© 2022 Veeam Software.

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

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

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

CONTACTING VEEAM SOFTWARE ................................................................. 7
ABOUT THIS DOCUMENT ........................................................................... 8
OVERVIEW .................................................................................................. 9
  Solution Architecture ................................................................................ 10
  Standalone and Managed Operation Modes .......................................... 11
  Data Backup ............................................................................................ 12
    File-Level Backup .................................................................................... 13
    WPAR Backup .......................................................................................... 15
  How Backup Works .................................................................................... 16
  Backup Job .................................................................................................. 17
  Backup Chain .............................................................................................. 19
  Backup Repository ...................................................................................... 23
  Data Restore ............................................................................................... 24
  Veeam Recovery Media .............................................................................. 25
  Integration with Veeam Backup & Replication ......................................... 26
MANAGING VEEAM AGENT IN VEEAM BACKUP & REPLICATION ................................................. 27
PLANNING AND PREPARATION ................................................................. 28
  System Requirements ................................................................................ 29
    RAM Requirements for Large Numbers of Files ..................................... 31
  Used Ports .................................................................................................. 32
INSTALLATION AND CONFIGURATION ...................................................... 33
  Before You Begin ...................................................................................... 34
    Installing Prerequisite Software .......................................................... 35
  Installing Veeam Agent for IBM AIX ....................................................... 36
  Managing Veeam Agent Operation Mode ................................................. 37
    Viewing Operation Mode .......................................................................... 38
    Resetting to Standalone Operation Mode ............................................... 39
    Connecting to Veeam Backup & Replication ........................................... 40
    Synchronizing with Veeam Backup Server ............................................ 41
    Exporting Logs to Veeam Backup Server ............................................... 42
    Upgrading Product ................................................................................... 43
    Uninstalling Product ............................................................................... 45
    Granting Permissions to Users ............................................................... 46
GETTING STARTED ..................................................................................... 47
GETTING TO KNOW USER INTERFACE .................................................... 48
  Viewing Help ............................................................................................... 50
**LICENSING**

License Agreement ............................................................................................................................................... 52
Managing License ............................................................................................................................................... 53
  Accepting License Agreements ......................................................................................................................... 54
  Installing License ........................................................................................................................................... 55
  Viewing License Information ............................................................................................................................. 56
  Removing License ........................................................................................................................................ 58

**PERFORMING BACKUP**

Creating Veeam Recovery Media ...................................................................................................................... 60
Creating Backup Jobs ......................................................................................................................................... 61
Configuring Backup Schedule ............................................................................................................................ 67
  Specifying Backup Schedule ............................................................................................................................... 68
  Enabling Backup Schedule ................................................................................................................................. 70
  Viewing Backup Schedule ................................................................................................................................ 71
  Disabling Backup Schedule ................................................................................................................................. 72
Configuring Active Full Backup Schedule ........................................................................................................... 73
  Specifying Active Full Backup Schedule ........................................................................................................... 74
  Enabling Active Full Backup Schedule ............................................................................................................ 76
  Viewing Active Full Backup Schedule ................................................................................................................ 77
  Disabling Active Full Backup Schedule .......................................................................................................... 78
Starting and Stopping Backup Jobs ......................................................................................................................... 79
  Starting Backup Job .................................................................................................................................... 80
  Creating Active Full Backups .............................................................................................................................. 81
  Stopping Backup Job ..................................................................................................................................... 82
Managing Backup Jobs .......................................................................................................................................... 83
  Viewing List of Backup Jobs ............................................................................................................................... 84
  Viewing Backup Job Settings .............................................................................................................................. 85
  Editing Backup Job Settings ............................................................................................................................... 87
  Deleting Backup Job .................................................................................................................................... 91
Managing Backup Repositories ............................................................................................................................. 92
  Creating Backup Repository ............................................................................................................................... 93
  Viewing List of Backup Repositories ................................................................................................................ 94
  Editing Backup Repository ................................................................................................................................. 95
  Rescanning Backup Repository ........................................................................................................................ 97
  Deleting Backup Repository .............................................................................................................................. 98
Managing Veeam Backup & Replication Servers .................................................................................................. 99
  Connecting to Veeam Backup Server ................................................................................................................ 100
  Viewing List of Veeam Backup Servers ............................................................................................................ 102
  Viewing Backup Server Details ........................................................................................................................ 103
# Using with Veeam Backup & Replication

- **Perfoming Restore**
  - **Bare-Metal Recovery**
    - Before You Begin
    - Booting from Veeam Recovery Media
    - Restoring Data with Recovery Wizard
    - Restoring Data in Command Line Interface
  - **Restoring Files and Directories**
    - Before You Begin
    - Restoring from Backup
    - Restoring from Restore Point
  - Restoring Data from Encrypted Backups

- **Reporting**
  - Viewing Session Status
  - Viewing Session Logs

- **Managing Configuration Database**
  - Configuration Format
  - Exporting Configuration Database
  - Importing Configuration

- **Exporting Product Logs**

- **Getting Support**

- **Using with Veeam Backup & Replication**
  - Setting Up User Permissions on Backup Repositories
  - Managing License
    - Managing Instance Consumption by Veeam Agents
    - Viewing Licensed Agents and Revoking License
  - Performing Data Protection Tasks
    - Backing Up to Backup Repositories
    - Performing Backup Copy for Veeam Agent Backups
    - Archiving Veeam Agent Backups to Tape
  - Performing Restore Tasks
Restoring Files and Directories ............................................................................................................. 206
Exporting Disks ........................................................................................................................................ 207
Exporting Restore Point to Full Backup File ........................................................................................... 214
Performing Administration Tasks .................................................................................................................. 215
Importing Veeam Agent Backups .................................................................................................................... 216
Enabling and Disabling Backup Jobs ............................................................................................................ 218
Viewing Veeam Agent Backup Job Statistics ............................................................................................... 219
Deleting Veeam Agent Backup Jobs ............................................................................................................ 220
Removing Veeam Agent Backups .................................................................................................................. 221
Viewing Veeam Agent Backup Properties ..................................................................................................... 223
Configuring Global Settings ......................................................................................................................... 224
Assigning Roles to Users .............................................................................................................................. 225
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 main features of Veeam Agent for IBM AIX 4.0.

Intended Audience

The user guide is intended for anyone who wants to use Veeam Agent for IBM AIX to protect their computer.
Overview

Veeam Agent for IBM AIX is a data protection and disaster recovery solution for machines running the IBM AIX operating system.

Veeam Agent for IBM AIX can be used by IT administrators who run IBM AIX infrastructure. The solution runs inside the IBM AIX machine OS and can be installed in the root file system of the IBM AIX machine (LPAR) or in a specific WPAR.

Veeam Agent for IBM AIX lets you back up directories and files of your IBM AIX machine. 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 restore the necessary data from backups to its original location or a new location.

Veeam Agent for IBM AIX integrates with Veeam Backup & Replication. Backup administrators who work with Veeam Backup & Replication can perform advanced tasks with Veeam Agent for IBM AIX backups: restore data from backups, perform tasks with backup jobs configured in Veeam Agent for IBM AIX and backups created with these jobs.
Solution Architecture

Veeam Agent for IBM AIX is set up on an IBM AIX machine whose data you want to protect.

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

- **Veeam Agent for IBM AIX Service (veeamservice)** is a service responsible for managing all tasks and resources in Veeam Agent for IBM AIX. The `veeamservice` component is managed by the `veeamsvc` subsystem that is registered in the IBM AIX OS upon the product installation. The subsystem is started automatically when you start the OS, or after it is incorrectly stopped.

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

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

- **SQLite** database engine used to store Veeam Agent for IBM AIX configuration data. SQLite requires only few files to install and takes little resources to run on an IBM AIX OS.
Standalone and Managed Operation Modes

Veeam Agent for IBM AIX can operate in two modes: standalone mode and managed mode.

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

  For Veeam Agent for IBM AIX 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 IBM AIX operating in the standalone mode only.

- **Managed mode** – in this mode, Veeam Agent for IBM AIX operates under control from Veeam Backup & Replication. To use Veeam Agent operating in the managed mode, you must create a protection group for pre-installed Veeam Agents in Veeam Backup & Replication and export Veeam Agent installation packages and configuration file. After that, you must install Veeam Agent and apply the configuration file on each machine whose data you want to protect.

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

  Features and limitations of Veeam Agent for IBM AIX 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 Veeam 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.

Veeam Agent for IBM AIX copies backed-up data at the file level. It retrieves data that you choose to back up and stores it in backup files in the target location. To learn more, see File-Level Backup.

You can set up Veeam Agent for IBM AIX 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 specific directories and files of your machine.

You can set up Veeam Agent for IBM AIX to create multiple backups — with individual backup scope, upon individual schedule or in different locations.

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

- Removable storage device
- Local machine drive
- NFS or SMB (CIFS) network shared folder
- Backup repository managed by a Veeam backup server
File-Level Backup

Veeam Agent for IBM AIX copies backed-up data at the file level. The file-level backup captures data of individual directories and files on the machine. You can use the file-level backup to restore files and directories that you have added to the backup scope.

With Veeam Agent for IBM AIX, 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 (except those subdirectories that you excluded from the backup) and files in these directories.

- You can include or exclude specific files 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. Files whose names match the specified exclude masks will not be present in the backup.
By default, Veeam Agent for IBM AIX excludes the following file systems from the backup: AHAFS, AutoFS, CacheFS, CDRFS, CIFS, FTPFS, NameFS, NFS, PMEMFS, PROCFS, SFTPFS, SMBFS, SSHFS, STNFS, UDFS, VXODM. If necessary, you can include in the backup mount points pertaining to the following file systems: NFS, SMBFS, SSHFS, FTPFS, SFTPFS. To do this, you must specify mount points explicitly in the backup job settings.

**NOTE**

The NameFS file system is excluded from the backup only in case Veeam Agent is installed and performs backup in the LPAR. The file system is not excluded from the backup in case Veeam Agent is installed and performs backup in a WPAR.

**Limitations for File-Level Backup**

- Veeam Agent for IBM AIX does not back up extended attributes and ACLs of backed-up files and directories.
- Sparse files are not supported. Veeam Agent for IBM AIX backs up and restores sparse files as regular files.
- Veeam Agent for IBM AIX does not support JFS2 snapshots.
WPAR Backup

You can use Veeam Agent for IBM AIX to back up data pertaining to individual WPARs configured in the IBM AIX OS. Veeam Agent offers two scenarios for WPAR backup.

Scenario 1: backup from the LPAR

You can install Veeam Agent in the LPAR and configure the backup job to include directories with files pertaining to a WPAR whose data you want to back up.

This scenario has the following requirements:

- The root account of the host system (LPAR) must have access to the file system of the WPAR.
- The LPAR must own the storage device that contains the file system of the WPAR. If the WPAR whose files you want to back up has a storage device allocated to it, the file systems on such device are automatically excluded from the backup.

If the global environment does not meet either of these requirements, use Scenario 2.

**NOTE**

It is not required to stop the backed-up WPAR before the backup process starts. To ensure consistency of the backed-up data, you can use custom scripts, for example, to stop and start a database during backup.

To learn more about custom scripts, see Backup Job Scripts.

Scenario 2: backup from a WPAR

You can install Veeam Agent in the WPAR whose data you want to back up and specify which files and directories to back up in the same way as in case you back up data of the LPAR.

**NOTE**

- You must install the product license in each Veeam Agent installed in each WPAR.
- You cannot use backups created from within a WPAR for bare-metal recovery because such backups do not contain the required system metadata file.
How Backup Works

During backup, Veeam Agent for IBM AIX performs the following operations:

1. Veeam Agent for IBM AIX creates a backup file in the target location.

2. In the backup file, Veeam Agent for IBM AIX creates a virtual disk. The disk contains a volume with the ext4 file system.

3. Veeam Agent for IBM AIX reads data that you selected for backup, compresses it and copies it to the target location. As part of the file backup process, Veeam Agent performs the following steps:
   a. For each file included in the backup, creates a target file in the volume inside the backup file.
   b. Opens the source and target files.
   c. Reads data from the source file and transfers it to the target file.
   d. Closes the source and target files.

   [For incremental backup] To detect files that changed on the Veeam Agent machine 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. During incremental backup, Veeam Agent copies only new or modified files to the target location. To learn about full and incremental backup, see Backup Chain.

Veeam Agent for IBM AIX locks backed-up files during the backup process. However, Veeam Agent does not track whether backed-up data changes in the original location since the time when the backup process started. For example, if a new file appears in a directory included in the backup after the backup process starts, Veeam Agent will not copy this file to the target location. To make sure that data in the backup is in the consistent state, it is recommended that you do not perform write operations in the file system that contains the backed-up data until the backup process completes.
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.

In Veeam Agent for IBM AIX, you can configure several backup jobs with different settings. For example, 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.

Backup Schedule

Veeam Agent for IBM AIX 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 user accounts of the IBM AIX OS. For every backup job, Veeam Agent for IBM AIX creates a record in the `crontab` configuration file of the root account. As a result, Veeam Agent for IBM AIX can start a backup job automatically regardless of the currently running user session.

You can define schedule for a job in Veeam Agent for IBM AIX or edit the `crontab` record 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 IBM AIX to run custom pre-job and post-job scripts within the backup job session. For example, you may want to use custom scripts to configure email notifications about jobs performed by Veeam Agent or to create a snapshot of the file system to ensure consistency of the backed-up data.

Script settings are enabled at the job level: you can specify individual scripts for each job configured in Veeam Agent for IBM AIX.

Scripts must be created beforehand. You must specify paths to them in the job settings. Veeam Agent for IBM AIX supports scripts in the SH file format.

Veeam Agent for IBM AIX executes the pre-job script directly before the backup job starts. After the backup job completes, Veeam Agent for IBM AIX executes the post-job script.

Veeam Agent for IBM AIX starts the backup job regardless of the pre-job script result. If the pre-job script fails to execute, Veeam Agent for IBM AIX will always start the backup job. Then, after the backup job completes, Veeam Agent for IBM AIX 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 for IBM AIX 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 for IBM AIX also displays a warning in the job session.

File System Indexing

You can instruct Veeam Agent for IBM AIX to create an index of files and directories located on the Veeam Agent machine 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.
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 IBM AIX will nevertheless index all files located in the directories that have been selected for backup.

For example, you have included the /home directory in the backup and specified the * .pdf exclusion mask. The --indexall 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

The IBM AIX system must have the mlocate utility installed. The utility is provided along with Veeam Agent in the product installation media.

NOTE

File system indexing is optional. If you do not enable this option in the backup job settings, you will still be able to perform 1-click restore from the backup created with such backup job. For more information, see the Preparing for File Browsing and Restore section in the Veeam Backup Enterprise Manager User Guide.
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 IBM AIX performs full backup. Veeam Agent for IBM AIX copies all data that you have chosen to back up 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 IBM AIX 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 modified files, 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 IBM AIX 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 machine on which the backup was performed, 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 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 IBM AIX retains the number of latest restore points defined by the user. During every backup job session, Veeam Agent 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 IBM AIX 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 uses the following rotation scheme:

1. During every backup job session Veeam Agent for IBM AIX 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 IBM AIX transforms the backup chain. As part of this process, it performs the following operations:
   a. Veeam Agent for IBM AIX 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 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 IBM AIX lets you create active full backups.

When Veeam Agent for IBM AIX 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 IBM AIX 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 (on specific week days or specific day of a month). To learn more, see Creating Active Full Backups and Configuring Active Full Backup Schedule.

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 for IBM AIX 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.

Note that if the job is not scheduled to run automatically, Veeam Agent will not create active full backups automatically as well.

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 IBM AIX 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 IBM AIX will not delete the previous backup chain. Veeam Agent 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.

Note that if the backup job is set up to create periodic active full backups, Veeam Agent for IBM AIX will never transform the backup chain. Instead, Veeam Agent will always wait for at least one full backup file plus the necessary number of incremental backup files to be created. After that, Veeam Agent will delete the obsolete active full backup file and its dependent incremental backup files. In this example, Veeam Agent will delete the previous backup chain every Saturday. 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 most of the time.

In contrary, in a situation where you manually create an active full backup once, Veeam Agent for IBM AIX will treat the active full backup in the same way as a regular full backup. If some restore point becomes obsolete, Veeam Agent 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 will remove the earliest incremental backup file from the chain as redundant.
A backup job configured in Veeam Agent for IBM AIX 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 as 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 11a (build 11.0.1.1261) or later backup repository (Veeam Cloud Connect repositories are not supported)

**IMPORTANT**

[For local storage] A backup repository should be created on a separate volume from a volume that contains data you plan to back up.

The way you work with backup repositories depends on where you want to store backup files.

- If you want to keep backup files on a local storage, remote storage or in a network shared folder, you must create a backup repository. You must perform this task in advance, before you configure the backup job. When you create a backup repository, you specify a local directory in which Veeam Agent for IBM AIX will create backup files and a name for the backup repository. To learn more, see Creating Backup Repository.

  If you back up your data to a remote storage or network shared folder, you must mount this remote location to the specified local directory before you start a backup job. Veeam Agent for IBM AIX does not check whether the remote backup location is mounted to the local directory. If the remote location is not mounted, Veeam Agent will create a new backup chain directly in the local directory. Besides, if the directory to which the remote location should be mounted resides on the backed-up volume, a backup job may fail.

- If you want to keep backup files on a Veeam backup repository, you do not need to create repositories. Before configuring the backup job, you must connect to the Veeam backup server. Veeam Agent will obtain information about backup repositories managed by this backup server. To learn more, see Connecting to Veeam Backup Server.

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.
Data Restore

File-Level Restore

If you have lost or modified files and directories on your machine by mistake, you can restore a copy of the necessary objects from the backup.

Veeam Agent does not simply extract files and directories from the backup file. Instead, Veeam Agent mounts backup file content to the mount point directory in the machine’s file system. You can specify a directory in which Veeam Agent will mount the backup content.

After the backup content is mounted, you can use IBM AIX 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.

Bare-Metal Recovery

If the operating system on your machine fails to start, you can perform bare-metal recovery of your system. To do this, you must have Veeam Recovery Media that you created on your functional system and a full backup with system metadata.

At the first stage of bare-metal recovery, you must boot your machine from Veeam Recovery Media which launches the recovery image OS in your machine RAM. You then import the backup file into the Veeam Agent database, select restore method and run the restore. Veeam Agent erases all data on the machine, reconstructs partition structure using system metadata, restores data from the backup and creates the boot loader.

Before you reboot the machine upon successful bare-metal recovery, you may need to restore additional data from another backup. To do this, you can use the standard file-level restore functionality. Veeam Agent mounts the backup file to the file system of the recovery image OS. After that, you can copy the necessary files or directories to a desired location.

If the recovery is successful, upon reboot the system loads the recovered OS and data from the machine’s hard drive.
Veeam Recovery Media

Veeam Agent for IBM AIX lets you create Veeam Recovery Media — a recovery image of your IBM AIX OS that provides an alternative way to boot the machine in the event of a disaster.

The recovery image contains the IBM AIX OS with limited functionality. It includes the IBM AIX kernel and a set of IBM AIX utilities necessary to boot the machine and perform basic administration tasks. If the OS installed on the machine fails to start, you can boot the recovery image OS.

To create Veeam Recovery Media, use the `veeamconfig createIso` command in Veeam Agent for IBM AIX. To learn more, see Creating Veeam Recovery Media.

Considerations and Limitations

- We recommend using Veeam Recovery Media to restore your system to the original hardware.

  If you want to restore your system to a different machine, keep in mind the hardware setup of the target machine must be exactly the same as that of the original machine. Otherwise, the system may fail to boot due to mismatches or missing drivers. These settings include:

  - Amount of RAM
  - Number and type of CPU cores
  - Number and type of network adapters
  - Number of disks and volumes
  - Block size of disks
  - Size of volumes
  - HDD Controllers

- When you boot the machine from Veeam Recovery Media, the recovery environment contains a new installation of Veeam Agent for IBM AIX with limited functionality. Veeam Agent for IBM AIX does not retain any user-defined configuration settings.

  For more information on the prerequisites and limitations of bare-metal recovery in Veeam Agent for IBM AIX 4.0, see Before You Begin.
Integration with Veeam Backup & Replication

If you plan to use Veeam Agent for IBM AIX 4.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 11a (build 11.0.1.1261) or later on the Veeam backup server.

You can store backup files created with Veeam Agent for IBM AIX on backup repositories managed by Veeam Backup & Replication. To do this, you must specify a Veeam backup repository as a target location in the backup job settings. A list of available Veeam backup repositories appears in Veeam Agent after you connect to the Veeam backup server. To learn more, see Managing Veeam Backup & Replication Servers.

To store Veeam Agent backups, you can use a simple backup repository or scale-out backup repository.

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

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

- The Veeam Agent backup job is displayed in the list of jobs in Veeam Backup & Replication.
- Backup files created with Veeam Agent 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 for IBM AIX backups:

- Perform data protection operations: copy Veeam Agent for IBM AIX backups to secondary backup repositories and archive these backups to tape.
- Perform restore operations: restore individual files and directories from Veeam Agent for IBM AIX backups and export data from these backups to virtual disks of the VMDK, VHD or VHDX format.
- Perform administrative tasks: disable and delete Veeam Agent backup jobs, remove Veeam Agent backups and so on.
Managing Veeam Agent in Veeam Backup & Replication

Veeam Backup & Replication lets you automate management of Veeam Agent for IBM AIX on multiple machines in your infrastructure. You can use the Veeam Backup & Replication console to obtain installation packages and configuration file for Veeam Agent for IBM AIX, configure Veeam Agent backup policies and perform other data protection and administration tasks. To use the Veeam Agent management functionality, you must install Veeam Backup & Replication 11a (build 11.0.1.1261) or later on the Veeam backup server.

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

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

A machine that you plan to protect with Veeam Agent for IBM AIX must meet requirements listed in the table below.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>Memory: 1 GB RAM (for standard backup and restore operations) / 4 GB RAM (for bare-metal recovery). For information about RAM requirements for backup of a great number of files, see <a href="#">RAM Requirements for Large Numbers of Files</a>. Disk space: 1.5 GB free disk space for product installation. Network: 10 Mbps or faster network connection to a backup target.</td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>IBM AIX versions starting from version 7.1 up to the latest update of version 7.3 are supported. <strong>Note:</strong> - IBM AIX 6.1 has an experimental support status. For details about experimental support, see this Veeam KB article. - Backup of a Virtual I/O Server (VIOS) is not supported. - Only GA versions of the IBM AIX OS that have been released before version 4.0 of Veeam Agent for IBM AIX are supported.</td>
</tr>
<tr>
<td><strong>File System</strong></td>
<td>All file systems supported by the supported operating systems. Consider the following: - Total size of all file systems included in a file-level backup must not exceed 218 TB. - The maximum number of files in one backup job is 20,000,000. To back up a greater number of files, use multiple jobs. - Size of a file in a backup must not exceed 16 TB. - Name of a file in a backup must not be larger than 254 bytes. Keep in mind that characters that you can use in the file name may be encoded in 2 bytes or more. - Sparse files are not supported. Veeam Agent backs up and restores sparse files as regular files. - JFS2 snapshots are not supported.</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>The following utilities must be installed on the machine: - <code>mlocate</code> (version 0.26-1) — required for file system indexing. It is provided along with the product in the product installation media.</td>
</tr>
<tr>
<td>Specification</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>tar</td>
<td>required for file system indexing, exporting and rotating logs. It is installed with the product.</td>
</tr>
<tr>
<td>gzip</td>
<td>required for file system indexing, exporting and rotating logs. It must be installed separately.</td>
</tr>
<tr>
<td>mkisofs</td>
<td>required for creating Veeam recovery Media.</td>
</tr>
</tbody>
</table>

[For IBM AIX 7.3, 7.2 and 7.1 TL1 or higher] This utility is pre-installed in the OS and does not require separate installation.

[For IBM AIX 7.1 TLO and 6.1] You must install version 1.13 of the mkisofs utility.

### AIX Environment

The **LIBPATH** AIX environment variable on the Veeam Agent computer must be set to blank (default value). If a different value is specified for this variable, you must make adjustments to the AIX environment for proper operation of Veeam Agent. For details, see this Veeam KB article.

### Backup Target

Backup can be performed to the following types of storage:

- 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 11a (build 11.0.1.1261) or later backup repository (Veeam Cloud Connect repositories are not supported)

### Network

Consider the following:

- If you back up to a repository managed by a Veeam backup server, Veeam Agent for IBM AIX must be able to establish a direct IP connection to the Veeam Backup & Replication server. Veeam Agent for IBM AIX cannot work with Veeam Backup & Replication that is located behind a NAT gateway.
- Domain names of the Veeam Agent machine, Veeam Backup & Replication server and other servers in the Veeam backup infrastructure must be resolvable into IPv4 addresses.
RAM Requirements for Large Numbers of Files

Amount of RAM used by Veeam Agent for IBM AIX to process backed-up files depends on the number of files included in the backup. For large environments with great number of backed-up files, use the following RAM sizing recommendations.

<table>
<thead>
<tr>
<th>Number of Backed-Up Files</th>
<th>RAM (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000,000</td>
<td>2</td>
</tr>
<tr>
<td>2,000,000</td>
<td>4</td>
</tr>
<tr>
<td>3,000,000</td>
<td>4.7</td>
</tr>
<tr>
<td>4,000,000</td>
<td>7.8</td>
</tr>
<tr>
<td>5,000,000</td>
<td>8.5</td>
</tr>
<tr>
<td>6,000,000</td>
<td>9.3</td>
</tr>
<tr>
<td>7,000,000</td>
<td>14.7</td>
</tr>
<tr>
<td>8,000,000</td>
<td>15.5</td>
</tr>
<tr>
<td>9,000,000</td>
<td>16.2</td>
</tr>
<tr>
<td>10,000,000</td>
<td>17</td>
</tr>
<tr>
<td>15,000,000</td>
<td>30</td>
</tr>
<tr>
<td>20,000,000</td>
<td>33</td>
</tr>
</tbody>
</table>
# Used Ports

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

<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 for IBM AIX machine</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 IBM AIX machine and backup repositories is transferred directly, bypassing Veeam backup servers.</td>
</tr>
</tbody>
</table>

**Communication with Veeam Backup & Replication Repositories**

<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 for IBM AIX machine</td>
<td>Linux server performing the role of a backup repository</td>
<td>TCP</td>
<td>22</td>
<td>Port used as a control channel from the Veeam Agent for IBM AIX machine to the target Linux host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>2500 to 3300</td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
</tr>
<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 later)</td>
<td>Dynamic RPC port range. For more information, see <a href="#">this Microsoft KB article</a>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP</td>
<td>2500 to 3300</td>
<td>Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.</td>
</tr>
</tbody>
</table>
Installation and Configuration

The product installation media is supplied as an archive file of the .tar.gz format. The archive file for Veeam Agent for IBM AIX has the following name:

```
VeeamAgentAIX-4.0.0.891-ppc64.tar.gz
```

The product installation media contains the Veeam Agent for IBM AIX software package and prerequisite software packages in the RPM format.
Before You Begin

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

1. The machine on which you plan to install Veeam Agent for IBM AIX must meet the system requirements. To learn more, see System Requirements.

2. To install and run Veeam Agent for IBM AIX, you must use the root account or any user account that has super user (root) privileges on the machine where you plan to install the product.

3. Installation of Veeam Agent for IBM AIX requires the rpm.rte package version 3.0.5.20 or later. This package manager is shipped with the IBM AIX operating system starting from version 6.1. To make sure the rpm.rte fileset on the machine where you want to install Veeam Agent is not missing or outdated, do the following:
   a. Check the version of the rpm.rte fileset with the lslpp -l rpm.rte command. Use the information from this web page to verify the version of the installed rpm.rte fileset is compatible with the OS version on the machine.
   b. If the installed rpm.rte fileset is outdated or is not installed, you can download an rpm.rte fileset that meets the requirements from this web page.

4. Make sure that /opt, /var, /usr, /etc and other file systems have sufficient amount of free space to install the product. If required, use the chfs tool to increase the size of the file system.

5. If you plan to enable file system indexing in the backup job settings, you must install the mlocate utility on the Veeam Agent machine. The utility is provided along with Veeam Agent in the product installation media. To learn more, see Installing Prerequisite Software.

6. If you plan to create Veeam Recovery Media, you must have the mkisofs command functional on the Veeam Agent machine.

7. You can install and operate Veeam Agent for IBM AIX in an LPAR or WPAR.
Installing Prerequisite Software

If you plan to enable file system indexing in the backup job settings, you must install the `mlocate` utility on the Veeam Agent machine. The utility is provided along with Veeam Agent in the product installation media.

To install the `mlocate` utility:

1. Obtain the Veeam Agent for IBM AIX installation archive.
2. Extract the contents of the installation archive to a directory that can be accessed from the machine where you want to install the product. For example, this can be a directory in the local file system or an NFS directory.
3. Navigate to the directory where you extracted the archive with the `cd` command, and then use the following command:

   ```
   rpm -ivh mlocate-0.26-1.aix6.1.ppc.rpm
   ```
Installing Veeam Agent for IBM AIX

You can install Veeam Agent for IBM AIX using the RPM Package Manager. To install Veeam Agent for IBM AIX:

1. Download the Veeam Agent for IBM AIX installation archive from the Veeam Download page.

2. Extract the contents of the installation archive to a directory that can be accessed from the machine where you want to install the product. For example, this can be a directory in the local file system or an NFS directory.

3. Navigate to the directory where you extracted the archive with the `cd` command, and then use the following command:

   ```bash
   rpm -ivh VeeamAgent-4.0.0.891-ppc64.rpm
   ```
Managing Veeam Agent Operation Mode

Veeam Agent for IBM AIX can operate in two different modes. Depending on the selected mode, Veeam Agent has 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><strong>Owner</strong></td>
<td>Name of the backup repository that manages Veeam Agent.</td>
</tr>
<tr>
<td></td>
<td>If Veeam Agent operates in the standalone mode, Veeam Agent will display the <em>Not Set</em> value.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Current Veeam Agent operating mode. Possible values:</td>
</tr>
<tr>
<td></td>
<td>- <em>Standalone</em> — Veeam Agent operates in the standalone mode.</td>
</tr>
<tr>
<td></td>
<td>- <em>Pre-installed agent</em> — Veeam Agent operates in the managed mode as 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: Pre-installed agent
```

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:

- Veeam Agent computer will be automatically removed from the protection group in Veeam Backup & Replication.
- 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.

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 setup files that you must obtain from your System Administrator. To learn more about deployment using external tools, see the Deploying Veeam Agent for Unix section in the Agent Management Guide.

To connect Veeam Agent 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 --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/AIX\ Servers\ Distrib\s/Unix/AIXServers.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:

```
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.
Upgrading Product

Veeam Agent for IBM AIX supports upgrade from version 3.0 to version 4.0. To upgrade the product:

1. Download the Veeam Agent for IBM AIX installation archive from the Veeam Download page.
2. Extract the contents of the installation archive to a directory that can be accessed from the machine where you want to install the product. For example, this can be a directory in the local file system or an NFS directory.
3. Navigate to the directory where you extracted the archive with the `cd` command, and then use the following command:

   ```bash
   rpm -U VeeamAgent-4.0.0.891-ppc64.rpm
   ```

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

Upgrading Product from Version 1.0

If you run Veeam Agent for IBM AIX 1.0, you must upgrade the product to version 2.0, then to version 3.0, and then upgrade it to version 4.0.

Keep in mind that Veeam Agent for IBM AIX 4.0 does not support restore from backups created with Veeam Agent for IBM AIX 1.0. To be able to restore data from such backups, you need to copy product configuration files before you upgrade Veeam Agent for IBM AIX 1.0 to a newer version.

To do this, complete the following steps:

1. Copy Veeam Agent for IBM AIX 1.0 configuration files from the product installation directory to a separate directory on the Veeam Agent machine or to a network shared folder. These configuration files are required to restore data from backups created with Veeam Agent for IBM AIX 1.0. The following files are required:
   - `/etc/veeam/devices.ini`
     This file contains information about backup locations configured in Veeam Agent for IBM AIX 1.0.
   - `/etc/veeam/ubax.ini`
     This file contains information about the default backup location specified in Veeam Agent for IBM AIX 1.0.
   - `/etc/veeam/scripts/veeam.scp` (or custom script that you specified in Veeam Agent for IBM AIX 1.0 backup settings)
     This file is required to restore data from a Veeam Agent for IBM AIX 1.0 full backup using a restore script.
   - `/etc/veeam/media/*.lml`
     Media library (*.lml) files are required to restore data from a Veeam Agent for IBM AIX 1.0 full backup using a media library entry.
IMPORTANT

Make sure you have copied configuration files before you proceed to the step 2. Otherwise, when you uninstall Veeam Agent for IBM AIX 1.0, these files will be deleted along with the product.

2. Uninstall Veeam Agent for IBM AIX 1.0. To do this, use the following command:

```
rpm -e VeeamAgent
```

During the uninstallation process, backup files created with Veeam Agent for IBM AIX 1.0 are not impacted in any way.

In case you need to restore data from a backup created with Veeam Agent for IBM AIX 1.0, you will be able to install this version of the product once again and perform the necessary restore tasks. Alternatively, you can perform such tasks in Veeam Agent for IBM AIX 2.0 that supports restore from Veeam Agent for IBM AIX 1.0 backups. For details, refer to the product documentation at Veeam Help Center.
Uninstalling Product

To uninstall Veeam Agent for IBM AIX, use the following command:

```
rpm -e VeeamAgent
```
Granting Permissions to Users

When you install Veeam Agent for IBM AIX, the product program files are placed to the directories on the system volume. For full access to Veeam Agent for IBM AIX 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 for IBM AIX at the process of the product installation. To let regular users work with Veeam Agent for IBM AIX 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 for IBM AIX commands and perform backup and restore tasks under a regular user account.

To add a user to the veeam group, use the following command:

```
chgrp -m + <username> veeam
```

where `<username>` is a user name of the account to which you want to grant access to Veeam Agent for IBM AIX.

For example:

```
root@srv01:~# chgrp -m + user01 veeam
```

**IMPORTANT**

Mind the following:

- To add a user to the veeam group, you must have super user (root) privileges in the IBM AIX OS.
- After a user is added to the veeam group, the user must re-login to the IBM AIX OS to complete the procedure of adding the user to the group.
- Add only trusted users to the veeam group. Veeam Agent for IBM AIX 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 use of pre-job/post-job scripts.

To check whether the user who is currently logged in to the IBM AIX 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
```
Getting Started

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

1. **Create Custom Veeam Recovery Media.**
   Veeam Recovery Media provides an alternate way to boot your machine in the event of a disaster. If your machine fails to start or the hard disk gets corrupted, you can boot the IBM AIX OS from Veeam Recovery Media and restore your data.
   To learn more, see Creating Veeam Recovery Media.

2. **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:** what directories and files you want to back up.
     **IMPORTANT**
     Performing full file-level restore with Veeam Recovery Media requires a backup that includes the full contents of the root directory. To configure such backup job, set the value of the --includedirs option to /, for example, veeamconfig job create --name system\backup --reponame [vbr01] --includedirs /. The backup job with such scope generates an additional configuration file required for restoring your files during bare-metal recovery.
   - **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.
   To learn more, see Performing Backup.

3. **Monitor backup task performance.**
   You can get information about backup and restore sessions status and view session logs. To learn more, see Reporting.

4. In case of a disaster, you can **restore data from a Veeam Agent backup.** To learn more, see Performing Restore.
Getting to Know User Interface

With Veeam Agent for IBM AIX, you can perform backup, restore and configuration tasks using the command line interface.

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

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

You must 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. The following commands are available in Veeam Agent for IBM AIX:
  - agreement
  - backup
  - config
  - create
  - createIso
  - grablogs
  - help
  - job
  - license
  - mode
  - point
  - repository
  - schedule
  - session
  - 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:
  - create
  - delete
- edit
- help
- list
- 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 [<command>] help` do not require parameters.

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

```
user@srv01:~$ veeamconfig repository list
Name          ID                                      Location            Typ
Backup server            {818e3a0f-8155-4a51-9430-248a203a43d1}  /home/backups       local
Repository_1   {2155a2e7-a1e9-4347-9d8b-cf8f3a6f3fcb}  172.17.53.47/veeam  cif
```

Viewing Help

You can view short help information about the specific Veeam Agent for IBM AIX command. To view help, use the following command:

```
veeamconfig <command> help
```

where `<command>` is a 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 for IBM AIX, you must obtain a license and install it on the protected machine. Until you install a license, you will not be able to use the product.

Veeam Agent for IBM AIX supports Enterprise Plus license edition only. For more information on licensing, see Veeam Licensing Policy.

You can use the Veeam Agent for IBM AIX command line interface to install a license, monitor status of the installed license or remove the license if necessary.

If you use Veeam Agent for IBM AIX with Veeam Backup & Replication, you must install and manage the license in the Veeam Backup & Replication console or in Veeam Backup Enterprise Manager.
License Agreement

After you install Veeam Agent for IBM AIX, 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 Veeam Agent for IBM AIX.

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

When you run a Veeam Agent for IBM AIX 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.
Managing License

You can perform the following operations with the Veeam Agent for IBM AIX license:

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

To work with Veeam Agent for IBM AIX, 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 help` (or `veeamconfig agreement -h` or `veeamconfig agreement --help`)
- `veeamconfig agreement show`
- `veeamconfig help` (or `veeamconfig -h` or `veeamconfig --help`)
- `veeamconfig version` (or `veeamconfig -v` or `veeamconfig --version`)

To accept license agreements, use the following command:

```
veeamconfig agreement accepteula && veeamconfig agreement acceptthirdpartylicences
```

**TIP**

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

To use Veeam Agent for IBM AIX, you must obtain and install a license. Without a valid license installed, you will not be able to use the product.

In case you are already using the product, you can install a license once again, for example, after you removed an originally installed license. You may also need to install a new license after an original license expires.

To install a license, use the following command:

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

where `<path>` is a path to the license key file in the local file system of your machine.

Veeam Agent for IBM AIX 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
License was installed successfully.
License information:
  License source: Local license
  Mode: Server
  Expiration date: 2020/10/10 (158 days left)
  Grace period ends: 2020/11/09
  Status: License is valid
  Issued to: TechCompany
  Email: administrators@tech.com
```
Viewing License Information

You can view detailed information about the license currently installed in Veeam Agent for IBM AIX. To do this, use the following command:

```
veeamconfig license show
```

Veeam Agent for IBM AIX will display the following information about the license:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>License source</strong></td>
<td>Defines whether the license is installed on the local machine or in Veeam Backup &amp; Replication. You must install a license on the Veeam Agent machine to start working with Veeam Agent for IBM AIX. If you use Veeam Agent with Veeam Backup &amp; Replication, after you connect to the Veeam backup server, Veeam Agent uses a license installed in Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Product operation mode. Veeam Agent for IBM AIX always operates in the server mode.</td>
</tr>
<tr>
<td><strong>Expiration date</strong></td>
<td>Date when the license will expire, and the number of days left before the expiration date.</td>
</tr>
<tr>
<td><strong>Grace period ends</strong></td>
<td>Date when the grace period will expire. To ensure a smooth license update procedure Veeam Agent for IBM AIX offers a grace period after the license expires. During the grace period, Veeam Agent for IBM AIX continues to operate in a regular way. After the grace period expires, you will not be able to use the product. To continue using the product, you must install a new license.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Status of the installed license: <em>The license is valid</em>, <em>The license has expired</em> or <em>The license is corrupted</em>.</td>
</tr>
<tr>
<td><strong>Issued to</strong></td>
<td>Name of the user or company to which the license was issued.</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td>Email of the user or company to which the license was issued.</td>
</tr>
</tbody>
</table>

**NOTE**

If you use Veeam Agent for IBM AIX with Veeam Backup & Replication, the `veeamconfig license show` command displays information about the license source and product operation mode only. Other information for the license is available in the Veeam Backup & Replication console.
For example:

**For a Veeam Agent license installed locally on the Veeam Agent machine**

```
user@srv01:~$ veeamconfig license show
License information:
 License source: Local license
 Mode: Server
 Expiration date: 2020/10/10 (158 days left)
 Grace period ends: 2020/11/09
 Status: License is valid
 Issued to: TechCompany
 Email: administrators@tech.com
```

**For a license installed in Veeam Backup & Replication and used by Veeam Agent**

```
user@srv01:~$ veeamconfig license show
License information:
 License source: Veeam Backup & Replication
 Mode: Server
```
Removing License

You can remove the Veeam Agent for IBM AIX license if necessary. After you remove a license, you will not be able to use the product. To continue using the product, you must install the license once again.

To remove a license, use the following command:

```bash
veeamconfig license remove
```
Performing Backup

You can back up your data to protect files and directories on your machine. To back up your data, you must configure a backup job. Veeam Agent for IBM AIX lets you configure several backup jobs targeted at the same or different backup repositories.

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

You must create Veeam Recovery Media on a functional machine. If you update the system, you must create a new recovery image. When Veeam Agent generates Veeam Recovery Media, it copies the IBM AIX kernel running on the machine with its currently loaded modules and includes them into the recovery media. If the OS fails to start, you can boot it from the Veeam Recovery Media that you created on this machine.

To create Veeam Recovery Media, use the following command:

```bash
veeamconfig createIso --output <iso_path> [--overwrite][--tempPath <temp_path>][--edit]
```

where:

- `<iso_path>` — full path to the image file. Use this required option to specify the name and location of the output image file.
- `--overwrite` — option that allows you to overwrite the output image file if it already exists in the specified location.
- `<temp_path>` — path to the directory for the temporary files created during Veeam Recovery Media generation. By default, Veeam Agent stores temporary files in the `/tmp/veeamrcd` directory. Use this option to change the default location — for example, if the `tmp` directory does not have enough space.
- `--edit` — option that allows you to edit the content of the recovery image in interactive mode during creation of Veeam Recovery Media. For more information, see Editing Recovery Image Content During Creation.

For example:

```bash
# veeamconfig createIso --output /mnt/veeam-recovery-media-svr01.iso --overwrite --tempPath /external/veeamtmp
```

Editing Recovery Image Content During Creation

You can include additional files into the image — for example, commands binaries, configuration files, special disaster recovery documents with instructions, and so on. To do this:

1. Add the `--edit` option to the `createIso` command and run it.

   After Veeam Agent starts creating Veeam Recovery Media, it will launch a new shell instance.

   ```bash
   Preparing resource files.
   Creating a recovery media image.
   Writing a detailed log to `/var/log/veeam/RecoveryMediaBuilder.log`.
   Starting new shell instance.
   Change Recovery Media content in `/tmp/veeamrcd/mkisofs_workspace/cd_fs/new`.
   Type 'exit' to continue execution.
   ```

2. Add content to the `/tmp/veeamrcd/mkisofs_workspace/cd_fs/new` directory.

3. After you add the content, type `exit` to finish creating Veeam Recovery Media.
Creating Backup Jobs

To back up files and directories of your machine, you must configure a backup job. The backup job settings define what data to back up as well as where and how to back up data.

You can configure one or more backup jobs to back up your data. Configuring several backup jobs may be useful in the following situations:

- 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.

To create a backup job, use the following command:

```bash
veeamconfig job create --name <job_name> --reponame <repository_name> <objects> [ <advanced_options> ] [ <schedule_options> ] [ <active_full_backup_options> ] [--indexall]
```

where:

- `<job_name>` — name for the created backup job.
- `<repository_name>` — name of the backup repository that will be used as a target location for backup files.
- `<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.
- `--indexall` — defines that Veeam Agent for IBM AIX must index files in the directories included in the backup. To learn more, see File System Indexing.

If you want to create Veeam Agent backups on a local storage or in a network shared folder, you must create the backup repository in advance, before configuring the backup job. To learn more, see Creating Backup Repository.

If you want to create Veeam Agent backups in the Veeam backup repository, you must connect to the Veeam backup server in advance, before configuring the backup job. To learn more, see Connecting to Veeam Backup Server.
TIP

Consider the following:

- If a value of a command option contains the space character, specify the value in single quotation marks (') or double quotation marks ("''). Alternatively, use the backslash character (\) as an escape character. For example, this may be required if you want to specify the backup job name, backup repository name or path to a folder you want to back up.
- You can also specify backup schedule and active full backup schedule settings later, after you create the job. To learn more, see Configuring Backup Schedule and Configuring Active Full Backup Schedule.

For example:

```bash
$ veeamconfig job create --name system\ backup --reponame [vbr01]\ Backup\ Vol\ 01 --includedirs / --excludemasks "*.pdf" --maxpoints 7 --indexall
```

File Inclusion Options

When you create a 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 must be included in backup, for example: /home/user. You can specify one or more paths to directories in the machine file system. To separate several paths, use the ',' (comma) character, for example: /home/user/Documents,/home/user/reports. <strong>IMPORTANT!</strong> Restoring from Veeam Recovery Media requires a backup that includes the full contents of the root directory. To configure such backup job, set the value of the --includedirs option to /, for example: veeamconfig job create --name system\ backup --reponame VeeamBackup --includedirs / This backup job generates an additional configuration file required for restoring your files during bare-metal recovery. If use excludedirs, includemasks or excludemasks options in backup job settings, mind that no system data is excluded from backup.</td>
</tr>
<tr>
<td>--excludedirs</td>
<td>Full path to a directory that must be excluded from backup. The directory specified with this option should be a subdirectory of one of the directories specified with the --includedirs option. Otherwise, the --excludedirs option does not have any effect on backup. To separate several paths, use the ',' (comma) character, for 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>
</tbody>
</table>
| `--includemasks` | File name mask that defines files that must be included in backup. You can use the following UNIX wildcard characters for file name masks:  
  - `'*':` a substitution for zero 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`.  

  If you use wildcard characters in file name masks, you must specify masks in double quotation marks (`"`). To separate several masks, use a `,` (comma) character. For example: `--includemasks "*.bak,*.pdf"`.  

  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 `report?.pdf` file name mask, Veeam Agent for IBM AIX will back up the `/home/user/Documents/report.pdf` file and will not back up the `/home/user/reports/report.pdf` file.                                                                                                                                                                                                                                                                                                                                 |

| `--excludemasks` | File name mask that defines files that must be excluded from backup. You can use the following UNIX wildcard characters for file name masks:  
  - `'*':` a substitution for zero 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`.  

  If you use wildcard characters in file name masks, you must specify masks in double quotation marks (`"`). To separate several masks, use a `,` (comma) character. For example: `--excludemasks "*.bak,*.pdf"`.  

  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 `--includemasks` 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  

  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 `--includemasks` option. For example, you may want to specify the following backup scope for the backup job:
Option | Description and values
---|---

- Exclude files that match the *.odt file name mask.

In this case, Veeam Agent for IBM AIX 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>
</table>
| **--compressionlevel** | Data compression level. Possible values:  
   - 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** | Number of restore points that you want to store in the backup location. By default, Veeam Agent for IBM AIX keeps 7 latest restore points. When the new restore point that exceeds the specified number is created, Veeam Agent for IBM AIX will remove the earliest restore point from the backup chain. |
| **--prejob** | Path to the script that will be executed at the start of the backup job. |
| **--postjob** | Path to the script that will 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 IBM AIX will prompt you to specify a password for data encryption and hint for the password.  
   You cannot use this option if you want to save backup files on a Veeam Backup & Replication repository. Encryption options for Veeam Agent backup jobs targeted at a Veeam backup repository are managed by a
<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>backup administrator working with Veeam Backup &amp; Replication. To learn more, see Setting Up User Permissions on Backup Repositories.</td>
</tr>
<tr>
<td>--deleteold</td>
<td>Number of days to keep the backup created with the backup job in the target location. If Veeam Agent for IBM AIX 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. By default, the retention period for old backups is 30 days. You can specify this option only for backup jobs targeted at a Veeam Backup &amp; Replication repository.</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>--daily</td>
<td>Defines that the backup job must start daily at specific time.</td>
</tr>
<tr>
<td>--weekdays</td>
<td>Weekdays when the backup job must start 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>--at</td>
<td>Time of day when the backup job must start specified in the HH:MM format. For example: 20:00.</td>
</tr>
</tbody>
</table>

After the backup job is created, Veeam Agent for IBM AIX 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><strong>--weekdays-full</strong></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><strong>--thisday-full</strong></td>
<td>Days of the month when the backup job must create an active full backup separated by a comma (','). Possible values are: 1-31.</td>
</tr>
<tr>
<td></td>
<td>Note that if the specified value is greater than the number of days in the month, the backup job will not create an active full backup that month. For example, if you schedule active full backups for the 31st day of the month, Veeam Agent will not create active full backups during shorter months.</td>
</tr>
</tbody>
</table>

After the backup job is created, Veeam Agent for IBM AIX 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.
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 IBM AIX. With the Veeam Agent for IBM AIX command-line interface, you can perform the following actions with the backup job schedule:

- Specify schedule settings for the job.
- Enable schedule for the job.
- View the schedule defined for the job.
- Disable schedule for the job.
Specifying Backup Schedule

You can schedule a backup job to start at specific times daily or on specific week days.

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.

- `<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:

```
veeamconfig schedule set --jobid <job_id> --weekdays <days> --at <time>
```

or

```
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.
- `<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:

```
user@srv01:~$ veeamconfig schedule set --jobname DailyBackup --weekdays Monday,Wednesday,Friday --at 20:00
```
Enabling Backup Schedule

After you specify backup schedule settings for the backup job, Veeam Agent for IBM AIX automatically enables schedule for the job. You can also enable backup schedule manually, for example, if you previously disabled it for the backup job. To enable backup schedule, 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 IBM AIX 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 the 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 IBM AIX. With the Veeam Agent for IBM AIX command line interface, you can perform the following actions with the active full backup schedule:

- Specify active full backup schedule.
- Enable active full backup schedule.
- View active full backup schedule.
- Disable active full backup schedule.
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.

**NOTE**

Active full backup schedule depends on the regular backup schedule. To create active full backup automatically, in addition to configuring active full backup schedule, you must also set up the job to run upon schedule. To learn more, see Active Full Backup Schedule.

Specifying Monthly Active Full Backup Schedule

To instruct Veeam Agent for IBM AIX to perform active full backup on a specific day of the month, use the following command:

```bash
veeamconfig schedule activefull set --jobid <job_id> --thisday <day>
```

or

```bash
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.

- `<day>` — days of the month when the backup job must create an active full backup separated by a comma (,'). Possible values are: 1-31.

  Note that if the specified value is greater than the number of days in the month, the backup job will not create an active full backup that month. For example, if you schedule active full backups for the 31st day of the month, Veeam Agent will not create active full backups during shorter months.

For example:

```bash
user@ srv01:~$ veeamconfig schedule activefull set --jobname DailyBackup --thisday 1
```
Specifying Weekly Active Full Backup Schedule

To instruct Veeam Agent for IBM AIX 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.

- `<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 for IBM AIX 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 Active Full 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 IBM AIX 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 &lt;value&gt;</td>
<td>Days on which the backup job creates active full backups. For example: <em>Every Monday</em> or <em>Every 1 day of every month.</em></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
```
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.
Starting Backup Job

You can start a backup job with the command line interface. When you start a backup job, Veeam Agent for IBM AIX 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 for IBM AIX performs 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**

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:

```bash
$ 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_20200316_102309_{381532f7-426a-4e89-b9fc-43d98942c71a}].
```

You can check the backup job session status or view the backup job session log.
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_20200316_122900_{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.
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 for IBM AIX will not produce a new restore point during the session, and the session will finish with the *Failed* status.

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. You can get the list of sessions with the `veeamconfig session list` command.

- `--force` — with this option enabled, Veeam Agent for IBM AIX 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 381532f7-426a-4e89-b9fc-43d98942c71a
```
Managing Backup Jobs

You can perform the following actions with backup jobs configured in Veeam Agent for IBM AIX:

- 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 IBM AIX, use the following command:

```bash
veeamconfig job list
```

In the list of backup jobs, Veeam Agent for IBM AIX 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>Type</td>
<td>Backup type. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• All System — the backup job is set to back up the entire system (the root mount point).</td>
</tr>
<tr>
<td></td>
<td>• FileLevel — the backup job is set to back up specific files and directories.</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:

```bash
user@srv01:~$ veeamconfig job list
Name           ID                                      Type        Repository
system backup  {9183490c-1549-4dca-846b-7b95e7bef784}  All System  [srv14] Back
up Vol 01
file backup    {ff0b79ae-21cc-4d2c-b45d-3d35de3db1dd}  FileLevel   [srv14] Back
up Vol 01
```
Viewing Backup Job Settings

To view detailed information about the backup jobs settings, use the following command:

\[\text{veeamconfig job info --name <job_name>}\]

or

\[\text{veeamconfig job info --id <job_id>}\]

where:
- \(<\text{job_name}>\) — name of the backup job for which you want to view settings.
- \(<\text{job_id}>\) — ID of the backup job for which you want to view settings.

Veeam Agent for IBM AIX 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></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>Max points</td>
<td>Number of restore points to keep on disk (the default value is 7).</td>
</tr>
<tr>
<td>Block size</td>
<td>Data block size in kilobytes.</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>
<tr>
<td><strong>Schedule</strong></td>
<td>[Optional] Schedule settings enabled for the job.</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
<td>[Optional] Old backup retention settings enabled for the job (only for backup jobs targeted at a Veeam backup repository).</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:-$ veeamconfig job info --name system\ backup
Backup job:
  ID: {fa1ebf29-62f1-47d4-ae91-4e7c209abcd2}
  Name: system backup
  Repository ID: {88788f9e-d8f5-4eb4-bc4f-9b3f5403bcec}
  Repository name: [srv14] Default Backup Repository
  Creation time: 2021-08-23 11:19:56
  Options:
    Compression: ZlibHigh
    Max points: 5
    Block size: 1024 KB
    File system indexing is disabled
  Objects for backup:
    Include Directory: /
  Schedule:
    Days: Monday, Tuesday, Wednesday, Thursday, Friday
    At: 14:00
    Active full: Every Saturday.
```
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:

```bash
veeamconfig job edit <option> for --name <job_name>
```

or

```bash
veeamconfig job edit <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:

```bash
user@srv01:~$ veeamconfig job edit --name DailyBackup for --name SystemBackup
```

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>
<tbody>
<tr>
<td>--name</td>
<td>Name of the backup job.</td>
</tr>
<tr>
<td>--reponame</td>
<td>Name of the backup repository that will be used as a target location for backup files.</td>
</tr>
<tr>
<td>--compressionlevel</td>
<td>Data compression level. Possible values:</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. The default value is 1024.</td>
</tr>
<tr>
<td>Option</td>
<td>Description and values</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--maxpoints</td>
<td>The number of restore points that you want to store in the backup location. By default, Veeam Agent for IBM AIX keeps 7 latest restore points. When the new restore point that exceeds the specified number is created, Veeam Agent for IBM AIX will remove the earliest restore point from the backup chain.</td>
</tr>
<tr>
<td>--includedirs</td>
<td>Full path to a directory that should be included in backup, for example: /home/user. You can specify one or several paths to directories in the machine file system. To separate several paths, use a ',' (comma) character, for example: /home/user/Documents,/home/user/reports. <strong>IMPORTANT!</strong> Restoring from Veeam Recovery Media requires a backup that includes the full contents of the root directory. To configure such backup job, set the value of the --includedirs option to /, for example: veeamconfig job create --name system\ backup --reponame VeeamBackup --includedirs /. This backup job generates an additional configuration file required for restoring your files during bare-metal recovery. If use excludedirs, includemasks or excludemasks options in backup job settings, mind that no system data is excluded from backup.</td>
</tr>
<tr>
<td>--excludedirs</td>
<td>Full path to a directory that should be excluded from backup. The directory specified with this option should be a subdirectory of one of the directories specified with the --includedirs option. Otherwise, the --excludedirs option does not have any effect on backup. To separate several paths, use a ',' (comma) character, for example, /home/user/Documents,/home/user/reports.</td>
</tr>
</tbody>
</table>
| --includemasks | File name mask that defines files that must be included in backup. You can use the following UNIX wildcard characters for file name masks:  
  - '*' — a substitution for zero 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, repor?.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.  
  
  If you use wildcard characters in file name masks, you must specify masks in double quotation marks (" "). To separate several masks, use a ',' (comma) character. For example: --includemasks "report.*,reports.*".  
  
  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 for IBM AIX will back up the... |
<table>
<thead>
<tr>
<th>Option</th>
<th>Description and values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--excludemasks</strong></td>
<td>File name mask that defines files that must be excluded from backup.</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 zero 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 href="%5B%5D"></a>' — 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>If you use wildcard characters in file name masks, you must specify masks in double quotation marks (&quot; &quot;). To separate several masks, use a ',', (comma) character. For example, --excludemasks &quot;report.<em>,reports.</em>&quot;.</td>
</tr>
<tr>
<td></td>
<td>File exclusion option is applied to all directories that are specified with the <strong>--includedirs</strong> option and files that match file name masks specified with the <strong>--includemasks</strong> option. 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>
<tr>
<td></td>
<td>In this case, Veeam Agent for IBM AIX 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.</td>
</tr>
<tr>
<td><strong>--indexnothing</strong></td>
<td>Defines that file system indexing options are disabled for the backup job.</td>
</tr>
<tr>
<td><strong>--indexall</strong></td>
<td>Defines that Veeam Agent for IBM AIX must index all files included in backup.</td>
</tr>
<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 veeamconfig job edit command with the <strong>--setencryption</strong> option, Veeam Agent for IBM AIX will prompt you to specify a password for data encryption and hint for the password.</td>
</tr>
<tr>
<td></td>
<td>You cannot use this option if you want to save backup files on a Veeam Backup &amp; Replication repository. Encryption options for Veeam Agent backup jobs targeted at a Veeam backup repository are managed by a backup administrator working with Veeam.</td>
</tr>
<tr>
<td>Option</td>
<td>Description and values</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Backup &amp; Replication. To learn more, see <a href="#">Setting Up User Permissions on Backup Repositories</a></strong>.</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. You cannot use this option if you want to save backup files on a Veeam Backup &amp; Replication repository. Encryption options for Veeam Agent backup jobs targeted at a Veeam backup repository are managed by a backup administrator working with Veeam Backup &amp; Replication. To learn more, see <a href="#">Setting Up User Permissions on Backup Repositories</a>.</td>
</tr>
<tr>
<td><strong>--prejob</strong></td>
<td>Path to the script that will be executed at the start of the backup job.</td>
</tr>
<tr>
<td><strong>--postjob</strong></td>
<td>Path to the script that will be executed after the backup job completes.</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 IBM AIX 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. By default, the retention period for old backups is 30 days. You can specify this option only for backup jobs targeted at a Veeam Backup &amp; Replication repository.</td>
</tr>
</tbody>
</table>

**NOTE**

Mind the following:

- If you change the target location for the backup job, during the next backup job session Veeam Agent for IBM AIX will perform full backup. All subsequent backup sessions will produce incremental backups — Veeam Agent for IBM AIX 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 IBM AIX will create a new incremental backup. The backup will contain new files added to the backup scope and existing files in the backup scope that changed on the Veeam Agent machine since the previous backup job session.
- 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 IBM AIX 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 IBM AIX. When you delete a backup job, backup files created by this job remain intact on the backup repository.

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 IBM AIX 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 11a (build 11.0.1.1261) or later backup repository
Creating Backup Repository

A backup job configured in Veeam Agent for IBM AIX creates backup files in a backup repository. If you want to back up your data to a directory in the machine's local file system or a network shared folder (NFS or CIFS share), you must create a backup repository in advance, before you create a backup job.

**NOTE**
Consider the following:

- A backup repository should be created on a separate volume from a volume whose data you plan to back up.
- If you want to create Veeam Agent backups in the Veeam backup repository, you must connect to the Veeam backup server in advance, before configuring the backup job. To learn more, see [Connecting to Veeam Backup Server](#).

To create a backup repository, use the following command:

```
veeamconfig repository create --name <repository_name> --location <path>
```

where:

- `<repository_name>` — desired name for the backup repository.
- `<path>` — path to the directory in the local file system of your machine in which backup files should be stored.

For example:

```
$ veeamconfig repository create --name BackupVol01 --location /home/backups
```

**NOTE**
To create a backup repository in a network shared folder, you must mount the network shared folder to a directory in your machine's file system in advance. After you mount the network shared folder, you can create the backup repository in the same way as in a local directory.
Viewing List of Backup Repositories

To view backup repositories configured in Veeam Agent for IBM AIX, use the following command:

```
veeamconfig repository list
```

Veeam Agent for IBM AIX 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>
</tbody>
</table>
| Location      | Backup repository location. The parameter value depends on the backup repository type:  
|               | • For a local backup repository, location is a directory in the local file system specified as a target location for backup files.  
|               | • For a Veeam backup repository, location is a name of the Veeam backup server that manages the backup repository. |
| Type          | Type of the backup repository. Possible values:  
|               | • Local (for a local backup repository)  
|               | • Backup server (for a Veeam backup repository)                              |
| Accessible    | Indicates whether the backup repository is accessible from the Veeam Agent machine. |
| Backup server | Backup server on which Veeam backup repository added to Veeam Agent for IBM AIX is configured. |

For example:

```
user@srv01:~$ veeamconfig repository list
Name                   ID                                      Location     Type
[vbr01] Backup Vol 01  {88788f9e-d8f5-4eb4-bc4f-9b3f5403bcec}  vbr01        bac
                    true        vbr01                        local
backup01             {c17cd683-decf-48f5-b076-1e8b27595f32}  /mnt/backup  loc
                    true
```

94 | Veeam Agent for IBM AIX | User Guide
Editing Backup Repository

You can edit settings for a backup repository created with Veeam Agent for IBM AIX.

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 for IBM AIX 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 34587 97-3ffe-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 Backup Repository

You can rescan a backup repository configured in Veeam Agent for IBM AIX. This may be useful, for example, after information about a backup stored in the backup repository is deleted from the Veeam Agent configuration database, or after you copy a backup to the backup repository. Veeam Agent will refresh the list of backups in the backup repository.

To rescan a 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:

```
$ veeamconfig repository rescan --name [vbr01]BackupVol01
```

You can also rescan all backup repositories configured in Veeam Agent at once. Use the following command:

```
veeamconfig repository rescan --all
```
Deleting Backup Repository

You can delete a backup repository configured with Veeam Agent for IBM AIX. When you delete a backup repository, Veeam Agent for IBM AIX removes record about 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> [--answer <yes/no>]
```

or

```
veeamconfig repository delete --name <repository_name> [--answer <yes/no>]
```

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.
- `<yes/no>` — answer to the prompt whether to remove records about backups stored on the deleted backup repository from the Veeam Agent database. If you do not specify the `--answer` option for the command, Veeam Agent for IBM AIX will prompt you to specify whether you want to remove backups from database. You will need to enter the answer for each backup residing on the deleted backup repository.

For example:

```
user@srv01:~$ veeamconfig repository delete --name Repository_1 --answer yes
```

**NOTE**

You cannot delete a backup repository that is specified as a backup location in the backup job settings.
Managing Veeam Backup & Replication Servers

You can store backup files created with Veeam Agent for IBM AIX 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**

Consider the following:

- Veeam Agent for IBM AIX can be connected to one Veeam backup server only. If you want to create backups on the backup repository managed by another backup server, you need to delete the 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, backups created on the Veeam backup repository managed by the original backup server 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 connection to the original backup server. After that, all backups previously stored on the backup repository will become available again. You will need to re-create all backup jobs that use the original backup server as well.

- 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 IBM AIX to a Veeam backup server, use the following command:

```bash
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>` — IP address of the Veeam backup server.

- `<vbr_port>` — port over which Veeam Agent for IBM AIX must communicate with Veeam Backup & Replication. The default port used for communication with the Veeam backup server is 10006.

- `<username>` — a user name of the account that has access to the Veeam backup repository.

  You can specify a user name in the `username` or `username@domain` format. In the latter case, you do not need to specify a domain as a value of the `--domain` option.

  **NOTE**

  You cannot provide a user name in the `domain\username` format.

- `<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. If you do not specify a password as a value of the `--password` option, Veeam Agent will prompt you to enter the password when you run the `veeamconfig vbrserver add` command.

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:

```
veeamconfig vbrserver add --name vbr01 --address 172.17.53.1 --port 10006 --login veeam --domain tech --password P@ssw0rd
```

When Veeam Agent for IBM AIX connects to a Veeam Backup & Replication server, Veeam Agent for IBM AIX 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 IBM AIX is connected, use the following command:

```
veeamconfig vbrserver list
```

Veeam Agent for IBM AIX will display the list of Veeam backup servers.

For the Veeam backup server in the list, Veeam Agent for IBM AIX 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 for IBM AIX database.</td>
</tr>
<tr>
<td>Endpoints</td>
<td>IP address of the Veeam backup server and port over which Veeam Agent for IBM AIX communicates with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>Username</td>
<td>Name of the account used to connect to the Veeam backup server.</td>
</tr>
<tr>
<td>Domain</td>
<td>Name of the domain in which the account used to connect to the Veeam backup server is registered.</td>
</tr>
</tbody>
</table>

For example:

```
user01@unixsrv01:$ veeamconfig vbrserver list
Name       ID                                      Endpoints               Use
rname       Domain                               vbr01.tech.local:10006  vbr01
vbr01       {1725183d-a66b-42ff-9e79-5e12de65b32d}  vbr01.tech.local:10006  vbr01\administrator vbr01
```
Viewing Backup Server Details

You can view detailed information about the Veeam backup server to which Veeam Agent for IBM AIX is connected. Use the following command:

```bash
veeamconfig vbrserver info --name <vbr_name>
```

or

```bash
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 for IBM AIX database.

Veeam Agent for IBM AIX 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 for IBM AIX 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 IBM AIX communicates with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>Login</td>
<td>Name of the account used to connect to the Veeam backup server.</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:

```bash
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>` — IP address of the Veeam backup server.
- `<vbr_port>` — port over which Veeam Agent for IBM AIX 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 for IBM AIX 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>` — a user 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.

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 IBM AIX 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
```

For example:

```
user@srv01:~$ 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 for IBM AIX is currently connected. When you delete a connection to a Veeam backup server, Veeam Agent for IBM AIX removes record for 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 the Veeam backup server in the following situations:

- Veeam Agent operates in the managed mode. To delete connection to the 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 the 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:

```
veeamconfig vbrserver delete --name <vbr_name>
```

or

```
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:

```
user@srv01:~$ veeamconfig vbrserver delete --name vbr01
```
Managing Backups

You can perform the following operations with backups created by backup jobs configured in Veeam Agent for IBM AIX:

- View backups.
- View backup details.
- View restore points in backup.
- Import backup to the Veeam Agent database.
- Delete backup.
Viewing Backups

To view a list of backups created by a backup job configured in Veeam Agent for IBM AIX, use the following command:

```
veeamconfig backup list [--all]
```

In the list of backups, Veeam Agent displays information about backups stored on local backup repositories and backup repositories managed by a Veeam backup server.

The `--all` option instructs Veeam Agent to display information about all Veeam Agent for IBM AIX backups in backup repositories configured in the product. If you do not use this option, Veeam Agent will display information about backups of the current Veeam Agent computer only (that is, the computer where you run the `veeamconfig backup list` command).

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>Name of the backup 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.</td>
</tr>
</tbody>
</table>

Imported backups are marked as *Imported* in the Repository column. For information about the import procedure, see Importing Backups.

| Created at  | Date and time when the backup was created.                                  |

For example:

```
user@unixsrv:-$ veeamconfig backup list
Job name               Backup ID                               Repository
unixsrv system backup  {bd99e384-b62f-47dc-ad38-f0b3dc5d3c40}  [srv14] Default Backup Repository  2020-03-16 11:49
unixsrv file backup    {d2bc5ec7-9545-4740-b452-7a91db7a90c8}  backup0  2020-03-16 13:30
```
Viewing Backup Details

You can view detailed information about specific backup. To view backup details, use the following command:

```
veeamconfig backup show --id <backup_id>
```

where `<backup_id>` is an ID of the backup for which you want to view detailed information.

For a file-level backup, Veeam Agent for IBM AIX displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine name</strong></td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td><strong>Backed up</strong></td>
<td>Backup scope for the file-level backup job.</td>
</tr>
<tr>
<td><strong>Include masks</strong></td>
<td>File name masks that define files that must be included in the backup. This information is displayed if file name masks are specified for the backup job.</td>
</tr>
<tr>
<td><strong>Excluded from backup</strong></td>
<td>Directories that must be excluded from backup.</td>
</tr>
<tr>
<td><strong>Exclude masks</strong></td>
<td>File name masks that define files that must be excluded from the backup. This information is displayed if file name masks are specified for the backup job.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup show --id ea64a7e5-038a-4c86-970a-6d59d4cf3968
Machine name: srv01 system backup
File-level backup
Backed up:
/
Excluded from backup:
/mnt/NFS
/proc
/tmp/veeam
```
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> [--all]
```

where:

- `<backup_id>` — ID of the backup whose restore points you want to view.
- `--all` — instructs Veeam Agent to display information about the restore points in the backup that was created by Veeam Agent for IBM AIX on another machine.

For example:

```
user@srv01:~$ veeamconfig backup info --id 4f75bb20-a6b6-4323-9287-1c6c8cecccb6b
```

or

```
user@srv01:~$ veeamconfig point list --backupid 4f75bb20-a6b6-4323-9287-1c6c8cecccb6b
```

Veeam Agent for IBM AIX 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. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
</tbody>
</table>
For example:

```
user@unixsrv:~$ veeamconfig point list --backupid bd99e384-b62f-47dc-ad38-f0b3dc5d3c40

<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>unixsrv system backup</td>
<td>{2159eb5a-1f18-4b67-be90-98615c0057f3}</td>
<td>Full</td>
<td>2020-03-16 11:50</td>
<td>false</td>
</tr>
<tr>
<td>unixsrv system backup</td>
<td>{6303185a-37fe-460a-8e6c-65746708fe77}</td>
<td>Increment</td>
<td>2020-03-16 12:29</td>
<td>false</td>
</tr>
<tr>
<td>unixsrv system backup</td>
<td>{530843a2-5b7d-4a12-9718-b8d9a66b6a70}</td>
<td>Increment</td>
<td>2020-03-16 14:00</td>
<td>false</td>
</tr>
</tbody>
</table>
```
Importing Backups

You can import a backup created by Veeam Agent for IBM AIX 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 for IBM AIX installed on another machine. You cannot import backups that reside in a Veeam Backup & Replication repository.

To import a backup:

1. Start the import process with the following command:

   ```bash
   veeamconfig backup import --path <path>
   ```

   where `<path>` is a path to the VBM file of the backup that you want to import.

   For example:

   ```bash
   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:

   ```bash
   veeamconfig session log --id <session_id>
   ```

   where `<session_id>` is an ID of the import session.

   For example:

   ```bash
   user@srv01:~$ veeamconfig session log --id 4031f058-766c-4f2c-a7ae-7257adb2929f
   2020-03-19 13:21:33 UTC {6ae2922d-454b-4a8d-a11b-2b5c7a85029d} [info] Importing backup
   2020-03-19 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:

   ```bash
   veeamconfig backup list
   ```
Importing Encrypted Backups

You can import an encrypted backup created by Veeam Agent for IBM AIX into the Veeam Agent database. This operation is required if you want to restore data from an encrypted backup created by Veeam Agent for IBM AIX running on another machine. Note that you cannot import backups that reside in a Veeam Backup & Replication repository.

To import an encrypted backup:

1. Start the import process with the following command:

   ```bash
   veeamconfig backup import --path <path>
   ```

   where `<path>` is a path to the VBM file of the backup that you want to import.

   For example:

   ```bash
   user@srv01:~$ veeamconfig backup import --path /home/share/srv15\ Backup/Backup.vbm
   ```

2. Veeam Agent for IBM AIX will prompt you to provide a password for the backup file. Type in the password and press `[Enter]` to import the backup.

   Veeam Agent for IBM AIX 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 for IBM AIX will decrypt the backup file and import it into the database.

   If you do not enter the password, Veeam Agent will import the backup in the database but will not decrypt the backup file. In this case, because no password is stored in the Veeam Agent database, you will need to provide the password later, when you mount the backup or restore point during file-level restore.

   ```bash
   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
y    Created at
srv15 Backup        {4b1f873c-857d-b984-4f22-6ce66bf62570}  Importe
d    2020-03-12 20:20
srv01 ServerBackup  {f212f641-54aa-40de-a0eb-8727be56760b}  Importe
d    2020-03-12 20:04
```
Deleting Backups

Backup files created with Veeam Agent for IBM AIX are removed automatically according to the retention policy settings. You can also remove backups from the target location and/or Veeam Agent for IBM AIX configuration database manually if necessary.

Removing Backup from Configuration

To remove a backup from the Veeam Agent for IBM AIX configuration database, use the following command:

```
veeamconfig backup delete --id <backup_id>
```

where `<backup_id>` is an ID of the backup that you want to delete.

The way Veeam Agent for IBM AIX 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 for IBM AIX 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 IBM AIX will remove records about the deleted backup from the configuration database and, additionally, delete backup files themselves from the backup location.
Performing Restore

If you experience a problem with your machine, your data gets lost or corrupted, you can use one of the following options to restore your data or bring the machine back to work.

In This Section

- Bare-Metal Recovery
- Restoring Files and Directories
- Restoring Data from Encrypted Backups
Bare-Metal Recovery

If the OS on the machine fails to start, you can boot the OS from Veeam Recovery Media. After that, you can use Veeam Agent for IBM AIX to perform system and data restore. You can also use standard IBM AIX command line utilities to diagnose problems and fix errors.

Before you initiate bare-metal recovery, check the prerequisites; then boot the machine from Veeam Recovery Media. To restore data, you can use the Veeam Recovery Media wizard or command line interface (CLI).

In This Section

- Before You Begin
- Booting from Veeam Recovery Media
- Restoring Data with Recovery Wizard
- Restoring Data in Command Line Interface
Before You Begin

Before you boot from the recovery image and restore your data, review the following prerequisites and considerations:

- You must have a recovery image on any media from which your machine can boot: CD/DVD/BD, removable storage device or Virtual Media Library.

- To restore the system and data, you must have both Veeam Recovery Media and data backup. Make sure that the backup is available on the machine drive (local or external), on a network shared folder or on the backup repository managed by a Veeam Backup server.

  Restoring files with Veeam Recovery Media requires a backup that includes the full contents of the root directory. To configure a job for such backup, set the value of the --includedirs option to /. For details, see Creating Backup Jobs.

- The media type on which you have created the recovery image must be set as a primary boot source on the machine.

- The backup from which you plan to restore data must be successfully created at least once.

- [For backups stored in network shared folders or 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 Veeam backup repository, you must have permissions to access that backup repository. To learn more, see Setting Up User Permissions on Backup Repositories.

- When you restore data with Veeam Recovery Media, Veeam Agent for IBM AIX restores backup content directly to the available disks of the recovered system and replaces the current disk content.
Booting from Veeam Recovery Media

To boot your machine from Veeam Recovery Media:

1. Attach the media with the recovery image to your machine:
   - [For CD/DVD/BD] Insert the media with the recovery image into the machine drive.
   - [For removable storage device] Attach the removable storage device with the recovery image to the machine.
   - [For virtual drives/devices] Mount CD/DVD drive or removable storage device with the recovery image to the virtual machine.

2. Set the device that contains the recovery image as the primary boot source on the machine.

3. Boot the machine.

4. Wait for Veeam Agent to load files from Veeam Recovery Media.

   **NOTE**
   
   When the machine boots, the system automatically configures network interfaces using DHCP. In case DHCP server is not available, you can configure network settings manually. For details, see *Configure Network Settings*. For more information on configuring network settings using command line, see IBM AIX documentation.

5. As the OS boots, you will be asked to define the system console. Type 1 and press **Enter** to select the current terminal.
6. 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 10 seconds.

If you do not want to start the SSH server, make sure that the **Skip starting SSH server** button is selected and press **Enter**.

7. 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 machine booted from the Veeam Recovery Media
- User name and password of the account for connecting to the Veeam Recovery Media
- Fingerprints of the machine booted from the Veeam Recovery Media
8. 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**.

### Veeam Recovery Media Menu

The main menu of Veeam Recovery Media offers the following options:

- **Restore the entire machine** – launches the Veeam Recovery wizard to perform bare-metal recovery. For details, see [Restoring Data with Recovery Wizard](#).
- **Restore files** – launches the File-Level Restore wizard to restore additional data. For details, see [Restore Additional Files](#).
- **Settings** – contains two options:
  - **Configure network** – allows you to verify the network settings have been configured correctly or to configure network adapter manually. To learn more, see [Configure Network Settings](#).
  - **Restore method** – allows you to select the restore algorithm for bare-metal recovery. To learn more, see [Select Restore Method](#).
- **Stop SSH / Start SSH** – allows you to stop or start the SSH server.
- **Exit to shell** – launches Command Line Interface. Select this option if you want to [run bare-metal recovery using Veeam Agent commands in the terminal](#).
- **Reboot** – restarts the machine. Select this option to finish working with Veeam Recovery Media.
- **Shutdown** – powers off the machine.
NOTE

If you exit the Veeam Recovery Media menu, you can return to it any time by running this command in the terminal: `veeamconfig recoveryui`.

Navigating Veeam Recovery Media Menu and Wizards

In the Veeam Recovery Media wizard, the use of mouse is not supported. To navigate the 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 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.
- **Escape** — to return to the previous step of the wizard or to exit the wizard if you are in the main menu.
Restoring Data with Recovery Wizard

In the event of a disaster, you can boot the machine from Veeam Recovery Media and restore data using the Recovery wizard.

Before you initiate bare-metal recovery, review the prerequisites. Then boot the system from the Recovery Media and complete these steps:

1. Configure network settings.
2. Select restore method.
3. Launch Recovery wizard.
4. Select backup location.
5. Specify backup location settings.
6. Select backup and restore point.
7. Review setup and launch restore process.
8. [Optional] Restore additional files.

Related Topics

- Data Restore
- Creating Veeam Recovery Media
Step 1. Configure Network Settings

You can use the Configure Network wizard to verify network settings automatically configured during system boot or to configure the network adapter manually.

To open the Configure Network wizard, do the following:

1. In the main menu of Veeam Recovery Media, select **Settings** and press **Enter**.

2. In the **Settings** list, select **Configure network** and press **Enter**.
Veeam Agent displays network adapters that are available on the system.

If there is a DHCP server in your network, Veeam Agent configured network settings automatically and displays the IP address assigned to the network adapter. You can then press Esc to return to the main menu.

If network settings were not configured automatically, you can specify them manually.

### Specifying Network Settings

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 (static)** option and press Enter.

3. In the **Adapter settings** dialog, specify the following network settings: IP address, subnet mask, default gateway and DNS server.

4. Select **Apply** and press Enter.
Resetting Adapter to Auto Configuration

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 (DHCP) option and press Enter. Veeam Agent will automatically configure network settings for the adapter.

Disabling Network Adapter

To disable the selected network adapter, in the Configure adapter dialog select Disable. The Choose adapter list displays the down status of the disabled adapter.
Step 2. Select Restore Method

By default, during restore Veeam Agent uses the algorithm that first recreates logical volumes with greater number of copies and allocates them to available devices according to their allocation requests. This approach covers most system configurations. To suit a specific system structure, you can select a different restore algorithm for the recovery. To do this, complete the following steps:

1. From the main menu of Veeam Recovery Media, select **Settings**.

2. In the **Settings** list, select **Restore method**.

3. Choose one of the available options:
   - **Simple** — select this method for environments with simple structure. This restore algorithm recreates logical volumes (LVs) in their latest state without reconstructing the exact distribution of physical partitions by disks.
   - **Use PP map** — select this method if you are restoring to the original hardware and want to restore the original physical partition layout. This restore algorithm attempts to restore physical partition allocation as close to the original system as possible.
Use order – keep this default method selected to cover complex setups with multiple copies of the same LV. This restore algorithm recreates LVs with greater number of copies first and does not preserve LV devices' major and minor numbers.

4. Use the Tab key to select Continue and press Enter.

5. Press Esc to return to the main menu.
Step 3. Launch Recovery Wizard

To launch the Recovery wizard, in the main menu select **Restore the entire machine**.
Step 4. Select Backup Location

At the **Select backup location** step of the wizard, specify the location of the backup file from which you want to restore data.

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 machine or storage drive. 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.

**NOTE**

The `/dev/ram0` option represents the disk generated by the system in the machine RAM. It contains the file system of the recovery image OS. When you boot the machine from Veeam Recovery Media, this file system does not contain any backups. You can use this option after you mount a network shared folder or local disk to the file system of the recovery image OS to browse for backup files in the mounted location.
Step 5. Specify Backup Location Settings

Specify settings for the target storage that contains the 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.

Specifying Shared Folder Settings

The *Mount shared folder* step of the wizard appears if you have selected to restore data from a backup file located in a network shared folder.

**NOTE**

Consider the following:

- For bare-metal recovery, Veeam Agent for IBM AIX 4.0 only supports connection to servers that use version 3 of the NFS protocol.
- If the backup file from which you want to restore resides in an SMB (CIFS) network shared folder, you must mount it using command line interface prior to launching the Recovery wizard. For details, see [Mounting Backup Storage](#).

To specify settings for an NFS network shared folder:

1. 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.

![Mount Shared Folder](image)
2. Press **Enter** to connect to the network shared folder. Veeam Agent mounts the specified network shared folder to the `/tmp/veeam` directory of the recovery image OS file system and displays the content of the network shared folder.

![Screenshot of Veeam Recovery Media](image)

**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 machine drive.

1. Veeam Recovery Media wizard displays the content of the volume groups imported from all known disks. Select the device that contains the backup and press **Enter**.

![Screenshot of Veeam Recovery Media](image)

Veeam Agent for IBM AIX will mount the selected device to the `/tmp` directory of the recovery image OS file system and displays the contents of the directory.
2. Browse to the directory that contains the backup file, select the backup file and press **Enter**.

Veeam Agent will import the selected backup file.

Veeam Agent will also add the mounted local drive directly to the list of available backup locations:

**Specifying Veeam 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 a Veeam backup server.

**IMPORTANT**

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](#).
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 the name of the account that has access to the Veeam backup repository.

4. [Optional] If the server is assigned to a domain, in the **Domain** field, type the name of the domain in which the account that has access to the Veeam backup repository is registered — for example, *tech*.

5. In the **Password** field, type the 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 display the list of backups for your machine that are located in the selected Veeam backup repository.
Step 6. Select Backup and Restore Point

At this step of the wizard, select the backup and restore point from which you want to restore data.

The **wizard** window has two panes:

- The **Imported backups** pane on the left displays information about backup: host name of the machine whose data is stored in the backup file, backup job name and number of restore points.

  **TIP**

  By default, the **Imported backups** pane displays backups of the machine on which Veeam Recovery Media was created. If you want to restore data from a backup that was created on another machine, select the **Show all** option to choose from the list of all backups available in the current location.

- The **Restore points** pane on the right displays the 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 restore 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 **Select Backup Location**.
2. In the **Restore points** pane, with **Up** and **Down** keys select the restore point from which you want to restore data and press **Enter**.

3. If you selected an encrypted backup for data restore, Veeam Agent prompts you to provide a password to unlock the encrypted file.

To learn more, see [Restoring Data from Encrypted Backups](#).
Step 7. Review Setup and Launch Restore Process

At the **Recovery summary** step of the wizard, complete the setup of the bare-metal recovery procedure.

1. Review the recovery summary.

2. Press **Enter** to start the recovery process.

   Veeam Agent will first remove data from the disks that were selected for recovery, then restore system structure and data from the backup, and finally create the boot loader.

   **TIP**
   
   You can stop the recovery process any time by pressing the **s** key. The operation will be canceled and you will return to the main menu.
3. Once the recovery is completed successfully, press **Esc** to return to the main menu.

<table>
<thead>
<tr>
<th>Time</th>
<th>Action</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:14:59</td>
<td>Job started at 2022-05-12 10:14:59 UTC</td>
<td></td>
</tr>
<tr>
<td>10:15:02</td>
<td>Starting base metal restore</td>
<td></td>
</tr>
<tr>
<td>10:15:03</td>
<td>Repository does not support log export</td>
<td></td>
</tr>
<tr>
<td>10:15:04</td>
<td>Waiting for backup infrastructure res...</td>
<td>00:00:02</td>
</tr>
<tr>
<td>10:15:07</td>
<td>Created rootvg volume group</td>
<td>00:00:45</td>
</tr>
<tr>
<td>10:15:08</td>
<td>Created logical volumes on rootvg vol...</td>
<td>00:00:38</td>
</tr>
<tr>
<td>10:15:12</td>
<td>Created file systems on rootvg volume...</td>
<td>00:00:41</td>
</tr>
<tr>
<td>10:15:15</td>
<td>Created mount points on rootvg volume...</td>
<td>00:00:41</td>
</tr>
<tr>
<td>10:15:57</td>
<td>Restoring files</td>
<td>00:02:50</td>
</tr>
<tr>
<td>10:15:57</td>
<td>Restoring files from [/] to [/]</td>
<td></td>
</tr>
<tr>
<td>10:15:57</td>
<td>Exclude dir []</td>
<td></td>
</tr>
<tr>
<td>10:16:05</td>
<td>Restoring the bootloader</td>
<td>00:00:16</td>
</tr>
</tbody>
</table>
Step 8. Restore Additional Files

Before you reboot the machine upon successful bare-metal recovery, you may need to restore additional data from another backup. To do this, you can use the file-level restore functionality of the Recovery wizard. Veeam Agent mounts the backup file to the file system of the recovery image OS. After that, you can copy the necessary files or directories to a desired location.

**NOTE**

If the additional files you want to restore are not required for correct system startup after reboot, you can perform file-level restore after you reboot the machine upon successful bare-metal recovery. In this case, follow the standard procedure as described in Restoring Files and Directories.

To perform additional file-level restore using Recovery wizard, do the following:

1. From the main menu of Veeam Recovery Media, select **Restore files**.

   The wizard switches directly to the backup location you previously defined during bare-metal recovery.

2. Select the backup file and restore point you want to use for file-level restore as described in Select Backup and Restore Point.

   **NOTE**
   
   If your backup file is in a different location:
   
   1. Press the **j** key to get to the **Select backup location** step of the wizard.
   2. **Select backup location**.
   3. **Specify backup location settings**.
   4. **Select backup and restore point**.
3. Press **Enter** to mount the backup file. By default, backup content is mounted into the `/mnt/backup` directory of the recovery image OS file system.

4. On the confirmation message, select **Ok** and press **Enter**.

5. From the main menu, select **Exit to shell**.

6. In the terminal, save the necessary files and directories to a desired location. For details, see Save Restored Files.
Step 9. Finish Working with Veeam Recovery Media

When the restore operation is completed, finish working with Veeam Recovery Media and start your operating system.

**NOTE**

Consider the following before you reboot the recovered system:

- Veeam recovery environment starts in the machine RAM. Bare-metal recovery (BMR) logs are saved to the `/var/log/veeam` directory of the recovery system OS file system and to the repository that contains the backup file you used for data restore. If the repository does not support log export, you risk losing all BMR logs because local logs are lost on system reboot. We recommend saving them to a remote location or to the recovered file system for further reference.
- If the system recovers successfully, at the next launch the machine will automatically boot from the hard drive.

1. Reboot the machine.
2. Wait for the IBM AIX operating system to start.
3. Verify network settings. If necessary, reconfigure the network interface.
4. [Optional] If Veeam Agent on the original machine had integration with Veeam backup server, verify connection to the server by running the following command:

   ```bash
   veeamconfig vbrserver resync
   ```

   If the machine obtained a different ID after recovery, Veeam Agent may have a problem connecting to Veeam backup server. To fix the issue, use the following command:

   ```bash
   veeamconfig vbrserver edit --password
   ```

   Veeam Agent prompts you to re-enter the password for the backup server account. After Veeam backup server confirms the password, the integration gets restored.
Restoring Data in Command Line Interface

In the event of a disaster, you can boot the machine from Veeam Recovery Media and use Veeam Agent for IBM AIX to restore data in command line interface. When you restore data with Veeam Recovery Media, Veeam Agent for IBM AIX restores backup content directly to the available disks of the recovered system and replaces any current disk content.

**IMPORTANT**

Be careful while working with file system of the recovery image OS in command line. Since you log in to the recovery image OS under the super user (root) account, you can perform unlimited operations including deleting files and directories on the mounted volume or in the mounted network shared folder.
Step 1. Launch Terminal

When the machine boots from Veeam Recovery Media, Veeam Agent automatically launches the Veeam Recovery Media menu.

To activate the terminal dialog, from the main menu of Veeam Recovery Media, select **Exit to shell**.

**NOTE**

After you exit the Veeam Recovery Media menu, you can return to it any time by running this command in the terminal: `veeamconfig recoveryui`. 
Step 2. Specify Backup Location

When you boot the machine from Veeam Recovery Media, the recovery environment contains a new installation of Veeam Agent for IBM AIX. Before you restore data, you must point the Veeam Agent to the repository that contains the backup file you plan to restore from. You can also import the backup file, in which case you do not need to place the backup file into a repository.

- To restore data from a backup file stored on a local disk or in a network shared folder, you must complete the following steps to provide Veeam Agent with access to the backup file:
  a. Mount the backup storage to the file system of the recovery image OS. To learn more, see Mounting Backup Storage.
  b. Create a local backup repository. For details, see Creating Backup Repository.
  c. Rescan your local backup repository. To learn more, see Rescanning Backup Repository.

**NOTE**
Alternatively, after you mount the backup storage, you can import the backup file. This will make the backup file visible to Veeam Agent without creating a repository in the backup file storage location. To learn more, see Importing Backup File.

- To restore data from a backup file that resides in a repository managed by Veeam Backup & Replication, you must connect to the Veeam Backup & Replication server. To learn more, see Connecting to Veeam Backup Server.

Mounting Backup Storage

You can mount the following types of backup storage:

- Block device that represents a volume on a local disk or external drive on which the backup file resides. To learn more, see Mounting File System.
- Network shared folder — NFS or SMB (CIFS). To learn more, see Mounting Network Shared Folder.

Mounting File System

To mount a file system where the backup file resides, you must do the following using standard IBM AIX shell commands:

- Import the volume group that contains the logical volume with the backup file.

**NOTE**
- The name of the imported volume group must be different from its original name.
- If the volume group spans several disks, all of them must be available to the system before import.

- Rename the logical volumes and file systems in the imported volume groups to avoid name conflict during data restore.
- Create a mount point.
- Mount the file system with the backup file to the mount point directory.
Mounting Network Shared Folder

Depending on the version of your IBM AIX OS and the file system type of the network shared folder — NFS or SMB (CIFS) — syntax for mounting a network folder may vary. For more information on using the `mount` command in your specific OS environment, see IBM AIX documentation.

If the backup that you want to use for bare-metal recovery resides in an SMB (CIFS) network shared folder, consider the following:

- IBM AIX OS does not provide native support of SMB (CIFS) protocol and needs additional packages installed to handle it. During bare-metal recovery, you can mount an SMB (CIFS) shared folder only if SMB (CIFS) support was implemented on the original system.

- Prior to mounting an SMB (CIFS) shared folder to the recovery image OS file system, you must create an `nsmb0` device by running the `/SPOT/usr/bin/smbd-start` script in the recovery environment. After you execute the script, you can mount an SMB (CIFS) folder using the standard `mount` command.

  **NOTE**
  
  If you run the `/SPOT/usr/bin/smbd-start` script to create an `nsmb0` device, some volume groups may become unavailable after reboot. For details, see [this Veeam KB article](#).

Creating Backup Repository

After you mounted the storage with a backup file, set it as a Veeam Agent backup repository. To do this, use the following command:

```
veeamconfig repository create --name <repository_name> --location <path>
```

where:

- `<repository_name>` – desired name for the backup repository.
- `<path>` – path to the directory in the local file system of the machine in which the backup file is stored.

For example:

```
root@srv01:/# veeamconfig repository create --name VeeamBackup --location /mnt/backup
```
Rescanning Backup Repository

After you created the backup repository, you must rescan the repository to refresh the list of available backups.

To rescan a 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:

```
root@srv01:/# veeamconfig repository rescan --name VeeamBackup
```

Importing Backup File

When you perform bare-metal recovery, you can restore data from an imported backup file created by Veeam Agent for IBM AIX. To do this, you first mount the backup storage, then import the backup file into the Veeam Agent database. You cannot import backups that reside in a Veeam Backup & Replication repository.

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:

```
root@srv01:/# veeamconfig backup import --path /mnt/backup/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:

```
root@srv01:/' veeamconfig session log --id 4031f058-766c-4f2c-a7ae-7257adb2929f  
2020-03-19 13:21:33 UTC {6ae2922d-454b-4a8d-a11b-2b5c7a85029d} [info] Importing backup  
2020-03-19 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:

```
root@srv01:/ # veeamconfig backup list
Job name            Backup ID                               Repository
BackupJob           {64957b1d-d219-456c-a9cd-9598292c10cd}  Imported 2022-01-26 16:21
```

**Importing Encrypted Backups**

You can import an encrypted backup created by Veeam Agent for IBM AIX into the Veeam Agent database. This operation is required in the following situations:

- During bare-metal recovery if you want to restore data from any encrypted backup file.
- During standard file-level restore if you want to restore data from an encrypted backup file created by Veeam Agent on another machine.

**NOTE**

You cannot import backups that reside in a repository managed by Veeam backup server.

To import an encrypted backup:

1. Start the import process with the following command:

```
veeamconfig backup import --path <path>
```

where `<path>` is a 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 for IBM AIX will prompt you to provide a password for the backup file. Type in the password and press [Enter] to import the backup.

Veeam Agent for IBM AIX 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 for IBM AIX will decrypt the backup file and import it into the database.

If you do not enter the password, Veeam Agent will import the backup in the database but will not decrypt the backup file. In this case, because no password is stored in the Veeam Agent database, you will need to provide the password later, when you mount the backup or restore point during file-level restore.

```
user@srv01:~$ veeamconfig backup import --path /home/share/srv15\ Backup/B
ackup.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
ty    Created at
srv15 Backup        {4b1f873c-857d-b984-4f22-6ce66bf62570}  Importe
d    2020-03-12 20:20
drv01 ServerBackup  {f212f641-54aa-40de-a0eb-8727be567f60b}  Importe
d    2020-03-12 20:04
```

Connecting to Veeam Backup Server

If the backup file from which you plan to restore data resides in a repository managed by Veeam backup server, you must connect to that Veeam backup server.

**IMPORTANT**

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.
To connect to Veeam backup server, use the following command:

```
veeamconfig vbrserver add --name <vbr_server_name> --address <vbr_server_ip_address> [--port <vbr_port>] --login <username> [--domain <domain>] [--password <user_password>]
```

where:

- `<vbr_name>` — name of the Veeam backup server that manages the backup repository.
- `<vbr_address>` — IP address of the Veeam backup server.
- `<vbr_port>` — Veeam Agent for IBM AIX uses the default port 10006 to communicate with the Veeam Backup & Replication server.
- `<username>` — user name of the account that has access to the Veeam backup repository.
  You can specify a user name in the `username` or `username@domain` format. In the latter case, you do not need to specify a domain as a value of the `--domain` option.

**NOTE**

You cannot provide a user name in the `domain\username` format.

- `<domain>` — use this option to specify the domain of the Veeam Backup & Replication server if your IBM AIX machine and the Veeam Backup & Replication server are in different domains.
- `<password>` — password of the account that has access to the Veeam backup repository. If you do not specify the password, Veeam Agent will prompt you to provided it prior to executing the `veeamconfig vbrserver add` command.

For example:

```
root@srv01:/# veeamconfig vbrserver add --name vbr01 --address 172.24.137.4 --login veeam --domain tech --password P@ssw0rd
```

For more information on interacting with Veeam Backup & Replication servers, see Managing Veeam Backup & Replication Servers.
Step 3. Locate Backup

To view the list of backups created by Veeam Agent for IBM AIX, use the following command:

```
veeamconfig backup list
```

By default, this command includes the `--all` option and instructs Veeam Agent to display information about all Veeam Agent for IBM AIX backups in backup repositories configured in Veeam Agent.

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>Name of the backup 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.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time when the backup was created.</td>
</tr>
</tbody>
</table>

For example:

```
root@srv01:# veeamconfig backup list
Job name               Backup ID                               Repository
y          Created at
srv01 system backup  {bd99e384-b62f-47dc-ad38-f0b3dc5d3c40}    VeeamBacku
p 2022-01-26 11:49
```
Step 4. Explore Backup Content

To view detailed information about specific backup, use the following command:

```
veeamconfig backup show --id <backup_id>
```

where `<backup_id>` is the ID of the backup that you want to explore.

Veeam Agent displays the following information about a file-level backup:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine name</strong></td>
<td>Host name of the machine on which the backup job is configured and the name of the job.</td>
</tr>
<tr>
<td><strong>Backed up</strong></td>
<td>Backup scope for the file-level backup job.</td>
</tr>
<tr>
<td><strong>Include masks</strong></td>
<td>File name masks that define files that must be included in the backup. This information is displayed if file name masks are specified for the backup job.</td>
</tr>
<tr>
<td><strong>Excluded from backup</strong></td>
<td>Directories that must be excluded from backup.</td>
</tr>
<tr>
<td><strong>Exclude masks</strong></td>
<td>File name masks that define files that must be excluded from the backup. This information is displayed if file name masks are specified for the backup job.</td>
</tr>
</tbody>
</table>

For example:

```
root@srv01:/# veeamconfig backup show --id bd99e384-b62f-47dc-ad38-f0b3dc5d3c40
Machine name: srv01 system backup
File-level backup
Backed up:
 /
Excluded from backup:
 /mnt/NFS
 /proc
 /tmp/veeam
```
Step 5. 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> [--all]
```

where:

- `<backup_id>` — ID of the backup whose restore points you want to view.
- `--all` — instructs Veeam Agent to display information about the restore points in the backup that was created by Veeam Agent for IBM AIX on another machine.

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>
<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. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
</tbody>
</table>
For example:

```
root@srv01:~$ veeamconfig backup info --id bd99e384-b62f-47dc-ad38-f0b3dc5d3c40
```

```
<table>
<thead>
<tr>
<th>Job name</th>
<th>OIB ID</th>
<th>Type</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv01 system backup</td>
<td>{2159eb5a-1f18-4b67-be90-98615c0057f3}</td>
<td>Full</td>
<td>2022-01</td>
</tr>
<tr>
<td>-26 11:50</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 system backup</td>
<td>{6303185a-37fe-460a-8e6c-65746708fe77}</td>
<td>Increment</td>
<td>2022-01</td>
</tr>
<tr>
<td>-26 12:29</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 system backup</td>
<td>{530843a2-5b7d-4a12-9718-b8d9a66b6a70}</td>
<td>Increment</td>
<td>2022-01</td>
</tr>
<tr>
<td>-26 14:00</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 system backup</td>
<td>{27abf598-ca38-40de-8d44-93231fcd5ea6}</td>
<td>Increment</td>
<td>2022-01</td>
</tr>
<tr>
<td>-27 14:00</td>
<td>false</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

or

```
root@srv01:~$ veeamconfig point list --backupid bd99e384-b62f-47dc-ad38-f0b3dc5d3c40
```

```
<table>
<thead>
<tr>
<th>Job name</th>
<th>OIB ID</th>
<th>Type</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>srv01 system backup</td>
<td>{2159eb5a-1f18-4b67-be90-98615c0057f3}</td>
<td>Full</td>
<td>2022-01</td>
</tr>
<tr>
<td>-26 11:50</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 system backup</td>
<td>{6303185a-37fe-460a-8e6c-65746708fe77}</td>
<td>Increment</td>
<td>2022-01</td>
</tr>
<tr>
<td>-26 12:29</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 system backup</td>
<td>{530843a2-5b7d-4a12-9718-b8d9a66b6a70}</td>
<td>Increment</td>
<td>2022-01</td>
</tr>
<tr>
<td>-26 14:00</td>
<td>false</td>
<td></td>
<td></td>
</tr>
<tr>
<td>srv01 system backup</td>
<td>{27abf598-ca38-40de-8d44-93231fcd5ea6}</td>
<td>Increment</td>
<td>2022-01</td>
</tr>
<tr>
<td>-27 14:00</td>
<td>false</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step 6. Start Restore Process

You can perform data restore in one of the following ways:

- Restore data from a backup. Veeam Agent restores files from the latest restore point. For details, see Restoring Files from Backup.
- Restore data from a restore point. Veeam Agent restores files from a specific point within a backup. For details, see Restoring Files from Restore Point.

Restoring Files from Backup

To start the process of data restore from a backup file, use the following command:

```
veeamconfig backup restore {--id <backup_id> | --path <vbm_path>} [--method <1|2|3>] [--ExcludeDirs <dir_list>]
```

where:

- `<backup_id>` — ID of the backup file. Alternatively, you can specify path to metadata file of the backup instead of ID by using the `--path` option.
- `<vbm_path>` — path to the metadata file (VBM) of the backup. You can use this option to specify a path to the metadata file of the backup that has not yet been imported into the Veeam Agent database. Veeam Agent will automatically import the backup file from the specified location and start the restore process.
- `<1|2|3>` — restore method to be used during bare-metal recovery:
  - 1 — **Simple**. Select this method for environments with simple structure. This restore algorithm recreates logical volumes (LVs) in their latest state without reconstructing the exact distribution of physical partitions by disks.
  - 2 — **Use PP map**. Select this method if you are restoring to the original hardware and want to restore the original physical partition layout. This restore algorithm attempts to restore physical partition allocation as close to the original system as possible.
  - 3 — **Use order**. Select this method to cover complex setups with multiple copies of the same LV. This restore algorithm recreates LVs with greater number of copies first and does not preserve LV devices’ major and minor numbers.

If you do not specify the restore method, Veeam Agent will use the default **Use order** algorithm for bare-metal recovery.

- `<dir_list>` — comma-separated list of directories to exclude during data restore.

For example:

```
root@srv01:~# veeamconfig backup restore --id 12cfdd6-3bd1-44ae-baa1-653eb90e92e
Restoring file-level backup.
Backup: [12cfdd6-3bd1-44ae-baa1-653eb90e92e]
File-level restore from backup has started.
Session ID: [{cab490e6-3744-4a12-b8d6-deff4f1da640}].
Logs stored in: [/var/log/veeam/Restore/Session_{cab490e6-3744-4a12-b8d6-deff4f1da640}].
```
Restoring Files from Restore Point

To start the restore process from a restore point, use the following command:

```
veeamconfig point restore --id <point_id> [--method <1|2|3>] [--ExcludeDirs <dir_list>]
```

where:

- `<point_id>` — ID of the restore point.
- `<1|2|3>` — restore method to be used during bare-metal recovery:
  - 1 — **Simple**. Select this method for environments with simple structure. This restore algorithm recreates logical volumes (LVs) in their latest state without reconstructing the exact distribution of physical partitions by disks.
  - 2 — **Use PP map**. Select this method if you are restoring to the original hardware and want to restore the original physical partition layout. This restore algorithm attempts to restore physical partition allocation as close to the original system as possible.
  - 3 — **Use order**. Keep this default method selected to cover complex setups with multiple copies of the same LV. This restore algorithm recreates LVs with greater number of copies first and does not preserve LV devices' major and minor numbers.

If you do not specify the restore method, Veeam Agent will use the default **Use order** algorithm for bare-metal recovery.

- `<dir_list>` — comma-separated list of directories to exclude during data restore.

For example:

```
root@srv01:/# veeamconfig point restore --id 6303185a-37fe-460a-8e6c-65746708fe77
Restoring point.
Restore point: 6303185a-37fe-460a-8e6c-65746708fe77

File-level 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}].
```
Step 7. Monitor Restore Process

You can monitor the restore process by viewing the restore session log. To do this, use the following command:

```
veeamconfig session log --id <session_id>
```

where `<session_id>` — ID of the restore session.

For example:

```
root@srv01:/# veeamconfig session log --id 12cfddd6-3bd1-44ae-baa1-653eb909e92e
2022-01-27 10:35:58 UTC {ed66af6-5216-4596-a7b5-be10dd10c32f} [info] Starting file-level restore
2022-01-27 10:36:12 UTC {ed66af6-5216-4596-a7b5-be10dd10c32f} [processing] Restoring files...
```

**TIP**

You can also check the restore session status with the `veeamconfig session info` command. To learn more, see [Viewing Session Status](#).
Step 8. Finish Working with Veeam Recovery Media

When the restore operation completes, finish working with Veeam Recovery Media and start your operating system.

**NOTE**

Before you reboot the recovered system, consider the following:

- Before you reboot the machine upon successful bare-metal recovery, you may need to restore additional data from another backup. In this case, follow the standard procedure of file-level restore as described in Restoring Files and Directories.
- Veeam recovery environment starts in the machine RAM. Bare-metal recovery (BMR) logs are saved to the `/var/log/veeam` directory of the recovery system OS file system and to the repository that contains the backup file you used for data restore. If the repository does not support log export, you risk losing all BMR logs because local logs are lost on system reboot. We recommend saving them to a remote location or to the recovered file system for further reference.
- If the system recovers successfully, at the next launch the machine will automatically boot from the hard drive.

1. Reboot the machine.
2. Wait for the IBM AIX operating system to start.
3. Verify network settings. If necessary, reconfigure the network interface.
4. [Optional] If Veeam Agent on the original machine had integration with Veeam backup server, verify connection to the server by running the following command:

   ```
   veeamconfig vbrserver resync
   ```

   If the machine obtained a different ID after recovery, Veeam Agent may have a problem connecting to Veeam backup server. To fix the issue, use the following command:

   ```
   veeamconfig vbrserver edit --password
   ```

   Veeam Agent prompts you to re-enter the password for the backup server account. After Veeam backup server confirms the password, the integration gets restored.
Restoring Files and Directories

If some files and directories on your machine get lost or corrupted, you can restore them from a backup.

When you perform file-level restore, Veeam Agent for IBM AIX publishes the backup content directly into the machine file system. You can browse files and directories in the backup, restore files and directories to their initial location, copy files and directories to a new location or simply target applications to restored files and work with them as usual.

You can use Veeam Agent for IBM AIX to restore files and directories in one of the following ways:

- **Restore from backup**
  
  When you restore files and directories from a backup, Veeam Agent for IBM AIX will automatically select the latest restore point in the backup. You can restore files and directories to the state in which they were at the time when the latest restore point was created.

- **Restore from restore point**
  
  When you restore files and directories from a 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 and 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.

**NOTE**

Veeam Agent for IBM AIX cannot start a backup job in the LPAR if a restore session is running in a WPAR at the time when the job must start.
Restoring from Backup

With Veeam Agent for IBM AIX command line interface, you can restore files and directories from the backup. When you perform file-level restore from the backup, Veeam Agent for IBM AIX automatically selects the latest restore point in the backup. You can restore files and directories to the state in which they were at the time when the latest restore point was created.
Step 1. Locate Backup

To view the list of backups created by Veeam Agent for IBM AIX, use the following command:

```
veeamconfig backup list [--all]
```

Where `--all` is an option that instructs Veeam Agent to display information about all Veeam Agent for IBM AIX backups in backup repositories configured in the product. If you do not use this option, Veeam Agent will display information about backups of the current Veeam Agent computer only (that is, the machine where you run the `veeamconfig backup list` command).

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>Name of the backup job by which the backup was created.</td>
</tr>
<tr>
<td>Backup UUID</td>
<td>ID of the backup.</td>
</tr>
<tr>
<td>Repository</td>
<td>Name of the backup repository in which the backup was created.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time when the backup was created.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup list --all
Job name             Backup ID                                                                 Repository Created at
unixsrv system backup {bd99e384-b62f-47dc-ad38-f0b3dc5d3c40} [srv14] Default Backup Repository 2020-03-16 11:49
unixsrv file backup  {d2bc5ec7-9545-4740-b452-7a91db7a90c8} backup0 1 2020-03-16 13:30
```

**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 for IBM AIX, you can import such backup into the Veeam Agent for IBM AIX database on your machine. 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>` is an ID of the backup for which you want to view detailed information.

Veeam Agent for IBM AIX displays the following information about file-level backup:

<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>
<tr>
<td>Include masks</td>
<td>File name masks that define files that must be included in the backup. This information is displayed if file name masks are specified for the backup job.</td>
</tr>
<tr>
<td>Excluded from backup</td>
<td>Directories that must be excluded from backup.</td>
</tr>
<tr>
<td>Exclude masks</td>
<td>File name masks that define files that must be excluded from the backup. This information is displayed if file name masks are specified for the backup job.</td>
</tr>
</tbody>
</table>

For example:

```
user@srv01:~$ veeamconfig backup show --id bd99e384-b62f-47dc-ad38-f0b3dc5d3c40
Machine name: srv01 system backup
File-level backup
Backed up:

Excluded from backup:
/mnt/NFS
/proc
/tmp/veeam
```
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 machine file system for file-level restore.

- `<path>` — path to the directory to which you want to mount the backup file content. If you do not specify the path with the `--mountdir` option, Veeam Agent will mount the backup to the `/mnt/backup` directory.

For example:

```
user@srv01:~$ veeamconfig backup mount --id bd99e384-b62f-47dc-ad38-f0b3dc5d3c40 --mountdir /mnt/backup
Backup has been mounted.
Session ID: {dbdf3609-d48c-40bb-9978-2e5baf02f5ba}.
Logs stored in: [/var/log/veeam/Mount/Session_20200317_151317_{dbdf3609-d48c-40bb-9978-2e5baf02f5ba}].
```
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 for IBM AIX session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where `<session_id>` is an ID of the backup mount session.

For example:

```
user@srv01:~$ veeamconfig session log --id dbdf3609-d48c-40bb-9978-2e5baf02f5ba
2020-03-17 14:13:17 UTC {9cef8fc7-7fa0-4971-932e-4d71b4ba2fb4} [info] Job started at 2020-03-17 15:13:17 CET
2020-03-17 14:13:22 UTC {74c7fd91-57cd-4a1c-b5d0-a1310407d650} [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 machine file system, you can use IBM AIX 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 a new location with the IBM AIX command line utilities:

```
user@srv01:~$ ls Documents/
Reports
user@srv01:~$ ls /mnt/backup/home/user/Documents/Reports/
user@srv01:~$ cp /mnt/backup/home/user/Documents/Reports/Report1.pdf Documents/
user@srv01:~$ ls Documents/
Report1.pdf  Reports
```
Step 6. Stop Backup Mount Session

When Veeam Agent for IBM AIX mounts a backup for file-level restore, Veeam Agent for IBM AIX starts a new backup mount session. After you have finished working with restored files and directories, you should 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>` is an ID of the backup mount session that you want to stop.

Veeam Agent for IBM AIX will stop the mount session and unmount the backup from the machine file system. For example:

```
user@srv01:~$ veeamconfig session stop --id dbdf3609-d48c-40bb-9978-2e5baf02f5ba
Session has stopped.
user@srv01:~$ ls /mnt/backup
user@srv01:~$
```
Restoring from Restore Point

With Veeam Agent for IBM AIX command line interface, you can restore files and directories from the specific restore point. When you restore files and directories 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 for IBM AIX, use the following command:

```
veeamconfig backup list [--all]
```

Where `--all` is an option that instructs Veeam Agent to display information about all Veeam Agent for IBM AIX backups in backup repositories configured in the product. If you do not use this option, Veeam Agent will display information about backups of the current Veeam Agent computer only (that is, the machine where you run the `veeamconfig backup list` command).

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>Name of the backup 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.</td>
</tr>
<tr>
<td>Created at</td>
<td>Date and time of the backup creation.</td>
</tr>
</tbody>
</table>

For example:

```
user@unixsrv:~$ veeamconfig backup list --all
Job name               Backup ID                               Repository
unixsrv system backup  {bd99e384-b62f-47dc-ad38-f0b3dc5d3c40}  [srv14] Default Backup Repository 2020-03-16 11:49
unixsrv file backup    {d2bc5ec7-9545-4740-b452-7a91db7a90c8}  backup0 1 2020-03-16 13:30
```

**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 for IBM AIX, you can import such backup into the Veeam Agent for IBM AIX database on your machine. To learn more, see Importing Backups.
Step 2. Explore Restore Points

To view information about restore points in the backup, use the following command:

```bash
veeamconfig backup info --id <backup_id>
```

or

```bash
veeamconfig point list --backupid <backup_id> [--all]
```

where:

- `<backup_id>` — ID of the backup whose restore points you want to view.
- `--all` — instructs Veeam Agent to display information about the restore points in the backup that was created by Veeam Agent for IBM AIX on another machine.

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. Possible values:</td>
</tr>
<tr>
<td></td>
<td>• True</td>
</tr>
<tr>
<td></td>
<td>• False</td>
</tr>
</tbody>
</table>
For example:

```
user@unixsrv:~$ veeamconfig backup info --id bd99e384-b62f-47dc-ad38-f0b3dc5d3c40
Job name               OIB ID                                  Type       Creat
ed at        Is corrupt
unixsrv system backup  (2159eb5a-1f18-4b67-be90-98615c0057f3)  Full       2020-
03-16 11:50  false
unixsrv system backup  (6303185a-37fe-460a-8e6c-65746708fe77)  Increment 2020-
03-16 12:29  false
unixsrv system backup  (530843a2-5b7d-4a12-9718-b8d9a66b6a70)  Increment 2020-
03-16 14:00  false
unixsrv system backup  (27abf598-ca38-40de-8d44-93231fcd5ea6)  Increment 2020-
03-17 14:00  false
```

or

```
user@unixsrv:~$ veeamconfig point list --backupid ea64a7e5-038a-4c86-970a-6d59d4cf3968
Job name               OIB ID                                  Type       Creat
ed at        Is corrupt
unixsrv system backup  (2159eb5a-1f18-4b67-be90-98615c0057f3)  Full       2020-
03-16 11:50  false
unixsrv system backup  (6303185a-37fe-460a-8e6c-65746708fe77)  Increment 2020-
03-16 12:29  false
unixsrv system backup  (530843a2-5b7d-4a12-9718-b8d9a66b6a70)  Increment 2020-
03-16 14:00  false
unixsrv system backup  (27abf598-ca38-40de-8d44-93231fcd5ea6)  Increment 2020-
03-17 14:00  false
```
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 machine file system for file-level restore.
- `<path>` — path to the directory to which you want to mount the backup file content. If you do not specify the `path` with the `--mountdir` option, Veeam Agent will mount the restore point to the `/mnt/backup` directory.

For example:

```
user@srv01:~$ veeamconfig point mount --id 530843a2-5b7d-4a12-9718-b8d9a66b6a70 --mountdir /mnt/backup
Restore point is mounted.
Session ID: [{43516539-1573-4ebc-b52d-01757d38a5aa}].
Logs stored in: [/var/log/veeam/Mount/Session_20200317_153040_{43516539-1573-4ebc-b52d-01757d38a5aa}].
```
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 for IBM AIX session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where `<session_id>` is an ID of the restore point mount session.

For example:

```
user@srv01:~$ veeamconfig session log --id 43516539-1573-4ebc-b52d-01757d38a5aa
2020-03-17 14:30:40 UTC {8b7b6415-73be-4505-aedd-4790e4c7a7e3} [info] Job started at 2020-03-17 15:30:40 CET
2020-03-17 14:30:40 UTC {263b0fc9-45b8-4c08-8ff7-d4640604cfff} [info] Mounting restore point
2020-03-17 14:30:45 UTC {901e9e50-9593-4b91-9e9e-a2adc590cf0a} [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 machine file system, you can use IBM AIX 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 restore point to a new location with the IBM AIX command line utilities:

```
user@srv01:~$ ls Documents/
Reports
user@srv01:~$ ls /mnt/backup/home/user/Documents/Reports/
user@srv01:~$ cp /mnt/backup/home/user/Documents/Reports/Report1.pdf Documents/
user@srv01:~$ ls Documents/
Report1.pdf Reports
```
Step 6. Stop Backup Mount Session

When Veeam Agent for IBM AIX mounts a restore point for file-level restore, Veeam Agent for IBM AIX starts a new restore point mount session. After you have finished working with restored files and directories, you should stop the mount session to unmount the restore point.

To stop the restore point mount session, use the following command:

```bash
veeamconfig session stop --id <session_id>
```

where `<session_id>` is an ID of the restore point mount session that you want to stop.

Veeam Agent for IBM AIX will stop the mount session and unmount the restore point from the machine file system. For example:

```bash
user@srv01:$ veeamconfig session stop --id 43516539-1573-4ebc-b52d-01757d38a5a
Session has stopped.
user@srv01:$ ls /mnt/backup
user@srv01:$
```
Restoring Data from Encrypted Backups

When you restore data from an encrypted backup, Veeam Agent for IBM AIX 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 for IBM AIX database, that is, if you encrypt and decrypt the backup file on the same Veeam Agent machine, you do not need to specify the password. Veeam Agent for IBM AIX 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 for IBM AIX 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 for IBM AIX, you can use the latest password to restore data form 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.

To restore data from an encrypted backup, complete the following steps:

1. Import the encrypted backup file to the Veeam Agent for IBM AIX database. To learn more, see Importing Encrypted Backups.

2. Perform the restore operation in a regular manner. To learn more, see Restoring Files and Folders.
Reporting

For every data transfer operation, for example data backup and restore, backup import and export, Veeam Agent for IBM AIX starts a new session. You can monitor performance of sessions started by Veeam Agent for IBM AIX in the following ways:

- View the session status.
- View session logs.
Viewing Session Status

You can view status of every session that was started by Veeam Agent for IBM AIX. To view the session status, use the following command:

```
veeamconfig session info --id <session_id>
```

where `<session_id>` is an ID of the session for which you want to check status.

Veeam Agent for IBM AIX 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 for IBM AIX 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 for IBM AIX 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 for IBM AIX displays value for this parameter only for completed sessions.</td>
</tr>
</tbody>
</table>

The following example shows status information about the running backup job session:

```
user@srv01:~$ veeamconfig session info --id fb9104a7-b507-46f8-90ea-10601863e8d7
Backup session
  ID: {fb9104a7-b507-46f8-90ea-10601863e8d7}
  Job name: system backup
  Job ID: {fa1ebf29-62f1-47d4-ae91-4e7c209abcd2}
  State: Running
  Start time: 2020-03-16 11:49:47 UTC
  End time: 
```
Viewing Session Logs

You can monitor the backup and restore process by viewing the backup job session and restore session logs. To view a session log, use the following command:

```
veeamconfig session log --id <session_id>
```

where `<session_id>` is an ID of the backup job or restore session.

For example:

```
user@srv01:~$ veeamconfig session log --id fb9104a7-b507-46f8-90ea-10601863e8d7
2020-03-16 10:49:47 UTC {87da2cfc-d6d3-410e-b08f-d723e29e3ed8} [info] Job system backup started at 2020-03-16 11:49:47 CET
2020-03-16 10:49:49 UTC {0d0ec3b2-3e4b-46f2-81e0-db355e888607} [info] Preparing to backup
2020-03-16 10:49:55 UTC {30657591-e968-40bd-ba28-07eafe07bab6} [processing] Waiting for backup infrastructure resources availability
2020-03-16 10:49:57 UTC {30657591-e968-40bd-ba28-07eafe07bab6} [info]
2020-03-16 10:50:05 UTC {d9a40968-5f89-44de-ad88-a550f0da4315} [info] Starting full backup to [srv14] Default Backup Repository
2020-03-16 10:50:06 UTC {bcb20912-b95d-4ef7-893e-2eaa4f8bc3cc} [info] File system indexing is disabled
2020-03-16 10:50:06 UTC {d98e15f8-994c-4375-91c9-1cade3b5410c} [processing] Backing up files /
```
Managing Configuration Database

You can perform the following operations with the Veeam Agent for IBM AIX configuration database:

- Export configuration database to a configuration file.
- Import configuration to the Veeam Agent database.

You can also adjust settings in a configuration file prior to importing configuration. To learn more, see Configuration Format.
Configuration Format

To export and import product configuration, Veeam Agent for IBM AIX uses configuration files in the XML format. A configuration file contains three main blocks:

- Local backup repository settings
- Backup job settings
- Veeam backup server settings

For a sample configuration file, see Example.

Backup Repository Settings

The Repositories block contains backup repository settings. The block contains information about backup repositories that use a local storage, remote storage or network shared folder as a target location for backups. The block has the following structure:

```xml
<Repositories>
  <Repository Name="<LocalRepoName>" Type="LocalDrive">
    <LocalRepoOptions Version="1" Location="/mnt/repo1" DeviceMountPoint=""/>
  </Repository>
  <Repository Name="<LocalRepoName2>" Type="LocalDrive">
    <LocalRepoOptions Version="1" Location="/mnt/repo2" DeviceMountPoint=""/>
  </Repository>
  ...
</Repositories>
```

Adjustable variables:

- Repository Name — backup repository name of your choice.
- Location — path to a mount point where Veeam Agent will create backups.

Backup Job Settings

The Jobs block contains backup job settings. The block contains sub-blocks for each job configured in Veeam Agent for IBM AIX. The block has the following structure:

```xml
Jobs
  Job1
    Job options
    Schedule settings
    Active full backup settings
    Old backups retention
    Objects for backup
  Job2
  ...
```
For example:

```xml
<Job Name="Machine Backup" creation_time="2021-04-28 20:00:00" RepoName="[VBRNAME] VbrRepoName" password="yourpassword" hint="passhint">
  <JobOptions>
    <Schedule />
    <ActiveFullOptions />
    <EnableDeletedVmDataRetention />
    <ObjectsForBackup />
  </JobOptions>
</Job>
```

Adjustable variables:

- **Name** — name of the backup job.
- **creation_time** — date and time when the job was created in the `%Y-%m-%d %H:%M:%S` format.
- **RepoName** — name of the backup repository used as a target location for backup files. The `VBRNAME` value must be the same as the value of the `Name` element in the `VbrServer` section. The `VbrRepoName` value must be the actual name of the repository managed by the backup server.
- **password** — password used for backup data encryption. Applicable to backup jobs targeted at backup repositories other than Veeam backup repository.
- **hint** — password hint. Can be used only with the `password` element.

The `password` and `hint` elements are optional and can be omitted.

**Job Options**

The `JobOptions` block contains backup job settings. The block has the following structure:

```xml
<JobOptions Version="2" Compression="ZlibHigh" BlockSize="KbBlockSize1024" PrejobCommand="" PostjobCommand="" MaxPoints="7" RetryCount="1" RetryTimeOutMs="600000" Schedule="true">
  ...
</JobOptions>
```
Adjustable variables:

- **Compression** — data compression level. Possible values: *none, Rle, Lz4, ZlibLow, ZlibHigh*.
- **BlockSize** — data block size in kilobytes. Possible values: *KbBlockSize256, KbBlockSize512, KbBlockSize1024, KbBlockSize4096, KbBlockSize8192*.
- **PrejobCommand** — path to a pre-job script.
- **PostjobCommand** — path to a post-job script.
- **MaxPoints** — number of restore points to keep in the backup location.
- **RetryCount** — number of retries in case the job fails.
- **RetryTimeOutMs** — time to wait before retry in milliseconds.
- **Schedule** — defines whether schedule is enabled for the job.

**Schedule Settings**

The **Schedule** block contains backup schedule settings. The block has the following structure:

```xml
<Schedule Hours="6" Minutes="0" Type="0" Version="3" IsEnabled="true" WeekDayNumber="Every" DayOfMonth="0">
  <Time Type="0" Hours="6" Minutes="0" />
  <WeekMask Monday="true" Tuesday="true" Wednesday="true" Thursday="true" Friday="true" Saturday="true" Sunday="true" />
  <MonthMask January="true" February="true" March="true" April="true" May="true" June="true" July="true" August="true" September="true" October="true" November="true" December="true" />
</Schedule>
```
Adjustable variables:

- **isEnabled** — defines whether schedule is enabled for the backup job.
- **Hours** — hour when the backup job must start.
- **Minutes** — minute when the backup job must start.
- **WeekMask** — the block that specifies days of the week when the job must start.

### Active Full Backup Settings

The ActiveFullOptions block contains active full backup schedule settings. The block has the following structure:

```xml
<ActiveFullOptions Version="1" IsEnabled="true" WeekDayNumber="Every" DayOfMonth="0">
  <WeekMask>
    Monday="false"
    Tuesday="false"
    Wednesday="false"
    Thursday="false"
    Friday="false"
    Saturday="false"
    Sunday="true"
  </WeekMask>
  <MonthMask>
    January="true"
    February="true"
    March="true"
    April="true"
    May="true"
    June="true"
    July="true"
    August="true"
    September="true"
    October="true"
    November="true"
    December="true"
  </MonthMask>
</ActiveFullOptions>
```

Adjustable variables:

- **isEnabled** — defines whether active full backup schedule is enabled for the backup job.
- **DayOfMonth** — defines active full backup schedule. Set to a number (1-31) to perform active full backup on a specific day of the month. In this case, all values in the **WeekMask** and **MonthMask** blocks should be set to **true**.

Alternatively, you can set the value of this element to 0 (zero). In this case, active full backup will be performed on **true** days from **WeekMask** block.
Old Backups Retention Settings

This block contains retention settings for old backups. These settings are applicable to backup jobs targeted at a Veeam backup repository. To learn more, see Creating Backup Jobs.

The entire block can be removed if not required.

The block has the following structure:

```
<EnableDeletedVmDataRetention EnableDeletedVmDataRetention="true" />
<RetainDays RetainDays="30" />
```

Adjustable variable:

- **RetainDays** – number of days to keep the backup created with the backup job in the target location.

Backup Object Settings

The **ObjectsForBackup** block contains backup scope settings. The block contains **Object** sub-blocks for each object (directory or file mask) included in or excluded from backup.

The **Object** block has the following structure:

```
<Object ObjectType="Directory" RecordType="Include" Value="/var" />
```

Adjustable variables:

- **RecordType** – defines whether to include or exclude an object.
- **Value** – path to an object.

Veeam Backup Server Settings

The **VbrServers** block contains Veeam backup server settings. The block has the following structure:

```
<VbrServers>
    <VbrServer
        Name="VBRNAME"
        login="USERNAME"
        domain=""
        fqdn=""
        password="<your password here>"
        Endpoint="<DNS name/IP address>:<Port>"/>
</VbrServers>
```

Adjustable variables:

- **Name** – arbitrary name of your choice to label the backup server.
- **login** – user name of the account used to connect to the backup server.
- **domain** – to be used in a domain. If the backup server is not in domain then leave the value as is.
• **password** — password of the account used to connect to the backup server. During configuration export, Veeam Agent does not specify the password in this element. For configuration import, specify an actual password manually or leave the element empty. In the latter case Veeam Agent will prompt you to enter a password during configuration import.

• **Endpoint** — resolvable domain name or IP address of the backup server and port over which to connect to the backup server (the default value is 10006).

**Example**

This example displays configuration of Veeam Agent for IBM AIX with the following settings:

- **Backup objects:** `/etc`, `/var`
- **Excluded objects:** `/etc/system.d`
- **Target repository:** `VbrRepoName`
- **Veeam Backup & Replication server name:** `VBRNAME`
- **Veeam Backup & Replication server IP address and port:** `10.1.1.10:10006`
- **Schedule:** every day at 22:15, active full backup on Sunday

```
<?xml version="1.0" encoding="UTF-8"?>
<Config Version="4" PlatformId="{b671deaf-a237-4c3e-0004-000000000003}"

<VbrServers>
  <VbrServer
    Name="VBRNAME"
    login="USERNAME"
    domain=""
    fqdn=""
    password="Pa$$w0rd"
    Endpoint="10.1.1.10:10006"/>
</VbrServers>

<Repositories>
  <Repository Name="LocalRepoName" Type="LocalDrive">
    <LocalRepoOptions Version="1" Location="/mnt/repo" DeviceMountPoint="" />
  </Repository>
</Repositories>

<Jobs>
  <Job Name="MyJob1" creation_time="2021-04-28 20:00:00" RepoName="[VBRNAME] VbrRepoName">
    <JobOptions
      Version="2"
      Compression="ZlibHigh"
      BlockSize="KbBlockSize1024"
      PrejobCommand=""
      PostjobCommand=""
      MaxPoints="7"
      RetryCount="1"
      RetryTimeOutMs="600000"
      Schedule="true">
```

186 | Veeam Agent for IBM AIX | User Guide
<EnableDeletedVmDataRetention EnableDeletedVmDataRetention="true" />
<RetainDays RetainDays="30" />

<Schedule Hours="6" Minutes="0" Type="0" Version="3" IsEnabled="true" WeekDayNumber="Every" DayOfMonth="0">
  <Time Type="0"
    Hours="6"
    Minutes="0" />
  <WeekMask
    Monday="true"
    Tuesday="true"
    Wednesday="true"
    Thursday="true"
    Friday="true"
    Saturday="true"
    Sunday="true"
  />
  <MonthMask
    January="true"
    February="true"
    March="true"
    April="true"
    May="true"
    June="true"
    July="true"
    August="true"
    September="true"
    October="true"
    November="true"
    December="true"
  />
</Schedule>

<ActiveFullOptions Version="1" IsEnabled="true" WeekDayNumber="Every" DayOfMonth="0">
  <WeekMask
    Monday="false"
    Tuesday="false"
    Wednesday="false"
    Thursday="false"
    Friday="false"
    Saturday="false"
    Sunday="true"
  />
  <MonthMask
    January="true"
    February="true"
    March="true"
    April="true"
    May="true"
    June="true"
    July="true"
    August="true"
    September="true"
  />
</ActiveFullOptions>
October="true"
November="true"
December="true"
/>

</ActiveFullOptions>

</JobOptions>

<ObjectsForBackup>

<Object ObjectType="Directory" RecordType="Include" Value="/etc" />
<Object ObjectType="Directory" RecordType="Include" Value="/var" />
<Object ObjectType="Directory" RecordType="Exclude" Value="/etc/system.d" />

</ObjectsForBackup>
</Job>
</Jobs>
Exporting Configuration Database

You can export the Veeam Agent for IBM AIX configuration database to a configuration file in the XML format. This may be useful, for example, if you want to change Veeam Agent for IBM AIX settings by editing a configuration file or copy the Veeam Agent for IBM AIX configuration to another machine.

To export the Veeam Agent for IBM AIX configuration database, use the following command:

```
veeamconfig config export --file <path> [--overwrite]
```

where:

- `<path>` — path to the configuration file to which you want to export configuration.
- `--overwrite` — option that instructs Veeam Agent to overwrite the configuration file if the file already exists at the specified path.

**NOTE**

A directory in which you want to save the configuration file must exist in the file system.

For example:

```
user@srv01:~$ veeamconfig config export --file veeam/config.xml --overwrite
```
Importing Configuration

You can import the Veeam Agent for IBM AIX configuration from a file in the XML format to the configuration database. This may be useful, for example, if you have changed the product settings by editing a configuration file or want to apply configuration of another instance of Veeam Agent for IBM AIX to Veeam Agent installed on your machine.

Keep in mind that Veeam Agent for IBM AIX does not export passwords to an XML configuration file. When you import configuration, Veeam Agent will prompt you to enter the necessary passwords, for example, a password used to connect to the Veeam backup server and passwords for encrypted backups. Alternatively, you can specify passwords manually in the configuration file before importing configuration.

To import the Veeam Agent for IBM AIX configuration, use the following command:

```
veeamconfig config import --file <path>
```

where `<path>` is a path to the configuration file from which you want to import configuration.

For example:

```
user@srv01:~$ veeamconfig config import --file veeam/config.xml
```
Exporting Product Logs

Veeam Agent for IBM AIX 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 for IBM AIX 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 current working directory on the Veeam Agent machine.

To export logs, use the following command:

```
veeamconfig grablogs
```

Veeam Agent for IBM AIX will collect logs, export them to an archive file with the name `veeam_logs_AIX_<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 for IBM AIX, you can use one of the following options:

- You can search for the information about the necessary subject in the current Veeam Agent for IBM AIX User Guide.
- You can visit Veeam R&D Forums and share your opinion or ask a question.
- You can visit the 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 IBM AIX together with Veeam Backup & Replication.

**IMPORTANT**

If you plan to use Veeam Agent for IBM AIX 4.0 with Veeam Backup & Replication, you must install Veeam Backup & Replication 11a (build 11.0.1.1261) or later on the Veeam backup server.

**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.

Veeam Agent for IBM AIX integrates with Veeam Backup & Replication and lets you perform a number of additional disaster recovery tasks and administrative actions with Veeam Agent backups. You can perform the following tasks:

*Data protection tasks*

- Create Veeam Agent backups on backup repositories
- Copy Veeam Agent backups to secondary backup repositories
- Archive Veeam Agent backups to tape

*Restore tasks*

- Restore files and directories from Veeam Agent backups
- Restore data from Veeam Agent backups to virtual disks
- Export Veeam Agent backups to standalone full backup files

*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 properties
- 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 policies 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 Active Directory groups by the backup administrator working with Veeam Backup & Replication. Users with granted access permissions can target Veeam Agent for IBM AIX 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 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 at the backup repository side using its built-in encryption mechanism. To learn more, see Veeam Backup & Replication Documentation.

The Encrypt backups stored in this repository option applies to Veeam Agent for IBM AIX backups and all other backups created on the backup repository.
Managing License

If you plan to use Veeam Agent for IBM AIX 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 IBM AIX machines for which you plan to create backups on a Veeam backup repository. The number of backup jobs configured in Veeam Agent for IBM AIX does not affect instance consumption. To learn more about per-instance licensing in Veeam Backup & Replication, see the Licensing section in the Veeam Backup & Replication User Guide.

Veeam Agent for IBM AIX supports paid types of license. Mind the following limitations:

- Starter license package is not supported.
- Standard license edition is not supported.

After Veeam Agent for IBM AIX connects to Veeam Backup & Replication, Veeam Agent for IBM AIX automatically starts consuming the license.

Veeam Agent for IBM AIX keeps information about the license in its database. Information about the license is valid for 32 days. If Veeam Agent for IBM AIX 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 you restrict instance consumption, Veeam Agent for IBM AIX 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. In the displayed window, click Yes.
5. Click Close.
Viewing Licensed Agents and Revoking License

When Veeam Agent for IBM AIX 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.
- Copy Veeam Agent backups from the backup repository to a secondary backup repository with backup copy jobs.
- Archive Veeam Agent backups to tapes with backup to tape jobs.
Back to Back Up to Backup Repositories

You can store backups created with Veeam Agent for IBM AIX 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. Connect Veeam Agent to the Veeam backup server.
3. Create a Veeam Agent backup job targeted at the backup repository.

The user who creates a Veeam Agent for IBM AIX backup on the Veeam backup repository is set as the owner of the backup file. Only the backup file owner can access this file and restore data from it. Other users cannot see backups created by the backup file owner.

**NOTE**

If the user is granted restore permissions on the Veeam backup server, they will be able to see all backups on the backup repository.

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 for IBM AIX are available under the Backups > Disk node in the Home view.

The backup administrator working with Veeam Backup & Replication can manage Veeam Agent for IBM AIX backup jobs and restore data from these backups. To learn more, see Performing Restore Tasks and Performing Administration Tasks.
Performing Backup Copy for Veeam Agent Backups

You can configure backup copy jobs that will copy backups created with Veeam Agent for IBM AIX to a secondary backup repository.

Backup copy jobs process Veeam Agent for IBM AIX backups in the similar way as VM backups. To learn more about backup copy jobs, see the Backup Copy section in the Veeam Backup & Replication User Guide.

The setup procedure for a Veeam Agent backup copy job practically does not differ from the same procedure for a VM backup copy job. Consider the following:

- You can process backups created by Veeam Agent for IBM AIX only with backup copy jobs for IBM AIX machine backups. You cannot add a Veeam Agent backup as an additional source of a backup copy job that processes VM backups or other backups.
- You can process backups created by Veeam Agent for IBM AIX only with backup copy jobs operating in the periodic copy mode. Immediate copy mode is not supported.

To create a Veeam Agent for IBM AIX backup copy job:

1. In the Veeam Backup & Replication console, in the Home view, right-click the Jobs node in the inventory pane or right-click anywhere in the working area, and select Backup copy > IBM AIX computer backup.
2. Follow the steps of the New Backup Copy Job wizard. At the Objects step of the wizard, you will be able to add Veeam Agent for IBM AIX backups to the job.

To learn more about how to configure backup copy jobs, see the Creating Backup Copy Jobs for VMs and Physical Machines section in the Veeam Backup & Replication User Guide.
Restoring Data from Copies of Veeam Agent Backups

The process of data restore from Veeam Agent for IBM AIX backups created by backup copy jobs does not differ from data restore from Veeam Agent backups created by backup jobs. To learn more, see Performing Restore Tasks.
Archiving Veeam Agent Backups to Tape

You can configure backup to tape jobs to archive Veeam Agent for IBM AIX backups to tape.

Backup to tape jobs treat Veeam Agent for IBM AIX backups as usual backup files. The archiving job setup and processing procedures practically do not differ from the regular ones. To learn more about backup to tape jobs, see the Machines Backup to Tape section in the Veeam Backup & Replication User Guide.

**NOTE**

Note 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 machine.

### New Backup to Tape Job

<table>
<thead>
<tr>
<th>Name</th>
<th>Backups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Backups

**Specify objects to be processed by this tape job.**

- **univm04 file backup**: IBM AIX Agent ...
- **univm04 server backup**: IBM AIX Agent ...

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>univm04 file</td>
<td>IBM AIX Agent</td>
<td>34.1 MBytes</td>
</tr>
<tr>
<td>univm04 server</td>
<td>IBM AIX Agent</td>
<td>7.25 GBytes</td>
</tr>
</tbody>
</table>

**Full:**

| 7.25 GB |

**Incremental:**

| 43.7 MB |

[Image of the New Backup to Tape Job interface]

[Table of backup objects with columns for Name, Type, and Size]

[Buttons for Add, Remove, Up, Down, Previous, Next, Finish, Cancel]
Performing Restore Tasks

You can perform the following restore operations with Veeam Agent for IBM AIX backups:

- Restore individual files and directories from Veeam Agent backups.
- Export backup data as VMDK, VHD or VHDX disks.
- Export restore points of Veeam Agent backups to standalone full backup files.
Restoring Files and Directories

You can restore individual files and directories from Veeam Agent for IBM AIX backups.

The procedure of file-level restore from a Veeam Agent backup practically does not differ from the same procedure for a VM backup. To learn more about file-level restore, see the Restore from Linux, Unix and Other File Systems section in the Veeam Backup & Replication User Guide.

File-level restore from a Veeam Agent for IBM AIX backup has one limitation: you cannot restore files and directories to their original location or another UNIX machine. Use the Copy To option to save a file or directory on the Veeam backup server or another non-UNIX machine added to the Veeam backup infrastructure.
Exporting Disks

You can restore machine disks from Veeam Agent backups and convert them to virtual disks of the VMDK, VHD or VHDX format.

During disks restore, Veeam Agent for IBM AIX 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 Agent for IBM AIX 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 Agent for IBM AIX 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 format.

VHD/VHDX disks are always restored as dynamically expanding.

You can use exported virtual disks with a VM whose OS supports the ext4 file system. For example, you can attach a virtual disk to a VMware vSphere or Microsoft Hyper-V VM that runs a Linux OS.

To restore disks, use the Export Disk wizard.
Step 1. Launch Export Disk Wizard

To launch the Export Disk wizard:

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

2. In the inventory pane, click Disk under the Backups node. In the working area, expand the Agents node, right-click the necessary backup and select Export content as virtual disks. You will pass to the Restore Point step of the wizard.
Step 2. Select Restore Point

At the **Restore Point** step of the wizard, select the necessary restore point from which you want to restore disk. In the list of restore points, Veeam Agent for IBM AIX displays all restore points that have been created.
Step 3. Select Disks

At the **Disks** step of the wizard, select check boxes next to the disk that you want to export.

For Veeam Agent for IBM AIX backups, Veeam Backup & Replication always offers to export the *Disk 0* disk only. This is the disk that contains the volume with files and directories in the backup file. To learn more, see [How Backup Works](#).

---

![Disks selection screen](image-url)
Step 4. Select Destination and Disk Format

At the **Target** step of the wizard, select the destination for disk export and format in which you want to save the resulting virtual disk.

1. From the **Server** list, select a server on which the resulting virtual disks must be saved. If you plan to save the disks in the VMDK format on a datastore, select an ESXi host to which this datastore is connected.

2. In the **Path to folder** field, specify a folder on the server or datastore where the virtual disks must be placed.

3. Select the export format for disks:
   - **VMDK** — select this option if you want to save the resulting virtual disk in the VMware VMDK format.
   - **VHD** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHD format.
   - **VHDX** — select this option if you want to save resulting virtual disk in the Microsoft Hyper-V VHDX format (supported by Microsoft Windows Server 2012 and later).

**NOTE**

If you have selected to store the resulting virtual disk to a datastore, you will be able to save the virtual disk in the VMDK format only. Other options will be disabled.
Step 5. Specify Restore Reason

At the Reason step of the wizard, enter a reason for exporting the virtual disk.

**NOTE**

If you do not want to display the Restore Reason step of the wizard in future, select the Do not show me this page again check box.
Step 6. Complete Restore Process

At the **Summary** step of the wizard, complete the disk restore procedure.

1. Review details for the disk to be restored.
2. Click **Finish** to start the restore procedure and exit the wizard.
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 for IBM AIX 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.
- View Veeam Agent backup job statistics.
- Delete Veeam Agent backup jobs.
- 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 for IBM AIX backup in the Veeam Backup & Replication console in the following situations:

- The Veeam Agent for IBM AIX backup is stored on a drive managed by another machine (not the Veeam backup server).
- The Veeam Agent for IBM AIX backup is stored on a backup repository managed by another Veeam backup server.
- The Veeam Agent for IBM AIX backup has been removed in the Veeam Backup & Replication console.

After importing, the Veeam Agent for IBM AIX 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 machine from which you plan to import the backup must be added as a managed server in 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 for IBM AIX backup:

1. In Veeam Backup & Replication, click **Import Backup** on the **Home** tab.
2. From the **Computer** list, select the 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 IBM AIX.

To import an encrypted backup file:

1. On the Home tab, click Import Backup.
2. From the Computer list, select the server 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 form 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 Backup Jobs

You can disable and enable Veeam Agent for IBM AIX 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 for IBM AIX 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.
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.
Deleting Veeam Agent Backup Jobs

You can delete Veeam Agent for IBM AIX 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 upon 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 prevent the job from starting permanently, you must delete the job and unassign access rights permissions for this user from the backup repository. To completely delete the job, you must perform this operation in Veeam Agent for IBM AIX on the Veeam Agent machine.

To delete 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.
Removing Veeam Agent Backups

You can remove Veeam Agent for IBM AIX backups from Veeam Backup & Replication or permanently delete Veeam Agent for IBM AIX backups from the Veeam backup repository.

Removing from Configuration

When you remove a Veeam Agent for IBM AIX 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 Backups.

To remove a Veeam Agent for IBM AIX 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 for IBM AIX 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 for IBM AIX 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. To learn more, see the Specifying I/O Settings topic in the Veeam Backup & Replication User Guide.

- Configure the following global notification settings to get alerted about the Veeam Agent backup job results:
  
  - Email notifications. To learn more, see the Specifying Email Settings section in the Veeam Backup & Replication User Guide.

  - SNMP notifications. To learn more, see the Specifying SNMP Settings section in the Veeam Backup & Replication User Guide.
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.