Veeam Backup for Red Hat Virtualization

Version 2.0
User Guide
October, 2022
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTACTING VEEAM SOFTWARE</td>
<td>6</td>
</tr>
<tr>
<td>ABOUT THIS DOCUMENT</td>
<td>7</td>
</tr>
<tr>
<td>WELCOME TO VEEAM BACKUP FOR RED HAT VIRTUALIZATION</td>
<td>8</td>
</tr>
<tr>
<td>ARCHITECTURE OVERVIEW</td>
<td>9</td>
</tr>
<tr>
<td>PLANNING AND PREPARATION</td>
<td>10</td>
</tr>
<tr>
<td>System Requirements</td>
<td>10</td>
</tr>
<tr>
<td>Permissions</td>
<td>11</td>
</tr>
<tr>
<td>Ports</td>
<td>12</td>
</tr>
<tr>
<td>LICENSING</td>
<td>15</td>
</tr>
<tr>
<td>DEPLOYMENT</td>
<td>16</td>
</tr>
<tr>
<td>Installing RHV Plug-In</td>
<td>17</td>
</tr>
<tr>
<td>Upgrading to Veeam Backup for RHV 2.0</td>
<td>19</td>
</tr>
<tr>
<td>Uninstalling RHV Plug-In</td>
<td>21</td>
</tr>
<tr>
<td>CONFIGURING BACKUP INFRASTRUCTURE</td>
<td>22</td>
</tr>
<tr>
<td>Configuring Backup Repositories</td>
<td>22</td>
</tr>
<tr>
<td>Connecting RHV Manager</td>
<td>22</td>
</tr>
<tr>
<td>Adding RHV Manager to Backup Infrastructure</td>
<td>22</td>
</tr>
<tr>
<td>Editing RHV Manager Properties</td>
<td>28</td>
</tr>
<tr>
<td>Rescanning RHV Manager</td>
<td>29</td>
</tr>
<tr>
<td>Removing RHV Manager</td>
<td>30</td>
</tr>
<tr>
<td>Managing RHV Backup Proxy</td>
<td>31</td>
</tr>
<tr>
<td>Deploying New RHV Backup Proxy</td>
<td>31</td>
</tr>
<tr>
<td>Connecting Existing RHV Backup Proxy</td>
<td>41</td>
</tr>
<tr>
<td>Editing RHV Backup Proxy</td>
<td>51</td>
</tr>
<tr>
<td>Enabling SSH on RHV Backup Proxy</td>
<td>52</td>
</tr>
<tr>
<td>Rescanning RHV Backup Proxy</td>
<td>53</td>
</tr>
<tr>
<td>Removing RHV Backup Proxy</td>
<td>54</td>
</tr>
<tr>
<td>ACCESSING WEB CONSOLE</td>
<td>56</td>
</tr>
<tr>
<td>CONFIGURING GENERAL SETTINGS</td>
<td>58</td>
</tr>
<tr>
<td>Editing Network Settings</td>
<td>59</td>
</tr>
<tr>
<td>Editing Administrator Account</td>
<td>60</td>
</tr>
<tr>
<td>Configuring Time Zone Settings</td>
<td>61</td>
</tr>
<tr>
<td>Configuring Notifications</td>
<td>62</td>
</tr>
<tr>
<td>Configuring Email Notification Settings</td>
<td>63</td>
</tr>
<tr>
<td>Performing Configuration Backup and Restore</td>
<td>65</td>
</tr>
<tr>
<td>Performing Configuration Backup</td>
<td>66</td>
</tr>
</tbody>
</table>
# index

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restoring Configuration Data</td>
<td>67</td>
</tr>
<tr>
<td>PERFORMING BACKUP</td>
<td>71</td>
</tr>
<tr>
<td>How Backup Works</td>
<td>71</td>
</tr>
<tr>
<td>Backup Chain</td>
<td>72</td>
</tr>
<tr>
<td>Retention Policy</td>
<td>75</td>
</tr>
<tr>
<td>Creating Backup Jobs</td>
<td>76</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>76</td>
</tr>
<tr>
<td>Step 1. Launch New Job Wizard</td>
<td>77</td>
</tr>
<tr>
<td>Step 2. Configure General Settings</td>
<td>78</td>
</tr>
<tr>
<td>Step 3. Select VMs to Back Up</td>
<td>79</td>
</tr>
<tr>
<td>Step 4. Specify Repository</td>
<td>81</td>
</tr>
<tr>
<td>Step 5. Define Job Schedule</td>
<td>83</td>
</tr>
<tr>
<td>Step 6. Finish Working with Wizard</td>
<td>84</td>
</tr>
<tr>
<td>Editing Backup Job Settings</td>
<td>85</td>
</tr>
<tr>
<td>Starting and Stopping Backup Jobs</td>
<td>86</td>
</tr>
<tr>
<td>Enabling and Disabling Backup Jobs</td>
<td>87</td>
</tr>
<tr>
<td>Deleting Backup Jobs</td>
<td>88</td>
</tr>
<tr>
<td>Creating Active Full Backups</td>
<td>89</td>
</tr>
<tr>
<td>MANAGING BACKUPS</td>
<td>90</td>
</tr>
<tr>
<td>Viewing Backup Properties</td>
<td>90</td>
</tr>
<tr>
<td>Importing Backups</td>
<td>91</td>
</tr>
<tr>
<td>Exporting Backups</td>
<td>92</td>
</tr>
<tr>
<td>Copying Backups</td>
<td>93</td>
</tr>
<tr>
<td>Copying Backups to Tapes</td>
<td>94</td>
</tr>
<tr>
<td>Deleting Backups</td>
<td>95</td>
</tr>
<tr>
<td>PERFORMING RESTORE</td>
<td>98</td>
</tr>
<tr>
<td>Performing VM Restore</td>
<td>99</td>
</tr>
<tr>
<td>Restoring VMs Using Veeam Backup &amp; Replication Console</td>
<td>100</td>
</tr>
<tr>
<td>Restoring VMs Using RHV Backup Proxy Console</td>
<td>110</td>
</tr>
<tr>
<td>Performing Disk Restore</td>
<td>118</td>
</tr>
<tr>
<td>Step 1. Launch Virtual Disk Restore Wizard</td>
<td>119</td>
</tr>
<tr>
<td>Step 2. Select Virtual Machine</td>
<td>120</td>
</tr>
<tr>
<td>Step 3. Select Restore Point</td>
<td>121</td>
</tr>
<tr>
<td>Step 4. Configure Mapping Settings</td>
<td>122</td>
</tr>
<tr>
<td>Step 5. Specify Reason for Restore</td>
<td>123</td>
</tr>
<tr>
<td>Step 6. Finish Working with Wizard</td>
<td>124</td>
</tr>
<tr>
<td>Performing Instant VM Recovery</td>
<td>125</td>
</tr>
<tr>
<td>Performing File-Level Restore</td>
<td>126</td>
</tr>
<tr>
<td>Exporting Disks</td>
<td>127</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Performing VM Restore to Amazon Web Services</td>
<td>128</td>
</tr>
<tr>
<td>Performing VM Restore to Microsoft Azure</td>
<td>129</td>
</tr>
<tr>
<td>Performing VM Restore to Google Cloud</td>
<td>130</td>
</tr>
<tr>
<td>MONITORING EVENTS</td>
<td>131</td>
</tr>
<tr>
<td>UPDATING RHV BACKUP PROXY</td>
<td>132</td>
</tr>
<tr>
<td>Checking for Updates</td>
<td>132</td>
</tr>
<tr>
<td>Installing Updates</td>
<td>133</td>
</tr>
<tr>
<td>Viewing Update History</td>
<td>137</td>
</tr>
<tr>
<td>GETTING TECHNICAL SUPPORT</td>
<td>138</td>
</tr>
<tr>
<td>Viewing Product Details</td>
<td>138</td>
</tr>
<tr>
<td>Exporting Logs Using RHV Backup Proxy Web Console</td>
<td>139</td>
</tr>
<tr>
<td>Exporting Logs Using Veeam Backup &amp; Replication Console</td>
<td>140</td>
</tr>
</tbody>
</table>
Contacting Veeam Software

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

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal 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 is designed for IT professionals who plan to use Veeam Backup for Red Hat Virtualization. The guide includes system requirements, licensing information and step-by-step deployment instructions. It also provides a comprehensive set of features to ensure easy execution of protection and disaster recovery tasks in Red Hat Virtualization environments.
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 perform the following operations:

- Create backups of RHV VMs and store them in backup repositories.
- Create several instances (copies) of the same backup data in different locations.
- Restore VMs from RHV VM backups to the RHV environment.
- Restore VMs from RHV VM backups to Microsoft Azure, Amazon Web Services (AWS) and Google Cloud environments.
- Perform Instant Recovery of RHV VMs to Nutanix AHV, VMware vSphere and Microsoft Hyper-V environments.
- Restore files and folders of RHV VM guest OSes.
- Restore RHV VM disks and attach them to VMs running on RHV hosts.
- Export disks of backed-up RHV VMs to VMDK, VHD and VHDX formats.
Architecture Overview

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

1. **Backup Server** is a Windows-based physical or virtual machine 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 operations, controls job scheduling and manages resource allocation.

2. **RHV Manager** is a Linux-based physical or virtual machine that manages RHV resources such as VMs, hosts, clusters, storage domains and networks. Veeam Backup for RHV uses the RHV manager to access RHV resources while performing 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 in backup repositories.

- **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.

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>Virtualization</td>
<td>Veeam Backup for RHV is compatible with Red Hat Virtualization version 4.4 SP1 only (Red Hat Virtualization manager version 4.5.0).</td>
</tr>
<tr>
<td>Platform</td>
<td></td>
</tr>
<tr>
<td>Veeam Software</td>
<td>Veeam Backup &amp; Replication version 11a (11.0.1.1261 P20220302) with RHV Plug-in version 11.0.2.253 (or later) must be deployed on the backup server. Note: The RHV manager, RHV hosts and the RHV backup proxy must be able to resolve the FQDN of the backup server.</td>
</tr>
<tr>
<td>RHV Backup</td>
<td>The RHV backup proxy must be provided with sufficient compute resources to handle backup and restore tasks 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. The default RHV backup proxy configuration has the maximum number of concurrent tasks set to 4 and includes the following compute resources:</td>
</tr>
<tr>
<td>Proxy</td>
<td>• <strong>CPU</strong>: 8 vCPU</td>
</tr>
<tr>
<td></td>
<td>• <strong>Memory</strong>: 4 GB RAM</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disk Space</strong>: 64 GB for product installation, internal database files and logs</td>
</tr>
<tr>
<td>Notes:</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>2. The RHV backup proxy must be able to resolve FQDNs of the backup server, RHV manager and all RHV hosts.</td>
</tr>
</tbody>
</table>
Permissions

The accounts used to deploy 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 Virtualization documentation.
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>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>
<td></td>
</tr>
<tr>
<td>Ubuntu Security and OS Update repository (security.ubuntu.com, archive.ubuntu.com)</td>
<td>80</td>
<td>HTTP</td>
<td>Used to get OS security updates.</td>
<td></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>.NET Core Update repository</td>
<td>RHV backup proxy, Veeam Backup &amp; Replication console</td>
<td>443</td>
<td>HTTPS</td>
<td>Used to get .NET Core updates.</td>
</tr>
<tr>
<td>Veeam Updater repository</td>
<td>RHV manager</td>
<td>443</td>
<td>TCP</td>
<td>Used to download RHV backup proxy update packages.</td>
</tr>
<tr>
<td>Nginx repository (nginx.org/packages/, nginx.org/packages/keys/)</td>
<td>RHV manager</td>
<td>443</td>
<td>TCP</td>
<td>Used to download nginx packages required for RHV backup proxy web console updates.</td>
</tr>
</tbody>
</table>

* This range of ports applies to newly added backup infrastructure components. If you upgrade to Veeam Backup & Replication 11a (11.0.1.1261 P20220302) 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</td>
<td>Backup server</td>
<td>8544</td>
<td>HTTPS</td>
<td>Used to communicate with the Platform Service REST API.</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>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>RHV manager</td>
<td>54323</td>
<td>TCP</td>
<td>Used to communicate with the RHV manager (hosted engine).</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 backup proxy</td>
<td>443, 8100</td>
<td>HTTPS</td>
<td></td>
<td>Used by the RHV Platform Service to connect to the RHV backup proxy.</td>
</tr>
</tbody>
</table>

**NOTE**

For 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 the 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 can 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 backup server.

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 installation 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` installation 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.

![Installation Path](image)

6. Click **Install** to begin installation.

![Ready to Install](image)
Upgrading to Veeam Backup for RHV 2.0

You can upgrade 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 (11.0.1.1261 P20220302) 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 (11.0.1.1261 P20220302). 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 add the RHV backup proxy to the backup infrastructure, the backup server will upgrade all the existing backup infrastructure components including 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.

3. Upgrade Veeam Backup & Replication to version 11a (11.0.1.1261 P20220302). 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 Virtualization 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.

![Uninstall dialog box](image-url)
Configuring Backup Infrastructure

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

Configuring Backup Repositories

A backup repository is a storage location where Veeam Backup for RHV keeps backup files. By default, the backup server performs the role of a backup repository. To keep your backups in 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 Data Domain, HPE StoreOnce.

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

**IMPORTANT**

Veeam Backup for RHV does not support storing backups in Veeam Cloud Connect 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 add 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 using the Veeam Backup & Replication console.

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, do the following:

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.
Step 3. Enter Credentials

At the Credentials step of the wizard, specify credentials for 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 Virtualization documentation.

For credentials to be displayed in the Credentials list, they must be added to the Credentials Manager as described in the Veeam Backup & Replication User Guide, section Standard Accounts. If you have not added the necessary credentials to the Credentials Manager beforehand, you can do this without closing the New Red Hat Virtualization Manager wizard. To add an account, do the following:

1. Click Add.
2. In the Credentials window, do the following
   a. 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.
   b. In the Password field, enter the password for the account.
3. Click OK.

The backup server will connect to the RHV manager and 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.
Step 4. Apply Settings

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

![New Red Hat Virtualization Manager window with Apply step message]

Message: RHV Virtualization Manager podcope19@virobofish.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 has been successfully added and click Finish.

TIP

After you complete the wizard, it is required that you configure an RHV backup proxy. You can proceed to the New Red Hat Virtualization Proxy wizard immediately, or launch 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. However, the data synchronization process may take some time to complete. 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**.

**TIP**

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 that you can add only one RHV backup proxy for each RHV manager.

Deploying New RHV Backup Proxy

To deploy an RHV backup proxy and to add it 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. 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 of the wizard, select the **Deploy a new proxy** option.

- **Deploy a new proxy**
  - Deploy and configure a new Red Hat Virtualization backup proxy.

- **Connect to an existing proxy**
  - Register an existing Red Hat Virtualization backup proxy.
Step 3. Specify VM Configuration

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

1. Click Choose next to the RHV Cluster field, and specify an RHV cluster where the RHV backup proxy will be deployed in the Select RHV Cluster window.
   
   For a cluster to be displayed in the list of the available clusters, it must be added to the RHV infrastructure as described in Red Hat Virtualization documentation.

2. In the Name field, specify a name for the RHV backup proxy.

3. Click Choose next to the Storage Domain field, and specify a storage domain where RHV backup proxy system files will be stored in the Select Storage Domain window.
   
   For a domain to be displayed in the list of the available domains, it must be configured in the RHV infrastructure as described in Red Hat Virtualization documentation.

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 the currently running tasks finishes.
   
   The default number of concurrent tasks is set to 4. When you change this value, the wizard automatically adjusts the amount of resources that will be allocated to the VM running as the RHV backup proxy. If you want to specify the amount of resources manually, click Advanced. Note that you must take into account the RHV backup proxy system requirements.

TIP

After you deploy the RHV backup proxy, you will be not able to change the number of vCPU cores and the amount of RAM allocated to the RHV backup proxy using the Veeam Backup & Replication console. However, you can change the VM hardware configuration in the RHV Administration Portal. For more information, see Red Hat Virtualization 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 RHV backup proxy will be connected.
   
   For a network to be displayed in the list of the available networks, it must be configured in the RHV infrastructure as described in Red Hat Virtualization documentation.

2. In the **Hostname** field, specify a hostname (with domain name excluded) that will be assigned to the RHV backup proxy.
   
   The maximum length of the hostname is 63 characters. The hyphen-minus character (-) is supported, but you cannot use it as the first or the last character of the name.

3. If DHCP is enabled for the selected network adapter, the IP address and DNS settings of the RHV backup proxy can be obtained automatically.
   
   If DHCP is disabled for the selected network adapter, or you want to specify an IP address and configure DNS settings manually, click **Configure** and do the following in the **Network settings** window:
   
   - To specify an IP address, select the **Use the following IP address** option and enter the RHV backup proxy IP address, subnet mask and default gateway.
   - To configure DNS settings, select the **Use the following DNS server address** option and enter the IP addresses of the preferred and alternate DNS servers.
     
     If you select this option, you must also specify domain names that the RHV backup proxy will use to resolve the hostnames of the backup server, the RHV manager and RHV hosts. Use commas to separate multiple domain names.

**TIP**

After you deploy the RHV backup proxy, you will be able to change the configured network settings in the web console as described in section **Configuring General Settings**.
Step 5. Specify Credentials

At the **Credentials** step of the wizard, select credentials for an account that will be created on the RHV backup proxy for accessing the web console.

**IMPORTANT**
Do not select Active Directory accounts – the RHV backup proxy does not support LDAP integration.

For credentials to be displayed in the **Credentials** list, they must be added to the Credentials Manager as described in the Veeam Backup & Replication User Guide, section **Standard Accounts**. If you have not added the necessary credentials to the Credentials Manager beforehand, you can do this without closing the **New Red Hat Virtualization Proxy** wizard. To add credentials, do the following:

1. Click **Add**.
2. In the **Credentials** window, specify a user name and password for the account.
   The user name must contain only lowercase Latin letters and numeric characters, and must not match Linux system user names (such as *root*, *daemon*). The minimum length of the password is 6 characters.
3. Click **OK**.
Step 6. Grant Permissions

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

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

- Select the **Allow access to the following backup repositories** option if you want the RHV backup proxy to have access to specific 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. For a backup repository to be displayed in the **Repository** list, it must be added to the backup infrastructure.
Step 7. Apply Settings

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

**IMPORTANT**

If the wizard displays a warning notifying that the RHV backup proxy is unable to connect to the backup server, configure your network to allow the RHV backup proxy to resolve the hostname of the backup server. Then, **launch the Edit Red Hat Virtualization Proxy wizard** and click **Finish** to ensure that the RHV backup proxy has been added to the backup infrastructure without warnings and errors.
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 RHV backup proxy that has already been deployed but was removed from the backup infrastructure, you can connect it to the backup server. You may also want to connect an existing RHV backup proxy in the following situations:

- To upgrade an RHV backup proxy from version 1.0 or 1a to 2.0.
- To connect an RHV backup proxy that was previously connected to another backup server.

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.

After you connect the RHV backup proxy, the backup server will retrieve information about all backup jobs the proxy has ever processed. If the backup server configuration database contains records about RHV VM backups and if the backup files are still available in repositories, you can import backups to the RHV backup proxy and use them to restore entire VMs and VM disks.
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, select the Connect to an existing proxy option.
Step 3. Specify VM Configuration

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

1. Click Choose next to the RHV Cluster field, and specify the RHV cluster where the RHV backup proxy is deployed in the Select RHV Cluster window.
   For a cluster to be displayed in the list of the available clusters, it must be added to the RHV infrastructure as described in Red Hat Virtualization documentation.

2. Click Choose next to the Name field, and specify the VM running as the RHV backup proxy in the Select Virtual Machine window.

   NOTE
   You cannot change the storage domain – it 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 the currently running tasks finishes.
   The default number of concurrent tasks is set to 4. However, this value does not take into account the actual compute resources allocated to the VM running as the RHV backup proxy. If you want to adjust the number of concurrent tasks, consider the RHV backup proxy system requirements.

   NOTE
   When connecting an existing RHV backup proxy, you cannot change the number of vCPU cores and the amount of RAM allocated to the VM running as the RHV backup proxy using the Veeam Backup & Replication console. However, you can change the VM hardware configuration in the RHV Administration Portal. For more information, see Red Hat Virtualization documentation.
Step 4. Check Network Settings

When you connect an existing RHV backup proxy, you cannot change the network it is connected to, its hostname, IP address and DNS settings. At the **Networks** step of the wizard, review network settings configured for the RHV backup proxy and then click **Next**.

**TIP**

After you connect the RHV backup proxy, you will be able to change the configured network settings in the web console as described in section **Configuring General Settings**.
Step 5. Enter Credentials

At the **Credentials** step of the wizard, select credentials for the account that you use to access the RHV backup proxy web console.

For credentials to be displayed in the **Credentials** list, they must be added to the Credentials Manager as described in the Veeam Backup & Replication User Guide, section **Standard Accounts**. If you have not added the necessary credentials to the Credentials Manager beforehand, you can do this without closing the **New Red Hat Virtualization Proxy** wizard. To add credentials, do the following:

1. Click **Add**.
2. In the **Credentials** window, specify a user name and password for the account.
3. Click **OK**.
Step 6. Grant Permissions

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

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

- Select the **Allow access to the following backup repositories** option if you want the RHV backup proxy to have access to specific 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. For a backup repository to be displayed in the **Repository** list, it must be added to the backup infrastructure.
Step 7. Apply Settings

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

**IMPORTANT**

If the wizard displays a warning notifying that the RHV backup proxy is unable to connect to the backup server, configure your network to allow the RHV backup proxy to resolve the hostname of the backup server. Then, launch the Edit Red Hat Virtualization Proxy wizard and click Finish to ensure that the RHV backup proxy has been added to the backup infrastructure without warnings and errors.
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.
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 **Backup Proxies**.
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:
   a. To provide a new description for the RHV backup proxy and change the number of tasks that the proxy is able to handle in parallel, follow the instructions provided in section **Connecting Existing RHV Backup Proxy** (step 3).
   b. To change credentials for the account that is used to access the RHV backup proxy web console, follow the instructions provided in section **Connecting Existing RHV Backup Proxy** (step 5).
   c. To specify backup repositories the RHV backup proxy can access, follow the instructions provided in section **Connecting Existing RHV Backup Proxy** (step 6).
   d. To save changes made to the proxy settings, click **Finish**.

**TIP**

You cannot change the proxy IP address and DNS settings using the Veeam Backup & Replication console. However, you can do it using the RHV backup proxy web console. For more information, see **Editing Network Settings**.
Enabling SSH on RHV Backup Proxy

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

1. Log in to the Red Hat Virtualization Administration Portal.
2. In the main menu, navigate to Compute > Virtual Machines.
3. Select the VM running as the RHV backup proxy.
4. Click Console on the toolbar to download a Virt Viewer (.VV) file with all the settings required to connect to the VM. The file will be saved locally in the default download folder.
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 while deploying the RHV backup proxy.
7. In the VM console, execute the following command:

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

If the RHV backup proxy becomes unavailable, you can rescan it to synchronize data with the backup server. The rescan operation will update the proxy configuration 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 Backup Proxies > Unavailable.
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 the RHV backup proxy from the backup infrastructure if you no longer need it and want to add another proxy to the backup server, or if you want to connect this proxy to another backup server.

**IMPORTANT**

After you remove the RHV backup proxy:

- You will not be able to perform RHV VM backup, entire VM restore and VM disk restore operations unless you deploy a new RHV backup proxy. However, you will still be able to manage RHV VM backups and perform all other restore operation described in section Performing Restore.
- Records about all backup jobs that have been ever processed by the RHV backup proxy will be deleted from the Veeam Backup & Replication configuration database. Backups created by these jobs are displayed under the **Backups > Disk (Orphaned)** node in the **Home** view of the Veeam Backup & Replication console.

To remove the RHV backup proxy, do the following:

1. 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 **Remove Proxy** on the ribbon, or right-click the RHV backup proxy and select **Remove**.
4. In the **Veeam Backup & Replication** window, choose whether you want to permanently remove the VM running as the RHV backup proxy.

**IMPORTANT**

Unless you remove the VM running as the RHV backup proxy, the configuration settings and records about backup jobs ever processed by the proxy will be retained in the proxy database. This can be helpful if you want to **connect the RHV backup proxy to another backup server**.
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 during the initial RHV backup proxy configuration.

**TIP**

If you do not remember the password, you can reset it by running the RHV backup proxy in recovery mode. For more information, see this Veeam KB article.
Configuring General Settings

In the RHV backup proxy web console, you can perform the following administrative tasks:

- **Edit network settings.**
- **Edit the Administrator account.**
- **Configure time zone and synchronization settings.**
- **Configure settings for update and space usage notifications.**
- **Configure notification settings for automated delivery of backup job results.**
- **Back up and restore proxy configuration.**
Editing Network Settings

You can view and modify network settings configured for the proxy while connecting it to the backup server:

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

2. Switch to the Network tab.

3. If DHCP is enabled for the network adapter, the IP address and DNS settings of the RHV backup proxy can be obtained automatically.

   If DHCP is disabled for the network adapter, or you want to specify an IP address and configure DNS settings manually, do the following:
   
   o To specify an IP address, clear the Obtain an IP address automatically check box and enter the RHV backup proxy IP address, subnet mask and default gateway.
   
   o To configure DNS settings, clear the Obtain DNS server address automatically and enter the IP addresses of the preferred and alternate DNS servers.

   You must also specify domain names that the RHV backup proxy will use to resolve the hostnames of the backup server, the RHV manager and RHV hosts. Use commas to separate multiple domain names.

4. Click Apply.
Editing Administrator Account

You can edit the account that is used to access the RHV backup proxy web console or provide a new password for the account:

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

2. Switch to the Security tab and do the following:
   - To change the password:
     i. In the Old password field, enter the currently used password.
     ii. In the New password and Confirm password fields, enter and confirm a new password. The minimum length of the password is 6 characters.
   - To specify credentials for a new account:
     i. In the Login field, specify a user name. The user name must contain only lowercase Latin letters and numeric characters, and must not match Linux system user names (such as root, daemon).
     ii. In the Old password field, enter the currently used password.
     iii. In the New password and Confirm password fields, enter and confirm a password for a new account. The minimum length of the password is 6 characters.

3. Click Apply to save the settings.

IMPORTANT

If you modify the account, you must also update account credentials in the RHV backup proxy configuration using 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 RHV backup proxy to match the time on the workstation from which you access the proxy.

**NOTE**

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

To configure 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. Switch to the **Time zone** tab and then click **Settings**.
3. In the **Change Time Settings** window, do the following:
   a. Choose the necessary time zone from the **Select the time zone** list.
   b. Choose whether you want the time set on the RHV backup proxy to be synchronized with the time of specific NTP servers or with the time of the guest OS running on the host where the proxy is deployed.
Configuring Notifications

You can enable notifications to get informed about available product updates and backup repositories running low on free disk space:

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

2. Switch to the Notifications tab.

3. Select notifications you want to receive.

4. Click Apply.
Configuring Email Notification Settings

You can specify email notification settings for automated delivery of backup job results. To connect an SMTP server that will be used for sending email notifications:

1. Click the Settings icon at the top right corner of the RHV backup proxy web console, and select Appliance Settings.
2. Switch to the E-mail settings tab.
3. Select the Enable e-mail notifications check box.
4. In the SMTP server field, enter the full DNS name or IP address of the SMTP server. All email notifications (including test messages) will be sent by this SMTP server.
5. Click Advanced to specify an account that will be used when authenticating against the SMTP server and to configure other connection settings.

In the Advanced SMTP Settings window:
   a. In the SMTP Port field, specify a communication port for SMTP traffic. The default SMTP port is 25.
   b. For an SMTP server with SSL/TLS support, select the Connect using SSL check box to enable SSL data encryption.
   c. If your SMTP server requires authentication, select the This SMTP server requires authentication check box and specify credentials that will be used to connect to the SMTP server.
   d. Click OK.
6. In the From field, enter an email address of the notification sender. This email address will be displayed in the From field of notifications.
7. In the To field, enter an email address of a recipient. Use a semicolon to separate multiple recipient addresses.
8. In the Subject field, specify a subject for notifications. You can use the following runtime variables:
   o %JobName% — a backup job name.
   o %JobResult% — a backup job result.
   o %ObjectCount% — the number of VMs in a backup job.
9. Choose whether you want to receive email notifications in case backup jobs complete successfully, complete with warnings or complete with errors.
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. Click Apply.
TIP

Veeam Backup for RHV allows you to send a test message to check whether you have configured the settings correctly. To do that, click **Test message**. A test message will be sent to the specified email address.
Performing Configuration Backup and Restore

You can back up and restore the configuration database that stores data collected from the RHV backup proxy for the existing backup jobs, logged session records and network settings. If the proxy goes down for some reason, you can redeploy it and quickly restore its configuration from a configuration backup. You can also use a configuration backup to migrate the configuration of one proxy to another proxy in the RHV infrastructure.

It is recommended that you regularly perform configuration backup for every proxy present in the backup infrastructure. Periodic configuration backups reduce the risk of data loss and minimize the administrative overhead costs in case any problems with the backup proxy occur.
Performing Configuration Backup

While performing configuration backup, Veeam Backup for RHV exports data from the RHV backup proxy configuration database and saves it to a backup file. To back up the configuration database of the 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. Switch to the **Summary** tab and then click **Configuration Backup**.

3. In the **Configuration Backup** window, select items that you want to back up, specify a password that will be used to encrypt saved files, and provide a password hint that will help you remember your password if you forgot it.

   If you select the **Common** option, Veeam Backup for RHV will back up both all the existing proxy configuration settings and information about created backup jobs. If you select the **Events** option, Veeam Backup for RHV will back up session logs only.

4. Click **Download**.

As soon as you click **Download**, Veeam Backup for RHV will save the exported backup file to the default download directory on the local machine.
Restoring Configuration Data

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

- You want to recover data from a configuration backup because the configuration database got corrupted.
- You want to roll back the configuration database to a specific point in time.
- You want to apply a backed-up configuration to a newly deployed RHV backup proxy.

To restore the configuration, 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. Switch to the **Summary** tab.
3. Click **Configuration Restore** to launch the **Configuration Restore** wizard.
4. 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 while performing configuration backup.

![Configuration File Step](image)

5. At the **Network Settings** step of the wizard, choose whether you want to use the existing network settings saved in the backup file or to configure new network settings for the restored configuration. To edit the settings, select the **Configure new settings** option and do the following:

   a. To change the hostname of the RHV backup proxy, enter a new name in the **Appliance host name** field.

   b. If DHCP is disabled for the network adapter, or you want to specify an IP address manually, clear the **Obtain an IP address automatically** check box and enter the RHV backup proxy IP address, subnet mask and default gateway.

   c. If DHCP is disabled for the network adapter, or you want configure DNS settings manually, clear the **Obtain DNS server address automatically** and enter the IP addresses of the preferred and alternate DNS servers.

   You must also specify domain names that the RHV backup proxy will use to resolve the hostnames of the backup server, the RHV manager and RHV hosts. Use commas to separate multiple domain names.
IMPORTANT
If you change the RHV backup proxy network settings, you must also update the RHV backup proxy configuration using the Veeam Backup & Replication console.

Configuration Restore

Network Settings
Specify the network settings for the Veeam Backup for Red Hat Virtualization Beta.

- Use existing settings from configuration backup.
- Configure new settings:

  - Appliance host name: RHV-Backup-Proxy
  - Obtain an IP address automatically
    - IP address: 172.25.16.50
    - Subnet mask: 255.255.252.0
    - Default gateway: 172.25.16.1
  - Obtain DNS server address automatically
    - Preferred DNS server: 172.25.16.41
    - Second DNS server: 172.25.16.42
    - Search domains
      (separated by commas, each search domain name must comply with RFC1123)
6. At the **Summary** step of the wizard, review the configured settings and click **Finish** to start the restore process.
Performing Backup

To produce backups of RHV VMs, Veeam Backup for RHV runs backup jobs. A backup job is a collection of settings that define the way backup operations are performed: what data to back up, where to store backups, when to start the backup process, and so on.

One backup job can be used to process multiple VMs, but you can back up each VM with one backup job at a time. If a VM is added to more than one backup job, it will be processed only by the backup job that started earlier.

You can instruct the Veeam Backup for RHV to run jobs automatically according to a specified schedule or start them manually.

How Backup Works

Veeam Backup for RHV does not install agent software inside VMs to retrieve data. To back up VMs, Veeam Backup for RHV uses native RHV capabilities. During every backup session, Veeam Backup for RHV creates a snapshot for each VM added to a backup job. The snapshot is further used to create a backup of the VM.

During the VM backup process, the following steps are performed:

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 source RHV host over REST API and creates snapshots of all VMs added to the job.
4. The RHV backup proxy creates a volume group on the RHV cluster, mounts VM disks over 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.
Backup Chain

Veeam Backup for RHV creates a new backup file in a backup repository during every backup session. A sequence of backup files created during a set of backup sessions makes up a backup chain. Each backup chain contains data for one VM only. If a backup job includes several VMs, Veeam Backup for RHV creates one backup chain for each VM processed by the job.

The backup chain includes backup files of the following types:

- **VBK** — a full backup file stores a copy of the full VM image.
- **VIB** — incremental backup files store incremental changes of the VM image.
- **VBM** — backup metadata files store information about the backup job, VMs processed by the backup job, number and structure of backup files, restore points, and so on. Metadata files facilitate import of backups, backup mapping and other operations.

To create a backup chain for a VM protected by a backup job, Veeam Backup for RHV implements the forever forward incremental backup method:

1. During the first (full) backup session, Veeam Backup for RHV copies the full VM image and creates a full backup file in the backup repository. The full backup file becomes a starting point in the backup chain.
2. During subsequent backup sessions, Veeam Backup for RHV copies only those data blocks that have changed since the previous backup session, and stores these data blocks to incremental backup files in the backup repository. The content of each incremental backup file depends on the content of the full backup file and the preceding incremental backup files in the backup chain.

**NOTE**

If the UUID of a VM changes (for example, if the VM was migrated to another cluster), Veeam Backup for RHV will be unable to continue the backup chain for this VM. After you re-add the VM to the backup job, Veeam Backup for RHV will start a new backup chain for it. However, you will still be able to perform restore operations using backups from the old backup chain.

Full and incremental backup files act as restore points for backed-up VMs that let you roll back VM data to the necessary state. To recover a VM to a specific point in time, the chain of backup files created for the VM must contain a full backup file and a set of incremental backup files dependent on the full backup file.

If some file in the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, you must not delete individual backup files from the backup repository manually. Instead, you must specify retention policy settings that will let you maintain the necessary number of backup files in the backup repository.
Active Full Backup

In some cases, you need to regularly create a full backup. 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 allows you to create active full backups (either manually or automatically according to a specific schedule).

When creating an active full backup, Veeam Backup for RHV starts a new backup chain for the VM. All further created incremental backups use the latest active full backup file as a new starting point. The old full backup file from the old backup chain remains on disk until it is automatically deleted according to the retention policy.

Veeam Backup for RHV triggers a backup job to create an active full backup even if a regular backup session is not scheduled on this day. The active full backup session starts at the same time when the backup job is scheduled. For example, if you schedule the backup job to run at 12:00 AM Sunday through Friday, and schedule active full backup to be created on Saturday, Veeam Backup for RHV will start a backup job session that will produce an active full backup at 12:00 AM on Saturday.

If the backup job is not scheduled to run automatically or is disabled, Veeam Backup for RHV will not perform active full backup. If a regular backup session and an active full backup session are scheduled on the same day, Veeam Backup for RHV will produce an active full backup — an incremental backup that should have been created by the regular backup session will not be added to the backup chain. However, if you run the backup job again on the same day manually, Veeam Backup for RHV will perform incremental backup in a regular manner.
Changed Block Tracking

The changed block tracking (CBT) mechanism allows Veeam Backup for RHV to increase the speed and efficiency of incremental backups:

- During a full backup session Veeam Backup for RHV reads only written data blocks, while unallocated data blocks are filtered out.
- During an incremental backup session, Veeam Backup for RHV reads only those data blocks that have changed since the previous backup session.

To detect unallocated and changed data blocks, CBT relies on the RHV REST API:

1. During the first (full) backup session, Veeam Backup for RHV creates a snapshot of a VM using native RHV capabilities. To do that, Veeam Backup for RHV sends API requests to access the content of the snapshot and to detect unallocated data blocks.
2. During subsequent sessions, new snapshots are created. Veeam Backup for RHV sends API requests to access and to compare the content of the snapshot created during the previous backup session and the snapshot created during the current backup session. This allows Veeam Backup for RHV to detect data blocks that have changed since the previous backup session.

**IMPORTANT**

If Veeam Backup for RHV is unable to use CBT while creating incremental backups, you may get the following warnings in backup session logs:

- "Unable to enable ovirt incremental backups for disk. Full scan backups will be performed". To resolve the issue, follow the Veeam KB article.
- "The Disk id=<disk id> has RAW format and can be backed up only in full scan mode". To resolve the issue, take a VM snapshot in the RHV Administration Portal as described in Red Hat Virtualization documentation. Alternatively, back up the VM and restore its VM disks with the Restore all VM disks to QCOW2 format option selected at the Configure Mapping Settings step of the Virtual Disk Restore wizard.
Retention Policy

Backups created by backup jobs are not kept forever — they are removed according to retention policy settings specified while creating the jobs as described in section Creating Backup Jobs.

Retention policy is specified in restore points, which means that the backup chain can contain the allowed number of restore points only. If the number of allowed restore points is exceeded, Veeam Backup for RHV removes the earliest restore point from the chain.

To track and remove redundant restore points from a backup chain, Veeam Backup for RHV performs the following actions:

1. During every successful backup session, Veeam Backup for RHV adds a new incremental backup file to the backup chain.
2. If Veeam Backup for RHV detects that the number of restore points in the backup chain exceeds the allowed number, it transforms the backup chain in the following way:
   a. Rebuilds the full backup file to include there data of the incremental backup file that follows the full backup file. To do that, Veeam Backup for RHV injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, the full backup 'moves' forward in the backup chain.
   b. Removes the earliest incremental backup file from the chain as redundant — this data has already been injected into the full backup file.
Creating Backup Jobs

To create a backup job, do the following:

1. Check prerequisites and limitations.
2. Launch the New Job wizard.
3. Configure general settings.
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, consider the following 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 processing this VM until the currently running 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 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 while previewing its snapshot. For more information, see Red Hat Virtualization documentation.

- You cannot include into a backup job a VM being backed up by 3rd party software or an RHV backup proxy connected to another backup server. Wait for the backup process to complete or stop the job manually, and then add the VM to a backup job.

  If the backup process fails to complete, disable the job manually and then add the VM to a backup job. If you cannot disable the job, submit a support case in the Veeam Customer Support Portal.

- 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 the start, stop or reboot REST API request; however, this will cause backup job failure.

- By default, Veeam Backup for RHV applies the following deduplication and compression settings to backed-up data:
  
  o Deduplication: Enabled
  
  o Data compression level: Optimal
  
  o Storage optimization: Local target (1024 KB block size)

  Due to technical limitations, you cannot change these settings while configuring backup jobs.
• By default, **backup encryption** is disabled for backed-up data. However, you can enable encryption at the repository level. For more information, see the Veeam Backup & Replication User Guide, section Access Permissions.

• **VM guest OS file indexing** is not supported for backups created with Veeam Backup for RHV.

## Step 1. Launch New Job Wizard

In the inventory pane, select **Jobs** and navigate to **Backup > Red Hat Virtualization**. The RHV backup proxy console will open in your browser.

![Backup proxy console](image)

**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 2. Configure General Settings

At the **General Settings** step of the wizard, use the **Name** and **Description** fields to enter a name for the new backup job and to provide a description for future reference. The maximum length of the name is 127 characters; the following characters are not supported: \ / " ' [ ] : | < > + = ; , ? * @ & _.
Step 3. Select VMs to Back Up

At the Virtual Machines step of the wizard, specify the backup scope — select VMs that Veeam Backup for RHV will back up.

1. Click Add.
2. In the Add Objects window, choose whether you want to back up specific VMs or groups of VMs arranged by tags:
   - If you select the VM option, you must specify the machines explicitly.
     - By default, backup jobs process all disks attached to the selected VMs. If you want to exclude specific disks of a VM from the backup scope, do the following. First, click Exclusions, select the VM and click Edit in the Exclusions window. Then, select the Selected disks option and click Add in the Select Disks window. Finally, choose a bus type of the disks that you want to back up and select the necessary disks in the Add Disks window. Disks that you do not select will be excluded from the backup job.
   - If you select the TAG option and add a tag the backup scope, Veeam Backup for RHV will regularly check for new VMs assigned the added tag and automatically update the backup job settings to include these VMs in the scope. 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.
     - By default, backup jobs process all VMs to which the added tags are assigned. If you want to exclude specific VMs from the backup scope, click Exclusions and specify a VM name mask in the Exclusions window.

NOTE

If any of the selected VMs have disks in the RAW format attached, Veeam Backup for RHV will display the following warning: "There are some vm disk(s) which do not support ovirt incremental backup. The policy will do a full scan backup for those disk(s)". Due to technical limitations, Veeam Backup for RHV is only able to apply the CBT mechanism to disks in the QCOW2 format while performing incremental backup.

You can proceed with the wizard and resolve the issue later by using one of the following workarounds:

- Take VM snapshots in the RHV Administration Portal as described in Red Hat Virtualization documentation.
- Back up the VMs and restore their disks with the Restore all VM disks to QCOW2 format option selected at the Configure Mapping Settings step of the Virtual Disk Restore wizard.

- If you select the TAG option and add a tag the backup scope, Veeam Backup for RHV will regularly check for new VMs assigned the added tag and automatically update the backup job settings to include these VMs in the scope. 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.

By default, backup jobs process all VMs to which the added tags are assigned. If you want to exclude specific VMs from the backup scope, click Exclusions and specify a VM name mask in the Exclusions window.
**Virtual Machines**

Select virtual machines or vm tags for this policy to process.

Total VMs: 130  
Selected objects: 1  

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>File_Server</td>
<td>Virtual Machine</td>
<td>6.07 GB</td>
</tr>
</tbody>
</table>
Step 4. 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.
   - For a backup repository to be displayed in the list of the available repositories, it must be added to the backup infrastructure, and the RHV backup proxy must have access to the repository.

2. In the **Restore Points to keep** field, specify the number of restore points that you want to keep in a backup chain.
   - When the restore point limit is exceeded, Veeam Backup for RHV removes the earliest restore point from the chain. For more information, see section Retention Policy.

3. To configure retention settings for VMs that are no longer processed by the backup job, do the following:
   - a. Click **Advance**.
      - b. On the **Maintenance** tab of the Advanced Settings window, select the **Remove deleted VMs data after** check box and specify the number of days (or months) during which Veeam Backup for RHV will keep backups of the VMs excluded from the job.

4. To schedule active full backups, do the following:
   - a. Click **Advance**.
      - b. On the **Backup** tab of the Advanced Settings window, select the **Run active full backup periodically** check box, and choose whether you want to create active full backups on selected days every week or on selected days of selected months.
      - Alternatively, you can create active full backups manually when needed. For more information, see Creating Active Full Backup.

**IMPORTANT**

If you use hardened repositories to store RHV VM backups, you must consider the following requirements:

- Active full backups must be scheduled in the backup job settings.
- The backup job retention period must be longer than the backup repository immutability period.

For example, if the backup repository immutability period is set to 25 days, you can configure a one-month retention period: specify 4 as the number of restore points, **schedule one backup per week** and schedule active full backup to run on the last day of the month.
Backup Destination
Specify backup repository to store the backups produced by this job and customize advanced job settings if required.

Selected VMs: 1
Approximate backup size: 6.07 GB

Backup repository:
Default Backup Repository
- 5 GB free of 129 GB

Advanced Settings include active full and deleted VM retention settings.
Step 5. Define Job Schedule

At the **Schedule** step of the wizard, you can instruct Veeam Backup for RHV to start the backup job automatically according to a specific backup schedule. The backup schedule defines how often data of the VMs added to the backup job will be backed up.

To help you implement a comprehensive backup strategy, Veeam Backup for RHV allows you to create schedules of the following types:

- **Daily at this time** — the backup job will create restore points at a specific time on specific days.
- **Monthly at this time** — the backup job will create restore points once a month on a specific day.
- **Periodically every** — the backup job will create restore points repeatedly with a specific time interval every day.

**TIP**

You can instruct Veeam Backup for RHV to run the backup job again if it fails on the first try. To do that, select the **Automatic Retry** check box, and specify the maximum number of attempts to run the backup job and the time interval between retries. When retrying backup jobs, Veeam Backup for RHV processes only those VMs that failed to be backed up during the previous attempt.
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review summary information and click **Finish**. As soon as Veeam Backup for RHV starts the job, the backup progress will be displayed on the **Events** page.

**TIP**

If you want to start the job immediately, select the **Run job when I click Finish** check box and then click **Finish**.
Editing Backup Job Settings

For each backup job, you can modify settings configured while creating the 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 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:
   a. To provide a new name and description for the job, follow the instructions provided in section Creating Backup Jobs (step 1).
   b. To edit to the backup scope, follow the instructions provided in section Creating Backup Jobs (step 2).
   c. To change the backup repository where backups are stored, to configure backup job retention settings and to schedule active full backups, follow the instructions provided in section Creating Backup Jobs (step 3).
   d. To modify the job schedule and configure automatic retry settings, follow the instructions provided in section Creating Backup Jobs (step 4).
   e. At the Summary step of the wizard, review configuration information and click Finish.

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.
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 manually 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. 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, do the following:

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.
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, 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 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 configuration database if you no longer need it. When you delete a job, backups created by this job are displayed under the **Backups > Disk (Orphaned)** node in the **Home** view of the Veeam Backup & Replication console. If you want to delete backup files as well, follow the instructions provided in section **Deleting 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**.
Creating Active Full Backups

You can manually create an active full backup for all VMs added to a backup job.

1. Switch to the Jobs page.
2. Select the necessary backup job and click Active Full.
3. Click Yes.

**TIP**

To create active full backup automatically according to a specific schedule, configure backup job settings as described in section Creating Backup Jobs (step 3).
Managing Backups

Veeam Backup for RHV stores information on all protected RHV VMs in the configuration database. Even if a VM is no longer protected by any configured backup job and even if the VM no longer exists in the RHV infrastructure, records about created backups will not be deleted from the database until Veeam Backup for RHV automatically removes all restore points associated with this VM according to the retention settings saved in the backup metadata. You can manage RHV VM backups as long as their records are present in the configuration database.

Viewing Backup Properties

After a backup job successfully creates a backup of an RHV VM according to the specified schedule, or after you create an active full backup of a VM manually, the backup is displayed under the **Backups** node in the **Home** view of the Veeam Backup & Replication console. Each backup is represented with a set of properties, such as:

- **Objects** — the names and sizes of backed-up VMs.
- **Restore Points** — the date and time of all restore points created for a VM.
- **Files** — the size of processed VM data, the size of backed-up VM data, the ratio of data deduplication and the ratio of data compression.

To view backup properties, 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**.
Importing Backups

If you remove the RHV backup proxy from the backup infrastructure and connect a new one, you can import backups created by the old proxy and use them to restore VMs and VM disks.

**NOTE**

When you import backups, the backup jobs that produced those backups are not re-created. To re-create the jobs, restore the RHV backup proxy configuration as described in section [Restoring Configuration Data](#).  

To import RHV VM backups, do the following:

1. Ensure that the RHV backup proxy has access to repositories where the necessary backups are stored.
2. Click the **Settings** icon at the top right corner of the RHV backup proxy web console, and select **Manage Backup Server**.
3. Click **Import Backups** and then click **Proceed**.

   The RHV backup proxy will scan the repositories and import all RHV VM backups created by Veeam Backup for RHV. You can track the progress of the import operation on the Events page.

To see the list of imported backups, switch to the **Protected VMs** page and click **View as tree**.
Exporting Backups

Exporting backups allows you to synthesize a complete and independent full backup file using restore points located in your backup repositories. That is, you can transform any backup chain into a standalone full backup file and save it to the same repository where the selected restore points reside.

To export a backup, 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 a VM for which you want to synthesize a full backup file, and select **Export Backup**.
4. Complete the **New Export** wizard as described in the Veeam Backup & Replication User Guide, section **Performing Export**.

Once the export operation completes, the exported backup will be displayed under the **Backups > Disk (VeeamZIP)** node in the **Home** view of the Veeam Backup & Replication console.
Copying Backups

With backup copy, you can create several instances of a backup and copy them to secondary (target) backup repositories for long-term storage. Target backup repositories can be located in the same site as the source backup repository or can be deployed off-site. Since the backup copy has the same format as the original backup, you can restore VM data directly from the backup copy in case a disaster strikes. For more information on the backup copy functionality, see the Veeam Backup & Replication User Guide, section Backup Copy.

NOTE
The **Immediate copy** mode is not supported for backups created with Veeam Backup for RHV.

To copy backups to a secondary backup repository, do the following:

1. In the Veeam Backup & Replication console, open the **Home** view.
2. In the inventory pane, right-click **Jobs** and select **Backup Copy > Red Hat Virtualization Plug-in for Veeam Backup & Replication backup**.
Copying Backups to Tapes

You can create archives of RHV VM backups and copy them to tapes for long-term storage. Veeam Backup for RHV allows you to manage tape archives the same way you manage backups in backup repositories. However, it usually takes more time to access archived data on tapes than to access backed-up data in repositories. For more information on tapes, see the Veeam Backup & Replication User Guide, section Tape Devices Support.

To archive RHV VM backups to tape, do the following:

1. **Configure the tape infrastructure:**
   b. Perform initial configuration of the tape infrastructure as described in the Veeam Backup & Replication User Guide, section Getting Started with Tapes (steps 1–3).

2. **Create a backup to tape job as described in the Veeam Backup & Replication User Guide, section Creating Backup to Tape Jobs.**

**NOTE**

You cannot restore RHV VMs directly from tapes. To restore an RHV VM, you must first restore its backups to a repository as described in the Veeam Backup & Replication User Guide, section Backup Restore from Tape to Repository.
Deleting Backups

By default, Veeam Backup for RHV maintains backups in backup repositories according to retention policy settings saved in the backup metadata. If Veeam Backup for RHV detects that the number of restore points in the backup chain exceeds the allowed number, it automatically removes obsolete backups. If you need to delete backups manually, you can perform one of the following operations:

- **Remove from configuration** — removes records about backups from the configuration database but keeps the backup files in repositories.
- **Delete from disk** — permanently deletes backup files from backup repositories and removes records about the backups from the configuration database.

Removing Backups From Configuration

To remove a backup from the configuration database, 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, right-click the job that created the backup and select **Remove from configuration**.

**NOTE**

When you remove backups using the Veeam Backup & Replication console, the list of available backups in the RHV backup proxy web console is not updated automatically. To update the list manually, perform the backup import operation.
TIP
You cannot remove a backup from the configuration database using the RHV backup proxy console. However, you can use it to remove records about specific restore points created by a backup job. To do that, log in to the web console, switch to the Protected VMs page, click View as tree, and click the job name to expand the list of backed-up VMs and their restore points. Then, select the restore points you want to remove and click Delete.

Note that at least one restore point must remain for each VM. Otherwise, the VM backup files will be permanently deleted from backup repositories.

Deleting Backups From Disk

To delete backup files created for an RHV VM, 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, expand the job that created the backup, right-click the VM name and select Delete from disk.

NOTE
When you delete backup files using the Veeam Backup & Replication console, the list of available backups in the RHV backup proxy web console is not updated automatically. To update the list manually, perform the backup import operation.
You can also delete backup files created by a backup job for an RHV VM using the RHV backup proxy web console. To do that, log in to the web console, switch to the Protected VMs page, click View as tree, and click the job name to expand the list of backed-up VMs and their restore points. Then, click the VM to select all its restore points and click Delete.
Performing Restore

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

- **Entire VM restore** — recover RHV VMs to the original location or to a new location.
- **VM disk restore** — recover a specific VM disk and attach it to the original VM or to another VM.
- **Instant VM recovery** — instantly start an RHV VM directly from a backup.
- **File-level restore** — recover individual VM guest OS files and folders.
- **VM disk export** — restore VM disks and convert them to disks of the VMDK, VHD or VHDX format.
- **Restore to Amazon AWS** — restore RHV VMs to Amazon Web Services as EC2 instances.
- **Restore to Microsoft Azure** — restore RHV VMs to Microsoft Azure as VMs.
- **Restore to Google Cloud** — restore RHV VMs to Google Cloud as VM instances.

You can restore VM data to the most recent state or to any available restore point.
Performing VM Restore

In case of a disaster, you can restore an entire RHV VM from a backup. Veeam Backup for RHV allows you to restore one or more VMs at a time, to the original location or to a new location.

How VM Restore Works

During the VM restore process, the following steps are performed:

1. The Veeam Backup & Replication console sends the restore session configuration data to the RHV backup proxy.
   If multiple VMs are added to the restore session, these VMs are processed in parallel.
2. [This step applies only if you perform restore to the original location and if the source VM is still present in the location] The RHV backup proxy powers off the source VM and removes it from the RHV infrastructure.
3. The RHV backup proxy connects to the target RHV host over REST API and creates a VM in the target location.
4. The RHV backup proxy creates empty virtual disks in the target location. The number of empty disks equals the number of disks attached to the source VM.
5. The RHV backup proxy connects to the backup repository and restores backed-up data to the empty disks.
   If multiple disks are attached to the source VM, the RHV backup proxy restores these disks sequentially, one disk at a time.
6. The RHV backup proxy attaches the created disks with the restored data to the VM.

How to Perform VM Restore

To restore a protected VM, you can use either the Veeam Backup & Replication console or the RHV backup proxy web console. However, only the Veeam Backup & Replication console allows you to restore multiple VMs at a time and to choose a location for the restored VMs.

NOTE

The SureBackup feature that allows you to verify any restore point of a backed-up VM is not supported for backups created with Veeam Backup for RHV.
Restoring VMs Using Veeam Backup & Replication Console

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

To restore a protected VM, do the following:

1. Launch the Full VM Restore to Red Hat Virtualization wizard.
2. Select a restore point.
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. Configure 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**.

**TIP**

Alternatively, you can launch the **Full VM Restore to Red Hat Virtualization** wizard from the **Home** view of the Veeam Backup for RHV console. To do that, expand the necessary backup, select the VM that you want to restore and select **Restore > RHV** on the ribbon.
Step 2. Select Restore Point

At the Virtual Machines step of the wizard, select a restore point that will be used to restore the selected VM. By default, Veeam Backup for RHV uses the most recent valid restore point. However, you can restore the VM data to an earlier state.

To select a restore point, do the following:

1. Select the VM.
2. Click Point.
3. In the Restore Points window, select the necessary restore point and click OK.

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 that created the restore point and the date when the restore point was created.
- **Type** — the type of the restore point.
- **Location** — the repository where the restore point is stored.
Step 3. Choose Restore Mode

At the **Restore Mode** step of the wizard, choose whether you want to restore the selected VM to the original or to a custom location. You can also choose whether you want the recovered VM to have the same tags as the original VM.

**TIP**

You can instruct Veeam Backup for RHV to restore disks attached to the recovered VM in the QCOW2 format. This will **increase speed and efficiency of incremental backups** further created for the VM.
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 recovered VM will belong.

For a cluster to be displayed in the list of the available clusters, it must be added to the RHV infrastructure as described in Red Hat Virtualization documentation.
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 virtual disks of the recovered VM will be stored.

For a domain to be displayed in the list of the available domains, it must be configured in the RHV infrastructure as described in Red Hat Virtualization documentation.
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)

At the **Name** step of the wizard, you can specify a new name for the recovered VM.

**TIP**

If you want the recovered VM to have the same ID as the original VM, select the **Preserve virtual machine ID** check box. However, in this case Veeam Backup for RHV will remove the original VM if it is still present in the RHV infrastructure.
Step 7. Configure 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 a network to which the recovered VM will be connected. If you do not want to connect the VM to any virtual network, select the VM and click Disconnect.

For a network to be displayed in the list of the available networks, it must be configured in the RHV infrastructure as described in Red Hat Virtualization documentation.
Step 8. Specify Restore Reason

At the **Reason** step of the wizard, specify a reason for restoring the VM. This information will be saved to the session history, and you will be able to reference it later.
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 recovered VM 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 RHV VM to the cluster where the original VM belongs.

To restore a protected VM, do the following:

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

Step 1. Launch Full VM Restore Wizard

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

1. Switch to the Protected VMs page.
2. Click the VM that you want to restore.
3. On the Restore Points page, click Restore.
Step 2. Select Restore Point

At the Virtual Machine step of the wizard, select a restore point that will be used to restore the selected VM. By default, Veeam Backup for RHV uses the most recent valid restore point. However, you can restore the VM data to an earlier state.

To select a restore point, do the following:

1. Click **Point**.
2. In the Restore Points window, select the necessary restore point and click **OK**.

   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 that created the restore point.
   - **Date** — the date when the restore point was created.
   - **Type** — the type of the restore point.
Step 3. Choose Restore Mode

At the **Restore Mode** step, choose whether you want to restore the VM with the original settings or to specify new settings (such as VM network and disk storage settings).
Step 4. Specify VM Name

[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 **Name** step of the wizard, you can specify a new name for the recovered VM.

**TIP**

If you want the recovered VM to have the same ID as the original VM, select the **Preserve virtual machine ID** check box. However, in this case Veeam Backup for RHV will remove the original VM if it is still present in the RHV infrastructure.
**Step 5. 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, choose a storage domain where virtual disks of the recovered VM will be stored.

For a domain to be displayed in the list of the available domains, it must be configured in the RHV infrastructure as described in *Red Hat Virtualization documentation*. 

---

**Screenshot of the Storage Domain Step**

1. Virtual Machine
2. Restore Mode
3. Name
4. Storage Domain
5. Network Settings
6. Reason
7. Summary

**Storage Domain**

By default, original storage domain and disk type are used for each VM disk. You can change storage domain by clicking "Domain" button.

<table>
<thead>
<tr>
<th>Disk</th>
<th>Size</th>
<th>Domain</th>
<th>Disk type</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMS_Server</td>
<td>64 GB</td>
<td>ISCSI_SSD</td>
<td>VIRTIQ_SCSI</td>
</tr>
<tr>
<td>disk0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>disk1</td>
<td>128 MB</td>
<td>ISCSI_SSD</td>
<td>VIRTIQ_SCSI</td>
</tr>
</tbody>
</table>

**Select Domain**

Select Domain:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdcqap18kowrcrobofish.local</td>
<td>Active</td>
</tr>
<tr>
<td>hosted_storage</td>
<td>Active</td>
</tr>
<tr>
<td>ISCSI_SSD</td>
<td>Active</td>
</tr>
<tr>
<td>ISCSI_SSD</td>
<td>Active</td>
</tr>
<tr>
<td>NFS_SSD</td>
<td>Active</td>
</tr>
</tbody>
</table>

[OK] [Cancel]
Step 6. Configure 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 step of the wizard, choose a network to which the recovered VM will be connected. If you do not want to connect the VM to any virtual network, click Disconnected.

For a network to be displayed in the list of the available networks, it must be configured in the RHV infrastructure as described in Red Hat Virtualization documentation.
Step 7. Specify Reason for Restore

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

Reason

Enter the reason for performing this restore operation. This information will be logged in the restore session's history for later reference.

Restoring failed VM
Step 8. Finish Working with Wizard

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

If you want to start the recovered VM as soon as the restore process completes, select the **Power on target VM after restore** check box. If you want the recovered VM to have the same tags as the original VM, select the **Restore VM tags** check box.

**TIP**

You can instruct Veeam Backup for RHV to restore disks attached to the recovered VM in the QCOW2 format. This will increase speed and efficiency of incremental backups further created for the VM.
Performing Disk Restore

In case a disaster strikes, you can restore a disk of an RHV VM from a backup. Veeam Backup for RHV allows you to attach the restored disk to the original VM or any other RHV VM in the RHV infrastructure.

NOTE

You can restore only one virtual disk per restore session.

How Disk Restore Works

During the VM disk restore process, the following steps are performed:

1. The RHV backup proxy web console sends the restore session configuration data to the RHV backup proxy.
2. The RHV backup proxy powers off the target VM.
3. The RHV backup proxy creates an empty virtual disk in the RHV infrastructure.
4. The RHV backup proxy connects to the backup repository and restores backed-up data to the empty disk.
5. [This step applies only if you restore the disk to the original VM and if you choose to replace the existing disk] The RHV backup proxy detaches the original disk from the VM and removes it from the RHV infrastructure.
6. The RHV backup proxy attaches the created disk with the restored data to the target VM.

How to Perform Disk Restore

To restore a disk attached to a protected VM, do the following:

1. Launch the Virtual Disk Restore wizard.
2. Select a virtual machine.
3. Select a restore point.
5. Specify a reason for the restore.
6. Finish working with the wizard.
Step 1. 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**.
Step 2. Select Virtual Machine

At the Virtual Machine step of the wizard, expand the backup job tree and select the VM whose virtual disk you want to restore.
Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point that will be used to restore data. By default, Veeam Backup for RHV uses the most recent valid restore point. However, you can restore the data to an earlier state.
Step 4. Configure Mapping Settings

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

1. Choose a target VM to which you want to attach the restored disk.
   
   By default, Veeam Backup for RHV attaches the restored disk to the original VM. To attach the disk to another VM, click **Browse**.

   **IMPORTANT**
   
   During disk restore, Veeam Backup for RHV turns off the target VM to reconfigure its settings and attach the restored disk. It is recommended that you stop all activities on the target VM till the restore session completes.

2. Select a virtual disk to restore.
   
   By default, Veeam Backup for RHV attaches the restored disk to the target VM as a new disk. If you want the restored disk to replace the existing disk, or if you want to change the disk bus type and to specify a storage domain for the restored disk, click **Change**.

   **TIP**
   
   You can instruct Veeam Backup for RHV to restore the disk in the QCOW2 format. This will increase speed and efficiency of incremental backups further created for the VM.
Step 5. Specify Reason for Restore

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

![Reason step of the wizard](image)
Step 6. Finish Working with Wizard

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

**TIP**

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

With Instant VM Recovery, you can immediately restore RHV VMs as VMware vSphere, Microsoft Hyper-V or Nutanix AHV VMs to your production environment by running them directly from their backups. Instant VM Recovery helps you improve recovery time objectives, minimize disruption and downtime of production workloads. For more information on Instant VM Recovery, see the Veeam Backup & Replication User Guide, section VM Recoveryhttps://helpcenter.veeam.com/docs/backup/vsphere/vm_restores.html?ver=110.

To perform Instant VM 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, right-click the VM you want to restore, and select Instant Recovery.
   - To restore the VM to VMware vSphere, complete the Instant Recovery wizard as described in the Veeam Backup & Replication User Guide for VMware vSphere, section Performing Instant VM Recovery of Workloads to VMware vSphere VMs.
   - To restore the VM to Microsoft Hyper-V, complete the Instant Recovery wizard as described in the Veeam Backup & Replication User Guide for Microsoft Hyper-V, section Performing Instant VM Recovery of Workloads to Hyper-V VMs.
   - To restore the VM to Nutanix AHV, complete the Instant Recovery wizard as described in the Veeam Backup for Nutanix AHV User Guide, section Performing Instant VM Recovery of Workloads to Nutanix AHV.
Performing File-Level Restore

With guest OS file recovery (file-level restore), you can restore individual guest OS files and folders from RHV VM backups created with Veeam Backup for RHV. When restoring files and folders, you do not need to extract the VM image to a staging location or start the VM prior to restore. For more information on VM guest OS file restore, see the Veeam Backup & Replication User Guide, section Guest OS File Recovery.

To restore VM guest OS files and folders, 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 VM that contains files you want to restore and do the following:
   - If you want to restore files of a Microsoft Windows machine, select Restore guest files > Microsoft Windows and complete the Guest File Restore wizard as described in the Veeam Backup & Replication User Guide, section Restoring VM Guest OS Files (FAT, NTFS or ReFS).
   - If you want to restore files of a Linux, Solaris, BSD, Novell Storage Services, Unix or Mac machine, select Restore guest files > Linux and others and complete the Guest File Restore wizard as described in the Veeam Backup & Replication User Guide, section Restoring VM Guest OS Files (Multi-OS).

TIP

Alternatively, you can use Veeam Backup Enterprise Manager to restore guest OS files and folders as described in the Veeam Backup Enterprise Manager Guide, section Restoring VM Guest OS Files.
Exporting Disks

Veeam Backup for RHV allows you to export disks, that is, restore disks from RHV VM backups and convert them to the VMDK, VHD and VHDX formats. You can save the exported disks to any server added to the backup infrastructure or place the disks on a datastore connected to an ESXi host (for the VMDK disk format only). For more information, see the Veeam Backup & Replication User Guide, section Disk Export.

To export disks of an RHV VM, 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 VM that contains disks you want to export and select Export content as virtual disks.
Performing VM Restore to Amazon Web Services

Veeam Backup for RHV allows you to restore RHV VMs to Amazon Web Services (AWS) as EC2 instances. For more information, see the Veeam Backup & Replication User Guide, section Restore to Amazon EC2.

To restore a VM to Amazon EC2, 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 VM that you want to restore and select Restore to Amazon EC2.
4. Complete the Restore to Amazon EC2 wizard as described in the Veeam Backup & Replication User Guide, section Restoring to Amazon EC2.
Performing VM Restore to Microsoft Azure

Veeam Backup for RHV allows you to restore RHV VMs to Microsoft Azure as VMs. For more information, see the Veeam Backup & Replication User Guide, section Restore to Microsoft Azure.

To restore a VM to Microsoft Azure, 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 VM that you want to restore and select Restore to Microsoft Azure.
Performing VM Restore to Google Cloud

Veeam Backup for RHV allows you to restore RHV VMs to Google Cloud as VM instances. For more information, see the Veeam Backup & Replication User Guide, section Restore to Google Compute Engine.

To restore a VM to Google Cloud, 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 VM that you want to restore and select **Restore to Google CE**.
4. Complete the **Restore to Google Compute Engine** wizard as described in the Veeam Backup & Replication User Guide, section **Restoring to Google Compute Engine**.
Monitoring Events

For each performed data protection or disaster recovery operation, Veeam Backup for RHV starts a new session and creates a record in the configuration database. You can track real-time statistics of all running and completed operations on the Events page.

To view the full list of tasks executed during an operation, click the link in the Date column. Use the Type drop-down list to filter operations by type (for example, to display all operations completed with warnings or errors).

To mark a warning or error operation that you have already seen, select the check box next to the operation and click Resolve — the review time will be displayed in the Resolved column. Use the Resolved drop-down list to filter operations by status (for example, to display all operations you have not marked as resolved yet).
Updating RHV Backup Proxy

Veeam Backup for RHV allows you to check for new product versions and available package updates, download and install them right from the RHV backup proxy web console.

It is recommended that you timely install available updates to avoid issues while working with the product. For example, timely installed security updates may help you prevent potential security issues and reduce the risk of compromising sensitive data.

Checking for Updates

Veeam Backup for RHV automatically notifies you about newly released product versions and package updates available for the operating system running on the backup proxy. However, you can check for the available updates manually if required:

1. Click the Settings icon at the top right corner of the RHV backup proxy web console, and select Appliance Settings.
2. Switch to the Updates tab.
3. Click Check and View Updates.

If new updates are available, Veeam Backup for RHV will display them on the Updates tab of the Veeam Updater page. To view detailed information on an update, select the check box next to the update and click What's new?
Installing Updates

To download and install new product versions and available package updates, you can use either of the following options:

- Install updates immediately
- Schedule update installation

You can also set a reminder to send update notifications.

**IMPORTANT**

You can update the Veeam Backup for RHV using the Veeam updater service only. Updating of the backup proxy manually is not supported.

Installing Updates

**IMPORTANT**

Before you install a product update, make sure all backup jobs are stopped and restore tasks are finished. Otherwise, the update process will interrupt the running activities, which may result in data loss.

To download and install available product and package updates:

1. Open the Veeam Updater page:
   a. Click the Settings icon at the top right corner of the RHV backup proxy web console, and select Appliance Settings.
   b. Switch to the Updates tab.
   c. Click Check and View Updates.

2. On the Veeam Updater page, do the following:
   a. In the Updates are available for this system section, select check boxes next to the necessary updates.
   b. In the Choose action section, select the Install updates now option, select the Reboot automatically after install if required check box to allow Veeam Backup for RHV to reboot the backup proxy if needed, and then click Install Updates Now.

**NOTE**

The updater may require you to read and accept the Veeam license agreement and the 3rd party components license agreement. If you reject the agreements, you will not be able to continue installation.
Veeam Backup for RHV will download and install the updates; the results of the installation process will be displayed on the History tab. Keep in mind that it may take several minutes for the installation process to complete.

**NOTE**

When installing product updates, Veeam Backup for RHV restarts all services running on the backup proxy, including the Web UI service. That is why Veeam Backup for RHV will log you out when the update process completes.
Scheduling Update Installation

You can instruct Veeam Backup for RHV to automatically download and install available product versions and package updates on a specific date at a specific time:

1. On the Veeam Updater page, in the Updates are available for this system section, select check boxes next to the necessary updates.

2. In the Choose action section, do the following:
   a. Select the Schedule updates installation option and configure the necessary schedule.

   IMPORTANT
   When selecting a date and time for the update installation, make sure no backup jobs are scheduled to run on the selected time. Otherwise, the update process will interrupt the running activities, which may result in data loss.

   b. Select the Reboot automatically after install if required check box to allow Veeam Backup for RHV to reboot the backup proxy if needed.

   c. Click Schedule Updates.

Veeam Backup for RHV will automatically download and install the updates on the selected date at the selected time; the results of the installation process will be displayed on the History tab.
Setting Update Reminder

If you have not decided when to install available product versions and package updates, you can set an update reminder — instruct Veeam Backup for RHV to send an update notification later.

To do that, on the Veeam Updater page, in the Choose action section, do the following:

1. Select the Remind me later option and choose when you want to receive the reminder.

   If you select the Next Week option, Veeam Backup for RHV will send the reminder next Monday.

2. Click Remind me later.
Viewing Update History

To see the results of the update installation performed on the 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. Switch to the **Updates** tab.

3. Click **Check and View Updates**.

4. On the **Veeam Updater** page, switch to the **History** tab.

For each date when an update was installed, the **Veeam Updater** page will display the name of the update and its status (whether the installation process completed successfully, completed with warnings or failed to complete).

To download logs for the installed updates, select the necessary date in the **Date** section, and click **View Full Log**. Veeam Backup for RHV will save the logs as a single file to the default download directory on the local machine.
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.

Viewing Product Details

To view 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. Switch to the **Summary** tab.

The **Summary** tab displays the following information:

- **Appliance Hostname** — the hostname of the VM running as RHV backup proxy.
- **Product** — the name of the solution.
- **Appliance Version** — the currently installed version of Veeam Backup for RHV.
Exporting Logs Using RHV Backup Proxy Web Console

To collect logs from 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.

3. In the Support Bundle window, choose whether you want to collect logs for the Veeam Backup Agent service, Veeam Data Mover service, Veeam internal API service and Veeam Updater service.

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

To collect logs for the RHV backup proxy from 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.