Veeam Backup & Replication

Version 13

Quick Start Guide

May, 2026

© 2026 Veeam Software.

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

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

NOTE

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

Contents

CONTACTING VEEAM SOFTWARE 5
GETTING STARTED 6
ABOUT VEEAM BACKUP & REPLICATION 7
BACKUP INFRASTRUCTURE 8
Backup Infrastructure Components 9
Deployment Scenarios 10
Deployment Options 12
PLANNING AND PREPARATION 13
Supported Platforms 14
System Requirements 15
Ports 16
VEEAM BACKUP & REPLICATION UI 17
DEPLOYMENT 19
Step 1. Installing Veeam Backup & Replication 20
Linux 21
Microsoft Windows 26
Step 2. Installing Veeam Backup & Replication Console 28
Step 3. Adding VMware vSphere Virtual Infrastructure Servers 33
Step 4. Adding Microsoft Hyper-V Virtual Infrastructure Servers 36
Step 5. Configuring VMware Backup Proxy 40
Step 6. Configuring Backup Proxy 46
Step 7. Configuring Backup Repository 47
Step 8. Configuring Object Storage Repositories 54
Step 9. Configuring Scale-Out Backup Repositories 60
VM BACKUP 64
Backup Methods 65
Creating Backup Job 67
Monitoring Job Performance in Real Time 72
Start Backup Job Manually 73
Locating Backup Files 74
Creating Application-Aware Backup Job 75
DATA RECOVERY 79
Restoring Entire VM 80
Restoring VM Files 85
Restoring VM Virtual Disks 87
Restoring Guest OS Files 91
Restoring Application Items 94

Exporting Disks 97
BACKUP COPY 101
VM REPLICATION 106
Creating Replication Job 107
Monitoring Job Performance in Real Time 115
Start Replication Job Manually 116
Replica Failover and Failback 117
Performing Replica Failover 119
Performing Permanent Failover 121
Undoing Failover 122
Performing Failback 123
Committing Failback 125
Undoing Failback 126
ENTERPRISE MANAGER 127
Installing Veeam Backup Enterprise Manager 128
Linux 129
Microsoft Windows 134
Adding Backup Servers 137
Managing Jobs 139
Performing 1-Click File Restore 142
Performing Self-Restore of VM Guest OS Files 144
BACKING UP PHYSICAL MACHINES 148
Creating Protection Group 149
Creating Veeam Agent Backup Job 154
RESTORING DATA OF PHYSICAL MACHINES 159
GETTING TECHNICAL SUPPORT 160

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

Getting Started

Document Structure

The guide contains instructions on the following:

- Veeam Backup & Replication functionality: how to deploy Veeam Backup & Replication, perform backup, replication, and restore operations.
- Integration with Veeam Backup Enterprise Manager: a free tool for managing distributed infrastructure.
- Agent management: built-in Veeam Backup & Replication feature to back up physical machines using Veeam Agents.

Help and Support

This guide provides a high-level overview of Veeam Backup & Replication primary features and should be regarded as a supplement to existing technical documentation. The complete set of documentation can be found on the Veeam Technical Documentation page.

For technical support and assistance, use the following resources:

- Veeam R&D Forums
- Customer Support Portal

About Veeam Backup & Replication

What is Veeam Backup & Replication?

Veeam Backup & Replication is a data protection and disaster recovery solution for virtual, physical and cloud environments. With Veeam Backup & Replication you can:

- Create crash-consistent and application-consistent backups of virtual and physical machines.
- Quickly restore physical machines, EC2 instances, Microsoft Azure VMs, Google VM instances, VMs, VM disks, guest OS files and application items.
- Perform backup health check to verify that backups are not corrupted and are ready for restoring.
- Create VM replicas and switch to them in case of a disaster.
- Automate transferring of backups to tapes and other external repositories.

Note that in this guide, we will not overview all the Veeam Backup & Replication capabilities. You can find them in the Veeam Backup & Replication User Guide.

What Else Can I Do?

Veeam Backup & Replication provides utilities not mentioned in this guide that can help you secure and manage your data:

- Veeam Backup for Microsoft 365: backup and restore solution for Microsoft 365 data.
- Veeam Backup for Nutanix AHV: backup and restore solution for Nutanix AHV VMs.
- Veeam Backup for Oracle Linux Virtualization Manager and Red Hat Virtualization: backup and restore solution for oVirt VMs.
- Veeam Backup for Proxmox VE: backup and restore solution for Proxmox VE VMs.
- Plug-in for Veeam Backup for AWS: extension for integration with Veeam Backup for AWS.
- Plug-in for Veeam Backup for Microsoft Azure: extension for integration with Veeam Backup for Microsoft Azure.
- Plug-in for Veeam Backup for Google Cloud: extension for integration with Veeam Backup for Google Cloud.

Veeam Backup & Replication also provides the following tools for monitoring and management:

- Veeam ONE: real-time monitoring, reporting, alerting and managing tool for virtual and physical environments.
- Veeam Management Pack for Microsoft System Center: Microsoft System Center extension for managing and monitoring VMware vSphere, Microsoft Hyper-V, and Veeam Backup & Replication.
- Veeam Availability Orchestrator: a tool for automated creation and testing of DR plans that comply regulatory requirements.

Backup Infrastructure

This section describes main Veeam Backup & Replication infrastructure components and deployment scenarios.

Backup Infrastructure Components

To start working with Veeam Backup & Replication, you must set up the backup infrastructure. The basic Veeam Backup & Replication infrastructure consists of the following core components:

- **Backup server**

  A machine on which Veeam Backup & Replication is installed. The backup server performs main management operations: coordinates backup, replication and restore tasks, controls job scheduling and resource allocation.

- **Backup repository**

  A component where Veeam Backup & Replication keeps backup files, backup copies and metadata of replicated VMs.

- **[For VMware vSphere] VMware backup proxy**

  A component that retrieves data from the source host, processes it and transfers to the backup repository.

- **[For Microsoft Hyper-V] Backup proxy (on-host or off-host)**

  A component that retrieves data from the source host, processes it and transfers to the backup repository.

- **Infrastructure servers and hosts**

  VMware vSphere and Microsoft Hyper-V hosts that you plan to use as source and target for backup, replication and other activities. Microsoft Windows and Linux servers for which you plan to assign roles of a backup proxy or backup repository.

Reference

For details on all backup infrastructure components, see the Backup Infrastructure Components section in the Veeam Backup & Replication User Guide.

Deployment Scenarios

You can use Veeam Backup & Replication in virtual environments of any size and complexity. The architecture of the solution supports onsite and offsite data protection, operations across remote sites and geographically dispersed locations. Veeam Backup & Replication provides flexible scalability and easily adapts to the needs of your virtual environment.

Veeam Backup & Replication supports several deployment scenarios, and each one includes the core infrastructure components: backup server, backup proxy and backup repository. Depending on the size of your virtual environment, you can use one of the following scenarios:

- Simple deployment

  For small virtual environments. In this scenario, the roles of all components required for data protection tasks are assigned to one machine.

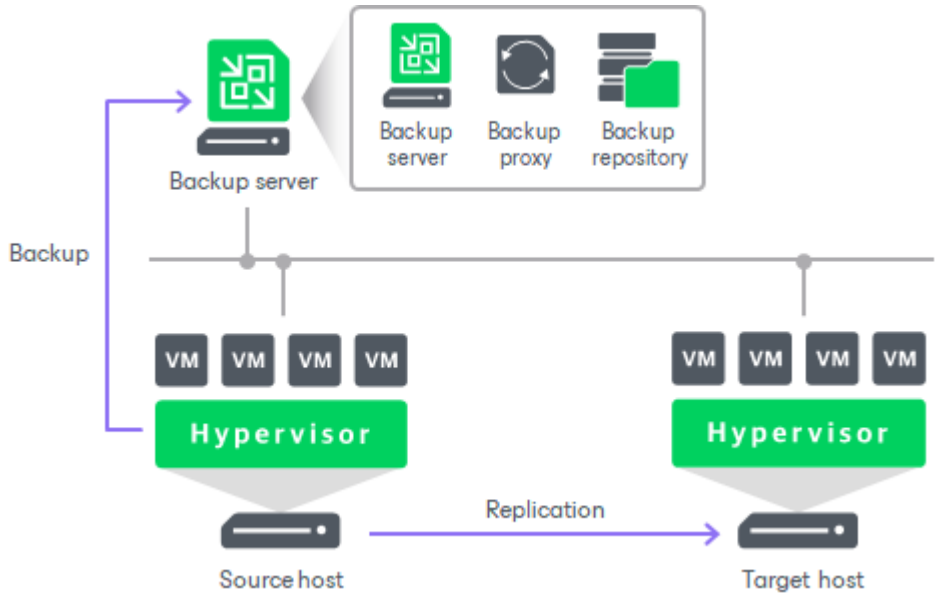
- Advanced deployment

  For medium-sized and large-scale virtual environments. In this scenario, the roles of components required for data protection tasks are assigned to dedicated machines.

Veeam Backup & Replication also supports the distributed deployment scenario for large geographically dispersed environments with multiple backup servers. We omit detailed description of this scenario because this guide is aimed for quick overview of basic features. For details on the distributed scenario, see the Distributed Deployment section in the Veeam Backup & Replication User Guide.

Simple Deployment

In the simple deployment scenario, the roles of the backup server, backup proxy and backup repository are assigned to a single machine. These roles are assigned automatically to the machine where you install Veeam Backup & Replication.



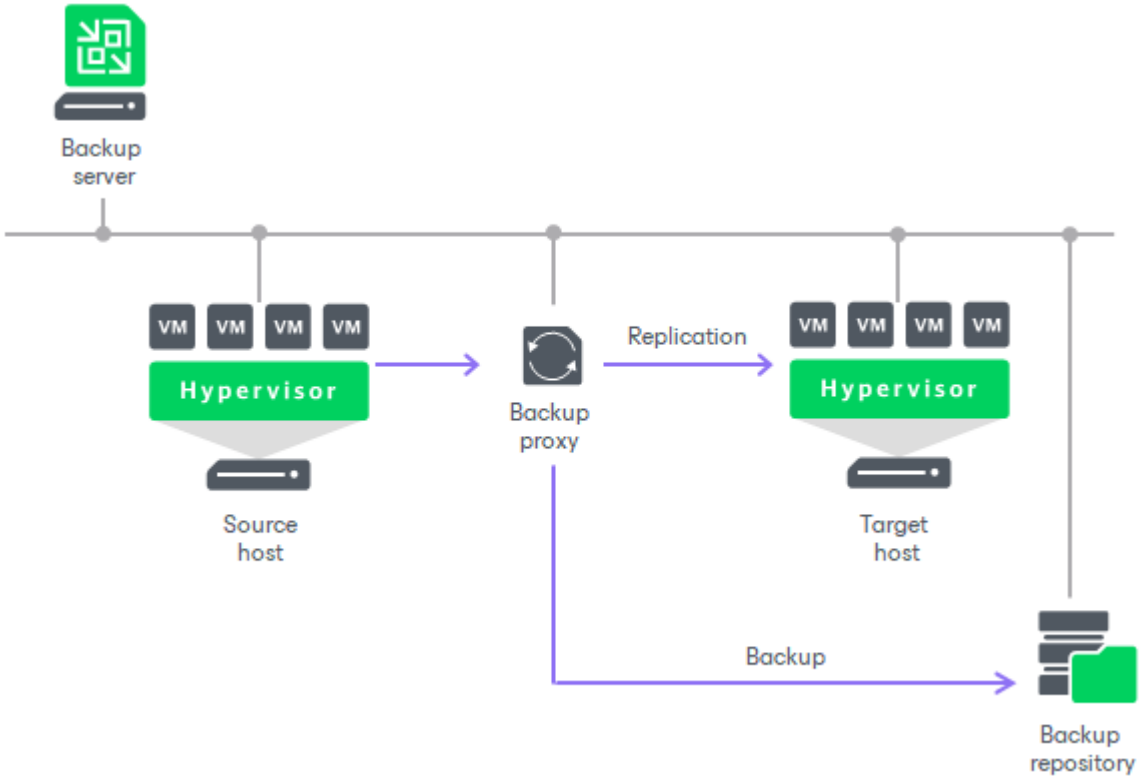
The drawback of the simple deployment scenario is that only the backup server handles and stores all data. For medium-sized or large-scale environments, the capacity of a single backup server may not be enough. To take the load off the backup server and balance it throughout your backup infrastructure, it is recommended to use the advanced deployment scenario.

Advanced Deployment

In the advanced deployment scenario, the roles of the backup server, backup proxy and backup repository are assigned to different machines. This gives the following advantages:

- The processing load is moved from backup server to backup proxy.
- Increased fault tolerance: you can store data on a separate machine (the backup repository).

Note that this scenario requires that you assign the roles of the proxy and repository manually.



Depending on production environment and backup and replication scenarios you plan to use, the advanced deployment scenario may include multiple backup proxies and backup repositories, both on-site and off-site, controlled by a single backup server.

Deployment Options

You can deploy Veeam Backup & Replication on a Linux-based or Microsoft Windows-based server. Veeam Backup & Replication provides multiple deployment options described in the Deployment Options section in the Veeam Backup & Replication User Guide. In this guide, you will learn how to install Veeam Backup & Replication from .ISO files.

Veeam Backup & Replication on Linux

To install Veeam Backup & Replication on Linux, Veeam provides Veeam Software Appliance ISO. This ISO image includes the preconfigured Rocky Linux distribution and the Veeam Backup & Replication software. Veeam Software Appliance is secure-by-default thanks to the OS preconfigured according to DISA STIG guidelines. This helps avoid risky misconfigurations and minimizes attack surface.

Despite the .ISO is based on Linux, no Linux OS expertise is required. Veeam provides a simple text-based user interface (TUI) and a web-based console that covers all OS management tasks such as network or time configuration.

Veeam Backup & Replication on Microsoft Windows

To install Veeam Backup & Replication on Microsoft Windows, Veeam provides .ISO with installable software. This .ISO contains only the Veeam Backup & Replication software that must be installed on the already configured Microsoft Windows machine.

Veeam Backup & Replication Access Options

To access the Veeam Backup & Replication server, you can use the Veeam Backup & Replication console on a dedicated Microsoft Windows machine or use the web UI.

Planning and Preparation

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

Supported Platforms

Veeam Backup & Replication supports backup and recovery operations for the following virtualization platforms:

- VMware vSphere
- Microsoft Hyper-V
- Azure Local (formerly Azure Stack HCI)
- Nutanix AHV
- Proxmox VE
- Scale Computing HyperCore
- Oracle Linux Virtualization Manager
- Red Hat Virtualization

Veeam Backup & Replication also supports backup and recovery for the following applications and workloads:

- Applications:
  - Application-aware image processing and Veeam Explorers
  - Veeam Plug-Ins for enterpise applications
  - Microsoft Entra ID Plug-In for Veeam Backup & Replication
- Unstructured data:
  - Object storage repositories
  - Files shares
  - File servers
  - Enterprise NAS systems
- Operating systems:
  - Microsoft Windows computers
  - Linux computers
  - Unix machines
  - Mac computers

For the full list of supported platforms, see the Supported Platforms, Applications and Workloads section in the Veeam Backup & Replication User Guide.

> **TIP**
>
> In this guide, we overview VMware vSphere, Microsoft Hyper-V and Microsoft Windows computers.

System Requirements

Make sure that servers that you plan to use as backup infrastructure components meet the system requirements listed in the following sections of the Veeam Backup & Replication User Guide:

- System Requirements for Backup Server
- System Requirements for VMware Backup Proxy Server
- System Requirements for Backup Repository Server
- System Requirements for Enterprise Manager
- System Requirements for Supported Applications
- System Requirements for Veeam Explorer for Microsoft SQL Server

Reference

For the full list of system requirements, see the System Requirements section in the Veeam Backup & Replication User Guide.

Ports

Veeam Backup & Replication automatically creates firewall rules for the required ports on backup infrastructure components. These rules allow communication between the components.

You can find the lists of the ports in the following sections of the Veeam Backup & Replication User Guide:

- Backup Server Connections
- Microsoft Windows Server Connections
- Linux Server Connections
- [For VMware vSphere] Backup VMware Proxy Connections
- [For Microsoft Hyper-V] Backup Proxy Connections
- Backup Repository Connections
- Mount Server Connections
- VM Guest OS Connections
- Veeam Backup Enterprise Manager Connections
- Veeam Explorer for Microsoft SQL Server Connections
- Physical Machine Connections

> **TIP**
>
> In this guide, we assume that all ports are open in your infrastructure.

Reference

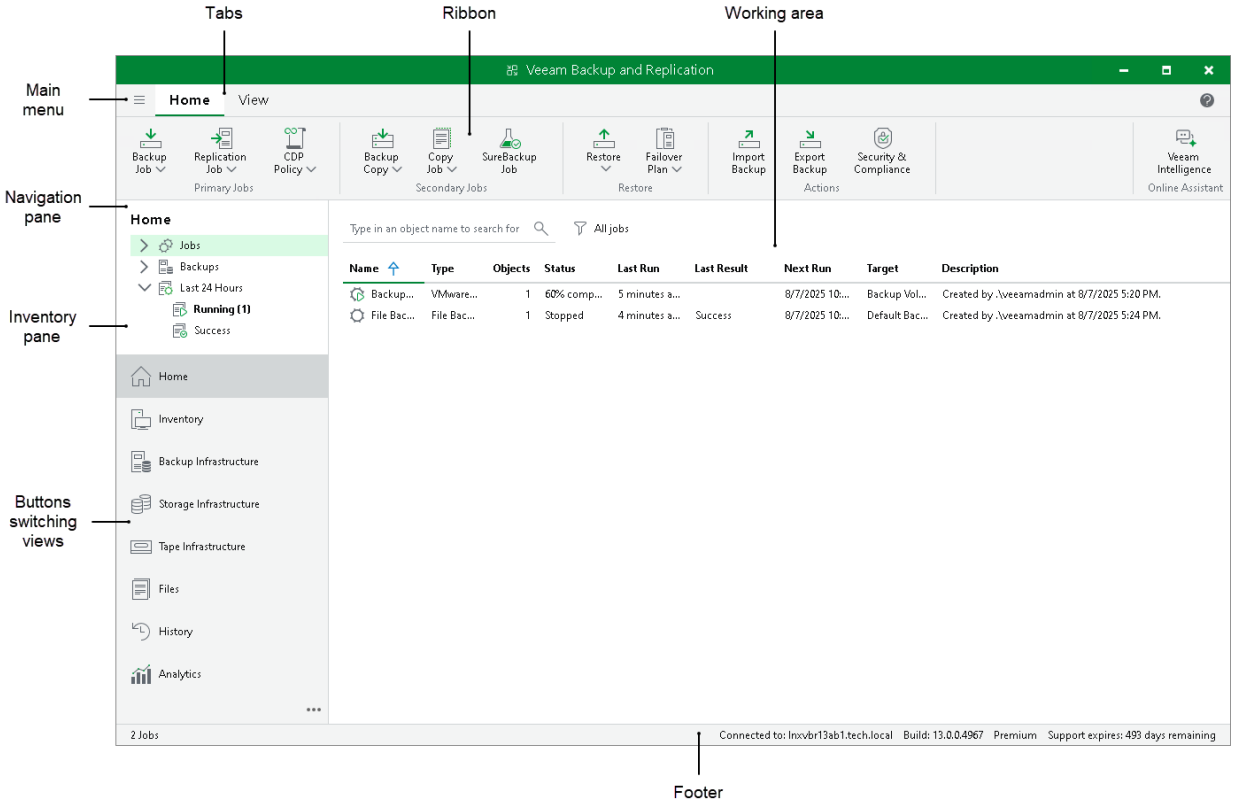
For the full list of ports, see the Ports section in the Veeam Backup & Replication User Guide.

Veeam Backup & Replication UI

You can access Veeam Backup & Replication using Veeam Backup & Replication console UI or Web UI. In this guide, you will work with the Veeam Backup & Replication console.

Veeam Backup & Replication Console UI

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



> **TIP:**
>
> To open online help, press [F1] in any Veeam Backup & Replication wizard or window. You will be redirected to the corresponding section of the Veeam Backup & Replication User Guide.

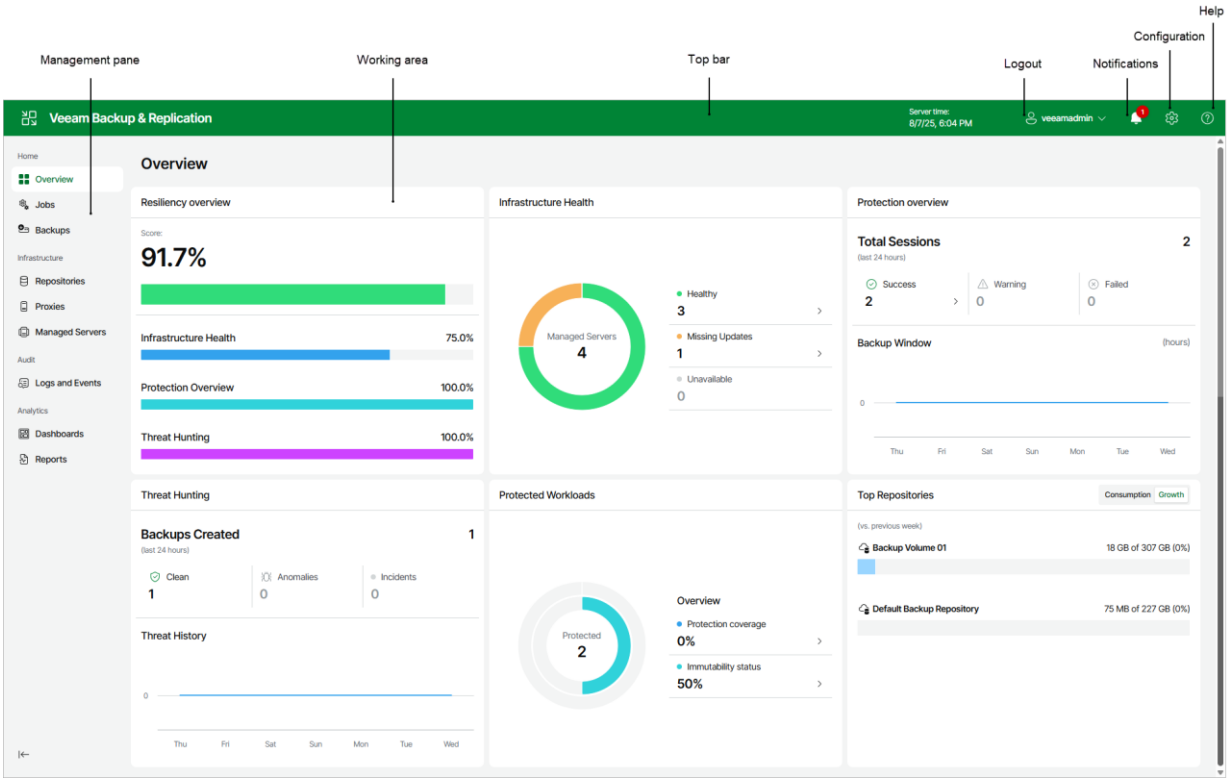
Veeam Backup & Replication Web UI

The Veeam Backup & Replication web UI is a browser-based interface that provides different data protection operations. The overall look and feel of the Veeam Backup & Replication web UI is consistent with the Veeam product family, ensuring familiarity for users of the Veeam Backup & Replication console.

IMPORTANT

Consider the following:

- The Veeam Backup & Replication web UI is not available in the Community Edition. A valid license is required to use this functionality.
- Only the Veeam Backup Administrator can log in to the web UI.
- The web UI has a developing functionality. For more information, see the Veeam Backup & Replication Web UI Features section in the Veeam Backup & Replication User Guide.



Reference

For details, see the Veeam Backup & Replication Console UI and Veeam Backup & Replication Web UI sections in the Veeam Backup & Replication User Guide.

Deployment

To start using Veeam Backup & Replication, do the following:

1. Install Veeam Backup & Replication.
2. Install the Veeam Backup & Replication console.
3. [For VMware vSphere] Add virtual infrastructure servers.
4. [For Microsoft Hyper-V] Add virtual infrastructure servers.
5. [For VMware vSphere] Configure VMware backup proxy.
6. [For Microsoft Hyper-V] Configure backup proxy.
7. Configure backup repository.
8. [Optional] Configure object storage repository.
9. [Optional] Configure scale-out backup repository.

> **NOTE:**
>
> In the simple deployment scenario, Veeam Backup & Replication uses the backup server also as the backup proxy and backup repository. For this reason, you can skip steps 5-7.

Step 1. Installing Veeam Backup & Replication

Install Veeam Backup & Replication on a Linux-based or Microsoft Windows-based physical or virtual machine.

Before You Begin

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

- The machine on which you plan to install Veeam Backup & Replication must meet the system requirements for the backup server. For details, see the System Requirements section in the Veeam Backup & Replication User Guide.
- The machine on which you plan to install Veeam Backup & Replication must meet the naming conventions. For details, see the Naming Conventions section in the Veeam Backup & Replication User Guide.
- [For Veeam Backup & Replication on Microsoft Windows] The account used to install the product must have the local Administrator permissions on the target machine. After installation, users can have standard (non-administrative) privileges to connect to the Veeam Backup & Replication console.
- [For Veeam Backup & Replication on Linux] Consider the following:
    - Check the Consideration and Limitations for Veeam Software Appliance Installation section in the Veeam Backup & Replication User Guide.
    - The account used to install the product must have access to manage input/output and boot devices. If you install Veeam Backup & Replication on a virtual machine, the account must also have permission to create virtual machines with attached disk images on the hypervisor level.

Linux

To install Veeam Backup & Replication, do the following:

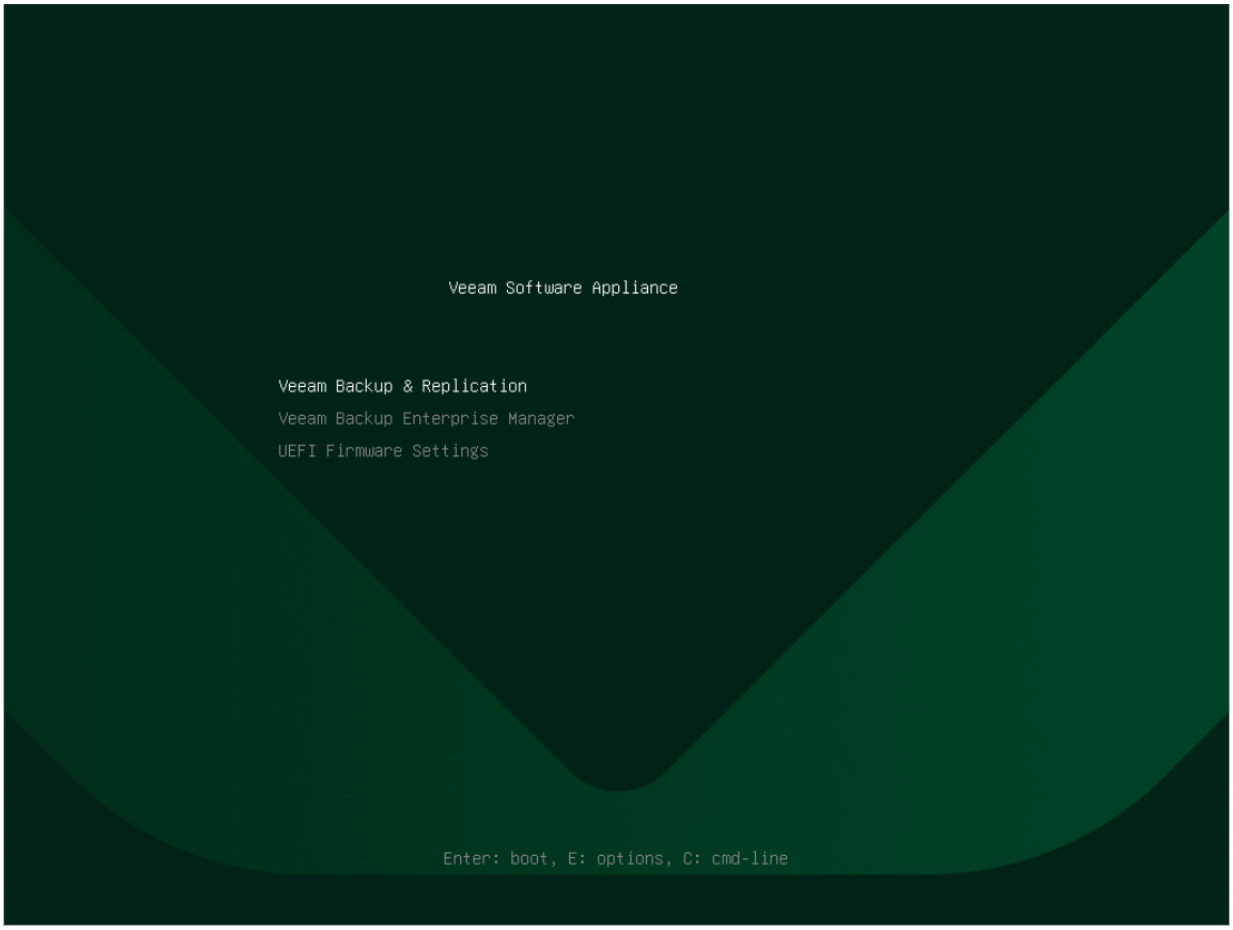
1. Download the latest version of the Veeam Software Appliance installation image from the Product Downloads page. The ISO is located under the **Hardened Software Appliance** tab.

   You must sign in with your Veeam account. If you do not have the account, register with your business email address.

2. Mount the ISO file to the machine where you plan to install Veeam Software Appliance or burn the ISO file to a flash drive or other removable storage device. If you plan to install Veeam Software Appliance on a virtual machine, use the built-in tools of the virtualization management software to mount the ISO file.

> **NOTE**
>
> To create a bootable USB stick, it is recommended that you use Rufus with the default settings. Note that you need to select **Write in DD Image mode** option when prompted.

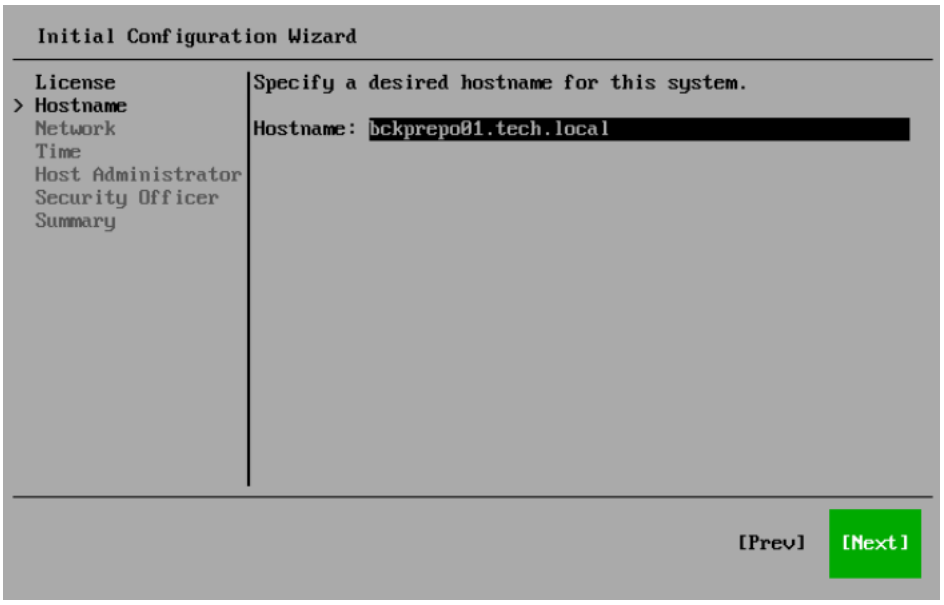
3. In the Boot Manager, select the drive where you mounted the ISO file and press [Enter].
4. In the installation menu, select **Veeam Backup & Replication** and press [Enter].



5. In the installation menu, select **Install** and press [Enter]. When the installer is loaded, confirm the operation and wait for the system to reboot automatically.
6. At the **License** step of the **Initial Configuration** wizard, read and accept Veeam license agreements and policies.

> **TIP**
>
> To close a document you have read, press [Q].

7. At the **Hostname** step of the **Initial Configuration** wizard, specify the a Fully Qualified Domain Name (FQDN) of the server and select **Next**.



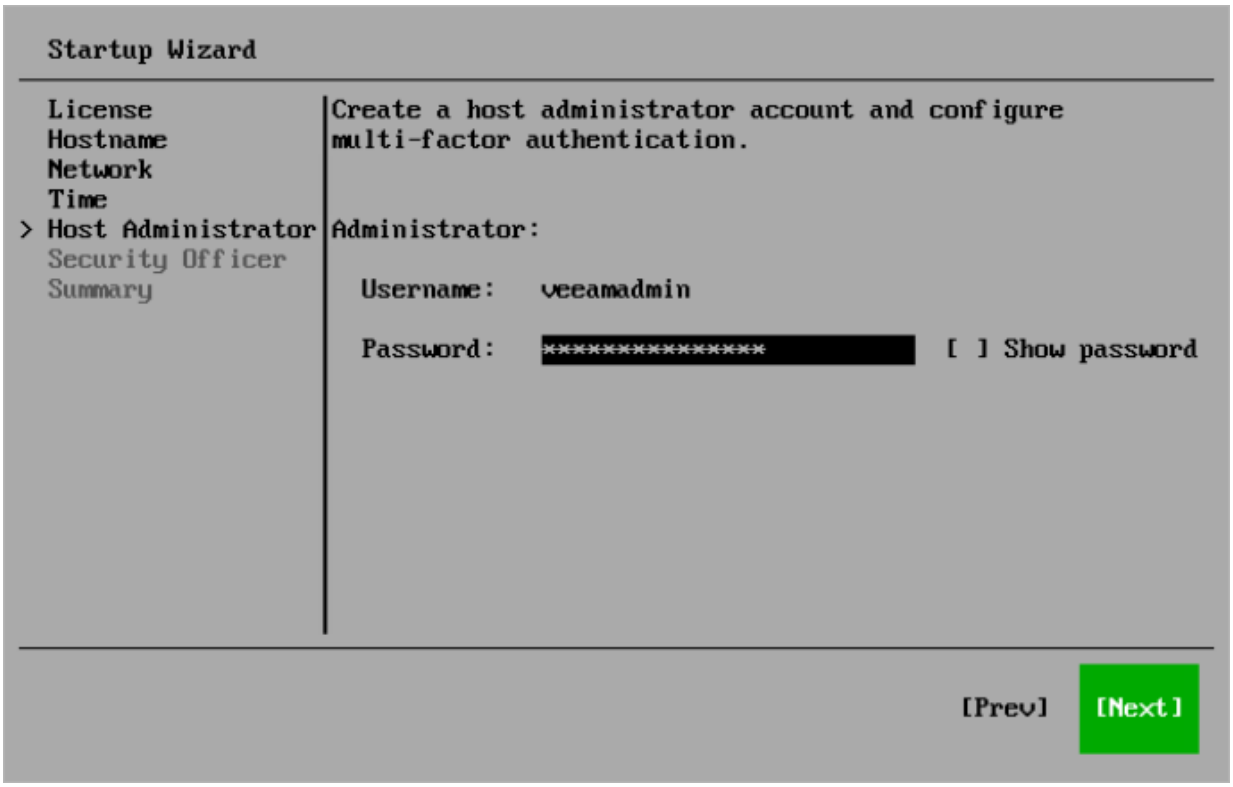
8. At the **Network** step of the **Initial Configuration** wizard, review the network configuration and select **Next**.
9. At the **Time** step of the **Initial Configuration** wizard, review server time configuration.

   By default, the UTC time zone is used. To specify another time zone, select **Change**.
10. At the **Host Administrator** step of the **Initial Configuration** wizard, configure the default host administrator account to perform administrator activities in the Host Management Console — *veeamadmin*. For more information about operations available for this role, see the Managing Users and Roles section in the Veeam Backup & Replication User Guide.

    In the **Password** field, specify the password for the *veeamadmin* user. The password must comply with the following requirements:

    - 15 characters minimum.
    - 1 upper case character.
    - 1 lower case character.
    - 1 numeric character.
    - 1 special character.

- No more than 3 characters of the same class in a row. For example, not more than 3 lowercase or 3 numerical characters in sequence.



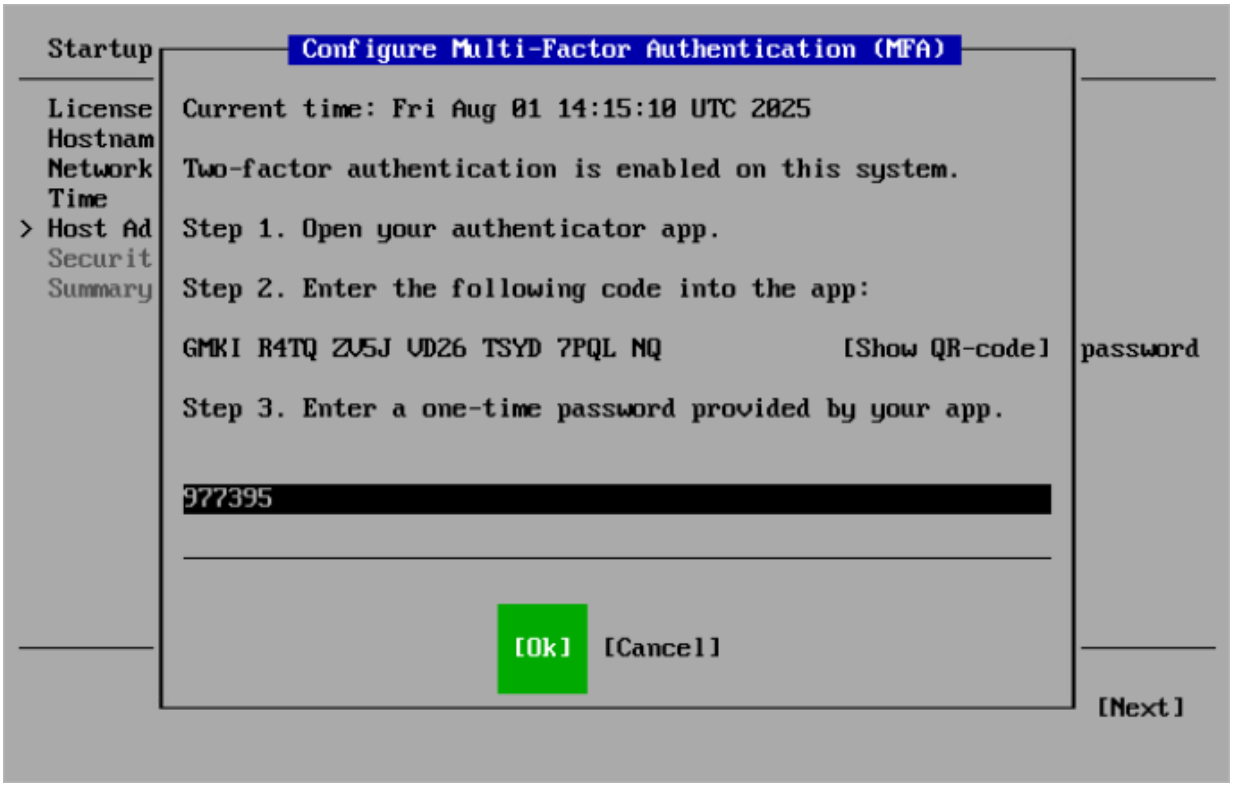
After you specify the password, select **Next** and configure multi-factor authentication (MFA):

a. Open your authentication application. Enter the code or scan the QR code.

b. Specify the one-time code provided by the application.

c. Press [Ok].

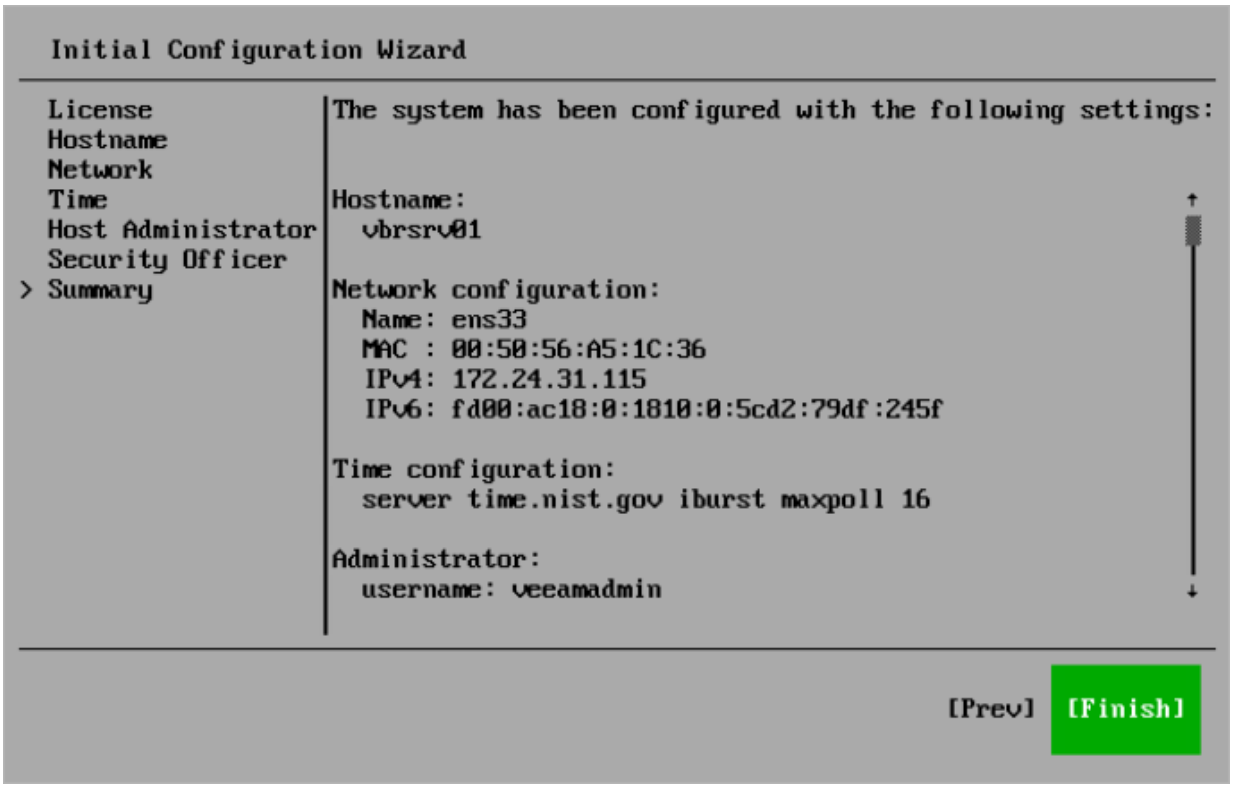
> **NOTE**
>
> Multi-factor authentication is compatible with mobile authentication applications that support RFC4226 and RFC6238.



11. At the **Security Officer** step of the **Initial Configuration** wizard, select **Skip setting up Security Officer** to skip configuring the security officer account.

> **TIP**
>
> The security officer account type provides an additional security layer to protect your infrastructure against malicious system administration. You can skip configuring this account to test the functionality of Veeam Backup & Replication. In the production environments, we recommend configuring this account. For more information about operations available for the security officer, see the Managing Users and Roles section in the Veeam Backup & Replication User Guide.

12. At the **Summary** step of the **Initial Configuration** wizard, review the system configuration and select **Finish**. The system will apply the configuration and restart required services.



After you finish the initial configuration, general information about the server will be displayed. You can use it to log in to the Host Management Console or Veeam Backup & Replication web UI and continue configuring Veeam Software Appliance and Veeam Backup & Replication.

Reference

For details on how to configure the backup server deployed from Veeam Software Appliance, see the Configuring Veeam Appliances section in the Veeam Backup & Replication User Guide.

Microsoft Windows

To install Veeam Backup & Replication, do the following:

1. Download the latest version of the Veeam Backup & Replication installation image from the Download Veeam products page.

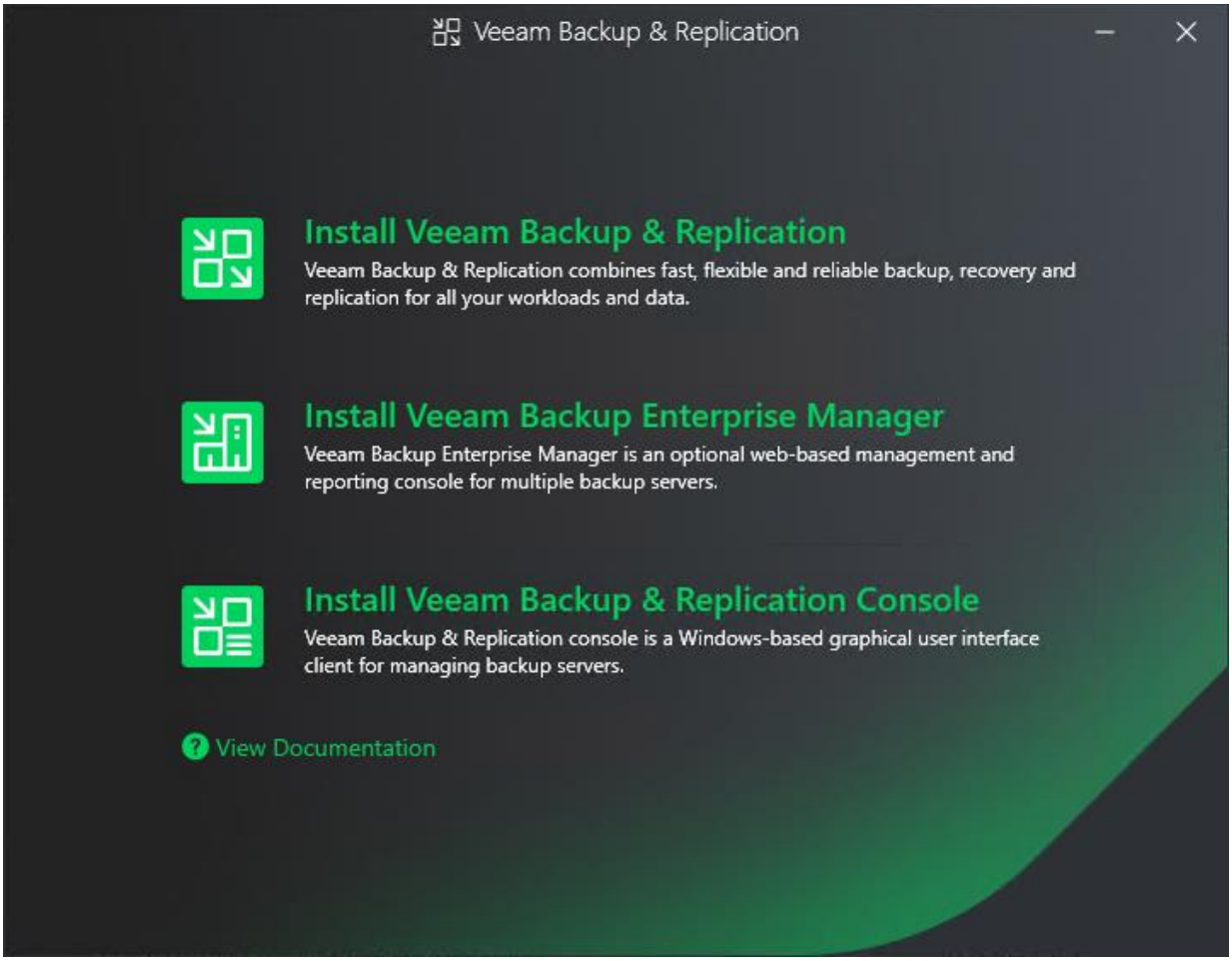
   You must sign in with your Veeam account. If you do not have the account, register with your business email address.

2. Mount the installation image to the machine on which you plan to install Veeam Backup & Replication or burn the image file to a flash drive or other removable storage device.

   If you plan to install Veeam Backup & Replication on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM.

3. Run the `Setup.exe` file from the image or disk to open the splash screen.

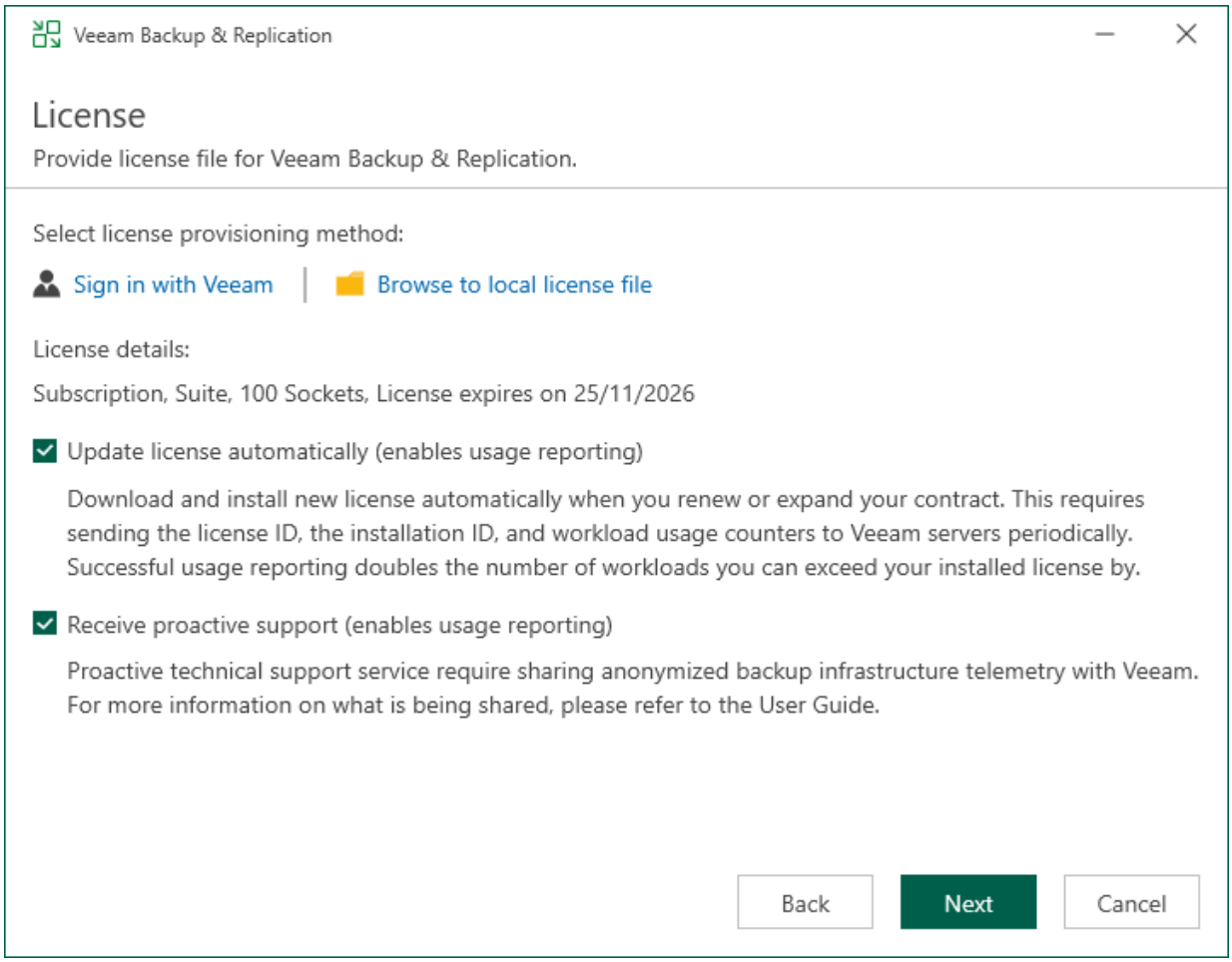
4. In the window, click **Install Veeam Backup & Replication**.



5. At the **License Agreement** step of the wizard, read the license agreements and click **I Accept**.

6. At the **License** step of the wizard, specify the path to the license key.

   If you skip this step, Veeam Backup & Replication will operate in the Community edition mode. You can switch to the full version of the product if you install the license. For more information, see Veeam Backup & Replication Community Edition.



7. At the **System Configuration Check** step of the wizard, install missing software components, if any.

   > **NOTE**
   >
   > If all required components are already installed on the machine, the **System Configuration Check** step is skipped.

8. At the **Ready to Install** step of the wizard, click **Install** to begin the installation.

Step 2. Installing Veeam Backup & Replication Console

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. Install the Veeam Backup & Replication console on a dedicated Windows server to access the backup server remotely.

[For Veeam Backup & Replication on Microsoft Windows] By default, the Veeam Backup & Replication console is installed on the backup server automatically when you install Veeam Backup & Replication. You do not need to install the console manually. However, in addition to the default console, you can install the Veeam Backup & Replication console on a dedicated machine to access the backup server remotely.

Before You Begin

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

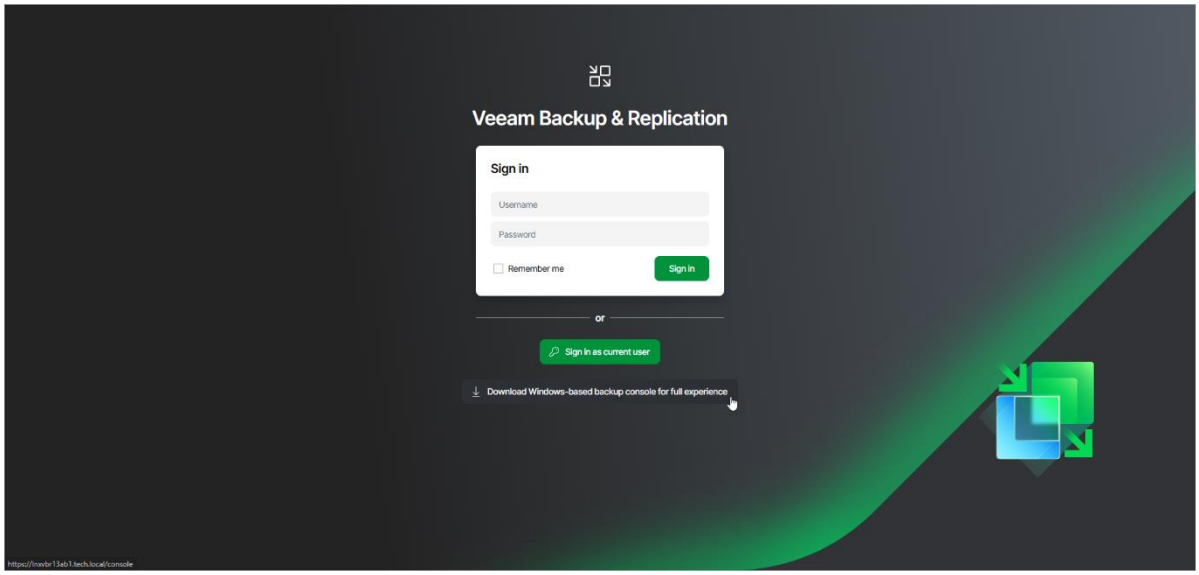
- The machine on which you plan to install the Veeam Backup & Replication console must meet the system requirements. For more information, see System Requirements.
- The account used to install the Veeam Backup & Replication console must have the local Administrator permissions on the machine where the console will be installed. After installation, users can have standard (non-administrative) privileges to connect to the console.
- The Veeam Backup & Replication console must be of the same version as Veeam Backup & Replication installed on the backup server.
- The system time on both the backup server and the console must be synchronized with an external time source, such as a Network Time Protocol (NTP) server.

Installing Veeam Backup & Replication Console

To install the Veeam Backup & Replication console, do the following:

1. Start the console installation:
    - [For Veeam Backup & Replication on Linux] In the browser address bar, enter `https://<VBR-Host-Name>:443`, replacing *<VBR-Host-Name>* with the IP address of your backup server. This will open the web UI. Download the Veeam Backup & Replication Console installer. Run the downloaded installer package.

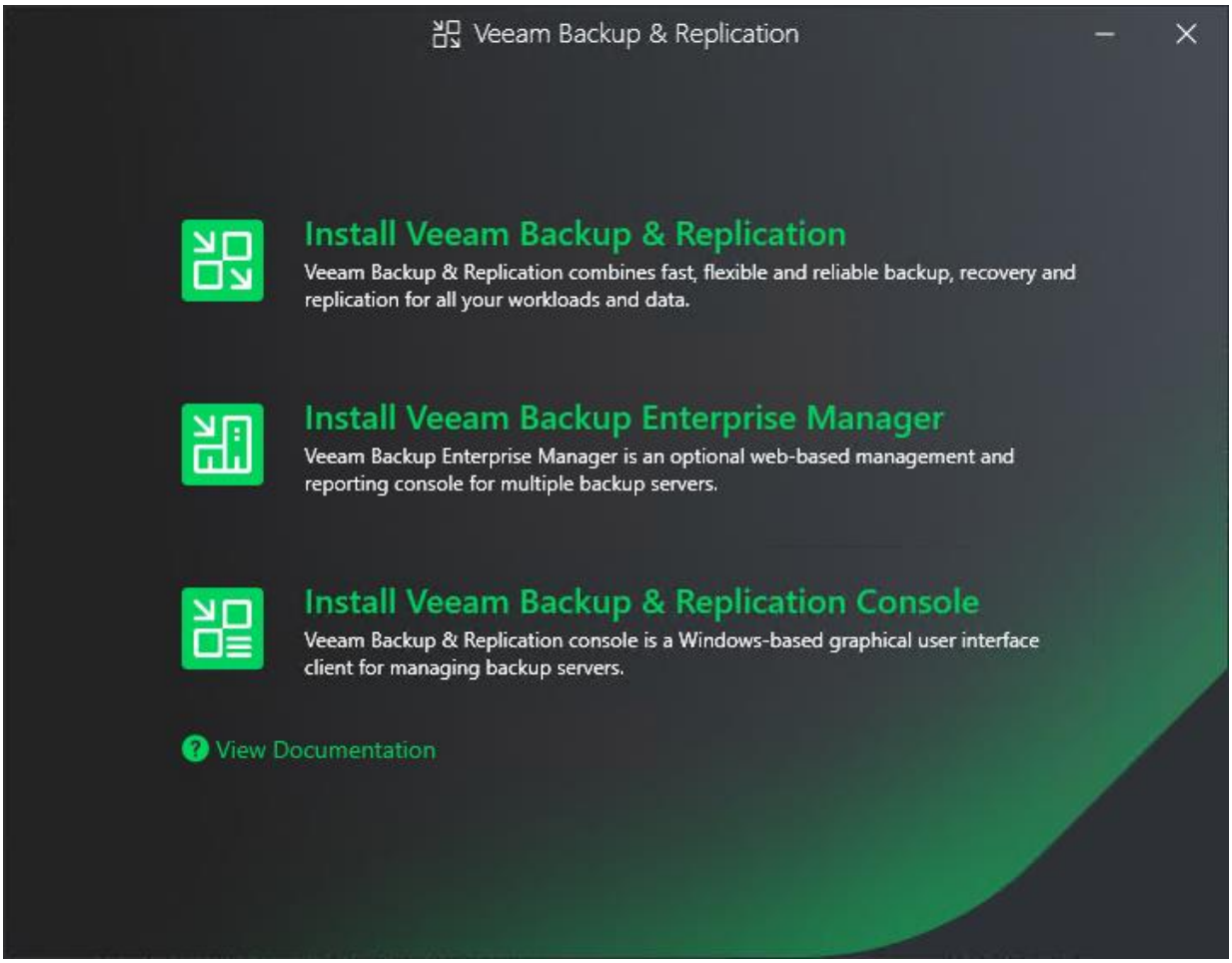
      > **TIP:**
      >
      > You can also specify the backup server name if the server is added to the domain as described in the Managing Domain Settings section in the Veeam Backup & Replication User Guide. For the simplicity, we skip this procedure in this guide.



- [For Veeam Backup & Replication on Microsoft Windows] Mount the installation image downloaded at step 1 of the deployment process to the machine on which you plan to install the Veeam Backup & Replication console or burn the image file to a flash drive or other removable storage device. If you plan to install the Veeam Backup & Replication console on a VM, use built-in tools of the virtualization management software to mount the installation image to the VM. Run the Setup.exe file from the image or disk. In the splash screen, click **Install**.



2. At the **Select Veeam Backup & Replication Component** step of the wizard, select **Install Veeam Backup & Replication Console**.



3. At the **License Agreement** step of the wizard, read the license agreements and click **I Accept**.
4. At the **System Configuration Check** step of the wizard, the setup wizard checks if the required software is installed on the machine. If some of the required components are missing, the setup will try to install them automatically. After the components are successfully installed, reboot is required. To reboot the machine, click **Reboot**.

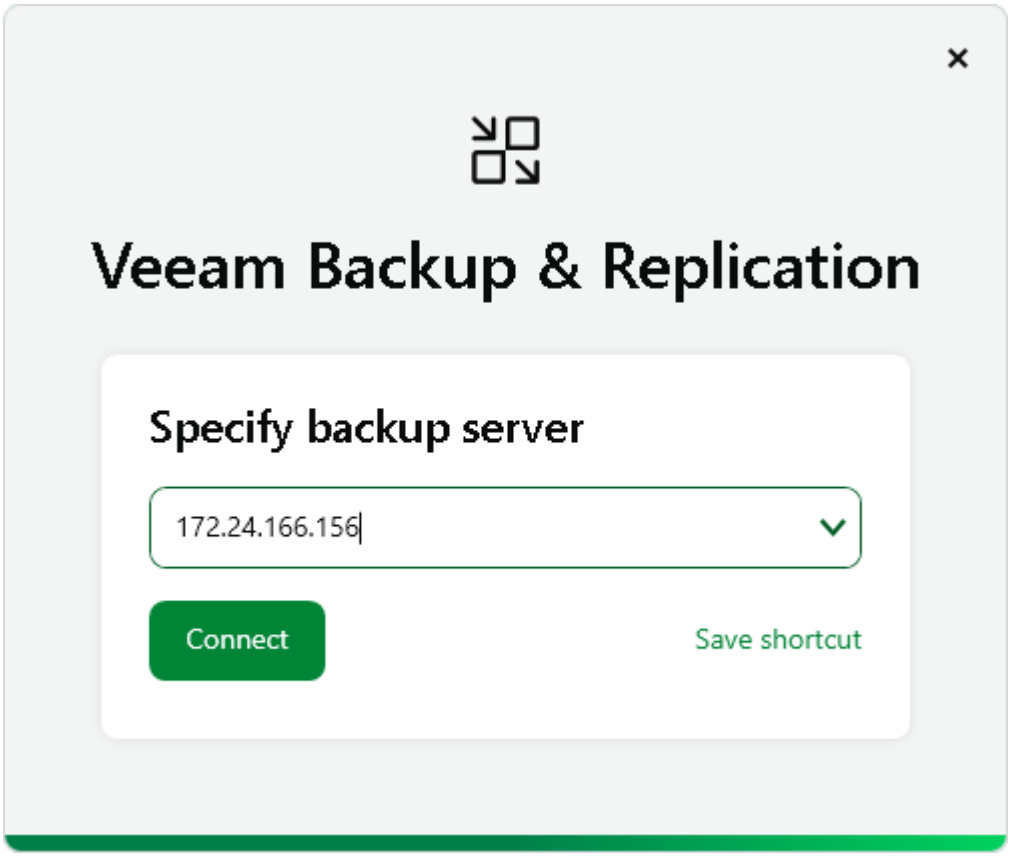
   If the setup wizard cannot install some of the required software components automatically, install them manually and click **Retry**.
5. At the **Ready to Install** step of the wizard, click **Install**.

Accessing Veeam Backup & Replication Console

To start Veeam Backup & Replication, do the following:

1. In the Microsoft Windows **Start** menu, select **Apps** > **Veeam** > **Veeam Backup & Replication Console**.
2. At the **Specify backup server** step, type the IP address of the backup server. Click **Connect**.

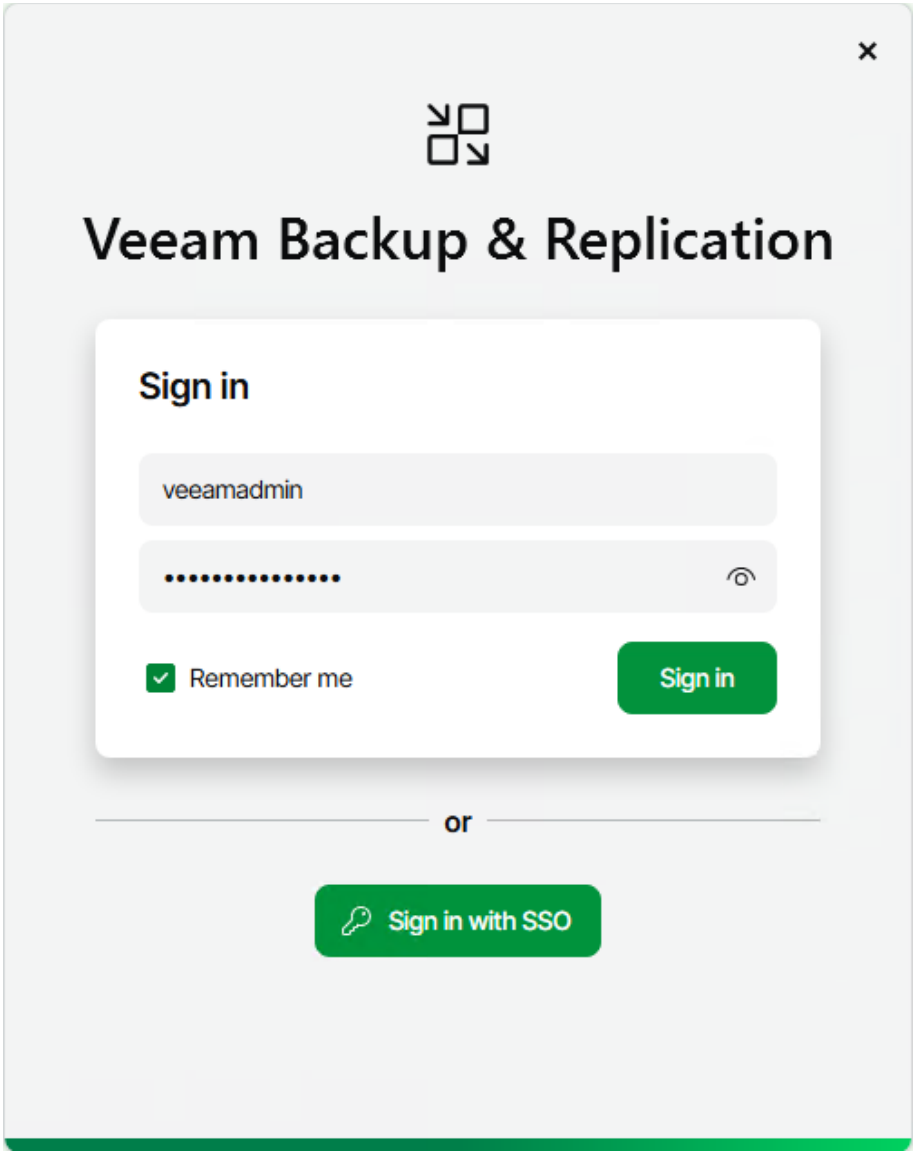
> **TIP**
>
> You can also specify the backup server name if the server is added to the domain. For information on how to configure the Linux-based backup server, see the Managing Domain Settings section in the Veeam Backup & Replication User Guide.



3. At the **Server certificate** step, select if you trust the server certificate. Click **Yes**.

4. At the **Sign in** step, enter the credentials of the user account that you want to use to connect to the backup server. Click **Sign-in**.

   For the Linux-based backup server, you can use the *veeamadmin* account configured during installation. For the Microsoft Windows-based backup server, you can use an account with the local Administrator permissions on the backup server.



After the Veeam Backup & Replication console opens, it will suggest you to install the license. In the **License** window, click **Browse** and select the license file. Some features of Veeam Backup & Replication can be not available without the proper license. For more information, see the Licensing section in the Veeam Backup & Replication User Guide.

Reference

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

Step 3. Adding VMware vSphere Virtual Infrastructure Servers

To protect VMware vSphere virtual machines with Veeam Backup & Replication, you must add the virtual infrastructure servers hosting these machines to the backup infrastructure.

You can add vCenter Servers and ESXi hosts. If an ESXi host is managed by a vCenter Server, it is recommended that you add the vCenter Server, not a standalone ESXi host.

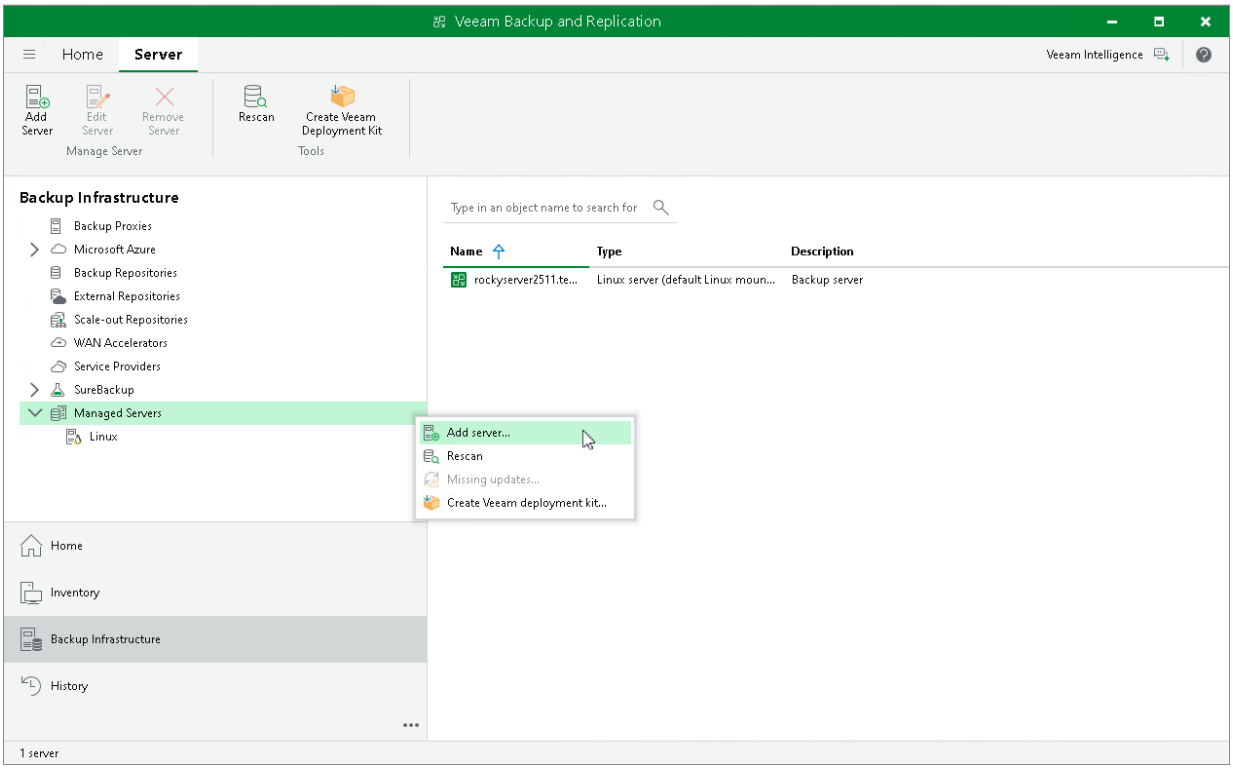
Before You Begin

- Make sure that the version of your VMware vSphere platform is supported. For details, see the Platform Support section in the Veeam Backup & Replication User Guide.
- The user account used to add the server, must have root permissions on the ESXi host. For details, see the Permissions section in the Veeam Backup & Replication User Guide.

Adding Infrastructure Server

To add the server, do the following:

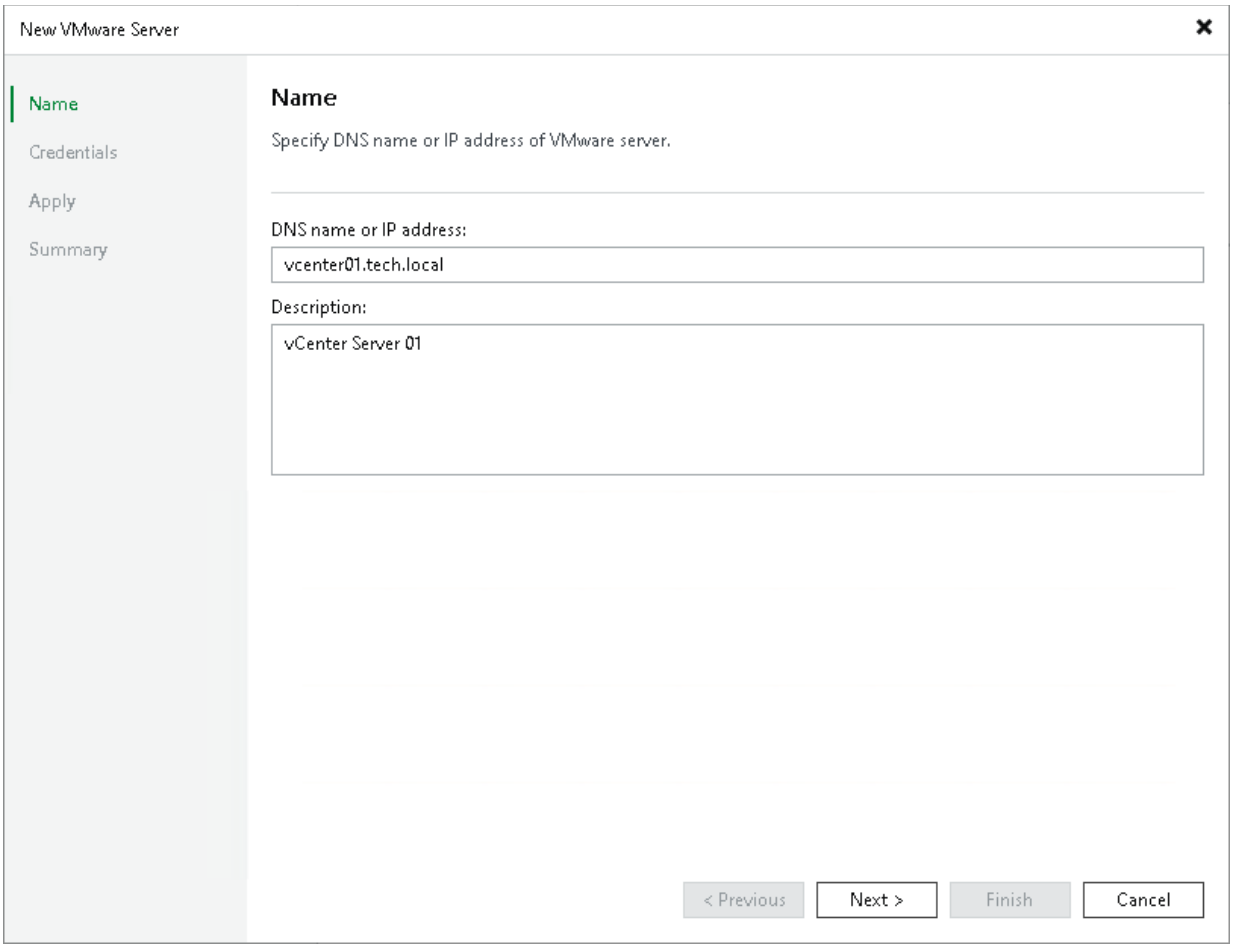
1. In the inventory pane of the **Backup Infrastructure** view, right-click the **Managed Servers** node and select **Add Server**.



2. In the **Add Server** window, click **VMware vSphere** > **vSphere** to launch the **New VMware Server** wizard.

3. At the **Name** step of the wizard, specify the DNS name or IP address of the server.

   Note that you can use IPv6 addresses only if IPv6 communication is enabled as described in the IPv6 Support section in the Veeam Backup & Replication User Guide.



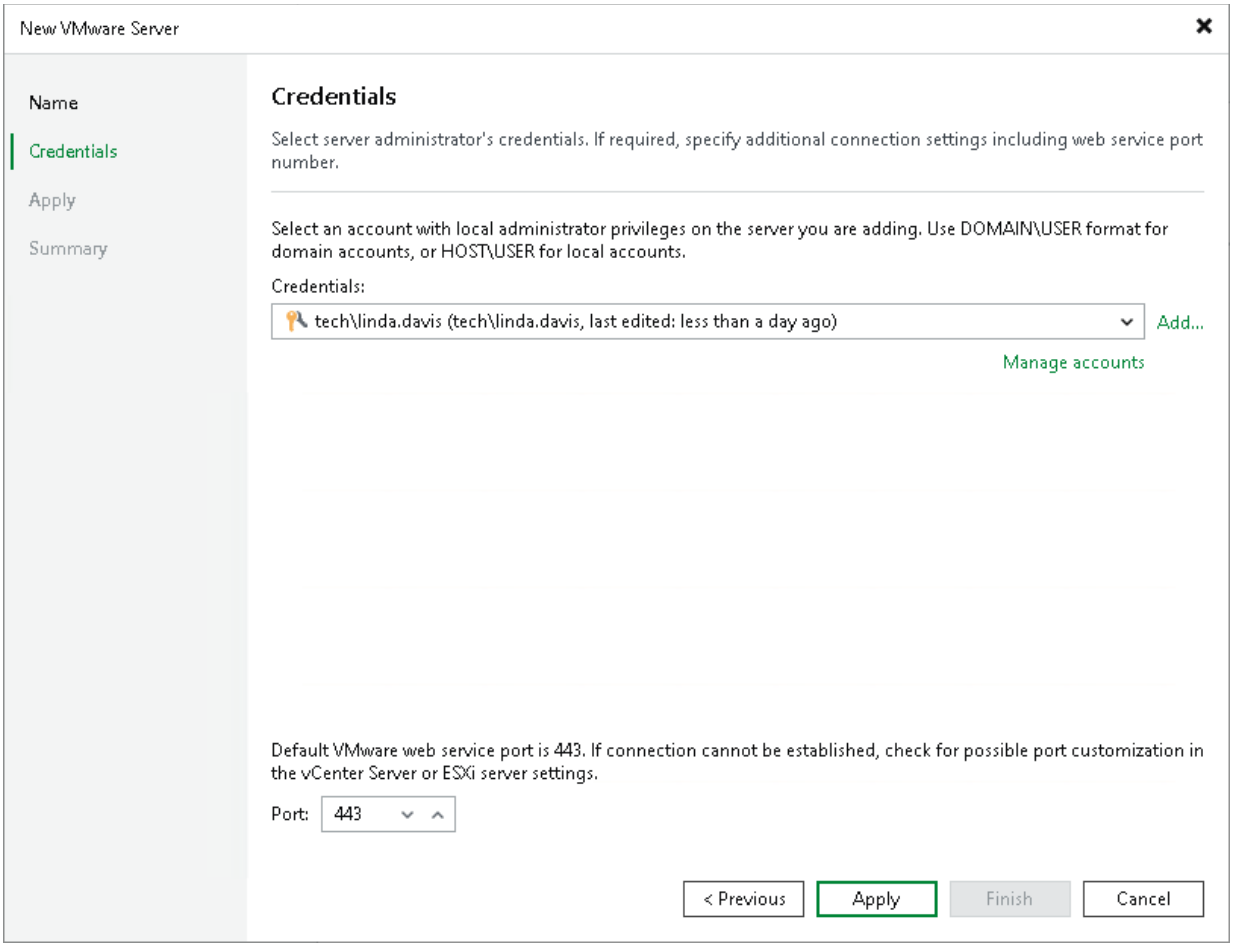
4. At the **Credentials** step of the wizard, specify credentials for the user account with Administrator permissions on the added server.

   To add the account, do the following:

   a. Click **Add**.

   b. In the **Credentials** window, specify the username and password used to connect to the added server.

c. Click **OK**.



5. Follow the next steps of the wizard. At the **Summary** step, click **Finish**.
6. Open the **Backup Infrastructure** view and click the **Managed Servers** node. The added server will be available in the working area.

Reference

For details on adding virtual infrastructure servers, see the Virtualization Servers and Hosts section in the Veeam Backup & Replication User Guide.

Step 4. Adding Microsoft Hyper-V Virtual Infrastructure Servers

To protect Microsoft Hyper-V virtual machines with Veeam Backup & Replication, you must add the virtual infrastructure servers hosting these machines to the backup infrastructure.

You can add standalone Hyper-V hosts, Hyper-V clusters or SCVMM servers. If a Hyper-V host is a part of a cluster, it is recommended that you add the cluster, not a standalone Hyper-V host, to the backup infrastructure.

Before You Begin

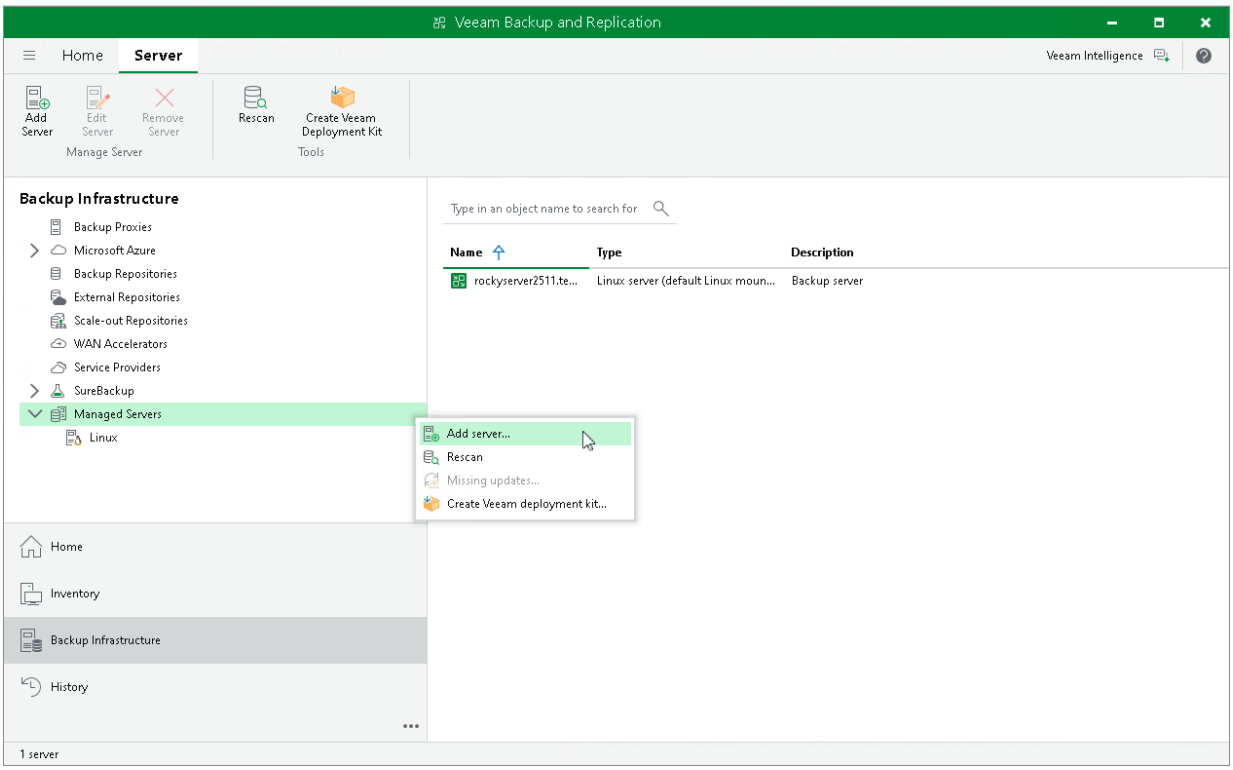
Check the following prerequisites:

- The version of your Microsoft Hyper-V platform must be supported. For details, see the Platform Support section in the Veeam Backup & Replication User Guide.
- You must enable file and printer sharing in the network connection settings of the host. Without sharing enabled, Veeam Backup & Replication fails to deploy the required components.
- The user account used to add the server, must have administrator privileges on the Hyper-V host. For details, see the Permissions section in the Veeam Backup & Replication User Guide.
- For the full list of requirements, see the Adding Microsoft Hyper-V Servers section in the Veeam Backup & Replication User Guide.

Adding Infrastructure Server

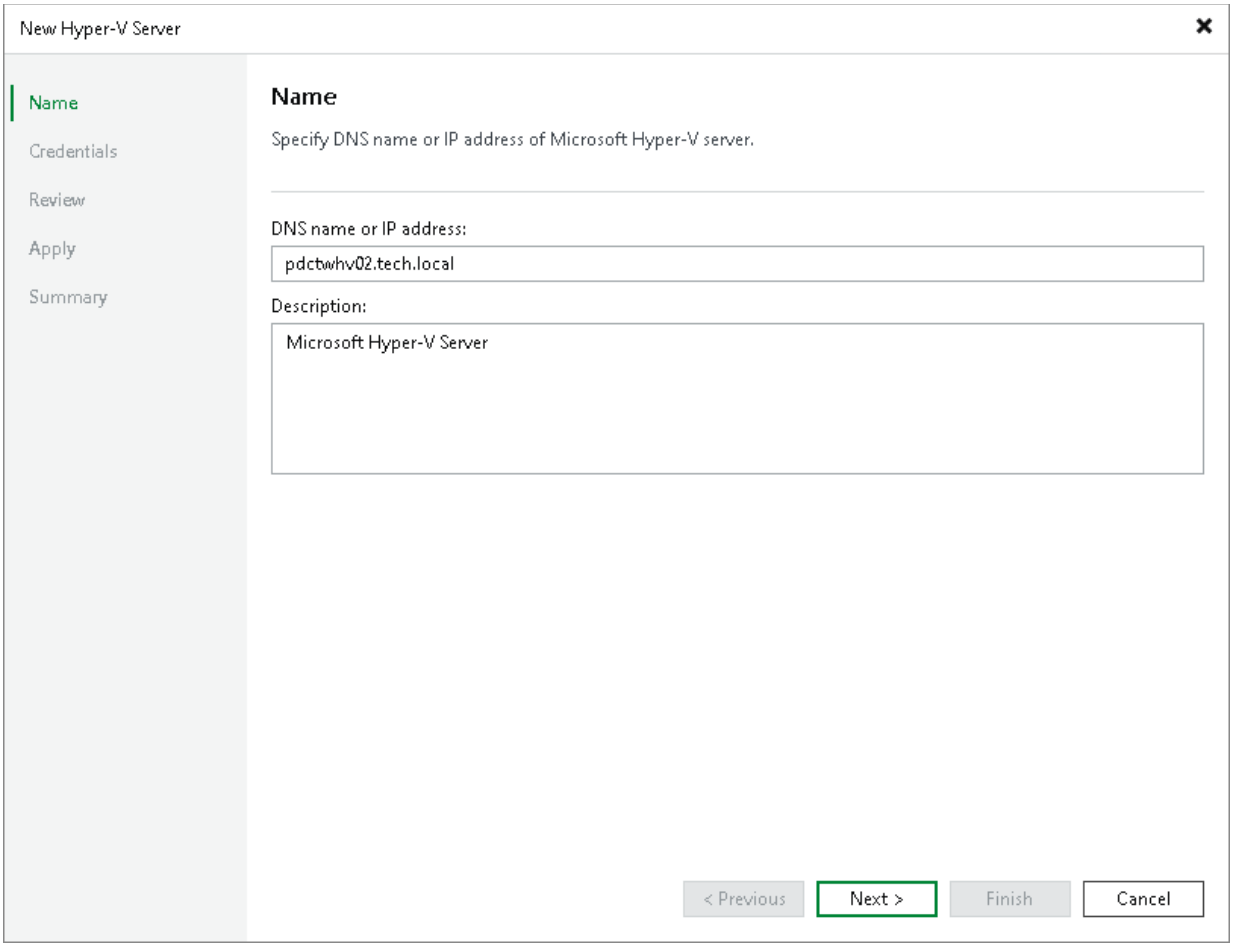
To add the server, do the following:

1. In the inventory pane of the **Backup Infrastructure** view, right-click the **Managed Servers** node and select **Add Server**.



2. In the **Add Server** window, click **Microsoft Hyper-V** > **Hyper-V** > **Microsoft Hyper-V Server** to add a standalone Hyperv-V host.

3. At the **Name** step of the wizard, specify the DNS name or IP address of the server.



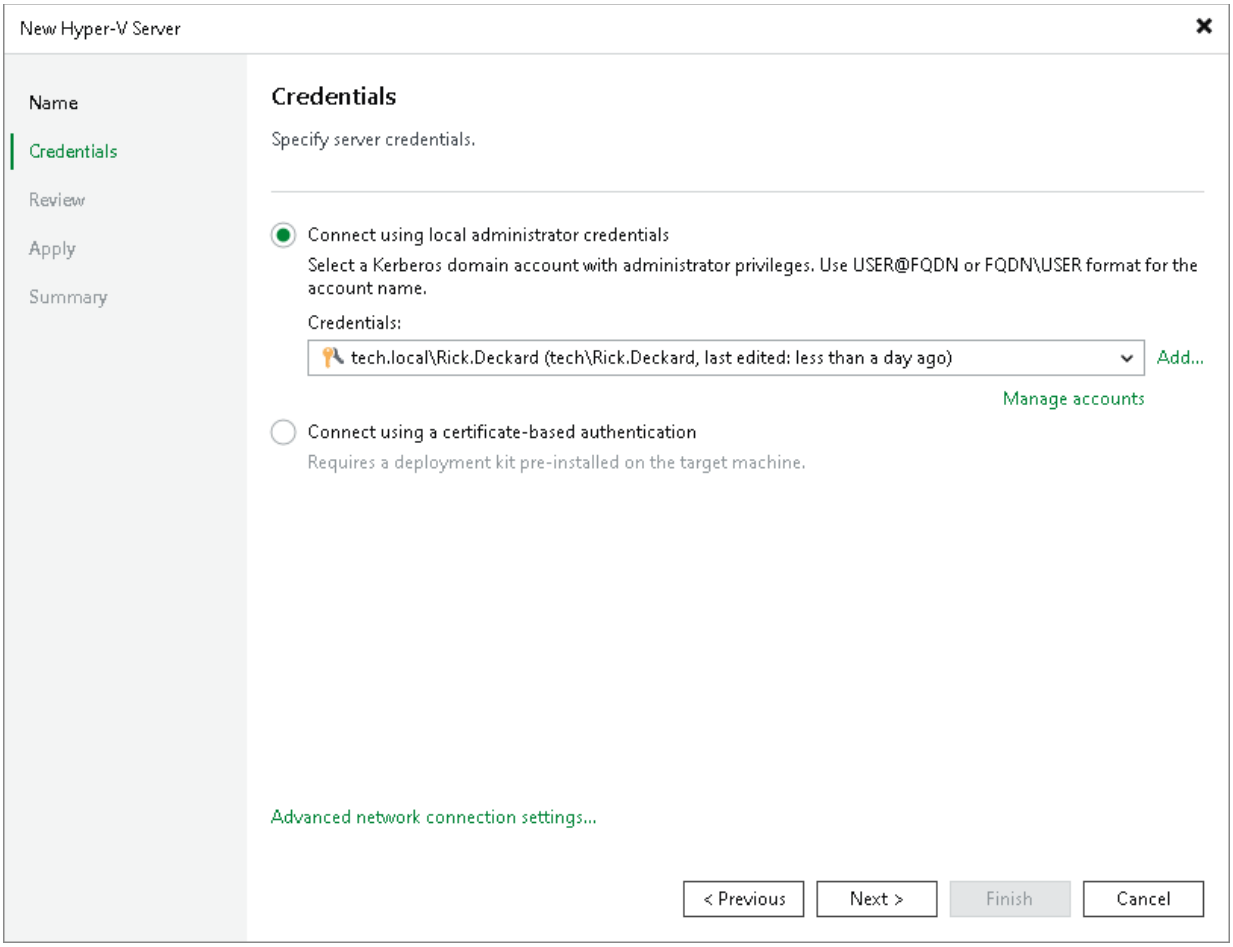
4. At the **Credentials** step of the wizard, specify credentials for the user account with Administrator permissions on the added server.

   To add the account, do the following:

   a. Click **Add**.

   b. In the **Credentials** window, specify the username and password used to connect to the added server.

c. Click **OK**.



5. Follow the next steps of the wizard. At the **Summary** step, click **Finish**.
6. Open the **Backup Infrastructure** view and click the **Managed Servers** node. The added server will be available in the working area.

Reference

For details on adding virtual infrastructure servers, see the Virtualization Servers and Hosts section in the Veeam Backup & Replication User Guide.

Step 5. Configuring VMware Backup Proxy

The VMware backup proxy retrieves data from the production storage, compresses, deduplicates and sends it to the backup repository. This proxy is used for the VMware vSphere infrastructure.

To configure the VMware backup proxy, you must add a Microsoft Windows or Linux server and assign the role of the backup proxy to it. In this section, you will learn how to add a Microsoft Windows proxy.

> **TIP**
>
> For Linux-based components, Veeam Backup & Replication provides Veeam Infrastructure Appliance — a bundle that includes the preconfigured Rocky Linux distribution and required Veeam components and services. For the full list of the roles that can be assigned to a Linux server deployed from Veeam Infrastructure Appliance, see the Considerations and Limitations section in the Veeam Backup & Replication User Guide.

Before You Begin

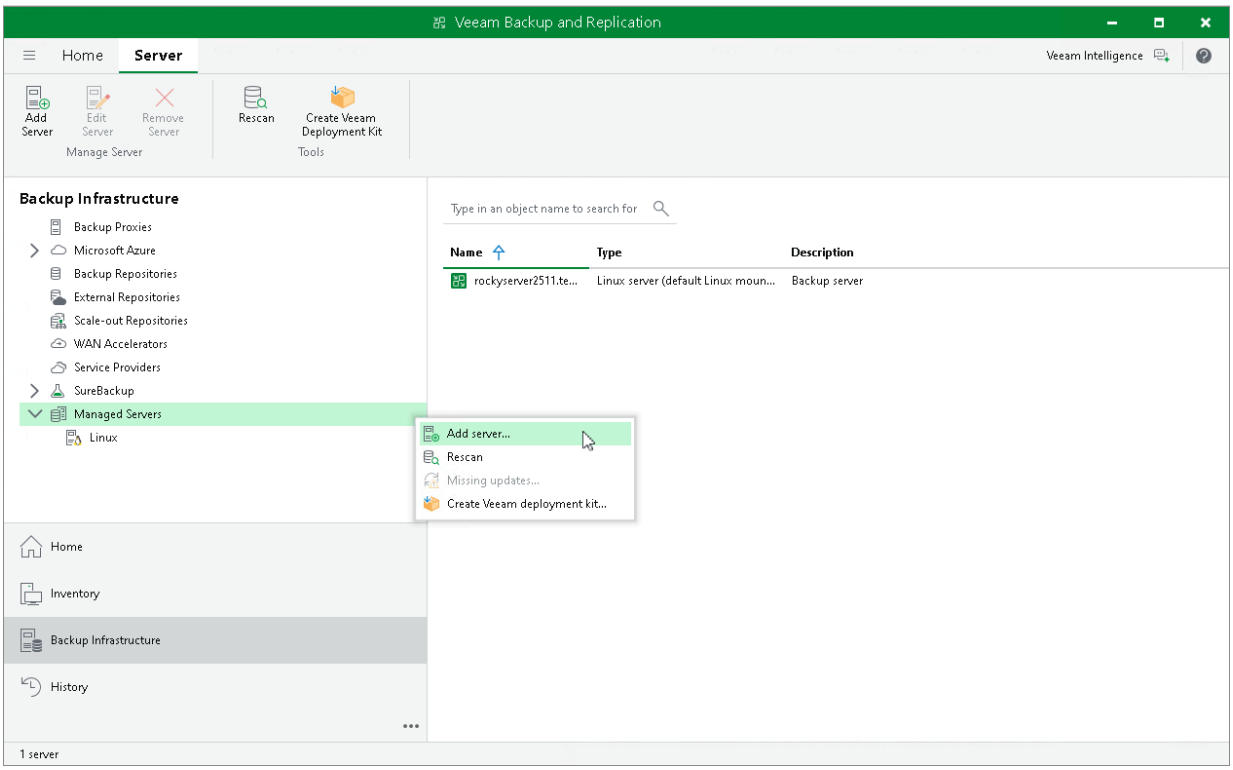
Check the following prerequisites:

- The machine that you plan to use as the VMware backup proxy must meet system requirements. For details, see the System Requirements section in the Veeam Backup & Replication User Guide.
- The machine must have access to the backup server, source datastore and backup repository.
- File and printer sharing must be enabled in network connection settings of the added Microsoft Windows machine. On this machine, Veeam Backup & Replication deploys the required components. Without sharing enabled, Veeam Backup & Replication fails to deploy these components.

Adding Server

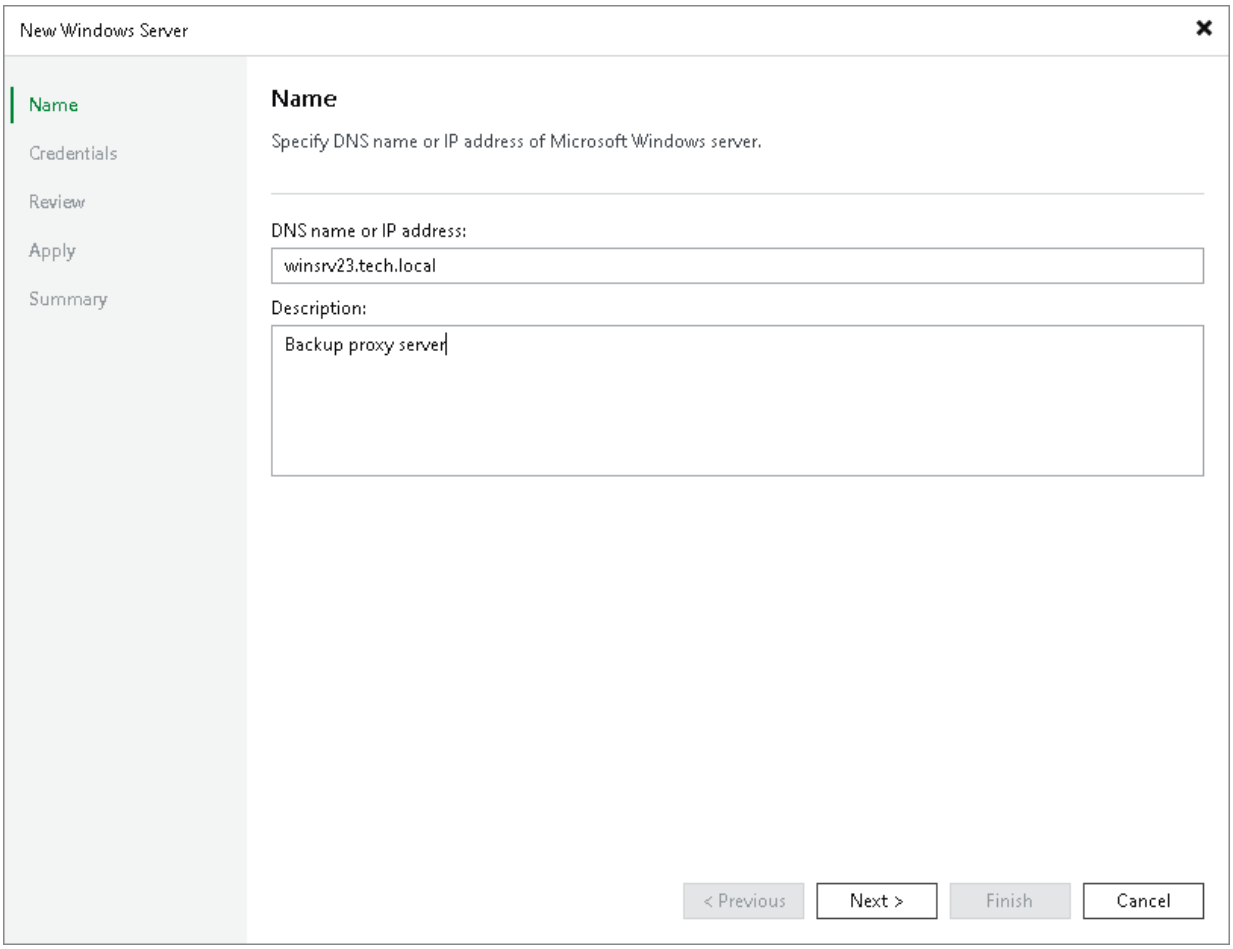
To add a server, do the following:

1. In the inventory pane of the **Backup Infrastructure** view, right-click the **Managed Servers** node and select **Add Server**.



2. In the **Add Server** window, click **Microsoft Windows** to launch the **New Windows Server** wizard.

3. At the **Name** step of the wizard, specify the DNS name or IP address of the server that will perform the role of the VMware backup proxy.



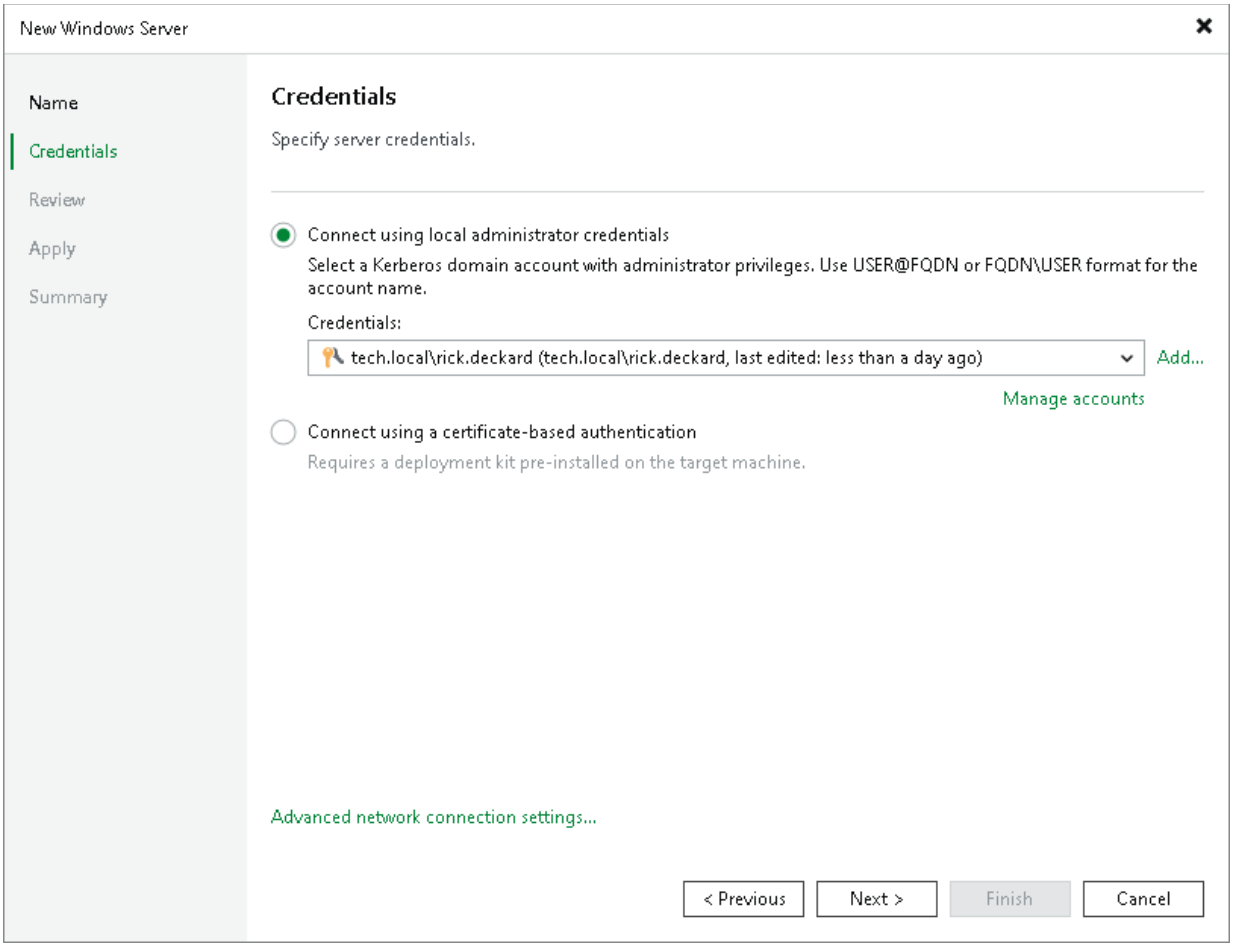
4. At the **Credentials** step of the wizard, specify credentials for the user account with Administrator permissions on the added server.

   To add the account, do the following:

   a. Click **Add**.

   b. Specify the username and password used to connect to the added server.

c. Click **OK**.



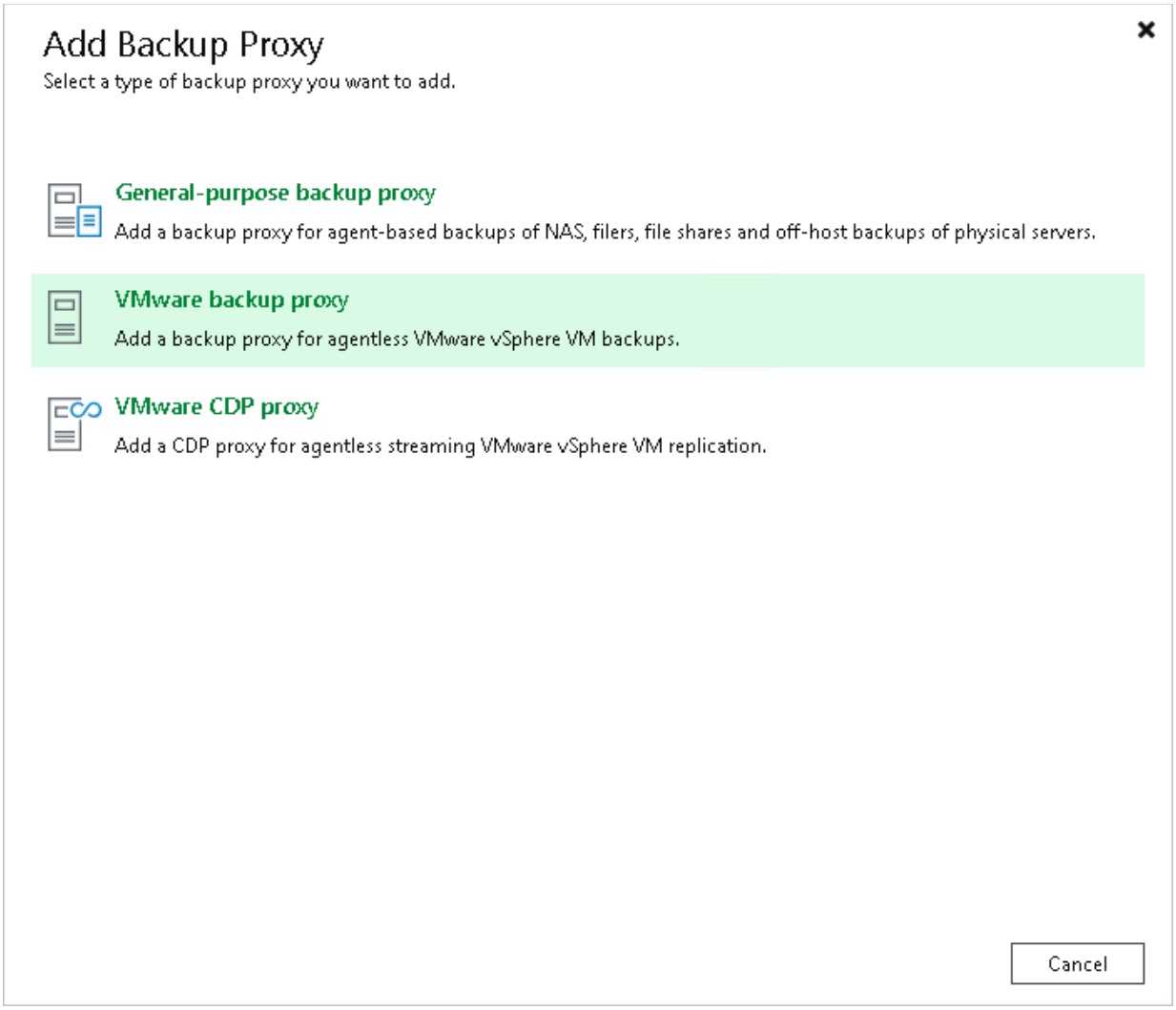
5. Follow the next steps of the wizard. At the **Summary** step of the wizard, click **Finish**.
6. Open the **Backup Infrastructure** view and click the **Managed Servers** node. The added server must be available in the working area.

Assigning VMware Backup Proxy Role to Added Server

To assign the role of the VMware backup proxy:

1. In the inventory pane of the **Backup Infrastructure** view, right-click the **Backup Proxies** node and select **Add Proxy**.

2. In the **Add Backup Proxy** window, select **VMware backup proxy**.

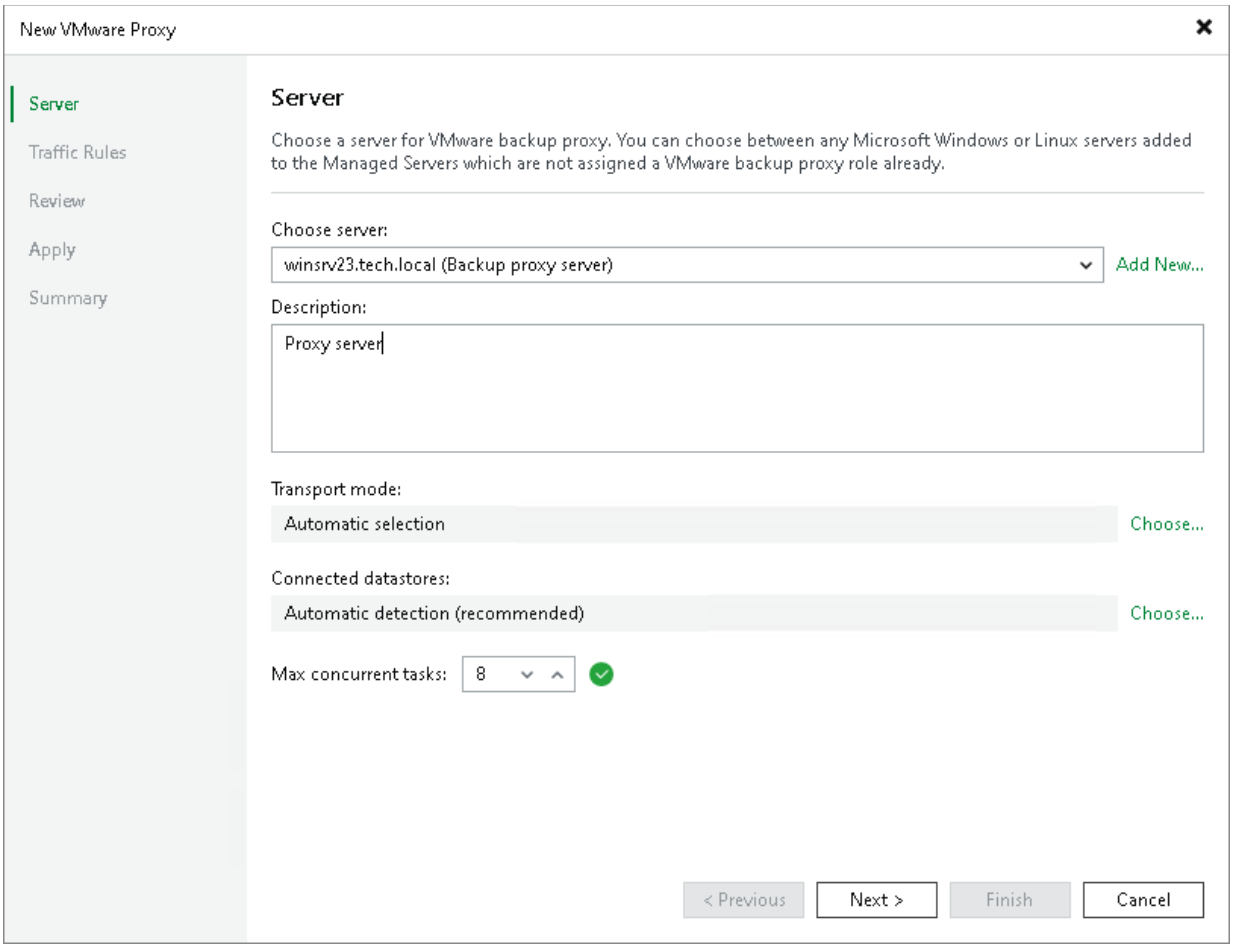


3. At the **Server** step of the wizard, do the following:
   - In the **Choose server** list, select the server that you have added.
   - In the **Transport mode** field, leave the **Automatic selection** option selected.

     Veeam Backup & Replication will analyze the VMware backup proxy configuration, define to which datastores it has access and automatically select the best way to retrieve and restore data depending on the type of connection between the VMware backup proxy and the source datastore.

- In the **Connected datastores** field, leave the **Automatic detection** option selected.

  Veeam Backup & Replication will detect datastores to which the VMware backup proxy has a direct SAN or NFS connection.



4. At the **Traffic Rules** step of the wizard, keep the default settings.

   Network traffic throttling rules help you manage bandwidth usage and minimize impact of data protection and disaster recovery tasks on network performance. Setting up traffic throttling is not described in this guide. For details, see the Network Traffic Management section in the Veeam Backup & Replication User Guide.

5. At the **Apply** step of the wizard, click **Next** and then **Finish** to exit the wizard.

6. Open the **Backup Infrastructure** view and click the **Backup Proxies** node. The added VMware backup proxy must be available in the working area.

Reference

For details on the VMware backup proxy, see the VMware Backup Proxy section in the Veeam Backup & Replication User Guide.

Step 6. Configuring Backup Proxy

The backup proxy compresses, deduplicates and sends data to the backup repository. In the Microsoft Hyper-V infrastructure, the role of the backup proxy is assigned to the host by default. The on-host backup proxy does not need any manual configuration.

You can deploy an off-host backup proxy to remove unwanted overhead on the production Hyper-V host. The off-host backup proxy is used in complicated scenarios, that is why we omit its configuration in this guide. For more information, see the Off-Host Backup Proxy section in the Veeam Backup & Replication User Guide.

Step 7. Configuring Backup Repository

The backup repository is a storage where Veeam Backup & Replication keeps backup files and, in case of replication, metadata for replicated VMs. You can use different types of storage as the backup repository. The full list of storage types is available in the Backup Repository section in the Veeam Backup & Replication User Guide.

In this section, you will learn how to use a Microsoft Windows server as the backup repository. To configure the backup repository, you must add the server to the backup infrastructure and assign the role of the backup repository to it.

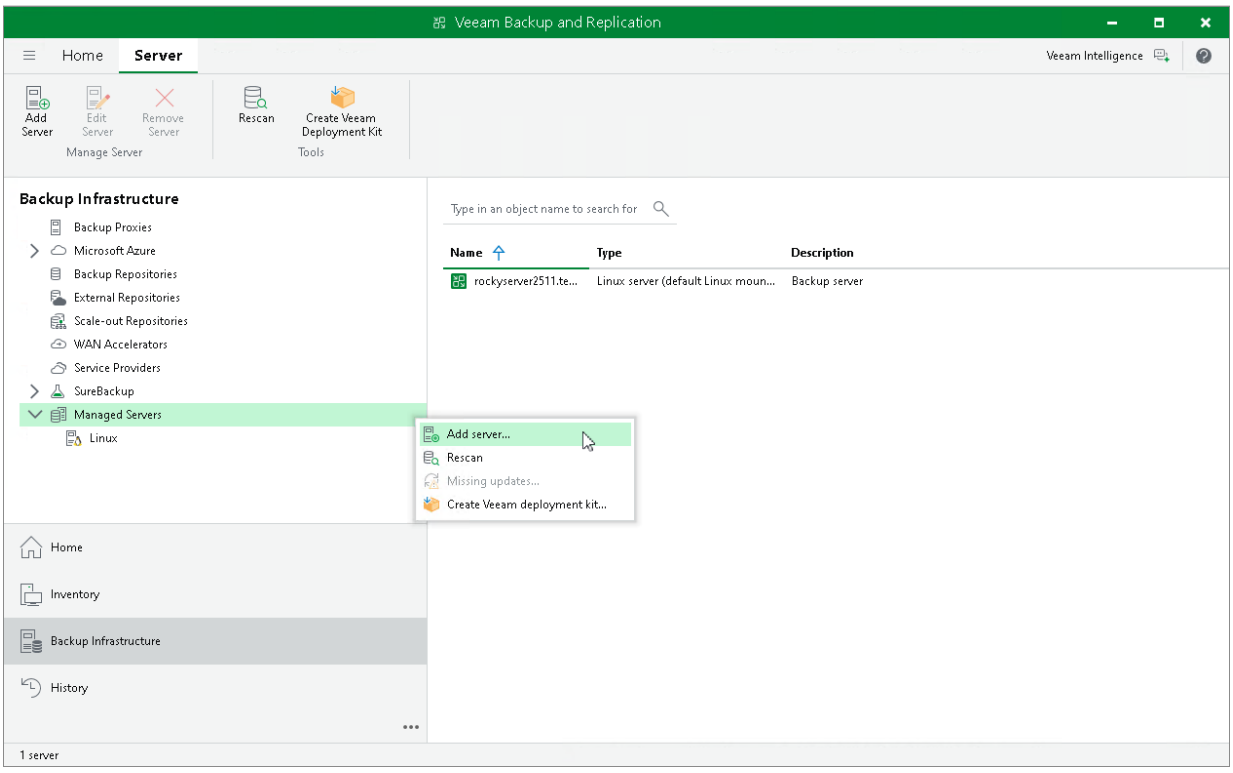
Before You Begin

The Microsoft Windows machine that you plan to use as a backup repository must meet system requirements. For details, see the System Requirements section in the Veeam Backup & Replication User Guide.

Adding a Server

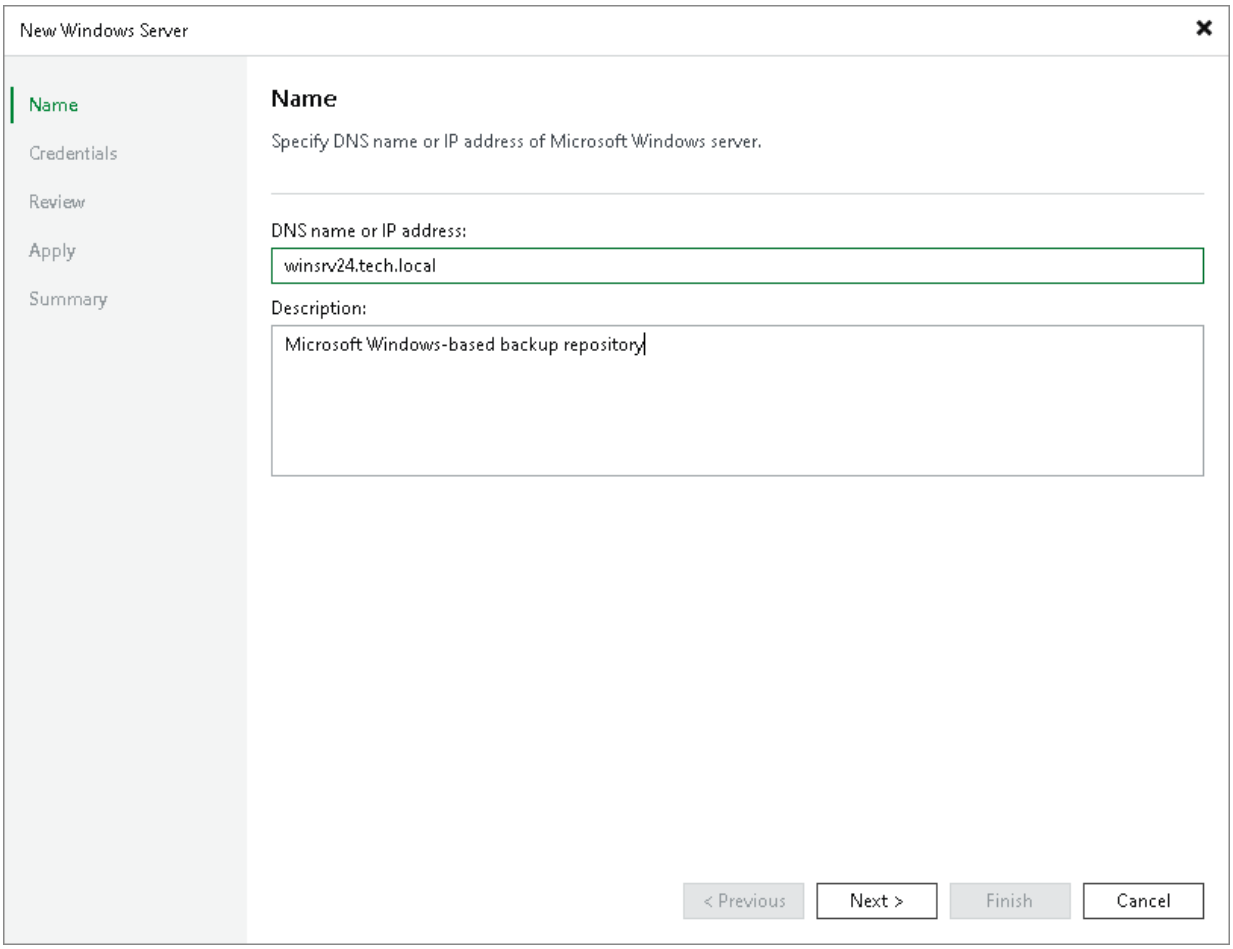
To add a server to the Veeam Backup & Replication infrastructure, do the following.

1. In the inventory pane of the **Backup Infrastructure** view, right-click the **Managed Servers** node and select **Add Server**.



2. In the **Add Server** window, select **Microsoft Windows** to launch the **New Windows Server** wizard.

3. At the **Name** step of the wizard, specify the DNS name or IP address of the server that will perform the role of the backup repository.



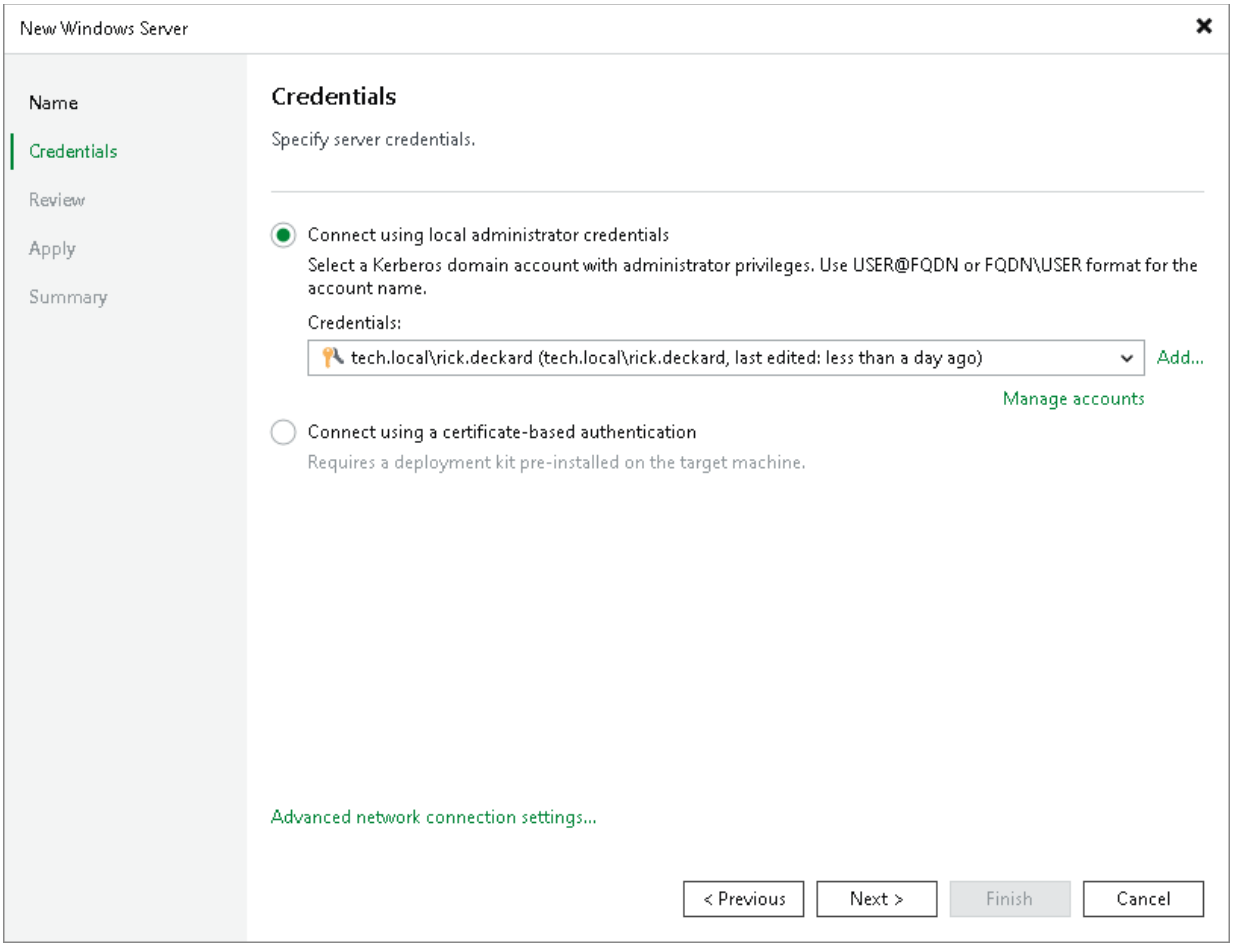
4. At the **Credentials** step of the wizard, enter credentials for the user account with local Administrator permissions to the added server.

   To add the account, do the following:

   a. Click **Add**.

   b. Specify the username and password used to connect to the added server.

c. Click **OK**.



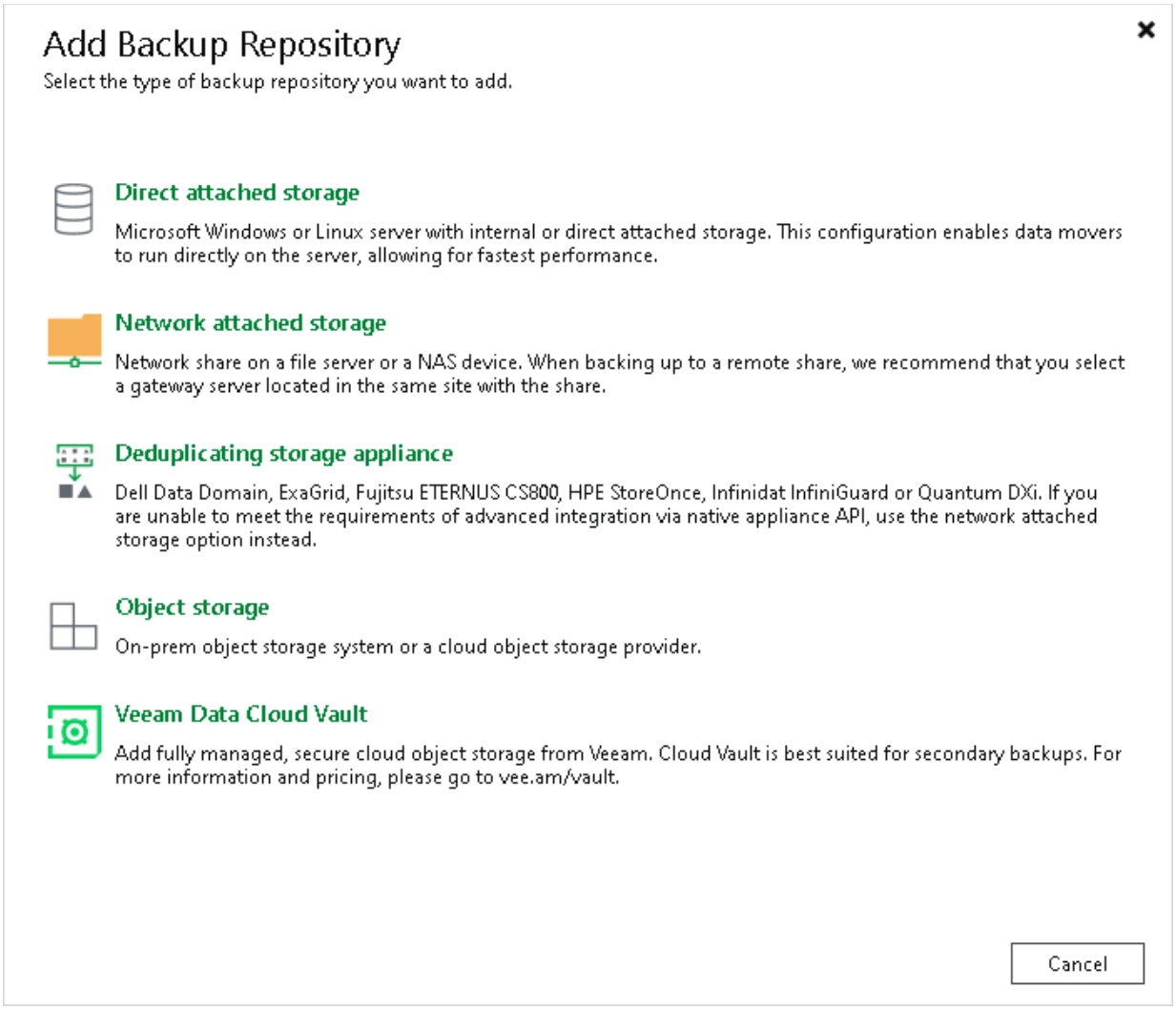
5. Follow the next steps of the wizard. At the last step of the wizard, click **Finish** to add the server.
6. Open the **Backup Infrastructure** view and click the **Managed Servers** node. The added server must be available in the working area.

Assigning Backup Repository Role to Added Server

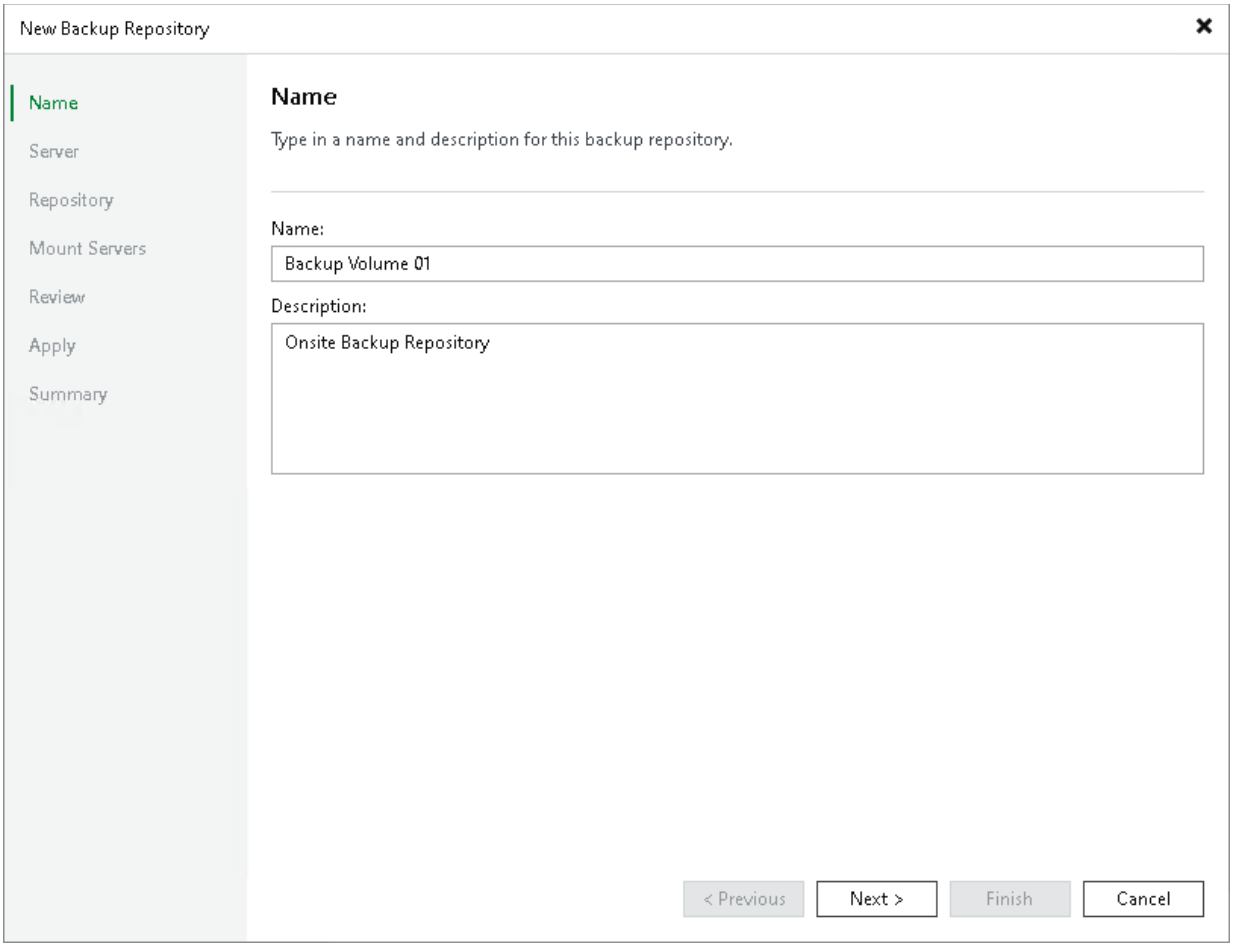
To assign the role of the backup repository:

1. In the inventory pane, right-click the **Backup Repositories** node and select **Add Backup Repository** to launch the **New Backup Repository** wizard.

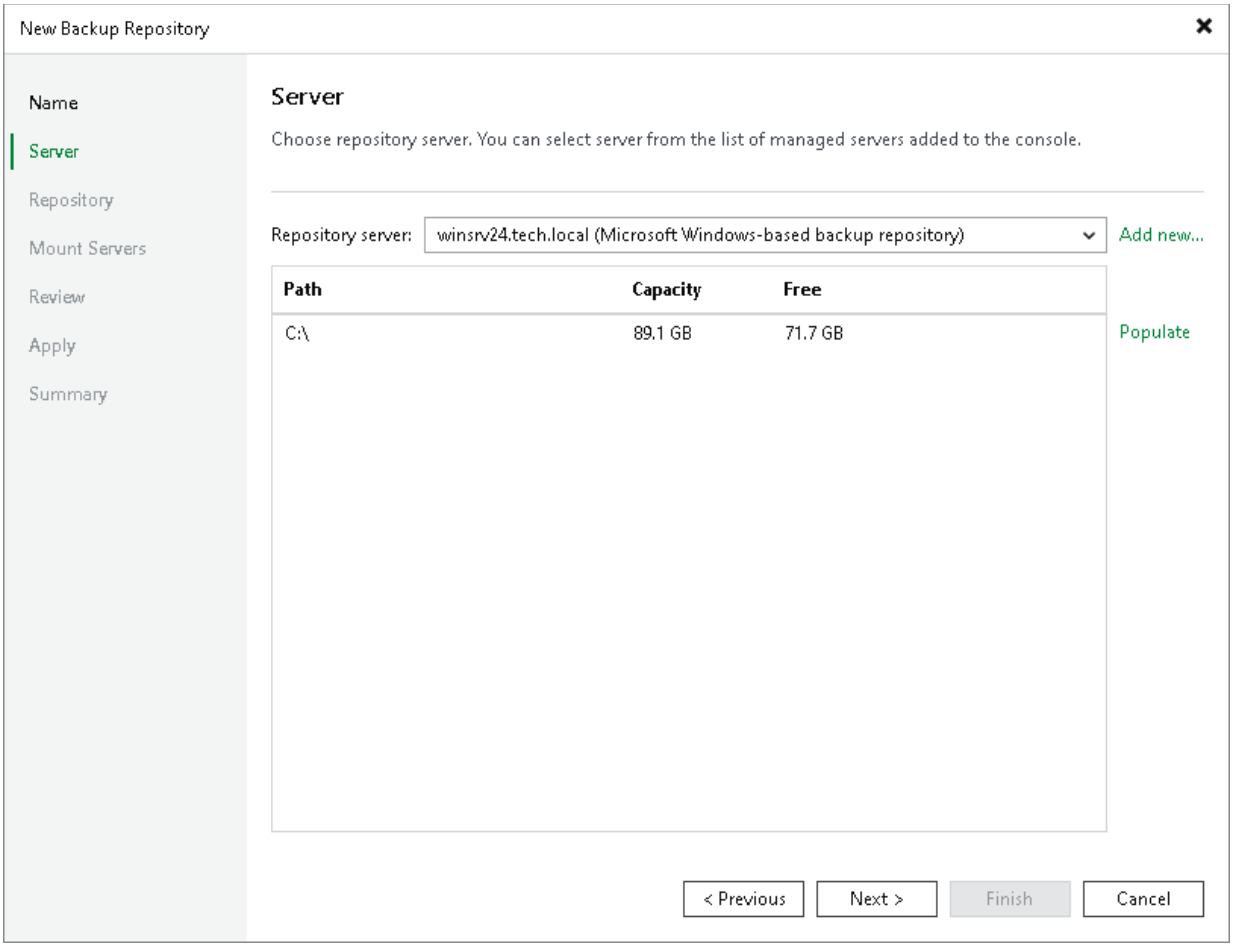
2. In the **Add Backup Repository** window, click **Direct attached storage** >**Microsoft Windows**.



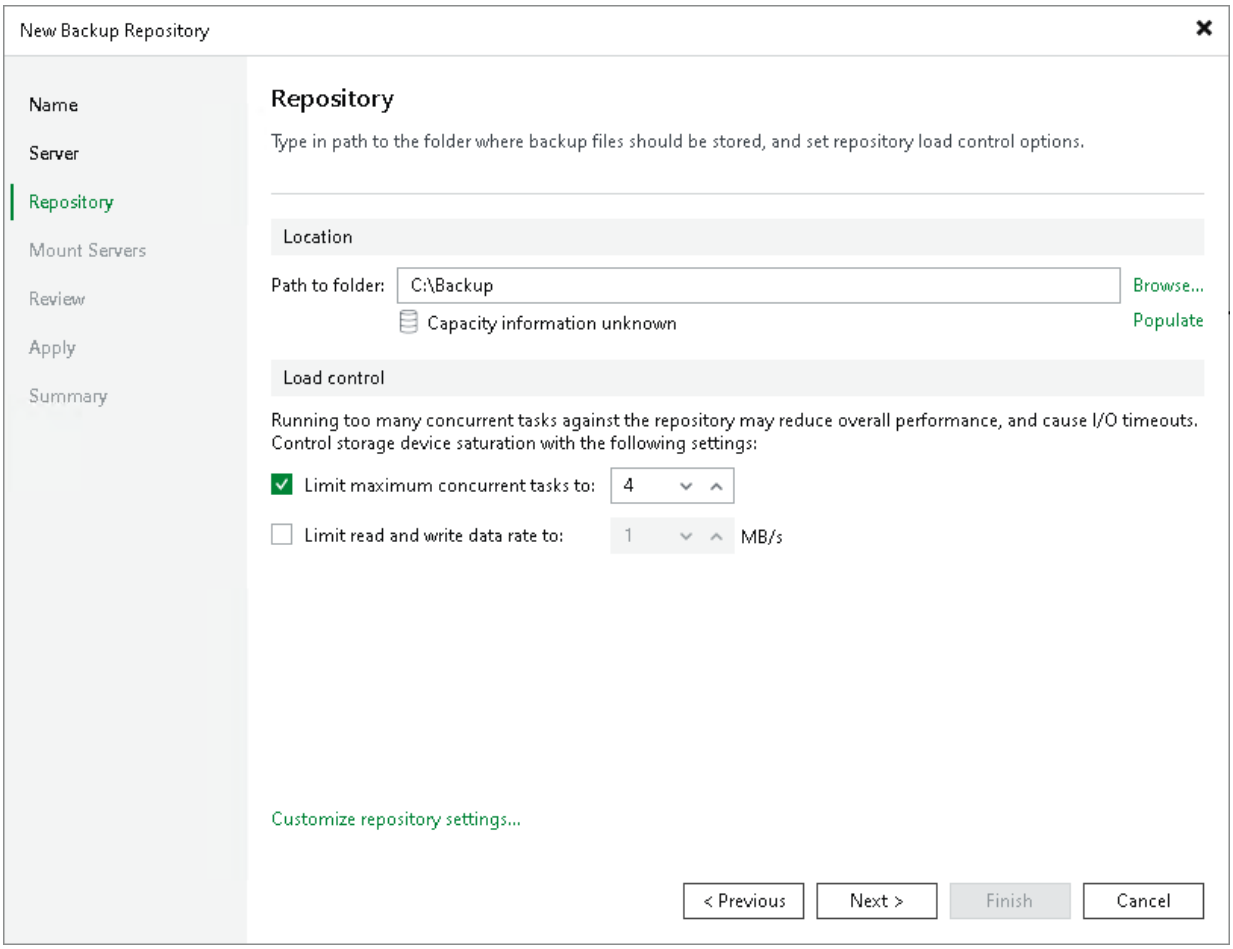
3. At the **Name** step of the wizard, specify the name for the added backup repository.



4. At the **Server** step of the wizard, select the machine that you have added.



5. At the **Repository** step of the wizard, specify a path to the folder where backup files will be stored. In addition to them, auxiliary replica files will be placed in this folder.



6. At the **Mount Server** step of the wizard, keep the default settings.
7. Follow the next steps of the wizard. At the **Summary** step, click **Finish**.
8. Open the **Backup Infrastructure** view and click the **Backup Repositories** node. The added backup repository must be available in the working area.

Reference

For details on the backup repository, see the Backup Repository section in the Veeam Backup & Replication User Guide.

Step 8. Configuring Object Storage Repositories

An object storage repository is a repository intended for long-term data storage. It can be based on either a cloud solution or an S3 compatible storage solution. Configuring an object storage repositories is an optional step.

Veeam Backup & Replication supports the following types of object storage repositories:

- S3 compatible
- Amazon S3, Amazon S3 Glacier and Amazon Snowball Edge
- Google Cloud
- IBM Cloud
- Microsoft Azure Blob, Azure Archive Storage and Azure Data Box

In this section, you will learn how to configure Amazon S3 storage system as a backup repository.

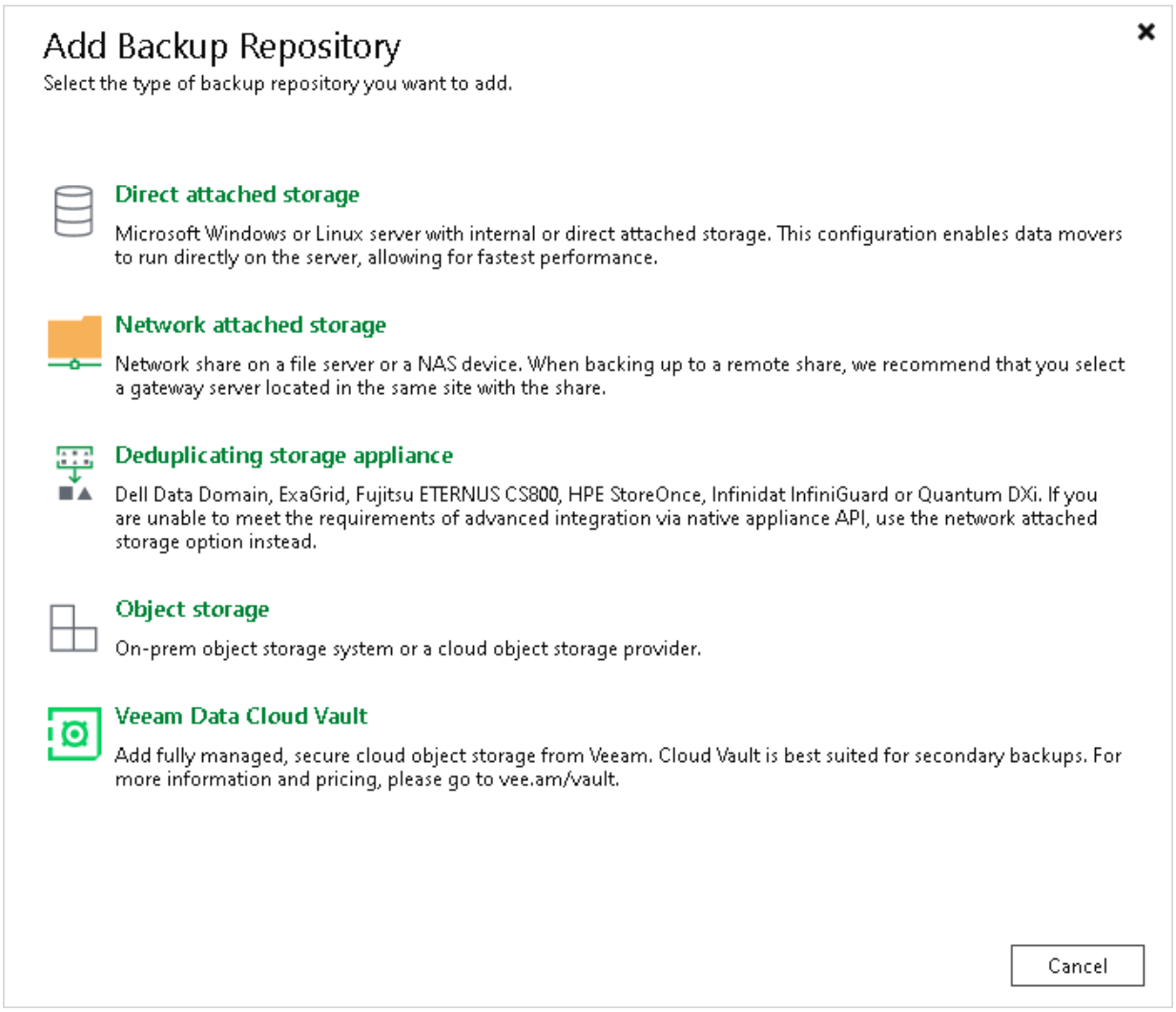
Before You Begin

Before you add an object storage repository, check limitations. To learn about limitations for different storage repositories, see the Considerations and Limitations section in the Veeam Backup & Replication User Guide.

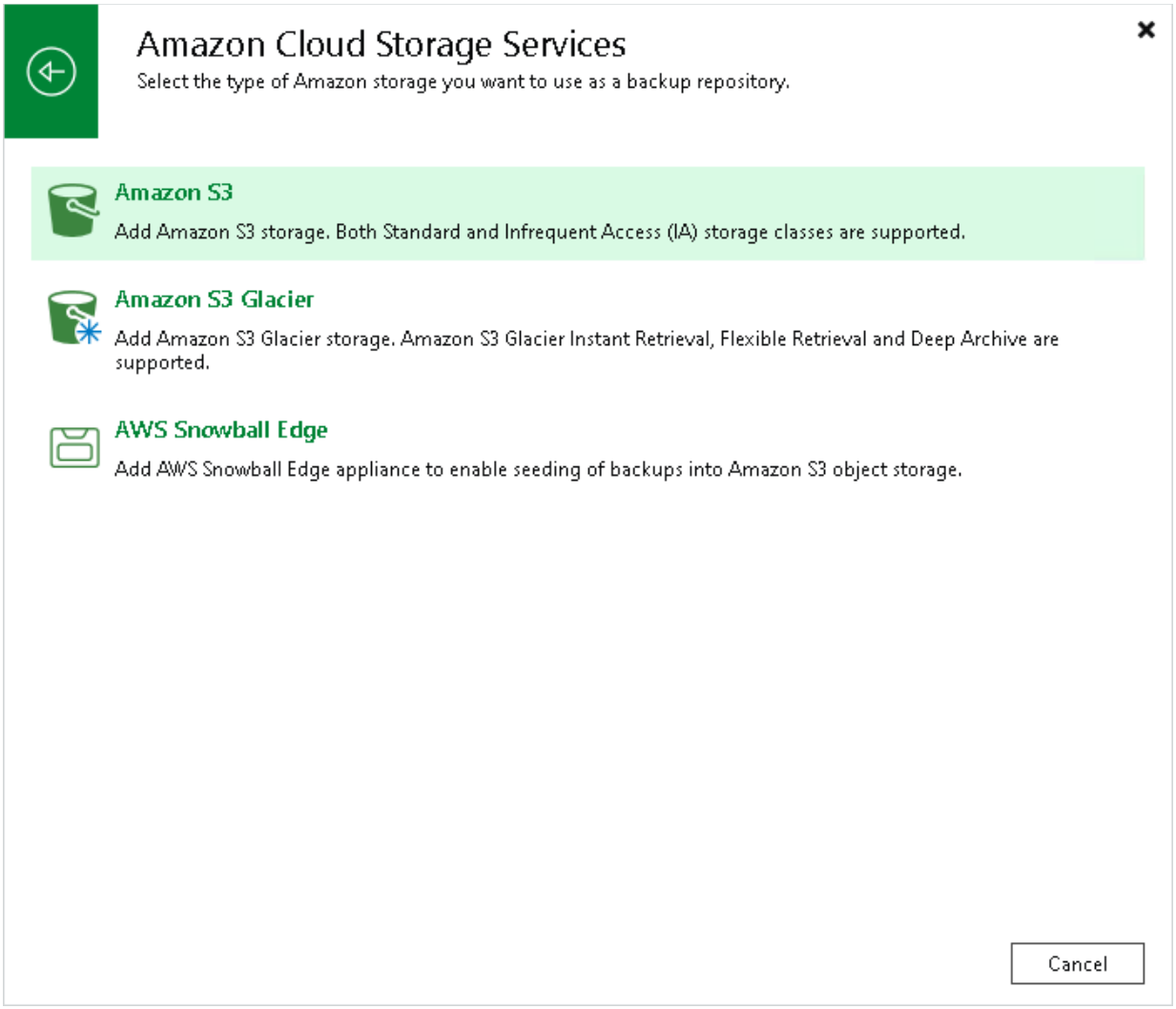
Configuring Object Storage Repository

To add an object storage repository to the Veeam Backup & Replication infrastructure, do the following:

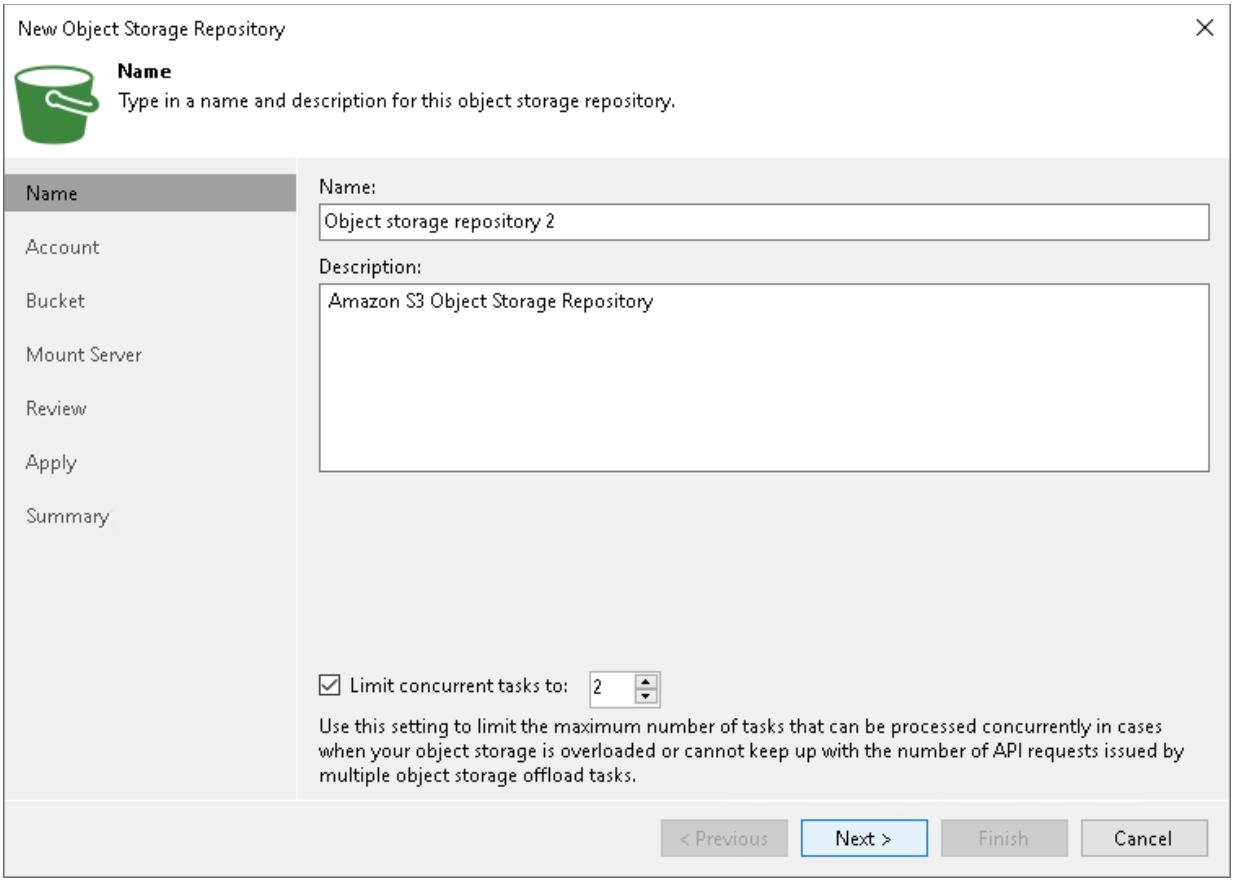
1. Open the **Backup Infrastructure** view. In the inventory pane, right-click the **Backup Repositories** node and select **Add Backup Repository**. In the **Add Backup Repository** dialog, select **Object Storage**.



2. In the **Object Storage** dialog, select **HyperScales** > **S3 Compatible** > **Amazon S3** > **Amazon S3**.



3. At the **Name** step of the wizard, specify the name and description for the object storage repository.

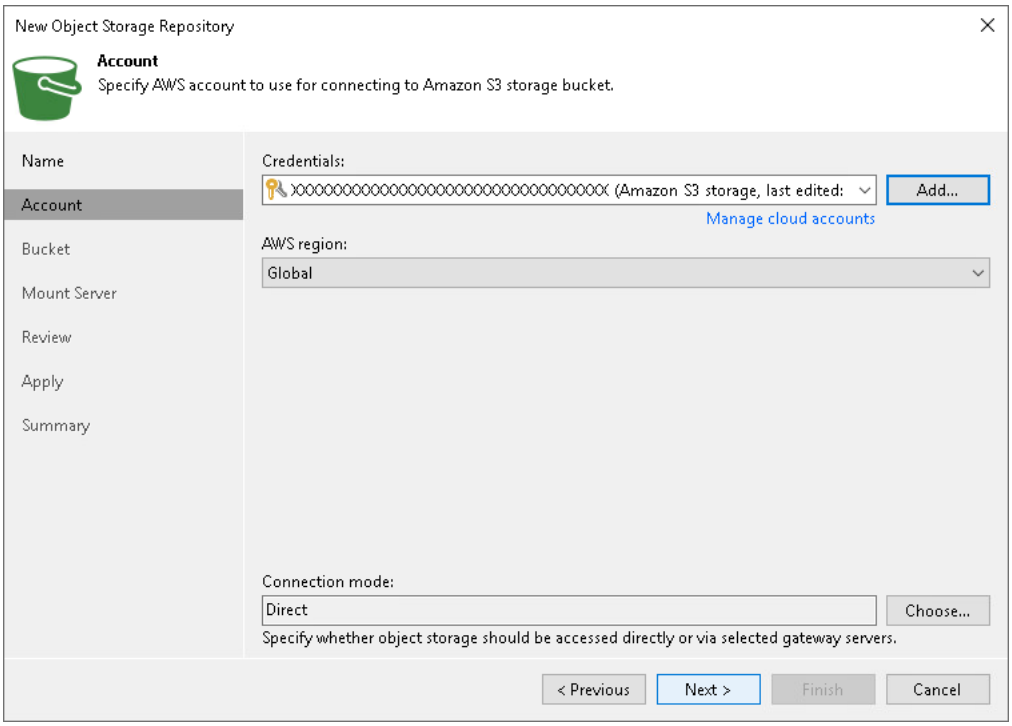


4. At the **Account** step of the wizard, specify the connection settings:

   a. From the **Credentials** drop-down list, select user credentials to access your object storage. If you already have a credentials record that was configured in advance, select such a record from the drop-down list. Otherwise, click Add and provide your access and secret keys. For more information, see the Cloud Credentials Manager section in the Veeam Backup & Replication User Guide.

b. In the **AWS region** drop-down list, select a region type.

If your organization has NAT or different types of firewalls and your access to the internet is limited, you may want to use a gateway server. To do so, click **Choose**, select the **Through a gateway server** check box and choose a server from the list.



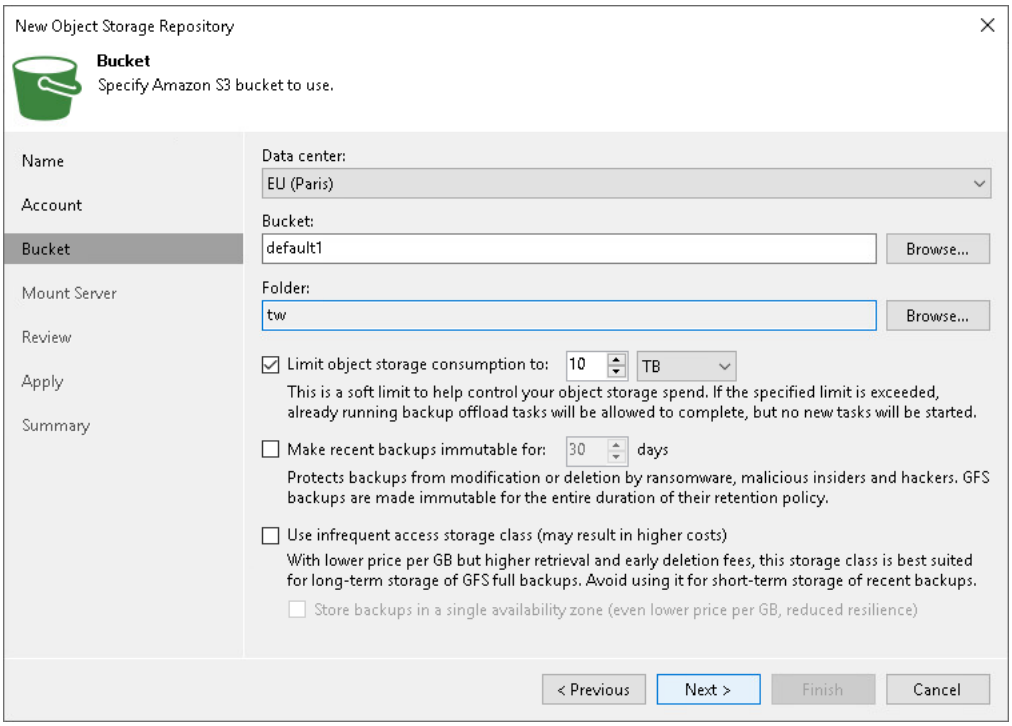
5. At the **Bucket** step of the wizard, specify how your data will be stored.

   a. From the **Data center** drop-down list, select a region.

   b. From the **Bucket** drop-down list, select a bucket. Make sure that the bucket you want to use to store your backup data was created in advance.

   c. In the **Folder** field, select a cloud folder to which you want to map your object storage repository. To do it, click **Browse** and either select an existing folder or create a new one by clicking **New Folder**.

d. To define a soft limit for your object storage consumption that can be exceeded temporarily, select the **Limit object storage consumption to** check box and provide the value in TB or PB.



6. Follow the next steps of the wizard and leave the default settings. At the **Summary** step of the wizard, review the settings and click **Finish**.
7. Open the **Backup Infrastructure** view and click the **Backup Repositories** node. The added object storage repository must be available in the working area.

Reference

For details on adding object storage repositories, see the Adding Object Storage Repositories section in the Veeam Backup & Replication User Guide.

Step 9. Configuring Scale-Out Backup Repositories

A scale-out backup repository is a repository system for multi-tier storage of data, where the capacities of all the added storage devices and systems are summarized. A scale-out backup repository consists of one or more backup repositories called performance extents, and can be expanded with an object repository called capacity extent.

Configuring a scale-out backup repository is an optional step. For more information on scale-out backup repositories, see the Scale-Out Backup Repository section in the Veeam Backup & Replication User Guide.

Before You Begin

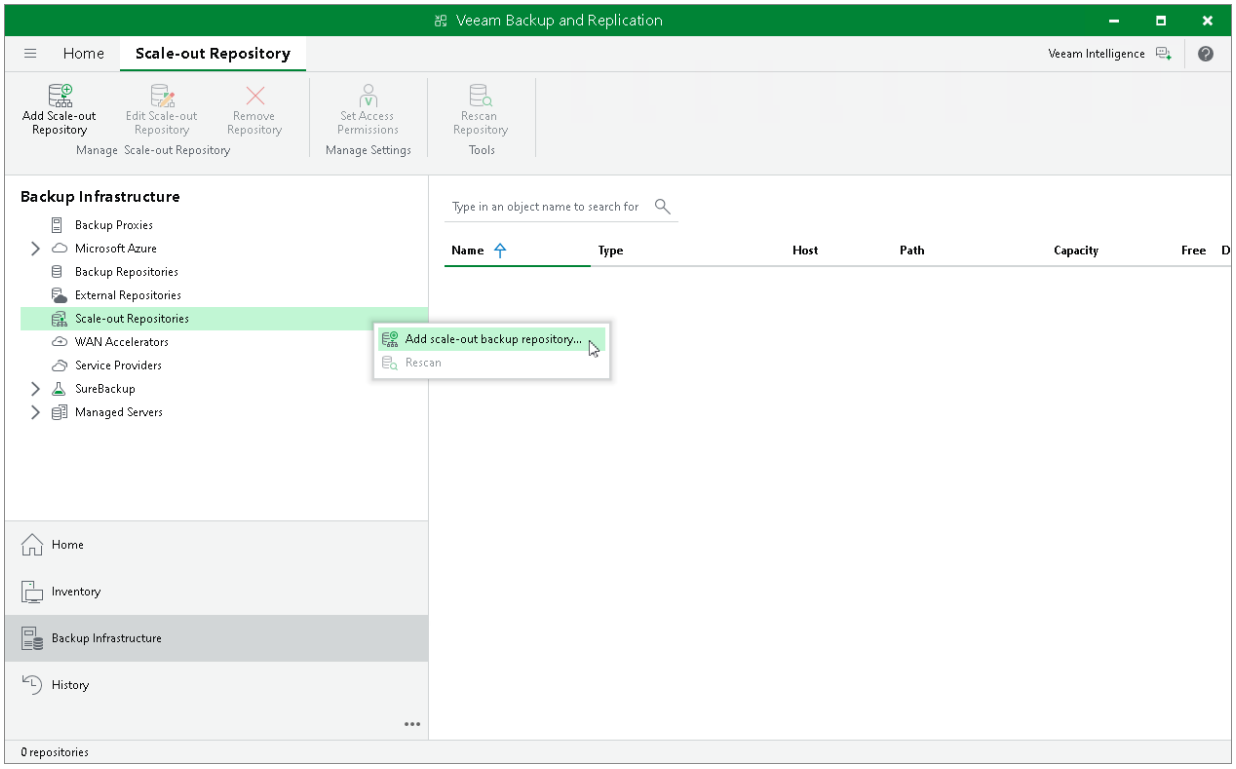
Before you add a scale-out backup repository to the backup infrastructure, check the following prerequisites:

- Backup repositories that you plan to add as performance extents to the scale-out backup repository must be added to the backup infrastructure. For more information, see Configuring Backup Repository.
- If you wish to use the capacity tier option of the scale-out backup repository, an object storage repository that you plan to add as a capacity extent to the scale-out backup repository must be added to the backup infrastructure. For more information, see Configuring Object Storage Repository.
- Check limitations for scale-out backup repositories. For more information, see Limitations for Scale-Out Backup Repositories in the Veeam Backup & Replication User Guide.

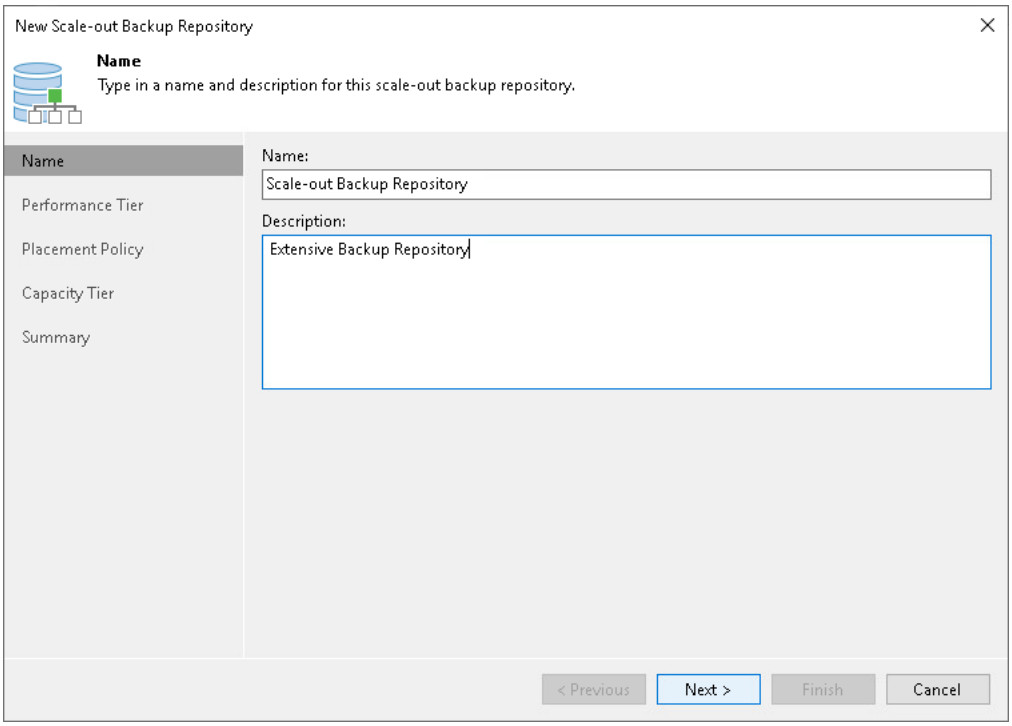
Configuring Scale-Out Backup Repository

To add a scale-out backup repository to the Veeam Backup & Replication infrastructure, do the following:

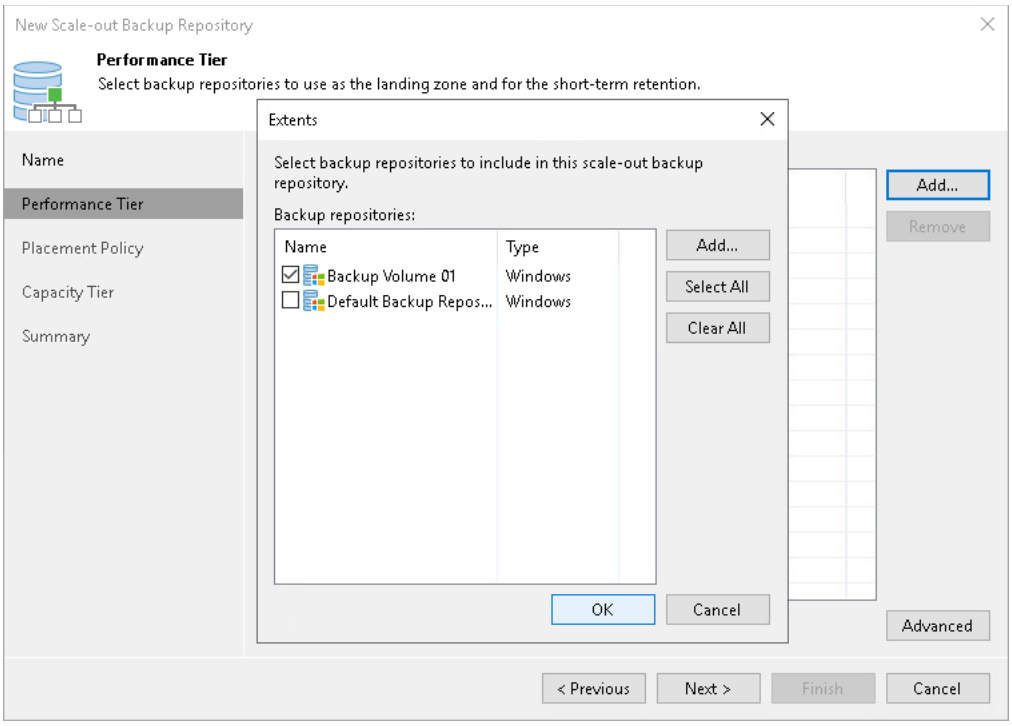
1. In the inventory pane, right-click **Scale-out Repositories** and select **Add Scale-out Backup Repository.**



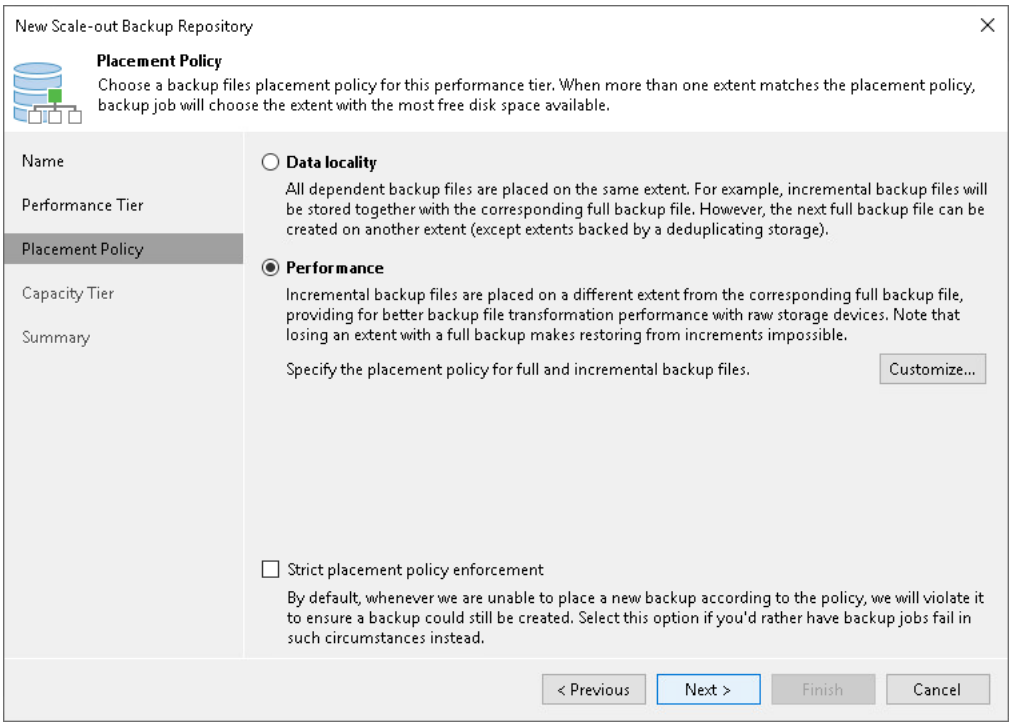
2. At the **Name** step of the wizard, specify a name and an optional description for the scale-out backup repository.



3. At the **Performance Tier** step of the wizard, specify which backup repositories you want to add as performance extents, and configure options for the scale-out backup repository. To do it, on the right side of the **Extents** list, click **Add**. In the **Extents** window, select check boxes next to backup repositories that you want to add as performance extents. Then click **OK**.



4. At the **Placement Policy** step of the wizard, select **Performance** to store full and incremental backup files at different performance extents of the scale-out backup repository.



5. At the **Capacity Tier** step of the wizard, select an object storage repository that you want to add as a capacity extent and specify when to move or copy data. This is an optional step.

   To configure the capacity tier, do the following:

   a. Select the **Extend scale-out backup repository capacity with object storage** check box.

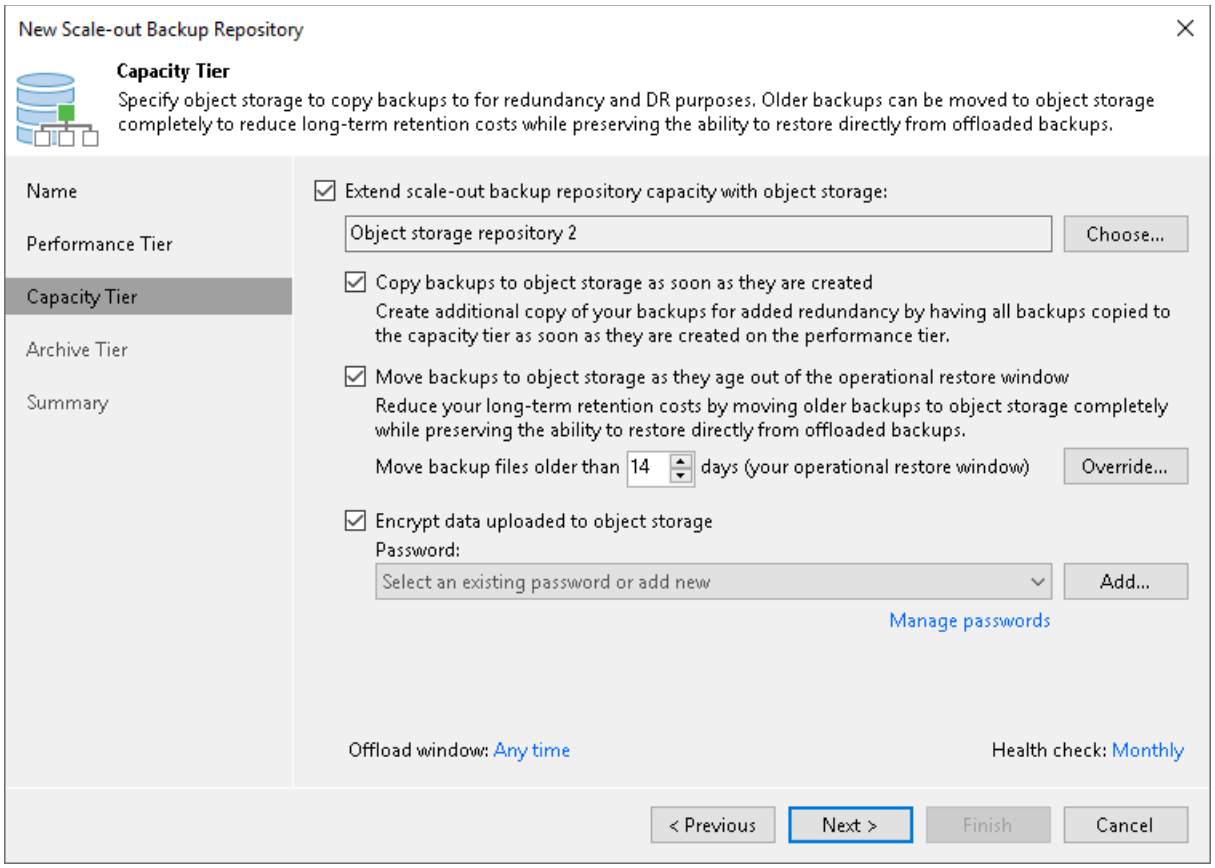
   b. From the drop-down list, select an object storage repository to which you want to offload your data.

   c. Click **Window** and specify when it is allowed or prohibited to move or copy data to object storage.

   d. Select the **Copy backups to object storage as soon as they are created** check box to copy new backups as soon as they are created.

   e. Select the **Move backups to object storage as they age out of the operational restores window** check box to move inactive backup chains to the capacity extent.

f. To offload data encrypted, select the **Encrypt data uploaded to object storage** check box and provide a strong password. If you have not created the password beforehand, click **Add** or use the **Manage passwords** link to specify a new password.



6. Follow the next steps of the wizard. At the last step of the wizard, click **Finish** to add the repository.
7. Open the **Backup Infrastructure** view and click the **Scale-Out Repositories** node. The added scale-out backup repository must be available in the working area.

Reference

For details on adding scale-out backup repositories, see the Adding Scale-Out Backup Repositories section in the Veeam Backup & Replication User Guide.

VM Backup

When you perform a backup, Veeam Backup & Replication retrieves VM data from the source storage, compresses and deduplicates it. After that, Veeam Backup & Replication writes data to the backup repository in Veeam proprietary format.

In Veeam Backup & Replication, backup is a job-driven process. To perform the backup, you need to configure a backup job. For details, see Creating Backup Job.

During runs of backup jobs, Veeam Backup & Replication creates backup chains. The chain consists of the following backup files:

- Full backup file (.VBK) that contains a copy of the entire VM.
- Incremental backup file (.VIB or .VRB) that contains only those data blocks that have changed since the last backup job session.
- Metadata file (.VBM) that contains information on the backup job, VMs in the backup, number and structure of backup files, restore points and so on.

The amount of these files and how Veeam Backup & Replication places them depend on the chosen backup method. For details, see Backup Methods.

After you performed backups, you can use them to restore the following instances: entire VM, VM files, guest OS files and application items. For details on restore, see Data Recovery.

Reference

For details, see About VMware vSphere Backup and About Microsoft Hyper-V Backup sections in the Veeam Backup & Replication User Guide.

Backup Methods

Veeam Backup & Replication provides three methods for creating backup chains:

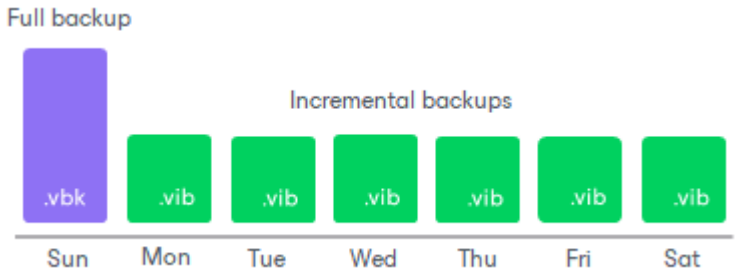
- Forever forward incremental backup
- Forward incremental backup

Forever Forward Incremental Backup Method

The forever forward incremental backup method produces a backup chain that consists of the first full backup file (.VBK) and a set of forward incremental backup files (.VIB) following it.

During the first session of a backup job, Veeam Backup & Replication creates a full backup file on the backup repository. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session and saves these blocks as an incremental backup file in the backup chain.

After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy for the job and deletes outdated restore points. For details, see the Forever Forward Incremental Backup Retention Policy section in the Veeam Backup & Replication User Guide.



Forward Incremental Backup Method

The forward incremental backup method produces a backup chain that consists of the first full backup file (.VBK) and a set of forward incremental backup files (.VIB) following it.

Additionally, the forward incremental backup chain contains full backup files that "split" the backup chain into shorter series. The subsequent full backup files can be the following:

- **Active**

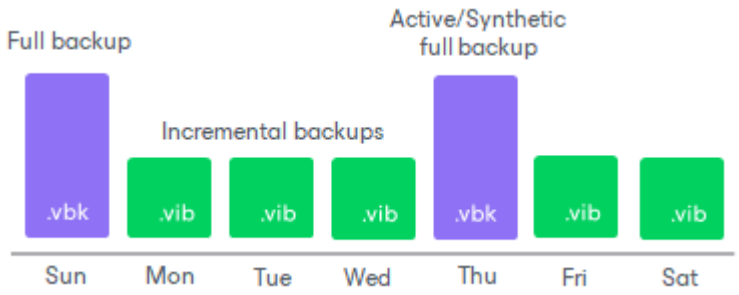
  The active full backup contains the copy of a VM. This backup is similar to the full backup created when you run a job for the first time. Veeam Backup & Replication retrieves data for the whole VM from the source, compresses and deduplicates it and stores it to the active full backup file.

- **Synthetic**

  The synthetic full backup also contains the copy of a VM. However, this copy is created from the backup files that you already have on the backup repository. Veeam Backup & Replication does not retrieve VM data from the source datastore.

During the first backup job session, Veeam Backup & Replication creates a full backup file. During subsequent backup job sessions, Veeam Backup & Replication copies only VM data blocks that have changed since the last backup job session and saves these blocks as an incremental backup file in the backup chain. On a day when the synthetic or active full backup is scheduled, Veeam Backup & Replication creates a full backup file and adds it to the backup chain.

After adding a new restore point to the backup chain, Veeam Backup & Replication checks the retention policy and deletes outdated restore points. For details, see the Forward Incremental Backup Retention Policy section in the Veeam Backup & Replication User Guide.



Reference

For details, see the following section in the Veeam Backup & Replication User Guide:

- Retention Policy (VMware vSphere)
- Retention Policy (Microsoft Hyper-V)
- Active Full Backup (VMware vSphere)
- Active Full Backup (Microsoft Hyper-V)
- Synthetic Full Backup (VMware vSphere)
- Synthetic Full Backup (Microsoft Hyper-V)
- Backup Methods (VMware vSphere)
- Backup Methods (Microsoft Hyper-V)

Creating Backup Job

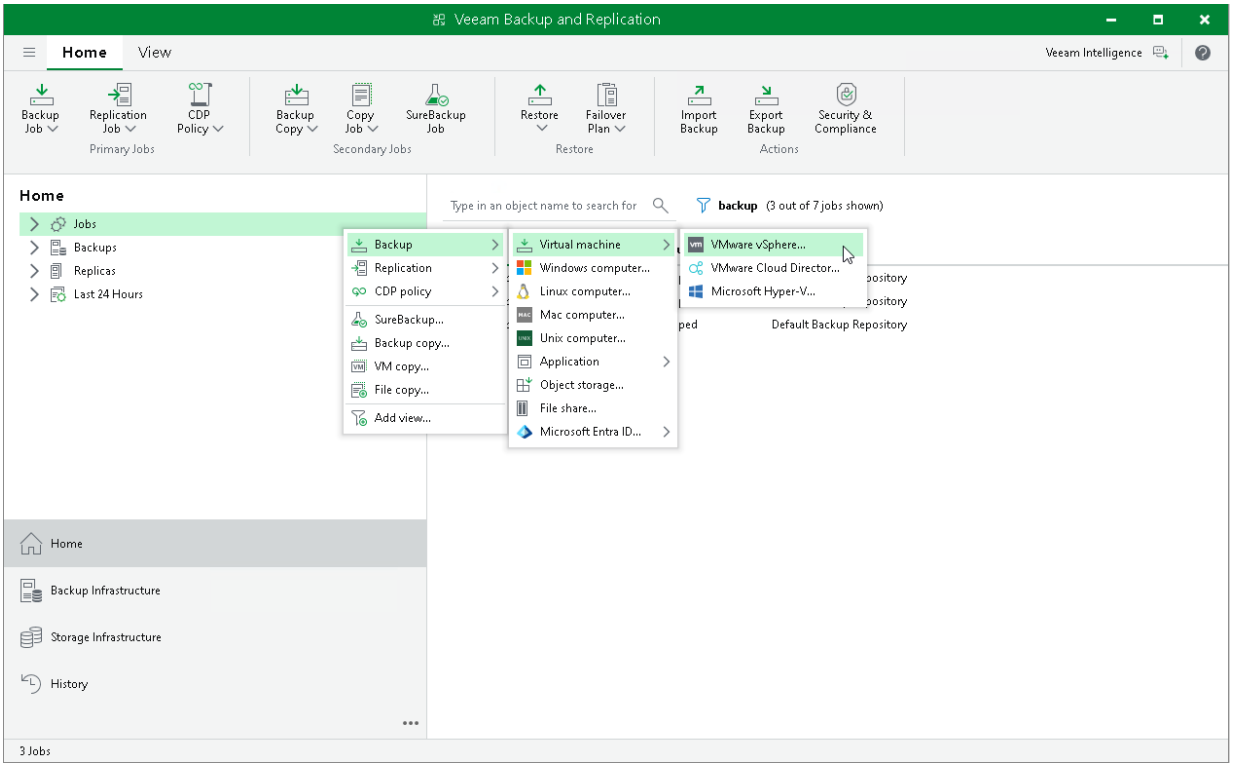
Before You Begin

Make sure that all backup infrastructure components that take part in the backup process are added to the backup infrastructure. These components include hosts on which VMs are registered, backup proxy and backup repository.

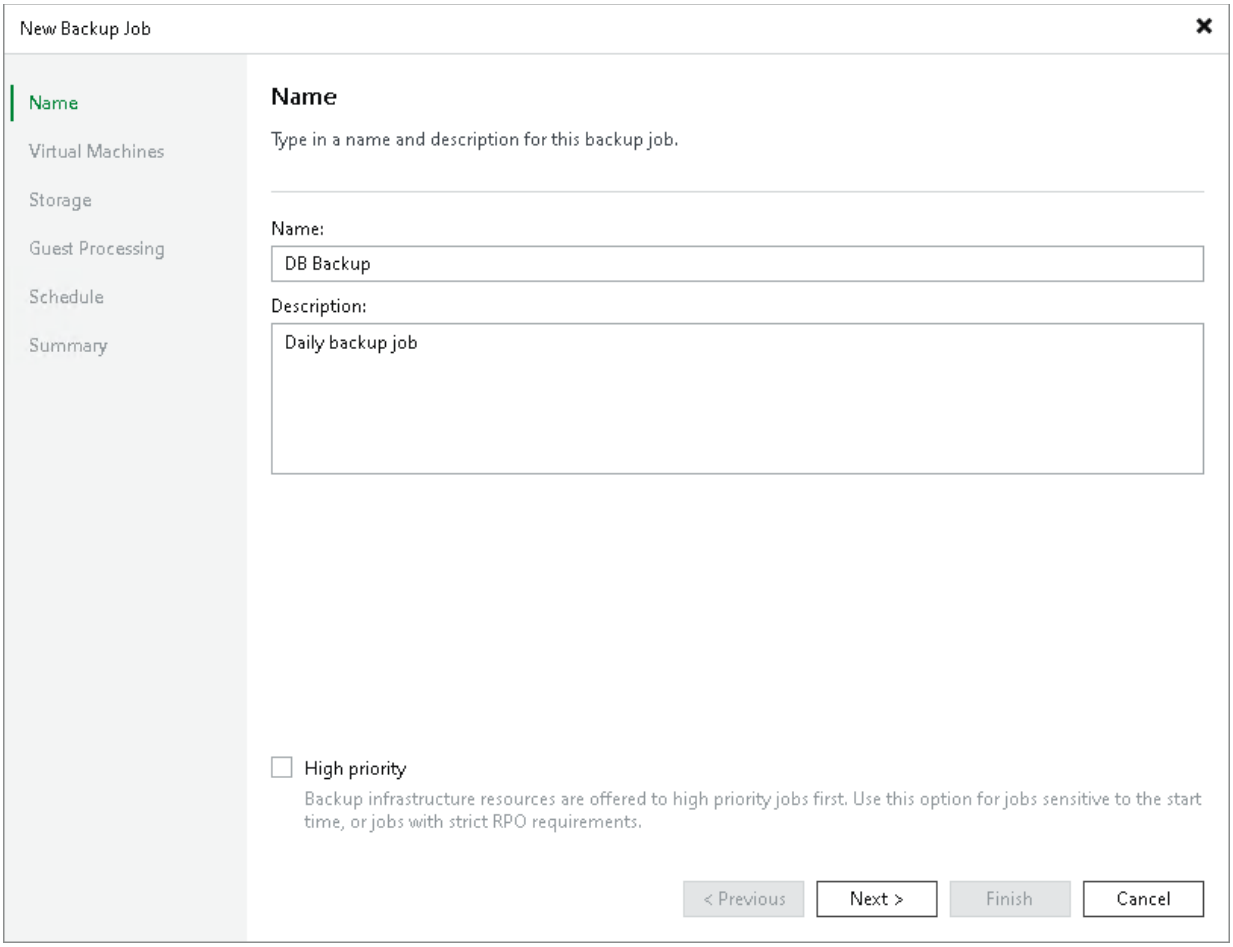
Creating Backup Job

To back up VMs, do the following:

1. In the inventory pane of the **Home** view, right-click **Jobs** and select **Backup** > **Virtual Machine** > *<platform>* to launch the **New Backup Job** wizard.

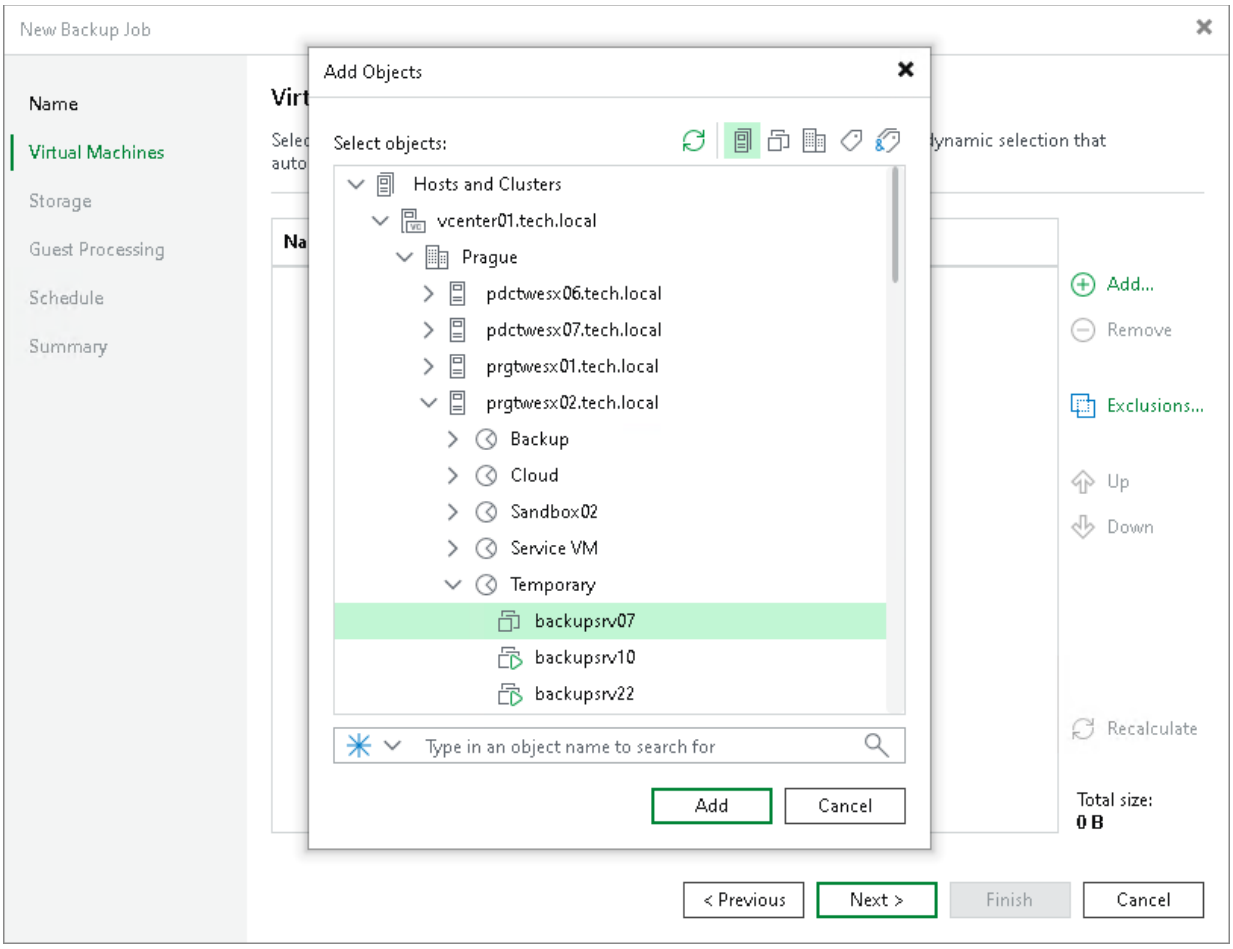


2. At the **Name** step of the wizard, specify a name and description for the backup job.



3. At the **Virtual Machines** step of the wizard, click **Add**. From the list, select VMs that you want to back up.

   You can also back up VM containers and so on. If you add a new VM to the container after the backup job is created, Veeam Backup & Replication automatically updates the job to include the new VM.

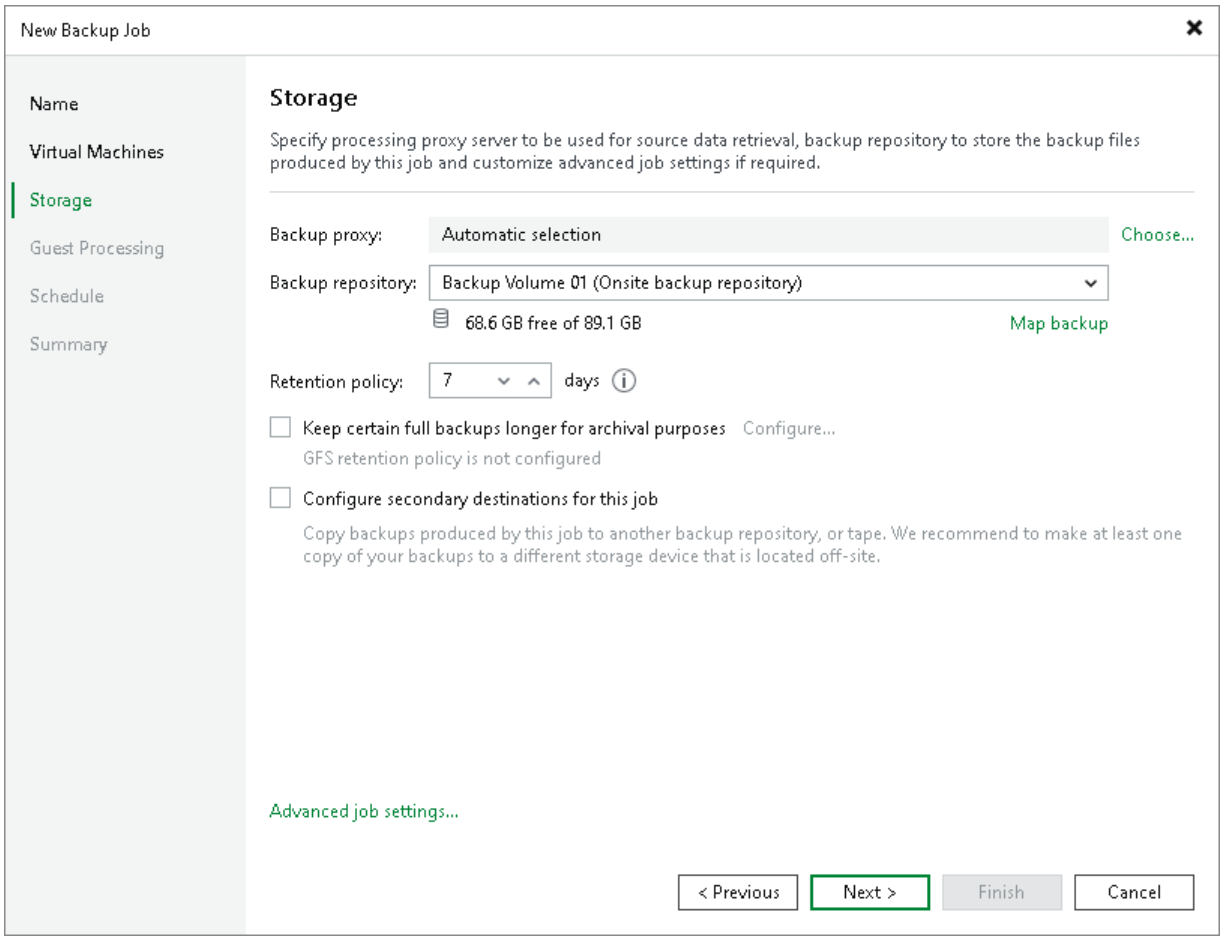


4. At the **Storage** step of the wizard, do the following:

   a. From the **Backup repository** list, select the backup repository that you configured in the Configure Backup Repository section.

b. In the **Retention policy** field, define the number of days to keep the restore points.

When the number of days exceeds the allowed value, Veeam Backup & Replication automatically removes the earliest restore point from the backup chain. For more information, see the Retention Policy section in the Veeam Backup & Replication User Guide.



5. At the **Guest Processing** step of the wizard, leave the default settings.

   The settings of this step are detailed in the Creating Application-Aware Backup Job section.

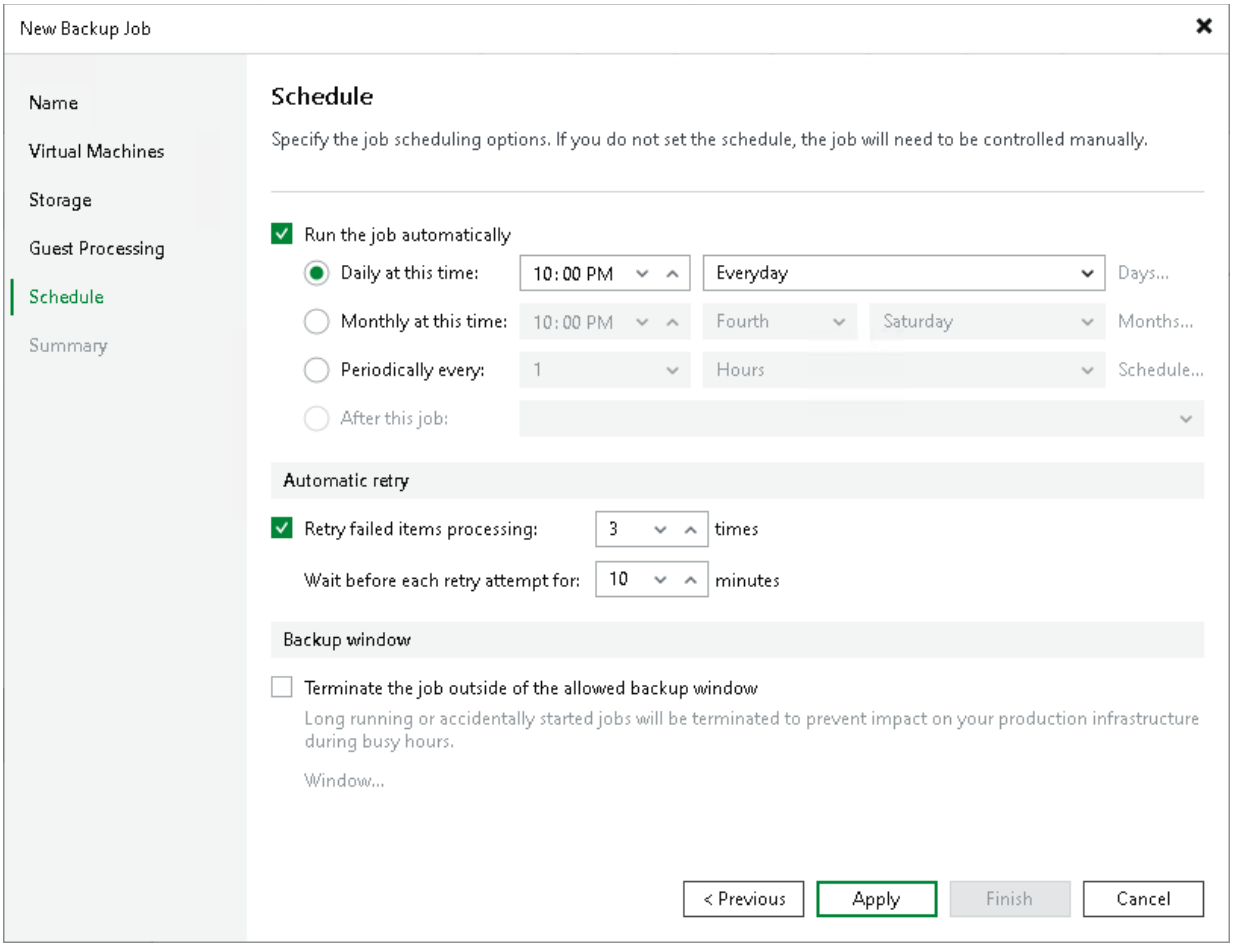
6. At the **Schedule** step of the wizard, do the following:

   a. Select the **Run the job automatically** check box. If you do not select this check box, you will have to launch the job manually. For details, see Start Backup Job Manually.

   b. Select the schedule type: daily, monthly or periodically.

   c. Make sure the **Retry failed VM processing** check box is selected.

d. Click **Apply**.



7. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.
8. In the inventory pane of the **Home** view, expand the **Last 24 Hours** node to see the created job.

Reference

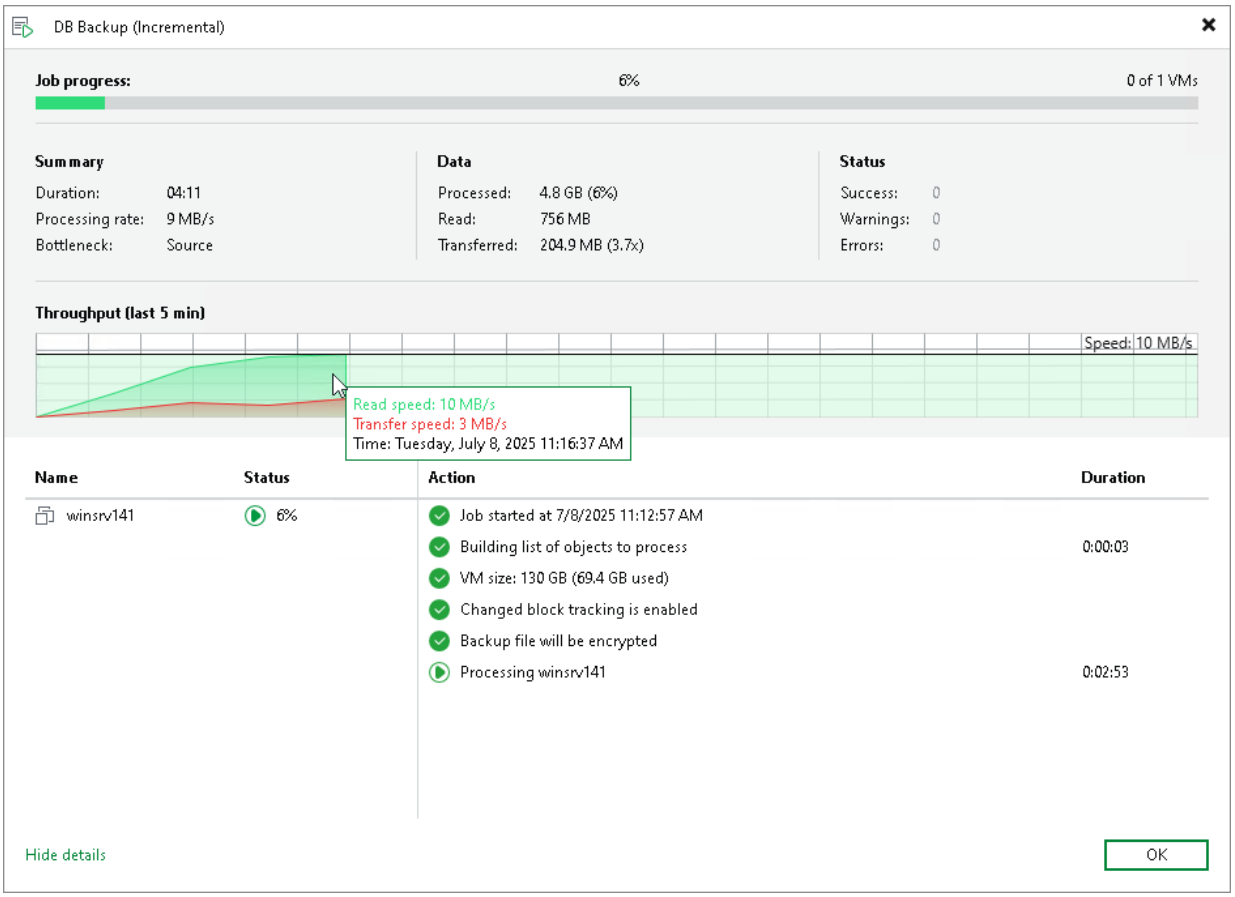
For more information on backup creation, see the Creating Backup Jobs (VMware vSphere) and Creating Backup Jobs (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Monitoring Job Performance in Real Time

When the job is running, you can view job statistics in real time. Statistics include job progress, duration, processing rate, performance bottlenecks, the amount of read and transferred data, and other details of the job performance.

To view the job statistics, do the following:

1. In the inventory pane of the **Home** view, select the **Jobs** node.
2. In the working area, right-click a running job and click **Statistics**.
3. In the opened window, select a VM to view its statistics.



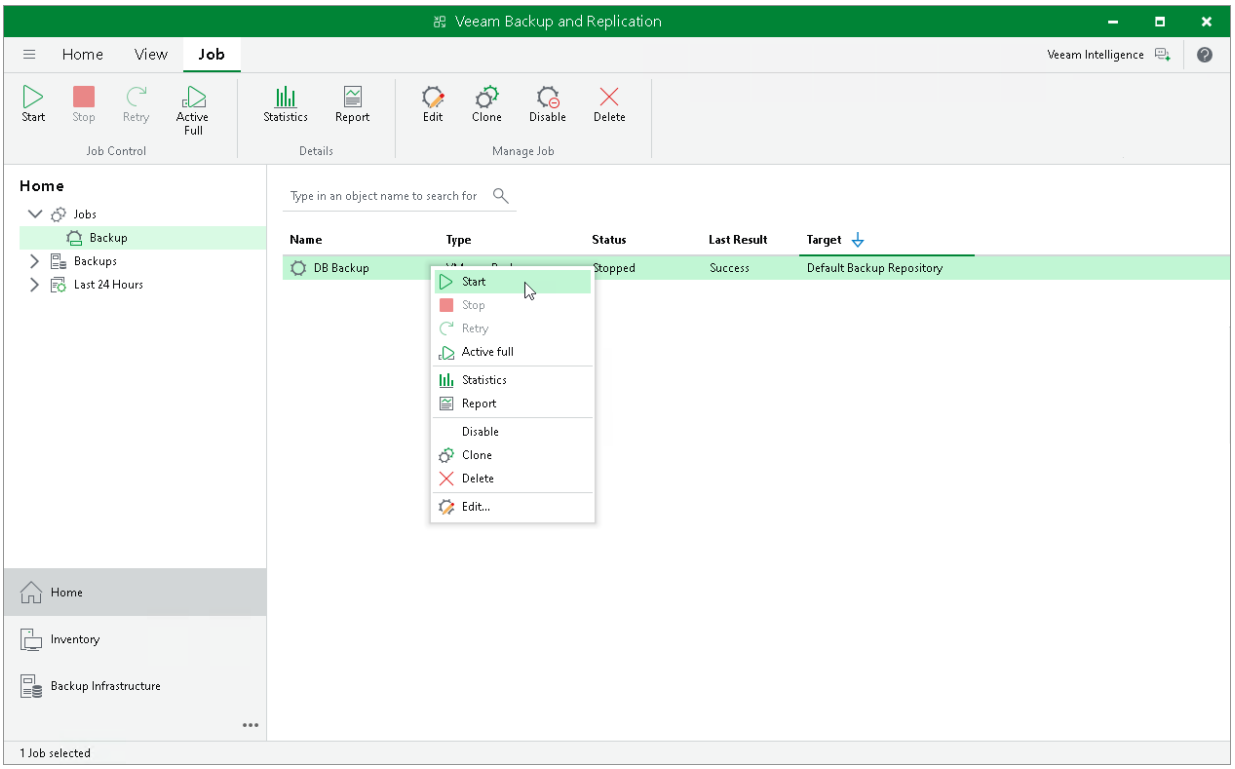
Note that the job must complete with the *Success* or *Warning* status. If the job completes with the *Failed* status, Veeam Backup & Replication does not create the backup file is not able to perform restore operations.

You can configure email notifications to get job results. For details, see the Configuring Global Email Notification Settings (VMware vSphere) and Configuring Global Email Notification Settings (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Start Backup Job Manually

If you do not schedule a backup job, you must start it manually. To start the job, do the following:

1. Open the **Home** view.
2. In the inventory pane, select the **Jobs** node.
3. In the working area, right-click the job and select **Start**. Wait for the job to complete. Note that the job must complete with the *Success* or *Warning* status.

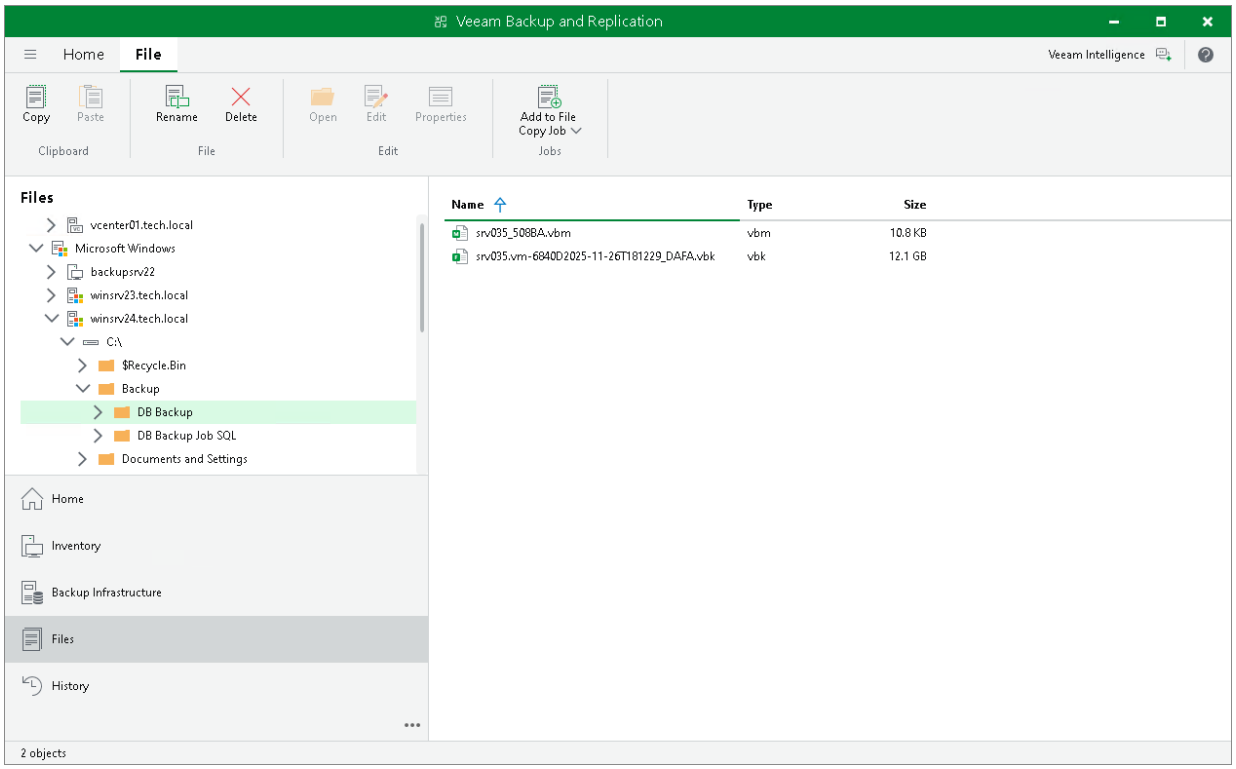


Locating Backup Files

When a backup job finishes, Veeam Backup & Replication saves backup files in the backup repository that you specified as a backup target.

To locate backup files using the Veeam Backup & Replication console, do the following:

1. Open the **Files** view.
2. In the inventory pane, expand the backup repository file tree and open the **Backup** folder.
3. In the **Backup** folder, find the subfolder with the backup job name and open it. It must contain a .VBK and .VBM files. If the job was run several times, the subfolder also contains .VIB or .VRB files.



Creating Application-Aware Backup Job

Application-aware processing allows you to create transactionally consistent backups. These backups allow you to further restore application items: emails for mail agents, tables for DB servers, accounts for domain controllers.

Veeam Backup & Replication can create transactionally consistent backups of VMs that run the following applications:

- Microsoft Exchange
- Active Directory
- SharePoint
- SQL Server
- Oracle Database

In this section, you will learn how to create the application-aware backup job for a Microsoft SQL Server.

> **IMPORTANT!**
>
> Application-aware processing is supported only for the listed applications and VSS-aware applications. If an application that you want to back up is not supported, you can use VMware Tools or Microsoft Hyper-V guest quiescence with pre-freeze and post-thaw scripts. For more information, see the VMware Tools Quiescence and Pre-Freeze and Post-Thaw Scripts (VMware vSphere), Microsoft Hyper-V Guest Quiescence and Pre-Freeze and Post-Thaw Scripts (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Before You Begin

Make sure that the version of your Microsoft SQL Server is supported. For details, see the System Requirements section in the Veeam Backup & Replication User Guide.

Creating Application-Aware Backup

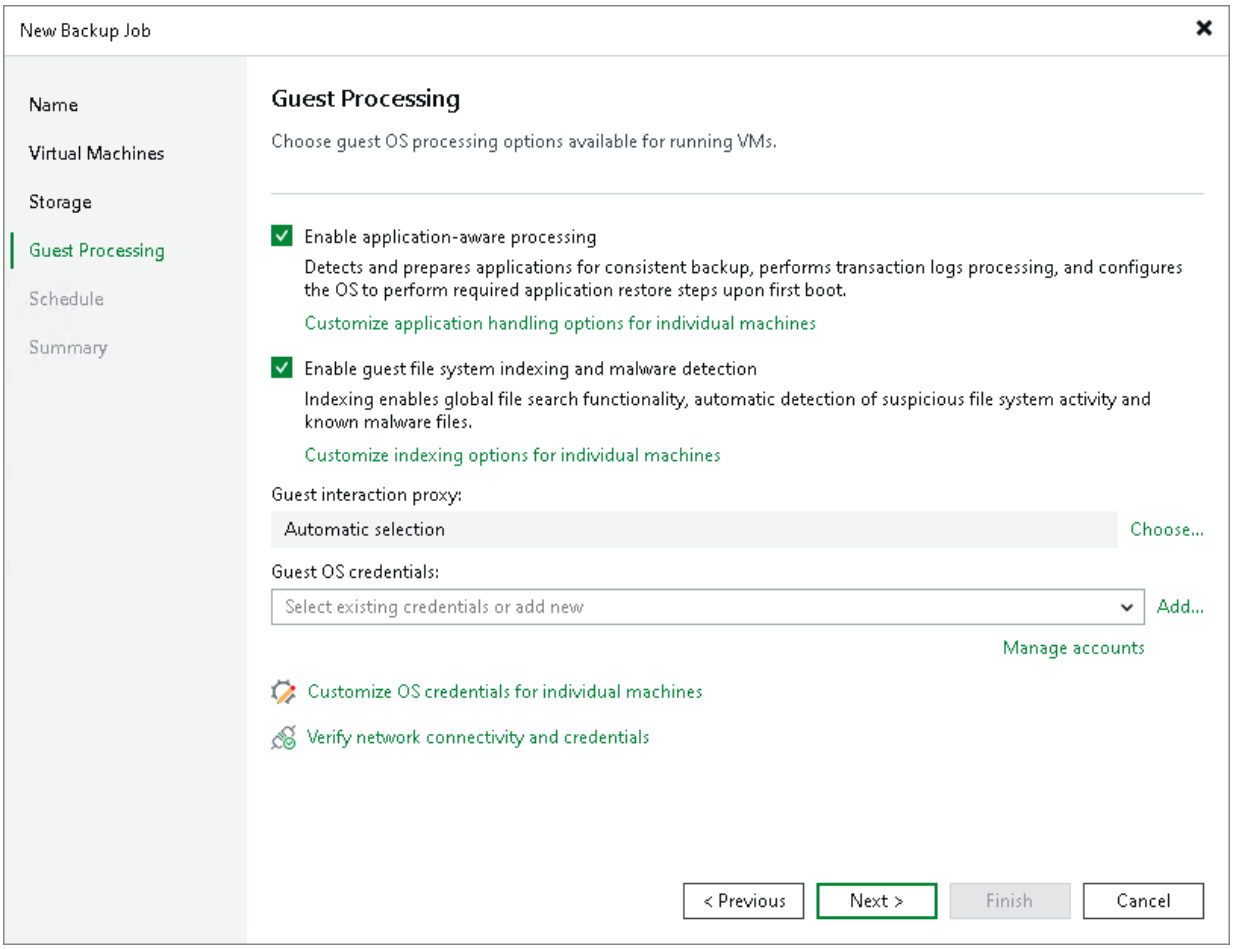
To create the application-aware backup job for the Microsoft SQL Server, do the following:

1. In the inventory pane of the **Home** view, right-click **Jobs** and select **Backup** > **Virtual Machine** > *<platform>* to launch the **New Backup Job** wizard.
2. At the **Name** step of the wizard, specify a name and description for the backup job.
3. At the **Virtual Machines** step of the wizard, select the VM.
4. At the **Storage** step of the wizard, select a backup repository or keep the default settings.
5. At the **Guest Processing** step of the wizard, do the following:
   a. Select the **Enable application-aware processing** check box.
   b. Select the **Enable guest file system indexing** check box.

      VM guest OS file indexing allows you to search for VM guest OS files inside VM backups and perform 1-click restore in Veeam Backup Enterprise Manager. For details, see the VM Guest OS File Indexing section in the Veeam Backup & Replication User Guide.

c. In the **Guest OS credentials** section, specify credentials of a user account to connect to the VM guest OS. The user account must have Administrator permissions on the Microsoft SQL Server.

d. Click the **Customize application handling options for individual machines** button at the top of the window.



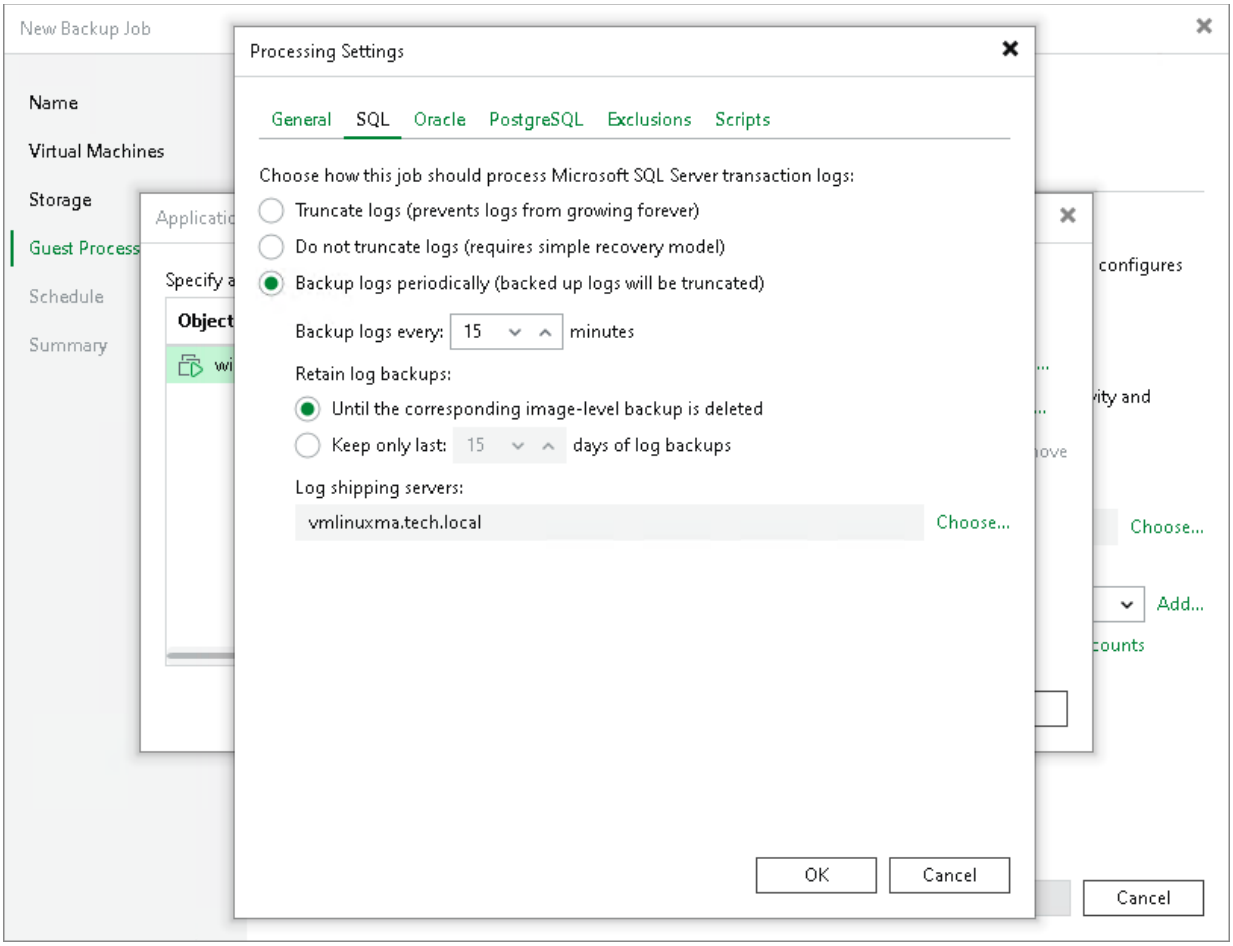
6. In the opened window, select the Microsoft SQL Server from the list and click **Edit**.

7. In the **Processing Settings** windows, do the following:

   a. In the **VSS Settings** section of the **General** tab, check that the **Process transaction logs with this job** option is selected.

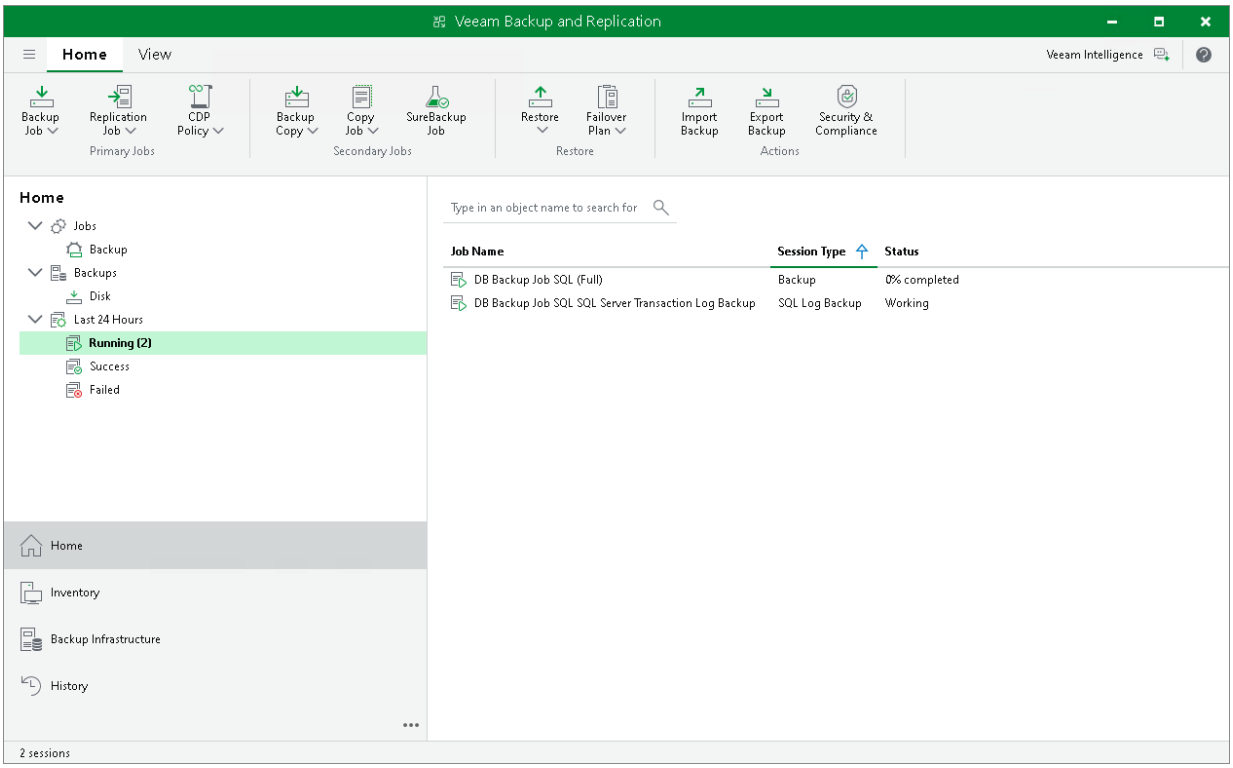
b. On the **SQL** tab, select **Backup logs periodically** option.

Veeam Backup & Replication will create an auxiliary job that runs continuously and ships database transaction logs. Transaction logs are shipped to the backup repository and saved in .VLB files next to other backup job files. Thus, you have a chain of restore points and a set of transaction logs that cover intervals between these restore points.



8. At the **Schedule** step of the wizard, define scheduling settings for the job.
9. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.

10. In the inventory pane of the **Home** view, expand the **Last 24 Hours** node to see the created jobs. You must see two jobs: one that processes the Microsoft SQL Server and the other one that ships transaction logs.



Reference

For more information on application-aware backups, see Application-Aware Processing (VMware vSphere) and Application-Aware Processing (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Data Recovery

Veeam Backup & Replication allows you to perform the following data recovery operations:

- Restore entire VM
- Restore guest OS files
- [For VMware vSphere] Restore VM virtual disks
- Recover VM files
- Recover application items
- Export disks

Restoring Entire VM

If a VM fails, you can restore it from a backup file. You can restore a single VM or multiple VMs to the original or new location.

In this section, you will learn how to restore a VM to the original location.

Before You Begin

Before you restore a VM from a backup, consider the following:

- You can restore the VM from a backup that has at least one successfully created restore point.

  To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

- [For VMware vSphere] When you restore the VM to its original location, and the original VM is still running, Veeam Backup & Replication powers off the original VM and restores only those disks that are included in the backup. All other disks remain unchanged.

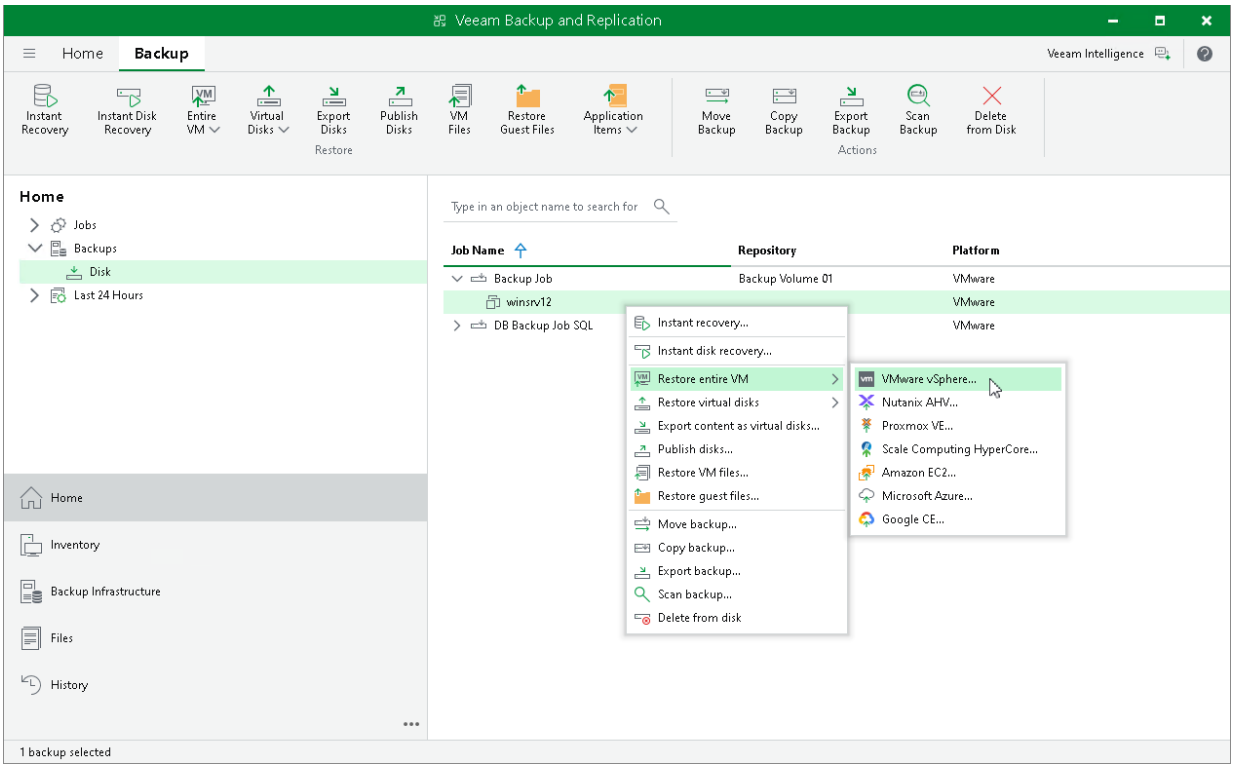
- [For Microsoft Hyper-V] When you restore the VM to its original location, and the original VM is still running, Veeam Backup & Replication powers off the original VM and deletes it before the restore.

Restoring Entire VM

To restore an entire VM to its original location, do the following.

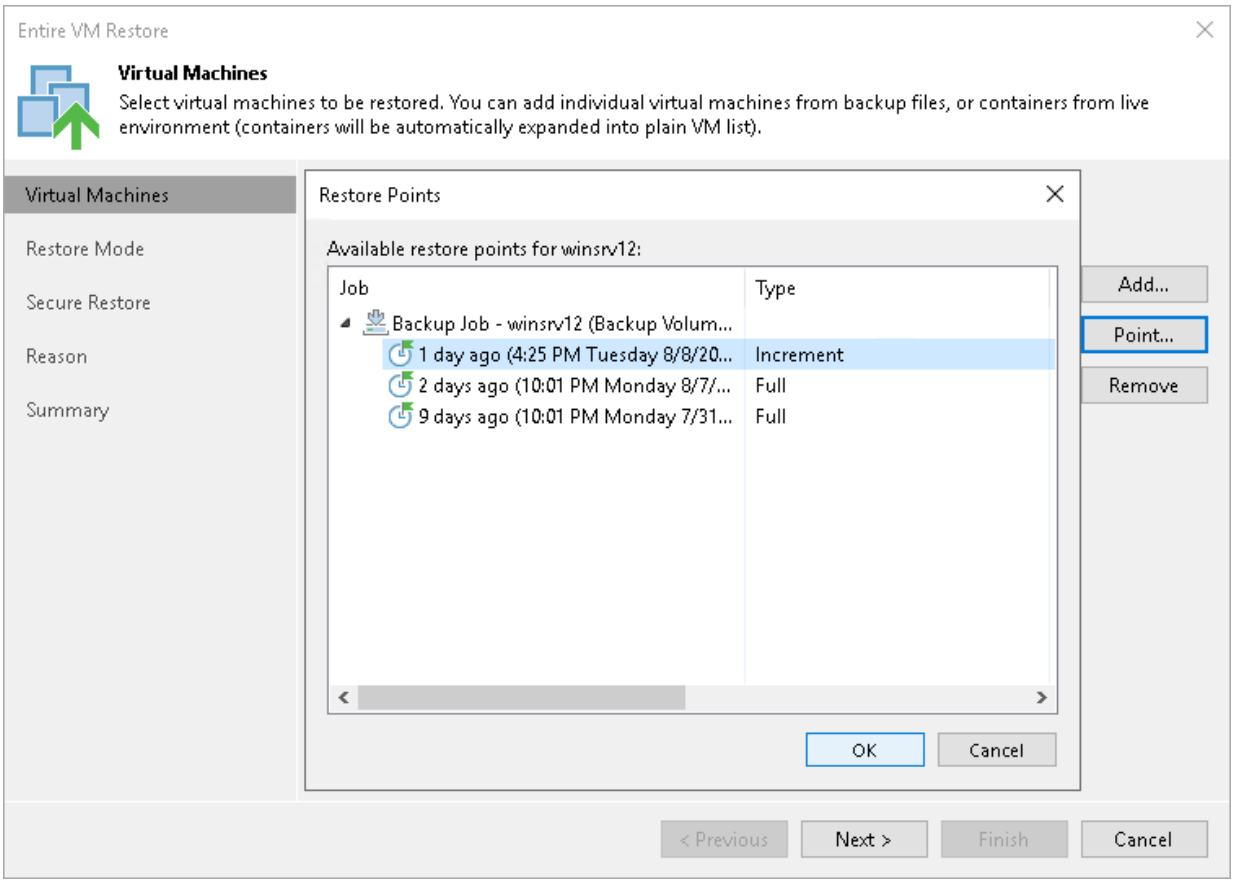
1. Open the **Home** view.

2. In the inventory pane, select the **Backups** > **Disk** node. Expand the backup job in the working area, right-click a VM in a backup job and select **Restore entire VM** > **VMware vSphere** to launch the **Entire VM Restore** wizard.



3. At the **Virtual Machines** step of the wizard, select the VM from the list, click the **Point** button and choose a restore point.

   If you select an incremental restore point, Veeam Backup & Replication automatically restores data blocks from the full backup file and the chain of incremental backup files.



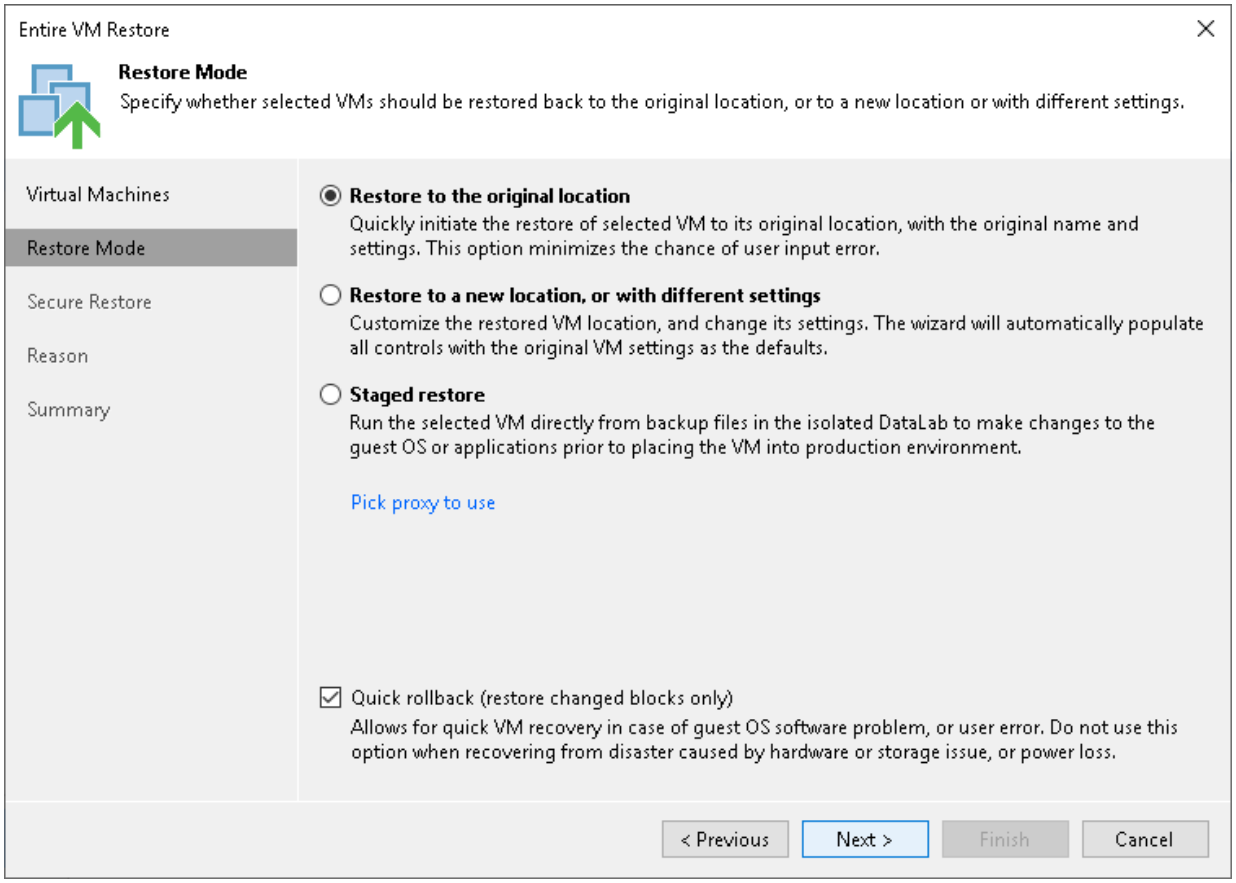
4. At the **Restore mode** step of the wizard, do the following:

   a. Select the **Restore to the original location** option.

   b. Select the **Quick rollback** check box.

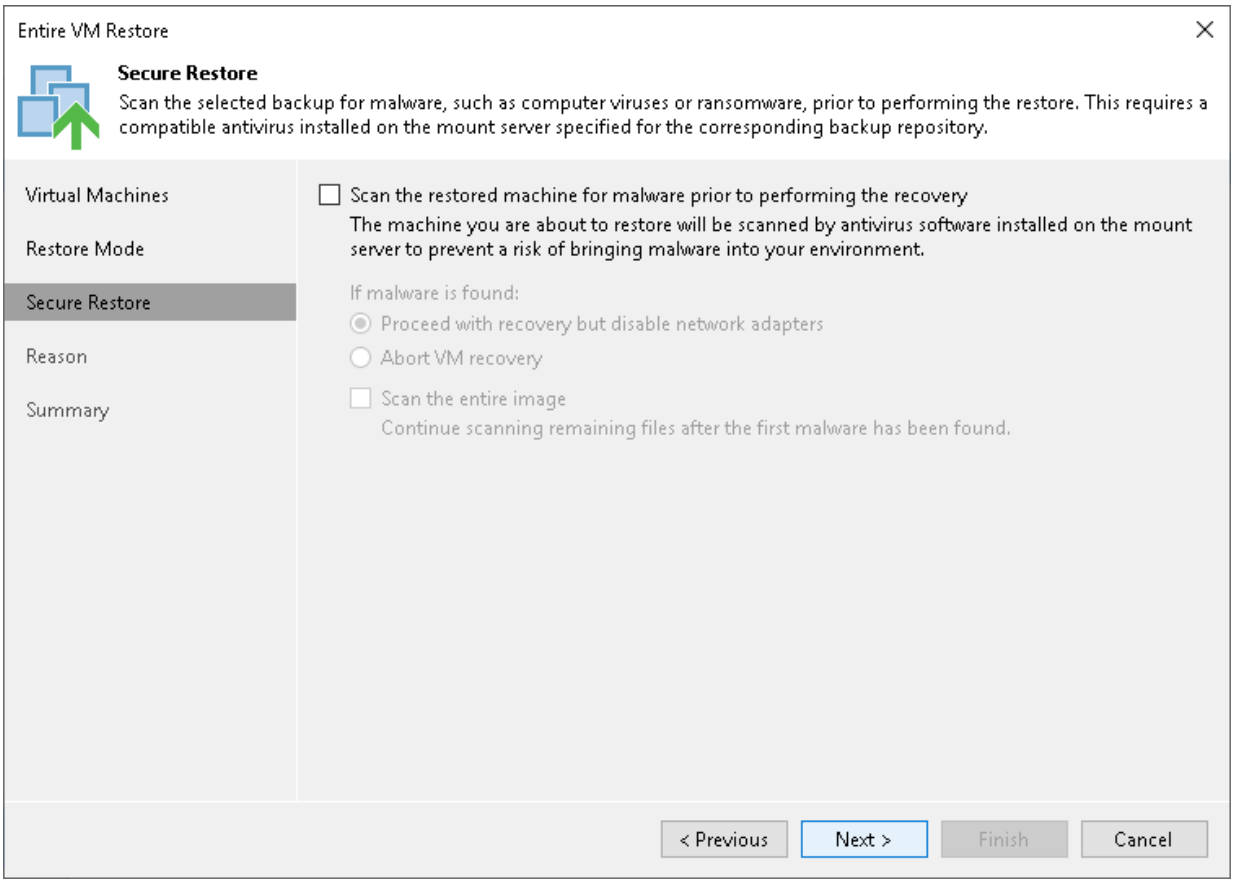
      Veeam Backup & Replication will get data blocks that are necessary to revert the VM to an earlier point in time and will restore only these data blocks from the backup. Quick rollback significantly reduces the restore time.

      > **IMPORTANT**
      >
      > Do not enable the **Quick rollback** option if the problem occurred at the VM hardware level, storage level or due to a power loss.


Entire VM Restore
Restore Mode
Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.
Virtual Machines
Restore Mode
Secure Restore
Reason
Summary
Restore to the original location
Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.
Restore to a new location, or with different settings
Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.
Staged restore
Run the selected VM directly from backup files in the isolated DataLab to make changes to the guest OS or applications prior to placing the VM into production environment.
Pick proxy to use
Quick rollback (restore changed blocks only)
Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.
< Previous
Next >
Finish
Cancel

5. At the **Secure Restore** step of the wizard, enable scanning of the machine or leave the default settings.

   If secure restore is enabled, Veeam Backup & Replication uses antivirus software to scan machine data before restoring the machine to the production environment. For details, see the Secure Restore section in the Veeam Backup & Replication User Guide.



6. At the **Reason** step of the wizard, specify the reason for restoring the VM.
7. At the **Summary** step of the wizard, select the **Power on VM after restoring** check box and click **Finish**.

Reference

For more information on how to restore the VM to another location, see the Restoring Entire VM (VMware vSphere) and Restoring Entire VM (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Restoring VM Files

Veeam Backup & Replication can help you restore VM files. For example, your VM configuration file is missing and you need to restore it. Instead of restoring the entire VM image, you can restore a single VM file.

You can restore VM files to the latest state or any valid point in time. You can also restore them to the original or new location.

Before You Begin

Before you restore VM files from a backup, consider the following:

- You can restore VM files a backup that has at least one successfully created restore point.

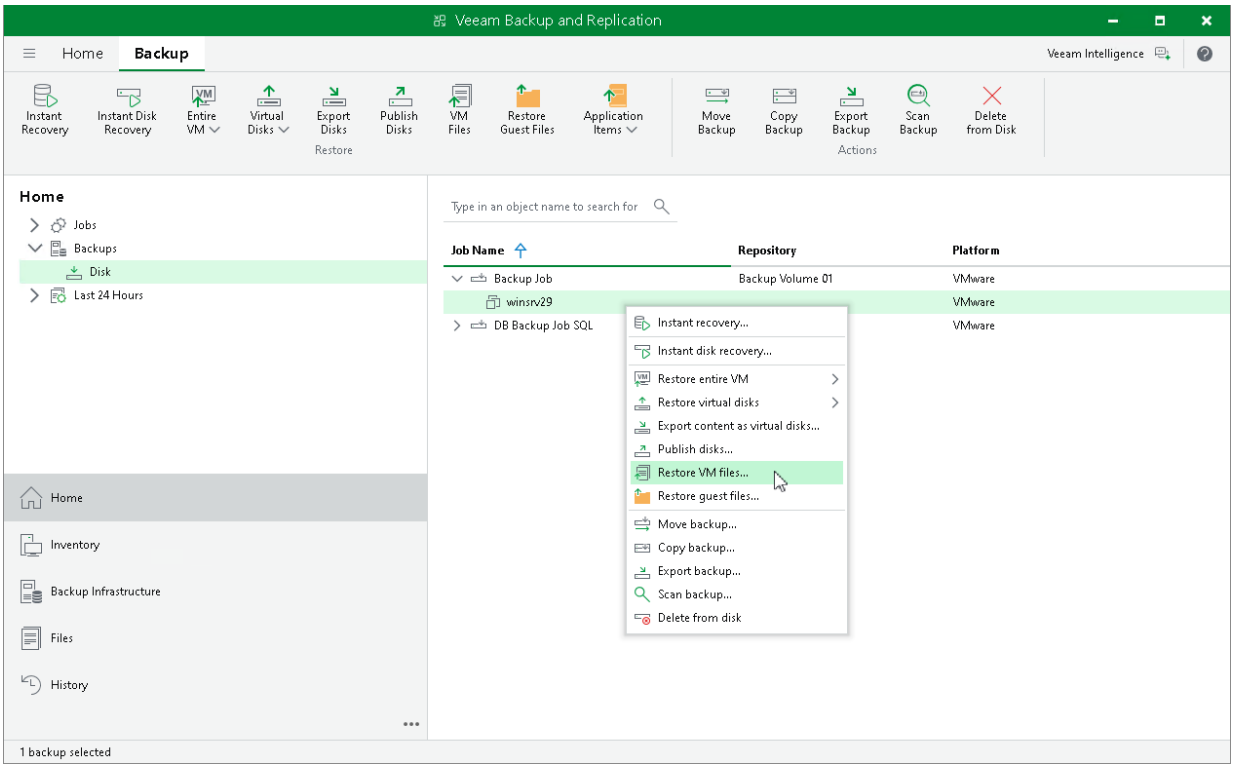
  To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

- The server on which you plan to save the restored VM files must be added to the backup infrastructure.

Restoring VM Files

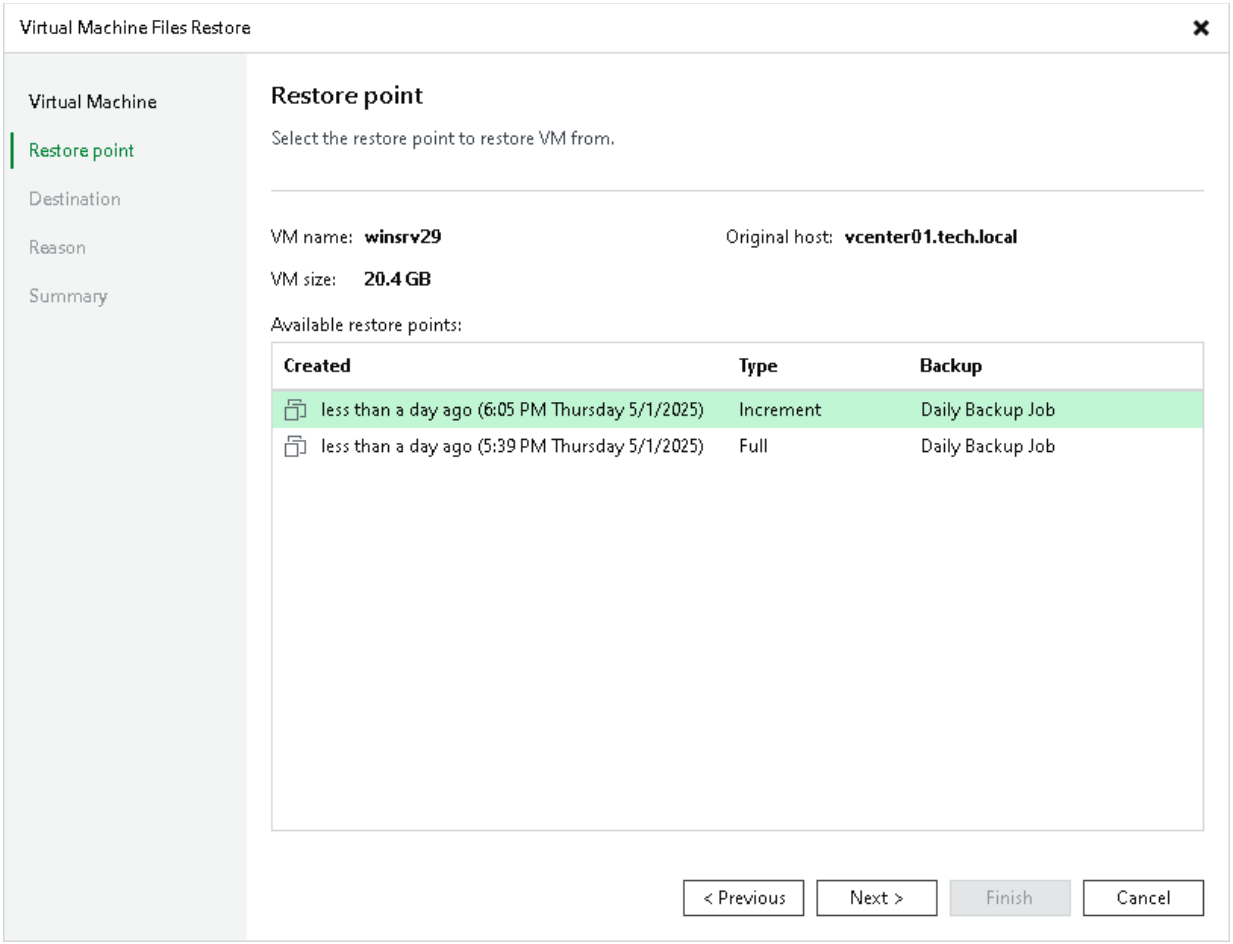
To recover VM files, do the following.

1. Open the **Home** view.
2. In the inventory pane, select the **Backups** > **Disk** node. Expand a backup job in the working area, right-click a VM and choose **Restore VM files** to launch the wizard.



3. At the **Restore Point** step of the wizard, select a restore point.

   If you select an incremental restore point, Veeam Backup & Replication automatically restores data blocks from the full backup file and the chain of incremental backup files.



4. At the **Destination** step of the wizard, do the following:
   a. In the **Server** list, select the server to which you want to restore VM files.
   b. In the **Path to folder** field, specify the path to the folder where you want to restore files.
   c. In the **VM files to restore** section, select the required files.
5. At the **Reason** step of the wizard, specify the reason for restoring files.
6. At the **Summary** step of the wizard, click **Finish** to restore the VM files.

Reference

For more information on restoring VM files, see the VM Files Restore (VMware vSphere) and VM Files Restore (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Restoring VM Virtual Disks

Veeam Backup & Replication allows you to recover individual virtual disks of a VMware vSphere VM. Recovered virtual disks can be attached to the original VM or to any other VM. This recovery option can be helpful if a VM virtual disk becomes corrupted.

You can restore VM virtual disk to the latest state or any valid restore point. You can preserve the format of a recovered virtual disk or convert it to the thin or thick provisioned disk format.

> **NOTE:**
>
> Restore of VM virtual disks is not available for Microsoft Hyper-V VMs.

Before You Begin

Before you restore VM virtual disks from a backup, consider the following:

- You can restore virtual disks from a backup that has at least one successfully created restore point.

  To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

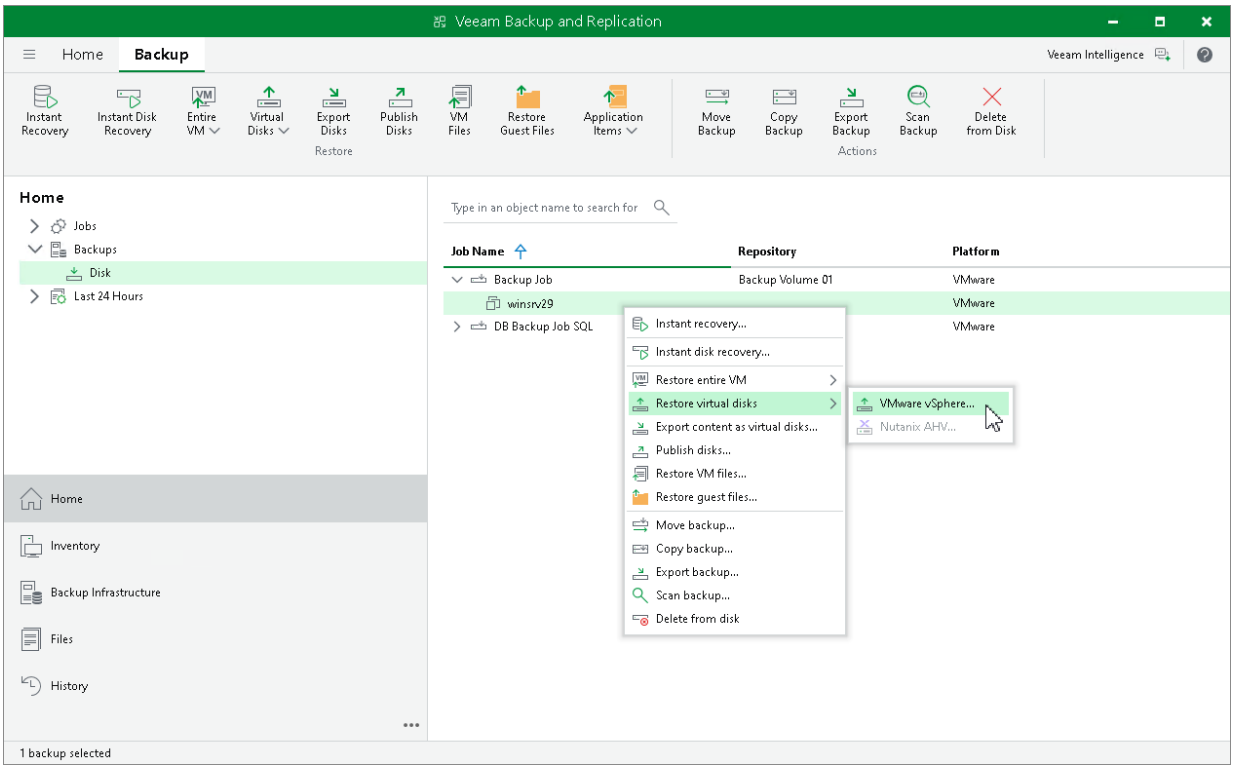
- During the virtual disk restore, Veeam Backup & Replication turns off the target VM (the VM to which you plan to attach the restored virtual disk) to reconfigure its settings and connect restored disks. It is recommended that you stop all activities on the target VM for the restore period.

Restoring Virtual Disks

To restore a VM virtual disk and attach it to another VM as a new drive, do the following:

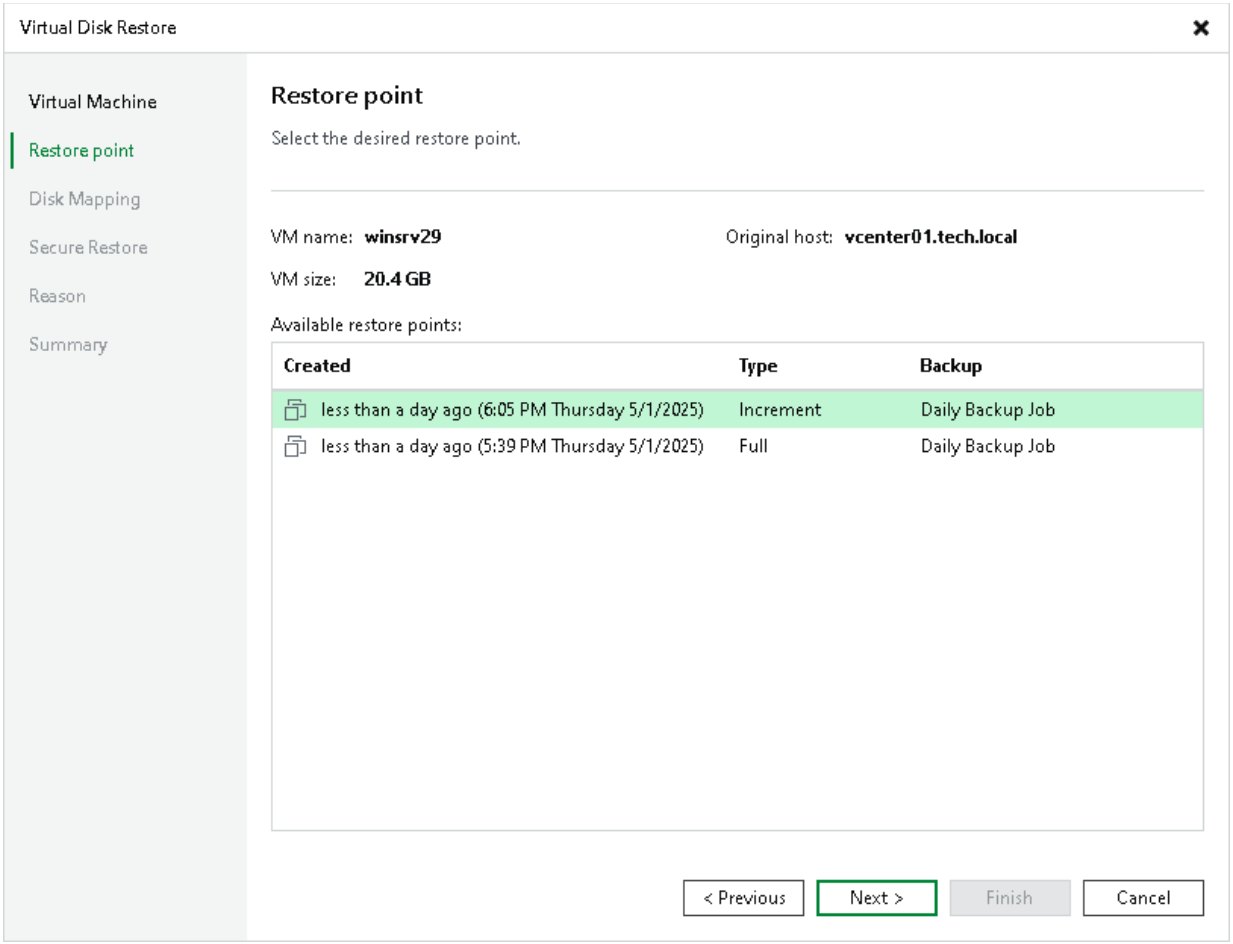
1. Open the **Home** view.

2. In the inventory pane, select the **Backups** > **Disk** node. Expand the backup job in the working area, right-click a VM and select **Restore virtual disks** > **VMware vSphere** to launch the **Virtual Disk Restore** wizard.



3. At the **Restore Point** step of the wizard, select a restore point.

   If you select an incremental restore point, Veeam Backup & Replication automatically restores data blocks from the full backup file and the chain of incremental backup files.



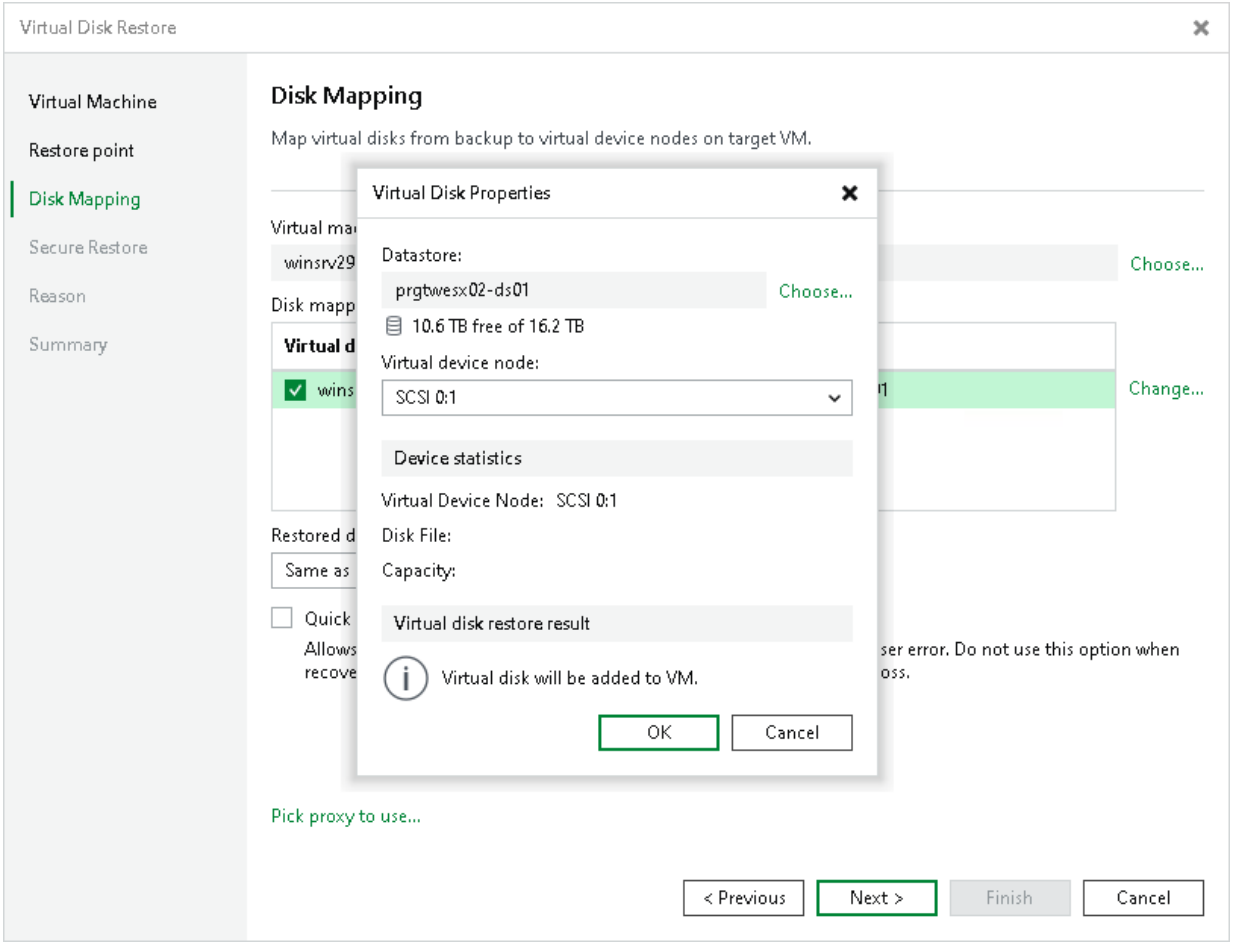
4. At the **Disk Mapping** step of the wizard, do the following:

   a. Click **Browse** and select the VM to which the restored hard disk must be attached.

   b. Select the virtual hard disk that you want to restore.

   c. To change the disk format, select the required option from the **Restored disk type** list: same as the original disk, thin or thick (lazy or eager zeroed).

d. Select the VM disk in the list and click **Change**. From the **Virtual device node** list, select a node that is not occupied yet. Click **OK**.



5. At the **Secure Restore** step of the wizard, enable scanning of the machine or leave the default setting.

   If secure restore is enabled, Veeam Backup & Replication uses antivirus software to scan machine data before restoring the machine to the production environment. For details, see the Secure Restore section in the Veeam Backup & Replication User Guide.

6. At the **Reason** step of the wizard, specify the reason for restoring.

7. At the last step of the wizard, select the **Power on VM after restoring** check box and click **Finish**.

Reference

For more information on restoring virtual disks, see the Virtual Disks Restore section in the Veeam Backup & Replication User Guide.

Restoring Guest OS Files

Veeam Backup & Replication allows you to recover individual guest OS files and folders. You can restore files and folders directly from a backup or replica. This makes the restore process fast and does not require additional storage resources. For more information on guest OS restore, see the Guest OS File Restore section in the Veeam Backup & Replication User Guide.

Before You Begin

Consider the following:

- Check the supported file systems. For details, see the File-Level Restore section in the Veeam Backup & Replication User Guide.
- You can restore guest OS files from a backup that has at least one successfully created restore point.

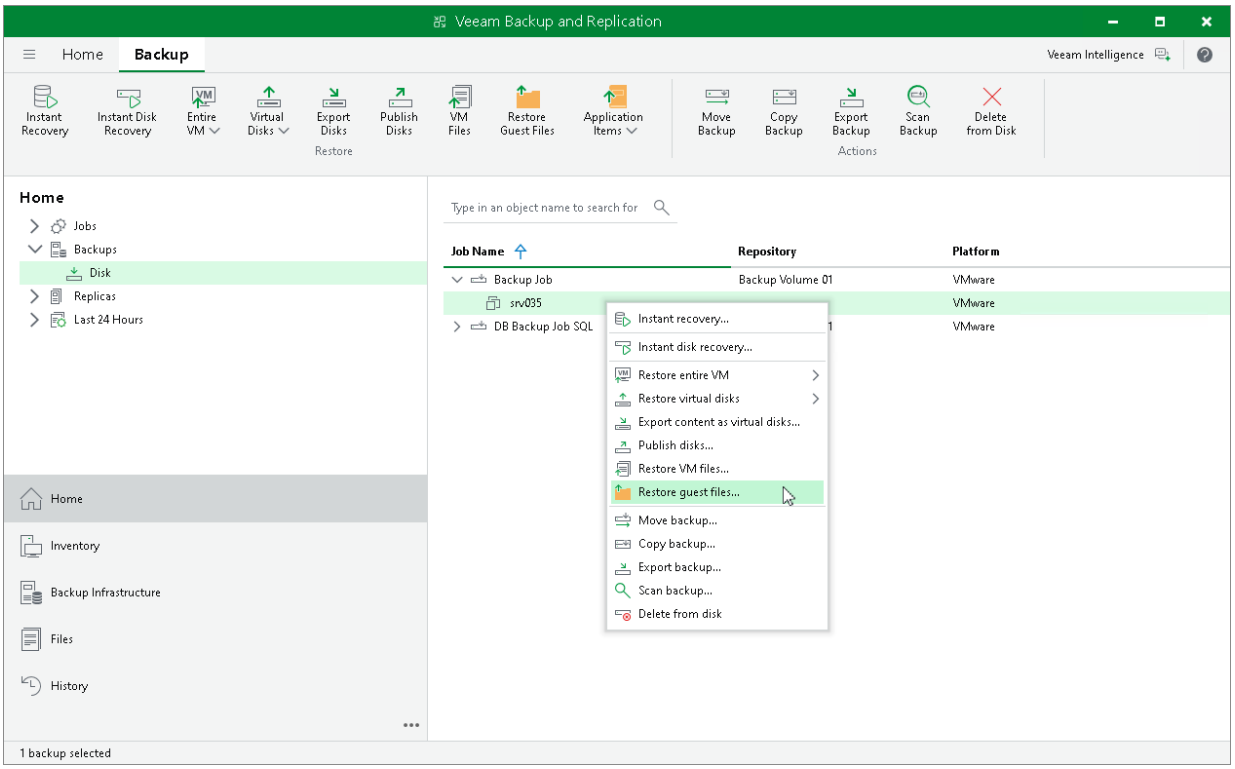
  To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.
- You cannot restore files from a VM being currently backed up or replicated.
- For the full list of considerations and imitations, see the Considerations and Limitations section in the Veeam Backup & Replication User Guide.

Restoring Guest OS Files

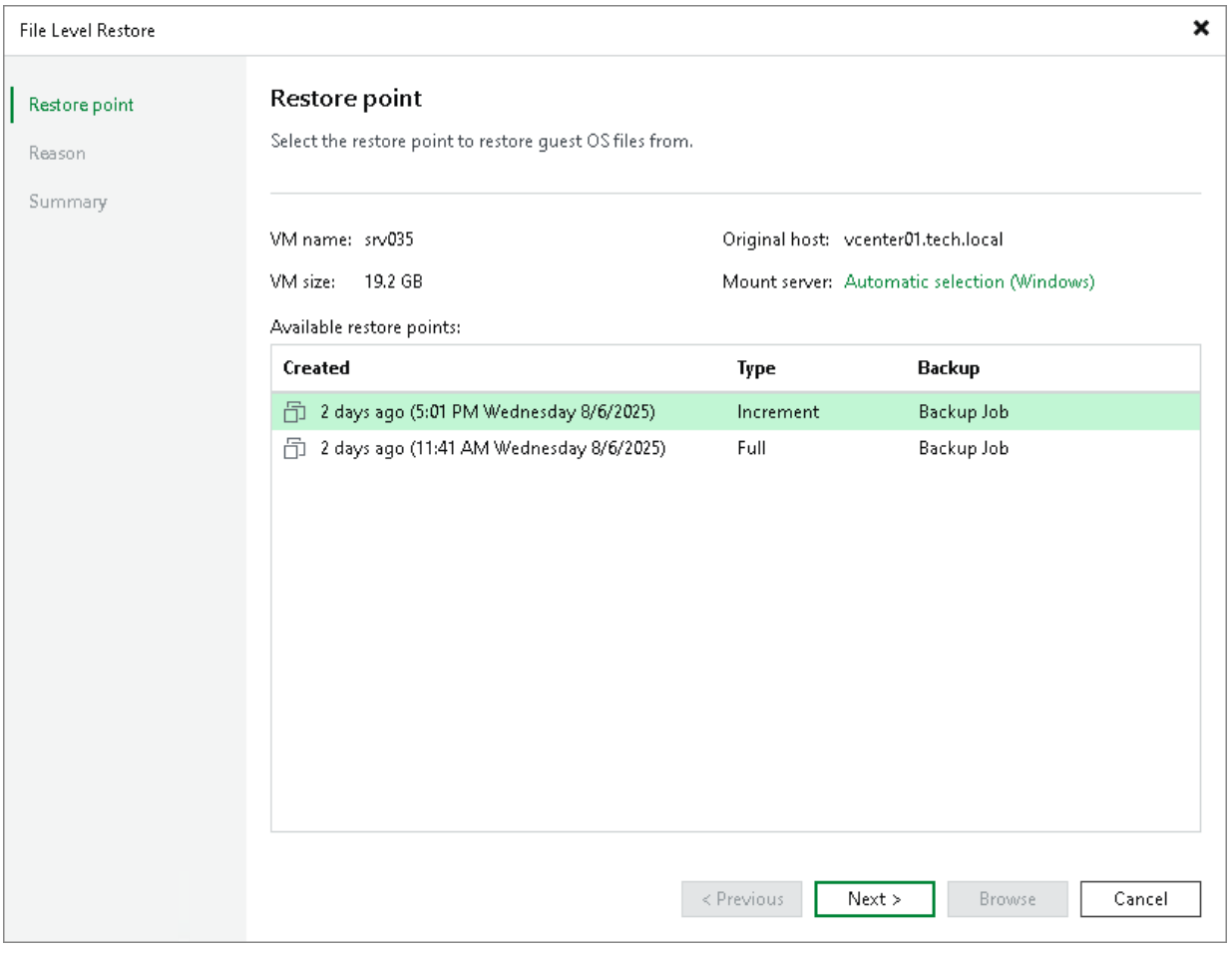
To recover guest OS files, do the following:

1. Open the **Home** view.

2. In the inventory pane, select the **Backups** > **Disk** node. Expand a backup job in the working area, right-click a VM and choose **Restore guest files** > **Microsoft Windows** to launch the **File Level Restore** wizard.



3. At the **Restore Point** step of the wizard, select the necessary restore point. For the mount server, leave the default option.



4. At the **Reason** step of the wizard, specify the reason for restoring.
5. At the last step of the wizard, click **Browse**.
6. Veeam Backup & Replication will display the **Backup Browser** window with the file system tree of the VM. Right-click the necessary file or folder, select **Copy To**.

   For the full list of available operations, see the Finalize Recovery section in the Veeam Backup & Replication User Guide.
7. In the opened window, specify the location to which you want to restore files or folders. This location can be a network shared folder, a folder on the backup server or, for Linux file restore, to a Linux server that is not added to the Veeam Backup & Replication infrastructure.

Reference

For more information on restoring guest OS files, see the Restore from FAT, NTFS or ReFS section in the Veeam Backup & Replication User Guide.

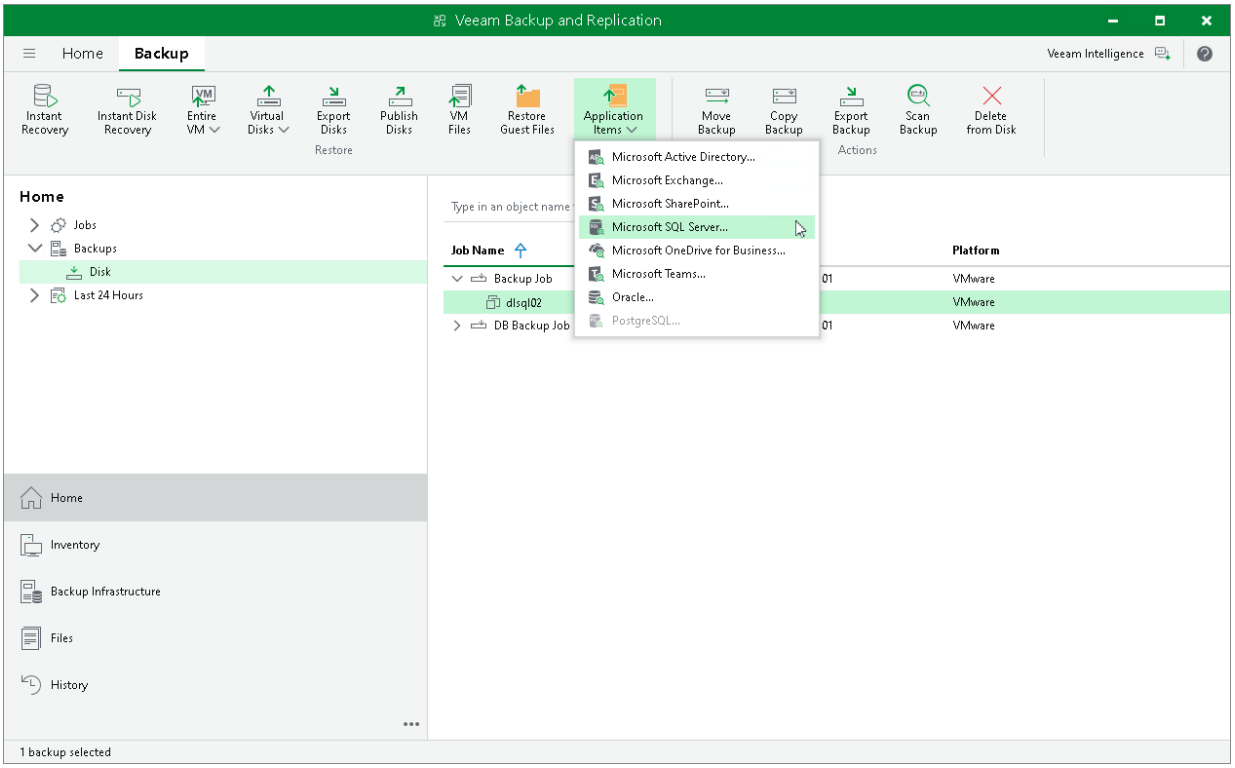
Restoring Application Items

If you have an application-aware backup, you can restore application items for Microsoft SQL Server, Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, and Oracle Database. To restore application items, Veeam Backup & Replication uses special built-in tools — Veeam Explorers.

Veeam Explorers mount the file system of the backed up VM, detect available applications and display their content in the convenient interface. You can then browse for necessary application items and restore them to the original or new location. For details, see the Veeam Backup Explorers User Guide.

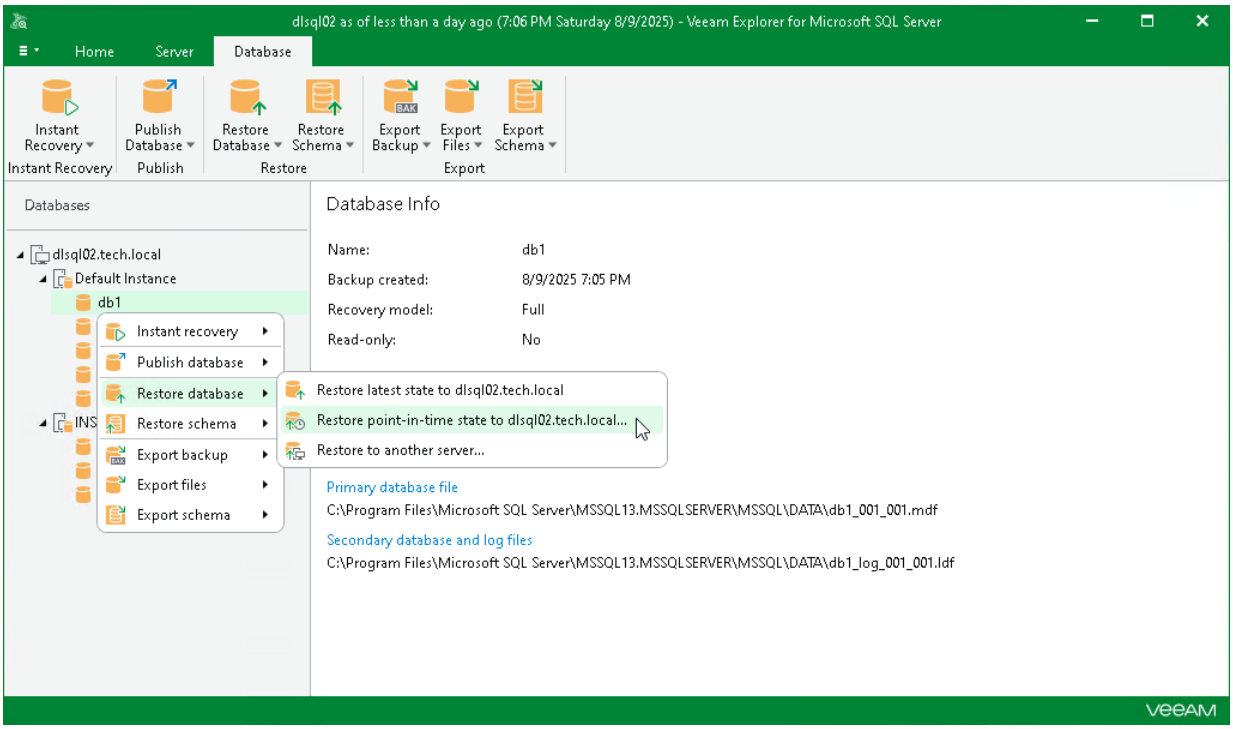
In this section, you will learn how to restore application items for the Microsoft SQL Server. For this purpose, you will use the backup created in Creating Application-Aware Backup Job.

1. In the inventory pane of the **Home** view, click the **Backups** node.
2. In the working area, expand the backup job that processes the VM with Microsoft SQL Server. Select the VM and click **Restore application items** > **Microsoft SQL Server databases** on the ribbon to open the **Microsoft SQL Server Database Restore** wizard.



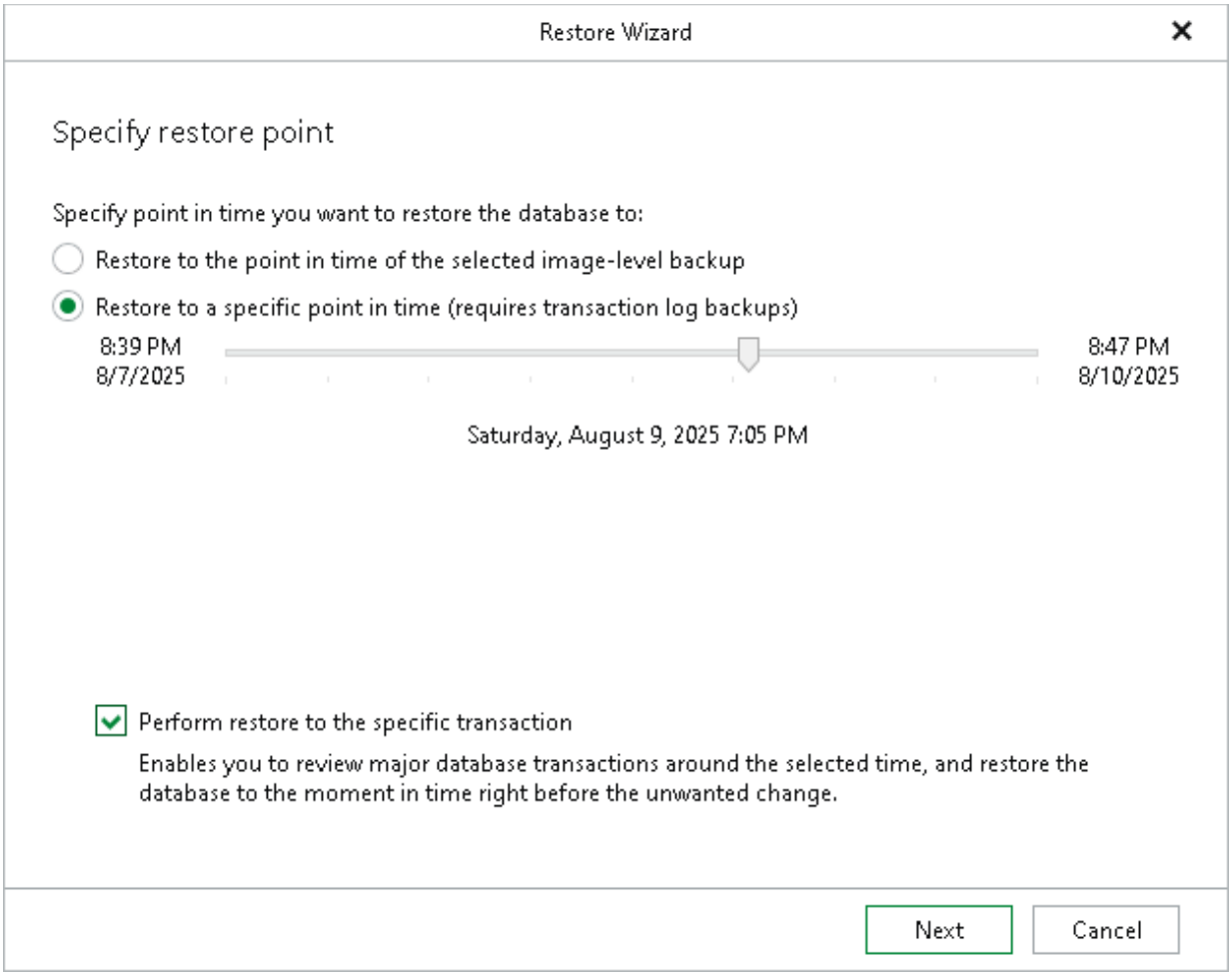
3. At the **Restore Point** step of the wizard, select the required restore point.
4. At the **Reason** step of the wizard, specify the reason for restoring.
5. At the last step of the wizard, click **Finish** to start the recovery process.
6. Veeam Backup & Replication will display the **Veeam Explorer for Microsoft SQL Server** window with available databases.

7. In the **Databases** pane of the window, right-click a database and select **Restore point-in-time state to <Microsoft SQL Server\Instance Name>**.



8. At the **Specify restore point** step of the wizard:
   a. Select the **Restore to a specific point in time** option.
   b. Use the slider to define the exact point in time to which you want to restore the database.

c. Select the **Perform restore to the specific transaction** check box and click **Next**.



9. At the **Fine-tune the restore point** step of the wizard, select the transaction to which you want to restore the database and click **Restore**.

   Veeam Backup & Replication will start restoring the database to the selected transaction. When the restore process is complete, Veeam Explorer for Microsoft SQL Server will display a popup message with the results of the restore operation.

Reference

For more information on restoring application items, see Application Items Restore in the Veeam Backup & Replication User Guide.

Exporting Disks

Veeam Backup & Replication allows you to export disks, that is, convert disks of different workloads (EC2 instances, Microsoft Azure VMs and so on) in the VMDK, VHD or VHDX formats. You can save the exported disks to any server added to the backup infrastructure or place disks on a datastore connected to a host.

Before You Begin

Before you export content as virtual disks, consider the following:

- You can export disks from a backup that has at least one successfully created restore point.

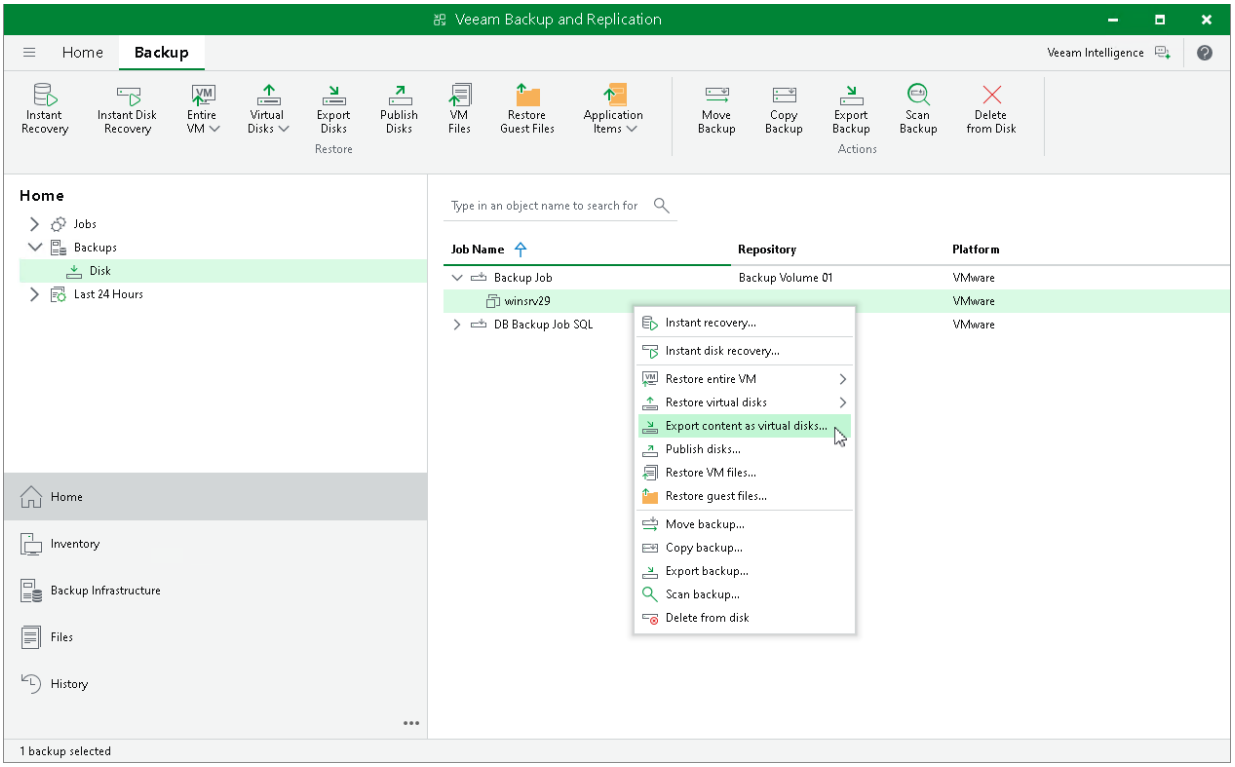
  To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available for the VM.

- If you export disks to an ESXi datastore, VMDK format is the only available option.

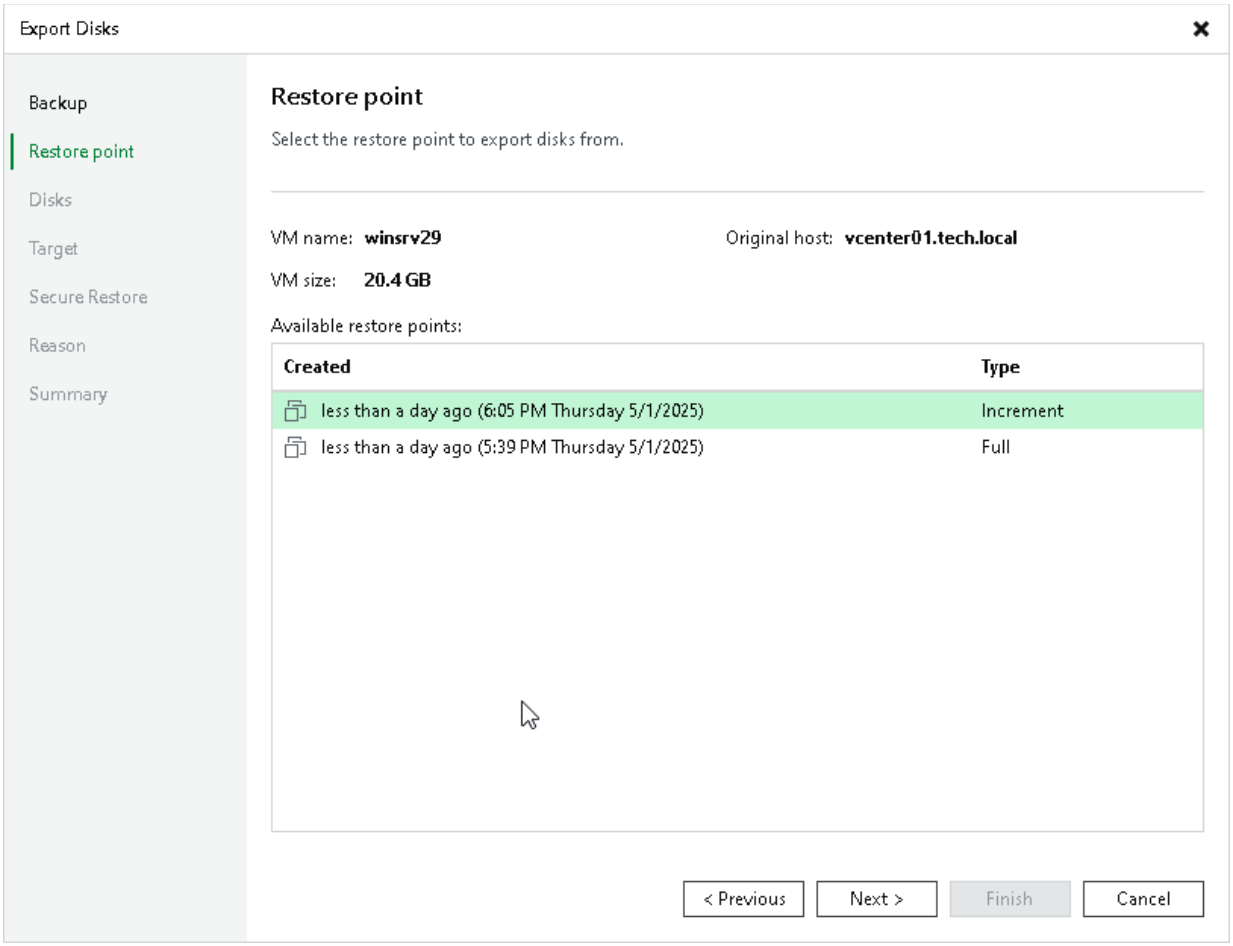
Exporting Disks

To export disks from backups and convert them into VMDK format for Microsoft Hyper-V VMs or VHD/VHDX format for VMware vSphere VMs, do the following:

1. Open the **Home** view.
2. In the inventory pane, select the **Backups** > **Disk** node. Expand the backup job in the working area, right-click a VM and select **Export content as virtual disks** to launch the **Export Disk** wizard.



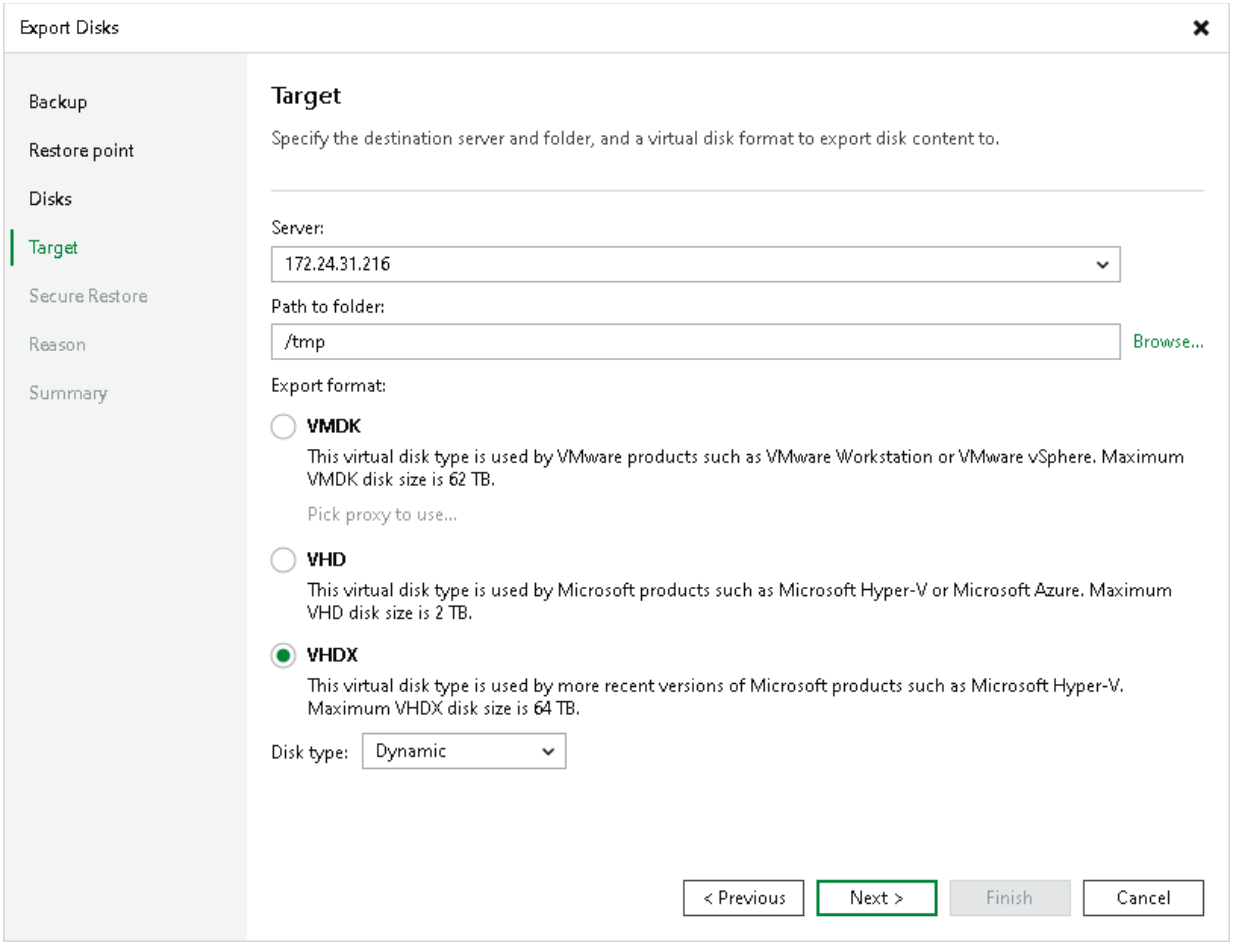
3. At the **Restore Point** step of the wizard, select a restore point.



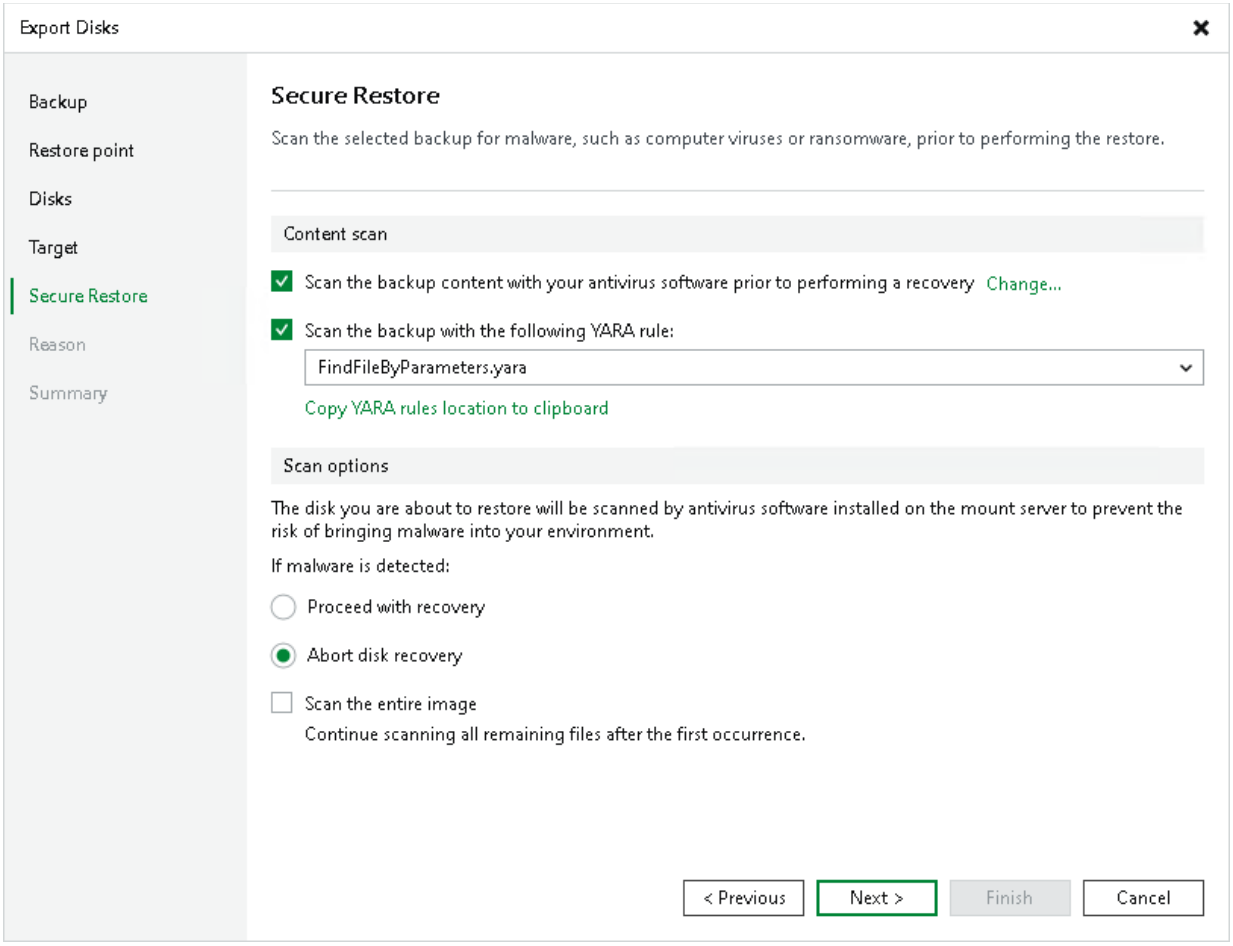
4. At the **Disks** step of the wizard, select which disks you want to export.
5. At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disks:
   a. From the **Server** list, select a server on which the resulting virtual disks must be saved.
   b. In the **Path to folder** field, specify a datastore or folder on the server where the virtual disks must be placed.
   c. In the **Export format** list, select VMDK format to save the resulting virtual disk in the VMware vSphere compatible format. Select VHD/VHDX format to save the resulting virtual disk in the Microsoft Hyper-V VHD/VHDX format.

d. From the **Disk Type** drop-down list, select a disk type for the exported disks.

[For Microsoft Hyper-V] Disk type selection for VMDK format is available when the disk is exported to an ESXi host, in all other cases it is **Thick (lazy)** type by default.



6. At the **Secure Restore** step of the wizard, you can instruct Veeam Backup & Replication to perform secure restore — scan exported disk data with antivirus software before restoring the disk. For more information on secure restore, see Secure Restore.



7. At the **Reason** step of the wizard, enter a reason for disk export.
8. At the **Summary** step of the wizard, review the configured settings and click **Finish**.

Reference

For more information on exporting disks, see the Exporting Disks section in the Veeam Backup & Replication User Guide.

Backup Copy

Backup copy allows you to create several instances of the same backup data in different locations. This is the mechanism that Veeam Backup & Replication provides to help you follow the the 3-2-1 rule:

- 3: You must have at least three copies of your data: the original production data and two backups.
- 2: You must use at least two different types of media to store copies of your data, for example, local disk and cloud.
- 1: You must keep at least one backup offsite (for example, in the cloud or in a remote site).

In Veeam Backup & Replication, backup copy is a job-driven process. When the backup copying job starts, Veeam Backup & Replication accesses backup files on the source backup repository, retrieves data blocks for a specific machine from the backup file, copies them to the target backup repository, and composes copied blocks into a backup file on the target backup repository. This backup file has the same format as the primary backup file.

Before You Begin

Before you create a backup copy job, consider the following:

- The source and target backup repositories that take part in the backup copy process must be added to the backup infrastructure.
- You must have a backup that has been successfully run at least once.

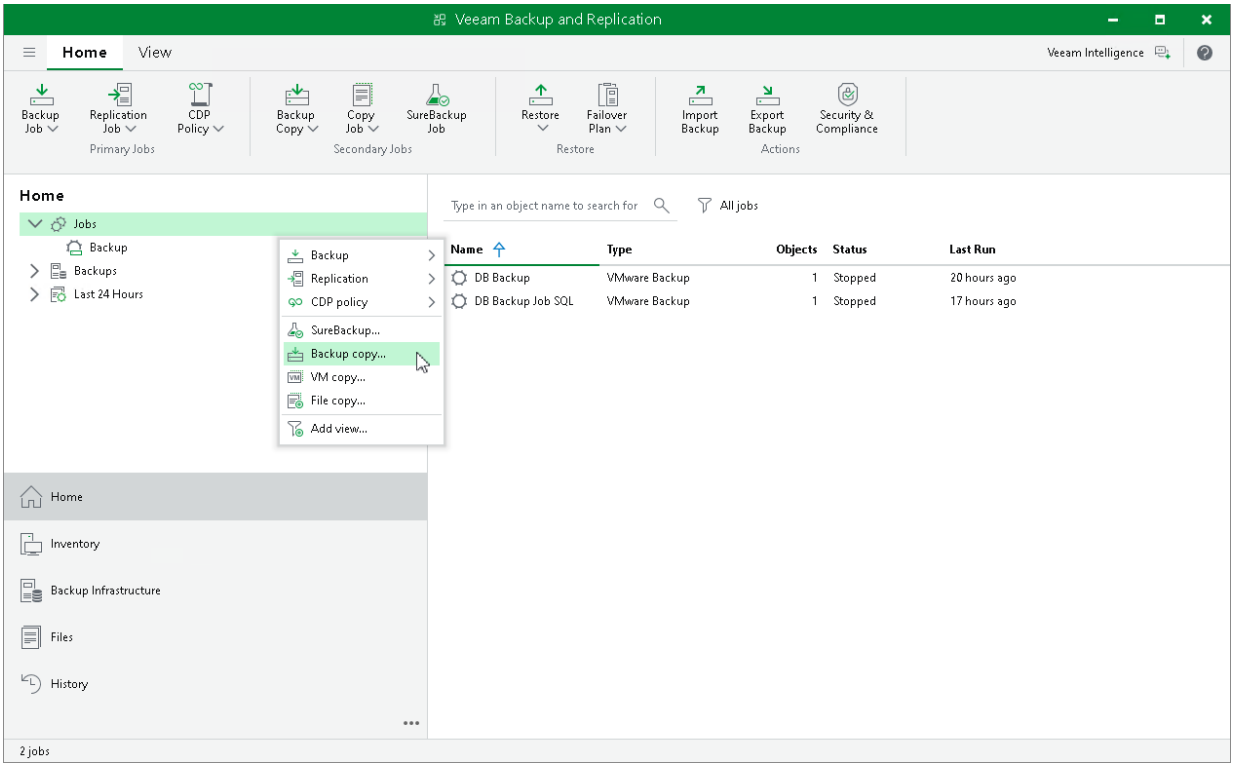
  To check whether restore points are created, open the inventory pane of the **Home** view and select the **Backups** node. Then, expand the backup job and verify that there is at least one restore point available.

Creating Backup Copy Job

To create a backup copy job, do the following:

1. Open the **Home** view.

2. In the inventory pane, right-click **Jobs** and select **Backup Copy** to launch the **New Backup Copy Job** wizard.

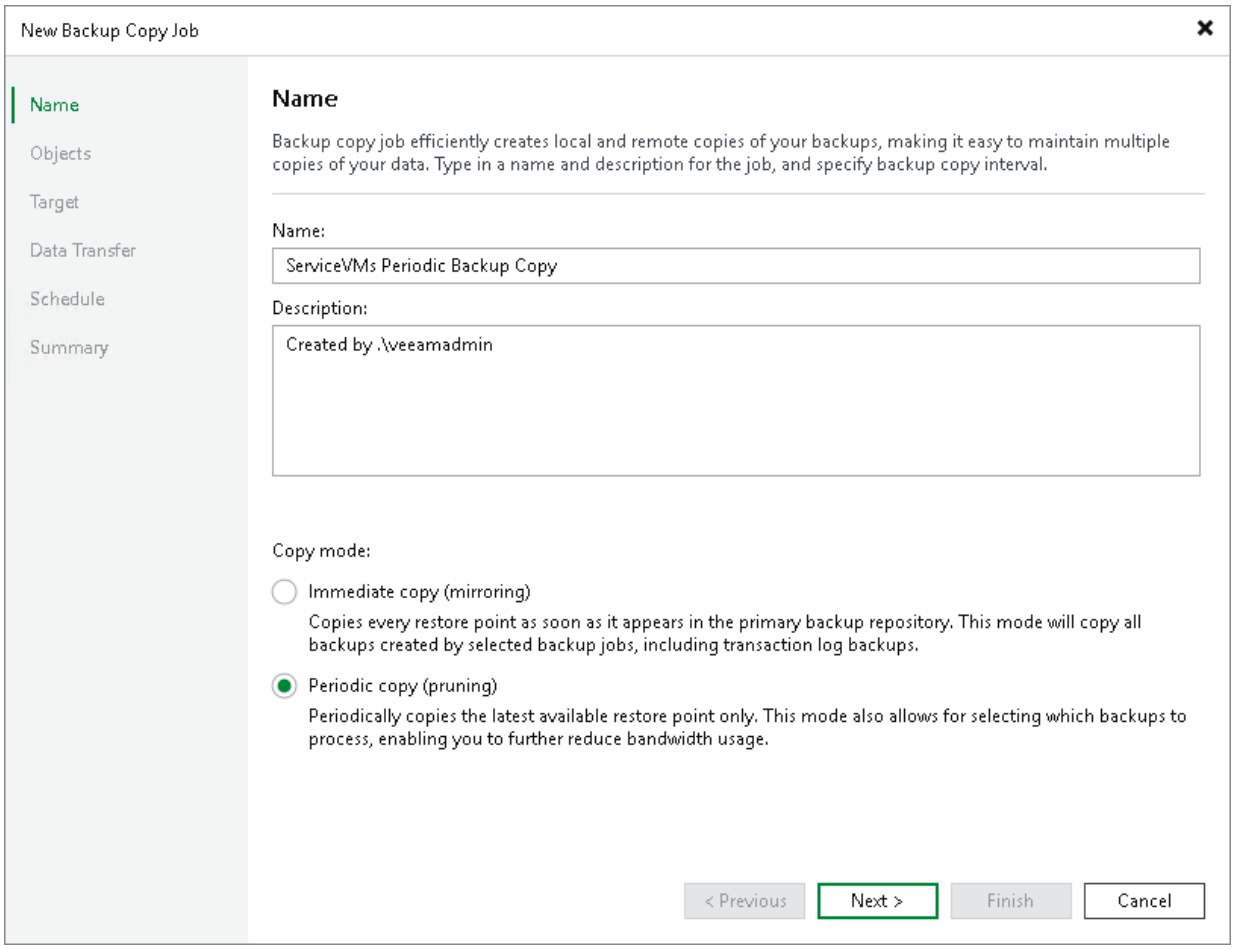


3. At the **Job** step of the wizard, do the following:

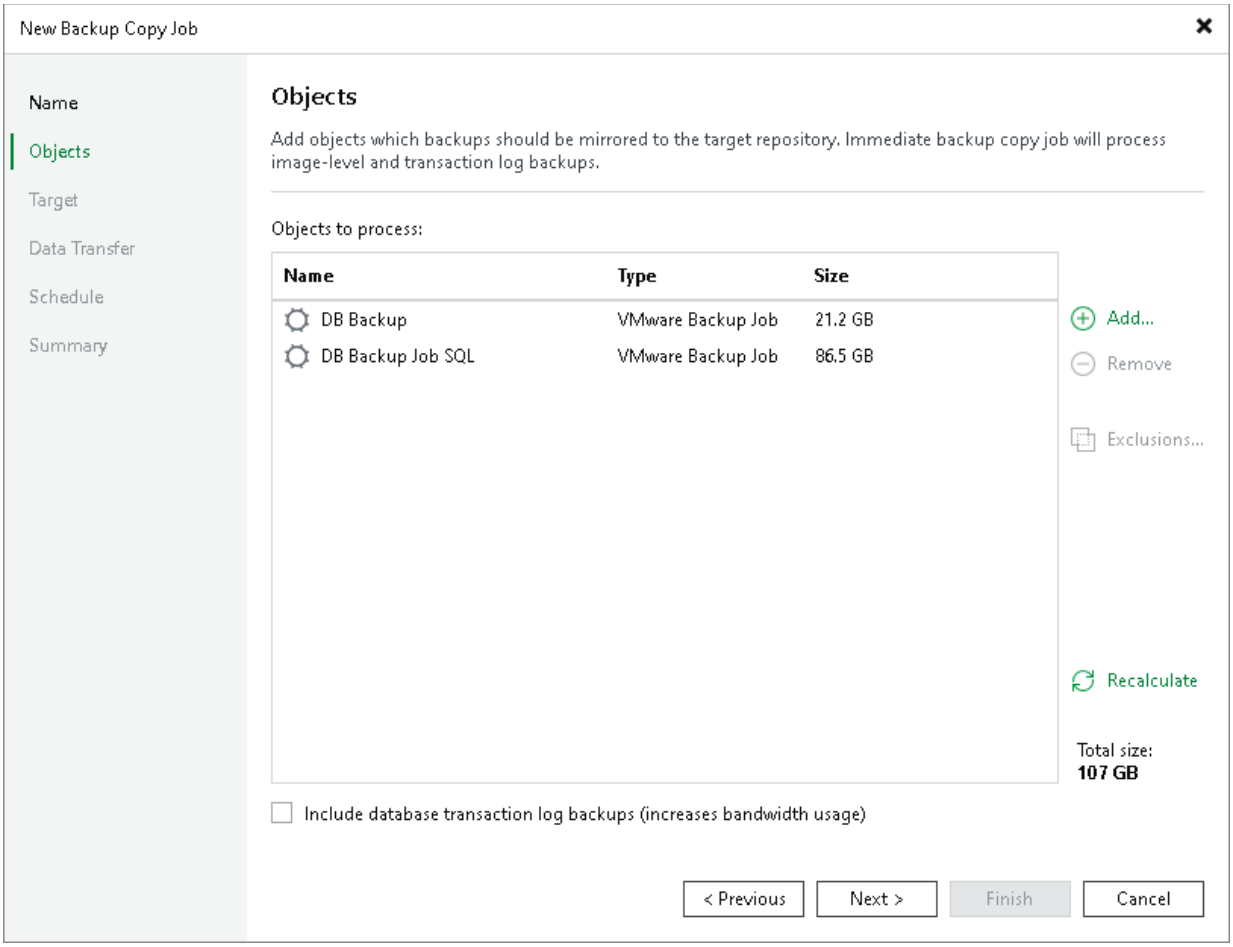
   a. Specify a name and description for the backup copy job.

b. In the **Copy mode** field, check that the **Immediate copy** is selected.

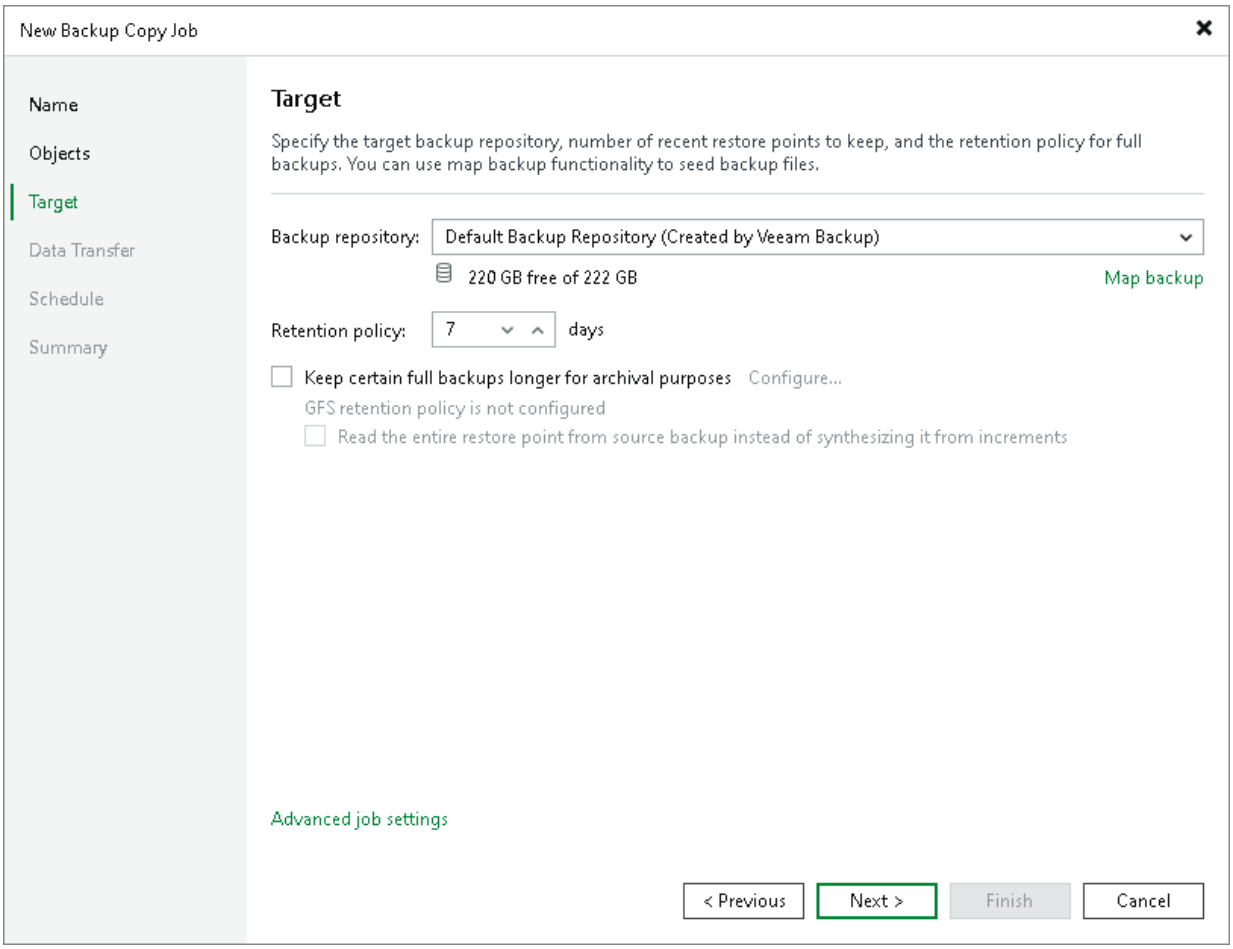
In the immediate copy mode, Veeam Backup & Replication copies new data as soon as it appears on the source repository. For more information, see the Backup Copy Modes section in the Veeam Backup & Replication User Guide.



4. At the **Objects** step of the wizard, click **Add** and select backup jobs that you want to copy.



5. At the **Target** step of the wizard, select the backup repository where you want to store the backup copy. For other settings, keep the default values.



6. At the **Data Transfer** step of the wizard, keep the default settings.
7. At the **Schedule** step of the wizard, define the period of time when the backup copy job is allowed to transport data over the network.
8. At the last step of the wizard, select the **Enable the job when I click Finish** check box and click **Finish**. The job will start running in the continuous mode.

Reference

For more information on the backup copy, see the Backup Copy section in the Veeam Backup & Replication User Guide.

VM Replication

When you replicate a VM, Veeam Backup & Replication creates the exact copy of the VM in the native VMware vSphere format on a host and keeps this copy synchronized with the original VM.

Replication provides the best recovery time objective (RTO) values. You actually have the copy of a VM in the ready-to-start state. That is why replication is recommended for VMs running most critical applications.

Replication is a job-driven process. During the first run of a replication job, Veeam Backup & Replication copies data of the original VM running on the source host and creates its full replica on the target host. During next job runs, Veeam Backup & Replication copies only those data blocks that have changed since the last replication job session. Veeam Backup & Replication writes these changes to restore points, so that you can further publish this replica in the required state.

Veeam Backup & Replication supports several replication scenarios. Depending on the location of the host where you plan to store replicas, you can choose the following scenarios:

- Onsite replication

  The target host is located in the same site as the source host.

- Offsite replication

  The target host is located on another site.

In this section, you will learn how to work with onsite replicas. For more information on offsite replication, see the Replication Scenarios (VMware vSphere) and Replication Scenarios (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Reference

For more information on replication, see the Replication (VMware vSphere) and Replication (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Creating Replication Job

Before You Begin

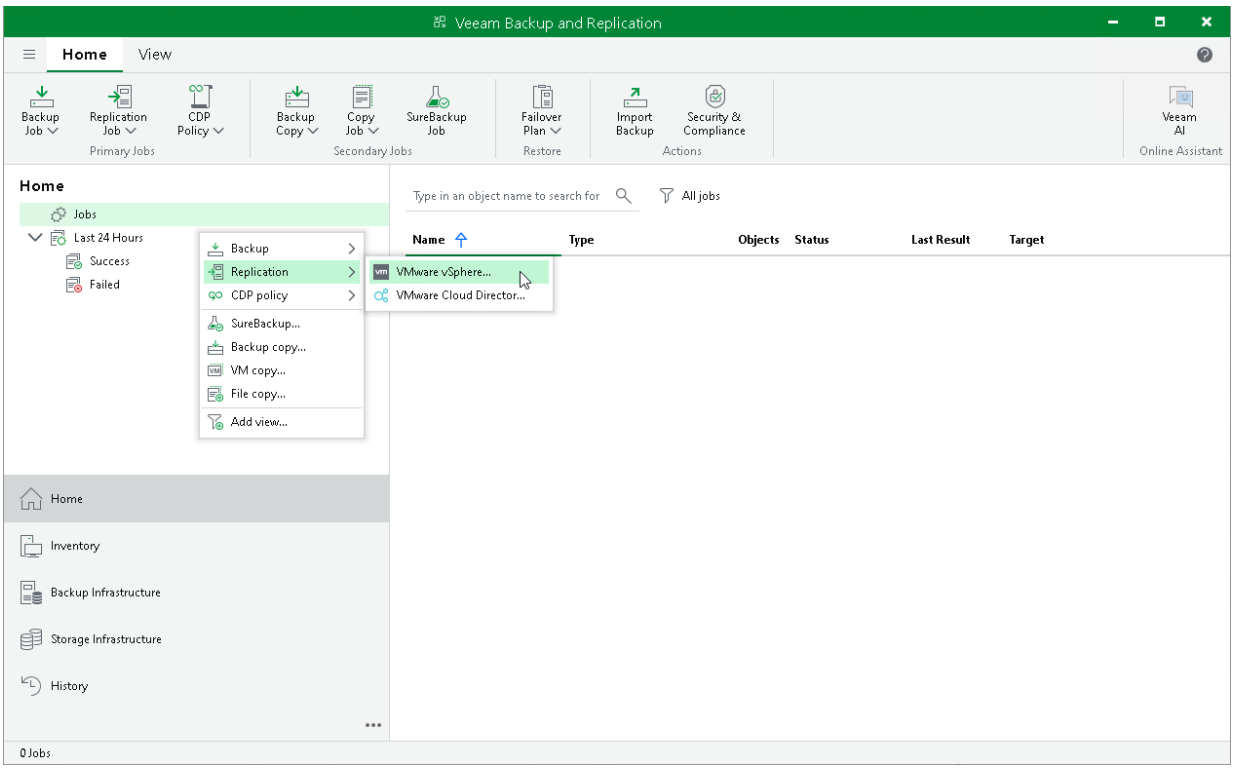
Before you replicate a VM, consider the following:

- You must add all components needed for the replication process to the backup infrastructure. These components are source and target hosts, backup proxy and backup repository.
- [For VMware vSphere] Due to VMware vSphere limitations, if you change the size of VM disks on the source VM, Veeam Backup & Replication deletes all available restore points on the VM replica during the next replication job session. For more information, see this Veeam KB article.
- [For Microsoft Hyper-V] You cannot replicate VMs with shared VHDX and VHDS disks.

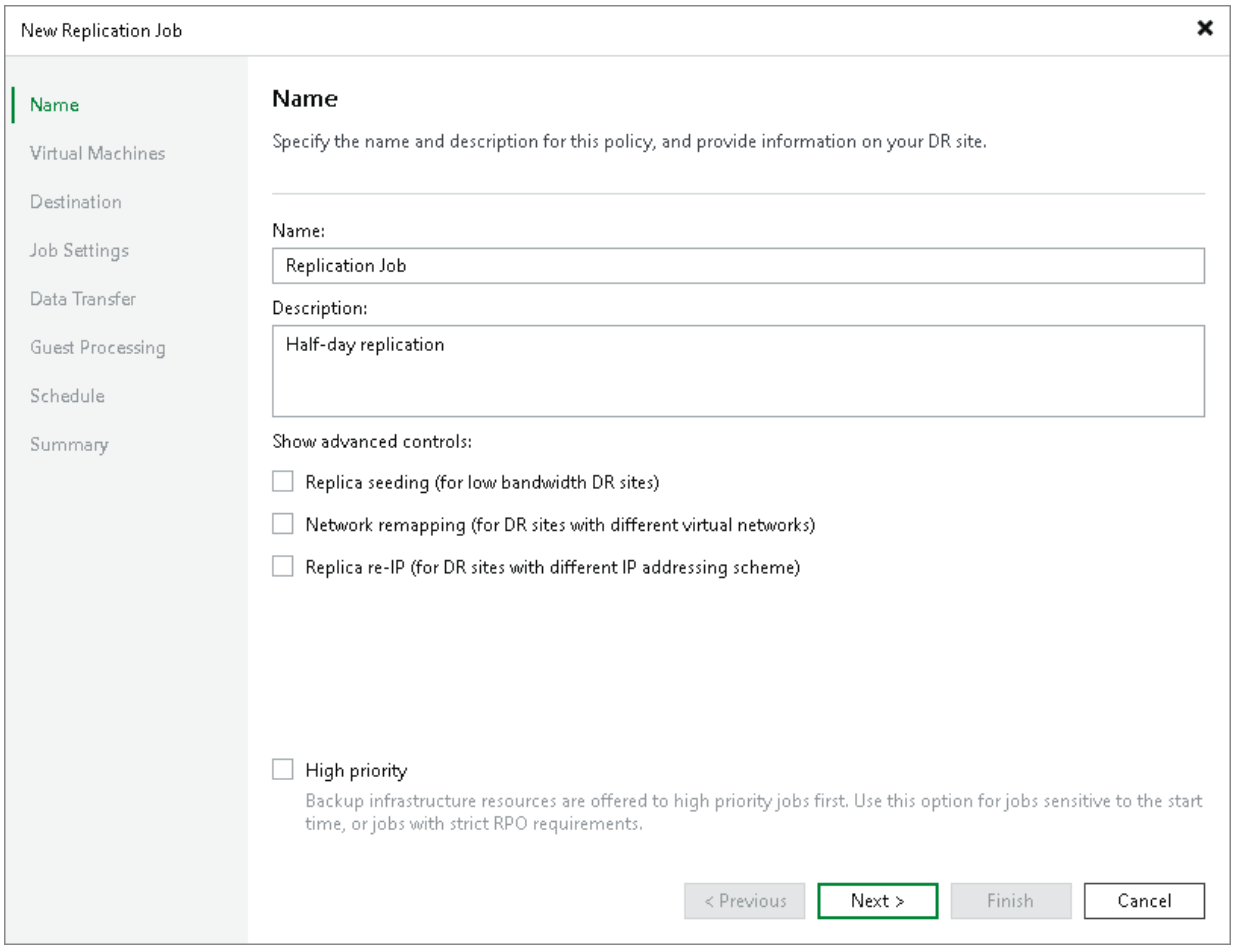
Creating Replication Job

To replicate a VM, do the following:

1. Open the **Home** view.
2. In the inventory pane of the **Home** view, right-click the **Jobs** node and select **Replication** > **Virtual machine** > *<platform>* to launch the **New Replication Job** wizard.

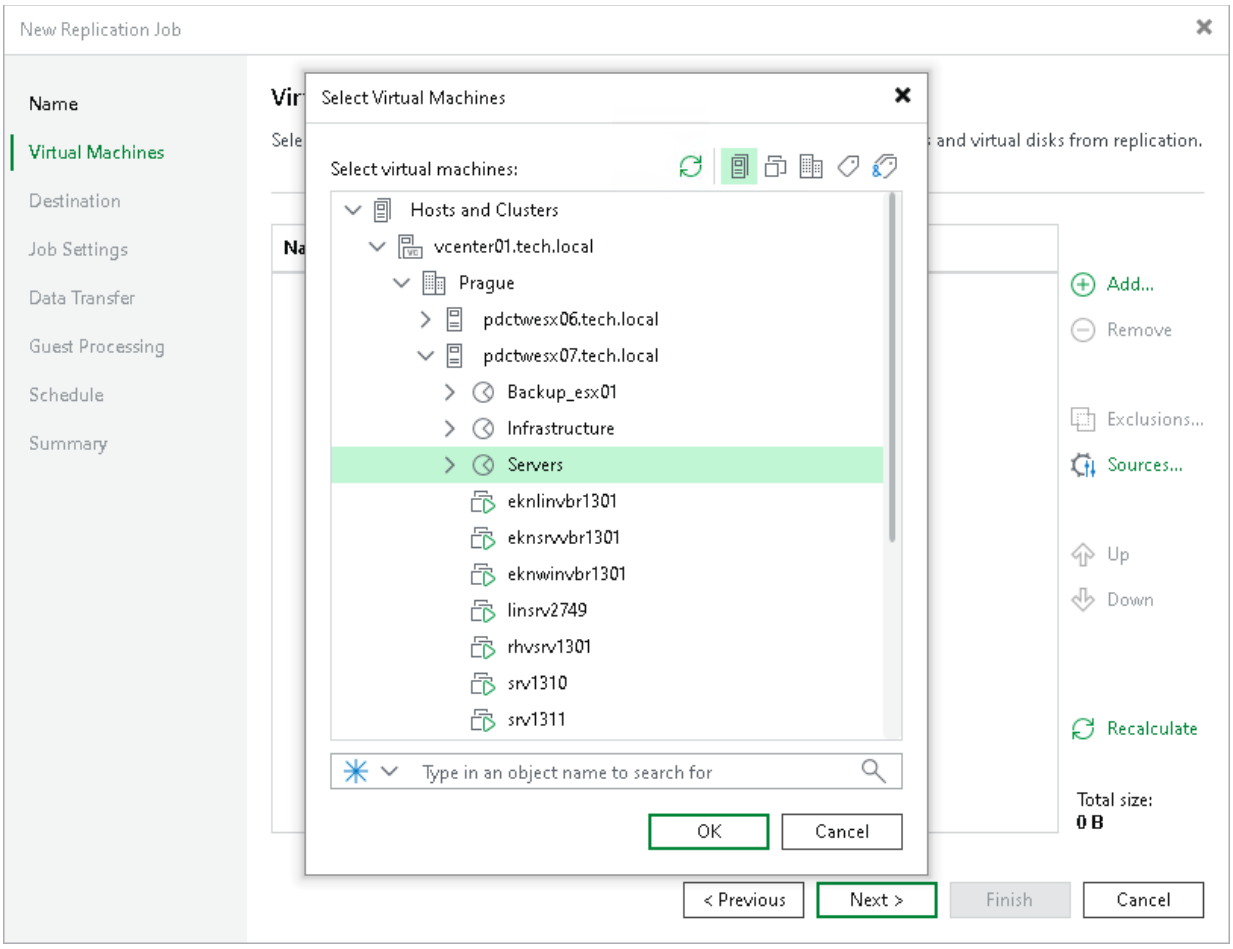


3. At the **Name** step of the wizard, specify a name and description for the replication job. For other settings, leave the default values.



4. At the **Virtual Machines** step of the wizard, click **Add**. From the list, select VMs that you want to replicate.

   You can also replicate VM containers. If you add a new VM to the container after the replication job is created, Veeam Backup & Replication automatically updates the job to include the new VM.



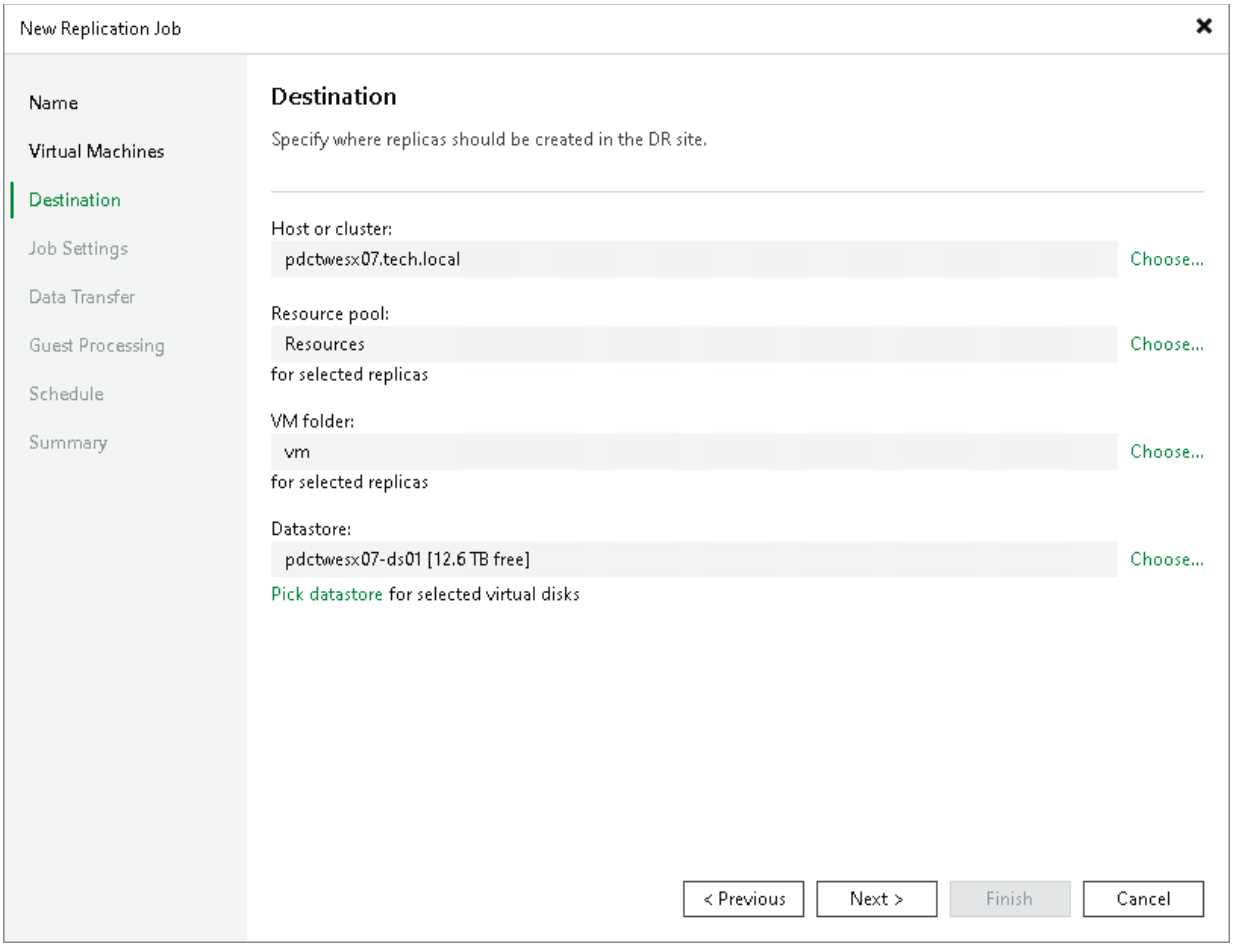
5. [For VMware vSphere] At the **Destination** step of the wizard, do the following:

   a. Click **Choose** next to the **Host or cluster** field and select a host on which the VM replica must be registered.

   b. Click **Choose** next to the **Resource pool** field and select the target resource pool.

   c. Click **Choose** next to the **VM folder** field and select the folder in which the replica must be placed.

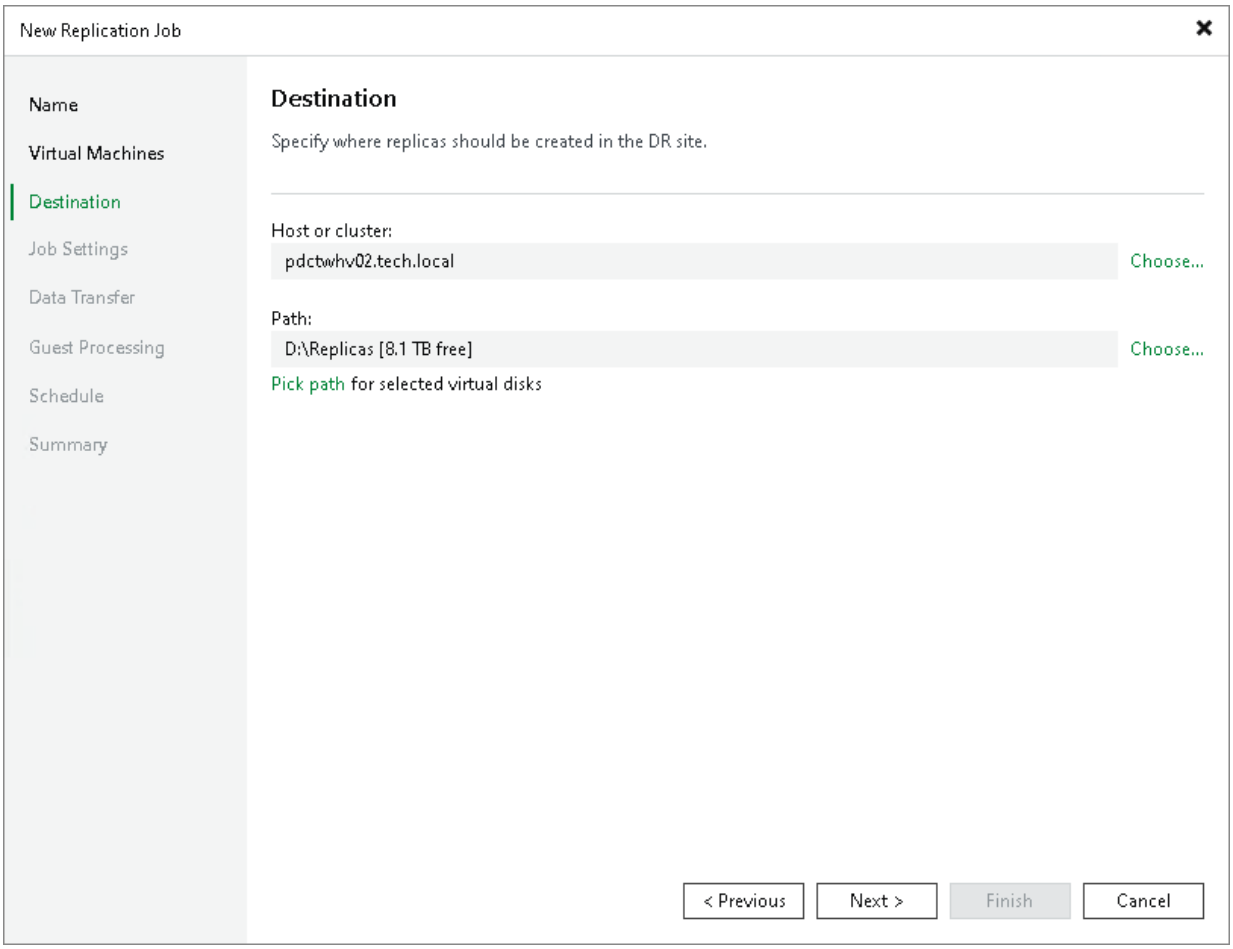
d. Click **Choose** next to the **Datastore** field and select a datastore where VM replica files must be stored.



6. [For Microsoft Hyper-V] At the **Destination** step of the wizard, do the following:

   a. Click **Choose** next to the **Host or cluster** field and select a host on which the VM replica must be registered.

b. Click **Choose** next to the **Path** field and specify a path to a location where VM replica files should be stored.



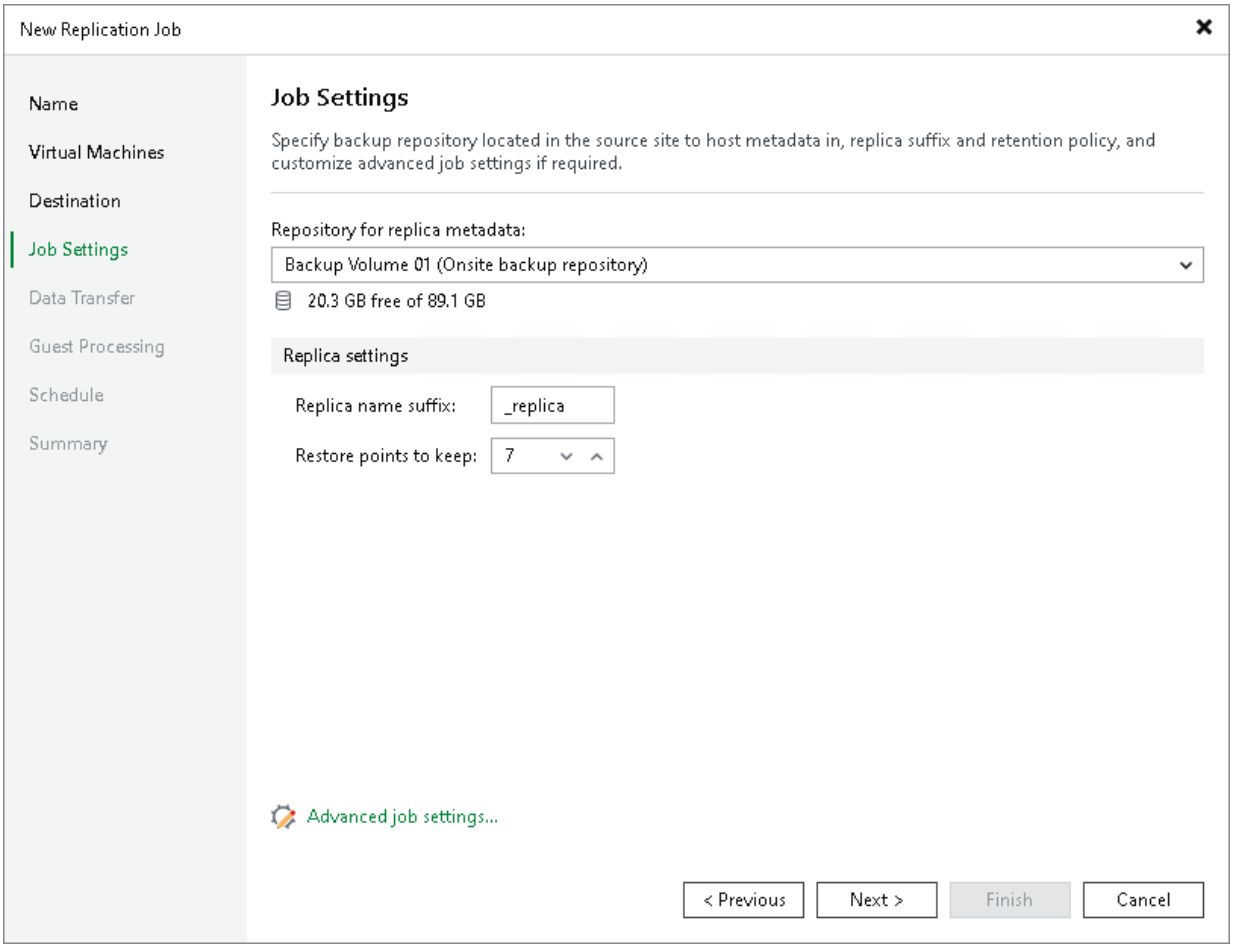
7. At the **Job Settings** step of the wizard, do the following:

   a. In the **Repository for replica metadata** list, select the backup repository where you want to store the metadata file.

   b. In the **Replica name suffix** field, specify the suffix that will be appended to the name of the original VM.

c. In the **Restore points to keep** field, define the number of restore points to keep.

When this number is exceeded, the earliest restore point is removed.



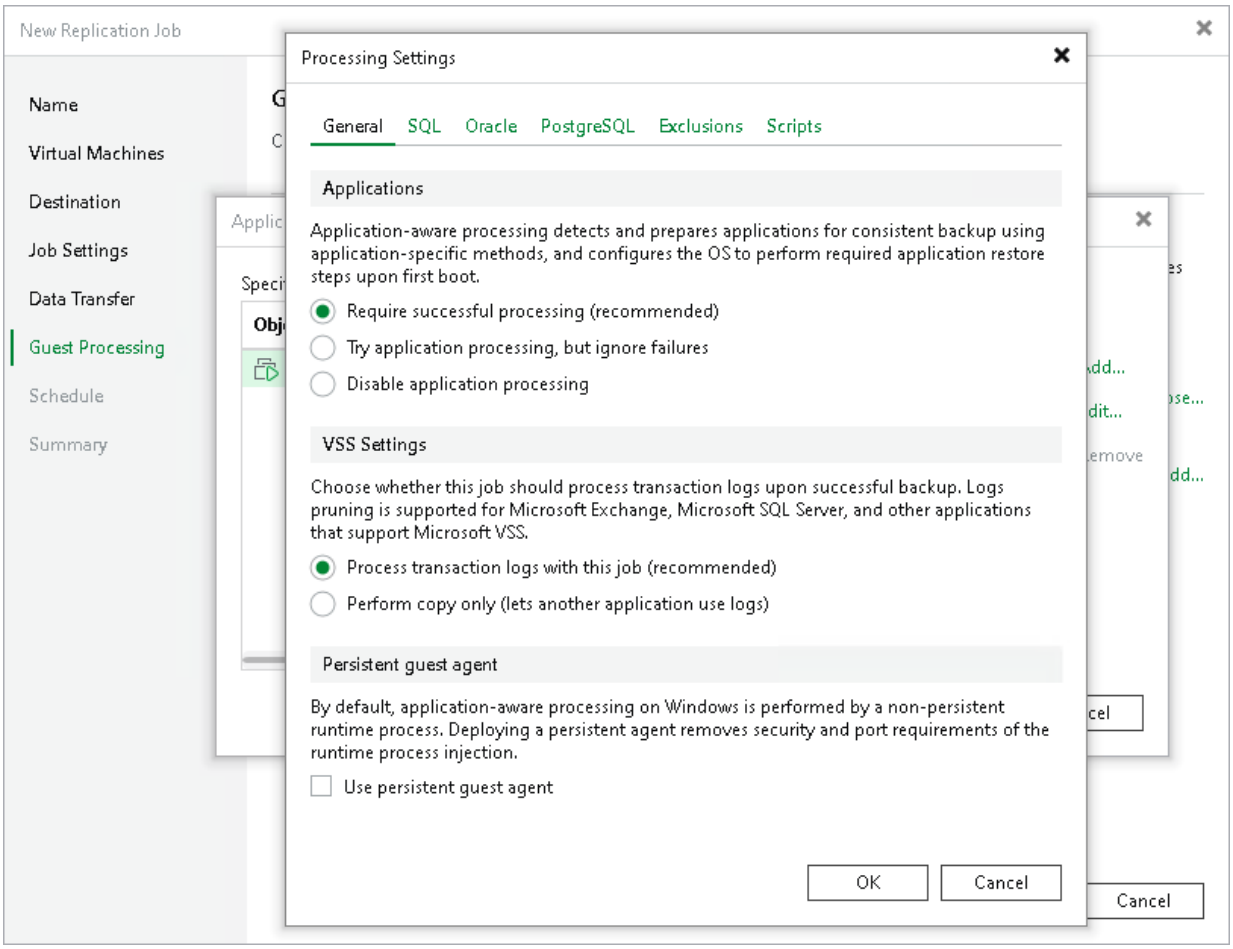
8. At the **Data Transfer** step of the wizard, leave the default settings.

9. At the **Guest Processing** step of the wizard, leave the default settings if you do not need transactionally consistent replicas. Otherwise, select the **Enable application-aware processing** check box and specify credentials of a user account to connect to the VM guest OS. The user account must have Administrator permissions.

   To specify advanced options for VSS processing, click **Applications**. Select a VM in the list and click **Edit**. In the opened window on the **General** tab, do the following:

   a. In the **Applications** section, select **Try application processing, but ignore failures** to continue the replication job even if VSS errors occur. If VSS processing fails, the created replica will not be transactionally consistent but crash consistent.

b. In the **Transaction logs** section, check that the **Process transaction logs with this job** option is selected.



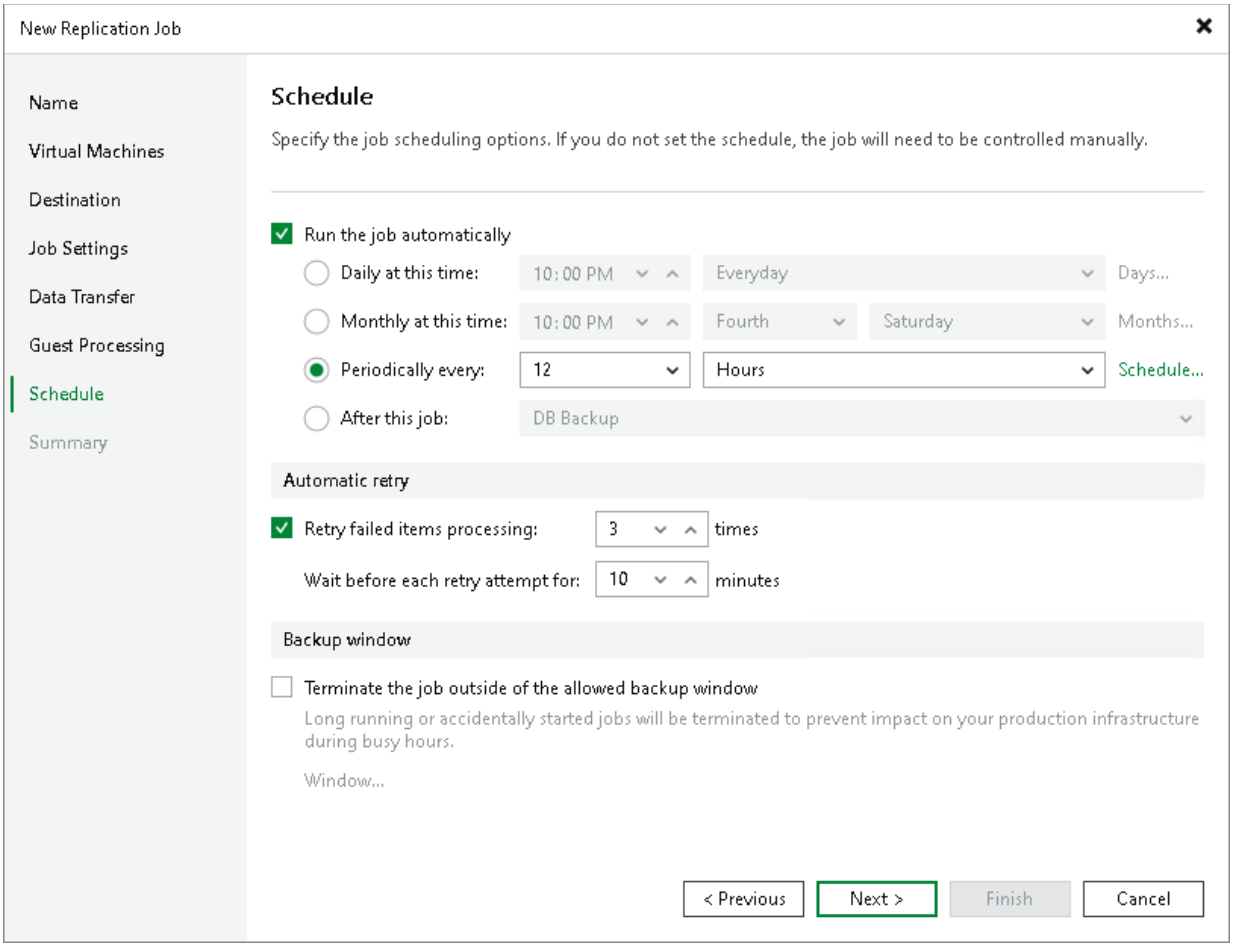
10. At the **Schedule** step of the wizard, do the following:

    a. Select the **Run the job automatically** check box. If you do not select this check box, you will have to launch the job manually. For details, see Start Replication Job Manually.

    b. Select the schedule type: daily, monthly or periodically.

    In the **Periodically every** field, you can select **Continiously** to run the job in a non-stop manner. A new session of the job will start as soon as the previous job session completes.

c. Make sure the **Retry failed VM processing** check box is selected.



11. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.
12. In the inventory pane of the **Home** view, expand the **Last 24 Hours** node to see the created job.
13. Open **vSphere Client** or **Hyper-V Manager** and make sure that the replica appeared on the target host.

Reference

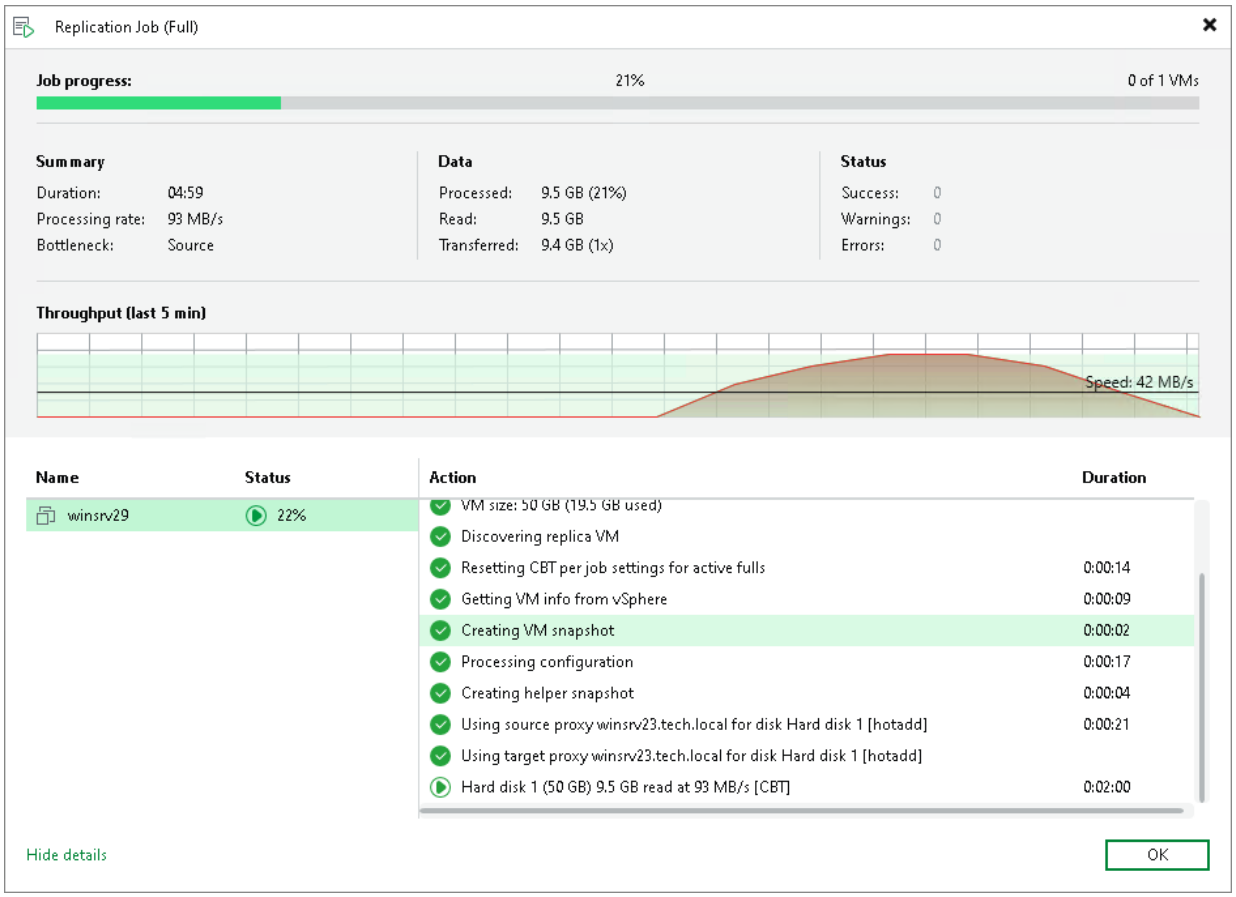
For more information on replica creation, see the Creating Replication Jobs (VMware vSphere) and Creating Replication Jobs (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Monitoring Job Performance in Real Time

When the job is running, you can view job statistics in real time. Statistics include job progress, duration, processing rate, performance bottlenecks, the amount of read and transferred data, and other details of the job performance.

To view the job statistics, do the following:

1. In the inventory pane of the **Home** view, select the **Jobs** > **Replication** node.
2. In the working area, right-click a job and click **Statistics**.
3. In the opened window, select a VM to view its statistics.



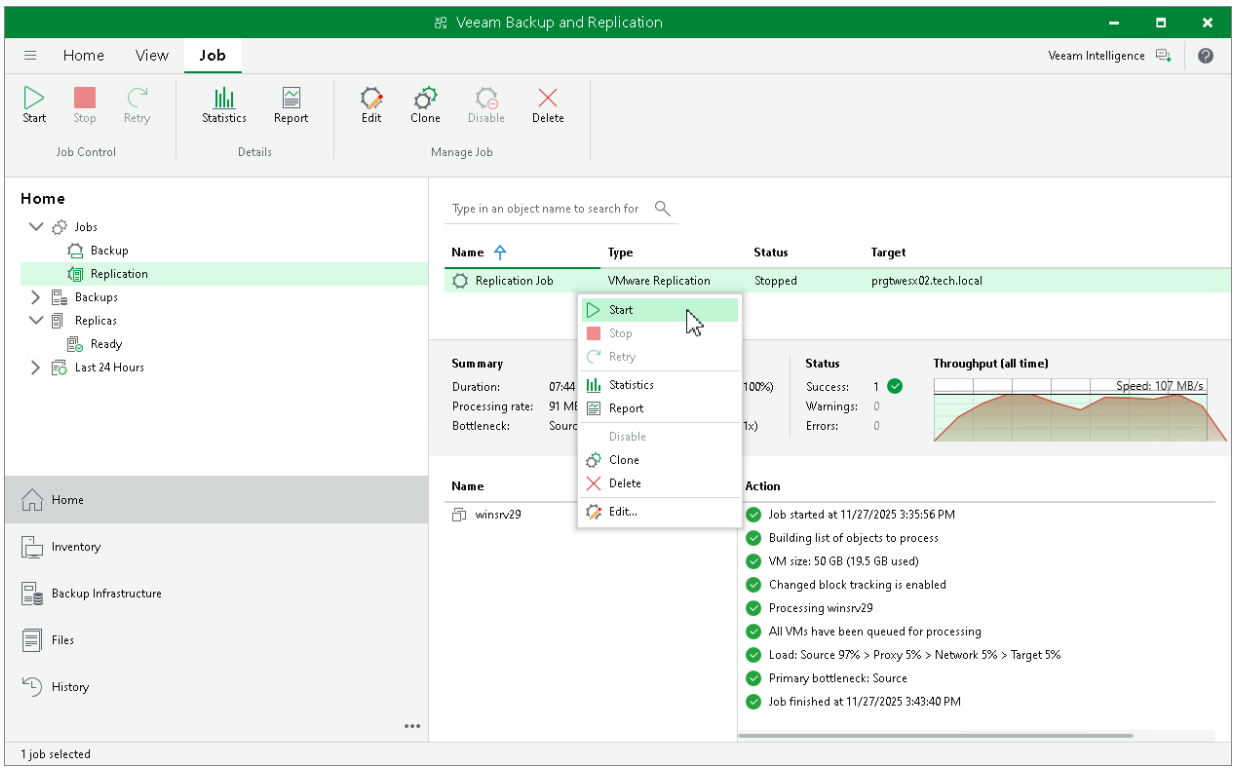
Note that the job must complete with the *Success* or *Warning* status. If the job completes with the *Failed* status, Veeam Backup & Replication does not create a replica and is not able to perform failover and failback operations.

You can configure email notifications to get job results. For details, see Configuring Global Email Notification Settings in the Veeam Backup & Replication User Guide.

Start Replication Job Manually

If you do not schedule a replication job, you must start it manually. To start the job, do the following:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs** > **Replication**.
3. In the working area, right-click the job and select **Start**. Wait for the job to complete. Note that the job must complete with the *Success* or *Warning* status.
4. Open **vSphere Client** or **Hyper-V Manager** and make sure that a VM replica is created.



Replica Failover and Failback

If the original VM in the production site becomes unavailable, you can quickly restore services by failing over to its replica. When you perform failover, the VM replica takes the role of the original VM. All processes shift from the original VM on the production host to the VM replica on the secondary host. You can fail over to the latest state of a replica or to any of its restore points.

When you fail over to the VM replica, Veeam Backup & Replication changes the replica state from *Normal* to *Failover*.

Failover is an intermediate step that needs to be finalized. Depending on a disaster recovery scenario, you can do one of the following:

- **Undo failover**

  When you undo failover, you switch back to the original VM and discard all changes made to the VM replica while it was running. The state of the VM replica gets back to *Normal*. You can use the undo failover scenario if you have failed over to the VM replica for testing and troubleshooting purposes and you do not need the changes made to the VM replica.

- **Perform failback**

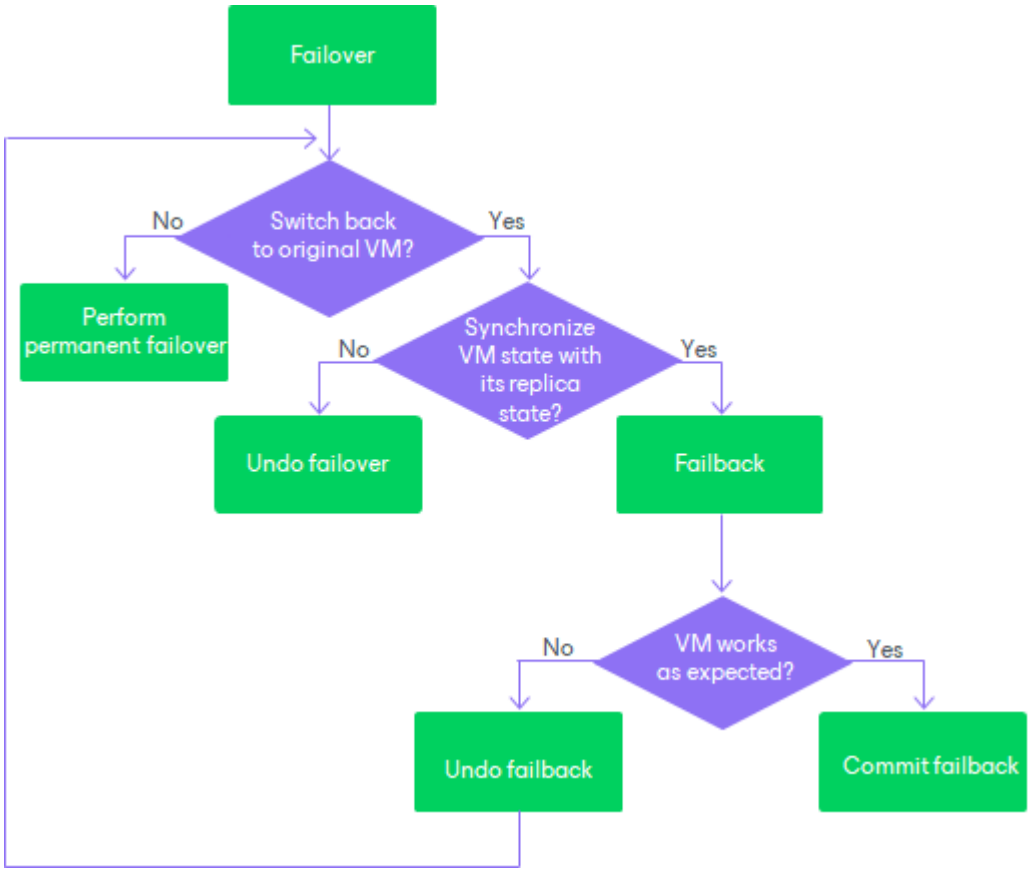
  When you perform failback, you switch back to the original VM and transfer all changes that took place while the VM replica was running to the original VM. If the source host is not available, you can restore the original VM to a new location and switch back to it.

  When you perform failback, changes are only transferred but not published. You must test whether the original VM works with these changes. Depending on the test results, you can do the following:

  - **Commit failback**. When you commit failback, you confirm that the original VM works as expected and you want to get back to it. The state of the VM replica gets back to *Normal*.
  - **Undo failback**. If the original VM is not working as expected, you can undo failback and get back to the VM replica. In this case, the state of the VM replica returns to *Failover*.

- **Perform permanent failover**

  When you perform failover, you permanently switch from the original VM to a VM replica and use this replica as the original VM. This scenario is acceptable if the original VM and VM replica are located in the same site and are nearly equal in terms of resources.



Veeam Backup & Replication supports failover and failback operations for several VMs simultaneously. In case one or several hosts fail, you can use batch processing to restore operations with minimum downtime.

Performing Replica Failover

Before You Begin

Before you perform failover, consider the following:

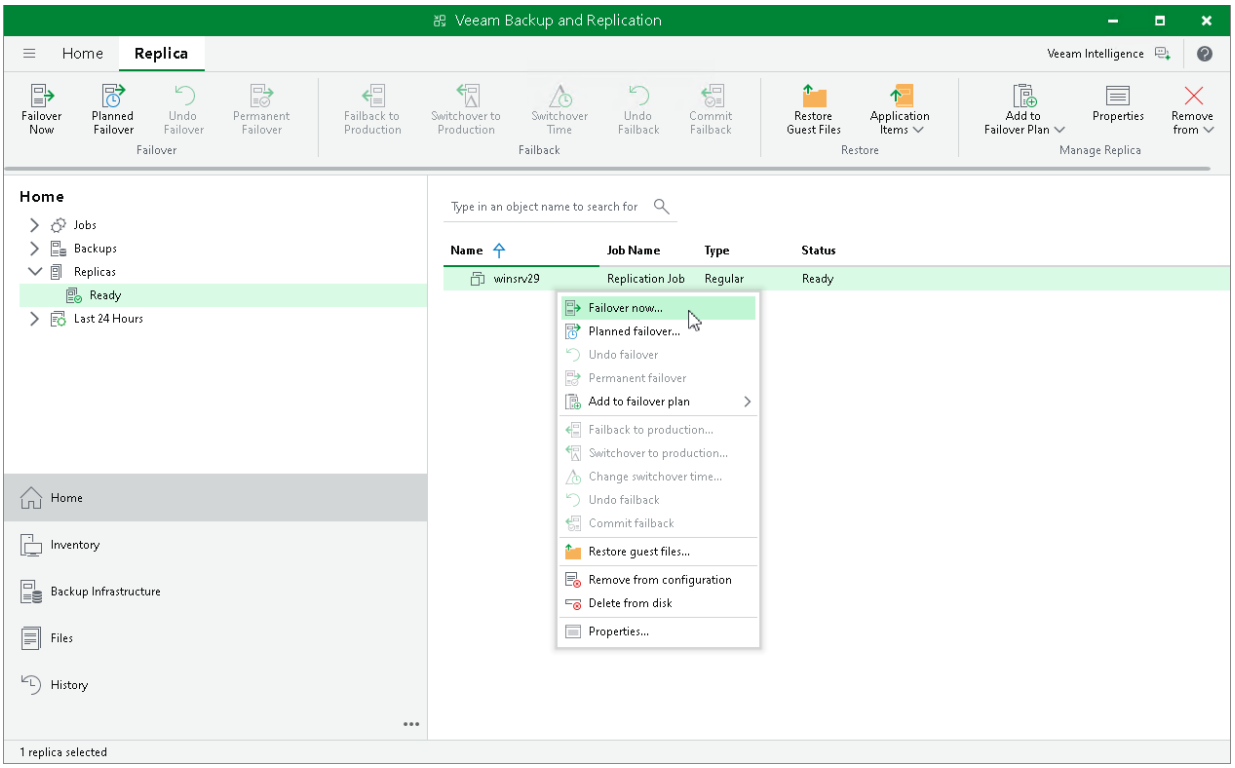
- For original VMs and replica VMs located in the same network. If you plan to perform replica failover while the original VM is running, consider temporarily disconnecting the original VM from the network to avoid IP addresses or machine names conflicts.
- To successfully fail over to a VM replica, make sure that this replica has at least one successfully created restore point.

  To check whether restore points are created, open the inventory pane of the **Home** view and select the **Replicas** node. Then, select the VM and verify that there is at least one restore point available for the VM.

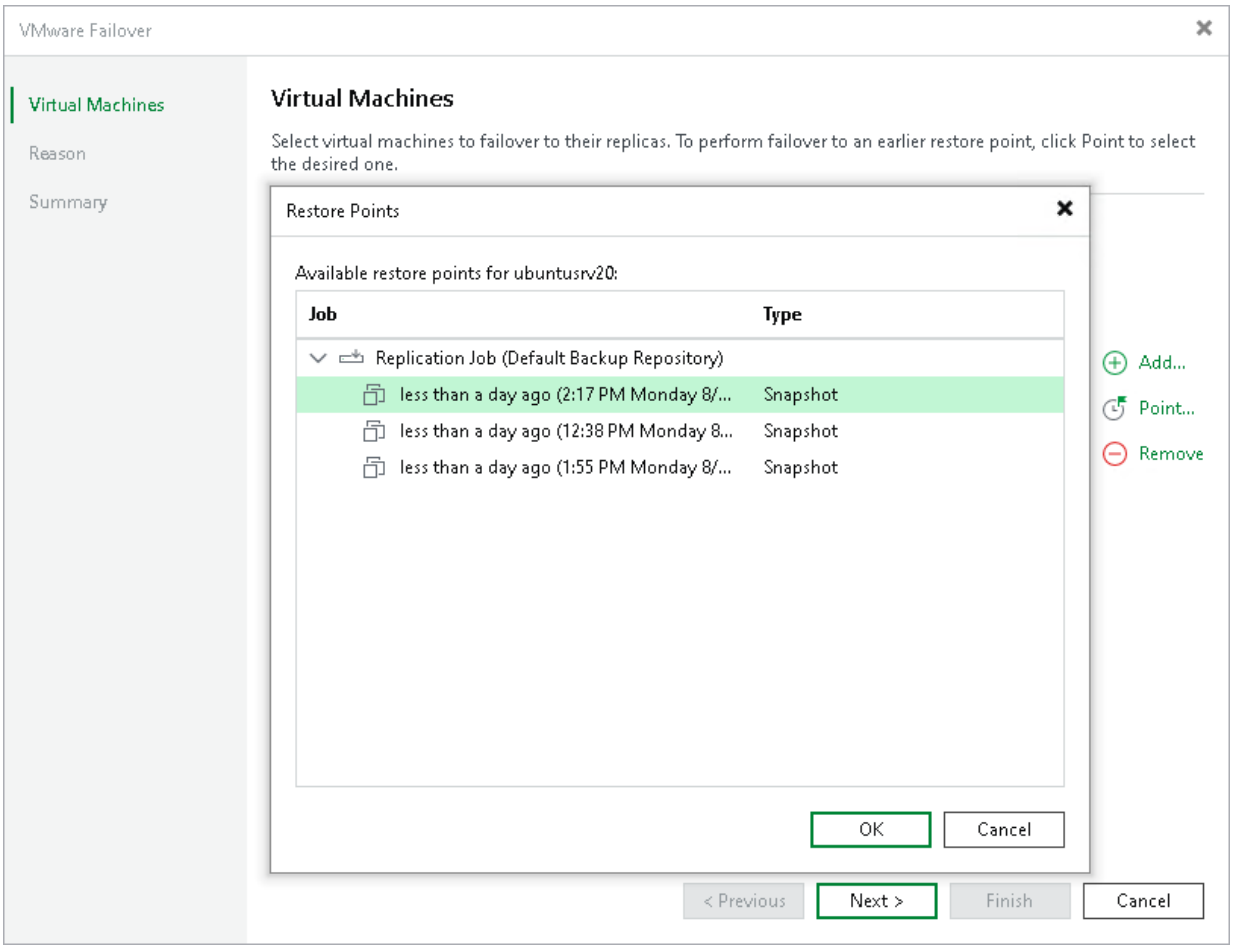
Performing Failover

To fail over to a VM replica, do the following.

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. Right-click the replicated VM and select **Failover Now** to launch the failover wizard.



3. At the **Virtual Machines** step of the wizard, select the VM from the list, click **Point** and choose the restore point to which you want to fail over.



4. At the **Reason** step of the wizard, specify the reason for failover.
5. At the **Summary** step of the wizard, click **Finish** to fail over to the VM replica.

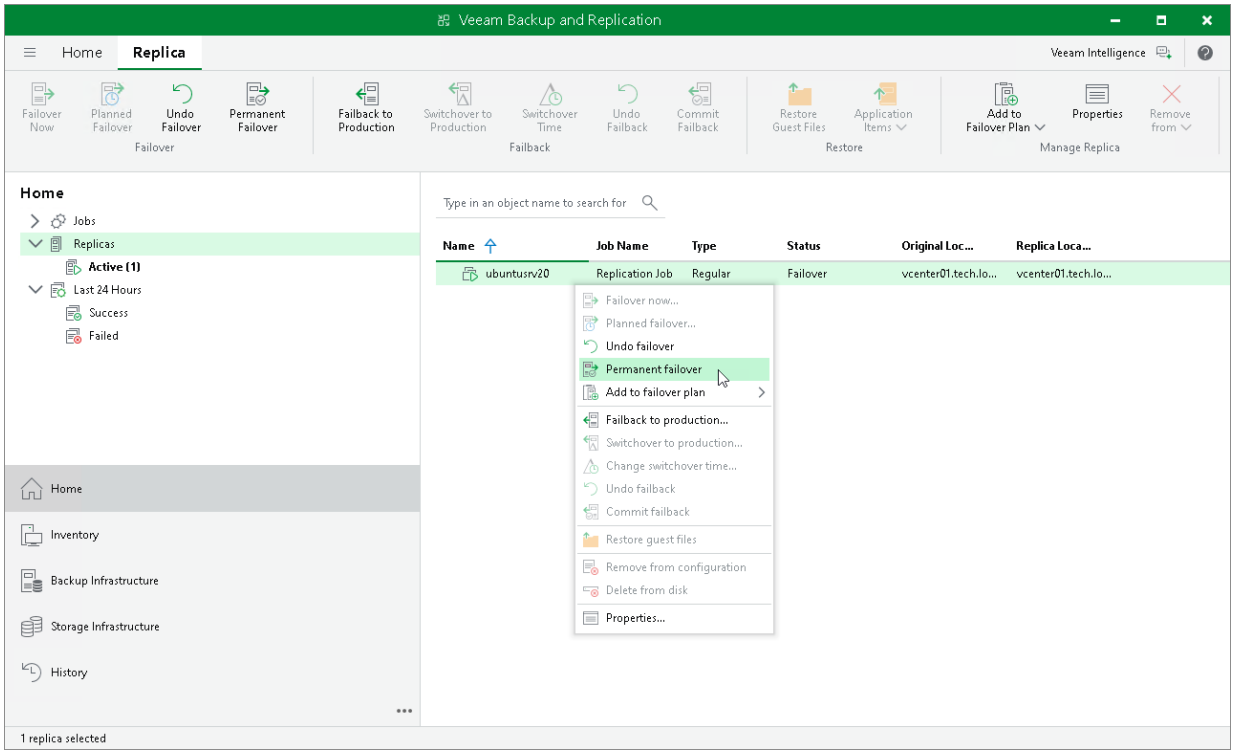
Reference

For more information on failover, see the Replica Failover (VMware vSphere) and Replica Failover (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Performing Permanent Failover

To perform permanent failover, do the following:

1. In the inventory pane of the **Home** view, click the **Replicas** node.
2. In the working area, right-click the VM replica and select **Permanent Failover**.
3. In the opened window, click **Yes** to confirm the operation.



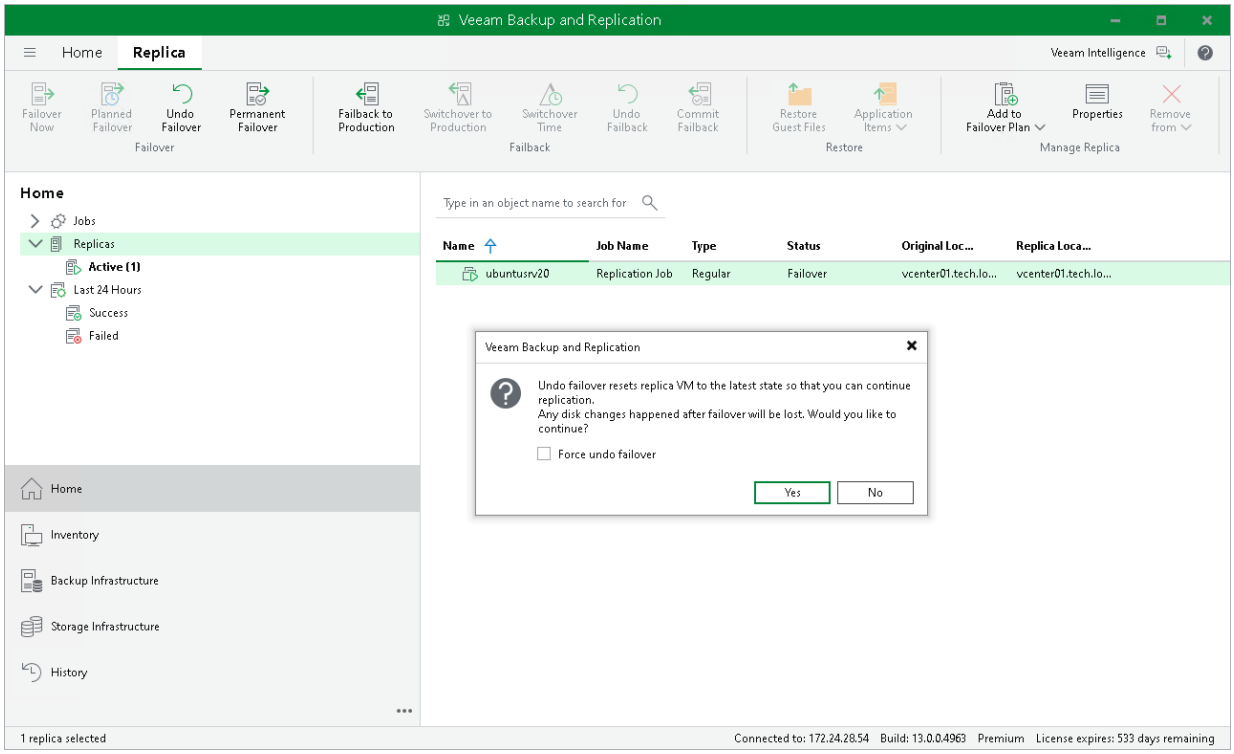
Reference

For more information on permanent failover, see the Permanent Failover (VMware vSphere) and Permanent Failover (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Undoing Failover

To undo failover, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Undo Failover**.
3. In the opened window, click **Yes** to confirm the operation.



Reference

For more information on undoing failover, see the Undo Failover (VMware vSphere) and Undo Failover (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Performing Failback

You can fail back to a VM in the original or new location. In this section, you will learn how to fail back to the original VM on the source host.

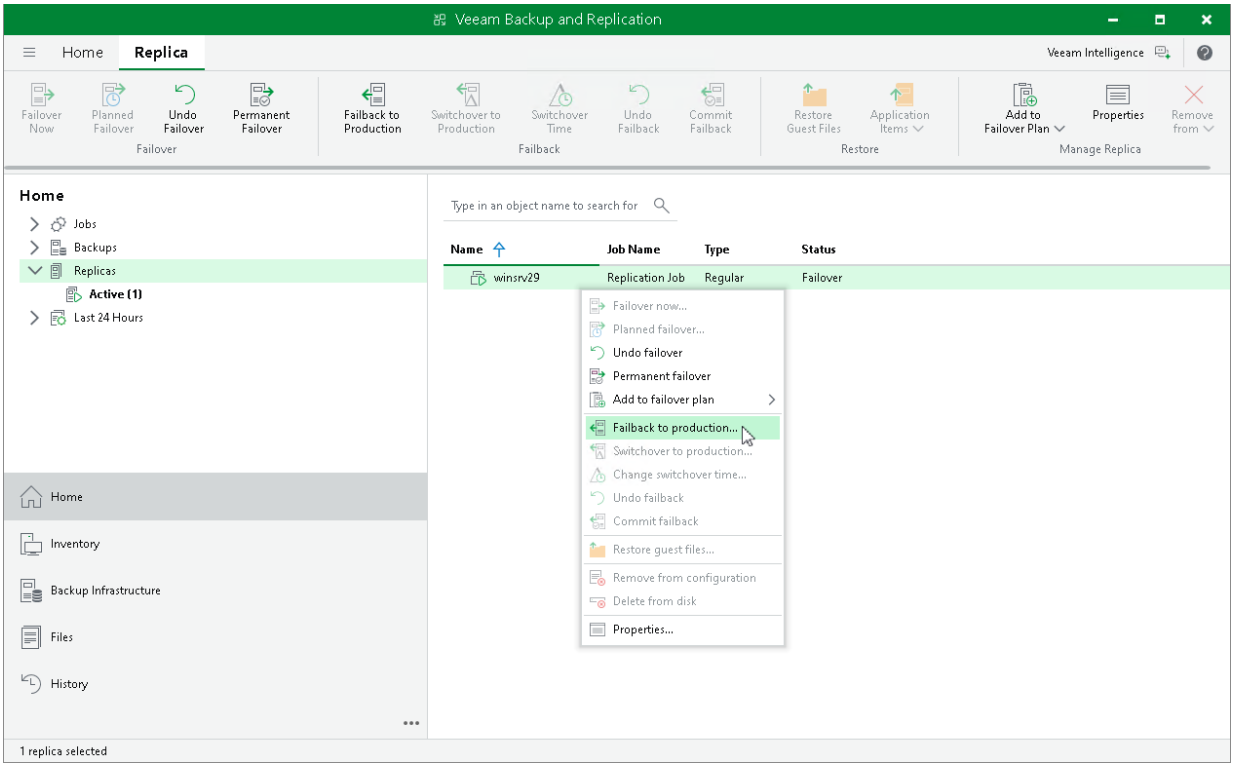
Before You Begin

Make sure that the VM replica for which you want to perform failback is in the *Failover* state. The replica gets into this state after you perform replica failover.

Performing Failback

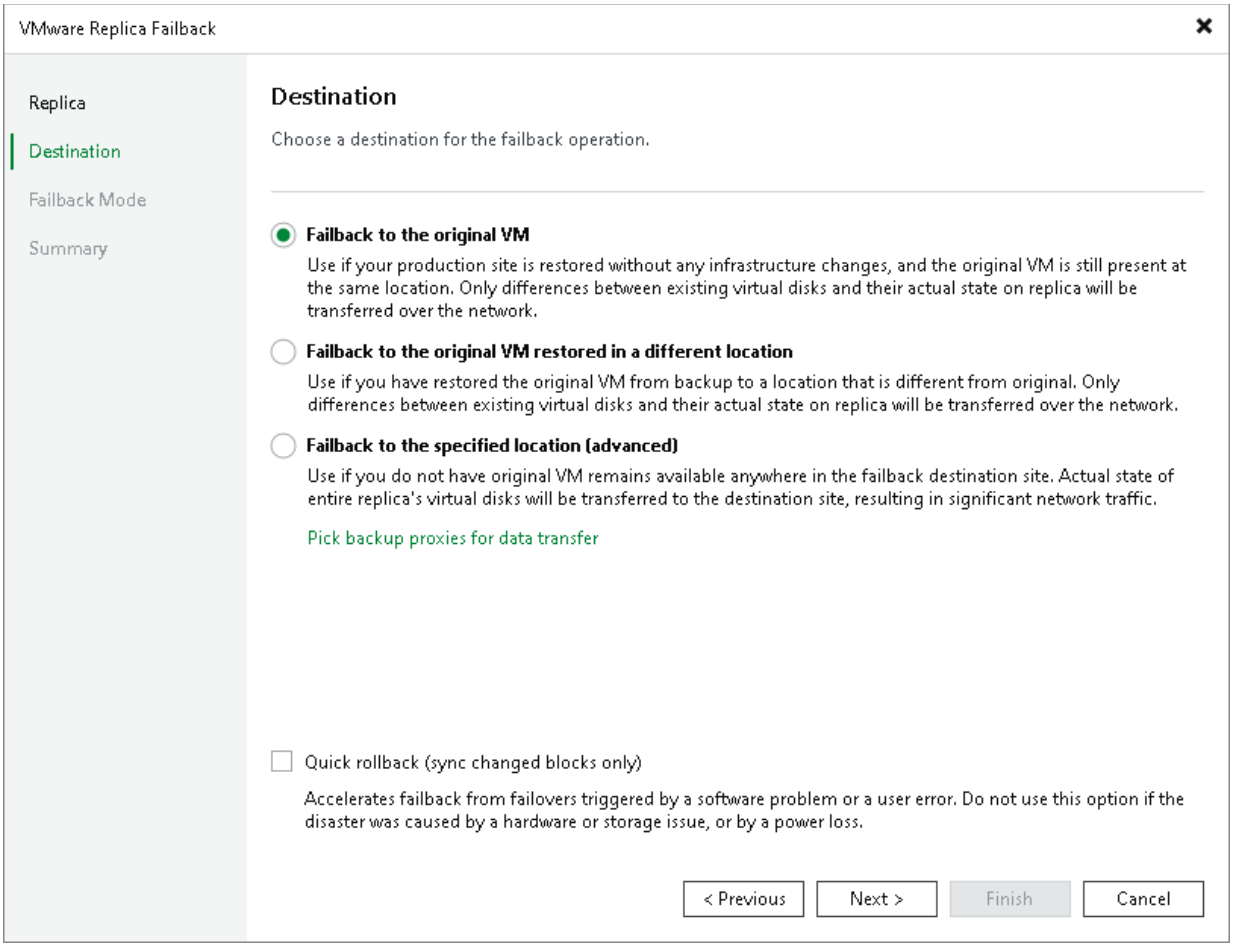
To fail back from VM replica to the original VM on the source host, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Failback to production** to launch the **Failback Wizard**.



3. At the **Replica** step of the wizard, click **Next**.

4. At the **Destination** step of the wizard, select **Failback to the original VM**.



5. [For VMware vSphere] At the **Failback Mode** step of the wizard, select **Auto**. In this case, failback will be performed as soon as VMs are ready.
6. At the **Summary** step of the wizard, select the **Power on VM after restoring** check box and click **Finish**.

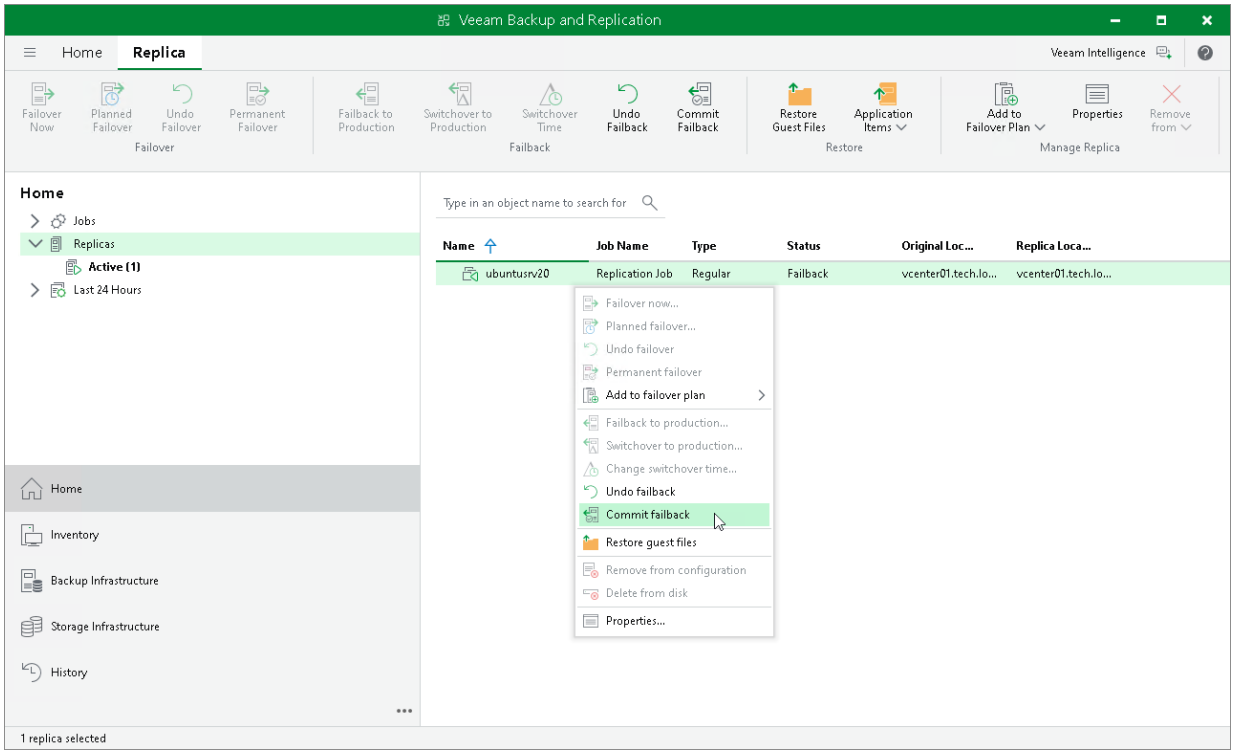
Reference

For more information on failback, see the Replica Failback (VMware vSphere) and Replica Failback (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Committing Failback

To commit a failback, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Commit Failback**.
3. In the opened window, click **Yes** to confirm the operation.



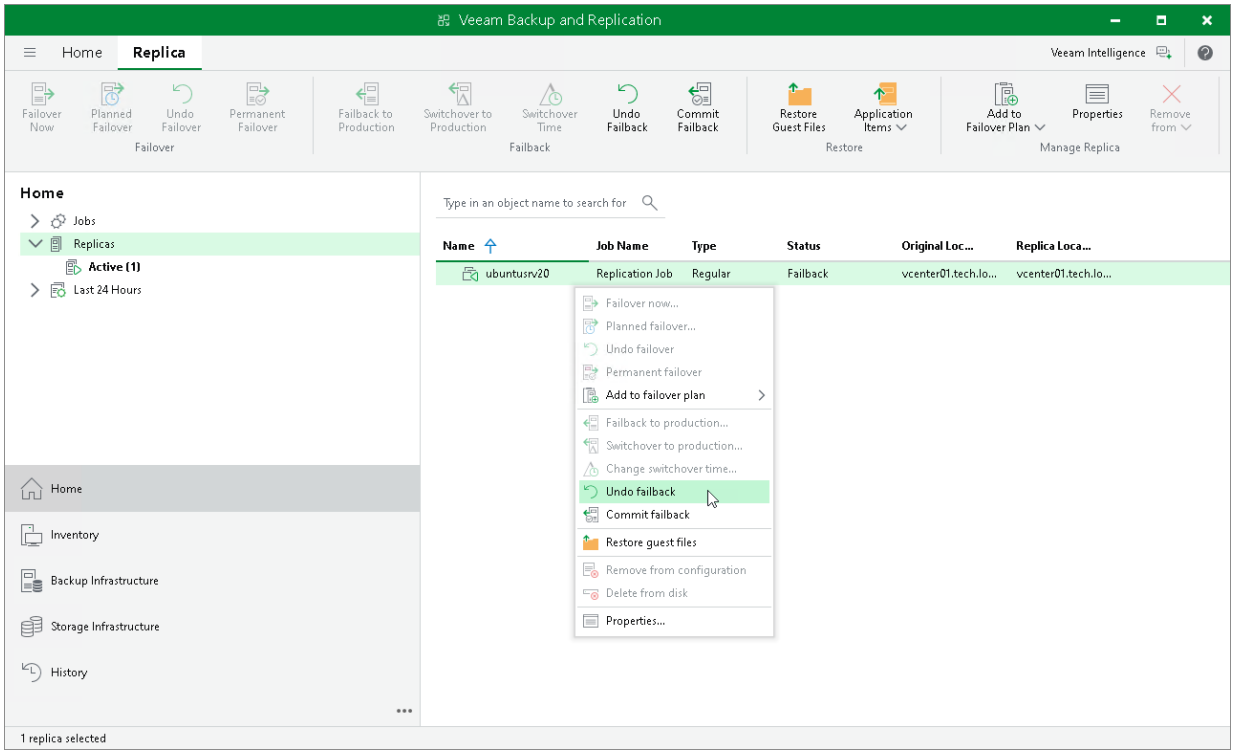
Reference

For more information on committing failback, see the Commit Failback (VMware vSphere) and Commit Failback (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Undoing Failback

To undo a failback, do the following:

1. In the inventory pane of the **Home** view, select the **Replicas** node.
2. In the working area, right-click the VM replica and select **Undo Failback**.
3. In the opened window, click **Yes** to confirm the operation.



Reference

For more information on undoing failback, see the Undo Failback (VMware vSphere) and Undo Failback (Microsoft Hyper-V) sections in the Veeam Backup & Replication User Guide.

Enterprise Manager

If you have a geographically dispersed virtual environment with multiple Veeam Backup & Replication servers, you can use Veeam Backup Enterprise Manager. Veeam Backup Enterprise Manager is a solution that helps manage multiple backup servers from a single web UI.

You can use Veeam Backup Enterprise Manager to perform the following tasks:

- Monitor and manage jobs configured on different backup servers from a single web console
- Edit and clone jobs
- Search for guest OS files in all backups and restore these files in one click
- Delegate guest OS file restore to other users with local Administrator permissions

For the full list of the Veeam Backup Enterprise Manager capabilities, see the About Veeam Backup Enterprise Manager section in the Enterprise Manager User Guide.

> **NOTE:**
>
> Veeam Backup Enterprise Manager is not shipped with the Community edition. For more information, see Editions Comparison.

Installing Veeam Backup Enterprise Manager

You can deploy Veeam Backup Enterprise Manager on a Linux or Microsoft Windows machine. No matter on which OS you deploy Veeam Backup Enterprise Manager, you can manage both Veeam Backup & Replication on Linux and Microsoft Windows.

Before You Begin

Consider the following:

- The machine on which you plan to install Veeam Backup Enterprise Manager must meet the system requirements. For details, see the System Requirements section in the Veeam Backup Enterprise Manager Guide.
- It is recommended to install the same product version on the Veeam Backup Enterprise Manager server and Veeam Backup & Replication backup servers.
- If you plan to install Veeam Backup Enterprise Manager on the same machine where the backup server runs, you must disable all backup and replication jobs and close the Veeam Backup & Replication console.
- Make sure that all necessary ports are opened. For details, see the Ports section in the Veeam Backup Enterprise Manager Guide.
- [Veeam Backup Enterprise Manager on Linux] For the list of considerations and limitations, see the Considerations and Limitations section in the Veeam Backup Enterprise Manager Guide.
- [Veeam Backup Enterprise Manager on Microsoft Windows] For the list of considerations and limitations, see the Before You Begin section in the Veeam Backup Enterprise Manager Guide.

Linux

To install Veeam Backup Enterprise Manager, do the following:

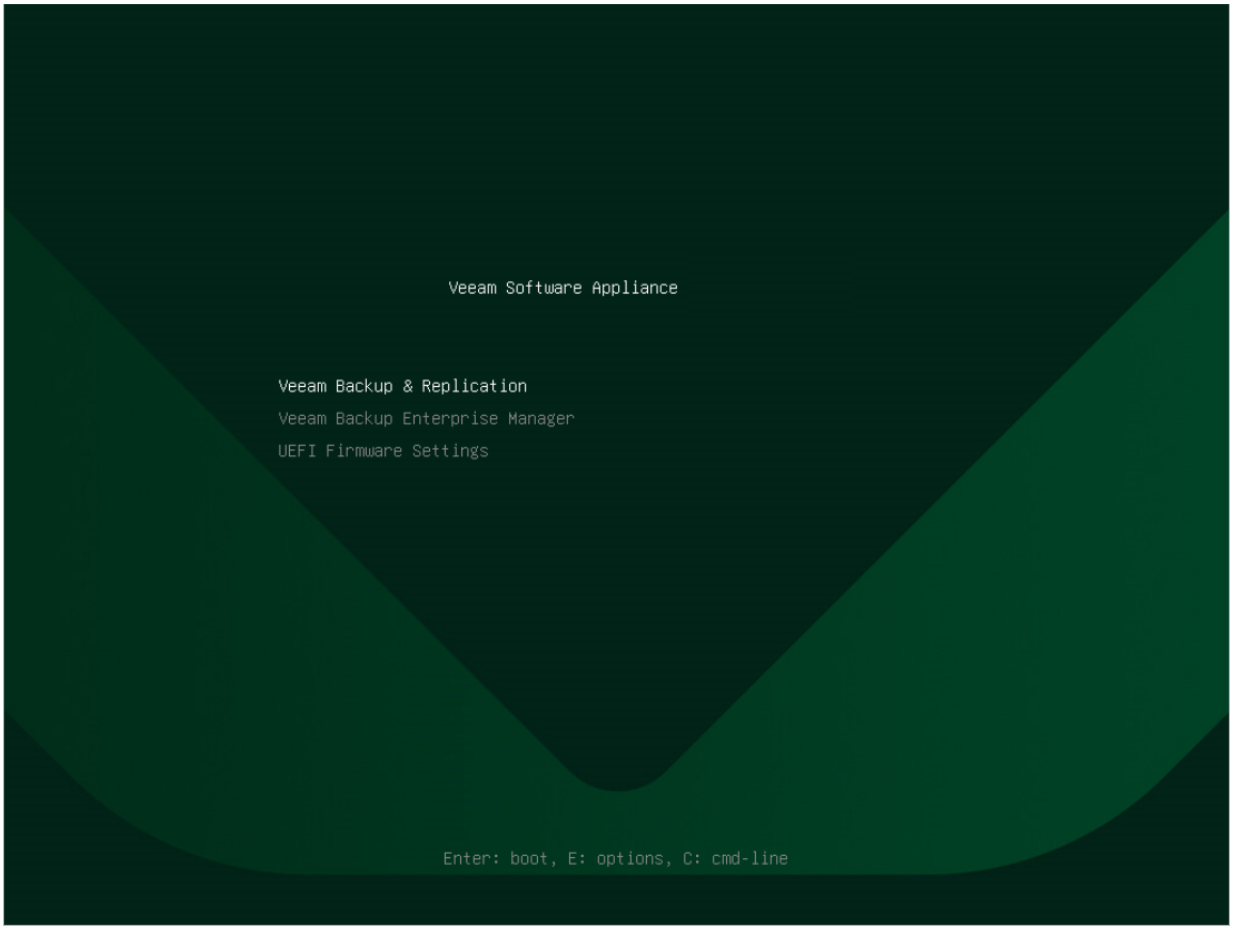
1. Download the latest version of the Veeam Software Appliance installation image from the Product Downloads page. The ISO is located under the **Hardened Software Appliance** tab.

   You must sign in with your Veeam account. If you do not have the account, register with your business email address.

2. Mount the ISO file to the machine where you plan to install Veeam Software Appliance or burn the ISO file to a flash drive or other removable storage device. If you plan to install Veeam Software Appliance on a virtual machine, use the built-in tools of the virtualization management software to mount the ISO file.

   > **NOTE**
   >
   > To create a bootable USB stick, it is recommended that you use Rufus with the default settings. Note that you need to select **Write in DD Image mode** option when prompted.

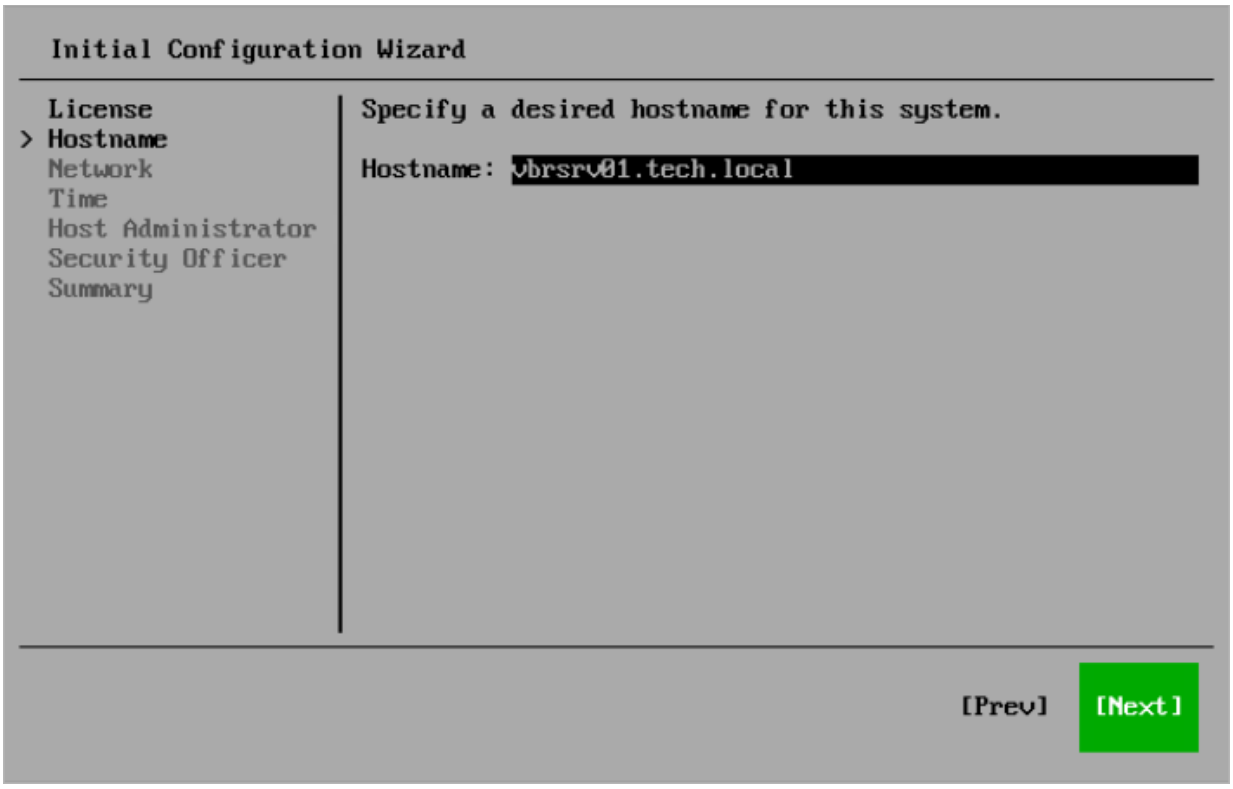
3. In the Boot Manager, select the drive where you mounted the ISO file and press [Enter].
4. In the installation menu, select **Veeam Backup Enterprise Manager** and press [Enter].



5. In the installation menu, select **Install** and press [Enter]. When the installer is loaded, confirm the operation and wait for the system to reboot automatically.
6. At the **License** step of the **Initial Configuration** wizard, read and accept Veeam license agreements and policies.

> **TIP**
>
> To close a document you have read, press [Q].

7. At the **Hostname** step of the **Initial Configuration** wizard, specify the a Fully Qualified Domain Name (FQDN) of the server and select **Next**.



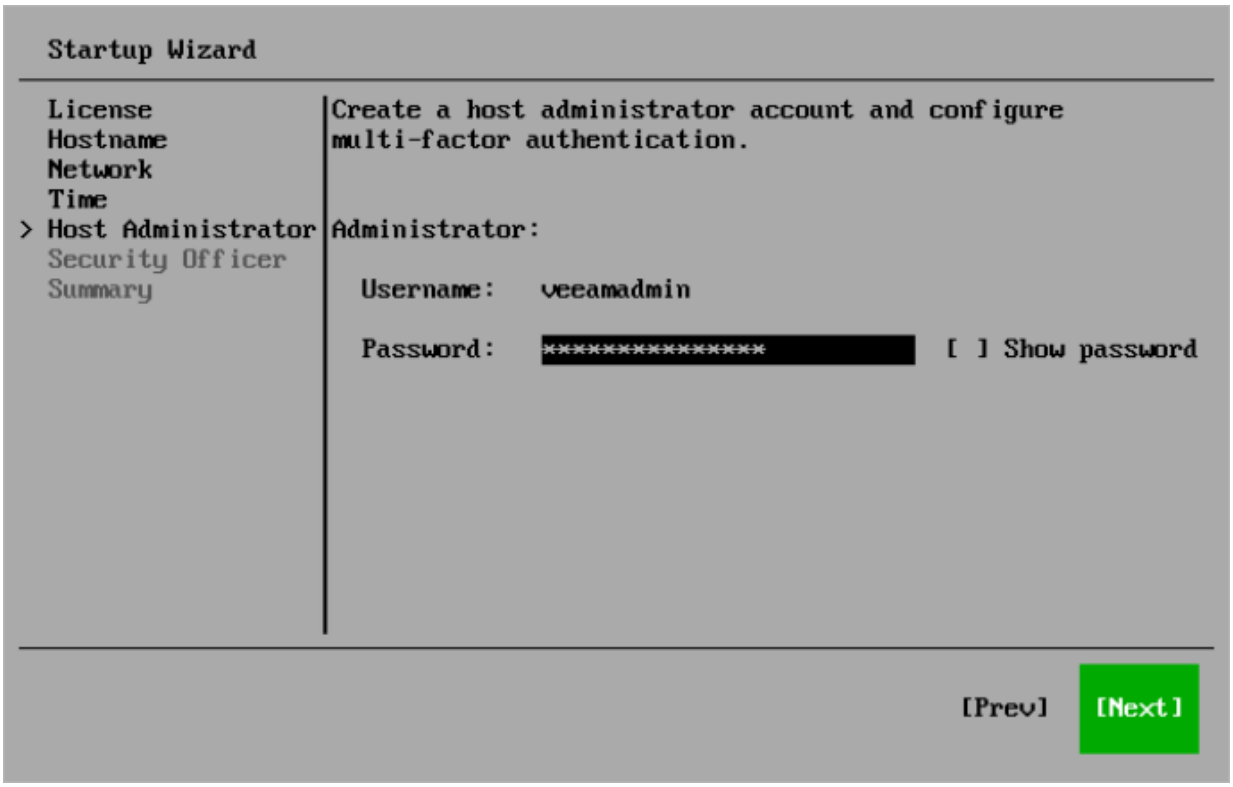
8. At the **Network** step of the **Initial Configuration** wizard, review the network configuration and select **Next**.
9. At the **Time** step of the **Initial Configuration** wizard, review server time configuration.

   By default, the UTC time zone is used. To specify another time zone, select **Change**.
10. At the **Host Administrator** step of the **Initial Configuration** wizard, configure the default host administrator account to perform administrator activities in the Host Management Console — *veeamadmin*. For more information about operations available for this role, see the Managing Users and Roles section in the Veeam Backup & Replication User Guide.

    In the **Password** field, specify the password for the *veeamadmin* user. The password must comply with the following requirements:

    - 15 characters minimum.
    - 1 upper case character.
    - 1 lower case character.
    - 1 numeric character.
    - 1 special character.

- No more than 3 characters of the same class in a row. For example, not more than 3 lowercase or 3 numerical characters in sequence.



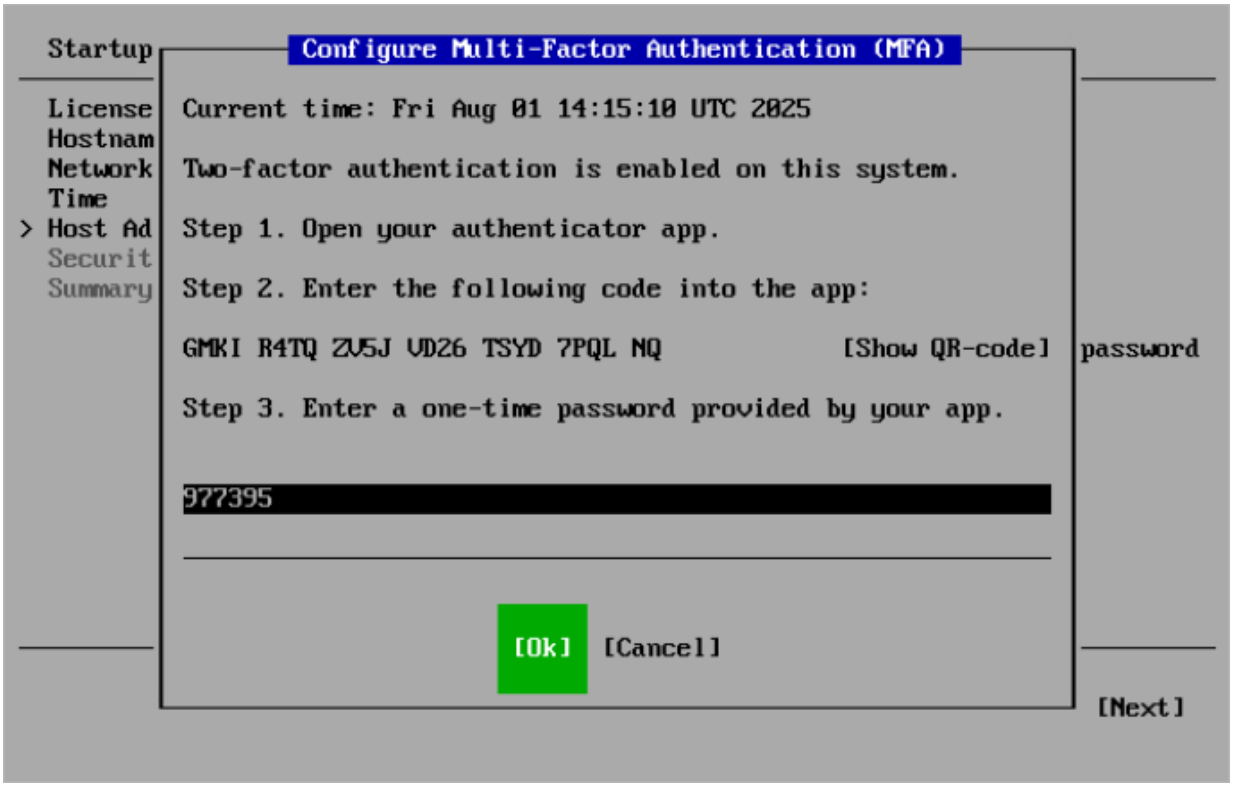
After you specify the password, select **Next** and configure multi-factor authentication (MFA):

a. Open your authentication application. Enter the code or scan the QR code.

b. Specify the one-time code provided by the application.

c. Press [Ok].

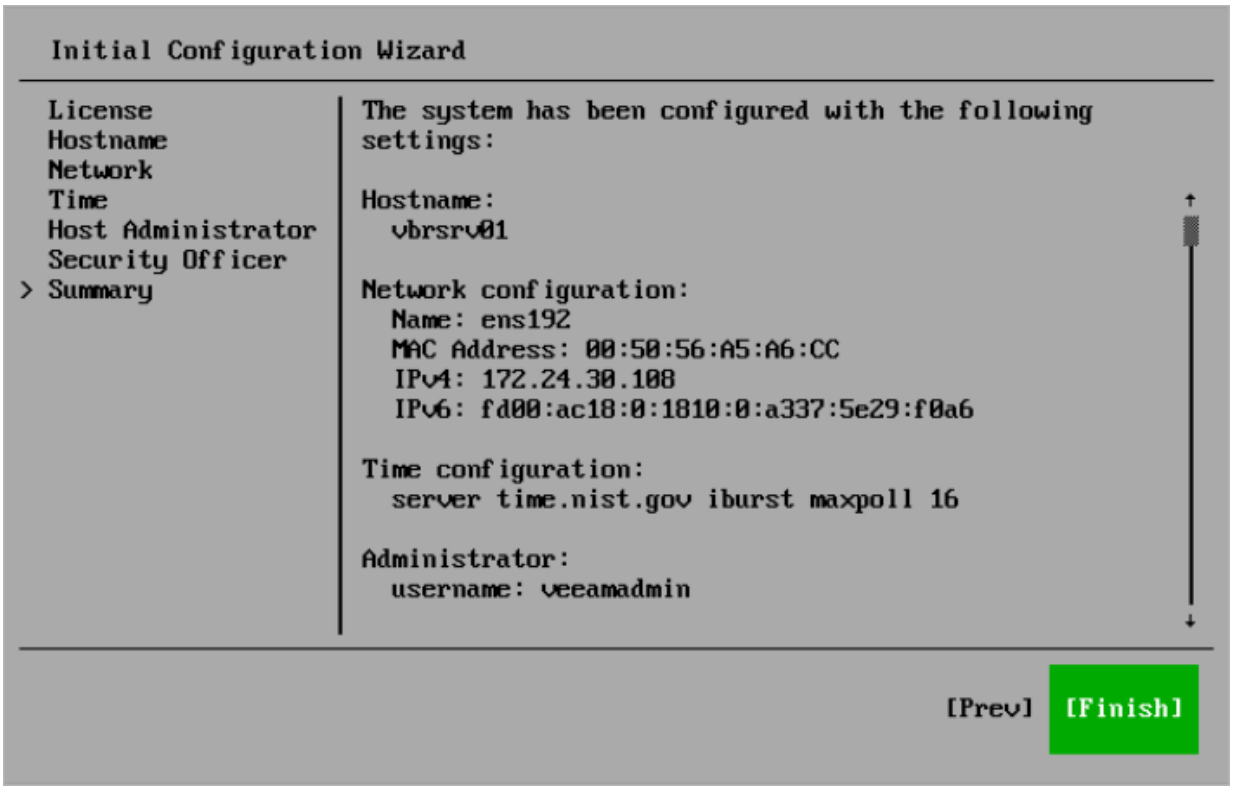
> **NOTE**
>
> Multi-factor authentication is compatible with mobile authentication applications that support RFC4226 and RFC6238.



11. At the **Security Officer** step of the **Initial Configuration** wizard, select **Skip setting up Security Officer** to skip configuring the security officer account.

> **TIP**
>
> The security officer account type provides an additional security layer to protect your infrastructure against malicious system administration. You can skip configuring this account to test the functionality of Veeam Backup & Replication. In the production environments, we recommend configuring this account. For more information about operations available for the security officer, see the Managing Users and Roles section in the Veeam Backup & Replication User Guide.

12. At the **Summary** step of the **Initial Configuration** wizard, review the system configuration and select **Finish**. The system will apply the configuration and restart required services.



After you finish the initial configuration, general information about the server will be displayed. You can use it to log in to the Host Management Console and continue configuring Veeam Software Appliance.

Reference

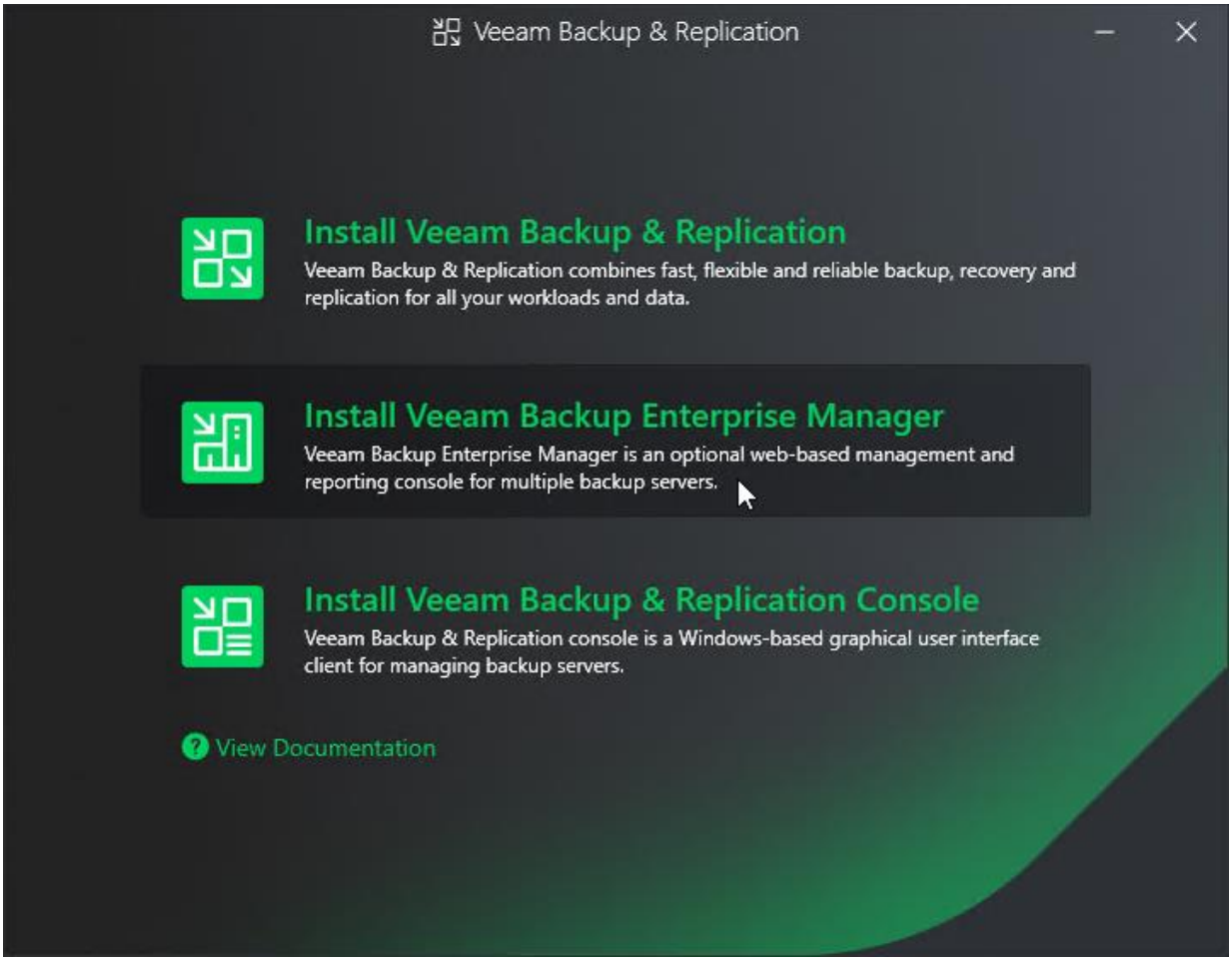
For details on how to configure the backup server deployed from Veeam Software Appliance, see the Host Management section in the Veeam Backup Enterprise Manager User Guide.

Microsoft Windows

Installing Enterprise Manager

To install Veeam Backup Enterprise Manager, perform the following:

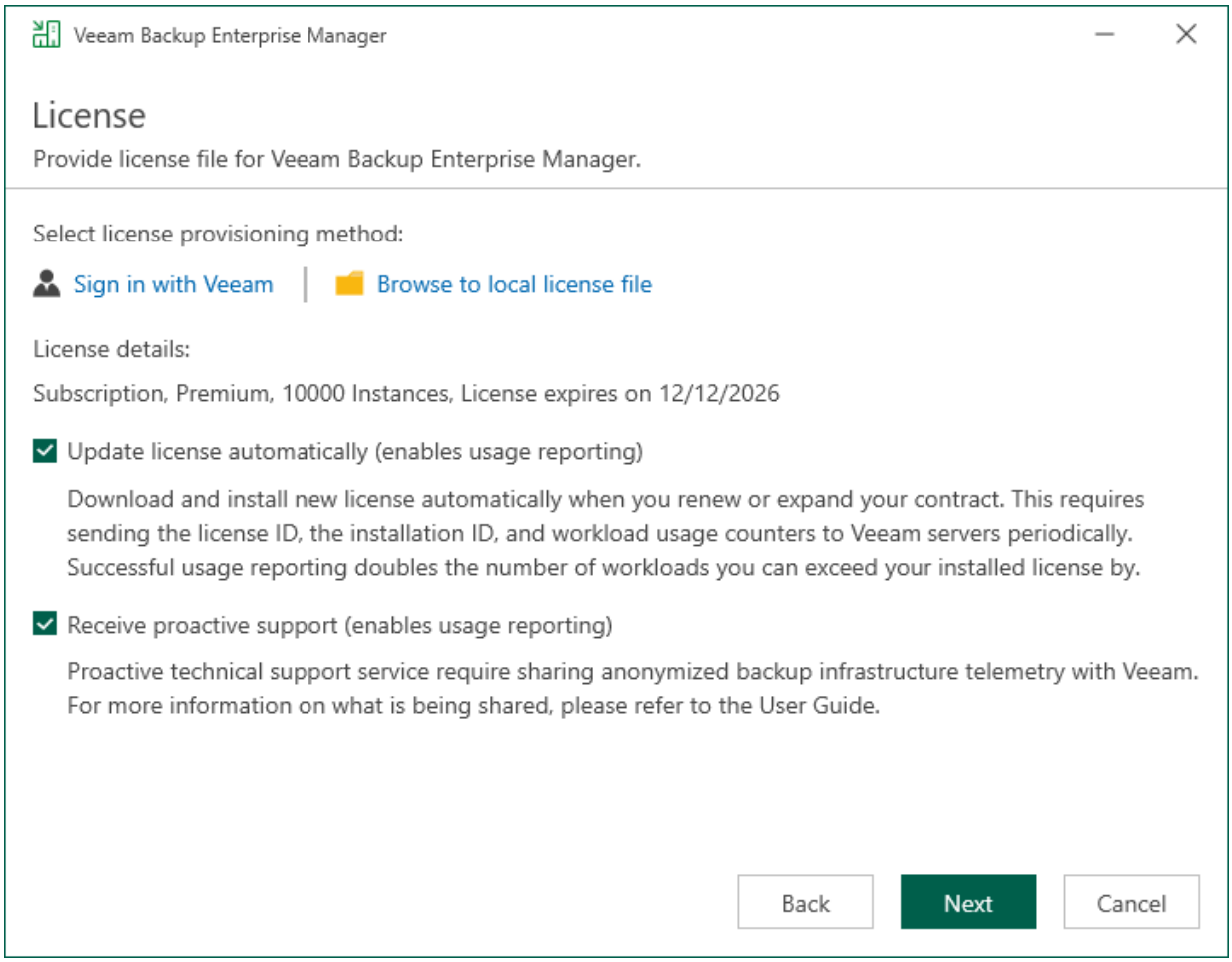
1. Download the latest version of Veeam Backup & Replication installation image from the Download Veeam products page.
2. Mount the installation image to the machine on which you plan to install Veeam Backup Enterprise Manager or burn the image file to a flash drive or other removable storage device.
3. Run the `Setup.exe` file from the image or disk to open the splash screen.
4. In the window, click **Install Veeam Backup Enterprise Manager** to launch the **Veeam Backup Enterprise Manager Setup** wizard.



5. At the **License Agreement** step of the wizard, read the license agreements and select check boxes to accept the terms.

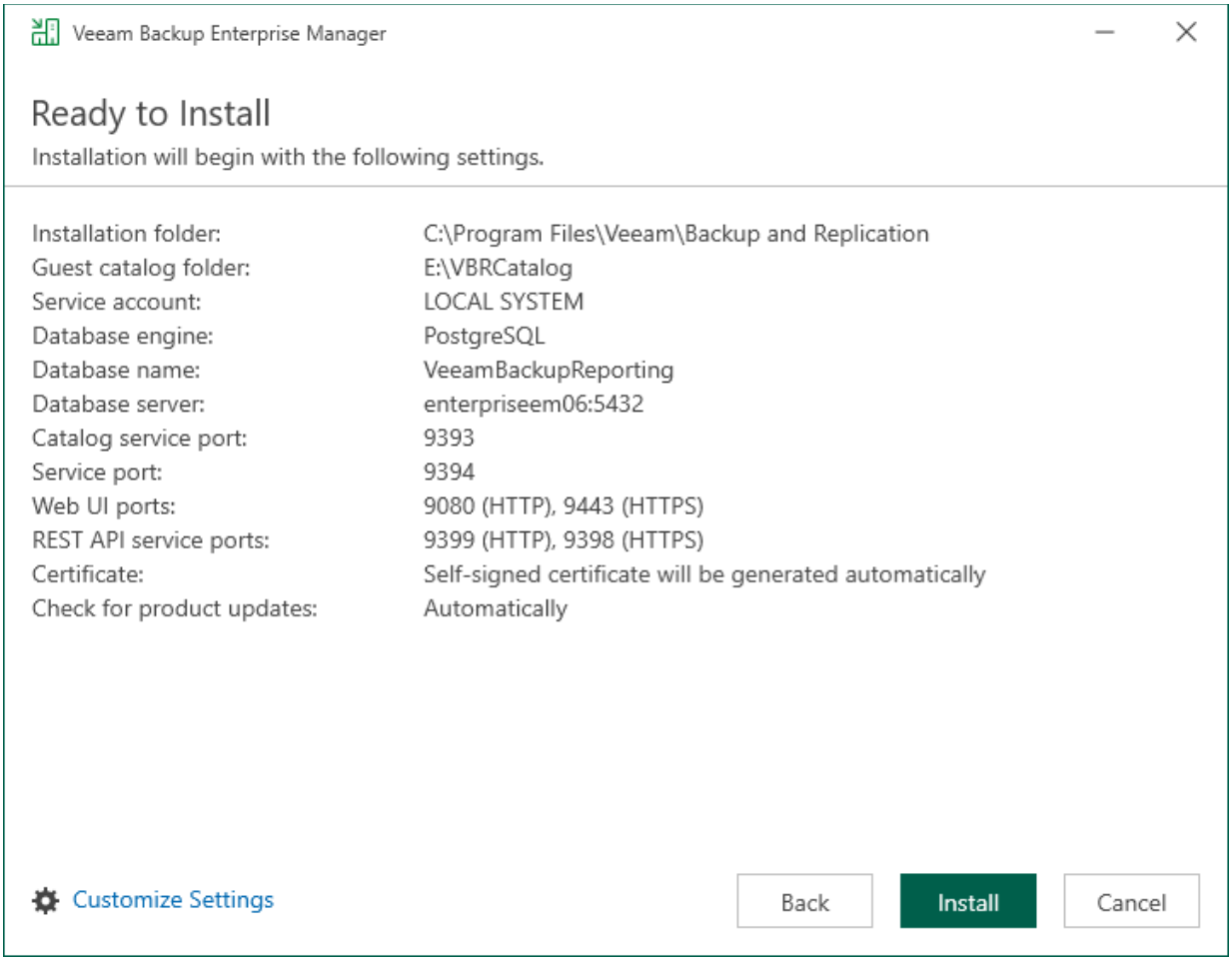
6. At the **Provide License** step of the wizard, specify the path to the license key.

   If you install Veeam Backup Enterprise Manager on the backup server, you can proceed without providing a license file. In this case, Veeam Backup Enterprise Manager will use the license that is already installed on the backup server.



7. At the **System Configuration Check** step of the wizard, install missing software components and enable missing features, if any.

8. At the **Ready to Install** step of the wizard, click **Install** to begin installation.



9. When the installation process completes, click **Finish** to close the wizard.

Adding Backup Servers

Veeam Backup & Replication allows you to manage jobs across multiple backup servers and perform recovery operations within a single application. To manage the data protection tasks from a single web console, you must add a backup server to Veeam Backup Enterprise Manager.

Before You Begin

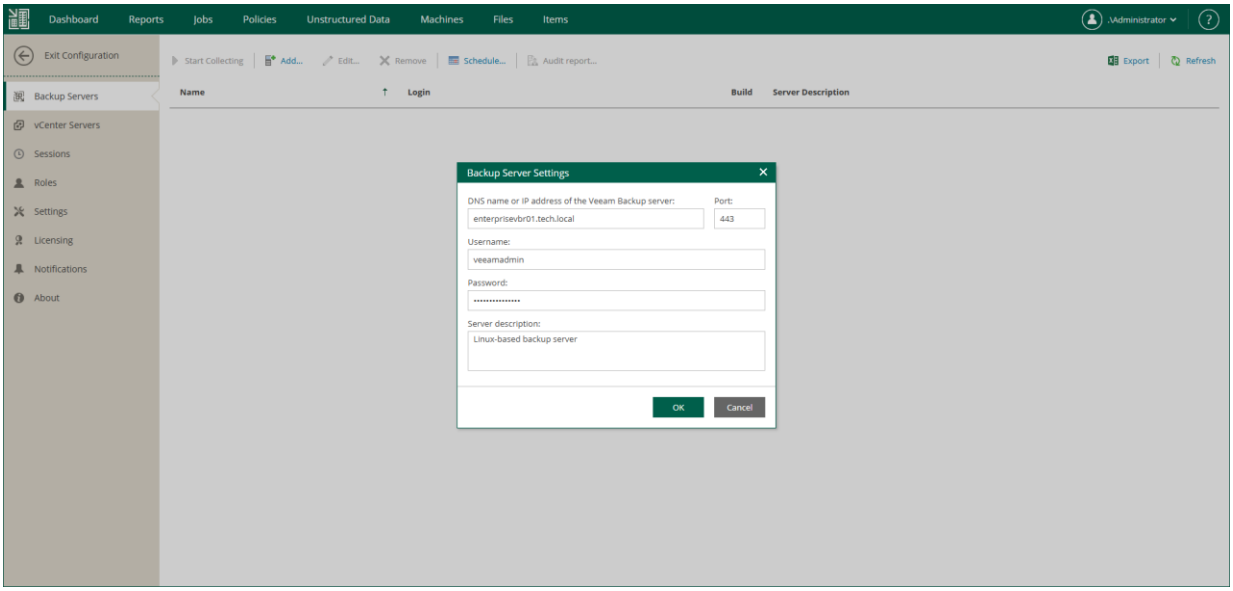
- It is recommended to add backup servers of the same major version. When Veeam Backup Enterprise Manager and Veeam Backup & Replication run different major or minor versions, some Veeam Backup Enterprise Manager features may not be available.
- For the list of considerations and limitations, see the Adding Backup Servers section in the Veeam Backup Enterprise Manager Guide.

Adding Backup Servers

To add a backup server to Veeam Backup Enterprise Manager, do the following:

1. From the Microsoft Windows **Start** menu, select **Programs** > **Veeam** > **Veeam Backup Enterprise Manager** to launch Veeam Backup Enterprise Manager.

   To access Veeam Backup Enterprise Manager remotely, use the following address: `https://enterprise_manager_server_address:9443`
2. In the **Username** and **Password** fields, specify credentials of the user with local Administrator rights or the user who installed Veeam Backup Enterprise Manager.
3. Click **Login**.
4. At the top right corner of the opened window, click **Configuration** to open the **Configuration** view.
5. Select the **Backup Servers** tab. In the working area, click **Add** to open the **Backup Server Settings** window.
6. In the opened window, specify the DNS name or IP address of the backup server you want to add. Provide the name and password of the user account with local Administrator rights on the added backup server for the Microsoft Windows-based backups server, or the *veeamadmin* account for the Linux-based backup server.



7. Click **OK**.

   Veeam Backup Enterprise Manager will start collecting data about all backup and replication jobs on the added backup server.

Reference

For more information on adding backup servers, see the Managing Veeam Backup Servers section in the Veeam Backup Enterprise Manager Guide.

Managing Jobs

Veeam Backup Enterprise Manager allows you to manage jobs that were configured on backup servers: start, stop, retry, edit and clone jobs.

In this section, you will learn how to clone and then edit jobs. When you clone a job, you create its exact copy. Configuration details of the created job copy are written to the same Microsoft SQL database where details of the original job are stored. You can work with the created job both in Veeam Backup Enterprise Manager and in the Veeam Backup & Replication console on the backup server.

Before You Begin

Consider the following:

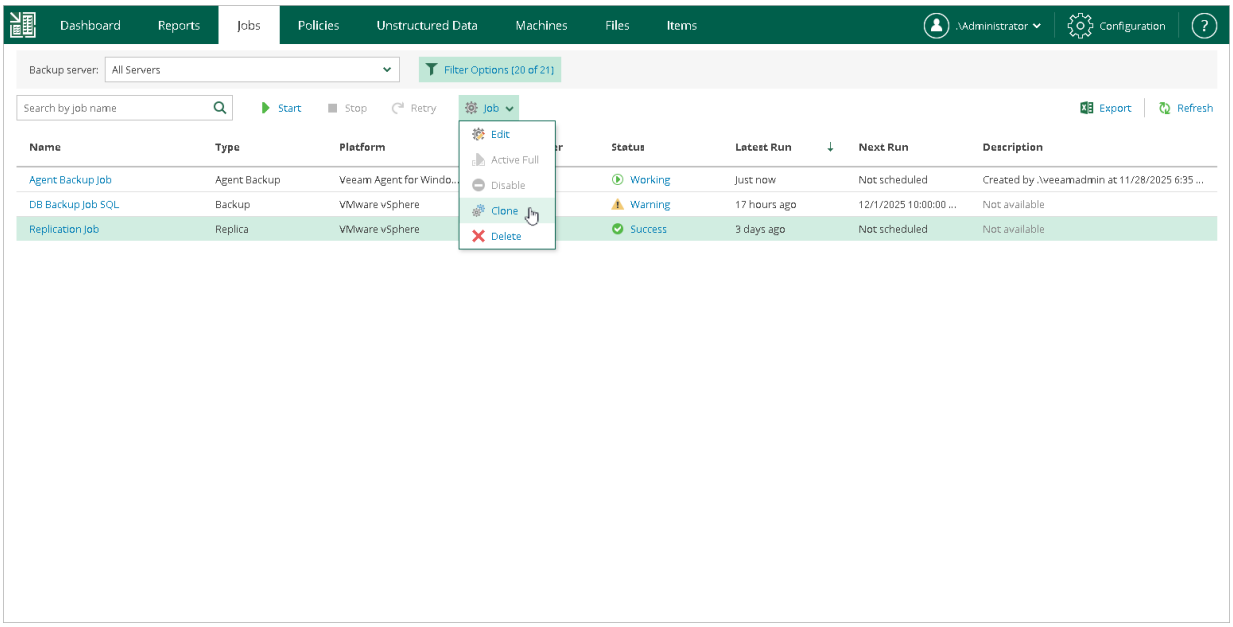
- Make sure that you have successfully connected backup servers to Veeam Backup Enterprise Manager and collected data from them. For details, see Adding Veeam Backup Server.
- You have created jobs on the backup server.

Cloning and Editing Job

To clone a job, perform the following.

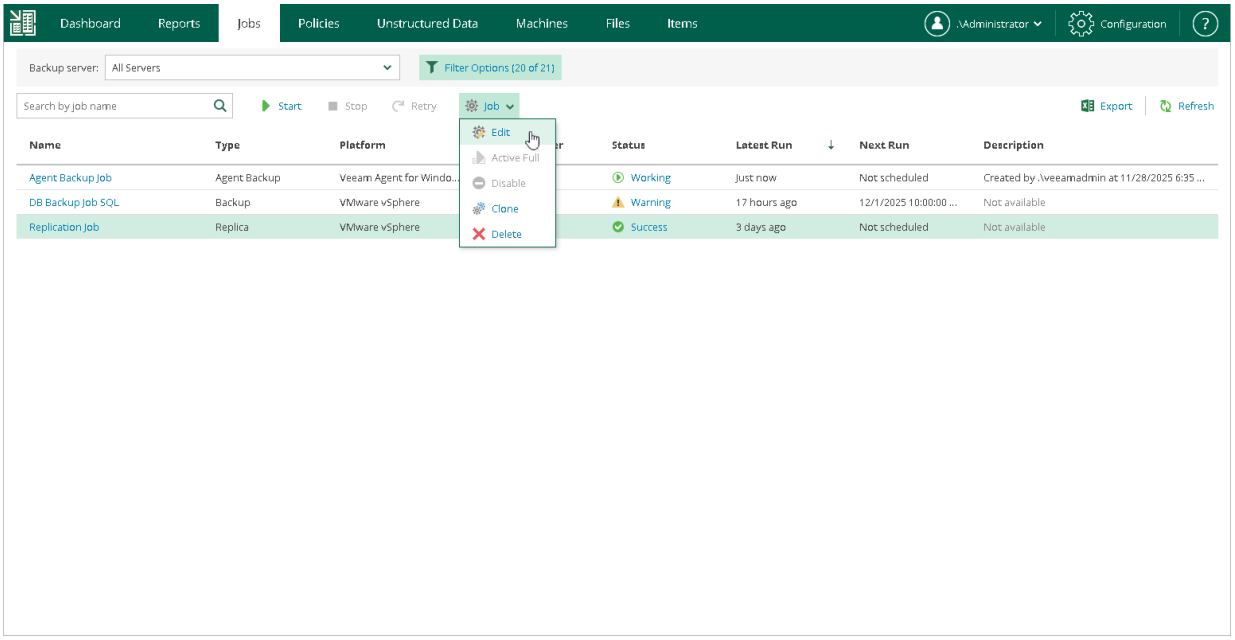
1. In Veeam Backup Enterprise Manager, click the **Jobs** tab.
2. Select the required job from the list, click **Job** at the top of the working area and click **Clone**.

   The cloned job has the same name as the original job plus the `_cloned` suffix.

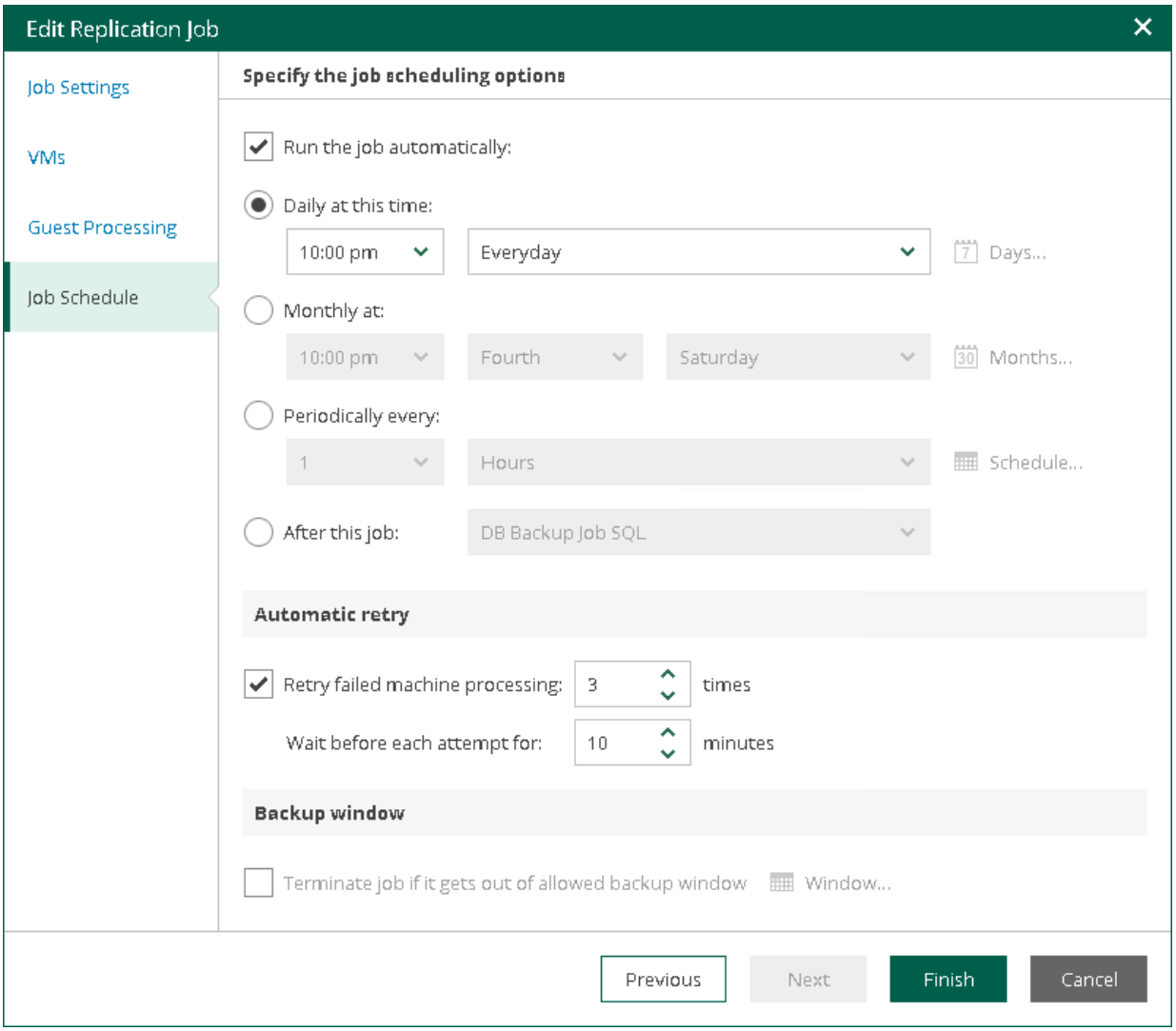


3. Select the cloned job from the list.

4. At the top of the working area, click **Job** and select **Edit**.



5. Follow the steps of the wizard and edit the job settings as required.



6. At the last step of the wizard, click **Finish**.

Reference

For more information on managing jobs, see the Managing Backup Jobs in Veeam Enterprise Manager section in the Veeam Backup Enterprise Manager Guide.

Performing 1-Click File Restore

Veeam Backup Enterprise Manager allows you to search through Microsoft Windows and Linux guest files in backed up VMs. Once you find the required file, you can immediately restore it using 1-Click file restore capability. The file can be restored to its original location or saved to a local machine.

Before You Begin

Consider the following:

- The Enterprise or Enterprise Plus license is installed on the Veeam Backup Enterprise Manager server.
- Make sure that you have successfully connected backup servers to Veeam Backup Enterprise Manager and collected data from them. For details, see Adding Veeam Backup Server.
- You can search files on machines that have at least one successfully created backup with guest file indexing enabled. For details, see Creating Application-Aware Backup Job.

Performing 1-Click Restore

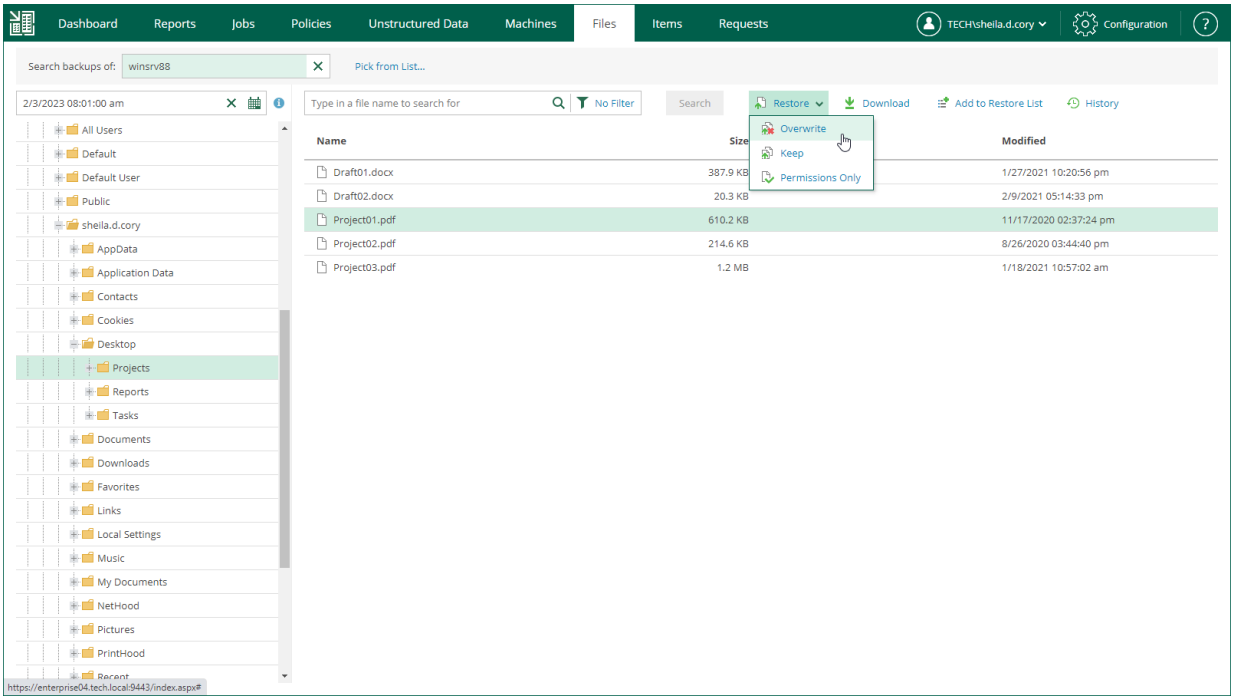
To restore a guest OS file, perform the following:

1. In the main view of Veeam Backup Enterprise Manager, click the **Files** tab.
2. In the **Type in machine name** field, specify the name of the backed up VM whose file system you want to browse.
3. In the field with the calendar icon, enter or choose a date and time of a restore point from which you want to restore files.
4. Click the **Mount** link and wait for Veeam Backup & Replication to mount the content of the backup file to the backup server.

   After the backup is mounted, you can browse the guest OS files.
5. Select the necessary file from the list.

6. At the top of the working area, click **Restore** > **Keep**.

   The original and restored files will be kept. The restored file will have the *Restored* prefix.



7. Click **Yes** to confirm the operation.

Reference

For more information on 1-click file restore, see the Performing 1-Click File Restore section in the Veeam Backup Enterprise Manager Guide.

Performing Self-Restore of VM Guest OS Files

Self-restore allows you to delegate guest OS file restore from backup administrators to users with local Administrator privileges on VMs. Users do not have to wait for backup administrators to recover deleted or modified files and folders.

For self-restore, Veeam Backup Enterprise Manager provides the Self Service File Restore portal. When users log on to the portal, they see only those VMs where they are members of local Administrators group. Other VMs are not visible to the users.

Before You Begin

Consider the following:

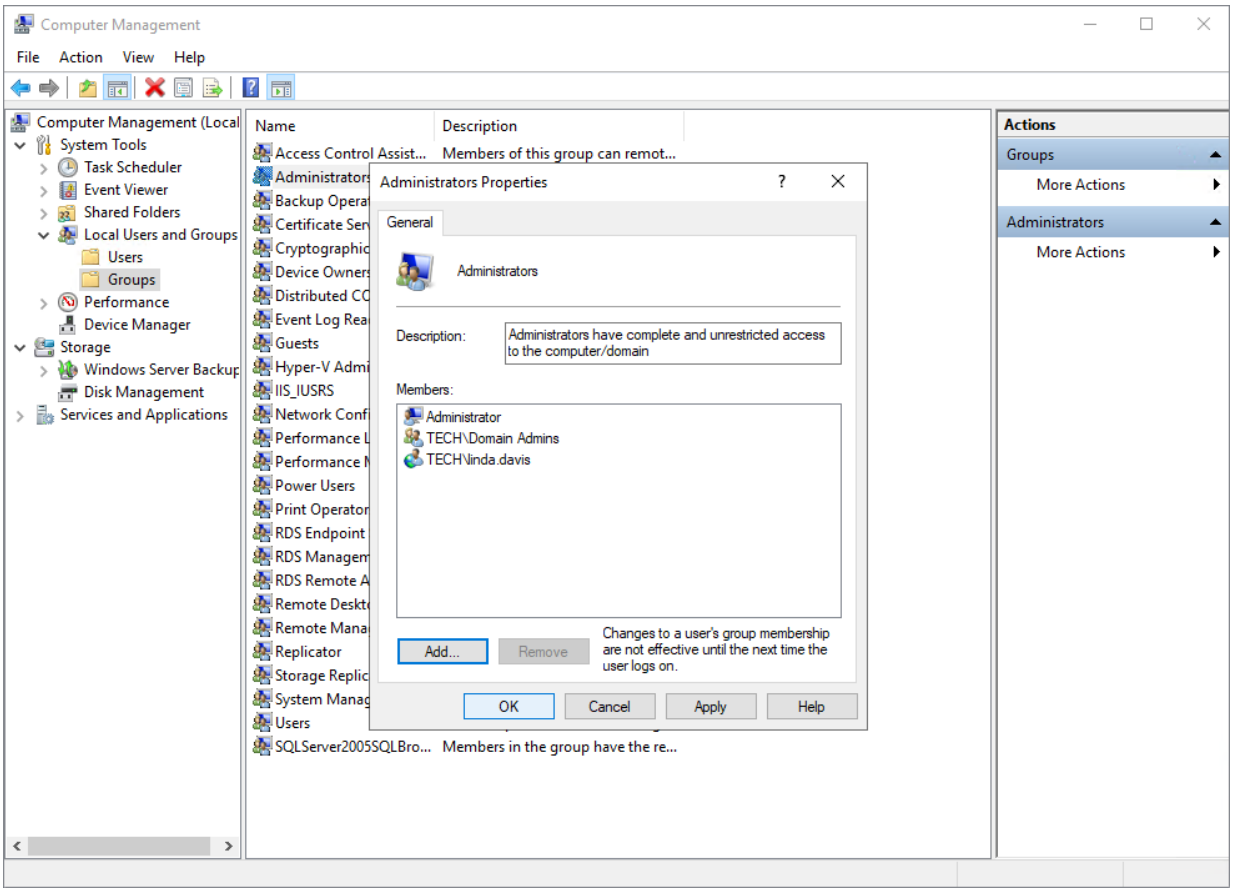
- The Enterprise Plus license is installed on the Veeam Backup Enterprise Manager server. You can use a valid trial license or paid license.
- Self-Service File Restore Portal is available only for users of Microsoft Windows machines. For Linux-based machines, guest OS file restore is performed in the Veeam Backup Enterprise Manager UI under a user account configured in Enterprise Manager. For more information, see the Configuring Accounts and Roles section in the Veeam Backup Enterprise Manager Guide.
- The account belongs to the trusted or same domain as the Enterprise Manager server (for the user account to be resolved to SID). Users from untrusted domains cannot utilize self-restore.
- The user must be a member of local Administrators group on the VM whose guest OS files you plan to restore.

  The user has access to restore points created after this user gets local Administrator privileges.
- You have successfully connected backup servers to Veeam Backup Enterprise Manager and collected data from them. For details, see Adding Veeam Backup Server.
- You have at least one successfully created backup with guest file indexing enabled. For details, see Creating Application-Aware Backup Job.

Performing Self-Restore

To restore VM guest OS files using the Veeam Self-Service File Restore portal:

1. Log in to the VM whose guest OS files you plan to restore. Make sure that the user account under which you plan to perform self-service restore is added to the local Administrators group on this VM.



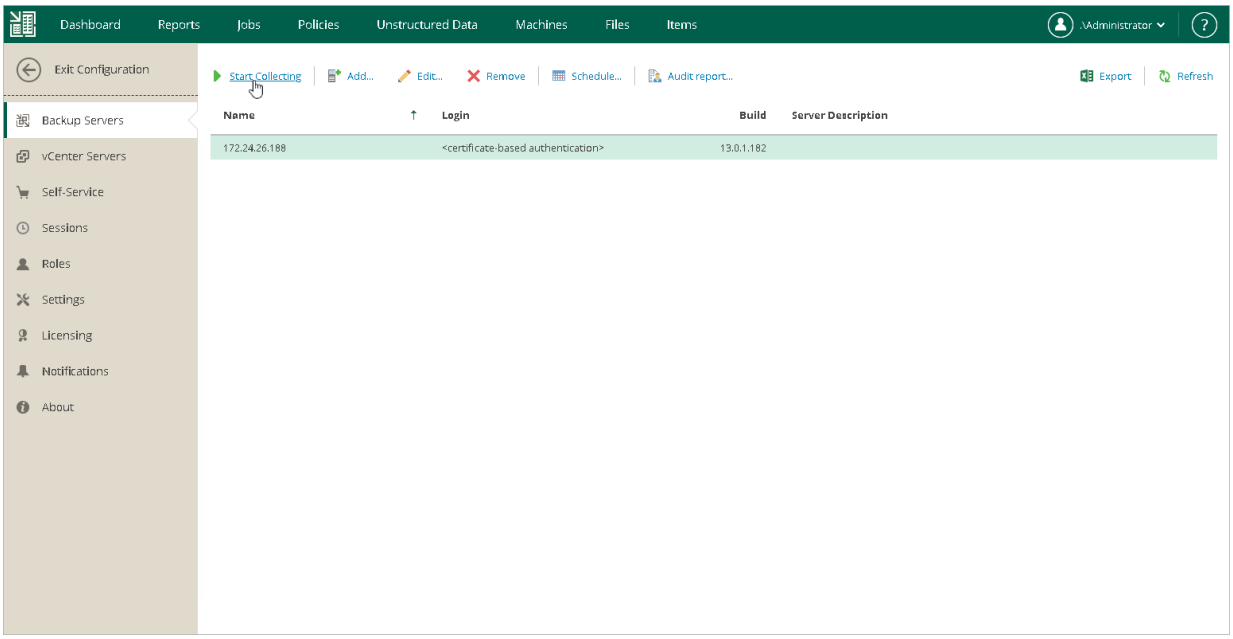
2. Log in to Veeam Backup Enterprise Manager using the user account under which you installed the program.

3. Open the **Jobs** tab and run the job with guest file indexing enabled. You can run the job several times to produce several restore points.

4. At the top right corner, click **Configuration** to open the **Configuration** view.

5. Select the **Backup Servers** tab. In the working area, click **Start Collecting**.

   Veeam Backup Enterprise Manager will collect data about jobs from the backup server. To check whether collecting data finished, click the **Sessions** tab. Make sure that the data collection session has completed with the *Success* status.



6. On another machine, open a browser and use the following address to access Veeam Self-Service File Restore portal remotely:
   `https://enterprise_manager_server_IP_address:9443/selfrestore`

7. Log in to the portal. Specify the user account with local Administrators privileges on the machine for which you plan to restore files. See the first step.

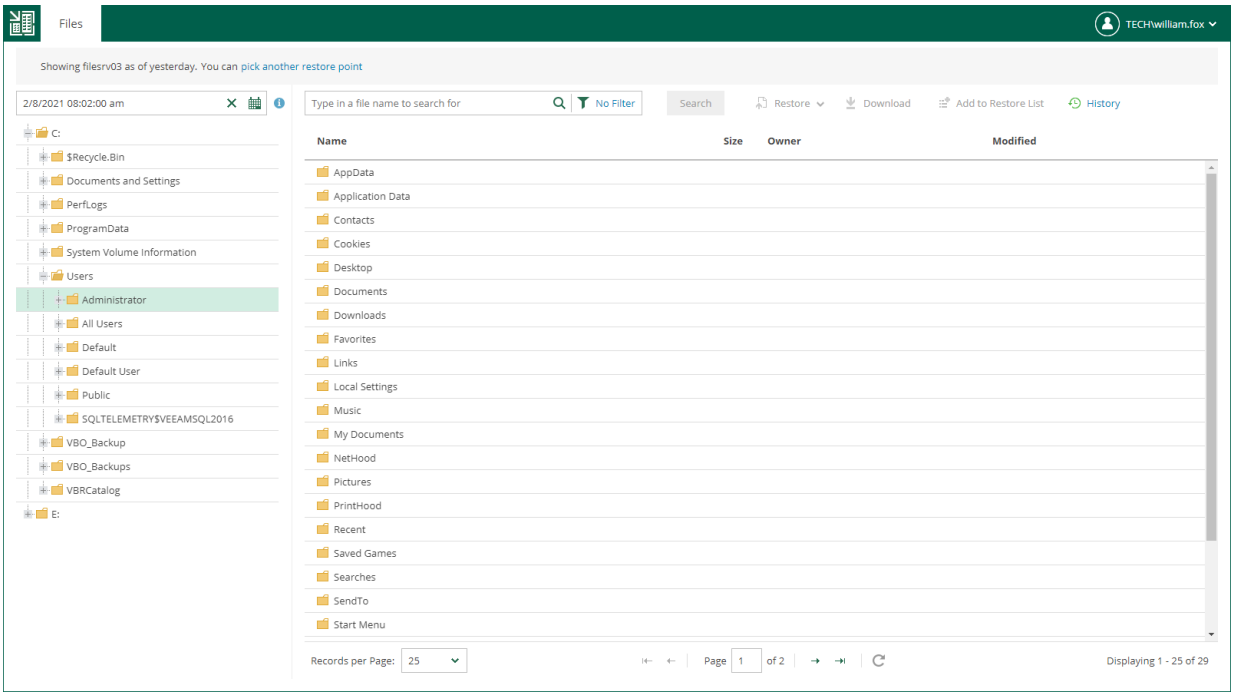
8. The portal will display only one tab — **Files.** At the top of the working area, click the **pick another restore point** link. Select the required point.

9. Click the field with the calendar icon to view guest files as of earlier restore point and select the restore point. To view guest files of another machine (if available to you), use the **Search** field or the **Pick from List** link.

10. At the top of the working area, click **Mount**.

11. Find the necessary file or folder, select it. At the top-right corner, click **Other Actions** > **Restore** > **Overwrite**.

    The original file will be overwritten.



Reference

For more information on self restore, see the Using Self-Service File Restore Portal to Restore Machine Guest Files section in the Veeam Backup Enterprise Manager Guide.

Backing Up Physical Machines

To back up physical machines, Veeam Backup & Replication uses Veeam Agents: Veeam Agent for Microsoft Windows and Veeam Agent for Linux.

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

How to back up physical machines

To back up physical machines using Veeam Backup & Replication, you must do the following:

1. Create a protection group

   When you create a protection group, you add individual machines or Active Directory containers to the protection group. Veeam Backup & Replication automatically installs agents and other required components on the machines included in the protection group.

2. Create an Agent backup job

   In the Veeam Backup & Replication console, create an agent job that will back up machines included in the protection group.

Reference

For more information on agents, see the following topics:

- Licensing Requirements
- Veeam Agent Backup
- Veeam Agent for Linux User Guide
- Veeam Agent for Microsoft Windows User Guide

Creating Protection Group

In Veeam Backup & Replication, protection groups are logical containers that pool protected computers of a specific type into groups. For example, you can create a protection group for computers of the same type (laptops, workstations or servers) or computers running the same OS type to simplify their management.

You can add individual machines or Active Directory objects that include several machines to the protection group. In this section. you will learn how to create the protection group with Active Directory objects.

Before You Begin

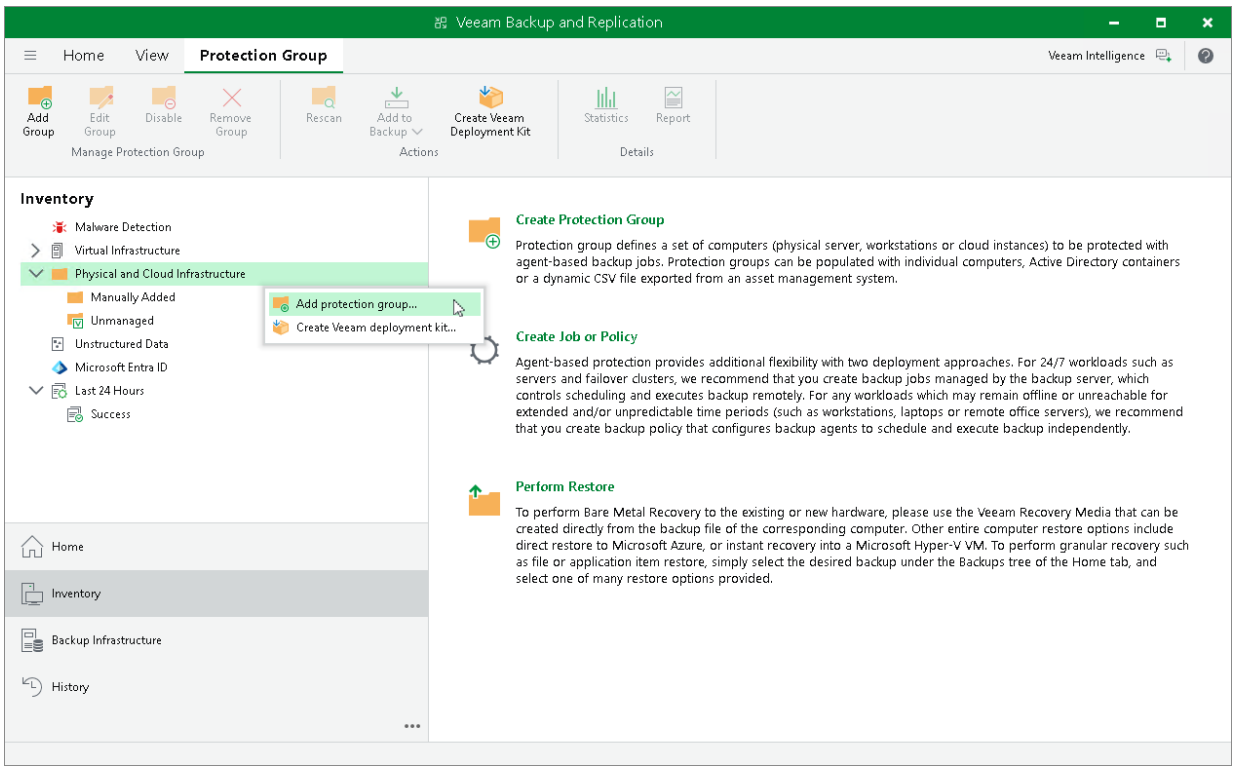
Consider the following:

- Make sure that all computers added to the protection group are powered on and can be accessed over the network.
- If you add 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.

Creating Protection Group

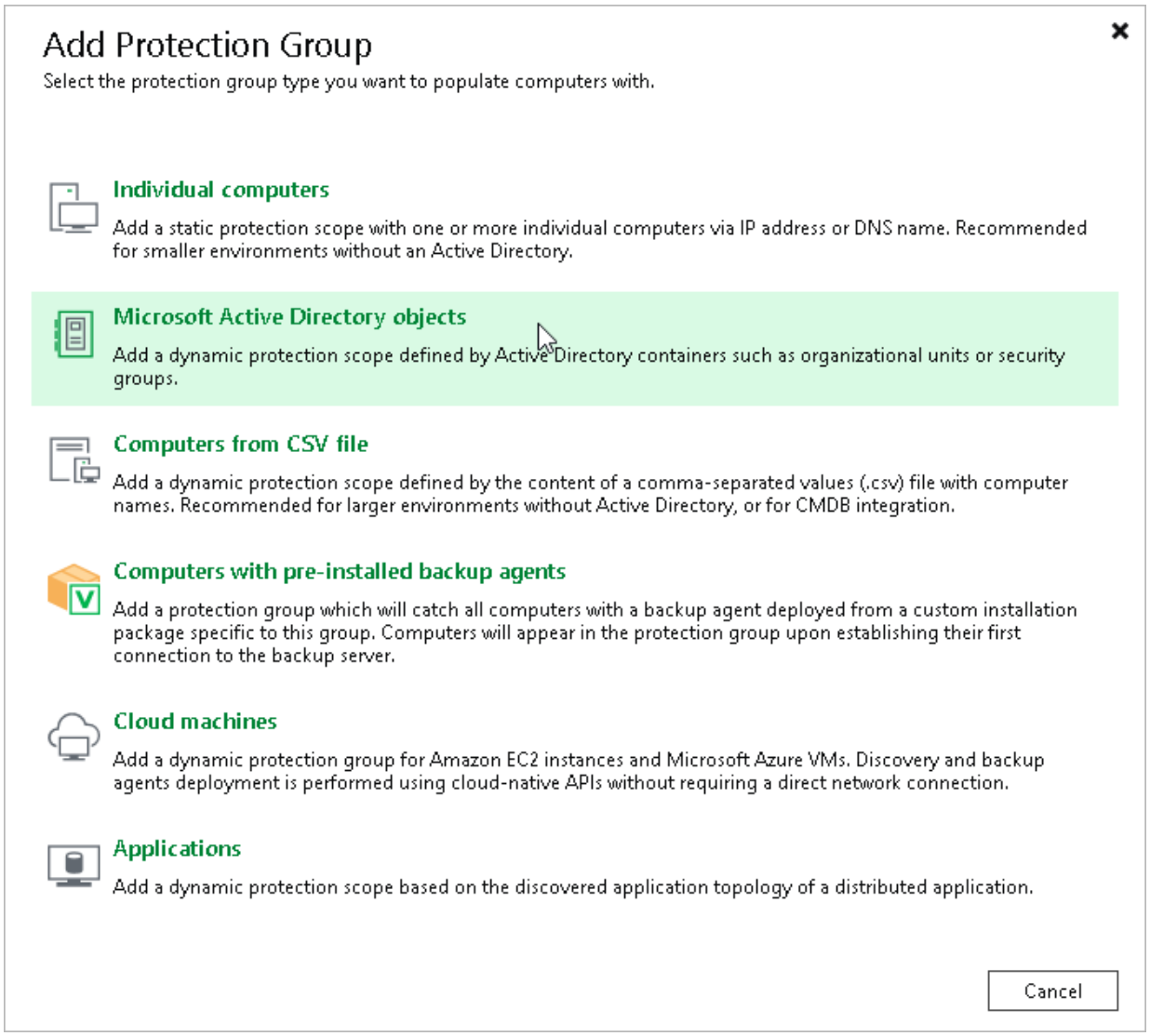
To create a protection group, do the following:

1. In the inventory pane of the **Inventory** view, right-click the **Physical Infrastructure** node and select **Add protection group**.

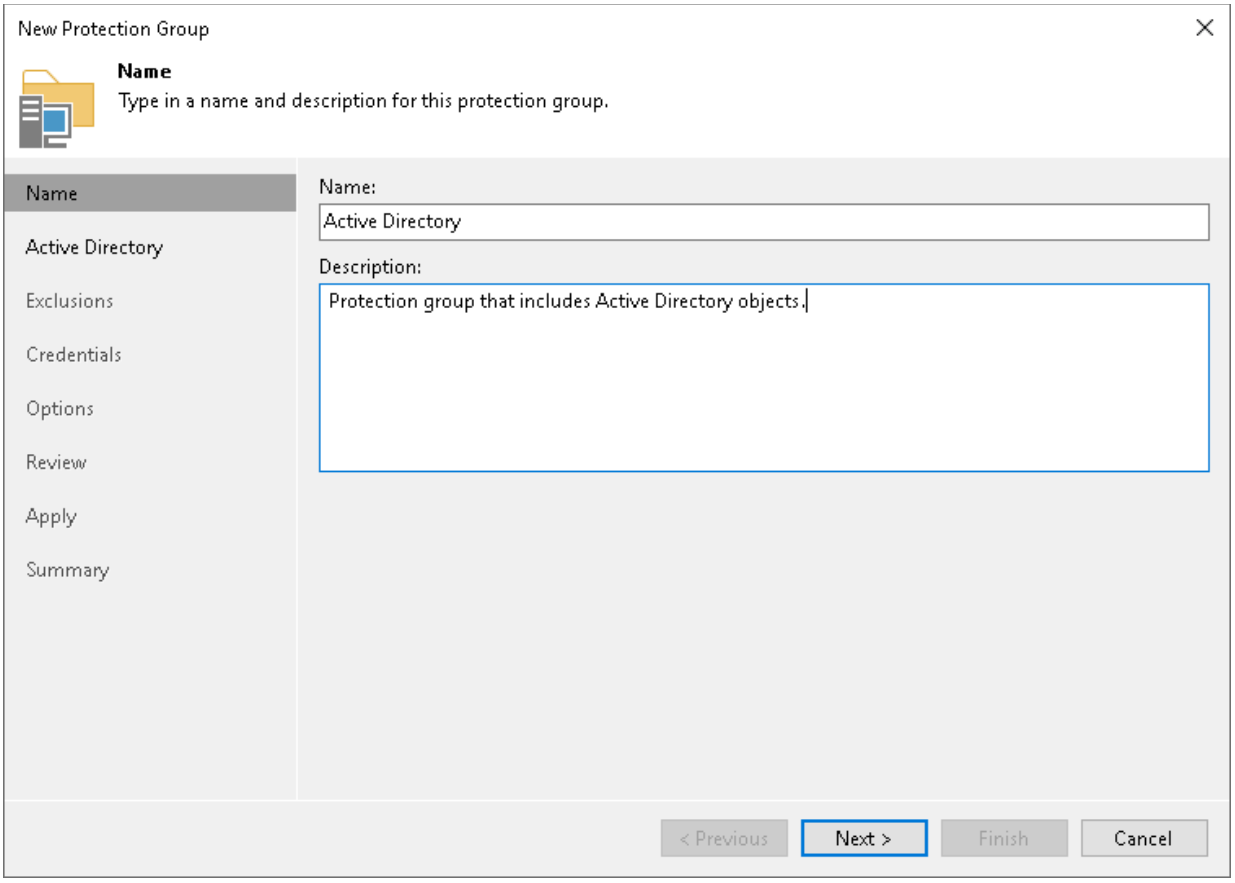


2. In the **Add Protection Group** window, select the **Microsoft Active Directory objects** option.

   Active Directory objects can be the following: entire domain, container, organization unit, group, computer or cluster. Protection groups that include Active Directory objects are dynamic. Veeam Backup & Replication discovers these computers and deploy Veeam Agent on them during the next rescan session.



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



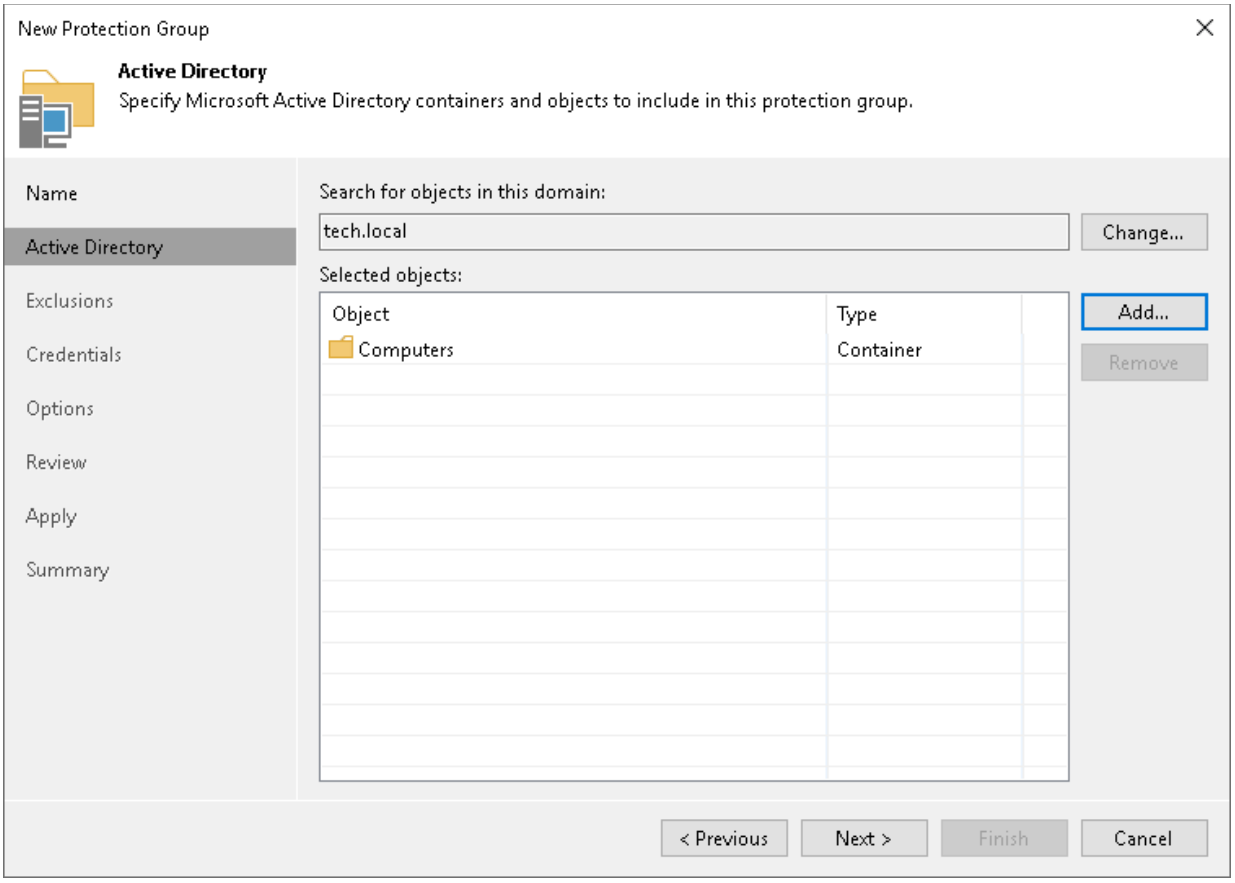
4. At the **Active Directory** step of the wizard, click **Change** near the **Search for objects in this domain field**. In the opened window, do the following:

   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, leave the default value.

   c. Near the **Account** field, click **Add** and specify user credentials. This user must have read access permissions to all hosts with the required AD objects.

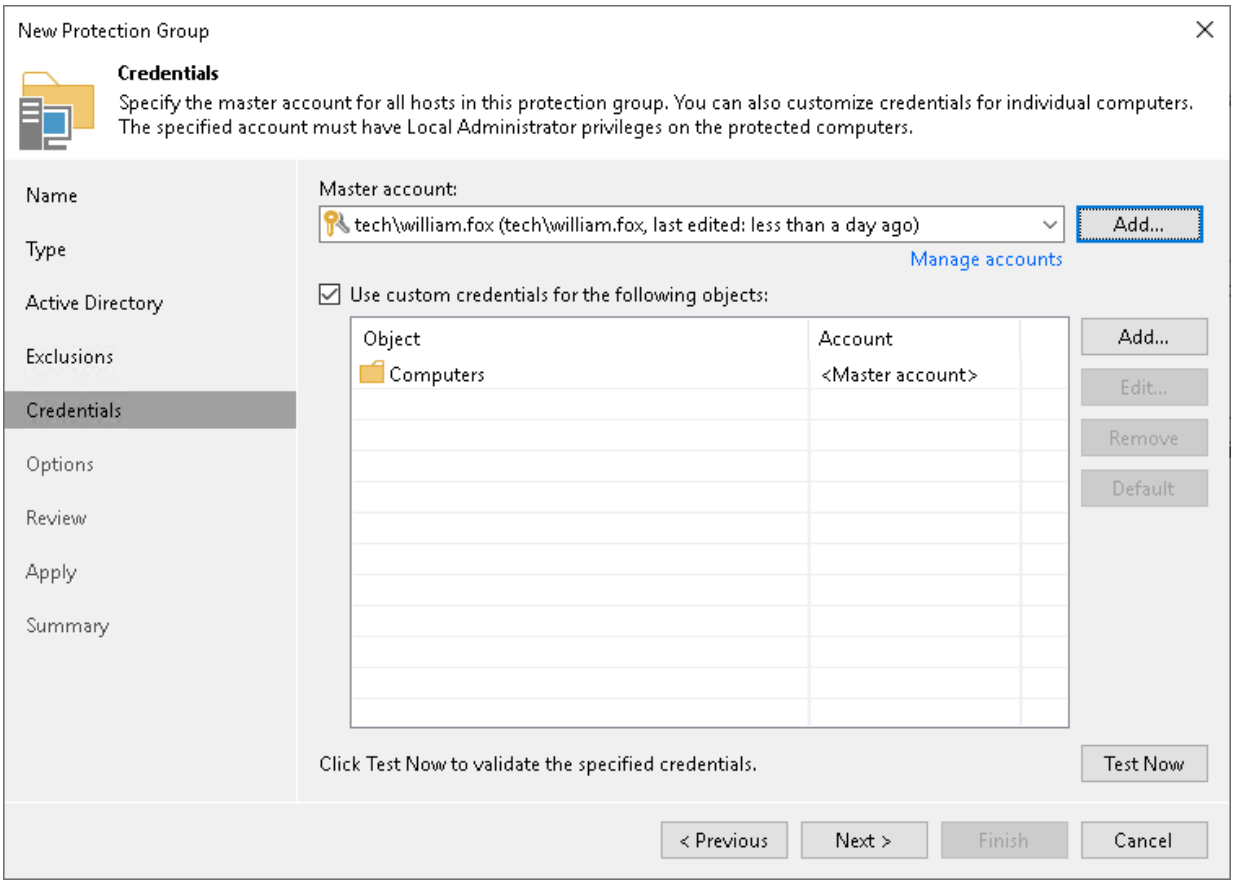
d. Click **OK**.



5. Click **Add** near the **Selected objects** field. In the **Add Objects** window, select the necessary Active Directory object and click **OK**.
6. At the **Exclusions** step of the wizard, clear the selection of **All virtual machines**.
7. At the **Credentials** step of the wizard, specify credentials to connect to computers included in the protection group.

   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 administrative permissions on all computers that you have added to the protection group.

You can also specify credentials for individual computes. For details, see the Specify Credentials section in the Veeam Backup & Replication User Guide.



8. At the **Options** step of the wizard, leave the default settings.
9. At the **Review** step of the wizard, review the components that will be installed. Click **Apply**.
10. At the **Apply** step of the wizard, Veeam Backup & Replication creates the configured protection group. Wait for the operation to complete and click **Next**.
11. At the **Summary** step of the wizard, select the **Run discovery when I click Finish** check box and click **Finish**.

Reference

For more information on creating protection groups, see the Creating Protection Groups section in the Veeam Backup & Replication User Guide.

Creating Veeam Agent Backup Job

To back up physical machines, you must configure a Veeam Agent backup job in the Veeam Backup & Replication console. In Veeam Backup & Replication, you can create Veeam Agent backup jobs of the following types:

- **Backup job**

  The backup job runs on the backup server, like VM backup jobs. The backup job is intended for computers that are connected to the backup server. This connection must not be interrupted.

- **Backup policy**

  The backup policy describes configuration of individual Veeam Agent backup jobs that run on protected computers. The backup policy is intended for computers that are connected to the backup server. The connection may be interrupted for short periods of time. For example, when you move your laptop from one location to another. Veeam Backup & Replication uses the backup policy as a template and applies settings from the backup policy to Veeam Agents that run on computers specified in the backup policy.

  In this guide, we do not detail backup policy. For more information, see Creating Veeam Agent Backup Policy.

Veeam Backup & Replication lets you create backup jobs for Microsoft Windows and Linux computers. In this section, you will learn how to create a Veeam Agent backup job for Microsoft Windows computes. For details on how to create back jobs for Linux computes, see the Creating Agent Backup Job for Linux Computers section in the Veeam Backup & Replication User Guide.

Before You Begin

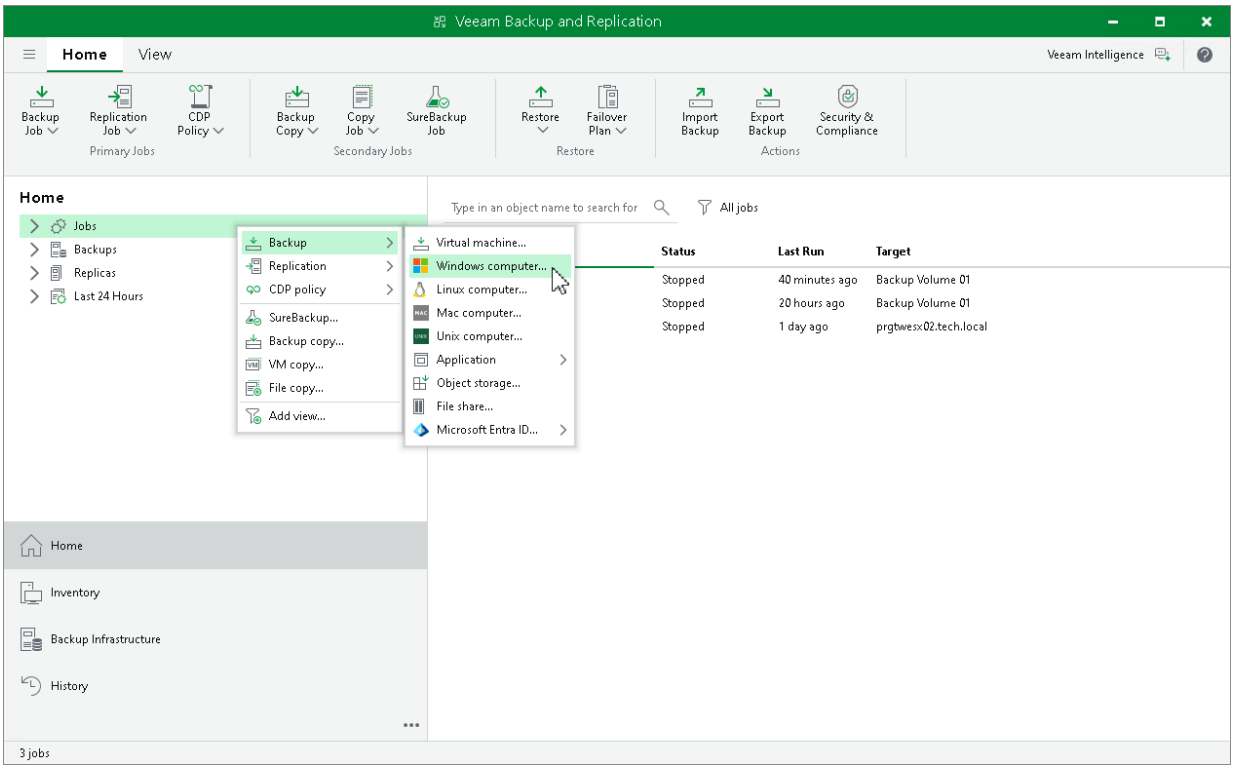
Consider the following:

- You must have at least one protection group. For details, see Creating Protection Group.
- You can create Veeam Agent backups on a Veeam backup repository only. Other types of target locations are not supported.
- 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.

Creating Veeam Agent Backup Job

1. Open the **Home** view.

2. In the inventory pane of the **Home** view, right-click the **Jobs** node and select **Backup** > **Windows computer** to open the **New Agent Backup Job** wizard.

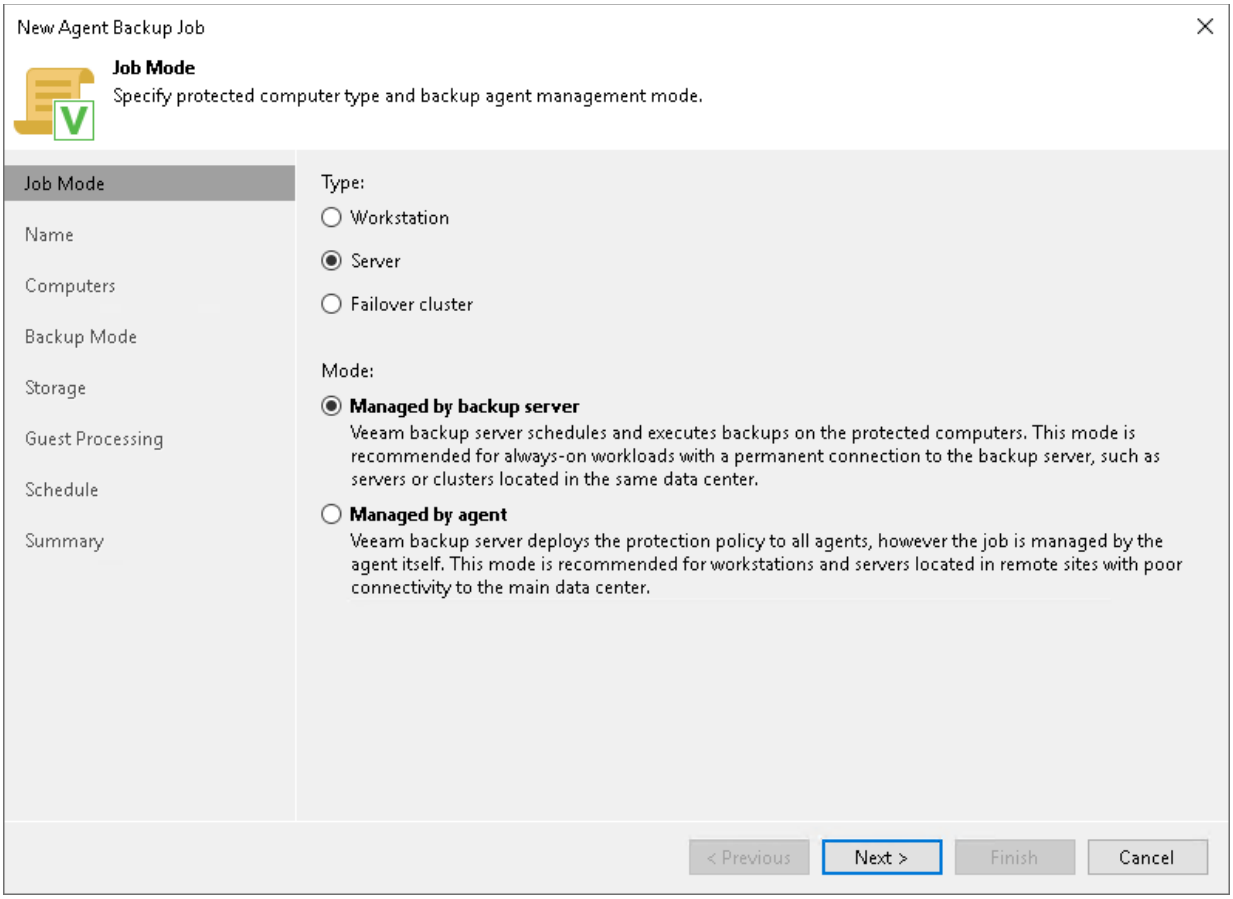


3. At the **Job Mode** step of the wizard, specify protection settings for the backup job:

   a. In the **Type** list, select **Server** to add to the backup job standalone servers that have permanent connection to the backup server.

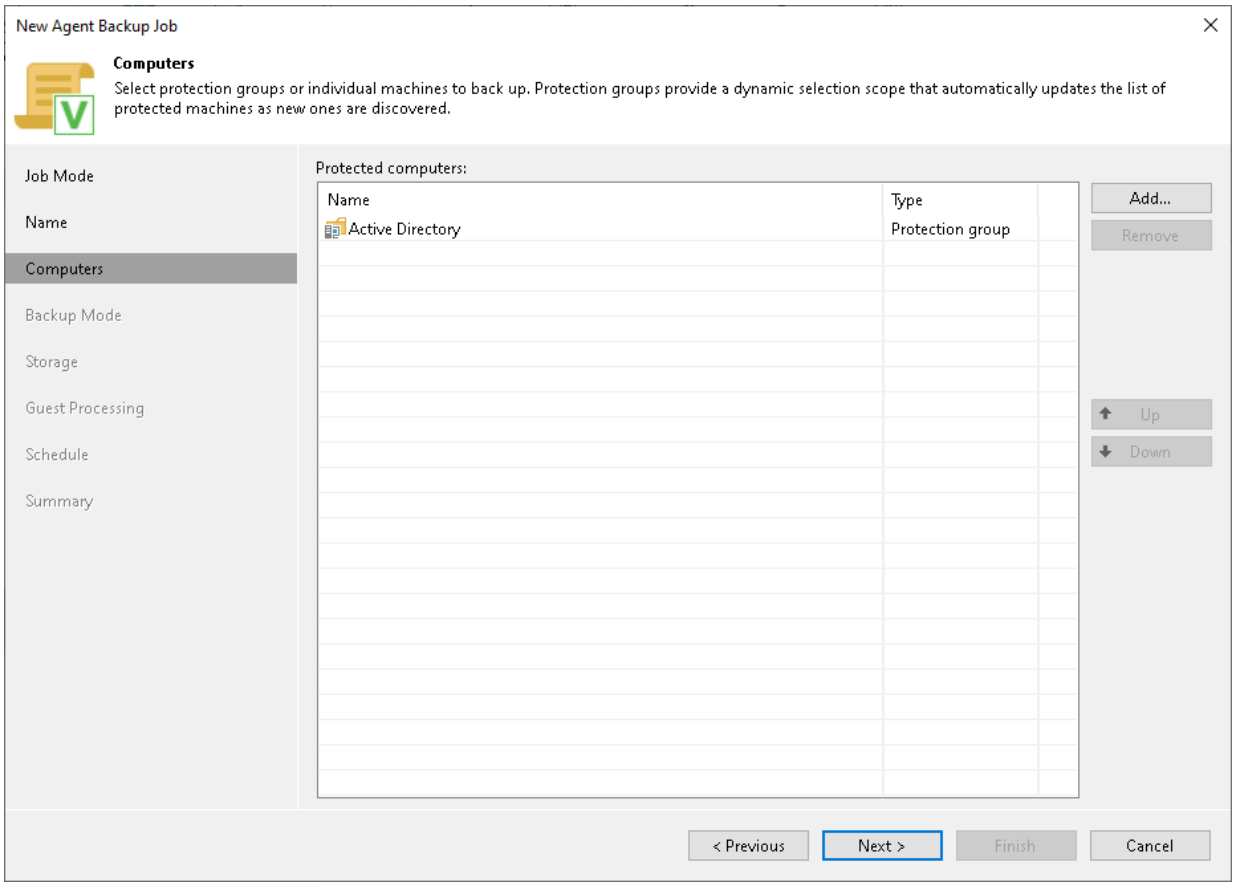
b. In the **Mode** list, select **Managed by backup server**.

When you create a Veeam Agent backup job managed by the backup server, Veeam Backup & Replication saves the job settings in its database. Veeam Backup & Replication performs all management tasks for the Veeam Agent backup job: starts a job upon the defined schedule, allocates backup infrastructure resources and so on.



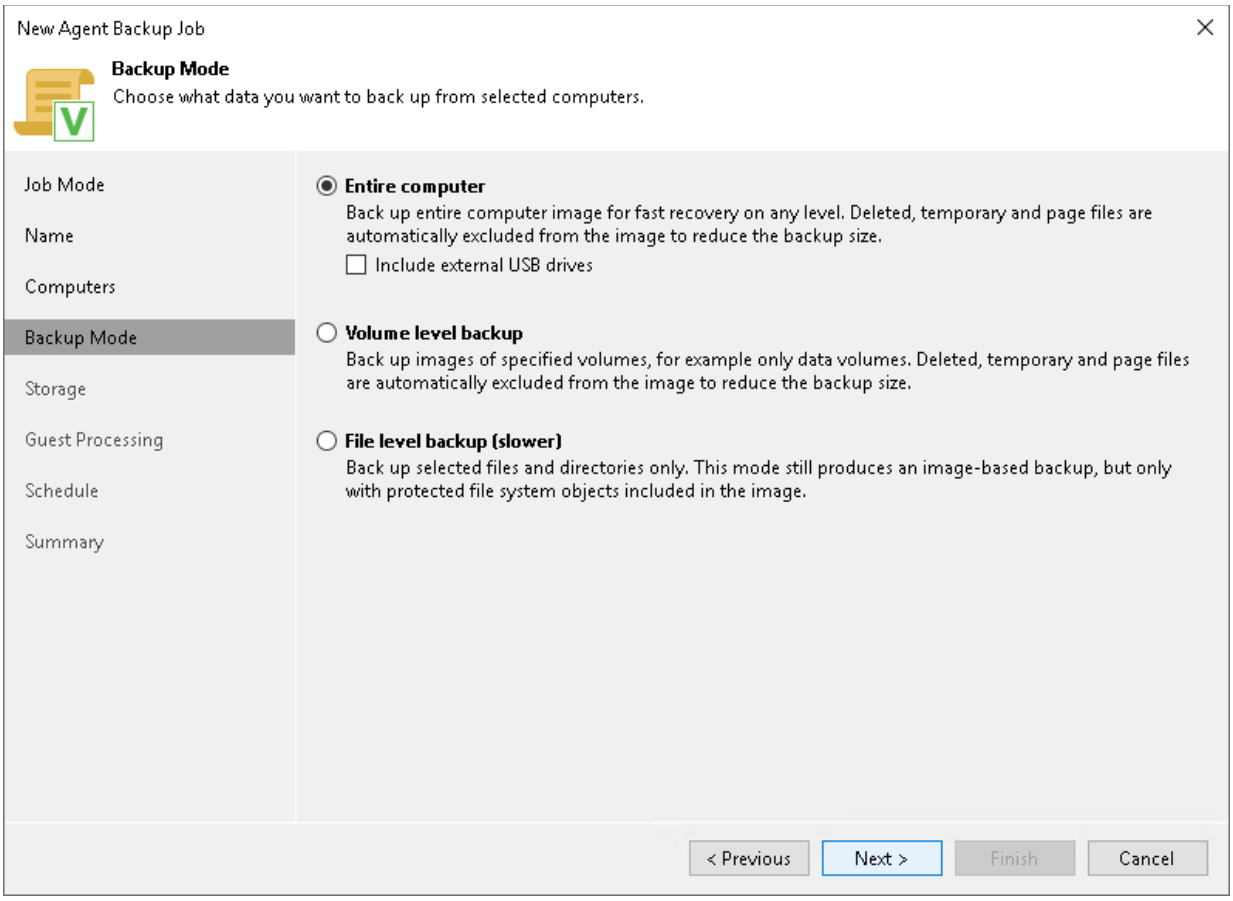
4. At the **Name** step of the wizard, specify a name and description for the backup job.

5. At the **Computers** step of the wizard, click **Add** and select one or several protection groups or computers in the list. Click **OK**.



6. At the **Backup Mode** step of the wizard, select **Entire computer**.

   When you restore data from such a backup, you are able to recover the entire computer image as well as data on specific computer volumes: files, folders and application data.



7. At the **Storage** step of the wizard, select the backup repository where you want to store your backups. For other settings, leave the default values.
8. At the **Guest Processing** step of the wizard, leave the default settings.
9. At the **Schedule** step of the wizard, define scheduling settings for the job.
10. At the **Summary** step of the wizard, select the **Run the job when I click Finish** check box and click the **Finish** button.
11. In the inventory pane of the **Home** view, expand the **Last 24 Hours** node to see the created job.

Reference

For more information on creating Veeam Agent backup jobs for Microsoft Windows computers, see the Creating Agent Backup Job for Windows Computers section in the Veeam Backup & Replication User Guide.

Restoring Data of Physical Machines

Veeam Backup & Replication allows you to restore data of physical machines. You can perform the following data restore tasks with Veeam Agent backups:

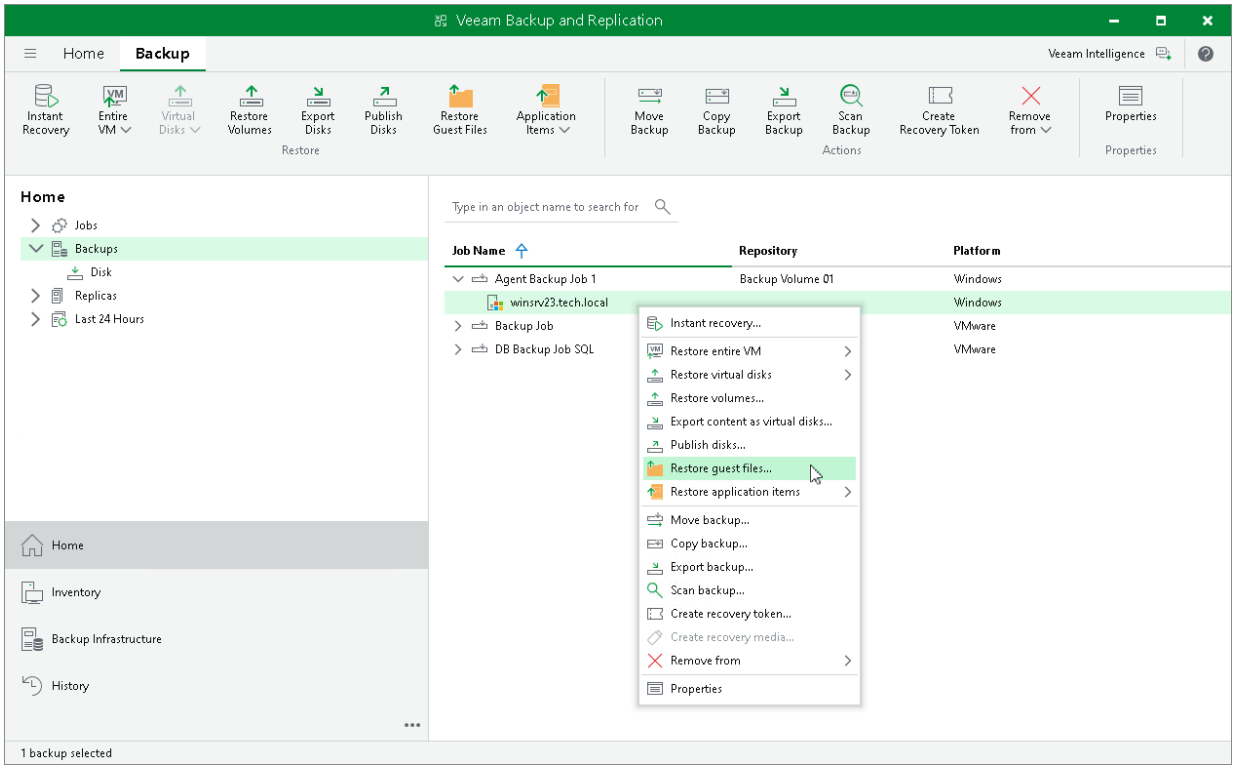
- Restoring Veeam Agent Backup to vSphere VM
- Restoring Veeam Agent Backup to Hyper-V VM
- Restoring to Microsoft Azure
- Restoring to Amazon EC2
- Restoring to Google Compute Engine
- Restoring Volumes
- Restoring Files and Folders
- Restoring Application Items

For the full list, see the Restoring Data from Veeam Agent Backups section in the Veeam Backup & Replication User Guide.

In this section, you will learn how to restore computer files and folders. For more information on other restore processes, follow the links in the list.

Restoring Files and Folders

The procedure of file-level restore from a Veeam Agent backup is similar to the same procedure for a VM backup. The difference is that you select a Veeam Agent backup instead of a VM backup in the **File Level Restore** wizard. To learn more, see Restoring VM Files.



Getting Technical Support

If you have any questions or issues with Veeam Backup & Replication, you can search for a resolution on Veeam R&D Forums or submit a support case in the Veeam Customer Support Portal.

When you submit a support case, it is recommended that you provide the Veeam Customer Support Team with the following information:

- Version information for the product and its infrastructure components
- The error message or an accurate description of the problem you are facing
- Log files

Downloading Logs

To export the product logs, do the following:

1. In the Veeam Backup & Replication console, open the main menu and navigate to **Help** > **Support Information**.
2. In the **Export Logs** wizard, do the following:
   a. At the **Scope** step, do the following:
      i. Select the **Export all logs for selected components** option.
      ii. In the **Managed servers** list, select the backup server.
      iii. If you use installed Veeam Backup & Replication with the PostgreSQL database and the same database is used to store tenant backups, select **Collect local PostgreSQL instance logs**.
   b. At the **Date Range** step, specify the time interval for which logs must be collected.
   c. At the **Location** step, specify the destination folder to which the logs will be exported.

d. Wait for the export process to complete, review the results and click the **Open folder** link to browse to exported log files and log package.

