User's Guide

Acronis®
True Image 9.1
Server for Linux

Acronis
Compute with confidence
www.acronis.com

END-USER LICENSE AGREEMENT

BY ACCEPTING, YOU (ORIGINAL PURCHASER) INDICATE YOUR ACCEPTANCE OF THESE TERMS. IF YOU DO NOT WISH TO ACCEPT THE PRODUCT UNDER THESE TERMS, YOU MAY CHOOSE NOT TO ACCEPT BY SELECTING "I decline..." AND NOT INSTALLING THE SOFTWARE.

The Acronis® True Image Server for Linux (the Software) is Copyright © Acronis, Inc., 2000-2007. All rights are reserved. The ORIGINAL PURCHASER is granted a LICENSE to use the software only, subject to the following restrictions and limitations.

1. The license is to the original purchaser only, and is not transferable without prior written permission from Acronis.
2. The original purchaser may use the software on a single computer owned or leased by the original purchaser. You may not use the software on more than a single machine, even if you own or lease all of them, without the written consent of Acronis.
3. The original purchaser may not engage in, nor permit third parties to engage in, any of the following:

A. Providing or permitting use of or disclosing the software to third parties.

B. Providing use of the software in a computer service business, network, timesharing or multiple-user arrangement to users who are not individually licensed by Acronis.

C. Making alterations or copies of any kind in the software (except as specifically permitted above).

D. Attempting to un-assemble, de-compile or reverse engineer the software in any way.

E. Granting sublicenses, leases or other rights in the software to others.

F. Making copies or verbal or media translations of the users guide.

G. Making telecommunication data transmission of the software.

Acronis has the right to terminate this license if there is a violation of its terms or default by the original purchaser. Upon termination for any reason, all copies of the software must be immediately returned to Acronis, and the original purchaser shall be liable to Acronis for any and all damages suffered as a result of the violation or default.

ENTIRE RISK

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU THE PURCHASER. ACRONIS DOES NOT WARRANT THAT THE SOFTWARE OR ITS FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE OR THAT ANY DEFECTS WILL BE CORRECTED. NO LIABILITY FOR CONSEQUENTIAL DAMAGES - IN NO EVENT SHALL ACRONIS OR ITS VENDORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR THE LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF ACRONIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOFTWARE USAGE TERMS AND CONDITIONS

Under current legislation, the «License Agreement» is considered a contract between you and Acronis Inc. The contract is a legal document and its violation may result in legal action.

Illegal use and/or distribution of this software will be prosecuted.

Table of Contents

Chapter 1. Introduction

1.1 Acronis® True Image Server for Linux– a complete solution for corporate users

You have come to rely on your servers to run your business and retain key enterprise data. Acronis True Image Server for Linux provides comprehensive, reliable, and cost-effective system protection and recovery for corporate servers, running Linux. With Acronis True Image Server for Linux you have peace of mind knowing you are protected and can recover from any situation.

Minimizes downtime

Acronis True Image Server for Linux enables you to restore systems in minutes, not hours or days. An entire system can be restored from an image that includes everything the system needs to run: the operating system, applications, databases, and configurations. No reinstallation or reconfiguration is required. Moreover, complete system restoration can be performed to an existing system or to a new system with different hardware or to virtual machines. File-based backups provide you with the flexibility to only backup selected critical files.

Eases Administration

Wizards guide users through backup and recovery tasks, ensuring the product can be implemented with minimal user training.

Automates Backup

With the scheduling capability in Acronis True Image Server for Linux, you simply create backup tasks, tailored by group, at certain times or at certain events, automating backups.

To ensure that backups have occurred, or user intervention is required, you can request notifications via email or pop-up. You can view events in Acronis own log.

The product also supports the creation of custom commands before and after backups. For example, users can automatically run anti-virus products before an image is created and verify the validity of backups after they have been created.

Ensures 24 X 7 Uptime

With the Acronis Drive Snapshot systems can be imaged while they are in use, supporting 24 by 7 availability. This technology enables the product to backup and image critical operating system files, the master boot record and any partition-based boot records without requiring a reboot. A CPU allocation feature allows you to limit the amount of CPU usage for the application to maximize the CPUs available for mission critical applications. Moreover, users can control hard disk drive writing speeds and control network bandwidth used during backups, allowing you minimally disrupt business operations.

For correct backup of mission critical databases, Acronis True Image Server for Linux will execute your custom commands, that suspend and resume database processing, before and after data capture.

Supports Cutting Edge Technology

Businesses today are moving to leverage the latest technologies, dual-core 64 bit processors and 64 bit operating systems. With Acronis True Image Server for Linux, you can protect these new machines, as well as legacy ones, running one solution.

Leverages Existing Technology Investments

The product can leverage your current storage infrastructure by supporting a wide variety of storage media, so you can avoid costly hardware purchases to implement the solution. The product supports key storage technologies such as: Direct Attached Storage (DAS), Network Attached Storage (NAS), Storage Area Networks (SAN), Redundant Arrays of Independent Disks (RAID) devices, tapes, USB and IEEE-1394 (FireWire) compliant storage devices, CDs, removable drives (Floppy, Zip, etc.) and shared storage. Moreover, the product ensures that you maximize the space on these resources with four levels of compression.

Disk cloning and new disk deployment

Acronis True Image Server for Linux can be used to clone an image onto multiple servers. For example, a company purchased several servers and needs similar environments on each of them. Traditionally, an IT manager should install the operating system and programs on every server. With Acronis True Image Server for Linux, the IT manager can create a disk image of the first system deployed. That image can then be duplicated onto multiple servers.

If you need to upgrade the server hard disk drive, Acronis True Image Server for Linux simplifies the task to few mouse clicks creating the exact copy of your old disk to a new one and adjusting partitions size to fit a new hard disk.

1.2 Features of Acronis True Image Server for Linux

- Image creation without system shutdown
- Acronis True Image Server for Linux images only the sectors that contain data, so images are created in just a few minutes
- Support for a wide variety of IDE, SCSI, USB, FireWire, and PC Card (formerly PCMCIA) storage media. CD-R/RW and tape drives are supported as well (except for console mode)
- Support for all hard disks, regardless of capacity
- Support for all Linux and Windows file systems, including Linux Ext2/Ext3, ReiserFS, JFS, XFS, Linux Swap, FAT16, FAT32, NTFS; sector-based support for other file systems. JFS and XFS are supported without resize while restore
- Backup and restore software RAIDs (md devices) both on running system and from rescue CD
- Full and incremental backups
- Scheduled and periodical image creation using *cron jobs* utility

- Restore of individual files and directories (by mounting image archives as if they were kernel space block devices)
- Transparent NFS and Samba network drives access (in X Window mode NFS and Samba appear among available devices, in console mode a path to the network drive may be specified)
- OS-independent operation of Acronis True Image Server for Linux from the bootable CD, including restore over NFS or Samba Network
- Comprehensive wizards simplify even the most complex operations

ADDITIONAL FEATURES

- Control of data compression level, image volume splitting and password protection
- The ability to change a partition type, file system, size and location during recovery or disk cloning
- The ability to clone a disk drive so that multiple systems will have the exact same base disk drive configuration and software
- The ability to migrate data from one drive to another

NEW IN Acronis True Image 9.1 Server for Linux

File-based backups with exclude files feature

Differential backups

Scheduling backups in X Window environment

Acronis Secure Zone and Startup Recovery manager

Backup to/restore from FTP servers

Bootable media builder

x86_64-bit processors support

CPU/Network Bandwidth/Disk Write speed throttling

Default backup/restore options

Mounting images in X Window environment in Read-Only or R/W mode

Bootable images on CD

Notifications (e-mail, Winpopup)

Viewing logs

Context Help

1.3 Technical support

Users of legally purchased copies of Acronis True Image Server for Linux are entitled to free technical support from Acronis. If you experience problems installing or using Acronis products that you can't solve yourself by using this guide, then please contact Acronis Technical Support.

For more information visit http://www.acronis.com/enterprise/support/.

Chapter 2. Installation and operation

2.1 System requirements

Acronis True Image Server for Linux requires the following hard-/software:

- Pentium or compatible PC
- 256 MB RAM
- CD-RW drive for rescue CD creating
- Mouse (recommended)
- Linux 2.4.18 or later kernel (including 2.6.x kernels).
- SuSE 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 9.3, RedHat 9.0, Advanced Server 2.1, Advanced Server 3.0, Advanced Server 4.0, Fedora Core 1, Fedora Core 2, Fedora Core 3, Fedora Core 4, Enterprise Server 3.0, Mandrake 8.0, 9.2, 10.0, 10.1, Slackware 10, Debian stable and unstable (sarge), ASPLinux 9.2, ASPLinux 10, ASPLinux 11, ASPLinux Server II, ASPLinux Server IV, Virtuozzo 2.6.x, Gentoo, UnitedLinux 1.0, Ubuntu 4.10, TurboLinux 8.0, TurboLinux 10.0 and some others Linux distributions are supported.

To obtain the up-to-date information about distributions, supported by your copy of Acronis True Image Server for Linux, see readme.txt file supplied with the program.

2.2 Installing Acronis True Image Server for Linux

To install Acronis True Image Server for Linux:

- Assign to the setup file the attribute **Executable**
- Run the setup process
- Follow setup program instructions.

If the setup could not compile the necessary module for your Linux distribution, please refer to the file HOWTO.INSTALL:

```
/usr/lib/Acronis/TrueImageServer/HOWTO.INSTALL
```

You can choose to install, besides Acronis True Image Server for Linux, **Rescue Media Builder** tool.

With Rescue Media Builder you can create bootable rescue disks or their ISO images (see details in *Chapter 10 Creating bootable media*). You might not need this tool if you purchased a boxed product that contains a bootable CD. Installing the Rescue Media Builder will allow you to create bootable media or its ISO image at any time running Rescue Media Builder on its own.

2.3 Running Acronis True Image Server for Linux

- To run the program under the X Window System interface, use the **trueimage** command or select **Acronis True Image Server for Linux** from the system tools menu.
- To work in the console mode, use **trueimagecmd** and **trueimagemnt** tools, described in *Chapter 11*. See also **man trueimagecmd** or **man trueimagemnt**.

2.4 Removing the program

To remove Acronis True Image Server for Linux, do the following:

1. Issue the following commands:

```
# cd /usr/lib/Acronis/TrueImageServer/uninstall/
# ./uninstall
```

2. Remove the sources of the SnapAPI module:

```
# rm -rf /usr/src/snapapi*
```

Chapter 3. General information and proprietary Acronis technologies

3.1 The difference between file archives and disk/partition images

A backup archive is a file or a group of files (also called in this Guide “backups”), that contains a copy of selected files/folders data or a copy of all information stored on selected disks/partitions.

When you back up files and folders, only the data, along with the folder tree, is compressed and stored.

Backing up disks and partitions is performed in a different way: Acronis True Image Server for Linux stores a sector-by-sector snapshot of the disk, which includes the operating system, drivers, software applications and data files. This procedure is called “creating a disk image,” and the resulting backup archive is often called a disk/partition image.

Acronis True Image Server for Linux stores only those hard disk sectors that contain data (for supported file systems). This reduces image size and speeds up image creation and restoration from an image.

A partition image contains all its files and folders independently of their attributes (including system files), a boot record and file system super block.

A disk image includes images of all disk partitions as well as the zero track with master boot record (MBR).

By default, files in all Acronis True Image Server for Linux archives have a “.tib” extension.

It is important to note, that you can restore files and folders not only from file archives, but from disk/partition images, too. To do so, mount the image (see *9.1 Mounting an image* or *11.3 Restoring files with trueimagemnt*), or start the image restoration and select **Restore specified files or folders**.

3.2 Full, incremental and differential backups

Acronis True Image Server for Linux can create full, incremental and differential backups.

A full backup contains all data at the moment of backup creation. It forms a base for further incremental or differential backup or is used as a standalone archive. A full backup has the shortest restore time as compared to incremental or differential ones.

An incremental backup file only contains data changed since the last full or incremental backup creation. Therefore, it is smaller and takes less time to create. But as it doesn’t contain all data, all the previous incremental backups and the initial full backup are required for restoration.

Unlike incremental backup, when every backup procedure creates the next file in a “chain,” a differential backup creates an independent file, containing all changes against the initial

full archive. Generally, a differential backup will be restored faster than an incremental one, as it does not have to process through a long chain of previous backups.

A standalone full backup may be an optimal solution if you often roll back the system to the initial state (like in a gaming club or Internet café, to undo changes, made by the guests). In this case, you need not to re-create the initial full image, so the backup time is not crucial, and the restore time will be minimal.

Alternatively, if you are interested in saving only the last data state to be able to restore it in case of system failure, consider the differential backup. It is particularly effective if your data changes tend to be little as compared to the full data volume.

The same is true for incremental backup. In addition, it is most useful when you need frequent backups and possibility to roll back to any of stored states. Having created a full backup once, if you then create an incremental backup each day of a month, you will get the same result as if you created full backups every day. However, the cost in time and disk space (or removable media usage) will be as little as one tenth as much.

It is important to note that the above arguments are nothing but examples for your information. Feel free to make up your own backup policy in accordance with your specific tasks and conditions. Acronis True Image Server for Linux is flexible enough to meet any real-life demands.

An incremental or differential backup created after a disk is defragmented might be considerably larger than usual. This is because the defragmentation program changes file locations on disk and the backups reflect these changes. Therefore, it is recommended that you re-create a full backup after disk defragmentation.

3.3 Acronis Secure Zone

The Acronis Secure Zone is a special partition for storing archives on the computer system itself. In the Acronis True Image Server for Linux Wizards' windows the zone is listed along with all partitions available for storing archives. Acronis Secure Zone is necessary for using Acronis Startup Recovery Manager (see below).

Acronis Secure Zone helps the user to get rid of outdated backups. If there is not enough space for the new archive, older archives will be deleted to create space.

Acronis True Image Server for Linux uses the following scheme to clean up Acronis Secure Zone:

- If there is not enough free space in the zone to create a backup, the program deletes the oldest full backup with all subsequent incremental/differential backups.
- If there is only one full backup (with subsequent incremental/differential backups) left and a full backup is in progress, then the old full backup and incremental/differential backups are deleted.
- Otherwise, (only one full backup left, and an incremental/differential backup is in progress) you will get a message about space error. In that case you will have to either re-create the full backup or increase Acronis Secure Zone.

Thus, you can back up data automatically on a schedule (see *Chapter 7 Scheduling tasks*), and not worry about zone overflow issues. However, if you keep long chains of incremental

backups, it will be a good practice to periodically check the zone free space, indicated on the second page of the Manage Acronis Secure Zone wizard.

How to create, resize or delete Acronis Secure Zone using this wizard, see in *Chapter 8 Managing Acronis Secure Zone.*

3.4 Acronis Startup Recovery Manager

3.4.1 How it works

The Acronis Startup Recovery Manager enables starting Acronis True Image Server for Linux without loading the operating system. With this feature, if the system won't load for some reason, you can run Acronis True Image Server for Linux by itself to restore damaged partitions. As opposed to booting from Acronis removable media, you will not need a separate media to start Acronis True Image Server for Linux.

3.4.2 How to use

To be able to use Acronis Startup Recovery Manager at boot time, prepare as follows:

1. Install Acronis True Image Server for Linux.

2. Create Acronis Secure Zone on the server hard disk and activate Acronis Startup Recovery Manager (see *8.1 Creating Acronis Secure Zone*).

When Acronis Startup Recovery Manager is activated, it overwrites the master boot record (MBR) with its own boot code. If you have any third-party boot managers installed, you will have to reactivate them after activating the Startup Recovery Manager. For Linux loaders (e.g. LiLo and GRUB), you might consider installing them to a Linux root (or boot) partition boot record instead of MBR before activating Acronis Startup Recovery Manager.

If failure occurs, turn on the computer and press F11 when you see the "Press F11 for Acronis Startup Recovery Manager" message. This will run a standalone version of Acronis True Image Server for Linux that only slightly differs from the complete version. For information on restoring damaged partitions, see *Chapter 6 Restoring the backup data under X Window System*.

After Acronis Startup Recovery Manager was initially activated, you can deactivate it or activate again at any time. See details in *8.1.1 Activating and deactivating Acronis Startup Recovery Manager*.

3.5 Working from a rescue CD

In some situations (e.g. if the operating system fails to boot, or when cloning a mounted disk), you might have to work with Acronis True Image Server for Linux without loading the OS. In those cases, you can use the Acronis rescue CD. It is highly recommended that you create it as described in *Chapter 10 Creating bootable media*.

3.6 Working from a remote terminal

You can control the image creation or restoration process remotely from any computer in the local network or Internet, operating under Windows, Mac OS or any UNIX clone.

To act as a remote terminal, this computer must have X Server software installed. Start the X Server and log on to the server using SSH-enabled software. For example, Putty is one of the most popular Windows programs of that type.

Then you can invoke Acronis True Image Server for Linux GUI with the **trueimage** command or use **trueimagecmd** command line tool.

3.7 Backing up software and hardware RAID arrays

Acronis True Image Server for Linux supports software and hardware RAID arrays as if these were simple single hard drives. However, as such arrays have a structure different from typical hard disks, there are peculiarities affecting the way data is stored.

Software RAID arrays under Linux OS combine several hard disks partitions and make solid block devices (/dev/md0, ... /dev/md31), information of which is stored in /etc/raidtab or in dedicated areas of that partitions. Acronis True Image Server for Linux enables you to create images of active (mounted) software arrays similar to typical hard disk images.

Partitions that are part of software arrays are listed alongside other available partitions as if they had a corrupted file system or without a file system at all. There's no sense in creating images of such partitions when a software array is mounted, as it won't be possible to restore them.

Parameters of software disk arrays are not stored in images, so they can only be restored to a normal partition, or unallocated space, or previously configured array.

Operating from a rescue CD, Acronis True Image Server for Linux tries to access parameters of a software disk array and configure it. However, if the necessary information is lost, the array cannot be configured automatically. In this case, create a software array manually and restart the restoration procedure.

Hardware RAID arrays under Linux combine several physical drives to create a single partitionable disk (block device). The special file related to a hardware disk array is usually located in /dev/ataraid. Acronis True Image Server for Linux enables you to create images of hardware disk arrays similar to images of typical disks and partitions.

Physical drives that are part of hardware disk arrays are listed alongside other available drives as if they had a bad partition table or no partition table at all. There's no sense in creating images of such drives, as it won't be possible to restore them.

3.8 Support for LVM volumes

When running in Linux environment with 2.6.x kernel, Acronis True Image Server for Linux supports disks, managed by Logical Volume Manager (LVM). You can back up data of one or more LVM volumes and restore it to a previously created LVM volume or MBR disk (partition), likewise it is also possible to restore MBR volume data to an LVM volume. In each case, the program stores and restores volume contents only. The type or other properties of the target volume will not be changed.

In rescue mode (when booted with Bootable Rescue media or using F11) Acronis True Image Server for Linux cannot access LVM disks. This means that:

- an LVM volume image can be deployed on a MBR disk only

- to be able to recover data in rescue mode, you must keep its backup on a basic, network, or removable disk.

A system, restored from an LVM volume image over an MBR disk, cannot boot because its kernel tries to mount the root file system at the LVM volume. To boot the system, change the loader configuration and /etc/fstab so that LVM is not used. Then reactivate your boot manager as described in section 6.3.11.

When restoring an LVM volume over an MBR partition, resizing of the partition is possible.

LVM volumes appear at the end of the list of hard disks available for backup. Hard disk partitions included in LVM volumes are also shown in the list with **None** in the **Type** column. If you select to back up such partitions, the program will image it sector-by-sector. Normally it is not needed. To back up all available disks, specify all dynamic volumes plus partitions not belonging to them.

The following is an example of a list of drives obtained with the --list command (GUI wizards display a similar table). The system has three physical disks (1, 2, 3). Two dynamic volumes 4-1 and 4-2 are arranged across partitions 1-2 and 2-1. Hard drive 3 includes Acronis Secure Zone which is not normally imaged.

Num	Partition	Flags	Start	Size	Type
Disk 1:					
1-1	hda1 (/boot)	Pri,Act	63	208782	Ext3
1-2	hda2	Pri	208845	8177085	None
Disk 2:					
2-1	hdb1	Pri,Act	63	8385867	None
Disk 3:					
3-1	hdd1	Pri,Act	63	1219617	Ext3
3-2	Acronis Secure Zone	Pri	1219680	2974608	FAT32
Dynamic Volumes:					
4-1	VolGroup00-LogVol00			15269888	Ext3
4-2	VolGroup00-LogVol01			1048576	Linux Swap

To image dynamic volume 4-1, select partition 4-1.

To image all three physical drives, select partitions 1-1, 3-1, 4-1, 4-2.

If you select disk 2, partition 1-2 or 2-1, the program will create a sector-by-sector copy.

3.9 Backing up to tape drive

Acronis True Image Server for Linux supports SCSI tape drives. It can store backups on the tape and restore data from the tape, store large backups to multiple tapes, and append incremental/differential changes to a tape with the existing archives.

If a SCSI tape drive is connected to the server, the list of devices available for backup storage will be extended with a name corresponding to the drive type.

Backup and restore on the tape proceed in the same way as with other devices, with the following exceptions.

1. A full backup can be stored on an empty tape only. If you use tape that already contains data, its contents will be overwritten.

2. In case you want to keep more than one archive on the tape, for example, back up two disks separately, choose incremental backup mode when creating initial full backup for the second disk. In other situations, incremental backup is used for appending changes to the previously created archive.

3. You do not have to provide filenames for backups.

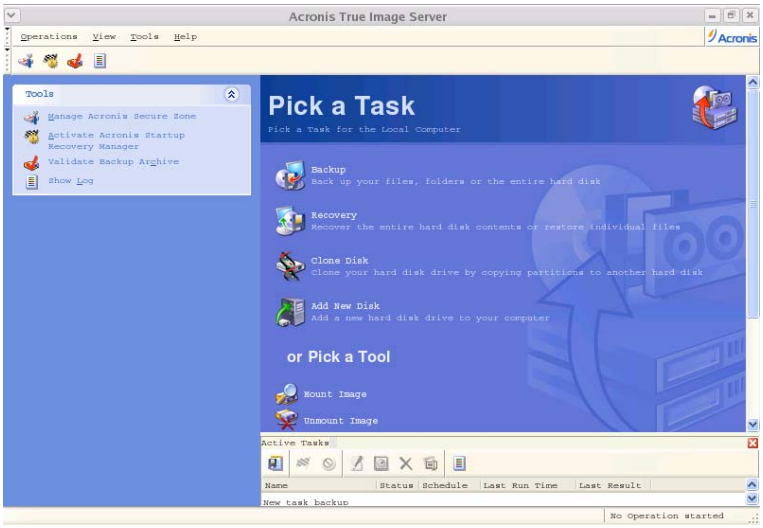
You might experience short pauses that are required to rewind the tape.

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

Chapter 4. Main program interface under X Window System

Acronis True Image Server for Linux features a user-friendly interface under X Window System.

The main program window contains the menu, the toolbar, the **Active Tasks** pane and the main area. The main area contains operation icons.



Most of the operations are represented two or even three times in different window areas, providing several ways to select them for more convenience. For example, you can start the necessary operation or tool by clicking its icon in the main area or by selecting the same item from the **Operations** or **Tools** menu.

The main window contains two groups of icons.

The **Task** group contains the following operations:

- **Backup** – create a backup archive
- **Recovery** – restore data from a previously created archive
- **Clone Disk** – transfer the OS, applications and data from the old disk to the new one
- **Add New Disk** – add a new disk for data storage leaving the OS and applications on the old one.

The **Tools** group contains the following items:

- **Mount image** – mounts a partition image
- **Unmount image** – unmounts a partition image

- **Manage Acronis Secure Zone** – used to create, delete and resize a special partition for storing archives (Acronis Secure Zone)
- **Activate Acronis Startup Recovery Manager** – activates the boot restoration manager (F11 key)
- **Validate Backup Archive** – runs the archive integrity checking procedure.

Program menu

The menu contains the following submenus: **Operations**, **View**, **Tools**, **Help**.

The **Operations** menu contains a list of the available operations, including scheduling tasks.

The **View** menu contains items for managing the program window look:

- **Toolbars** – contains commands that control toolbar icons
- **Common Task Bar** – enables/disables the sidebar
- **Status Bar** – enables/disables the status bar
- **Active tasks** – enables/disables the Active Tasks pane at the bottom of the main area.

The **Tools** menu contains the following items:

- **Manage Acronis Secure Zone** – used to create, delete and resize a special partition for storing archives (Acronis Secure Zone)
- **Activate Acronis Startup Recovery Manager** – activates the boot restoration manager (F11 key)
- **Validate Backup Archive** – runs the archive integrity checking procedure.
- **Show Log** – opens the Log Viewer window
- **Options** – opens a window for editing default backup/restore options, setting text appearance (fonts), configuring email/Winpopup notifications etc.

The **Help** menu is used to invoke help and obtain information about Acronis True Image Server for Linux.

Active Tasks pane

The **Active Tasks** pane displays the scheduled and currently-being-executed tasks. It features its own toolbar. You can customize this toolbar view by right-clicking on it and selecting the desired options.

Status bar

At the bottom of the main window, there is a status bar, indicating Acronis True Image Server for Linux operation progress and results. If you double-click on the operation results, you will see the logs window.

Disk and partition information

In all disk configurations provided by wizards, you will be able to change the way they are represented.

To the right, there are three icons: **Arrange Icons by...**, **Choose details** and **Properties** (the last duplicated in the context menu invoked by a right-click on the object).

To enable sorting by selected column, click its header (click again to reverse) or click **Arrange Icons by ...** and select the sorting parameter.

To select columns to display, right-click on column headers or click **Choose details** and check the columns that will be displayed.

Click **Properties** to invoke the properties window of the selected partition or disk.

This window has two panels. The left contains the properties tree, while the right describes the property selected. Disk information includes its physical parameters (connection, type, capacity, etc.). Partition information includes both physical (sectors, location on disk, etc.) and logical parameters (file system, free space, etc.).

You can resize columns by dragging their borders with a mouse.

Chapter 5. Creating backup archives under X Window System

To be able to restore the lost data or roll back your system to a predetermined state, you should first create a data or entire-system backup file.

If you are not concerned about restoration of your operating system along with all settings and applications, but plan to keep safe only certain data (the current project, for example), choose file/folder backup. This will reduce the archive size, thus saving disk space and possibly reducing removable media costs.

Backing up the entire system disk (creating a disk image) takes more disk space but enables you to restore the system in minutes in case of severe data damage or hardware failure. Moreover, the imaging procedure is much faster than copying files, and may significantly speed the backup process when it comes to backing up large volumes of data (see details in *3.1 The difference between file archives and disk/partition images*).

This chapter describes creating backup archives using Acronis True Image Server for Linux GUI under X Window System. See *Chapter 11* for using console or *Cron* service.

Under X Window System interface, Acronis True Image Server for Linux offers user-friendly wizards. They simplify image creation and restoration operations, so even users not very familiar with Linux can work with them.

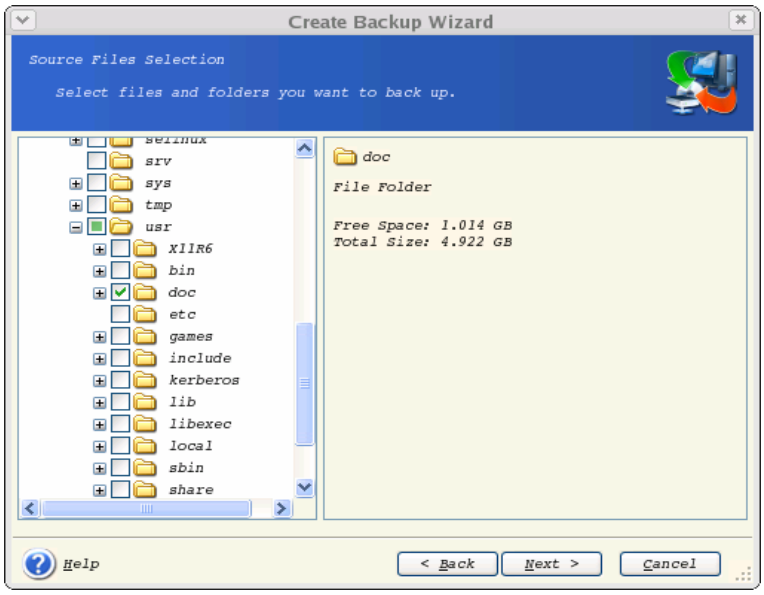
5.1 Backing up files and folders (file backup)

1. Invoke the **Create Backup Wizard** by clicking on the backup operation icon in the main program window.

2. Click **Next**.

3. Select **Backup files** and click **Next**.

4. From the tree pane, select files and folders to back up. You can select a random set of files, folders, partitions, disks and even computers.

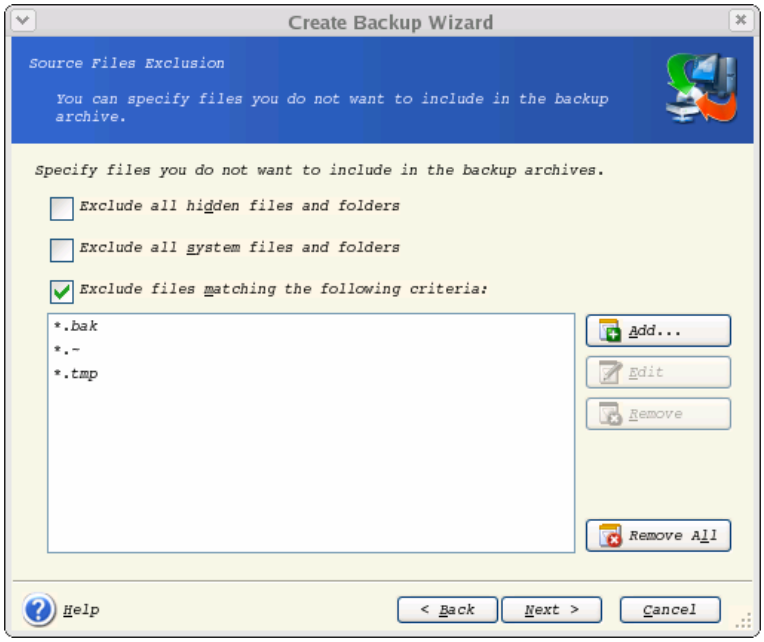


If you select a partition, disk or computer, and archive all its files, including system and hidden files, the bare-metal restore of that disk (partition, computer) still will not be possible. You also may not be able to boot the restored operating system. Therefore, it is recommended that you select only files and folders containing user data. To back up a disk or partition, use image backup.

5. Click **Next**.

6. Set filters for not to back up files of specific types. For example, you may want hidden and system files and folders not to be stored in the archive.

You can also apply custom filters, using the common masking rules. For example, to exclude all files with extension **.tib**, add ***.tib** mask. **My???.tib** mask will reject all **.tib** files with names, consisting of five symbols and starting with “my”.



All of these settings will take effect for the current task. How to set the default filters, that will be called each time you create a file backup task, see in *5.3 Setting backup options*.

7. Click **Next**.

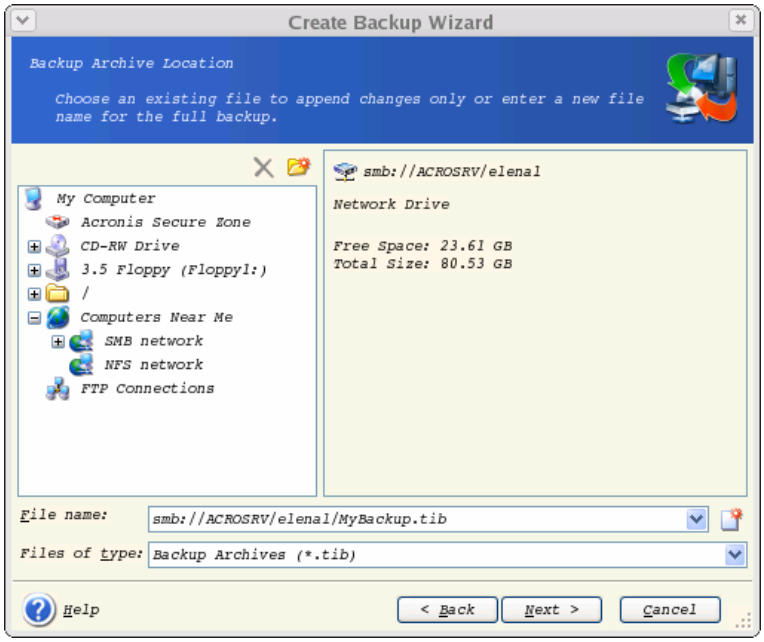
8. Select the name and location of the archive file.

If you are going to create a full backup, type the file name in the **File Name** line, or use the file name generator (a button to the right of the line). If you select an existing archive, it will be overwritten.

If you are going to create an incremental backup (see *3.2 Full, incremental and differential backups*), select the latest full or incremental backup you have.

In fact, if all incremental backup files are stored together, it doesn't matter which one you select, as the program will recognize them as a single archive. If you stored the files on several removable disks, you must provide the latest archive file; otherwise, restoration problems might occur.

If you are going to create a differential backup, select the full backup which will be a base, or any of existing differential archives. Either way, the program will create a new differential archive file.



The “farther” you store the archive from the original folders, the safer it will be in case of data damage. For example, saving the archive to another hard disk will protect your data if the primary disk is damaged. Data saved to a network disk, ftp-server or removable media will survive even if all your local hard disks are down. In addition to NFS, Acronis True Image Server for Linux supports the SMBFS network file system.

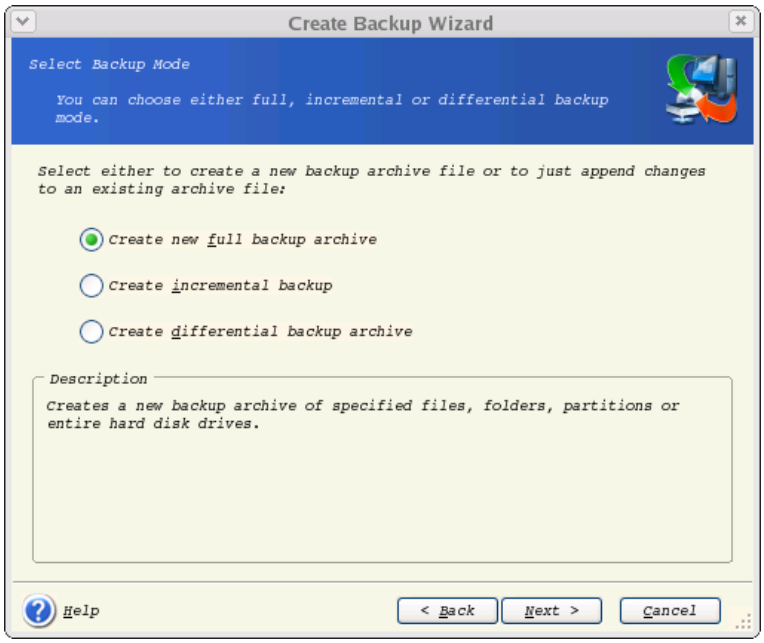
Please check, that the network backup node is accessible for Acronis True Image Server for Linux Rescue CD Network Browser, otherwise you cannot restore images stored on this node.

An FTP server must allow passive mode for file transfers. To enable data recovery directly from FTP server split the archive to files no more than 2 Gb in size.

You can also use Acronis Secure Zone (see details in *3.3 Acronis Secure Zone*) for storing backups. In that case, you need not provide the file name.

9. Click **Next**.

10. Select whether you want to create a full, incremental or differential backup. If you have not backed up the selected files/folders yet, or the full archive seems too old to append incremental changes to it, choose full backup. Otherwise it is recommended that you create an incremental or differential backup (see *3.2 Full, incremental and differential backups*).



11. Click **Next**.

12. Select the backup options (that is, backup file splitting, compression level, password protection, pre/post backup commands etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current backup task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *5.3 Setting backup options* for more information.

13. Click **Next**.

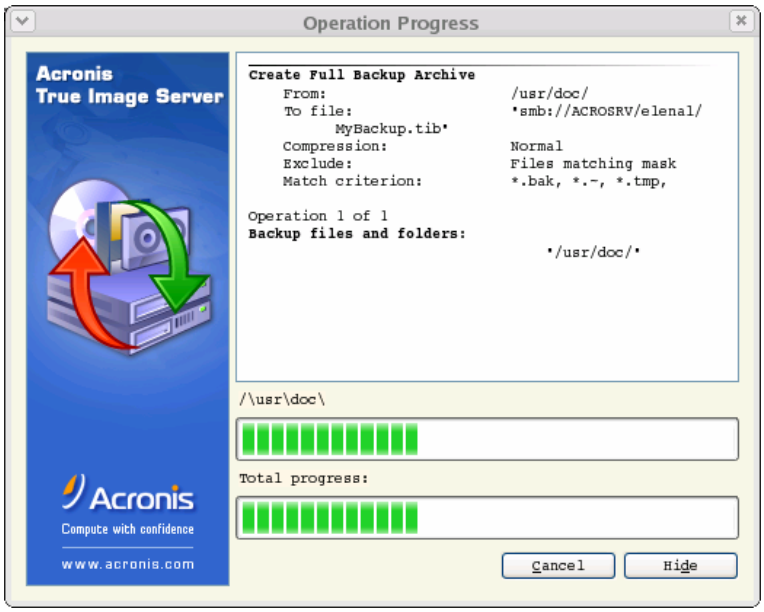
14. Provide a comment for the archive. This can help prevent you from restoring the wrong files. However, you can choose not to make any notes. The backup file size and creation date are automatically appended to the description, so you do not need to enter this information.

15. Click **Next**.

16. At the final step, the backup task summary is displayed. Up to this point, you can click **Back** to make changes in the created task. Clicking **Proceed** will launch the task execution.

17. The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the special window. You can stop the procedure by clicking **Cancel**.

You can also close the progress window by clicking **Hide**. The backup creation will continue, but you will be able to start another operation or close the main program window. In the latter case, the program will continue working in the background and will automatically close once the backup archive is ready. If you prepare some more backup operations, they will be queued after the current one.



If you burn an archive to several removable media, be sure to number them, since you will have to insert them in order during the restoration.

18. You may want to see the log when the task is completed. To view the log, click the **Show Operation Logs** button on the toolbar.

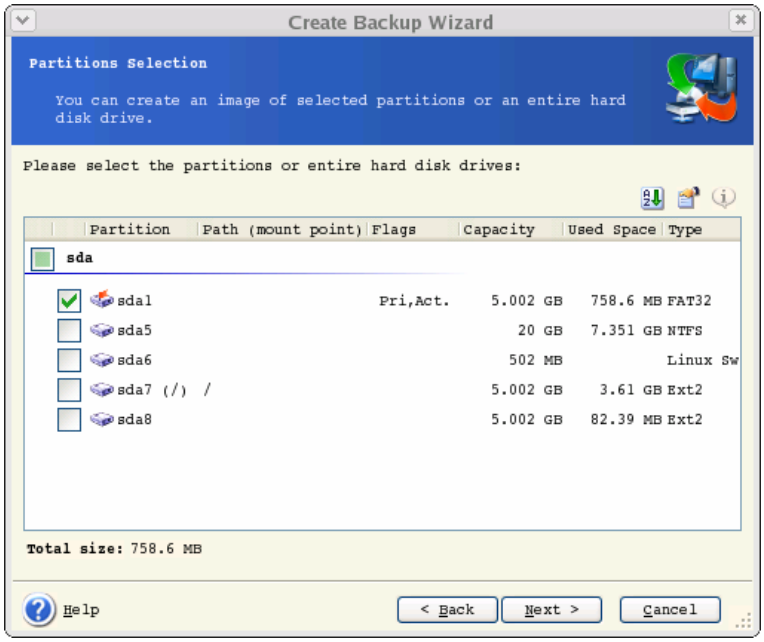
5.2 Backing up disks and partitions (image backup)

1. Invoke the **Create Backup Wizard** by clicking on the backup operation icon in the main program window.

2. Click **Next**.

3. Select **Backup disks** and click **Next**.

4. Select disks or partitions to back up. You can select a random set of disks and partitions.



5. Click **Next**.

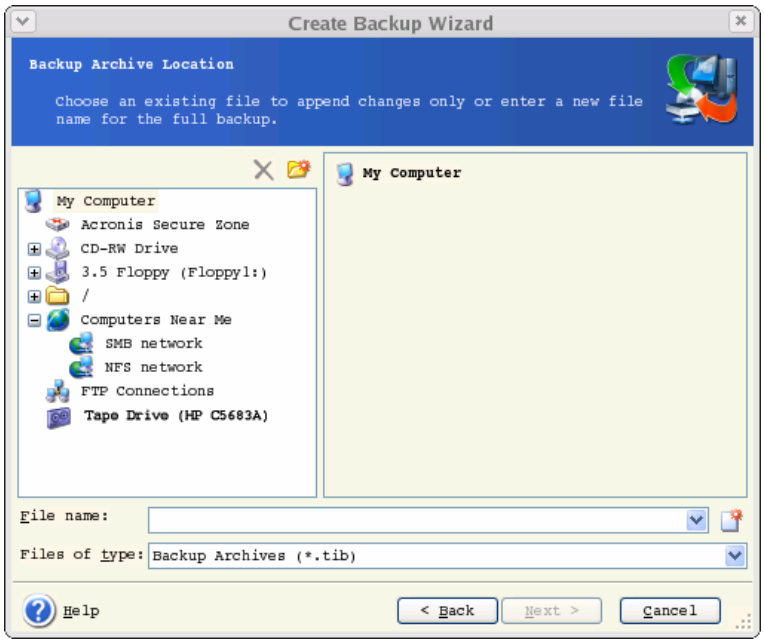
6. Select the name and location of the archive file.

If you are going to create a full backup, type the file name in the **File Name** line, or use the file name generator (a button to the right of the line). If you select an existing archive, it will be overwritten.

If you are going to create an incremental backup (see *3.2 Full, incremental and differential backups*), select the latest full or incremental backup you have.

In fact, if all incremental backup files are stored together, it doesn't matter which one you select, as the program will recognize them as a single archive. If you stored the files on several removable disks, you must provide the latest archive file; otherwise, restoration problems might occur.

If you are going to create a differential backup, select the full backup which will be a base, or any of existing differential archives. Either way, the program will create a new differential archive file.



The “farther” you store the archive from the original partition, the safer it will be in case of data damage. For example, saving the archive to another hard disk will protect your data if the primary disk is damaged. Data saved to a network disk, ftp-server or removable media will survive even if all your local hard disks are down. In addition to NFS, Acronis True Image Server for Linux supports the SMBFS network file system.

Please check, that the network backup node is accessible for Acronis True Image Server for Linux Rescue CD Network Browser, otherwise you cannot restore images stored on this node.

An FTP server must allow passive mode for file transfers. To enable data recovery directly from FTP server split the archive to files no more than 2 Gb in size.

You can also use Acronis Secure Zone (see details in *3.3 Acronis Secure Zone*) for storing backups. In that case, you need not provide the file name.

7. Click **Next**.

8. Select whether you want to create a full, incremental or differential backup. If you have not backed up the selected disks/partitions yet, or the full archive seems too old to append incremental changes to it, choose full backup. Otherwise it is recommended that you create an incremental or differential backup (see *3.2 Full, incremental and differential backups*).

9. Click **Next**.

10. Select the backup options (that is, backup file splitting, compression level, password protection, pre/post backup commands etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current backup task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *5.3 Setting backup options* for more information.

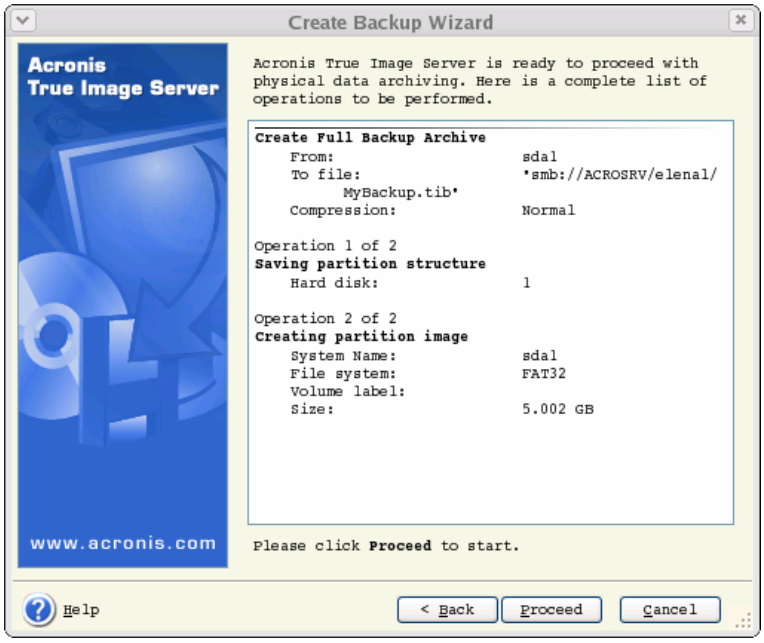
11. Click **Next**.

12. Provide a comment for the archive. This can help prevent you from restoring the wrong disk/partition. However, you can choose not to make any notes. The backup file size and

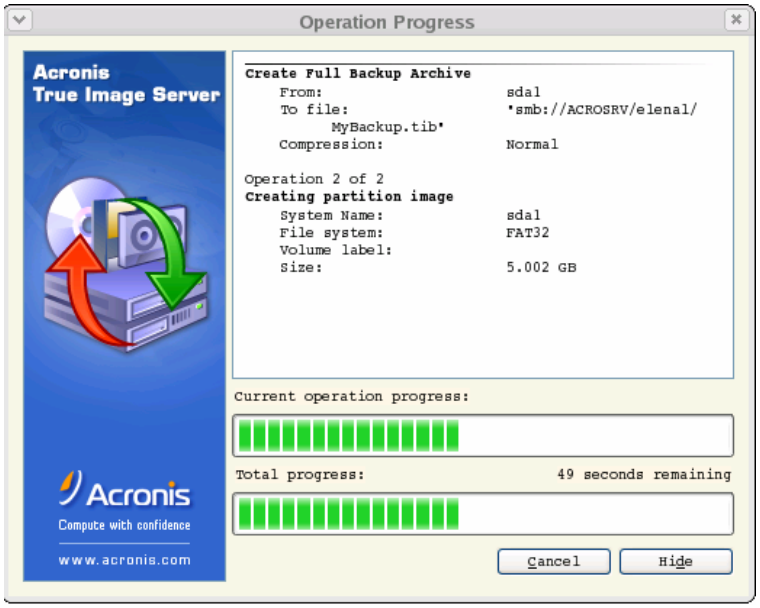
creation date are automatically appended to the description, so you do not need to enter this information.

13. Click **Next**.

14. At the final step, the backup task summary is displayed. Up to this point, you can click **Back** to make changes in the created task. Clicking **Proceed** will launch the task execution.



15. The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the special window. You can stop the procedure by clicking **Cancel**.



You can also close the progress window by clicking **Hide**. The backup creation will continue, but you will be able to start another operation or close the main program window. In the latter case, the program will continue working in the background and will automatically close

once the backup archive is ready. If you prepare some more backup operations, they will be queued after the current one.

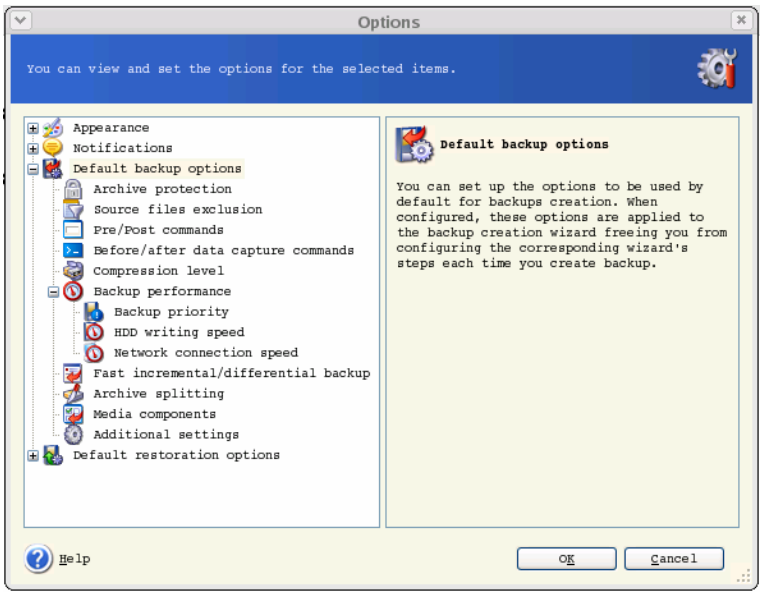
If you burn an archive to several removable media, be sure to number them, since you will have to insert them in order during the restoration.

16. You may want to see the log when the task is completed. To view the log, click the **Show Operation Logs** button on the toolbar.

5.3 Setting backup options

To view or edit the default backup options, select **Tools -> Options -> Default Backup Options** from the main program menu.

You can edit the default (or set the temporary) backup options while creating a backup task as well.



5.3.1 Archive protection

The default setting – **no password**.

An archive can be protected with a password. To protect the archive from being restored by anybody except you, enter a password and its confirmation into the text fields. A password should consist of at least eight symbols and contain both letters (in the upper and lower cases preferably) and numbers to make it more difficult to guess.

If you try to restore data from a password-protected archive, or append an incremental/differential backup to such an archive, Acronis True Image Server for Linux will ask for the password in a special window, allowing access only to authorized users.

5.3.2 Source files exclusion

The default setting – **all files from the selected folders will be included into the archive**.

You can set the default filters for not to back up files of specific types. For example, you may want hidden and system files and folders not to be stored in the archive.

You can also apply custom filters, using the common masking rules. For example, to exclude all files with extension **.tib**, add ***.tib** mask. **My???.tib** mask will reject all **.tib** files with names, consisting of five symbols and starting with "my".

This option is effective for file/folders backup only. When creating a disk/partition image, you cannot filter out any files.

5.3.3 Pre/post commands

You can specify commands or executable files to be automatically executed before and after the backup procedure. For example, you may want to remove some tmp files from the disk before starting backup or configure a third-party antivirus product to be started each time before the backup starts. Click **Edit** to open the **Edit Command** window where you can easily input the command, its arguments and working directory or browse folders to find an executable file.

Unchecking the **Do not perform operations** until the commands execution is complete box, checked by default, will permit the backup process to run concurrently with your commands execution.

5.3.4 Before/after data capture commands

Database servers, such as My SQL Server, prove to be troublesome to backup, partially due to open files and indexes and partially due to rapid data changes. Therefore many system administrators prefer to suspend the database at the backup (capturing the Snapshot) moment.

To ensure that the database will be ready to access immediately after recovery, the administrator must ensure completion of all transactions before the backup process starts. Once the backup process starts, you can resume server operations. It is not necessary to suspend the applications for the duration of the imaging process.

The transactions completion can be ensured with executing scripts that pause the appropriate services and automatically resume them after data capture.

Create scripts in any text editor (for example, name it 'pause_services.bat' and 'resume_services.bat'. Use **Edit** buttons to the right of **Before data capture command** and **After data capture command** fields, to open the **Edit Command** window where you can browse folders to find the respective scripts. A single command can be specified in the same window along with its arguments and working directory.

It is critical to note that these commands, as opposed to **Pre/post commands** above, will be executed before and after data capture process, which takes seconds, while the entire backup procedure may take quite long time. Therefore, the database idle time will be minimal.

Unchecking the **Do not perform operations until the commands execution is complete** box, checked by default, will permit the backup process to run concurrently with your commands execution.

5.3.5 Compression level

The default setting – **Normal**.

If you select **None**, the data will be copied without any compression, which may significantly increase the backup file size. However, if you select **Maximum** compression, the backup will take longer to create.

The optimal data compression level depends on the type of files stored in the archive. For example, even maximum compression will not significantly reduce the archive size if the archive contains essentially compressed files, like .jpg, .pdf or .mp3.

Generally, it is recommended that you use the default **Normal** compression level. You might want to select **Maximum** compression for removable media to reduce the number of blank disks required.

5.3.6 Backup performance

The three options below might have a more or less noticeable effect on the backup process speed. This depends on overall system configuration and physical characteristics of devices.

1. Backup process priority

The default setting – **Low**.

The priority of any process, running in a system, determines the amount of CPU usage and system resources allocated to that process. Decreasing the backup priority will free more resources for other CPU tasks. Increasing of backup priority may speed up the backup process due to taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

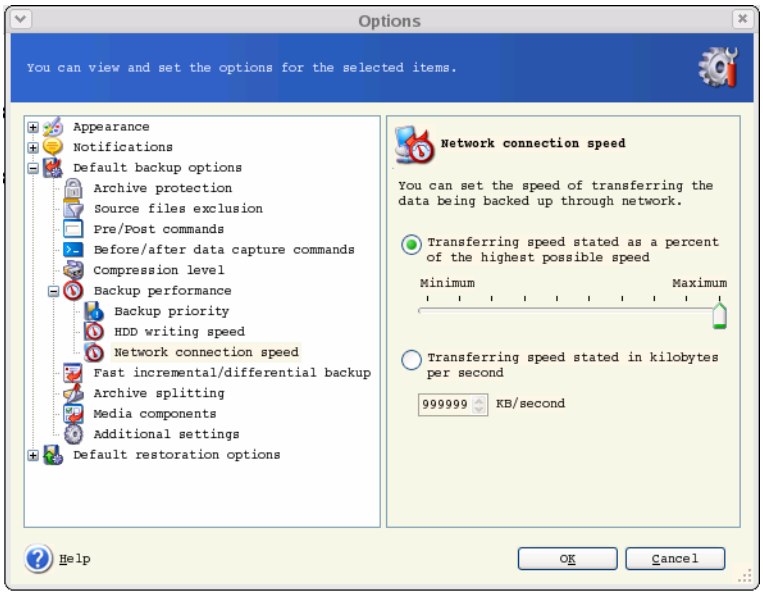
2. HDD writing speed

The default setting – **Maximum**.

Backing up in the background to an internal hard disk (for example, to Acronis Secure Zone) may slow other programs performance because of large amounts of data transferred to the disk. You can limit the hard disk usage by Acronis True Image Server for Linux to a desired level. To set the desired HDD writing speed for data being backed up, drag the slider or enter the writing speed in kilobytes per second.

3. Network connection speed

The default setting – **Maximum**.



If you frequently backup data to network drives, think of limiting the network usage used by Acronis True Image Server for Linux. To set the desired data transfer speed, drag the slider or enter the bandwidth limit for transferring backup data in kilobytes per second.

5.3.7 Fast incremental/differential backup

The default setting – **Use fast incremental/differential backup**.

Incremental/differential backup captures only changes in data occurred since the last backup. To speed up the backup process, Acronis True Image Server for Linux determines whether the file has changed by file size and the date/time when the file was last saved. Disabling this feature will make the program compare the entire file contents to that stored in the archive.

This option relates only to disk/partition (image) backup.

5.3.8 Archive splitting

Sizeable backups can be split into several files that together make the original backup. A backup file can be split for burning to removable media or saving on ftp-server (data recovery directly from ftp-server requires the archive to be split into files no more than 2 Gb in size).

The default setting – **Automatic**. With this setting, Acronis True Image Server for Linux will act as follows.

When backing up to the hard disk: If the selected disk has enough space and its file system allows the estimated file size, the program will create a single archive file.

If the storage disk has enough space, but its file system does not allow the estimated file size, Acronis True Image Server for Linux will automatically split the backup into several files.

If you do not have enough space to store the image on your hard disk, the program will warn you and wait for your decision as to how you plan to fix the problem. You can try to free some additional space and continue or click **Back** and select another disk.

When backing up to a diskette or CD-R/RW: Acronis True Image Server for Linux will ask you to insert a new disk when the previous one is full.

Alternatively, you can select **Fixed size** and 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. That comes in handy when backing up to a hard disk with a view to burning the archive to CD-R/RW or DVD±R/RW later on.

Creating images directly on CD-R/RW might take considerably more time than it would on a hard disk.

5.3.9 Media components

The default setting – **disabled**.

When backing up to removable media, you can make this media bootable by writing to it additional components. Thus, you will not need a separate rescue disk.

Choose the basic components, necessary for boot and restoring data, on the **General** tab.

The **Acronis One-Click Restore** is a minimal addition to your rescue media, allowing one-click data recovery from an image archive, stored on this media. This means that at boot from the media and clicking "restore" all data will be silently restored to the original place. No options or selections like resizing partitions will be possible.

If you want more functionality during restoration, write a standalone version of Acronis True Image Server for Linux to the rescue disk. Then you will be able to configure the restore task using **Restore Data Wizard**.

Under **Advanced** tab you can select full, safe or both Acronis True Image Server for Linux loader version. The safe version does not have USB, PC card or SCSI drivers and is useful only in case the full version does not load.

In case you check **Do not place additional components if there is no free space** box, the program will try to write at least basic components to media, short of space.

5.3.10 Additional settings

1. Validate backup archive upon operation completion

The default setting – **disabled**.

When enabled, the program will check integrity of the just created or supplemented archive immediately after backup.

To check archive data integrity you must have all incremental and differential backups belonging to the archive and the initial full backup. If any of successive backups is missing, validation is not possible.

2. Overwrite data on a tape without user confirmation

The default setting – **disabled**.

A full backup, when created on a tape drive, overwrites all data stored on the tape (see *3.9 Backing up to tape drive* for more information). In this situation, Acronis True Image Server for Linux will warn that you are about to lose data on the tape. To disable this warning, check the middle box.

3. Ask for first media while creating backup archives on removable media

The default setting – **enabled**.

You can choose whether to display the **Insert First Media** prompt when backing up to removable media. With the default setting, backing up to removable media may be impossible if the user is away, because the program will wait for pressing **OK** in the prompt box. Therefore, you should disable the prompt when scheduling a backup to removable media. Then, if the removable media is available (for example, CD-R/RW inserted) the task can run unattended.

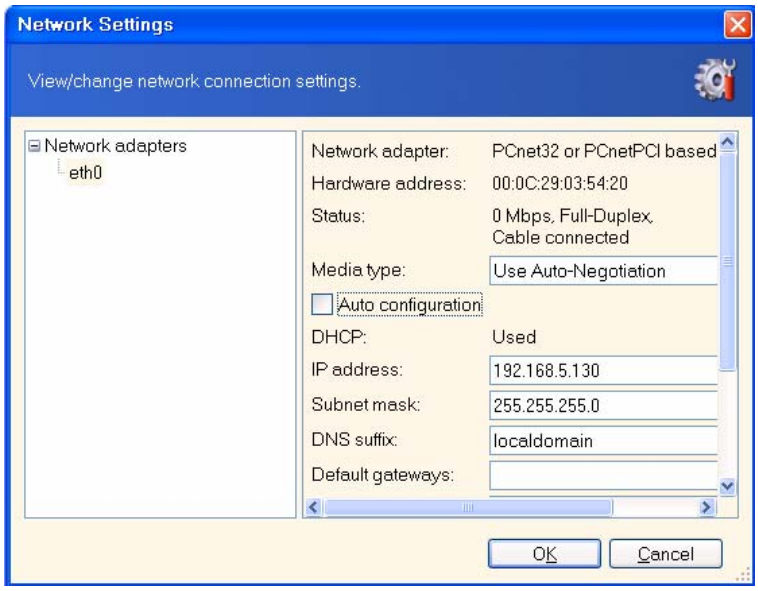
Chapter 6. Restoring the backup data under X Window System

This chapter describes data recovery using Acronis True Image Server for Linux GUI under X Window System. See *Chapter 11* for using console.

6.1 Network settings in rescue mode

When booted from removable media or by Startup Recovery Manager, Acronis True Image Server for Linux may not detect the network. Such might be the case if there is no DHCP server in your network or your computer address was not identified automatically for some reason.

To enable connection, specify network settings manually in the window, available at **Tools -> Options -> Network adapters**.



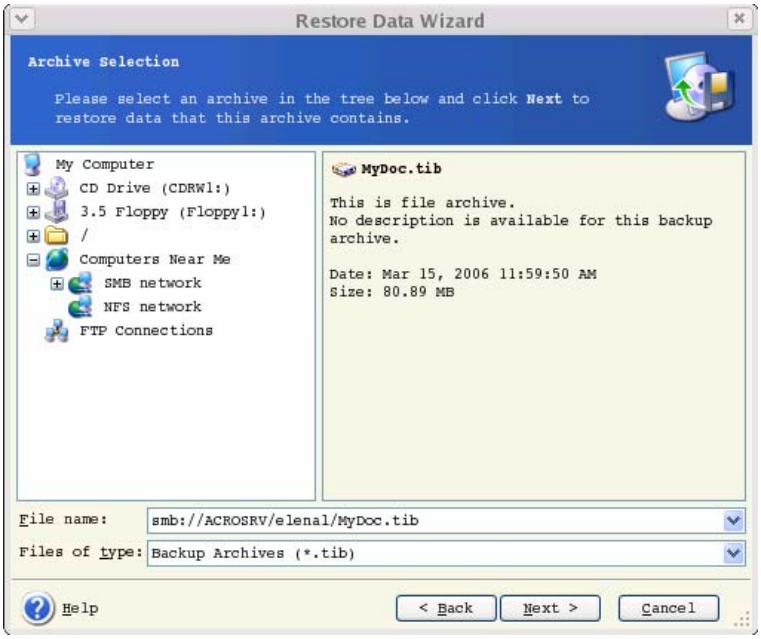
6.2 Restoring files and folders from file archives

Here we describe how to restore file/folders from a file backup archive. You can restore the desired files/folders from a disk/partition image as well. To do so, mount the image (see *9.1 Mounting an image* or *11.3 Restoring files with trueimagemnt*), or start the image restoration and select **Restore specified files or folders** (see *6.3 Restoring disks/partitions or files from images)*.

1. Invoke the **Restore Data Wizard** by clicking on the recovery operation icon in the main program window.

2. Click **Next**.

3. Select the archive. If the archive is located in Acronis Secure Zone, select it to choose the archive on the next step.



If the archive is located on removable media, e.g. CD, first insert the last CD and then insert disks in reverse order when **Restore Data Wizard** prompts.

Data recovery directly from ftp-server requires the archive to consist of files no more than 2 Gb in size. If you suppose that some of the files may be larger, first copy the entire archive (along with the initial full backup) to a local hard disk or network share disk.

If you added a comment to the archive, it will be displayed to the right of the drives tree. If the archive was protected with a password, Acronis True Image Server for Linux will ask for it. The comment and the **Next** button will be unavailable until you enter the correct password.

4. Click **Next**.

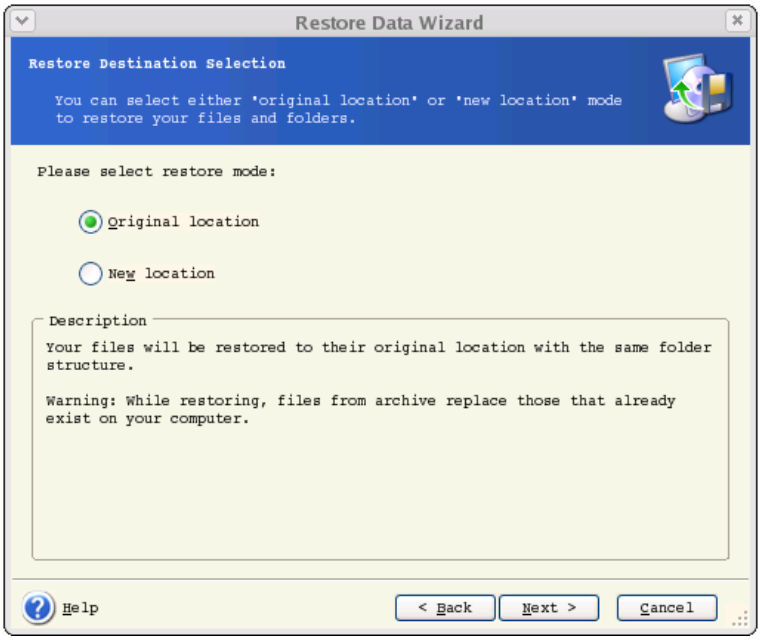
5. If you are to restore files from an archive, containing incremental backups, Acronis True Image Server for Linux will suggest that you select one of successive incremental backups by date/time of its creation. Thus, you can return the files/folders to a certain moment.

To restore data from an incremental backup, you must have all previous incremental backup files and the initial full backup. If any of successive backups is missing, restoration is impossible.

To restore data from a differential backup, you must have the initial full backup as well.

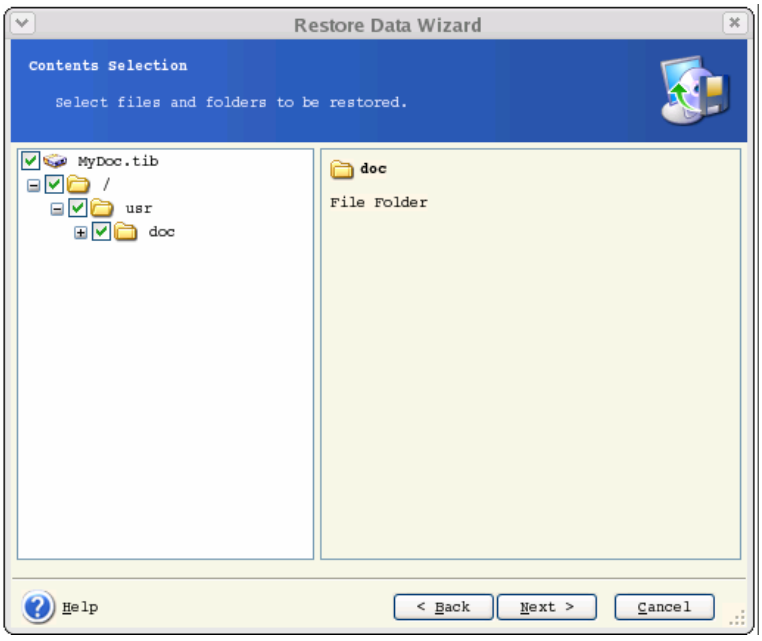
6. Click **Next**.

7. Select a folder on your computer where you want to restore selected folders/files (a target folder). You can restore data to their original location or choose another folder, if necessary.



8. Click **Next**.

9. Select files and folders to restore. You can choose to restore all data or browse the archive contents and select the desired folders or files.



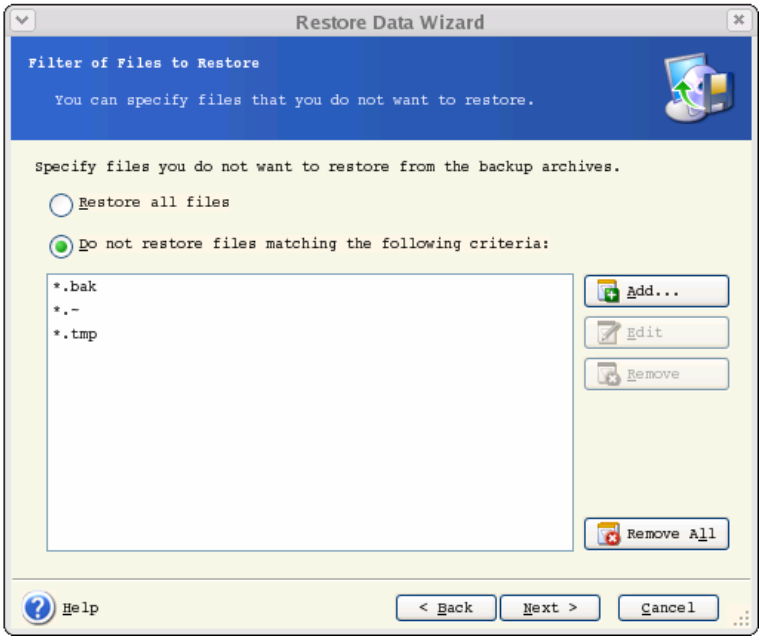
10. Click **Next**.

11. Select the options for restoration process (that is, pre/post restoration commands, restoration process priority etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current restore task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *6.5 Setting restore options* for more information.

12. Click **Next**.

13. Set filters for not to restore files of specific types. For example, you may want hidden and system files and folders not to be restored from the archive.

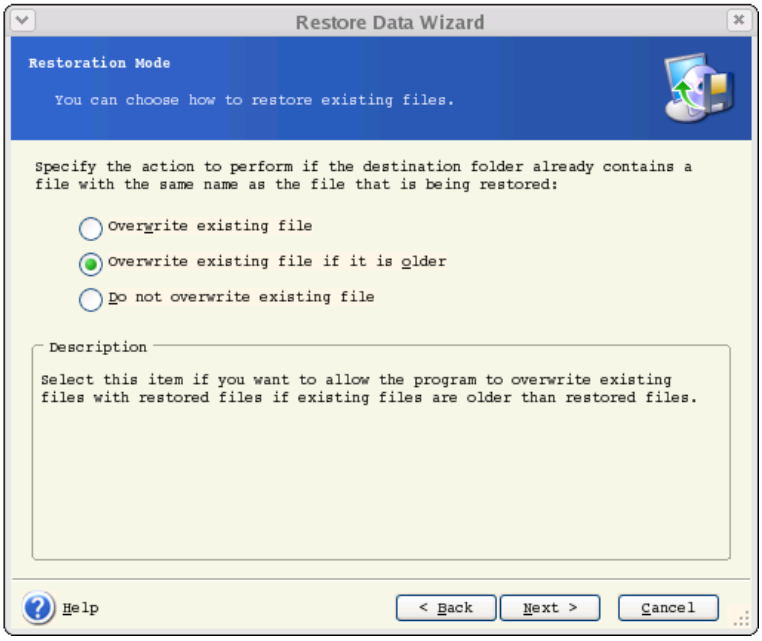
You can also apply custom filters, using the common masking rules. For example, to exclude all files with extension **.tib**, add ***.tib** mask. **My???.tib** mask will reject all **.tib** files with names, consisting of five symbols and starting with “my”.



All of these settings will take effect for the current task. How to set the default filters, that will be called each time you restore data, see in *6.5.1 Files to restore exclusion*.

14. Click **Next**.

15. The next selection allows you to keep useful data changes, made since the selected backup. Choose what to do if the program finds in the target folder a file with the same name as in the archive.

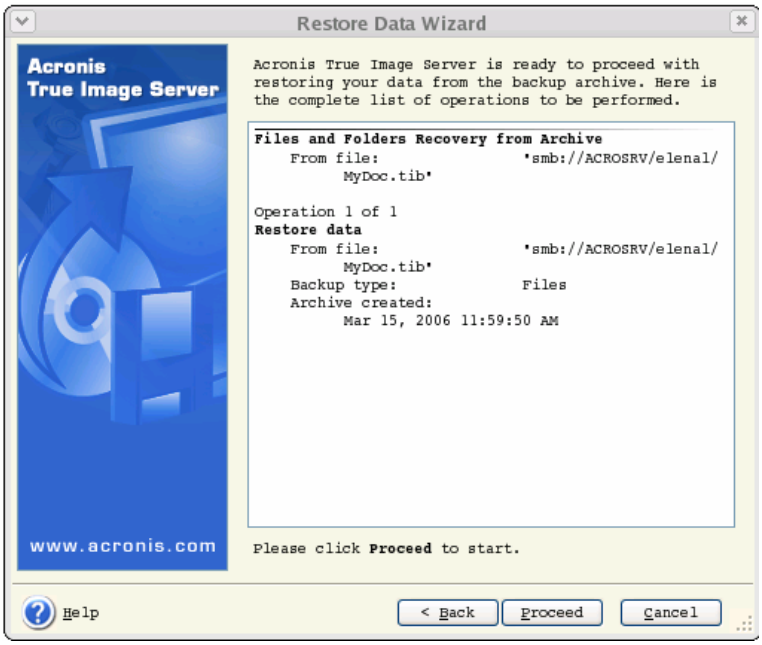


Overwrite existing file – this will give the archived file unconditional priority over the file on the hard disk.

Overwrite existing file if it is older – this will give the priority to the most recent file modification, whether it is in the archive or on the disk

Do not overwrite existing file – this will give the file on the hard disk unconditional priority over the archived file.

16. At the final step, the restoration summary is displayed. Up to this point, you can click **Back** to make changes in the created task. Clicking **Proceed** will launch the task execution.



17. The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the special window. You can stop the procedure by clicking **Cancel**. Please keep in mind that the aborted procedure still may cause changes in the destination folder

6.3 Restoring disks/partitions or files from images

To restore a partition (disk) from an image, Acronis True Image Server for Linux must obtain exclusive access to the target partition (disk). This means no other applications can access it at that time. If you receive a message stating that the partition (disk) can not be blocked, close applications that use this partition (disk) and start over. If you can not determine which applications use the partition (disk), close them all.

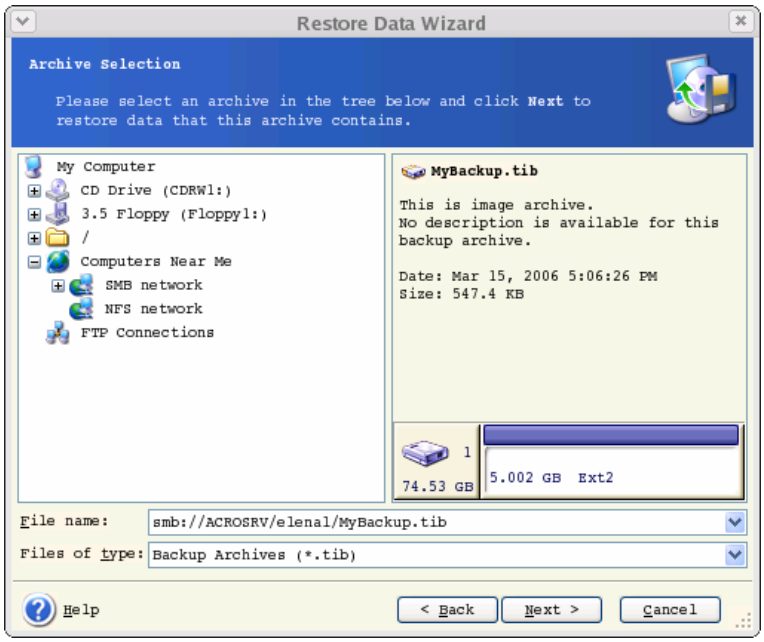
6.3.1 Starting the Restore Data Wizard

1. Invoke the **Restore Data Wizard** by clicking on the restore operation icon in the main program window.

2. Click **Next**.

6.3.2 Archive selection

1. Select the archive. If the archive is located in Acronis Secure Zone, select it to choose the archive at the next step.



If the archive is located on removable media, e.g. CD, first insert the last CD and then insert disks in reverse order when **Restore Data Wizard** prompts.

Data recovery directly from ftp-server requires the archive to be split into files no more than 2 Gb in size. If you suppose that some of the files may be larger, first copy the entire archive (along with the initial full backup) to a local hard disk or network share disk.

If you added a comment to the archive, it will be displayed to the right of the drives tree. If the archive was protected with a password, Acronis True Image Server for Linux will ask for

it. The partitions layout, the comment and the **Next** button will be unavailable until you enter the correct password.

2. Click **Next**.

3. If you are to restore data from an archive, containing incremental backups, Acronis True Image Server for Linux will suggest that you select one of successive incremental backups by date/time of its creation. Thus, you can return the disk/partition to a certain moment.

To restore data from an incremental backup, you must have all previous incremental backup files and the initial full backup. If any of successive backups is missing, restoration is impossible.

To restore data from a differential backup, you must have the initial full backup as well.

4. Click **Next**.

6.3.3 Restoration type selection

1. Select what you want to restore:

Restore specified files or folders

With this selection, you will be further offered to select where to restore selected folders/files (original or new location), choose files/folders to be restored and so on. These steps look like those in file archive restore. However, watch your selection: if you are to restore files instead of disk/partition, uncheck the unnecessary folders. Otherwise you will restore a lot of excessive files. Then you will be taken directly to Restoration Summary screen (*6.3.11 Restoration summary and executing restoration*).

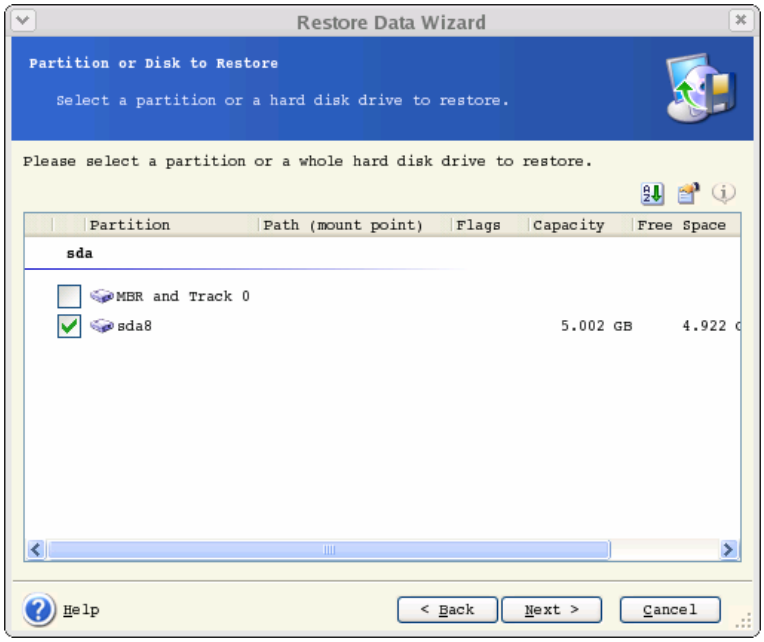
Restore disks or partitions

Having selected a usual way of disks/partitions recovery, you will have to make all settings described below.

2. Click **Next**.

6.3.4 Selecting a disk/partition to restore

1. The selected archive file can contain images of several partitions or even disks. Select which disk/partition to restore.

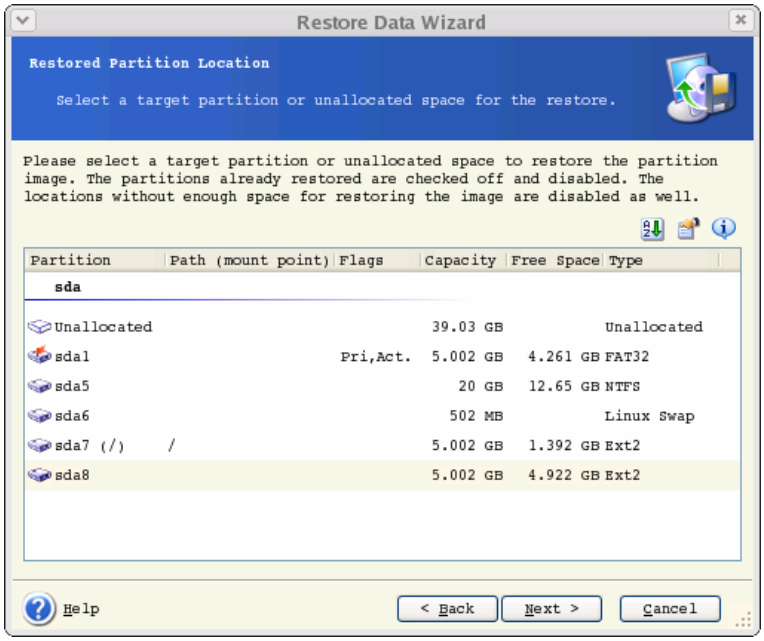


Disks and partitions images contain a copy of track 0 along with MBR (Master Boot Record). It appears in this window in a separate line. You can choose whether to restore MBR and track 0 by checking the respective box. Restore MBR if it is critical to your system boot.

2. Click **Next**.

6.3.5 Selecting a target disk/partition

1. Select a target disk or partition where you want to restore the selected image. You can restore data to their initial location, to another disk/partition or to an unallocated space. The target partition should be at least the same size as the uncompressed image data.



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

2. Click **Next**.

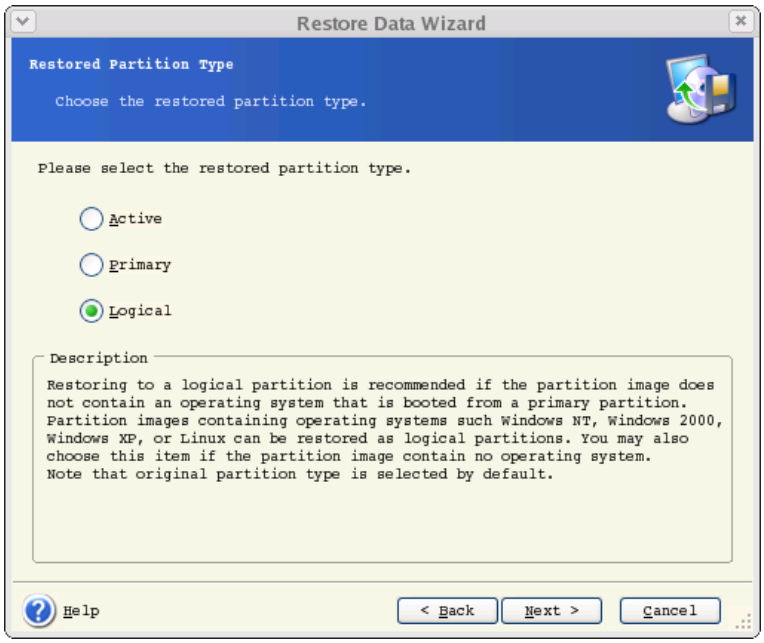
6.3.6 Changing the restored partition type

1. When restoring a partition, you can change its type, though it is not required in most cases.

To illustrate why you might need to do this, let's imagine that both the operating system and data were stored on the same primary partition on a damaged disk.

If you are restoring a system partition to the new (or the same) disk and want to load an operating system from it, you will select **Active**.

If you restore a system partition to another hard disk with its own partitions and OS, most probably, you will need only the data. In this case, you can restore the partition as **Logical** to access the data only.



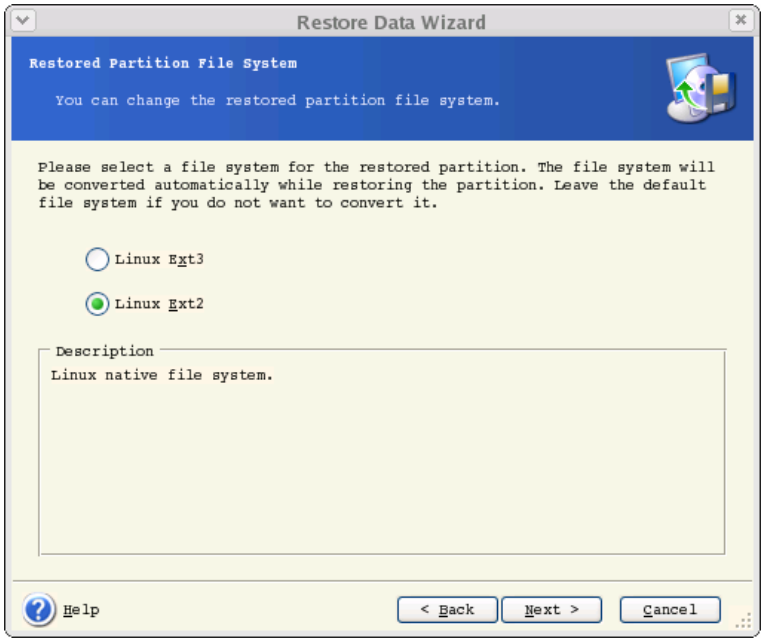
By default, the original partition type is selected.

Selecting **Active** for a partition without an installed operating system could prevent your server from booting.

2. Click **Next**.

6.3.7 Changing the restored partition file system

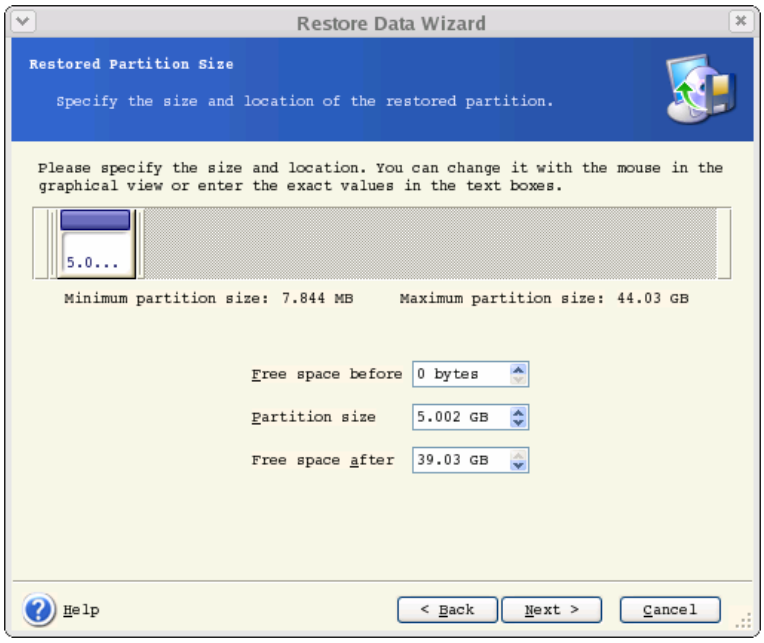
1. Though seldom required, you can change the partition file system during its restoration. Acronis True Image Server for Linux can make the following file system conversions: **FAT 16 -> FAT 32, Ext2 -> Ext3**. For partitions with other native file systems this option is not available.



2. Click **Next**.

6.3.8 Changing the restored partition size and location

1. You can resize and relocate a partition by dragging it or its borders with a mouse or by entering corresponding values into the appropriate fields.



Using this feature, you can redistribute the disk space between partitions being restored. In this case, you will have to restore the partition to be reduced first.

These changes might be useful if you are to copy your hard disk to a new high-capacity one by creating its image and restoring it to a new disk with larger partitions.

2. Click **Next**.

6.3.9 Restoring several partitions at once

1. During a single session, you can restore several partitions or disks, one by one, by selecting one disk and setting its parameters first and then repeating these actions for every partition or disk to be restored.

If you want to restore another disk (partition), select **Yes, I want to restore another partition or hard disk drive**. Then you will return to the partition selection window (6.3.4) again and will have to repeat the above steps. Otherwise, don't set this switch.

2. Click **Next**.

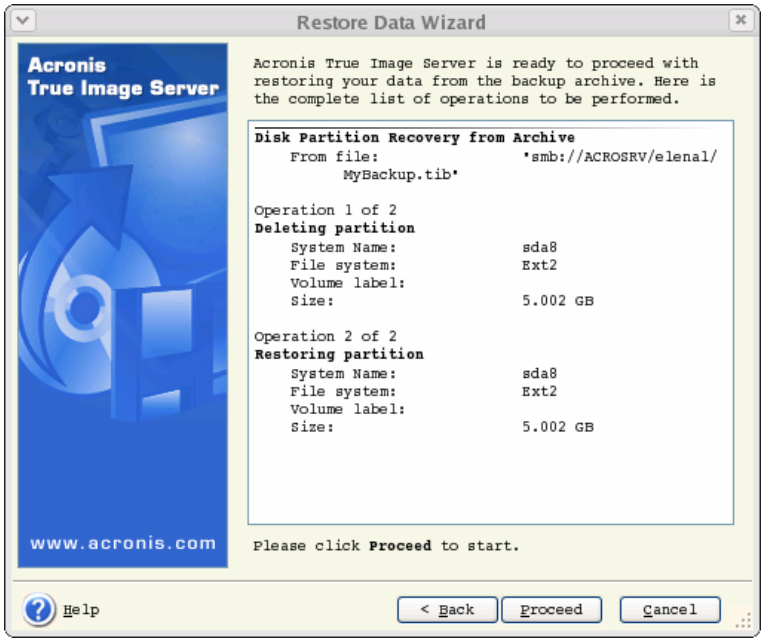
6.3.10 Setting restore options

1. Select the options for restoration process (that is, pre/post restoration commands, restoration process priority etc.). You may **Use default options** or **Set the options manually**. If the latter is the case, the settings will be applied only to the current restore task. Alternatively, you can edit the default options from the current screen. Then your settings will be saved as default. See *6.5 Setting restore options* for more information.

2. Click **Next**.

6.3.11 Restoration summary and executing restoration

1. At the final step, the restoration summary is displayed. Up to this point, you can click **Back** to make changes in the created task. If you click **Cancel**, no changes will be made to disk(s). Clicking **Proceed** will launch the task execution.



2. The task will appear on the **Active tasks** pane of the main window. The task progress will be shown in the special window.

You can stop the procedure by clicking **Cancel**. However, it is critical to note that the target partition will be deleted and its space unallocated – the same result you will get if the restoration is unsuccessful. To recover the "lost" partition, you will have to restore it from the image again.

If you restore a system disk (partition), you might have to reactivate your boot manager. Please consult your boot loader manual pages to find out the appropriate information.

In case the system disk (partition) is restored to identical hardware, the following steps would usually help:

Boot the computer from the Linux installation CD

Enter rescue mode

Issue the following commands:

#mkdir /mnt/tmp

#mount /dev/hdXY /mnt/tmp (/dev/hdXY is the device, corresponding to root partition)

#chroot /mnt/tmp

If /boot is a separate partition, mount it with

#mount /dev/hdXZ /boot (/dev/hdXZ is the device, corresponding to boot partition)

Issue a command according to your loader type:

LILO:

#/sbin/lilo

GRUB:

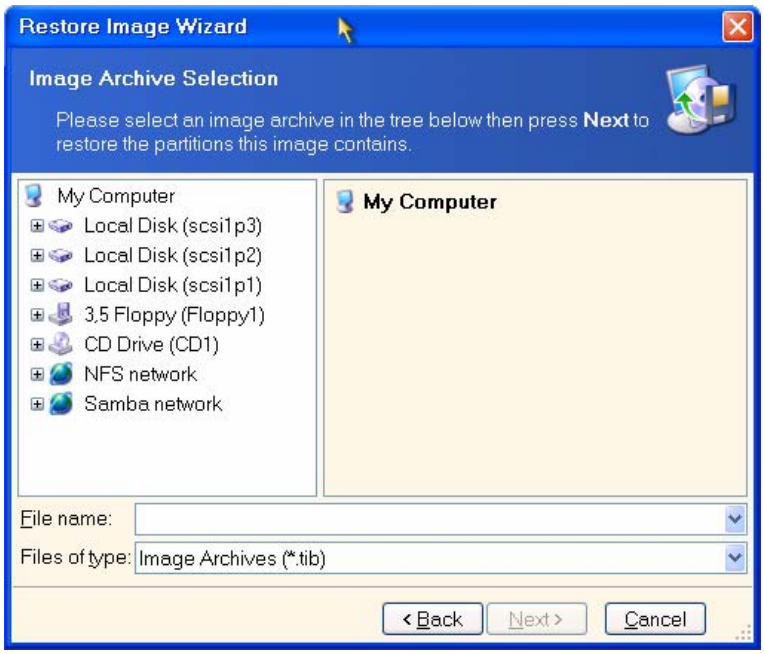
#/sbin/grub-install /device_name (/device_name is hd: hda, hdal, hda2, sdal, sda2 etc)

6.4 Restoring data with a rescue CD

To restore data from an archive, using a rescue CD of Acronis True Image Server for Linux, you initially have to create such disk as described in *Chapter 10 Creating bootable media*.

Insert the rescue CD and reboot (you might have to enable the CD bootup option in BIOS). You will see a standard Acronis True Image Server for Linux main window (see *Chapter 4 Main program interface under X Window System*).

The procedure of disk (partition) restoration from an image is almost identical to the one described above. The only difference is that the **Archive Selection** window will list all local disks (partitions) as unmounted:



Selecting an archive when booted from a rescue CD

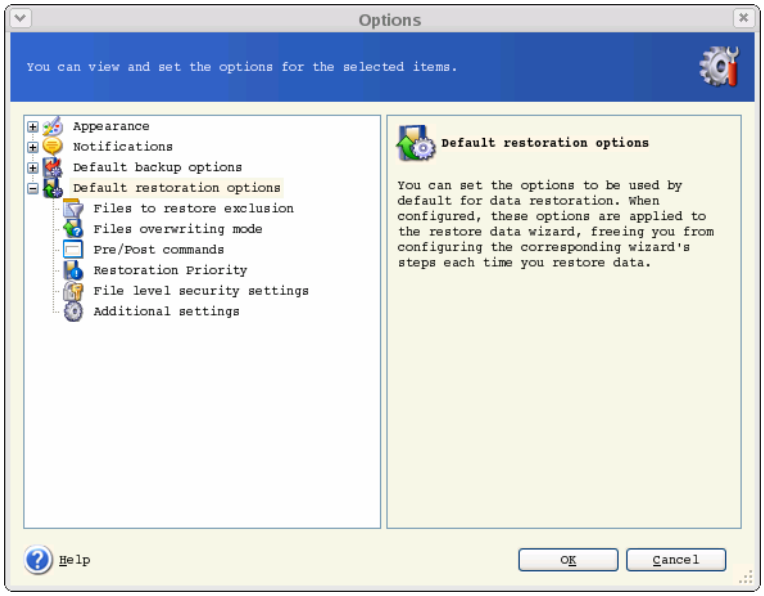
In rescue mode Acronis True Image Server for Linux cannot access LVM disks. This means that an LVM volume image can be deployed on a MBR disk only.

A system, restored from an LVM volume image over an MBR disk, cannot boot because its kernel tries to mount the root at LVM volume. To boot the system, change the loader configuration and /etc/fstab so that LVM is not used. Then reactivate your boot manager as described in 6.3.11.

6.5 Setting restore options

To view or edit the default restore options, select **Tools -> Options -> Default Restoration Options** from the main program menu.

You can edit the default (or set the temporary) restore options while creating a restore task as well.



6.5.1 Files to restore exclusion

The default setting – **Restore all files**.

You can set the default filters for not to restore files of specific types. Use the common masking rules. For example, to exclude all files with extension **.tib**, add ***.tib** mask. **My???.tib** mask will reject all **.tib** files with names, consisting of five symbols and starting with “my”.

This option is effective only when restoring files from file/folders archives. When restoring files from a disk/partition image, you cannot filter out any files.

6.5.2 Files overwriting mode

This option allows you to keep useful data changes, made since the backup being restored was done. 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 archived file unconditional priority over the file on the hard disk.

Overwrite existing file if it is older – this will give the priority to the most recent file modification, whether it is in the archive or on the disk.

Do not overwrite existing file – this will give the file on the hard disk unconditional priority over the archived file.

This option is effective only when restoring files from file/folders archives.

6.5.3 Pre/post commands

You can specify commands or batch files to be automatically executed before and after the restore procedure. Click **Edit** to open the **Edit Command** window where you can easily input the command, its arguments and working directory or browse folders to find a batch file.

Unchecking the **Do not perform operations until the commands execution is complete** box, checked by default, will permit the restore procedure to run concurrently with your commands execution.

6.5.4 Restoration priority

The default setting – **Low**.

The priority of any process, running in a system, determines the amount of CPU usage and system resources allocated to that process. Decreasing the restoration priority will free more resources for other CPU tasks. Increasing of restoration priority may speed up the restore process due to taking resources from the other currently running processes. The effect will depend on total CPU usage and other factors.

6.5.5 File-level security settings

The default setting – **Restore files with their security settings**.

You can choose whether to restore the original files' security settings (i.e. permissions for read, write and execute, set in file **Properties -> Permissions**), or let the files inherit the security settings of the folder where they will be restored.

This option is effective only when restoring files from file/folders archives.

6.5.6 Additional settings

1. You can choose whether to restore files' date and time from the archive or assign the files the current date and time.

2. Before data is restored from the archive, Acronis True Image Server for Linux can check its integrity. If you suspect that the archive might have been corrupted, select **Validate backup archive before restoration**.

To check archive data integrity you must have all incremental and differential backups belonging to the archive and the initial full backup. If any of successive backups is missing, validation is not possible.

3. Having restored a disk/partition from an image, Acronis True Image Server for Linux can check the integrity of its file system. To do so, select **Check file system** after restoration.

Verification of the file system is available only when restoring disk/partitions under Linux (i.e. not in standalone Acronis True Image Server for Linux version, booted from the rescue CD) and only for Ext2, Ext3, Reiser4, ReiserFS, Linux Swap, XFS and JFS file systems.

Chapter 7. Scheduling tasks

Acronis True Image Server for Linux allows you to schedule periodic backup tasks. Doing so will give you peace of mind, knowing that your data are safe.

You can create more than one independently scheduled task. For example, you can back up your current project daily and back up the application disk once a week.

All the scheduled tasks appear in the **Active Tasks** area of the main window. You can start, stop, edit, delete and rename the scheduled tasks.

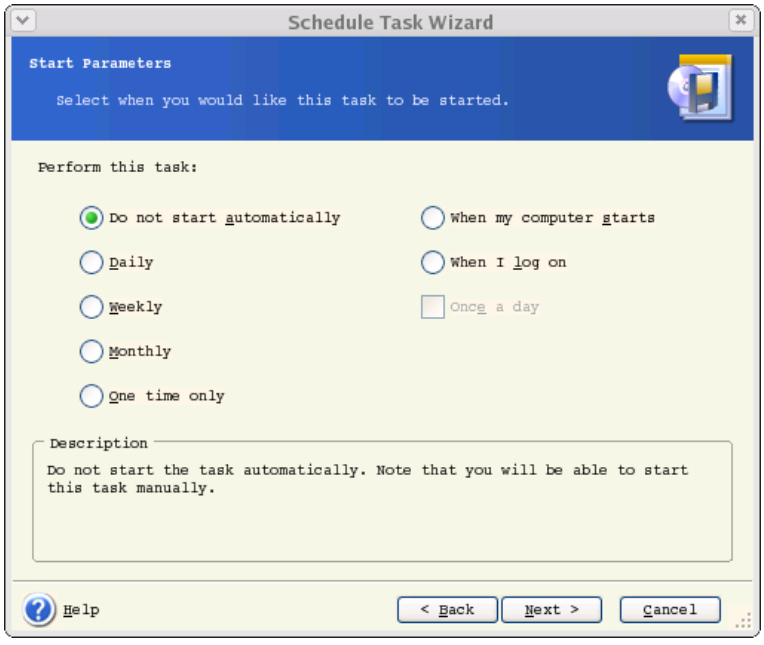
7.1 Creating scheduled tasks

1. To invoke the **Schedule Task Wizard**, click on its icon on the **Active Tasks** toolbar or select **Operations -> Schedule Task** from the main menu.

2. Click **Next**.

3. Configure a backup task in the usual way (see *Chapter 5 Creating backup archives under X Window System*). If you choose to create the backup archive on a network drive, you will have to enter a user name and a password for network access.

4. Set the task execution periodicity.



Do not start automatically – the task will be saved, but not launched automatically. You will be able to launch it later by clicking the start button on the Active Tasks pane

- **Daily** – the task will be executed once a day or once in several days

- **Weekly** – the task will be executed once a week or once in several weeks on selected day
- **Monthly** – the task will be executed once a month on the selected day
- **One time only** – the task will be executed once at the specified time and day
- **When my computer starts** – the task will be executed at every OS startup
- **When I log on** – the task will be executed each time the current user logs in to the OS
- **When my computer shuts down** – the task will be executed before every server shutdown or reboot
- **When I log off** – the task will be executed each time the current user logs off of the OS.

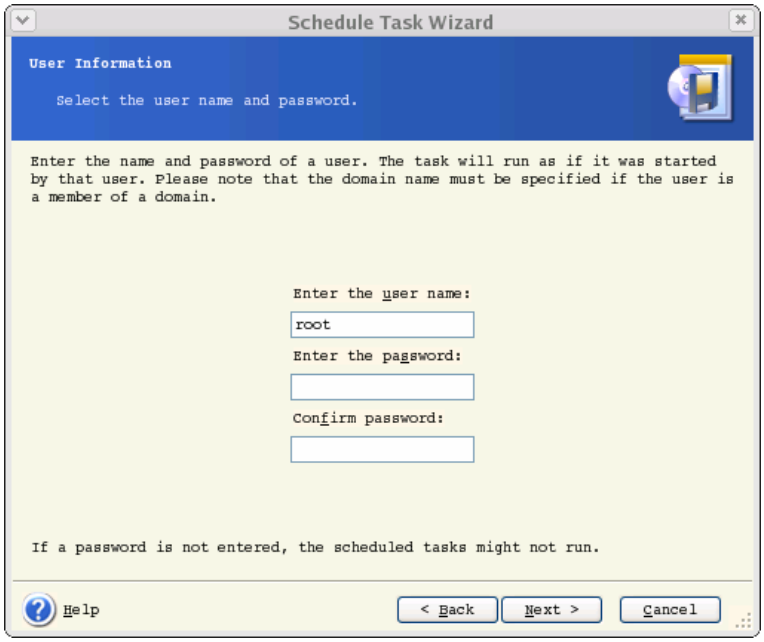
Some of these options might be disabled depending on the operating system.

5. Click **Next**.

6. Specify the task start time and other schedule parameters, according to the selected periodicity (see 7.1.1 - 7.1.4).

7. Click **Next**.

8. Next you will have to specify the name of the user who owns the executed task; otherwise no scheduled execution will be available.



In the upper field, enter a user name. Enter a password twice in two fields below.

9. At the final step, the task configuration is displayed. Up to this point, you can click **Back** to make changes in the created task. If you click **Cancel**, all settings will be lost. Click **Finish** to save the task.

10. The task schedule and default name appear on the **Active tasks** pane of the main window. You are prompted to rename the task just now. If you do not want to do it, press Enter or Esc key.

7.1.1 Setting up daily execution

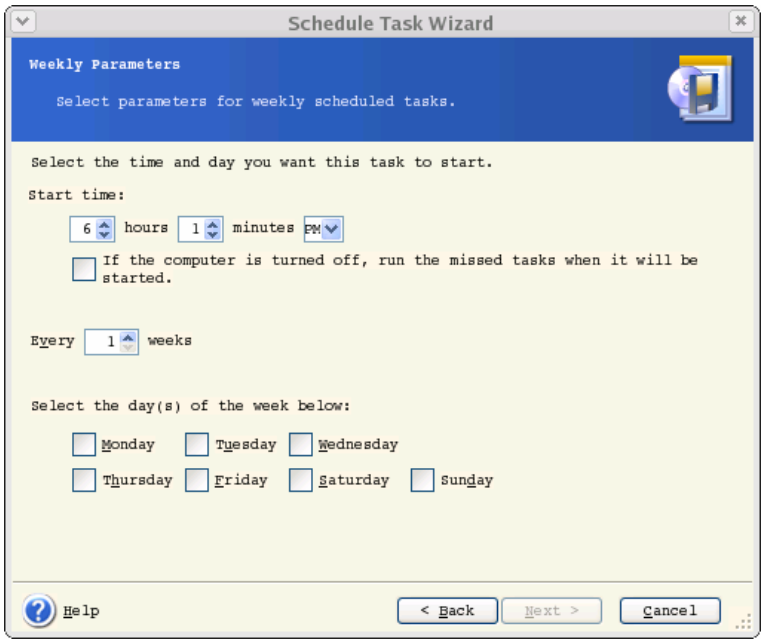
If you select the daily execution, set the **Start time** and days on which you want to execute the task:

- **Every day**
- **Weekdays**
- **Every x days** – once in several days (specify the interval).

If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

7.1.2 Setting up weekly execution

If you select the weekly execution, set the **Start time**, specify the task execution periodicity in the **Every x weeks** box (every week, every two weeks, etc.) and check days on which to execute the task.

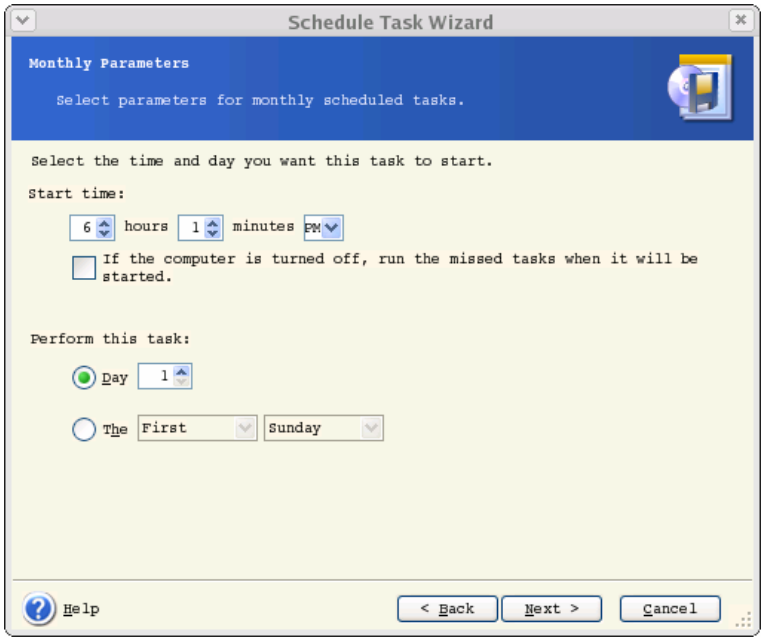


If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

7.1.3 Setting up monthly execution

If you select the monthly execution, set the **Start time** and days on which to execute the task:

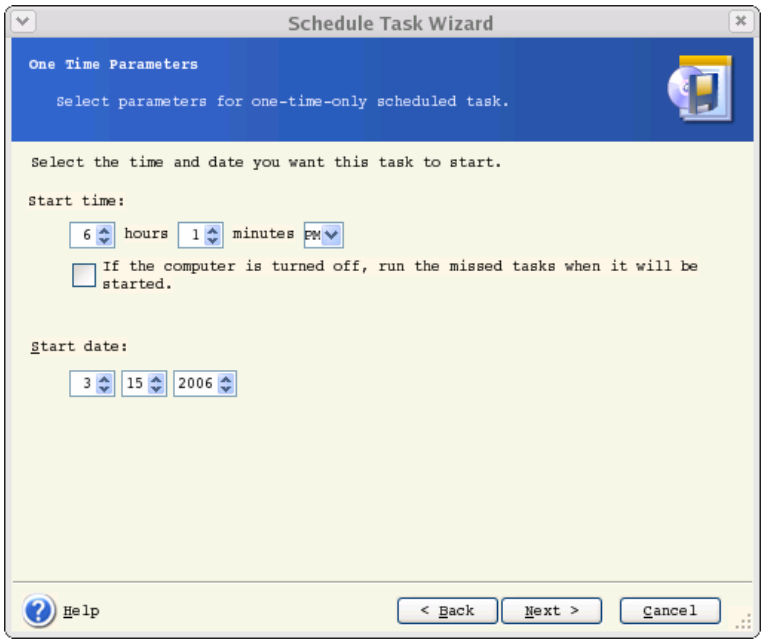
- **Day** – on the specified date
- **The <specify a day>** – on the specified day (e.g. on second Tuesday or fourth Friday); select this from the drop-down lists.



If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

7.1.4 Setting up one-time execution

If you select the one-time execution, set the **Start time** and date on which to execute the task:



If the computer is off when the scheduled time comes, the task won't be performed, but you can force the missed task to launch at the next system startup by checking a box under the **Start time** fields.

7.2 Managing scheduled tasks

The task **Status**, **Schedule**, **Last Run Time** and **Last Result** are shown on the **Active tasks** pane of the main window. To view the other task details, right-click on its name.

There are two ways of changing the task parameters. Editing allows you to change any task parameters. This is performed in the same way as creation, however, the earlier selected options will be set, so you have to enter only the changes. To edit a task, select it and click **Edit the Selected Task** on the **Active tasks** toolbar.

If you want to change only periodicity and/or start time, click **Schedule the Selected Task** on the **Active tasks** toolbar. Then you will have to perform only scheduling steps, leaving the backup settings the same.

To delete a task with confirmation, select it and click **Delete the Selected Task** on the **Active tasks** toolbar.

To rename a task, select it, click **Rename the Selected Task** on the **Active tasks** toolbar, enter the new task name and press Enter.

Chapter 8. Managing Acronis Secure Zone

The Acronis Secure Zone is a special partition for storing archives on the computer system itself. Acronis Secure Zone is necessary for using Acronis Startup Recovery Manager. For more information about these functions see *3.3 Acronis Secure Zone* and *3.4 Acronis Startup Recovery Manager.*

8.1 Creating Acronis Secure Zone

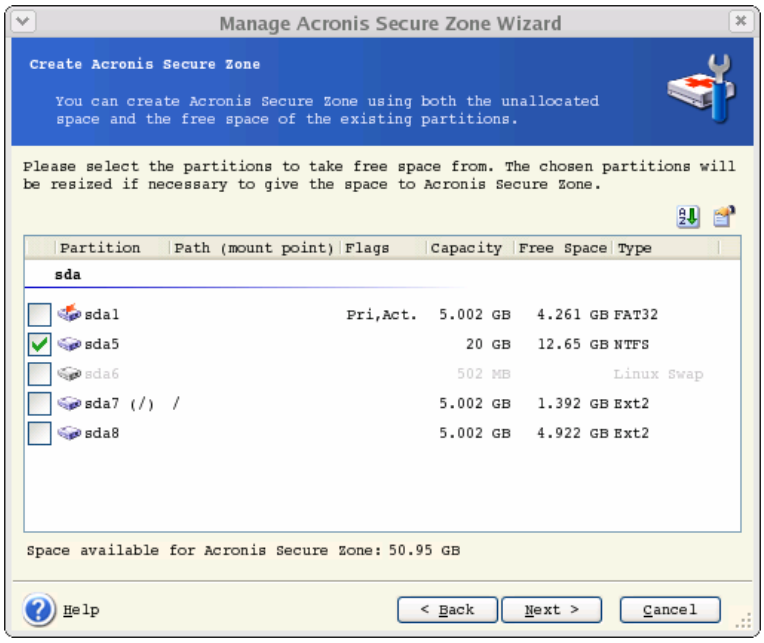
Acronis Secure Zone can be located on any local disk. It is created using unallocated space, if available, or at the expense of free space on a partition. A computer can have only one secure zone. To create a zone on another disk, you must first delete an existing zone.

When you click **Manage Acronis Secure Zone** in the menu, the program searches for the zone on all local drives. If a zone is found, the wizard will offer to delete or resize it. If there is no zone, you'll be prompted to create it.

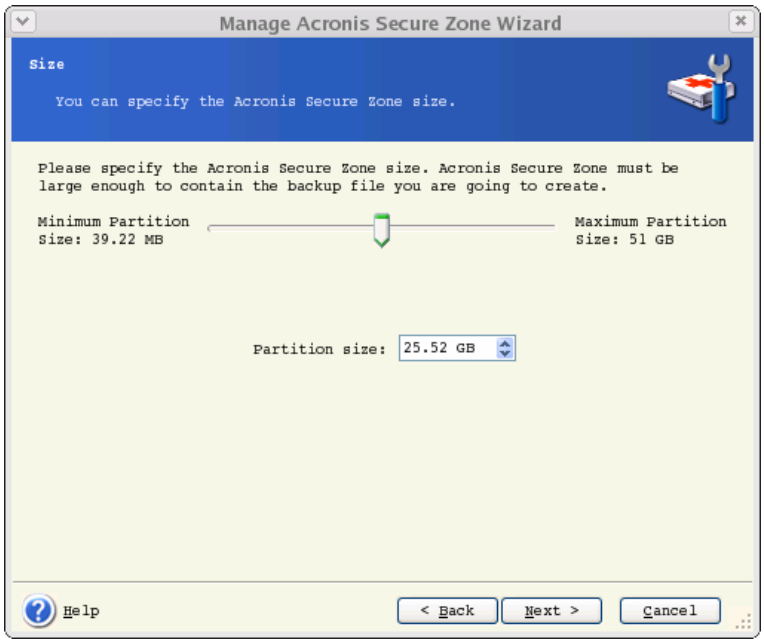
1. Before creating the Acronis Secure Zone, you can estimate its size. To do this, start backup and select all data you are going to backup into the Acronis Secure Zone. At the **Set Backup Options** step choose **Set the options manually**, then set compression level. You will see the estimated full backup size. Multiply this by about 1.5 to be able to create incremental or differential archives.

2. If there are several disks installed, select one on which to create Acronis Secure Zone.

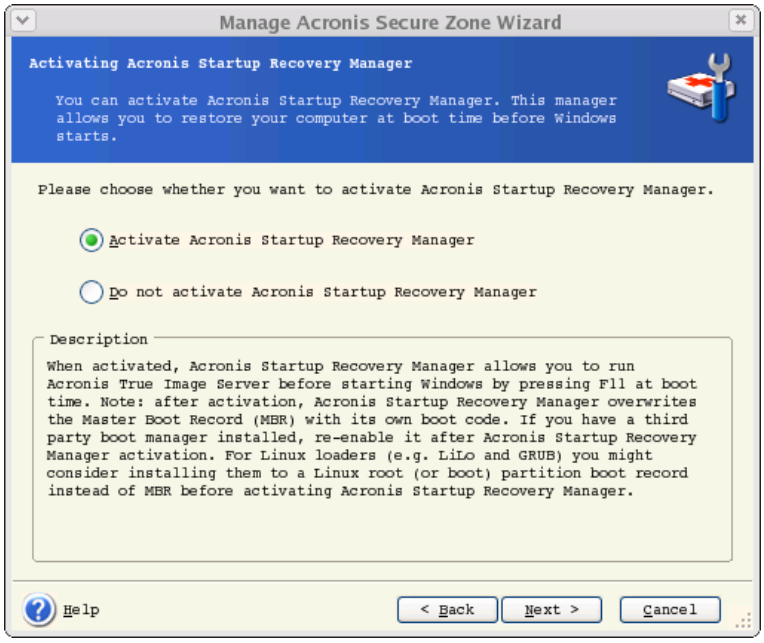
3. Select the partitions from which space will be used to create the zone.



4. In the next window, enter the size of the zone or drag the slider.



5. After this, you will be prompted to activate Acronis Recovery Manager, to be able to start Acronis True Image Server for Linux at boot time by pressing F11 key. Alternatively, you can activate this feature later from main program window.



6. Then you will see a list of operations to be performed on partitions (disks).

If you selected to activate Acronis Startup Recovery Manager, take note of the partition number that will be assigned to Acronis Secure Zone.

After you click **Proceed**, Acronis True Image Server for Linux will start creating the zone. Progress will be reflected in the special window. If necessary, you can stop zone creation by clicking **Cancel**. However, the procedure will be canceled only after the current operation is finished.

Acronis Secure Zone creation might take several minutes or more. Please wait until the whole procedure is finished.

7. If you selected to activate Acronis Startup Recovery Manager, all files required for loading Acronis True Image Server for Linux standalone version has been copied to Acronis Secure Zone by now. To enable the program launch at boot time by pressing F11 key, add an entry to the configuration file, allowing boot from Acronis Secure Zone.

For example, if you use grub loader, add to /boot/grub/grub.conf or /boot/grub/menu.lst the following lines:

title Acronis //or any desired title

root (hd0,3) //ASZ location (available on summary screen), here: disk 0, partition 3

makeactive

chainloader +1

After that issue the following command:

grub-install /dev/hda //the hard disk from which grub will be loaded

When Acronis Startup Recovery Manager is activated, it overwrites the master boot record (MBR) with its own boot code. If you have any third-party boot managers installed, you will have to reactivate them after activating the Startup Recovery Manager. For Linux loaders (e.g. LiLo and GRUB), you might consider installing them to a Linux root (or boot) partition boot record instead of MBR before activating Acronis Startup Recovery Manager.

8.1.1 Activating and deactivating Acronis Startup Recovery Manager

After Acronis Startup Recovery Manager was initially activated, you can deactivate it or activate again at any time. To do so, simply delete the above entry from the configuration file or add it again.

If you did not activate Acronis Startup Recovery Manager when creating Acronis Secure Zone, select **Activate Acronis Startup Recovery Manager** on the sidebar or the **Tools** menu and follow the Wizard's instructions. Then add an entry to the configuration file as described in step 7 of 8.1.

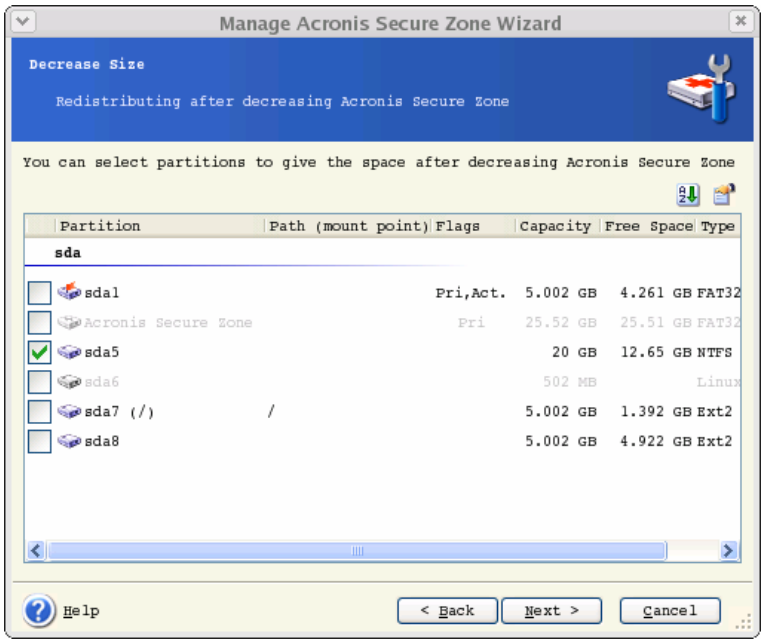
If you try to activate Acronis Startup Recovery Manager while Acronis Secure Zone is missing from the system, you will be prompted to create the zone, then Acronis Startup Recovery Manager will be activated.

8.2 Resizing Acronis Secure Zone

1. When prompted by the wizard, select **Manage Acronis Secure Zone**.

2. Select to increase or decrease the zone. You might need to increase it to provide more space for archives. The opposite situation might arise if either partition lacks free space.

3. Select partitions from which free space will be used to increase Acronis Secure Zone or that will receive free space after the zone is reduced.



4. Enter the new size of the zone or drag the slider.

5. Next you will see a list of briefly described operations to be performed on partitions (disks).

After you click **Proceed**, Acronis True Image Server for Linux will start resizing the zone. Progress will be reflected in the special window. If necessary, you can stop the procedure by clicking **Cancel**. However, the procedure will be canceled only after the current operation is finished.

Zone resizing can take several minutes or longer. Please wait until the whole procedure is finished.

8.3 Deleting Acronis Secure Zone

1. When prompted by the wizard, select **Remove Acronis Secure Zone**.

2. Select the partitions to which you want to add the space freed from the secure zone. If you select several partitions, the space will be distributed proportionally to each partition's size.

3. Next, you will see a list of briefly described operations to be performed on partitions (disks).

After you click **Proceed**, Acronis True Image Server for Linux will start deleting the zone. Progress will be reflected in the opened window. If necessary, you can stop the procedure by clicking **Cancel**. However, the procedure will be canceled only after the current operation is finished.

Zone deletion might take several minutes or more. Please wait until the whole procedure is finished.

Acronis Secure Zone deletion will automatically disable Acronis Startup Recovery Manager if it is activated and destroy all backups stored in the zone.

Chapter 9. Mounting partition images

Acronis True Image Server for Linux can mount partition images, thus letting you access them as though they were physical drives. This means that you will be able to use the virtual disk in the same way as the real one: open, save, copy, move, create, delete files or folders. If necessary, the image can be mounted in read-only mode.

Please keep in mind that, though both file archives and disk/partition images have a default ".tib" extension, only partition images can be mounted. If you want to view file archive contents, use the Restore Data Wizard (see *6.2 Restoring files and folders from file archives*, steps 1-9).

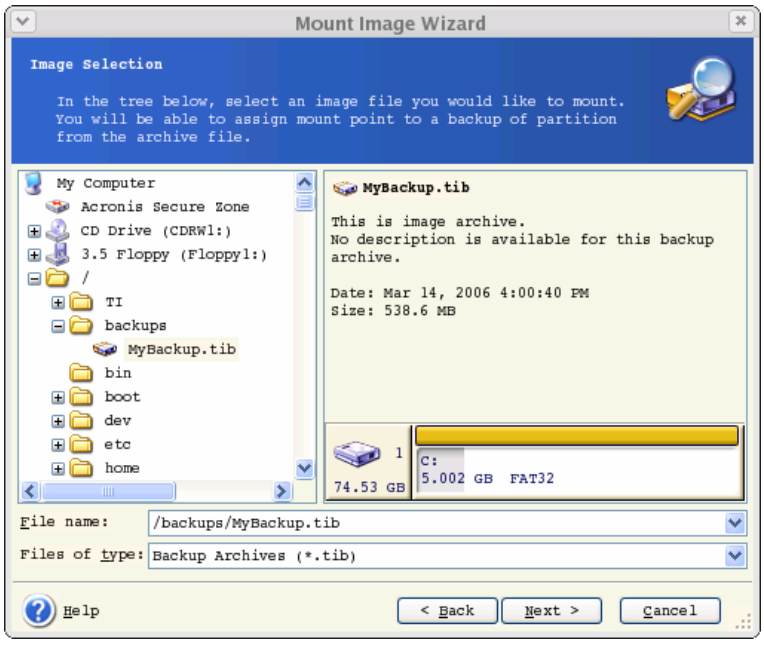
The current version of Acronis True Image Server for Linux can mount an image archive only if all its volumes reside in the same directory. If your archive spans several CD-R/RW discs and you wish to mount the image, you should copy all volumes to a hard disk drive or network drive.

9.1 Mounting an image

1. Invoke the **Mount Image Wizard** by clicking on the **Mount Image** operation icon in the main program window.

2. Click **Next**.

3. Select the archive from the drives tree. If the archive is located in Acronis Secure Zone, select it to choose the archive at the next step.



If you added a comment to the archive, it will be displayed to the right of the drives tree. If the archive was protected with a password, Acronis True Image Server for Linux will ask for it. Neither the partitions layout, nor the **Next** button will be enabled until you enter the correct password.

4. Click **Next**.

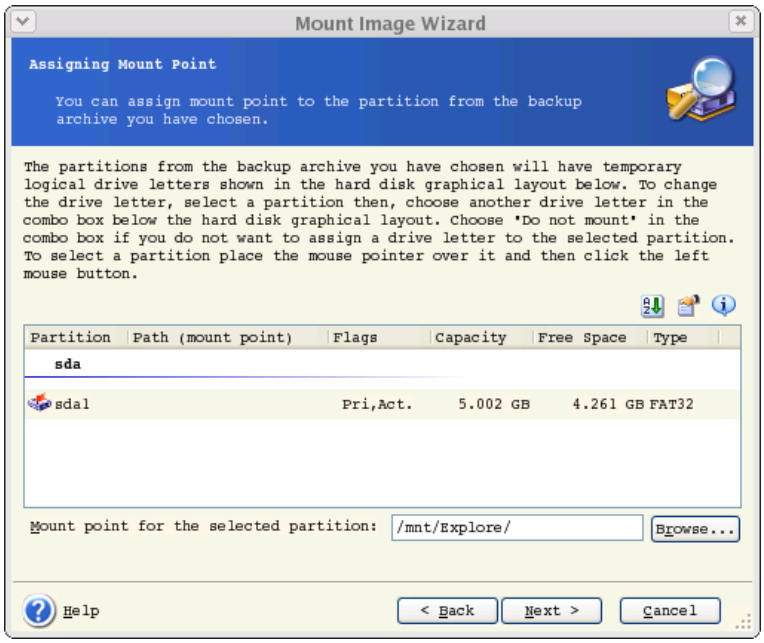
5. If you are to mount an incremental image, Acronis True Image Server for Linux will suggest that you select one of successive incremental archives by date/time of its creation. Thus, you can explore the partition state to a certain moment.

To mount an incremental image, you must have all previous incremental images and the initial full image. If any of successive images is missing, connection is impossible.

To mount a differential image, you must have the initial full image as well.

6. Click **Next**.

7. Select a partition to mount (note that you cannot mount the entire disk) and specify the mount point for the selected partition.



8. Click **Next**.

9. Select whether you want to mount image in **Read-only** or **Read/Write** mode.

10. Click **Next**.

11. If you select **Read/Write** mode, the program assumes that the mounted image will be modified, and creates an incremental archive file to capture the changes. It is strongly recommended that you list the forthcoming changes in the comment to this file.

12. The program displays a summary containing a single operation. Click **Proceed** to mount the selected partition image.

13. After the image is mounted, you can operate with files or folders as if they were located on a real disk.

You can mount multiple partition images. If you want to mount another partition image, repeat the procedure.

9.2 Unmounting an image

We recommend that you unmount image after all necessary operations are finished, as keeping up virtual disks takes considerable system resources. If you do not, the virtual disk will disappear after your server is turned off.

To unmount an image, click **Unmount Image** and select the folder to unmount.

Chapter 10. Creating bootable media

You can run Acronis True Image Server for Linux on a bare metal or on a crashed computer that cannot boot. You can even back up disks on a non-Linux computer, copying all its data sector-by-sector into the backup archive. To do so, you will need bootable media with the standalone Acronis True Image Server for Linux version. Such media is also used when cloning a mounted hard disk.

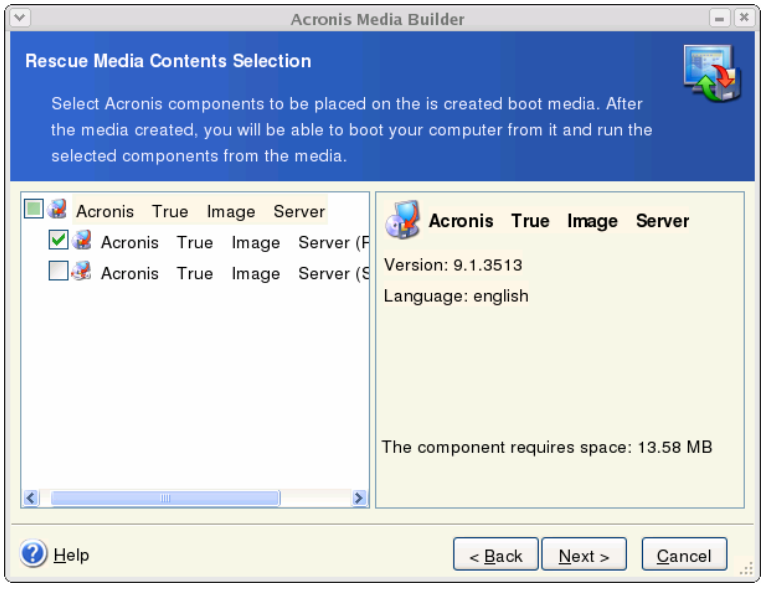
If you purchased the boxed product, you already have such a bootable CD, because the installation CD contains, besides the program installation files, the Acronis True Image Server for Linux standalone bootable version.

If you purchased Acronis True Image Server for Linux on the Web, you can create bootable media using the **Rescue Media Builder**. For this, you will need a CD-R/RW blank, several formatted diskettes (the wizard will tell you the exact number), or any other media your server can boot from, such as a Zip drive.

Acronis True Image Server for Linux also provides the ability to create an ISO image of a bootable disk on the hard disk.

1. Run **Rescue Media Builder** by entering command **mediabuilder**.

2. Select which components you want to place on the bootable media.



Acronis True Image Server for Linux offers the following components:

- **Acronis True Image Server for Linux full version**

Includes support of USB, PC Card and SCSI interfaces along with the storage devices connected via them, therefore is highly recommended.

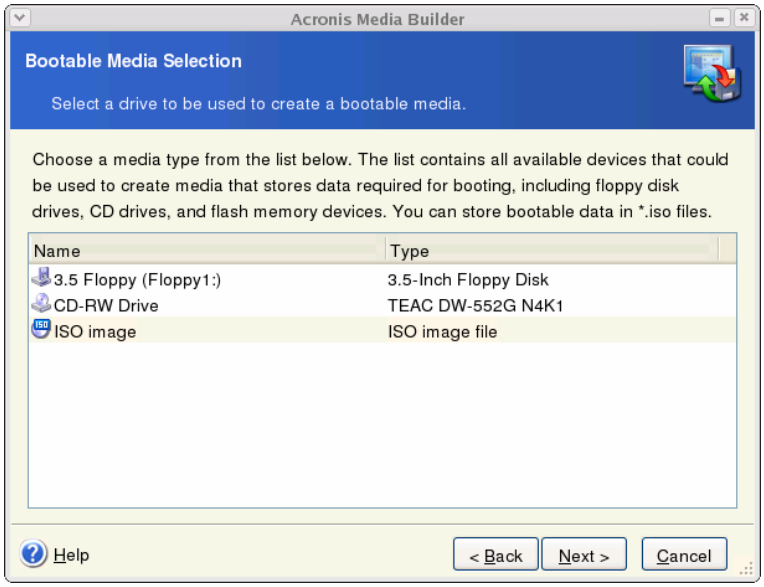
- **Acronis True Image Server for Linux safe version**

Does not include USB, PC Card, or SCSI drivers. Recommended for use in case of problems with running **Full version.**

3. Select the type of bootable media (CD-R/RW or 3.5" diskettes) to create. If your BIOS has this feature, you can create other bootable media such as removable USB flash drives. You can also choose to create a bootable disk ISO image.

Having created an ISO disk image, you will be able to burn it onto any kind of DVD recordable, using DVD recording software. Creating a bootable DVD directly from Bootable Media Builder is impossible.

When using 3.5" diskettes, you will be able to write on a diskette (or a set of the diskettes) only one component at a time (for example, Acronis True Image Server for Linux full version). To write another component, start Bootable Media Builder once again.



4. If you are creating diskettes or removable media other than CD, insert the blank disk so the program can determine its capacity. If you chose to create a bootable disk ISO image, specify the ISO file name and the folder where to place it.

5. Next, the program will calculate how many blank disks are required (in case you have not chosen ISO) and give you time to prepare them. When you are finished, click **Proceed**.

After you create a boot disk, identify it and keep it in a safe place.

Chapter 11. Console mode

Console is a natural part of Linux OS. Acronis True Image Server for Linux supports it through the **trueimagecmd** command line tool. It provides a way to initiate data backup and recovery operations. **Trueimagecmd** also enables you to automate backup with '*cron*' service.

The **trueimagecmd** functionality is somewhat limited as compared to the GUI mode. **trueimagecmd** does not support operations that require reboot of the system, such as restore a system partition or clone system drive. Therefore, under complex conditions, we recommend that you use the more powerful trueimage operating mode under X Window System.

Another useful tool, **trueimagemnt**, allows you to extract files or directories from images by mounting images as if they were Linux kernel block devices. See also **man trueimagecmd** or **man trueimagemnt**.

11.1 Backup, restore and other operations in the console mode (trueimagecmd)

11.1.1 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, other 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	/filename:[filename] /password:[password] /asz /incremental /differential /compression:[0…9] /split:[size in MB] /oss_numbers /log:[filename]	/harddisk:[disk number] /partition:[partition number] /raw /progress:[on|off]
filebackup Backs up specified files and folders	/filename:[filename] /password:[password] /asz /incremental /differential /compression:[0…9] /split:[size in MB] /reboot /log:[filename]	/include:[names] /exclude_names:[names] /exclude_masks:[masks] /exclude_system /exclude_hidden
restore Restores disks and partitions from an image	/filename:[filename] /password:[password] /asz /index:N /oss_numbers /log:[filename]	/harddisk:[disk number] /partition:[partition number] /target_harddisk:[disk number] /target_partition:[partition number] /start:[start sector] /fat16_32 /size:[partition size in sectors] /type:[active|primary|logical] /preserve_mbr

filerestore Restores files / folders from a file archive	/filename:[filename] /password:[password] /asz /index:N /log:[filename]	/target_folder:[target folder] /overwrite:[older|never|always] /restore_security:[on|off] /original_date:[on|off]
verify Verifies the archive data integrity	/filename:[file name] /password:[password] /asz /log:[filename]	
list Lists available drives and partitions. With the filename option, lists the image contents	/password:[password] /index:N /asz	/filename:[file name]
asz_create Creates the Acronis Secure Zone on the selected drive	/oss_numbers /log:[filename]	/harddisk:X /partition:[partition number] /size:[ASZ size in sectors] /asz_activate
asz_activate Activates Acronis Startup Recovery Manager.	/password:[password]	
asz_content Displays the Acronis Secure Zone size, free space and contents	/password:[password]	
asz_delete Deletes the Acronis Secure Zone	/password:[password] /oss_numbers /log:[filename]	/partition:[partition number]
clone Clones a hard disk		/harddisk:[disk number] /target_harddisk:[disk number]
help Shows usage		

11.1.2 Common options (options common for most trueimagecmd commands)

Option	Description	Archive location
Access to archives		
filename:[filename]*	Archive name	Other than ASZ
password:[password]	Specify the password for the archive (if required)	Other than ASZ
	Specify the password for the ASZ (if required)	ASZ

asz:[number of archive]	Addresses to Acronis Secure Zone and selects the archive (a full backup with or without increments). To get the archive number, use `/asz_content`	ASZ
index:N N = Number of the backup in an archive: 1 = basic full backup 2 = 1st increment... and so on 0 (default) = latest increment	Select a backup in a sequence of incremental backups inside the archive. To get a backup index from ASZ, use `/asz_content`	Any
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	Any
differential	Set the backup type to differential. If not specified or there is no basic full backup, a full backup will be created	Any
compression:[0…9]	Specify the data compression level. It ranges from 0 to 9 and is set to 3 by default	Any
split:[size in MB]	Split the backup into parts of the specified size	Other than ASZ
General options		
oss_numbers	Declares that numbers of partitions in the `partition` option are adjusted for MBR partition table rather than be simple ascending numbers. This means that primary partitions have numbers 1-1, 1-2, 1-3 (and 1-4 if there are not logical partitions on the disk) and logical partitions numbers start with 1-4. 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:1-1,1-4,1-5`	Any
log:[filename]	Create a log file of the current operation with the specified file name	Any

* To access a NFS network drive, specify the image file name as follows:

nfs://hostname/share name:/remote filename

For example:

trueimagecmd --list --filename:`nfs://dhcp6-223.acronis.com/sdb3/nfs_root:/mike/md1.tib`

shows contents of /mike/md1.tib archive. /mike/md1.tib is located on dhcp6-223.acronis.com node in /sdb3/nfs_root directory exported by NFS.

To get Samba network access, specify the image file name as follows:

smb://hostname/share name/remote filename

Hostname may be specified with username and password as:

username:password@hostname

For example:

trueimagecmd --list --filename:smb://dhcp6-223.acronis.com/sdb3/mike/md1.tib

shows contents of /mike/md1.tib archive. /mike/md1.tib is located on dhcp6-223.acronis.com node in /sdb3 directory exported by Samba.

11.1.3 Specific options (options specific for individual trueimagecmd commands)

Option	Description
create	
harddisk:[disk number]	Specifies numbers of the hard disks to be imaged (comma separated). For example: --harddisk:1,3 You can obtain the list of available hard disks using the --list command. The list includes LVM disks and md (multiple devices) as additional drives that can also be imaged.
partition:[partition number]	Specifies the partitions to include into the image file by numbers. The list of available partitions is provided by the --list command. Partition numbers are specified as <disk number>-<partition number>, e.g.: --partition:1-1,1-2,3-1
raw	Use this option to create an image of a disk (partition) with 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.
progress:[on | off]	Shows/hides the progress information (percent completed). It is shown by default.
filebackup	
include:[names]	Files and folders to be included in the backup (semicolon separated, the whole file list enclosed in apostrophes). For example: --include:'/home/bot/ATIESsafe.iso;/home/bot/ATIW.iso'
exclude_names:[names]	Files and folders to be excluded from the backup (semicolon separated, the whole file list enclosed in apostrophes). See the above example.
exclude_masks:[masks]	Applies masks to select files to be excluded from the backup. Use the common masking rules. For example, to exclude all files with extension .exe, add ***.exe** mask. **My???.exe** mask will reject all .exe files with names consisting of five symbols and starting with “my”.
exclude_system	Excludes all system files from the backup.
exclude_hidden	Excludes all hidden files from the backup.
restore	

`harddisk:[disk number]`	Specifies the hard disks to restore by numbers.
`partition:[partition number]`	Specifies the partitions to restore by numbers.
`target_harddisk:[disk number]`	Specifies the hard disk number where the image will be restored.
`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.
`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 2GB. 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 stay 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 not 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.
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 program finds in the target folder a file with the same name as in the archive: `older` – this will give the 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 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 assign the current date and time to the restored files. If not specified, the current date is assigned.
list	
`filename:[filename]`	With this option, the image contents is displayed. When listing image contents, 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 `--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`.
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]`	Sets the Acronis Secure Zone size (in sectors). If not specified, is set as an average between the maximal (using unallocated space and free space on all the listed partitions) and minimal values.
`asz_activate`	Activates the Acronis Startup Recovery Manager. The option will not take effect if the system partition is resized during Acronis Secure Zone creation. In that case, use the separate `asz_activate` command.
asz_activate	
`password:[password]`	Sets a password for the Acronis Secure Zone.
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 to each partition's size.
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.

11.1.4 Trueimagecmd usage examples

- This will list available partitions:

```
trueimagecmd --list
```

- This will list the partitions (and their indices) saved in backup.tib:

```
trueimagecmd --list --filename:backup.tib
```

- This will create an image named backup.tib of partition 1-1:

```
trueimagecmd --partition:1-1 --filename:backup.tib \
--create
```

- This will create an incremental image of the partition above:

```
trueimagecmd --partition:1-1 --filename:backup.tib \
--create --incremental
```

- This will create an image of partition 1-1 in the Acronis Secure Zone:

```
trueimagecmd --partition:1-1 --asz --create
```

- This will restore a partition from backup.tib:

```
trueimagecmd --partition:1-1 --filename:backup.tib \
--restore
```

11.2 Automatic image creation using cron service

As a rule, disk/partition images are created regularly, often daily. To automate this operation, you can use the **cron** service familiar to many UNIX users.

As an example, let's consider a situation where you (the system administrator) need to back up one or more disk partitions regularly.

Use `--list` to obtain the necessary partition number:

```
Disk 1:
1-1             hda1      Pri,Act     31.35 MB     26.67 MB      FAT16
                Table                                            Table
1-2             hda5                  980.5 MB                   Linux Swap
1-3             hda6                  4.887 GB     135.9 MB      Ext2
1-4             hda7                  9.767 GB     1.751 GB      Ext2
1-5             hda8                  3.462 GB     1.3 GB        Ext2
Disk 2:
2-1 (/1)        hdd1      Pri,Act     4.806 GB     4.627 GB      Ext3
                Table                                            Table
2-2             hdd5                  3 GB         1.319 GB      Ext3
2-3             hdd6                  3.906 GB                   Ext3
```

You need to back up partition 2-1. Let's suppose a complete image has to be created weekly supported by incremental images created daily.

To do this, place the respective executable files (e.g. **trueimage.cron**) into **/etc/cron.daily** and **/etc/cron.weekly** folders.

To initiate **weekly** creation of a complete image of partition 2-1, add the following line to the above file:


```
#!/bin/bash
/usr/sbin/trueimagecmd --create --partition:2-1 --
filename:/mnt/backups/my_host/backup.tib
```

Where **/mnt/backups/my_host/backup.tib** is image name and path.

The second executable file is needed to initiate daily creation of incremental images:

```
#!/bin/bash
/usr/sbin/trueimagecmd --create --incremental --partition:2-1 --
filename:/mnt/backups/my_host/backup.tib
```

If needed, users can make their own backup schedule. For more information, see Help on the **cron** service.

11.3 Restoring files with trueimagemnt

The **trueimagemnt** tool is designed to restore files from partition/disk images. It mounts Acronis True Image archives as if they were kernel space block devices. The program implements the user level part of the Acronis True Image Server for Linux user mode block device service. The large part of functionality is handled by the snumbd kernel module.

SYNOPSIS

trueimagemnt [-h|--help] [-l|--list] [-m|--mount mountpoint**] [-u|--umount** mountpoint**] [-s|--stop** pid**] [-o|--loop] [-f|--filename** archive filename**] [-p|--password** password**] [-t|--fstype** filesystem type**] [-i|--index** partition index**] [-w|--read-write] [-d|--description** archive description**] [-k|--keepdev]**

11.3.1 Supported commands

Trueimagemnt supports the following commands:

-h|--help

Shows usage.

-l|--list

Lists already mounted user mode block devices.

-m|--mount mountpoint

Mounts the archive image specified by `-f|--filename` option into the folder specified by `mountpoint` option. The partition index should be specified by `-i|--index` option. Image file contents (partitions and their indices) may be listed by `trueimagecmd --list --filename:filename` command.

To mount an incremental image, you must have all previous incremental images and the initial full image. If any of successive images is missing, the mounting is impossible.

-u|--umount mountpoint

Unmounts the device mounted at `mountpoint`, destroys kernel space block device and stops user space daemon.

-s|--stop pid

Destroys kernel space block device and stops user space daemon specified by `pid`. This command should be used if an error occurs while mounting and unmounted user space daemon/kernel space block device pair survives. Such a pair is listed by `-l|--list` command with none in `mountpoint` field.

-o|--loop

A test command. Mounts a file, specified in `-f|--filename` option, containing valid Linux filesystem, as if it is Acronis True Image archive. The command may be used, for example, to estimate an image compression level, by comparing the time, necessary for copying a file from the image, with the time for copying the mounted (non-compressed) file.

Trueimagemnt supports the following command options:

-f|--filename archive filename

The image file name. **trueimagemnt** transparently supports NFS and Samba network access. To access a NFS network drive, specify the image file name as follows:

nfs://hostname/share name:/remote filename

For example:

```
trueimagemnt -m /mnt/md1 -f nfs://dhcp6-
223.acronis.com/sdb3/nfs_root:/mike/md1.tib -i 2
```

mounts /mike/md1.tib archive, located on dhcp6-223.acronis.com node in /sdb3/nfs_root directory exported by NFS.

To get Samba network access, specify the image file name as follows:

smb://hostname/share name/remote filename

Hostname may be specified with username and password as:

username:password@hostname

For example:

```
trueimagemnt -m /mnt/md1 -f smb://dhcp6-
223.acronis.com/sdb3/mike/md1.tib -i 2
```

mounts /mike/md1.tib archive, located on dhcp6-223.acronis.com node in /sdb3 directory exported by Samba.

-p|--password password

Specifies the password to explore password protected images.

-t|--fstype filesystem type

Specifies explicit filesytem type to be passed to the standard "mount" command. This option is useful if the standard "mount" command can't guess filesystem type by some reason.

-i|--index partition index

Index of the partition.

-w|--read-write

Opens the image in read-write mode. After umount all changed data will be saved into the archive with a new index.

-d|--description archive description

If an image is mounted in **read-write** mode, the program assumes that the image will be modified, and creates an incremental archive file to capture the changes. The option enables you to list the forthcoming changes in the comment to this file.

-k|--keepdev

Keeps kernel space block device and user space daemon if an error occurs while mounting. This option may be used to get raw access to imaged partition data.

11.3.2 Trueimagemnt usage examples

- This will list the mounted archives:

```
trueimagemnt --list
```

- This will mount the archive backup.tib of partition with index 2, to /mnt/backup:

```
trueimagemnt --mount /mnt/backup --filename backup.tib --index 2
```

- This will unmount a partition mounted at /mnt/backup:

```
trueimagemnt --umount /mnt/backup
```

Chapter 12. Other operations

12.1 Validating backup archives

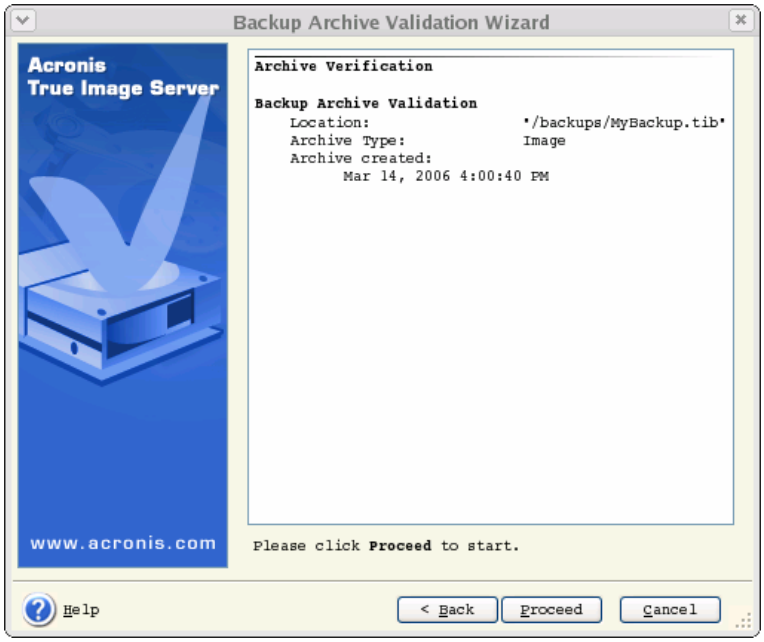
To be certain that your archives are not damaged, you can check their integrity.

1. To invoke the **Backup Archive Validation Wizard**, select **Validate Backup Archive** in the main window or in the **Tools** group or click **Validate Backup Archive** on the toolbar.

2. Click **Next**.

3. Select the archive to validate. The Acronis Secure Zone can be selected only as a whole because all its contents is considered as a single archive.

4. Click **Next**.



5. Clicking **Proceed** will launch the validation procedure. After the validation is complete, you will see the results window. You can cancel checking by clicking **Cancel**.

To check archive data integrity you must have all incremental and differential backups belonging to the archive and the initial full backup. If any of successive backups is missing, validation is not possible.

12.2 Operation results notification

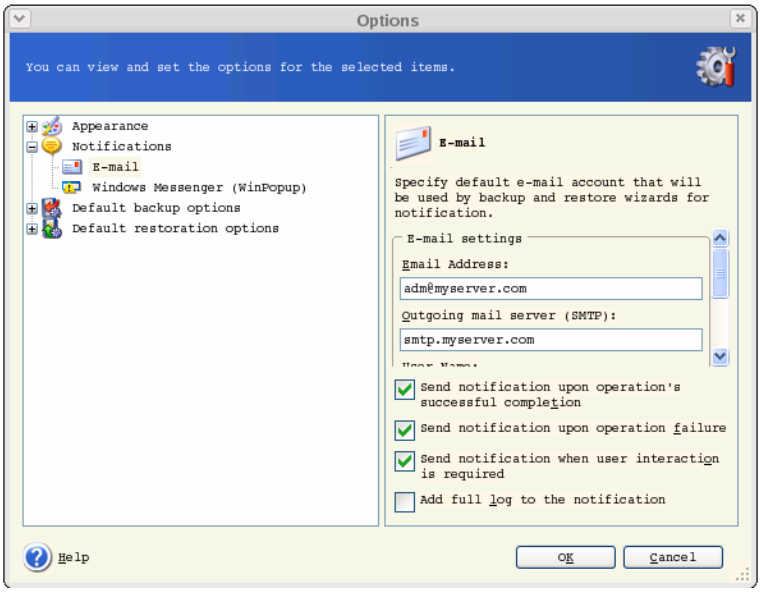
Sometimes a backup or restore procedure can last for 30 minutes or more. Acronis True Image Server for Linux can notify you when it is finished using the WinPopup service (if you address the notification to a computer, running Windows) or via e-mail. The program can

also duplicate messages issued during the operation or send you the full operation log after operation completion.

By default all notifications are disabled.

12.2.1 Email notification

To set up the e-mail notification, select **Tools -> Options -> Notifications -> E-mail**:



Provide the email address to which notifications will be sent and the outgoing SMTP server name. A user name and a password might also be needed if the SMTP server requires authentication.

Below in this window you can choose whether you want to get notifications:

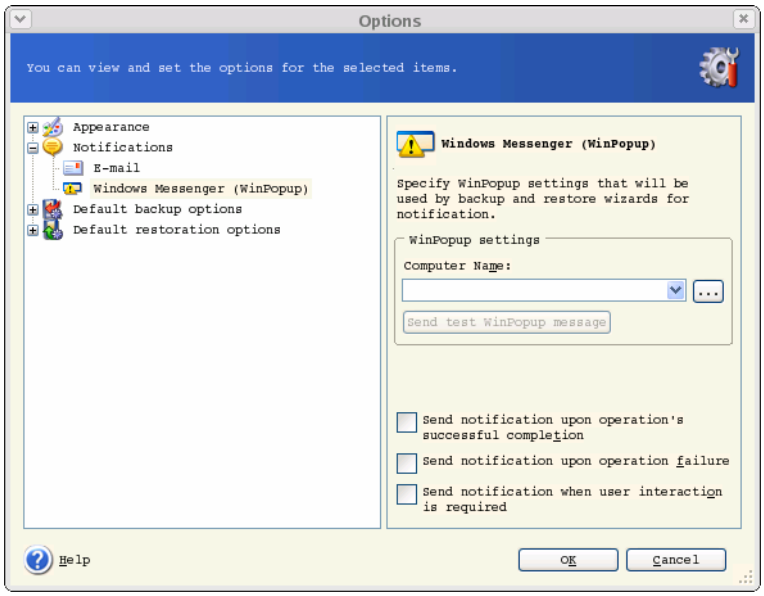
- when the operation is completed successfully (check **Add full log to the notification** to add the full operation log to the message)

- when the operation failed (check **Add full log to the notification** to add the full operation log to the message)

- during the operation when user interaction is required.

12.2.2 WinPopup notification

To set up WinPopup notification, select **Tools -> Options -> Notifications -> WinPopup**:



Provide the name of the Windows computer to which notifications will be sent.

Below in this window you can choose whether you want to get notifications:

- when the operation is completed successfully

- when the operation failed

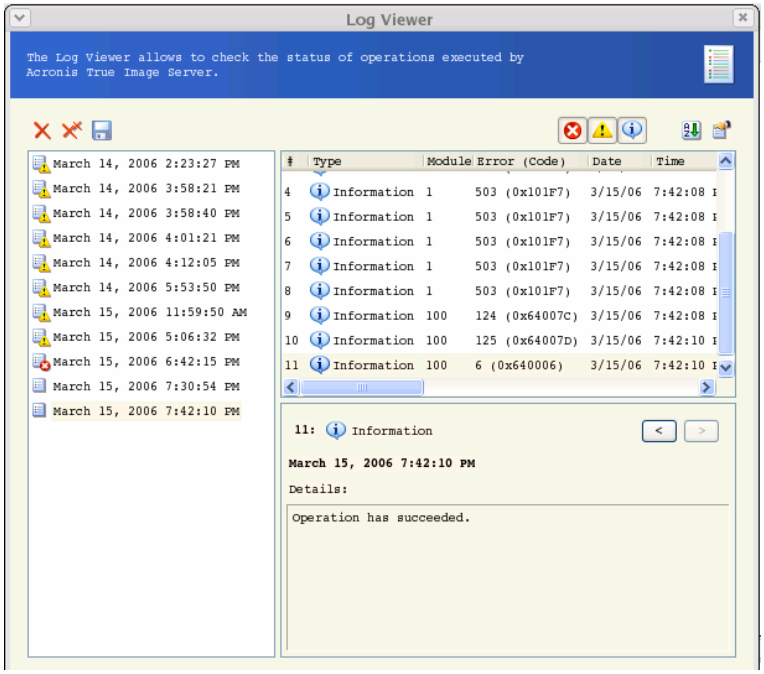
- during the operation when user interaction is required.

12.3 Viewing logs

Acronis True Image Server for Linux allows users to view its working logs. They can provide information about scheduled backup results, including reasons for failure, if any.

To invoke the log window, select **Show log** on the toolbar or from the **Tools** menu.

The log browsing window contains two panes: the left one features the log list, while the right one shows selected log contents.



The left panel can contain up to 50 logs. If there are more, you can browse the list using the **More** and **Less** buttons with the left and right arrows.

To delete a log, select it and click **Delete**.

If any step was terminated by an error, the corresponding log will be marked with a red circle with a white cross inside.

The right window features the list of steps contained in the selected log. The three buttons to the right control message filters: the white cross in the red circle filters error messages, the exclamation sign in a yellow triangle filters warnings, and the “i” in the blue circle filters information messages.

To select columns (step parameters) to display, right-click the headers line or left-click the **Choose Details** button. Then check the desired parameters.

To sort messages by a particular parameter, click its header (click again to reverse order) or the **Arrange Icons by** button (the second from the right) and select the desired parameter.

You can also change column width by dragging the borders with a mouse.

Chapter 13. Transferring the system to a new disk

13.1 General information

Sooner or later, most server administrators discover that they are out of free disk space. If just more data storage space is needed, you can add a new disk, following instructions in the next chapter.

Sometimes your hard disk can't provide enough space for the operating system and installed applications, preventing you from updating your software. In this case, you have to transfer the system to a larger-capacity hard disk.

When transferring an operating system to a new disk, don't forget to add the disk first.

If the server has no more space for new disks, you can temporarily unplug a CD-ROM drive from the IDE cable and use its connector for the new drive. If this option is unavailable, you can clone a disk by creating an image of the old one and restoring it onto a higher-capacity new disk, resizing partitions as needed.

There are two transfer modes available: automatic and manual.

In the automatic mode, you will merely have to take several simple actions to transfer all the data, including partitions, folders and files, to a newer disk, making it bootable (if the original was bootable as well).

There will be only one difference between these disks — partitions on the newer disk will be larger. Everything else, including the installed operating systems, data and disk labels, will remain the same.

Note that you can not clone, add or replace mounted disks, so you will have to run Acronis True Image Server for Linux from a rescue CD in such cases. How to create a rescue CD see in *Chapter 10 Creating bootable media.*

Of course, this is the only result available in the automatic mode. The program can only duplicate the older disk layout to the new one. To obtain a different result, you will have to answer additional questions about cloning parameters.

The manual mode will provide more data transfer flexibility.

1. You will be able to select the method of partitions and data transfer:
   - As is
   - New disk space is proportionally distributed among the old disk partitions
   - New disk space is distributed manually
2. You will also be able to select operations to perform on the old disk:
   - Leave partitions (and data!) on the old disk
   - Remove all information from the old disk
   - Create new partitions on the old disk (and remove all the older information.)

On program screens, damaged partitions are marked with a red circle with a white cross inside in the upper left corner. Before you start cloning, you should check such disks for errors using corresponding OS tools.

13.2 Security

Note the following: if the power goes out or you accidentally press **RESET** during the transfer, the procedure will be incomplete and you will have to partition and format or clone the hard disk again.

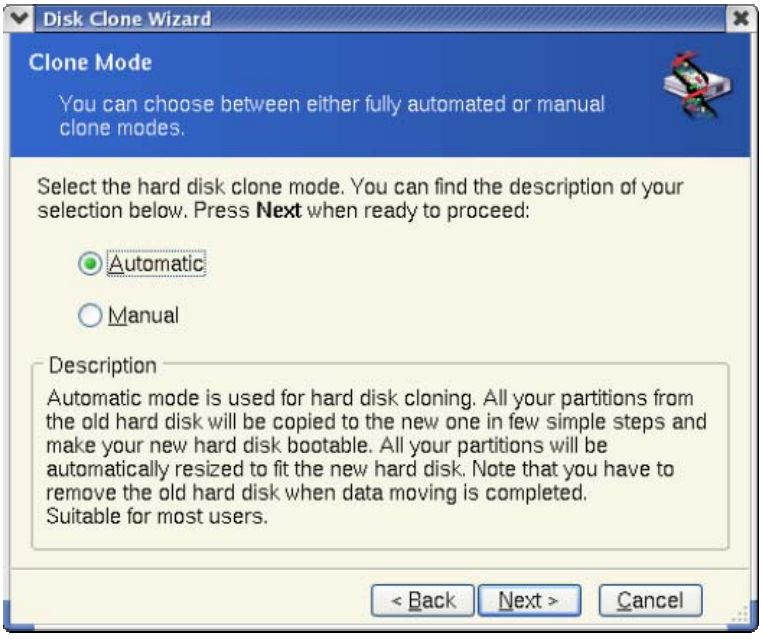
No data will be lost because the original disk is only being read (no partitions are changed or resized) until data transfer is completed.

Nevertheless, we don't recommend that you delete data from the old disk until you are sure it is correctly transferred to the new disk, the server boots up from new disk, and all applications work.

13.3 Executing transfers

13.3.1 Selecting transfer mode

You will see the **Select transfer mode** window just after the welcome window.



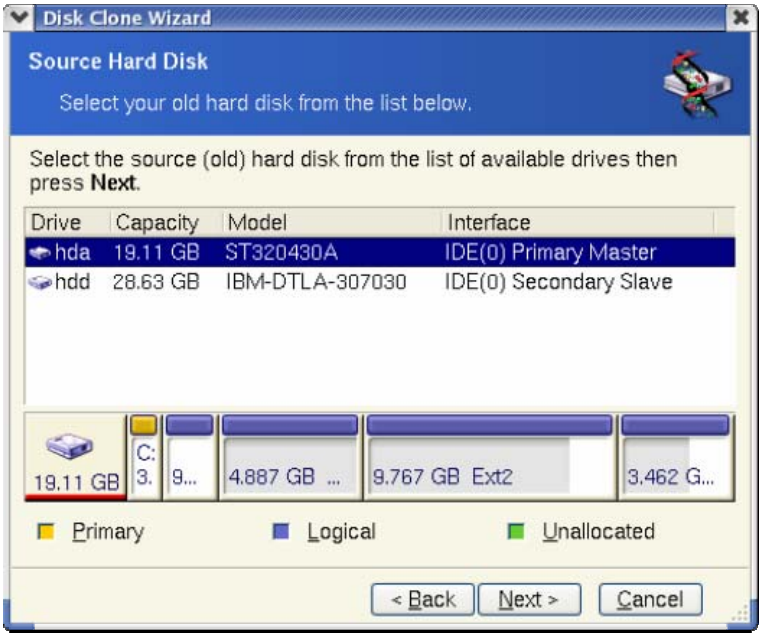
Transfer mode selection

We recommend using automatic mode as it is suitable for most cases. The manual mode can be helpful if you need to change disk partition layout.

If the program finds two disks, one partitioned and another unpartitioned, it will automatically recognize the source and destination, so the next two steps will be bypassed.

13.3.2 Selecting the source disk

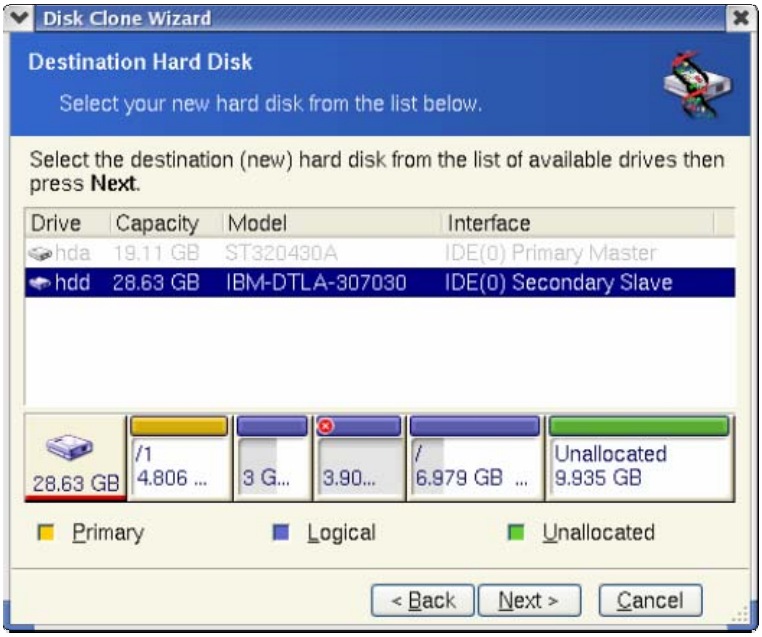
If the program finds several partitioned disks, it will ask you what is the source (i.e. the older data disk).



You can determine the source and destination using the information provided in this window (disk number, capacity, label, partition and file system information).

13.3.3 Selecting the destination disk

After you select the source disk, you have to select the destination to clone to.

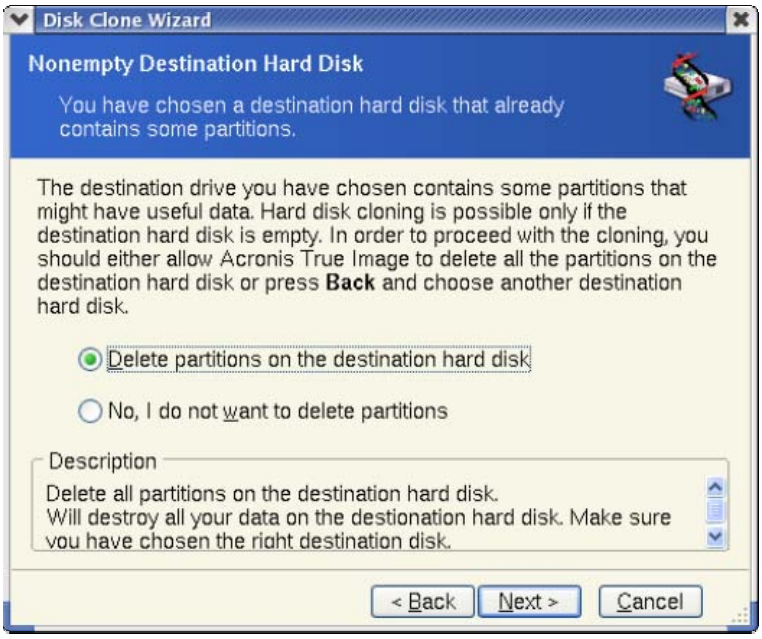


The previously selected source becomes grayed-out and disabled for selection.

If either disk is unpartitioned, the program will automatically recognize it as destination and bypass this step.

13.3.4 Partitioned destination disk

At this point, the program checks if the destination disk is free of partitions. If not, you will be prompted by the **Partitioned destination disk** window stating that the destination disk contains partitions, perhaps with data.



You can continue once existing partitions are deleted

You will have to select between:

- **Delete partitions on the destination hard disk** — all existing partitions will be deleted during cloning and all their data will be lost.
- **No, I do not want to delete partitions** — no existing partition will be deleted, making the cloning impossible. You will only be able to cancel this operation and return to select another disk.

To continue, select the first choice and click **Next**.

No real changes and data destruction will be performed at this time! For now, the program will just create a cloning script. All changes will be implemented only when you click **Proceed**, after the script is formed.

13.3.5 Old and new disk partition layout

If you have selected the automatic mode before, the program will ask you for nothing more. You will see the window graphically illustrating information (as rectangles) about the source disk (partitions and unallocated space), and the destination disk layout.

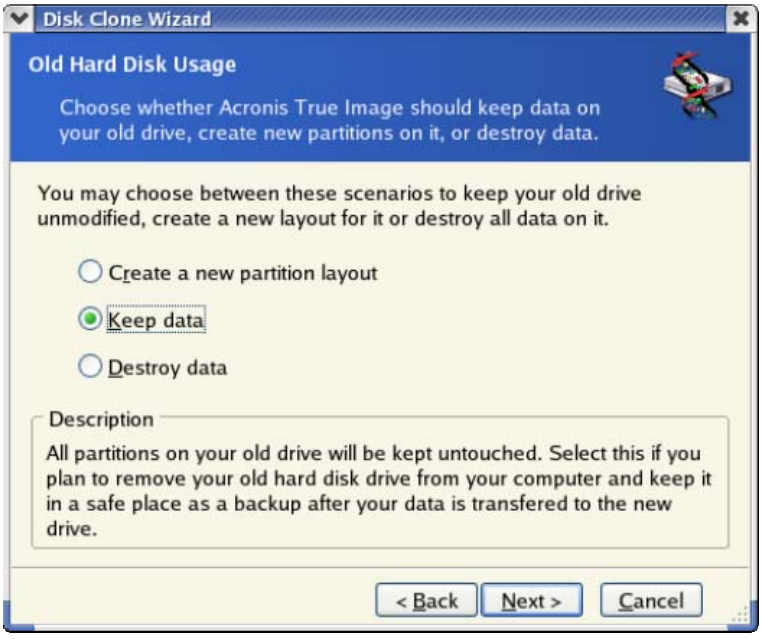
Along with the disk number some additional information is provided: capacity, label, partition and file system information. Partition types — primary, logical — and unallocated space are marked with different colors.

Next you will see the cloning script.

13.3.6 Old disk data

If you selected the manual mode, the program will ask you what to do with the old disk:

- **Create a new partition layout** — create a new partition layout. All existing partitions and their data will be deleted (but they will also be cloned to the new disk, so you won't lose them)
- **Keep data** — leave the old disk partitions and data intact
- **Destroy data** — delete partitions (and data) from the old disk



If you are going to sell, give away or otherwise part with your old disk, we recommend that you clean all information from it to avoid the data getting into unfriendly hands.

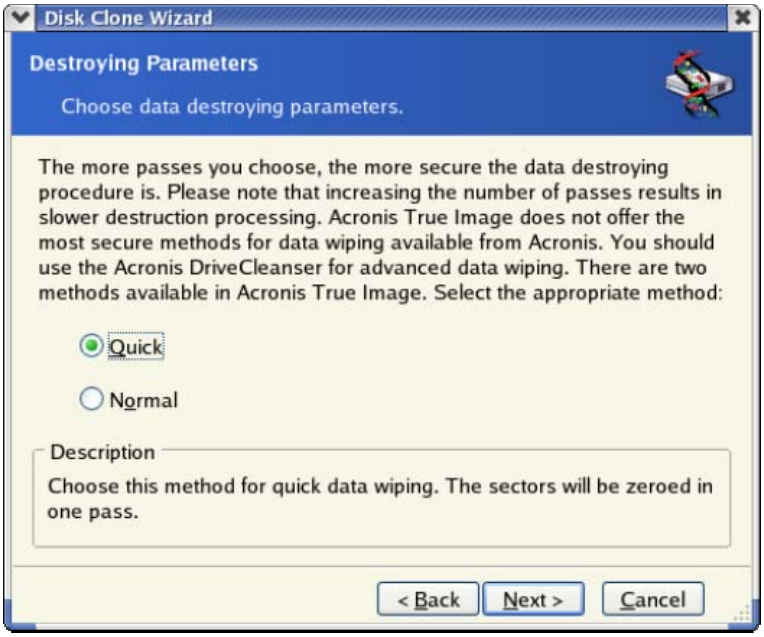
If you are going to keep the old disk and use it for data storage, you can create a new partition layout on it. In this case, the disk will be ready to use right after cloning is complete.

To protect yourself from unforeseen consequences, it is recommended that you leave the old disk data intact until you are certain that the cloning process worked. You can wipe the old disk anytime you want later.

13.3.7 Destroying the old disk data

If you decided to destroy the old disk data on the previous step, you will have to select the destruction method now:

- **Quick** — one-pass destruction (takes several minutes)
- **Normal** — guaranteed multipass destruction (takes additional time)



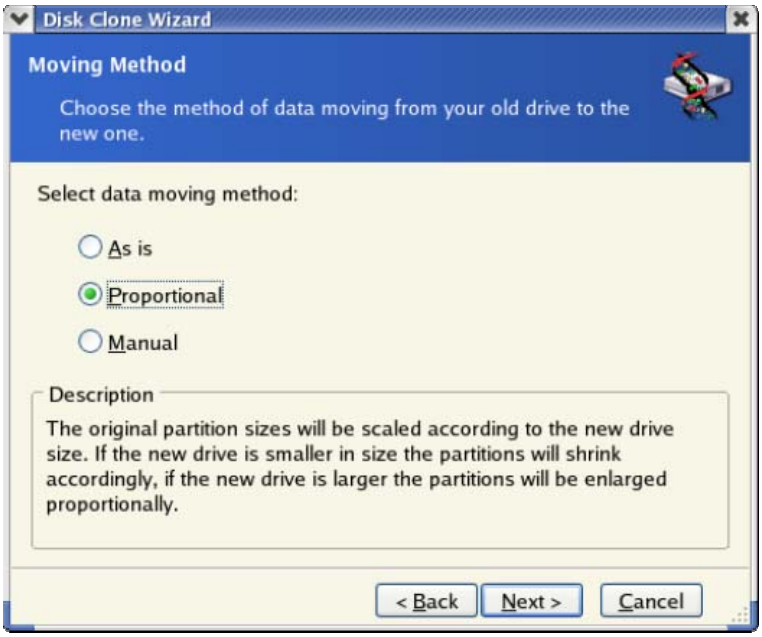
The second method takes more time, but makes it impossible to recover data afterwards, even with special equipment.

The first method is less secure but is still suitable for most cases.

13.3.8 Selecting partition transfer method

Acronis True Image Server for Linux will offer you the following data transfer methods:

- **As is**
- **Proportional** — the new disk space will be proportionally distributed among cloned partitions
- **Manual** — you will specify the new size and other parameters yourself



If you decide to transfer information "as is," a new partition will be created for every old one with the same size and type, file system and label. The unused space will become unallocated. Further you will be able to use it to create new partitions or to enlarge the existing partitions with special tools (e.g. Acronis Disk Director Suite.)

As a rule, "as is" transfers are discouraged, as they leave a lot of unallocated space on the new disk.

If you transfer data proportionally, each partition will be enlarged, according to the old and new disk capacities proportion.

In some cases, some partitions may still be transferred "as is" or be enlarged to the lesser extent compared to the other.

"As is," Acronis True Image Server for Linux transfers unsupported and damaged file systems.

Note that FAT16 partitions have a 2 GB maximum size limit.

Depending on the selected combination, you will proceed to either the old disk partitioning window or disk partition layout window (see below).

13.3.9 Partitioning the old disk

If you have selected **Create a new partition layout** before, it's now time to re-partition your old disk.

At this point, you will see the current disk partition layout. Initially the disk has unallocated space only. This will change when you create new partitions.

Having completed the required steps, you will add a new partition. To create another one, simply repeat these steps.

If you make a mistake, click **Back** to redo the operation.

After you create the necessary partitions, uncheck the **Create new partition in unallocated space** box and click **Next**.

13.3.10 Old and new disk partition layouts

In the next window, you will see rectangles indicating the source hard disk, including its partitions and unallocated space, as well as the new disk layout.

Along with the hard disk number, you will see its capacity, label, partition and file system information. Primary, logical partitions and unallocated space are colored differently.

If you have selected manual partition creation before, the partition layout will look different. That partitioning method is described below.

13.3.11 Cloning script

In the next window, you will see the disk cloning script containing a list of briefly described operations to be performed on the disks.

After you click **Proceed**, Acronis True Image Server for Linux will start cloning, indicating the progress in the special window. You can stop this procedure by clicking **Cancel**. In this case, you will have to re-partition and format the new disk or repeat the cloning procedure.

After the operation is complete, you will see the results message.

13.4 Cloning with manual partitioning

13.4.1 Old and new disk partition layouts

The manual transfer method enables you to resize partitions on the new disk. By default, the program resizes them proportionally.

In the next window, you will see rectangles indicating the source hard disk, including its partitions and unallocated space, as well as the new disk layout.

Along with the hard disk number, you will see its capacity, label, partition and file system information. Different partition types, including primary, logical, and unallocated space, are all colored differently.

To resize either partition, check the **Proceed Relayout** box. If you are satisfied with the partition layout shown, uncheck this box (if checked). Clicking **Next,** you will proceed to the cloning script window.

Be careful! Clicking **Back** in this window will reset all size and location changes that you've selected, so you will have to specify them again.

First, select a partition to resize. It will become underlined in red.

Resize and relocate it on the next step.

You can do this by entering values to **Unallocated space before**, **Partition size**, **Unallocated space after** fields, by dragging partition borders, or the partition itself.

If the cursor turns to two vertical lines with left and right arrows, it's pointed at the partition border and you can drag it. If the cursor turns to four arrows, it's pointed at the partition and you can move it to the left or right (if there's unallocated space near it).

Having provided the new location and size, click **Next**. You will be taken two steps back to the partition layout. You may have to perform some more resizing and relocation before you get the layout you need.

Chapter 14. Adding a new hard disk

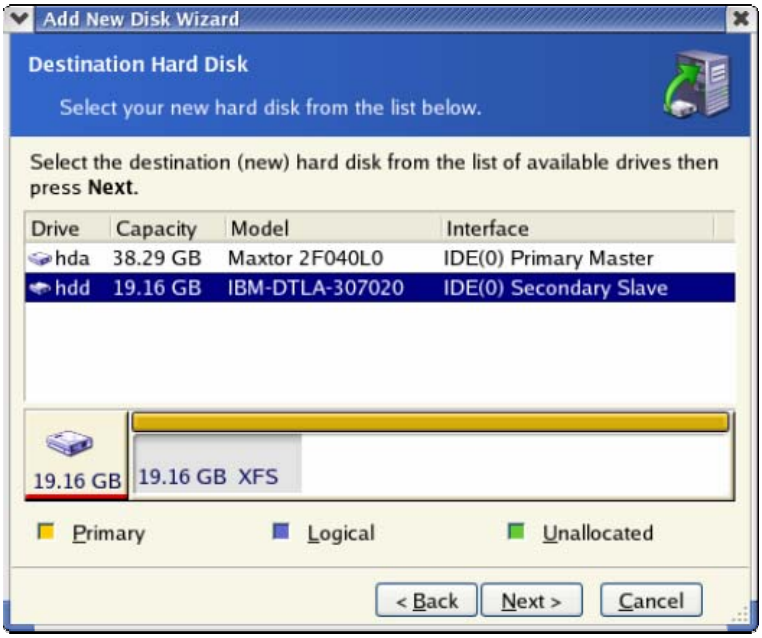
If you don't have enough space for your data, you can replace the old disk with a higher-capacity one (data transfers to new disks are described in the previous chapter). But you can also add a new disk only to store data, leaving the system on the old disk. If the server has space for another disk, it would be easier to add it, then clone.

To add a new disk, you must first install it on your server.

Note that **disk cloning and disk addition operations are not available for mounted disks**. In such cases, you will need to run Acronis True Image Server for Linux from a rescue CD.

14.1 Selecting a hard disk

Select the disk you've added to the server.



This window might be bypassed if the program detects the new disk itself. In that case, you will immediately proceed to the **New partition creation**.

If there are any partitions on the new disk, they must be deleted first.

Select **Delete partitions on the destination hard disk** and click **Next** to continue.

14.2 Creating a new partition

At this step, you will see the current partition layout. Initially, all disk space will be unallocated. This will change after you add partitions.

To create a partition in the unallocated space, select **Create new partition in unallocated space** and click **Next** to perform steps required by the partition creation wizard.

If you make a mistake at partitioning, click **Back** to redo the operation.

After you create the necessary partition layout, uncheck the **Create new partition in unallocated space** box and click **Next**.

14.3 Disk adding script

In the next window, you will see the disk add script containing a list of briefly described operations to be performed on disks.

Add New Disk script

After you click **Proceed**, Acronis True Image Server for Linux will start creating and formatting new partitions, indicating the progress in the special window. You can stop this procedure by clicking **Cancel**. In that case, you will have to re-partition and format the new disk or repeat the disk add procedure.

After the operation is complete, you will see the results message.