© 2022 Veeam Software.

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

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

NOTE

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTACTING VEEAM SOFTWARE</td>
<td>8</td>
</tr>
<tr>
<td>ABOUT THIS DOCUMENT</td>
<td>12</td>
</tr>
<tr>
<td>OVERVIEW</td>
<td>14</td>
</tr>
<tr>
<td>Solution Architecture</td>
<td>15</td>
</tr>
<tr>
<td>Standalone and Managed Operation Modes</td>
<td>16</td>
</tr>
<tr>
<td>Data Backup</td>
<td>17</td>
</tr>
<tr>
<td>Backup Types</td>
<td>18</td>
</tr>
<tr>
<td>How Backup Works</td>
<td>23</td>
</tr>
<tr>
<td>Backup Job</td>
<td>28</td>
</tr>
<tr>
<td>Backup Repository</td>
<td>34</td>
</tr>
<tr>
<td>Backup Chain</td>
<td>37</td>
</tr>
<tr>
<td>Backup of Database Systems</td>
<td>44</td>
</tr>
<tr>
<td>Data Restore</td>
<td>58</td>
</tr>
<tr>
<td>Volume-Level Restore</td>
<td>59</td>
</tr>
<tr>
<td>File-Level Restore</td>
<td>61</td>
</tr>
<tr>
<td>Veeam Recovery Media</td>
<td>62</td>
</tr>
<tr>
<td>Veeam Recovery Media Versions</td>
<td>63</td>
</tr>
<tr>
<td>Drivers in Veeam Recovery Media</td>
<td>66</td>
</tr>
<tr>
<td>Integration with Veeam Backup &amp; Replication</td>
<td>67</td>
</tr>
<tr>
<td>Backup to Veeam Cloud Connect Repository</td>
<td>69</td>
</tr>
<tr>
<td>Managing Veeam Agent in Veeam Backup &amp; Replication</td>
<td>70</td>
</tr>
<tr>
<td>PLANNING AND PREPARATION</td>
<td>71</td>
</tr>
<tr>
<td>System Requirements</td>
<td>72</td>
</tr>
<tr>
<td>Used Ports</td>
<td>82</td>
</tr>
<tr>
<td>Live Patching Support</td>
<td>84</td>
</tr>
<tr>
<td>INSTALLATION AND CONFIGURATION</td>
<td>85</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>86</td>
</tr>
<tr>
<td>Installing Veeam Agent for Linux</td>
<td>87</td>
</tr>
<tr>
<td>Installing Veeam Agent for Linux in Offline Mode</td>
<td>91</td>
</tr>
<tr>
<td>Upgrading Veeam Agent for Linux</td>
<td>99</td>
</tr>
<tr>
<td>Granting Permissions to Users</td>
<td>106</td>
</tr>
<tr>
<td>Performing Initial Setup</td>
<td>107</td>
</tr>
<tr>
<td>Step 1. Accept License Agreements</td>
<td>108</td>
</tr>
<tr>
<td>Step 2. Create Custom Veeam Recovery Media</td>
<td>109</td>
</tr>
<tr>
<td>Step 3. Install Product License</td>
<td>112</td>
</tr>
<tr>
<td>Configuring Advanced Settings</td>
<td>114</td>
</tr>
</tbody>
</table>
Managing Veeam Agent Operation Mode ................................................................. 117
Viewing Operation Mode .......................................................................................... 118
Resetting to Standalone Operation Mode ............................................................... 119
Connecting to Veeam Backup & Replication ........................................................ 120
Synchronizing with Veeam Backup Server ............................................................ 121
Exporting Logs to Veeam Backup Server .............................................................. 122
Uninstalling Veeam Agent for Linux ......................................................................... 123
GETTING STARTED ................................................................................................. 124
GETTING TO KNOW USER INTERFACE ............................................................... 125
Veeam Agent for Linux Control Panel ................................................................. 126
Command Line Interface ....................................................................................... 128
Viewing Help ......................................................................................................... 130
LICENSING ............................................................................................................. 131
Product Editions .................................................................................................... 132
License Agreement ............................................................................................... 134
Installing License ................................................................................................. 135
Viewing License Information .............................................................................. 137
Removing License ............................................................................................... 138
License Expiration ............................................................................................... 139
Managing License with Command Line Interface .............................................. 140
Accepting License Agreements ........................................................................... 141
Installing License ................................................................................................ 142
Viewing License Information .............................................................................. 143
Removing License ............................................................................................... 144
PERFORMING BACKUP ......................................................................................... 145
Creating Custom Veeam Recovery Media ........................................................... 146
Creating Custom Veeam Recovery Media with Control Panel ....................... 147
Creating Custom Veeam Recovery Media with Command Line Interface ........ 150
Veeam Recovery Media ISO Files ........................................................................ 153
Creating Backup Jobs .......................................................................................... 154
Creating Backup Job with Backup Job Wizard ................................................. 155
Creating Backup Job with Command Line Interface ...................................... 204
Starting and Stopping Backup Jobs ..................................................................... 250
Starting Backup Job from Control Panel ......................................................... 251
Starting Backup Job from Command Line Interface ...................................... 252
Creating Active Full Backups ............................................................................ 253
Stopping Backup Job .......................................................................................... 254
Managing Backup Jobs ....................................................................................... 257
Viewing List of Backup Jobs .............................................................................. 258
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Backup Job Settings</td>
<td>259</td>
</tr>
<tr>
<td>Editing Backup Job Settings</td>
<td>261</td>
</tr>
<tr>
<td>Deleting Backup Job</td>
<td>267</td>
</tr>
<tr>
<td>Managing Backup Repositories</td>
<td>270</td>
</tr>
<tr>
<td>Creating Backup Repository</td>
<td>271</td>
</tr>
<tr>
<td>Viewing List of Backup Repositories</td>
<td>276</td>
</tr>
<tr>
<td>Editing Backup Repository</td>
<td>277</td>
</tr>
<tr>
<td>Rescanning Veeam Backup Repository</td>
<td>281</td>
</tr>
<tr>
<td>Deleting Backup Repository</td>
<td>282</td>
</tr>
<tr>
<td>Managing Veeam Backup &amp; Replication Servers</td>
<td>283</td>
</tr>
<tr>
<td>Connecting to Veeam Backup Server</td>
<td>284</td>
</tr>
<tr>
<td>Viewing List of Veeam Backup Servers</td>
<td>286</td>
</tr>
<tr>
<td>Viewing Backup Server Details</td>
<td>287</td>
</tr>
<tr>
<td>Editing Connection to Veeam Backup Server</td>
<td>288</td>
</tr>
<tr>
<td>Updating List of Veeam Backup Repositories</td>
<td>293</td>
</tr>
<tr>
<td>Deleting Connection to Veeam Backup Server</td>
<td>294</td>
</tr>
<tr>
<td>Managing Service Providers</td>
<td>295</td>
</tr>
<tr>
<td>Connecting to Service Provider</td>
<td>296</td>
</tr>
<tr>
<td>Viewing List of Service Providers</td>
<td>297</td>
</tr>
<tr>
<td>Editing Connection to Service Provider</td>
<td>298</td>
</tr>
<tr>
<td>Updating List of Cloud Repositories</td>
<td>303</td>
</tr>
<tr>
<td>Deleting Connection to Service Provider</td>
<td>304</td>
</tr>
<tr>
<td>Managing Backups</td>
<td>305</td>
</tr>
<tr>
<td>Viewing Backups</td>
<td>306</td>
</tr>
<tr>
<td>Viewing Backup Details</td>
<td>308</td>
</tr>
<tr>
<td>Viewing Restore Points in Backup</td>
<td>310</td>
</tr>
<tr>
<td>Importing Backups</td>
<td>311</td>
</tr>
<tr>
<td>Deleting Backups</td>
<td>314</td>
</tr>
<tr>
<td>PERFORMING RESTORE</td>
<td>317</td>
</tr>
<tr>
<td>Restoring from Veeam Recovery Media</td>
<td>318</td>
</tr>
<tr>
<td>Restoring Volumes</td>
<td>319</td>
</tr>
<tr>
<td>Restoring Files and Folders</td>
<td>360</td>
</tr>
<tr>
<td>Restoring Volumes with Command Line Interface</td>
<td>392</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>393</td>
</tr>
<tr>
<td>Restoring from Backup</td>
<td>394</td>
</tr>
<tr>
<td>Restoring from Restore Point</td>
<td>400</td>
</tr>
<tr>
<td>Restoring Files and Folders with Recovery Wizard</td>
<td>407</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>408</td>
</tr>
<tr>
<td>Step 1. Launch File Level Restore Wizard</td>
<td>409</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Step 2. Select Backup and Restore Point</td>
<td>410</td>
</tr>
<tr>
<td>Step 3. Save Restored Files</td>
<td>414</td>
</tr>
<tr>
<td>Step 4. Stop Backup Mount Session</td>
<td>415</td>
</tr>
<tr>
<td>Restoring Files and Folders with Command Line Interface</td>
<td>416</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>417</td>
</tr>
<tr>
<td>Restoring from Backup</td>
<td>418</td>
</tr>
<tr>
<td>Restoring from Restore Point</td>
<td>427</td>
</tr>
<tr>
<td>Exporting Backup to Virtual Disk</td>
<td>436</td>
</tr>
<tr>
<td>Exporting Backups</td>
<td>437</td>
</tr>
<tr>
<td>Exporting Restore Points</td>
<td>439</td>
</tr>
<tr>
<td>Restoring Data from Encrypted Backups</td>
<td>441</td>
</tr>
<tr>
<td>REPORTING</td>
<td>445</td>
</tr>
<tr>
<td>Viewing Job Session Progress</td>
<td>446</td>
</tr>
<tr>
<td>Viewing Real-Time Job Session Statistics</td>
<td>447</td>
</tr>
<tr>
<td>Viewing Job Session Result</td>
<td>450</td>
</tr>
<tr>
<td>Viewing Session Status</td>
<td>452</td>
</tr>
<tr>
<td>Viewing Session Logs</td>
<td>454</td>
</tr>
<tr>
<td>MANAGING CONFIGURATION DATABASE</td>
<td>455</td>
</tr>
<tr>
<td>Exporting Configuration Database</td>
<td>456</td>
</tr>
<tr>
<td>Importing Configuration Database</td>
<td>457</td>
</tr>
<tr>
<td>EXPORTING PRODUCT LOGS</td>
<td>458</td>
</tr>
<tr>
<td>Exporting Logs with Control Panel</td>
<td>459</td>
</tr>
<tr>
<td>Exporting Logs with Command Line Interface</td>
<td>461</td>
</tr>
<tr>
<td>GETTING SUPPORT</td>
<td>462</td>
</tr>
<tr>
<td>USING WITH VEEAM BACKUP &amp; REPLICATION</td>
<td>463</td>
</tr>
<tr>
<td>Setting Up User Permissions on Backup Repositories</td>
<td>465</td>
</tr>
<tr>
<td>Managing License</td>
<td>468</td>
</tr>
<tr>
<td>Mananging Instance Consumption by Veeam Agents</td>
<td>469</td>
</tr>
<tr>
<td>Assigning License to Veeam Agent</td>
<td>470</td>
</tr>
<tr>
<td>Viewing Licensed Agents and Revoking License</td>
<td>471</td>
</tr>
<tr>
<td>Performing Data Protection Tasks</td>
<td>474</td>
</tr>
<tr>
<td>Backing Up to Backup Repositories</td>
<td>475</td>
</tr>
<tr>
<td>Backing Up to Cloud Repositories</td>
<td>476</td>
</tr>
<tr>
<td>Performing Backup Copy for Veeam Agent Backups</td>
<td>479</td>
</tr>
<tr>
<td>Archiving Veeam Agent Backups to Tape</td>
<td>481</td>
</tr>
<tr>
<td>Performing Restore Tasks</td>
<td>482</td>
</tr>
<tr>
<td>Restoring Veeam Agent Backup to vSphere VM</td>
<td>483</td>
</tr>
<tr>
<td>Restoring Veeam Agent Backup to Hyper-V VM</td>
<td>485</td>
</tr>
<tr>
<td>Restoring Veeam Agent Backup to Nutanix AHV VM</td>
<td>486</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 user guide provides information about Veeam Agent for Linux.
Intended Audience

The user guide is intended for anyone who wants to use Veeam Agent for Linux 5.0 or later to protect their machine.
Overview

Veeam Agent for Linux is a data protection and disaster recovery solution for physical endpoints and virtual machines running Linux-based operating systems.

Veeam Agent can be used by IT administrators who run Linux infrastructure to protect different types of computers and devices: servers, desktops and laptops. The solution runs inside the guest OS and does not need access to virtualization infrastructure components. Thus, Veeam Agent can be used to protect Linux server instances deployed in the public cloud, for example, in Microsoft Azure environment.

NOTE

Veeam Agent can operate in either standalone or managed mode. Depending on the mode, Veeam Agent provides different features and limitations. To learn more, see Standalone and Managed Operation Modes.

Veeam Agent offers a variety of features to protect your data. You can create an entire system image backup, back up specific machine volumes or individual directories and files. Backups can be stored on a local hard drive, on an external hard drive, in a network shared folder or on a Veeam backup repository.

In case of a disaster, you can perform the following restore operations:

- Start the OS from the Veeam Recovery Media and use standard Linux command line tools to diagnose and fix problems.
- Perform bare metal restore.
- Restore necessary data from backups to its original location or a new location.

Veeam Agent integrates with Veeam Backup & Replication. Backup administrators who work with Veeam Backup & Replication can perform advanced tasks with Veeam Agent backups: restore files and disks from backups, manage backup jobs configured in Veeam Agent or backups created with these jobs.
Solution Architecture

Veeam Agent for Linux is set up on a Linux-based physical endpoint or virtual machine whose data you want to protect.

When you install the product, Veeam Agent deploys the following components:

- **Veeam Agent for Linux Service (veeamservice)** is a service responsible for managing all tasks and resources in Veeam Agent. The veeamservice component is registered as a daemon in the Linux OS upon the product installation. The service is started automatically when you start the OS, and runs in the background.

- **Veeam Agent for Linux Job Manager (veeamjobman)** is a process started by Veeam Agent for Linux Service for every backup job session.

- **Veeam Agent** that communicates with the Veeam Agent for Linux Service and Veeam Agent for Linux Job Manager. Veeam Agent is started by Veeam Agent for Linux Manager to perform data transfer operations of any kind: copy data from the backed-up volume to the backup location during backup, from the backup location to the target volume during restore, perform data compression, and so on.

- **Veeam Agent for Linux Driver (veeamsnap)** is a Veeam driver (Linux kernel module) used to create volume snapshots in the Linux OS and keep track of changed data blocks.

- To store its configuration data, Veeam Agent uses the SQLite database engine. SQLite requires only few files to install and takes little resources to run on a Linux OS.
Standalone and Managed Operation Modes

Veeam Agent for Linux can operate in two modes: *standalone mode* and *managed mode*.

- **Standalone mode** — in this mode, Veeam Agent for Linux operates as a standalone product. To use Veeam Agent operating in the standalone mode, you must manually install the product directly on the machine whose data you want to protect.

  For Veeam Agent for Linux operating in the standalone mode, data protection, disaster recovery, and administration tasks are performed in Veeam Agent by a user. You can also use Veeam Agent operating in the standalone mode with Veeam Backup & Replication. In this scenario, you can use a Veeam backup repository as a target location for Veeam Agent backups and use the Veeam Backup & Replication console to perform a number of tasks with Veeam Agent backup jobs and backups.

  The current User Guide covers subjects related to Veeam Agent for Linux operating in the standalone mode only.

- **Managed mode** — in this mode, Veeam Agent for Linux operates under control from Veeam Backup & Replication. To use Veeam Agent operating in the managed mode, you must deploy the product in one of the following ways:

  - remotely from Veeam Backup & Replication
  - manually using external tools

    To learn more about managed Veeam Agent deployment, see the Protected Computers Discovery and Veeam Agent Deployment section in the Agent Management Guide

  For Veeam Agent for Linux operating in the managed mode, data protection, disaster recovery, and administration tasks are performed by a backup administrator in the Veeam Backup & Replication console.

  Features and limitations of Veeam Agent for Linux operating in the managed mode are different from those in the standalone mode. To learn about Veeam Agent operating in the managed mode, see the Agent Management Guide.
Data Backup

It is recommended that you regularly back up data stored on your machine. Backup creates a safety copy of your data. If any kind of disaster strikes, you can restore your data from the backup and be sure that you will not lose the necessary information.

You can set up Veeam Agent to perform automatic scheduled backups (triggered at specific time of the day), or you can choose to back up data manually when needed. You can back up the entire computer image, specific computer volumes or individual directories and files.

You can set up Veeam Agent to create multiple backups — with individual backup scope, upon individual schedule or in different locations. This functionality is available if Veeam Agent operates in the Server edition. To learn more about editions, see Product Editions.

Backups created with Veeam Agent can be saved to the following locations:

- Removable storage device
- Local computer drive
- NFS or SMB (CIFS) network shared folder
- Backup repository managed by a Veeam backup server
- Veeam Cloud Connect repository
Backup Types

Veeam Agent for Linux lets you create the following backup types:

- Volume-level backup
- File-level backup
Volume-Level Backup

You can set up Veeam Agent for Linux to create volume-level backup. The volume-level backup captures the whole image of a data volume on your computer. You can use the volume-level backup to restore a computer volume, specific files and folders on the volume or perform bare metal recovery.

Veeam Agent for Linux supports backup of the following types of computer volumes:

- Simple volumes
- LVM logical volumes
- Btrfs subvolumes

You can back up all computer volumes or specific computer volumes.

- When you back up the entire computer image, Veeam Agent captures the content of all volumes on your computer. The resulting backup file contains all volume data and Linux OS system data: system partition, partition table and bootloader.

- When you back up a specific computer volume, Veeam Agent captures only the data that resides on this specific volume: files, folder, application data and so on.

If you choose to back up the system volume (volume to which the root file system is mounted), Veeam Agent automatically includes the bootloader into the backup scope.
File-Level Backup

You can set up Veeam Agent for Linux to create file-level backup. The file-level backup captures only data of individual directories and files on the computer. You can use the file-level backup to restore files and directories that you have added to the backup scope.

With Veeam Agent for Linux, you can specify which files and directories to back up:

- You can include individual directories in the backup. When you include a directory in the backup, its subdirectories are automatically included in the backup too. When you recover from such backup, you will be able to restore directories that you have selected to back up, all subdirectories of these directories and files in these directories.

- You can exclude from the backup some subdirectories of the directories that are included in the backup. When you recover from such backup, you will be able to restore directories that you have selected to back up, specific subdirectories of these directories and files in these directories.
You can include or exclude files of a specific type in/from the backup. You can specify file names explicitly or use UNIX wildcard characters to define include and exclude file name masks. When you recover from such backup, you will be able to restore directories that you have selected to back up with files whose names match the specified include masks.
Snapshot-Less File-Level Backup

You can set up Veeam Agent for Linux to create file-level backup in the snapshot-less mode. This allows you to back up data that resides in any file system mounted to the root file system of the Veeam Agent computer. For example, you can use the snapshot-less mode to back up data that resides in a file system that is not supported for snapshot-based backup with Veeam Agent, such as UFS, ZFS, GFS, GFS2 or OCFS2. You can also use it to back up data that resides in an NFS or CIFS network shared folder.

To create backups in the snapshot-less mode, you must enable this mode in the properties of the file-level backup job. To learn more, see Creating Backup Jobs.

In the snapshot-less mode, Veeam Agent does not create a snapshot of the backed-up volume. Instead, when the backup process starts, Veeam Agent reads files and directories that you selected to back up, and copies backed-up data to the target location.

**IMPORTANT**

During backup in the snapshot-less mode, Veeam Agent does not track whether files and directories have changed in their original location since the time when the backup process started. To make sure that data in the backup is in the consistent state, you must not perform write operations in the file system that contains the backed-up data until the backup process completes.
How Backup Works

Veeam Agent for Linux performs backup differently depending on the backup type:

- Volume-level backup
- File-level backup
How Volume-Level Backup Works

During volume-level backup, Veeam Agent performs the following operations for every backup job session:

1. When a new job session starts, Veeam Agent creates a backup file in the target location.

2. In the backup file, Veeam Agent creates a disk for each backed-up disk. In disks, Veeam Agent creates blank partitions that have the same size and location as partitions in backed-up disks.

3. Veeam Agent creates a snapshot of the volume whose data you want to back up. The snapshot is created on the volume that has enough free disk space to contain the snapshot data. To create a snapshot, Veeam Agent uses the Veeam Agent for Linux Driver.

   The snapshot helps make sure that the data on the volume is consistent and does not change at the moment of backup. If a data block is about to change on disk during backup, Veeam Agent will copy this block to the snapshot. After the data block is overwritten on the source location, its original copy will remain intact in the snapshot.

   **NOTE**

   Consider the following:

   - If you instruct Veeam Agent to back up a database system, Veeam Agent prepares databases for backup before creating a snapshot of the volume. To learn more, see Backup of Database Systems.
   - During backup of data that resides in the Btrfs file system, Veeam Agent does not use its driver to create a snapshot. Instead, Veeam Agent leverages Btrfs capabilities to create a Btrfs snapshot.

4. [For incremental backup] Veeam Agent uses the Veeam Agent for Linux Driver to detect what blocks have changed on the volume since the previous job session. The driver keeps this information as a changed block tracking map in the RAM of your computer.

   Mind that every time the driver is unloaded or the Veeam Agent computer is rebooted, the changed block tracking map is reset as well. In such case, to detect what data blocks have changed since the previous job session, Veeam Agent rescans the entire data added to the backup scope and creates a new changed block tracking map. In this case, backup requires greater time.

   To learn about full and incremental backup, see Backup Chain.

5. Veeam Agent copies the partition table and bootloader located on the hard disk to the backup file in the target location.

6. [For incremental backup] Veeam Agent calculates checksums for each data block and compares them with checksums from the backup file created during the previous job session. If checksums do not match, Veeam Agent will copy the data block to the target location during the next backup process step.
7. Veeam Agent copies data from the following sources:
   - Data that did not change on disk during backup is transferred from the source volume.
   - Data that changed on disk during backup is transferred from the snapshot.
   After all the data is transferred, Veeam Agent removes the snapshot.
How File-Level Backup Works

During file-level backup, Veeam Agent performs the following operations for every backup job session:

1. When a new job session starts, Veeam Agent creates a backup file in the target location.
2. In the backup file, Veeam Agent creates a disk. The disk contains a volume with the ext4 file system.
3. Veeam Agent creates a snapshot of the volume which data you want to back up. The snapshot is created on the volume that has enough free disk space to contain the snapshot data. To create a snapshot, Veeam Agent uses the Veeam Agent for Linux Driver.
   The snapshot helps make sure that the data on the volume is consistent and does not change at the moment of backup. If a data block is about to change on disk during backup, Veeam Agent will copy this block to the snapshot. After the data block is overwritten on the source location, its original copy will remain intact in the snapshot.

   **TIP**
   Mind the following:
   - You can also set up Veeam Agent to create a file-level backup in the snapshot-less mode. This mode allows you to back up data that resides in any file system mounted to the root file system of the Veeam Agent computer. However, Veeam Agent does not track whether source files have changed since the backup process start. To learn more, see Snapshot-Less File-Level Backup.
   - Compared to the volume-level backup, the file-level backup, Veeam Agent does not provide changed block tracking mechanism and does not split source files into data blocks. As a result, if you plan to back up a significant amount of data, the file-level backup will require greater time, and created backup files will have greater size.
      For example, you have a 1 GB file, and since the previous backup session only one data block of this file has changed. In case of the file-level backup, Veeam Agent will send the whole 1 GB file to the target again.

4. [For incremental backup] To detect files that changed on the Veeam Agent computer since the previous backup session, Veeam Agent reads file metadata and compares last modification time of files in the original location and files in the backup created during the previous job session. If the file has modification time later than the previous job session start time, Veeam Agent considers the file as changed.
   To learn about full and incremental backup, see Backup Chain.
5. [For incremental backup] Veeam Agent calculates checksums for each data block and compares them with checksums from the backup file created during the previous job session. If checksums do not match, Veeam Agent will copy the data block to the target location during the next backup process step.
6. Veeam Agent copies data that you selected for backup to the target location. As part of this process, Veeam Agent performs the following operations:

a. Enumerates all files in the source location.

b. For each enumerated file, creates a target file in the volume inside the backup file.

c. Opens the source and the target files.

d. Copies file data to the target location from the following sources:
   - Data blocks that did not change on disk during backup are transferred from the source volume.
   - Data blocks that changed on disk during backup are transferred from the snapshot.

e. Closes the source and target files.

After all backed-up files and directories are transferred, Veeam Agent removes the snapshot.
Backup Job

To back up your data, you must configure a backup job. The backup job settings define what data you want to back up, what the target location and retention policy for created backups are and how to back up your data. If necessary, you can re-configure the backup job and change its settings at any time.

NOTE
You cannot change the backup job type from volume-level to file-level, and vice versa.

In Veeam Agent for Linux, you can configure several backup jobs with different settings. For example, you can configure one backup job to create volume-level backup and another backup job to create file-level backup. You can configure backup jobs targeted at different backup locations to keep several copies of your backed-up data. You can also configure several backup jobs with individual schedule to fine-tune automatic backup creation process.

NOTE
You can create more than one backup job only if Veeam Agent operates in the Workstation or Server edition. To learn more, see Product Editions.

Veeam Agent launches the backup job according to the schedule you define. You can schedule the job to start at specific time daily or on specific week days. You can also start a backup job manually to perform backup on demand when needed.

Backup job scheduling settings are configured globally for all accounts of the Linux OS. For every backup job, Veeam Agent creates a record in its database and in the crontab configuration file of the root account. As a result, Veeam Agent can start a backup job automatically regardless of the currently running user session.

You can define schedule for a job in Veeam Agent or edit the crontab file directly to fine-tune the schedule. To learn more, refer to the Cron job scheduler documentation.
Backup Job Scripts

You can instruct Veeam Agent for Linux to run custom scripts within the backup job session:

- **Pre-job and post-job scripts** — Veeam Agent runs these scripts before the backup job starts and after the backup job completes. You can use pre-job and post-job scripts, for example, to configure email notifications about jobs performed by Veeam Agent.

- **Pre-freeze and post-thaw scripts** (in the Server edition only) — Veeam Agent runs these scripts before and after creating a snapshot. For example, the pre-freeze script may quiesce the file system and application data to bring the Linux OS to a consistent state before Veeam Agent creates a snapshot. After the snapshot is created, the post-thaw script may bring the file system and applications to their initial state.

Script settings are enabled at the job level. If Veeam Agent operates in the Server edition and you want to configure multiple backup jobs, you can specify individual scripts for each job.

Scripts must be created beforehand. You must specify paths to them in the job settings. Veeam Agent supports scripts in the SH file format.
Pre-Job and Post-Job Scripts

You can instruct Veeam Agent for Linux to run custom pre-job and post-job scripts. Veeam Agent executes the pre-job script directly before the backup job starts. After the backup job completes, Veeam Agent executes the post-job script.

Veeam Agent starts the backup job regardless of the pre-job script result. If the pre-job script fails to execute, Veeam Agent will always start the backup job. Then, after the backup job completes, Veeam Agent will execute the post-job script.

The script is considered to be executed successfully if "0" is returned.

The default time period for script execution is 10 minutes. After this period expires, Veeam Agent stops executing the script and displays a warning message in the job session. If the script fails to execute before the timeout expires, Veeam Agent does not display warning messages in the job session.
Pre-Freeze and Post-Thaw Scripts

You can instruct Veeam Agent for Linux to run custom pre-freeze and post-thaw scripts. Veeam Agent executes the pre-freeze script before creating a snapshot. After the snapshot is created, Veeam Agent executes the post-thaw script.

The script is considered to be executed successfully if "0" is returned.

The default time period for script execution is 10 minutes. After this period expires, Veeam Agent stops executing the script.

By default, if the pre-freeze or post-thaw script fails to execute, Veeam Agent does not start the backup job. However, you can instruct Veeam Agent to ignore errors that occur during the script execution process. To allow Veeam Agent to start backup jobs regardless of the script execution result, in the /etc/veeam/veeam.ini configuration file, uncomment the `ignoreFreezeThawFailures` parameter and set its value to `true`.

If Veeam Agent is set up to ignore script errors, and the pre-freeze or post-thaw script fails to execute, Veeam Agent will start the backup job. After the job successfully completes, Veeam Agent will display the `Warning` status for the job session.

**NOTE**

You can specify pre-freeze and post-thaw scripts only if Veeam Agent for Linux operates in the Server edition. If these scripts were enabled for the job while Veeam Agent operated in the Server edition, and then Veeam Agent has switched to another edition (for example, to the Free edition after the license has expired), the backup job will fail. You will need to delete the existing job and create a new backup job without pre-freeze and post-thaw scripts enabled.
File System Indexing

You can instruct Veeam Agent for Linux to create an index of files and directories located on the Veeam Agent computer during backup. File indexing allows you to search for specific files inside Veeam Agent backups and perform 1-click restore in Veeam Backup Enterprise Manager.

File indexing is enabled at the job level. You can specify granular indexing settings for each job.

**IMPORTANT**

Indexing mechanism does not recognize file exclusion masks. If you specify masks to exclude certain files in a file-level backup job, Veeam Agent for Linux will nevertheless index all files located in the directories that have been selected for backup.

For example, you have included the `/home` directory into the backup and specified the `*.pdf` exclusion mask. The *Index everything* option is enabled for the backup job. In this case, when you browse the resulting backup in Veeam Backup Enterprise Manager, PDF files will be displayed in the `/home` directory as if they were backed up.
Requirements for File System Indexing

- Veeam Agent for Linux must have either Workstation or Server license installed.
- The following utilities must be installed on the computer: tar, mlocate and gzip (standard utilities for majority of Linux distributions).

**NOTE**

Consider the following:

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

A backup job configured in Veeam Agent for Linux creates backup files in a backup repository. A backup repository is a directory on the storage where you want to keep backup files. You can use the following types of disk-based storage to create a backup repository:

- Local (internal) storage of the protected machine (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) or NFS share.
- Veeam Backup & Replication 11 or later backup repository.
- Veeam Backup & Replication 11 or later cloud repository.

**IMPORTANT**
A backup repository must be created on a separate volume from a volume whose data you plan to back up.

Veeam Agent for Linux works with backup storage differently depending on the way you configure and start backup jobs — with the Veeam Agent control panel or command line interface.
Backup Location and Control Panel

If you use the Veeam Agent control panel to perform backup tasks, you do not have to deal with backup repositories. When you specify a target location for backup in the Backup Job wizard, Veeam Agent configures the backup repository automatically. Veeam Agent saves path to the specified backup location, assigns to this location a unique name and ID and saves this information in the database. The information is used by Veeam Agent and is not displayed in the control panel.

If you target a backup job at the network shared folder, every time the backup job starts, Veeam Agent will automatically mount the shared folder to the `/tmp/veeam` directory in the computer file system and create a backup file in this directory. After the backup job completes, Veeam Agent will automatically unmount the network shared folder.

You can target several backup jobs to individual backup locations or use the same target location for several backup jobs. This may be useful if you want to back up different types of data to separate locations or to keep all backed-up data at one place.
Backup Repository and Command Line Interface

If you work with Veeam Agent for Linux using the command line interface, you must deal with backup repositories depending on the target location selected for the backup job.

If you target a backup job at a local directory or network shared folder, you must create a repository before you configure a backup job:

- In case of a local directory, you specify a name for the repository and a local directory in which Veeam Agent will create backup files. To learn more, see Creating Repository in Local Directory.

- In case of a network shared folder, you specify a name for the repository, a path to the network shared folder in which Veeam Agent will create backup files, a type of the network shared folder and additional mounting options.

  Every time the backup job starts, Veeam Agent will automatically mount the shared folder to the /tmp/veeam directory in the computer file system and create a backup file in this directory. After the backup job completes, Veeam Agent will automatically unmount the network shared folder. To learn more, see Creating Repository in NFS Share and Creating Repository in SMB Share.

  If the directory to which the shared folder should be mounted resides on the backed-up volume, the backup job may fail.

If you target a backup job at a Veeam backup repository or cloud repository, you do not need to create repositories. Before configuring the backup job, you must connect to the Veeam backup server or Veeam Cloud Connect service provider. To learn more, see Connecting to Veeam Backup Server and Connecting to Service Provider.

You can configure several backup repositories and target different backup jobs at these repositories. This may be useful if you want to back up different types of data to separate locations or to keep several copies of your backed-up data.
Backup Chain

Every backup job session produces a new backup file in the target location. Backup files make up a backup chain. The backup chain can contain files of two types: full backups and incremental backups.

- During the first backup job session, Veeam Agent for Linux performs full backup. Veeam Agent for Linux copies all data that you have chosen to back up (entire volumes and directories) and stores the resulting full backup file (VBK) in the target location. The full backup takes significant time to complete and produces a large backup file: you have to copy the whole amount of data.

- During subsequent backup job sessions, Veeam Agent for Linux performs incremental backups. It copies only new or changed data relatively to the last backup job session and saves this data as an incremental backup file (VIB) in the target location. Incremental backups typically take less time than full backup: you have to copy only changes, not the whole amount of data.

After several backup cycles, you have a chain of backup files in the target location: the first full backup file and subsequent incremental backup files. Every backup file contains a restore point for backed up data. A restore point is a "snapshot" of your data at a specific point in time. You can use restore points to roll back your data to the necessary state.

To recover data to a specific restore point, you need a chain of backup files: a full backup file plus a set of incremental backup files following this full backup file. If some file from the backup chain is missing, you will not be able to roll back to the necessary state. For this reason, it is recommended that you do not delete separate backup files manually. To learn more, see Deleting Backups.
Types of Backup Files

Veeam Agent for Linux produces backup files of the following types:

- **VBK** — full backup file.
- **VIB** — incremental backup file.
- **VBM** — backup metadata file. The backup metadata file is updated with every backup job session. It contains information about the computer on which the backup was created, every restore point in the backup chain, how restore points are linked to each other and so on. The backup metadata file is required for performing file-level and volume-level restore operations.
Backup Retention Policy

Restore points in the backup chain are not kept forever. They are removed according to the retention policy. The retention policy helps maintain the life cycle of restore points and make sure that backup files do not consume the whole disk space.

Veeam Agent for Linux retains the number of latest restore points defined by the user. During every backup job session, Veeam Agent for Linux checks if there is any obsolete restore point in the backup chain. If some restore point is obsolete, it is removed from the chain.
Removing Backups by Retention

When removing obsolete restore points, Veeam Agent for Linux does not simply delete backup files from disk. It transforms the backup chain so that the backup chain always contains a full backup file on which subsequent incremental backup files are dependent. To maintain the consistency of the backup chain, Veeam Agent for Linux uses the following rotation scheme:

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

2. If an obsolete restore point exists, Veeam Agent for Linux transforms the backup chain. As part of this process, it performs the following operations:
   
   a. Veeam Agent for Linux re-builds the full backup file to include in it data of the incremental backup file that follows the full backup file. To do this, Veeam Agent for Linux injects into the full backup file data blocks from the earliest incremental backup file in the chain. This way, a full backup 'moves' forward in the backup chain.

   b. The earliest incremental backup file is removed from the chain as redundant: its data has already been injected into the full backup file, and the full backup file includes data of this incremental backup file.
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 Agent for Linux lets you create active full backups.

When Veeam Agent for Linux performs active full backup, it produces a full backup file and adds this file to the backup chain.

The active full backup resets the backup chain. All incremental backup files use the latest active full backup file as a new starting point. A previously used full backup file and its subsequent incremental backup files remain on the disk. After the last incremental backup file created prior to the active full backup becomes outdated, Veeam Agent for Linux automatically deletes the previous backup chain. To learn more, see Retention Policy for Active Full Backups.

You can create active full backups manually or schedule a backup job to create active full backups periodically. To do this, you can use the Veeam Agent for Linux control panel or command line interface.

- To learn how to configure active full backup schedule and create active full backups with the Veeam Agent for Linux control panel, see Active Full Backup Settings and Starting Backup Job from Control Panel.
- To learn how to configure active full backup schedule and create active full backups with the Veeam Agent for Linux command line interface, see Configuring Active Full Backup Schedule and Creating Active Full Backups.
Active Full Backup Schedule

You can schedule a backup job to create active full backups periodically.

Active full backup schedule depends on the regular backup schedule. For every backup job with enabled backup schedule, Veeam Agent saves active full schedule settings to the crontab configuration file of the root account.

- In case active full backup is scheduled on a week day, Veeam Agent modifies the crontab record associated with the regular schedule.
  
  For example, the regular backup schedule is set to Monday and Tuesday at 15:00. Active full backup schedule is set to Friday. In this case, the crontab record for the regular backup schedule will contain information that the job must start on Monday, Tuesday and Friday at 15:00.

- In case active full backup is scheduled on a day of the month, Veeam Agent creates a separate crontab record that instructs the backup job to run on this day at the same time as it must run upon the regular schedule.

Keep in mind that if the job is not scheduled to run automatically, Veeam Agent will not create a crontab record. Veeam Agent will save schedule settings for active full backup in its database only. As a result, active full backup will not run automatically.

For information about how to configure job schedule, see Configuring Backup Schedule and Configuring Active Full Backup Schedule.
Retention Policy for Active Full Backups

To be able to restore data from a Veeam Agent backup, you need to have a full backup file and a chain of subsequent incremental backup files on the disk. If you delete a full backup file, the whole chain of incremental backup files will become useless. In a similar manner, if you delete any incremental backup file before the point to which you want to roll back, you won’t be able to restore data (since later incremental backup files depend on earlier incremental backup files).

For this reason, if you create an active full backup, in some days there will be more restore points on the disk than specified by retention policy settings. Veeam Agent for Linux will remove the full backup chain only after the last incremental backup file in the chain becomes outdated.

For example, the retention policy is set to 3 restore points. A full backup file is created on Sunday, incremental backup files are created on Monday and Tuesday, and an active full backup is created on Wednesday. Although the backup chain now contains 4 restore points, Veeam Agent for Linux will not delete the previous backup chain. Veeam Agent for Linux will wait for the next 2 incremental backup files to be created, and only then will delete the whole previous chain, which will happen on Friday. As a result, although the retention policy is set to 3 restore points, the actual number of backup files on the disk will be greater for some time.

Veeam Agent for Linux treats the active full backup in the same way as a regular full backup. If some restore point becomes obsolete, Veeam Agent for Linux will re-build the full backup file to include in it data of the incremental backup file that follows the full backup file. After that, Veeam Agent for Linux will remove the earliest incremental backup file from the chain as redundant.
Backup of Database Systems

You can use Veeam Agent for Linux to create transactionally consistent backups of Veeam Agent machines that run one of the following database systems:

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

**IMPORTANT**

Consider the following:

- You can specify settings for database system processing only if Veeam Agent for Linux operates in the Server edition.
- Veeam Agent supports processing of database systems for the volume-level backup only.
- Veeam Agent does not support processing of multiple database systems on one Veeam Agent computer.
  
  For example, successful processing of MySQL and PostgreSQL database systems installed on the same server is not guaranteed.
- Veeam Agent does not support 32-bit database systems installed on a 64-bit Linux OS.

To process database systems with Veeam Agent for Linux, enable application-aware processing for the backup job:

- If you work with Veeam Agent using the Veeam Agent control panel, configure application-specific settings at the Advanced step of the Backup Job wizard. To learn more, see Specify Advanced Backup Settings.

- If you work with Veeam Agent using the command line interface, create the backup job, then specify application-specific settings for this job. To learn more, see Creating Volume-Level Backup Job and Configuring Database Processing Settings.
Oracle Backup

You can use Veeam Agent for Linux to create transactionally consistent backups of Veeam Agent machines that run the Oracle database system.

**NOTE**

You can use Veeam Explorer for Oracle to restore Oracle databases from a Veeam Agent for Linux backup. For information about item-level recovery of Oracle systems, see Veeam Explorers User Guide.
How Oracle Processing Works

To ensure that the backed-up data is in the consistent state, Veeam Agent for Linux performs the Oracle database system processing. To process the database system, Veeam Agent performs the following operations:

1. When the backup job starts, Veeam Agent obtains information about Oracle databases that run on the Veeam Agent machine.

2. Veeam Agent connects to the Oracle database and operates depending on the database state:
   - Shutdown state
   - ARCHIVELOG mode
   - NOARCHIVELOG mode

After Veeam Agent for Linux finishes database system processing, Veeam Agent proceeds to the next step of the backup process. To learn more, see How Backup Works.

Processing of Database in Shutdown State

If the database is shut down, Veeam Agent skips it and connects to the next database. The skipped database will be included in the backup. To restore such database, you must restore the entire volume that contains the database. You cannot restore the database as an independent item using Veeam Explorer for Oracle. To learn more, see Veeam Explorers User Guide.

Veeam Agent displays a warning message about the database that is shut down in the job session logs. The backup job does not fail.

Processing of Database in ARCHIVELOG Mode

If the Oracle database is running in the ARCHIVELOG mode, the Oracle database system keeps archived logs that allow to recover all committed transactions of the database. To learn more, see Oracle documentation.

If the database operates in the ARCHIVELOG mode, Veeam Agent performs the following operations:

1. Veeam Agent switches the database to the backup mode. Veeam Agent changes the database state using the Oracle functionality.

2. Veeam Agent creates a snapshot of the volume.

3. Veeam Agent returns the database to the initial state.

Processing of Database in NOARCHIVELOG Mode

If the Oracle database is running in the NOARCHIVELOG mode, the Oracle database system does not create archived logs. Logs that are created before the database is switched to NOARCHIVELOG remain untouched. In this mode, you can only restore the database to the point of full database backup. You cannot recover transactions subsequent to that full database backup.

If the database operates in the NOARCHIVELOG mode, Veeam Agent performs the following operations:

1. Veeam Agent shuts down the database. Veeam Agent changes the database states using the Oracle functionality.

2. Veeam Agent creates a snapshot of the volume.

3. Veeam Agent returns the database to the initial state.
Authentication Methods

Veeam Agent for Linux can connect to the Oracle database system and perform Oracle archived logs backup and/or deletion using one of the following account types:

- **System account** — Veeam Agent uses the account of the Veeam Agent machine OS. To connect to the Oracle database system, the account must be a member of the group that owns configuration files for the Oracle database (for example, the oinstall group).

- **Oracle account** — Veeam Agent uses the Oracle account. To connect to the Oracle database system, the account must have SYSDBA rights.
Archived Log Processing

**NOTE**
Veeam Agent for Linux operating in the standalone mode supports the backup of archived logs, but does not support a separate schedule and retention policy for the backup of archived logs. This functionality is available only for Veeam Agent for Linux operating in the managed mode within the Veeam Agent management scenario. For more information, see Oracle Archived Log Settings section in the Veeam Agent Management Guide.

In the ARCHIVELOG mode, the Oracle database system stores database archived logs to a certain location on the machine that runs the database system, as specified by the database administrator. Veeam Agent allows you to set up the following ways of archived logs processing:

- **Delete logs older than the specified time (in hours).** After the backup job completes, Veeam Agent deletes archived logs that are older than the specified time from the Veeam Agent machine. This helps make sure that logs do not overflow the storage space on the processed machine.

- **Delete oldest logs larger than the specified size (in GB).** After the backup job completes, Veeam Agent checks whether the total size of archived logs exceeds the specified size. After that, Veeam Agent deletes oldest archived logs that exceed the specified size from the processed machine. This helps make sure that logs do not overflow the storage space on the Veeam Agent machine.

- **Do not delete archived logs.** Log files remain untouched on the Veeam Agent machine.

Veeam Agent processes archive logs via Oracle Call Interface (OCI).
Requirements and Limitations for Oracle Processing

- Oracle Database versions 11g – 21c are supported for all operating systems supported by Veeam Agent for Linux. To learn more, see System Requirements.
- Automatic Storage Management (ASM) is not supported.
- Oracle Real Application Clusters (RAC) are not supported.
- Oracle Grid Infrastructure is not supported.
- Oracle Database Express Edition (XE) is not supported.
- SAP on Oracle is not supported.
- Oracle Database architectures with Data Guard are not supported.
MySQL Backup

You can use Veeam Agent for Linux to create transactionally consistent backups of Veeam Agent machines that run the MySQL database system.
How MySQL Processing Works

To ensure that the backed-up data is in the consistent state, Veeam Agent for Linux performs the MySQL
database system processing. To process the database system, Veeam Agent performs the following operations:

1. When the backup job starts, Veeam Agent connects to the MySQL database system and obtains the list of
tables.

2. Veeam Agent locks base tables that are based on the MyISAM storage engine. Veeam Agent changes the
table state using the MySQL functionality. Tables based on the InnoDB storage engine do not require
locking.

   Keep in mind that Veeam Agent supports processing of tables based on the MyISAM and InnoDB storage
   engines only. Veeam Agent does not support tables that use other storage engines.

3. Creates a snapshot of the volume.

4. Unlocks tables locked at the step 2.

After Veeam Agent unlocks tables, Veeam Agent proceeds to the next step of the backup process. To learn
more, see How Backup Works.
Authentication Methods

IMPORTANT
To process the MySQL database system, the MySQL account must have the following privileges:

- SELECT for all tables. If the MySQL account does not have the SELECT privilege for the table, Veeam Agent cannot access table metadata. As a result, Veeam Agent does not process the table. To learn more, see MySQL documentation.
- LOCK TABLES. If the MySQL account does not have the LOCK TABLES privilege, Veeam Agent does not process tables based on the MyISAM storage engine.

To obtain information about privileges that are assigned to the account, use MySQL functionality, for example, the SHOW GRANTS statement. To learn more, see MySQL documentation.

Veeam Agent for Linux can connect to the MySQL database system using one of the following methods:

- **Password** — Veeam Agent uses the MySQL account credentials that you specify in the backup job settings.
- **Password file** — Veeam Agent uses the MySQL account credentials that are stored in the `.my.cnf` password file. To learn more about password file configuration, see Preparing Password File for MySQL Processing.
Requirements and Limitations for MySQL Processing

- Veeam Agent for Linux supports processing of MySQL database system version 5.6 - 8.0.
- Configurations with multiple MySQL installations and/or instances on the same machine are not supported.
- MySQL Cluster versions are not supported.
PostgreSQL Backup

You can use Veeam Agent for Linux to create transactionally consistent backups of Veeam Agent machines that run the PostgreSQL database system.
How PostgreSQL Processing Works

To ensure that the backed-up data is in the consistent state, Veeam Agent performs the PostgreSQL database processing. To process the database system, Veeam Agent performs the following operations:

1. When the backup job starts, Veeam Agent forces a write-ahead log checkpoint. This command fastens the database system restore. To learn more, see PostgreSQL documentation.

2. Creates a snapshot of the volume and proceeds to the next step of the backup process. To learn more, see How Backup Works.
Authentication Methods

Veeam Agent for Linux can connect to the PostgreSQL database system using one of the following methods:

- *Database user with password* — Veeam Agent uses the PostgreSQL account credentials that you specify in the backup job settings.

- *Database user with password file* — Veeam Agent the PostgreSQL database system to use account credentials that are stored in the `.pgpass` password file. To learn more about password file configuration, see Preparing Password File for PostgreSQL Processing.

- *System user without password* — Veeam Agent uses the peer authentication. In the peer authentication method, Veeam Agent for Linux uses the OS account as the PostgreSQL database user name.
Requirements and Limitations for PostgreSQL Processing

- Veeam Agent for Linux supports processing of the PostgreSQL database system version 9.5 – 14.0.
- Configurations with multiple PostgreSQL installations and/or instances on the same server are not supported.
Data Restore

Veeam Agent for Linux offers two data restore scenarios:

- You can perform volume-level restore to recover the entire system image of your computer or specific computer volumes. To learn more, see Volume-Level Restore.

- You can perform file-level restore to recover individual files and directories. To learn more, see File-Level Restore.
Volume-Level Restore

If data on a computer volume gets corrupted, you can restore this volume from the backup. For volume-level restore, you can use backups that were created at the volume level. File-level backups cannot be used for volume restore.

When you perform volume-level restore, Veeam Agent for Linux restores the entire content of the volume. It retrieves from the backup data blocks pertaining to a specific volume and copies them to the necessary location.

Keep in mind that you cannot browse the volume in the backup and select individual files and directories for restore. For granular file-level restore, you can use the File-Level Restore option.

A volume can be restored to its original location or new location. If you restore the volume to its original location, Veeam Agent for Linux overwrites data on the original volume. If you restore the volume to a new location, and the target disk contains any data, Veeam Agent for Linux overwrites data in the target location with data retrieved from the backup.
Limitations for Volume-Level Restore

Volume restore has the following limitations:

- You cannot restore the system volume to its original location.
- You cannot restore a volume to the volume on which the Linux swap space is hosted.
- You cannot restore a volume to the volume where the backup file used for restore is located.

To overcome the first two limitations, you can create a Veeam Recovery Media and use the Volume Restore wizard for volume-level restore. To learn more, see Veeam Recovery Media.
File-Level Restore

If you have lost or modified files and directories on your computer by mistake, you can restore a copy of the necessary objects from the backup. For file-level restore, you can use a backup of any type:

- Volume-level backup
- File-level backup

Veeam Agent for Linux does not simply extract files and folders from the backup file. During file-level restore, Veeam Agent for Linux performs the following operations:

1. Veeam Agent for Linux associates the backup file with a loop device, for example, /dev/loop0, to make the backup file accessible as a block device.

2. Veeam Agent for Linux mounts the loop device to the mount point directory in the computer’s file system.
   - For file-level restore with the Veeam Agent for Linux control panel or Veeam Recovery Media, Veeam Agent for Linux mounts the backup content to the /mnt/backup directory.
   - For file-level restore with the command line interface, you can specify a directory in which Veeam Agent for Linux should mount the backup content.

After the backup content is mounted, you can use Linux command line utilities or preferred file browser to work with restored files and directories. You can browse for files and directories in the mounted backup and copy them to their initial location or to a new location.
Veeam Recovery Media

Veeam Agent for Linux lets you use the Veeam Recovery Media — a recovery image of the Linux OS that provides an alternative way to boot your computer.

The recovery image includes a custom Linux OS with the limited functionality. It comprises Linux kernel and a set of GNU/Linux utilities necessary to boot the computer and perform basic administration tasks. If the OS installed on the computer fails to start for some reason, you can boot the recovery image OS. After booting, you can do the following:

- You can restore data from a backup to your computer. For this scenario, you must have a backup created with Veeam Agent for Linux.
- You can use Linux OS tools to diagnose problems and fix errors on your computer.

The recovery image can be helpful if one of the following errors occur:

- The OS on the computer fails to start.
- You want to perform bare metal restore from the backup on the computer without the OS and other software installed.
- You want to restore the system volume of the computer and so on.

Veeam Recovery Media is distributed as an ISO image. The ISO image file can be downloaded from this Veeam webpage. You can burn the ISO image file to different kinds of media:

- Removable storage devices such as USB drives or SD cards
- CD/DVD/BD

**NOTE**

Consider the following:

- You can also download the Veeam Recovery Media ISO image from the Veeam software repository. In addition to the regular recovery image, the repository offers a legacy recovery image intended for Veeam Agent computers that run an earlier version of Linux kernel with custom drivers. To learn more, see Veeam Recovery Media Versions.
- For information about how to burn the ISO image to a removable storage device, as well as workaround for accessing the Veeam recovery UI, see this Veeam KB article.

When you boot from the Veeam Recovery Media, you can use the recovery environment to fix the OS system errors on your computer or restore data from the backup. Veeam Agent for Linux offers a set of tools for the computer system image and data recovery:

- Restore volumes — the Veeam Recovery wizard to recover data on the original computer or perform bare metal recovery.
- Restore files — the File Level Restore wizard to restore files and folders to the original location or to a new location.
- Exit to shell — Linux shell prompt with standard utilities to diagnose problems and fix errors.
Veeam Recovery Media Versions

Veeam Agent for Linux offers the following versions of Veeam Recovery Media:

- **Regular recovery image** suitable for the majority of Linux machines.
- **Legacy recovery image** that allows you to perform bare metal recovery of Linux machines that run an earlier version of Linux kernel with custom drivers.
Regular Recovery Image

The regular recovery image is intended for Veeam Agent computers that run Linux kernel version 3.10 and later. This version of Veeam Recovery Media is based on the Debian live install image and allows you to boot your computer using Linux kernel of either stable Debian release or testing release. In Veeam Agent for Linux 5.0, this Veeam Recovery Media offers Linux kernel versions 4.19.0 and 5.10.0.

You can download the regular recovery image from the following sources:

- **Veeam website**
  
  Recovery image ISO files downloaded from the Veeam website have the following names:
  
  - veeam-recovery-media-5.0.2.4567_i386.iso — for Veeam Agent computers based on the x86 architecture
  
  - veeam-recovery-media-5.0.2.4567_x86_64.iso — for Veeam Agent computers based on the x64 architecture

- **Veeam software repository**
  
  Recovery image ISO files downloaded from the Veeam software repository have the following names:
  
  - veeam-recovery-i386-5.0.0.iso — for Veeam Agent computers based on the x86 architecture
  
  - veeam-recovery-amd64-5.0.0.iso — for Veeam Agent computers based on the x64 architecture

The size of the regular recovery image file depends on the Veeam Agent computer architecture: 460 MB for x86 computers and 490 MB for x64 computers.

In the scenario where you instruct Veeam Agent to download and patch the recovery image during initial product setup on a computer that runs Linux kernel version 3.10 and later, Veeam Agent downloads the regular recovery image from the Veeam software repository.

Consider the following:

- The regular recovery image supports EFI.
- The regular recovery image supports Secure Boot.
- The regular recovery image contains a larger set of software packages than the legacy recovery image. You can also install additional software from a software repository using the `apt` package manager. Keep in mind that to install software from a repository, the computer booted from the Veeam Recovery Media must have internet connection.

  By default, the list of repositories contains the following package sources: DebianStable, DebianBackports, StableUpdates, DebianSecurity. You can also add custom repositories if necessary. For information about how to do this, see [Debian documentation](https://吕min/debian-guide/).
Legacy Recovery Image

The legacy recovery image is intended for Veeam Agent computers that run Linux kernel version earlier than 3.10 with custom drivers. It allows you to create a custom Veeam Recovery Media for such computers. In the scenario where you instruct Veeam Agent to download and patch the recovery image during initial product setup on such a computer, Veeam Agent downloads this version of the recovery image from the Veeam software repository. You can also download it manually from the repository.

The name and size of the legacy recovery image ISO file is veeam-recovery-media-5.0.0.iso. The size of the ISO file depends on the Veeam Agent computer architecture: 136 MB for x86 computers and 139 MB for x64 computers.

The legacy recovery image does not support EFI by default. You can enable EFI support for a custom Veeam Recovery Media based on this version of recovery image. To learn more, see Create Custom Veeam Recovery Media and Creating Custom Veeam Recovery Media.
Drivers in Veeam Recovery Media

The generic Veeam Recovery Media available for download from the Veeam website or Veeam software repository contains the following data:

1. Set of files required to start the recovery image OS from the recovery media.
2. Set of Veeam tools for the computer system image and data recovery.
3. Set of Linux command line tools to diagnose problems and fix errors on your computer. For the regular recovery image, in addition to the standard set of tools, you can install custom software from a software repository.
4. Drivers required to run hardware and devices on your computer in a regular way. The regular recovery image contains drivers included in the Linux kernel versions 4.19.0 and 5.10.0. The legacy recovery image contains drivers included in the Linux kernel version 5.1.15.

When you boot your computer from the Veeam Recovery Media, drivers from the Veeam Recovery Media are automatically loaded on the recovery image OS.

If your computer uses hardware that requires drivers not included in the generic Veeam Recovery Media, you can create a custom recovery image. Veeam Agent will copy the Linux kernel running on your computer with its currently loaded modules and include them into the custom Veeam Recovery Media. To learn more, see Creating Custom Veeam Recovery Media.
Integration with Veeam Backup & Replication

If you plan to use Veeam Agent for Linux 5.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 11a on the Veeam backup server. Veeam Agent for Linux 4.0 supports integration with Veeam Backup & Replication 11 or later as well.

You can store backup files created with Veeam Agent for Linux on backup repositories managed by Veeam Backup & Replication. To do this, you must select a Veeam Backup & Replication backup repository as a target location in the properties of the backup job. To store Veeam Agent backups, you can use a simple backup repository or a scale-out backup repository.

NOTE

Consider the following:

- The current guide covers subjects related to Veeam Agent for Linux operating in the standalone mode.
- You can also use Veeam Backup & Replication to manage Veeam Agent for Linux on computers in your infrastructure. As part of the Veeam Agent management scenario, you can remotely deploy Veeam Agent to your computers, as well as configure and manage Veeam Agent backup jobs in Veeam Backup & Replication. To learn more, see Veeam Agent Management Guide.
- If you create a backup job with the Veeam Agent command line interface, you need to specify a Veeam backup repository in the backup job settings. Veeam backup repository appears in the list of backup repositories after you connect to a Veeam backup server. To learn more, see Managing Veeam Backup & Replication Servers.

Veeam Agent for Linux works with the Veeam Backup & Replication backup repository as with any other backup repository. Backup files are stored to a separate folder; you can perform standard restore operations using these files.

Information about Veeam Agent backups stored on the Veeam Backup & Replication backup repositories, backup jobs and sessions becomes available in the Veeam Backup & Replication console:

- The Veeam Agent for Linux backup job is displayed in the list of jobs in Veeam Backup & Replication.
- Backup files created with Veeam Agent for Linux are displayed in the list of backups, under the Agents node.
- Performed job sessions are available in the History view of Veeam Backup & Replication.

Backup administrators working with Veeam Backup & Replication can perform a set of operations with Veeam Agent backups:

- Perform data protection operations: copy Veeam Agent backups to secondary backup repositories and archive these backups to tape.
- Perform restore operations: restore individual files and directories, application items from Veeam Agent backups; restore computer disks and convert them to the VMDK, VHD or VHDX format; restore to Microsoft Azure and Amazon EC2.
- Perform administrative tasks: disable and delete Veeam Agent backup jobs, remove Veeam Agent backups and so on.
Backup to Veeam Cloud Connect Repository

If you want to store your data in the cloud, you can connect to a Veeam Cloud Connect service provider (SP) and create Veeam Agent backups in a cloud repository. To do this, you must provide credentials of the tenant (or subtenant) account that you obtained from the SP, and select a cloud repository as a target for backup files in the properties of the backup job. To learn more, see Veeam Cloud Connect Repository Settings.

**NOTE**

Consider the following:

- You can create Veeam Agent backups in a cloud repository if the SP backup server runs Veeam Backup & Replication 11 or later.
- Backup to a cloud repository is available if Veeam Agent for Linux operates in the Workstation or Server edition.
Managing Veeam Agent in Veeam Backup & Replication

Veeam Backup & Replication lets you automate management of Veeam Agent on multiple computers in your infrastructure. You can deploy Veeam Agent for Linux, configure Veeam Agent backup jobs and perform other data protection and administration tasks on remote computers. To use the Veeam Agent management functionality in Veeam Backup & Replication, you must install Veeam Backup & Replication on the Veeam backup server.

To learn more, see Veeam Agent Management Guide.
Planning and Preparation

Before you install Veeam Agent for Linux, make sure that the target computer meets the system requirements and all required ports are open.
System Requirements

The protected Linux computer must meet requirements listed in the table below.

NOTE

The following system requirements apply to the following Veeam Agent for Linux configuration:

- Veeam Agent version is 5.0.
  To learn system requirements for Veeam Agent previous versions, see Release Notes for Veeam Agent for Linux 5.0 and Release Notes for Veeam Agent for Linux 5.0.1.
- Veeam Agent is operating in the standalone mode.
  To learn about system requirements for Veeam Agent managed by Veeam Backup & Replication, see the System Requirements section in the Veeam Agent Management Guide.
- Veeam Agent is installed with veeam and veeamsnap packages.
  To learn about system requirements for Veeam Agent installed using veeam-nosnap package, see Appendix A. Requirements for veeam-nosnap.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>x86 (starting from i386) or x64 processor.</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB RAM or more. Memory consumption varies depending on the backup type and the total amount of backed-up data.</td>
</tr>
<tr>
<td>Disk Space</td>
<td>100 MB free disk space for product installation.</td>
</tr>
<tr>
<td>Network</td>
<td>10 Mbps or faster network connection to a backup target.</td>
</tr>
<tr>
<td>System firmware</td>
<td>BIOS or UEFI.</td>
</tr>
<tr>
<td>Disk layout</td>
<td>MBR or GPT.</td>
</tr>
<tr>
<td>For virtual machines</td>
<td>Only full virtualization type is supported. Oracle VM virtual machines are supported with limitations. Virtual I/O (VirtIO) devices have experimental support status. Other containers and paravirtualized instances are not supported.</td>
</tr>
<tr>
<td>Specification</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>OS</td>
<td><strong>Important!</strong> Check considerations and limitations that apply to the list of supported OSes.</td>
</tr>
</tbody>
</table>

Linux kernel version 2.6.32 or later is supported.

Both 64-bit and 32-bit versions (if applicable) of the following distributions are supported:

- Debian 9.0 – 11.1
- RHEL 6.0 – 8.5
- RHEL 8.6, 9.0 (requires updating Veeam Agent to version 5.0.2.4619. For details, see [this Veeam KB article](#))
- CentOS 7.0 – 8.5
- Oracle Linux 6 – 8.5 (RHCK)
- Oracle Linux 6 (starting from UEK R2) - Oracle Linux 8 (up to UEK R6 U2, kernel version 5.4.17-2102)
- Oracle Linux 8.6 (requires updating Veeam Agent to version 5.0.2.4619. For details, see [this Veeam KB article](#))
- Oracle Linux 9.0 (requires updating Veeam Agent to version 5.0.2.4623. For details, see [this Veeam KB article](#))
- SLES 11 SP4, 12 SP2 – 15 SP3
- SLES for SAP 11 SP4, 12 SP2 – 15 SP3
- SLES 15 SP4 (requires updating Veeam Agent to version 5.0.2.4619. For details, see [this Veeam KB article](#))
- Fedora 33, 34, 35
- openSUSE Leap 15.2 – 15.3
- openSUSE Leap 15.4 (requires updating Veeam Agent to version 5.0.2.4619. For details, see [this Veeam KB article](#))
- openSUSE Tumbleweed
<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File System</strong></td>
<td><strong>Important!</strong> Check <strong>considerations and limitations</strong> that apply to the list of supported file systems.</td>
</tr>
</tbody>
</table>

Veeam Agent for Linux supports consistent snapshot-based data backup for the following file systems:

- Btrfs (for OSes that run Linux kernel 3.16 or later)
- Ext 2/3/4
- F2FS
- FAT16
- FAT32
- HFS
- HFS+
- JFS
- NILFS2
- NTFS
- ReiserFS
- XFS

The supported file system (except for Btrfs) can reside on a simple volume or LVM2 volume; volumes protected with encryption software such as dm-crypt are supported. Btrfs is supported only if it resides directly on a physical device with no additional abstraction layers (such as LVM, software RAID, dm-crypt and so on) below or above it.

Data that resides on other file systems and volumes (including NFS and SMB shares) can be backed up using the snapshot-less mode. For details, see **Snapshot-Less File-Level Backup**.
### Specification

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
</tr>
</tbody>
</table>

**Important!** Check [considerations and limitations](#) that apply to the list of supported components.

Protected computer must have the following components installed:

- dkms
- gcc
- make
- perl
- linux-headers (for Debian-based systems)
- kernel-headers (for RedHat-based systems)
- kernel-devel (for RedHat-based systems)
- kernel-uek-devel (for Oracle Linux with UEK)
- libudev
- libacl
- libattr
- lvm2
- libfuse
- libncurses5
- dmidecode
- libmysqlclient
- libpq5
- python3
- efibootmgr (for UEFI-based systems)
- isolinux (for Debian-based systems)
- syslinux (for RedHat-based systems)
- btrfs-progs (for backup of Btrfs file system)
- mksquashfs (for custom Veeam Recovery Media)
- unsquashfs (for custom Veeam Recovery Media)
- wget (for custom Veeam Recovery Media)
- xorriso (for custom Veeam Recovery Media with EFI support)
- mlocate (for file system indexing)
- tar (for file system indexing, log export and rotation)
- gzip (for file system indexing, log export and rotation)
Considerations and Limitations

OS

- Linux kernel version 2.6.32 or later is supported as long as you use kernels supplied by your distribution. Consider the following limitations:
  - Ubuntu, Fedora, and openSUSE Tumbleweed are supported up to kernel 5.15.7.
  - Linux kernel 2.6.32-754.6.3 in RHEL and Oracle Linux (RHCK) is not supported.
  - If you work with the Veeam Agent for Linux 5.0 build earlier than 5.0.1.4493 and the protected computer is running Linux kernel version 5.8 or later, only snapshot-less file-level backup is supported. For details, see Snapshot-Less File-Level Backup.

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

- For the following distributions, we recommend you to install Veeam Agent from a pre-built binary veeamsnap kernel module packages provided by Veeam:
  - CentOS 7.0 – 8.5
  - RHEL 6.0 – 8.5
  - SLES 11 SP4, 12 SP2 – 15 SP3
  - SLES for SAP 11 SP4, 12 SP2 – 15 SP3
  - openSUSE Leap 15.2 – 15.3
  - For other supported distributions, use the dkms packages instead of the pre-built binary veeamsnap kernel module packages.
    - Keep in mind that the pre-built binary veeamsnap kernel module packages require kernel 2.6.32-131.0.15 or later for RHEL 6 (excluding 2.6.32-279.el6.i686) and 3.10.0-123 or later for CentOS / RHEL 7.0 – 7.9.
  - To ensure proper functioning of the veeamsnap kernel module, verify that your system does not have any of the following modules installed: hcdriver, snapapi26, snapapi, snapper, dattobd, dattobd-dkms, dkms-dattobd, cdr or cxbf.
  - The Linux OS must be set up to receive software updates from the default repositories enabled in the OS after installation.
  - For cloud-based installations that use customized kernels (such as Linux distributions deployed from AWS Marketplace or Azure Marketplace), the veeamsnap kernel module has experimental support status.
  - RHEL, CentOS and Oracle Linux (RHCK) are supported up to certain kernel versions. For details, see this Veeam KB article.
  - Ubuntu 21.10 minimal install is not supported.
File System

- Veeam Agent for Linux does not back up the following objects:
  - LVM snapshots
  - Volumes that reside on USB devices and SD cards

- File-level backup has the following limitations:
  - Total size of all file systems must not exceed 218 TB. This limitation applies to all file systems where files you plan to back up are located.
  - Size of a file must not exceed 16 TB.
  - Name of a file must not be larger than 254 bytes.
    
    Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more.

- Veeam Agent supports backup of extended attributes with the following limitations:
  - Veeam Agent backs up extended attributes only with the following public namespaces: system, security, trusted, and user.
  - All extended attribute names and values of a file must not exceed 4096 bytes (size of a default ext4 file system block). Veeam Agent does not back up attributes exceeding the limit.
    
    For the kernel version 4.13 or later, if a value of extended attribute exceeds the limit, Veeam Agent uses the ea_inodes feature. Backups created using the ea_inodes feature cannot be mounted on kernel versions up to 4.12.

- Backup of file and directory attributes (for example, a — append only, c — compressed, and so on) is not supported.

- Each volume included in a backup must have a unique UUID.

- The veeamsnap module provides RAM-based changed block tracking (CBT) mechanism. Every time the module is unloaded or Veeam Agent for Linux computer is rebooted, CBT data is reset. As a result, Veeam Agent reads the entire data added to the backup scope to detect what blocks have changed since the last job session, and incremental backup requires greater time.

- The following limitations apply to the backup of machines used as cluster nodes:
  - If your cluster nodes consist of LVM logical volumes or volume groups, you can back up them using the veeam-nosnap package. For details, see Appendix A. Requirements for veeam-nosnap.
  - If your cluster nodes do not consist of LVM logical volumes or volume groups, you can back up them using only file-level backup in the snapshot-less mode. Other backup modes are not supported.

- Certain limitations for Dell PowerPath configuration apply. To learn more, see this Veeam KB article.

- BFQ I/O scheduler is not supported.

- Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files.

Software

**IMPORTANT**

Linux user account used to work with Veeam Agent for Linux must have the /bin/bash shell set as the default shell.
• The following packages are not required for CentOS, RHEL and SLES distributions if a pre-built binary 
veeam snap package is to be installed.
  o dkms
  o gcc
  o make
  o perl
  o kernel-headers (for RedHat-based systems)
  o kernel-devel (for RedHat-based systems)
For details, see Installing Veeam Agent for Linux.

• Version of the following packages varies according to the Linux kernel version that you use:
  o linux-headers (for Debian-based systems)
  o kernel-headers (for RedHat-based systems)
  o kernel-devel (for RedHat-based systems)

• For openSUSE and SLES distributions, either of the following packages is required: libncurses5 or
  libncurses6.

• The dmidecode package is required for Veeam Agent management — a valid BIOS UUID must be
  obtainable either from dmidecode | grep -i uuid or from /sys/class/dmi/id/product_uuid. Each Veeam
  Agent that consumes a license installed in Veeam Backup & Replication must have a unique
  BIOS UUID. If a valid UUID cannot be obtained, Veeam will generate it automatically.

• The libmysqlclient package is required to process MySQL database system located on the Veeam
  Agent server. For details, see Backup of MySQL Database. Package version varies according to the MySQL
  database system version that you use.

• The libpq5 package is required to process PostgreSQL database system located on the Veeam Agent
  server. For details, see Backup of PostgreSQL Database.

• The python3 package or another RPM package providing a /usr/bin/python3 binary is required for
  CentOS, RHEL 7.0 and later distributions if a pre-built binary kmod-veeam snap package is to be installed.

• The btrfs-progs package version 3.16 or later is required.

• The lvm2 package version up to 2.03.12 is required. Later versions are not supported.

• Live patching of Linux kernel is supported with limitations. For details, see Live Patching Support.
Backup Source

Any file systems and devices that are accessible from the host OS. To learn about limitations, see File System.
Backup Target

Backup can be performed to the following types of storage:

- Local (internal) storage of the protected computer (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) or NFS share. Requires `cifs-utils` or `nfs-utils` packages to be installed on the Veeam Agent for Linux computer, depending on a network storage type.
- Veeam Backup & Replication 11 or later backup repository.
- Veeam Cloud Connect 11 or later cloud repository.
Network

Consider the following:

- If you back up to a repository managed by a Veeam backup server, Veeam Agent for Linux must be able to establish a direct IP connection to the Veeam Backup & Replication server. Veeam Agent for Linux cannot work with Veeam Backup & Replication that is located behind a NAT gateway.

- Domain names of the Veeam Agent computer, Veeam Backup & Replication server and other servers in the Veeam backup infrastructure must be resolvable into IPv4 addresses.
# Used Ports

Make sure that you open ports listed below to enable proper work of Veeam Agent for Linux.

<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Agent computer</td>
<td>Veeam backup server</td>
<td>TCP</td>
<td>10006</td>
<td>Default port used for communication with the Veeam backup server. Data between the Veeam Agent for Linux computer and backup repositories is transferred directly, bypassing Veeam backup servers.</td>
</tr>
<tr>
<td>Shared folder SMB (CIFS) share</td>
<td>TCP</td>
<td>137 to 139, 445</td>
<td></td>
<td>Ports used as a data transmission channel from the Veeam Agent for Linux computer to the target SMB (CIFS) share. Ports 137 to 139 are used by backup infrastructure components to communicate using NetBIOS.</td>
</tr>
<tr>
<td>Shared folder NFS share</td>
<td>TCP</td>
<td>111, 2049</td>
<td></td>
<td>Standard NFS ports used as a data transmission channel from the Veeam Agent for Linux computer to the target NFS share.</td>
</tr>
<tr>
<td>Veeam Agent computer</td>
<td>TCP</td>
<td>2500 to 3300</td>
<td></td>
<td>Default range of ports used for communication between Veeam Agent for Linux components during data transmission. For every TCP connection that a backup job uses, one port from this range is assigned. Ports must be open for incoming and outgoing traffic. Established connections must be allowed.</td>
</tr>
</tbody>
</table>

## Communication with Veeam Backup & Replication Repositories

<table>
<thead>
<tr>
<th>Veeam Agent computer</th>
<th>Linux server performing the role of a backup repository</th>
<th>TCP</th>
<th>2500 to 3300</th>
<th>Default range of ports used as data transmission channels. For every TCP connection that a backup job uses, one port from this range is assigned.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows server performing the role of a backup repository</td>
<td>TCP</td>
<td>49152 to 65535 (for Microsoft Windows 2008 and newer)</td>
<td></td>
<td>Dynamic RPC port range. For more information, see <a href="#">this Microsoft article</a>.</td>
</tr>
<tr>
<td>From</td>
<td>To</td>
<td>Protocol</td>
<td>Port</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------</td>
<td>----------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>backup repository</td>
<td>TCP</td>
<td>2500 to 3300</td>
<td></td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a backup job uses, one port from this range is assigned.</td>
</tr>
</tbody>
</table>

**Communication with Veeam Cloud Connect Repositories**

<table>
<thead>
<tr>
<th>Veeam Agent computer</th>
<th>Cloud gateway</th>
<th>TCP</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP 6180</td>
<td></td>
<td></td>
<td>Port on the cloud gateway used to transport Veeam Agent data to the Veeam Cloud Connect repository.</td>
</tr>
<tr>
<td>Certificate Revocation Lists</td>
<td>TCP 80 or 443 (most popular)</td>
<td></td>
<td></td>
<td>Veeam Agent computer needs access to CRLs (Certificate Revocation Lists) of the CA (Certification Authority) who issued a certificate to the Veeam Cloud Connect service provider. Generally, information about CRL locations can be found on the CA website.</td>
</tr>
</tbody>
</table>

**IMPORTANT**

The list of ports required for computers booted from the Veeam Recovery Media is the same as the list of ports required for Veeam Agent computers.
Live Patching Support

The live patching technology allows you to patch a running Linux kernel without the need to reboot or change kernel-related files on the disk.

If you plan to use live patching, consider the following limitations:

- Only kGraft, kpatch and Ksplice kernel extensions are supported.
- Live patching is supported only for the following Linux distributions:
  - SLES 11 SP4, 12 SP2 – 15 SP3
  - SLES for SAP 11 SP4, 12 SP2 – 15 SP3
  - RHEL 6.0 – 8.5
  - Oracle Linux 6 – 8.5 (RHCK)
  - Oracle Linux 6 (starting from UEK R2) – Oracle Linux 8 (up to UEK R6 U2, kernel version 5.4.17-2102)

Before live patching, check the following prerequisites:

- Before you start live patching on a production environment, make sure that a kernel patch does not harm your system in any way using a spare Veeam Agent computer.
- Back up an entire Veeam Agent computer before live patching.
- Make sure that there is no backup jobs running on the Veeam Agent computer during live patching.
Installation and Configuration

You can install Veeam Agent for Linux on any Linux-based endpoint whose data you plan to protect — virtual machine or physical device (server, desktop or laptop).
Before You Begin

Before you start the installation process, check the following prerequisites:

1. The computer on which you plan to install Veeam Agent for Linux must satisfy system requirements specified in this document. To learn more, see System Requirements.

2. To install Veeam Agent for Linux software packages, you must use the root account or any user account that has super user (root) privileges on the computer where you plan to install the product.

3. If you have used the Beta version of Veeam Agent for Linux, you must remove Veeam Agent for Linux software packages prior to installing the release version of the product. To learn more, see Uninstalling Veeam Agent for Linux.
Installing Veeam Agent for Linux

NOTE
To make UEFI systems with Secure Boot work with the pre-built veeamsnap kernel module, Veeam Agent requires the Veeam public key enrolled to the MOK list. The key is available in the veeamsnap-ueficert-5.0.2.4567-1.noarch package residing on the Veeam software repository. Veeam Agent requests the key enrollment during the package installation. After that, you must reboot computer to enroll the key into the UEFI database.

After the package installation, you can check that the key enrollment is planned for the next reboot with the following command: mokutil -N. If the command output shows that the key enrollment is not planned, you can do the following:

1. Request the enrollment of the public key manually with the following command: mokutil --import veeamsnap-ueficert.crt.
2. Reboot the Veeam Agent computer to enroll the key into the UEFI database.
3. Check that the key is successfully enrolled with the following command: mokutil -l.

To install Veeam Agent for Linux:

1. Download the Veeam software repository installation package (veeam-release) from the this Veeam webpage, and save the downloaded package on the computer where you plan to install the product.

   TIP
   If the computer where you want to install Veeam Agent for Linux is not connected to the internet, you can download and install Veeam Agent for Linux packages manually. To learn more, see Installing Veeam Agent for Linux in Offline Mode.

2. Navigate to the directory where you have saved the veeam-release package and install the package with the following commands:

   For CentOS / RHEL / Oracle Linux / Fedora

   ```
   rpm -ivh ./veeam-release* && yum check-update
   ```

   For openSUSE / SLES

   ```
   zypper in ./veeam-release* && zypper refresh
   ```

   For Debian / Ubuntu

   ```
   dpkg -i ./veeam-release* && apt-get update
   ```
3. Install Veeam Agent for Linux packages from the Veeam software repository. To install Veeam Agent for Linux, you can use a package manager of your choice that works with software packages in your Linux distribution. For example, use the following commands:

For Fedora

```
yum install veeam
```

For CentOS / RHEL

```
yum install kmod-veeamsnap veeam
```

With this command, the non-DKMS version of the veeamsnap kernel module will be installed from the pre-built kmod-veeamsnap binary package.

NOTE

Alternatively, if the dkms package is already installed in the OS, you can install Veeam Agent with the following command:

```
yum install veeam
```

With this command, the veeamsnap kernel module will be installed from the source RPM package using dkms.

For Oracle Linux

```
yum install veeamsnap
yum install veeam
```

For openSUSE Tumbleweed

```
zypper in veeam
```

For openSUSE Leap 15.3

```
zypper in veeamsnap-kmp-default
zypper in veeam
```

For SLES with Default kernel

```
zypper in veeamsnap-kmp-default
zypper in veeam
```

For SLES with Trace kernel

```
zypper in veeamsnap-kmp-trace
zypper in veeam
```
For SLES with Xen kernel

zypper in veeamsnap-kmp-xen
zypper in veeam

For SLES with PAE kernel

zypper in veeamsnap-kmp-pae
zypper in veeam

For SLES with Preempt kernel

zypper in veeamsnap-kmp-preempt
zypper in veeam

For Debian / Ubuntu

apt-get install veeam
Managing Package Dependencies

The following dependency packages may require special handling in case you see installation errors:

- **The dkms package is not present in default repositories for some Linux distributions. You should obtain it from third-party repositories:**
  - EPEL repository (for CentOS / RHEL / Oracle Linux / Fedora)
  - Packman repository (for openSUSE). To learn more, see Installing dkms in openSUSE.
  
  For SLES, the dkms package is not available in the Packman repository. You must use the package intended for openSUSE. To learn more, see this Veeam KB article.

- **Extended kernels, such as kernel-pae, kernel-uek and other, require appropriate kernel-devel packages to be installed, for example, kernel-pae-devel, kernel-uek-devel, and so on.**

  Version of the kernel-devel package must match your current kernel version. To check your current kernel version, run the `uname -r` command.

  The kernel-devel package may also require special handling for its own dependencies. For example, the libdtrace-ctf package that is a dependency for the kernel-uek-devel package. To learn more, see this Veeam KB article.

  [For RHEL and derivatives] If the yum package manager installs packages that do not match your current kernel version, you should either update your system or fetch older versions of the required packages from the CentOS Vault repository.

### Installing dkms in openSUSE

In openSUSE systems, while installing the dkms package, you may see an error similar to the following:

| Problem: nothing provides kernel-devel needed by dkms-2.2.0.3-14.1.noarch |
|-----------------------------|---------------------------------|
| Solution 1: do not install dkms-2.2.0.3-14.1.noarch |
| Solution 2: break dkms-2.2.0.3-14.1.noarch by ignoring some of its dependencies |

To install the dkms package, do the following:

1. **Make sure that you have an appropriate kernel-devel package installed and its version matches your kernel version. For example:**

   ```
   root@localhost:~> rpm -qa | grep kernel-default
   kernel-default-devel-3.0.101-91.1
   kernel-default-3.0.101-91.1
   ```

2. **Install the dkms package ignoring dependencies:**

   ```
   zypper -n install --force dkms
   ```

3. **Make sure that you have allowed unsupported modules. To learn more, see this SUSE webpage.**
Installing Veeam Agent for Linux in Offline Mode

If a computer where you want to install Veeam Agent for Linux has no connection to the internet, for example, for security reasons, you can install Veeam Agent in the offline mode. In this scenario, you do not need to download and install the Veeam software repository installation package (veeam-release). Instead, you need to download all Veeam Agent packages from the Veeam software repository and install them on the target computer.

To install Veeam Agent:

1. On a computer that is connected to the internet, download Veeam Agent packages intended for your Linux distribution from the Veeam software repository.
   The repository has the following structure:
   - For Debian packages: Package format > Package
     For example, Veeam Agent packages in the Debian format reside in the /deb/veeam/, /deb/veeamsnap/ and /deb/veeam-nosnap/ folders of the Veeam software repository.
   - For RPM packages: Package format > Distribution > Version > Architecture
     For example, Veeam Agent packages for 64-bit RHEL 7 reside in the /rpm/el/7/x86_64/ folder of the Veeam software repository, and packages for 64-bit SLES 15 SP2 reside in the /rpm/sles/SLE_15_SP2/x86_64/ folder.

2. Save Veeam Agent packages to a directory that can be accessed from the computer where you want to install the product, for example, a directory on a local drive or USB drive, or a network shared folder.

3. On the computer where you want to install Veeam Agent, navigate to the directory where you have saved the packages and install Veeam Agent:
   - Installing Veeam Agent for Linux in CentOS / RHEL
   - Installing Veeam Agent for Linux in Oracle Linux
   - Installing Veeam Agent for Linux in Fedora
   - Installing Veeam Agent for Linux in SLES
   - Installing Veeam Agent for Linux in openSUSE
   - Installing Veeam Agent for Linux in Debian / Ubuntu

**TIP**

You can also set up a local mirror of the Veeam software repository in your internal network and add this repository to the list of software sources on a computer where you want to install the product. These operations may differ depending on the Linux distribution and package manager that you use. To learn more, refer to the documentation of your Linux distribution.

After you add a local repository to the list of software sources on a computer, you will be able to install and upgrade Veeam Agent in a regular way. To learn more, see Installing Veeam Agent for Linux and Upgrading Veeam Agent for Linux.
Installing Veeam Agent for Linux in CentOS / RHEL

To install Veeam Agent for Linux, use the following commands:

For 32-bit RHEL 6

```
rpm -i <...>/kmod-veeamsnap-5.0.2.4567-2.6.32_131.0.15.el6.i386.rpm
rpm -i <...>/veeam-5.0.2.4567-1.el6.i386.rpm
```

For 64-bit RHEL 6

```
rpm -i <...>/kmod-veeamsnap-5.0.2.4567-2.6.32_131.0.15.el6.x86_64.rpm
rpm -i <...>/veeam-5.0.2.4567-1.el6.x86_64.rpm
```

For CentOS 7 / RHEL 7

```
rpm -i <...>/kmod-veeamsnap-5.0.2.4567-1.el7.x86_64.rpm
rpm -i <...>/veeam-5.0.2.4567-1.el7.x86_64.rpm
```

For CentOS 8 / RHEL 8

```
rpm -i <...>/kmod-veeamsnap-5.0.2.4567-4.18.0_80.el8.x86_64.rpm
rpm -i <...>/veeam-5.0.2.4567-1.el8.x86_64.rpm
```

where:

<...> — path to a directory where you have saved Veeam Agent packages.

**NOTE**

The pre-built veeamsnap binaries require kernel 2.6.32-131.0.15 or later for RHEL 6 (excluding 2.6.32-279.el6.i686) and kernel 3.10.0-123 or later for CentOS / RHEL 7.0 – 7.7 to operate.
Installing Veeam Agent for Linux in Oracle Linux

To install Veeam Agent for Linux, use the following commands:

**For Oracle Linux 6**

```
rpm -i <...>/veeamsnap-5.0.2.4567-1.noarch.rpm
rpm -i <...>/veeam-5.0.2.4567-1.el6.x86_64
```

**For Oracle Linux 7**

```
rpm -i <...>/veeamsnap-5.0.2.4567-1.noarch.rpm
rpm -i <...>/veeam-5.0.2.4567-1.el7.x86_64.rpm
```

**For Oracle Linux 8**

```
rpm -i <...>/veeamsnap-5.0.2.4567-1.noarch.rpm
rpm -i <...>/veeam-5.0.2.4567-1.el8.x86_64.rpm
```

where:

<...> — path to a directory where you have saved Veeam Agent packages.
Installing Veeam Agent for Linux in Fedora

To install Veeam Agent for Linux, use the following commands:

```
rpm -i <...>/veeamsnap-5.0.2.4567-1.noarch.rpm
rpm -i <...>/veeam-5.0.2.4567-1.fc24.x86_64.rpm
```

where:

<...> — path to a directory where you have saved Veeam Agent packages.
Installing Veeam Agent for Linux in SLES

**NOTE**

If you use a Trace, Xen, PAE, or preempt kernel, you need to choose the corresponding `veeamsnap` package for installation instead of the default one, for example, `veeamsnap-kmp-trace-5.0.2.4567_3.0.101_63-2.1.i586.rpm` instead of `veeamsnap-kmp-default-5.0.2.4567_3.0.101_63-2.1.i586.rpm`.

To install Veeam Agent for Linux, use the following commands:

**For 32-bit SLES 11 SP4**

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k3.0.101_63-2.i586.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles11.i386.rpm
```

**For 64-bit SLES 11 SP4**

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k3.0.101_63-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles11.x86_64.rpm
```

**For 64-bit SLES 12 SP2**

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k4.4.21_69-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```

**For 64-bit SLES 12 SP3**

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k4.4.73_5-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```

**For 64-bit SLES 12 SP4**

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k4.12.14_94.41-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```

**For 64-bit SLES 12 SP5**

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k4.12.14_120-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```

**For 64-bit SLES 15 SP0**

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k4.12.14_23-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```
For 64-bit SLES 15 SP1

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k4.12.14_195-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```

For 64-bit SLES 15 SP2

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k5.3.18_22-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```

For 64-bit SLES 15 SP3

```bash
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k5.3.18_57-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.sles12.x86_64.rpm
```

where:

<...> — path to a directory where you have saved Veeam Agent packages.
Installing Veeam Agent for Linux in openSUSE

To install Veeam Agent for Linux, use the following commands:

For 32-bit openSUSE Tumbleweed

```
zypper in <...>/veeamsnap-5.0.2.4567-1.sles.noarch.rpm
zypper in <...>/veeam-5.0.2.4567-1.suse.i386.rpm
```

For 64-bit openSUSE Tumbleweed

```
zypper in <...>/veeamsnap-5.0.2.4567-1.sles.noarch.rpm
zypper in <...>/veeam-5.0.2.4567-1.suse.x86_64.rpm
```

For 64-bit openSUSE Leap 15.2

```
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k5.3.18_lp152.19-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.suse.x86_64.rpm
```

For 64-bit openSUSE Leap 15.3

```
zypper in <...>/veeamsnap-kmp-default-5.0.2.4567_k5.3.18_57-2.x86_64.rpm
zypper in <...>/veeam-5.0.2.4567-1.suse.x86_64.rpm
```

where:

`<...>` — path to a directory where you have saved Veeam Agent packages.
## Installing Veeam Agent for Linux in Debian / Ubuntu

To install Veeam Agent for Linux, use the following commands:


```
dpkg -i <...>/veeamsnap_5.0.2.4567_all.deb  
dpkg -i <...>/veeam_5.0.2.4567_i386.deb
```


```
dpkg -i <...>/veeamsnap_5.0.2.4567_all.deb  
dpkg -i <...>/veeam_5.0.2.4567_amd64.deb
```

where:

<...> — path to a directory where you have saved Veeam Agent packages.
Upgrading Veeam Agent for Linux

For Veeam Agent for Linux, upgrade to newer versions is supported. You can start the upgrade process when the new version becomes available.

During the upgrade process, configuration and backup files that were created with the previous version of Veeam Agent are not impacted in any way.

IMPORTANT
Before starting the upgrade process, make sure that there are no jobs running on the Veeam Agent computer.

The upgrade procedure differs depending on the Linux distribution that you use:

- Upgrading Veeam Agent for Linux in CentOS / RHEL
- Upgrading Veeam Agent for Linux in Fedora / Oracle Linux
- Upgrading Veeam Agent for Linux in openSUSE
- Upgrading Veeam Agent for Linux in SLES 11 SP4
- Upgrading Veeam Agent for Linux in SLES 12 SP2 – SLES 15 SP3
- Upgrading Veeam Agent for Linux in Debian / Ubuntu
Upgrading Veeam Agent for Linux in CentOS / RHEL

To upgrade Veeam Agent for Linux, use the following commands:

```
yum update veeam
rpm -e --nodeps dkms veeamsnap
yum install kmod-veeamsnap*
```

or

```
yum install kmod-veeamsnap*
yum update veeam
rpm -e dkms veeamsnap
```

* With these commands, a pre-built `veeamsnap` binary package will be installed in your system. To stay on the DKMS version of the `veeamsnap` kernel module, use the following command for upgrade:

```
yum update veeamsnap && yum update veeam
```
Upgrading Veeam Agent for Linux in Fedora / Oracle Linux

To upgrade Veeam Agent for Linux, use the following command:

```
yum update veeam
```
Upgrading Veeam Agent for Linux in openSUSE

To upgrade Veeam Agent for Linux, use the following commands:

**For openSUSE Tumbleweed**

```
zypper up veeam
```

**For openSUSE Leap 15.2**

```
zypper in veeamsnap-kmp-default-5.0.2.4567_k5.3.18_lp152.19-2.x86_64
zypper in --force veeamsnap-kmp-default-5.0.2.4567_k5.3.18_lp152.19-2.x86_64
```

**For openSUSE Leap 15.3**

```
zypper in veeamsnap-kmp-default-5.0.2.4567_k5.3.18_57-2.x86_64
zypper in --force veeamsnap-kmp-default-5.0.2.4567_k5.3.18_57-2.x86_64
```

With these commands, a pre-built `veeamsnap` binary package will be installed in your system. The `--force` key is required to properly replace the missing link to `.ko` in case of update from the DKMS version of the `veeamsnap` kernel module to a pre-built binary. To stay on the DKMS version, use the following command for upgrade:

```
zypper update veeam
```
Upgrading Veeam Agent for Linux in SLES 11 SP4

To upgrade Veeam Agent for Linux, use the following commands:

**For Default kernel**

```
zypper in veeamsnap-kmp-default
zypper in --force veeamsnap-kmp-default
```

**For Xen kernel**

```
zypper in veeamsnap-kmp-xen
zypper in --force veeamsnap-kmp-xen
```

**For Trace kernel**

```
zypper in veeamsnap-kmp-trace
zypper in --force veeamsnap-kmp-trace
```

**For PAE kernel**

```
zypper in veeamsnap-kmp-pae
zypper in --force veeamsnap-kmp-pae
```

With these commands, a pre-built `veeamsnap` binary package will be installed in your system. The `--force` key is required to properly replace the missing link to `.ko` in case of update from the DKMS version of the `veeamsnap` module to a pre-built binary. To stay on the DKMS version, use the following command for upgrade:

```
zypper update veeam
```
Upgrading Veeam Agent for Linux in SLES 12 SP2 - SLES 15 SP3

To upgrade Veeam Agent for Linux:

1. Download the Veeam software repository installation package (veeam-release) from the Veeam Download page, and save the downloaded package on the computer where you plan to install the product.

2. Install the Veeam software repository installation package with the following command:

   ```
   zypper in ./veeam-release* && zypper refresh
   ```

3. Upgrade Veeam Agent for Linux with the following commands:

   **For Default kernel**
   ```
   zypper in veeamsnap-kmp-default
   zypper in --force veeamsnap-kmp-default
   ```

   **Preempt kernel**
   ```
   zypper in veeamsnap-kmp-preempt
   zypper in --force veeamsnap-kmp-preempt
   ```

   With this command, a pre-built veeamsnap binary package will be installed in your system. The `--force` key is required to properly replace the missing link to `.ko` in case of update from the DKMS version of the veeamsnap module to a pre-built binary. To stay on the DKMS version, use the following command for upgrade:

   ```
   zypper update veeam
   ```
## Upgrading Veeam Agent for Linux in Debian / Ubuntu

To upgrade Veeam Agent for Linux, use the following commands:

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>apt-get update</code></td>
</tr>
<tr>
<td><code>apt-get install veeam</code></td>
</tr>
</tbody>
</table>
Granting Permissions to Users

When you install Veeam Agent for Linux, the product program files are placed to the folders on the system volume. For full access to Veeam Agent files, super user (root) privileges are required. Rights to execute product files and run commands are also granted to users that belong to the veeam group.

The veeam group is automatically created by Veeam Agent at the process of the product installation. To let regular users work with Veeam Agent without the need to gain root privileges, you can add the necessary users to this group. Users in the veeam group will be able to execute Veeam Agent commands and perform backup and restore tasks under regular user account.

To add a user to the veeam group, in most of Linux distributions you can use the following command:

```
usermod -a -G veeam <username>
```

where:

<username> — name of the account to which you want to grant access to Veeam Agent.

For example:

```
root@srv01:~# usermod -a -G veeam user
```

**IMPORTANT**

Consider the following:

- To add a user to the veeam group, you must have super user (root) privileges in the Linux OS.
- After the user is added to the veeam group, the user must re-login to the Linux OS.
- Add only trusted users to the veeam group. Veeam Agent for Linux daemon runs and executes commands and scripts with the super user privileges. Thus, users who belong to this group can potentially escalate their privileges through the creative use of pre-freeze/post-thaw or pre-job/post-job scripts.

To check whether the user who is currently logged in to the Linux OS is added to the veeam group, you can use the following command:

```
groups
```

For example:

```
user@srv01:~$ groups
user adm cdrom sudo dip plugdev lpadmin sambashare veeam
```
Performing Initial Setup

After you install Veeam Agent for Linux, you can use the Veeam Agent for Linux control panel to perform initial product setup. When you launch the control panel for the first time, Veeam Agent displays the initial setup wizard. The wizard offers you to accept license agreements, install a license and create a custom Veeam Recovery Media that will include drivers of your Veeam Agent computer.

To perform initial setup, launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command. Then use the initial setup wizard to complete the following steps:

1. Accept Veeam and third-party license agreements.
2. Create a custom Veeam Recovery Media.
3. Install a license.
Step 1. Accept License Agreements

At the Agreements step of the initial setup wizard, accept the terms of the product license agreement and license agreements for third-party components of the product. You must accept the license agreements to start using the product. Until you accept the license agreements, you will not be able to perform backup and data recovery tasks with the Veeam Agent for Linux control panel and command line interface.

To accept the license agreements:

1. Make sure that the I accept the terms of the Veeam license agreement option is selected and press Space.
2. Select the I accept the terms of the 3rd party components license agreements option with the Down or Tab key and press Space.
3. Press Enter.

![License Agreement Screen]

License Agreements

<table>
<thead>
<tr>
<th>Agreements</th>
<th>Recovery ISO License</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You must accept the license terms to proceed</td>
</tr>
<tr>
<td></td>
<td>(X) I accept the terms of the Veeam license agreement</td>
</tr>
<tr>
<td></td>
<td><a href="https://www.veeam.com/eula.html">https://www.veeam.com/eula.html</a></td>
</tr>
<tr>
<td></td>
<td>Local path: /usr/share/doc/veeam/EULA</td>
</tr>
<tr>
<td></td>
<td>(X) I accept the terms of the 3rd party components license agreements</td>
</tr>
<tr>
<td></td>
<td>Local path: /usr/share/doc/veeam/3rdPartyNotices.txt</td>
</tr>
</tbody>
</table>

[Next]  [Cancel]
Step 2. Create Custom Veeam Recovery Media

At the **Recovery ISO** step of the initial setup wizard, specify settings for the custom Veeam Recovery Media.

In addition to the generic Veeam Recovery Media that is available for download at the Veeam website, you can create a custom Veeam Recovery Media. This option may be helpful if your computer uses hardware that requires drivers not included in the generic Veeam Recovery Media. When you create the custom Veeam Recovery Media, Veeam Agent for Linux copies the Linux kernel running on your computer with its currently loaded modules and includes them into the custom recovery media.

Before you create a custom Veeam Recovery Media, check the following prerequisites:

- The Linux system must have the `genisoimage` package installed. For openSUSE and SLES 15 SPO – SP3 distributions, the Linux system must have the `mkisofs` package installed instead.
- The Linux system must have the `mksquashfs` and `unsquashfs` utilities installed.
- For custom Veeam Recovery Media with EFI support, the Linux system must have the following packages installed:
  - `xorriso`
  - `isolinux` (or `syslinux`, if the software package repository of your Linux distribution lacks the `isolinux` package)
- For the scenario where you create a custom Veeam Recovery Media using the **Download and patch ISO** option, the Linux system must have the `wget` utility installed.

**TIP**

If you do not want to create a custom Veeam Recovery Media at the process of initial product setup, switch to the **Next** button with the **Tab** key and press **Enter**. You will proceed immediately to the **License** step of the initial setup wizard.

You can create the custom Veeam Recovery Media later, at any time you need, using the Veeam Agent for Linux command line interface. To learn more, see [Creating Custom Veeam Recovery Media](#).

To specify settings for the custom Veeam Recovery Media:

1. Make sure that the **Patch Veeam Recovery Media ISO** option is selected and press **Space**.
2. If you want the Veeam Recovery Media to be able to boot on EFI-based systems, select the **EFI system** option with the **Tab** key and press **Space**.
   
   If you do not enable this option, the custom Veeam Recovery Media will be able to boot on BIOS-based systems only.
3. Press **Tab** and select how you want to create a custom Veeam Recovery Media depending on the location of the generic recovery media ISO file:
   - If you did not download the generic Veeam Recovery Media from the Veeam website, make sure that the **Download and patch ISO** option is selected and press **Tab**. When you start the custom recovery media creation process, Veeam Agent for Linux will download the ISO file of the generic Veeam Recovery Media from the [Veeam software repository](#) to the `/tmp/veeam` directory on the Veeam Agent computer and use this image to create the custom Veeam Recovery Media.

   Veeam Agent for Linux automatically downloads one of the following Veeam Recovery Media ISO files depending on the Veeam Agent computer architecture:
- *veeam-recovery-i386-5.0.0.iso* — for x86 computers that run Linux kernel version 3.10 and later. The size of the downloaded ISO file is about 450 MB.
- *veeam-recovery-amd64-5.0.0.iso* — for x64 computers that run Linux kernel version 3.10 and later. The size of the downloaded ISO file is about 500 MB.
- *veeam-recovery-media-5.0.0.iso* — for x86 and x64 computers that run Linux kernel version earlier than 3.10. The size of the downloaded ISO file is about 150 MB.

If you have already downloaded a recovery media ISO file to a local directory on the Veeam Agent computer or to a network shared folder, select the **Patch local ISO** option with the Down key and press Tab. If you select this option, you will be able to specify a path to the ISO file of the generic Veeam Recovery Media.

The name of the generic Veeam Recovery Media ISO file depends on the recovery image version, Veeam Agent computer architecture and the source from which you downloaded the ISO file: from the product download page or Veeam software repository. To learn more, see Veeam Recovery Media Versions.

4. If you selected the **Patch local ISO** option, in the **Path to ISO** field, specify a path to the ISO file of the generic Veeam Recovery Media:
   a. Select the **Browse** option with the **Tab** key and press **Enter**.
   b. In the **Path to ISO** window, select the necessary directory and press **Enter**.
   c. Repeat the step 'b' until a path to the directory in which the recovery media ISO file resides appears in the **Current directory** field.
   d. In the directory where the recovery media ISO file resides, select the ISO file and press **Enter**.

5. In the **Save patched ISO to** field, specify a path to the resulting ISO file of the custom Veeam Recovery Media:
   a. Select the **Browse** option with the **Tab** key and press **Enter**.
   b. In the **Save patched ISO to** window, select the necessary directory and press **Enter**.
   c. Repeat the step 'b' until a path to the directory where you want to save the resulting custom recovery media ISO file appears in the **Current directory** field.
   d. Select the **OK** button with the **Tab** key and press **Enter**.

6. To start the custom recovery media creation process, select the **Next** button with the **Tab** key and press **Enter**.
## Custom Recovery Media

<table>
<thead>
<tr>
<th>Agreements</th>
<th>Recovery ISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Add drivers from this machine into Veeam Recovery ISO. It might be required for a successful bare-metal restore:</td>
</tr>
<tr>
<td></td>
<td>[X] Patch Veeam Recovery Media ISO</td>
</tr>
<tr>
<td></td>
<td>[X] EFI system</td>
</tr>
<tr>
<td></td>
<td>( ) Download and patch ISO</td>
</tr>
<tr>
<td></td>
<td>(X) Patch local ISO</td>
</tr>
</tbody>
</table>

Path to ISO: `recovery-media.iso` [Browse]
Save patched ISO to: `/home/user01/veeam` [Browse]

[Prev] [Next] [Cancel]
Step 3. Install Product License

At the **License** step of the initial setup wizard, install the license. You can choose to install the license immediately or postpone this operation.

- If you choose to install the license, you can immediately browse for the license key on your computer and complete the license installation process.
- If you choose to postpone the license installation process, you will be able to install a license later at any time you need.

Until you install a license, Veeam Agent for Linux will operate in the Free edition. To learn more, see [Product Editions](#).

**NOTE**

If you choose not to install a license and use Veeam Agent in the Free edition, Veeam Agent will display a notification offering to install a license every time you open the control panel. The notification will appear in the control panel until Veeam Agent completes the first backup job session.

To install a license:

1. In the **File location** field, specify a path to the license key:
   a. Select the **Browse** option with the **Tab** key and press **Enter**.
   b. In the **Choose license file location** window, select the necessary directory and press **Enter**.
   c. Repeat the step 'a' until a path to the directory in which the license key resides appears in the **Current directory** field.
   d. In the directory where the license key resides, select the license key and press **Enter**.

2. In the **Choose agent edition to use on this computer** section, select the product edition in which Veeam Agent will operate and press **Enter** to install the license and finish working with the initial setup wizard.

**TIP**

Consider the following:

- If you do not want to install a license, to finish working with the initial setup wizard, switch to the **Finish** button with the **Tab** key and press **Enter**.
- You can view information about the installed license (expiration date, status of the license, current edition of the product and so on) in the Veeam Agent control panel or using the Veeam Agent command line interface. To learn more, see [Viewing License](#).
Provide license file for Veeam Agent for Linux

<table>
<thead>
<tr>
<th>Agreements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery ISO</td>
</tr>
<tr>
<td>License</td>
</tr>
</tbody>
</table>

**File Location:**

`/var/lib/veeam/license/subscription_ent+1000.lic` [Browse]

Choose agent edition to use on this computer:

- [ ] Workstation
- [X] Server

If you do not have a license, then just click [Finish] and the product will operate in Free Edition mode.
Configuring Advanced Settings

Veeam Agent for Linux allows you to configure the following settings:

- HTTP proxy settings for Veeam Cloud Connect repository
- Connection settings for Veeam backup server
HTTP Proxy Settings for Veeam Cloud Connect Repository

If you want to use Veeam Agent for Linux to back up your data to a Veeam Cloud Connect repository, it might be required that you specify HTTP proxy settings for Veeam Agent.

Veeam Agent computer needs access to CRLs (Certificate Revocation Lists) of the CA (Certification Authority) who issued a certificate to the Veeam Cloud Connect service provider. In case it is not possible to establish a direct connection to CRLs, you must configure an HTTP proxy and specify settings to connect to the proxy in Veeam Agent.

To specify settings for an HTTP proxy, uncomment and edit the following lines in the [cloudconnect] section of the /etc/veeam/veeam.ini configuration file:

```
[cloudconnect]
...
# httpproxylogin= <username>
...
# httpproxypasswd= <password>
...
# httpproxyurl= <URL>
```

where:
- `<username>` — name of the account used to connect to the HTTP proxy.
- `<password>` — password of the account used to connect to the HTTP proxy.
- `<URL>` — URL of a proxy used for CRL checks.

**NOTE**

If the proxy does not require authentication, you do not need to specify the account name and password. Keep in mind that only the basic authentication method is supported for connection to a proxy.

For example:

```
[cloudconnect]
...
# HTTP proxy login
httpproxylogin= user01
# HTTP proxy password
httpproxypasswd= P@ssw0rd
# HTTP proxy URL for CRL checks
httpproxyurl= http://proxy.company.lan:3128
```
Connection Settings for Veeam Backup Server

If you want to connect Veeam Agent computer to Veeam backup server as a member of the protection group for pre-installed Veeam Agents, you must apply connection settings from the configuration file. The configuration file is one of the Veeam Agent for Linux setup files that you must obtain from your System Administrator. To learn more about protection group for pre-installed Veeam Agents, see the Protection Group Types section in the Veeam Agent Management Guide.

To connect Veeam Agent for Linux to Veeam backup server:

1. Get the configuration file from your System Administrator and upload this file on the Veeam Agent computer.
2. Navigate to the directory where you have saved the configuration file and run the following command:

   ```
   veeamconfig mode setvbrsettings --cfg <file_name>.xml
   ```

   where `<file_name>` is a configuration file name.

   Alternatively, you can specify the full path to the configuration file with the `--cfg` option.

   For example:

   ```
   user@srv01:~# veeamconfig mode setvbrsettings --cfg /home/Linux\ Servers\ Distr ibs/Linux/LinuxServers.xml
   ```

Mind that the connection between Veeam backup server and Veeam Agent computer added as a member of the protection group for pre-installed Veeam Agents is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. To synchronize Veeam Agent immediately, run the following command from the Veeam Agent computer:

```
veeamconfig mode syncnow
```
Managing Veeam Agent Operation Mode

Veeam Agent for Linux can operate in different modes. Depending on the selected mode, Veeam Agent offers different features and limitations. To learn more, see Standalone and Managed Operation Modes.

Veeam Agent allows you to perform the following actions to manage the operation mode:

- View operation mode details.
- Reset to the standalone operation mode.
- Connect to Veeam backup server.
- Synchronize with Veeam backup server.
- Export logs to Veeam backup server.
Viewing Operation Mode

To view the current Veeam Agent operation mode, use the following command:

```
veeamconfig mode info
```

Veeam Agent displays the operation mode details:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Name of the backup repository that manages Veeam Agent. If Veeam Agent operates in the standalone mode, Veeam Agent will display the <em>Not Set</em> value.</td>
</tr>
<tr>
<td>Mode</td>
<td>Current Veeam Agent operating mode. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• <em>Not Set</em> — Veeam Agent operates in the standalone mode.</td>
</tr>
<tr>
<td></td>
<td>• <em>Job</em> — Veeam Agent operates in the managed mode. Veeam Agent computer is protected by a backup job managed by backup server.</td>
</tr>
<tr>
<td></td>
<td>• <em>Policy</em> — Veeam Agent operates in the managed mode. Veeam Agent computer is protected by a backup job managed by Veeam Agent for Linux. Veeam Agent computer is connected to the Veeam backup server as a member of any protection group excluding protection group for pre-installed Veeam Agents.</td>
</tr>
<tr>
<td></td>
<td>• <em>Catch-All</em> — Veeam Agent operates in the managed mode. Veeam Agent computer is protected by a backup job managed by Veeam Agent for Linux. Veeam Agent computer is connected to the Veeam backup server as a member of a protection group for pre-installed Veeam Agents.</td>
</tr>
</tbody>
</table>

Keep in mind that features and limitations of Veeam Agent operating in the managed mode are different from those in the standalone mode. To learn more about managed mode, see the Agent Management Guide.

For example:

```
user@srv01:-$ veeamconfig mode info
Owner:  Backup server (backupserver001.tech.local)
Mode:   Catch-All
```

If Veeam Agent operates in the managed mode, you can reset it to the standalone mode at any time. To learn more, see Resetting to Standalone Operation Mode.
Resetting to Standalone Operation Mode

If Veeam Agent operates in the managed mode, you can manually reset it to the standalone mode from the Veeam Agent side. To learn more about operation modes, see the Standalone and Managed Operation Modes.

Before you reset Veeam Agent to the standalone mode, consider the following:

- All backup jobs configured on Veeam Agent computer will be deleted. If you plan to protect this computer with a standalone Veeam Agent, you will need to create new backup jobs.
- Veeam backup server settings including protection group configuration settings will be deleted.
- Previously created backup files will remain in the target backup repository. If the target repository is managed by the Veeam backup server, in the Veeam Backup & Replication console, they will be marked as Orphaned.
- If you want to reset Veeam Agent that operates in the Job or Policy mode, we recommend that you do the following:
  - Remove Veeam Agent computer from the protection group using the Veeam Backup & Replication console. To learn more about removing computers from a protection group in the Veeam Backup & Replication console, see the Removing Computer from Protection Group section in the Agent Management Guide.
  - If Veeam Agent does not automatically switch to the standalone mode after that, reset the operating mode on the Veeam Agent computer.
  - If Veeam Agent operates in the Catch-All mode, Veeam Agent computer will be automatically removed from the protection group for pre-installed Veeam Agents in Veeam Backup & Replication.

To reset Veeam Agent to the standalone operating mode, run the following command:

```
veeamconfig mode reset
```

You can use the `--force` option to override additional input prompts and error messages:

```
veeamconfig mode reset --force
```
Connecting to Veeam Backup & Replication

If you want to connect a Veeam Agent computer to the Veeam backup server as a member of the protection group for pre-installed Veeam Agents, you must apply connection settings from the configuration file. The configuration file is one of the Veeam Agent for Linux setup files that you must obtain from your System Administrator. To learn more about deployment using external tools, see the Deploying Veeam Agent for Linux section in the Agent Management Guide.

To connect Veeam Agent for Linux to Veeam backup server:

1. Get the configuration file from your System Administrator and upload this file on the Veeam Agent computer.
2. Navigate to the directory where you have saved the configuration file and run the following command:

   ```bash
   veeamconfig mode setvbrsettings --cfg <file_name>.xml --force
   ```

   where:
   - `<file_name>` — configuration file name.
   - `--force` — with this option enabled, Veeam Agent will override additional input prompts and error messages. This parameter is optional.

Alternatively, you can specify the full path to the configuration file with the `--cfg` option.

For example:

```
user@srv01:~$ veeamconfig mode setvbrsettings --cfg /home/Linux\ Servers\ Dists/Linux/LinuxServers.xml
```
Synchronizing with Veeam Backup Server

After you connected Veeam Agent to the Veeam backup server, you may need to synchronize them. The reason is that the connection between the Veeam backup server and Veeam Agent computer added as a member of the protection group for pre-installed Veeam Agents is not persistent. Veeam Agent synchronizes with Veeam Backup & Replication every 6 hours. During the synchronization, Veeam Agent gets updated backup policies and configuration settings from the Veeam backup server, the Veeam backup server gets certificate details and session logs from Veeam Agent.

Keep in mind that this command is available only for Veeam Agent connected to the Veeam backup server as a member of the protection group for pre-installed Veeam Agents. To learn more, see the Protection Group Types section in the Veeam Agent Management Guide.

To synchronize Veeam Agent immediately, run the following command:

```
veeamconfig mode syncnow
```
Exporting Logs to Veeam Backup Server

If Veeam Agent is connected to the Veeam backup server as a member of the protection group for pre-installed Veeam Agents, Veeam Agent can collect product logs, export them to an archive file and send to the Veeam backup server. This operation may be required if you want to report an issue and need to attach log files to the support case.

Keep in mind that this command is available only for Veeam Agent connected to the Veeam backup server as a member of the protection group for pre-installed Veeam Agents. To learn more, see the Protection Group Types section in the Agent Management Guide.

To export logs, use the following command:

```bash
veeamconfig mode exportdebuglogs
```

Veeam Agent will collect logs, export them to an archive file with the name `veeam_logs_<date>_<time>.tar.gz` and save the archive to the following folder on the Veeam backup server:

```
C:\ProgramData\Veeam\Backup\Endpoint\Other\AgentLogs\<computer_name>
```

where `<computer_name>` — name of the computer with Veeam Agent installed.

**TIP**

You can also export logs to a local directory on the Veeam Agent computer. To learn more, see Exporting Product Logs.
Uninstalling Veeam Agent for Linux

To uninstall Veeam Agent for Linux, you need to remove the `veeam` and `veeamsnap` packages. For this operation, you can use any package manager that works with software packages in your Linux distribution.

The following examples show commands to uninstall Veeam Agent:

*For CentOS / RHEL / Oracle Linux / Fedora*

```bash
yum remove veeam veeamsnap
```

*For openSUSE / SLES*

```bash
zypper rm veeam veeamsnap
```

*For Debian / Ubuntu*

```bash
apt-get remove veeam veeamsnap
```
Getting Started

To protect your computer from a disaster of any kind, you must perform the following operations in Veeam Agent for Linux:

1. **Define what data you want to back up and configure the backup job.**
   
   Before you configure the backup job, you should decide on the following backup details:
   
   - **Backup destination:** where you want to store your backed-up data.
   - **Backup scope:** entire computer image, individual computer volumes or specific computer folders and files.
   - **Backup schedule:** how often you want to back up your data.

   After that, you can configure one or several backup jobs. The backup job captures the data that you have added to the backup scope and creates a chain of restore points in the target location. If your data gets lost or corrupted, you can restore it from the necessary restore point.

   In Veeam Agent, you can configure the backup job in one of the following ways:
   
   - With the Backup Job wizard
   - With the command line interface

2. **Monitor backup task performance.**

   You can use the Veeam Agent Control Panel to check how backup tasks are being performed, what errors have occurred during backup job sessions and so on. You can also use Veeam Agent command line interface to get information on backup and restore sessions status and view session logs. To learn more, see **Reporting**.

3. In case of a disaster, you can **restore the entire computer image or specific data** on the computer. With Veeam Agent, you can perform data recovery operations in several ways:

   - You can boot from the Veeam Recovery Media and perform volume-level restore or file-level restore.
   - You can perform volume-level restore with Veeam Agent command line interface.
   - You can perform file-level restore with the Veeam Agent File Level Restore wizard.
   - You can export backup to a VHD virtual disk and attach this disk to a virtual machine to recover your computer in virtual environment.

   To learn more, see **Performing Restore**.
Getting to Know User Interface

With Veeam Agent for Linux, you can perform backup, restore and configuration tasks in the following ways:

- **With Veeam Agent control panel**
  Veeam Agent control panel is a GUI-like user interface based on the `ncurses` programming library. With Veeam Agent control panel, you can perform all basic data protection tasks. You can configure a backup job, start and stop backup jobs, monitor backup job session performance and recover files and folders. When you perform restore tasks after booting from the Veeam Recovery Media, you can also perform volume-level restore with the Veeam Recovery Media wizard.

- **With the command line interface**
  With Veeam Agent command line interface, in addition to operations that can be performed with the Veeam Agent control panel, you can perform a set of advanced tasks. For example, you can:

  - Configure advanced settings for backup jobs: specify compression level and data block size.
  - Perform operations with backup repositories.
  - Perform volume-level restore without the need to boot from the Veeam Recovery Media.
  - Export backups to VHD virtual disks.
  - Monitor performance and status of any backup, restore and other data transfer session that was started in Veeam Agent.
  - View detailed information on every backup that was created with Veeam Agent.
  - Export/import Veeam Agent configuration database to/from a configuration file.
Veeam Agent for Linux Control Panel

Veeam Agent for Linux control panel is a GUI-like user interface that lets users perform main backup and restore tasks in an easy way. With Veeam Agent for Linux control panel, you do not need to work with Linux shell and remember numerous commands. However, some advanced Veeam Agent for Linux operations are not supported by the control panel and can be performed with the command line interface only.

**IMPORTANT**

You cannot use Veeam Agent for Linux control panel on terminals that do not support colors (for example, VT100).

To launch the Veeam Agent for Linux control panel, you can use the following commands:

```
veeamconfig ui
```

or

```
veeam
```

**NOTE**

Veeam Agent for Linux control panel is based on the ncurses programming library. To use the Veeam Agent for Linux control panel, you must have the ncurses library installed in your Linux OS. To learn more, see System Requirements.

When you launch the Veeam Agent for Linux control panel for the first time, Veeam Agent for Linux offers you to perform initial product setup. To learn more, see Performing Initial Setup.

After you perform initial product setup, before you configure the first backup job, you can use the Veeam Agent for Linux control panel to perform the following operations:

- Configure a new backup job.
- Restore files and folders from existing backup.
- Manage license and product logs.
- Create a custom Veeam Recovery Media

After you configure one or several backup jobs, you can also use the control panel to start a backup job and work with backup job sessions.
Navigating Veeam Agent for Linux Control Panel

In the Veeam Agent for Linux control panel, the use of a mouse is not supported. To start an operation, you need to use a specific key on your keyboard. For example, you can press the 'c' key to start the backup job configuration, press the 's' key to start a backup job or press the 'r' key to start the file-level restore process. Short help information on the currently available operations and keys is displayed at the bottom of the control panel.

To navigate the control panel, backup job configuration and file-level restore wizards, you can use the following keys:

- **Tab** — to switch between controls and buttons in the Backup Job wizard.
- **Up** and **Down** — to switch between items in a scrollable list.
- **Space** — to select the necessary item in a list. The selected item's mark may vary in different steps of the wizard.
- **Enter** — to proceed to the next step of a wizard or to view details of the backup job session selected in the list of sessions.
- **Backspace** — to return to the previous step of a wizard (you cannot use this button to change wizard steps when a text field is selected).
- **Esc** — to exit the currently used wizard or close the Veeam Agent for Linux control panel.

---

Thank you for installing our product!

As the first step, you will need to configure a backup job. You can choose between backing up the entire computer, individual volumes or select files and directories only. In any case, we will create an image-level backup containing the selected data. Press [C] to create your first backup job now.

If you already have any type of backup created and want to perform a restore of individual files, press [R] now. To restore the entire computer or an individual volume, you will need to boot from Veeam Recovery Media first.

Need help? Check out Veeam Agent for Linux forum at https://forums.veeam.com
Command Line Interface

Veeam Agent command line interface is a powerful tool that lets users perform advanced operations that are not supported by the Veeam Agent control panel.

To work with Veeam Agent using command line interface, you can use a terminal console (TTY) or a terminal emulator of your choice. All tasks in Veeam Agent are performed with the `veeamconfig` command-line utility. To perform tasks with Veeam Agent, you should construct the necessary command and type it in the Linux shell prompt.

You can view short help information on every Veeam Agent command at any time you need. To learn more, see Viewing Help.

You should construct a command in the following format:

```
veeamconfig <command_1> <command_2> --<parameter_1> --<parameter_2> --<parameter_n>
```

where:

- `<command_1>` — command that defines a type of an object with which you want to perform a task. Currently, the following commands are available in Veeam Agent:
  - aap
  - agreement
  - backup
  - cloud
  - config
  - downloadiso
  - grablogs
  - help
  - job
  - license
  - mode
  - patchiso
  - point
  - repository
  - schedule
  - session
  - ui
  - version
  - vbrserver
• `<command_2>` — command that defines a task that you want to perform with an object of the specified type. For example, you can perform the following commands with backup repositories:
  o create
  o delete
  o edit
  o help
  o list
  o rescan

• `<parameter_1>, <parameter_2>, <parameter_n>` — parameters for the command that you want to execute. Commands may require one or several mandatory or optional parameters. Some commands, for example, `veeamconfig ui` and `veeamconfig [<command>] help` do not require parameters.

The following example shows the command that displays a list of backup repositories configured in Veeam Agent and the output of this command:

```
user@srv01:$ veeamconfig repository list
Name          ID                                      Location            Typ
Backup server Repository_1  {818e3a0f-8155-4a51-9430-248a203a43d1}  /home/backups       local
Repository_2  {2155a2e7-a1e9-4347-9d8b-cf8f3a6f3fc8}  172.17.53.47/veeam  cifs
```
Viewing Help

You can view short help information on the specific Veeam Agent command. To view help, use the following command:

```
veeamconfig <command> help
```

where:

<command> — name of the command for which you want to view help information.

For example:

```
user@srv01:~$ veeamconfig help
```

or

```
user@srv01:~$ veeamconfig job help
```

or

```
user@srv01:~$ veeamconfig job create help
```

You can also view the manual page for the `veeamconfig` utility. Use the following command:

```
man veeamconfig
```
Licensing

To work with Veeam Agent, you must accept terms of the product license agreement and license agreements for third-party components operating as part of the product.

If you want to use a commercial version of Veeam Agent, you must obtain a license and install it on the protected computer. If you do not install a license, the product will operate in the Free edition.

You can use the Veeam Agent control panel or Veeam Agent command line interface to install a license, monitor status of the installed license or remove the license if necessary.
Product Editions

Veeam Agent for Linux offers three product editions that define product functionality and operation modes:

- **Server** — a commercial edition that provides access to all product functions and is intended for performing data protection tasks on servers that run Linux OS. Veeam Agent for Linux can operate in the server edition if a commercial license that supports this edition is installed on the protected computer.

- **Workstation** — a commercial edition that offers limited capabilities that are sufficient for performing data protection tasks on desktop computers and laptops that run Linux OS. Veeam Agent for Linux can operate in the workstation edition if a commercial license that supports this edition is installed on the protected computer.

- **Free** — a free edition that offers the same capabilities as the Workstation edition but does not come with a commercial support program. In contrast to the workstation and server editions, the Free edition does not require a license.

For more information about product editions, pricing and features available for them, see this Veeam webpage.

**TIP**

To check in which edition Veeam Agent for Linux currently operates, you can use the Veeam Agent for Linux control panel or command line interface. To learn more, see Viewing License Information.

When you install a license on the protected computer, you can select in which edition Veeam Agent for Linux will operate: server edition or workstation edition (if both editions are supported by the license). If you use Veeam Agent for Linux with Veeam Backup & Replication, you must manage product licenses and editions from the Veeam Backup & Replication console. To learn more, see Managing License with Veeam Backup & Replication.

After the license expires, Veeam Agent for Linux automatically switches to the Free edition. To learn more, see License Expiration.
Limitations for Free and Workstation Editions

Compared to the Server edition of Veeam Agent for Linux, Free and Workstation editions have the following limitations:

1. [For Free edition] The number of backup jobs that you can configure in Veeam Agent for Linux is limited to one.
2. [For Free edition] You cannot use a Veeam Cloud Connect repository as a target location for backup files.
3. [For Workstation edition] The number of backup jobs that you can configure in Veeam Agent for Linux is limited to one backup job targeted at a local drive, network shared folder or Veeam backup repository plus unlimited number of backup jobs targeted at a Veeam Cloud Connect repository.
4. You cannot specify pre-freeze and post-thaw scripts in the backup job settings.
5. You cannot specify database system processing settings.
License Agreement

After you install Veeam Agent for Linux, you must accept terms of the product license agreement and license agreements for third-party components operating as part of the product. Until you accept the license agreements, you will not be able to perform backup and data recovery tasks with the Veeam Agent for Linux control panel and command line interface.

License agreements are located in the /usr/share/doc/veeam directory of the machine where you installed the product.

The process of accepting license agreements differs depending on the way you work with Veeam Agent for Linux — using the control panel or command line interface.

- When you launch the Veeam Agent for Linux control panel for the first time, Veeam Agent prompts you to accept the license agreements at the Agreements step of the initial setup wizard. To learn more, see Accept License Agreements.

- When you run a Veeam Agent for Linux command, for example, veeamconfig repository create, Veeam Agent prompts you to accept license agreements. To accept the license agreement, type y or yes in the command prompt and press Enter.

Alternatively, you can accept license agreements using the dedicated commands. To learn more, see Accepting License Agreements.
Installing License

When you launch the Veeam Agent for Linux control panel for the first time, Veeam Agent for Linux offers you to install a license at the License step of the initial setup wizard. You can choose to install the license immediately or postpone this operation.

If you choose to postpone the license installation process, you can install a license later at any time you need. Until you install a license, Veeam Agent for Linux will operate in the Free edition. To learn more, see Product Editions.

**NOTE**

If you choose not to install a license and use Veeam Agent for Linux in the Free edition, Veeam Agent for Linux will display a notification offering to install a license every time you open the control panel. The notification will appear in the control panel until Veeam Agent for Linux completes the first backup job session.

To install a license:

1. Launch the Veeam Agent for Linux control panel with the `veeam` or `veeamconfig ui` command.
2. In the Veeam Agent for Linux control panel, press the 'm' key to open the Miscellaneous menu.
3. In the menu, make sure that the Manage License option is selected and press Enter.
4. In the Manage license window, make sure that the Install button is selected and press Enter.
5. In the **Choose license** window, in the **File location** field, specify a path to the license key:
   a. Select the **Browse** option with the **Tab** key and press **Space** or **Enter**.
   b. In the **Choose license file location** window, select the necessary directory and press **Enter**.
   c. Repeat the step 'b' until a path to the directory in which the license key resides appears in the **Current directory** field.

**TIP**
If you chose to install the license immediately from the Veeam Agent for Linux welcome screen notification, you will pass to the **Choose license** step right from the notification window.

6. In the **Choose agent edition to use on this computer** section, select the product edition in which Veeam Agent for Linux will operate and press **Enter**. To learn more about editions, see **Product Editions**.

7. Veeam Agent for Linux will install the license and display a window notifying that the license is successfully installed. Press **Enter** to finish the license installation process.

**TIP**
After you install a license, you can view information about the license (expiration date, status of the license, current edition of the product and so on) in the **Manage license** window. You can also check information about the license using the Veeam Agent for Linux command line interface. To learn more, see **Viewing License**.
Viewing License Information

To view information about the installed license, do the following:

1. Launch the Veeam Agent for Linux control panel with the `veeam` or `veeamconfig ui` command.
2. In the Veeam Agent for Linux control panel, press the ‘m’ key to open the Miscellaneous menu.
3. In the menu, make sure that the Manage License option is selected and press Enter.

Veeam Agent for Linux will display information about the license.

```
Support expiration: 2020/10/10 (204 days left)
Issued to: Veeam Software GmbH
E-mail: root@veeam.com
Status: License is valid
Mode: Server
License source: Local license
```

[Install] [Remove] [Close]
Removing License

You can remove the license if necessary. To remove a license:

1. Launch the Veeam Agent for Linux control panel with the `veeam` or `veeamconfig ui` command.
2. In the Veeam Agent for Linux control panel, press the 'm' key to open the Miscellaneous menu.
3. In the menu, make sure that the Manage License option is selected and press Enter.
4. In the Manage license window, press Tab to select the Remove button, then press Enter.
5. Veeam Agent for Linux will remove the license and display a window notifying that the license is successfully removed. Press Enter to finish the license removal process.

**NOTE**

After you remove the license, Veeam Agent for Linux will continue to operate in the Free edition. Consider the following:

- If Veeam Agent for Linux operated in the Server edition and multiple backup jobs were configured, after switching to the Free edition, all backup jobs will fail.
- If prefreeze and/or post-thaw scripts were specified for a backup job, after switching to the Free edition, this backup job will fail.
- If database system processing was set for a backup job, after switching to the Free edition, this backup job will fail.
License Expiration

30 days before the license expiration date, Veeam Agent for Linux will display a warning at the top of the control panel. After the license expires, Veeam Agent for Linux will switch to the Free edition.

Consider the following:

- If Veeam Agent for Linux operated in the Server edition and multiple backup jobs were configured, after switching to the Free edition, all backup jobs will be failing.
- If pre-freeze and/or post-thaw scripts were specified for a backup job, after switching to the Free edition, this backup job will be failing.
- If database system processing was set for a backup job, after switching to the Free edition, this backup job will be failing.

You can switch to the Free edition manually at any time if necessary. To learn more, see Removing License.

<table>
<thead>
<tr>
<th>Job name</th>
<th>State</th>
<th>Started at</th>
<th>Finished at</th>
</tr>
</thead>
<tbody>
<tr>
<td>SystemBackup</td>
<td>Success</td>
<td>2016-12-07 15:00:15</td>
<td>2016-12-07 15:00:15</td>
</tr>
<tr>
<td>DocumentsBackup</td>
<td>Success</td>
<td>2016-12-07 15:00:10</td>
<td>2016-12-07 15:00:10</td>
</tr>
<tr>
<td>DocumentsBackup</td>
<td>Success</td>
<td>2016-12-07 15:00:09</td>
<td>2016-12-07 15:00:09</td>
</tr>
<tr>
<td>SystemBackup</td>
<td>Success</td>
<td>2016-12-07 15:00:14</td>
<td>2016-12-07 15:00:14</td>
</tr>
</tbody>
</table>
Managing License with Command Line Interface

You can use the Veeam Agent for Linux command line interface to perform the following operations with the license:

- Accept license agreements for the product itself and its third-party components.
- Install a license on the protected computer.
- View information about the license.
- Remove the license.
Accepting License Agreements

To work with Veeam Agent for Linux, you must accept terms of the product license agreement and license agreements for third-party components operating as part of the product. Until you accept license agreements, you can use the `veeamconfig` utility to run the following commands only:

- `veeamconfig agreement show`
- `veeamconfig help` (or `veeamconfig -h` or `veeamconfig --help`)
- `veeamconfig mode info`
- `veeamconfig mode reset`
- `veeamconfig version` (or `veeamconfig -v` or `veeamconfig --version`)
- `veeamconfig ui`

To accept license agreements, use the following command:

```
veeamconfig agreement accepteula && veeamconfig agreement acceptthirdpartylicenses
```

**TIP**

To check whether license agreements are accepted, use the following command: `veeamconfig agreement show`. 
Installing License

To install a license, use the following command:

```
veeamconfig license install --path <path> --workstation
```

or

```
veeamconfig license install --path <path> --server
```

where:

- `<path>` — path to the license key file in the local file system of your computer.
- `workstation` or `server` — edition in which Veeam Agent will operate. To learn more about editions, see Product Editions.

Veeam Agent for Linux will install the license and display information about the license. You can also view this information later at any time. To learn more, see Viewing License Information.

For example:

```
user@srv01:~$ veeamconfig license install --path /home/user/veeam/license/veeam.lic --server
License was installed successfully.
License information:
  License source: Local license
  Mode: Server
  Support expiration: 2019/09/20 (649 days left)
  Status: License is valid.
  Issued to: TechCompany
  E-mail: administrators@tech.com
```

**TIP**

You can also install a license using the Veeam Agent control panel. To learn more, see Installing License.
Viewing License Information

You can view information about the installed license. Use the following command:

```
veeamconfig license show
```

Veeam Agent for Linux will display information about the license. For example:

```
user@srv01:~$ veeamconfig license show
License information:
  License source: Local license
  Mode: Server
  Support expiration: 2019/09/20 (649 days left)
  Status: License is valid.
  Issued to: TechCompany
  E-mail: administrators@tech.com
```
Removing License

You can remove a license with the following command:

```
veeamconfig license remove
```

After you remove the license, Veeam Agent for Linux will continue to operate in the Free edition. Consider the following:

- If Veeam Agent operated in the Server edition and multiple backup jobs were configured, after switching to the Free edition, all backup jobs will be failing.
- If pre-freeze and/or post-thaw scripts were specified for a backup job, after switching to the Free edition, this backup job will be failing.
- If database system processing was set for a backup job, after switching to the Free edition, this backup job will be failing.
Performing Backup

You can back up your data to protect the entire computer image, individual volumes or folders and files on your computer. To back up your data, you must configure a backup job. Depending on the product edition, Veeam Agent lets you configure one or several backup jobs targeted at the same or different backup repositories.

You can configure a backup job that will automatically back up your data by the defined schedule. You can also start a backup job manually at any time.
Creating Custom Veeam Recovery Media

In addition to the generic Veeam Recovery Media that is available for download at the Veeam website, you can create a custom Veeam Recovery Media. This option may be helpful if your computer uses hardware that requires drivers not included in the generic Veeam Recovery Media. When you create a custom Veeam Recovery Media, Veeam Agent copies the Linux kernel running on your computer with its currently loaded modules and includes them into the custom recovery image.

Keep in mind the following:

- The custom recovery image comprises an unsigned Linux kernel. As a result, you cannot use it for UEFI systems with enabled Secure Boot.
- If you plan to use live patching to create a custom recovery image, consider the limitations.

You can create a custom Veeam Recovery Media in one of the following ways:

- With the Veeam Agent control panel. You can perform this operation in the following conditions:
  - At the process of initial product setup, at the Recovery ISO step of the initial setup wizard.
  - At any time you need, in the Miscellaneous menu. For details, see Creating Custom Veeam Recovery Media with Control Panel.
- With the Veeam Agent command line interface. For details, see Creating Custom Veeam Recovery Media with Command Line Interface.
  
  If you create a custom Veeam Recovery Media using the command line interface, you can also specify a directory that contains additional drivers that you want to include in the recovery media.

Before you create custom Veeam Recovery Media, check the following prerequisites:

- The Linux system must have the genisoimage package installed. For openSUSE and SLES 15 SPO – SP3 distributions, the Linux system must have the mkisofs package installed.
- The Linux system must have the mksquashfs and unsquashfs utilities installed.
- For custom Veeam Recovery Media with EFI support, the Linux system must have the following packages installed:
  - xorriso
  - isolinux (or syslinux, if the software package repository of your Linux distribution lacks the isolinux package)
Creating Custom Veeam Recovery Media with Control Panel

To create custom Veeam Recovery Media with the Veeam control panel, do the following:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command.
2. In the Veeam Agent control panel, press the 'm' key to open the Miscellaneous menu.
3. In the menu, select the Patch Recovery Media option and press Enter.

4. Press Tab and select how you want to create a custom Veeam Recovery Media depending on the location of the generic recovery media ISO file:
   - If you have not downloaded the generic Veeam Recovery Media from the Veeam website, make sure that the Download and patch ISO option is selected and press Tab. If you select this option, Veeam Agent will download the ISO file of the generic Veeam Recovery Media from the Veeam software repository to the directory of your choice on the Veeam Agent computer and use this image to create the custom Veeam Recovery Media.

Veeam Agent downloads the Veeam Recovery Media ISO file depending on the Veeam Agent computer architecture. For details, see Veeam Recovery Media ISO Files.
If you want only to download the generic Veeam Recovery Media from the Veeam website, select the **Only download ISO** option with the **Down** key and press **Tab**. If you select this option, Veeam Agent will download the ISO file of the generic Veeam Recovery Media from the Veeam software repository to the directory of your choice on the Veeam Agent computer. You can use the downloaded ISO file later to boot your Veeam Agent computer or to create a custom Veeam Recovery Media.

Veeam Agent downloads the Veeam Recovery Media ISO file depending on the Veeam Agent computer architecture. For details, see [Veeam Recovery Media ISO Files](#).

If you have already downloaded the generic Veeam Recovery Media to a local directory on the Veeam Agent computer or to a network shared folder, select the **Patch local ISO** option with the **Down** key and press **Tab**. If you select this option, Veeam Agent will use the generic Veeam Recovery Media ISO file to create the custom Veeam Recovery Media.

The name of the generic Veeam Recovery Media ISO file depends on the recovery image version, Veeam Agent computer architecture and the source from which you downloaded the ISO file: from the product download page or Veeam software repository. To learn more, see [Veeam Recovery Media Versions](#).

5. If you selected the **Download and patch ISO** or **Patch local ISO** option, the **EFI system** option is available. If you want to boot the Veeam Recovery Media on EFI-based systems, select the **EFI system** option with the **Tab** key and press **Space**.

   If you do not enable this option, the custom Veeam Recovery Media will be able to boot on BIOS-based systems only.

6. If you selected the **Patch local ISO** option, in the **Path to local ISO** field, specify a path to the ISO file of the generic Veeam Recovery Media:
   a. Select the **Browse** option with the **Tab** key and press **Enter**.
   b. In the **Path to ISO** window, select the necessary directory and press **Enter**.
   c. Repeat the step ‘b’ until a path to the directory in which the recovery media ISO file resides appears in the **Current directory** field.
   d. In the directory where the recovery media ISO file resides, select the ISO file and press **Enter**.

7. Specify a path to the resulting ISO file of the Veeam Recovery Media.

   If you selected the **Download and patch ISO** or **Patch local ISO** option, in the **Save patched ISO** to field, you can specify a path to the resulting ISO file of the custom Veeam Recovery Media; if you selected the **Only download ISO** option, in the **Save ISO to** field, specify a path to the resulting ISO file of the generic Veeam Recovery Media:
   a. Select the **Browse** option with the **Tab** key and press **Enter**.
   b. In the **Save patched ISO to** window, select the necessary directory and press **Enter**.
   c. Repeat the step ‘b’ until a path to the directory where you want to save the resulting custom recovery media ISO file appears in the **Current directory** field.
   d. Select the **OK** button with the **Tab** key and press **Enter**.
8. To start the custom recovery media creation process, select the **Next** button with the **Tab** key and press Enter.

![Custom Recovery Media window](image)

Add drivers from this machine into Veeam Recovery ISO, it might be required for a successful bare-metal restore:
- ( ) Download and patch ISO
- ( ) Only download ISO
- (X) Patch local ISO

[ ] EFI system

Path to local ISO: **recovery-media.iso** [Browse]

Save patched ISO to: **/home/user01/veeam** [Browse]

[OK] [Close]
Creating Custom Veeam Recovery Media with Command Line Interface

To create a custom Veeam Recovery Media, you need to perform the following operations:

- Download the ISO file of the generic Veeam Recovery Media. You can download this file from the Veeam software repository.
- Using the downloaded ISO file, create the Custom Veeam Recovery Media.
Downloading Generic Recovery Media

To download the generic Veeam Recovery Media with the command line interface, use the following command:

```
veeamconfig downloadiso --output <output_path>
```

where:

`<output_path>` — path to the downloaded ISO file of the generic Veeam Recovery Media.

Veeam Agent downloads the ISO file of the generic Veeam Recovery Media depending on the Veeam Agent computer architecture. For details, see Veeam Recovery Media ISO Files.

For example:

```
$ veeamconfig downloadiso --output /mnt/veeam/iso
```
Creating Custom Recovery Media

To create custom Veeam Recovery Media with the command line interface, use the following command:

```
veeamconfig patchiso --input <input_path> --output <output_path> --copy <additional_path>
```

or

```
veeamconfig patchiso --efi --input <input_path> --output <output_path> --copy <additional_path>
```

where:
- `<input_path>` — path to the ISO file of the generic Veeam Recovery Media.
- `<output_path>` — path to the resulting ISO file of the custom Veeam Recovery Media.
- `<additional_path>` — path to a directory with additional drivers that you want to include in the Veeam Recovery Media.

When you boot from the custom Veeam Recovery Media, the content of the directory specified with the `<additional_path>` parameter will be available in the root folder of the recovery environment.

- `--efi` — option that defines whether custom Veeam Recovery Media should be able to boot on EFI-based systems. Without this option, the custom Veeam Recovery Media will be able to boot on BIOS-based systems only.

For example:

```
$ veeamconfig patchiso --input /mnt/veeam/iso/veeam-recovery-amd64-5.0.0.iso --output /mnt/veeam/iso/veeam-recovery-media-srv01.iso --copy /tmp/template --efi
```
Veeam Recovery Media ISO Files

To create a custom Veeam Recovery Media, you need the ISO file of the generic Veeam Recovery Media from the Veeam software repository. Veeam Agent uses this image to create the custom Veeam Recovery Media.

Veeam Agent for Linux automatically downloads one of the following Veeam Recovery Media ISO files depending on the Veeam Agent computer architecture:

- **veeam-recovery-i386-5.0.0.iso** — for x86 computers that run Linux kernel version 3.10 and later. The size of the downloaded ISO file is about 450 MB.

- **veeam-recovery-amd64-5.0.0.iso** — for x64 computers that run Linux kernel version 3.10 and later. The size of the downloaded ISO file is about 500 MB.

- **veeam-recovery-media-5.0.0.iso** — for x86 and x64 computers that run Linux kernel version earlier than 3.10. The size of the downloaded ISO file is about 150 MB.
Creating Backup Jobs

You can choose one of the following backup modes:

- Backup of an entire computer image
- Backup of specific computer volumes, for example, a system volume or secondary volume
- Backup of individual files and folders

[For Server Edition] You can configure one or several backup jobs to back up your data. Configuring several backup jobs may be useful in the following situations:

- You can configure separate backup jobs for volume-level backup and file-level backup.
- You can configure backup jobs targeted at different backup repositories to keep several copies of your backed-up data at different locations.
- You can configure several backup jobs and define individual schedule for every job to back up necessary data at the desired time.

With Veeam Agent, you can configure the backup job in one of the following ways:

- With the Backup Job wizard
- With the command line interface
Creating Backup Job with Backup Job Wizard

You can configure volume-level and file-level backup jobs with the Backup Job wizard.
Before You Begin

Before you configure the backup job, check the following prerequisites:

- The target location where you plan to store backup files must have enough free space.
- When you configure the backup job with the Backup Job wizard, Veeam Agent creates the job with default advanced settings: compression level and data block size. To specify these parameters explicitly, you should create a backup job with the command line interface.
- [For Veeam Backup & Replication repository targets] You can store created backups in a backup repository only if the backup server runs Veeam Backup & Replication 11 or later.
- [For Veeam Backup & Replication repository targets] If you plan to use a Veeam Backup & Replication repository as a target for backups, you must pre-configure user access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.

Backup has the following limitations:

- You cannot save the backup of entire computer on the local computer disk. Use an external hard drive or USB drive, network shared folder or backup repository as a target location.
- Veeam Agent does not back up data to which symbolic links are targeted. It only backs up the path information that the symbolic links contain. After restore, identical symbolic links are created in the restore destination.
- Keep in mind that Veeam Agent stops running the backup job after 21 days (504 hours).
Navigating Backup Job Wizard

The Backup Job wizard window comprises the following areas:

- The navigation pane, located on the left of the window, displays the list of wizard steps and currently selected step of the wizard.
- The working area displays controls relating to a specific step of the wizard.
- The buttons area, located at the bottom of the window, displays buttons that you can use to switch between steps of the wizard (Previous and Next) and close the wizard (Cancel and Finish).

In the Backup Job wizard, the use of a mouse is not supported. To navigate the Backup Job wizard and associated dialog windows, you can use the following keys:

- **Tab** — to switch between displayed controls in the working area and buttons in the buttons area. The currently selected control or button is highlighted with a green color.
- **Up** and **Down** — to switch between items in a scrollable list.
- **Space** — to select the necessary item in a list. The selected item's mark may vary in different steps of the wizard.
- **Enter** — to proceed to the next step of the wizard or to open a directory.
- **Backspace** — to return to the previous step of a wizard.
- **Escape** — to cancel the backup job configuration and exit the wizard.

**TIP**

You can switch between steps of the Backup Job wizard in two ways. The easier and more comfortable way is to use the **Enter** key to proceed to the next step and **Backspace** key to return to the previous step of the wizard. You can also use the **Tab** key to select the **Next** or **Previous** button in the buttons area and then press **Enter** to switch to the next or previous step of the wizard respectively.
Step 1. Launch Backup Job Wizard

To launch the Backup Job wizard, do the following:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command:

2. If you have not configured any backup jobs yet, Veeam Agent will display a welcome screen. Press the 'c' key to proceed to the Backup Job wizard and configure the backup job.

3. If you have already configured and performed a backup job, Veeam Agent will display the list of backup job sessions. When you press 'c' to launch the Backup Job wizard, Veeam Agent will display a list of configured backup jobs. To configure a new backup job, select the Configure new job option and press Enter.

**NOTE**

The Configure new job option is not available if Veeam Agent for Linux operates in the Free edition and you have already configured one backup job.

To edit settings of a backup job that you have already configured, select the job in the list and press Enter. To learn more, see Editing Backup Job Settings.

If you have decided not to create a backup job, press Escape to close the list of backup jobs and return to the welcome screen. After that, you can press Escape once again to return to the command line interface.
Step 2. Specify Backup Job Name

At the **Name** step of the wizard, in the **Job name** field, type the name for the backup job and press **Enter**.

**TIP**
To proceed to the next step of the wizard, you can also select the **Next** button with the **Tab** key and then press **Enter**.
Step 3. Select Backup Mode

At the **Backup mode** step of the wizard, select the mode in which you want to create a backup:

1. Select the necessary backup mode. You can select one of the following options:
   - **Entire machine** — select this option if you want to create a backup of the entire computer image. When you restore data from such backup, you will be able to recover the entire computer image as well as data on specific computer volumes: files, folders, application data and so on. With this option selected, you will pass to the **Destination** step of the wizard.
   - **Volume level backup** — select this option if you want to create a backup of specific computer volumes, for example, the system volume. When you restore data from such backup, you will be able to recover data on these volumes only: files, folders, application data and so on. With this option selected, you will pass to the **Volumes** step of the wizard.
   - **File level backup** — select this option if you want to create a backup of individual directories on your computer. With this option selected, you will pass to the **Files** step of the wizard.

2. [For file-level backup] If you want to perform backup in the snapshot-less mode, select **Disable snapshot**. With this option selected, Veeam Agent will not create a snapshot of the backed-up volumes during backup. This allows Veeam Agent to back up data residing in file systems that are not supported for snapshot-based backup with Veeam Agent. To learn more, see [Snapshot-Less File-Level Backup](#).

**IMPORTANT**

Consider the following:

- [For entire machine backup] Certain limitations for Dell PowerPath configuration apply. To learn more, see this Veeam KB article.
- [For volume-level backup] Volume-level backup job relies on a device name in the `/dev` directory. Device names in the `/dev` directory (e.g. `/dev/md-127`, `/dev/dm-1`) must stay persistent for backed-up volumes. Otherwise, the job will back up the wrong volume.
- [For file-level backup] If the backed-up file system has a complex directory structure with many hierarchy levels, during incremental backup, the inbound network traffic on the Veeam Agent computer may exceed by far the outbound traffic. Significant amount of data can be transferred to the Veeam Agent computer from the target backup location even if few files are changed since the previous job session.

**TIP**

File-level backup is typically slower than volume-level backup. If you plan to back up all directories with files on a specific volume, it is recommended that you configure volume-level backup instead of file-level backup.
### Choose what data you want to back up from this computer

<table>
<thead>
<tr>
<th>Name</th>
<th>Backup mode</th>
<th>Destination</th>
<th>Location</th>
<th>Advanced</th>
<th>Schedule</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( ) Entire machine (recommended)</td>
<td>Back up the entire host for fast recovery on any level.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>( ) Volume level backup</td>
<td>Back up images of selected partitions and volumes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(X) File level backup</td>
<td>Back up individual files and folders.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(X) Disable snapshot</td>
<td>Crash-consistent file-level backup without snapshot.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Prev] [Next] [Cancel]
Step 4. Specify Backup Scope Settings

Specify backup scope for the backup job:

- **Select volumes to back up** — if you have selected the *Volume level backup* option at the *Backup Mode* step of the wizard.

- **Select files and directories to back up** — if you have selected the *File level backup* option at the *Backup Mode* step of the wizard.
Selecting Volumes to Back Up

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

At this step of the wizard, you must specify the backup scope — define what volumes you want to include in the backup. Veeam Agent lets you include the following types of objects in the volume-level backup:

- Block devices (entire disks and individual volumes)
- Mount points
- LVM logical volumes and volume groups
- Btrfs storage pools and subvolumes
Selecting Devices

To add a block device to the backup scope, do the following:

1. At the Volume step of the wizard, make sure that the Device option is selected and press Enter.

2. In the Add devices to scope window, select individual volumes or entire computer disks that you want to include in the backup and press Enter.
   
   - To include individual volumes of your computer in the backup, select block devices that represent volumes that you want to back up, for example: sda1 and/or sda6.
   
   - To include all volumes on a computer disk in the backup, select block devices that represent disks whose volumes you want to back up, for example: sda and/or sdb. All volumes on the selected disk will be automatically selected, too.

To navigate the list of volumes and select the necessary items, use Up, Down and Space keys. To learn more, see Navigating Backup Job Wizard.

If you have created several system partitions, for example, a separate partition for the /boot directory, you should remember to include all of these partitions in the backup. Otherwise, Veeam Agent does not guarantee that the OS will boot properly when you attempt to recover from such backup.

NOTE

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

To add a mount point to the backup scope, do the following:

1. At the Volume step of the wizard, select the Mountpoint option and press Enter.

2. In the Add mountpoints to scope window, select mount points that you want to include in the backup and press Enter.

To navigate the list of mount points and select the necessary mount points, use Up, Down and Space keys. To learn more, see Navigating Backup Job Wizard.
Selecting LVM Volumes

To add an LVM logical volume or volume group to the backup scope, do the following:

1. At the Volume step of the wizard, select the LVM option and press Enter.

2. In the Add LVM to scope window, select LVM logical volumes or volume groups that you want to include in the backup and press Enter.

   To navigate the list of LVM volumes and select the necessary items, use Up, Down and Space keys. To learn more, see Navigating Backup Job Wizard.

   If you include an LVM volume group in the backup, all LVM logical volumes in the selected volume group will be automatically selected, too.

NOTE

Veeam Agent does not back up LVM snapshots.
Selecting Btrfs Volumes

To add a Btrfs storage pool or subvolume to the backup scope, do the following:

1. At the **Volume** step of the wizard, select the **BTRFS** option and press **Enter**.
2. In the **Add BTRFS to scope** window, select Btrfs storage pools or subvolumes that you want to include in the backup and press **Enter**.

   To navigate the list of Btrfs pools and subvolumes and select the necessary items, use **Up**, **Down** and **Space** keys. To learn more, see *Navigating Backup Job Wizard*.

**NOTE**

Consider the following:

- Veeam Agent identifies Btrfs storage pools by UUIDs specified in the fstab configuration file. Other identifiers are not supported.
- If you include a Btrfs storage pool in the backup, all Btrfs subvolumes in the selected pool will be automatically selected, too.
- You cannot add read-only Btrfs snapshots to the backup scope.
Selecting Files and Directories to Back Up

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

At this step of the wizard, you must specify the backup scope — define what directories with files you want to include in the backup.

In the file-level backup mode, you must include in the backup at least one directory. If you do not want to back up some subdirectories of the specified directory, you can exclude these directories from the backup.

You can also include or exclude files of a specific type in/from the backup. You can specify file names explicitly or use UNIX wildcard characters to define file name masks. Veeam Agent will apply the specified file name masks to files in directories that are included in the backup.

To specify the backup scope:

1. At the **Files** step of the wizard, make sure that the Add directories option is selected and press **Enter**.
2. In the Choose directories window, select one or several directories that you want to include in the file-level backup.
   - To navigate the list of directories, use the **Up** and **Down** keys.
   - To browse for subdirectories, navigate to the necessary directory and press **Enter**.
   - To include a directory in the backup, navigate to the necessary directory and press **Space**. The included directory will be marked with the ‘+’ character. All subdirectories of the selected directory will be included in the backup too.
3. Specify directories that you want to exclude from the file-level backup. To exclude a directory:
   a. Browse for subdirectories of a directory that you have included in the backup.
   b. Navigate to the directory that you want to exclude from the backup and press Space. The excluded directory will not be marked with the '+' character.

4. Switch to the OK button and press Enter. Veeam Agent will display a list of paths to the selected directories and the number of excluded subdirectories for each directory in the list.

5. Specify file name masks for files that you want to include or exclude in/from the backup:
   a. Select the File Masks option with the Tab key and press Enter.
   b. In the File masks window, make sure that the Create Mask button is selected and press Enter.
   c. In the Mask field, enter the file name mask, for example, report.pdf, *filename* or *.odt.
      Keep in mind that you must specify all names with masks in double quotation marks ("").
d. In the **Type** field, select one of the following options:

- **Exclude** — if you do not want to back up files whose names match the specified mask. Veeam Agent will back up all files in the directories selected for backup except for such files.

- **Include** — if you want to back up files whose names match the specified mask. Veeam Agent will create a backup only for such files in the directories selected for backup.

You can use a combination of include and exclude masks. Keep in mind that exclude masks have a higher priority than include masks. For example, you can specify masks in the following way:

- **Include mask**: `report.*`  
- **Exclude mask**: `*.odt`

Veeam Agent will include in the backup all files whose name begins with `report` except for the files of the ODT format.

![File masks window](image)

- **Press Enter**. Veeam Agent will display in the **File masks** window the specified file mask and its type: **Include** or **Exclude**.

- **Repeat steps 'b'–'e' for each mask that you want to specify.**

- **After you specify all file masks, switch to the **OK** button and press **Enter**.**
TIP

To remove a file name mask, in the **File masks** window, select the necessary mask and press **Delete**.
Step 5. Select Backup Destination

At the **Destination** step of the wizard, select a target location for the created backup.

You can select one of the following options:

- **Local** — select this option if you want to save the backup on a removable storage device attached to the computer or on a local computer drive. With this option selected, you will pass to the **Location** step of the wizard.

- **Shared Folder** — select this option if you want to save the backup in a network shared folder. With this option selected, you will pass to the **Network** step of the wizard.

- **Veeam Backup & Replication** — select this option if you want to save the backup on a backup repository managed by the Veeam backup server. With this option selected, you will pass to the **Veeam** step of the wizard.

- **Veeam Cloud Connect repository** — select this option if you want to create the backup on a cloud repository exposed to you by the Veeam Cloud Connect service provider. With this option selected, you will pass to the **Service Provider** step of the wizard.

It is recommended that you store backups in the external location like USB storage device or network shared folder. You can also keep your backup files on the separate non-system local drive.
Step 6. Specify Backup Storage Settings

Specify backup storage settings for the backup job:

- **Local storage settings** — if you have selected the Local storage option at the Destination step of the wizard.

- **Shared folder settings** — if you have selected the Shared folder option at the Destination step of the wizard.

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

- **Veeam Cloud Connect repository settings** — if you have selected the Veeam Cloud Connect repository option at the Destination step of the wizard.

**NOTE**

The Veeam Cloud Connect repository option is available if Veeam Agent operates in the Workstation or Server edition.
Local Storage Settings

The Location step of the wizard is available if you have selected the Local option at the Destination step of the wizard. Specify location for the backup file and retention policy for the backup job:

1. To specify location for the backup file, browse to the directory where backup files must be saved:
   a. Select the Browse option with the Tab key and press Space or Enter.
   b. In the Choose backup location window, select the necessary directory and press Enter.
   c. Repeat the step ‘b’ until a path to the directory in which you want to save backup files appears in the Current directory field.
   d. To create a new directory, switch to the Create Dir button, press Enter, then type a name for the new directory and press Enter.
   e. Switch to the OK button and press Enter. Veeam Agent will display the path to the specified directory in the Location field.

   Alternatively, you can type a path to the directory in which you want to save backup files in the Location field.

   After you specify location for the backup, Veeam Agent will display the following information on the volume where the directory selected for backup storage resides:
   - Space — total size of the volume on which the selected directory resides.
   - Free — free space on the volume where the selected directory resides.
   - Type — file system type of the volume on which the selected directory resides.

2. In the Restore points field, specify the number of backup files that you want to keep in the target location.
   By default, Veeam Agent keeps 7 latest backup files. When the number of restore points is exceeded, Veeam Agent for Linux will remove the earliest restore point from the backup chain.
IMPORTANT
Consider the following:

- The backup location must reside on a separate volume from a volume whose data you plan to back up.
- USB storage devices formatted as FAT32 do not allow storing files larger than 4 GB in size. For this reason, it is recommended that you do not use such USB storage devices as a backup target.
Shared Folder Settings

The **Network** step of the wizard is available if you have selected the **Shared Folder** option at the **Destination** step of the wizard.

To save backup files in a remote network location, Veeam Agent mounts to the local file system of your computer the network shared folder that you specify as a location for the backup. When you specify the network shared folder settings, Veeam Agent saves information about the network shared folder and its mount point in the database.

You do not need to mount the network shared folder in advance before every backup job run. Veeam Agent will do it automatically when the backup job is started manually or upon schedule.

After the backup job completes, Veeam Agent will automatically unmount the network shared folder.

Specify shared folder settings:

1. Select the type of a network shared folder:
   - **NFS** — to connect to a network shared folder using the NFS protocol.
   - **SMB** — to connect to a network shared folder using the SMB (CIFS) protocol.

2. In the **Path** field, specify the network shared folder name in the **SERVER/DIRECTORY** format: type an IP address or domain name of the server and the name of the network shared folder in which you want to store backup files.

   Every time the backup job starts, Veeam Agent will automatically mount the specified network shared folder to the `/tmp/veeam` directory in the computer file system. After the backup job completes, Veeam Agent will unmount the network shared folder.

3. [For SMB network shared folder] In the **Domain** field, type a name of the domain in which the account that has access permissions on the shared folder is registered, for example: **DOMAIN**.

4. [For SMB network shared folder] In the **Username** field, type a name of the account that has access permissions on the shared folder.

5. [For SMB network shared folder] In the **Password** field, type a password of the account that has access permissions on the shared folder.

6. In the **Restore points** field, specify the number of backup files that you want to keep in the target location. By default, Veeam Agent keeps 7 latest backup files. When the number of restore points is exceeded, Veeam Agent will remove the earliest restore point from the backup chain.
<table>
<thead>
<tr>
<th>Specify a network location to backup to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
</tr>
<tr>
<td>Backup mode:</td>
</tr>
<tr>
<td>Volumes:</td>
</tr>
<tr>
<td>Destination:</td>
</tr>
<tr>
<td>Network:</td>
</tr>
<tr>
<td>Advanced:</td>
</tr>
<tr>
<td>Schedule:</td>
</tr>
<tr>
<td>Summary:</td>
</tr>
<tr>
<td>( ) NFS</td>
</tr>
<tr>
<td>(X) SMB</td>
</tr>
<tr>
<td>Path: 172.17.53.57 / Veeam</td>
</tr>
<tr>
<td>Domain: tech</td>
</tr>
<tr>
<td>Username: Veeam</td>
</tr>
<tr>
<td>Password: * * * * * * *</td>
</tr>
<tr>
<td>Restore points: 7</td>
</tr>
</tbody>
</table>

[Prev] [Next] [Cancel]
Veeam Backup Repository Settings

If you have selected to store backup files on a Veeam Backup & Replication repository, specify settings to connect to the backup repository:

1. Specify backup server settings.
2. Select the Veeam backup repository.
Specifying Backup Server Settings

The Veeam step of the wizard is available if you have chosen to store backup files on a Veeam Backup & Replication repository.

Specify settings for the Veeam backup server that manages the target backup repository:

1. In the **Address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify a number of the port over which Veeam Agent must communicate with the backup repository. By default, Veeam Agent uses port 10006.
3. In the **Login** field, type a name of the account that has access to the Veeam backup repository.
4. In the **Domain** field, type a name of the domain in which the account that has access to the Veeam backup repository is registered, for example: `DOMAIN`.
5. In the **Password** field, type a password of the account that has access to the Veeam backup repository.

Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.

**IMPORTANT**

If you specify a DNS name of the Veeam backup server, make sure that the Veeam backup server name is resolved into IPv4 address on the machine where Veeam Agent is installed. The Veeam Backup Service in Veeam Backup & Replication listens on IPv4 addresses only. If the Veeam backup server name is resolved into IPv6 address, Veeam Agent will fail to connect to the Veeam backup server.
Selecting Backup Repository

The Repository step of the wizard is available if you have chosen to save backup files on a Veeam Backup & Replication repository.

Specify settings for the target backup repository:

1. From the list of available backup repositories, select a backup repository where you want to store backups. The list of backup repositories displays only those repositories on which you have permissions to store data. To learn more, see Setting Up User Permissions on Backup Repositories.

2. In the Restore points field, specify the number of restore points that you want to store in the target location. By default, Veeam Agent keeps 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

To learn more, see Backup Retention Policy.

![Selecting Backup Repository interface](image.png)
Veeam Cloud Connect Repository Settings

If you have selected to store backup files on a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

1. Specify service provider settings.
2. Verify the TLS certificate and specify user account settings.
3. Select the cloud repository.

NOTE

The Veeam Cloud Connect repository option is available if Veeam Agent operates in the Workstation or Server edition.
Specifying Service Provider Settings

The Provider step of the wizard is available if you have chosen to save backup files on a Veeam Cloud Connect repository.

Specify settings for the cloud gateway that the Veeam Cloud Connect service provider (SP) or your backup administrator has provided to you:

1. In the Address field, enter a full DNS name or IP address of the cloud gateway.
2. In the Port field, specify the port over which Veeam Agent will communicate with the cloud gateway. By default, port 6180 is used.

![Image showing the Provider step of the wizard with default settings: Address: 172.17.53.62, Port: 6180]
Specifying User Account Settings

The **Credentials** step of the wizard is available if you have chosen to save backup files on a cloud repository and specified settings for the cloud gateway.

Verify TLS certificate settings and specify settings for the tenant account or subtenant account that you want to use to connect to the cloud repository.

1. In the **Certificate details** window, review information about the TLS certificate obtained from the SP side and verify the TLS certificate:
   - [Optional] To verify the TLS certificate with a thumbprint, do the following:
     i. Select the **Verify thumbprint** button with the **Tab** key and press **Enter**.
     ii. Copy the thumbprint you obtained from the SP to the Clipboard and enter it to the **Thumbprint verification** field.
     iii. Switch to the **Verify** button and press **Enter**. Veeam Agent will check if the thumbprint you entered matches the thumbprint of the obtained TLS certificate.
   - TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.
   - To accept the TLS certificate, select the **Accept** button with the **Tab** key and press **Enter**.

2. In the **Username** field, enter the name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the **TENANT\SUBTENANT** format.

3. In the **Password** field, provide a password for the tenant or subtenant account.
Selecting Cloud Repository

The **Repository** step of the wizard is available if you have chosen to save backup files on a cloud repository and specified settings to connect to the SP.

Specify settings for the cloud repository:

1. From the **Repository** list, select a cloud repository where you want to store created backups. The **Repository** list displays only those cloud repositories that can be accessed by the tenant or subtenant account that you use to connect to the service provider.

2. In the **Restore points** field, specify the number of restore points that you want to store in the target location. By default, Veeam Agent keeps 7 latest restore points. After this number is exceeded, Veeam Agent will remove the earliest restore points from the backup chain.

To learn more, see **Backup Retention Policy**.

![Cloud backup repositories that the service provider has assigned to you.](image)
Step 7. Specify Advanced Backup Settings

At the Advanced step of the wizard, specify advanced settings for the backup job:

- Data encryption settings
- File indexing settings
- Oracle database system processing settings
- MySQL database system processing settings
- PostgreSQL database system processing settings
- Active full backup settings
- Backup maintenance settings
- Script settings
NOTE
Consider the following:

- You cannot specify encryption settings for the backup job if you have chosen to save backup files on a Veeam backup repository. Encryption options for Veeam Agent backup jobs targeted at the backup repository are managed by a backup administrator working with Veeam Backup & Replication. To learn more about data encryption capabilities available in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.
- You can specify file indexing settings only if Veeam Agent operates in the Workstation or Server edition.
- You can specify settings for Oracle, MySQL or PostgreSQL database system processing only if Veeam Agent operates in the Server edition. The settings are available for a volume-level backup job only.
- You can specify backup maintenance settings only if you have selected the Veeam backup repository or Veeam Cloud Connect repository option at the Destination step of the wizard.
- You cannot specify data compression settings when you configure a backup job with the Backup Job wizard. If you want to specify these settings, consider creating the backup job with the Veeam Agent command line interface. To learn more, see Advanced Backup Job Settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup encryption</td>
<td>Disabled</td>
</tr>
<tr>
<td>File system indexing</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oracle processing</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

DESCRIPTION:
Data encryption transforms data to an unreadable, scrambled format with the help of a cryptographic algorithm and a secret key. If encrypted data is intercepted, it cannot be unlocked and read by the eavesdropper.
Data Encryption Settings

If you want to encrypt the content of backup files, at the Advanced step of the wizard, specify data encryption settings for the backup job:

1. Select the Backup encryption option with the Tab key and press Enter.

**NOTE**

The Backup encryption option is unavailable if you have chosen to save backup files on a Veeam backup repository. Encryption options for Veeam Agent backup jobs targeted at the backup repository are managed by a backup administrator working with Veeam Backup & Replication. To learn more about data encryption capabilities available in Veeam Backup & Replication, see the Data Encryption section in the Veeam Backup & Replication User Guide.

2. In the Encryption window, make sure that the Enable backup file encryption option is selected and press Space.

3. In the Password field, type a password that you want to use for encryption.

4. In the Hint field, type a hint for the password. In case you lose the password, the specified hint will help you to remember the lost password.

5. Switch to the Ok button and press Enter.
File Indexing Settings

At the **Advanced** step of the wizard, specify file indexing settings for the backup job:

1. Select the **File system indexing** option with the **Tab** and **Down** keys and press **Enter**.

**NOTE**
The **File system indexing** option is available if Veeam Agent for Linux operates in the Workstation or Server edition.

2. In the **Indexing** window, specify the indexing scope:
   - **Select Index everything** if you want to index all files within the backup scope that you have specified at the **Backup mode** step of the wizard. Veeam Agent for Linux will index all files that reside:
     - On your computer OS (for entire machine backup)
     - On the volumes that you have selected for backup (for volume-level backup)
     - In the directories that you have selected for backup (for file-level backup)
   - **[For entire machine and volume-level backups]** Select **Index everything except** if you want to index all files within the specified backup scope except those files that reside in specific directories. Enter paths to directories whose files you do not want to index. To separate several paths, use the ',' (comma) character.
   - **[For entire machine and volume-level backups]** Select **Index only following directories** to define directories that you want to index. Enter paths to the necessary directories. To separate several paths, use the ',' (comma) character.

3. Switch to the **Ok** button and press **Enter**.
Oracle Database Processing Settings

At the Advanced step of the wizard, specify processing settings for the Oracle database system:

1. Select the Oracle processing option with the Tab and Down keys and press Enter.

2. In the Oracle processing section, select one of the following options:
   - Require successful processing. With this option selected, Veeam Agent will stop the backup process if an error occurs while processing the Oracle database system.
   - Try application processing, ignore failures. With this option selected, Veeam Agent will continue the backup process even if errors occur when processing the Oracle database system.

3. In the Archived logs processing section, specify how Veeam Agent will process archived logs on the Oracle database:
   - Select Do not delete archived logs if you want Veeam Agent to keep archived logs. When the backup job completes, Veeam Agent will not delete archived logs.
     It is recommended that you select this option when you do not have databases running in the ARCHIVELOG mode. If the database is running in the ARCHIVELOG mode, archived logs may grow large and consume all disk space. In this case, the database administrator must take care of archived logs themselves.
   - Select Delete logs older than <N> hours or Delete oldest logs exceeding <N> GB if you want Veeam Agent to delete archived logs that are older than <N> hours or larger than <N> GB. Veeam Agent will wait for the backup job to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session.
4. In the **Specify Oracle account with SYSDBA privileges** section, specify which account type Veeam Agent will use to connect to the database system.

   - **Select System account** if you want Veeam Agent to use an account of the Veeam Agent machine OS. The account must be a member of the group that owns configuration files for the Oracle database (for example, the oinstall group).

   - **Select Oracle account** if you want Veeam Agent to use an Oracle account. The account must have SYSDBA rights.
MySQL Database Processing Settings

IMPORTANT

To process the MySQL database system, the MySQL account must have the following privileges:

- SELECT for all tables. If the MySQL account does not have the SELECT privilege for the table, Veeam Agent cannot access table metadata. As a result, Veeam Agent does not process the table. To learn more, see MySQL documentation.
- LOCK TABLES. If the MySQL account does not have the LOCK TABLES privilege, Veeam Agent does not process tables based on the MyISAM storage engine.
- RELOAD. This privilege is required to allow the MySQL account to perform FLUSH operations.

To obtain information about privileges that are assigned to the account, use MySQL functionality, for example, the SHOW GRANTS statement. To learn more, see MySQL documentation.

At the Advanced step of the wizard, specify processing settings for the MySQL database system:

1. Select the MySQL processing option with the Tab and Down keys and press Enter.
2. In the MySQL processing section, select one of the following options:
   - Require successful processing. With this option selected, Veeam Agent will stop the backup process if an error occurs when processing the MySQL database system.
   - Try application processing, ignore failures. With this option selected, Veeam Agent will continue the backup process even if errors occur when processing the MySQL database system.
3. In the **Authentication method** section, specify how Veeam Agent will connect to the MySQL database:

- **Select Password** if you want Veeam Agent to connect with the MySQL account name and password. With this option selected, you must specify account name and password in the backup job settings.
Select **Password file** if you want Veeam Agent to connect with the MySQL account name and password that are stored in the `.my.cnf` password file. With this option selected, you must specify a path to the password file, but do not need to specify account credentials in the backup job settings. To learn more about password file configuration, see *Preparing Password File for MySQL Processing*. 
Preparing Password File for MySQL Processing

You can use MySQL account credentials that are stored in the password file to connect Veeam Agent for Linux to the MySQL database system.

**NOTE**

Consider the following:

- If you specify a custom path to the password file, specify a full path. Specifying relative paths is not supported.
- The password file can also contain user-specific connection settings that Veeam Agent will apply to connect to the MySQL database system. For example, if you want to connect to the MySQL database system using the custom socket, specify the socket path in the password file. To learn more, see MySQL documentation.

If you want to use a password file for authentication, create a file. By default, Veeam Agent expects the password file to have the `.my.cnf` name and to be in the home directory of the `root` user. If the password file has a custom name or is stored in another directory, you can specify a custom path.

The password file must have the following contents:

```plaintext
[client]
user=<username>
password=<password>
```

where:

- `<username>` — name of the account that Veeam Agent will use to connect to the MySQL database system.
- `<password>` — password of the account that Veeam Agent will use to connect to the MySQL database system.

For example:

```plaintext
[client]
user=root
password=P@ssw0rd
```
PostgreSQL Database Processing Settings

At the Advanced step of the wizard, specify processing settings for the PostgreSQL database system:

1. Select the PostgreSQL processing option with the Tab and Down keys and press Enter.

2. In the PostgreSQL processing section, select one of the following options:
   - **Require successful processing.** With this option selected, Veeam Agent will stop the backup process if an error occurs when processing the PostgreSQL database system.
   - **Try application processing, ignore failures.** With this option selected, Veeam Agent will continue the backup process even if errors occur when processing the PostgreSQL database system.

3. In the Authentication method section, specify how Veeam Agent for Linux will connect to the PostgreSQL database:
   - **Database user with password** if you want Veeam Agent to connect with the PostgreSQL account name and password. With this method selected, you must specify account name and password in the backup job settings.
   - **Database user with password file** if you want Veeam Agent to connect with the PostgreSQL account password that is stored in the .pgpass password file. With this method selected, you must specify account name only in the backup job settings. To learn more about password file configuration, see Password File for PostgreSQL.
   - **System user without password** if you want Veeam Agent to connect using a peer authentication method. In the peer authentication method, Veeam Agent uses the OS account as the PostgreSQL database user name. With this option selected, you must specify OS account in the backup job settings. To learn more about peer authentication, see PostgreSQL documentation.
Preparing Password File for PostgreSQL Processing

You can use PostgreSQL account credentials that are stored in the password file to connect Veeam Agent to the PostgreSQL database system.

If you want to use a password file for authentication, create the .pgpass file in the home directory of the root user.

The password file must have the following contents:

```
<hostname>:<port>:<database>:<username>:<password>
```

where:

- `<hostname>` — name of the host where the PostgreSQL database system is located.
- `<port>` — number of the free port that Veeam Agent will use to connect to the PostgreSQL database system.
- `<database>` — name of the PostgreSQL database.
- `<username>` — name of the account that Veeam Agent will use to connect to the PostgreSQL database system.
- `<password>` — password of the account that Veeam Agent will use to connect to the PostgreSQL database system.

For example:

```
srv01:5432:mydb:postgres:P@ssw0rd
```

For more information about the password file, see PostgreSQL documentation.
Active Full Backup Settings

At the Advanced step of the wizard, specify active full backup settings for the backup job:

1. Select the Active full option with the Tab and Down keys and press Enter.

2. In the Active full window, make sure that the Create active full backups periodically option is selected and press Space.

3. Specify schedule for periodic active full backups:
   - If you want active full backups to run monthly, select the Monthly on this day option and specify the day of a month when Veeam Agent will perform active full backup.
   - If you want active full backups to run weekly, do the following:
     i. Select the Weekly on selected days option, then select Days with the Tab key and press Enter.
     ii. In the Days window, specify days on which Veeam Agent will perform active full backup. By default, Veeam Agent performs active full backup every Saturday. To select days, use Up, Down, Right, Left and Space keys.
     iii. Switch to the Ok button with the Tab key and press Enter.
Maintenance Settings

At the **Advanced** step of the wizard, specify backup maintenance settings for the backup job:

1. Select the **Maintenance** option with the **Tab** and **Down** keys and press **Enter**.

**NOTE**
The **Maintenance** option is available if you have selected the **Veeam backup repository** or **Veeam Cloud Connect repository** option at the **Destination** step of the wizard.

2. In the **Maintenance** window, make sure that the **Allow backup server to prune old backups** option is selected and press **Space**.

3. In the **If this agent has been unavailable <N> days** field, specify the number of days for which you want to keep the backup created with the backup job in the target location. If Veeam Agent for Linux does not create new restore points for the backup, the backup will remain in the target location for the period that you have specified. When this period is over, the backup will be removed from the target location.

By default, the retention period for old backups is 30 days. Do not set this retention period to 1 day or a similar short interval. In the opposite case, the backup job may work not as expected and remove data that you still require.
Script Settings

At the **Advanced** step of the wizard, specify script settings for the backup job:

1. Select the **Scripts** option with the **Tab** and **Down** keys and press **Enter**.

2. In the **Scripts** window, in the **Job scripts** section, specify custom scripts that you want to execute before and/or after the backup job:
   - In the **Pre-job** field, specify a path to the script that should be executed before the backup job starts.
   - In the **Post-job** field, specify a path to the script that should be executed after the backup job completes.

3. In the **Scripts** window, in the **Snapshot scripts** section, specify custom scripts that you want to execute before Veeam Agent creates a snapshot of the backed-up volume and/or after the snapshot is created:
   - In the **Pre-freeze** field, specify a path to the script that should be executed before Veeam Agent creates a volume snapshot.
   - In the **Post-thaw** field, specify a path to the script that should be executed after Veeam Agent creates a volume snapshot.

4. Switch to the **Ok** button and press **Enter**.

**IMPORTANT**

You can specify snapshot script settings only if Veeam Agent for Linux operates in the Server edition. To learn more about editions, see **Product Editions**.
Specifying Path to Script

You can specify a path to the executable file of the job or snapshot script in one of the following ways:

1. Type a path to the executable file.
2. Browse to the executable file:
   a. Select the **Browse** option with the **Tab** key and press **Enter**.
   b. In the **Choose script location** window, select the directory being a part of the path to the script and press **Enter**.
   c. Repeat the step 'b' until a path to the directory in which the executable file resides appears in the **Current directory** field.
   d. Select the necessary executable file and press **Enter**.
      
      Alternatively, you can switch to the **Ok** button and press **Enter**.

**TIP**

If you do not want to execute a script, you can leave the corresponding field blank and proceed to the next step of the wizard.
Step 8. Specify Backup Schedule

At the **Schedule** step of the wizard, specify the schedule according to which you want to perform backup.

1. Make sure that the **Run the job automatically** check box is selected.
   
   If you want to configure the backup job without schedule, you can clear the **Run the job automatically** check box. In this case you will be able start the configured backup job manually at any time you need.

2. In the **Daily at** field, specify the time of day when the backup job must start.

3. In the list of days of the week, specify days on which the job must start. By default, Veeam Agent will start the backup job daily at the specified time. To exclude specific days from the schedule, clear check boxes next to the necessary days.

Veeam Agent for Linux will save the scheduling settings for the backup job in its database and in the **crontab** configuration file of the root account. Thus, Veeam Agent can start a backup job automatically regardless of the currently running user session. You can change schedule settings at any time in Veeam Agent or edit the **crontab** file manually to fine-tune the schedule. To learn more, refer to the Cron job scheduler documentation.
Step 9. Review Backup Job Settings

At the Summary step of the wizard, complete the backup job configuration process.

1. Review settings of the configured backup job.

2. To start the job after you close the wizard, make sure that the Start job now check box is selected.
   If you want to start the backup job later, you can clear the Start job now check box. You will be able to start the backup job manually at any time you need. To learn more, see Starting Backup Job.

3. Press Enter to exit the wizard.

![Summary screen showing backup job settings](image)
What You Do Next

After you configure the backup job, you can start the backup job at any time you need. To learn more, see Starting Backup Job.

If some of your data gets lost or corrupted, you can do the following:

- Recover all computer volumes or specific volumes from the backup.
- Recover individual files and folders from the backup.
Creating Backup Job with Command Line Interface

You can configure the backup job with the command line interface. Using Veeam Agent for Linux commands, you can create volume-level and file-level backup jobs, specify advanced settings for the created backup job, define backup schedule and enable backup encryption.
Creating Volume-Level Backup Job

**IMPORTANT**

Volume-level backup job relies on a device name in the `/dev` directory. Device names in the `/dev` directory (for example, `/dev/md-127`, `/dev/dm-1`) must stay persistent for backed-up volumes. Otherwise, the job will back up the wrong volume.

You can create a volume-level backup of the entire computer image or specific volumes.

To back up the entire computer image, use the following command:

```bash
veeamconfig job create volumelevel --name <job_name> --reponame <repository_name> --backupallsystem <advanced_options> <schedule_options> <active_full_backup_options> <indexing_options>
```

To back up specific volumes, use the following command:

```bash
veeamconfig job create volumelevel --name <job_name> --reponame <repository_name> --objects <volume_to_backup> <advanced_options> <schedule_options> <active_full_backup_options> <indexing_options>
```

where:

- `<job_name>` — name for the created backup job.
- `<repository_name>` — name of the backup repository that should be used as a target location for the backup job. The backup repository must be created in advance. To learn more, see Creating Backup Repository.

If you want to create Veeam Agent backups in a Veeam backup repository of cloud repository, you need connect to the Veeam backup server or Veeam Cloud Connect service provider in advance, before configuring the backup job. To learn more, see Connecting to Veeam Backup Server and Connecting to Service Provider.

- `<volume_to_backup>` — object that should be included in backup:
  - For simple volumes — name of a block device that represents a volume or an entire disk that should be included in backup. You can specify entire disk to create backup of the entire computer image or individual computer volumes to create backup of specific volumes. If you want to back-up several disks or volumes, specify them one after another using the ',' (comma) character as a separator.

  **NOTE**

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

  - For LVM volumes — name of an LVM logical volume that should be included in backup. If you want to back-up several LVM logical volumes, specify them one after another using the ',' (comma) character as a separator.
• `<advanced_options>` — advanced options for the backup job. To learn more, see Advanced Backup Job Settings.

• `<schedule_options>` — schedule options for the backup job. To learn more, see Schedule Settings.

• `<active_full_backup_options>` — active full backup schedule options for the backup job. To learn more, see Active Full Backup Schedule Settings.

• `<indexing_options>` — file system indexing options for the backup job. To learn more, see File System Indexing Settings.

For example:

```
$ veeamconfig job create volumelevel --name SystemBackup --reponame Repository_01 --objects /dev/sda1 --weekdays Mon,Sun --weekdays-full Thu
```

**TIP**

Consider the following:

- You can also specify backup schedule for the backup job after you create the backup job. For details, see Configuring Backup Schedule.
- You can also specify active full backup schedule for the backup job after you create the backup job. For details, see Configuring Active Full Backup Schedule.
- You can also specify database processing settings for the volume-level backup job. For details, see Configuring Database Processing Settings.
## Advanced Backup Job Settings

You can specify the following advanced options for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
</table>
| --compressionlevel | Data compression level. Possible values are:  
  - 0 — No compression  
  - 1 — Rle  
  - 2 — Lz4  
  - 3 — ZlibLow  
  - 4 — ZlibHigh  
  The default value is 2. |
| --blocksize    | Data block size in kilobytes. Possible values are 256, 512, 1024, 4096 or 8192. 
  The default value is 1024. |
| --maxpoints    | The number of restore points that you want to store in the backup location. By default, Veeam Agent for Linux keeps 7 latest restore points. When the new restore point that exceeds the specified number is created, Veeam Agent for Linux will remove the earliest restore point from the backup chain. |
| --prefreeze    | Path to the script that should be executed before the snapshot creation. 
  This option is available only if Veeam Agent for Linux operates in the Server edition. 
  To learn about editions, see Product Editions. |
| --postthaw     | Path to the script that should be executed after the snapshot creation. 
  This option is available only if Veeam Agent for Linux operates in the Server edition. 
  To learn about editions, see Product Editions. |
<p>| --prejob       | Path to the script that should be executed at the start of the backup job. |
| --postjob      | Path to the script that should be executed after the backup job completes. |
| --setencryption | Defines that data encryption option is enabled for the job. When you use the veeamconfig job create command with the --setencryption option, Veeam Agent for Linux will prompt you to specify a password for data encryption and hint for the password. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--deleteold</td>
<td>The number of days to keep the backup created with the backup job in the target location. If Veeam Agent for Linux does not create new restore points for the backup, the backup will remain in the target location for the specified number of days. When this period is over, the backup will be removed from the target location. Possible values are: 1-999. If you do not specify the --deleteold option, Veeam Agent will not apply this setting. The backup will be stored in the target location until you delete it manually.</td>
</tr>
</tbody>
</table>
## Schedule Settings

You can specify schedule options for the backup job to create backups daily or on specific weekdays at specific time:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--daily</strong></td>
<td>Defines that the backup job must start daily at specific time.</td>
</tr>
</tbody>
</table>
| **--weekdays** | Weekdays when the backup job must start separated by a comma (','). Possible values are:  
  - *Mon* — Monday  
  - *Tue* — Tuesday  
  - *Wed* — Wednesday  
  - *Thu* — Thursday  
  - *Fri* — Friday  
  - *Sat* — Saturday  
  - *Sun* — Sunday |
| **--at** | Time of day when the backup job must start specified in the *HH:MM* format. For example: 20:00. |

After the backup job is created, Veeam Agent for Linux automatically enables backup schedule. To learn about how to configure backup schedule for an existing backup job, see [Configuring Backup Schedule](#).
Active Full Backup Schedule Settings

You can specify schedule options for the backup job to create active full backups on specific weekdays or days of the month:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--weekdays-full</td>
<td>Weekdays when the backup job must create an active full backup separated by a comma (','). Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Mon — Monday</td>
</tr>
<tr>
<td></td>
<td>• Tue — Tuesday</td>
</tr>
<tr>
<td></td>
<td>• Wed — Wednesday</td>
</tr>
<tr>
<td></td>
<td>• Thu — Thursday</td>
</tr>
<tr>
<td></td>
<td>• Fri — Friday</td>
</tr>
<tr>
<td></td>
<td>• Sat — Saturday</td>
</tr>
<tr>
<td></td>
<td>• Sun — Sunday</td>
</tr>
<tr>
<td>--thisday-full</td>
<td>Days of the month when the backup job must create an active full backup separated by a comma (','). Possible values are: 1-30 (or 1-31, depending on the month length).</td>
</tr>
</tbody>
</table>

After the backup job is created, Veeam Agent for Linux automatically enables active full backup schedule. To learn about how to configure active full backup schedule for an existing backup job, see Configuring Active Full Backup Schedule.
File System Indexing Settings

You can specify one the following file system indexing options for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--indexall</td>
<td>Defines that Veeam Agent for Linux must index all files on the volumes included in backup.</td>
</tr>
<tr>
<td>--indexonly</td>
<td>Path to a directory that contains files that you want to index. Enter paths to the necessary directories. To separate several paths, use the ', ' (comma) character.</td>
</tr>
<tr>
<td>--indexexcept</td>
<td>Path to a directory that contains files that you do not want to index. You can specify one or more paths. To separate several paths, use the ', ' (comma) character.</td>
</tr>
</tbody>
</table>

To learn more about file indexing, see File System Indexing.
Creating File-Level Backup Job

To create a file-level backup job, use the following command:

```
veeamconfig job create filelevel --name <job_name> --reponame <repository_name>
<objects> <advanced_options> <schedule_options> <active_full_backup_options> <indexing_options> --nosnap
```

where:

- `<job_name>` — name for the created backup job.
- `<repository_name>` — name of the backup repository that should be used as a target location for the backup job. The backup repository must be created in advance. To learn more, see Creating Backup Repository

If you want to create Veeam Agent backups in the Veeam backup repository, you should connect to the Veeam backup server in advance, before configuring the backup job. To learn more, see Connecting to Veeam Backup Server.

- `<objects>` — files and directories inclusion/exclusion options. To learn more, see File Inclusion Options.
- `<advanced_options>` — advanced options for the backup job. To learn more, see Advanced Backup Job Settings.
- `<schedule_options>` — schedule options for the backup job. To learn more, see Schedule Settings.
- `<active_full_backup_options>` — active full backup schedule options for the backup job. To learn more, see Active Full Backup Schedule Settings.
- `<indexing_options>` — file system indexing options for the backup job. To learn more, see File System Indexing Settings.

- `--nosnap` — option that instructs Veeam Agent for Linux to perform backup in the snapshot-less mode. With this option enabled, Veeam Agent for Linux will not create a snapshot of the backed-up volumes during backup. This allows Veeam Agent to back up data residing in file systems that are not supported for snapshot-based backup with Veeam Agent for Linux. Keep in mind that the snapshot-less file-level backup does not guarantee that data in the backup is consistent. To learn more, see Snapshot-Less File-Level Backup.

For example:

```
$ veeamconfig job create filelevel --name HomeFolderBackup --reponame NetworkRepository --includedirs /home/user --excludedirs /home/user/temp --excludemasks "*.pdf"
```

**TIP**

Consider the following:

- You can also specify backup schedule for the backup job after you create the backup job. For details, see Configuring Backup Schedule.
- You can also specify active full backup schedule for the backup job after you create the backup job. For details, see Configuring Active Full Backup Schedule.
File Inclusion Options

When you create a file-level backup job, you must specify at least one directory that should be included in backup. If you do not want to back up some files and directories in the specified directory, you can exclude specific files and directories from backup.

To define the backup scope for the file-level backup job, you can use the following command-line options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--includedirs</td>
<td>Full path to a directory that should be included in backup, for example: /home/user.</td>
</tr>
<tr>
<td></td>
<td>You can specify one or several paths to directories in the computer file system. To</td>
</tr>
<tr>
<td></td>
<td>separate several paths, use the ', ' (comma) character, for example:</td>
</tr>
<tr>
<td></td>
<td>/home/user/Documents,/home/user/reports.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> If you want to back up the root directory and specify the '/' (slash) character,</td>
</tr>
<tr>
<td></td>
<td>Veeam Agent does not automatically include mount points in the backup scope. To</td>
</tr>
<tr>
<td></td>
<td>include mount points, you need to specify paths to these mount points manually.</td>
</tr>
<tr>
<td></td>
<td>For example, you have a file system mounted to the /home/media directory. If you add</td>
</tr>
<tr>
<td></td>
<td>/ as an object to the backup scope, Veeam Agent will not back up the mounted file</td>
</tr>
<tr>
<td></td>
<td>system. To back up the root directory and the mounted file system, add the following</td>
</tr>
<tr>
<td></td>
<td>objects to the backup scope: /,/home/media.</td>
</tr>
<tr>
<td>--excludedirs</td>
<td>Full path to a directory that should be excluded from backup. The directory specified</td>
</tr>
<tr>
<td></td>
<td>with this option must be a subdirectory of the directory specified with the --</td>
</tr>
<tr>
<td></td>
<td>includedirs option. To separate several paths, use the ' , ' (comma) character, for</td>
</tr>
<tr>
<td></td>
<td>example, /home/user/Documents,/home/user/reports.</td>
</tr>
<tr>
<td>Option</td>
<td>Description and values</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>--includemasks</strong></td>
<td>Mask for file name or path that should be included in backup. You can use the following UNIX wildcard characters for file name masks:</td>
</tr>
<tr>
<td></td>
<td>- <code>*</code> — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, <code>*.pdf</code>.</td>
</tr>
<tr>
<td></td>
<td>- <code>?</code> — a substitution of one character in the file name or path. For example, <code>report?.pdf</code>.</td>
</tr>
<tr>
<td></td>
<td>- <code>[ ]</code> — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the <code>-' character). For example: </code>report_201[3456].pdf<code>or</code>report_201[3-6].pdf`.</td>
</tr>
<tr>
<td></td>
<td>Keep in mind that you must specify all names with masks in double quotation marks (&quot;&quot;). For example: <code>--includemasks &quot;*.bak&quot;</code>.</td>
</tr>
<tr>
<td></td>
<td>If you want to use several file name masks, you must specify them in double quotation marks (&quot;&quot; ) and separated with a comma (,). For example: <code>--includemasks &quot;*.bak,*.pdf&quot;</code>.</td>
</tr>
<tr>
<td></td>
<td>File inclusion option is applied to all directories that are specified with the <code>--includedirs</code> option. For example, if you include in backup the /home/user/Documents directory and files that match the <code>report?.pdf</code> file name mask, Veeam Agent for Linux will back up the /home/user/Documents/report.pdf file and will not back up the /home/user/reports/report.pdf file.</td>
</tr>
<tr>
<td><strong>--excludemasks</strong></td>
<td>Mask for file name or path that should be excluded from backup. You can use the following UNIX wildcard characters for file name masks:</td>
</tr>
<tr>
<td></td>
<td>- <code>*</code> — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, <code>*.pdf</code>.</td>
</tr>
<tr>
<td></td>
<td>- <code>?</code> — a substitution of one character in the file name or path. For example, <code>report?.pdf</code>.</td>
</tr>
<tr>
<td></td>
<td>- <code>[ ]</code> — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the <code>-' character). For example: </code>report_201[3456].pdf<code>or</code>report_201[3-6].pdf`.</td>
</tr>
<tr>
<td></td>
<td>Keep in mind that you must specify all names with masks in double quotation marks (&quot;&quot;). For example: <code>--excludemasks &quot;*.bak&quot;</code>.</td>
</tr>
<tr>
<td></td>
<td>If you want to use several file name masks, you must specify them in double quotation marks (&quot;&quot; ) and separated with a comma (,). For example: <code>--excludemasks &quot;*.bak,*.pdf&quot;</code>.</td>
</tr>
</tbody>
</table>
|            | File exclusion option is applied to all directories that are specified with the `--includedirs` option and files that match file name masks specified with the `--`
<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>includemasks</td>
<td>For example, you may want to specify the following backup scope for the backup job:</td>
</tr>
<tr>
<td></td>
<td>• Include in backup the /home/user/Documents directory</td>
</tr>
<tr>
<td></td>
<td>• Include files that match the report.* file name mask</td>
</tr>
<tr>
<td></td>
<td>• Exclude files that match the *.odt file name mask.</td>
</tr>
</tbody>
</table>

In this case, Veeam Agent for Linux will back up the /home/user/Documents/report.pdf file and will not back up /home/user/Documents/report.odt and /home/user/reports/report.pdf files.
### Advanced Backup Job Settings

You can specify the following advanced options for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--compressionlevel</td>
<td>Data compression level. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• 0 — No compression</td>
</tr>
<tr>
<td></td>
<td>• 1 — Rle</td>
</tr>
<tr>
<td></td>
<td>• 2 — Lz4</td>
</tr>
<tr>
<td></td>
<td>• 3 — ZlibLow</td>
</tr>
<tr>
<td></td>
<td>• 4 — ZlibHigh</td>
</tr>
<tr>
<td>--blocksize</td>
<td>Data block size in kilobytes. Possible values are 256, 512, 1024, 4096 or 8192.</td>
</tr>
<tr>
<td></td>
<td>The default value is 1024.</td>
</tr>
<tr>
<td>--maxpoints</td>
<td>The number of restore points that you want to store in the backup location. By</td>
</tr>
<tr>
<td></td>
<td>default, Veeam Agent for Linux keeps 7 latest restore points. When the new restore</td>
</tr>
<tr>
<td></td>
<td>point that exceeds the specified number is created, Veeam Agent for Linux will</td>
</tr>
<tr>
<td></td>
<td>remove the earliest restore point from the backup chain.</td>
</tr>
<tr>
<td>--prefreeze</td>
<td>Path to the pre-freeze script that should be executed before the snapshot creation.</td>
</tr>
<tr>
<td></td>
<td>This option is available only if Veeam Agent for Linux operates in the Server edition.</td>
</tr>
<tr>
<td></td>
<td>To learn about editions, see <a href="#">Product Editions</a>.</td>
</tr>
<tr>
<td>--postthaw</td>
<td>Path to the post-thaw script that should be executed after the snapshot creation.</td>
</tr>
<tr>
<td></td>
<td>This option is available only if Veeam Agent for Linux operates in the Server edition.</td>
</tr>
<tr>
<td></td>
<td>To learn about editions, see <a href="#">Product Editions</a>.</td>
</tr>
<tr>
<td>--prejob</td>
<td>Path to the script that should be executed at the start of the backup job.</td>
</tr>
<tr>
<td>--postjob</td>
<td>Path to the script that should be executed after the backup job completes.</td>
</tr>
<tr>
<td>--setencryption</td>
<td>Defines that data encryption option is enabled for the job. When you use the</td>
</tr>
<tr>
<td></td>
<td>veeamconfig job create command with the --setencryption option, Veeam Agent</td>
</tr>
<tr>
<td></td>
<td>Agent for Linux will prompt you to specify a password for data encryption and hint for</td>
</tr>
<tr>
<td></td>
<td>the password.</td>
</tr>
<tr>
<td>Option</td>
<td>Description and values</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>--deleteold</strong></td>
<td>The number of days to keep the backup created with the backup job in the target location. If Veeam Agent for Linux does not create new restore points for the backup, the backup will remain in the target location for the specified number of days. When this period is over, the backup will be removed from the target location. Possible values are: 1–999. If you do not specify the <strong>--deleteold</strong> option, Veeam Agent will not apply this setting. The backup will be stored in the target location until you delete it manually.</td>
</tr>
</tbody>
</table>
Schedule Settings

You can specify schedule options for the backup job to create backups daily or on specific weekdays at specific time:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--daily</strong></td>
<td>Defines that the backup job must start daily at specific time.</td>
</tr>
<tr>
<td><strong>--weekdays</strong></td>
<td>Weekdays when the backup job must start separated by a comma (<code>,</code>). Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Mon — Monday</td>
</tr>
<tr>
<td></td>
<td>• Tue — Tuesday</td>
</tr>
<tr>
<td></td>
<td>• Wed — Wednesday</td>
</tr>
<tr>
<td></td>
<td>• Thu — Thursday</td>
</tr>
<tr>
<td></td>
<td>• Fri — Friday</td>
</tr>
<tr>
<td></td>
<td>• Sat — Saturday</td>
</tr>
<tr>
<td></td>
<td>• Sun — Sunday</td>
</tr>
<tr>
<td><strong>--at</strong></td>
<td>Time of day when the backup job must start specified in the \textit{HH:MM} format. For example: 20:00.</td>
</tr>
</tbody>
</table>

After the backup job is created, Veeam Agent for Linux automatically enables backup schedule. To learn about how to configure backup schedule for an existing backup job, see \textit{Configuring Backup Schedule}. 
Active Full Backup Schedule Settings

You can specify schedule options for the backup job to create active full backups on specific weekdays or days of the month:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
</table>
| --weekdays-full| Weekdays when the backup job must create an active full backup separated by a comma (’,’). Possible values are:  
|                | • Mon — Monday         |
|                | • Tue — Tuesday        |
|                | • Wed — Wednesday      |
|                | • Thu — Thursday       |
|                | • Fri — Friday         |
|                | • Sat — Saturday       |
|                | • Sun — Sunday         |
| --thisday-full | Days of the month when the backup job must create an active full backup separated by a comma (’,’). Possible values are: 1-30 (or 1-31, depending on the month length). |

After the backup job is created, Veeam Agent for Linux automatically enables active full backup schedule. To learn about how to configure active full backup schedule for an existing backup job, see Configuring Active Full Backup Schedule.
File System Indexing Settings

You can specify the following file system indexing option for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--indexall</td>
<td>Defines that Veeam Agent for Linux must index all files in the directories included in backup.</td>
</tr>
</tbody>
</table>

To learn more about file indexing, see [File System Indexing](#).
Configuring Backup Schedule

To run a backup job periodically without the user intervention, you can schedule it to start automatically. You can specify schedule settings individually for every job created in Veeam Agent for Linux. You can perform the following actions with the backup job schedule via the command-line interface:

- Specify schedule settings for the job.
- Enable schedule for the job.
- View the schedule defined for the job.
- Disable schedule for the job.

**TIP**
You can also specify backup schedule for the backup job when you create the job. For details, see Creating Volume-Level Backup Job and Creating File-Level Backup Job.
Specifying Backup Schedule

You can schedule a backup job to start at specific time daily or on specific weekdays.
Specifying Daily Schedule

To specify daily schedule settings for the backup job, use the following command:

```
veeamconfig schedule set --jobid <job_id> --daily --at <time>
```

or

```
veeamconfig schedule set --jobname <job_name> --daily --at <time>
```

where:

- `<job_id>` — ID of the backup job for which you want to configure the schedule. You should look up the job ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Jobs.

- `<job_name>` — name of the backup job for which you want to configure the schedule.

TIP

To view IDs or names of all existent backup jobs, you can press the Tab key right after you type the `--jobid` or `--jobname` option.

- `<time>` — time of day when the backup job must start specified in the `HH:MM` format. For example: 20:00.

For example:

```
user@srv01:$ veeamconfig schedule set --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f --daily --at 20:00
```
Specifying Schedule on Specific Days

To specify schedule settings for the backup job, use the following command:

```sh
to specify schedule settings for the backup job, use the following command:
```

```sh
veeamconfig schedule set --jobid <job_id> --weekdays <days> --at <time>
```

or

```sh
veeamconfig schedule set --jobname <job_name> --weekdays <days> --at <time>
```

where:

- `<job_id>` — ID of the backup job for which you want to configure the schedule. You should look up the job ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Jobs.

- `<job_name>` — name of the backup job for which you want to configure the schedule.

TIP

To view IDs or names of all existent backup jobs, you can press the Tab key right after you type the `--jobid` or `--jobname` option.

- `<days>` — days when the backup job must start separated by a comma (`,`). For example: Monday,Tuesday,Wednesday,Thursday,Friday.

- `<time>` — time of day when the backup job must start specified in the `HH:MM` format. For example: 20:00.

For example:

```sh
user@srv01:~$ veeamconfig schedule set --jobname DailyBackup --weekdays Monday, Tuesday, Wednesday, Thursday, Friday --at 20:00
```
Enabling Backup Schedule

To run a backup job automatically upon the defined schedule, you must enable the schedule for the job. Use the following command:

```
veeamconfig schedule enable --jobid <job_id>
```

or

```
veeamconfig schedule enable --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup job for which you want to enable the schedule. You should look up the job ID in advance, for example, with the veeamconfig job list command. To learn more, see Viewing List of Backup Jobs.

- `<job_name>` — name of the backup job for which you want to enable the schedule.

For example:

```
user@srv01:~$ veeamconfig schedule enable --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
```

You can disable the schedule for the job at any time. To learn more, see Disabling Backup Schedule.
Viewing Backup Schedule

To view the schedule defined for the backup job, use the following command:

```
veeamconfig schedule show --jobid <job_id>
```

or

```
veeamconfig schedule show --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup job for which you want to view the schedule.
- `<job_name>` — name of the backup job for which you want to view the schedule.

Veeam Agent for Linux displays the following information about the backup job schedule:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days</td>
<td>Days on which the backup job runs automatically.</td>
</tr>
<tr>
<td>At</td>
<td>Time of day when the backup job starts automatically.</td>
</tr>
<tr>
<td>Run automatically</td>
<td>State of backup schedule. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig schedule show --jobid 4849a3ae-1935-4969-98a3-d8acd2f6c73f
Days: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
At: 20:00
Run automatically: enabled
```
Disabling Backup Schedule

To disable the schedule for the backup job, use the following command:

```
veeamconfig schedule disable --jobid <job_id>
```

or

```
veeamconfig schedule disable --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup job for which you want to disable the schedule.
- `<job_name>` — name of the backup job for which you want to disable the schedule.

For example:

```
user@srv01:~$ veeamconfig schedule disable --jobid 4849a3ae-1935-4969-98a3-d8ac d2f6c73f
```
Configuring Active Full Backup Schedule

You can schedule a backup job to create active full backups periodically. You can specify active full schedule settings individually for every job created in Veeam Agent for Linux. You can perform the following actions with the active full backup schedule via the command-line interface:

- Specify active full backup schedule.
- Enable active full backup schedule.
- View active full backup schedule.
- Disable active full backup schedule.

**TIP**
You can also specify active full backup schedule for the backup job when you create the job. For details, see [Creating Volume-Level Backup Job](#) and [Creating File-Level Backup Job](#).
Specifying Active Full Backup Schedule

You can schedule a backup job to create active full backups on a specific day of the month or on specific week days.
Specifying Monthly Active Full Backup Schedule

To instruct Veeam Agent to perform active full backup on a specific day on the month, use the following command:

```
veeamconfig schedule activefull set --jobid <job_id> --thisday <day>
```

or

```
veeamconfig schedule activefull set --jobname <job_name> --thisday <day>
```

where:

- `<job_id>` — ID of the backup job for which you want to configure the active full backup schedule. You should look up the job ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Jobs.

- `<job_name>` — name of the backup job for which you want to configure the active full backup schedule.

**TIP**

To view IDs or names of all existent backup jobs, you can press the Tab key right after you type the `--jobid` or `--jobname` option.

- `<day>` — number of the day of the month when Veeam Agent must perform active full backup.

For example:

```
user@srv01:~$ veeamconfig schedule activefull set --jobname DailyBackup --thisday 1
```
Specifying Weekly Active Full Backup Schedule

To instruct Veeam Agent to perform active full backup on specific week days, use the following command:

```
veeamconfig schedule activefull set --jobid <job_id> --weekdays <days>
```

or

```
veeamconfig schedule activefull set --jobname <job_name> --weekdays <days>
```

where:

- `<job_id>` — ID of the backup job for which you want to configure the active full backup schedule. You should look up the job ID in advance, before configuring the schedule, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Jobs.

- `<job_name>` — name of the backup job for which you want to configure the active full backup schedule.

TIP

To view IDs or names of all existent backup jobs, you can press the Tab key right after you type the `--jobid` or `--jobname` option.

- `<days>` — days when the backup job must create an active full backup separated by a comma (','). For example: `Monday,Friday`. The backup job will create an active full backup on the specified days at the time specified in the backup job schedule settings.

For example:

```
user@srv01:~$ veeamconfig schedule activefull set --jobname DailyBackup --weekdays Monday,Friday
```
Enabling Active Full Backup Schedule

After you specify active full backup schedule settings for the backup job, Veeam Agent automatically enables active full backup schedule for the job. You can also enable active full backup schedule manually, for example, if you previously disabled it for the backup job. To enable active full backup schedule, use the following command:

```
veeamconfig schedule activefull enable --jobid <job_id>
```

or

```
veeamconfig schedule activefull enable --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup job for which you want to enable the active full backup schedule. You should look up the job ID in advance, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Jobs.

- `<job_name>` — name of the backup job for which you want to enable the active full backup schedule.

For example:

```
user@srv01:$ veeamconfig schedule activefull enable --jobname DailyBackup
```

You can disable the schedule for the job at any time. To learn more, see Disabling Backup Schedule.
Viewing Active Full Backup Schedule

To view the active full backup schedule defined for the backup job, use the following command:

```
veeamconfig schedule activefull show --jobid <job_id>
```

or

```
veeamconfig schedule activefull show --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup job for which you want to view the active full backup schedule.
- `<job_name>` — name of the backup job for which you want to view the active full backup schedule.

Veeam Agent for Linux displays the following information about the active full backup schedule:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every <code>&lt;value&gt;</code></td>
<td>Days on which the backup job creates active full backups. For example: Every Monday or Every 1 day of every month.</td>
</tr>
<tr>
<td>Run automatically</td>
<td>State of the active full backup schedule. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig schedule activefull show --jobname DailyBackup
Every Monday
Run automatically: enabled
```
Disabling Active Full Backup Schedule

To disable the active full backup schedule for the backup job, use the following command:

```
veeamconfig schedule activefull disable --jobid <job_id>
```

or

```
veeamconfig schedule activefull disable --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup job for which you want to disable the active full backup schedule.
- `<job_name>` — name of the backup job for which you want to disable the active full backup schedule.

For example:

```
user@srv01:$ veeamconfig schedule activefull disable --jobname DailyBackup
```
Configuring Database Processing Settings

You can enable database processing settings in the properties of a volume-level backup job configured in Veeam Agent for Linux. With database processing settings enabled, Veeam Agent will create transactionally consistent backups of Veeam Agent machines that run database systems.

You can perform the following actions with database processing settings via the command-line interface:

- Specify Oracle database processing settings
- Specify MySQL database processing settings
- Specify PostgreSQL database processing settings
- View database processing settings
- Disable database processing settings
Specifying Oracle Processing Settings

You can enable Oracle processing settings in the properties of a volume-level backup job configured in Veeam Agent for Linux.

To enable Oracle processing settings for the backup job, use the following command:

\[
\text{veeamconfig aap set oracle --jobid <job_id> <oracle_options>}
\]

or

\[
\text{veeamconfig aap set oracle --jobname <job_name> <oracle_options>}
\]

where:

- `<job_id>` — ID of the backup job for which you want to enable Oracle processing settings. You should look up the job ID in advance, before configuring Oracle processing settings, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Jobs.
- `<job_name>` — name of the backup job for which you want to enable Oracle processing settings.
- `<oracle_options>` — Oracle processing settings for the backup job. To learn more, see Oracle Processing Settings.

TIP

To view IDs or names of all existent backup jobs, you can press the Tab key right after you type the `--jobid` or `--jobname` option.
### Oracle Processing Settings

You can specify the following Oracle processing settings for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--tryprocess</strong></td>
<td>Defines that Veeam Agent must continue the backup process if errors occur when processing the Oracle database system. If you do not specify this option, Veeam Agent will stop the backup process if an error occurs when processing the Oracle database system.</td>
</tr>
</tbody>
</table>
| **--prunelogs** | The number of hours to keep Oracle archived logs or the size of archived logs to keep.  
- If you want Veeam Agent to delete archived logs that are older than \(<N>\) hours, specify the necessary value in the \(<N>H\) format. For example, \(10H\).  
- If you want Veeam Agent to delete archived logs that are larger than \(<N>\) GB, specify the necessary value in the \(<N>G\) format. For example: \(10G\).  
Veeam Agent will wait for the backup job to complete successfully and then trigger archived logs truncation via Oracle Call Interface (OCI). If the backup job fails, the logs will remain untouched until the next successful backup job session. |
| **--usroracleos** | Name of the Veeam Agent machine OS account. To connect to the Oracle database system, the account must be a member of the group that owns configuration files for the Oracle database (for example, the oinstall group).  
You do not need this option if you want to use the Oracle account to connect to the database. Instead, specify the necessary account with the **--usroracledb** option. |
| **--usroracledb** | Name of the Oracle account. To connect to the Oracle database system, the account must have SYSDBA rights on the databases to be processed.  
You do not need this option if you want to use the OS account to connect to the database. Instead, specify the necessary account with the **--usroracleos** option. |

For example:

```bash
user@srv01:~$ veeamconfig aap set oracle --jobid 29bc2e1a-e35c-4efb-8d37-b7177b8ea75 --tryprocess --prunelogs 10G --usroracledb system
```
Specifying MySQL Processing Settings

You can enable MySQL processing settings in the properties of a volume-level backup job configured in Veeam Agent for Linux.

**IMPORTANT**
To process the MySQL database system, the MySQL account must have the following privileges:

- SELECT for all tables. If you do not have the SELECT privilege for the table, Veeam Agent does not process the table.
- LOCK TABLES. If you do not have the LOCK TABLES privilege, Veeam Agent does not process MyISAM tables.
- RELOAD. This privilege is required to allow the MySQL account to perform FLUSH operations.

To obtain information about privileges that are assigned to the account, use MySQL functionality, for example, the SHOW GRANTS statement. To learn more, see [MySQL documentation](#).

To enable MySQL processing settings for the backup job, use the following command:

```
veeamconfig aap set mysql --jobid <job_id> <mysql_options>
```

or

```
veeamconfig aap set mysql --jobname <job_name> <mysql_options>
```

where:

- `<job_id>` — ID of the backup job for which you want to enable MySQL processing settings. You should look up the job ID in advance, before configuring MySQL processing settings, for example, with the `veeamconfig job list` command. To learn more, see [Viewing List of Backup Jobs](#).
- `<job_name>` — name of the backup job for which you want to enable MySQL processing settings.
- `<mysql_options>` — MySQL processing settings for the backup job. To learn more, see [MySQL Processing Settings](#).

**TIP**
To view IDs or names of all existent backup jobs, you can press the Tab key right after you type the `--jobid` or `--jobname` option.
MySQL Processing Settings

You can specify the following MySQL processing settings for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--tryprocess</td>
<td>Defines that Veeam Agent must continue the backup process if errors occur when processing the MySQL database system. If you do not specify this option, Veeam Agent will stop the backup process if an error occurs when processing the MySQL database system.</td>
</tr>
<tr>
<td>--usrmysqidb</td>
<td>Name of the MySQL account. Veeam Agent can connect to the MySQL database system in one of the following ways:</td>
</tr>
<tr>
<td></td>
<td>• If you specify account name (--usrmysqidb option) only, Veeam Agent will prompt you to specify a password to access the MySQL database system.</td>
</tr>
<tr>
<td></td>
<td>• If you specify account name and password (--usrmysqidb and --password options), Veeam Agent will access the MySQL database system.</td>
</tr>
<tr>
<td></td>
<td>• If you do not specify account credentials (--usrmysqidb and --password options), Veeam Agent will use a password file to connect to the MySQL database system. To learn more about password file configuration, see Preparing Password File for MySQL Processing.</td>
</tr>
<tr>
<td>--password</td>
<td>Password of the MySQL account. If you do not specify the --password value, Veeam Agent will prompt you to specify a password to access the MySQL database. Keep in mind, if you specify the password using the --password option, password is stored in terminal in plain text.</td>
</tr>
<tr>
<td>--defaults-file</td>
<td>Path to a password file. You must specify a full path to a password file if you want Veeam Agent to use a password file located in specific directory. Specifying relative paths is not supported.</td>
</tr>
<tr>
<td></td>
<td>With this method selected, you do not need to specify account credentials in the backup job settings.</td>
</tr>
<tr>
<td></td>
<td>You do not need this option in the following cases:</td>
</tr>
<tr>
<td></td>
<td>• Veeam Agent uses account name and password that are specified in the backup job settings to connect to the MySQL database.</td>
</tr>
<tr>
<td></td>
<td>• Veeam Agent uses account credentials that are stored in the password file in /root/.my.cnf.</td>
</tr>
</tbody>
</table>
Examples

Authentication with password:

```bash
user@srv01:~$ veeamconfig aap set mysql --jobid 29bc2e1a-e35c-4efb-8d37-b7177bea75 --tryprocess --usrmysqldb root --password P@ssw0rd
```

Authentication with password file:

```bash
user@srv01:~$ veeamconfig aap set mysql --jobid 29bc2e1a-e35c-4efb-8d37-b7177bea75 --tryprocess --defaults-file /data/root/.my.cnf --password P@ssw0rd
```
Preparing Password File for MySQL Processing

You can use MySQL account credentials that are stored in the password file to connect Veeam Agent for Linux to the MySQL database system.

**NOTE**

Consider the following:

- If you specify a custom path to the password file, specify a full path. Specifying relative paths is not supported.
- The password file can also contain user-specific connection settings that Veeam Agent will apply to connect to the MySQL database system. For example, if you want to connect to the MySQL database system using the custom socket, specify the socket path in the password file. To learn more, see MySQL documentation.

If you want to use a password file for authentication, create a file. By default, Veeam Agent expects the password file to have the `.my.cnf` name and to be in the home directory of the `root` user. If the password file has a custom name or is stored in another directory, you can specify a custom path.

The password file must have the following contents:

```
[client]
user=<username>
password=<password>
```

where:

- `<username>` — name of the account that Veeam Agent will use to connect to the MySQL database system.
- `<password>` — password of the account that Veeam Agent will use to connect to the MySQL database system.

For example:

```
[client]
user=root
password=P@ssw0rd
```
Specifying PostgreSQL Processing Settings

You can enable PostgreSQL processing settings in the properties of a volume-level backup job configured in Veeam Agent for Linux.

To enable PostgreSQL processing settings for the backup job, use the following command:

```
veeamconfig aap set postgres --jobid <job_id> <postgres_options>
```

or

```
veeamconfig aap set postgres --jobname <job_name> <postgres_options>
```

where:

- `<job_id>` — ID of the backup job for which you want to enable PostgreSQL processing settings. You should look up the job ID in advance, before configuring PostgreSQL processing settings, for example, with the `veeamconfig job list` command. To learn more, see Viewing List of Backup Jobs.

- `<job_name>` — name of the backup job for which you want to enable PostgreSQL processing settings.

- `<postgres_options>` — PostgreSQL processing settings for the backup job. To learn more, see PostgreSQL Processing Settings.

**TIP**

To view IDs or names of all existent backup jobs, you can press the **Tab** key right after you type the `--jobid` or `--jobname` option.
PostgreSQL Processing Settings

You can specify the following PostgreSQL processing settings for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--tryprocess</td>
<td>Defines that Veeam Agent must continue the backup process if errors occur when processing the PostgreSQL database system. If you do not specify this option, Veeam Agent will stop the backup process if an error occurs when processing the PostgreSQL database system.</td>
</tr>
<tr>
<td>--usrpgdb</td>
<td>Name of the PostgreSQL account.</td>
</tr>
<tr>
<td></td>
<td>If you uses a password file to connect to the PostgreSQL database system, the --usrpgdb option allows to select the user from the password file.</td>
</tr>
<tr>
<td></td>
<td>You do not need this option if you want to use a Veeam Agent machine OS account to connect to the PostgreSQL database system. Instead, specify the OS account with the --usrpgos option.</td>
</tr>
<tr>
<td>--password</td>
<td>Password of the PostgreSQL account.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify this option, Veeam Agent will prompt to enter the password. If you do not specify the password in prompt, Veeam Agent uses a password file to connect to the PostgreSQL database system. To learn more about password file configuration, see Preparing Password File for PostgreSQL Processing.</td>
</tr>
<tr>
<td></td>
<td>Keep in mind, if you specify the password using the --password option, password is stored in terminal in plain text.</td>
</tr>
<tr>
<td>--usrpgos</td>
<td>Name of the OS account. Veeam Agent will use the name to connect to the PostgreSQL database system using the peer authentication method. In the peer authentication method, Veeam Agent uses the OS account as the PostgreSQL database user name. With this option selected, you must specify OS account only. To learn more about peer authentication, see PostgreSQL documentation.</td>
</tr>
<tr>
<td></td>
<td>You do not need this option if you want to use a PostgreSQL account to connect to the database system. Instead, specify the PostgreSQL account with the --usrpgdb option.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:$ veeamconfig aap set postgres --jobid 29bc2e1a-e35c-4efb-8d37-b7177b8ea75 --tryprocess --usrpgdb postgres --password P@ssw0rd
```
Preparing Password File for PostgreSQL Processing

You can use PostgreSQL account credentials that are stored in the password file to connect Veeam Agent to the PostgreSQL database system.

If you want to use a password file for authentication, create the `.pgpass` file in the home directory of the root user.

The password file must have the following contents:

```
<hostname>:<port>:<database>:<username>:<password>
```

where:

- `<hostname>` — name of the host where the PostgreSQL database system is located.
- `<port>` — number of the free port that Veeam Agent will use to connect to the PostgreSQL database system.
- `<database>` — name of the PostgreSQL database.
- `<username>` — name of the account that Veeam Agent will use to connect to the PostgreSQL database system.
- `<password>` — password of the account that Veeam Agent will use to connect to the PostgreSQL database system.

For example:

```
srv01:5432:mydb:postgres:P@ssw0rd
```

For more information about the password file, see PostgreSQL documentation.
Viewing Database Processing Settings

To view database processing settings defined for the backup job, use the following command:

```
veeamconfig aap show --jobid <job_id>
```

or

```
veeamconfig aap show --jobname <job_name>
```

where:

- `<job_id>` — ID of the backup job for which you want to view database processing settings.
- `<job_name>` — name of the backup job for which you want to view database processing settings.

Veeam Agent for Linux displays the following information about database processing settings:

- Oracle processing settings
- MySQL processing settings
- PostgreSQL processing settings
## Oracle Processing Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Oracle processing          | Oracle processing settings status. Possible values:  
  - *Required* — Oracle processing settings are enabled for the job. If an error occurs when processing the Oracle database system, Veeam Agent will stop the backup process.  
  - *Try* — Oracle processing settings are enabled for the job. If an error occurs when processing the Oracle database system, Veeam Agent will continue the backup process.  
  - *Disabled* — Oracle processing settings are disabled for the job using command line interface. |
| Account used for processing| Account used to connect to the Oracle database. Possible values:  
  - *System account (username: <username>)* — if Veeam Agent connects to the Oracle database system with the account of the Veeam Agent machine OS.  
  - *Oracle account (username: <username>)* — if Veeam Agent connects to the Oracle database system with the Oracle account.  
    where `<username>` is a name of the user account that Veeam Agent will use to connect to the Oracle database. |
| Delete logs over `<N>` Gb  | Veeam Agent displays this information if Veeam Agent is set to delete archived logs that are larger than `<N>` GB.                                  |
| Delete logs older `<N>` Hr | Veeam Agent displays this information if Veeam Agent is set to delete archived logs that are older than `<N>` hours.                             |

For example:

```
user@srv01:$ veeamconfig aap show --jobid 29bc2e1a-e35c-4efb-8d37-b7177b8ea75
Oracle processing: required
  Account used for processing: Oracle account (username: sys)
  Delete logs over 10 Gb
```
## MySQL Processing Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **MySQL processing**      | MySQL processing settings status. Possible values:  
|                            | • *Required* — MySQL processing settings are enabled for the job. If an error occurs when processing a MySQL database, Veeam Agent will stop the backup process.  
|                            | • *Try* — MySQL processing settings are enabled for the job. If an error occurs when processing a MySQL database, Veeam Agent will continue the backup process.  
|                            | • *Disabled* — MySQL processing settings are disabled for the job using command line interface. |
| **Account used for processing** | Veeam Agent displays this information if Veeam Agent is set to connect to the MySQL database system with the account name and password. |
| **Path to a password file** | Veeam Agent displays this information if Veeam Agent is set to connect to the MySQL database system with the account credentials that are stored in the password file. |

For example:

```bash
user@srv01:~$ veeamconfig aap show --jobid 29bc2e1a-e35c-4efb-8d37-b7177b8ea75
MySQL processing: required
   Account used for processing: username: root
```
## PostgreSQL Processing Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL processing</td>
<td>PostgreSQL processing settings status. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• <em>Required</em> — PostgreSQL processing settings are enabled for the job. If an error occurs when processing a PostgreSQL database, Veeam Agent will stop the backup process.</td>
</tr>
<tr>
<td></td>
<td>• <em>Try</em> — PostgreSQL processing settings are enabled for the job. If an error occurs when processing a PostgreSQL database, Veeam Agent will continue the backup process.</td>
</tr>
<tr>
<td></td>
<td>• <em>Disabled</em> — PostgreSQL processing settings are disabled for the job using command line interface.</td>
</tr>
<tr>
<td>Account used for processing</td>
<td>Account used to connect to the PostgreSQL database. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;username&gt; (password)</code> — Veeam Agent displays this information if Veeam Agent is set to connect to the PostgreSQL database with the PostgreSQL account.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;username&gt; (file)</code> — Veeam Agent displays this information if Veeam Agent is set to connect to the PostgreSQL database with the password file.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;username&gt; (peer)</code> — Veeam Agent displays this information if Veeam Agent is set to connect to the PostgreSQL database with the Veeam Agent machine OS account.</td>
</tr>
<tr>
<td></td>
<td>where <code>&lt;username&gt;</code> is a name of the account that Veeam Agent will use to connect to the PostgreSQL database.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig aap show --jobid 29bc2e1a-e35c-4efb-8d37-b7177b8ea75
PostgreSQL processing: required
   Account used for processing: postgres (password)
```
Disabling Database Processing Settings

To disable database processing settings defined for the backup job, use the following command:

```bash
veeamconfig aap disable <db_sys> --jobid <job_id>
```

or

```bash
veeamconfig aap disable <db_sys> --jobname <job_name>
```

where:

- `<db_sys>` — name of the database system that you want to disable. Possible values:
  - `oracle` – Oracle database processing to be disabled.
  - `mysql` – MySQL database processing to be disabled.
  - `postgres` – PostgreSQL database processing to be disabled.
- `<job_id>` – ID of the backup job for which you want to disable database processing settings.
- `<job_name>` – name of the backup job for which you want to disable database processing settings.

For example:

```bash
user@srv01:~$ veeamconfig aap disable oracle --jobid 29bc2e1a-e35c-4efb-8d37-b7177b8ea759
Oracle processing was disabled.
```
Starting and Stopping Backup Jobs

You can start a backup job manually at any time you need, for example, if you want to create an additional restore point for Veeam Agent backup and do not want to change the job schedule. You can also stop the running backup job before the job session completes, if necessary.

You can start and stop backup jobs in one of the following ways:

- With the Veeam Agent control panel
- With the Veeam Agent command line interface
Starting Backup Job from Control Panel

You can start a backup job with the Veeam Agent control panel.

**NOTE**
Veeam Agent can currently perform only one backup job at a time. You cannot start a backup job when another backup job is already running.

To start a backup job:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command.
2. Press the 's' key to open the **Select job to start** dialog window.
3. Select the necessary backup job in the list and start the job in one of the following ways:
   - To start an incremental backup job session, press **Enter**.
   - To create an active full backup, press 'f'.
4. Veeam Agent will immediately start the backup job and display a notification window informing that the job has been started. Press **Enter** to close the window and proceed to the list of backup job sessions.

You can monitor the backup job performance in the Veeam Agent control panel. To learn more, see Viewing Real-Time Job Session Statistics.

<table>
<thead>
<tr>
<th>Name</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>DailyBackup</td>
<td>/home/user/veeam</td>
</tr>
<tr>
<td>SystemBackup</td>
<td>[srv12] Default Backup Repo...</td>
</tr>
<tr>
<td>srvo1cloudBackup</td>
<td>[172.17.53.62] TechCompany...</td>
</tr>
</tbody>
</table>
Starting Backup Job from Command Line Interface

You can start a backup job with the command line interface. When you start a backup job, Veeam Agent initiates a new backup job session and provides you with a Session ID. You can monitor the progress of the backup job session or view the session status.

NOTE

Veeam Agent can currently perform only one backup job at a time. You cannot start a backup job when another backup job is already running.

To start a backup job, use the following command:

```bash
veeamconfig job start --name <job_name>
```

or

```bash
veeamconfig job start --id <job_id>
```

where:

- `<job_name>` — name of the backup job that you want to start.
- `<job_id>` — ID of the backup job that you want to start.

TIP

Consider the following:

- You can use the `veeamconfig job start` command with the `--nosnap` option to start a file-level backup job. In this case, Veeam Agent will not create a snapshot of the backed-up volume during the backup job session. Keep in mind that the snapshot-less file-level backup does not guarantee that data in the backup is consistent. To learn more, see Snapshot-Less File-Level Backup.

- You can use the `veeamconfig job start` command with the `--activefull` option to create active full backups. To learn more, see Creating Active Full Backups.

For example:

```
$ veeamconfig job start --name SystemBackup
Backup job has been started.
Session ID: [381532f7-426a-4e89-b9fc-43d98942c71a].
Logs stored in: [/var/log/veeam/Backup/SystemBackup/Session_20161207_162608_{381532f7-426a-4e89-b9fc-43d98942c71a}].
```

You can check the backup job session status or view the backup job session log using the Veeam Agent command line interface.

You can also monitor the backup job performance in the Veeam Agent control panel. To learn more, see Viewing Real-Time Job Session Statistics.
Creating Active Full Backups

You can create an ad-hoc full backup — active full backup, and add it to the backup chain on the target storage. The active full backup resets the backup chain. All subsequent incremental backups use the active full backup as a starting point. The previously used full backup will remain on the target storage until it is removed from the backup chain according to the retention policy.

Before you create an active full backup, check the following prerequisites:

- The backup job must be configured.
- You cannot create an active full backup if a backup task of any type is currently running.

To perform active full backup, use the following command:

```
veeamconfig job start --name <job_name> --activefull
```

or

```
veeamconfig job start --id <job_id> --activefull
```

where:

- `<job_name>` — name of the backup job that you want to start to create an active full backup.
- `<job_id>` — ID of the backup job that you want to start to create an active full backup.

For example:

```
$ veeamconfig job start --name SystemBackup --activefull
Backup job has been started.
Session ID: [{ce864e24-8211-4df7-973a-741adce96fe7}].
Logs stored in: [/var/log/veeam/Backup/SystemBackup/Session_20180611_150046_{ce864e24-8211-4df7-973a-741adce96fe7}].
```

You can view the progress for the active full backup session in the same way as for any other backup job session. In particular, you can check the backup job session status or view the backup job session log using the Veeam Agent command line interface.

You can also monitor the backup job performance in the Veeam Agent control panel. To learn more, see Viewing Real-Time Job Session Statistics.
Stopping Backup Job

You can stop the running backup job before the job session completes, for example, if the backup process is about to take long, and you do not want the job to produce workload on the production environment during business hours.

When you stop a backup job, the job session will finish immediately. Veeam Agent will not produce a new restore point during the session, and the session will finish with the *Failed* status.

You can stop a job in one of the following ways:

- With the control panel
- With the command line interface
Stopping Job from Control Panel

To stop a backup job:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command.
2. In the Veeam Agent control panel, in the list of backup job sessions, select the currently running session with `Up` and `Down` keys and press `Enter`.
3. In the session statistics window, press 's'.
4. In the displayed window, make sure that the Yes button is selected and press `Enter`. 

![Image of Veeam Agent control panel showing job status and options to stop the job]
Stopping Job from Command Line Interface

To stop a backup job, use the following command:

```
veeamconfig session stop --id <session_id>
```

or

```
veeamconfig session stop --force --id <session_id>
```

where:

- `<session_id>` — ID of the currently running backup job session that you want to stop.
- `--force` — with this option enabled, Veeam Agent will immediately stop the backup session even if it is unable to stop the `veeamjobman` process for some reason.

For example:

```
$ veeamconfig session stop --id 301532f7-426a-4e89-b9fc-43d98942c71a
Session has stopped.
```
Managing Backup Jobs

You can perform the following actions with backup jobs configured in Veeam Agent for Linux:

- View the list of configured backup jobs.
- View information about the backup job settings.
- Edit the backup job settings.
- Delete a backup job.
Viewing List of Backup Jobs

To view a list of backup jobs configured in Veeam Agent for Linux, use the following command:

```
veeamconfig job list
```

In the list of backup jobs, Veeam Agent for Linux displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the backup job.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the backup job.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository that is specified as a backup storage for the backup job.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig job list
Name       ID                                      Repository
SystemBackup {2495911e-58db-4452-b4d1-f53dcfbc600e}  Repository_1
DocumentsBackup {bcf821e6-b35f-4d57-b1c3-d3a477605cb9}  Repository_1
HomePartitionBackup {2aaa8c71-2434-4f12-a168-3d8e225fa416}  Repository_2
```
Viewing Backup Job Settings

To view detailed information about the backup jobs settings, use the following command:

```bash
veeamconfig job info --name <job_name>
```

or

```bash
veeamconfig job info --id <job_id>
```

where:

- `<job_name>` — name of the backup job for which you want to view settings.
- `<job_id>` — ID of the backup job for which you want to view settings.

Veeam Agent for Linux displays the following information about the backup job:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the backup job.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the backup job.</td>
</tr>
<tr>
<td>Repository ID</td>
<td>ID of the backup repository that is specified as a backup storage for the backup job.</td>
</tr>
<tr>
<td>Repository name</td>
<td>Name of the backup repository that is specified as a backup storage for the backup job.</td>
</tr>
<tr>
<td>Creation time</td>
<td>Date and time of the backup job creation.</td>
</tr>
<tr>
<td>Compression</td>
<td>Data compression level. Possible values are:</td>
</tr>
<tr>
<td>Max Points</td>
<td>Number of restore points to keep on disk. By default, Veeam Agent for Linux keeps 7 latest restore points. When the new restore point that exceeds the specified number is created, Veeam Agent for Linux will remove the earliest restore point from the backup chain.</td>
</tr>
<tr>
<td>Index</td>
<td>File system indexing options defined for the backup job.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Objects for backup</strong></td>
<td>Backup scope specified for the backup job.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig job info --name SystemBackup
Backup job
  ID: {2495911e-58db-4452-b4d1-f53dcfbc600e}
  Name: SystemBackup
  Repository ID: {4557ef7a-9c44-4f28-b8d0-44d78e5ddd5d}
  Repository name: Repository_1
  Creation time: 2017-04-06 13:29:03
  Options:
    Compression: Lz4
    Max Points: 7
    Index all mounted filesystems on the volumes selected for backup
  Objects for backup:
  Include Disk: sda1
```
Editing Backup Job Settings

If you want to change settings of the backup job, you can edit it at any time. For example, you may want to edit the backup job to add a new directory to the backup scope or change the target location.

To edit a backup job, use the following command:

For volume-level backup jobs

```
veeamconfig job edit volumelevel <option> for --name <job_name>
```

or

```
veeamconfig job edit volumelevel <option> for --id <job_id>
```

For file-level backup jobs

```
veeamconfig job edit filelevel <option> for --name <job_name>
```

or

```
veeamconfig job edit filelevel <option> for --id <job_id>
```

where:

- `<option>` — option that you want to edit for the job. You can specify one or several options at a time. To learn more about available options, see Backup Job Options.

- `<job_name>` — name of the backup job that you want to edit.

- `<job_id>` — ID of the backup job that you want to edit.

For example:

```
user@srv01:-$ veeamconfig job edit volumelevel --name SystemVolumeBackup for --name SystemVolume
```
## Backup Job Options

You can use the following options to edit parameters for the backup job:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
</table>
| **--compressionlevel** | Data compression level. Possible values are:  
  - 0 — No compression  
  - 1 — Rle  
  - 2 — Lz4  
  - 3 — ZlibLow  
  - 4 — ZlibHigh |
| **--blocksize**    | Data block size in kilobytes. Possible values are 256, 512, 1024, 4096 or 8192.  
The default value is **1024**. |
| **--maxpoints**    | Number of restore points that you want to store in the backup location. By default,  
Veeam Agent keeps 7 latest restore points. When the new restore point that exceeds  
the specified number is created, Veeam Agent will remove the earliest restore point  
from the backup chain. |
| **--prefreeze**    | Pre-freeze command that should be executed before the snapshot creation. |
| **--postthaw**     | Post-thaw command that should be executed after the snapshot creation. |
| **--objects**      | Object that should be included in backup:  
  - For simple volumes — name of a block device that represents a volume or an entire disk that should be included in backup. You can specify entire disk to create backup of the entire computer image or individual computer volumes to create backup of specific volumes. If you want to back-up several disks or volumes, specify them one after another using a ',' (comma) character as a separator.  
  - For LVM volumes — name of an LVM logical volume that should be included in backup. If you want to back-up several LVM logical volumes, specify them one after another using a ',' (comma) character as a separator.  
  This option is available for volume-level backup jobs only. |
| **--includedirs**  | Full path to a directory that should be included in backup, for example: `/home/user`.  
The option is available for file-level backup jobs only.  
  You can specify one or several paths to directories in the computer file system. To separate several paths, use a ',' (comma) character, for example: `~/home/user/Documents,~/home/user/reports`. |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td>--excludedirs</td>
<td>Full path to a directory that should be excluded from backup. The option is available for file-level backup jobs only.</td>
</tr>
<tr>
<td></td>
<td>The directory specified with this option must be a subdirectory of the directory specified with the --includedirs option. To separate several paths, use a ',' (comma) character, for example, /home/user/Documents,/home/user/reports.</td>
</tr>
<tr>
<td>--includedirs</td>
<td>Mask for file name or path that should be included in backup. The option is available for file-level backup jobs only.</td>
</tr>
<tr>
<td></td>
<td>You can use the following UNIX wildcard characters for file name masks:</td>
</tr>
<tr>
<td></td>
<td>•  '*' — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, *.pdf.</td>
</tr>
<tr>
<td></td>
<td>•  '?' — a substitution of one character in the file name or path. For example, repor?.pdf.</td>
</tr>
<tr>
<td></td>
<td>•  '[]' — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the '-' character). For example: report_201[3456].pdf or report_201[3-6].pdf.</td>
</tr>
<tr>
<td></td>
<td>To separate several masks, use a ',' (comma) character, for example, report.<em>,reports.</em>.</td>
</tr>
<tr>
<td></td>
<td>File inclusion option is applied to all directories that are specified with the --includedirs option. For example, if you include in backup the /home/user/Documents directory and files that match the repor?.pdf file name mask, Veeam Agent will back up the /home/user/Documents/report.pdf file and will not back up the /home/user/reports/report.pdf file.</td>
</tr>
<tr>
<td>Option</td>
<td>Description and values</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| **--excludemasks** | Mask for file name or path that should be excluded from backup. The option is available for file-level backup jobs only. You can use the following UNIX wildcard characters for file name masks:  
  - `'*'` — a substitution for one or more characters in the file name or path. Can be used for any sequence of characters (including no characters). For example, `.pdf`.  
  - `'?'` — a substitution of one character in the file name or path. For example, `report?.pdf`.  
  - `'[]'` — a substitution of one character in the file name or path with any of the characters enclosed in square brackets (or a range of characters defined with the `'-'` character). For example: `report_201[3456].pdf` or `report_201[3-6].pdf`.  

To separate several masks, use a `,` (comma) character, for example, `report.*,reports.*`.  

File exclusion option is applied to all directories that are specified with the **--includedirs** option and files that match file name masks specified with the **--excludemasks** option. For example, you may want to specify the following backup scope for the backup job:  
- Include in backup the `/home/user/Documents` directory  
- Include files that match the `report.*` file name mask  
- Exclude files that match the `*.odt` file name mask.  

In this case, Veeam Agent will back up the `/home/user/Documents/report.pdf` file and will not back up `/home/user/Documents/report.odt` and `/home/user/reports/report.pdf` files.  

If you want to use several name masks, you must specify them in double quotation marks, for example: `veeamconfig job create filelevel --name BackupJob1 --reponame vault13 --includedirs /home --excludemasks "*.bak,*.pdf"`. |
<p>| <strong>--indexnothing</strong> | Defines that file system indexing options are disabled for the backup job. |
| <strong>--indexall</strong> | Defines that Veeam Agent must index all files on the volumes included in backup. |
| <strong>--indexonly</strong> | Path to a directory that contains files that you want to index. Enter paths to the necessary directories. To separate several paths, use the <code>,</code> (comma) character. The option is available for volume-level backup jobs only. |
| <strong>--indexexcept</strong> | Path to a directory that contains files that you do not want to index. You can specify one or more paths. To separate several paths, use the <code>,</code> (comma) character. The option is available for volume-level backup jobs only. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--setencryption</strong></td>
<td>Defines that data encryption option is enabled for the job. You can use this option to enable encryption for the existing backup job or change a password used for encryption for the backup job. When you use the <code>veeamconfig job edit</code> command with the <code>--setencryption</code> option, Veeam Agent for Linux will prompt you to specify a password for data encryption and hint for the password.</td>
</tr>
<tr>
<td><strong>--resetencryption</strong></td>
<td>Defines that data encryption option is disabled for the job. You can use this option to disable encryption for the existing backup job.</td>
</tr>
<tr>
<td><strong>--deleteold</strong></td>
<td>The number of days to keep the backup created with the backup job in the target location. If Veeam Agent for Linux does not create new restore points for the backup, the backup will remain in the target location for the specified number of days. When this period is over, the backup will be removed from the target location. Possible values are: 1–999. If you do not specify the <code>--deleteold</code> option, Veeam Agent will not apply this setting. The backup will be stored in the target location until you delete it manually. If you specified the value earlier and want to disable this setting, specify the <code>false</code> value for this option: <code>--deleteold false</code>. After the next successful backup session, this setting will be disabled for the backup in the target location.</td>
</tr>
</tbody>
</table>
| **--nosnap** | Defines whether Veeam Agent must perform backup in the snapshot-less mode. Possible values:  
  - `true` — if you use this option, Veeam Agent will create a snapshot of the backed-up volumes during file-level backup.  
  - `false` — if you use this option, Veeam Agent will not create a snapshot of the backed-up volumes during file-level backup.  
Keep in mind that the snapshot-less file level backup does not guarantee that data in the backup is consistent. To learn more, see [Snapshot-Less File-Level Backup](#). |
NOTE

Consider the following:

- If you change the target location for the backup job, during the next backup job session Veeam Agent for Linux will perform full data backup. All subsequent backup sessions will produce incremental backups — Veeam Agent for Linux will copy only changed data to the target location and add a new incremental backup file to the backup chain.

- If you change the backup scope for the backup job, during the next backup job session Veeam Agent for Linux will create a new incremental backup. The backup will contain all data blocks pertaining to new data added to the backup scope and changed data blocks pertaining to original data in the backup scope (data that was processed by the job at the time before you changed the backup scope).

- If you enable or disable encryption for the existing backup job that has already created one or more restore points, during the next job session, Veeam Agent for Linux will create active full backup.

- Full backup takes much more time than incremental backup. If you change the target location, you can copy an existing backup chain to the new location manually. In this case, the new backup job session will produce an incremental backup file and add it to the backup chain.
Deleting Backup Job

You can delete a backup job configured in Veeam Agent for Linux. When you delete a backup job, backup files created by this job remain intact on the backup repository.

You can delete backup jobs in one of the following ways:

- With the Veeam Agent for Linux control panel
- With the Veeam Agent for Linux command line interface
Deleting Backup Job with Control Panel

You can delete a backup job with the Veeam Agent control panel.

To delete a backup job:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command.
2. Press the 'c' key to open the **Select job to configure** dialog window or the 's' key to open the **Select job to start** dialog window.
3. Select the necessary backup job in the list and press **Delete**.
4. In the displayed notification window, make sure that the **Yes** button is selected and press **Enter**.
Deleting Backup Job with Command Line Interface

You can delete a backup job with the Veeam Agent command line interface. To delete a backup job, use the following command:

```
veeamconfig job delete --name <job_name>
```

or

```
veeamconfig job delete --id <job_id>
```

where:

- `<job_name>` — name of the backup job that you want to delete.
- `<job_id>` — ID of the backup job that you want to delete.

For example:

```
$ veeamconfig job delete --name SystemBackup
```
Managing Backup Repositories

A backup repository is a storage location where Veeam Agent for Linux keeps backup files. You can use the following types of disk-based storage as a target location for a backup job:

- Local (internal) storage of the protected machine (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) or NFS share.
- Veeam Backup & Replication 11 or later backup repository.
- Veeam Backup & Replication 11 or later cloud repository.
Creating Backup Repository

Veeam Agent for Linux creates backup files in a backup repository. When you create a backup job with the Backup Job wizard, you must specify a target location for the backup. Veeam Agent will create a backup repository in the specified location and save information about this repository in the database.

**IMPORTANT**

A backup repository must be created on a separate volume from a volume whose data you plan to back up.

If you want to create backups in local directory or network shared folder, you must create a repository. To learn more, see the following sections:

- Creating a repository in a local directory
- Creating a repository in an NFS network shared folder
- Creating a repository in an SMB network shared folder

If you want to create Veeam Agent backups in a Veeam backup repository of cloud repository, you do not need to create repositories. Before configuring the backup job, you need to connect to the Veeam backup server or Veeam Cloud Connect service provider. To learn more, see the following sections:

- Connecting to Veeam Backup Server
- Connecting to Service Provider
Creating Repository in Local Directory

To create a repository in a local directory, use the following command:

```
veeamconfig repository create --name <repository_name> --location <path_to_repository>
```

where:
- `<repository_name>` — name of the repository.
- `<path_to_repository>` — path to the directory in which backup files will be stored.

For example:

```
$ veeamconfig repository create --name VeeammBackup --location /home/backups
```
Creating Repository in NFS Share

To create a repository in an NFS share, use the following command:

```bash
veeamconfig repository create --name <repository_name> --type nfs --location <path_to_repository> --options <mounting_options>
```

where:

- `<repository_name>` — name of the backup repository.
- `<path_to_repository>` — path to the network shared folder where backup files will be stored in the `SERVER:/DIRECTORY` format.
- `<mounting_options>` — additional options that Veeam Agent will use to mount the network shared folder to the Veeam Agent machine file system. You can use the standard Linux `mount` command content as mounting options. This parameter is optional.

For example:

```bash
$ veeamconfig repository create --name VeeamBackup --type nfs --location srv01:/VeeamRepository --options vers=3,hard,retry=1
```

**TIP**

If you mount a network shared folder to a directory in the Veeam Agent machine file system in advance, you can create the backup repository in the same way as in a local directory. For details, see Creating Repository in Local Directory.
Creating Repository in SMB Share

To create a repository in an SMB share, use the following command:

```bash
veeamconfig repository create --name <repository_name> --type smb --location <path_to_repository>
--username <user_name> --password --domain <domain> --options <mounting_options>
```

where:

- `<repository_name>` — name for the backup repository.
- `<path_to_repository>` — path to the network shared folder where backup files will be stored in the \SERVER\DIRECTORY format.
- `<user_name>` — account name that Veeam Agent will use to access the SMB network shared folder.
- `<domain>` — domain in which the account that has access permissions on the shared folder is registered.
- `<mounting_options>` — options that Veeam Agent will use to mount the network shared folder to the Veeam Agent machine file system. You can use the standard Linux `mount` command content as mounting options. This parameter is optional.

You can specify account name and domain for the SMB network shared folder using the `--username` and `--domain` parameters. If a password is required to access the network shared folder, you must also specify the `--password` parameter. When you run the `veeamconfig repository create` command, Veeam Agent will prompt you to type a password of the specified account.

Alternatively, you can specify account name, password and domain for the network shared folder as values for the `--options` parameter. Mind that these values will override values of the `--username`, `--password` and `--domain` parameters.
Examples

Command with --username, --password and --domain parameters:

$ veeamconfig repository create --name VeeamBackup --type smb --location //srv0 2/VeeamRepository --username Administrator --password --domain srv02

Command with --options parameter:

$ veeamconfig repository create --name VeeamBackup --type smb --location //srv0 2/VeeamRepository --options username=Administrator,password=P@ssw0rd,domain=srv02,port=666

TIP

If you mount a network shared folder to a directory in the Veeam Agent machine file system in advance, you can create the backup repository in the same way as in a local directory. For details, see Creating Repository in Local Directory.
# Viewing List of Backup Repositories

To view backup repositories configured in Veeam Agent for Linux, use the following command:

```
veeamconfig repository list
```

Veeam Agent will display a list of backup repositories.

You can view the following information about backup repositories:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the backup repository.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the backup repository.</td>
</tr>
<tr>
<td>Location</td>
<td>Directory in the local file system specified as a target location for backup files.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the backup repository. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- Local</td>
</tr>
<tr>
<td></td>
<td>- Backup server</td>
</tr>
<tr>
<td>Backup server</td>
<td>Backup server on which Veeam backup repository added to Veeam Agent is configured.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig repository list
Name          | ID                                      | Location       | Type        | Backup server |
BackupVol01    | {818e3a0f-8155-4a51-9430-248a203a43d1}  | /home/backups  | local       |              |
BackupVol02    | {2155a2e7-a1e9-4347-9d8b-cf8f3a6f3fcf}  | /home/backups2 | local       |              |
```
Editing Backup Repository

You can edit settings for a backup repository created with Veeam Agent for Linux.

You can edit the following parameters for the backup repository:

- Name of the backup repository
- Location of the backup repository

**NOTE**

Consider the following:

- If you change location for the backup repository that is already used by a backup job and contains backup files, during the next backup job run, Veeam Agent will create a new backup chain in the new repository location.
- You can temporarily change backup repository location if you want to create an ad hoc full backup in addition to the backup chain created by the backup job in the original repository location.
Changing Backup Repository Name

To change a name for the backup repository, use the following command:

```
veeamconfig repository edit --name <new_name> for --name <old_name>
```

or

```
veeamconfig repository edit --name <new_name> for --id <id>
```

where:

- `<old_name>` — current name of the backup repository.
- `<new_name>` — desired name for the backup repository.
- `<id>` — ID of the backup repository.

For example:

```
user@srv01:~$ veeamconfig repository edit --name LocalRepository for --name Repository_1
```
Changing Backup Repository Location

To change location for the backup repository, use the following command:

```
veeamconfig repository edit --location <path> for --name <name>
```

or

```
veeamconfig repository edit --location <path> for --id <id>
```

where:

- `<path>` — desired path for the backup repository.
- `<name>` — current name of the backup repository.
- `<id>` — ID of the backup repository.

For example:

```
user@srv01:~$ veeamconfig repository edit --location /home/veeam for --id 3458797-3ffe-45bc-870e-c5628643bbb3
```
Changing Backup Repository Name and Location

You can change a name and location for the backup repository at the same time, for example:

```
user@srv01:~$ veeamconfig repository edit --name LocalRepository --location /home/veeam for --name Repository_1
```
Rescanning Veeam Backup Repository

If Veeam Agent for Linux fails to display backups stored in the Veeam Backup & Replication backup repository for some reason, you can rescan the Veeam backup repository. Veeam Agent will try to reconnect to the Veeam backup server and refresh the list of backups in the backup repository.

To rescan a Veeam backup repository, use the following command:

```
veeamconfig repository rescan --id <repository_id>
```

or

```
veeamconfig repository rescan --name <repository_name>
```

where:

- `<repository_id>` — ID of the backup repository that you want to rescan.
- `<repository_name>` — name of the backup repository that you want to rescan.

For example:

```
user@srv01:~$ veeamconfig repository rescan --name [vbr01]BackupVol01
```

You can also rescan all Veeam backup repositories managed by the backup server to which Veeam Agent is connected with the following command:

```
veeamconfig repository rescan --all
```

**TIP**

With commands mentioned above, you can also rescan local backup repositories. This may be useful, for example, after information about a backup stored in the local repository is deleted from the Veeam Agent configuration database, or after you copy a backup to the local repository.
Deleting Backup Repository

You can delete a backup repository configured with Veeam Agent for Linux. When you delete a backup repository, Veeam Agent removes record of the deleted repository from its database. Backup files created by a backup job targeted at the deleted backup repository remain intact on the backup storage.

To delete a backup repository, use the following command:

```
veeamconfig repository delete --id <repository_id>
```

or

```
veeamconfig repository delete --name <repository_name>
```

where:

- `<repository_id>` — ID of the backup repository that you want to delete.
- `<repository_name>` — name of the backup repository that you want to delete.

For example:

```
user@srv01:$ veeamconfig repository delete --name Repository_1
```

**NOTE**

You cannot delete a backup repository that is specified as a backup storage location in the backup job settings.
Managing Veeam Backup & Replication Servers

You can store backup files created with Veeam Agent for Linux on backup repositories managed by Veeam Backup & Replication. To do this, you must connect to a Veeam backup server. After that, you can specify a Veeam backup repository as a target location for backup files in the properties of the backup job.
Connecting to Veeam Backup Server

To create Veeam Agent backups on a backup repository managed by Veeam Backup & Replication, you must connect to a Veeam backup server.

**IMPORTANT**
Currently, Veeam Agent for Linux can be connected to one Veeam Backup & Replication server only. If you want to create backups on the backup repository managed by another Veeam backup server, you need to delete currently used backup server and all jobs targeted at backup repositories managed by this backup server. To learn more, see Deleting Connection to Veeam Backup Server.

If you add a connection to another backup server, backup jobs targeted at the original backup server will fail, and backups created on the Veeam backup repository will become unavailable in Veeam Agent. To continue using the original backup server, you need to delete the connection to the new backup server and re-create all backup jobs that use the original backup server.

If you change an account to connect to the Veeam backup server and then start a backup job targeted at the backup repository managed by this backup server, Veeam Agent will start a new backup chain on the backup repository.

To connect Veeam Agent for Linux to a Veeam backup server, use the following command:

```
veeamconfig vbrserver add --name <vbr_name> --address <vbr_address> --port <vbr_port> --login <username> --domain <domain> --password <password>
```

where:

- `<vbr_name>` — name of the Veeam backup server that manages the backup repository.
- `<vbr_address>` — DNS name or IP address of the Veeam backup server.

**IMPORTANT**
If you specify a DNS name of the Veeam backup server, make sure that the Veeam backup server name is resolved into IPv4 address on the machine where Veeam Agent is installed. The Veeam Backup Service in Veeam Backup & Replication listens on IPv4 addresses only. If the Veeam backup server name is resolved into IPv6 address, Veeam Agent will fail to connect to the Veeam backup server.

- `<vbr_port>` — port over which Veeam Agent must communicate with Veeam Backup & Replication. The default port used for communication with the Veeam backup server is 10006.
- `<username>` — a name of the account that has access to the Veeam backup repository.
- `<domain>` — a name of the domain in which the account that has access to the Veeam backup repository is registered.
- `<password>` — password of the account that has access to the Veeam backup repository.

Permissions on the backup repository managed by the target Veeam backup server must be granted beforehand. To learn more, see Setting Up User Permissions on Backup Repositories.
For example:

```
user@srv01:~$ veeamconfig vbrserver add --name vbr01 --address 172.17.53.1 --port 10006 --login veeam --domain tech --password P@ssw0rd
```

When Veeam Agent for Linux connects to a Veeam Backup & Replication server, Veeam Agent retrieves information about backup repositories managed by this Veeam backup server and displays them in the list of available backup repositories. You can then specify a Veeam backup repository as a target for a backup job.

**TIP**

To view the list of backup repositories, use the `veeamconfig repository list` command. To learn more, see [Viewing List of Backup Repositories](#).
Viewing List of Veeam Backup Servers

To view a list of Veeam backup servers to which Veeam Agent for Linux is connected, use the following command:

```
veeamconfig vbrserver list
```

Veeam Agent will display the list of Veeam backup servers.

For the Veeam backup server in the list, Veeam Agent for Linux displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the Veeam backup server.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the Veeam backup server in the Veeam Agent database.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>IP address of the Veeam backup server and port over which Veeam Agent for Linux communicates with Veeam Backup &amp; Replication.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig vbrserver list
Name                                       ID                                      Endpoint
vbr01                                      {0fc87c11-6a8d-48c1-8aeb-7f765738796} 172.17.53.1:10006
```
Viewing Backup Server Details

You can view detailed information about the Veeam backup server to which Veeam Agent for Linux is connected. Use the following command:

```
veeamconfig vbrserver info --name <vbr_name>
```
or

```
veeamconfig vbrserver info --id <vbr_id>
```

where:

- `<vbr_name>` — name of the Veeam backup server.
- `<vbr_id>` — ID of the Veeam backup server in the Veeam Agent database.

Veeam Agent for Linux displays the following information about the Veeam backup server:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the Veeam backup server in the Veeam Agent database.</td>
</tr>
<tr>
<td>Name</td>
<td>Display name of the Veeam backup server.</td>
</tr>
<tr>
<td>Endpoint</td>
<td>IP address of the Veeam backup server and port over which Veeam Agent for Linux communicates with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>Login</td>
<td>Name of the account that has access to the Veeam backup repository.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the domain in which the account that has access to the Veeam backup repository is registered.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig vbrserver info --name vbr01
VBR server
   ID: {0fc87c11-6a8d-48c1-8aeb-7f7655738796}
   Name: vbr01
   Endpoint: 172.17.53.1:10006
   Login: veeam
   Domain: tech
```
Editing Connection to Veeam Backup Server

You can edit the following parameters for a connection to a Veeam backup server:

- **Display name of the Veeam backup server**
- **IP address and port used to connect to the Veeam backup server**
- **Account to connect to the Veeam backup server**
Changing Veeam Backup Server Name

To change a name for the Veeam backup server, use the following command:

```
veeamconfig vbrserver edit --name <new_vbr_name>
```

where:

- `<new_vbr_name>` — desired name for the backup server.

For example:

```
user@srv01:~$ veeamconfig vbrserver edit --name vbr01
```
Changing IP Address and Port for Veeam Backup Server

To change the IP address and port used to connect to the Veeam backup server, use the following command:

```
veeamconfig vbrserver edit --address <vbr_address> --port <vbr_port>
```

where:

- `<vbr_address>` — DNS name or IP address of the Veeam backup server.

**IMPORTANT**

If you specify a DNS name of the Veeam backup server, make sure that the Veeam backup server name is resolved into IPv4 address on the machine where Veeam Agent is installed. The Veeam Backup Service in Veeam Backup & Replication listens on IPv4 addresses only. If the Veeam backup server name is resolved into IPv6 address, Veeam Agent will fail to connect to the Veeam backup server.

- `<vbr_port>` — port over which Veeam Agent for Linux must communicate with Veeam Backup & Replication.

For example:

```
user@srv01:~$ veeamconfig vbrserver edit --address 172.17.53.1 --port 10006
```
Changing Account to Connect to Veeam Backup Server

NOTE
If you change an account to connect to the Veeam backup server and then start a backup job targeted at the backup repository managed by this backup server, Veeam Agent will start a new backup chain on the backup repository.

To change an account whose credentials will be used to connect to the Veeam backup server, use the following command:

```
veeamconfig vbrserver edit --login <username> --domain <domain> --password
```

where:

- `<username>` — name of the account that has access to the Veeam backup repository.
- `<domain>` — name of the domain in which the account that has access to the Veeam backup repository is registered.

When you run the command, Veeam Agent will prompt you to enter the password of the specified account.

For example:

```
user@srv01:$ veeamconfig vbrserver edit --login veeam --domain tech --password
Enter password:
```
Changing Several Backup Server Parameters

You can change several parameters for the connection to the Veeam backup server simultaneously. For example, the following command changes the name and connection settings for the Veeam backup server:

```
user@srv01:~$ veeamconfig vbrserver edit --name vbr02 --address 172.17.53.2 --port 10006
```
Updating List of Veeam Backup Repositories

When you connect to a Veeam backup server, Veeam Agent for Linux retrieves information about backup repositories managed by this Veeam backup server and displays them in the list of available backup repositories. You can refresh information about available Veeam backup repositories manually at any time. This may be useful, for example, after a new backup repository was added on the Veeam backup server.

To update the list of backup repositories managed by the Veeam backup server, use the following command:

```
veeamconfig vbrserver resync
```

**TIP**

To view updated list of available Veeam backup repositories after resync, use the `veeamconfig repository list` command. To learn more, see Viewing List of Backup Repositories.
Deleting Connection to Veeam Backup Server

You can delete a connection to the Veeam backup server to which Veeam Agent is currently connected. When you delete a connection to a Veeam backup server, Veeam Agent removes record on the deleted backup server from its database. Veeam backup repositories managed by the deleted backup server are removed from the list of available backup repositories. Backup files created by backup jobs targeted these repositories remain intact on the backup storage.

You cannot delete a connection to a Veeam backup server in the following situations:

- Veeam Agent operates in the managed mode. To delete connection to a Veeam backup server, reset Veeam Agent to the standalone mode. For details, see Resetting to Standalone Operation Mode.
- Veeam Agent has a backup job that saves backup files to a repository managed by this backup server. To remove such connection to a Veeam backup server, you first need to delete reference to the Veeam backup repository in the job settings.

To delete a connection to the Veeam backup server, use the following command:

```bash
veeamconfig vbrserver delete --name <vbr_name>
```

or

```bash
veeamconfig vbrserver delete --id <vbr_id>
```

where:

- `<vbr_name>` — name of the Veeam backup server.
- `<vbr_id>` — ID of the Veeam backup server.

For example:

```bash
user@srv01:~$ veeamconfig vbrserver delete --name vbr01
```
Managing Service Providers

You can store backup files created with Veeam Agent for Linux on a cloud repository exposed to you by a Veeam Cloud Connect service provider. To do this, you must connect to a service provider. After that, you can specify a cloud repository as a target location for backup files in the properties of the backup job.
Connecting to Service Provider

To create Veeam Agent backups on a cloud repository, you must connect to a Veeam Cloud Connect service provider.

To connect Veeam Agent for Linux to a service provider, use the following command:

```
veeamconfig cloud add --name <sp_name> --address <sp_address> --port <sp_port>
--login <username> --password <password> --fingerprint <sp_thumbprint>
```

where:

- `<sp_name>` — name of the service provider to which you want to connect.
- `<sp_address>` — IP address or full DNS name of the cloud gateway that the SP or your backup administrator has provided to you.
- `<sp_port>` — port over which Veeam Agent must communicate with the cloud gateway. The default port used for communication with the cloud gateway is 6180.
- `<username>` — name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the `TENANT/SUBTENANT` format.
- `<password>` — password of the tenant or subtenant account used to connect to the service provider.
- `<sp_thumbprint>` — thumbprint used to verify the TLS certificate that the SP has provided to you.

For example:

```
user@srv01:~$ veeamconfig cloud add --name SP --address 172.17.53.15 --port 6180 --login TechCompany/User01 --password P@ssw0rd --fingerprint 92FA988A3D9E80EE095DDAB75BF06B05DF6F205B
```

**NOTE**

When you enter the `veeamconfig cloud add` command, Veeam Agent will display information about the TLS certificate obtained from the SP. To accept the certificate, type `yes` in the command prompt and press Enter.

When Veeam Agent connects to the service provider, Veeam Agent retrieves information about cloud repositories available to the tenant or subtenant and displays them in the list of available backup repositories. You can then specify a cloud repository as a target for a backup job.

**TIP**

To view the list of available cloud repositories, use the `veeamconfig repository list` command. To learn more, see Viewing List of Backup Repositories.
Viewing List of Service Providers

To view a list of service providers to which Veeam Agent is connected, use the following command:

```
veeamconfig cloud list
```

Veeam Agent will display the list service providers.

For the service provider in the list, Veeam Agent for Linux displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the service provider.</td>
</tr>
<tr>
<td>ID</td>
<td>ID of the service provider in the Veeam Agent database.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the cloud gateway and port over which Veeam Agent communicates with the cloud gateway.</td>
</tr>
<tr>
<td>Gate servers</td>
<td>IP address of the cloud gateway and port over which Veeam Agent communicates with the cloud gateway.</td>
</tr>
<tr>
<td>Username</td>
<td>Name of the tenant or subtenant account used for connection to the service provider.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig cloud list
Name        ID                                      Address                Gate servers  Username
SP          {0840f770-354d-426a-b5ce-1aa80f56cc08}  172.17.53.15:618
            TechCompany
```
Editing Connection to Service Provider

You can edit the following parameters for a connection to a Veeam Cloud Connect service provider:

- Display name of the Veeam Cloud Connect service provider
- IP address and port used to connect to the cloud gateway
- Account to connect to the service provider
- Thumbprint to connect to the service provider
Changing SP Name

To change a name for the SP, use the following command:

```
veeamconfig cloud edit --name <new_sp_name> for --name <old_sp_name>
```

or

```
veeamconfig cloud edit --name <new_sp_name> for --id <sp_id>
```

where:

- `<old_sp_name>` — current name of the SP.
- `<new_sp_name>` — desired name for the SP.
- `<sp_id>` — ID of the SP.

For example:

```
user@srv01:~$ veeamconfig cloud edit --name SP for --id 7d3022de-4f4d-4c70-85eb-e8a946a555cd
```
Changing IP Address and Port for Cloud Gateway

To change the IP address and port of the cloud gateway provided by the SP, use the following command:

```
veeamconfig cloud edit --address <sp_address> --port <sp_port> for --name <sp_name>
```

or

```
veeamconfig cloud edit --address <sp_address> --port <sp_port> for --id <sp_id>
```

where:

- `<sp_address>` — IP address or full DNS name of the cloud gateway that the SP or your backup administrator has provided to you.
- `<sp_port>` — port over which Veeam Agent must communicate with the cloud gateway. The default port used for communication with the cloud gateway is 6180.
- `<sp_name>` — name of the SP.
- `<sp_id>` — ID of the SP.

For example:

```
user@srv01:~$ veeamconfig cloud edit --address 172.17.53.67 --port 6180 for --name SP
```
Changing Account to Connect to SP

To change an account whose credentials will be used to connect to the SP, use the following command:

```
veeamconfig cloud edit --login <username> --password <password> for --name <sp_name>
```

or

```
veeamconfig cloud edit --login <username> --password <password> for --id <sp_id>
```

where:

- `<username>` — name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the TENANT/SUBTENANT format.
- `<password>` — password of the tenant or subtenant account used to connect to the service provider.
- `<sp_name>` — name of the SP.
- `<sp_id>` — ID of the SP.

For example:

```
user@srv01:~$ veeamconfig cloud edit --login ABC_Compan/User01 --password P@ssw0rd for --name SP
```
Changing Thumbprint to Connect to SP

To change a thumbprint that will be used to connect to the SP, use the following command:

```
veeamconfig cloud edit --fingerprint <sp_thumbprint> for --name <sp_name>
```

or

```
veeamconfig cloud edit --fingerprint <sp_thumbprint> for --id <sp_id>
```

where:

- `<sp_thumbprint>` — thumbprint used to verify the TLS certificate and connect to the service provider.
- `<sp_name>` — name of the SP.
- `<sp_id>` — ID of the SP.

For example:

```
user@srv01:~$ veeamconfig cloud edit --fingerprint 92FA988A3D9E80EE095DDAB75BF06B05DF6F205B for --name SP
```
Updating List of Cloud Repositories

When you connect to the Veeam Cloud Connect service provider, Veeam Agent for Linux retrieves and saves to the database information about cloud repositories available to the tenant or subtenant whose account you use to connect to the SP. You can refresh information about available cloud repositories manually at any time. This may be useful, for example, after the SP changes backup resource settings for the tenant.

To update the list of cloud repositories, use the following command:

```
veeamconfig cloud resync
```

If the cloud repository currently used as a target location for Veeam Agent backups becomes unavailable, and Veeam Agent fails to reflect this change in its database for some reason, the `veeamconfig cloud resync` command may finish with errors. In this case, you can use the `--force` option to refresh information about available cloud repositories. For example:

```
veeamconfig cloud resync --force
```

With the `--force` option, Veeam Agent will retrieve the list of available cloud repositories from the service provider and save the new information about cloud repositories in the Veeam Agent database.

**TIP**

To view updated list of available cloud repositories after resync, use the `veeamconfig cloud list` command. To learn more, see Viewing List of Service Providers.
Deleting Connection to Service Provider

You can delete a connection to the service provider to which Veeam Agent for Linux is currently connected. When you delete a connection to a service provider, Veeam Agent removes the record on the deleted service provider from the database. Cloud repositories managed by the deleted service provider are removed from the list of available backup repositories. Backup files created by backup jobs targeted at these repositories remain intact on the cloud repository.

You cannot delete a connection to the service provider if a cloud repository managed by this service provider is used by a backup job. To remove such connection to a service provider, you first need to delete a reference to the cloud repository in the job settings.

To delete a connection to the service provider, use the following command:

```
veeamconfig cloud delete --name <sp_name>
```

or

```
veeamconfig cloud delete --id <sp_id>
```

where:

- `<sp_name>` — name of the service provider.
- `<sp_id>` — ID of the service provider.

For example:

```
user@srv01:$ veeamconfig cloud delete --name SP
```
Managing Backups

You can perform the following operations with backups created by backup jobs configured in Veeam Agent for Linux:

- View backups
- View backup details
- View restore points in backup
- Export backup to a virtual disk
- Import backup to the Veeam Agent database
- Delete backup
Viewing Backups

To view a list of backups created by Veeam Agent, use the following command:

```
veeamconfig backup list --all
```

In the list of backups, Veeam Agent displays information about all Veeam Agent for Linux backups stored in all backup repositories. If Veeam Agent is connected to a Veeam backup server, all Veeam Agent for Linux backups that are kept on Veeam backup repositories managed by this server also appear in this list.

The `--all` parameter is optional. If you do not use this option, Veeam Agent displays information about backups created by the current Veeam Agent computer only.

For security reasons, if you work with Veeam Agent connected to a Veeam backup server as a member of a protection group for pre-installed Veeam Agents, the `veeamconfig backup list --all` command will display backups created only by the current Veeam Agent computer with the current connection settings. To learn more about protection groups for pre-installed Veeam Agents, see the Protection Group Types section in the Veeam Agent Management Guide.

For each backup, Veeam Agent displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Host name of the computer on which the backup job was configured and name of the job by which the backup was created.</td>
</tr>
<tr>
<td>Backup ID</td>
<td>ID of the backup.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository in which the backup was created. Imported backups are marked as Imported in the Repository column. For information about the import procedure, see Importing Backups.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the backup creation.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup list --all
Job name       Backup ID                                       Repository
srv01 SystemBackup {45f074d2-d2d9-423d-84e9-8f1798b08d4c} Repository_
srv01 DocumentsBackup {ea64a7e5-038a-4c86-970a-6d59d4cf39d8} Repository_
srv01 HomePartitionBackup {4f75bb20-a6b6-4323-9287-1c6c8cecc86b} Repository_
wrk01 SystemBackup {951ac571-dd29-45ac-8624-79b8cc5b45863} Repository_
wrk02 SystemBackup {8d6dd39-f1b2-48b1-ac7a-84f2d6fbd167} Repository_
```

306 | Veeam Agent for Linux | User Guide
TIP

If you want to recover data from a backup that is stored in another location, for example, a backup created with another instance of Veeam Agent, you can import such backup into the Veeam Agent database on your computer. To learn more, see Importing Backups.
Viewing Backup Details

You can view detailed information about specific backup. To view backup details, use the following command:

```bash
veeamconfig backup show --id <backup_id>
```

where:

- `<backup_id>` — ID of the backup for which you want to view detailed information.

For a volume-level backup, Veeam Agent for Linux displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the volume in the backup.</td>
</tr>
<tr>
<td>Device</td>
<td>Path to the block device file that represents the volume.</td>
</tr>
<tr>
<td>FS UUID</td>
<td>File system ID.</td>
</tr>
<tr>
<td>Offset</td>
<td>Position of the volume on the computer disk.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the volume in the backup.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup show --id 4f75bb20-a6b6-4323-9287-1c6c8cecccb6b
Machine name: srv01 SystemBackup
Name: [sda1]
Device: [/dev/sda1]
FS UUID: [6945f2eb-e8bb-48fe-a276-5ba67b9030a5]
Offset: [1048576] bytes (2048 sectors)
Size: [9999220736] bytes (19529728 sectors)
```

For a file-level backup, Veeam Agent for Linux displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td>Backed up</td>
<td>Backup scope for the file-level backup job.</td>
</tr>
</tbody>
</table>
For example:

```
user@srv01:~$ veeamconfig backup show --id ea64a7e5-038a-4c86-970a-6d59d4cf3968
  Machine name: srv01 DocsBackup
    File-level backup
    Backed up:
      /home/user/Documents
```
Viewing Restore Points in Backup

To view information about restore points in the backup, you can use one of the following commands:

```
veeamconfig backup info --id <backup_id>
```

or

```
veeamconfig point list --backupid <backup_id>
```

where:

- `<backup_id>` — ID of the backup for which you want to view information on restore points.

For example:

```
user@srv01:$ veeamconfig backup info --id 4f75bb20-a6b6-4323-9287-1c6c8ceccb6b
```

or

```
user@srv01:$ veeamconfig point list --backupid 4f75bb20-a6b6-4323-9287-1c6c8ceccb6b
```

Veeam Agent for Linux displays the following information about restore points in the backup:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job name</strong></td>
<td>Name of the backup job by which the backup was created.</td>
</tr>
<tr>
<td><strong>OIB ID</strong></td>
<td>ID of the restore point in the backup.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of the restore point. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Full</td>
</tr>
<tr>
<td></td>
<td>• Increment</td>
</tr>
<tr>
<td><strong>Created at</strong></td>
<td>Date and time of the restore point creation.</td>
</tr>
<tr>
<td><strong>Is corrupt</strong></td>
<td>Indicates whether restore point in the backup is corrupted. For example, restore point is still being created or backup job failed to create a working backup. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
</tbody>
</table>
Importing Backups

You can import a backup created by Veeam Agent into the Veeam Agent database. For example, you may want to import a previously deleted backup or backup that was created in a network shared folder by Veeam Agent installed on another computer.

To import a backup:

1. Start the import process with the following command:

   ```
   veeamconfig backup import --path <path>
   ```

   where:

   `<path>` — path to the VBM file of the backup that you want to import.

   For example:

   ```
   user@srv01:~$ veeamconfig backup import --path /home/share/BackupJob/BackupJob.vbm
   Backup has been imported successfully.
   Session ID: [{4031f058-766c-4f2c-a7ae-7257adb2929f}].
   Logs stored in: [/var/log/veeam/Import/Session_{4031f058-766c-4f2c-a7ae-7257adb2929f}].
   ```

2. You can monitor the import process and result by viewing the import session log with the following command:

   ```
   veeamconfig session log --id <session_id>
   ```

   where:

   `<session_id>` — ID of the import session.

   For example:

   ```
   user@srv01:~$ veeamconfig session log --id 4031f058-766c-4f2c-a7ae-7257adb2929f
   2016-11-19 13:21:33 UTC {6ae2922d-454b-4a8d-a11b-2b5c7a85029d} [info] Importing backup
   2016-11-19 13:21:33 UTC {783f40a7-ead7-4555-9c35-545d875990ee} [info] Backup has been imported.
   ```

3. Imported backup will be displayed in the list of backups. To view the list of backups, use the following command:

   ```
   veeamconfig backup list
   ```
For example:

```bash
user@srv01:~$ veeamconfig backup list
Job name            Backup ID                               Repository
y    Created at
srv01 SystemBackup  {45f074d2-d2d9-423d-84e9-8f1798b08d4c}  Repository_ 1  2016-11-11 17:37
srv01 DocsBackup    {ea64a7e5-038a-4c86-970a-6d59d4cf3968}  Repository_ 1  2016-11-11 18:30
srv01 HomeBackup    {4f75bb20-a6b6-4323-9287-1c6c8cecc6b}  Repository_ 2  2016-11-15 11:28
BackupJob           {64957b1d-d219-456c-a9cd-9598292c10cd}  Importe  2016-11-19 19:12
```
Importing Encrypted Backups

You can import an encrypted backup created by Veeam Agent into the Veeam Agent database. This operation is required if you want to use the Veeam Agent command line interface to restore data from an encrypted backup created by Veeam Agent running on another computer.

To import an encrypted backup:

1. Start the import process with the following command:

   ```
   veeamconfig backup import --path <path>
   ```

   where:

   `<path>` — path to the VBM file of the backup that you want to import.

   For example:

   ```
   user@srv01:~$ veeamconfig backup import --path /home/share/srv15\ Backup/Backup.vbm
   ```

2. Veeam Agent will prompt you to provide a password for the backup file. Type in the password and press the **Enter** key to import the backup.

   Veeam Agent displays a hint for the password that was used to encrypt the backup file. Use the hint to recall the password.

   If you enter the correct password, Veeam Agent will decrypt the backup file and import it into the database.

   ```
   user@srv01:~$ veeamconfig backup import --path /home/share/srv15\ Backup/Backup.vbm
   [Info] Backup srv15 Backup encrypted
   [Info] Press "Enter" to skip. Enter password to decrypt the backup:
   [Info] Hint: Standard password
   Password: Backup imported successfully
   ```

3. Imported backup will be displayed in the list of backups. To view the list of backups, use the following command:

   ```
   veeamconfig backup list
   ```

   For example:

   ```
   user@srv01:~$ veeamconfig backup list
   Job name            Backup ID                               Repositor      Created at
   srv15 Backup        {4b1f873c-857d-b984-4f22-6ce66bf62570}  Imported      2018-06-12 20:20
   srv01 ServerBackup  {f212f641-54aa-40de-a0eb-8727be56760b}  Imported      2018-06-12 20:04
   ```
Deleting Backups

Backup files created with Veeam Agent are removed automatically according to the retention policy settings. You can also remove backups from the target location and/or Veeam Agent configuration database manually if necessary.
Removing Backup from Configuration

To remove a backup from the Veeam Agent configuration database, use the following command:

```bash
veeamconfig backup delete --id <backup_id>
```

where `<backup_id>` is an ID of the backup that you want to delete.

The way Veeam Agent removes a backup from configuration depends on the backup location:

- If the backup resides in a local directory or network shared folder, Veeam Agent removes records about the deleted backup from the Veeam Agent database. Backup files themselves (VBK, VIB, VBM) remain in the backup repository.

  You can import information about the removed backup later to Veeam Agent and perform restore operations with the imported backup. To import information about the removed backup, use the `veeamconfig repository rescan --all` command.

- If the backup resides in a Veeam Backup & Replication repository, Veeam Agent removes records about the deleted backup from the Veeam Agent database and Veeam Backup & Replication database. Backup files themselves (VBK, VIB, VBM) remain in the backup repository.

  If you want to import information about the removed backup later to Veeam Agent and perform restore operations with this backup, you must contact backup administrator working with Veeam Backup & Replication. The administrator must rescan the backup repository that contained the backup in the Veeam Backup & Replication console. For details, see the Rescanning Backup Repositories section in the Veeam Backup & Replication User Guide.

  After rescan, the backup will be displayed in the list of backups on the Veeam Agent machine connected to the Veeam backup server.
Deleting Backup Files

To delete backup files from the target location and Veeam Agent database, use the following command:

```
veeamconfig backup delete --id <backup_id> --purge
```

where `<backup_id>` is an ID of the backup that you want to delete.

Veeam Agent for Linux will remove records about the deleted backup from the Veeam Agent database and, additionally, delete backup files themselves from the destination storage.
Performing Restore

If you experience a problem with your computer, your data gets lost or corrupted, you can use one of the following options to recover your data or bring the computer back to work:

- **Restore from the Veeam Recovery Media**
  - Restore volumes
  - Restore files and folders
- **Restore volumes with the command line interface**
- **Restore files and folders:**
  - Restore files and folders with the File Level Restore wizard
  - Restore files and folders with the command line interface
- **Export data as VHD disks**
- **Restore data from encrypted backups**
Restoring from Veeam Recovery Media

If the OS on your computer fails to start, you can use the Veeam Recovery Media to recover your computer. The Veeam Recovery Media will help you boot the computer in the limited mode. After booting, you can use a backup created with Veeam Agent for Linux to restore the whole system image of your computer, specific volumes on your computer or specific files and folders. You can also use standard Linux command line utilities to diagnose problems and fix errors.

IMPORTANT

If you plan to use the custom Veeam Recovery Media, Veeam Agent requires 3 GB RAM or more installed on the target computer or virtual machine. Memory consumption varies depending on size and number of modules included into the recovery media. To learn more, see Creating Custom Veeam Recovery Media.
Restoring Volumes

You can restore a specific computer volume or all volumes from the volume-level backup.

Volumes can be restored to their original location or to a new location.

- If you restore a volume to its original location, Veeam Agent will overwrite the data on the original volume with the data restored from the backup.
- If you restore volume data to a new location, Veeam Agent will restore data from the backup and write it to the selected destination. If necessary, you can specify new disk mapping settings for the restored volume.
Before You Begin

Before you boot from the recovery image and recover your data, check the following prerequisites and limitations:

- You must have a recovery image on any type of media: CD/DVD/BD or removable storage device.
- To recover data on your computer, you must have both the Veeam Recovery Media and data backup. For volume-level restore, you can use a volume-level backup created with Veeam Agent for Linux. Make sure that the backup or system image is available on the computer drive (local or external), on a network shared folder or on the backup repository managed by a Veeam backup server.
- The media type on which you have created the recovery image must be set as a primary boot source on your computer.
- The volume-level backup from which you plan to restore data must be successfully created at least once.
- [For backups stored in network shared folders, on Veeam backup repositories and Veeam Cloud Connect repositories] You must have access to the target location where the backup file resides.
- [For Veeam backup repository targets] If you plan to restore data from a backup stored on a Veeam backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.
- You cannot restore a volume to the volume where the backup file that you use for restore is located.
- Veeam Recovery Media 3.0 and later versions do not support Oracle VM virtual machines. Use an earlier version of Veeam Recovery Media or contact Veeam Customer Support for workarounds.
Step 1. Boot from Veeam Recovery Media

To boot from the Veeam Recovery Media:

1. [For CD/DVD/BD] Power on your computer. Insert the media with the recovery image to the drive and power off the computer.
   
   [For removable storage device] Attach the removable storage device with the recovery image to your computer.

2. Start your computer.

3. [For regular recovery image] In the boot menu, select what Linux kernel version to use to boot your computer and specify boot options if necessary.

   You can select a Linux kernel version if you use generic Veeam Recovery Media downloaded from the Veeam website or Veeam software repository. If you created a custom Veeam Recovery Media, you will be prompted to boot using the Linux kernel of your Veeam Agent computer included in the recovery image.

   To specify boot options, press the **Tab** key and type the necessary options in the command prompt.

   **NOTE**

   For the legacy recovery image, the boot menu is unavailable. After you start your computer, Veeam Agent will immediately start loading files from the Veeam Recovery Media.

4. Wait for Veeam Agent to load files from the Veeam Recovery Media.
5. After the recovery image OS has loaded, choose whether you want to start the SSH server. The SSH server allows you to connect to the Veeam Recovery Media from a remote machine.

The Veeam Recovery Media starts the SSH server automatically after a time-out. The default value for the time-out is 60 seconds.

If you do not want to start the SSH server, make sure that the **Proceed without SSH** button is selected and press **Enter**. You will proceed immediately to the step 7.
6. After the SSH server has started, review settings to connect to the Veeam Recovery Media and press Enter.

The Veeam Recovery Media displays the following connection settings:

- IP address of the computer booted from the Veeam Recovery Media
- User name and password of the account used to connect to the Veeam Recovery Media
- Fingerprints of the computer booted from the Veeam Recovery Media

**NOTE**

The user name of the account used to work with the Veeam Recovery Media depends on the recovery image version:

- `veeamuser` — for the regular recovery image
- `root` — for the legacy recovery image

If you want to use command-line utilities built in the regular recovery image, use the `sudo` command to provide the `veeamuser` account with privileges of the `root` account.
7. Accept the terms of the product license agreement and license agreements for third-party components of the product:
   a. Make sure that the I accept Veeam End User Software License Agreement option is selected and press Space.
   b. Select the I accept the terms of the following 3rd party software components license agreements option with the Tab key and press Space.
   c. Switch to the Continue button with the Tab key and press Enter.

8. Make sure that network settings are specified correctly and configure the network adapter if necessary. To learn more, see Configure Network Settings.
9. Choose the necessary recovery option. Veeam Agent offers the following tools:
   - **Restore volumes** — the Veeam Recovery wizard to recover data on the original computer or perform bare metal recovery.
   - **Restore files** — the File Level Restore wizard to restore files and folders to the original location or to a new location.
   - **Exit to shell** — Linux shell prompt with standard utilities to diagnose problems and fix errors.

**TIP**
To stop working with the Veeam Recovery Media and shut down or restart your computer, in the Veeam Recovery Media main menu, select the **Reboot** or **Shutdown** option and press **Enter**.

```
MAIN MENU
Restore volumes
Restore files
Configure network
Exit to shell
Reboot
Shutdown
```

Enter: Select
Up/Down: Navigate
Step 2. Configure Network Settings

To open the **Network settings** dialog, in the Veeam Recovery Media main menu, select the **Configure network** option and press **Enter**.

Veeam Agent for Linux will display network adapters that are available on the system. If there is a DHCP server in your network, Veeam Agent will configure the network settings automatically and display the IP address assigned to the network adapter. You can then press **Esc** to return to the Veeam Recovery Media main menu and launch the Volume Restore wizard.

You can manually configure TPC/IP v4 settings for network adapters if necessary. To learn more, see **Specifying Network Settings**.

![Select network adapter dialog]

Choose adapter

```
eth0  00:50:56:91:0f:4d - 172.17.53.18
```
Specifying Network Settings

You can manually configure TPC/IP v4 settings for the network adapter. To configure network settings:

1. In the Choose adapter list, select the network adapter that you want to use to connect to the network shared folder or Veeam backup repository where the backup resides and press Enter.

2. In the Configure adapter dialog, select the Manual option and press Enter.

3. In the Adapter settings dialog, specify the following network settings:
   - IP address
   - Subnet mask
   - Default gateway
   - DNS server

4. Select the Apply button and press Enter.

If there is a DHCP server in your network, you can return to automatic IP addressing:

1. In the Choose adapter list, select the necessary network adapter and press Enter.

2. In the Configure adapter dialog, select the Auto option and press Enter. Veeam Agent will automatically configure network settings for the adapter.
Step 3. Launch Volume Restore Wizard

To launch the volume restore wizard, in the Veeam Recovery Media main menu, select Restore volumes and press Enter.

![Veeam Recovery Media Menu](image)

- Restore volumes
- Restore files
- Configure network
- Switch to command line
- Reboot
- Shutdown
Step 4. Select Backup Location

At the **Select backup location** step of the wizard, specify where the backup file that you want to use for data recovery is located.

To recover data from backup, you need to mount the backup storage on which the backup file resides to the recovery image OS file system. Veeam Agent for Linux automatically mounts external USB drives that are connected to the computer and displays them in the list of available backup locations. You can select the necessary device and press **Enter** to pass to the **Browse for backup files** step of the wizard.

If the backup file is located in a network shared folder, on a local drive or on a Veeam backup repository, select one of the following options:

- **Add shared folder** — select this option if the backup file is located in a network shared folder. With this option selected, you will pass to the **Mount shared folder** step of the wizard.

- **Mount local disk** — select this option if the backup file resides on the local computer drive, external drive or removable storage device that is currently connected to your computer. With this option selected, you will pass to the **Select local disk** step of the wizard.

- **Add VBR server** — select this option if the backup file resides on a backup repository managed by the Veeam backup server. With this option selected, you will pass to the **Specify backup server parameters** step of the wizard.

- **Add Cloud provider** — select this option if the backup file resides on a cloud repository exposed to you by a Veeam Cloud Connect service provider. With this option selected, you will pass to the **Specify Cloud provider parameters** step of the wizard.
Step 5. Specify Backup Location Settings

Specify settings for the target storage that contains a backup file from which you plan to restore data:

- **Specify shared folder settings** — if you have selected the Add shared folder option at the Select backup location step of the wizard.

- **Select local drive** — if you have selected the Mount local disk option at the Select backup location step of the wizard.

- **Specify Veeam backup repository settings** — if you have selected the Add VBR server option at the Select backup location step of the wizard.

- **Specify Veeam Cloud Connect repository settings** — if you have selected the Add Cloud provider option at the Select backup location step of the wizard.
Specifying Shared Folder Settings

The **Mount shared folder** step of the wizard is available if you have selected to restore data from a backup file located in a network shared folder.

Specify settings for the network shared folder:

1. Select the type of a network shared folder:
   - **NFS** — to connect to a network shared folder using the NFS protocol.
   - **SMB** — to connect to a network shared folder using the SMB (CIFS) protocol.
2. In the **Path** field, specify the network shared folder name in the `SERVER/DIRECTORY` format: type an IP address or domain name of the server and the name of the network shared folder in which the backup file resides.
3. [For SMB network shared folder] In the **Domain** field, type a name of the domain in which the account that has access permissions on the shared folder is registered, for example: `DOMAIN`.
4. [For SMB network shared folder] In the **Username** field, type a name of the account that has access permissions on the shared folder.
5. [For SMB network shared folder] In the **Password** field, type a password of the account that has access permissions on the shared folder.
6. Press **Enter** to connect to the network shared folder. Veeam Agent will mount the specified network shared folder to the `/media` directory of the recovery image OS file system and display content of the network shared folder.
TIP

You can mount several network shared folders to work with backup files that are stored in different locations if needed. To do this, return to the Select Backup Location step of the wizard and select the Add shared folder option once again. For every mounted location, Veeam Agent displays its name, type and mount point. You can view the list of mounted network shared folders and browse for a backup file located on the necessary storage.

![Mount Shared Folder Dialog Box](image-url)
Selecting Local Drive

The Select local disk step of the wizard is available if you have selected to restore data from a backup file located on a computer drive.

In the list of devices, select the necessary disk or disk partition and press Enter. Veeam Agent will mount the selected device to the /media directory of the recovery image OS file system and display content of the directory.

**TIP**

You can mount several devices to work with backup files that are stored in different locations if needed. To do this, return to the Select Backup Location step of the wizard and select the Mount local disk option once again. For every mounted location, Veeam Agent displays its name, type and mount point. You can view the list of mounted devices and browse for a backup file located on the necessary storage.

<table>
<thead>
<tr>
<th>Device</th>
<th>Size</th>
<th>Filesystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>sda1</td>
<td>9.31G</td>
<td>ext4</td>
</tr>
<tr>
<td>sda6</td>
<td>38.00G</td>
<td>ext4</td>
</tr>
<tr>
<td>sr0</td>
<td>108.0M</td>
<td>iso9660</td>
</tr>
</tbody>
</table>

Veeam Recovery Media
Specifying Backup Server Settings

The **Specify Backup Server parameters** step of the wizard is available if you have selected to restore data from a backup repository managed by the Veeam backup server.

Specify settings for the Veeam backup server that manages the backup repository where the backup file resides:

1. In the **Address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify a number of the port over which Veeam Agent must communicate with the backup repository. By default, Veeam Agent uses port 10006.
3. In the **Login** field, type a name of the account that has access to the Veeam backup repository.
4. In the **Domain** field, type a name of the domain in which the account that has access to the Veeam backup repository is registered, for example: **DOMAIN**.
5. In the **Password** field, type a password of the account that has access to the Veeam backup repository.
6. Press **Enter**. Veeam Agent will connect to the Veeam backup server, and you will pass immediately to the **Backup** step of the wizard.

![Specify Backup Server parameters dialog box](image)
Specifying Service Provider Settings

If you have selected to restore data from a backup file located on a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

1. Specify service provider settings.
2. Verify the TLS certificate.
3. Specify user account settings.
Specifying Service Provider Settings

The **Specify Cloud provider parameters** step of the wizard is available if you have selected to restore data from a cloud repository exposed to you by a Veeam Cloud Connect service provider.

Specify service provider settings that the SP or your backup administrator has provided to you:

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the cloud gateway.
2. In the **Port** field, specify the port over which Veeam Agent will communicate with the cloud gateway. By default, port 6180 is used.
3. Press **Enter**. Veeam Agent will connect to the service provider and display the Certificate details window.
Verifying TLS Certificate

In the Certificate details window, review information about the TLS certificate obtained from the SP side and verify the TLS certificate.

- To accept the TLS certificate, select the Accept button with the Tab key and press Enter.
- [Optional] To verify the TLS certificate with a thumbprint, do the following:
  a. Select the Verify thumbprint button with the Tab key and press Enter.
  b. In the Thumbprint verification field, enter the thumbprint that you obtained from the SP.
  c. Switch to the Verify button and press Enter. Veeam Agent will check if the thumbprint that you entered matches the thumbprint of the obtained TLS certificate.

TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.
Specifying User Account Settings

The **Specify Cloud provider credentials** step of the wizard is available if you have chosen to restore data from a cloud repository and specified settings for the cloud gateway.

1. In the **Username** field, enter the name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the `TENANT\SUBTENANT` format.

2. In the **Password** field, provide a password for the tenant or subtenant account.

3. Press **Enter**. Veeam Agent will connect to the cloud repository, and you will pass immediately to the **Backup** step of the wizard.
Step 6. Browse for Backup File

At the **Browse for backup files** step of the wizard, select the backup file that you plan to use for volume-level restore:

1. In the file system tree, select a directory in which the backup file you plan to use for restore resides:
   - Use **Up** and **Down** arrow keys to select a directory.
   - Use the **Enter** key to open the necessary directory.

2. In the directory where the backup file resides, select the backup file and press **Enter**.

![Backup File Browser]
Step 7. Select Backup and Restore Point

At the Backup step of the wizard, select a backup and restore point from which you want to recover data.

The Backup step window comprises two panes:

- The Imported backups pane on the left displays information about backup: host name of the computer whose data is stored in the backup file, backup job name and number of restore points.
- The Restore points pane on the right displays a list of restore points in the backup.

To select backup and restore point:

1. In the Imported backups pane, ensure that the backup from which you want to recover data is selected and press Enter.

   If you want to select another backup, press the 'i' key and browse for the necessary backup file. To learn more, see Locate Backup File.

2. In the Restore points pane, select with Up and Down keys the restore point from which you want to recover data and press Enter.
NOTE

If you selected an encrypted backup for data restore, Veeam Agent will prompt you to provide a password to unlock the encrypted file. To learn more, see Restoring Data from Encrypted Backups.

<table>
<thead>
<tr>
<th>IMPORTED BACKUPS</th>
<th>RESTORE POINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Hostname</td>
</tr>
<tr>
<td>SystemBackup</td>
<td>srv42</td>
</tr>
<tr>
<td>Show all...</td>
<td></td>
</tr>
</tbody>
</table>
Step 8. Map Restored Disks

At the Disk Mapping step of the wizard, select what volumes you want to restore and map volumes from the backup to volumes on your computer.

**IMPORTANT**

It is strongly recommended that you change disk mapping settings only if you have experience in working with Linux disks and partitions. If you make a mistake, your computer data may get corrupted.

You can map volumes in the backup (source volumes) and volumes on your computer (target volumes) in one of the following ways:

- Map a source volume to a target volume
- Map a target volume to a source volume

As well as individual volumes, you can also map entire disks:

- Map a source disk to a target disk
- Map a target disk to a source disk

If you choose to restore an entire disk, Veeam Agent will try to map all volumes that reside on this disk.

If you want to restore Btrfs subvolumes, you must map subvolumes in the backup to a Btrfs pool on the Veeam Agent computer. To learn more, see Mapping Btrfs Subvolumes.
Mapping Source Volume to Target Volume

The In backup pane of the Veeam Recovery Media wizard contains a list of disks and volumes in the backup. You can select volumes in the backup that you want to restore to your computer and specify mapping rules for these volumes.

To map a source volume to a target volume:

1. In the In backup pane, select a volume in the backup whose data you want to recover and press Enter.

2. Veeam Agent for Linux will display a window with information on the selected volume (partition type, file system type, mount point and volume size) and a list of available operations:
   - Restore volume to
   - Close

   Select this option if you want to restore the selected volume to your computer.
   Select this option if you want to close the window and select another volume.
3. Select the **Restore volume to** option and press **Enter**.

4. Veeam Agent for Linux will display a list of volumes on your computer. Select the volume that you want to restore and press **Enter**.
5. In the **Current system** pane, in the **Restore** column, Veeam Agent will display which volume from backup will be restored to the target volume.

<table>
<thead>
<tr>
<th>Device</th>
<th>Size</th>
<th>Restore</th>
</tr>
</thead>
<tbody>
<tr>
<td>/boot</td>
<td>60.0G</td>
<td></td>
</tr>
<tr>
<td>/</td>
<td>10.0G</td>
<td></td>
</tr>
<tr>
<td>/var</td>
<td>10.0G</td>
<td></td>
</tr>
<tr>
<td>/dev</td>
<td>10.0G</td>
<td></td>
</tr>
<tr>
<td>/mnt</td>
<td>10.0G</td>
<td></td>
</tr>
<tr>
<td>/tmp</td>
<td>10.0G</td>
<td></td>
</tr>
<tr>
<td>/dev</td>
<td>10.0G</td>
<td></td>
</tr>
</tbody>
</table>

6. Repeat steps 1–5 for all volumes that you want to restore.

7. Press ‘s’ to start the restore process.
Mapping Target Volume to Source Volume

The **Current system** pane of the **Veeam Recovery Media** wizard displays a partition table of your computer booted from the Veeam Recovery Media. In this pane, you can select volumes on your computer which you want to restore and specify mapping rules for these volumes. If necessary, you can edit the disk layout before restoring volumes.

To map a target volume to a source volume:

1. In the **Current system** pane, select a volume on your computer whose data you want to recover and press **Enter**.

2. Veeam Agent for Linux will display a window with information on the selected volume (partition type, file system type, mount point and volume size) and a list of available operations:
   - **Restore volume from** — select this option if you want to recover the selected volume from the backup.
   - **Delete partition** [for simple volumes] or **Delete volume** [for LVM volumes] — select this option if you want to change the disk layout before restoring a volume. After you delete a partition or volume, you will be able to create a new partition or volume of the desired size and map a volume in the backup to the volume on your computer.
   - **Create LVM physical volume** — select this option if you want to create an LVM physical volume on the selected disk partition. In the created physical volume, you will be able to create a volume group and restore to this volume group LVM logical volumes from the backup.
   - **Close** — select this option if you want to close the window and select another volume.
3. Select the **Restore volume from** option and press **Enter**.

4. Veeam Agent for Linux will display a window with a list of volumes in the backup. Select the volume that you want to restore and press **Enter**.
5. In the **Current system** pane, in the **Restore** column, Veeam Agent will display which volume from backup will be restored to the target volume.

6. Repeat steps 1–5 for all volumes that you want to restore.

7. Press ‘s’ to start the restore process.
Mapping Source Disk to Target Disk

The **In backup** pane of the Veeam Recovery Media wizard contains a list of disks and volumes in the backup. As well as individual volumes, you can select for restore entire computer disks.

To map a source disk to a target disk:

1. In the **In backup** pane, select a disk in the backup volumes on which you want to recover and press **Enter**.

2. Veeam Agent for Linux will display a window with information on the selected disk (partition table type, bootloader type and disk size) and a list of available operations:
   - **Restore whole disk to** — select this option if you want to restore all volumes on the selected disk in the backup to your computer.
   - **Restore bootloader to** — select this option if you want to restore a bootloader from the disk in the backup to your computer.
   - **Close** — select this option if you want to close the window and select another disk or volume.
3. To restore volumes that reside on the selected disk, select the **Restore whole disk to** option and press \textbf{Enter}.

![Image of Veeam Recovery Media window showing disk selection]

4. Veeam Agent for Linux will display a list of disks and volumes on your computer. Select the disk whose volumes you want to restore and press \textbf{Enter}.

![Image of Veeam Recovery Media window showing volume selection]
5. In the **Current system** pane, in the **Restore** column, Veeam Agent will display which volumes from the disk in the backup will be restored to the target disk.

6. Repeat steps 1–5 for all computer disks whose volumes you want to restore.

7. Press ‘s’ to start the restore process.
Mapping Target Disk to Source Disk

The **Current system** pane of the **Veeam Recovery Media** wizard displays a partition table of your computer booted from the Veeam Recovery Media. As well as individual volumes, you can select for restore entire computer disks. If necessary, you can edit the disk layout before restoring volumes.

To map a target disk to a source disk:

1. In the **Current system** pane, select a disk on your computer to which you want to restore volumes and press **Enter**.

2. Veeam Agent for Linux will display a window with information on the selected disk (partition table type, bootloader type and disk size) and a list of available operations:
   - **Restore whole disk from** — select this option if you want to restore to the selected disk all volumes from a disk in the backup.
   - **Restore bootloader from** — select this option if you want to restore to the selected disk a bootloader from a disk in the backup.
   - **Delete partition table** — select this option if you want to change the disk layout before restoring volumes. After you delete a partition table, you will be able to create a new partition table, create disk partitions and volumes of the desired size, and map volumes in the backup to volumes on your computer.
   - **Close** — select this option if you want to close the window and select another disk or volume.
3. To restore volumes to the selected disk, select the **Restore whole disk from** option and press **Enter**.

4. Veeam Agent for Linux will display a list of disks and volumes in the backup. Select the disk whose volumes you want to restore and press **Enter**.
5. In the **Current system** pane, in the **Restore** column, Veeam Agent will display which volumes from the disk in the backup will be restored to the target disk.

<table>
<thead>
<tr>
<th>CURRENT SYSTEM</th>
<th>IN BACKUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Restore</td>
</tr>
<tr>
<td>sda (boot)</td>
<td>sda1 (/)</td>
</tr>
<tr>
<td>sda2</td>
<td>sda2 (/home)</td>
</tr>
<tr>
<td>sda3</td>
<td>sda3 (swap)</td>
</tr>
<tr>
<td>sdb (boot)</td>
<td>10.06G</td>
</tr>
<tr>
<td>sdb1 (lun)</td>
<td>10.06G</td>
</tr>
<tr>
<td>vg</td>
<td>10.06G</td>
</tr>
<tr>
<td>lv1</td>
<td>5.006G</td>
</tr>
<tr>
<td>lv2</td>
<td>5.006G</td>
</tr>
</tbody>
</table>

6. Repeat steps 1-5 for all disks whose volumes you want to restore.

7. Press ‘s’ to start the restore process.
Mapping Btrfs Subvolumes

If the backup contains Btrfs file system data, in the In backup pane of the Veeam Recovery Media wizard, Veeam Agent displays the list of backed-up Btrfs subvolumes. Information about the original Btrfs pool that contained these subvolumes is not included in the backup.

You can restore from the backup all Btrfs subvolumes or selected subvolumes. To restore a subvolume, you must specify a target Btrfs pool — a Btrfs pool on the computer where you perform restore using the Veeam Recovery Media.

You can restore Btrfs subvolumes to the original Btrfs pool or new Btrfs pool. If the target Btrfs pool contains a subvolume with the same name as the name of the subvolume that you selected for restore, Veeam Agent will automatically map these subvolumes. During the restore process, Veeam Agent will overwrite data on the target subvolume with the data retrieved from the backup.

NOTE

Veeam Agent for Linux does not check whether the target Btrfs pool has enough disk space to restore the selected subvolumes. If the total size of the restored data is larger than the size of the target Btrfs pool, after the restore process completes, the restored data will be corrupted.

To map a source Btrfs subvolume to a target Btrfs pool:

1. In the In backup pane, select a subvolume in the backup whose data you want to restore and press Enter.

You can also choose to restore all subvolumes from the backup at once. To do this, in the In backup pane, select btrfs and press Enter.
2. In the displayed window, select the necessary option for Btrfs restore and press **Enter**. The available options depend on what Btrfs subvolumes you selected for restore: all subvolumes or specific subvolume.

   - **Restore subvolume to** — this option is available if you chose to restore a specific Btrfs subvolume from the backup. Select this option to restore the selected subvolume to your computer.

   - **Restore btrfs to** — this option is available if you chose to restore all Btrfs subvolumes from the backup. Select this option to restore subvolumes to your computer.

   - **Close** — select this option if you want to close the window and select another subvolume.

3. Veeam Agent for Linux will display a list of Btrfs pools on your computer. Select the Btrfs pool where you want to restore data from the backup and press **Enter**.
4. In the **Current system** pane, in the **Restore** column, Veeam Agent for Linux will display which subvolume from backup will be restored to the target Btrfs pool.

```
+-----------------+-----------------+-------------+
<table>
<thead>
<tr>
<th>Device</th>
<th>Restore</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>sda (boot)</td>
<td></td>
<td>60.00G</td>
</tr>
<tr>
<td>sda1</td>
<td></td>
<td>10.03G</td>
</tr>
<tr>
<td>sda2</td>
<td></td>
<td>30.31G</td>
</tr>
<tr>
<td>sda3</td>
<td></td>
<td>3.066G</td>
</tr>
<tr>
<td>sdb</td>
<td></td>
<td>10.00G</td>
</tr>
<tr>
<td>sdb1 (lvm)</td>
<td></td>
<td>10.00G</td>
</tr>
<tr>
<td>sdc</td>
<td></td>
<td>30.00G</td>
</tr>
<tr>
<td>sdc1 (btrfs)</td>
<td></td>
<td>10.00G</td>
</tr>
<tr>
<td>sdc2 (btrfs)</td>
<td></td>
<td>10.00G</td>
</tr>
<tr>
<td>sdc3 (btrfs)</td>
<td></td>
<td>10.00G</td>
</tr>
<tr>
<td>vg</td>
<td></td>
<td>10.00G</td>
</tr>
<tr>
<td>lv1</td>
<td></td>
<td>5.006</td>
</tr>
<tr>
<td>lv2</td>
<td></td>
<td>5.006</td>
</tr>
<tr>
<td>btrfs_pool</td>
<td></td>
<td>30.00G</td>
</tr>
<tr>
<td>/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/sub1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/sub2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

5. If you want to restore more than one subvolume, repeat steps 1-4 for all subvolumes that you want to restore.

6. Press ‘s’ to start the restore process.
Step 9. Complete Restore Process

At the **Recovery summary** step of the wizard, complete the procedure of volume-level restore.

1. Review the specified recovery settings.

2. Press **Enter** to start the volume-level restore process. Veeam Agent for Linux will perform partition reallocation operations if necessary, restore the necessary data from the backup and overwrite data on your computer with it.
Step 10. Finish Working with Veeam Recovery Media

When the restore operation completes, finish working with the Veeam Recovery Media and start your operating system.

1. Press **Esc** to return to the Veeam Recovery Media main menu.
2. Eject the media or removable storage device with the recovery image.
3. In the Veeam Recovery Media main menu, select the **Reboot** option and press **Enter**.
4. Wait for your Linux operating system to start.
Restoring Files and Folders

If some files and folders on your computer get lost or corrupted, you can restore them from backups. For file-level restore, you can use backups of any type:

- Volume-level backups (backups of the entire computer or specific volumes)
- File-level backups

When you perform file-level restore with the Veeam Recovery Media, Veeam Agent publishes the backup content directly into the recovery image OS file system and displays it in the file browser. You can restore files and folders to their initial location or copy files and folders to a new location.
Before You Begin

Before you boot from the recovery image and recover your data, check the following prerequisites:

- You must have a recovery image on any type of media: CD/DVD/BD or removable storage device.
- To recover data on your computer, you must have both the Veeam Recovery Media and data backup. For data recovery, you can use a volume-level or file-level backup created with Veeam Agent for Linux. Make sure that the backup or system image is available on the computer drive (local or external), on a network shared folder or on the backup repository managed by a Veeam backup server.
- The media type on which you have created the recovery image must be set as a primary boot source on your computer.
- The backup from which you plan to restore data must be successfully created at least once.
- [For backups stored in network shared folders, on Veeam backup repositories and Veeam Cloud Connect repositories] You must have access to the target location where the backup file resides.
- [For Veeam backup repository targets] If you plan to restore data from a backup stored on a Veeam backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.
- Veeam Recovery Media 3.0 and later versions do not support Oracle VM virtual machines. Use an earlier version of Veeam Recovery Media or contact Veeam Customer Support for workarounds.
Step 1. Boot from Veeam Recovery Media

To boot from the Veeam Recovery Media:

1. [For CD/DVD/BD] Power on your computer. Insert the media with the recovery image to the drive and power off the computer.
   [For removable storage device] Attach the removable storage device with the recovery image to your computer.

2. Start your computer.

3. [For regular recovery image] In the boot menu, select what Linux kernel version to use to boot your computer and specify boot options if necessary.

   You can select a Linux kernel version if you use generic Veeam Recovery Media downloaded from the Veeam website or Veeam software repository. If you created a custom Veeam Recovery Media, you will be prompted to boot using the Linux kernel of your Veeam Agent computer included in the recovery image.

   To specify boot options, press the Tab key and type the necessary options in the command prompt.

   **NOTE**
   
   For the legacy recovery image, the boot menu is unavailable. After you start your computer, Veeam Agent will immediately start loading files from the Veeam Recovery Media.

4. Wait for Veeam Agent to load files from the Veeam Recovery Media.
5. After the recovery image OS has loaded, choose whether you want to start the SSH server. The SSH server allows you to connect to the Veeam Recovery Media from a remote machine.

The Veeam Recovery Media starts the SSH server automatically after a time-out. The default value for the time-out is 60 seconds.

If you do not want to start the SSH server, make sure that the **Proceed without SSH** button is selected and press **Enter**. You will proceed immediately to the step 7.
6. After the SSH server has started, review settings to connect to the Veeam Recovery Media and press Enter.

   The Veeam Recovery Media displays the following connection settings:
   - IP address of the computer booted from the Veeam Recovery Media
   - User name and password of the account used to connect to the Veeam Recovery Media
   - Fingerprints of the computer booted from the Veeam Recovery Media

   **NOTE**

   The user name of the account used to work with the Veeam Recovery Media depends on the recovery image version:
   - `veeamuser` — for the regular recovery image
   - `root` — for the legacy recovery image

   If you want to use command-line utilities built in the regular recovery image, use the `sudo` command to provide the `veeamuser` account with privileges of the `root` account.
7. Accept the terms of the product license agreement and license agreements for third-party components of the product:
   
a. Make sure that the I accept Veeam End User Software License Agreement option is selected and press Space.

b. Select the I accept the terms of the following 3rd party software components license agreements option with the Tab key and press Space.

c. Switch to the Continue button with the Tab key and press Enter.

8. Make sure that network settings are specified correctly and configure the network adapter if necessary. To learn more, see Configure Network Settings.
9. Choose the necessary recovery option. Veeam Agent offers the following tools:

- **Restore volumes** — the Veeam Recovery wizard to recover data on the original computer or perform bare metal recovery.

- **Restore files** — the File Level Restore wizard to restore files and folders to the original location or to a new location.

- **Exit to shell** — Linux shell prompt with standard utilities to diagnose problems and fix errors.

**TIP**

To stop working with the Veeam Recovery Media and shut down or restart your computer, in the Veeam Recovery Media main menu, select the **Reboot** or **Shutdown** option and press Enter.
Step 2. Configure Network Settings

To open the **Network settings** dialog, in the Veeam Recovery Media main menu, select the **Configure network** option and press **Enter**.

Veeam Agent for Linux will display network adapters that are available on the system. If there is a DHCP server in your network, Veeam Agent will configure the network settings automatically and display the IP address assigned to the network adapter. You can then press **Esc** to return to the Veeam Recovery Media main menu and launch the Volume Restore wizard.

You can manually configure TPC/IP v4 settings for network adapters if necessary. To learn more, see [Specifying Network Settings](#).

![Choose adapter dialog](image)
Specifying Network Settings

You can manually configure TPC/IP v4 settings for the network adapter. To configure network settings:

1. In the Choose adapter list, select the network adapter that you want to use to connect to the network shared folder or Veeam backup repository where the backup resides and press Enter.

2. In the Configure adapter dialog, select the Manual option and press Enter.

3. In the Adapter settings dialog, specify the following network settings:
   - IP address
   - Subnet mask
   - Default gateway
   - DNS server

4. Select the Apply button and press Enter.

If there is a DHCP server in your network, you can return to automatic IP addressing:

1. In the Choose adapter list, select the necessary network adapter and press Enter.

2. In the Configure adapter dialog, select the Auto option and press Enter. Veeam Agent will automatically configure network settings for the adapter.
Step 3. Launch File Level Restore Wizard

To launch the file-level restore wizard, in the Veeam Recovery Media main menu, select **Restore files** and press Enter.
Step 4. Select Backup Location

At the **Select backup location** step of the wizard, specify where the backup file that you want to use for data recovery is located.

To recover data from backup, you need to mount the backup storage on which the backup file resides to the recovery image OS file system. Veeam Agent automatically mounts external USB drives that are connected to the computer and displays them in the list of available backup locations. You can select the necessary device and press **Enter** to pass to the **Browse for backup files** step of the wizard.

If the backup file is located in a network shared folder or on a local drive, select one of the following options:

- **Add shared folder** — select this option if the backup file is located in a network shared folder. With this option selected, you will pass to the **Mount shared folder** step of the wizard.

- **Mount local disk** — select this option if the backup file resides on the local computer drive, external drive or removable storage device that is currently connected to your computer. With this option selected, you will pass to the **Select local disk** step of the wizard.

- **Add VBR server** — select this option if the backup file resides on a backup repository managed by the Veeam backup server. With this option selected, you will pass to the **Specify backup server parameters** step of the wizard.

- **Add Cloud provider** — select this option if the backup file resides on a cloud repository exposed to you by a Veeam Cloud Connect service provider. With this option selected, you will pass to the **Specify Cloud provider parameters** step of the wizard.
Step 5. Specify Backup Location Settings

Specify settings for the target storage that contains a backup file from which you plan to restore data:

- **Specify shared folder settings** — if you have selected the Add shared folder option at the Select backup location step of the wizard.

- **Select local drive** — if you have selected the Mount local disk option at the Select backup location step of the wizard.

- **Specify Veeam backup repository settings** — if you have selected the Add VBR server option at the Select backup location step of the wizard.

- **Specify Veeam Cloud Connect repository settings** — if you have selected the Add Cloud provider option at the Select backup location step of the wizard.
Specifying Shared Folder Settings

The **Mount shared folder** step of the wizard is available if you have selected to restore data from a backup file located in a network shared folder.

Specify settings for the network shared folder:

1. Select the type of a network shared folder:
   - **NFS** — to connect to a network shared folder using the NFS protocol.
   - **SMB** — to connect to a network shared folder using the SMB (CIFS) protocol.

2. In the **Path** field, specify the network shared folder name in the `SERVER/DIRECTORY` format: type an IP address or domain name of the server and the name of the network shared folder in which the backup file resides.

3. [For SMB network shared folder] In the **Domain** field, type a name of the domain in which the account that has access permissions on the shared folder is registered, for example: `DOMAIN`.

4. [For SMB network shared folder] In the **Username** field, type a name of the account that has access permissions on the shared folder.

5. [For SMB network shared folder] In the **Password** field, type a password of the account that has access permissions on the shared folder.

**TIP**

You can mount several network shared folders to work with backup files that are stored in different locations if needed. To do this, return to the Select Backup Location step of the wizard and select the **Add shared folder** option once again. For every mounted location, Veeam Agent displays its name, type and mount point. You can view the list of mounted network shared folders and browse for a backup file located on the necessary storage.
Selecting Local Drive

The **Select local disk** step of the wizard is available if you have selected to restore data from a backup file located on a computer drive.

In the list of devices, select the necessary disk or disk partition and press **Enter**. Veeam Agent will mount the selected device to the `/media` directory of the recovery image OS file system and display content of the directory.

**TIP**

You can mount several devices to work with backup files that are stored in different locations if needed. To do this, return to the **Select Backup Location** step of the wizard and select the **Mount local disk** option once again. For every mounted location, Veeam Agent displays its name, type and mount point. You can view the list of mounted devices and browse for a backup file located on the necessary storage.

![Veeam Recovery Media]

<table>
<thead>
<tr>
<th>Device</th>
<th>Size</th>
<th>Filesystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>sda1</td>
<td>9.31G</td>
<td>ext4</td>
</tr>
<tr>
<td>sda6</td>
<td>39.00G</td>
<td>ext4</td>
</tr>
<tr>
<td>sr0</td>
<td>100.0M</td>
<td>iso9660</td>
</tr>
</tbody>
</table>
Specifying Backup Server Parameters

The **Specify backup server parameters** step of the wizard is available if you have selected to restore data from a backup repository managed by the Veeam backup server.

Specify settings for the Veeam backup server that manages the backup repository where the backup file resides:

1. In the **Address** field, specify a DNS name or IP address of the Veeam backup server.
2. In the **Port** field, specify a number of the port over which Veeam Agent must communicate with the backup repository. By default, Veeam Agent uses port 10006.
3. In the **Login** field, type a name of the account that has access to the Veeam backup repository.
4. In the **Domain** field, type a name of the domain in which the account that has access to the Veeam backup repository is registered, for example: `DOMAIN`.
5. In the **Password** field, type a password of the account that has access to the Veeam backup repository.
6. Press **Enter**. Veeam Agent will connect to the Veeam backup server, and you will pass immediately to the **Backup** step of the wizard.
Specifying Service Provider Settings

If you have selected to restore data from a backup file located on a Veeam Cloud Connect repository, specify settings to connect to the cloud repository:

1. Specify service provider settings.
2. Verify the TLS certificate.
3. Specify user account settings.
Specifying Service Provider Settings

The **Specify Cloud provider parameters** step of the wizard is available if you have selected to restore data from a cloud repository exposed to you by a Veeam Cloud Connect service provider.

Specify service provider settings that the SP or your backup administrator has provided to you:

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the cloud gateway.
2. In the **Port** field, specify the port over which Veeam Agent will communicate with the cloud gateway. By default, port 6180 is used.
3. Press **Enter**. Veeam Agent will connect to the service provider and display the Certificate details window.
Verifying TLS Certificate

In the **Certificate details** window, review information about the TLS certificate obtained from the SP side and verify the TLS certificate.

- To accept the TLS certificate, select the **Accept** button with the **Tab** key and press **Enter**.
- [Optional] To verify the TLS certificate with a thumbprint, do the following:
  a. Select the **Verify thumbprint** button with the **Tab** key and press **Enter**.
  b. In the **Thumbprint verification** field, enter the thumbprint that you obtained from the SP.
  c. Switch to the **Verify** button and press **Enter**. Veeam Agent for Linux will check if the thumbprint that you entered matches the thumbprint of the obtained TLS certificate.

TLS certificate verification is optional. You can use this option to verify self-signed TLS certificates. TLS certificates signed by the CA do not require additional verification.
Specifying User Account Settings

The Specify Cloud provider credentials step of the wizard is available if you have chosen to restore data from a cloud repository and specified settings for the cloud gateway.

1. In the Username field, type a name of the tenant or subtenant account that the SP or your backup administrator has provided to you. The name of the subtenant account must be specified in the TENANT\SUBTENANT format.

2. In the Password field, provide a password for the tenant or subtenant account.

3. Press Enter. Veeam Agent for Linux will connect to the cloud repository, and you will pass immediately to the Backup step of the wizard.
Step 6. Browse for Backup File

At the **Browse for backup files** step of the wizard, select the backup file that you plan to use for volume-level restore:

1. In the file system tree, select a directory in which the backup file you plan to use for restore resides:
   - Use **Up** and **Down** arrow keys to select a directory.
   - Use the **Enter** key to open the necessary directory.

2. In the directory where the backup file resides, select the backup file and press **Enter**.
Step 7. Select Backup and Restore Point

At the Backup step of the wizard, select a backup and restore point from which you want to recover data.

The Backup step window comprises two panes:

- The Imported backups pane on the left displays information about backup: host name of the computer whose data is stored in the backup file, backup job name and number of restore points.

- The Restore points pane on the right displays a list of restore points in the backup.

To select backup and restore point:

1. In the Imported backups pane, ensure that the backup from which you want to recover data is selected and press Enter.

   If you want to select another backup, press the 'i' key and browse for the necessary backup file. To learn more, see Locate Backup File.
2. In the **Restore points** pane, select with **Up** and **Down** keys the restore point from which you want to recover data and press **Enter**.

**NOTE**
If you selected an encrypted backup for data restore, Veeam Agent will prompt you to provide a password to unlock the encrypted file. To learn more, see [Restoring Data from Encrypted Backups](#).
3. Veeam Agent will mount the content of the backup file to the `/mnt/backup` directory in the recovery image OS file system and display a notification window with the corresponding message. Press `Enter` to proceed to the File Level Restore wizard menu, open the file manager and save restored files.

When you perform file-level restore with the File Level Restore wizard, Veeam Agent always mounts the backup to the `/mnt/backup` directory. If you want to specify another directory for backup mount, you can perform file-level restore with the Veeam Agent command line interface. To learn more, see Restoring Files and Folders with Command Line Interface.
Step 8. Save Restored Files

When the backup file content is mounted to the recovery image OS file system, Veeam Agent opens the File Level Restore wizard menu displaying a list of available operations.

You can perform the following operations with file-level backup:

- **Start file commander** — select this option if you want to start the file manager and work with restored files and folders. To learn more, see [Working with Midnight Commander](#).

- **Stop backup mount** — select this option if you want to stop the backup mount session and unmount the backup file content from the `/mnt/backup` directory of the recovery image OS file system. To learn more, see [Stopping Backup Mount Session](#).

- **Exit to shell** — select this option if you want to open the Linux shell prompt and use common Linux command-line tools.

**TIP**

To stop working with the Veeam Recovery Media and shut down or restart your computer, in the File Level Restore wizard menu, select the **Reboot** or **Shutdown** option and press Enter.
Working with Midnight Commander

To work with restored files and folders, you can use Midnight Commander — a file manager that is included into the Veeam Recovery Media. With the Midnight Commander file manager, you can browse the mounted backup content and file system on your computer, and save restored files and folders to the original location or to a new location.

To launch the file manager, in the File Level Restore wizard menu, select **Start file browser** and press **Enter**.

When you launch Midnight Commander, Veeam Agent displays in the file manager the directory with the backup content and your computer’s file system:

- In the left pane, Veeam Agent displays a directory of your computer’s file system mounted under the `/mnt/system` directory of the recovery image OS file system. By default, Veeam Agent mounts to the recovery image OS file system the following volumes of your computer:
  
  - If you use a volume-level backup for file-level restore, Veeam Agent detects the partition table in the backup, mounts to the `/mnt/system` directory block devices that represent volumes of your computer with the same names as volumes in the backup. For example, if your volume-level backup contains `/dev/sda1` and `/dev/sda6` volumes with `/` and `/home` mount points, Veeam Agent will mount to the `/mnt/system` directory both root (`/`) and `/home` partitions.
  
  - If you use a file-level backup for file-level restore, Veeam Agent mounts to the `/mnt/system` directory only the system volume of your computer, for example, `/dev/sda1`. If you want to save restored files and folders to a directory on another computer volume or to a network shared folder, you need to mount this volume or folder manually. To mount a target storage for restored files:
    
    i. In Midnight Commander, press **F10** to close the file manager.
    
    ii. In the **File Level Restore** wizard menu, select the **Exit to shell** option and press **Enter**.
    
    iii. Mount the target storage for the restored files and folders with the `mount` command.

- In the right pane, Veeam Agent displays a directory in which the backup content is mounted. Veeam Agent mounts the backup content under the `/mnt/backup` folder.
While the Midnight Commander file manager is open, you can perform the following operations with restored files and folders:

- **Save files to initial location**
- **Save files to a new location**

After you finish working with files and folders, **finish working with the Veeam Recovery Media**.
Saving Files to Initial Location

To save restored files or folders to their initial location on your computer, do the following:

1. In the left pane of the file manager window, open the directory in your computer's file system in which the backed-up file or folder that you want to restore originally resided.

2. In the right pane of the file manager window, open the directory that contains the file or folder in the backup that you want to restore to its original location.

3. Select the file or folder that you want to restore and press F5.

4. In the Copy dialog window, review the file or folder copy settings, select Ok and press Enter.
5. If the file or folder you want to restore exists in its original location, Midnight Commander will display a warning. In the warning window, select the necessary operation with the target file or folder and press **Enter**. Midnight Commander will save the file or folder in its original location.

6. After you finish working with files and folders, press **F10** to close the file manager.
Saving Files to New Location

To save restored files or folders to a new location on your computer or to a network shared folder, do the following:

1. In the left pane of the file manager window, open the directory in your computer's file system in which you want to restore a file or folder.
2. In the right pane of the file manager window, open the directory that contains the file or folder in the backup that you want to restore.
3. Select the file or folder that you want to restore and press **F5**.
4. In the **Copy** dialog window, review the file or folder copy settings, select **Ok** and press **Enter**.
5. Midnight Commander will save the file or folder to the specified location.

6. After you finish working with files and folders, press F10 to close the file manager.
Stopping Backup Mount Session

When Veeam Agent mounts a backup for file-level restore, Veeam Agent starts a new backup mount session. To unmount a backup, you need to stop the backup mount session. This may be required, for example, if you want to stop working with files and folders in one backup and mount another backup for file-level restore.

To stop the backup mount session with the Veeam Recovery Media, in the File Level Restore wizard menu, select the **Stop backup mount** option and press **Enter**. Veeam Agent will stop the backup mount session, unmount the backup from the `/mnt/backup` directory of the recovery image OS file system, exit the File Level Restore wizard and display the Veeam Recovery Media main menu.
Step 9. Finish Working with Veeam Recovery Media

When the restore operation completes, finish working with the Veeam Recovery Media and start your operating system.

1. Eject the media or removable storage device with the recovery image.
2. In the File Level Recovery wizard menu or Veeam Recovery Media main menu, select the Reboot option and press Enter.
3. Wait for your Linux operating system to start.
Restoring Volumes with Command Line Interface

You can restore a specific computer volume or all volumes from the volume-level backup.

**NOTE**
You cannot use the Veeam Agent for Linux command line interface to restore Btrfs subvolumes.

Volumes can be restored to their original location or to a new location.

- If you restore a volume to its original location, Veeam Agent will overwrite the data on the original volume with the data restored from the backup.
- If you restore volume data to a new location, Veeam Agent will restore data from the backup and write it to the selected destination. If necessary, you can specify new disk mapping settings for the restored volume.

You can use Veeam Agent commands to restore volumes from a backup or restore point:

- **Restore from backup**
  When you restore a volume from the backup, Veeam Agent will automatically select the latest restore point in the backup. The volume will be restored to the state in which the volume was at the time when the latest restore point was created.

- **Restore from a restore point**
  When you restore a volume from the restore point, you can select the necessary restore point in the backup to recover data to a specific point in time.
Before You Begin

Before you begin the volume-level restore process, check the following prerequisites:

- The volume-level backup from which you plan to restore data must be successfully created at least once.
- [For backups stored in network shared folders and on Veeam backup repositories] You must have access to the target location where the backup file resides.
- [For Veeam backup repository targets] If you plan to restore data from a backup stored on a backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.

Volume-level restore has the following limitations:

- You cannot restore the system volume to its original location.
- You cannot restore a volume to the volume on which the Linux swap space is hosted.
- You cannot restore a volume to the volume where the backup file that you use for restore is located.

To overcome the first two limitations, you can boot from the recovery image and use the Veeam Recovery Media tools for volume-level restore. To learn more, see Restoring from Veeam Recovery Media.
Restoring from Backup

With Veeam Agent command line interface, you can restore volumes from the backup. When you restore a volume from the backup, Veeam Agent automatically selects the latest restore point in the backup and restores the volume to the state in which the volume was at the time when the latest restore point was created.
Step 1. Locate Backup

To view a list of backups created by Veeam Agent, use the following command:

```
veeamconfig backup list --all
```

In the list of backups, Veeam Agent displays information about all Veeam Agent for Linux backups stored in all backup repositories. If Veeam Agent is connected to a Veeam backup server, all Veeam Agent for Linux backups that are kept on Veeam backup repositories managed by this server also appear in this list.

The `--all` parameter is optional. If you do not use this option, Veeam Agent displays information about backups created by the current Veeam Agent computer only.

For security reasons, if you work with Veeam Agent connected to a Veeam backup server as a member of a protection group for pre-installed Veeam Agents, the `veeamconfig backup list --all` command will display backups created only by the current Veeam Agent computer with the current connection settings. To learn more about protection groups for pre-installed Veeam Agents, see the Protection Group Types section in the Veeam Agent Management Guide.

For each backup, Veeam Agent displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Host name of the computer on which the backup job was configured and name of the job by which the backup was created.</td>
</tr>
<tr>
<td>Backup ID</td>
<td>ID of the backup.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository in which the backup was created. Imported backups are marked as <em>Imported</em> in the Repository column. For information about the import procedure, see Importing Backups.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the backup creation.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup list --all
Job name       Backup ID                               Repository
y    Created at
srv01 SystemBackup         {45f074d2-d2d9-423d-84e9-8f1798b08d4c}  Repository
1  2016-11-11 17:37
srv01 DocumentsBackup      {ea64a7e5-038a-4c86-970a-6d59d4cf3968}  Repository
1  2016-11-11 18:30
srv01 HomePartitionBackup  {4f75bb20-a6b6-4323-9287-1c6c8cecc6b}  Repository
2  2016-11-15 11:28
wrk01 SystemBackup         {951ac571-dd29-45ac-8624-79b8c45863}  Repository
2  2016-11-13 15:26
wrk02 SystemBackup         {8d6d4d39-51b2-48b1-ac7a-84f2d6dbc167}  Repository
3  2016-11-13 15:59
```
TIP

If you want to recover data from a backup that is stored in another location, for example, a backup created with another instance of Veeam Agent, you can import such backup into the Veeam Agent database on your computer. To learn more, see Importing Backups.
Step 2. Explore Backup Content

To view detailed information about specific backup, use the following command:

```
veeamconfig backup show --id <backup_id>
```

where:

<backup_id> — ID of the backup for which you want to view detailed information.

For a volume-level backup, Veeam Agent displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the volume in the backup.</td>
</tr>
<tr>
<td>Device</td>
<td>Path to the block device that represents the volume.</td>
</tr>
<tr>
<td>FS UUID</td>
<td>File system ID.</td>
</tr>
<tr>
<td>Offset</td>
<td>Position of the volume on the computer disk.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the volume in the backup.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup show --id 4f75bb20-a6b6-4323-9287-1c6c8cecc6b
Machine name: srv01 HomePartitionBackup
Name: [sda6]
Device: [/dev/sda6]
FS UUID: [4967f2eb-e8bb-48fe-a694-5ba67b9030a5]
Offset: [11813257216] bytes (23072768 sectors)
Size: [41872785408] bytes (81782784 sectors)
```
Step 3. Start Restore Process

To start the process of volume-level restore from the backup, use the following command:

```
veeamconfig backup restore --id <backup_id> --targetdev <target_volume> --backupdev <volume_in_backup>
```

where:

- `<backup_id>` — ID of the backup.
- `<target_volume>` — path to a block device that represents a volume on your computer that you want to recover.
- `<volume_in_backup>` — path to a block device that represents a volume in the backup.

This parameter is optional. If you do not specify this parameter, Veeam Agent will restore from the backup a volume that has the same name as a `<target_volume>`.

For example:

```
user@srv01:~$ veeamconfig backup restore --id 4f75bb20-a6b6-4323-9287-1c6c8cecc b6b --targetdev /dev/sdb --backupdev /dev/sda6
Restoring backup.
Backup: 4f75bb20-a6b6-4323-9287-1c6c8ceccb6b
Devices:
    Device in current system: [/dev/sdb]  In backup: [/dev/sda6];
You are sure? (y/n)
y
Volume restore from backup has been started.
Session ID: [0b72ef45-4c88-4639-b940-ad3828b1cd4e].
Logs stored in: [/var/log/veeam/Restore/Session_{0b72ef45-4c88-4639-b940-ad3828b1cd4e}].
```

**IMPORTANT**

You can restore a backed-up volume only to a target volume that is not used by your Linux OS (that does not have file system mount points). For example, you can add a new disk to your computer and restore a volume in the backup to this disk. To restore a volume to its original location or to another volume used by Linux OS, you should boot from the Veeam Recovery Media and perform volume-level restore with the Volume Restore wizard.
Step 4. Monitor Restore Process

You can monitor the restore process by viewing the restore session log in the command line interface.

To view Veeam Agent for Linux session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where:

`<session_id>` — ID of the restore session.

For example:

```
user@srv01:~$ veeamconfig session log --id 0b72ef45-4c88-4639-b940-ad3828blcd4e
2016-11-27 11:04:04 UTC {b141f32a-3e77-45a6-b55a-c100a464d67} [info] Job started
2016-11-27 11:04:04 UTC {9b60ac03-2de0-4fe2-a00e-bec556d98ee8} [info] Starting volume restore
2016-11-27 11:04:07 UTC {ced9af4a-6af1-4756-8ff8-8ec1325e18ec} [processing] sdb
2016-11-27 11:04:15 UTC {ced9af4a-6af1-4756-8ff8-8ec1325e18ec} [info] sdb 512.0 kB at 58.6kB/s (0%)
2016-11-27 11:14:35 UTC {ced9af4a-6af1-4756-8ff8-8ec1325e18ec} [info] sdb 6.5GB at 10.6MB/s (97%)
2016-11-27 11:14:37 UTC {ced9af4a-6af1-4756-8ff8-8ec1325e18ec} [info] sdb 6.5GB at 10.6MB/s (100%)
2016-11-27 11:14:37 UTC {00add723-cbfa-4cc8-b299-d2349a051d6f} [warn] /dev/sdb has a duplicate filesystem UUID
2016-11-27 11:14:37 UTC {ced9af4a-6af1-4756-8ff8-8ec1325e18ec} [info] sdb restored 6.5GB at 10.6MB/s
2016-11-27 11:14:37 UTC {8b8742a2-1c80-4e14-bbf1-45a3612bc3a7} [info] Volume restore completed
```

TIP

You can also check the restore session status with the `veeamconfig session info` command. To learn more, see Viewing Session Status.
Restoring from Restore Point

With Veeam Agent command line interface, you can restore volumes from the specific restore point. When you restore a volume from the restore point, you can select the necessary restore point in the backup to recover data to a desired point in time.
Step 1. Locate Backup

To view a list of backups created by Veeam Agent, use the following command:

```
veeamconfig backup list --all
```

In the list of backups, Veeam Agent displays information about all Veeam Agent for Linux backups stored in all backup repositories. If Veeam Agent is connected to a Veeam backup server, all Veeam Agent for Linux backups that are kept on Veeam backup repositories managed by this server also appear in this list.

The `--all` parameter is optional. If you do not use this option, Veeam Agent displays information about backups created by the current Veeam Agent computer only.

For security reasons, if you work with Veeam Agent connected to a Veeam backup server as a member of a protection group for pre-installed Veeam Agents, the `veeamconfig backup list --all` command will display backups created only by the current Veeam Agent computer with the current connection settings. To learn more about protection groups for pre-installed Veeam Agents, see the Protection Group Types section in the Veeam Agent Management Guide.

For each backup, Veeam Agent displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Host name of the computer on which the backup job was configured and name of the job by which the backup was created.</td>
</tr>
<tr>
<td>Backup ID</td>
<td>ID of the backup.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository in which the backup was created. Imported backups are marked as <em>Imported</em> in the Repository column. For information about the import procedure, see Importing Backups.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the backup creation.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup list --all
Job name           | Backup ID                                      | Repository
--------------------|-----------------------------------------------|----------------------
srv01 SystemBackup | {45f074d2-d2d9-423d-84e9-8f1798b08d4c}        | Repository_
1 2016-11-11 17:37 |                                               |
srv01 DocumentsBackup | {ea64a7e5-038a-4c86-970a-6d59d4cf3968}        | Repository_
1 2016-11-11 18:30 |                                               |
srv01 HomePartitionBackup | {4f75bb20-a6b6-4323-9287-1c6c8ceccb6b}       | Repository_
2 2016-11-15 11:28 |                                               |
wrk01 SystemBackup  | {951ac571-dd29-45ac-8624-79b8ccb45863}        | Repository_
2 2016-11-13 15:26 |                                               |
wrk02 SystemBackup  | {8d6d4d39-51b2-48b1-ac7a-84f2d6dbc167}        | Repository_
3 2016-11-13 15:59 |                                               |
```
TIP

If you want to recover data from a backup that is stored in another location, for example, a backup created with another instance of Veeam Agent, you can import such backup into the Veeam Agent database on your computer. To learn more, see Importing Backups.
Step 2. Explore Restore Points

To view information about restore points in the backup, use the following command:

```
veeamconfig backup info --id <backup_id>
```

or

```
veeamconfig point list --backupid <backup_id>
```

where

`<backup_id>` — ID of the backup for which you want to view information on restore points.

You can view the following information about restore points in the backup:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Name of the backup job by which the backup was created.</td>
</tr>
<tr>
<td>OIB ID</td>
<td>ID of the restore point in the backup.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of the restore point. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• Full</td>
</tr>
<tr>
<td></td>
<td>• Increment</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the restore point creation.</td>
</tr>
<tr>
<td>Is corrupt</td>
<td>Indicates whether restore point in the backup is corrupted. For example, restore point is still being created or backup job failed to create a working backup. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup info --id 4f75bb20-a6b6-4323-9287-1c6c8cecccb6b
Job name                   OIB ID                                  Type       C
created at     Is corrupt  
srv01 HomePartitionBackup  {23cb927d-5e2d-42fe-a4a4-e5f254a6413e}  Full       2
016-11-15 11:28 false
srv01 HomePartitionBackup  {25e31075-4c30-4d67-86a6-293c0887f4eb}  Increment  2
016-11-15 11:58 false
srv01 HomePartitionBackup  {9375140d-720a-4d3e-a69b-ab9cf60d53fa}  Increment  2
016-11-27 13:15 false
```
```bash
user@srv01:~$ veeamconfig point list --backupid 4f75bb20-a6b6-4323-9287-1c6c8ce ccb6b

<table>
<thead>
<tr>
<th>Job name</th>
<th>OIB ID</th>
<th>Type</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv01 HomePartitionBackup</td>
<td>{23cb927d-5e2d-42fe-a4a4-e5f254a6413e}</td>
<td>Full</td>
<td>2</td>
</tr>
<tr>
<td>016-11-15 11:28</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 HomePartitionBackup</td>
<td>{25e31075-4c30-4d67-86a6-293c0887f4eb}</td>
<td>Increment</td>
<td>2</td>
</tr>
<tr>
<td>016-11-15 11:58</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 HomePartitionBackup</td>
<td>{9375140d-720a-4d3e-a69b-ab9cf60d53fa}</td>
<td>Increment</td>
<td>2</td>
</tr>
<tr>
<td>016-11-27 13:15</td>
<td>false</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Step 3. Start Restore Process

To start the process of volume-level restore from the specific restore point, use the following command:

```bash
veeamconfig point restore --id <point_id> --targetdev <target_volume> --backupdev <volume_in_backup>
```

where:

- `<point_id>` — ID of the restore point.
- `<target_volume>` — path to a block device that represents a volume on your computer that you want to recover.
- `<volume_in_backup>` — path to a block device that represents a volume in the backup.

This parameter is optional. If you do not specify this parameter, Veeam Agent will restore from the backup a volume that has the same name as a `<target_volume>`.

For example:

```bash
user@srv01:~$ veeamconfig point restore --id 9375140d-720a-4d3e-a69b-ab9cf60d53fa --backupdev /dev/sda6 --targetdev /dev/sdb
Restoring point.
Restore point: 9375140d-720a-4d3e-a69b-ab9cf60d53fa
Devices:
  Device in current system: [/dev/sdb]  In backup: [/dev/sda6];
You are sure? (y/n)
y
Volume restore by point has been started.
Session ID: [{697d9348-9001-4845-8764-3cc4fb3f296b}].
Logs stored in: [/var/log/veeam/Restore/Session_{697d9348-9001-4845-8764-3cc4fb3f296b}].
```

**IMPORTANT**

You can restore a backed-up volume only to a target volume that is not used by your Linux OS (that does not have file system mount points). For example, you can add a new disk to your computer and restore a volume in the backup to this disk. To restore a volume to its original location or to another volume used by Linux OS, you should boot from the Veeam Recovery Media and perform volume-level restore with the Volume Restore wizard.
Step 4. Monitor Restore Process

You can monitor the restore process by viewing the restore session log in the command line interface.

To view Veeam Agent session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where:

<session_id> — ID of the restore session.

For example:

```
user@srv01:~$ veeamconfig session log --id 697d9348-9001-4845-8764-3cc4fb3f296b
```

```
2016-11-27 10:35:47 UTC {ed661f6-5216-4596-a7b5-be10dd10c32f} [info] Starting volume restore
2016-11-27 10:35:50 UTC {2e37de47-c4e2-46f9-8b70-f24fbff3697d} [processing] sdb
2016-11-27 10:35:59 UTC {2e37de47-c4e2-46f9-8b70-f24fbff3697d} [info] sdb 512.0 kB at 59.1kB/s (0%)
...
2016-11-27 10:46:27 UTC {2e37de47-c4e2-46f9-8b70-f24fbff3697d} [info] sdb 6.5GB at 10.5MB/s (100%)
2016-11-27 10:46:28 UTC {da1e18c8-eb7c-4e14-9832-f0bd089b329} [warn] /dev/sdb has a duplicate filesystem UUID
2016-11-27 10:46:28 UTC {2e37de47-c4e2-46f9-8b70-f24fbff3697d} [info] sdb restored 6.5GB at 10.5MB/s
2016-11-27 10:46:28 UTC {a21a89d9-d0ca-4f5c-8399-28ae599f2f1c} [info] Volume restore completed
```

TIP

You can also check the restore session status with the `veeamconfig session info` command. To learn more, see Viewing Session Status.
Restoring Files and Folders with Recovery Wizard

If some files and folders on your computer get lost or corrupted, you can restore them from backups. For file-level restore, you can use backups of any type:

- Volume-level backups (backups of the entire computer or specific volumes)
- File-level backups

When you perform file-level restore, Veeam Agent publishes the backup content directly into the computer file system. You can browse to files and folders in the backup, restore files and folders to their initial location, copy files and folders to a new location or simply target applications to restored files and work with them as usual.
Before You Begin

Before you begin the file-level restore process, check the following prerequisites:

- The backup from which you plan to restore data must be successfully created at least once.

- [For backups stored in network shared folders, on Veeam backup repositories and Veeam Cloud Connect repositories] You must have access to the target location where the backup file resides.

- [For Veeam backup repository targets] If you plan to restore data from a backup stored on a backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.

- [For backups of Btrfs file system] A machine on which you perform file-level restore must run the same or later Linux kernel version as the machine on which the backup was created.

  For example, you created a backup of a machine that runs Linux kernel version 4.14. If you perform file-level restore from this backup on another machine that runs Linux kernel 2.6, the file-level restore process will fail.
Step 1. Launch File Level Restore Wizard

To launch the **File Level Restore** wizard, do the following:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command.

2. In the Veeam Agent control panel, press the 'r' key to proceed to the File Level Restore wizard.

```
<table>
<thead>
<tr>
<th>Job name</th>
<th>State</th>
<th>Started at</th>
<th>Finished at</th>
</tr>
</thead>
<tbody>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-14 06:10:04</td>
<td>2017-12-14 06:16:30</td>
</tr>
<tr>
<td>srv02CloudBackup</td>
<td>Failed</td>
<td>2017-12-14 06:00:03</td>
<td>2017-12-14 06:00:04</td>
</tr>
<tr>
<td>srv02CloudBackup</td>
<td>Success</td>
<td>2017-12-14 06:00:03</td>
<td>2017-12-14 06:07:11</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-13 21:54:32</td>
<td>2017-12-13 22:00:22</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-13 20:44:16</td>
<td>2017-12-13 20:46:56</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-13 06:10:01</td>
<td>2017-12-13 06:10:42</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Failed</td>
<td>2017-12-13 06:00:01</td>
<td>2017-12-13 06:00:01</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-13 06:00:01</td>
<td>2017-12-13 06:00:44</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-12 21:15:04</td>
<td>2017-12-12 21:20:21</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-12 19:51:40</td>
<td>2017-12-12 19:52:21</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-12 15:58:57</td>
<td>2017-12-12 15:58:57</td>
</tr>
</tbody>
</table>
```

Enter | Show | C | Configure | S | Start Job | R | Recover Files | M | Misc | Esc | Delist
Step 2. Select Backup and Restore Point

At the Backup step of the wizard, select a backup and restore point from which you want to recover data.

The Backup step window comprises two panes:

- The Imported backups pane on the left displays available backups and information about each backup: host name of the computer whose data is stored in the backup file, backup job name and number of restore points.

- The Restore points pane on the right displays a list of restore points in the backup.

To select backup and restore point:

1. In the Imported backups pane, select with Up and Down keys the backup from which you want to recover data and press Enter.

In the list of backups, Veeam Agent displays backups that were created by backup jobs configured with Veeam Agent on your computer. If Veeam Agent for Linux is connected to a Veeam Backup & Replication server or a Veeam Cloud Connect service provider, backups created in the Veeam backup repository or cloud repository also appear in the list.

By default, Veeam Agent displays in the list only those backups in the Veeam backup repository that were created under your account. If you used an account to which the Veeam Backup Administrator role is assigned to connect to the Veeam backup server, you can also view all Veeam Agent backups that are stored in the Veeam backup repository to which Veeam Agent is connected. To view such backups, click the Show all link at the bottom of the list.

If Veeam Agent fails to display backups stored in the Veeam backup repository for some reason, you can press the ‘r’ key to rescan the backup repository. Veeam Agent will try to reconnect to the Veeam backup server and refresh the list of backups.
If you want to recover data from a backup that is stored in another location, for example, a backup created with another instance of Veeam Agent in a network shared folder, you can import such backup. Press the 'i' key, browse to the directory in which the backup file resides and select the necessary backup file. The selected backup file will be added to the list of backups.

2. In the Restore points pane, select with Up and Down keys the restore point from which you want to recover data and press Enter.
NOTE
If you selected an encrypted backup for data restore, Veeam Agent will prompt you to provide a password to unlock the encrypted file. To learn more, see Restoring Data from Encrypted Backups.

<table>
<thead>
<tr>
<th>Job name</th>
<th>Hostname</th>
<th>Points</th>
<th>Created at</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv02 DailyBackup</td>
<td>srv02</td>
<td>4</td>
<td>06:10 14-12-2017</td>
</tr>
<tr>
<td>srv02 srv02CloudBackup</td>
<td>srv02</td>
<td>5</td>
<td>06:10 13-12-2017</td>
</tr>
<tr>
<td>srv02 srv02CloudBackup(encrypted) srv02</td>
<td></td>
<td>2</td>
<td>05:00 12-12-2017</td>
</tr>
<tr>
<td>srv02</td>
<td></td>
<td>22:14 11-12-2017</td>
<td></td>
</tr>
</tbody>
</table>
3. Veeam Agent will mount the content of the backup file to the `/mnt/backup` directory in the computer's file system and display a notification window with the corresponding message. Press **Enter** to close the window and return to the Veeam Agent control panel.

### Latest backup sessions:

<table>
<thead>
<tr>
<th>Job name</th>
<th>State</th>
<th>Started at</th>
<th>Finished at</th>
</tr>
</thead>
<tbody>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-14 06:10:04</td>
<td>2017-12-14 06:16:30</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Failed</td>
<td>2017-12-14 06:00:03</td>
<td>2017-12-14 06:00:04</td>
</tr>
<tr>
<td>srv02CloudBackup</td>
<td>Success</td>
<td>2017-12-13 21:54:12</td>
<td>2017-12-13 22:00:22</td>
</tr>
<tr>
<td>srv02CloudBackup</td>
<td>Success</td>
<td>2017-12-13 20:46:16</td>
<td>2017-12-13 20:46:50</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-13 06:10:01</td>
<td>2017-12-13 06:10:42</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Failed</td>
<td>2017-12-13 06:00:01</td>
<td>2017-12-13 06:00:01</td>
</tr>
<tr>
<td>srv02CloudBackup</td>
<td>Success</td>
<td>2017-12-13 06:00:44</td>
<td>2017-12-13 06:00:44</td>
</tr>
<tr>
<td>srv02CloudBackup</td>
<td>Success</td>
<td>2017-12-12 15:00:24</td>
<td>2017-12-12 15:00:24</td>
</tr>
<tr>
<td>srv02CloudBackup</td>
<td>Success</td>
<td>2017-12-12 15:43:40</td>
<td>2017-12-12 15:43:40</td>
</tr>
<tr>
<td>DailyBackup</td>
<td></td>
<td>2017-12-12 06:00:58</td>
<td>2017-12-12 06:00:58</td>
</tr>
</tbody>
</table>

**TIP**

When you finish working with restored files and folders, you can unmount the backup from the `/mnt/backup` folder. To learn more, see **Stop Backup Mount Session**.
Step 3. Save Restored Files

When the backup file content is mounted to the `/mnt/backup` directory in the computer’s file system, you can use Linux command line utilities or preferred file browser to work with restored files and directories. You can browse for files and directories in the mounted backup and copy files and directories that you want to restore to their initial location or to a new location.

In the following example, the restored file `Report1.pdf` is copied from the mounted backup to the new location with Linux command line utilities:

```
user@srv01:~$ ls Documents/
Reports
user@srv01:~$ ls /mnt/backup/FileLevelBackup_0/home/user/Documents/Reports/
user@srv01:~$ cp /mnt/backup/FileLevelBackup_0/home/user/Documents/Reports/Report1.pdf Documents/
user@srv01:~$ ls Documents/
Report1.pdf  Reports
```
Step 4. Stop Backup Mount Session

When Veeam Agent mounts a backup for file-level restore, Veeam Agent starts a new backup mount session. To unmount a backup, you need to stop the backup mount session. This may be required, for example, if you want to stop working with files and folders in one backup and mount another backup for file-level restore. You can also stop the backup mount session to unmount a backup after you have finished working with restored files and folders.

To stop the backup mount session, do the following:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command:
2. In the Veeam Agent control panel, press the 'u' key to unmount a backup.
3. Veeam Agent will stop the backup mount session and display a notification window. Press Enter to close the window and return to the Veeam Agent control panel.

<table>
<thead>
<tr>
<th>Job name</th>
<th>State</th>
<th>Started at</th>
<th>Finished at</th>
</tr>
</thead>
<tbody>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-14 06:10:00</td>
<td>2017-12-14 06:15:30</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Failed</td>
<td>2017-12-14 06:10:00</td>
<td>2017-12-14 06:10:04</td>
</tr>
<tr>
<td>srvv2CloudBackup</td>
<td>Success</td>
<td>2017-12-13 21:04:12</td>
<td>2017-12-13 23:00:22</td>
</tr>
<tr>
<td>srvv2CloudBackup</td>
<td>Success</td>
<td>2017-12-13 20:44:16</td>
<td>2017-12-13 20:46:50</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Success</td>
<td>2017-12-13 06:10:01</td>
<td>2017-12-13 06:10:42</td>
</tr>
<tr>
<td>DailyBackup</td>
<td>Failed</td>
<td>2017-12-13 06:10:00</td>
<td>2017-12-13 06:10:01</td>
</tr>
<tr>
<td>srvv2CloudBackup</td>
<td></td>
<td>2017-12-13 06:00:01</td>
<td>2017-12-13 06:00:44</td>
</tr>
<tr>
<td>srvv2CloudBackup</td>
<td></td>
<td>2017-12-12 21:20:21</td>
<td>2017-12-12 21:20:21</td>
</tr>
<tr>
<td>DailyBackup</td>
<td></td>
<td>2017-12-12 15:48:40</td>
<td>2017-12-12 15:48:40</td>
</tr>
<tr>
<td>DailyBackup</td>
<td></td>
<td>2017-12-12 06:00:58</td>
<td>2017-12-11 22:19:24</td>
</tr>
</tbody>
</table>
Restoring Files and Folders with Command Line Interface

If some files and folders on your computer get lost or corrupted, you can restore them from backups. For file-level restore, you can use backups of any type:

- Volume-level backups (backups of the entire computer or specific volumes)
- File-level backups

When you perform file-level restore, Veeam Agent publishes the backup content directly into the computer file system. You can browse to files and folders in the backup, restore files and folders to their initial location, copy files and folders to a new location or simply target applications to restored files and work with them as usual.

With the Veeam Agent command line interface, you can restore files and folders in a more flexible way than with the use of the File Level Restore wizard. In particular, you can specify a directory in which Veeam Agent should mount the backup file content for file-level restore. You can also mount several backups to different directories to work with files and folders restored from different backups simultaneously.

You can use Veeam Agent commands to restore files and folders from backup or from specific restore point:

- **Restore from backup**
  When you restore files and folders from the backup, Veeam Agent will automatically select the latest restore point in the backup. You can restore files and folders to the state in which they were at the time when the latest restore point was created.

- **Restore from a restore point**
  When you restore files and folders from the restore point, you can select the necessary restore point in the backup to recover data to a specific point in time.
Before You Begin

Before you begin the file-level restore process, check the following prerequisites:

- The backup from which you plan to restore data must be successfully created at least once.

- [For backups stored in network shared folders, on Veeam backup repositories and Veeam Cloud Connect repositories] You must have access to the target location where the backup file resides.

- [For Veeam backup repository targets] If you plan to restore data from a backup stored on a backup repository, you must have access permissions on this backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.

- [For backups of Btrfs file system] A machine on which you perform file-level restore must run the same or later Linux kernel version as the machine on which the backup was created.

  For example, you created a backup of a machine that runs Linux kernel version 4.14. If you perform file-level restore from this backup on another machine that runs Linux kernel 2.6, the file-level restore process will fail.
Restoring from Backup

With Veeam Agent command line interface, you can restore files and folders from the backup. When you perform file-level restore from the backup, Veeam Agent for Linux automatically selects the latest restore point in the backup. You can restore files and folders to the state in which they were at the time when the latest restore point was created.
Step 1. Locate Backup

To view a list of backups created by Veeam Agent, use the following command:

```
veeamconfig backup list --all
```

In the list of backups, Veeam Agent displays information about all Veeam Agent for Linux backups stored in all backup repositories. If Veeam Agent is connected to a Veeam backup server, all Veeam Agent for Linux backups that are kept on Veeam backup repositories managed by this server also appear in this list.

The `--all` parameter is optional. If you do not use this option, Veeam Agent displays information about backups created by the current Veeam Agent computer only.

For security reasons, if you work with Veeam Agent connected to a Veeam backup server as a member of a protection group for pre-installed Veeam Agents, the `veeamconfig backup list --all` command will display backups created only by the current Veeam Agent computer with the current connection settings. To learn more about protection groups for pre-installed Veeam Agents, see the Protection Group Types section in the Veeam Agent Management Guide.

For each backup, Veeam Agent displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Host name of the computer on which the backup job was configured and name of the job by which the backup was created.</td>
</tr>
<tr>
<td>Backup ID</td>
<td>ID of the backup.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository in which the backup was created. Imported backups are marked as <em>Imported</em> in the Repository column. For information about the import procedure, see Importing Backups.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the backup creation.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup list --all
Job name              | Backup ID                                                                 | Repository     |
----------------------|---------------------------------------------------------------------------|----------------|
srv01 SystemBackup    | {45f074d2-d2d9-423d-84e9-8f1798b08d4c}                                   | Repository_    |
1 2016-11-11 17:37    |                                                                          |                |
srv01 DocumentsBackup | {ea64a7e5-038a-4c86-970a-6d59d4cf3968}                                   | Repository_    |
1 2016-11-11 18:30    |                                                                          |                |
srv01 HomePartitionBackup | {4f75bb20-a6b6-4323-9287-1c6c8ceccbb6b}                           | Repository_    |
2 2016-11-15 11:28    |                                                                          |                |
wrk01 SystemBackup    | {951ac571-dd29-45ac-8624-79b8cbb45863}                                   | Repository_    |
2 2016-11-13 15:26    |                                                                          |                |
wrk02 SystemBackup    | {8d6d4d39-51b2-48b1-ac7a-84f2d6dbc167}                                   | Repository_    |
3 2016-11-13 15:59    |                                                                          |                |
```
TIP

If you want to recover data from a backup that is stored in another location, for example, a backup created with another instance of Veeam Agent, you can import such backup into the Veeam Agent database on your computer. To learn more, see Importing Backups.
Step 2. Explore Backup Content

For file-level restore, you can use backups of any type:

- Volume-level backups (backups of the entire computer or specific volumes)
- File-level backups

To view detailed information about specific backup, use the following command:

```
veeamconfig backup show --id <backup_id>
```

where:

- `<backup_id>` — ID of the backup for which you want to view detailed information.

For a volume-level backup, Veeam Agent for Linux displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the volume in the backup.</td>
</tr>
<tr>
<td>Device</td>
<td>Path to the block device that represents the volume.</td>
</tr>
<tr>
<td>FS UUID</td>
<td>File system ID.</td>
</tr>
<tr>
<td>Offset</td>
<td>Position of the volume on the computer disk.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the volume in the backup.</td>
</tr>
</tbody>
</table>

For a file-level backup, Veeam Agent for Linux displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine name</td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td>Backed up</td>
<td>Backup scope for the file-level backup job.</td>
</tr>
</tbody>
</table>
For example:

```
user@srv01:~$ veeamconfig backup show --id ea64a7e5-038a-4c86-970a-6d59d4cf3968
Machine name: srv01 DocumentsBackup
  File-level backup
    Backed up:
      /home/user/Documents
```
Step 3. Mount Backup

To mount a backup for file-level restore, use the following command:

```
veeamconfig backup mount --id <backup_id> --mountdir <path>
```

where:

- `<backup_id>` — ID of the backup that you want to mount to the computer file system for file-level restore.
- `<path>` — path to the directory to which you want to mount the backup file content.

For example:

```
user@srv01:~$ veeamconfig backup mount --id ea64a7e5-038a-4c86-970a-6d59d4cf3968 --mountdir /mnt/backup
Backup is mounted.
Session ID: {2a313184-32d0-4d3a-a1b0-2eebac986047}.
Logs stored in: [/var/log/veeam/Mount/Session_{2a313184-32d0-4d3a-a1b0-2eebac986047}].
```
Step 4. Monitor Mount Process and Result

You can monitor the backup mount process by viewing the mount session log in the command line interface.

To view Veeam Agent session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where:

<session_id> — ID of the backup mount session.

For example:

```
user@srv01:~$ veeamconfig session log --id 2a313184-32d0-4d3a-a1b0-2eebac986047
2016-11-22 17:30:34 UTC {30878c82-27d0-45dc-ab21-6f27d5082fd4} [info] Job started at 2016-11-22 20:30:34
2016-11-22 17:30:34 UTC {714b21d0-0d20-486e-b1e5-22d5fb5a8ee9} [info] Mounting restore point
2016-11-22 17:30:35 UTC {d331f038-5b7c-4549-85cf-5e1b54dbaf71} [info] Restore point has been mounted
```

To ensure that the backup is successfully mounted, you can browse to the directory that you specified in the `veeamconfig backup mount` command. For example:

```
user@srv01:~$ ls /mnt/backup/
FileLevelBackup_0
```

**TIP**

You can also check the restore session status with the `veeamconfig session info` command. To learn more, see Viewing Session Status.
Step 5. Save Restored Files

When the backup file content is mounted to the computer file system, you can use Linux command line utilities or preferred file browser to work with restored files and folders. You can browse for files and folders in the mounted backup and copy files and folders that you want to restore to their initial location or to a new location.

In the following example, the restored file `Report1.pdf` is copied from the mounted backup to a new location with the Linux command line utilities:

```bash
user@srv01:~$ ls Documents/
Reports
user@srv01:~$ ls /mnt/backup/FileLevelBackup_0/home/user/Documents/Reports/
user@srv01:~$ cp /mnt/backup/FileLevelBackup_0/home/user/Documents/Reports/Report1.pdf Documents/
user@srv01:~$ ls Documents/
Report1.pdf  Reports
```
Step 6. Stop Backup Mount Session

When Veeam Agent mounts a backup for file-level restore, Veeam Agent starts a new backup mount session. After you have finished working with restored files and folders, you can stop the backup mount session to unmount the backup.

To stop the backup mount session, use the following command:

```
veeamconfig session stop --id <session_id>
```

where:

*<session_id>* — ID of the backup mount session that you want to stop.

Veeam Agent will stop the mount session and unmount the backup from the computer file system. For example:

```
user@srv01:~$ veeamconfig session stop --id 2a313184-32d0-4d3a-a1b0-2eebac986047
Session has stopped.
user@srv01:~$ ls /mnt
user@srv01:~$
```
Restoring from Restore Point

With Veeam Agent command line interface, you can restore files and folders from the specific restore point. When you restore files and folders from the restore point, you can select the necessary restore point in the backup to recover data to a specific point in time.
Step 1. Locate Backup

To view a list of backups created by Veeam Agent, use the following command:

```
veeamconfig backup list --all
```

In the list of backups, Veeam Agent displays information about all Veeam Agent for Linux backups stored in all backup repositories. If Veeam Agent is connected to a Veeam backup server, all Veeam Agent for Linux backups that are kept on Veeam backup repositories managed by this server also appear in this list.

The `--all` parameter is optional. If you do not use this option, Veeam Agent displays information about backups created by the current Veeam Agent computer only.

For security reasons, if you work with Veeam Agent connected to a Veeam backup server as a member of a protection group for pre-installed Veeam Agents, the `veeamconfig backup list --all` command will display backups created only by the current Veeam Agent computer with the current connection settings. To learn more about protection groups for pre-installed Veeam Agents, see the Protection Group Types section in the Veeam Agent Management Guide.

For each backup, Veeam Agent displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job name</td>
<td>Host name of the computer on which the backup job was configured and name of the job by which the backup was created.</td>
</tr>
<tr>
<td>Backup ID</td>
<td>ID of the backup.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository in which the backup was created. Importantly, backups are marked as <strong>Imported</strong> in the Repository column. For information about the import procedure, see Importing Backups.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the backup creation.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup list --all
Job name                  Backup ID                               Repository
srv01 SystemBackup        {45f074d2-d2d9-423d-84e9-8f1798b08d4c} Repository_
  1  2016-11-11 17:37
srv01 DocumentsBackup     {ea64a7e5-038a-4c86-970a-6d59d4cf3968} Repository_
  1  2016-11-11 18:30
srv01 HomePartitionBackup {4f75bb20-a6b6-4323-9287-1c6c8cecccb6} Repository_
  2  2016-11-15 11:28
wrk01 SystemBackup        {951ac571-dd29-45ac-8624-79b8cc45863} Repository_
  2  2016-11-13 15:26
wrk02 SystemBackup        {8d6d4d39-51b2-48b1-ac7a-84f2d6dbc167} Repository_
  3  2016-11-13 15:59
```
TIP

If you want to recover data from a backup that is stored in another location, for example, a backup created with another instance of Veeam Agent, you can import such backup into the Veeam Agent database on your computer. To learn more, see Importing Backups.
Step 2. Explore Restore Points

To view information about restore points in the backup, use the following command:

```
veeamconfig backup info --id <backup_id>
```

or

```
veeamconfig point list --backupid <backup_id>
```

where:

- `<backup_id>` — ID of the backup for which you want to view information on restore points.

You can view the following information about restore points in the backup:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Job name</strong></td>
<td>Name of the backup job by which the backup was created.</td>
</tr>
<tr>
<td><strong>OIB ID</strong></td>
<td>ID of the restore point in the backup.</td>
</tr>
</tbody>
</table>
| **Type** | Type of the restore point. Possible values:  
  - Full  
  - Increment. |
| **Created at** | Date and time of the restore point creation. |
| **Is corrupt** | Indicates whether restore point in the backup is corrupted. For example, restore point is still being created or backup job failed to create a working backup. Possible values:  
  - True  
  - False |
For example:

```bash
user@srv01:~$ veeamconfig backup info --id ea64a7e5-038a-4c86-970a-6d59d4cf3968
```

<table>
<thead>
<tr>
<th>Job name</th>
<th>OIB ID</th>
<th>Type</th>
<th>Created at</th>
<th>Is corrupt</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{0f3c9f3e-3985-4dc9-8cd6-979dba810c2f}</td>
<td>Full</td>
<td>2016-11-11 18:31</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{ff0c6969-8b9b-4865-b4f9-d686f4af1d50}</td>
<td>Increment</td>
<td>2016-11-14 13:35</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{a9e420df-d749-4b9a-b675-19d8e94c3bf1}</td>
<td>Increment</td>
<td>2016-11-14 13:43</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{51e6056b-c0ae-40bc-bcf4-4ad7339f647a}</td>
<td>Increment</td>
<td>2016-11-14 15:48</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{b127e64e-1f1c-4e0b-bb36-b087761267b3}</td>
<td>Increment</td>
<td>2016-11-20 19:52</td>
<td>false</td>
</tr>
</tbody>
</table>

or

```bash
user@srv01:~$ veeamconfig point list --backupid ea64a7e5-038a-4c86-970a-6d59d4cf3968
```

<table>
<thead>
<tr>
<th>Job name</th>
<th>OIB ID</th>
<th>Type</th>
<th>Created at</th>
<th>Is corrupt</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{0f3c9f3e-3985-4dc9-8cd6-979dba810c2f}</td>
<td>Full</td>
<td>2016-11-11 18:31</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{ff0c6969-8b9b-4865-b4f9-d686f4af1d50}</td>
<td>Increment</td>
<td>2016-11-14 13:35</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{a9e420df-d749-4b9a-b675-19d8e94c3bf1}</td>
<td>Increment</td>
<td>2016-11-14 13:43</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{51e6056b-c0ae-40bc-bcf4-4ad7339f647a}</td>
<td>Increment</td>
<td>2016-11-14 15:48</td>
<td>false</td>
</tr>
<tr>
<td>srv01 DocumentsBackup</td>
<td>{b127e64e-1f1c-4e0b-bb36-b087761267b3}</td>
<td>Increment</td>
<td>2016-11-20 19:52</td>
<td>false</td>
</tr>
</tbody>
</table>
Step 3. Mount Restore Point

To mount a backup for file-level restore, use the following command:

```
veeamconfig point mount --id <point_id> --mountdir <path>
```

where:

- `<point_id>` — ID of the restore point that you want to mount to the computer file system for file-level restore.
- `<path>` — path to the directory to which you want to mount the backup file content.

For example:

```
user@srv01:~$ veeamconfig point mount --id b127e64e-1f1c-4e0b-bb36-b087761267b3 --mountdir /mnt/backup
Restore point is mounted.
Session ID: [{4d69dd85-ac60-4cff-883d-50f25f49a9c8}].
Logs stored in: [/var/log/veeam/Mount/Session_{4d69dd85-ac60-4cff-883d-50f25f49a9c8}].
```
Step 4. Monitor Mount Process and Result

You can monitor the restore point mount process by viewing the mount session log in the command line interface.

To view Veeam Agent session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where:

<session_id> — ID of the restore point mount session.

For example:

```
user@srv01:~$ veeamconfig session log --id 4d69dd85-ac60-4cff-883d-50f25f49a9c8
2016-11-23 12:44:55 UTC {4ac10045-a74b-4a41-9c5e-53521c7a1045} [info] Mounting restore point
2016-11-23 12:44:56 UTC {540a61f7-5d5c-47d5-a2b8-51daa694d5ec} [info] Restore point has been mounted
```

To ensure that the restore point is successfully mounted, you can browse to the directory that you specified in the `veeamconfig point mount` command. For example:

```
user@srv01:~$ ls /mnt/backup/
FileLevelBackup_0
```

**TIP**

You can also check the restore session status with the `veeamconfig session info` command. To learn more, see Viewing Session Status.
Step 5. Save Restored Files

When the restore point is mounted to the computer file system, you can use Linux command line utilities or preferred file browser to work with restored files and folders. You can browse for files and folders in the mounted backup and copy files and folders that you want to restore to their initial location or to a new location.

In the following example, the restored file `Report1.pdf` is copied from the mounted restore point to a new location with the Linux command line utilities:

```
user@srv01:~$ ls Documents/
Reports
user@srv01:~$ ls /mnt/backup/FileLevelBackup_0/home/user/Documents/Reports/
user@srv01:~$ cp /mnt/backup/FileLevelBackup_0/home/user/Documents/Reports/Report1.pdf Documents/
user@srv01:~$ ls Documents/
Report1.pdf  Reports
```
Step 6. Stop Backup Mount Session

When Veeam Agent mounts a restore point for file-level restore, Veeam Agent starts a new restore point mount session. After you have finished working with restored files and folders, you can stop the mount session to unmount the restore point.

To stop the restore point mount session, use the following command:

```
veeamconfig session stop --id <session_id>
```

where:

`<session_id>` — ID of the restore point mount session that you want to stop.

Veeam Agent will stop the mount session and unmount the restore point from the computer file system. For example:

```
user@srv01:~$ veeamconfig session stop --id 4d69dd85-ac60-4cff-883d-50f25f49a9c8
Session has stopped.
user@srv01:~$ ls /mnt
user@srv01:~$
```
Exporting Backup to Virtual Disk

You can export a backup to a virtual disk in the VHD format. You can then attach the created VHD disc to a virtual machine to recover your computer in a virtual environment.

- Exporting Backups
- Exporting Restore Points
Exporting Backups

You can export the backup file to a virtual disk in the VHD format. When you export a backup, you export to a virtual disk data pertaining to the latest restore point in the backup. The created VHD disk will reflect the state in which backed-up volumes were at the time when the latest restore point was created.

To export backup to a VHD disk:

1. Start the export process with the following command:

   ```
   veeamconfig backup export --id <backup_id> --outdir <path>
   ```

   where:
   - `<backup_id>` — ID of the backup that you want to export to a virtual disk.
   - `<path>` — full path to a directory in which you want to save the created virtual disk. Specifying relative paths is not supported.

   For example:

   ```
   user@srv01:~$ veeamconfig backup export --id 45f074d2-d2d9-423d-84e9-8f1798b08d4c --outdir /home/user/disk
   Export has been started.
   Session ID: [{5f001367-8937-46e0-a756-449bf9f1a182}].
   Logs stored in: [/var/log/veeam/Export/Session_{5f001367-8937-46e0-a756-449bf9f1a182}].
   ```

2. You can monitor the export process and result by viewing the export session log with the following command:

   ```
   veeamconfig session log --id <session_id>
   ```

   where:
   - `<session_id>` — ID of the export session.

   For example:

   ```
   user@srv01:~$ veeamconfig session log --id 5f001367-8937-46e0-a756-449bf9f1a182
   2016-11-27 11:20:56 UTC {b5af37c-35a6-4807-80d2-0f070f024e69} [info] Job started at 2016-11-27 14:20:56
   2016-11-27 11:20:56 UTC {48d699d2-86c8-4a32-b9c8-ab51b8325f3c} [info] Exporting virtual disks content
   2016-11-27 11:20:57 UTC {0e2e7d97-f067-4823-8d8e-084c401eb62b} [processing] Restoring device: [30460cb5].
   2016-11-27 11:22:59 UTC {0e2e7d97-f067-4823-8d8e-084c401eb62b} [info] Device [30460cb5] has been exported
   2016-11-27 11:23:00 UTC {36f0dc05-2af7-48d8-abc2-c8ef9aafffc54} [info] Virtual disks content has been exported
   ```

   You can also check the restore session status with the `veeamconfig session info` command. To learn more, see Viewing Session Status.
3. Exported backup will be saved as a virtual disk file in the specified directory. You can check this with a file browser or with the following command:

```
ls <path>
```

where:

`<path>` — path to the directory in which the virtual disk with the backup is saved.

For example:

```
user@srv01:~$ ls disk/
dev_30460cb5.vhd
```
Exporting Restore Points

You can export the specific restore point to a virtual disk in VHD format. When you export a restore point, you select the necessary restore point in the backup to recover data to a desired point in time. The created VHD disk will reflect the state in which backed-up volumes were at the time when the selected restore point was created.

To export restore point to a VHD disk:

1. Start the export process with the following command:

   veeamconfig point export --id <point_id> --outdir <path>

   where:
   
   o <point_id> — ID of the restore point that you want to export to a virtual disk.
   
   o <path> — full path to a directory in which you want to save the created virtual disk. Specifying relative paths is not supported.

   For example:

   user@srv01:~$ veeamconfig point export --id b319e1f-59a2-41ea-9ca3-b668e86ac941 --outdir /home/user/veeam/
   Export has been started.
   Session ID: [{aeb9c549-a660-4a0e-b89c-cb076b8b08fa85}].
   Logs stored in: [/var/log/veeam/Export/Session_{aeb9c549-a660-4a0e-b89c-cb076b8b08fa85}].

2. You can monitor the export process and result by viewing the export session log with the following command:

   veeamconfig session log --id <session_id>

   where:

   <session_id> — ID of the export session.

   For example:

   user@srv01:~$ veeamconfig session log --id aeb9c549-a660-4a0e-b89c-cb076b8b08fa85
   2016-05-05 11:15:21 UTC {32d56391-9002-431e-ae6b-2285537a67e5} [info] Exporting virtual disks content
   2016-05-05 11:15:22 UTC {ba3dabe0-0556-430c-9671-9448a6dc4bcb} [processing] Restoring device: [30460cb5].
   2016-05-05 11:17:26 UTC {ba3dabe0-0556-430c-9671-9448a6dc4bcb} [info] Device [30460cb5] has been exported
   2016-05-05 11:17:26 UTC {9e945c29-900e-4a07-9e3b-ccf7f156807d} [info] Virtual disks content has been exported

   You can also check the restore session status with the veeamconfig session info command. To learn more, see Viewing Session Status.
3. Exported backup will be saved as a virtual disk file in the specified directory. You can check this with a file browser or with the following command:

```bash
ls <path>
```

where

`<path>` — path to the directory in which the virtual disk with the backup is saved.

For example:

```bash
user@srv01:~$ ls /home/user/veeam/
devel_30460cb5.vhd
```
Restoring Data from Encrypted Backups

When you restore data from an encrypted backup, Veeam Agent performs data decryption automatically in the background or requires you to specify a password.

- If encryption keys required to unlock the backup file are available in the Veeam Agent database, that is, if you encrypt and decrypt the backup file on the same Veeam Agent computer, you do not need to specify the password. Veeam Agent uses keys from the database to unlock the backup file. Data decryption is performed in the background, and data restore from the encrypted backup does not differ from that from an unencrypted one.

- If encryption keys are not available in the Veeam Agent database, you need to provide a password to unlock the encrypted file. The password must be the same as the password that was used to encrypt the backup file. If the password has changed once or several times, you need to specify the latest password. In Veeam Agent, you can use the latest password to restore data from all restore points in the backup chain, including restore points that were encrypted with an old password and restore points that were created before you have enabled the encryption option for the job.

The process of unlocking an encrypted backup file differs depending on what Veeam Agent user interface you use for data restore.

  - [Veeam Agent graphical user interface](#)
  - [Veeam Agent command line interface](#)
Restoring Data from Encrypted Backups Using GUI

To restore data from an encrypted backup using the Veeam Agent graphical user interface:

1. Launch the necessary data restore wizard:
   - If you want to perform file-level restore from an encrypted backup that was created on another Veeam Agent computer, launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command. To learn more, see Restoring Files and Folders.
   - If you want to perform volume-level restore or file-level restore recovery from an encrypted backup, boot from the Veeam Recovery Media and launch the necessary data restore wizard. To learn more, see Restoring from Veeam Recovery Media.

2. Follow the steps of the wizard to specify where the encrypted backup file that you plan to use for restore resides. If the backup file resides in a remote location, select the backup location type and specify settings to connect to the backup location.

3. Select the encrypted backup and restore point from which you want to restore data.

4. Veeam Agent will display the Encryption window. Enter the password for the backup file.

   In the **Hint** field of the Encryption window, Veeam Agent displays a hint for the password that was used to encrypt the backup file. Use the hint to recall the password.

   If you changed the password one or several times while the backup chain was created, you need to specify the latest password. In Veeam Agent, you can use the latest password to restore data from all restore points in the backup chain, including those restore points that were encrypted with an old password.
If you enter correct password, Veeam Agent will decrypt the backup metadata. You will be able to continue the restore operation in a regular manner.
Restoring Data from Encrypted Backups Using Command Line Interface

To restore data from an encrypted backup using the Veeam Agent command line interface, complete the following steps:

1. Import the encrypted backup file to the Veeam Agent database. To learn more, see Importing Encrypted Backups.

2. Perform the necessary restore operation in a regular manner. To learn more, see Restoring Volumes with Command Line Interface and Restoring Files and Folders with Command Line Interface.
Reporting

Veeam Agent for Linux provides several ways to get information about performed operations:

- With the Veeam Agent control panel
- With the Veeam Agent command line interface

For every data transfer operation, for example data backup and restore, backup import and export, Veeam Agent starts a new session. You can monitor performance of sessions started by Veeam Agent in the following ways:

- Monitor backup job session progress with the control panel.
- View real-time backup job session statistics with the control panel.
- View backup job sessions results with the control panel.
- View the session status using the command line interface.
- View session logs.
Viewing Job Session Progress

You can monitor the backup job session progress in the list of sessions in the Veeam Agent control panel. For the currently running backup job session, Veeam Agent shows session status and percentage of session completion in the **State** column of the list of sessions.

To view backup job session progress, do the following:

1. If you have started the backup job from the command line, launch the Veeam Agent control panel with the `veeam` command.

2. In the Veeam Agent control panel, in the list of backup job sessions, monitor progress of the currently running session.

   If you have started the backup job from the Veeam Agent control panel, Veeam Agent will immediately display the list of backup job sessions with the currently running session.

**TIP**

You can stop the backup job session at any time. To stop the backup job session, press the 's' key.
Viewing Real-Time Job Session Statistics

You can view real-time statistics for a job session in the Veeam Agent control panel. Veeam Agent shows detailed data for every backup job session: job progress, duration, processing rate, performance bottlenecks, amount of processed data, read and transferred data and details of the session performance, for example, warnings and errors that have occurred in the process of operation.

To view detailed information on the currently running backup job session, do the following:

1. If you have started the backup job from the command line, launch the Veeam Agent control panel with the `veeam` command.

2. In the Veeam Agent control panel, in the list of backup job sessions, select the currently running session with Up and Down keys and press Enter.

   If you have started the backup job from the Veeam Agent control panel, the current session will be already selected in the list of backup job sessions.

**TIP**

You can stop the backup job session at any time. To stop the backup job session, press the 's' keyboard key.
Statistics Counters

Veeam Agent for Linux displays jobs statistics for the following counters:

- The pane at the top of the control panel shows information on the job session type, percentage of the job completion and session status. If Veeam Agent operates in the Server edition and you have created more than one backup job, the job name also appears on the pane.

- The **Summary** box shows general information about the job:
  - **Duration** — time from the job start till the job end.
  - **Processing rate** — average speed of data processing. This counter is a ratio between the amount of processed data (**Processed** counter) and job duration (**Duration** counter).
  - **Bottleneck** — bottleneck in the data transmission process.

- The **Data** box shows information about processed data:
  - **Processed** — total size of all volumes processed by the job.
  - **Read** — amount of data read from the backed-up volume by Veeam Agent for Linux prior to applying compression. For incremental job runs, the value of this counter is typically lower than the value of the **Processed** counter. Veeam Agent reads only data blocks that have changed since the last job session, processes and copies these data blocks to the target location.
  - **Transferred** — amount of data transferred from the backed-up volume to the backup location after applying compression. This counter does not directly indicate the size of the resulting files. Depending on the backup infrastructure and job settings, Veeam Agent can perform additional activities with data, for example, decompress data prior to writing the file to disk. The activities can impact the size of the resulting file.

- The box in the center of the control panel shows a list of operations performed during the job session, their start time and duration time. To scroll the list of operations, use **Up** and **Down** arrow keys on the keyboard.

- The pane at the lower side of the control panel shows help information on how to navigate the control panel.
Backup [SystemBackup] 56%  Status: Running

Summary  Data
Duration: 00:01:11  Processed: 2.8 GB (56%)
Processing Rate: 42.1 MB/s  Read: 2.0 GB
Bottleneck: Agent  Transferred: 1.9 GB (2.1x)

Time  Action  Duration
14:27:14  Job SystemBackup started at 2016-12-07 14:27:14 MSK
14:27:14  Preparing To backup
14:27:15  Creating Volume snapshot  00:00:00
14:27:15  Starting full backup to Repository_1
14:27:16  Backing up BIOS bootloader on /dev/sda  00:00:01
14:27:17  Backing up sda 2.0 GB at 40.0 MB/s (56%)  00:01:06

S: Stop  Esc: Back
Viewing Job Session Result

You can view detailed statistics on every backup job session performed by Veeam Agent for Linux.

To view statistics for a specific job session:

1. Open the Veeam Agent control panel with one of the following commands:

   veeam

   or

   veeamconfig ui

   or

   veeamconfig session ui

2. In the Latest backup sessions list, select the necessary backup job session with Up and Down keys and press Enter.

   TIP

   To return to the list of backup job sessions, press Esc. You can then select another backup job session or exit the Veeam Agent control panel in one of the following ways:

   • with the Esc key — if you opened the control panel with the veeam or veeamconfig ui command.
   • with the 'q' key — if you opened the control panel with the veeamconfig session ui command.
<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>14:27:14</td>
<td>Job SystemBackup started at 2015-12-07 14:27:14 MSK</td>
<td></td>
</tr>
<tr>
<td>14:27:14</td>
<td>Preparing To backup</td>
<td></td>
</tr>
<tr>
<td>14:27:15</td>
<td>Creating Volume snapshot</td>
<td></td>
</tr>
<tr>
<td>14:27:15</td>
<td>Starting full backup to Repository_1</td>
<td></td>
</tr>
<tr>
<td>14:27:15</td>
<td>Backing up /dev/sda from /dev/sda</td>
<td></td>
</tr>
<tr>
<td>14:27:17</td>
<td>Backing up sda 5.0 GB at 42.1 MB/s</td>
<td></td>
</tr>
<tr>
<td>14:27:18</td>
<td>Backing up summary.xml</td>
<td></td>
</tr>
<tr>
<td>14:29:21</td>
<td>Releasing snapshot</td>
<td></td>
</tr>
<tr>
<td>14:29:22</td>
<td>Backup completed</td>
<td></td>
</tr>
</tbody>
</table>
Viewing Session Status

You can view status of every session that was started by Veeam Agent for Linux. To view the session status, use the following command:

```
veeamconfig session info --id <session_id>
```

where:

`<session_id>` — ID of the session for which you want to check status.

Veeam Agent displays the following information about sessions:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ID of the session.</td>
</tr>
<tr>
<td>Job name</td>
<td>Name of the backup job parent to the session. Veeam Agent displays value for this parameter only for backup job sessions.</td>
</tr>
<tr>
<td>Job ID</td>
<td>ID of the backup job parent to the session. Veeam Agent displays value for this parameter only for backup job sessions.</td>
</tr>
<tr>
<td>State</td>
<td>Current status of the session.</td>
</tr>
<tr>
<td>Start time</td>
<td>Date and time of the session start.</td>
</tr>
<tr>
<td>End time</td>
<td>Date and time of the session completion. Veeam Agent displays value for this parameter only for completed sessions.</td>
</tr>
</tbody>
</table>

The following example shows status information on the completed backup job session:

```
user@srv01:~$ veeamconfig session info --id 1592755d-3a2b-40a9-a036-5c81853b369e
Backup session
  ID: {1592755d-3a2b-40a9-a036-5c81853b369e}
  Job name: SystemBackup
  Job ID: {2495911e-58db-4452-b4d1-f53dfb50e60f}
  State: Success
  Start time: 2016-11-11 14:37:21 UTC
  End time: 2016-11-11 14:40:02 UTC
```
The following example shows status information on the running volume restore session:

```
user@srv01:~$ veeamconfig session info --id 697d9348-9001-4845-8764-3cc4fb3f296b
Restore session
  ID: {697d9348-9001-4845-8764-3cc4fb3f296b}
  State: Running
  Start time: 2016-11-27 10:35:47 UTC
  End time:
```
Viewing Session Logs

You can monitor the backup and restore process by viewing the backup job session and restore session logs in the Veeam Agent command line interface.

To view Veeam Agent session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where:

`<session_id>` — ID of the backup job or restore session.

For example:

```
user@srv01:$ veeamconfig session log --id 0b72ef45-4c88-4639-b940-ad3828b1cd4e
2016-11-27 11:04:04 UTC {b141f32a-3e77-45a6-b55a-c100a1464d67} [info] Job started at 2016-11-27 14:04:04
2016-11-27 11:04:04 UTC {9b60ac03-2de0-4fe2-a00e-bec556d98ee8} [info] Starting volume restore
2016-11-27 11:04:07 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [processing] sdb
2016-11-27 11:04:15 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [info] sdb 512.0 kB at 58.6kB/s (0%)
2016-11-27 11:04:25 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [info] sdb 125.0 MB at 6.7MB/s (0%)
2016-11-27 11:04:35 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [info] sdb 238.5 MB at 8.3MB/s (1%)
...
2016-11-27 11:14:32 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [info] sdb 6.5GB at 10.7MB/s (92%)
2016-11-27 11:14:35 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [info] sdb 6.5GB at 10.6MB/s (97%)
2016-11-27 11:14:37 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [info] sdb 6.5GB at 10.6MB/s (100%)
2016-11-27 11:14:37 UTC {00add723-cbfa-4cc8-b299-d2349a051d6f} [warn] /dev/sdb has a duplicate filesystem UUID
2016-11-27 11:14:37 UTC {ced9af4a-6af1-475e-8ff8-8ec1325e18ec} [info] sdb restored 6.5GB at 10.6MB/s
2016-11-27 11:14:37 UTC {8b8742a2-1c80-4e14-bbf1-45a3612bc3a7} [info] Volume restore completed
```
Managing Configuration Database

You can perform the following operations with the Veeam Agent configuration database:

- Export configuration database to a configuration file.
- Import configuration database to Veeam Agent.
Exporting Configuration Database

You can export the Veeam Agent configuration database to a configuration file in the XML format. This may be useful, for example, if you want to change Veeam Agent settings by editing a configuration file or copy the Veeam Agent configuration to another computer.

To export the Veeam Agent configuration database, use the following command:

```bash
veeamconfig config export --file <path>
```

where:

- `<path>` — path to a configuration file to which you want to export the configuration database.

For example:

```bash
user@srv01:$ veeamconfig config export --file veeam/config.xml
```

NOTE

A directory in which you want to save the configuration file must exist in the file system.
Importing Configuration Database

You import the Veeam Agent configuration from a file in the XML format to the configuration database. This may be useful, for example, if you have changed Veeam Agent for Linux settings by editing a configuration file or want to apply configuration of another instance of Veeam Agent to Veeam Agent installed on your computer.

**NOTE**

Veeam Agent for Linux 5.0 does not support import of XML configuration files generated by earlier versions of Veeam Agent.

To import the Veeam Agent configuration database, use the following command:

```
veeamconfig config import --file <path>
```

where:

<path> — path to a configuration file from which you want to import the configuration database.

For example:

```
user@srv01:~$ veeamconfig config import --file veeam/config.xml
```
Exporting Product Logs

Veeam Agent offers a simple and convenient way to collect product logs and export them to an archive file. This operation may be required if you want to report an issue and need to attach log files to the support case.

When you export logs, Veeam Agent collects its log files and configuration files, exports them to an archive file in the `tar.gz` format and saves this archive file to a directory on the Veeam Agent computer.

You can perform the export logs operation in one of the following ways:

- **With the Veeam Agent control panel** — in this case, you can specify a directory to which Veeam Agent should save the log archive.

- **With the command line interface** — in this case, Veeam Agent will save the log archive to the current working directory.

**TIP**

When you perform restore operations after booting from the Veeam Recovery Media, Veeam Agent also saves restore logs to the backup location. Restore logs are saved to an archive file with the name `veeam_logs_<date>_<time>.tar.gz`. The archive is placed to the folder that contains the backup file from which you restored data.

If you encounter problems after restoring from the Veeam Recovery Media, it is recommended that you attach restore logs, as well as product logs collected by Veeam Agent, to the support case.
Exporting Logs with Control Panel

You can use the Veeam Agent control panel to collect and export product logs. When you export logs with the control panel, you can choose where Veeam Agent should save the resulting log archive.

To export logs:

1. Launch the Veeam Agent control panel with the `veeam` or `veeamconfig ui` command.
2. In the Veeam Agent control panel, press the 'm' key to open the **Miscellaneous** menu.
3. In the menu, select the **Export Logs** option and press **Enter**.

4. In the **Choose logs directory** window, specify a directory to which you want to save the log archive:
   a. In the **Choose logs directory** window, select the necessary directory and press **Enter**.
   b. Repeat the step 'a' until a path to the directory in which you want to save exported logs appears in the **Current directory** field.
   c. To create a new directory, switch to the **Create Dir** button, press **Enter**, then type a name for the new directory and press **Enter**.
   d. Switch to the **Ok** button and press **Enter**. Veeam Agent will collect logs, export them to an archive file with the name `veeam_logs_<date>_<time>.tar.gz`, and save the archive to the specified directory.
Choose log directory

Current directory: /home/user/veeam

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>../</td>
<td>dir</td>
<td>05-12-2016</td>
</tr>
</tbody>
</table>

[Create Dir] [OK] [Cancel]
You can use the Veeam Agent command line interface to collect and export product logs. To export logs, use the following command:

```
veeamconfig grablogs
```

Veeam Agent will collect logs, export them to an archive file with the name `veeam_logs_<date>_<time>.tar.gz`, and save the archive to the current working directory.

For example:

```
user@srv01:~$ veeamconfig grablogs
Logs have been exported successfully.
```
Getting Support

If you have any questions or want to share your feedback about Veeam Agent, you can use one of the following options:

- You can search for the information on the necessary subject in the current Veeam Agent for Linux User Guide.
- You can visit Veeam R&D Forums and share your opinion or ask a question.
- If you use Veeam Agent with an active license installed, you can visit Veeam Customer Support Portal and submit a support case to the Veeam Customer Support Team.
Using with Veeam Backup & Replication

If you have the Veeam backup infrastructure deployed in the production environment, you can use Veeam Agent for Linux together with Veeam Backup & Replication.

IMPORTANT

If you plan to use Veeam Agent for Linux 5.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 11a on the Veeam backup server. Veeam Agent for Linux 4.0 supports integration with Veeam Backup & Replication 11 or later as well.

NOTE

The subsequent sections describe tasks available for Veeam Agent operating in the standalone mode. For information about Veeam Agent management in Veeam Backup & Replication, see Veeam Agent Management Guide.
Tasks with Veeam Backup & Replication

Veeam Backup & Replication lets you perform a number of additional disaster recovery tasks and administrative actions with Veeam Agent backups. You can:

Data protection tasks

- Create Veeam Agent backups on backup repositories
- Create Veeam Agent backups on a Veeam Cloud Connect repository
- Copy Veeam Agent backups to secondary backup repositories
- Archive Veeam Agent backups to tape

Restore tasks

- Restore a Veeam Agent backup to a VMware vSphere VM
- Restore a Veeam Agent Backup to a Microsoft Hyper-V VM
- Restore files and folders from Veeam Agent backups
- Restore application items from Veeam Agent backups with Veeam Explorer for Oracle
- Restore disks from Veeam Agent backups
- Export Veeam Agent backups to standalone full backup files
- Restore data from Veeam Agent backups to Microsoft Azure
- Restore data from Veeam Agent backups to Amazon EC2

Administrative tasks

- Import Veeam Agent backups
- Enable and disable Veeam Agent backup jobs
- View Veeam Agent backup job statistics
- Delete Veeam Agent backup jobs
- Remove Veeam Agent backups
- View Veeam Agent backup statistics
- Configure global settings
- Assign roles to users
Setting Up User Permissions on Backup Repositories

To be able to store backups on a backup repository managed by a Veeam backup server, the user must have access permissions on this backup repository.

NOTE

If you plan to create backups on a Veeam backup repository with Veeam Agent backup jobs configured in Veeam Backup & Replication, you do not need to grant access permissions on the backup repository to users. In the Veeam Agent management scenario, to establish a connection between the backup server and protected computers, Veeam Backup & Replication uses a TLS certificate. To learn more, see the Configuring Security Settings section in the Veeam Agent Management Guide.

Access permissions are granted to security principals such as users and AD groups by the backup administrator working with Veeam Backup & Replication. Users with granted access permissions can target Veeam Agent backup jobs at this backup repository and perform restore from backups located on this backup repository.

Right after installation, access permissions on the default backup repository are set to Allow to everyone for testing and evaluation purposes. If necessary, you can change these settings.

After you create a new backup repository, access permissions on this repository are set to Deny to everyone. To allow users to store backups on the backup repository, you must grant users with access permissions to this repository.

To grant access permissions to a security principal:

1. In Veeam Backup & Replication, open the Backup Infrastructure view.
2. In the inventory pane, click one of the following nodes:

   - The Backup Repositories node — if you want to grant access permissions on a regular backup repository to Veeam Agent users.

   - The Scale-out Repositories node — if you want to grant access permissions on a scale-out backup repository to Veeam Agent users.
3. In the working area, select the necessary backup repository and click Set Access Permissions on the ribbon or right-click the backup repository and select Access permissions. If you do not see the Set Access Permissions button on the ribbon or the Access permissions command is not available in the shortcut menu, press and hold the Ctrl key, right-click the backup repository and select Access permissions.

4. In the Access Permissions window, specify to whom you want to grant access permissions on this backup repository:

- **Allow to everyone** — select this option if you want all users to be able to store backups on this backup repository. Setting access permissions to Everyone is equal to granting access rights to the Everyone Microsoft Windows group (Anonymous users are excluded). Note, however, this scenario is recommended for demo environments only.

- **Allow to the following accounts or groups only** — select this option if you want only specific users to be able to store backups on this backup repository. Click Add to add the necessary users and groups to the list.
5. If you want to encrypt Veeam Agent backup files stored on the backup repository, select the **Encrypt backups stored in this repository** check box and choose the necessary password from the field below. If you have not specified a password beforehand, click **Add** on the right or the **Manage passwords** link to add a new password. Veeam Backup & Replication will encrypt files on the backup repository side using its built-in encryption mechanism. To learn more, see Veeam Backup & Replication Documentation.

![Screen shot of Access Permissions](image-url)
Managing License

If you plan to use Veeam Agent for Linux with Veeam Backup & Replication, you must have a license installed in Veeam Backup & Replication. The license must have a total number of instances that is sufficient to protect Linux-based machines (servers and workstations) on which you plan to install Veeam Agent. The number of backup jobs configured in Veeam Agent does not consume the license. To learn more about per-instance licensing in Veeam Backup & Replication, see the Licensed Objects section in the Veeam Backup & Replication User Guide.

After Veeam Agent for Linux connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. By default, Veeam Agent operates in the Server edition. You can switch Veeam Agent to the Workstation edition manually if needed.

If one or more Veeam Agents operating in the Free edition are already connected to the backup server, they will start consuming the license immediately after the license is installed in Veeam Backup & Replication. Veeam Agents that exceed the license limit will not be able to back up data to the Veeam backup repository.

Veeam Agent keeps information about the license in its database. Information about the license is valid for 32 days. If Veeam Agent for Linux does not connect to Veeam Backup & Replication during this period, Veeam Backup & Replication will revoke its license.
Managing Instance Consumption by Veeam Agents

By default, Veeam Backup & Replication allows Veeam Agents to connect to the Veeam backup server and consume instances in the license. If you do not want Veeam Agents to consume instances, you can restrict instance consumption. After instance consumption is restricted, Veeam Agents will not be able to back up data to a Veeam backup repository.

To restrict instance consumption by Veeam Agents:

1. In Veeam Backup & Replication, from the main menu, select License.
2. In the License Information window, click the Instances tab.
3. On the Instances tab, clear the Allow unlicensed agents to consume instances check box.
4. Click Close.
Assigning License to Veeam Agent

After Veeam Agent connects to Veeam Backup & Replication, Veeam Agent automatically starts consuming the license. If the license allows Veeam Agent to operate in both the Workstation Server editions, Veeam Agent will operate in the Server edition.

You can also assign a license to Veeam Agent manually if needed. When you assign a license, you can select in which edition the licensed Veeam Agent will operate.

To assign a license:

1. In Veeam Backup & Replication, from the main menu, select **License**.
2. In the **License Information** window, select the **Instances** tab and click **Manage**.
3. In the **Licensed Instances** window, select the Veeam Agent to which you want to assign the license, click **Assign** and select the desired edition: **Workstation** or **Server**.
Viewing Licensed Agents and Revoking License

When Veeam Backup & Replication connects to the backup server, Veeam Backup & Replication applies a license to the Veeam Agent. You can view to which Veeam Agents the license is currently applied.

To view a list of licensed Veeam Agents:

1. In Veeam Backup & Replication, from the main menu, select License.
2. In the License Information window, select the Instances tab and click Manage.

In the list of licensed instances, Veeam Backup & Replication displays Veeam Agents that have established a connection with the backup server during a Veeam Agent backup job session.
Revoking License from Veeam Agents

You can revoke the license from some Veeam Agents and re-apply it to other protected workloads. License revoking can be helpful, for example, if you do not want to use some Veeam Agents with Veeam Backup & Replication anymore.

To revoke a license from the Veeam Agent:

1. In Veeam Backup & Replication, from the main menu, select License.
2. In the License Information window, select the Instances tab and click Manage.
3. In the Licensed Instances window, select the Veeam Agent from which you want to revoke the license and click Revoke. Veeam Backup & Replication will revoke the license from the Veeam Agent, and the license will be freed for other workloads protected with Veeam Backup & Replication.
The Veeam Agent from which you have revoked the license will become unable to connect to the Veeam backup server but will remain in the **Licensed Instances** list. To allow this Veeam Agent to create backups in the Veeam backup repository, select the Veeam Agent and click **Remove**. During the next backup job session, the Veeam Agent will connect to the Veeam backup server and start consuming the license.
Performing Data Protection Tasks

You can perform the following data protection tasks:

- Back up your data and store the resulting backup files on a backup repository managed by a Veeam backup server.
- Back up your data and store the resulting backup files on a Veeam Cloud Connect Repository.
- Copy Veeam Agent for Linux backups from the backup repository to a secondary backup repository with backup copy jobs.
- Archive Veeam Agent for Linux backups to tapes with backup to tape jobs.
Back Up to Backup Repositories

You can store backups created with Veeam Agent on backup repositories connected to Veeam backup servers. To do this, you must perform the following actions:

1. **Set up user permissions at the backup repository side.**
2. **Point the Veeam Agent for Linux backup job to the backup repository.**

**NOTE**

Consider the following:

- A Veeam Agent backup job can be started automatically upon the defined schedule or manually from the Veeam Agent computer. You cannot start, stop, retry or edit Veeam Agent backup jobs in the Veeam Backup & Replication console.
- If the user is granted restore permissions on the Veeam backup server, the user will be able to see all backups on the backup repository.
- The user who creates a Veeam Agent backup on the backup repository is set as the owner of the backup file. The backup file owner can access this file and restore data from it. If the user who is not the backup file owner needs to perform operations with the backup file, the user must have the Veeam Backup & Replication role that allows to perform these operations. To learn more about roles, see the **Roles and Users** section in the Veeam Backup & Replication User Guide.

Backup jobs targeted at the backup repository become visible in Veeam Backup & Replication under the **Jobs > Backup** node in the **Home** view. Backups created with Veeam Agent are available under the **Backups > Disk** node in the **Home** view.

The Veeam Backup Administrator working with Veeam Backup & Replication can manage Veeam Agent backup jobs and restore data from these backups. To learn more, see **Performing Restore Tasks** and **Performing Administration Tasks**.
Backing Up to Cloud Repositories

You can use Veeam Agent to create backups on cloud repositories provided to you by a Veeam Cloud Connect service provider. To do this, you must connect to the service provider and point the backup job to the cloud repository. To connect to the service provider, you can use credentials of the tenant or subtenant account that your provider or backup administrator communicated to you. To learn more, see Veeam Cloud Connect Repository Settings.
Veeam Agent Backups on Tenant Side

Backups created with Veeam Agent are available under the **Backups > Cloud** node in the **Home** view of the Veeam Backup & Replication console deployed on the tenant side.

The backup administrator working with Veeam Backup & Replication on the tenant side can manage Veeam Agent backups created on the cloud repository and restore data from such backups. To recover data from a Veeam Agent for Linux backup, you can export disks of the Veeam Agent computer as virtual disks. To learn more, see [Exporting Disks](#).

![Veeam Backup and Replication Console](image-url)
Veeam Agent Backups on Service Provider Side

The service provider can view information about backup and restore sessions performed by Veeam Agent users within the last 24 hours period. The list of sessions is available under the **Last 24 Hours** node in the **Cloud Connect** view of the Veeam Backup & Replication console deployed on the service provider side.

The service provider cannot perform restore tasks with Veeam Agent backups that are stored on the cloud repository.
Performing Backup Copy for Veeam Agent Backups

You can configure backup copy jobs that will copy backups created with Veeam Agent to a secondary backup repository.

Backup copy jobs treat Veeam Agent backups as usual backup files. The backup copy job setup and processing procedures practically do not differ from the same procedures for a backup copy job that processes VM backups. To learn more about backup copy jobs, see the Backup Copy section in the Veeam Backup & Replication User Guide.

Mind the following:

- You can process backups created by Veeam Agent only with backup copy jobs for Linux machine backups. You cannot add a Veeam Agent backup as an additional source of a backup copy job that processes VM backups.
- You can process backups created by Veeam Agent operating in the standalone mode only with backup copy jobs operating in the periodic copy mode. Immediate copy mode is not supported.
- You can process backups created by Veeam Agent operating in the managed mode with backup copy jobs operating in the periodic and immediate copy modes. Mind that for immediate copy mode, only Veeam Agent backups created by jobs managed by the backup server are supported.
- When mapping a backup copy job to a Veeam Agent backup, consider the limitations listed in the Backup File Mapping section in the Veeam Backup & Replication User Guide.
Restoring Data from Copies of Veeam Agent Backups

Backups copied to the secondary backup repository do not preserve user access permissions. At the same time, users who created backups do not have access permissions on these secondary repositories. For this reason, users cannot restore data from their backups residing in the secondary site.

To overcome this limitation, you can delegate the restore task to backup administrators who work with Veeam Backup & Replication. Backup administrators can use Veeam Backup & Replication to export data contained in backup files as virtual disks.
Archiving Veeam Agent Backups to Tape

You can configure backup to tape jobs to archive Veeam Agent backups to tape.

Backup to tape jobs treat Veeam Agent backups as usual backup files. The archiving job setup and processing procedures practically do not differ from the regular ones. To learn more about backup to tape jobs, see Veeam Backup & Replication Documentation.

**NOTE**

Keep in mind that in backup to tape job schedule, you cannot select the *After this job option* for a Veeam Agent job configured directly on a Veeam Agent computer.
Performing Restore Tasks

You can perform the following restore operations:

- Restore a Veeam Agent backup to a VMware vSphere VM
- Restore a Veeam Agent backup to a Microsoft Hyper-V VM
- Restore a Veeam Agent backup to a Nutanix AHV VM
- Restore data from Veeam Agent backups to Microsoft Azure.
- Restore data from Veeam Agent backups to Amazon EC2.
- Restore data from Veeam Agent backups to Google Cloud Platform.
- Restore individual files and folders from Veeam Agent for Linux backups.
- Restore application items from Veeam Agent backups with Veeam Explorer for Oracle.
- Export computer disks as VMDK, VHD or VHDX disks.
- Export restore points of Veeam Agent backups to standalone full backup files.
Restoring Veeam Agent Backup to vSphere VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a VMware vSphere VM in your virtualization environment. For Instant Recovery to a VMware vSphere VM, you can use Veeam Agent backups created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

A restored VMware vSphere VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM. These settings include:

- Amount of RAM
- Number of CPU cores
- Number of network adapters
- Network adapter settings
- BIOS UUID
  - If you do not want to preserve the backed-up machine UUID for a VMware vSphere VM, you can create a new UUID during the Instant Recovery configuration process.
- Number of disks and volumes
- Size of volumes

If you restore a Veeam Agent computer to a VMware vSphere VM, consider the following:

- Make sure that the target host has enough resources for a new VM. Otherwise, your VM will reduce the target host performance.

- If you restore a workload to the production network, make sure that the original workload is powered off.

- If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.
The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the Performing Instant Recovery of Workloads to VMware vSphere VMs section in the Veeam Backup & Replication User Guide.
Restoring Veeam Agent Backup to Hyper-V VM

You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Hyper-V VM in your virtualization environment. For Instant Recovery to a Hyper-V VM, you can use Veeam Agent backups created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

Mind that to restore to a Hyper-V VM, you must consider the Hyper-V limitations. To learn more, see this Microsoft article.

A restored Hyper-V VM has the same settings as a backed-up Veeam Agent computer. During the restore process, Veeam Backup & Replication retrieves settings of the Veeam Agent computer from the backup and applies them to the target VM.

**IMPORTANT**

If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of Instant Recovery for a Veeam Agent computer practically does not differ from the same procedure for a VM. The main difference from Instant Recovery is that you do not need to select the recovery mode, because Veeam Agent computers are always restored to a new location. To learn more, see the Performing Instant Recovery of Workloads to Hyper-V VMs section in the Veeam Backup & Replication User Guide.
You can use the Veeam Backup & Replication console to restore a Veeam Agent computer as a Nutanix AHV VM in your virtualization environment. For restore to Nutanix AHV, you can use backups created on the Veeam backup repository. You cannot perform this operation with Veeam Agent backups created on the Veeam Cloud Connect repository.

Mind that to restore to Nutanix AHV, you must install Enter value on the Veeam Backup & Replication server. To learn more, see the Installation section in the Veeam Backup for Nutanix AHV User Guide.

**IMPORTANT**

[For Veeam Agent backups of Linux computers] If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Nutanix AHV for a Veeam Agent computer practically does not differ from the same procedure for a VM. To learn more about restore to Nutanix AHV, see the Restoring VMs Using Veeam Backup & Replication Console section in the Veeam Backup for Nutanix AHV User Guide.
Restoring to Microsoft Azure

You can restore Linux machines from Veeam Agent backups to Microsoft Azure. You can use backups created on the Veeam backup repository. Only volume-level backups are supported.

If you restore a Veeam Agent machine to Microsoft Azure, consider the following:

- If you recover a EFI-based system to Microsoft Azure, Veeam Agent will restore a BIOS-based Generation 1 VM.

- Veeam Backup & Replication offers experimental support for generation 2 VMs within restore to Microsoft Azure feature. To learn more, see the Generation 2 VM Support section in the Veeam Backup & Replication User Guide.

- If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Microsoft Azure from a Veeam Agent backup practically is similar to the same restore procedure from a VM backup. To learn more, see the Restore to Microsoft Azure section in the Veeam Backup & Replication User Guide.
Restoring to Amazon EC2

You can restore Linux machines from Veeam Agent backups to Amazon EC2. You can use backups created on the Veeam backup repository. Only volume-level backups are supported.

**IMPORTANT**

If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Amazon EC2 from a Veeam Agent backup practically is similar to the same restore procedure from a VM backup. To learn more, see the Restore to Amazon EC2 section in the Veeam Backup & Replication User Guide.
Restoring to Google Cloud Platform

You can restore Linux machines from Veeam Agent backups to Google Cloud Platform. You can use backups created on the Veeam backup repository. Only volume-level backups are supported.

**IMPORTANT**

If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of restore to Google Cloud Platform practically does not differ from a regular one. To learn more about restore to Google Cloud Platform, see the Restore to Google Cloud Platform section in the Veeam Backup & Replication User Guide.
Restoring Files and Folders

You can restore individual files and folders from Veeam Agent backups.

When you perform the file-level restore procedure, Veeam Backup & Replication provides the following options for mounting disks of a Linux computer from the backup or replica:

- Mounting disks to a helper host — a target host where you want to restore files from the backup or any other Linux host.

- Mounting disks to a helper appliance — a helper VM required to mount Linux computer disks from the backup.

If you have selected to mount disks to a helper appliance, it is recommended that you add a vCenter Server and not a standalone ESXi host in the Veeam backup console. If Veeam Backup & Replication is set up to deploy a helper appliance on a standalone ESXi host, after Veeam Backup & Replication removes the helper appliance, the helper VM will be displayed in vCenter as orphaned.

To learn more about these options, see the Restore from Linux, Unix and Other File Systems section in the Veeam Backup & Replication User Guide.

The procedure of file-level restore from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. The difference is that you select a Veeam Agent backup instead of a VM backup in the File Level Restore wizard. To learn more, see the Guest OS File Recovery section in the Veeam Backup & Replication User Guide.
Restoring Application Items

You can use Veeam Explorer for Oracle to restore application items from backups created with Veeam Agent for Linux.

The procedure of application-item restore from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about the application-items restore procedure, see the Restoring Oracle Items section in the Veeam Backup & Replication User Guide.
Exporting Disks

You can restore computer disks from volume-level backups and convert them to disks of the VMDK, VHD or VHDX format.

During disks restore, Veeam Backup & Replication creates standard virtual disks that can be used by VMware vSphere and Microsoft Hyper-V VMs.

- When you restore a disk in the VMDK format, Veeam Backup & Replication creates a pair of files that make up the VM virtual disk: a descriptor file and file with the virtual disk content.
- When you restore a disk in the VHD/VHDX format, Veeam Backup & Replication creates a file of the VHD or VHDX format.

You can save converted disks locally on any server added to the backup infrastructure or place disks on a datastore connected to an ESXi host (for VMDK disk format only). VMDK disks can be restored as thin provision and thick provision disks:

- Disks restored to a datastore are saved in the thin provisioned format.
- Disks restored to a server are saved in the thick provisioned format.

VHD/VHDX disks are always restored as dynamically expanding.

Veeam Backup & Replication supports batch disk restore. For example, if you choose to restore 2 computer disks, Veeam Backup & Replication will convert them to 2 virtual disks and store these disks in the specified location.

**IMPORTANT**

Consider the following:

- If the backup from which you restore disks contains a Btrfs storage pool, during the disk restore process Veeam Backup & Replication will create a separate disk and restore the Btrfs pool to this disk.
- If the disk you want to restore contains an LVM volume group, Veeam Agent will restore the original disk and the LVM volume group as 2 separate disks. Among other things, this leads to the increase of the required storage space. For example, you restore a machine with 2 disks, and a separate LVM volume group is configured on each of these disks. In this case, Veeam Agent will restore 4 disks. The restored disks will consume storage space equal to the size of 2 original disks and 2 LVM volume groups from these disks.

The procedure of volume-level restore from a standalone Veeam Agent backup does not differ from the same procedure for a backup created with Veeam Agent that operates in the managed mode. To learn more, see the Exporting Disks section in the Veeam Agent Management Guide.
Exporting Restore Point to Full Backup File

You can restore data from a specific restore point in a Veeam Agent backup and export this data to a standalone full backup file. The procedure of Veeam Agent backup export does not differ from the same procedure for a VM. To learn more, see the Exporting Backups section in the Veeam Backup & Replication User Guide.
Performing Administration Tasks

You can manage Veeam Agent backup jobs and backups created with these jobs. Veeam Backup & Replication allows you to perform the following administration tasks:

• Import Veeam Agent backups
• Enable and disable Veeam Agent backup jobs
• Remove Veeam Agent backup jobs
• View Veeam Agent backup job statistics
• Remove Veeam Agent backups
• View Veeam Agent backup properties
• Configure global settings
• Assign roles to users
Importing Veeam Agent Backups

You may need to import a Veeam Agent backup in the Veeam Backup & Replication console in the following situations:

- The Veeam Agent backup is stored on a drive managed by another computer (not the Veeam backup server).
- The Veeam Agent backup is stored on a backup repository managed by another Veeam backup server.
- The Veeam Agent backup has been removed in the Veeam Backup & Replication console.

After importing, the Veeam Agent backup becomes available in the Veeam Backup & Replication console. You can restore data from such backup in a regular manner.

Before importing a backup, check the following prerequisites:

- The computer or server from which you plan to import the backup must be added to Veeam Backup & Replication. Otherwise you will not be able to access backup files.
- To be able to restore data from previous backup restore points, make sure that you have all incremental restore points in the same folder where the full backup file resides.

To import a Veeam Agent backup:

1. In Veeam Backup & Replication, click Import Backup on the Home tab.
2. From the Computer list, select the computer or server on which the backup you want to import is stored.
3. Click Browse and select the necessary VBM or VBK file. If you select the VBM file, the import process will be notably faster. It is recommended that you use the VBK files for import only if a corresponding VBM file is not available.
4. Click OK. The imported backup will become available in the Home view, under the Backups > Disk (imported) node in the inventory pane.
Importing Encrypted Backups

You can import Veeam Agent backups that were encrypted by Veeam Backup & Replication or Veeam Agent for Linux.

To import an encrypted backup file:

1. On the **Home** tab, click **Import Backup**.
2. From the **Computer** list, select the host on which the backup you want to import is stored.
3. Click **Browse** and select the VBM or VBK file.
4. Click **OK**. The encrypted backup will appear under the **Backups > Disk (encrypted)** node in the inventory pane.
5. In the working area, select the imported backup and click **Specify Password** on the ribbon or right-click the backup and select **Specify password**.
6. In the **Password** field, enter the password for the backup file. If you changed the password one or several times while the backup chain was created, you need to specify the latest password. For Veeam Agent backups, you can use the latest password to restore data from all restore points in the backup chain, including those restore points that were encrypted with an old password.

If you enter correct password, Veeam Backup & Replication will decrypt the backup file. The backup will be moved under the **Backups > Disk (imported)** node in the inventory pane.
Enabling and Disabling Veeam Agent Backup Jobs

You can disable and enable Veeam Agent backup jobs in Veeam Backup & Replication.

When you disable the job, you prohibit the user to store the resulting backup to the backup repository. If the user starts a disabled job manually or the job starts by schedule, the job session will fail and report the "Job is disabled on backup server" error. To let Veeam Agent store backups to the backup repository again, you must enable the disabled job.

To disable or enable the scheduled backup job in Veeam Backup & Replication:

1. In Veeam Backup & Replication, open the Home view.
2. In the inventory pane, click the Jobs node.
3. Select the necessary job in the working area and click Disable on the ribbon or right-click the necessary job in the working area and select Disable. To enable the disabled job, click Disable on the toolbar or right-click the job and select Disable once again.
Deleting Veeam Agent Backup Jobs

You can delete Veeam Agent backup jobs.

When you delete a Veeam Agent backup job, Veeam Backup & Replication removes all records about the job from its database and console. When the user starts a new Veeam Agent backup job session manually or the job starts automatically by schedule, the job will appear in the Veeam Backup & Replication console again, and records about a new job session will be stored to the Veeam Backup & Replication database. To remove the job permanently, you must delete the job and unassign access rights permissions for this user from the backup repository.

To remove a job:

1. In Veeam Backup & Replication, open the Home view.
2. In the inventory pane, click the Jobs node.
3. Select the necessary job in the working area and click Delete on the toolbar or right-click the necessary job in the working area and select Delete.
Viewing Veeam Agent Backup Job Statistics

You can view statistics about Veeam Agent backup jobs in the Veeam Backup & Replication console. Veeam Backup & Replication displays statistics for Veeam Agent backup jobs in the similar way as for regular backup jobs. The difference is that the list of objects included in the job contains a Veeam Agent machine instead of one or several VMs.

To view Veeam Agent backup job statistics:

1. In Veeam Backup & Replication, open the Home view.
2. In the inventory pane, click the Jobs node.
3. In the working area, select the necessary Veeam Agent backup job and click Statistics on the ribbon or right-click the job and select Statistics.
Removing Veeam Agent Backups

You can remove Veeam Agent backups from Veeam Backup & Replication or permanently delete Veeam Agent backups from the Veeam backup repository.
Removing from Configuration

When you remove a Veeam Agent backup from configuration, Veeam Backup & Replication deletes all records about the backup from its database and console. The actual backup files remain on the backup repository. You can import the backup to the Veeam Backup & Replication at any time later and restore data from it. To learn more, see Importing Veeam Agent for Linux Backups.

To remove a Veeam Agent backup from configuration:

1. In Veeam Backup & Replication, open the Home view.
2. In the inventory pane, click Disk under the Backups node.
3. In the working area, expand the Agents node, select the necessary backup and click Remove from > Configuration on the toolbar or right-click the backup and select Remove from configuration.
Removing from Veeam Backup Repository

When you remove a Veeam Agent backup from the Veeam backup repository, Veeam Backup & Replication deletes all records about the backup from its database and console. The actual backup files are removed from the backup repository, too.

To remove a Veeam Agent backup from the backup repository:

1. In Veeam Backup & Replication, open the Home view.
2. In the inventory pane, click Disk under the Backups node.
3. In the working area, expand the Agents node, select the necessary backup and click Remove from > Disk on the toolbar or right-click the backup and select Delete from disk.
Viewing Veeam Agent Backup Properties

You can view statistics about Veeam Agent backups.

To view Veeam Agent backup statistics:

1. In Veeam Backup & Replication, open the Home view.
2. In the inventory pane, click Disk under the Backups node.
3. In the working area, expand the Agents node, select the necessary backup and click Properties on the toolbar or right-click the backup and select Properties.
Configuring Global Settings

Global settings configured on the Veeam backup server apply to Veeam Agent backup jobs as well. You can:

- Configure network throttling settings so that Veeam Agent backup job does not consume all network resources.
- Configure global email settings to get alerted about the Veeam Agent backup job results.

To learn more, see Veeam Backup & Replication Documentation.
Assigning Roles to Users

User roles configured on the Veeam backup server apply to Veeam Agent backup jobs as well. To learn more, see the Roles and Users section in the Veeam Backup & Replication User Guide.
Appendix A. Requirements for veeam-nosnap

Starting from build 5.0.1.4493, you can use a `veeam-nosnap` package to install Veeam Agent for Linux. This package allows Veeam Agent to operate without `veeamsnap` kernel module.

The `veeam-nosnap` package can be useful in the following cases:

- You do not want to install kernel sources and compilers on your computer.
- You want to use third-party tools to create data snapshots.
- You want to perform bare metal restore, but Veeam Recovery Media does not work with your computer. In this case you can install the `veeam-nosnap` package on LiveCD of your choice and access the Veeam recovery UI.
- You want to back up machines used as cluster nodes and these cluster nodes consist of LVM logical volumes or volume groups. Veeam Agent can perform this operation because the `veeam-nosnap` package supports native LVM snapshots.

Before you install Veeam Agent using the `veeam-nosnap` package, consider the following limitations:

- The `veeam-nosnap` package has an experimental support status. For details about experimental support, see this Veeam KB article.
- The RAM-based changed block tracking (CBT) mechanism is not supported. As a result, if you plan to back up a significant amount of data, the backup will require greater time.
- Veeam Agent can create a snapshot of LVM logical volumes and Btrfs subvolumes. To back up data that resides on other file systems and volumes, you can use only file-level backup in the snapshot-less mode. For details, see Snapshot-Less File-Level Backup.
- For a successful backup, Veeam Agent requires unallocated extents on volume groups.
- For a successful bare metal restore, all disks of the Veeam Agent computer you want to restore must be available in the backup.
# System Requirements for veeam-nosnap

If you plan to use the veeam-nosnap package to install Veeam Agent, the protected Linux computer meet requirements listed in the table below. To learn about system requirements for Veeam Agent installed using the veeamsnap kernel module, see System Requirements.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| **Hardware**  | CPU: x86-64 processor (i386 or later).  
Memory: 1 GB RAM or more. Memory consumption varies depending on the backup type and the total amount of backed-up data.  
Disk Space: 100 MB free disk space for product installation.  
Network: 10 Mbps or faster network connection to a backup target.  
System firmware: BIOS or UEFI.  
Disk layout: MBR or GPT.  
For virtual machines: Only full virtualization type is supported. Containers and paravirtualized instances are not supported. Oracle VM virtual machines are supported with limitations. |
| **OS**        | **Important!** Check considerations and limitations that apply to the list of supported OSes.  
Linux kernel version 2.6.32 or later is supported.  
Both 64-bit and 32-bit versions (if applicable) of the following distributions are supported:  
- Debian 9.0 – 11.1  
- RHEL 6.0 – 8.5  
- CentOS 7.0 – 8.5  
- Oracle Linux 6 – 8.5 (RHCK)  
- Oracle Linux 6 (starting from UEK R2) – Oracle Linux 8 (up to UEK R6 U2, kernel version 5.4.17-2102) |
### File System

**Important!** Check [considerations and limitations](#) that apply to the list of supported file systems.

Veeam Agent for Linux supports consistent snapshot-based data backup for the following file systems:

- **LVM**
  
  LVM volumes protected with encryption software such as dm-crypt are supported.

- **Btrfs (for OSes that run Linux kernel 3.16 or later)**
  
  Btrfs is supported only if it resides directly on a physical device with no additional abstraction layers (such as LVM, software RAID, dm-crypt and so on) below or above it.

Data that resides on other file systems and volumes (including NFS and SMB shares) can be backed up using the snapshot-less mode. For details, see [Snapshot-Less File-Level Backup](#).

### Software

**Important!** Check [considerations and limitations](#) that apply to the list of supported components.

Protected computer must have the following components installed:

- **perl**
- **linux-headers** (for Debian-based systems)
- **libudev**
- **libacl**
- **libattr**
- **lvm2**
- **libfuse**
- **dmidecode**
- **libmysqlclient**
- **libpq5**
- **efibootmgr** (for UEFI-based systems)
- **isolinux** (for Debian-based systems)
- **syslinux** (for RedHat-based systems)
- **btrfs-progs** (for backup of Btrfs file system)
- **mksquashfs** (for custom Veeam Recovery Media)
- **unsquashfs** (for custom Veeam Recovery Media)
- **wget** (for custom Veeam Recovery Media)
- **xorriso** (for custom Veeam Recovery Media with EFI support)

For file system indexing, the following utilities are required: `tar`, `mlocate` and `gzip`. 
Considerations and Limitations

**OS**

- Linux kernel version 2.6.32 or later is supported as long as you use kernels supplied by your distribution with the following limitation: Linux kernel 2.6.32-754.6.3 in RHEL and Oracle Linux (RHCK) is not supported.

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

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

- RHEL, CentOS and Oracle Linux (RHCK) are supported up to certain kernel versions. For details, see this Veeam KB article.

**File System**

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

- File-level backup has the following limitations:
  - Total size of all file systems must not exceed 218 TB.
  - Size of a file must not exceed 16 TB.
  - Name of a file must not be larger than 254 bytes.

  Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more.

- Veeam Agent supports backup of extended attributes with the following limitations:
  - Veeam Agent backs up extended attributes only with the following public namespaces: system, security, trusted, and user.
  - All extended attribute names and values of a file must not exceed 4096 bytes (size of a default ext4 file system block). Veeam Agent does not back up attributes exceeding the limit.
    
    For the kernel version 4.13 or later, if a value of extended attribute exceeds the limit, Veeam Agent uses the ea_inodes feature. Backups created using the ea_inodes feature cannot be mounted on kernel versions up to 4.12.

- Backup of file and directory attributes (for example, a – append only, c – compressed, and so on) is not supported.

- Each volume included in a backup must have a unique UUID.

- You cannot back up an entire system image or specific volumes of machines used as cluster nodes. Only **snapshot-less file-level backup** of cluster nodes is supported. That includes backup of machines that use shared disks, clustered file systems or clustered LVM.

- Certain limitations for Dell PowerPath configuration apply. To learn more, see this Veeam KB article.

- BFQ I/O scheduler is not supported.

- Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files.
Software

**IMPORTANT**

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

- Version of the `linux_headers` package (for Debian-based systems) varies according to the Linux kernel version that you use.
- The `dmidecode` package is required for Veeam Agent management — a valid BIOS UUID must be obtainable either from `dmidecode | grep -i uuid` or from `/sys/class/dmi/id/product_uuid`. Each Veeam Agent that consumes a license installed in Veeam Backup & Replication must have a unique BIOS UUID. If a valid UUID cannot be obtained, Veeam will generate it automatically.
- The `libmysqlclient` package is required to process MySQL database system located on the Veeam Agent server. For details, see [Backup of MySQL Database](#). Package version varies according to the MySQL database system version that you use.
- The `libpq` package is required to process PostgreSQL database system located on the Veeam Agent server. For details, see [Backup of PostgreSQL Database](#).
- The `btrfs-progs` package version 3.16 or later is required.
Backup Source

Any file systems and devices that are accessible from the host OS. To learn about limitations, see File System.
Backup Target

Backup can be performed to the following types of storage:

- Local (internal) storage of the protected computer (not recommended).
- Direct attached storage (DAS), such as USB, eSATA or Firewire external drives.
- Network Attached Storage (NAS) able to represent itself as SMB (CIFS) or NFS share. Requires `cifs-utils` or `nfs-utils` packages to be installed on the Veeam Agent for Linux computer, depending on a network storage type.
- Veeam Backup & Replication 11 or later backup repository (including deduplication appliances).
- Veeam Cloud Connect 11 or later cloud repository.
Network

Consider the following:

- Veeam Agent for Linux should be able to establish a direct IP connection to the Veeam Backup & Replication server. Thus, Veeam Agent for Linux cannot work with Veeam Backup & Replication that is located behind the NAT gateway.

- Domain names of the Veeam Agent computer, Veeam Backup & Replication server and other servers in the Veeam backup infrastructure must be resolvable into IPv4 addresses.