Veeam Backup for RHV

Version 2.0

User Guide

June, 2022
© 2022 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 .............................................................................. 6
- ABOUT THIS DOCUMENT .......................................................................................... 7
- WELCOME TO VEEAM BACKUP FOR RED HAT VIRTUALIZATION .............................. 8
- ARCHITECTURE OVERVIEW ...................................................................................... 9
- PLANNING AND PREPARATION .................................................................................. 10
  - System Requirements ............................................................................................... 11
  - Required Permissions ............................................................................................... 12
  - Used Ports ................................................................................................................ 13
- LICENSING .................................................................................................................. 16
- DEPLOYMENT ................................................................................................................ 17
  - Installing RHV Plug-In ............................................................................................. 18
  - Upgrading to Veeam Backup for RHV 2.0 .............................................................. 20
  - Uninstalling RHV Plug-In ......................................................................................... 22
- CONFIGURING BACKUP INFRASTRUCTURE ................................................................ 23
  - Configuring Backup Repositories ............................................................................ 24
  - Connecting RHV Manager ....................................................................................... 25
    - Adding RHV Manager to Backup Infrastructure ...................................................... 26
    - Editing RHV Manager Properties ......................................................................... 32
  - Rescanning RHV Manager ...................................................................................... 33
  - Removing RHV Manager ......................................................................................... 34
  - Managing RHV Backup Proxy ................................................................................ 35
    - Deploying New RHV Backup Proxy ...................................................................... 36
    - Connecting Existing RHV Backup Proxy ............................................................... 46
    - Editing RHV Backup Proxy .................................................................................... 55
  - Enabling SSH on RHV Backup Proxy VM ............................................................... 56
  - Rescanning RHV Backup Proxy .............................................................................. 57
  - Removing RHV Backup Proxy ................................................................................ 58
  - Managing TLS Certificates .................................................................................... 60
    - Generating Self-Signed Certificates .................................................................... 61
    - Importing Certificates from Certificate Store ..................................................... 64
    - Importing Certificates from PFX Files .................................................................. 66
    - Using Certificate Signed by Internal CA ............................................................. 68
- ACCESSING WEB CONSOLE ....................................................................................... 72
- CONFIGURING GENERAL SETTINGS ......................................................................... 74
  - Configuring Network Settings ................................................................................ 75
  - Configuring Administrator Account ....................................................................... 76
PERFORMING DATA PROTECTION OPERATIONS ......................................................... 91
Backup Jobs ............................................................................................................. 92
  How Backup Works ................................................................................................. 93
  Creating Backup Jobs ............................................................................................ 96
  Creating Active Full Backup .................................................................................... 110
Backup Copy Jobs .................................................................................................... 111
Backup to Tape Jobs ................................................................................................. 112
Managing Backup Jobs ............................................................................................ 113
  Starting and Stopping Backup Jobs ........................................................................ 114
  Editing Backup Job Settings .................................................................................... 115
  Enabling and Disabling Backup Jobs ........................................................................ 116
  Deleting Backup Jobs .............................................................................................. 117
Managing Backups ..................................................................................................... 118
  Viewing Backup Properties ...................................................................................... 119
  Importing Backups .................................................................................................. 120
  Exporting Backups .................................................................................................. 122
  Deleting Backups .................................................................................................... 124
PERFORMING DATA RECOVERY OPERATIONS ......................................................... 127
Entire VM Restore ..................................................................................................... 128
  Before You Begin .................................................................................................... 129
  Restoring VMs Using Veeam Backup & Replication Console ................................ 130
  Restoring VMs Using RHV Backup Proxy Console ................................................. 141
VM Disks Restore ..................................................................................................... 153
  Before You Begin .................................................................................................... 154
  Launch Virtual Disk Restore Wizard ....................................................................... 155
  Step 1. Select Virtual Machine ................................................................................ 156
  Step 2. Select Restore Point ..................................................................................... 157
  Step 3. Configure Mapping Settings ......................................................................... 158
  Step 4. Specify Reason for Restore .......................................................................... 161
  Step 5. Finish Working with Wizard ........................................................................ 162
Instant VM Recovery .................................................................................................. 163
VM Guest OS Files Restore ......................................................................................... 164
VM Disk Export.........................................................................................166
Restore to Amazon EC2........................................................................167
Restore to Microsoft Azure....................................................................168
Restore to Google CE ..........................................................................169

MONITORING EVENTS..............................................................................170

GETTING TECHNICAL SUPPORT..........................................................171
Exporting Logs in RHV Backup Proxy Web Console.................................172
Exporting Logs in Veeam Backup & Replication Console.........................173
Checking RHV Backup Proxy Version......................................................174
Contacting Veeam Software

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

Customer Support

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

Company Contacts

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

Online Support

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

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

This guide provides information about main features of Veeam Backup for Red Hat Virtualization (Veeam Backup for RHV). The document describes how to deploy, configure and use Veeam Backup for RHV.

Intended Audience

This guide is designed for IT specialists who plan to use Veeam Backup for RHV to protect VMs residing on RHV hosts.
Welcome to Veeam Backup for Red Hat Virtualization

Veeam Backup for Red Hat Virtualization (Veeam Backup for RHV) is a solution developed for protection and disaster recovery tasks for the Red Hat Virtualization (RHV) environment. With Veeam Backup for RHV, you can back up VMs and restore them from files stored on backup repositories. As Veeam Backup for RHV uses an agentless approach to back up RHV VMs, no additional software is required.

With Veeam Backup for RHV, you can perform the following backup and restore operations:

- Create backups of RHV VMs and store them in backup repositories.
- Create backup copies.
- Restore VMs from backups to the RHV environment.
- Restore RHV VMs from backups to Microsoft Azure Blob, Amazon EC2 and Google CE.
- Perform Instant Recovery of RHV VMs to Nutanix AHV, VMware vSphere and Microsoft Hyper-V environments.
- Restore files of VM guest OS.
- Restore VM disks and attach them to VMs running on RHV hosts.
- Export disks of backed-up VMs to VMDK, VHD and VHDX formats.
Architecture Overview

Veeam Backup for RHV infrastructure comprises the following set of components:

1. **Backup server** is a Windows-based server on which Veeam Backup & Replication is installed. The backup server is the configuration, administration and management component of the backup infrastructure. It coordinates backup and restore tasks, controls job scheduling and manages resource allocation.

2. **RHV manager** is a Linux-based server that manages RHV resources such as VMs, hosts, clusters, storage domains and networks, and provides access to them. Veeam Backup for RHV uses the RHV manager as source and target for backup and restore operations.

3. **RHV Plug-in** is an architecture component that enables integration between the backup server and the RHV manager. RHV Plug-in also allows the backup server to deploy and manage the RHV backup proxy.

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

   The RHV backup proxy is a Linux-based VM that resides on an RHV host and runs the following applications and services:

   - **Veeam RHV backup proxy Web console** is an interface that allows you to manage backup and restore operations and to configure settings of the RHV backup proxy.

   - **Veeam Data Mover** is a service that performs data processing tasks on behalf of Veeam Backup & Replication, such as retrieving source machine data, performing data deduplication and compression, and storing backed-up data on the target repository.

   - **Veeam Updater** is a service that is responsible for installing and scheduling updates for the RHV backup proxy.

5. **Backup repository** is an architecture component where the Veeam Backup for RHV stores backup files. The backup repository also runs the Veeam Data Mover service that retrieves backed-up data from the RHV backup proxy.
Planning and Preparation

Before you start deploying Veeam Backup for RHV, check supported virtualization platforms, system requirements, permissions and network ports used for data transmission.

In This Section:

- System Requirements
- Required Permissions
- Used Ports
- Licensing
# System Requirements

Before you start deploying Veeam Backup for RHV, make sure the RHV environment and the backup infrastructure components meet the following requirements.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtualization Platform</strong></td>
<td>Veeam Backup for RHV is compatible with Red Hat Virtualization version 4.4 SP1 only.</td>
</tr>
<tr>
<td><strong>Veeam Software</strong></td>
<td>Veeam Backup &amp; Replication version 11a CP4 with RHV Plug-in version 11.0.2.253 (or later) must be deployed on the backup server. <strong>Note:</strong> The RHV manager, RHV hosts and the RHV backup proxy must be able to resolve the FQDN of the backup server.</td>
</tr>
</tbody>
</table>
| **RHV backup proxy** | The RHV backup proxy must be provided with sufficient computing resources to handle tasks (backup or restore sessions) in parallel. The maximum number of concurrent tasks is configured in RHV backup proxy settings. If this number is exceeded, the backup proxy will not start a new task until one of the current tasks finishes. In the default RHV backup proxy configuration, the maximum number of concurrent tasks is set to 4, and the following computing resources are allocated:  
  - **CPU:** 8 vCPU  
  - **Memory:** 4 GB RAM  
  - **Disk Space:** 64 GB for product installation, internal database files, logs and other data  
  **Notes:**  
  1. While deploying a new RHV backup proxy or editing settings of an existing one, you can increase the maximum number of concurrent tasks, however, you must allocate 1 vCPU (2 vCPUs recommended) and 1 GB RAM for each additional task. When configuring the maximum number of concurrent tasks, you must also take into account the network traffic throughput in your virtual infrastructure.  
  2. The RHV backup proxy must be able to resolve FQDNs of the backup server, RHV manager and all RHV hosts. |
Required Permissions

The accounts used to install and administer Veeam Backup for RHV infrastructure components must have the following permissions.

Backup Server Windows Account Permissions

The Windows account used to install Veeam Backup & Replication and RHV Plug-in on the backup server must have the following permissions.

<table>
<thead>
<tr>
<th>Account</th>
<th>Required Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup Account</td>
<td>The account used to install Veeam Backup &amp; Replication and RHV Plug-in must have the Local Administrator permissions on the backup server.</td>
</tr>
<tr>
<td>Veeam Backup &amp; Replication User Account</td>
<td>The account used to run Veeam Backup &amp; Replication services must be a LocalSystem account or must have the Local Administrator permissions on the backup server.</td>
</tr>
</tbody>
</table>

Red Hat Virtualization Permissions

The RHV administrator account that the backup server uses to access the RHV manager must have the SuperUser privileges. For more information on RHV system permissions, see Red Hat Product Documentation.
Used Ports

Veeam Backup for RHV automatically creates firewall rules for the ports required to allow communication between the RHV backup proxy and the backup server.

**IMPORTANT**
Some Linux distributions require manual configuration of firewall rules. For more information, see this Veeam KB article.

**RHV backup proxy**

The following table describes network ports that must be open to ensure proper communication of the RHV backup proxy with other backup infrastructure components.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation web browser</td>
<td>RHV backup proxy</td>
<td>443, 8100</td>
<td>HTTPS</td>
<td>Used to access the RHV backup proxy web console.</td>
</tr>
<tr>
<td>RHV backup proxy</td>
<td>RHV manager</td>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Used to communicate with the REST API service running on the RHV manager.</td>
</tr>
<tr>
<td>RHV manager</td>
<td>54323</td>
<td>TCP</td>
<td></td>
<td>Used to communicate with RHV Manager (hosted engine).</td>
</tr>
<tr>
<td>RHV host</td>
<td>443</td>
<td>TCP/HTTPS</td>
<td></td>
<td>Used to communicate with the REST API service running on an RHV host.</td>
</tr>
<tr>
<td>RHV host</td>
<td>54322</td>
<td>TCP</td>
<td></td>
<td>Used to communicate with RHV hosts.</td>
</tr>
<tr>
<td>Veeam backup repository or gateway server</td>
<td>2500-3300*</td>
<td>TCP</td>
<td></td>
<td>Default range of ports used as transmission channels for jobs and restore sessions. For each TCP connection that a job uses, one port from this range is assigned.</td>
</tr>
<tr>
<td>Ubuntu Security and OS Update repository (security.ubuntu.com, archive.ubuntu.com)</td>
<td>80</td>
<td>HTTP</td>
<td>Required to get OS security updates.</td>
<td></td>
</tr>
</tbody>
</table>
### Backup Server

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

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Core Update repository</td>
<td></td>
<td>443</td>
<td>HTTPS</td>
<td>Required to get .NET Core updates.</td>
</tr>
<tr>
<td>Veeam Updater repository</td>
<td></td>
<td>443</td>
<td>TCP</td>
<td>Required to download RHV backup proxy update packages.</td>
</tr>
<tr>
<td>Nginx repository</td>
<td></td>
<td>443</td>
<td>TCP</td>
<td>Required to download nginx packages.</td>
</tr>
</tbody>
</table>

* This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 11a CP4 from earlier versions of the product, the range of ports from 2500 to 5000 applies to the already added components.

---

**Backup Server**

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

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Port</th>
<th>Protocol</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHV backup proxy, Veeam Backup &amp; Replication console and Veeam ONE server</td>
<td>Backup server</td>
<td>8544</td>
<td>HTTPS</td>
<td>Used by the RHV Platform Service.</td>
</tr>
<tr>
<td>Backup server</td>
<td>FLR helper appliance</td>
<td>22</td>
<td>TCP</td>
<td>Used to connect to the helper appliance during file-level restore.</td>
</tr>
<tr>
<td>Backup server</td>
<td></td>
<td>6172</td>
<td>HTTPS</td>
<td>Used used by the RHV Platform Service to connect to a component that enables communication with the Veeam Backup &amp; Replication database.</td>
</tr>
<tr>
<td>RHV manager</td>
<td></td>
<td>443</td>
<td>TCP/HTTPS</td>
<td>Used to communicate with the REST API service running on the RHV manager.</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Port</td>
<td>Protocol</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------</td>
<td>--------</td>
<td>----------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RHV manager</td>
<td>RHV manager</td>
<td>54323</td>
<td>TCP</td>
<td>Used to communicate with the RHV manager (hosted engine).</td>
</tr>
<tr>
<td>RHV backup proxy</td>
<td>RHV backup proxy</td>
<td>443, 8100</td>
<td>HTTPS</td>
<td>Used by the RHV Platform Service to connect to the RHV backup proxy.</td>
</tr>
</tbody>
</table>

**NOTE**

To see the list of ports used by the backup server to communicate with backups repositories, see the Veeam Backup & Replication User Guide, section *Used Ports*. 
Licensing

Veeam Backup for RHV is licensed by the number of protected RHV VMs. Each protected RHV VM consumes one Veeam Universal License instance from the license scope. An RHV VM is considered protected if it has a restore point created during the past 31 days.

Obtaining New License

You can obtain the following types of licenses for Veeam Backup for RHV:

- **Evaluation license** is a free license that can be used for product evaluation. The license is valid for 30 days from the moment of the product download.
  
  To obtain this license, request a trial key on the Veeam downloads page as described in the Veeam Backup & Replication User Guide, section Obtaining and Renewing License.

- **Subscription license** is a paid license with a limited subscription term. The expiration date of the Subscription license is set to the end of the subscription term. The Subscription license term is normally 1-5 years from the license issue date.
  
  To obtain this license, choose the required subscription term on the Veeam Backup & Replication Pricing page and contact Veeam Sales Team.

- **Perpetual license** is a paid license without an expiration date. The Perpetual license typically includes one year period of basic support and maintenance that can be extended.
  
  To obtain this license, contact a reseller in your region.

After you obtain a license, install it on the backup server as described in the Veeam Backup & Replication User Guide, section Installing License.

Using Existing License

If you already use Veeam Backup & Replication and you have spare Veeam Universal License instances on your backup server, they will be used to protect RHV VMs. You can check the number of available license instances in the Veeam Backup & Replication console as described in the Veeam Backup & Replication User Guide, section Viewing License Information.

If you have a legacy perpetual per-socket license, you must obtain Veeam Universal License instances and merge them with the existing perpetual socket license as described in the Veeam Backup & Replication User Guide, section Merging Licenses.
Deployment

To deploy Veeam Backup for RHV, do the following:

1. Deploy the backup server as described in the Veeam Backup & Replication User Guide, section Installing Veeam Backup & Replication.

   Alternatively, you can use a backup server that already exists in your backup infrastructure if it meets the Veeam Backup for RHV system requirements.

2. Install RHV Plug-in on the backup server.

3. Perform initial configuration of Veeam Backup for RHV:
   a. Configure backup repositories where Veeam Backup for RHV will store backups of RHV VMs.
   b. Add to the backup infrastructure the RHV manager that administers RHV resources you want to protect.
   c. Deploy an RHV backup proxy that will process backup and restore operations.
Installing RHV Plug-In

The default installation package of Veeam Backup & Replication does not provide features that allow you to protect RHV resources. To be able to add your RHV manager and RHV backup proxy to the backup infrastructure, you must install RHV Plug-in on the backup server.

NOTE

If you use a remote Veeam Backup & Replication console, you do not need to install RHV Plug-in on the workstation where the remote Veeam Backup & Replication console is deployed. However, you must install RHV plug-in on the back.

To install RHV Plug-in, do the following:

1. Log in to the backup server using an account with the local Administrator permissions.
2. Download the product file RHVPlugin_11.0.2.253.zip from the Veeam downloads page.
3. Open the downloaded archive file and launch the RHVPlugin_11.0.2.253.exe file.
   Before proceeding with installation, the installer will check whether you have Microsoft .NET Core Runtime installed on the backup server. In case the required version is missing, the installer will offer to install it automatically. To do that, click OK.
4. At the License Agreement step of the RHV Plug-In for Veeam Backup & Replication Setup wizard, read and accept both the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.

To read the terms of the license agreement for the 3rd party components, click View.
5. At the **Installation Path** step of the wizard, you can change the installation directory if necessary.

6. Click **Install** to begin installation.
Upgrading to Veeam Backup for RHV 2.0

You can upgrade the Veeam Backup for RHV from version 1.0 and 1a to 2.0.

Before you start the upgrade process, do the following:

- Install all available updates on the RHV backup proxy.
- Download Veeam Backup & Replication version 11a CP4 from the Veeam downloads page.
- Download the latest RHV Plug-in version from the Veeam downloads page.
- Plan a maintenance period. Typically, the upgrade process takes up to one hour. Make sure there are no jobs currently running or scheduled to run during this period. Wait for the jobs to complete or disable the jobs manually before you start upgrading Veeam Backup for RHV.
- Make sure the RHV backup proxy is powered on.

Online Upgrade

If your backup server and the RHV backup proxy are connected to the internet, do the following:

1. Back up the configuration database of the RHV backup proxy. For more information, see Performing Configuration Backup.
2. Upgrade Veeam Backup & Replication to version 11a CP4. For more information, see the Veeam Backup & Replication User Guide, section Upgrading to Veeam Backup & Replication 11 or 11a.
3. Install RHV Plug-in. For more information, see Installing RHV Plug-In.
4. Add the RHV manager to the backup infrastructure. For more information, see Adding RHV Manager to Backup Infrastructure.
5. Add the RHV backup proxy to the backup infrastructure. To do that, launch the New Red Hat Virtualization Proxy Wizard and select the Connect to an existing proxy option at the Deployment Mode step of the wizard. For more information, see Connecting Existing RHV Backup Proxy.

After you complete the wizard, the backup server will upgrade the RHV backup proxy. If the proxy fails to be upgraded, you can retry the upgrade:

1. In the Veeam Backup & Replication console, open the Backup Infrastructure view.
2. Navigate to Backup Proxies > Out of Date.
3. Select the RHV backup proxy and click Upgrade Proxy on the ribbon.
4. In the Components Update window, click Apply.

Offline Upgrade

If your backup server or the RHV backup proxy is not connected to the internet, do the following:

1. Back up the configuration database of the RHV backup proxy. For more information, see Performing Configuration Backup.
2. Shut down the RHV backup proxy. For more information, see Rebooting or Shutting Down Proxy.
3. Upgrade Veeam Backup & Replication to version 11a CP4. For more information, see the Veeam Backup & Replication User Guide, section Upgrading to Veeam Backup & Replication 11 or 11a.
4. Install RHV Plug-in. For more information, see Installing RHV Plug-In.

5. Add the RHV manager to the backup infrastructure. For more information, see Adding RHV Manager to Backup Infrastructure.

6. Deploy a new RHV backup proxy. For more information, see Deploying New RHV Backup Proxy.

7. Use the backed-up configuration of the old RHV backup proxy to restore the configuration settings to the new RHV backup proxy. For more information, see Restoring Configuration Data.

8. After the configuration settings are restored successfully and you ensure the new RHV backup proxy functions properly, remove the old RHV backup proxy from the RHV infrastructure. For more information on removing RHV VMs, see Red Hat Product Documentation.
Uninstalling RHV Plug-In

To uninstall RHV Plug-in, do the following:

1. Log in to the backup server using an account with the Local Administrator permissions.
2. Open the Start menu and click the Control Panel icon.
3. In the Settings window, navigate to System > Apps and Features.
4. In the program list, click Red Hat Virtualization Plug-in for Veeam Backup & Replication and click Uninstall.
5. In the opened window, click Remove.

Related Topics

- Removing RHV Backup Proxy
- Removing RHV Manager
Configuring Backup Infrastructure

To configure the backup infrastructure, you must set up backup repositories that will store RHV VM backups, connect the RHV manager that will provide the backup server with access to RHV resources, and add an RHV backup proxy that will process backup and restore operations.

In This Section

- Configuring Backup Repositories
- Connecting RHV Manager
- Managing RHV Backup Proxy
- Managing TLS Certificates
Configuring Backup Repositories

A backup repository is a storage location where Veeam Backup for RHV keeps backup files. By default, backups are stored on the backup server as it is assigned the role of a repository. To keep your backups on another storage location, you can configure the following types of repositories:

- **Direct attached storage**: Microsoft Windows and Linux virtual and physical machines.
- **Network attached storage**: CIFS (SMB) shares and NFS shares.
- **Deduplicating storage appliances**: ExaGrid, Quantum DXi, Dell EMC Data Domain, HPE StoreOnce.

To combine repositories of different types in one repository, you can also set up a scale-out backup repository.

To learn how to add backup repositories to the backup infrastructure, see the Veeam Backup & Replication User Guide, section Adding Backup Repositories.

**NOTE**

Mind the following limitations:

- **Veeam Cloud Connect** repositories are not supported for backups created by Veeam Backup for RHV.
- If you want to store RHV VM backups on a hardened repository, make sure that you enable creation of active full backups in the backup job settings and make sure that the backup job retention period is longer than the immutability period of the repository. Otherwise, the backup chain transformation will fail because merging of incremental backups into a full backup is not possible in hardened repositories.
Connecting RHV Manager

The RHV manager allows the backup server to access RHV resources such as VMs, hosts, clusters, storage domains and networks. After you connect the RHV manager to the backup infrastructure, you will be able to deploy an RHV backup proxy and to manage data protection tasks for RHV VMs in the Veeam Backup & Replication console.

In This Section

- Adding RHV Manager to Backup Infrastructure
- Editing RHV Manager Properties
- Rescanning RHV Manager
- Removing RHV Manager
Adding RHV Manager to Backup Infrastructure

To add the RHV manager to the backup infrastructure, do the following:

1. Launch the New Red Hat Virtualization Manager wizard.
2. Specify the RHV manager domain name or IP address.
3. Enter credentials to access the RHV manager.
4. Apply RHV manager settings.
5. Finish working with the wizard.
Step 1. Launch New Red Hat Virtualization Manager Wizard

To launch the **New Red Hat Virtualization Manager** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers**.
3. On the ribbon, click **Add Server**.
4. In the **Add Server** window, select **Red Hat Virtualization** to launch the New Red Hat Virtualization Manager wizard.
Step 2. Specify Domain Name or IP Address of RHV manager

At the **Name** step of the wizard, specify an address and description for the RHV manager:

1. In the **DNS name or IP address** field, enter the FQDN or IP address of the RHV manager.
2. In the **Description** field, provide a description for future reference. The field already contains a default description with information about the user who added the manager, date and time when the manager was added.

![New Red Hat Virtualization Manager](image)
Step 3. Enter Credentials

At the Credentials step of the wizard, specify an administrator account with the SuperUser role that is used to access the RHV manager. For more information on RHV system administrator roles, see Red Hat Product Documentation.

1. In the Credentials list, select the RHV manager administrator account.
   
   For an account to be displayed in the Credentials list, it must be added to Credentials Manager. To add an account, do the following:
   
   a. Click Add.
   
   b. In the Credentials window, enter a user name and password for the account.
      
      ▪ In the Username field, enter the name of a user account with administrative privileges and the name of the internal user domain in the following format: <username>@<local RHV user domain>, for example, admin@internal.
      
      For more information on RHV user domains, see Red Hat Product Documentation.
      
      ▪ In the Password field, enter the password for the account.
   
   c. Click OK.

2. Click Next.

The backup server will connect to the RHV manager and will check its TLS certificate. If the certificate is not installed on the backup server, the Certificate Security Alert Window will display a warning notifying that secure communication cannot be guaranteed. To allow the backup server to connect to the RHV manager using the certificate, click Continue. For more information on TLS certificate configuration, see Managing TLS Certificates.
Step 4. Apply Settings

At the **Apply** step of the wizard, wait until the RHV manager is added to the backup infrastructure and click **Next**.

![New Red Hat Virtualization Manager window](image)

Message: RHV Virtualization Manager pdcqa1@rovert.roborfish.local has been added. Duration: 0:00:10
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, check that the RHV manager is added. Then click **Finish** to exit the wizard.

![Summary Step of the Wizard](image)

After you finish the wizard, you will be asked to add an RHV backup proxy — you can confirm to proceed with the **New Red Hat Virtualization Proxy Wizard** immediately or start the wizard later as described in section **Managing RHV Backup Proxy**.
Editing RHV Manager Properties

To edit properties of the RHV manager added to the backup infrastructure, do the following:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select Managed Servers > Red Hat Virtualization.
3. In the working area, select the RHV manager and click Edit Manager on the ribbon, or right-click the RHV manager and select Properties.
4. Complete the Edit RHV manager wizard as described in section Adding RHV Manager to Backup Infrastructure.
Rescanning RHV Manager

Veeam Backup for RHV retrieves information about the protected RHV infrastructure from the RHV manager. If you make any changes to the RHV infrastructure and want both the Veeam Backup & Replication console and the RHV backup proxy web console to display the changes immediately, you can rescan the RHV manager manually.

To rescan the RHV manager, do the following:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers > Red Hat Virtualization**.
3. In the working area, select the RHV manager and click **Rescan** on the ribbon, or right-click the RHV manager and select **Rescan**.

Alternatively, in the RHV backup proxy web console, click the **Settings** icon at the top right corner of the RHV backup proxy web console, select **Manage Visualization Manager** and click **Rescan**.
Removing RHV Manager

If you do not want to protect resources managed by the connected RHV manager anymore, you can remove it from the backup infrastructure.

**IMPORTANT**
Before you remove the RHV manager, you must remove the RHV backup proxy that processes protection jobs for the RHV resources managed by the RHV manager.

To remove the RHV manager from the Veeam Backup & Replication infrastructure:

1. Open the **Backup Infrastructure** view.
2. In the inventory pane, select **Managed Servers > Red Hat Virtualization**.
3. In the working area, select the RHV manager and click **Remove Manager** on the ribbon, or right-click the RHV manager and select **Remove**.
Managing RHV Backup Proxy

To be able to back up VMs residing on hosts that are managed by the RHV manager, you must add to the backup infrastructure an RHV backup proxy that will process backup jobs and deliver backup traffic to backup repositories.

To add an RHV backup proxy, you can either deploy a new RHV backup proxy or connect an existing one.

**NOTE**

You can add only one RHV backup proxy to back up RHV VMs residing on hosts that are managed by one RHV manager.

In This Section

- Deploying New RHV Backup Proxy
- Connecting Existing RHV Backup Proxy
- Editing RHV Backup Proxy
- Enabling SSH on RHV Backup Proxy VM
- Rescanning RHV Backup Proxy
- Removing RHV Backup Proxy
Deploying New RHV Backup Proxy

To deploy an RHV backup proxy and to add it the backup infrastructure, do the following:

1. Launch the New Red Hat Virtualization Proxy wizard.
2. Select the proxy deployment mode.
3. Specify proxy VM configuration.
4. Specify proxy network settings.
5. Specify credentials for the proxy account.
6. Grant permissions to the proxy.
7. Apply proxy settings.
8. Finish working with wizard.
Step 1. Launch New Red Hat Virtualization Proxy Wizard

To launch the **New Red Hat Virtualization Proxy** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. In the inventory pane, select **Backup Proxies**.
3. On the ribbon, select **Add Proxy > Add RHV backup proxy**.
Step 2. Select Deployment Mode

At the **Deployment Mode** step, do the following:

1. Select the **Deploy a new proxy** option.
2. Click **Next**.
Step 3. Specify VM Configuration

At the Virtual Machine step of the wizard, do the following:

1. Click Choose to select an RHV cluster where the RHV backup proxy will be deployed.
2. At the Name field, specify a name for the RHV backup proxy.
3. Click Choose and select the storage domain where RHV backup proxy system files will be stored.
4. In the Proxy description field, provide a description for future reference. The field already contains a default description with information about the user who added the proxy, date and time when the proxy was added.
5. In the Max concurrent tasks field, specify the number of tasks that the RHV backup proxy will be able to handle in parallel. If this value is exceeded, the backup proxy will not start a new task until one of current tasks finishes.

   If you want to change the default value that is set to 4, consider RHV backup proxy system requirements and allocate additional resources to the VM:
   
   a. Click Advanced.
   
   b. In the Number of vCPU cores field of the Hardware Settings window, specify the number of virtual CPU cores that will be allocated to the RHV backup proxy.
   
   c. In the Memory size (GB) field, specify the memory size that will be allocated to the RHV backup proxy.
   
   d. Click OK to save the configuration.
6. Click Next.
NOTE

After you deploy the RHV backup proxy, you will be not able to change the number of vCPU cores and RAM allocated to the RHV backup proxy in the Veeam Backup & Replication console. However, you can change the VM hardware configuration in the RHV Administration Portal. For more information, see Red Hat Product Documentation.
Step 4. Specify Network Settings

At the **Networks** step of the wizard, do the following:

1. Click **Browse** to select a network adapter to which the proxy will be connected.

2. In the **Hostname** field, specify a hostname that will be assigned to the RHV backup proxy.
   
   The maximum length of the hostname is 63 characters; the - special character is only supported, however, you cannot use it as the first or the last character. Note that the hostname does not contain a domain name.

3. To set the RHV backup proxy IP address and the DNS servers manually, click **Configure** and do the following:
   
   a. In the **Network Settings** window, select the **Use the following IP address** option and specify the RHV backup proxy IP address, subnet mask and default gateway.

   b. Select the **Use the following DNS server address** option and specify the IP address of your DNS servers and domain names that the RHV backup proxy will use to resolve the hostnames of the backup server and the RHV manager.
      
      You can specify multiple domain names separated with commas.

   c. Click **OK**.

4. Click **Next**.
Step 5. Specify Credentials

At the **Credentials** step of the wizard, do the following:

1. In the **Credentials** list, select an account that will be created on the RHV backup proxy for accessing the web console.

   **IMPORTANT**
   
   Note that you must not use select an Active Directory account as the RHV backup proxy does not support LDAP integration.

   For an account to be displayed in the **Credentials** list, it must be added to **Credentials Manager**. To add an account, do the following:

   a. Click **Add**.

   b. In the **Credentials** window, specify a user name and password for the account.

      The user name must contain only letters and numbers and must not match the Linux system user names, such as *root*, *daemon*. The password must be at least 6 characters long.

   c. Click **OK**.

2. Click **Next**.
Step 6. Grant Permissions

At the **Access Permissions** step of the wizard, do the following:

- Select the option **Allow access to all backup repositories** if the RHV backup proxy will have access to all backup repositories added to the backup infrastructure.

- Select the option **Allow access to the following backup repositories** if the RHV backup proxy will have access to specified backup repositories only.

  If you select the **Allow access to the following backup repositories** option, you must also specify backup repositories to which the RHV backup proxy will have access.

**NOTE**

If you do not select any repositories, Veeam Backup for RHV will not be able to create backups. However, you still will be able to restore VMs from existing backups using the Veeam Backup & Replication console.
Step 7. Apply Settings

At the **Apply** step of the wizard, wait for the RHV backup proxy to be added to the backup infrastructure, then click **Next**.

**IMPORTANT**

If the wizard displays a warning notifying that the proxy hostname is not resolved, check your DNS server configuration, otherwise, backup and restore operations will fail.
Step 8. Finish Working with Wizard

At the Summary step of the wizard, review summary information and click Finish. To open the RHV backup proxy web console in your web browser, click Web Console.
Connecting Existing RHV Backup Proxy

If you have an already deployed RHV backup proxy that is not connected to the backup server, you can add it to the backup infrastructure. This can be necessary in the following scenarios:

- You want to re-connect an RHV backup proxy that was removed from the backup infrastructure.
- You want to connect an RHV backup proxy version 1.0 and upgrade it to version 2.0.
- You want to connect an RHV backup proxy that was previously connected to another backup server.

After you connect the RHV backup proxy, the backup server will retrieve information about all backup jobs the proxy has processed.

To add an existing RHV backup proxy to the backup infrastructure, do the following:

1. Launch the New Red Hat Virtualization Proxy wizard.
2. Select the proxy deployment mode.
3. Specify proxy VM configuration.
4. Check network settings.
5. Enter credentials for the proxy account.
6. Grant permissions to the proxy.
7. Apply proxy settings.
8. Finish working with wizard.
Step 1. Launch New Red Hat Virtualization Proxy Wizard

To launch the **New Red Hat Virtualization Proxy** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. In the inventory pane, select **Backup Proxies**.
3. On the ribbon, select **Add Proxy > Add RHV backup proxy**.
Step 2. Select Deployment Mode

At the **Deployment Mode** step, do the following:

1. Select the **Connect to an existing proxy** option.
2. Click **Next**.
Step 3. Specify VM Configuration

At the **Virtual Machine** step of the wizard, do the following:

1. Click **Choose** and select the RHV cluster where the RHV backup proxy is deployed.

2. Click **Choose** and select the name of the VM running as the RHV backup proxy.
   
The storage domain is automatically populated when you select the VM.

3. In the **Proxy description** field, provide a description for future reference. The field already contains a default description with information about the user who added the proxy, date and time when the proxy was added.

4. In the **Max concurrent tasks** field, specify the number of tasks that the RHV backup proxy will be able to handle in parallel. If this value is exceeded, the backup proxy will not start a new task until one of current tasks finishes.
   
   If you want to change the default value that is set to 4, consider resources allocated to the VM and RHV backup proxy system requirements.

   **IMPORTANT**

   When you connect a deployed RHV backup proxy, you cannot change the number of vCPU cores and RAM allocated to the RHV backup proxy. However, you can change VM hardware configuration in the RHV Administration Portal. For more information, see [Red Hat Product Documentation](https://www.redhat.com/).

5. Click **Next**.
Step 4. Check Network Settings

When you connect an existing RHV backup proxy, network settings are automatically obtained from the RHV backup proxy configuration data. At the **Networks** step of the wizard, view the obtained settings, then click **Next**.
Step 5. Enter Credentials

At the **Credentials** step of the wizard, do the following:

1. In the **Credentials** list, select the account that you use to access the RHV backup proxy web console.
   
   For an account to be displayed in the **Credentials** list, it must be added to **Credentials Manager**. To add an account, do the following:
   
   a. Click **Add**.
   
   b. In the **Credentials** window, specify the user name and password of the account.
   
   c. Click **OK**.

2. Click **Next**.
Step 6. Grant Permissions

At the Access Permissions step of the wizard, do the following:

- Select the option **Allow access to all backup repositories** if the RHV backup proxy will have access to all backup repositories added to the backup infrastructure.

- Select the option **Allow access to the following backup repositories** if the RHV backup proxy will have access to specified backup repositories only.

  If you select the **Allow access to the following backup repositories** option, you must also specify backup repositories to which the RHV backup proxy will have access.

**NOTE**

If you do not select any repositories, Veeam Backup for RHV will not be able to create backups. However, you still will be able to restore VMs from existing backups using the Veeam Backup & Replication console.
Step 7. Apply Settings

At the **Apply** step of the wizard, wait for the RHV backup proxy to be added to the backup infrastructure, then click **Next**.

**IMPORTANT**

If the wizard displays a warning notifying that the proxy hostname is not resolved, check your DNS server configuration, otherwise, backup and restore operations will fail.
Step 8. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**. To open the RHV backup proxy web console in your web browser, click **Web Console**.

![New Red Hat Virtualization Proxy](image)

**Summary**

You can copy the configuration information below for future reference.

- **Summary:**
  - Proxy has been registered successfully.
  - Virtualization manager: pdcqa189ovirt.robofish.local
  - Virtual machine: RHV-Backup-Proxy
  - Network options:
    - Hostname: RHVProxy
    - Network adapter: ovirtmgmt
    - IP Address: 172.23.16.113
    - DNS server: 172.23.16.41
  - Access permissions: All repositories

Additional proxy settings can be configured in **Web Console**.
Editing RHV Backup Proxy

You can edit settings of the RHV backup proxy that were specified while adding the proxy to the backup infrastructure.

To edit RHV backup proxy settings, do the following:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select the Backup Proxies node.
3. In the working area, select the RHV backup proxy and click Edit Proxy on the ribbon, or right-click the RHV backup proxy and select Properties.
4. Complete the Edit Red Hat Virtualization Proxy wizard as described in section Connecting Existing RHV Backup Proxy.

NOTE

If you change the number of maximum concurrent tasks in RHV backup proxy configuration, the hardware resources (number of vCPU cores and RAM) allocated to the RHV backup proxy VM will not change. However, you can change VM hardware configuration in the RHV Administration Portal. For more information, see Red Hat Product Documentation.
Enabling SSH on RHV Backup Proxy VM

For security reasons, SSH is disabled on the RHV backup proxy by default. However, you can enable it for manual management or troubleshooting purposes:

1. Log in to the Red Hat Virtualization Administration Portal.
2. In the main menu, navigate to Compute > Virtual Machines.
3. Select the VM where the RHV backup proxy is deployed.
4. Click Console on the toolbar to download a Virt Viewer VV file.
5. Launch the file to connect to the VM console.

**TIP**

If you have no application to open the file, click the arrow next to the Console button. In the Console options window, click Console Client to see the guidelines on how to get and install the Virt Viewer application.

6. Log in to the VM console using the credentials of the user account that you specified at the Specify Credentials step of the New Red Hat Virtualization Proxy wizard.
7. In the VM console, execute the following command:

```
sudo ufw allow ssh
```
Rescanning RHV Backup Proxy

If an RHV backup proxy becomes unavailable, you can rescan it to synchronize data between the RHV backup proxy and the backup server. The rescan operation will update current RHV backup proxy settings and backup job statistics on the backup server.

To rescan the RHV backup proxy, do the following:

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

You can remove an RHV backup proxy from the backup infrastructure if you want to replace it with another RHV backup proxy or to connect it to another backup server. When you remove the RHV backup proxy, information about backup jobs processed by the RHV backup proxy is deleted from the Veeam Backup & Replication database, and you cannot perform RHV VM backup and entire VM restore operations until a new RHV backup proxy is deployed. However, backup files are not deleted from your repositories, and you can use them, for example, for instant recovery or VM guest OS file restore operations.

To remove the RHV backup proxy, do the following:

1. Open the Backup Infrastructure view.
2. In the inventory pane, select the Backup Proxies node.
3. In the working area, select the RHV backup proxy and click Remove Proxy on the ribbon, or right-click the RHV backup proxy and select Remove.
4. In the Veeam Backup & Replication window, confirm that you want to remove the RHV backup proxy VM.

By default, Veeam Backup & Replication removes information about the RHV backup proxy and its jobs only from the Veeam Backup & Replication database. In this case, the RHV backup proxy will keep its configuration and information about backup jobs. This can be useful if you want to connect the RHV backup proxy to another backup server.
If you want to permanently delete the RHV backup proxy VM, select the **Permanently delete the proxy VM from the cluster and all of its backup jobs (Irreversible)** check box and click **Yes**.
Managing TLS Certificates

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

- You can choose to keep the default self-signed TLS certificate generated by the backup server.
- You can use Veeam Backup & Replication to generate a new self-signed TLS certificate. For more information, see Generating Self-Signed Certificates.
- You can select an existing TLS certificate from the certificates store. For more information, see Importing Certificates from Certificate Store.
- You can import a TLS certificate from a file in the PFX format. For more information, see Importing Certificates from PFX Files.

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

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

To generate TLS certificates, Veeam Backup & Replication employs the RSA Full cryptographic service provider by Microsoft Windows installed on the backup server. The created TLS certificate is saved to the *Shared* certificate store. The following types of users can access the generated TLS certificate:

- User who created the TLS certificate
- LocalSystem user account
- Local Administrators group

If you use a self-signed TLS certificate generated by Veeam Backup & Replication in case of initial RHV backup proxy deployment, you do not need to take any additional actions to deploy the TLS certificate on an RHV backup proxy VM. When you add an RHV backup proxy to the Veeam Backup & Replication infrastructure, a matching TLS certificate with a public key is installed on the RHV backup proxy VM. During discovery, Veeam Installer Service deployed on the RHV backup proxy VM retrieves the TLS certificate with a public key from the backup server and installs a TLS certificate with a public key on the RHV backup proxy VM.

If you currently work with the deployed RHV backup proxy and you try to re-generate self-signed TLS certificate, the connection with backup server will be lost and all subsequent backup jobs fail. In this case, you can manually re-apply settings for RHV backup proxy in the Veeam Backup & Replication console.

**NOTE**

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

To generate a self-signed TLS certificate:

1. From the main menu of the Veeam Backup & Replication console, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, select **Generate new certificate**.

5. At the **Generate Certificate** step of the wizard, specify a friendly name for the created self-signed TLS certificate.
6. At the **Summary** step of the wizard, review the certificate properties. Use the **Copy to clipboard** link to copy and save information about the generated TLS certificate. You will be able to use the copied information to verify the TLS certificate with the certificate thumbprint.

7. Click **Finish**. Veeam Backup & Replication will save the generated certificate in the *Shared* certificate store on the backup server.
Importing Certificates from Certificate Store

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

To select a certificate from the Microsoft Windows Certificate store:

1. From the main menu of the Veeam Backup & Replication console, select General Options.
2. Click the Security tab.
3. In the Security tab, click Install.
4. At the Certificate Type step of the wizard, choose Select certificate from the Certificate Store.

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep existing certificate</td>
<td>Keep the current certificate intact</td>
</tr>
<tr>
<td>Generate new certificate</td>
<td>Generate a new self-signed certificate that is verifiable with the thumbprint</td>
</tr>
<tr>
<td>Select certificate from the Certificate Store</td>
<td>Use an existing certificate already present in the local Certificate Store of this server</td>
</tr>
<tr>
<td>Import certificate from a file</td>
<td>Select this option to import certificate from PFX file. The certificate will be automatically imported into the local Certificate Store of this server</td>
</tr>
</tbody>
</table>
5. At the **Pick Certificate** step of the wizard, select a TLS certificate that you want to use. You can select only certificates that contain both a public key and a private key. Certificates without private keys are not displayed in the list.

![Manage Certificate Window](image)

6. At the **Summary** step of the wizard, review the certificate properties.

7. Click **Finish** to apply the certificate.
Importing Certificates from PFX Files

You can import a TLS certificate in the following situations:

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

**IMPORTANT**

The TLS certificate must pass validation on the backup server. Otherwise, you will not be able to import the TLS certificate.

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

1. From the main menu of the Veeam Backup & Replication console, select **General Options**.
2. Click the **Security** tab.
3. In the **Security** tab, click **Install**.
4. At the **Certificate Type** step of the wizard, choose **Import certificate from a file**.
5. At the **Import Certificate** step of the wizard, specify a path to the PFX file.
6. If the PFX file is protected with a password, specify the password in the field below.

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

8. Click **Finish** to apply the certificate.
Using Certificate Signed by Internal CA

To establish a secure connection with the RHV backup proxy VM, the backup server uses a TLS certificate. By default, the backup server uses a self-signed certificate. The backup server generates this certificate when you install Veeam Backup & Replication on the machine.

**IMPORTANT**

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

- The backup server must trust the CA. That means that the Certification Authority certificate must be added to the Trusted Root Certification Authority store on the backup server.
- Certificate Revocation List (CRL) must be accessible from the backup server.
- When issuing the certificate, make sure the Subject Alternative Name field contains both the FQDN and the NetBIOS name. You can add multiple DNS entries in the following format: DNS:vbrserver.domain.local, DNS:vbrserver.

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

- The certificate subject must be equal to the fully qualified domain name of the backup server. For example: vbrserver.domain.local.

- The minimum key size is 2048 bits.

- The following key usage extensions must be enabled in the certificate to sign and deploy child certificates for the RHV backup proxy VM:
  - Digital Signature
  - Certificate Signing
  - Off-line CRL Signing
○ CRL Signing (86)

If you use Windows Server Certification Authority, we recommend you to issue a backup server certificate based on the built-in "Subordinate Certification Authority" template or templates similar to it.

- The key type in the certificate must be set to Exchange.

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

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

In the Key Type section, select Exchange.

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

### Reconnecting to RHV backup proxy

After you specify the signed certificate on the backup server, the RHV backup proxy is not able to communicate with the backup server and backup jobs fail. To reconnect the backup server to the RHV backup proxy, do the following:

1. In the Veeam Backup & Replication console, open the Backup Infrastructure view.
2. In the inventory pane, select the Backup Proxies node.
3. In the working area, select the RHV backup proxy and click Edit Proxy on the ribbon, or right-click the RHV backup proxy and select Properties.
4. Complete the **Edit Red Hat Virtualization Proxy** wizard as described in section **Connecting Existing RHV Backup Proxy**.
Accessing Web Console

To log in to the web console of the RHV backup proxy, do the following:

1. In the Veeam Backup & Replication console, open the **Backup Infrastructure** view.
2. In the inventory pane, select **Backup Proxies**.
3. In the working area, select the RHV backup proxy and click **Open Web Console** on the ribbon, or right-click the RHV backup proxy and select **Open Web Console**.

Alternatively, you can navigate to the IP address or hostname of the RHV backup proxy in a web browser.

4. On the welcome screen, enter credentials of the administrator account that you have specified in the **RHV backup proxy configuration**.
TIP
If you do not remember the password, you can reset it running the RHV backup proxy recovery mode. For more information, see this Veeam KB article.
Configuring General Settings

The RHV backup proxy allows you to perform the following administrative tasks:

- Edit network settings.
- Edit the Administrator account.
- Select the time zone and configure time synchronization settings.
- Enable notifications.
- Configure email settings.
- Back up configuration settings.
- Restore configuration settings.
- Reboot or shut down the appliance.
- Export logs.
Configuring Network Settings

To change network settings of the RHV backup proxy, do the following:

1. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.

2. On the **Network** tab, configure network settings or select the appropriate check boxes to obtain IP address and DNS server address automatically.

   **NOTE**
   If you specify a new DNS server, make sure it resolves the domain name of the RHV backup proxy.

3. Click **Apply**.
Configuring Administrator Account

To change the user name and password of the administrator account that you use to access the RHV backup proxy web console, do the following:

1. Click the Settings icon at the top right corner of the RHV backup proxy web console and select Appliance Settings.
2. Click the Security tab.
3. In the Login field, enter the user name. If you specify a new user name, mind the following requirements:
   - The name must contain only letters and numbers.
   - The user name must not match the Linux system user accounts, such as root, daemon and so on.
4. In the Old password field, enter the current password for the administrator account.
5. In the New password field, assign a new password for the administrator account. The password must be at least 6 characters long.
6. In the Confirm new password field, enter the new password again.
7. Click Apply to save the settings. The web console updates the user name automatically.

**IMPORTANT**

If you change the administrator account credentials, you must also update the credentials in the RHV backup proxy configuration in the Veeam Backup & Replication console..
Configuring Time Zone Settings

Veeam Backup for RHV performs all data protection and disaster recovery operations according to the time zone set on the RHV backup proxy. By default, the time zone is set to Coordinated Universal Time (UTC), however, you can change it if required. For example, you may want the time on the backup appliance to match the time on the workstation from which you access RHV backup proxy.

**NOTE**

When you change the time zone, the RHV backup proxy does not adjust the starting time of already scheduled jobs.

To edit time zone settings, do the following:

1. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.
2. Click the **Time zone** tab and then click **Settings**.
3. In the **Select the time zone** list, choose the necessary time zone.
4. Specify the synchronization mode:
   - **NTP**: Time of the proxy will be synchronized with the specified NTP servers.
   - **Host**: Time of the proxy will be synchronized with the time on guest OS of the host where the proxy is installed.
5. [For NTP mode] Specify required NTP servers in the **NTP Servers** text field.
Updating RHV Backup Proxy

By default, RHV backup proxy allows you to check for new product versions and available package updates, download and install them from the web console. The RHV backup proxy automatically checks for available updates and notifies you about them with a red dot on the bell icon at the top-right of the web console.

**IMPORTANT**
Before you install updates for the RHV backup proxy, make sure all required ports are open. For more information, see Used Ports.

To check and install updates, do the following:

1. Open the **Veeam Updater** portal:
   a. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.
   b. On the **Updates** tab, click **Check and view updates**.

2. In the **Updates are available for this system** section, select packages that you want to install.

3. In the **Choose action** section, you can select whether you want to install updates now or schedule the installation at the specified time and date:
   - **Install updates now**: select this option if you want to install the updates immediately.
     **IMPORTANT**
     If you start the update while backup or restore processes are running, these backup or restore sessions will be interrupted and finished with an error.
   - **Schedule updates installation**: select this option if you want to install the updates at the specified date and time.
     For this option, specify the date and time when updates must be installed. Make sure backup jobs are not scheduled to run on the specified date at the specified time. Otherwise, the update process will interrupt running activities, which may result in data loss.
   - **Remind me later**: if you have not decided when to install updates, you can set an update reminder for the next day or next Monday.

4. After you install the updates, you must reboot the RHV backup proxy. You can select the **Reboot automatically after install if required** check box if you want to reboot the proxy automatically. Otherwise, reboot the RHV backup proxy manually. For more information, see Rebooting or Shutting Down VM.
5. Depending on the option you have chosen, click the **Install Updates Now**, **Schedule Updates Installation** or **Remind me later** button.
Configuring E-mail Settings

You can configure email settings to receive email notifications. The RHV backup proxy sends the following notifications:

- Backup jobs results.
- Availability of RHV backup proxy updates.
- RHV backup proxy security updates installation results.
- Configuration database backups results.

To configure notification settings, do the following:

1. Click the Settings icon at the top right corner of the RHV backup proxy web console and select Appliance Settings.
2. On the E-mail settings tab, select the Enable e-mail notifications check box.
3. In the SMTP server field, enter the full DNS name or IP address of the SMTP server that will be used for sending email notifications.
4. Click the Advanced button to specify SMTP settings.
   a. Specify the port number for the SMTP server.
   b. To use a secure connection for email operations, select the Connect using SSL check box.
c. If you need to connect to the SMTP server using a specific account, select the **This SMTP server requires authentication** check box and specify credentials that will be used to connect to the SMTP server.

5. In the **From** field, specify an email address from which email notifications must be sent.

7. In the **To** field, specify the recipient addresses. Use a semicolon to separate multiple addresses. Recipients specified in this field will receive notification about every job managed by the backup server.

8. In the **Subject** field, specify a subject for the sent message. You can use the following variables:
   
   - %JobName% – name of the job.
   - %JobResult% – status with which the job has finished.
   - %ObjectCount% – number of objects in the job.

9. Select the **Notify on success**, **Notify on warning** and (or) **Notify on failure** check boxes to receive email notification if a job was completed successfully, not successfully or with a warning.

10. Select the **Suppress notifications until the last retry** check box to receive a notification about the final job status. If you do not enable this option, the RHV backup proxy will send one notification per every job retry.

11. To send a test email, click **Test Message**. The RHV backup proxy will send a test email to check if all settings have been configured correctly.

12. Click **Apply** to finish configuration.
Configuring Notifications

If you want to receive notifications of available product updates or low storage space on backup repositories, you can enable notifications at the **Notifications** tab. Note that to receive email notifications, you must configure **E-mail settings** beforehand.

To enable notifications, do the following:

1. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.
2. On the **Notifications** tab, select notifications you want to receive.
3. Click **Apply**.

![Image of the RHV backup proxy web console showing the Notifications tab with options to enable updates and low storage space notifications.]
Performing Configuration Backup

You can back up the configuration database of the RHV backup proxy. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead if any problem with the backup servers occurs. The RHV backup proxy retrieves data from the configuration database, writes this data into a set of JSON and DAT files and archives them to a ZIP file. The default naming scheme for the configuration backup file is `config_<hostname>_DD_MM_YYYY_HH_MM_SS.zip`.

The RHV backup proxy backs up information about the following objects:

- backups created by the RHV backup proxy
- backup jobs created by the RHV backup proxy
- events performed by job sessions and configuration changes
- RHV backup proxy appliance settings

To back up configuration settings of the RHV backup proxy, do the following:

1. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.
2. On the **Summary** tab, click **Config Backup**.
3. In the **Configuration Backup** window:
   a. Select items that you want to back up:
      - **Common**: configuration settings, added RHV hosts, backup servers, backup jobs, and so on.
      - **Events**: list of events and event details.
   b. In the **Protect passwords in exported files** field, specify a password that will be used to encrypt saved files.
   c. In the **Password hint** field, specify a reminder that will help you remember your password if you forgot it.
d. Click **Download**. A configuration backup file will be downloaded to your machine.

![Configuration Backup](image)

**Related Topic**

*Restoring Configuration Data*
Restoring Configuration Data

You can restore the configuration database of the RHV backup proxy, which can be helpful in the following situations:

- The configuration database got corrupted, and you want to recover data from a configuration backup.
- You want to roll back the configuration database to a specific point in time.
- You deployed a new RHV backup proxy and want to apply the configuration from the old proxy configuration backup.

To restore the configuration database, do the following:

1. Click the Settings icon at the top right corner of the RHV backup proxy web console and select Appliance Settings.
2. On the Summary tab, click Configuration Restore to launch the Configuration Restore wizard.
3. At the **Configuration File** step of the wizard, browse to the necessary backup file and provide a password that was used to encrypt the file when backing up the configuration.

![Configuration File](image)

4. At the **Network Settings** step of the wizard, choose whether you want to use the existing network settings saved in the backed-up configuration or to configure new network settings for the restored configuration.
**IMPORTANT**
If you change the RHV backup proxy network settings, you must update the RHV backup proxy configuration in the Veeam Backup & Replication console.

<table>
<thead>
<tr>
<th>Network Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance host name:</td>
</tr>
<tr>
<td>IP address:</td>
</tr>
<tr>
<td>Subnet mask:</td>
</tr>
<tr>
<td>Default gateway:</td>
</tr>
<tr>
<td>Obtain DNS server address automatically</td>
</tr>
<tr>
<td>Prefered DNS server:</td>
</tr>
<tr>
<td>Second DNS server:</td>
</tr>
<tr>
<td>Search domains</td>
</tr>
<tr>
<td>(separated by comma, each search domain name should comply with RFC1123)</td>
</tr>
</tbody>
</table>
5. At the **Summary** step of the wizard, review the configured settings and click **Finish** to start the restore process.

### Related Topic

**Performing Configuration Backup**
Rebooting or Shutting Down VM

To reboot or shut down the RHV backup proxy VM, do the following:

1. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.

2. On the **Summary** tab, click **Reboot** or **Shutdown**.

![Appliance Settings Screen](image-url)
Performing Data Protection Operations

With Veeam Backup for RHV, you can perform the following data protection tasks:

- Create backups of RHV VMs.
- Copy backups to secondary location.
- Copy backups to tape devices.
- Start, stop, edit, delete or disable jobs.
- Import, export or delete backups.
Backup Jobs

The RHV backup proxy creates image-level backups of VMs. The RHV backup proxy retrieves VM data from the RHV host at a block level, compresses and deduplicates it, and then forwards it to a backup repository in the Veeam proprietary format. You can use image-level backups to restore VMs and VM files.

Veeam Backup & Replication does not install agent software inside the VM guest OS to retrieve VM data. To back up VMs, it leverages RHV checkpoint capabilities. Backup is a job-driven process. To perform a backup, you need to configure a backup job. Backup job is a configuration unit with which you can specify VMs that you want to back up, select a backup repository, define schedule and other backup settings.

In This Section

- Backup Chain and Retention Policy
- Creating Backup Jobs
- Creating Active Full Backup
How Backup Works

When you launch a backup job in the RHV backup proxy web console, the following happens:

1. The web console sends the backup job configuration data to the RHV backup proxy.
2. The RHV backup proxy starts the backup job and forwards the backup session data to the backup server.
3. The RHV backup proxy connects to the RHV host over REST API and creates a checkpoint of all VMs added to the job.
4. The RHV backup proxy creates a volume group on the RHV cluster, mounts VM disks through iSCSI and retrieves the VM data on the block level.
5. The Veeam Data Mover service compresses and deduplicates the VM data and forwards it to the target backup repository in the native Veeam format.

Related Topics

- Backup Infrastructure Components
- Creating Backup Jobs

Backup Chain and Retention Policy

For backups of RHV VMs, RHV backup proxy implements the forever forward incremental and forward incremental backup methods. For more information, see the Veeam Backup & Replication User Guide, section Backup Methods.

To back up RHV VMs, you must configure a backup job in the RHV backup proxy web console.

During the first backup session, the RHV backup proxy copies the whole content of the VM and creates a full backup file (VBK) in the repository. The full backup file acts as a starting point of the backup chain.
During the second and further backup sessions, the RHV backup proxy copies only those data blocks that have changed since the previous backup session. Changed data blocks are stored as an incremental backup file in the repository. Incremental backup files depend on the full backup file and preceding incremental backup files of the backup chain. In the backup job settings, you can also enable periodic creation of active full backups.

One backup job can be used to process one or several VMs. The RHV backup proxy creates per-VM backup chains: one backup chain contains data for one VM only. Even if you add several VMs to the backup job, the RHV backup proxy creates several backup chains on the backup repository, one per each VM processed by the job.

You can instruct the RHV backup proxy to run jobs automatically according to a specified schedule or you can start them manually.

Backup jobs and backup files created by the RHV backup proxy are visible in the Veeam Backup & Replication console. However, some of the Veeam Backup & Replication functionality is not available for backups of RHV VMs. For more information, see Backup Job Limitations.

### Changed Block Tracking (CBT)

When the RHV backup proxy performs incremental backup, it needs to know what data blocks have changed since the previous job session. To get the list of changed data blocks, the RHV backup proxy uses the RHV changed block tracking mechanism (CBT). CBT increases the speed and efficiency of incremental backups.

RHV CBT uses REST API to determine the changed metadata regions on RHV virtual disks. CBT compares two checkpoints: a checkpoint of the current virtual disks environment with the checkpoint that was obtained during the previous backup. Only the changed metadata regions that the API detects are backed up and written to the backup repository. After the backup completes, the current checkpoint will become the previous checkpoint for comparison in the next backup operation. Only one snapshot per VM will be retained for comparison.

### Retention Policy

Every successful backup job session creates a new restore point that lets you roll back VM data to an earlier point in time. To control the number of restore points in the backup chain, you must specify retention policy settings. The retention policy defines how many restore points you want to retain on disk and thus how ‘far’ you are able to roll back. After the allowed number of restore points is exceeded, the RHV backup proxy automatically removes the earliest restore point from the backup chain.

To define the retention policy for a backup job, you must specify the necessary number of restore points in the Restore points to keep field in the backup job settings. By default, Veeam Backup for RHV keeps 7 restore points. In the Schedule step of the New Job wizard you can select the following units of retention policy.

For more information on the retention policy for RHV VM backups, see the Forward Incremental Backup Retention Policy section of the Veeam Backup & Replication User Guide.

### Active Full Backup

In some cases, you need to regularly create full backups. For example, your corporate backup policy may require that you create a full backup on weekend and run incremental backup on work days. To let you conform to these requirements, Veeam Backup for RHV lets you create active full backups.

The active full backup produces a full backup of a VM, just as if you run the backup job for the first time. The RHV backup proxy retrieves data for the whole VM from the source, compresses and deduplicates it and stores it to the full backup file — VBK.

The active full backup resets a backup chain. All incremental backup files use the latest active full backup file as a new starting point. A previously used full backup file remains on disk until it is automatically deleted according to the retention policy.
You can create active full backups manually or schedule a backup job to create active full backups periodically.

- To create an active full backup manually, see Creating Active Full Backup.
- To schedule active full backups, specify scheduling settings in the Advanced section of a backup job. You can schedule active full backups to run weekly, for example, every Saturday, or monthly, for example, every fourth Sunday of a month. For more information, see Specify Repository.

**Related Topics**

Creating Backup Jobs

**Enabling Incremental Backup**

Veeam Backup for RHV can perform incremental backup of a virtual disk if the following requirements are met:

- The disk is formatted in QCOW2 format.
- The Enable Incremental Backup option is enabled in disk configuration.

For new disks, you must manually select the Enable Incremental Backup check box in the New Virtual Disk window. This will result in creating a disk in QCOW2 format. For more information on virtual disk creation, see Red Hat Product Documentation.

For existing disks in QCOW2 format, the RHV backup proxy enables the option automatically when you start a backup job.

**NOTE**

If the RHV backup proxy fails to enable the option, you will see the warning: "Unable to enable ovirt incremental backups for disk. Full scan backups will be performed". Follow the Veeam KB article to resolve the issue.

For existing disks in RAW format, you can take a snapshot of your VM — this will generate a QCOW2 layer on top of RAW formatted disks and enable the Enable Incremental Backup option. You will be able to perform incremental backup for these disks until you delete the snapshot. Alternatively, you can back up the VM and restore the VM using the Restore all VM disks to QCOW2 format option at the Restore Mode step of the Full VM Restore to Red Hat Virtualization wizard.
Creating Backup Jobs

To back up VMs, configure a backup job. Backup job defines the VMs that will be protected, repository where the backup file will be stored, the job schedule and other settings.

To create a backup job, do the following:

1. Check prerequisites and limitations.
2. Launch the New Job wizard.
4. Select VMs to backup.
5. Specify the backup repository where backups will be stored.
6. Define the job schedule.
7. Finish working with the wizard.

Before You Begin

Before you create a backup job, check the following prerequisites and limitations.

Prerequisites

- A backup repository where you want to store backup files must be added to the backup infrastructure.
- A backup repository where you want to store backup files must have enough space to store the files.
- The RHV backup proxy must have access to the backup repository. If the repository is unavailable, check permissions in the RHV backup proxy settings.
- The hostnames of the RHV manager and all RHV hosts must be resolved on the RHV backup proxy.

Backup Job Functionality Limitations

- You can back up each VM with one backup job at a time. If a VM is already being processed by a backup job, another backup job will not start backing up the same VM until the current backup operation completes.
- You cannot back up a VM being restored. Wait for the restore process to complete, and then start the backup job.
- You cannot include into a backup job a VM being backed up by a 3rd party software or an RHV backup proxy connected to another backup server. Wait for the backup process to complete or stop the backup operation manually.
- You cannot include a VM into a backup job if the VM last backup has failed. This limitation applies to backup operations performed by a 3rd party software or by an RHV backup proxy that is connected to another backup server. To resolve the issue, you must manually disable the job that is currently processing the VM. If you cannot disable the job, submit a support case in the Veeam Customer Support Portal.
- You cannot back up hosted-engine VMs, however, you can create oVirt configuration backup. For more information, see oVirt Developer Documentation.
• You cannot back up a VM in the snapshot preview mode. For more information on snapshot previews, see Red Hat Product Documentation.

• You cannot power on, power off or reboot a VM being backed up. Wait for the backup process to complete or stop the job manually, and then change the VM power state.

  If you need to change the power state of a VM while a backup operation is still running, you can send a REST API request, however, this will cause backup job failure. For more information on REST API requests, see Red Hat Product Documentation.

• Only full backups are created for virtual disks in RAW format attached to a VM. For more information, see Enabling Incremental Backup.

• You cannot disable deduplication and compression of backups. Veeam Backup for RHV applies the following settings that cannot be changed:
  o Data compression level: Optimal
  o Storage optimization: Local target (1024 KB block size)

  For more information on the data compression level and storage optimization settings, see the Veeam Backup & Replication User Guide, section Data Compression and Deduplication.

• You cannot enable encryption for a backup job, however, you can configure encryption parameters for backup repositories that you use to store RHV VM backups. For more information, see the Veeam Backup & Replication User Guide, section Access Permissions.

• If you connect an RHV backup proxy to another backup server, records about backups are removed from the RHV backup proxy configuration. However, backup up files are not deleted from repositories.

  If the backup server configuration contains records about RHV VM backups, you can import backups to the RHV backup proxy configuration.

Backup Chain Limitations

• The RHV backup proxy creates per-VM backup chains: one backup chain contains data for one VM only. Even if you add several VMs to a backup job, the RHV backup proxy creates several backup chains on the backup repository, one per each VM processed by the job.

• If a VM has an active backup chain and at some point the UUID of the VM changes (for example, due to migration to another cluster), the RHV backup proxy will become unable to continue the old backup chain for this VM. However, you can still use backups from the old backup chain for restore operations. Note that you can re-add this VM to the backup job, and the RHV backup proxy will create a new backup chain for the VM with a new UUID.

Backup Files and Jobs in Veeam Backup & Replication Console

You can view jobs and backups created by the RHV backup proxy in the Veeam Backup & Replication console. However, if you choose an option to create or edit a backup job in the Veeam Backup & Replication console, you will be redirected to the RHV backup proxy web console.

Launch New Job Wizard

To launch the New Job wizard, do the following:

1. In the Veeam Backup & Replication console, open the Home view.
2. In the inventory pane, select Jobs and navigate to Backup > Red Hat Virtualization.

The RHV backup proxy web console will be opened in your browser to start the New Job wizard.

TIP
You can also launch the New Job wizard using the RHV backup proxy web console. To do that, log in to the web console, switch to the Jobs page and click Add.
Step 1. Specify General Settings

At the **General Settings** step of the wizard, specify a name and description for the job:

1. In the **Job Name** field, enter a name for the backup job.

2. In the **Description** field, provide a description for future reference. The field already contains a default description with information about the user who created the job, date and time when the job was created.
Step 2. Select VMs to Back Up

At the **Virtual Machines** step of the wizard, specify VMs that you want to back up.

1. Click **Add**.

2. In the **Add Objects** window, do the following:
   a. Choose one of the following views:
      - **VM** — displays a list of VM names. In the VM view, you select VMs individually.
- **TAG** — displays a list of tags that are used to arrange VMs into groups. In the TAG view, you select groups of VMs with the same tag. For a tag to be displayed in the list, it must be created in the RHV Administration Portal and assigned to a VM. For more information on RHV tags, see Red Hat Product Documentation.

3. **[This step applies only if you have switched to the TAG view]**

To exclude specific VMs from the backup job, do the following:

a. Click **Exclusions**.
b. In the **VMs** window, specify a full name of a VM you want to exclude or a mask to filter VMs which will be excluded from the backup job.

![Image of VMs window with Exclusions dialog]

4. To exclude specific VM disks from the backup job, do the following:
   a. Click **Exclusions**.
b. Select a VM and click **Edit**.
c. In the **Select Disks** window, select **Selected disks** and click **Add**.

   ![Select Disks Window](image)

   **Select Disks** window with options to select disks and a button to add them.

   - **Disks to process:**
     - **All disks**
     - **Selected disks:**
       - **Add**

   ![Add Disks Window](image)

   **Add Disks** window with options to select a bus type and disks for backup.

   d. In the **Add Disks** window, select a bus type that you want to include and select the disks that you want to back up, not the disks that you want to exclude.

   ![Add Disks Window](image)

   **Add Disks** window with options to select a bus type and disks for backup.
**IMPORTANT**

Disks that you do not select will be excluded from the backup job.
Step 3. Specify Repository

At the **Backup Destination** step of the wizard, do the following:

1. In the **Backup repository** list, select a backup repository where you want to store backups. The wizard only displays the repositories that are managed by the backup server.

2. In the **Restore Points to keep** field, specify the number of restore points that you want to keep.

   When this number is exceeded, the earliest restore point will be removed from the backup chain. For more information on the retention policy for VM backups, see the Veeam Backup & Replication User Guide, section **Forward Incremental Backup Retention Policy**.

**NOTE**

You can select only the repositories to which the RHV backup proxy has access.
3. Click **Advanced** to configure the retention policy for backups that are no longer included into the backup job and specify how often you want to create backups:

   a. In the **Advanced Settings > Maintenance** window, select the **Remove deleted VMs data after** check box and specify the number of days.

   ![Advanced Settings window]

   b. In the **Advanced Settings > Backup** window, select the **Run active full backup periodically** check box to create full backups regularly. Choose one of the following options:

   - **Weekly on selected days**: the RHV backup proxy creates an active full backup every week on selected days. Use the drop-down list to select the required week days.

   - **Monthly on**: the RHV backup proxy creates an active full backup on selected days of selected months. Use drop-down lists to select required days and months. For example: every first Monday of all months. By default, all months are selected.

   **NOTE**

   Before scheduling periodic full backups, make sure that you have enough free space on the backup repository. Alternatively, you can create active full backups manually when needed. For more information, see **Creating Active Full Backup**.

   ![Advanced Settings window]
Step 4. Define Job Schedule

At the Schedule step of the wizard, do the following:

1. Select the **Run the job automatically** check box. If you do not select this check box, you will have to start the job manually.

2. Configure scheduling options for the job:
   - To run the job at specific time daily or on specific week days, select **Daily at this time**.
   - To run the job once a month on specific days, select **Monthly at this time**.
   - To run the job repeatedly throughout a day with a specific time interval, select **Periodically every**.

For more information on scheduling options, see the Veeam Backup & Replication User Guide, sections **Backup Job Scheduling**.

3. Select the **Automatic Retry** check box to define whether the RHV backup proxy must attempt to run the job again if the job fails. Specify the number of retry attempts and the period of time between the attempts. During a job retry, the RHV backup proxy processes failed VMs only.
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

**TIP**

If you want to start the job right after you finish working with the wizard, select the **Run job when I click Finish** check box.
Creating Active Full Backup

When you run an active full backup process, the RHV backup proxy creates a new full backup file and adds it to the backup chain. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain in the backup repository until it is removed from the backup chain according to the retention policy.

To perform an active full backup, do the following:

1. Switch to the Jobs page.
2. Select the required backup job and click Active Full on the toolbar.
3. Click Yes to confirm the action and run the active full backup process for the selected job.
Backup Copy Jobs

To build a successful data protection and disaster recovery plan, you can follow the 3-2-1 rule:

- Store at least 3 copies of your data: the original production data and two backups.
- Use at least 2 different types of media to store the copies of your data (local disk and cloud).
- Keep at least 1 backup offsite (in the cloud or in a remote site).

Thus, you must have at least two backups and they must be in different locations. If a disaster takes out your production data and local backup, you can still recover from your offsite backup.

To help you adopt the 3-2-1 rule, Veeam Backup & Replication offers the backup copy functionality. Backup copy allows you to create several instances of the same backup data in different locations, whether onsite or offsite. Backup copies have the same format as those created by backup jobs and you can recover your data from them when you need it.

Backup copy is a job-driven process. Veeam Backup & Replication fully automates the backup copy process and lets you specify retention settings to maintain the desired number of restore points, as well as full backups for archival purposes.

Creating Backup Copy Jobs

To learn how to create a backup copy job, see the Creating Backup Copy Jobs section of the Veeam Backup & Replication User Guide.

NOTE
The Immediate Copy mode is not supported for backups created with Veeam Backup for RHV.
Backup to Tape Jobs

Veeam Backup & Replication allows you to automate the process of copying RHV VM backups to tape devices and lets you specify scheduling, archiving and media automation options. For more information on tape jobs, see the Veeam Backup & Replication User Guide, section How Machines Backup to Tape Works.

In the Veeam Backup & Replication console, you can copy your backups to a tape device. Before you can create backup to tape jobs, you must add the target tape server to the backup infrastructure, create media pools, and configure media vaults. For more information, see one of the following sections of the Veeam Backup & Replication User Guide:

- Supported Devices and Configuration
- Tape Devices Deployment
- Machines Backup to Tape
Managing Backup Jobs

You can perform the following operations with backup jobs:

- Start and stop backup jobs manually.
- Edit backup job settings.
- Enable and disable backup jobs.
- Delete backup jobs.
Starting and Stopping Backup Jobs

You can start a backup job manually, for example, if you want to create an additional restore point and do not want to modify the configured job schedule. You can also stop a backup job if processing of an RHV VM is about to take too long, and you do not want the job to have an impact on the production environment during business hours.

**NOTE**
- When you start a job manually, Veeam Backup for RHV creates an incremental backup of all VMs added to the job. If it is the first session of the job, Veeam Backup for RHV creates a full backup.
- When you stop a running job, Veeam Backup for RHV creates a new restore point only for those VMs that have already been processed by the time you stop the job.

To start or stop a backup job:

1. Open the **Home** view.
2. In the inventory pane, select **Jobs > Backup**.
3. In the working area, select the job and click **Start** or **Stop** on the ribbon, or right-click the job and select **Start** or **Stop**.

**TIP**
You can also start or stop a backup job using the RHV backup proxy web console. To do that, log in to the **web console**, switch to the **Jobs** page, select the job and click **Start** or **Stop**.
Editing Backup Job Settings

For each backup job, you can modify settings configured while creating the job. For example, you can change the specified schedule or add more VMs to the job.

To edit backup job settings, do the following:

1. In the Veeam Backup & Replication console, open the Home view.
2. In the inventory pane, select Jobs > Backup.
3. In the working area, select the job and click Edit on the ribbon, or right-click the job and select Edit.
4. Complete the Edit Job wizard in the RHV backup proxy web console as described in section Creating Backup Jobs..

TIP
You can also change backup job settings using the RHV backup proxy web console. To do that, log in to the web console, switch to the Jobs page, select the job and click Edit. Then, complete the Edit Job wizard as described in Creating Backup Jobs.
Enabling and Disabling Backup Jobs

By default, all created backup jobs run according to the specified schedules. However, you can temporarily disable a job so that it does not run automatically. You will still be able to manually start or enable the disabled job at any time you need.

To enable or disable a backup job:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Jobs > Backup**.
3. In the working area, select the job and click **Enable** or **Disable** on the ribbon, or right-click the job and select **Enable** or **Disable**.

**TIP**

You can also enable or disable a backup job using the RHV backup proxy web console. To do that, **log in to the web console**, switch to the **Jobs** page, select the job and click **Enable** or **Disable**.
Deleting Backup Jobs

You can permanently delete a backup job from the Veeam Backup for RHV and from the configuration database if you no longer need it. When you delete a job, backup files created by the job are not deleted. The backup files remain in the repository and will be tagged as imported. If you want to delete the backup files as well, follow the instructions provided in section Managing Backups.

To delete a backup job, do the following:

1. In the Veeam Backup & Replication console, open the Home view.
2. In the inventory pane, select Jobs > Backup.
3. In the working area, select the job and click Delete on the ribbon, or right-click the job and select Delete.

TIP

You can also delete a backup job using the RHV backup proxy web console. To do that, log in to the web console, switch to the Jobs page, select the job and click Delete.
Managing Backups

You can perform the following operations with backups:

- **View backup properties** — see detailed information on created backups.
- **Import backups** — import RHV VM backups created by another RHV backup proxy to the current RHV backup proxy.
- **Export backups** — synthesize a complete and independent full backup file out of selected restore points that are located in your backup repositories.
- **Delete backups** — delete records about backups from the Veeam Backup & Replication configuration database and delete backup files from the backup repository.
Viewing Backup Properties

After a backup job successfully creates a restore point of an RHV VM, Veeam Backup for RHV adds summary information on the restore point to backup properties. Each backup is represented with a set of properties, such as:

- **Objects** – VMs added to the backup and their size.
- **Restore Points** – the date and type of restore points created for the VM.
- **Files** – the backup files created for restore points:
  - **Name** – the name and type of a backup file created for a restore point.
  - **Data Size** – the original size of the backed-up data.
  - **Backup Size** – the size of the backup file.
  - **Deduplication** – the ratio of data deduplication.
  - **Compression** – the ratio of data compression.
  - **Date** – the date of backup file created for a restore point.

To view summary information for backup files, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, right-click the backup and select **Properties**.

   To see the list of available restore points, select the required VM in the **Objects** list.
Importing Backups

If you have backups of RHV VMs created by another RHV backup proxy, you can import these backup files to the current instance. Once imported, you can use the backups to restore VMs and VM disks.

When you import backups from a backup repository, the RHV backup proxy rescans the repository and removes information about manually deleted backups from the database.

NOTE

You cannot import backups from unsupported backup repository types. This can affect imports from backup copy jobs. For the list of supported backup repository types, see Configure Backup Repository.

To import RHV VM backups, do the following:

1. Transfer the backups to the required backup repository. The RHV backup proxy must have access to this repository.
2. In the Veeam Backup & Replication console, rescan the repository. For more information, see the Veeam Backup & Replication User Guide, section Rescanning Backup Repositories.
3. Click the Settings icon at the top right corner of the RHV backup proxy web console and select Manage Backup Server.
4. Select the required backup server from the list.
5. Click Import backups and then Proceed to confirm the action. The RHV backup proxy will scan the backup repositories and import all compatible backups of RHV VMs.

Once the backups are imported, switch to the Protected VMs page. You will see imported backups labeled with the Imported icon.
If you want to see the status of the import, switch to the **Events** page.
Exporting Backups

Exporting backups allows you to synthesize a complete and independent full backup file out of selected restore points that are located in your backup repositories. This means, you can transform any incremental backup chain (all dependent .vbk, .vib files) into a standalone .vbk file.

**NOTE**

Mind the following:

- The restore point that is being exported as a new full backup file is saved to the same repository, where the source selected restore points reside.

- Once export is complete, the exported backup files will be attached under the **Backups > Disk (Imported)** node.

- If a restore point that is being exported resides on the tenant side, a new full backup file will also be exported to the same repository (on the tenant side) from which the source restore point is being taken.

- If you select a backup job consisting of multiple virtual machines, Veeam Backup & Replication will synthesize a separate full backup file per each machine.

- Export session results are saved to the configuration database and available for viewing, as described in the Veeam Backup & Replication User Guide, section Viewing Session Statistics.

To export backup files, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.

2. In the inventory pane of the **Home** view, select **Backups**.
3. In the working area, select the backup or separate VM in the backup and click \textbf{Export Backup} on the ribbon.

You can also right-click the backup and select \textbf{Export backup}. For more information, see the Veeam Backup & Replication User Guide, section \textbf{Performing Export}. 
Deleting Backups

You have the following options to delete backups:

- **Remove from configuration** — remove records about backups from the Veeam Backup & Replication console and configuration databases. In this case, backup files are not deleted from the repository, and you can import the backups later. For more information on this option, see the Veeam Backup & Replication User Guide, section Removing Backups from Configuration.

- **Remove from disk** — permanently delete backup files from backup repositories and remove records about backups from the Veeam Backup & Replication console and configuration databases. For more information on this option, see the Veeam Backup & Replication User Guide, section Deleting Backups from Disk.

  Note that you can delete backup files for a specific VM only as described in the Veeam Backup & Replication User Guide, section Deleting VM from Backups.

**IMPORTANT**

Do not delete backup files from backup repositories manually. This may cause backup job failures and restore point corruption.

Deleting Backups in Veeam Backup & Replication Console

To delete a backup in the Veeam Backup & Replication console, do the following:

1. Open the **Home** view.
2. In the inventory pane of the **Home** view, select **Backups**.
3. In the working area, right-click the backup and choose whether you want to remove the backup from configuration or to delete backup files.
IMPORTANT

After you delete a backup in the Veeam Backup & Replication console, you must perform the backup import operation in the RHV backup proxy web console to see the changes.

Deleting Backups in Web Console

To delete a backup in the RHV backup proxy web console, do the following:

1. Switch to the Protected VMs page.
2. Click View as tree to see detailed information about backup jobs.
3. Click the backup job name to see the backed-up VMs and their restore points.
4. Select a VM whose restore points you want to delete, or a specific restore point.

IMPORTANT

If you select all VM restore points for deleting, backup files will be removed from the repository.

If at least one VM restore point remains in the backup chain, only records about deleted backups are removed, and backup files remain available in the repository.

5. Click Delete.
After you delete a backup in the RHV backup proxy web console, the Veeam Backup & Replication database will be automatically synchronized with the RHV backup proxy database to update the backup.
Performing Data Recovery Operations

In various disaster recovery scenarios, Veeam Backup for RHV allows you to perform the following operations using backed-up data:

- **Entire VM Restore** recovers a VM from a backup file to an RHV host.
- **VM Disks Restore** recovers a specific hard drive of a VM from a backup and attaches it to the original VM or to another VM.
- **Instant VM Recovery** instantly starts a VM directly from a backup file.
- **VM Guest OS Files Restore** recovers individual VM guest OS files and folders from VM backups.
- **VM Disk Export** restores VM disks from backups and converts them to disks of the VMDK, VHD or VHDX format.
- **Restore to Amazon EC2** restores VMs from backup files to Amazon EC2 as EC2 instances.
- **Restore to Microsoft Azure** restores VMs from backup files to Azure Blob storage as Microsoft Azure VMs.
- **Restore to Google CE** restores VMs from backup files to Google Compute Engine (CE) as VM instances.
Entire VM Restore

You can restore RHV VMs from backup files created by Veeam Backup for RHV. When you perform entire VM restore, the RHV backup proxy retrieves VM disk data from the backup, copies it to the storage domain and registers a restored VM on an RHV host.

Related Topics

- Restoring VMs Using Veeam Backup & Replication Console
- Restoring VMs Using RHV Backup Proxy Console
Before You Begin

Before you start the RHV VM restore process, mind the following limitations:

- You can restore multiple VMs at a time in the Veeam Backup & Replication console but only a single VM in the RHV backup proxy web console.

- When restoring VMs in the Veeam Backup & Replication console, you can select a storage domain for each VM virtual disk. When restoring a VM in the RHV backup proxy web console, a storage domain is selected for all disks of the VM.

- The SureBackup feature that allows you to verify any restore point of a backed-up VM is not supported for backups created by Veeam Backup for RHV.

- If multiple disks are attached to a VM that is added to the restore session, the RHV backup proxy restores these disks sequentially, one disk at a time. VMs added to the restore session are processed in parallel.

- After you restore a VM, a full VM backup will be created during a next backup session.
Restoring VMs Using Veeam Backup & Replication Console

In Veeam Backup & Replication console, you can restore one or multiple RHV VMs to any RHV cluster managed by the RHV manager.

Before you start restoring VMs, check the prerequisites and limitations, then launch the Full VM Restore to Red Hat Virtualization wizard to restore VMs.

1. Launch the Full VM Restore to Red Hat Virtualization wizard.
2. Select VMs to restore.
3. Choose a restore mode.
4. Specify a target cluster.
5. Select the storage domain where VM virtual disks will be stored.
6. Specify a name for the restored VM.
7. Specify network settings.
8. Specify a restore reason.
Step 1. Launch Full VM Restore to Red Hat Virtualization Wizard

To launch the **Full VM Restore to Red Hat Virtualization** wizard, do the following:

1. In the Veeam Backup & Replication console, open the **Backup** view.
2. In the inventory pane, select **Backups**.
3. In the working area, expand the necessary backup, select the VM that you want to restore and click **Entire VM** on the ribbon, or right-click the VM and select **Restore entire VM to RHV**.

Alternatively, to launch the **Full VM Restore to Red Hat Virtualization** wizard, you can do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, select **Backups**.
3. In the working area, expand the necessary backup, select the VM that you want to restore and select **Restore > RHV** on the ribbon.

4. Click **Restore from RHV backup**.
Step 2. Select VMs

At the **Virtual Machines** step of the wizard, select VMs that you want to restore:

1. To restore multiple VMs during one restore session, do the following:
   a. Click **Add**.
   b. In the **Backup Browser** window, expand a backup job tree that contains backups of VMs you want to restore and select a VM.
   c. Click **OK**.

2. By default, Veeam Backup for RHV restores VMs using the most recent restore point. To restore VM data to an earlier state, do the following:
   a. Select the VM in the list of virtual machines to restore and click **Point**.
      
      To help you choose a restore point, Veeam Backup for RHV provides the following information on each available restore point:
      
      ▪ **Job** — the name of the backup job and the date when the restore point was created.
      ▪ **Type** — the backup method used to create the restore point.
      ▪ **Location** — the repository where backup files for the restore point are stored.
   b. In the **Restore Points** window, select a restore point.
   c. Click **OK**.
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, do the following:

1. Choose whether you want to restore VMs to the original or to a custom location:
   - **Restore to the original location** — select this option if you want to recover VMs with their initial settings and to their original location. If this option is selected, you will pass directly to the **Reason** step of the wizard.
   - **IMPORTANT**
     If you recover a VM with the original settings, and the original VM still exists in the RHV infrastructure, the original VM will be removed.
   - **Restore to a new location, or with different settings** — select this option if you want to recover VMs to a new location, or to any location but with different settings (such as VM location, network settings, format of recovered virtual disks and so on). If this option is selected, the wizard will include additional steps for customizing VM settings.

2. Select the **Restore VM tags** check box if you want to recover tags that were assigned to the original VMs and assign them to the restored VMs.

3. Select the **Restore all VM disks to QCOW2 format** check box if you want to restore VM virtual disks in QCOW2 format. For more information on QCOW2 format and limitations that apply to RAW format, see **Enabling Incremental Backup**.
Step 4. Specify Target Cluster

[This step applies only if you have selected the *Restore to a new location, or with different settings* option at the *Restore Mode* step of the wizard]

At the **Cluster** step of the wizard, choose the cluster to which the VMs will be restored:

1. Select a VM and click **Cluster**.

2. In the **Select Cluster** window, select the necessary cluster and click **OK**.

![Full VM Restore to Red Hat Virtualization](image)

*By default, original cluster is selected as restore destination for each VM. You can change cluster by selecting desired VM and clicking Cluster. Use multi-select (Ctrl-click and Shift-click) to select multiple VMs at once.*

Select multiple VMs and click **Cluster** to apply changes in bulk.
Step 5. Select Storage Domain

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the Storage Domain step of the wizard, choose the storage domain where you want to store virtual disks of the restored VMs:

1. Select a VM or a VM virtual disk and click Domain.

2. In the Select Storage Domain window, select the necessary domain and click OK.
Step 6. Specify VM Name

[This step applies only if you have selected the **Restore to a new location, or with different settings** option at the **Restore Mode** step of the wizard]

**IMPORTANT**

By default, VMs are restored with their original names. If you restore VMs to the original location and do not specify new names for the VMs, the original VMs will be removed.

At the **VM name** step of the wizard, you can specify new names for the restored VMs:

1. Select a VM and click **Name**.
2. In the **Rename VM** window, do the following:
   - In the **Set name** field, specify a new name for the restored VM.
   - Check the **Add prefix** check box to specify a prefix that will be added to the name of the restored VM.
   - Check the **Add suffix** check box to specify a suffix that will be added to the name of the restored VM.
   - Click **OK**.
3. Select the **Preserve virtual machine ID** check box if the original VMs still exist in the RHV infrastructure and you want Veeam Backup for RHV to remove the original VMs.
Step 7. Specify Network Settings

[This step applies only if you have selected the Restore to a new location, or with different settings option at the Restore Mode step of the wizard]

At the **Network** step of the wizard, choose the network to which the restored VMs will be connected:

1. Select a VM and click **Network**.
2. In the **Select Network** window, select a network and click **OK**.

**NOTE**

If you do not want to connect a VM to any virtual network, select the VM in the list and click **Disconnect**.
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring VMs. This information will be saved to the session history and you will be able to reference it later.

![Full VM Restore to Red Hat Virtualization](image)

- **Reason**
  - Type in the reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.

- **Restore reason:**
  - Corrupted disks

- **Do not show me this page again**

- **Navigation buttons:**
  - Previous
  - Next
  - Finish
  - Cancel
Step 9. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

**TIP**

If you want to start the restored VMs as soon as the restore process completes, select the **Power on target VM after restore** check box.
Restoring VMs Using RHV Backup Proxy Console

In the RHV backup proxy web console, you can restore an individual RHV VM to the cluster where the original VM belongs.

Before you start restoring a VM, check the prerequisites and limitations, then launch the Full VM Restore wizard to restore a VM:

1. Select a VM to restore.
2. Choose the restore mode.
3. Specify a new name for the restored VM.
4. Select the storage domain where VM virtual disks will be stored.
5. Specify network settings.
6. Specify a restore reason.
7. Finish working with the wizard.

Launch Full VM Restore Wizard

To launch the Full VM Restore wizard, do the following:

1. Switch to the Protected VMs page.
2. Click Restore to launch the Full VM Restore wizard.
Step 1. Select VM to Restore

At the Virtual Machine step of the Full VM Restore wizard, select a VM that you want to restore.

1. Click Add.
2. In the **Backups Browser** window, expand the job that creates restore points for the VM, select the VM and click **Add**.

![Backups Browser](image)

3. By default, Veeam Backup for RHV restores VMs using the most recent restore point. To restore VM data to an earlier state, do the following:

   a. Click **Point**.

      To help you choose a restore point, Veeam Backup for RHV provides the following information on each available restore point:

      - **Job** — the name of the backup job.
      - **Date** — the date when the restore point was created.
      - **Type** — the backup method used to create the restore point.

      ![Restore Points](image)

   b. In the **Restore Points** window, select a restore point.

   c. Click **OK**.
Step 2. Choose Restore Mode

At the **Restore Mode** step of the **Full VM Restore** wizard, choose whether you want to restore the selected VM instance to the original or to a custom location.

**Restore Mode**

Specify whether selected VM should be restored back to the original location, or to a new location or with different settings.

- **Restore to the original location**
  
  Quickly initiate restore of selected VM to the original location, and with original name and settings. This option minimizes the chance of user input error.

- **Restore to a new location**
  
  Customize restore VM location, and change its settings. This wizard will automatically populate all controls with the original VM settings as the default settings.
Step 3. Specify Name for Restored VM

[This step applies only if you have selected the Restore to a new location option at the Restore Mode step of the wizard]

**IMPORTANT**

By default, a VM is restored with its original name. If you restore the VM to the original location and do not specify a new name for the VM, the original VM will be removed.

At the Name step of the wizard, you can specify a new name for the restored VM:

1. Select the VM and click Name.

2. In the Rename VM window, do the following:
   - In the Name field, specify a new name for the restored VM.
   - Check the Add prefix check box to specify a prefix that will be added to the name of the restored VM.
- Check the Add suffix check box to specify a suffix that will be added to the name of the restored VM.
- Click OK.

3. Select the **Preserve virtual machine ID** check box if the original VM still exist in the RHV infrastructure and you want Veeam Backup for RHV to remove the original VM.
Step 4. Select Storage Domain

[This step applies only if you have selected the Restore to a new location option at the Restore Mode step of the wizard]

At the Storage Domain step of the wizard, you can change the storage domain where you want to store virtual disks of the restored VM:

1. Click Domain.

2. In the Select Domain window, expand the domain tree, select the domain and click OK.
TIP
The selected domain will be used to store all virtual disks of the VM. However, if you choose to restore the VM using the Veeam Backup & Replication console, you will be able to select a storage domain for each virtual disk individually.
Step 5. Specify Network Settings

[This step applies only if you have selected the Restore to a new location option at the Restore Mode step of the wizard]

At the Network Settings step of the wizard, you can change the network to which the restored VM will be connected:

1. Select the network you want to change and click Network.
2. In the **Select Network Profile** window, select a network and click **OK**.

**NOTE**
If you do not want to connect the VM to any virtual network, select the VM and click **Disconnect**.
Step 6. Specify Reason for Restore

At the Reason step of the wizard, specify a reason for restoring VM. This information will be saved to the session history and you will be able to reference it later.
Step 7. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**.

**TIP**

If you want to start the restored VM as soon as the restore process completes, select the **Power on target VM after restore** check box.

If you want to recover tags that were assigned to the original VM and assign them to the restored VM, select the **Restore VM tags** check box.

If you want to restore VM virtual disks in QCOW2 format, select the **Restore all VM disks to QCOW2 format** check box. For more information on QCOW2 format and limitations that apply to RAW format, see [Enabling Incremental Backup](#).
VM Disks Restore

If a VM virtual disk gets corrupted for some reason, you can restore it from a backup. After restore, you can attach restored virtual disks to the original VM to replace the corrupted disk or connect as a new disk to any other VM.

To restore disks, do the following:

1. Check the limitations.
2. Launch the Virtual Disk Restore wizard.
3. Select a virtual machine.
4. Select a restore point.
5. Configure mapping settings.
6. Specify a reason for the restore.
7. Finish working with the wizard.
Before You Begin

Before you start the VM disk restore process, mind the following limitations:

- If a VM added to the restore session contains multiple disks, the RHV backup proxy restores one disk per job.
- As soon as you finish configuring the restore settings, the RHV backup proxy powers off the target VM and powers it on after the restore process completes.
Launch Virtual Disk Restore Wizard

To launch the Virtual Disk Restore wizard, do the following:

1. Switch to the Protected VMs page.
2. Click Disk Restore to launch the Virtual Disk Restore wizard.
Step 1. Select Virtual Machine

At the **Virtual Machine** step of the wizard, select VMs that contain disks that you want to restore.

In the list of jobs, expand the job tree and select a VM which disks you want to restore.
Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the required restore point for the VM.

<table>
<thead>
<tr>
<th>Job name</th>
<th>Date</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fileserver Backup</td>
<td>10/11/2021 9:22:08 AM</td>
<td>Incremental</td>
</tr>
<tr>
<td>Fileserver Backup</td>
<td>10/11/2021 8:12:06 AM</td>
<td>Full</td>
</tr>
</tbody>
</table>
Step 3. Configure Mapping Settings

At the **Disk Mapping** step of the wizard, configure VM disk mapping settings:

1. Select a VM to which you want to attach the restored disk.
   a. Click **Browse**.

   ![Disk Mapping step of the wizard](image)

   **Virtual Disk Restore**

   **Disk Mapping**
   Map virtual disks from backup to virtual devices on target VM.
   - Virtual machine: RHV-Proxy-GCP
   - Select disk for restore:
     - **Disk Alias**: VMDISK1
       - **Storage container**: hosted_storage_old_202110...
       - **Size**: 64 GB

   ![Select Virtual Machine window](image)

   **Select Virtual Machine**

   **Select virtual machine**:
   - Raw-template
   - rhv_backup_vm_master_1460_7ec9ba
   - RHV_Tapes
   - RHV-Proxy-GCP
   - RHVProxy-aws
   - TW_RHVBackup
   - VAT-CentOS-1
   - VAT-kvm-1169
   - VAT-1010

   ![Previous, Next, Cancel buttons](image)

   ![Refresh, OK, Cancel buttons](image)

   b. In the **Select Virtual Machine** window, select the VM and click **OK**.
2. If you want to change the target storage domain, disk address or the bus type, do the following:
   
a. Select the disk from the **Select disk for restore** field and click **Change**.

   ![Virtual Disk Restore](image)

   b. In the **Virtual Disk Properties** window:
      
      - Click **Choose** to select another target container.
      - From the **Bus Type** drop-down list, select one of the following bus type for the restored disk: IDE, SATA, SPAPR_VSCSI, VIRTIO, VIRTIO_SCSI.
- From the **Disk Destination** drop-down list, select the location where disks will be stored. If you select the default disk destination, after successful restore process, the existing virtual disk will be replaced. If you select a non-default disk destination, the restored virtual disk will be added to the VM as a new disk.

![Virtual Disk Properties](image)

3. Select the **Restore all VM disks to QCOW2 format** check box if you want to restore virtual disks in the QCOW2 format. You can create an incremental backup for virtual disks in QCOW2 format only. Virtual disks in RAW format support only full backup.
Step 4. Specify Reason for Restore

At the **Reason** step of the wizard, provide a reason for restoring the disk. The information you provide will be saved in the session history and you can reference it later.

![Reason step of the wizard](image)

Type in reason for performing this restore operation. This information will be logged in the restore sessions history for later reference.

Restore reason:

- Corrupted Virtual Disk
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**. The RHV backup proxy will power off the target VM.

**TIP**

If you want to start the restored VM as soon as the restore process completes, select the **Power on VM after restore** check box.
Instant VM Recovery

With Instant Recovery, you can immediately restore an RHV VM to VMware vSphere, Hyper-V or Nutanix AHV by running it directly from a compressed and deduplicated backup file. Instant Recovery helps to improve recovery time objectives, minimize disruption and downtime of production VMs.

To perform instant recovery, do the following:

1. In the Veeam Backup & Replication console, open the Home view.
2. In the inventory pane, select Backups.
3. In the working area, select the required VM in the backup and click Instant Recovery on the ribbon. You can also right-click the VM and select Instant Recovery.
4. Follow the steps of the Instant Recovery to VMware vSphere, Hyper-V or Nutanix AHV wizard. Depending on the platform to which you want to recover RHV VMs, see the following documents:
   - The Veeam Backup & Replication User Guide for VMware vSphere, section Performing Instant VM Recovery of Workloads to VMware vSphere VMs.
   - The Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Performing Instant VM Recovery of Workloads to Hyper-V VMs.
   - The Veeam Backup for Nutanix AHV User Guide, section Performing Instant VM Recovery of Workloads to Nutanix AHV.
VM Guest OS Files Restore

You can use Veeam Backup & Replication to recover individual VM guest OS files and folders from VM backups created by the Veeam Backup for RHV. VM guest OS file (or file-level) restore does not require you to extract the VM image to a staging location or start the VM prior to restore. You can restore files and folders directly from a regular image-level backup to the necessary point in time.

NOTE
Mind the following:

- You can also use Veeam Backup Enterprise Manager to file-level restore guest OS files of RHV VMs. For more information, see the Veeam Backup Enterprise Manager User Guide, section Restoring Guest OS Files.
- VM guest OS file indexing is not supported for RHV VM backups.

You can perform guest OS files restore for any VM guest OS file system. Veeam Backup & Replication offers different tools and methods for different file systems.

For guest OS files restore from FAT, NTFS, ReFS file systems, Veeam Backup & Replication deploys a small temporary VM (helper appliance) on an ESXI host. The helper appliance is a helper VM running a stripped down Linux kernel that has a minimal set of components. The appliance is around 50 MB. It requires 1024 MB RAM and takes around 10 seconds to boot. To learn how to configure a helper appliance, see the Veeam Backup & Replication User Guide, section Performing Instant Recovery to VMware vSphere.

File-Level Restore from Backups

You can use Veeam Backup & Replication to restore from Linux, Unix and other file systems. During restore from a backup, Veeam Backup & Replication mounts disks of the VM from the backup to a helper appliance (for Linux and other OSes), and launches the Veeam Backup Browser with the VM file system on the backup server.

How to Restore VM Guest OS Files

To restore VM guest OS files, do the following:

1. In the Veeam Backup & Replication console, open the Home view.
2. In the inventory pane, under Backups select Disk to restore from a backup.
3. In the working area, select the required VM in the backup and click Guest Files (Others) on the ribbon. You can also right-click the VM and select Restore guest files > Linux and other.
4. Follow the steps of the File Level Restore wizard. For further instructions, see one of the following section from the Veeam Backup & Replication User Guide:

   - Restoring VM Guest OS Files (FAT, NTFS or ReFS)
Restoring VM Guest OS Files (Multi-OS)
VM Disk Export

You can restore VM disks from backups created by the RHV backup proxy and convert them to disks of the VMDK, VHD or VHDX format. You can store the exported disks locally on any server added to the backup infrastructure. You can also store the exported disks on a datastore connected to an ESXi host. After disk export, you can mount the exported disk to any VM in the virtual infrastructure.

To export a VM disk, do the following:

1. In the Veeam Backup & Replication console, open the Home view.
2. In the inventory pane, under Backups select Disk to export from a backup.
3. In the working area, select the required VM in the backup and click Export Disks on the ribbon.
   You can also right-click the VM and select Export disk content as virtual disks.
4. Follow the steps of the Export Disk wizard. For more information, see the Veeam Backup & Replication User Guide, section Exporting Disks.
Restore to Amazon EC2

You can restore VMs from backup files created by Veeam Backup for RHV to Amazon EC2 as EC2 instances.

To restore a VM to Amazon EC2, do the following:

1. In the Veeam Backup & Replication console, open the Home view.
2. In the working area, expand the necessary backup node, right-click the VM that you want to restore, select Amazon EC2 and follow the steps of the Restore to Amazon EC2 wizard as described in the Veeam Backup & Replication User Guide, section Restore to Amazon EC2.
Restore to Microsoft Azure

You can restore VMs from backup files created by Veeam Backup for RHV to Azure Blob storage as Microsoft Azure VMs.

**TIP**

If you do not have the Microsoft Azure compute account to enable direct restore of any backup to Microsoft Azure, the wizard will start an initial configuration setting. For more information, see the Veeam Backup & Replication User Guide, section Configuring Initial Settings.

To restore a VM to Microsoft Azure, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.

2. In the working area, expand the necessary backup node, right-click the VM that you want to restore, select **Microsoft Azure** and follow the steps of the **Restore to Microsoft Azure** wizard as described in the Veeam Backup & Replication User Guide, section Restore to Microsoft Azure.
Restore to Google CE

You can restore VMs from backup files created by Veeam Backup for RHV to Google Compute Engine (CE) as VM instances.

To restore a VM to Google CE, do the following:

1. In the Veeam Backup & Replication console, open the Home view.

2. In the working area, expand the necessary backup node, right-click the VM that you want to restore, select Restore to Google CE and follow the steps of the Restore to Google Compute Engine wizard as described in the Veeam Backup & Replication User Guide, section Restore to Google Compute Engine.
Monitoring Events

On the Events page of the RHV backup proxy web console, you can view the list of internal events including changes in the backup infrastructure, started and stopped jobs, errors, warnings. You can use the search field to find a specific event and use the Resolved and Type filters to display events according to a status or an event type.

Use the following tips for working with events:

- To mark an event as resolved, select the check boxes on a left of required events and click the Resolve button. The time of resolution will appear at the Resolved column of the table.

- To see session details of a backup or restore operation, click the date of the event.

- Use the Type filter to view only certain types of events: Information, Warning, Error.

![Monitoring Events Page](image)
Getting Technical Support

If you have any questions or issues with Veeam Backup for RHV, 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
- Error message or accurate description of the problem you are facing
- Log files

To export logs for Veeam Backup for RHV, you must collect logs from both the Veeam Backup & Replication console and the RHV backup proxy web console.
Exporting Logs in RHV Backup Proxy Web Console

To collect logs in the RHV backup proxy web console, do the following:

1. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.
2. Click **Support Bundle**.

4. In the **Support Bundle** window, select types of logs that you want to export:
   - Select the **Service logs** option to collect logs of the RHV backup proxy Veeam Backup Agent service.
   - Select the **Agent logs** option to collect logs of the Veeam Data Mover service that is responsible for data transfer between the RHV backup proxy and backup repositories.
   - Select the **Library logs** option to collect logs of the VM Backup API.
   - Select the **Veeam Updater Logs** option to collect logs of the Veeam Updater component.

   After you click **Download**, the logs will be saved locally in the default download folder as a single .ZIP archive.
Exporting Logs in Veeam Backup & Replication Console

To collect logs for the RHV backup proxy in the Veeam Backup & Replication console, do the following:

1. From the main menu of the Veeam Backup & Replication console, select Help > Support Information.

2. At the Scope step of the Export Logs wizard, select the Export all logs for selected components option. Then, in the Managed servers list, select the backup server and the VM running as the RHV backup proxy.

Complete the wizard as described in the Veeam Backup & Replication User Guide, section Exporting Logs.
Checking RHV Backup Proxy Version

To check the product details, do the following:

1. Click the **Settings** icon at the top right corner of the RHV backup proxy web console and select **Appliance Settings**.

2. On the **Summary** tab, check the **Appliance Version** field.

![Screenshot of Appliance Settings tab](image.png)