nosnap versions of Veeam Agent for Linux, see System Requirements for Linux Computers (nosnap Veeam Agent).

> NOTE
>
> You can add computers with the nosnap version of Veeam Agent for Linux on Power installed only to the protection group for pre-installed Veeam Agents.

Veeam Agent Computer (Veeam Kernel Module)

Specification	Requirement
Hardware	**IMPORTANT!** Check considerations and limitations that apply to the list of supported hardware. CPU: x86 or x64. Memory: 1 GB RAM or more. Memory consumption varies depending on the backup type and the total amount of backed-up data. Disk Space: 100-500 MB for product installation. Required disk space varies depending on the Veeam Agent usage scenario. 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.

Specification	Requirement
OS	**IMPORTANT!** Check considerations and limitations that apply to the list of supported OSes. Linux kernel version 2.6.32 to version 6.12 is supported. Veeam Agent supports the 64-bit versions of the following distributions: • Debian 10.13 - 12.8 • Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10, 23.04, 23.10, 24.04 and 24.10 • RHEL 6.4 - 9.5 • CentOS 7 • Oracle Linux 6 - 9.5 (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 5.15.0-302.167.6.el9uek) • SLES 12 SP4, 12 SP5, 15 SP1 - 15 SP6 • SLES for SAP 12 SP4, 12 SP5, 15 SP1 - 15 SP6 • Fedora 36, 37, 38 and 39 • openSUSE Leap 15.3 - 15.6 • Rocky Linux 8.10, 9.3 - 9.5 • AlmaLinux 8.10, 9.3 - 9.5 • openSUSE Tumbleweed has an experimental support status. To learn more about experimental support, see this Veeam KB article. • Amazon Linux 2 (starting from kernel version 5.10) and Amazon Linux 2023 — these distribution are supported for cloud machines only and have an experimental support status. 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: • BTRFS (for OSes that run Linux kernel 3.16 or later) • Ext 2/3/4 • F2FS • FAT16 • FAT32 • HFS • HFS+ • JFS • 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. Other file systems, file systems that are not located on logical volumes, as well as network file systems like NFS or SMB shares can be backed up using the snapshot-less mode only. For details, see the Snapshot-Less File-Level Backup section in the Veeam Agent for Linux User Guide.

Specification	Requirement
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) • kernel-uek-devel (for Oracle Linux systems with UEK) • libudev • libacl • libattr • lvm2 • libfuse2 (FUSE libraries for Debian-based and SLES-based systems) • fuse-libs (FUSE libraries for RedHat-based and Fedora systems) • libncurses5 • 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) • tar (for file system indexing, log export and rotation) • gzip (for file system indexing, log export and rotation)

Considerations and Limitations

Hardware

- 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; backup of such devices may result in corruption of the source file system — for more information, see this Veeam KB article.
- Devices managed by Veritas Volume Manager are not supported.

OS

- Linux kernel version 2.6.32 to version 6.12 is supported as long as you use kernels supplied by your distribution with the following limitation: 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.

  If a new version of a supported Linux distribution is released after the release of the current version of Veeam Agent, Veeam Agent may require a patch to support this new OS version. To learn more about Veeam Agent compatibility with Linux OS versions, see this Veeam KB article. Customers with a valid contract can request a patch from Veeam Support; for other customers, the support of the new Linux distribution will be provided with the next release of Veeam Agent.
- [For RHEL 6 and 7] Veeam Agent supports the following versions of RHEL with Extended Life-cycle Support Add-On: 6.10 and 7.9.
- [For RHEL 8 and 9] Veeam Agent supports the following versions of RHEL with Extended Update Support Add-On: 8.4, 8.6, 8.8, 8.10, 9.0, 9.2 and 9.4.
- To ensure proper functioning of the Veeam kernel module, verify that your system does not have any of the following modules installed: `hcpdriver`, `snapapi26`, `snapapi`, `snapper`, `dattobd`, `dattobd-dkms`, `dkms-dattobd`, `cdr` or `cxbf`.
- 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 that are not in the list of supported OSes), the `veeamsnap` kernel module has an experimental support status.
- For backups of cloud machines running Amazon Linux 2 and Amazon Linux 2023, only file-level restore is supported.
- Automatic Veeam Agent deployment and upgrade 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. To learn more, see the Installing Veeam Agent for Linux section in the Veeam Agent for Linux User Guide.
- Automatic upgrade from Veeam backup console is not supported for manually deployed Veeam Agents.
- RHEL, CentOS, and Oracle Linux (RHCK) are supported up to certain kernel versions. To learn more, see this Veeam KB article.
- Ubuntu with Linux kernel for KVM (Kernel-based Virtual Machine) is not supported. For the list of linux-kvm kernels for Ubuntu, see Ubuntu documentation.
- You must not install Veeam Agent on the server that is used as a hardened repository in the Veeam Backup & Replication infrastructure.

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 216 TiB. 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 TiB.
  - 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.
- To store volume snapshots, the `blksnap` kernel module requires an Ext4, BTRFS or XFS file system. Snapshot file cannot be stored on multi-device BTRFS.
- 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 shared 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.
- Backup of pseudo file systems, such as /proc, /sys, tmpfs, devfs and others, is not supported.
- Backup of BTRFS volumes and subvolumes with enabled file-system compression is not supported.

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 package with Veeam kernel module is to be installed.
  - dkms
  - gcc
  - make
  - perl
  - kernel-headers (for RedHat-based systems)
  - kernel-devel (for RedHat-based systems)

  To learn more, 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)
  - kernel-uek-devel (for Oracle Linux systems with UEK)
- 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.

System Requirements for Linux Computers (nosnap Veeam Agent)

If you plan to use a nosnap package to install Veeam Agent, the protected Linux computer must meet the following system requirements:

Specification	Requirement
Hardware	[For nosnap Veeam Agent for Linux] CPU: x86 or x64. [For nosnap Veeam Agent for Linux on Power] CPU: IBM POWER9 or POWER10. 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. Disk layout: MBR or GPT.
OS	**Important!** Check considerations and limitations that apply to the list of supported OSes. **Nosnap Veeam Agent for Linux** supports the 64-bit versions of the following distributions: • Debian 10.13 - 12.8 • Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10, 23.04, 23.10, 24.04 and 24.10 • RHEL 6.4 - 9.5 • CentOS 7 • Oracle Linux 6 - 9.5 (RHCK) • Oracle Linux 6 (starting from UEK R2) - Oracle Linux 9 (up to 5.15.0-209.161.7.2.el9uek) • SLES 12 SP4, 12 SP5, 15 SP1 - 15 SP6 • SLES for SAP 12 SP4, 12 SP5, 15 SP1 - 15 SP6 • openSUSE Leap 15.3 - 15.6 • Rocky Linux 8.10, 9.3 - 9.5 • AlmaLinux 8.10, 9.3 - 9.5 • openSUSE Tumbleweed has an experimental support status. For details about experimental support, see this Veeam KB article. Nosnap Veeam Agent supports 32-bit versions of RHEL 6 and Oracle Linux 6 distributions only. **Nosnap Veeam Agent for Linux on Power** supports little endian versions of the following Linux distributions for IBM Power: • SLES 15 SP3 - 15 SP6 • SLES for SAP 12 SP5, 15 SP3 - 15 SP6 • RHEL 8.4, 8.6, 8.8., 8.10 and 9.4 • RHEL for SAP 8.4, 8.6, 8.8., 8.10 and 9.4

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: • All supported file systems that are built on top of LVM logical volumes. • BTRFS (for OSes that run Linux kernel 3.16 or later) [For nosnap Veeam Agent for Linux] 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. [For nosnap Veeam Agent for Linux on Power] If BTRFS has additional abstraction layers (such as LVM, software RAID, dm-crypt and so on) above it, only file-level restore operations are supported. Instant Recovery, restore verification (SureBackup), bare metal recovery and volume-level restore are not supported. Supported file systems that are not located on logical volumes, other file systems and network file systems like NFS or SMB shares can be backed up using the snapshot-less mode only. 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: • libacl • libattr • lvm2 • libfuse2 (FUSE libraries for Debian-based and SLES-based systems) • fuse-libs (FUSE libraries for RedHat-based and Fedora systems) • dmidecode[2] • efibootmgr (for UEFI-based systems)[2] • isolinux (for Debian-based systems)[2] • syslinux (for RedHat-based systems) • btrfs-progs (for backup of BTRFS file system) • mksquashfs (for custom Veeam Recovery Media)[2] • unsquashfs (for custom Veeam Recovery Media)[2] • wget (for custom Veeam Recovery Media)[2] • xorriso (for custom Veeam Recovery Media with EFI support)[2] • tar (for file system indexing, log export and rotation) • gzip (for file system indexing, log export and rotation) [2] Nosnap Veeam Agent for Linux on Power does not require the following packages: dmidecode, efibootmgr, isolunux, mksquashfs, unsquashfs, wget and xorriso.

Considerations and Limitations

OS

- Only GA versions of the supported distributions that have been released before the current version of Veeam Agent for Linux are supported.

  If a new version of a supported Linux distribution is released after the release of the current version of Veeam Agent, Veeam Agent may require a patch to support this new OS version. For details on Veeam Agent compatibility with Linux OS versions, see this Veeam KB article. Customers with a valid contract can request a patch from Veeam Support; for other customers, the support of the new Linux distribution will be provided with the next release of Veeam Agent.

- The Linux OS must be set up to receive software updates from the default repositories enabled in the OS after installation.

- [For nosnap Veeam Agent for Linux] Veeam Agent supports the following versions of RHEL with Extended Life-cycle Support Add-On: 6.10 and 7.9. Veeam Agent supports the following versions of RHEL with Extended Update Support Add-On: 8.4, 8.6, 8.8, 8.10, 9.0, 9.2 and 9.4.

- [For nosnap Veeam Agent for Linux on Power] Veeam Agent supports the following versions of RHEL with Extended Update Support Add-On: 8.4, 8.6, 8.8, 8.10 and 9.4.

- You must not install Veeam Agent on the server that is used as a hardened repository in the Veeam Backup & Replication infrastructure.

File System

- Veeam Agent for Linux does not back up volumes that reside on USB devices and SD cards.

- LVM volumes encrypted with `dm-crypt` software are not supported.

- Total size of all file systems must not exceed 216 TiB. 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 TiB.

- 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.

- The amount of space required for LVM snapshots largely depends on the IO intensity. Generally, from 10% to 20% of the system's occupied space should be enough for storing an LVM snapshot.

- Veeam Agent supports backup of extended attributes with the following limitations:

  - Veeam Agent 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.

- Consider the following about the backup of machines used as cluster nodes:
    - To back up data on local LVM volumes, you can use file-level backup or volume-level backup.

      > NOTE
      >
      > Consider the following:
      >
      > - During volume-level backup, data from shared disks, clustered file systems or clustered LVM will not be backed up.
      > - To perform volume-level backup, Veeam Agent for Linux will create an LVM snapshot, which can cause instability of the cluster or cluster software. This can happen due to the failover conditions configured for the cluster. However, if the cluster instability is caused by creation of an LVM snapshot only during backup, contact Veeam support for assistance.

    - Backup of clustered file systems using a native file system snapshot is not supported. This includes snapshots created with the help of custom pre-job or post-job scripts.
    - The following objects can be backed up only by snapshot-less file-level backup:
        - Files on shared disks, clustered file systems or clustered LVM.
        - Files on local file systems that are not hosted by LVM.
- Certain limitations for Dell PowerPath configuration apply. To learn more, see this Veeam KB article.
- Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files.
- Backup of pseudo file systems, such as `/proc`, `/sys`, `tmpfs`, `devfs` and others, is not supported.
- Backup of BTRFS volumes and subvolumes with enabled file-system compression is not supported.

Software

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

- [For nosnap Veeam Agent for Linux] 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. For details, see the MySQL Backup section in the Veeam Agent for Linux User Guide. 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. For details, see the PostgreSQL Backup section in the Veeam Agent for Linux User Guide.
- The `btrfs-progs` package version 3.16 or later is required.

System Requirements for Unix Computers

This topic lists system requirements for Veeam Agent computers that run on IBM AIX or Oracle Solaris.

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 standard backup and restore operations) / 4 GB RAM (for bare metal recovery). 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 7.1 – 7.3 TL2 are supported. **Note:** • IBM AIX 7.3 TL2 is supported starting from Veeam Agent version 4.1. • 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 4.6 are are supported.
File System	All file systems supported by the supported operating systems. Consider the following: • Total size of all file systems included in a file-level backup must not exceed 216 TiB. • Size of a file in a backup must not exceed 16 TiB. • 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. • JFS2 snapshots are not supported. • Backup of clustered systems (including IBM PowerHA SystemMirror) is not supported.

Specification	Requirement
Software	**IMPORTANT!** The user account used to work with Veeam Agent for IBM AIX installed on the protected computer must have the `/bin/bash` shell set as the default shell. The following utilities must be installed on the machine: • `mlocate` — required for file system indexing. You must use the `mlocate` utility that is provided with Veeam Agent in the product installation media. If you upgrade to Veeam Agent for IBM AIX version 12.1 and you have the `mlocate` utility provided with one of the previous versions of Veeam Agent for IBM AIX installed in your system, you must replace the existing `mlocate` utility with the `mlocate` utility provided with Veeam Agent 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. [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] You must install version 1.13 of the `mkisofs` utility. • [For IBM AIX 7.1] `bos.rte.libc` version 7.1.5.0 or later must be installed.

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. To learn more, 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 standard backup and restore operations) / 4 GB RAM (for bare metal recovery). 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 1/13, 11.0 – 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 4.6 are supported.
File System	All file systems supported by the supported operating systems. Consider the following: • Total size of all file systems included in a file-level backup must not exceed 216 TiB. • Size of a file in a backup must not exceed 16 TiB. • 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. • Backup of clustered systems is not supported.

Specification	Requirement
Software	**IMPORTANT!** The user account used to work with Veeam Agent for Oracle Solaris installed on the protected computer must have the `/bin/bash` shell set as the default shell. 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`.

System Requirements for Mac Computers

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[1]. • Memory: 2 GB RAM or more. Memory consumption varies depending on the total amount of backed-up data. • Disk Space: 450 MB free disk space for product installation. • Network: 10 Mbps or faster network connection to a backup target. [1] 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: • 15 Sequoia[2] • 14 Sonoma[2] • 13 Ventura • 12 Monterey • 11 Big Sur • 10.15 Catalina • 10.14 Mojave • 10.13.6 High Sierra [2] MacOS 15 Sequoia is supported starting from version 2.3, macOS 14 Sonoma is supported starting from version 2.1.

Specification	Requirement
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 216 TiB. • Size of a file in a backup must not exceed 16 TiB. • 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 storage targets listed below.

Veeam Agent Backup Jobs Managed by Backup Server

- [For Veeam Agent for Microsoft Windows 6.3, Veeam Agent for Linux 6.3 and Veeam Agent for Mac 2.3] Veeam Backup & Replication version 12.3 backup repository
- [For Veeam Agent for IBM AIX 4.6 and Veeam Agent for Oracle Solaris 4.6] Veeam Backup & Replication version 12.1 or later backup repository
- Veeam Cloud Connect 12.0 or later cloud repository

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] Storage devices with the exFAT file system are not supported as a backup target.

- 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 (except backups of Unix computers)
- [For Veeam Agent for Microsoft Windows 6.3, Veeam Agent for Linux 6.3 and Veeam Agent for Mac 2.3] Veeam Backup & Replication version 12.3 backup repository
- [For Veeam Agent for IBM AIX 4.6 and Veeam Agent for Oracle Solaris 4.6] Veeam Backup & Replication version 12.1 or later backup repository
- Veeam Cloud Connect 12.0 or later cloud repository

  > **IMPORTANT**
  >
  > Veeam Cloud Connect repository is not supported as a backup and backup copy target for the following Veeam Agents:
  >
  > - Veeam Agent for IBM AIX
  > - Veeam Agent for Oracle Solaris
  > - Veeam Agent for Linux on Power

Network

Consider the following about network requirements:

- Veeam Agent must 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)
  - [Not applicable to Veeam Agent for Unix] Kerberos

  To learn more, see the Kerberos Authentication section in the Veeam Backup & Replication User Guide.
- 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.

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 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
  >
  > Keep in mind that if you want to use Veeam Agent to protect a VM residing on a virtualization host, Veeam Backup & Replication will use sockets to license such a VM. In this scenario, Veeam Agent will not consume instances in the license, but if no sockets are available, Veeam Agent will not be able to perform backup.

- *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 in the Community edition of the product, you cannot use Veeam Agents to protect computers running on Unix or Linux on Power. To protect such computers, you must use the 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.

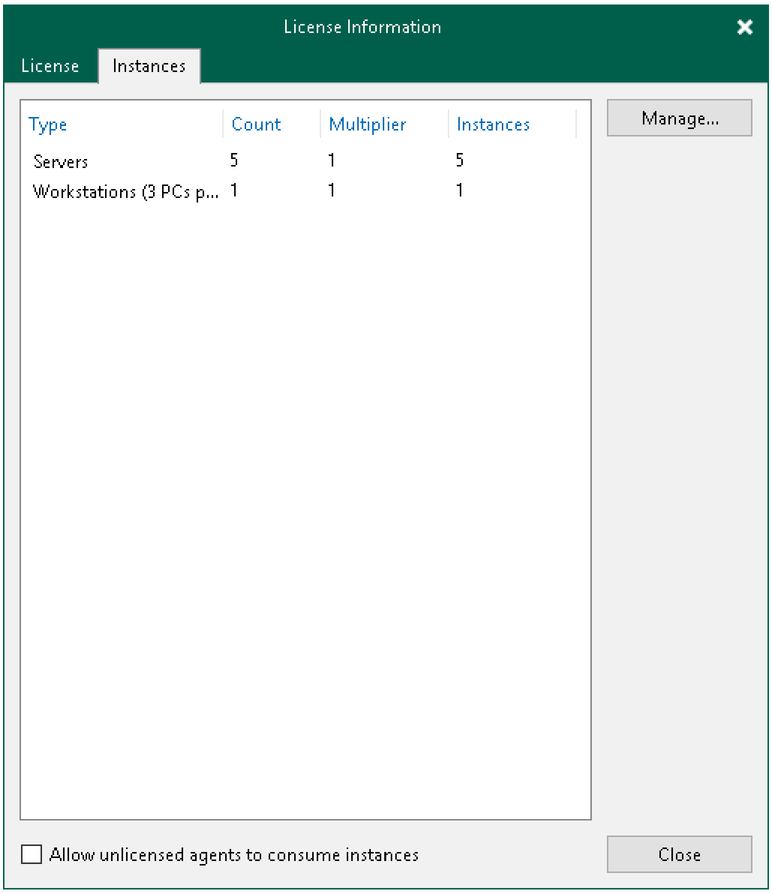
Managing Instance Consumption by Veeam Agents

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 all managed 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**.



Type	Count	Multiplier	Instances
Servers	5	1	5
Workstations (3 PCs p...	1	1	1

☐ Allow unlicensed agents to consume instances

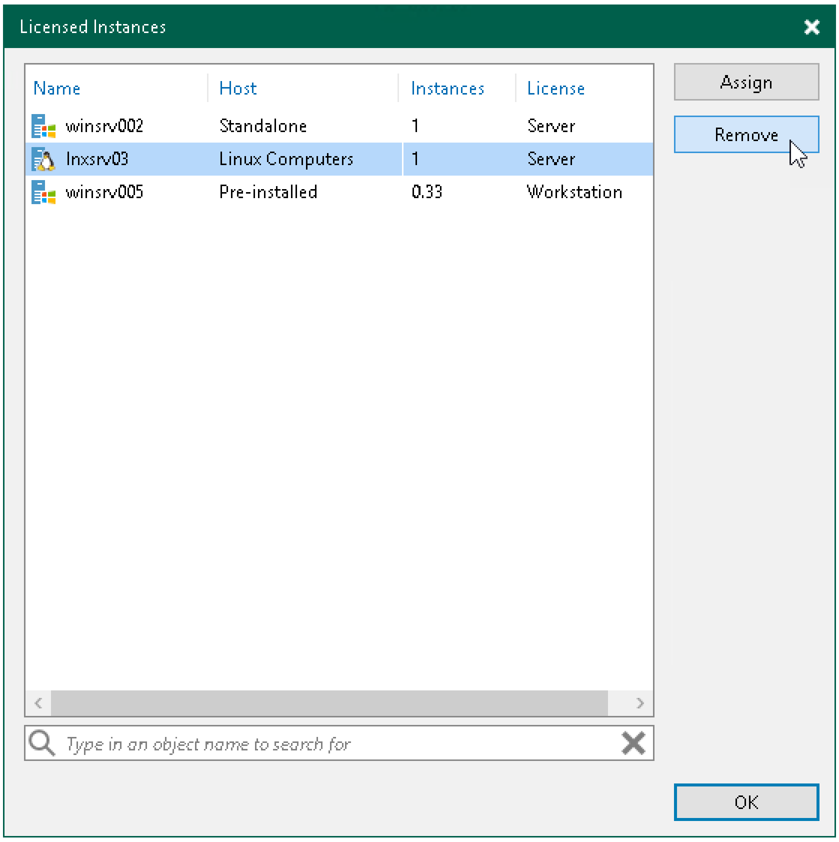
If you do not want to restrict license consumption for all managed Veeam Agents, you can revoke a license from specific Veeam Agents.

To restrict instance consumption by specific Veeam Agents:

1. From the main menu, select **License**.
2. In the **License Information** window, click the **Instances** tab and click **Manage**.
3. In the **Licensed Instances** window, select a Veeam Agent and click **Remove**.

NOTE

Keep in mind that Veeam Agent will start consuming the license again during the next backup job session.



Name	Host	Instances	License
winsrv002	Standalone	1	Server
lnxsrv03	Linux Computers	1	Server
winsrv005	Pre-installed	0.33	Workstation

TIP

With the **Assign** button, you can assign a license to Veeam Agents operating in the standalone mode. For example, see the Assigning License to Veeam Agent section in the Veeam Agent for Microsoft Windows User Guide.

You cannot assign a license with the **Assign** button to Veeam Agents operating in the managed mode. The license type of Veeam Agents operating in the managed mode depends on the job mode specified in the backup job settings. To learn more, see Working with Veeam Agent Backup Jobs and Policies.

Permissions

For general requirements for permissions that must be provided to the user account to install and work with Veeam Backup & Replication, see the Permissions section in the Veeam Backup & Replication User Guide. In addition to general port requirements, for the Veeam Agent management scenarios the following permissions must be provided .

Keep in mind that the list of required permissions differs depending on the functionality that you use. Make sure that user accounts have permissions listed in the following subsections:

- Permissions for Backup of Cloud Machines
- Permissions for Backup to Object Storage
- Permissions for Guest Processing

> **NOTE**
>
> If you plan to back up data using a direct connection between the Veeam Agent computer and object storage, consider the access permissions in Access Permissions for Direct Connection to Object Storage.

Permissions for Backup of Cloud Machines

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

- Microsoft Azure virtual machines
- Amazon EC2 instances

Microsoft Azure Virtual Machines

If you want to back up Microsoft Azure virtual machines, a Microsoft Azure Compute Account that you use must have the following permissions:

```
{
 "actions": [
   "Microsoft.Compute/virtualMachines/instanceView/read",
   "Microsoft.Compute/virtualMachines/read",
   "Microsoft.Compute/virtualMachines/runCommand/action",
   "Microsoft.Resources/subscriptions/locations/read",
   "Microsoft.Storage/storageAccounts/read"
 ],
   "notActions": [],
   "dataActions": [],
   "notDataActions": []
}
```

The permissions are assigned in the following ways:

- If you use an existing Microsoft Azure Compute Account, make sure to assign the required permissions.
- If you create a new Microsoft Azure Compute Account with Veeam Backup & Replication, the required permissions are assigned to the newly created account automatically.

To learn more, see the Microsoft Azure Compute Accounts section in the Veeam Backup & Replication User Guide.

Amazon EC2 Instances

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

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

Permissions for Backup to Object Storage

The general permissions for backup to object storage are listed in the Using Object Storage Repositories section in the Veeam Backup & Replication User Guide. Additional permissions are required for object storage in the Veeam Agent management infrastructure. The list of additional permissions differs depending on the selected object storage and the way you set your backup infrastructure:

- Amazon S3
- S3 compatible (including IBM Cloud Object Storage and Wasabi Cloud Storage)
- Google Cloud Storage

Amazon S3

Consider the following:

- Make sure the user 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.

Make sure that your infrastructure configuration fits the following description:

- 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.

If you plan to back up data using such infrastructure configuration, make sure the user account that you use to connect to the object storage has the following permissions:

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

S3 Compatible (Including IBM Cloud Object Storage, Wasabi Cloud Storage)

Consider the following:

- Make sure the user 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.

Make sure that your infrastructure configuration fits the following description:

- 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 such infrastructure configuration, make sure the user account that you use to connect to the object storage has the following permissions:

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

Google Cloud Storage

Make sure that your infrastructure configuration fits the following description:

- 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 such infrastructure configuration, make sure the user account that you specify in the Helper Appliance settings has the following permissions:

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

Permissions for Guest Processing

To use guest processing, make sure to configure user accounts according to the following requirements.

Consider the following general requirements when choosing a user account:

- For Linux computers, choose a user account with root privileges and with the home directory created.
- If you plan to perform file indexing for Microsoft Windows computers, choose a user account that has administrator privileges.
- If you plan to use guest processing over network for Microsoft Windows computers without listed applications, choose a user account that has administrator privileges.
- When using Active Directory accounts, make sure to provide a user account in the *DOMAIN\Username* format.
- When using local user accounts, make sure to provide a user account in the *Username or HOST\Username* format.
- To process a Domain Controller server, make sure that you are using a user account that is a member of the *DOMAIN\Administrators* group.
- To back up a Read-Only Domain controller, a delegated RODC administrator account is sufficient. For more information, see Microsoft Documentation.

Depending on the application you need to back up, the user must have the permissions listed in the following table:

Application	Required Permission
Microsoft SQL Server	To back up Microsoft SQL Server data, the user whose account you plan to use must be: • Local Administrator on the Veeam Agent computer. • System administrator (has the *Sysadmin* role) on the target Microsoft SQL Server. If you need to provide minimal permissions, the user account must be assigned the following roles and permissions: • SQL Server instance-level role: *public* and *dbcreator*. • Database-level roles and roles for the model system database: *db_backupoperator*, *db_denydatareader*, *public*; for the master system database — *db_backupoperator*, *db_datareader*, *public*; for the msdb system database — *db_backupoperator*, *db_datareader*, *public, db_datawriter*. • Securables: *view any definition*, *view server state, connect SQL*.
Microsoft Active Directory	To back up Microsoft Active Directory data, the user account must be a member of the built-in *Administrators* group.
Microsoft Exchange	To back up Microsoft Exchange data, the user account must have the local Administrator permissions in Microsoft Exchange.
Oracle	On Microsoft Windows computers To back up Oracle data on a Microsoft Windows computer, the user account must be configured as follows: • The user account must be a member of both the Local Administrators group and the *ORA_DBA* group (if OS authentication is used). • The user account must be granted *SYSDBA* privileges.

Application	Required Permission
	On Linux computers To back up Oracle data on a Linux computer, the user account must be configured as follows: - The user account must be granted *SYSDBA* privileges. - To back up Oracle database archived logs, the user account must have the primary membership in the Oracle Inventory Group (oinstall) group. To learn how to configure the Oracle Inventory Group, see Oracle documentation. Also, consider the following about backup of Oracle data on a Linux computer: - You can use either the same account that was specified at the Guest Processing step if such an account is a member of the *OSDBA* and *OINSTALL* groups, or you can use any other account that has *SYSDBA* privileges. For more information about specifying a user account, see Application-Aware Processing. - To perform guest processing for Oracle databases on Linux servers, make sure that the /tmp directory is mounted with the exec option. Otherwise, you will get a "Permission denied" error.
Microsoft SharePoint	To back up Microsoft SharePoint server, the user account must have the Farm Administrator role. To back up Microsoft SQL databases of the Microsoft SharePoint Server, the user account must have the same privileges as for the Microsoft SQL Server.
MySQL	To process the MySQL database system, the MySQL user account must have the following privileges: - SELECT for all tables. This privilege is required to allow Veeam Agent to access table metadata. To learn more, see MySQL documentation. - LOCK TABLES. This privilege is required to allow Veeam Agent to process tables based on the MyISAM storage engine. - RELOAD. This privilege is required to allow the MySQL account to perform FLUSH operations.
PostgreSQL	To back up PostgreSQL instances, the user account must have the superuser privileges for the PostgreSQL instance. For more information, see PostgreSQL documentation.

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.

From	To	Protocol	Port	Notes
		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 if you use NetBIOS in your infrastructure. Ports 137 to 139 and 445 are used in the following cases: • deployment of Veeam Installer Service • restore started from the Veeam Backup & Replication console Ports 6160 and 11731 are used to deploy Veeam Agent on the computer and to perform 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 section in the Veeam Backup & Replication User Guide.
		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 Always On Availability Groups.
		TCP	6160, 11731	Port used for the volume-level restore.
		TCP	6162	Default port used by the Veeam Data Mover.

From	To	Protocol	Port	Notes
	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 Deployer Service and Veeam Transport Service. **Note**: You can customize ports 6160 and 6162 using registry keys. To learn more, see this Veeam KB article.
		TCP	6162	Default port used by the Veeam Data Mover. **Note** You can customize port 6162 using registry keys. To learn more, see this Veeam KB article.
		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. **Note**: Ports 2500 – 3300 are required if during data transmission, the Veeam Data Mover Service is started on the Veeam backup server — for example, when the backup is targeted at the default backup repository of the Veeam backup server or when Veeam backup server acts as a gateway to the target backup repository.
	Veeam Agent Computer (Unix)	TCP	22	Port 22 is used to establish an SSH connection from the Veeam Backup Server to the Veeam Agent computer.

From	To	Protocol	Port	Notes
		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. **Note**: Ports 2500 - 3300 are required if during data transmission, the Veeam Data Mover Service is started on the Veeam backup server — for example, when the backup is targeted at the default backup repository of the Veeam backup server or when Veeam backup server acts as a gateway to the target backup repository.
	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 if you use NetBIOS in your infrastructure. 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. **Note** You can customize port 6160 using registry keys. To learn more, see this Veeam KB article.
		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.
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.

From	To	Protocol	Port	Notes
		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 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 Deployer Service and Veeam Transport Service. **Note**: You can customize ports 6160 and 6162 using registry keys. To learn more, see this Veeam KB article.
	Veeam Agent Computer (Unix)	TCP	22	Port 22 is used to establish an SSH connection for Veeam Agent packages transmission and deployment control.
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.
		TCP	10001	Port used by Veeam Agent for direct connection to the Veeam backup server using credentials. For example, during bare metal restore from a backup created by Veeam Agent operating in the managed mode.
		TCP	2500 to 3300	Default range of ports used to publish the ransomware index. For every TCP connection that a backup job uses, one port from this range is assigned.

From	To	Protocol	Port	Notes
Veeam Agent Computer (Linux)	Veeam Backup Server	TCP	10002, 10006	Default ports used for communication with the Veeam Backup server. Data between the Veeam Agent computer and backup repositories is transferred directly, bypassing Veeam backup servers. **Note**: By default, port 10002 is used only by Veeam Agent version 1.x.
Veeam Agent Computer (Unix, macOS)	Veeam Backup Server	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 SMB (CIFS) share	TCP UDP	137 to 139, 445	Ports used as a transmission channel from the Veeam Agent computer to the target SMB (CIFS) share. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS if you use NetBIOS in your infrastructure.
	Gateway Microsoft Windows server	TCP UDP	137 to 139, 445	If an SMB (CIFS) 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 if you use NetBIOS in your infrastructure.

From	To	Protocol	Port	Notes
		TCP	49152 to 65535	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.

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 that must be opened to ensure proper communication with object storage if you back up data to object storage that Veeam Agent accesses directly. For more information about object storage connection modes, see Backup to Object Storage.

From	To	Protocol	Port	Notes
Gateway server or backup server	Amazon S3 object storage	TCP	443	Used to communicate with the Amazon S3 object storage through the following endpoints: • `*.amazonaws.com` (for both *Global* and *Government* regions) • `*.amazonaws.com.cn` (for *China* region) All AWS service endpoints are specified in the AWS documentation.
			80	Used to verify the certificate status through the following endpoints: • `*.amazontrust.com` • `*.cloudfront.net` Consider 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.
	Microsoft Azure object storage	TCP	443	Used to communicate with the Microsoft Azure object storage through the following endpoints: • `xxx.blob.core.windows.net` (for *Global* region) • `xxx.blob.core.chinacloudapi.cn` (for *China* region) • `xxx.blob.core.usgovcloudapi.net` (for *Government* region) Consider that the <xxx> part of the address must be replaced with your actual storage account URL that can be found in the Azure management portal.

From	To	Protocol	Port	Notes
			80	Used to verify the certificate status through the following endpoints: • `ocsp.digicert.com` • `ocsp.msocsp.com` Consider 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. For more details, see also Microsoft documentation.
	Google Cloud storage	TCP	443	Used to communicate with Google Cloud storage through the following endpoints: • `storage.googleapis.com` All cloud endpoints are specified in this Google article.
			80	Used to verify the certificate status through the following endpoints: • `ocsp.pki.goog` • `pki.goog` • `crl.pki.goog` Consider 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.
	IBM Cloud object storage	TCP	Depends on device configuration	Used to communicate with IBM Cloud object storage.
	S3 compatible object storage	TCP	Depends on device configuration	Used to communicate with S3 compatible object storage.
	Veeam Data Cloud Vault storage	TCP	443	Used to communicate with the Veeam Data Cloud Vault storage through the `xxx.blob.core.windows.net` endpoint.

Communication with Cloud Machines

The following table describes network ports that must be opened to ensure proper communication between Veeam Backup & Replication and Veeam Agents installed on Amazon EC2 instances or Microsoft Azure virtual machines (both objects can be also referred to as cloud machines).

From	To	Protocol	Port/Endpoint	Notes
Veeam Backup & Replication, Amazon EC2 instance with Veeam Agent	Amazon cloud	TCP	443	Port and endpoints used for communication from Veeam Backup & Replication and Amazon EC2 instance to the Amazon cloud where the instance is located.
		HTTPS	**AWS service endpoints:** • *.amazonaws.com (for *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	
		TCP	443	

From	To	Protocol	Port/Endpoint	Notes
Veeam Backup & Replication, Microsoft Azure virtual machine with Veeam Agent	Microsoft Azure cloud	HTTPS	**Global region endpoints:** • management.core.windows.net • xxx.blob.core.windows.net • xxx.queue.core.windows.net • core.windows.net **China region endpoints:** • management.core.chinacloudapi.cn • xxx.blob.core.chinacloudapi.cn • xxx.queue.core.chinacloudapi.cn • core.chinacloudapi.cn **Government region endpoints:** • management.core.usgovcloudapi.net • xxx.blob.core.usgovcloudapi.net • xxx.queue.core.usgovcloudapi.net • core.usgovcloudapi.net	Port and endpoints used for communication from Veeam Backup & Replication and Microsoft Azure virtual machine to the Microsoft Azure cloud where the virtual machine is located. 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.
		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:** • *.digicert.com • *.digicert.cn (for *China* region) • ocsp.msocsp.com	

Communication with 3rd Party Components

The following table describes network ports that must be opened to ensure proper communication between Veeam backup server and 3rd party infrastructure components.

From	To	Protocol	Port	Notes
Backup server	Microsoft Active Directory	TCP UDP	389	LDAP connections.
		TCP	636	LDAPS (Secure LDAP) connections.

From	To	Protocol	Port	Notes
	DNS server with forward/reverse name resolution of all backup servers	UDP	53	Port used for communication with the DNS Server.

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	Requirements and Limitations
Microsoft Active Directory Domain Controllers	The following versions of Microsoft Active Directory Domain Services servers (domain controllers) are supported: • Microsoft Windows Server 2025 • 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	Requirements and Limitations
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 2025 • 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. • 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. For information on the limitations of data base processing, see Backup of Database Systems. System requirements for database processing are listed in the following table.

Specification	Requirements and Limitations
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 5.7 to 9.0 are supported. • Configurations with multiple MySQL installations or instances on the same machine are not supported. • MySQL Cluster versions are not supported.
PostgreSQL	• PostgreSQL database system versions 12 – 17 are supported. • PostgreSQL clusters are not supported.

Supported Veeam Agents

The following table describes what Veeam Agents are supported by the Veeam Backup & Replication 12.3.

Supported functionality	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
Full functionality	6.3	6.3	4.6	4.6	2.3	Veeam Agents of these versions fully support features of Veeam Backup & Replication 12.3.
Upgrade and limited functionality	5.0 - 6.2	5.0 - 6.2	3.0 - 4.5	3.0 - 4.5	1.0.1 - 2.2	Veeam Agents can be used for standard backup and restore operations, but the latest functionality may not be supported. If you want to use the latest functionality, you must upgrade Veeam Agents to the latest versions. To learn more, see Upgrading Veeam Agents.
Upgrade only	4.0	4.0	2.0	2.0 - 2.1	1.0	To start working with Veeam Backup & Replication 12.3, you must upgrade Veeam Agents. To learn more, see Upgrading Veeam Agents.

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. 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 Working with Protection Groups and Managing Protected Computers.

   Make sure to install all available updates for the operating system on the computer you want to protect. Otherwise, the correct functioning of Veeam Agent is not guaranteed.

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 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. To learn more, see Creating Veeam Agent Backup Jobs.

   - Veeam Agent backup job managed by Veeam Agent, or Veeam Agent backup policy. To learn more, see Creating Veeam Agent Backup Policies,

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 Managing Veeam Agent Backup Jobs and Managing Veeam Agent Backup 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, except computers with pre-installed Veeam Agents, to establish a connection to the backup server using the SSH fingerprint. To learn more about computers with pre-installed Veeam Agents, see Deploying Veeam Agents Using Generated Setup Files.

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 **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.

          When you specify a trusted host in the *known_hosts* file, it must follow the same format as the `~/.ssh/known_hosts` file. It must include the network name hash, the type of key, and the public key.

Example of a trusted host entry:

```
|1|y/XiVUB2z/ZBb3vuOYm0x9RUiQA=|9zTpxEaAKbGPe7JyS/OyIWvsTz8= ssh-ed2
5519 AAAAC3NzaC1lZDI1NTE5AAAAIHhO7S1tp0EAgainstjkXSAi4a+JIPKnTUpABC8
BGyWk9
```

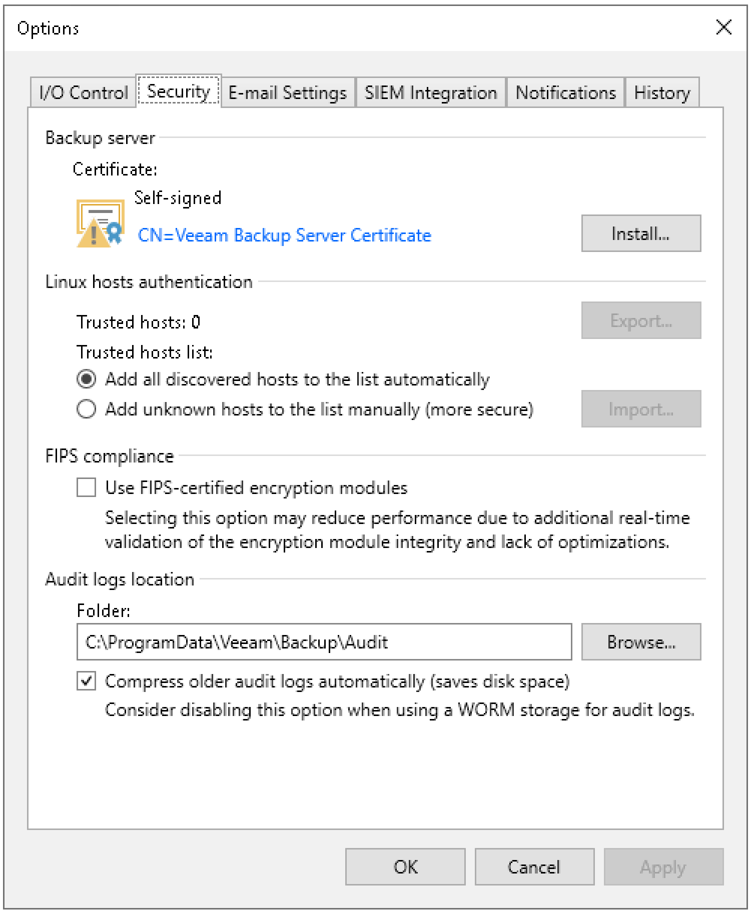
- Protected computers added to the list of trusted hosts in the Veeam Backup & Replication console. To learn more, see Adding Computers to Trusted Hosts List.

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.



Options

I/O Control | Security | E-mail Settings | SIEM Integration | Notifications | History

Backup server

Certificate:

Self-signed

CN=Veeam Backup Server Certificate

Install...

Linux hosts authentication

Trusted hosts: 0

Export...

Trusted hosts list:

● Add all discovered hosts to the list automatically

○ Add unknown hosts to the list manually (more secure)

Import...

FIPS compliance

□ Use FIPS-certified encryption modules

Selecting this option may reduce performance due to additional real-time validation of the encryption module integrity and lack of optimizations.

Audit logs location

Folder:

C:\ProgramData\Veeam\Backup\Audit

Browse...

☑ Compress older audit logs automatically (saves disk space)

Consider disabling this option when using a WORM storage for audit logs.

OK | Cancel | Apply

Managing TLS Certificates

When you configure the Veeam Backup & Replication infrastructure, you can specify what TLS certificate must be used to establish a secure connection from backup infrastructure components to the backup server. Veeam Backup & Replication offers the following options for TLS certificates:

- Keep the default self-signed TLS certificate generated by Veeam Backup & Replication at the process of upgrading to a new version of Veeam Backup & Replication.
- Use Veeam Backup & Replication to generate a new self-signed TLS certificate. To learn more, see Generating Self-Signed Certificates.
- Select an existing TLS certificate from the certificate store. To learn more, see Importing Certificates from Certificate Store.
- Import a TLS certificate from a file in the PFX format. To learn more, see Importing Certificates from PFX Files.

If you plan to use a certificate issued by your own Certificate Authority (CA), make sure that the certificate meets the requirements. For more information, see Using Certificate Signed by Internal CA.

NOTE

Consider the following:

- To avoid potential synchronization issues, make sure that Veeam Agents are synchronized with Veeam Backup & Replication before you change the existing certificate. To learn more, see Rescan Job.
- [For protection groups for pre-installed Veeam Agents] If you change the existing certificate, you must export a new package with setup files to deploy Veeam Agents on new computers that you want to add to the protection group.To learn more, see Specifying Packages.

Generating Self-Signed Certificates

You can use Veeam Backup & Replication to generate a self-signed certificate for authenticating parties in the Veeam Backup & Replication infrastructure.

To generate TLS certificates, Veeam Backup & Replication employs the RSA Full cryptographic service provider by Microsoft Windows installed on the 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 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.

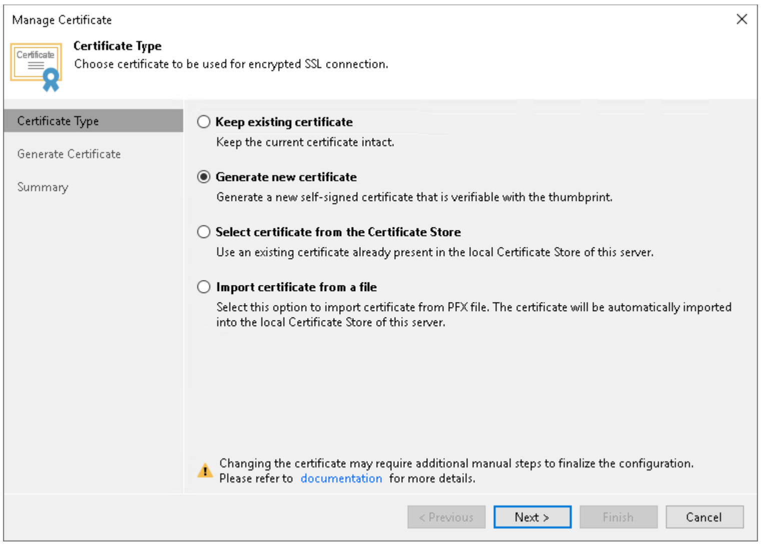
> NOTE
>
> When you generate a self-signed TLS certificate with Veeam Backup & Replication, you cannot include several aliases to the certificate and specify a custom value in the *Subject* field. The *Subject* field value is taken from the Veeam Backup & Replication license installed on the Veeam backup server.

> IMPORTANT
>
> If you update the TLS certificate used on the backup server, you must also update info about the certificate on the specific backup infrastructure components as described in section Managing TLS Certificates.

To generate a self-signed TLS certificate, do the following:

1. From the main menu, select **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**.



Manage Certificate

Certificate Type
Choose certificate to be used for encrypted SSL connection.

○ **Keep existing certificate**
Keep the current certificate intact.

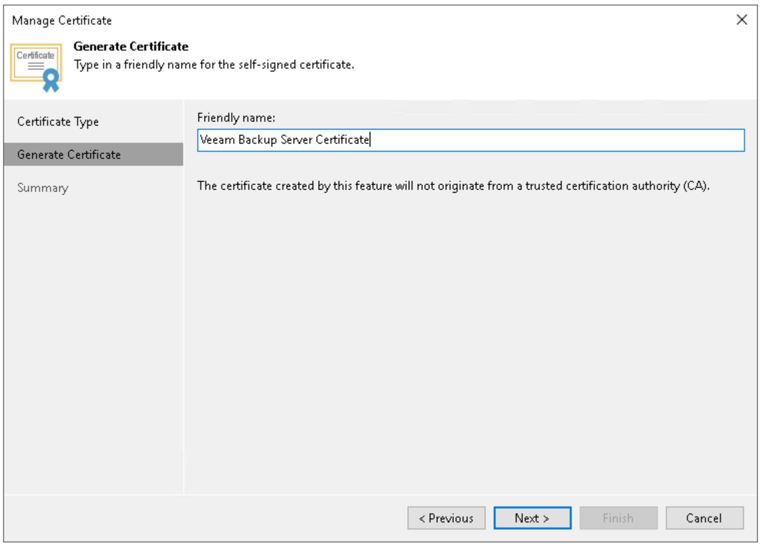
● **Generate new certificate**
Generate a new self-signed certificate that is verifiable with the thumbprint.

○ **Select certificate from the Certificate Store**
Use an existing certificate already present in the local Certificate Store of this server.

○ **Import certificate from a file**
Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server.

Changing the certificate may require additional manual steps to finalize the configuration.
Please refer to documentation for more details.

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



Manage Certificate

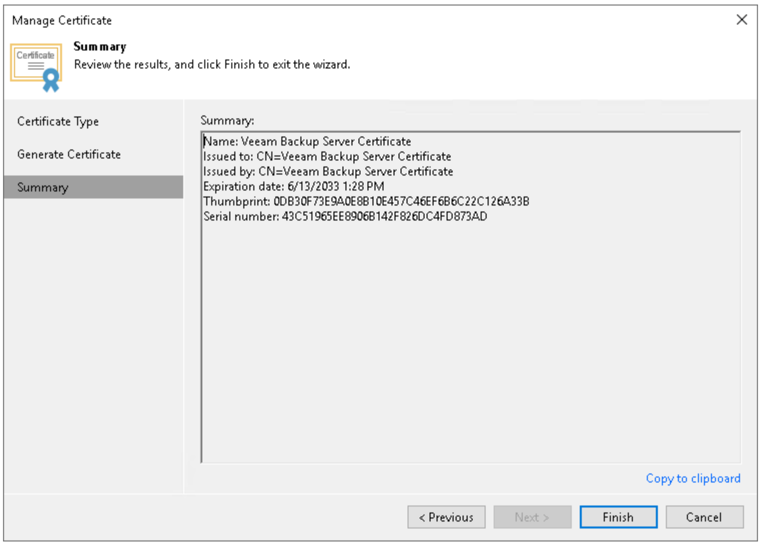
Generate Certificate
Type in a friendly name for the self-signed certificate.

Friendly name: Veeam Backup Server Certificate

The certificate created by this feature will not originate from a trusted certification authority (CA).

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.



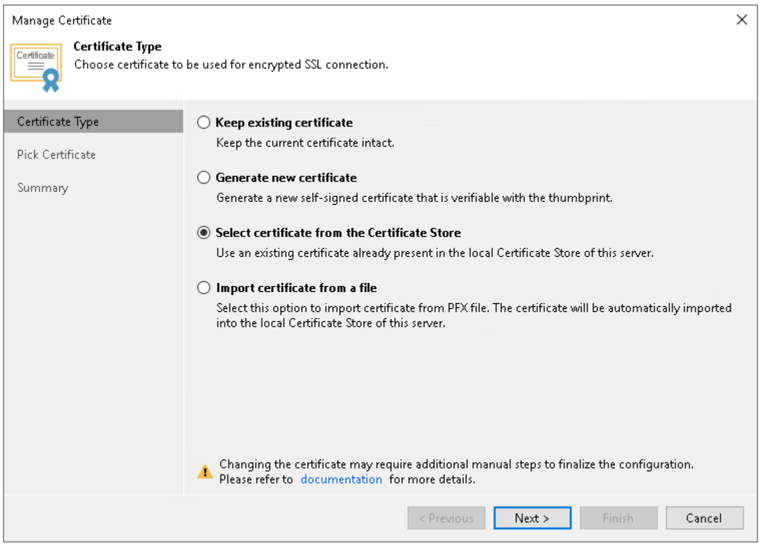
```
Name: Veeam Backup Server Certificate
Issued to: CN=Veeam Backup Server Certificate
Issued by: CN=Veeam Backup Server Certificate
Expiration date: 6/13/2033 1:28 PM
Thumbprint: 0DB30F73E9A0E8B10E457C46EF6B6C22C126A33B
Serial number: 43C51965EE8906B142F826DC4FD873AD
```

Importing Certificates from Certificate Store

If the Veeam backup server has been issued a TLS certificate signed by a CA and the TLS certificate is located in the Microsoft Windows certificate store, you can use this certificate for authenticating parties in the Veeam Backup & Replication infrastructure.

To select a certificate from the Microsoft Windows certificate store, do the following:

1. From the main menu, select **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**.



Manage Certificate

Certificate Type

Choose certificate to be used for encrypted SSL connection.

○ **Keep existing certificate**
Keep the current certificate intact.

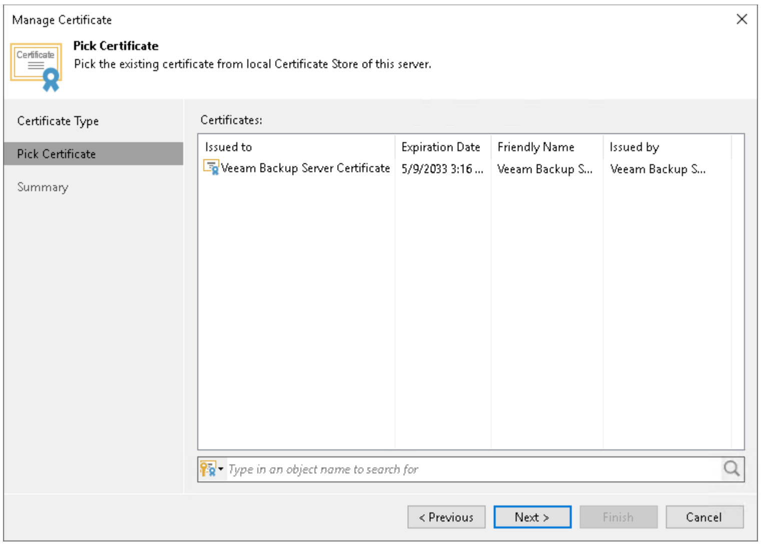
○ **Generate new certificate**
Generate a new self-signed certificate that is verifiable with the thumbprint.

● **Select certificate from the Certificate Store**
Use an existing certificate already present in the local Certificate Store of this server.

○ **Import certificate from a file**
Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server.

Changing the certificate may require additional manual steps to finalize the configuration. Please refer to documentation for more details.

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.



Manage Certificate

Pick Certificate

Pick the existing certificate from local Certificate Store of this server.

Certificates:

Issued to	Expiration Date	Friendly Name	Issued by
Veeam Backup Server Certificate	5/9/2033 3:16 ...	Veeam Backup S...	Veeam Backup S...

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

Importing Certificates from PFX Files

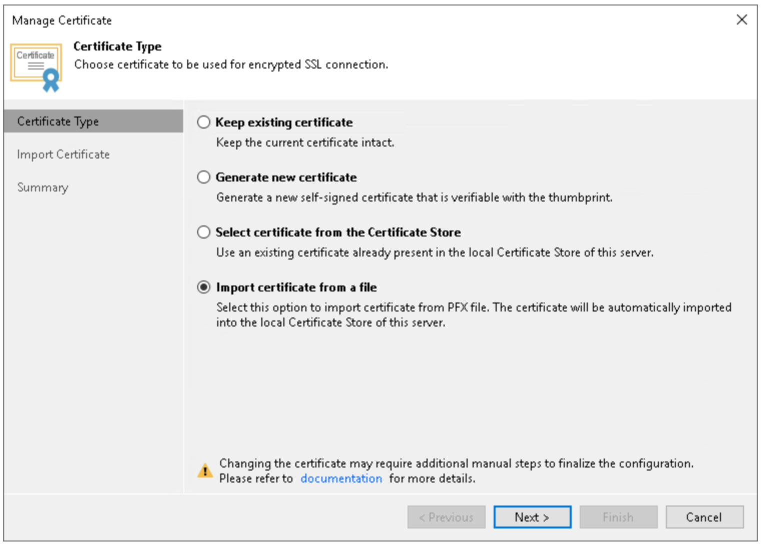
You can import a TLS certificate in the following situations:

- 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.

> NOTE
>
> Consider the following:
>
> - The TLS certificate must pass validation on the Veeam backup server. Otherwise, you will not be able to import the TLS certificate.
> - If a PFX file contains a certificate chain, only the end entity certificate will be imported.

To import a TLS certificate from a PFX file, do the following:

1. From the main menu, select **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**.



Certificate Type

Choose certificate to be used for encrypted SSL connection.

○ **Keep existing certificate**
Keep the current certificate intact.

○ **Generate new certificate**
Generate a new self-signed certificate that is verifiable with the thumbprint.

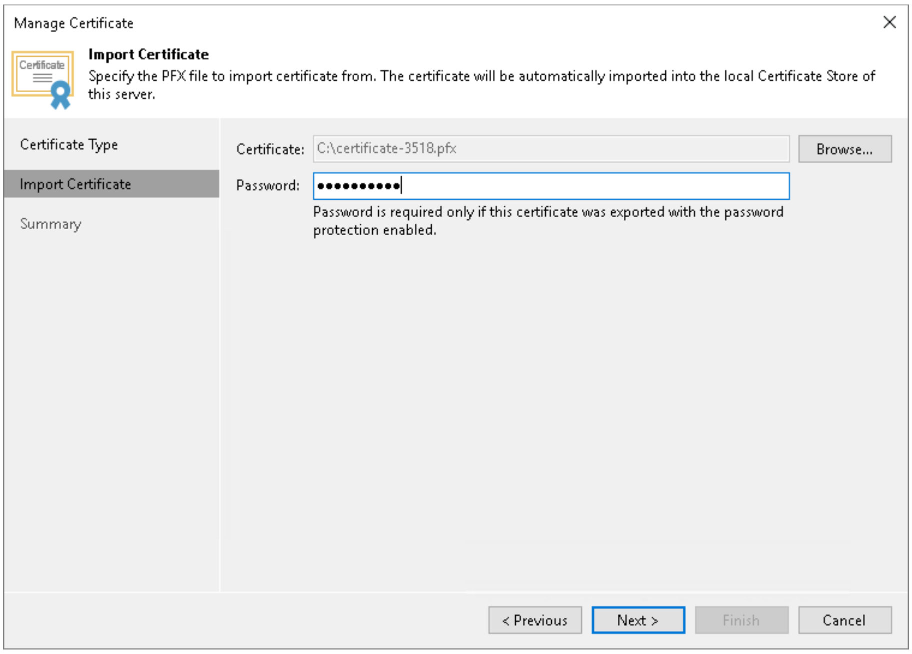
○ **Select certificate from the Certificate Store**
Use an existing certificate already present in the local Certificate Store of this server.

● **Import certificate from a file**
Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server.

⚠ Changing the certificate may require additional manual steps to finalize the configuration. Please refer to documentation for more details.

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

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



Manage Certificate

Import Certificate

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

Certificate: C:\certificate-3518.pfx

Password: ●●●●●●●●●●

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

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

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

Using a Certificate Signed by Internal CA

If you want to use a certificate signed by an internal Certificate Authority (CA), consider the following:

- Make sure that Veeam Backup & Replication server and Veeam Agents trust the CA. That means that the Certification Authority certificate must be added to the Trusted Root Certification Authority store on the Veeam Backup & Replication server. Also, Certificate Revocation List (CRL) must be accessible from the Veeam Backup & Replication server.

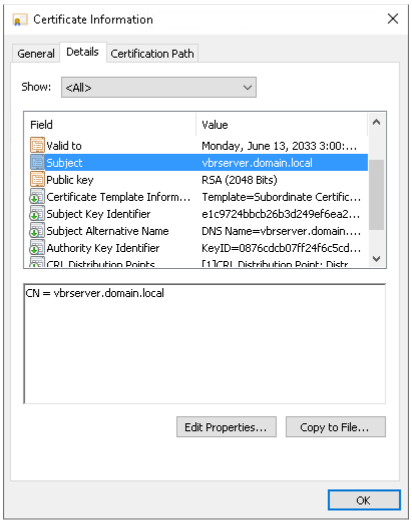
- If you use Windows Server Certification Authority, issue a Veeam Backup & Replication certificate based on the built-in *Subordinate Certification Authority* template or templates similar to it. You can manage templates with the **Certificate Templates** MMC snap-in.

- [For Linux-based Veeam Agent computers] OpenSSL version 1.0 or later must be installed on the Veeam Agent computer.

> **IMPORTANT**
>
> The following certificates are not supported:
>
> - Certificates issued by public CAs
> - Elliptic Curve Signature (ECC) certificates
> - Cryptography API: Next Generation (CNG) certificates

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

- The certificate subject is equal to the fully qualified domain name of the Veeam Backup & Replication server. For example: `vbrserver.domain.local`.



Field	Value
Valid to	Monday, June 13, 2033 3:00:...
Subject	vbrserver.domain.local
Public key	RSA (2048 Bits)
Certificate Template Inform...	Template=Subordinate Certific...
Subject Key Identifier	e1c9724bbcb26b3d249ef6ea2...
Subject Alternative Name	DNS Name=vbrserver.domain....
Authority Key Identifier	KeyID=0876cdcb07ff24f6c5cd...
CRL Distribution Points	[1]CRL Distribution Point: Distr

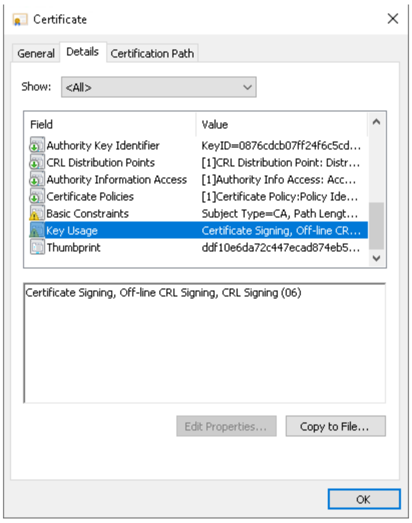
CN = vbrserver.domain.local

- The **Subject Alternative Name** field contains both the FQDN and the NetBIOS name. You can add multiple DNS entries in the following format: `DNS:vbrserver.domain.local,DNS:vbrserver`.

- The minimum key size is 2048 bits.

- The following key usage extensions are enabled in the certificate:
  - Digital Signature
  - Certificate Signing
  - Off-line CRL Signing

- CRL Signing (86)



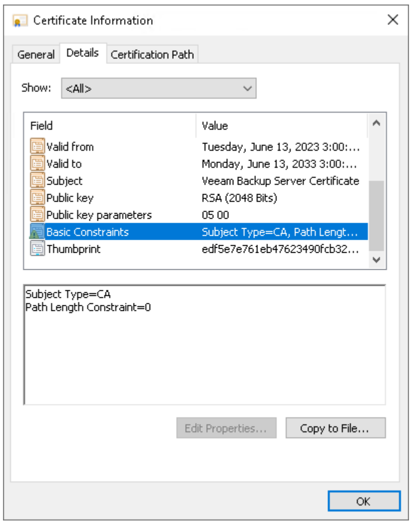
Certificate

Show: <All>

Field	Value
Authority Key Identifier	KeyID=0876cdcb07ff24f6c5cd...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=CA, Path Lengt...
Key Usage	Certificate Signing, Off-line CR...
Thumbprint	ddf10e6da72c447ecad874eb5...

Certificate Signing, Off-line CRL Signing, CRL Signing (06)

- The **Path Length Constraint** parameter in the **Basic Constraints** extension is set to *0*.



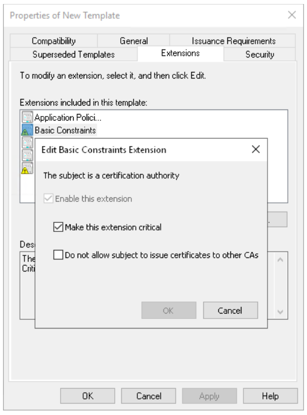
Certificate Information

Show: <All>

Field	Value
Valid from	Tuesday, June 13, 2023 3:00:...
Valid to	Monday, June 13, 2033 3:00:...
Subject	Veeam Backup Server Certificate
Public key	RSA (2048 Bits)
Public key parameters	05 00
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint	edf5e7e761eb47623490fcb32...

Subject Type=CA
Path Length Constraint=0

If you use Windows Server Certification Authority, open the **Certificate Templates** MMC snap-in and select the certificate template based on the built-in *Subordinate Certification Authority* template or templates similar to it. On the **Extensions** tab, enable the **Do not allow subject to issue certificates to other CAs** option.



Properties of New Template

To modify an extension, select it, and then click Edit.

Extensions included in this template:

Application Polici...
Basic Constraints

Edit Basic Constraints Extension

The subject is a certification authority

☑ Enable this extension

☑ Make this extension critical

☐ Do not allow subject to issue certificates to other CAs

- The key type in the certificate is set to *Exchange*.

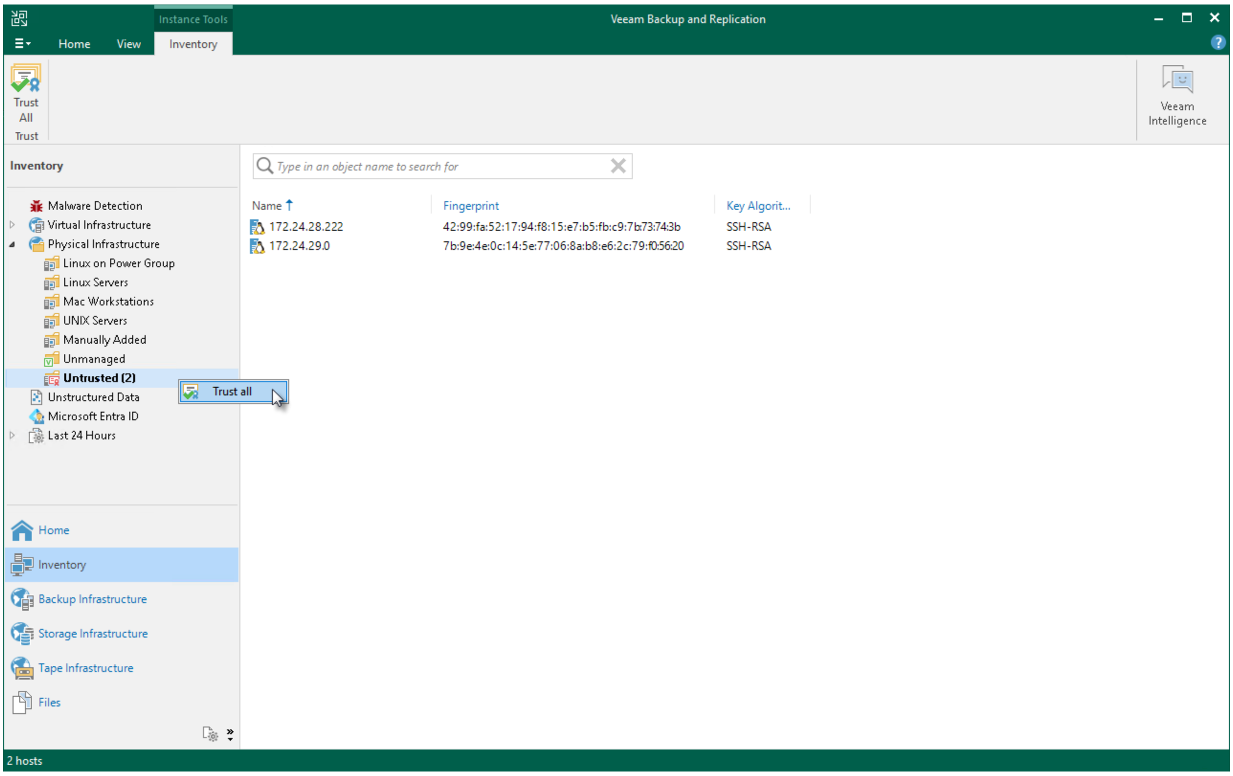
To start using the signed certificate, you must select it from the certificates store on the Veeam Backup & Replication server. To learn more, see Importing Certificates from Certificate Store.

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 computer to the list of trusted hosts in the Veeam Backup & Replication console.

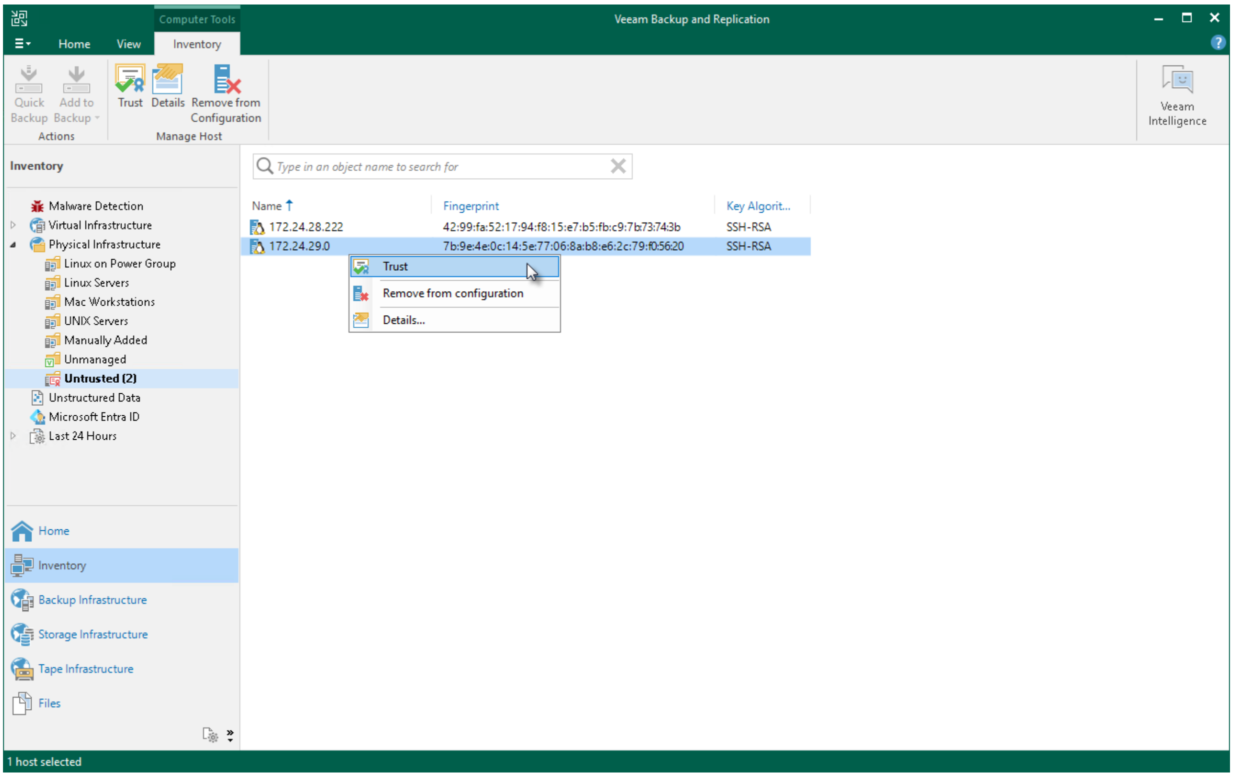
To add a computer to the list of trusted hosts:

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**.



Name	Fingerprint	Key Algorit...
172.24.28.222	42:99:fa:52:17:94:f8:15:e7:b5:fb:c9:7b:73:74:3b	SSH-RSA
172.24.29.0	7b:9e:4e:0c:14:5e:77:06:8a:b8:e6:2c:79:f0:56:20	SSH-RSA

- 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**.



Name	Fingerprint	Key Algorit...
172.24.28.222	42:99:fa:52:17:94:f8:15:e7:b5:fb:c9:7b:73:74:3b	SSH-RSA
172.24.29.0	7b:9e:4e:0c:14:5e:77:06:8a:b8:e6:2c:79:f0:56:20	SSH-RSA

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.

> NOTE
>
> Before you create a protection group, consider the following:
>
> - 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.
>
>   You cannot add a computer from a protection group for pre-installed Veeam Agents to any other protection group.
> - 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.

You can create protection groups of the following types:

> IMPORTANT
>
> The current guide does not cover subjects related to protection groups that include applications. To learn about this protection group type, see the Creating Protection Group for MongoDB Deployments section in the Veeam Plug-ins for Enterprise Applications Guide.

- Individual computers — create a protection group for these objects 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.
- Microsoft Active Directory objects — create a protection group for these objects 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 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.

  > NOTE
  >
  > You can add a failover cluster only to a protection group that includes Microsoft Active Directory objects.

- Computers from CSV file — create a protection group for these objects if you want to add to the protection scope computers listed in a CSV or TXT file that resides in a local folder on the backup server or in an SMB 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 the 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.
- Computers with pre-installed backup agents — create a protection group for these objects 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 temporary certificate to connect to the Veeam backup server. A temporary certificate 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.

  The **Computers with pre-installed backup agents** option is the only applicable option for the following objects: Mac computers with pre-installed Veeam Agent for Mac and Linux computers with pre-installed Veeam Agent for Linux on Power.

  > IMPORTANT
  >
  > Make sure that the setup and configuration files are stored in a secure place. If a third-party uncovers the files, they can use any host to connect to the protection group, receive the configuration options, create backups and perform other actions.

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

- Cloud machines — create a protection group for these objects 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.

Creating Protection Group for Individual Computers

Before you create a protection group for individual computers, check prerequisites. Then use the **New Protection Group** wizard to configure a protection group.

1. Launch the New Protection Group wizard.
2. Specify protection group name and description.
3. Specify computers.
4. Specify discovery and deployment options.
5. Specify advanced protection group settings.
6. Review components.
7. Assess results.
8. Finish working with the wizard.

Before You Begin

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

- 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.
- We recommend 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.
- We recommend 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.
- 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.

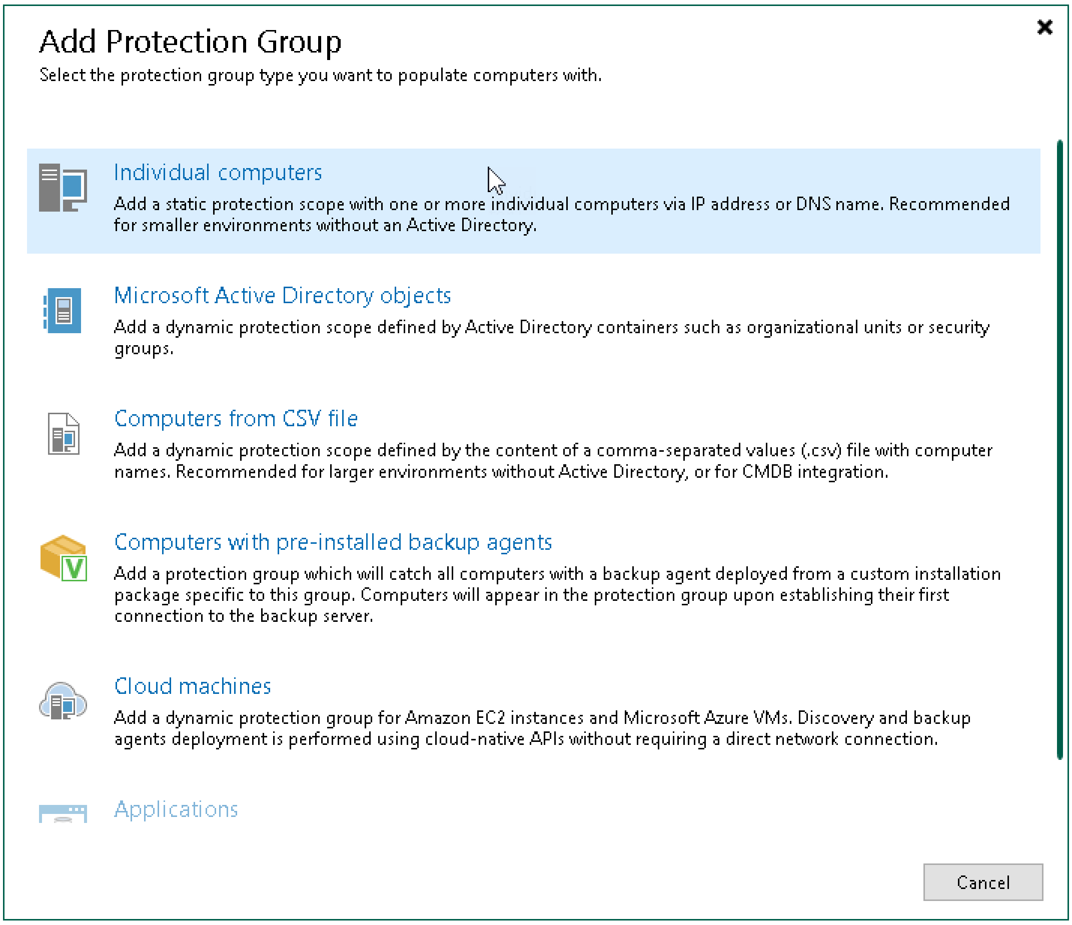
  Note that in client Microsoft Windows OSes access to the administrative share is forbidden by default for local accounts. You can enable this option with a registry key. To learn more, see this Microsoft KB article.
- Veeam Backup & Replication does not support usage of a Linux account for which system 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.

- To connect to the Linux-based computer where you want to install Veeam Agent for Linux, you must specify the user account that has a home directory. The specified user account must also have the read and write permissions for their home directory.
    - You must not install Veeam Agent on the server that is used as a hardened repository in the Veeam Backup & Replication infrastructure.

Step 1. Launch New Protection Group Wizard

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

1. Open the Add Protection Group window. To open the window, 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**.
2. In the **Add Protection Group** window, select the **Individual computers** option.



Add Protection Group

Select the protection group type you want to populate computers with.

Individual computers

Add a static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

Microsoft Active Directory objects

Add a dynamic protection scope defined by Active Directory containers such as organizational units or security groups.

Computers from CSV file

Add a dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names. Recommended for larger environments without Active Directory, or for CMDB integration.

Computers with pre-installed backup agents

Add a protection group which will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

Cloud machines

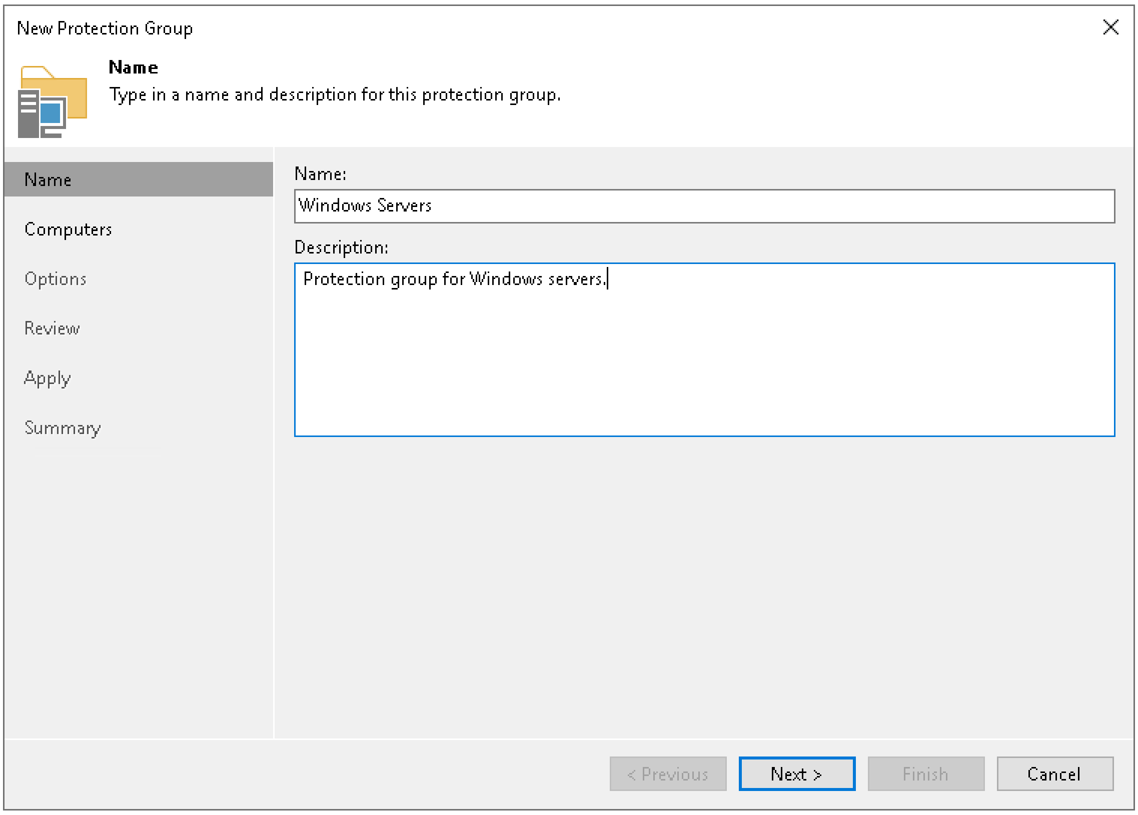
Add a dynamic protection group for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

Applications

Step 2. Specify Protection Group Name and Description

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

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



New Protection Group

Name

Type in a name and description for this protection group.

Name:

Windows Servers

Description:

Protection group for Windows servers.

Step 3. Specify Computers

At the **Computers** 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. Select a method to connect to the computer:
   - **Connect using admin credentials**. In this case, 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.

     You can add the following types of credentials:

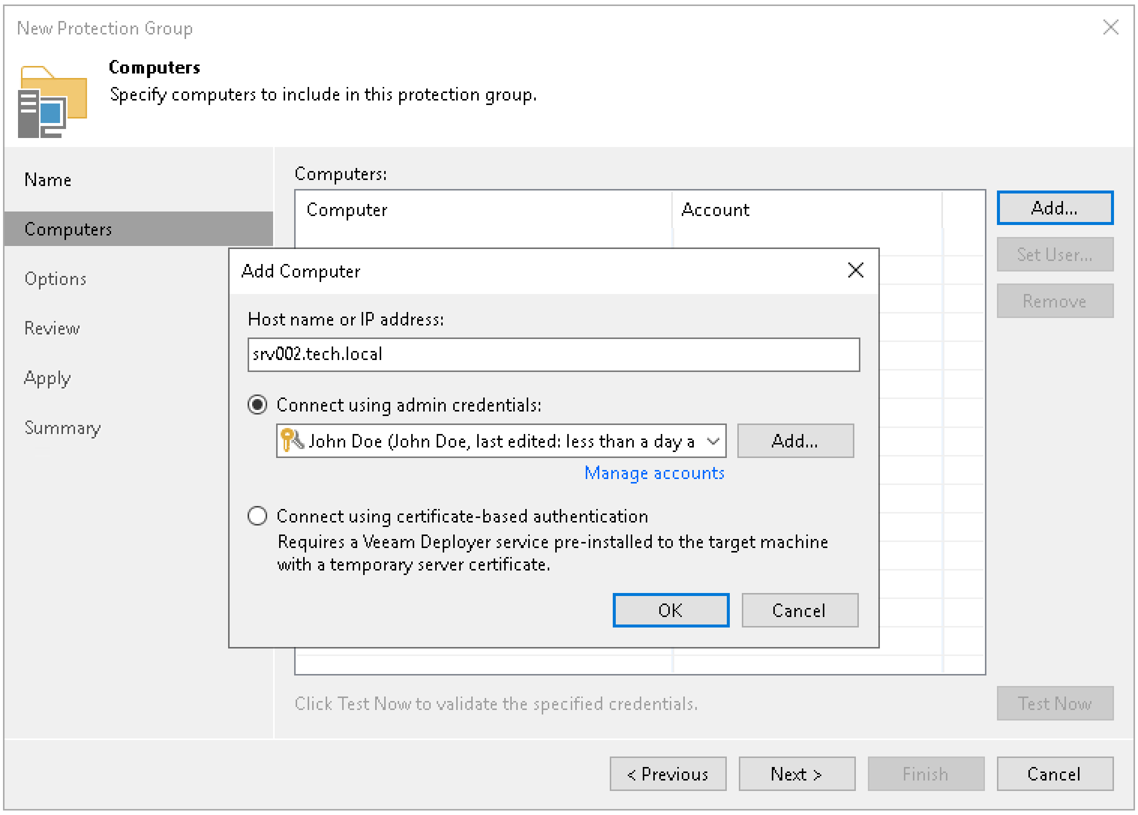
     - Stored credentials. Select stored credentials if you want Veeam Backup & Replication to use the specified user name and password for each connection to Veeam Agent.
     - [For Linux computers] Single-use credentials. Select single-use credentials if you do not want Veeam Backup & Replication to store credentials in the configuration database. With this option selected, Veeam Backup & Replication will use the specified user name and password to deploy Veeam components. After the components are successfully deployed, 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.
   - [For Linux computers] **Connect using certificate-based authentication**. Select this option, if you chose to pre-install Veeam Deployer Service on the Linux computer that you want to add to the protection group. In this case, Veeam Backup & Replication will communicate with the Linux computer using a certificate. Veeam Backup & Replication will install Transport Service that will be used to perform the necessary operations on the computer: upload and install Veeam Agent, and so on. To learn more, see Deploying Veeam Agent for Linux Using Pre-Installed Veeam Deployer Service.
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 method 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.



New Protection Group

Computers

Specify computers to include in this protection group.

Add Computer

Host name or IP address: srv002.tech.local

● Connect using admin credentials: John Doe (John Doe, last edited: less than a day a

○ Connect using certificate-based authentication

Requires a Veeam Deployer service pre-installed to the target machine with a temporary server certificate.

Click Test Now to validate the specified credentials.

Step 4. Specify Discovery and Deployment Options

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

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

To specify discovery and deployment options:

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

   - 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, 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.

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 and Veeam Transport 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. If Veeam Transport Service is already installed on a computer, Veeam Backup & Replication checks its version and upgrade Veeam Transport Service if a later version is available.

> IMPORTANT
>
> Automatic installation of nonsnap Veeam Agent for Linux is not available. If you want to add a computer with nonsnap Veeam Agent for Linux to a protection group, you must deploy Veeam Agent on the protected computer first. For more information on standalone installation of nonsnap Veeam Agent for Linux, see the Installation and Configuration section of the Veeam Agent for Linux User Guide.

> 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 Veeam Backup & Replication server, in the **Deployment** section, make sure that the **Auto-update backup agents and plug-ins** check box is selected.

   > IMPORTANT
   >
   > Automatic upgrade of nosnap Veeam Agent for Linux is not available. You must upgrade such Veeam Agents on the protected computer side, manually or using third-party tools.

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.

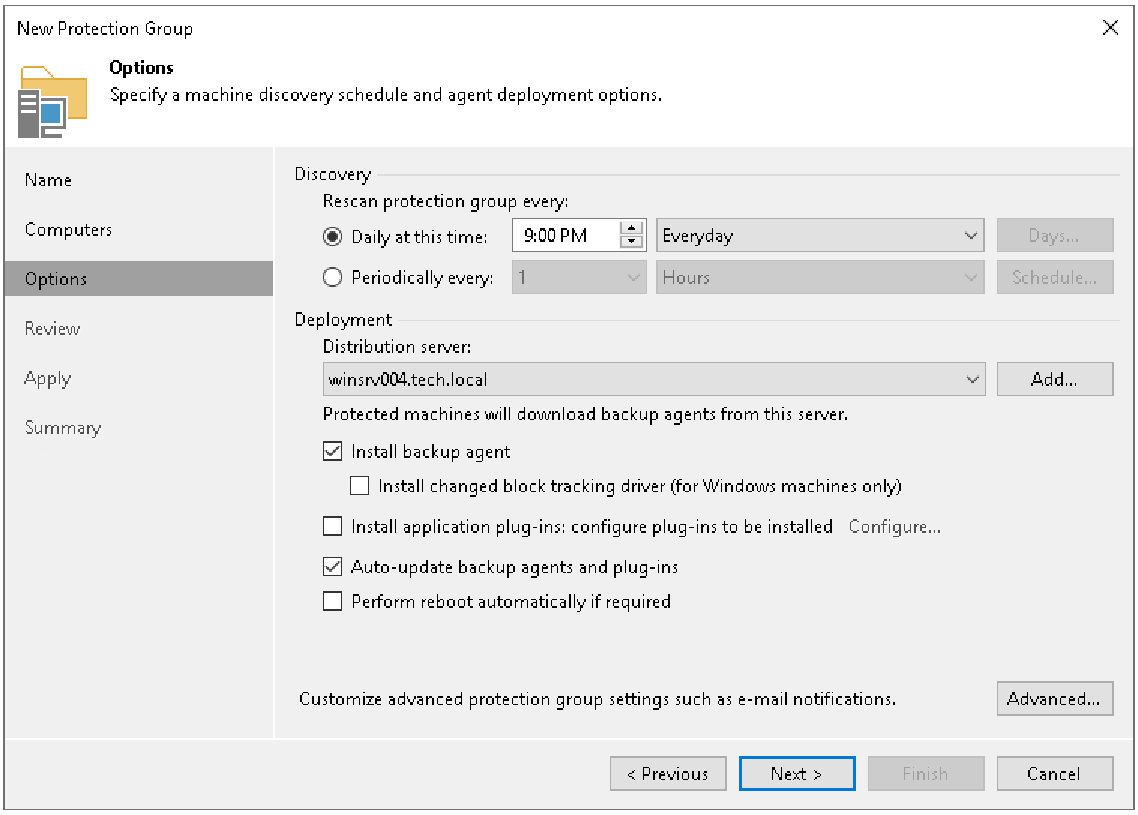
   Keep in mind that Veeam Backup & Replication will install the CBT driver only on those computers that run supported Microsoft Windows OS versions.

   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.



New Protection Group

Options

Specify a machine discovery schedule and agent deployment options.

Discovery

Rescan protection group every:

● Daily at this time: 9:00 PM Everyday Days...

○ Periodically every: 1 Hours Schedule...

Deployment

Distribution server:

winsrv004.tech.local Add...

Protected machines will download backup agents from this server.

☑ Install backup agent

□ Install changed block tracking driver (for Windows machines only)

□ Install application plug-ins: configure plug-ins to be installed Configure...

☑ Auto-update backup agents and plug-ins

□ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications. Advanced...

Step 5. 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
   >
   > Consider 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.

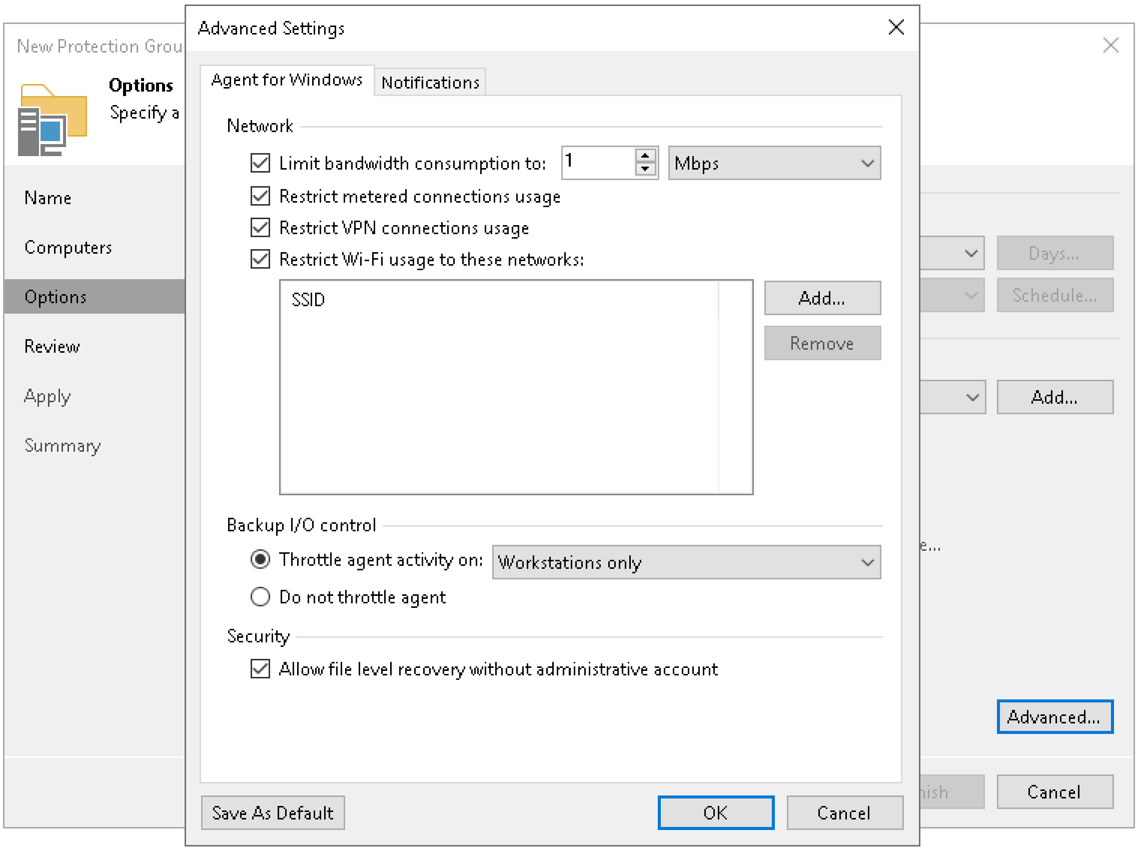
6. If you want to throttle Veeam Agent activities during backup, in the **Backup I/O control** section, make sure that the **Throttle agent activity on** option is selected. Then select the type of computers on which to throttle Veeam Agent backup activities: *Workstations only*, *Servers only* or *All 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 Restoring Files from Backup without Administrator Privileges.


Advanced Settings

Network

☑ Limit bandwidth consumption to: 1 Mbps

☑ Restrict metered connections usage

☑ Restrict VPN connections usage

☑ Restrict Wi-Fi usage to these networks:

SSID

Backup I/O control

● Throttle agent activity on: Workstations only

○ Do not throttle agent

Security

☑ Allow file level recovery without administrative account

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.

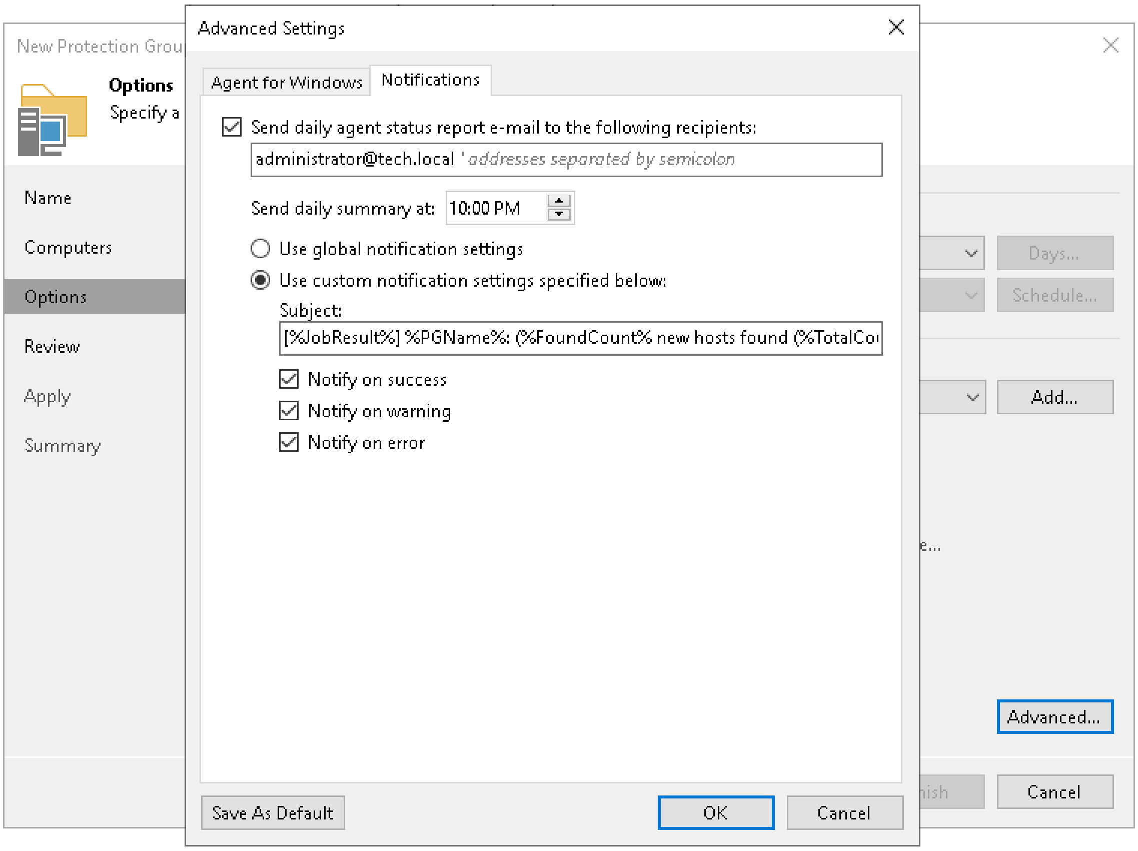
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the daily email report for the protection group.

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 **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.



Advanced Settings

Agent for Windows | Notifications

☑ Send daily agent status report e-mail to the following recipients:

administrator@tech.local ' *addresses separated by semicolon*

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success

☑ Notify on warning

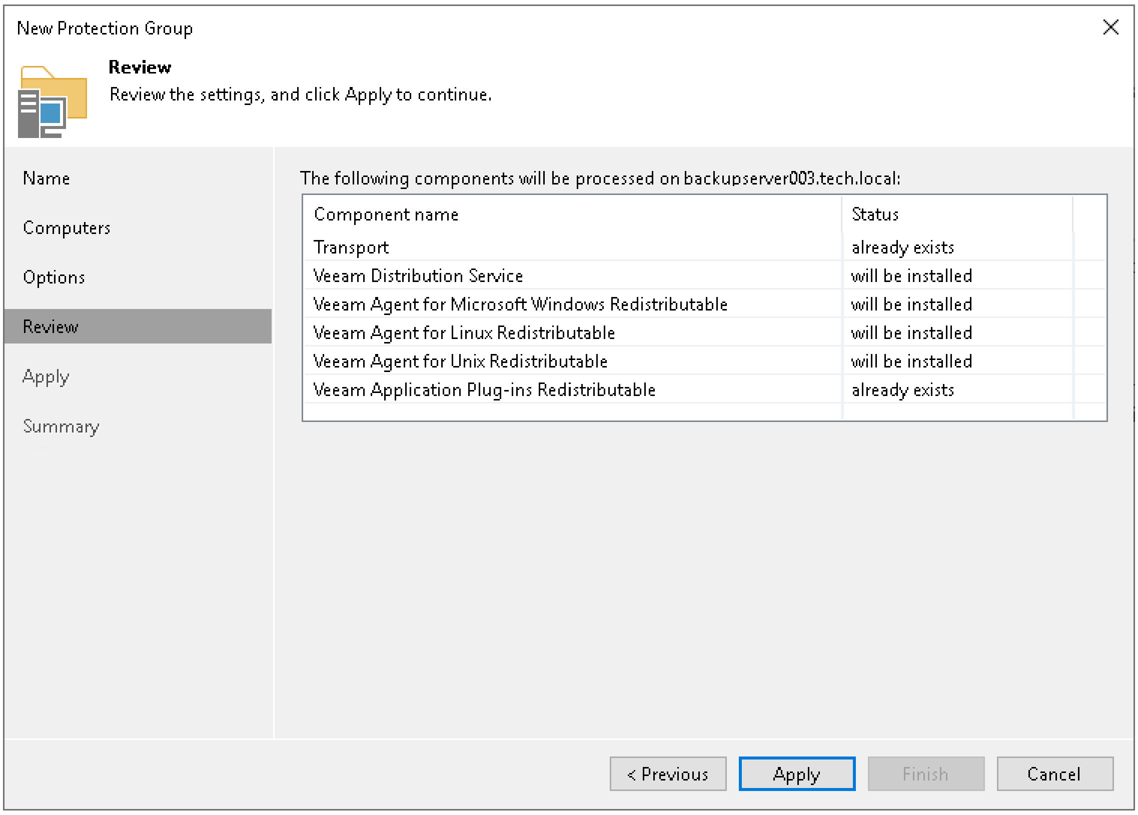
☑ Notify on error

Step 6. Review Components

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

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

> **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.

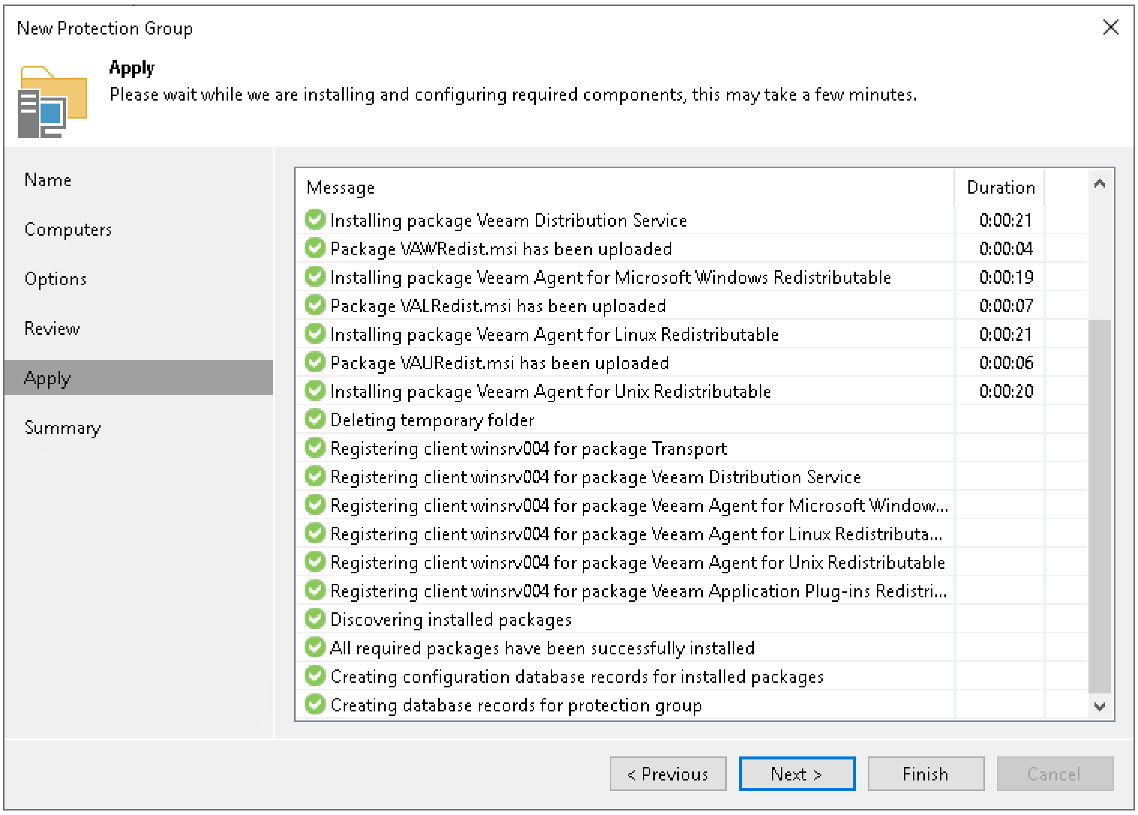


The following components will be processed on backupserver003.tech.local:

Component name	Status
Transport	already exists
Veeam Distribution Service	will be installed
Veeam Agent for Microsoft Windows Redistributable	will be installed
Veeam Agent for Linux Redistributable	will be installed
Veeam Agent for Unix Redistributable	will be installed
Veeam Application Plug-ins Redistributable	already exists

Step 7. 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.



New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

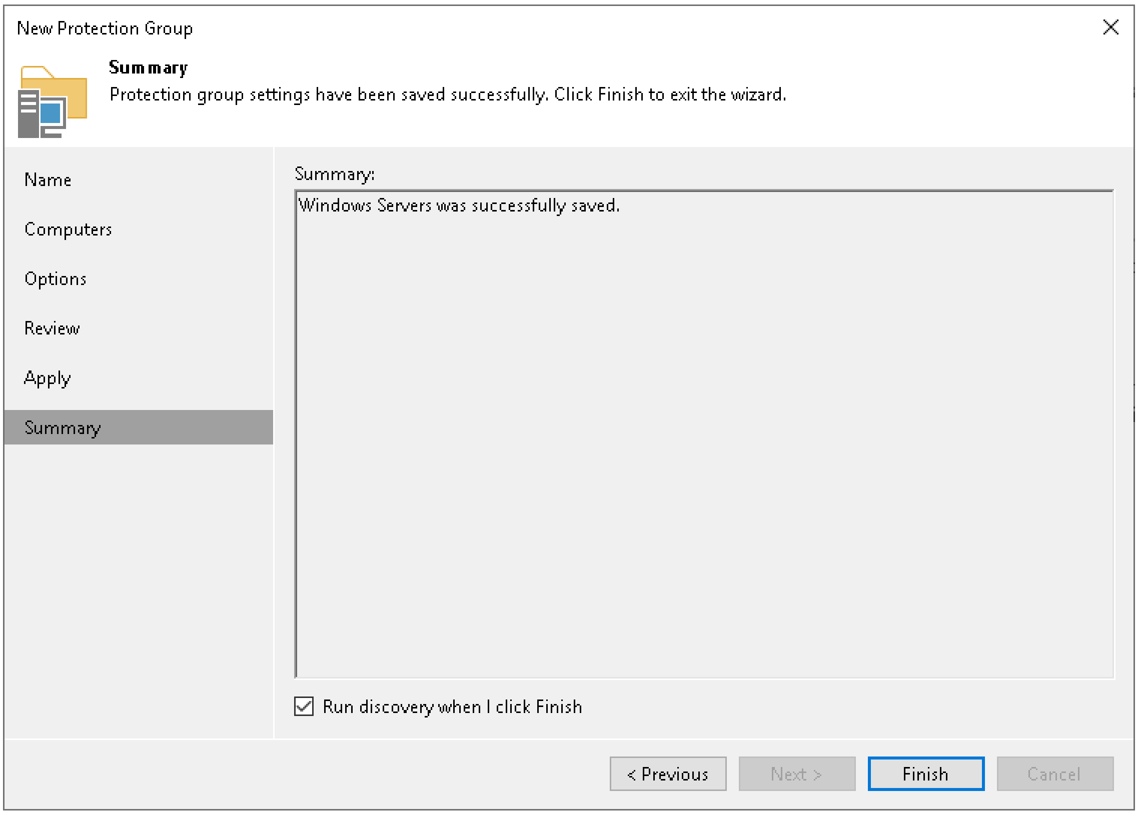
Message	Duration
✓ Installing package Veeam Distribution Service	0:00:21
✓ Package VAWRedist.msi has been uploaded	0:00:04
✓ Installing package Veeam Agent for Microsoft Windows Redistributable	0:00:19
✓ Package VALRedist.msi has been uploaded	0:00:07
✓ Installing package Veeam Agent for Linux Redistributable	0:00:21
✓ Package VAURedist.msi has been uploaded	0:00:06
✓ Installing package Veeam Agent for Unix Redistributable	0:00:20
✓ Deleting temporary folder	
✓ Registering client winsrv004 for package Transport	
✓ Registering client winsrv004 for package Veeam Distribution Service	
✓ Registering client winsrv004 for package Veeam Agent for Microsoft Window...	
✓ Registering client winsrv004 for package Veeam Agent for Linux Redistributa...	
✓ Registering client winsrv004 for package Veeam Agent for Unix Redistributable	
✓ Registering client winsrv004 for package Veeam Application Plug-ins Redistri...	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating configuration database records for installed packages	
✓ Creating database records for protection group	

Step 8. 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**.



Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:

Windows Servers was successfully saved.

☑ Run discovery when I click Finish

Creating Protection Group for Microsoft Active Directory Objects

Before you create a protection group for Microsoft Active Directory objects, check prerequisites. Then use the **New Protection Group** wizard to configure a protection group.

1. Launch the New Protection Group wizard.
2. Specify protection group name and description.
3. Specify Active Directory objects.
4. Exclude objects from the protection group.
5. Specify credentials.
6. Specify discovery and deployment options.
7. Specify advanced protection group settings.
8. Review components.
9. Assess results.
10. Finish working with the wizard.

Before You Begin

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

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

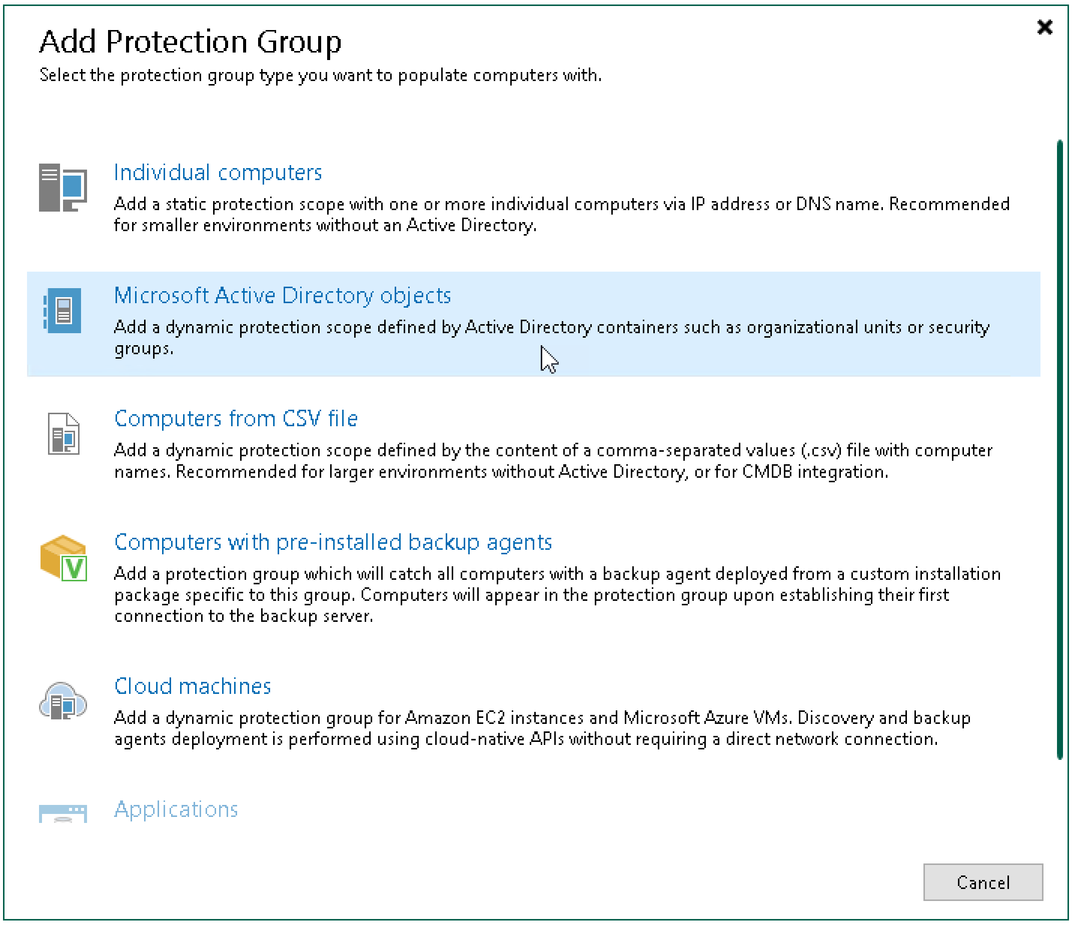
- To deploy Veeam Installer Service and Veeam Agent for Microsoft Windows on a protected computer, Veeam Backup & Replication uses the administrative share (admin$) of the target computer. An account that you plan to use to connect to a computer included in the protection group must have access to the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

  Keep in mind 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. To learn more, see this Microsoft KB article.

Step 1. Launch New Protection Group Wizard

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

1. Open the Add Protection Group window. To open the window, 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**.
2. In the **Add Protection Group** window, select the **Microsoft Active Directory objects** option.



Add Protection Group

Select the protection group type you want to populate computers with.

Individual computers

Add a static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

Microsoft Active Directory objects

Add a dynamic protection scope defined by Active Directory containers such as organizational units or security groups.

Computers from CSV file

Add a dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names. Recommended for larger environments without Active Directory, or for CMDB integration.

Computers with pre-installed backup agents

Add a protection group which will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

Cloud machines

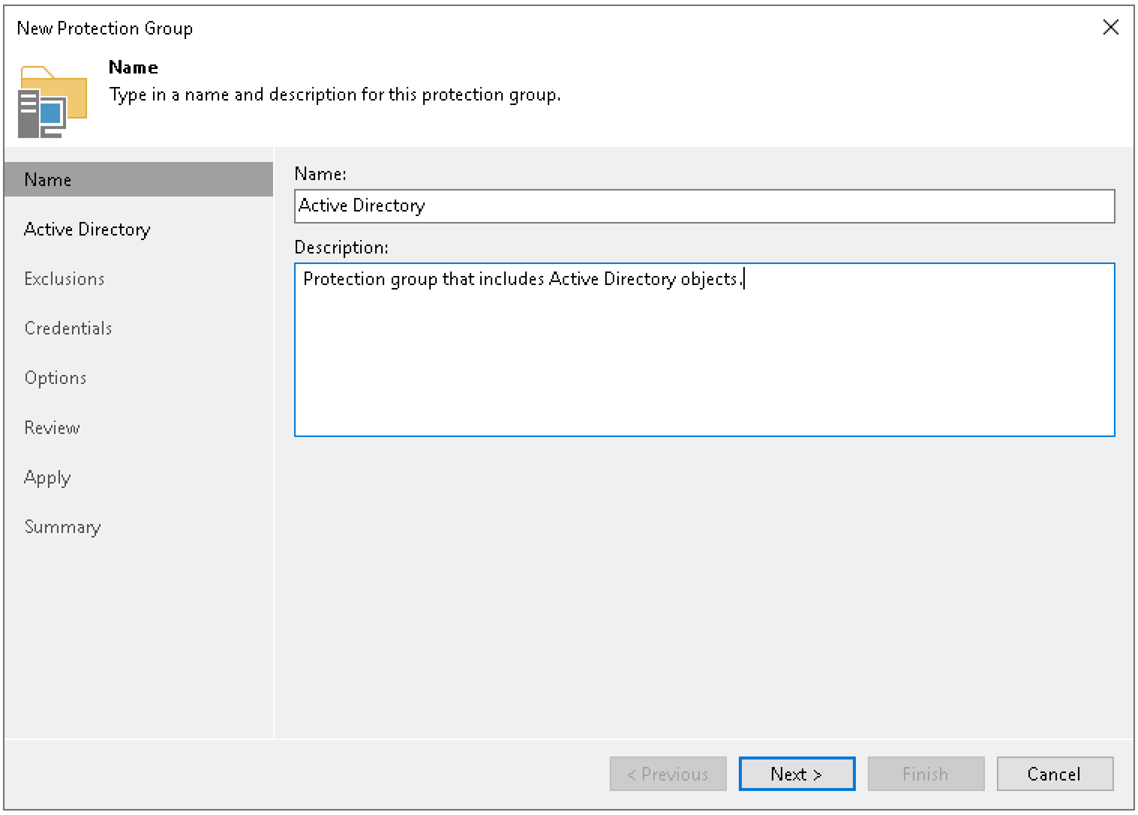
Add a dynamic protection group for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

Applications

Step 2. Specify Protection Group Name and Description

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

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



New Protection Group

Name

Type in a name and description for this protection group.

Name: Active Directory

Description: Protection group that includes Active Directory objects.

Step 3. Specify Active Directory Objects

At the **Active Directory** 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 Creating Protection Group for Computers from CSV File.

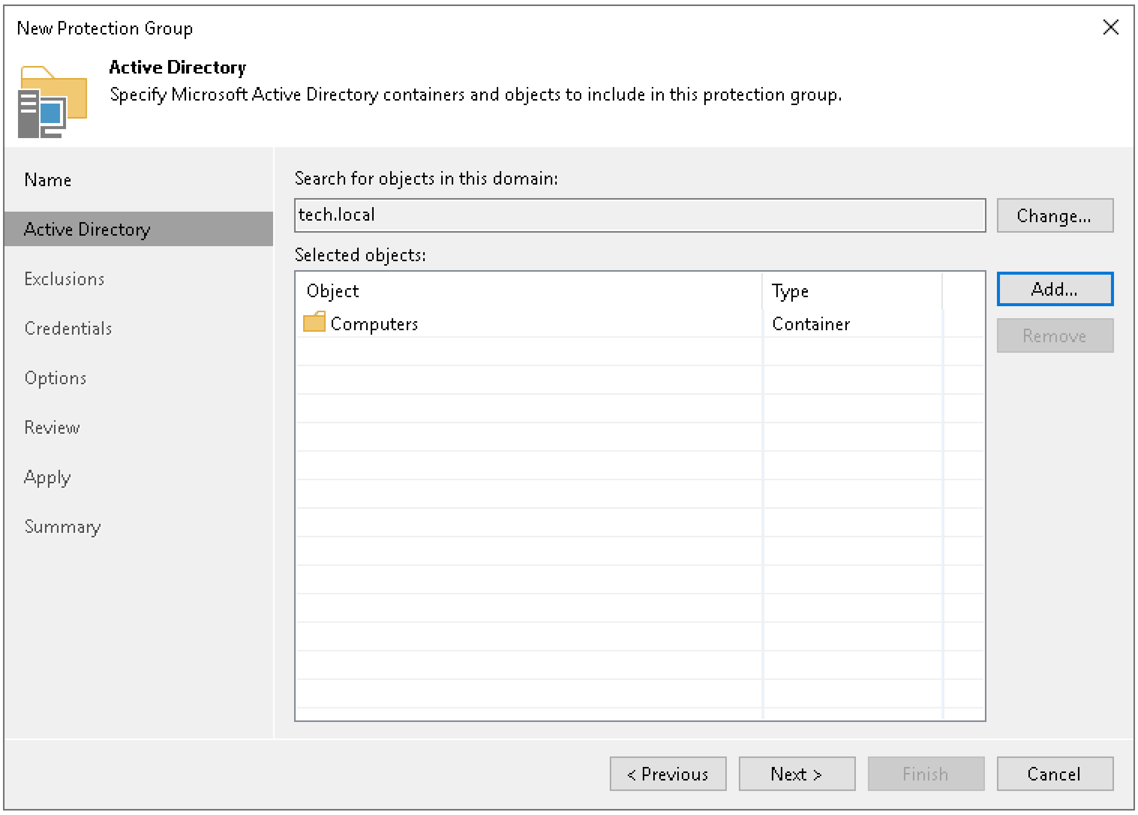
3. In the **Selected objects** field, click **Add**.
4. In the **Add Objects** window, select the necessary Active Directory object in the tree and click **OK**. You can press and hold the [Ctrl] key to select multiple objects at once.

   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].



New Protection Group

Active Directory

Specify Microsoft Active Directory containers and objects to include in this protection group.

Search for objects in this domain: tech.local

Selected objects:

Object	Type
Computers	Container

Step 4. Exclude Objects from Protection Group

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

- All virtual machines — all VMs residing in the domain. You can select this option, for example, if you do not want to protect VMs with Veeam Agents and want to back up VM data with Veeam Backup & Replication instead.
- All computers that have been offline for over 30 days — all computers in the domain that have not logged on to Active Directory for more than 30 days.
- Specific Active Directory objects: computers, failover clusters, groups, organizational units and containers.

Excluding Individual Active Directory Objects

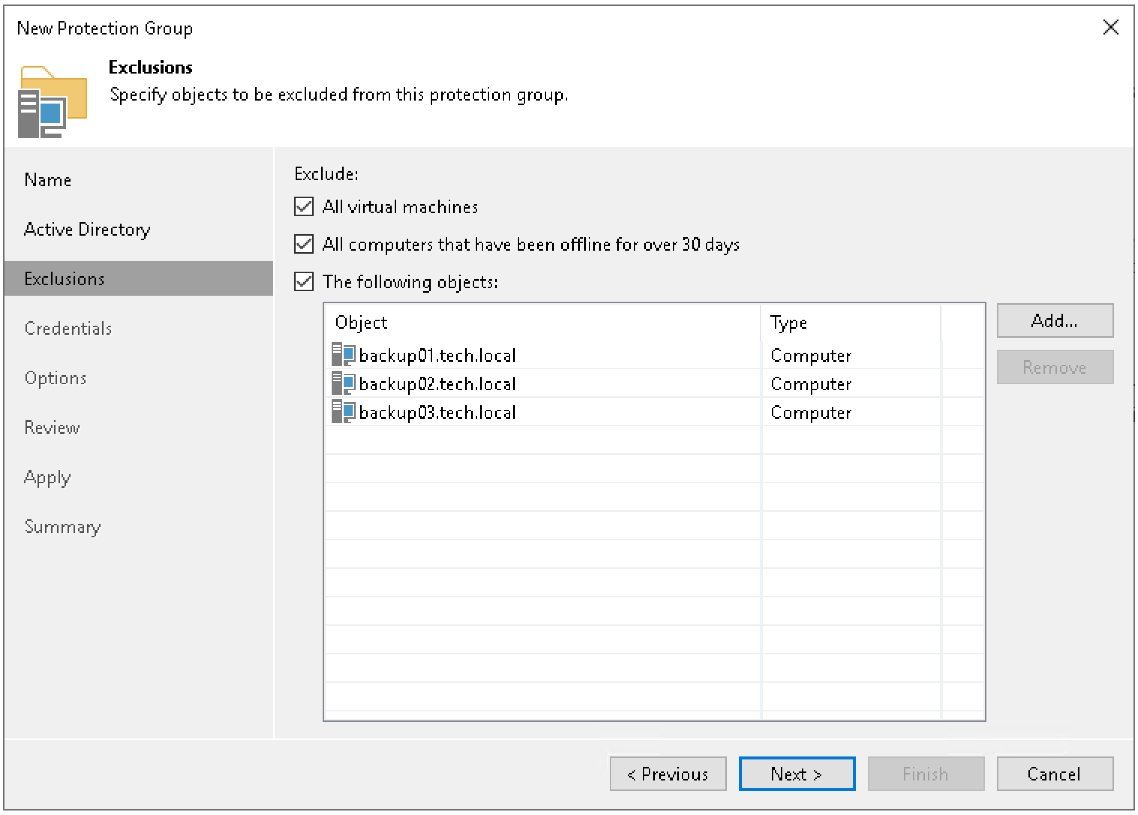
To exclude Active Directory objects:

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 the [Ctrl] key 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].



New Protection Group

Exclusions

Specify objects to be excluded from this protection group.

Exclude:

☑ All virtual machines

☑ All computers that have been offline for over 30 days

☑ The following objects:

Object	Type
backup01.tech.local	Computer
backup02.tech.local	Computer
backup03.tech.local	Computer

Step 5. Specify Credentials

At the **Credentials** 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.

   Select stored credentials if you want Veeam Backup & Replication to use the specified user name and password for each connection to Veeam Agent.

   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.

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.

   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:

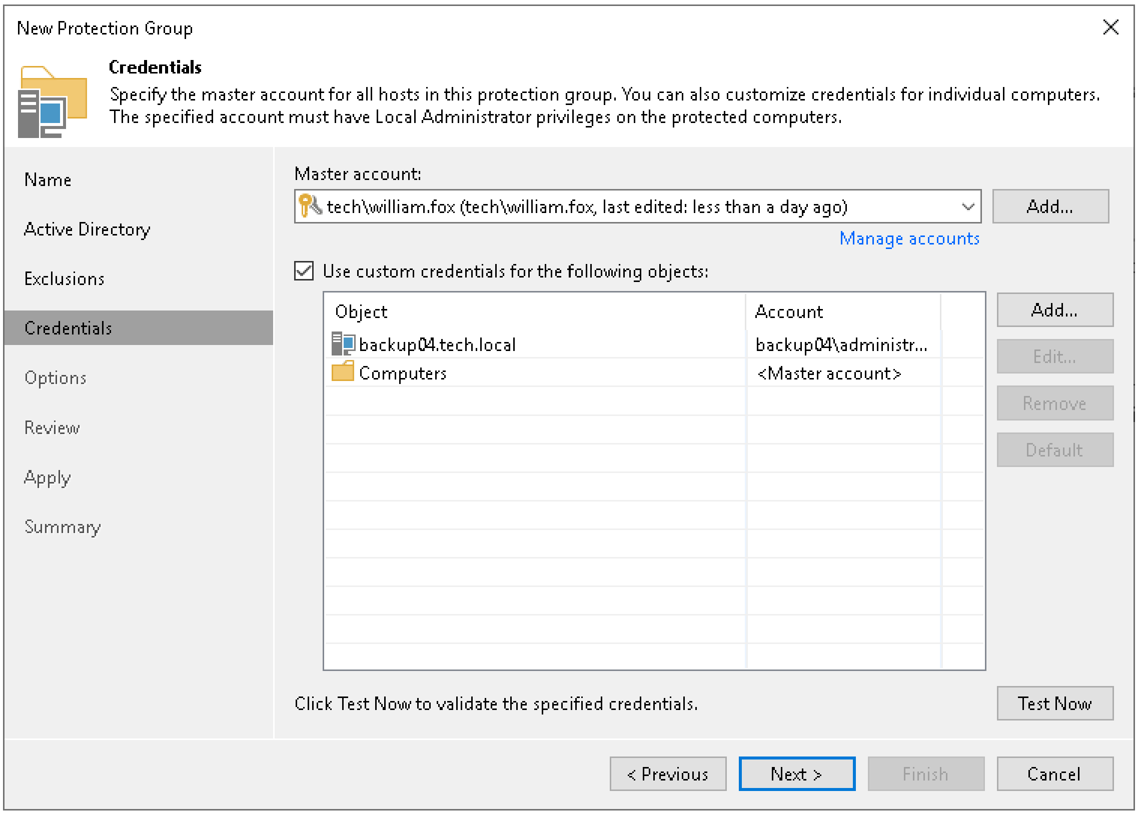
      - For Active Directory accounts — *DOMAIN\Username*
      - For local accounts — *Username* or *HOST\Username*

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.
- 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.
- You cannot use an Azure Active Directory account to connect to computers included in the protection 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.



New Protection Group

Credentials

Specify the master account for all hosts in this protection group. You can also customize credentials for individual computers. The specified account must have Local Administrator privileges on the protected computers.

Master account: tech\william.fox (tech\william.fox, last edited: less than a day ago)

☑ Use custom credentials for the following objects:

Object	Account
backup04.tech.local	backup04\administr...
Computers	<Master account>

Click Test Now to validate the specified credentials.

Step 6. Specify Discovery and Deployment Options

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

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

To specify discovery and deployment options:

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

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 and Veeam Transport 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. If Veeam Transport Service is already installed on a computer, Veeam Backup & Replication checks its version and upgrade Veeam Transport Service if a later version is available.

    > 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 Veeam Backup & Replication server, in the **Deployment** section, make sure that the **Auto-update backup agents and plug-ins** check box is selected.

5. 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.

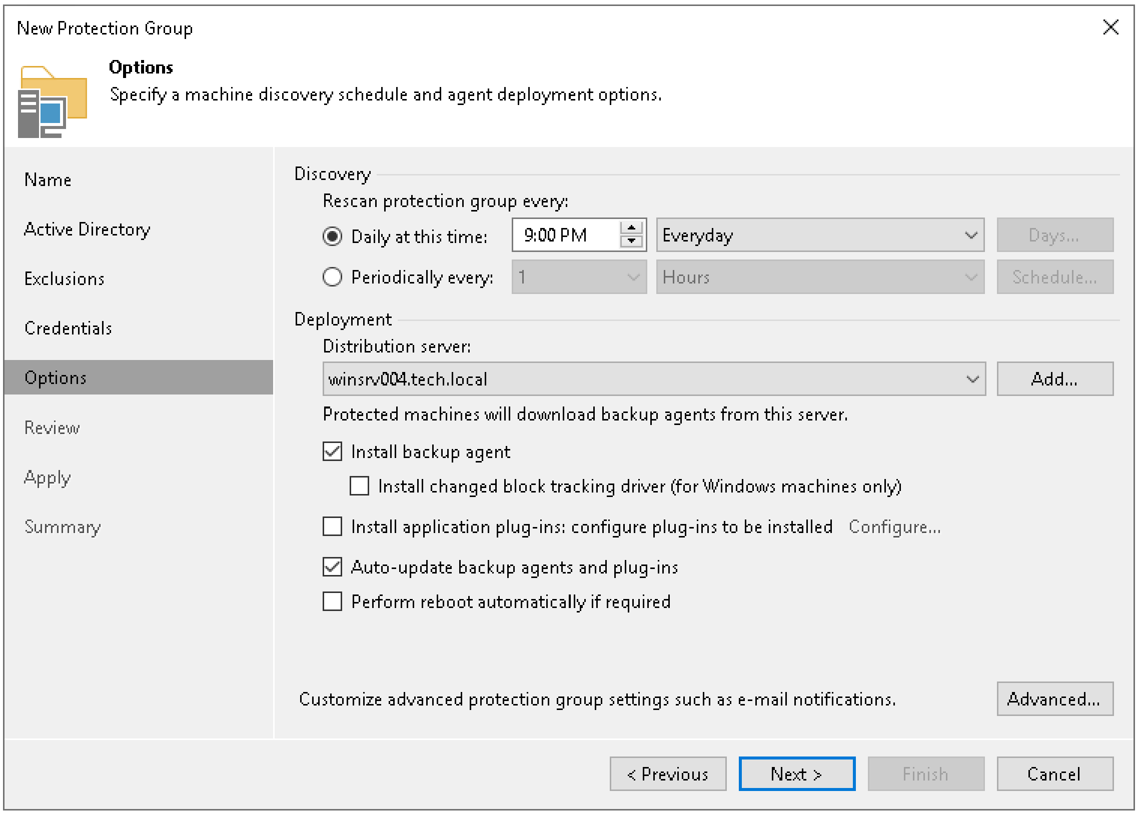
   Keep in mind that Veeam Backup & Replication will install the CBT driver only on those computers that run supported Microsoft Windows OS versions.

   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.



New Protection Group

Options

Specify a machine discovery schedule and agent deployment options.

Discovery

Rescan protection group every:

● Daily at this time: 9:00 PM | Everyday | Days...

○ Periodically every: 1 | Hours | Schedule...

Deployment

Distribution server: winsrv004.tech.local | Add...

Protected machines will download backup agents from this server.

☑ Install backup agent

□ Install changed block tracking driver (for Windows machines only)

□ Install application plug-ins: configure plug-ins to be installed Configure...

☑ Auto-update backup agents and plug-ins

□ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications. Advanced...

Step 7. 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
   >
   > Consider 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.

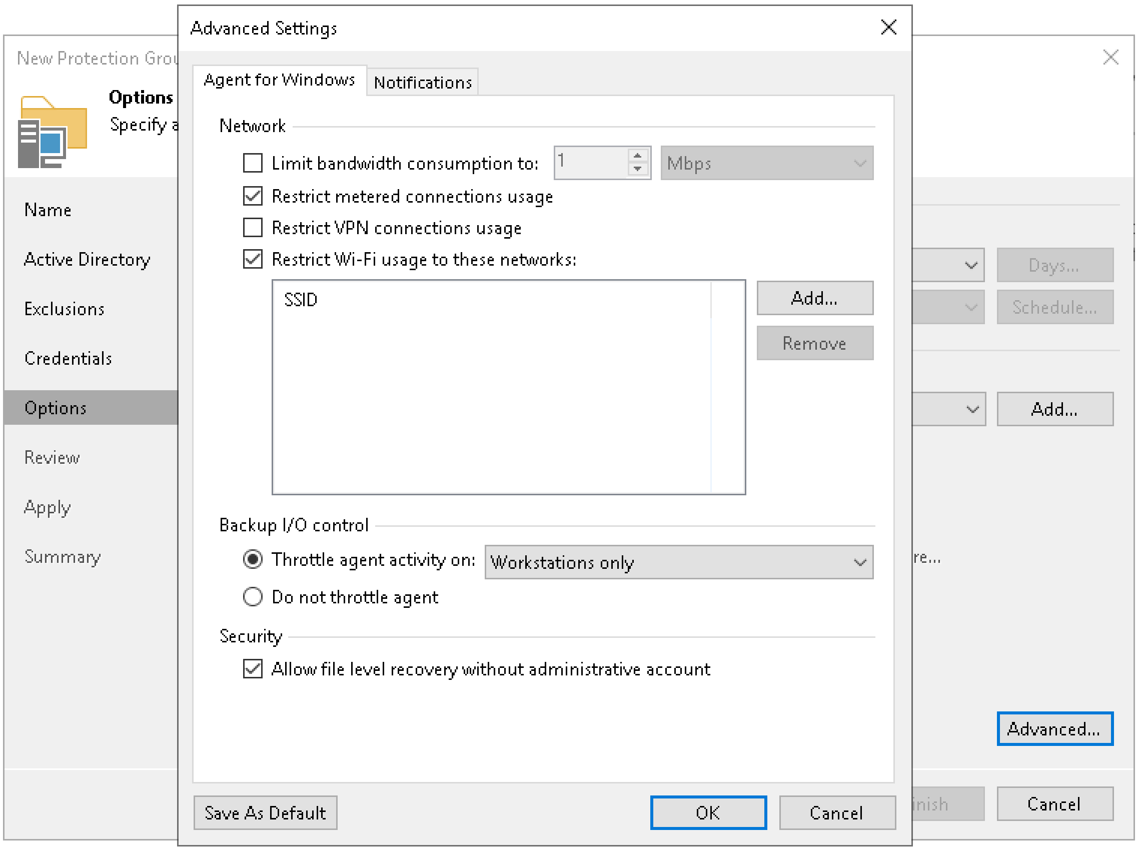
6. If you want to throttle Veeam Agent activities during backup, in the **Backup I/O control** section, make sure that the **Throttle agent activity on** option is selected. Then select the type of computers on which to throttle Veeam Agent backup activities: *Workstations only*, *Servers only* or *All 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 Restoring Files from Backup without Administrator Privileges.



Network

☐ Limit bandwidth consumption to: 1 Mbps

☑ Restrict metered connections usage

☐ Restrict VPN connections usage

☑ Restrict Wi-Fi usage to these networks:

SSID

Backup I/O control

● Throttle agent activity on: Workstations only

○ Do not throttle agent

Security

☑ Allow file level recovery without administrative account

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.

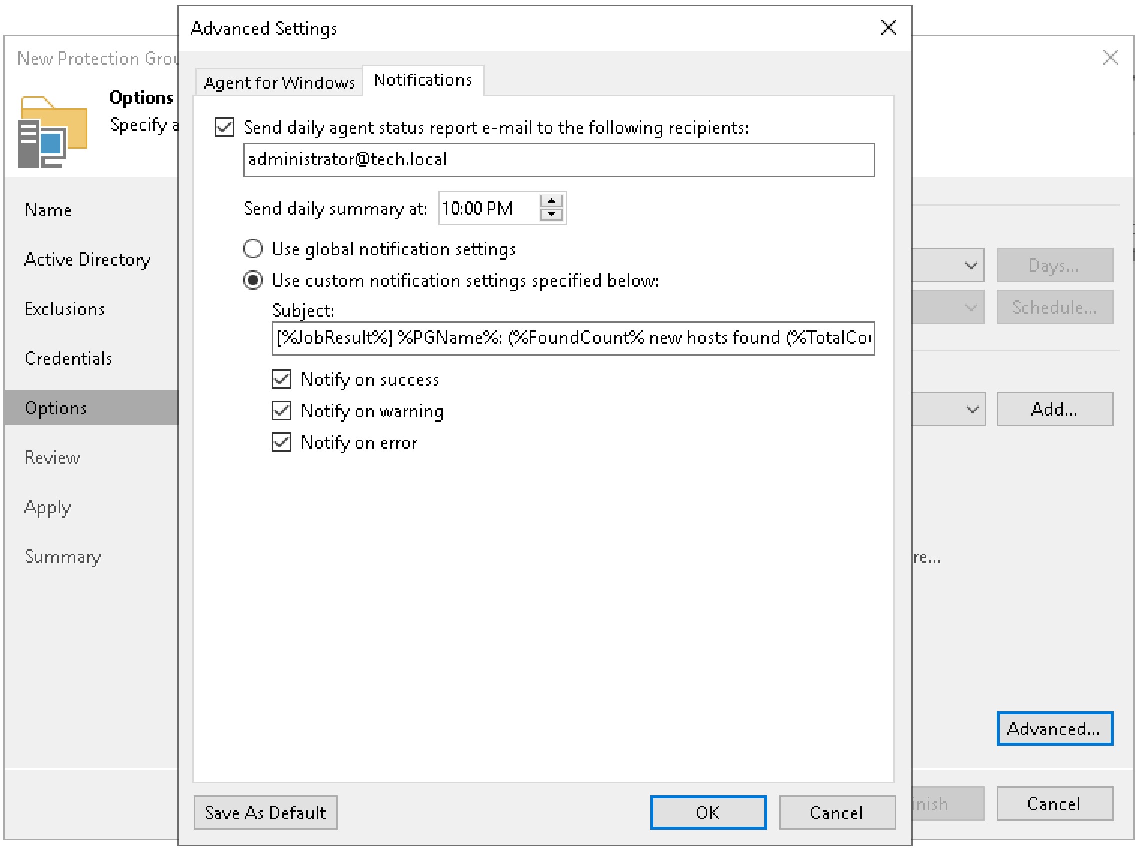
   To receive a typical notification for the protection group, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the protection group global email notification settings specified for the backup server.

   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 **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.



☑ Send daily agent status report e-mail to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success

☑ Notify on warning

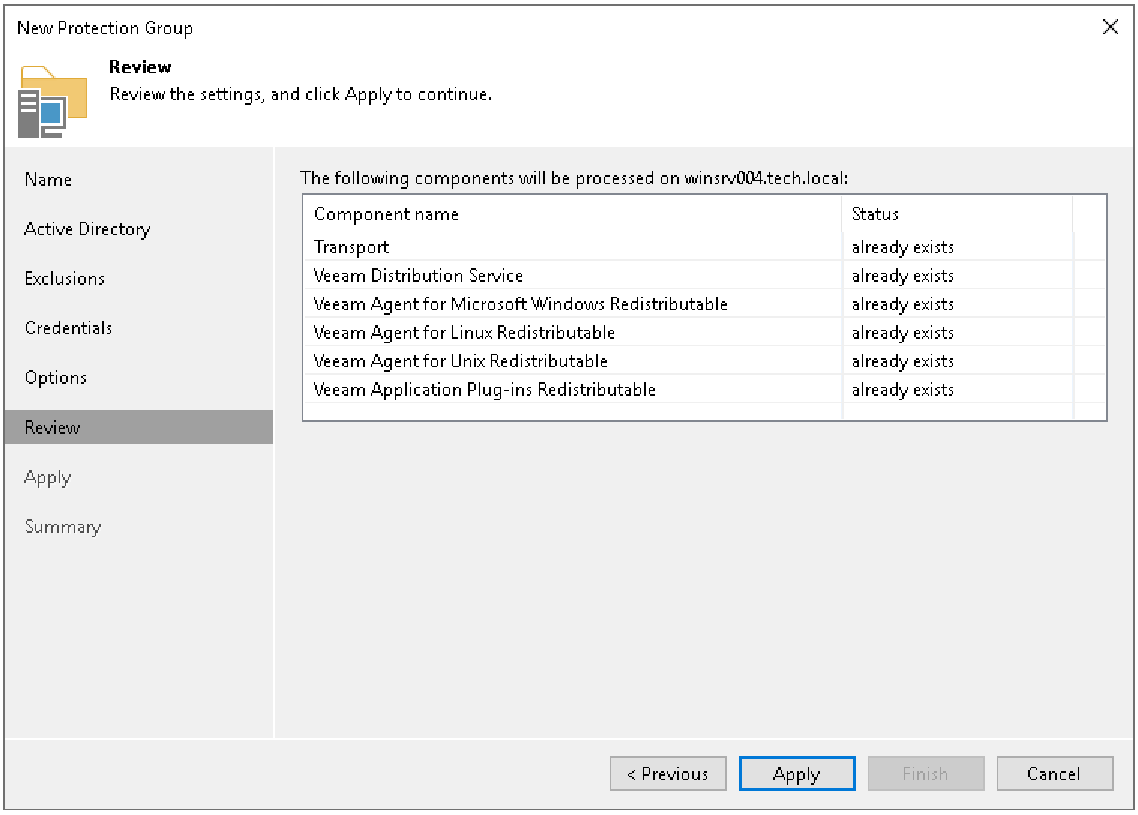
☑ Notify on error

Step 8. Review Components

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

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

> **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.

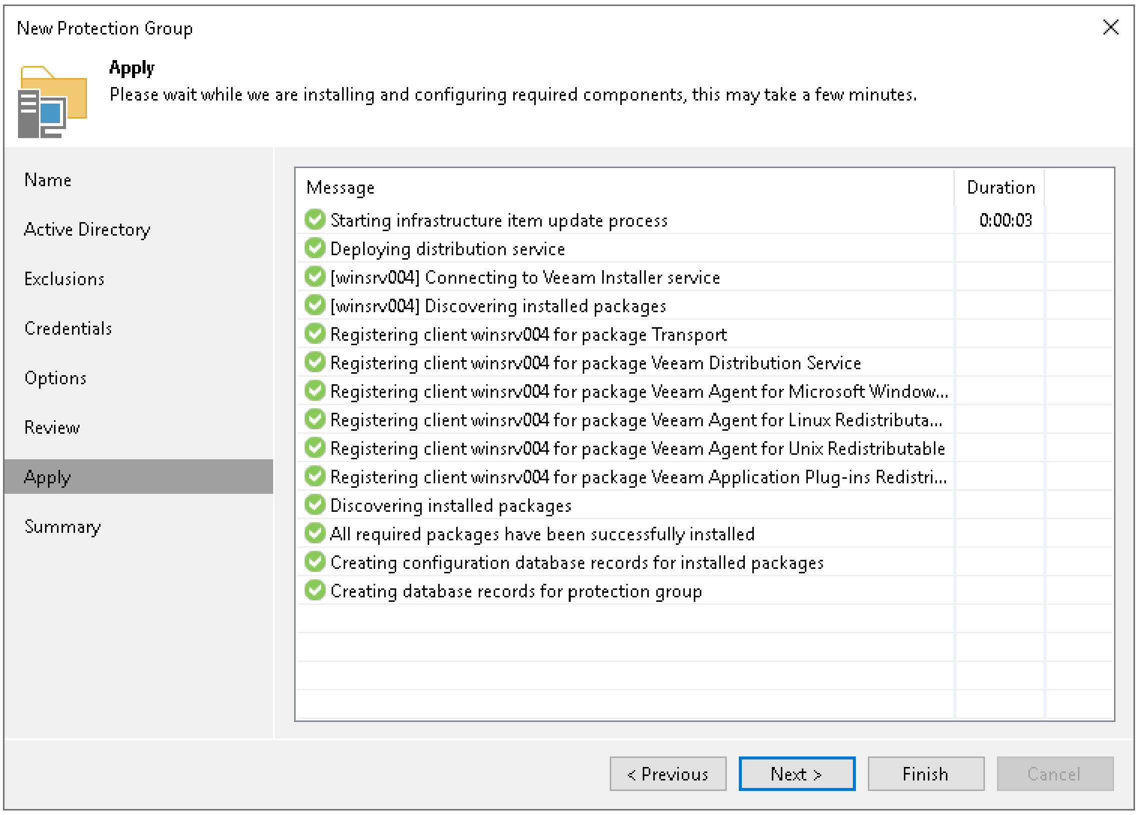


The following components will be processed on winsrv004.tech.local:

Component name	Status
Transport	already exists
Veeam Distribution Service	already exists
Veeam Agent for Microsoft Windows Redistributable	already exists
Veeam Agent for Linux Redistributable	already exists
Veeam Agent for Unix Redistributable	already exists
Veeam Application Plug-ins Redistributable	already exists

Step 9. 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.



New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

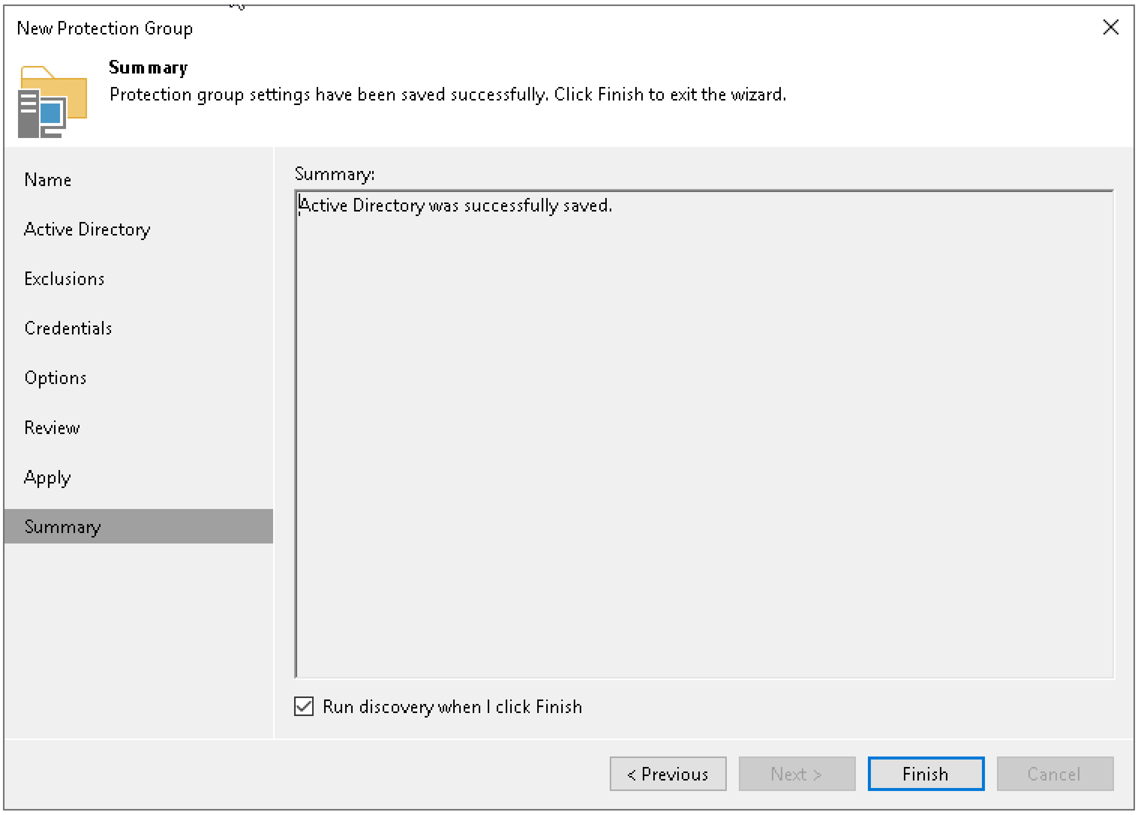
Message	Duration
✓ Starting infrastructure item update process	0:00:03
✓ Deploying distribution service	
✓ [winsrv004] Connecting to Veeam Installer service	
✓ [winsrv004] Discovering installed packages	
✓ Registering client winsrv004 for package Transport	
✓ Registering client winsrv004 for package Veeam Distribution Service	
✓ Registering client winsrv004 for package Veeam Agent for Microsoft Window...	
✓ Registering client winsrv004 for package Veeam Agent for Linux Redistributa...	
✓ Registering client winsrv004 for package Veeam Agent for Unix Redistributable	
✓ Registering client winsrv004 for package Veeam Application Plug-ins Redistri...	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating configuration database records for installed packages	
✓ Creating database records for protection group	

Step 10. 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**.



New Protection Group

Summary

Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:

Active Directory was successfully saved.

☑ Run discovery when I click Finish

Creating Protection Group for Computers from CSV File

Before you create a protection group for computers from a CSV file, check prerequisites. Then use the **New Protection Group** wizard to configure a protection group.

1. Launch the New Protection Group wizard.
2. Specify protection group name and description.
3. Specify CSV file.
4. Specify credentials.
5. Specify discovery and deployment options.
6. Specify advanced protection group settings.
7. Review components.
8. Assess results.
9. Finish working with the wizard.

Before You Begin

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

- 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.

- We recommend 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.

- We recommend 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.

- 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. To learn more, see this Microsoft KB article.

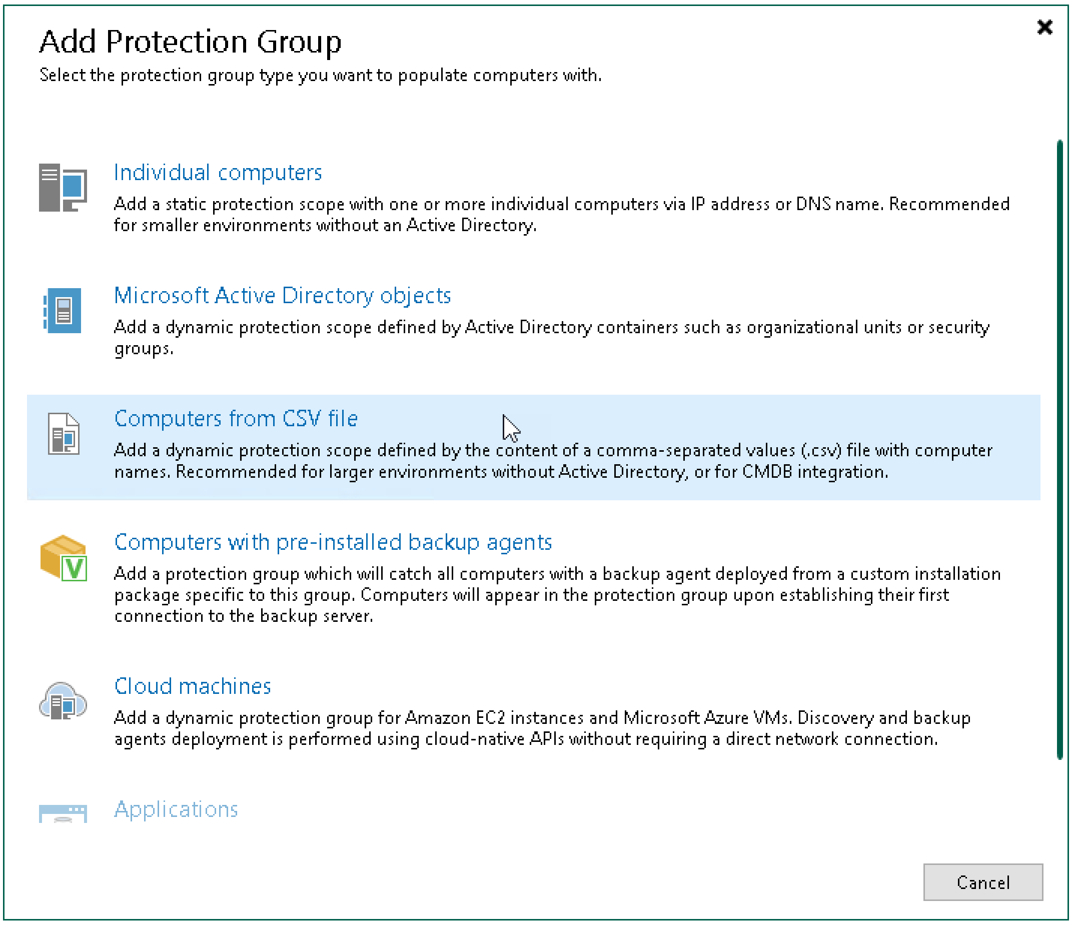
- Veeam Backup & Replication does not support usage of a Linux account for which system settings modify shell output results to connect to a computer included in the protection group. For example, this includes Linux accounts with the modified *PS1* shell variable.

- To connect to the Linux-based computer where you want to install Veeam Agent for Linux, you must specify the user account that has a home directory. The specified user account must also have the read and write permissions for their home directory.
    - You cannot install Veeam Agent for Linux on the server used as a hardened repository.

Step 1. Launch New Protection Group Wizard

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

1. Open the Add Protection Group window. To open the window, 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**.
2. In the **Add Protection Group** window, select the **Computers from CSV file** option.



Add Protection Group

Select the protection group type you want to populate computers with.

Individual computers

Add a static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

Microsoft Active Directory objects

Add a dynamic protection scope defined by Active Directory containers such as organizational units or security groups.

Computers from CSV file

Add a dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names. Recommended for larger environments without Active Directory, or for CMDB integration.

Computers with pre-installed backup agents

Add a protection group which will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

Cloud machines

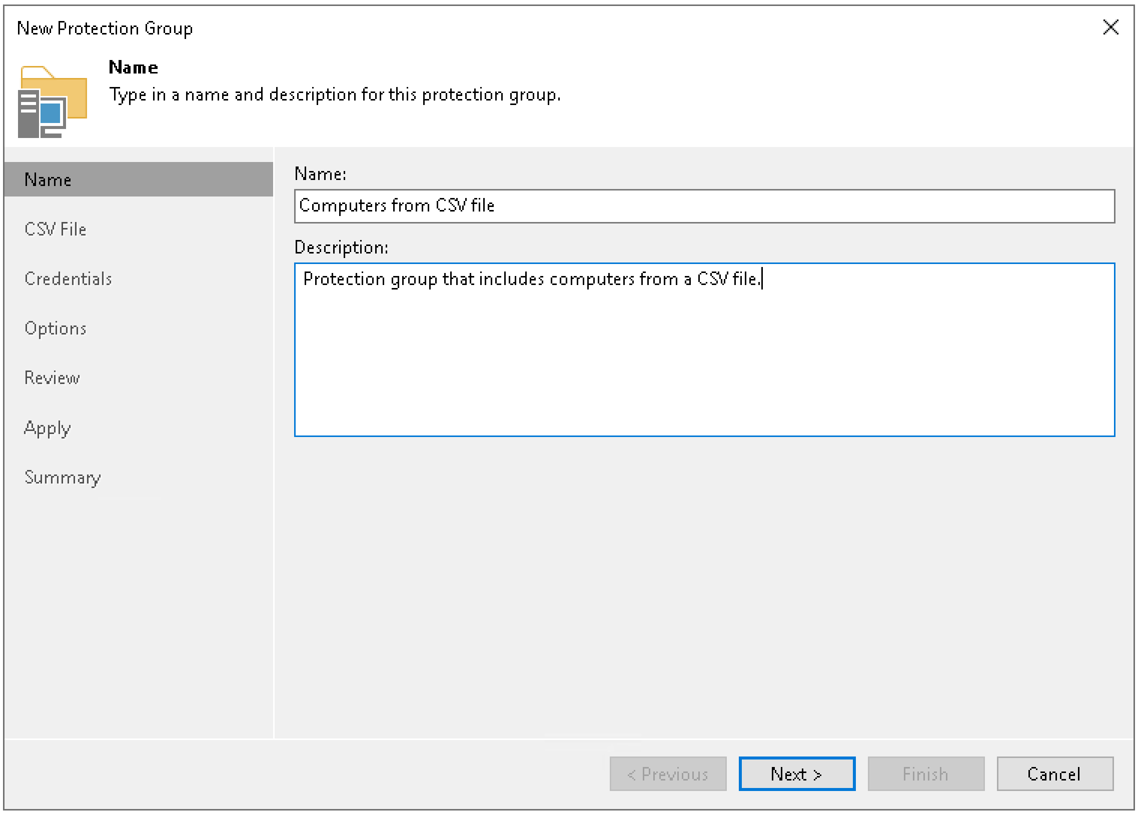
Add a dynamic protection group for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

Applications

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.



Name: Computers from CSV file

Description: Protection group that includes computers from a CSV file.

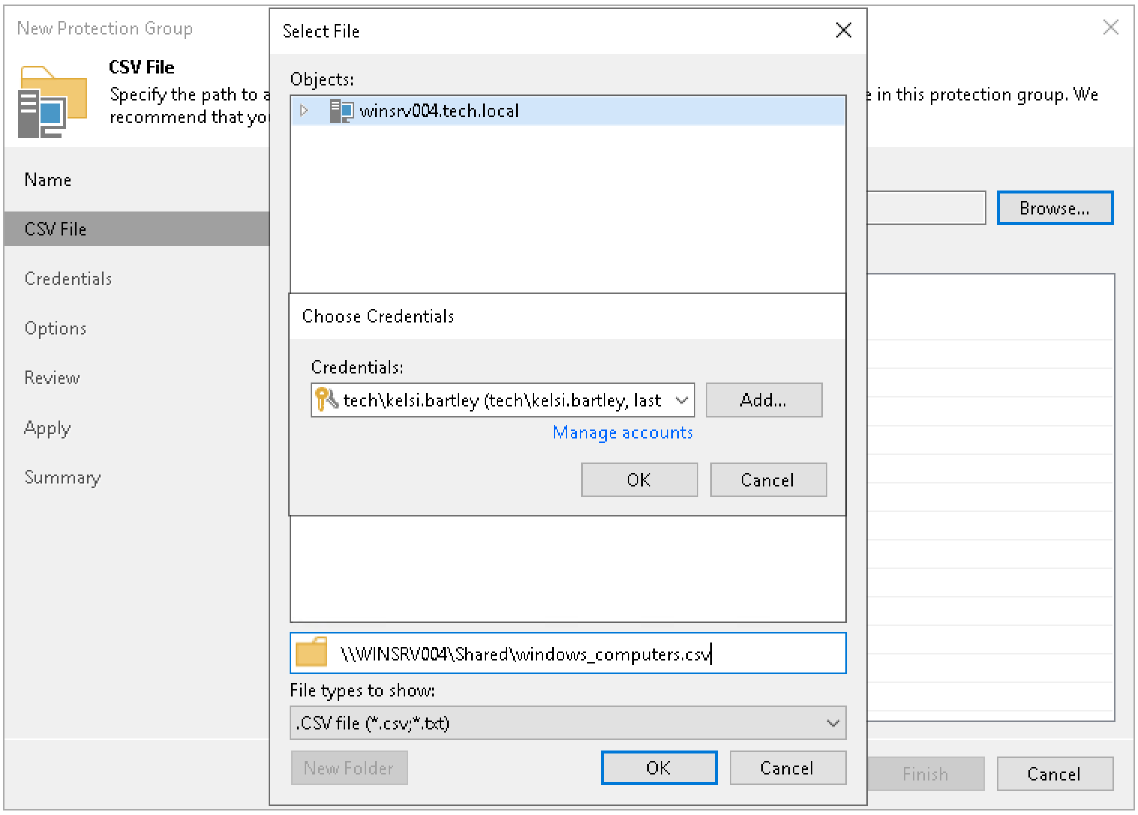
Step 3. Specify CSV File

At the **CSV File** 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 an SMB network shared folder accessible from the backup server.

   If the SMB network shared folder requires authentication, specify credentials to access the folder. Veeam Backup & Replication will store the credentials in its database.



New Protection Group

CSV File

Specify the path to a … recommend that yo… … in this protection group. We

Select File

Objects: winsrv004.tech.local

Choose Credentials

Credentials: tech\kelsi.bartley (tech\kelsi.bartley, last

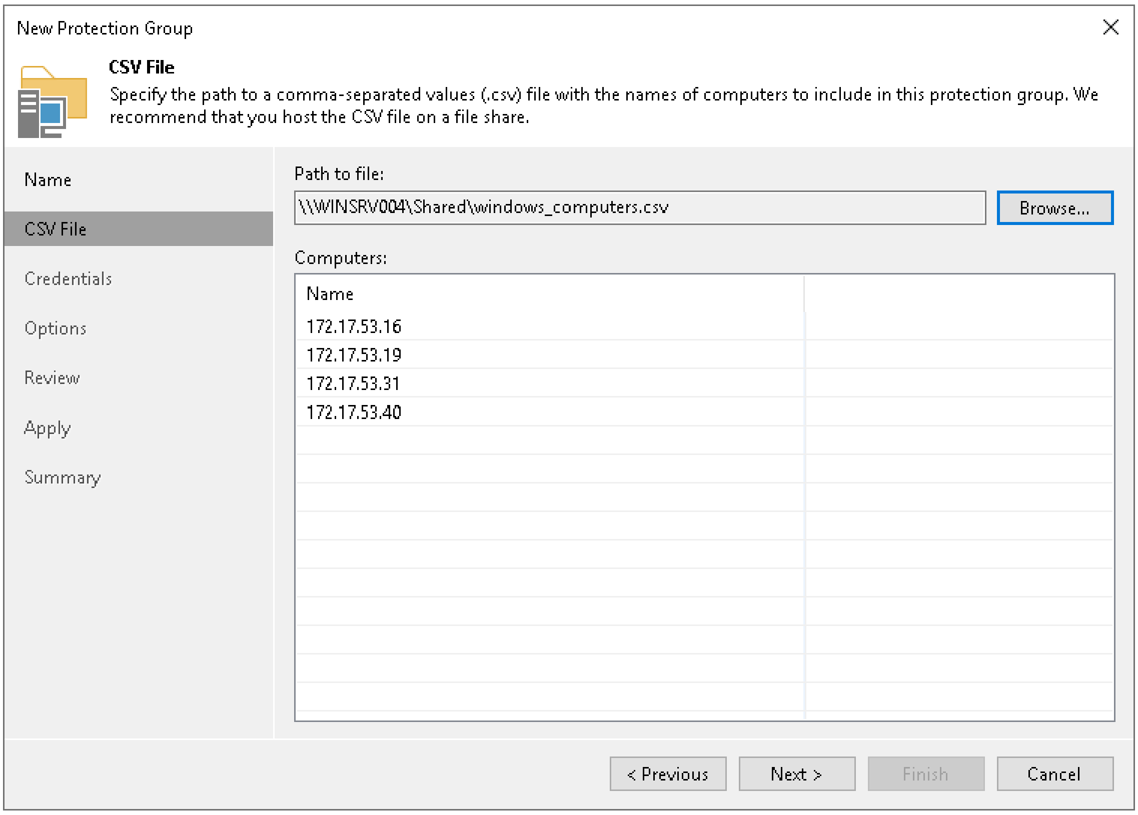
\\WINSRV004\Shared\windows_computers.csv

File types to show: .CSV file (*.csv;*.txt)

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.



New Protection Group

CSV File

Specify the path to a comma-separated values (.csv) file with the names of computers to include in this protection group. We recommend that you host the CSV file on a file share.

Path to file: \\WINSRV004\Shared\windows_computers.csv

Computers:

Name
172.17.53.16
172.17.53.19
172.17.53.31
172.17.53.40

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 characters.

For example:

```
172.17.53.16
172.17.53.19
172.17.53.31
172.17.53.40
```

IMPORTANT

For correct import of the CSV file, make sure to use newline characters of the CR LF type.

Step 4. Specify Credentials

At the **Credentials** 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.

   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.

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 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:

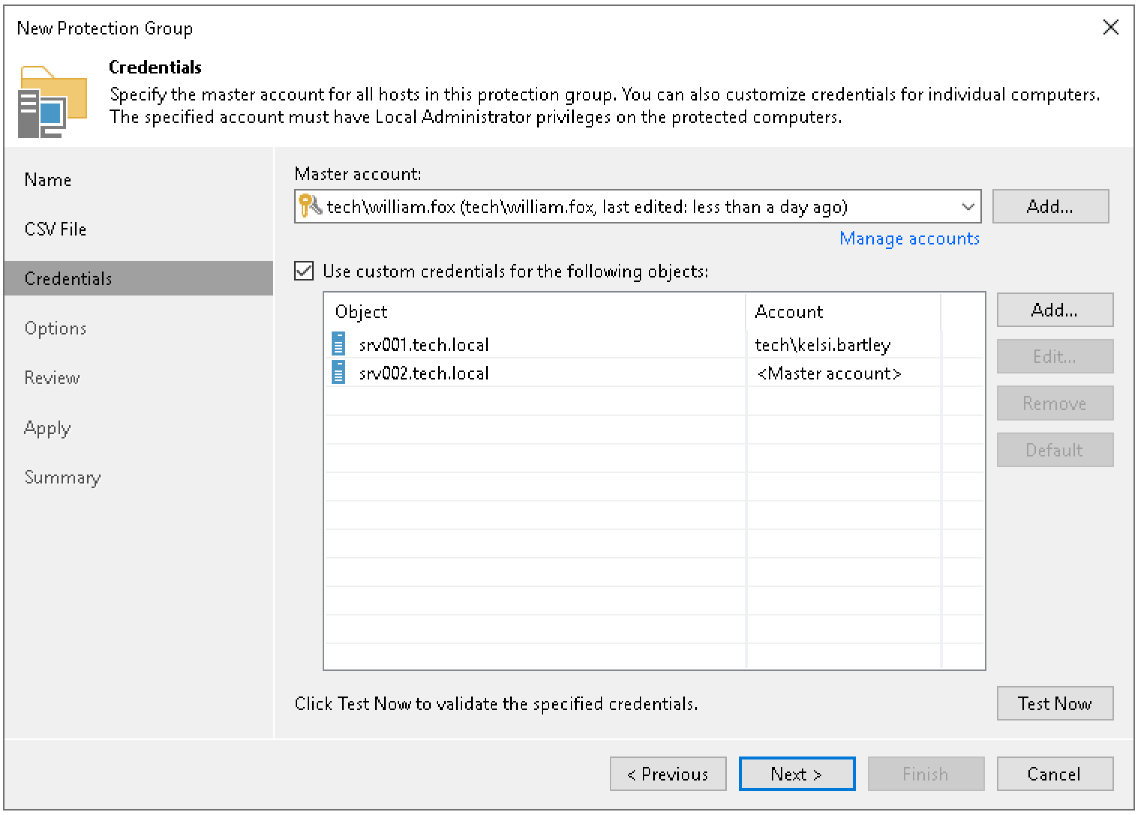
      - For Active Directory accounts — *DOMAIN\Username*
      - For local accounts — *Username* or *HOST\Username*

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 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).
- You cannot use an Azure Active Directory account to connect to computers included in the protection 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.



New Protection Group

Credentials

Specify the master account for all hosts in this protection group. You can also customize credentials for individual computers. The specified account must have Local Administrator privileges on the protected computers.

Master account: tech\william.fox (tech\william.fox, last edited: less than a day ago)

☑ Use custom credentials for the following objects:

Object	Account
srv001.tech.local	tech\kelsi.bartley
srv002.tech.local	<Master account>

Click Test Now to validate the specified credentials.

Step 5. Specify Discovery and Deployment Options

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

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

To specify discovery and deployment options:

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

   - 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, 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.

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 and Veeam Transport 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. If Veeam Transport Service is already installed on a computer, Veeam Backup & Replication checks its version and upgrade Veeam Transport Service if a later version is available.

   > 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 Veeam Backup & Replication 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.

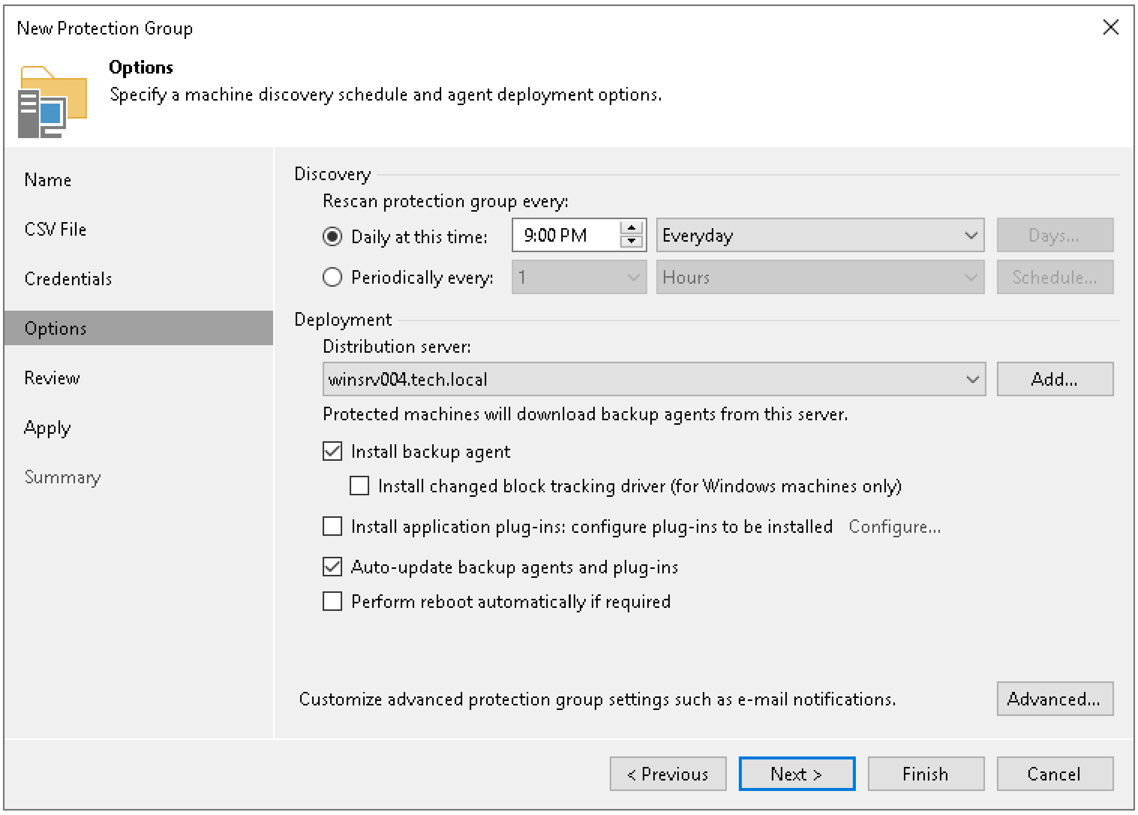
   Keep in mind that Veeam Backup & Replication will install the CBT driver only on those computers that run supported Microsoft Windows OS versions.

   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.



New Protection Group

Options

Specify a machine discovery schedule and agent deployment options.

Discovery

Rescan protection group every:

● Daily at this time: 9:00 PM Everyday Days...

○ Periodically every: 1 Hours Schedule...

Deployment

Distribution server: winsrv004.tech.local Add...

Protected machines will download backup agents from this server.

☑ Install backup agent

□ Install changed block tracking driver (for Windows machines only)

□ Install application plug-ins: configure plug-ins to be installed Configure...

☑ Auto-update backup agents and plug-ins

□ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications. Advanced...

Step 6. 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
   >
   > Consider 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.

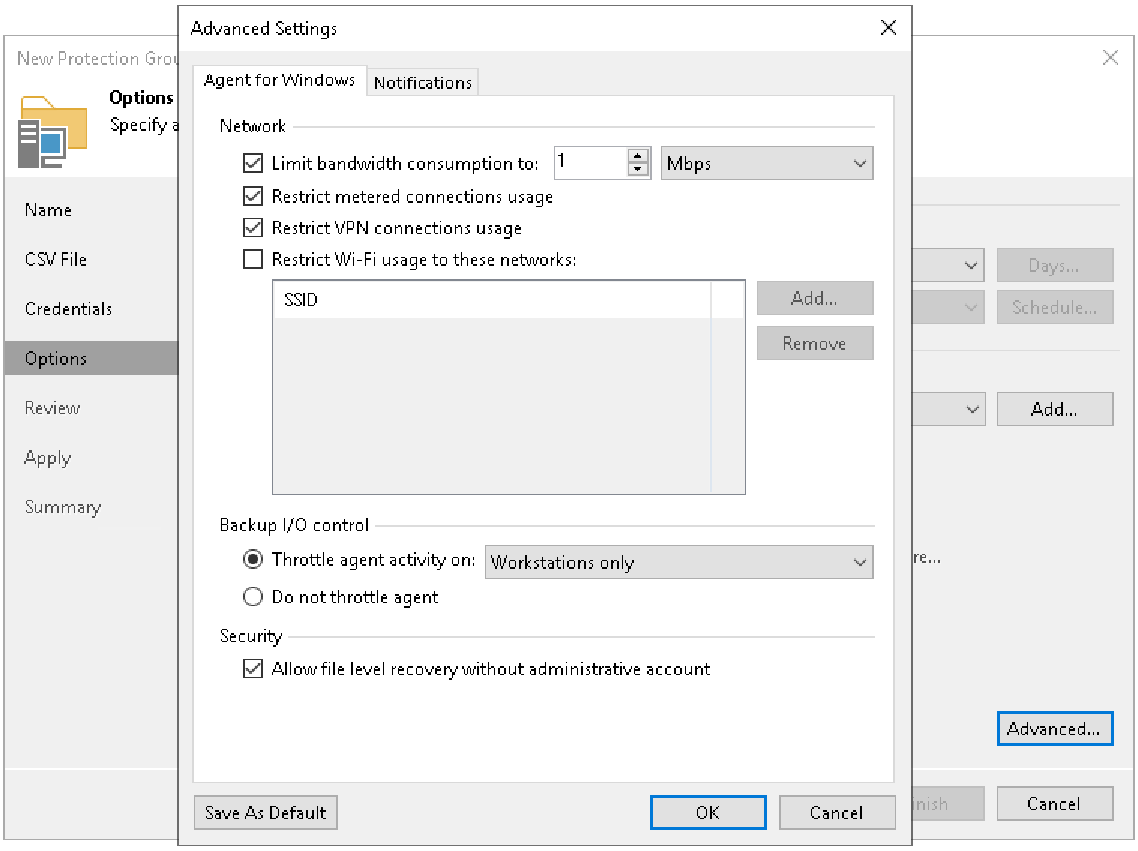
6. If you want to throttle Veeam Agent activities during backup, in the **Backup I/O control** section, make sure that the **Throttle agent activity on** option is selected. Then select the type of computers on which to throttle Veeam Agent backup activities: *Workstations only*, *Servers only* or *All 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 Restoring Files from Backup without Administrator Privileges.



Network

☑ Limit bandwidth consumption to: 1 Mbps

☑ Restrict metered connections usage

☑ Restrict VPN connections usage

☐ Restrict Wi-Fi usage to these networks:

Backup I/O control

● Throttle agent activity on: Workstations only

○ Do not throttle agent

Security

☑ Allow file level recovery without administrative account

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.

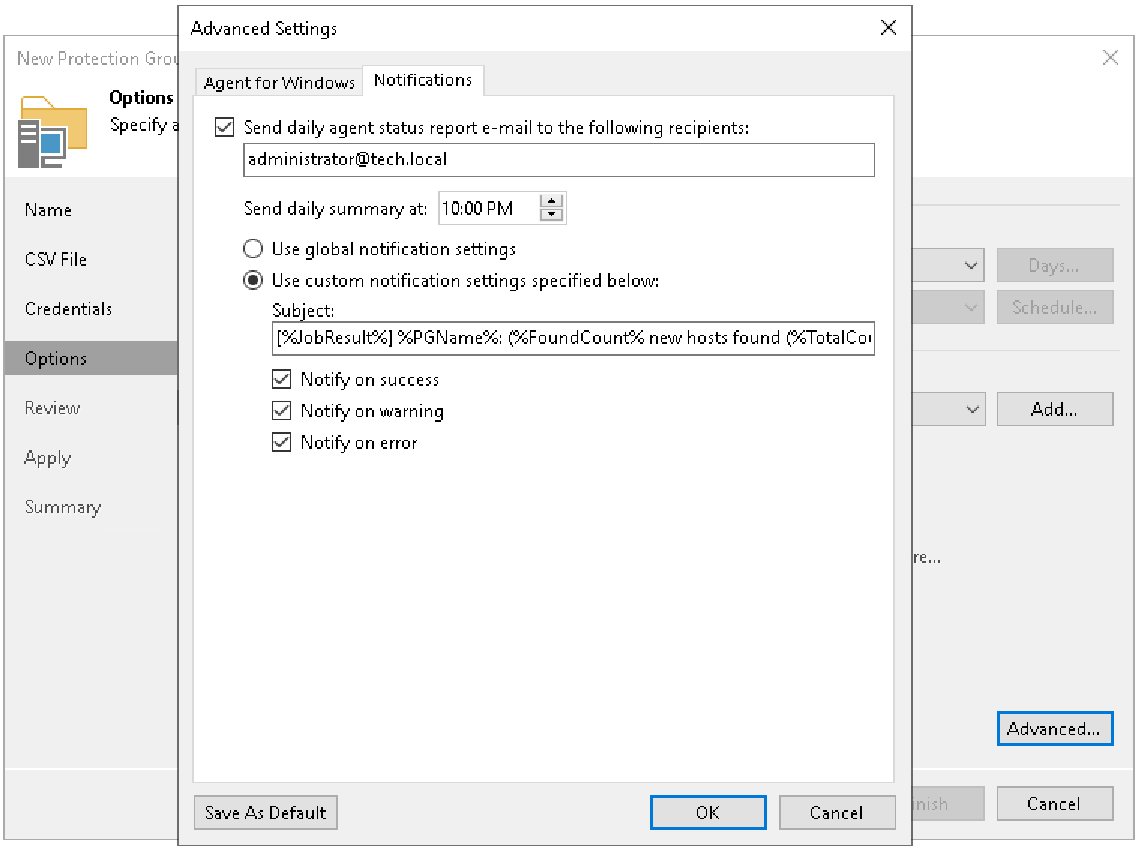
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the daily email report for the protection group.

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 **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.



☑ Send daily agent status report e-mail to the following recipients:
administrator@tech.local

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:
[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success

☑ Notify on warning

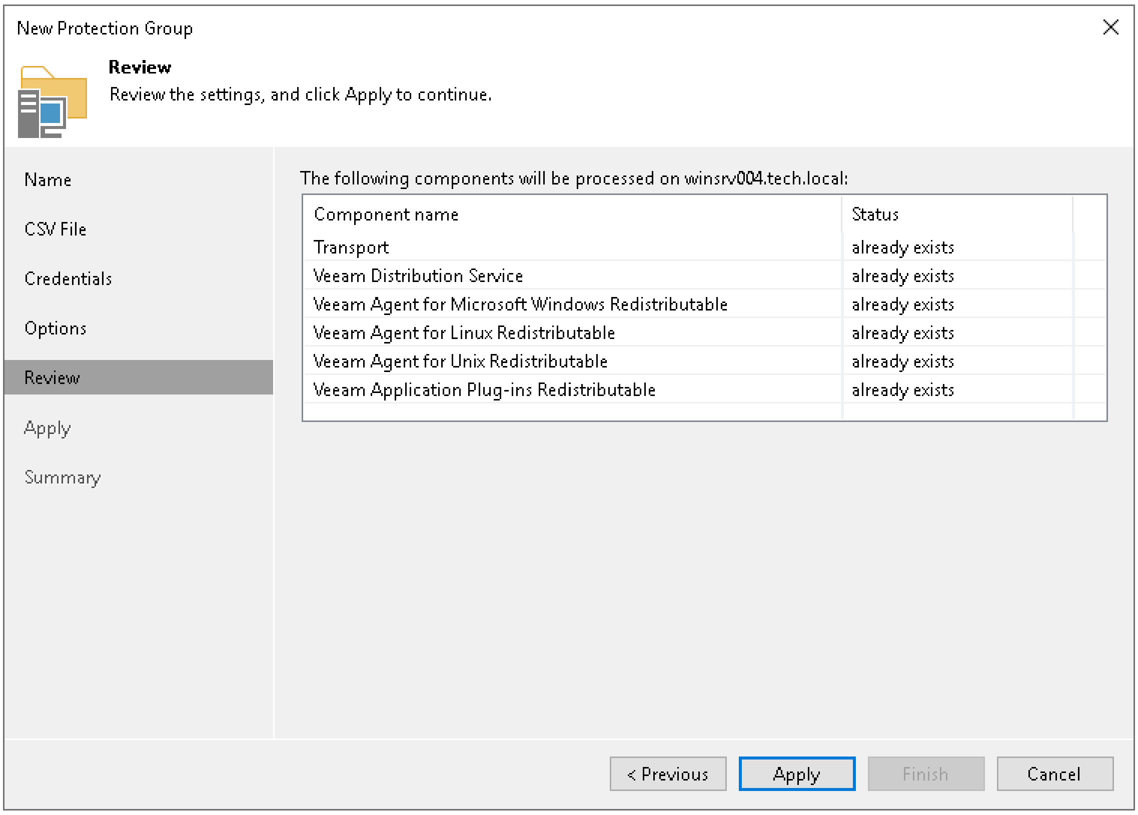
☑ Notify on error

Step 7. Review Components

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

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

> **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.

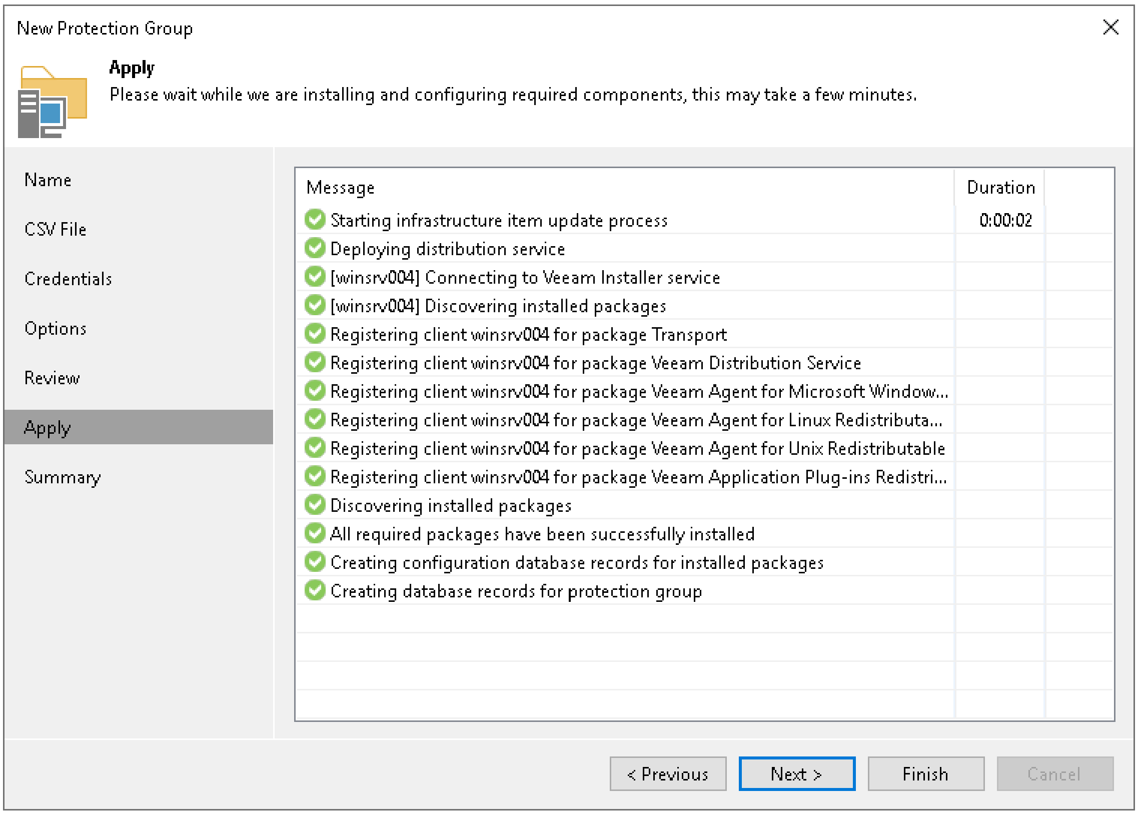


The following components will be processed on winsrv004.tech.local:

Component name	Status
Transport	already exists
Veeam Distribution Service	already exists
Veeam Agent for Microsoft Windows Redistributable	already exists
Veeam Agent for Linux Redistributable	already exists
Veeam Agent for Unix Redistributable	already exists
Veeam Application Plug-ins Redistributable	already exists

Step 8. 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.



New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

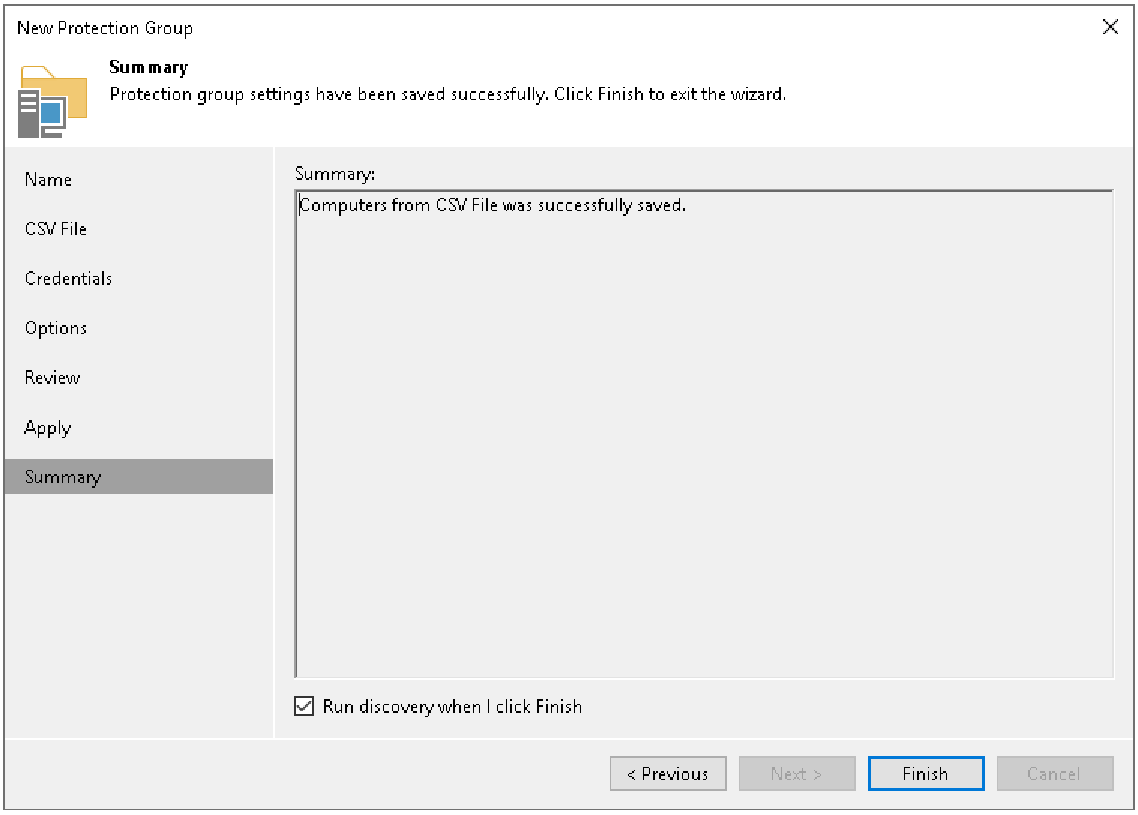
Message	Duration
✓ Starting infrastructure item update process	0:00:02
✓ Deploying distribution service	
✓ [winsrv004] Connecting to Veeam Installer service	
✓ [winsrv004] Discovering installed packages	
✓ Registering client winsrv004 for package Transport	
✓ Registering client winsrv004 for package Veeam Distribution Service	
✓ Registering client winsrv004 for package Veeam Agent for Microsoft Window...	
✓ Registering client winsrv004 for package Veeam Agent for Linux Redistributa...	
✓ Registering client winsrv004 for package Veeam Agent for Unix Redistributable	
✓ Registering client winsrv004 for package Veeam Application Plug-ins Redistri...	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating configuration database records for installed packages	
✓ Creating database records for protection group	

Step 9. 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**.



New Protection Group

Summary
Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:
Computers from CSV File was successfully saved.

☑ Run discovery when I click Finish

Creating Protection Group for Computers with Pre-installed Backup Agents

Before you create a protection group for computers with pre-installed backup agents, check prerequisites. Then use the **New Protection Group** wizard to configure a protection group.

1. Launch the New Protection Group wizard.
2. Specify protection group name and description.
3. Specify packages.
4. Specify advanced protection group settings.
5. Assess results.
6. Finish working with the wizard.

Before You Begin

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

- 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.
- You can add a protection group of the computers with pre-installed backup 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.
- You cannot add a computer from a protection group for pre-installed Veeam Agents to any other protection group.

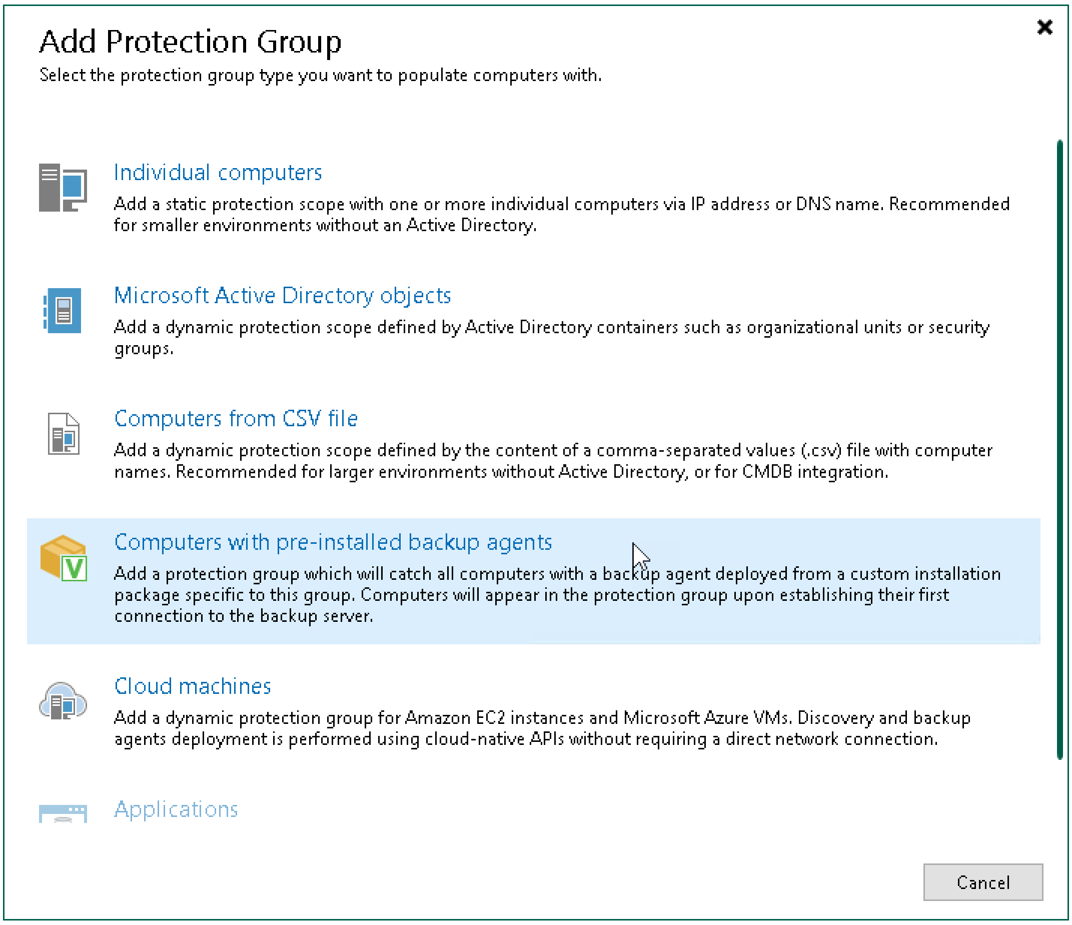
  > **TIP**
  >
  > After you create the protection group, you will be able to move a Veeam Agent for Microsoft Windows or Veeam Agent for Linux computer to another protection group. To learn more, see Moving Computer to Protection Group.

- You cannot install Veeam Agent for Linux on the server used as a hardened repository.
- If you want to add new computers to a protection group for pre-installed Veeam Agents after updating the TLS certificate on the Veeam backup server, you must first recreate the setup files. To learn more, see Specify Packages.

Step 1. Launch New Protection Group Wizard

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

1. Open the Add Protection Group window. To open the window, 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**.
2. In the **Add Protection Group** window, select the **Computers with pre-installed backup agents** option.



Add Protection Group

Select the protection group type you want to populate computers with.

Individual computers

Add a static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

Microsoft Active Directory objects

Add a dynamic protection scope defined by Active Directory containers such as organizational units or security groups.

Computers from CSV file

Add a dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names. Recommended for larger environments without Active Directory, or for CMDB integration.

Computers with pre-installed backup agents

Add a protection group which will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

Cloud machines

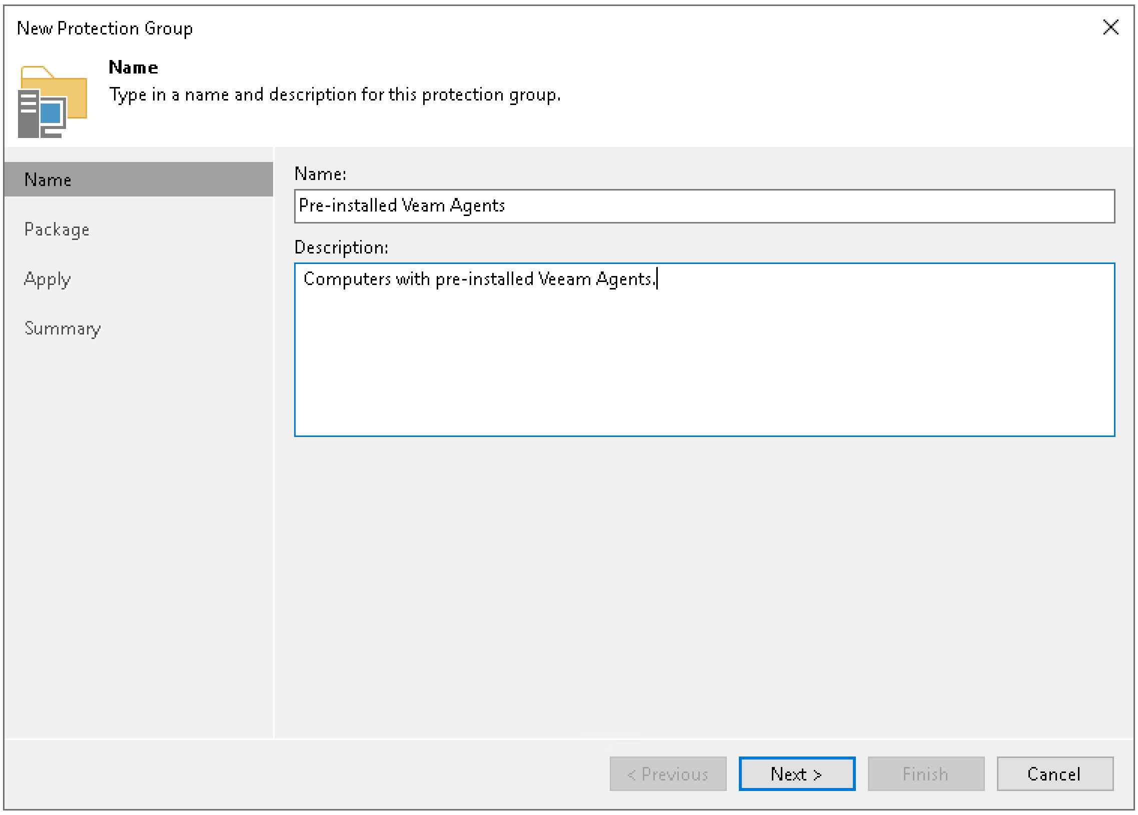
Add a dynamic protection group for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

Applications

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.



Name: Pre-installed Veam Agents

Description: Computers with pre-installed Veeam Agents.

Step 3. Specify Packages

At the **Package** 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 an SMB 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 packages for specific Unix distributions.

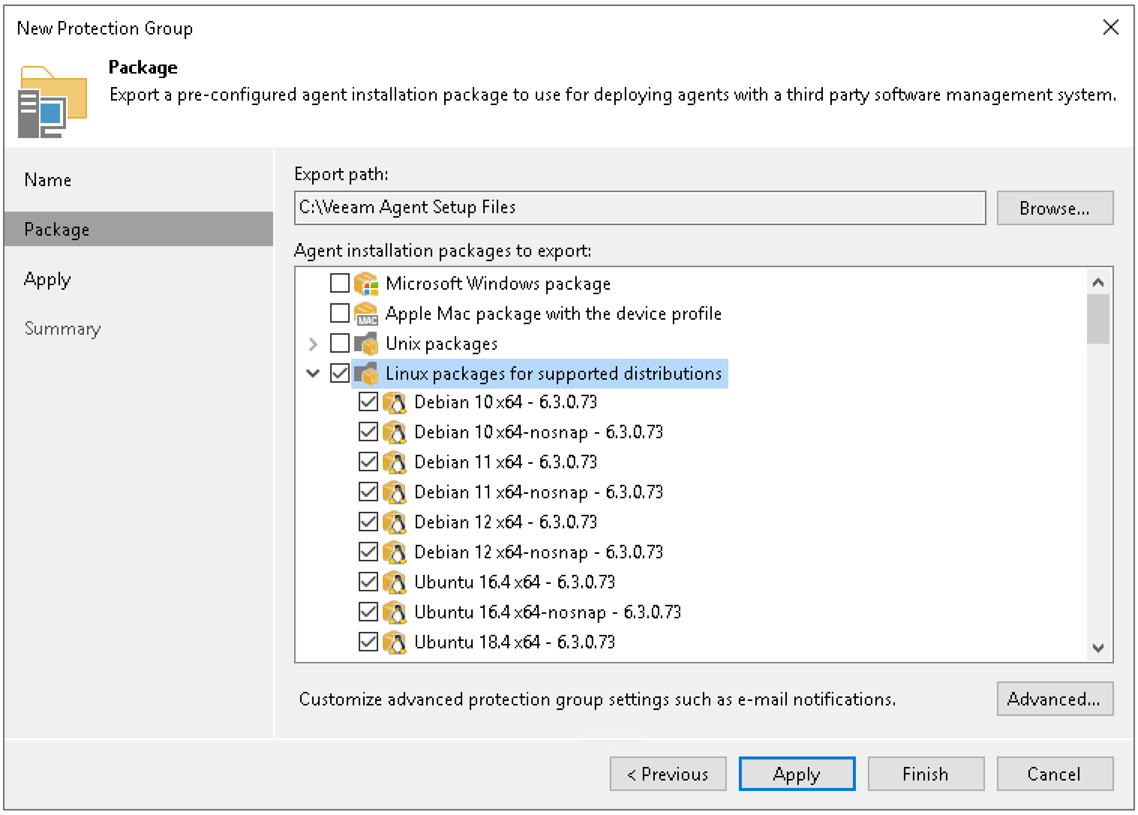
    If you select the **Unix Packages** option, Veeam Backup & Replication will export setup files for all Unix distributions supported by Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris.

    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.

    > NOTE
    >
    > You can also export installation packages of the nosnap version of Veeam Agent for Linux (including Veeam Agent for Linux on Power) for the supported Linux distributions.

    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.



New Protection Group

Package

Export a pre-configured agent installation package to use for deploying agents with a third party software management system.

Export path:

C:\Veeam Agent Setup Files

Agent installation packages to export:

- □ Microsoft Windows package
- □ Apple Mac package with the device profile
- □ Unix packages
- ☑ Linux packages for supported distributions
  - ☑ Debian 10 x64 - 6.3.0.73
  - ☑ Debian 10 x64-nosnap - 6.3.0.73
  - ☑ Debian 11 x64 - 6.3.0.73
  - ☑ Debian 11 x64-nosnap - 6.3.0.73
  - ☑ Debian 12 x64 - 6.3.0.73
  - ☑ Debian 12 x64-nosnap - 6.3.0.73
  - ☑ Ubuntu 16.4 x64 - 6.3.0.73
  - ☑ Ubuntu 16.4 x64-nosnap - 6.3.0.73
  - ☑ Ubuntu 18.4 x64 - 6.3.0.73

Customize advanced protection group settings such as e-mail notifications.

Step 4. 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
   >
   > Consider 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 Restoring 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.

> **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.

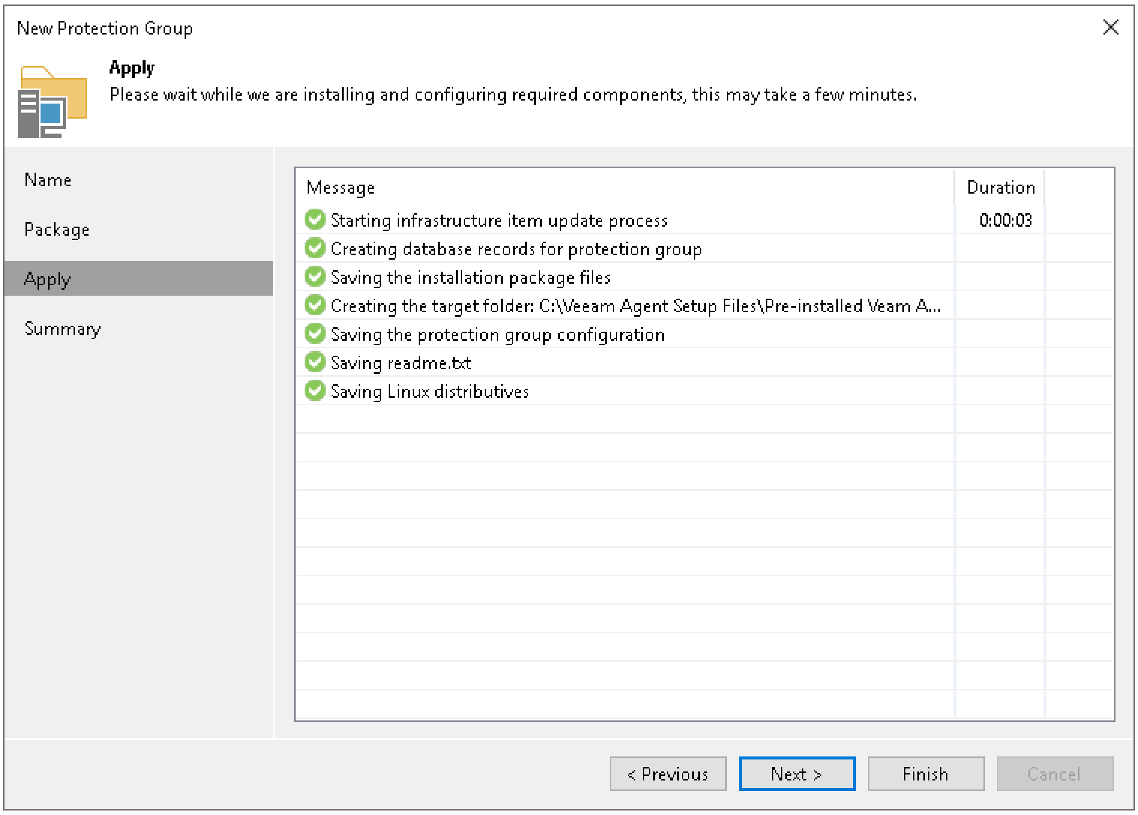
   To receive a typical notification for the protection group, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the protection group global email notification settings specified for the backup server.

   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:
     - *%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 **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.

Step 5. 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.



New Protection Group

Apply

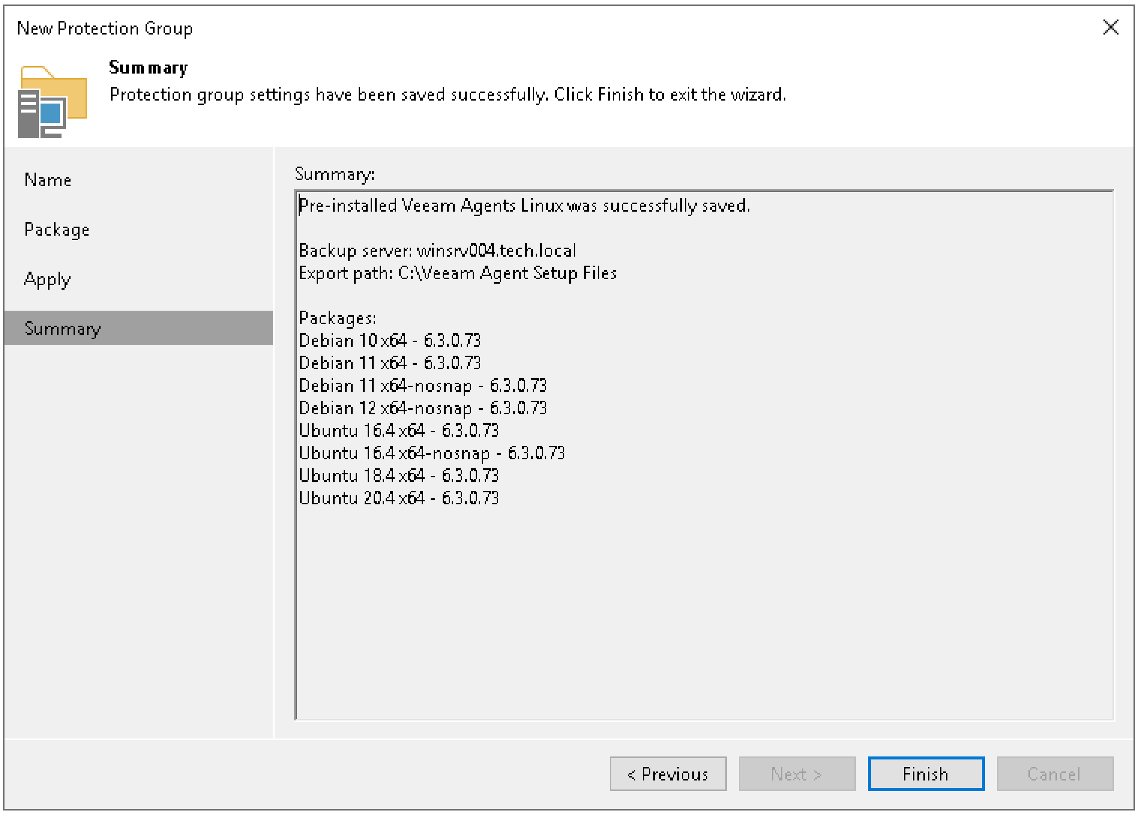
Please wait while we are installing and configuring required components, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:03
✓ Creating database records for protection group	
✓ Saving the installation package files	
✓ Creating the target folder: C:\Veeam Agent Setup Files\Pre-installed Veam A...	
✓ Saving the protection group configuration	
✓ Saving readme.txt	
✓ Saving Linux distributives	

Step 6. 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. Click **Finish to close the wizard**.



New Protection Group
Summary
Protection group settings have been saved successfully. Click Finish to exit the wizard.
Name
Package
Apply
Summary
Summary:
< Previous
Next >
Finish
Cancel

```
Pre-installed Veeam Agents Linux was successfully saved.

Backup server: winsrv004.tech.local
Export path: C:\Veeam Agent Setup Files

Packages:
Debian 10 x64 - 6.3.0.73
Debian 11 x64 - 6.3.0.73
Debian 11 x64-nosnap - 6.3.0.73
Debian 12 x64-nosnap - 6.3.0.73
Ubuntu 16.4 x64 - 6.3.0.73
Ubuntu 16.4 x64-nosnap - 6.3.0.73
Ubuntu 18.4 x64 - 6.3.0.73
Ubuntu 20.4 x64 - 6.3.0.73
```

Creating Protection Group for Cloud Machines

Before you create a protection group for cloud machines, check prerequisites. Then use the **New Protection Group** wizard to configure a protection group.

1. Launch the New Protection Group wizard.
2. Specify protection group name and description.
3. Specify account.
4. Specify cloud machines.
5. Exclude objects from the protection group.
6. Specify permissions.
7. Specify discovery and deployment options.
8. Specify advanced protection group settings.
9. Assess results.
10. Finish working with the wizard.

Before You Begin

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

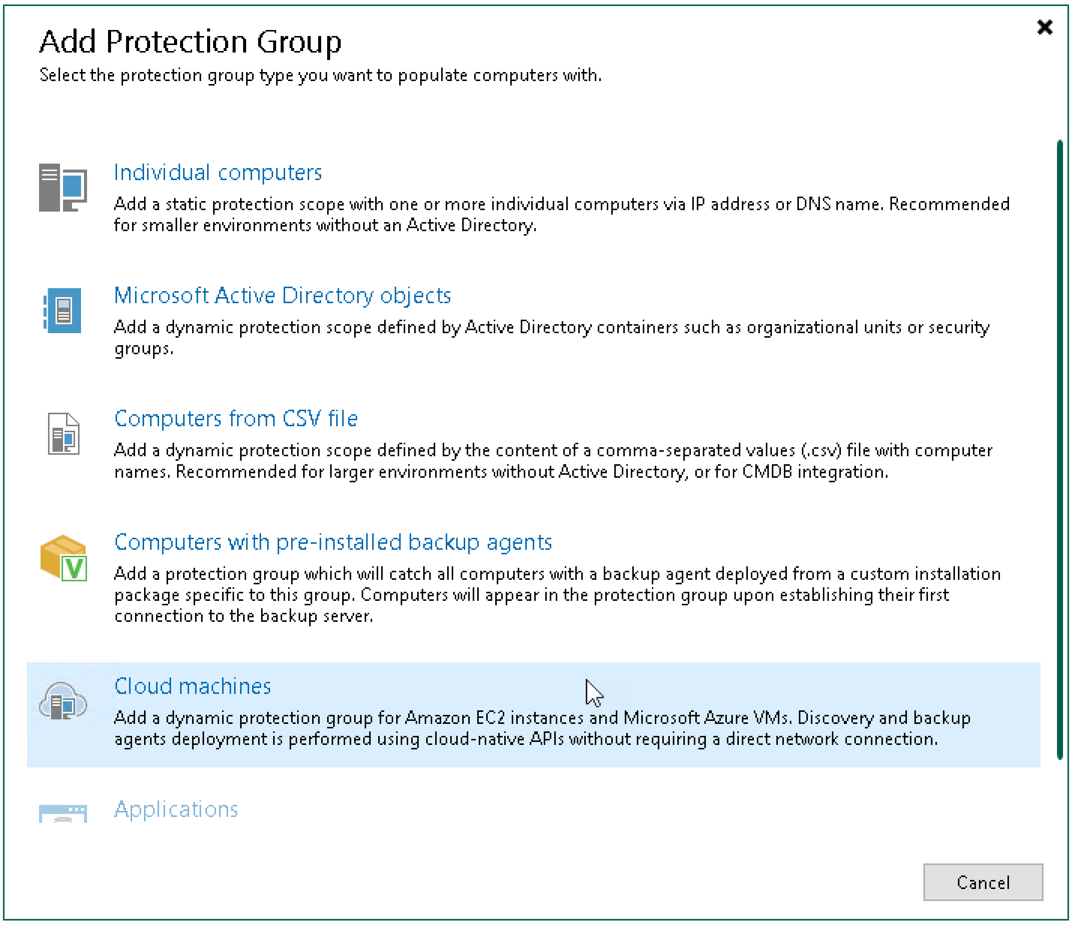
- When Veeam Backup & Replication performs discovery of protected machines, Veeam Backup & Replication connects to every machine added to the protection group. If you instruct Veeam Backup & Replication to perform discovery immediately after the protection group is created, make sure that all machines 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 machine and perform the required operations.
- 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.
- A protection group for cloud machines can include only the following objects:
  - Amazon EC2 instances
  - Microsoft Azure virtual machines
- A protection group for cloud machines can include objects running only supported Microsoft Windows and Linux OSes.
- 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.

- 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.
- 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 1. Launch New Protection Group Wizard

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

1. Open the Add Protection Group window. To open the window, 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**.
2. In the **Add Protection Group** window, select the **Cloud machines** option.



Add Protection Group

Select the protection group type you want to populate computers with.

Individual computers

Add a static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

Microsoft Active Directory objects

Add a dynamic protection scope defined by Active Directory containers such as organizational units or security groups.

Computers from CSV file

Add a dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names. Recommended for larger environments without Active Directory, or for CMDB integration.

Computers with pre-installed backup agents

Add a protection group which will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

Cloud machines

Add a dynamic protection group for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

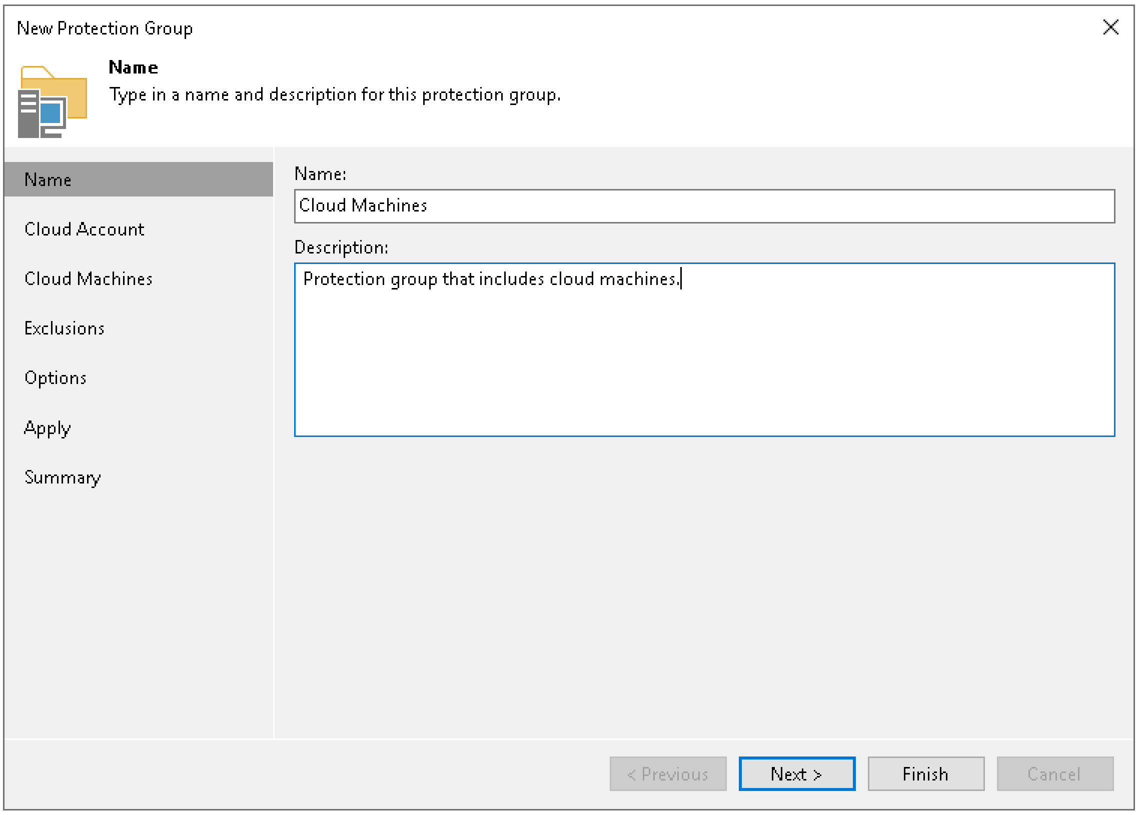
Applications

Step 2. Specify Protection Group Name and Description

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

1. In the **Name** field, specify a name for the protection group.

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



New Protection Group

Name

Type in a name and description for this protection group.

Name: Cloud Machines

Description: Protection group that includes cloud machines.

Step 3. Specify Account

At the **Cloud Account** 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 the Access Keys for AWS Users and Microsoft Azure Compute Accounts sections 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.

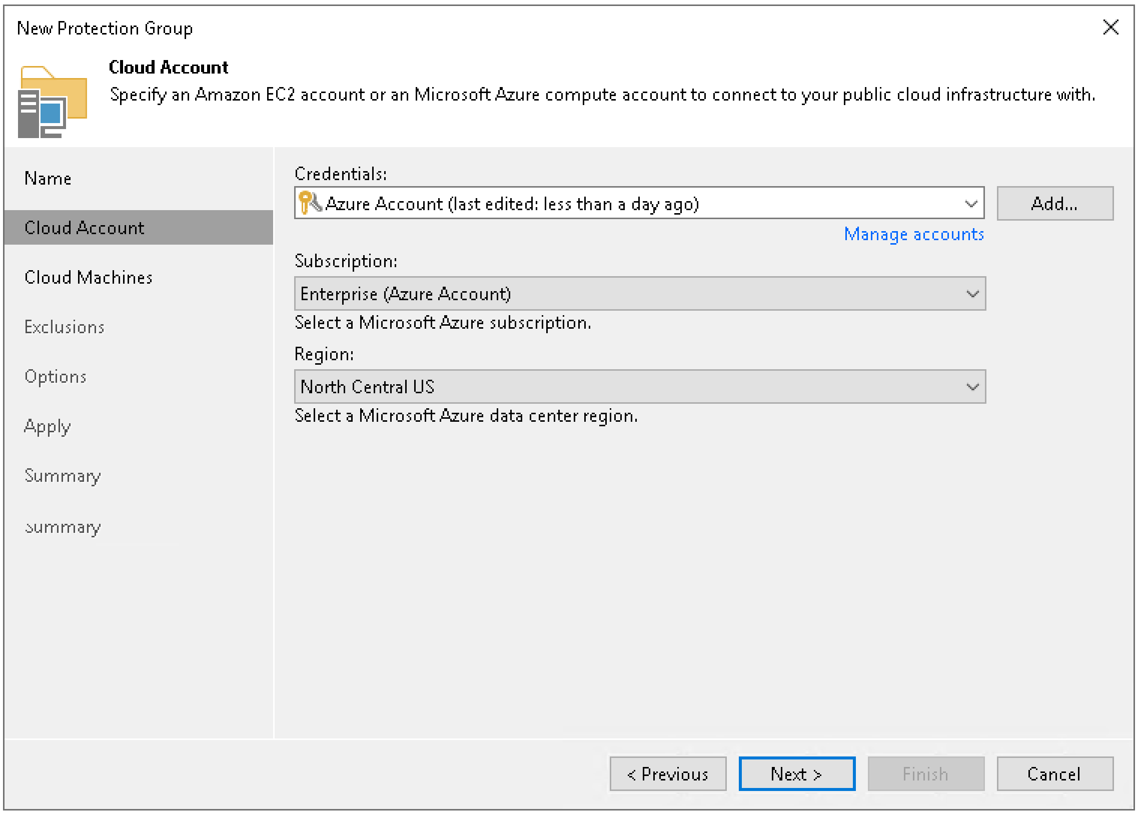
   b. From the **Data center** list, select the geographic region where Veeam Backup & Replication will deploy Veeam Agents on cloud machines.

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.

   > **IMPORTANT**
   >
   > A Microsoft Azure Compute Account must be in the same subscription as the storage account specified in the settings of the Azure Blob Storage repository used as a distribution repository. For more information about the distribution repository, see Distribution Repository.

b. From the **Region** list, select a geographic region where you want to deploy Veeam Agents on cloud machines.



New Protection Group

Cloud Account

Specify an Amazon EC2 account or an Microsoft Azure compute account to connect to your public cloud infrastructure with.

Credentials: Azure Account (last edited: less than a day ago)

Subscription: Enterprise (Azure Account)

Select a Microsoft Azure subscription.

Region: North Central US

Select a Microsoft Azure data center region.

Step 4. Specify Cloud Machines

At the **Cloud Machines** 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.

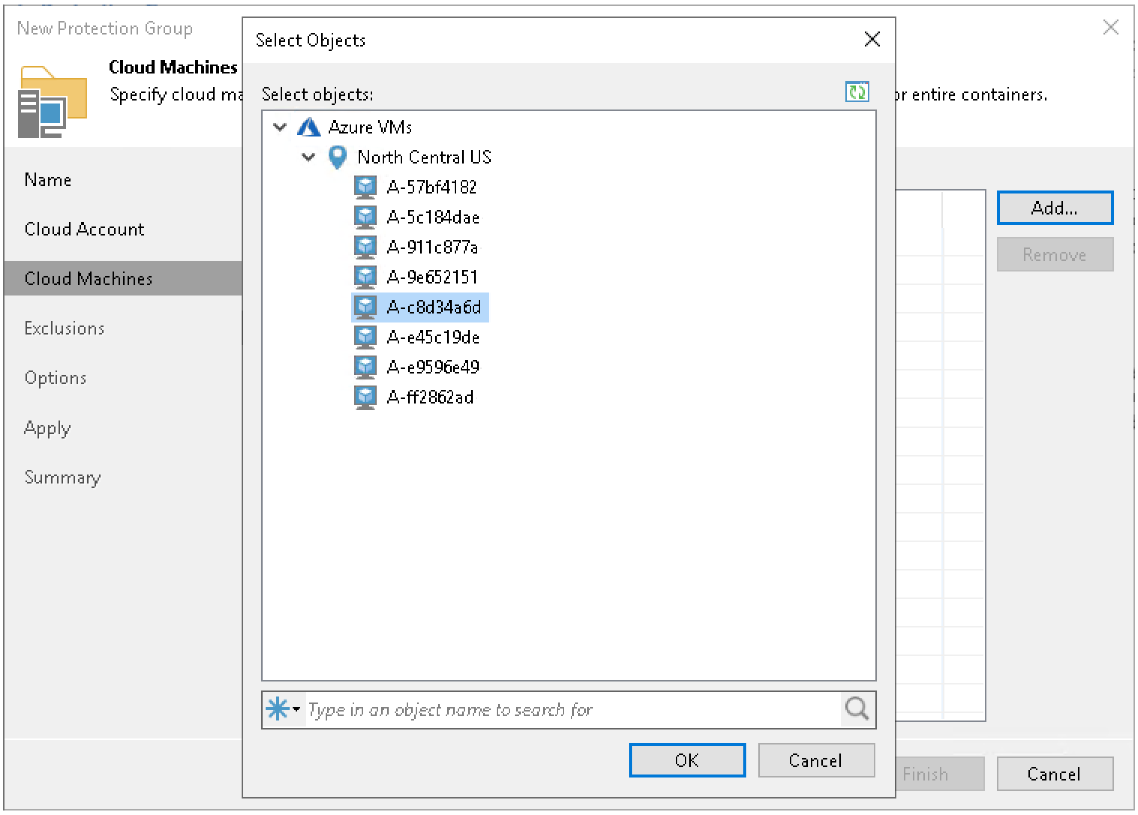
Adding Individual Cloud Machine or Datacenter

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 the [Ctrl] key 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].



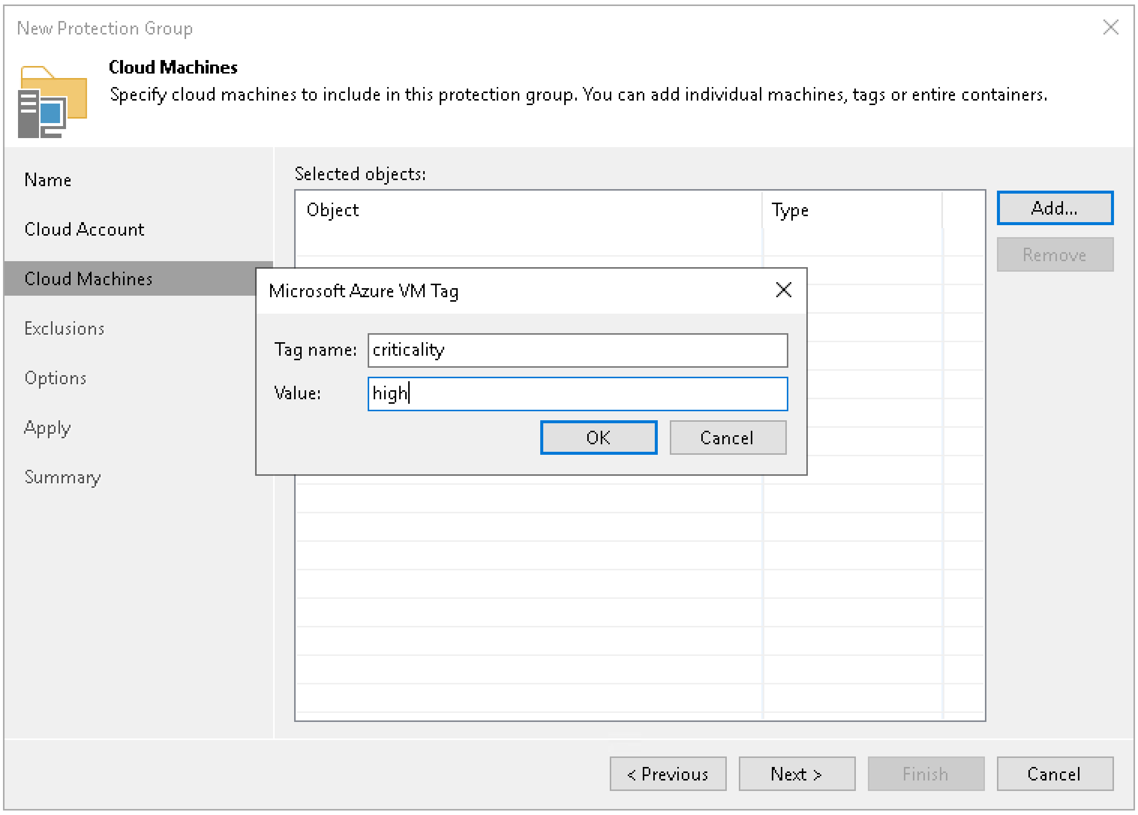
Adding Cloud Machines Using Metadata Tag

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**.

IMPORTANT

Make sure to use only lowercase symbols.



Tag name: criticality

Value: high

Step 5. Exclude Objects from Protection Group

At the **Exclusions** 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:

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

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

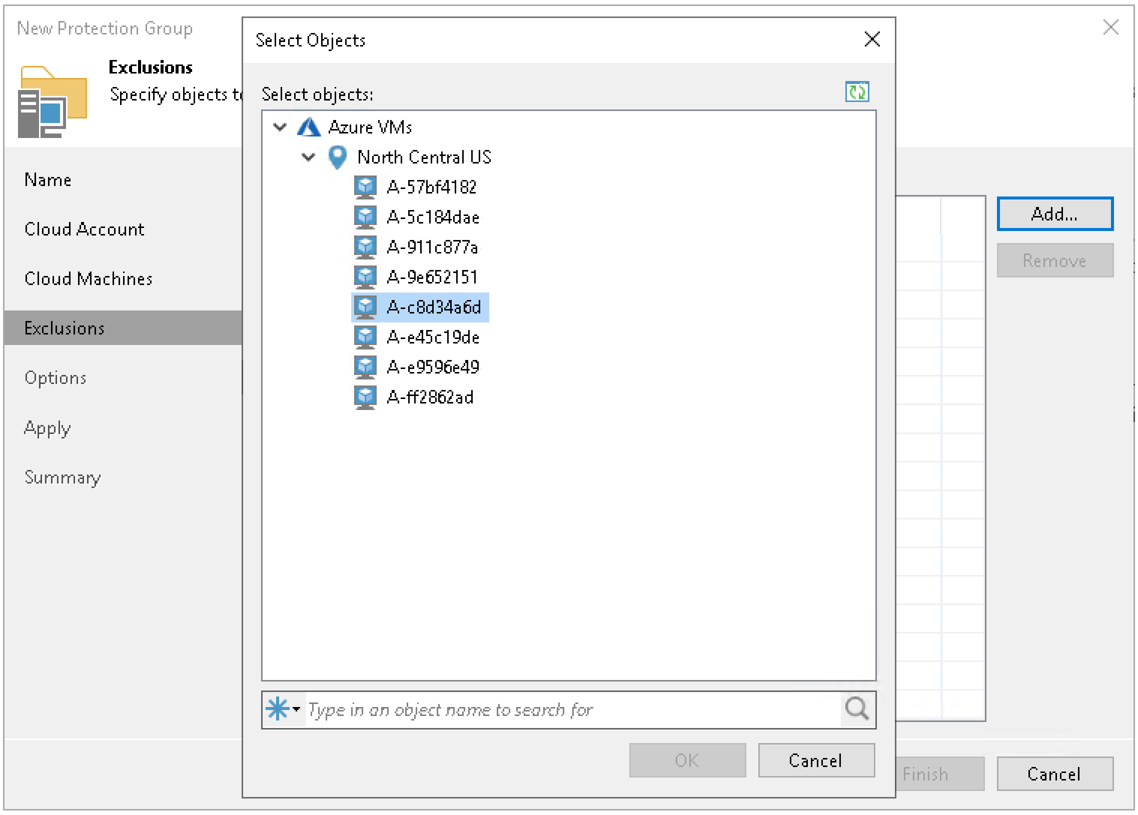
Excluding Individual Cloud Machines

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 the [Ctrl] key 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:

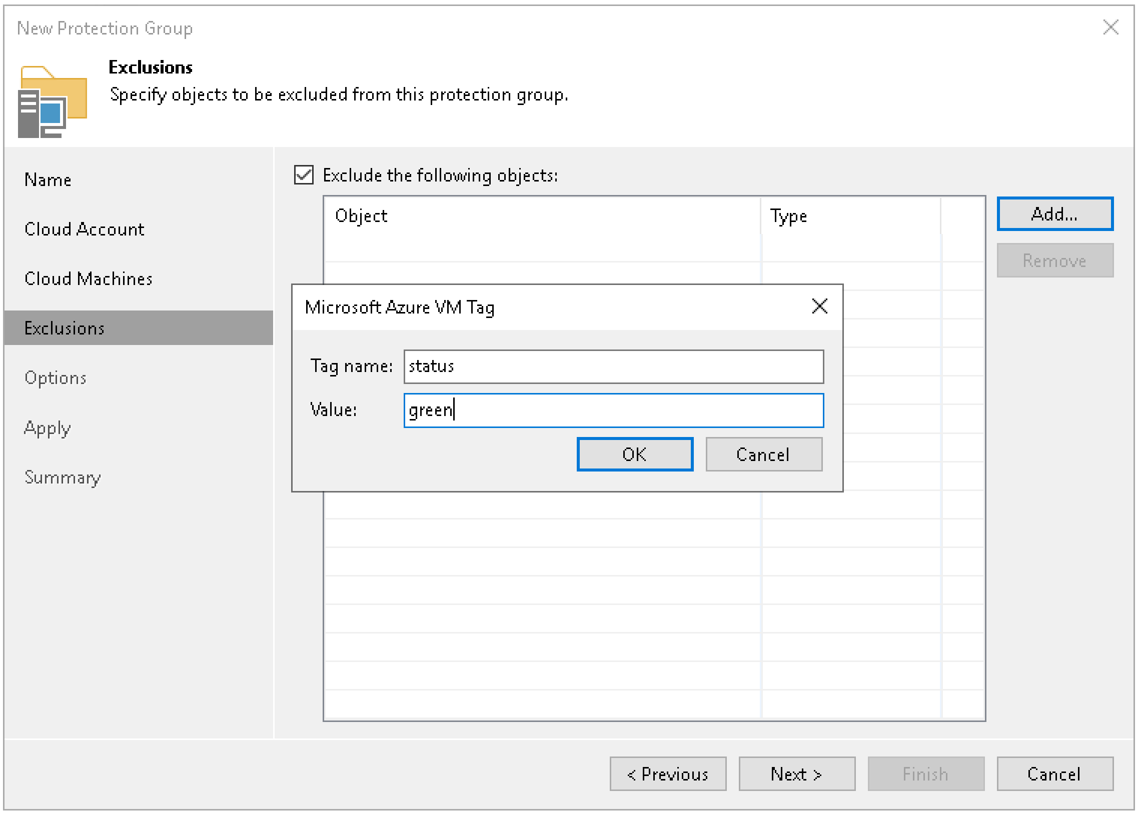
1. Click **Add** > **Tags**.

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.

> **IMPORTANT**
>
> Make sure to use only lowercase symbols.



Tag name: status

Value: green

Step 6. 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:

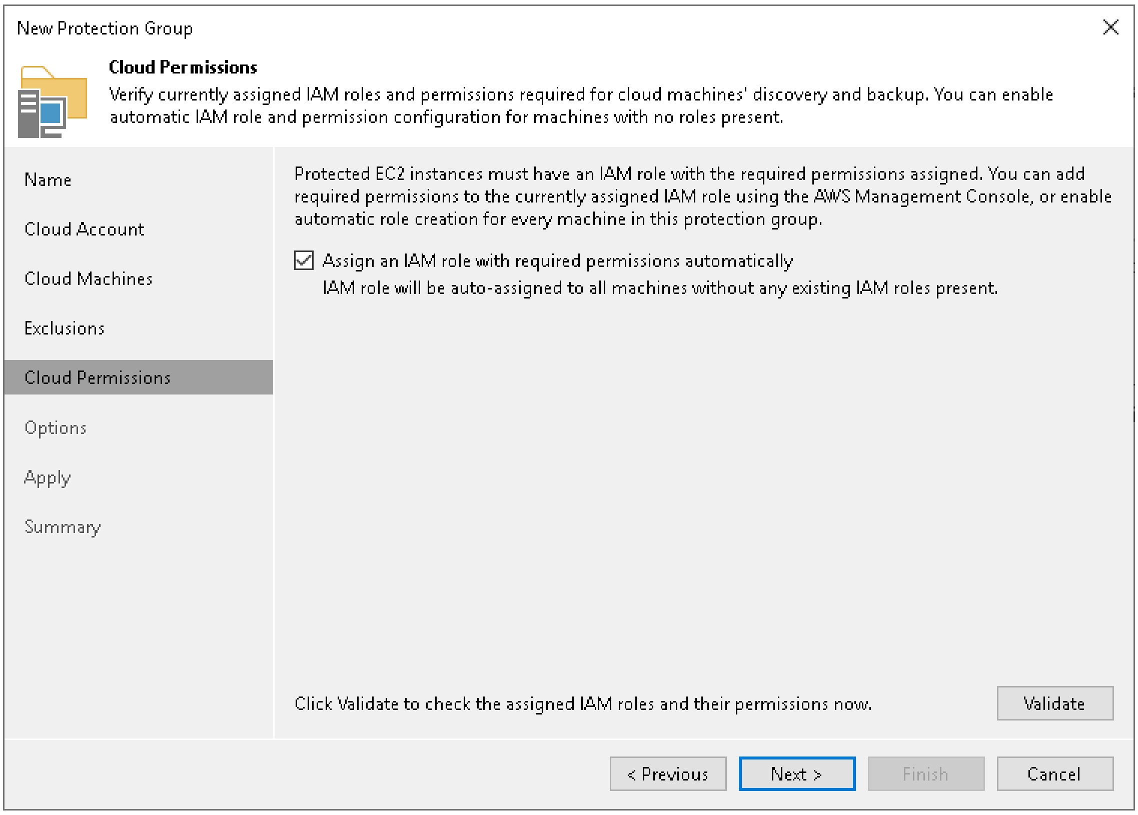
1. If you want to instruct Veeam Backup & Replication to automatically set the required role and policy, select the **Assign an IAM role with required permissions automatically** check box. If necessary, Veeam Backup & Replication will set the IAM role with the *AmazonSSMManagedInstanceCore* policy to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



New Protection Group

Cloud Permissions

Verify currently assigned IAM roles and permissions required for cloud machines' discovery and backup. You can enable automatic IAM role and permission configuration for machines with no roles present.

Protected EC2 instances must have an IAM role with the required permissions assigned. You can add required permissions to the currently assigned IAM role using the AWS Management Console, or enable automatic role creation for every machine in this protection group.

☑ Assign an IAM role with required permissions automatically

IAM role will be auto-assigned to all machines without any existing IAM roles present.

Click Validate to check the assigned IAM roles and their permissions now.

Step 7. Specify Discovery and Deployment Options

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

Veeam Backup & Replication regularly connects to protected machines 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 machines. 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 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, 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. To learn more, 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, consider the following:
   >
   > - You must add a repository using a general-purpose v2 storage account. Other account types are not supported.
   > - A Microsoft Azure Compute Account must be in the same subscription as the storage account specified in the settings of the Azure Blob Storage repository used as a distribution repository.
   > - You cannot add a repository using the Microsoft Entra ID account.

3. If you want to instruct Veeam Backup & Replication to automatically deploy Veeam Agents on all discovered machines 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 machine 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 and Veeam Transport Service on every machine added to the protection group even if the **Install backup agent** check box is not selected in the protection group settings. If Veeam Transport Service is already installed on a computer, Veeam Backup & Replication checks its version and upgrade Veeam Transport Service if a later version is available.

   > 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 machines when a new version of Veeam Agent appears on the Veeam Backup & Replication 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 machines] Select the **Install changed block tracking driver** check box if you want to install the advanced changed block tracking (CBT) driver on machines protected with Veeam Agent for Microsoft Windows.

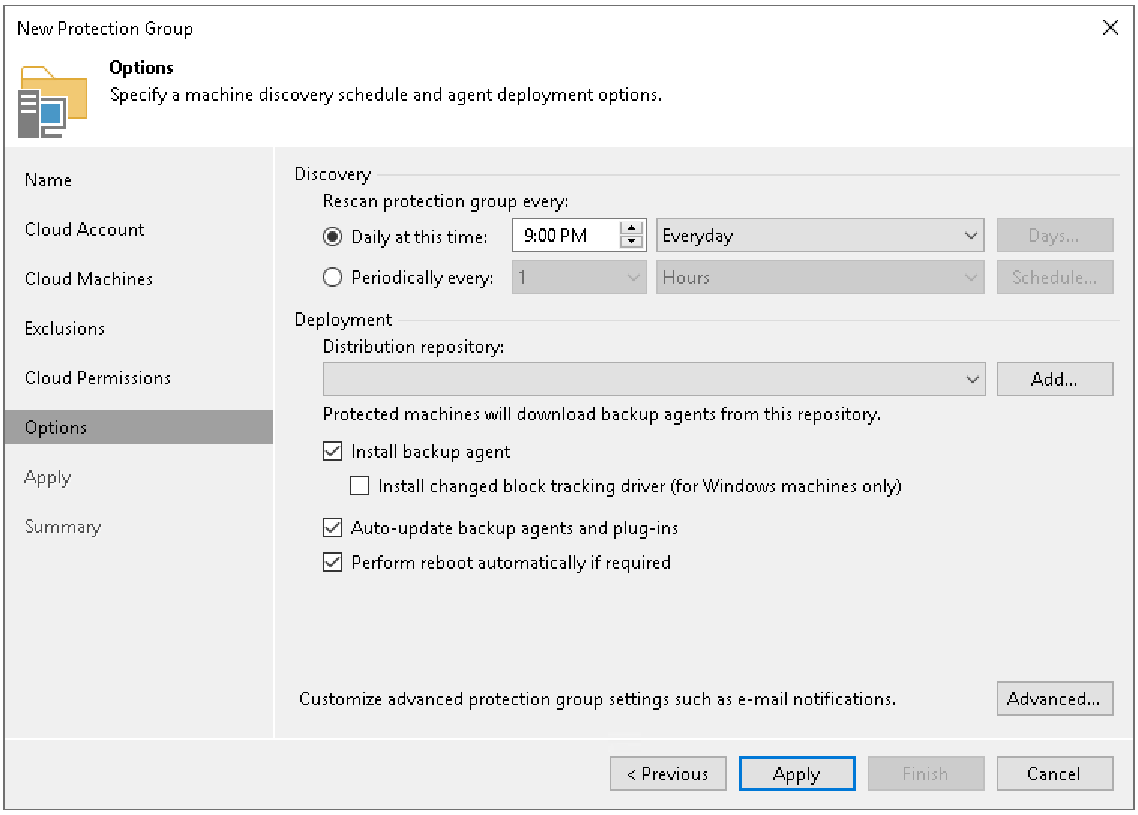
   Keep in mind that Veeam Backup & Replication will install the CBT driver only on those machines that run supported Microsoft Windows OS versions.

   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 machines 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 machine. 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.



New Protection Group

Options

Specify a machine discovery schedule and agent deployment options.

Discovery

Rescan protection group every:

● Daily at this time: 9:00 PM Everyday Days...

○ Periodically every: 1 Hours Schedule...

Deployment

Distribution repository:

Add...

Protected machines will download backup agents from this repository.

☑ Install backup agent

□ Install changed block tracking driver (for Windows machines only)

☑ Auto-update backup agents and plug-ins

☑ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications. Advanced...

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
   >
   > Consider 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.

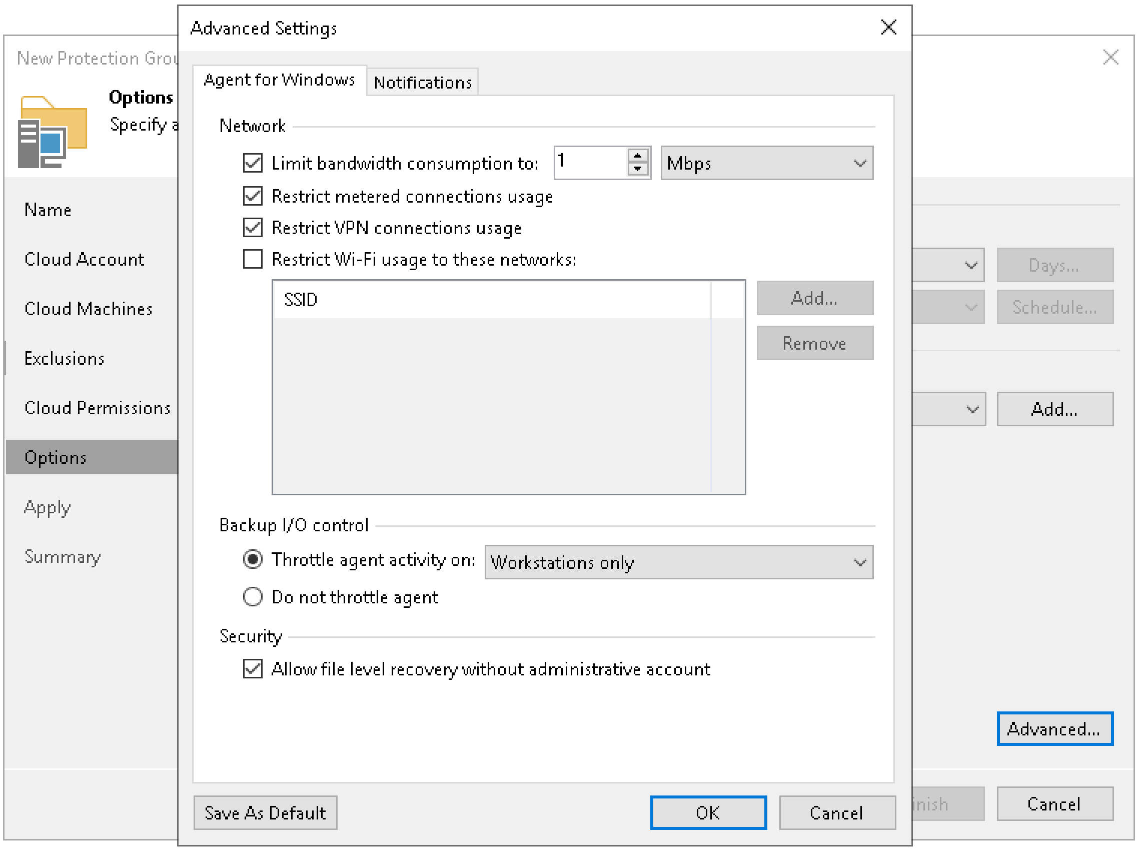
   > TIP
   >
   > If you want to restrict usage over any wireless networks, select the **Restrict Wi-Fi usage to these networks only** check box and do not add any networks to the list.

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 Restoring Files from Backup without Administrator Privileges.



Network

☑ Limit bandwidth consumption to: 1 Mbps

☑ Restrict metered connections usage

☑ Restrict VPN connections usage

□ Restrict Wi-Fi usage to these networks:

Backup I/O control

● Throttle agent activity on: Workstations only

○ Do not throttle agent

Security

☑ Allow file level recovery without administrative account

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.

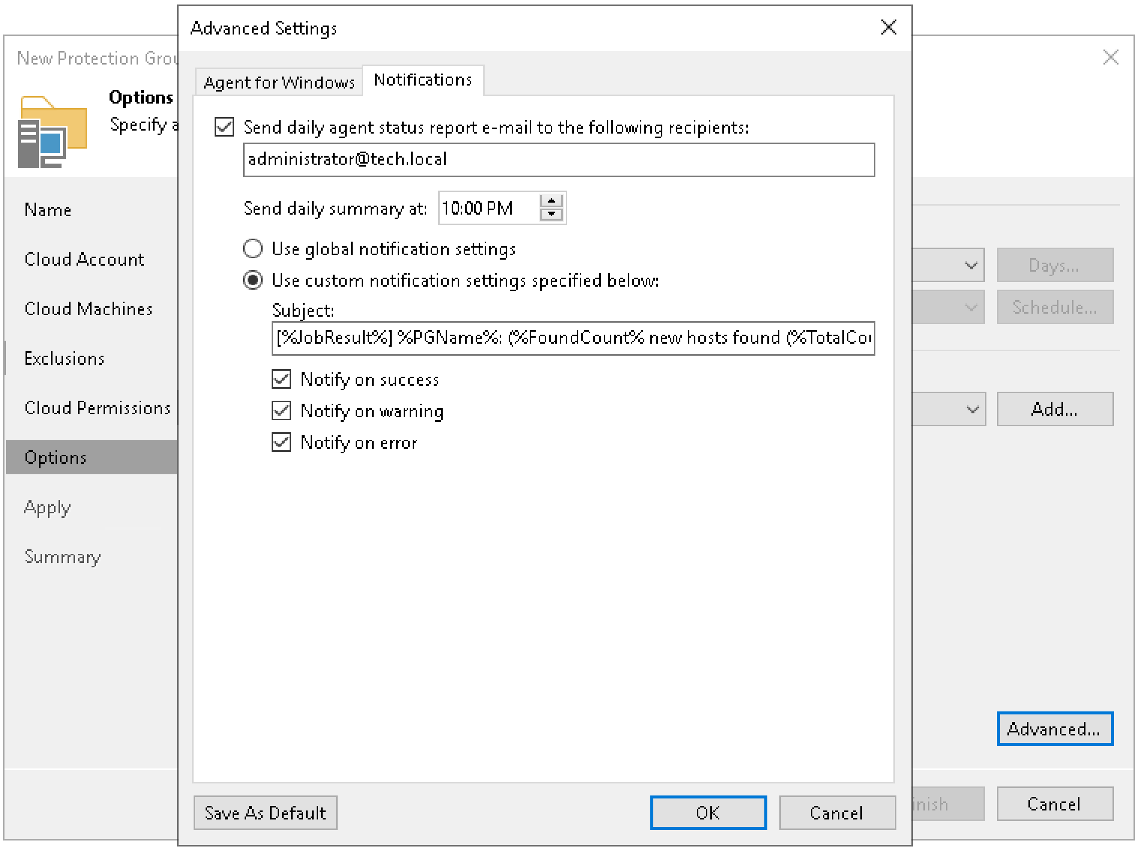
4. In the **Send daily summary at** field, specify the time when Veeam Backup & Replication must send the daily email report for the protection group.

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 **Notify on error** check boxes to receive email notification if the protection group rescan job completes successfully, completes with a warning or fails.



☑ Send daily agent status report e-mail to the following recipients:
administrator@tech.local

Send daily summary at: 10:00 PM

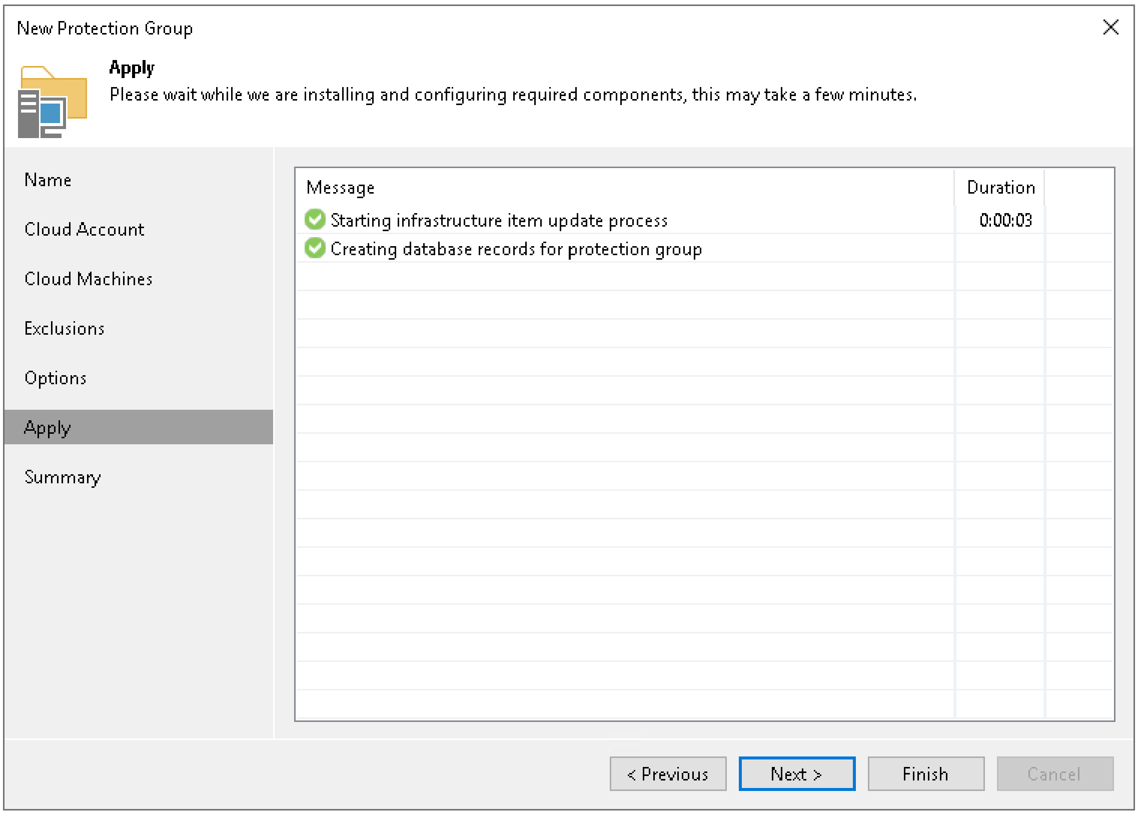
○ Use global notification settings
● Use custom notification settings specified below:

Subject:
[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success
☑ Notify on warning
☑ Notify on error

Step 9. 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.



New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

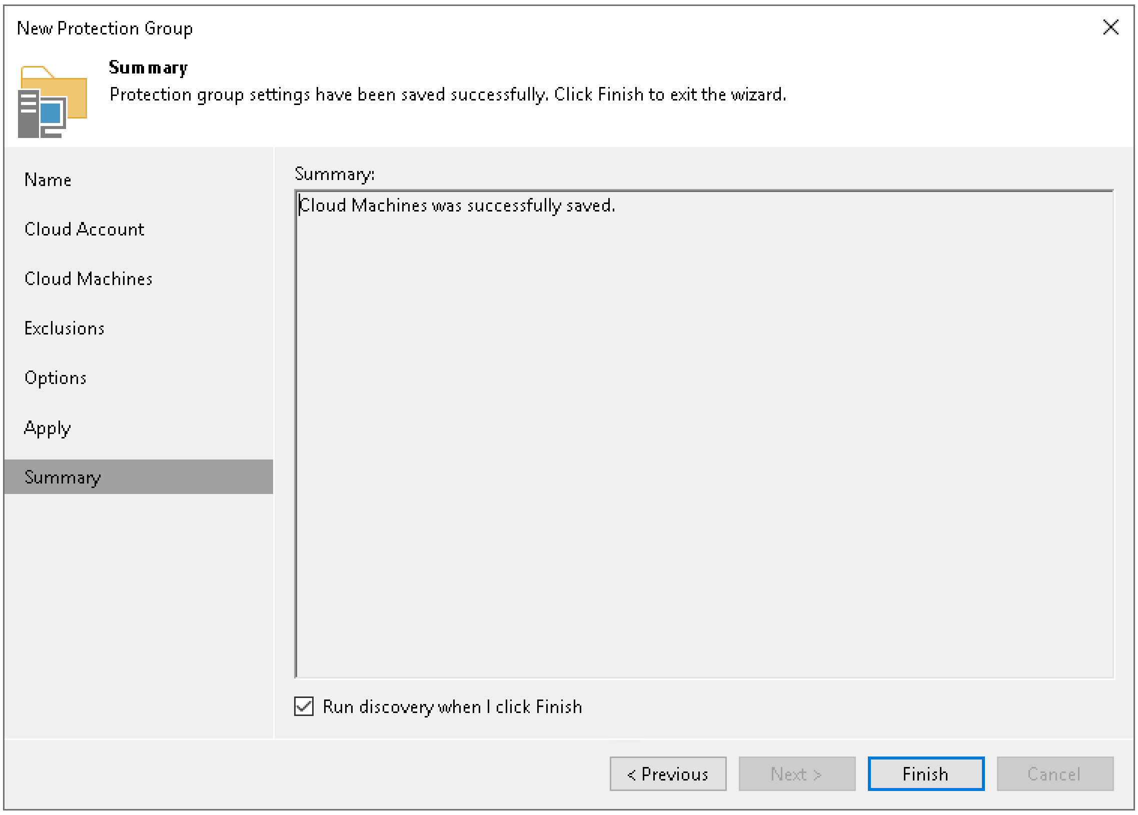
Message	Duration
✓ Starting infrastructure item update process	0:00:03
✓ Creating database records for protection group	

Step 10. 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**.



Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:

Cloud Machines was successfully saved.

☑ Run discovery when I click Finish

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 backup agents type. If you selected this protection group type, you must deploy Veeam Agents on the computers that you plan to protect.

Before You Begin

Consider the following before you start Veeam Agent deployment:

- 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 backup 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.
- If you migrate from one Veeam backup server to another, you must update Veeam backup server settings on each computer in the protection group for pre-installed Veeam Agents. To do this:
  a. Edit the protection group settings and regenerate setup files. To learn more, see Specifying Packages.

  b. Repeat the configuration step of the Veeam Agent deployment scenario using the regenerated configuration file.
- You must not install Veeam Agent on the server that is used as a hardened repository in the Veeam Backup & Replication infrastructure.

Deploying Veeam Agents

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/6.3.0.177` 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/6.3.0.177/VAW/x86/CRT`	`Windows6.1-KB2999226-x86.msu`
	Windows 8 or Windows Server 2012		`Windows8-RT-KB2999226-x86.msu`

OS Architecture	OS Version	File Location	File Name
	Windows 8.1 or Windows Server 2012 R2		`Windows8.1-KB2999226-x86.msu`
64-bit	Windows 7 or Windows Server 2008 R2	`<path_to_setup_files>/Windows/6.3.0.177/VAW/x64/CRT`	`Windows6.1-KB2999226-x64`
	Windows 8 or Windows Server 2012		`Windows8-RT-KB2999226-x64`
	Windows 8.1 or Windows Server 2012 R2		`Windows8.1-KB2999226-x64`

If the computer runs a later version of Microsoft Windows, skip this step.

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/6.3.0.177/VAW` folder

   For 64-bit Windows

   - Double-click the `Veeam_B&R_Endpoint_x64.msi` file located in the `<path_to_setup_files>/Windows/6.3.0.177/VAW` folder

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.

Consider 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

NOTE

You can also generate setup files for nosnap versions of Veeam Agent for Linux (including Veeam Agent for Linux on Power).

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. To learn more, see the Installing Veeam Agent for Linux in Offline Mode section in the Veeam Agent for Linux User Guide.

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.

Consider 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 Linux Using Pre-installed Veeam Deployer Service

You have an option to install Veeam Agent on Linux computers using certificate-based authentication instead of credentials. To do so, you must install Veeam Deployer Service on the computer and then add the computer to a protection group of the Individual computers type. In this case, Veeam Backup & Replication does not require SSH connection to install Veeam Agent for Linux.

> **IMPORTANT**
>
> You cannot use this deployment method to install and configure a nosnap Veeam Agent for Linux on Power.

Deploying Veeam Agent

To deploy Veeam Agent for Linux using pre-installed Veeam Deployer Service, perform the following steps:

1. On the Veeam Backup & Replication side, start a Veeam PowerShell session. For more information, see the Starting Veeam PowerShell Sessions in the Veeam PowerShell Reference.
2. Run the `Generate-VBRBackupServerDeployerKit` cmdlet to generate the Veeam Deployer Service temporary certificate and export the Veeam Backup & Replication Deployer Client certificate and Veeam Deployer Service installation packages. To learn more, see the Generate-VBRBackupServerDeployerKit section in the Veeam PowerShell Reference.
3. Upload the obtained files on the computer that you want to protect.
4. On the Veeam Agent computer side, navigate to the directory where you have saved the files and install Veeam Deployer Service using a package manager.
5. Run the following commands to install the certificates:

```
/opt/veeam/deployment/veeamdeploymentsvc --install-server-certificate server-cert.p12
/opt/veeam/deployment/veeamdeploymentsvc --install-certificate client-cert.pem
/opt/veeam/deployment/veeamdeploymentsvc --restart
```

6. On the Veeam Backup & Replication side, create a protection group with the following parameters:
   a. At the **Type** step of the wizard, select **Individuals computers**.
   b. At the **Computers** step of the wizard, specify a computer and select the **Connect using certificate-based authentication** method to connect to the computer.

   To learn more, see Creating Protection Groups.

After you create the protection group, Veeam Backup & Replication will rescan the protection group. During the rescan operation, Veeam Backup & Replication will replace the Veeam Deployer Service temporary certificate, connect to the Veeam Deployer Service and install Veeam Agent. To learn more, see Rescan Job.

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. To learn more, 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.

Consider 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. To learn more, see the Installing Veeam Agent section in the Veeam Agent for Mac User Guide.

3. Grant full disk access to Veeam Agent for Mac. To learn more, 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. To learn more, 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. To learn more, see the Importing Configuration from Backup Server 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. To learn more, see the 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.

Consider 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 a protection group for pre-installed Veeam Agents to a backup job for Mac computers and Linux computers with nosnap version of Veeam Agent for Linux (including Veeam Agent for Linux on Power) installed. 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 group. 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*.

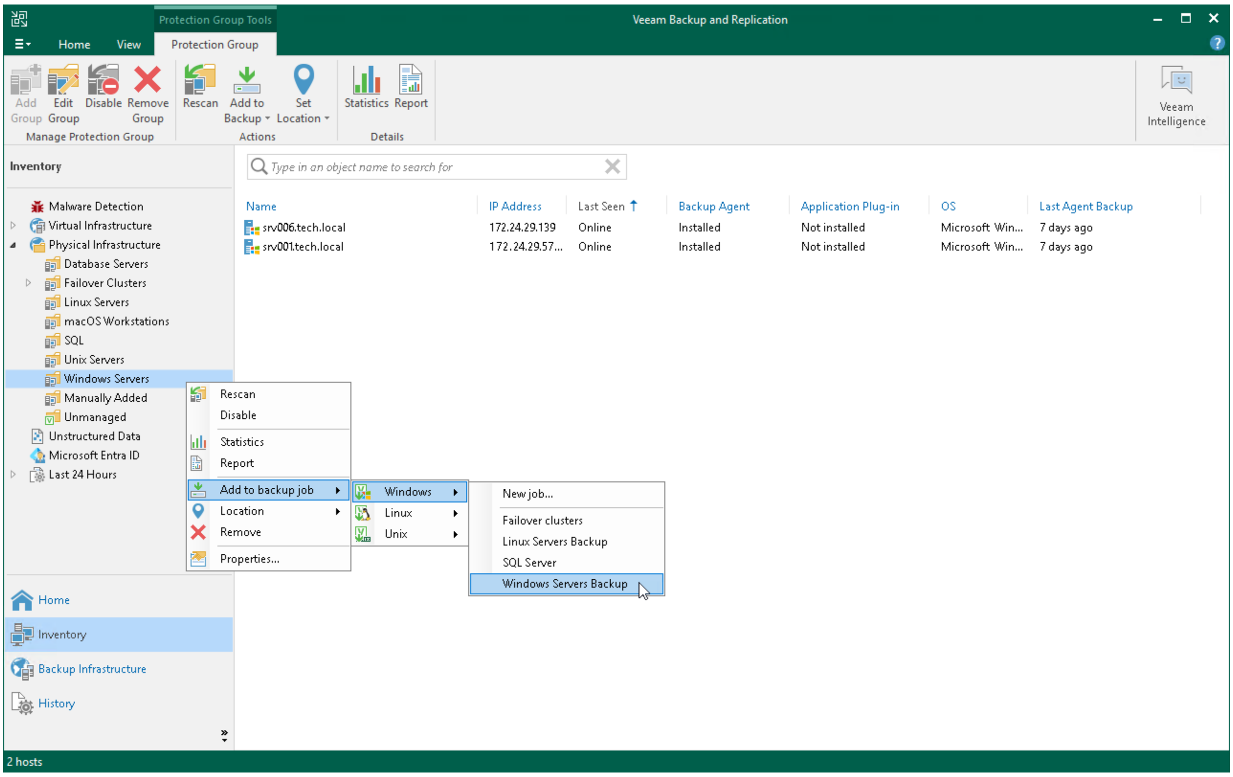
   For Unix computers

   - 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*.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

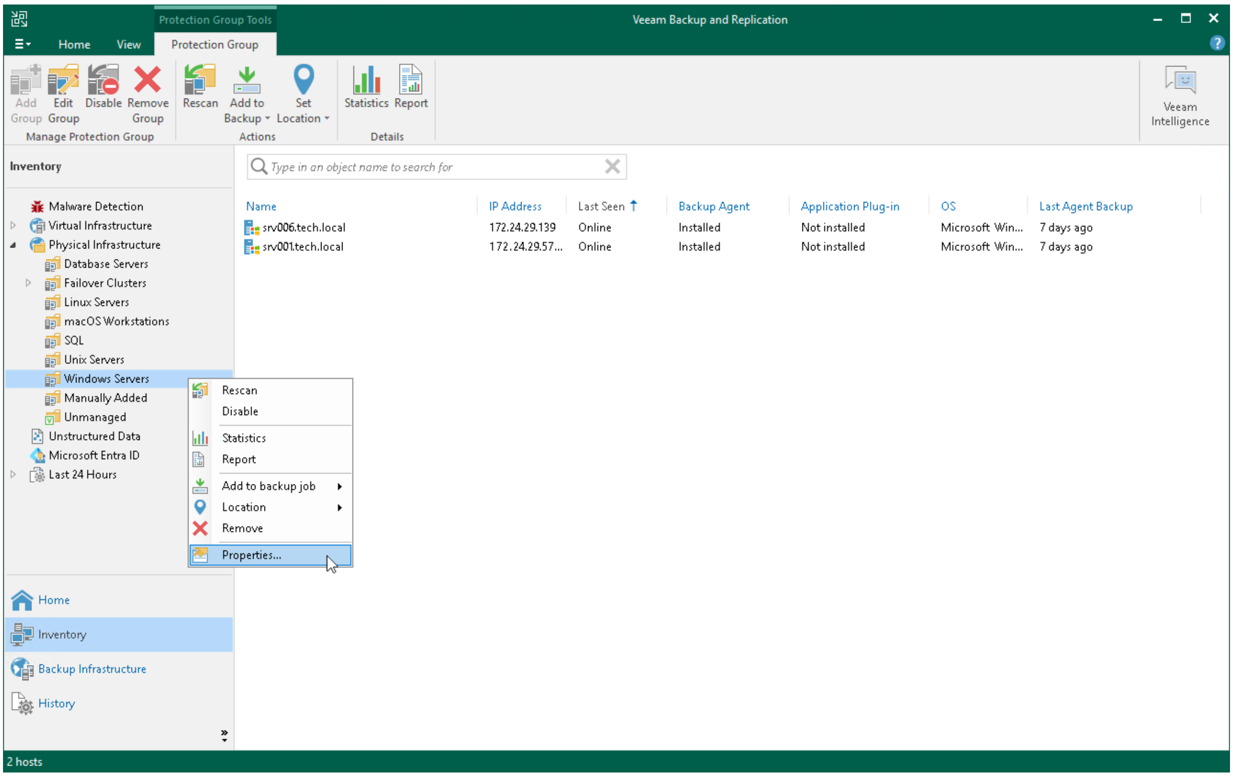
Editing Protection Group Settings

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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

Rescanning Protection Group

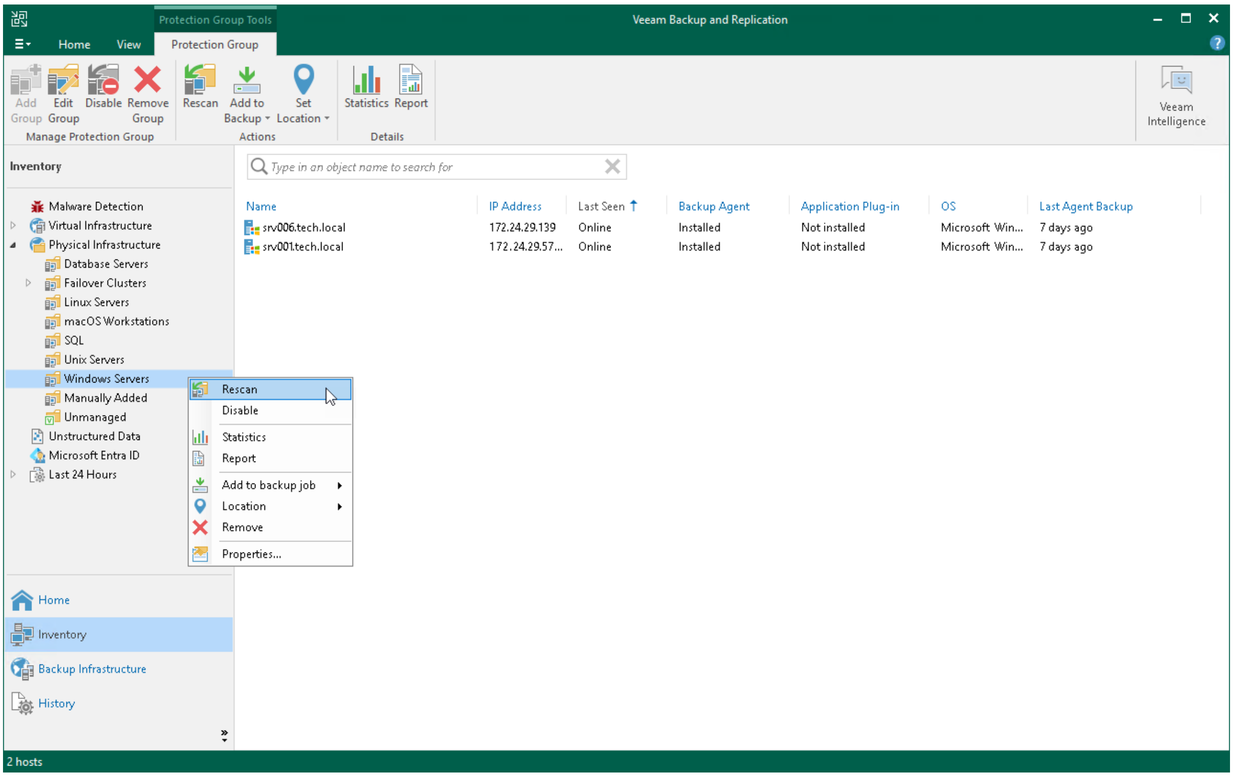
You can rescan a protection group configured in the inventory. When you perform protection group rescan, you manually start the discovery process for the protection group. This operation may be required, for example, if you want to discover new computers added to the protection group without waiting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



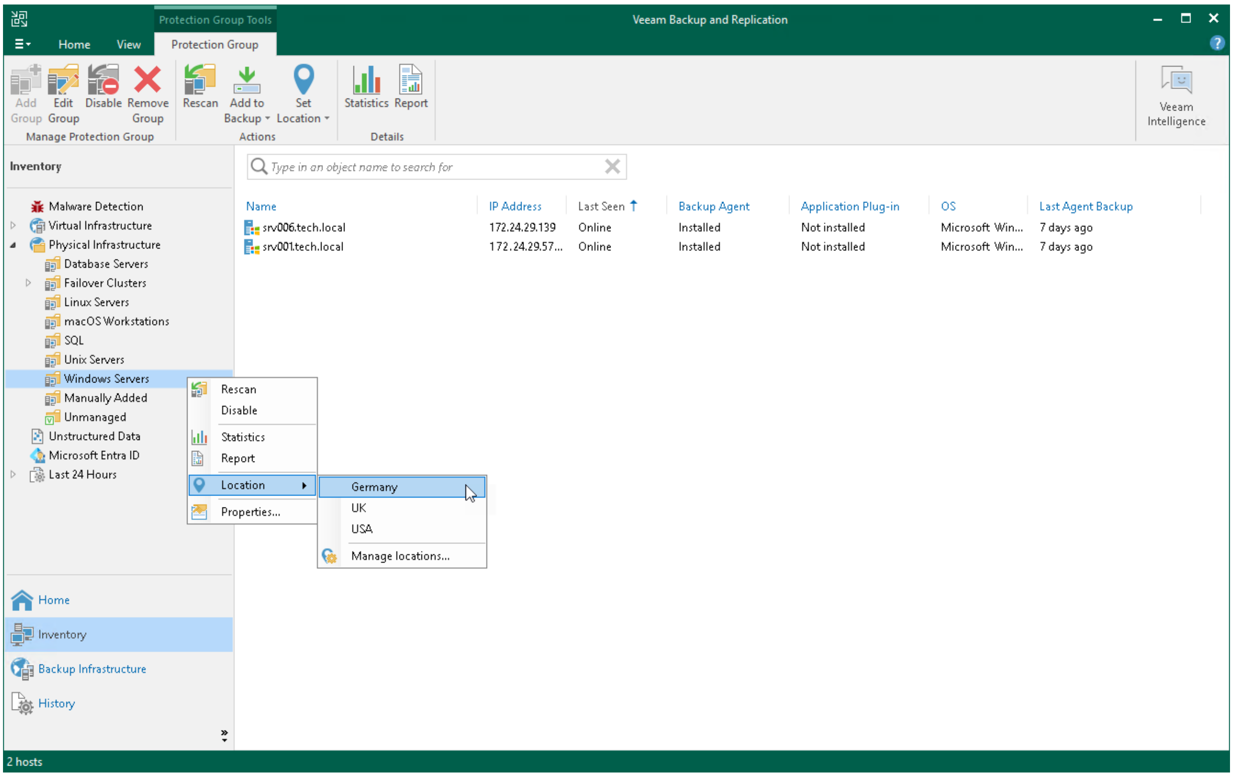
Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

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 the Veeam Backup & Replication 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:

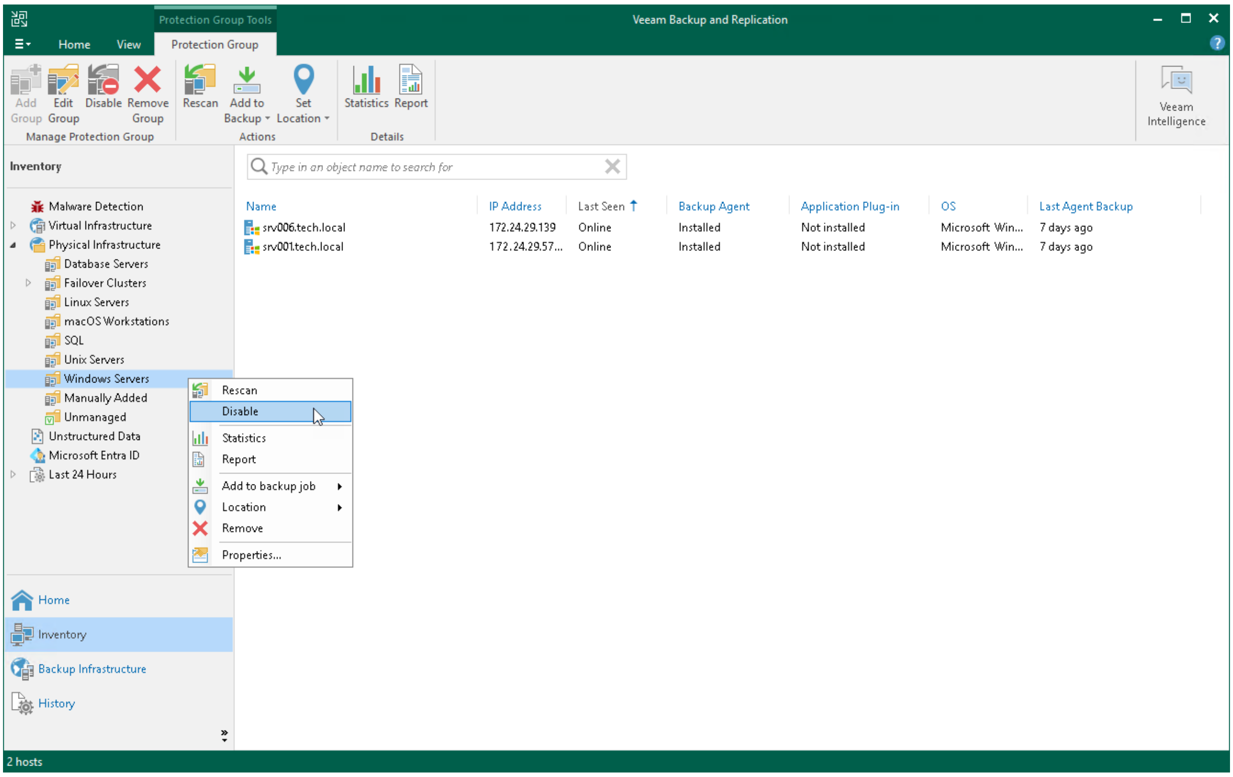
1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node.
3. In the inventory pane, select the necessary protection group and click **Disable** on the ribbon or right-click the necessary protection group and select **Disable**.

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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

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.

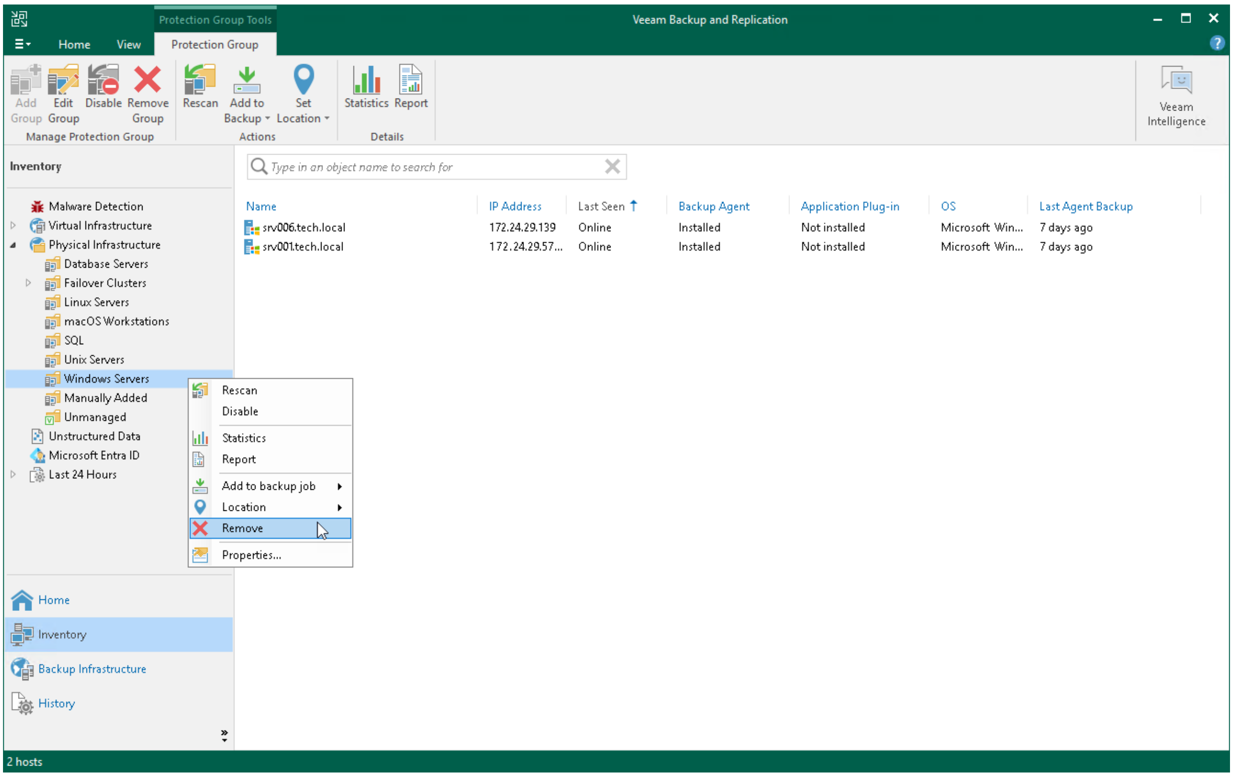
> NOTE
>
> Consider the following:
>
> - You cannot remove a protection group if the entire protection group or a separate computer included in this protection group is added to a Veeam Agent backup job.
> - You cannot remove default protection groups, such as *Manually Added*, *Unmanaged*, and so on.

> 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. [Not applicable for protection groups for pre-installed Veeam Agents] If you want to remove Veeam Agent deployed on protected computers, in the displayed window, select the **Uninstall everything** 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 other Veeam components from every computer in the deleted protection group. Veeam Backup & Replication will remove the same components that can be removed from a specific Veeam Agent computer. To learn more, see Uninstalling Veeam Agent and Other Veeam Components.

5. In the displayed window, click **Yes**.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

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.

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 job 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.

> TIP
>
> When Veeam Agent operates under control of Veeam Backup & Replication, all data protection, data restore and administration tasks can be performed from the Veeam Backup & Replication console. But some operations are also available on the Veeam Agent computer side. To learn more, see Operations Available on Veeam Agent Computer.

Related Topics

Veeam Agent Backup Jobs and Policies

Related Tasks

- Creating Agent Backup Job for Windows Computers
- Creating Agent Backup Policy for Windows Computers
- Creating Agent Backup Job for Linux Computers

- Creating Agent Backup Policy for Linux Computers
- Creating Agent Backup Policy for Unix Computers
- Creating Agent Backup Policy for Mac Computers

Creating Veeam Agent Backup Jobs

To create a Veeam Agent backup job managed by the backup server, you must create a backup job with the **Managed by backup server** option selected in the job settings. You will be able to add one or more individual computers and 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.

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 backup job managed by Veeam Agent (backup policy). To learn more, see Creating Policy for Unix Computers and Creating Policy for Mac Computers.

Creating Job for Windows Computers

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

Before You Begin

Before you create a Veeam Agent backup job managed by the backup server 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 workstations that you plan to add to the Veeam Agent backup job. To learn more, see Licensing Requirements.
- 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.

Veeam Agent backup jobs have the following limitations:

- You can store backups created by a Veeam Agent backup job 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 Creating Policy for Windows Computers.
- 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.
- You cannot map a Veeam Agent backup job managed by the backup server to a Veeam Agent backup chain created by another type of a Veeam Agent backup job. After you change the mode of a Veeam Agent computer, Veeam Backup & Replication starts a new backup chain in a target location specified in the backup job settings.
- The backup cache is not supported for Veeam Agent backup jobs managed by backup server.
- 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.
- You cannot add a Veeam Agent computer protected by a Veeam Agent backup policy to a backup job managed by the backup server. To add such a computer to a backup job managed by the backup server, first remove the computer from the Veeam Agent backup policy.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup job managed by the backup server 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 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 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:

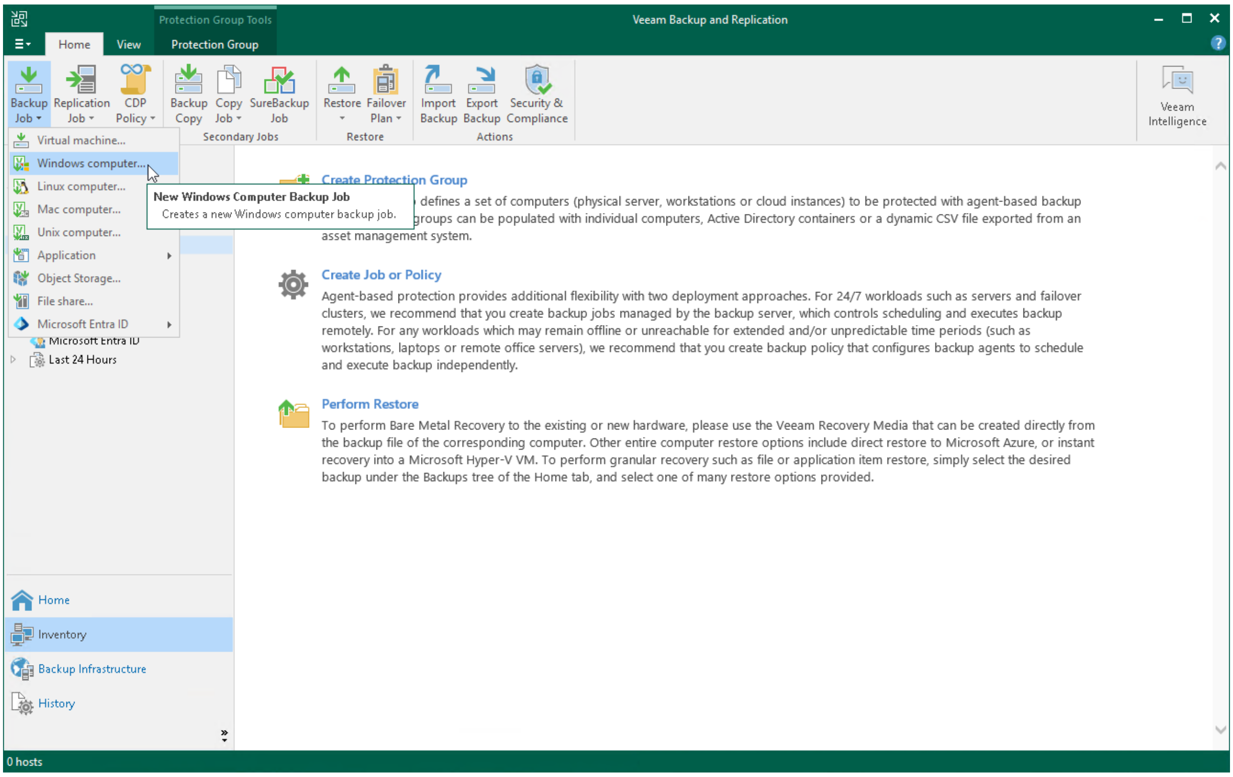
- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup job. In the working area, select one or more computers that you want to add to the job, right-click the selected computer and select **Add to backup job** >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

TIP

Consider the following:

- You can press and hold the [Ctrl] key 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.



New Windows Computer Backup Job

Creates a new Windows computer backup job.

Create Protection Group

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

Create Job or Policy

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

Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify protection settings for the Veeam Agent backup job managed by the backup server:

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 on servers, select the job mode.

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. For the backup job managed by backup server, you can select one of the following computer types:

- **Server** — select this option if you want to back up data on 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 the 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 on 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.

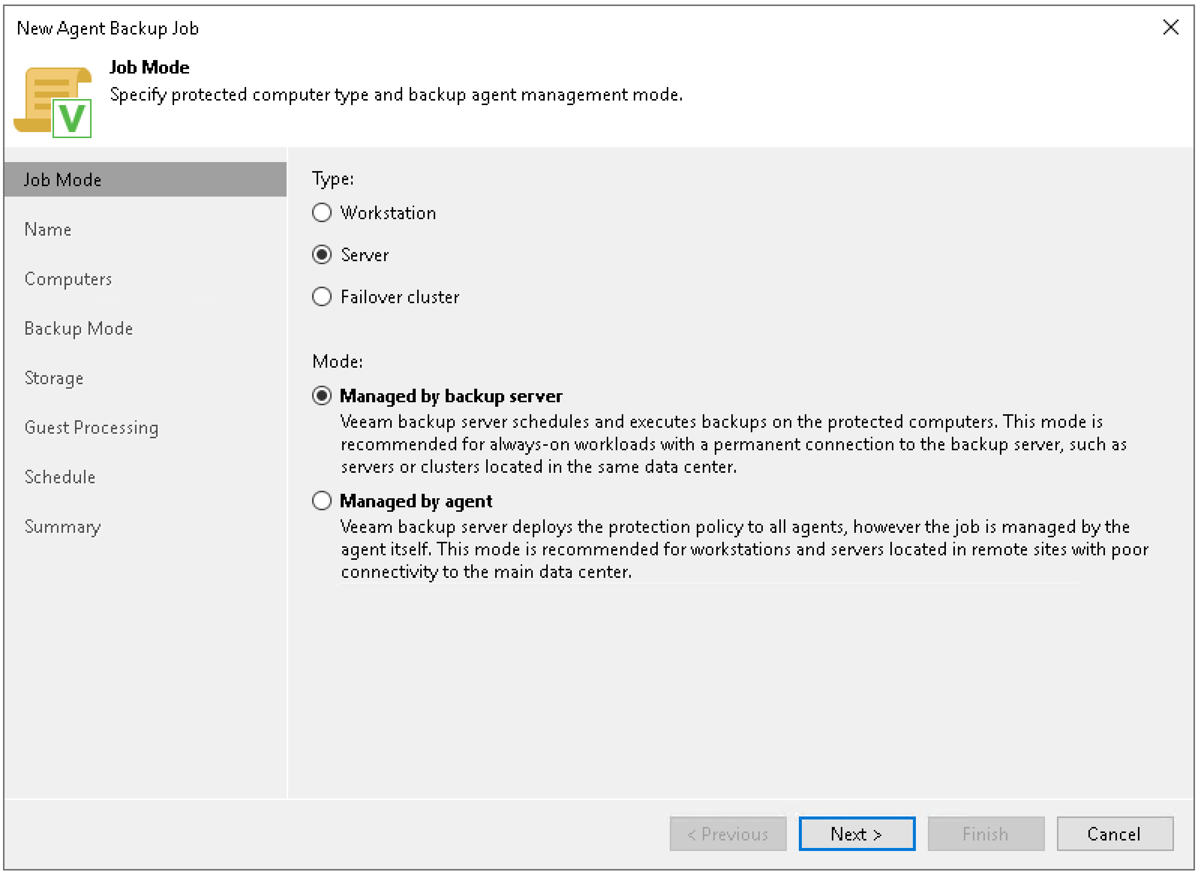
> NOTE
>
> You cannot select the **Workstation** option if you want to create a backup job managed by backup server.

Selecting Job Mode

If you selected the **Server** computer type in the **Type** field, in the **Mode** field, select the **Managed by backup server** job mode. If you select the **Managed by agent** job mode, you will create a Veeam Agent backup policy.

If you selected the **Failover cluster** computer type in the **Type** field, you do not need to select the job mode in the **Mode** field, the **Managed by backup server** job mode will be selected automatically.

If you want to create a Veeam Agent backup policy, see Creating Policy for Windows Computers.



New Agent Backup Job

Job Mode

Specify protected computer type and backup agent management mode.

Type:

○ Workstation

● Server

○ Failover cluster

Mode:

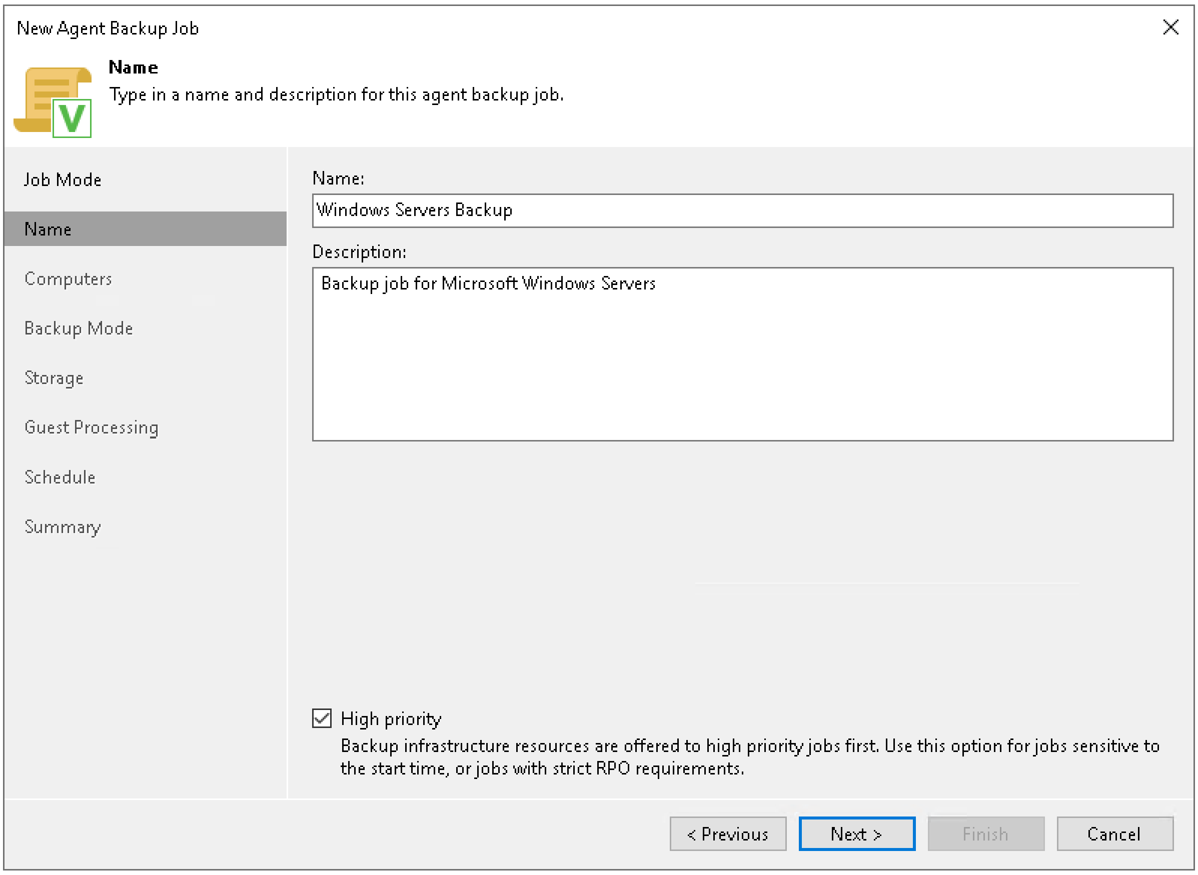
● **Managed by backup server**
Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

○ **Managed by agent**
Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

Step 3. Specify Job Name and Description

At the **Name** step of the wizard, specify a name and description for the Veeam Agent backup job managed by the backup server.

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. 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.



Name
Type in a name and description for this agent backup job.

Name: Windows Servers Backup

Description: Backup job for Microsoft Windows Servers

☑ High priority
Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and individual computers whose data you want to back up with the Veeam Agent backup job managed by the backup server.

You can add to the Veeam Agent backup job managed by the backup server one or more protection groups and individual computers from the Veeam Backup & Replication inventory. 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.

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

Adding Protection Groups and Computers from Inventory

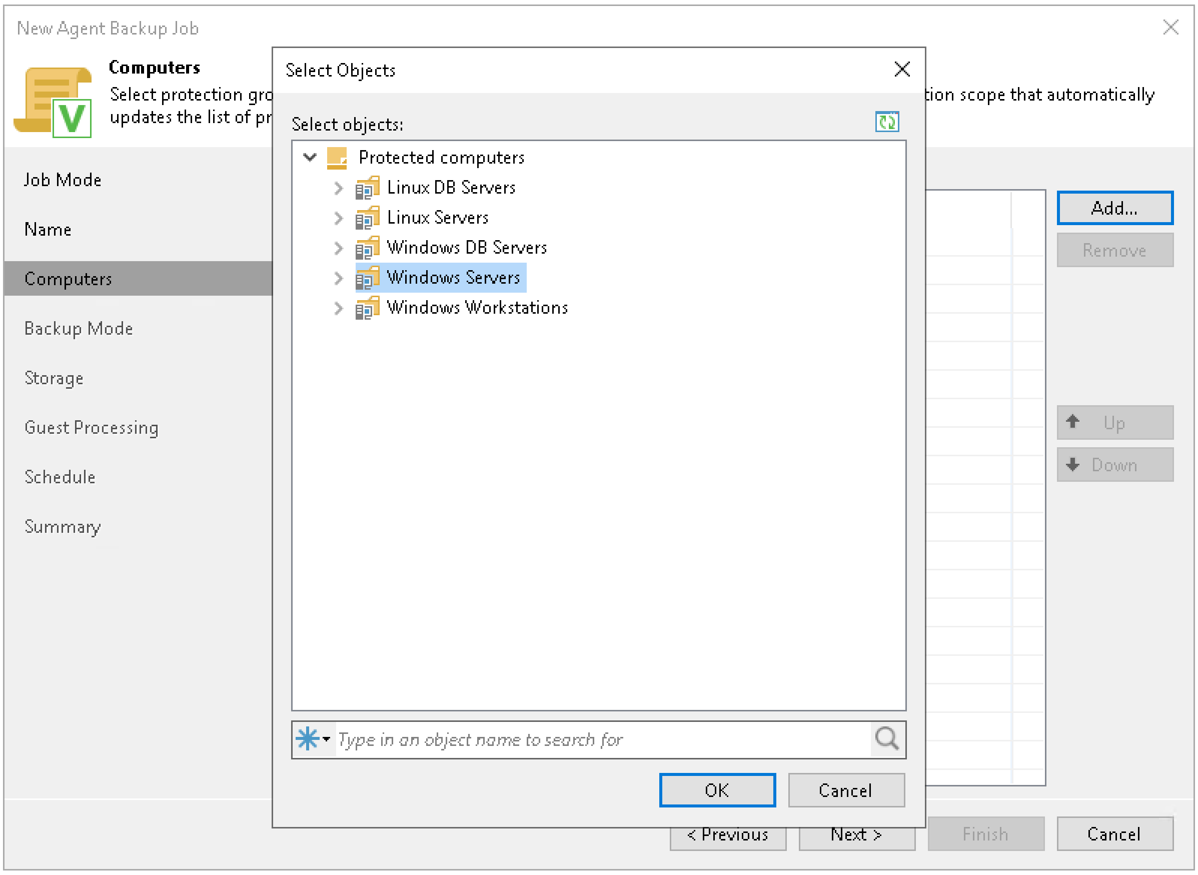
To add protection groups and individual computers to the Veeam Agent backup job, do the following:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and computers in the list and click **OK**. You can press and hold the [Ctrl] or [Shift] key 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].

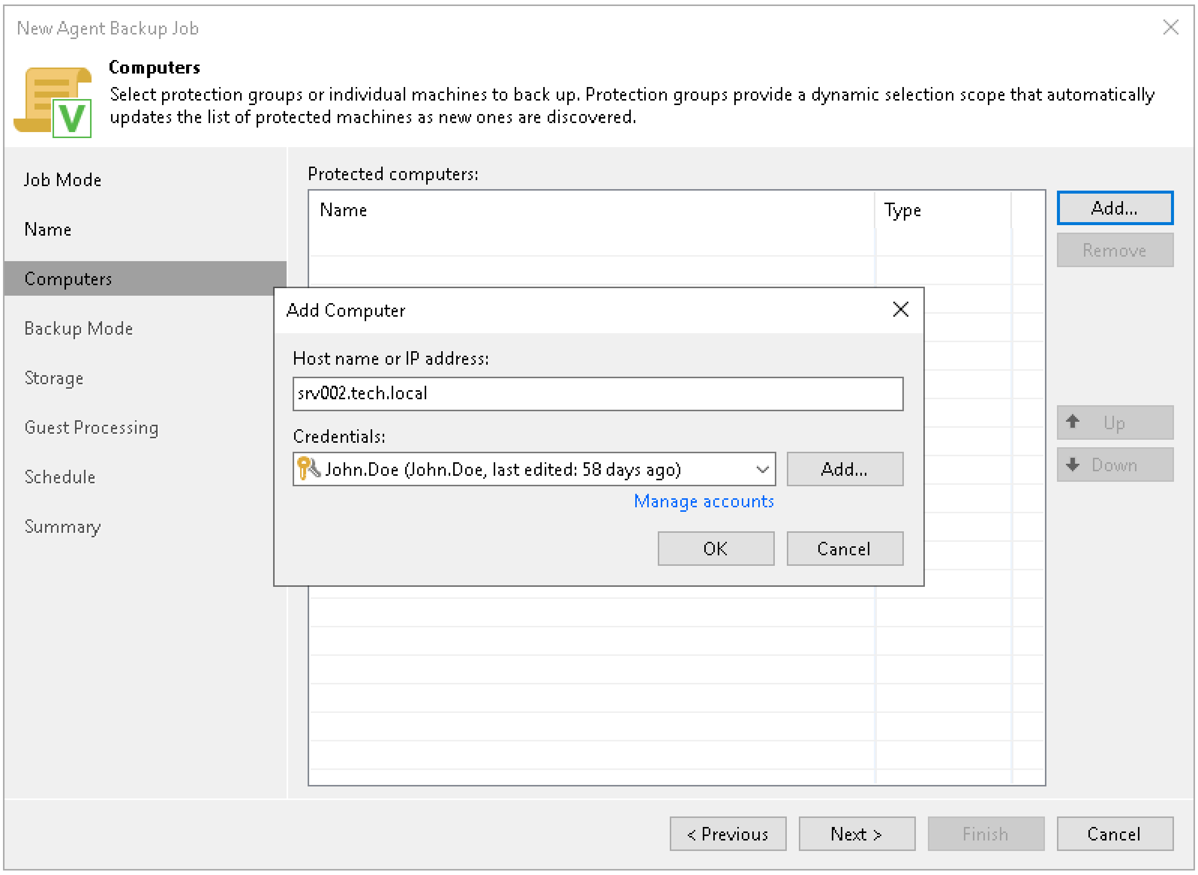


Adding New Computers

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

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.

After you complete the backup job configuration, the added computers will appear in the *Manually Added* protection group. To learn more, see Predefined Protection Groups.



New Agent Backup Job

Computers

Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

Protected computers:

Add Computer

Host name or IP address: srv002.tech.local

Credentials: John.Doe (John.Doe, last edited: 58 days ago)

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 Storage 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 located 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.

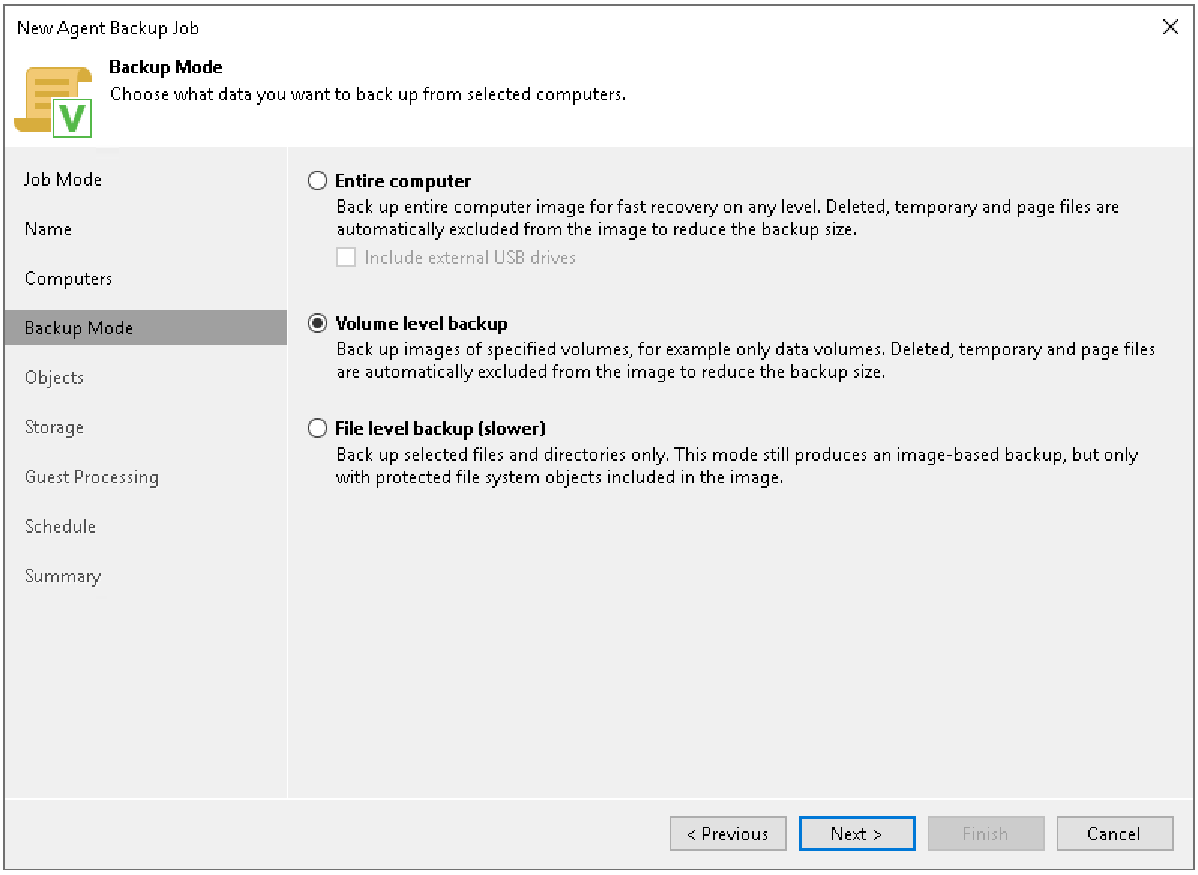
   - **File level backup** — select this option if you want to create a backup of individual folders on your computer. With this option selected, you will pass to the Objects step of the wizard.

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

Consider the following:

- The **File level backup** option is not available if you have selected the **Failover cluster** option at the Job Mode step of the wizard.
- File-level backup is typically slower than volume-level backup. Depending on the performance capabilities of your computer and backup environment, the difference between file-level and volume-level backup job performance may increase significantly. If you plan to back up all folders with files on a specific volume or back up large amount of data, we recommend that you configure volume-level backup instead of file-level backup.



Backup Mode

Choose what data you want to back up from selected computers.

○ **Entire computer**
Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
□ Include external USB drives

● **Volume level backup**
Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **File level backup (slower)**
Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.

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 managed by the backup server:

- 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 on 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, 2022 and 2025, 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.

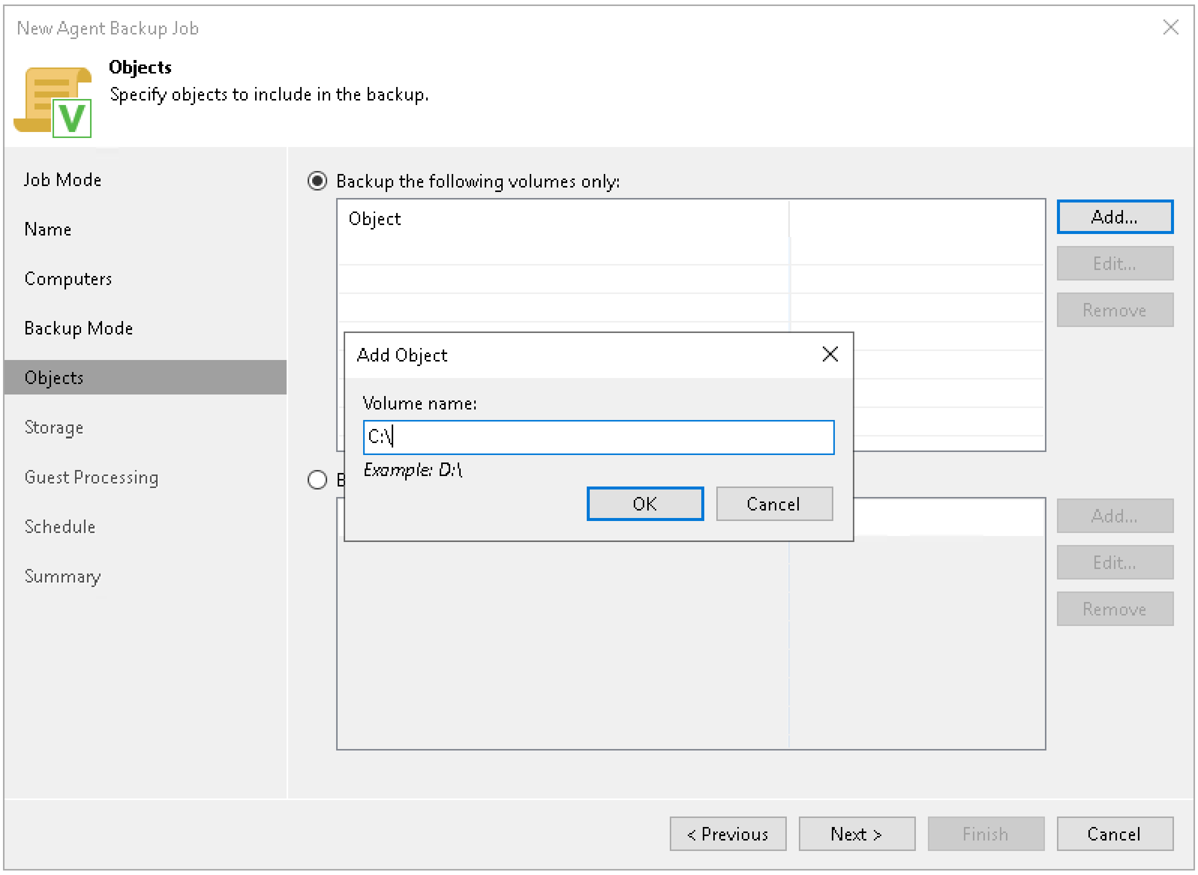
  b. In the **Add Object** window, type the path to a folder that is an entry point to the mounted volume you want to back up, for example, `C:\Data`, and click **OK**.

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

NOTE

Consider 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.



Add Object

Volume name: C:\

Example: D:\

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 by defining 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.

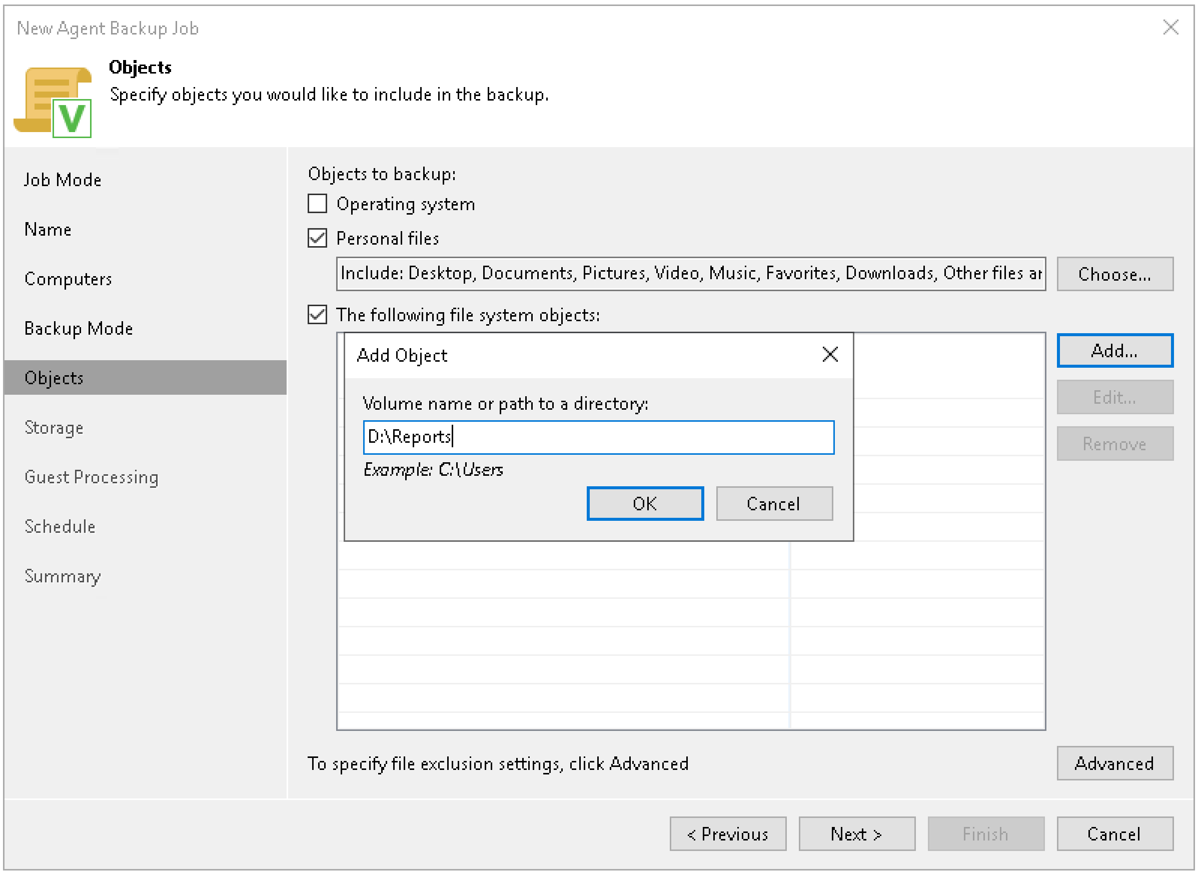
   Consider the following:

   - 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

Consider 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.



New Agent Backup Job

Objects

Specify objects you would like to include in the backup.

Objects to backup:

☐ Operating system

☑ Personal files

Include: Desktop, Documents, Pictures, Video, Music, Favorites, Downloads, Other files ar

☑ The following file system objects:

Add Object

Volume name or path to a directory:

D:\Reports

Example: C:\Users

To specify file exclusion settings, click Advanced

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.
- If you want to include or exclude files in/from the file-level backup, you can use file names and masks for file types as filters. You cannot use paths to files.

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 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 paths to folders that contain files that you do not want to back up and file names and 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 that reside in the backed-up folder except files in the specified folders and 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*`

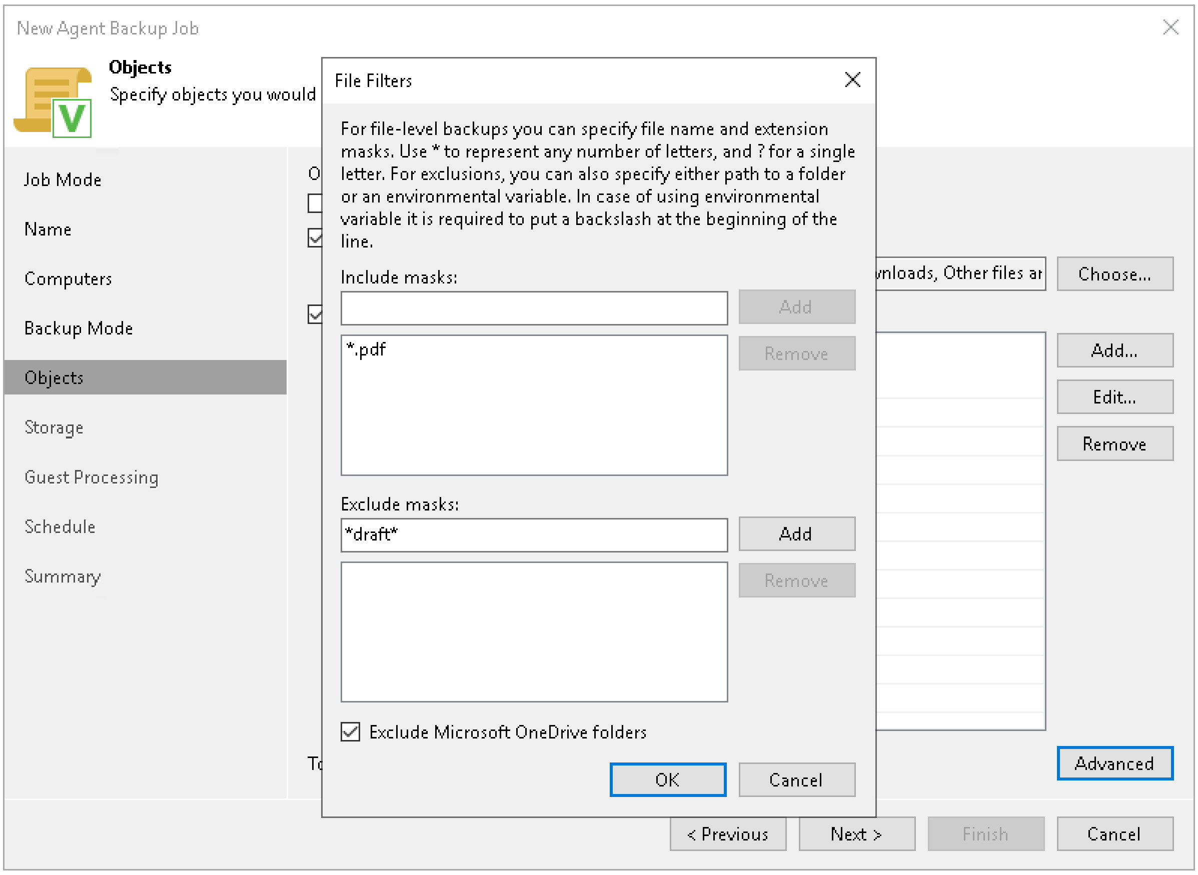
The resulting Veeam Agent backup will contain all files of the PDF format that do not contain *draft* in their names.

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 limitations:

- 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.



File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks: *.pdf

Exclude masks: *draft*

☑ Exclude Microsoft OneDrive folders

Step 7. Specify Backup Storage Settings

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
   >
   > 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:

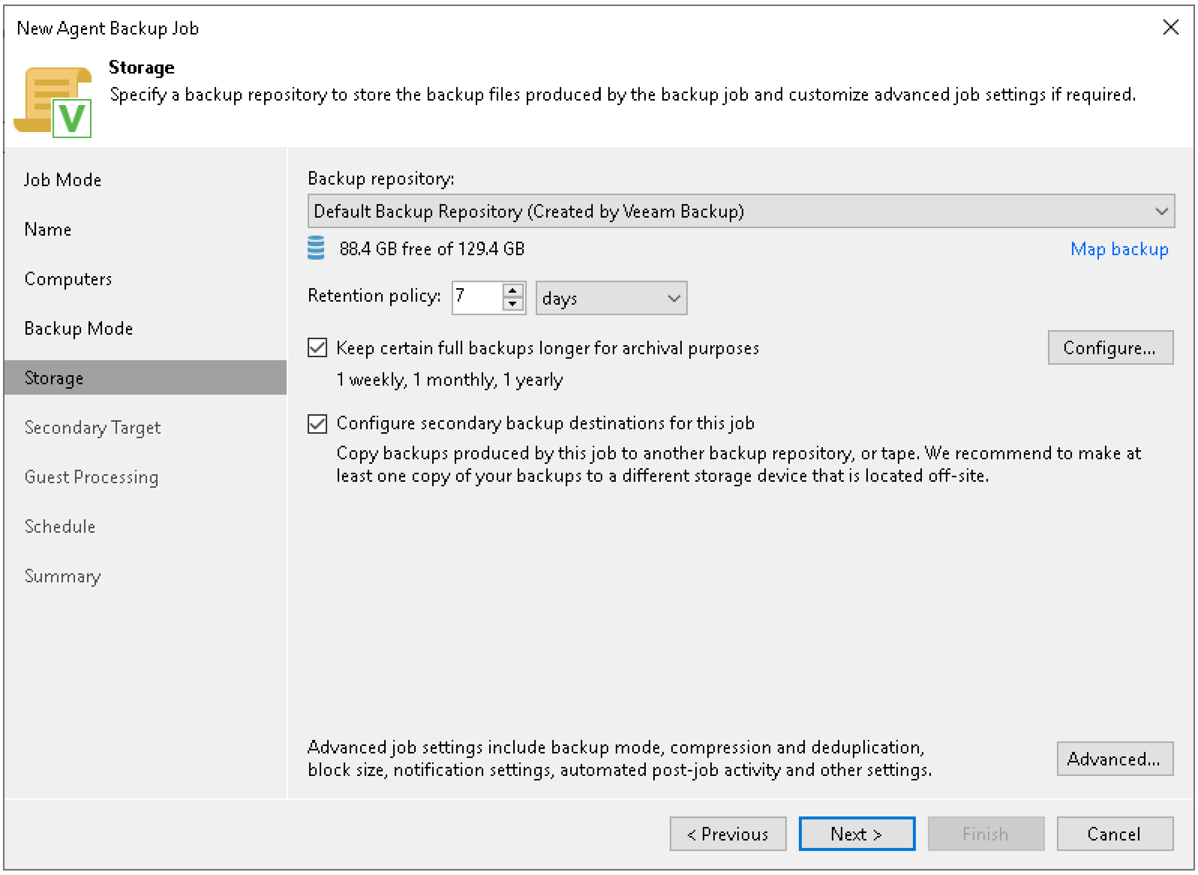
   - From the **Retention policy** list, select *restore points* and specify the number of restore points for which you want to store backup files in the target location. By default, Veeam Backup & Replication keeps backup files created for 7 latest restore points. After this number is exceeded, Veeam Backup & Replication removes 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 calendar days, including days when backup files are not created. After this period is over, Veeam Backup & Replication removes 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.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Default Backup Repository (Created by Veeam Backup)

88.4 GB free of 129.4 GB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

☑ Configure secondary backup destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Step 8. Specify Advanced Backup Settings

In the **Advanced Settings** window, specify advanced settings for the Veeam Agent backup job managed by the backup server:

- Backup settings
- Maintenance settings
- Storage settings
- Notification 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 the **Storage** step of the wizard.
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.

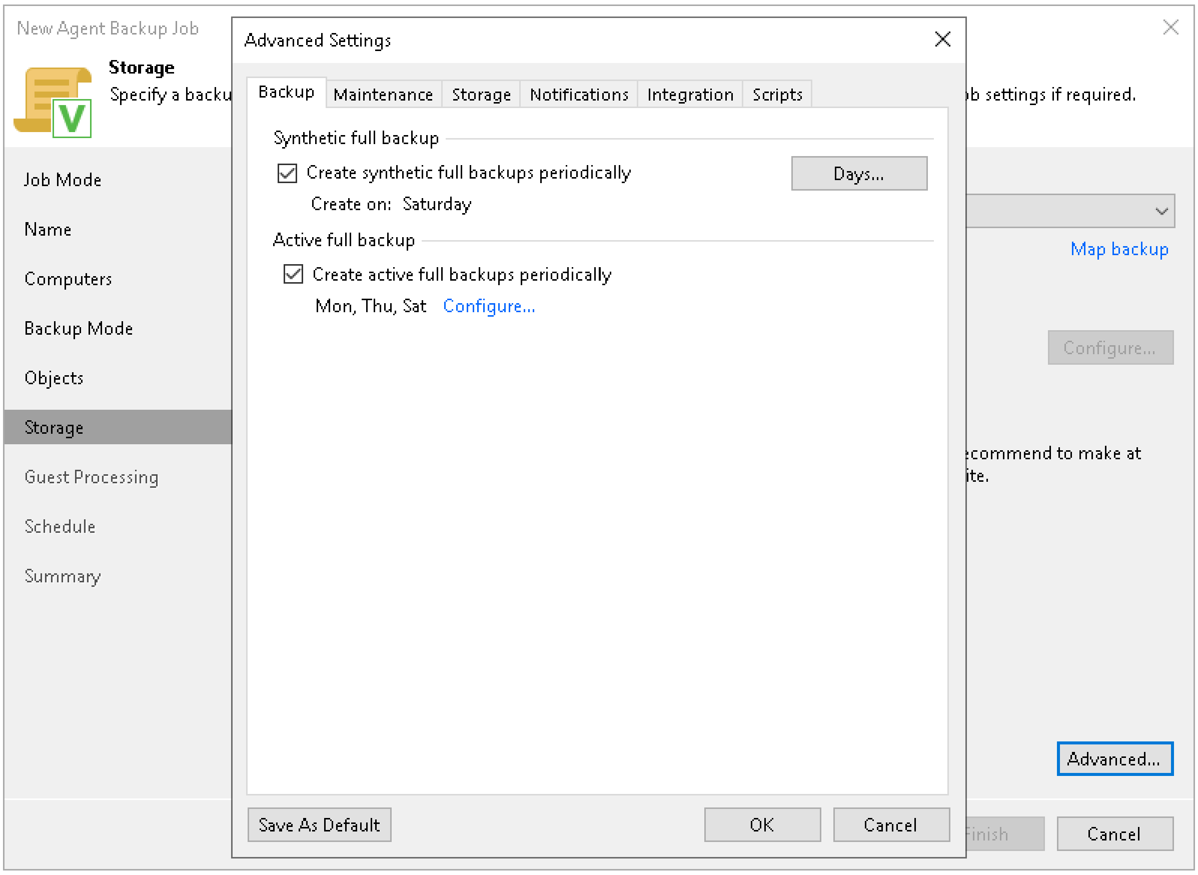
   > **NOTE**
   >
   > Synthetic full backup is not available for backup jobs targeted at an object storage repository.

3. If you want to periodically create active full backups, select the **Create active full backups periodically** check box. Click **Configure** and use the **Monthly on** or **Weekly** options to define scheduling settings.

NOTE

Consider the following:

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


Advanced Settings — Backup tab:

Synthetic full backup

☑ Create synthetic full backups periodically

Create on: Saturday

Active full backup

☑ Create active full backups periodically

Mon, Thu, Sat

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.

To specify maintenance settings for the backup job:

1. Click **Advanced** at the **Storage** step of the wizard.
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.

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 Items section in the Veeam Backup & Replication 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.

   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.

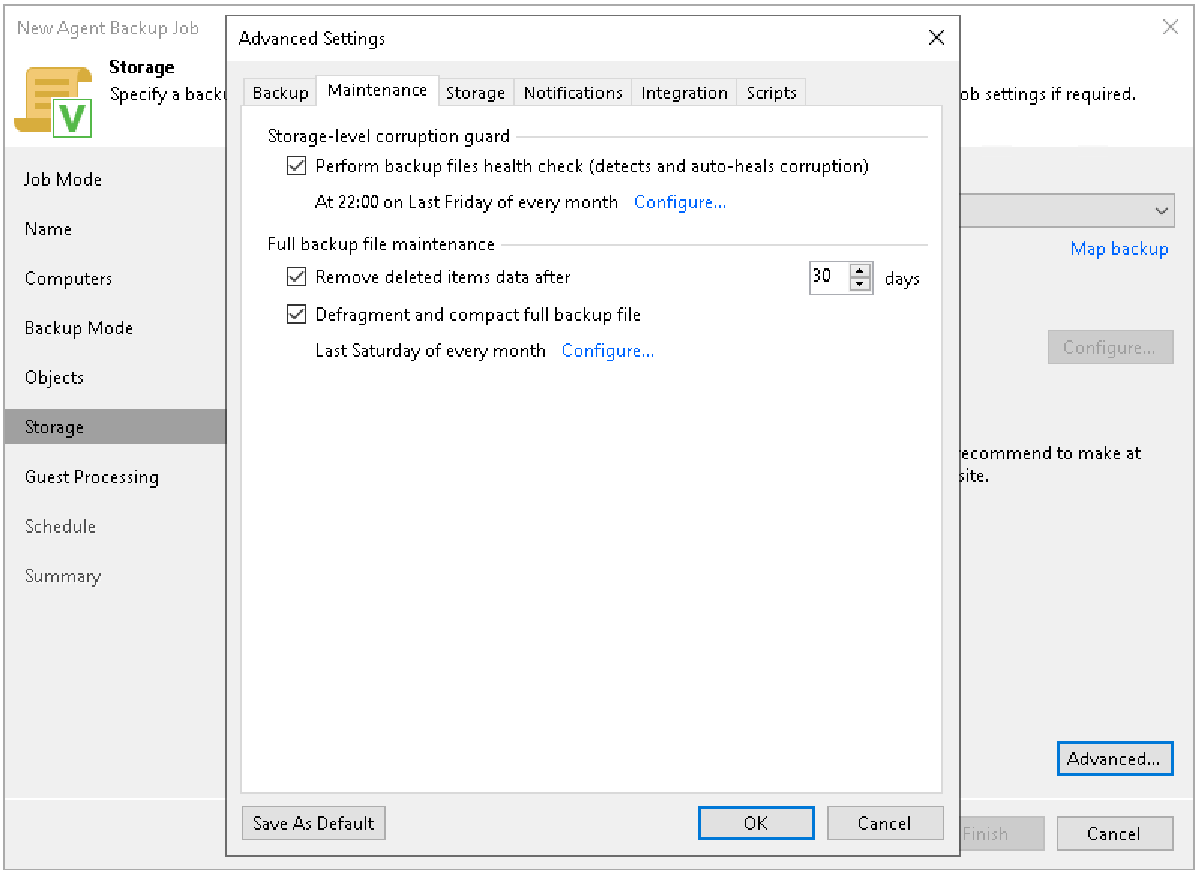
   > NOTE
   >
   > The **Defragment and compact full backup file** option is not available for backup jobs targeted at object storage.

   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.

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.



Advanced Settings — Maintenance tab

Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption)

At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 30 days

☑ Defragment and compact full backup file

Last Saturday of every month Configure...

Storage Settings

To specify storage settings for the backup job:

1. Click **Advanced** at the **Storage** step of the wizard.
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 **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*. To learn more about the compression levels, see the Data Compression section in the Veeam Agent for Microsoft Windows User Guide.

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.

   > NOTE
   >
   > If you change the storage optimization settings for the backup job, new settings will not have any effect on previously created files in the chain. They will be applied to new files created after the settings were changed.
   >
   > To apply new storage optimization settings in backup jobs, you must create an active full backup after you change storage optimization settings. Veeam Backup & Replication will use the new block size for the active full backup and subsequent backup files in the backup chain. To learn about the active full backup, see Performing Active Full Backup.

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.

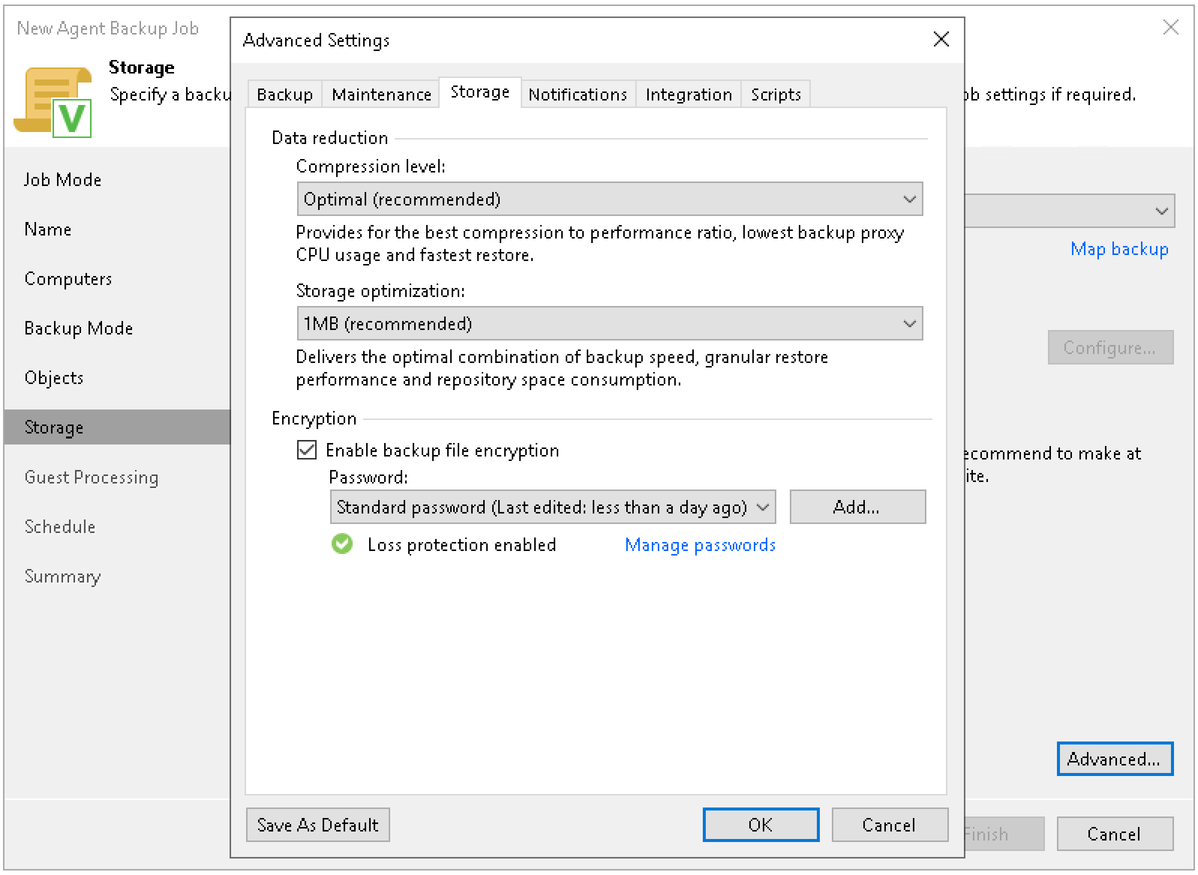
   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it. For more information, see the Decrypting Data Without Password section in the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

   You can select a Key Management System (KMS) server in the **Password** field. The KMS server must be added to Veeam Backup & Replication in advance. If you choose to use KMS keys for backup file encryption at this step of the wizard, Veeam Backup & Replication immediately starts communication with the KMS server to retrieve the encryption keys. To learn more, see the Key Management System Keys section in the Veeam Backup & Replication User Guide.

NOTE

Consider the following:

- If you plan to encrypt the content of backup files, consider the limitations listed in the Data Encryption Limitations subsection.
- You must encrypt the backup job if you want to back up data to the Veeam Data Vault storage.



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

Data Encryption Limitations

If you plan to encrypt the content of backup files, consider the following limitations:

- Data encryption settings for Veeam Agent backup jobs configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database.
- If you enable or disable 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 Backup & Replication will encrypt the backup chain starting from the next restore point created with this job.

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

Notification Settings

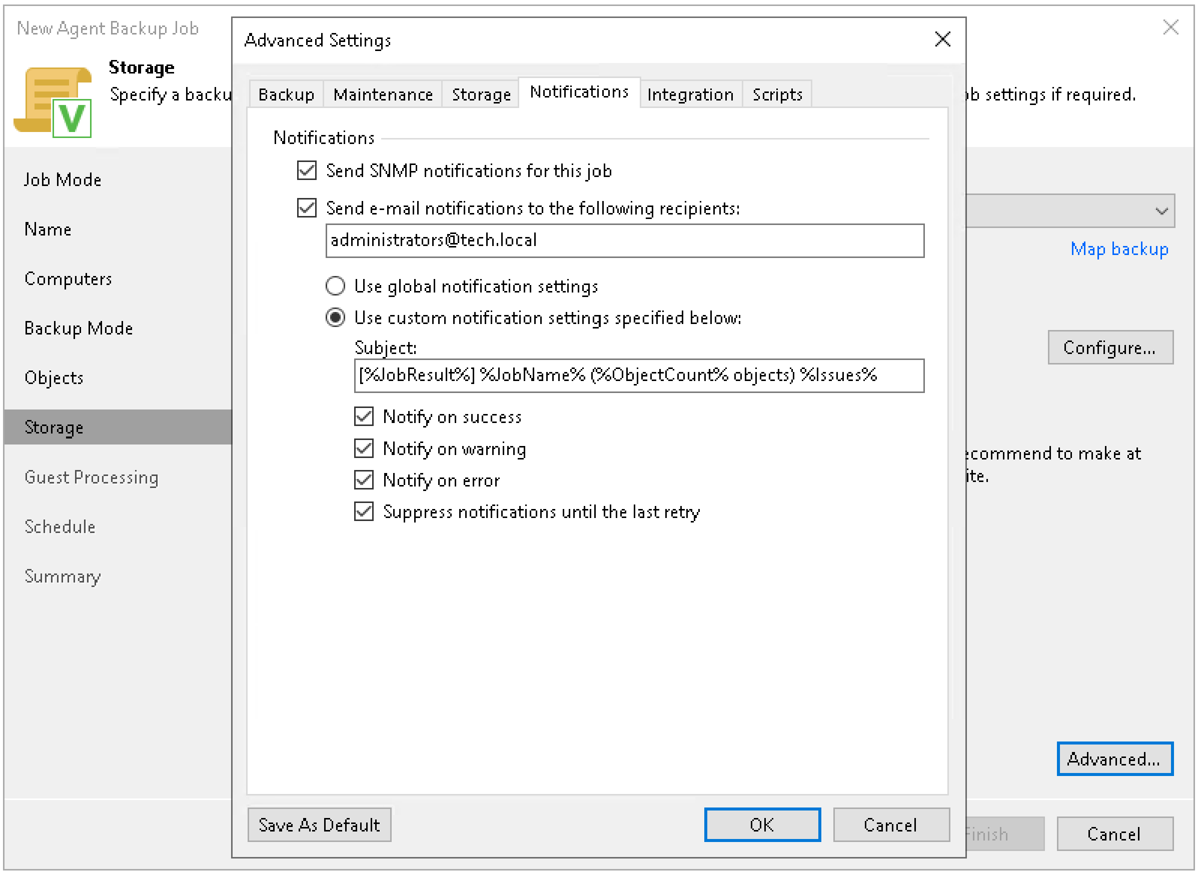
You can specify notification settings for Veeam Agent backup jobs configured in Veeam Backup & Replication. To specify notification settings:

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.



Notifications

☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrators@tech.local

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

☑ Notify on error

☑ Suppress notifications until the last retry

Integration Settings

You can specify storage integration settings for the job managed by backup server.

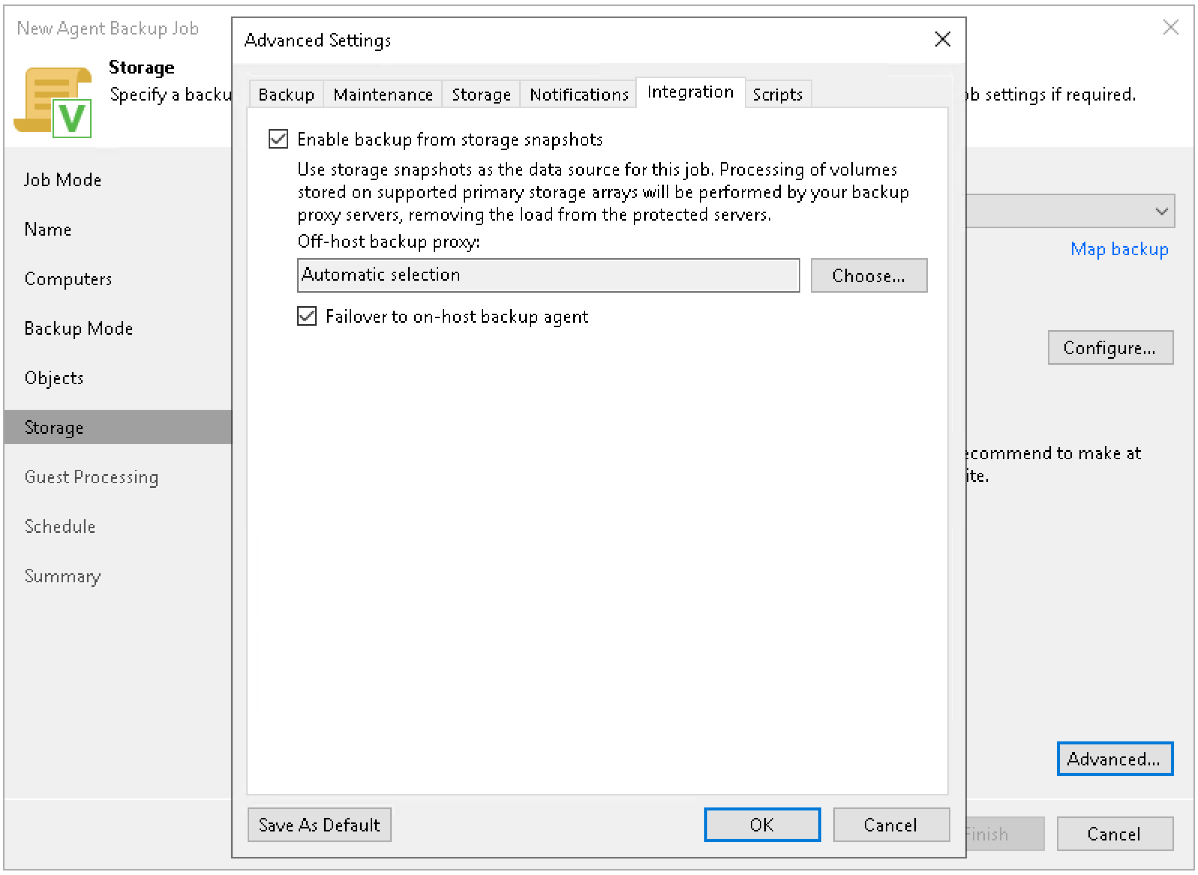
Keep in mind that storage integration settings are unavailable if you work with protection group for cloud machines.

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.



☑ Enable backup from storage snapshots

Use storage snapshots as the data source for this job. Processing of volumes stored on supported primary storage arrays will be performed by your backup proxy servers, removing the load from the protected servers.

Off-host backup proxy: Automatic selection

☑ Failover to on-host backup agent

Selecting Off-Host Backup Proxy

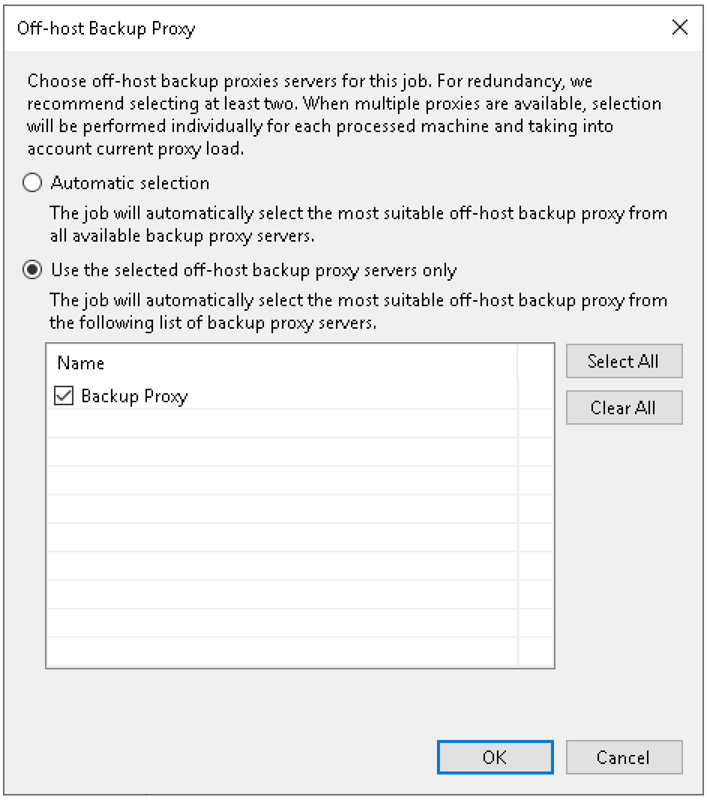
To specify what backup proxies Veeam Backup & Replication will use during the backup process, click **Choose** and select one of the following options in the **Off-host Backup Proxy** window:

- 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.


Off-host Backup Proxy

Choose off-host backup proxies servers for this job. For redundancy, we recommend selecting at least two. When multiple proxies are available, selection will be performed individually for each processed machine and taking into account current proxy load.

○ Automatic selection

The job will automatically select the most suitable off-host backup proxy from all available backup proxy servers.

● Use the selected off-host backup proxy servers only

The job will automatically select the most suitable off-host backup proxy from the following list of backup proxy servers.

Name
☑ Backup Proxy

Script Settings

You can specify script settings for the job managed by backup server.

To specify script settings for the backup job:

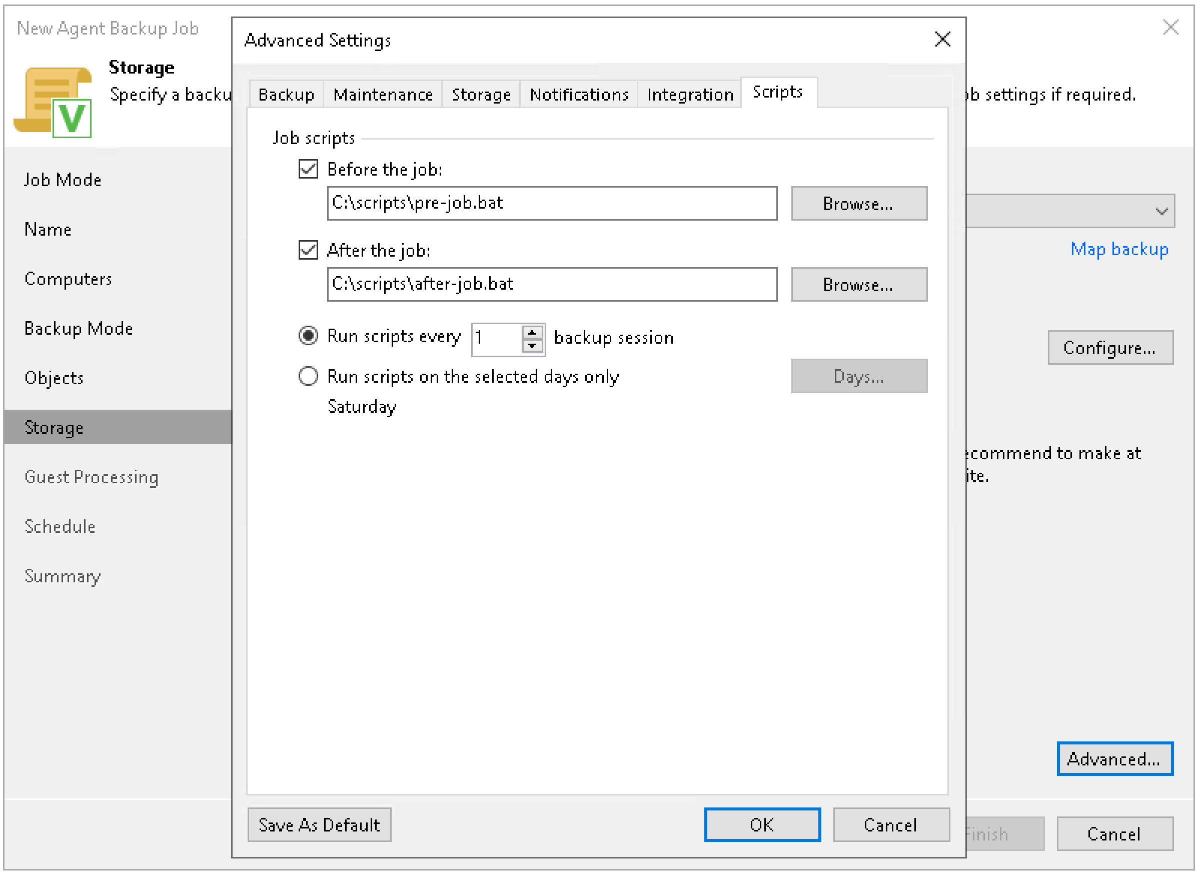
1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Scripts** tab.
3. If you want to execute custom scripts before or after the backup job, select the **Before the job** or **After the job** check boxes and click **Browse** to choose executable files from a local folder on the 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.



Job scripts

☑ Before the job:

C:\scripts\pre-job.bat

☑ After the job:

C:\scripts\after-job.bat

● Run scripts every 1 backup session

○ Run scripts on the selected days only

Saturday

Step 9. Specify Secondary Target

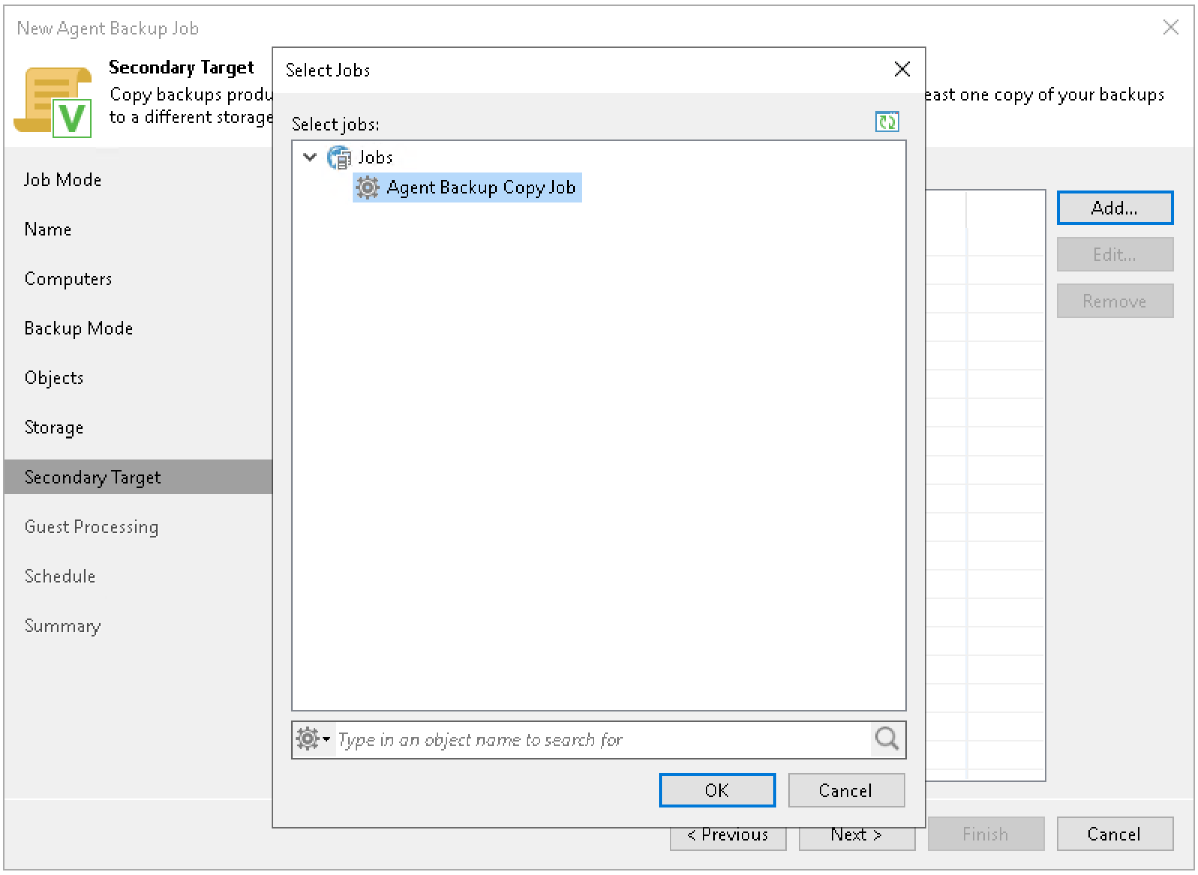
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the 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:

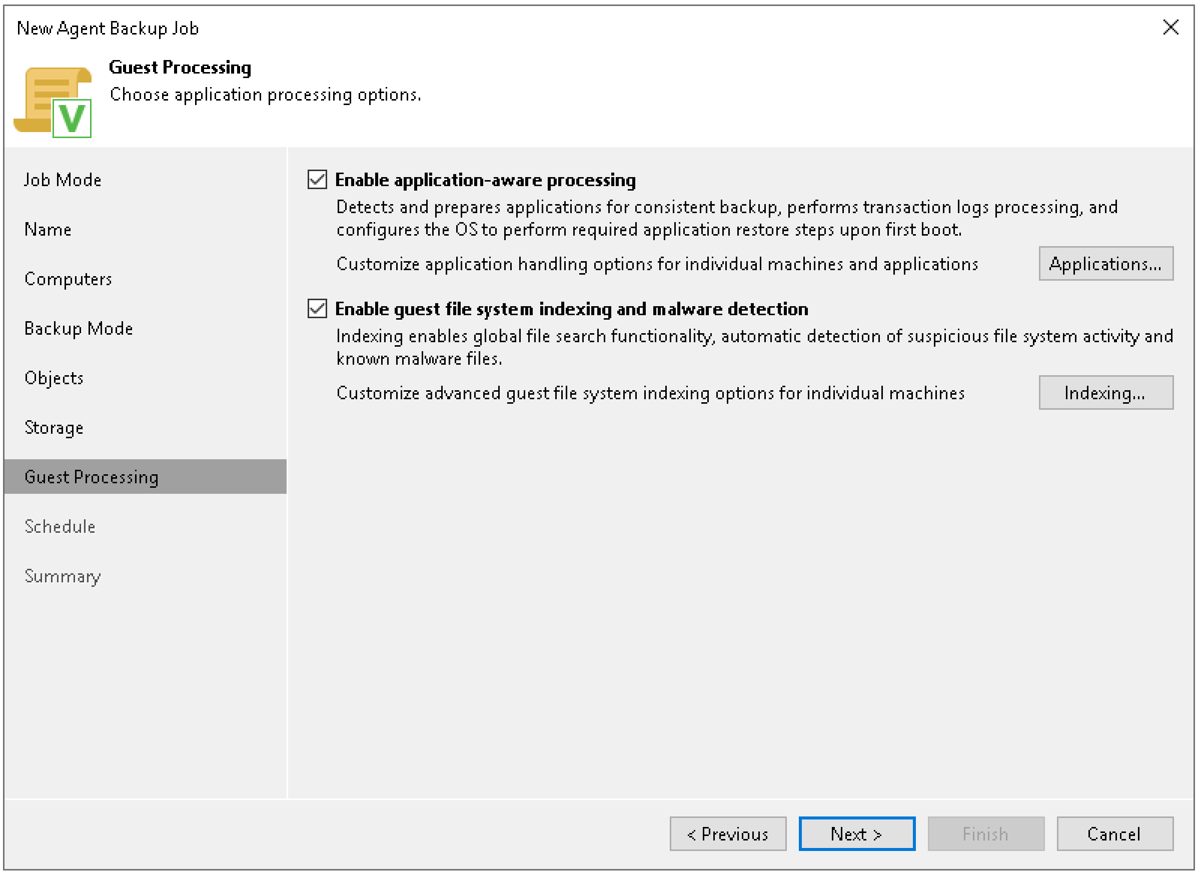
1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the Veeam Agent backup job. You can link several jobs to the backup job — for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom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



Step 10. Specify Guest Processing Settings

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

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



☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing and malware detection**

Indexing enables global file search functionality, automatic detection of suspicious file system activity and known malware files.

Customize advanced guest file system indexing options for individual machines

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.

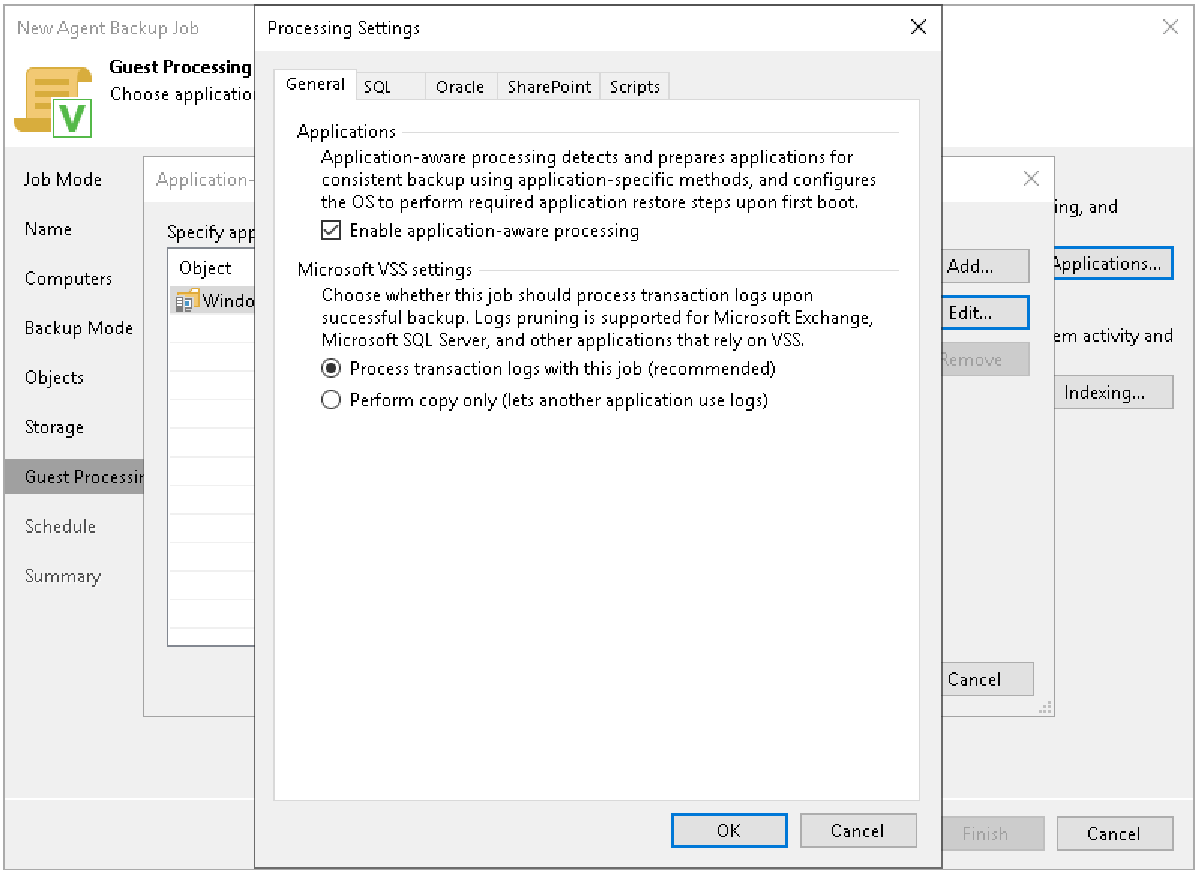
     [For Microsoft SQL Server and Oracle] You will have to specify settings for database log handling on the **SQL** and **Oracle** tabs of the **Processing Settings** window. For more information, see Microsoft SQL Server Transaction Log Settings and Oracle Archived Log Settings.

   - 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, you can enable log backup settings only for one of the installed applications: Microsoft SQL Server or Oracle Server.



Applications

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

☑ Enable application-aware processing

Microsoft VSS settings

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server, and other applications that rely on VSS.

● Process transaction logs with this job (recommended)

○ Perform copy only (lets another application use logs)

Microsoft SQL Server Transaction Log Settings

IMPORTANT

If the Microsoft OLE DB Driver 19 is installed on the SQL server host, consider the following:

- If the mandatory or strict encryption is enabled for the SQL server, you must additionally specify settings for connection to the SQL server using registry values. To learn more, contact Veeam Customer Support.
- If the SQL server instances have different encryption settings, Veeam Agent will back up only those whose settings match the settings specified in the registry values.
- If an earlier version of the Microsoft OLE DB Driver is also installed on the SQL server host, Veeam Agent will still use the Microsoft OLE DB Driver 19 to connect to the SQL server.

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 section Permissions for Guest Processing. 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.

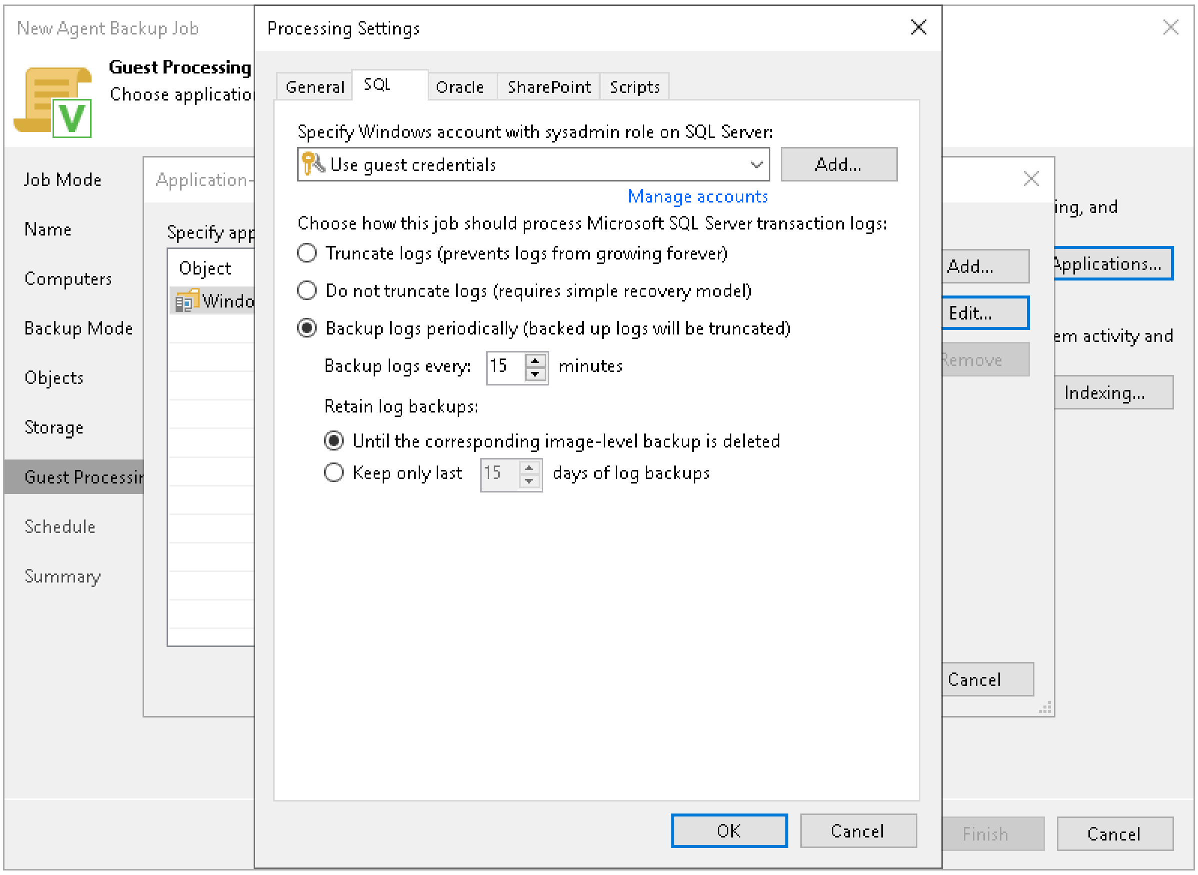
     We recommend that you enable this option only for databases with log truncation managed by a database administrator and databases that use the *Simple* recovery model. If you enable this option for databases that use the *Full* or *Bulk-logged* recovery model, transaction logs may grow large and consume all disk space. In this case, the database administrator must take care of transaction logs.
   - 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 for Microsoft Windows User Guide.

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

1. In the **Backup logs every <N> minutes** field, specify the frequency for transaction logs backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
2. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup location.
   - 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.



Processing Settings

General | SQL | Oracle | SharePoint | Scripts

Specify Windows account with sysadmin role on SQL Server:

Use guest credentials — Add...

Manage accounts

Choose how this job should process Microsoft SQL Server transaction logs:

○ Truncate logs (prevents logs from growing forever)

○ Do not truncate logs (requires simple recovery model)

● Backup logs periodically (backed up logs will be truncated)

Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

OK | Cancel

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 redo 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 job to complete successfully and then trigger archived logs deletion from the Oracle Call Interface (OCI) according to the specified settings. If the backup job fails, the logs will remain untouched until the next successful backup job session.

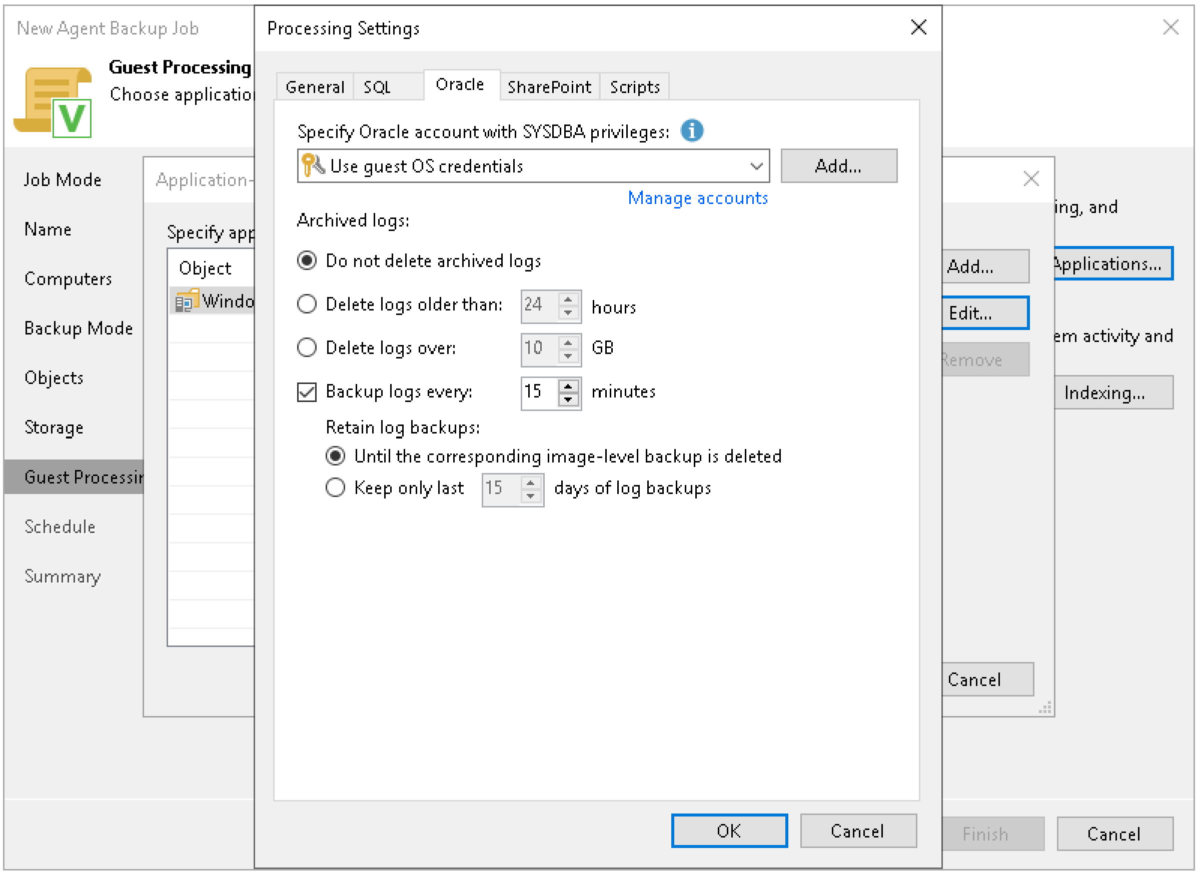
     > TIP
     >
     > If you configure backup job to back up archived logs, Veeam Agent for Microsoft Windows also triggers archived logs deletion during each interval of the log backup job.

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.



Processing Settings

General | SQL | Oracle | SharePoint | Scripts

Specify Oracle account with SYSDBA privileges: Use guest OS credentials

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

☑ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

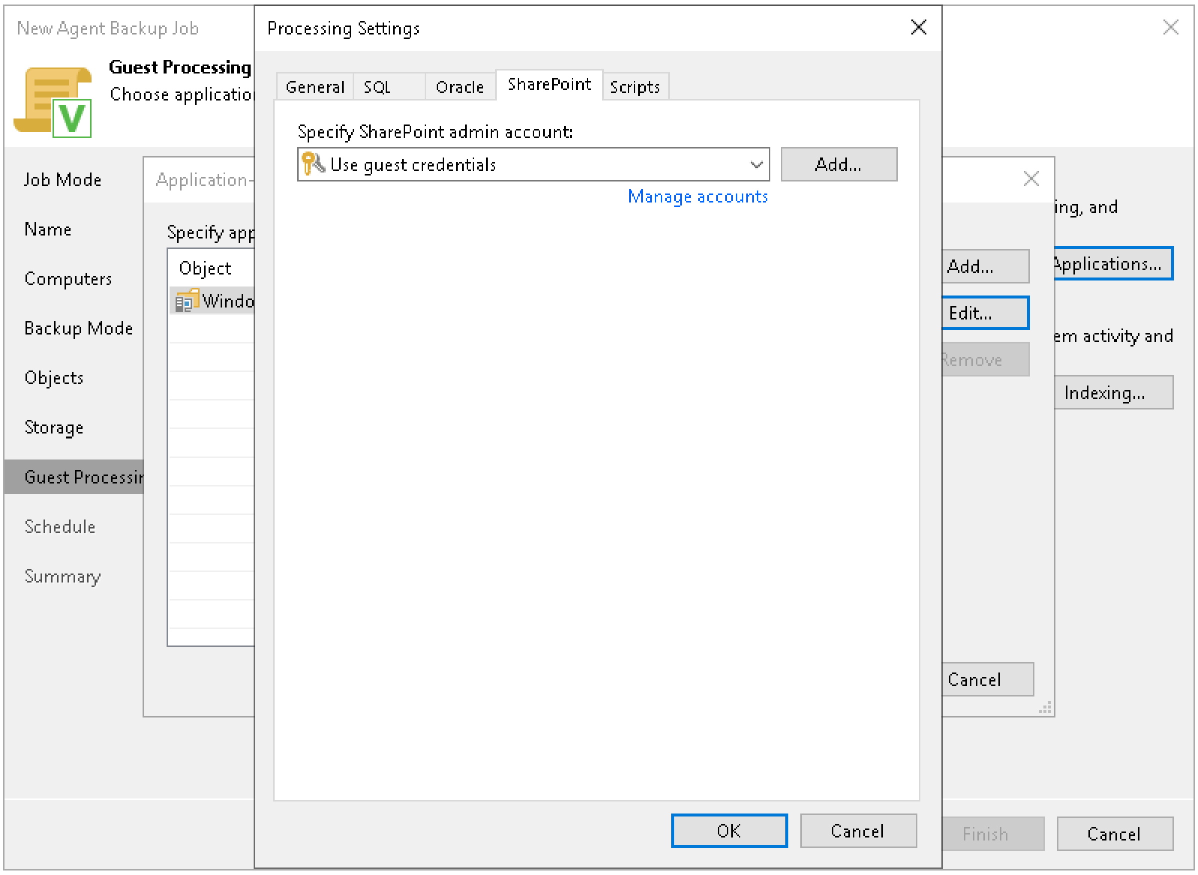
Microsoft SharePoint Account Settings

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.



Processing Settings

Specify SharePoint admin account: Use guest credentials

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 requests the creation of 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:

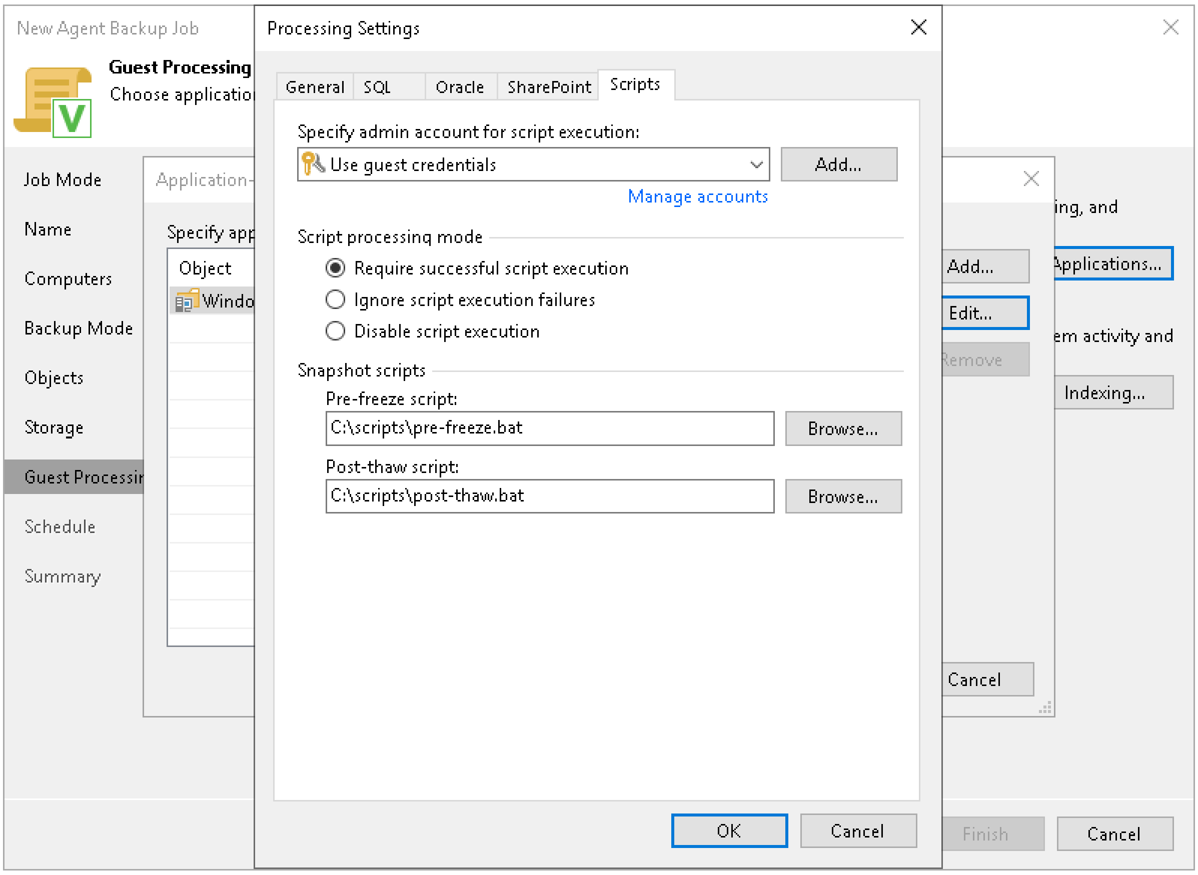
   - Select **Require successful script execution** if you want Veeam Agent for Microsoft Windows to stop the backup process if the script fails.
   - Select **Ignore script execution failures** if you want to continue the backup process even if script errors occur.
   - Select **Disable script execution** 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.



Specify admin account for script execution: Use guest credentials

Script processing mode

● Require successful script execution
○ Ignore script execution failures
○ Disable script execution

Snapshot scripts

Pre-freeze script: C:\scripts\pre-freeze.bat

Post-thaw script: C:\scripts\post-thaw.bat

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.

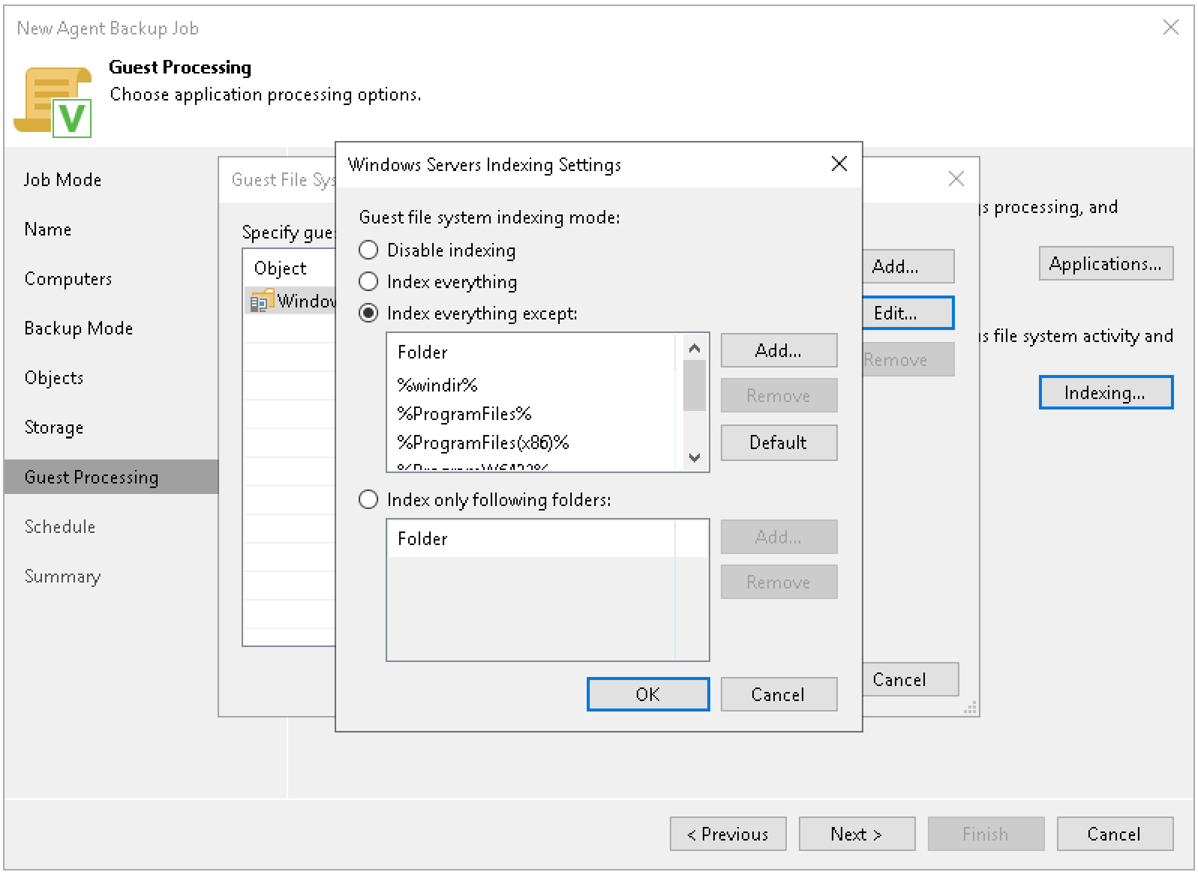
> NOTE
>
> File system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the backup created with such backup job. For more information, see the Preparing for File Browsing and Restore section in the Veeam Backup Enterprise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

To specify file indexing options:

1. At the **Guest Processing** step of the wizard, select the **Enable guest file system indexing and malware detection** 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%*.



New Agent Backup Job

Guest Processing

Choose application processing options.

Job Mode
Name
Computers
Backup Mode
Objects
Storage
Guest Processing
Schedule
Summary

Windows Servers Indexing Settings

Guest file system indexing mode:

○ Disable indexing
○ Index everything
● Index everything except:

Folder
%windir%
%ProgramFiles%
%ProgramFiles(x86)%

○ Index only following folders:

Folder

Step 11. 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.

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

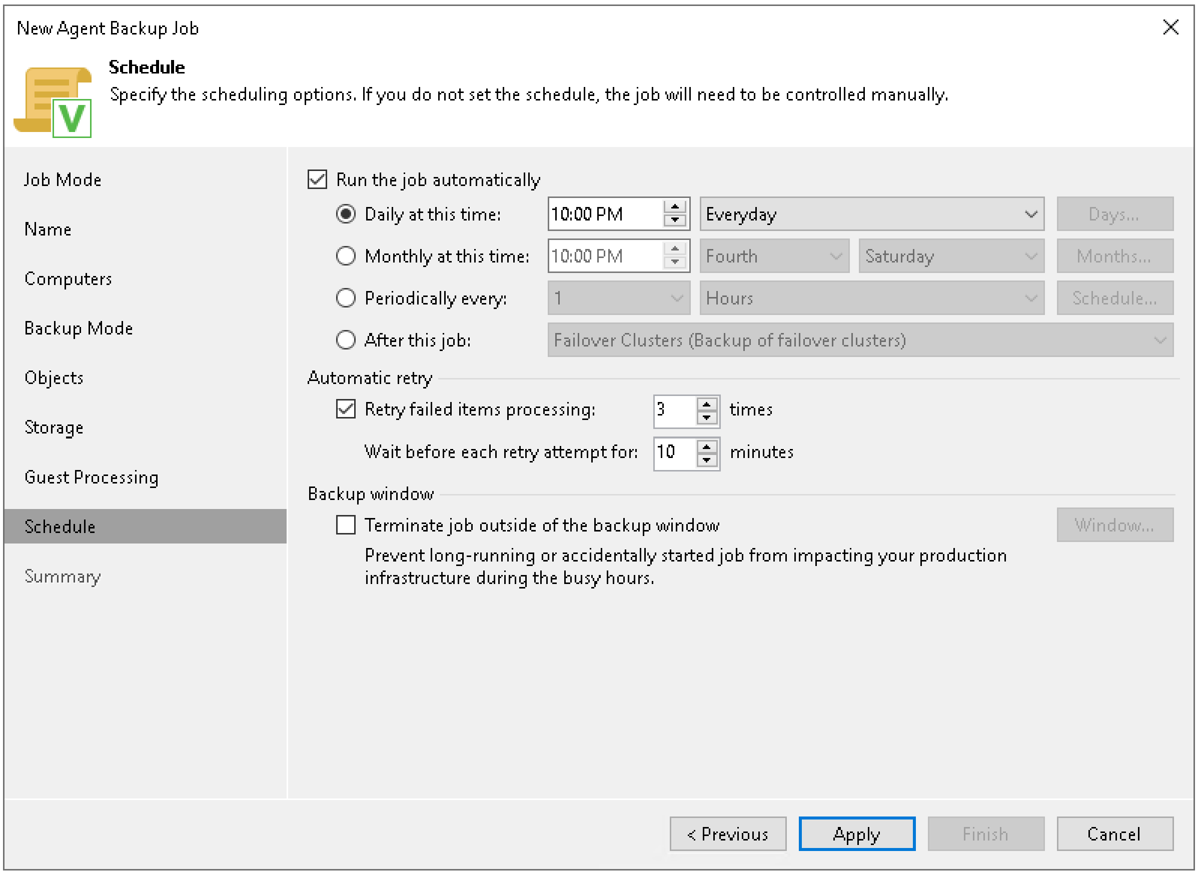
> **NOTE**
>
> The automatic retry does not start if you run the backup job manually. In this case, you can manually retry the backup job. To learn more, see Retrying Veeam Agent Backup Job.

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.



New Agent Backup Job

Schedule

Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

○ Periodically every: 1 Hours

○ After this job: Failover Clusters (Backup of failover clusters)

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

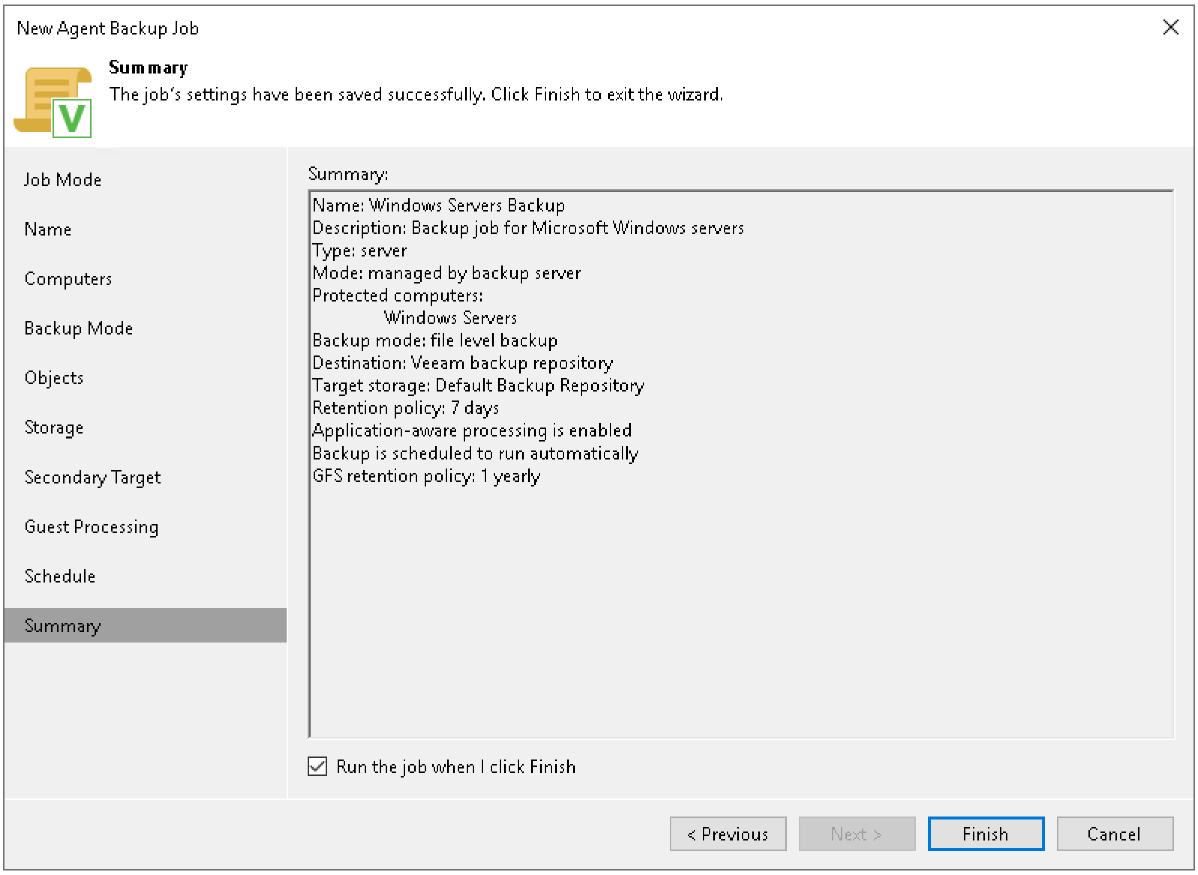
☐ Terminate job outside of the backup window

Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.

Step 12. 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. 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.



```
Name: Windows Servers Backup
Description: Backup job for Microsoft Windows servers
Type: server
Mode: managed by backup server
Protected computers:
            Windows Servers
Backup mode: file level backup
Destination: Veeam backup repository
Target storage: Default Backup Repository
Retention policy: 7 days
Application-aware processing is enabled
Backup is scheduled to run automatically
GFS retention policy: 1 yearly
```

☑ Run the job when I click Finish

Creating Job for Linux Computers

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

Before You Begin

Before you create a Veeam Agent backup job managed by the backup server 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 workstations that you plan to add to the Veeam Agent backup job. To learn more, see Licensing Requirements.
- 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.

Veeam Agent backup jobs have the following limitations:

- If you want to perform a volume-level restore of a machine using Veeam Agent, the BIOS boot partition of this machine must be associated with a block device. Otherwise, Veeam Agent supports only file-level restore from the backup of the machine.
- 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 Creating Policy for Linux Computers.
- You cannot map a Veeam Agent backup job managed by the backup server to a Veeam Agent backup chain created by another type of a Veeam Agent backup job. After you change the mode of a Veeam Agent computer, Veeam Backup & Replication starts a new backup chain in a target location specified in the backup job settings.
- 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.
- Veeam Agent does not support backup of bind mount points. In the scope of the backup job, you must specify the path to the original mount point instead.
- If you plan to create a Veeam Agent backup job for computers with nosnap Veeam Agent installed, consider the limitations and system requirements listed in section System Requirements for Linux Computers (nosnap Veeam Agent).
- You cannot add a Veeam Agent computer protected by a Veeam Agent backup policy to a backup job managed by the backup server. To add such a computer to a backup job managed by the backup server, first remove the computer from the Veeam Agent backup policy.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup job managed by the backup server 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 and 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 individual computers to the job later on, when you pass through the wizard steps.

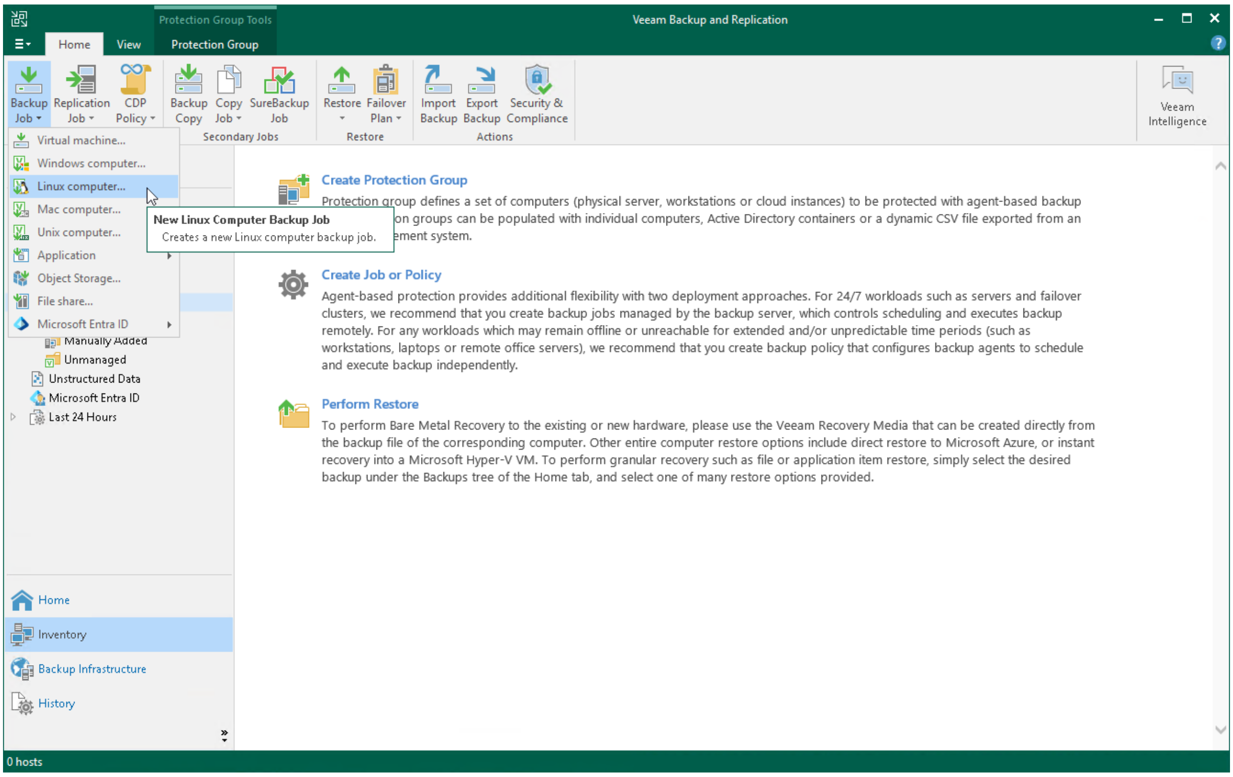
Adding Computers to New Backup Job

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 protection groups to the job later on, when you pass through the wizard steps.

> **TIP**
>
> Consider the following:
>
> - You can press and hold the [Ctrl] key 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.



Create Protection Group

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

Create Job or Policy

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

Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify protection settings for the Veeam Agent backup job managed by the backup server:

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 on servers, select the job mode.

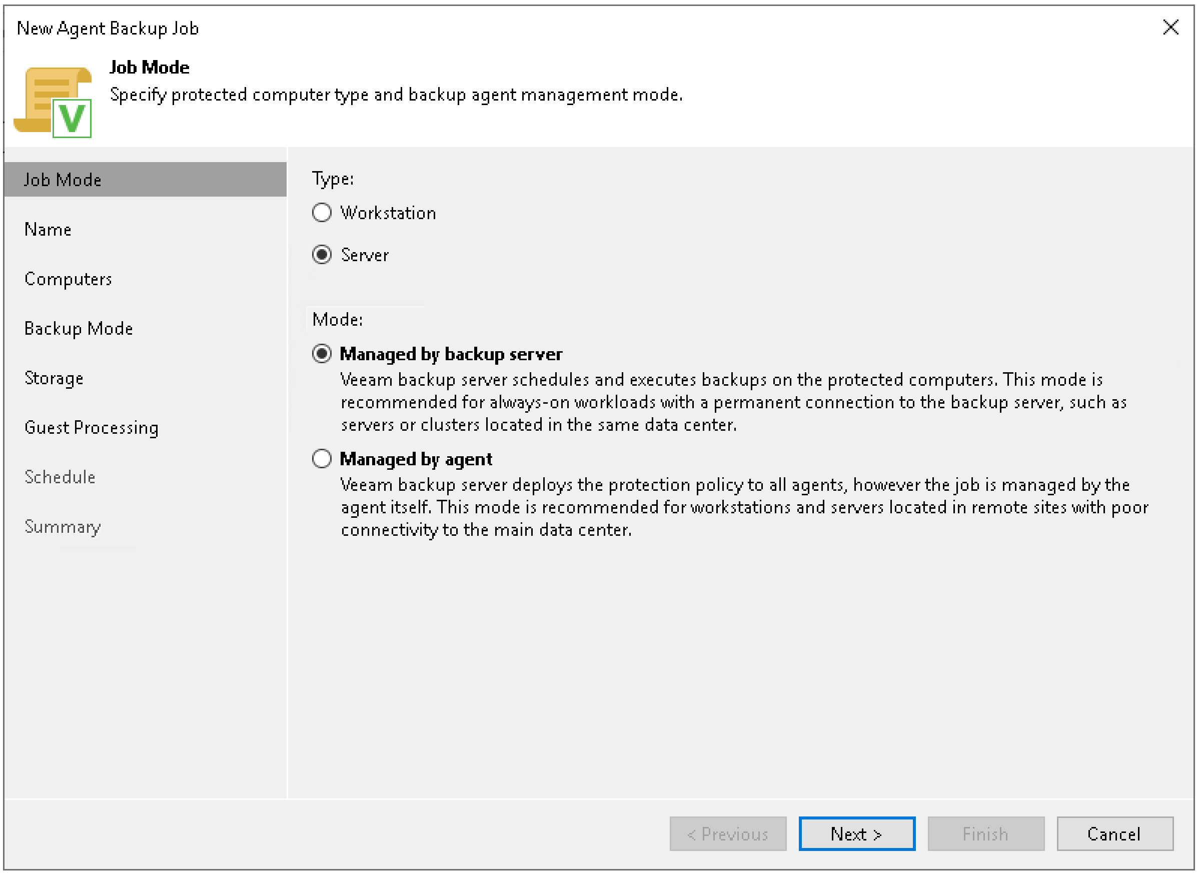
Selecting Protected Computer Type

To create a Veeam Agent backup job managed by the backup server, at the **Job Mode** step of the wizard, in the **Type** field, select the **Server** option.

> **NOTE**
>
> You cannot select the **Workstation** option if you want to create a Veeam Agent backup job managed by backup server.

Selecting Job Mode

If you selected the **Server** option in the Type field, in the **Mode** field, select the **Managed by backup server** job mode to create a Veeam Agent backup job managed by the backup server. If you select the **Managed by agent** job mode, you will create a Veeam Agent backup policy.



New Agent Backup Job

Job Mode

Specify protected computer type and backup agent management mode.

Type:

○ Workstation

● Server

Mode:

● **Managed by backup server**

Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

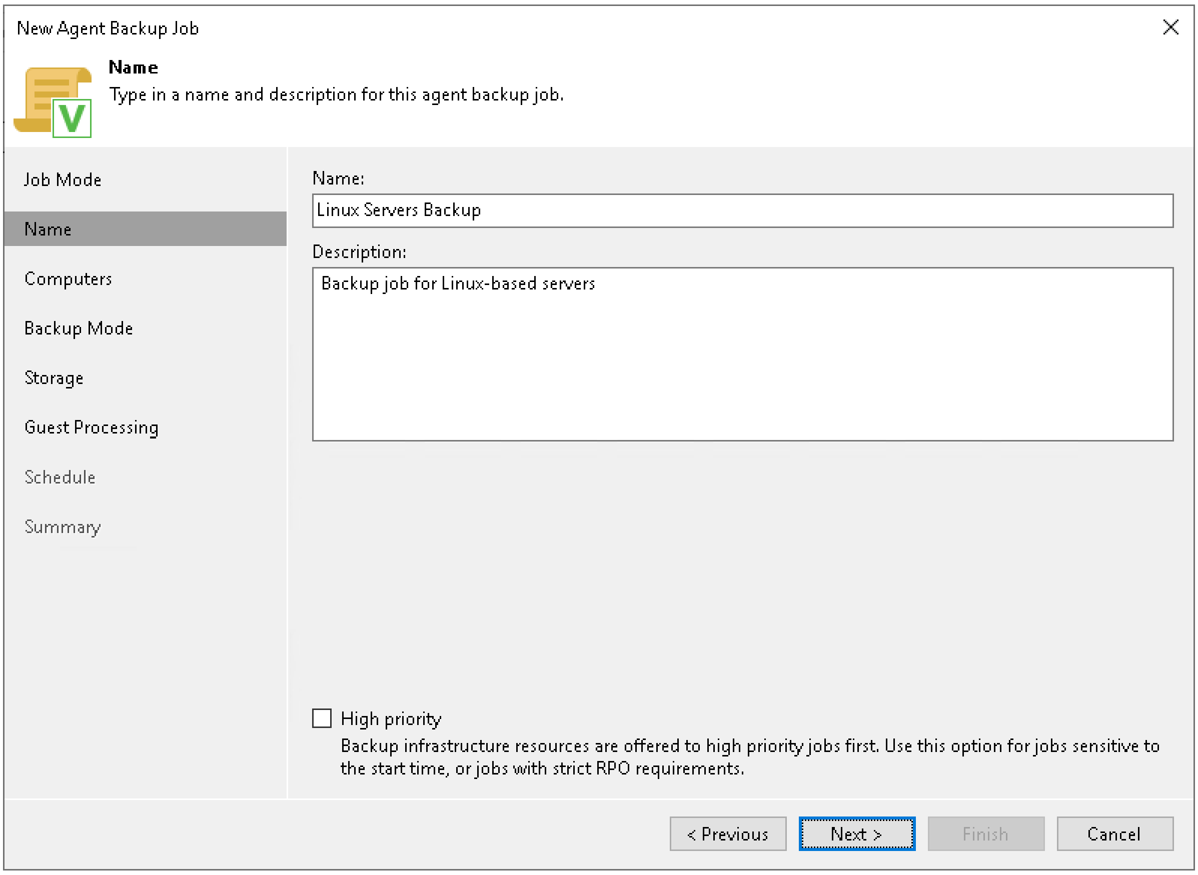
○ **Managed by agent**

Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

Step 3. Specify Job Name and Description

At the **Name** step of the wizard, specify a name and description for the Veeam Agent backup job managed by the backup server.

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. 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.



New Agent Backup Job

Name
Type in a name and description for this agent backup job.

Name: Linux Servers Backup

Description: Backup job for Linux-based servers

□ High priority
Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and individual computers that you want to back up with the Veeam Agent backup job managed by the backup server.

You can add to the backup job one or more protection groups and individual computers from the Veeam Backup & Replication inventory. 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.

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

Adding Protection Groups and Computers from Inventory

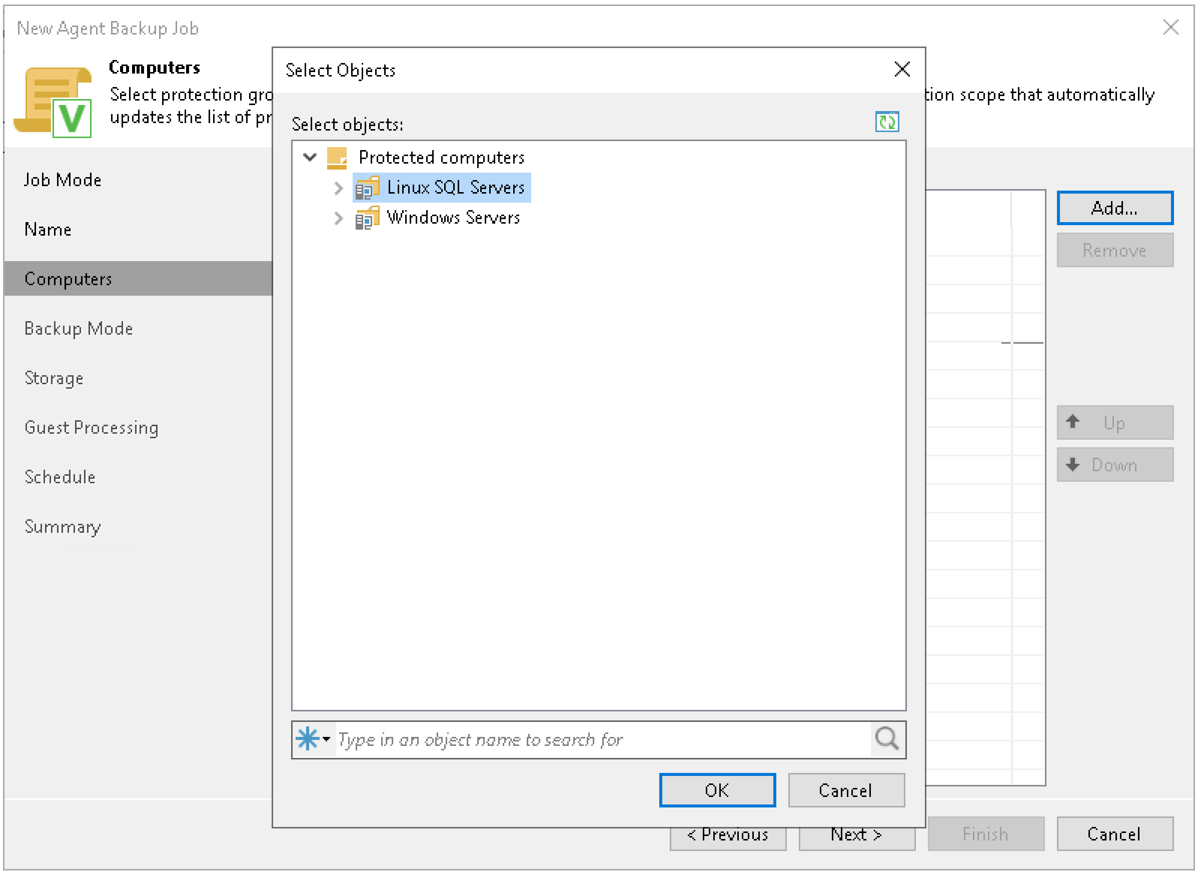
To add protection groups and individual computers to the Veeam Agent backup job, do the following:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and computers in the list and click **OK**. You can press and hold the [Ctrl] or [Shift] key 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 managed by the backup server new computers that do not exist in the inventory, do the following:

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. Select a method to connect to the computer:
    - **Connect using admin credentials.** In this case, 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.

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

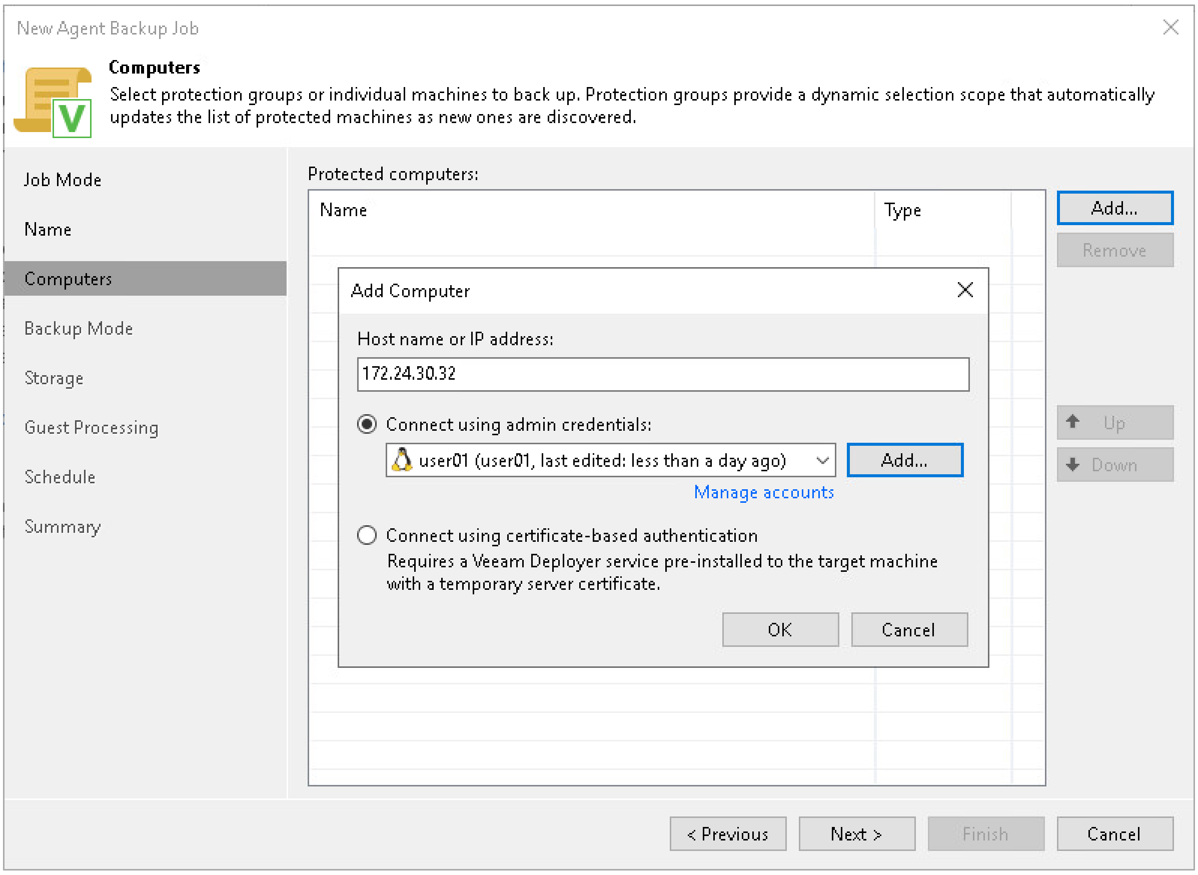
        - **Stored** credentials. Select stored credentials if you want Veeam Backup & Replication to use the specified user name and password for each connection to Veeam Agent.

    - **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.

- Select this option, if you chose to pre-install Veeam Deployer Service on the Linux computer that you want to add to the backup job. In this case, Veeam Backup & Replication will communicate with the Linux computer using a certificate. To learn more, see Deploying Veeam Agent for Linux Using Pre-Installed Veeam Deployer Service



New Agent Backup Job

Computers

Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

Protected computers:

Name	Type

Add Computer

Host name or IP address: 172.24.30.32

● Connect using admin credentials: user01 (user01, last edited: less than a day ago)

○ Connect using certificate-based authentication

Requires a Veeam Deployer service pre-installed to the target machine with a temporary server certificate.

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 the Storage step of the wizard.

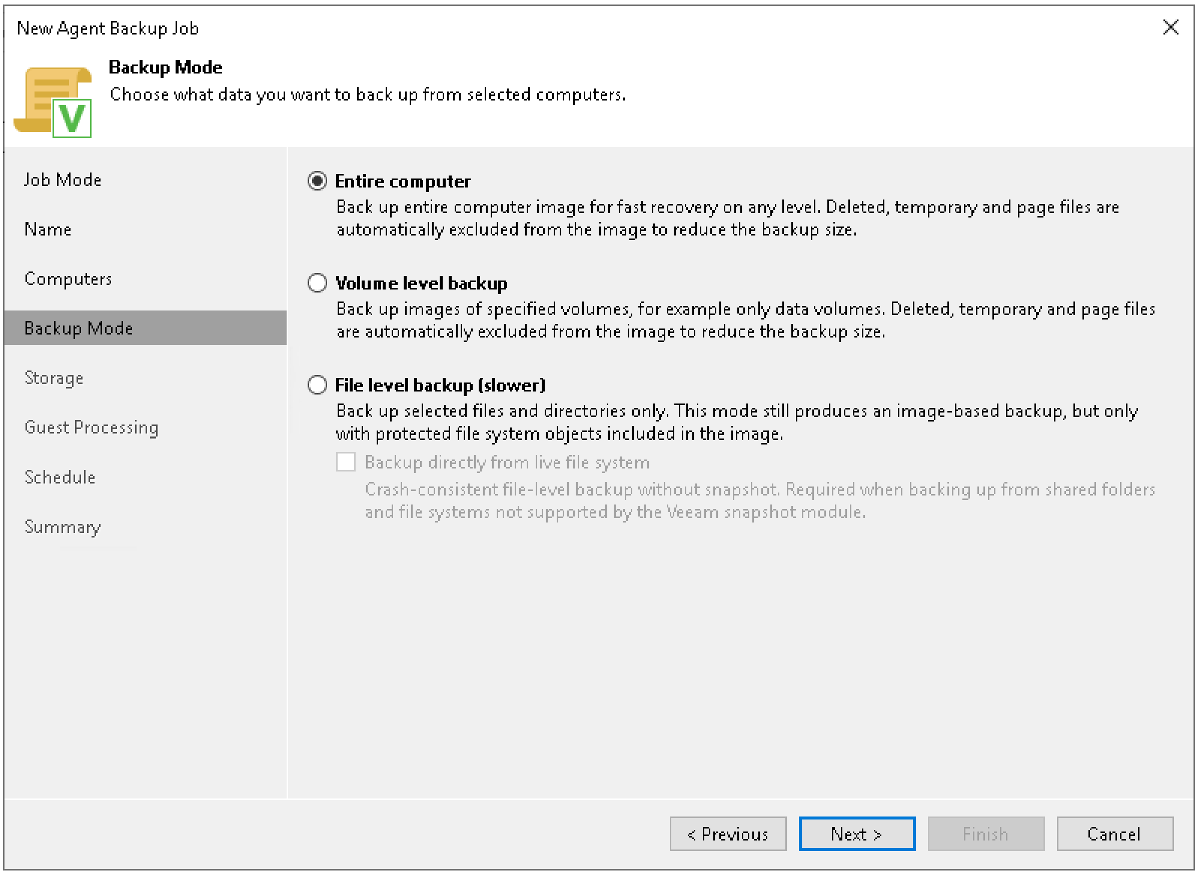
   - **Volume level backup** – select this option if you want to create a backup of specific computer volumes, for example, the system volume. When you restore data from such backup, you will be able to recover data located on these volumes only: files, directories, application data and so on. With this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



New Agent Backup Job

Backup Mode

Choose what data you want to back up from selected computers.

● **Entire computer**
Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **Volume level backup**
Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **File level backup (slower)**
Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.

□ Backup directly from live file system
Crash-consistent file-level backup without snapshot. Required when backing up from shared folders and file systems not supported by the Veeam snapshot module.

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 managed by the backup server:

- 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.

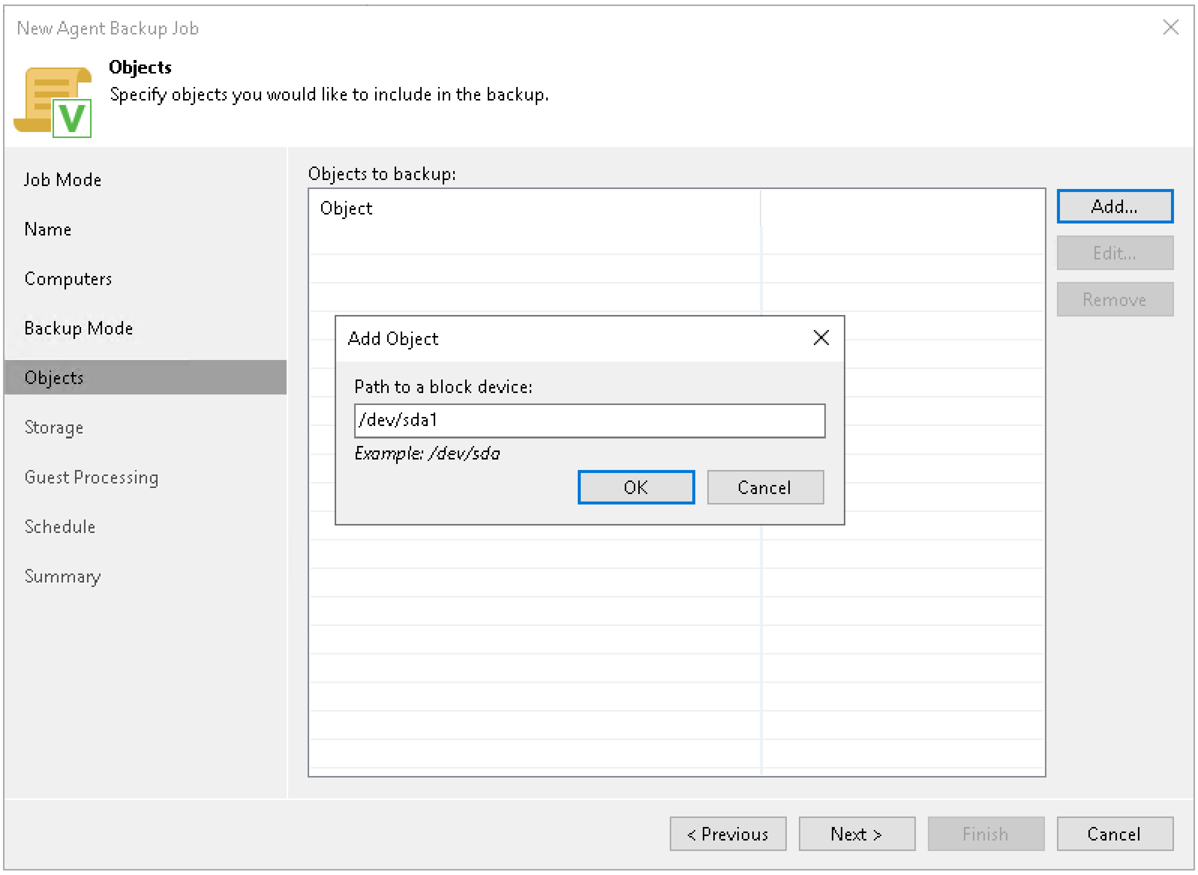
     > IMPORTANT
     >
     > Veeam Agent does not support backup of bind mount points. You must specify the path to the original mount point instead.

   - *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.



Path to a block device: /dev/sda1

Example: /dev/sda

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 by defining 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**.

IMPORTANT

Veeam Agent does not support backup of bind mount points. You must specify the path to the original mount point instead.

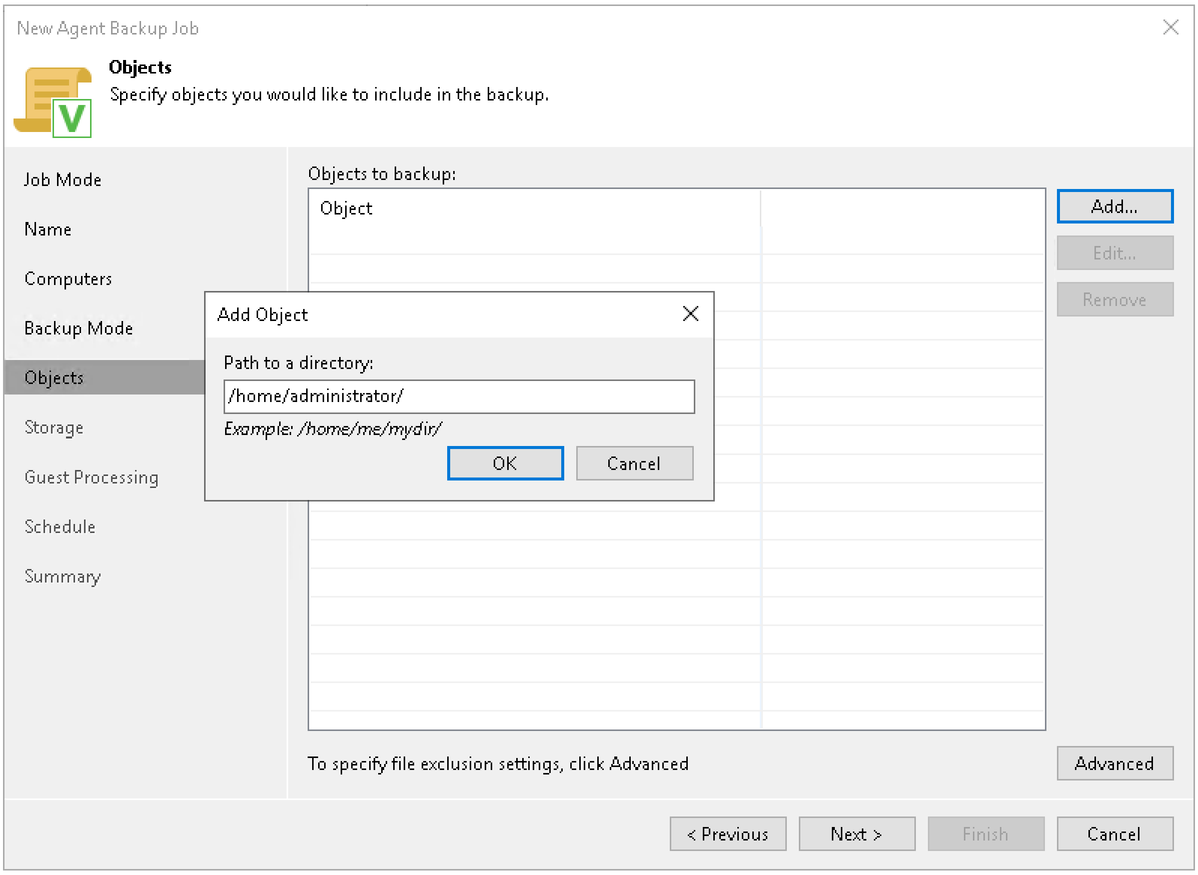
3. Repeat steps 1–2 for all directories that you want to back up.

TIP

If you want to back up the root directory and specify '/' in the **Path to a directory** field, Veeam Agent will not automatically include into the backup scope the network file system mount points — for example, NFS or SMB network shared folders. To include such mount points, you need to specify paths to these mount points manually.

For example, you have a network 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 network file system, add the following objects to the backup scope:

- `/`
- `/home/media`


New Agent Backup Job

Objects
Specify objects you would like to include in the backup.

Objects to backup:

Add Object

Path to a directory: /home/administrator/

Example: /home/me/mydir/

To specify file exclusion settings, click Advanced

Configuring Filters

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

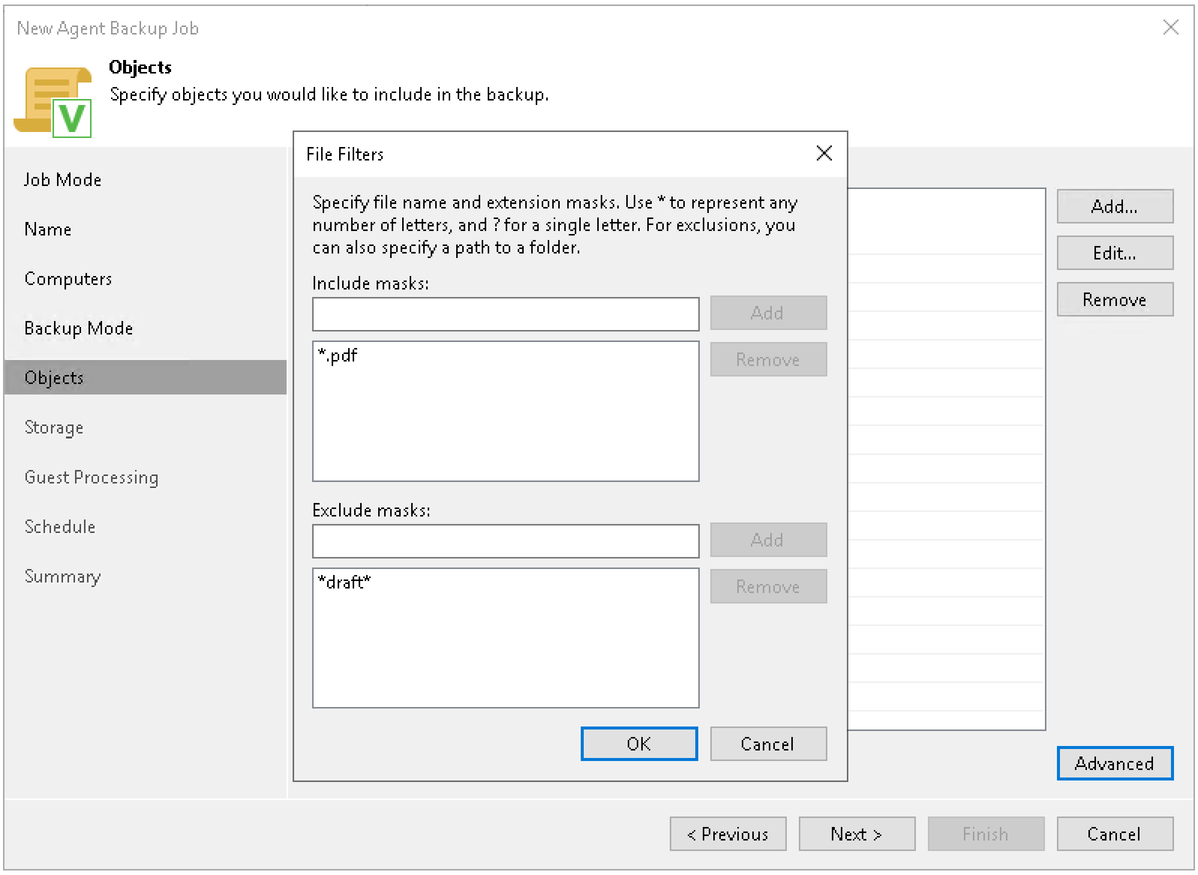
To configure a filter:

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 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 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.



File Filters

Specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify a path to a folder.

Include masks: *.pdf

Exclude masks: *draft*

Step 7. Specify Backup Storage Settings

At the **Storage** step of the wizard, specify settings for the target backup repository managed by the same backup server that manages the Veeam Agent 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
   >
   > 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.

   To learn more, see Short-Term Retention Policy.

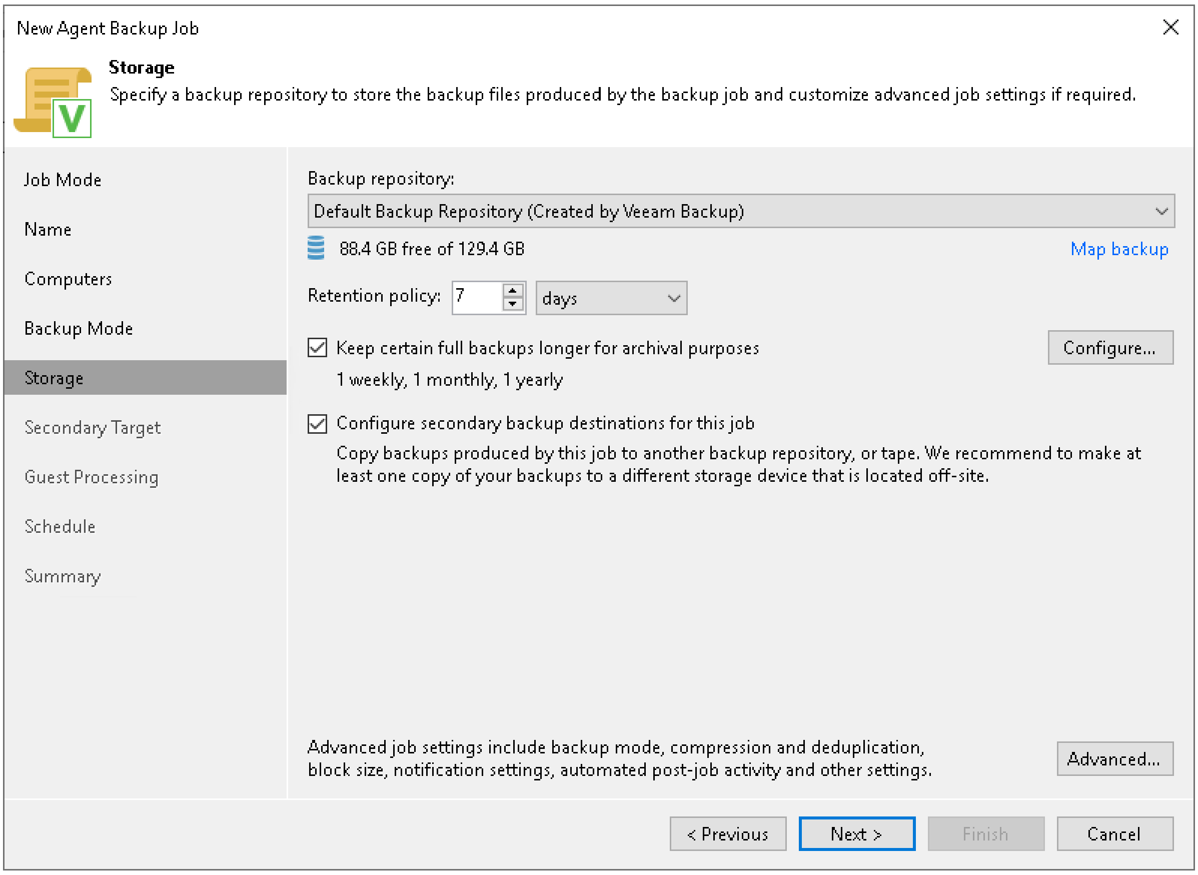
4. To use the GFS (Grandfather-Father-Son) retention scheme, select the **Keep certain full backups longer for archival purposes** check box and click **Configure**. In the **Configure GFS** window, specify how weekly, monthly and yearly full backups must be retained. To learn more, see the Long-Term 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.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Default Backup Repository (Created by Veeam Backup)

88.4 GB free of 129.4 GB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

☑ Configure secondary backup destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Step 8. Specify Advanced Backup Settings

In the **Advanced Settings** window, specify advanced settings for the Veeam Agent backup job managed by the backup server:

- Backup settings
- Maintenance settings
- Storage settings
- Notification settings
- 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 Veeam Agent backup job managed by the backup server:

1. Click **Advanced** at the **Storage** step of the wizard.
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.

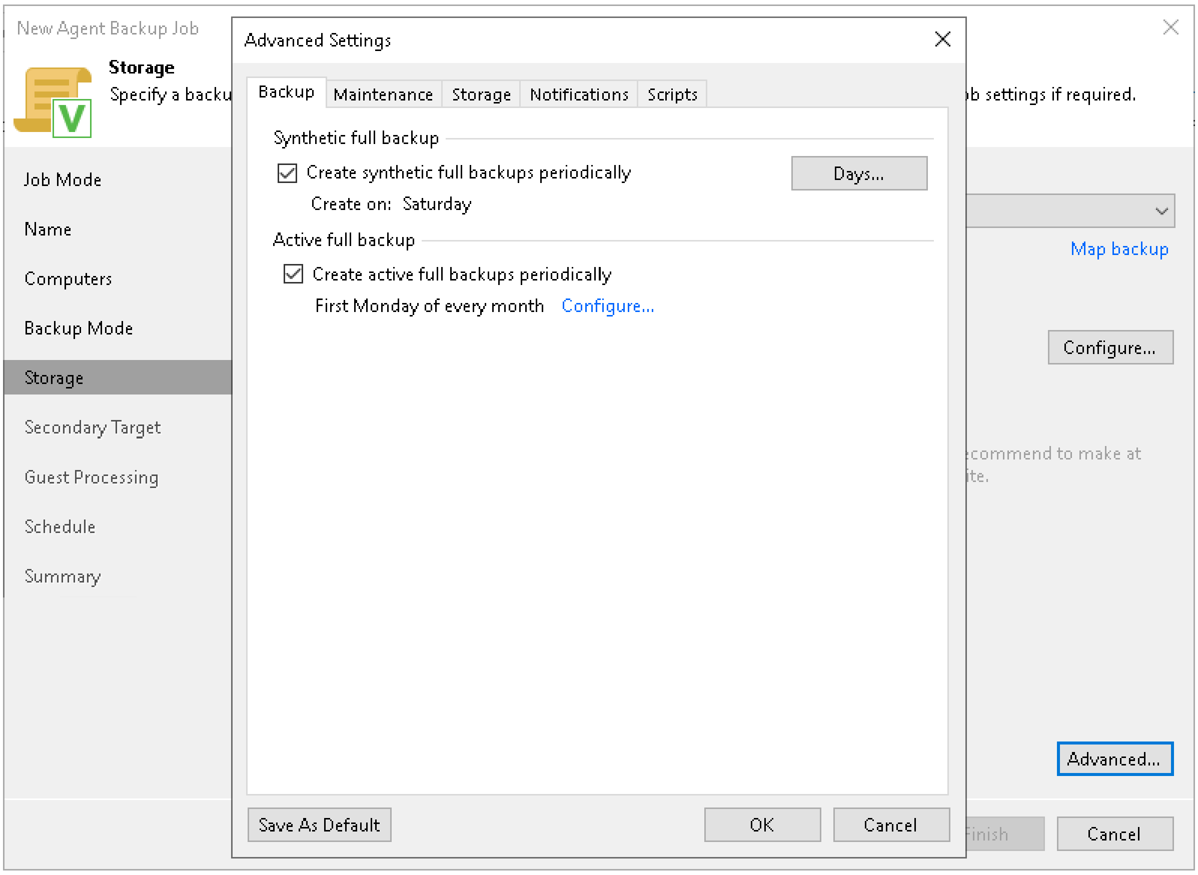
   > NOTE
   >
   > Synthetic full backup is not available for backup jobs targeted at an object storage repository.

3. If you want to periodically create active full backups, select the **Create active full backups periodically** check box 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.



Advanced Settings

Backup | Maintenance | Storage | Notifications | Scripts

Synthetic full backup

☑ Create synthetic full backups periodically

Create on: Saturday

Active full backup

☑ Create active full backups periodically

First Monday of every month

Maintenance Settings

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

To specify maintenance settings for the backup job:

1. At the **Storage** step of the wizard, click **Advanced**.
2. Click the **Maintenance** tab.

3. To periodically perform a health check for the latest restore point in the backup chain, in the **Storage-level corruption guard** section select the **Perform backup files health check** check box and 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 Veeam Agent 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 Items section in the Veeam Backup & Replication 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. 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.

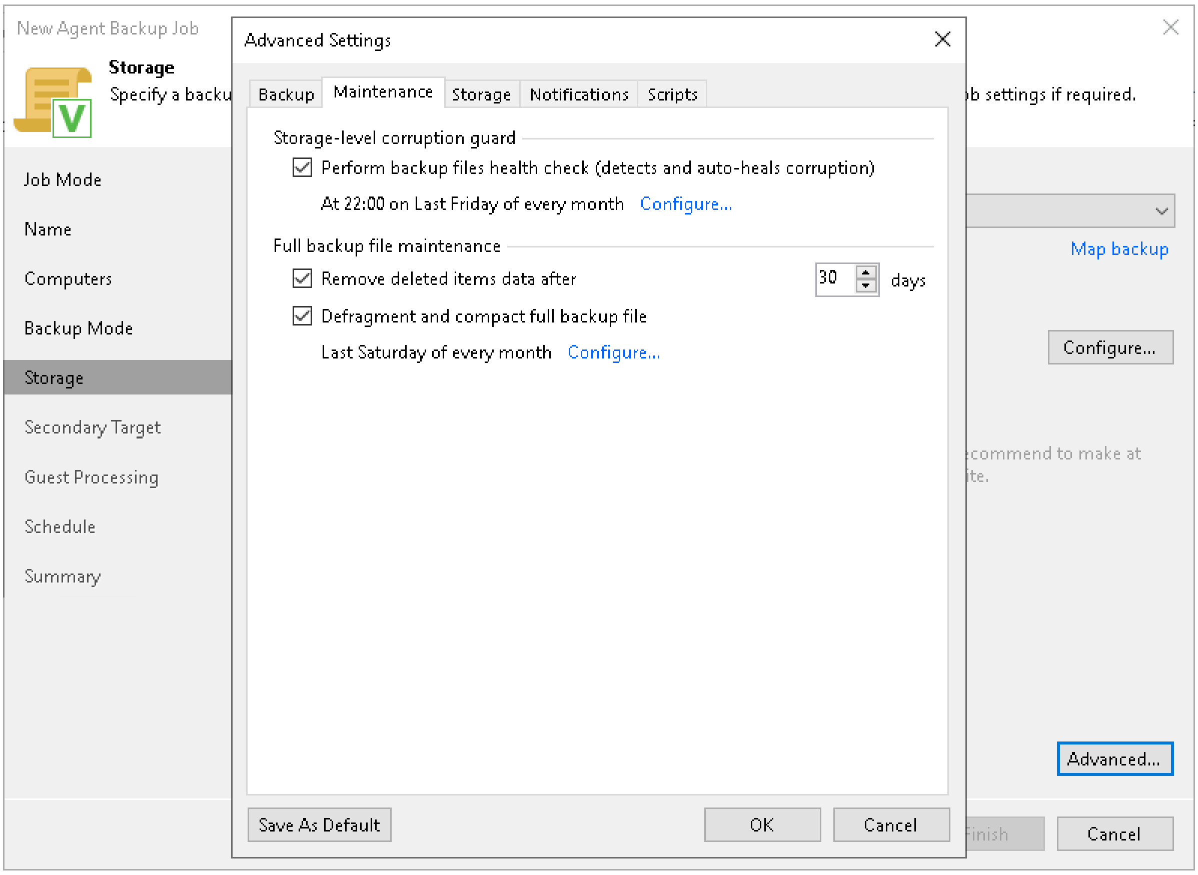
   During the compact operation, Veeam Backup & Replication creates a new empty file and copies to it data blocks from the full backup file. As a result, the full backup file gets defragmented and the speed of reading and writing from/to the backup file increases.

   If the full backup file contains data blocks for deleted items (protection groups or individual computers), Veeam Backup & Replication removes 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-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption)

At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 30 days

☑ Defragment and compact full backup file

Last Saturday of every month Configure...

Storage Settings

To specify storage settings for the Veeam Agent backup job managed by the backup server:

1. Click **Advanced** at the **Storage** step of the wizard.
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*. To learn more about the compression levels, see the Data Compression section in the Veeam Agent for Microsoft Windows User Guide.
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*.

> NOTE
>
> If you change the storage optimization settings for the backup job, new settings will not have any effect on previously created files in the chain. They will be applied to new files created after the settings were changed.
>
> To apply new storage optimization settings in backup jobs, you must create an active full backup after you change storage optimization settings. Veeam Backup & Replication will use the new block size for the active full backup and subsequent backup files in the backup chain. To learn about the active full backup, see Performing Active Full Backup.

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.

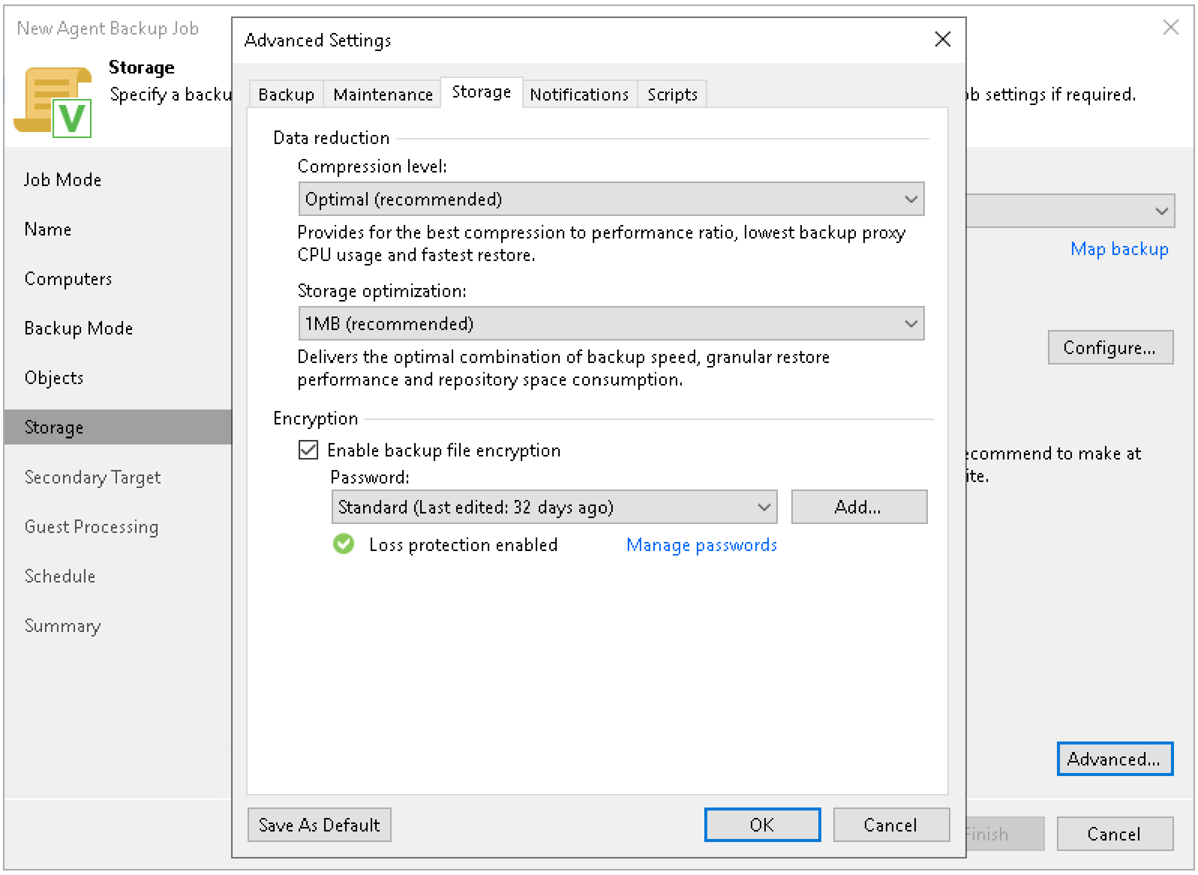
   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it: *Loss protection disabled*. For more information, see the Decrypting Data Without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

   You can select a Key Management System (KMS) server in the Password field. The KMS server must be added to Veeam Backup & Replication in advance. If you choose to use KMS keys for backup file encryption at this step of the wizard, Veeam Backup & Replication immediately starts communication with the KMS server to retrieve the encryption keys. To learn more, see the Key Management System Keys section in the Veeam Backup & Replication User Guide.

NOTE

Consider the following:

- If you plan to encrypt the content of backup files, consider the limitations listed in the Data Encryption Limitations subsection.
- You must encrypt the backup job if you want to back up data to the Veeam Data Vault storage.



Advanced Settings

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 (Last edited: 32 days ago)

✓ Loss protection enabled

Data Encryption Limitations

If you plan to encrypt the content of backup files, consider the following limitations:

- 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.

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

Notification Settings

To specify notification settings for the Veeam Agent backup job managed by the backup server:

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.

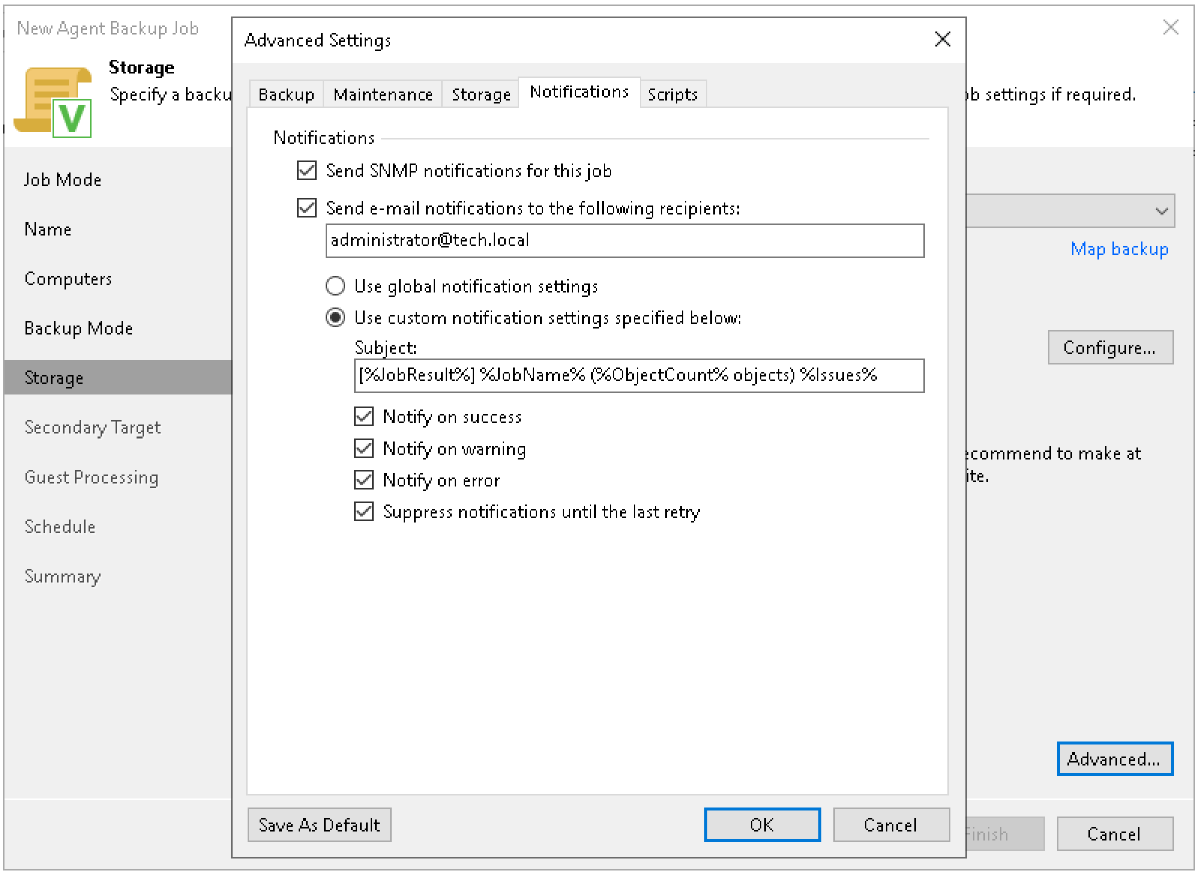
   - To receive a typical notification for the job, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the job global email notification settings specified for the backup server.

   - 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 **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.



Notifications

☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

administrator@tech.local

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

☑ Notify on error

☑ Suppress notifications until the last retry

Script Settings

You can specify what scripts Veeam Backup & Replication will execute on the backup server before and after the session of the Veeam Agent backup job managed by the backup server.

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 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).

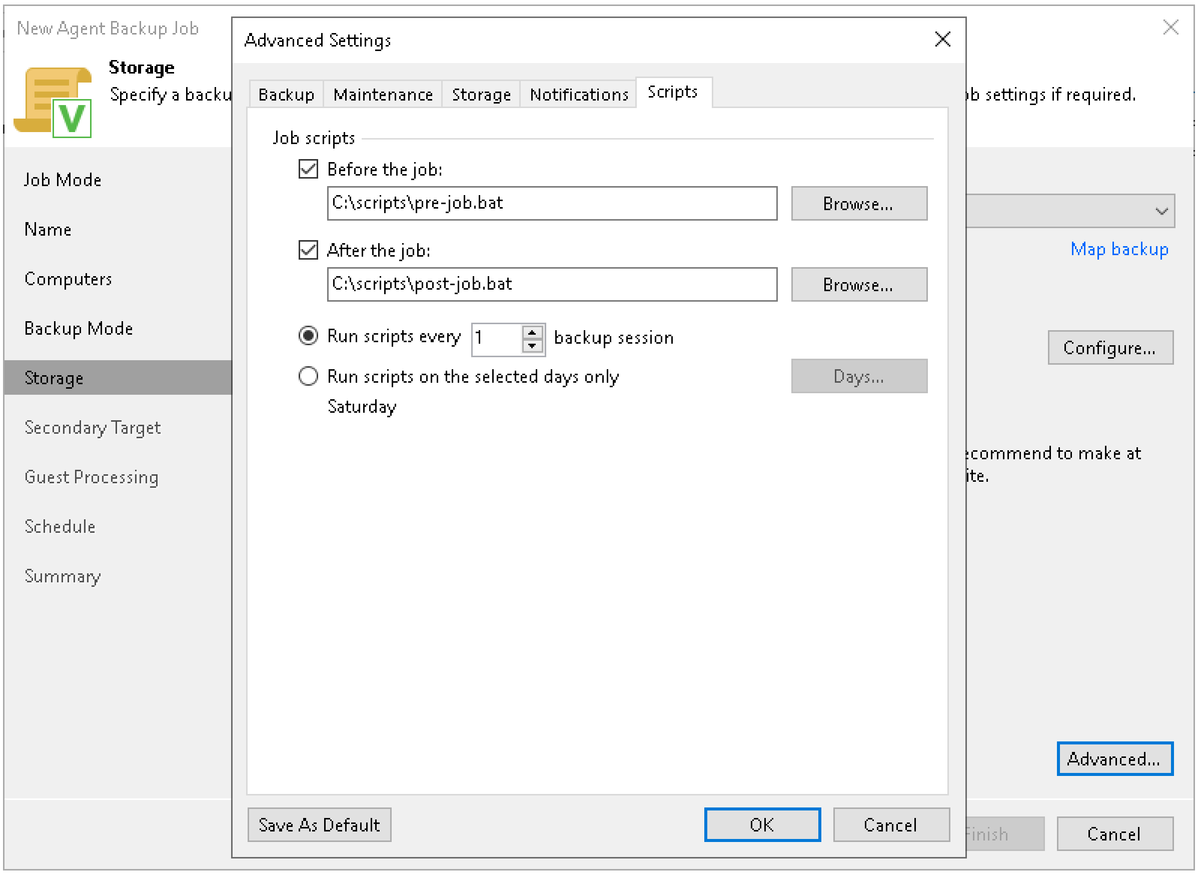
   You can select to execute pre- and post-backup actions after a number of backup sessions or on specific week days.

   - 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 after the backup job session. To learn more, see Backup Job and Snapshot Scripts.



Advanced Settings

Job scripts

☑ Before the job: C:\scripts\pre-job.bat

☑ After the job: C:\scripts\post-job.bat

● Run scripts every 1 backup session

○ Run scripts on the selected days only

Saturday

Step 9. Specify Secondary Target

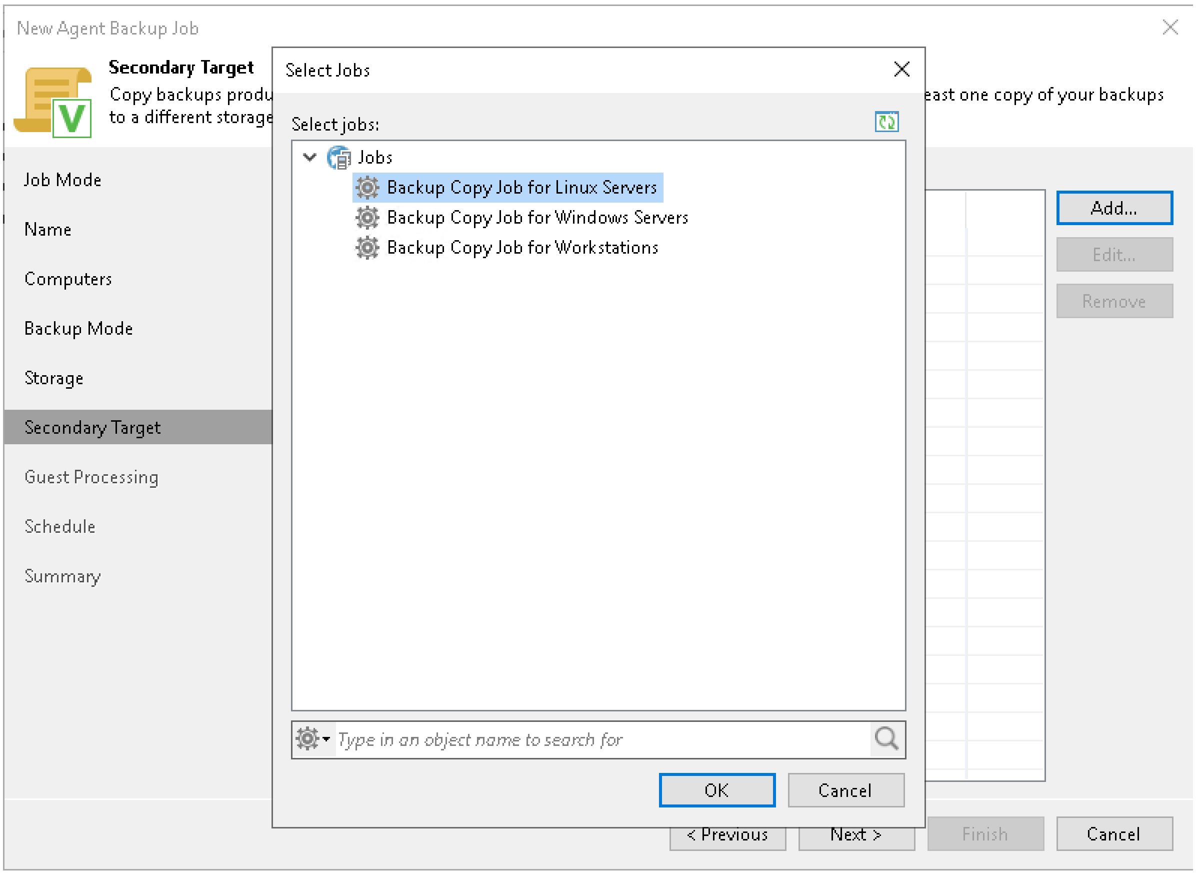
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent backup job managed by the backup server 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 10. 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

Configuring Application-Aware Processing

Before you begin, review the limitations of database processing.

To configure application-aware processing, do the following:

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. 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 credentials 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 about 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.

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

   If you specify custom credentials for a particular computer or a protection group in the **Guest OS Credentials** window, Veeam Agent will use these custom credentials instead of the credentials specified in the **Guest OS credentials** list (see Step 4).

   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, MySQL processing and scripts execution, Veeam Agent always uses the `root` account.

6. 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

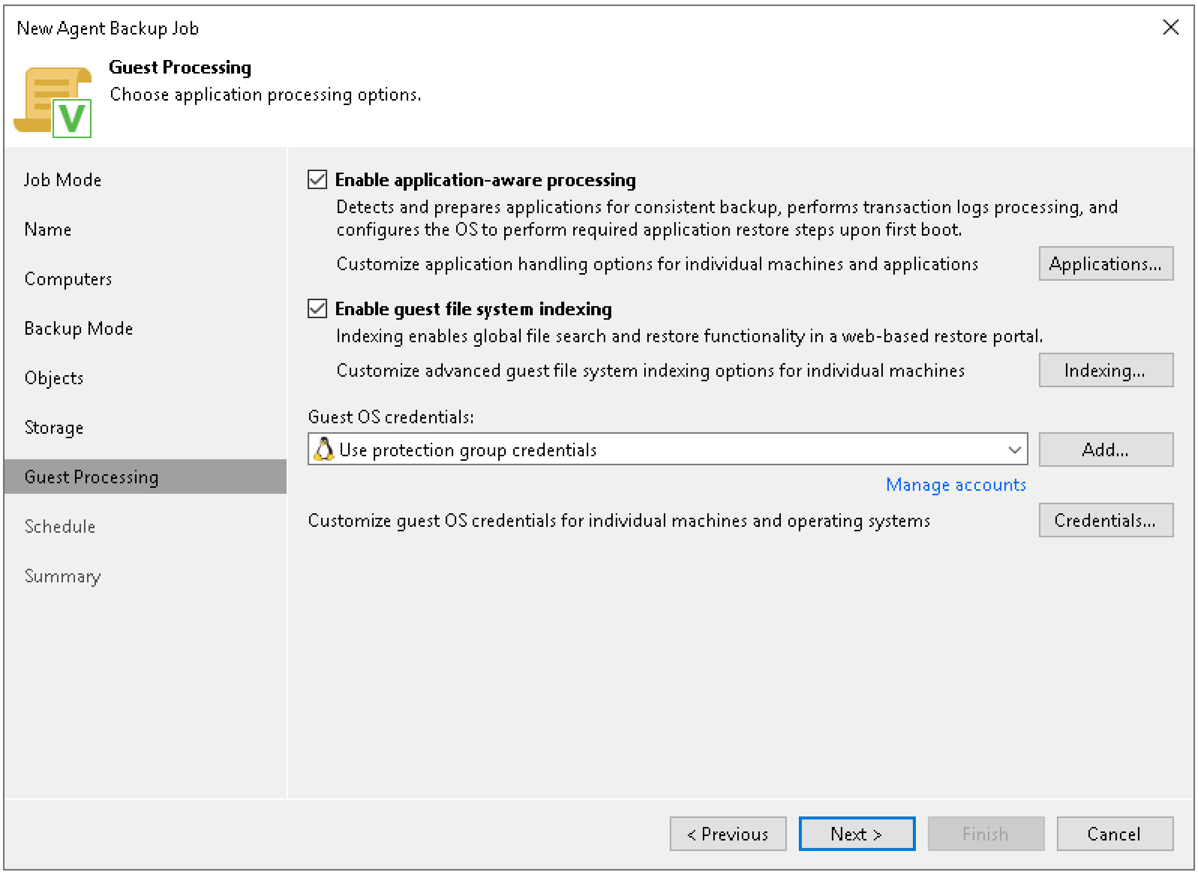
Configuring File Indexing

To configure file indexing settings:

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.



New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Indexing enables global file search and restore functionality in a web-based restore portal.

Customize advanced guest file system indexing options for individual machines

Guest OS credentials: Use protection group credentials

Customize guest OS credentials for individual machines and operating systems

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 Begin

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 more information, see Guest Processing Settings.

Configuring 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 and click **Edit**.

3. On the **General** tab, in the **Applications** section, specify the behavior scenario for application-aware processing:

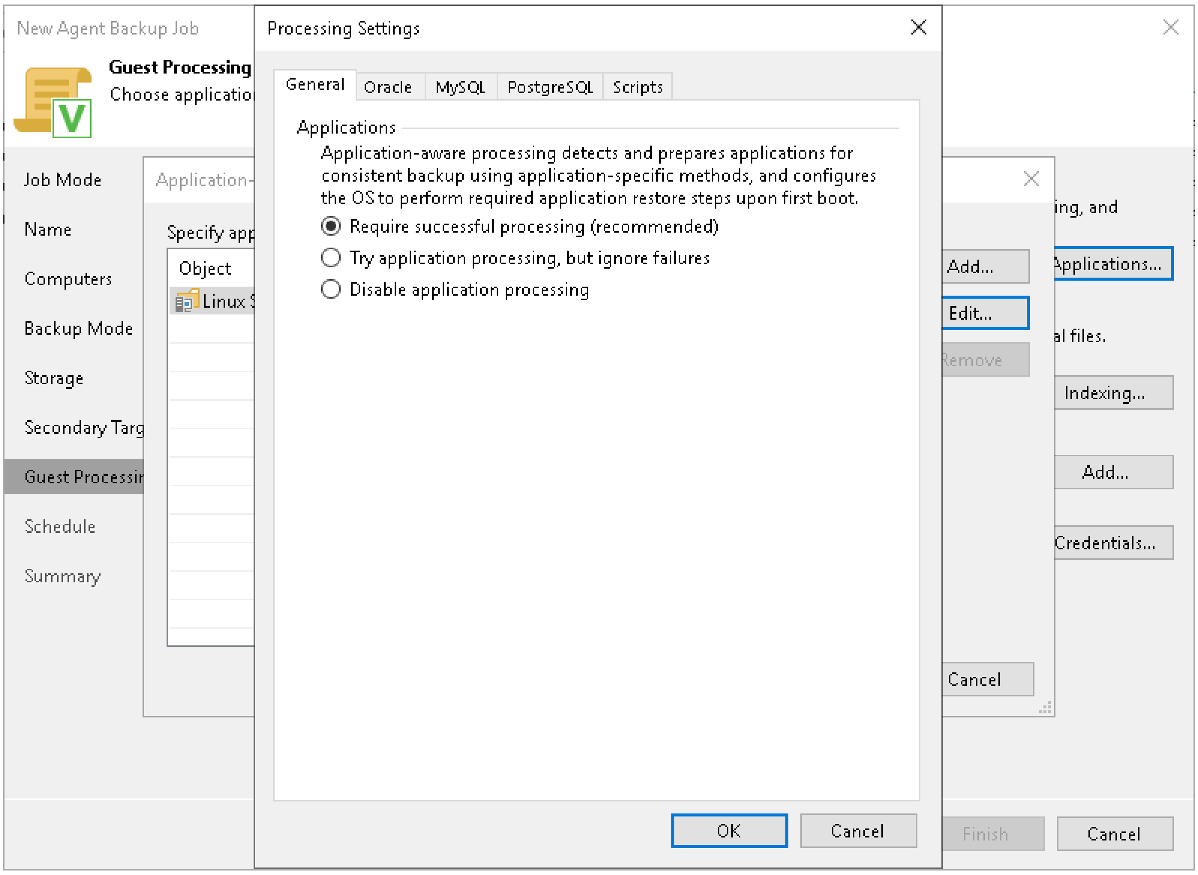
   - Select **Require successful processing** if you want Veeam Agent for Linux to process database systems. With this option selected, if an error occurs when processing a database or database instance, Veeam Agent for Linux will stop the backup process.

     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 database systems. With this option selected, if an error occurs when processing a database or database instance, Veeam Agent for Linux will not stop the backup process. Instead, Veeam Agent for Linux will skip this database or database instance and proceed to the next one. Information about the skipped database or database instance will be displayed in a warning message in the job session statistics. After the backup process is completed, you will be able to restore data from the backup and restore databases or database instances 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 database systems. 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.



Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

● Require successful processing (recommended)
○ Try application processing, but ignore failures
○ Disable application processing

Oracle Processing Settings

You can specify how Veeam Agent for Linux must process the Oracle database system.

Before You Begin

Before you start working with the Oracle database system, 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.

To learn more, 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.

To learn more, see Application-Aware Processing.

Configuring Oracle Processing

To specify how Veeam Agent for Linux must process the Oracle database system, 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, specify a user account that Veeam Agent for Linux will use to connect to the Oracle database. You can do one of the following:
   - Select from the **Specify Oracle account with SYSDBA privileges** list a database user account that has SYSDBA rights on the Oracle database.

     If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. With this option selected, Veeam Agent for Linux will connect to the Oracle database under the account that you have selected in the **Specify Oracle account with SYSDBA privileges** list.
   - Select the **Use guest OS credentials** option.

     With this option selected, Veeam Agent for Linux will do the following:

     i. Veeam Agent will check if you specified custom credentials for the computer or protection group in the **Guest OS Credentials** window at the **Guest Processing** step of the wizard.

        If you specified custom credentials for the computer or protection group in the **Guest OS Credentials** window, Veeam Agent will process the Oracle database under the OS account that you have specified in this window.

        If you have not specified custom credentials for the computer or protection group, Veeam Agent will do as described in the step ii of this procedure.

        To learn more, see step 5 in Specify Guest Processing Settings.

     ii. Veeam Agent will check what have you selected in the **Guest OS credentials** list at the **Guest Processing** step of the wizard.

        If you specified credentials in the **Guest OS credentials** list, Veeam Agent will process the Oracle database under the account that you have specified in this list.

If you have not specified credentials in the list and selected the **Use protection group credentials** option instead, Veeam Agent will do as described in the step iii of this procedure.

To learn more, see step 4 in Specify Guest Processing Settings.

iii. Veeam Agent will check what credentials have you specified for the computer or protection group at the **Computers** step of the wizard.

If you specified stored credentials for this computer in the protection group settings, Veeam Agent will process the Oracle database using the specified account.

If you specified single-use credentials for this computer in the protection group settings, Veeam Agent will process the Oracle database using the root user.

To learn more, see Specifying Computers.

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 themselves.

   - 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 through Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.

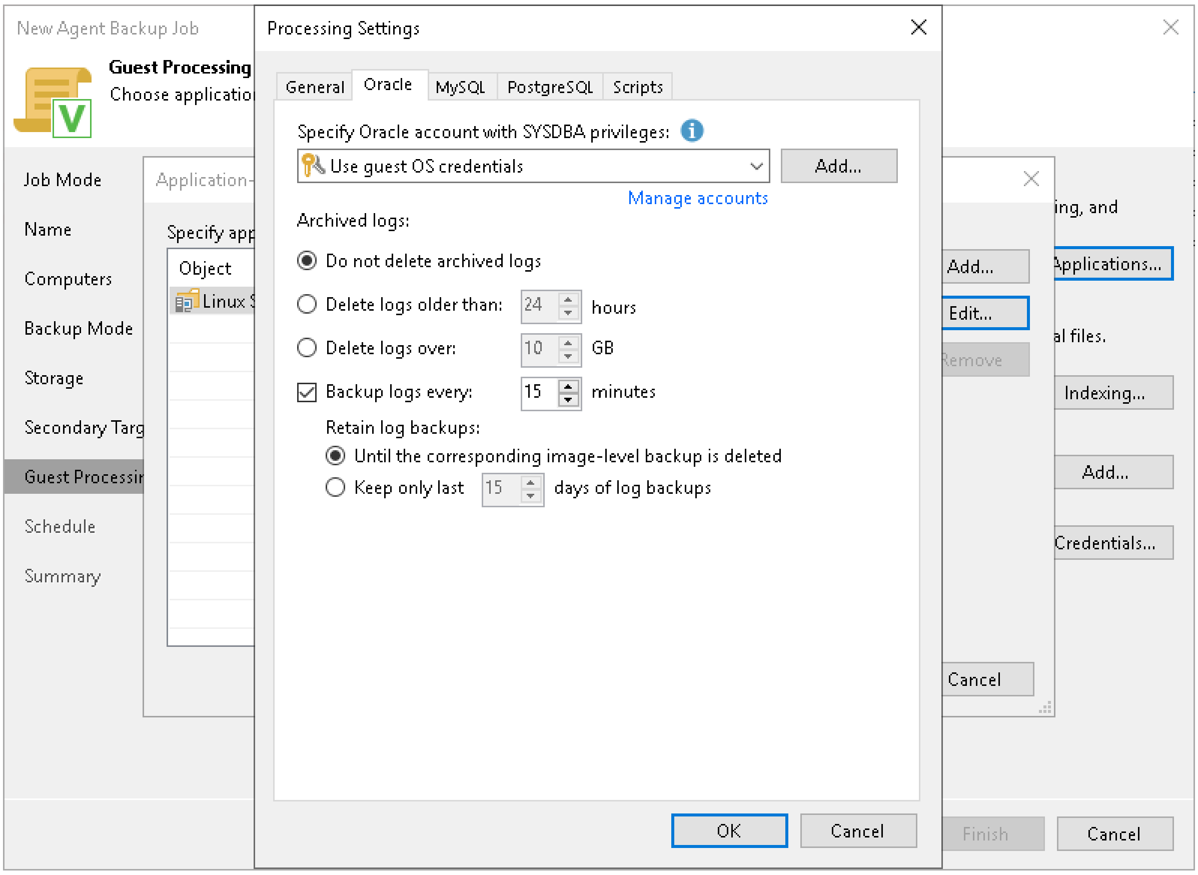
     > TIP
     >
     > If you configure backup job to back up archived logs, Veeam Agent for Linux will not trigger archived logs deletion after each log backup job session. To prevent Oracle database logs from overgrowing, run the backup job for the Veeam Agent computer more often.

5. 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. 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.



Specify Oracle account with SYSDBA privileges: Use guest OS credentials

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

☑ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

MySQL Processing Settings

You can specify how Veeam Agent for Linux must process a MySQL database.

Before You Begin

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.

To learn more, 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**.

To learn more, see Application-Aware Processing.

4. MySQL tables with the MyISAM storage engine must be locked to keep them in a consistent state while Veeam Agent is creating the system snapshot. To correctly process such tables, make sure that the user account you want to specify in the MySQL processing settings has the following instance-wide privileges:

   - `SELECT`. This privilege enables Veeam Agent to access tables' metadata and select for a lock the tables that use the MyISAM storage engine. Without this privilege, the processing of the MySQL database system will run successfully but MyISAM tables will not be locked, which may result in an inconsistent state of the backed up data.

   - `LOCK TABLES`. This privilege is required for locking the selected MyISAM tables. If some MyISAM tables are selected but the MySQL account does not have the `LOCK TABLES` privilege, the processing of the MySQL database system will fail.

   - `RELOAD` or `FLUSH_TABLES`. If some MyISAM tables are selected but the MySQL account does not have either `RELOAD` or `FLUSH_TABLES` privilege, the processing of the MySQL database system will fail.

   To obtain information about the privileges that are assigned to an account, use MySQL functionality, for example, the `SHOW GRANTS` statement. To learn more, see MySQL documentation.

Configuring MySQL Processing

To specify how Veeam Agent for Linux must process a MySQL database system, 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.

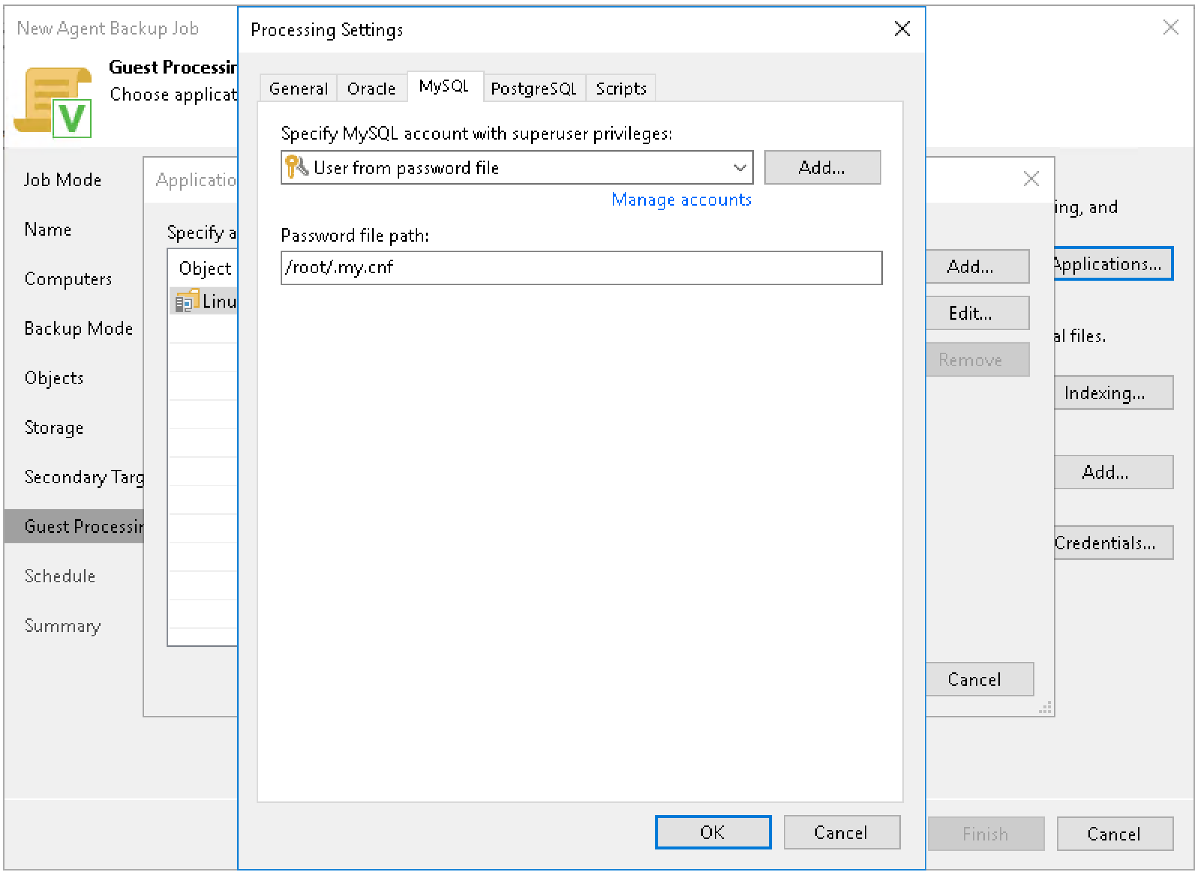
3. On the **MySQL** tab, specify a user account that Veeam Agent for Linux will use to connect to the MySQL database, from the **Specify MySQL account with superuser privileges** list, select a user account.

   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.


Processing Settings

Specify MySQL account with superuser privileges: User from password file

Password file path: /root/.my.cnf

PostgreSQL Processing Settings

You can specify how Veeam Agent for Linux must process the PostgreSQL database system.

Before You Begin

Before you configure the PostgreSQL processing, consider the following:

- Enable the following prerequisite settings:

   a. At the **Guest Processing** step of the wizard, the **Enable application-aware processing** check box is selected.

   b. 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.

   c. At the **Guest Processing** step of the wizard, in the **Guest OS credentials** list, a necessary user account is selected.

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

   To learn more, see Guest Processing Settings and Application-Aware Processing.

- Consider the Requirements and Limitations section in the Veeam Backup & Replication User Guide.

Configuring PostgreSQL Processing

> NOTE
>
> By default, Veeam Agent recursively scans the `/etc/postgresql`, `/var/lib/postgresql` and `/var/lib/pgsql` directories for the configuration files of PostgreSQL instances. If you keep configuration files in custom directories, the *pgsqlagent agent* will use its own `VeeamPostgreSQLAgent.xml` configuration file that is located in the `/etc/veeam/` directory. The pgsqlagent agent configuration file must be a single line XML.
>
> To explicitly include or exclude specific configuration files from rescan, you can add the following commands to the `VeeamPostgreSQLAgent.xml` file:
>
> - `ExcludeConfigDirs` — use this element to exclude configuration files.
> - `AddConfigDirs` — use this element to include configuration files.
>
> For example: `<config AddConfigDirs="/opt/psql/" ExcludeConfigDirs="/var/lib/postgresql/13/main45/,/var/lib/postgresql/13/maindd/" />`

To specify how Veeam Agent for Linux must process the PostgreSQL database system, 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. On the **PostgreSQL** tab, specify a user account that Veeam Agent for Linux will use to connect to the PostgreSQL database. You can do one of the following:

   - Select from the **Specify PostgreSQL account with superuser privileges** list a user account that has the required rights for the database.

     If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. With this option selected, Veeam Agent for Linux will connect to the PostgreSQL database under the account that you have selected in the **Specify PostgreSQL account with superuser privileges** list.

     Keep in mind that if you plan to select the peer authentication method at the step 4 of this procedure, you can add a user account in the Credentials Manager without specifying the password for the account.

   - Select the **Use guest OS credentials** option.

     With this option selected, Veeam Agent for Linux will do the following:

     i. Veeam Agent will check if you have specified custom credentials for the computer or protection group in the **Guest OS Credentials** window at the **Guest Processing** step of the wizard.

        If you specify custom credentials for the computer or protection group in the **Guest OS Credentials** window, Veeam Agent will process the PostgreSQL database under the account that you have specified in this window.

        If you do not specify custom credentials for the computer or protection group, Veeam Agent will do as described in the step ii of this procedure.

        To learn more, see step 5 in Specify Guest Processing Settings.

   ii. Veeam Agent will check what you have selected in the **Guest OS credentials** list at the **Guest Processing** step of the wizard.

       If you specify credentials in the **Guest OS credentials** list, Veeam Agent will process the PostgreSQL database under the account that you specify in this list.

       If you do not specify credentials in the list and select the **Use protection group credentials** option instead, Veeam Agent will do as described in the step iii of this procedure.

       To learn more, see step 4 in Specify Guest Processing Settings.

   iii. Veeam Agent will check what credentials you have specified for the computer or protection group at the **Computers** step of the wizard.

       If you specify stored credentials for this computer in the protection group settings, Veeam Agent will process the PostgreSQL database using the specified account.

       If you specify single-use credentials for this computer in the protection group settings, Veeam Agent will process the PostgreSQL database using the root user.

       To learn more, see Specifying Computers.

4. In the **The specified user is** field, specify how Veeam Agent will connect to the PostgreSQL database.

   The **The specified user is** field is connected closely with the **Specify PostgreSQL account with superuser privileges** list. Veeam Agent will do the following depending on what you specified using these two controls.

Control		Veeam Agent Behavior
Specify PostgreSQL Account with Superuser Privileges	The Specified User Is	
The **Use guest OS credentials** option is selected.	The **Database user with password** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the database user with the same name as the guest OS user.
	The **Database user with password file** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the password file stored in the home directory of the guest OS user.
	The **System user without password** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will use the guest OS user for peer connection to the PostgreSQL database.

Control		Veeam Agent Behavior
Specify PostgreSQL Account with Superuser Privileges	The Specified User Is	
The user account is specified.	The **Database user with password** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the database user specified in the **Specify PostgreSQL account with superuser privileges** list.
	The **Database user with password file** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the password file stored in the home directory of the user specified in the **Specify PostgreSQL account with superuser privileges** list.
	The **System user without password** option is selected.	• Veeam Agent will apply the user specified in the **Specify PostgreSQL account with superuser privileges** list. • Veeam Agent will use the selected user for peer connection to the PostgreSQL database.

5. 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. 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.

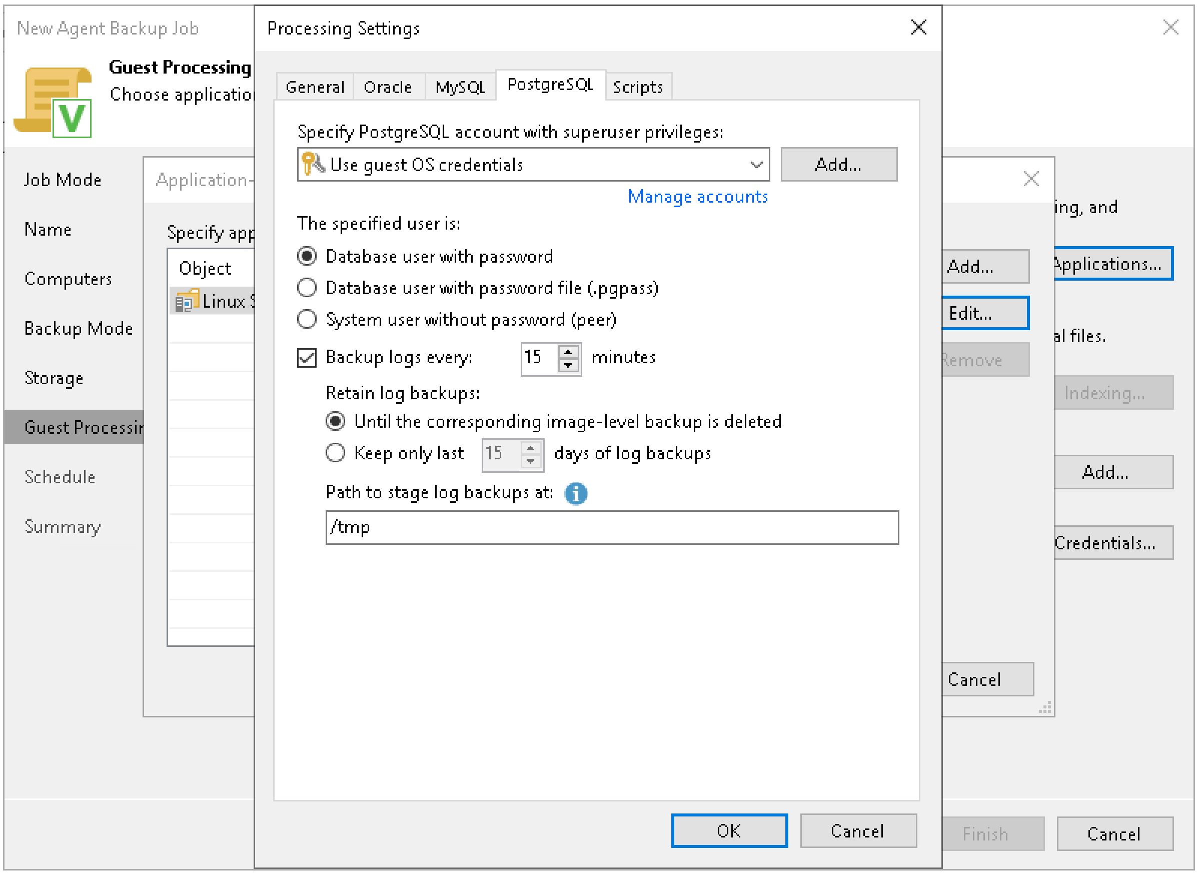
7. In the **Path to stage log backups at** field, specify temporary storage location for the archive logs.

   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.



Processing Settings

General | Oracle | MySQL | PostgreSQL | Scripts

Specify PostgreSQL account with superuser privileges:

Use guest OS credentials [Add...]

Manage accounts

The specified user is:

● Database user with password

○ Database user with password file (.pgpass)

○ System user without password (peer)

☑ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

Path to stage log backups at:

/tmp

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 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.

  You can specify only backup job scripts that will be executed on Linux computers if you selected the **Backup directly from live file system** option at the Backup Mode step of the wizard.

TIP

You can also specify custom scripts that will be executed on the backup server before and 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**.

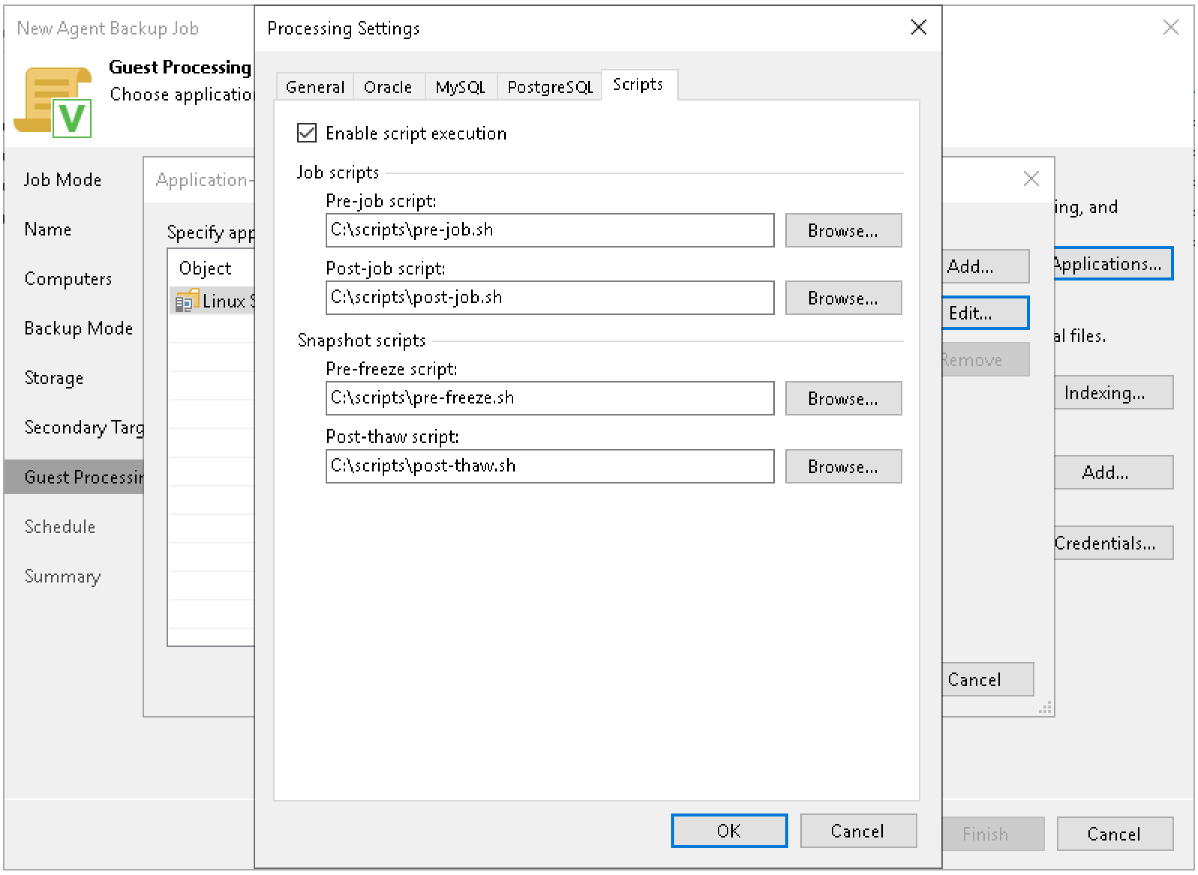
   To define custom settings for a computer added as a part of a protection group, you must include the computer to the list as a standalone object. To do this, click **Add** and choose the computer whose settings you want to customize. Then select the computer in the list and define the necessary settings.
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 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 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.



☑ Enable script execution

Job scripts

Pre-job script: C:\scripts\pre-job.sh

Post-job script: C:\scripts\post-job.sh

Snapshot scripts

Pre-freeze script: C:\scripts\pre-freeze.sh

Post-thaw script: C:\scripts\post-thaw.sh

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**.

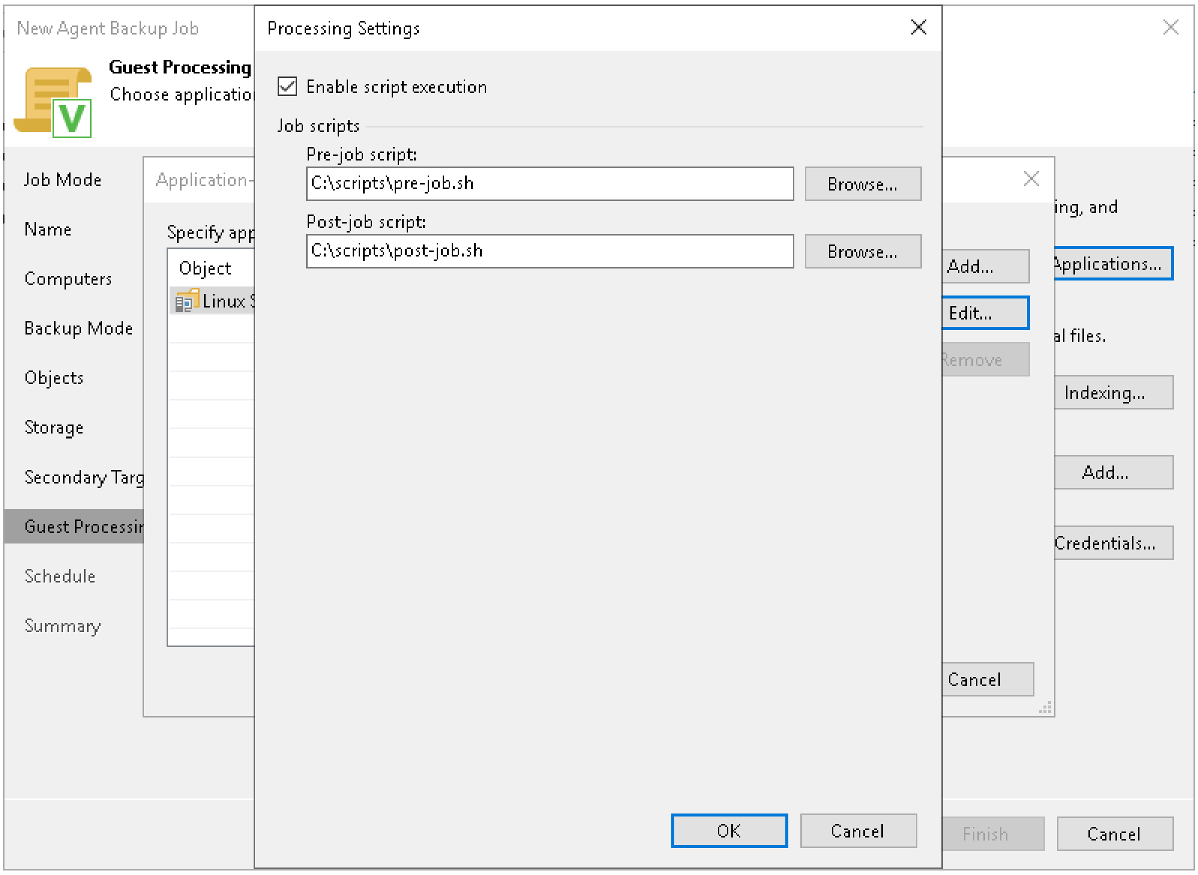
3. In the displayed list, select a protection group or individual computer and click **Edit**.

   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.



☑ Enable script execution

Job scripts

Pre-job script: C:\scripts\pre-job.sh

Post-job script: C:\scripts\post-job.sh

File Indexing

You can instruct the Veeam Agent backup job managed by the backup server 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. For more information on file system indexing, see the File System Indexing topic in the Veeam Agent for Linux User Guide.

> **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 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 add 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.

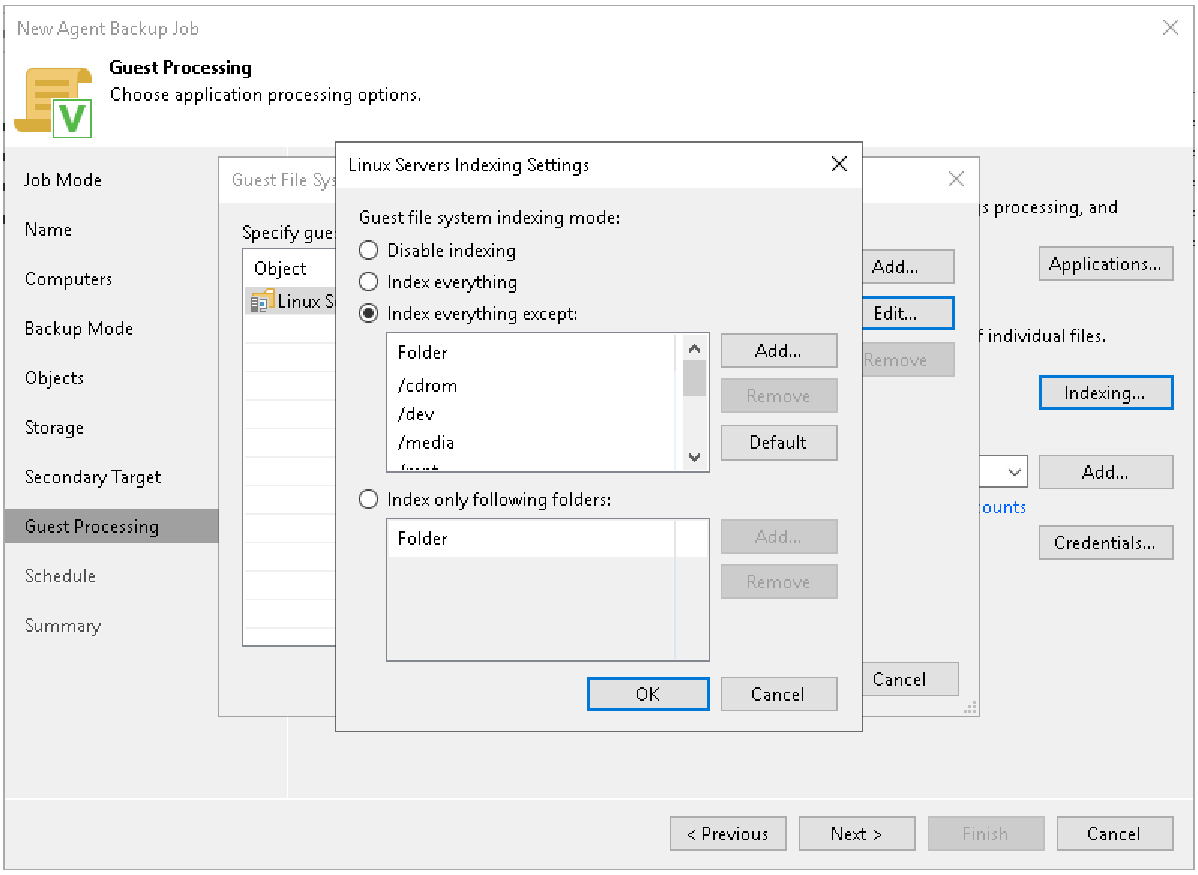
4. In the **Indexing Settings** window, specify the indexing scope:

   - 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.



New Agent Backup Job

Guest Processing

Choose application processing options.

Linux Servers Indexing Settings

Guest file system indexing mode:

○ Disable indexing

○ Index everything

● Index everything except:

Folder
/cdrom
/dev
/media

○ Index only following folders:

Folder

Step 11. 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 do one of the following:

     - Select the necessary time unit: *Hours* or *Minutes*.

     - 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.

   - 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.

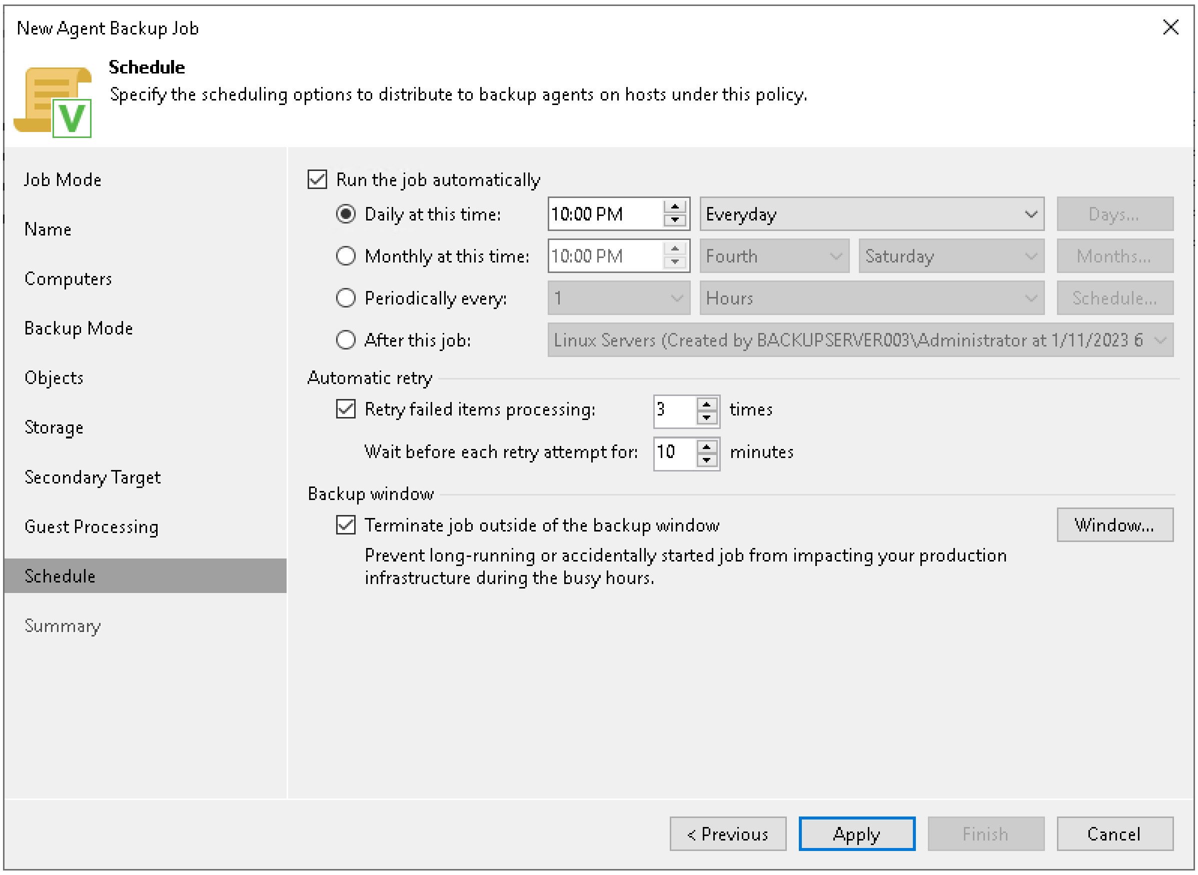
     > NOTE
     >
     > The **After this job** function will automatically start a job if the first job in the chain is started automatically by schedule. If you start the first job manually, Veeam Backup & Replication will display a notification. You will be able to choose whether Veeam Backup & Replication 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.



New Agent Backup Job

Schedule

Specify the scheduling options to distribute to backup agents on hosts under this policy.

Job Mode
Name
Computers
Backup Mode
Objects
Storage
Secondary Target
Guest Processing
Schedule
Summary

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday Days...

○ Monthly at this time: 10:00 PM Fourth Saturday Months...

○ Periodically every: 1 Hours Schedule...

○ After this job: Linux Servers (Created by BACKUPSERVER003\Administrator at 1/11/2023 6

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

☑ Terminate job outside of the backup window Window...

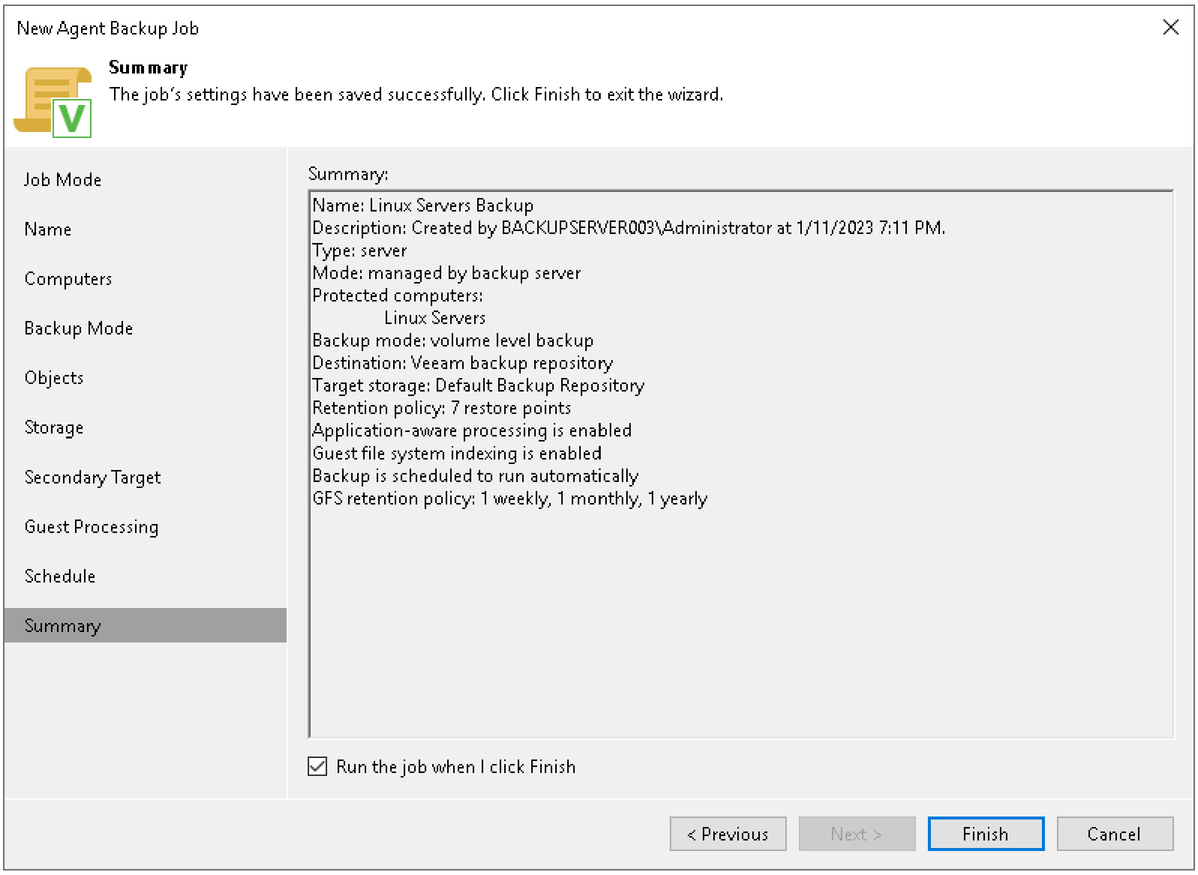
Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.

< Previous Apply Finish Cancel

Step 12. 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. 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.



```
Name: Linux Servers Backup
Description: Created by BACKUPSERVER003\Administrator at 1/11/2023 7:11 PM.
Type: server
Mode: managed by backup server
Protected computers:
            Linux Servers
Backup mode: volume level backup
Destination: Veeam backup repository
Target storage: Default Backup Repository
Retention policy: 7 restore points
Application-aware processing is enabled
Guest file system indexing is enabled
Backup is scheduled to run automatically
GFS retention policy: 1 weekly, 1 monthly, 1 yearly
```

☑ Run the job when I click Finish

Creating Veeam Agent Backup Policies

To create a Veeam Agent backup policy, you must create a backup job 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

Consider the following:

- After you create a Veeam Agent 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.
- You must create a Veeam Agent backup policy if you want to protect computers with pre-installed Veeam Agents. To learn more, see Protection Group Types.
- 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.
- You cannot create a Veeam Agent backup policy if you want to protect cloud machines. In this case, you must create a Veeam Agent backup job managed by the backup server. To learn more, see Creating Veeam Agent Backup Jobs

Creating Policy for Windows Computers

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

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 workstations that you plan to add to the Veeam Agent backup policy. To learn more, see Licensing Requirements.
- 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.
- [For backup policies 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:

- 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.
- You cannot map a Veeam Agent backup policy to a Veeam Agent backup chain created by another type of a Veeam Agent backup job. After you change the mode of a Veeam Agent computer, Veeam Backup & Replication starts a new backup chain in a target location specified in the backup policy settings.
- 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 policy targeted at a cloud repository.
- You cannot add a Veeam Agent computer protected by a backup job managed by the backup server to a Veeam Agent backup policy. To add such a computer to a Veeam Agent backup policy, first remove the computer from the backup job managed by the backup server.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup policy for protected computers that run a Microsoft Windows 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 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** > **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 Policy

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** > **Windows** > **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** > **Windows** > **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 individual computers to the policy later on, when you pass through the wizard steps.

Adding Computers to New Backup Policy

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

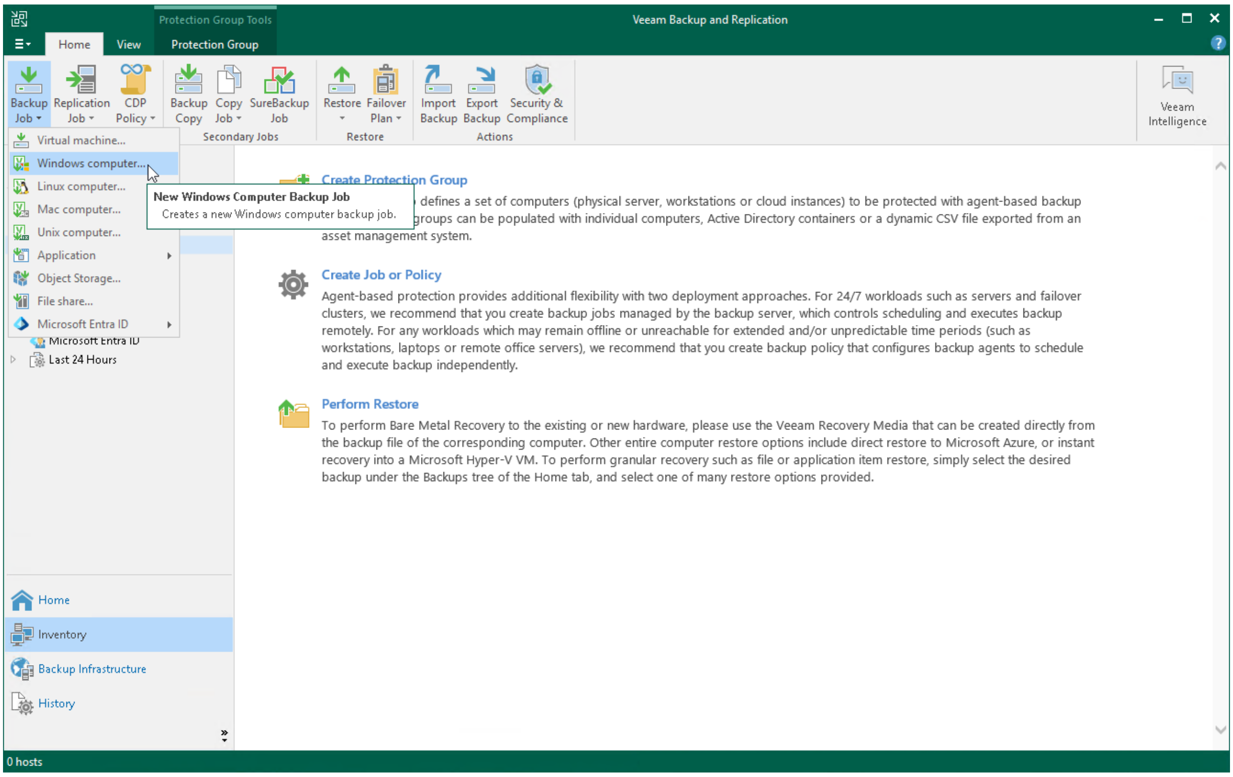
- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup policy. In the working area, select one or more computers that you want to add to the policy, right-click the selected computer and select **Add to backup job** > **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 protection groups to the policy later on, when you pass through the wizard steps.

TIP

Consider the following:

- You can press and hold the [Ctrl] key 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.



Create Protection Group

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

Create Job or Policy

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

Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify the type of protected computers and select the **Managed by agent** job mode:

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 on servers, select the job mode.

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 policy and what policy settings will be available at subsequent steps of the wizard. For Veeam Agent backup policy, you can select one of the following computer types:

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

  For backup policies 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 the Veeam Agent for Microsoft Windows User Guide.

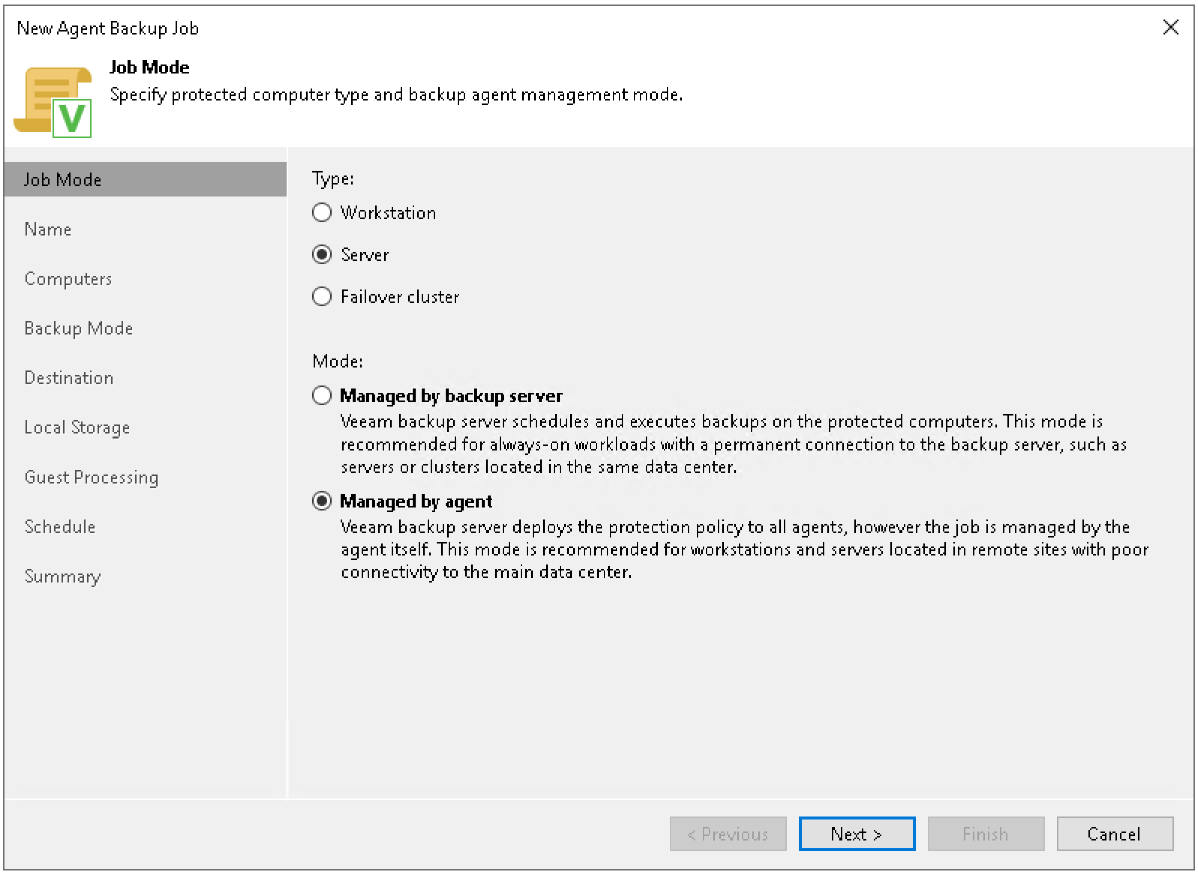
  With this option selected, you can also select the job mode. To learn more, see Selecting Job Mode.

> NOTE
>
> You cannot select the **Failover cluster** option if you want to create a backup job managed by Veeam Agent.

Selecting Job Mode

If you selected the **Workstation** computer type in the **Type** field, you do not need to select the job mode in the **Mode** field, the **Managed by agent** job mode will be selected automatically.

If you selected the **Server** computer type in the **Type** field, in the **Mode** field, select the **Managed by agent** job mode to create a Veeam Agent backup policy. If you select the **Managed by backup server** job mode, you will create a Veeam Agent backup job managed by the backup server.



New Agent Backup Job

Job Mode

Specify protected computer type and backup agent management mode.

Type:

○ Workstation

● Server

○ Failover cluster

Mode:

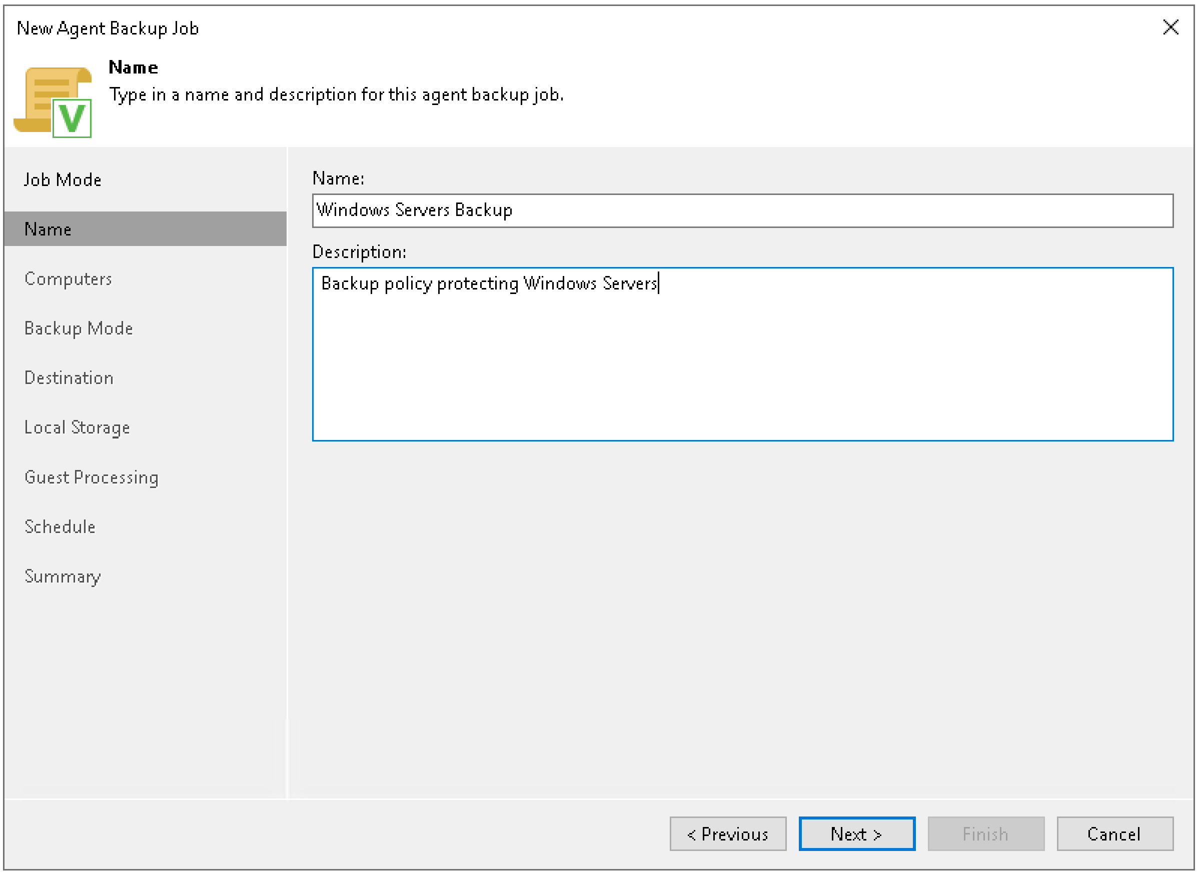
○ **Managed by backup server**
Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

● **Managed by agent**
Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

Step 3. Specify Job 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 job, date and time when the job was created.



Name: Windows Servers Backup

Description: Backup policy protecting Windows Servers

Step 4. Select Computers to Back Up

At the **Computers** step of the wizard, select protection groups and individual computers whose data you want to back up with Veeam Agent backup policy.

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

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
>
> Consider the following:
>
> - 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 policy. You can remove some computers from the policy or add new computers to the policy, if necessary.
> - You cannot add protection groups for cloud machines to backup policies. 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. To learn more, see Selecting Job Mode.

Adding Protection Groups and Computers from Inventory

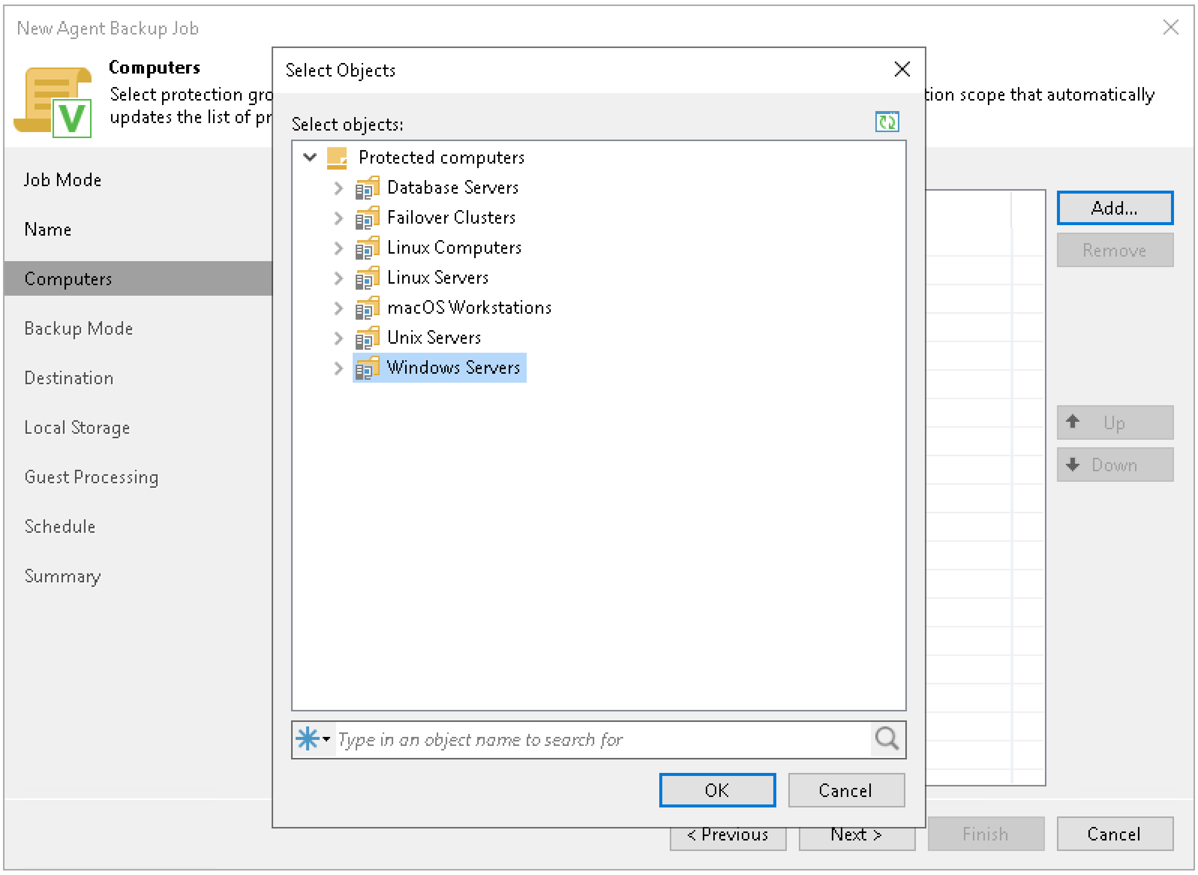
To add protection groups and individual computers to the Veeam Agent backup policy, do the following:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and computers in the list and click **OK**. You can press and hold the [Ctrl] or [Shift] key 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].



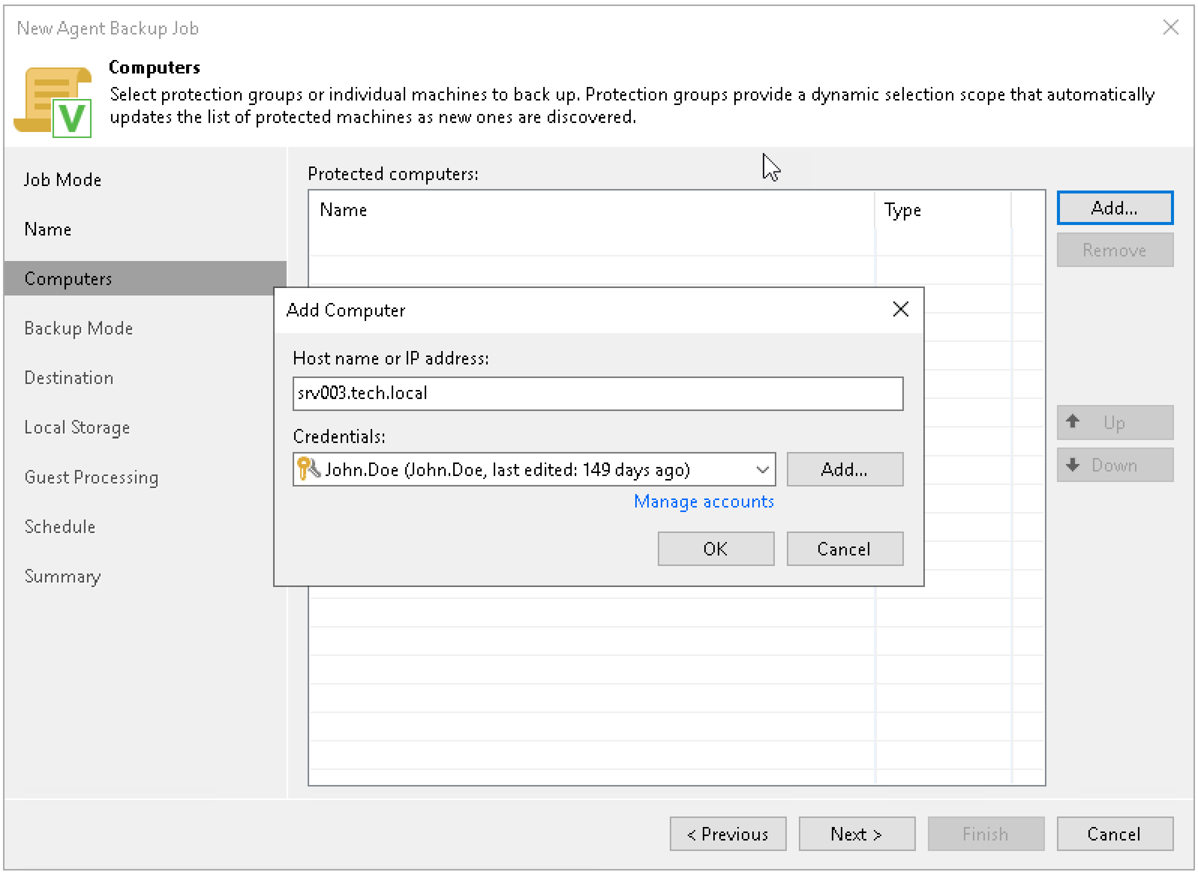
Adding New Computers

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

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 policy.

3. From the **Credentials** list, select a user account that has administrative permissions on the computer that you want to add to the policy. 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.



Computers

Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

Add Computer

Host name or IP address: srv003.tech.local

Credentials: John.Doe (John.Doe, last edited: 149 days ago)

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 the Destination step of the wizard.

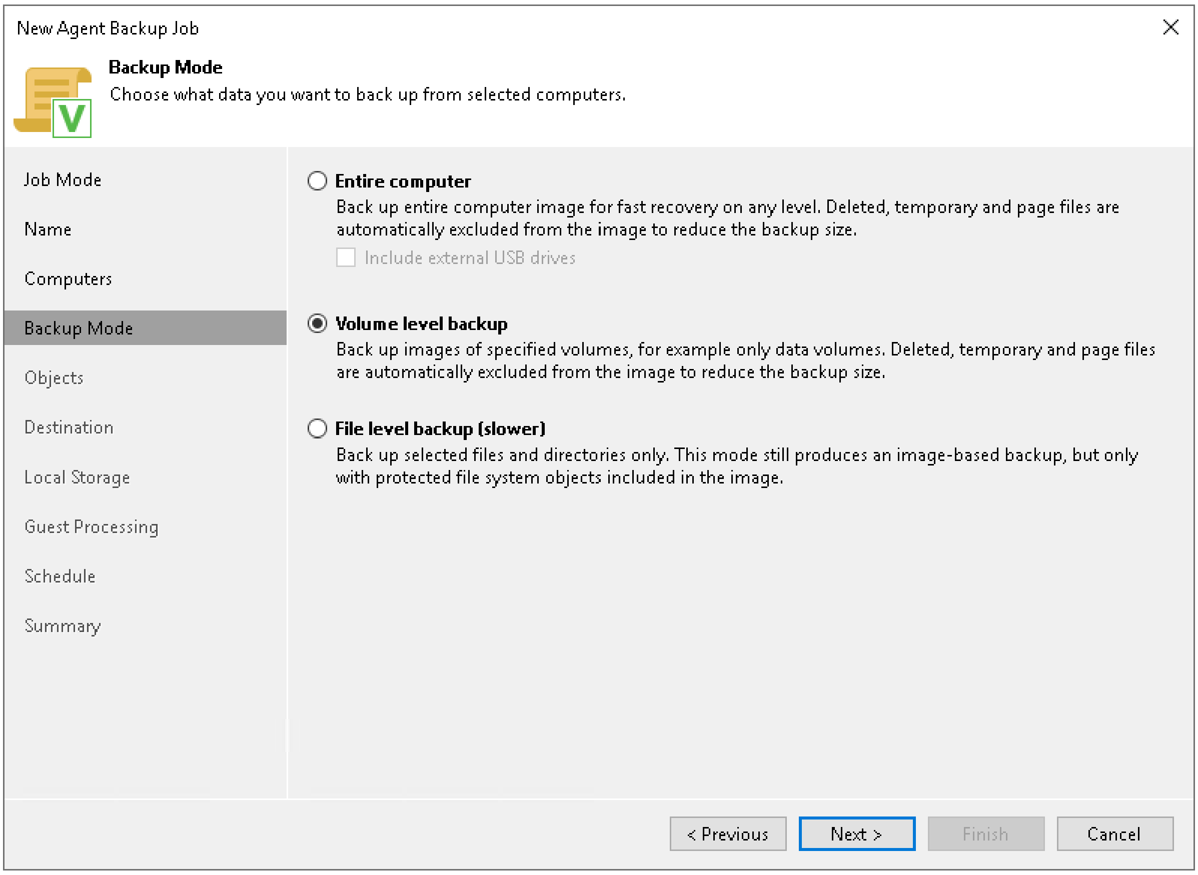
   - **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, all volumes except the system one. When you restore data from such backup, you will be able to recover data located on these volumes only: files, folders, application data and so on. 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 policy starts. To learn more, see the Backup of External Drives section in the Veeam Agent for Microsoft Windows User Guide.

NOTE

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 policy 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, we recommend that you configure volume-level backup instead of file-level backup.



New Agent Backup Job

Backup Mode

Choose what data you want to back up from selected computers.

○ **Entire computer**

Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

□ Include external USB drives

● **Volume level backup**

Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **File level backup (slower)**

Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.

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 policy:

- 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 policy. If a specified volume does not exist on one or more computers in the policy, the policy 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 on 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, 2022 and 2025, 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.

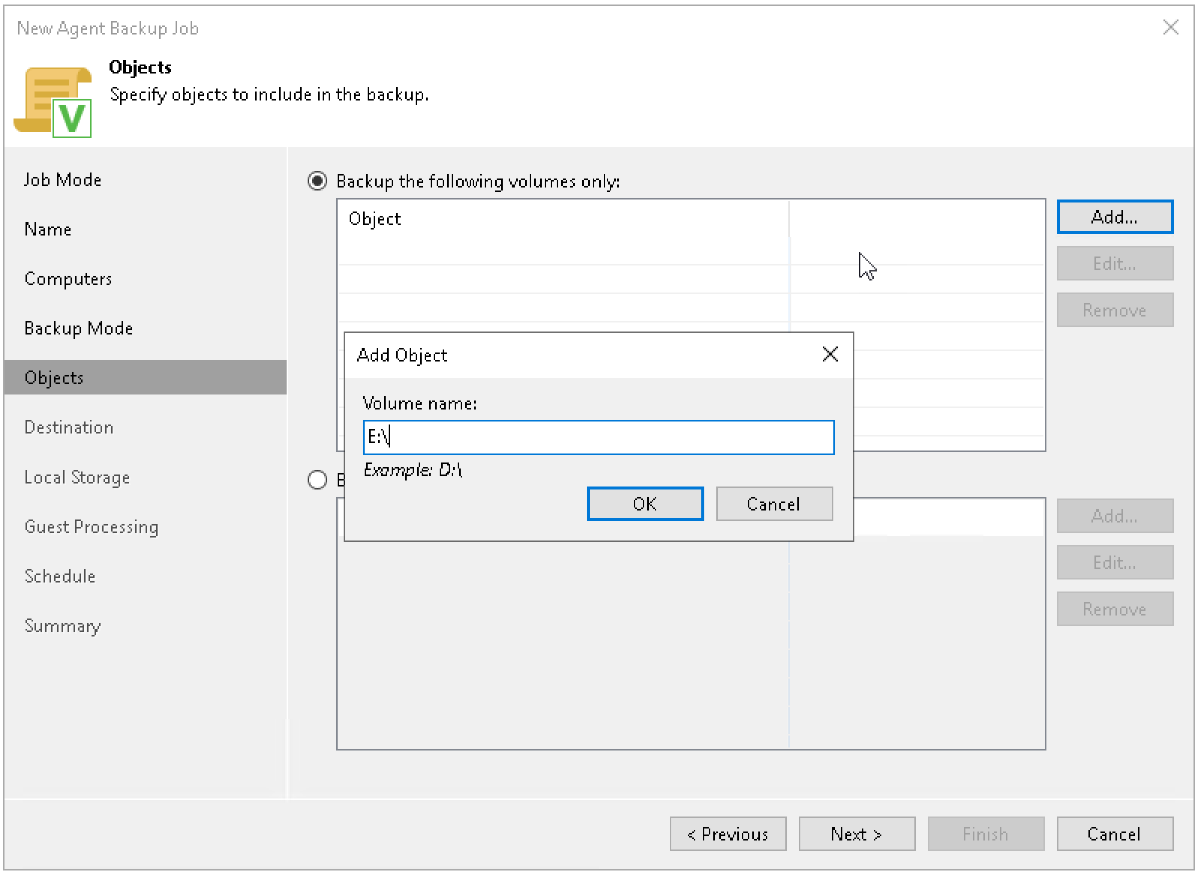
  b. In the **Add Object** window, type the path to a folder that is an entry point to the mounted volume you want to back up, for example, `C:\Data`, and click **OK**.

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

NOTE

Consider 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.


New Agent Backup Job

Objects
Specify objects to include in the backup.

● Backup the following volumes only:

Add Object

Volume name: E:\

Example: D:\

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 by defining 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 policy. If a specified object does not exist on one or more computers in the policy, the policy 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 policy run different versions of Microsoft Windows OSes, and actual paths to directories that contain data of the same type differ on these computers.

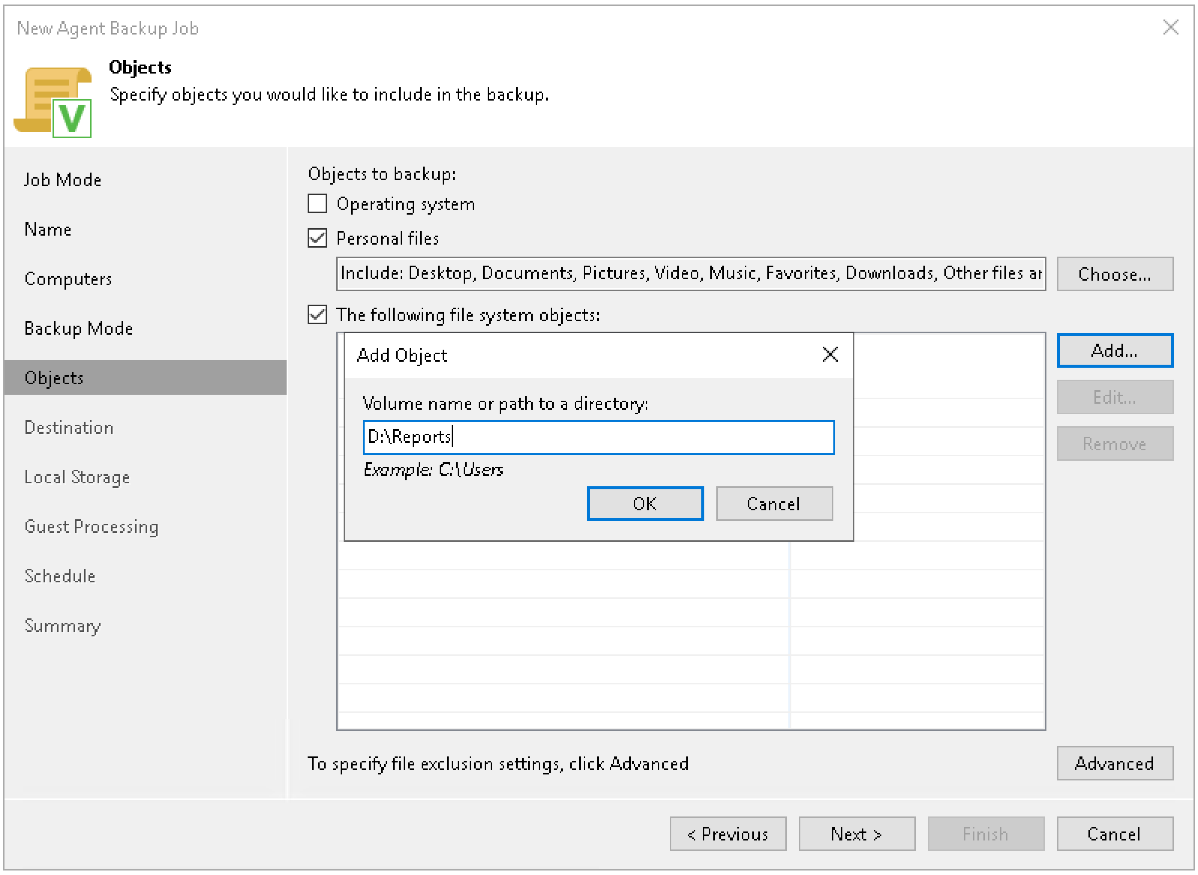
   Consider the following:

   - You can use only system environment variables — variables defined for the Local System account on computers added to the backup policy. 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

Consider 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.


New Agent Backup Job

Objects

Specify objects you would like to include in the backup.

Objects to backup:

☐ Operating system

☑ Personal files

Include: Desktop, Documents, Pictures, Video, Music, Favorites, Downloads, Other files ar

☑ The following file system objects:

Add Object

Volume name or path to a directory:

D:\Reports

Example: C:\Users

To specify file exclusion settings, click Advanced

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.
- If you want to include or exclude files in/from the file-level backup, you can use file names and masks for file types as filters. You cannot use paths to files.

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 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 paths to folders that contain files that you do not want to back up and file names and 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 that reside in the backed-up folder except files in the specified folders and 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 policy, 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*`

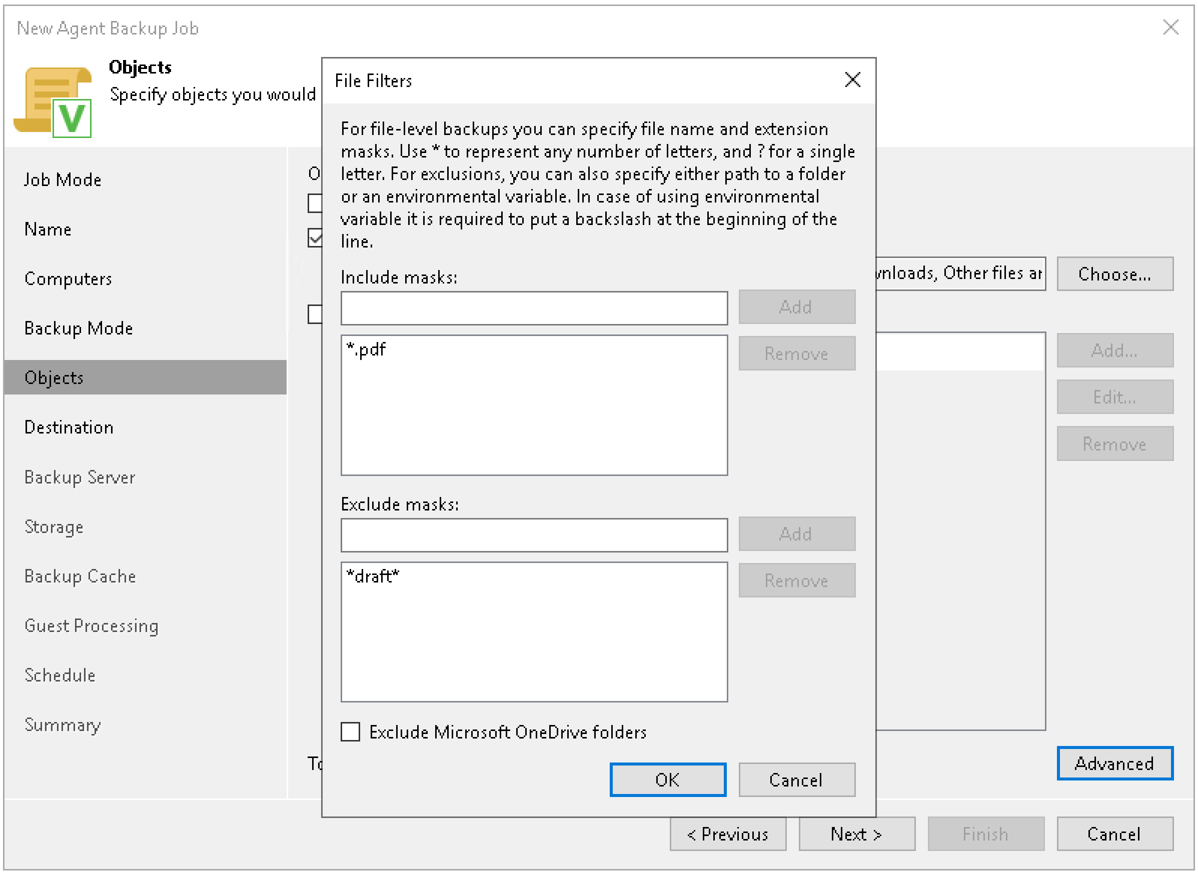
The resulting Veeam Agent backup will contain all files of the PDF format that do not contain *draft* in their names.

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.



New Agent Backup Job

Objects

Specify objects you would

File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks:

*.pdf

Exclude masks:

draft

□ Exclude Microsoft OneDrive folders

Step 7. Select Backup Destination

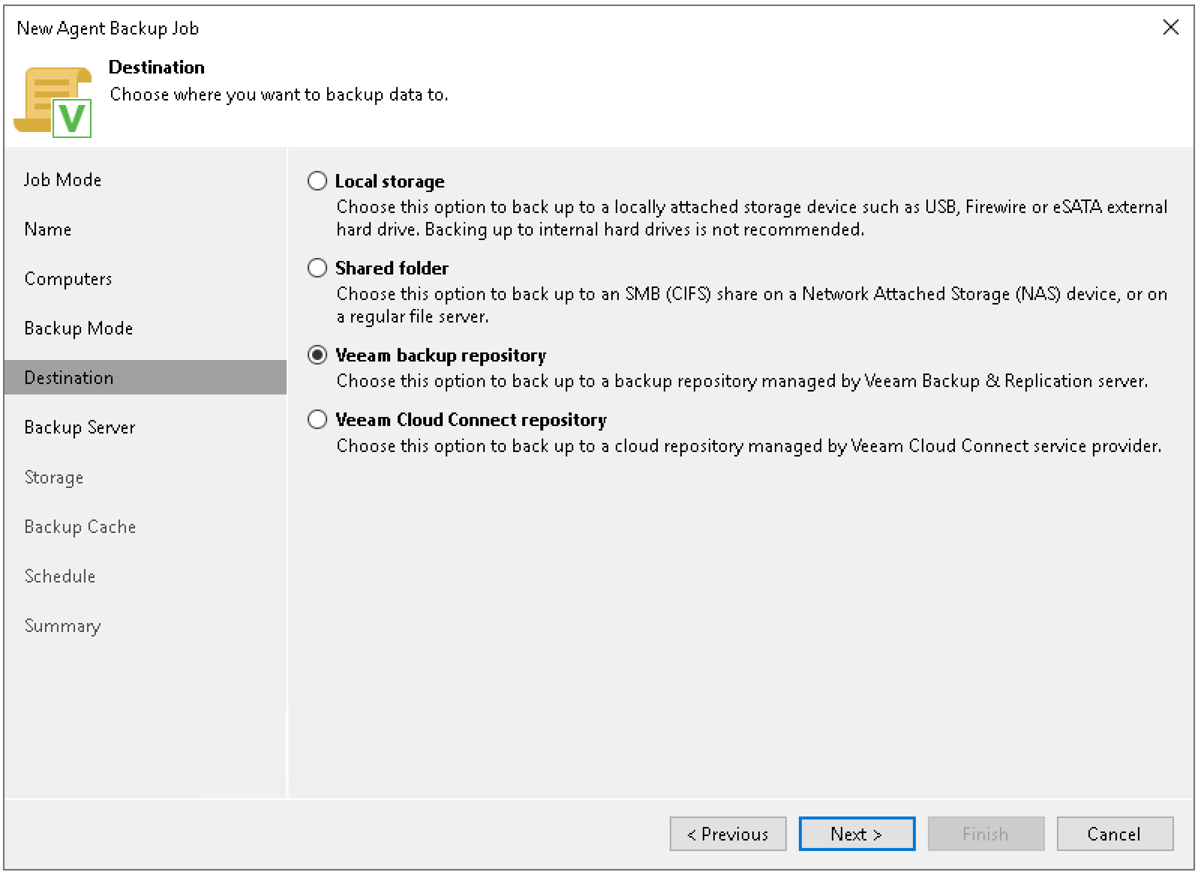
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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
>
> Consider the following:
>
> - It is strongly recommended that you store backups in the external location like USB storage device or network shared 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 an SMB 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 policy 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.



New Agent Backup Job

Destination
Choose where you want to backup data to.

○ **Local storage**
Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.

○ **Shared folder**
Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.

● **Veeam backup repository**
Choose this option to back up to a backup repository managed by Veeam Backup & Replication server.

○ **Veeam Cloud Connect repository**
Choose this option to back up to a cloud repository managed by Veeam Cloud Connect service provider.

Step 8. Specify Backup Storage Settings

Specify backup storage settings for the Veeam Agent backup policy:

- 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

At the **Local Storage** step of the wizard, 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 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, we recommend that you do not use such USB storage devices as a backup target.
   > - We do not recommend targeting a backup policy 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 except days when no backup files are created. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

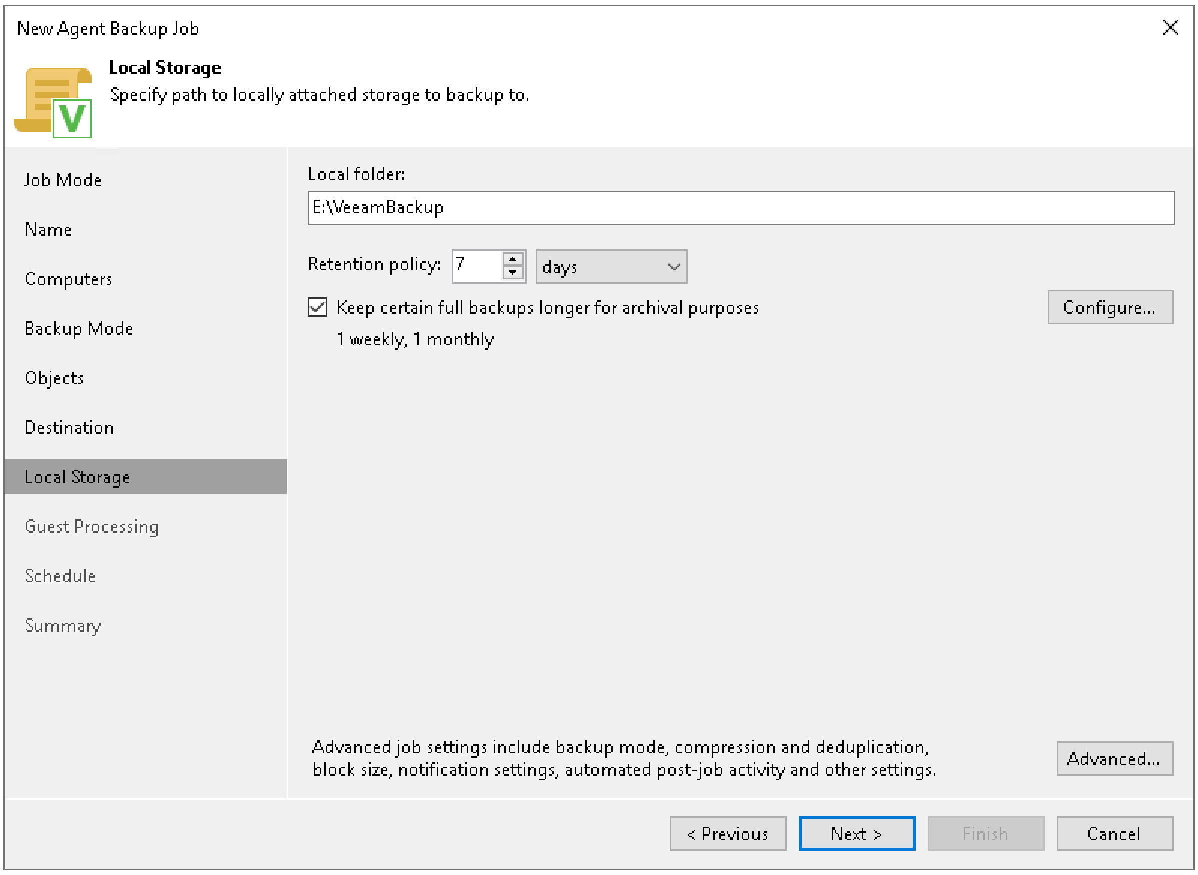
     Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

   To learn more, see Short-Term Retention Policy.

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 policy. To learn more, see Specify Advanced Backup Settings.



Local folder: E:\VeeamBackup

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Shared Folder Settings

At the **Shared Folder** step of the wizard, specify shared folder settings:

1. In the **Shared folder** field, type a UNC name of the SMB 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 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.

   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 except days when no backup files are created. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

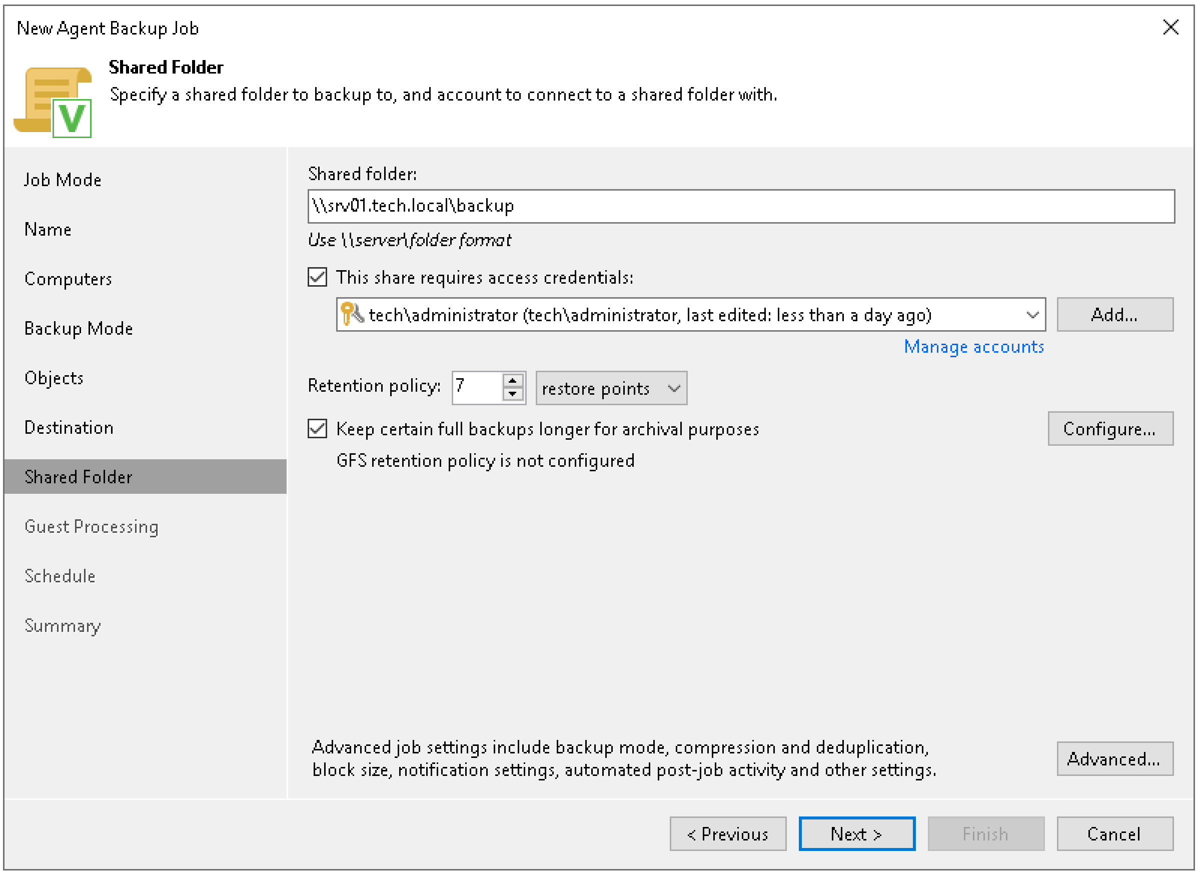
  Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

To learn more, see Short-Term Retention Policy.

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 policy. To learn more, see Specify Advanced Backup Settings.



Shared Folder

Specify a shared folder to backup to, and account to connect to a shared folder with.

Shared folder: \\srv01.tech.local\backup

Use \\server\folder format

☑ This share requires access credentials:

tech\administrator (tech\administrator, last edited: less than a day ago)

Retention policy: 7 restore points

☑ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Veeam Backup Repository Settings

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

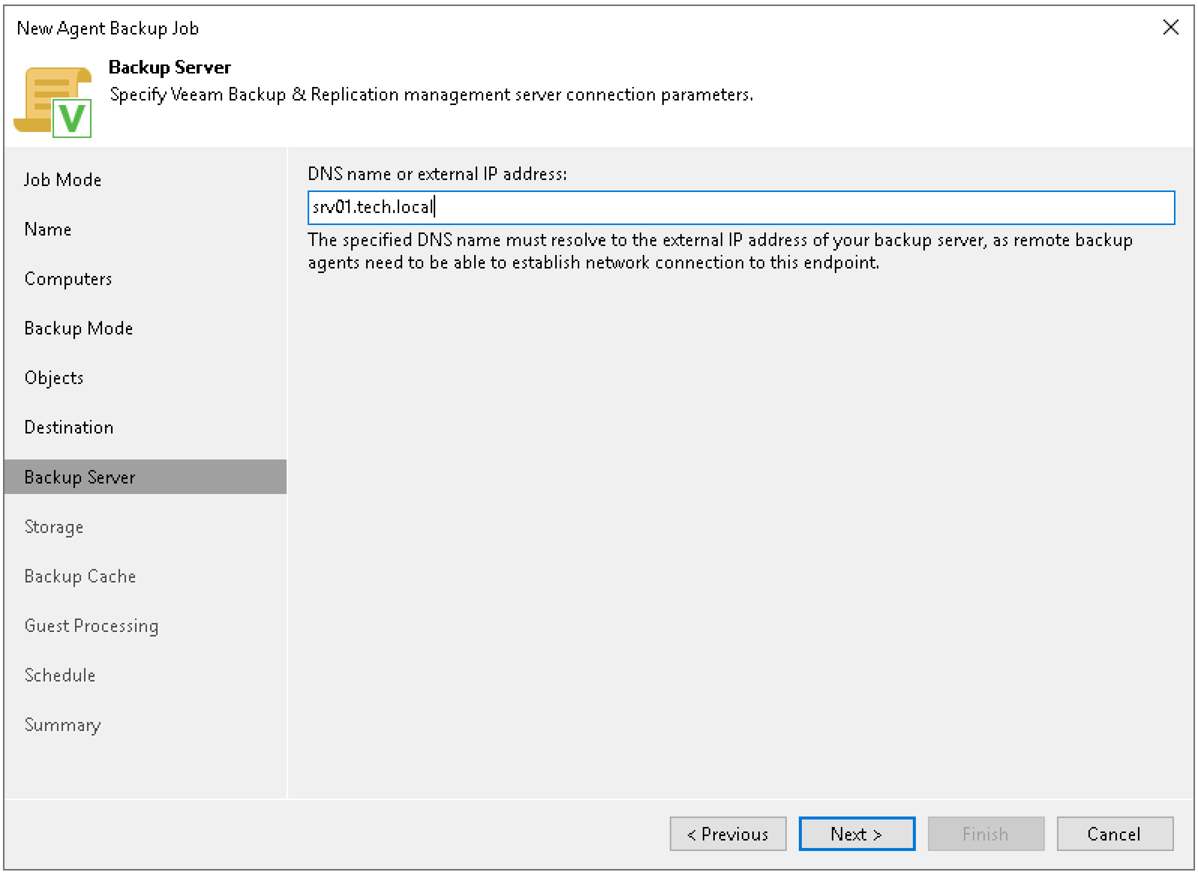
1. At the Backup Server step of the wizard, specify backup server settings.
2. At the Storage step of the wizard, select the Veeam backup repository.

Specifying Backup Server Settings

The **Backup Server** step of the wizard is available if you have chosen to store backup files in a Veeam backup repository.

In the **DNS name or external IP address field**, make sure that the name or IP address of the Veeam backup server, on which you configure the Veeam Agent backup policy, is displayed. Do not specify the name or IP address of another Veeam backup server. The specified DNS name or IP address must be resolvable from Veeam Agent computers.

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


New Agent Backup Job

Backup Server

Specify Veeam Backup & Replication management server connection parameters.

DNS name or external IP address: srv01.tech.local

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

Selecting Backup Repository

The **Storage** step of the wizard is available if you have 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 except days when no backup files are created. 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.

   To learn more, see Short-Term Retention Policy.

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.

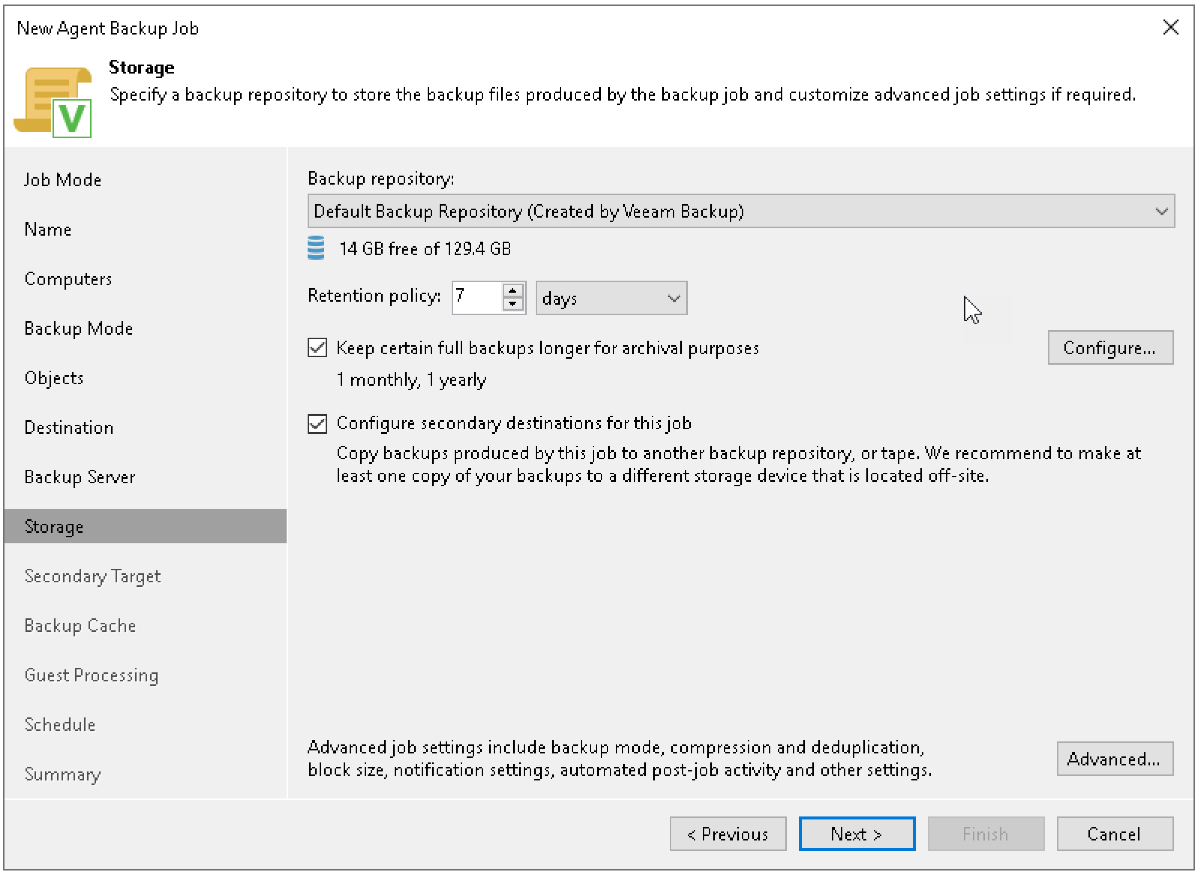
4. If you want to archive backup files created with the backup job to a secondary destination (backup repository or tape), select the **Configure secondary destinations for this job** check box. With this option enabled, the **New Agent Backup Job** wizard will include an additional step — Secondary 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 policy. To learn more, see Specify Advanced Backup Settings.

NOTE

You must enable backup file encryption in the backup job storage settings if you back up data to the Veeam Data Cloud Vault storage added as a Veeam backup repository.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Default Backup Repository (Created by Veeam Backup)

14 GB free of 129.4 GB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

1 monthly, 1 yearly

☑ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Cloud Repository Settings

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 Before You Begin.

At the **Storage** step of the wizard, 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 except days when no backup files are created. After this period is over, Veeam Backup & Replication will remove the earliest restore points from the backup chain.

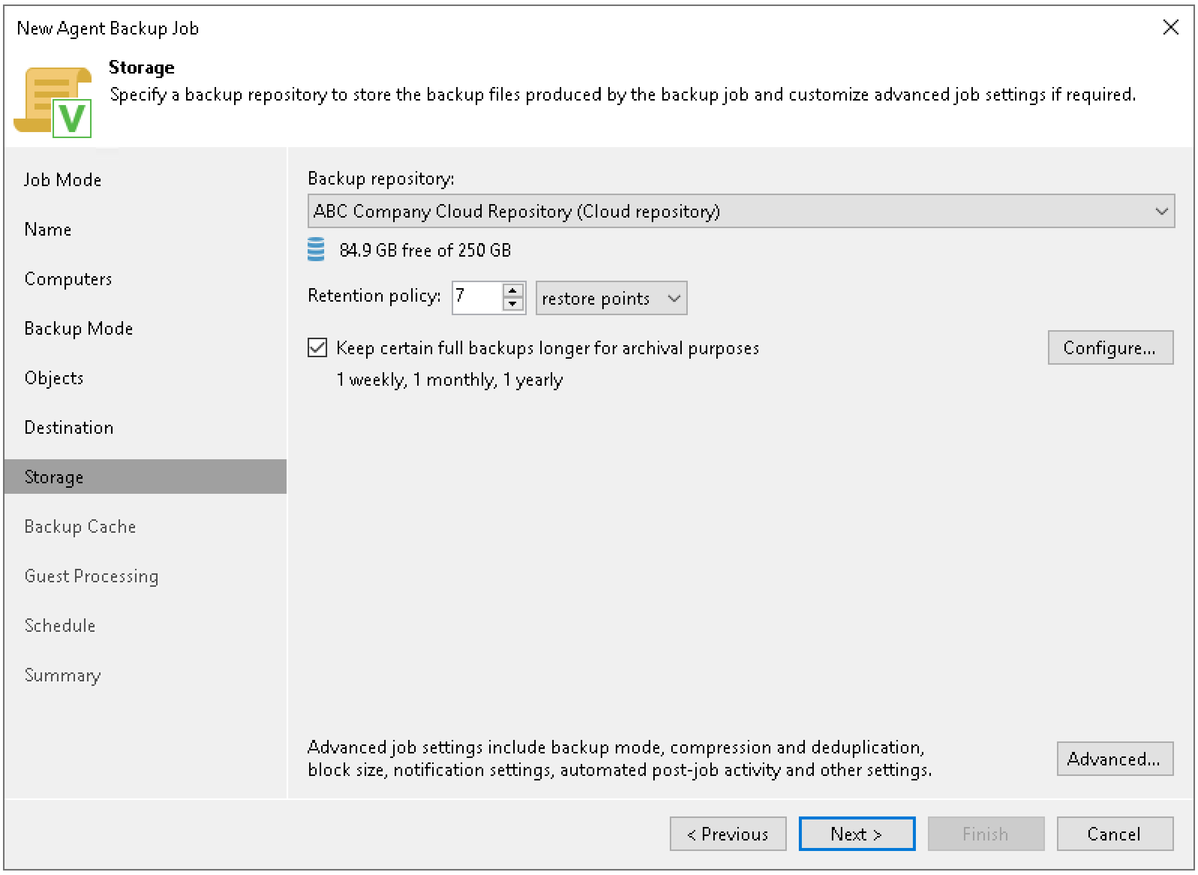
  Keep in mind that if you have selected the **Workstation** type at the Job Mode step of the wizard, you can specify retention policy only in days.

To learn more, see Short-Term Retention Policy.

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.

> **IMPORTANT**
>
> You must enable backup file encryption in the backup job storage settings if you back up data to the Veeam Data Cloud Vault storage added as a Veeam Cloud Connect repository.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: ABC Company Cloud Repository (Cloud repository)

84.9 GB free of 250 GB

Retention policy: 7 restore points

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other 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:
   - **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.

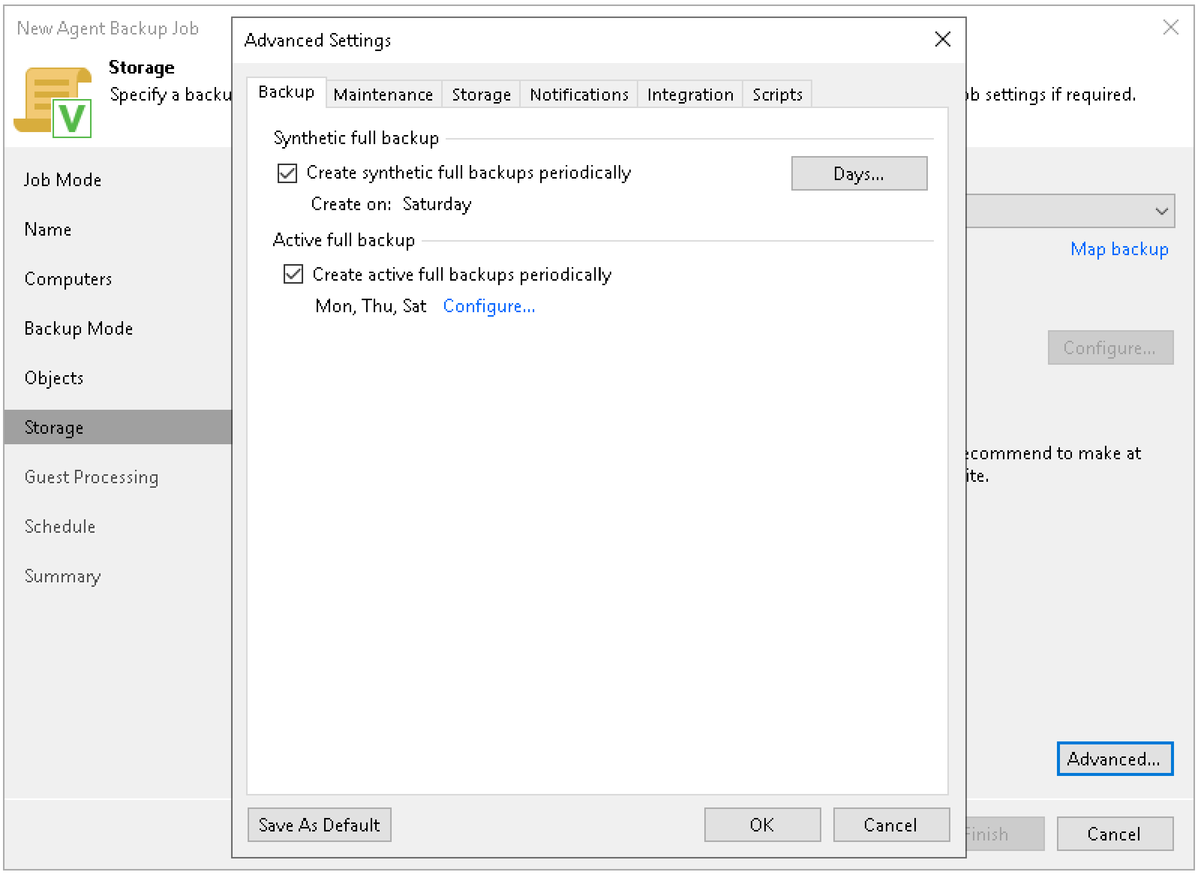
   > **NOTE**
   >
   > Synthetic full backup is not available for backup policies targeted at an object storage repository.

3. If you want to periodically create active full backups, select the Create active full backups periodically check box. Click Configure and use the **Monthly on** or **Weekly** options to define scheduling settings.

NOTE

Consider the following:

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



Synthetic full backup

☑ Create synthetic full backups periodically

Create on: Saturday

Active full backup

☑ Create active full backups periodically

Mon, Thu, Sat Configure...

Maintenance Settings

To specify maintenance 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. 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 policies, 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 policy settings. Keep in mind that enabling this setting may result in additional charges from your object storage provider.

4. [For backup 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 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. 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 policy 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 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.

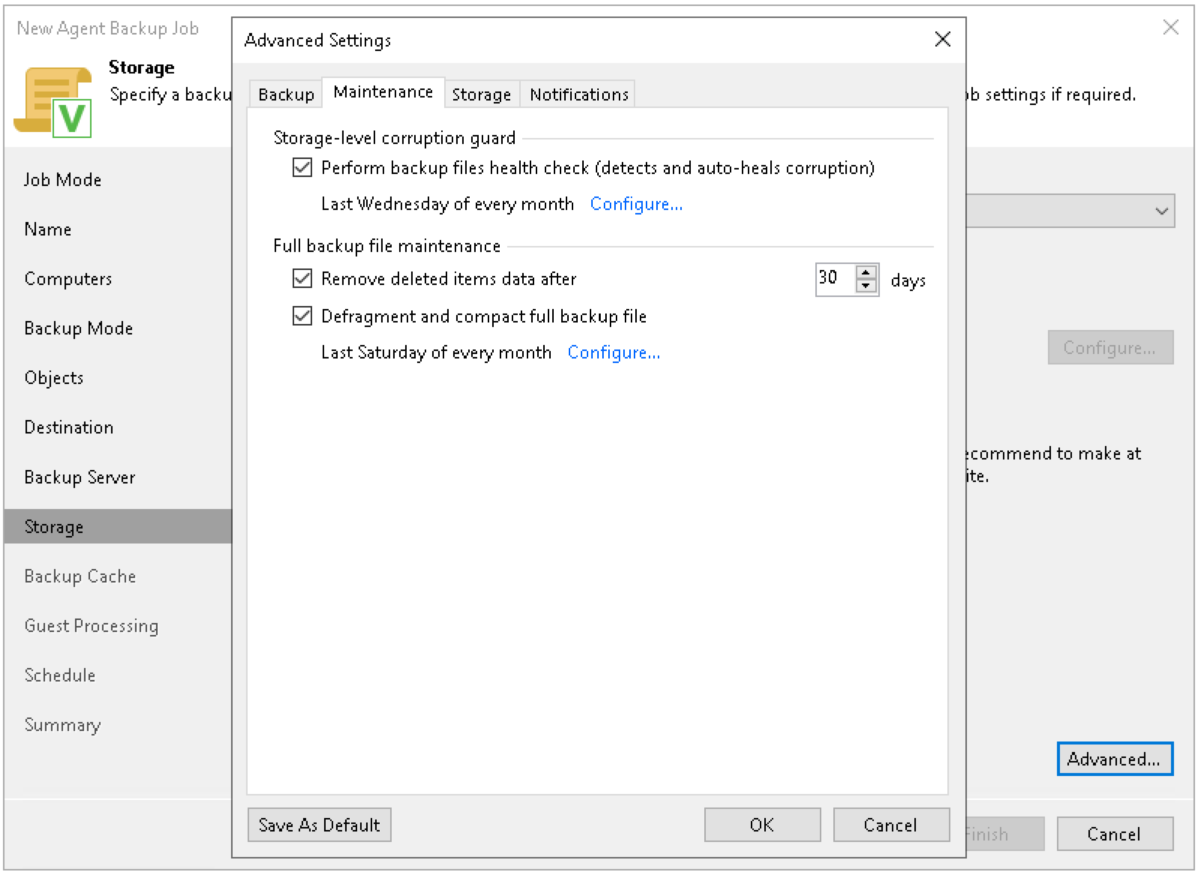
   > NOTE
   >
   > The **Defragment and compact full backup file** option is not available for backup policies targeted at object storage.

   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-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption)

Last Wednesday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 30 days

☑ Defragment and compact full backup file

Last Saturday of every month Configure...

Storage Settings

To specify storage 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 **Storage** tab.

3. From the **Compression level** list, select a compression level for the backup: *None*, *Dedupe-friendly*, *Optimal*, *High* or *Extreme*. To learn more about the compression levels, see the Data Compression section in the Veeam Agent for Linux User Guide.

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 for Microsoft Windows will use data blocks of the chosen size to optimize the size of backup files and job performance.

   > NOTE
   >
   > If you change the storage optimization settings for the backup job, new settings will not have any effect on previously created files in the chain. They will be applied to new files created after the settings were changed.
   >
   > To apply new storage optimization settings in backup jobs, you must create an active full backup after you change storage optimization settings. Veeam Backup & Replication will use the new block size for the active full backup and subsequent backup files in the backup chain. To learn about the active full backup, see Performing Active Full Backup.

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.

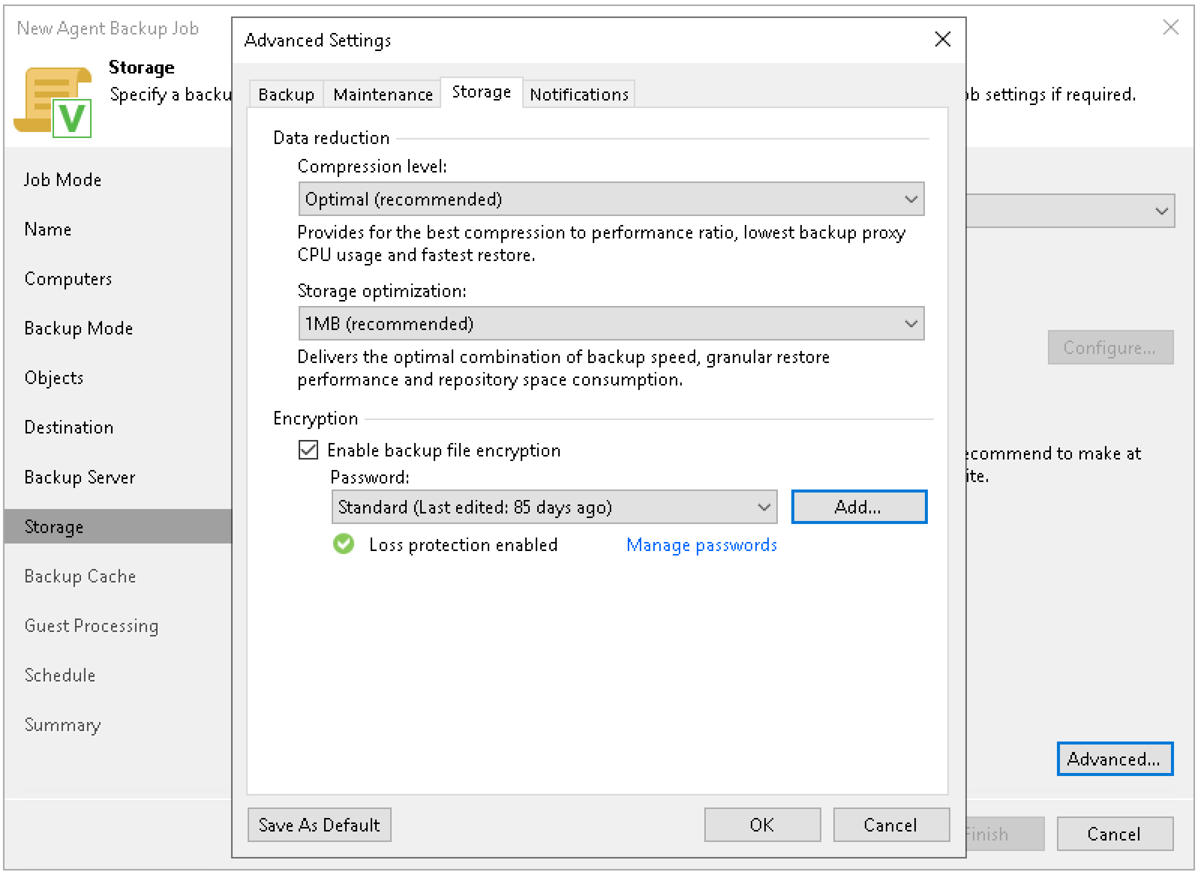
   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it. For more information, see the Decrypting Data Without Password section in the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

NOTE

Consider the following:

- If you plan to encrypt the content of backup files, consider the limitations listed in the Data Encryption Limitations subsection.
- You must encrypt the backup policy if you want to back up data to the Veeam Data Vault storage.
- You cannot use Key Management System (KMS) keys for data encryption with a Veeam Agent backup policy. To be able to use KMS keys, create a backup job managed by the backup server.

  To learn more about KMS keys, see the Key Management System Keys section in the Veeam Backup & Replication User Guide.



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 (Last edited: 85 days ago) Add...

Loss protection enabled Manage passwords

Data Encryption Limitations

If you plan to encrypt the content of backup files, consider the following limitations:

- Data encryption settings for Veeam Agent backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database.

  For backup policies targeted at a Veeam backup repository, all data encryption operations are performed in Veeam Backup & Replication. 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 an SMB network shared folder, or at a cloud repository. Veeam Backup & Replication passes encryption settings 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 backup policies targeted at a Veeam backup repository are saved to the Veeam Backup & Replication database and are not passed to a Veeam Agent computer.
- If you enable or disable 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 policy, Veeam Agent for Microsoft Windows will encrypt the backup chain starting from the next restore point created with this policy.
- [For backup policies targeted at a local drive, network shared folder or cloud repository] When you enable data encryption for a backup policy, Veeam Backup & Replication uses the specified password to encrypt backups of all Veeam Agent computers added to the backup policy. A Veeam Agent computer user can restore data from the backup of this computer without providing a password to decrypt backup. To restore data from a backup of another computer in this backup policy, a user must provide a password specified in the backup policy settings.

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

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

Notification Settings

You can specify 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.

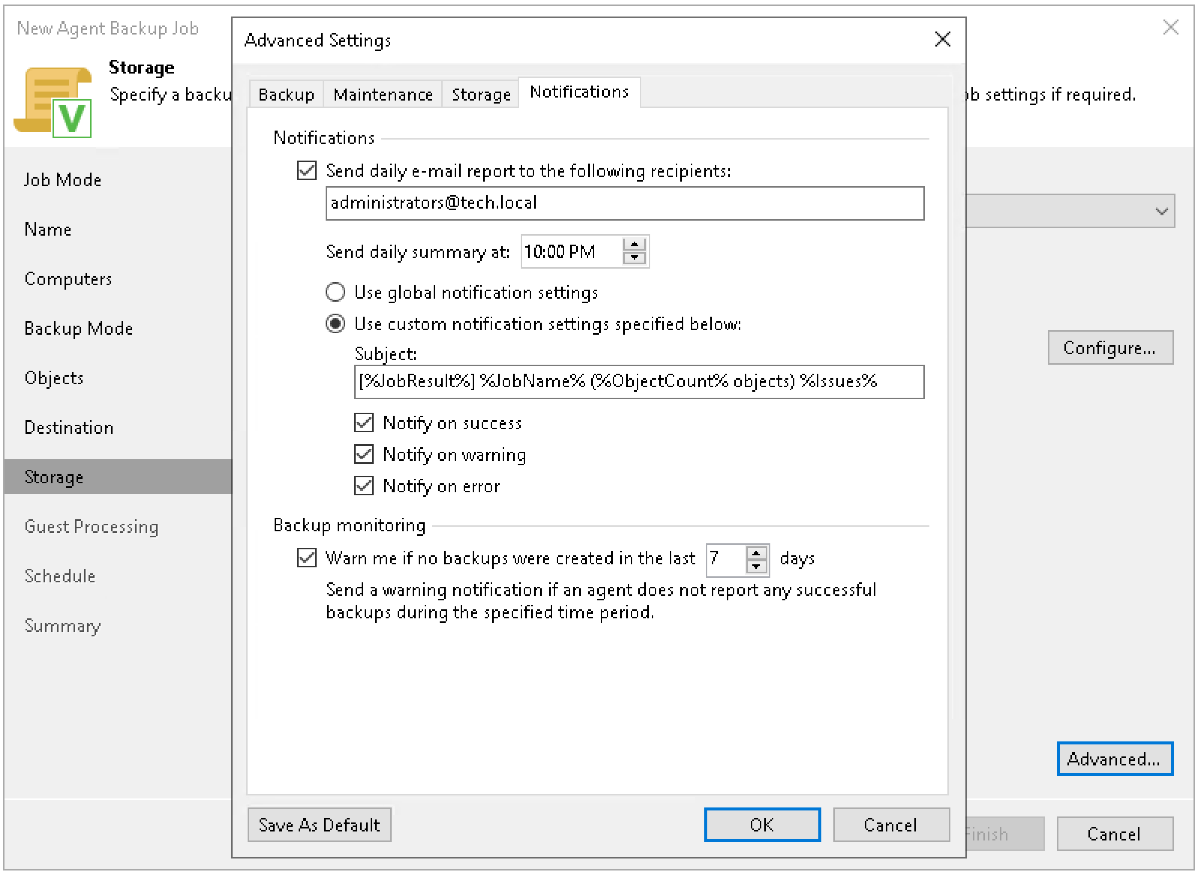
   ○ To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server.

   ○ 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 policy 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.



Notifications

☑ Send daily e-mail report to the following recipients:

administrators@tech.local

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

☑ Notify on error

Backup monitoring

☑ Warn me if no backups were created in the last 7 days

Send a warning notification if an agent does not report any successful backups during the specified time period.

Step 10. Specify Secondary Target

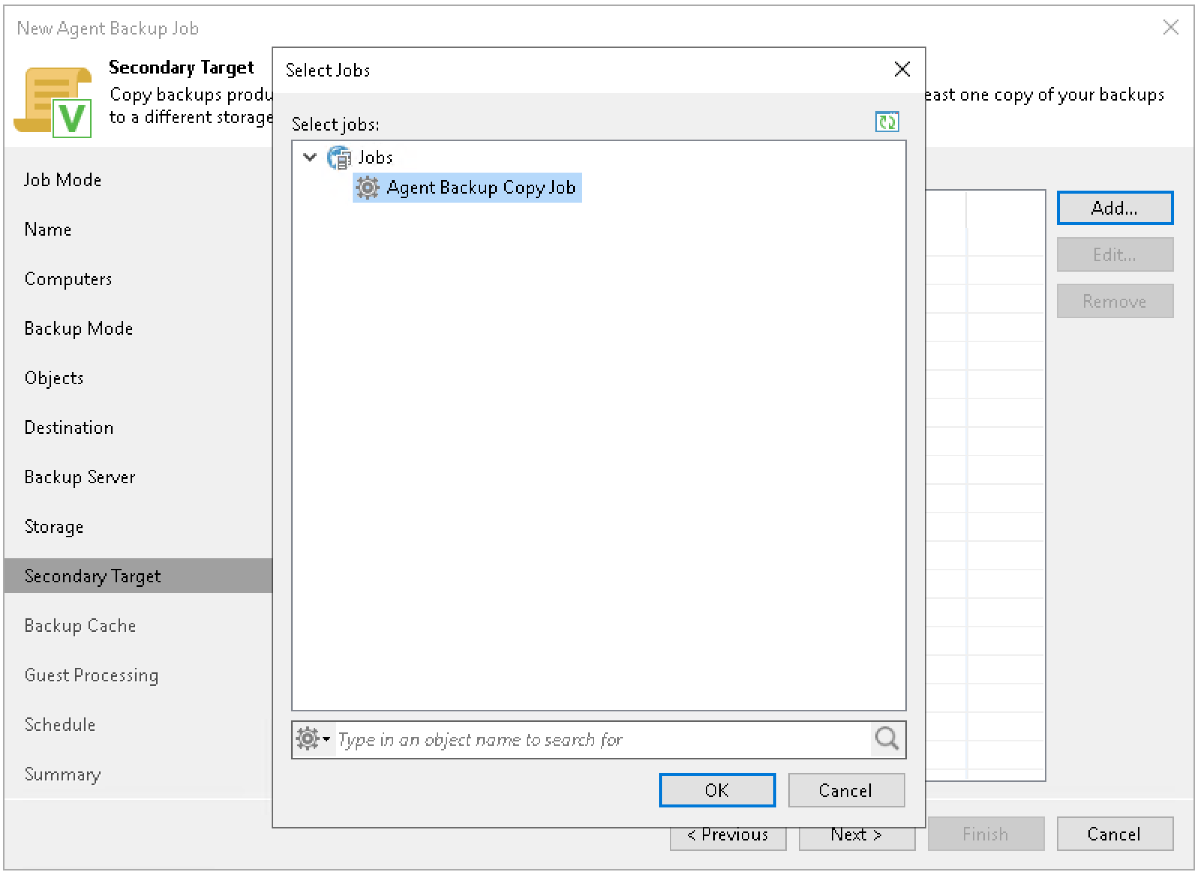
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent backup policy to a backup to tape or backup copy job. As a result, the backup policy will be added as a source to the backup to tape or backup copy job. Backup files created with the backup policy 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 policy to these jobs, Veeam Backup & Replication will automatically update the linked policies to define the Veeam Agent backup policy 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 policy. You can link several jobs to the backup policy — 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 **Veeam backup repository** or **Veeam Cloud Connect repository** option at the Destination step of the wizard.

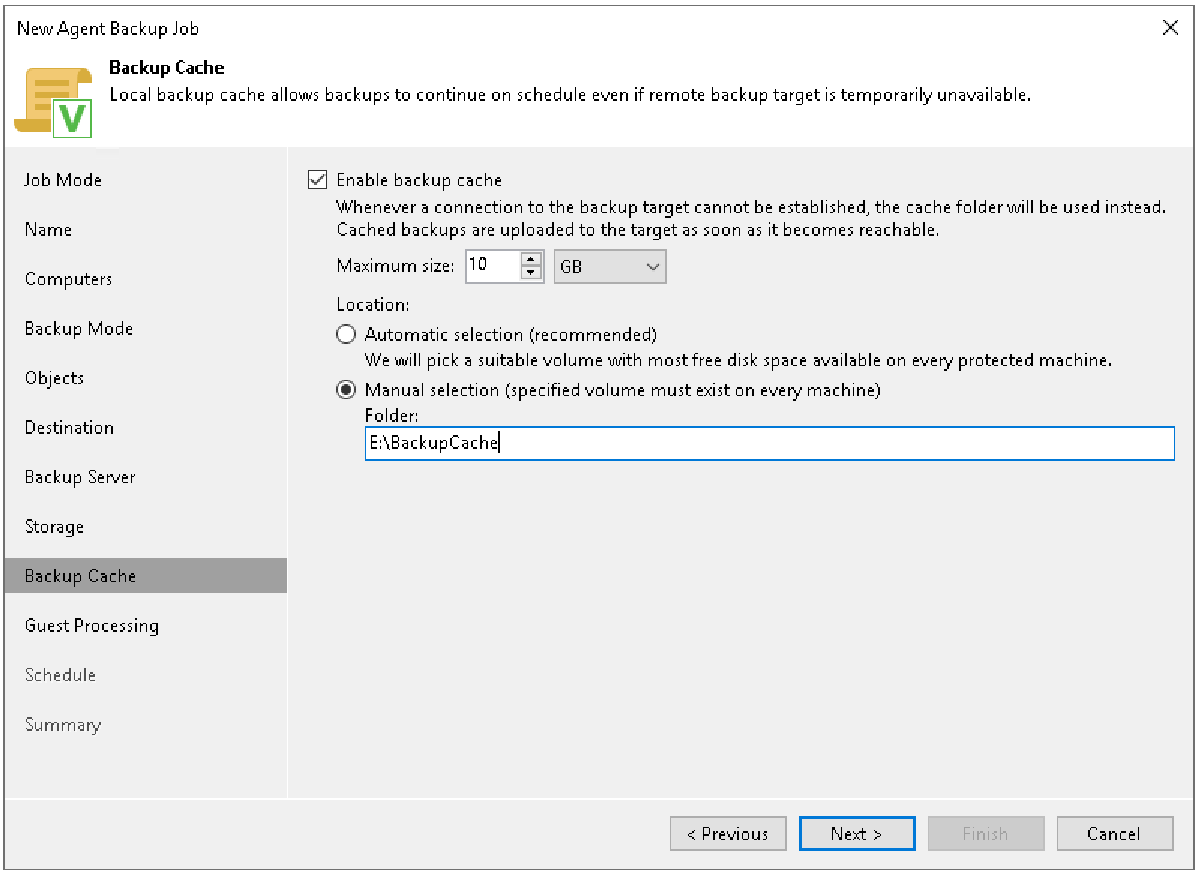
To specify backup cache settings:

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.



Backup Cache

Local backup cache allows backups to continue on schedule even if remote backup target is temporarily unavailable.

☑ Enable backup cache

Whenever a connection to the backup target cannot be established, the cache folder will be used instead. Cached backups are uploaded to the target as soon as it becomes reachable.

Maximum size: 10 GB

Location:

○ Automatic selection (recommended)

We will pick a suitable volume with most free disk space available on every protected machine.

● Manual selection (specified volume must exist on every machine)

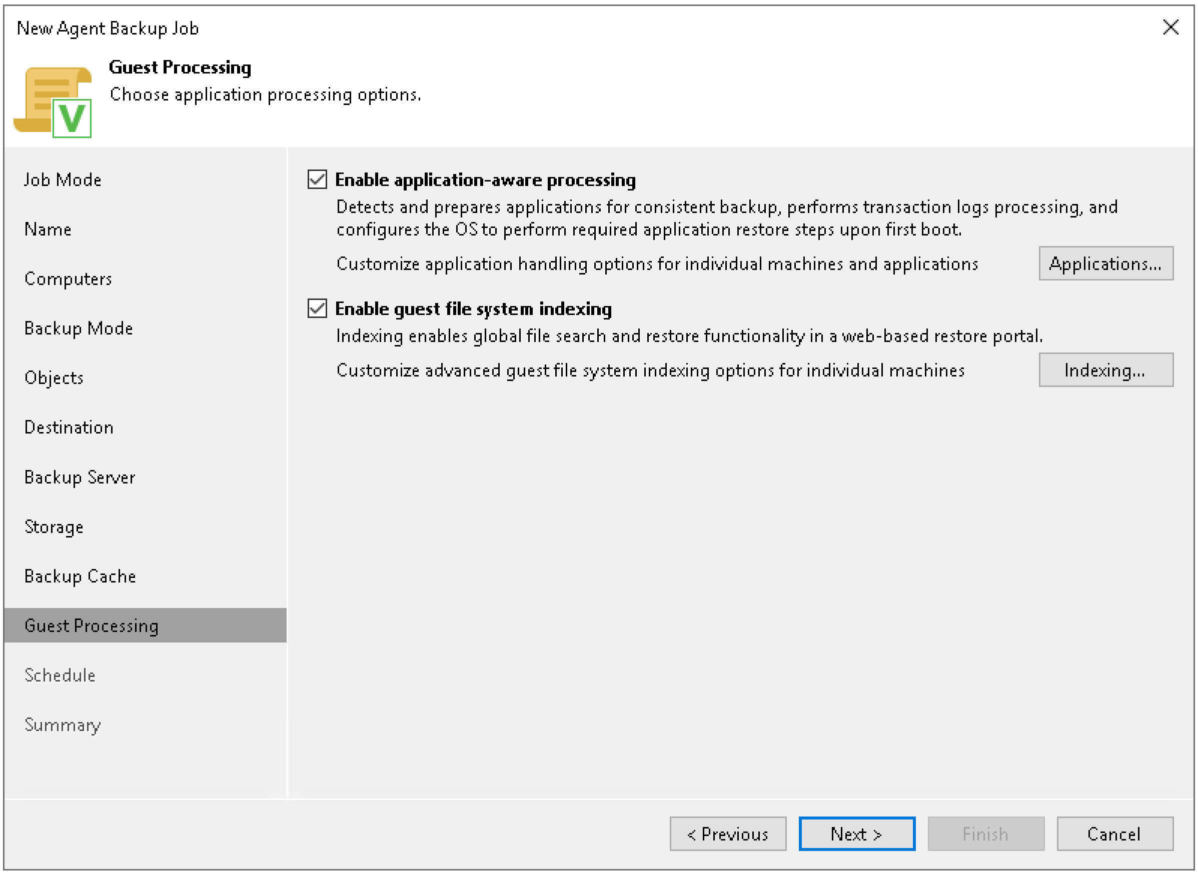
Folder: E:\BackupCache

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 policy that includes Windows-based computers, you can enable the following guest OS processing settings:

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



☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Indexing enables global file search and restore functionality in a web-based restore portal.

Customize advanced guest file system indexing options for individual machines

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 policy 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 policy fails, the logs will remain untouched until the next backup policy session.

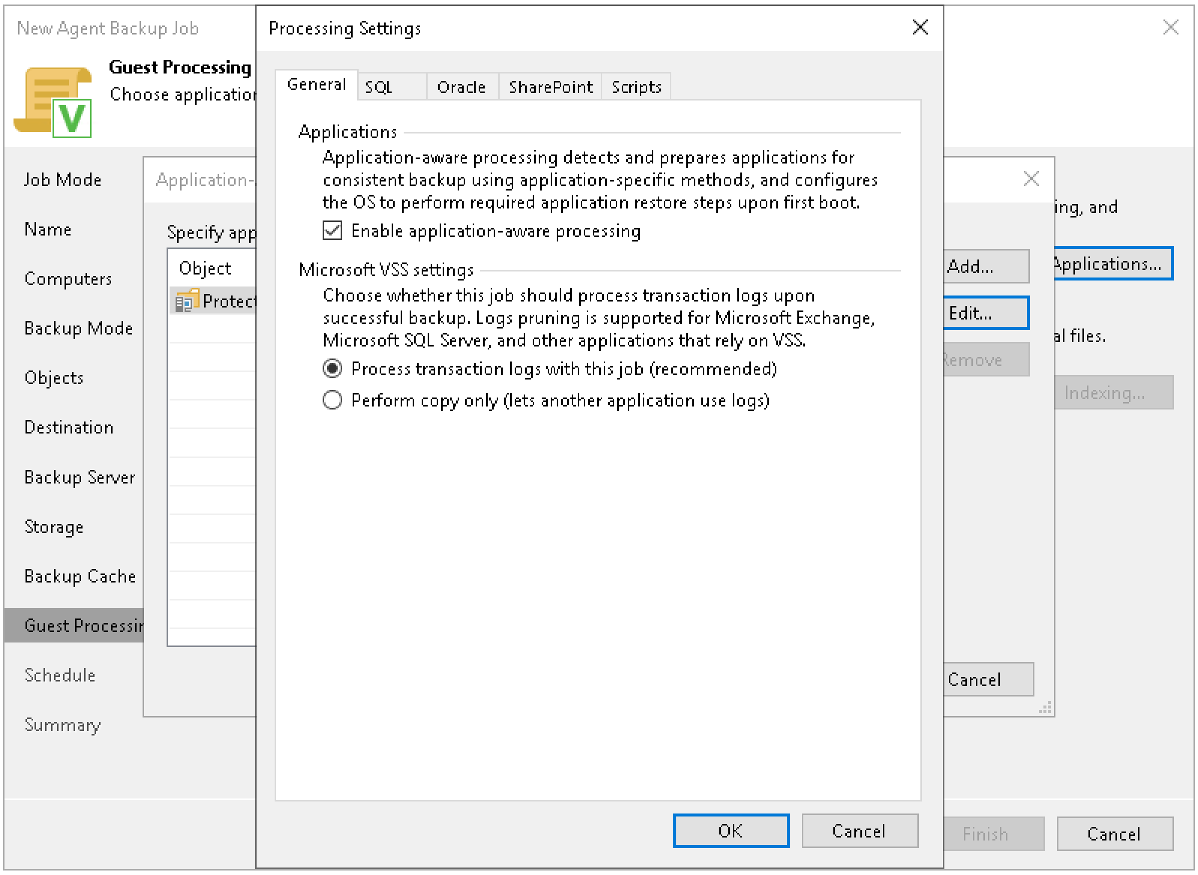
     [For Microsoft SQL Server and Oracle] You will have to specify settings for database log handling on the **SQL** and **Oracle** tabs of the **Processing Settings** window. For more information, see Microsoft SQL Server Transaction Log Settings and Oracle Archived Log Settings.

   - 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 policy.
- [For Microsoft SQL Server and Oracle] If both Microsoft SQL Server and Oracle Server are installed on one guest OS, you can enable log backup settings only for one of the installed applications: Microsoft SQL Server or Oracle Server.



Applications

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

☑ Enable application-aware processing

Microsoft VSS settings

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server, and other applications that rely on VSS.

● Process transaction logs with this job (recommended)

○ Perform copy only (lets another application use logs)

Microsoft SQL Server Transaction Log Settings

IMPORTANT

If the Microsoft OLE DB Driver 19 is installed on the SQL server host, consider the following:

- If the mandatory or strict encryption is enabled for the SQL server, you must additionally specify settings for connection to the SQL server using registry values. To learn more, contact Veeam Customer Support.
- If the SQL server instances have different encryption settings, Veeam Agent will back up only those whose settings match the settings specified in the registry values.
- If an earlier version of the Microsoft OLE DB Driver is also installed on the SQL server host, Veeam Agent will still use the Microsoft OLE DB Driver 19 to connect to the SQL server.

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 section Permissions for Guest Processing. 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 policy fails, the logs will remain untouched until the next backup policy session.
   - Select **Do not truncate logs** to preserve transaction logs. When the backup policy completes, Veeam Agent will not truncate transaction logs.

     We recommend that you enable this option only for databases with log truncation managed by a database administrator and 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.
   - 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 policy session, transaction logs will be truncated.

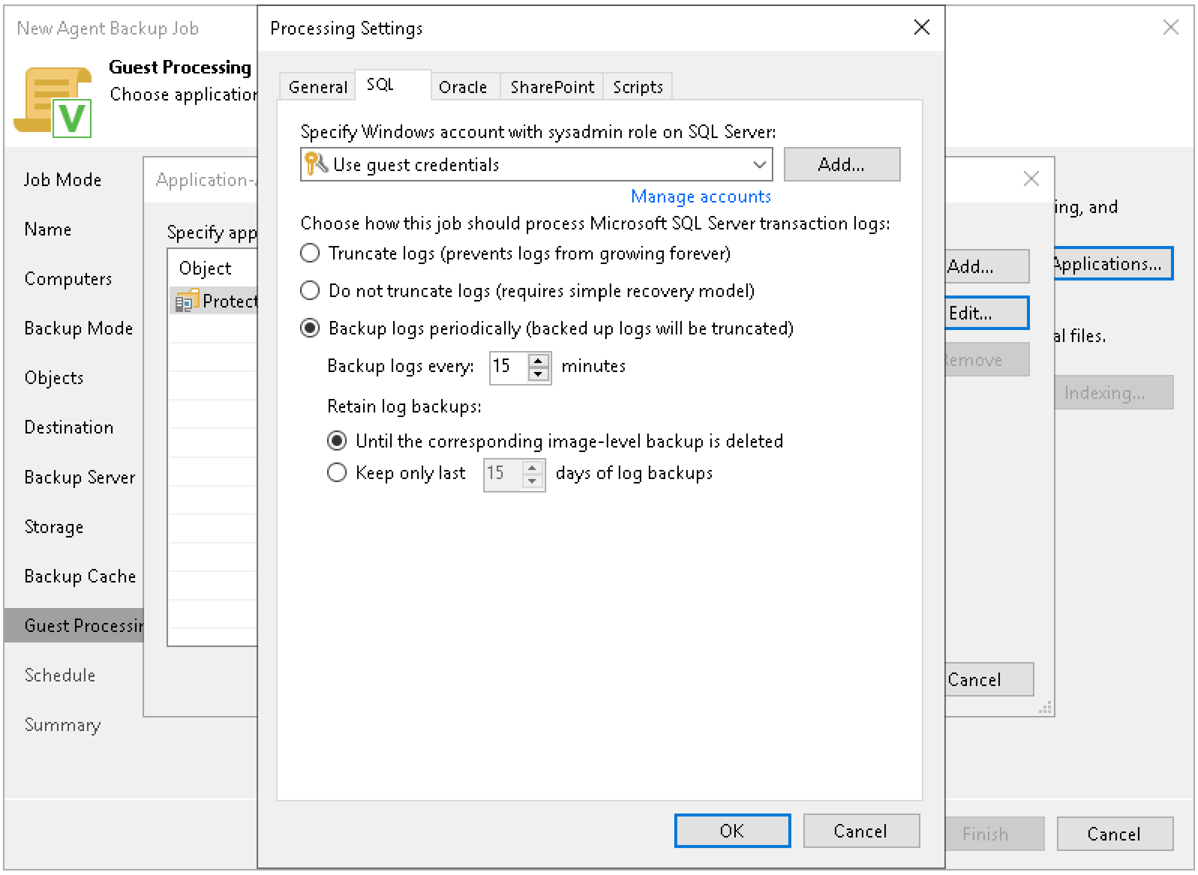
     > NOTE
     >
     > Backup of transaction logs to the cloud repository is not supported.

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

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

1. In the **Backup logs every <N> minutes** field, specify the frequency for transaction logs backup. By default, transaction logs are backed up every 15 minutes. The maximum log backup interval is 480 minutes.
2. In the **Retain log backups** section, specify retention policy for transaction logs stored in the backup location.
   - 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.



Processing Settings

General | SQL | Oracle | SharePoint | Scripts

Specify Windows account with sysadmin role on SQL Server:
Use guest credentials [Add...]
Manage accounts

Choose how this job should process Microsoft SQL Server transaction logs:
○ Truncate logs (prevents logs from growing forever)
○ Do not truncate logs (requires simple recovery model)
● Backup logs periodically (backed up logs will be truncated)

Backup logs every: 15 minutes

Retain log backups:
● Until the corresponding image-level backup is deleted
○ Keep only last 15 days of log backups

[OK] [Cancel]

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 redo 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 policy 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 policy to complete successfully and then trigger archived logs deletion from the Oracle Call Interface (OCI) according to the specified settings. If the backup policy fails, the logs will remain untouched until the next successful backup policy session.

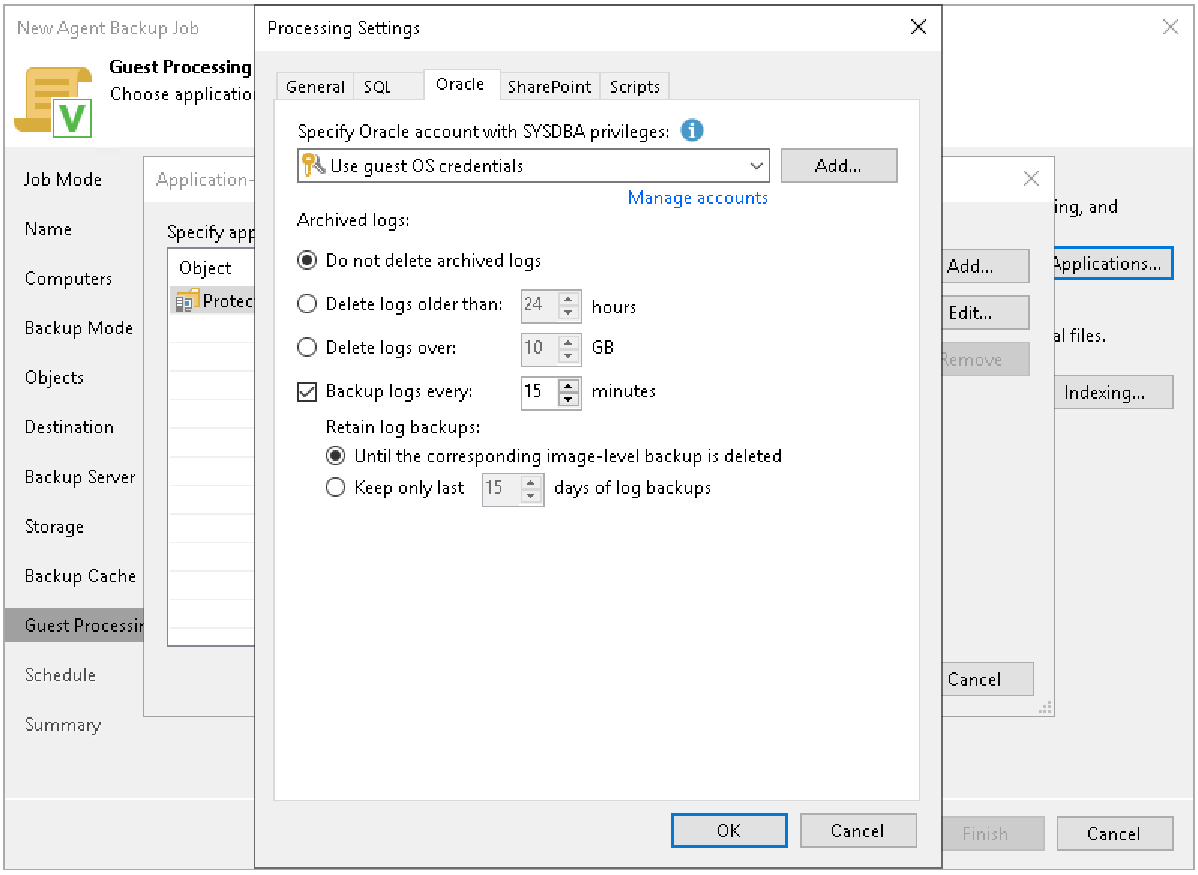
     > TIP
     >
     > If you configure backup policy to back up archived logs, Veeam Agent for Microsoft Windows also triggers archived logs deletion after each log backup job session.

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.



Processing Settings

General | SQL | Oracle | SharePoint | Scripts

Specify Oracle account with SYSDBA privileges: Use guest OS credentials [Add...]

Manage accounts

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

☑ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

[OK] [Cancel]

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.

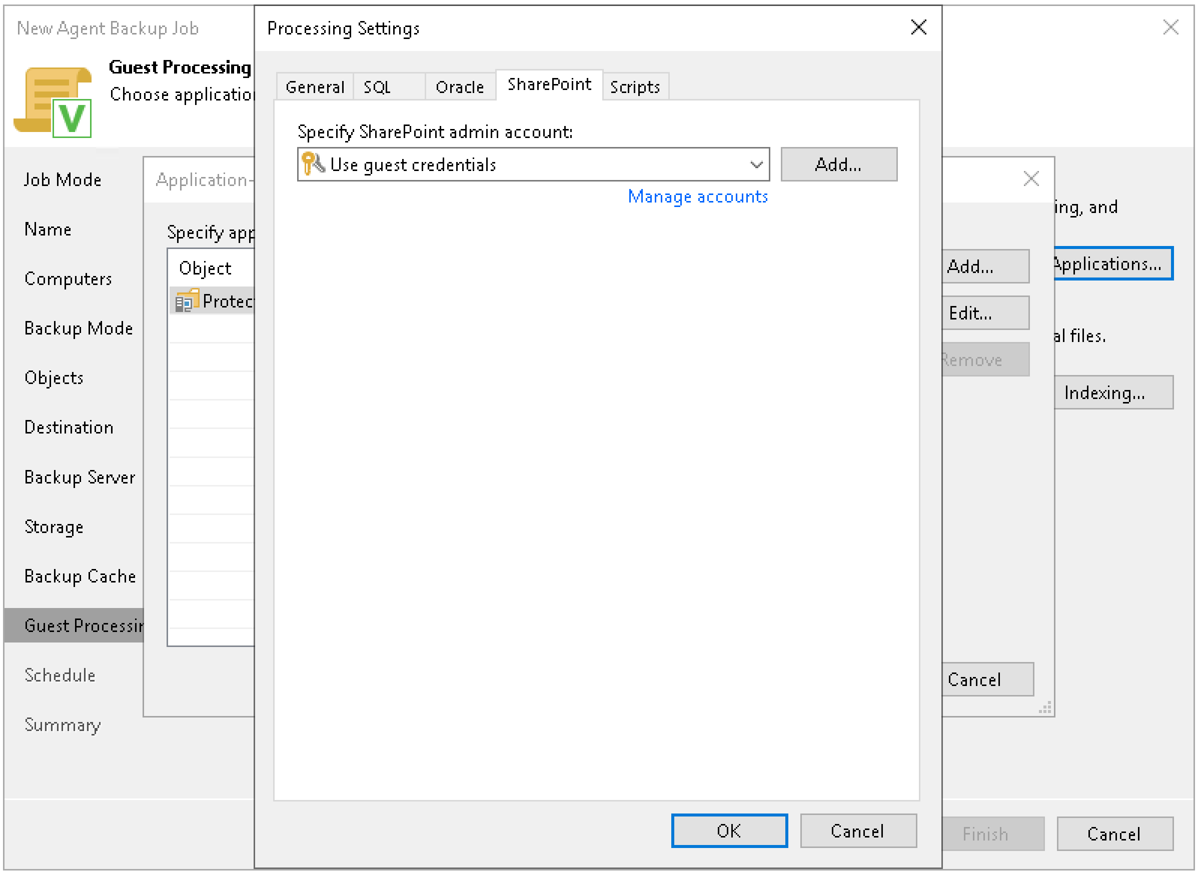
2. Click **Applications**.

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 requests the creation of 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 policy:

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:

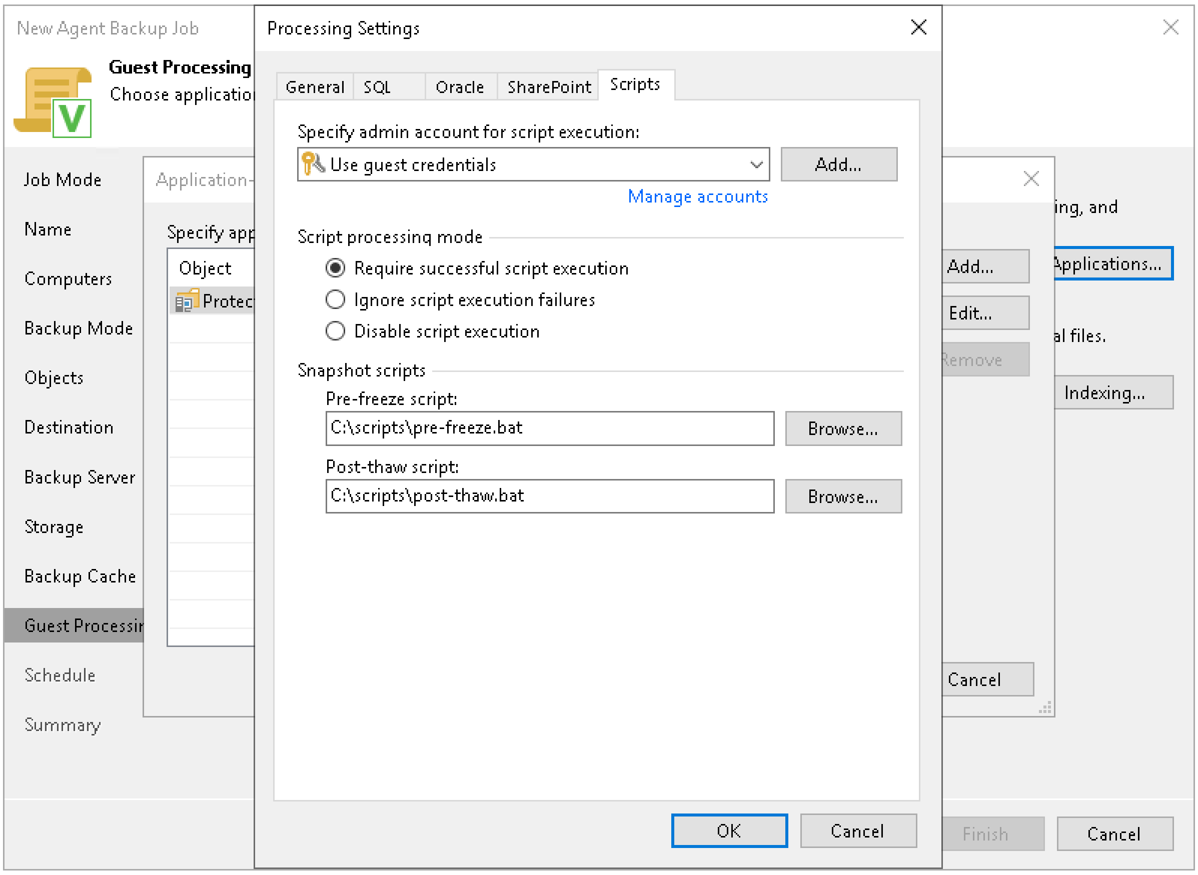
   - Select **Require successful script execution** if you want Veeam Agent for Microsoft Windows to stop the backup process if the script fails.
   - Select **Ignore script execution failures** if you want to continue the backup process even if script errors occur.
   - Select **Disable script execution** 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 policy session, Veeam Backup & Replication will upload the scripts to Veeam Agent computers added to the policy 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.



Processing Settings

Specify admin account for script execution: Use guest credentials

Script processing mode

● Require successful script execution
○ Ignore script execution failures
○ Disable script execution

Snapshot scripts

Pre-freeze script: C:\scripts\pre-freeze.bat

Post-thaw script: C:\scripts\post-thaw.bat

File Indexing

You can instruct the backup policy 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.

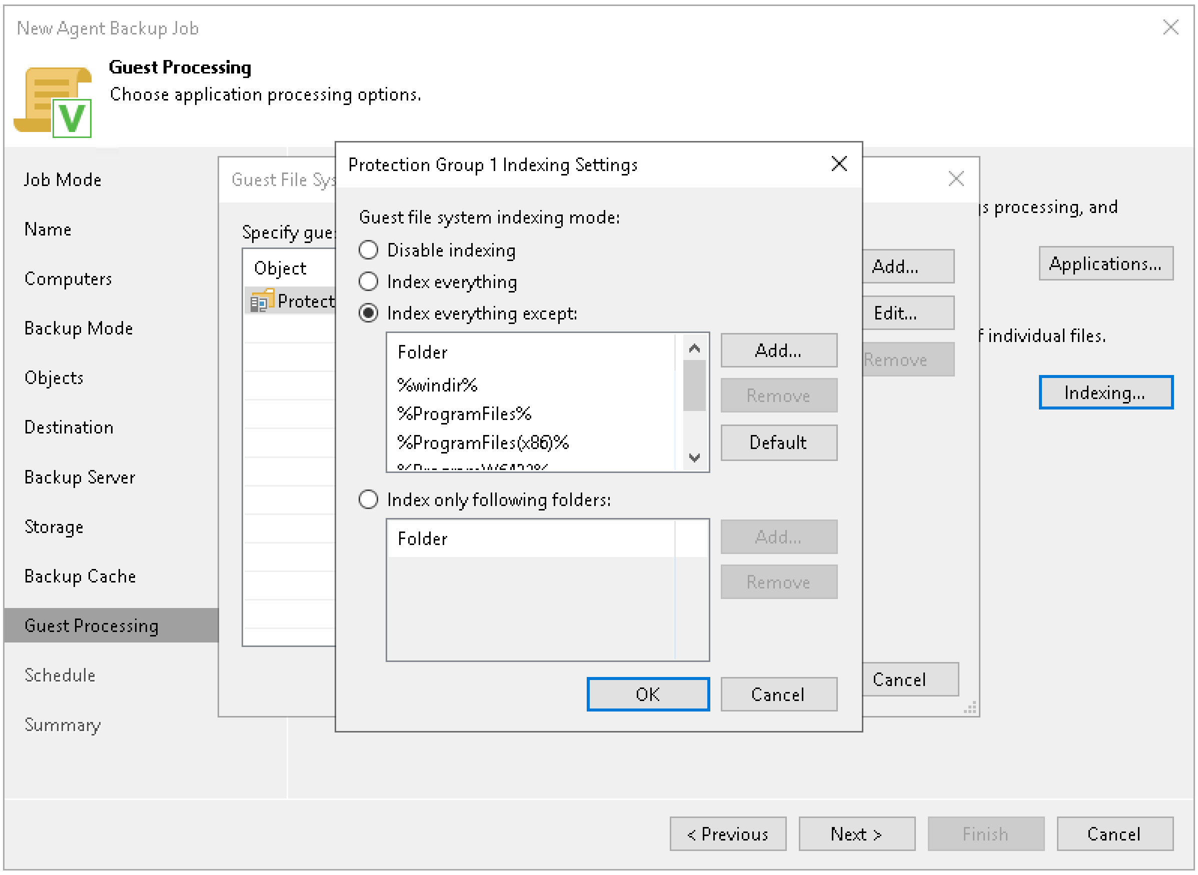
> NOTE
>
> File system indexing is optional. If you do not enable this option in the backup policy settings, you will still be able to perform 1-click restore from the backup created with such backup policy. For more information, see the Preparing for File Browsing and Restore section in the Veeam Backup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



New Agent Backup Job

Guest Processing

Choose application processing options.

Protection Group 1 Indexing Settings

Guest file system indexing mode:

○ Disable indexing

○ Index everything

● Index everything except:

Folder
%windir%
%ProgramFiles%
%ProgramFiles(x86)%

○ Index only following folders:

Folder

Step 13. Specify Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup. At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup. Backup policy scheduling options differ depending on the computer type that you have selected at the Job Mode step of the wizard:

- Scheduling Settings for Workstations
- Scheduling Settings for Servers

> NOTE
>
> 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 policy schedule:

1. Select the **Daily at** check box and use the fields on the right to specify time and days when the backup policy must start:
    - *Everyday* — select this option to start the policy at specific time daily.
    - *On week-days* — select this option to start the policy at specific time on week-days.
    - *On these days* — select this option to start the policy at specific time on selected days.

   You can leave the **Daily at** check box unchecked to configure the backup policy without daily schedule. In this case, you will be able to use the backup policy 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 policy 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 policy must start.
    - *Backup once powered on* — select this option if you want Veeam Agent for Microsoft Windows to start the scheduled backup policy 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 policy 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 policy 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 policy 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 policy launch:

   - Select the **Lock** check box if you want to start the backup policy when the user locks the Veeam Agent computer.

   - Select the **Log off** check box if you want to start the backup policy 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 policy 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 policy 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 policies triggered by the *When backup target is connected* event. In case of backup policies 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 policy completes successfully.

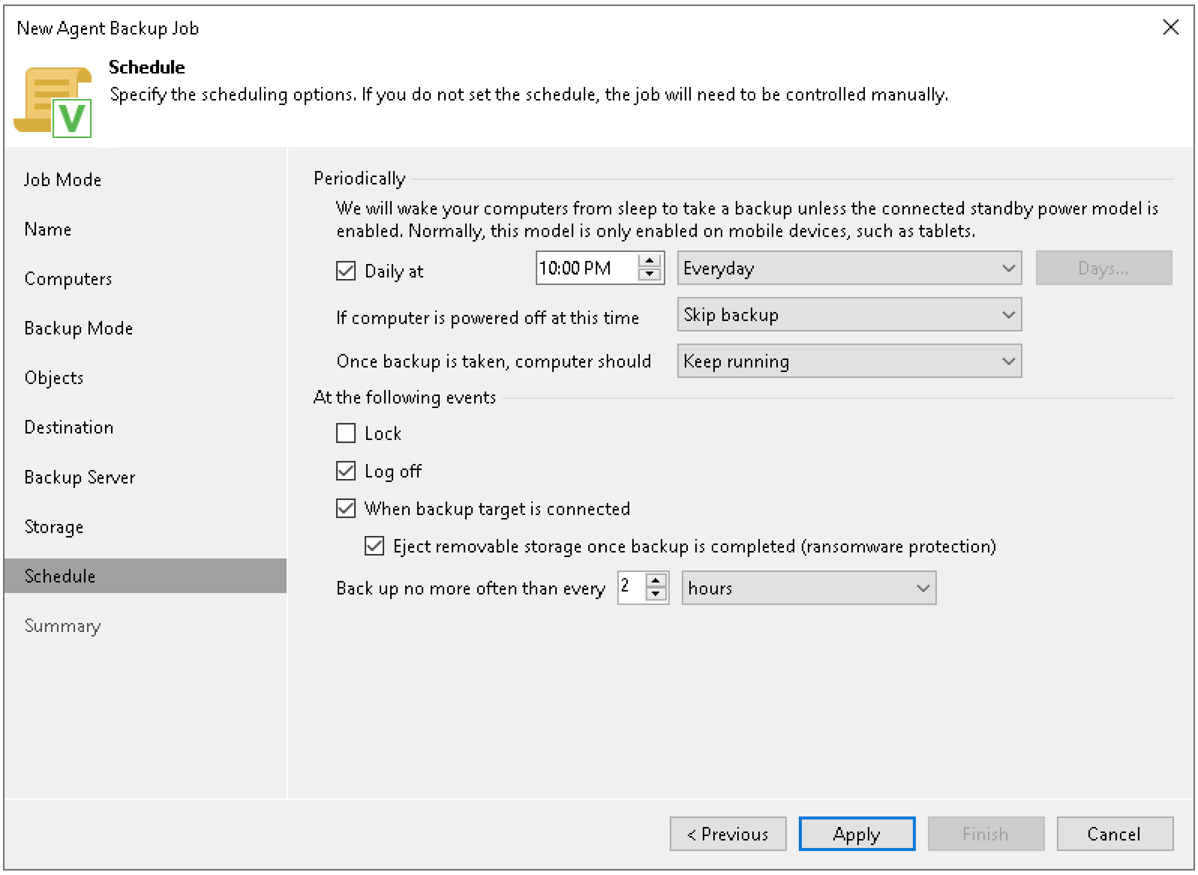
     > IMPORTANT
     >
     > The *Eject removable storage once backup is completed* option does not guarantee a bulletproof protection against ransomware. To ensure your backups are safe, keep the OS up to date and regularly scan your backup repository for virus threats using modern antivirus software.

   - Use the **Back up no more often than every <N> <time units>** field to restrict the frequency of backup policy sessions. Specify a minutely, hourly or daily interval between the backup policy sessions.

     The *Back up no more often than every <N> <time units>* option is applied only to policy 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**.



New Agent Backup Job

Schedule

Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Periodically

We will wake your computers from sleep to take a backup unless the connected standby power model is enabled. Normally, this model is only enabled on mobile devices, such as tablets.

☑ Daily at 10:00 PM Everyday Days...

If computer is powered off at this time: Skip backup

Once backup is taken, computer should: Keep running

At the following events

☐ Lock

☑ Log off

☑ When backup target is connected

☑ Eject removable storage once backup is completed (ransomware protection)

Back up no more often than every 2 hours

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 policy schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup policy manually to create backup.
2. Define scheduling settings for the policy:
   - To run the policy 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 policy 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 policy 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 policy. In the **Start time within an hour** field, specify the exact time when the policy must start.

     A repeatedly run policy is started by the following rules:

        - The defined interval always starts at 12:00 AM. For example, if you configure to run a policy with a 4-hour interval, the policy 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 policy, after the denied interval is over, the policy will start immediately and then run by the defined schedule.

      For example, you have configured a policy 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 policy will first run at 9:00 AM, when the denied period is over. After that, the policy will run at 10:00 AM, 12:00 PM, 2:00 PM and 4:00 PM.

    - To run the policy continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup policy session will start as soon as the previous backup policy session finishes.

3. In the **Automatic retry** section, define whether Veeam Agent for Microsoft Windows must attempt to run the backup policy again if the policy fails for some reason. Enter the number of attempts to run the policy and define time intervals between them. If you select continuous backup, Veeam Backup & Replication or Veeam Agent for Microsoft Windows retries the policy for the defined number of times without any time intervals between the policy runs.

   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.

   > NOTE
   >
   > The automatic retry does not start if you run the backup policy manually. In this case, you can manually retry the backup policy. To learn more, see Retrying Veeam Agent Backup Job.

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

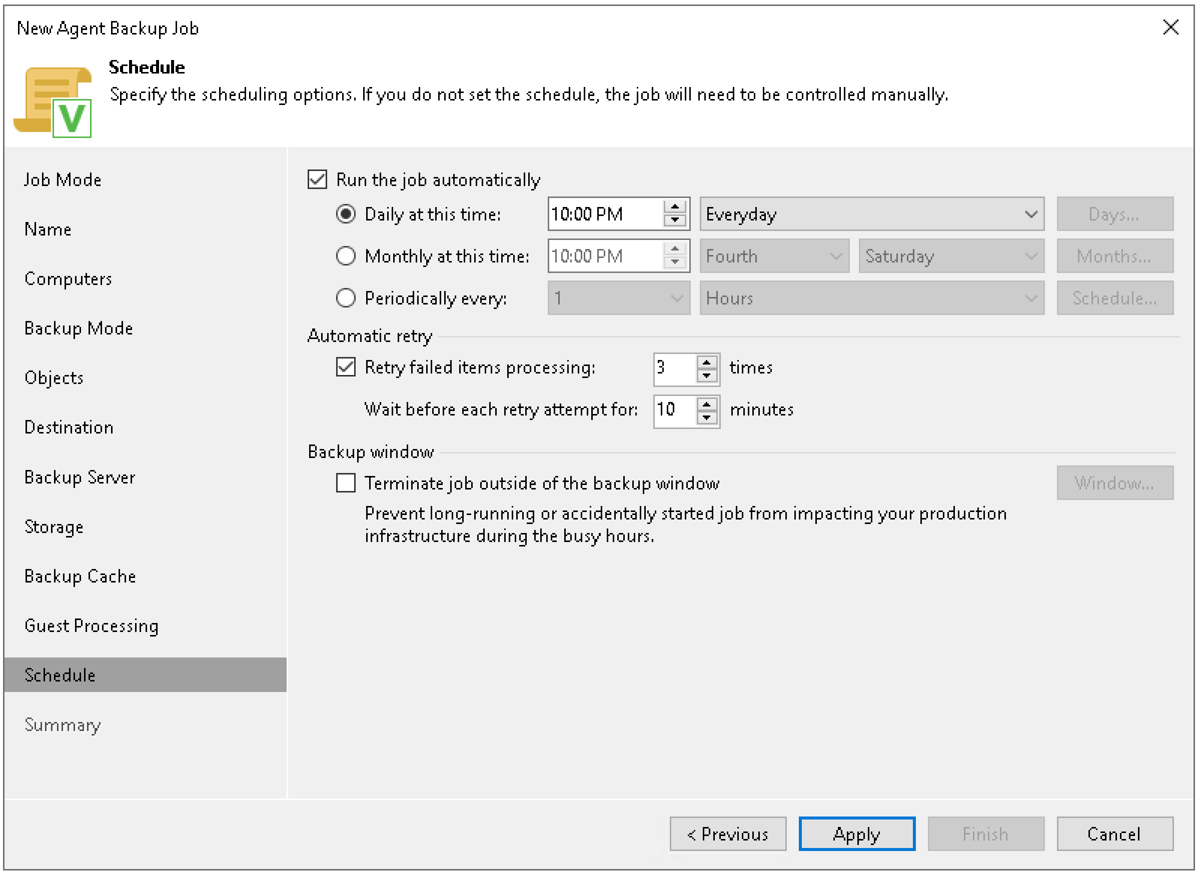
   a. Select the **Terminate job if it exceeds allowed backup window** check box and click **Window**.

   b. In the **Time Periods** window, define the allowed hours and prohibited hours for backup.

      If the policy 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

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.



New Agent Backup Job

Schedule

Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday [Days...]

○ Monthly at this time: 10:00 PM Fourth Saturday [Months...]

○ Periodically every: 1 Hours [Schedule...]

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

Backup window

□ Terminate job outside of the backup window [Window...]

Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.

Step 14. Review Backup Job Settings

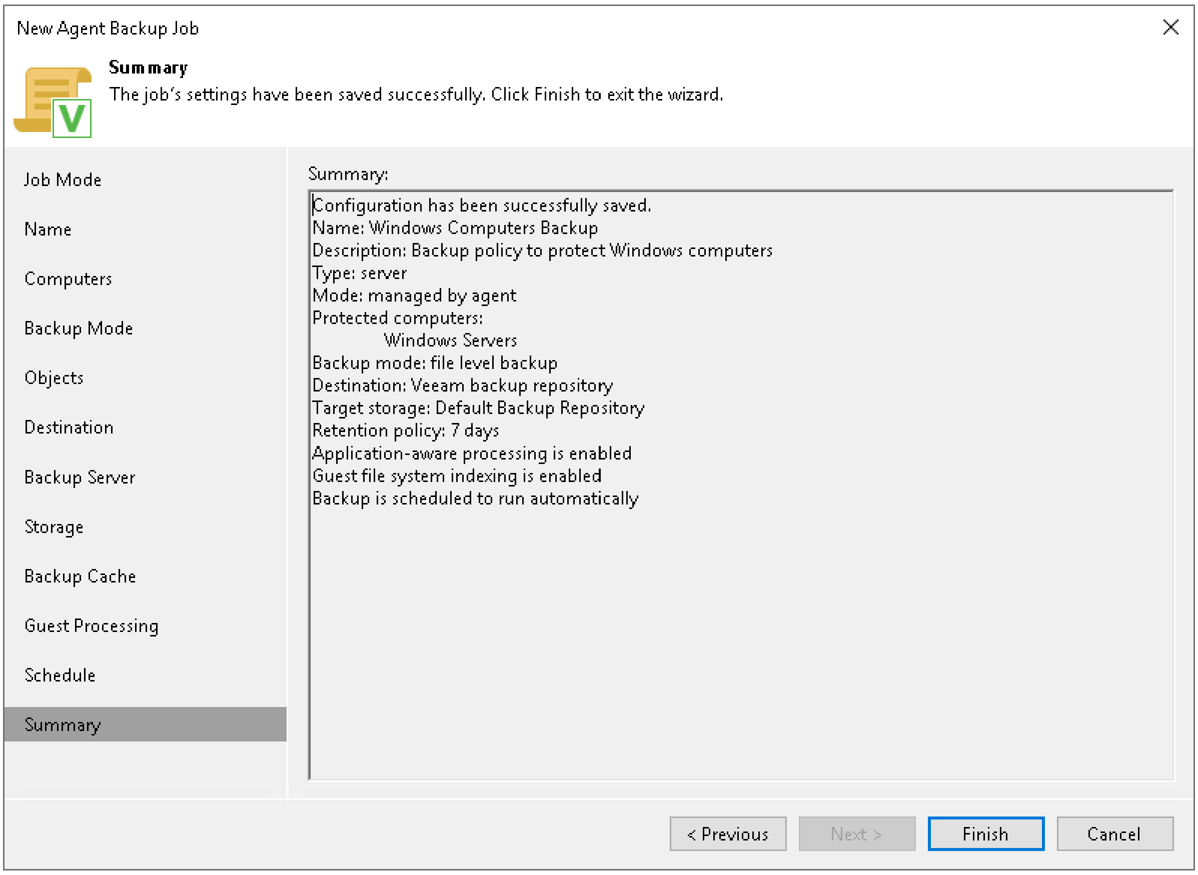
At the **Summary** step of the wizard, complete the backup policy configuration process.

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

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

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 Configuration.



```
Configuration has been successfully saved.
Name: Windows Computers Backup
Description: Backup policy to protect Windows computers
Type: server
Mode: managed by agent
Protected computers:
            Windows Servers
Backup mode: file level backup
Destination: Veeam backup repository
Target storage: Default Backup Repository
Retention policy: 7 days
Application-aware processing is enabled
Guest file system indexing is enabled
Backup is scheduled to run automatically
```

Creating Policy for Linux Computers

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

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 workstations that you plan to add to the backup policy. To learn more, see Licensing Requirements.
- 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.
- [For backup policies 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:

- If you want to perform a volume-level restore of a computer using Veeam Agent, the BIOS boot partition of this computer must be associated with a block device. Otherwise, Veeam Agent supports only file-level restore from the backup of the computer.
- You cannot map a Veeam Agent backup policy to a Veeam Agent backup chain created by another type of a Veeam Agent backup job. After you change the mode of a Veeam Agent computer, Veeam Backup & Replication starts a new backup chain in a target location specified in the backup policy settings.
- 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 policy targeted at the cloud repository.
- Veeam Agent does not support backup of bind mount points. In the scope of the backup policy, you must specify the path to the original mount point instead.
- If you plan to create a Veeam Agent backup policy for computers with nosnap Veeam Agent installed, consider the limitations and system requirements listed in section System Requirements for Linux Computers (nosnap Veeam Agent).
- You cannot add a Veeam Agent computer protected by a backup job managed by the backup server to a Veeam Agent backup policy. To add such a computer to a Veeam Agent backup policy, first remove the computer from the backup job managed by the backup server.

Step 1. Launch New Agent Backup Job Wizard

You can create a Veeam Agent backup policy for protected computers that run a Linux 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 and 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** > **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 Policy

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** > **Linux** > **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** > **Linux** > **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 individual computers to the policy later on, when you pass through the wizard steps.

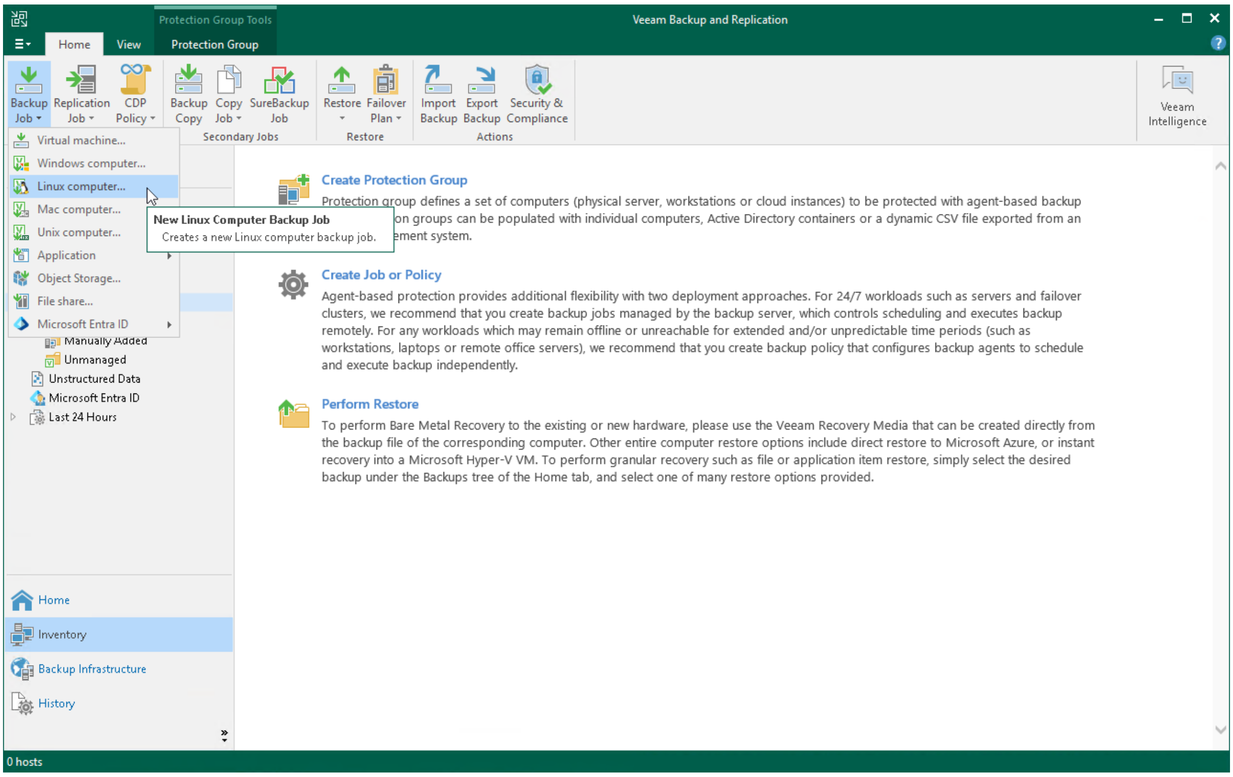
Adding Computers to New Backup Policy

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 protection groups to the policy later on, when you pass through the wizard steps.

> **TIP**
>
> Consider the following:
>
> - You can press and hold the [Ctrl] key 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.



New Linux Computer Backup Job
Creates a new Linux computer backup job.

Create Protection Group

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

Create Job or Policy

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

Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

Step 2. Select Job Mode

At the **Job Mode** step of the wizard, specify protection settings for the Veeam Agent backup policy:

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 on servers, select the job mode.

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 policy. You can select one of the following computer types:

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

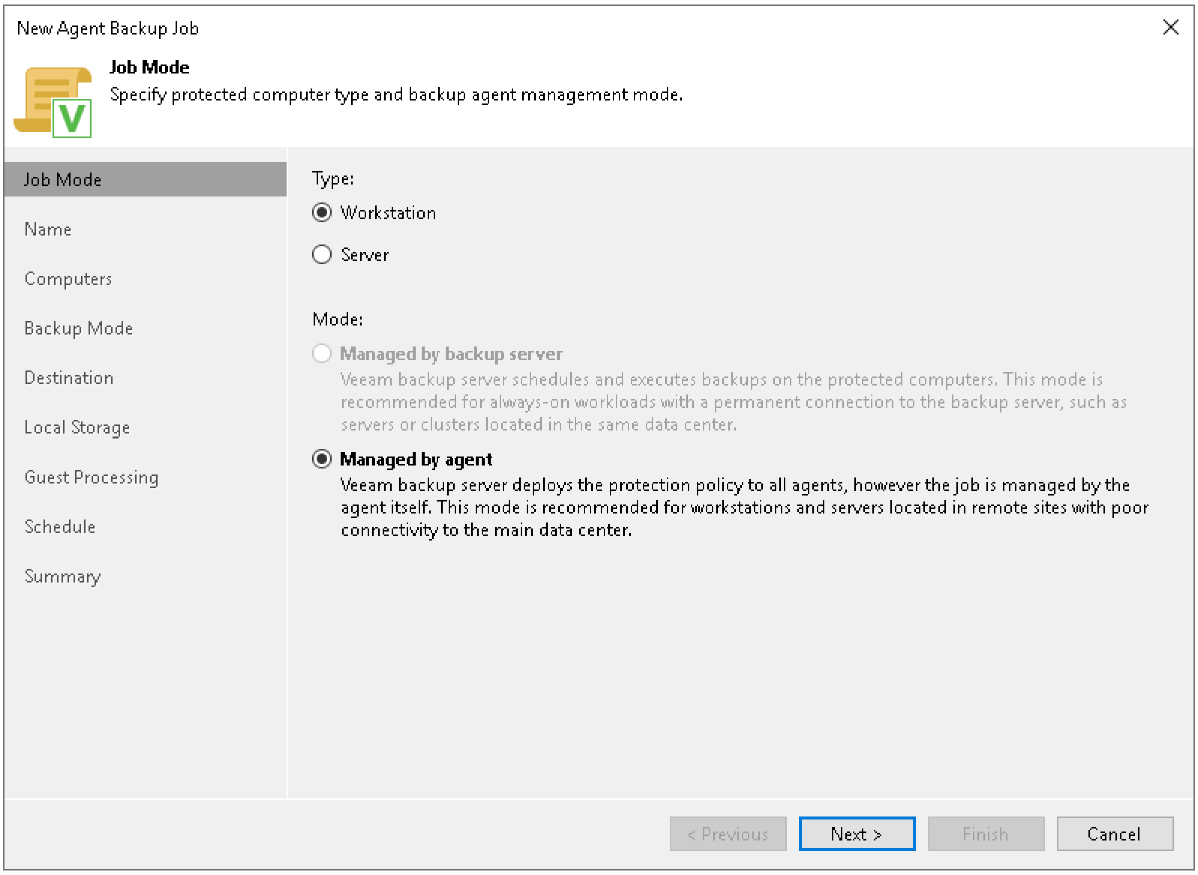
  For backup policies that process servers, Veeam Backup & Replication offers settings similar to the job settings available in Veeam Agent for Linux operating in the Server mode. To learn more, see the Veeam Agent for Linux User Guide.

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

Selecting Job Mode

If you selected the **Workstation** computer type in the **Type** field, you do not need to select the job mode in the **Mode** field, the **Managed by agent** job mode will be selected automatically.

If you selected the **Server** option in the Type field, in the **Mode** field, select the **Managed by agent** job mode to create a Veeam Agent backup policy. If you select the **Managed by backup server** job mode, you will create a Veeam Agent backup job managed by the backup server.



Job Mode

Specify protected computer type and backup agent management mode.

Type:

● Workstation

○ Server

Mode:

○ **Managed by backup server**

Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

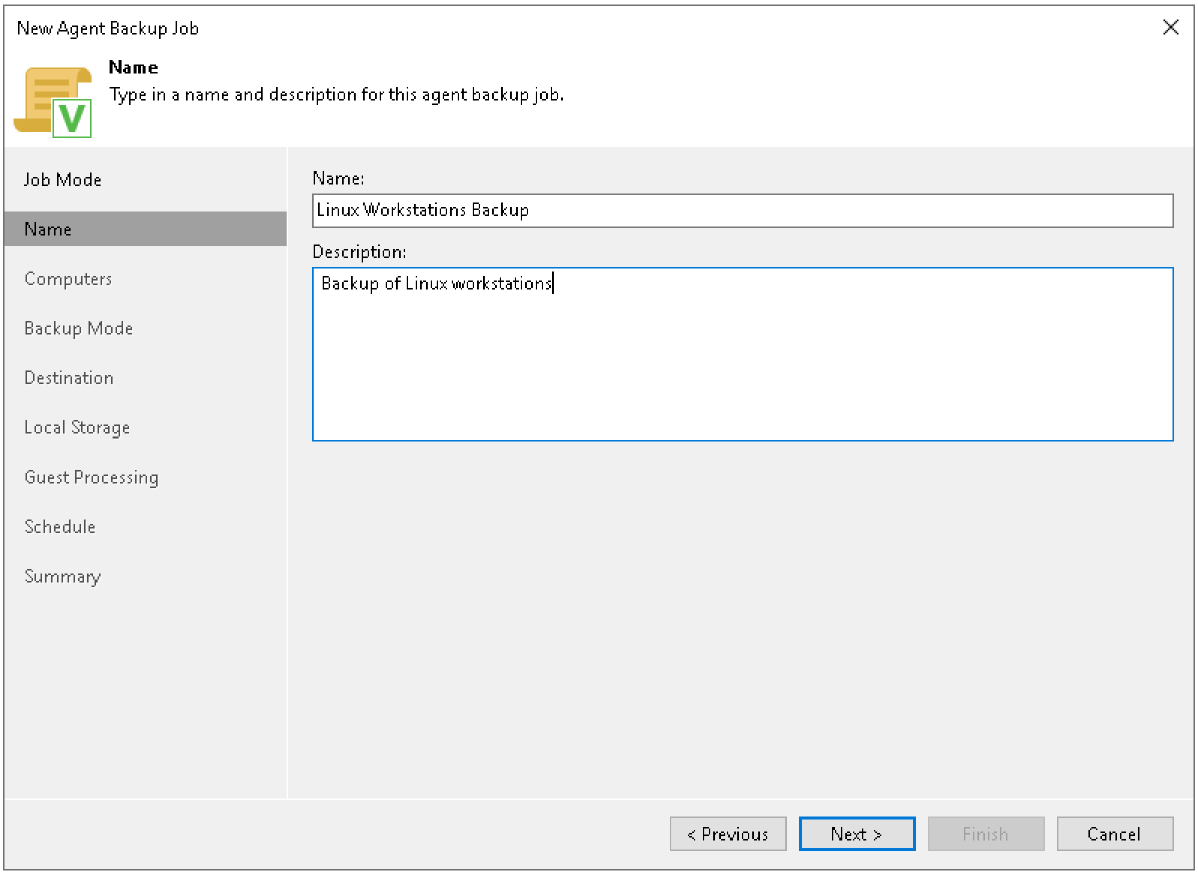
● **Managed by agent**

Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

Step 3. Specify Job 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.



Name: Linux Workstations Backup

Description: Backup of Linux workstations

Step 4. Select Computers to Back Up

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

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

Policies 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 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** > **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 policy. You can remove some computers from the policy or add new computers to the policy, if necessary.

Adding Protection Groups and Computers from Inventory

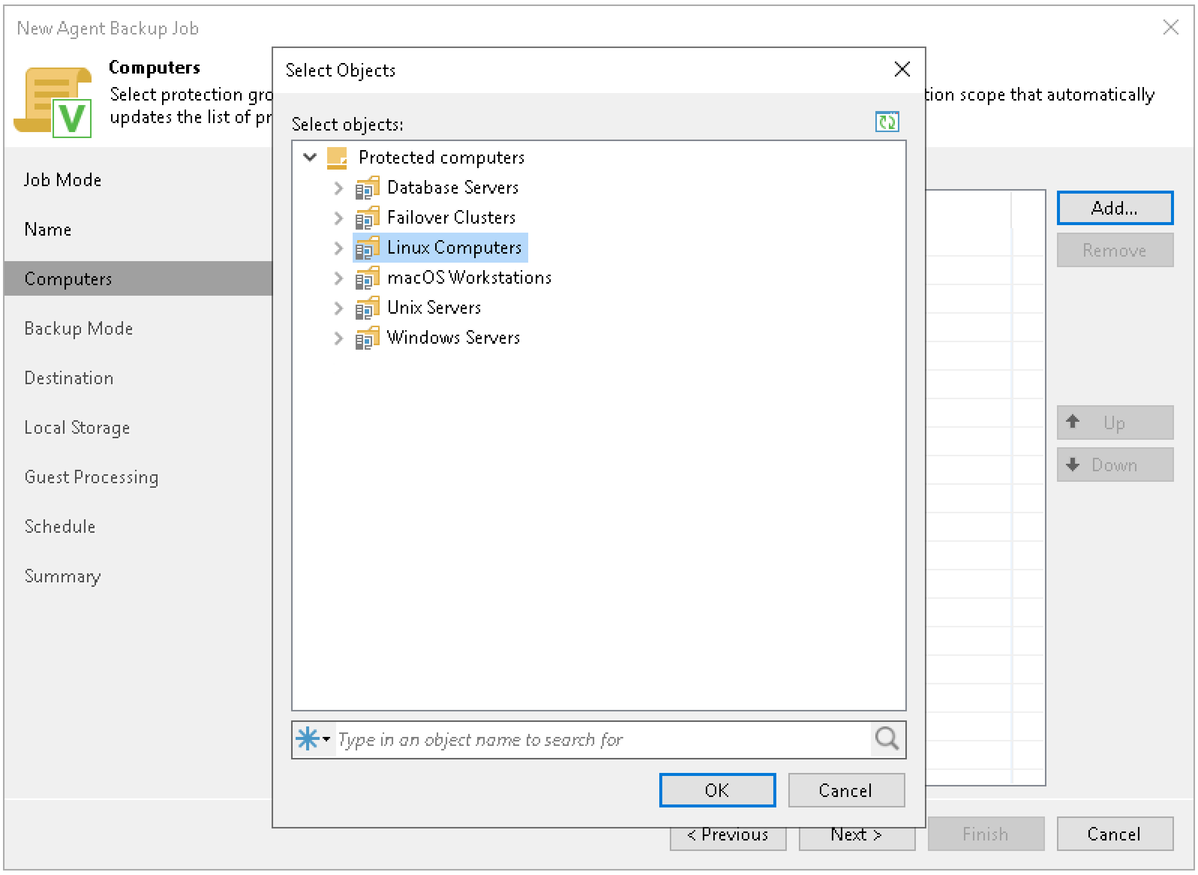
To add protection groups and individual computers to the Veeam Agent backup policy, do the following:

1. Click **Add** > **Protection group**.
2. In the **Select Objects** window, select one or more protection groups and computers in the list and click **OK**. You can press and hold the [Ctrl] or [Shift] key 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 policy new computers that do not exist in the inventory, do the following:

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 policy.
3. Select a method to connect to the computer:

   - **Connect using admin credentials.** In this case, 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.

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

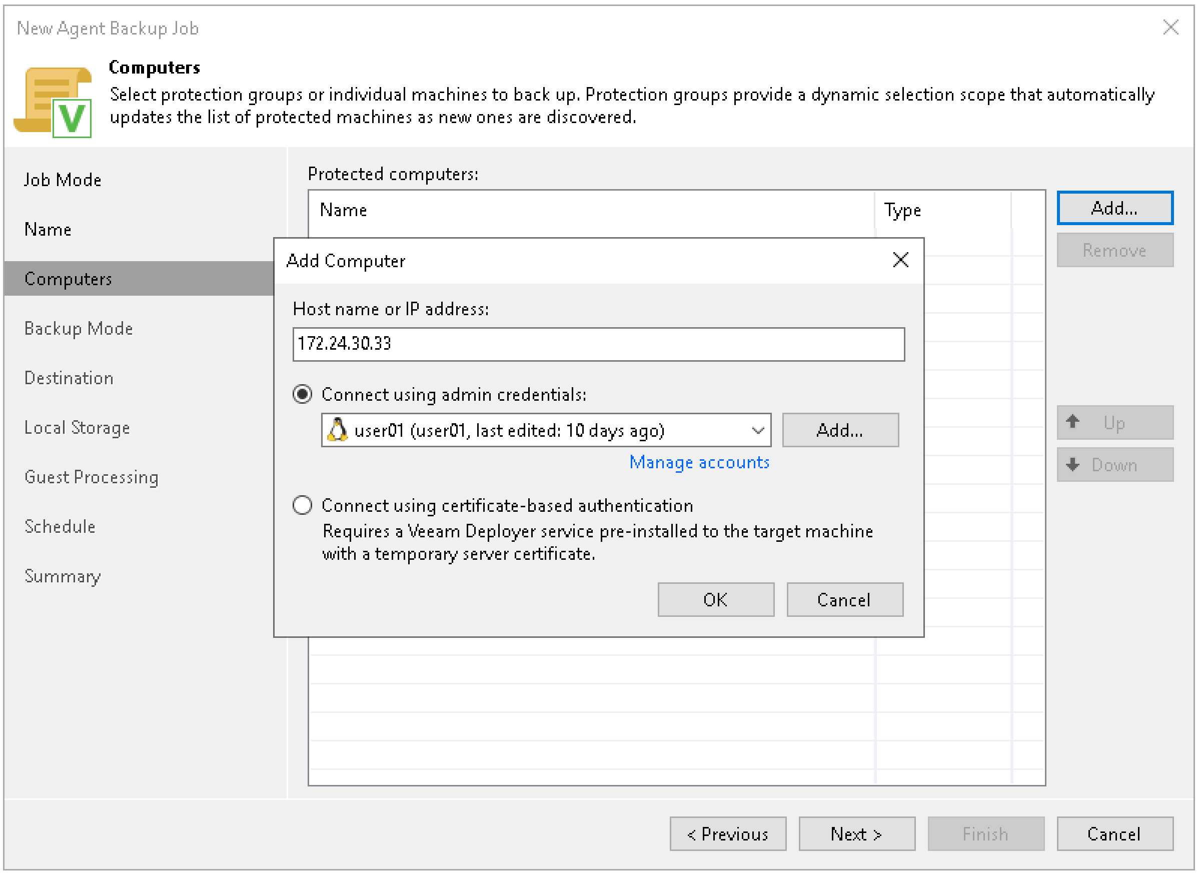
     - **Stored** credentials. Select stored credentials if you want Veeam Backup & Replication to use the specified user name and password for each connection to Veeam Agent.

  - **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.

- Select this option, if you chose to pre-install Veeam Deployer Service on the Linux computer that you want to add to the backup policy. In this case, Veeam Backup & Replication will communicate with the Linux computer using a certificate. To learn more, see Deploying Veeam Agent for Linux Using Pre-Installed Veeam Deployer Service


New Agent Backup Job
Computers
Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.
Job Mode
Name
Computers
Backup Mode
Destination
Local Storage
Guest Processing
Schedule
Summary
Protected computers:
Name
Type
Add...
Remove
Up
Down
Add Computer
Host name or IP address:
172.24.30.33
● Connect using admin credentials:
user01 (user01, last edited: 10 days ago)
Add...
Manage accounts
○ Connect using certificate-based authentication
Requires a Veeam Deployer service pre-installed to the target machine with a temporary server certificate.
OK
Cancel
< Previous
Next >
Finish
Cancel

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 the Destination step of the wizard.

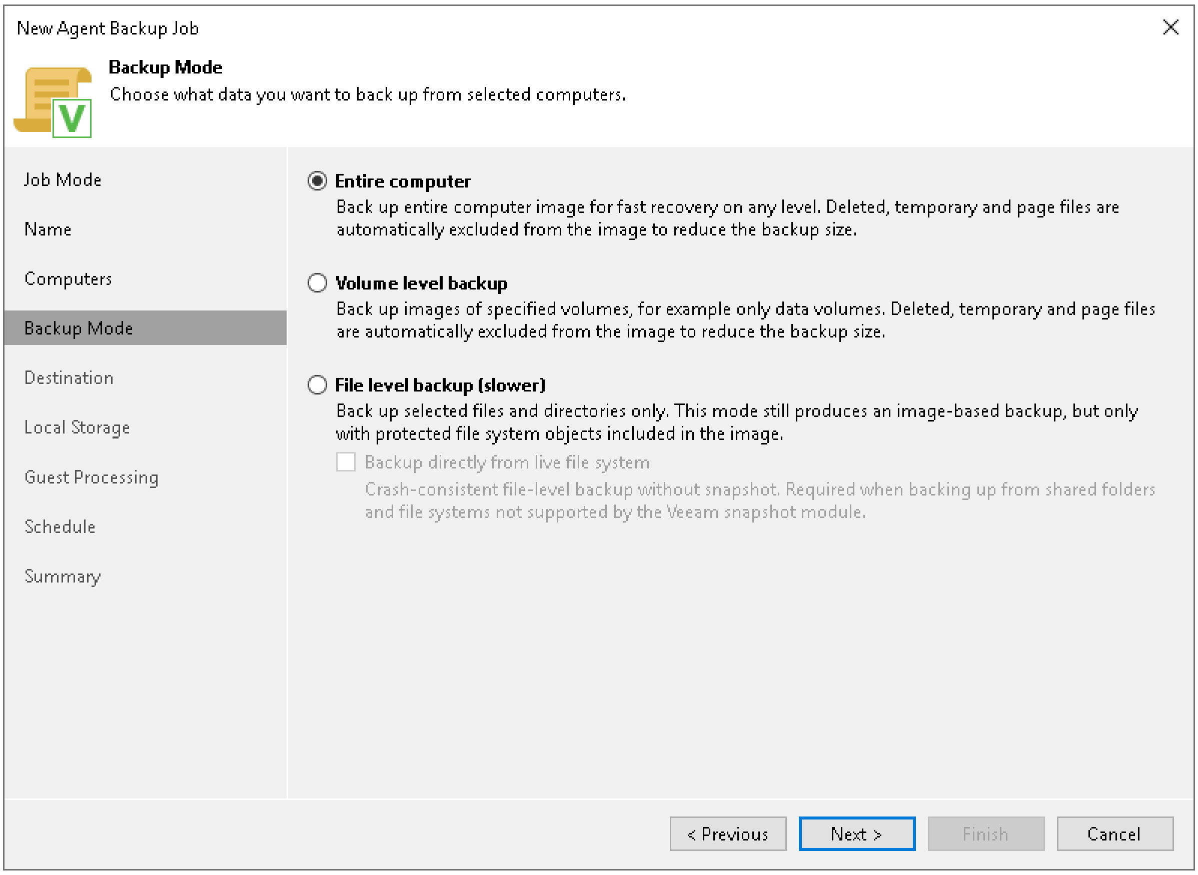
   - **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, the system volume. When you restore data from such backup, you will be able to recover data located on these volumes only: files, directories, application data and so on. With this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


New Agent Backup Job

Backup Mode

Choose what data you want to back up from selected computers.

● **Entire computer**

Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **Volume level backup**

Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **File level backup (slower)**

Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.

□ Backup directly from live file system

Crash-consistent file-level backup without snapshot. Required when backing up from shared folders and file systems not supported by the Veeam snapshot module.

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 policy:

- 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 policy. If a specified volume does not exist on one or more computers in the policy, the policy 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.

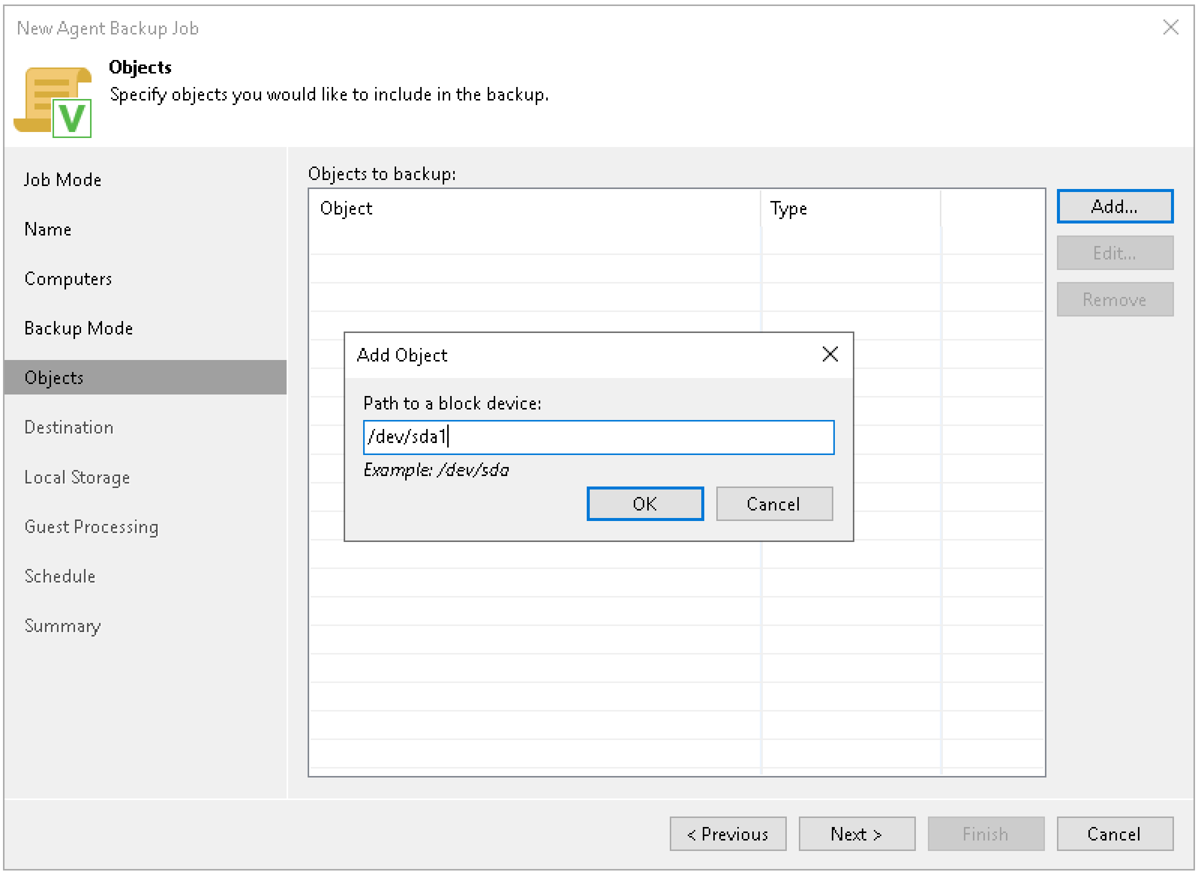
     > IMPORTANT
     >
     > Veeam Agent does not support backup of bind mount points. You must specify the path to the original mount point instead.

   - *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.



Path to a block device: /dev/sda1

Example: /dev/sda

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 by defining 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 folder on those computers and back up existing ones.

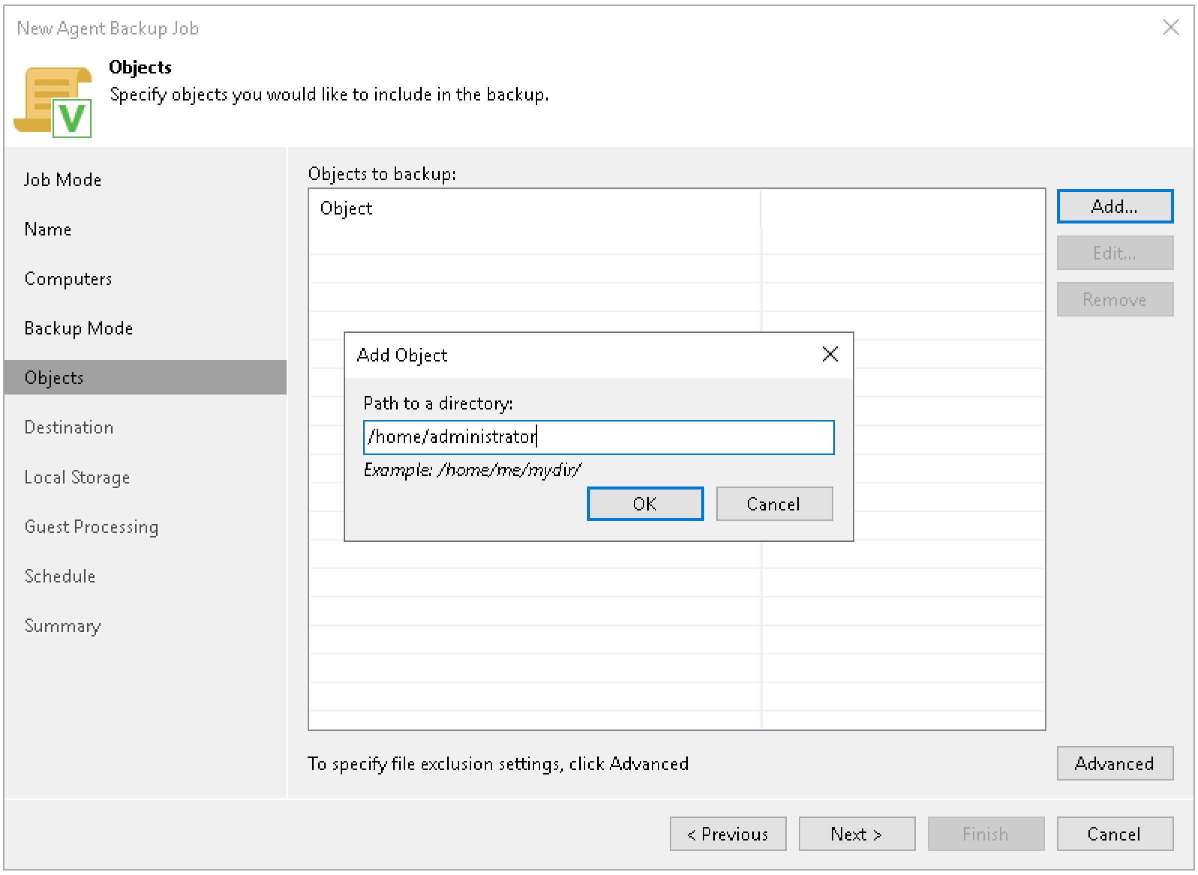
To specify directories to back up:

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**.

> **IMPORTANT**
>
> Veeam Agent does not support backup of bind mount points. You must specify the path to the original mount point instead.

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 will not automatically include into the backup scope the network file system mount points — for example, NFS or SMB network shared folders. To include such mount points, you need to specify paths to these mount points manually.
>
> For example, you have a network 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 network 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.

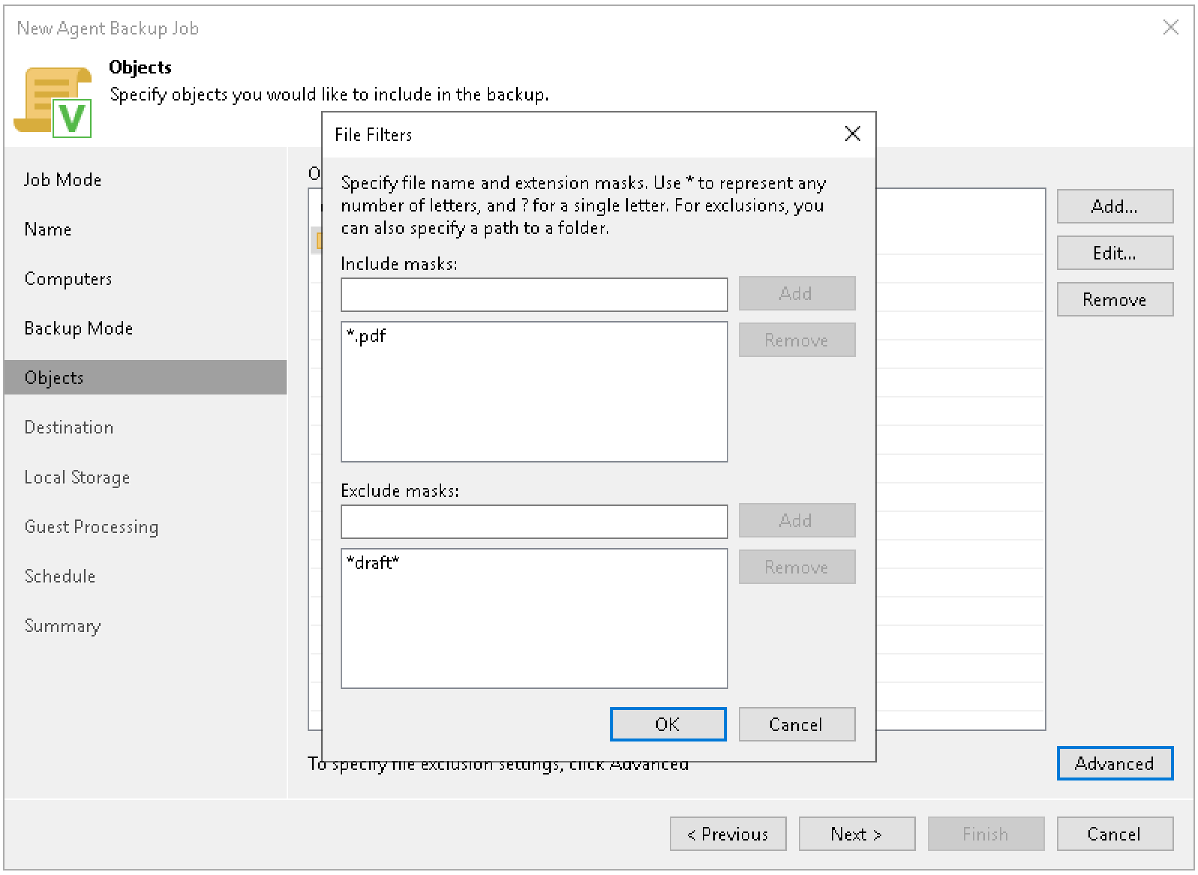
To configure a filter:

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 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 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.



Specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify a path to a folder.

Include masks: *.pdf

Exclude masks: *draft*

Step 7. Select Backup Destination

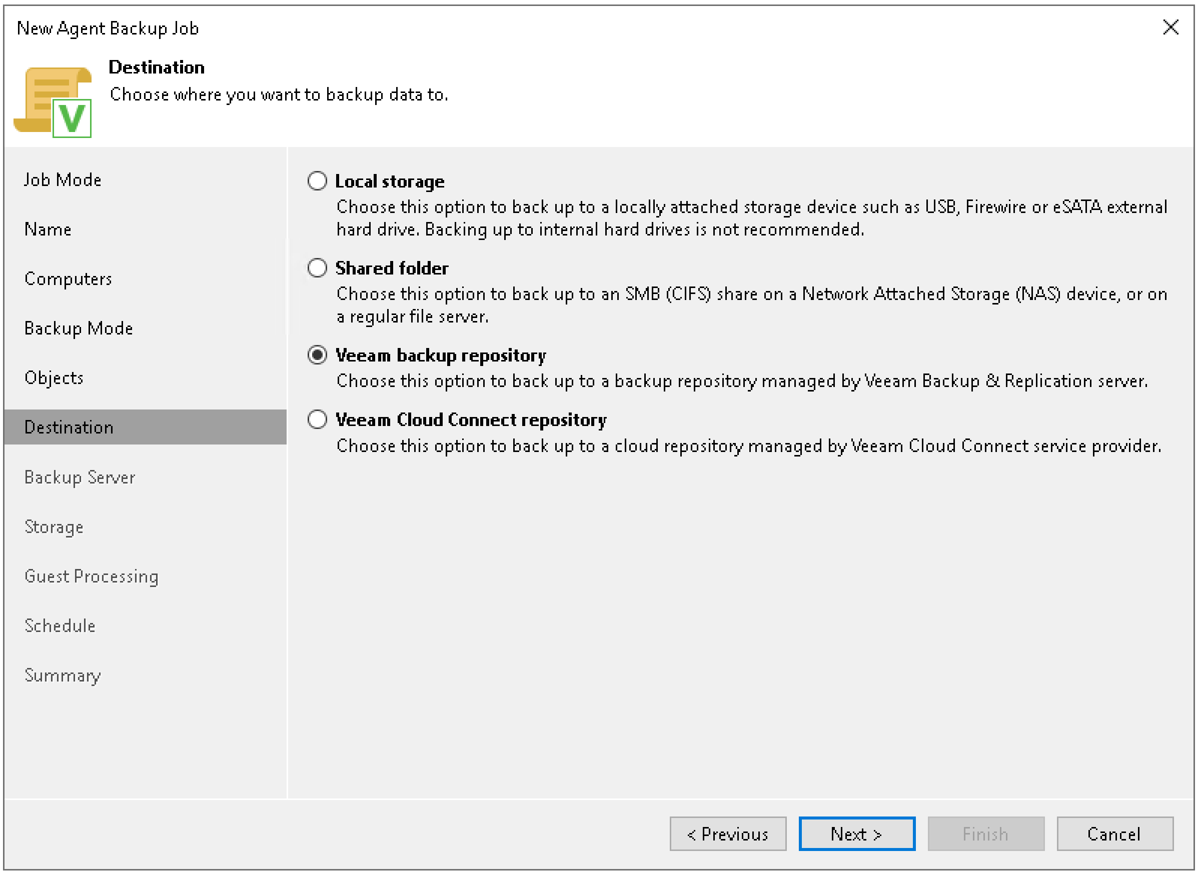
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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 network shared 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 in a backup repository managed by the 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.



New Agent Backup Job

Destination
Choose where you want to backup data to.

○ **Local storage**
Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.

○ **Shared folder**
Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.

● **Veeam backup repository**
Choose this option to back up to a backup repository managed by Veeam Backup & Replication server.

○ **Veeam Cloud Connect repository**
Choose this option to back up to a cloud repository managed by Veeam Cloud Connect service provider.

Step 8. Specify Backup Storage Settings

Specify backup storage settings for the backup policy:

- 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

At the **Local Storage** step of the wizard, 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 policy settings to this computer.

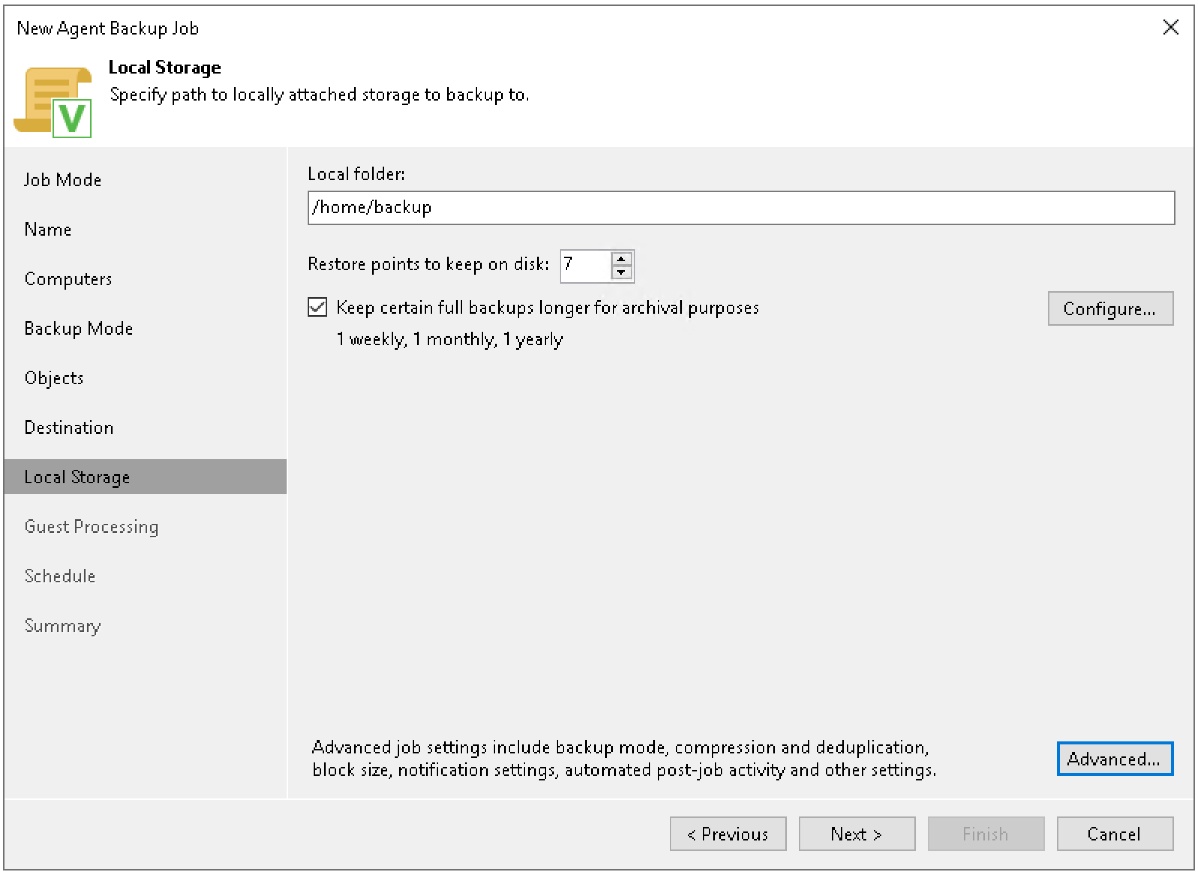
   > **IMPORTANT**
   >
   > USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.

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 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. To learn more, see Short-Term Retention Policy.

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 policy. To learn more, see Specify Advanced Backup Settings.



New Agent Backup Job

Local Storage

Specify path to locally attached storage to backup to.

Local folder: /home/backup

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Shared Folder Settings

At the **Shared Folder** step of the wizard, specify shared folder settings:

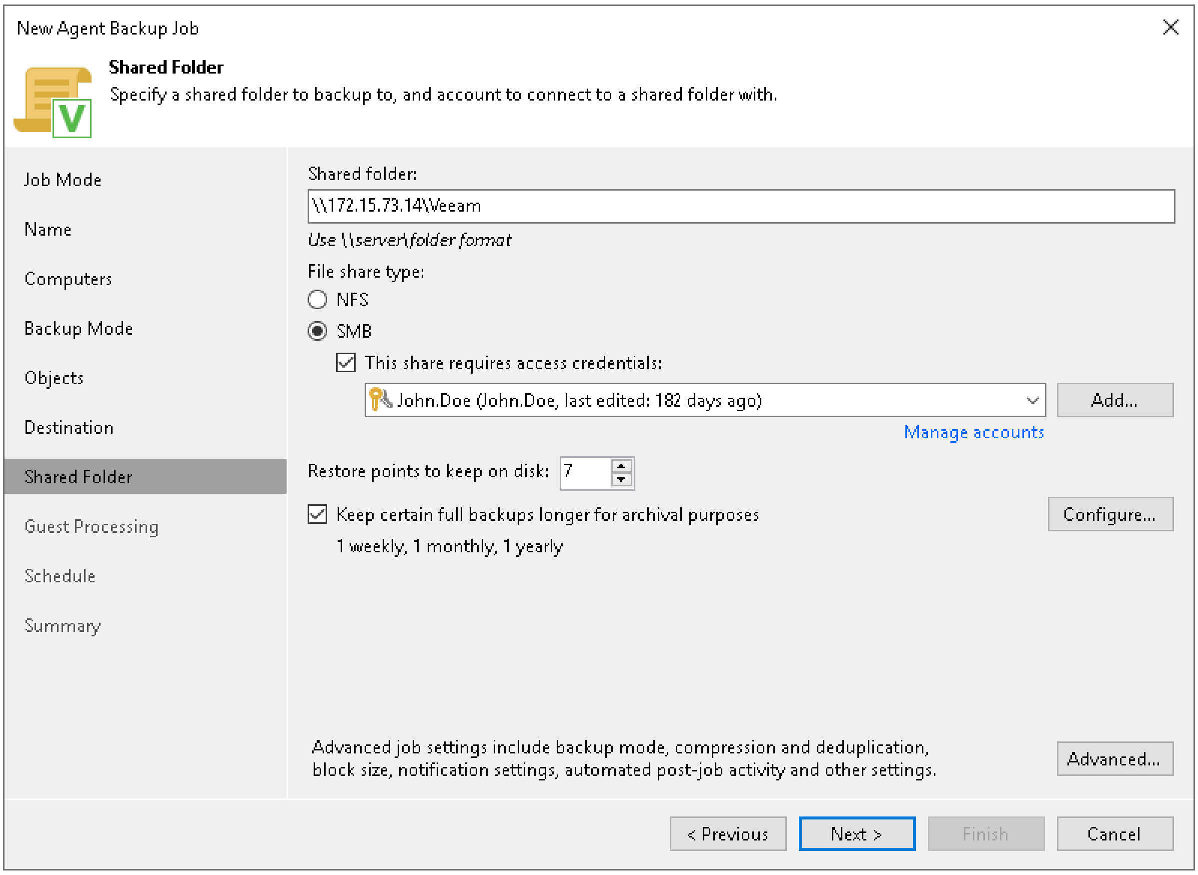
1. In the **File share type** section, select the type of a network shared folder:
   - **NFS** — to connect to a network shared folder using the NFS protocol.
   - **SMB** — to connect to a network shared folder using the SMB (CIFS) protocol.
2. In the **Shared folder** field, type a name of the network 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. To learn more, see Short-Term Retention Policy.

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 policy. To learn more, see Specify Advanced Backup Settings.



New Agent Backup Job

Shared Folder

Specify a shared folder to backup to, and account to connect to a shared folder with.

Shared folder: \\172.15.73.14\Veeam

Use \\server\folder format

File share type:

○ NFS

● SMB

☑ This share requires access credentials:

John.Doe (John.Doe, last edited: 182 days ago)

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Veeam Backup Repository Settings

At the **Backup Server** step of the wizard, specify settings to connect to the backup repository:

1. At the Backup Server step of the wizard, specify backup server settings.

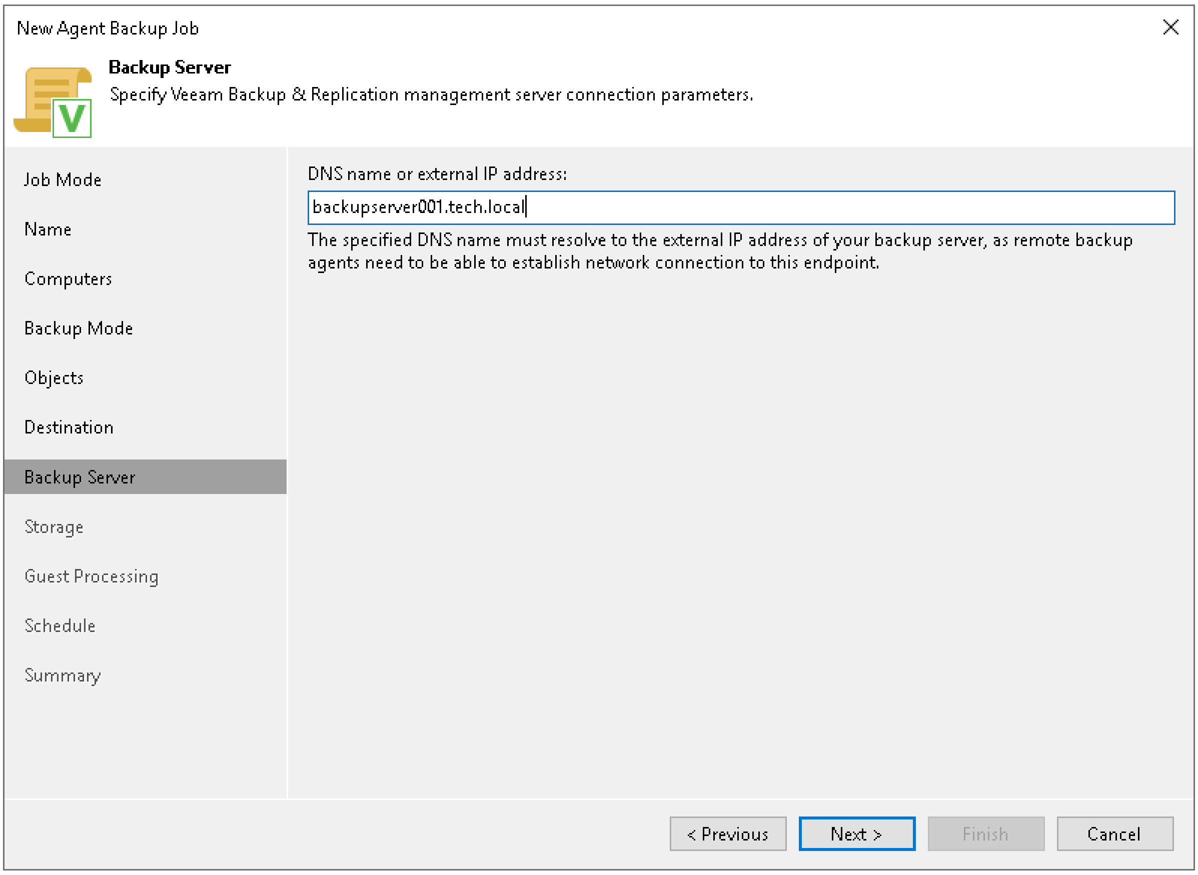
2. At the Backup Repository step of the wizard, select the Veeam backup repository.

Specifying Backup Server Settings

In the **DNS name or external IP address field**, make sure that the name or IP address of the Veeam backup server, on which you configure the Veeam Agent backup policy, is displayed. Do not specify the name or IP address of another Veeam backup server. The specified DNS name or IP address must be resolvable 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.



DNS name or external IP address: backupserver001.tech.local

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

Selecting Backup Repository

At the **Backup Repository** 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 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. To learn more, see Short-Term Retention Policy.

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.

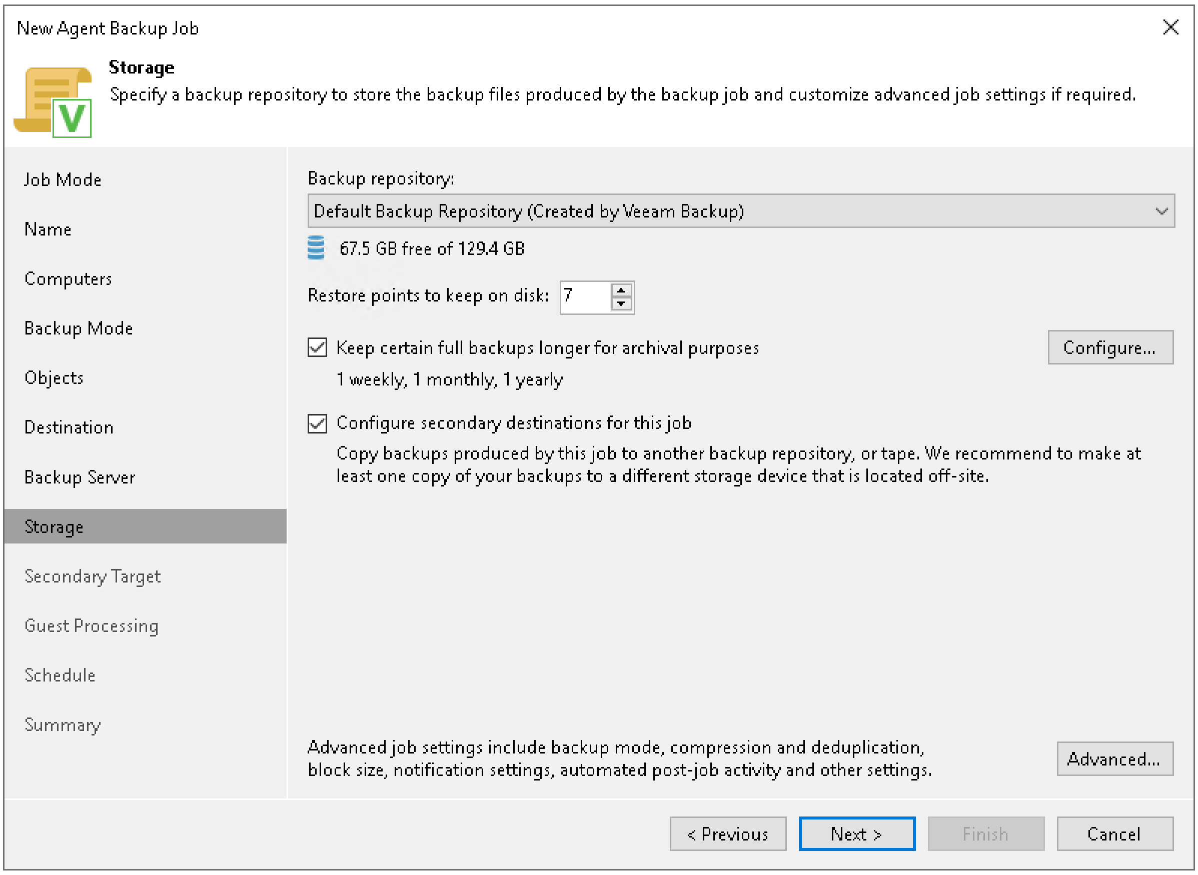
   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

4. If you want to archive backup files created with the backup policy 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.

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

   > NOTE
   >
   > You must enable backup file encryption in the backup job storage settings if you back up data to the Veeam Data Cloud Vault storage added as a Veeam backup repository.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Default Backup Repository (Created by Veeam Backup)

67.5 GB free of 129.4 GB

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

☑ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

Cloud Repository Settings

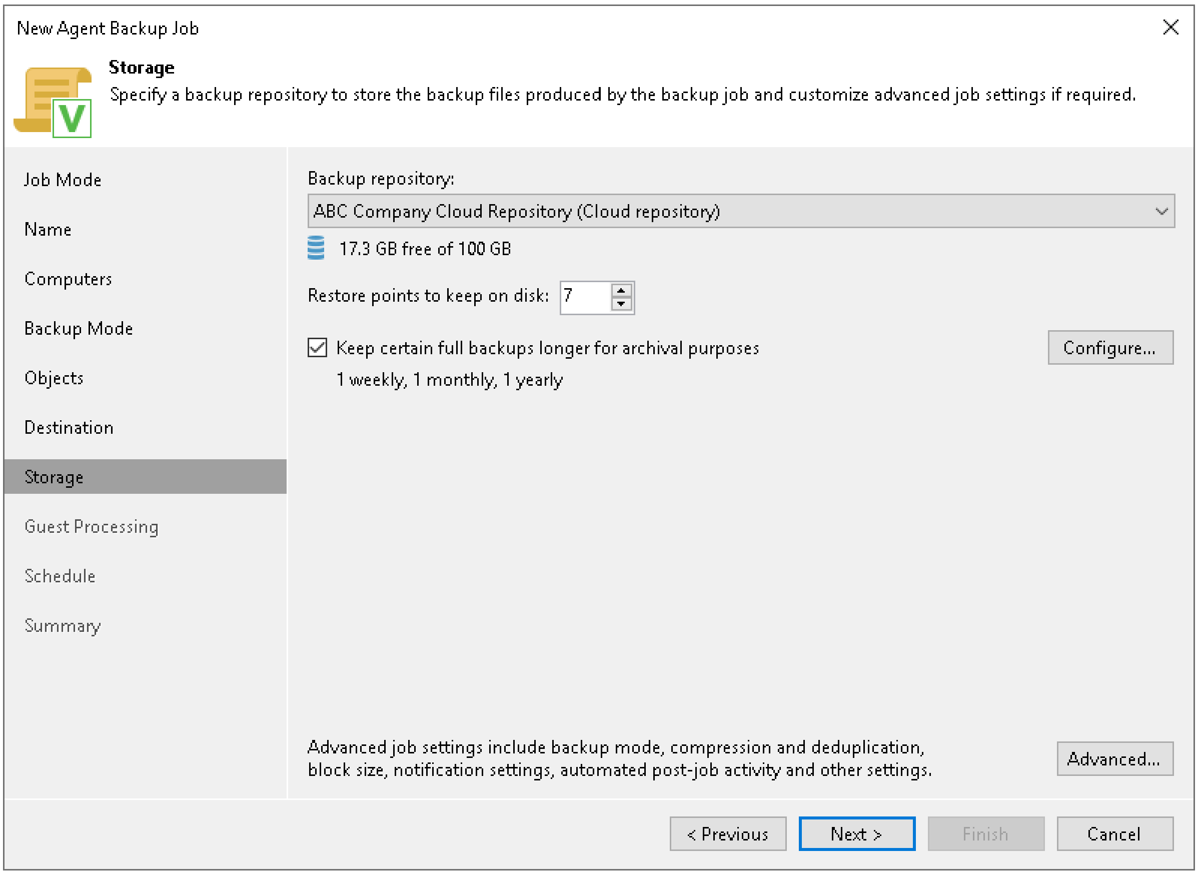
> NOTE
>
> Keep in mind that FQDN or IP addresses of Veeam Agent computers that you back up to the cloud repository will be visible to the Veeam Cloud Connect service provider. To learn more, see Before You Begin.

At the **Storage** step of the wizard, 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. To learn more, see Short-Term Retention Policy.
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 policy. To learn more, see Specify Advanced Backup Settings.

   > **IMPORTANT**
   >
   > You must enable backup file encryption in the backup job storage settings if you back up data to the Veeam Data Cloud Vault storage added as a Veeam Cloud Connect repository.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: ABC Company Cloud Repository (Cloud repository)

17.3 GB free of 100 GB

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other 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.

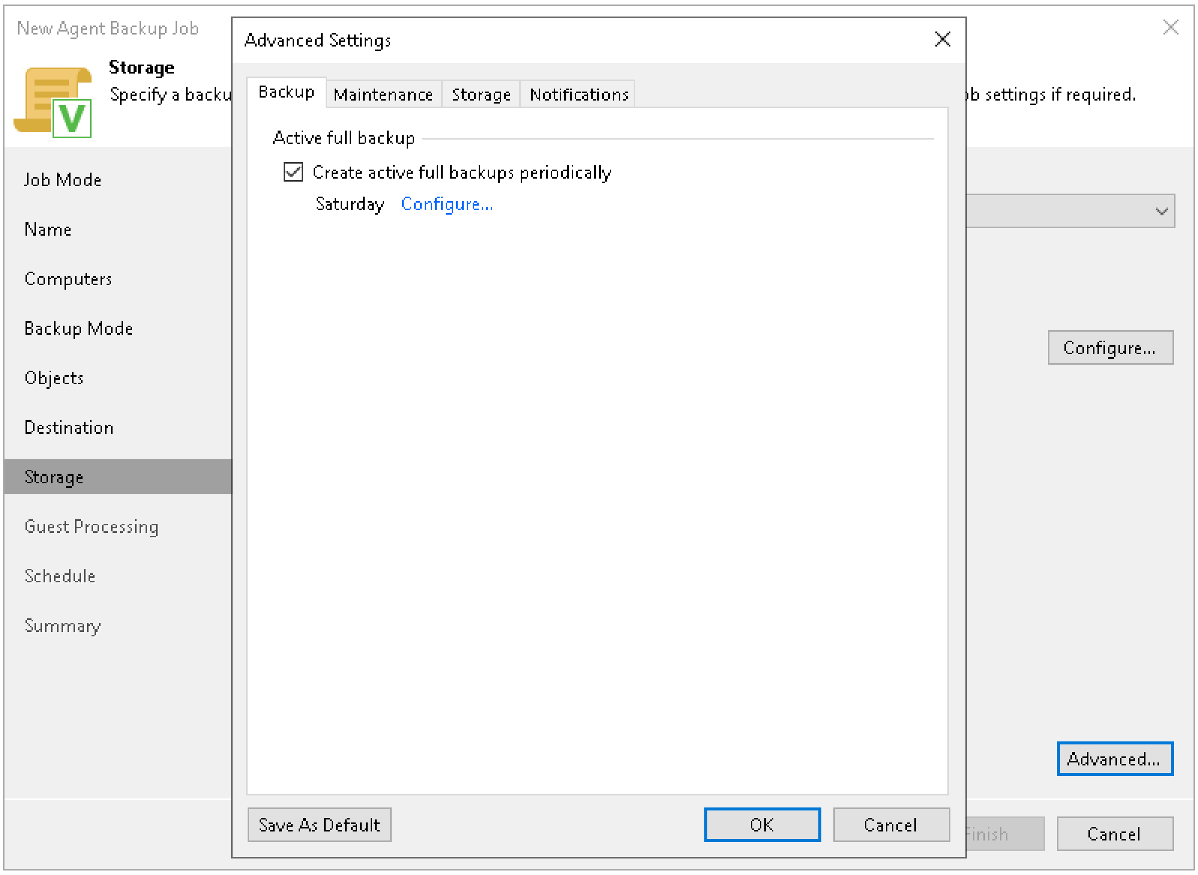
Backup Settings

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

1. Click **Advanced** at the **Storage** step of the wizard.
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.



Active full backup

☑ Create active full backups periodically

Saturday Configure...

Maintenance Settings

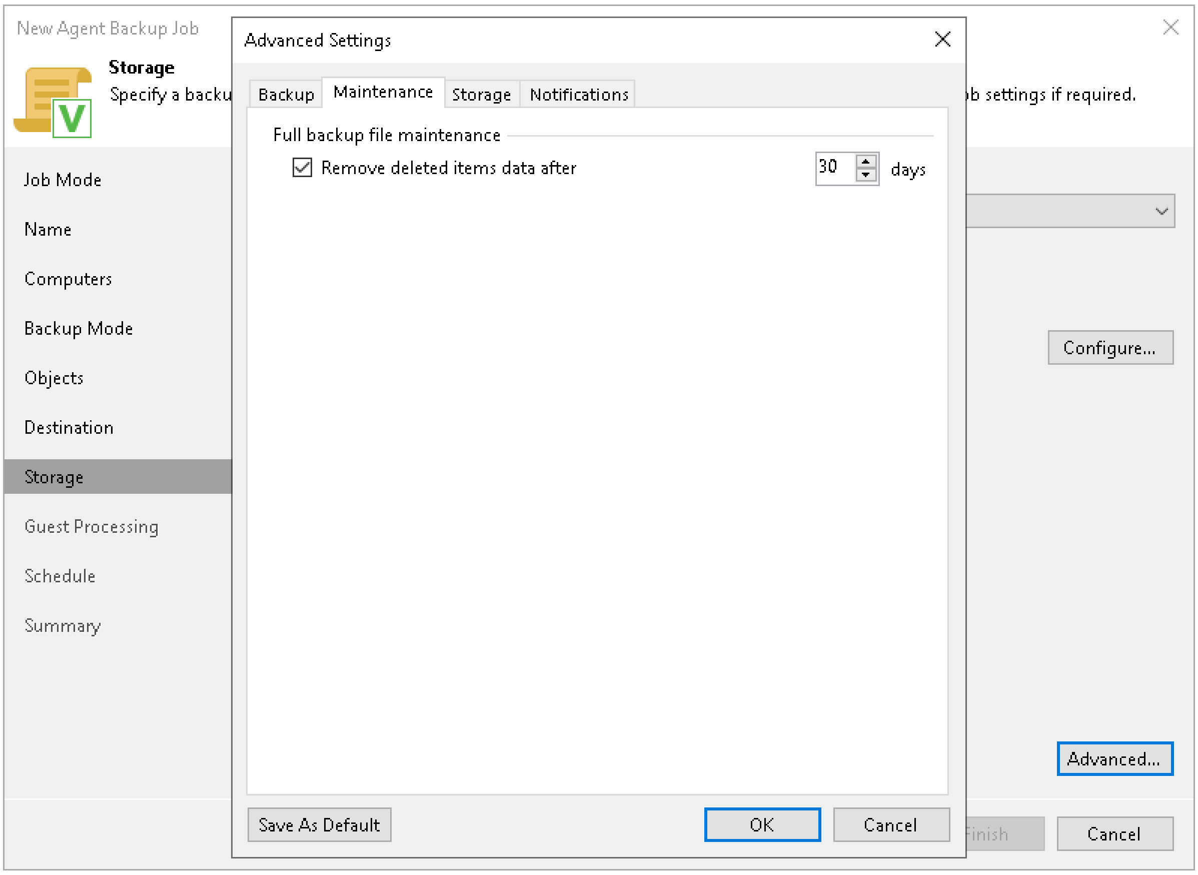
You can specify maintenance settings for a backup chain created with the Veeam Agent backup policy. Maintenance operations help make sure that the backup chain remains valid and consistent.

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 job in 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. In the opposite case, the backup job may work not as expected and remove data that you still require.


Advanced Settings

Full backup file maintenance

☑ Remove deleted items data after 30 days

Storage Settings

To specify storage settings for the Veeam Agent backup policy:

1. Click **Advanced** at the **Storage** step of the wizard.
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*. To learn more about the compression levels, see the Data Compression section in the Veeam Agent for Linux User Guide.
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 policy performance: *4 MB*, *1 MB*, *512 KB* or *256 KB*.

> NOTE
>
> If you change the storage optimization settings for the backup policy, new settings will not have any effect on previously created files in the chain. They will be applied to new files created after the settings were changed.
>
> To apply new storage optimization settings in backup policies, you must create an active full backup after you change storage optimization settings. Veeam Backup & Replication will use the new block size for the active full backup and subsequent backup files in the backup chain. To learn about the active full backup, see Performing Active Full Backup.

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.

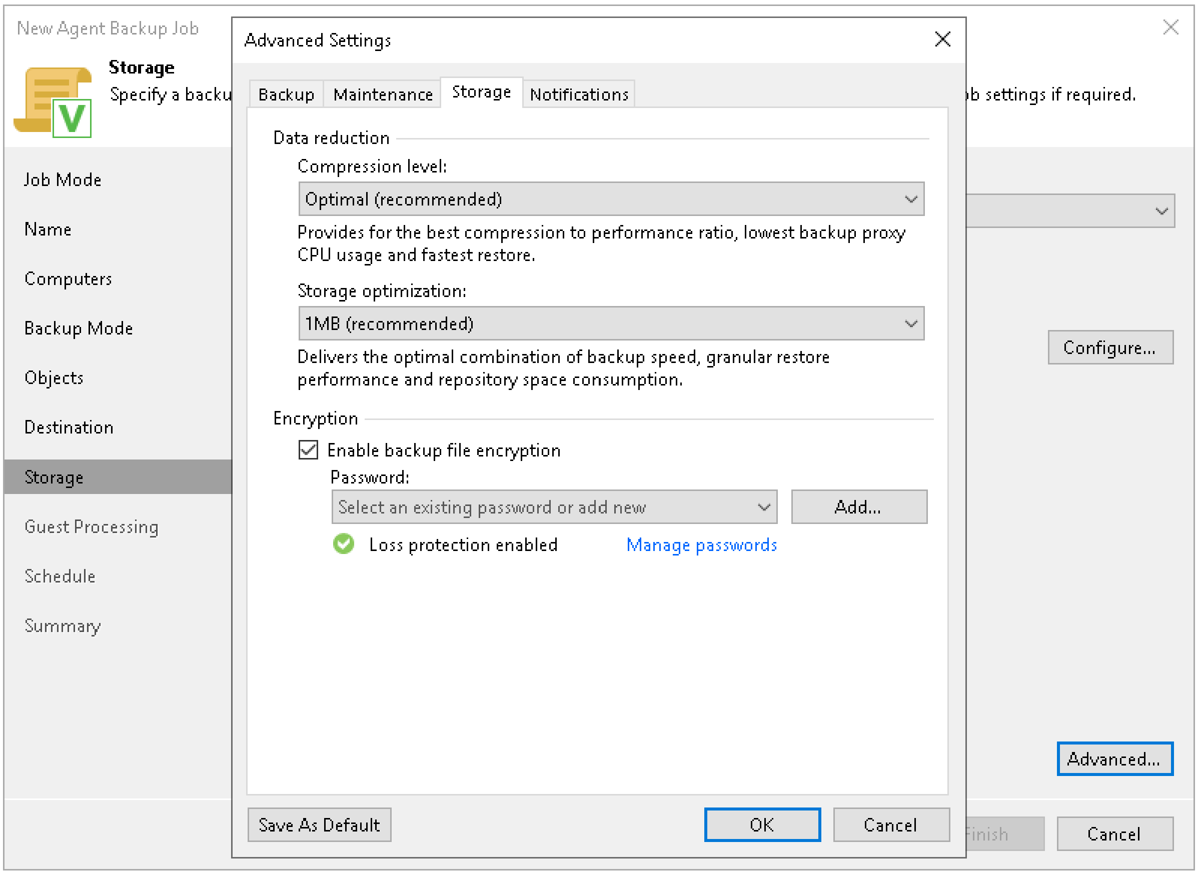
   If the backup server is not connected to Veeam Backup Enterprise Manager, you will not be able to restore data from encrypted backups in case you lose the password. Veeam Backup & Replication will display a warning about it: *Loss protection disabled*. For more information, see the Decrypting Data Without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

NOTE

Consider the following:

- If you plan to encrypt the content of backup files, consider the limitations listed in the Data Encryption Limitations subsection.
- You must encrypt the backup policy if you want to back up data to the Veeam Data Vault storage.
- You cannot use Key Management System (KMS) keys for data encryption with a Veeam Agent backup policy. To be able to use KMS keys, create a backup job managed by the backup server.

  To learn more about KMS keys, see the Key Management System Keys section in the Veeam Backup & Replication User Guide.



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: Select an existing password or add new [Add...]

✓ Loss protection enabled Manage passwords

Data Encryption Limitations

If you plan to encrypt the content of backup files, consider the following limitations:

- Data encryption settings for Veeam Agent backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup 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 an SMB 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 or disable encryption for an existing Veeam Agent backup 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 policy, Veeam Agent will encrypt the backup chain starting from the next restore point created with this policy.
- 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 & 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.

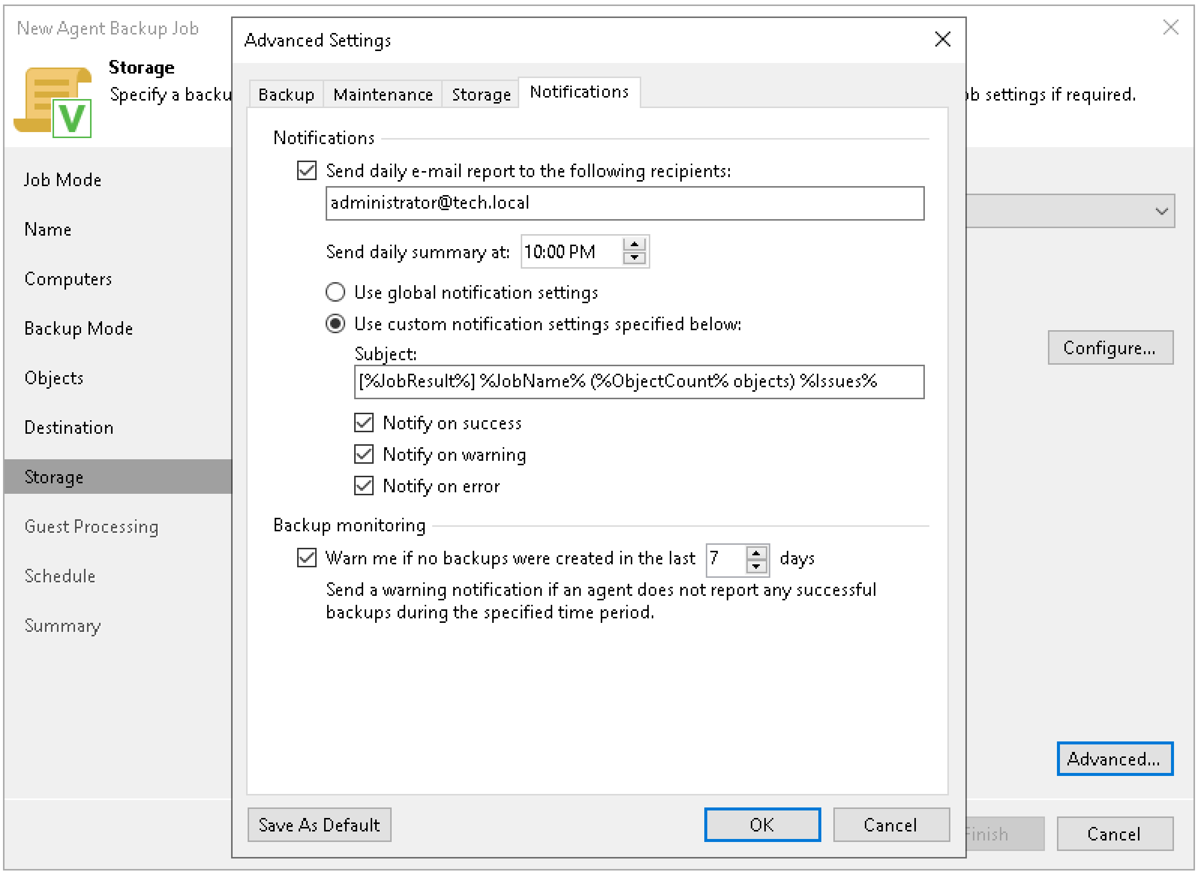
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server. Veeam Backup & Replication will send the email report containing 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 **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.



Advanced Settings

Backup | Maintenance | Storage | Notifications

Notifications

☑ Send daily e-mail report to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

☑ Notify on error

Backup monitoring

☑ Warn me if no backups were created in the last 7 days

Send a warning notification if an agent does not report any successful backups during the specified time period.

Save As Default | OK | Cancel

Step 10. Specify Secondary Target

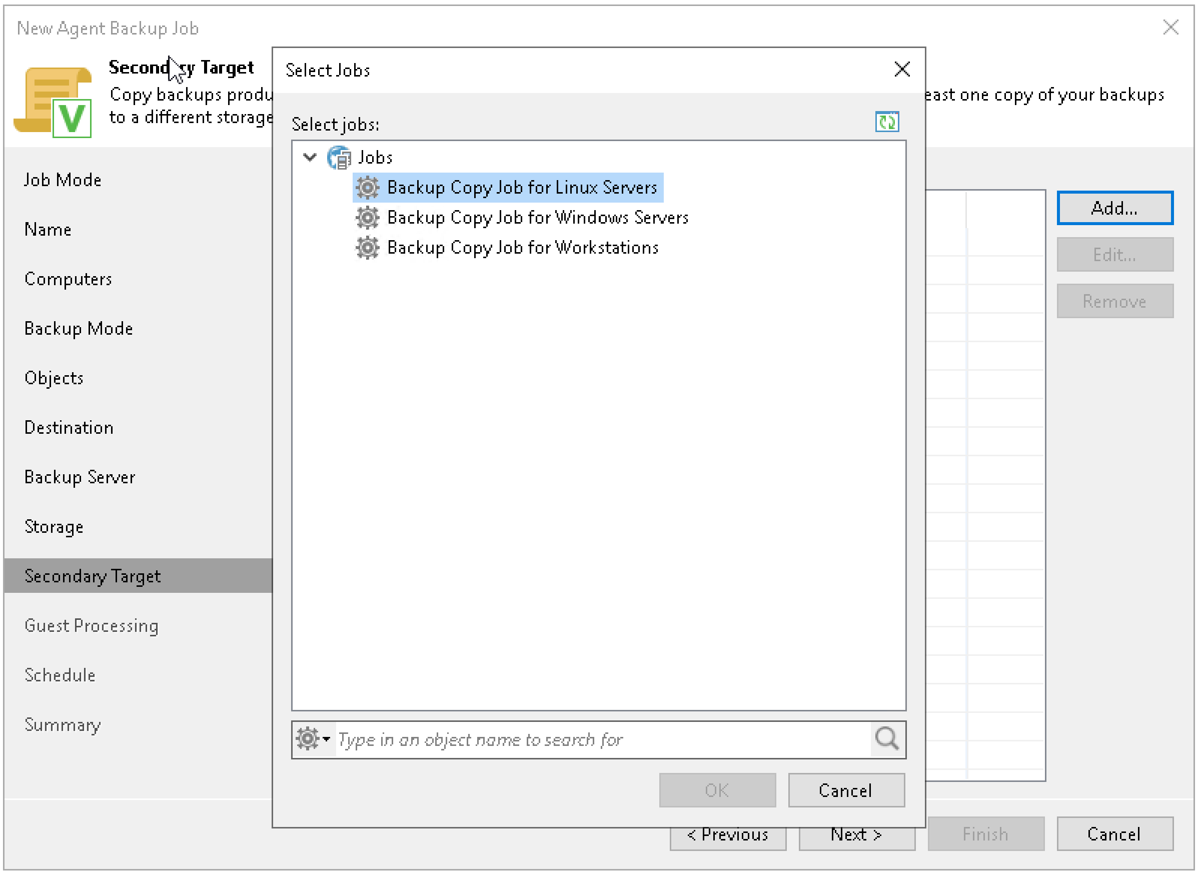
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

At the **Secondary Target** step of the wizard, you can link the Veeam Agent backup policy to a backup to tape or backup copy job. As a result, the backup policy will be added as a source to the backup to tape or backup copy job. Backup files created with the backup policy 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 policy to these jobs, Veeam Backup & Replication will automatically update the linked jobs to define the Veeam Agent backup policy 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 policy. You can link several jobs to the backup policy — 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 policy that protects Linux-based computers:

- Application-aware processing
- File indexing

Configuring Application-Aware Processing

Before you begin, review the limitations of database processing.

To configure application-aware processing, do the following:

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. 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 credentials 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 about 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.
5. To specify credentials for a particular computer or a protection group, click **Credentials** on the right to set up credentials. In the **Guest OS Credentials** window, select a protection group or individual computer and click **Set User**.

   If you specify custom credentials for a particular computer or a protection group in the **Guest OS Credentials** window, Veeam Agent will use these custom credentials instead of the credentials specified in the **Guest OS credentials** list (see Step 4).

   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, MySQL processing and scripts execution, Veeam Agent always uses the `root` account.

6. Configure the necessary settings for the selected protection group or individual computer:
   - [For backup policies that protect servers] General Settings
   - [For backup policies that protect servers] Processing settings for Oracle database system
   - [For backup policies that protect servers] Processing settings for MySQL database system
   - [For backup policies that protect servers] Processing settings for PostgreSQL database system
   - Backup job and snapshot scripts

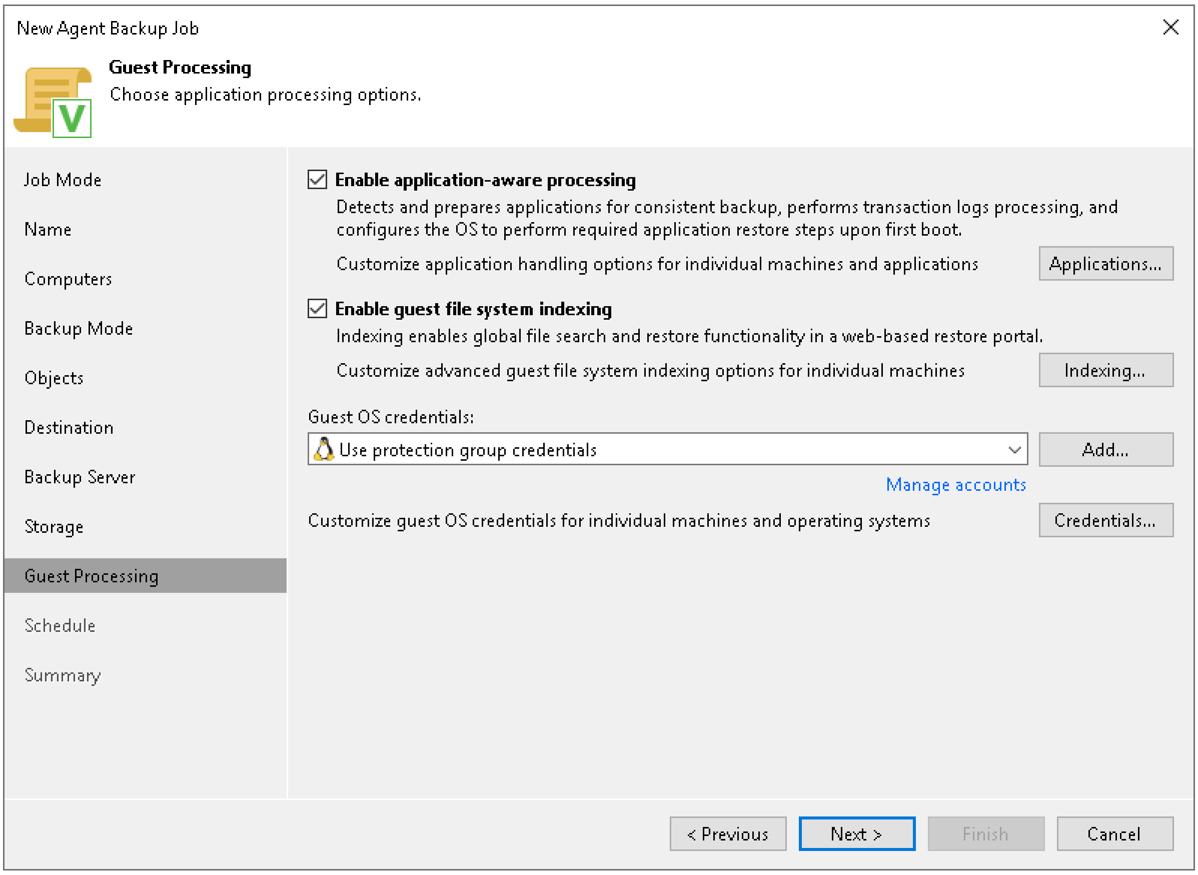
File Indexing

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.


New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Indexing enables global file search and restore functionality in a web-based restore portal.

Customize advanced guest file system indexing options for individual machines

Guest OS credentials: Use protection group credentials

Customize guest OS credentials for individual machines and operating systems

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 Begin

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 more information, see Guest Processing Settings.

Configuring 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 and click **Edit**.

3. On the **General** tab, in the **Applications** section, specify the behavior scenario for application-aware processing:

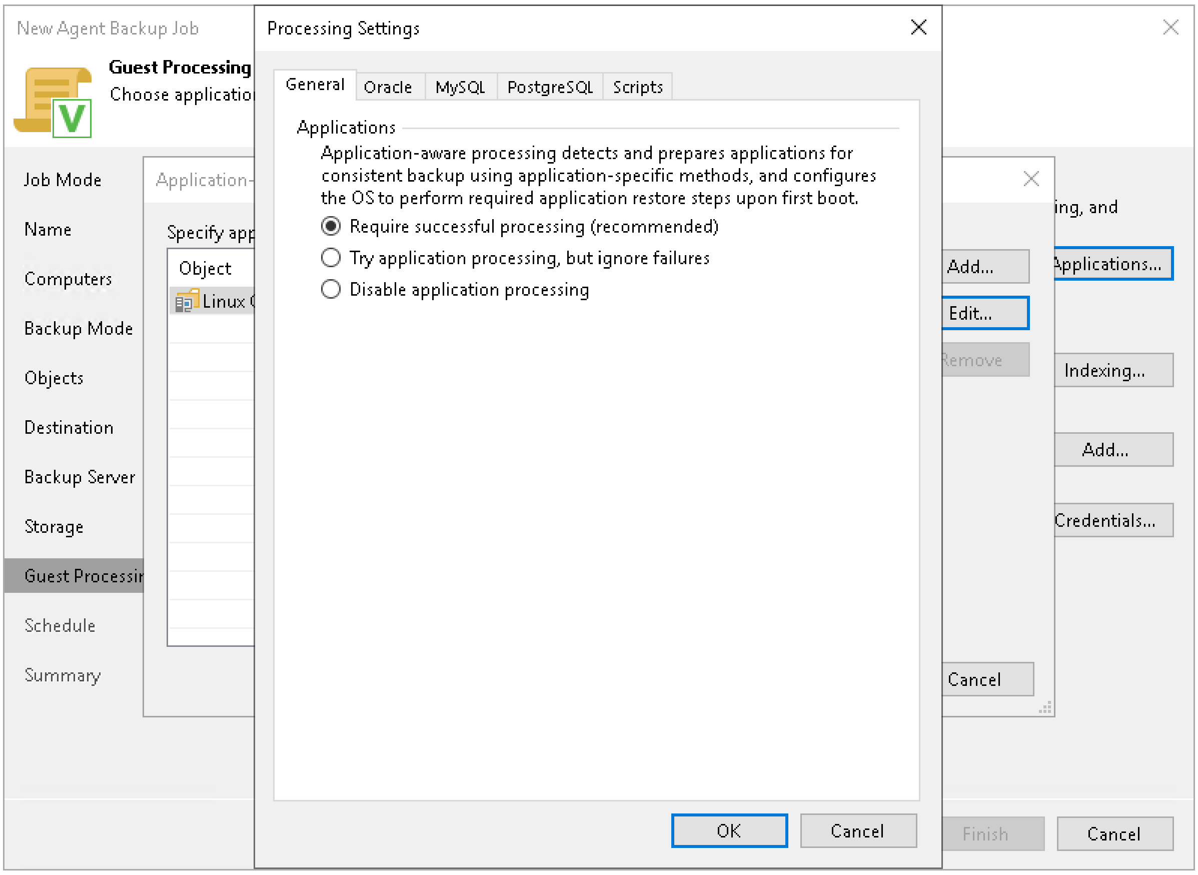
   - Select **Require successful processing** if you want Veeam Agent for Linux to process database systems. With this option selected, if an error occurs when processing a database or database instance, Veeam Agent for Linux will stop the backup process.

     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 database systems. With this option selected, if an error occurs when processing a database or database instance, Veeam Agent for Linux will not stop the backup process. Instead, Veeam Agent for Linux will skip this database or database instance and proceed to the next one. Information about the skipped database or database instance will be displayed in a warning message in the policy session statistics. After the backup process is completed, you will be able to restore data from the backup and restore databases or database instances 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 database systems. 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 policy on the **Scripts** tab of the window.



Applications

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

● Require successful processing (recommended)

○ Try application processing, but ignore failures

○ Disable application processing

Oracle Processing Settings

You can specify how Veeam Agent for Linux must process the Oracle database system.

Before You Begin

Before you start working with the Oracle database system, 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.

To learn more, 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.

To learn more, see Application-Aware Processing.

Configuring Oracle Processing

To specify how Veeam Agent for Linux must process the Oracle database system, 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, specify a user account that Veeam Agent for Linux will use to connect to the Oracle database. You can do one of the following:

   - Select from the **Specify Oracle account with SYSDBA privileges** list a database user account that has SYSDBA rights on the Oracle database.

     If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. With this option selected, Veeam Agent for Linux will connect to the Oracle database under the account that you have selected in the **Specify Oracle account with SYSDBA privileges** list.

   - Select the **Use guest OS credentials** option.

     With this option selected, Veeam Agent for Linux will do the following:

     i. Veeam Agent will check if you specified custom credentials for the computer or protection group in the **Guest OS Credentials** window at the **Guest Processing** step of the wizard.

        If you specified custom credentials for the computer or protection group in the **Guest OS Credentials** window, Veeam Agent will process the Oracle database under the OS account that you have specified in this window.

        If you have not specified custom credentials for the computer or protection group, Veeam Agent will do as described in the step ii of this procedure.

        To learn more, see step 5 in Specify Guest Processing Settings.

     ii. Veeam Agent will check what have you selected in the **Guest OS credentials** list at the **Guest Processing** step of the wizard.

        If you specified credentials in the **Guest OS credentials** list, Veeam Agent will process the Oracle database under the account that you have specified in this list.

If you have not specified credentials in the list and selected the **Use protection group credentials** option instead, Veeam Agent will do as described in the step iii of this procedure.

To learn more, see step 4 in Specify Guest Processing Settings.

iii. Veeam Agent will check what credentials have you specified for the computer or protection group at the **Computers** step of the wizard.

If you specified stored credentials for this computer in the protection group settings, Veeam Agent will process the Oracle database using the specified account.

If you specified single-use credentials for this computer in the protection group settings, Veeam Agent will process the Oracle database using the root user.

To learn more, see Specifying Computers.

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

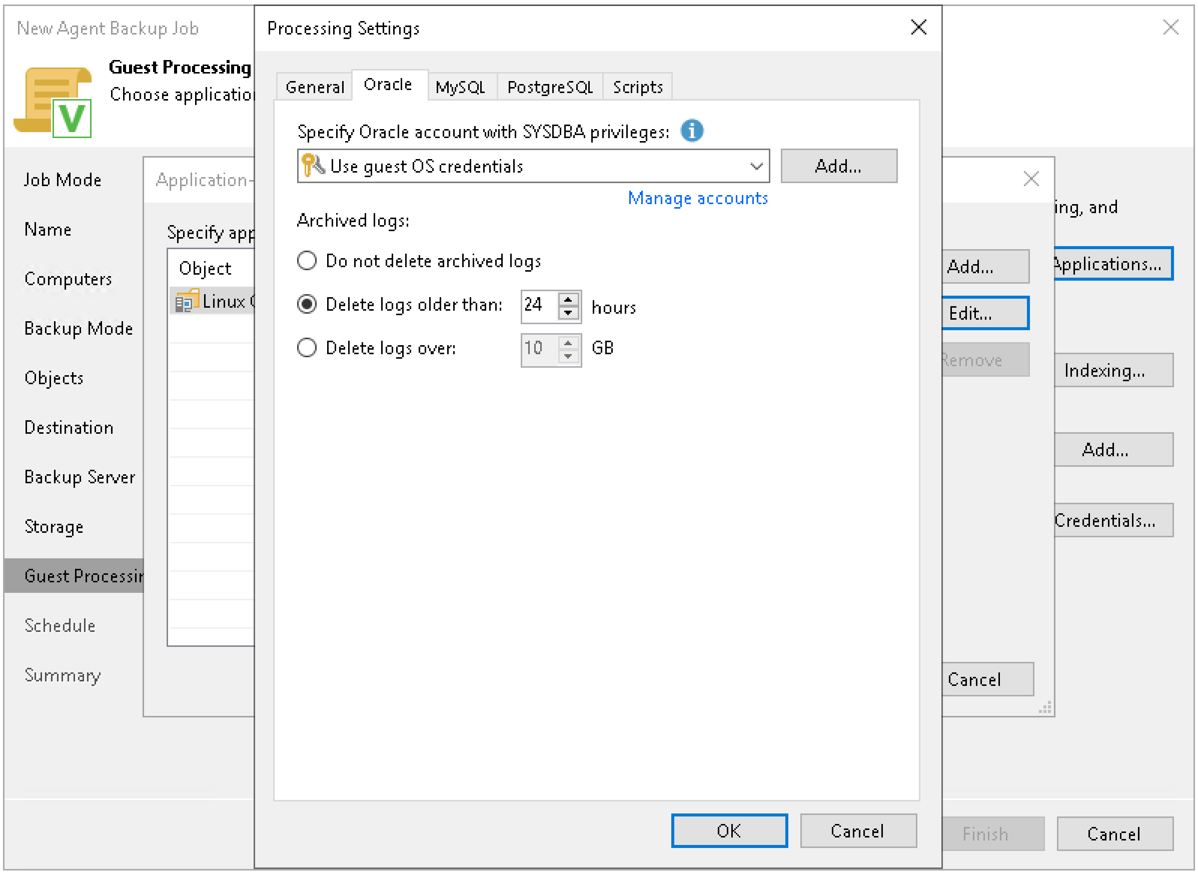
   - Select **Do not delete archived logs** if you want Veeam Agent for Linux to preserve archived logs. When the backup policy completes, Veeam Agent for Linux will not delete archived logs.

     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 themselves.

   - 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 policy to complete successfully and then trigger archived logs truncation through Oracle Call Interface (OCI). If the backup policy fails, the logs will remain untouched until the next successful backup policy session.

TIP

If you configure backup policy to back up archived logs, Veeam Agent for Linux will not trigger archived logs deletion after each log backup policy session. To prevent Oracle database logs from overgrowing, run the backup policy for the Veeam Agent computer more often.



Specify Oracle account with SYSDBA privileges: Use guest OS credentials

Archived logs:

○ Do not delete archived logs

● Delete logs older than: 24 hours

○ Delete logs over: 10 GB

MySQL Processing Settings

You can specify how Veeam Agent for Linux must process a MySQL database.

Before You Begin

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.

To learn more, 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**.

To learn more, see Application-Aware Processing.

4. MySQL tables with the MyISAM storage engine must be locked to keep them in a consistent state while Veeam Agent is creating the system snapshot. To correctly process such tables, make sure that the user account you want to specify in the MySQL processing settings has the following instance-wide privileges:

   - `SELECT`. This privilege enables Veeam Agent to access tables' metadata and select for a lock the tables that use the MyISAM storage engine. Without this privilege, the processing of the MySQL database system will run successfully but MyISAM tables will not be locked, which may result in an inconsistent state of the backed up data.

   - `LOCK TABLES`. This privilege is required for locking the selected MyISAM tables. If some MyISAM tables are selected but the MySQL account does not have the `LOCK TABLES` privilege, the processing of the MySQL database system will fail.

   - `RELOAD` or `FLUSH_TABLES`. If some MyISAM tables are selected but the MySQL account does not have either `RELOAD` or `FLUSH_TABLES` privilege, the processing of the MySQL database system will fail.

   To obtain information about the privileges that are assigned to an account, use MySQL functionality, for example, the `SHOW GRANTS` statement. To learn more, see MySQL documentation.

Configuring MySQL Processing

To specify how Veeam Agent for Linux must process a MySQL database system, 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.

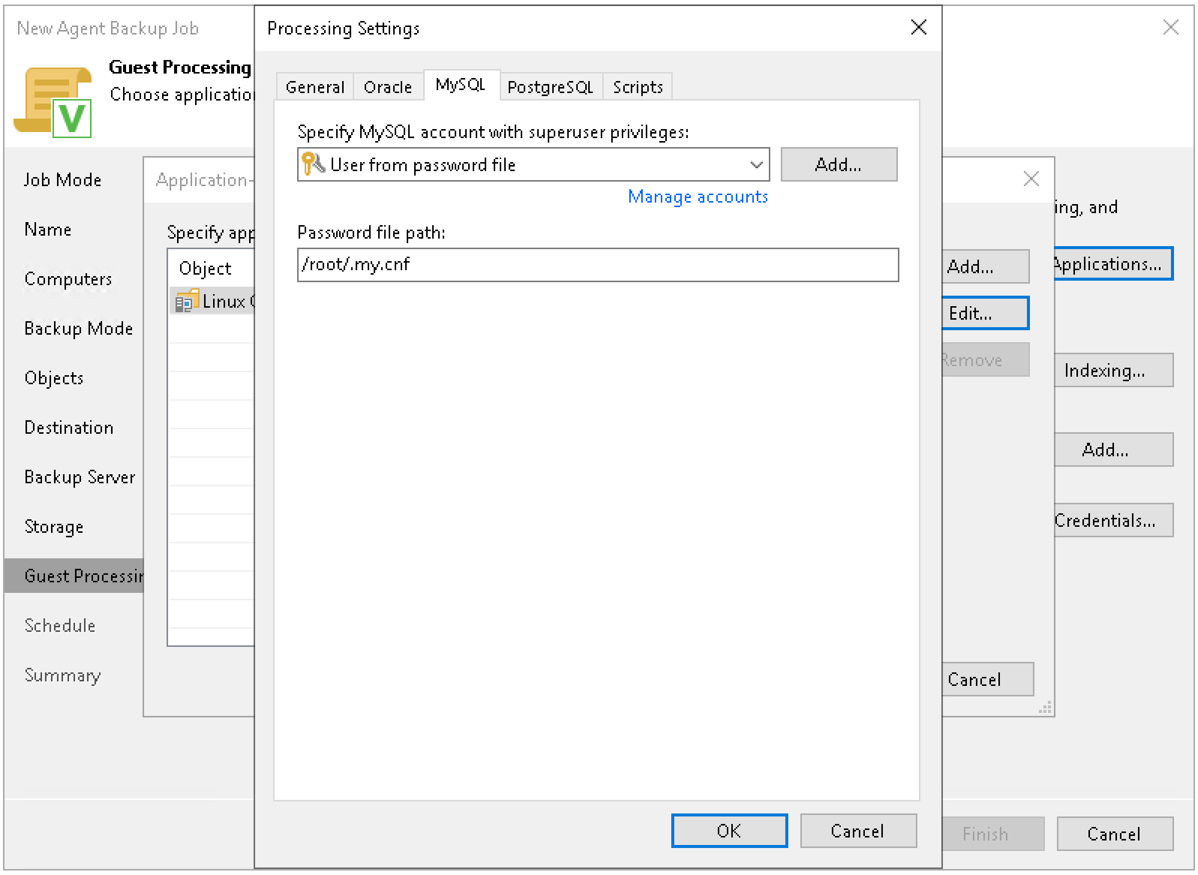
3. On the **MySQL** tab, specify a user account that Veeam Agent for Linux will use to connect to the MySQL database, from the **Specify MySQL account with superuser privileges** list, select a user account.

   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.



Specify MySQL account with superuser privileges: User from password file

Password file path: /root/.my.cnf

PostgreSQL Processing Settings

You can specify how Veeam Agent for Linux must process the PostgreSQL database system.

Before You Begin

Before you configure the PostgreSQL processing, consider the following:

- Enable the following prerequisite settings:

    a. At the **Guest Processing** step of the wizard, the **Enable application-aware processing** check box is selected.

    b. 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.

    c. At the **Guest Processing** step of the wizard, in the **Guest OS credentials** list, a necessary user account is selected.

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

    To learn more, see Guest Processing Settings and Application-Aware Processing.

- Consider the Requirements and Limitations section in the Veeam Backup & Replication User Guide.

Configuring PostgreSQL Processing

> NOTE
>
> By default, Veeam Agent recursively scans the `/etc/postgresql`, `/var/lib/postgresql` and `/var/lib/pgsql` directories for the configuration files of PostgreSQL instances. If you keep configuration files in custom directories, the *pgsqlagent agent* will use its own `VeeamPostgreSQLAgent.xml` configuration file that is located in the `/etc/veeam/` directory. The pgsqlagent agent configuration file must be a single line XML.
>
> To explicitly include or exclude specific configuration files from rescan, you can add the following commands to the `VeeamPostgreSQLAgent.xml` file:
>
> - `ExcludeConfigDirs` — use this element to exclude configuration files.
> - `AddConfigDirs` — use this element to include configuration files.
>
> For example: `<config AddConfigDirs="/opt/psql/" ExcludeConfigDirs="/var/lib/postgresql/13/main45/,/var/lib/postgresql/13/maindd/" />`

To specify how Veeam Agent for Linux must process the PostgreSQL database system, 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. On the **PostgreSQL** tab, specify a user account that Veeam Agent for Linux will use to connect to the PostgreSQL database. You can do one of the following:

   - Select from the **Specify PostgreSQL account with superuser privileges** list a user account that has the required rights for the database.

     If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right to add credentials. With this option selected, Veeam Agent for Linux will connect to the PostgreSQL database under the account that you have selected in the **Specify PostgreSQL account with superuser privileges** list.

     Keep in mind that if you plan to select the peer authentication method at the step 4 of this procedure, you can add a user account in the Credentials Manager without specifying the password for the account.

   - Select the **Use guest OS credentials** option.

     With this option selected, Veeam Agent for Linux will do the following:

     i. Veeam Agent will check if you have specified custom credentials for the computer or protection group in the **Guest OS Credentials** window at the **Guest Processing** step of the wizard.

        If you specify custom credentials for the computer or protection group in the **Guest OS Credentials** window, Veeam Agent will process the PostgreSQL database under the account that you have specified in this window.

        If you do not specify custom credentials for the computer or protection group, Veeam Agent will do as described in the step ii of this procedure.

        To learn more, see step 5 in Specify Guest Processing Settings.

ii. Veeam Agent will check what you have selected in the **Guest OS credentials** list at the **Guest Processing** step of the wizard.

If you specify credentials in the **Guest OS credentials** list, Veeam Agent will process the PostgreSQL database under the account that you specify in this list.

If you do not specify credentials in the list and select the **Use protection group credentials** option instead, Veeam Agent will do as described in the step iii of this procedure.

To learn more, see step 4 in Specify Guest Processing Settings.

iii. Veeam Agent will check what credentials you have specified for the computer or protection group at the **Computers** step of the wizard.

If you specify stored credentials for this computer in the protection group settings, Veeam Agent will process the PostgreSQL database using the specified account.

If you specify single-use credentials for this computer in the protection group settings, Veeam Agent will process the PostgreSQL database using the root user.

To learn more, see Specifying Computers.

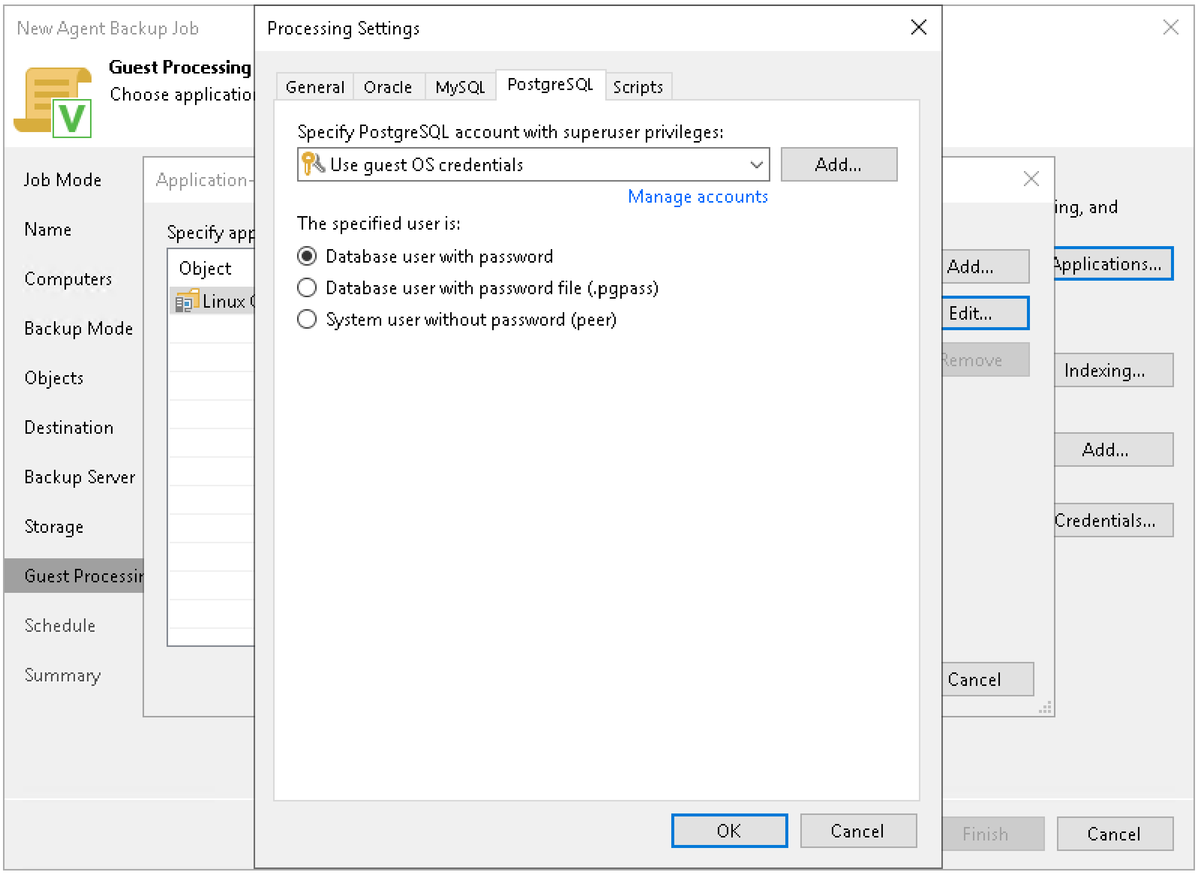
4. In the **The specified user is** field, specify how Veeam Agent will connect to the PostgreSQL database.

The **The specified user is** field is connected closely with the **Specify PostgreSQL account with superuser privileges** list. Veeam Agent will do the following depending on what you specified using these two controls.

Control		Veeam Agent Behavior
Specify PostgreSQL Account with Superuser Privileges	The Specified User Is	
The **Use guest OS credentials** option is selected.	The **Database user with password** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the database user with the same name as the guest OS user.
	The **Database user with password file** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the password file stored in the home directory of the guest OS user.
	The **System user without password** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will use the guest OS user for peer connection to the PostgreSQL database.

Control		Veeam Agent Behavior
Specify PostgreSQL Account with Superuser Privileges	**The Specified User Is**	
The user account is specified.	The **Database user with password** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the database user specified in the **Specify PostgreSQL account with superuser privileges** list.
	The **Database user with password file** option is selected.	• Veeam Agent will apply the guest OS user for processing. • Veeam Agent will connect to the PostgreSQL database using the password file stored in the home directory of the user specified in the **Specify PostgreSQL account with superuser privileges** list.
	The **System user without password** option is selected.	• Veeam Agent will apply the user specified in the **Specify PostgreSQL account with superuser privileges** list. • Veeam Agent will use the selected user for peer connection to the PostgreSQL database.

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.



Processing Settings

Specify PostgreSQL account with superuser privileges: Use guest OS credentials

The specified user is:

● Database user with password

○ Database user with password file (.pgpass)

○ System user without password (peer)

Backup Job and Snapshot Scripts

You can specify custom scripts that will be executed within the backup policy 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 policy 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 policy if 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.

  You can specify only backup policy scripts that will be executed on Linux computers if you selected the **Workstation** computer type at the Job Mode step of the wizard or if you selected the **Backup directly from live file system** option at the Backup Mode step of the wizard.

Specifying Backup Job and Snapshot Scripts

To specify custom scripts for the policy:

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 policy] In the **Processing Settings** window, click the **Scripts** tab.

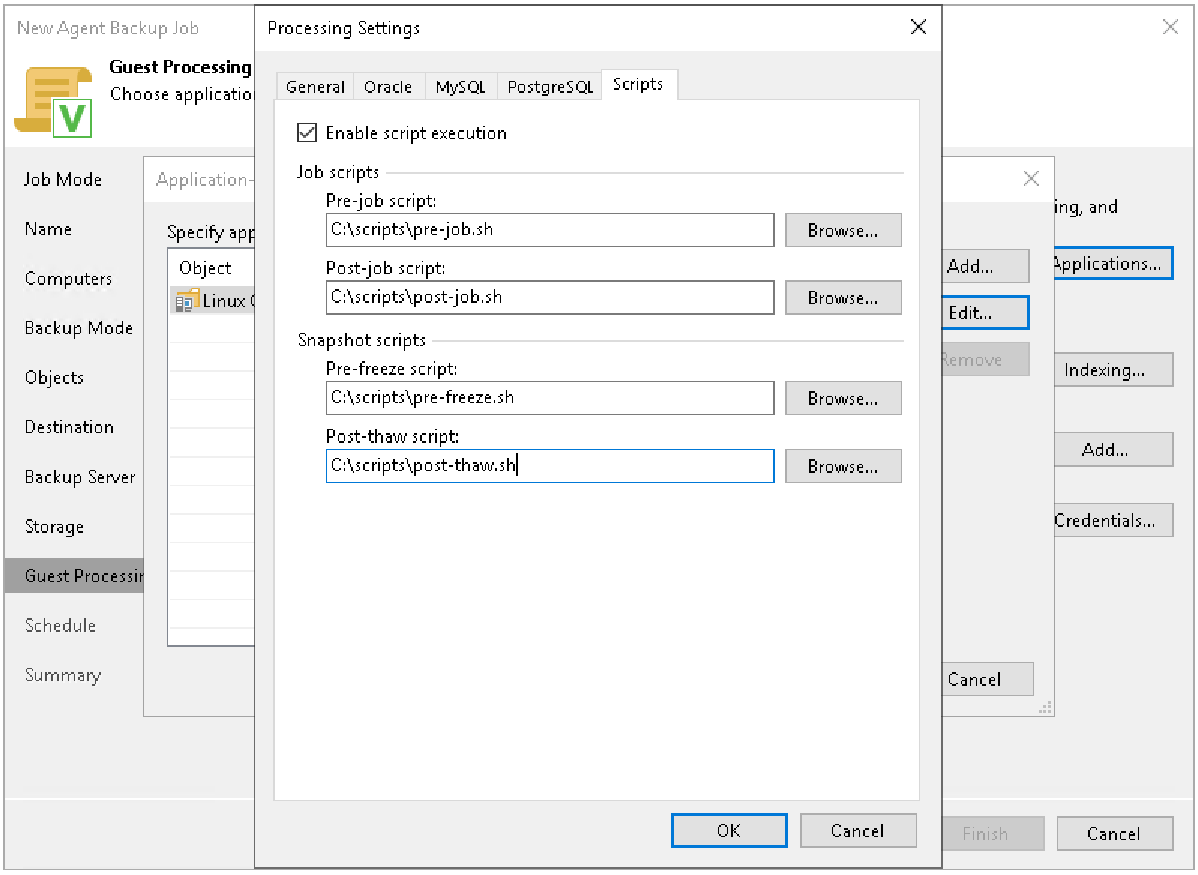
> NOTE
>
> For a file-level backup policy, application-aware processing and database processing options are not available, and no tabs are displayed in the **Processing Settings** window.

5. Select the **Enable script execution** check box.

6. In the **Job scripts** section, specify custom scripts that you want to execute before and after the backup policy 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 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 policy session, Veeam Backup & Replication will upload the scripts to the `/var/lib/veeam/scripts` directory on each Veeam Agent computer added to the backup policy and execute them on these computers.



☑ Enable script execution

Job scripts

Pre-job script: C:\scripts\pre-job.sh

Post-job script: C:\scripts\post-job.sh

Snapshot scripts

Pre-freeze script: C:\scripts\pre-freeze.sh

Post-thaw script: C:\scripts\post-thaw.sh

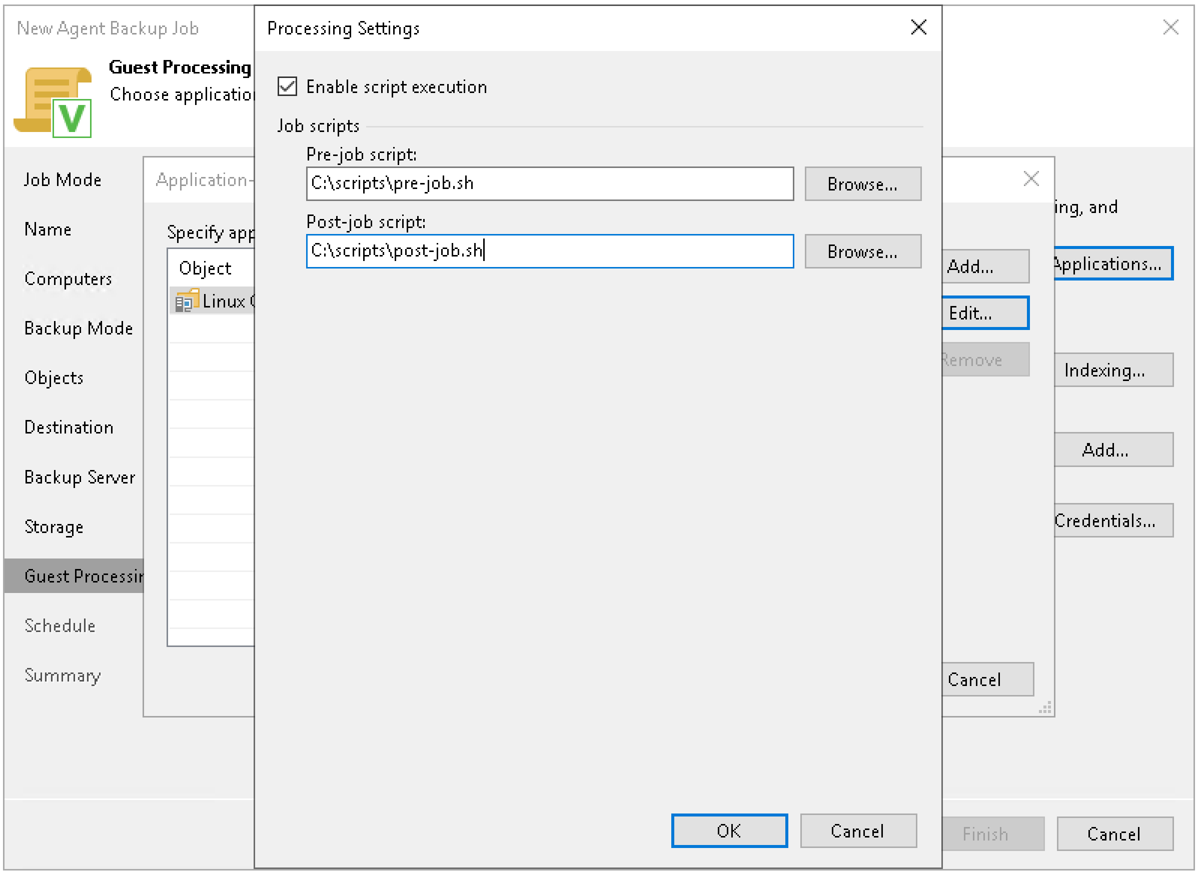
Specifying Backup Job Scripts

To specify custom scripts for the policy:

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 policy session, Veeam Backup & Replication will upload the scripts to the `/var/lib/veeam/scripts` directory on each Veeam Agent computer added to the policy and execute them on these computers.



☑ Enable script execution

Pre-job script: C:\scripts\pre-job.sh

Post-job script: C:\scripts\post-job.sh

File Indexing

You can instruct the Veeam Agent backup policy 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. For more information on file system indexing, see the File System Indexing topic in the Veeam Agent for Linux User Guide.

> **NOTE**
>
> File system indexing is optional. If you do not enable this option in the backup policy settings, you will still be able to perform 1-click restore from the backup created with such backup policy. 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 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 add 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)

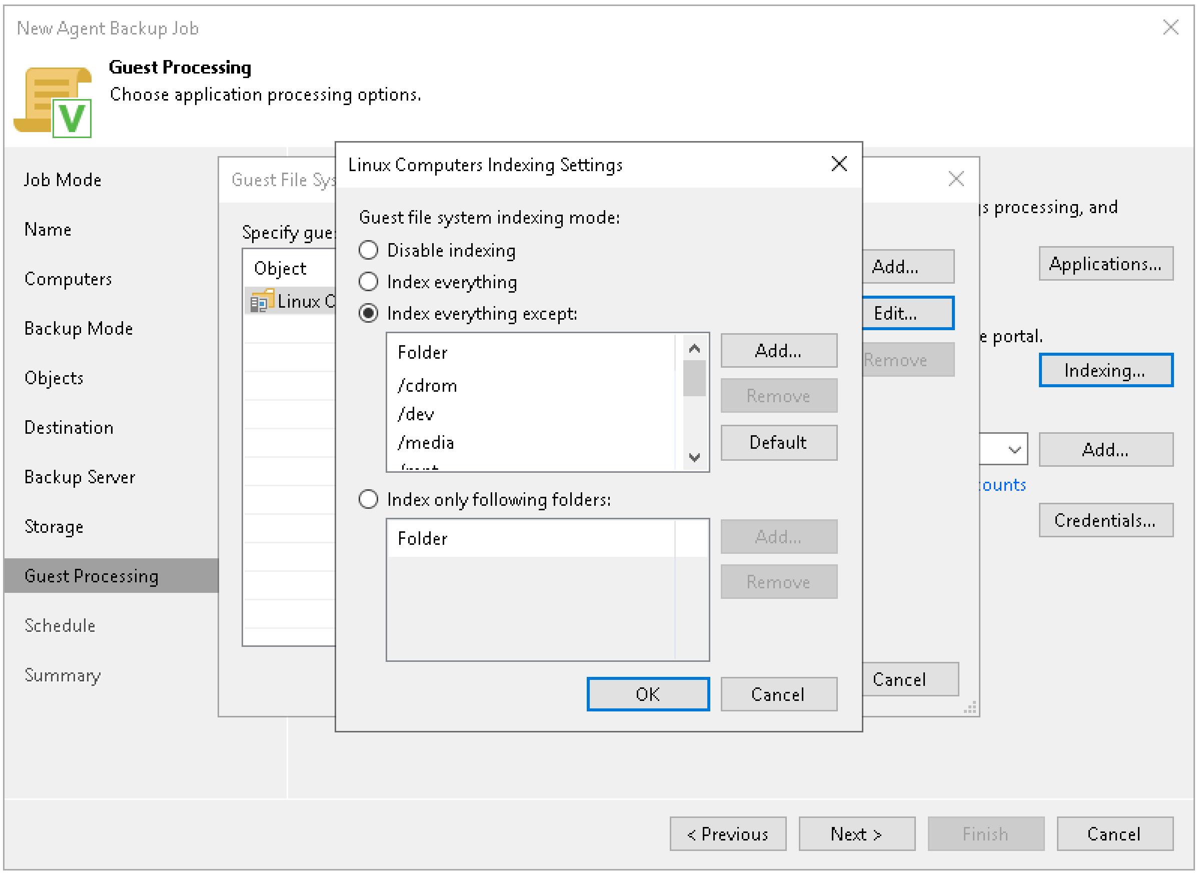
   - [For volume-level backup only] Select **Index everything except** if you want to index all files on your computer OS except those defined in the list. By default, system directories `/cdrom`, `/dev`, `/media`, `/mnt`, `/proc`, `/tmp` and `/lost+found` are excluded from indexing. You can add or delete 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 policy. For a file-level backup policy that processes Linux-based computers, only the **Index everything** option is available.



New Agent Backup Job

Guest Processing

Choose application processing options.

Linux Computers Indexing Settings

Guest file system indexing mode:

○ Disable indexing

○ Index everything

● Index everything except:

Folder
/cdrom
/dev
/media

○ Index only following folders:

Folder

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 Veeam Agent backup policy schedule:

1. Select the **Run the job automatically** check box. If this check box is not selected, you will have to start the backup policy manually to create backup.

   > NOTE
   >
   > Depending on the type of protected computer you selected at the Job Mode step of the wizard, Veeam Backup & Replication provides the following scheduling options for the backup job:
   >
   > - [For Workstation] You can set the backup job to run automatically on specific days of the week or daily.
   > - [For Server] You can configure daily, monthly and periodic schedules for the backup job.

2. Define scheduling settings for the policy:

   - To run the policy 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 policy once a month on specific days, select **Monthly at this time**. Use the fields on the right to configure the necessary schedule.

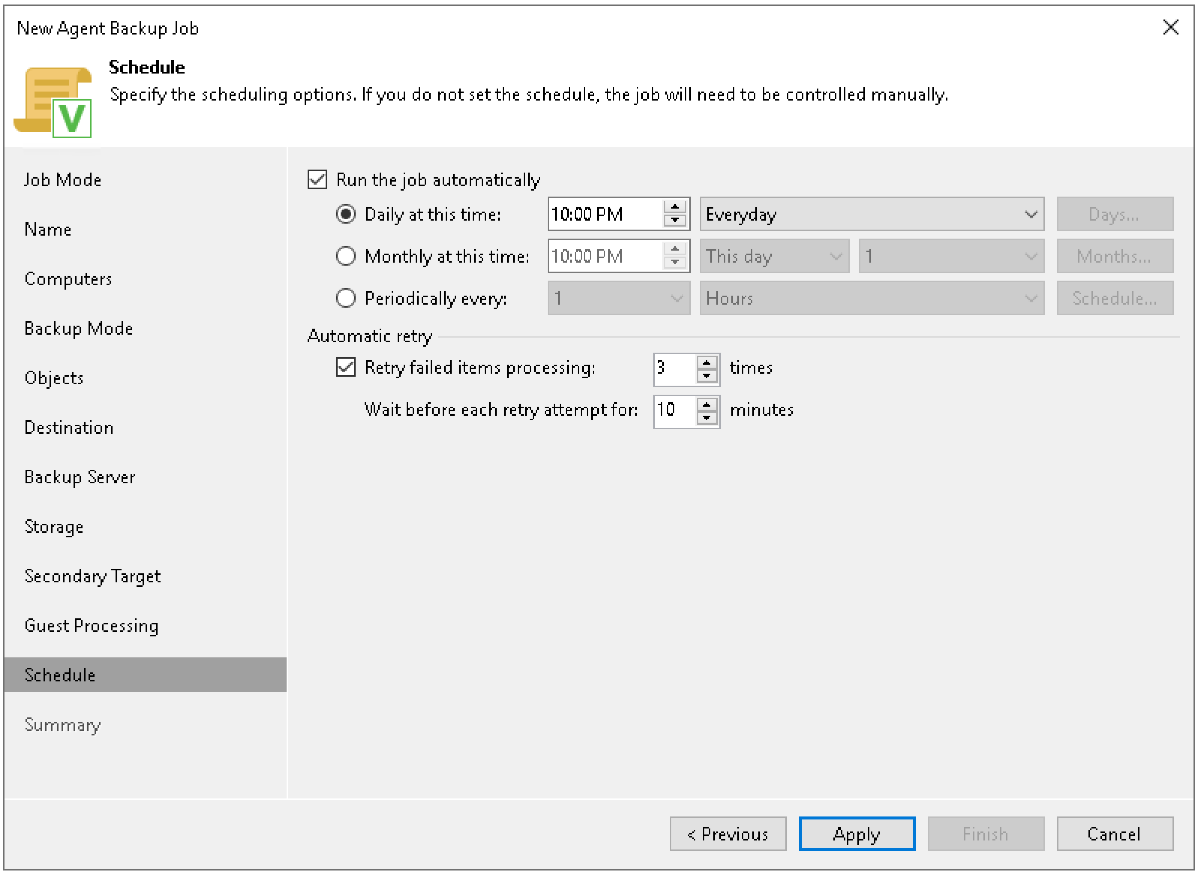
   - To run the policy repeatedly throughout a day with a specific time interval, select **Periodically every**. In the field on the right, select the necessary time unit: *Hours* or *Minutes*.

   - To run the policy continuously, select the **Periodically every** option and choose **Continuously** from the list on the right. A new backup policy session will start as soon as the previous backup policy session finishes.

3. In the **Automatic retry** section, define whether Veeam Agent for Linux must attempt to run the backup policy again if the policy fails for some reason. Enter the number of attempts to run the policy and define time intervals between them. If you select continuous backup, Veeam Agent for Linux will retry the policy for the defined number of times without any time intervals between the policy runs.

NOTE

After you click **Apply** at the **Schedule** step of the wizard, Veeam Backup & Replication will immediately apply the backup policy to protected computers.



New Agent Backup Job

Schedule

Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM This day 1

○ Periodically every: 1 Hours

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

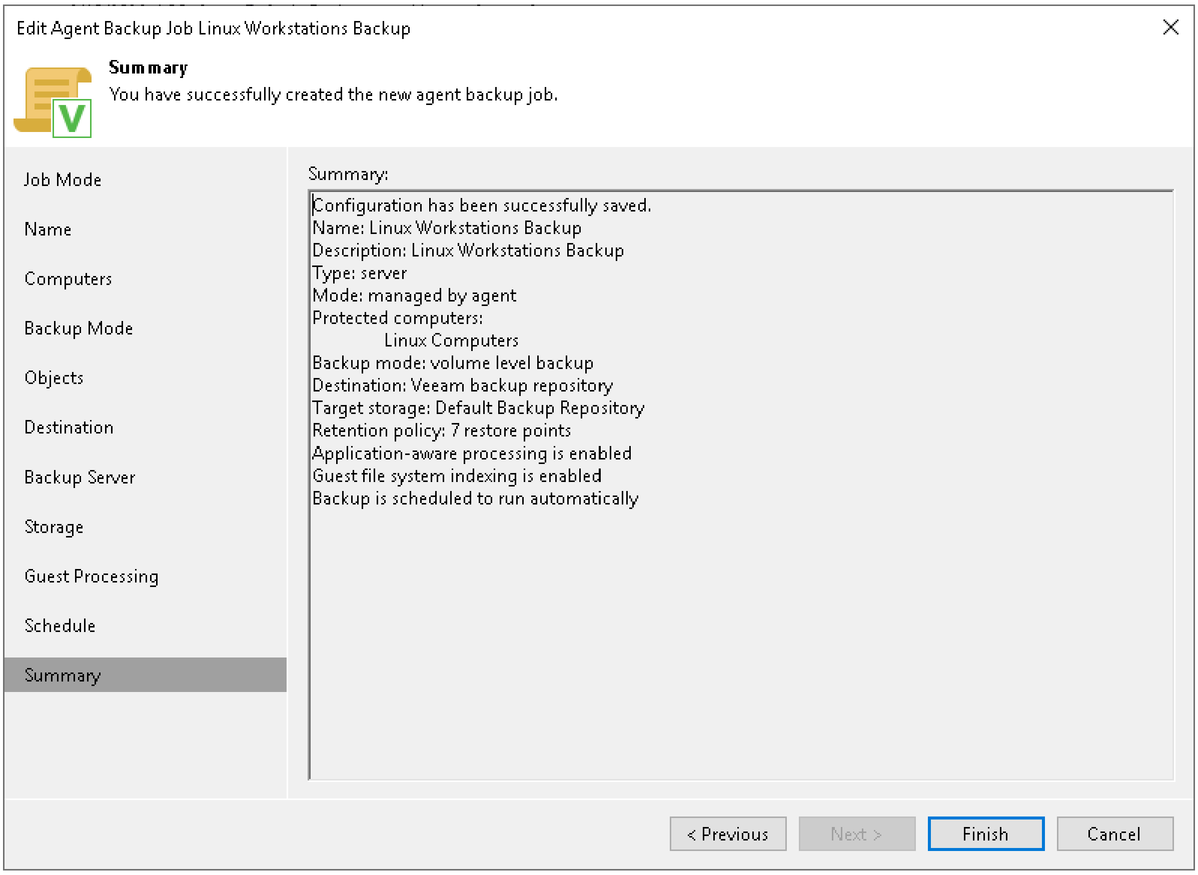
Step 13. Review Backup Job Settings

At the **Summary** step of the wizard, complete the Veeam Agent 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 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 Configuration.



```
Configuration has been successfully saved.
Name: Linux Workstations Backup
Description: Linux Workstations Backup
Type: server
Mode: managed by agent
Protected computers:
            Linux Computers
Backup mode: volume level backup
Destination: Veeam backup repository
Target storage: Default Backup Repository
Retention policy: 7 restore points
Application-aware processing is enabled
Guest file system indexing is enabled
Backup is scheduled to run automatically
```

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 that you plan to add to the Veeam Agent backup policy. To learn more, see Licensing Requirements.
- 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 policy must be of the computers with pre-installed backup agents type.You can also add protection groups of the individual computers and computers from CSV file 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 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 Policy

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 individual computers to the policy later on, when you pass through the wizard steps.

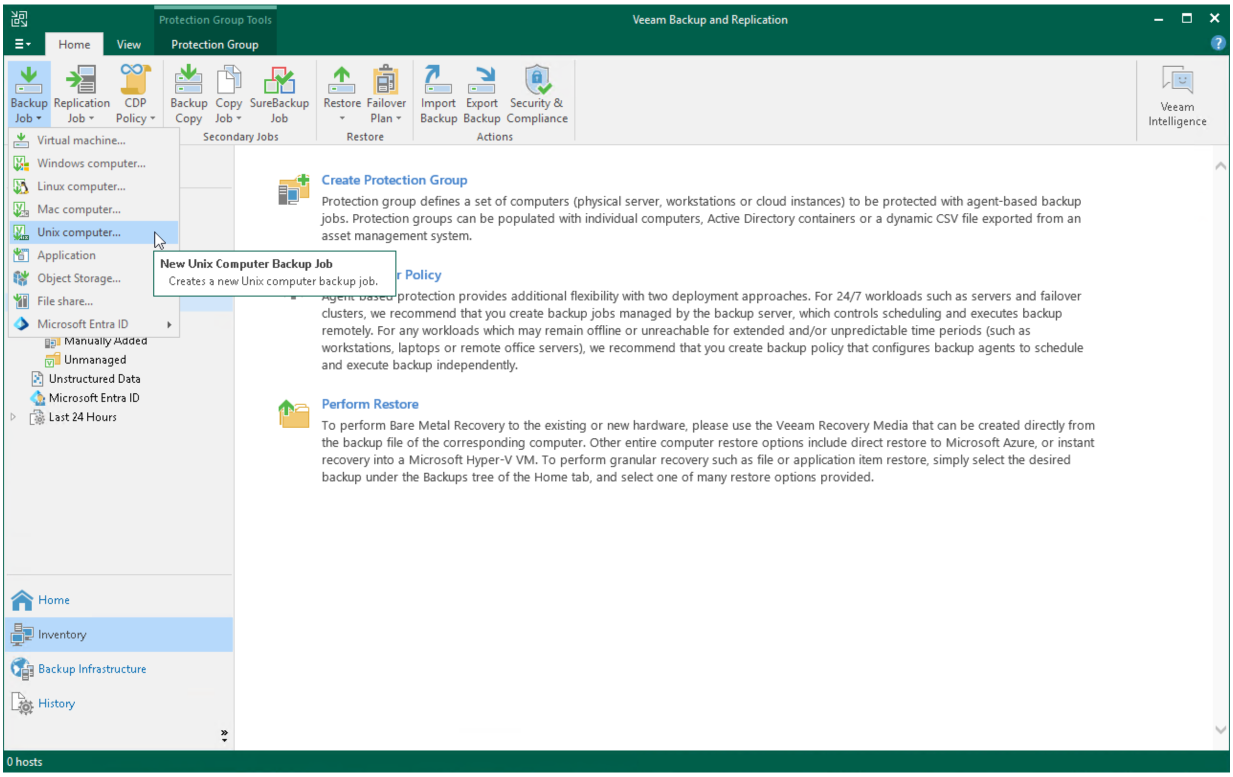
Adding Computers to New Backup Policy

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 protection groups to the policy later on, when you pass through the wizard steps.

> ### TIP
>
> Consider the following:
>
> - You can press and hold the [Ctrl] key 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.



Create Protection Group

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

r Policy

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

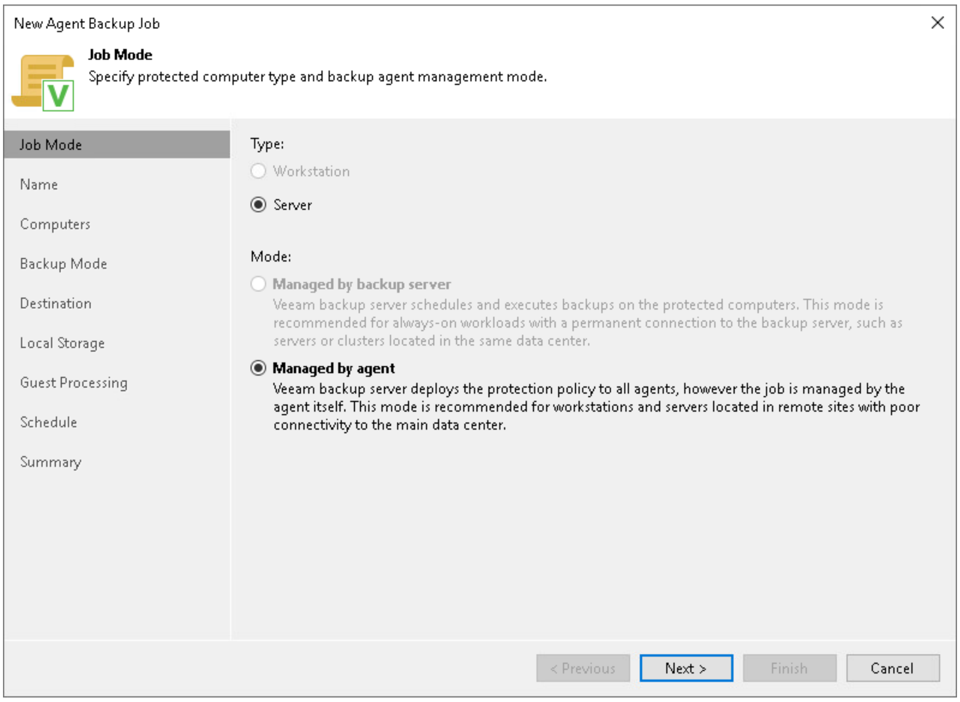
Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

Step 2. 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.



New Agent Backup Job

Job Mode

Specify protected computer type and backup agent management mode.

Type:

○ Workstation

● Server

Mode:

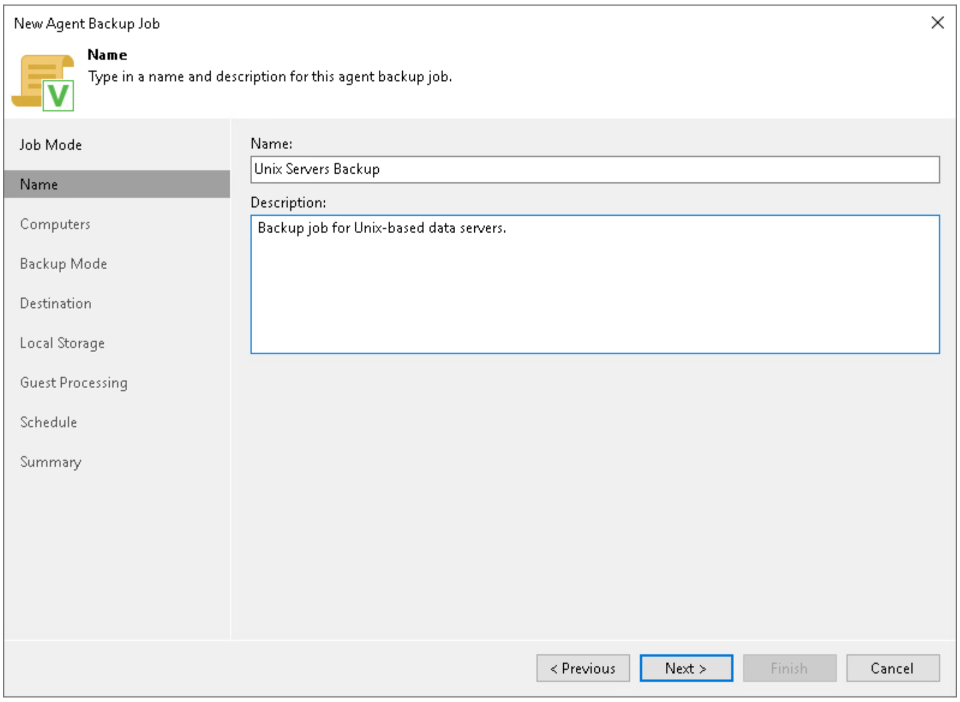
○ **Managed by backup server**
Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

● **Managed by agent**
Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

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.



New Agent Backup Job

Name

Type in a name and description for this agent backup job.

Name: Unix Servers Backup

Description: Backup job for Unix-based data servers.

Step 4. Select Computers to Back Up

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

You can add to the Veeam Agent backup policy one or more protection groups and 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.

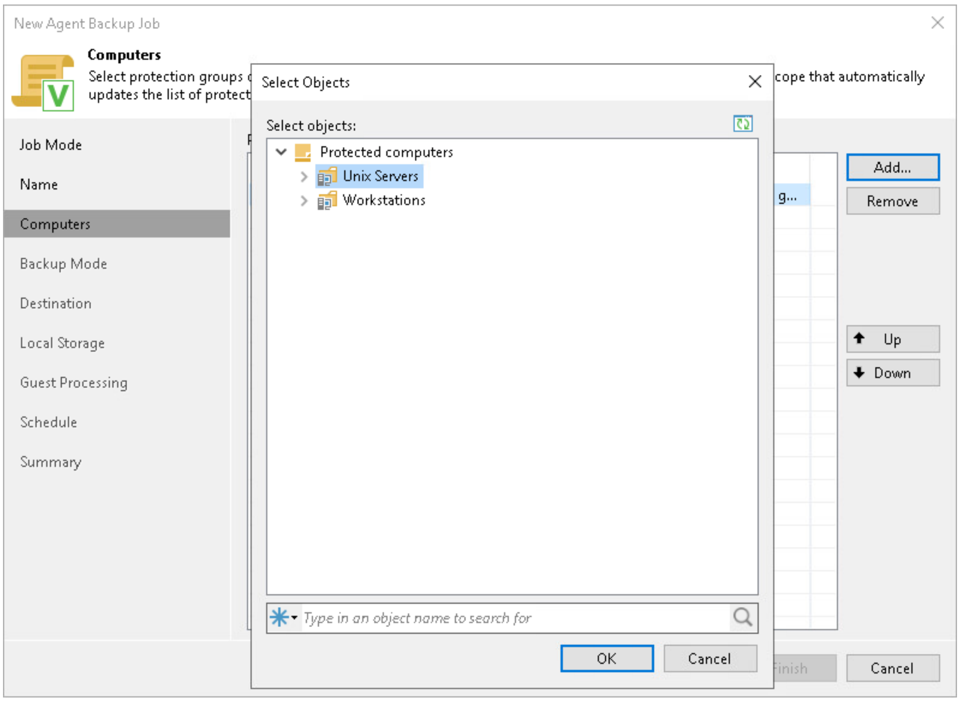
> **NOTE**
>
> If you used the **Add to backup job** > **Unix** > **New job** option to launch the **New Agent Backup Job** wizard, the **Protected computers** list will already contain computers that you have selected to add to the policy. You can remove some computers from the policy or add new computers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

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

1. Click **Add**.
2. In the **Select Objects** window, select one or more protection groups and computers in the list and click **OK**. You can press and hold the [Ctrl] key 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

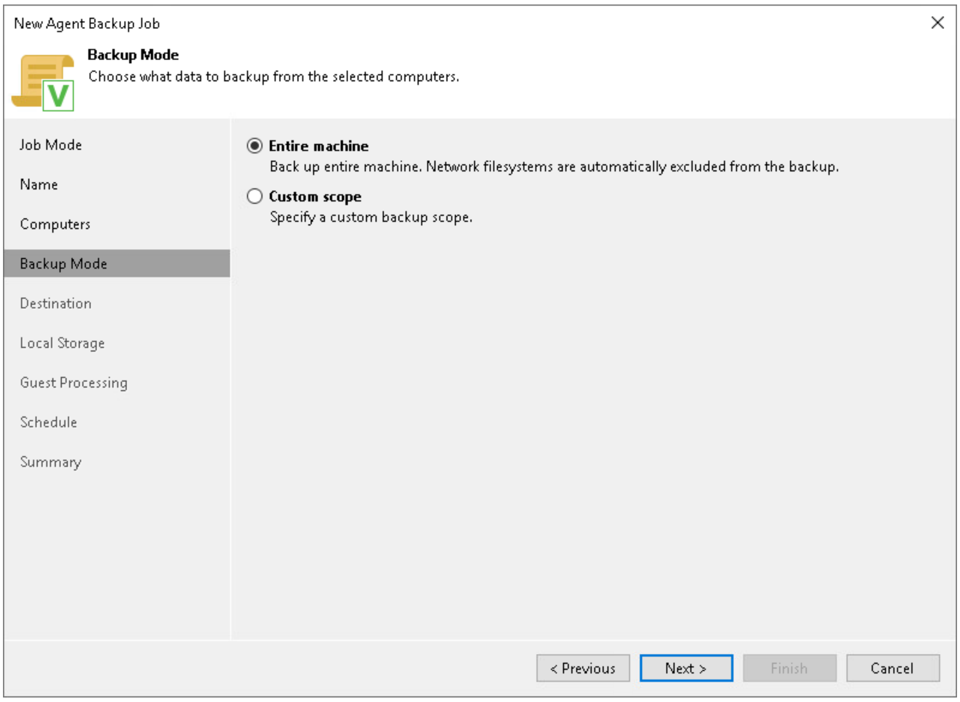
At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup. You can select one of the following options:

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

  Consider 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.



New Agent Backup Job

Backup Mode

Choose what data to backup from the selected computers.

● **Entire machine**
Back up entire machine. Network filesystems are automatically excluded from the backup.

○ **Custom scope**
Specify a custom backup scope.

Step 6. Specify Backup Scope Settings

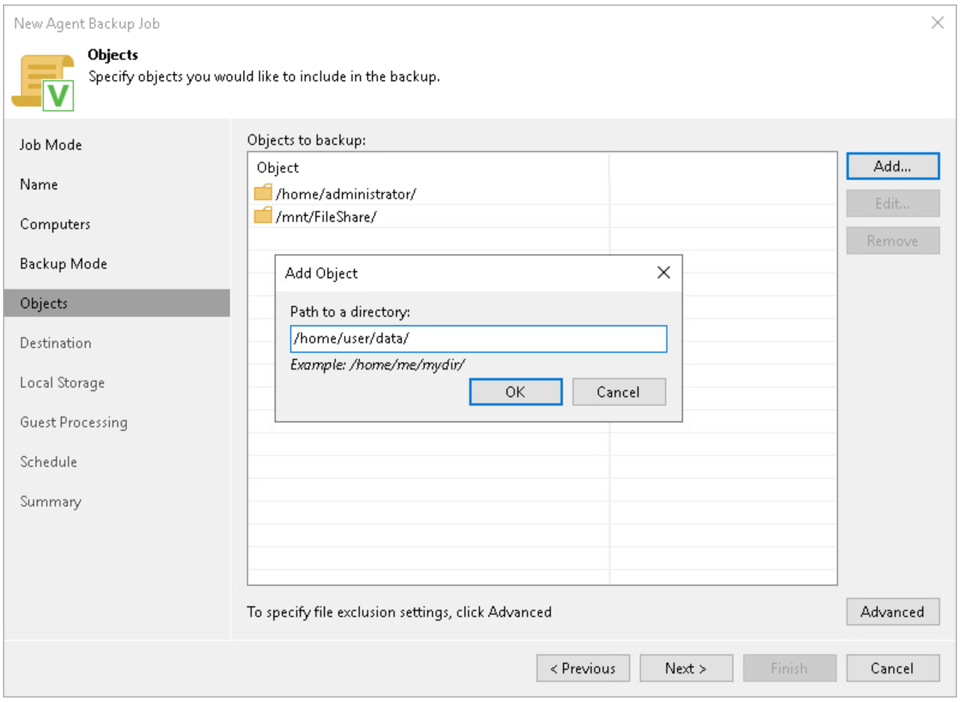
The **Objects** step of the wizard is available if you have chosen the **Custom scope** mode at the Backup Mode step of the wizard.

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`



New Agent Backup Job

Objects

Specify objects you would like to include in the backup.

Objects to backup:

Object
/home/administrator/
/mnt/FileShare/

Add Object

Path to a directory: /home/user/data/

Example: /home/me/mydir/

To specify file exclusion settings, click Advanced

Configuring Filters

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

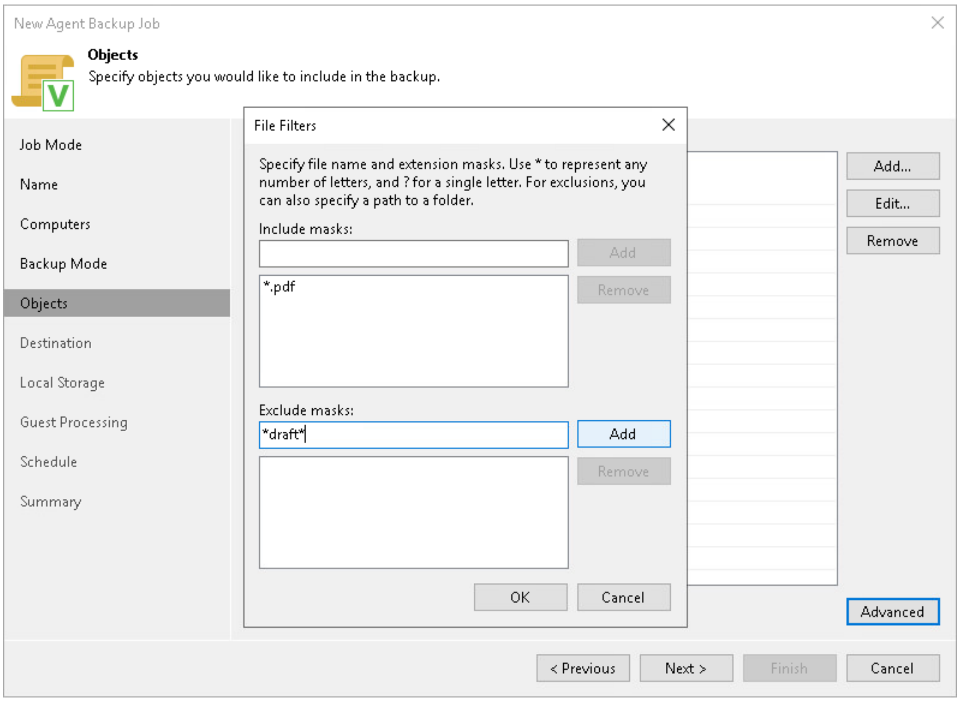
To configure a filter:

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 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 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.



New Agent Backup Job

Objects

Specify objects you would like to include in the backup.

File Filters

Specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify a path to a folder.

Include masks:

*.pdf

Exclude masks: *draft*

Step 7. Select Backup Destination

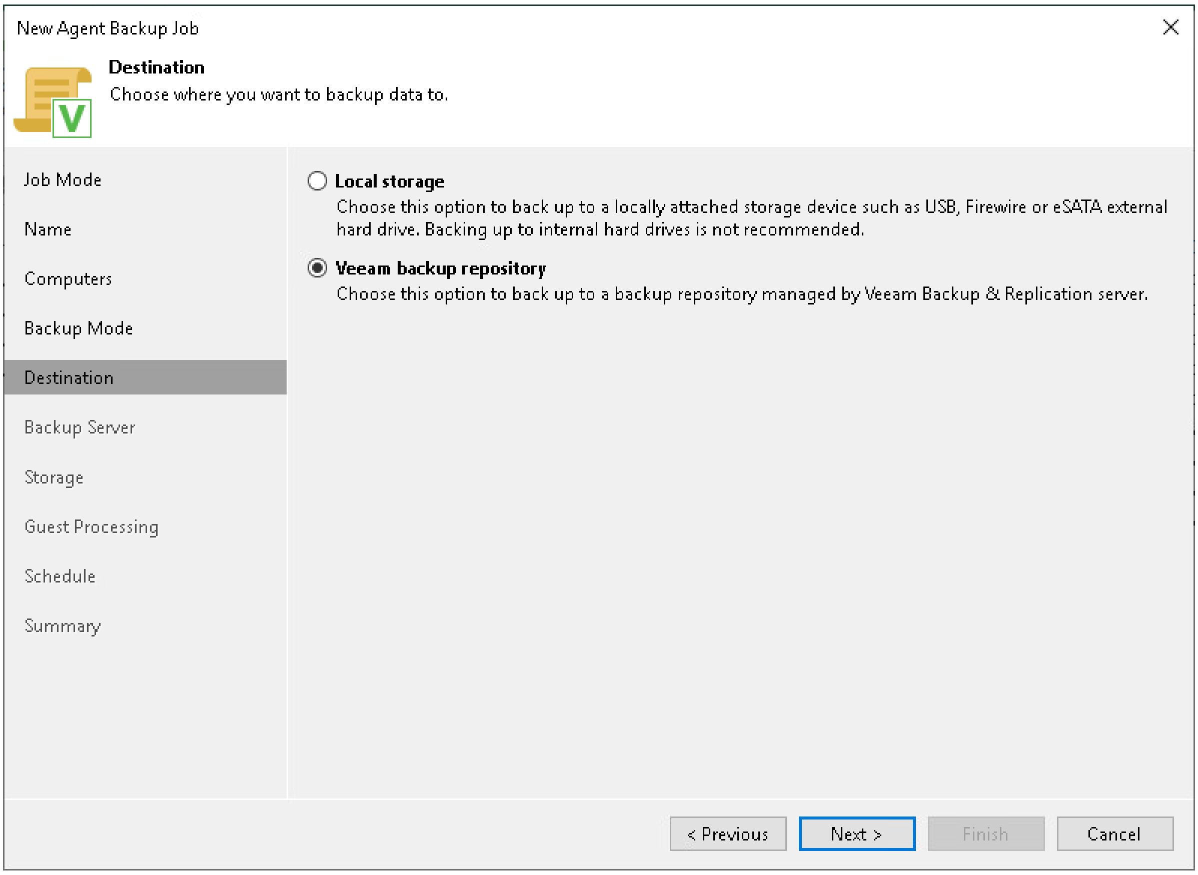
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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 network shared 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 in a backup repository managed by a Veeam backup server. With this option selected, you will pass to the Backup Server step of the wizard.


New Agent Backup Job

Destination
Choose where you want to backup data to.

○ **Local storage**
Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.

● **Veeam backup repository**
Choose this option to back up to a backup repository managed by Veeam Backup & Replication server.

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.

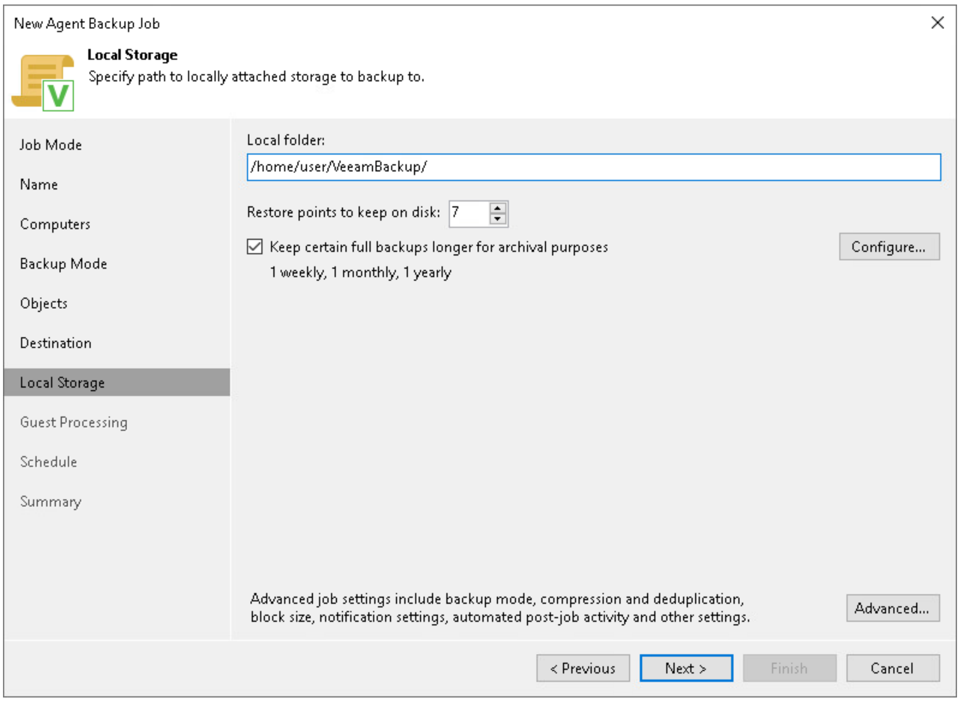
   > **IMPORTANT**
   >
   > USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.

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. To learn more, see Short-Term Retention Policy.

3. You can apply GFS (Grandfather-Father-Son) retention scheme to the backup policy. To specify GFS retention, 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 policy. To learn more, see Specify Advanced Backup Settings.


New Agent Backup Job

Local Storage

Specify path to locally attached storage to backup to.

Local folder: /home/user/VeeamBackup/

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other 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.

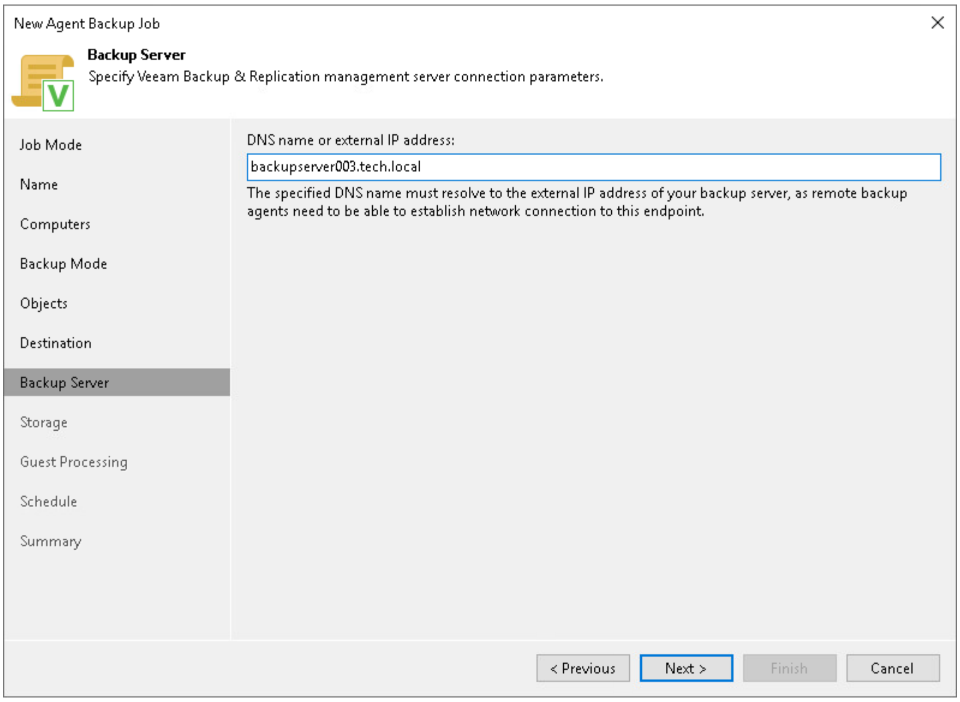
Specifying Backup Server Settings

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**, make sure that the name or IP address of the Veeam backup server, on which you configure the Veeam Agent backup policy, is displayed. Do not specify the name or IP address of another Veeam backup server. The specified DNS name or IP address must be resolvable 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.



DNS name or external IP address:

backupserver003.tech.local

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

Selecting Backup Repository

Specify settings for the target backup repository:

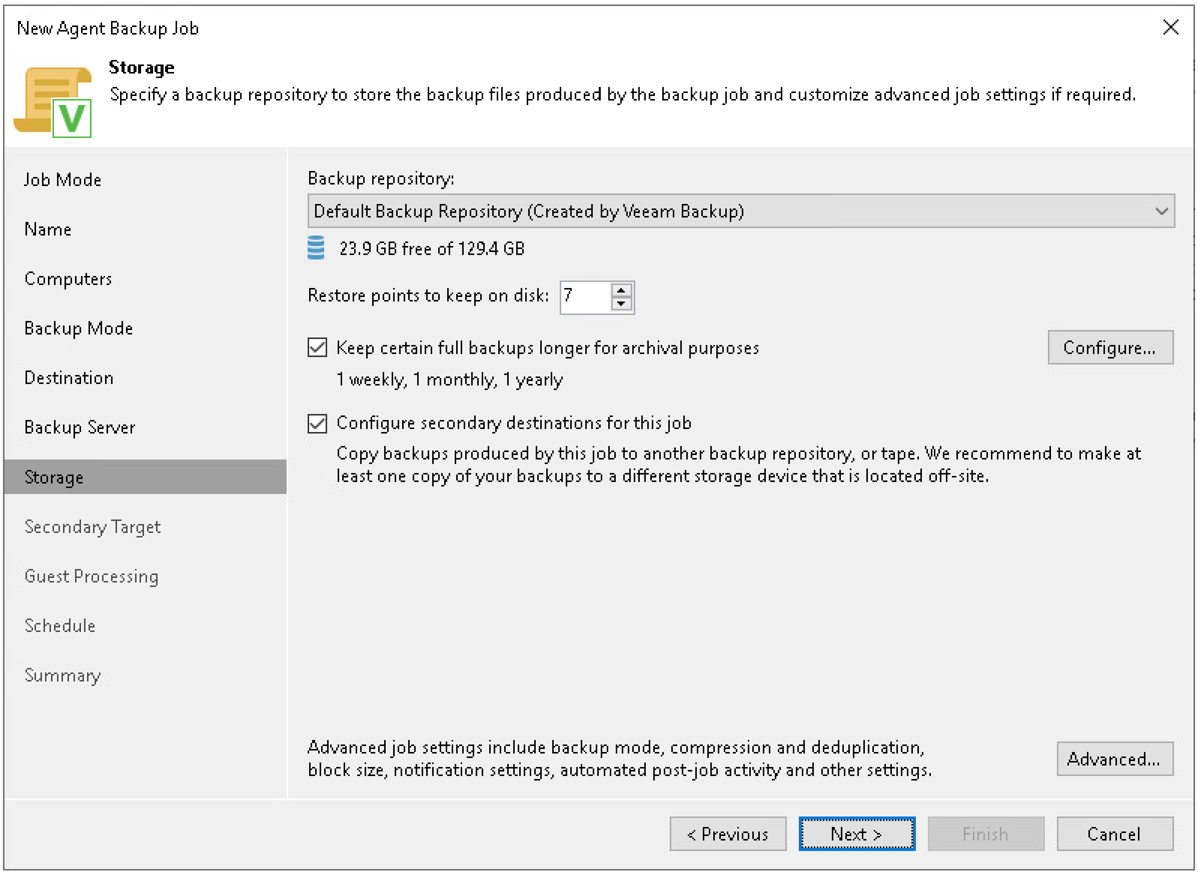
1. From the **Backup repository** list, select a backup repository where you want to store created backups. When you select a backup repository, Veeam Backup & Replication automatically checks how much free space is available on the backup repository.
2. In the **Restore points to keep on disk** field, 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. To learn more, see Short-Term Retention Policy.
3. You can apply GFS (Grandfather-Father-Son) retention scheme to the backup policy. To specify GFS retention, 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 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.

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



Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Default Backup Repository (Created by Veeam Backup)

23.9 GB free of 129.4 GB

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

☑ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other 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.

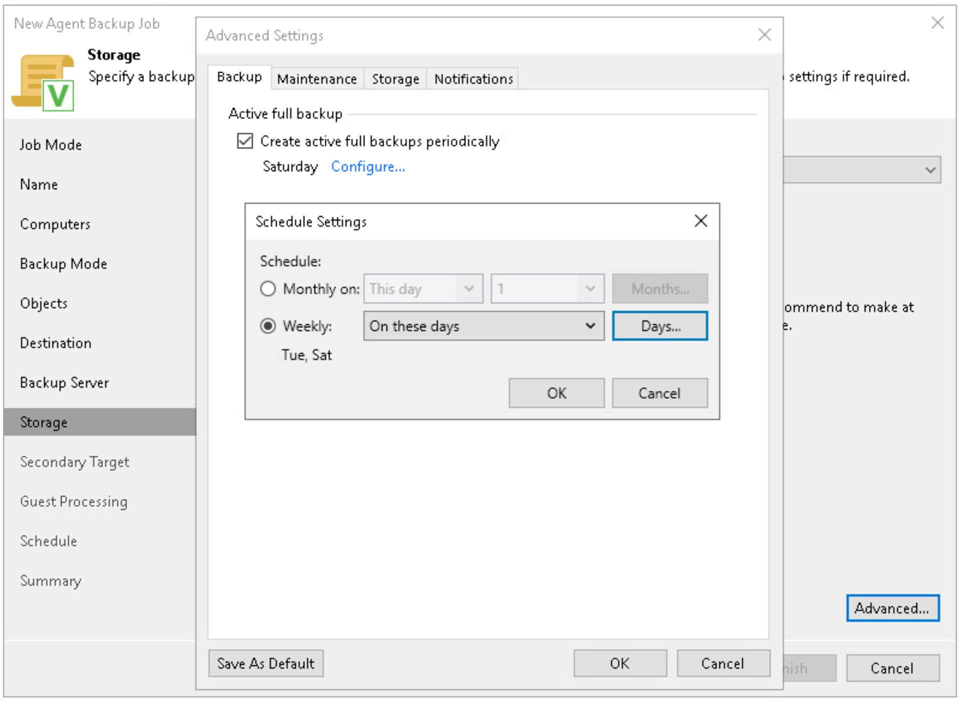
Backup Settings

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.
   - **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.



☑ Create active full backups periodically

Saturday Configure...

○ Monthly on: This day 1

● Weekly: On these days

Tue, Sat

Maintenance Settings

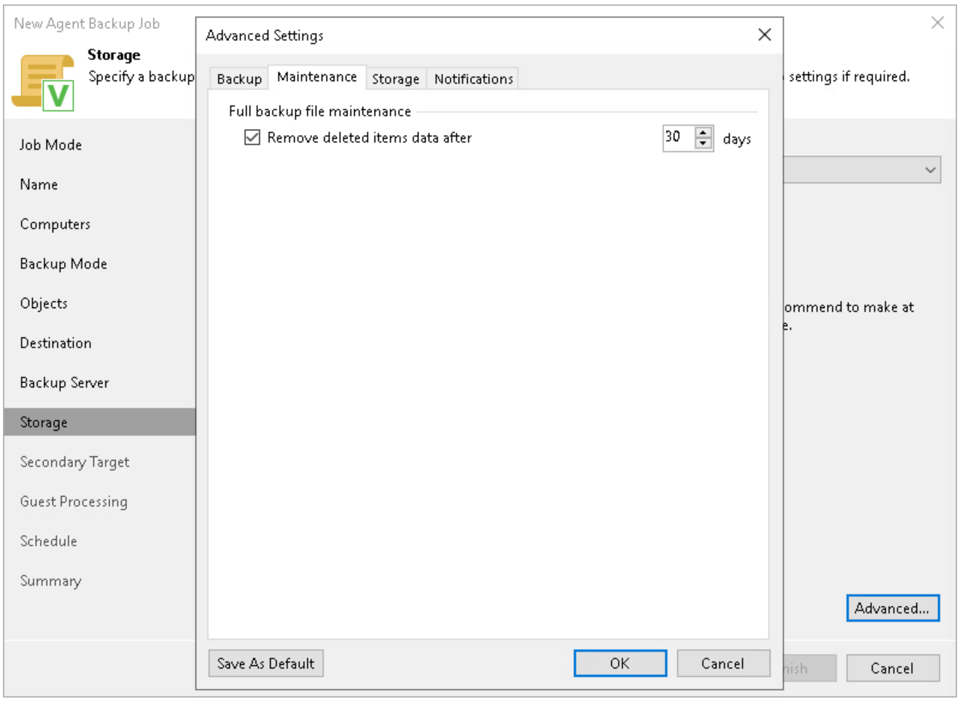
You can specify maintenance settings for a backup policy targeted at a Veeam backup repository. Maintenance operations help make sure that the backup chain remains valid and consistent.

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.



Full backup file maintenance

☑ Remove deleted items data after 30 days

Storage Settings

To specify storage settings for the backup policy:

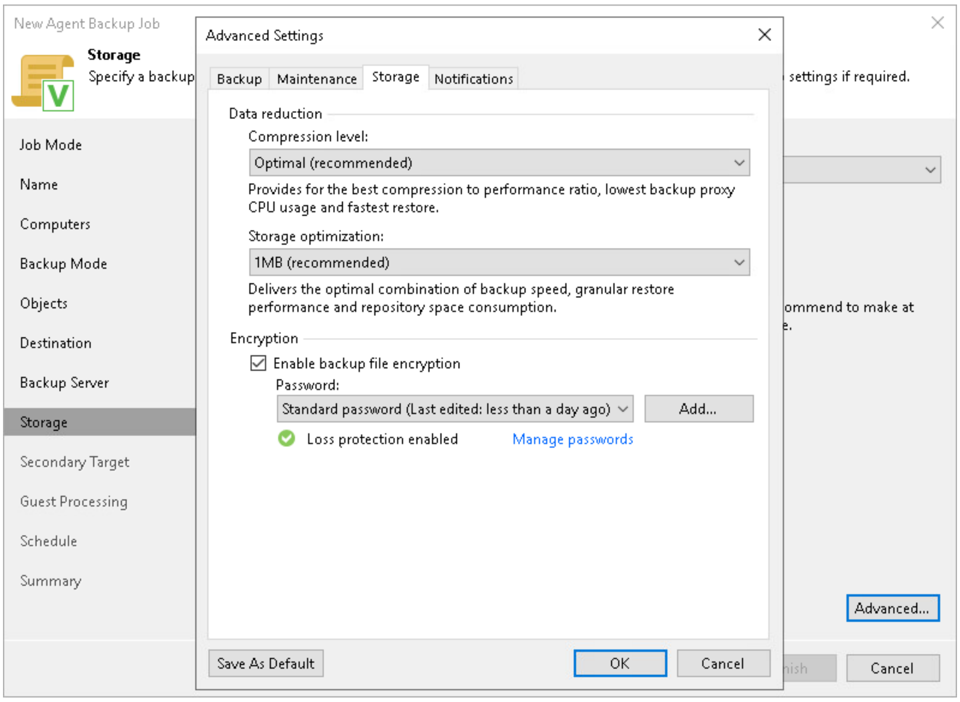
1. Click **Advanced** at one of the following steps of the wizard:
   - **Local Storage** — if you have selected to save backup files on a local storage of a Veeam Agent computer.
   - **Storage** — if you have selected to save backup files in a Veeam backup repository.
2. Click the **Storage** tab.
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.

> NOTE
>
> If you change the storage optimization settings for the backup job, new settings will not have any effect on previously created files in the chain. They will be applied to new files created after the settings were changed.
>
> To apply new storage optimization settings in backup jobs, you must create an active full backup after you change storage optimization settings. Veeam Backup & Replication will use the new block size for the active full backup and subsequent backup files in the backup chain. To learn about the active full backup, see Performing Active Full Backup.

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:
   >
   > - If you plan to encrypt the content of backup files, consider the limitations listed in the Data Encryption Limitations subsection.
   > - You cannot use Key Management System (KMS) keys for data encryption with a Veeam Agent backup policy.



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)

✓ Loss protection enabled

Data Encryption Limitations

If you plan to encrypt the content of backup files, consider the following limitations:

- Data encryption settings for Veeam Agent backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup 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 or disable encryption for an existing Veeam Agent backup 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 policy, Veeam Agent will encrypt the backup chain starting from the next restore point created with this policy.
- 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 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.

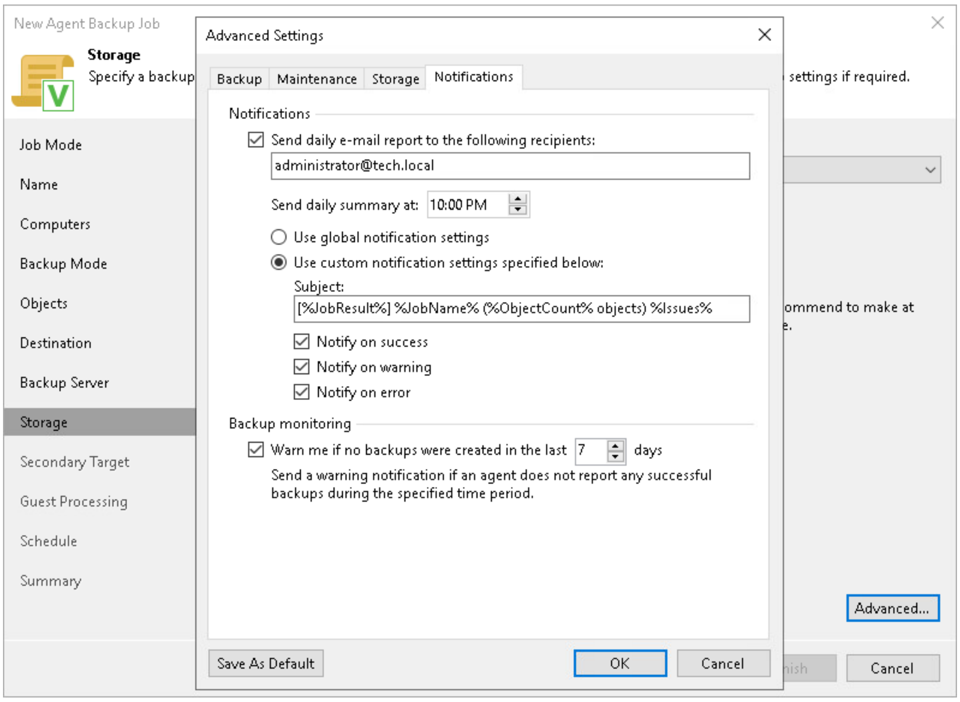
> NOTE
>
> Email reports with backup policy statistics will be sent if you configure global email notification settings in Veeam Backup & Replication. For more information, see the Configuring Global Email Notification Settings section in the Veeam Backup & Replication User Guide.
>
> After you enable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



Notifications

☑ Send daily e-mail report to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

☑ Notify on error

Backup monitoring

☑ Warn me if no backups were created in the last 7 days

Send a warning notification if an agent does not report any successful backups during the specified time period.

Step 10. Specify Secondary Target

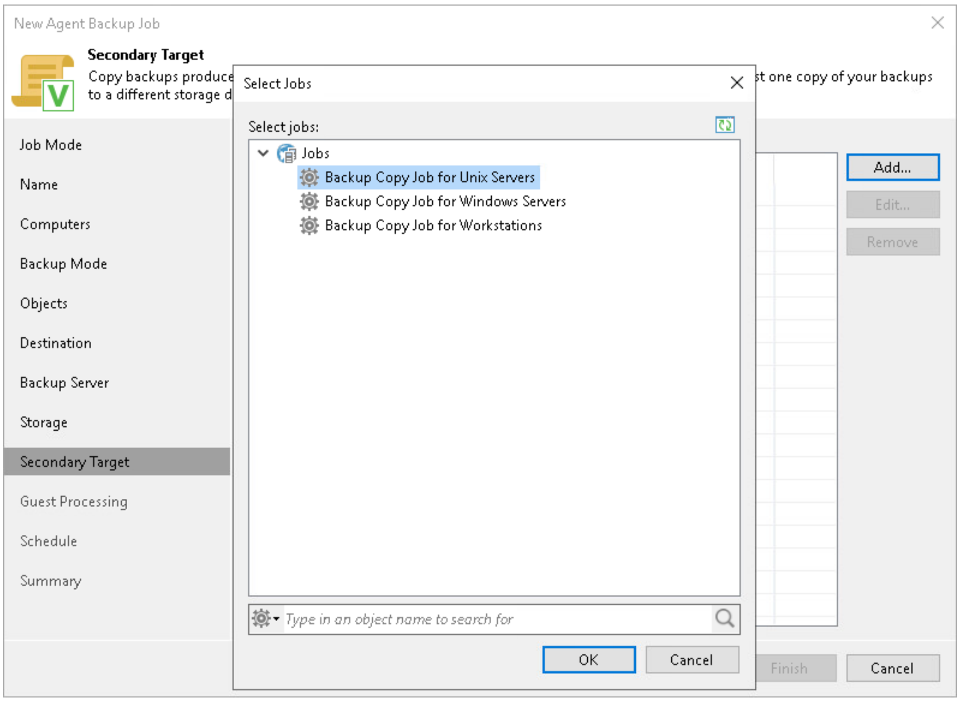
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

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:

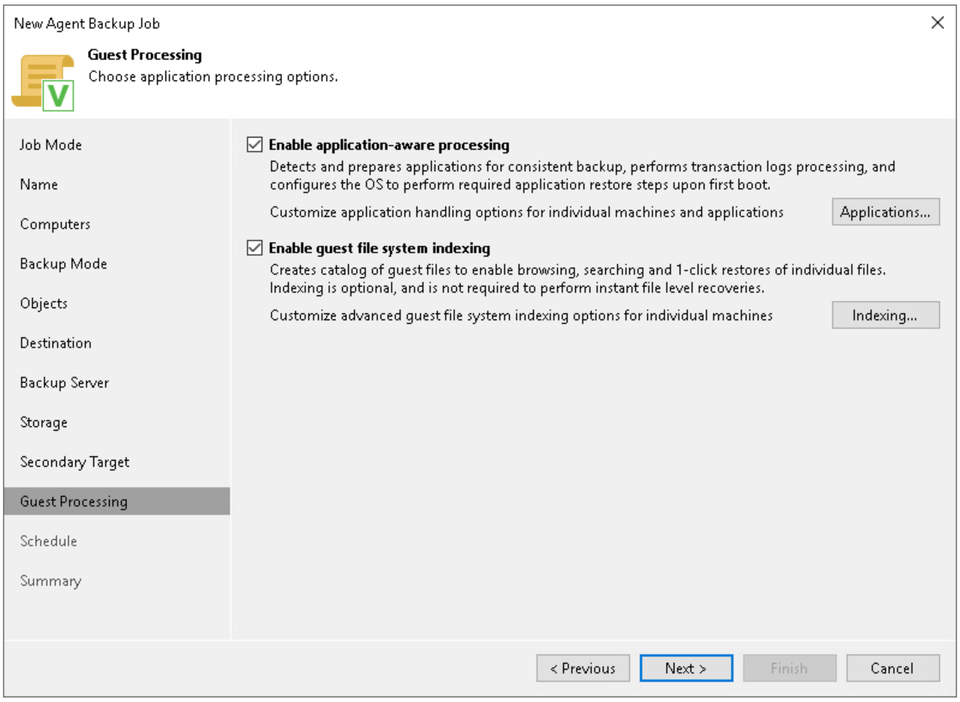
1. Click **Add**.
2. From the jobs list, select a backup to tape or backup copy job that must be linked to the Veeam Agent backup job. You can link several jobs to the backup job, for example, one backup to tape job and one backup copy job. To quickly find the job, use the search field at the bottom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



Step 11. Specify 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 scripts
- File indexing



New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

Backup Job Scripts

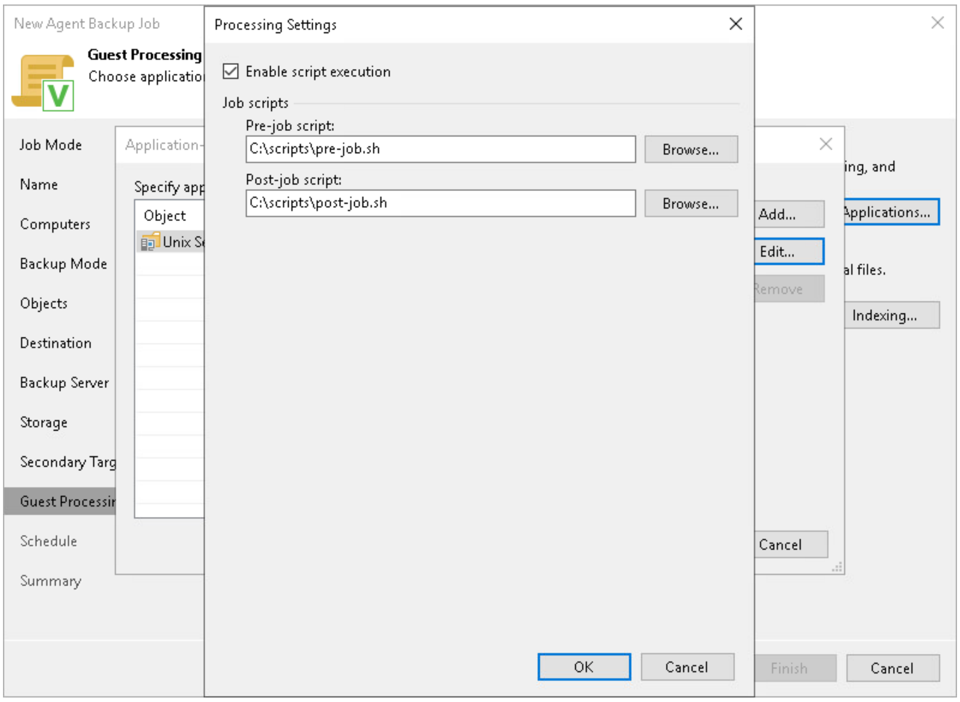
You can specify custom backup job scripts that will be executed within the backup job session on Unix computers. Veeam Agent supports pre-job and post-job scripts that run on the Veeam Agent computer before and after the backup job session. To learn more, see Backup Job Scripts.

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.



Processing Settings

☑ Enable script execution

Job scripts

Pre-job script: C:\scripts\pre-job.sh

Post-job script: C:\scripts\post-job.sh

File Indexing

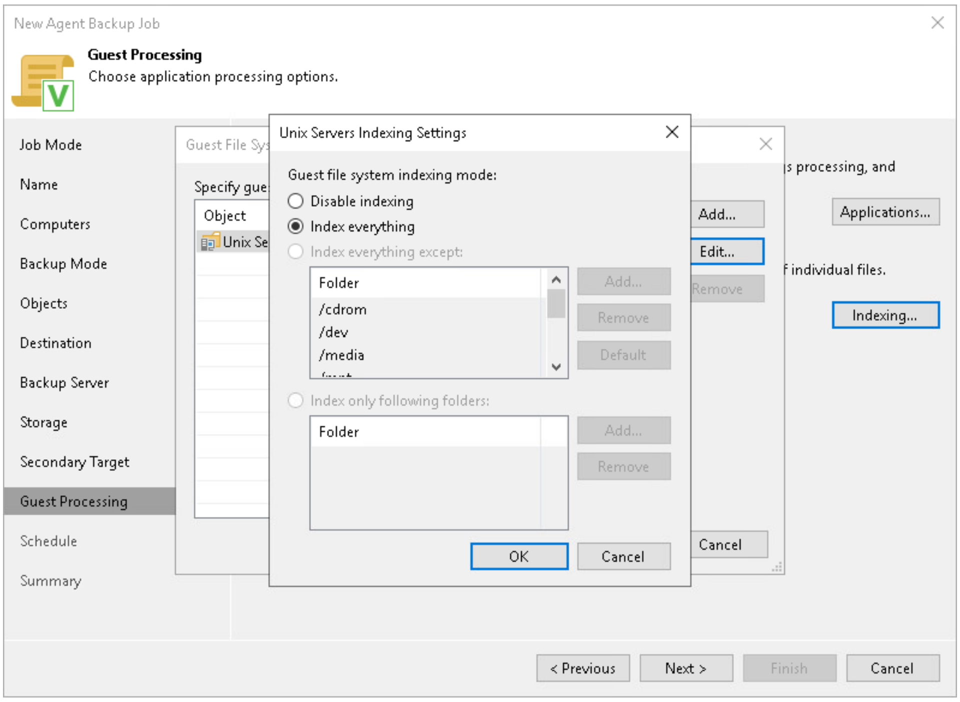
To specify file indexing options:

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 Select Backup Mode 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.



Unix Servers Indexing Settings

Guest file system indexing mode:

○ Disable indexing

● Index everything

○ Index everything except:

Folder
/cdrom
/dev
/media

○ Index only following folders:

Folder

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:

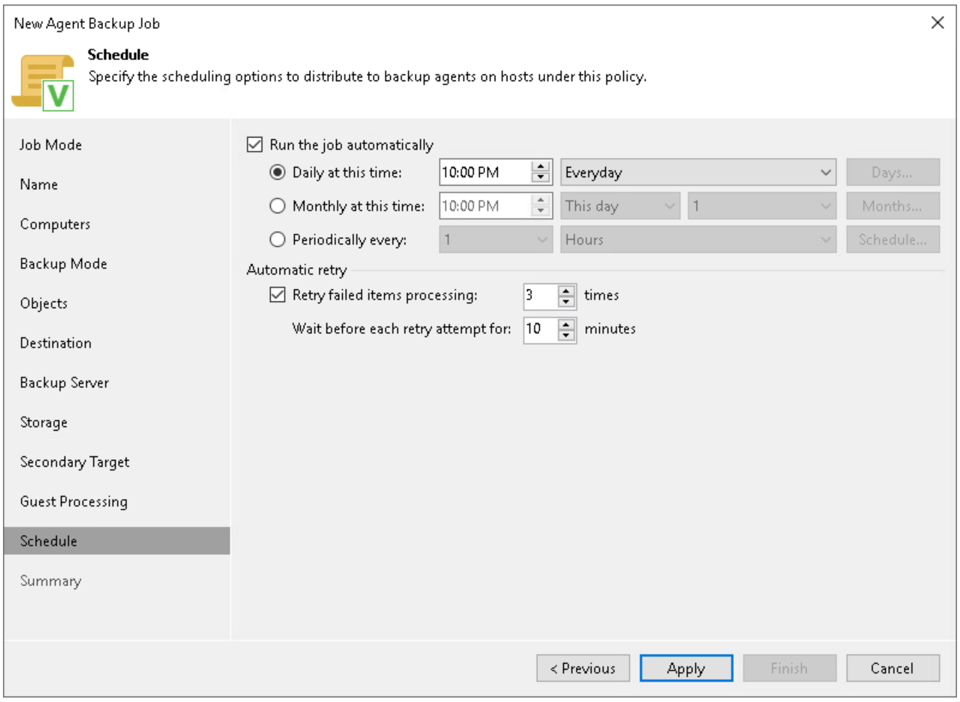
     - The defined interval always starts at 12:00 AM. For example, if you configure to run a job with a 4-hour interval, the job will start at 12:00 AM, 4:00 AM, 8:00 AM, 12:00 PM, 4:00 PM and so on.

     - 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.



New Agent Backup Job

Schedule

Specify the scheduling options to distribute to backup agents on hosts under this policy.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM This day 1

○ Periodically every: 1 Hours

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

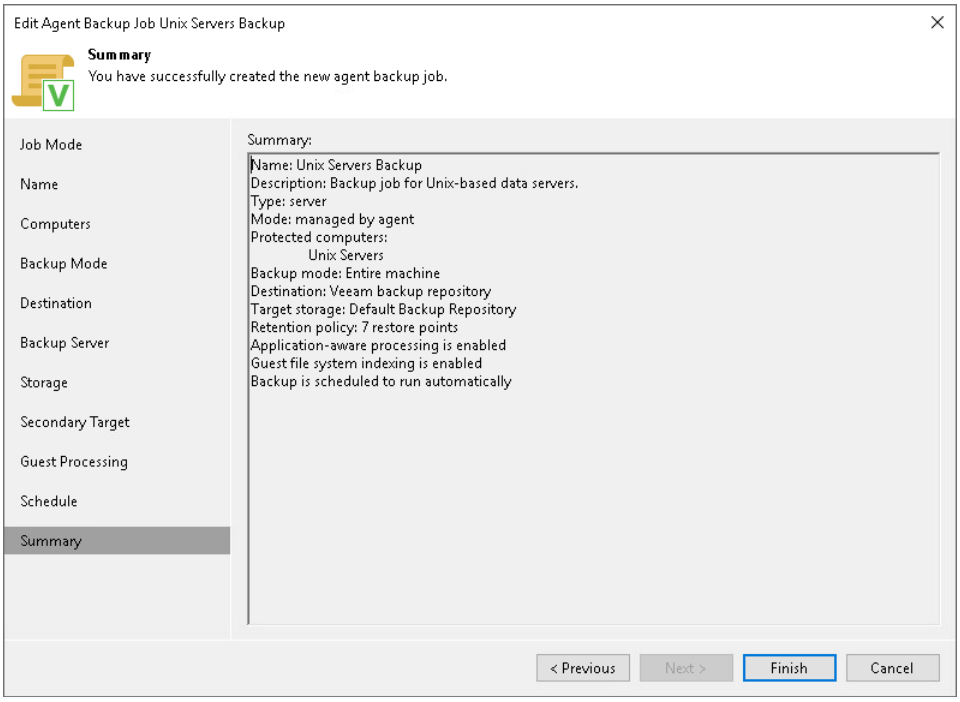
Step 13. Review Backup Job Settings

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 Configuration.



```
Name: Unix Servers Backup
Description: Backup job for Unix-based data servers.
Type: server
Mode: managed by agent
Protected computers:
            Unix Servers
Backup mode: Entire machine
Destination: Veeam backup repository
Target storage: Default Backup Repository
Retention policy: 7 restore points
Application-aware processing is enabled
Guest file system indexing is enabled
Backup is scheduled to run automatically
```

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 workstations that you plan to add to the Veeam Agent backup policy. To learn more, see Licensing Requirements.
- 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 computers with pre-installed backup 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.

Consider the following about Veeam Agent backup policies:

- 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.
- Veeam Agent backup policy may fail unexpectedly due to restrictions applied on the Veeam Agent computer side. For more information, see Backup Job Restrictions in the Veeam Agent for Mac User Guide.

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 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 Policy

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 individual computers to the policy later on, when you pass through the wizard steps.

Adding Computers to New Backup Policy

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

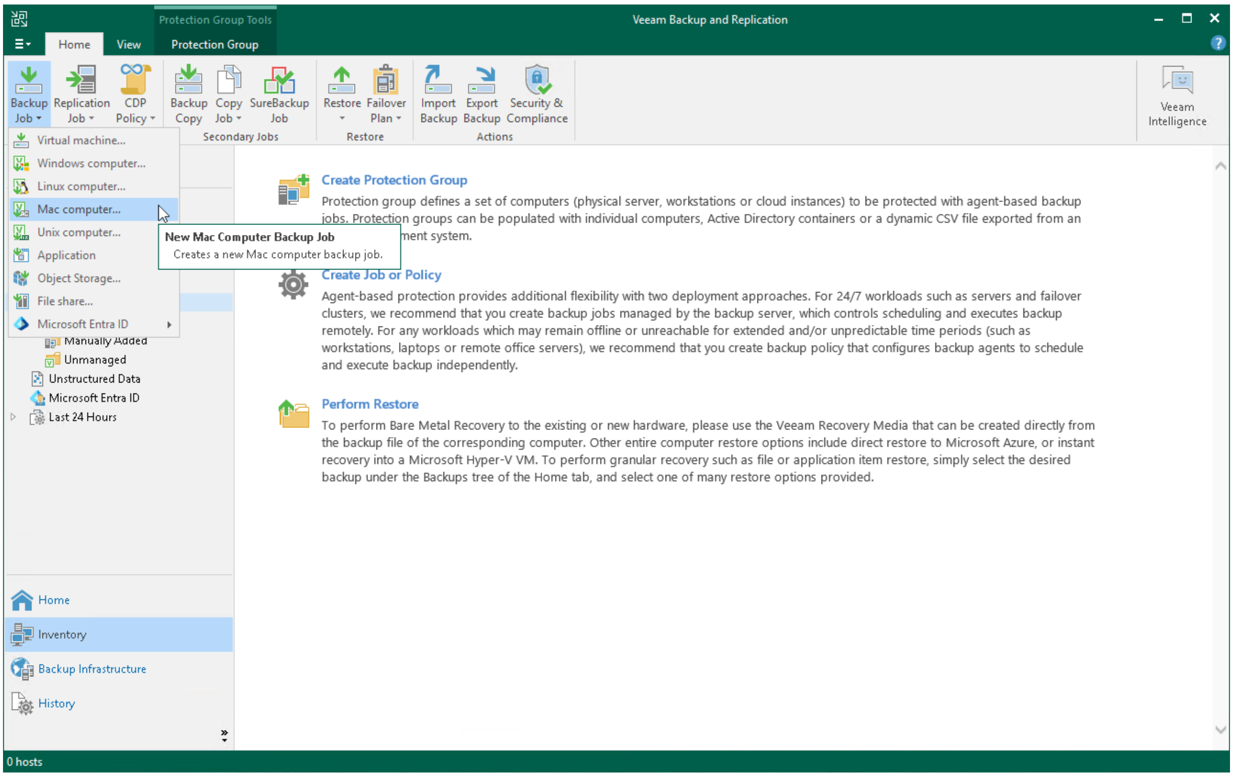
- Open the **Inventory** view. In the **Physical Infrastructure** node, click the protection group whose computers you want to add to the backup policy. In the working area, select one or more computers that you want to add to the policy, right-click the selected computer and select **Add to backup job** > **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 protection groups to the policy later on, when you pass through the wizard steps.

TIP

Consider the following:

- You can press and hold the [Ctrl] key 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.



New Mac Computer Backup Job

Creates a new Mac computer backup job.

Create Protection Group

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

Create Job or Policy

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

Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

Step 2. 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:

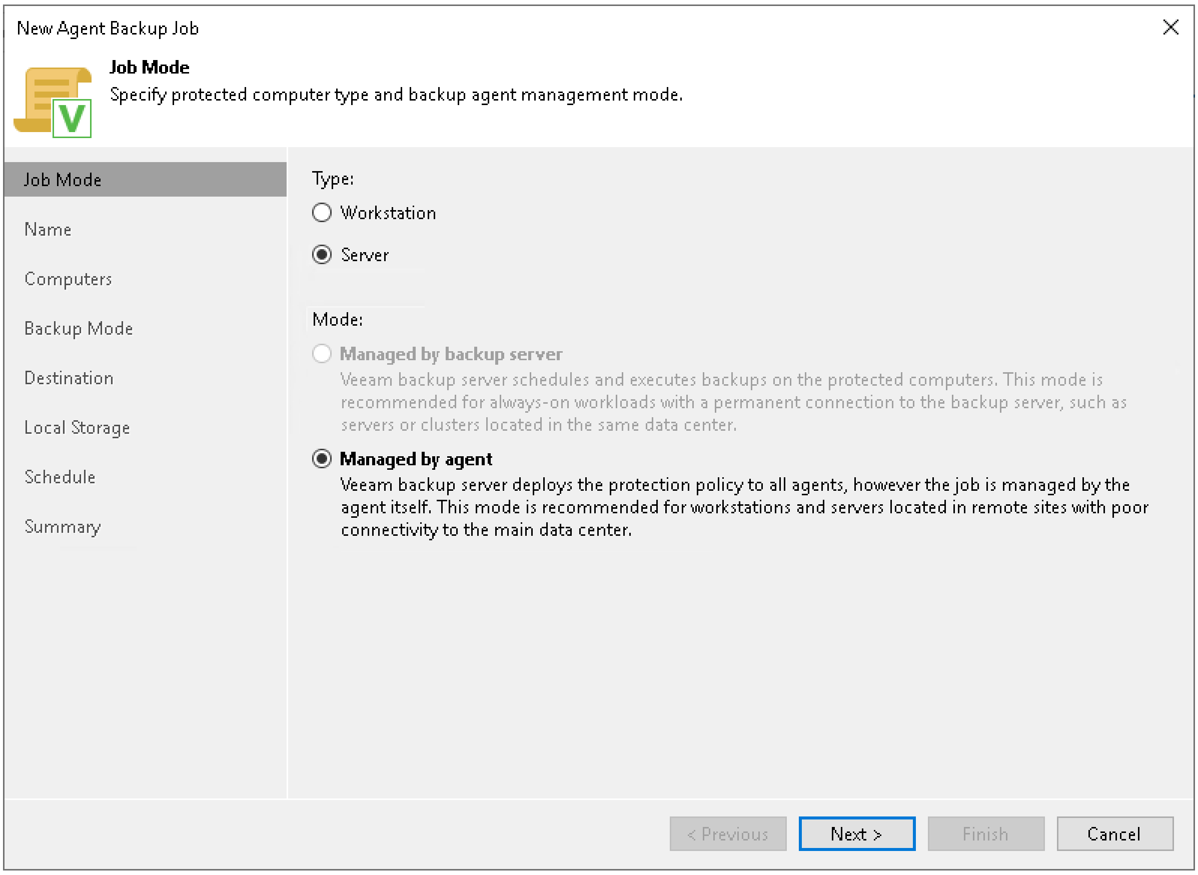
- **Workstation** — select this option if you want to back up data on macOS workstations or laptops. This option is suitable for computers that reside in a remote location and may have limited connection to the backup server.

  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 on 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.



Type:

○ Workstation

● Server

Mode:

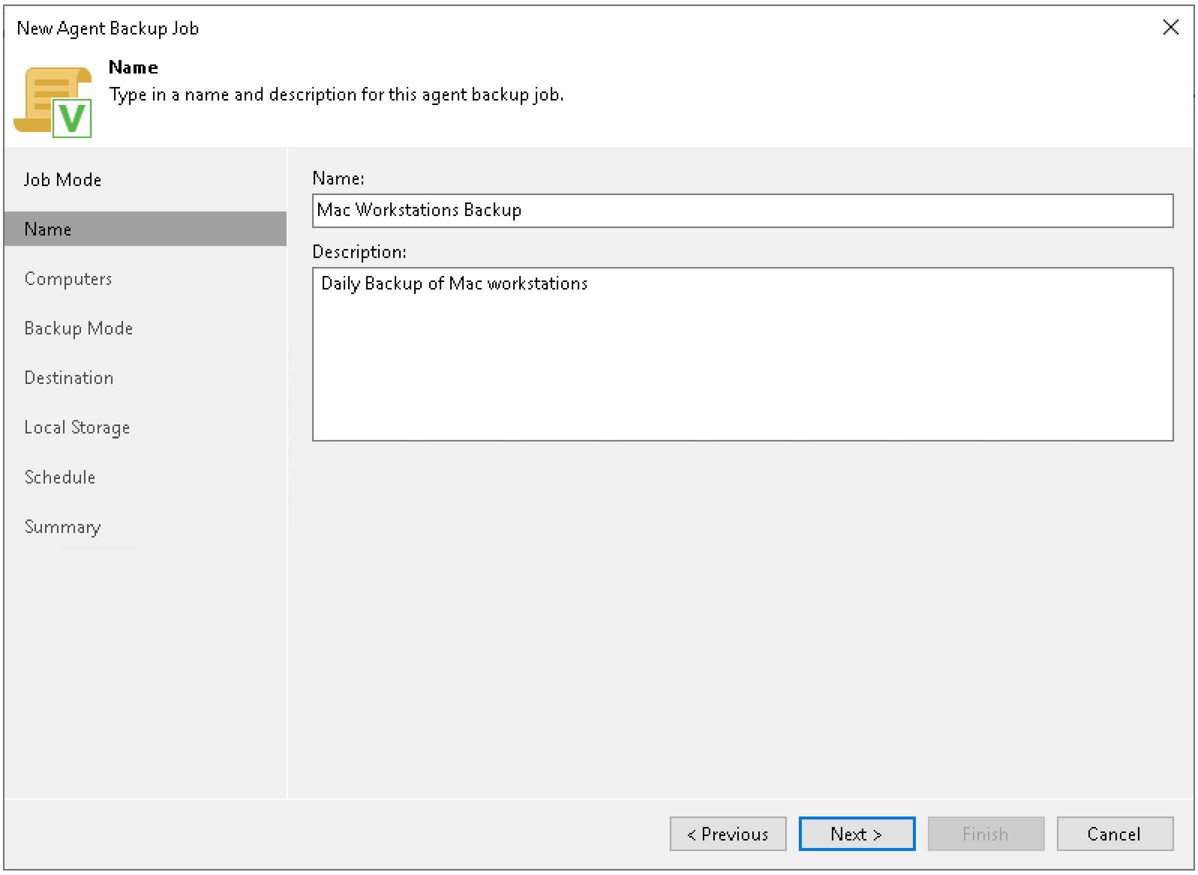
○ **Managed by backup server**
Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

● **Managed by agent**
Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

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.



Name: Mac Workstations Backup

Description: Daily Backup of Mac workstations

Step 4. Select Computers to Back Up

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

You can add to the Veeam Agent backup policy one or more protection groups and 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.

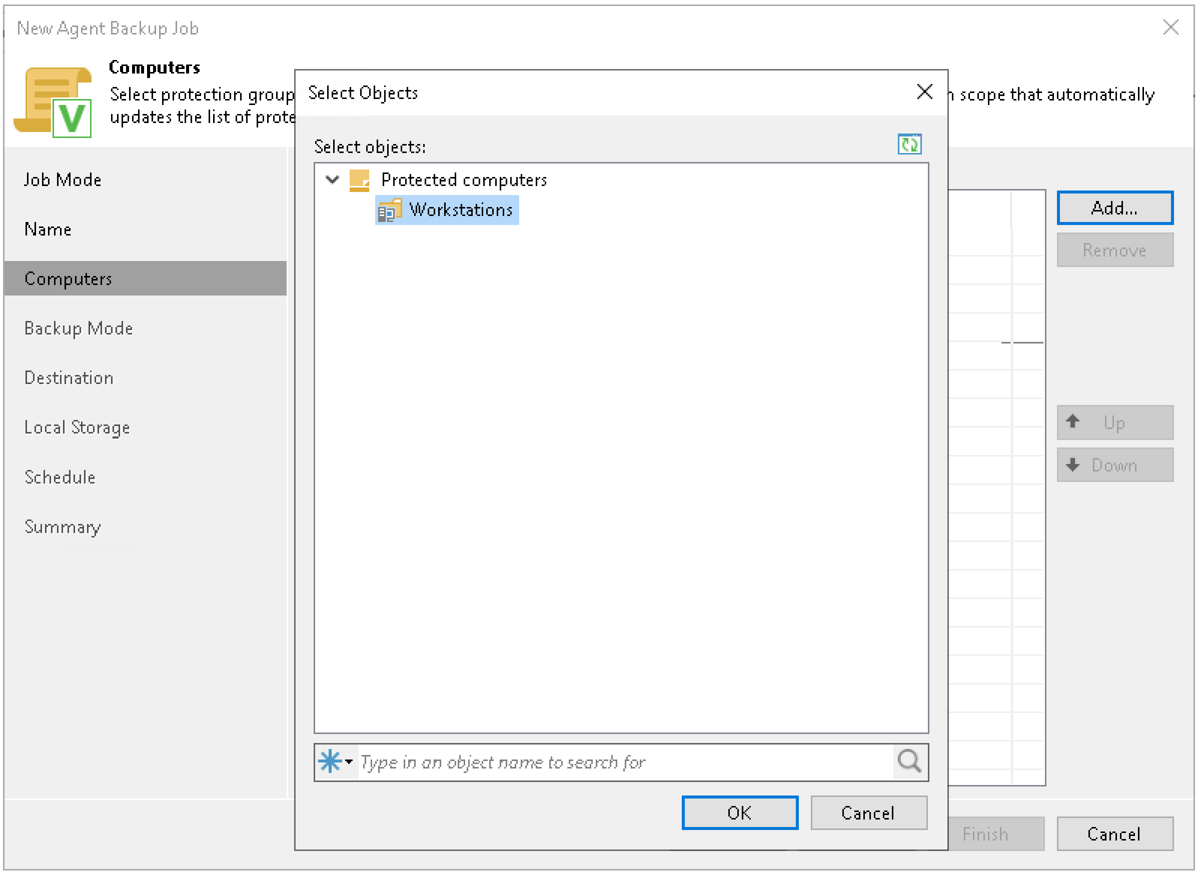
> NOTE
>
> If you used the **Add to backup job** > **Mac** > **New job** option to launch the **New Agent Backup Job** wizard, the **Protected computers** list will already contain computers that you have selected to add to the policy. You can remove some computers from the policy or add new computers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

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

1. Click **Add**.
2. In the **Select Objects** window, select one or more protection groups and computers in the list and click **OK**. You can press and hold the [Ctrl] key 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

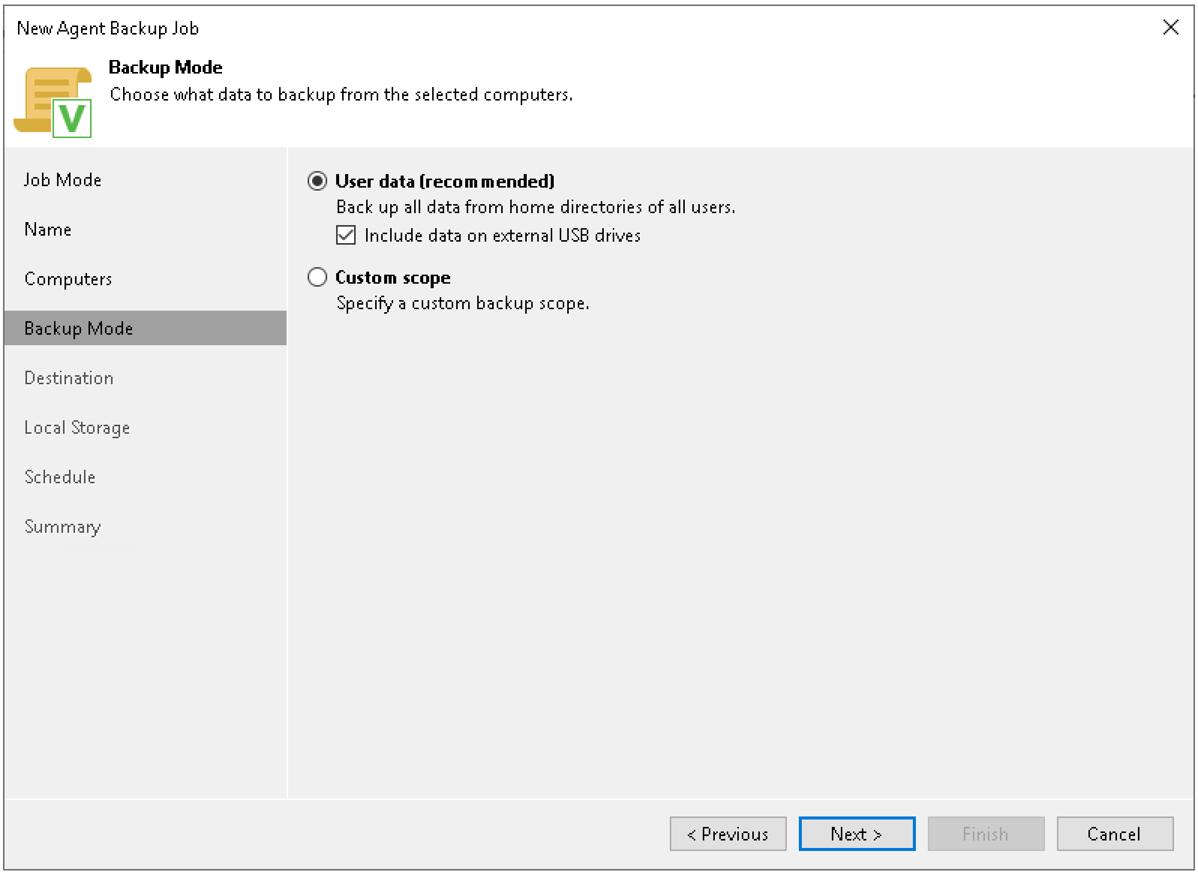
At the **Backup Mode** step of the wizard, select the mode in which you want to create a backup. You can select one of the following options:

- **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.



New Agent Backup Job

Backup Mode
Choose what data to backup from the selected computers.

● **User data (recommended)**
Back up all data from home directories of all users.
☑ Include data on external USB drives

○ **Custom scope**
Specify a custom backup scope.

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 Data 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:

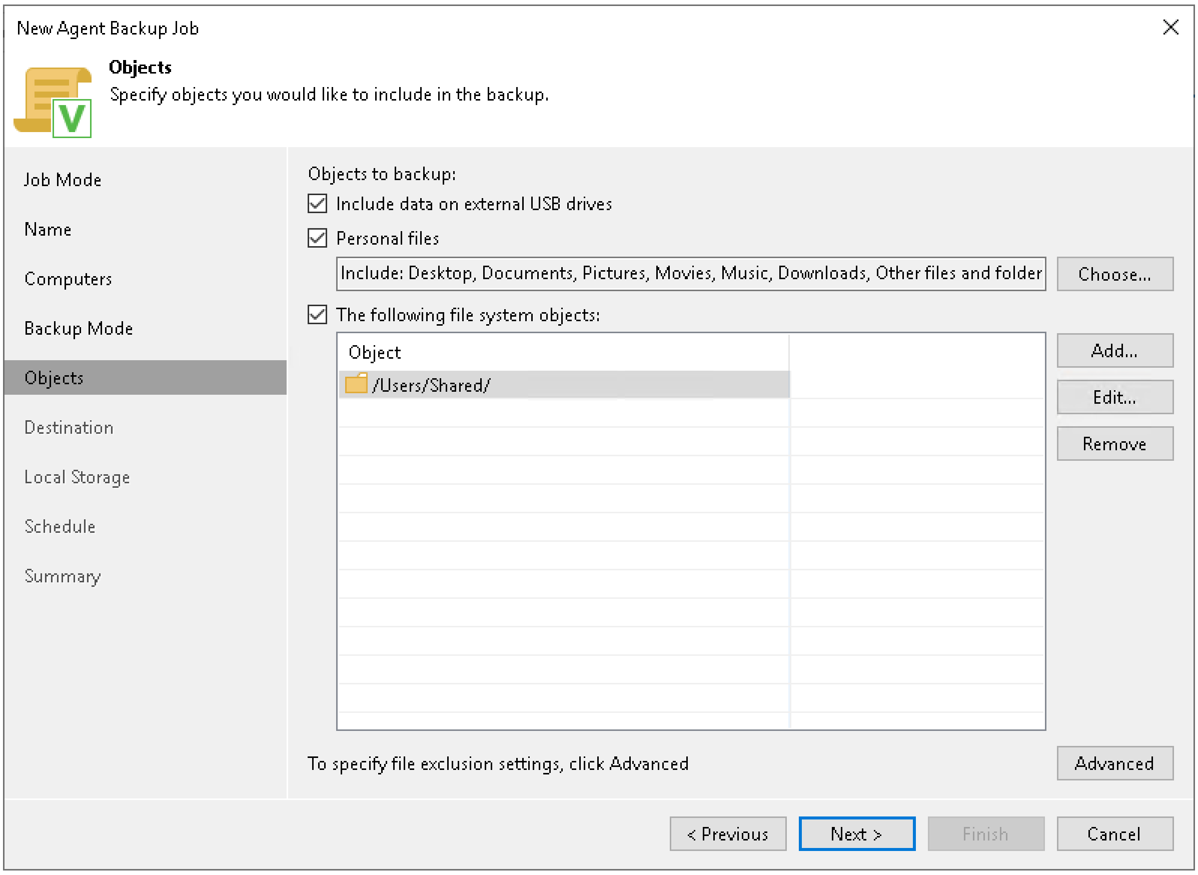
1. Select the **The following file system objects** check box and click **Add**.
2. In the **Add Object** window, type the path to a folder, mount point folder, or volume that you want to back up, for example, */Users/Shared/* or */Users/Administrator/Documents/*, and click **OK**.
3. Repeat steps 1-2 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`



New Agent Backup Job

Objects
Specify objects you would like to include in the backup.

Objects to backup:

☑ Include data on external USB drives

☑ Personal files

Include: Desktop, Documents, Pictures, Movies, Music, Downloads, Other files and folder

☑ The following file system objects:

Object
/Users/Shared/

To specify file exclusion settings, click Advanced

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 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.

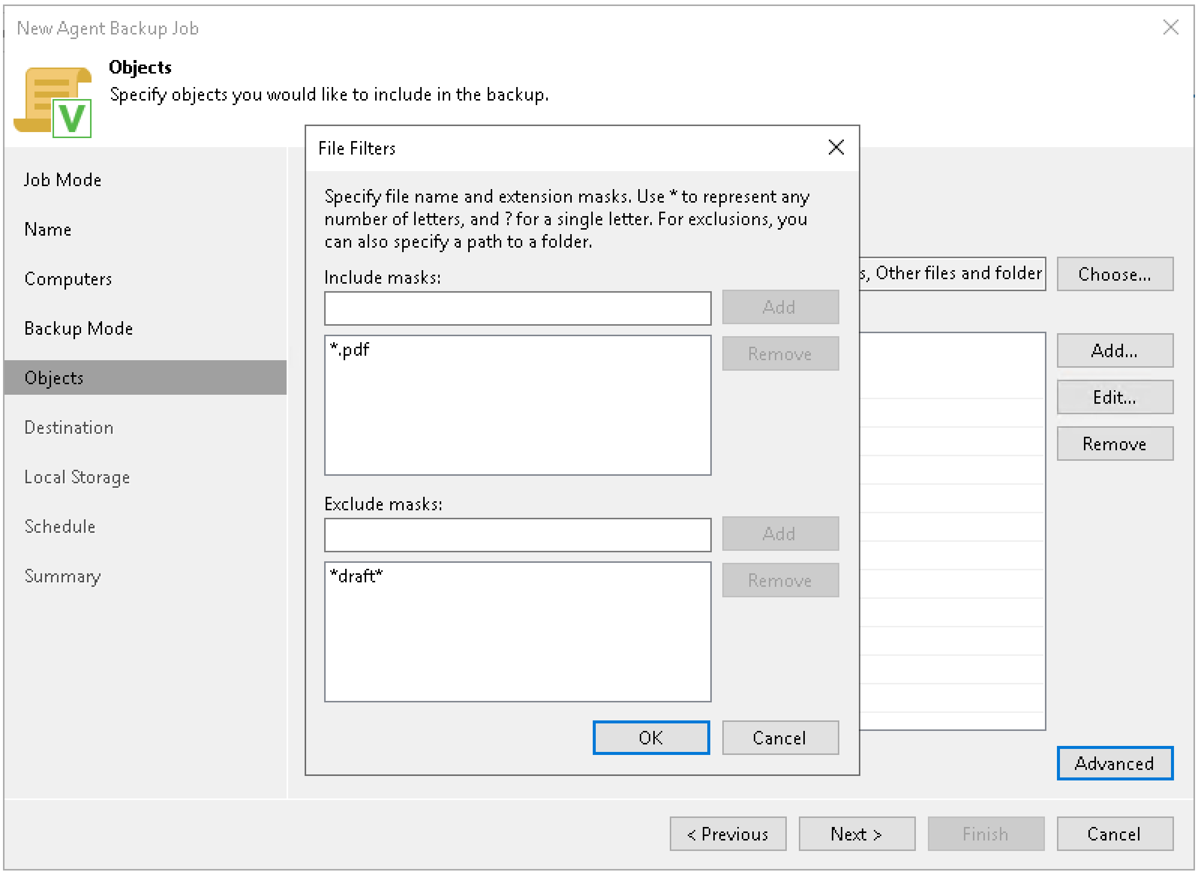
- In the **Exclude masks** field, specify file names and masks for file types that you do not want to back up, for example, `OldReports.tar.gz` or `*.odt`. Veeam Agent will back up all files except files of the specified type.

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.



New Agent Backup Job

Objects

Specify objects you would like to include in the backup.

File Filters

Specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify a path to a folder.

Include masks:

*.pdf

Exclude masks:

draft

Step 7. Select Backup Destination

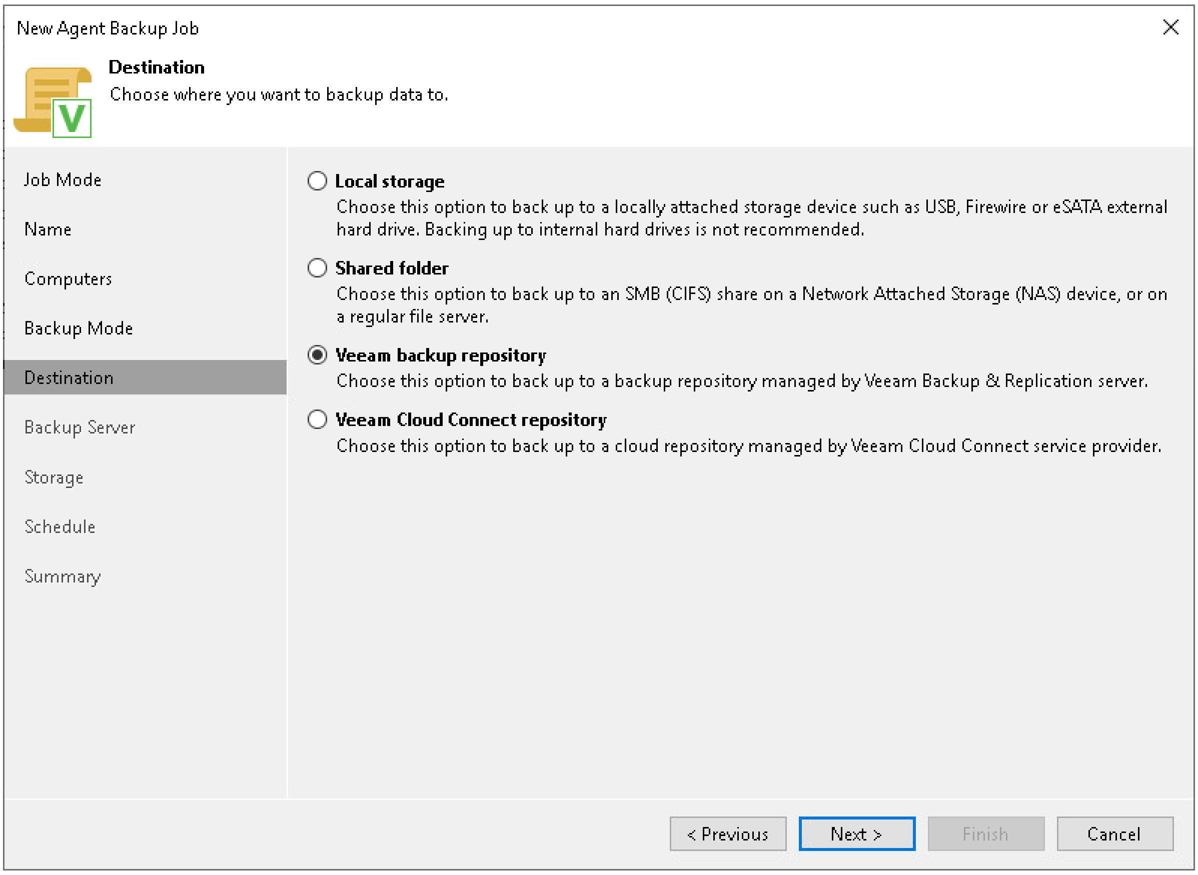
At the **Destination** step of the wizard, select a target location for backups created by Veeam Agents installed on protected computers.

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 network shared 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 an SMB 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 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.



○ **Local storage**
Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.

○ **Shared folder**
Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.

● **Veeam backup repository**
Choose this option to back up to a backup repository managed by Veeam Backup & Replication server.

○ **Veeam Cloud Connect repository**
Choose this option to back up to a cloud repository managed by Veeam Cloud Connect service provider.

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.

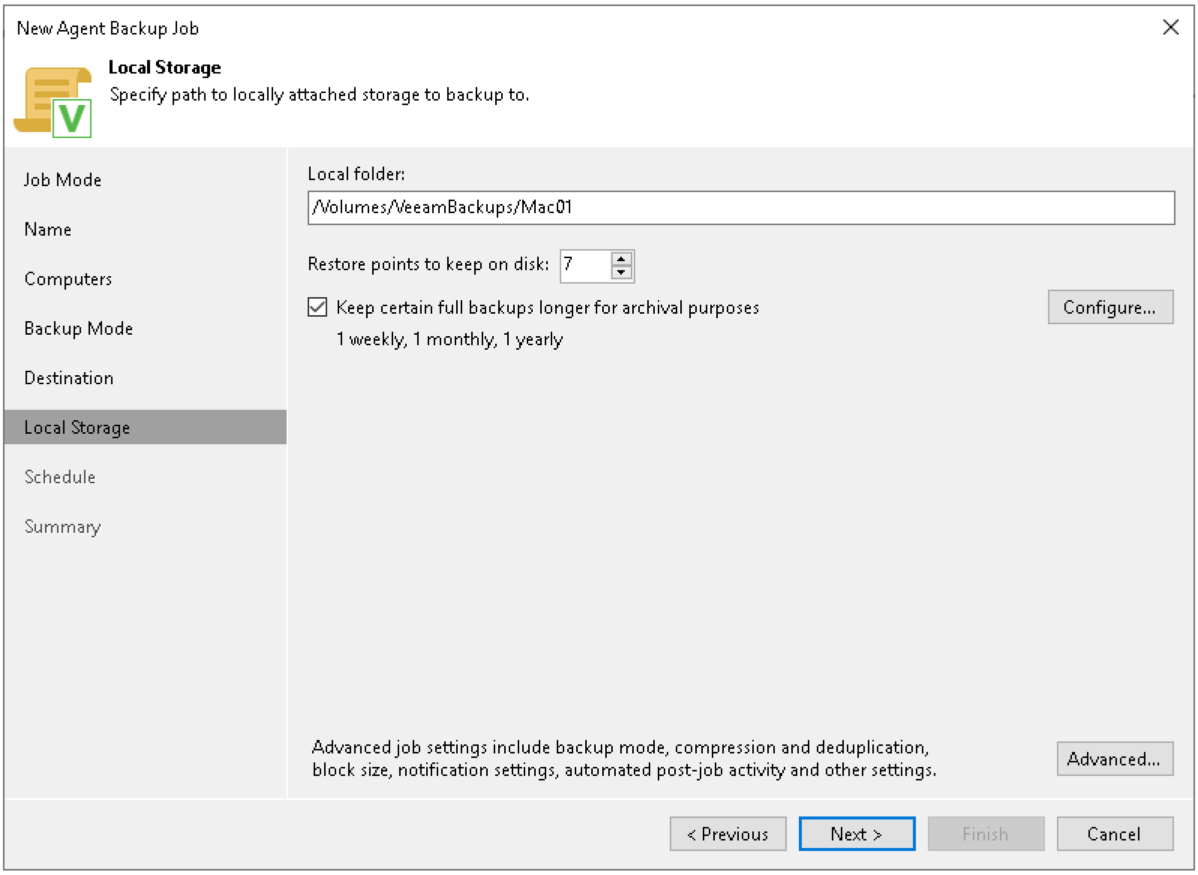
   > **IMPORTANT**
   >
   > USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.

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. To learn more, see Short-Term Retention Policy.

3. You can apply GFS (Grandfather-Father-Son) retention scheme to the backup policy. To specify GFS retention, 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 policy. To learn more, see Specify Advanced Backup Settings.



Local Storage

Specify path to locally attached storage to backup to.

Local folder: /Volumes/VeeamBackups/Mac01

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other 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 (\\).

   Consider that Veeam Backup & Replication does not support the NFS shares for Mac computers.

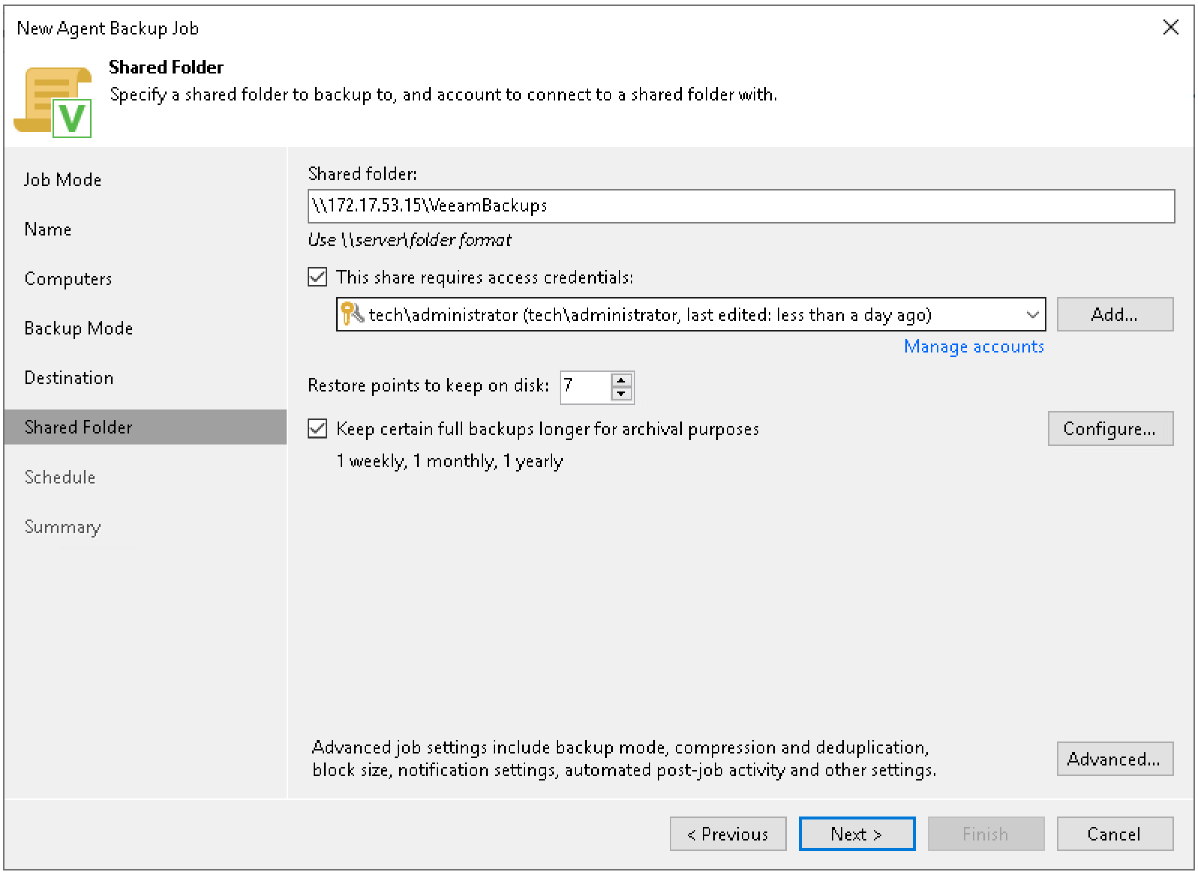
2. If the SMB network shared folder requires authentication, select the **This share requires access credentials** check box and select from the list a user account that has access permissions on this shared folder. If you have not set up credentials beforehand, click the **Manage accounts** link or 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. To learn more, see Short-Term Retention Policy.

4. You can apply GFS (Grandfather-Father-Son) retention scheme to the backup policy. To specify GFS retention, 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 policy. To learn more, see Specify Advanced Backup Settings.


New Agent Backup Job

Shared Folder

Specify a shared folder to backup to, and account to connect to a shared folder with.

Shared folder: \\172.17.53.15\VeeamBackups

Use \\server\folder format

☑ This share requires access credentials:

tech\administrator (tech\administrator, last edited: less than a day ago)

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other 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.

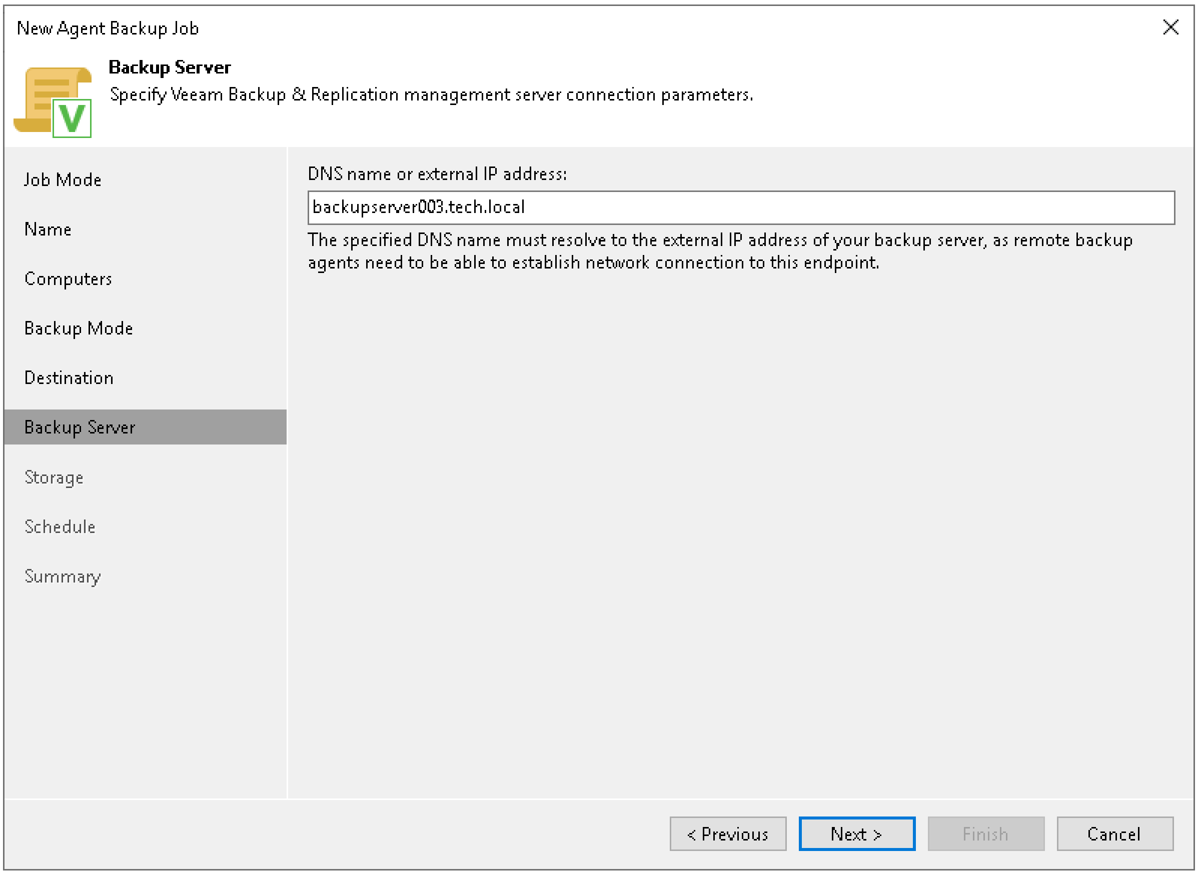
Specifying Backup Server Settings

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**, make sure that the name or IP address of the Veeam backup server, on which you configure the Veeam Agent backup policy, is displayed. Do not specify the name or IP address of another Veeam backup server. The specified DNS name or IP address must be resolvable 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.



DNS name or external IP address:

backupserver003.tech.local

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

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. To learn more, see Short-Term Retention Policy.

3. You can apply GFS (Grandfather-Father-Son) retention scheme to the backup policy. To specify GFS retention, 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.

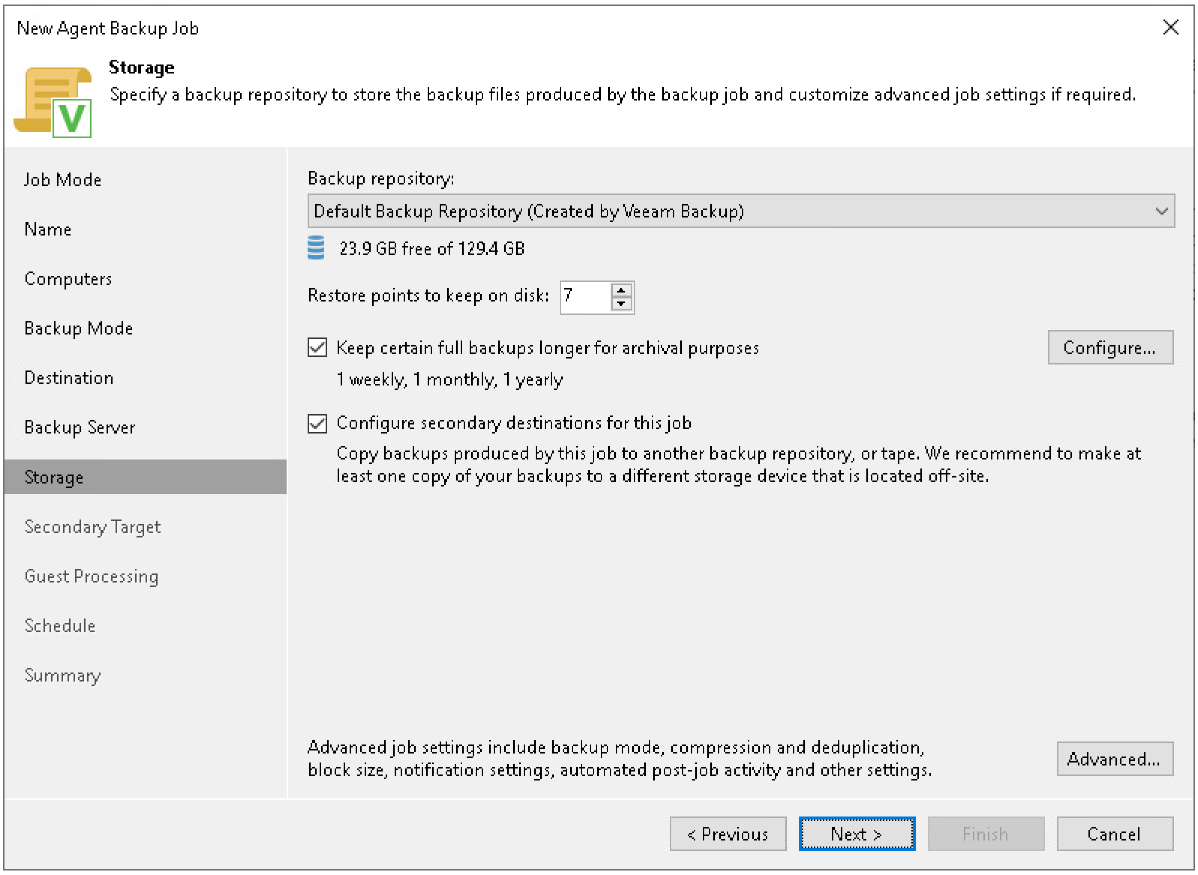
   Keep in mind that to use the GFS retention policy, you must set Veeam Agent to create full backups. To learn more, see Backup Settings.

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 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.

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

   > NOTE
   >
   > You must enable backup file encryption in the backup job storage settings if you back up data to the Veeam Data Cloud Vault storage added as a Veeam backup repository.



Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Default Backup Repository (Created by Veeam Backup)

23.9 GB free of 129.4 GB

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

☑ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

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 Before You Begin.

Specify settings for the cloud repository:

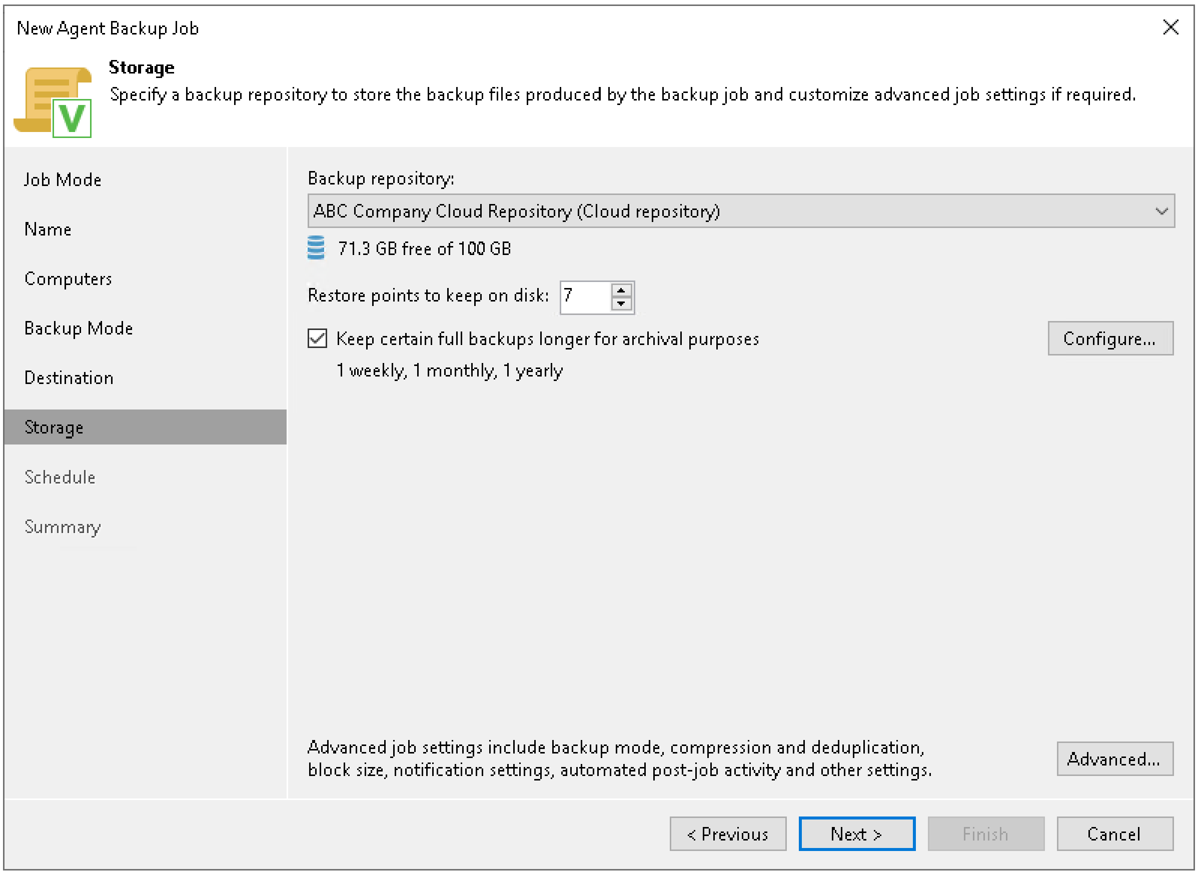
1. From the **Backup repository** list, select a cloud repository where you want to store created backups. The **Backup repository** list displays cloud repositories allocated to your tenant account by the Veeam Cloud Connect service provider. When you select a cloud repository, Veeam Backup & Replication 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. To learn more, see Short-Term Retention Policy.

3. You can apply GFS (Grandfather-Father-Son) retention scheme to the backup policy. To specify GFS retention, 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 policy. To learn more, see Specify Advanced Backup Settings.

> IMPORTANT
>
> You must enable backup file encryption in the backup job storage settings if you back up data to the Veeam Data Cloud Vault storage added as a Veeam Cloud Connect repository.



Backup repository: ABC Company Cloud Repository (Cloud repository)

71.3 GB free of 100 GB

Restore points to keep on disk: 7

☑ Keep certain full backups longer for archival purposes

1 weekly, 1 monthly, 1 yearly

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other 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.

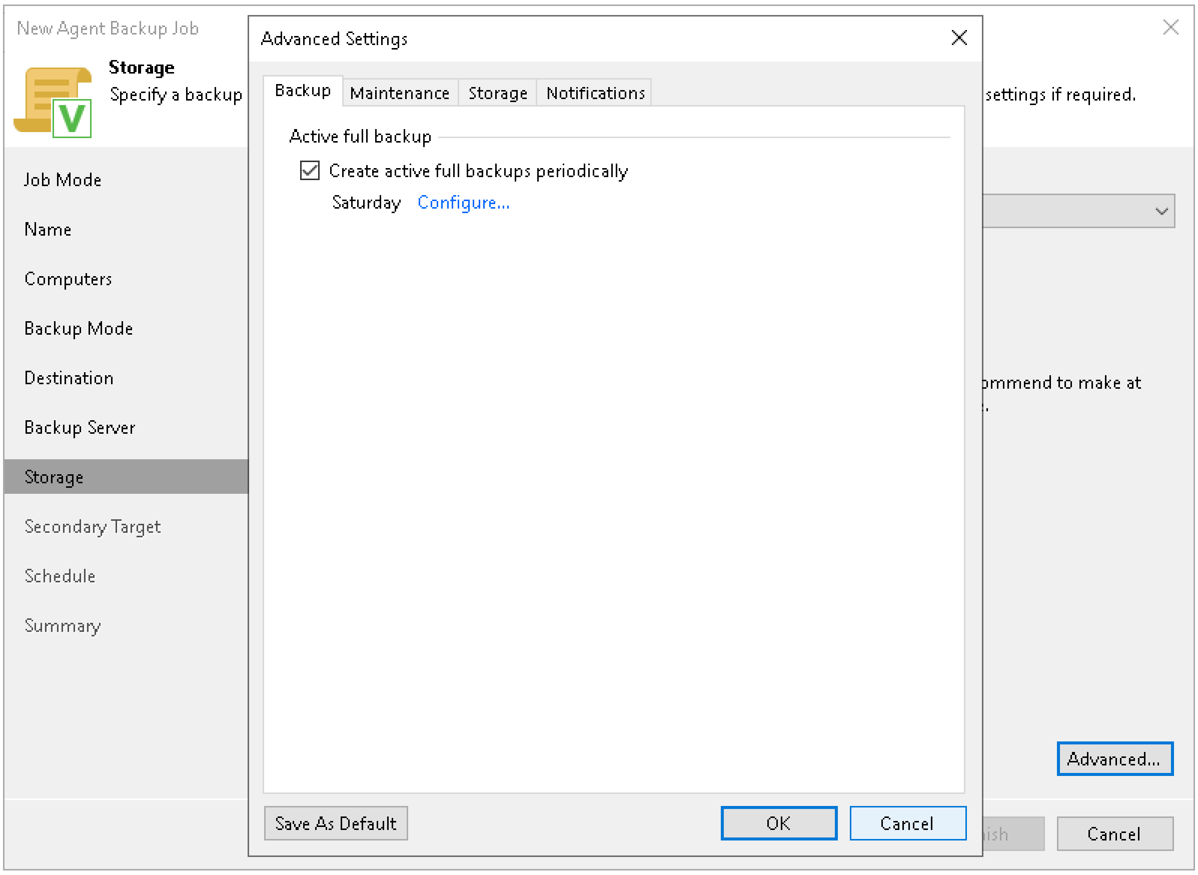
Backup Settings

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.



Active full backup

☑ Create active full backups periodically

Saturday Configure...

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.

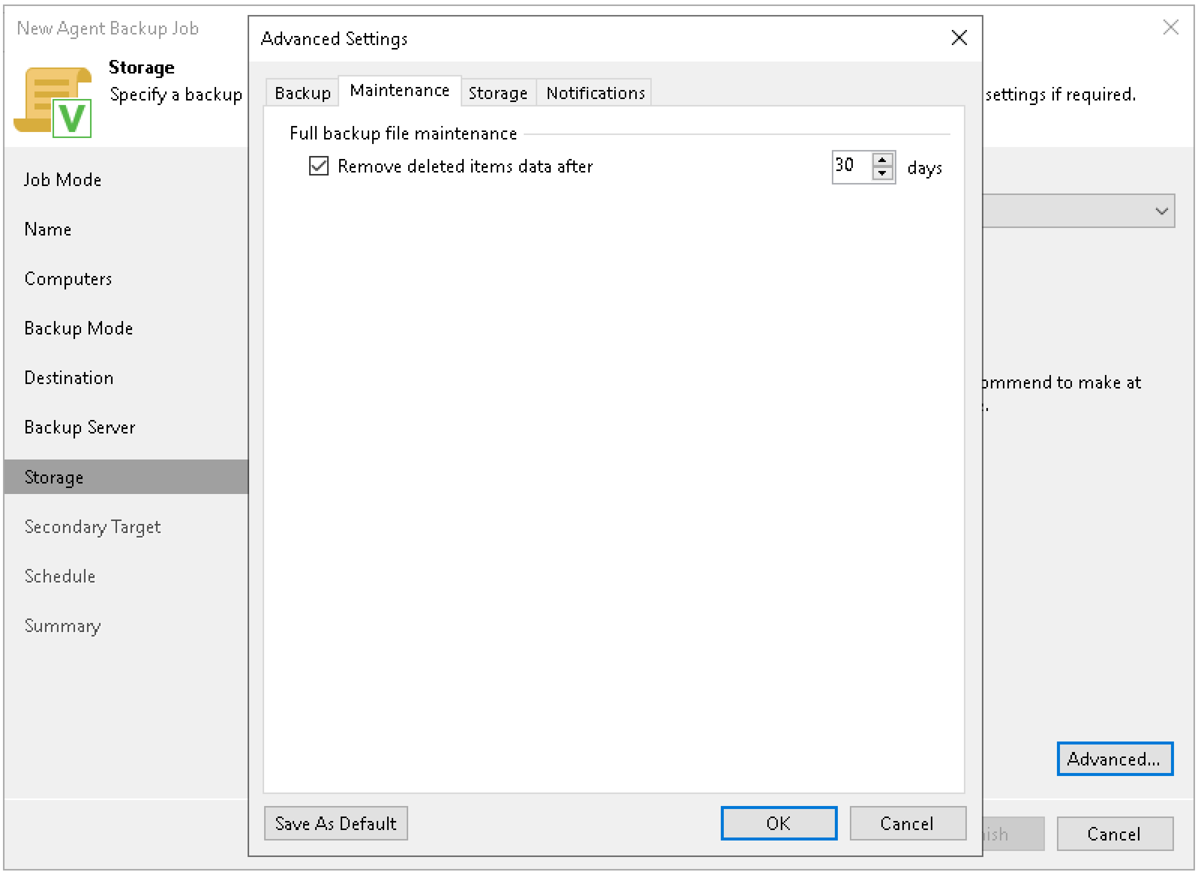
To specify maintenance settings for the backup policy:

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. To learn more, see Scheduling Health Check.



Full backup file maintenance

☑ Remove deleted items data after 30 days

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.

   > NOTE
   >
   > If you change the storage optimization settings for the backup job, new settings will not have any effect on previously created files in the chain. They will be applied to new files created after the settings were changed.
   >
   > To apply new storage optimization settings in backup jobs, you must create an active full backup after you change storage optimization settings. Veeam Backup & Replication will use the new block size for the active full backup and subsequent backup files in the backup chain. To learn about the active full backup, see Performing Active Full Backup.

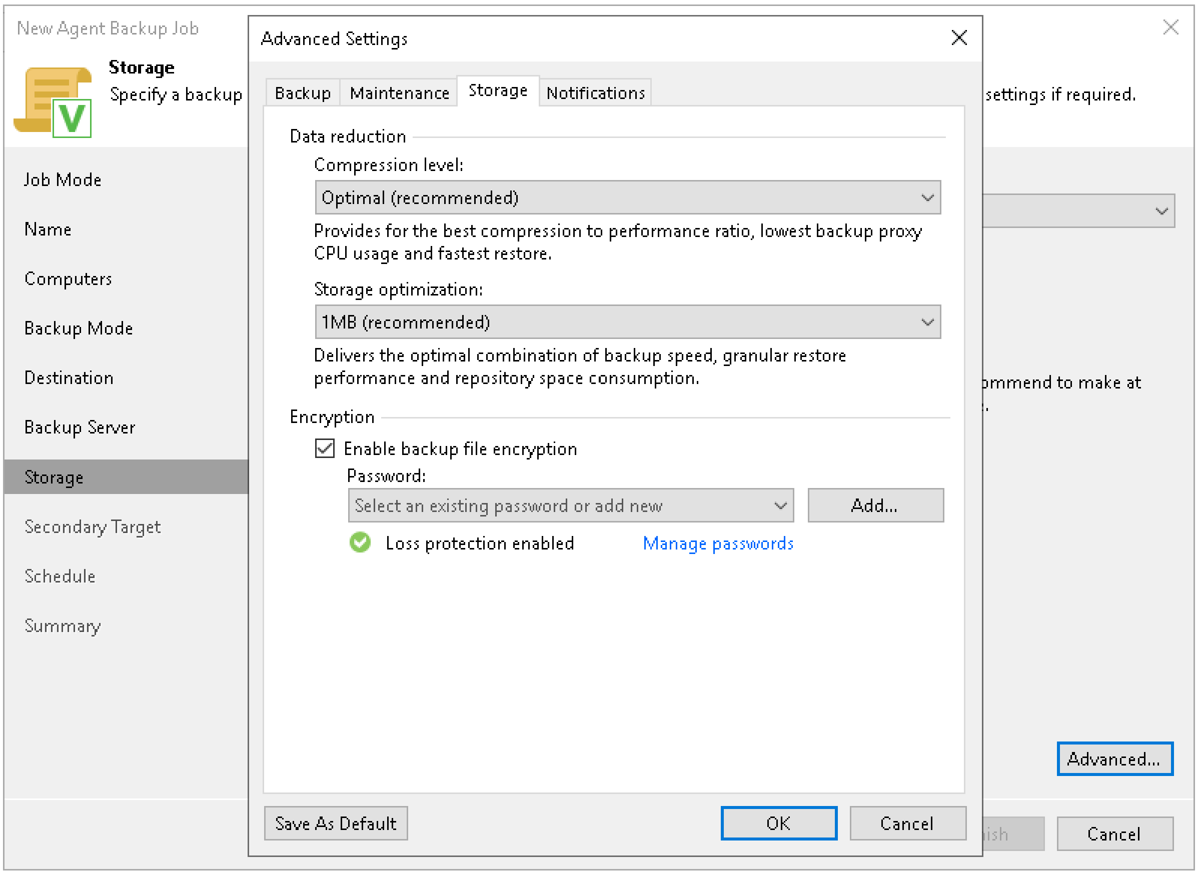
5. To encrypt the content of backup files, select the **Enable backup file encryption** check box. In the **Password** field, select a password that you want to use for encryption. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password. 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:

- If you plan to encrypt the content of backup files, consider the limitations listed in the Data Encryption Limitations subsection.
- You must encrypt the backup policy if you want to back up data to the Veeam Data Vault storage.
- You cannot use Key Management System (KMS) keys for data encryption with a Veeam Agent backup policy.



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: Select an existing password or add new

✓ Loss protection enabled

Data Encryption Limitations

If you plan to encrypt the content of backup files, consider the following limitations:

- Data encryption settings for Veeam Agent backup policies configured in Veeam Backup & Replication are stored to the Veeam Backup & Replication database. For backup 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 an SMB 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 or disable encryption for an existing Veeam Agent backup 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 policy, Veeam Agent will encrypt the backup chain starting from the next restore point created with this policy.
- 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.

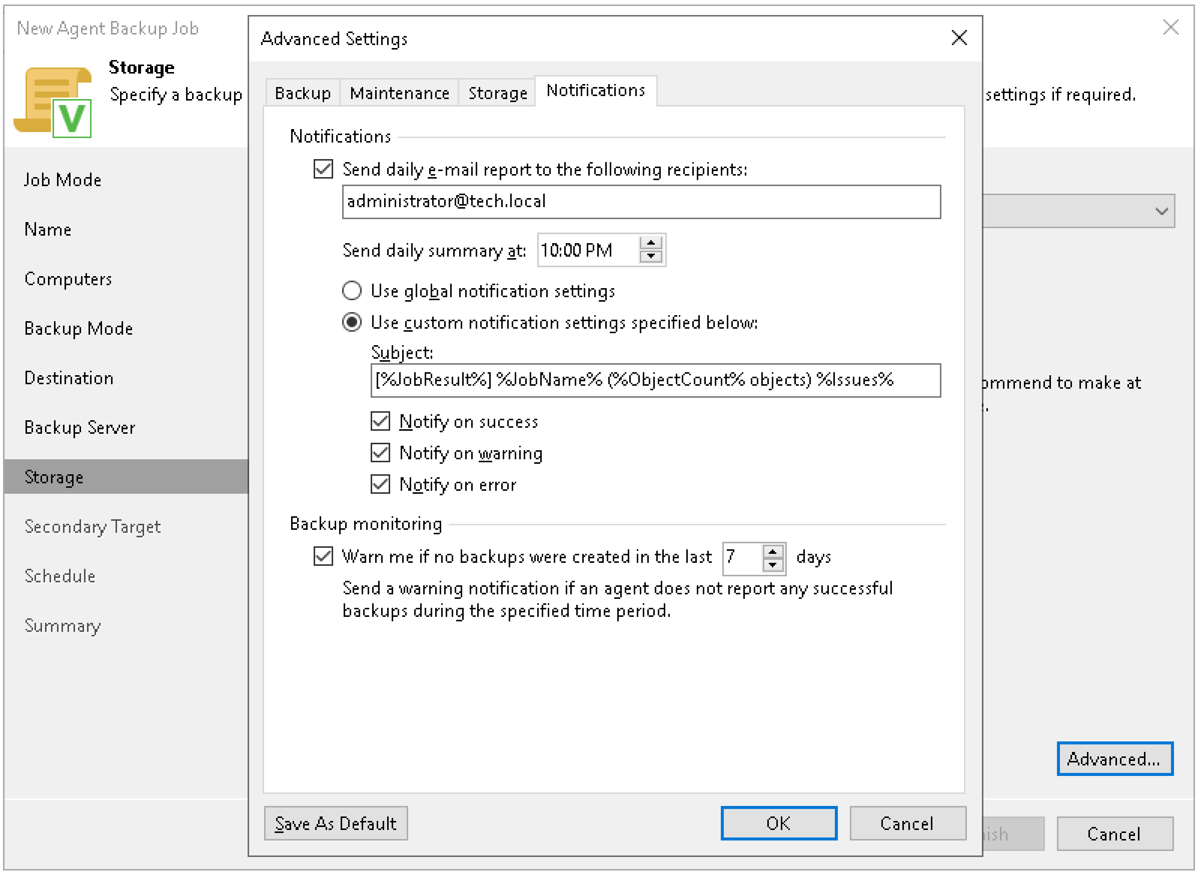
   - To receive a typical notification for the backup policy, select **Use global notification settings**. In this case, Veeam Backup & Replication will apply to the backup policy global email notification settings specified for the backup server. Veeam Backup & Replication will send the email report containing 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 **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.



New Agent Backup Job

Storage

Specify a backup

settings if required.

ommend to make at

Advanced Settings

Notifications

☑ Send daily e-mail report to the following recipients:

administrator@tech.local

Send daily summary at: 10:00 PM

○ Use global notification settings

● Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

☑ Notify on error

Backup monitoring

☑ Warn me if no backups were created in the last 7 days

Send a warning notification if an agent does not report any successful backups during the specified time period.

Step 10. Specify Secondary Target

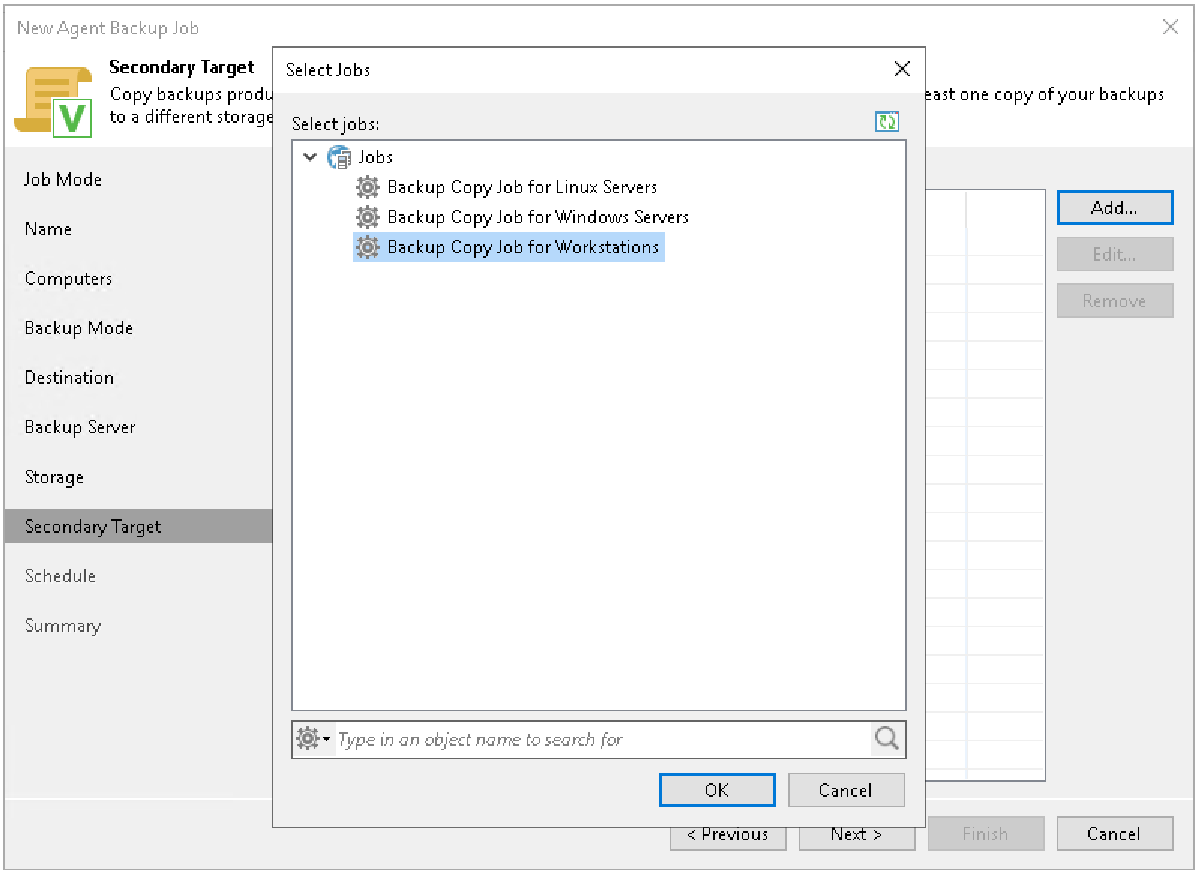
The **Secondary Target** step of the wizard is available if you have enabled the **Configure secondary destinations for this job** option at the **Storage** step of the wizard.

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 tap e 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:

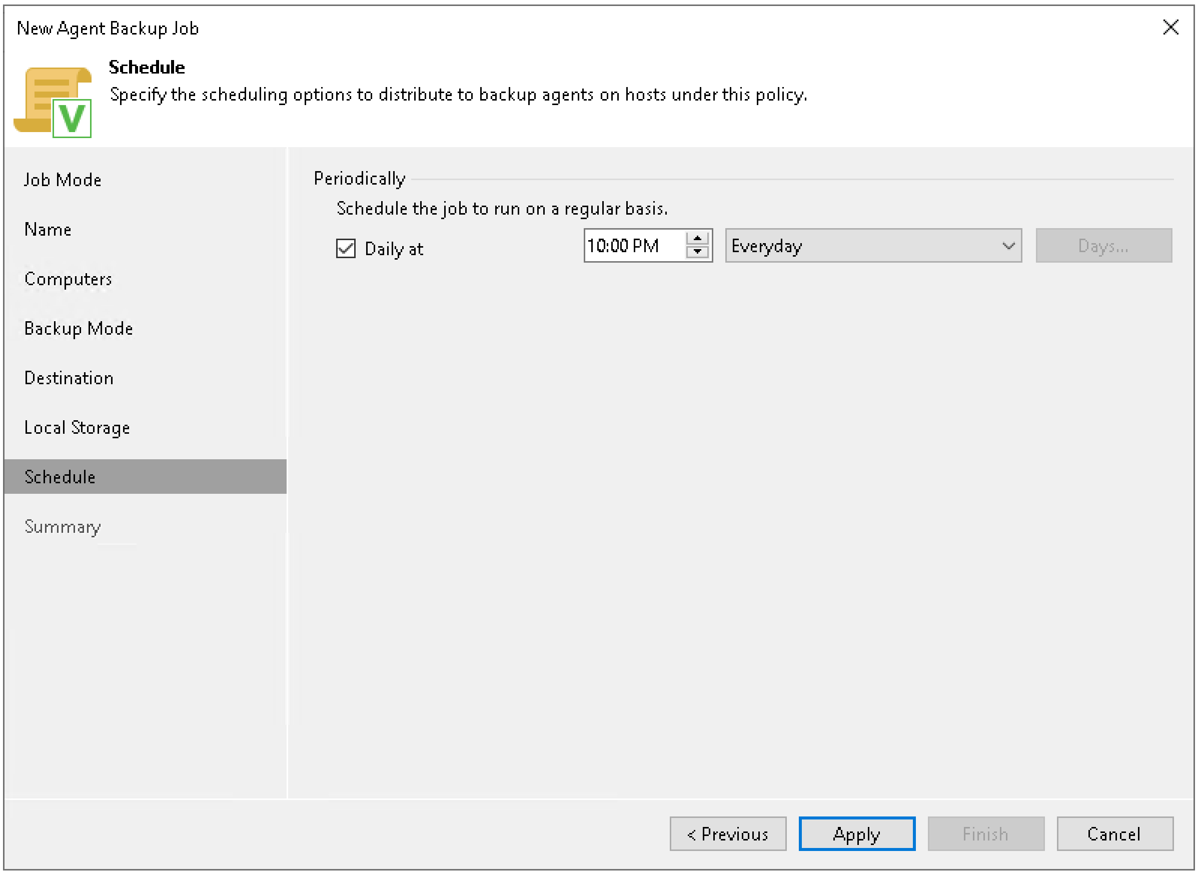
- Scheduling Settings for Workstations
- Scheduling Settings for Servers

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 weekdays* — select this option to start the job at specific time on weekdays.
   - *On these days* — select this option to start the job at specific time on selected days.



New Agent Backup Job

Schedule

Specify the scheduling options to distribute to backup agents on hosts under this policy.

Periodically

Schedule the job to run on a regular basis.

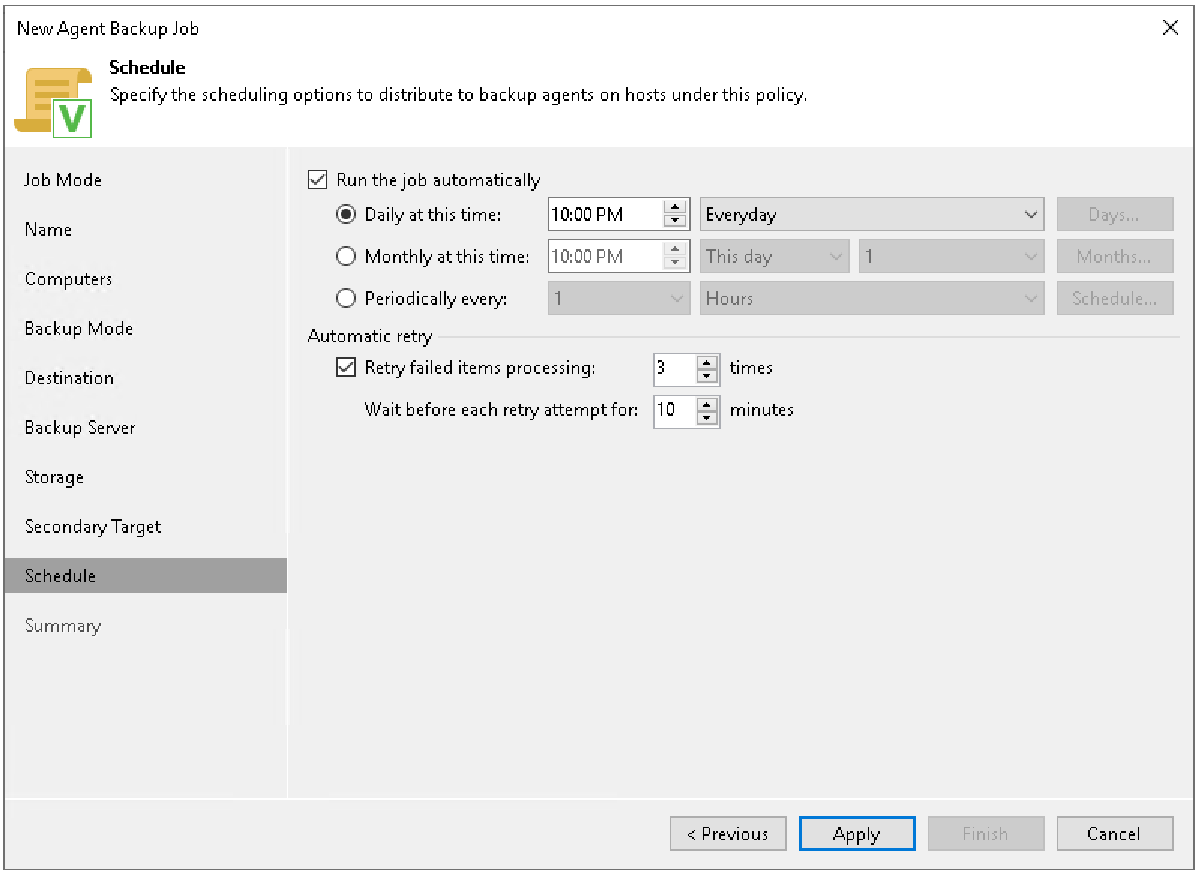
☑ Daily at 10:00 PM Everyday

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.


New Agent Backup Job

Schedule

Specify the scheduling options to distribute to backup agents on hosts under this policy.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM This day 1

○ Periodically every: 1 Hours

Automatic retry

☑ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

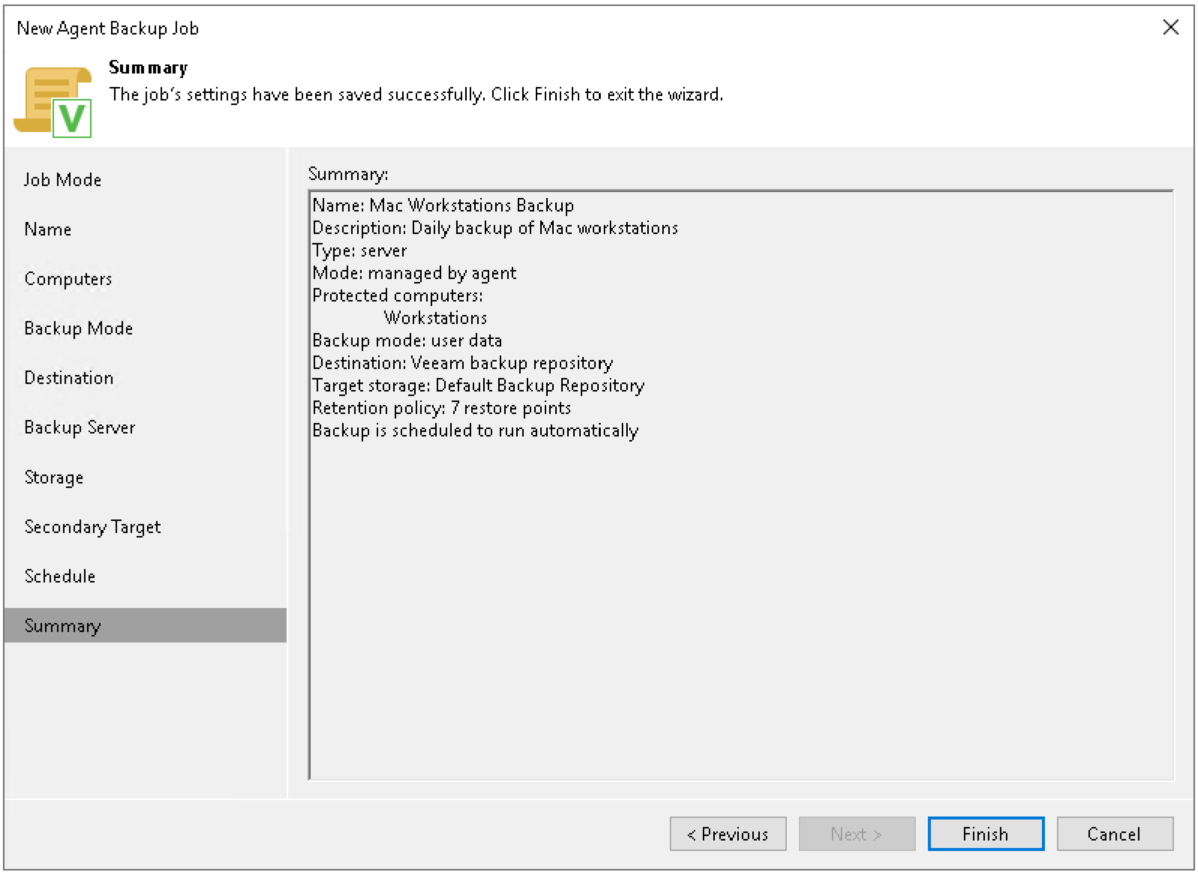
Step 12. Review Backup Job Settings

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 Configuration.



The job's settings have been saved successfully. Click Finish to exit the wizard.

Summary:

```
Name: Mac Workstations Backup
Description: Daily backup of Mac workstations
Type: server
Mode: managed by agent
Protected computers:
            Workstations
Backup mode: user data
Destination: Veeam backup repository
Target storage: Default Backup Repository
Retention policy: 7 restore points
Backup is scheduled to run automatically
```

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.

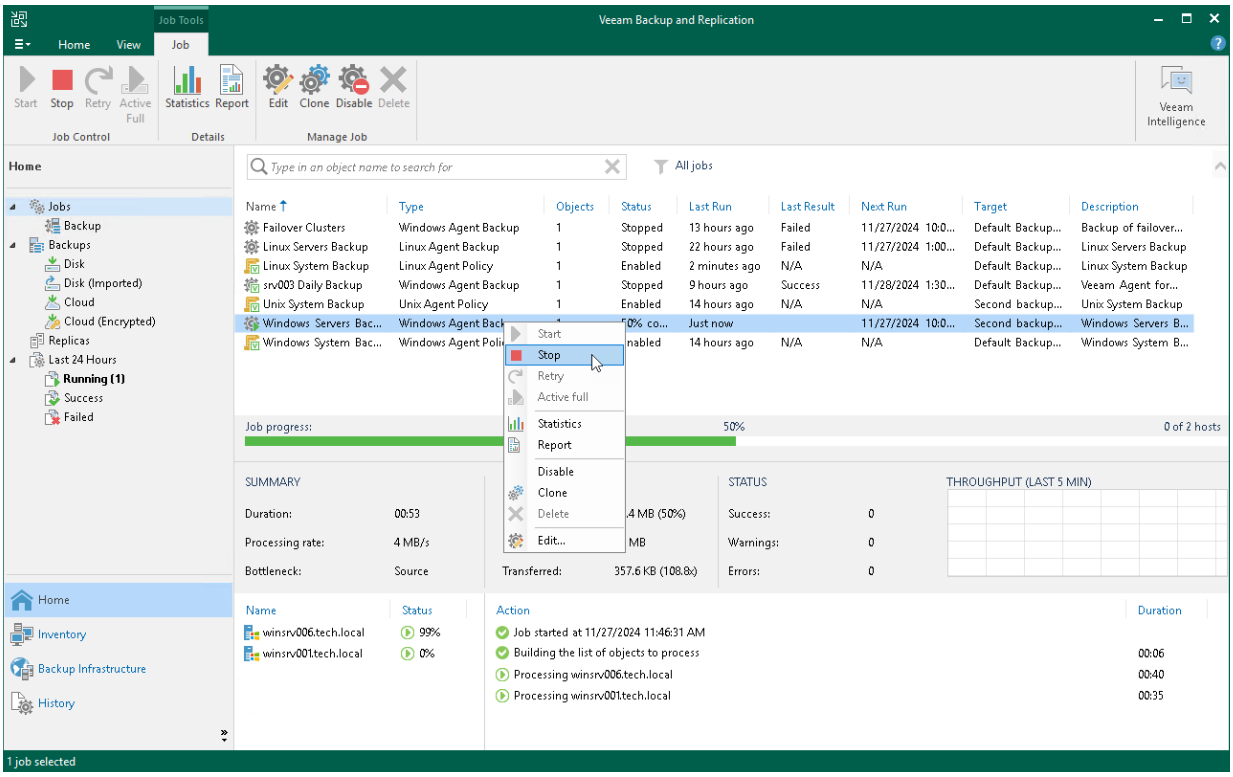
To stop a job immediately:

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**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	13 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	22 hours ago	Failed	11/27/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	2 minutes ago	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup	1	Stopped	9 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy	1	Enabled	14 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Back		0% co...	Just now		11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Poli		nabled	14 hours ago	N/A	N/A	Default Backup...	Windows System B...

Job progress: 50% 0 of 2 hosts

Duration: 00:53
Processing rate: 4 MB/s
Bottleneck: Source

.4 MB (50%)
MB
Transferred: 357.6 KB (108.8x)

Success: 0
Warnings: 0
Errors: 0

Name	Status
winsrv006.tech.local	99%
winsrv001.tech.local	0%

Action	Duration
Job started at 11/27/2024 11:46:31 AM	
Building the list of objects to process	00:06
Processing winsrv006.tech.local	00:40
Processing winsrv001.tech.local	00:35

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.

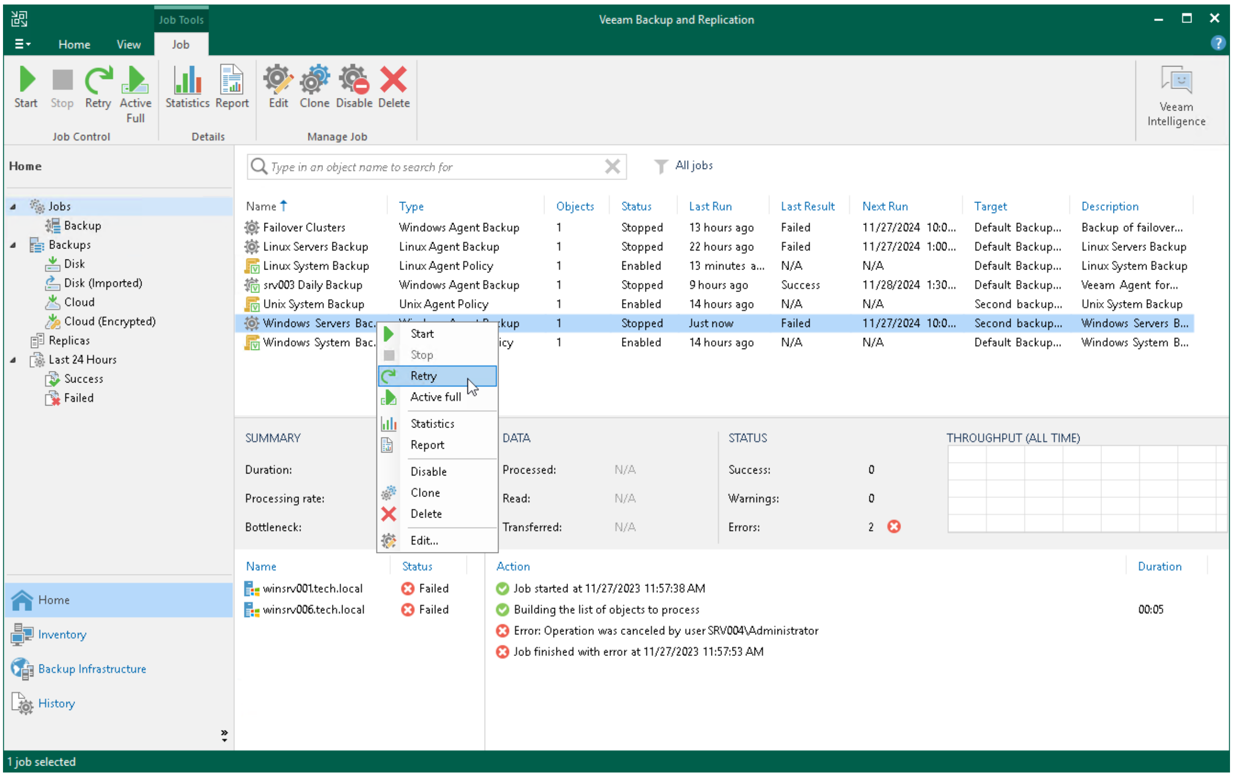
To retry a job:

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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	13 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	22 hours ago	Failed	11/27/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	13 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup	1	Stopped	9 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy	1	Enabled	14 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	...kup	1	Stopped	Just now	Failed	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	...icy	1	Enabled	14 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Duration:

Processing rate:

Bottleneck:

DATA

Processed: N/A

Read: N/A

Transferred: N/A

STATUS

Success: 0

Warnings: 0

Errors: 2

THROUGHPUT (ALL TIME)

Name	Status
winsrv001.tech.local	Failed
winsrv006.tech.local	Failed

Action	Duration
Job started at 11/27/2023 11:57:38 AM	
Building the list of objects to process	00:05
Error: Operation was canceled by user SRV004\Administrator	
Job finished with error at 11/27/2023 11:57:53 AM	

Retrying Job for Individual Computer

To retry a backup job for an individual computer:

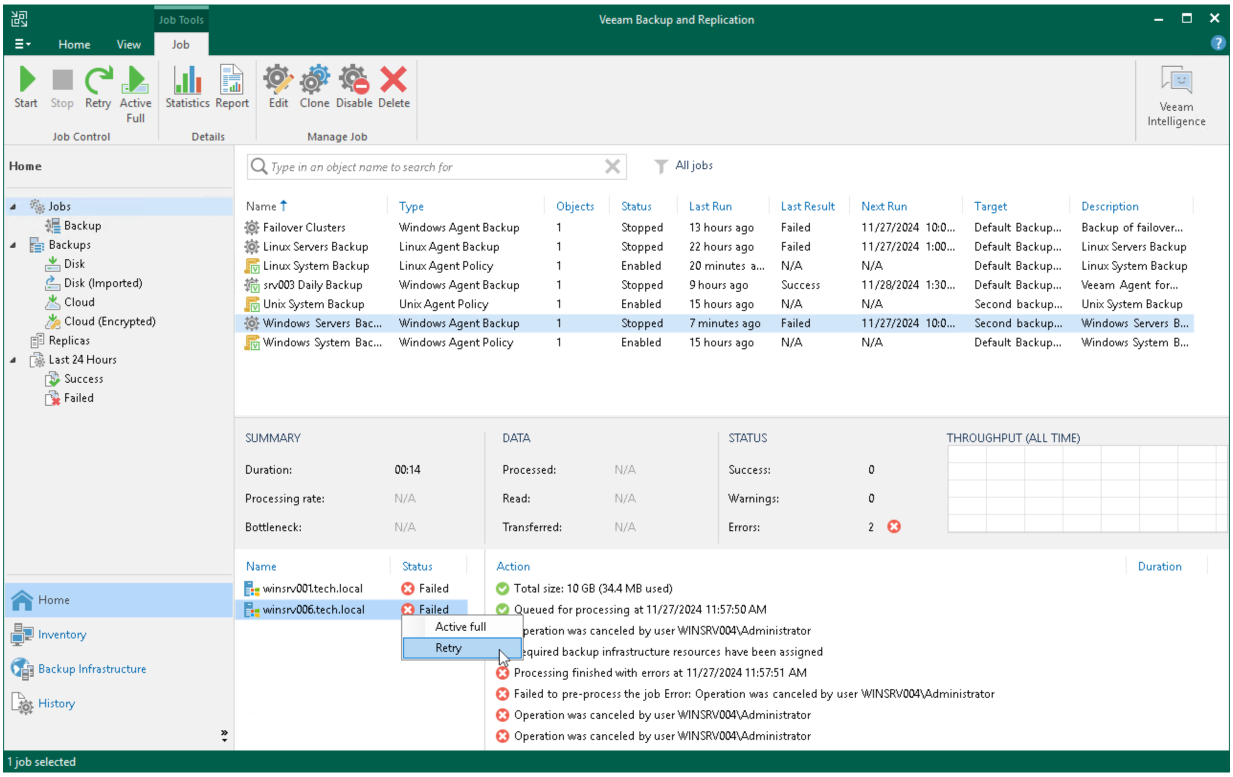
1. Open the **Home** view.

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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	13 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	22 hours ago	Failed	11/27/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	20 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup	1	Stopped	9 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy	1	Enabled	15 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopped	7 minutes ago	Failed	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Policy	1	Enabled	15 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY		DATA		STATUS	
Duration:	00:14	Processed:	N/A	Success:	0
Processing rate:	N/A	Read:	N/A	Warnings:	0
Bottleneck:	N/A	Transferred:	N/A	Errors:	2 ☒

THROUGHPUT (ALL TIME)

Name	Status
winsrv001.tech.local	☒ Failed
winsrv006.tech.local	☒ Failed

Action	Duration
✓ Total size: 10 GB (34.4 MB used)	
✓ Queued for processing at 11/27/2024 11:57:50 AM	
peration was canceled by user WINSRV004\Administrator	
equired backup infrastructure resources have been assigned	
☒ Processing finished with errors at 11/27/2024 11:57:51 AM	
☒ Failed to pre-process the job Error: Operation was canceled by user WINSRV004\Administrator	
☒ Operation was canceled by user WINSRV004\Administrator	
☒ Operation was canceled by user WINSRV004\Administrator	

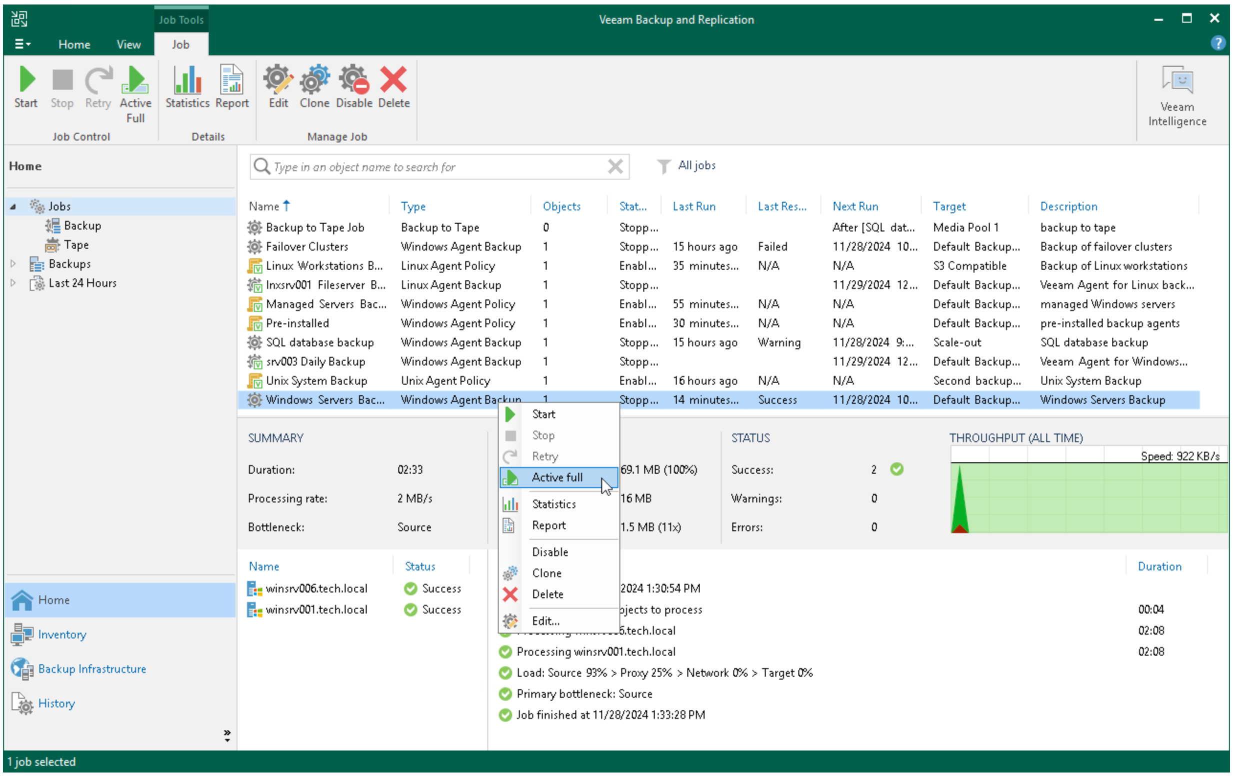
Performing Active Full Backup

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.



Name	Type	Objects	Stat...	Last Run	Last Res...	Next Run	Target	Description
Backup to Tape Job	Backup to Tape	0	Stopp...			After [SQL dat...	Media Pool 1	backup to tape
Failover Clusters	Windows Agent Backup	1	Stopp...	15 hours ago	Failed	11/28/2024 10...	Default Backup...	Backup of failover clusters
Linux Workstations B...	Linux Agent Policy	1	Enabl...	35 minutes...	N/A	N/A	S3 Compatible	Backup of Linux workstations
lnxsrv001 Fileserver B...	Linux Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Linux back...
Managed Servers Bac...	Windows Agent Policy	1	Enabl...	55 minutes...	N/A	N/A	Default Backup...	managed Windows servers
Pre-installed	Windows Agent Policy	1	Enabl...	30 minutes...	N/A	N/A	Default Backup...	pre-installed backup agents
SQL database backup	Windows Agent Backup	1	Stopp...	15 hours ago	Warning	11/28/2024 9:...	Scale-out	SQL database backup
srv003 Daily Backup	Windows Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Windows...
Unix System Backup	Unix Agent Policy	1	Enabl...	16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopp...	14 minutes...	Success	11/28/2024 10...	Default Backup...	Windows Servers Backup

SUMMARY

Duration: 02:33
Processing rate: 2 MB/s
Bottleneck: Source

69.1 MB (100%)
16 MB
1.5 MB (11x)

STATUS

Success: 2
Warnings: 0
Errors: 0

THROUGHPUT (ALL TIME)

Speed: 922 KB/s

Name	Status
winsrv006.tech.local	Success
winsrv001.tech.local	Success

2024 1:30:54 PM
ojects to process 00:04
6.tech.local 02:08
Processing winsrv001.tech.local 02:08
Load: Source 93% > Proxy 25% > Network 0% > Target 0%
Primary bottleneck: Source
Job finished at 11/28/2024 1:33:28 PM

Performing Active Full Backup for Individual Computer

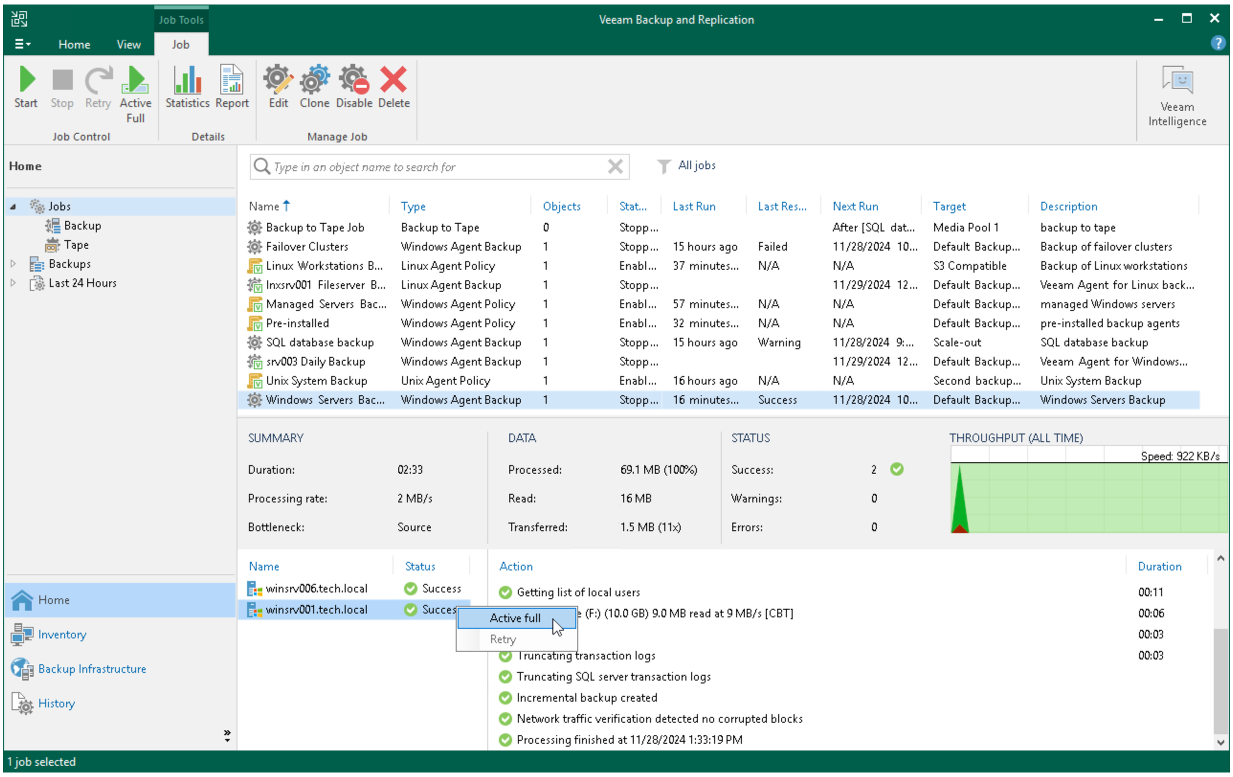
To create an active full backup for an individual computer:

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.



Name	Type	Objects	Stat...	Last Run	Last Res...	Next Run	Target	Description
Backup to Tape Job	Backup to Tape	0	Stopp...			After [SQL dat...	Media Pool 1	backup to tape
Failover Clusters	Windows Agent Backup	1	Stopp...	15 hours ago	Failed	11/28/2024 10...	Default Backup...	Backup of failover clusters
Linux Workstations B...	Linux Agent Policy	1	Enabl...	37 minutes...	N/A	N/A	S3 Compatible	Backup of Linux workstations
lnxsrv001 Fileserver B...	Linux Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Linux back...
Managed Servers Bac...	Windows Agent Policy	1	Enabl...	57 minutes...	N/A	N/A	Default Backup...	managed Windows servers
Pre-installed	Windows Agent Policy	1	Enabl...	32 minutes...	N/A	N/A	Default Backup...	pre-installed backup agents
SQL database backup	Windows Agent Backup	1	Stopp...	15 hours ago	Warning	11/28/2024 9:...	Scale-out	SQL database backup
srv003 Daily Backup	Windows Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Windows...
Unix System Backup	Unix Agent Policy	1	Enabl...	16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopp...	16 minutes...	Success	11/28/2024 10...	Default Backup...	Windows Servers Backup

SUMMARY
Duration: 02:33
Processing rate: 2 MB/s
Bottleneck: Source

DATA
Processed: 69.1 MB (100%)
Read: 16 MB
Transferred: 1.5 MB (11x)

STATUS
Success: 2
Warnings: 0
Errors: 0

THROUGHPUT (ALL TIME)
Speed: 922 KB/s

Name	Status
winsrv006.tech.local	Success
winsrv001.tech.local	Succes

Action	Duration
Getting list of local users	00:11
e (F:) (10.0 GB) 9.0 MB read at 9 MB/s [CBT]	00:06
	00:03
Truncating transaction logs	00:03
Truncating SQL server transaction logs	
Incremental backup created	
Network traffic verification detected no corrupted blocks	
Processing finished at 11/28/2024 1:33:19 PM	

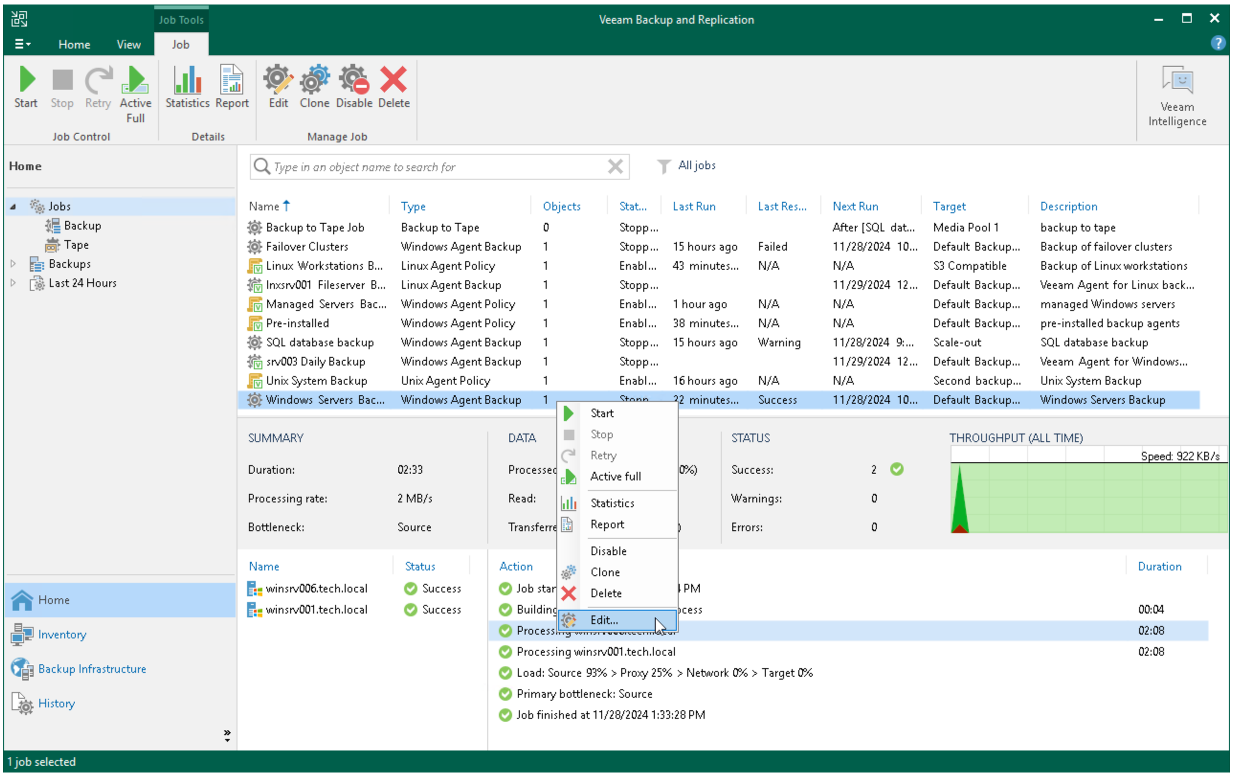
Editing Veeam Agent Backup Job Settings

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**
>
> Consider 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.



Name	Type	Objects	Stat...	Last Run	Last Res...	Next Run	Target	Description
Backup to Tape Job	Backup to Tape	0	Stopp...			After [SQL dat...	Media Pool 1	backup to tape
Failover Clusters	Windows Agent Backup	1	Stopp...	15 hours ago	Failed	11/28/2024 10...	Default Backup...	Backup of failover clusters
Linux Workstations B...	Linux Agent Policy	1	Enabl...	43 minutes...	N/A	N/A	S3 Compatible	Backup of Linux workstations
lnxsrv001 Fileserver B...	Linux Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Linux back...
Managed Servers Bac...	Windows Agent Policy	1	Enabl...	1 hour ago	N/A	N/A	Default Backup...	managed Windows servers
Pre-installed	Windows Agent Policy	1	Enabl...	38 minutes...	N/A	N/A	Default Backup...	pre-installed backup agents
SQL database backup	Windows Agent Backup	1	Stopp...	15 hours ago	Warning	11/28/2024 9:...	Scale-out	SQL database backup
srv003 Daily Backup	Windows Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Windows...
Unix System Backup	Unix Agent Policy	1	Enabl...	16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopp...	22 minutes...	Success	11/28/2024 10...	Default Backup...	Windows Servers Backup

SUMMARY

Duration: 02:33
Processing rate: 2 MB/s
Bottleneck: Source

DATA

Processed ... 0%)
Read:
Transferre...

STATUS

Success: 2
Warnings: 0
Errors: 0

THROUGHPUT (ALL TIME)

Speed: 922 KB/s

Name	Status
winsrv006.tech.local	Success
winsrv001.tech.local	Success

Action	Duration
Job star... PM	
Building... ocess	00:04
Processing...	02:08
Processing winsrv001.tech.local	02:08
Load: Source 93% > Proxy 25% > Network 0% > Target 0%	
Primary bottleneck: Source	
Job finished at 11/28/2024 1:33:28 PM	

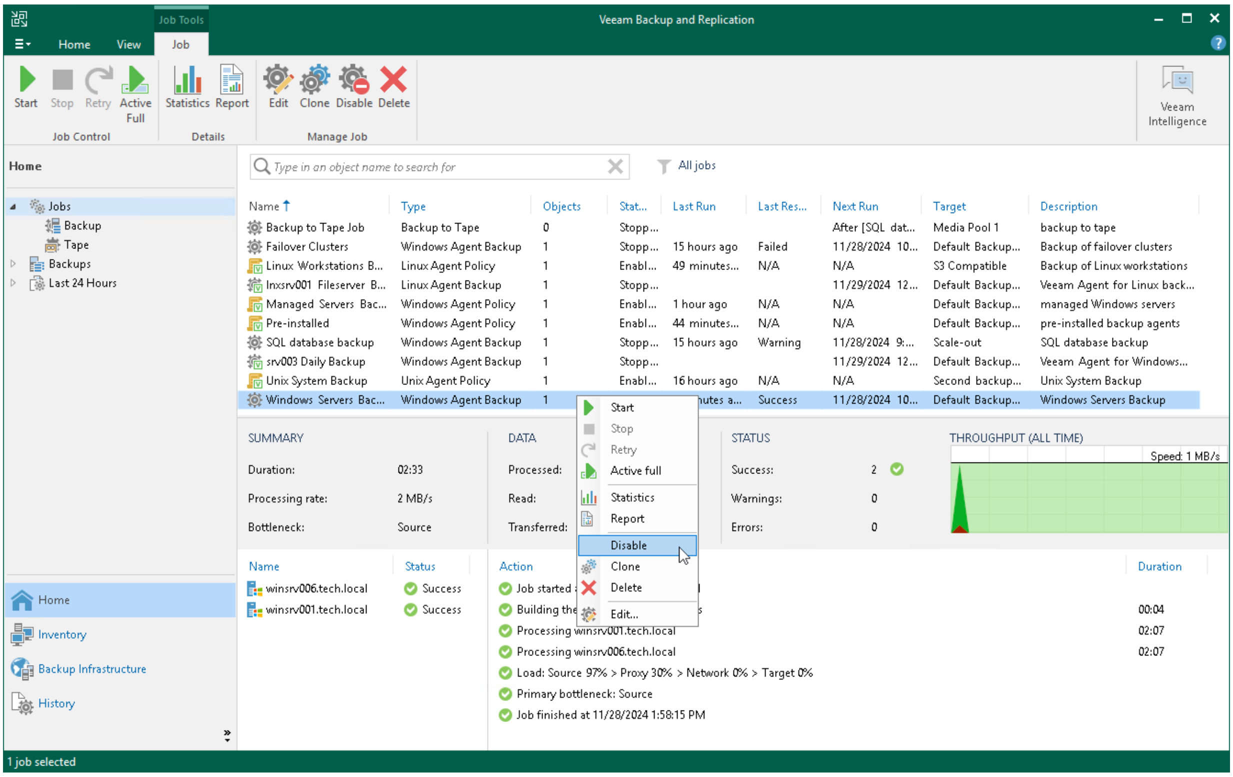
Enabling and Disabling Veeam Agent Backup Job

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.



Name	Type	Objects	Stat...	Last Run	Last Res...	Next Run	Target	Description
Backup to Tape Job	Backup to Tape	0	Stopp...			After [SQL dat...	Media Pool 1	backup to tape
Failover Clusters	Windows Agent Backup	1	Stopp...	15 hours ago	Failed	11/28/2024 10...	Default Backup...	Backup of failover clusters
Linux Workstations B...	Linux Agent Policy	1	Enabl...	49 minutes...	N/A	N/A	S3 Compatible	Backup of Linux workstations
lnxsrv001 Fileserver B...	Linux Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Linux back...
Managed Servers Bac...	Windows Agent Policy	1	Enabl...	1 hour ago	N/A	N/A	Default Backup...	managed Windows servers
Pre-installed	Windows Agent Policy	1	Enabl...	44 minutes...	N/A	N/A	Default Backup...	pre-installed backup agents
SQL database backup	Windows Agent Backup	1	Stopp...	15 hours ago	Warning	11/28/2024 9:...	Scale-out	SQL database backup
srv003 Daily Backup	Windows Agent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Windows...
Unix System Backup	Unix Agent Policy	1	Enabl...	16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1		nutes a...	Success	11/28/2024 10...	Default Backup...	Windows Servers Backup

SUMMARY

Duration: 02:33

Processing rate: 2 MB/s

Bottleneck: Source

DATA

Processed:

Read:

Transferred:

STATUS

Success: 2

Warnings: 0

Errors: 0

Name	Status
winsrv006.tech.local	Success
winsrv001.tech.local	Success

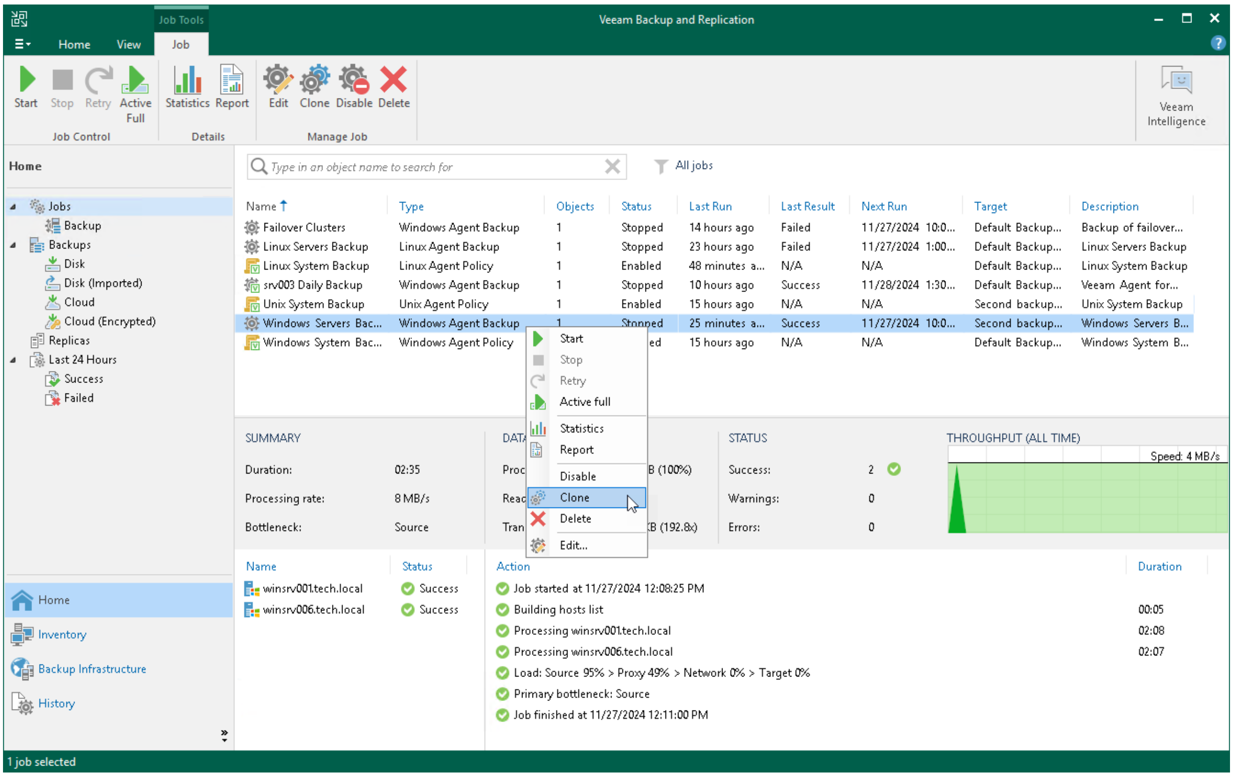
Action	Duration
Job started	
Building the	00:04
Processing winsrv001.tech.local	02:07
Processing winsrv006.tech.local	02:07
Load: Source 97% > Proxy 30% > Network 0% > Target 0%	
Primary bottleneck: Source	
Job finished at 11/28/2024 1:58:15 PM	

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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	23 hours ago	Failed	11/27/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	48 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup	1	Stopped	10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy	1	Enabled	15 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopped	25 minutes a...	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Policy		ed	15 hours ago	N/A	N/A	Default Backup...	Windows System B...

Duration:	02:35
Processing rate:	8 MB/s
Bottleneck:	Source

Proc... B (100%)
Read...
Tran... B (192.8x)

Success:	2
Warnings:	0
Errors:	0

Name	Status
winsrv001.tech.local	Success
winsrv006.tech.local	Success

Action	Duration
Job started at 11/27/2024 12:08:25 PM	
Building hosts list	00:05
Processing winsrv001.tech.local	02:08
Processing winsrv006.tech.local	02:07
Load: Source 95% > Proxy 49% > Network 0% > Target 0%	
Primary bottleneck: Source	
Job finished at 11/27/2024 12:11:00 PM	

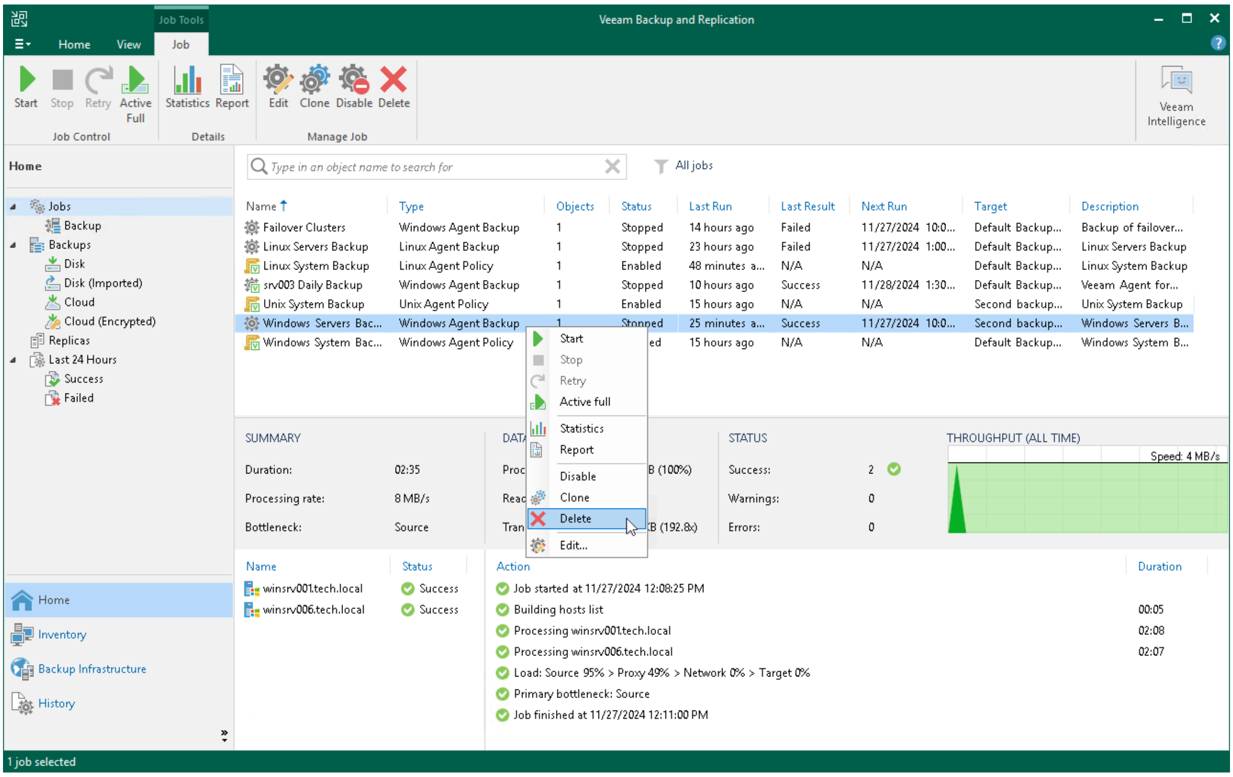
Removing Veeam Agent Backup Job

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.

When you remove a backup job, Veeam Backup & Replication does not delete Veeam Agent from computers protected by this backup job.

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**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	23 hours ago	Failed	11/27/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	48 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup	1	Stopped	10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy	1	Enabled	15 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopped	25 minutes a...	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Policy		ed	15 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Duration: 02:35

Processing rate: 8 MB/s

Bottleneck: Source

DATA

Proc B (100%)

Reac

Tran B (192.8x)

STATUS

Success: 2

Warnings: 0

Errors: 0

Name	Status
winsrv001.tech.local	Success
winsrv006.tech.local	Success

Action	Duration
Job started at 11/27/2024 12:08:25 PM	
Building hosts list	00:05
Processing winsrv001.tech.local	02:08
Processing winsrv006.tech.local	02:07
Load: Source 95% > Proxy 49% > Network 0% > Target 0%	
Primary bottleneck: Source	
Job finished at 11/27/2024 12:11:00 PM	

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:

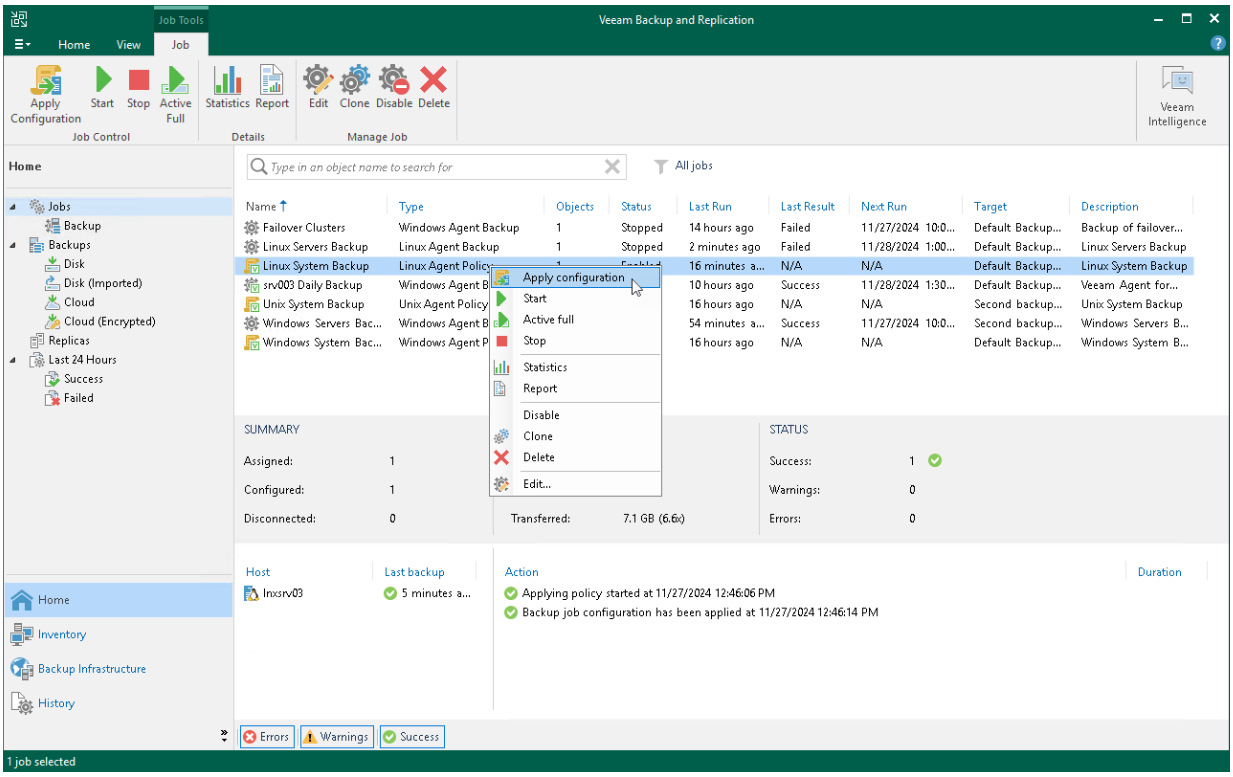
1. Open the **Home** view.

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.

> **TIP**
>
> If necessary, you can synchronize Veeam Agent with Veeam Backup & Replication running a command from the Veeam Agent computer. To learn more, see Backup Policy Application Methods.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	2 minutes ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	16 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent B			10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy			16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent B			54 minutes a...	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent P			16 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1

Configured: 1

Disconnected: 0

Transferred: 7.1 GB (6.6x)

STATUS

Success: 1

Warnings: 0

Errors: 0

Host	Last backup	Action	Duration
lnxsrv03	5 minutes a...	Applying policy started at 11/27/2024 12:46:06 PM	
		Backup job configuration has been applied at 11/27/2024 12:46:14 PM	

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**.

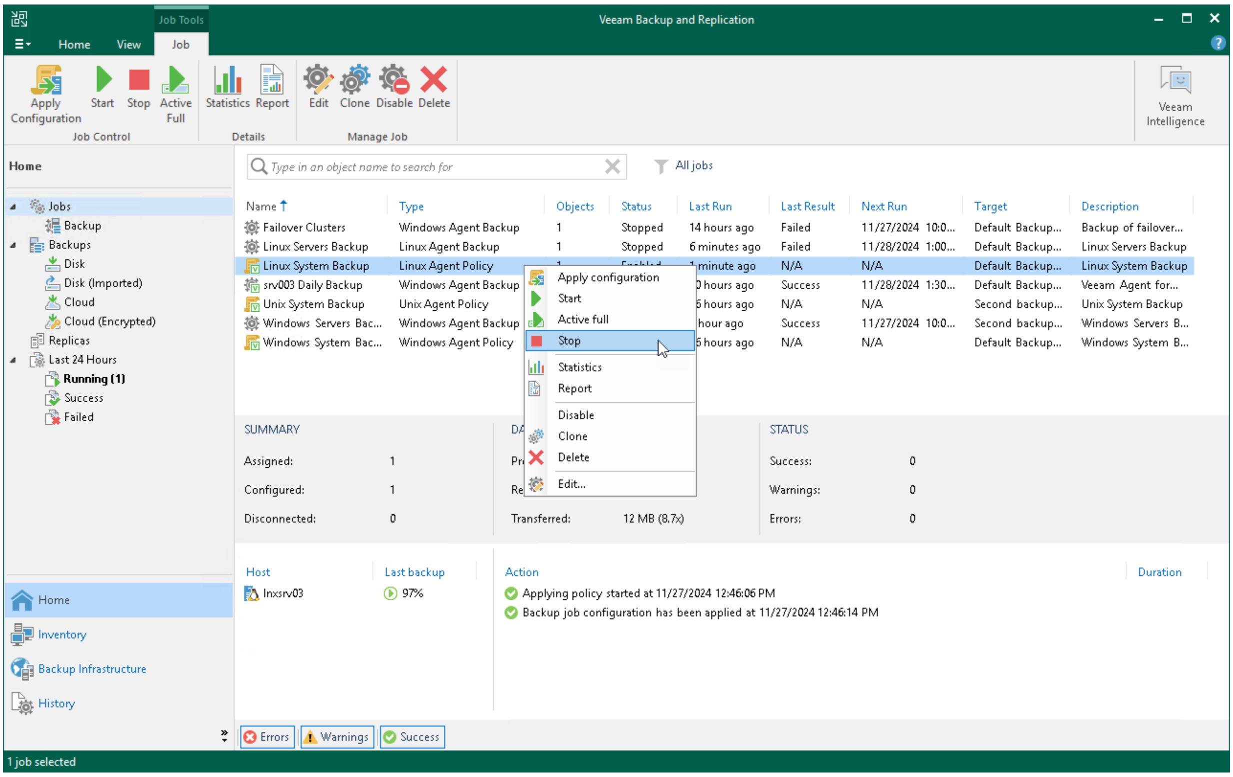
> **TIP**
>
> You can also start a Veeam Agent backup job directly on a protected computer from the Veeam Agent user interface.

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**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	6 minutes ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	1 minute ago	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup			0 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy			5 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup			hour ago	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Policy			5 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1

Configured: 1

Disconnected: 0

DA

Pr

Re

Transferred: 12 MB (8.7x)

STATUS

Success: 0

Warnings: 0

Errors: 0

Host	Last backup
lnxsrv03	97%

Action	Duration
Applying policy started at 11/27/2024 12:46:06 PM	
Backup job configuration has been applied at 11/27/2024 12:46:14 PM	

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.

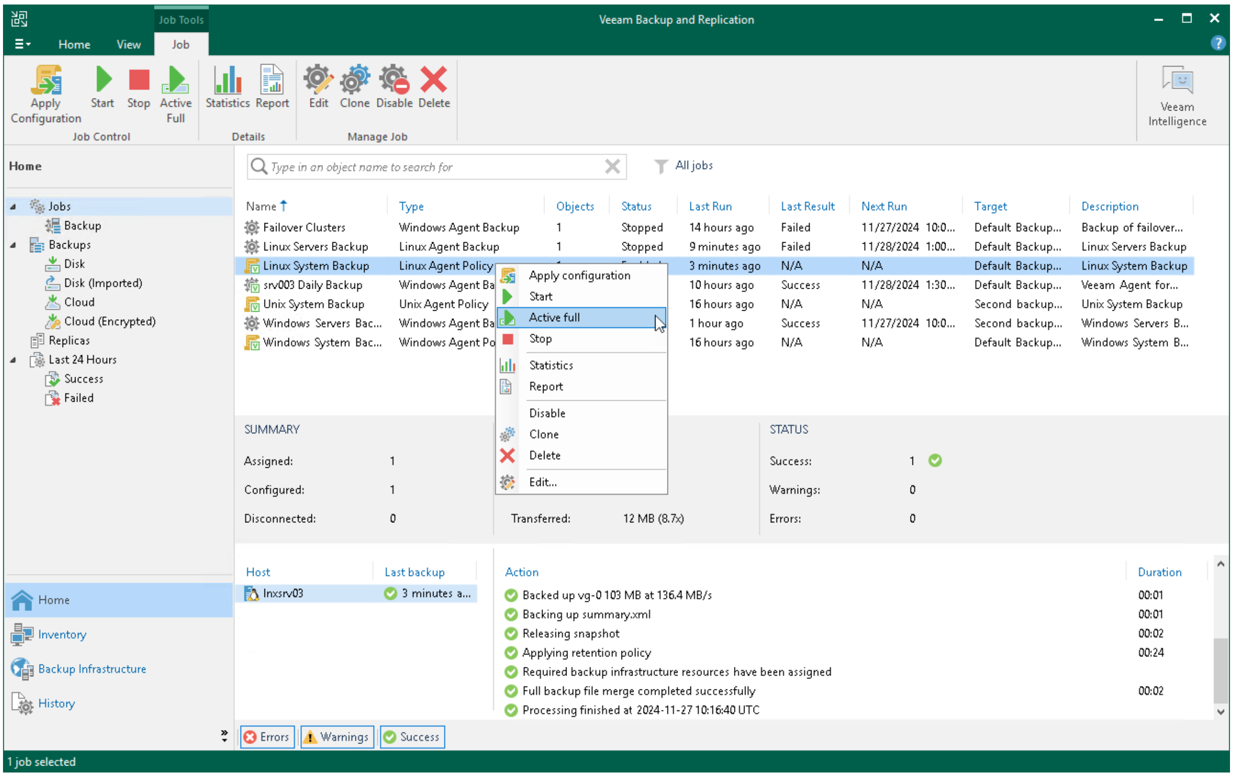
When you start active full backup for a backup policy, Veeam Backup & Replication applies the policy to Veeam Agent computers and sends a command to perform active full backup on these computers. Veeam Backup & Replication does not check whether connection to Veeam Agent computers is active at the time 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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	9 minutes ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy			3 minutes ago	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Ba			10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy			16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Ba			1 hour ago	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Po			16 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1
Configured: 1
Disconnected: 0

Transferred: 12 MB (8.7x)

STATUS

Success: 1
Warnings: 0
Errors: 0

Host	Last backup
lnxsrv03	3 minutes a...

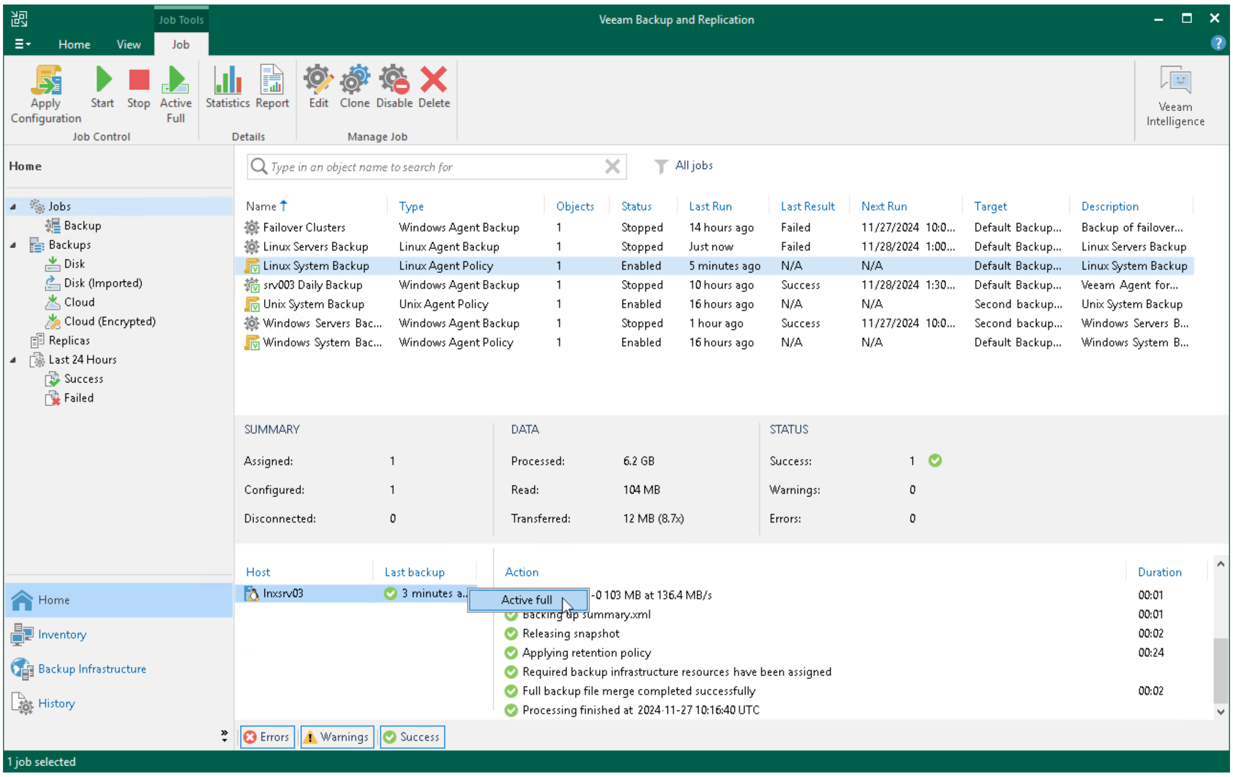
Action	Duration
Backed up vg-0 103 MB at 136.4 MB/s	00:01
Backing up summary.xml	00:01
Releasing snapshot	00:02
Applying retention policy	00:24
Required backup infrastructure resources have been assigned	
Full backup file merge completed successfully	00:02
Processing finished at 2024-11-27 10:16:40 UTC	

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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	Just now	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	5 minutes ago	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup	1	Stopped	10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy	1	Enabled	16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopped	1 hour ago	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Policy	1	Enabled	16 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY		DATA		STATUS	
Assigned:	1	Processed:	6.2 GB	Success:	1 ✓
Configured:	1	Read:	104 MB	Warnings:	0
Disconnected:	0	Transferred:	12 MB (8.7x)	Errors:	0

Host	Last backup	Action	Duration
lnxsrv03	✓ 3 minutes a...	-0 103 MB at 136.4 MB/s	00:01
		✓ Backing up summary.xml	00:01
		✓ Releasing snapshot	00:02
		✓ Applying retention policy	00:24
		✓ Required backup infrastructure resources have been assigned	
		✓ Full backup file merge completed successfully	00:02
		✓ Processing finished at 2024-11-27 10:16:40 UTC	

Clearing Backup Cache

You can use the Veeam backup console to delete restore points from the backup cache on computers added to the backup policy. This operation may be required, for example, if the backup cache contains one or more restore points, and the backup chain in the target location has changed prior to the time when Veeam Agent starts uploading restore points to the target location.

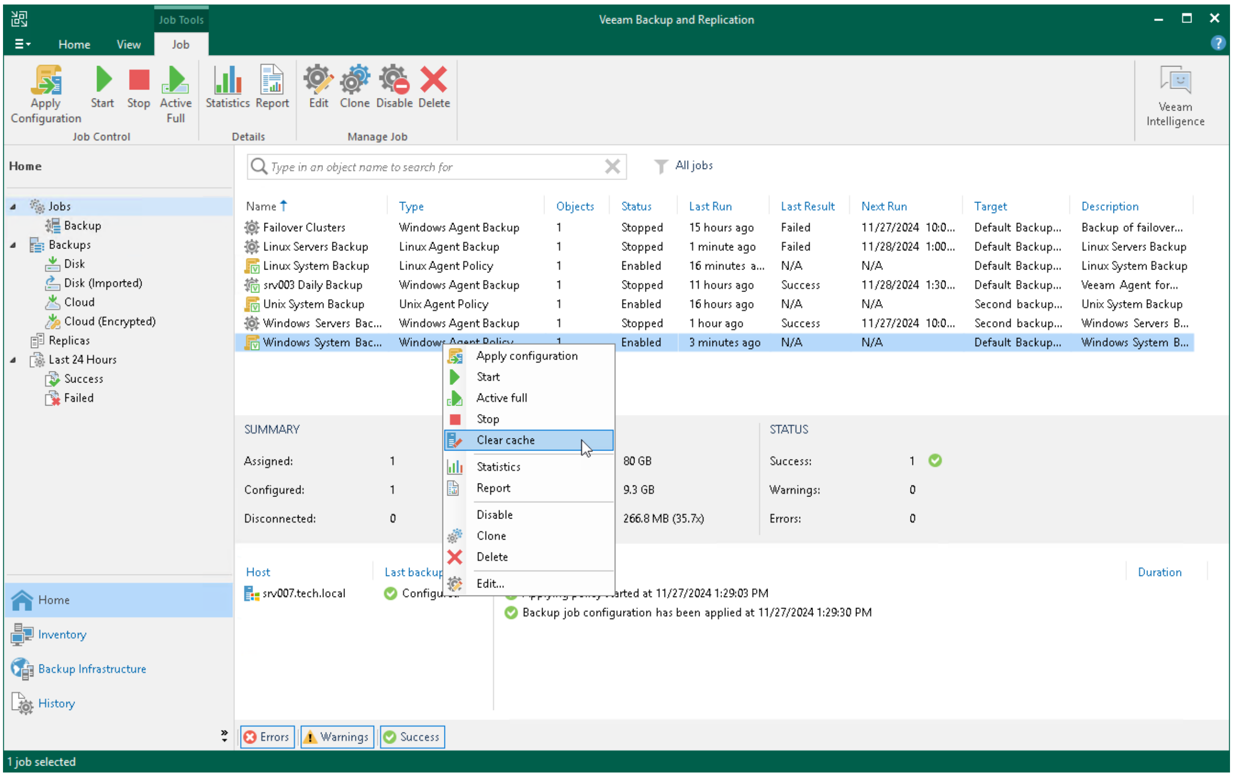
Keep in mind that the clear cache operation is available only for computers that are protected with Veeam Agent for Microsoft Windows and are members of any protection group excluding protection group for pre-installed Veeam Agents.

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 learn more, see Backup Cache.

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, select the backup policy, press and hold the [Ctrl] key, right-click the backup policy and select **Clear cache**.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	15 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	1 minute ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	16 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent Backup	1	Stopped	11 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy	1	Enabled	16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent Backup	1	Stopped	1 hour ago	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent Policy	1	Enabled	3 minutes ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1
Configured: 1
Disconnected: 0

80 GB
9.3 GB
266.8 MB (35.7x)

STATUS

Success: 1 ✓
Warnings: 0
Errors: 0

Host	Last backup		Duration
srv007.tech.local	✓ Configu...	✓ ...arted at 11/27/2024 1:29:03 PM ✓ Backup job configuration has been applied at 11/27/2024 1:29:30 PM	

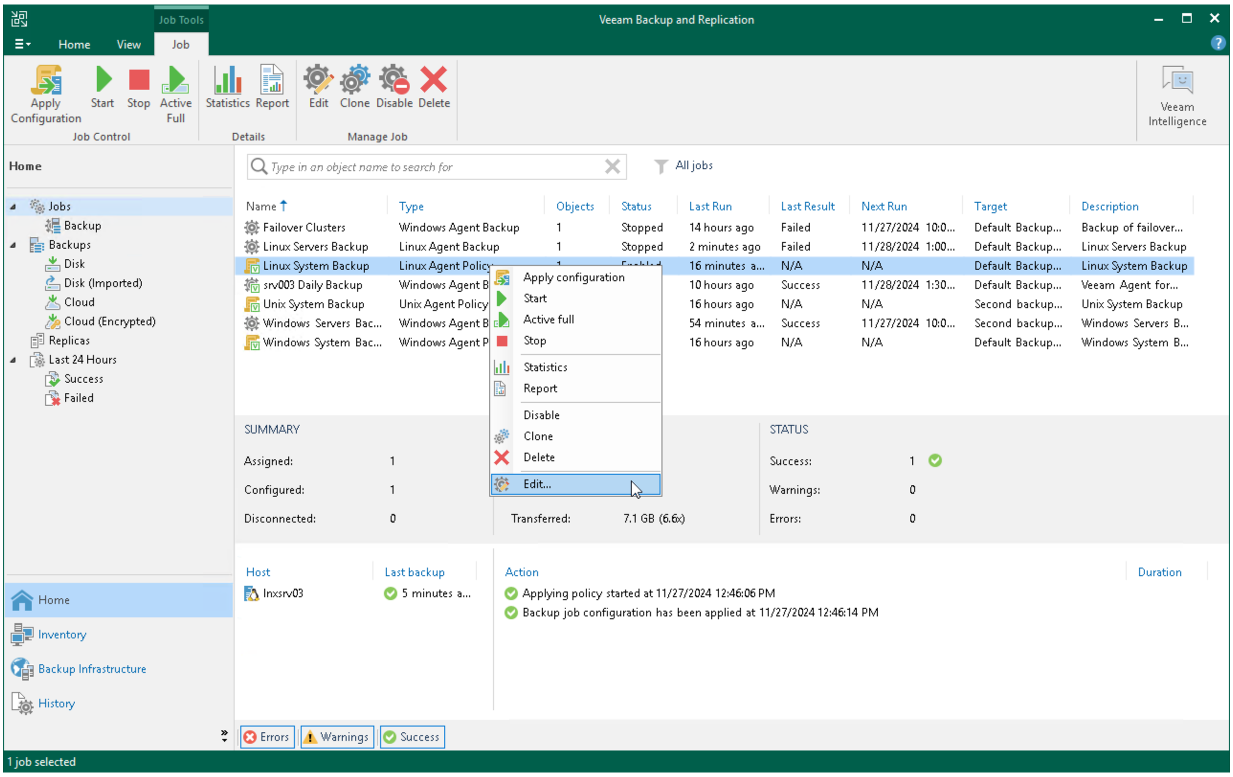
Editing Backup Policy Settings

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**
>
> Consider 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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	2 minutes ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	16 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent B			10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy			16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent B			54 minutes a...	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent P			16 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1

Configured: 1

Disconnected: 0

Transferred: 7.1 GB (6.6x)

STATUS

Success: 1

Warnings: 0

Errors: 0

Host	Last backup	Action	Duration
lnxsrv03	5 minutes a...	Applying policy started at 11/27/2024 12:46:06 PM	
		Backup job configuration has been applied at 11/27/2024 12:46:14 PM	

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**.

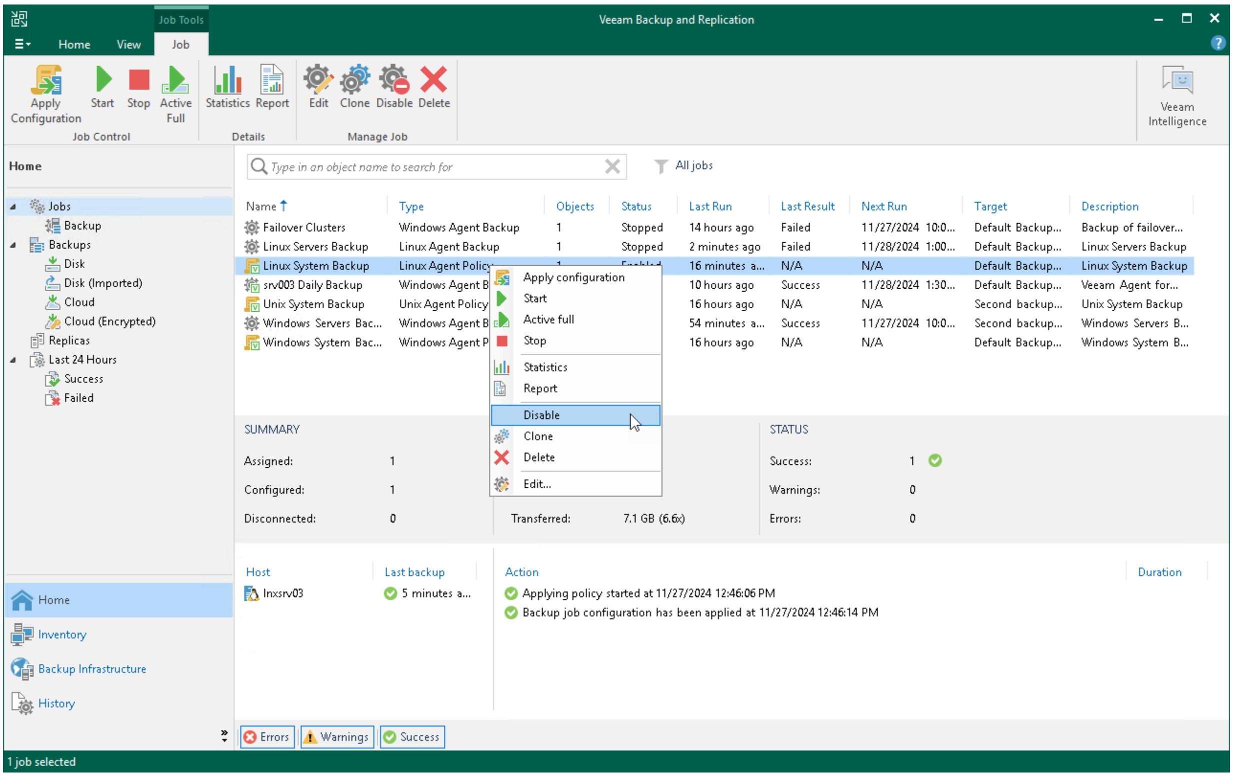
   Keep in mind that Veeam Backup & Replication does not immediately disable a backup policy for protection groups for pre-installed Veeam Agents and their members. Veeam Agents installed on computers included in these groups connect to Veeam Backup & Replication every 6 hours and get updated backup policy 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.

   > TIP
   >
   > If necessary, you can synchronize Veeam Agent with Veeam Backup & Replication running a command from the Veeam Agent computer. To learn more, see Backup Policy Application Methods.

   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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	2 minutes ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	16 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent B			10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy			16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent B			54 minutes a...	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent P			16 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1

Configured: 1

Disconnected: 0

Transferred: 7.1 GB (6.6x)

STATUS

Success: 1 ✓

Warnings: 0

Errors: 0

Host	Last backup
lnxsrv03	✓ 5 minutes a...

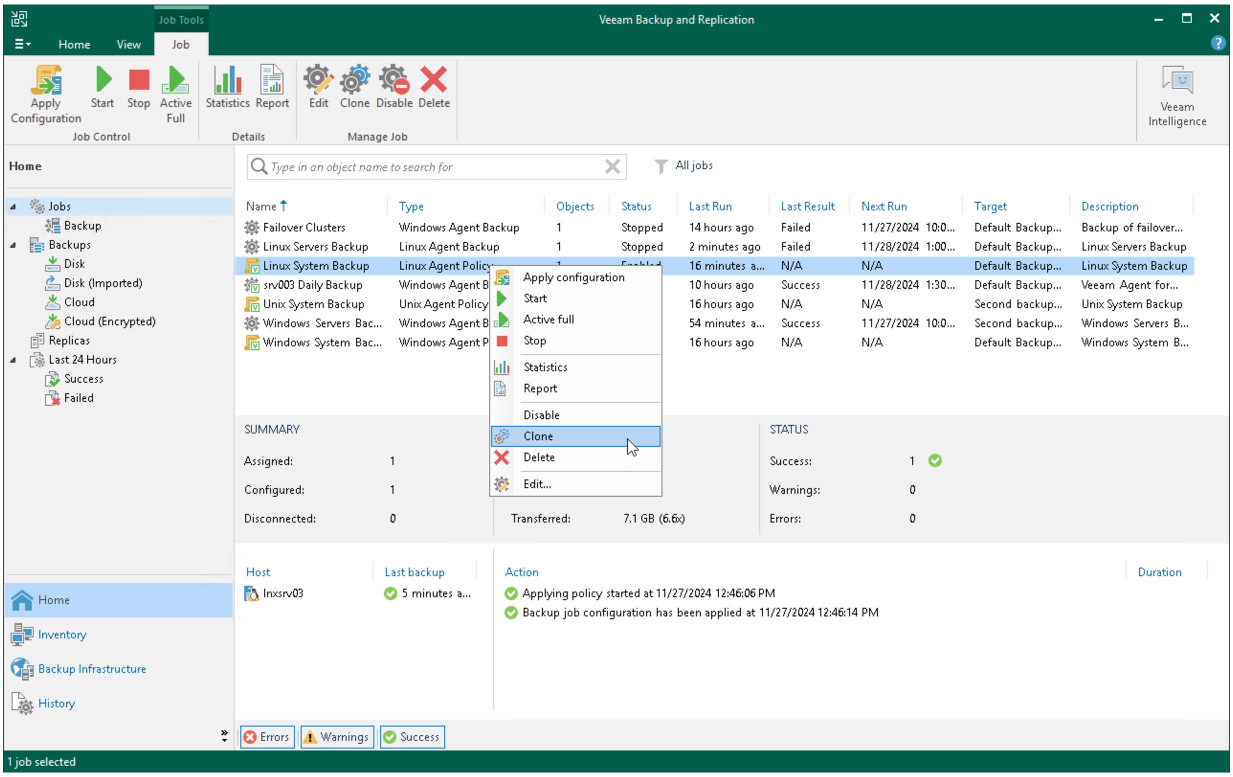
Action	Duration
✓ Applying policy started at 11/27/2024 12:46:06 PM	
✓ Backup job configuration has been applied at 11/27/2024 12:46:14 PM	

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.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	2 minutes ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy			16 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent B			10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy			16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent B			54 minutes a...	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent P			16 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1

Configured: 1

Disconnected: 0

Transferred: 7.1 GB (6.6x)

STATUS

Success: 1 ✓

Warnings: 0

Errors: 0

Host	Last backup
lnxsrv03	✓ 5 minutes a...

Action	Duration
✓ Applying policy started at 11/27/2024 12:46:06 PM	
✓ Backup job configuration has been applied at 11/27/2024 12:46:14 PM	

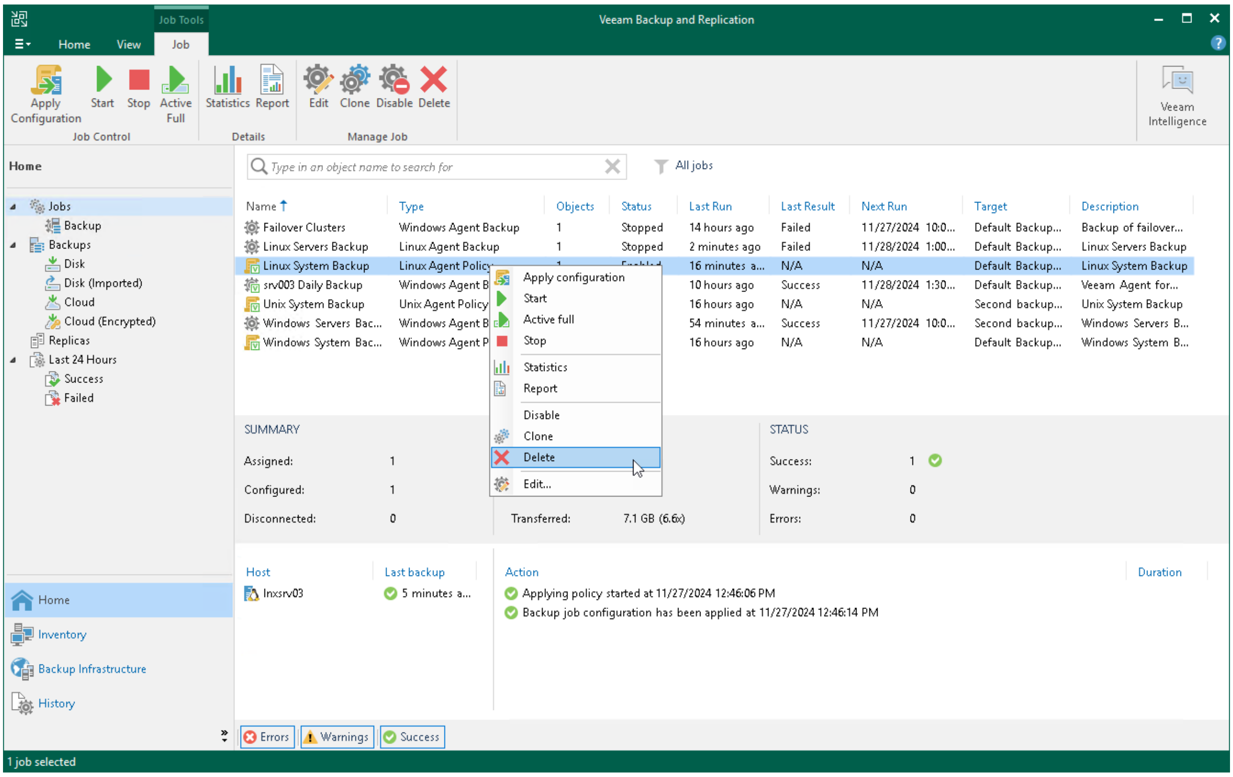
Removing Backup Policy

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**.

> **NOTE**
>
> [For computers with pre-installed Veeam Agents] The child jobs will continue running till the next synchronization with Veeam Backup & Replication.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
Failover Clusters	Windows Agent Backup	1	Stopped	14 hours ago	Failed	11/27/2024 10:0...	Default Backup...	Backup of failover...
Linux Servers Backup	Linux Agent Backup	1	Stopped	2 minutes ago	Failed	11/28/2024 1:00...	Default Backup...	Linux Servers Backup
Linux System Backup	Linux Agent Policy	1	Enabled	16 minutes a...	N/A	N/A	Default Backup...	Linux System Backup
srv003 Daily Backup	Windows Agent B			10 hours ago	Success	11/28/2024 1:30...	Default Backup...	Veeam Agent for...
Unix System Backup	Unix Agent Policy			16 hours ago	N/A	N/A	Second backup...	Unix System Backup
Windows Servers Bac...	Windows Agent B			54 minutes a...	Success	11/27/2024 10:0...	Second backup...	Windows Servers B...
Windows System Bac...	Windows Agent P			16 hours ago	N/A	N/A	Default Backup...	Windows System B...

SUMMARY

Assigned: 1

Configured: 1

Disconnected: 0

Transferred: 7.1 GB (6.6x)

STATUS

Success: 1

Warnings: 0

Errors: 0

Host	Last backup	Action	Duration
lnxsrv03	5 minutes a...	Applying policy started at 11/27/2024 12:46:06 PM Backup job configuration has been applied at 11/27/2024 12:46:14 PM	

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 a 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.
- Uninstalling Veeam Agent and other Veeam Components from 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 a computer to a protection group.
- Add a protected computer to a Veeam Agent backup job.
- View properties of a protected computer.

Moving Computer to Protection Group

You can quickly move an unmanaged Veeam Agent computer or a computer from a protection group for pre-installed Veeam Agents to a protection group in the Veeam Backup & Replication inventory. Keep in mind, that you can move a Veeam Agent computer only to a protection group that includes individual computers or a protection group for pre-installed Veeam Agents. You can move computers in the following way:

- If you want to move computers to a protection group for individual computers, use the Veeam Backup & Replication console. In this case, you can move unmanaged computers, or Veeam Agent for Microsoft Windows or Veeam Agent for Linux computers from protection groups for pre-installed Veeam Agents.
- If you want to move computers to a protection group for pre-installed Veeam Agents, do it 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 to a new protection group or protection group that you have already created.

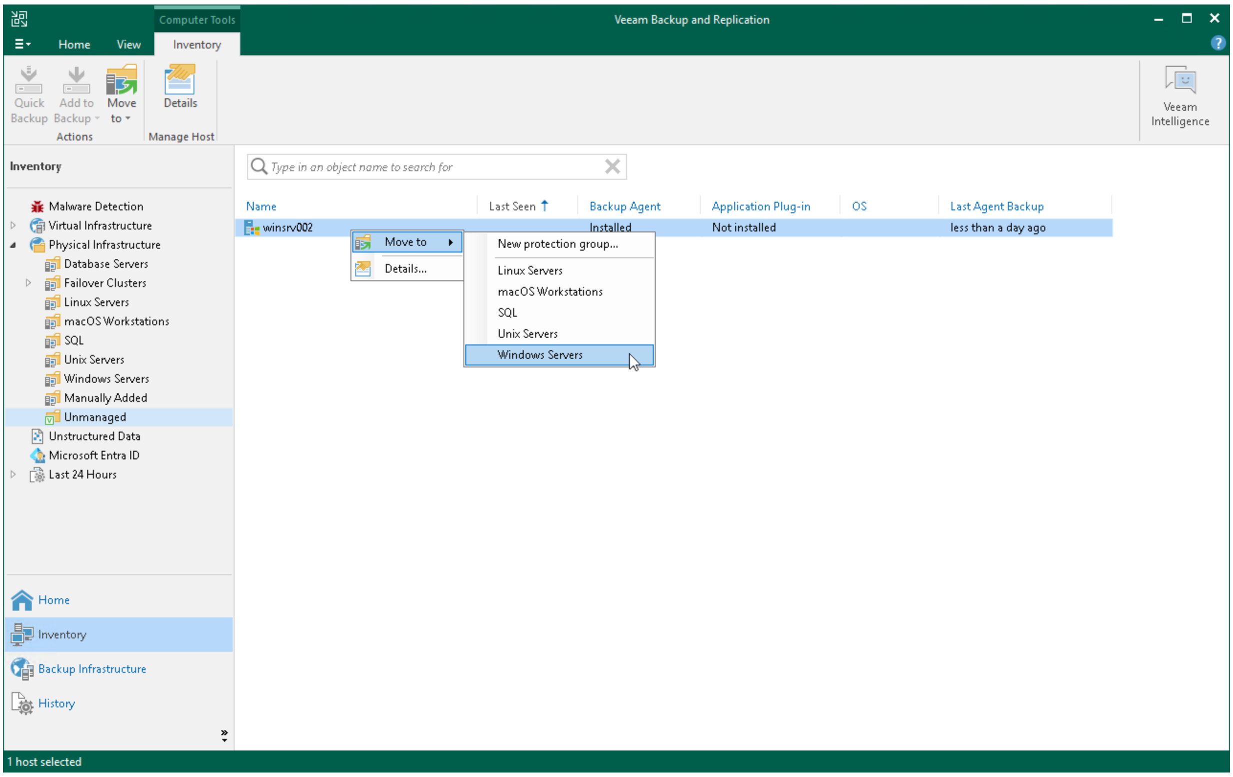
- When you move a computer to a new protection group, Veeam Backup & Replication creates the protection group and adds the computer to this group. In the protection group settings, you can define discovery and deployment options according to which Veeam Backup & Replication will process the added computer.
- When you move a 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 a computer to a protection group:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the protection group that includes the Veeam Agent computer that you want to move.
3. Do either of the following
   - If you want to move a computer to a new protection group, 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**.

- If you want to move a computer to a protection group that is already created in the inventory, 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*.

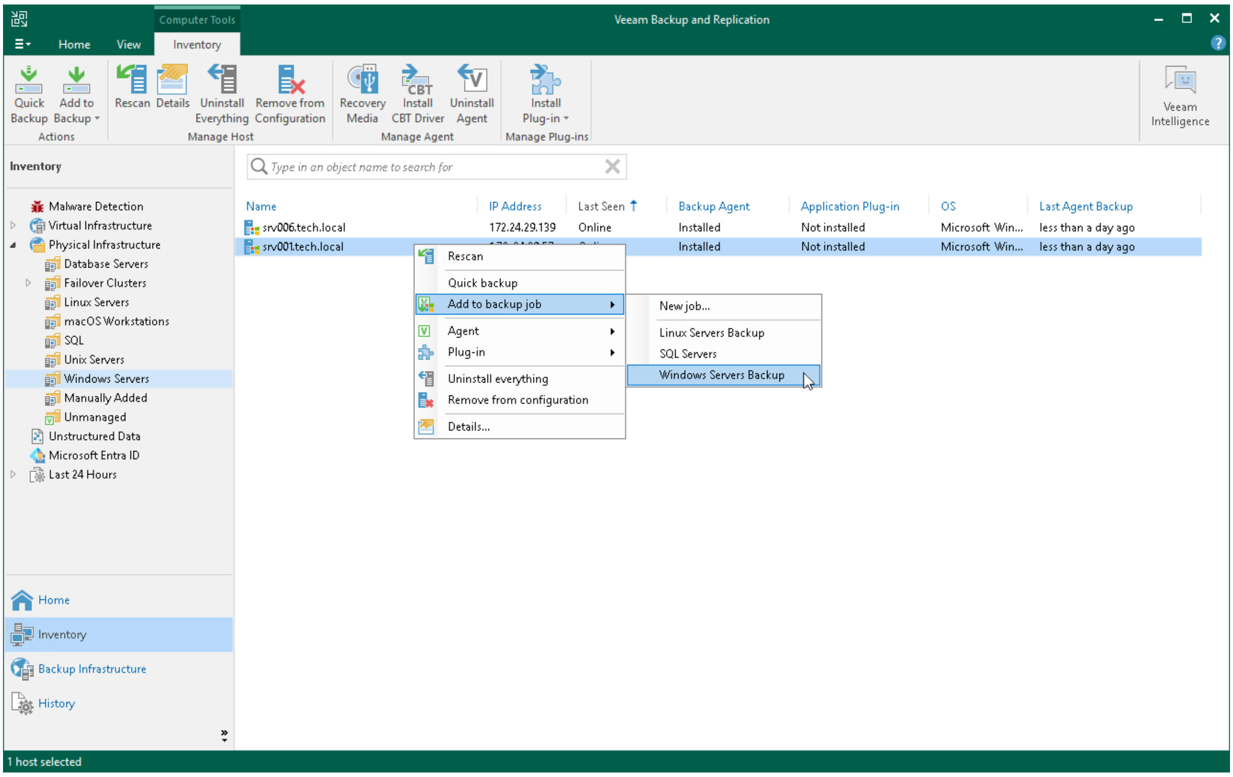


Adding Computer to Backup Job

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 Working with Veeam Agent Backup Jobs and Policies.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local	[illegible]	[illegible]	Installed	Not installed	Microsoft Win...	less than a day ago

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:

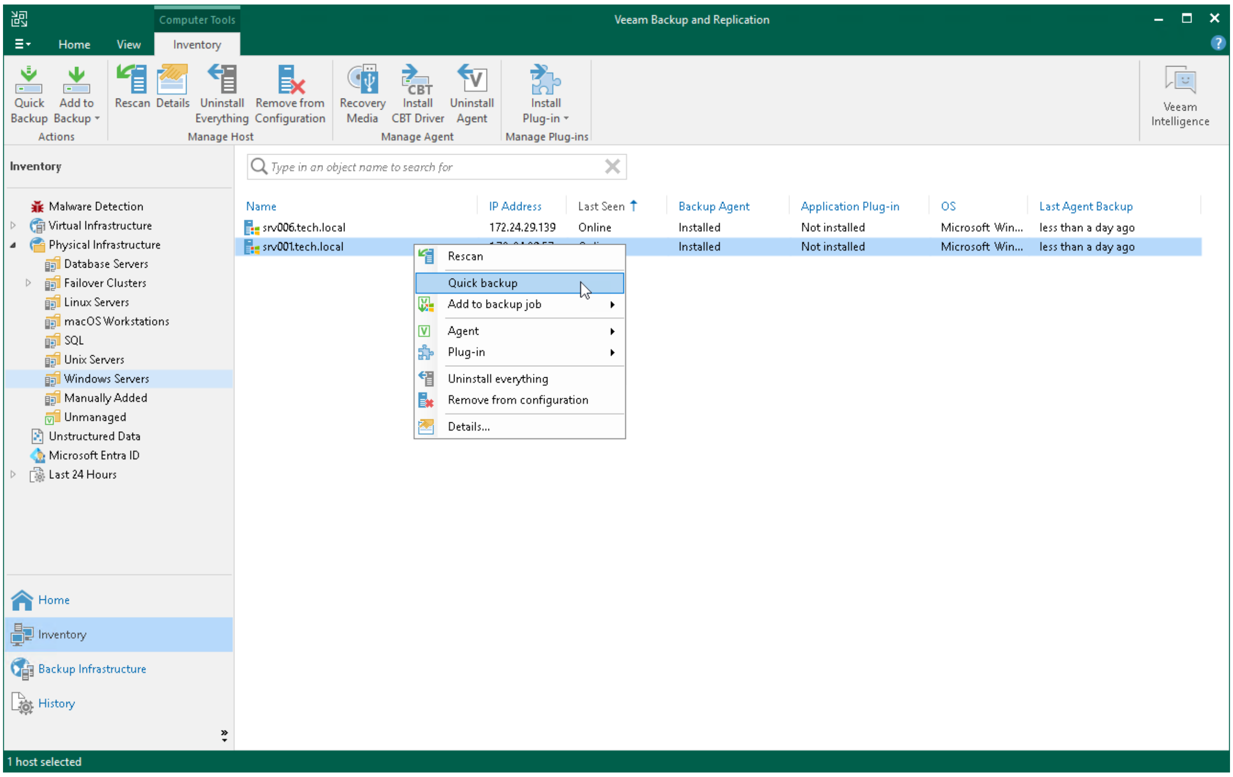
- A protected computer is added to a Veeam Agent backup job managed by the backup server.
- A full backup file for the protected computer exists on the backup repository configured in the backup infrastructure and is mapped to a backup job managed by the backup server.

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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local			Installed	Not installed	Microsoft Win...	less than a day ago

Viewing Properties

You can view detailed information about protected computers. The detailed information provides the following data:

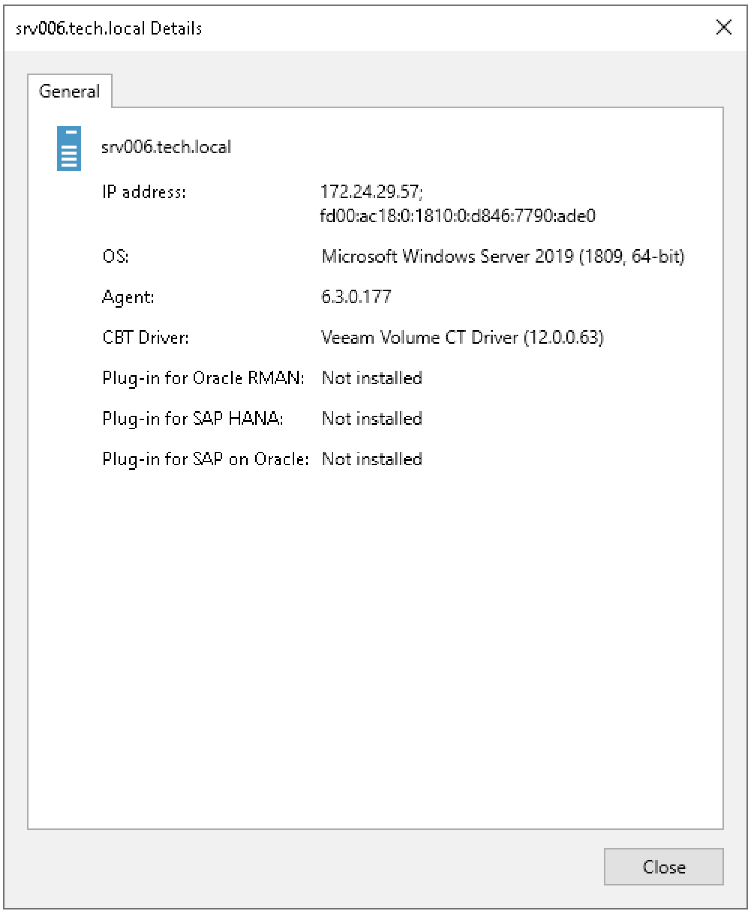
- Host name
- IP address
- Fingerprint — for computers running a Linux OS
- Key algorithm — for computers running a Linux OS
- Operating system
- Veeam Agent version
- CBT driver version — for computers running a Microsoft Windows Server OS

> NOTE
>
> **IP address** and **Fingerprint** information does not apply to members of protection groups for pre-installed Veeam Agents and cloud machines. **Key algorithm** information does not apply to members of protection groups for pre-installed Veeam Agents.

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**.



srv006.tech.local Details

General

srv006.tech.local

IP address:	172.24.29.57; fd00:ac18:0:1810:0:d846:7790:ade0
OS:	Microsoft Windows Server 2019 (1809, 64-bit)
Agent:	6.3.0.177
CBT Driver:	Veeam Volume CT Driver (12.0.0.63)
Plug-in for Oracle RMAN:	Not installed
Plug-in for SAP HANA:	Not installed
Plug-in for SAP on Oracle:	Not installed

Rescanning Protected Computer

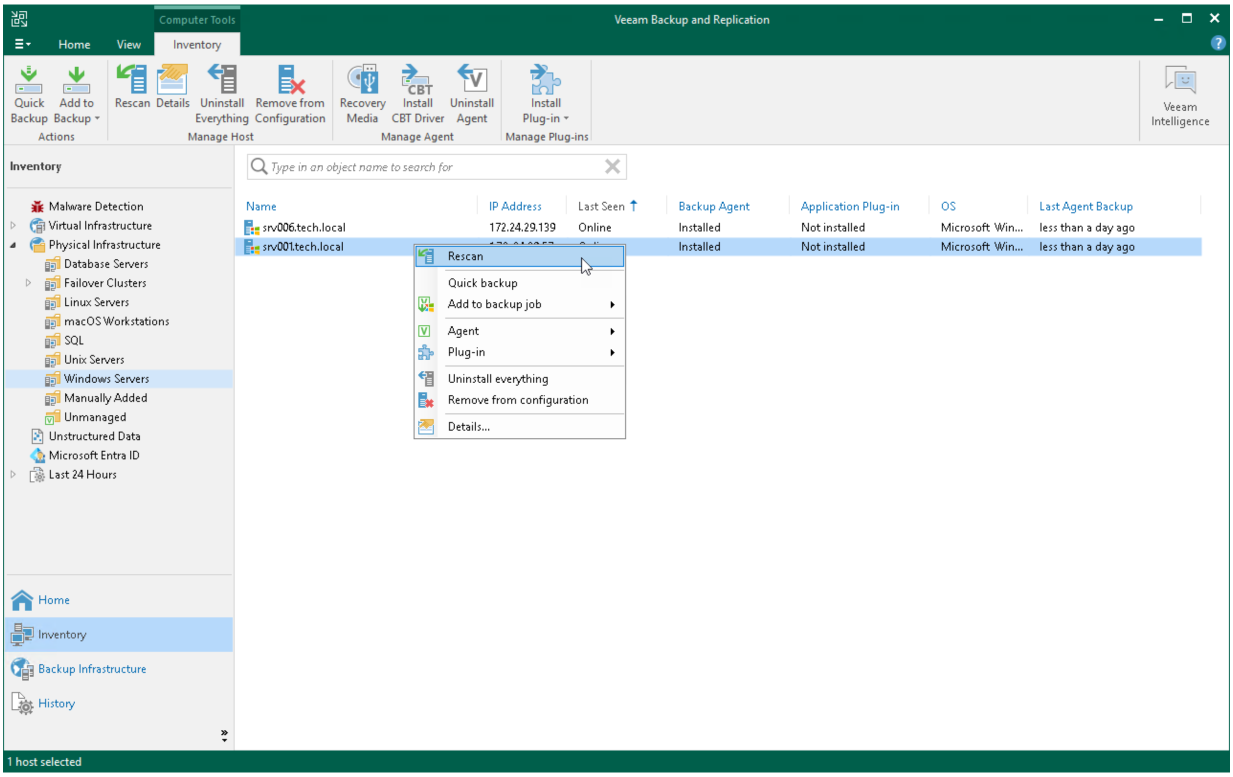
You can rescan protected computers added to the inventory. The rescan operation may be required, for example, if you want to refresh information about the protected computer in the Veeam Backup & Replication database. During the rescan operation, Veeam Backup & Replication communicates to Veeam Installer 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. If necessary, you can synchronize Veeam Agent with Veeam Backup & Replication running a command from the Veeam Agent computer. To learn more, see Backup Policy Application Methods.

> **NOTE**
>
> During the rescan of a separate protected computer, Veeam Backup & Replication does not perform deployment operations specified in the protection group settings. To perform the deployment operations, rescan the protection group.

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**.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local	[illegible]	[illegible]	Installed	Not installed	Microsoft Win...	less than a day ago

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
- Veeam Agent for Unix

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.

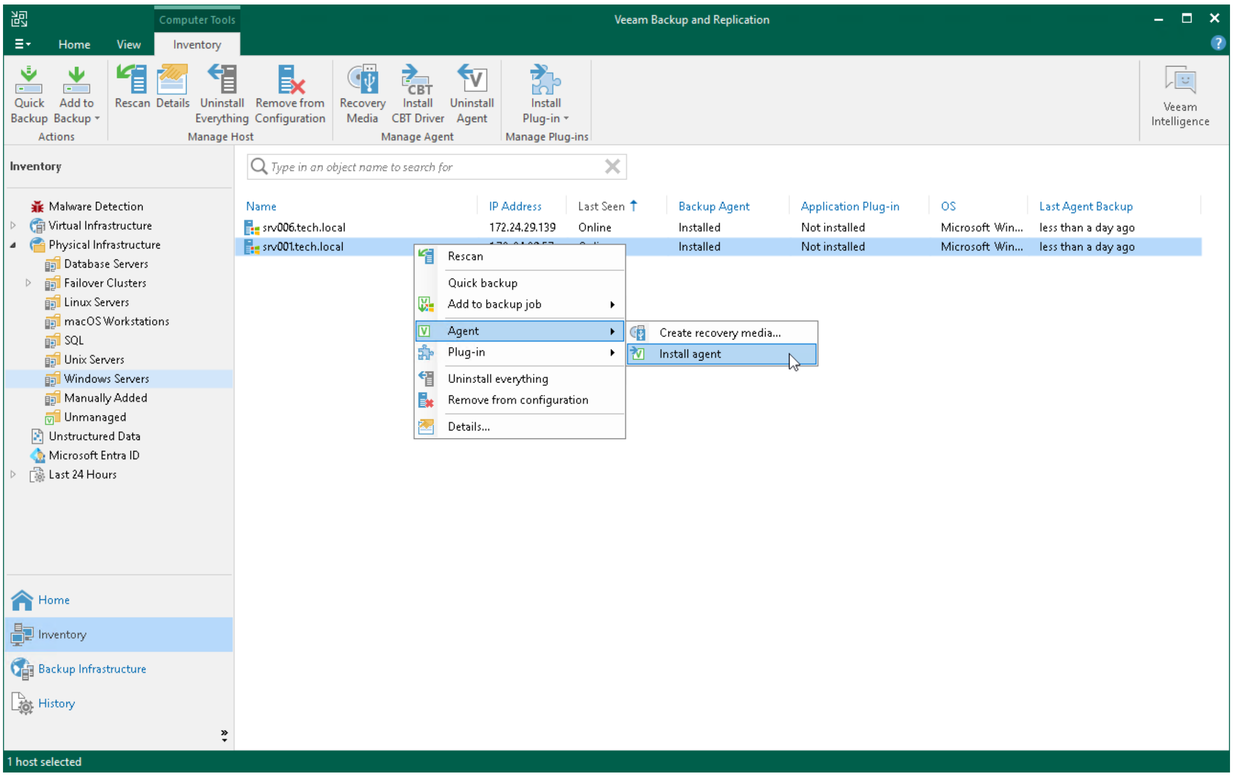
Before you install Veeam Agent, check the following prerequisites:

- 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.
>
> You can instruct Veeam Backup & Replication to automatically reboot the Veeam Agent computer. To do so, select the **Perform reboot automatically if required** check box in the protection group settings.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local	[illegible]	[illegible]	Installed	Not installed	Microsoft Win...	less than a day ago

Upgrading Veeam Agent

Depending on your infrastructure setup, you can upgrade Veeam Agent in the following ways:

- From the Veeam Backup & Replication console
- On the Veeam Agent computer side

Upgrading from Veeam Backup & Replication Console

In the Veeam Backup & Replication console, you can upgrade Veeam Agent on the computers that are added to a protection group of one of the following types:

- Protection group for individual computers (Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris)
- Protection group for computers from CSV file (Veeam Agent for Microsoft Windows, Veeam Agent for Linux, Veeam Agent for IBM AIX and Veeam Agent for Oracle Solaris)
- Protection group for Microsoft Active Directory objects (Veeam Agent for Microsoft Windows)
- Protection group for cloud machines (Veeam Agent for Microsoft Windows and Veeam Agent for Linux)

Automatic and Manual Upgrades

From the Veeam Backup & Replication console, you can upgrade Veeam Agent on a protected computer in two ways:

- Automatically — You can use this method to upgrade all outdated Veeam Agents on computers in a protection group. To enable Veeam Agent auto updates, select the **Auto-update backup agents and plug-ins** option in the protection group settings. For more information, see Creating Protection Groups.
- Manually — You can upgrade Veeam Agent on an individual computer in a protection group. This method may be required, for example, if you did not allow Veeam Backup & Replication to automatically upgrade Veeam Agent on computers included in the protection group and want to test the upgrade process on a selected computer first.

Before You Begin

Before you upgrade Veeam Agent, verify the following:

- The protected computer is powered on and able to be connected over the network.
- 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 Veeam Backup & Replication server. If a newer version of Veeam Agent becomes available, 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.

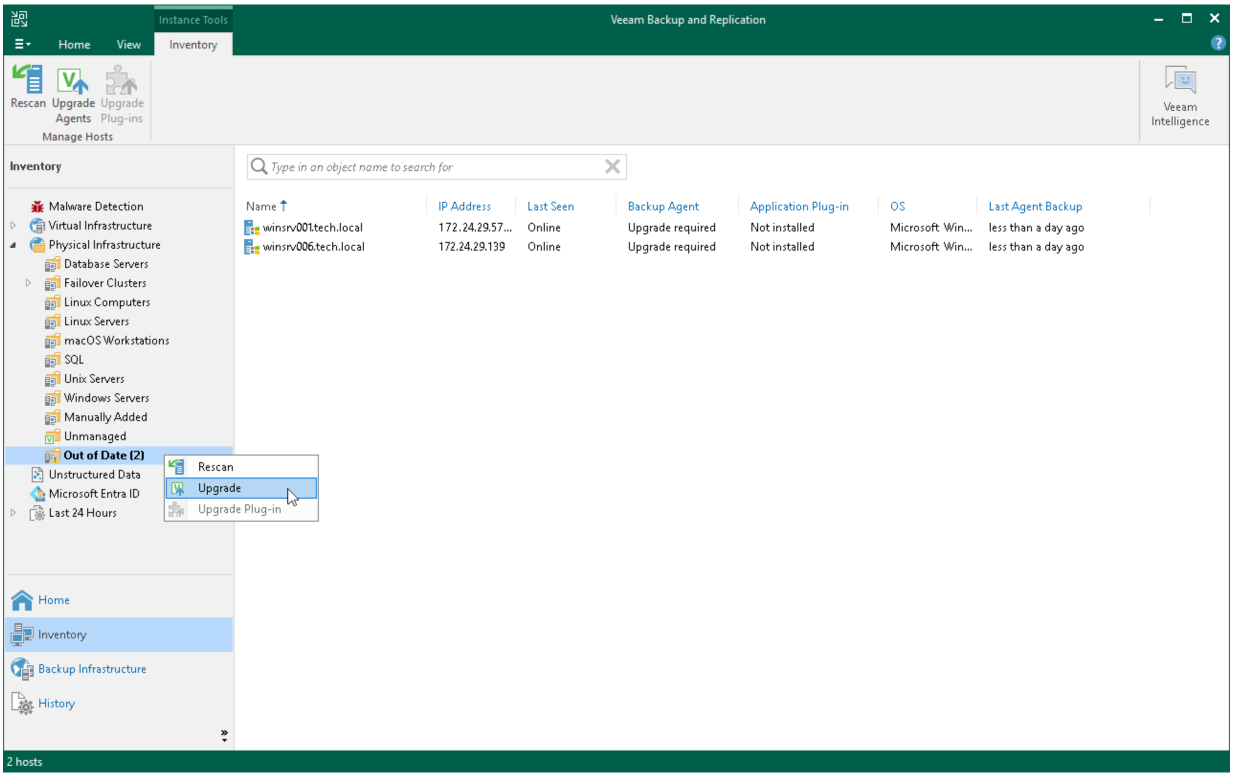
Upgrading Veeam Agent on Multiple Computers

You can automatically 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 a new version of Veeam Agent for Microsoft Windows may require computer reboot.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
winsrv001.tech.local	172.24.29.57...	Online	Upgrade required	Not installed	Microsoft Win...	less than a day ago
winsrv006.tech.local	172.24.29.139	Online	Upgrade required	Not installed	Microsoft Win...	less than a day ago

Upgrading Veeam Agent on Individual Computers

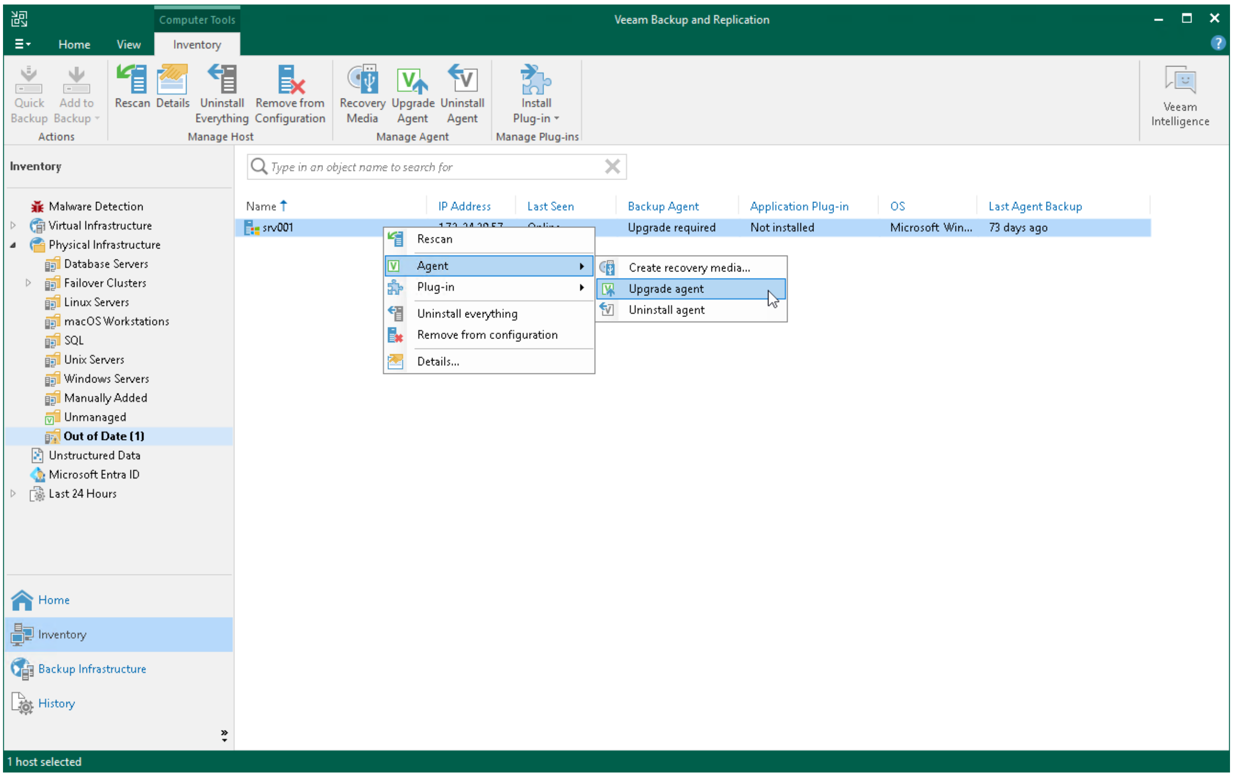
To upgrade Veeam Agent on a protected computer:

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 a new version of Veeam Agent for Microsoft Windows may require computer reboot.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv001	172.24.29.57	Online	Upgrade required	Not installed	Microsoft Win...	73 days ago

Upgrading on Protected Computer Side

You must perform the upgrade of Veeam Agent on the computers added to protection groups for pre-installed Veeam Agents on the protected computer side.

> **NOTE**
>
> Upgrade of Veeam Agent on the protected computer side is the only option available for Veeam Agent for Mac.

> **TIP**
>
> During each 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 Begin

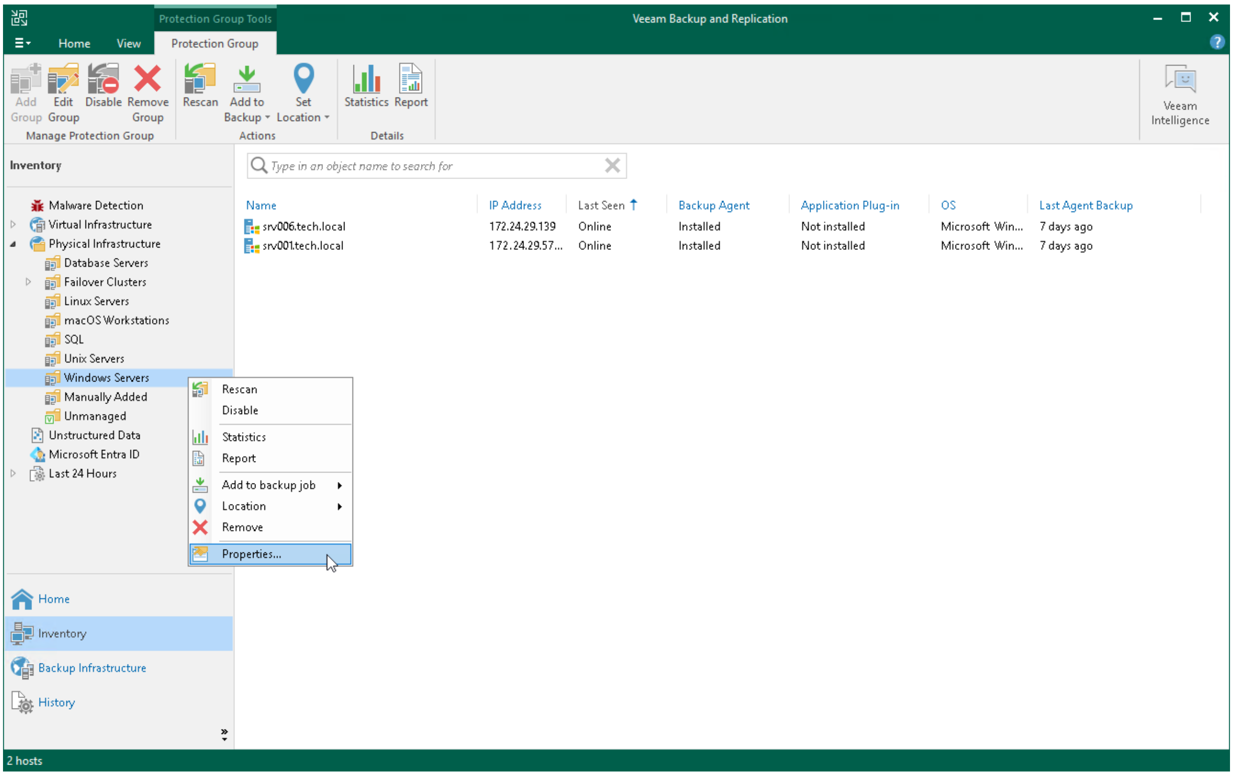
Before you upgrade pre-installed Veeam Agent, do the following:

- Check that the latest update for Veeam Backup & Replication is installed on your backup server. To learn more, see the Upgrading to Veeam Backup & Replication 12.3 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 Administrator privileges.

Updating Protection Group Settings

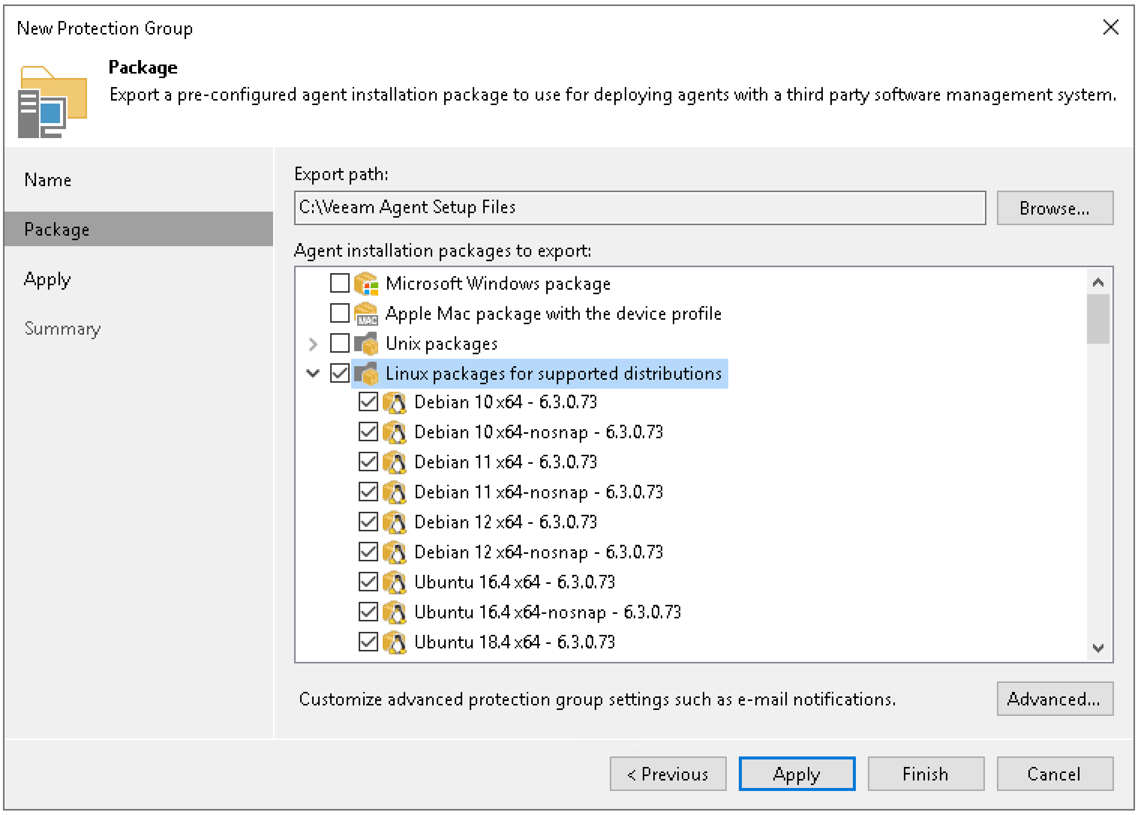
To update pre-installed Veeam Agent, you must generate new Veeam Agent setup files on the Veeam Backup & Replication side. To do so, edit the protection group settings:

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**.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

4. At the **Package** step, check that the export path and setup files for OSes that run on computers with Veeam Agents you want to update are specified correctly.



New Protection Group

Package

Export a pre-configured agent installation package to use for deploying agents with a third party software management system.

Export path: C:\Veeam Agent Setup Files

Agent installation packages to export:

- □ Microsoft Windows package
- □ Apple Mac package with the device profile
- □ Unix packages
- ☑ Linux packages for supported distributions
  - ☑ Debian 10 x64 - 6.3.0.73
  - ☑ Debian 10 x64-nosnap - 6.3.0.73
  - ☑ Debian 11 x64 - 6.3.0.73
  - ☑ Debian 11 x64-nosnap - 6.3.0.73
  - ☑ Debian 12 x64 - 6.3.0.73
  - ☑ Debian 12 x64-nosnap - 6.3.0.73
  - ☑ Ubuntu 16.4 x64 - 6.3.0.73
  - ☑ Ubuntu 16.4 x64-nosnap - 6.3.0.73
  - ☑ Ubuntu 18.4 x64 - 6.3.0.73

Customize advanced protection group settings such as e-mail notifications.

5. Click **Apply** to generate setup files. Then click **Finish** to close the wizard.

Upgrading Veeam Agent on the Protected Computer Side

On the Veeam Agent computer side, the update procedure differs depending on the OS of the protected computer:

- Upgrade procedure for Microsoft Windows computers
- Upgrade procedure for Linux computers
- Upgrade procedure for Unix computers with IBM AIX OS
- Upgrade procedure for Unix computers with Oracle Solaris OS
- Upgrade procedure for Mac computers

Windows Computers

To update pre-installed Veeam Agent on a Microsoft Windows computer, perform the following operations:

1. Upload the Veeam Agent setup files on the computer you want to protect.
2. 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.

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/<Veeam Agent version>/VAW` folder.
   - [For 64-bit Windows] Double-click the `Veeam_B&R_Endpoint_x64.msi` file located in the `<path_to_setup_files>/Windows/<Veeam Agent version>/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" -syn
cnow
```

Linux Computers

To update pre-installed Veeam Agent on a 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. To learn more, see the Installing Veeam Agent for Linux in Offline Mode section in the Veeam Agent for Linux User Guide.
3. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
veeamconfig mode syncnow
```

Unix Computers with IBM AIX OS

To update pre-installed Veeam Agent on a Unix computer that runs an IBM AIX operating system, 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 the setup files and install Veeam Agent using the `rpm` command with the `-U` parameter. To learn more, see the Upgrading Product topic in the Veeam Agent for IBM AIX User Guide.
3. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
veeamconfig mode syncnow
```

Unix Computers with Oracle Solaris OS

To update pre-installed Veeam Agent on a Unix computer that runs an Oracle Solaris operating system, 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 the setup files and install Veeam Agent. This procedure is similar to the default installation of the Veeam Agent for Oracle Solaris. To learn more, see the Installing Veeam Agent for Oracle Solaris topic in the Veeam Agent for Oracle Solaris User Guide.

3. If necessary, immediately synchronize Veeam Agent with Veeam Backup & Replication running the following command:

```
veeamconfig mode syncnow
```

Mac Computers

To update pre-installed Veeam Agent on Mac 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. To learn more, see the Installing Veeam Agent topic 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
```

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 (from versions 21H2 to version 24H2)
  - 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.

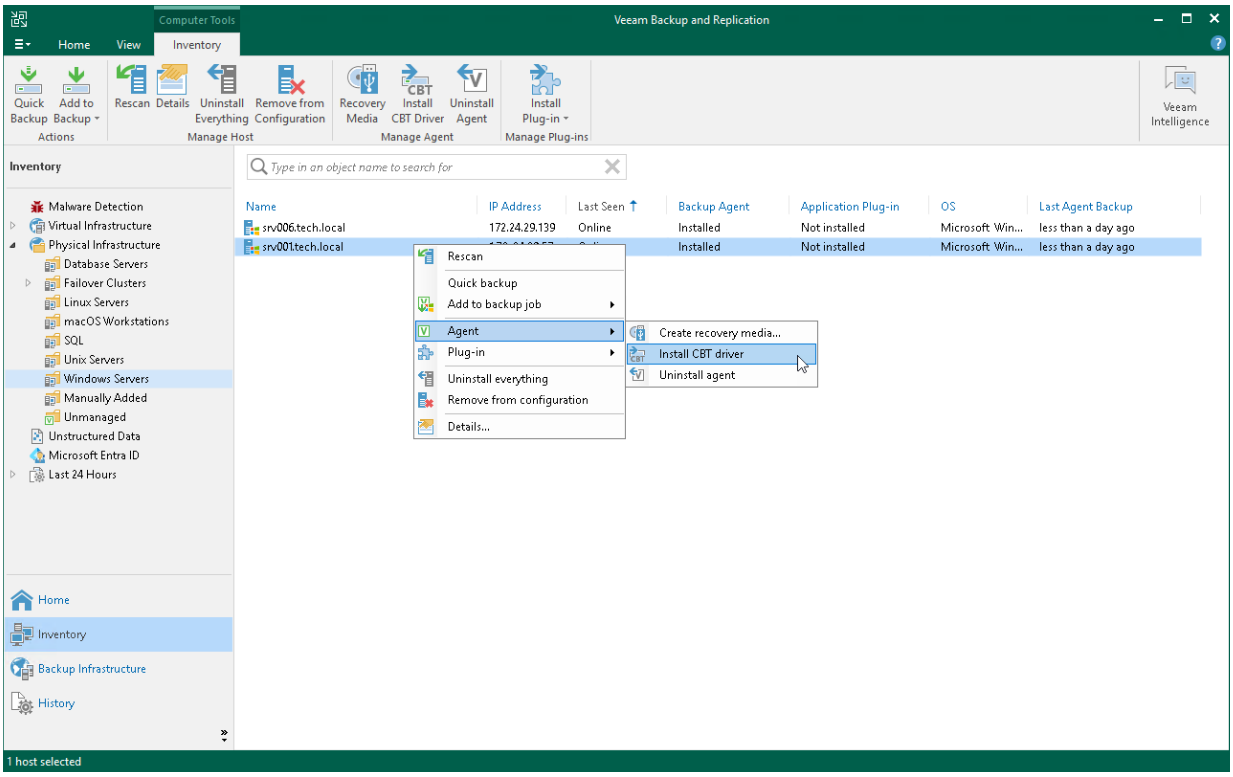
> **IMPORTANT**
>
> - Prior to installing the Veeam CBT driver on a computer running Microsoft Windows Server 2008 R2 SP1, make sure that update KB3033929 is installed in the OS.
>
>   The update adds the SHA-2 code signing support that is required for verification of the Veeam CBT driver signature. 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.
> - Do not install the Veeam CBT driver on a computer if you plan to use devices with hardware encryption made according to the TCG Opal Security Subsystem Class Specification. Operation of the driver on such devices may lead to a crash of the operating system. To learn more about the TCG Opal Security Subsystem Class Specification, see this Trusted Computing Group webpage.

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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local			Installed	Not installed	Microsoft Win...	less than a day ago

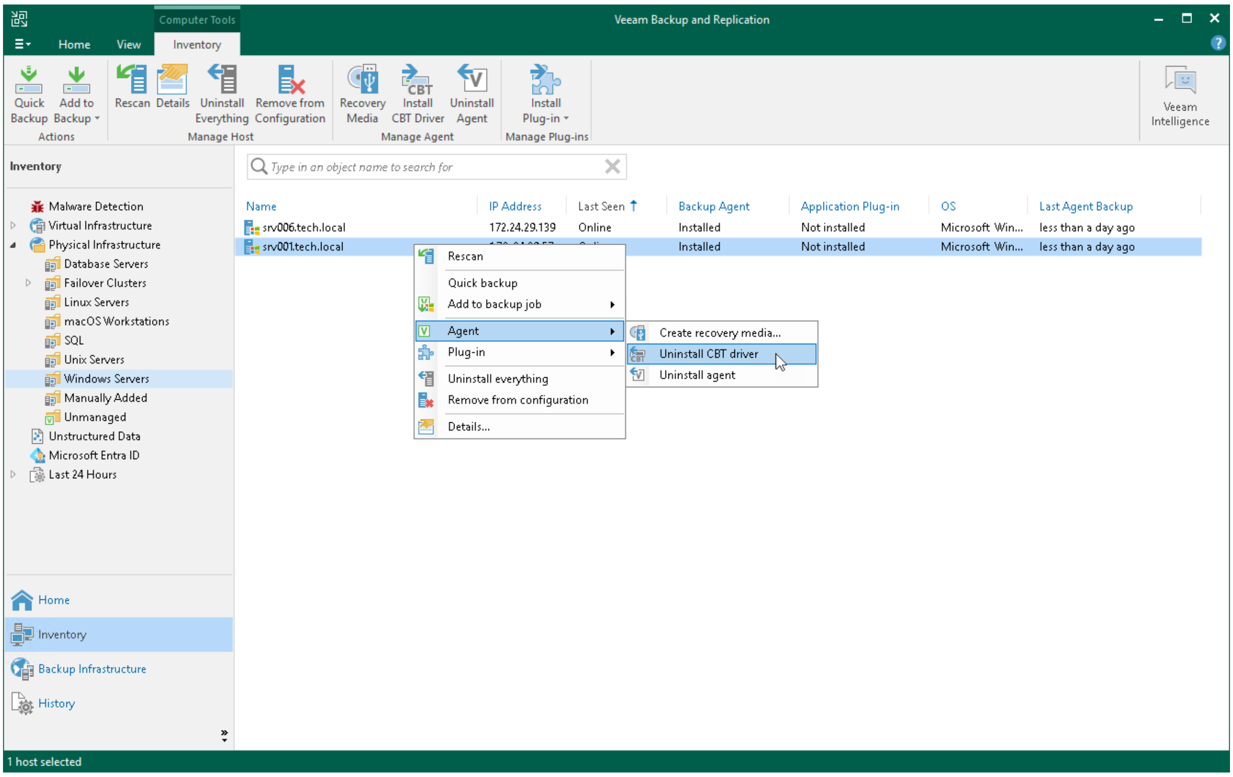
Uninstalling Veeam CBT Driver

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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local			Installed	Not installed	Microsoft Win...	less than a day ago

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.

Keep in mind that you can uninstall 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 about protection groups for pre-installed Veeam Agents, see Protection Group Types.

> TIP
>
> You can remove Veeam Agent and other Veeam components as one operation. To learn more, see Uninstalling Veeam Agent and Other Veeam Components.

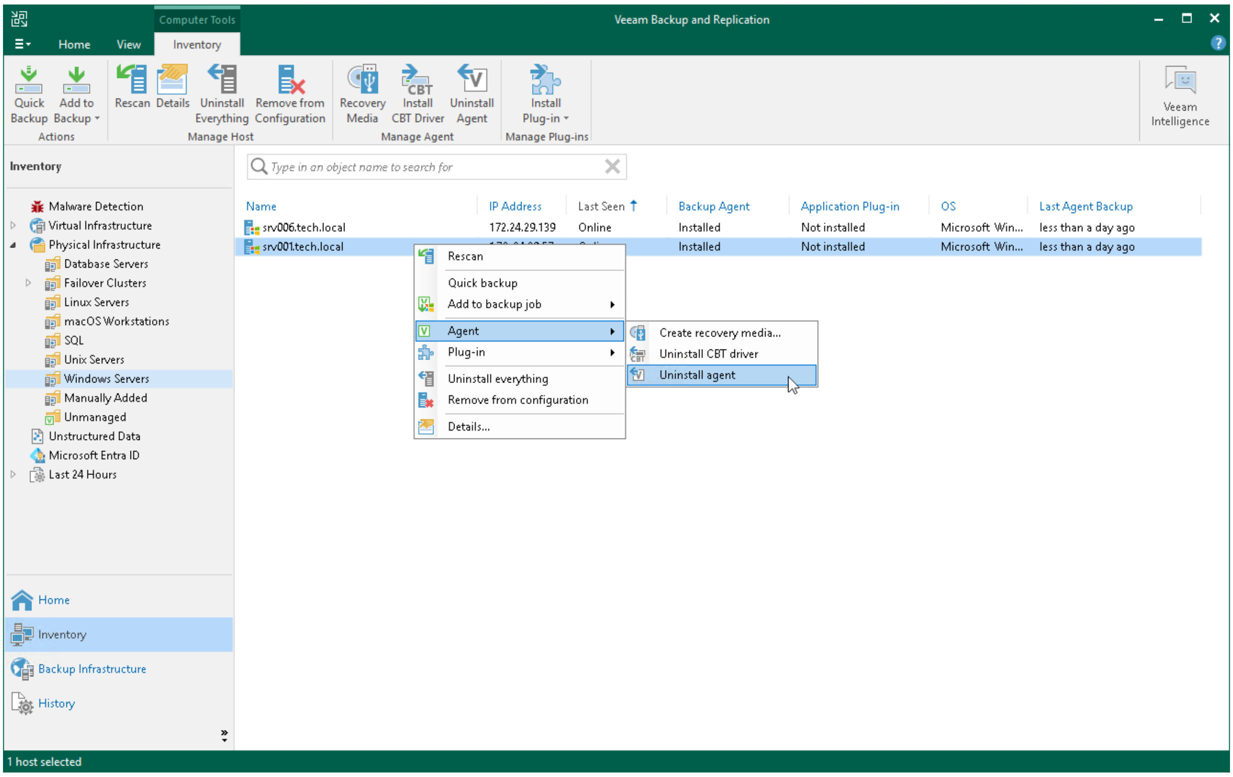
To uninstall Veeam Agent:

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

Consider 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. You can remove the remaining components from the side of 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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local			Installed	Not installed	Microsoft Win...	less than a day ago

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. 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). As a workaround, you can create a Veeam Recovery Media directly on the failover cluster node. To learn more, see this Veeam KB article.

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

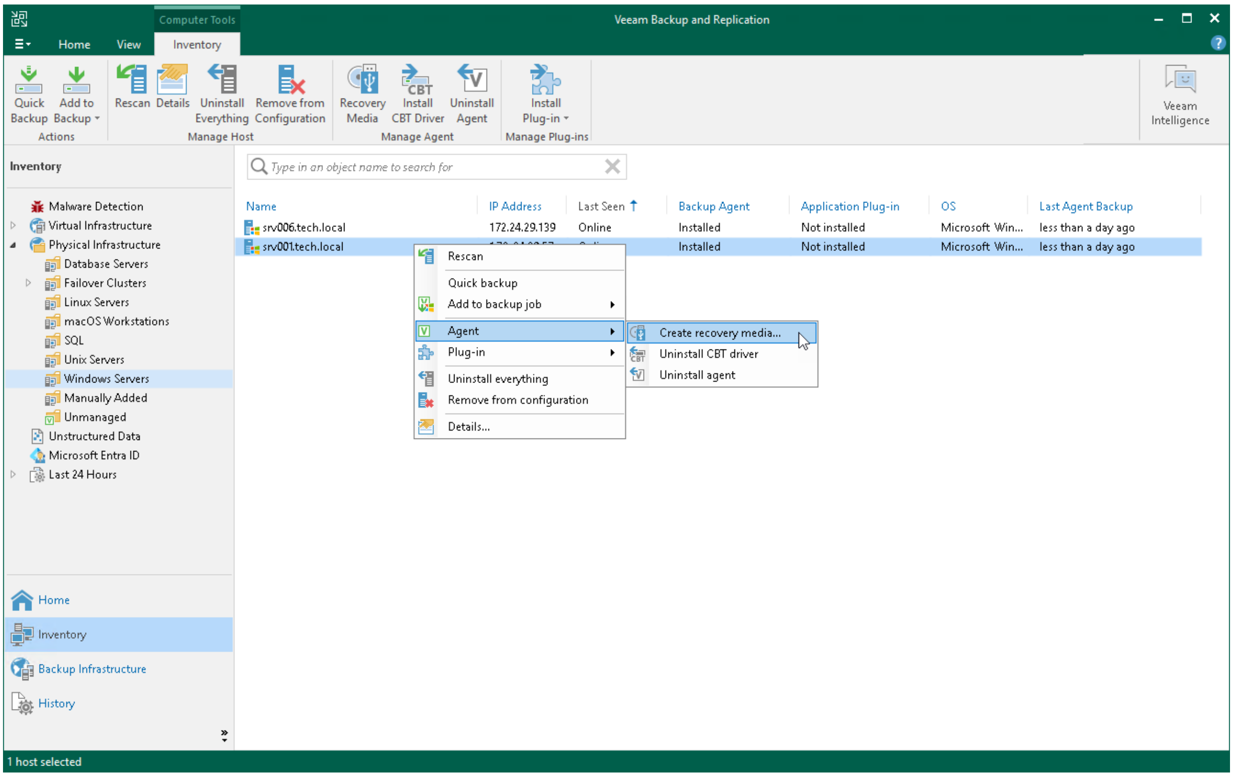
- An empty or re-writable CD/DVD/BD must be inserted into a CD/DVD/BD drive on the computer.
- The CD/DVD/BD must have enough capacity to store the created recovery image. On average, the size of the created recovery image without manually loaded drivers is 500 MB.
- [For RW CD/DVD/BD] During the recovery 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.



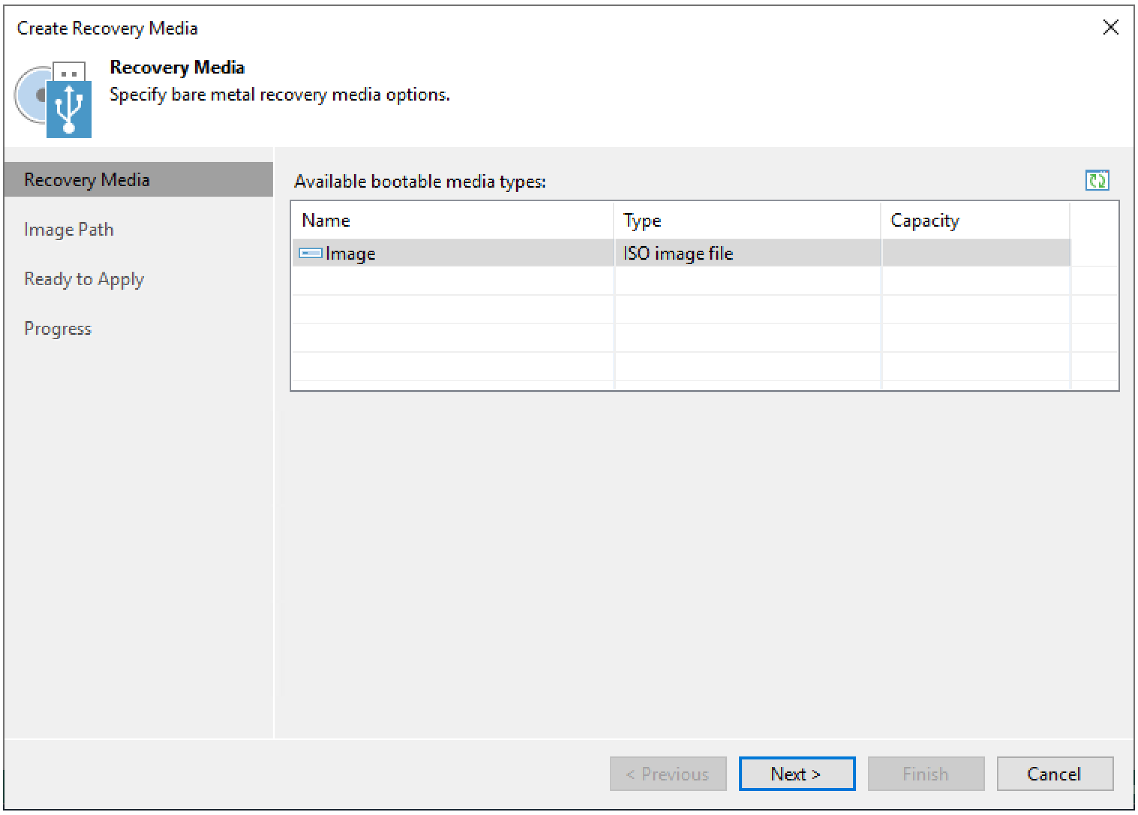
Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local	[illegible]	[illegible]	Installed	Not installed	Microsoft Win...	less than a day ago

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.



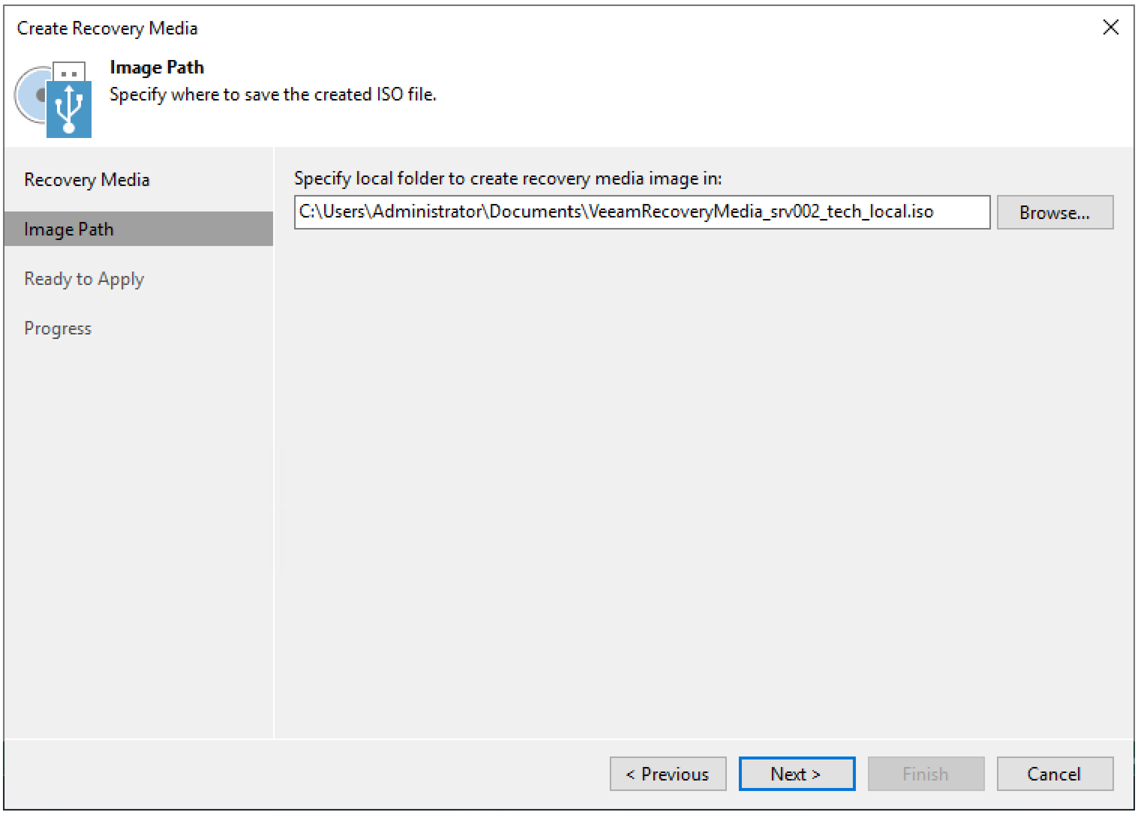
Available bootable media types:

Name	Type	Capacity
Image	ISO image file	

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. You cannot save the ISO file in a shared folder. Thus, the recovery image will always be available should Veeam Agent computer volumes get corrupted or the computer fail to start.

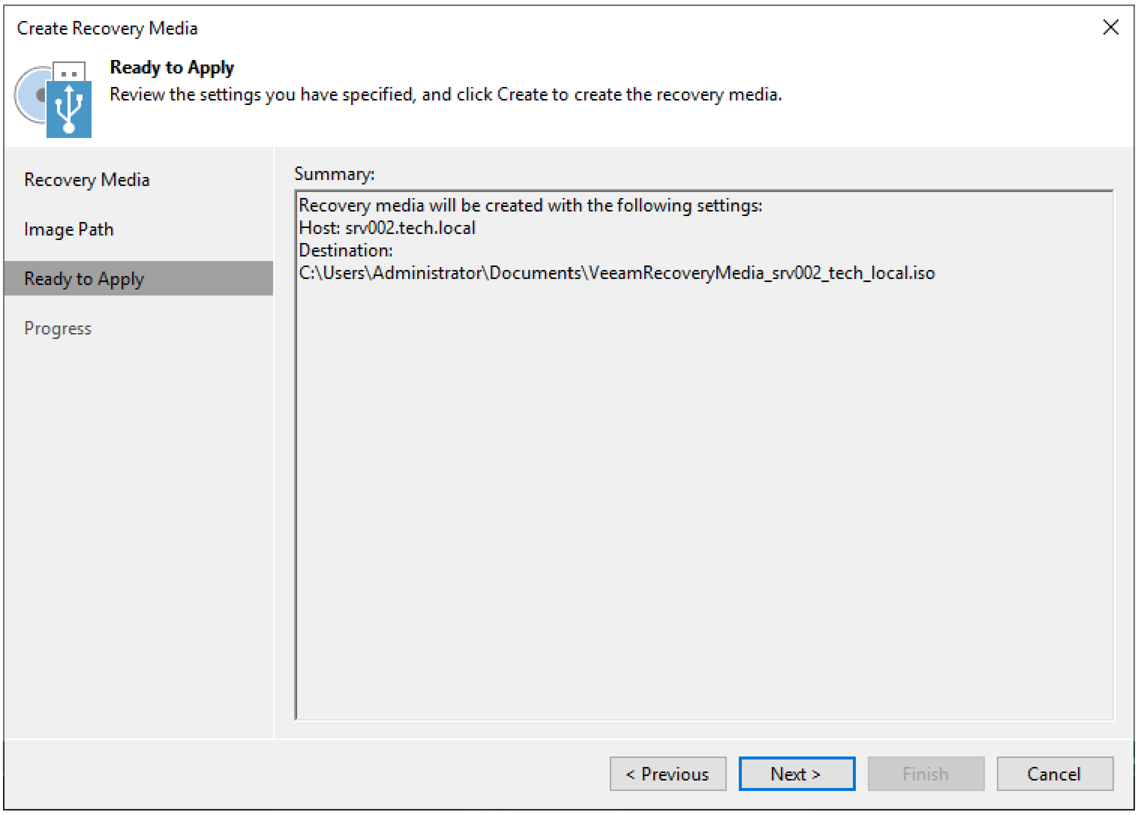


Specify local folder to create recovery media image in: C:\Users\Administrator\Documents\VeeamRecoveryMedia_srv002_tech_local.iso

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.



Review the settings you have specified, and click Create to create the recovery media.

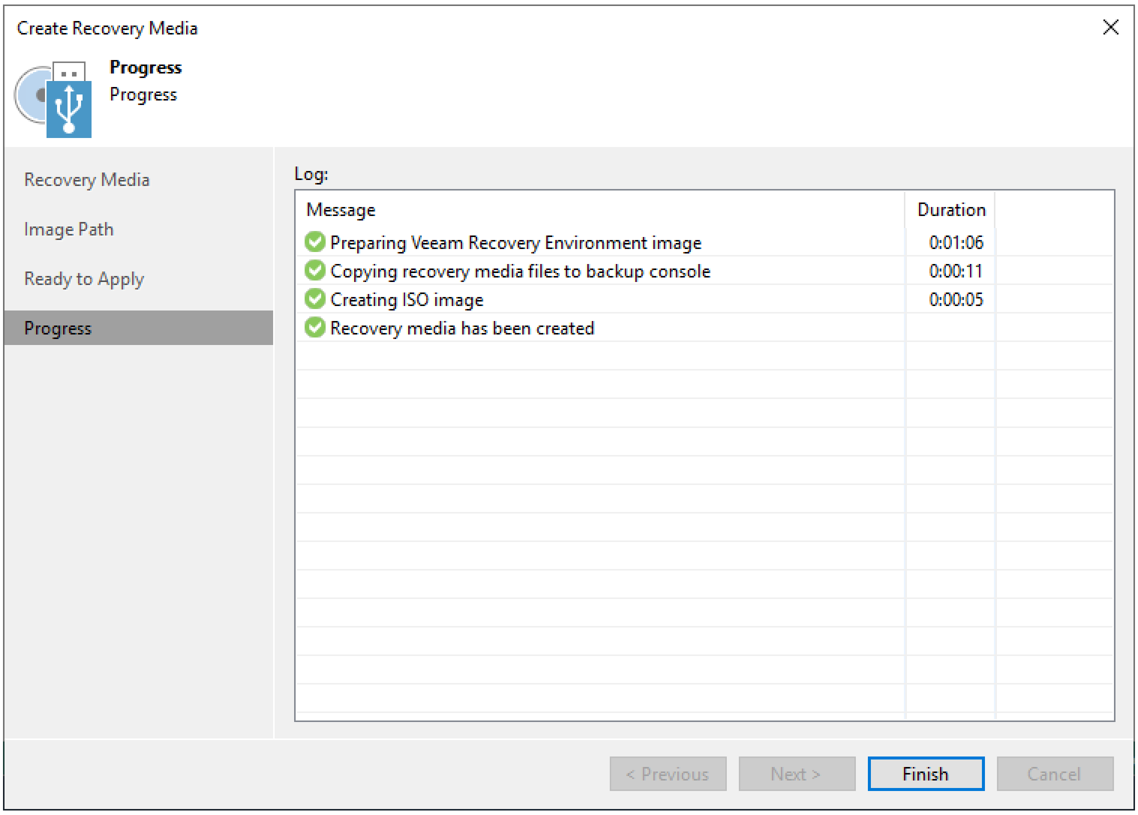
Summary:

Recovery media will be created with the following settings:
Host: srv002.tech.local
Destination:
C:\Users\Administrator\Documents\VeeamRecoveryMedia_srv002_tech_local.iso

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.



Message	Duration
✓ Preparing Veeam Recovery Environment image	0:01:06
✓ Copying recovery media files to backup console	0:00:11
✓ Creating ISO image	0:00:05
✓ Recovery media has been created	

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.

> TIP
>
> After the recovery image is created, you can predefine settings for restore from the Veeam Recovery Media. To learn more, see the Defining Veeam Recovery Media Operation Mode section in the Veeam Agent for Microsoft Windows User Guide.

Rebooting Protected Computer

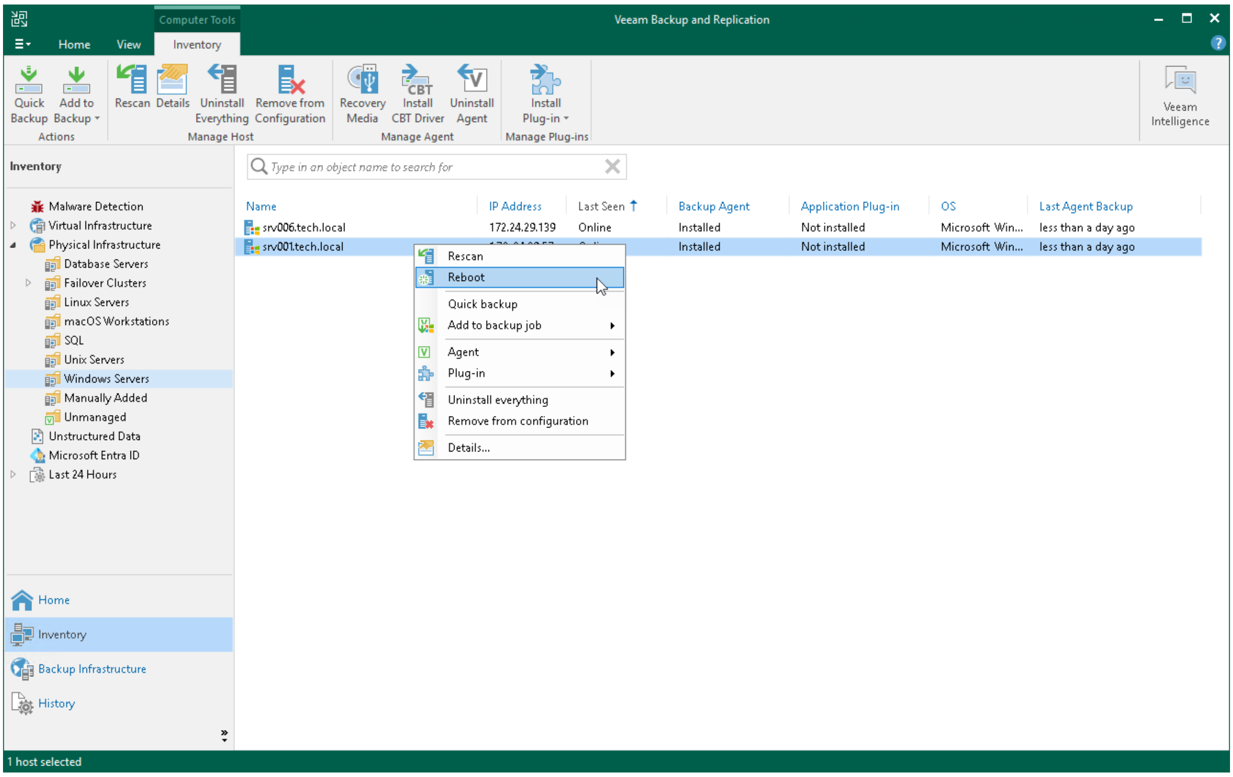
You can use the Veeam Backup & Replication console to reboot a protected computer running a Microsoft Windows OS. This operation may be required, for example, if you have installed the CBT driver on a selected computer and need to reboot this computer to finish the installation process and enable the 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, select the necessary computer, press and hold the [Ctrl] key, right-click the computer and select **Agent** > **Reboot**.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local	[illegible]	[illegible]	Installed	Not installed	Microsoft Win...	less than a day ago

Uninstalling Veeam Agent and Other Veeam Components

You can remove Veeam Agent and the following Veeam components installed on a protected computer as one operation:

- Veeam Plug-ins
- [For Microsoft Windows computers] Veeam Installer Service
- [For Linux computers] Veeam Deployer Service
- [For Microsoft Windows and Linux computers] Veeam Transport Service
- [For Microsoft Windows computers] Veeam CBT driver

> TIP
>
> - To learn about Veeam Plug-ins for enterprise applications, see Veeam Plug-ins for Enterprise Applications Guide.
> - To learn about the Veeam Installer Service, Veeam Deployer Service and Veeam Transport Service, see Rescan Job.
> - To learn about the Veeam CBT driver, see Installing Veeam CBT Driver.

Before you start the uninstall process, consider the following:

- [For Microsoft Windows and Linux computers] Veeam Installer Service, Veeam Deployer Service and Veeam Transport Service are not removed from the Veeam Agent computer if the computer is added to the Veeam backup infrastructure as a managed server. To learn more, see the Virtualization Servers and Hosts section in the Veeam Backup & Replication User Guide.
- [For Linux computers] Veeam Deployer Service is not removed if Veeam Backup & Replication connects to the protected computer with single-use credentials. To learn more, see Creating Veeam Agent Backup Jobs.
- 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. To learn more, see Creating Protection Groups.

  > NOTE
  >
  > [For Microsoft Windows and Linux computers] If automatic installation of Veeam Agent is not enabled in the protection group settings, Veeam Backup & Replication will not install Veeam Agent during the next rescan job session started by schedule but will install the Veeam Installer Service or Veeam Deployer Service and Veeam Transport Service on the computer.

- You can uninstall Veeam Agent, Veeam Plug-ins and Veeam components on a computer added to a protection group for pre-installed Veeam Agents only from the Veeam Agent computer side. To learn more about protection groups for pre-installed Veeam Agents, see Protection Group Types.
- 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.

- Prerequisite components installed and used by Veeam Agent are not removed during the uninstall process. You can remove the remaining components from the side of the computer from which you uninstalled Veeam Agent.

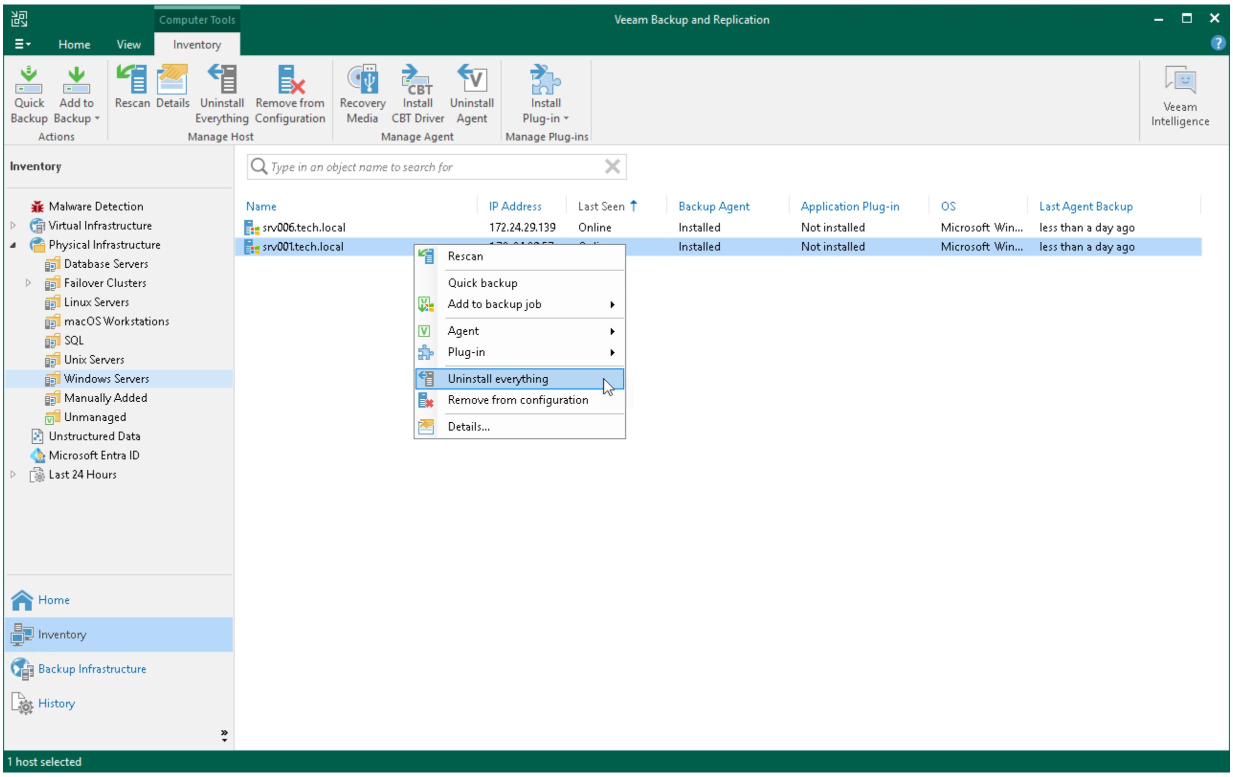
To uninstall Veeam Agent, Veeam Plug-ins and Veeam components:

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**.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local	[illegible]	[illegible]	Installed	Not installed	Microsoft Win...	less than a day ago

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 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.

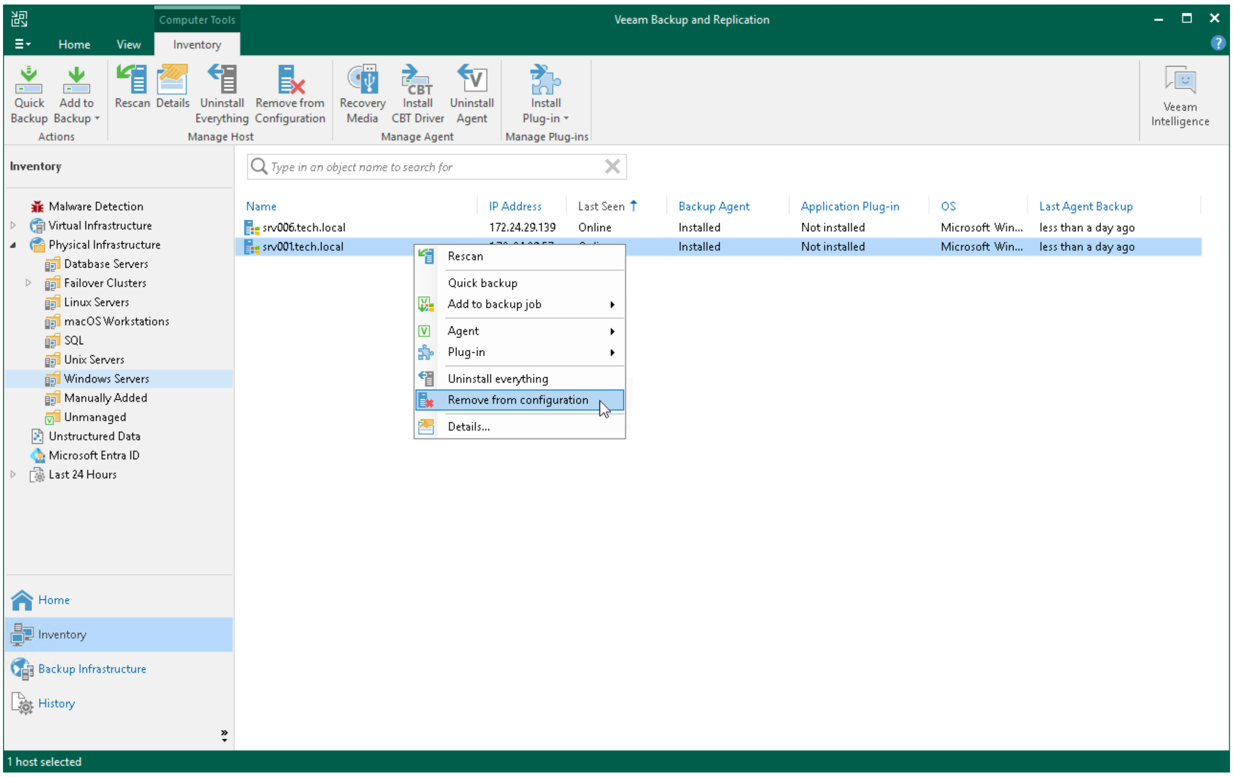
To remove a computer from a protection group:

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.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	less than a day ago
srv001.tech.local	[illegible]	[illegible]	Installed	Not installed	Microsoft Win...	less than a day ago

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 Veeam Agent backups created by backup jobs configured in Veeam Backup & Replication. For data restore with the Veeam backup console, you can use the 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 Veeam Agent backups to VMware vSphere VMs
- Restore Veeam Agent backups to Hyper-V VMs
- Restore Veeam Agent backups to Nutanix AHV VMs
- Restore Veeam Agent backups to Proxmox VE VMs
- Restore Veeam Agent backups to oVirt KVM VM
- Restore disks from Veeam Agent backups to oVirt KVM VM
- Restore data from Veeam Agent backups to Microsoft Azure
- Restore data from Veeam Agent backups to Amazon EC2
- Restore data from Veeam Agent backups to Google Compute Engine
- Restore computer volumes from Veeam Agent backups
- Restore individual files and folders from Veeam Agent backups
- Restore application items from Veeam Agent backups with Veeam Explorers
- Export computer disks as VMDK, VHD or VHDX disks
- Publish disks to analyze backup content
- Export restore points of Veeam Agent backups to standalone full backup files

Restoring Data with Veeam Recovery Media

In addition to data restore tasks available in the Veeam backup console, you can also recover data on a Veeam Agent computer using the Veeam Recovery Media. To do this, you must have a backup of the computer whose data you want to restore and the Veeam Recovery media created for this computer.

- For a Microsoft Windows computer, you can create the Veeam Recovery Media with the Veeam backup console. To learn more, see Creating Veeam Recovery Media.
- For a Linux computer, you can download the Veeam Recovery Media from the Veeam website or create a custom Veeam Recovery Media. To learn more, see the Veeam Recovery Media section in the Veeam Agent for Linux User Guide.

The process of data restore with the Veeam Recovery Media in the Veeam Agent management scenario does not differ from the same process on a computer that runs Veeam Agent operating in the standalone mode.

- For information on data restore with the Veeam Recovery Media on a Microsoft Windows computer, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.
- For information on data restore with the Veeam Recovery Media on a Linux computer, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Linux User Guide.

Restoring Veeam Agent Backup to vSphere VM

In the Veeam Backup & Replication console, you can use Instant Recovery to restore a Veeam Agent computer as a VMware vSphere VM in your virtualization environment.

A restored VMware vSphere VM will have the same settings as the backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves the 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.

Considerations and Limitations

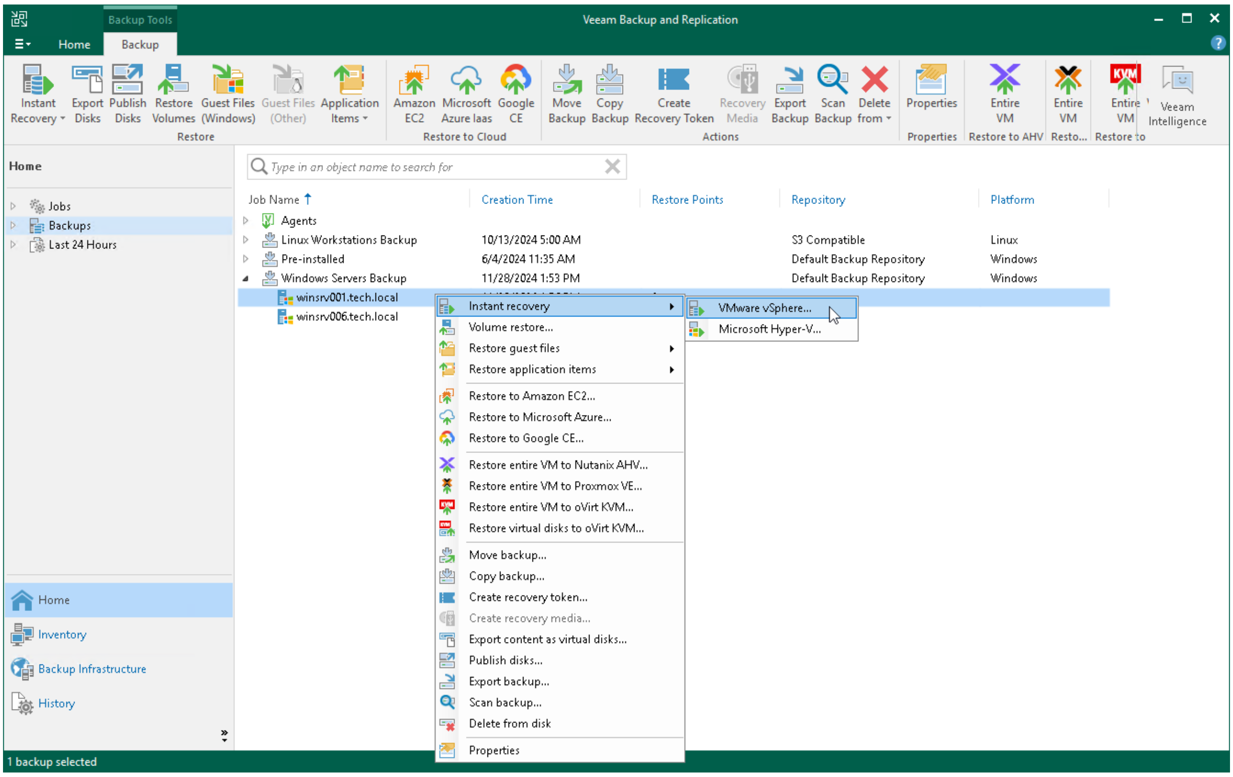
If you restore a Veeam Agent computer to a VMware vSphere VM, consider the following:

- You can use entire machine or volume-level backups of Microsoft Windows and Linux computers. Volume-level backups of Windows computers must include the computer system drive. Volume-level backups of Linux computers must include the `root` file system (`/`) and all partitions specified in the `/etc/fstab` file.
- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- 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 a Logical Volume Manager (LVM) volume group, consider the following:
  - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Backup & Replication will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
  - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 Backup & Replication will restore 4 disks. The restored disks will consume the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

> **TIP**
>
> After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to vSphere VM

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 section in the Veeam Backup & Replication User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

Restoring Veeam Agent Backup to Hyper-V VM

In the Veeam Backup & Replication console, you can use Instant Recovery to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment.

A restored Hyper-V VM will have the same settings as the 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.

Considerations and Limitations

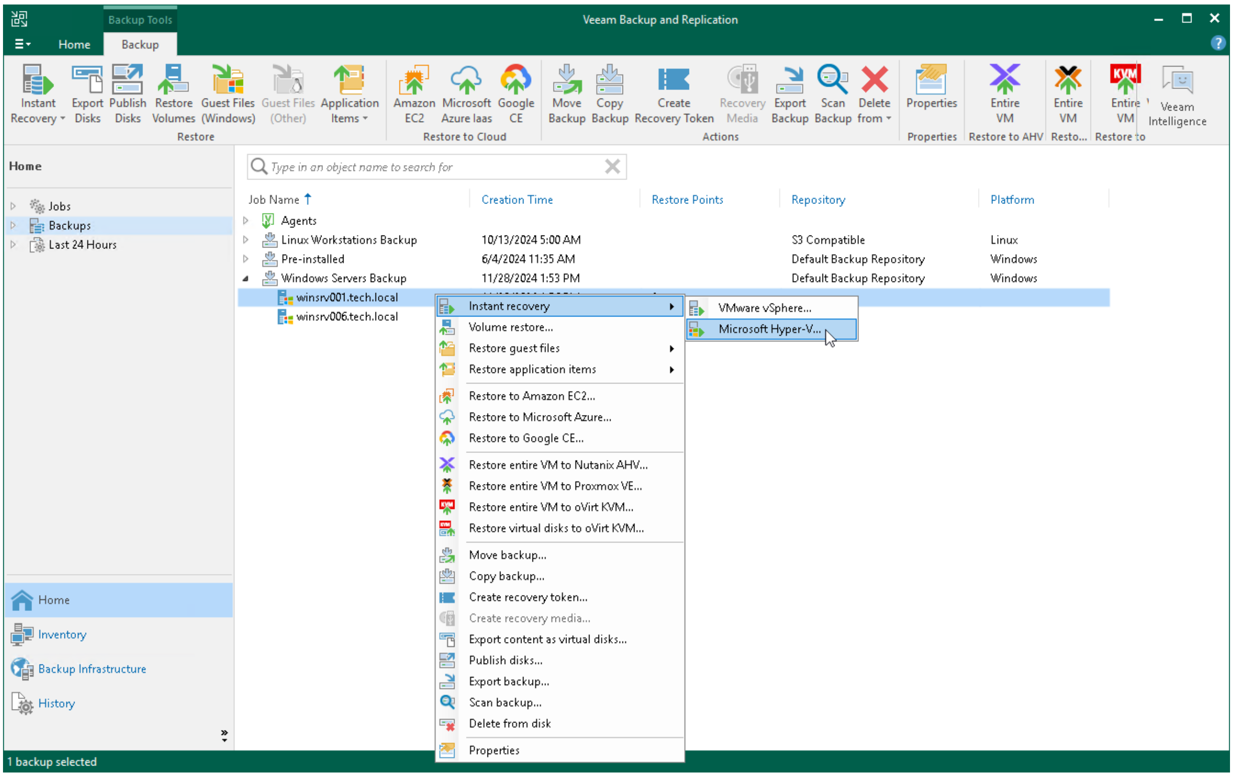
If you restore a Veeam Agent computer to a Hyper-V VM, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot use backups stored in a Veeam Cloud Connect repository for this operation.
- To restore to a Hyper-V VM from a backup of a Linux computer, you must consider the Hyper-V limitations. To learn more, see this Microsoft article.
- [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 a Logical Volume Manager (LVM) volume group, consider the following:
    - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Backup & Replication will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
    - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 Backup & Replication will restore 4 disks. The restored disks will consume the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > TIP
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to Hyper-V VM

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 section in the Veeam Backup & Replication User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

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.

Considerations and Limitations

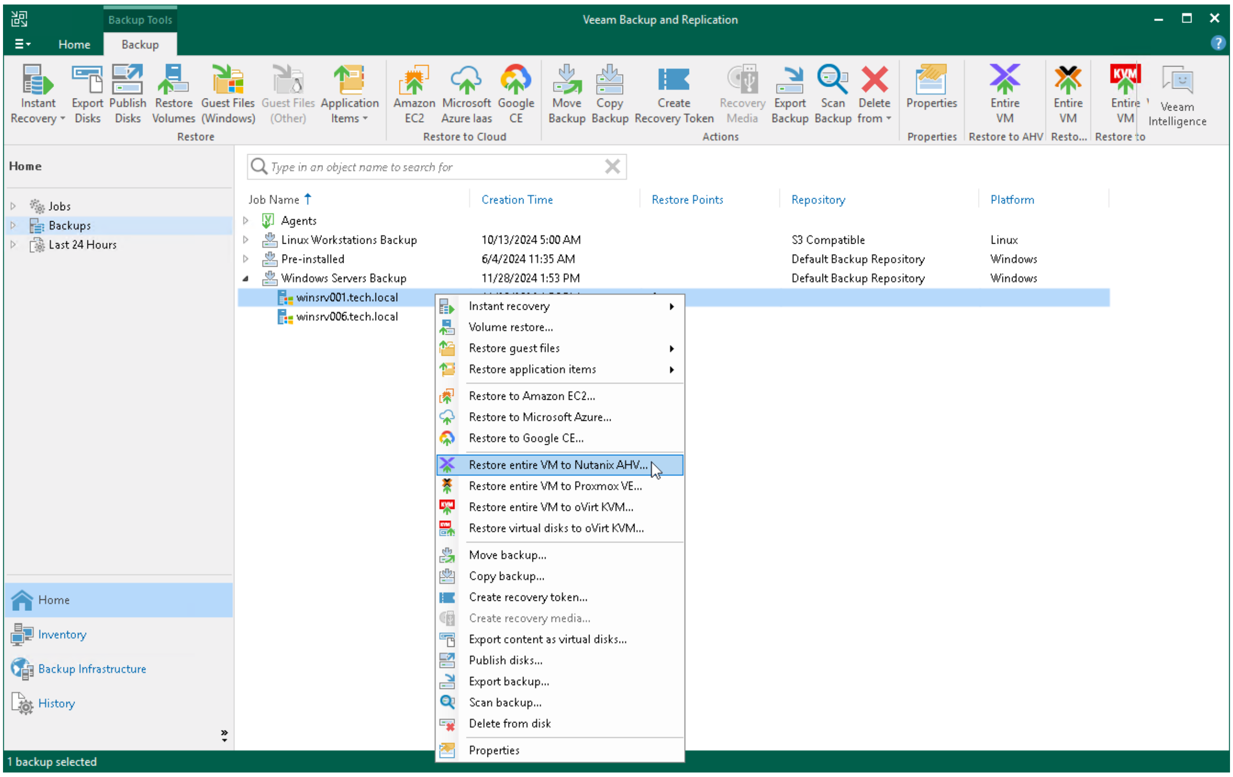
If you restore a Veeam Agent computer to a Nutanix AHV VM, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- [For backups of Linux computers] If the disk you want to restore contains a Logical Volume Manager (LVM) volume group, consider the following:
  - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
  - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > TIP
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to Nutanix AHV

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.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

1 backup selected

Restoring Veeam Agent Backup to Proxmox VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Proxmox VE VM in your virtualization environment.

Considerations and Limitations

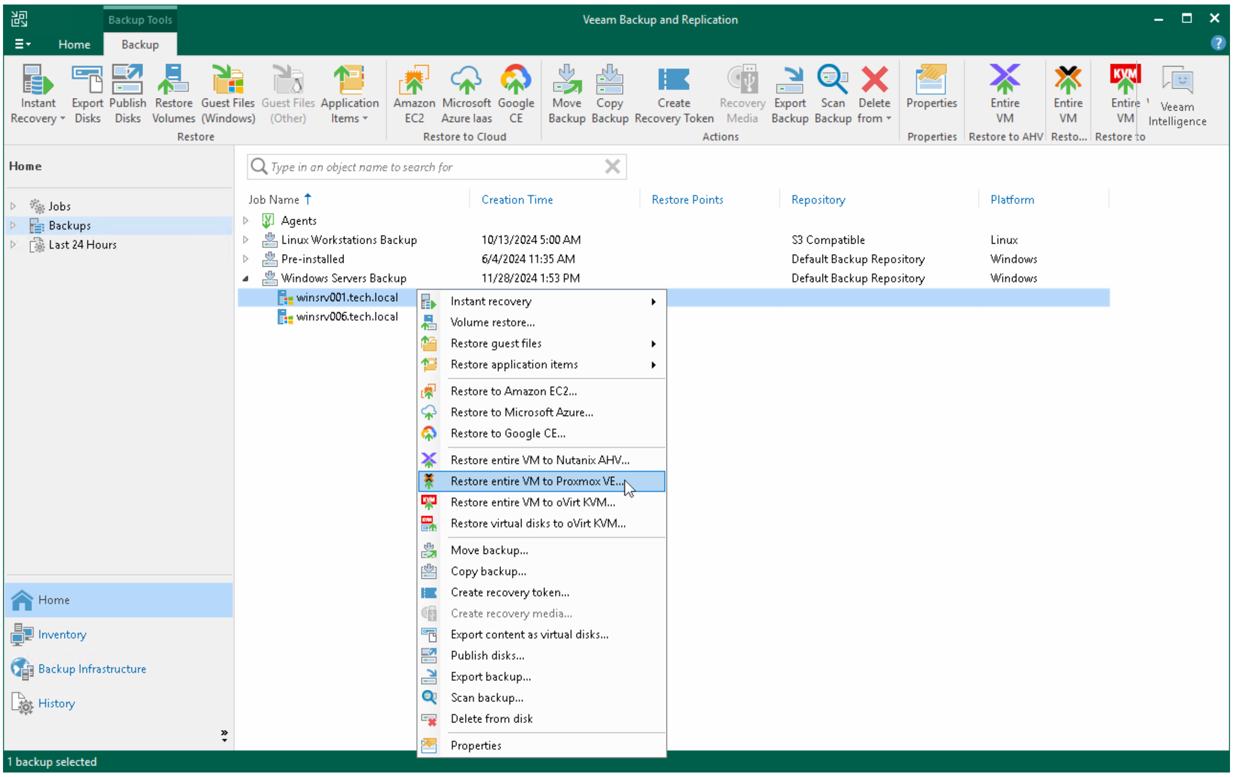
If you restore a Veeam Agent computer to a Proxmox VE VM, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- [For backups of Linux computers]If the disk you want to restore contains a Logical Volume Manager (LVM) volume group, consider the following:
  - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
  - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > TIP
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to Proxmox VE

The procedure of restore to Proxmox VE for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more about restore to Proxmox VE, see the Performing VM Restore section in the Veeam Backup for Proxmox VE User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

Restoring Veeam Agent Backup to oVirt KVM VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as an oVirt KVM VM in your virtualization environment.

Considerations and Limitations

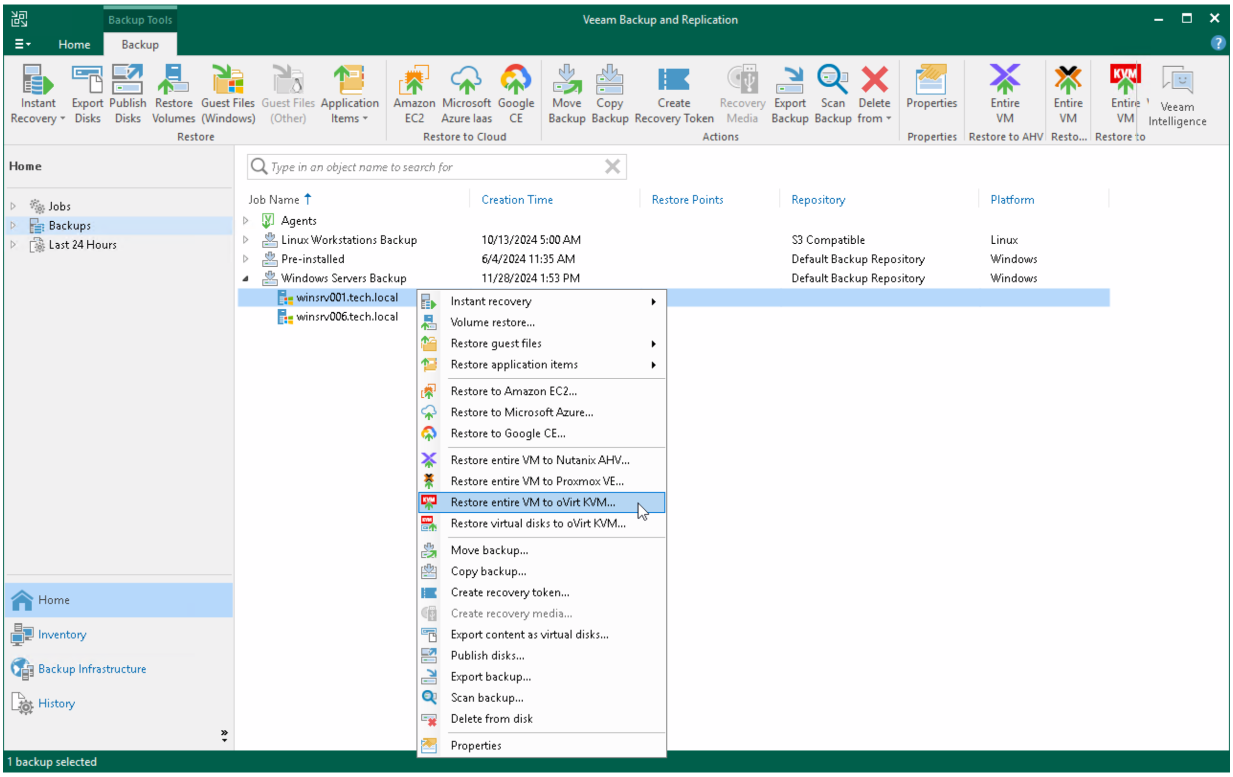
If you restore a Veeam Agent computer to an oVirt KVM VM, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- [For backups of Linux computers]If the disk you want to restore contains a Logical Volume Manager (LVM) volume group, consider the following:
    - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
    - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > TIP
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to oVirt KVM VM

The procedure of restore to an oVirt KVM VM for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more, see the Performing VM Restore section in the Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

Restoring Disk from Veeam Agent Backup to oVirt KVM

You can use the Veeam Backup & Replication console to restore disks from a Veeam Agent computer backup to an oVirt KVM VM in your virtualization environment.

Considerations and Limitations

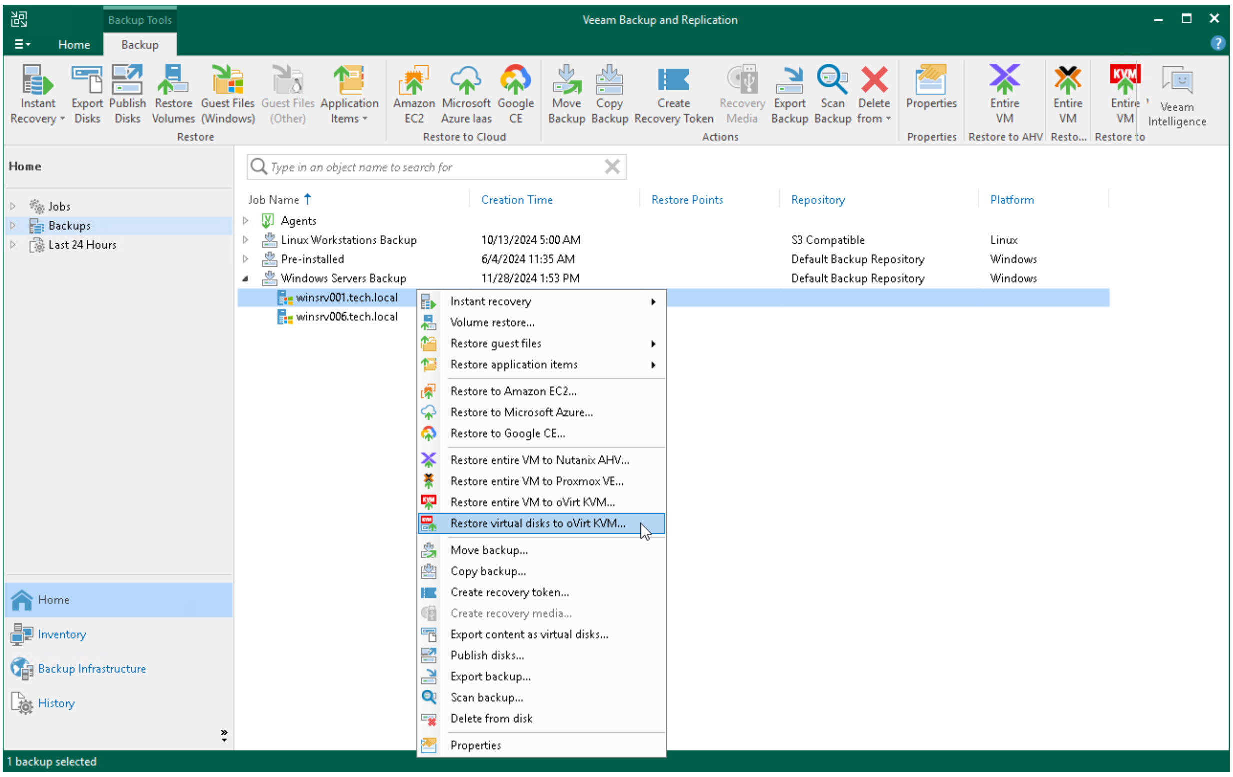
If you restore disks to an oVirt KVM VM, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- [For backups of Linux computers]If the disk you want to restore contains a Logical Volume Manager (LVM) volume group, consider the following:
  - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
  - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > TIP
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to oVirt KVM VM

The procedure of restoring disks to an oVirt KVM VM for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more, see the Performing Disk Restore section in the Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

Restoring to Microsoft Azure

You can use the Veeam Backup & Replication console to restore computers from Veeam Agent backups to Microsoft Azure.

Considerations and Limitations

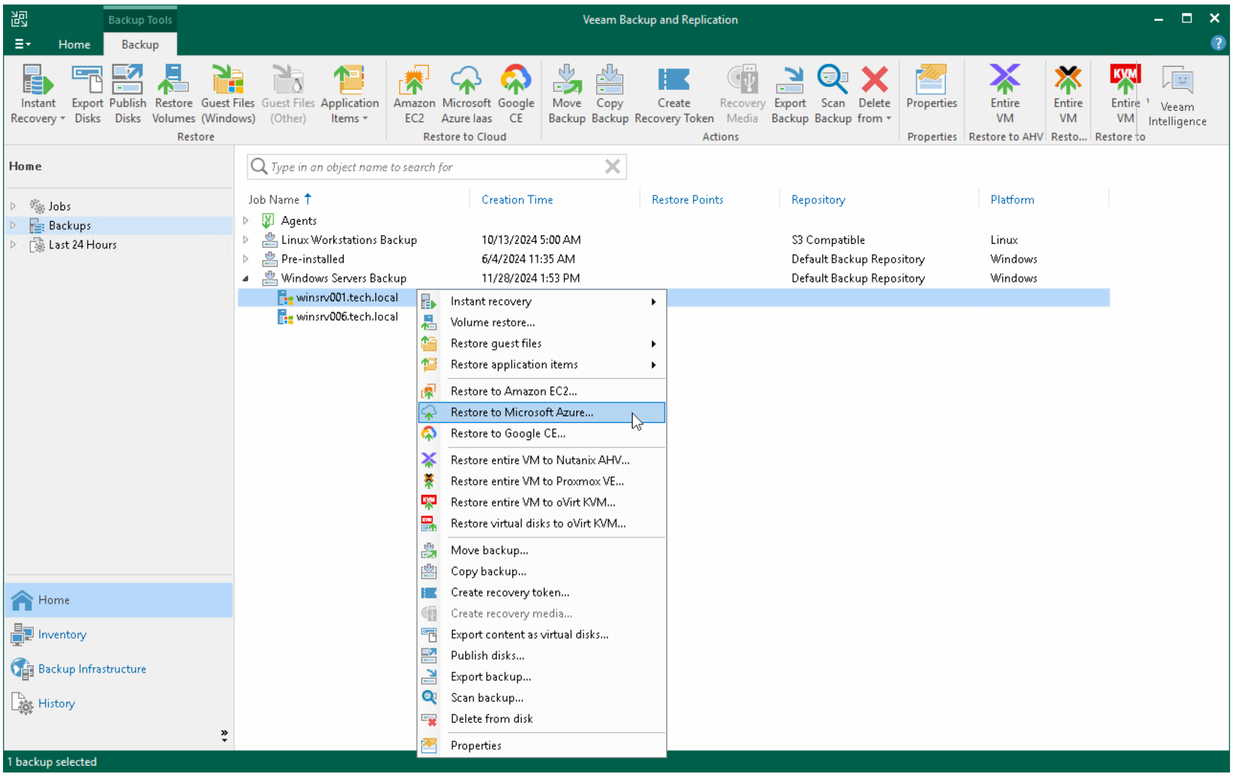
If you restore a Veeam Agent computer to Microsoft Azure, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- Veeam Agent backups must be created at the entire computer level or volume level.
- If you recover an 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 a Logical Volume Manager (LVM) volume group, consider the following:
  - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
  - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > **TIP**
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to Microsoft Azure

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 Restoring to Microsoft Azure section in the Veeam Backup & Replication User Guide.



Job Name ↑	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

Restoring to Amazon EC2

You can use the Veeam Backup & Replication console to restore computers from Veeam Agent backups to Amazon EC2.

Considerations and Limitations

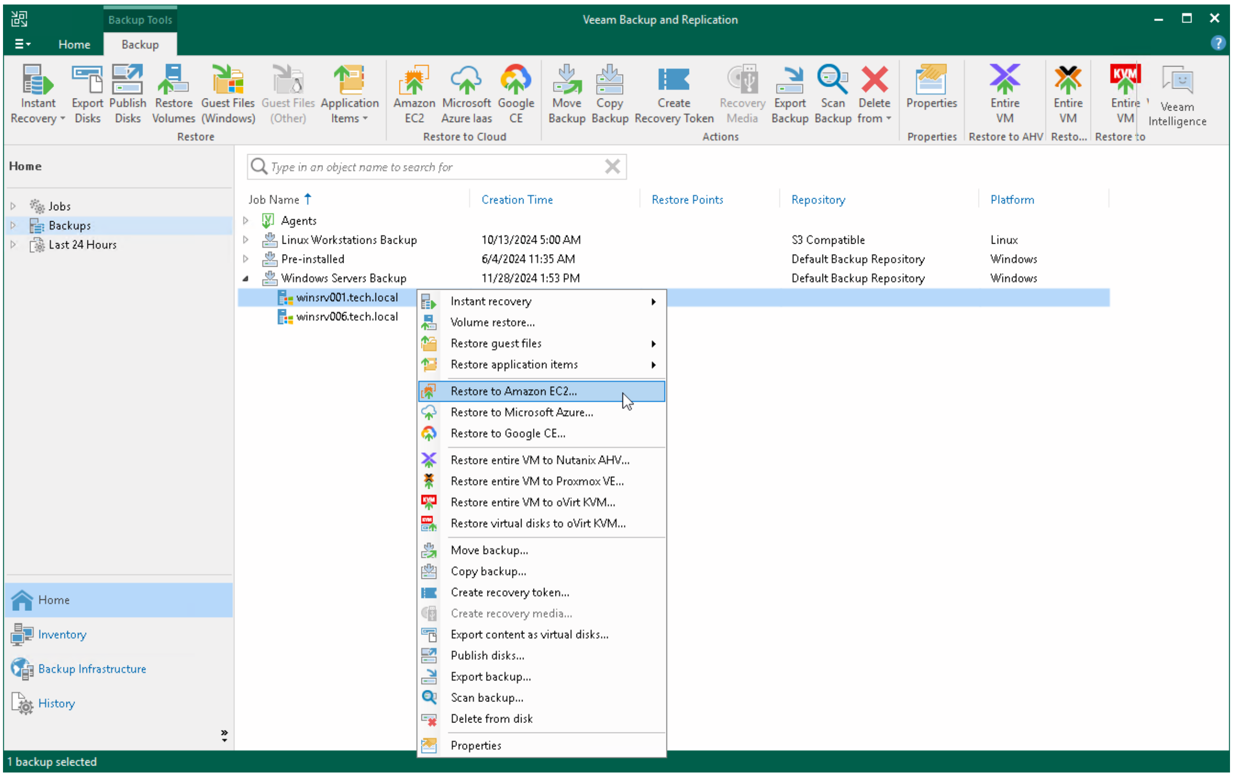
If you restore a Veeam Agent computer to Amazon EC2, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository only. You cannot perform this operation with Veeam Agent backups stored in a Veeam Cloud Connect repository.
- Veeam Agent backups must be created at the entire computer level or volume level.
- [For backups of Linux computers] If the disk you want to restore contains a Logical Volume Manager (LVM) volume group, consider the following:
  - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
  - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > TIP
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to Amazon EC2

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 Restoring to Amazon EC2 section in the Veeam Backup & Replication User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

Restoring to Google Compute Engine

You can use the Veeam Backup & Replication console to restore computers from Veeam Agent backups to Google Compute Engine.

Considerations and Limitations

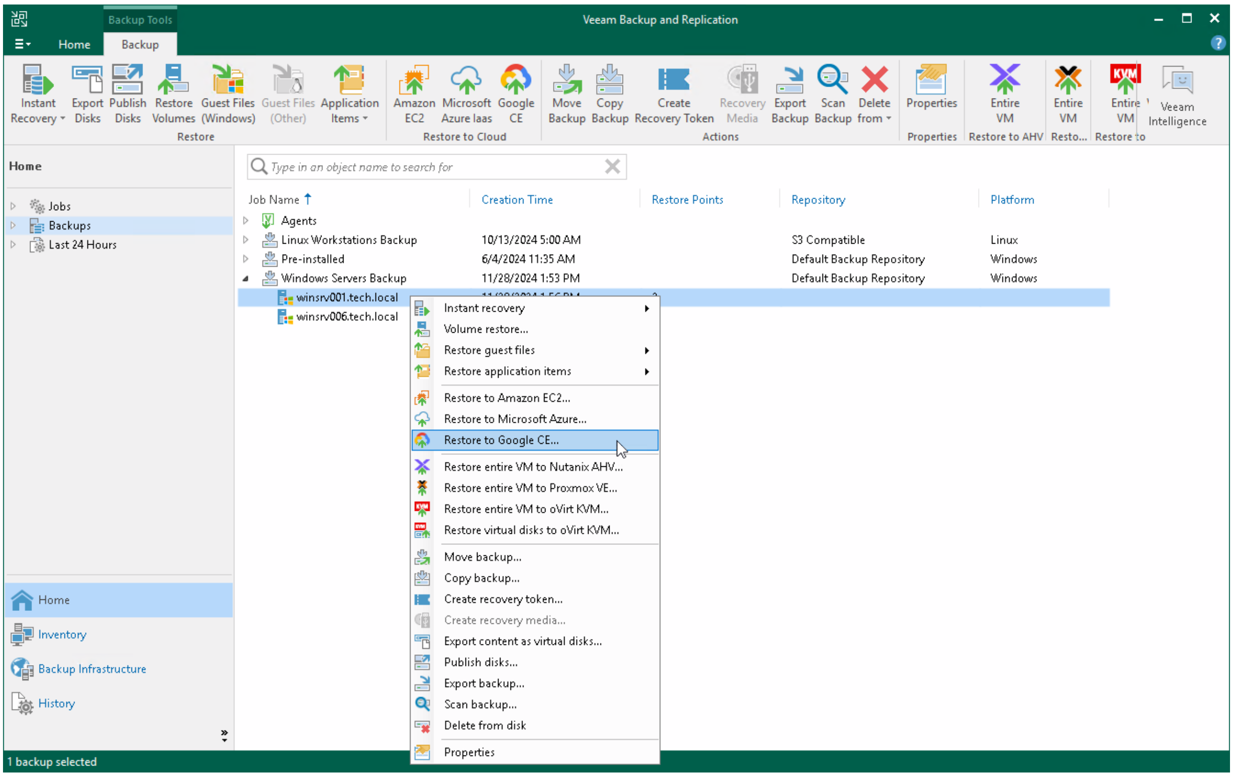
If you restore a Veeam Agent computer to Google Compute Engine, consider the following:

- You can use backups of Microsoft Windows and Linux computers stored in a Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.
- Veeam Agent backups must be created at the entire computer level or volume level.
- [For backups of Linux computers] If the disk you want to restore contains a Logical Volume Manager (LVM) volume group, consider the following:
    - Since LVM volume group is a logical entity that spans across the physical disks, Veeam Agent treats the original disk and the LVM volume group as separate entities. Therefore, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. This way, all data, including the data within the LVM volume group, is accurately restored.
    - Root file system partition and boot partition must not be on LVM logical volumes. For more information on this limitation, see Google documentation.
    - Restoring the original disk and the LVM volume groups as 2 separate disks requires an increased amount of 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 the storage space equal to the size of the 2 original disks and the 2 LVM volume groups from these disks.

    > TIP
    >
    > After restore, you can remove unnecessary disks from the machine. To learn more, see this Veeam KB article.

Restore to Google Compute Engine

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 Restoring to Google Compute Engine section in the Veeam Backup & Replication User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local				
winsrv006.tech.local				

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.

- Complete the restore process.

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.

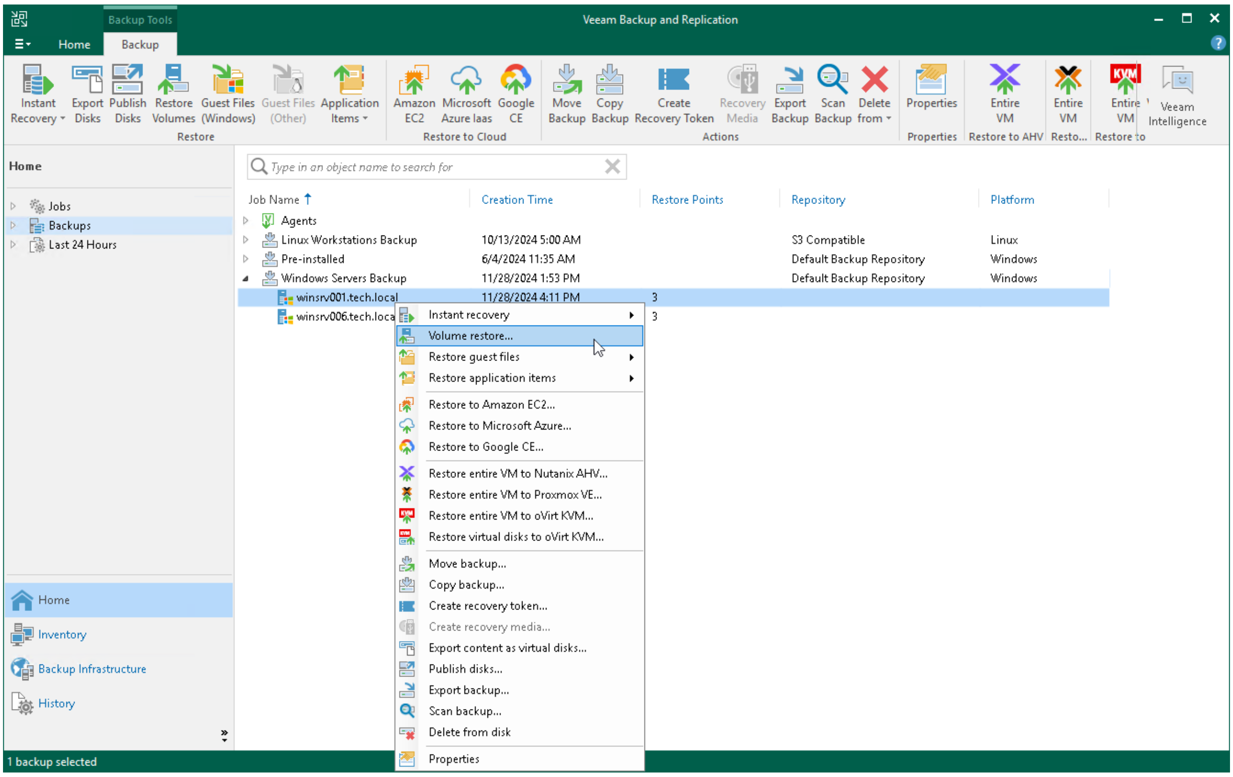
Volume-level restore has the following limitations:

- 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. To learn more, 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.



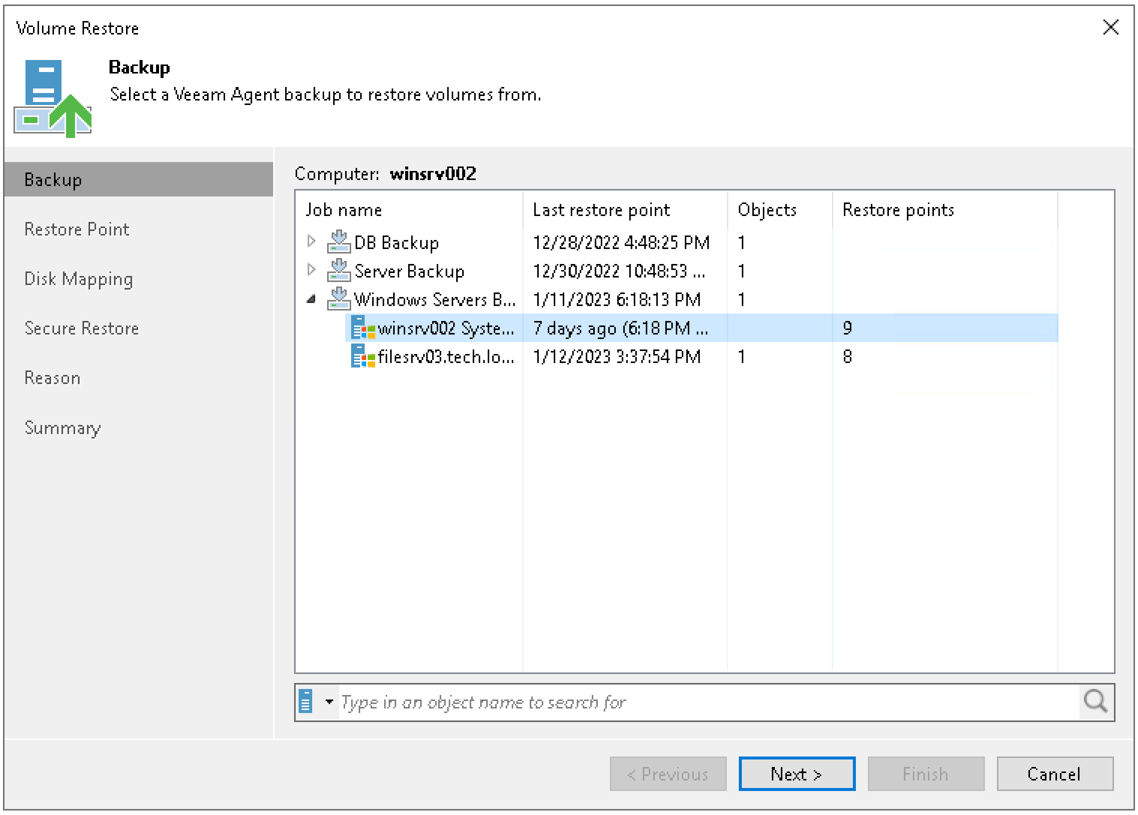
Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local	11/28/2024 4:11 PM	3		
winsrv006.tech.loca		3		

Step 2. Select Backup

At the **Backup** step of the wizard, select a backup that contains volumes 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]**.

Backups created with Veeam Agent for Linux are not displayed.



Volume Restore

Backup

Select a Veeam Agent backup to restore volumes from.

Computer: **winsrv002**

Job name	Last restore point	Objects	Restore points
DB Backup	12/28/2022 4:48:25 PM	1	
Server Backup	12/30/2022 10:48:53 ...	1	
Windows Servers B...	1/11/2023 6:18:13 PM	1	
winsrv002 Syste...	7 days ago (6:18 PM ...		9
filesrv03.tech.lo...	1/12/2023 3:37:54 PM	1	8

Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to recover data.

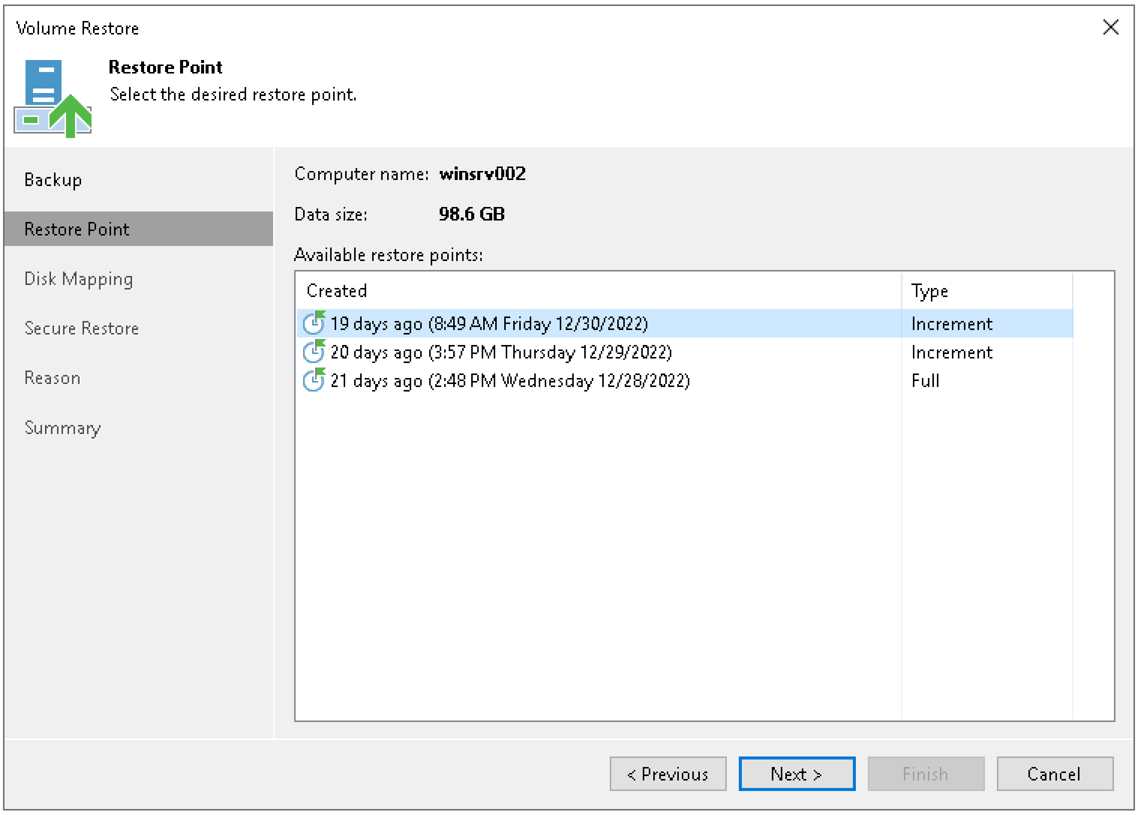
By default, Veeam Backup & Replication uses the latest restore point. However, you can select any valid restore point to recover volumes to a specific point in time.

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.

To select a restore point:

1. Select a restore point from the **Available restore points** section.
2. [For restore from backups created by pre-installed Veeam Agents] Do the following:
   a. In the **Agent Credentials** window, select the Veeam Agent computer which volumes you want to restore and click **Set**.

   b. In the **Credentials** window, specify credentials for the user account that has access to the protected computer. Veeam Backup & Replication will not store these credentials in its database.



Computer name: **winsrv002**

Data size: **98.6 GB**

Available restore points:

Created	Type
19 days ago (8:49 AM Friday 12/30/2022)	Increment
20 days ago (3:57 PM Thursday 12/29/2022)	Increment
21 days ago (2:48 PM Wednesday 12/28/2022)	Full

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.

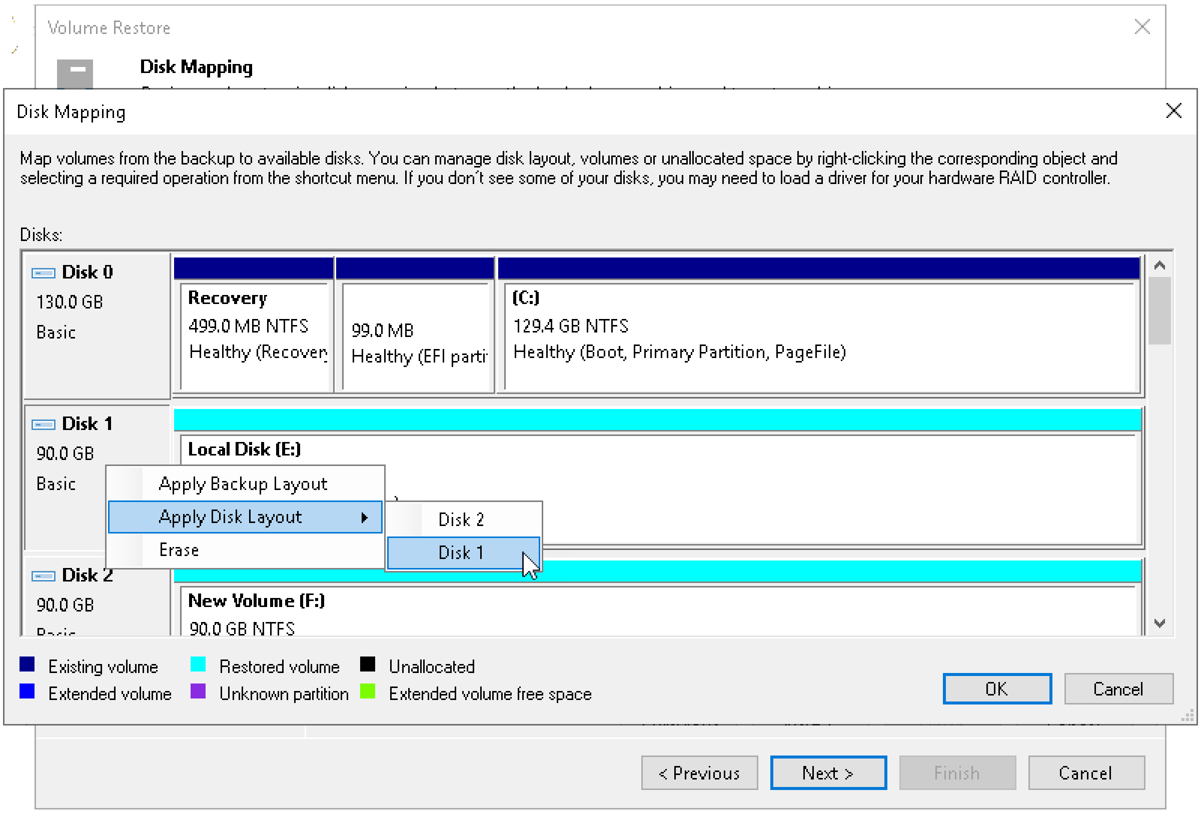
To select volumes for restore:

1. In the **Destination host** field, specify the target computer where you want to restore volumes. Click **Choose** and select the necessary computer. You can restore volumes only to computers that are added to the Veeam Backup & Replication inventory and run Veeam Agent for Microsoft Windows.
2. In the **Disk mapping** section, select check boxes next to volumes that you want to restore from the backup. By default, Veeam Backup & Replication restores volumes to their initial location and maps the restored volumes automatically. If the initial location is unavailable, a volume is restored to a disk of the same or larger size. If you want to map the restored volume to another computer disk, at the bottom of the wizard click **Customize disk mapping**.

   > NOTE
   >
   > If Veeam Backup & Replication cannot map a volume automatically, Veeam Backup & Replication will prompt you to perform disk mapping manually. To proceed to the **Disk Mapping** window, click **Yes**.

3. 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.



Volume Restore

Disk Mapping

Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

Disks:

Disk 0
130.0 GB
Basic

Recovery
499.0 MB NTFS
Healthy (Recovery

99.0 MB
Healthy (EFI parti

(C:)
129.4 GB NTFS
Healthy (Boot, Primary Partition, PageFile)

Disk 1
90.0 GB
Basic

Local Disk (E:)

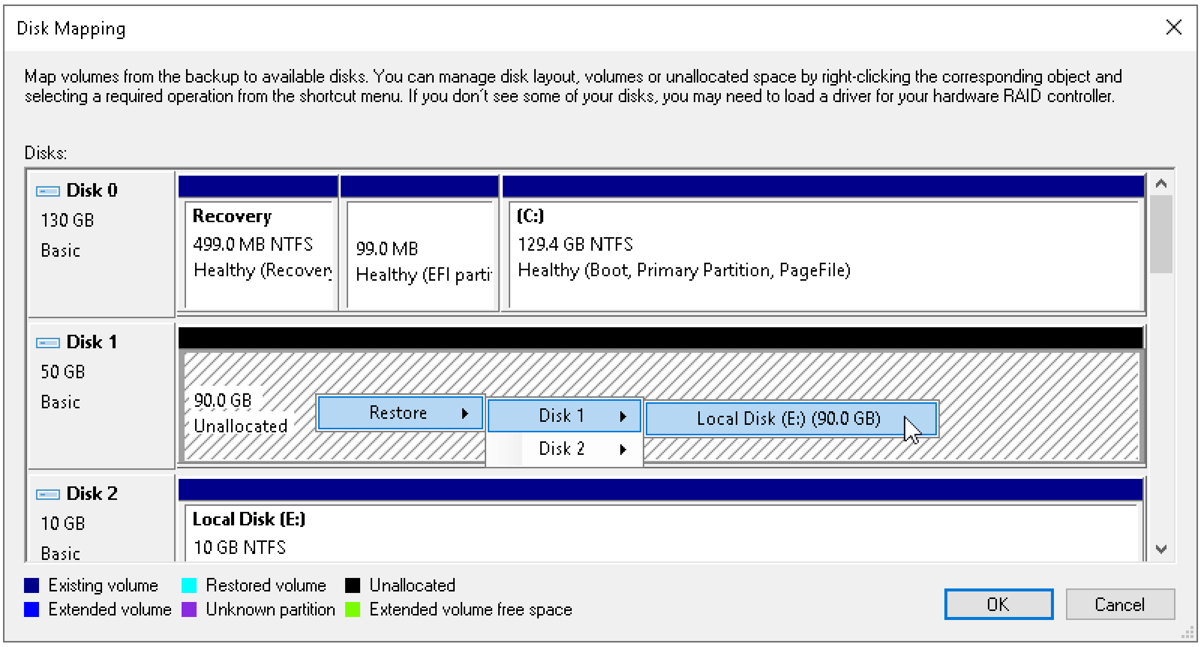
Disk 2
90.0 GB
Basic

New Volume (F:)
90.0 GB NTFS

■ Existing volume ■ Restored volume ■ Unallocated
■ Extended volume ■ Unknown partition ■ Extended volume free space

- 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.



Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

Disks:

Disk 0
130 GB
Basic

Recovery
499.0 MB NTFS
Healthy (Recovery

99.0 MB
Healthy (EFI parti

(C:)
129.4 GB NTFS
Healthy (Boot, Primary Partition, PageFile)

Disk 1
50 GB
Basic

90.0 GB
Unallocated

Disk 2
10 GB
Basic

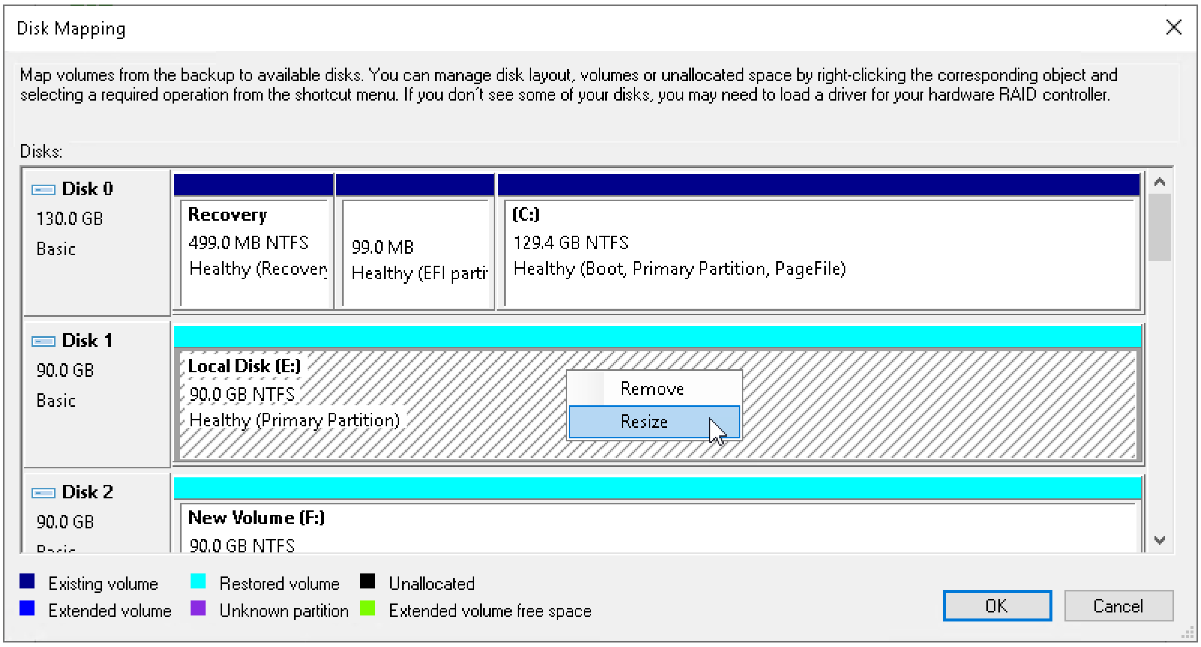
Local Disk (E:)
10 GB NTFS

■ Existing volume ■ Restored volume ■ Unallocated
■ Extended volume ■ Unknown partition ■ Extended volume free space

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.



Disk Mapping

Map volumes from the backup to available disks. You can manage disk layout, volumes or unallocated space by right-clicking the corresponding object and selecting a required operation from the shortcut menu. If you don't see some of your disks, you may need to load a driver for your hardware RAID controller.

Disks:

Disk 0
130.0 GB
Basic

Recovery
499.0 MB NTFS
Healthy (Recover

99.0 MB
Healthy (EFI parti

(C:)
129.4 GB NTFS
Healthy (Boot, Primary Partition, PageFile)

Disk 1
90.0 GB
Basic

Local Disk (E:)
90.0 GB NTFS
Healthy (Primary Partition)

Disk 2
90.0 GB
Basic

New Volume (F:)
90.0 GB NTFS

🟦 Existing volume
🟦 Extended volume
🟦 Restored volume
🟪 Unknown partition
⬛ Unallocated
🟩 Extended volume free space

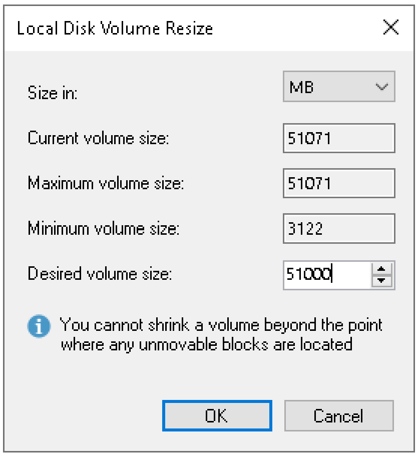
Step 5. Resize Restored Volumes

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.



Local Disk Volume Resize

Size in: MB

Current volume size: 51071

Maximum volume size: 51071

Minimum volume size: 3122

Desired volume size: 51000

You cannot shrink a volume beyond the point where any unmovable blocks are located

Step 6. Specify Secure Restore Settings

At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore. To learn more about secure restore, see the Secure Restore section in the Veeam Backup & Replication User Guide.

To specify secure restore settings:

1. In the **Content scan** section, specify the following:

   a. If you want to scan the restored volume with a scan engine or antivirus software, select the method you want to use for data scan:

      - Select the **Scan restore points with Veeam Threat Hunter** option to use Veeam Threat Hunter.

        This option is available if you configured Veeam Threat Hunter as the detection engine in the malware detection settings. To learn more, see the Signature Detection section in the Veeam Backup & Replication User Guide.

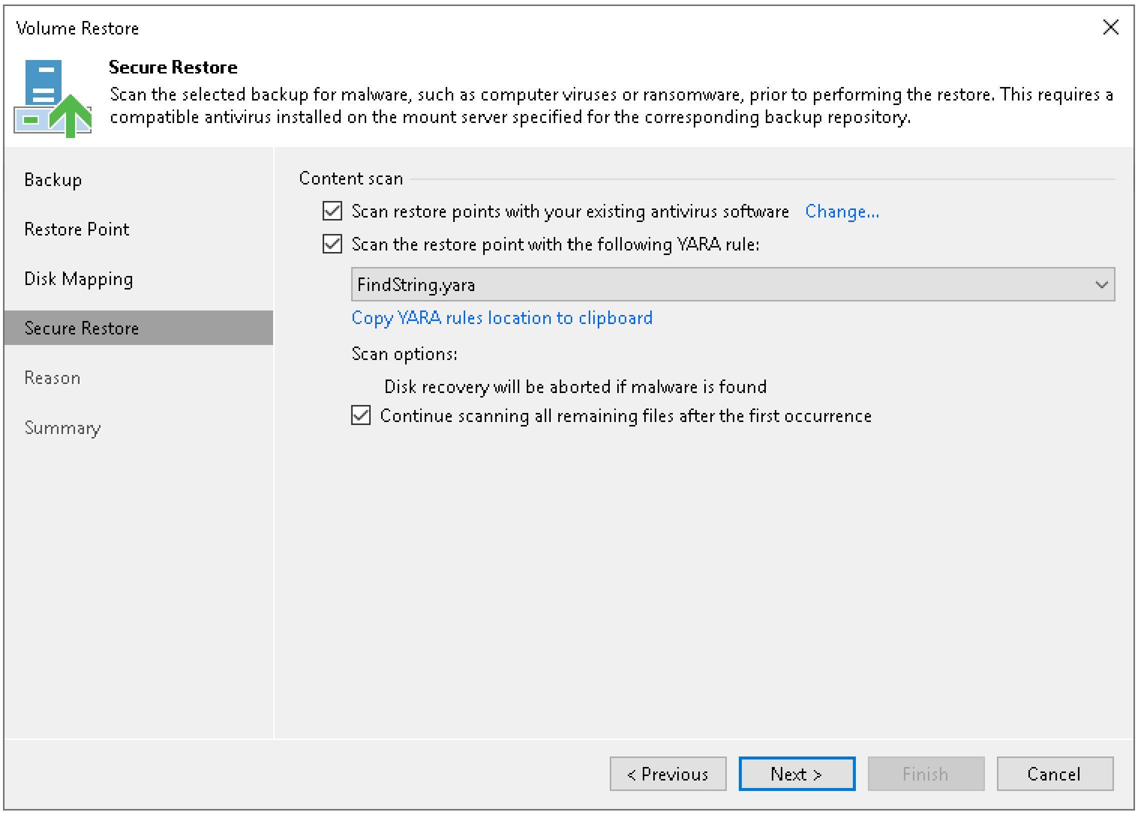
      - Select the **Scan restore points with your existing antivirus software** option to use third-party antivirus software.

        This option is available if you configured a third-party antivirus as the detection engine in the malware detection settings. To learn more, see the Signature Detection section in the Veeam Backup & Replication User Guide.

        > TIP
        >
        > Click **Change** to open the **Malware Detection Settings** window where you can change the detection engine to Veeam Threat Hunter.

   b. If you want to scan the restored volume with a YARA rule, select the **Scan backup content with the following YARA** rule check box and select a YARA rule from the drop-down list. By default, the YARA rules are located in the folder by the following path: `C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules`.

2. In the **Scan options** section, select the **Continue scanning all remaining files after the first occurence** check box if you want 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 Malware Scan Results section in the Veeam Backup & Replication User Guide.



Volume Restore

Secure Restore

Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.

Content scan

☑ Scan restore points with your existing antivirus software Change...

☑ Scan the restore point with the following YARA rule:

FindString.yara

Copy YARA rules location to clipboard

Scan options:

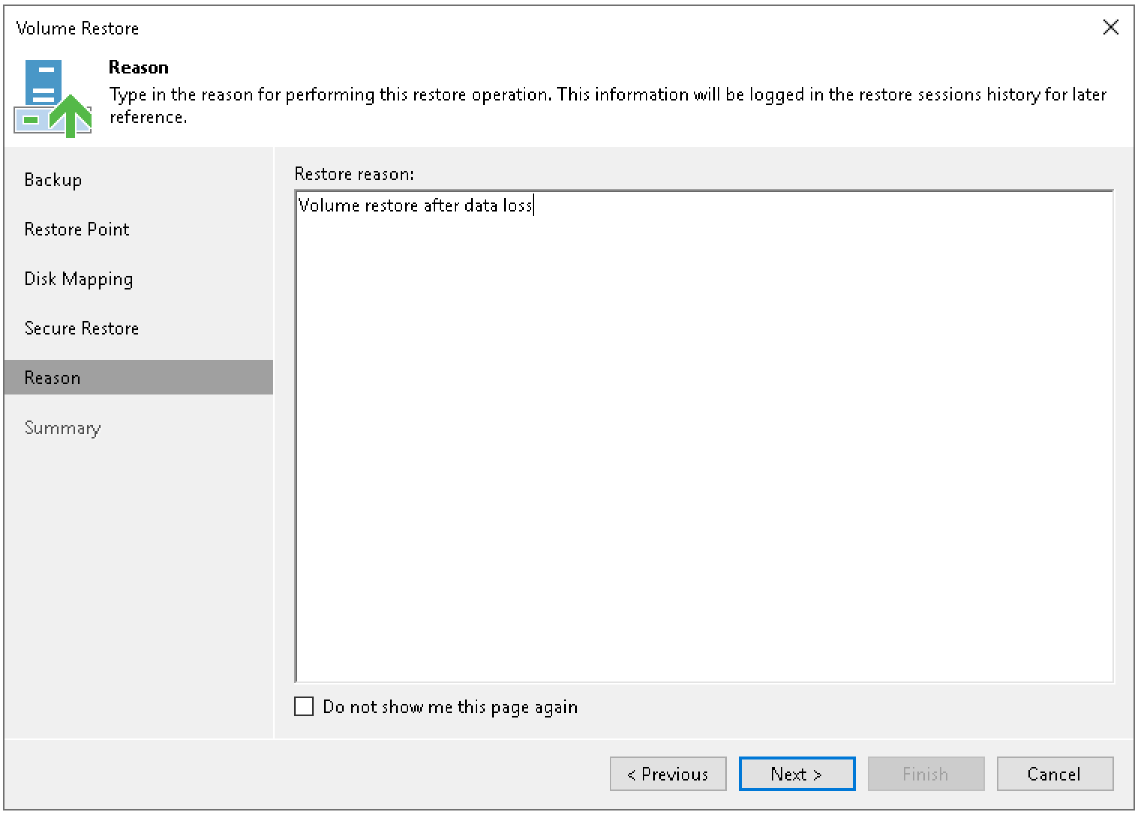
Disk recovery will be aborted if malware is found

☑ Continue scanning all remaining files after the first occurrence

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.



Volume Restore

Reason

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

Restore reason:

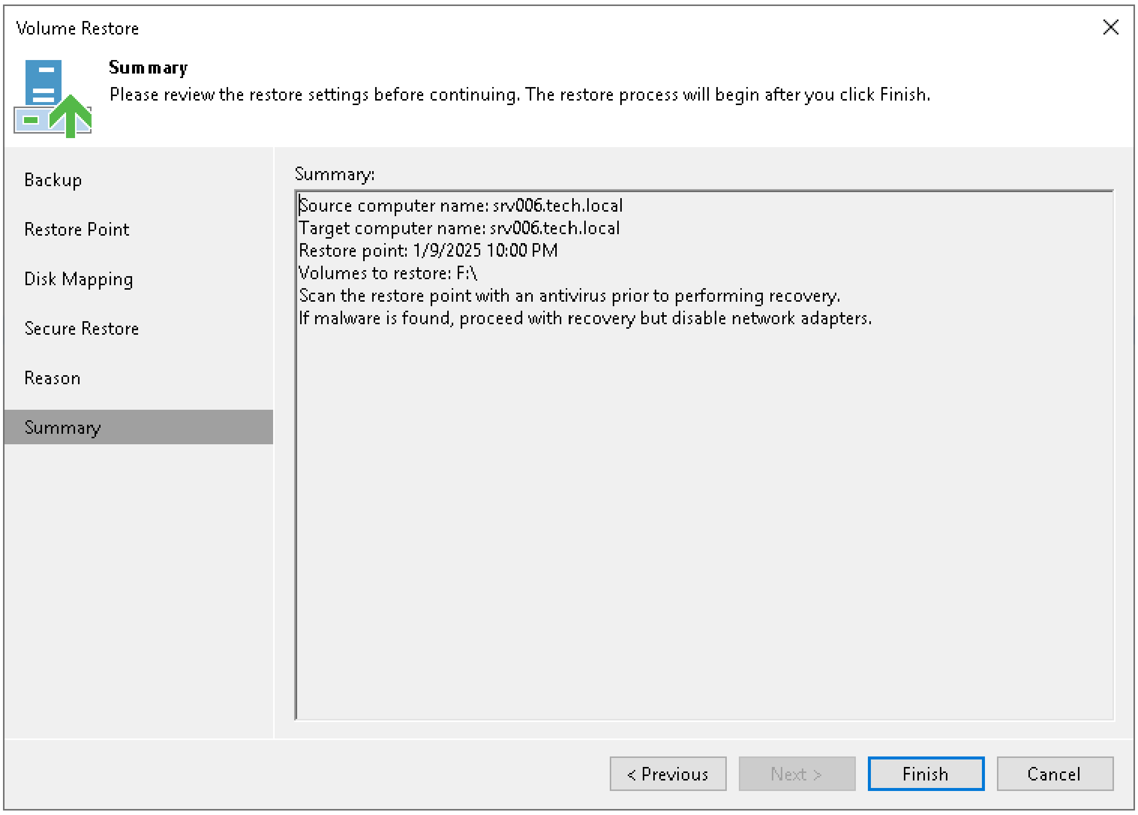
Volume restore after data loss

☐ Do not show me this page again

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, apply secure restore settings if specified, restore the necessary volume data from the backup and overwrite volume data on the target computer with the restored data.



Source computer name: srv006.tech.local
Target computer name: srv006.tech.local
Restore point: 1/9/2025 10:00 PM
Volumes to restore: F:\
Scan the restore point with an antivirus prior to performing recovery.
If malware is found, proceed with recovery but disable network adapters.

Restoring Files and Folders

You can use the Veeam Backup & Replication console to restore individual files and folders from Veeam Agent backups.

The procedure of file-level restore from a Veeam Agent backup is similar to the same procedure for a VM backup. To learn more about file-level restore, see the Restore from Microsoft Windows File Systems and Restore from Linux, Unix and Other File Systems sections in the Veeam Backup & Replication User Guide.

Consider the following:

- [For backups of Microsoft Windows computers] For file-level restore, you can only use Veeam Agent backups stored in a 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.
- [For backups of Linux, Unix and Mac computers] For file-level restore, you can only use Veeam Agent backups stored in a Veeam backup repository.
- [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.
- [For backups of Linux, Unix and Mac computers] When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of the machine from the backup or replica:
  - Mounting disks to the original host — the protected computer.

    > NOTE
    >
    > This option is not available for backups of Mac computers.

  - Mounting disks to a helper host — any Linux host from your infrastructure with a supported operating system.

    For mounting disks of Unix-based computers, you can use Linux or Unix-based helper hosts.

    > IMPORTANT
    >
    > Consider the following about using Unix-based helper hosts:
    >
    > - Unix-based helper hosts can be used for mounting disks from Veeam Agent for Unix backups only.
    > - Unix-based helper hosts must not be deployed to a WPAR or non-global zone.

  - Mounting disks to a temporary helper appliance — a helper VM required to mount computer disks from the backup.

    If you have selected to mount disks to a temporary 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*.

- [For backups of Mac computers] You cannot restore files or folders from Veeam Agent for Mac backup to the original host. You can only save files and folders to a new location over the network by using the **Copy To** option.

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:

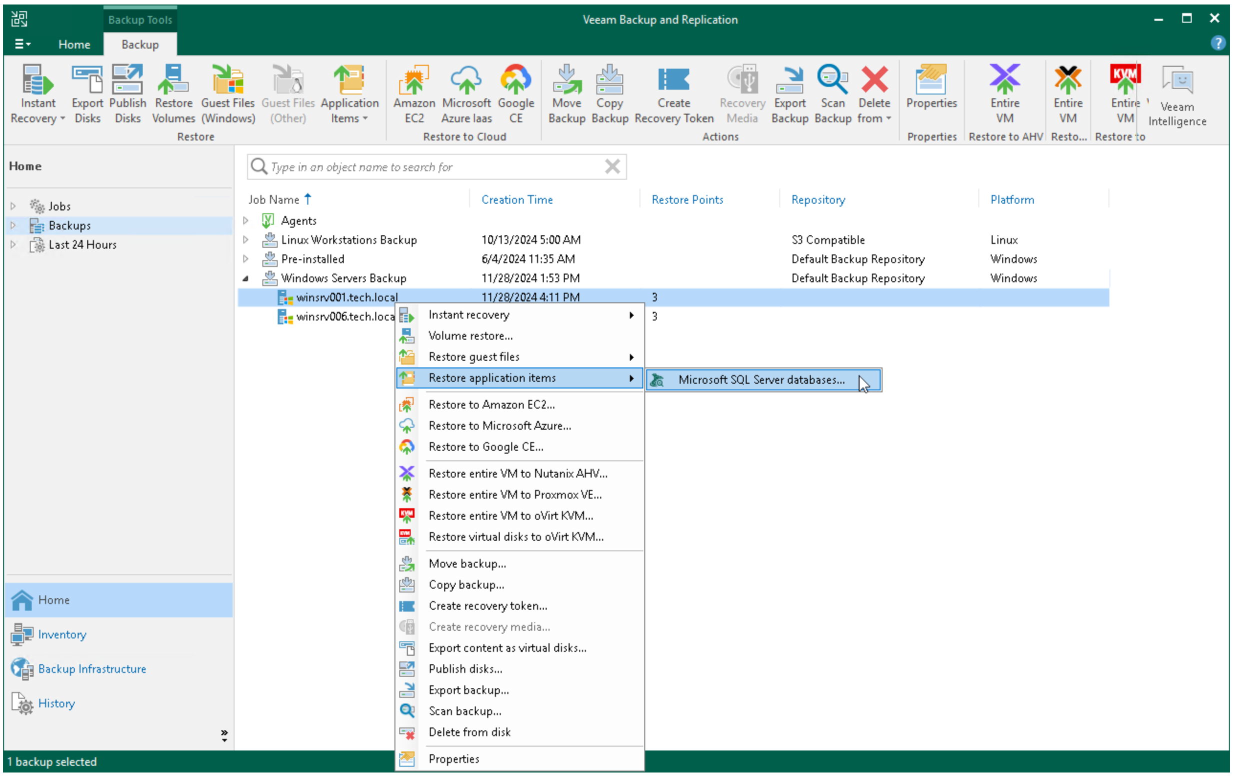
From backups created with Veeam Agent for Microsoft Windows

- 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 Application Item Restore section in the Veeam Backup & Replication User Guide.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local	11/28/2024 4:11 PM	3		
winsrv006.tech.local		3		

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 or SMB share 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 a Logical Volume Manager (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.

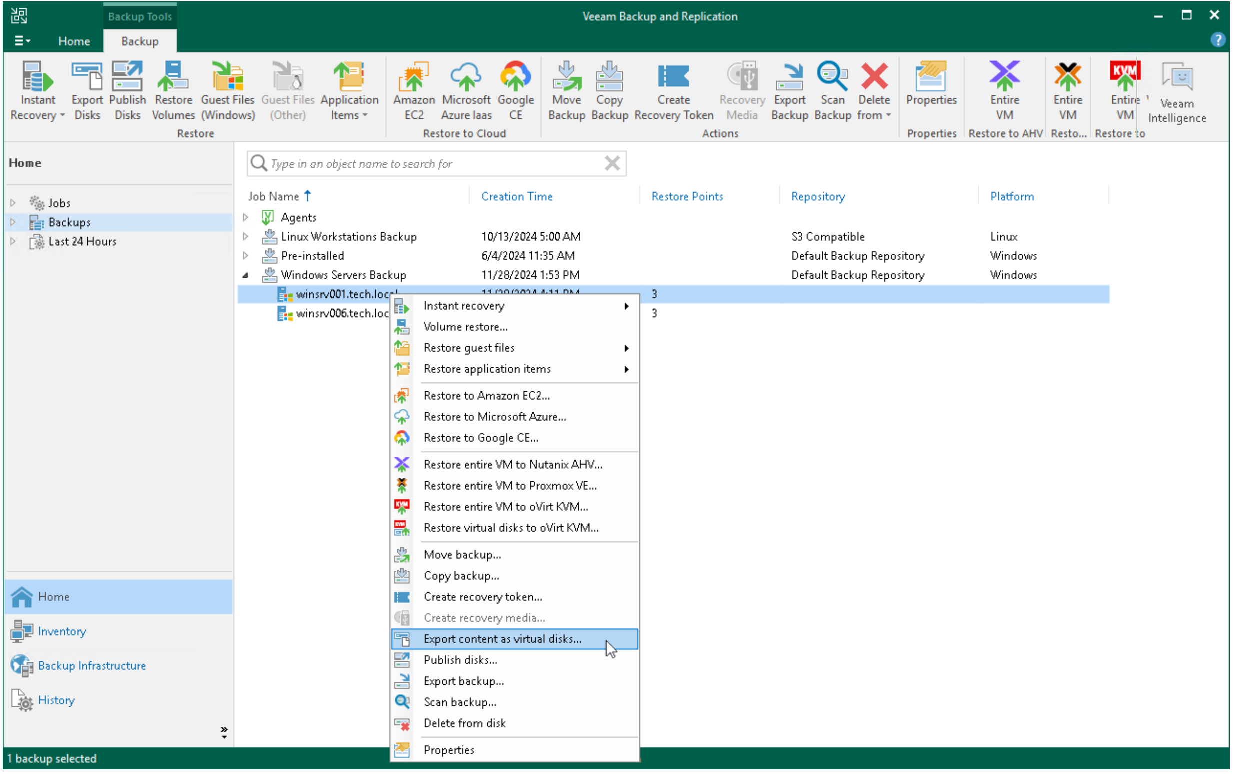
To restore disks and convert them to the VMDK, VHD or VHDX format, perform the following steps in the **Export Disk** wizard:

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**.

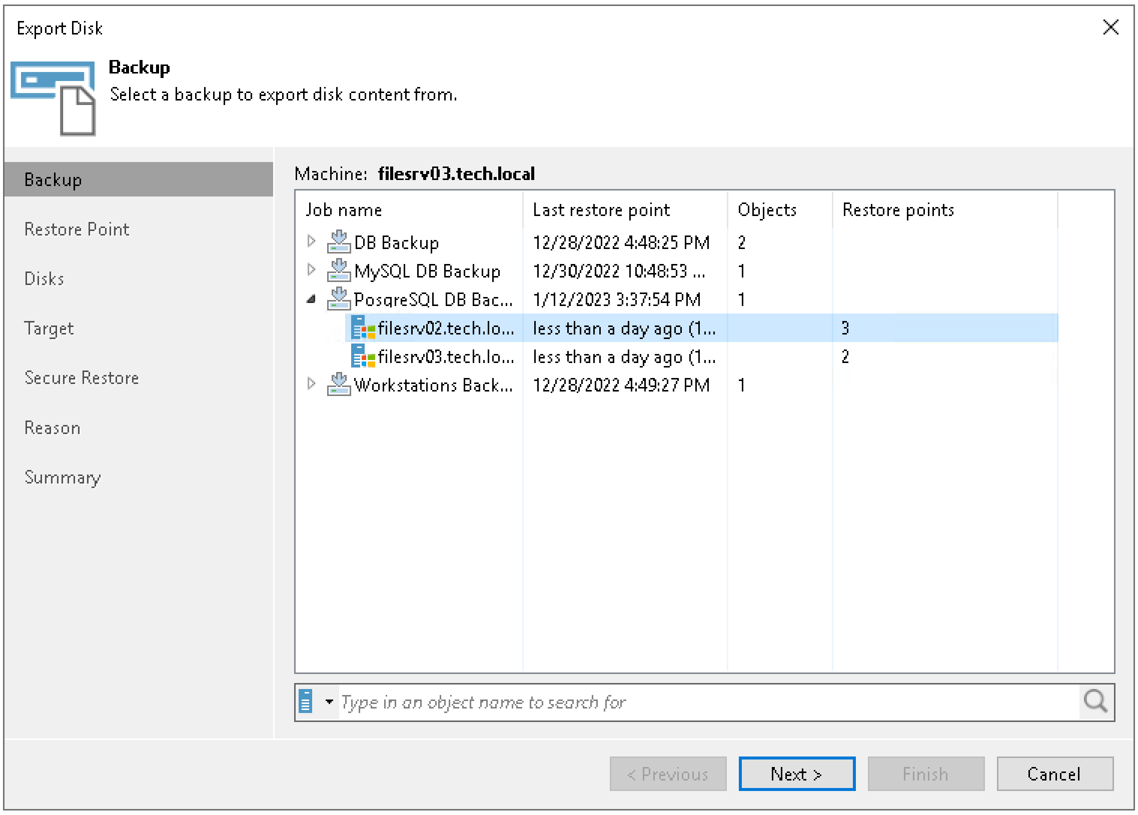
  In this case, you will pass immediately to the Restore Point step of the wizard.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.loc		3		
winsrv006.tech.loc		3		

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.



Export Disk

Backup

Select a backup to export disk content from.

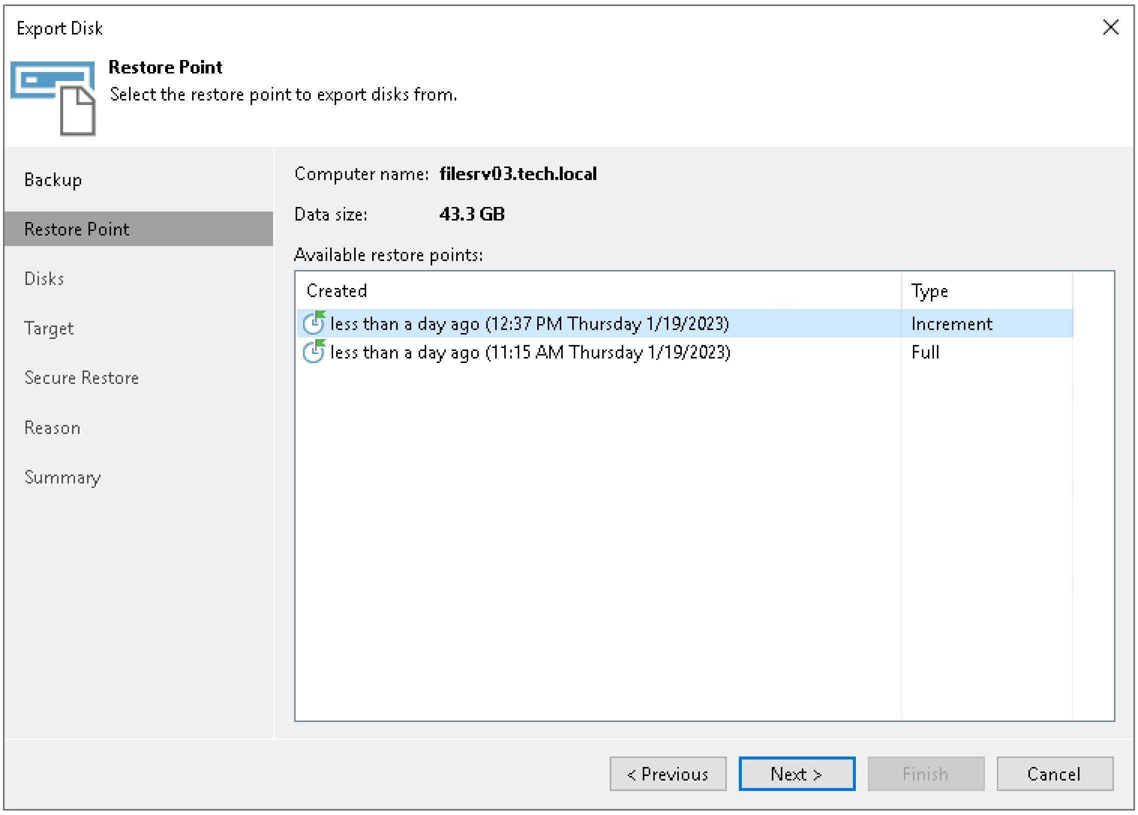
Machine: **filesrv03.tech.local**

Job name	Last restore point	Objects	Restore points
DB Backup	12/28/2022 4:48:25 PM	2	
MySQL DB Backup	12/30/2022 10:48:53 ...	1	
PosgreSQL DB Bac...	1/12/2023 3:37:54 PM	1	
filesrv02.tech.lo...	less than a day ago (1...		3
filesrv03.tech.lo...	less than a day ago (1...		2
Workstations Back...	12/28/2022 4:49:27 PM	1	

Type in an object name to search for

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.



Export Disk

Restore Point

Select the restore point to export disks from.

Computer name: **filesrv03.tech.local**

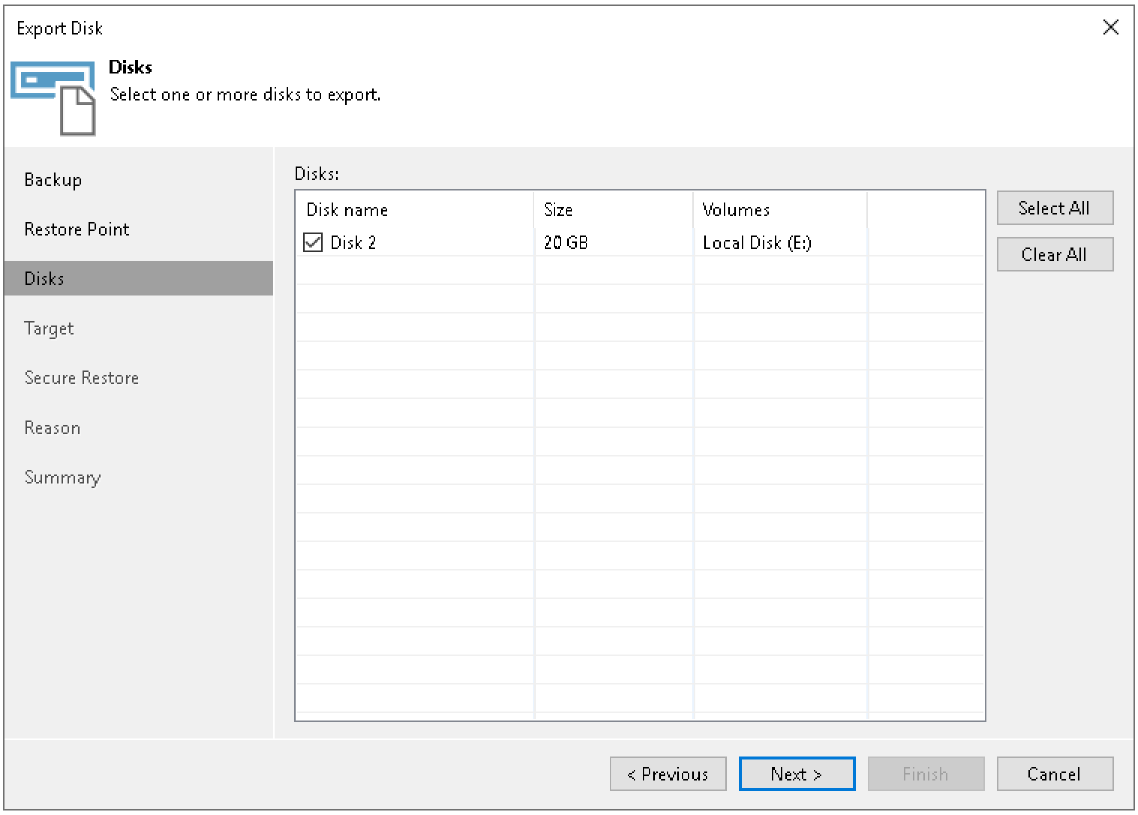
Data size: **43.3 GB**

Available restore points:

Created	Type
less than a day ago (12:37 PM Thursday 1/19/2023)	Increment
less than a day ago (11:15 AM Thursday 1/19/2023)	Full

Step 4. Select Disks

At the **Disks** step of the wizard, select check boxes next to those disks that you want to export.



Export Disk

Disks

Select one or more disks to export.

Disks:

Disk name	Size	Volumes
☑ Disk 2	20 GB	Local Disk (E:)

Step 5. Select Destination and Disk Format

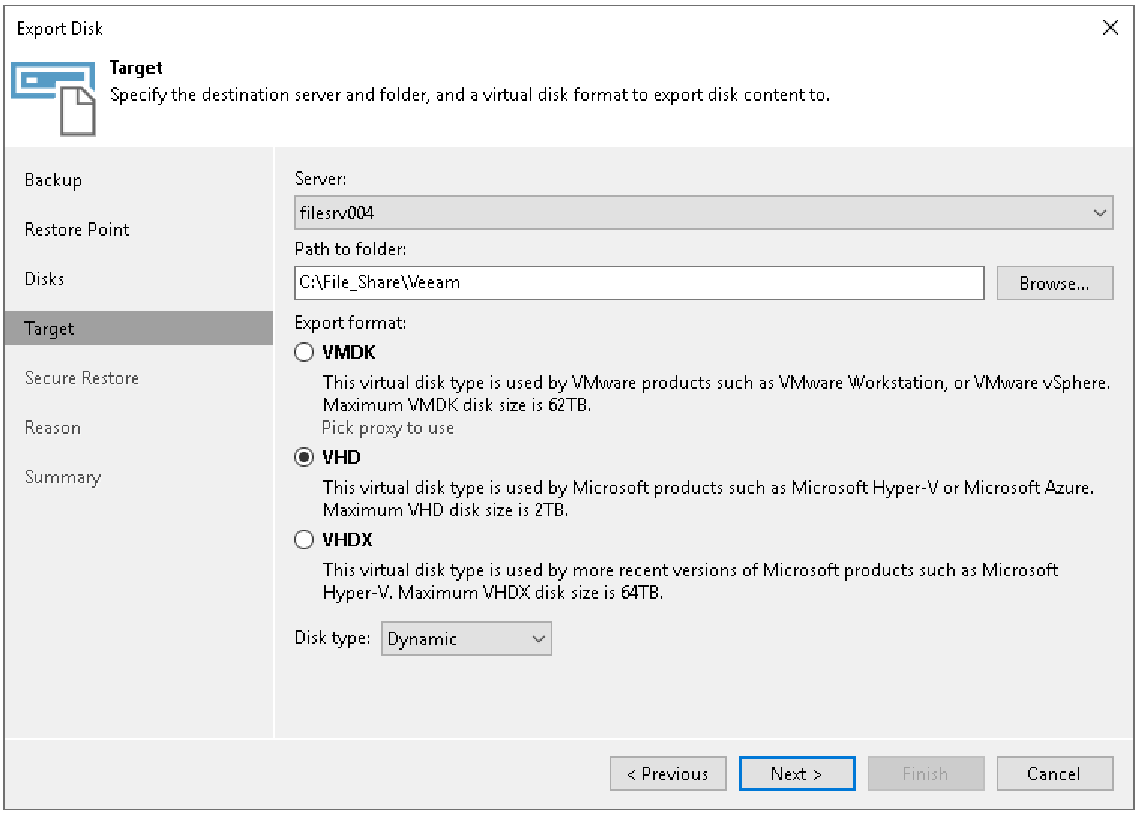
At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk.

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 in 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.

Server: filesrv004

Path to folder: C:\File_Share\Veeam

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

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 the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan restored disk data with antivirus software before restoring the disk. To learn more about secure restore, see the Secure Restore section in the Veeam Backup & Replication User Guide.

To specify secure restore settings:

1. In the **Content scan** section, specify the following:

   a. If you want to scan the restored volume with a scan engine or antivirus software, select the method you want to use for data scan:

      - Select the **Scan restore points with Veeam Threat Hunter** option to use Veeam Threat Hunter.

        This option is available if you configured Veeam Threat Hunter as the detection engine in the malware detection settings. To learn more, see the Signature Detection section in the Veeam Backup & Replication User Guide.

      - Select the **Scan restore points with your existing antivirus software** option to use third-party antivirus software.

        This option is available if you configured a third-party antivirus as the detection engine in the malware detection settings. To learn more, see the Signature Detection section in the Veeam Backup & Replication User Guide.

        > **TIP**
        >
        > Click **Change** to open the **Malware Detection Settings** window where you can change the detection engine to Veeam Threat Hunter.

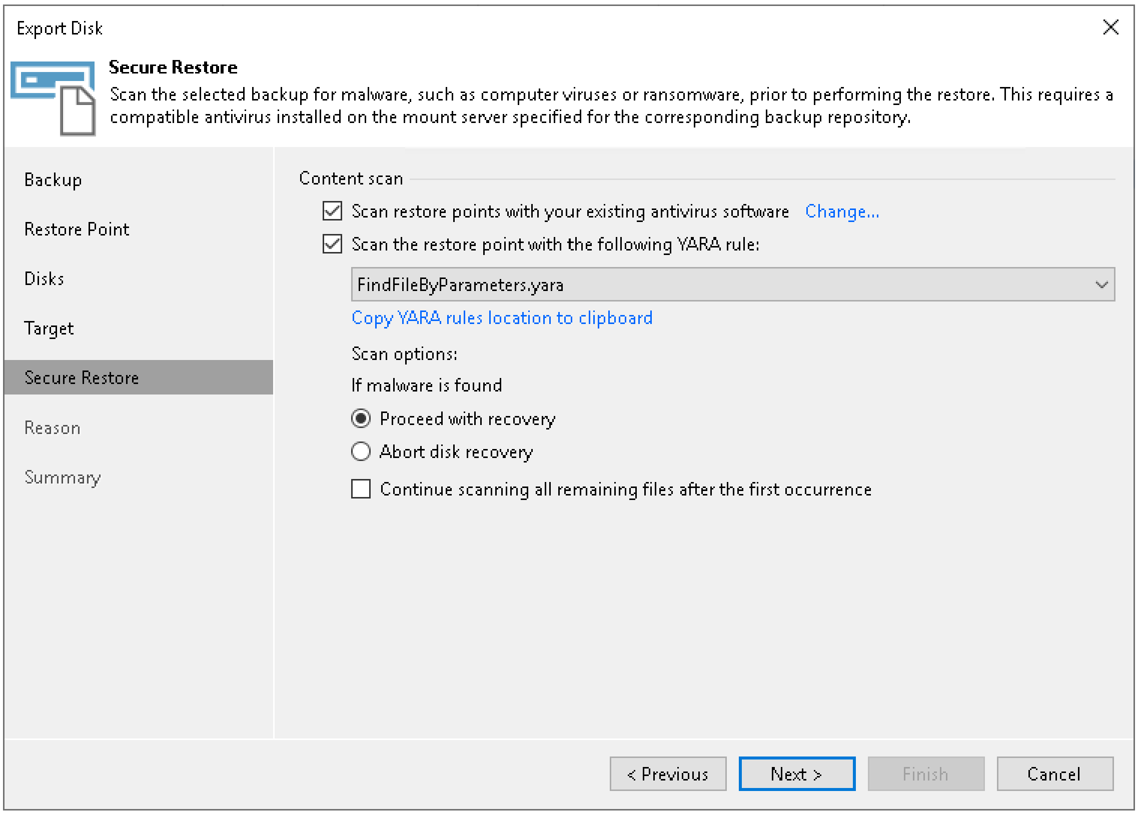
   b. To use a YARA rule as a scan engine, select the **Scan the restore point with the following YARA** rule check box and choose a YARA rule from the drop-down list. By default, the YARA rules are located in the folder by the following path: `C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules`.

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. In the **Scan options** section, select the **Continue scanning all remaining files after the first occurrence** 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 Malware Scan Results section in the Veeam Backup & Replication User Guide.



Export Disk

Secure Restore

Scan the selected backup for malware, such as computer viruses or ransomware, prior to performing the restore. This requires a compatible antivirus installed on the mount server specified for the corresponding backup repository.

Content scan

☑ Scan restore points with your existing antivirus software Change...

☑ Scan the restore point with the following YARA rule:

FindFileByParameters.yara

Copy YARA rules location to clipboard

Scan options:

If malware is found

● Proceed with recovery

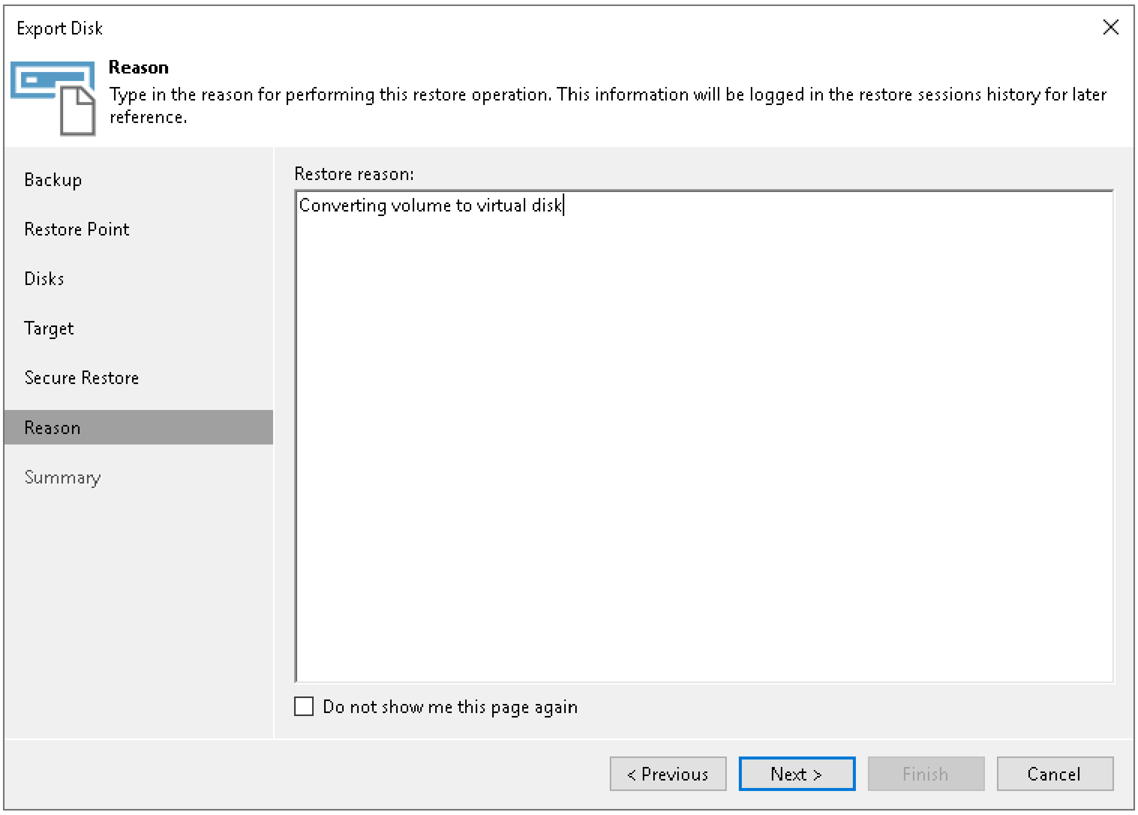
○ Abort disk recovery

□ Continue scanning all remaining files after the first occurrence

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.



Export Disk

Reason

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

Restore reason:

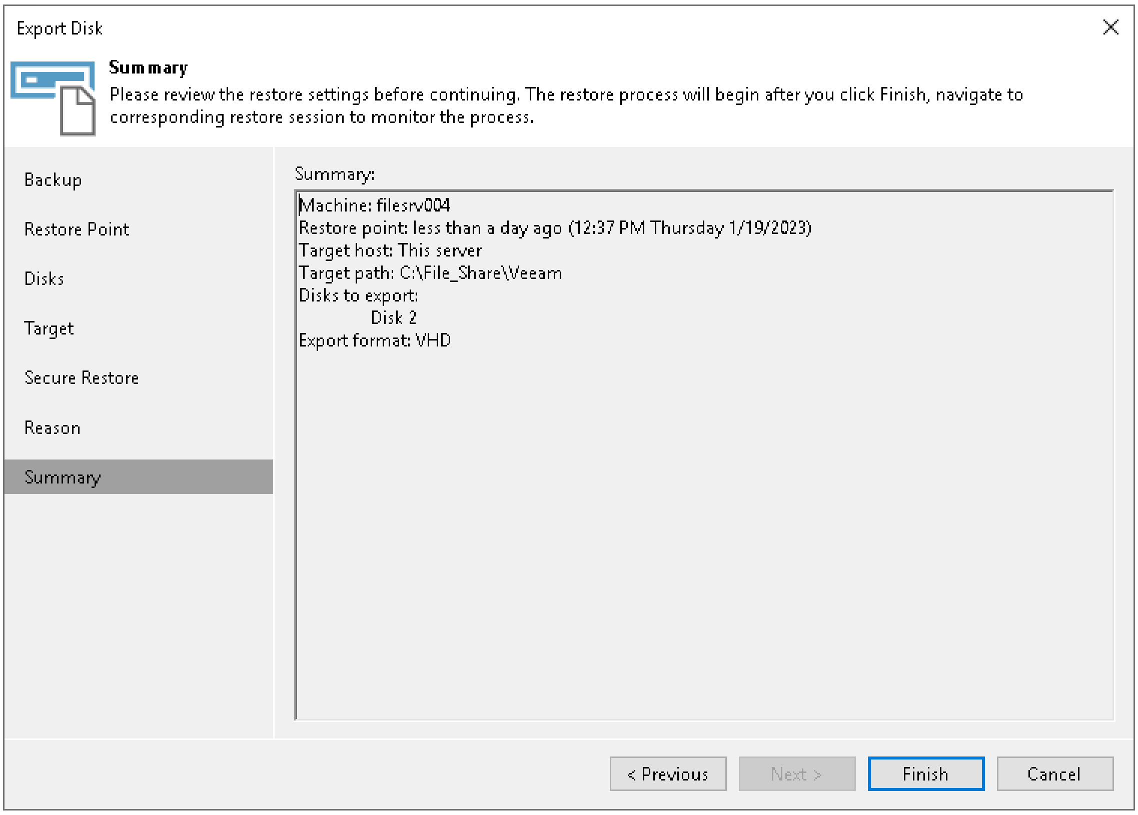
Converting volume to virtual disk

□ Do not show me this page again

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.



Export Disk

Summary

Please review the restore settings before continuing. The restore process will begin after you click Finish, navigate to corresponding restore session to monitor the process.

Summary:

```
Machine: filesrv004
Restore point: less than a day ago (12:37 PM Thursday 1/19/2023)
Target host: This server
Target path: C:\File_Share\Veeam
Disks to export:
            Disk 2
Export format: VHD
```

Publishing Disks

You can use the Veeam backup console to publish disks from Veeam Agent backups.

> TIP
>
> You can publish disks using the PowerShell console. To learn more, see the Disk Publishing (Data Integration API) section in the Veeam PowerShell Reference.

Disk publishing allows you to save time by getting backup content of one or multiple disks instead of all disks from a backup. This technology gives read-only access to data and helps if you want to analyze data of your backup. For example, look for specific documents or usage patterns, or perform antivirus scan of backed-up data.

You can publish disks from backups of Veeam Agent computers created with the following Veeam Agents:

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

To publish disks from a backup of a Veeam Agent computer to a target server, Veeam Backup & Replication uses one of the following storage network protocols depending on the target server OS:

- [For Windows-based target servers] iSCSI
- [For Linux and macOS-based target servers] FUSE
- [For Unix-based target servers] NFS

To learn more, see the Disk Publishing section in the Veeam Backup & Replication User Guide.

Performing Disk Publish

Before you publish disks, check prerequisites. Then use the **Publish Disks** wizard.

1. Launch the wizard.
2. Select a Veeam Agent computer whose disks you want to publish.
3. Select a restore point.
4. Select disks.
5. Specify the target server.
6. Specify a reason for disk publishing.
7. Finish working with the wizard.

Before You Begin

Before you publish disks, check the following requirements and limitations:

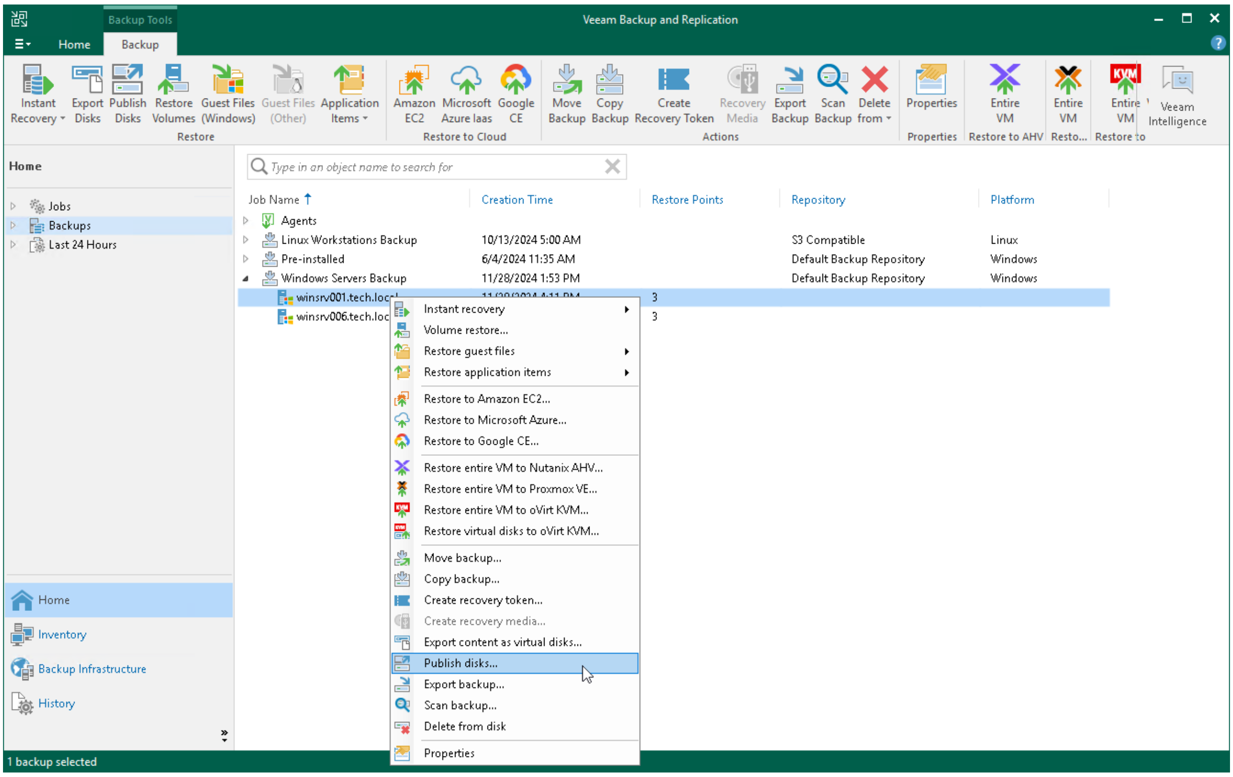
- The necessary ports must be opened on the target server. For more information, see Ports.
- The target server must support the file system of the disk that you plan to publish.
- macOS computers are not supported as target servers.
- Unix servers are supported as target servers for publishing disks only from backups of Unix-based computers
- If data deduplication is enabled for some disks in a backup, data deduplication must be enabled on the target server.
- [For Microsoft Windows-based Veeam Agent computers] The target Microsoft Windows server must support the same ReFS version or later than the version used on the Veeam Agent computer from which you plan to publish disks. For more information on which OSes support which ReFS, see the ReFS versions and compatibility matrix.
- [For Linux-based, Unix-based and macOS-based Veeam Agent computers] The 32-bit version of a Linux server is not supported as the target server.
- [For Linux-based, Unix-based and macOS-based Veeam Agent computers] You cannot publish disks from backups stored in the Veeam Cloud Connect repository.

For the full list of limitations, see the Considerations and Limitations section in the Veeam Backup & Replication User Guide.

Step 1. Launch Publish Disks Wizard

To launch the **Publish Disks** wizard, do either of the following:

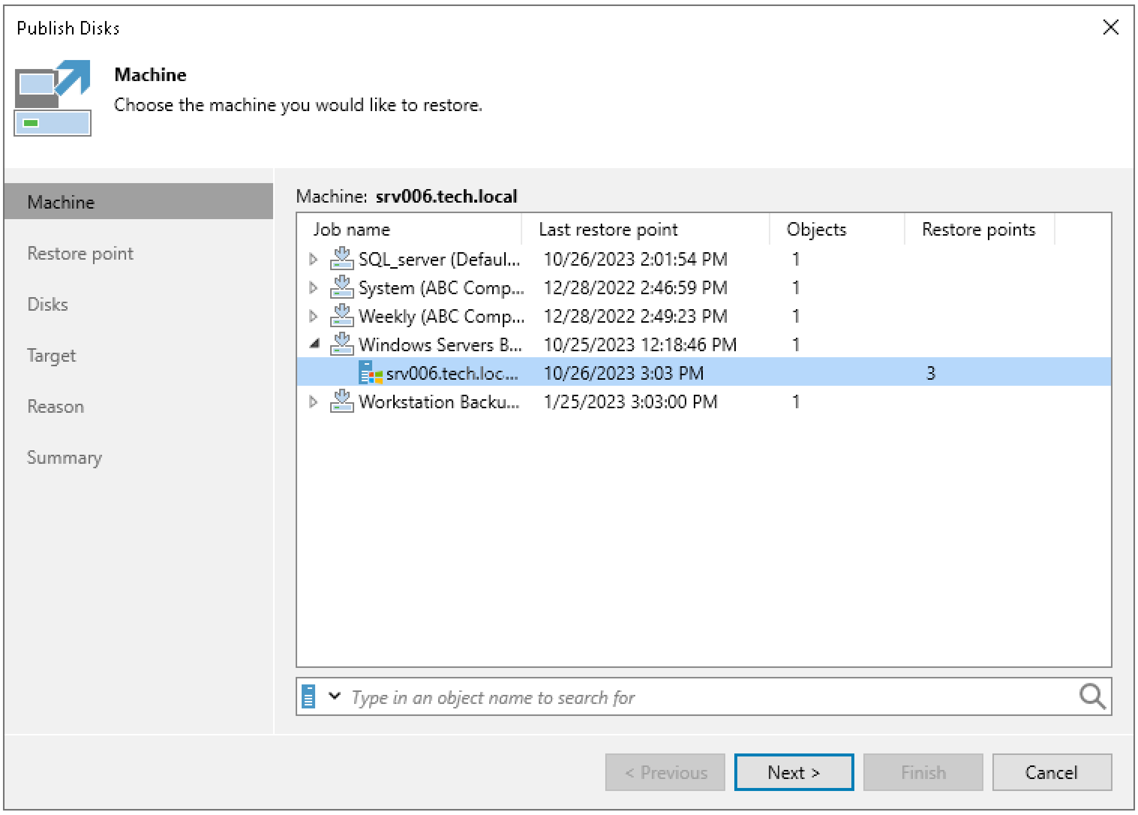
- On the **Home** tab, click **Restore** > **Agent** > **Disk Restore** > **Publish disk**.
- Open the **Home** view. In the inventory pane, click **Backups**. In the working area, expand the necessary Veeam Agent backup, select a computer whose disks you want to publish and click **Publish Disks** on the ribbon. Alternatively, you can right-click the computer and select **Publish disks**. In this case, you will proceed to the Restore point step of the wizard.



Job Name ↑	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local	11/28/2024 4:11 PM	3		
winsrv006.tech.loc		3		

Step 2. Select Computer

At the **Machine** step of the wizard, expand a backup and select a Veeam Agent computer whose disks you want to publish.



Publish Disks

Machine

Choose the machine you would like to restore.

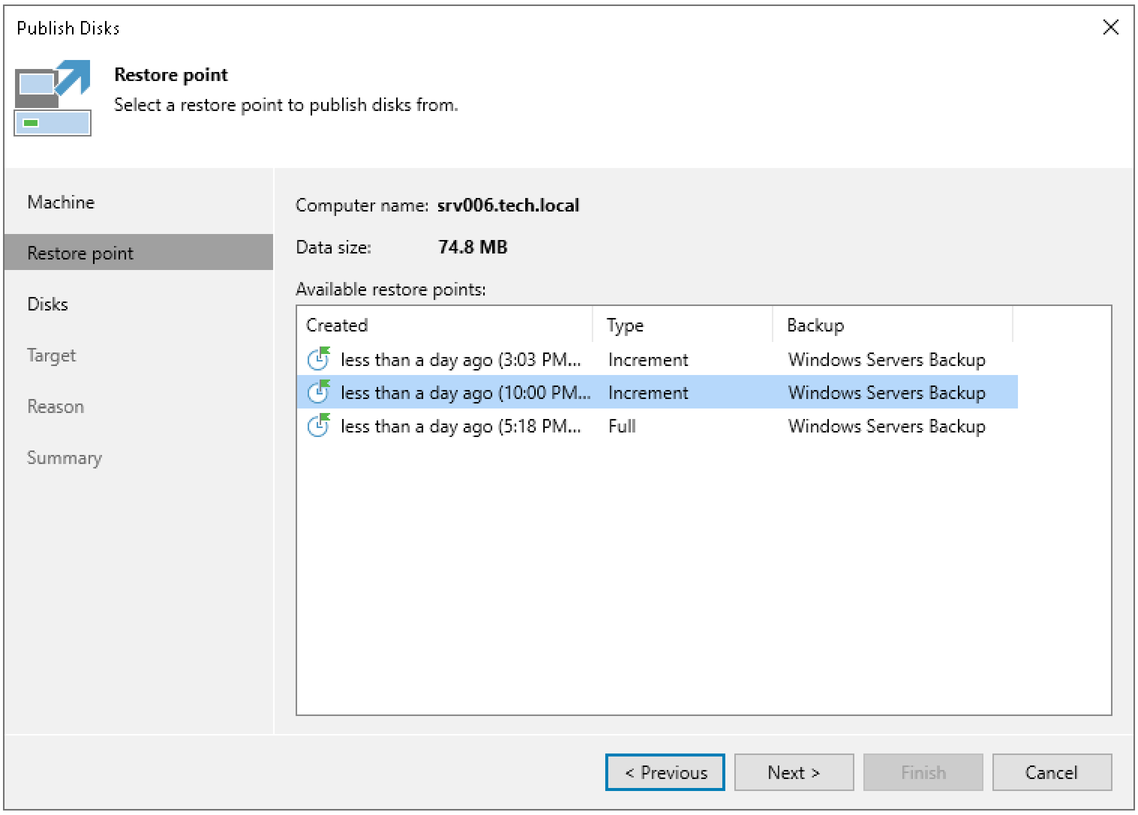
Machine: **srv006.tech.local**

Job name	Last restore point	Objects	Restore points
SQL_server (Defaul...	10/26/2023 2:01:54 PM	1	
System (ABC Comp...	12/28/2022 2:46:59 PM	1	
Weekly (ABC Comp...	12/28/2022 2:49:23 PM	1	
Windows Servers B...	10/25/2023 12:18:46 PM	1	
srv006.tech.loc...	10/26/2023 3:03 PM		3
Workstation Backu...	1/25/2023 3:03:00 PM	1	

Type in an object name to search for

Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to publish disks.



Publish Disks

Restore point

Select a restore point to publish disks from.

Computer name: **srv006.tech.local**

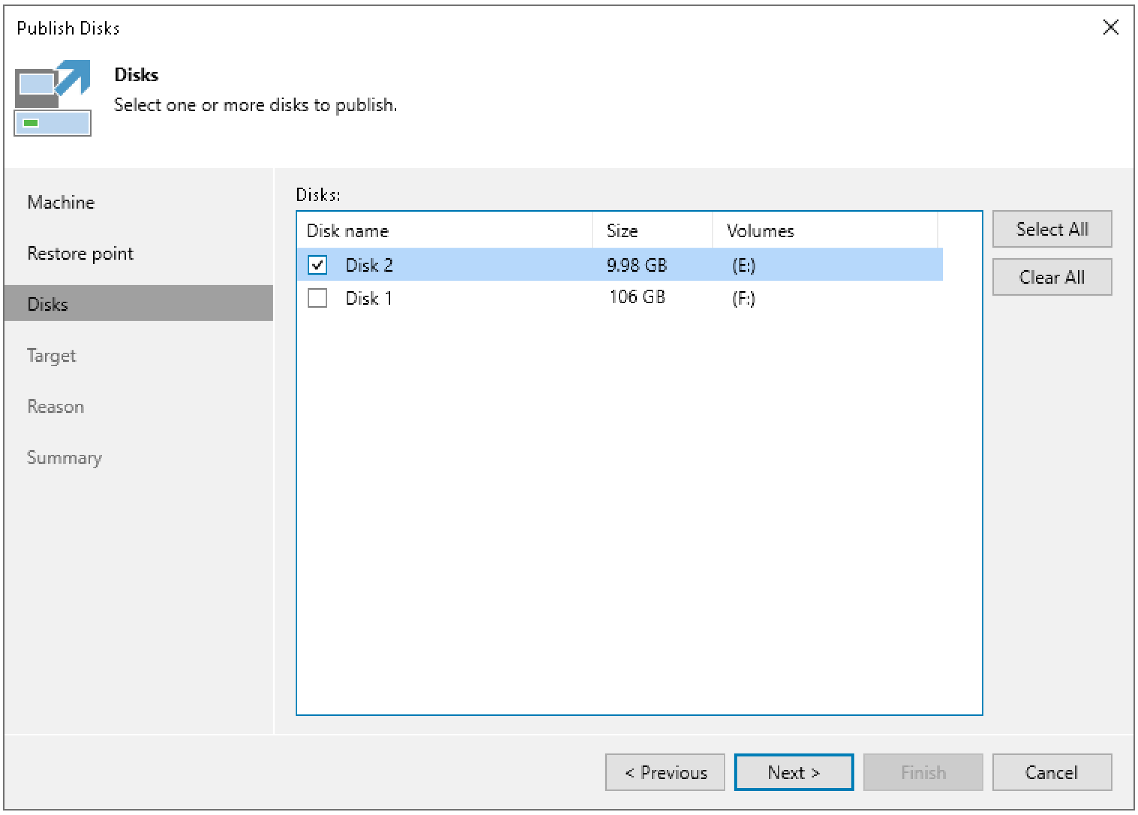
Data size: **74.8 MB**

Available restore points:

Created	Type	Backup
less than a day ago (3:03 PM...	Increment	Windows Servers Backup
less than a day ago (10:00 PM...	Increment	Windows Servers Backup
less than a day ago (5:18 PM...	Full	Windows Servers Backup

Step 4. Select Disks

At the **Disks** step of the wizard, select a check box next to the disks that you want to publish. Click **Select All** if you want to select all disks from the backup.



Publish Disks

Disks

Select one or more disks to publish.

Disks:

Disk name	Size	Volumes
☑ Disk 2	9.98 GB	(E:)
□ Disk 1	106 GB	(F:)

Step 5. Select Target Server

At the **Target** step of the wizard, select a server that will have access to disk content. You can select the following servers depending on the OS of the Veeam Agent computer:

- Linux server — for Linux-based, Unix-based and macOS-based Veeam Agent computers.
- Microsoft Windows server — for Microsoft Windows-based Veeam Agent computers.

You can select one of the following types of servers:

- A server added to the backup infrastructure.

  If you want to add a new backup server to the backup infrastructure at this step, click **Add**. In this case, you will be able to add a new Microsoft Windows server or a new Linux server. To learn more, see the Adding Microsoft Windows Servers and the Adding Linux Servers section in the Veeam Backup & Replication User Guide.

- A temporary server. In this case, select *Specify a different host* from the drop-down list. In the **Target Server** window, specify the following settings:

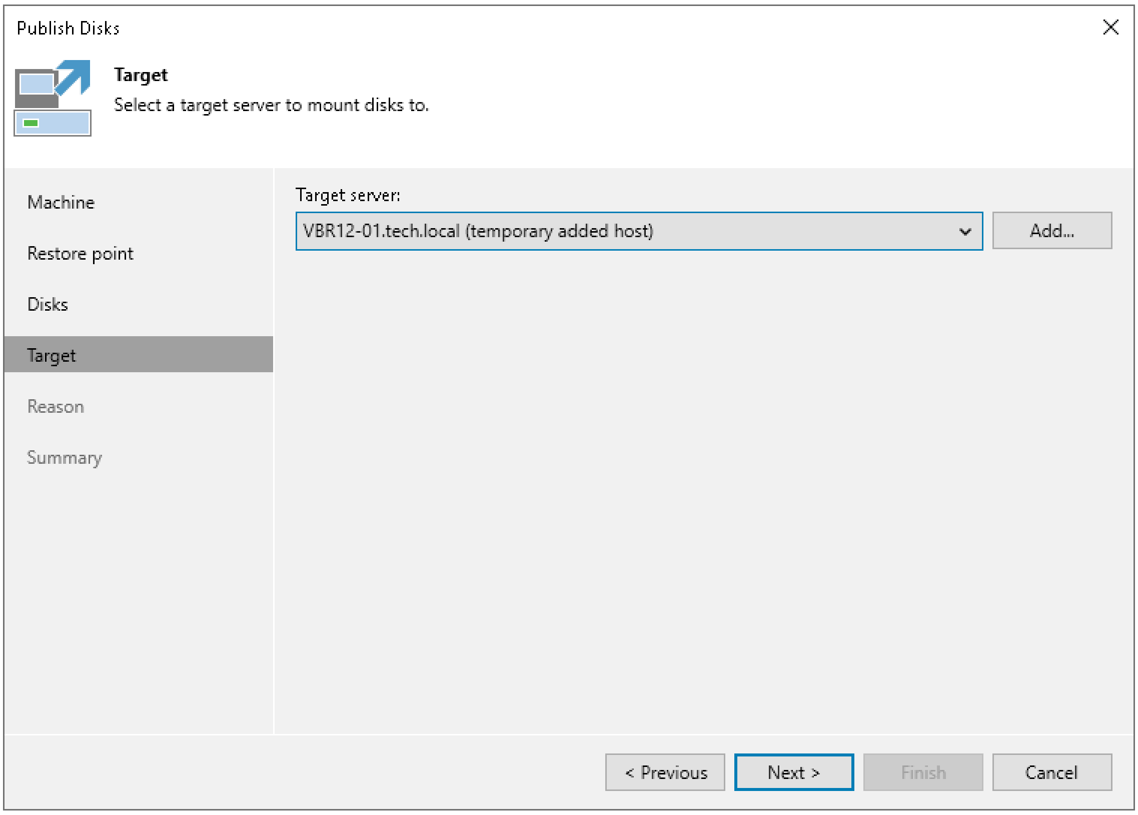
  a. In the **Host name** field, specify a server name or IP address of the server.

  b. 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 a new account in the Credentials Manager. To learn more, see the Credentials Manager section in the Veeam Backup & Replication User Guide.

  c. [For Linux-based, Unix-based and macOS-based Veeam Agent computers] Click **Advanced** and customize connection settings in the **Network Settings window**. To learn more, see Customizing Connection Settings.

- [For Microsoft Windows-based and Linux-based Veeam Agent computers] The original server. In this case, select *Original server* from the drop-down list.

If prompted, specify credentials for the target server.


Publish Disks

Target
Select a target server to mount disks to.

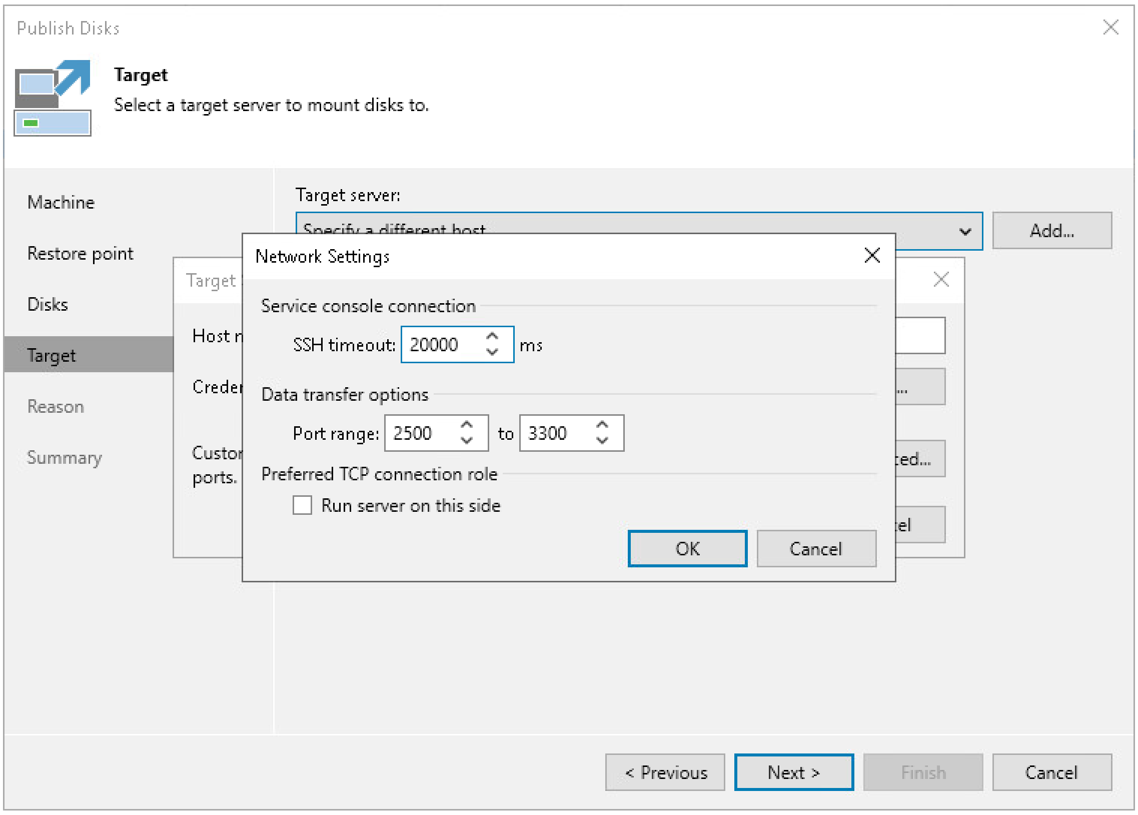
Target server: VBR12-01.tech.local (temporary added host)

Customizing Connection Settings

If necessary, you can customize connection settings for a target Linux server at the **Target** step of the **Publish Disks** wizard. To do so, click **Advanced** in the **Target Server** window and specify settings in the **Network Settings window**:

1. In the **Service console connection** section, specify an SSH timeout.
2. In the **Data transfer options** section, specify connection settings for file copy operations.
3. [For Linux server deployed outside NAT] In the **Preferred TCP connection role** section, select the **Run server on this side** check box.

To learn more about these settings, see the Specify Credentials and SSH Settings section in the Veeam Backup & Replication User Guide.



SSH timeout: 20000 ms

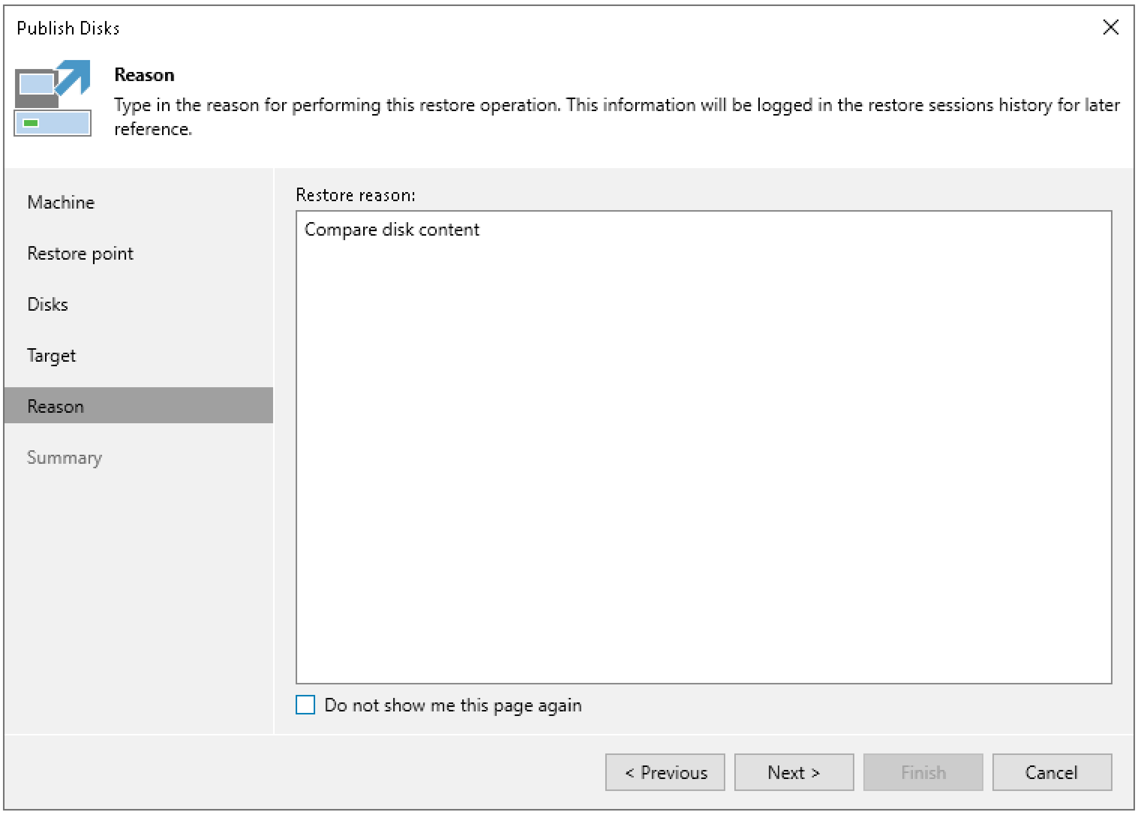
Port range: 2500 to 3300

□ Run server on this side

Step 6. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for publishing disks.

> **TIP**
>
> If you do not want to show this page, select the **Do not show me this page again** check box. If you further will want to return this page, follow the instructions described in this Veeam KB article.



Publish Disks

Reason

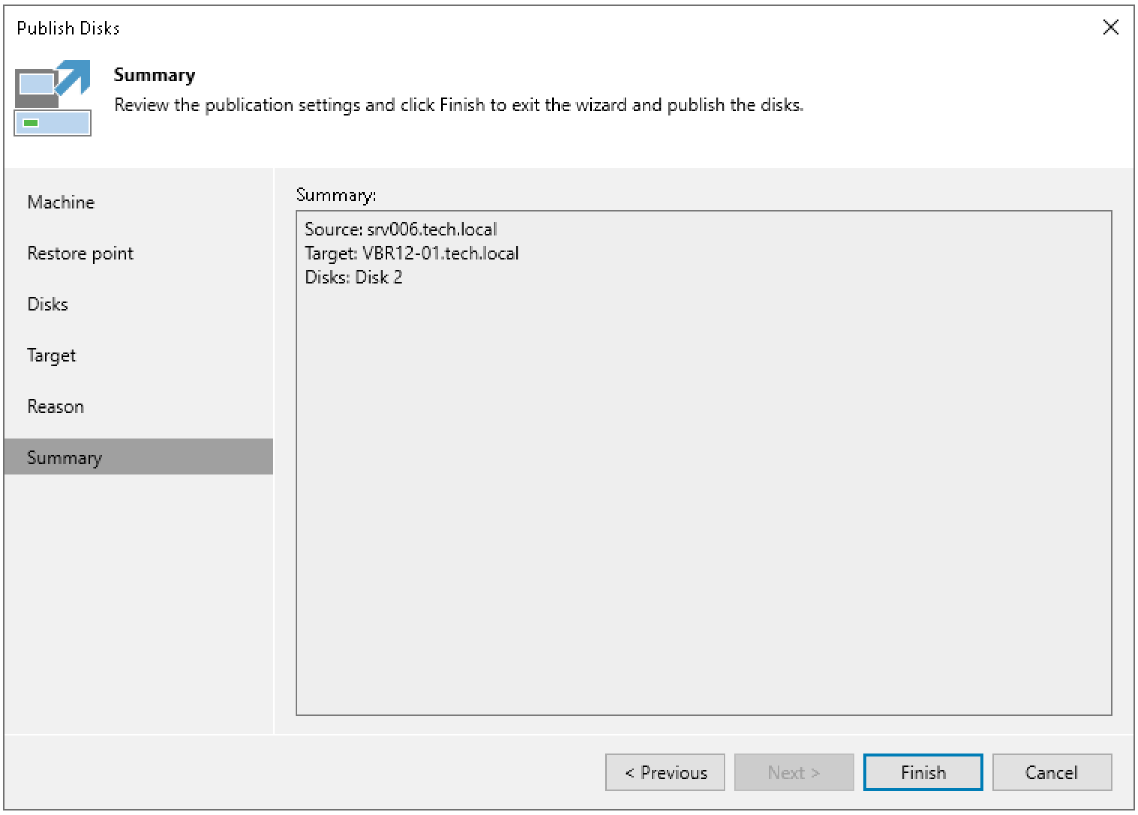
Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.

Restore reason: Compare disk content

□ Do not show me this page again

Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review the configured settings and click **Finish**.



Summary:

Source: srv006.tech.local
Target: VBR12-01.tech.local
Disks: Disk 2

What You Do Next

After the disks are published, go to the following locations on the target server to browse disks content:

- [For Windows servers] Go to `C:\VeeamFLR\` folder.
- [For Linux servers] Go to the `/tmp/Veeam.Mount.Disks` location to browse disks images. Go to the `/tmp/Veeam.Mount.FS` location to browse disks content.

After you started a disks publishing session, you can view the session statistics or stop the session from the Veeam backup console. To learn more, see Managing Publishing Disks Session.

Managing Publishing Disks Session

After you started a publishing session, you can check details about the session or stop it.

Viewing Statistics on Publishing Session

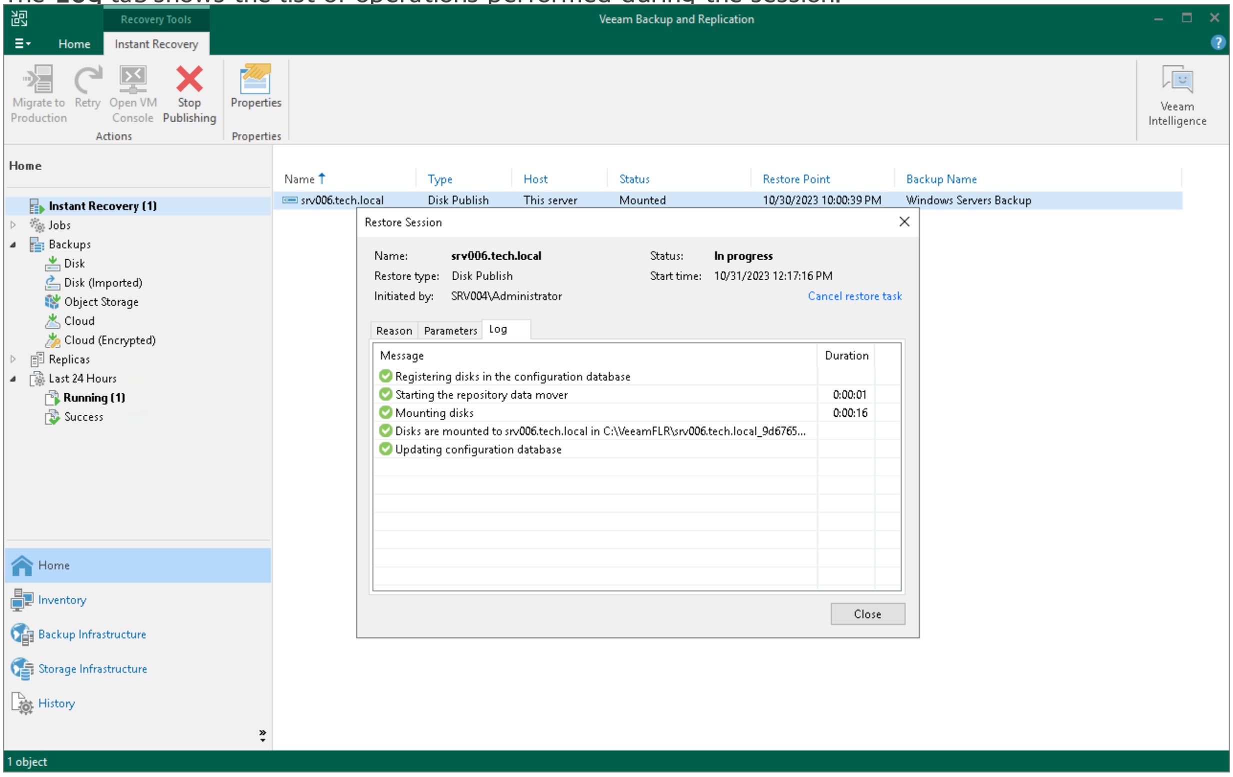
To view publishing session statistics, do one of the following:

- Open the **Home** view. In the inventory pane, select **Instant Recovery.** In the working area, select the necessary publishing session and click **Properties** on the ribbon. Alternatively, right-click the session and **Properties**.
- Open the **Home** view. In the inventory pane select **Last 24 hours**. In the working area, double-click the necessary publishing session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.
- Open the **History** view. In the inventory pane select **Restore**. In the working area, double-click the necessary publishing session. Alternatively, you can select the session and click **Statistics** on the ribbon or right-click the session and select **Statistics**.

The publishing statistics provides the following data:

- At the top of the **Restore Session** window, Veeam Backup & Replication shows general session statistics. It includes a name of the Veeam Agent computer whose disk you want to publish, a name of the backup server which initiated the publishing session, a user name of the account under which the session was started, session status and duration details.
- The **Reason** tab shows the reason for the publishing session.
- The **Parameters** tab shows information about the target server, the Veeam Agent computer whose disks you publish and the restore point selected for publishing.

- The **Log** tab shows the list of operations performed during the session.



Name	Type	Host	Status	Restore Point	Backup Name
srv006.tech.local	Disk Publish	This server	Mounted	10/30/2023 10:00:39 PM	Windows Servers Backup

Name: **srv006.tech.local**
Restore type: Disk Publish
Initiated by: SRV004\Administrator
Status: **In progress**
Start time: 10/31/2023 12:17:16 PM

Message	Duration
✓ Registering disks in the configuration database	
✓ Starting the repository data mover	0:00:01
✓ Mounting disks	0:00:16
✓ Disks are mounted to srv006.tech.local in C:\VeeamFLR\srv006.tech.local_9d6765...	
✓ Updating configuration database	

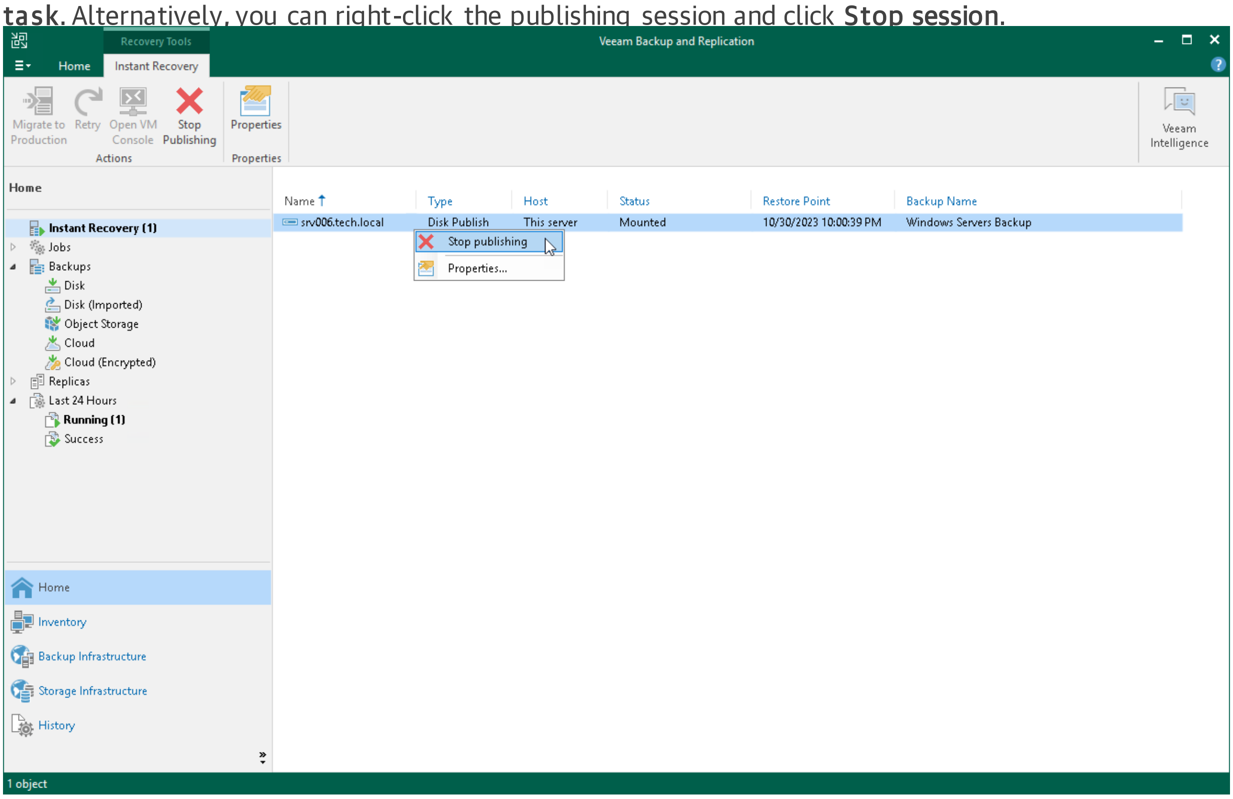
Stopping Publishing Session

To stop a publishing session, do one of the following:

- Open the **Home** view. In the inventory pane select **Instant Recovery**. In the working area, double-click the necessary publishing session and click **Cancel restore task** in the **Restore Session** window. Alternatively, you can select the necessary publishing session and click **Stop Publishing** on the ribbon or right-click the session and click **Stop Publishing**.

- Open the **Home** view. In the inventory pane select **Last 24 hours**. In the working area, double-click the necessary publishing session and click **Cancel restore task** in the **Restore Session** window. Alternatively, you can select the necessary publishing session and click **Stop** on the ribbon or right-click the session and click **Stop session**.

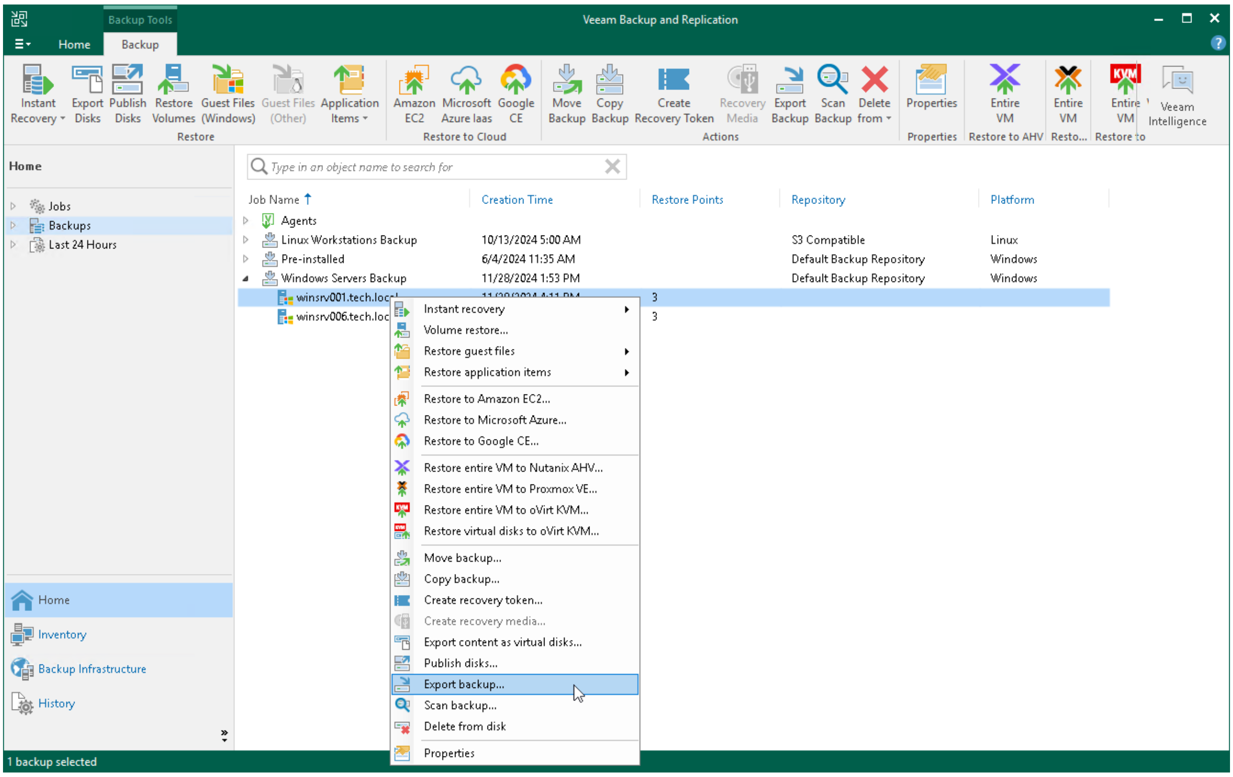
- Open the **History** view. In the inventory pane select **Restore**. In the working area, select the necessary publishing session and double-click it. In the **Restore Session** window, click **Cancel restore task**. Alternatively, you can right-click the publishing session and click **Stop session**.



Name	Type	Host	Status	Restore Point	Backup Name
srv006.tech.local	Disk Publish	This server	Mounted	10/30/2023 10:00:39 PM	Windows Servers Backup

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.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local	11/28/2024 4:11 PM	3		
winsrv006.tech.loc		3		

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 following tasks:

- Create a SureBackup job.
- Move a Veeam Agent backup.
- Copy a Veeam Agent backup.
- Perform a backup copy for Veeam Agent backup.
- Archive Veeam Agent Backups to Tape.
- Create a recovery token.
- Create Veeam Recovery Media for a computer.
- Detach a Veeam Agent backup from a backup job.
- Delete a Veeam Agent backup from disk.
- Remove a Veeam Agent backup from configuration.
- View properties of a Veeam Agent backup.
- Scan backup.

Using SureBackup

A SureBackup job is a task for recovery verification. You can run the SureBackup job manually or schedule it to run automatically.

SureBackup job can operate in two different backup verification modes:

- **Full recoverability testing**. Veeam Backup & Replication runs machines in an isolated environment directly from backup and performs tests against live applications.This mode ensures recoverability of your production workloads in a disaster recovery event. To learn more, see the Full Recoverability Testing section in the Veeam Backup & Replication User Guide.
- **Backup verification and content scan only**. Veeam Backup & Replication performs backup integrity check and its content analysis to detect traces of malware or any other unwanted or sensitive data. These tests do no require setting up a virtual lab or an application group. To learn more, see the Backup verification and content scan only section in the Veeam Backup & Replication User Guide.

Getting Started

Before you configure a SureBackup job that will test your backup, you must complete the following steps:

1. Consider limitations listed in section 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, see Working with Veeam Agent Backup Jobs and Policies.

   c. Run the backup job to create a backup.
3. [For full recoverability testing mode] 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.

   > TIP
   >
   > You can add a virtual lab during creating a SureBackup job at the Virtual Lab step of the **New SureBackup Job** wizard.

   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.

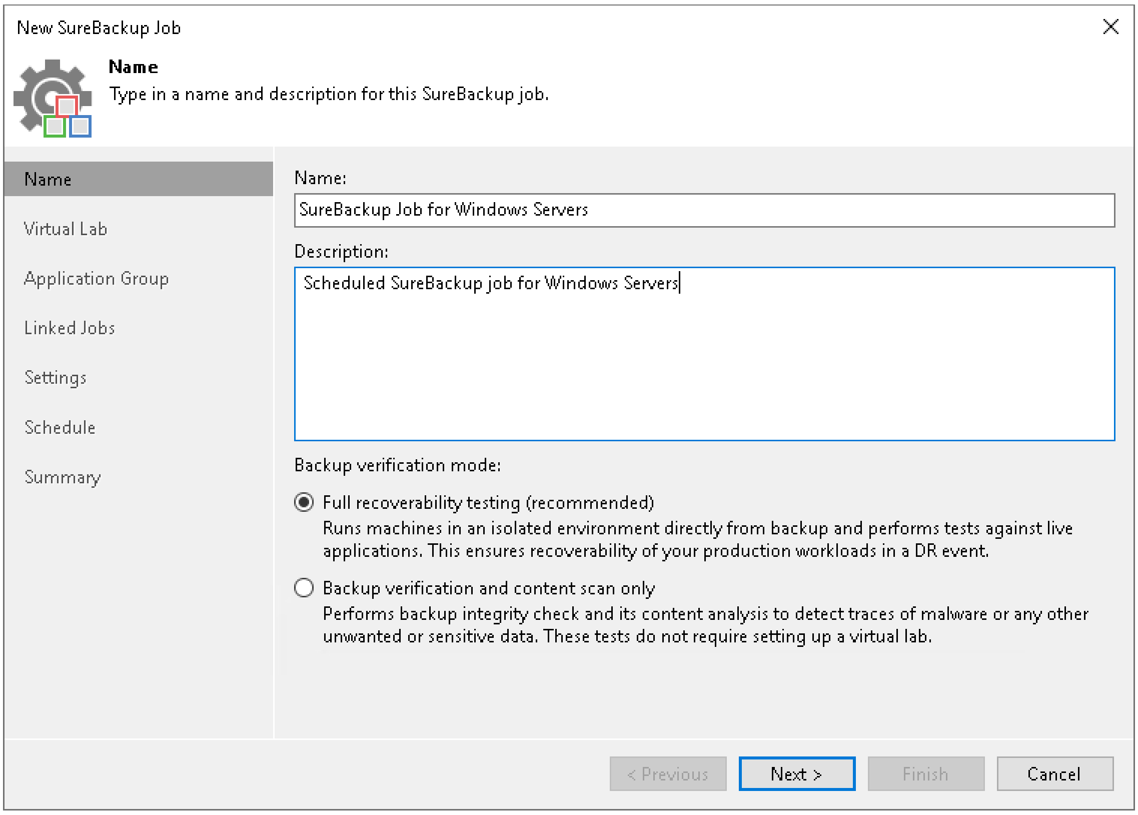
> TIP
>
> Consider the following:
>
> - You can add an application group during creating a SureBackup job at the Application Group step of the New SureBackup Job wizard.
> - The application group is optional for the SureBackup job. If you do not create an application group, you can still use a backup 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 Creating SureBackup Job.

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 Job** to launch the SureBackup Job wizard.
2. At the **Name** step of the wizard, specify a name, description and backup verification mode for the SureBackup job.



Name: SureBackup Job for Windows Servers

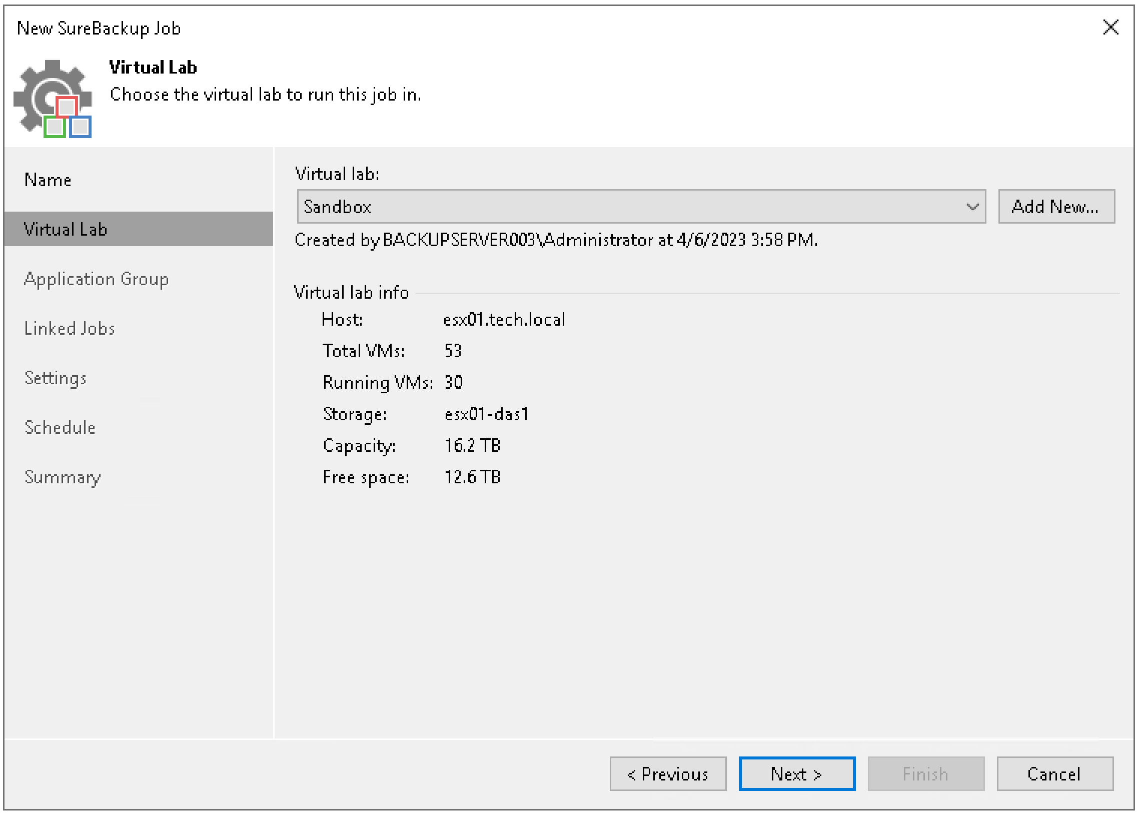
Description: Scheduled SureBackup job for Windows Servers

Backup verification mode:

● Full recoverability testing (recommended)
Runs machines in an isolated environment directly from backup and performs tests against live applications. This ensures recoverability of your production workloads in a DR event.

○ Backup verification and content scan only
Performs backup integrity check and its content analysis to detect traces of malware or any other unwanted or sensitive data. These tests do not require setting up a virtual lab.

3. [For full recoverability testing mode] At the **Virtual Lab** step of the wizard, select or add a virtual lab that Veeam Backup & Replication will use to recover your computer as a VM.



New SureBackup Job

Virtual Lab

Choose the virtual lab to run this job in.

Virtual lab: Sandbox

Created by BACKUPSERVER003\Administrator at 4/6/2023 3:58 PM.

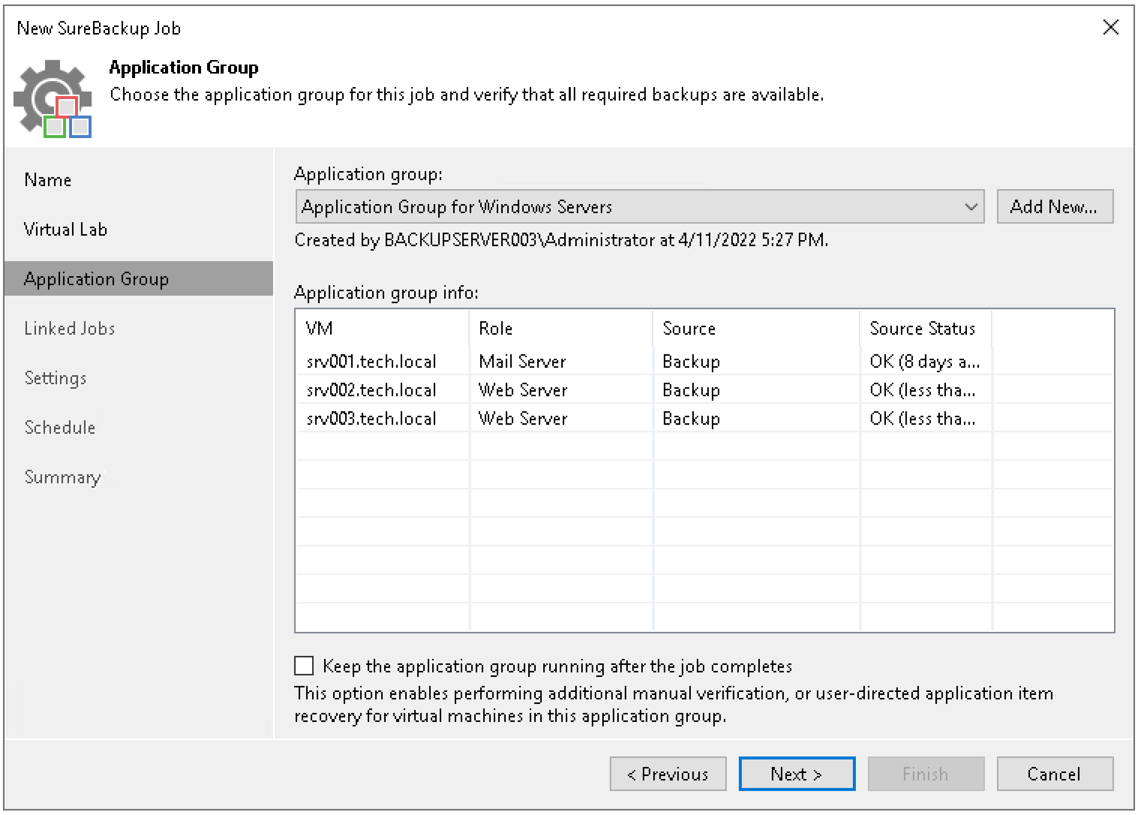
Virtual lab info

Host:	esx01.tech.local
Total VMs:	53
Running VMs:	30
Storage:	esx01-das1
Capacity:	16.2 TB
Free space:	12.6 TB

4. [For full recoverability testing mode] At the **Application Group** step of the wizard, select or add an application group with backups you want to test.

TIP

You can skip this step and add a backup job as a source of backups at the Linked Jobs step of the wizard.



Application group: Application Group for Windows Servers

Created by BACKUPSERVER003\Administrator at 4/11/2022 5:27 PM.

Application group info:

VM	Role	Source	Source Status
srv001.tech.local	Mail Server	Backup	OK (8 days a...
srv002.tech.local	Web Server	Backup	OK (less tha...
srv003.tech.local	Web Server	Backup	OK (less tha...

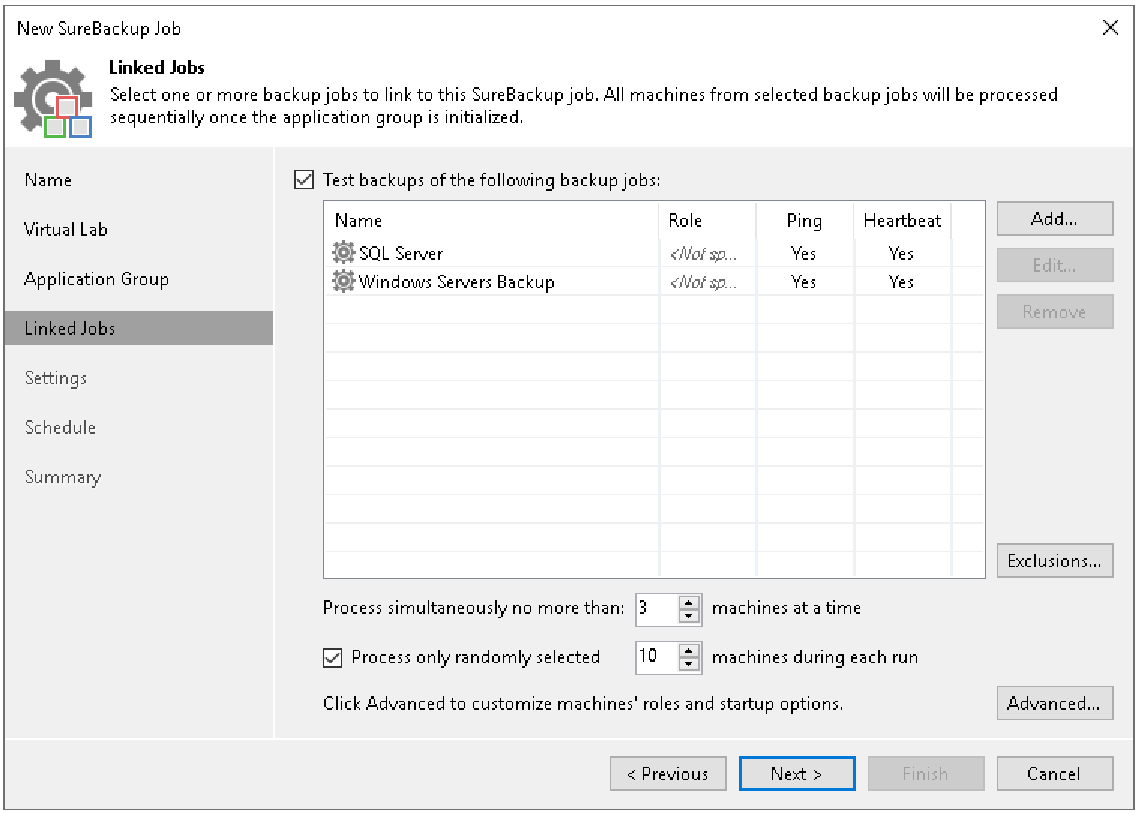
□ Keep the application group running after the job completes

This option enables performing additional manual verification, or user-directed application item recovery for virtual machines in this application group.

5. At the **Linked Jobs** step of the wizard, add a backup job to use as a source of backups for the SureBackup job and specify settings for backup job processing. To learn more, see the Link Backup or Replication Job and Specify Recovery Verification Options and Tests sections in the Veeam Backup & Replication User Guide.

TIP

[For full recoverability testing mode] You can skip this step if you selected an application group at the Application Group step of the wizard.



New SureBackup Job

Linked Jobs

Select one or more backup jobs to link to this SureBackup job. All machines from selected backup jobs will be processed sequentially once the application group is initialized.

☑ Test backups of the following backup jobs:

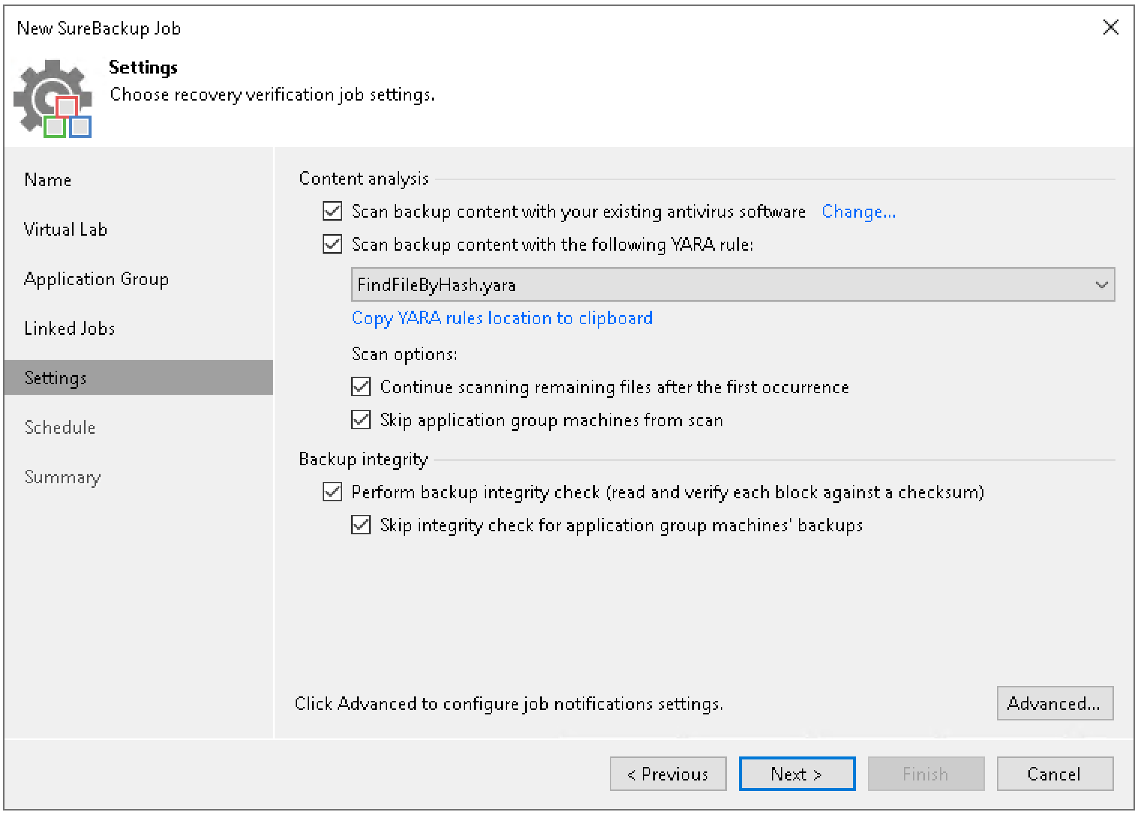
Name	Role	Ping	Heartbeat
SQL Server	<Not sp...	Yes	Yes
Windows Servers Backup	<Not sp...	Yes	Yes

Process simultaneously no more than: 3 machines at a time

☑ Process only randomly selected 10 machines during each run

Click Advanced to customize machines' roles and startup options.

6. At the **Settings** step of the wizard, specify additional settings for the SureBackup job. To learn more, see the Specify Additional Job Settings section in the Veeam Backup & Replication User Guide.



New SureBackup Job

Settings

Choose recovery verification job settings.

Content analysis

☑ Scan backup content with your existing antivirus software Change...

☑ Scan backup content with the following YARA rule:

FindFileByHash.yara

Copy YARA rules location to clipboard

Scan options:

☑ Continue scanning remaining files after the first occurrence

☑ Skip application group machines from scan

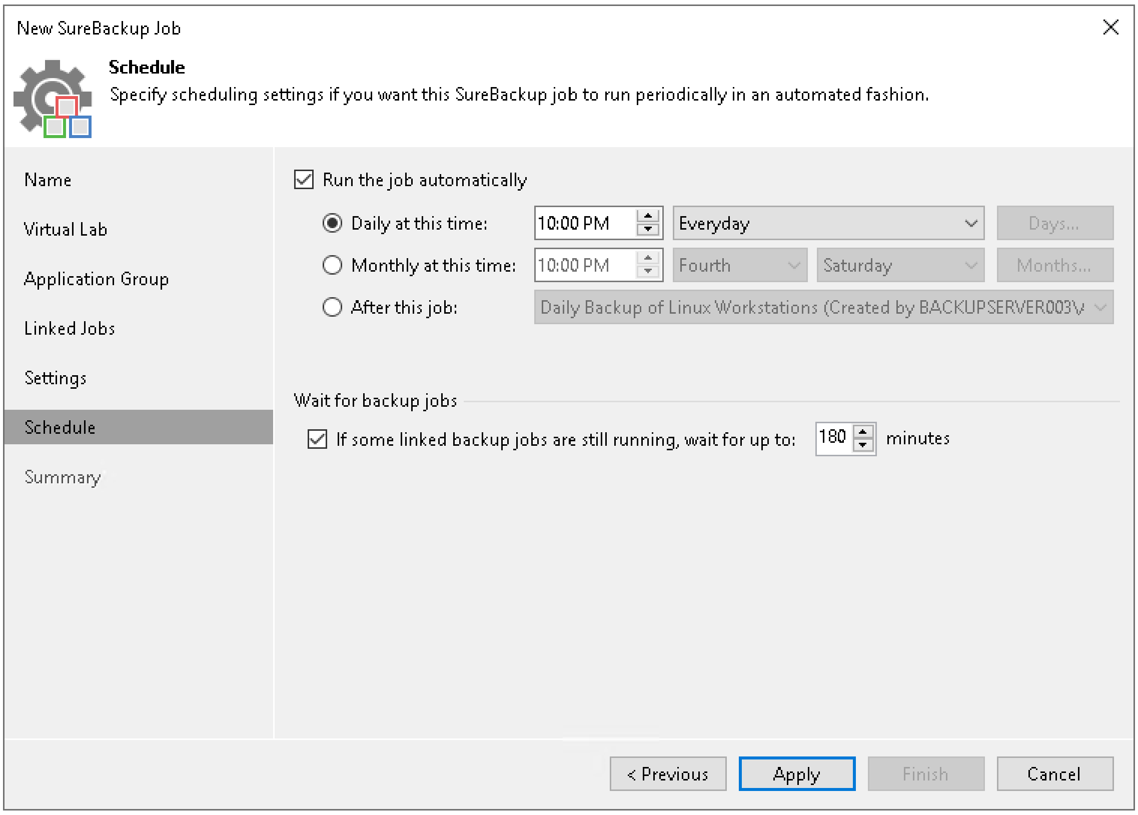
Backup integrity

☑ Perform backup integrity check (read and verify each block against a checksum)

☑ Skip integrity check for application group machines' backups

Click Advanced to configure job notifications settings.

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.



New SureBackup Job

Schedule

Specify scheduling settings if you want this SureBackup job to run periodically in an automated fashion.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

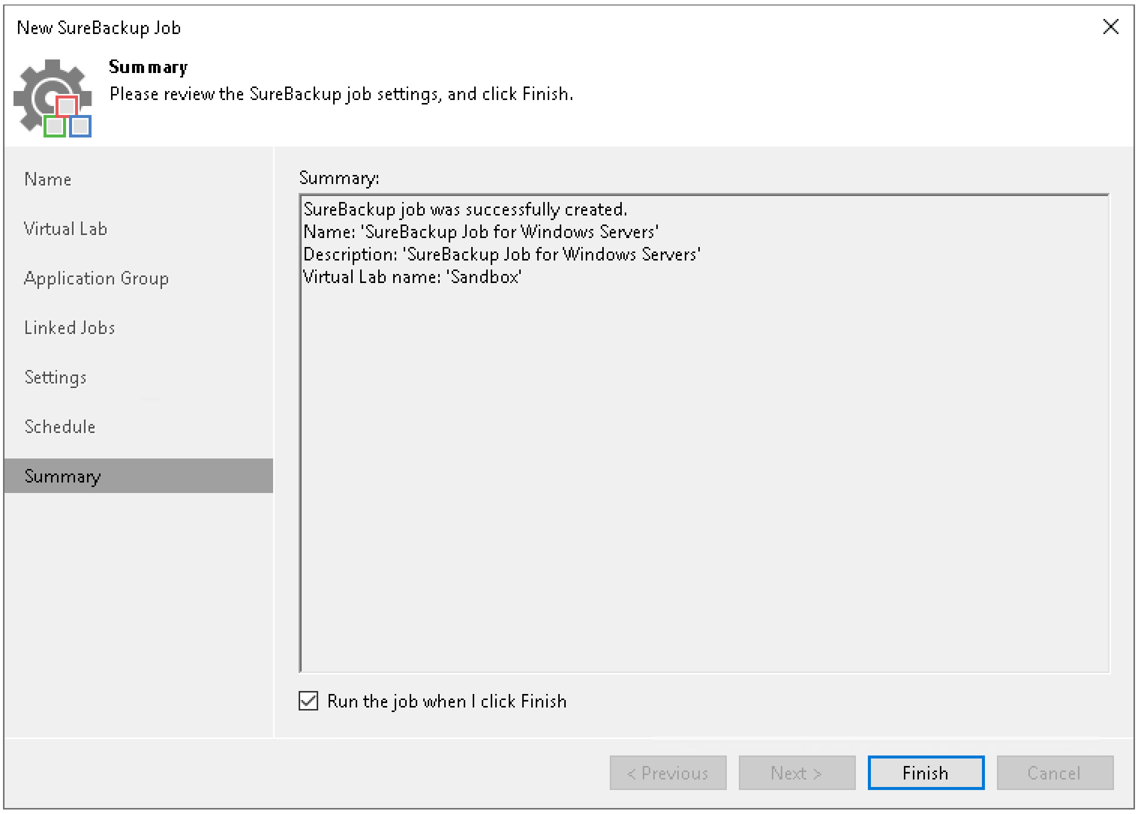
○ Monthly at this time: 10:00 PM Fourth Saturday

○ After this job: Daily Backup of Linux Workstations (Created by BACKUPSERVER003\

Wait for backup jobs

☑ If some linked backup jobs are still running, wait for up to: 180 minutes

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 finish working with the wizard.



New SureBackup Job

Summary

Please review the SureBackup job settings, and click Finish.

Summary:

```
SureBackup job was successfully created.
Name: 'SureBackup Job for Windows Servers'
Description: 'SureBackup Job for Windows Servers'
Virtual Lab name: 'Sandbox'
```

☑ Run the job when I click Finish

9. Click **Finish**

Moving Backup

You can move backups created with Veeam Agent in the following ways:

- Move Veeam Agent backup from one backup job to another.
- Move Veeam Agent backup from one repository to another.

> NOTE
>
> The move backup feature does not support moving backups between extents of a scale-out backup repository. To learn how to manage backups within the scale-out backup repository, see the Scale-Out Backup Repositories section in the Veeam Backup & Replication User Guide.

Before You Begin

Before you perform the move operation, consider the following limitations:

- You cannot move backups between Veeam Cloud Connect repositories.
- If you move backups from an immutable repository, the move operation does not delete the backups from the original repository. In this case, backups from the original repository are deleted according to the retention policy. For more information, see Backup Immutability.
- [For Veeam Agent backup policies] You cannot move backups to/from/between object storage repositories.
- [For Veeam Agent backup jobs] You cannot move a backup to another job if the target job already contains a backup of the same Veeam Agent computer or protection group.
- [For Veeam Agent backup jobs] You cannot move an encrypted backup to a job where encryption is not enabled and the other way around.

To learn about how moving to another repository and moving to another job work, see the How Moving to Another Repository Works and How Moving to Another Job Works sections in the Veeam Backup & Replication User Guide.

For the full list of limitations, see the Requirements and Limitations section in the Veeam Backup & Replication User Guide.

Moving Backup to Another Job

> NOTE
>
> You cannot move to another job backups created by a backup job managed by Veeam Agent (backup policy).

To move a backup to another Veeam Agent backup job:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area, expand the backup whose files you want to move, right-click the backup and select **Move backup** or click **Move backup** on the ribbon.

4. In the **Move Backup to Another Job** window, select the target backup job to which you want to move your backup.

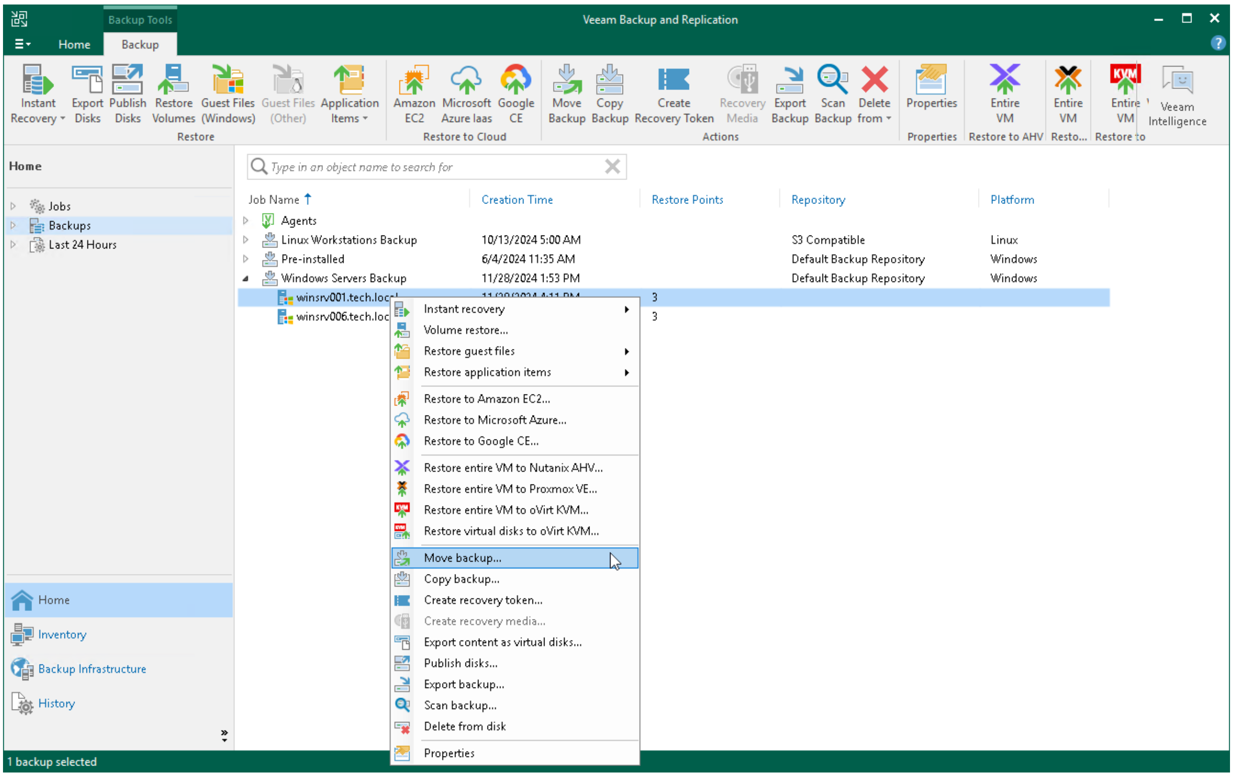
   Keep in mind that Veeam Backup & Replication displays only those backup jobs in the list that have the same backup mode and backed-up computer type as the original backup job. For example, if the original job is a backup job managed by Veeam backup server for Windows-based computers, Veeam Backup & Replication will display in the list only backup jobs managed by Veeam backup server for Windows-based computers.

5. Click **OK**.

As a result of the move operation:

- The backup is moved to the repository specified in the settings of the target backup job.
- In the Veeam Backup & Replication console, all restore points of the backup are displayed in the node of the target backup job.

> **NOTE**
>
> Consider the following:
>
> - When you move a backup to another backup job, Veeam Backup & Replication disables the original backup job only for the period of the move operation. If you do not want the original backup job to create new backups after the move, you must edit the backup job settings or disable the backup job. For more information, see Managing Veeam Agent Backup Jobs.
> - If you want to map the target backup job to the moved backup files, you must add the computers protected by the original backup job to the settings of the target backup job. In this case, the target backup job will continue the backup chain for the moved backups after the start. For more information, see Adding Protection Groups and Computers from Inventory.



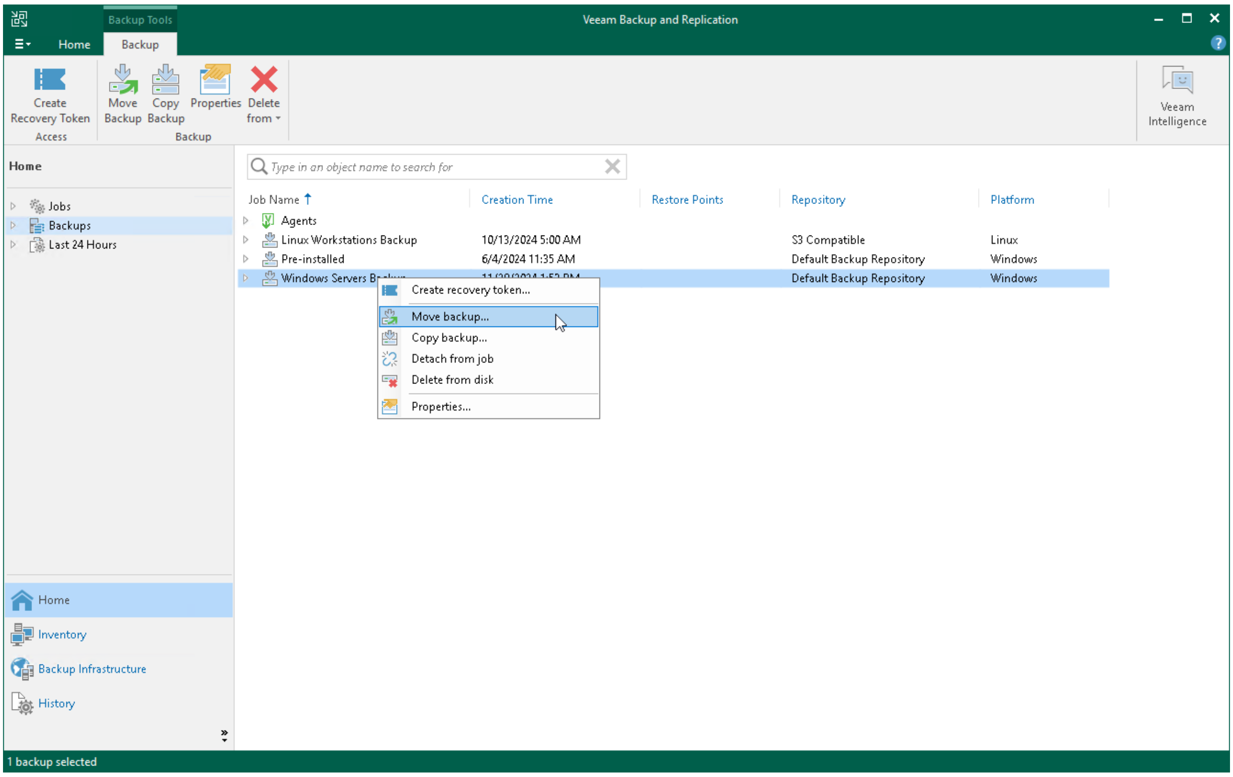
Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.loc	11/28/2024 4:11 PM	3		
winsrv006.tech.loc		3		

Moving Backup to Another Repository

To move a backup to another repository, do the following:

1. Open the **Home** view.
2. In the inventory pane, select the **Backups** node.
3. In the working area, select the necessary backup job or backup policy.
4. Right-click the job or the policy and select **Move backup. Alternatively,** click **Move Backup** on the ribbon.
5. In the **Move Backup to Another Location** window, select the repository to which you want to move backups.
6. Click **OK**.

> **TIP**
>
> You can also change the repository in backup job or backup policy settings. After you change the repository, Veeam Backup & Replication will suggest moving backups from the original repository to a new repository. You can select to move backups or leave them in the original repository.
>
> To learn how to edit backup job and backup policy settings, see Editing Veeam Agent Backup Job Settings and Editing Backup Policy Settings.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/20/2024 1:52 PM		Default Backup Repository	Windows

Managing Failed Activities

If the move operation fails, Veeam Backup & Replication assigns the *User action required* status to it. In this case, you need to decide how to finish the operation:

1. Open the **Home** view.

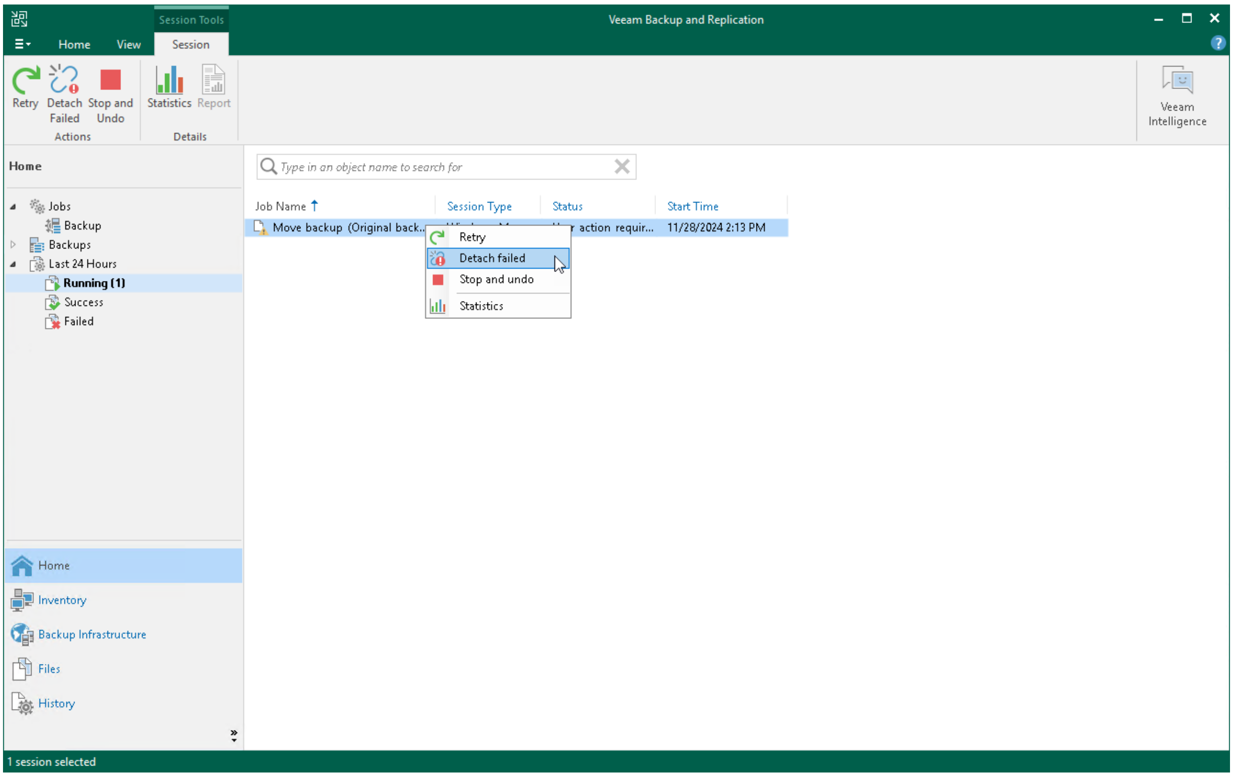
2. In the inventory pane, select the **Last 24 Hours** node.
3. Right-click the failed move session and select the required action or select the required action on the ribbon:
   - **Retry** — to retry the move operation for failed backups.

     During the retry operation, Veeam Backup & Replication does not relaunch the move operation for the whole backup. Veeam Backup & Replication tries to copy or delete those backup files that were not copied or deleted during the move.
   - **Detach failed** — to detach failed backups.

     The detached backups will be shown under the **Backups** > **Orphaned** node in the inventory pane.

     > NOTE
     >
     > The **Detached failed** operation is not available for Veeam Agent backup policies.
   - **Stop and undo** — to cancel all changes.

> NOTE
>
> The original backup job will be in the disabled state until you finalize the failed move operation.



Job Name	Session Type	Status	Start Time
Move backup (Original back...		...r action requir...	11/28/2024 2:13 PM

Copying Backup

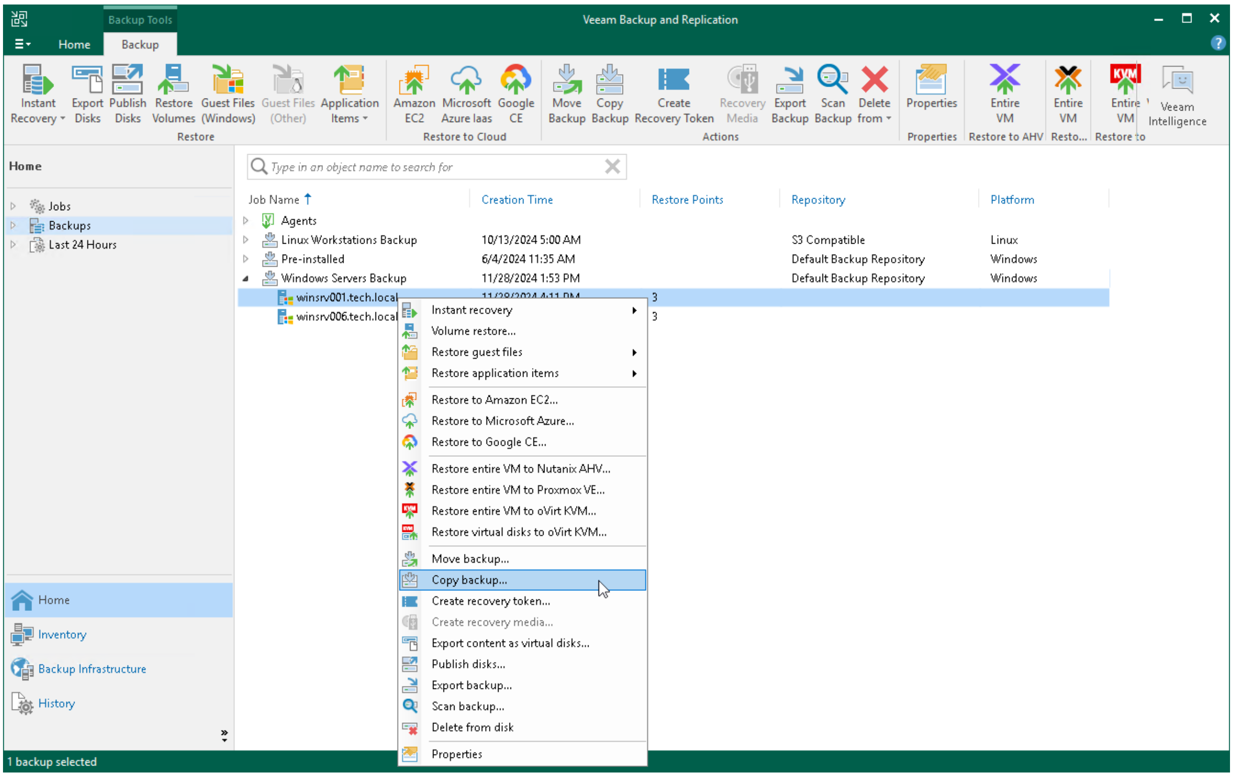
You can copy backups created by a backup job managed by Veeam backup server. This functionality allows you to create several copies of the same backup in different locations, whether onsite or offsite. Backup copies have the same format as files created by backup jobs and you can recover your data from them when you need it.

When Veeam Backup & Replication performs the copy operation, it disables the job, copies files to the target location and then enables the job. To learn more, see the Copying Backups section of the Veeam Backup & Replication User Guide.

> **NOTE**
>
> Consider the following:
>
> - You cannot copy backups created by a backup job managed by Veeam Agent (backup policy). To learn about types of Veeam Agent backup jobs, see Veeam Agent Backup Jobs and Policies.
> - The copy backup feature does not support copying backups between extents of a scale-out backup repository. To learn how to manage backups within the scale-out backup repository, see the Scale-Out Backup Repositories section in 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**.
4. In the **Copy Backup to Another Location** window, choose where you want to copy backups — to a repository or to a local or shared folder.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local	11/28/2024 4:11 PM	3		
winsrv006.tech.local		3		

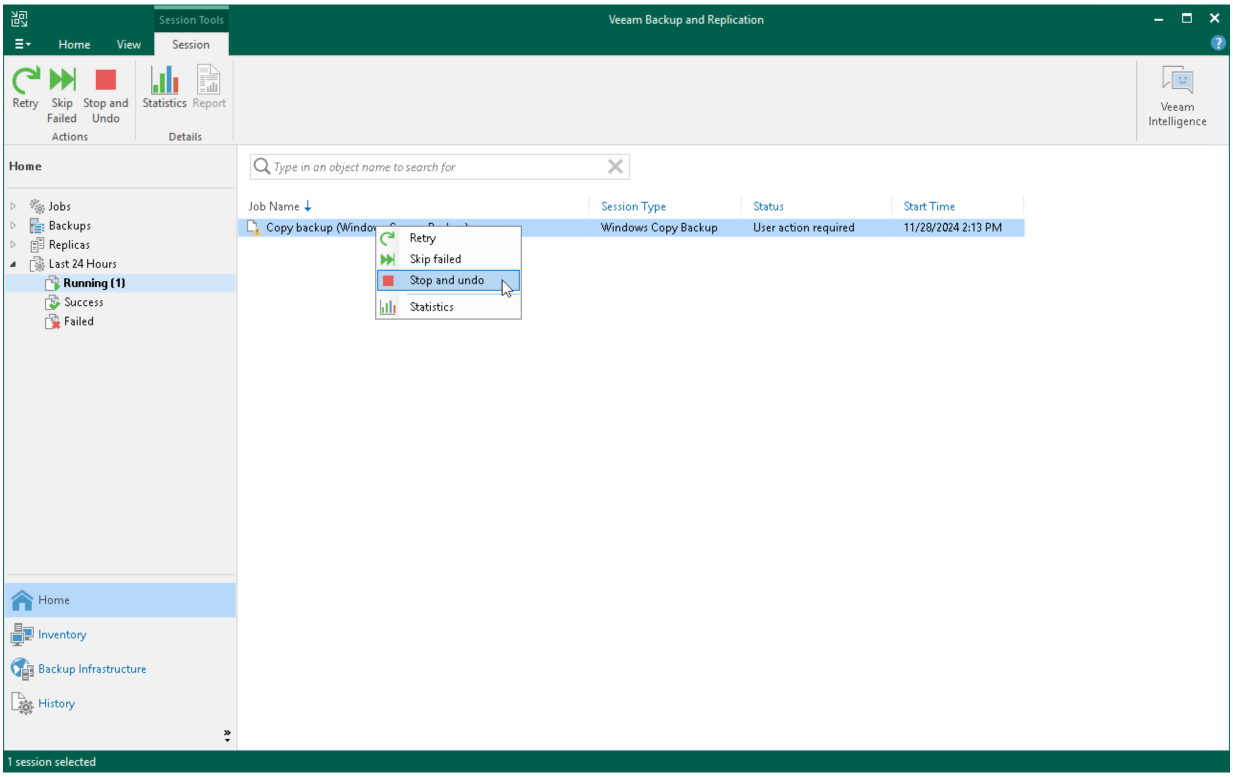
Managing Failed Activities

If the copy operation fails, Veeam Backup & Replication assigns the *User action required* status to it. In this case, you need to decide how to finish the operation:

1. Open the **Home** view.
2. In the inventory pane, select the **Last 24 Hours** node.
3. Right-click the failed copy session and select the required action or select the required action on the ribbon:
   - **Retry** — to retry the copy operation for failed backups.

     During the retry operation, Veeam Backup & Replication does not relaunch the copy operation for the whole backup. Veeam Backup & Replication tries to copy those backup files that were not copied during the move.
   - **Skip failed** — to skip failed backups.
   - **Stop and undo** — to cancel all changes.

> **NOTE**
>
> The original backup job will be in the disabled state until you finalize the failed copy operation.



Job Name	Session Type	Status	Start Time
Copy backup (Windo...	Windows Copy Backup	User action required	11/28/2024 2:13 PM

Performing Backup Copy for Veeam Agent Backups

You can configure backup copy jobs that will copy backups created with Veeam Agent to a secondary backup repository.

Backup copy jobs treat Veeam Agent backups as usual backup files. The backup copy job setup and processing procedures practically do not differ from the same procedures for a backup copy job that processes VM backups. To learn more about backup copy jobs, see the Backup Copy section in the Veeam Backup & Replication User Guide.

Prerequisites and Limitations

Before creating a backup copy for Veeam Agents backups, consider the following:

- When you copy Veeam Agent backup jobs that process failover clusters, the backup copy 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.

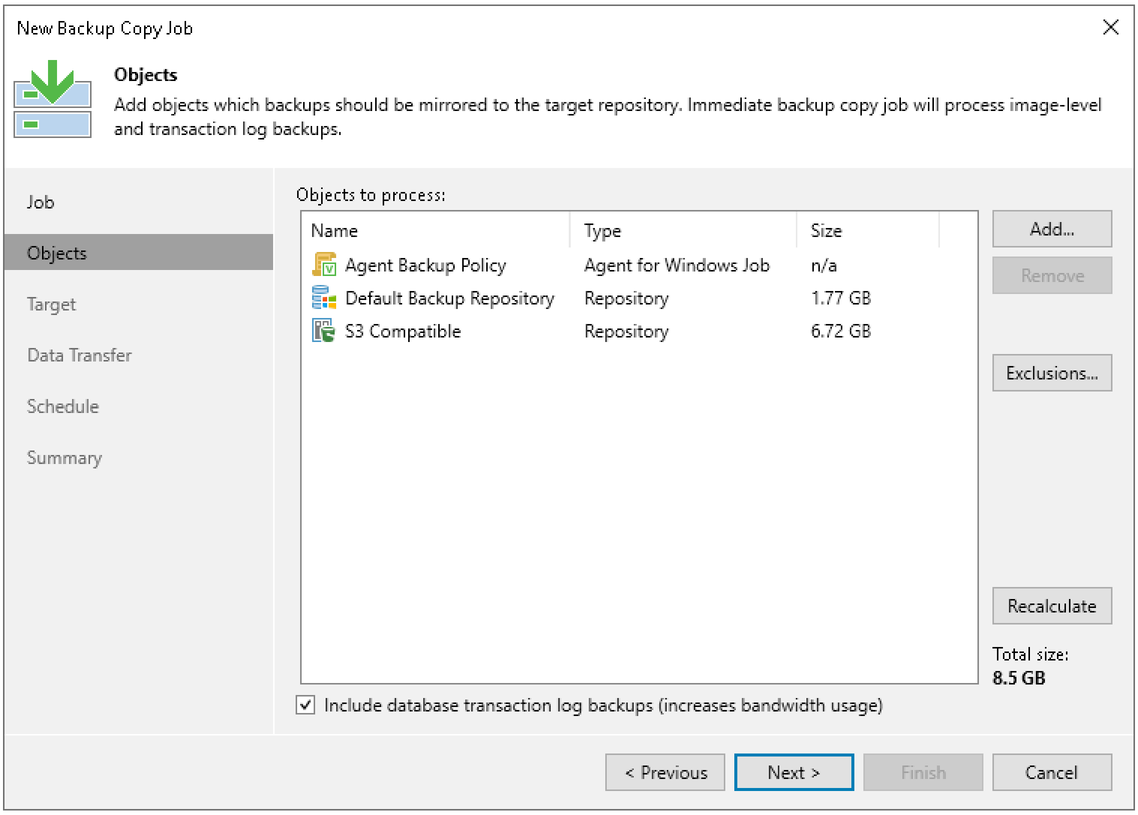
  To learn more, see the Backup Chain Formats section in the Veeam Backup & Replication User Guide.

- When you copy Veeam Agent backup jobs that process failover clusters with shared disks, the network traffic is higher compared to the traffic sent when Veeam Agent backup jobs run. This happens because Veeam Agent backup copy jobs send data as it is stored in the storage — each node with the cloned data — unlike Veeam Agent backup jobs that send data of shared disks only with the owner node and then, within the target storage, clone this data to other nodes.

- Data deduplication is not available when you copy Veeam Agent backup jobs that process failover clusters with shared disks to an object storage repository.

  > IMPORTANT
  >
  > In this case, you may require additional free space on the target location, because Veeam Backup & Replication creates in the target location as many copies of the cluster shared disks as there are nodes in the cluster.

- [For the legacy periodic copy mode] You can map a Veeam Agent backup copy job only to a backup created by backup copy job that processes backups created by Veeam Agent operating in the standalone mode.



New Backup Copy Job

Objects

Add objects which backups should be mirrored to the target repository. Immediate backup copy job will process image-level and transaction log backups.

Objects to process:

Name	Type	Size
Agent Backup Policy	Agent for Windows Job	n/a
Default Backup Repository	Repository	1.77 GB
S3 Compatible	Repository	6.72 GB

Total size:
8.5 GB

☑ Include database transaction log backups (increases bandwidth usage)

Restoring Data from Copies of Veeam Agent Backups

Backups copied to the secondary backup repository do not preserve user access permissions. At the same time, users who created backups do not have access permissions on these secondary repositories. For this reason, users cannot restore data from their backups residing in the secondary site.

To overcome this limitation, you can delegate the restore task to backup administrators who work with Veeam Backup & Replication. Backup administrators can use Veeam Backup & Replication options to recover data from such backups: for example, perform file-level restore or retrieve necessary application items with Veeam Explorers.

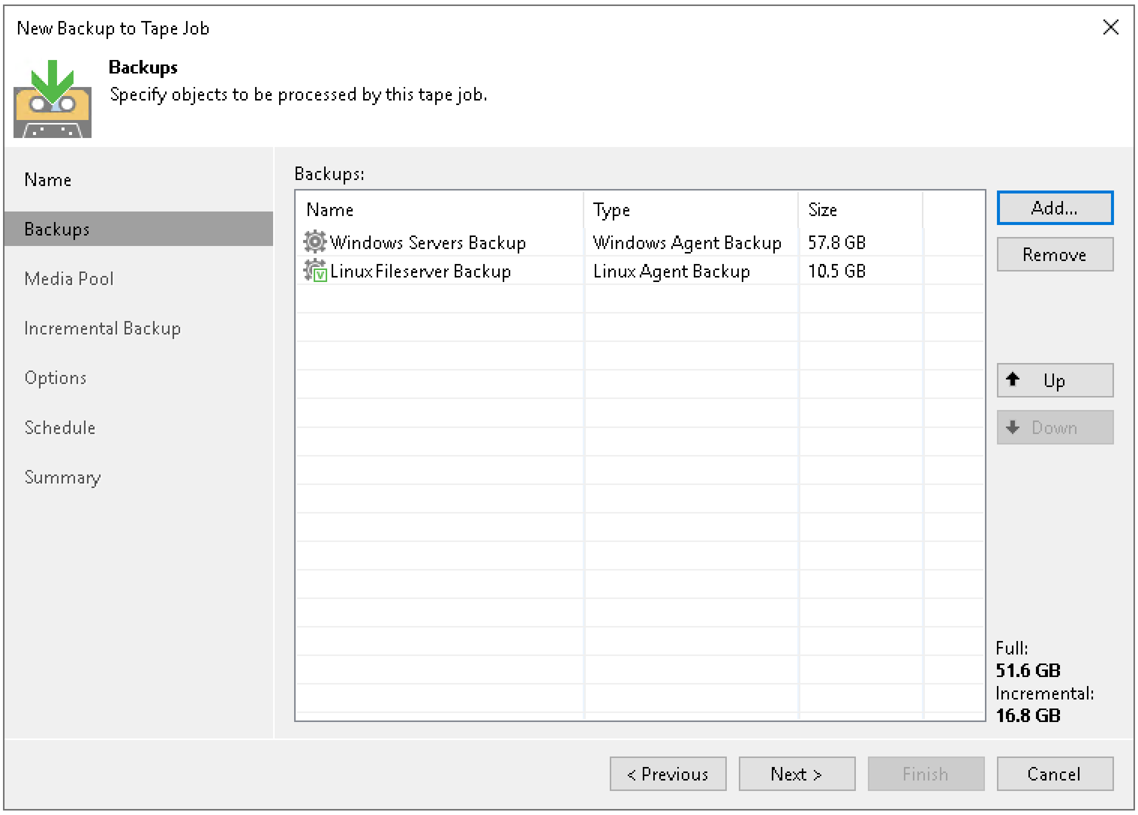
You can also restore data from the copied backup stored in the target repository using Veeam Agent.

Archiving Veeam Agent Backups to Tape

You can configure backup to tape jobs to archive Veeam Agent backups to tape.

Backup to tape jobs treat Veeam Agent backups as usual backup files. The archiving job setup and processing procedures practically do not differ from the regular ones. To learn more about backup to tape jobs, see the Backup to Tape section in the Veeam Backup & Replication User Guide.

> **NOTE**
>
> For the **After this job** option in the backup to tape job schedule settings, you cannot select a backup job managed by Veeam Agent or a standalone Veeam Agent backup job as the preceding backup job.



New Backup to Tape Job

Backups

Specify objects to be processed by this tape job.

Backups:

Name	Type	Size
Windows Servers Backup	Windows Agent Backup	57.8 GB
Linux Fileserver Backup	Linux Agent Backup	10.5 GB

Full: **51.6 GB**

Incremental: **16.8 GB**

Creating Recovery Token

If you want to recover files, volumes or an entire computer from a specific backup, 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 is stored in the backup. 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
- Veeam Agent for Oracle Solaris
- Veeam Agent for IBM AIX
- Veeam Agent for Mac

Considerations and Limitations

Before creating a recovery token, consider the following prerequisites and limitations:

- Recovery tokens stay valid for 24 hours.
- You can recover data only from the backup for that the recovery token is generated.
- 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**.

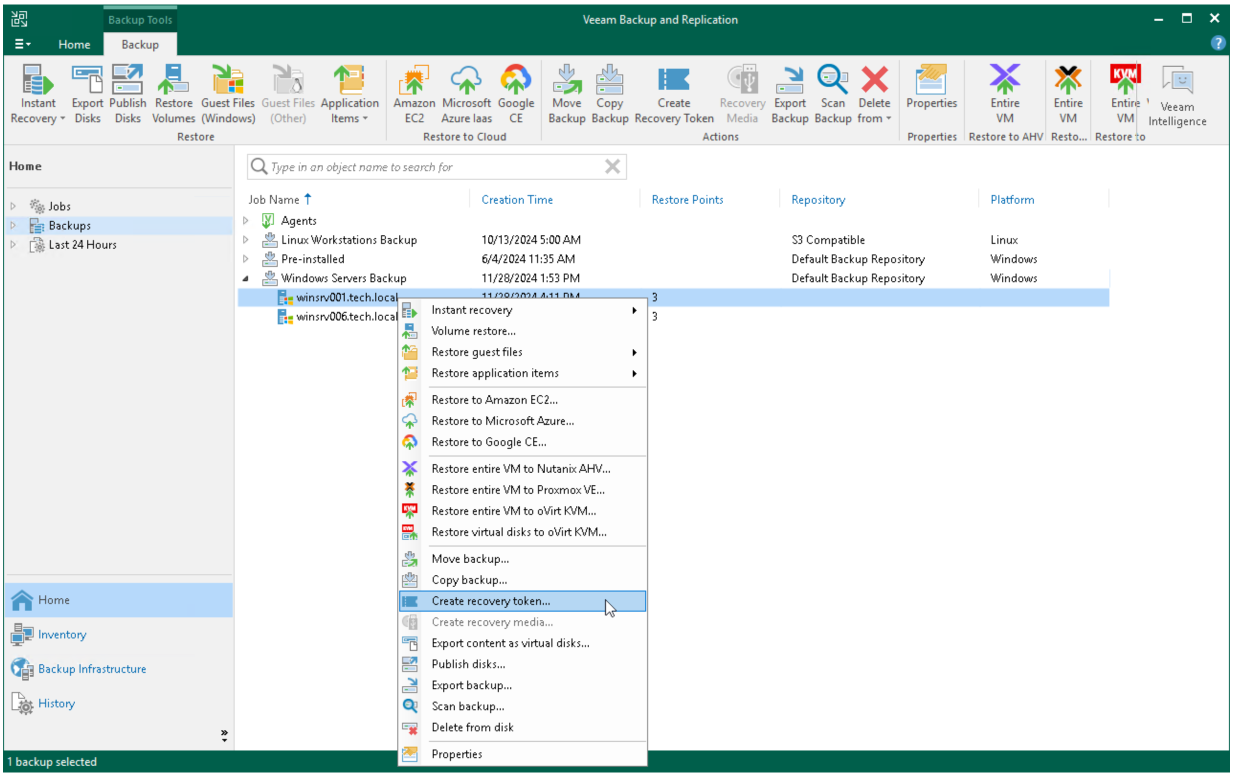
   You can create a recovery token for several backups. To do this, press and hold the [Ctrl] key, select multiple backups, right-click one of the selected backups and select **Create recovery token**.
4. In the **Create Recovery Token** window, click **Create**.

You can also create and modify the existing recovery token using the PowerShell console. To learn more, see the Working with Tokens section in the Veeam PowerShell Reference.

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
- Veeam Agent for Oracle Solaris
- Veeam Agent for IBM AIX
- Veeam Agent for Mac



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local	11/28/2024 4:11 PM	3		
winsrv006.tech.local		3		

1 backup selected

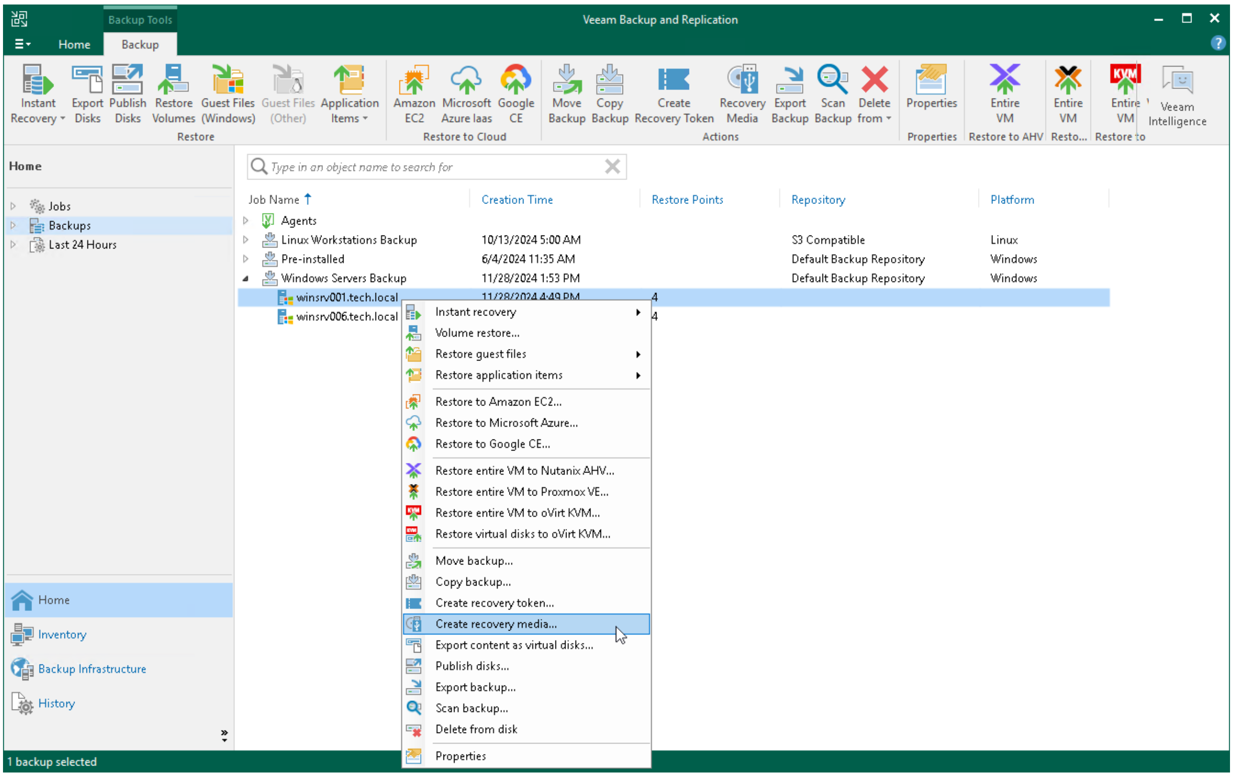
Creating Veeam Recovery Media from Backup

You can create the Veeam Recovery Media for a Microsoft Windows computer whose Veeam Agent backup resides on a Veeam backup repository or Veeam Cloud Connect 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.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.local	11/28/2024 4:49 PM	4		
winsrv006.tech.local		4		

Detaching Backup from Job

If you want a backup job to stop processing backup files, you can use the **Detach from job** operation.

When you detach backups from a job, the backup job will create an active full backup during the next run. This active full backup will reset the backup chain. All incremental backup files will use this active full backup file as a new starting point. A previously used full backup file and its subsequent incremental backup files will remain in the backup repository and also in the Veeam Backup & Replication console. Veeam Backup & Replication shows the detached backups in the **Backups > Disk (Orphaned)** node of the **Home** view. Veeam Backup & Replication manages such backups depending on the short-term retention that was set for the backup job:

- If the detached backups belonged to the job with retention period set in days, the background retention process retains the backups according to the configured retention and deletes the backups from the repository after the retention period ends. To learn more, see the Background Retention section in the Veeam Backup & Replication User Guide.

- If the detached backups belonged to the job with retention period set in restore points, the background retention process does not delete the backups. If you do not need the backups, you must delete them manually. To learn more about how to delete backups manually, see Deleting Backup from Disk.

Before detaching backups, consider the following:

- Before detaching backups from a backup job, you must disable this backup job and all depending secondary backup jobs.

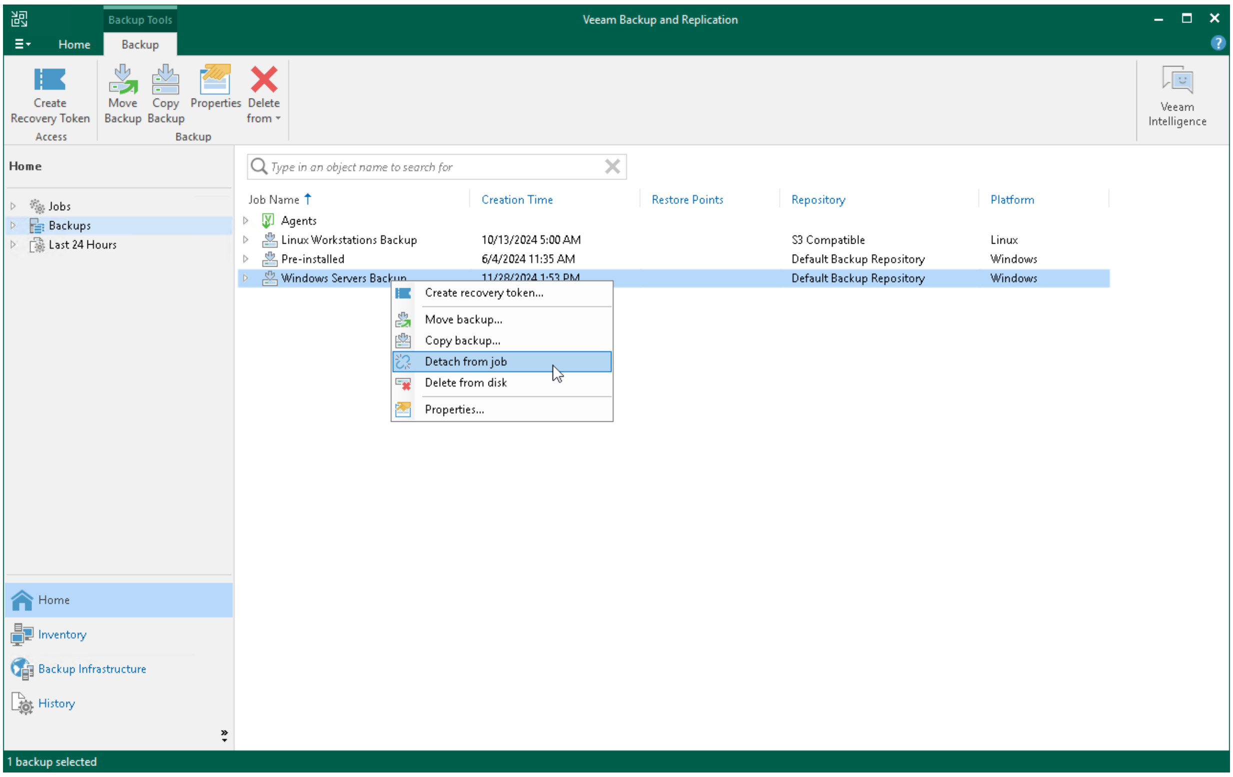
- You cannot detach backups of individual objects included in a backup job. You can only detach all backups of a backup job.

To detach backups from a job:

1. Open the **Home** view.

2. In the inventory pane, select the **Backups** node.

3. In the working area, click **Delete from** > **Job** on the ribbon or right-click the necessary backup and select **Detach from job**.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows

Deleting Backup from Disk

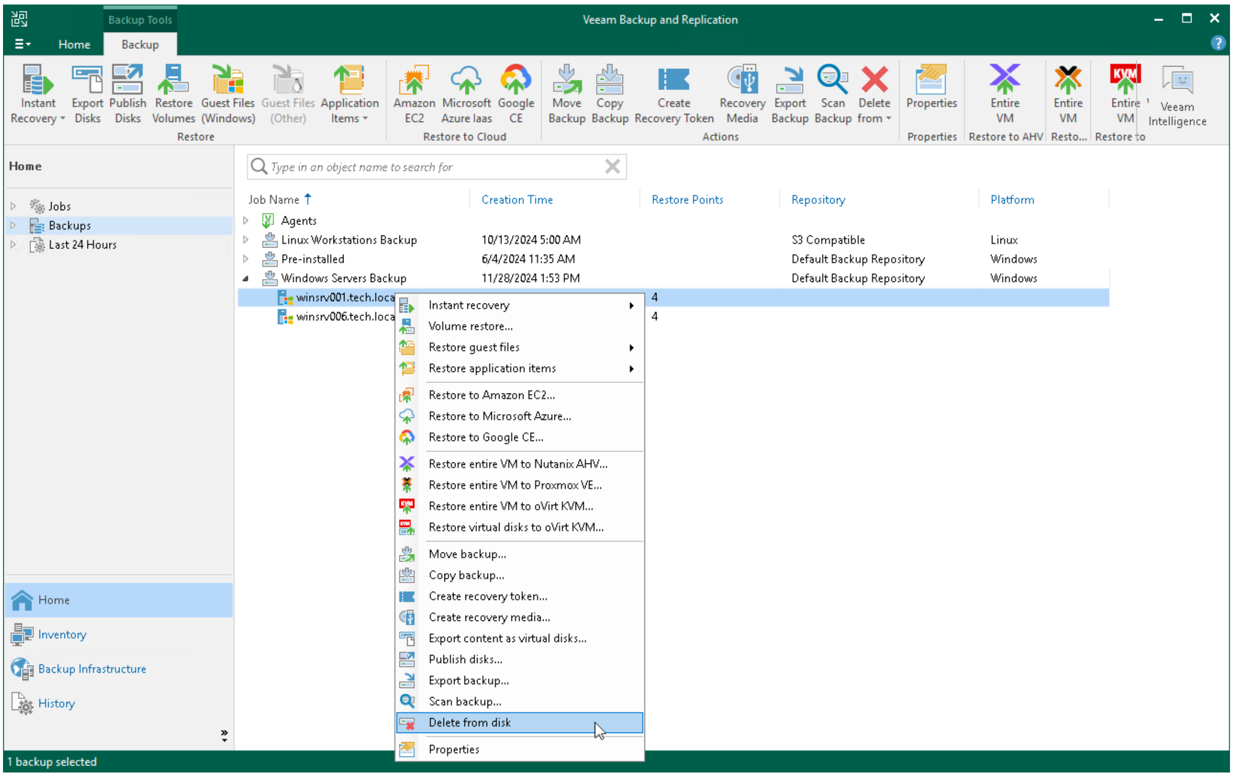
If you want to delete records about backups from the Veeam Backup & Replication console and configuration database and, additionally, delete backup files from the backup repository, you can use the **Delete from disk** operation.

> NOTE
>
> - You can use the Veeam Backup & Replication console to remove backups created by Veeam Agent backup jobs on the Veeam backup repository or Veeam Cloud Connect 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**.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech.loca		4		
winsrv006.tech.loca		4		

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.

> IMPORTANT
>
> Removing backups from configuration is designed for experienced users only. Consider using the Detach from job or Delete from disk operations instead.
>
> Create encrypted configuration backup before removing backups from configuration. To learn more, see the Creating Encrypted Configuration Backups section in the Veeam Backup & Replication User Guide.

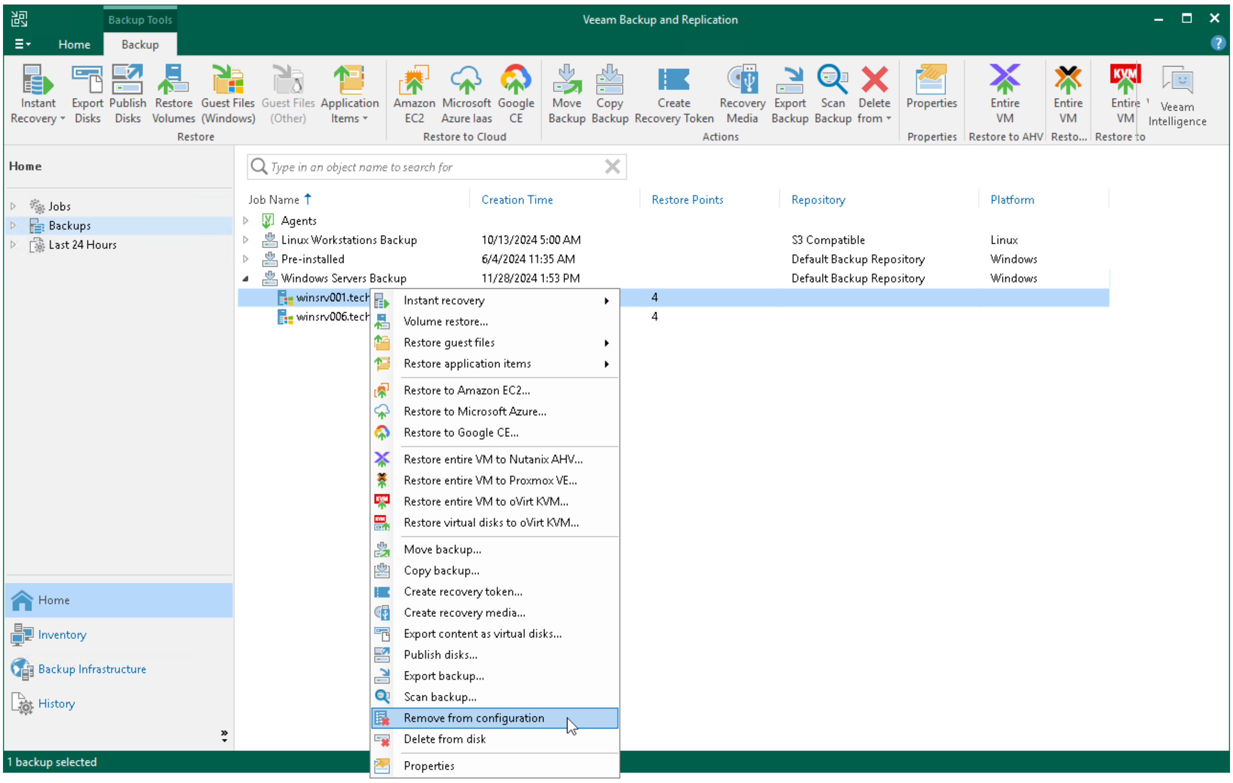
You can remove an entire backup related to a Veeam Agent backup job or remove specific child backups — backups related to individual computers in the backup.

> NOTE
>
> Consider the following:
>
> - You can remove backups created by Veeam Agent backup jobs stored in the Veeam backup repository or Veeam Cloud Connect 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.

To remove a Veeam Agent backup from configuration:

1. Open the **Home** view.
2. In the inventory pane, click **Backups**.
3. In the working area select and remove the necessary backup:
    - To remove the entire backup related to the Veeam Agent backup job or policy, select the backup, press and hold the [Ctrl] key, right-click the backup and select **Remove from configuration**.

- To remove a backup of a specific computer in the Veeam Agent backup job or policy, expand the parent backup, select the necessary computer, press and hold the [Ctrl] key, right-click the computer and select **Remove from configuration**.



Job Name	Creation Time	Restore Points	Repository	Platform
Agents				
Linux Workstations Backup	10/13/2024 5:00 AM		S3 Compatible	Linux
Pre-installed	6/4/2024 11:35 AM		Default Backup Repository	Windows
Windows Servers Backup	11/28/2024 1:53 PM		Default Backup Repository	Windows
winsrv001.tech		4		
winsrv006.tech		4		

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.
- Malware status of restore points.
- Date of restore points creation.
- Compression and deduplication ratios.
- Data size and backup size.
- GFS retention policy applied to restore points (W — weekly; M — monthly; Y — yearly).

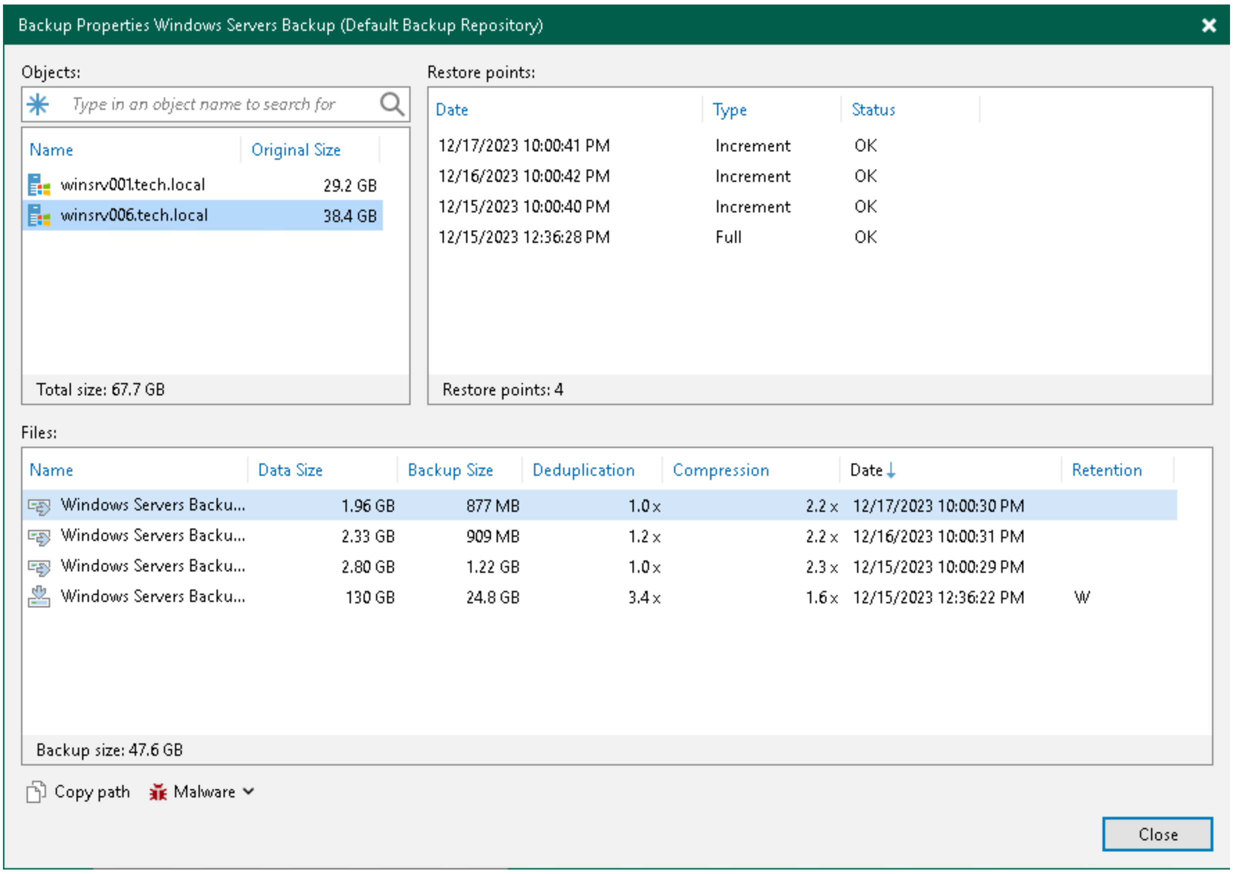
You can view summary information for the following types of Veeam Agent backups:

- 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:

4. Open the **Home** view.
5. In the inventory pane, select **Backups**.

6. In the working area, select the backup and click **Properties** on the ribbon or right-click the backup and select **Properties**.



Backup Properties Windows Servers Backup (Default Backup Repository)

Objects:

Name	Original Size
winsrv001.tech.local	29.2 GB
winsrv006.tech.local	38.4 GB

Total size: 67.7 GB

Restore points:

Date	Type	Status
12/17/2023 10:00:41 PM	Increment	OK
12/16/2023 10:00:42 PM	Increment	OK
12/15/2023 10:00:40 PM	Increment	OK
12/15/2023 12:36:28 PM	Full	OK

Restore points: 4

Files:

Name	Data Size	Backup Size	Deduplication	Compression	Date	Retention
Windows Servers Backu...	1.96 GB	877 MB	1.0 x	2.2 x	12/17/2023 10:00:30 PM	
Windows Servers Backu...	2.33 GB	909 MB	1.2 x	2.2 x	12/16/2023 10:00:31 PM	
Windows Servers Backu...	2.80 GB	1.22 GB	1.0 x	2.3 x	12/15/2023 10:00:29 PM	
Windows Servers Backu...	130 GB	24.8 GB	3.4 x	1.6 x	12/15/2023 12:36:22 PM	W

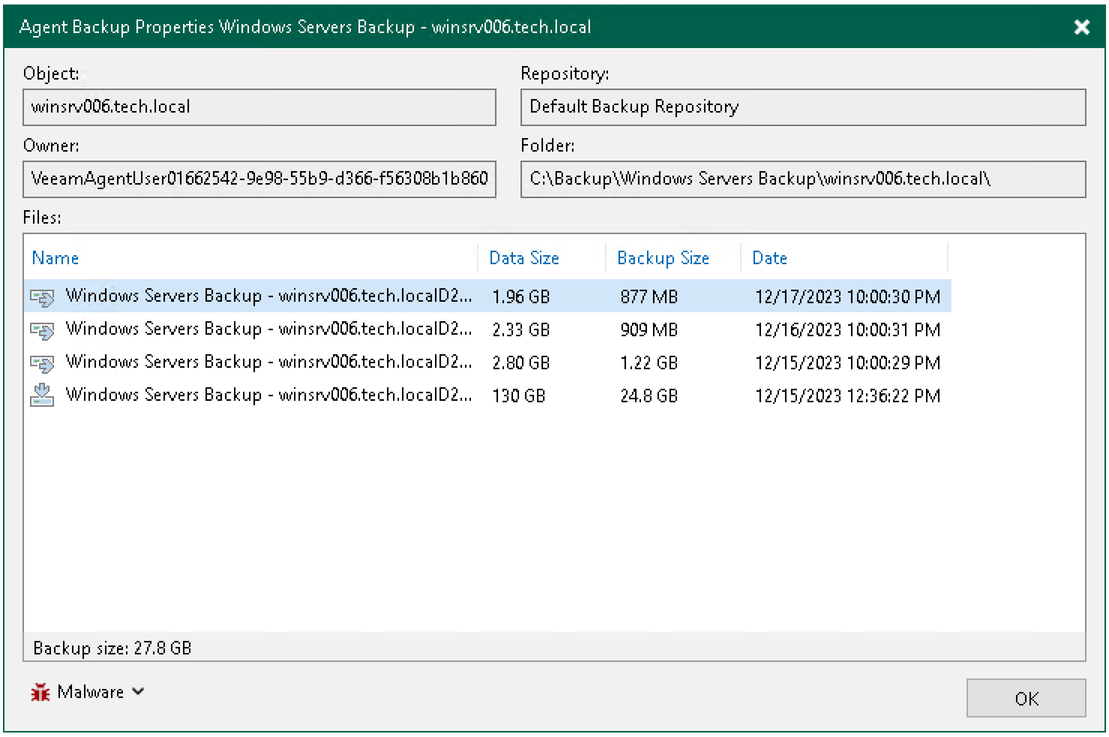
Backup size: 47.6 GB

To view summary information for a child backup (backup of a specific Veeam Agent computer):

4. Open the **Home** view.

5. In the inventory pane, select **Backups**.

6. In the working area, expand the parent backup, select the necessary child backup and click **Properties** on the ribbon or right-click the child backup and select **Properties**.



Agent Backup Properties Windows Servers Backup - winsrv006.tech.local

Object: winsrv006.tech.local

Repository: Default Backup Repository

Owner: VeeamAgentUser01662542-9e98-55b9-d366-f56308b1b860

Folder: C:\Backup\Windows Servers Backup\winsrv006.tech.local\

Files:

Name	Data Size	Backup Size	Date
Windows Servers Backup - winsrv006.tech.localD2...	1.96 GB	877 MB	12/17/2023 10:00:30 PM
Windows Servers Backup - winsrv006.tech.localD2...	2.33 GB	909 MB	12/16/2023 10:00:31 PM
Windows Servers Backup - winsrv006.tech.localD2...	2.80 GB	1.22 GB	12/15/2023 10:00:29 PM
Windows Servers Backup - winsrv006.tech.localD2...	130 GB	24.8 GB	12/15/2023 12:36:22 PM

Backup size: 27.8 GB

Scanning Backup

You can scan restore points of a backup created by Veeam Agent for Microsoft Windows after a malware attack or to look for some sensitive data in a backup.

You cannot scan backups created by Veeam Agent for Linux, Veeam Agent for IBM AIX, Veeam Agent for Oracle Solaris or Veeam Agent for Mac.

To run the scan backup session:

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 **Scan Backup** on the ribbon or right-click the computer and select **Scan Backup**.
4. Specify the scan mode you want to use:
   - **Find the last clean restore point**
   - **Find the last clean restore point in range**
   - **Scan content of all restore points in range**
5. If you want to scan the restored volume with a scan engine or antivirus software, select the method you want to use for data scan:
   - Select the **Scan restore points with Veeam Threat Hunter** option to use Veeam Threat Hunter.

     This option is available if you configured Veeam Threat Hunter as the detection engine in the malware detection settings. To learn more, see the Signature Detection section in the Veeam Backup & Replication User Guide.
   - Select the **Scan restore points with your existing antivirus software** option to use third-party antivirus software.

     This option is available if you configured a third-party antivirus as the detection engine in the malware detection settings. To learn more, see the Signature Detection section in the Veeam Backup & Replication User Guide.

     > **TIP**
     >
     > Click **Change** to open the **Malware Detection Settings** window where you can change the detection engine to Veeam Threat Hunter.
6. If you want to use a YARA rule as a scan engine, select the **Scan restore points with the following YARA rule** check box and specify the YARA file located in the Veeam Backup & Replication product folder: `C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules`.

   If you do not want to create a malware detection event for a YARA rule, you can add a `SuppressMalwareDetectionNotification` tag to the name of the rule. For example:

   ```
   rule SearchFileHash : SuppressMalwareDetectionNotification
   ```

   In this case, the malware detection event will not be created but the scan backup session will be finished with the *Warning* status.

7. Click **Scan Range** to configure the scan range. You can specify the following options:

   - Scan all restore points, from most recent restore point to the oldest available restore point.
   - Scan restore points created during a specific time period.

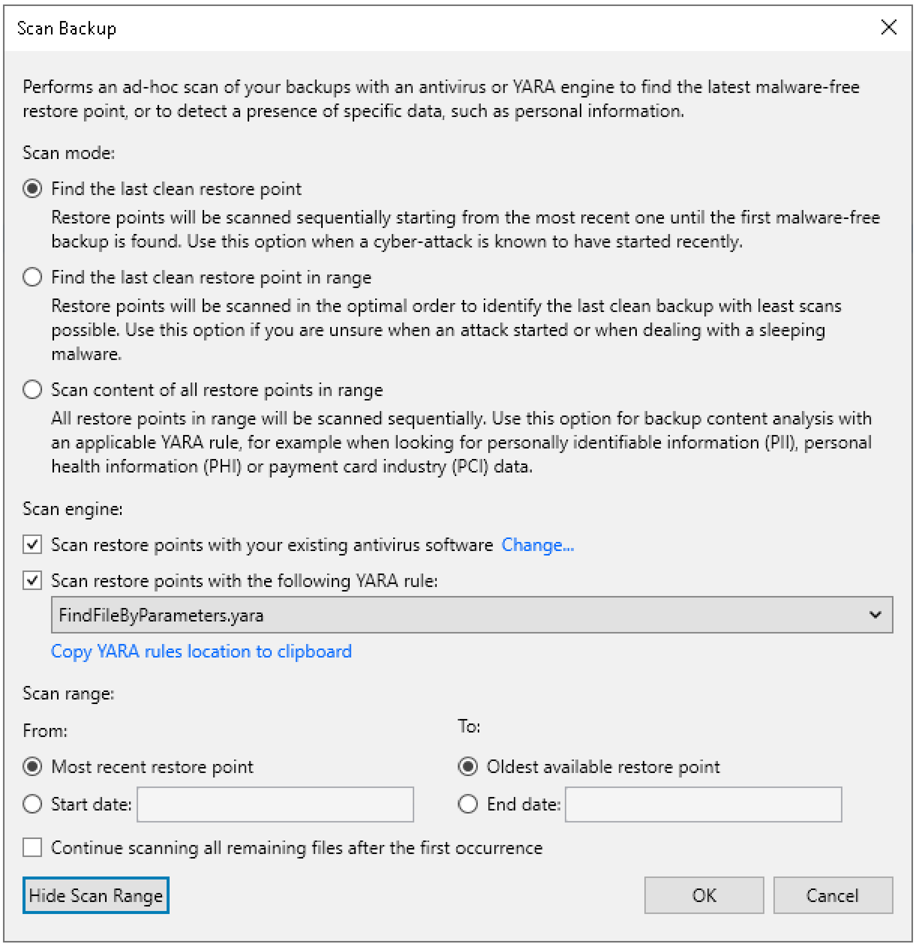
   Veeam Backup & Replication selects the order in which to scan restore points depending on the selected scan mode:

   - In the **Find the last clean restore point** mode, Veeam Backup & Replication scans restore points from the most recent to the oldest.
   - In the **Find the last clean restore point in range** mode, Veeam Backup & Replication scans restore points in the optimal order.
   - In the **Scan content of all restore points in range** mode, Veeam Backup & Replication scans restore points from the oldest to the most recent.

   If you want to continue the scan backup session after the first malware or the first piece of specific information is found, select the **Continue scanning all remaining files after the first occurence** check box.

8. Click **OK**.

To learn more, see the Scan Backup section in the Veeam Backup & Replication User Guide.



Scan Backup

Performs an ad-hoc scan of your backups with an antivirus or YARA engine to find the latest malware-free restore point, or to detect a presence of specific data, such as personal information.

Scan mode:

● Find the last clean restore point
Restore points will be scanned sequentially starting from the most recent one until the first malware-free backup is found. Use this option when a cyber-attack is known to have started recently.

○ Find the last clean restore point in range
Restore points will be scanned in the optimal order to identify the last clean backup with least scans possible. Use this option if you are unsure when an attack started or when dealing with a sleeping malware.

○ Scan content of all restore points in range
All restore points in range will be scanned sequentially. Use this option for backup content analysis with an applicable YARA rule, for example when looking for personally identifiable information (PII), personal health information (PHI) or payment card industry (PCI) data.

Scan engine:

☑ Scan restore points with your existing antivirus software Change...

☑ Scan restore points with the following YARA rule:

FindFileByParameters.yara

Copy YARA rules location to clipboard

Scan range:

From:
● Most recent restore point
○ Start date:

To:
● Oldest available restore point
○ End date:

□ Continue scanning all remaining files after the first occurrence

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.

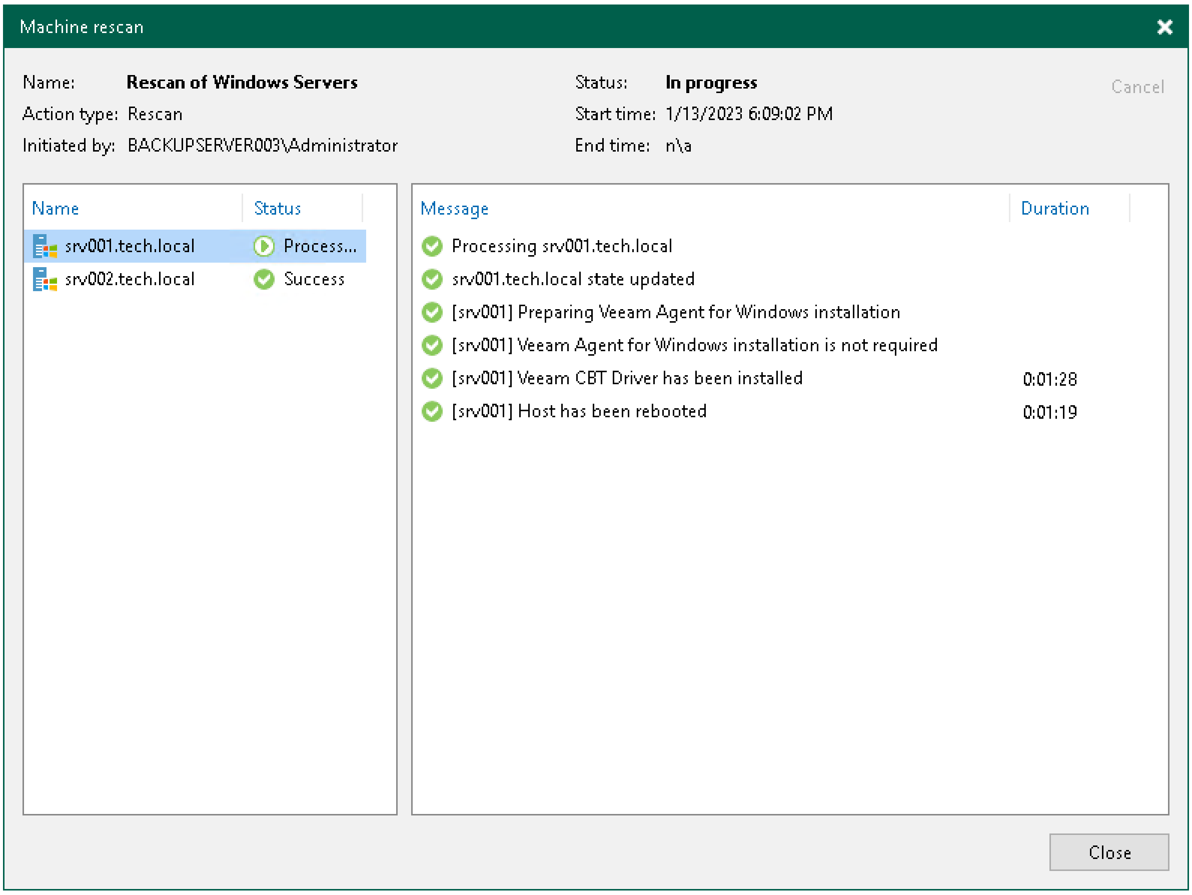
Viewing Rescan Job Statistics

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**.



Name: **Rescan of Windows Servers**
Action type: Rescan
Initiated by: BACKUPSERVER003\Administrator

Status: **In progress**
Start time: 1/13/2023 6:09:02 PM
End time: n\a

Name	Status
srv001.tech.local	Process...
srv002.tech.local	Success

Message	Duration
✓ Processing srv001.tech.local	
✓ srv001.tech.local state updated	
✓ [srv001] Preparing Veeam Agent for Windows installation	
✓ [srv001] Veeam Agent for Windows installation is not required	
✓ [srv001] Veeam CBT Driver has been installed	0:01:28
✓ [srv001] Host has been rebooted	0:01:19

Viewing Rescan Job Report

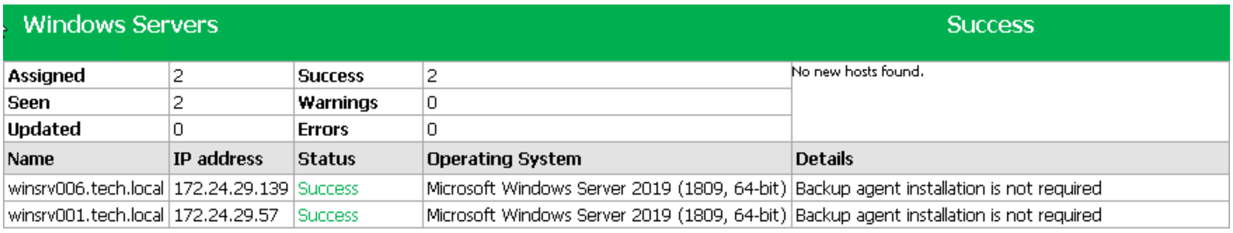
You can generate reports with details about rescan job sessions performed for a specific protection group. The report contains data on the latest rescan job session initiated for the job upon schedule. To generate a report:

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	No new hosts found.
Seen	2	**Warnings**	0	
Updated	0	**Errors**	0	
Name	**IP address**	**Status**	**Operating System**	**Details**
winsrv006.tech.local	172.24.29.139	Success	Microsoft Windows Server 2019 (1809, 64-bit)	Backup agent installation is not required
winsrv001.tech.local	172.24.29.57	Success	Microsoft Windows Server 2019 (1809, 64-bit)	Backup agent installation is not required

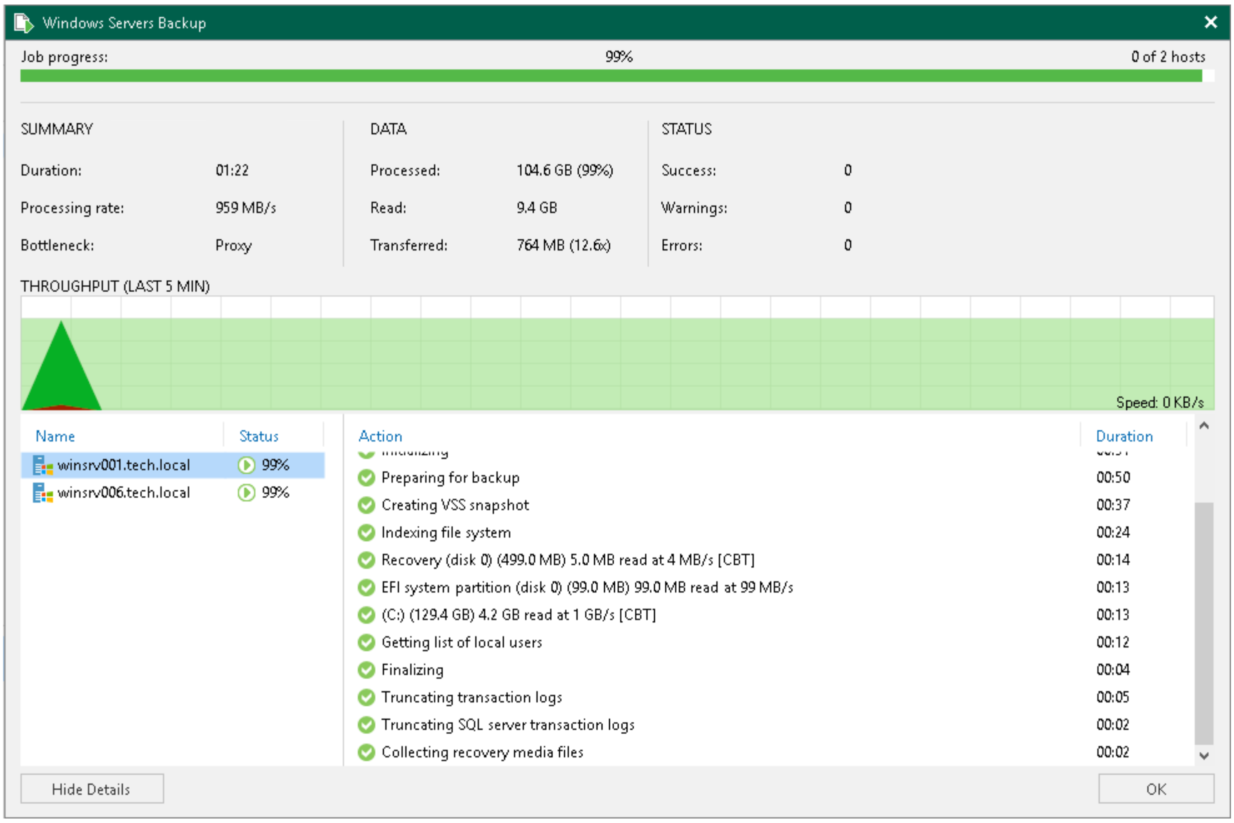
Viewing Veeam Agent Backup Job Statistics

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. Depending on the backup job settings, do the following:
   - If the backup job does not back up Microsoft SQL Server transaction logs, in the working area, select the necessary job and click **Statistics** on the ribbon or right-click the job and select **Statistics**.
   - If the backup job backs up Microsoft SQL Server transaction logs, in the working area, select the necessary job and click **Statistics** > **Instance Backup** on the ribbon or right-click the job and select **Statistics** > **Instance Backup**.

   For more information about backup of Microsoft SQL Server transaction logs, see Microsoft SQL Server Transaction Log Settings.



Windows Servers Backup

Job progress: 99% 0 of 2 hosts

SUMMARY		DATA		STATUS	
Duration:	01:22	Processed:	104.6 GB (99%)	Success:	0
Processing rate:	959 MB/s	Read:	9.4 GB	Warnings:	0
Bottleneck:	Proxy	Transferred:	764 MB (12.6x)	Errors:	0

THROUGHPUT (LAST 5 MIN)

Speed: 0 KB/s

Name	Status
winsrv001.tech.local	99%
winsrv006.tech.local	99%

Action	Duration
Initializing	00:51
Preparing for backup	00:50
Creating VSS snapshot	00:37
Indexing file system	00:24
Recovery (disk 0) (499.0 MB) 5.0 MB read at 4 MB/s [CBT]	00:14
EFI system partition (disk 0) (99.0 MB) 99.0 MB read at 99 MB/s	00:13
(C:) (129.4 GB) 4.2 GB read at 1 GB/s [CBT]	00:13
Getting list of local users	00:12
Finalizing	00:04
Truncating transaction logs	00:05
Truncating SQL server transaction logs	00:02
Collecting recovery media files	00:02

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. Depending on the backup job settings, do the following:
   - If the backup job does not back up Microsoft SQL Server transaction logs, in the working area, select the necessary job and click **Report** on the ribbon or right-click the job and select **Report**.
   - If the backup job backs up Microsoft SQL Server transaction logs, in the working area, select the necessary job and click **Report** > **Instance Backup** on the ribbon or right-click the job and select **Report** > **Instance Backup**.

   For more information about backup of Microsoft SQL Server transaction logs, see Microsoft SQL Server Transaction Log Settings.

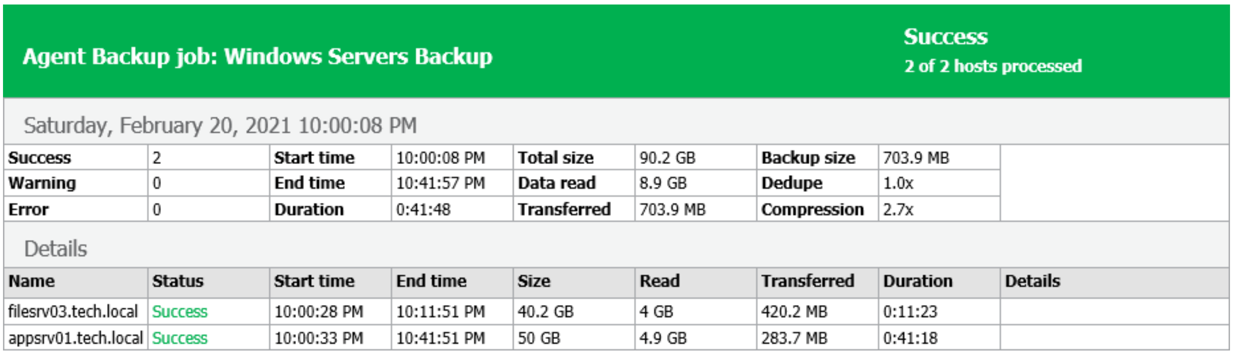
The report contains data on the latest job session:

- 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

Consider the following:

- You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.
- You can generate a separate report with details about SQL transaction log backup. To learn more, see Viewing SQL Transaction Log Backup Report.



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 **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.

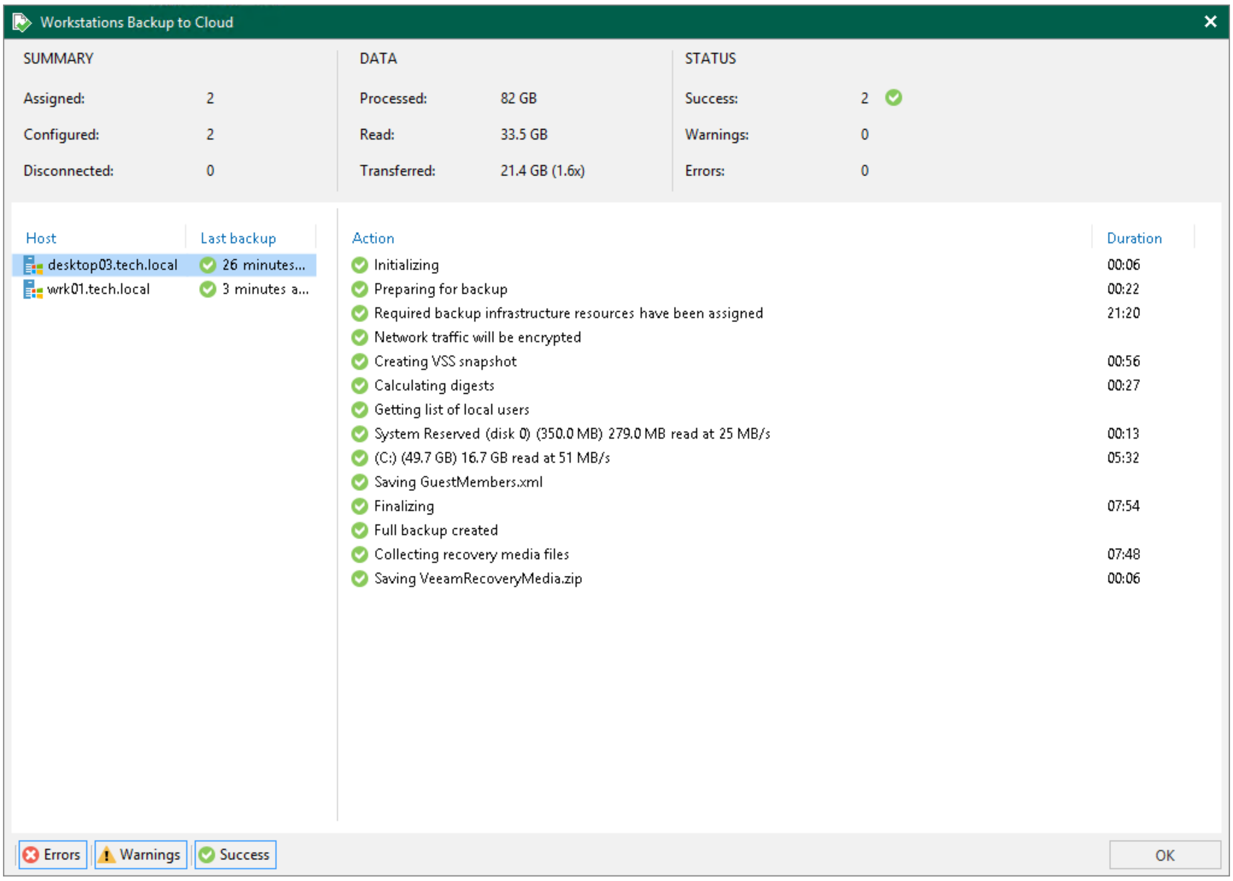
2. In the inventory pane, click the **Jobs** node.

3. Depending on the backup policy settings, do the following:

   - If the backup policy does not back up Microsoft SQL Server transaction logs, in the working area, select the necessary policy and click **Statistics** on the ribbon or right-click the policy and select **Statistics**.

   - If the backup policy backs up Microsoft SQL Server transaction logs, in the working area, select the necessary policy and click **Statistics** > **Instance Backup** on the ribbon or right-click the policy and select **Statistics** > **Instance Backup**.

   For more information about backup of Microsoft SQL Server transaction logs, see Microsoft SQL Server Transaction Log Settings.



Workstations Backup to Cloud

SUMMARY		DATA		STATUS	
Assigned:	2	Processed:	82 GB	Success:	2 ✓
Configured:	2	Read:	33.5 GB	Warnings:	0
Disconnected:	0	Transferred:	21.4 GB (1.6x)	Errors:	0

Host	Last backup
desktop03.tech.local	✓ 26 minutes...
wrk01.tech.local	✓ 3 minutes a...

Action	Duration
✓ Initializing	00:06
✓ Preparing for backup	00:22
✓ Required backup infrastructure resources have been assigned	21:20
✓ Network traffic will be encrypted	
✓ Creating VSS snapshot	00:56
✓ Calculating digests	00:27
✓ Getting list of local users	
✓ System Reserved (disk 0) (350.0 MB) 279.0 MB read at 25 MB/s	00:13
✓ (C:) (49.7 GB) 16.7 GB read at 51 MB/s	05:32
✓ Saving GuestMembers.xml	
✓ Finalizing	07:54
✓ Full backup created	
✓ Collecting recovery media files	07:48
✓ Saving VeeamRecoveryMedia.zip	00:06

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. Depending on the backup policy settings, do the following:
   - If the backup policy does not back up Microsoft SQL Server transaction logs, in the working area, select the necessary policy and click **Report** on the ribbon or right-click the policy and select **Report**.
   - If the backup policy backs up Microsoft SQL Server transaction logs, in the working area, select the necessary policy and click **Report > Instance Backup** on the ribbon or right-click the policy and select **Report > Instance Backup**.

   For more information about backup of Microsoft SQL Server transaction logs, see Microsoft SQL Server Transaction Log Settings.

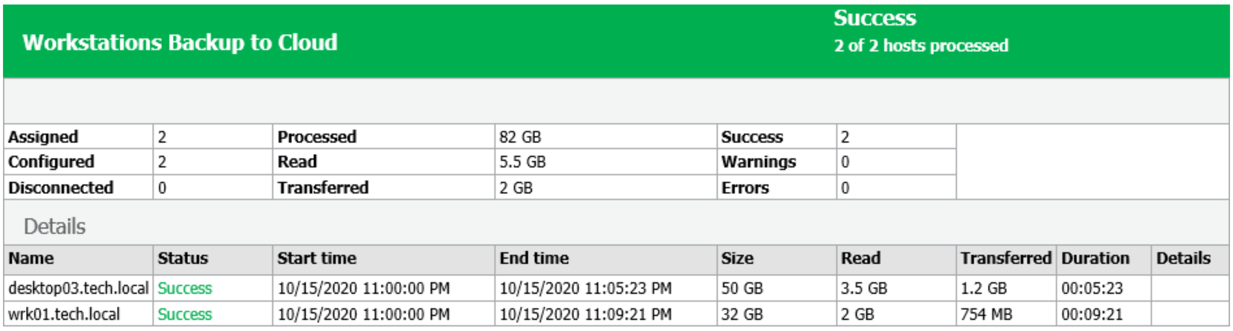
The report contains data on the latest job session:

- 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

Consider the following:

- You can also set up Veeam Backup & Replication to send reports automatically by email. To learn more, see Enabling Email Reporting.
- You can generate a separate report with details about SQL transaction log backup. To learn more, see Viewing SQL Transaction Log Backup Report.



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	

Viewing SQL Server Transaction Log Backup Statistics

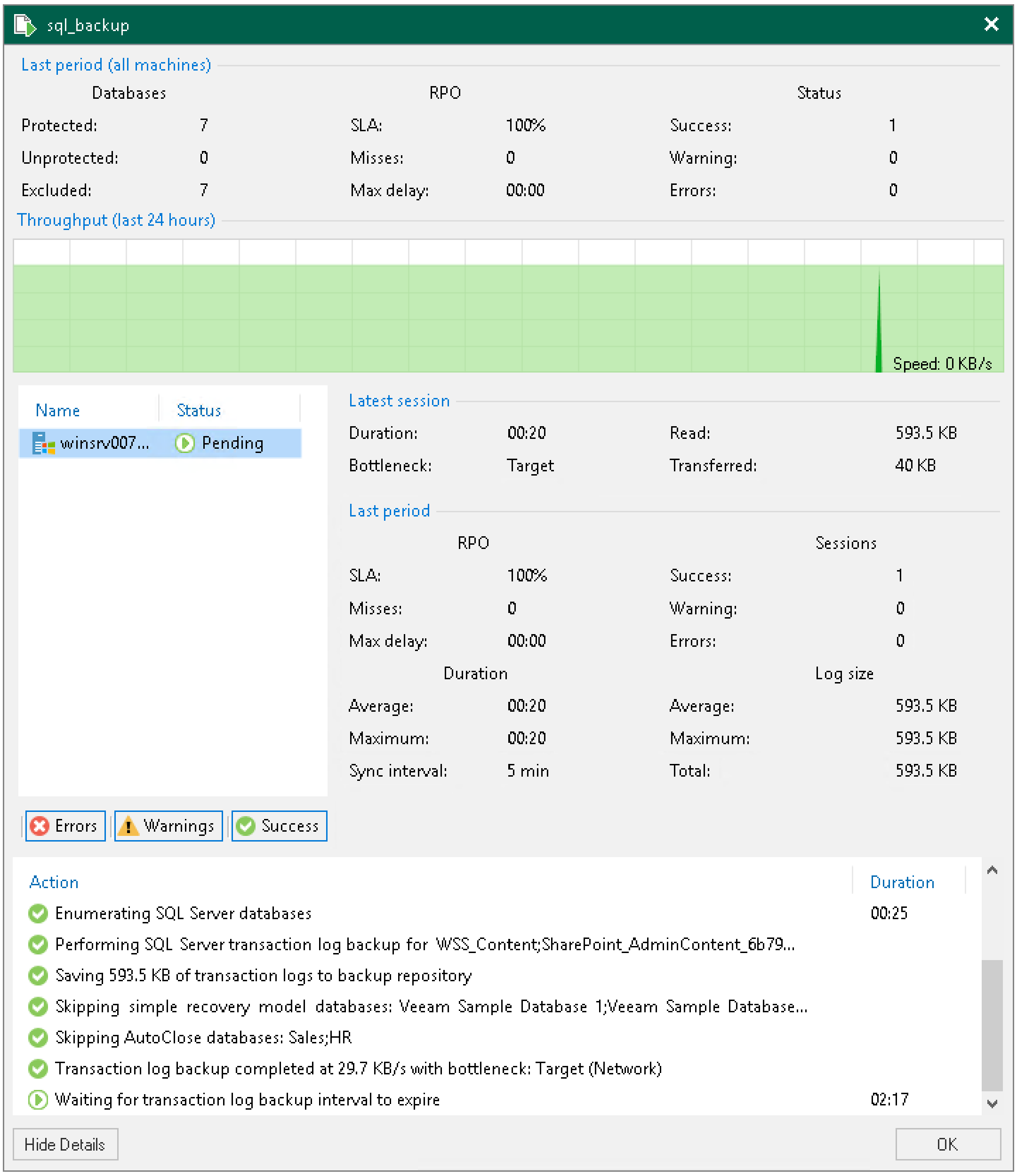
If you configure a backup job or backup policy to back up Microsoft SQL Server transaction logs, you can view statistics about the SQL Server transaction log backup job session performed on protected computers. For more information about backup of Microsoft SQL Server transaction logs, see Microsoft SQL Server Transaction Log Settings.

For Veeam Agent backup jobs and policies, Veeam Backup & Replication displays statistics in the similar way as for backup jobs for VM data backup. To learn more, see the Transaction Log Backup Statistics section in the Veeam Backup & Replication User Guide.

To view Veeam Agent backup job or backup policy statistics:

1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.

3. In the working area, select the necessary backup job or backup policy and click **Statistics** > **SQL Server log backup** on the ribbon. Alternatively, you can right-click the backup job or backup policy and select **Statistics** > **SQL Server log backup**.



sql_backup

Last period (all machines)

Databases		RPO		Status	
Protected:	7	SLA:	100%	Success:	1
Unprotected:	0	Misses:	0	Warning:	0
Excluded:	7	Max delay:	00:00	Errors:	0

Throughput (last 24 hours)

Name	Status
winsrv007...	Pending

Latest session

Duration:	00:20	Read:	593.5 KB
Bottleneck:	Target	Transferred:	40 KB

Last period

RPO		Sessions	
SLA:	100%	Success:	1
Misses:	0	Warning:	0
Max delay:	00:00	Errors:	0
Duration		**Log size**	
Average:	00:20	Average:	593.5 KB
Maximum:	00:20	Maximum:	593.5 KB
Sync interval:	5 min	Total:	593.5 KB

Action	Duration
✓ Enumerating SQL Server databases	00:25
✓ Performing SQL Server transaction log backup for WSS_Content;SharePoint_AdminContent_6b79...	
✓ Saving 593.5 KB of transaction logs to backup repository	
✓ Skipping simple recovery model databases: Veeam Sample Database 1;Veeam Sample Database...	
✓ Skipping AutoClose databases: Sales;HR	
✓ Transaction log backup completed at 29.7 KB/s with bottleneck: Target (Network)	
Waiting for transaction log backup interval to expire	02:17

Viewing SQL Server Transaction Log Backup Report

If you configure a backup job or backup policy to back up Microsoft SQL Server transaction logs, you can generate a report with details about the SQL Server transaction log backup job session performed on protected computers. For more information about backup of Microsoft SQL Server transaction logs, see Microsoft SQL Server Transaction Log Settings.

To generate the SQL Server transaction log backup report, do the following:

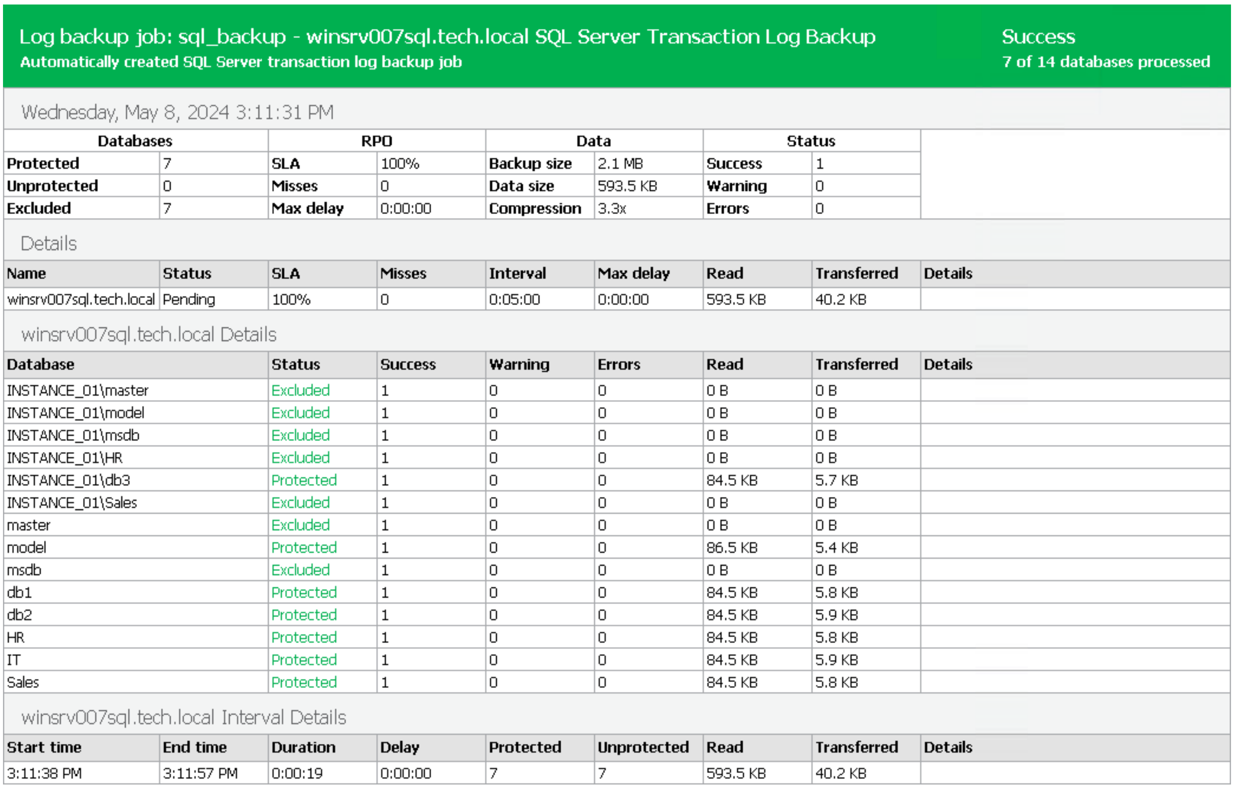
1. Open the **Home** view.
2. In the inventory pane, click the **Jobs** node.
3. In the working area, select the necessary backup job or backup policy and click **Report** > **SQL Server log backup** on the ribbon. Alternatively, you can right-click the backup job or backup policy and select **Report** > **SQL Server log backup**.

The report contains data on the latest SQL Server transaction log backup job session:

- Cumulative session statistics: number of processed databases, details on session performance, size of backed-up data, compression ratio, backup job session status.
- Detailed statistics for every computer processed within the session: session performance, amount of read and transferred data, list of warnings and errors (if any).
- Statistics for processed SQL databases: processing duration details, number of processed databases, amount of read and transferred data, list of warnings and errors (if any).

TIP

[For Veeam Agent backup jobs] If you set up Veeam Backup & Replication to send reports automatically by email, SQL Server transaction log backup reports is sent to the specified email address after each transaction log backup job session. For more information about email notifications, see Enabling Email Reporting.



Log backup job: sql_backup - winsrv007sql.tech.local SQL Server Transaction Log Backup
Automatically created SQL Server transaction log backup job

Success
7 of 14 databases processed

Wednesday, May 8, 2024 3:11:31 PM

Databases		RPO		Data		Status	
Protected	7	SLA	100%	Backup size	2.1 MB	Success	1
Unprotected	0	Misses	0	Data size	593.5 KB	Warning	0
Excluded	7	Max delay	0:00:00	Compression	3.3x	Errors	0

Details

Name	Status	SLA	Misses	Interval	Max delay	Read	Transferred	Details
winsrv007sql.tech.local	Pending	100%	0	0:05:00	0:00:00	593.5 KB	40.2 KB	

winsrv007sql.tech.local Details

Database	Status	Success	Warning	Errors	Read	Transferred	Details
INSTANCE_01\master	Excluded	1	0	0	0 B	0 B	
INSTANCE_01\model	Excluded	1	0	0	0 B	0 B	
INSTANCE_01\msdb	Excluded	1	0	0	0 B	0 B	
INSTANCE_01\HR	Excluded	1	0	0	0 B	0 B	
INSTANCE_01\db3	Protected	1	0	0	84.5 KB	5.7 KB	
INSTANCE_01\Sales	Excluded	1	0	0	0 B	0 B	
master	Excluded	1	0	0	0 B	0 B	
model	Protected	1	0	0	86.5 KB	5.4 KB	
msdb	Excluded	1	0	0	0 B	0 B	
db1	Protected	1	0	0	84.5 KB	5.8 KB	
db2	Protected	1	0	0	84.5 KB	5.9 KB	
HR	Protected	1	0	0	84.5 KB	5.8 KB	
IT	Protected	1	0	0	84.5 KB	5.9 KB	
Sales	Protected	1	0	0	84.5 KB	5.8 KB	

winsrv007sql.tech.local Interval Details

Start time	End time	Duration	Delay	Protected	Unprotected	Read	Transferred	Details
3:11:38 PM	3:11:57 PM	0:00:19	0:00:00	7	7	593.5 KB	40.2 KB	

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)

Exporting Logs

If you want to submit a support ticket, we recommend that you include log files to ensure that overall and comprehensive information is provided to Veeam Customer Support. Veeam Agent logs for computers of all protection group types are stored on the Veeam backup server. If you back up computers with pre-installed Veeam Agents, you can also collect logs directly from the protected computer.

To learn more, see the following subsections:

- Exporting Logs from Veeam Backup & Replication Console — if you want to collect the logs from the Veeam backup server.
- Exporting Logs from Veeam Agent Computers — if you want to collect the logs from a Veeam Agent computer with pre-installed Veeam Agent.

Exporting Logs from Veeam Backup & Replication Console

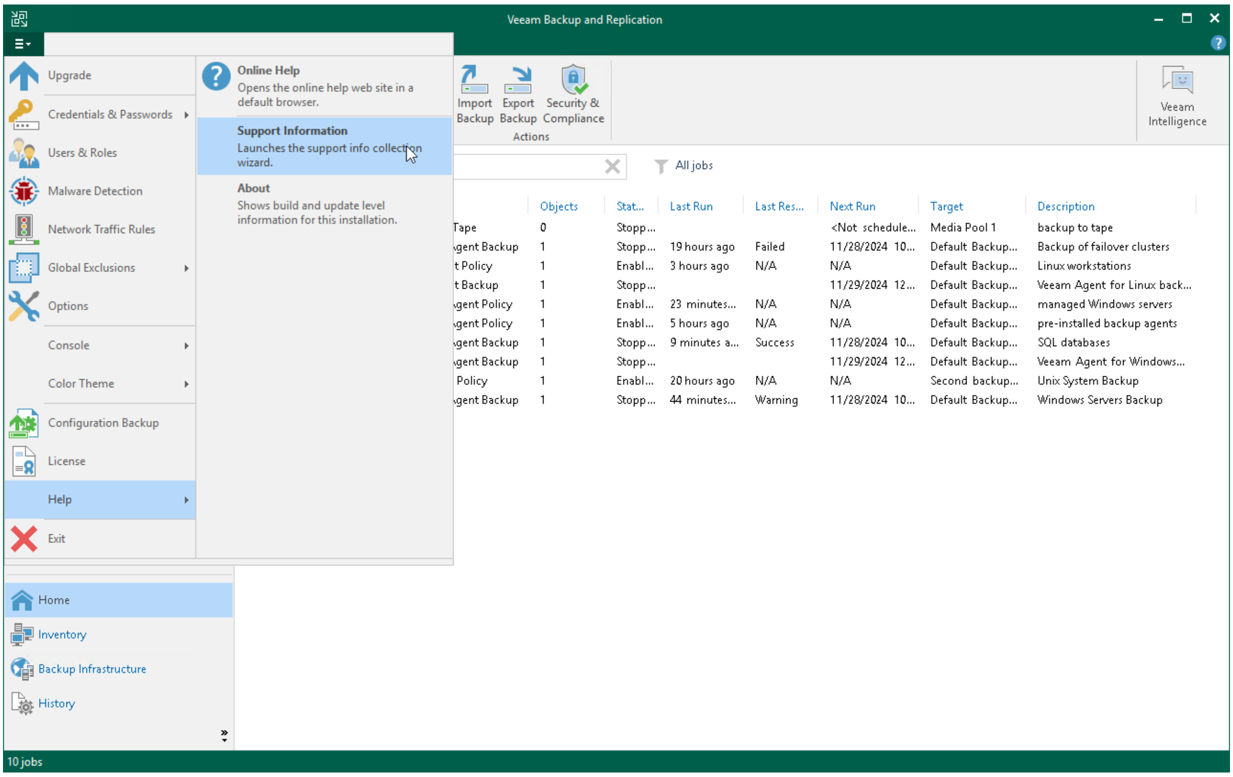
Veeam Backup & Replication stores log files in different locations. To learn more, see the Managing Logs section in the Veeam Backup & Replication User Guide.

To export all log files to one location, use the **Export Logs** wizard.

> **TIP**
>
> If you do not have access to the Veeam Backup & Replication console and you cannot use the built-in log export, export logs manually as described in this Veeam KB article.

Step 1. Launch Export Logs Wizard

To launch the **Export Logs** wizard, in the main menu of Veeam Backup & Replication select **Help** > **Support Information**.



	Objects	Stat...	Last Run	Last Res...	Next Run	Target	Description
Tape	0	Stopp...			<Not schedule...	Media Pool 1	backup to tape
gent Backup	1	Stopp...	19 hours ago	Failed	11/28/2024 10...	Default Backup...	Backup of failover clusters
t Policy	1	Enabl...	3 hours ago	N/A	N/A	Default Backup...	Linux workstations
t Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Linux back...
gent Policy	1	Enabl...	23 minutes...	N/A	N/A	Default Backup...	managed Windows servers
gent Policy	1	Enabl...	5 hours ago	N/A	N/A	Default Backup...	pre-installed backup agents
gent Backup	1	Stopp...	9 minutes a...	Success	11/28/2024 10...	Default Backup...	SQL databases
gent Backup	1	Stopp...			11/29/2024 12...	Default Backup...	Veeam Agent for Windows...
Policy	1	Enabl...	20 hours ago	N/A	N/A	Second backup...	Unix System Backup
gent Backup	1	Stopp...	44 minutes...	Warning	11/28/2024 10...	Default Backup...	Windows Servers Backup

Step 2. Select Physical Infrastructure Scope

At the **Scope** step of the wizard, define the scope for Veeam Agent logs export. You can select one of the following options:

- **Export logs for this job** — select this option if you want to export logs for specific backup jobs. Click **Choose** and specify the necessary backup job.

  In this case, Veeam Backup & Replication exports only the Veeam Metrics Collector Log (VMC.log) file that collects product usage metrics and infrastructure information for each Veeam Agent installation.

- **Export logs for these objects** — select this option if you want to export logs for specific Veeam Agent computers. Click **Choose** and specify the necessary Veeam Agent computer. If you export logs for a computer with pre-installed Veeam Agent, specify credentials for the user account that has access to the protected computer in the **Agent Credentials** window. Veeam Backup & Replication will not store these credentials in its database.

  In this case, Veeam Backup & Replication exports all Veeam Agent log files available on the Veeam backup server.

NOTE

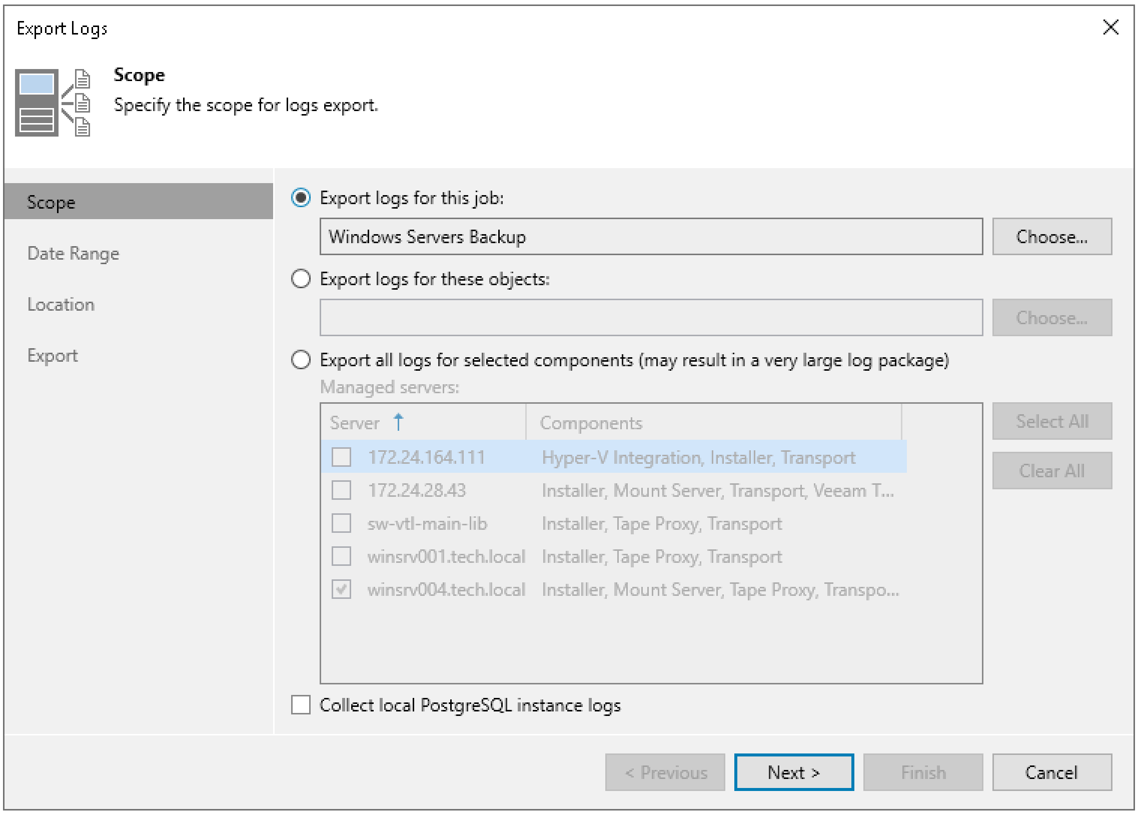
Consider the following:

- Do not select the **Export all logs for selected components** option if you want to export Veeam Agent logs. With this option selected, Veeam Backup & Replication retrieves logs from backup infrastructure components where Veeam Agent is not installed.
- When you export logs from the Veeam Backup & Replication console, the exported logs will be copied to the machine where the console is installed. The log archive will also contain logs from the console machine.

TIP

To select multiple jobs or objects at once, do one of the following:

- Hold [Ctrl] and click items to add to your selection.
- Hold [Shift] and select a range of items between the currently selected item and the one you click.



Export Logs

Scope

Specify the scope for logs export.

● Export logs for this job:

Windows Servers Backup

○ Export logs for these objects:

○ Export all logs for selected components (may result in a very large log package)

Managed servers:

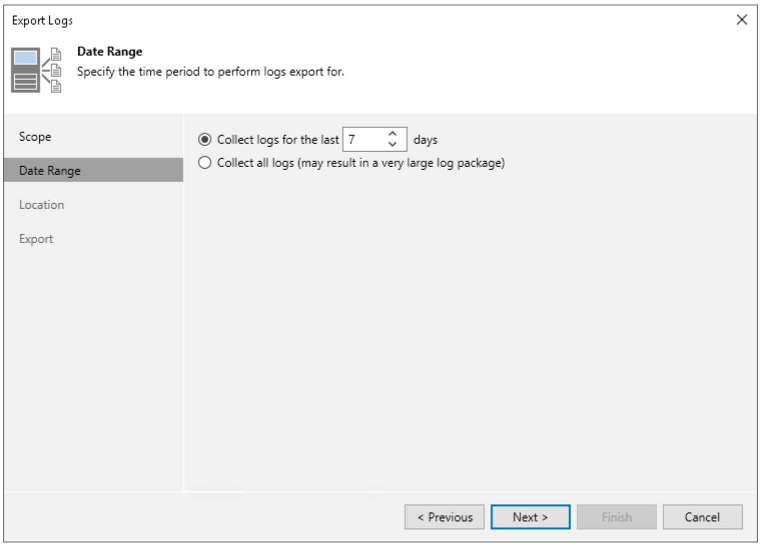
	Server	Components
□	172.24.164.111	Hyper-V Integration, Installer, Transport
□	172.24.28.43	Installer, Mount Server, Transport, Veeam T...
□	sw-vtl-main-lib	Installer, Tape Proxy, Transport
□	winsrv001.tech.local	Installer, Tape Proxy, Transport
☑	winsrv004.tech.local	Installer, Mount Server, Tape Proxy, Transpo...

□ Collect local PostgreSQL instance logs

Step 3. Specify Time Interval

At the **Date Range** step of the wizard, define the time interval for which logs must be collected. You can select one of the following options:

- Collect logs for the last <N> days
- Collect all available logs



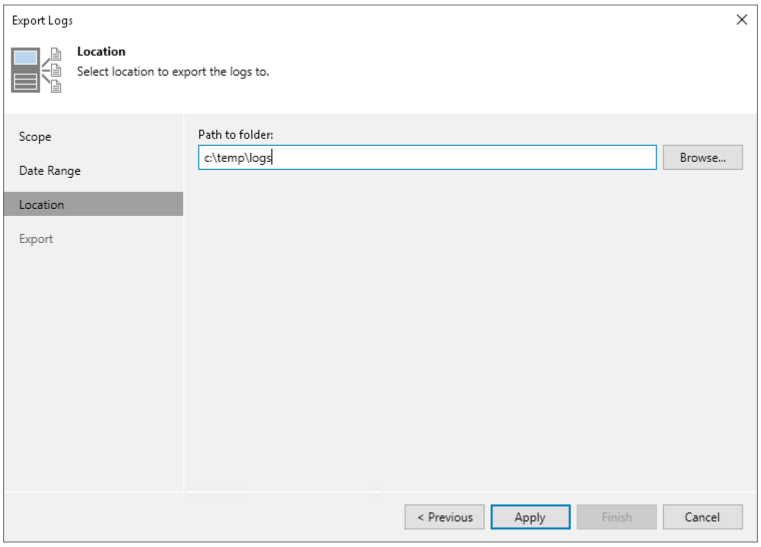
● Collect logs for the last 7 days

○ Collect all logs (may result in a very large log package)

Step 4. Specify Destination Folder

At the **Location** step of the wizard, specify the destination folder to which the logs will be exported.

In the **Path to folder** field, specify a path to an archive with log files that will be created. By default, the archive is placed to the `C:\temp\logs` folder on the backup server.



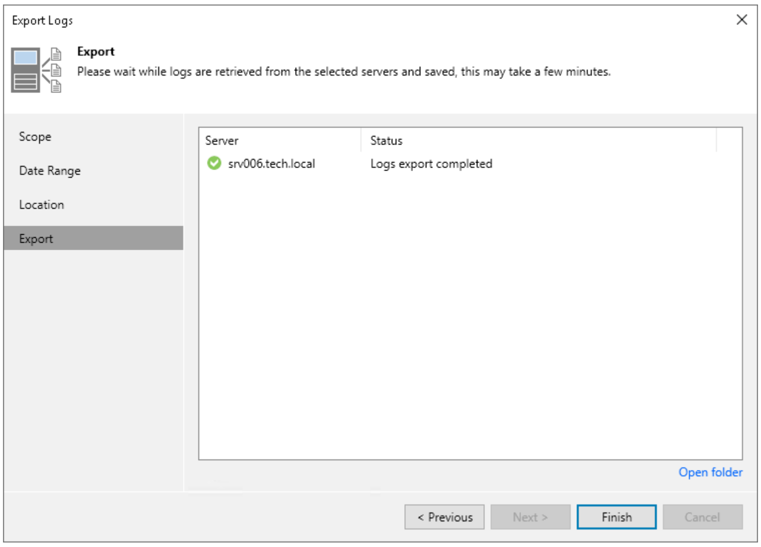
Path to folder: c:\temp\logs

Step 5. Review Results

At the **Export** step of the wizard, Veeam Backup & Replication will collect specified logs and create a log archive. Wait for the export process to complete, review the results and click the **Open folder** link to browse the exported log files.

TIP

During the log export process, Veeam Backup & Replication locks the console, so you cannot close the **Export Logs** wizard. If you do not want to wait until the log export process completes, you can run another session of the Veeam Backup & Replication concurrently and continue work with it.



Export Logs

Export

Please wait while logs are retrieved from the selected servers and saved, this may take a few minutes.

Server	Status
✓ srv006.tech.local	Logs export completed

Exporting Logs from Veeam Agent Computers

If Veeam Agent computer is connected to a Veeam backup server as a member of a protection group for pre-installed Veeam Agents, you can export Veeam Agent logs directly from the Veeam Agent computer.

When you export product logs, Veeam Agent collects its log files, exports them to an archive file in the `tar.gz` format and saves this archive file to the following folder on the Veeam backup server:

```
C:\ProgramData\Veeam\Backup\Endpoint\Other\AgentLogs\<computer_name>
```

where `<computer_name>` — name of the computer with Veeam Agent installed.

For more information on exporting product logs from a Veeam Agent computer, see the following user guides depending on the Veeam Agent that you use:

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

Operations Available on Veeam Agent Computer

If Veeam Agent operates under control of Veeam Backup & Replication, the Veeam backup administrator can perform all data protection, data restore and administration tasks from the Veeam Backup & Replication console.

On the Veeam Agent computer side, the list of available operations depends on how the backup job for this computer is managed: by Veeam backup server or by Veeam Agent. For more information about backup job types, see Veeam Agent Backup Jobs and Policies.

The list of operations that can be performed in Veeam Agent operating in the managed mode varies depending on the operating system of the protected computer:

- Operations available on Windows Computers
- Operations available on Linux Computers
- Operations available on Unix Computers
- Operations available on Mac Computers

Operations Available on Windows Computers

The list of operations that you can perform on a Windows-based Veeam Agent computer managed by Veeam Backup & Replication depends on the backup job type:

- If a Veeam Agent computer is protected by a backup job managed by the backup server, on the Veeam Agent computer side you can perform restore from Veeam Recovery Media. To learn more, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.

  > NOTE
  >
  > Make sure that Veeam Recovery Media was created beforehand and you can access it. For a Veeam Agent computer protected by a backup job managed by the backup server, you can create Veeam Recovery Media from the Veeam Backup & Replication console. To learn more, see Creating Veeam Recovery Media.

- If a Veeam Agent computer is protected by a backup job managed by Veeam Agent, on the Veeam Agent computer side you can perform the following operations:

  - View information about Veeam Agent.
  - Create Veeam Recovery Media.
  - Perform incremental backup.
  - Stop backup job.
  - Perform restore.
  - View session statistics.
  - Get support.

Viewing Information About Veeam Agent

You can view the Veeam Agent version, product edition and information about the backup server that manages the Veeam Agent computer:

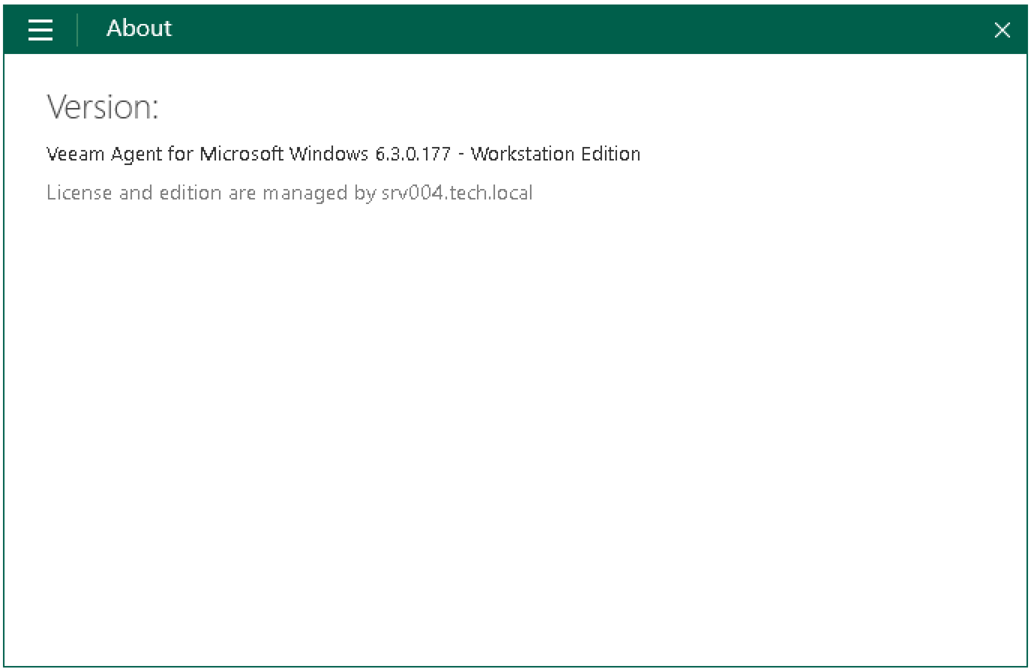
1. Double-click the Veeam Agent icon in the system tray, or right-click the Veeam Agent icon in the system tray and select **Control Panel**.

   If you do not see the Veeam Agent icon in the system tray, run Veeam Agent for Microsoft Windows from the Microsoft Windows Start menu.

2. Open the **About** tab.

TIP

You can update the license and product edition from the Veeam Backup & Replication console. For more information, see the Updating License section in the Veeam Backup & Replication User Guide.



Version:

Veeam Agent for Microsoft Windows 6.3.0.177 - Workstation Edition

License and edition are managed by srv004.tech.local

Creating Veeam Recovery Media

The procedure of creating Veeam Recovery Media for Veeam Agent operating in the managed mode does not differ from the same procedure for Veeam Agent operating in the standalone mode. You can create Veeam Recovery Media in the following ways:

- With the **Create Recovery Media** wizard. For more information, see the Creating Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.
- Using the command line interface. For more information, see the Creating Veeam Recovery Media with Command Line Interface section in the Veeam Agent for Microsoft Windows User Guide.

Performing Incremental Backup

The procedure of creating ad-hoc incremental backup for Veeam Agent operating in the managed mode does not differ from the same procedure for Veeam Agent operating in the standalone mode. You can create ad-hoc incremental backup in the following ways:

- From the Veeam Agent control panel. For more information, see the Creating Incremental Backups section in the Veeam Agent for Microsoft Windows User Guide.
- Using the command line interface. For more information, see the Creating Backups section in the Veeam Agent for Microsoft Windows User Guide.

Stopping Backup Job

You can stop any running backup job from the Veeam Agent control panel. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see the Stopping Backup Job section in the Veeam Agent for Microsoft Windows User Guide.

Performing Restore

If you experience a problem with your computer, your data gets lost or corrupted, you can recover your data or bring the computer back to work. The restore options for Veeam Agent operating in the managed mode does not differ from the same options for Veeam Agent operating in the standalone mode. You can perform restore in the following ways:

- You can perform restore from Veeam Recovery Media. For more information, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.
- You can perform restore using Veeam Agent and Microsoft Windows Tools. For more information, see the Using Veeam Agent and Microsoft Windows Tools section in the Veeam Agent for Microsoft Windows User Guide.
- You can perform restore using Microsoft Windows Recovery Environment. For more information, see the Using Microsoft Windows Recovery Environment section in the Veeam Agent for Microsoft Windows User Guide.
- You can restore volumes. For more information, see the Restoring Volumes section in the Veeam Agent for Microsoft Windows User Guide.
- You can restore individual files and folders. For more information, see the Restoring Files and Folders in the Veeam Agent for Microsoft Windows User Guide.
- You can perform restore from an encrypted backup. For more information, see the Restoring Data from Encrypted Backups section in the Veeam Agent for Microsoft Windows User Guide.

> NOTE
>
> By default, restore from the Veeam Agent computer side is available only for user accounts with Local Administrator permissions.
>
> If you want to perform restore under accounts that do not have administrative privileges, make sure that the **Allow file level recovery without administrative account** check box in the Veeam Agent for Microsoft Windows settings is selected before you start the restore process. To learn more, see Veeam Agent for Microsoft Windows Settings.

Viewing Session Progress, Statistics and Results

You can get information about backup and restore sessions. Available options do not differ from those for Veeam Agent operating in the standalone mode:

- You can view statistics of the completed sessions in the Veeam Agent control panel. For more information, see the Viewing Statistics in Control Panel section in the Veeam Agent for Microsoft Windows User Guide.
- You can get information about the backup state using the Veeam Agent for Microsoft Windows tray agent. For more information, see the Monitoring Backup State with Tray Agent section in the Veeam Agent for Microsoft Windows User Guide.
- You can get information about the backup progress using the Veeam Agent for Microsoft Windows taskbar button. For more information, see the Monitoring Backup Process in Taskbar Button section in the Veeam Agent for Microsoft Windows User Guide.

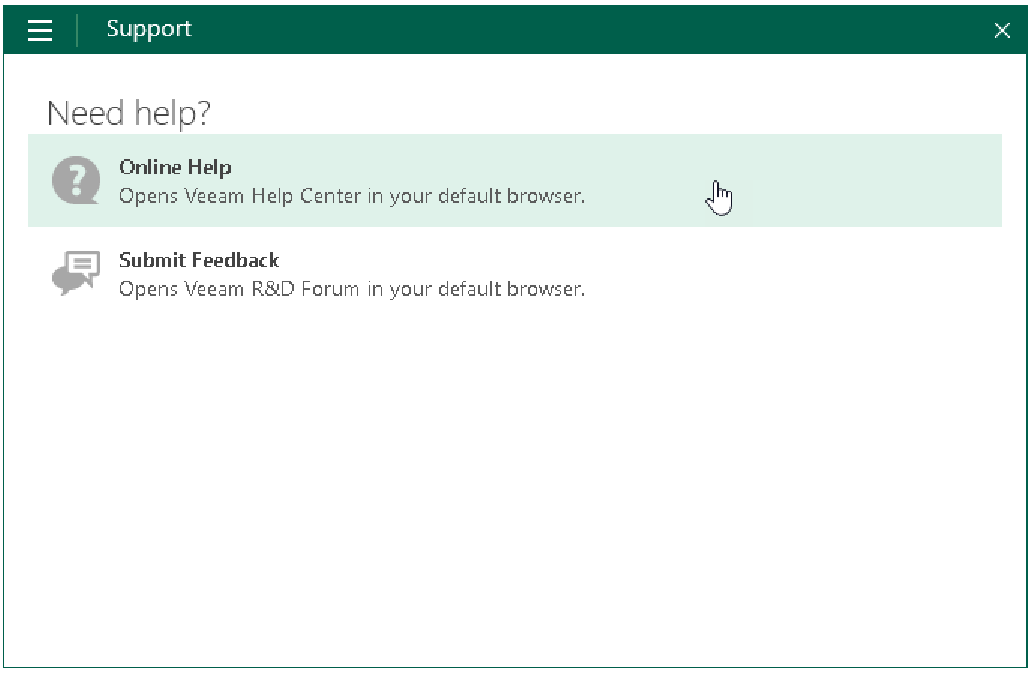
Getting Support

If you have any questions or want to share your feedback about Veeam Agent, you can use one of the following options:

- Contact your Veeam backup administrator.
- Search for the information on the necessary subject in the current Veeam Agent for Microsoft Windows User Guide.
- Visit Veeam R&D Forums and share your opinion or ask a question.

To access help and support options in Veeam Agent:

1. Right-click the Veeam Agent for Microsoft Windows icon in the system tray and select **Control Panel**.
2. From the main menu, select **Support**.
3. Click one of available options to get support on the product.



Online Help
Opens Veeam Help Center in your default browser.

Submit Feedback
Opens Veeam R&D Forum in your default browser.

Operations Available on Linux Computers

The list of operations that you can perform on a Linux-based Veeam Agent computer managed by Veeam Backup & Replication depends on the backup job type. Some operations are available only if the computer is protected with a backup job managed by Veeam Agent.

If Veeam Agent computer is protected by a backup job managed by either backup server or Veeam Agent, on the Veeam Agent computer side you can perform the following operations:

- View information about Veeam Agent.
- Create Veeam Recovery Media.
- Stop backup job.
- View session statistics.
- Perform restore.
- Manage operation mode.
- Export logs.

If Veeam Agent computer is protected by a backup job managed by Veeam Agent, on the Veeam Agent computer side you can also perform the following operations:

- View backup job details.
- Start backup job.
- Start active full backup.

Viewing Information About Veeam Agent

You can view the following information about Veeam Agent in the command line interface:

- Veeam Agent version. To view the version of Veeam Agent, run the following command:

  ```
  veeamconfig version
  ```

- Veeam Agent license.

  > **NOTE**
  >
  > You can view information about Veeam Agent license only if the computer is protected with a backup job managed by Veeam Agent.

  To view information on the Veeam Agent license, run the following command:

  ```
  veeamconfig license show
  ```

- Veeam Agent operation mode. To view information on the Veeam Agent operation mode, run the following command:

```
veeamconfig mode info
```

> TIP
>
> You can also change the operation mode of Veeam Agent. For more information, see Manage Operation Mode.

Creating Veeam Recovery Media

You can create a custom recovery media for the protected Linux computer. The procedure of creating custom Veeam Recovery Media for Veeam Agent operating in the managed mode does not differ from the same procedure for Veeam Agent operating in the standalone mode. For more information, see the Creating Custom Veeam Recovery Media section in the Veeam Agent for Linux User Guide.

Viewing Backup Job Details

> NOTE
>
> This operation is available only if the computer is protected with a backup job managed by Veeam Agent.

You can view the settings of backup jobs managed by Veeam Agent. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see Viewing Backup Job Settings in the Veeam Agent for Linux User Guide.

Starting Backup Job

> NOTE
>
> This operation is available only if the computer is protected with a backup job managed by Veeam Agent.

On the Veeam Agent computer side, you can start a backup job managed by Veeam Agent from the Veeam Agent control panel or using the command line interface. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see Starting Backup Job from Control Panel and Starting Backup Job from Command Line Interface in the Veeam Agent for Linux User Guide.

Starting Active Full Backup

> NOTE
>
> This operation is available only if the computer is protected with a backup job managed by Veeam Agent.

On the Veeam Agent computer side, you can create ad-hoc active full backups. You can start a backup job that will create an active full backup from the Veeam Agent control panel or using the command line interface. The procedure of creating an active full backup does not differ from the same procedure for Veeam Agent operating in the standalone mode. For more information, see Starting Backup Job from Control Panel and Creating Active Full Backups in the Veeam Agent for Linux User Guide.

Stopping Backup Job

On the Veeam Agent computer side, you can stop any running backup job from the Veeam Agent control panel or using the command line interface. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see Stopping Backup Job in the Veeam Agent for Linux User Guide.

Viewing Session Progress, Statistics and Results

On the Veeam Agent computer side, you can view the statistics of the completed backup job and restore sessions from the Veeam Agent control panel or using the command line interface. You can also view the progress and statistics of a running session in real-time. The options of viewing session statistics do not differ from the same options for Veeam Agent operating in the standalone mode. For more information, see the Reporting section in the Veeam Agent for Linux User Guide.

Performing Restore

The restore options for Veeam Agent operating in the managed mode are similar to the restore options for Veeam Agent operating in the standalone mode.

> NOTE
>
> When Veeam Agent is managed by Veeam Backup & Replication, you cannot import backups to the Veeam Agent computer.

You can perform the following restore operations:

- You can perform restore from Veeam Recovery Media. For more information, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Linux User Guide.
- You can restore volumes. For more information, see the Restoring Volumes with Command Line Interface section in the Veeam Agent for Linux User Guide.
- You can restore individual files and folders. For more information, see the Restoring Files and Folders with Recovery Wizard and Restoring Files and Folders with Command Line Interface sections in the Veeam Agent for Linux User Guide.
- You can perform restore from an encrypted backup. For more information, see the Restoring Data from Encrypted Backups section in the Veeam Agent for Linux User Guide.

Managing Operation Mode

You can manage the operation mode of Veeam Agent. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see the Managing Veeam Agent Operation Mode section in the Veeam Agent for Linux User Guide.

Exporting Logs

This operation may be required if you want to report an issue and need to attach log files to the support case. The procedure of exporting product logs does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see the Exporting Product Logs section in the Veeam Agent for Linux User Guide.

Operations Available on Unix Computers

If a Unix-based Veeam Agent computer is managed by Veeam Backup & Replication, you can protect such computers only by a backup job managed by Veeam Agent.

On the Veeam Agent computer side, you can perform the following operations:

- View information about Veeam Agent.
- Create Veeam Recovery Media.
- View backup job details.
- Start backup job.
- Start active full backup.
- Stop backup job.
- View session statistics.
- Perform restore.
- Manage operation mode.
- Export logs.

Viewing Information About Veeam Agent

You can view the following information about Veeam Agent in the command line interface:

- Veeam Agent version. To view the version of Veeam Agent, run the following command:

  ```
  veeamconfig version
  ```

- Veeam Agent license. To view information on the Veeam Agent license, run the following command:

  ```
  veeamconfig license show
  ```

- Veeam Agent operation mode. To view information on the Veeam Agent operation mode, run the following command:

  ```
  veeamconfig mode info
  ```

  > TIP
  >
  > You can also change the operation mode of Veeam Agent. For more information, see Manage Operation Mode.

Creating Veeam Recovery Media

You can create a recovery media for the protected Unix computer. The procedure of creating Veeam Recovery Media for Veeam Agent operating in the managed mode does not differ from the same procedure for Veeam Agent operating in the standalone mode.

For more information on creating Veeam Recovery Media in Veeam Agent for IBM AIX, see the Creating Custom Veeam Recovery Media section in the Veeam Agent for IBM AIX User Guide.

For more information on creating Veeam Recovery Media in Veeam Agent for Oracle Solaris, see the Creating Custom Veeam Recovery Media section in the Veeam Agent for Oracle Solaris User Guide.

Viewing Backup Job Details

You can view the settings of backup jobs managed by Veeam Agent. This process does not differ from the one for Veeam Agent operating in the standalone mode.

For more information on viewing backup job settings in Veeam Agent for IBM AIX, see Viewing Backup Job Settings in the Veeam Agent for IBM AIX User Guide.

For more information on viewing backup job settings in Veeam Agent for Oracle Solaris, see Viewing Backup Job Settings in the Veeam Agent for Oracle Solaris User Guide.

Starting Backup Job

On the Veeam Agent computer side, you can start a backup job managed by Veeam Agent from the Veeam Agent control panel or using the command line interface. This process does not differ from the one for Veeam Agent operating in the standalone mode.

For more information on starting a backup job in Veeam Agent for IBM AIX, see Starting Backup Job from Control Panel and Starting Backup Job in Command Line Interface in the Veeam Agent for IBM AIX User Guide.

For more information on starting a backup job in Veeam Agent for Oracle Solaris, see Starting Backup Job from Control Panel and Starting Backup Job in Command Line Interface in the Veeam Agent for Oracle Solaris User Guide.

Starting Active Full Backup

On the Veeam Agent computer side, you can create ad-hoc active full backups. You can start a backup job that will create an active full backup either from the Veeam Agent control panel or using the command line interface. The procedure of creating an active full backup does not differ from the same procedure for Veeam Agent operating in the standalone mode.

For more information on creating active full backups in Veeam Agent for IBM AIX, see Starting Backup Job from Control Panel and Creating Active Full Backups in Command Line Interface in the Veeam Agent for IBM AIX User Guide.

For more information on creating active full backups in Veeam Agent for Oracle Solaris, see Starting Backup Job from Control Panel and Creating Active Full Backups in Command Line Interface in the Veeam Agent for Oracle Solaris User Guide.

Stopping Backup Job

On the Veeam Agent computer side, you can stop any running backup job from the Veeam Agent control panel or using the command line interface. This process does not differ from the one for Veeam Agent operating in the standalone mode.

For more information on stopping a backup job in Veeam Agent for IBM AIX, see Stopping Backup Job in the Veeam Agent for IBM AIX User Guide.

For more information on stopping a backup job in Veeam Agent for Oracle Solaris, see Stopping Backup Job in the Veeam Agent for Oracle Solaris User Guide.

Viewing Session Progress, Statistics and Results

On the Veeam Agent computer side, you can view the statistics of the completed backup job and restore sessions from the Veeam Agent control panel or using the command line interface. You can also view the progress and statistics of a running session in real-time. The options of viewing session statistics do not differ from the same options for Veeam Agent operating in the standalone mode.

For more information on viewing session statistics in Veeam Agent for IBM AIX, see the Reporting section in the Veeam Agent for IBM AIX User Guide.

For more information on viewing session statistics in Veeam Agent for Oracle Solaris, see the Reporting section in the Veeam Agent for Oracle Solaris User Guide.

Performing Restore

The restore options for Veeam Agent operating in the managed mode do not differ from the same options for Veeam Agent operating in the standalone mode. You can perform restore in the following ways:

- You can perform restore from Veeam Recovery Media.

  For more information on performing restore from Veeam Recovery Media in Veeam Agent for IBM AIX, see the Performing Bare Metal Recovery section in the Veeam Agent for IBM AIX User Guide.

  For more information on performing restore from Veeam Recovery Media in Veeam Agent for Oracle Solaris, see the Performing Bare Metal Recovery section in the Veeam Agent for Oracle Solaris User Guide.

- You can restore individual files and folders.

  For more information on file-level restore in Veeam Agent for IBM AIX, see the Restoring Files and Directories section in the Veeam Agent for IBM AIX User Guide.

  For more information on file-level restore in Veeam Agent for Oracle Solaris, see the Restoring Files and Directories section in the Veeam Agent for Oracle Solaris User Guide.

- You can perform restore from an encrypted backup.

  For more information on restoring from encrypted backups in Veeam Agent for IBM AIX, see the Restoring Data from Encrypted Backups section in the Veeam Agent for IBM AIX User Guide.

  For more information on restoring from encrypted backups in Veeam Agent for Oracle Solaris, see the Restoring Data from Encrypted Backups section in the Veeam Agent for Oracle Solaris User Guide.

Managing Operation Mode

You can manage the operation mode of Veeam Agent. This process does not differ from the one for Veeam Agent operating in the standalone mode.

For more information managing operation mod in Veeam Agent for IBM AIX, see the Managing Veeam Agent Operation Mode section in the Veeam Agent for IBM AIX User Guide.

For more information managing operation mod in Veeam Agent for Oracle Solaris, see the Managing Veeam Agent Operation Mode section in the Veeam Agent for Oracle Solaris User Guide.

Exporting Logs

This operation may be required if you want to report an issue and need to attach log files to the support case. The procedure of exporting product logs does not differ from the one for Veeam Agent operating in the standalone mode.

For more information on exporting logs in Veeam Agent for IBM AIX, see the Exporting Product Logs section in the Veeam Agent for IBM AIX User Guide.

For more information on exporting logs in Veeam Agent for Oracle Solaris, see the Exporting Product Logs section in the Veeam Agent for Oracle Solaris User Guide.

Operations Available on Mac Computers

Mac computers are managed by Veeam Backup & Replication through a protection group for pre-installed Veeam Agents. You can protect Mac computers only by a backup job managed by Veeam Agent.

On the Veeam Agent computer side, you can perform the following operations:

- View information about Veeam Agent.
- View backup job details.
- Start backup job.
- Start active full backup.
- Stop backup job.
- View session statistics.
- Perform restore.
- Manage operation mode.
- Export logs.
- Get support.

Viewing Information About Veeam Agent

You can view the following information about Veeam Agent in the command line interface:

- Veeam Agent version. To view the version of Veeam Agent, run the following command:

  ```
  veeamconfig version
  ```

- Veeam Agent license. To view information on the Veeam Agent license, run the following command:

  ```
  veeamconfig license show
  ```

- Veeam Agent operation mode. To view information on the Veeam Agent operation mode, run the following command:

  ```
  veeamconfig mode info
  ```

  > TIP
  >
  > You can also change the operation mode of Veeam Agent. For more information, see Manage Operation Mode.

Viewing Backup Job Details

You can view the settings of backup jobs managed by Veeam Agent. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see Viewing Backup Job Settings in the Veeam Agent for Mac User Guide.

Starting Backup Job

On the Veeam Agent computer side, you can start a backup job managed by Veeam Agent either from the Veeam Agent control panel or using the command line interface. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see Starting Backup Job and Starting Backup Job in CLI in the Veeam Agent for Mac User Guide.

Starting Active Full Backup

On the Veeam Agent computer side, you can create ad-hoc active full backups. You can start a backup job that will create an active full backup either from the Veeam Agent control panel or using the command line interface. The procedure of creating an active full backup does not differ from the same procedure for Veeam Agent operating in the standalone mode. For more information, see Creating Active Full Backup and Creating Active Full Backup in CLI in the Veeam Agent for Mac User Guide.

Stopping Backup Job

On the Veeam Agent computer side, you can stop any running backup job from the Veeam Agent control panel or using the command line interface. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see Stopping Backup Job and Stopping Backup Job in CLI in the Veeam Agent for Mac User Guide.

Viewing Session Progress, Statistics and Results

On the Veeam Agent computer side, you can view the statistics of the completed backup job and restore sessions from the Veeam Agent control panel or using the command line interface. You can also view the progress and statistics of a running session in real-time. The options of viewing session statistics do not differ from the same options for Veeam Agent operating in the standalone mode. For more information, see the Reporting section in the Veeam Agent for Mac User Guide.

Performing Restore

The restore options for Veeam Agent operating in the managed mode do not differ from the same options for Veeam Agent operating in the standalone mode. You can perform restore in the following ways:

- You can restore user profile data. For more information, see the Restoring User Data section in the Veeam Agent for Mac User Guide.
- You can restore individual files and folders. For more information, see the Restoring Files and Folders section in the Veeam Agent for Mac User Guide.
- You can perform restore from an encrypted backup. For more information, see the Restoring Data from Encrypted Backups section in the Veeam Agent for Mac User Guide.

Managing Operation Mode

You can manage the operation mode of Veeam Agent. This process does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see Managing Veeam Agent Operation Mode in the Veeam Agent for Mac User Guide.

Exporting Logs

This operation may be required if you want to report an issue and need to attach log files to the support case. The procedure of exporting product logs does not differ from the one for Veeam Agent operating in the standalone mode. For more information, see the Exporting Product Logs section in the Veeam Agent for Mac User Guide.

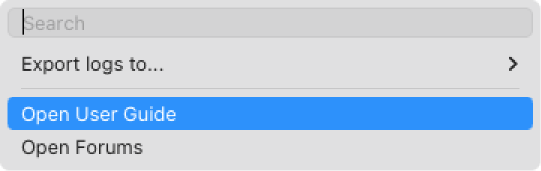
Getting Support

If you have any questions or want to share your feedback about Veeam Agent, you can use one of the following options:

- Contact your Veeam backup administrator.
- Search for the information on the necessary subject in the current Veeam Agent for Mac User Guide.
- Visit Veeam R&D Forums and share your opinion or ask a question.

To access help and support options in Veeam Agent:

1. In the Veeam Agent application menu, select **Help**.
2. In the **Help** menu, select one of available options to get support on the product:
   - Open User Guide
   - Open Forums



Appendix

This section provides information on additional procedures available for Veeam Agents operating in the managed mode.

In this Section

Deploying Hotfix on Protected Computers

A Veeam Agent hotfix is a set of updated Veeam Agent packages that addresses a certain issue in the product. This scenario describes how to deploy a hotfix on protected computers with one of the following installed Veeam Agents:

- Veeam Agent for Microsoft Windows
- Veeam Agent for Linux
- Veeam Agent for Unix (Veeam Agent for Oracle Solaris and Veeam Agent for IBM AIX)

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 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 added to protection groups for pre-installed Veeam Agents.

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.

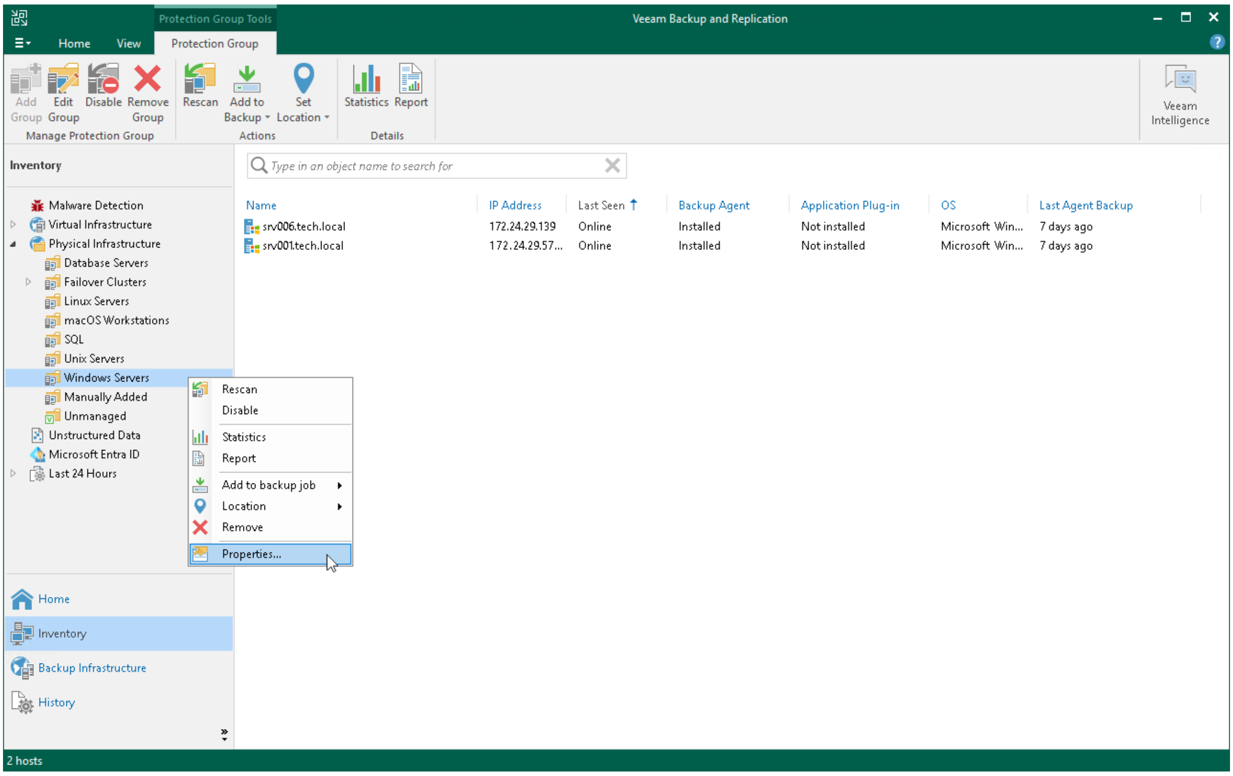
   We recommend that you do not stop running jobs and let them complete successfully. Disable any periodic jobs temporarily to prevent them from starting during the upgrade. If protected computers run VSS-aware applications and backup of database logs (Microsoft SQL Server transaction logs or Oracle archived 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.

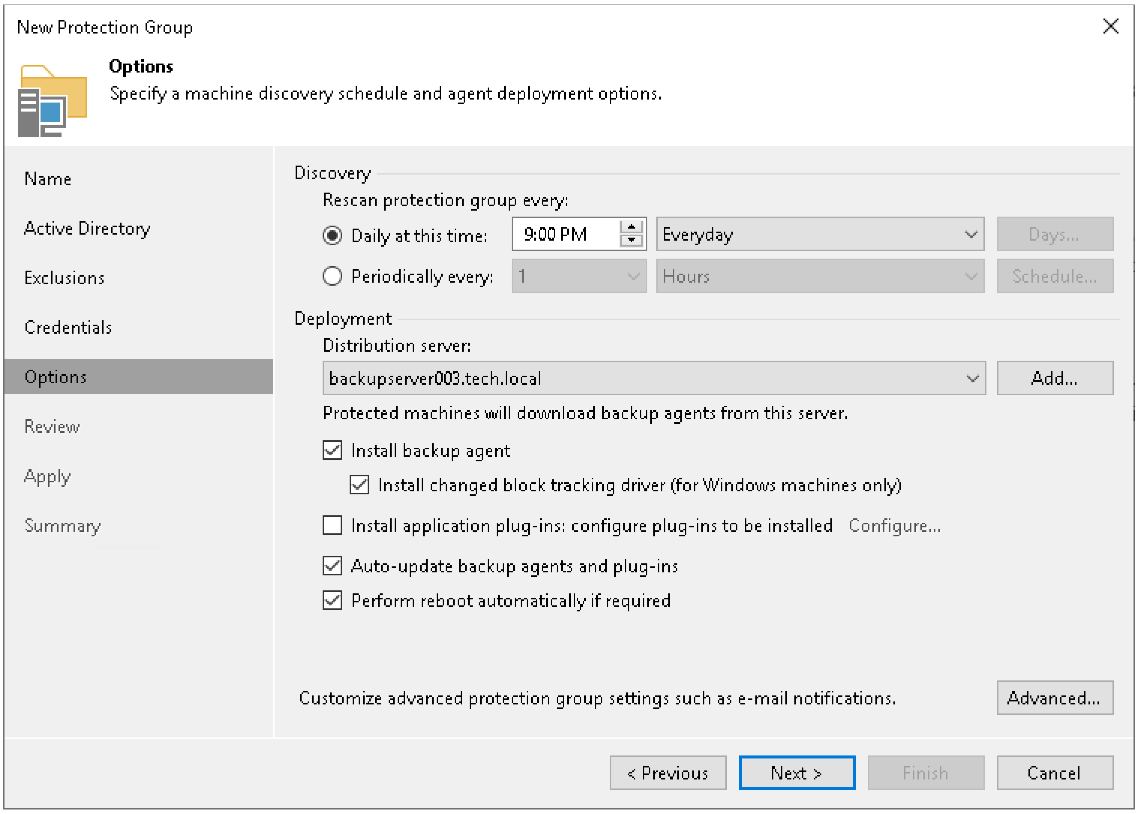
   b. In the inventory pane, expand the **Physical Infrastructure** node.

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**.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

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.



New Protection Group

Options

Specify a machine discovery schedule and agent deployment options.

Discovery

Rescan protection group every:

● Daily at this time: 9:00 PM Everyday

○ Periodically every: 1 Hours

Deployment

Distribution server: backupserver003.tech.local

Protected machines will download backup agents from this server.

☑ Install backup agent

☑ Install changed block tracking driver (for Windows machines only)

□ Install application plug-ins: configure plug-ins to be installed

☑ Auto-update backup agents and plug-ins

☑ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications.

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 Unix 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:

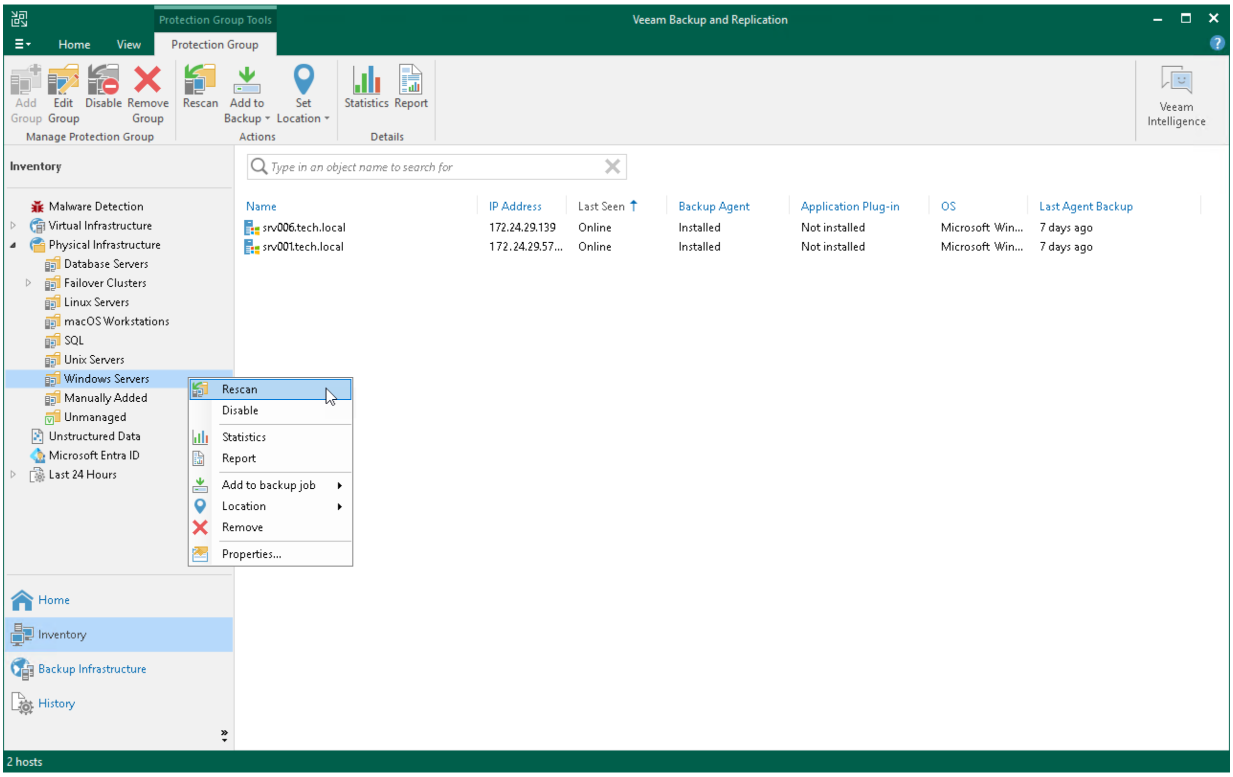
   ```
   C:\Program Files\Veeam\Veeam Distribution Service\Fixes\vaw\kb.<number>
   ```

   where `<number>` is a number of the hotfix provided by Veeam Customer Support.
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**.



Name	IP Address	Last Seen	Backup Agent	Application Plug-in	OS	Last Agent Backup
srv006.tech.local	172.24.29.139	Online	Installed	Not installed	Microsoft Win...	7 days ago
srv001.tech.local	172.24.29.57...	Online	Installed	Not installed	Microsoft Win...	7 days ago

Deployment Procedure for Linux Computers

Before You Begin

Hotfixes released by Veeam for Veeam Agent for Linux can contain updated packages for all or selected components of the Veeam Agent architecture:

- If the hotfix affects all Veeam Agent for Linux packages, follow the general procedure of deploying a hotfix for Veeam Agent for Linux. The general procedure instructions are further illustrated with Example 1.
- If the hotfix contains only an updated kernel module package, editing of the Veeam Agent for Linux package index file (Step 3 of the general procedure) is not required. The simplified procedure of hotfix deployment is illustrated in Example 2.

General Procedure for Deploying Hotfix on Linux Computers

To deploy a hotfix on Linux computers included in a protection group, perform the following steps:

1. Obtain the hotfix from Veeam Customer Support. To do this, open a support case.
2. Save Veeam Agent for Linux packages and their manifest files to the following folder on the Veeam backup server:

   For 32-bit RHEL / Oracle Linux

   ```
   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 Debian / Ubuntu

   ```
   C:\ProgramData\Veeam\Agents\val\x64\deb
   ```

3. Replace the names of the Veeam Agent for Linux packages in the index file:

   a. Open the `ValPackageIndex.xml` file that is located in the following folder on the Veeam backup server:

   ```
   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 information on deploying a hotfix for Veeam Agent for Linux version 6.0, see Example 1.

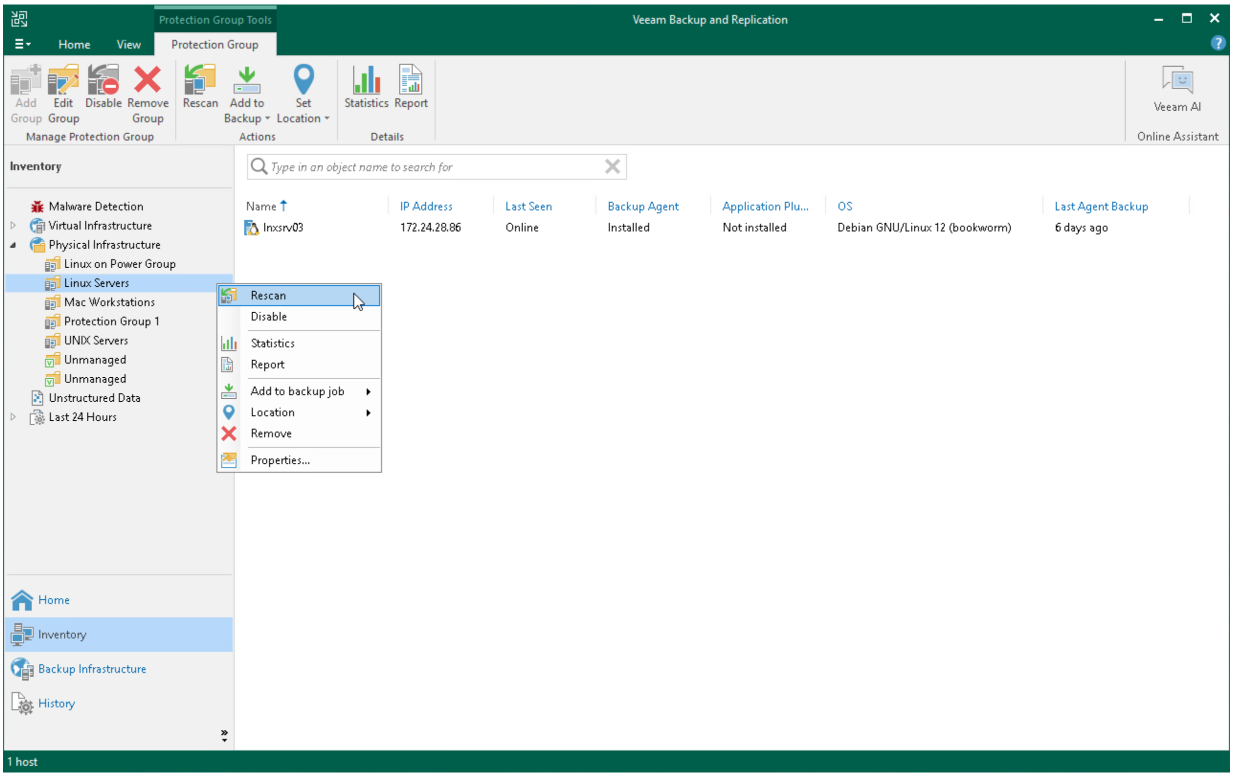
4. Rescan the protection group:

   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**.

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.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
lnxsrv03	172.24.28.86	Online	Installed	Not installed	Debian GNU/Linux 12 (bookworm)	6 days ago

Example 1: Deploying a Hotfix for Veeam Agent for Linux Using General Procedure

In this example, Veeam issued a hotfix for Veeam Agent for Linux 6.0 for 64-bit RHEL 9 and you want to deploy it on your Veeam Agent computers.

The hotfix consists of the following Veeam Agent packages:

- `blksnap-6.0.3.1228-1.noarch.rpm`
- `blksnap-6.0.3.1228-1.noarch.rpm.manifest.xml`
- `veeam-6.0.3.1228-1.el9.x86_64.rpm`
- `veeam-6.0.3.1228-1.el9.x86_64.rpm.manifest.xml`
- `kmod-blksnap-6.0.3.1228-1.el9.x86_64.rpm`
- `kmod-blksnap-6.0.3.1228-1.el9.x86_64.rpm.manifest.xml`

To deploy the hotfix, you need to do the following:

1. Obtain all updated Veeam Agent for Linux packages from Veeam Customer Support. To do this, open a support case.

2. Save the packages and their manifest files to the following folder on the Veeam backup server:

   ```
   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 Veeam backup server:

   ```
   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 in 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 6.0.3.1221 build version and the updated packages have the 6.0.3.1228 build version.

      In the example below, replaced package version and names are highlighted in green:

      ```
      ...
      <Distribution id="RHEL" displayName="Red Hat">
      ...
        <!-- EL9 -->
        <Version majorVersions="9">
           <Packages version="6.0.3.1228" arch="x64">
              <driver_noarch value="blksnap-6.0.3.1228-1.noarch.rpm"/>
              <driver_uefi_cert value="veeamsnap-ueficert-6.0.3.1221-1.noarch.rpm"/>
              <driver_bin value="kmod-blksnap-6.0.3.1228-1.el9.x86_64.rpm"/>
              <veeam value="veeam-6.0.3.1228-1.el9.x86_64.rpm"/>
           </Packages>
        </Version>
      </Distribution>
      ....
      ```

   c. Save changes and close the index file.

4. Rescan the protection group.

Example 2: Deploying a Hotfix for Veeam Agent for Linux Using Simplified Procedure

In this example, Veeam issued a hotfix for Veeam Agent for Linux 6.1 for 64-bit RHEL 9 and you want to deploy it on your Veeam Agent computers.

The hotfix consists of the following Veeam Agent packages:

- `kmod-blksnap-patch-6.1.0.1498-1.el9.x86_64.rpm`
- `kmod-blksnap-patch-6.1.0.1498-1.el9.x86_64.rpm.manifest.xml`

To deploy the hotfix, you need to do the following:

1. Obtain all updated Veeam Agent for Linux packages from Veeam Customer Support. To do this, open a support case.
2. Save the package and its manifest file to the following folder on the Veeam backup server:

   ```
   C:\ProgramData\Veeam\Agents\val\x64\rpm
   ```

3. Rescan the protection group.

Deployment Procedure for Unix Computers

You can add Unix-based servers with Veeam Agent for IBM AIX or Veeam Agent for Oracle Solaris installed to protection groups for individual computers.

To deploy a hotfix on Unix machines included in the protection group, perform the following steps:

1. Obtain a hotfix from Veeam Customer Support.
2. In the `C:\ProgramData\Veeam\Agents\vau` folder on the Veeam backup server, replace the original Veeam Agent for Unix package with the hotfix package.
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**.

   During rescan, Veeam Backup & Replication will update Veeam Agents on the protected machines.

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:

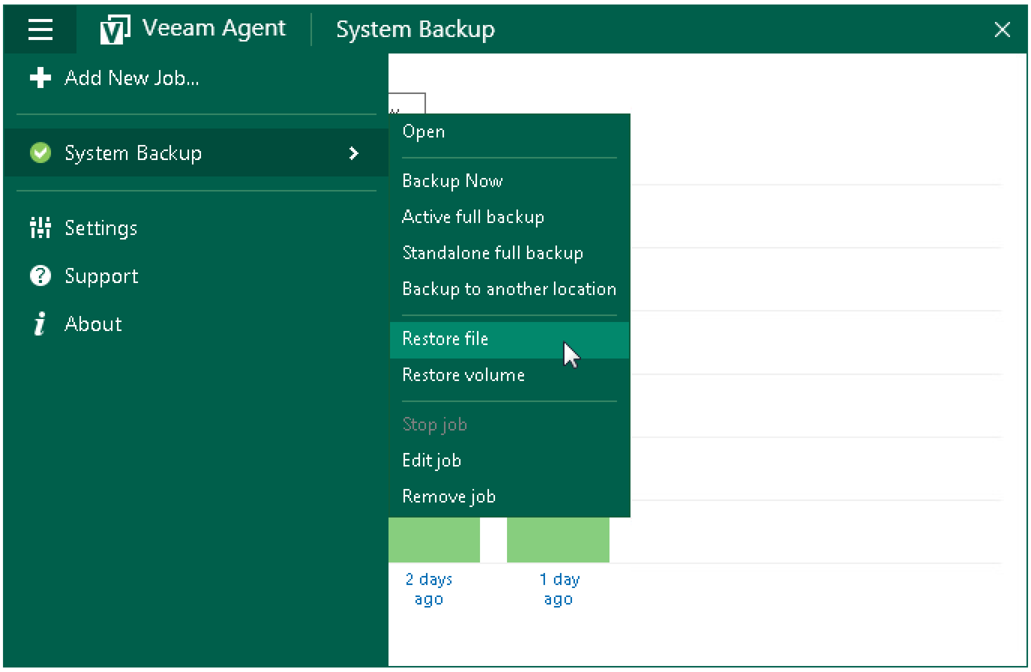
- Your Veeam Agent computer must be a member of a protection group for which file-level restore without Administrator privileges is allowed. To learn more, see Veeam Agent for Microsoft Windows Settings.
- You must restore from the backup created by a backup job managed by Veeam Agent. To learn more, see Working with Veeam Agent Backup Jobs and Policies.
- 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.

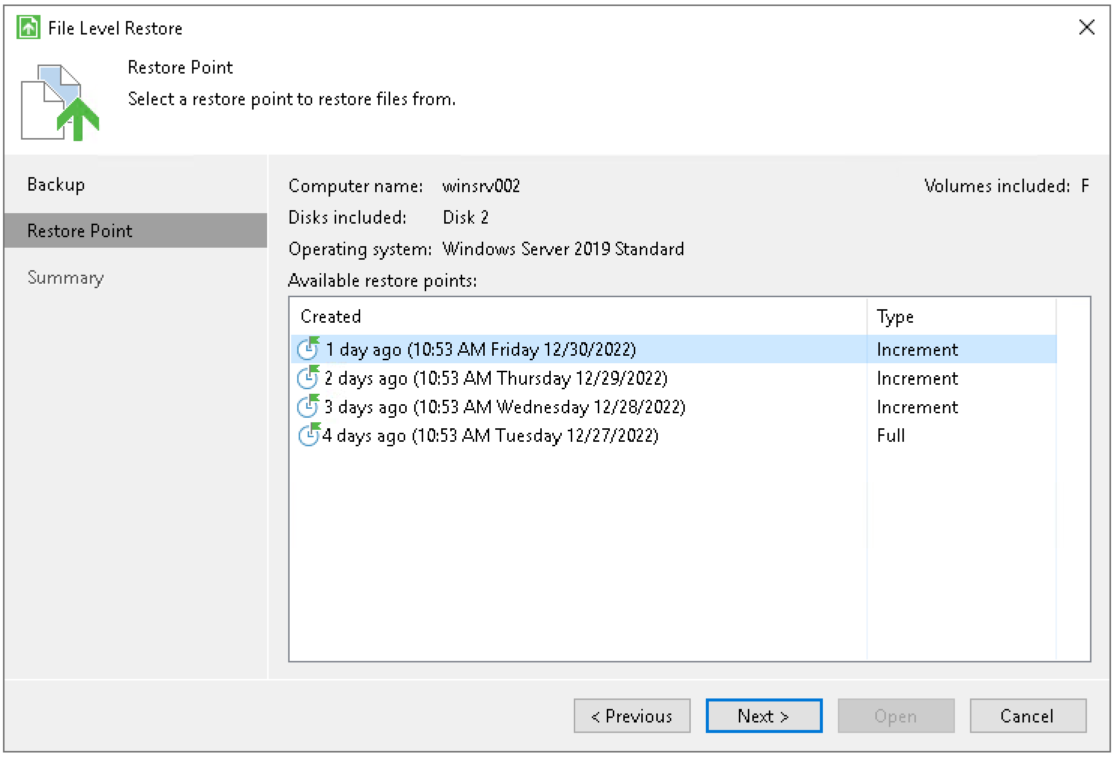
1. On the Veeam Agent computer, double-click the Veeam Agent for Microsoft Windows icon in the system tray, or right-click the icon in the system tray and select **Control Panel**.

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.

   Consider 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.



Computer name: winsrv002

Volumes included: F

Disks included: Disk 2

Operating system: Windows Server 2019 Standard

Available restore points:

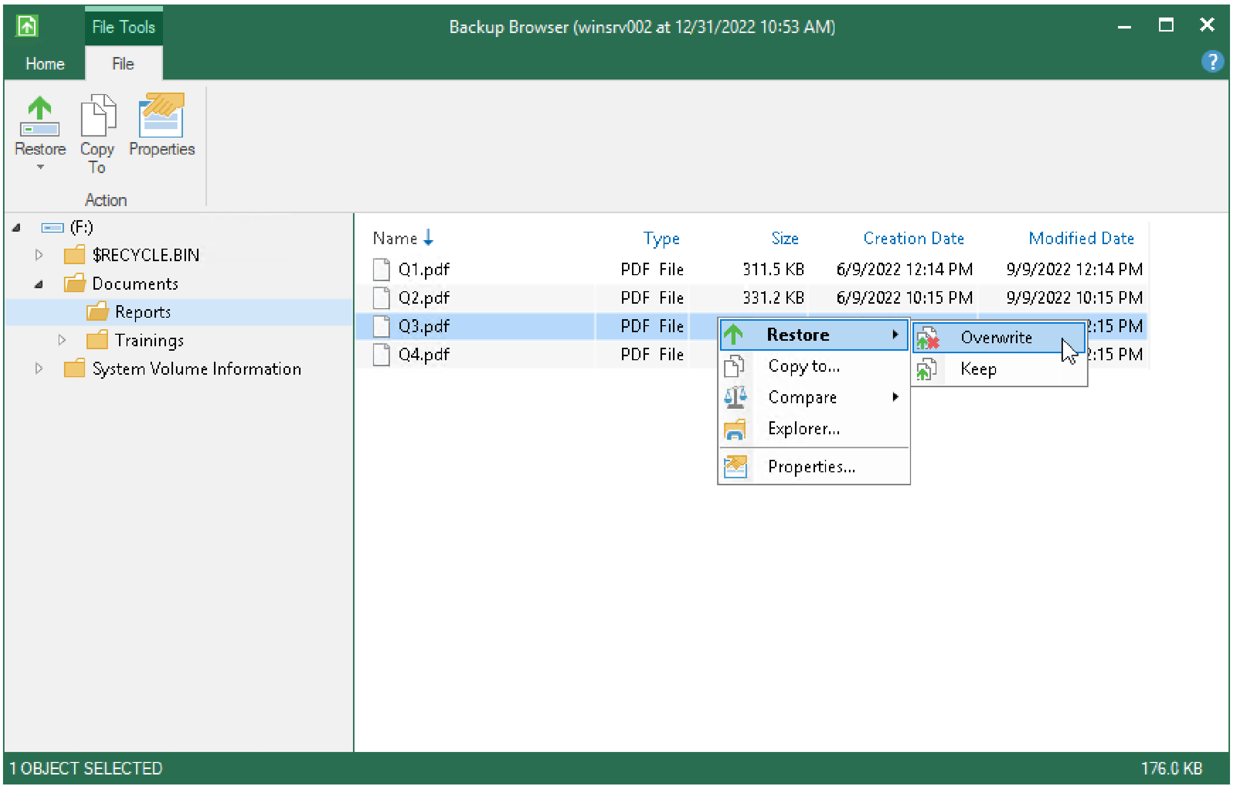
Created	Type
1 day ago (10:53 AM Friday 12/30/2022)	Increment
2 days ago (10:53 AM Thursday 12/29/2022)	Increment
3 days ago (10:53 AM Wednesday 12/28/2022)	Increment
4 days ago (10:53 AM Tuesday 12/27/2022)	Full

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.

   Consider 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.



Name	Type	Size	Creation Date	Modified Date
Q1.pdf	PDF File	311.5 KB	6/9/2022 12:14 PM	9/9/2022 12:14 PM
Q2.pdf	PDF File	331.2 KB	6/9/2022 10:15 PM	9/9/2022 10:15 PM
Q3.pdf	PDF File			:15 PM
Q4.pdf	PDF File			:15 PM

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 section 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 the How to Use Filters to Define File-Level Backup Scope section 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.

    To learn more about the FilesNotToSnapshot registry key, see this Microsoft article.

    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.

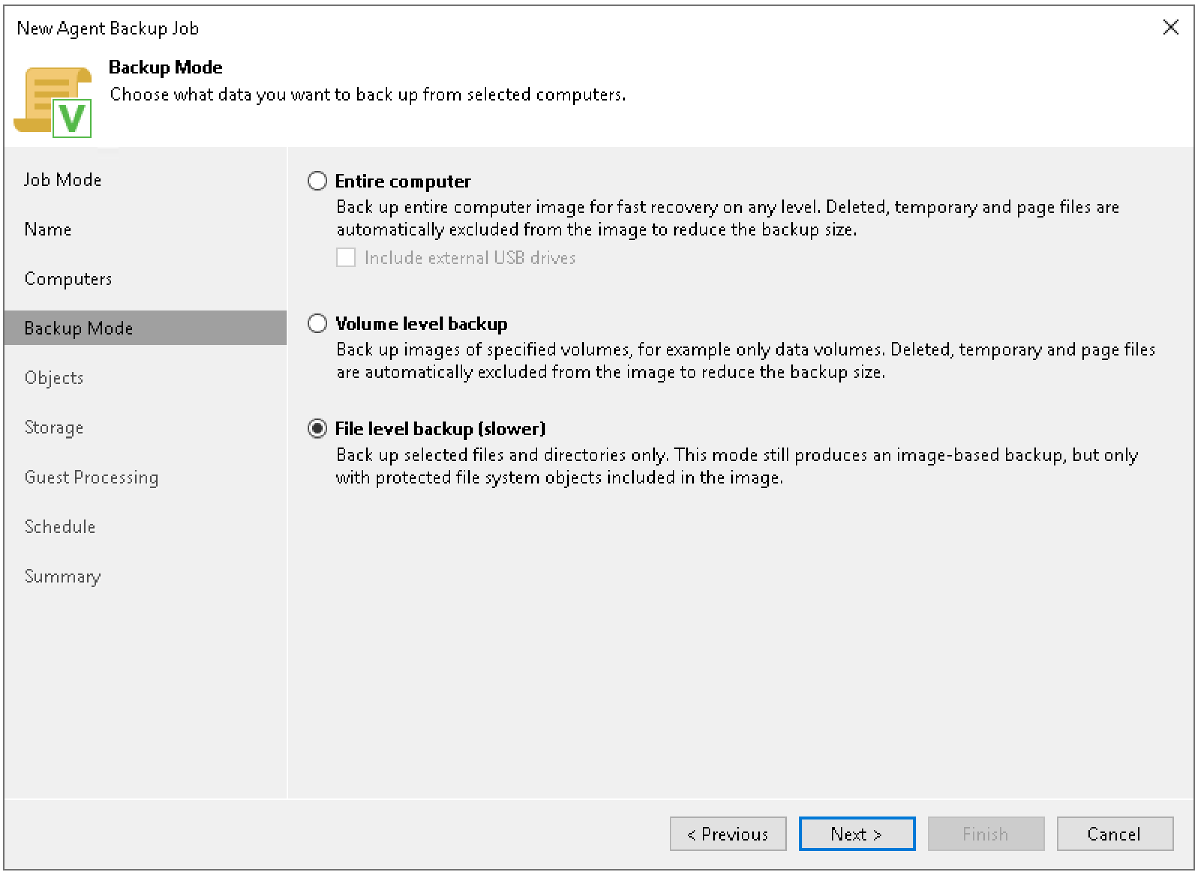
  - When you select an individual folder as an object of a file-level backup, Veeam Agent reads all data from the VSS snapshot first, then applies filters defined in the job configuration to save the data.

- 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.



New Agent Backup Job

Backup Mode

Choose what data you want to back up from selected computers.

○ **Entire computer**
Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
□ Include external USB drives

○ **Volume level backup**
Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

● **File level backup (slower)**
Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.

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:

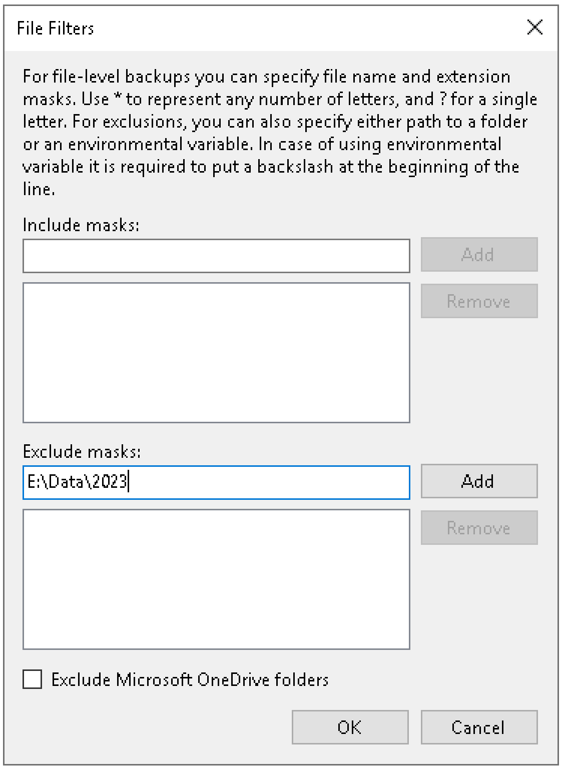
- Excluding a Folder Using Full Path.
- Excluding a Folder Using an Environment Variable in the Path.
- Excluding a Folder Using a Wildcard Character in the Path.
- Including or Excluding Specific Files.

- 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\2023` folder from the backup scope.

1. In the **Exclude masks** field, enter the full path to the folder — *E:|Data|2023*.



File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks:

Exclude masks: E:\Data\2023

□ Exclude Microsoft OneDrive folders

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\2023` folder.

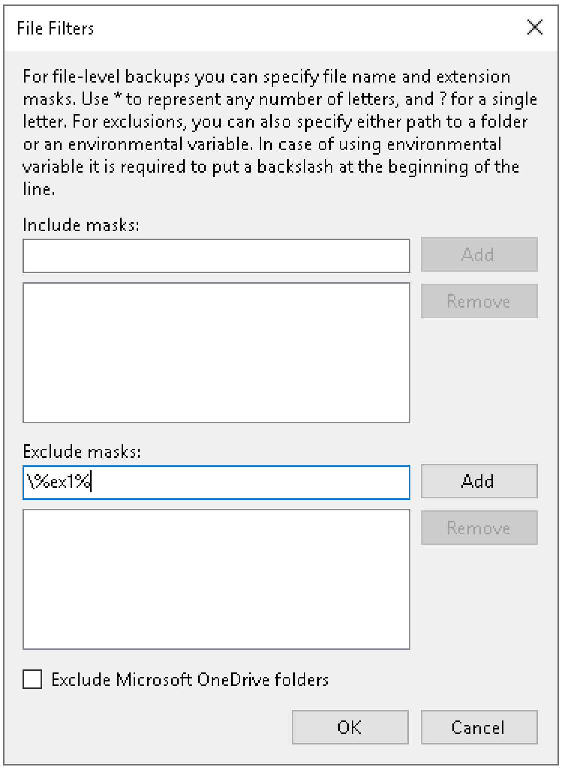
Excluding a Folder Using an Environment Variable in the Path

You can exclude a folder by specifying a system environment variable in its path. In this example, we will exclude the `E:\Data\2023\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.


File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks:

Exclude masks: \%ex1%

□ Exclude Microsoft OneDrive folders

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\2023\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

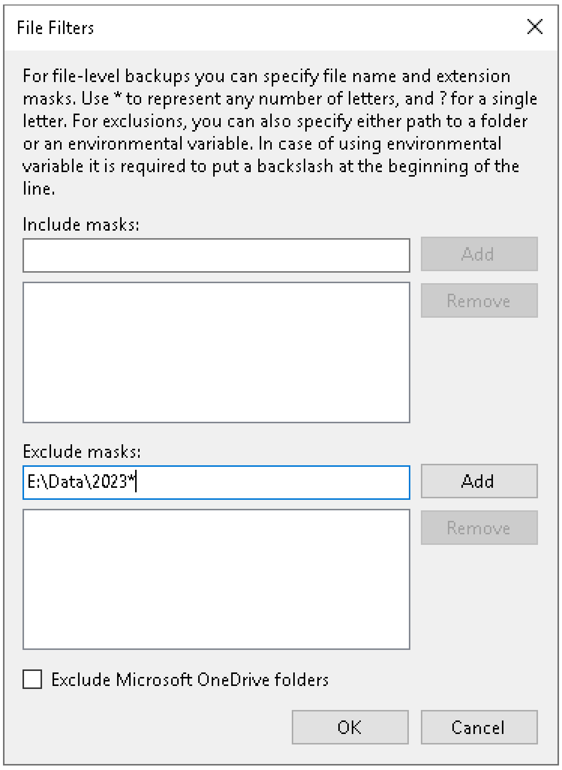
To exclude a folder from the backup, you can specify a partial path with a wildcard at the end.

NOTE

Note that you cannot use a wildcard in the middle of the path. For example, specifying _E:|*|2023_ 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.

In this example, we will exclude all subfolders of the `E:\Data` folder whose names begin with `2023`. To do this:

1. In the **Exclude masks** field, enter _E:\Data\2023*_.



File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks:

Exclude masks: E:\Data\2023*

☐ Exclude Microsoft OneDrive folders

2. Click **Add**.

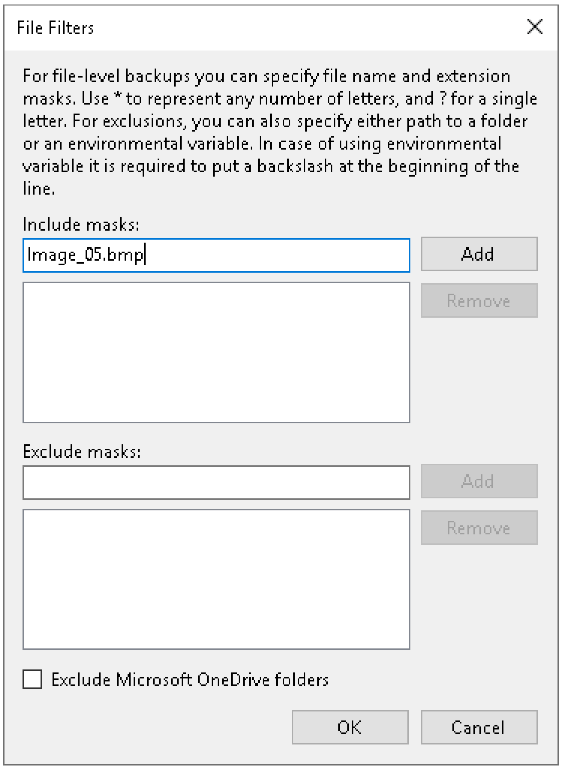
3. Click **OK** to complete the configuration.

As a result, the backup will contain all data from the backup scope except the folders whose names start with `2023` — for example `2023_Jan` or `2023_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*:



File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks: Image_05.bmp

Exclude masks:

□ Exclude Microsoft OneDrive folders

2. Click **Add**.
3. Click **OK** to complete the configuration.

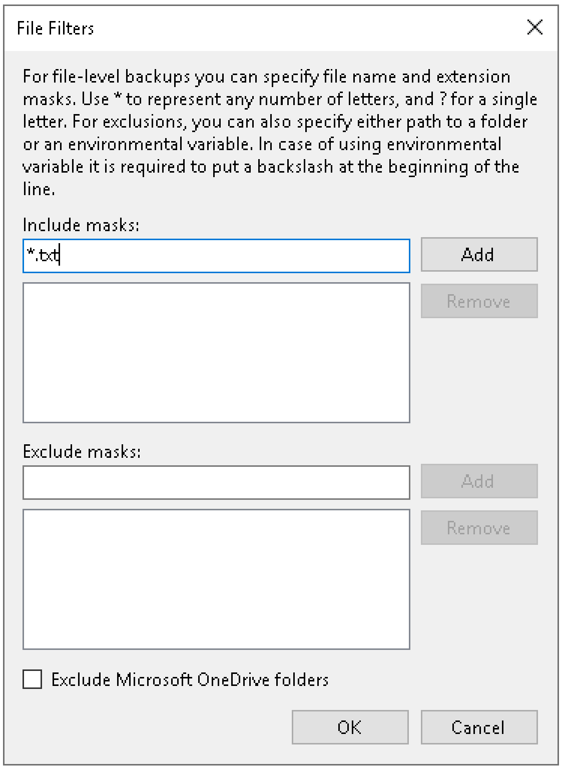
As a result, the backup will contain only the `Image_05.bmp` file from the specified backup scope.

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.



File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks: *.txt

Exclude masks:

□ Exclude Microsoft OneDrive folders

2. Click **Add**.

3. Click **OK** to complete the configuration.

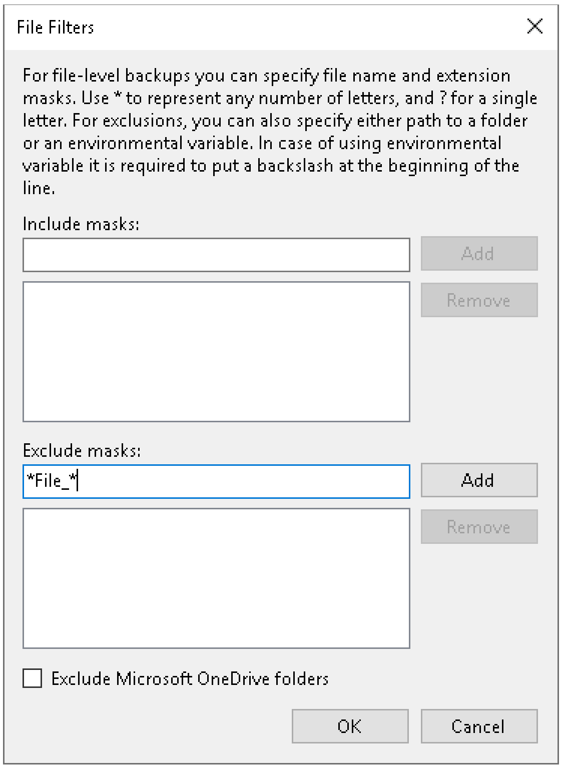
As a result, the backup will contain all the text files in the .txt format from the backup scope.

> **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_**.



File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks:

Exclude masks: *File_*

□ Exclude Microsoft OneDrive folders

This will select all files that contain this sequence of characters in any position in the file name.

5. Click **Add**.

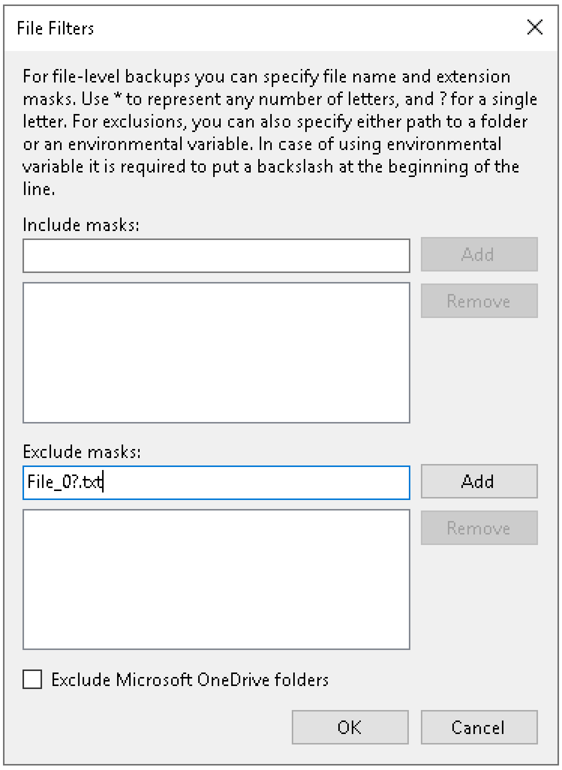
6. Click **OK** to complete the configuration.

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*.



File Filters

For file-level backups you can specify file name and extension masks. Use * to represent any number of letters, and ? for a single letter. For exclusions, you can also specify either path to a folder or an environmental variable. In case of using environmental variable it is required to put a backslash at the beginning of the line.

Include masks:

Exclude masks: File_0?.txt

□ Exclude Microsoft OneDrive folders

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`.

Deploying Settings to Veeam Agent Computers

If you want to automate application of Veeam Agent settings to protected computers, you can use the Veeam Backup PowerShell module. For more information about the module, see the Veeam PowerShell Reference.

> IMPORTANT
>
> Make sure that you have tested the cmdlets described in this section in a test lab before their execution in the production environment. Operations performed with these cmdlets can cause data loss, and you will not be able to undo changes.

Deploying Settings

To deploy settings to managed computers, perform the following steps:

1. Start a Veeam PowerShell session. For more information, see the Starting Veeam PowerShell Sessions in the Veeam PowerShell Reference.
2. Create a new configuration option for Veeam Agent settings using the `New-VBRDiscoveredComputerConfigurationOption` cmdlet. For more information, see the New-VBRDiscoveredComputerConfigurationOption section in the Veeam PowerShell Reference.
3. Add the created configuration option to a configuration policy and assign the configuration policy to a protected computer or a protection group using the `Add-VBRDiscoveredComputerConfigurationPolicy` cmdlet. For more information, see the Add-VBRDiscoveredComputerConfigurationPolicy section in the Veeam PowerShell Reference.
4. Rescan the protected computer or the protection group to apply new settings. For more information, see Rescanning Protected Computer or Rescanning Protection Group.

Checking Current Settings

To check what settings are applied to managed computers, use the `Get-VBRDiscoveredComputerConfigurationPolicy` cmdlet. For more information, see the Get-VBRDiscoveredComputerConfigurationPolicy section in the Veeam PowerShell Reference.

Deleting Settings

To delete a configuration policy that contains a configuration option for Veeam Agent settings, use the the `Remove-VBRDiscoveredComputerConfigurationPolicy` cmdlet. For more information, see the Remove-VBRDiscoveredComputerConfigurationPolicy section in the Veeam PowerShell Reference.

IMPORTANT

Consider the following:

- Before you apply other settings to Veeam Agent computers, make sure to delete the currently applied configuration policy with the `Remove-VBRDiscoveredComputerConfigurationPolicy` cmdlet. Otherwise, the policy settings will be reapplied after the rescan of the protected computer or protection group.
- The removal of the configuration policy does not update settings on Veeam Agent computers to which the policy has been applied. If you want to update the settings, you must create a new policy and assign it to discovered computers using the `Add-VBRDiscoveredComputerConfigurationPolicy` cmdlet. For more information, see the Add-VBRDiscoveredComputerConfigurationPolicy section in the Veeam PowerShell Reference.

How to Protect Failover Clusters

Veeam Backup & Replication lets you deploy and manage Veeam Agent for Microsoft Windows on failover clusters in your infrastructure.

This scenario describes how you can use Veeam Agent to protect failover clusters. For example, Windows File Server Failover Clusters. For the full list of failover cluster types that you can back up with Veeam Agent, see Failover Cluster Support.

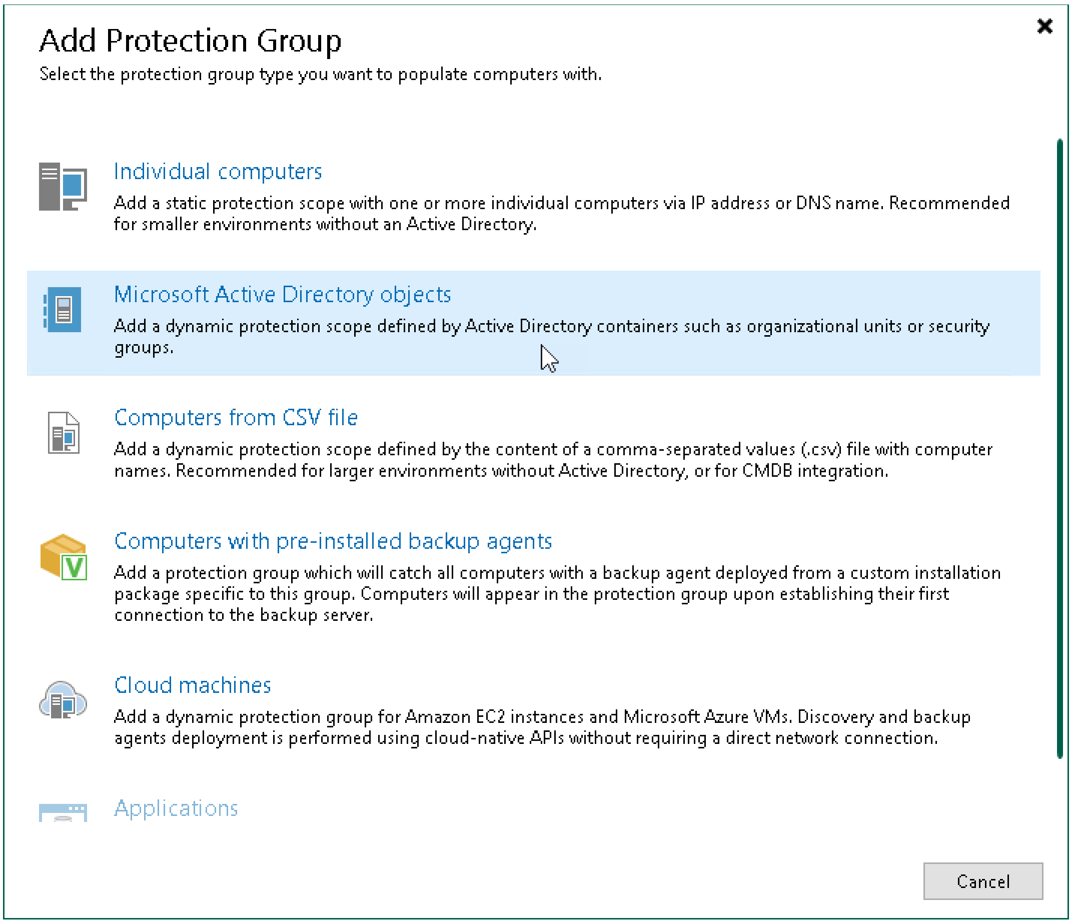
> NOTE
>
> If you want to back up a a Microsoft Exchange Database Availability Group without an Administrative Access Point (IP Less DAG), follow backup job configuration procedure for standalone servers. To learn more, see Backup of Database Availability Groups.

In this scenario, you will:

1. Create a failover cluster protection group.
2. Create a failover cluster backup job.

To create a protection group to backup failover clusters:

1. Launch the **New Protection Group** wizard. Select the **Microsoft Active Directory objects** protection group type.



Add Protection Group

Select the protection group type you want to populate computers with.

Individual computers

Add a static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

Microsoft Active Directory objects

Add a dynamic protection scope defined by Active Directory containers such as organizational units or security groups.

Computers from CSV file

Add a dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names. Recommended for larger environments without Active Directory, or for CMDB integration.

Computers with pre-installed backup agents

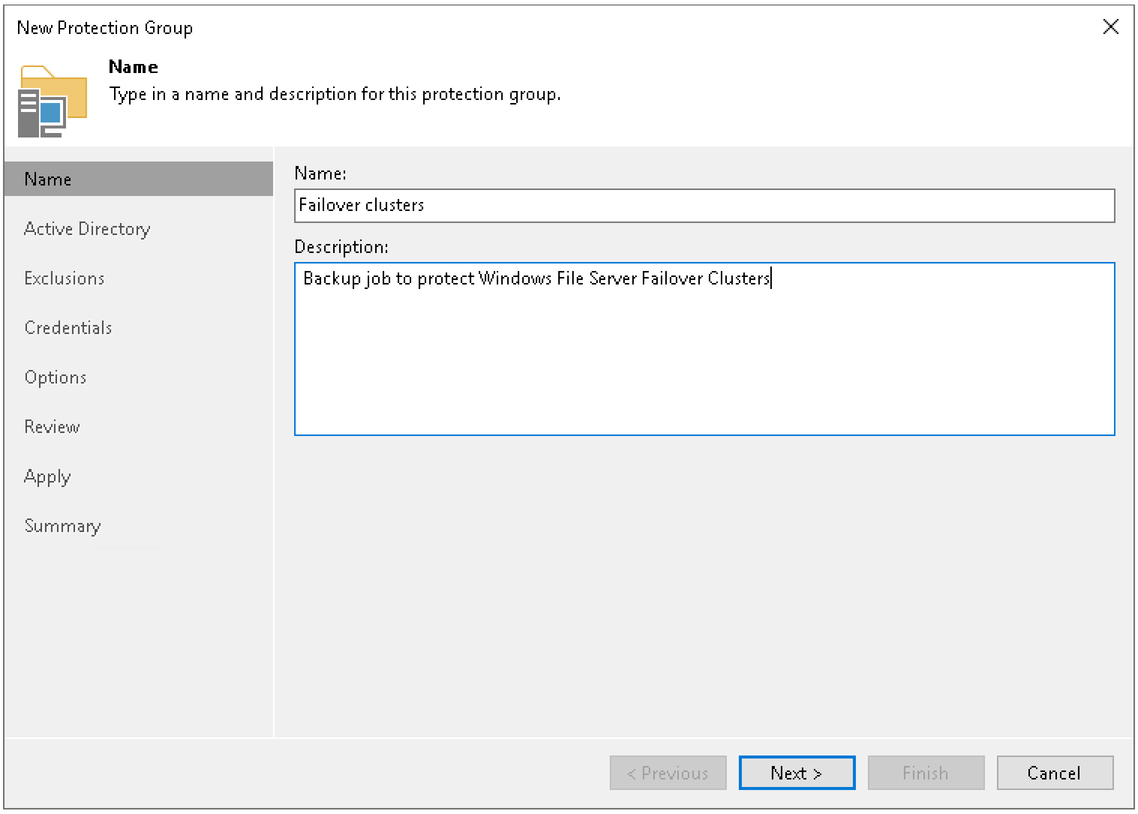
Add a protection group which will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

Cloud machines

Add a dynamic protection group for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

Applications

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



New Protection Group

Name

Type in a name and description for this protection group.

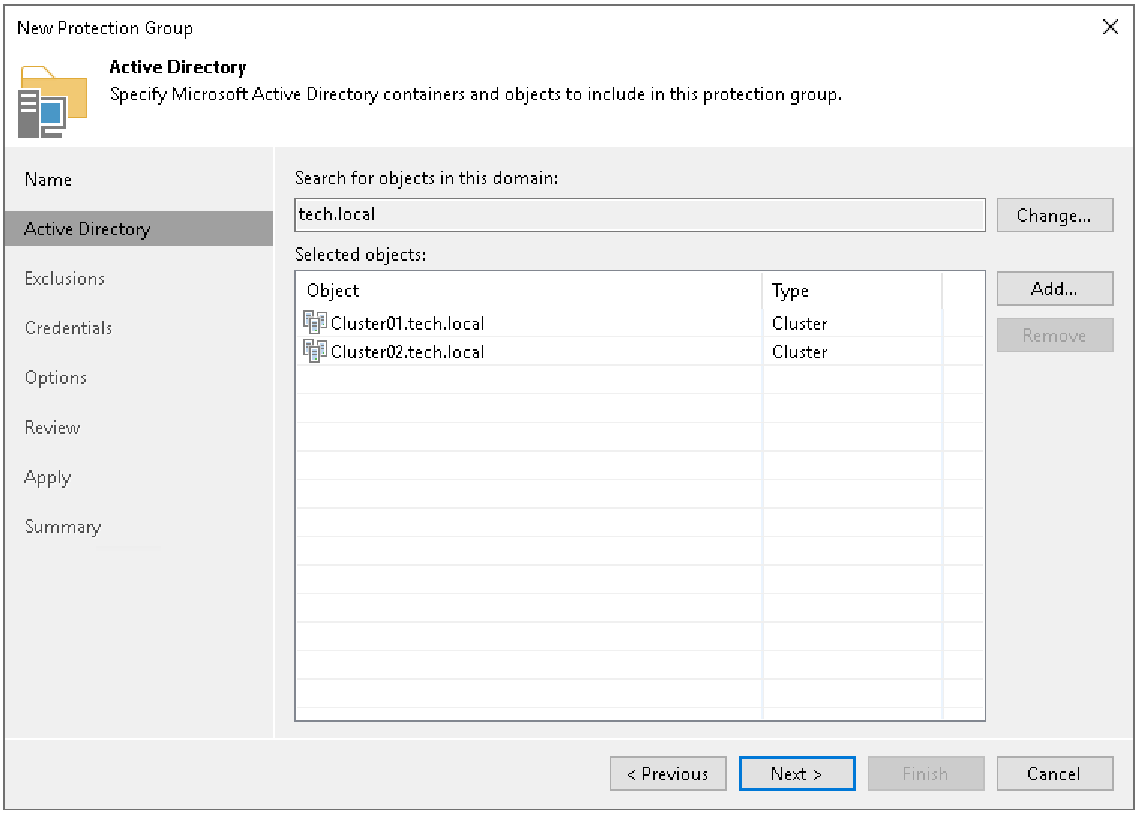
Name:

Failover clusters

Description:

Backup job to protect Windows File Server Failover Clusters

3. At the **Active Directory** step of the wizard, select failover clusters that you want to add to the protection group. Click **Next**.



New Protection Group

Active Directory

Specify Microsoft Active Directory containers and objects to include in this protection group.

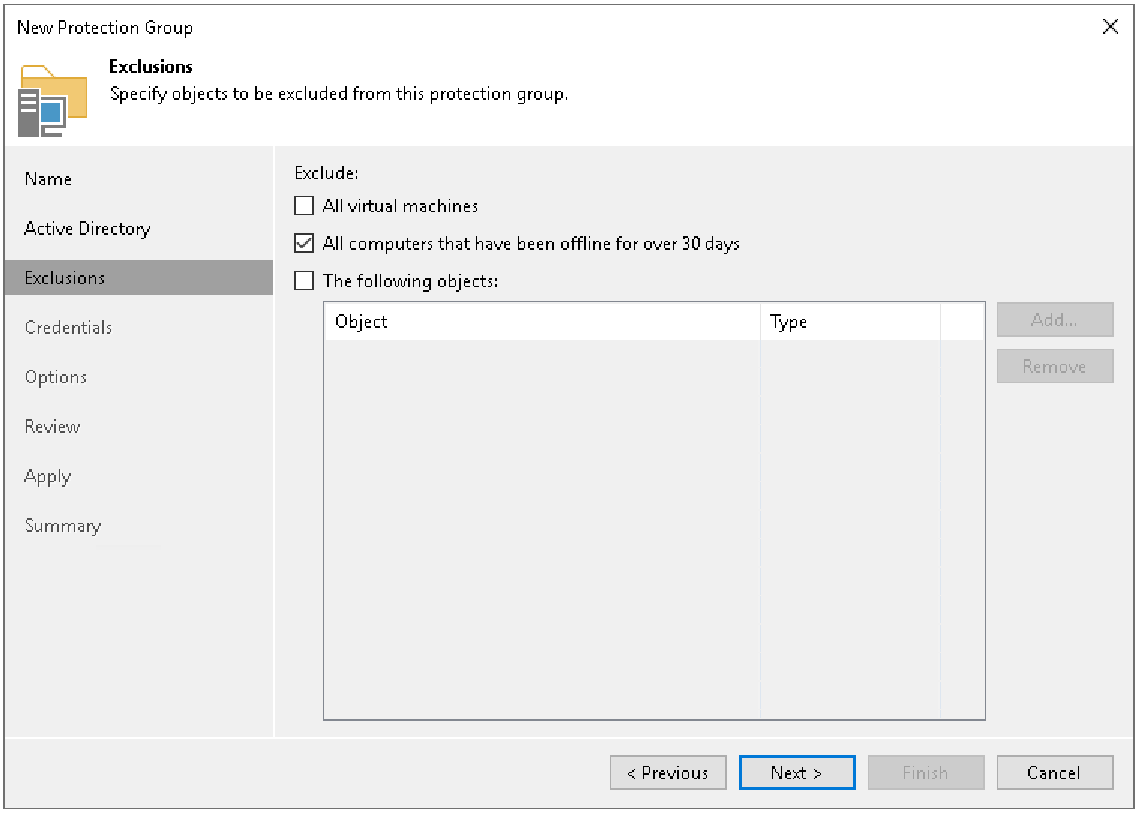
Search for objects in this domain:

tech.local

Selected objects:

Object	Type
Cluster01.tech.local	Cluster
Cluster02.tech.local	Cluster

4. At the **Exclusions** step of the wizard, make sure that none of the required hosts are excluded. Click **Next**.



New Protection Group

Exclusions

Specify objects to be excluded from this protection group.

Exclude:

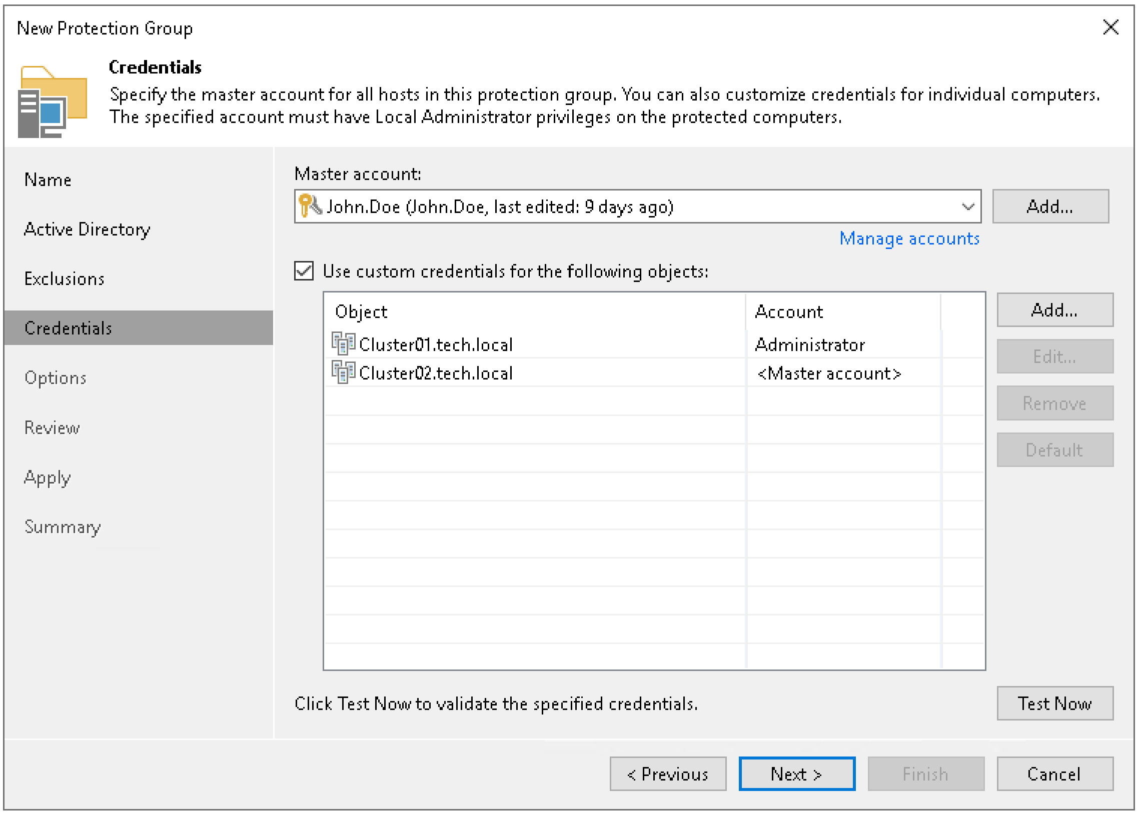
☐ All virtual machines

☑ All computers that have been offline for over 30 days

☐ The following objects:

Object	Type

5. At the **Credentials** step of the wizard, specify credentials to connect to each failover cluster. If you want to use the same credentials for all failover clusters, select the necessary user account from the **Master account** list. If some failover clusters require a different user account, specify custom credentials. Click **Next**.



New Protection Group

Credentials

Specify the master account for all hosts in this protection group. You can also customize credentials for individual computers. The specified account must have Local Administrator privileges on the protected computers.

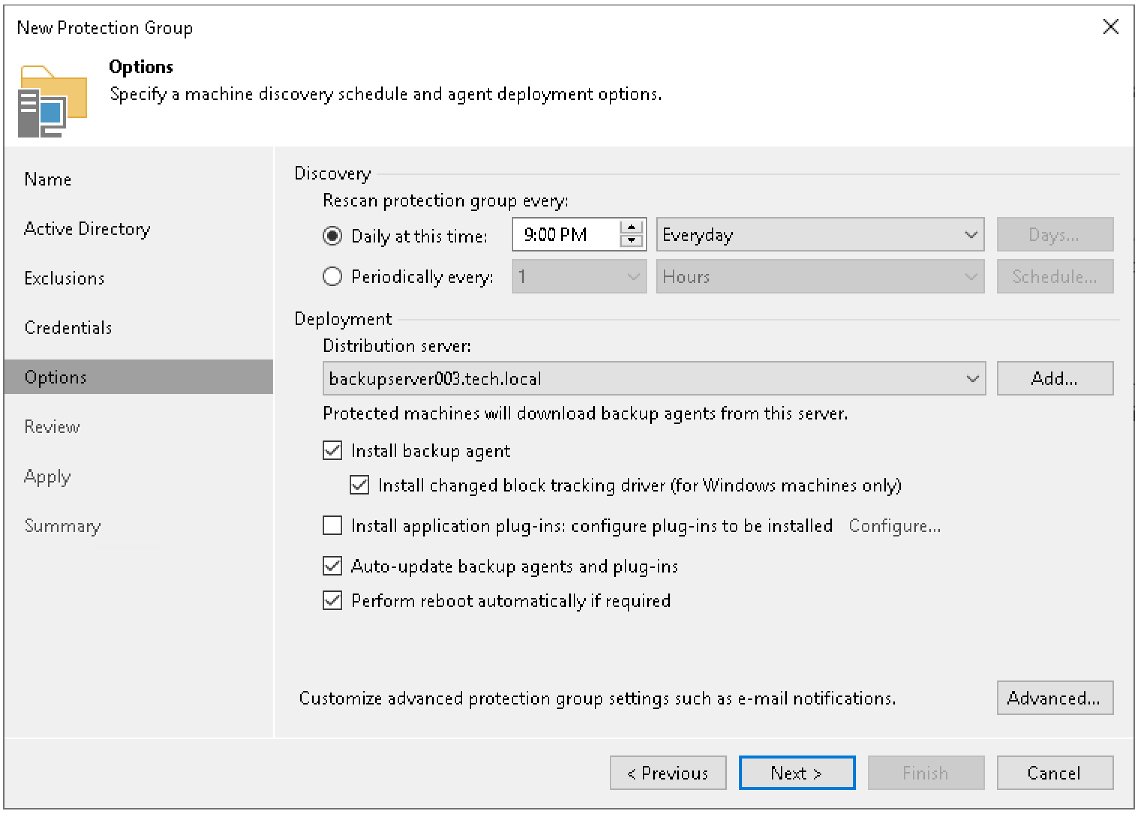
Master account: John.Doe (John.Doe, last edited: 9 days ago)

☑ Use custom credentials for the following objects:

Object	Account
Cluster01.tech.local	Administrator
Cluster02.tech.local	<Master account>

Click Test Now to validate the specified credentials.

6. At the **Options** step of the wizard, specify settings for discovery and Veeam Agent deployment. Click **Next**.



Discovery

Rescan protection group every:

● Daily at this time: 9:00 PM Everyday Days...

○ Periodically every: 1 Hours Schedule...

Deployment

Distribution server:

backupserver003.tech.local Add...

Protected machines will download backup agents from this server.

☑ Install backup agent

☑ Install changed block tracking driver (for Windows machines only)

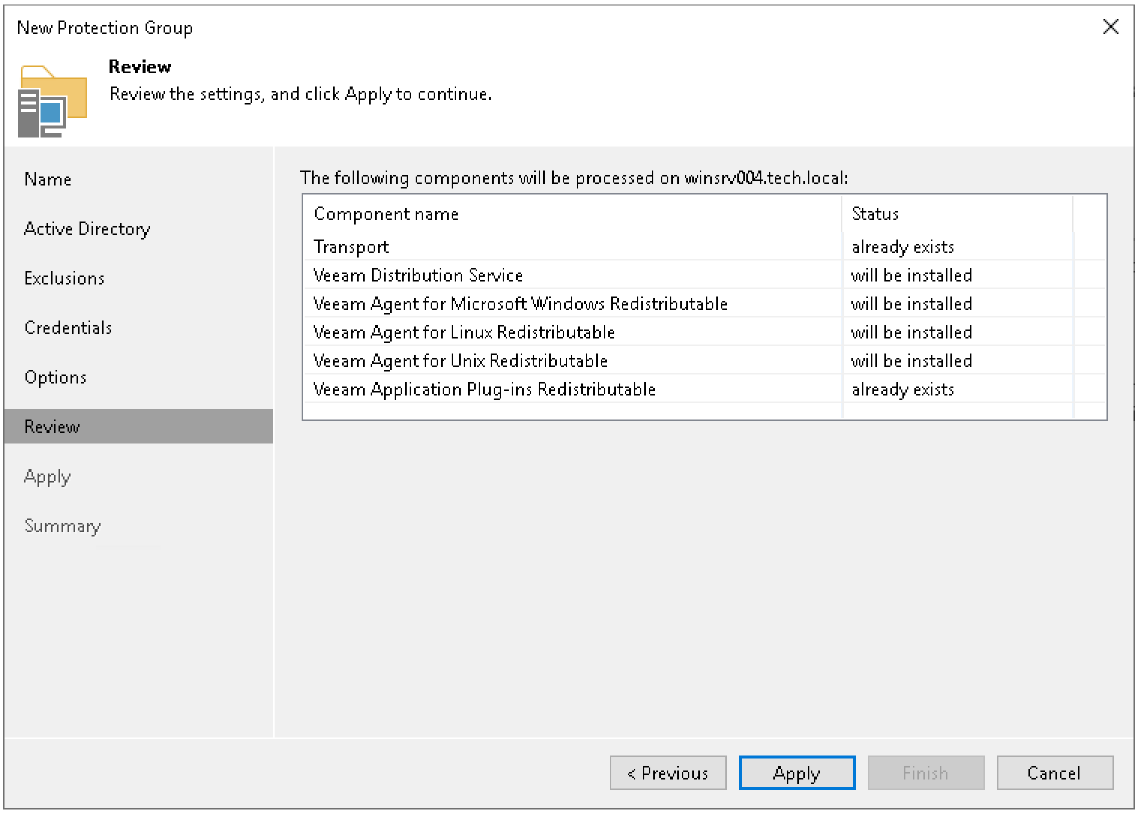
□ Install application plug-ins: configure plug-ins to be installed Configure...

☑ Auto-update backup agents and plug-ins

☑ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications. Advanced...

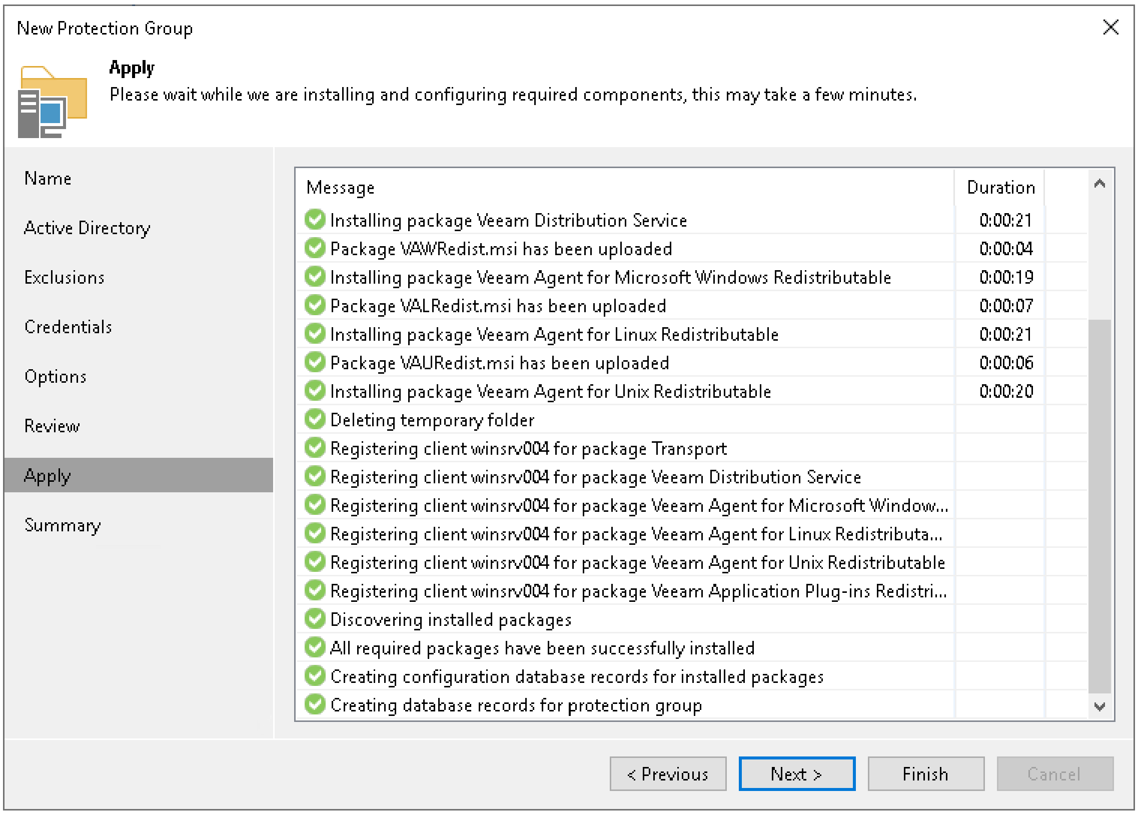
7. At the **Review** step of the wizard, review what Veeam Backup & Replication components are already installed on the distribution server specified for the protection group and what components will be installed. Click **Apply** to add the configured protection group to the inventory.



The following components will be processed on winsrv004.tech.local:

Component name	Status
Transport	already exists
Veeam Distribution Service	will be installed
Veeam Agent for Microsoft Windows Redistributable	will be installed
Veeam Agent for Linux Redistributable	will be installed
Veeam Agent for Unix Redistributable	will be installed
Veeam Application Plug-ins Redistributable	already exists

8. At the **Apply** step of the wizard, wait for the operation of the protection group creation to complete. Click **Next**.

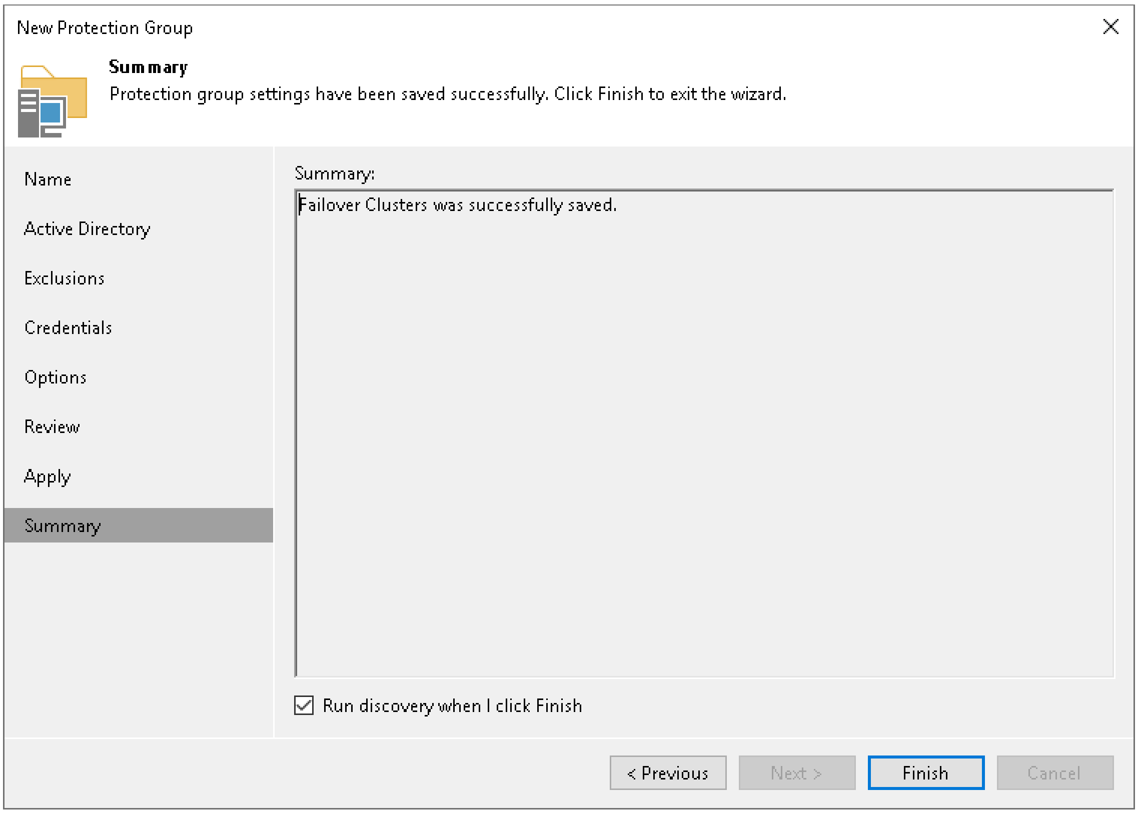

New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

Message	Duration
✓ Installing package Veeam Distribution Service	0:00:21
✓ Package VAWRedist.msi has been uploaded	0:00:04
✓ Installing package Veeam Agent for Microsoft Windows Redistributable	0:00:19
✓ Package VALRedist.msi has been uploaded	0:00:07
✓ Installing package Veeam Agent for Linux Redistributable	0:00:21
✓ Package VAURedist.msi has been uploaded	0:00:06
✓ Installing package Veeam Agent for Unix Redistributable	0:00:20
✓ Deleting temporary folder	
✓ Registering client winsrv004 for package Transport	
✓ Registering client winsrv004 for package Veeam Distribution Service	
✓ Registering client winsrv004 for package Veeam Agent for Microsoft Window...	
✓ Registering client winsrv004 for package Veeam Agent for Linux Redistributa...	
✓ Registering client winsrv004 for package Veeam Agent for Unix Redistributable	
✓ Registering client winsrv004 for package Veeam Application Plug-ins Redistri...	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating configuration database records for installed packages	
✓ Creating database records for protection group	

9. At the **Summary** step of the wizard, review information about the created protection group. Click **Finish** to close the wizard.


New Protection Group

Summary

Protection group settings have been saved successfully. Click Finish to exit the wizard.

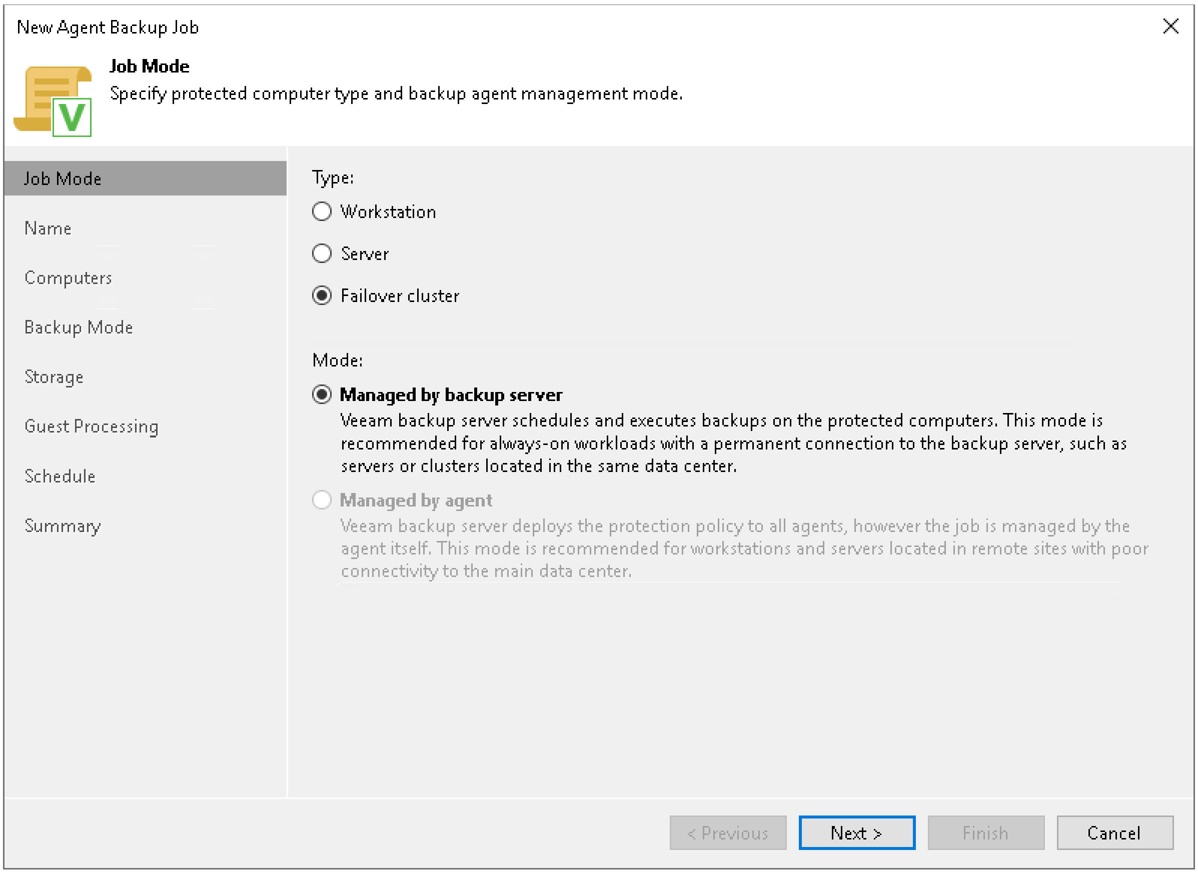
Summary:

Failover Clusters was successfully saved.

☑ Run discovery when I click Finish

To create a failover cluster backup job:

1. Select **Backup Job** > **Windows computer** to launch the **New Agent Backup Job** wizard.
2. At the **Job Mode** step of the wizard, in the **Type** field select **Failover Cluster**. Click **Next**.



New Agent Backup Job

Job Mode

Specify protected computer type and backup agent management mode.

Type:

○ Workstation

○ Server

● Failover cluster

Mode:

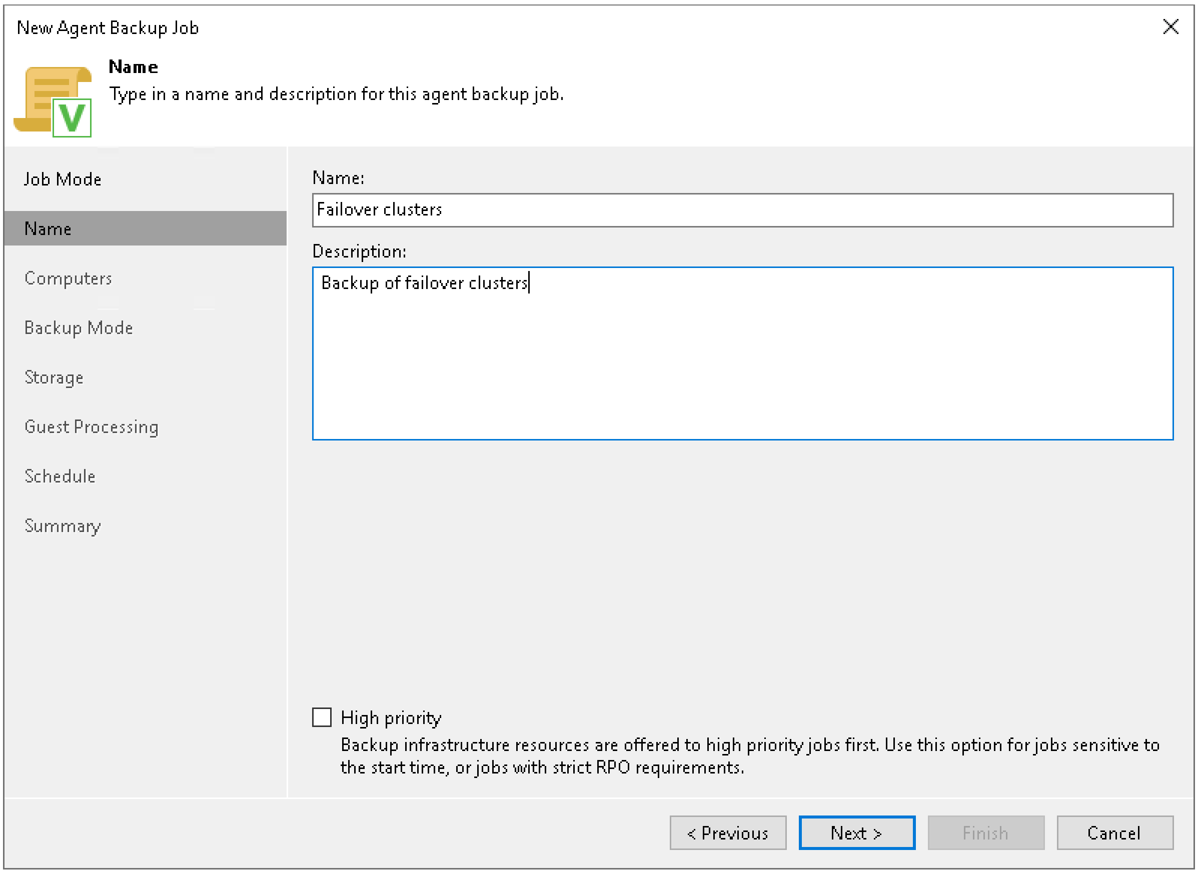
● **Managed by backup server**

Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

○ **Managed by agent**

Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

3. At the **Name** step of the wizard, specify a name and description for the backup job. Click **Next**.



New Agent Backup Job

Name

Type in a name and description for this agent backup job.

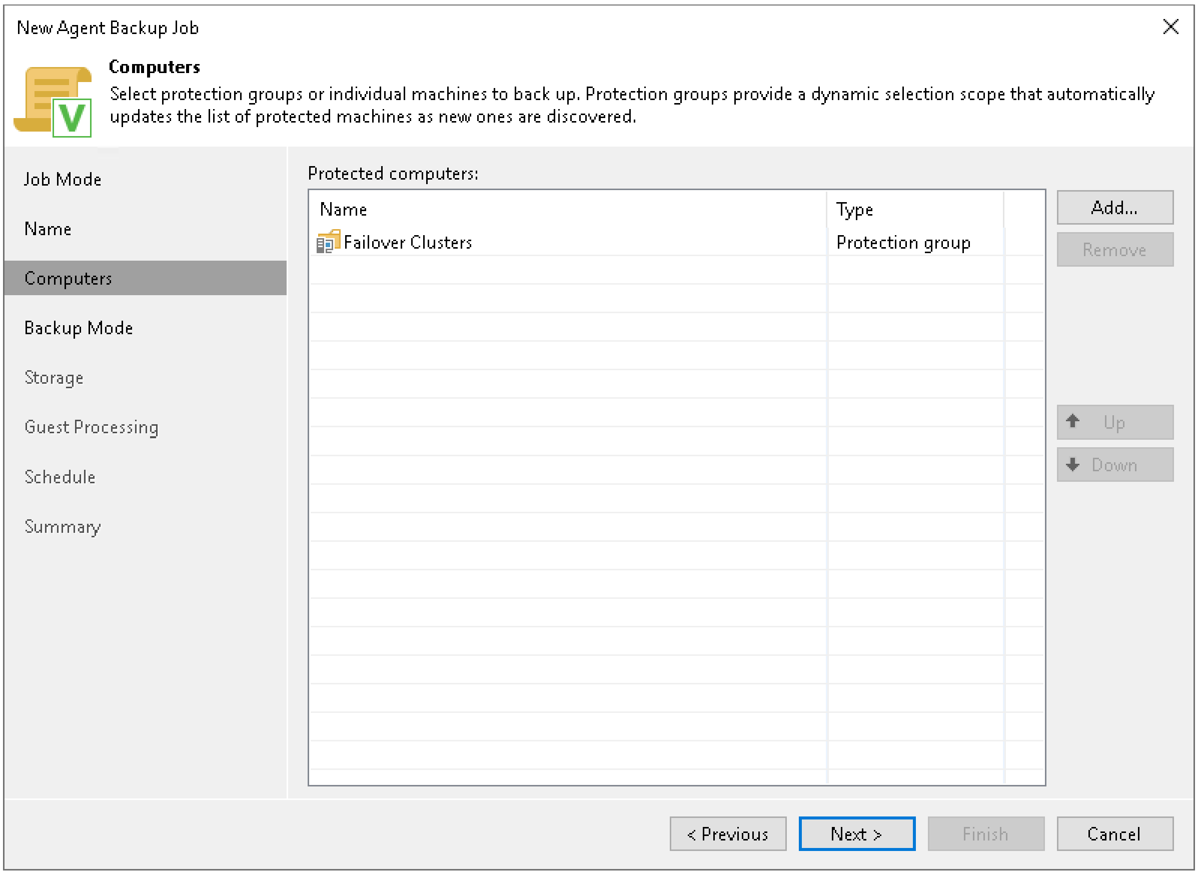
Name: Failover clusters

Description: Backup of failover clusters

□ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

4. At the **Computers** step of the wizard, select a protection group that contains failover clusters. Click **Next**.



New Agent Backup Job

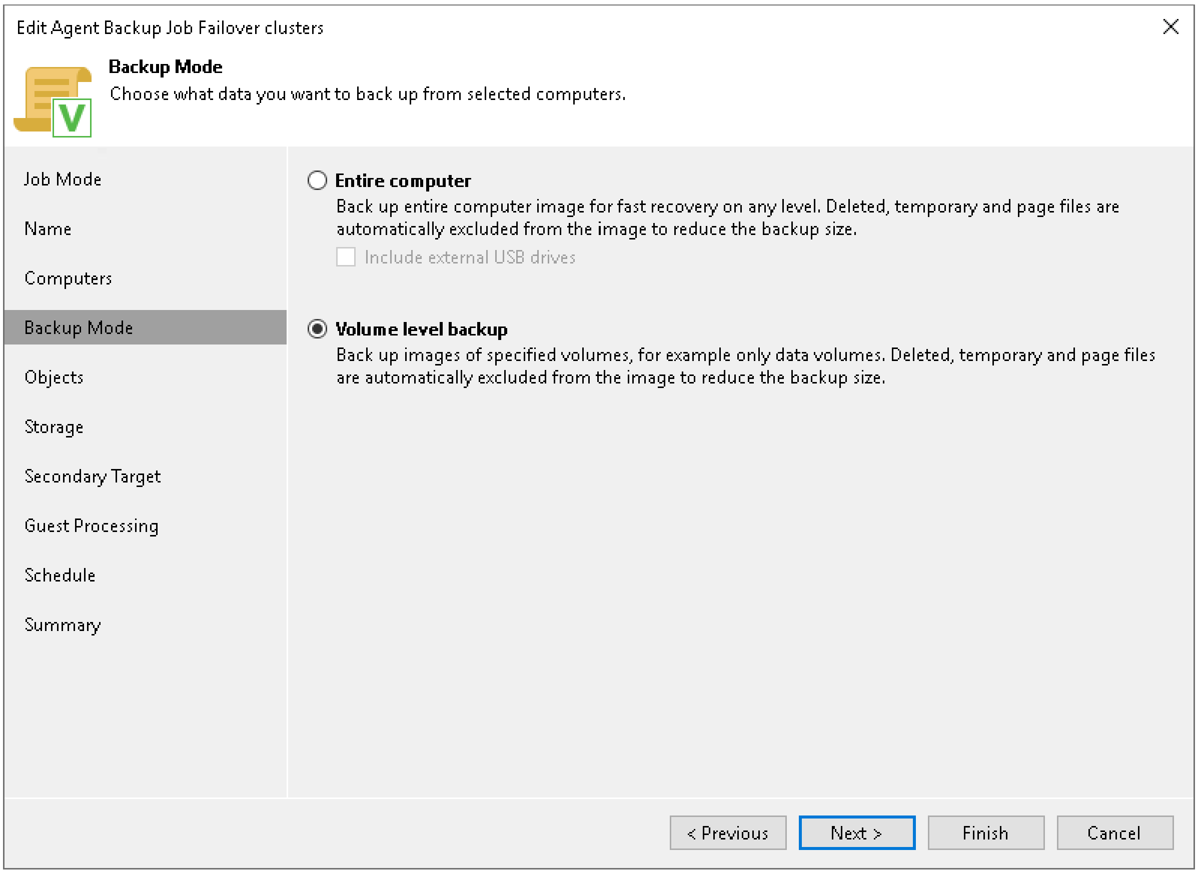
Computers

Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

Protected computers:

Name	Type
Failover Clusters	Protection group

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



Edit Agent Backup Job Failover clusters

Backup Mode

Choose what data you want to back up from selected computers.

○ **Entire computer**

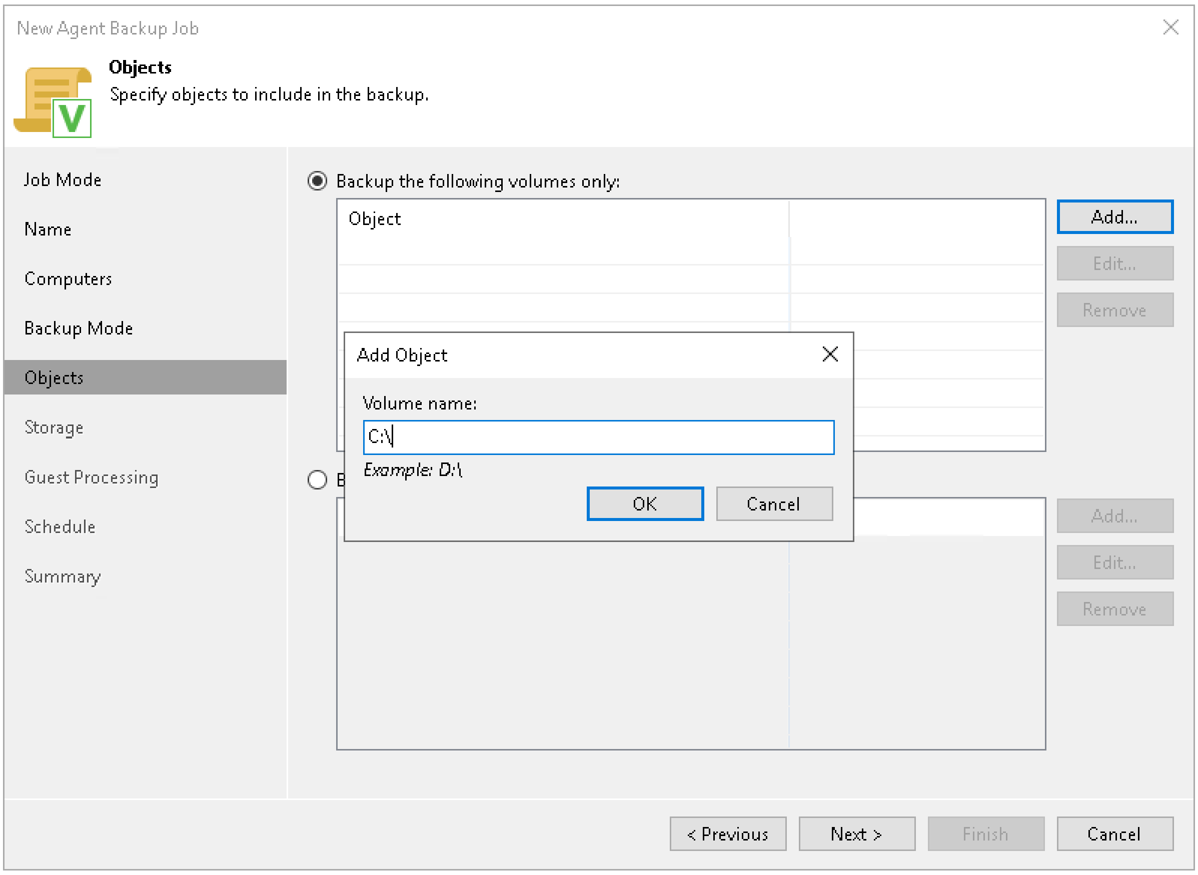
Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

□ Include external USB drives

● **Volume level backup**

Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

6. [For volume-level backup] At the **Objects** step of the wizard, specify volumes you want to include in the backup. Click **Next**.



New Agent Backup Job

Objects

Specify objects to include in the backup.

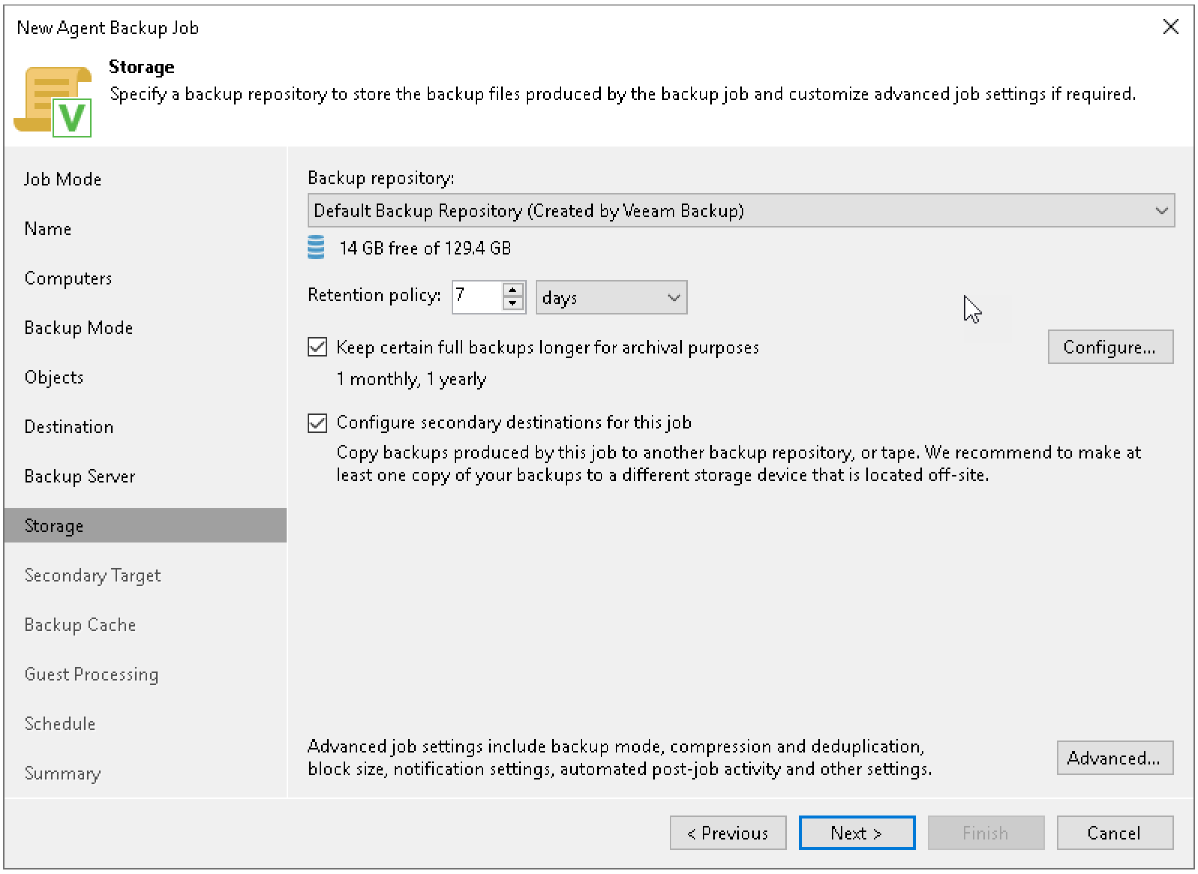
● Backup the following volumes only:

Add Object

Volume name: C:\

Example: D:\

7. At the **Storage** step of the wizard, specify settings for the target backup repository. Click **Next**.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Default Backup Repository (Created by Veeam Backup)

14 GB free of 129.4 GB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

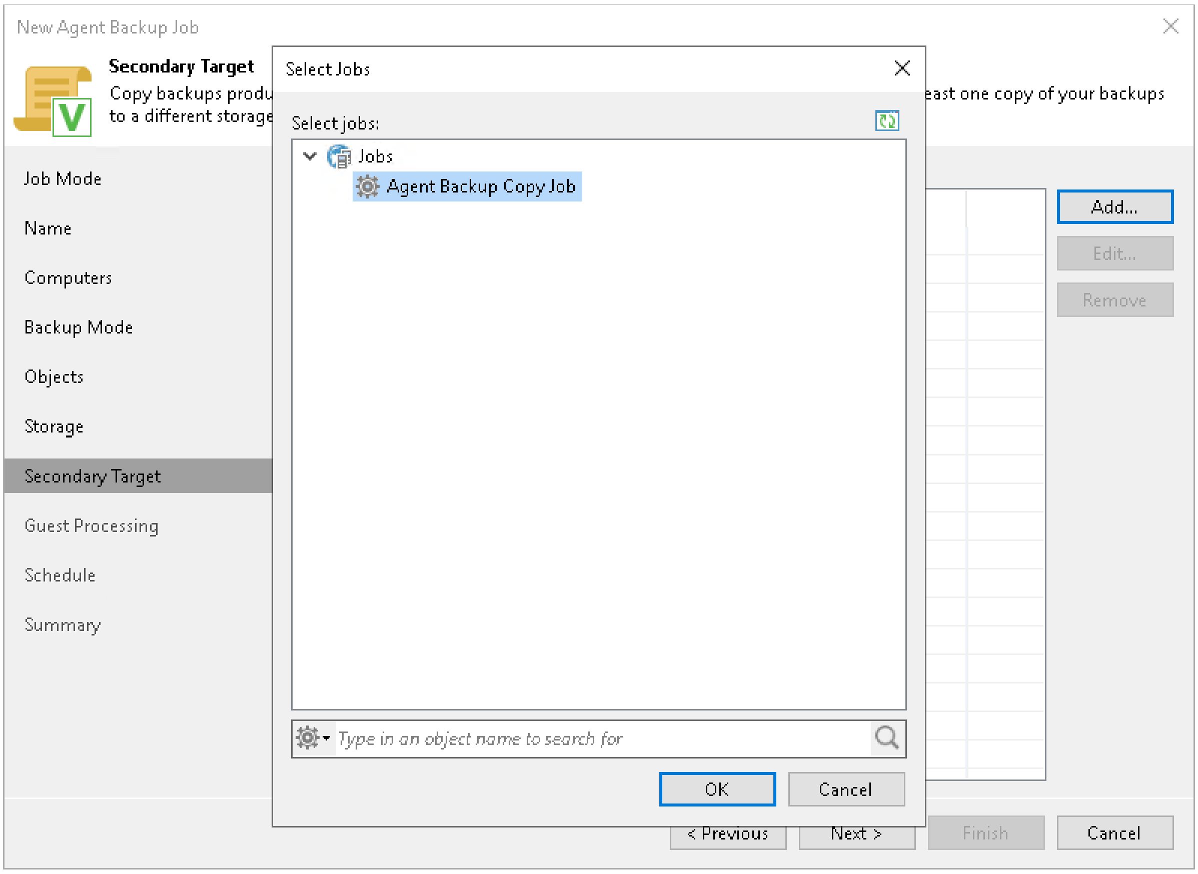
1 monthly, 1 yearly

☑ Configure secondary destinations for this job

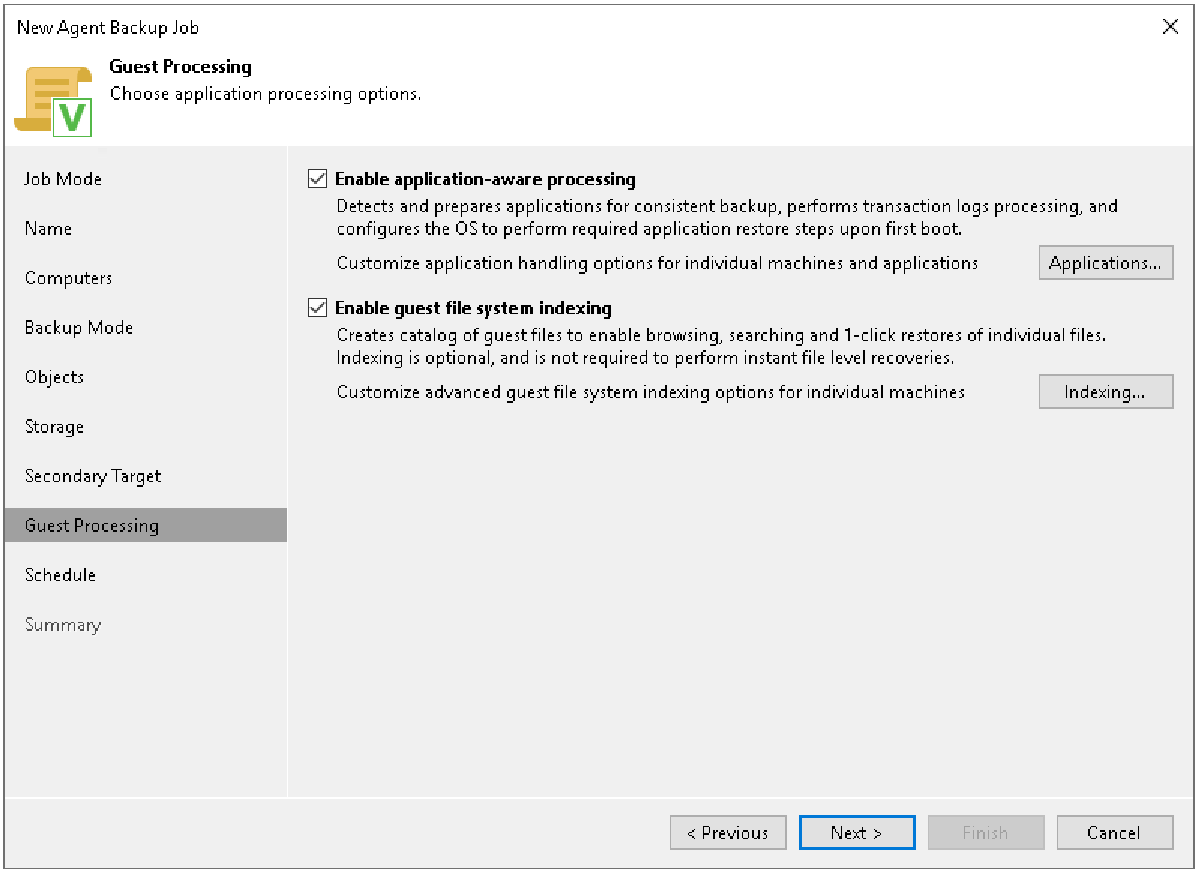
Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

8. [If you selected the **Configure secondary destinations for this job** check box at the **Storage** step of the wizard] At the **Secondary Target** step of the wizard, link the Veeam Agent backup job to a backup to tape or backup copy job. Click **Next**.



9. At the **Guest Processing** step of the wizard, specify guest OS processing settings. Click **Next**.



New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

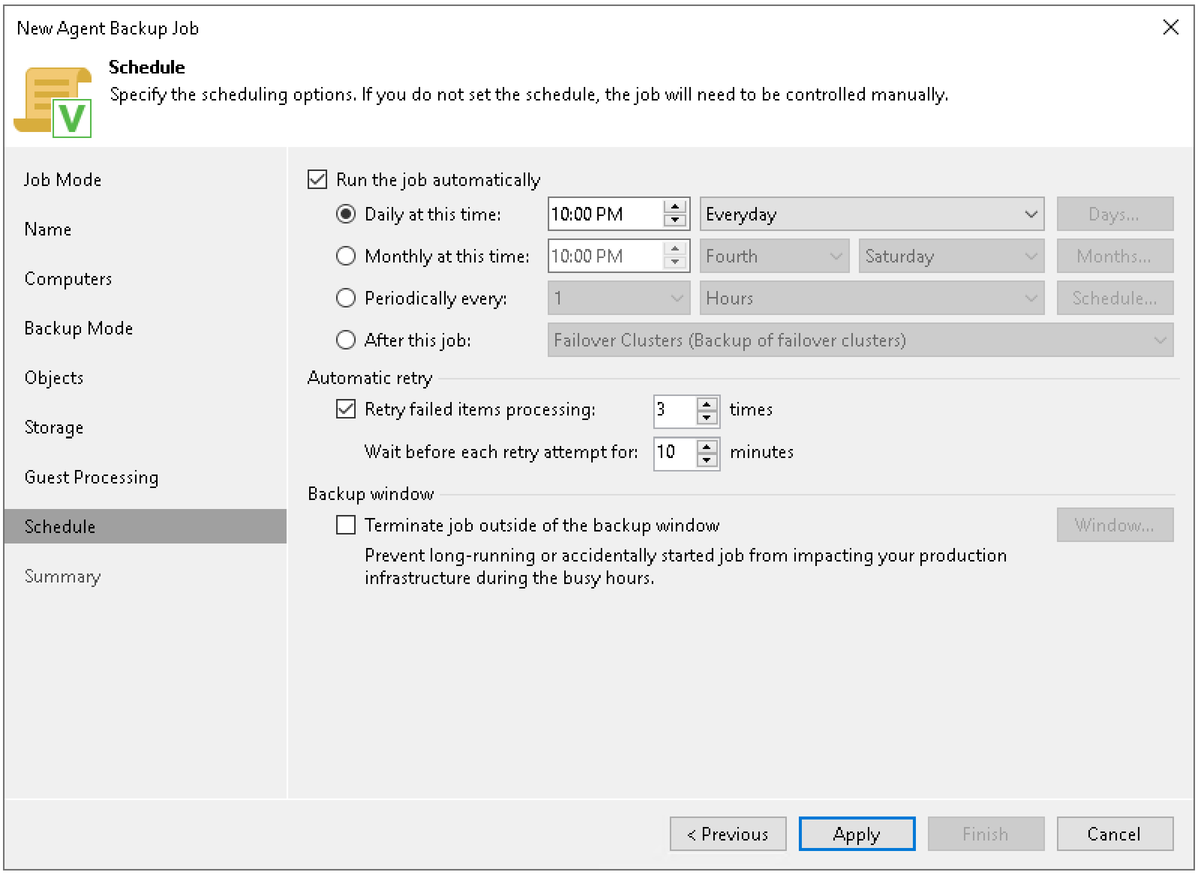
Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

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



New Agent Backup Job

Schedule

Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

○ Periodically every: 1 Hours

○ After this job: Failover Clusters (Backup of failover clusters)

Automatic retry

☑ Retry failed items processing: 3 times

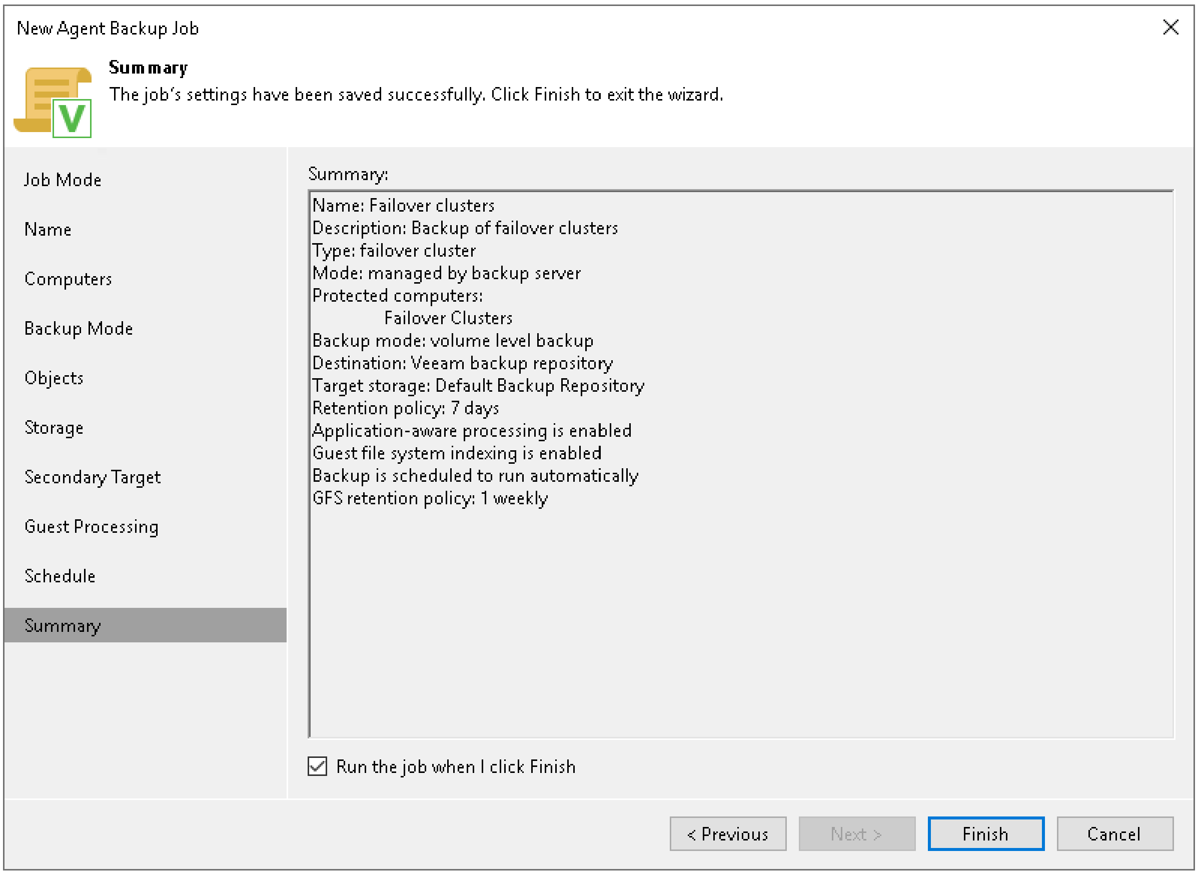
Wait before each retry attempt for: 10 minutes

Backup window

□ Terminate job outside of the backup window

Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.

11. At the **Summary** step of the wizard, review settings of the configured backup job. Click **Finish** to close the wizard.



The job's settings have been saved successfully. Click Finish to exit the wizard.

Summary:

```
Name: Failover clusters
Description: Backup of failover clusters
Type: failover cluster
Mode: managed by backup server
Protected computers:
        Failover Clusters
Backup mode: volume level backup
Destination: Veeam backup repository
Target storage: Default Backup Repository
Retention policy: 7 days
Application-aware processing is enabled
Guest file system indexing is enabled
Backup is scheduled to run automatically
GFS retention policy: 1 weekly
```

☑ Run the job when I click Finish

How to Move Unix Computers to Protection Group for Individual Computers

Veeam Backup & Replication allows you to manage Unix-based Veeam Agent computers through a protection group for individual computers. You can migrate your Unix computers from a protection group for pre-installed Veeam Agents to a protection group for individual computers without breaking the existing backup chains. For more information on protection group types, see Protection Group Types.

Before You Begin

Before you move a Unix computer from a protection group for pre-installed Veeam Agents to a protection group for individual computers, consider the following:

- The host name of the Veeam Agent computer that you move from a protection group for pre-installed Veeam Agents to a protection group for individual computers must be resolvable into an IP address by DNS or locally on Veeam backup server.
- To preserve the backup chain, you must make sure the backup job that used to protect the Unix computer you moved still has this Unix computer in its protection scope after the move.

  If the Unix computer is in the scope of the backup job as an individual machine, the backup job will continue the backup chain for this computer without any additional adjustments.

  If the Unix computer is in the scope of the backup job as a member of a protection group, after you move the Veeam Agent computer to another protection group, you must add the protection group that contains the moved machine to the backup job.
- You can move multiple Unix computers from a protection group for pre-installed Veeam Agents to a protection group for individual computers within a single move operation.

Moving Unix Computers to Protection Group for Individual Computers

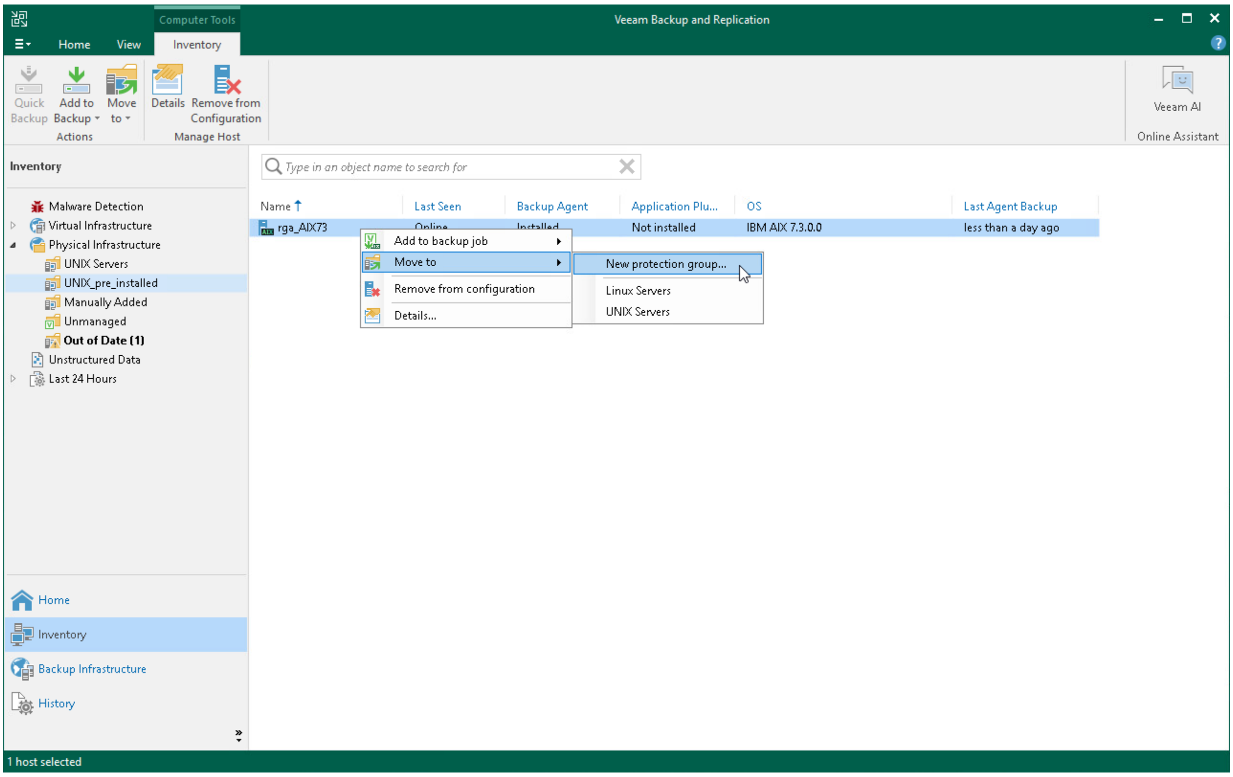
This scenario describes how to move Unix computers from a protection group for pre-installed Veeam Agents to a new or existing protection group for individual computers. In this example, the Unix computer is added to the scope of the backup job as a member of a protection group. The backup job name is *Agent Backup Policy UNIX*.

To move a Unix computer to a protection group for individual computers:

1. Open the **Inventory** view.
2. In the inventory pane, expand the **Physical Infrastructure** node and select the protection group for pre-installed Veeam Agents that contains the computer you want to move.
3. In the working area, select a single or multiple computers and click **Move to** on the ribbon or right click the selection and choose **Move to**.

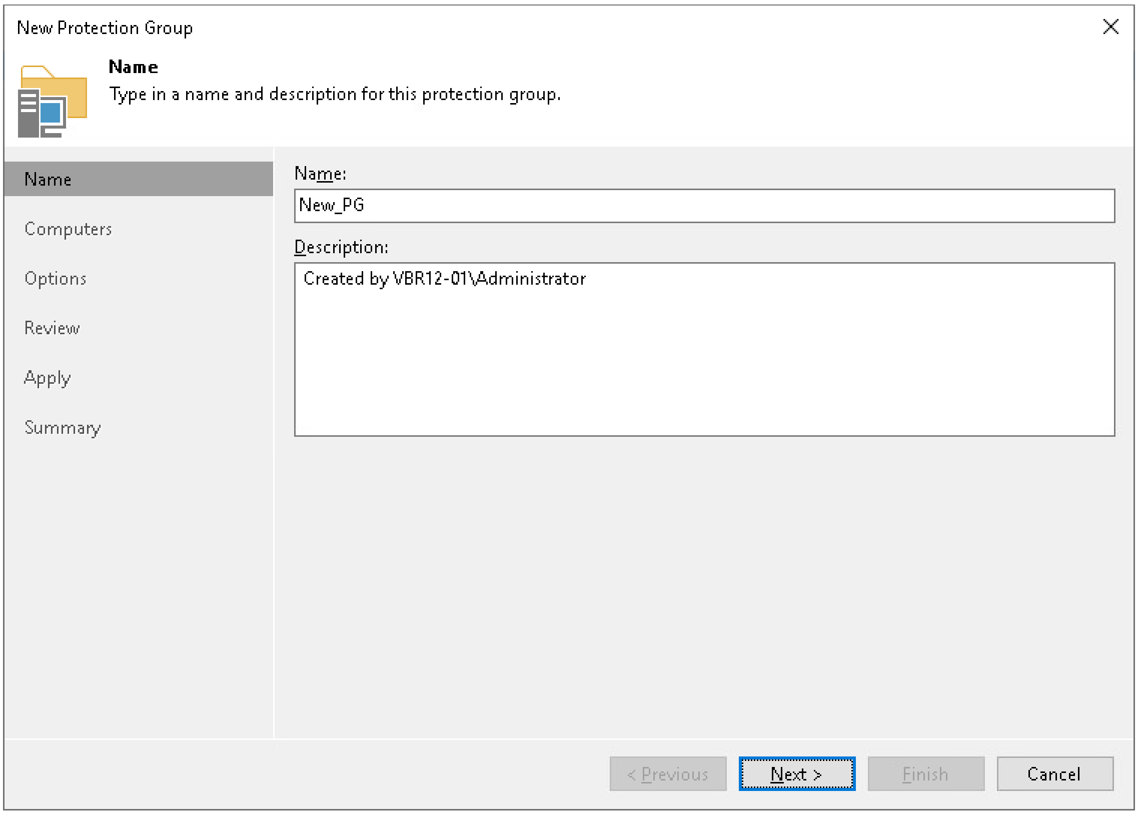
   If you want to move the Veeam Agent computer to a new protection group, from the **Move to** menu select **New protection group** and proceed to Step 4.

If you want to move the Veeam Agent computer to an existing protection group, from the **Move to** menu select the name of the existing protection group and proceed to Step 5.



In the **Move agent into the protection group?** dialog window, select **Yes**. Veeam Backup & Replication will open the protection group wizard where you can create new or edit existing protection group. For more information on creating or editing a protection group, see Creating Protection Groups.

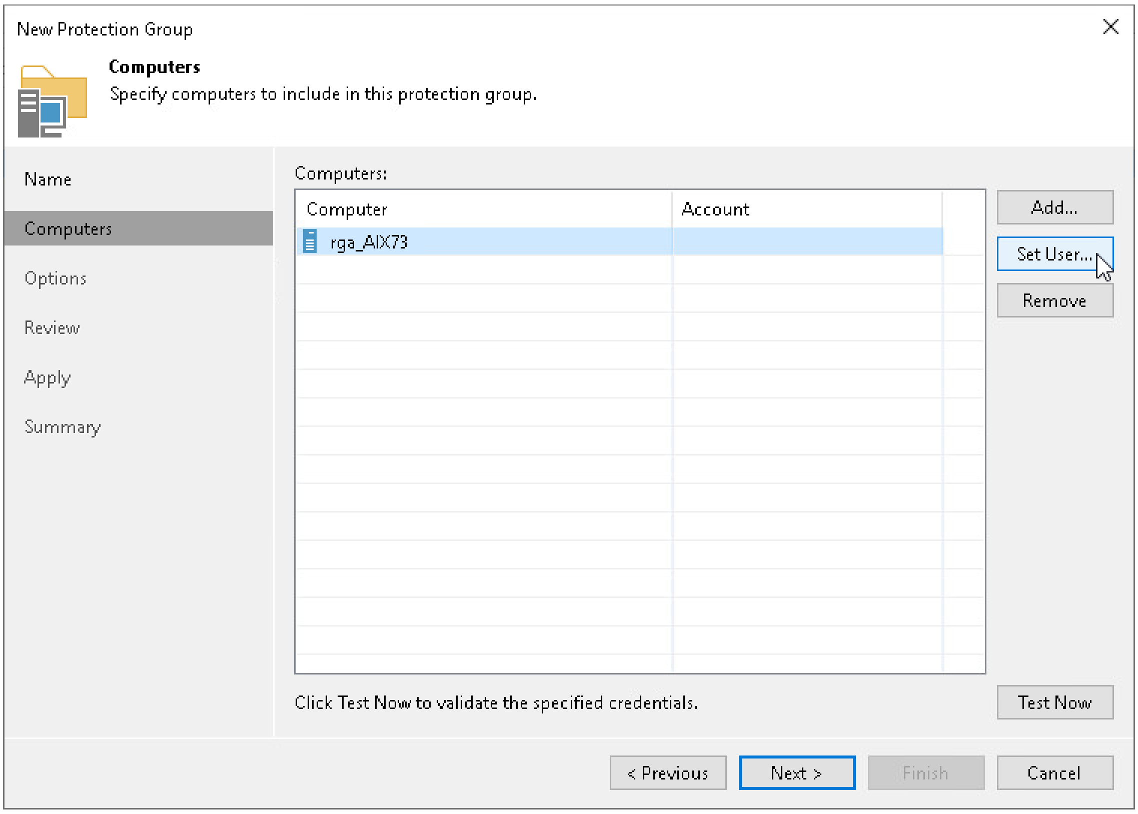
4. At the **Name** step of the wizard, specify a name and description for the protection group.



Name: New_PG

Description: Created by VBR12-01\Administrator

5. At the **Computers** step of the wizard, select the Unix computer you want to move and click **Set User**.



Specify computers to include in this protection group.

Computer	Account
rga_AIX73	

Click Test Now to validate the specified credentials.

To specify credentials for the user account that Veeam Backup & Replication will use to connect to the Unix computer, do the following:

a. In the **Credentials** window, click **Add** > **Stored** > **SSH Credentials**.

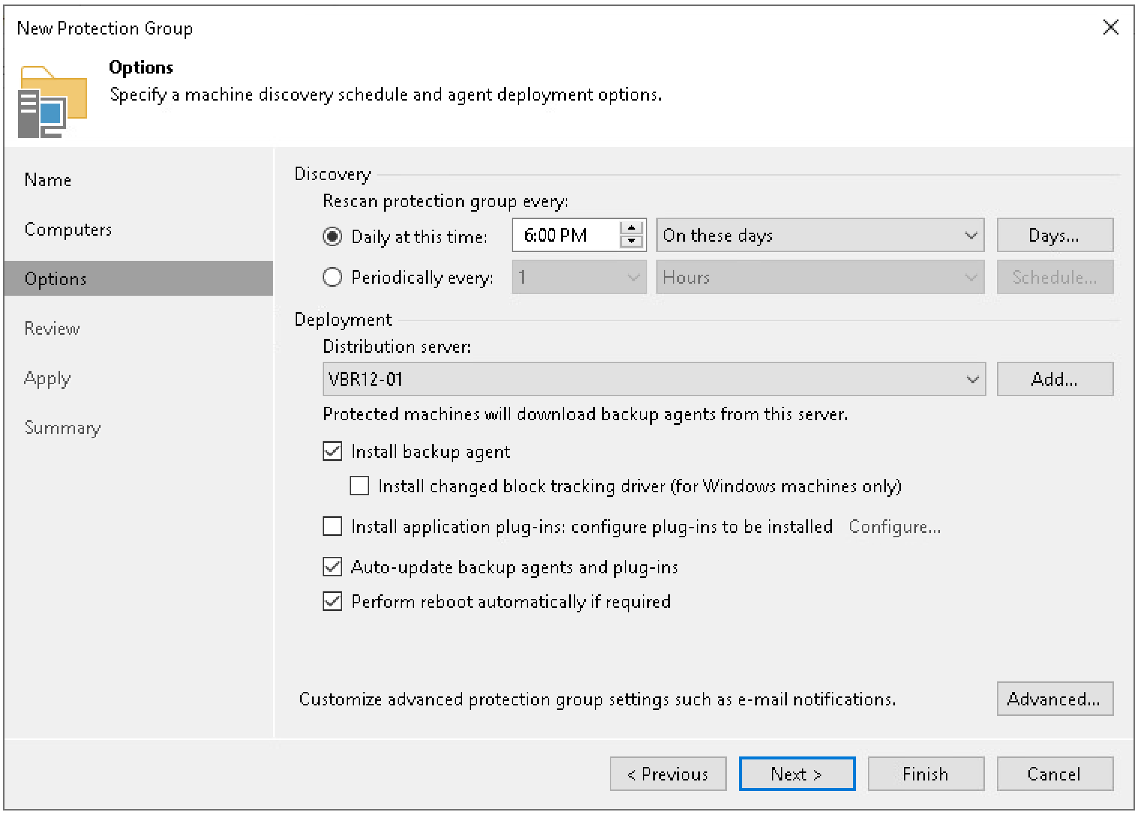
b. Specify user name and password, then click **OK**.

c. In the **Credentials** window, click **OK**.

> **NOTE**
>
> If you move multiple computers and you use the same set of credentials for them, you can select them all and click **Set User** to specify the credentials. If the computers you move have different credentials, specify credentials for each computer individually.

> **TIP**
>
> You can click **Test Now** to validate the specified credentials

6. At the **Options** step of the wizard, specify the discovery and deployment options for the Veeam Agent computer.



New Protection Group

Options

Specify a machine discovery schedule and agent deployment options.

Discovery

Rescan protection group every:

● Daily at this time: 6:00 PM On these days

○ Periodically every: 1 Hours

Deployment

Distribution server:

VBR12-01

Protected machines will download backup agents from this server.

☑ Install backup agent

□ Install changed block tracking driver (for Windows machines only)

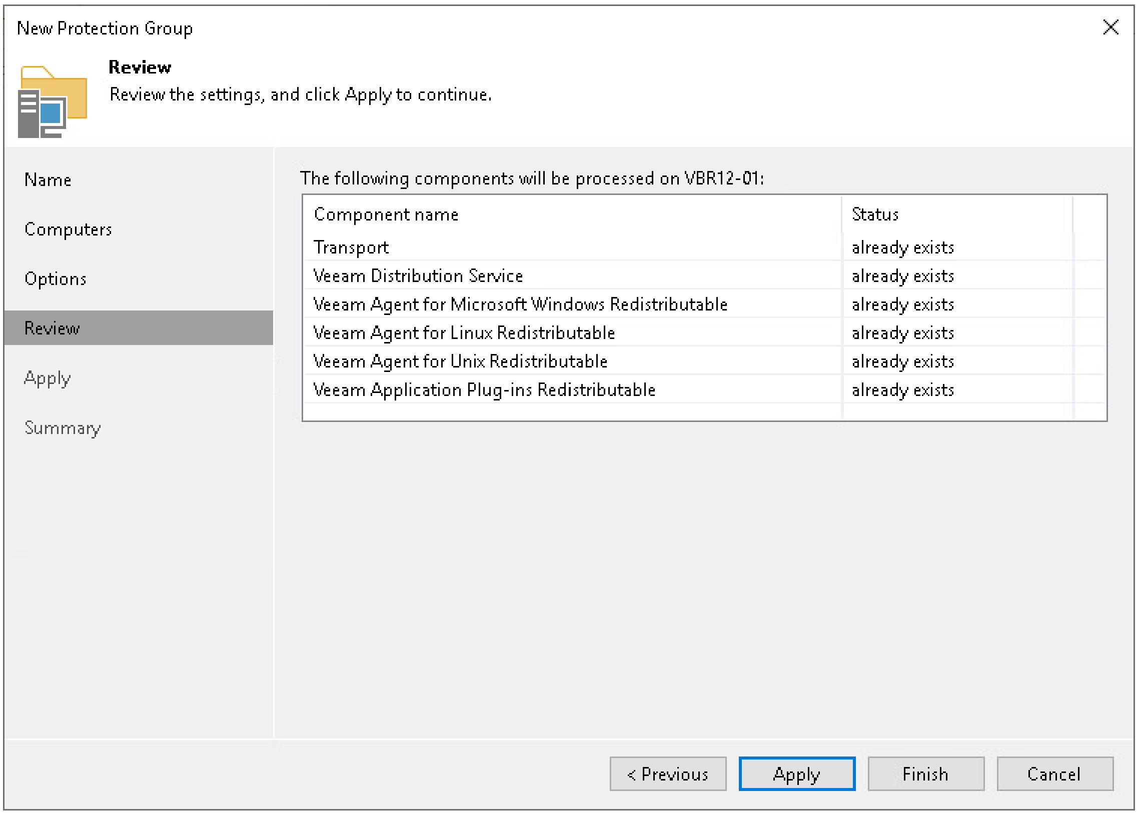
□ Install application plug-ins: configure plug-ins to be installed Configure...

☑ Auto-update backup agents and plug-ins

☑ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications.

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



New Protection Group

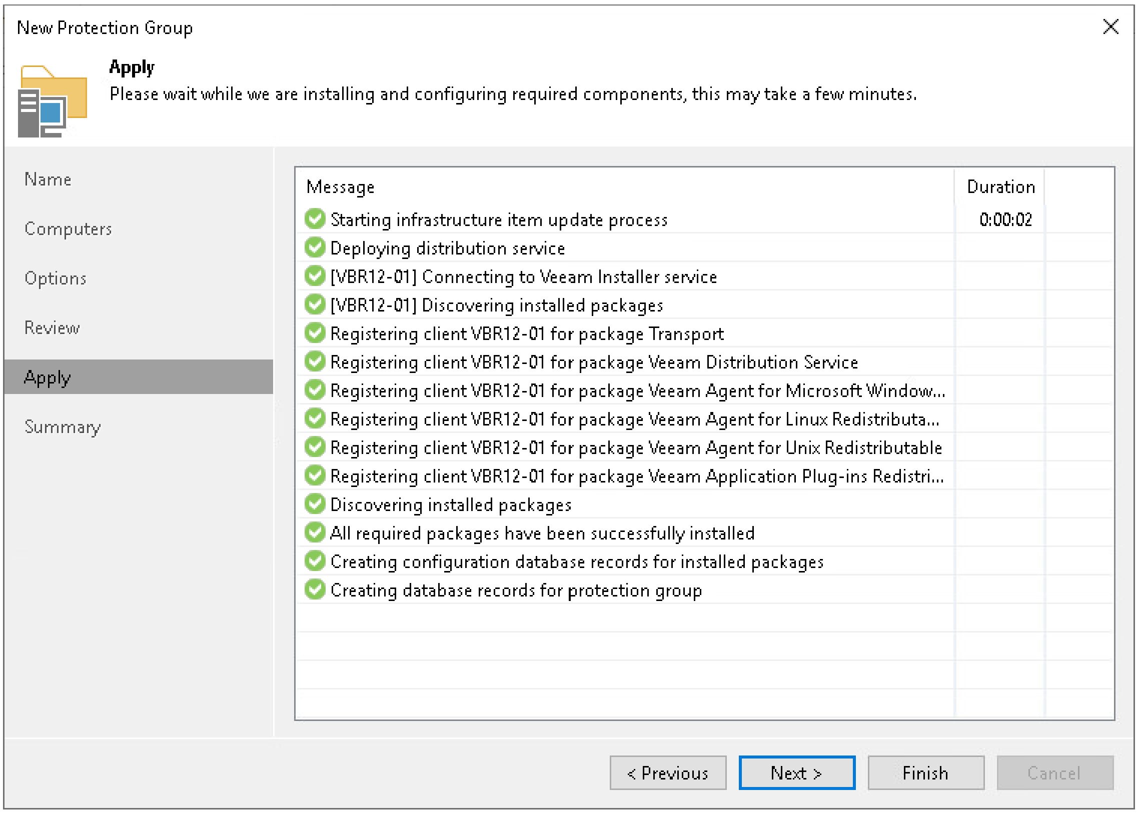
Review

Review the settings, and click Apply to continue.

The following components will be processed on VBR12-01:

Component name	Status
Transport	already exists
Veeam Distribution Service	already exists
Veeam Agent for Microsoft Windows Redistributable	already exists
Veeam Agent for Linux Redistributable	already exists
Veeam Agent for Unix Redistributable	already exists
Veeam Application Plug-ins Redistributable	already exists

8. At the **Apply** step of the wizard, monitor the installation and configuration of the required components.



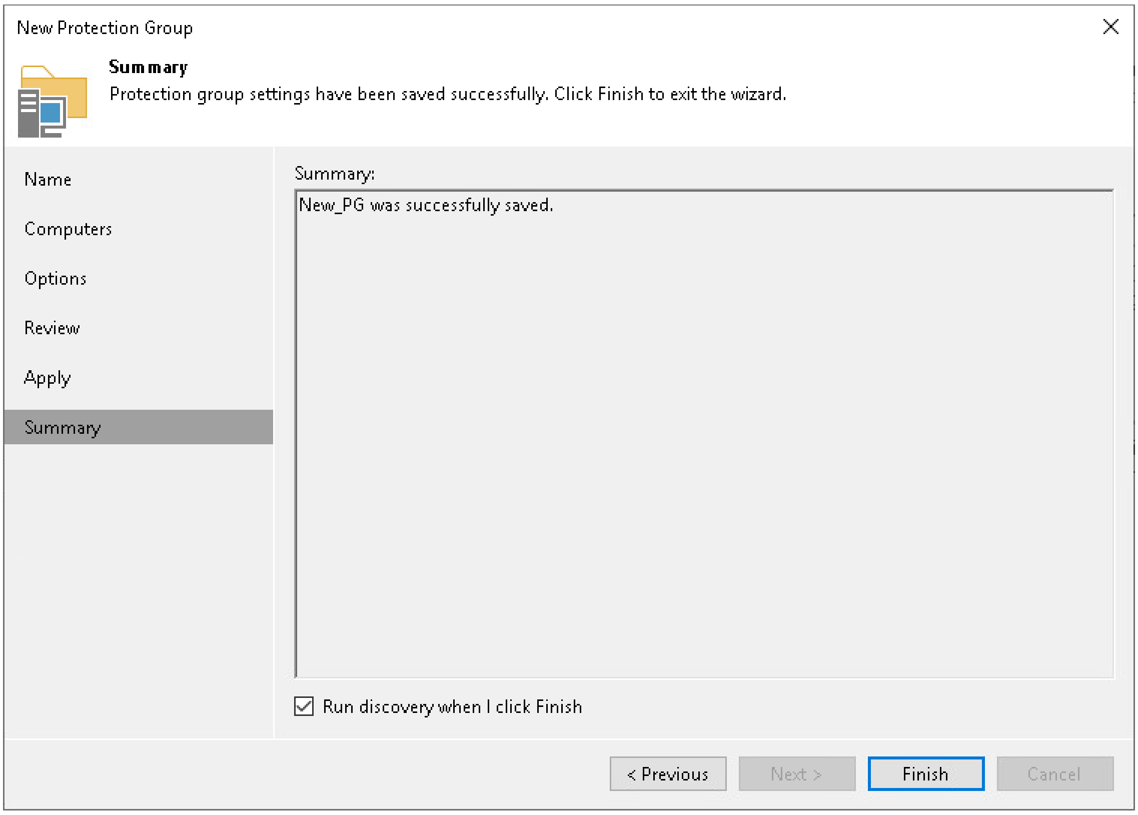
New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:02
✓ Deploying distribution service	
✓ [VBR12-01] Connecting to Veeam Installer service	
✓ [VBR12-01] Discovering installed packages	
✓ Registering client VBR12-01 for package Transport	
✓ Registering client VBR12-01 for package Veeam Distribution Service	
✓ Registering client VBR12-01 for package Veeam Agent for Microsoft Window...	
✓ Registering client VBR12-01 for package Veeam Agent for Linux Redistributa...	
✓ Registering client VBR12-01 for package Veeam Agent for Unix Redistributable	
✓ Registering client VBR12-01 for package Veeam Application Plug-ins Redistri...	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating configuration database records for installed packages	
✓ Creating database records for protection group	

9. At the **Summary** step of the wizard, click **Finish** to complete the protection group configuration.



New Protection Group

Summary

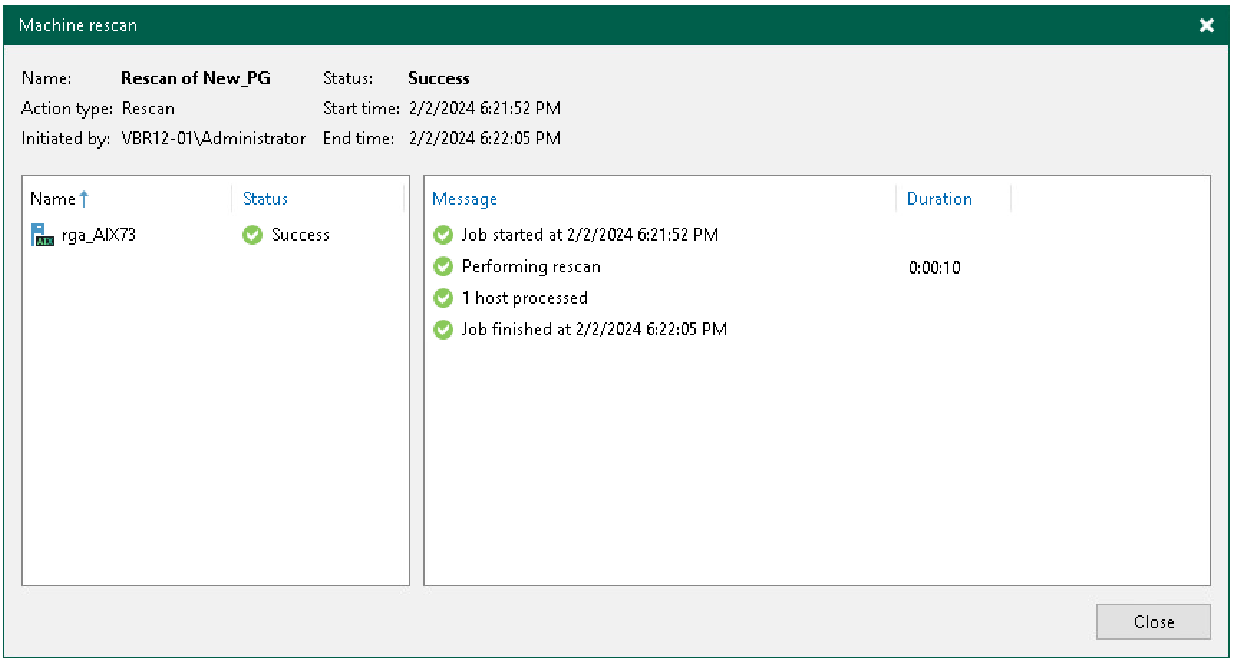
Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:

New_PG was successfully saved.

☑ Run discovery when I click Finish

10. In the inventory pane, expand the **Physical Infrastructure** node, select the protection group where you moved the Unix computer; then select **Rescan** on the ribbon. Alternatively, right click the protection group where you moved the Unix computer and select **Rescan**.



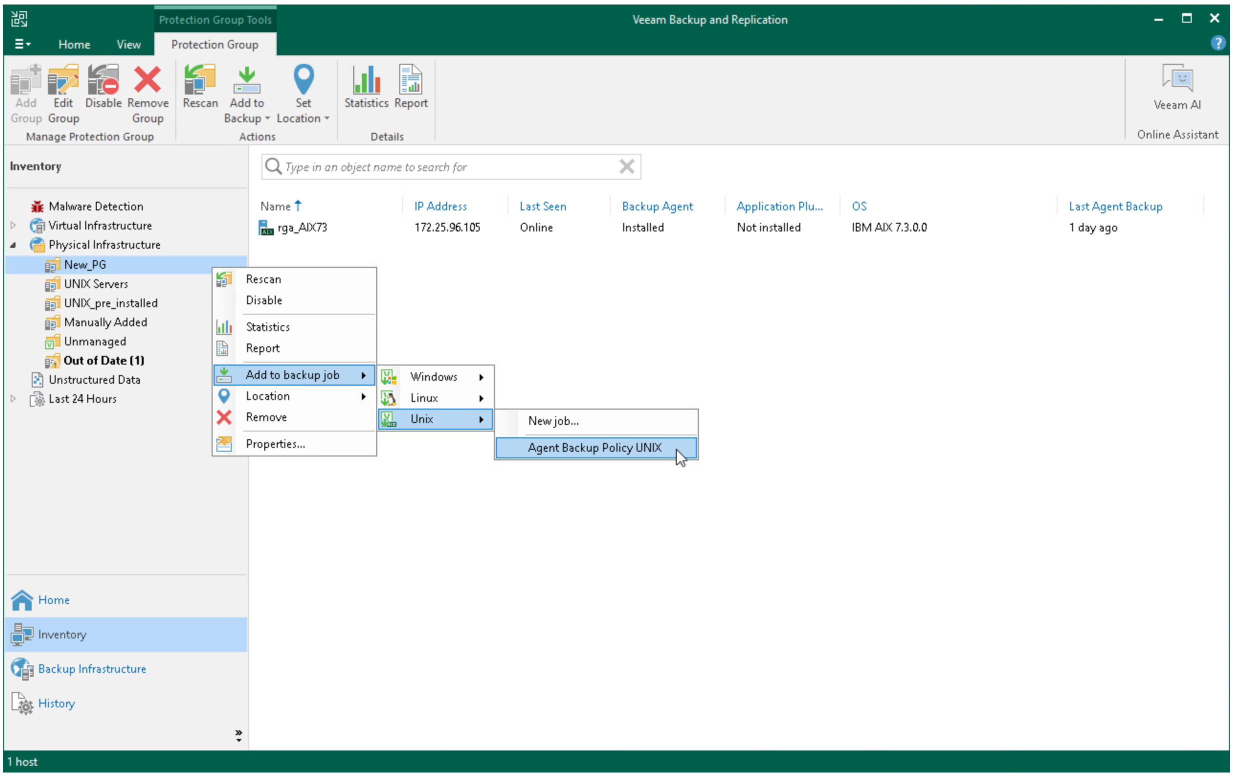
Machine rescan

Name: Rescan of New_PG
Status: Success
Action type: Rescan
Start time: 2/2/2024 6:21:52 PM
Initiated by: VBR12-01\Administrator
End time: 2/2/2024 6:22:05 PM

Name	Status
rga_AIX73	Success

Message	Duration
Job started at 2/2/2024 6:21:52 PM	
Performing rescan	0:00:10
1 host processed	
Job finished at 2/2/2024 6:22:05 PM	

11. In the **Physical Infrastructure** node, select the protection group where you moved the Unix computer; then select **Add to Backup** > **Unix** > **Agent Backup Policy UNIX** on the ribbon. Alternatively, right click the protection group where you moved the Unix computer and select **Add to Backup Job** > **Unix** > **Agent Backup Policy UNIX**.



Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Backup
rga_AIX73	172.25.96.105	Online	Installed	Not installed	IBM AIX 7.3.0.0	1 day ago

Veeam Backup & Replication will add the protection group for individual computers that contains the moved Unix computer to the original *Agent Backup Policy UNIX* backup job that used to protect the Unix computer when it was a member of the protection group for pre-installed Veeam Agents. The backup chain will continue uninterrupted.

How to Perform Bare Metal Restore for Clusters with Shared Disks

Veeam Backup & Replication allows you to protect failover clusters in your infrastructure using Veeam Agent for Microsoft Windows. If cluster nodes fail to start for any reason, you can restore affected nodes.

This scenario describes how to perform bare metal restore for a Windows Server Failover Cluster with a shared disk after the majority of the voting nodes of the cluster fail to start.

> NOTE
>
> The entire computer backup must be created beforehand. To learn more, see Select Backup Mode.

1. Perform bare metal restore for each failed node of the failover cluster. The restore process is the same as for restore of a computer protected with Veeam Agent for Microsoft Windows operating in the standalone mode. To learn more, see the Restoring from Veeam Recovery Media section in the Veeam Agent for Microsoft Windows User Guide.

2. Test the failover cluster configuration. For example, run failover cluster validation tests. To learn more, see Microsoft Documentation.

   Depending on the validation tests results, do the following:

   - If the validation report does not contain errors, proceed to step 3.
   - If the validation report contain errors, fix them or re-create the cluster. To learn more, see Microsoft Documentation.

3. Restore the cluster shared disk from the Veeam Backup & Replication console. To learn more, see Restoring Volumes.

   > IMPORTANT
   >
   > Do not restore the cluster shared disk from the Veeam Agent computer side. In this case, you will be able to restore only to a local disk.