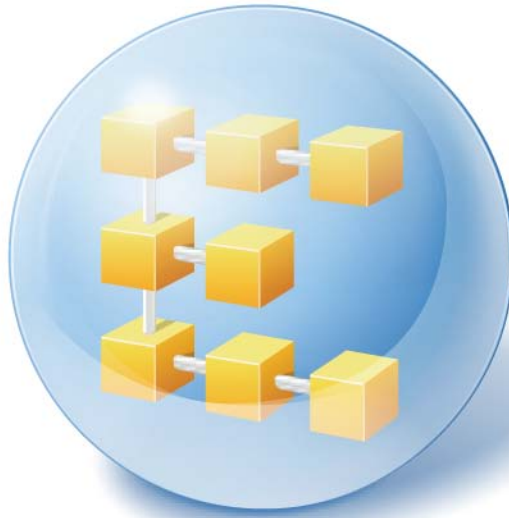




Acronis Backup & Recovery Server OEM

User's Guide

Copyright © Acronis, Inc., 2000-2010. All rights reserved.

“Acronis” and “Acronis Secure Zone” are registered trademarks of Acronis, Inc.

"Acronis Compute with Confidence", "Acronis Startup Recovery Manager", "Acronis Active Restore" and the Acronis logo are trademarks of Acronis, Inc.

Linux is a registered trademark of Linus Torvalds.

VMware and VMware Ready are trademarks and/or registered trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Windows and MS-DOS are registered trademarks of Microsoft Corporation.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of this work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Third party code may be provided with the Software and/or Service. The license terms for such third-parties are detailed in the license.txt file located in the root installation directory. You can always find the latest up-to-date list of the third party code and the associated license terms used with the Software and/or Service at <http://kb.acronis.com/content/7696>

Table of contents

1	Introducing Acronis Backup & Recovery Server OEM.....	6
1.1	Acronis Backup & Recovery Server OEM overview	6
1.2	Getting started.....	6
1.2.1	Using the management console	6
1.3	Acronis Backup & Recovery Server OEM components.....	13
1.3.1	Agent for Windows	13
1.3.2	Management Console.....	14
1.3.3	Bootable Media Builder (DM Windows)	14
1.4	Supported operating systems.....	14
1.5	Supported file systems	15
1.6	Hardware requirements	15
2	Understanding Acronis Backup & Recovery Server OEM.....	15
2.1	Basic concepts.....	16
2.2	Full backups	20
2.3	User privileges on a managed machine.....	21
2.4	Owners and credentials.....	21
2.5	Backing up dynamic volumes (Windows)	22
2.6	Tape support.....	24
2.6.1	Using a single tape drive	24
2.7	Proprietary Acronis technologies	25
2.7.1	Acronis Startup Recovery Manager	25
2.7.2	Universal Restore (Acronis Backup & Recovery Server OEM Universal Restore)	26
3	Options	27
3.1	Console options	27
3.1.1	Startup page	27
3.1.2	Pop-up messages	28
3.1.3	Time-based alerts.....	28
3.1.4	Fonts.....	28
3.2	Machine options	29
3.2.1	Event tracing.....	29
3.2.2	Log cleanup rules (UMMS)	31
3.3	Default backup and recovery options.....	31
3.3.1	Default backup options.....	31
3.3.2	Default recovery options	46
4	Vaults.....	53
4.1	Personal vaults.....	54
4.1.1	Working with the "Personal vault" view	55
4.1.2	Actions on personal vaults.....	56
4.2	Common operations	57
4.2.1	Operations with archives stored in a vault.....	57
4.2.2	Operations with backups.....	58
4.2.3	Deleting archives and backups.....	59
4.2.4	Filtering and sorting archives	59

5	Direct management	59
5.1	Administering a managed machine	59
5.1.1	Dashboard.....	60
5.1.2	Backup plans and tasks	62
5.1.3	Log	71
5.2	Creating a backup plan	74
5.2.1	Why is the program asking for the password?	75
5.2.2	Backup plan's credentials	75
5.2.3	Source type	75
5.2.4	Items to back up	76
5.2.5	Access credentials for source	76
5.2.6	Archive	77
5.2.7	Access credentials for archive location.....	78
5.2.8	Backup schemes	78
5.2.9	Archive validation	80
5.3	Recovering data	81
5.3.1	Task credentials	82
5.3.2	Archive selection	83
5.3.3	Data type.....	83
5.3.4	Content selection	83
5.3.5	Access credentials for location	84
5.3.6	Destination selection	85
5.3.7	Access credentials for destination	89
5.3.8	When to recover	89
5.3.9	Universal Restore	90
5.3.10	Bootability troubleshooting.....	91
5.4	Validating vaults, archives and backups	92
5.4.1	Task credentials	93
5.4.2	Archive selection	93
5.4.3	Backup selection.....	94
5.4.4	Location selection.....	94
5.4.5	Access credentials for source	94
5.4.6	When to validate	95
5.5	Mounting an image.....	95
5.5.1	Archive selection	96
5.5.2	Backup selection.....	96
5.5.3	Access credentials	97
5.5.4	Volume selection	97
5.6	Managing mounted images	97
5.7	Acronis Startup Recovery Manager	98
5.8	Bootable media.....	98
5.8.1	How to create bootable media	99
5.8.2	Working under bootable media.....	102
5.8.3	Recovering MD devices and logical volumes	104
5.9	Disk management	106
5.9.1	Supported file systems.....	107
5.9.2	Basic precautions.....	107
5.9.3	Running Acronis Disk Director Lite.....	107
5.9.4	Choosing the operating system for disk management	108
5.9.5	"Disk management" view	108
5.9.6	Disk operations.....	109
5.9.7	Volume operations.....	115

5.9.8	Pending operations	121
5.10	Collecting system information	121
6	Command-line mode and scripting in Windows	122
6.1	Agent for Windows command-line utility	122
6.1.1	Supported commands	122
6.1.2	Common options.....	126
6.1.3	Specific options.....	129
6.1.4	trueimagecmd.exe usage examples	138
6.2	Scripting	143
6.2.1	Script execution parameters	143
6.2.2	Script structure	144
6.2.3	Script usage examples.....	145
7	Glossary	146

1 Introducing Acronis Backup & Recovery Server OEM

1.1 Acronis Backup & Recovery Server OEM overview

Based on Acronis' patented disk imaging and bare metal restore technologies, Acronis Backup & Recovery Server OEM is the powerful disaster recovery solution.

1.2 Getting started

Direct management

1. Install Acronis Backup & Recovery Server OEM Management Console and Acronis Backup & Recovery Server OEM Agent.
2. Start the console.

Windows

Start the console by selecting it from the start menu.

3. Connect the console to the machine where the agent is installed.

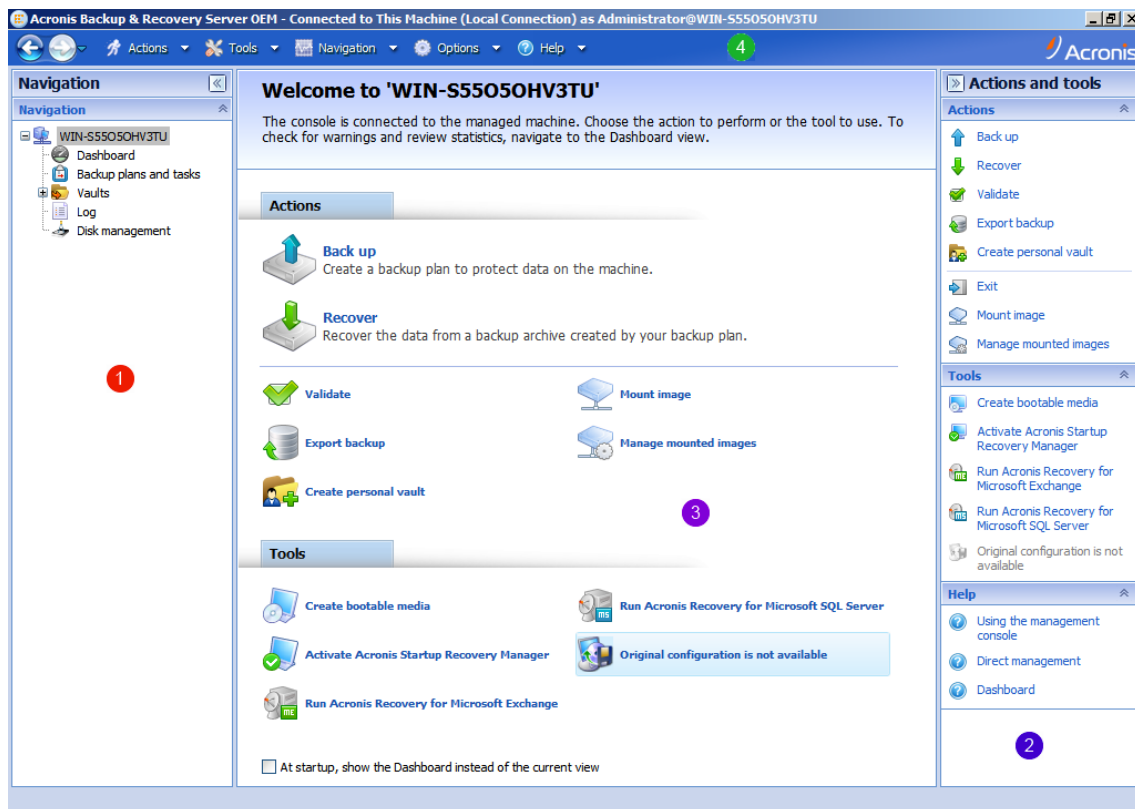
Where to go from here

For what to do next see "Basic concepts".

For understanding of the GUI elements see "Using the management console".

1.2.1 Using the management console

As soon as the console connects to a managed machine (p. 151), the respective items appear across the console's workspace (in the menu, in the main area with the **Welcome** screen, the **Navigation** pane, the **Actions and tools** pane) enabling you to perform agent-specific or server-specific operations.



Acronis Backup & Recovery Server OEM Management Console - Welcome screen

Key elements of the console workspace

	Name	Description
1	Navigation pane	Contains the Navigation tree and the Shortcuts bar and lets you navigate to the different views (see the Navigation pane section.)
2	Actions and tools pane	Contains bars with a set of actions that can be performed and tools (see the Actions and Tools pane section).
3	Main area	The main place of working, where you create, edit and manage backup plans, policies, tasks and perform other operations. Displays the different views and action pages (p. 10) depending on items selected in the menu, Navigation tree, or on the Actions and Tools pane.
4	Menu bar	Appears across the top of the program window and lets you perform all the operations, available on both panes. Menu items change dynamically.

1024x768 or higher display resolution is required for comfortable work with the management console.

1.2.1.1 "Navigation" pane

The navigation pane includes the **Navigation** tree and the **Shortcuts** bar.

Navigation tree

The **Navigation** tree enables you to navigate across the program views. Views depend on whether the console is connected to a managed machine.

Views for a managed machine

When the console is connected to a managed machine, the following views are available in the navigation tree.

-  **[Machine name]**. Root of the tree also called a **Welcome** view. Displays the name of the machine the console is currently connected to. Use this view for quick access to the main operations, available on the managed machine.
 -  **Dashboard**. Use this view to estimate at a glance whether the data is successfully protected on the managed machine.
 -  **Backup plans and tasks**. Use this view to manage backup plans and tasks on the managed machine: run, edit, stop and delete plans and tasks, view their states and statuses, monitor plans.
 -  **Vaults**. Use this view to manage personal vaults and archives stored in there, add new vaults, rename and delete the existing ones, validate vaults, explore backup content, mount backups as virtual drives, etc.
 -  **Log**. Use this view to examine information on operations performed by the program on the managed machine.
 -  **Disk management**. Use this view to perform operations on the machine's hard disk drives.

Shortcuts bar

The **Shortcuts** bar appears under the navigation tree. It offers you an easy and convenient way of connection to the machines in demand by adding them as shortcuts.

To add a shortcut to a machine

1. Connect the console to a managed machine.
2. In the navigation tree, right-click the machine's name (a root element of the navigation tree), and then select **Create shortcut**.

If the console and agent are installed on the same machine, the shortcut to this machine will be added to the shortcuts bar automatically as **Local machine [Machine name]**.

1.2.1.2 "Actions and tools" pane

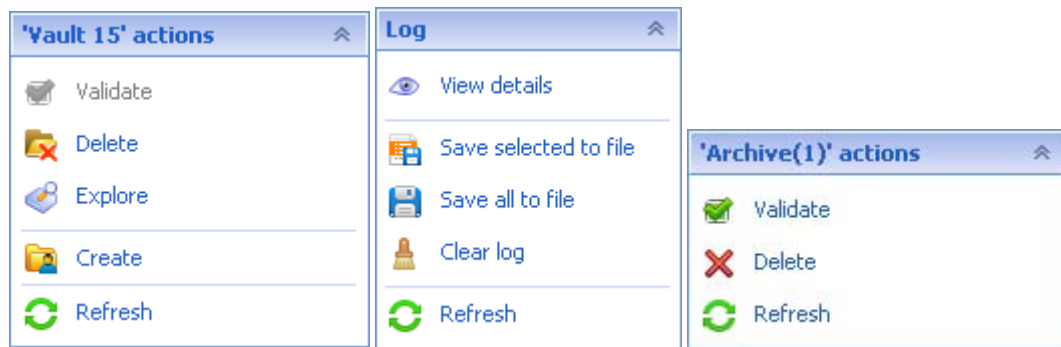
The **Actions and tools** pane enables you to easily and efficiently work with Acronis Backup & Recovery Server OEM. The pane's bars provide quick access to program's operations and tools. All items of the **Actions and tools** bar are duplicated in the program menu.

Bars

'[Item's name]' actions

Contains a set of actions that can be performed on the items selected in any of the navigation views. Clicking the action opens the respective action page. Items of different navigation views have their own set of actions. The bar's name changes in accordance with the item you select. For example, if you select the backup plan named *System backup* in the **Backup plans and tasks** view, the actions bar will be named as **'System backup' actions** and will have the set of actions typical to backup plans.

All actions can also be accessed in the respective menu items. A menu item appears on the menu bar when you select an item in any of the navigation views.

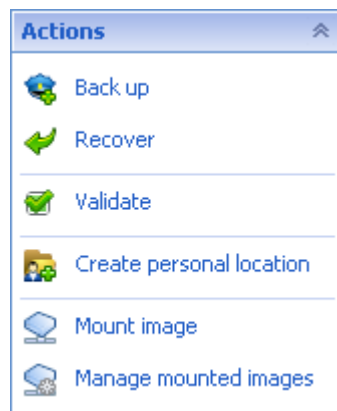


Examples of "'Item name' actions" bars

Actions

Contains a list of common operations that can be performed on a managed machine. Always the same for all views. Clicking the operation opens the respective action page (see the Action pages section.)

All the actions can also be accessed in the **Actions** menu.

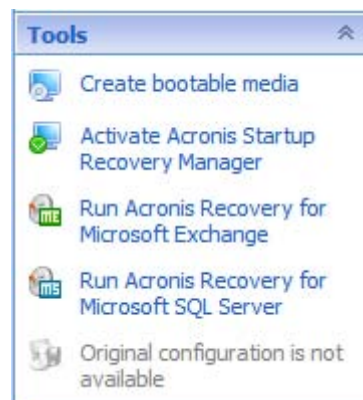


"Actions" bar on a managed machine

Tools

Contains a list of the Acronis tools. Always the same across all the program views.

All the tools can also be accessed in the **Tools** menu.



"Tools" bar

Help

Contains a list of help topics. Different views and action pages of Acronis Backup & Recovery Server OEM provided with lists of specific help topics.

1.2.1.3 Operations with panes

How to expand/minimize panes

By default, the **Navigation** pane appears expanded and the **Actions and Tools** - minimized. You might need to minimize the pane in order to free some additional workspace. To do this, click the chevron ( - for the **Navigation** pane;  - for the **Actions and tools** pane). The pane will be minimized and the chevron changes its direction. Click the chevron once again to expand the pane.

How to change the panes' borders

1. Point to the pane's border.
2. When the pointer becomes a double-headed arrow, drag the pointer to move the border.

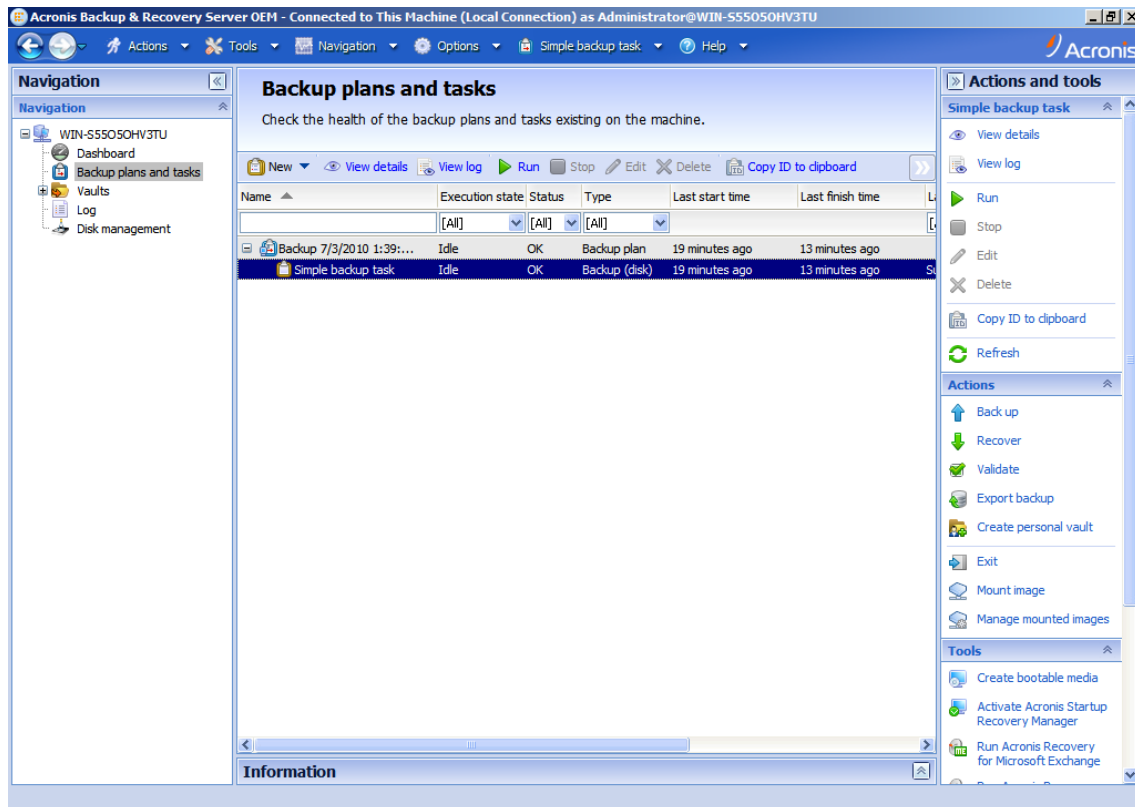
The management console "remembers" the way the panes' borders are set. When you run the management console next time, all the panes' borders will have the same position that was set previously.

1.2.1.4 Main area, views and action pages

The main area is a basic place where you work with the console. Here you create, edit and manage backup plans, policies, tasks and perform other operations. The main area displays different views and action pages according the items you select in the menu, **Navigation** tree, or on the **Actions and Tools** pane.

Views

A view appears on the main area when clicking any item in the **Navigation** tree in the Navigation pane.



"Tasks" view

Common way of working with views

Generally, every view contains a table of items, a table toolbar with buttons, and the **Information** panel.

- Use filtering and sorting capabilities to search the table for the item in question
- In the table, select the desired item
- In the **Information** panel (collapsed by default), view the item's details
- Perform actions on the selected item. There are several ways of performing the same action on selected items:
 - By clicking the buttons on the table toolbar;
 - By clicking in the items in the **[Item's name] Actions** bar (on the **Actions and Tools** pane);
 - By selecting the items in the **Actions** menu;
 - By right-clicking the item and selecting the operation in the context menu.

Action pages

An action page appears in the main area when clicking any action item in the **Actions** menu, or in the **Actions** bar on the **Actions and tools** pane. It contains steps you need to perform in order to create and launch any task, or a backup plan.

Action page - Create backup plan

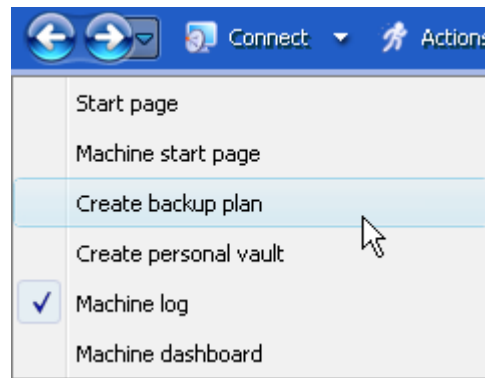
Using controls and specifying settings

The action pages offer two ways of representation: basic and advanced. The basic representation hides such fields as credentials, comments, etc. When the advanced representation is enabled, all the available fields are displayed. You can switch between the views by selecting the **Advanced view** check box at the top of the action page.

Most settings are configured by clicking the respective **Change...** links to the right. Others are selected from the drop-down list, or typed manually in the page's fields.

Action page - Controls

Acronis Backup & Recovery Server OEM remembers the changes you made on the action pages. For example, if you started to create a backup plan, and then for any reason switched to another view without accomplishing the plan creation, you can click the **Back** navigation button on the menu. Or, if you have passed several steps forward, click the **Down** arrow and select the page where you started the plan creation from the list. Thus, you can perform the remaining steps and accomplish the backup plan creation.



Navigation buttons

1.3 Acronis Backup & Recovery Server OEM components

This section contains a full list of Acronis Backup & Recovery Server OEM components with a brief description of their functionality.

Acronis Backup & Recovery Server OEM includes the following main types of components.

Components for a managed machine (agents)

These are applications that perform data backup, recovery and other operations on the machines managed with Acronis Backup & Recovery Server OEM. Agents require a license to perform operations on each managed machine. Agents have multiple features, or add-ons, that enable additional functionality and so might require additional licenses.

Console

The console provides Graphical User Interface and remote connection to the agents and other Acronis Backup & Recovery Server OEM components. Usage of the console is not licensed.

Bootable media builder

With bootable media builder, you can create bootable media in order to use the agents and other rescue utilities in a rescue environment. Availability of the agent add-ons in a rescue environment depends on whether an add-on is installed on the machine where the media builder is working.

1.3.1 Agent for Windows

This agent enables disk-level data protection under Windows.

Disk backup

Disk-level data protection is based on backing up either a disk or a volume file system as a whole, along with all the information necessary for the operating system to boot; or all the disk sectors using the sector-by-sector approach (raw mode). A backup that contains a copy of a disk or a volume in a packaged form is called a disk (volume) backup or a disk (volume) image. It is possible to recover disks or volumes as a whole from such backup, as well as individual folders or files.

Other operations

Disk management

Agent for Windows includes Acronis Disk Director Lite - a handy disk management utility. Disk management operations, such as cloning disks; converting disks; creating, formatting and deleting

volumes; changing a disk partitioning style between MBR and GPT or changing a disk label, can be performed either in the operating system or using bootable media.

1.3.1.1 Universal Restore

The Universal Restore add-on enables you to use the restore to dissimilar hardware functionality on the machine where the agent is installed, and create bootable media with this functionality. Universal Restore handles differences in devices that are critical for Windows start-up, such as storage controllers, motherboard or chipset.

1.3.2 Management Console

Acronis Backup & Recovery Server OEM Management Console is an administrative tool for remote or local access to Acronis Backup & Recovery Server OEM agents.

1.3.3 Bootable Media Builder (DM Windows)

Acronis Bootable Media Builder is a dedicated tool for creating bootable media. The media builder that installs on Windows can create bootable media based on either Windows Preinstallation Environment.

The Universal Restore (p. 14) add-on enables you to create bootable media with the restore to dissimilar hardware functionality. Universal Restore handles differences in devices that are critical for Windows start-up, such as storage controllers, motherboard or chipset.

1.4 Supported operating systems

Components for a managed machine

Acronis Backup & Recovery Server OEM Agent for Windows

- Windows 2000 Professional SP4/XP Professional SP2+
- Windows 2000 Server/2000 Advanced Server/Server 2003/Server 2008
- Windows SBS 2003/SBS 2008
- Windows XP Professional x64 Edition, Windows Server 2003/2008 x64 Editions
- Windows Vista - all editions except for Vista Home Basic and Vista Home Premium
- Windows 7 - all editions except for the Starter and Home editions

Acronis Backup & Recovery Server OEM Management Console

- Windows 2000 Professional SP4/XP Home Editions/XP Professional SP2+
- Windows 2000 Server/2000 Advanced Server/Server 2003/Server 2008
- Windows SBS 2003/SBS 2008
- Windows XP Professional x64 Edition, Windows Server 2003/2008 x64 Editions
- Windows Vista - all editions
- Windows 7 - all editions

1.5 Supported file systems

Acronis Backup & Recovery Server OEM can back up and recover the following file systems with the following limitations:

- FAT16/32
- NTFS
- Ext2/Ext3
- ReiserFS3
- ReiserFS4
- XFS - volume recovery without the volume resize capability;
- JFS

Acronis Backup & Recovery Server OEM can back up and recover corrupted or non-supported file systems using the sector-by-sector approach.

1.6 Hardware requirements

This section lists the minimum and recommended hardware requirements to install and run Acronis Backup & Recovery Server OEM components.

Acronis Backup & Recovery Server OEM Management Console

Item	Minimum requirements	Recommended
Computer processor	Modern processor, 800 MHz or faster Itanium platforms are not supported	1 GHz 32-bit (x86) or 64-bit (x64) processor
System memory	128 MB	512 MB or more
Screen resolution	800*600 pixels	1024*768 pixels or higher
Installation disk space	50 MB	
Other hardware	Mouse	
		Network interface card or a virtual network adapter
		CD-RW, DVD-RW, drive for bootable media creation

Acronis Backup & Recovery Server OEM Agent for Windows

Item	Minimum requirements	Recommended
System memory	256 MB	512 MB or more
Installation disk space	100 MB	

2 Understanding Acronis Backup & Recovery Server OEM

This section attempts to give its readers a clear understanding of the product so that they can use the product in various circumstances without step-by-step instructions.

2.1 Basic concepts

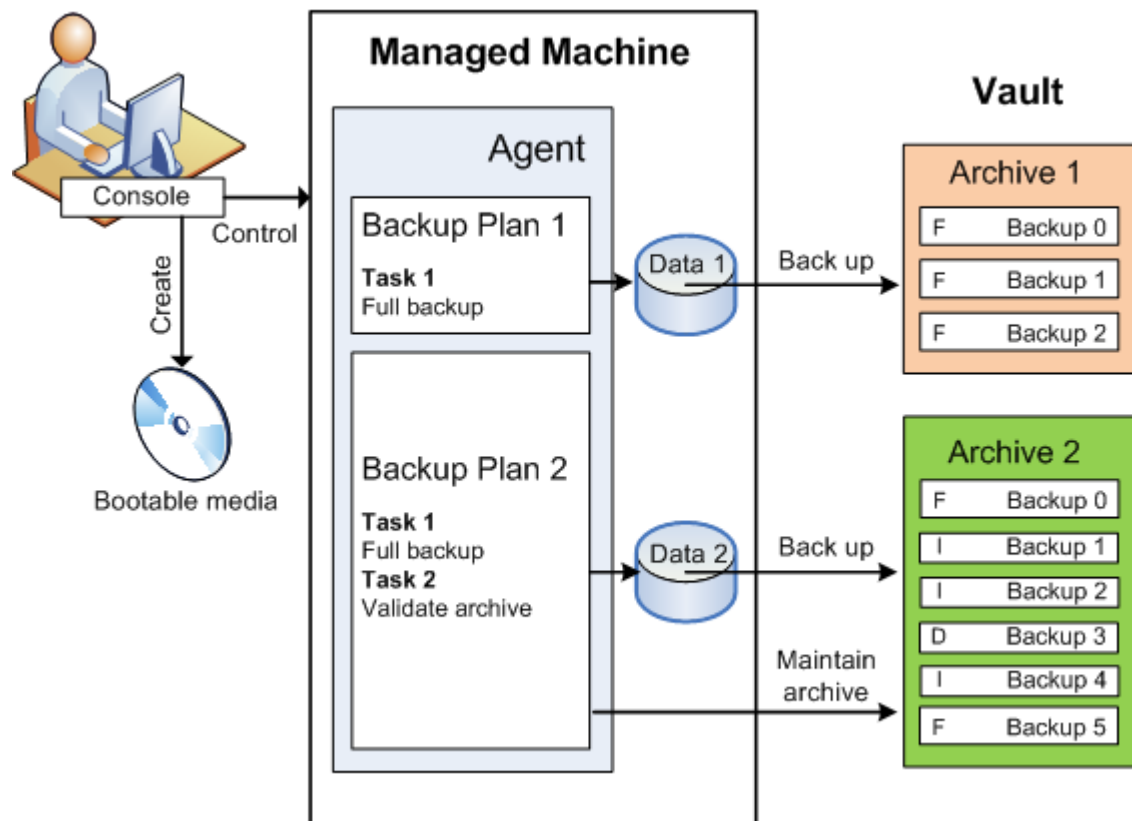
Please familiarize yourself with the basic notions used in the Acronis Backup & Recovery Server OEM graphical user interface and documentation. Advanced users are welcome to use this section as a step-by-step quick start guide. The details can be found in the context help.

Backup under operating system

1. To protect data on a machine, install Acronis Backup & Recovery Server OEM agent on the machine which becomes a managed machine (p. 151) from this point on.
2. To be able to manage the machine using Graphical User Interface, install Acronis Backup & Recovery Server OEM Management Console on the same machine or any machine from which you prefer to operate. If you have the standalone product edition, skip this step since in your case the console installs with the agent.
3. Run the console. To be able to recover the machine's operating system if the system fails to start, create bootable media.
4. Connect the console to the managed machine.
5. Create a backup plan.

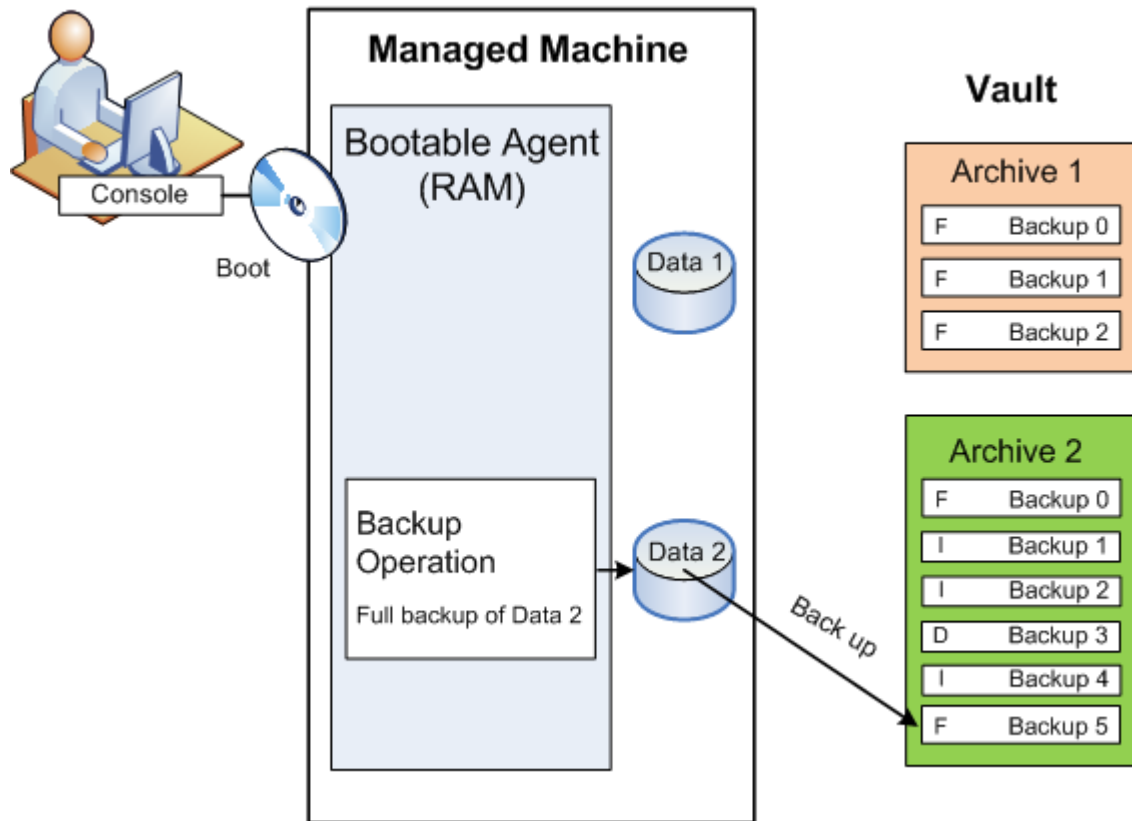
To do so, you have to specify, at the very least, the data to be protected and the location where the backup archive will be stored. This will create a minimal backup plan consisting of one task (p. 151) that will create a full backup (p. 147) of your data every time the task is manually started. A complex backup plan might consist of multiple tasks which run on schedule; create full backups; perform archive maintenance operations such as backup validation (p. 152) or deleting outdated backups. You can customize backup operations using various backup options, such as pre/post backup commands, network bandwidth throttling, error handling or notification options.
6. Use the **Backup plans and tasks** page to view information about your backup plans and tasks and monitor their execution. Use the **Log** page to browse the operations log.
7. The location where you store backup archives is called a vault (p. 152). Navigate to the **Vaults** page to view information about your vaults. Navigate further to the specific vault to view archives and backups and perform manual operations with them (mounting, validating, deleting, viewing contents). You can also select a backup to recover data from it.

The following diagram illustrates the notions discussed above. For more definitions please refer to the Glossary.



Backup using bootable media

You can boot the machine using the bootable media, configure the backup operation in the same way as a simple backup plan and execute the operation. This will help you extract files and logical volumes from a system that failed to boot, take an image of the offline system or back up sector-by-sector an unsupported file system.



Recovery under operating system

When it comes to data recovery, you create a recovery task on the managed machine. You specify the vault, then select the archive and then select the backup referring to the date and time of the backup creation, or more precisely, to the time when the creation has started. In most cases, the data will be reverted to that moment.

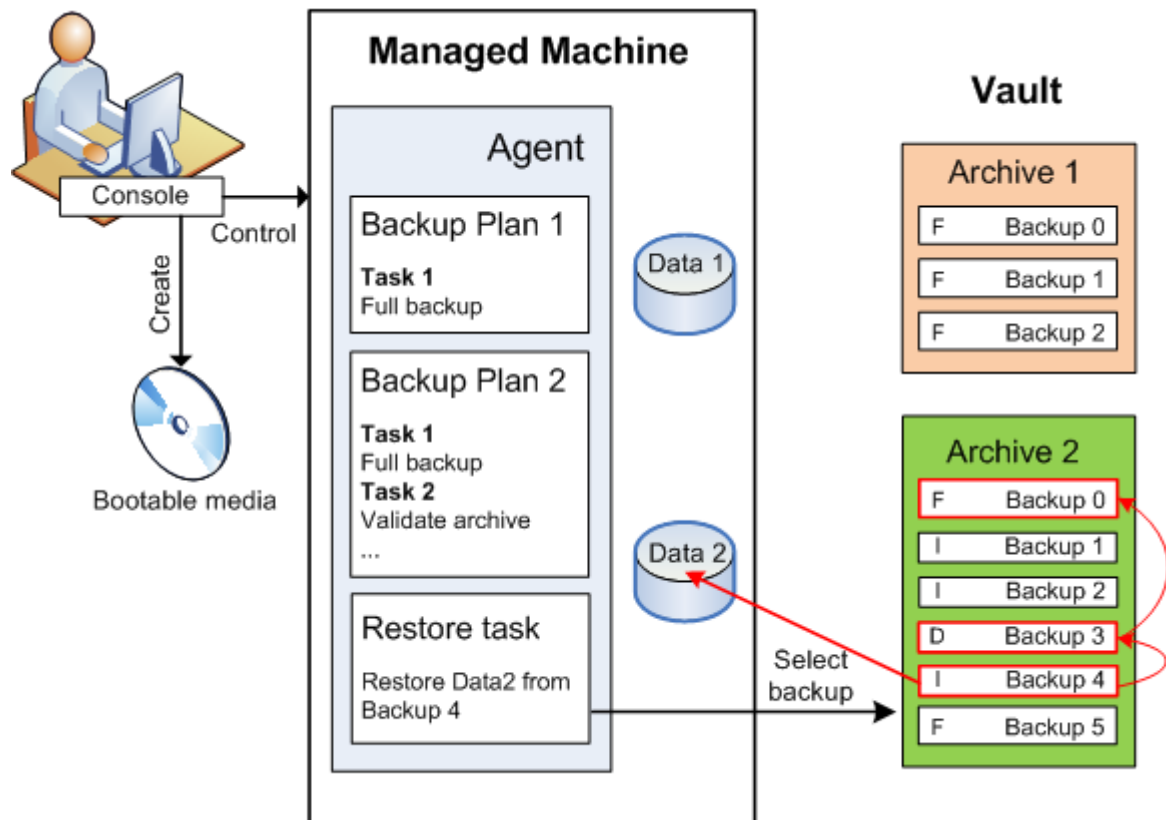
Examples of exceptions to this rule:

Recovering a database from a backup that contains the transaction log (a single backup provides multiple recovery points and so you can make additional selections).

Recovering multiple files from a file backup taken without snapshot (each file will be reverted to the moment when it was actually copied to the backup).

You also specify the destination where to recover the data. You can customize the recovery operation using recovery options, such as pre/post recovery commands, error handling or notification options.

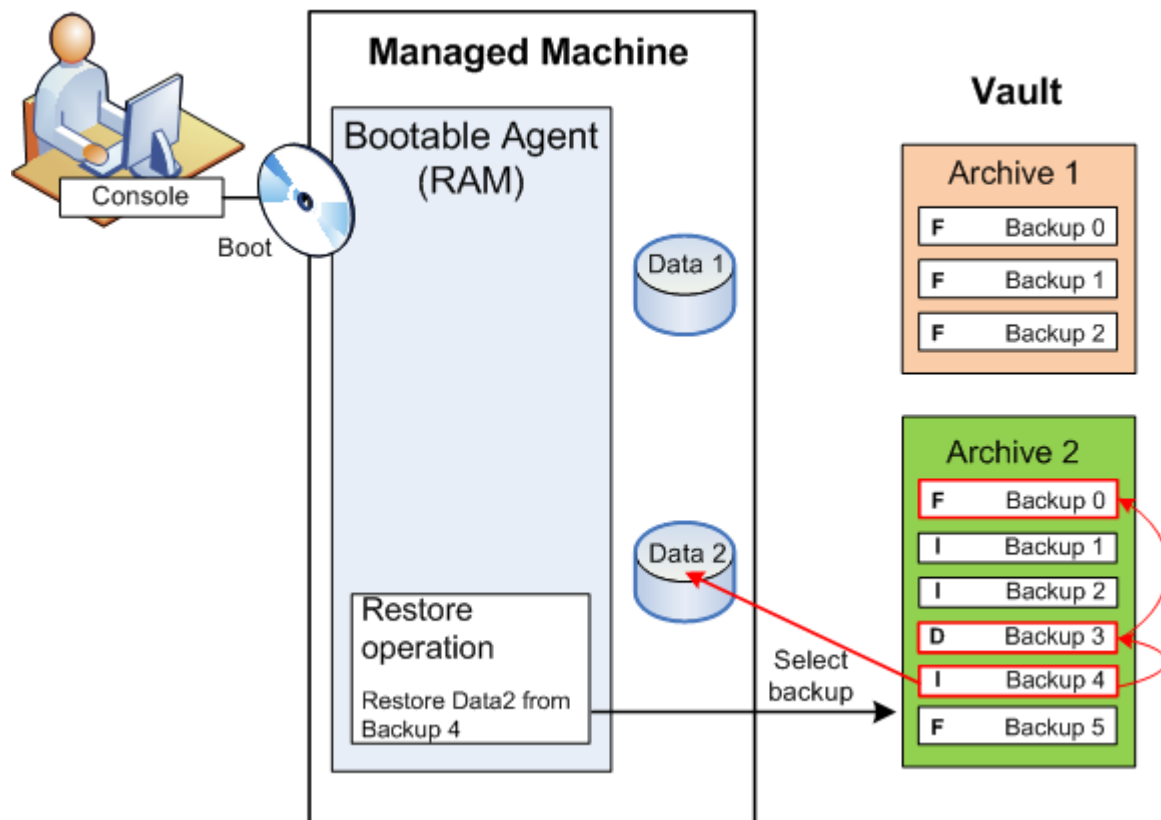
The following diagram illustrates data recovery under the operating system (online). No backup can proceed on the machine while the recovery operation is taking place. If required, you can connect the console to another machine and configure a recovery operation on that machine. This ability (remote parallel recovery) first appeared in Acronis Backup & Recovery Server OEM.



Recovery using bootable media

Recovery over a volume locked by the operating system, such as the volume where the operating system resides, requires a reboot to the bootable environment which is a part of the agent. After the recovery is completed, the recovered operating system goes online automatically.

If the machine fails to boot or you need to recover data to bare metal, you boot the machine using the bootable media and configure the recovery operation in the same way as the recovery task. The following diagram illustrates the recovery using the bootable media.



2.2 Full backups

Acronis Backup & Recovery Server OEM provides the capability to create custom backup schemes. All backup schemes are based on full backup method. The term "scheme" in fact denotes the algorithm of applying these methods plus the algorithm of the archive cleanup.

Comparing backup methods with each other does not make much sense because the methods work as a team in a backup scheme. Each method should play its specific role according to its advantages. A competent backup scheme will benefit from the advantages of all backup methods and lessen the influence of all the methods' shortcomings.

Full backup

A full backup stores all data selected for backup. An archive can contain multiple full backups or consist of only full backups. A full backup is self-sufficient - you do not need access to any other backup to recover data from a full backup.

It is widely accepted that a full backup is the slowest to do but the fastest to restore.

A full backup is most useful when:

- you need to roll back the system to its initial state
- this initial state does not change often, so there is no need for regular backup.

Example: An Internet cafe, school or university lab where the administrator often undoes changes made by the students or guests but rarely updates the reference backup (in fact, after installing

software updates only). The backup time is not crucial in this case and the recovery time will be minimal when recovering the systems from the full backup. The administrator can have several copies of the full backup for additional reliability.

2.3 User privileges on a managed machine

Windows

When managing a machine running Windows, the scope of a user's management rights depends on the user's privileges on the machine.

Regular users

A regular user, such as a member of the Users group, has the following management rights:

- Create backup plans and tasks and manage them.
- View—but not manage—backup plans and tasks created by other users.
- View the local event log.

Administrative users

A user who has administrative privileges on the machine, such as a member of the Administrators or Backup Operators group, additionally has the following management rights:

- Back up and recover the entire machine or any data on the machine, with or without using a disk snapshot.

Members of the Administrators group also can:

- View and manage backup plans and tasks owned by any user on the machine.

2.4 Owners and credentials

This section explains the concept of owner and the meaning of a backup plan's (or task's) credentials.

Plan (task) owner

A local backup plan owner is the user who created or last modified the plan.

Tasks, belonging to a backup plan are owned by the backup plan owner.

Tasks that do not belong to a backup plan, such as the recovery task, are owned by the user who has created or last modified the task.

Managing a plan (task) owned by another user

Having Administrator privileges on the machine, a user can modify tasks and local backup plans owned by any user registered in the operating system.

When a user opens a plan or task for editing, which is owned by another user, all passwords set in the task are cleared. This prevents the "modify settings, leave passwords" trick. The program displays a warning each time you are trying to edit a plan (task) last modified by another user. On seeing the warning, you have two options:

- Click **Cancel** and create your own plan or task. The original task will remain intact.
- Continue editing. You will have to enter all credentials required for the plan or task execution.

Archive owner

An archive owner is the user who saved the archive to the destination. To be more precise, this is the user whose account was specified when creating the backup plan in the **Where to back up** step. By default, the plan's credentials are used.

Plan's credentials and task credentials

Any task running on a machine runs on behalf of a user. When creating a plan or a task, you have the option to explicitly specify an account under which the plan or the task will run. Your choice depends on whether the plan or task is intended for manual start or for executing on schedule.

Manual start

You can skip the **Plan's (Task) credentials** step. Every time you start the task, the task will run under the credentials with which you are currently logged on. Any person that has administrative privileges on the machine can also start the task. The task will run under this person's credentials.

The task will always run under the same credentials, regardless of the user who actually starts the task, if you specify the task credentials explicitly. To do so, on the plan (task) creation page:

1. Select the **Advanced view** check box.
2. Select **General -> Plan's (Task) credentials -> Change**.
3. Enter the credentials under which the plan (task) will run.

Scheduled or postponed start

The plan (task) credentials are mandatory. If you skip the credentials step, you will be asked for credentials after finishing the plan (task) creation.

Why does the program compel me to specify credentials?

A scheduled or postponed task has to run anyway, regardless if any user is logged on or not (for example, the system is at the Windows "Welcome" screen) or a user other than the task owner is logged on. It is sufficient that the machine be on (that is, not in standby or hibernate) at the scheduled task start time. That's why the Acronis scheduler needs the explicitly specified credentials to be able to start the task.

2.5 Backing up dynamic volumes (Windows)

This section explains in brief how to back up and recover dynamic volumes (p. 150) using Acronis Backup & Recovery Server OEM. Basic disks that use the GUID Partition Table (GPT) are also discussed.

Dynamic volume is a volume located on dynamic disks (p. 149), or more exactly, on a disk group (p. 149). Acronis Backup & Recovery Server OEM supports the following dynamic volume types/RAID levels:

- simple/spanned
- striped (RAID 0)
- mirrored (RAID 1)
- a mirror of stripes (RAID 0+1)
- RAID 5.

Acronis Backup & Recovery Server OEM can back up and recover dynamic volumes and, with minor limitations, basic GPT volumes.

Backing up dynamic volumes

Dynamic and basic GPT volumes are backed up in the same way as basic MBR volumes. When creating a backup plan through the GUI, all types of volumes are available for selection as **Items to back up**. When using the command line, specify the dynamic and GPT volumes with the DYN prefix.

The boot code on basic GPT volumes is not backed up or recovered.

Recovering dynamic volumes

A dynamic volume can be recovered

- over any type of existing volume
- to unallocated space of a disk group
- to unallocated space of a basic disk.

Recovery over an existing volume

When a dynamic volume is recovered over an existing volume, either basic or dynamic, the target volume's data is overwritten with the backup content. The type of target volume (basic, simple/spanned, striped, mirrored, RAID 0+1, RAID 5) will not change. The target volume size has to be enough to accommodate the backup content.

Recovery to disk group unallocated space

When a dynamic volume is recovered to disk group unallocated space, both the type and the content of the resulting volume are recovered. The unallocated space size has to be enough to accommodate the backup content. The way unallocated space is distributed among the disks is also important.

Example

Striped volumes consume equal portions of space on each disk.

Assume you are going to recover a 30GB striped volume to a disk group consisting of two disks. Each disk has volumes and a certain amount of unallocated space. The total size of unallocated space is 40GB. The recovery will always result in a striped volume if the unallocated space is distributed evenly among the disks (20GB and 20GB).

If one of the disks has 10GB and the other has 30GB of unallocated space, then the recovery result depends on the size of the data being recovered.

- If the data size is less than 20GB, then one disk can hold, say, 10GB; the other will hold the remaining 10GB. This way, a striped volume will be created on both disks and 20GB on the second disk will remain unallocated.
- If the data size is more than 20GB, the data cannot be distributed evenly between the two disks, but can fit into a single simple volume. A simple volume accommodating all the data will be created on the second disk. The first disk will remain untouched.

	Backed up (source):		
Recovered to:	Dynamic volume	Basic MBR volume	Basic GPT volume
Dynamic volume	Dynamic volume Type as of the target	Dynamic volume Type as of the target	Dynamic volume Type as of the target

Unallocated space (disk group)	Dynamic volume Type as of the source	Dynamic volume Simple	N/A
Basic MBR volume	Basic MBR volume	Basic MBR volume	Basic MBR volume
Basic GPT volume	Basic GPT volume	Basic GPT volume	Basic GPT volume
Unallocated space (basic MBR disk)	Basic MBR volume	Basic MBR volume	Basic MBR volume
Unallocated space (basic GPT disk)	Basic GPT volume	Basic GPT volume	Basic GPT volume

Moving and resizing volumes during recovery

You can resize the resulting basic volume, both MBR and GPT, during recovery, or change the volume's location on the disk. A resulting dynamic volume cannot be moved or resized.

Preparing disk groups and volumes

Before recovering dynamic volumes to bare metal you should create a disk group on the target hardware.

You also might need to create or increase unallocated space on an existing disk group. This can be done by deleting volumes or converting basic disks to dynamic.

You might want to change the target volume type (basic, simple/spanned, striped, mirrored, RAID 0+1, RAID 5). This can be done by deleting the target volume and creating a new volume on the resulting unallocated space.

Acronis Backup & Recovery Server OEM includes a handy disk management utility which enables you to perform the above operations both under the operating system and on bare metal. To find out more about Acronis Disk Director Lite, see the Disk management section.

2.6 Tape support

Acronis Backup & Recovery Server OEM supports tape libraries, autoloaders, SCSI and USB tape drives as storage devices. A tape device can be locally attached to a managed machine (in this case, the Acronis Backup & Recovery Server OEM Agent writes and reads the tapes).

Backup archives created using different ways of access to tape have different formats.

Backups created using the bootable media can be recovered with the Acronis Backup & Recovery Server OEM Agent running in the operating system.

2.6.1 Using a single tape drive

A tape drive that is locally attached to a managed machine can be used by local backup plans as a storage device. The functionality of a locally attached autoloader or tape library is limited to the ordinary tape drive. This means that the program can only work with the currently mounted tape and you have to mount tapes manually.

Backup to a locally attached tape device

When creating a backup plan, you are able to select the locally attached tape device as the backup destination. An archive name is not needed when backing up to a tape.

An archive can span multiple tapes but can contain only one full backup. Every time you create a full backup, you start with a new tape and create a new archive. As soon as the tape is full, a dialog window with a request to insert a new tape will appear.

The content of a non-empty tape will be overwritten on prompt. You have an option to disable prompts, see Additional settings.

You might experience short pauses that are required to rewind the tape. Low-quality or old tape, as well as dirt on the magnetic head, might lead to pauses that can last up to several minutes.

Limitations

1. Multiple full backups within one archive are not supported.
2. Individual files cannot be recovered from a disk backup.
3. Backups cannot be deleted from a tape either manually or automatically during cleanup. Retention rules are disabled in the GUI when backing up to a locally attached tape.
4. Personal vaults cannot be created on tape devices.
5. Because the presence of an operating system cannot be detected in a backup located on a tape, Acronis Universal Restore is proposed at every disk or volume recovery, even when recovering a non-system Windows volume.

Recovery from a locally attached tape device

Before creating a recovery task, insert or mount the tape containing the backup you need to recover. When creating a recovery task, select the tape device from the list of available locations and then select the backup. After recovery is started, you will be prompted for other tapes if the tapes are needed for recovery.

2.7 Proprietary Acronis technologies

This section describes the proprietary technologies of Acronis Backup & Recovery Server OEM.

2.7.1 Acronis Startup Recovery Manager

A modification of the bootable agent can be placed on a system disk and configured to start at boot time when F11 is pressed. This eliminates the need for rescue media or network connection to start the bootable rescue utility. This feature has the trade name "Acronis Startup Recovery Manager".

Acronis Startup Recovery Manager is especially useful for mobile users. If a failure occurs, the user reboots the machine, hits F11 on prompt "Press F11 for Acronis Startup Recovery Manager..." and performs data recovery in the same way as with ordinary bootable media. The user can also back up using Acronis Startup Recovery Manager, while on the move.

On machines with the GRUB boot loader installed, the user selects the Acronis Startup Recovery Manager from the boot menu instead of pressing F11.

Activation and deactivation of the Acronis Startup Recovery Manager

The operation that enables using Acronis Startup Recovery Manager is called "activation". To activate Acronis Startup Recovery Manager, select **Tools > Activate Acronis Startup Recovery Manager** from the program menu.

You can activate or deactivate the Acronis Startup Recovery Manager at any time from the **Tools** menu. The deactivation will disable the boot time prompt "Press F11 for Acronis Startup Recovery

Manager..." (or removes the corresponding entry from GRUB's boot menu). This means you will need bootable media in case the system fails to boot.

Limitation

Acronis Startup Recovery Manager requires re-activation of third-party loaders after activation.

2.7.2 Universal Restore (Acronis Backup & Recovery Server OEM Universal Restore)

Acronis Backup & Recovery Server OEM Universal Restore is the Acronis proprietary technology that helps recover and boot up Windows on dissimilar hardware. The Universal Restore handles differences in devices that are critical for the operating system start-up, such as storage controllers, motherboard or chipset.

Acronis Backup & Recovery Server OEM Universal Restore purpose

A system can be easily recovered from a disk backup (image) onto the same system or to identical hardware. However, if you change a motherboard or use another processor version—a likely possibility in case of hardware failure—the recovered system could be unbootable. An attempt to transfer the system to a new, much more powerful computer will usually produce the same unbootable result because the new hardware is incompatible with the most critical drivers included in the image.

Using Microsoft System Preparation Tool (Sysprep) does not solve this problem, because Sysprep permits installing drivers only for Plug and Play devices (sound cards, network adapters, video cards etc.). As for system Hardware Abstraction Layer (HAL) and mass storage device drivers, they must be identical on the source and the target computers (see Microsoft Knowledge Base, articles 302577 and 216915).

The Universal Restore technology provides an efficient solution for hardware-independent system recovery by replacing the crucial Hardware Abstraction Layer (HAL) and mass storage device drivers.

Universal Restore is applicable for:

1. Instant recovery of a failed system on different hardware.
2. Hardware-independent cloning and deployment of operating systems.
3. Physical-to-physical machine migration.

The Universal Restore principles

1. Automatic HAL and mass storage driver selection.

Universal Restore searches for drivers in the network folders you specify, on removable media and in the default driver storage folders of the system being recovered. Universal Restore analyzes the compatibility level of all found drivers and installs HAL and mass storage drivers that better fit the target hardware. Drivers for network adapters are also searched and passed to the operating system which installs them automatically when first started.

*The Windows default driver storage folder is determined in the registry value **DevicePath**, which can be found in the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. This storage folder is usually **WINDOWS/inf**.*

2. Manual selection of the mass storage device driver.

If the target hardware has a specific mass storage controller (such as a SCSI, RAID, or Fibre Channel adapter) for the hard disk, you can install the appropriate driver manually, bypassing the automatic driver search-and-install procedure.

3. Installing drivers for Plug and Play devices.

Universal Restore relies on the built-in Plug and Play discovery and configuration process to handle hardware differences in devices that are not critical for the system start, such as video, audio and USB. Windows takes control over this process during the logon phase, and if some of the new hardware is not detected, you will have a chance to install drivers for it later manually.

Universal Restore and Microsoft Sysprep

Universal Restore is not a system preparation tool. You can apply it to any Windows image created by Acronis Backup & Recovery Server OEM, including images of systems prepared with Microsoft System Preparation Tool (Sysprep). The following is an example of using both tools on the same system.

Universal Restore does not strip the security identifier (SID) and user profile settings in order to run the system immediately after recovery without re-joining the domain or re-mapping network user profiles. If you are going to change the above settings on a recovered system, you can prepare the system with Sysprep, image it and recover, if need be, using the Universal Restore.

Limitations

Universal Restore is not available:

when a computer is booted with Acronis Startup Recovery Manager (using F11).

Getting Universal Restore

Universal Restore comes free with Acronis Backup & Recovery Server OEM.

3 Options

This section covers Acronis Backup & Recovery Server OEM options that can be configured using Graphical User Interface.

3.1 Console options

The console options define the way information is represented in the Graphical User Interface of Acronis Backup & Recovery Server OEM.

To access the console options, select **Options > Console** options from the top menu.

3.1.1 Startup page

This option defines whether to show the **Welcome** screen or the **Dashboard** upon connection of the console to a managed machine.

The preset is: the **Welcome** screen.

To make a selection, select or clear the check box for **Show the Dashboard view upon connection of the console to a machine**.

This option can also be set on the **Welcome** screen. If you select the check box for **At startup, show the Dashboard instead of the current view** on the **Welcome** screen, the setting mentioned above will be updated accordingly.

3.1.2 Pop-up messages

About tasks that need interaction

This option is effective when the console is connected to a managed machine.

The option defines whether to display the pop-up window when one or more tasks require user interaction. This window enables you to specify your decision, such as to confirm reboot or to retry after freeing-up the disk space, on all the tasks in the same place. Until at least one task requires interaction, you can open this window at any time from the managed machine's **Dashboard**. Alternatively, you can review the task execution states in the **Tasks** view and specify your decision on each task in the **Information** pane.

The preset is: **Enabled**.

To make a selection, select or clear the **Pop up the "Tasks Need Interaction" window** check box.

About the task execution results

This option is effective only when the console is connected to a managed machine.

The option defines whether to display the pop-up messages about task run results: successful completion, failure or success with warnings. When displaying of pop-up messages is disabled, you can review the task execution states and results in the **Tasks** view.

The preset is: **Enabled** for all results.

To make a setting for each result (successful completion, failure or success with warnings) individually, select or clear the respective check box.

3.1.3 Time-based alerts

Last backup

This option is effective when the console is connected to a managed machine (p. 151).

The option defines whether to alert if no backup was performed on a given machine for a period of time. You can configure the time period that is considered critical for your business.

The preset is: alert if the last successful backup on a machine was completed more than **5 days** ago.

The alert is displayed in the **Alerts** section of the **Dashboard**.

3.1.4 Fonts

This option is effective when the console is connected to a managed machine.

The option defines the fonts to be used in the Graphical User Interface of Acronis Backup & Recovery Server OEM. The **Menu** setting affects the drop-down and context menus. The **Application** setting affects the other GUI elements.

The preset is: **System Default** font for both the menus and the application interface items.

To make a selection, choose the font from the respective combo-box and set the font's properties. You can preview the font's appearance by clicking the button to the right.

3.2 Machine options

The machine options define the general behavior of all Acronis Backup & Recovery Server OEM agents operating on the managed machine, and so the options are considered machine-specific.

To access the machine options, connect the console to the managed machine and then select **Options > Machine options** from the top menu.

3.2.1 Event tracing

It is possible to duplicate log events generated by the agent(s), operating on the managed machine, in the Application Event Log of Windows; or send the events to the specified SNMP managers. If you do not modify the event tracing options anywhere except for here, your settings will be effective for each local backup plan and each task created on the machine.

You can override the settings set here, exclusively for the events that occur during backup or during recovery, in the Default backup and recovery options (p. 31). In this case, the settings set here will be effective for operations other than backup and recovery, such as archive validation or cleanup.

You can further override the settings set in the default backup and recovery options, when creating a backup plan or a recovery task. The settings you obtain in this case will be plan-specific or task-specific.

3.2.1.1 Windows event log

This option is effective only in Windows operating systems.

This option is not available when operating under the bootable media.

This option defines whether the agent(s) operating on the managed machine have to log events in the Application Event Log of Windows (to see this log, run **eventvwr.exe** or select **Control Panel > Administrative tools > Event Viewer**). You can filter the events to be logged.

You can override the settings set here, exclusively for the events that occur during backup or during recovery, in the Default backup and recovery options (p. 31). In this case, the settings set here will be effective for operations other than backup and recovery, such as archive validation or cleanup.

You can further override the settings set in the default backup and recovery options, when creating a backup plan or a recovery task. The settings you obtain in this case will be plan-specific or task-specific.

The preset is: **Disabled**.

To enable this option, select the **Log events** check box.

Use the **Types of events to log** check box to filter the events to be logged in the Application Event Log of Windows:

- **All events** - all events (information, warnings and errors)
- **Errors and warnings**
- **Errors only**.

To disable this option, clear the **Log events** check box.

3.2.1.2 SNMP notifications

This option is effective for Windows operating systems.

This option is not available when operating under the bootable media.

The option defines whether the agent(s) operating on the managed machine have to send the log events to the specified Simple Network Management Protocol (SNMP) managers. You can choose the types of events to be sent.

You can override the settings set here, exclusively for the events that occur during backup or during recovery, in the Default backup and recovery options (p. 31). In this case, the settings set here will be effective for operations other than backup and recovery, such as archive validation or cleanup.

You can further override the settings set in the default backup and recovery options, when creating a backup plan or a recovery task. The settings you obtain in this case will be plan-specific or task-specific.

For detailed information about using SNMP with Acronis Backup & Recovery Server OEM, please see "Support for SNMP".

The preset is: **Disabled**.

To set up sending SNMP messages

Select the Send messages to SNMP server check box.

Specify the appropriate options as follows:

Types of events to send – choose the types of events: All events, Errors and warnings, or Errors only.

Server name/IP – type the name or IP address of the host running the SNMP management application, the messages will be sent to.

Community – type the name of the SNMP community to which both the host running SNMP management application and the sending machine belong. The typical community is "public".

To disable sending SNMP messages, clear the Send messages to SNMP server check box.

The messages are sent over UDP.

The next section contains additional information about Setting up SNMP services on the receiving machine.

3.2.1.3 Setting up SNMP services on the receiving machine

Windows

To install the SNMP service on a machine running Windows:

1. **Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components.**
2. Select **Management and Monitoring Tools**.
3. Click **Details**.
4. Select the **Simple Network Management Protocol** check box.
5. Click **OK**.

You might be asked for Immib2.dll that can be found on the installation disc of your operating system.

3.2.2 Log cleanup rules (UMMS)

This option specifies how to clean up the Acronis Backup & Recovery Server OEM agent log.

This option defines the maximum size of the agent log folder (in Windows XP/2003 Server, %ALLUSERSPROFILE%\Application Data\ASM\UniversalBMR\UMMS\LogEvents).

The preset is: **Maximum log size: 1 GB. On cleanup, keep 95% of the maximum log size.**

When the option is enabled, the program compares the actual log size with the maximum size after every 100 log entries. Once the maximum log size is exceeded, the program deletes the oldest log entries. You can select the amount of log entries to retain. The default 95% setting will keep most of the log. With the minimum 1% setting, the log will be nearly cleared.

3.3 Default backup and recovery options

3.3.1 Default backup options

Availability of the backup options

The set of available backup options depends on:

- The environment the agent operates in (Windows media)
- The type of the data being backed up (disk)
- The backup destination (networked location or local disk)
- The backup scheme (Back up now or using the scheduler)

The following table summarizes the availability of the backup options.

	Agent for Windows	Bootable media (PE-based)
	Disk backup	Disk backup
Archive protection (password)	+	+
Pre/Post backup commands	+	PE only
Pre/Post data capture commands	+	-
Multi-volume snapshot	+	-
Use VSS (p. 36)	+	-
Compression level	+	+
Backup performance:		
Backup priority	+	-

HDD writing speed	Dest: HDD	Dest: HDD
Network connection speed	Dest: network share	Dest: network share
Backup splitting	+	+
Error handling:		
Do not show messages and dialogs while processing (silent mode)	+	+
Re-attempt if an error occurs	+	+
Ignore bad sectors	+	+
Task failure handling	+	-
Tape support	Dest: managed vault on a tape library	Dest: managed vault on a tape library
Additional settings:		
Overwrite data on a tape without prompting user for confirmation	Dest: Tape	Dest: Tape
Dismount media after backup is finished	Dest: removable media	Dest: removable media
Ask for first media while creating backup archives on removable media	Dest: removable media	Dest: removable media
Validate backup after creation	-	+
Reboot after the backup	-	+
Notifications:		
E-mail	+	-
Win Pop-up	+	-
Event tracing:		
Windows events log (p. 41)	+	-
SNMP	+	-

3.3.1.1 Archive protection

This option is effective for Windows operating systems and bootable media.

This option is effective for disk-level backup.

The preset is: **Disabled**.

To protect the archive from unauthorized access

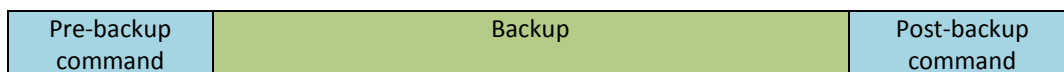
1. Select the **Set password for the archive** check box.
2. In the **Enter the password** field, type a password.
3. In the **Confirm the password** field, re-type the password.
4. Click **OK**.

3.3.1.2 Pre/Post commands

This option is effective for Windows operating systems and PE-based bootable media.

The option enables you to define the commands to be automatically executed before and after the backup procedure.

The following scheme illustrates when pre/post commands are executed.



Examples of how you can use the pre/post commands:

- delete some temporary files from the disk before starting backup
- configure a third-party antivirus product to be started each time before the backup starts
- copy an archive to another location after the backup ends.

The program does not support interactive commands, i.e. commands that require user input (for example, "pause").

To specify pre/post commands

1. Enable pre/post commands execution by checking the following options:
 - **Execute before the backup**
 - **Execute after the backup**
2. Do any of the following:
 - Click **Edit** to specify a new command or a batch file
 - Select the existing command or the batch file from the drop-down list
3. Click **OK**.

Pre-backup command

To specify a command/batch file to be executed before the backup process starts

1. In the **Command** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
2. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
3. In the **Arguments** field specify the command's execution arguments, if required.
4. Depending on the result you want to obtain, select the appropriate options as described in the table below.
5. Click **Test command** to check if the command is correct.

Check box	Selection
-----------	-----------

Fail the task if the command execution fails	Selected	Cleared	Selected	Cleared
Do not back up until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Perform the backup only after the command is successfully executed. Fail the task if the command execution fails.	Perform the backup after the command is executed despite execution failure or success.	N/A	Perform the backup concurrently with the command execution and irrespective of the command execution result.

Post-backup command

To specify a command/executable file to be executed after the backup is completed

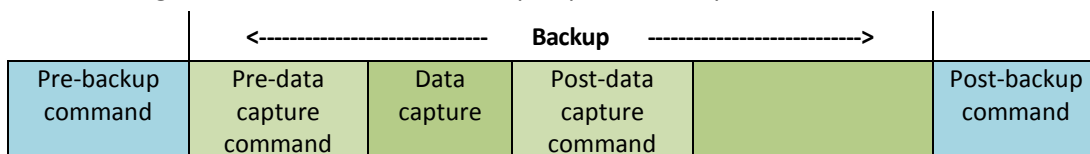
1. In the **Command** field, type a command or browse to a batch file.
2. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
3. In the **Arguments** field, specify the command execution arguments, if required.
4. If successful execution of the command is critical for your backup strategy, select the **Fail the task if the command execution fails** check box. In case the command execution fails, the program will remove the resulting TIB file and temporary files if possible, and the task will fail.
When the check box is not selected, the command execution result does not affect the task execution failure or success. You can track the command execution result by exploring the log or the errors and warnings displayed on the **Dashboard**.
5. Click **Test Command** to check if the command is correct.

3.3.1.3 Pre/Post data capture commands

This option is effective for Windows operating systems.

The option enables you to define the commands to be automatically executed before and after data capture (that is, taking the data snapshot) performed by Acronis Backup & Recovery Server OEM at the beginning of the backup procedure.

The following scheme illustrates when the pre/post data capture commands are executed.



If the Volume Shadow Copy Service (p. 36) option is enabled, the commands' execution and the Microsoft VSS actions will be sequenced as follows:

"Before data capture" commands -> VSS Suspend -> Data capture -> VSS Resume -> "After data capture" commands.

Using the pre/post data capture commands, you can suspend and resume a database or application that is not compatible with VSS. As opposed to the Pre/Post commands, the pre/post data capture commands will be executed before and after the data capture process, which takes seconds, while the entire backup procedure may take much longer, depending on the amount of data to be backed up. Therefore, the database or application idle time will be minimal.

To specify pre/post data capture commands

1. Enable pre/post data capture commands execution by checking the following options:
 - **Execute before the data capture**
 - **Execute after the data capture**
2. Do any of the following:
 - Click **Edit** to specify a new command or a batch file
 - Select the existing command or the batch file from the drop-down list
3. Click **OK**.

Pre-data capture command

To specify a command/batch file to be executed before data capture

1. In the **Command** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
2. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
3. In the **Arguments** field specify the command's execution arguments, if required.
4. Depending on the result you want to obtain, select the appropriate options as described in the table below.
5. Click **Test command** to check if the command is correct.

Check box	Selection			
Fail the backup task if the command execution fails	Selected	Cleared	Selected	Cleared
Do not perform the data capture until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Perform the data capture only after the command is successfully executed. Fail the task if the command execution fails.	Perform the data capture after the command is executed despite execution failure or success.	N/A	Perform the data capture concurrently with the command and irrespective of the command execution result.

Post-data capture command

To specify a command/batch file to be executed after data capture

1. In the **Command** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)

2. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
3. In the **Arguments** field specify the command's execution arguments, if required.
4. Depending on the result you want to obtain, select the appropriate options as described in the table below.
5. Click **Test command** to check if the command is correct.

Check box	Selection			
Fail the task if the command execution fails	Selected	Cleared	Selected	Cleared
Do not back up until the command execution is complete	Selected	Selected	Cleared	Cleared
Result				
	Preset Continue the backup only after the command is successfully executed. Delete the TIB file and temporary files and fail the task if the command execution fails.	Continue the backup after the command is executed despite command execution failure or success.	N/A	Continue the backup concurrently with the command execution and irrespective of the command execution result.

3.3.1.4 Multi-volume snapshot

This option is effective only for Windows operating systems.

This option applies to disk-level backup.

The option determines whether to take snapshots of multiple volumes at the same time or one by one.

The preset is: **Enable**.

When this option is set to **Enable**, snapshots of all volumes being backed up will be created simultaneously. Use this option to create a time-consistent backup of data spanned across multiple volumes, for instance for an Oracle database.

When this option is set to **Disable**, the volumes' snapshots will be taken one after the other. As a result, if the data spans across several volumes, the resulting backup may be not consistent.

3.3.1.5 Volume Shadow Copy Service

This option is effective only for Windows operating systems.

The option defines whether a Volume Shadow Copy Service (VSS) provider—either Acronis VSS or Microsoft VSS—has to notify VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications, in particular, completion of all database transactions, at the moment of taking the data snapshot by Acronis Backup & Recovery Server OEM.

Data consistency, in turn, ensures that the application will be recovered in the correct state and become operational immediately after recovery.

The preset is: **Create snapshots using VSS**

Acronis Backup & Recovery Server OEM will select the VSS provider automatically based on the operating system running on the machine and whether the machine is a member of an Active Directory domain.

Create snapshots without using VSS

Choose this option if your database is incompatible with VSS. The data snapshot will be taken by Acronis Backup & Recovery Server OEM. Backup process is fastest, but data consistency of the applications whose transactions are not completed at the time of taking a snapshot cannot be guaranteed. You may use Pre/Post data capture commands to indicate which commands should be performed before and after taking the snapshot, to ensure that the data is being backed up in a consistent state. For instance, specify pre-data capture commands that will suspend the database and flush all caches to ensure that all transactions are completed; and specify post-data capture commands that will resume the database operations after the snapshot is taken.

Volume shadow copy writers

Before backing up the data of VSS-aware applications, make sure that the volume shadow copy writers for those applications are turned on, by examining the list of writers that are present in the operating system. To view this list, run the following command:

```
vssadmin list writers
```

Note: In Microsoft Windows Small Business Server 2003, the writer for Microsoft Exchange Server 2003 is turned off by default. For instructions on how to turn it on, see the corresponding Microsoft Help and Support article <http://support.microsoft.com/kb/838183/en>.

3.3.1.6 Compression level

This option is effective for Windows operating systems and bootable media.

The option defines the level of compression applied to the data being backed up.

The preset is: **Normal**.

The optimal data compression level depends on the type of data being backed up. For example, even maximum compression will not significantly reduce the archive size if the archive contains essentially compressed files, such as .jpg, .pdf or .mp3. However, formats such as .doc or .xls will be compressed well.

To specify the compression level

Select one of the following:

- **None** – the data will be copied as is, without any compression. The resulting backup size will be maximal.
- **Normal** – recommended in most cases.
- **High** – the resulting backup size will typically be less than for the **Normal** level.
- **Maximum** – the data will be compressed as much as possible. The backup duration will be maximal. You may want to select maximum compression when backing up to removable media to reduce the number of blank disks required.

3.3.1.7 Backup performance

Use this group of options to specify the amount of network and system resources to allocate to the backup process.

Backup performance options might have a more or less noticeable effect on the speed of the backup process. This depends on the overall system configuration and the physical characteristics of devices the backup is being performed from or to.

Backup priority

This option is effective for Windows operating systems.

The priority of a process running in a system determines the amount of CPU and system resources allocated to that process. Decreasing the backup priority will free more resources for other applications. Increasing the backup priority might speed up the backup process by requesting the operating system to allocate more resources like the CPU to the backup application. However, the resulting effect will depend on the overall CPU usage and other factors like disk in/out speed or network traffic.

The preset is: **Low**.

To specify the backup process priority

Select one of the following:

- **Low** – to minimize resources taken by the backup process, leaving more resources to other processes running on the machine
- **Normal** – to run the backup process with normal speed, allocating resources on a par with other processes
- **High** – to maximize the backup process speed by taking resources from other processes.

HDD writing speed

This option is effective for Windows operating systems and bootable media.

This option is available when an internal (fixed) hard disk of the machine being backed up is selected as the backup destination

Backing up to a fixed hard disk may slow performance of the operating system and applications because of the large amounts of data that needs to be written to the disk. You can limit the hard disk usage by the backup process to the desired level.

The preset is: **Maximum**.

To set the desired HDD writing speed for backup

Do any of the following:

- Click **Writing speed stated as a percentage of the maximum speed of the destination hard disk**, and then drag the slider or select a percentage in the box
- Click **Writing speed stated in kilobytes per second**, and then enter the writing speed in kilobytes per second.

Network connection speed

This option is effective for Windows operating systems and bootable media.

This option is available when a location on the network (network share, managed vault or an FTP/SFTP server) is selected as the backup destination.

The option defines the amount of network connection bandwidth allocated for transferring the backup data.

By default the speed is set to maximum, i.e. the software uses all the network bandwidth it can get when transferring the backup data. Use this option to reserve a part of the network bandwidth to other network activities.

The preset is: **Maximum**.

To set the network connection speed for backup

Do any of the following:

- Click **Transferring speed stated as a percentage of the estimated maximum speed of the network connection**, and then drag the slider or type a percentage in the box
- Click **Transferring speed stated in kilobytes per second**, and then enter the bandwidth limit for transferring backup data in kilobytes per second.

3.3.1.8 Notifications

Acronis Backup & Recovery Server OEM provides the ability of notifying users about backup completion through e-mail or the messaging service.

E-mail

This option is effective for Windows operating systems.

This option is not available when operating under the bootable media.

The option enables you to receive e-mail notifications about the backup task's successful completion, failure or need for interaction along with the full log of the task.

The preset is: **Disabled**.

To configure e-mail notification

1. Select the **Send e-mail notifications** check box to activate notifications.
2. In the **E-mail addresses** field, type the e-mail address to which notifications will be sent. You can enter several addresses separated by semicolons.
3. Under **Send notifications**, select the appropriate check boxes as follows:
 - **When backup completes successfully** – to send a notification when the backup task has completed successfully
 - **When backup fails** – to send a notification when the backup task has failedThe **When user interaction is required** check box is always selected.
4. For the e-mail message to include the log entries related to the backup, select the **Add full log to the notification** check box.
5. Click **Additional e-mail parameters**, to configure additional e-mail parameters as follows, then click **OK**:
 - **From** - type the e-mail address of the user from whom the message will be sent. If you leave this field empty, messages will be constructed as if they are from the destination address.

- **Use encryption** – you can opt for encrypted connection to the mail server. SSL and TLS encryption types are available for selection.
- Some Internet service providers require authentication on the incoming mail server before being allowed to send something. If this is your case, select the **Log on to incoming mail server** check box to enable a POP server and to set up its settings:
 - **Incoming mail server (POP)** – enter the name of the POP server.
 - **Port** – set the port of the POP server. By default, the port is set to 110.
 - **User name** – enter the user name
 - **Password** – enter the password.
- Select the **Use the specified outgoing mail server** check box to enable an SMTP server and to set up its settings:
 - **Outgoing mail server (SMTP)** – enter the name of the SMTP server.
 - **Port** – set the port of the SMTP server. By default, the port is set to 25.
 - **User name** – enter the user name.
 - **Password** – enter the password.

Click **Send test e-mail message** to check if the settings are correct.

Messenger service (WinPopup)

This option is effective for Windows operating systems on the sending machine and only for Windows on the receiving machine.

This option is not available when operating under bootable media.

The option enables you to receive WinPopup notifications about the backup task's successful completion, failure or need for interaction.

The preset is: **Disabled**.

Before configuring WinPopup notifications, make sure the Messenger service is started on both the machine executing the task and the machine that will receive messages.

The Messenger service is not started by default in the Microsoft Windows Server 2003 family. Change the service Startup mode to Automatic and start the service.

To configure WinPopup notifications:

Select the Send WinPopup notifications check box.

In the Machine name field, enter the name of the machine to which notifications will be sent. Multiple names are not supported.

Under Send notifications, select the appropriate check boxes as follows:

- **When backup completes successfully** – to send notification when the backup operation is completed successfully
- **When backup fails** – to send notification when the backup operation is failed

The **When user interaction is required** check box – to send notification during the operation when user interaction is required – is always selected.

Click **Send test WinPopup message** to check if the settings are correct.

3.3.1.9 Event tracing

It is possible to duplicate log events of the backup operations, performed on the managed machine, in the Application Event Log of Windows; or send the events to the specified SNMP managers.

Windows event log

This option is effective only in Windows operating systems.

This option is not available when operating under the bootable media.

This option defines whether the agent(s) operating on the managed machine have to log events of the backup operations in the Application Event Log of Windows (to see this log, run **eventvwr.exe** or select **Control Panel > Administrative tools > Event Viewer**). You can filter the events to be logged.

The preset is: **Use the setting set in the Machine options.**

To select whether to log the backup operations events in the Application Event Log of Windows:

Choose one of the following:

- **Use the setting set in the Machine options** – to use the setting specified for the machine. For more information refer to Machine options.
- **Log the following event types** – to log events of the backup operations in the Application Event Log. Specify the types of events to be logged:
 - **All events** – log all events (information, warnings and errors)
 - **Errors and warnings**
 - **Errors only**
- **Do not log** - to disable logging events of the backup operations in the Application Event Log.

SNMP notifications

This option is effective for Windows operating systems.

This option is not available when operating under the bootable media.

The option defines whether the agent(s) operating on the managed machine have to send the log events to the specified Simple Network Management Protocol (SNMP) managers. You can choose the types of events to be sent.

You can override the settings set here, exclusively for the events that occur during backup or during recovery, in the Default backup and recovery options (p. 31). In this case, the settings set here will be effective for operations other than backup and recovery, such as archive validation or cleanup.

You can further override the settings set in the default backup and recovery options, when creating a backup plan or a recovery task. The settings you obtain in this case will be plan-specific or task-specific.

For detailed information about using SNMP with Acronis Backup & Recovery Server OEM, please see "Support for SNMP".

The preset is: **Disabled.**

To set up sending SNMP messages

Select the Send messages to SNMP server check box.

Specify the appropriate options as follows:

Types of events to send – choose the types of events: All events, Errors and warnings, or Errors only.

Server name/IP – type the name or IP address of the host running the SNMP management application, the messages will be sent to.

Community – type the name of the SNMP community to which both the host running SNMP management application and the sending machine belong. The typical community is "public".

To disable sending SNMP messages, clear the Send messages to SNMP server check box.

The messages are sent over UDP.

The next section contains additional information about Setting up SNMP services on the receiving machine.

3.3.1.10 Backup splitting

This option is effective for Windows operating systems and bootable media.

The option defines how a backup can be split.

The preset is: Automatic.

The following settings are available.

Automatic

With this setting, Acronis Backup & Recovery Server OEM will act as follows.

When backing up to a hard disk:

A single backup file will be created if the destination disk's file system allows the estimated file size.

The backup will automatically be split into several files if the destination disk's file system does not allow the estimated file size. Such might be the case when the backup is placed on FAT16 and FAT32 file systems that have a 4GB file size limit.

If the destination disk runs out of free space while creating the backup, the task enters the Need interaction state. You have the ability to free additional space and retry the operation. If you do so, the resulting backup will be split into the parts created before and after the retry.

When backing up to removable media (CD, DVD or a tape device locally attached to the managed machine):

The task will enter the Need interaction state and ask for a new media when the previous one is full.

Fixed size

Enter the desired file size or select it from the drop-down list. The backup will then be split into multiple files of the specified size. This comes in handy when creating a backup that you plan to burn to multiple CDs or DVDs later on. You might also want to split the backup destined to an FTP server, since data recovery directly from an FTP server requires the backup to be split into files no more than 2GB in size.

3.3.1.11 Error handling

These options are effective for Windows operating systems and bootable media.

These options enable you to specify how to handle errors that might occur during backup.

Do not show messages and dialogs while processing (silent mode)

The preset is: **Disabled**.

With the silent mode enabled, the program will automatically handle situations requiring user interaction (except for handling bad sectors, which is defined as a separate option). If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

Re-attempt, if an error occurs

The preset is: **Enabled. Number of attempts: 5. Interval between attempts: 30 seconds.**

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts is performed, depending on which comes first.

For example, if the backup destination on the network becomes unavailable or not reachable, the program will attempt to reach the destination every 30 seconds, but no more than 5 times. The attempts will be stopped as soon as the connection is resumed OR the specified number of attempts is performed, depending on which comes first.

Ignore bad sectors

The preset is: **Disabled**.

When the option is disabled, the program will display a pop-up window each time it comes across a bad sector and ask for a user decision as to whether to continue or stop the backup procedure. In order to back up the valid information on a rapidly dying disk, enable ignoring bad sectors. The rest of the data will be backed up and you will be able to mount the resulting disk backup and extract valid files to another disk.

3.3.1.12 Task failure handling

This option is effective for Windows operating systems.

This option is not available when operating under the bootable media.

This option determines the program behavior when any of the backup plan's tasks fails.

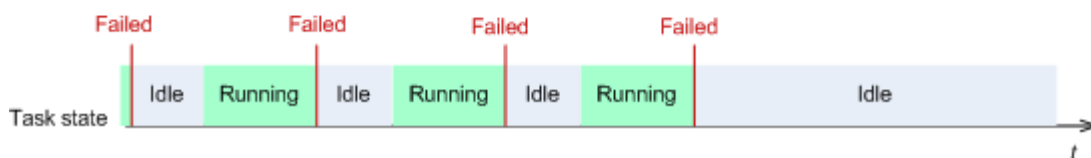
The preset is **not to restart a failed task**.

The program will try to execute the failed task again if you select the **Restart a failed task** check box and specify the number of attempts and the time interval between the attempts. The program stops trying as soon as an attempt completes successfully OR the specified number of attempts is performed, depending on which comes first.

N=3: 2nd attempt succeeded



N=3: none of attempts succeeded



If the task fails because of a mistake in the backup plan, you can edit the plan while the task is in the Idle state. While the task is running, you have to stop it prior to editing the backup plan.

3.3.1.13 Tape support

These options are effective when the backup destination is a managed vault located on a tape library.

Tape support options enable you to specify how the backup tasks will distribute backups among the tapes.

Some combinations of tape options might degrade usage efficiency of both the whole tape library and each tape. If you are not forced to modify these options by some specific needs, leave them unchanged.

An archive can occupy several tapes. In such cases a so-called **tape set** is used for keeping the data backups.

Tape set is a logical group of one or more tapes which contain backups of the specific protected data. A tape set can contain backups of other data as well.

Separate tape set is a tape set which contains only backups of the specific protected data. Other backups cannot be written to a separate tape set.

(For the backup plan to be created) Use a separate tape set

The preset is: **Disabled**.

If you leave this option unchanged, then the backups, belonging to the plan being created, might be written onto tapes containing backups written by different backup plans and comprising of data from different machines.

When this option is enabled, the backups, belonging to the plan being created, will be located on a separate tape set. Other backups will not be written to this tape set.

Always use a free tape

If you leave the options below unchanged, then each backup will be written onto the tape specified by the **Use a separate tape set** option. With some of the options below enabled, the program will add new tapes to the tape set every time when a full, incremental or differential backup is created.

- **For each full backup**

The preset is: **Disabled**.

When this option is enabled, each full backup will be written onto a free tape. The tape will be loaded to a drive especially for this operation. If the **Use a separate tape set** option is enabled, only incremental and differential backups of the same data will be appended to the tape.

3.3.1.14 Additional settings

Specify the additional settings for the backup operation by selecting or clearing the following check boxes.

Overwrite data on a tape without prompting for user confirmation

This option is effective only when backing up to a tape device.

The preset is: **Disabled**.

When starting backup to a non-empty tape in a locally attached tape device, the program will warn that you are about to lose data on the tape. To disable this warning, select this check box.

Dismount media after backup has finished

This option is effective in Windows operating systems.

This option is effective when backing up to a removable media (CD, DVD, tape or floppy disk.)

The preset is: **Disabled**.

The destination CD/DVD can be ejected or the tape can be dismounted after the backup is completed.

Ask for the first media while backing up to removable media

This option is effective only when backing up to removable media.

The option defines whether to display the **Insert First Media** prompt when backing up to removable media.

The preset is: **Enabled**.

When the option is enabled, backing up to removable media may be not possible if the user is away, because the program will wait for someone to press OK in the prompt box. Hence, you should disable the prompt when scheduling a backup to removable media. Then, if the removable media is available (for example, a DVD is inserted), the task can run unattended.

Restart the machine automatically after backup is finished

This option is available only when operating under bootable media.

The preset is: **Disabled**.

When the option is enabled, Acronis Backup & Recovery Server OEM will restart the machine after the backup process is completed.

For example, if the machine boots from a hard disk drive by default and you select this check box, the machine will be restarted and the operating system will start as soon as the bootable agent has finished creating the backup.

Use FTP in Active mode

The preset is: **Disabled**.

Enable this option if the FTP server supports active mode and you want this mode to be used for file transfers.

3.3.2 Default recovery options

Availability of the recovery options

The set of available recovery options depends on:

- The environment the agent operates in (Windows, bootable media)
- The type of data being recovered (disk)
- The operating system being recovered from the disk backup (Windows)

The following table summarizes the availability of the recovery options.

	Agent for Windows		Bootable media (PE-based)	
	Disk recovery	File recovery (also from a disk backup)	Disk recovery	File recovery (also from a disk backup)
Pre/Post recovery commands	+	+	PE only	PE only
Recovery priority	+	+	-	-
File-level security (p. 49):				
Recover files with their security settings	-	+	-	+
Error handling:				
Do not show messages and dialogs while processing (silent mode)	+	+	+	+
Re-attempt if an error occurs	+	+	+	+
Additional settings:				
Set current date and time for recovered files	-	+	-	+
Validate backup archive before recovery	+	+	+	+

Check file system after recovery	+	-	+	-
Reboot machine automatically if it is required for recovery	+	+	-	-
Notifications:				
E-mail	+	+	-	-
Win Pop-up	+	+	-	-
Event tracing:				
Windows events log (p. 51)	+	+	-	-
SNMP	+	+	-	-

3.3.2.1 Pre/Post commands

This option is effective for Windows operating systems and PE-based bootable media.

The option enables you to define the commands to be automatically executed before and after the data recovery.

Example of how you can use the pre/post commands:

- launch the `Checkdisk` command in order to find and fix logical file system errors, physical errors or bad sectors to be started before the recovery starts or after the recovery ends.

The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)

A post-recovery command will not be executed if the recovery proceeds with reboot.

To specify pre/post commands

1. Enable pre/post commands execution by checking the following options:
 - **Execute before the recovery**
 - **Execute after the recovery**
2. Do any of the following:
 - Click **Edit** to specify a new command or a batch file
 - Select the existing command or the batch file from the drop-down list
3. Click **OK**.

Pre-recovery command

To specify a command/batch file to be executed before the recovery process starts

1. In the **Command** field, type a command or browse to a batch file. The program does not support interactive commands, i.e. commands that require user input (for example, "pause".)
2. In the **Working directory** field, specify a path to a directory where the command/batch file will be executed.
3. In the **Arguments** field specify the command's execution arguments, if required.
4. Depending on the result you want to obtain, select the appropriate options as described in the table below.

5. Click **Test command** to check if the command is correct.

Check box	Selection			
	Selected	Cleared	Selected	Cleared
Fail the task if the command execution fails				
Do not recover until the command execution is complete				
Result				
	Preset Perform the recovery only after the command is successfully executed. Fail the task if the command execution failed.	Perform the recovery after the command is executed despite execution failure or success.	N/A	Perform the recovery concurrently with the command execution and irrespective of the command execution result.

Post-recovery command

To specify a command/executable file to be executed after the recovery is completed

1. In the **Command** field, type a command or browse to a batch file.
2. In the **Working** directory field, specify a path to a directory where the command/batch file will be executed.
3. In the **Arguments** field, specify the command execution arguments, if required.
4. If successful execution of the command is critical for you, select the **Fail the task if the command execution fails** check box. In case the command execution fails, the task run result will be set to Failed.

When the check box is not selected, the command execution result does not affect the task execution failure or success. You can track the command execution result by exploring the log or the errors and warnings displayed on the **Dashboard**.

5. Click **Test command** to check if the command is correct.

A post-recovery command will not be executed if the recovery proceeds with reboot.

3.3.2.2 Recovery priority

This option is effective for Windows operating systems.

This option is not available when operating under the bootable media.

The priority of a process running in a system determines the amount of CPU and system resources allocated to that process. Decreasing the recovery priority will free more resources for other applications. Increasing the recovery priority might speed up the recovery process by requesting the operating system to allocate more resources to the application that will perform the recovery. However, the resulting effect will depend on the overall CPU usage and other factors like disk I/O speed or network traffic.

The preset is: **Normal**.

To specify the recovery process priority

Select one of the following:

- **Low** – to minimize resources taken by the recovery process, leaving more resources to other processes running on the machine
- **Normal** – to run the recovery process with normal speed, allocating resources on a par with other processes
- **High** – to maximize the recovery process speed by taking resources from the other processes.

3.3.2.3 File-level security

This option is effective only for recovery from file-level backup of Windows files.

This option defines whether to recover NTFS permissions for files along with the files.

The preset is: **Recover files with their security settings**.

If the file NTFS permissions were preserved during backup, you can choose whether to recover the permissions or let the files inherit the NTFS permissions from the folder to which they are recovered.

3.3.2.4 Notifications

Acronis Backup & Recovery Server OEM provides the ability of notifying users about recovery completion through e-mail or the messaging service.

E-mail

This option is effective for Windows operating systems.

This option is not available when operating under the bootable media.

The option enables you to receive e-mail notifications about the backup task's successful completion, failure or need for interaction along with the full log of the task.

The preset is: **Disabled**.

To configure e-mail notification

1. Select the **Send e-mail notifications** check box to activate notifications.
2. In the **E-mail addresses** field, type the e-mail address to which notifications will be sent. You can enter several addresses separated by semicolons.
3. Under **Send notifications**, select the appropriate check boxes as follows:
 - **When backup completes successfully** – to send a notification when the backup task has completed successfully
 - **When backup fails** – to send a notification when the backup task has failed

The **When user interaction is required** check box is always selected.
4. For the e-mail message to include the log entries related to the backup, select the **Add full log to the notification** check box.
5. Click **Additional e-mail parameters**, to configure additional e-mail parameters as follows, then click **OK**:
 - **From** - type the e-mail address of the user from whom the message will be sent. If you leave this field empty, messages will be constructed as if they are from the destination address.
 - **Use encryption** – you can opt for encrypted connection to the mail server. SSL and TLS encryption types are available for selection.

- Some Internet service providers require authentication on the incoming mail server before being allowed to send something. If this is your case, select the **Log on to incoming mail server** check box to enable a POP server and to set up its settings:
 - **Incoming mail server (POP)** – enter the name of the POP server.
 - **Port** – set the port of the POP server. By default, the port is set to 110.
 - **User name** – enter the user name
 - **Password** – enter the password.
- Select the **Use the specified outgoing mail server** check box to enable an SMTP server and to set up its settings:
 - **Outgoing mail server (SMTP)** – enter the name of the SMTP server.
 - **Port** – set the port of the SMTP server. By default, the port is set to 25.
 - **User name** – enter the user name.
 - **Password** – enter the password.

Click **Send test e-mail message** to check if the settings are correct.

Messenger service (WinPopup)

This option is effective for Windows operating systems on the sending machine and only for Windows on the receiving machine.

This option is not available when operating under bootable media.

The option enables you to receive WinPopup notifications about the backup task's successful completion, failure or need for interaction.

The preset is: **Disabled**.

Before configuring WinPopup notifications, make sure the Messenger service is started on both the machine executing the task and the machine that will receive messages.

The Messenger service is not started by default in the Microsoft Windows Server 2003 family. Change the service Startup mode to Automatic and start the service.

To configure WinPopup notifications:

Select the Send WinPopup notifications check box.

In the Machine name field, enter the name of the machine to which notifications will be sent. Multiple names are not supported.

Under Send notifications, select the appropriate check boxes as follows:

- **When backup completes successfully** – to send notification when the backup operation is completed successfully
- **When backup fails** – to send notification when the backup operation is failed

The **When user interaction is required** check box – to send notification during the operation when user interaction is required – is always selected.

Click **Send test WinPopup message** to check if the settings are correct.

3.3.2.5 Event tracing

It is possible to duplicate log events of the recovery operations, performed on the managed machine, in the Application Event Log of Windows; or send the events to the specified SNMP managers.

Windows event log

This option is effective only in Windows operating systems.

This option is not available when operating under the bootable media.

This option defines whether the agent(s) operating on the managed machine have to log events of the recovery operations in the Application Event Log of Windows (to see this log, run **eventvwr.exe** or select **Control Panel > Administrative tools > Event Viewer**). You can filter the events to be logged.

The preset is: **Use the setting set in the Machine options.**

To select whether to log the recovery operations events in the Application Event Log of Windows:

Select one of the following:

- **Use the setting set in the Machine options** – to use the setting specified for the machine. For more information refer to Machine options.
- **Log the following event types** – to log events of the recovery operations in the Application Event Log. Specify the types of events to be logged:
 - **All events** – log all events (information, warnings and errors)
 - **Errors and warnings**
 - **Errors only**
- **Do not log** - to disable logging events of the recovery operations in the Application Event Log.

SNMP notifications

This option is effective for Windows operating systems.

This option is not available when operating under the bootable media.

The option defines whether the agent(s) operating on the managed machine have to send the log events to the specified Simple Network Management Protocol (SNMP) managers. You can choose the types of events to be sent.

You can override the settings set here, exclusively for the events that occur during backup or during recovery, in the Default backup and recovery options (p. 31). In this case, the settings set here will be effective for operations other than backup and recovery, such as archive validation or cleanup.

You can further override the settings set in the default backup and recovery options, when creating a backup plan or a recovery task. The settings you obtain in this case will be plan-specific or task-specific.

For detailed information about using SNMP with Acronis Backup & Recovery Server OEM, please see "Support for SNMP".

The preset is: **Disabled.**

To set up sending SNMP messages

Select the Send messages to SNMP server check box.

Specify the appropriate options as follows:

Types of events to send – choose the types of events: All events, Errors and warnings, or Errors only.

Server name/IP – type the name or IP address of the host running the SNMP management application, the messages will be sent to.

Community – type the name of the SNMP community to which both the host running SNMP management application and the sending machine belong. The typical community is "public".

To disable sending SNMP messages, clear the Send messages to SNMP server check box.

The messages are sent over UDP.

The next section contains additional information about Setting up SNMP services on the receiving machine.

3.3.2.6 Error handling

These options are effective for Windows operating systems and bootable media.

These options enable you to specify how to handle errors that might occur during recovery.

Do not show messages and dialogs while processing (silent mode)

The preset is: **Disabled**.

With the silent mode enabled, the program will automatically handle situations requiring user interaction where possible. If an operation cannot continue without user interaction, it will fail. Details of the operation, including errors, if any, can be found in the operation log.

Re-attempt, if an error occurs

The preset is: **Enabled**. **Number of attempts: 5**. **Interval between attempts: 30 seconds**.

When a recoverable error occurs, the program re-attempts to perform the unsuccessful operation. You can set the time interval and the number of attempts. The attempts will be stopped as soon as the operation succeeds OR the specified number of attempts is performed, depending on which comes first.

For example, if the network location becomes unavailable or not reachable, the program will attempt to reach the location every 30 seconds, but no more than 5 times. The attempts will be stopped as soon as the connection is resumed OR the specified number of attempts is performed, depending on which comes first.

3.3.2.7 Additional settings

Specify the additional settings for the recovery operation by selecting or clearing the following check boxes.

Set current date and time for recovered files

This option is effective only when recovering files.

The preset is **Enabled**.

This option defines whether to recover the files' date and time from the archive or assign the files the current date and time.

Validate backup before recovery

The preset is **Disabled**.

This option defines whether to validate a backup to ensure that the backup is not corrupted, before data is recovered from it.

Check file system after recovery

This option is effective only when recovering disks or volumes.

When operating under bootable media, this option is not effective for the NTFS file system.

The preset is **Disabled**.

This option defines whether to check the integrity of the file system after a disk or volume recovery.

Restart machine automatically if it is required for recovery

This option is effective when recovery takes place on a machine running an operating system.

The preset is **Disabled**.

The option defines whether to reboot the machine automatically if it is required for recovery. Such might be the case when a volume locked by the operating system has to be recovered.

Reboot machine after recovery

This option is effective when operating under bootable media.

The preset is **Disabled**.

This option enables booting the machine into the recovered operating system without user interaction.

Use FTP in Active mode

The preset is: **Disabled**.

Enable this option if the FTP server supports active mode and you want this mode to be used for file transfers.

4 Vaults

A vault is a location for storing backup archives. For ease of use and administration, a vault is associated with the archives' metadata. Referring to this metadata makes for fast and convenient operations with archives and backups stored in the vault.

A vault can be organized on a local or networked drive, detachable media.

There are no settings for limiting a vault size or number of backups in a vault. You can limit the size of each archive using cleanup, but the total size of archives stored in the vault is limited by the storage size only.

Why create vaults?

We recommend that you create a vault in each destination where you are going to store backup archives. This will ease your work as follows.

Quick access to the vault

You will not have to remember paths to the folders where the archives are stored. When creating a backup plan or a task that requires selection of an archive or an archive destination place, the list of vaults will be available for quick access without drilling down through the folders tree.

Easy archive management

A vault is available for access from the **Navigation** pane. Having selected the vault, you can browse the archives stored there and perform the following archive management operations:

- get a list of backups included in each archive
- recover data from a backup
- examine backup content
- validate all archives in the vault or individual archives or backups
- mount a volume backup to copy files from the backup to a physical disk
- safely delete archives and backups from the archives.

Creating vaults is highly recommended but is not obligatory. You may choose not to use the shortcuts and always specify the full path to the archive vault. All of the above operations except for archive and backup deletion can be performed without creating vaults.

The operation of creating a vault results in adding the vault name to the **Vaults** section of the **Navigation** pane.

Personal vaults

A vault is called personal if it was created using direct connection of the console to a managed machine. Personal vaults are specific for each managed machine.

Way of working with the "Vaults" view

 **Vaults** (on the navigation pane) - top element of the vaults tree. Click this item to display groups of personal vaults.

 **Personal**. This group is available when the console is connected to a managed machine. Expand this group to display a list of personal vaults created on the managed machine.

Click any personal vault in the vaults tree to open the detailed view of this vault and to take actions on the vault, archives and backups stored in there.

4.1 Personal vaults

A vault is called personal if it was created using direct connection of the console to a managed machine. Personal vaults are specific for each managed machine. Personal vaults are visible to any user that can log on to the system. A user's right to back up to a personal vault is defined by the user's permission for the folder or device where the vault is located.

A personal vault can be organized on detachable or removable media.

Personal vaults can be used by local backup plans or local tasks.

Sharing a personal vault

Multiple machines can refer to the same physical location, say, to the same shared folder, but each of the machines has its own shortcut in the **Vaults** tree. Users that back up to a shared folder can see and manage each other's archives according to their access permissions for that folder. To ease archive identification, the **Personal vault** view has the **Owner** column that displays the owner of each archive. To find out more about the owner concept see [Owners and credentials](#).

Metadata

The **.meta** folder is created during backup in every personal vault. This folder contains additional information about archives and backups stored in the vault, such as archive owners or the machine name. If you accidentally delete the **.meta** folder, it will be automatically recreated next time you access the vault. But some information like owner names and machine names may be lost.

4.1.1 Working with the "Personal vault" view

This section briefly describes the main elements of the **Personal vault** view, and suggests the ways to work with them.

Vault toolbar

The toolbar contains operational buttons that let you perform operations with the selected personal vault. See the [Actions on personal vaults](#) section for details.

Pie chart with legend

The **pie chart** lets you estimate the vault's load: it shows the proportion of the vault's free space and occupied space.

 - free space: space on the storage device, where the vault is located. For example, if the vault is located on a hard disk, the vault free space is free space of the appropriate volume.

 - occupied space: total size of backup archives and their metadata, if it is located in the vault. Other files that may be put to this folder by a user, are not counted.

The **legend** displays the following information about the vault:

- full path to the vault
- total number of archives and backups stored in the vault
- the ratio of the occupied space to the original data size.

Vault content

The Vault content section contains the archives table and toolbar. The archives table displays archives and backups that are stored in the vault. Use the archives toolbar to perform actions on the selected archives and backups. The list of backups is expanded by clicking the "plus" sign to the left of the archive's name. All the archives are grouped by type on the following tabs:

- The Disk archives tab lists all the archives that contain disk or volume backups (images).

Related sections:

[Operations with archives stored in a vault](#)

[Operations with backups](#)

[Filtering and sorting archives \(p. 59\)](#)

Bars of the "Actions and tools" pane

- **[Vault Name]** The **Actions** bar is available when clicking the vault in the vaults tree. Duplicates actions of the vault's toolbar.
- **[Archive Name]** The **Actions** bar is available when you select an archive in the archives table. Duplicates actions of the archives toolbar.
- **[Backup Name]** The **Actions** bar is available when you expand the archive and click on any of its backups. Duplicates actions of the archives toolbar.

4.1.2 Actions on personal vaults

To perform any operation (except for creation) with a vault, you must select it first.

All the operations described below are performed by clicking the corresponding buttons on the toolbar. These operations can be also accessed from the **[Vault name] actions** bar (on the **Actions and Tools** pane) and from the **[Vault name] actions** item of the main menu respectively.

The following is a guideline for you to perform operations with personal vaults.

To	Do
Create a personal vault	Click  Create . The procedure of creating personal vaults is described in-depth in the Creating a personal vault (p. 57) section.
Edit a vault	1. Select the vault. 2. Click  Edit . The Edit personal vault page lets you edit the vault's name and information in the Comments field.
Change user account for accessing a vault	Click Change user . In the appearing dialog box, provide the credentials required for accessing the vault.
Explore a vault's content	Click  Explore . In the appearing Explorer window, examine the selected vault's content.
Validate a vault	Click  Validate . You will be taken to the Validation (p. 92) page, where this vault is already pre-selected as a source. The vault validation checks all the archives stored in the vault.
Delete a vault	Click  Delete . The deleting operation actually removes only a shortcut to the folder from the Vaults view. The folder itself remains untouched. You have the option to keep or delete archives contained in the folder.
Refresh vault table information	Click  Refresh . While you are reviewing the vault content, archives can be added to the vault, deleted or modified. Click Refresh to update the vault information with the most recent changes.

4.1.2.1 Creating a personal vault

To create a personal vault

1. In the **Name** field, type a name for the vault being created.
2. [Optional] In the **Comments** field, add a description of the vault.
3. In the **Path** field, click **Change...**
In the opened **Personal Vault Path** window, specify a path to the folder that will be used as the vault. A personal vault can be organized on detachable or removable media, on a network share, or on FTP.
4. Click **OK**. As a result, the created vault appears in the **Personal** group of the vaults tree.

4.1.2.2 Merging and moving personal vaults

What if I need to move the existing vault from one place to another?

Proceed as follows

1. Make sure that none of the backup plans uses the existing vault while moving files, or temporarily disable (p. 69) schedules of the given plans.
2. Move the vault folder with all its archives to a new place manually by means of a third-party file manager.
3. Create a new vault.
4. Edit the backup plans and tasks: redirect their destination to the new vault.
5. Delete the old vault.

How can I merge two vaults?

Suppose you have two vaults *A* and *B* in use. Both vaults are used by backup plans. You decide to leave only vault *B*, moving all the archives from vault *A* there.

To do this, proceed as follows

1. Make sure that none of the backup plans uses vault *A* while merging, or temporarily disable (p. 69) schedules of the given plans.
2. Move the archives to vault *B* manually by means of a third-party file manager.
3. Edit the backup plans that use vault *A*: redirect their destination to vault *B*.
4. In the vaults tree, select vault *B* to check whether the archives are displayed. If not, click **Refresh**.
5. Delete vault *A*.

4.2 Common operations

4.2.1 Operations with archives stored in a vault

To perform any operation with an archive, you have to select it first. If the archive is protected with a password, you will be asked to provide it.

All the operations described below are performed by clicking the corresponding buttons on the toolbar. These operations can be also accessed from the **[Archive name] actions** bar (on the **Actions and tools** pane) and from the **[Archive name] actions** item of the main menu respectively.

The following is a guideline for you to perform operations with archives stored in a vault.

To	Do
----	----

Validate an archive	Click  Validate. The Validation (p. 92) page will be opened with the pre-selected archive as a source. Validation of an archive will check all the archive's backups.
Delete a single archive or multiple archives	1. Select the archive or one of the archives you want to delete. 2. Click  Delete. The program duplicates your selection in the Backups deletion window that has check boxes for each archive and each backup. Review the selection and correct if need be (select the check boxes for the desired archives), then confirm the deletion.
Delete all archives in the vault	Please be aware that if filters have been applied to the vaults list, you see only a part of the vault content. Be sure that the vault does not contain archives you need to retain before starting the operation. Click  Delete all. The program duplicates your selection in the new window that has check boxes for each archive and each backup. Review the selection and correct if need be, then confirm the deletion.

4.2.2 Operations with backups

To perform any operation with a backup, you have to select it first. To select a backup, expand the archive, then click the backup. If the archive is protected with a password, you will be asked to provide it.

All the operations described below are performed by clicking the corresponding buttons on the toolbar. These operations can be also accessed from the '**[Backup name]**' **actions** bar (on the **Actions and tools** pane) and from the '**[Backup name]**' **actions** item of the main menu.

The following is a guideline for you to perform operations with backups.

To	Do
View backup content in a separate window	Click  View content. In the Backup Content window, examine the backup content.
Recover	Click  Recover. The Recover data page will be opened with the pre-selected backup as a source.
Validate a backup	Click  Validate. The Validation (p. 92) page will be opened with the pre-selected backup as a source. Validation of a file backup imitates recovering of all files from the backup to a dummy destination. Validation of a disk backup calculates a checksum for every data block saved in the backup.
Delete a single or multiple backups	Select one of the backups you want to delete, then click  Delete. The program duplicates your selection in the Backups deletion window that has check boxes for each archive and each backup. Review the selection and correct if need be (select the check boxes for the desired backups), then confirm the deletion.
Delete all archives and backups in the vault	Please be aware that if filters have been applied to the vaults list, you see only a part of the vault content. Be sure that the vault does not contain archives you need to retain before starting the operation.

	Click  Delete all. The program duplicates your selection in the Backups deletion window that has check boxes for each archive and each backup. Review the selection and correct if need be, then confirm the deletion.
--	---

4.2.3 Deleting archives and backups

The **Backups deletion** window displays the same tab as for the vaults view, but with check boxes for each archive and backup. The archive or backup you have chosen to delete has the check mark. Review the archive or backup that you have selected to delete. If you need to delete other archives and backups select the respective check boxes, then click **Delete selected** and confirm the deletion.

The filters in this window are from the archives list of the vault view. Thus, if some filters have been applied to the archives list, only the archives and backups corresponding to these filters are displayed here. To see all content, clean all the filter fields.

4.2.4 Filtering and sorting archives

The following is a guideline for you to filter and sort archives in the archives table.

To	Do
Sort backup archives by any column	Click the column's header to sort the archives in ascending order. Click it once again to sort the archives in descending order.
Filter archives by name, owner, or machine.	In the field below the corresponding column's header, type the archive name (the owner name, or the machine name). As a result, you will see the list of the archives, whose names (owner names, or machine names) fully or just partly coincide with the entered value.

Configuring the archives table

By default, the table has seven columns that are displayed, others are hidden. If required, you can hide the displayed columns and show hidden ones.

To show or hide columns

1. Right-click any column header to open the context menu. The menu items that are ticked off correspond to the column headers presented in the table.
2. Click the items you want to be displayed/hidden.

5 Direct management

This section covers operations that can be performed directly on a managed machine by using the direct console-agent connection.

5.1 Administering a managed machine

This section describes the views that are available through the navigation tree of the console connected to a managed machine, and explains how to work with each view.

5.1.1 Dashboard

Use the Dashboard to estimate at a glance whether the data is successfully protected on the machine. The dashboard shows the summary of Acronis Backup & Recovery Server OEM agent's activities and enables you to rapidly identify and resolve any issues.

Alerts

The alerts section draws your attention to issues that have occurred on the machine and offers you ways of fixing or examining them. The most critical issues are displayed on the top. If there are no alerts or warnings at the moment, the system displays "No alerts or warnings".

Types of alerts

The table below illustrates the types of messages you may observe.

	Description	Offer	Comment
	Failed tasks: X	Resolve	Resolve will open the Backup plans and Tasks view with failed tasks, where you can examine the reason of failure.
	Tasks that need interaction: X	Resolve	Each time a task needs human interaction, the Dashboard shows a message to inform you what action has to be performed (for example, insert new CD or Stop/Retry/Ignore on an error).
	Failed to check the license for the current edition. X day(s) remaining until the software stops working. Please make sure you have a valid license on Acronis License Server.	Connect	Acronis Backup & Recovery Server OEM agent connects to Acronis License Server at the start and then every 1–5 days (the default is 1 day), as specified by the agent configuration parameters. If the license check does not succeed for 1–60 days, as specified by the agent configuration parameters (the default is 30 days), the agent will stop working until there has been a successful last license check.
	Cannot check the license key for the current edition for X days. Either Acronis License Server was unavailable, or the license key data was corrupted. Check connectivity to the server and run Acronis License Server to manage licenses. Please make sure you have a valid license on Acronis License Server.	Connect	Acronis Backup & Recovery Server OEM is stopped. For the past X days, the agent was unable to check whether its license is available on Acronis License Server. This is probably due to the license server being unavailable. You may also want to ensure that the licenses are present on the license server, or that the license key data was not corrupted. After a successful license check the agent will start working.
	Trial version of product expires in X day(s) Please make sure you have a valid license on Acronis License Server.	Connect	Once the trial version of the product is installed, the program starts the countdown of days remaining until the trial period expires.
	Trial period is over. Start the installer and enter a full license key. Please make sure you have a	Connect	15 day trial period has expired. Enter a full license key.

	valid license on Acronis License Server.		
	Vaults with low free space: X	View vaults	View vaults will take you to the Vaults view where you can examine the vault size, free space, content and take the necessary steps to increase the free space.
	Bootable media was not created	Create now	To be able to recover an operating system when the machine fails to boot, you must: 1. Back up the system volume (and the boot volume, if it is different) 2. Create at least one bootable media. Create now will launch the Bootable Media Builder (p. 151).
	No backups have been created for X days	Back up now	The Dashboard warns you that no data was backed up on the machine for a relatively long period of time. Back up now will take you to Create a Backup Plan page where you can instantly configure and run the backup operation. To configure the time interval that is considered as critical, select Options > Console options > Time-based alerts .
	Not connected to management server for X days	View the machines	This type of message can appear on a machine that is registered on a management server. The Dashboard warns you that the connection might be lost or the server might be unavailable and the machine is not centrally managed as a result.

Activities

The calendar lets you explore the history of the Acronis Backup & Recovery Server OEM agent's activities on the machine. Right-click on any highlighted date and select **View log** to see the list of log entries filtered by date.

On the **View** section (at the right of the calendar), you can select the activities to highlight depending on the presence and severity of the errors.

	How it is determined
Errors	Highlight the date in red if at least one "Error" entry appeared in the log on this date.
Warnings	Highlight the date in yellow if no "Error" entries appeared and at least one "Warning" entry appeared in the log on this date.
Information	Highlight the date in green if only "Information" log entries appeared on this date (normal activity.)

The **Select current date** link focuses selection to the current date.

System view

Shows summarized statistics of backup plans, tasks, and brief information on the last backup. Click the items in this section to obtain the relevant information. This will take you to the **Backup plans and tasks** (p. 62) view with pre-filtered plans or tasks. For instance, if you click **Local** under **Backup plans**, the **Backup plans and tasks** view will be opened with backup plans filtered by the **Local** origin.

5.1.1.1 Tasks need interaction

This window accumulates all the tasks that require user interaction in one place. It enables you to specify your decision, such as to confirm reboot or to retry after freeing-up the disk space, on each of the tasks. Until at least one task requires interaction, you can open this window at any time from the managed machine's **Dashboard** (p. 60).

If you select the check box for the **Do not show this window when tasks require interaction. I will see this information in the tasks' details and dashboard.** parameter, the tasks will be displayed on the **Dashboard** among other alerts and warnings.

Alternatively, you can review the task execution states in the **Backup plans and tasks** (p. 62) view and specify your decision on each task in the **Information** panel (or in the **Task details** window).

5.1.2 Backup plans and tasks

The **Backup plans and tasks** view keeps you informed of data protection on a given machine. It lets you monitor and manage backup plans and tasks.

A backup plan is a set of rules that specify how the given data will be protected on a given machine. Physically, a backup plan is a bundle of tasks configured for execution on a managed machine. To find out what a backup plan is currently doing on the machine, check the backup plan execution state. A backup plan state is a cumulative state of the plan's tasks. The status of a backup plan helps you to estimate whether the data is successfully protected.

A task is a set of sequential actions to be performed on a machine when a certain time comes or certain event occurs. To keep track of a task's current progress, examine its state (p. 63). Check a task status to ascertain the result of a task.

Way of working

- Use filters to display the desired backup plans (tasks) in the backup plans table. By default, the table displays all the plans of the managed machine sorted by name. You can also hide the unneeded columns and show the hidden ones. See the Filtering and sorting backup plans and tasks (p. 68) section for details.
- In the backup table, select the backup plan (task).
- Use the toolbar's buttons to take an action on the selected plan (task). See the Actions on backup plans and tasks section for details. You can run, edit, stop and delete the created plans and tasks.
- Use the **Information** panel to review detailed information on the selected plan (task). The panel is collapsed by default. To expand the panel, click the  chevron. The content of the panel is also duplicated in the **Plan details** and **Task details** windows respectively.

5.1.2.1 Understanding states and statuses

Backup plan execution states

A backup plan can be in one of the following execution states: **Idle**; **Waiting**; **Running**; **Stopping**; **Need Interaction**.

Plan states names are the same as task state names because a plan state is a cumulative state of the plan's tasks.

State	How it is determined	How to handle
-------	----------------------	---------------

1	Need interaction	At least one task needs user interaction. Otherwise, see 2.	Identify the tasks that need interaction (the program will display what action is needed) -> Stop the tasks or enable the tasks to run (change media; provide additional space on the vault; ignore the read error).
2	Running	At least one task is running. Otherwise, see 3.	No action is required.
3	Waiting	At least one task is waiting. Otherwise, see 4.	Waiting for condition. This situation is quite normal, but delaying a backup for too long is risky. The solution may be to set the maximum delay or force the condition (tell the user to log off, enable the required network connection.) Waiting while another task locks the necessary resources. A one-time waiting case may occur when a task start is delayed or a task run lasts much longer than usual for some particular reason and this way prevents another task from starting. This situation is resolved automatically when the obstructing task comes to an end. Consider stopping a task if it hangs for too long to enable the next task to start. Persistent task overlapping may result from an incorrectly scheduled plan or plans. It makes sense to edit the plan in this case.
4	Stopping	At least one task is stopping. Otherwise, see 5.	No action is required.
5	Idle	All the tasks are idle.	No action is required.

Task states

A task can be in one of the following states: **Idle**; **Waiting**; **Running**; **Stopping**; **Need interaction**. The initial task state is **Idle**.

Once the task is started manually or the event specified by the schedule occurs, the task enters either the **Running** state or the **Waiting** state.

Running

A task changes to the **Running** state when the event specified by the schedule occurs AND all the conditions set in the backup plan are met AND no other task that locks the necessary resources is running. In this case, nothing prevents the task from running.

Waiting

A task changes to the **Waiting** state when the task is about to start, but another task using the same resources is already running. In particular, more than one backup or recovery task cannot run simultaneously on a machine. A backup task and a recovery task also cannot run simultaneously. Once the other task unlocks the resource, the waiting task enters the **Running** state.

A task may also change to the **Waiting** state when the event specified by the schedule occurs but the condition set in the backup plan is not met. See Task start conditions for details.

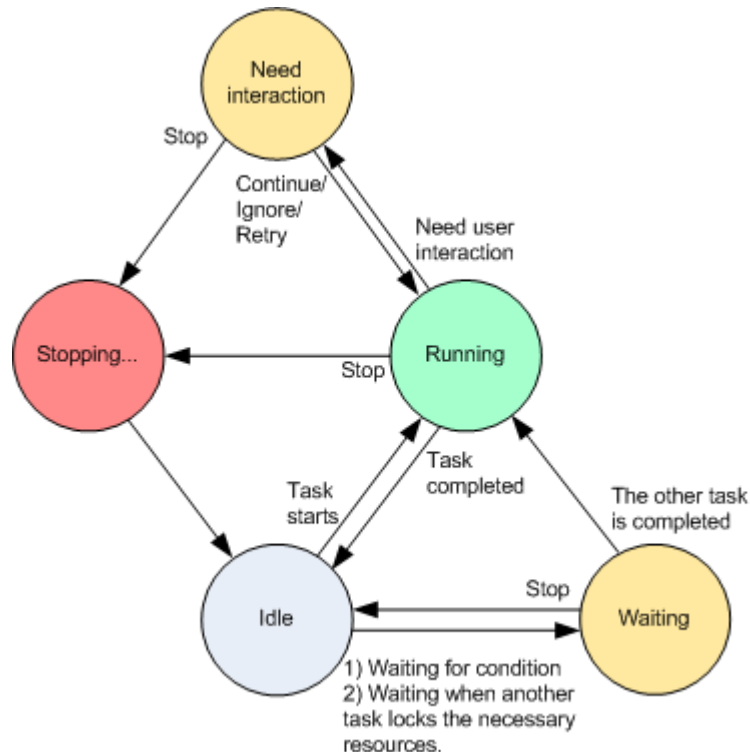
Need interaction

Any running task can put itself into the **Need interaction** state when it needs human interaction such as changing media or ignoring a read error. The next state may be **Stopping** (if the user chooses to stop the task) or **Running** (on selecting Ignore/Retry or another action, such as Reboot, that can put the task to the **Running** state.)

Stopping

The user can stop a running task or a task that needs interaction. The task changes to the **Stopping** state and then to the **Idle** state. A waiting task can also be stopped. In this case, since the task is not running, "stop" means removing it from the queue .

Task state diagram



Task statuses

A task can have one of the following statuses: **Error**; **Warning**; **OK**.

A task status is derived from the result of the last run of the task.

	Status	How it is determined	How to handle
1	Error	Last result is "Failed"	Identify the failed task -> Check the task log to find out the reason of the failure, then do one or more of the following: - Remove the reason of the failure -> [optionally] Start the failed task manually - Edit the failed task to prevent its future failure - Edit the local plan to prevent its future failure in case a local plan has failed
2	Warning	Last result is "Succeeded with warning"	View the log to read the warnings -> [optionally] Perform actions to prevent the future warnings or failure.
3	OK	Last result is	No action is required.

		"Succeeded", "-", or "Stopped"	The "-" state means that the task has never been started or has been started, but has not finished yet and so its result is not available.
--	--	--------------------------------	--

5.1.2.2 Working with backup plans and tasks

Actions on backup plans and tasks

The following is a guideline for you to perform operations with backup plans and tasks.

To	Do
Create a new backup plan, or a task	Click  New, then select one of the following: - Backup plan - Recovery task - Validation task (p. 92)
View details of a plan/task	Backup plan Click  View details. In the Plan Details window, review the plan details. Task Click  View details. In the Task Details window, review the task details.
View plan's/task's log	Backup plan Click  View log. You will be taken to the Log (p. 71) view containing the list of the plan-related log entries. Task Click  View log. You will be taken to the Log (p. 71) view containing the list of the task-related log entries.
Run a plan/task	Backup plan Click  Run. In the Run Backup Plan (p. 69) window, select the task you need to be run. Running the backup plan starts the selected task of that plan immediately in spite of its schedule and conditions. <i>Why can't I run the backup plan?</i> Do not have the appropriate privilege Without the Administrator privileges on the machine, a user cannot run plans owned by other users. Task Click  Run. The task will be executed immediately in spite of its schedule and conditions.

Stop a plan/task	<u>Backup plan</u> Click  Stop. Stopping the running backup plan stops all its tasks. Thus, all the task operations will be aborted. <u>Task</u> Click  Stop. <i>What will happen if I stop the task?</i> Generally, stopping the task aborts its operation (backup, recovery, validation, conversion, migration). The task enters the Stopping state first, then becomes Idle. The task schedule, if created, remains valid. To complete the operation you will have to run the task over again. ■ recovery task (from the disk backup): The target volume will be deleted and its space unallocated – you will get the same result if the recovery is unsuccessful. To recover the "lost" volume, you will have to run the task once again. ■ recovery task (from the file backup): The aborted operation may cause changes in the destination folder. Some files may be recovered, but some not, depending on the moment when you stopped the task. To recover all the files, you will have to run the task once again.
------------------	---

Edit a plan/task

Backup plan

Click  **Edit**.

Backup plan editing is performed in the same way as creation.

In all other cases the scheme can be changed, and should continue to operate as if existing archives were created by a new scheme. For empty archives all changes are possible.

Why can't I edit the backup plan?

- The backup plan is currently running.
Editing of the currently running backup plan is impossible.
- Do not have the appropriate privilege
Without the Administrator privileges on the machine, a user cannot edit plans owned by other users.

Task

Click  **Edit**.

Why can't I edit the task?

- Task belongs to a backup plan
- Only tasks that do not belong to a backup plan, such as a recovery task, can be modified by direct editing. When you need to modify a task belonging to a local backup plan, edit the backup plan.
- Do not have the appropriate privilege
Without the Administrator privileges on the machine, a user cannot modify tasks owned by other users.

Delete a plan/task	<u>Backup plan</u> Click  Delete. <i>What will happen if I delete the backup plan?</i> The plan's deletion deletes all its tasks. <i>Why can't I delete the backup plan?</i> ▪ The backup plan is in the "Running" state A backup plan cannot be deleted, if at least one of its tasks is running. ▪ Do not have the appropriate privilege Without the Administrator's privileges on the machine, a user cannot delete plans owned by other users. <u>Task</u> Click  Delete. <i>Why can't I delete the task?</i> ▪ Task belongs to a backup plan A task belonging to a backup plan cannot be deleted separately from the plan. Edit the plan to remove the task or delete the entire plan. ▪ Do not have the appropriate privilege Without the Administrator privileges on the machine, a user cannot delete tasks owned by other users.
Refresh table	Click  Refresh. The management console will update the list of backup plans and tasks existing on the machine with the most recent information. Though the list is refreshed automatically based on events, the data may not be retrieved immediately from the managed machine, due to some latency. Manual refresh guarantees that the most recent data is displayed.

Filtering and sorting backup plans and tasks

To	Do
Sort backup plans and tasks by: name, state, status, type, origin, etc.	Click the column's header to sort the backup plans and tasks in ascending order. Click it once again to sort the plans and tasks in descending order.
Filter plans/tasks by name or owner.	Type a plan's/task's name or an owner's name in the field below the corresponding header name. As a result you will see the list of tasks, whose names/owners' names fully or just partly coincide with the entered value.
Filter plans and tasks by state, status, type, origin, last result, schedule.	In the field below the corresponding header, select the required value from the list.

Configuring backup plans and the tasks table

By default, the table has six columns that are displayed, others are hidden. If required, you can hide the displayed columns and show hidden ones.

To show or hide columns

1. Right-click any column header to open the context menu. The menu items that are ticked off correspond to the column headers presented in the table.
2. Click the items you want to be displayed/hidden.

Run backup plan

The backup plan is considered as running if at least one of its tasks is running. The **Run backup plan** window lets you run the task of the selected backup plan manually, in spite of its schedule.

To run a task of the selected backup plan

1. Select the task of the backup plan you need to run. To make certain of your selection, check the task information gathered in tabs at the bottom of the window. This information is also duplicated in the **Task details** window.
2. Click **OK**.

Temporarily disabling a backup plan

Temporarily disabling a backup plan is needed when moving archives from one vault to another by means of the third-party file manager.

Applies to backup plans that use custom backup schemes only.

To disable a backup plan

1. Click  **Edit**.
2. Enter the backup scheme scheduling option and disable the schedule for the desired period by changing the **Start date** and/or **End date** parameters.

Task details

The **Task details** window (also duplicated on the **Information** panel) aggregates all information on the selected task.

When a task requires user interaction, a message and action buttons appear above the tabs. The message contains a brief description of the problem. The buttons allow you to retry or stop the task or the backup plan.

Types of tasks

The following table summarizes all types of tasks that exist in Acronis Backup & Recovery Server OEM. The actual types of tasks you might observe depend on the product edition and the product component the console is connected to.

Task name	Description
Backup (disk)	Backing up disks and volumes
Recovery (disk)	Disk backup recovery
Recovery (file)	File and folder recovery
Recovery (volume)	Recovery of volumes from a disk backup
Recovery (MBR)	Master boot record recovery
Validation (archive)	Validation of a single archive

Validation (backup)	Validation of backups
Validation (vault)	Validation of all archives stored in a vault
Cleanup	Deleting backups from a backup archive in accordance with retention rules
Disk management	Disk management operations

Depending on the type of task and whether it is running or not, a combination of the following tabs will appear:

Task

The **Task** tab is common for all types of tasks. It provides general information on the selected task.

Archive

The **Archive** tab is available for backup, archive validation and cleanup tasks.

Provides information on the archive: its name, type, size, where it is stored, etc.

Backup

Settings

The **Settings** tab displays information on scheduling and the options changed against the default values.

Progress

The **Progress** tab is available while the task is running. It is common for all types of tasks. The tab provides information about task progress, elapsed time and other parameters.

Backup plan details

The **Backup plan details** window (also duplicated on the **Information** panel) aggregates in four tabs all the information on the selected backup plan.

The respective message will appear at the top of the tabs, if one of the plan's tasks requires user interaction. It contains a brief description of the problem and action buttons that let you select the appropriate action or stop the plan.

Backup plan

Source

The **Source** tab provides the following information on the data selected for backup:

- **Source type** - the type of data selected for backing up.
- **Items to back up** - items selected to back up and their size.

Destination

The **Destination** tab provides the following information:

- **Location** - name of the vault or path to the folder, where the archive is stored.
- **Archive name** - name of the archive.
- **Archive comments** - comments on the archive (if provided).

Settings

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

- **Backup scheme** - the selected backup scheme and all its settings with schedules.
- **Validation** (if selected) - events before or after which the validation is performed, and validation schedule.
- **Backup options** - backup options changed against the default values.

5.1.3 Log

The Log stores the history of operations performed by Acronis Backup & Recovery Server OEM on the machine, or actions a user takes on the machine using the program. For instance, when a user edits a task, the respective entry is added to the log. When the program executes a task, it adds multiple entries. With the log, you can examine operations, results of tasks' execution including reasons for failure, if any.

Way of working with log entries

- Use filters to display the desired log entries. You can also hide the unneeded columns and show the hidden ones. See the Filtering and sorting log entries (p. 72) section for details.
- In the log table, select the log entry (or log entries) to take action on it. See the Actions on log entries section for details.
- Use the **Information** panel to review detailed information on the selected log entry. The panel is collapsed by default. To expand the panel, click the  chevron. The content of the panel is also duplicated in the **Log entry details** (p. 73) window.

Opening the Log with pre-filtered log entries

Having selected items in other administration views (**Dashboard**, **Backup plans and tasks**), you can open the **Log** view with pre-filtered log entries for the item in question. Thus, you do not have to configure filters in the log table yourself.

View	Action
Dashboard	In the calendar, right-click on any highlighted date, and then select  View log . The Log view appears with the list of log entries already filtered by the date in question.
Backup plans and tasks	Select a backup plan or a task, and then click  View log . The Log view will display a list of the log entries related to the selected plan or task.

5.1.3.1 Actions on log entries

All the operations described below are performed by clicking the corresponding items on the log **toolbar**. All these operations can also be performed with the context menu (by right-clicking the log entry), or with the **Log actions** bar (on the **Actions and tools** pane).

The following is a guideline for you to perform actions on log entries.

To	Do
Select a single log entry	Click on it.
Select multiple log entries	▪ <i>non-contiguous</i>: hold down CTRL and click the log entries one by one ▪ <i>contiguous</i>: select a single log entry, then hold down SHIFT and click another

	entry. All the entries between the first and last selections will be selected too.
View a log entry's details	1. Select a log entry. 2. Do one of the following ▪ Click  View Details. The log entry's details will be displayed in a separate window. ▪ Expand the Information panel, by clicking the chevron.
Save the selected log entries to a file	1. Select a single log entry or multiple log entries. 2. Click  Save Selected to File. 3. In the opened window, specify a path and a name for the file. Please note, logs can be saved only to a network share.
Save all the log entries to a file	1. Make sure, that the filters are not set. 2. Click  Save All to File. 3. In the opened window, specify a path and a name for the file. Please note, logs can be saved only to a network share.
Save all the filtered log entries to a file	1. Set filters to get a list of the log entries that satisfy the filtering criteria. 2. Click  Save All to File. 3. In the opened window, specify a path and a name for the file. Please note, logs can be saved only to a network share. As a result, the log entries of that list will be saved.
Delete all the log entries	Click  Clear Log. All the log entries will be deleted from the log, and a new log entry will be created. It will contain information about who deleted the entries and when.

5.1.3.2 Filtering and sorting log entries

The following is a guideline for you to filter and sort log entries.

To	Do
Display log entries for a given time period	1. In the From field, select the date starting from which to display the log entries. 2. In the To field, select the date up to which to display the log entries.
Filter log entries by type	Press or release the following toolbar buttons:  to filter error messages  to filter warning messages  to filter information messages
Filter log entries by the original backup plan or managed entity type	Under the Backup plan (or Managed entity type) column header, select the backup plan or the type of managed entity from the list.
Filter log entries by task, managed entity, machine, code, owner	Type the required value (task name, machine name, owner name, etc.) in the field below the respective column header. As a result you will see that the list of log entries fully or just partly coincide with the

	entered value.
Sort log entries by date and time	Click the column's header to sort the log entries in ascending order. Click it once again to sort the log entries in descending order.

Configuring the log table

By default, the table has seven columns that are displayed, others are hidden. If required, you can hide the shown columns and show the hidden ones.

To show or hide columns

1. Right-click any column header to open the context menu. The menu items that are ticked off correspond to the column headers presented in the table.
2. Click the items you want to be displayed/hidden.

5.1.3.3 Log entry details

Displays detailed information on the log entry you have selected and lets you copy the details to the clipboard.

To copy the details, click the **Copy to clipboard** button.

Log entry data fields

A local log entry contains the following data fields:

- **Type** - type of event (Error; Warning; Information)
- **Date** - date and time of the event occurrence
- **Backup plan** - the backup plan the event relates to (if any)
- **Task** - the task the event relates to (if any)
- **Code** - the program code of the event. Every type of event in the program has its own code. A code is an integer number that may be used by Acronis support service to solve the problem.
- **Module** - number of the program module where the event has occurred. It is an integer number that may be used by Acronis support service to solve the problem.
- **Owner** - user name of the backup plan owner (only under operating system)
- **Message** - a text description of the event.

The log entry's details that you copy will have the appearance as follows:

```
-----Log Entry Details-----
Type:                               Information
Date and time:                      DD.MM.YYYY HH:MM:SS
Backup plan:                        Backup plan name
Task:                               Task name
Message:                            Description of the operation
Code:                               12(3x45678A)
Module:                             Module name
Owner:                              Owner of the plan
-----
```

Date and time presentation varies depending on your locale settings.

5.2 Creating a backup plan

Before creating your first backup plan, please familiarize yourself with the basic concepts used in Acronis Backup & Recovery Server OEM.

To create a backup plan, perform the following steps.

General

Plan name

[Optional] Enter a unique name for the backup plan. A conscious name lets you identify the plan among others.

Plan's credentials (p. 75)

[Optional] The backup plan will run on behalf of the user who is creating the plan. You can change the plan account credentials if necessary. To access this option, select the **Advanced view** check box .

Comments

[Optional] Type a description of the backup plan. To access this option, select the **Advanced view** check box.

What to backup

Source type

Select the type of data to back up. The type of data depends on the agents installed on the machine.

Items to backup (p. 76)

Specify the data items to back up. A list of items to backup depends on the data type, specified previously.

Access credentials (p. 76)

[Optional] Provide credentials for the source data if the plan's account does not have access permissions to the data. To access this option, select the **Advanced view** check box .

Where to back up

Archive

Specify path to the location, where the backup archive will be stored, and the archive name. It is advisable that the archive name be unique within the location. The default archive name is Archive(N) where N is the sequence number of the archive in the location you have selected.

Access credentials

[Optional] Provide credentials for the location if the plan account does not have access permissions to the location. To access this option, select the **Advanced view** check box.

Archive comments

[Optional] Enter comments on the archive. To access this option, select the **Advanced view** check box.

How to back up

Backup scheme

Specify when and how often to back up your data; define for how long to keep the created backup archives in the selected location; set up schedule for the archive cleanup procedure. Create a custom backup scheme, or back up data once.

Archive validation

When to validate (p. 80)

[Optional] Define when and how often to perform validation and whether to validate the entire archive or the latest backup in the archive.

Backup options

Settings

[Optional] Configure parameters of the backup operation, such as pre/post backup commands, maximum network bandwidth allocated for the backup stream or the backup archive compression level. If you do nothing in this section, the default values will be used.

After any of the settings is changed against the default value, a new line that displays the newly set value appears. The setting status changes from **Default** to **Custom**. Should you modify the setting again, the line will display the new value unless the new value is the default one. When the default value is set, the line disappears and so you always see only the settings that differ from the default values in this section of the **Create backup plan** page.

To reset all the settings to the default values, click **Reset to default**.

5.2.1 Why is the program asking for the password?

A scheduled or postponed task has to run regardless of users being logged on. In case you have not explicitly specified the credentials, under which the task(s) will run, the program proposes using your account. Enter your password, specify another account or change the scheduled start to manual.

5.2.2 Backup plan's credentials

Provide the credentials for the account under which the plan's tasks will run.

To specify credentials

1. Select one of the following:

- **Run under the current user**

The tasks will run under the credentials with which the user who starts the tasks is logged on. If any of the tasks has to run on schedule, you will be asked for the current user's password on completing the plan creation.

- **Use the following credentials**

The tasks will always run under the credentials you specify, whether started manually or executed on schedule.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

2. Click **OK**.

To learn more about operations available depending on the user privileges, see the Users' privileges on a managed machine section.

5.2.3 Source type

Select the type of data you want to be backed up on the managed machine:

Disks/volumes

5.2.4 Items to back up

The items to backup depend on the source type selected previously.

5.2.4.1 Selecting disks and volumes

To specify disks/volumes to back up

1. Select the check boxes for the disks and/or volumes to back up. You can select a random set of disks and volumes.

If your operating system and its loader reside on different volumes, always include both volumes in the backup. The volumes must also be recovered together; otherwise there is a high risk that the operating system will not start.

2. [Optional] To create an exact copy of a disk or volume on a physical level, select the **Back up sector-by-sector** check box. The resulting backup will be equal in size to the disk being backed up (if the Compression level option is set to “None”). Use the sector-by-sector backup for backing up drives with unrecognized or unsupported file systems and other proprietary data formats.
3. Click **OK**.

What does a disk or volume backup store?

For supported file systems, with the sector-by-sector option turned off, a disk or volume backup stores only those sectors that contain data. This reduces the resulting backup size and speeds up the backup and recovery operations.

Windows

The swap file (pagefile.sys) and the file that keeps the RAM content when the machine goes into hibernation (hiberfil.sys) are not backed up. After recovery, the files will be re-created in the appropriate place with the zero size.

A volume backup stores all other files and folders of the selected volume independent of their attributes (including hidden and system files), the boot record, the file allocation table (FAT) if it exists, the root and the zero track of the hard disk with the master boot record (MBR). The boot code of GPT volumes is not backed up.

A disk backup stores all volumes of the selected disk (including hidden volumes such as the vendor's maintenance partitions) and the zero track with the master boot record.

5.2.5 Access credentials for source

Specify the credentials required for access to the data you are going to backup.

To specify credentials

1. Select one of the following:

- **Use the plan's credentials**

The program will access the source data using the credentials of the backup plan account specified in the General section.

- **Use the following credentials**

The program will access the source data using the credentials you specify. Use this option if the plan's account does not have access permissions to the data.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

2. Click **OK**.

5.2.6 Archive

Specify where the archive will be stored and the name of the archive.

1. Selecting the destination

Enter the full path to the destination in the **Path** field, or select the desired destination in the folders tree.

- To select a personal vault, expand the **Personal** group and click the appropriate vault.
- To select a local folder (CD/DVD drive, or locally attached tape device), expand the **Local folders** group and click the required folder.
- To select a network share, expand the **Network folders** group, select the required networked machine and then click the shared folder. If the network share requires access credentials, the program will ask for them.
- To select **FTP** or **SFTP** server, expand the corresponding group and click the appropriate folder on the server.

According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

2. Using the archives table

To assist you with choosing the right destination, the table displays the names of the archives contained in each location you select. While you are reviewing the location content, archives can be added, deleted or modified by another user or by the program itself according to scheduled operations. Use the **Refresh** button to refresh the list of archives.

3. Naming the new archive

Once you select the archive destination, the program generates a name for the new archive and displays it in the **Name** field. The name commonly looks like Archive(1). The generated name is unique within the selected location. If you are satisfied with the automatically generated name, click **OK**. Otherwise enter another unique name and click **OK**.

Backing up to an existing archive

You can configure the backup plan to back up to an existing archive. To do so, select the archive in the archives table or type the archive name in the **Name** field. If the archive is protected with a password, the program will ask for it in the pop-up window.

By selecting the existing archive, you are meddling in the area of another backup plan that uses the archive. This is not an issue if the other plan is discontinued, but in general you should follow the rule: "one backup plan - one archive". Doing the opposite will not prevent the program from functioning but is not practical or efficient, except for some specific cases.

Why two or more plans should not back up to the same archive

1. Backing up different sources to the same archive makes using the archive difficult from the usability standpoint. When it comes to recovery, every second counts, but you might be lost in the archive content.

Backup plans that operate with the same archive should back up the same data items (say, both plans back up volume C.)

Applying multiple retention rules to an archive makes the archive content in some way unpredictable. Since each of the rules will be applied to the entire archive, the backups belonging to one backup plan can be easily deleted along with the backups belonging to the other.

Normally, each complex backup plan should back up to its own archive.

5.2.7 Access credentials for archive location

Specify credentials required for access to the location where the backup archive will be stored. The user whose name is specified will be considered as the archive owner.

To specify credentials

1. Select one of the following:

- **Use the plan's credentials**

The program will access the source data using the credentials of the backup plan account specified in the General section.

- **Use the following credentials**

The program will access the source data using the credentials you specify. Use this option if the plan account does not have access permissions to the location. You might need to provide special credentials for a network share.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

Click **OK**.

Warning: According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

5.2.8 Backup schemes

Choose one of the available backup schemes:

- **Back up now** – to create a backup task for manual start and run the task immediately after its creation.
- **Back up later** – to create a backup task for manual start OR schedule one-time task execution in the future.
- **Simple** – to schedule when and how often to backup data and specify retention rules.
- **Custom** – to create a custom scheme, where you are free to set up a backup strategy in the way your enterprise needs it most: specify multiple schedules for different backup types, add conditions and specify the retention rules.

5.2.8.1 Back up now scheme

With the **Back up now** scheme, the full backup will be performed immediately, right after you click the **OK** button at the bottom of the page.

5.2.8.2 Back up later scheme

With the Back up later scheme, the backup will be performed only once, at the date and time you specify.

Specify the appropriate settings as follows

Backup type	Select the type of backup.
Date and time	Specify when to start the backup.
The task will be started manually	Select this check box, if you do not need to put the backup task on a schedule and wish to start it manually afterwards.

5.2.8.3 Simple scheme

With the simple backup scheme you just schedule when and how often to back up data and set the retention rule.

To set up the simple backup scheme, specify the appropriate settings as follows.

Backup	Set up the backup schedule - when and how often to back up the data. To learn more about setting up the schedule, see the Scheduling section.
Retention rule	With the simple scheme, only one retention rule is available. Set the retention period for the backups.

5.2.8.4 Custom backup scheme

At a glance

- Custom schedule and conditions for backups of each type
- Custom schedule and retention rules

Parameters

Parameter	Meaning
Full backup	Specifies on what schedule and under which conditions to perform a full backup. For example, the full backup can be set up to run every Sunday at 1:00 AM as soon as all users are logged off.
Clean up archive	Specifies how to get rid of old backups: either to apply retention rules regularly or clean up the archive during a backup when the destination location runs out of space. By default, the retention rules are not specified, which means older backups will not be deleted automatically. Using retention rules Specify the retention rules and when to apply them. This setting is recommended for backup destinations such as shared folders. When there is insufficient space while backing up The archive will be cleaned up only during backup and only if there is not enough space to create a new backup. In this case, the program will act as follows:

	▪ Delete the oldest full backup ▪ If there is only one full backup left and a full backup is in progress, then delete the last full backup This setting is recommended when backing up to a USB drive. This setting is not applicable to managed vaults. This setting enables deletion of the last backup in the archive, in case your storage device cannot accommodate more than one backup. However, you might end up with no backups if the program is not able to create the new backup for some reason.
Apply the rules (only if the retention rules are set)	Specifies when to apply the retention rules. For example, the cleanup procedure can be set up to run after each backup, and also on schedule. This option is available only if you have set at least one retention rule in Retention rules.
Cleanup schedule (only if On schedule is selected)	Specifies a schedule for archive cleanup. For example, the cleanup can be scheduled to start on the last day of each month. This option is available only if you selected On schedule in Apply the rules.

Examples

Weekly full backup

The following scheme yields a full backup performed every Friday night.

Full backup: Schedule: Weekly, every Friday, at 10:00 PM

Here, all parameters except **Schedule** in **Full backup** are left empty. All backups in the archive are kept indefinitely (no archive cleanup is performed).

5.2.9 Archive validation

Set up the validation task to check if the backed up data is recoverable. If the backup could not pass the validation successfully, the validation task fails and the backup plan gets the Error status.

To set up validation, specify the following parameters

1. **When to validate** – select when to perform the validation. As the validation is a resource-intensive operation, it makes sense to **schedule** the validation to the managed machine's off-peak period. On the other hand, if the validation is a major part of your data protection strategy and you prefer to be immediately informed whether the backed up data is not corrupted and can be successfully recovered, think of starting the validation right after backup creation.
2. **What to validate** – select either to validate the entire archive or the latest backup in the archive. Validation of a file backup imitates recovery of all files from the backup to a dummy destination. Validation of a volume backup calculates a checksum for every data block saved in the backup. Validation of the archive will validate all the archive's backups and may take a long time and a lot of system resources.
3. **Validation schedule** (appears only if you have selected the on schedule in step 1) - set the schedule of validation. For more information see the Scheduling section.

5.3 Recovering data

When it comes to data recovery, first consider the most functional method: connect the console to the managed **machine running the operating system** and create the recovery task.

If the managed machine's **operating system fails to start** or you need to **recover data to bare metal**, boot the machine from the bootable media or using Acronis Startup Recovery Manager. Then, create a recovery task.

Acronis Universal Restore lets you recover and boot up **Windows on dissimilar hardware** or a virtual machine.

A **dynamic volume** can be recovered over an existing volume, to unallocated space of a disk group, or to unallocated space of a basic disk. To learn more about recovering dynamic volumes, please turn to the Microsoft LDM (Dynamic volumes) section.

You might need to prepare target disks before recovery. Acronis Backup & Recovery Server OEM includes a handy disk management utility which enables you to create or delete volumes, change a disk partitioning style, create a disk group and perform other disk management operations on the target hardware, both under the operating system and on bare metal. To find out more about Acronis Disk Director LV, see the Disk management section.

To create a recovery task, perform the following steps

General

Task name

[Optional] Enter a unique name for the recovery task. A conscious name lets you quickly identify the task among the others.

Task credentials

[Optional] The task will run on behalf of the user who is creating the task. You can change the task account credentials if necessary. To access this option, select the **Advanced view** check box .

What to recover

Archive

Select the archive to recover data from.

Data type (p. 83)

Applies to: disk recovery

Choose the type of data you need to recover from the selected disk backup.

Content (p. 83)

Select the backup and content to be recovered.

Access credentials

[Optional] Provide credentials for the archive location if the task account does not have the right to access it. To access this option, select the **Advanced view** check box.

Where to recover

This section appears after the required backup is selected and the type of data to recover is defined. The parameters you specify here depend on the type of data being recovered.

Disks

Volumes

Files (p. 88)

You may have to specify credentials for the destination. Skip this step when operating on a machine booted with bootable media.

Access credentials (p. 89)

[Optional] Provide credentials for the destination if the task credentials do not enable recovery of the selected data. To access this option, select the **Advanced view** check box.

When to recover

Recover (p. 89)

Select when to start recovery. The task can start immediately after its creation, be scheduled for a specified date and time in the future or simply saved for manual execution.

[Optional] Acronis Universal Restore

Applies to: Windows OS and system volume recovery

Universal Restore

Use the Acronis Universal Restore when you need to recover and boot up Windows on dissimilar hardware.

Automatic drivers search

Specify where the program should search for HAL, mass storage and network adapter drivers. Acronis Universal Restore will install drivers that better fit the target hardware.

Mass storage drivers to install anyway

[Optional] Specify the mass storage drivers manually if the automatic drivers search has not found the appropriate drivers. To access this option, select the **Advanced view** check box.

Recovery options

Settings

[Optional] Customize the recovery operation by configuring the recovery options, such as pre/post recovery commands, recovery priority, error handling or notification options. If you do nothing in this section, the default values will be used.

After any of the settings is changed against the default value, a new line that displays the newly set value appears. The setting status changes from **Default** to **Custom**. Should you modify the setting again, the line will display the new value unless the new value is the default one. When the default value is set, the line disappears and so you always see only the settings that differ from the default values in the **Settings** section.

Clicking **Reset to default** resets all the settings to default values.

After you complete all the required steps, click **OK** to create the commit creating of the recovery task.

5.3.1 Task credentials

Provide credentials for the account under which the task will run.

To specify credentials

1. Select one of the following:

- **Run under the current user**

The task will run under the credentials with which the user who starts the tasks is logged on. If the task has to run on schedule, you will be asked for the current user's password on completing the task creation.

- **Use the following credentials**

The task will always run under the credentials you specify, whether started manually or executed on schedule.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

2. Click **OK**.

To learn more about using credentials in Acronis Backup & Recovery Server OEM, see the Owners and credentials section.

To learn more about operations available depending on the user privileges, see the User privileges on a managed machine section.

5.3.2 Archive selection

To select an archive

1. Enter the full path to the location in the Path field, or select the desired folder in the folders tree.
 - To select a personal vault, expand the **Personal** group and click the appropriate vault.
 - To select a local folder (CD/DVD drive, or locally attached tape device), expand the **Local folders** group and click the required folder.
 - To select a network share, expand the **Network folders** group, select the required networked machine and then click the shared folder. If the network share requires access credentials, the program will ask for them.
 - To select **FTP** or **SFTP** server, expand the corresponding group and click the appropriate folder on the server.

According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

1. In the table to the right of the tree, select the archive. The table displays the names of the archives contained in each vault/folder you select. If the archive is password-protected, provide the password.
2. While you are reviewing the location content, archives can be added, deleted or modified by another user or by the program itself according to scheduled operations. Use the **Refresh** button to refresh the list of archives.
3. Click **OK**.

5.3.3 Data type

Choose what type of data to recover from the selected disk backup:

- **Disks** - to recover disks
- **Volumes** - to recover volumes
- **Files** - to recover specific files and folders

5.3.4 Content selection

The representation of this window depends on the type of data stored in the archive.

5.3.4.1 Disks/volumes selection

To select a backup and disks/volumes to recover:

1. Select one of the successive backups by its creation date and time. Thus, you can revert the disk data to a certain moment in time.

Specify the items to recover. By default, all items of the selected backup will be selected. If you do not want to recover certain items, just uncheck them.

To obtain information on a disk/volume, right-click it and then click **Information**.

2. Click **OK**.

Selecting an MBR

You will usually select the disk's MBR if:

- The operating system cannot boot
- The disk is new and does not have an MBR
- Recovering custom or non-Windows boot loaders (such as LILO and GRUB)
- The disk geometry is different to that stored in the backup.

There are probably other times when you may need to recover the MBR, but the above are the most common.

When recovering the MBR of one disk to another Acronis Backup & Recovery Server OEM recovers Track 0, which does not affect the target disk's partition table and partition layout. Acronis Backup & Recovery Server OEM automatically updates Windows loaders after recovery, so there is no need to recover the MBR and Track 0 for Windows systems, unless the MBR is damaged.

5.3.4.2 Files selection

To select a backup and files to recover:

1. Select one of the successive backups by its creation date/time. Thus, you can revert the files/folders to a specific moment in time.
2. Specify the files and folders to recover by selecting the corresponding check boxes in the archives tree.

Selecting a folder automatically selects all its nested folders and files.

Use the table to the right of the archives tree to select the nested items. Selecting the check box for the **Name** column's header automatically selects all items in the table. Clearing this check box automatically deselects all the items.

3. Click **OK**.

5.3.5 Access credentials for location

Specify the credentials required for access to the location where the backup archive is stored.

To specify credentials

1. Select one of the following:
 - **Use the plan's credentials**
The program will access the source data using the credentials of the backup plan account specified in the General section.
 - **Use the following credentials**

The program will access the source data using the credentials you specify. Use this option if the plan account does not have access permissions to the location. You might need to provide special credentials for a network share.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

Click **OK**.

Warning: According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

5.3.6 Destination selection

Specify the destination the selected data will be recovered to.

5.3.6.1 Disks

Available disk destinations depend on the agents operating on the machine.

Recover to:

Physical machine

Available when the Acronis Backup & Recovery Server OEM Agent for Windows is installed.

The selected disks will be recovered to the physical disks of the machine the console is connected to. On selecting this, you proceed to the regular disk mapping procedure described below.

Disk #:

Disk # (MODEL) (p. 87)

Select the destination disk for each of the source disks.

NT signature

Select the way the recovered disk's signature will be handled. The disk signature is used by Windows and the Linux kernel version 2.6 and later.

Disk destination

To specify a destination disk:

1. Select a disk where you want the selected disk to recover to. The destination disk's space should be at least the same size as the uncompressed image data.
2. Click **OK**.

All the data stored on the target disk will be replaced by the backed up data, so be careful and watch out for non-backed-up data that you might need.

NT signature

When the MBR is selected along with the disk backup, you need to retain operating system bootability on the target disk volume. The operating system must have the system volume information (e.g. volume letter) matched with the disk NT signature, which is kept in the MBR disk record. But two disks with the same NT signature cannot work properly under one operating system.

If there are two disks having the same NT signature and comprising of a system volume on a machine, at the startup the operating system runs from the first disk, discovers the same signature on the second one, automatically generates a new unique NT signature and assigns it to the second disk. As a result, all the volumes on the second disk will lose their letters, all paths will be invalid on the disk, and programs won't find their files. The operating system on that disk will be unbootable.

To retain system bootability on the target disk volume, choose one of the following:

- **Select automatically**
A new NT signature will be created only if the existing one differs from the one in the backup. Otherwise, the existing NT signature will be kept.
- **Create new**
The program will generate a new NT signature for the target hard disk drive.
- **Recover from backup**
The program will replace the NT signature of the target hard disk with one from the disk backup. Recovering the disk signature may be desirable due to the following reasons:
 - Acronis Backup & Recovery Server OEM creates scheduled tasks using the signature of the source hard disk. If you recover the same disk signature, you don't need to re-create or edit the tasks created previously
 - Some installed applications use disk signature for licensing and other purposes
 - This enables to keep all the Windows Restore Points on the recovered disk
 - To recover VSS snapshots used by Windows Vista's "Previous Versions" feature
- **Keep existing**
The program will leave the existing NT signature of the target hard disk as is.

5.3.6.2 Volumes

Available disk destinations depend on the agents operating on the machine.

Recover to:

Physical machine

Available when the Acronis Backup & Recovery Server OEM Agent for Windows is installed.

The selected disks will be recovered to the physical disks of the machine the console is connected to. On selecting this, you proceed to the regular disk mapping procedure described below.

Disk #:

Disk # (MODEL) (p. 87)

Select the destination disk for each of the source disks.

NT signature

Select the way the recovered disk's signature will be handled. The disk signature is used by Windows.

MBR destination

To specify a destination disk:

1. Select the disk to recover the MBR to.
2. Click **OK**.

Volume destination

To specify a destination volume:

1. Select a volume or unallocated space where you want the selected volume to be recovered to. The destination volume/unallocated space should be at least the same size as the uncompressed image data.
2. Click **OK**.

All the data stored on the target volume will be replaced by the backed up data, so be careful and watch out for non-backed-up data that you might need.

When using bootable media

Disk letters seen under Windows-style bootable media might differ from the way Windows identifies drives. For example, the D: drive in the rescue utility might correspond to the E: drive in Windows.

Be careful! To be on the safe side, it is advisable to assign unique names to the volumes.

The Linux-style bootable media shows local disks and volumes as unmounted (sda1, sda2...).

Volume properties

Resizing and relocating

When recovering a volume to a basic MBR disk, you can resize and relocate the volume by dragging it or its borders with a mouse or by entering corresponding values in the appropriate fields. Using this feature, you can redistribute the disk space between the volumes being recovered. In this case, you will have to recover the volume to be reduced first.

Tip: A volume cannot be resized when being recovered from a backup split into multiple removable media. To be able to resize the volume, copy all parts of the backup to a single location on a hard disk.

Properties

Type

A basic MBR disk can contain up to four primary volumes or up to three primary volumes and multiple logical drives. By default, the program selects the original volume's type. You can change this setting, if required.

- **Primary.** Information about primary volumes is contained in the MBR partition table. Most operating systems can boot only from the primary volume of the first hard disk, but the number of primary volumes is limited.

If you are going to recover a system volume to a basic MBR disk, select the Active check box. Active volume is used for loading an operating system. Choosing active for a volume without an installed operating system could prevent the machine from booting. You cannot set a logical drive or dynamic volume active.

- **Logical.** Information about logical volumes is located not in the MBR, but in the extended partition table. The number of logical volumes on a disk is unlimited. A logical volume cannot be set as active. If you recover a system volume to another hard disk with its own volumes and operating system, you will most likely need only the data. In this case, you can recover the volume as logical to access the data only.

File system

Change the volume file system, if required. By default, the program selects the original volume's file system. Acronis Backup & Recovery Server OEM can make the following file system conversions: FAT 16 -> FAT 32 and Ext2 -> Ext3. For volumes with other native file systems, this option is not available.

Assume you are going to recover a volume from an old, low-capacity FAT16 disk to a newer disk. FAT16 would not be effective and might even be impossible to set on the high-capacity hard disk. That's because FAT16 supports volumes up to 4GB, so you will not be able to recover a 4GB FAT16 volume to a volume that exceeds that limit, without changing the file system. It would make sense here to change the file system from FAT16 to FAT32.

Older operating systems (MS-DOS, Windows 95 and Windows NT 3.x, 4.x) do not support FAT32 and will not be operable after you recover a volume and change its file system. These can be normally recovered on a FAT16 volume only.

Logical drive letter (for Windows only)

Assign a letter to the recovered volume. Select the desired letter from a drop-down list.

- With the default AUTO selection, the first unused letter will be assigned to the volume.
- If you select NO, no letter will be assigned to the recovered volume, hiding it from the OS. You should not assign letters to volumes that are inaccessible to Windows, such as to those other than FAT and NTFS.

5.3.6.3 File destination

To specify a destination:

1. Select a location to recover the backed up files to:
 - **Original location** - files and folders will be recovered to the same path(s) as they are in the backup. For example, if you have backed up all files and folders in C:\Documents\Finance\Reports\, the files will be recovered to the same path. If the folder does not exist, it will be created automatically.
 - **New location** - files will be recovered to the location that you specify in the tree. The files and folders will be recovered without recreating a full path, unless you clear the **Recover without full path** check box.
2. Click **OK**.

Exclusions

Set up exclusions for the specific types of files you do not wish to be overwritten during recovery.

To specify which files and folders to exclude:

Set up the following parameter:

*You can view file or folder attributes in the file/folder properties or by using the **attrib** command. For more information, refer to the Help and Support Center in Windows.*

- **Exclude files matching the following criteria**

Select this check box to skip files whose names match any of the criteria — called file masks — in the list; use the **Add**, **Edit**, **Remove** and **Remove All** buttons to create the list of file masks.

You can use one or more wildcard characters * and ? in a file mask:

The asterisk (*) substitutes for zero or more characters in a file name; for example, the file mask Doc*.txt yields files such as Doc.txt and Document.txt

The question mark (?) substitutes for exactly one character in a file name; for example, the file mask Doc?.txt yields files such as Doc1.txt and Docs.txt — but not the files Doc.txt or Doc11.txt

Exclusion examples

Criterion	Example	Description
By name	File1.log	Excludes all files named File1.log.
By path	C:\Finance\test.log	Excludes the file named test.log located in the folder C:\Finance
Mask (*)	*.log	Excludes all files with the .log extension.
Mask (?)	my???.log	Excludes all .log files with names consisting of five symbols and starting with “my”.

Overwriting

Choose what to do if the program finds in the target folder a file with the same name as in the archive:

- **Overwrite existing file** - this will give the file in the backup priority over the file on the hard disk.
- **Overwrite existing file if it is older** - this will give priority to the most recent file modification, whether it be in the backup or on the disk.
- **Do not overwrite existing file** - this will give the file on the hard disk priority over the file in the backup.

5.3.7 Access credentials for destination

To specify credentials

1. Select one of the following:

- **Use the task credentials**

The program will access the destination using the credentials of the task account specified in the General section.

- **Use the following credentials**

The program will access the destination using the credentials you specify. Use this option if the task account does not have access permissions to the destination.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

2. Click **OK**.

5.3.8 When to recover

Select when to start the recovery task:

- **Recover now** - the recovery task will be started immediately after you click the final **OK**.
- **Recover later** - the recovery task will be started at the date and time you specify.

If you do not need to schedule the task and wish to start it manually afterwards, select the **Task will be started manually (do not schedule the task)** check box.

5.3.9 Universal Restore

Use Acronis Backup & Recovery Server OEM Universal Restore when you need to recover and boot up Windows on dissimilar hardware. Universal Restore handles differences in devices that are critical for the operating system startup, such as storage controllers, motherboard or chipset.

To learn more about the Universal Restore technology, see the Universal Restore section.

Acronis Backup & Recovery Server OEM Universal Restore is not available when:

a machine is booted with Acronis Startup Recovery Manager (using F11) because these features are primarily meant for instant data recovery on the same machine.

Preparation

Before recovering Windows to dissimilar hardware, make sure that you have the drivers for the new HDD controller and the chipset. These drivers are critical to start the operating system. Use the CD or DVD supplied by the hardware vendor or download the drivers from the vendor's Web site. The driver files should have the *.inf, *.sys or *.oem extensions. If you download the drivers in the *.exe, *.cab or *.zip format, extract them using a third-party application, such as WinRAR (<http://www.rarlab.com/>) or Universal Extractor (<http://legroom.net/software/uniextract>).

The best practice is to store drivers for all the hardware used in your organization in a single repository sorted by device type or by the hardware configurations. You can keep a copy of the repository on a DVD or a flash drive; pick some drivers and add them to the bootable media; create the custom bootable media with the necessary drivers (and the necessary network configuration) for each of your servers. Or you can simply specify the path to the repository every time Universal Restore is used.

Universal Restore settings

Automatic driver search

Specify where the program will search for the Hardware Abstraction Layer (HAL), HDD controller driver and network adapter driver(s):

- If the drivers are on a vendor's disc or other removable media, turn on the **Search removable media**.
- If the drivers are located in a networked folder or on the bootable media, specify the path to the folder in the **Search folder** field.

During recovery, Universal Restore will perform the recursive search in all the sub-folders of the specified folder, find the most suitable HAL and HDD controller drivers of all those available, and install them into the recovered system. Universal Restore also searches for the network adapter driver; the path to the found driver is then transmitted by Universal Restore to the operating system. If the hardware has multiple network interface cards, Universal Restore will try to configure all the cards' drivers. In case Universal Restore cannot find a compatible driver in the specified locations, it will specify the problem device and ask for a disc or a network path to the driver.

Once Windows boots, it will initialize the standard procedure for installing new hardware. The network adapter driver will be installed silently if the driver has the Microsoft Windows signature. Otherwise, Windows will ask for confirmation whether to install the unsigned driver. After that, you will be able to configure the network connection and specify drivers for the video adapter, USB and other devices.

Mass storage drivers to install anyway

To access this option, select the **Advanced view** check box.

If the target hardware has a specific mass storage controller such as RAID (especially NVIDIA RAID) or a fibre channel adapter, specify the appropriate drivers in the **Drivers** field.

The drivers defined here will have priority. They will be installed, with appropriate warnings, even if the program finds a better driver.

Use this option only if the automatic drivers search does not help to boot the system.

5.3.10 Bootability troubleshooting

If a system was bootable at the time of backup, you expect that it will boot after recovery. However, the information the operating system stores and uses for booting up may become outdated during recovery, especially if you change volume sizes, locations or destination drives. Acronis Backup & Recovery Server OEM automatically updates Windows loaders after recovery. Other loaders might also be fixed, but there are cases when you have to re-activate the loaders.

Below is a summary of typical situations that require additional user actions.

Why a recovered operating system may be unbootable

- **The machine BIOS is configured to boot from another HDD.**
Solution: Configure the BIOS to boot from the HDD where the operating system resides.
- **The system was recovered on dissimilar hardware and the new hardware is incompatible with the most critical drivers included in the backup**
Solution for Windows: Recover the volume once again. When configuring recovery, opt for using Acronis Universal Restore and specify the appropriate HAL and mass storage drivers.
- **Windows was recovered to a dynamic volume that cannot be bootable**
Solution: Recover Windows to a basic, simple or mirrored volume.
- **A system volume was recovered to a disk that does not have an MBR**
When you configure recovery of a system volume to a disk that does not have an MBR, the program prompts whether you want to recover the MBR along with the system volume. Opt for not recovering, only if you do not want the system to be bootable.
Solution: Recover the volume once again along with the MBR of the corresponding disk.
- **The system loader points to the wrong volume**
This may happen when system or boot volumes are not recovered to their original location.
Solution:
Modification of the boot.ini or the boot\bcd files fixes this for Windows loaders. Acronis Backup & Recovery Server OEM does this automatically and so you are not likely to experience the problem.

5.3.10.1 About Windows loaders

Windows NT/2000/XP/2003

A part of the loader resides in the partition boot sector, the rest is in the files ntldr, boot.ini, ntdetect.com, ntbootdd.sys. boot.ini is a text file that contains the loader configuration. Example:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

Windows Vista/2008

A part of the loader resides in the partition boot sector, the rest is in the files bootmgr, boot\bcd. At starting Windows, boot\bcd is mounted to the registry key HKLM \BCD00000000.

5.4 Validating vaults, archives and backups

Validation is an operation that checks the possibility of data recovery from a backup.

Validation of a file backup imitates recovery of all files from the backup to a dummy destination. Validation of a disk or volume backup calculates a checksum for every data block saved in the backup. Both procedures are resource-intensive.

Validation of an archive will validate all the archive's backups. A vault (or a location) validation will validate all archives stored in this vault (location).

While successful validation means high probability of successful recovery, it does not check all factors that influence the recovery process. If you back up the operating system, only a test recovery in bootable environment to a spare hard drive can guarantee success of the recovery. At least ensure that the backup can be successfully validated using the bootable media.

Different ways to create a validation task

Using the Validation page is the most general way to create a validation task. Here you can validate immediately or set up a validation schedule for any backup, archive or location you have permission to access.

Validation of an archive or of the latest backup in the archive can be scheduled as part of the backup plan. For more information see the Creating a backup plan section.

You can access the **Validation** page from the **Vaults** view. Right-click the object to validate (archive, backup or vault) and select **Validate** from the context menu. The Validation page will be opened with the pre-selected object as a source. All you need to do is to select when to validate and (optionally) provide a name for the task.

To create a validation task, perform the following steps.

General

Task name

[Optional] Enter a unique name for the validation task. A conscious name lets you quickly identify the task among the others.

Credentials (p. 93)

[Optional] The validation task will run on behalf of the user who is creating the task. You can change the task credentials if necessary. To access this option, select the **Advanced view** check box.

What to validate

Validate

Choose an object to validate:

Archive - in that case, you need to specify the archive.

Backup (p. 94) - specify the archive first, and then select the desired backup in this archive.

Vault - select a vault (or other location), which archives to validate.

Access Credentials

[Optional] Provide credentials for accessing the source if the task account does not have enough privileges to access it. To access this option, select the check box for **Advanced view**.

When to validate

Validate (p. 95)

Specify when and how often to perform validation.

After you configure all the required settings, click **OK** to create the validation task.

5.4.1 Task credentials

Provide credentials for the account under which the task will run.

To specify credentials

1. Select one of the following:

- **Run under the current user**

The task will run under the credentials with which the user who starts the tasks is logged on. If the task has to run on schedule, you will be asked for the current user's password on completing the task creation.

- **Use the following credentials**

The task will always run under the credentials you specify, whether started manually or executed on schedule.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

2. Click **OK**.

To learn more about using credentials in Acronis Backup & Recovery Server OEM, see the Owners and credentials section.

To learn more about operations available depending on the user privileges, see the User privileges on a managed machine section.

5.4.2 Archive selection

To select an archive

1. Enter the full path to the location in the Path field, or select the desired folder in the folders tree.

- To select a personal vault, expand the **Personal** group and click the appropriate vault.
- To select a local folder (CD/DVD drive, or locally attached tape device), expand the **Local folders** group and click the required folder.
- To select a network share, expand the **Network folders** group, select the required networked machine and then click the shared folder. If the network share requires access credentials, the program will ask for them.

- To select **FTP** or **SFTP** server, expand the corresponding group and click the appropriate folder on the server.

According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

1. In the table to the right of the tree, select the archive. The table displays the names of the archives contained in each vault/folder you select. If the archive is password-protected, provide the password.
2. While you are reviewing the location content, archives can be added, deleted or modified by another user or by the program itself according to scheduled operations. Use the **Refresh** button to refresh the list of archives.
3. Click **OK**.

5.4.3 Backup selection

To specify a backup to validate

1. In the upper pane, select a backup by its creation date/time.
The bottom part of the window displays the selected backup content, assisting you to find the right backup.
2. Click **OK**.

5.4.4 Location selection

To select a location

Enter the full path to the location in the Path field or select the desired location in the folders tree.

- To select a personal vault, expand the **Personal** group and click the appropriate vault.
- To select a local folder (CD/DVD drive, or locally attached tape device), expand the **Local folders** group and click the required folder.
- To select a network share, expand the **Network folders** group, select the required networked machine and then click the shared folder. If the network share requires access credentials, the program will ask for them.
- To select **FTP** or **SFTP** server, expand the corresponding group and click the appropriate folder on the server.

According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

Using the archives table

To assist you with choosing the right location, the table displays the names of the archives contained in each location you select. While you are reviewing the location content, archives can be added, deleted or modified by another user or by the program itself according to scheduled operations. Use the **Refresh** button to refresh the list of archives.

5.4.5 Access credentials for source

Specify the credentials required for access to the location where the backup archive is stored.

To specify credentials

1. Select one of the following:

- **Use the plan's credentials**

The program will access the source data using the credentials of the backup plan account specified in the General section.

- **Use the following credentials**

The program will access the source data using the credentials you specify. Use this option if the plan account does not have access permissions to the location. You might need to provide special credentials for a network share.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

Click **OK**.

Warning: According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

5.4.6 When to validate

As validation is a resource-intensive operation, it makes sense to schedule validation to the managed machine's off-peak period. On the other hand, if you prefer to be immediately informed whether the data is not corrupted and can be successfully recovered, consider starting validation right after the task creation.

Choose one of the following:

- **Now** - to start the validation task right after its creation, that is, after clicking OK on the Validation page.
- **Later** - to start the one-time validation task, at the date and time you specify.

Specify the appropriate parameters as follows:

- **Date and time** - the date and time when to start the task.
- **The task will be started manually (do not schedule the task)** - select this check box, if you wish to start the task manually later.
- **On schedule** - to schedule the task. To learn more about how to configure the scheduling parameters, please see the Scheduling section.

5.5 Mounting an image

Mounting volumes from a disk backup (image) lets you access the volumes as though they were physical disks. Multiple volumes contained in the same backup can be mounted within a single mount operation. The mount operation is available when the console is connected to a managed machine running Windows.

Usage scenarios:

- **Sharing:** mounted images can be easily shared to networked users.

- **"Band aid" database recovery solution:** mount up an image that contains an SQL database from a recently failed machine. This will give access to the database until the failed machine is recovered.
- **Offline virus clean:** if a machine is attacked, the administrator shuts it down, boots with bootable media and creates an image. Then, the administrator mounts this image, scans and cleans it with an antivirus program, and finally recovers the machine.

To mount an image, perform the following steps.

Source

Archive

Specify the path to the archive location and select the archive containing disk backups.

Backup (p. 96)

Select the backup.

Access credentials

[Optional] Provide credentials for the archive location. To access this option, select the **Advanced view** check box.

5.5.1 Archive selection

To select an archive

1. Enter the full path to the location in the Path field, or select the desired folder in the folders tree.
 - To select a personal vault, expand the **Personal** group and click the appropriate vault.
 - To select a local folder (CD/DVD drive, or locally attached tape device), expand the **Local folders** group and click the required folder.
 - To select a network share, expand the **Network folders** group, select the required networked machine and then click the shared folder. If the network share requires access credentials, the program will ask for them.
 - To select **FTP** or **SFTP** server, expand the corresponding group and click the appropriate folder on the server.

According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

1. In the table to the right of the tree, select the archive. The table displays the names of the archives contained in each vault/folder you select. If the archive is password-protected, provide the password.
2. While you are reviewing the location content, archives can be added, deleted or modified by another user or by the program itself according to scheduled operations. Use the **Refresh** button to refresh the list of archives.
3. Click **OK**.

5.5.2 Backup selection

To select a backup:

1. Select one of the backups by its creation date/time.
2. To assist you with choosing the right backup, the bottom table displays the volumes contained in the selected backup.

To obtain information on a volume, right-click it and then click **Information**.

3. Click **OK**.

5.5.3 Access credentials

To specify credentials

1. Select one of the following:

- **Use the current user credentials**

The program will access the location using the credentials of the current user.

- **Use the following credentials**

The program will access the location using the credentials you specify. Use this option if the current user account does not have access permissions to the location. You might need to provide special credentials for a network share.

Specify:

- **User name.** When entering the name of an Active Directory user account, be sure to also specify the domain name (DOMAIN\Username or Username@domain)
- **Password.** The password for the account.

Click **OK**.

Warning: According to the original FTP specification, credentials required for access to FTP servers are transferred through a network as plaintext. This means that the user name and password can be intercepted by an eavesdropper using a packet sniffer.

5.5.4 Volume selection

Select the volumes to mount and configure the mounting parameters for each of the selected volumes as follows:

1. Select the check box for each volume you need to mount.
2. Click on the selected volume to set its mounting parameters.
 - **Access mode** - choose the mode you want the volume to be mounted in:
 - **Read only** - enables exploring and opening files within the backup without committing any changes.
 - **Assign letter** (in Windows) - Acronis Backup & Recovery Server OEM will assign an unused letter to the mounted volume. If required, select another letter to assign from the drop-down list.
3. If several volumes are selected for mounting, click on every volume to set its mounting parameters, described in the previous step.
4. Click **OK**.

5.6 Managing mounted images

Once a volume is mounted, you can browse files and folders contained in the backup using a file manager and copy the desired files to any destination. Thus, if you need to take out only a few files and folders from a volume backup, you do not have to perform the recovery procedure.

Exploring images

Exploring mounted volumes lets you view the volume's content.

To explore a mounted volume select it in the table and click  **Explore**. The default file manager window opens, allowing the user to examine the mounted volume contents.

Unmounting images

Maintaining the mounted volumes takes considerable system resources. It is recommended that you unmount the volumes after the necessary operations are completed. If not unmounted manually, a volume will remain mounted until the operating system restarts.

To unmount an image, select it in the table and click  **Unmount**.

To unmount all the mounted volumes, click  **Unmount all**.

5.7 Acronis Startup Recovery Manager

Acronis Startup Recovery Manager is a modification of the bootable agent, residing on the system disk in Windows and configured to start at boot time on pressing F11. It eliminates the need for a separate media or network connection to start the bootable rescue utility.

Activate

Enables the boot time prompt "Press F11 for Acronis Startup Recovery Manager..." (if you do not have the GRUB boot loader) or adds the "Acronis Startup Recovery Manager" item to GRUB's menu (if you have GRUB). If the system fails to boot, you will be able to start the bootable rescue utility, by pressing F11 or by selecting it from the menu, respectively.

The system disk should have at least 70 MB of free space to activate Acronis Startup Recovery Manager.

Unless you use the GRUB boot loader and it is installed in the Master Boot Record (MBR), Acronis Startup Recovery Manager activation overwrites the MBR with its own boot code. Thus, you may need to reactivate third-party boot loaders, if they are installed.

Do not activate

Disables boot time prompt "Press F11 for Acronis Startup Recovery Manager..." (or the menu item in GRUB). If Acronis Startup Recovery Manager is not activated, you will need the following to recover the system when it fails to boot:

- boot the machine from a separate bootable rescue media.

See the Bootable media section for details.

5.8 Bootable media

Bootable media

Bootable media is physical media (CD, DVD, USB drive or other media supported by a machine BIOS as a boot device) that boots on any PC-compatible machine and enables you to run Acronis Backup & Recovery Server OEM Agent in Windows Preinstallation Environment (WinPE), without the help of an operating system. Bootable media is most often used to:

- recover an operating system that cannot start
- access and back up the data that has survived in a corrupted system
- deploy an operating system on bare metal
- create basic or dynamic volumes on bare metal

- back up sector-by-sector a disk with an unsupported file system
- back up offline any data that cannot be backed up online because of restricted access, being permanently locked by the running applications or for any other reason.

A machine can be booted into the above environments either with physical media, or using the network boot from Windows Deployment Services (WDS) or Remote Installation Services (RIS). These servers with uploaded bootable components can be thought of as a kind of bootable media too. You can create bootable media or configure the WDS/RIS using the same wizard.

PE-based bootable media

PE-based bootable media contains a minimal Windows system called Windows Preinstallation Environment (WinPE) and Acronis Plug-in for WinPE, that is, a modification of Acronis Backup & Recovery Server OEM Agent that can run in the preinstallation environment.

WinPE proved to be the most convenient bootable solution in large environments with heterogeneous hardware.

Advantages:

- Having booted PC-compatible hardware into WinPE, you can use not only Acronis Backup & Recovery Server OEM Agent, but also PE commands and scripts and other plug-ins you've added to the PE.
- Media based on PE 2.x, that is, Windows Vista or Windows Server 2008 kernel, allows for dynamic loading of the necessary device drivers.

5.8.1 How to create bootable media

To enable creating physical media, the machine must have a CD/DVD recording drive or allow a flash drive to be attached. To enable WDS/RIS configuration, the machine must have a network connection. Bootable Media Builder can also create an ISO image of a bootable disk to burn it later on a blank disk.

PE-based bootable media

Acronis Plug-in for WinPE can be added to WinPE distributions based on any of the following kernels:

- Windows XP Professional with Service Pack 2 (PE 1.5)
- Windows Server 2003 with Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 and Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0)

If you already have media with PE1.x distribution, unpack the media ISO to a local folder and start the Bootable Media Builder either from the management console, by selecting **Tools > Create Bootable Media** or, as a separate component. The wizard will guide you through the necessary operations. Please refer to Adding the Acronis Plug-in to WinPE 1.x (p. 100) for details.

To be able to create or modify PE 2.x or 3.0 images, install Bootable Media Builder on a machine where Windows Automated Installation Kit (AIK) is installed. The further operations are described in the Adding the Acronis Plug-in to WinPE 2.x or 3.0 section.

If you do not have a machine with WAIK, prepare as follows:

1. Download and install Windows Automated Installation Kit (WAIK).

Automated Installation Kit (AIK) for Windows Vista (PE 2.0):

<http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en>

Automated Installation Kit (AIK) for Windows Vista SP1 and Windows Server 2008 (PE 2.1):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en>

Automated Installation Kit (AIK) for Windows 7 (PE 3.0):

<http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en>

2. [optional] Burn the WAIK to DVD or copy to a flash drive.
3. Install the Microsoft .NET Framework v.2.0 from this kit (NETFXx86 or NETFXx64, depending on your hardware.)
4. Install Microsoft Core XML (MSXML) 5.0 or 6.0 Parser from this kit.
5. Install Windows AIK from this kit.
6. Install Bootable Media Builder on the same machine.

It is recommended that you familiarize yourself with the help documentation supplied with Windows AIK. To access the documentation, select **Microsoft Windows AIK -> Documentation** from the start menu.

Using Bart PE

You can create a Bart PE image with Acronis Plug-in using the Bart PE Builder. Please refer to Building Bart PE with Acronis Plug-in from Windows distribution (p. 102) for details.

5.8.1.1 Adding the Acronis Plug-in to WinPE 1.x

Acronis Plug-in for WinPE can be added to:

- Windows PE 2004 (1.5) (Windows XP Professional with Service Pack 2)
- Windows PE 2005 (1.6) (Windows Server 2003 with Service Pack 1).

To add Acronis Plug-in to WinPE 1.x:

1. Unpack all files of your WinPE 1.x ISO to a separate folder on the hard disk.
2. Start the Bootable Media Builder either from the management console, by selecting **Tools > Create Bootable Media** or, as a separate component.
3. Select **Bootable media type: Windows PE**.
 - Select **Use WinPE files located in the folder I specify**
4. Specify path to the folder where the WinPE files are located.
5. Specify the full path to the resulting ISO file including the file name.
6. Check your settings in the summary screen and click **Proceed**.
7. Burn the .ISO to CD or DVD using a third-party tool or copy to a flash drive.

Once a machine boots into the WinPE, Acronis Backup & Recovery Server OEM starts automatically.

5.8.1.2 Adding the Acronis Plug-in to WinPE 2.x or 3.0

Bootable Media Builder provides three methods of integrating Acronis Backup & Recovery Server OEM with WinPE 2.x or 3.0:

- Adding the Acronis Plug-in to the existing PE ISO. This comes in handy when you have to add the plug-in to the previously configured PE ISO that is already in use.
- Creating the PE ISO with the plug-in from scratch.
- Adding the Acronis Plug-in to a WIM file for any future purpose (manual ISO building, adding other tools to the image and so on).

To be able to perform any of the above operations, install Bootable Media Builder on a machine where Windows Automated Installation Kit (WAIK) is installed. If you do not have such machine, prepare as described in [How to create bootable media](#).

Bootable Media Builder supports only x86 WinPE 2.x or 3.0. These WinPE distributions can also work on x64 hardware.

A PE image based on Win PE 2.0 requires at least 256MB RAM to work. The recommended memory size for PE 2.0 is 512MB. A PE image based on Win PE 3.0 requires at least 512MB RAM to work.

Adding Acronis Plug-in to WinPE 2.x or 3.0 ISO

To add Acronis Plug-in to WinPE 2.x or 3.0 ISO:

1. When adding the plug-in to the existing Win PE ISO, unpack all files of your Win PE ISO to a separate folder on the hard disk.
2. Start the Bootable Media Builder either from the management console, by selecting **Tools > Create Bootable Media** or, as a separate component.
3. Select **Bootable media type: Windows PE**.

When creating a new PE ISO:

- Select **Create Windows PE 2.x or 3.0 automatically**
- The software runs the appropriate script and proceeds to the next window.

When adding the plug-in to the existing PE ISO:

- Select **Use WinPE files located in the folder I specify**
- Specify path to the folder where the WinPE files are located.

4. [optional] Specify Windows drivers to be added to Windows PE. Once you boot a machine into Windows PE, the drivers can help you access the device where the backup archive is located. Click **Add** and specify the path to the necessary *.inf file for a corresponding SCSI, RAID, SATA controller, network adapter, tape drive or other device. You will have to repeat this procedure for each driver you want to be included in the resulting WinPE boot media.
5. Choose whether you want to create ISO or WIM image.
6. Specify the full path to the resulting image file including the file name.
7. Check your settings in the summary screen and click **Proceed**.
8. Burn the .ISO to CD or DVD using a third-party tool or copy to a flash drive.

Once a machine boots into WinPE, Acronis Backup & Recovery Server OEM starts automatically.

To create a PE image (ISO file) from the resulting WIM file:

- replace the default boot.wim file in your Windows PE folder with the newly created WIM file. For the above example, type:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- use the **Oscdimg** tool. For the above example, type:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO  
c:\winpe_x86\winpe_x86.iso
```

For more information on customizing Windows PE, see the Windows Preinstallation Environment User's Guide (Winpe.chm).

5.8.1.3 Building Bart PE with Acronis Plug-in from Windows distribution

1. Get the Bart PE builder.
2. Install Bootable Media Builder from the Acronis Backup & Recovery Server OEM setup file.
3. Change the current folder to the folder where the Acronis Plug-in for WinPE is installed—by default: C:\Program Files\Acronis\Bootable Components\WinPE.
If the plug-in is installed in a folder other than the default folder, change the path accordingly (check the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Bootable Components\Settings\WinPE for the plug-in location).
4. Run the following command:

```
export_license.bat
```
5. Copy the contents of the current folder—by default: C:\Program Files\Acronis\Bootable Components\WinPE—to the %BartPE folder%\plugins\Acronis.
6. Insert your Windows distribution CD if you do not have a copy of Windows installation files on the HDD.
7. Start the Bart PE builder.
8. Specify the path to the Windows installation files or Windows distribution CD.
9. Click **Plugins** and check whether the Acronis Backup & Recovery Server OEM plug-in is enabled. Enable if disabled.
10. Specify the output folder and the full path to the resulting ISO file including the file name or the media to create.
11. Build the Bart PE.
12. Burn the ISO to CD or DVD (if this has not been done yet) or copy to a flash drive.

Once the machine boots into the Bart PE and you configure the network connection, select **Go -> System -> Storage -> Acronis Backup & Recovery Server OEM** to start.

5.8.2 Working under bootable media

Operations on a machine booted with bootable media are very similar to backup and recovery under the operating system. The difference is as follows:

1. Disk letters seen under Windows-style bootable media might differ from the way Windows identifies drives. For example, the D: drive under the rescue utility might correspond to the E: drive in Windows.

Be careful! To be on the safe side, it is advisable to assign unique names to the volumes.

2. There is no **Navigation** tree in the media GUI. Use the **Navigation** menu item to navigate between views.
3. Tasks cannot be scheduled; in fact, tasks are not created at all. If you need to repeat the operation, configure it from scratch.
4. The log lifetime is limited to the current session. You can save the entire log or the filtered log entries to a file.

5.8.2.1 Setting up a display mode

For a machine booted from media, a display video mode is detected automatically based on the hardware configuration (monitor and graphics card specifications). If, for some reason, the video mode is detected incorrectly, do the following:

1. In the boot menu, press F11.
2. Add to the command prompt the following command: **vga=ask**, and then proceed with booting.
3. From the list of supported video modes, choose the appropriate one by typing its number (for example, **318**), and then press ENTER.

If you do not wish to follow this procedure every time you boot from media on a given hardware configuration, re-create the bootable media with the appropriate mode number (in our example, **vga=0x318**) typed in the **Kernel parameters** window (see the Bootable Media Builder section for details).

5.8.2.2 Configuring iSCSI and NDAS devices

This section describes how to configure Internet Small Computer System Interface (iSCSI) devices and Network Direct Attached Storage (NDAS) devices when working under bootable media.

These devices are connected to the machine through a network interface and appear as if they were locally-attached devices. On the network, an iSCSI device is identified by its IP address, and an NDAS device is identified by its device ID.

An iSCSI device is sometimes called an iSCSI target. A hardware or software component that provides interaction between the machine and the iSCSI target is called the iSCSI initiator. The name of the iSCSI initiator is usually defined by an administrator of the server that hosts the device.

To add an iSCSI device

1. In a bootable media (Linux-based or PE-based), run the management console.
2. Click **Configure iSCSI/NDAS devices** (in a Linux-based media) or **Run the iSCSI Setup** (in a PE-based media).
3. Specify the IP address and port of the iSCSI device's host, and the name of the iSCSI initiator.
4. If the host requires authentication, specify the user name and password for it.
5. Click **OK**.
6. Select the iSCSI device from the list, and then click **Connect**.
7. If prompted, specify the user name and password to access the iSCSI device.

To add an NDAS device

1. In a Linux-based bootable media, run the management console.
2. Click **Configure iSCSI/NDAS devices**.
3. In **NDAS devices**, click **Add device**.
4. Specify the 20-character device ID.
5. If you want to allow writing data onto the device, specify the five-character write key. Without this key, the device will be available in the read-only mode.
6. Click **OK**.

5.8.3 Recovering MD devices and logical volumes

To recover MD devices, known as Linux Software RAID, and/or devices created by Logical Volume Manager (LVM), known as logical volumes, you need to create the corresponding volume structure before starting the recovery.

You can create the volume structure in either of the following ways:

- Automatically in Linux-based bootable media by using the management console or a script—see [Creating the volume structure automatically](#).
- Manually by using the **mdadm** and **lvm** utilities—see [Creating the volume structure manually](#).

5.8.3.1 Creating the volume structure automatically

Suppose that you saved the volume structure to the **/etc/ASM** directory and that the volume with this directory is included in the archive.

To recreate the volume structure in Linux-based bootable media, use either of the methods described below.

Caution: As a result of the following procedures, the current volume structure on the machine will be replaced with the one stored in the archive. This will destroy the data that is currently stored on some or all of the machine's hard disks.

If disk configuration has changed. An MD device or a logical volume resides on one or more disks, each of its own size. If you replaced any of these disks between backup and recovery—or if you are recovering the volumes to a different machine—make sure that the new disk configuration includes enough disks whose sizes are at least those of the original disks.

To create the volume structure by using the management console

1. Boot the machine from a Linux-based bootable media.
2. Click **Acronis Bootable Agent**. Then, click **Run management console**.
3. In the management console, click **Recover**.
Under the archive contents, Acronis Backup & Recovery Server OEM will display a message saying that it detected information about the volume structure.
4. Click **Details** in the area with that message.
5. Review the volume structure, and then click **Apply RAID/LVM** to create it.

To create the volume structure by using a script

1. Boot the machine from a Linux-based bootable media.
2. Click **Acronis Bootable Agent**. Then, click **Run management console**.
3. On the toolbar, click **Actions**, and then click **Start shell**. Alternatively, you can press CTRL+ALT+F2.
4. Run the **restoreraids.sh** script, specifying the full file name of the archive—for example:

```
/bin/restoreraids.sh  
smb://server/backups/linux_machine_2010_01_02_12_00_00_123D.tib
```
5. Return to the management console by pressing CTRL+ALT+F1, or by running the command:
/bin/product
6. Click **Recover**, then specify the path to the archive and any other required parameters, and then click **OK**.

If Acronis Backup & Recovery Server OEM could not create the volume structure (or if it is not present in the archive), create the structure manually.

5.8.3.2 Creating the volume structure manually

The following are a general procedure for recovering MD devices and logical volumes by using a Linux-based bootable media, and an example of such recovery. You can use a similar procedure in Linux.

To recover MD devices and logical volumes

1. Boot the machine from a Linux-based bootable media.
2. Click **Acronis Bootable Agent**. Then, click **Run management console**.
3. On the toolbar, click **Actions**, and then click **Start shell**. Alternatively, you can press CTRL+ALT+F2.
4. Create the volume structure according to that in the archive, by using the **mdadm** utility (for MD devices), the **lvm** utility (for logical volumes), or both.

Note: Logical Volume Manager utilities such as **pvcreate** and **vgcreate**, which are normally available in Linux, are not included in the bootable media environment, so you need to use the **lvm** utility with a corresponding command: **lvm pvcreate**, **lvm vgcreate**, etc.

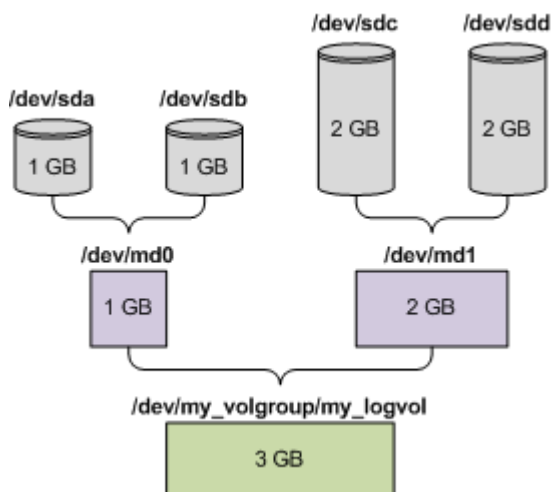
5. Return to the management console by pressing CTRL+ALT+F1, or by running the command:
/bin/product
(Do not reboot the machine at this point. Otherwise, you will have to create the volume structure again.)
6. Click **Recover**, then specify the path to the archive and any other required parameters, and then click **OK**.

Example

Suppose that you previously performed a disk backup of a machine with the following disk configuration:

- The machine has two 1-gigabyte and two 2-gigabyte SCSI hard disks, mounted on **/dev/sda**, **/dev/sdb**, **/dev/sdc**, and **/dev/sdd**, respectively.
- The first and second pairs of hard disks are configured as two MD devices, both in the RAID-1 configuration, and are mounted on **/dev/md0** and **/dev/md1**, respectively.
- A logical volume is based on the two MD devices and is mounted on **/dev/my_volgroup/my_logvol**.

The following picture illustrates this configuration.



Do the following to recover data from this archive.

Step 1: Creating the volume structure

1. Boot the machine from a Linux-based bootable media.
2. In the management console, press CTRL+ALT+F2.
3. Run the following commands to create the MD devices:

```
mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
```

4. Run the following commands to create the logical volume group:

Caution: The **pvcreeate** command destroys all data on the **/dev/md0** and **/dev/md1** devices.

```
lvm pvcreate /dev/md0 /dev/md1
lvm vgcreate my_volgroup /dev/md0 /dev/md1
lvm vgdisplay
```

The output of the **lvm vgdisplay** command will contain lines similar to the following:

```
--- Volume group ---
VG Name      my_volgroup
...
VG Access    read/write
VG Status    resizable
...
VG Size      1.99 GB
...
VG UUID      0qoQ41-Vk7W-yDG3-uF11-Q2AL-C0z0-vMeACu
```

5. Run the following command to create the logical volume; in the **-L** parameter, specify the size given by **VG Size**:

```
lvm lvcreate -L1.99G --name my_logvol my_volgroup
```

6. Activate the volume group by running the following command:

```
lvm vgchange -a y my_volgroup
```

7. Press CTRL+ALT+F1 to return to the management console.

Step 2: Starting the recovery

1. In the management console, click **Recover**.
2. In **Archive**, click **Change** and then specify the name of the archive.
3. In **Backup**, click **Change** and then select the backup from which you want to recover data.
4. In **Data type**, select **Volumes**.
5. In **Items to recover**, select the check box next to **my_volgroup-my_logvol**.
6. Under **Where to recover**, click **Change**, and then select the logical volume that you created in Step 1. Click the chevron buttons to expand the list of disks.
7. Click **OK** to start the recovery.

5.9 Disk management

Acronis Disk Director Lite is a tool for preparing a machine disk/volume configuration for recovering the volume images saved by the Acronis Backup & Recovery Server OEM software.

Sometimes after the volume has been backed up and its image placed into a safe storage, the machine disk configuration might change due to a HDD replacement or hardware loss. In such case with the help of Acronis Disk Director Lite, the user has the possibility to recreate the necessary disk configuration so that the volume image can be recovered exactly “as it was” or with any alteration of the disk or volume structure the user might consider necessary.

All operations on disks and volumes involve a certain risk of data damage. Operations on system, bootable or data volumes must be carried out very carefully to avoid potential problems with the booting process or hard disk data storage.

Operations with hard disks and volumes take a certain amount of time, and any power loss, unintentional turning off of the machine or accidental pressing of the Reset button during the procedure could result in volume damage and data loss.

All operations on volumes of dynamic disks in Windows XP and Windows 2000 require Acronis Managed Machine Service to be run under an account with administrator's rights.

Please take all necessary precautions to avoid possible data loss.

5.9.1 Supported file systems

Acronis Disk Director Lite supports the following file systems:

- FAT 16/32
- NTFS

5.9.2 Basic precautions

To avoid any possible disk and volume structure damage or data loss, please take all necessary precautions and follow these simple rules:

1. Create a disk image of the disk on which volumes will be created or managed. Having your most important data backed up to another hard disk or CD will allow you to work on disk volumes being reassured that your data is safe.

Acronis Backup & Recovery Server OEM is an extremely effective comprehensive data backup and recovery solution. It creates a data or disk backup copy stored in a compressed archive file that can be restored in case of any accident.

2. Test your disk to make sure it is fully functional and does not contain bad sectors or file system errors.
3. Do not perform any disk/volume operations while running other software that has low-level disk access. Close these programs before running Acronis Disk Director Lite.

With these simple precautions, you will protect yourself against accidental data loss.

5.9.3 Running Acronis Disk Director Lite

You can run Acronis Disk Director Lite under Windows or start it from a bootable media.

Running Acronis Disk Director Lite under Windows

If you run Acronis Backup & Recovery Server OEM Management Console, and connect it to a managed machine, the **Disk management** view will be available in the **Navigation** tree of the console, with which you can start Acronis Disk Director Lite.

Running Acronis Disk Director Lite from a bootable media

You can run Acronis Disk Director Lite on a bare metal, on a machine that cannot boot or on a non-Windows machine. To do so, boot the machine from a bootable media created with the Acronis Bootable Media Builder; run the management console and then click **Disk Management**.

5.9.4 Choosing the operating system for disk management

On a machine with two or more operating systems, representation of disks and volumes depends on which operating system is currently running.

A volume may have a different letter in different Windows operating systems. For example, volume E: might appear as D: or L: when you boot another Windows operating system installed on the same machine. (It is also possible that this volume will have the same letter E: under any Windows OS installed on the machine.)

A dynamic disk created in one Windows operating system is considered as a **Foreign Disk** in another Windows operating system or might be unsupported by this operating system.

When you need to perform a disk management operation on such machine, it is necessary to specify for which operating system the disk layout will be displayed and the disk management operation will be performed.

The name of the currently selected operating system is shown on the console toolbar after “**The current disk layout is for:**”. Click the OS name to select another operating system in the **Operating System Selection** window. Under bootable media, this window appears after clicking **Disk management**. The disk layout will be displayed according to the operating system you select.

5.9.5 "Disk management" view

Acronis Disk Director Lite is controlled through the Disk management view of the console.

The top part of the view contains a disks and volumes table enabling data sorting and columns customization and toolbar. The table presents the numbers of the disks, as well as assigned letter, label, type, capacity, free space size, used space size, file system, and status for each volume. The toolbar comprises of icons to launch the Undo, Redo and Commit actions intended for pending operations.

The graphic panel at the bottom of the view also graphically depicts all the disks and their volumes as rectangles with basic data on them (label, letter, size, status, type and file system).

Both parts of the view also depict all unallocated disk space that can be used in volume creation.

Starting the operations

Any operation can be launched:

From the volume or disk context menu (both in the table and the graphic panel)

From the Disk management menu of the console

From the Operations bar on the Actions and Tools pane

Note that the list of available operations in the context menu, the Disk management menu, and the Operations bar depends on the selected volume or disk type. The same is true for unallocated space as well.

Displaying operation results

The results of any disk or volume operation, you have just planned, are immediately displayed in the Disk management view of the console. For example, if you create a volume, it will be immediately

shown in the table, as well as in graphical form at the bottom of the view. Any volume changes, including changing the volume letter or label, are also immediately displayed in the view.

5.9.6 Disk operations

Acronis Disk Director Lite includes the following operations that can be performed on disks:

- Disk Initialization - initializes the new hardware added to the system
- Basic disk cloning - transfers complete data from the source basic MBR disk to the target
- Disk conversion: MBR to GPT - converts an MBR partition table to GPT
- Disk conversion: GPT to MBR (p. 112) - converts a GPT partition table to MBR
- Disk conversion: Basic to Dynamic - converts a basic disk to dynamic
- Disk conversion: Dynamic to Basic - converts a dynamic disk to basic

Acronis Disk Director Lite must obtain exclusive access to the target disk. This means no other disk management utilities (like Windows Disk Management utility) can access it at that time. If you receive a message stating that the disk cannot be blocked, close the disk management applications that use this disk and start again. If you cannot determine which applications use the disk, close them all.

5.9.6.1 Disk initialization

If you add any new disk to your machine, Acronis Disk Director Lite will notice the configuration change and scan the added disk to include it to the disk and volume list. If the disk is still not initialized or, possibly, has a file structure unknown to the machine system, that means that no programs can be installed on it and you will not be able to store any files there.

Acronis Disk Director Lite will detect that the disk is unusable by the system and needs to be initialized. The **Disk management** view will show the newly detected hardware as a gray block with a grayed icon, thus indicating that the disk is unusable by the system.

If you need to initialize a disk:

1. Select a disk to initialize.
2. Right-click on the selected volume, and then click **Initialize** in the context menu. You will be forwarded to the **Disk Initialization** window, that will provide the basic hardware details such as the disk's number, capacity and state to aid you in the choice of your possible action.
3. In the window, you will be able to set the disk partitioning scheme (MBR or GPT) and the disk type (basic or dynamic). The new disk state will be graphically represented in the **Disk Management** view of the console immediately.
4. By clicking **OK**, you'll add a pending operation of the disk initialization.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

After the initialization, all the disk space remains unallocated and so still impossible to be used for program installation or file storage. To be able to use it, proceed normally to the **Create volume** operation.

If you decide to change the disk settings it can be done later using the standard Acronis Disk Director Lite disk tools.

5.9.6.2 Basic disk cloning

Sometimes it is necessary to transfer all the disk data onto a new disk. It can be a case of expanding the system volume, starting a new system layout or disk evacuation due to a hardware fault. In any case, the reason for the **Clone basic disk** operation can be summed up as the necessity to transfer all the source disk data to a target disk exactly as it is.

Acronis Disk Director Lite allows the operation to be carried out to basic MBR disks only.

To plan the **Clone basic disk** operation:

1. Select a disk you want to clone.
2. Select a disk as target for the cloning operation.
3. Select a cloning method and specify advanced options.

The new volume structure will be graphically represented in the **Disk management** view immediately.

It is advisable that you deactivate Acronis Startup Recovery Manager, if it is active, before cloning a system disk. Otherwise the cloned operating system might not boot. You can activate the Acronis Startup Recovery Manager again after the cloning is completed. If deactivation is not possible, choose the **As is** method to clone the disk.

Selecting source and target disks

The program displays a list of partitioned disks and asks the user to select the source disk, from which data will be transferred to another disk.

The next step is selection of a disk as target for the cloning operation. The program enables the user to select a disk if its size will be sufficient to hold all the data from the source disk without any loss.

If there is some data on the disk that was chosen as the target, the user will receive a warning: “**The selected target disk is not empty. The data on its volumes will be overwritten.**”, meaning that all the data currently located on the chosen target disk will be lost irrevocably.

Cloning method and advanced options

The **Clone basic disk** operation usually means that the information from the source disk is transferred to the target “**As is**”. So, if the destination disk is the same size and even if it is larger, it is possible to transfer all the information there exactly as it is stored at the source.

But with the wide range of available hardware it is normal that the target disk would differ in size from the source. If the destination is larger, then it would be advisable to resize the source disk volumes to avoid leaving unallocated space on the target disk by selecting the **Proportionally resize volumes** option. The option to **Clone basic disk** “as is” remains, but the default method of cloning will be carried out with proportional enlargement of all the **source** disk volumes so that no unallocated space remains on the **target** disk .

If the destination is smaller, then the **As is** option of cloning will be unavailable and proportional resizing of the **source** disk volumes will be mandatory. The program analyzes the **target** disk to establish whether its size will be sufficient to hold all the data from the **source** disk without any loss. If such transfer with proportional resizing of the **source** disk volumes is possible, but without any data loss , then the user will be allowed to proceed. If due to the size limitations safe transfer of all the **source** disk data to the **target** disk is impossible even with the proportional resizing of the

volumes, then the **Clone basic disk** operation will be impossible and the user will not be able to continue.

If you are about to clone a disk comprising of a **system volume**, pay attention to the **Advanced options**.

By clicking **Finish**, you'll add the pending operation of the disk cloning.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

Using advanced options

When cloning a disk comprising of a **system volume**, you need to retain an operating system bootability on the target disk volume. It means that the operating system must have the system volume information (e.g. volume letter) matched with the disk NT signature, which is kept in the MBR disk record. But two disks with the same NT signature cannot work properly under one operating system.

If there are two disks having the same NT signature and comprising of a system volume on a machine, at the startup the operating system runs from the first disk, discovers the same signature on the second one, automatically generates a new unique NT signature and assigns it to the second disk. As a result, all the volumes on the second disk will lose their letters, all paths will be invalid on the disk, and programs won't find their files. The operating system on that disk will be unbootable.

You have the following two alternatives to retain system bootability on the target disk volume:

1. Copy NT signature – to provide the target disk with the source disk NT signature matched with the Registry keys also copied on the target disk.
2. Leave NT signature – to keep the old target disk signature and update the operating system according to the signature.

If you need to copy the NT signature:

1. Select the **Copy NT signature** check box. You receive the warning: “If there is an operating system on the hard disk, uninstall either the source or the target hard disk drive from your machine prior to starting the machine again. Otherwise, the OS will start from the first of the two, and the OS on the second disk will become unbootable.” The **Turn off the machine after the cloning operation** check box is selected and disabled automatically.
2. Click **Finish** to add the pending operation.
3. Click **Commit** on the toolbar and then click **Proceed** in the **Pending Operations** window.
4. Wait until the task is finished.
5. Wait until the machine is turned off.
6. Disconnect either the source or the target hard disk drive from the machine.
7. Start up the machine.

If you need to leave an NT signature:

1. Click to clear the **Copy NT signature** check box, if necessary.
2. Click to clear the **Turn off the machine after the cloning operation** check box, if necessary.
3. Click **Finish** to add the pending operation.
4. Click **Commit** on the toolbar and then click **Proceed** in the **Pending Operations** window.
5. Wait until the task is finished.

5.9.6.3 Disk conversion: MBR to GPT

You would want to convert an MBR basic disk to a GPT basic disk in the following cases:

- If you need more than 4 primary volumes on one disk.
- If you need additional disk reliability against any possible data damage.

If you need to convert a basic MBR disk to basic GPT:

1. Select a basic MBR disk to convert to GPT.
2. Right-click on the selected volume, and then click **Convert to GPT** in the context menu.
You will receive a warning window, stating that you are about to convert MBR into GPT.
3. By clicking **OK**, you'll add a pending operation of MBR to GPT disk conversion.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

Please note: A GPT-partitioned disk reserves the space in the end of the partitioned area necessary for the backup area, which stores copies of the GPT header and the partition table. If the disk is full and the volume size cannot be automatically decreased, the conversion operation of the MBR disk to GPT will fail.

The operation is irreversible. If you have a primary volume, belonging to an MBR disk, and convert the disk first to GPT and then back to MBR, the volume will be logical and will not be able to be used as a system volume.

If you plan to install an OS that does not support GPT disks, the reverse conversion of the disk to MBR is also possible through the same menu items the name of the operation will be listed as **Convert to MBR**.

Dynamic disk conversion: MBR to GPT

Acronis Disk Director Lite does not support direct MBR to GPT conversion for dynamic disks. However you can perform the following conversions to reach the goal using the program:

1. MBR disk conversion: dynamic to basic using the **Convert to basic** operation.
2. Basic disk conversion: MBR to GPT using the **Convert to GPT** operation.
3. GPT disk conversion: basic to dynamic using the **Convert to dynamic** operation.

5.9.6.4 Disk conversion: GPT to MBR

If you plan to install an OS that does not support GPT disks, conversion of the GPT disk to MBR is possible the name of the operation will be listed as **Convert to MBR**.

If you need to convert a GPT disk to MBR:

1. Select a GPT disk to convert to MBR.
2. Right-click on the selected volume, and then click **Convert to MBR** in the context menu.
You will receive a warning window, stating that you are about to convert GPT into MBR.
You will be explained the changes that will happen to the system after the chosen disk is converted from GPT to MBR. E.g. if such conversion will stop a disk from being accessed by the system, the operating system will stop loading after such conversion or some volumes on the selected GPT disk will not be accessible with MBR (e.g. volumes located more than 2 TB from the beginning of the disk) you will be warned here about such damage.

Please note, a volume, belonging to a GPT disk to convert, will be a logical one after the operation and is irreversible.

3. By clicking **OK**, you'll add a pending operation of GPT to MBR disk conversion.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

5.9.6.5 Disk conversion: basic to dynamic

You would want to convert a basic disk to dynamic in the following cases:

- If you plan to use the disk as part of a dynamic disk group.
- If you want to achieve additional disk reliability for data storage.

If you need to convert a basic disk to dynamic:

1. Select the basic disk to convert to dynamic.
2. Right-click on the selected volume, and then click **Convert to dynamic** in the context menu. You will receive a final warning about the basic disk being converted to dynamic.
3. If you click **OK** in this warning window, the conversion will be performed immediately and if necessary, your machine will be restarted.

Please note: A dynamic disk occupies the last megabyte of the physical disk to store the database, including the four-level description (Volume-Component-Partition-Disk) for each dynamic volume. If during the conversion to dynamic it turns out that the basic disk is full and the size of its volumes cannot be decreased automatically, the basic disk to dynamic conversion operation will fail.

Should you decide to revert your dynamic disks back to basic ones, e.g. if you want to start using an OS on your machine that does not support dynamic disks, you can convert your disks using the same menu items, though the operation now will be named **Convert to basic**.

System disk conversion

Acronis Disk Director Lite does not require an operating system reboot after basic to dynamic conversion of the disk, if:

1. There is a single Windows 2008/Vista operating system installed on the disk.
2. The machine runs this operating system.

Basic to dynamic conversion of the disk, comprising of system volumes, takes a certain amount of time, and any power loss, unintentional turning off of the machine or accidental pressing of the Reset button during the procedure could result in bootability loss.

In contrast to Windows Disk Manager the program ensures bootability of an **offline operating system** on the disk after the operation.

5.9.6.6 Disk conversion: dynamic to basic

You would want to convert dynamic disks back to basic ones, e.g. if you want to start using an OS on your machine that does not support dynamic disks.

If you need to convert a dynamic disk to basic:

1. Select the dynamic disk to convert to basic.
2. Right-click on the selected volume, and then click **Convert to basic** in the context menu. You will receive a final warning about the dynamic disk being converted to basic.

You will be advised about the changes that will happen to the system if the chosen disk is converted from dynamic into basic. E.g. if such a conversion will stop the disk from being accessed by the system, the operating system will stop loading after such conversion, or if the disk you want to convert to basic contains any volumes of the types that are only supported by

dynamic disks (all volume types except Simple volumes), then you will be warned here about the possible damage to the data involved in the conversion.

Please note, the operation is unavailable for a dynamic disk containing Spanned, Striped, or RAID-5 volumes.

3. If you click **OK** in this warning window, the conversion will be performed immediately.

After the conversion the last 8Mb of disk space is reserved for the future conversion of the disk from basic to dynamic.

In some cases the possible unallocated space and the proposed maximum volume size might differ (e.g. when the size of one mirror establishes the size of the other mirror, or the last 8Mb of disk space are reserved for the future conversion of the disk from basic to dynamic).

System disk conversion

Acronis Disk Director Lite does not require an operating system reboot after dynamic to basic conversion of the disk, if:

1. There is a single Windows 2008/Vista operating system installed on the disk.
2. The machine runs this operating system.

Dynamic to basic conversion of the disk, comprising of system volumes, takes a certain amount of time, and any power loss, unintentional turning off of the machine or accidental pressing of the Reset button during the procedure could result in bootability loss.

In contrast to Windows Disk Manager the program ensures:

- safe conversion of a dynamic disk to basic when it contains volumes **with data** for simple and mirrored volumes
- in multiboot systems, bootability of a system that was **offline** during the operation

5.9.6.7 Changing disk status

Changing disk status is effective for Windows Vista SP1, Windows Server 2008, Windows 7 operating systems and applies to the current disk layout (p. 108).

One of the following disk statuses always appears in the graphical view of the disk next to the disk's name:

- **Online**

The online status means that a disk is accessible in the read-write mode. This is the normal disk status. If you need a disk to be accessible in the read-only mode, select the disk and then change its status to offline by selecting **Change disk status to offline** from the **Operations** menu.

- **Offline**

The offline status means that a disk is accessible in the read-only mode. To bring the selected offline disk back to online, select **Change disk status to online** from the **Operations** menu.

If the disk has the offline status and the disk's name is **Missing**, this means that the disk cannot be located or identified by the operating system. It may be corrupted, disconnected, or powered off. For information on how to bring a disk that is offline and missing back online, please refer to the following Microsoft knowledge base article: <http://technet.microsoft.com/en-us/library/cc732026.aspx>.

5.9.7 Volume operations

Acronis Disk Director Lite includes the following operations that can be performed on volumes:

- Create Volume - Creates a new volume with the help of the Create Volume Wizard.
- Delete Volume - Deletes the selected volume.
- Set Active (p. 119) - Sets the selected volume Active so that the machine will be able to boot with the OS installed there.
- Change Letter (p. 119) - Changes the selected volume letter
- Change Label (p. 120) - Changes the selected volume label
- Format Volume (p. 120) - Formats a volume giving it the necessary file system

Acronis Disk Director Lite must obtain exclusive access to the target volume. This means no other disk management utilities (like Windows Disk Management utility) can access it at that time. If you receive a message stating that the volume cannot be blocked, close the disk management applications that use this volume and start again. If you can not determine which applications use the volume, close them all.

5.9.7.1 Creating a volume

You might need a new volume to:

- Recover a previously saved backup copy in the “exactly as was” configuration;
- Store collections of similar files separately — for example, an MP3 collection or video files on a separate volume;
- Store backups (images) of other volumes/disks on a special volume;
- Install a new operating system (or swap file) on a new volume;
- Add new hardware to a machine.

In Acronis Disk Director Lite the tool for creating volumes is the **Create volume Wizard**.

Types of dynamic volumes

Simple Volume

A volume created from free space on a single physical disk. It can consist of one region on the disk or several regions, virtually united by the Logical Disk Manager (LDM). It provides no additional reliability, no speed improvement, nor extra size.

Spanned Volume

A volume created from free disk space virtually linked together by the LDM from several physical disks. Up to 32 disks can be included into one volume, thus overcoming the hardware size limitations, but if at least one disk fails, all data will be lost, and no part of a spanned volume may be removed without destroying the entire volume. So, a spanned volume provides no additional reliability, nor a better I/O rate.

Striped Volume

A volume, also sometimes called RAID 0, consisting of equal sized stripes of data, written across each disk in the volume; it means that to create a striped volume, a user will need two or more dynamic disks. The disks in a striped volume don't have to be identical, but there must be unused space available on each disk that you want to include in the volume and the size of the volume will depend on the size of the smallest space. Access to the data on a striped volume is usually faster than access to the same data on a single physical disk, because the I/O is spread across more than one disk.

Striped volumes are created for improved performance, not for their better reliability - they do not contain redundant information.

Mirrored Volume

A fault-tolerant volume, also sometimes called RAID 1, whose data is duplicated on two identical physical disks. All of the data on one disk is copied to another disk to provide data redundancy. Almost any volume can be mirrored, including the system and boot volumes, and if one of the disks fails, the data can still be accessed from the remaining disks. Unfortunately, the hardware limitations on size and performance are even more severe with the use of mirrored volumes.

Mirrored-Striped Volume

A fault-tolerant volume, also sometimes called RAID 1+0, combining the advantage of the high I/O speed of the striped layout and redundancy of the mirror type. The evident disadvantage remains inherent with the mirror architecture - a low disk-to-volume size ratio.

RAID-5

A fault-tolerant volume whose data is striped across an array of three or more disks. The disks do not need to be identical, but there must be equally sized blocks of unallocated space available on each disk in the volume. Parity (a calculated value that can be used to reconstruct data in case of failure) is also striped across the disk array. And it is always stored on a different disk than the data itself. If a physical disk fails, the portion of the RAID-5 volume that was on that failed disk can be re-created from the remaining data and the parity. A RAID-5 volume provides reliability and is able to overcome the physical disk size limitations with a higher than mirrored disk-to-volume size ratio.

Create volume wizard

The **Create volume** wizard lets you create any type of volume (including system and active), select a file system, label, assign a letter, and also provides other disk management functions.

Its pages will enable you to enter operation parameters, proceeding step-by-step further on and return to any previous step if necessary to change any previously selected options. To help you with your choices, each parameter is supplemented with detailed instructions.

If you want to create a volume:

Run the **Create volume** wizard by selecting **Create volume** on the **Wizards** bar, or right-click any unallocated space and select **Create volume** in the appearing context menu.

Select the type of volume being created

At the first step you have to specify the type of volume you want to create. The following types of volume are available:

- Basic
- Simple/Spanned
- Striped
- Mirrored
- RAID-5

You will obtain a brief description of every type of volume for better understanding of the advantages and limitations of each possible volume architecture.

*If the current operating system, installed on this machine, does not support the selected type of volume, you will receive the appropriate warning. In this case the **Next** button will be disabled and you will have to select another type of volume to proceed with the new volume creation.*

After you click the **Next** button, you will proceed forward to the next wizard page: Select destination disks (p. 117).

Select destination disks

The next wizard page will prompt you to choose the disks, whose space will be used for the volume creation.

To create a basic volume:

- Select a destination disk and specify the unallocated space to create the basic volume on.

To create a Simple/Spanned volume:

- Select one or more destination disks to create the volume on.

To create a Mirrored volume:

- Select two destination disks to create the volume on.

To create a Striped volume:

- Select two or more destination disks to create the volume on.

To create a RAID-5 volume:

- Select three destination disks to create the volume on.

After you choose the disks, the wizard will calculate the maximum size of the resulting volume, depending on the size of the unallocated space on the disks you chose and the requirements of the volume type you have previously decided upon.

If you are creating a **dynamic** volume and select one or several **basic** disks, as its destination, you will receive a warning that the selected disk will be converted to dynamic automatically.

If need be, you will be prompted to add the necessary number of disks to your selection, according to the chosen type of the future volume.

If you click the **Back** button, you will be returned to the previous page: Select the type of volume being created (p. 116).

If you click the **Next** button, you will proceed to the next page: Set the volume size (p. 117).

Set the volume size

On the third wizard page, you will be able to define the size of the future volume, according to the previously made selections. In order to choose the necessary size between the minimum and the maximum values, use the slider or enter the necessary values into the special windows between the minimum and the maximum values or click on the special handle, and hold and drag the borders of the disk's picture with the cursor.

The maximum value normally includes the most possible unallocated space. But in some cases the possible unallocated space and the proposed maximum volume size might differ (e.g. when the size of one mirror establishes the size of the other mirror, or the last 8Mb of the disk space is reserved for the future conversion of the disk from basic to dynamic).

For basic volumes if some unallocated space is left on the disk, you also will be able to choose the position of the new volume on the disk.

If you click the **Back** button, you will be returned to the previous page: Select destination disks (p. 117).

If you click the **Next** button, you will proceed to the next page: Set the volume options (p. 118).

Set the volume options

On the next wizard page you can assign the volume **Letter** (by default - the first free letter of the alphabet) and, optionally, a **Label** (by default – none). Here you will also specify the **File system** and the **Cluster size**.

The wizard will prompt you to choose one of the Windows file systems: FAT16 (disabled, if the volume size has been set at more than 2 GB), FAT32 (disabled, if the volume size has been set at more than 2 TB), NTFS or to leave the volume **Unformatted**.

In setting the cluster size you can choose between any number in the preset amount for each file system. Note, the program suggests the cluster size best suited to the volume with the chosen file system.

If you are creating a basic volume, which can be made into a system volume, this page will be different, giving you the opportunity to select the volume **Type** — **Primary (Active Primary)** or **Logical**.

Typically **Primary** is selected to install an operating system to a volume. Select the **Active** (default) value if you want to install an operating system on this volume to boot at machine startup. If the **Primary** button is not selected, the **Active** option will be inactive. If the volume is intended for data storage, select **Logical**.

*A Basic disk can contain up to four primary volumes. If they already exist, the disk will have to be converted into dynamic, otherwise or **Active** and **Primary** options will be disabled and you will only be able to select the **Logical** volume type. The warning message will advise you that an OS installed on this volume will not be bootable.*

*If you use characters when setting a new volume label that are unsupported by the currently installed operation system, you will get the appropriate warning and the **Next** button will be disabled. You will have to change the label to proceed with the creation of the new volume.*

If you click the **Back** button, you will be returned to the previous page: Set the volume size (p. 117).

If you click the **Finish** button, you will complete the operation planning.

To perform the planned operation click **Commit** in the toolbar, and then click **Proceed** in the **Pending Operations** window.

If you set a 64K cluster size for FAT16/FAT32 or on 8KB-64KB cluster size for NTFS, Windows can mount the volume, but some programs (e.g. Setup programs) might calculate its disk space incorrectly.

5.9.7.2 Delete volume

After a volume is deleted, its space is added to unallocated disk space. It can be used for creation of a new volume or to change another volume's type.

If you need to delete a volume:

1. Select a hard disk and a volume to be deleted.

2. Select **Delete volume** or a similar item in the **Operations** sidebar list, or click the **Delete the selected volume** icon on the toolbar.

If the volume contains any data, you will receive the warning, that all the information on this volume will be lost irrevocably.

3. By clicking **OK** in the **Delete volume** window, you'll add the pending operation of volume deletion.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

5.9.7.3 Set active volume

If you have several primary volumes, you must specify one to be the boot volume. For this, you can set a volume to become active. A disk can have only one active volume, so if you set a volume as active, the volume, which was active before, will be automatically unset.

If you need to set a volume active:

1. Select a primary volume on a basic MBR disk to set as active.
2. Right-click on the selected volume, and then click **Mark as active** in the context menu.
If there is no other active volume in the system, the pending operation of setting active volume will be added.

Please note, that due to setting the new active volume, the former active volume letter might be changed and some of the installed programs might stop running.

3. If another active volume is present in the system, you will receive the warning that the previous active volume will have to be set passive first. By clicking **OK** in the **Warning** window, you'll add the pending operation of setting active volume.

Please note: even if you have the Operating System on the new active volume, in some cases the machine will not be able to boot from it. You will have to confirm your decision to set the new volume as active.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

The new volume structure will be graphically represented in the **Disk management** view immediately.

5.9.7.4 Change volume letter

Windows operating systems assign letters (C:, D:, etc) to hard disk volumes at startup. These letters are used by applications and operating systems to locate files and folders in the volumes.

Connecting an additional disk, as well as creating or deleting a volume on existing disks, might change your system configuration. As a result, some applications might stop working normally or user files might not be automatically found and opened. To prevent this, you can manually change the letters that are automatically assigned to the volumes by the operating system.

If you need to change a letter assigned to a volume by the operating system:

1. Select a volume to change a letter.
2. Right-click on the selected volume, and then click **Change letter** in the context menu.
3. Select a new letter in the **Change Letter** window.
4. By clicking **OK** in the **Change Letter** window, you'll add a pending operation to volume letter assignment.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

The new volume structure will be graphically represented in the **Disk management** view immediately.

5.9.7.5 Change volume label

The volume label is an optional attribute. It is a name assigned to a volume for easier recognition. For example, one volume could be called SYSTEM — a volume with an operating system, or PROGRAM — an application volume, DATA — a data volume, etc., but it does not imply that only the type of data stated with the label could be stored on such a volume.

In Windows, volume labels are shown in the Explorer disk and folder tree: LABEL1(C:), LABEL2(D:), LABEL3(E:), etc. LABEL1, LABEL2 and LABEL3 are volume labels. A volume label is shown in all application dialog boxes for opening and saving files.

If you need to change a volume label:

1. Right-click on the selected volume, and then click **Change label**.
2. Enter a new label in the **Change label** window text field.
3. By clicking **OK** in the **Change label** window, you'll add the pending operation of changing the volume label .

*If when setting a new volume label you use characters that are unsupported by the currently installed operating system, you will get the appropriate warning and the **OK** button will be disabled. You will have to use only supported characters to proceed with changing the volume label.*

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

The new label will be graphically represented in the **Disk Management** view of the console immediately.

5.9.7.6 Format volume

You might want to format a volume if you want to change its file system:

- to save additional space which is being lost due to the cluster size on the FAT16 or FAT32 file systems
- as a quick and more or less reliable way of destroying data, residing in this volume

If you want to format a volume:

1. Select a volume to format.
2. Right-click on the selected volume, and then click **Format** in the context menu.

You will be forwarded to the **Format Volume** window, where you will be able to set the new file system options. You can choose one of the Windows file systems: FAT16 (disabled, if the Volume Size is more than 2 GB), FAT32 (disabled, if the Volume Size is more than 2 TB) or NTFS.

In the text window you will be able to enter the volume label, if necessary: by default this window is empty.

In setting the cluster size you can choose between any number in the preset amount for each file system. Note, the program suggests the cluster size best suited to the volume with the chosen file system.

3. If you click **OK** to proceed with the **Format Volume** operation, you'll add a pending operation of formatting a volume.

(To finish the added operation you will have to commit it. Exiting the program without committing the pending operations will effectively cancel them.)

The new volume structure will be graphically represented in the **Disk management** view.

If you set a 64K cluster size for FAT16/FAT32 or an 8KB-64KB cluster size for NTFS, Windows can mount the volume, but some programs (e.g. Setup programs) might calculate its disk space incorrectly.

5.9.8 Pending operations

All operations, which were prepared by the user in manual mode or with the aid of a wizard, are considered pending until the user issues the specific command for the changes to be made permanent. Until then, Acronis Disk Director Lite will only demonstrate the new volume structure that will result from the operations that have been planned to be performed on disks and volumes. This approach enables you to control all planned operations, double-check the intended changes, and, if necessary, cancel operations before they are executed.

To prevent you from performing any unintentional change on your disk, the program will first display the list of all pending operations.

The **Disk management** view contains the toolbar with icons to launch the **Undo**, **Redo** and **Commit** actions intended for pending operations. These actions might also be launched from the **Disk management** menu of the console.

All planned operations are added to the pending operation list.

The **Undo** action lets you undo the latest operation in the list. While the list is not empty, this action is available.

The **Redo** action lets you reinstate the last pending operation that was undone.

The **Commit** action forwards you to the **Pending Operations** window, where you will be able to view the pending operation list. Clicking **Proceed** will launch their execution. You will not be able to undo any actions or operations after you choose the **Proceed** operation. You can also cancel the commitment by clicking **Cancel**. Then no changes will be done to the pending operation list.

Quitting Acronis Disk Director Lite without committing the pending operations effectively cancels them, so if you try to exit **Disk management** without committing the pending operations, you will receive the appropriate warning.

5.10 Collecting system information

The system information collection tool gathers information about the machine to which the management console is connected, and saves it to a file. You may want to provide this file when contacting Acronis technical support.

This option is available under bootable media and for machines where Agent for Windows is installed.

To collect system information

1. In the management console, select from the top menu **Help > Collect system information from 'machine name'**.
2. Specify where to save the file with system information.

6 Command-line mode and scripting in Windows

Acronis Backup & Recovery Server OEM supports the command-line mode and enables backup automation by executing XML scripts.

The following features are available:

1. Ability to use the before/after data capture commands.
2. Ability to use the VSS support option.
3. Ability to check for a license on the license server with the /ls_check command.
4. Ability to use file exclusion at disk backup.

Command line mode limitations

The command-line mode functionality is somewhat limited as compared to the GUI mode. You will not be able to perform operations that require:

- the reboot of the system, such as restore a system volume or clone a system disk
- a user interaction, such as inserting removable media (CD, DVD or tape) - the operation fails if there is no media in the drive or the inserted media is full.

These operations only can be done through the GUI.

Scripting is intended only for backup.

6.1 Agent for Windows command-line utility

An administrator might need a console interface in some situations. Acronis Backup & Recovery Server OEM supports this mode with trueimagecmd.exe utility. The file is located in the folder where Acronis Backup & Recovery Server OEM Agent for Windows has been installed, by default it is C:\Program Files\Acronis\BackupAndRecovery.

This utility is also available when operating under the PE-based bootable media.

6.1.1 Supported commands

trueimagecmd has the following format:

```
trueimagecmd /command /option1 /option2...
```

Commands may be accompanied with options. Some options are common for most trueimagecmd commands, while others are specific for individual commands. Below is a list of supported commands and compatible options.

Command	Common Options	Specific Options
create Creates an image of specified disks and partitions	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password]	/harddisk:[disk number] /partition:[partition number] /file_partition:[partition letter] /raw /exclude_names:[names] /exclude_masks:[masks] /exclude_system /exclude_hidden /before:[pre-data capture command] /after:[post-data capture command]

	/incremental /compression:[0...9] /split:[size in MB] /oss_numbers /progress:[on off] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/use_vss
deploy Restores disks and partitions, except for the MBR, from an image	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/file_partition:[partition letter] /harddisk:[disk number] /partition:[partition number] /target_harddisk:[disk number] /target_partition:[partition number] /start:[start sector] /size:[partition size in sectors] /fat16_32 /type:[active primary logical] /preserve_mbr
deploy_mbr Restores the MBR from a disk or partition image	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/harddisk:[disk number] /target_harddisk:[disk number]
filerestore Restores files and folders from a file archive	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/target_folder:[target folder] /overwrite:[older never always] /restore_security:[on off] /original_date:[on off]

verify Verifies the archive data integrity	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	
pit_info Displays the numbered list of backups, contained in the specified archive	/filename:[file name] /password:[password] /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password]	
export Creates a copy of an archive or a self-sufficient part copy of an archive in the location you specify	/vault:[path] /arc:[archive name] /arc_id:[archive id] /include_pits:[pits numbers] /password:[password] /ftp_user:[username] /ftp_password:[password] /progress:[on off] /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/net_src_user:[username] /net_src_password:[password] /ftp_src_user:[username] /ftp_src_password:[password] /target_vault:[target path] /target_arc:[target archive name] /net_user:[username] /net_password:[password]
list Lists available drives and partitions. When used with the filename option, it lists the image contents. When used with the vault option, it lists archives located in the specified location. When the arc , or the arc_id option is added, it lists all backups contained in the archive.	/password:[password] /index:N /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password]	/filename:[file name] /vault:[path] /arc:[archive name] /arc_id:[archive id]
explore Connects an image as a virtual drive	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name]* /password:[password] /asz:[number of archive]	/partition:[partition number] /letter:X

	/index:N /net_user:[username] /net_password:[password] /log:[file name] /log_net_user:[remote user] /log_net_password:[password] *for a split image, the name of the last created file	
unplug Disconnects the image connected as a virtual drive		/letter:X /letter:all
asz_create Creates the Acronis Secure Zone on the selected drive	/password:[password] /oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/harddisk:X /partition:[partition number] /size:[ASZ size in sectors unallocated]
asz_content Displays the Acronis Secure Zone size, free space and contents	/password:[password]	
asz_files Displays the Acronis Secure Zone size, free space and contents using the generated file names	/password:[password]	
asz_delete_files Deletes the most recent backup in the archive located in the Acronis Secure Zone	/filename:[file name] /password:[password] /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	
asz_delete Deletes the Acronis Secure Zone	/password:[password] /oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password]	/partition:[partition number]
asrm_activate Activates the Acronis Startup Recovery Manager		
asrm_deactivate Deactivates the Acronis Startup Recovery Manager		

clone Clones a hard disk	/reboot	/harddisk:[disk number] /target_harddisk:[disk number]
help Shows usage		
ls_check Checks if there are licenses for the local machine on the license server		

6.1.2 Common options

6.1.2.1 Access to archives

vault:[path]

Specifies a path to the location that contains the archive. Used in combination with the **arc**, or the **arc_id** option.

The following locations are supported:

- Local folders, e.g.: /vault:C:\Test, or /vault:"C:\Test 1"
- Network folders, e.g.: /vault:\\ServerA\Share\
- Managed vaults (for advanced product editions only), e.g.: /vault:bsp://StorageNode/VaultName
- FTP and SFTP, e.g.: /vault:ftp://ServerA/Folder1
- CD, DVD – with the path specified as a local path, e.g.: /vault:F:\
- Acronis Secure Zone, e.g.: /vault:atis:///asz
- Tapes, e.g.: /vault:atis:///tape?0
- Unmanaged vaults are specified by their path. For example, if a vault is located in a folder, specify the path to that folder.

If the **vault** option is specified the **filename** option is ignored.

arc:[archive name]

The name of the archive. If not specified, the **arc_id** option is used. If both the **arc** and **arc_id** options are specified, the **arc_id** option is used.

arc_id:[archive id]

Specifies the Universally Unique Identifier (UUID) of the archive, e.g.:

```
/arc_id:183DE307-BC97-45CE-9AF7-60945A568BE8
```

If not specified, the **arc** option is used. If both options are specified, the **arc_id** option is used.

filename:[file name]

- a) Backup file name, if the archive location is other than ASZ.

b) Archive name, when restoring or deleting files from ASZ. Can be obtained with `asz_files`.

If the **vault** option is specified the **filename** option is ignored.

`password:[password]`

a) Password for the archive, if the archive location is other than ASZ.

b) Password for the ASZ, if archive location is ASZ.

`asz:[number of archive]`

Addresses to the ASZ and selects the archive (a full backup with or without increments).

To get the archive number, use **asz_content**.

`index:N`

N = Number of the backup in an archive:

- 1 = basic full backup
- 2 = 1st increment... and so on
- 0 (default) = latest increment

Selects a backup in a sequence of incremental backups inside the archive.

To get a backup index from the ASZ, use **asz_content**.

`include_pits:[pits numbers]`

Specifies the backups (pits) to be included in the archive copy. To get the numbers of pits, use **pit_info**. Separate multiple values with a comma, for example:

```
/include_pits:2,4,5
```

The "0" value means the last backup in the archive, for example:

```
/include_pits:0
```

If not specified the whole archive is selected.

`net_user:[username]`

Specify a user name for network drive access.

`net_password:[password]`

Specify a password for network drive access.

`ftp_user:[username]`

Specify a user name for access to an FTP server.

`ftp_password:[password]`

Specify a password for access to an FTP server.

6.1.2.2 Backup options

incremental

Set the backup type to incremental.

If not specified or there is no basic full backup, a full backup will be created.

compression:[0...9]

Specify the data compression level.

It ranges from 0 to 9 and is set to 3 by default.

split:[size in MB]

Split the backup into parts of the specified size, if the archive location is other than ASZ.

6.1.2.3 General options

oss_numbers

Declares that numbers of partitions in the `/partition` option are adjusted for the MBR partition table rather than just as ascending numbers. This means that primary partitions have numbers 1-1, 1-2, 1-3, 1-4; logical partitions numbers start with 1-5. For example, if the disk has one primary and two logical partitions, their numbers can appear as follows:

```
/partition:1-1,1-2,1-3
```

or

```
/oss_numbers /partition:1-1,1-5,1-6
```

reboot

Reboot the machine before the operation (if required) and after the operation is completed.

Use this option when performing any operation that requires a reboot: recovering a system disk, creating Acronis Secure Zone on a system disk, cloning a system disk. The machine will be rebooted automatically. To postpone the operation until a user reboots the system manually, add the **/later** option. With this option, the operation will be performed after the user initiates a reboot.

The **/reboot** option can be used with operations that do not necessarily require a reboot. Examples of such operations are recovery under bootable media, recovering files that are not locked by the operating system, most cases of backup, archive validation. In those cases a reboot will be performed after the operation is completed. The **/later** option does not have sense.

The following table summarizes the software behavior with and without the **/reboot** and **/later** options.

	Reboot is necessary	Reboot is not required
/reboot /later	2 reboots, the 1st one is postponed	1 reboot after operation
/reboot	2 reboots	1 reboot after operation

no option	No reboot, operation fails	No reboot, operation succeeds
------------------	----------------------------	-------------------------------

log:[file name]

Create a log file of the current operation with the specified file name. Please note, logs can be saved only to a network share.

log_net_user:[remote user]

If the log file is created on a network share, include the user name for logon to the share.

log_net_password:[password]

If the log file is created on a network share, include the password for logon to the share.

progress:[on | off]

Shows/hides the progress information (percent completed). It is shown by default.

6.1.3 Specific options

6.1.3.1 create

harddisk:[disk number]

Specifies the hard disks to include into the image file. The list of available hard disks is provided by the `/list` command. An image may contain data of more than one hard disk. In that case, separate disk numbers by commas, e.g.:

```
/harddisk:1,3
```

By specifying

```
/harddisk:DYN
```

you will back up all dynamic volumes present in the system.

partition:[partition number]

Specifies the partitions to include into the image file. The list of available partitions is provided by `/list`. Partition numbers are specified as **<disk number>-<partition number>**, e.g.:

```
/partition:1-1,1-2,3-1
```

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/partition:DYN1,DYN2
```

Both basic partitions and dynamic volumes can be specified by their letters, for example:

```
/partition:"C"
```

Mixed notation is also acceptable, for example:

```
/partition:1-1,"D"
```

file_partition:[partition letter]

Specifies the partition where the image file will be stored (by letter or number). This option is used with **filename:[file_name]**. In that case the file name must be specified without a drive letter or root folder. For example:

```
/file_partition:D /filename:"\1.tib"
```

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/file_partition:DYN1 /filename:"\1.tib"
```

raw

Use this option to create an image of a disk (partition) with an unrecognized or unsupported file system. This will copy all disk/partition contents sector-by-sector. Without this option only the sectors containing useful system and user data are imaged (for the supported file systems).

exclude_names:[names]

Files and folders to be excluded from the backup (comma separated). For example:

```
/exclude_names:E:\MyProject\111.doc,E:\MyProject\Old
```

exclude_masks:[masks]

Applies masks to select files to be excluded from the backup. Use the common Windows masking rules. For example, to exclude all files with extension **.exe**, add ***.exe**. **My???.exe** will exclude all **.exe** files with names consisting of five symbols and starting with "my".

exclude_hidden

Excludes all hidden files from the backup.

before:[pre-data capture command]

Enables to define the command to be automatically executed before data capture at the beginning of the backup procedure. For example:

```
/before:"net stop MSSQLSERVER"
```

after:[post-data capture command]

Enables to define the command to be automatically executed after data capture at the beginning of the backup procedure. For example:

```
/after:"net start MSSQLSERVER"
```

use_vss

Notifies the VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications, in particular, completion of all database transactions, at the moment of taking the data snapshot. The data consistency, in turn, ensures that the application will be recovered in the correct state and become operational immediately after recovery.

6.1.3.2 deploy

file_partition:[partition letter]

Specifies the partition where the image file will be stored (by letter or number). This option is used with **filename:[file_name]**. In that case the file name must be specified without a drive letter or root folder. For example:

```
/file_partition:D /filename:"\1.tib"
```

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/file_partition:DYN1 /filename:"\1.tib"
```

harddisk:[disk number]

Specifies the basic hard disks to restore.

partition:[partition number]

Specifies the partitions to restore.

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/partition:DYN1
```

target_harddisk:[disk number]

Specifies the hard disk number where the image will be restored.

By specifying

```
/target_harddisk:DYN
```

you will select unallocated space on all dynamic disks that are present in the system.

target_partition:[partition number]

Specifies the target partition number for restoring a partition over the existing one. If the option is not specified, the program assumes that the target partition number is the same as the partition number specified with the /partition option.

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/target_partition:DYN1
```

start:[start sector]

Sets the start sector for restoring a partition to the hard disk unallocated space.

size:[partition size in sectors]

Sets the new partition size (in sectors).

fat16_32

Enables the file system conversion from FAT16 to FAT32 if the partition size after recovery is likely to exceed 2 GB. Without this option, the recovered partition will inherit the file system from the image.

type:[active | primary | logical]

Sets the restored partition active, primary or logical, if possible (for example, there cannot be more than four primary partitions on the disk). Setting a partition active always sets it primary, while a partition set primary may remain inactive.

If the type is not specified, the program tries to keep the target partition type. If the target partition is active, the restored partition is set active. If the target partition is primary, and there are other primary partitions on the disk, one of them will be set active, while the restored partition becomes primary. If no other primary partitions remain on the disk, the restored partition is set active.

When restoring a partition on unallocated space, the program extracts the partition type from the image. For the primary partition, the type will be set as follows:

- if the target disk is the 1st according to BIOS and it has no other primary partitions, the restored partition will be set active
- if the target disk is the 1st according to BIOS and there are other primary partitions on it, the restored partition will be set logical
- if the target disk is not the 1st, the restored partition will be set logical.

preserve_mbr

When restoring a partition over an existing one, the target partition is deleted from the disk along with its entry in the target disk MBR. Then, with the **preserve_mbr** option, the restored partition's entry will occupy the upper empty position in the target disk MBR. Thus, the target disk MBR is preserved. If not specified, the restored partition's entry will occupy the same position as in the source disk MBR saved in the image. If the position is not empty, the existing entry will be moved to another position.

Options specific for Universal Restore

The following options are available when using the Universal Restore add-on to Acronis Backup & Recovery Server OEM.

ur_path:[path]

Specifies using Acronis Universal Restore and the path to the drivers storage.

ur_username:[username]

Specifies using Acronis Universal Restore and a user name.

When getting access to a place located on the remote computer, the *username* depends on the service which is used to get access to the remote resource. E.g. if the remote resource is a shared folder located on a workgroup computer, the *username* must contain the remote computer name ("Computer_name\User_name"). If the resource is located on an FTP-server the computer name is not required. When the target and local computer are members of different domains, the *username* must contain the name of the domain the target computer is the member of (e.g. "Domain_name\User_name").

ur_password:[pwd]

Specifies using Acronis Universal Restore and a password associated with the **ur_username** option value.

ur_driver:[inf-filename]

Specifies using Acronis Universal Restore and the mass-storage driver to be installed.

6.1.3.3 deploy_mbr

harddisk:[disk number]

Specifies the basic hard disk to restore the MBR from.

target_harddisk:[disk number]

Specifies the target hard disk where the MBR will be deployed to.

6.1.3.4 filerestore

target_folder:[target folder]

Specifies a folder where folders/files will be restored (a target folder). If not specified, the original path is re-created from the archive.

overwrite:[older | never | always]

This option allows you to keep useful data changes made since the backup being restored was done. Choose what to do if the target folder contains a file with the same name as in the archive:

- *older* – this will give priority to the most recent file modification, whether it be in the archive or on the disk.
- *never* – this will give the file on the hard disk unconditional priority over the archived file.
- *always* – this will give the archived file unconditional priority over the file on the hard disk.

If not specified, the files on the disk will always be replaced with the archived files.

restore_security:[on | off]

Specifies whether to restore files' security attributes (default) or whether the files will inherit the security settings of the folder where they will be restored.

original_date:[on | off]

Specifies whether to restore files' original date and time from the archive or whether to assign the current date and time to the restored files. If not specified, the current date is assigned.

6.1.3.5 consolidate

target_filename:[file name]

Specifies the path to and name of the archive copy to be created. If there are two or more backups (pits) in the copy, numbers will be added to their names.

`net_src_user:[username]`

Specifies the user name for logon to the network share to access the source archive.

`net_src_password:[password]`

Specifies the *password* for logon to the network share to access the source archive.

`net_user:[username]`

Specifies the user name for logon to the network share to save the resulting archive.

`net_password:[password]`

Specifies the *password* for logon to the network share to save the resulting archive.

6.1.3.6 export

`net_src_user:[username]`

Specifies the user name for logon to the network share to access the source archive.

`net_src_password:[password]`

Specifies the *password* for logon to the network share to access the source archive.

`ftp_src_user:[username]`

Specifies the user name for logon to the FTP/SFTP server to access the source archive.

`ftp_src_password:[password]`

Specifies the password for logon to the FTP/SFTP server to access the source archive.

`target_vault:[target path]`

Specifies a path to the target location to export the archive to.

The following target locations are supported:

- Local folders, e.g.: `/target_vault:C:\Test`, or `/vault:"C:\Test 1"`
- Network folders, e.g.: `/target_vault:\\ServerA\Share\`
- Managed vaults (for advanced product editions only), e.g.:
`/target_vault:bsp://StorageNode/VaultName`
- FTP and SFTP, e.g.: `/target_vault:ftp://ServerA/Folder1`
- CD, DVD – with the path specified as a local path, e.g.: `/target_vault:F:\`
- Acronis Secure Zone, e.g.: `/target_vault:atis:///asz`
- Tapes, e.g.: `/target_vault:atis:///tape?0`
- Unmanaged vaults are specified by their path. For example, if a vault is located in a folder, specify the path to that folder.

target_arc:[target archive name]

The name of the target archive. Has to be unique within the target folder. If there is an archive with the same name, the operation will fail.

net_user:[username]

Specifies the user name for logon to the network share to save the resulting archive.

net_password:[password]

Specifies the *password* for logon to the network share to save the resulting archive.

6.1.3.7 convert

target_filename:[file name]

Specifies the path to and name of the virtual disk file to be created. The file extension corresponds to the type of virtual machine to which the virtual disk will be added:

- VMware virtual machine - **.vmdk**
- MS virtual machine and Citrix XenServer - **.vhd**
- Parallels virtual machine - **.hdd**.

harddisk:[disk number]

Specifies the hard disks to convert by numbers. For each disk, a separate virtual disk will be created.

By specifying

```
/harddisk:DYN
```

you will convert all dynamic volumes that are present in the system.

vm_type:[vmware|esx|Microsoft|parallels]

The type of virtual machine to which the virtual disk will be added.

ur

Use when converting the image of a disk, containing Windows, and the resulting virtual disk is supposed to be bootable. With this key, the program will add drivers, necessary for the virtual machine type selected with the **vm_type** key, to the resulting virtual disk. If the image was taken from a virtual machine of the same type, normally the key is not needed.

Drivers for the virtual machine reside in the storage, defined by the registry key *HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\UniversalRestore\DriversPackPath*. In case the storage has been moved, please change the key or use the command **ur_path:[path]**.

ur_path:[path]

The same as **ur** with custom path to the virtual machine drivers storage.

6.1.3.8 list

filename:[file name]

With this option, the image contents are displayed.

When listing image contents, the partition numbers may not coincide with those in the drives/partitions list, if the image does not contain all the disk partitions. For example, if the image contains partitions 2-3 and 2-5, they will be listed as 2-1 and 2-2.

If the **deploy /partition** command cannot find a partition in the image by its physical number, use the **partition:<number in the image> /target_partition:<physical number of the target partition>** keys. For the above example, to restore partition 2-5 to its original place use:

```
/partition:2-2 /target_partition:2-5
```

If the **vault** option is specified the **filename** option is ignored.

vault:[path]

Specifies a path to the location whose archives you want to list. Along with archive names, it lists Universally Unique Identifiers (UUID) that are used with the **arc_id** option.

The following locations are supported:

- Local folders, e.g.: `/vault:C:\Test` , or `/vault:"C:\Test 1"`
- Network folders, e.g.: `/vault:\\ServerA\Share\`
- Managed vaults (for advanced product editions only), e.g.: `/vault:bsp://StorageNode/VaultName`
- FTP and SFTP, e.g.: `/vault:ftp://ServerA/Folder1`
- CD, DVD – with the path specified as a local path, e.g.: `/vault:F:\`
- Acronis Secure Zone, e.g.: `/vault:atis:///asz`
- Tapes, e.g.: `/vault:atis:///tape?0`
- Unmanaged vaults are specified by their path. For example, if a vault is located in a folder, specify the path to that folder.

If the **vault** option is specified the **filename** option is ignored.

arc:[archive name]

Used in combination with the **vault** option. Lists all backups contained in the archive.

If not specified, the **arc_id** option is used. If both the **arc** and **arc_id** options are specified, the **arc_id** option is used.

arc_id:[archive id]

Used in combination with the **vault** option. Lists all backups of the selected archive.

If not specified, the **arc** option is used. If both the **arc** and **arc_id** options are specified, the **arc_id** option is used.

6.1.3.9 explore

partition:[partition number]

Specifies a list of partitions to be mounted as virtual drives. Without this option, all partitions stored in the image will be mounted.

To obtain the partition number for this option, list the image contents with the **/list/filename** command and use the number from the **Idx** column.

letter:X

Assigns letters to the mounted drives. This option is used with the **partition** option only.

6.1.3.10 unplug

letter:X

Specifies the virtual drive to be disconnected by letter.

letter:all

Disconnects all virtual drives.

6.1.3.11 asz_create

harddisk:X

Specifies the hard disk number where the Acronis Secure Zone will be created.

partition:[partition number]

Specifies partitions from which free space will be taken for Acronis Secure Zone.

size:[ASZ size in sectors | unallocated]

Sets the Acronis Secure Zone size (in sectors).

If not specified, the size is set as an average between the maximal (unallocated space plus free space on all partitions selected with the **partition** option) and minimal (about 35MB) values.

Either way, the program will first use the unallocated space. If there is not enough unallocated space, the selected partitions will be decreased. Resizing of locked partitions requires a reboot.

With “unallocated”, the zone will use all unallocated space on the disk. Partitions will be moved, if necessary, but not resized. Moving of locked partitions requires a reboot. The **partition** option is ignored.

6.1.3.12 asz_delete

partition:[partition number]

Specifies partitions to which free space will be added after the Acronis Secure Zone is deleted. If you specify several partitions, the space will be distributed proportionally based on each partition's size.

6.1.3.13 clone

harddisk:[disk number]

Specifies a source hard disk which will be cloned to the new hard disk.

target_harddisk:[disk number]

Specifies the target hard disk number where the source hard disk will be cloned.

6.1.4 trueimagecmd.exe usage examples

6.1.4.1 Image disks and partitions

The following command will create an image named 1.tib of partitions 2-1 and 1-3: `trueimagecmd /create /filename:"C:\Test\1.tib" /partition:2-1,1-3`

The image will be saved to the C:\Test\ folder.

The following command will create an image of partitions 2-1 and 1-3 in the Acronis Secure Zone: `trueimagecmd /create /asz /partition:2-1,1-3`

- The following command will create an image named 1.tib of partitions 2-1 and 1-3:

```
trueimagecmd /create /filename:"\Test\1.tib" /partition:2-1,1-3  
/file_partition:3-1
```

The image will be saved in the folder \Test on partition 3-1.

- The following command will append an incremental image to the image named 1.tib of hard disk 2:

```
trueimagecmd /create /filename:"C:\Test\1.tib" /password:qwerty  
/harddisk:2 /reboot /raw /incremental /compression:5 /split:640  
/progress:off
```

The image will be saved to C:\Test\ folder, protected with password “qwerty”, split into 640-MB parts, and contain all cluster data. Image compression level is 5. The server will be rebooted after the operation is completed.

- The following command will create an image of partition 2-1 named arc.tib in the shared folder [\\server1\folder](#):

```
trueimagecmd /create /partition:2-1 /filename:\\server1\folder\arc.tib  
/net_user:user1 /net_password:pw1 /log:\\server2\dir\log1.log  
/log_net_user:user2 /log_net_password:pw2
```

The operation log file log1.log will be saved on another share [\\server2\dir\](#). Credentials for both shares are provided.

- The following command will create an image of partition 2-1 in the archive.tib file located on the FTP server:

```
trueimagecmd /create /partition:2-1 /filename:ftp://server/folder/archive.tib  
/ftp_user:usr1 /ftp_password:pswd1
```

6.1.4.2 Restore disks and partitions

The following command will restore partition 2-1 from image 1.tib to the original location: `trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1`

- The following command will restore hard disk 2 from image 1.tib, protected with password ‘qwerty’, to the original hard disk:

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /password:qwerty  
/harddisk:2
```

- The following command will restore partition 2-1, stored in image 1.tib, to partition 1-1:

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1  
/target_partition:1-1
```

- The following command will restore partition 2-1, stored in image 1.tib, to hard disk 3:

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1  
/target_harddisk:3 /start:63 /size:64000 /type:logical
```

A new logical partition will be created on disk 3 starting from sector 63. The partition will occupy about 64000 sectors—the exact size will depend on disk geometry and the type of the file system.

- The following command will restore partition 1-1, stored in image Server30Cdrive.tib, protected with password '123qwe', to partition 2-1. The restored partition will be of the active type:

```
trueimagecmd /deploy /filename:z:\Server30Cdrive.tib /partition:1-1  
/target_partition:2-1 /type:active /password:123qwe
```

- The following command will restore the MBR from the image of hard disk 1 to the same hard disk 1. The image is contained in the 3rd backup created in archive number 2, located in Acronis Secure Zone that is protected with password 'pswd':

```
trueimagecmd /deploy_mbr /harddisk:1 /asz:2 /index:3 /password:pswd
```

- The following command will restore the MBR from the image of hard disk 1 to hard disk 2. The image is contained in the arc.tib file located on the FTP server:

```
trueimagecmd /deploy_mbr /harddisk:1 /target_harddisk:2  
/filename:ftp://server/folder/arc.tib /ftp_user:fuser  
/ftp_password:fpswd
```

6.1.4.3 Back up files

- The following command will back up files from the MyProject folder residing in D:\Workarea, except for files in the Old subfolder and hidden files, to the Myproject.tib file and save this file in the E:\Backups folder:

```
trueimagecmd /filebackup /filename:E:\Backups\Myproject.tib  
/include:D:\Workarea\MyProject /exclude_names: D:\Workarea\MyProject\Old  
/exclude_hidden
```

6.1.4.4 Restore files

- The following command will restore all files from E:\Backups\Myproject.tib to the original folder and assign the files the original date and time:

```
trueimagecmd /filerestore /filename:E:\Backups\Myproject.tib  
/original_date
```

Since the /overwrite option is not specified, the latest file modifications will be replaced with the original ones.

6.1.4.5 Consolidate backups

- The following command will display the numbered list of backups, contained in the archive Kons.tib residing on the network share [\\smbsrv\Archives\](#):

```
trueimagecmd /pit_info /filename:\\smbsrv\Archives\Kons.tib
```

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /pit_info
/filename:\\srv\elenel\kons.tib
Pit number: 1
    type: image; kind: base; date: 6/27/2009 11:39:10 AM
Pit number: 2
    type: image; kind: incremental; date: 6/27/2009 11:43:13 AM
Pit number: 3
    type: image; kind: incremental; date: 6/27/2009 11:44:04 AM
Pit number: 4
    type: image; kind: incremental; date: 6/27/2009 11:48:22 AM
Pit number: 5
    type: image; kind: incremental; date: 6/27/2009 11:50:32 AM

Operation has succeeded.
```

- The following command will create on disk D: an archive consisting of three files Kons_new.tib, (pit 2 of the archive [\\smbsrv\Archives\Kons.tib](#), former [\\smbsrv\Archives\Kons2.tib](#)) Kons_new2.tib (pit 4, former [\\smbsrv\Archives\Kons4.tib](#)) and Kons_new3.tib (pit 5, former [\\smbsrv\Archives\Kons5.tib](#)):

```
trueimagecmd /consolidate /filename:\\smbsrv\Archives\Kons.tib
/target_filename:D:\Kons_new.tib /include_pits:2,4,5
```

6.1.4.6 Export backups

- The following command will export 3 backups (pits) from the archive (Archive 1) located in D:\Backups to the new archive (Archive 2) on the FTP server (Server22/Vault3):
- The following command will export 2 backups (pits) from the archive (Archive 1) located in managed vault "Vault1" to the new archive (Archive 2) on the network share (Server15\Backups):

```
trueimagecmd /export /vault:D:\Backups /arc:"Archive 1" /include_pits:2,4,5
/target_vault:ftp://Server22/Vault3 /target_arc:"Archive 2"
/ftp_user:"user" /ftp_password:"password" /progress:on
```

```
trueimagecmd /export /vault:bsp://StorageNode/Vault1 /arc:"Archive 1"
/include_pits:2,3
/net_src_user:"user" /net_src_password:"password"
/target_vault:\\Server15\Backups\
/target_arc:"Archive 2" /net_user:"user" /net_password:"password" /progress:on
```

6.1.4.7 Convert an image to virtual disk

- The following command will convert images of disks 1 and 3, contained in the file C:\MyBackup.tib, to the virtual disks C:\MyHDD.vmdk and C:\MyHDD2.vmdk for using with VMware type virtual machines:

```
trueimagecmd /convert /filename:C:\MyBackup.tib
/target_filename:C:\MyHDD.vmdk /vm_type:vmware /harddisk:1,3
```

6.1.4.8 List

- The following command will list available partitions:

```
trueimagecmd /list
```

The following command will list contents of the latest image located in Acronis Secure Zone: trueimagecmd /list /asz

The following command will list contents of the specified image: `trueimagecmd /list /filename:"C:\My Folder\Backup.tib"`

The following command will list all archives and their UUID's in the specified location: `trueimagecmd /list /vault:D:Backups`

The following command will list all backups of the specified archive: `trueimagecmd /list /vault:D:Backups /arc:"Archive 1"`

6.1.4.9 Check for assigned licenses

- The following command will check if there are licenses assigned to the local machine on the license server.

```
trueimagecmd /ls_check
```

The result is a list of used licenses for the local machine in the following format:

```
SKU | (trial)/empty | valid/invalid
```

The empty "trial" field means that a standard license is assigned to this machine.

Example:

Acronis Backup & Recovery 10 Advanced Server	(trial)	invalid
Acronis Backup & Recovery 10 Advanced Server		valid

6.1.4.10 Acronis Secure Zone: managing backups by archive numbers

The following command will list the Acronis Secure Zone size, free space and contents: `trueimagecmd /asz_content`

Assume that the contents of Acronis Secure Zone are as follows:

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /asz_content
ASZ size: 34.439 GB
ASZ free space: 34.409 GB
ARCHIVE number: 1
    index: 1; type: file, base; creation time: 4/2/2009 3:52 PM
ARCHIVE number: 2
    index: 1; type: file, base; creation time: 4/2/2009 4:04 PM
    index: 2; type: file, incremental; creation time: 4/4/2009 6:31 PM
    index: 3; type: file, incremental; creation time: 4/4/2009 6:32 PM
```

In our example, the Acronis Secure Zone contains two archives. The older archive #1 consists of one full (base) file-level backup created on **4/2/2009 at 3:52**. The second archive contains a base file-level backup with two increments. You can restore data from any backup as follows:

```
trueimagecmd /filerestore /asz:2 /index:2 /target_folder:e:
```

This will restore files and folders from the backup created on **4/4/2009 at 6:31 PM** with their original paths to the root of partition E.

```
trueimage /list /filename:asz://2 /index:3 /password:aszipw
```

which is equal to:

```
trueimagecmd /list /asz:2 /index:3 /password:aszipw
```

This will list content of the 3rd backup created in archive number 2, located in Acronis Secure Zone that is protected with password 'aszipw'.

6.1.4.11 Acronis Secure Zone: managing backups by file names

- The following command will list the Acronis Secure Zone size, free space and contents using generated filenames:

```
trueimagecmd /asz_files /password:aszpw
```

Assume that the contents of Acronis Secure Zone are as follows:

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /asz_files
/password: aaa
ASZ size: 5.387 GB
ASZ free space: 4.363 GB
FILE name: AAA2.TIB; size: 56414317 byte
      type: image, base; creation time: 2/16/2009 3:43:34 PM
      type: image, incremental; creation time: 4/25/2009 11:44:47 AM
FILE name: FAAA.TIB; size: 3125550 byte
      type: file, base; creation time: 8/22/2009 12:28:40 PM
FILE name: FAAB2.TIB; size: 5147 byte
      type: file, base; creation time: 8/14/2009 2:17:45 PM
      type: file, incremental; creation time: 8/15/2009 2:19:43 AM
```

In our example, the Acronis Secure Zone contains three archives.

Archive AAA2 (2 stands for the number of backups in the archive) consists of:

- full (base) image backup created on **2/16/2009 at 3:43**
- incremental backup created on **4/25/2009 at 11:44**.

Archive FAAA (F means that this is a file-level archive) contains one base file-level backup.

Archive FAAB2 (B means that this is the second file-level archive in the zone) consists of:

- full (base) file-level backup created on **8/14/2009 at 2:17**
- incremental backup created on **8/15/2009 at 2:19**.

```
trueimagecmd /filerestore /filename:asz://FAAA /target_folder:e:
/password:aszpw
```

This will restore files and folders with their original paths from the sole base backup FAAA to the root of partition E.

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /filerestore
/filename:asz://FAAA /target_folder:e: /password:aaa
[#####] 100%
Operation has succeeded.
```

6.1.4.12 Acronis Secure Zone: deleting backups

The following command will delete the most recent backup in the FAAB archive:

```
trueimagecmd /asz_delete_files /password:aszpw /filename:FAAB.tib
```

Assume, the contents of Acronis Secure Zone are as follows:

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /asz_files
/password: aaa
ASZ size: 5.387 GB
ASZ free space: 4.363 GB
FILE name: AAA2.TIB; size: 56414317 byte
    type: image, base; creation time: 2/16/2009 3:43:34 PM
    type: image, incremental; creation time: 4/25/2009 11:44:47 AM
FILE name: FAAA.TIB; size: 3125550 byte
    type: file, base; creation time: 8/22/2009 12:28:40 PM
FILE name: FAAB2.TIB; size: 5147 byte
    type: file, base; creation time: 8/14/2009 2:17:45 PM
    type: file, incremental; creation time: 8/15/2009 2:19:43 AM
```

The above command will delete the incremental backup created on 8/15/2009 at 2:19.

The next execution of the same command will delete the base FAAB backup. By continuing with the FAAA and AAA names, you can clear the Acronis Secure Zone except for the last remaining base backup that cannot be deleted.

6.1.4.13 Clone

```
The following command will clone hard disk 2 to hard disk 3: trueimagecmd
/clone /harddisk:2 /target_harddisk:3
```

6.1.4.14 Explore image

- The following command will connect all images, stored in file mybackup.tib on the network drive, as virtual drives:

```
trueimagecmd /explore /filename:\\myserver\backup\mybackup.tib
/net_user:john /net_password:qwerty
```

6.2 Scripting

Scripting is intended only for backup.

6.2.1 Script execution parameters

Scripts are executed by the **TrueImageTerminal.exe** utility located in the Acronis Backup & Recovery Server OEM installation folder (i.e. C:\Program Files\Acronis\BackupAndRecovery). This utility is also used to monitor backup progress.

TrueImageTerminal execution parameters:

```
TrueImageTerminal.exe [arguments]
```

Arguments include the following:

/help – outputs help information about TrueImageTerminal.exe parameters.

/progress – outputs the progress of backup operations run either from Acronis Backup & Recovery Server OEM graphics user interface, or from the script.

/execute: [script file name] – executes a script. If there are several scripts to be executed, they are queued. An example for executing MyBackup.tis script:

```
TrueImageTerminal.exe /execute:C:\MyBackup.tis
```

/nowait – an optional script execution argument. Enables to terminate TrueImageTerminal before backup is finished. Example:

```
TrueImageTerminal /execute:C:\MyBackup.tis /nowait
```

*By pressing **Ctrl+C** you can forcibly turn off backup progress output and switch TrueImageTerminal to a background operation.*

*You can terminate the backup operation executed by TrueImageTerminal by pressing **Ctrl+B**.*

6.2.2 Script structure

Scripts are written in the XML language and you can use the following tags:

- Source (p. 144)
- Target (p. 144)
- Options (p. 144)

6.2.2.1 Source

Specifies the partitions or disks to be imaged. Letters assigned to partitions must be used without a colon. Disk numbers correspond to their system numbers. To create images of several partitions or disks, use the SOURCE tag for each of them, e.g.:

```
<source letter ="C" />
<source letter ="D" />
<source disk ="1" />
<source disk ="2" />
```

6.2.2.2 Target

Specifies the name and the location of an image file, e.g.:

```
<target file="E:\Mybackup2.tib" username="username" password="password" />
```

username and **password** parameters are optional. They are used to access networked resources.

As a target for the image files you can indicate a CD-R/RW or tape drive.

6.2.2.3 Options

This tag can be used with a number of additional parameters:

Compression

specifies the backup compression level. Can be **None**, **Normal**, **High**, **Maximum**.

Incremental

specifies whether you need to create an incremental image file. If equal to "false" (or "0"), a complete image file will be created. If there is already a file with the specified name, it will be replaced without warnings. If equal to "true" (or "1") and there is already a file with the specified name, an incremental image will be created. Otherwise the program will create a complete image file. The default value for this parameter is "true".

Description

adds a description to an image file. The comment must be a single string (though its length is not limited.)

Split

splits a large image file into a number of smaller files of the specified size, which can be provided in bytes, kilobytes, megabytes, etc.

Password

adds password protection to an image file.

6.2.3 Script usage examples

The following example illustrates the usage of a script to back up two partitions (logical drives), C and F. **mybackup2.tib** is specified as an incremental image file. High compression level is selected and the image will be split into 650-MB parts for recording to CD-R/RW media. Password protection will also be added. The entire script must be located between the **<backup>** and **</backup>** tags.

```
<? xml version="1.0" encoding="utf-8" ?>
<backup>
<source letter ="c" />
<source letter ="f" />
<target file="e:\mybackup2.tib" />
<options compression="high" incremental="true" description="this is my backup"
  split="650 Mb" password="" />
</backup>
```

The script for backing up to tape (tapeN specifies the tape numbers):

```
<? xml version="1.0" encoding="utf-8" ?>
<backup>
<source letter ="c" />
<source letter ="f" />
<target cdrw="\taperecorder\\\.\tape0|||" />
<target cdrw="\taperecorder\\\.\tape1|||" />
<options compression="high" incremental="true"
  description="this is my backup" />
</backup>
```

7 Glossary

A

Acronis Plug-in for WinPE

A modification of Acronis Backup & Recovery Server OEM Agent for Windows that can run in the preinstallation environment. The plug-in can be added to a WinPE image using Bootable Media Builder. The resulting bootable media can be used to boot any PC-compatible machine and perform, with certain limitations, most of the direct management operations without help of an operating system. Operations can be configured and controlled either locally through the GUI or remotely using the console.

Acronis Startup Recovery Manager (ASRM)

A modification of the bootable agent, residing on the system disk and configured to start at boot time when F11 is pressed. Acronis Startup Recovery Manager eliminates the need for rescue media or network connection to start the bootable rescue utility.

Acronis Startup Recovery Manager is especially useful for mobile users. If a failure occurs, the user reboots the machine, hits F11 on prompt "Press F11 for Acronis Startup Recovery Manager..." and performs data recovery in the same way as with ordinary bootable media.

Limitation: requires re-activation of loaders other than Windows loaders and GRUB.

Agent (Acronis Backup & Recovery Server OEM Agent)

An application that performs data backup and recovery and enables other management operations on the machine (p. 151), such as task management and operations with hard disks.

The type of data that can be backed up depends on the agent type. Acronis Backup & Recovery Server OEM includes the agents for backing up disks.

Agent-side cleanup

Cleanup performed by an agent according to the backup plan that produces the archive (p. 146). Agent-side cleanup is performed in unmanaged vaults (p. 152).

Agent-side validation

Validation (p. 152) performed by an agent according to the backup plan that produces the archive (p. 146). Agent-side validation is performed in unmanaged vaults (p. 152).

Archive

See Backup archive.

B

Backup

The result of a single backup operation (p. 147). Physically, it is a file or a tape record that contains a copy of the backed up data as of specific date and time. Backup files created by Acronis Backup & Recovery Server OEM have a TIB extension. The TIB files resulting from backup consolidation are also called backups.

Backup archive (Archive)

A set of backups (p. 147) created and managed by a backup plan. An archive can contain multiple full backups (p. 150). Backups belonging to the same archive are always stored in the same location. Multiple backup plans can back up the same source to the same archive, but the mainstream scenario is "one plan – one archive".

Backups in an archive are entirely managed by the backup plan. Manual operations with archives (validation (p. 152), viewing contents, mounting and deleting backups) should be performed using Acronis Backup & Recovery Server OEM. Do not modify your archives using non-Acronis tools such as Windows Explorer or third-party file managers.

Backup operation

An operation that creates a copy of the data that exists on a machine's (p. 151) hard disk for the purpose of recovering or reverting the data to a specified date and time.

Backup options

Configuration parameters of a backup operation (p. 147), such as pre/post backup commands, maximum network bandwidth allotted for the backup stream or data compression level. Backup options are a part of a backup plan.

Backup plan (Plan)

A set of rules that specify how the given data will be protected on a given machine. A backup plan specifies:

- what data to back up
- where to store the backup archive (the backup archive name and location)
- the backup scheme, that includes the backup schedule and [optionally] the retention rules
- [optionally] the archive validation rules (p. 152)
- the backup options (p. 147).

For example, a backup plan can contain the following information:

- back up volume C: (**this is the data the plan will protect**)
- name the archive MySystemVolume and place it to [\\server\backups\](#) (**this is the backup archive name and location**)
- perform full backup monthly on the last day of the month at 10:00AM. Delete backups that are older than 3 months (**this is a backup scheme**)
- validate the last backup immediately after its creation (**this is a validation rule**)
- protect the archive with a password (**this is an option**).

Physically, a backup plan is a bundle of tasks (p. 151) configured for execution on a managed machine (p. 151).

A backup plan can be created directly on the machine (local plan).

Backup scheme

A part of the backup plan that includes the backup schedule and [optionally] the retention rules and the cleanup schedule. For example: perform full backup (p. 150) monthly on the last day of the month at 10:00AM. Delete backups that are older than 3 months. Check for such backups every time the backup operation is completed.

Bootable agent

A bootable rescue utility that includes most of the functionality of the Acronis Backup & Recovery Server OEM Agent. Bootable agent is based on Linux kernel. A machine (p. 151) can be booted into a bootable agent using bootable media. Operations can be configured and controlled either locally through the GUI or remotely using the console.

Bootable media

A physical media (CD, DVD, USB flash drive or other media supported by a machine (p. 151) BIOS as a boot device) that contains the bootable agent or Windows Preinstallation Environment (WinPE) with the Acronis Plug-in for WinPE (p. 146). A machine can also be booted into the above environments using the network boot from Microsoft Remote Installation Service (RIS). These servers with uploaded bootable components can also be thought of as a kind of bootable media.

Bootable media is most often used to:

- recover an operating system that cannot start
- access and back up the data that has survived in a corrupted system
- deploy an operating system on bare metal
- create basic or dynamic volumes (p. 150) on bare metal
- back up sector-by-sector a disk that has an unsupported file system
- back up offline any data that cannot be backed up online because of restricted access, being permanently locked by the running applications or for any other reason.

C

Console (Acronis Backup & Recovery Server OEM Management Console)

A tool for local access to Acronis agents.

D

Direct management

Any management operation that is performed on a managed machine (p. 151) using the direct console-agent connection.

The direct management operations include:

- creating and managing local backup plans (p. 150)

- creating and managing local tasks (p. 151), such as recovery tasks
- creating and managing personal vaults (p. 151) and archives stored there
- viewing the state, progress and properties
- viewing and managing the log of the agent's operations
- disk management operations, such as clone a disk, create volume, convert volume.

A kind of direct management is performed when using bootable media.

Disk backup (Image)

A backup (p. 147) that contains a sector-based copy of a disk or a volume in a packaged form. Normally, only sectors that contain data are copied. Acronis Backup & Recovery Server OEM provides an option to take a raw image, that is, copy all the disk sectors, which enables imaging of unsupported file systems.

Disk group

A number of dynamic disks (p. 149) that store the common configuration data in their LDM databases and therefore can be managed as a whole. Normally, all dynamic disks created within the same machine (p. 151) are members of the same disk group.

As soon as the first dynamic disk is created by the LDM or another disk management tool, the disk group name can be found in the registry key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name.

The next created or imported disks are added to the same disk group. The group exists until at least one of its members exists. Once the last dynamic disk is disconnected or converted to basic, the group is discontinued, though its name is kept in the above registry key. In case a dynamic disk is created or connected again, a disk group with an incremental name is created.

When moved to another machine, a disk group is considered as 'foreign' and cannot be used until imported into the existing disk group. The import updates the configuration data on both the local and the foreign disks so that they form a single entity. A foreign group is imported as is (will have the original name) if no disk group exists on the machine.

For more information about disk groups please refer to the following Microsoft knowledge base article:

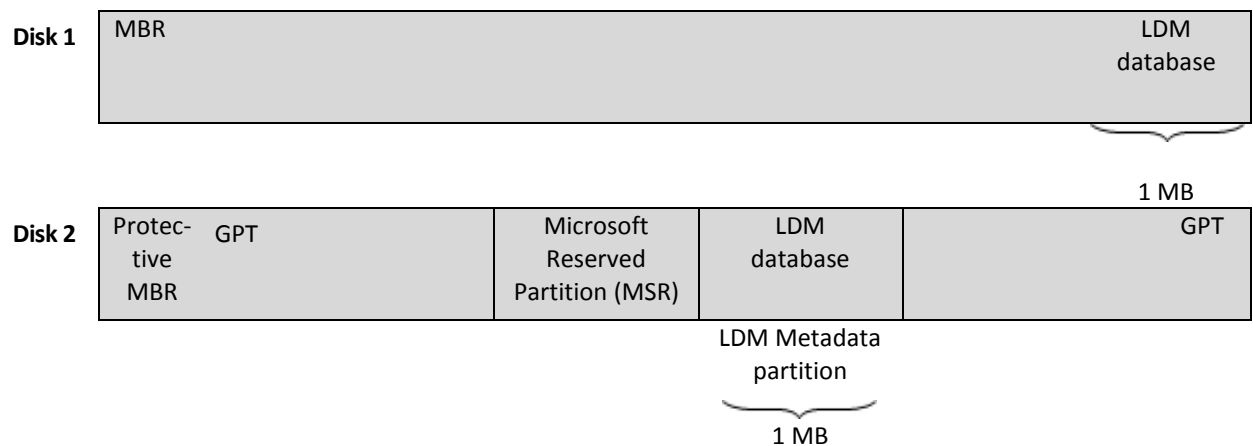
222189 Description of Disk Groups in Windows Disk Management
<http://support.microsoft.com/kb/222189/EN-US/>

Dynamic disk

A hard disk managed by Logical Disk Manager (LDM) that is available in Windows starting with Windows 2000. LDM helps flexibly allocate volumes on a storage device for better fault tolerance, better performance or larger volume size.

A dynamic disk can use either the master boot record (MBR) or GUID partition table (GPT) partition style. In addition to MBR or GPT, each dynamic disk has a hidden database where the LDM stores the dynamic volumes' configuration. Each dynamic disk holds the complete information about all dynamic volumes existing in the disk group which makes for better storage reliability. The database

occupies the last 1MB of an MBR disk. On a GPT disk, Windows creates the dedicated LDM Metadata partition, taking space from the Microsoft Reserved Partition (MSR.)



Dynamic disks organized on MBR (Disk 1) and GPT (Disk 2) disks.

For more information about dynamic disks please refer to the following Microsoft knowledge base articles:

Disk Management (Windows XP Professional Resource Kit) <http://technet.microsoft.com/en-us/library/bb457110.aspx>

816307 Best practices for using dynamic disks on Windows Server 2003-based computers <http://support.microsoft.com/kb/816307>

Dynamic volume

Any volume located on dynamic disks (p. 149), or more precisely, on a disk group (p. 149). Dynamic volumes can span multiple disks. Dynamic volumes are usually configured depending on the desired goal:

- to increase the volume size (a spanned volume)
- to reduce the access time (a striped volume)
- to achieve fault tolerance by introducing redundancy (mirrored and RAID-5 volumes.)

F

Full backup

A self-sufficient backup (p. 147) containing all data chosen for backup. You do not need access to any other backup to recover the data from a full backup.

I

Image

The same as Disk backup (p. 149).

L

Local backup plan

A backup plan created on a managed machine (p. 151) using direct management.

Local task

A task (p. 151) belonging to a local backup plan (p. 150) or a task that does not belong to any plan, such as a recovery task. A local task belonging to a backup plan can be modified by editing the plan only; other local tasks can be modified directly.

M

Machine

A physical or virtual computer uniquely identified by an operating system installation. Machines with multiple operating systems (multi-boot systems) are considered as multiple machines.

Managed machine

A machine (p. 151), either physical or virtual, where at least one Acronis Backup & Recovery Server OEM Agent is installed.

Media builder

A dedicated tool for creating bootable media.

P

Personal vault

A local or networked vault (p. 152) created using direct management. Once a personal vault is created, a shortcut to it appears under the **Personal vaults** item of the **Navigation** pane. Multiple machines can use the same physical location; for example, a network share; as a personal vault.

Plan

See Backup plan.

R

Recovery point

Date and time to which the backed up data can be reverted to.

T

Task

In Acronis Backup & Recovery Server OEM, a task is a set of sequential actions to be performed on a managed machine (p. 151) when a certain time comes or a certain event occurs. The actions are described in an xml script file. The start condition (schedule) exists in the protected registry keys.

U

Universal Restore (Acronis Backup & Recovery Server OEM Universal Restore)

The Acronis proprietary technology that helps boot up Windows on dissimilar hardware or a virtual machine. The Universal Restore handles differences in devices that are critical for the operating system start-up, such as storage controllers, motherboard or chipset.

The Universal Restore is not available:

when the machine is booted with Acronis Startup Recovery Manager (p. 146) (using F11), because these features are primarily meant for instant data recovery on the same machine.

Unmanaged vault

Any vault (p. 152) that is not a managed vault.

V

Validation

An operation that checks the possibility of data recovery from a backup (p. 147).

Validation of a file backup imitates recovery of all files from the backup to a dummy destination. The previous product versions considered a file backup valid when the metadata contained in its header was consistent. The current method is time-consuming but much more reliable. Validation of a volume backup calculates a checksum for every data block saved in the backup. This procedure is also resource-intensive.

While the successful validation means a high probability of successful recovery, it does not check all factors that influence the recovery process. If you back up the operating system, only a test recovery under the bootable media to a spare hard drive can guarantee successful recovery in the future.

Validation rules

A part of the backup plan. Rules that define when and how often to perform validation (p. 152) and whether to validate the entire archive or the latest backup in the archive.

Vault

A place for storing backup archives. A vault can be organized on a local or networked drive or detachable media, such as an external USB drive. There are no settings for limiting a vault size or the number of backups in a vault. You can limit the size of each archive using cleanup, but the total size of archives stored in the vault is limited by the storage size only.

W

WinPE (Windows Preinstallation Environment)

A minimal Windows system based on any of the following kernels:

- Windows XP Professional with Service Pack 2 (PE 1.5)
- Windows Server 2003 with Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 and Windows Server 2008 (PE 2.1).

WinPE is commonly used by OEMs and corporations for deployment, test, diagnostic and system repair purposes. A machine can be booted into WinPE via CD-ROM, USB flash drive or hard disk. The Acronis Plug-in for WinPE (p. 146) enables running the Acronis Backup & Recovery Server OEM Agent in the preinstallation environment.