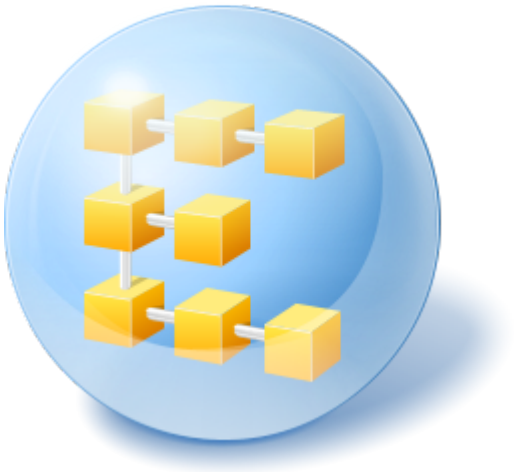

Acronis® Backup & Recovery ® 10 Server for Linux

Update 5

Command-Line Reference

Table of contents

1 Console mode in Linux 3

1.1 Backup, restore and other operations (trueimagecmd) 3

1.1.1 Supported commands 3

1.1.2 Common options 6

1.1.3 Specific options 9

1.1.4 trueimagecmd usage examples 17

1.2 Automatic image creation using cron service 18

1.3 Restoring files with trueimagemnt 19

1.3.1 Supported commands 19

1.3.2 Trueimagemnt usage examples 21

1 Console mode in Linux

Console is a natural part of Linux OS. Acronis Backup & Recovery 10 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 the **'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.
- a user interaction, such as inserting second media like CD, DVD, or tape when the first one is full. Likewise, if there is no media inserted in the drive at all, the operation fails.

Therefore, under complex conditions, we recommend that you use the more powerful **acronis_console** 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**.

These utilities are also available when operating under the Linux-based bootable media.

1.1 Backup, restore and other operations (trueimagecmd)

1.1.1 Supported commands

trueimagecmd has the following format:

```
trueimagecmd --command --option1 --option2…
```

Commands may be accompanied with options. Some options are common for most **trueimagecmd** commands, while others are specific for individual commands. Below is a list of supported commands and compatible options.

Command	Common Options	Specific Options
create Creates an image of specified disks and partitions	--vault:[path] --arc:[archive name] --arc_id:[archive id] --filename:[filename] --password:[password] --crypt:[AES128|AES192|AES256] --incremental --differential --compression:[0…9] --split:[size in MB] --oss_numbers --log:[filename] --silent	--harddisk:[disk number] --partition:[partition number] --raw --progress:[on|off] --exclude_names:[names] --exclude_masks:[masks] --exclude_hidden --before:[pre-data capture command] --after:[post-data capture command]
filebackup Backs up specified files and	--vault:[path] --arc:[archive name]	--include:[names] --exclude_names:[names]

folders	--arc_id:[archive id] --filename:[filename] --password:[password] --crypt:[AES128|AES192|AES256] --incremental --differential --compression:[0…9] --split:[size in MB] --log:[filename] --silent	--exclude_masks:[masks] --exclude_hidden --before:[pre-data capture command] --after:[post-data capture command] --progress:[on | off]
restore Restores disks and partitions from an image	--filename:[filename] --password:[password] --asz:[number of archive] --index:N --oss_numbers --log:[filename] --silent	--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 and folders from a file archive	--vault:[path] --arc:[archive name] --arc_id:[archive id] --filename:[filename] --password:[password] --asz:[number of archive] --index:N --log:[filename] --silent	--target_folder:[target folder] --overwrite:[older|never|always] --restore_security:[on|off] --original_date:[on|off] --include:[names]
deploy_mbr Restores the MBR from a disk or partition image	--vault:[path] --arc:[archive name] --arc_id:[archive id] --filename:[filename] --password:[password] --asz:[number of archive] --index:N --oss_numbers --log:[filename] --silent	--harddisk:[disk number] --target_harddisk:[disk number]
verify Verifies the archive data integrity	--vault:[path] --arc:[archive name] --arc_id:[archive id] --filename:[filename] --password:[password] --asz:[number of archive] --log:[filename] --silent	--folder_name:[path] --no_subdir
pit_info Displays the numbered list of backups, contained in the specified archive	--filename:[filename] --password:[password] --asz:[number of archive]	
consolidate	--include_pits:[pits numbers] --filename:[filename]	--target_filename:[file name]

Creates a consistent copy of the archive which will contain only the specified backups	--password:[password] --log:[filename] --silent	
export Creates a copy of an archive or a self-sufficient part copy of an archive in the location you specify	--vault:[path] --arc:[archive name] --arc_id:[archive id] --include_pits:[pits numbers] --password:[password] --progress:[on | off] --log:[filename] --net_user:[username] --net_password:[password] --ftp_user:[username] --ftp_password:[password] --silent	--target_vault:[target path] --target_arc:[target archive name]
list Lists available drives and partitions. When used with the **filename** option, it lists the image contents. When used with the **vault** option, it lists archives located in the specified location. When the **arc**, or the **arc_id** option is added, it lists all backups contained in the archive.	--password:[password] --index:N --asz:[number of archive]	--filename:[file name] --vault:[path] --arc:[archive name] --arc_id:[archive id]
asz_create Creates the Acronis Secure Zone on the selected drive	--password:[password] --oss_numbers --log:[filename] --silent	--harddisk:X --partition:[partition number] --size:[ASZ size in sectors]
asz_content Displays the Acronis Secure Zone size, free space and contents	--password:[password]	
asz_files Displays the Acronis Secure Zone size, free space and contents using the generated file names	--password:[password]	
asz_delete Deletes the Acronis Secure Zone	--password:[password] --oss_numbers --log:[filename] --silent	--partition:[partition number]
asrm_activate Activates the Acronis Startup Recovery Manager		

asrm_deactivate Deactivates the Acronis Startup Recovery Manager		
clone Clones a hard disk		--harddisk:[disk number] --target_harddisk:[disk number]
help Shows usage		
ls_check Checks if there are licenses for the local machine on the license server		
dumpraidinfo Saves information about MD devices and LVM volumes to the /etc/Acronis directory		

1.1.2 Common options

1.1.2.1 Access to archives

vault:[path]

Specifies a path to the location that contains the archive. Used in combination with the **arc**, or the **arc_id** option.

The following locations are supported:

- Local folders, e.g.: --`vault:/folder`, or --`vault:"/Folder 1"`
- Network folders, e.g.: --`vault:smb://Server/Share/`
- Managed vaults (for advanced product editions only), e.g.: --`vault:bsp://StorageNode/VaultName`
- FTP and SFTP, e.g.: --`vault:ftp://ServerA/Folder1`
- CD, DVD – with the path specified as a local path, e.g.: --`vault:/mnt/cdrom`
- Acronis Secure Zone, e.g.: --`vault:atis:///asz`
- Unmanaged vaults are specified by their path. For example, if a vault is located in a folder, specify the path to that folder.

If the **vault** option is specified the **filename** option is ignored.

*Please note, for **create**, **filebackup**, **filerestore**, **verify** commands only managed vaults and tapes are supported.*

arc:[archive name]

The name of the archive. If not specified, the **arc_id** option is used. If both the **arc** and **arc_id** options are specified, the **arc_id** option is used.

arc_id:[archive id]

Specifies the Universally Unique Identifier (UUID) of the archive, e.g.:

```
--arc_id:183DE307-BC97-45CE-9AF7-60945A568BE8
```

If not specified, the **arc** option is used. If both the **arc** and **arc_id** options are specified, the **arc_id** option is used.

filename:[filename]

Archive name, if the archive location is other than ASZ.

To get Samba network access, specify the backup file name and the log file name as follows:

```
--filename:smb://username:password@hostname/sharename/filename

--log:smb://username:password@hostname/sharename/logfilename
```

or:

```
--filename:smb://hostname/sharename/filename –-net_user:username \ --
net_password:password

--log:smb://hostname/sharename/logfilename –-log_net_user:username \ --
log_net_password:password
```

Only the last two options can be used if the user name or password contains the @ or / symbols.

To access an NFS network drive, specify the backup 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.

If the **vault** option is specified the **filename** option is ignored.

password:[password]

a) Password for the archive, if the archive location is other than ASZ.

b) Password for the ASZ, if archive location is ASZ.

asz:[number of archive]

Addresses to the ASZ and selects the archive (a full backup with or without increments).

To get the archive number, use **asz_content.**

index:N

N = Number of the backup in an archive:

- 1 = basic full backup
- 2 = 1st increment… and so on
- 0 (default) = latest increment

Selects a backup in a sequence of incremental backups inside the archive.

To get a backup index from the ASZ, use **asz_content**.

ftp_user:[username]

Specify a user name for access to an FTP server.

ftp_password:[password]

Specify a password for access to an FTP server.

net_user:[username]

Specifies the user name for logon to the network share to save the resulting archive.

net_password:[password]

Specifies the *password* for logon to the network share to save the resulting archive.

include_pits:[pits numbers]

Specifies the backups (pits) to be included in the archive copy. To get the numbers of pits, use **pit_info**. Separate multiple values with a comma, for example:

```
--include_pits:2,4,5
```

1.1.2.2 Backup options

incremental

Set the backup type to incremental.

If not specified or there is no basic full backup, a full backup will be created.

differential

Set the backup type to differential.

If not specified or there is no basic full backup, a full backup will be created.

compression:[0...9]

Specify the data compression level.

It ranges from 0 to 9 and is set to 3 by default.

crypt:[AES128|AES192|AES256]

Specifies the key size for the AES algorithm encryption of the password-protected archive. The option is used together with the **--password** (p. 7) option. For example:

```
--password:QWerTY123 --crypt:AES256
```

The randomly generated encryption key is then encrypted with AES-256 using a SHA-256 hash of the password as a key. The password itself is not stored anywhere on the disk or in the backup file; the

password hash is used for verification purposes. With this two-level security, the backup data is protected from any unauthorized access, but recovering a lost password is not possible.

If the **/crypt** option is not specified, the password-protected archive will be not encrypted.

split:[size in MB]

Split the backup into parts of the specified size, if the archive location is other than ASZ.

1.1.2.3 General options

oss_numbers

Declares that numbers of partitions in the **partition** option are adjusted for the MBR partition table rather than be simple ascending numbers. This means that primary partitions have numbers 1-1, 1-2, 1-3, 1-4 and logical partitions numbers start with 1-5. For example, if the disk has one primary and two logical partitions, their numbers can appear as follows:

```
--partition:1-1,1-2,1-3
```

or

```
--oss_numbers --partition:1-1,1-5,1-6
```

log:[file name]

Create a log file of the current operation with the specified file name.

silent

Suppresses the command's output.

1.1.3 Specific options

1.1.3.1 create

harddisk:[disk number]

Specifies the 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.

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
```

To specify a logical volume (also called LVM volume) or an MD device (also called Linux Software RAID), use the DYN prefix. For example:

```
--partition:dyn1
```

raw

Use this option to create an image of a disk (partition) with an unrecognized or unsupported file system. This will copy all disk/partition contents sector-by-sector. Without this option only the sectors containing useful system and user data are imaged (for the supported file systems).

progress:[on | off]

Shows/hides the progress information (percent completed). It is shown by default.

exclude_names:[names]

Specifies files and folders to be excluded from the backup (comma separated). Object names have to be specified relative to the objects' partitions root entry.

For example, if "**boot**" partition is mounted to the **/boot** directory and it is necessary to exclude the "**grub**" directory from a backup, then it must be specified as **/grub/**. If this directory is located on a root partition, then **/boot/grub/** should be specified to exclude it from the backup.

exclude_masks:[masks]

Applies masks to select files to be excluded from the backup. Use the common Linux masking rules. For example, to exclude all files with extension **.sh**, add ***.sh**. **My???.sh** will exclude all **.sh** files with names consisting of five symbols and starting with "my".

exclude_hidden

Excludes all hidden files from the backup.

In Linux, a file is considered hidden if the first symbol in the file name is a dot.

before:[pre-data capture command]

Enables to define the command to be automatically executed before data capture.

after:[post-data capture command]

Enables to define the command to be automatically executed after data capture.

1.1.3.2 filebackup

include:[names]

Files and folders to be included in the backup (comma separated). For example:

```
--include:'/home/bot/ATIESsafe.iso,/home/bot/ATIW.iso'
```

exclude_names:[names]

Files and folders to be excluded from the backup (comma separated). For example:

```
--exclude_names:'/home/bot/ATIESsafe.iso,/home/bot/MyProject/Old'
```

exclude_masks:[masks]

Applies masks to select files to be excluded from the backup. Use the common Linux masking rules. For example, to exclude all files with extension **.sh**, add ***.sh**. **My???.sh** will exclude all **.sh** 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.

In Linux, a file is considered hidden if the first symbol in the file name is a dot.

before:[pre-data capture command]

Enables to define the command to be automatically executed before data capture.

after:[post-data capture command]

Enables to define the command to be automatically executed after data capture.

progress:[on | off]

Shows/hides the progress information (percent completed). It is shown by default.

1.1.3.3 restore

harddisk:[disk number]

Specifies the hard disks to restore by numbers.

partition:[partition number]

Specifies the partitions to restore by numbers. For example:

```
--partition:1-1,1-2,3-1
```

To specify a logical volume (also called LVM volume) or an MD device (also called Linux Software RAID), use the DYN prefix. For example:

```
--partition:dyn1
```

To list the partitions stored in the backup, use the **--list** command. For example:

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

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.

fat16_32

Enables the file system conversion from FAT16 to FAT32 if the partition size after recovery is likely to exceed 2 GB. Without this option, the recovered partition will inherit the file system from the image.

size:[partition size in sectors]

Sets the new partition size (in sectors).

type:[active | primary | logical]

Sets the restored partition active, primary or logical, if possible (for example, there cannot be more than four primary partitions on the disk). Setting a partition active always sets it primary, while a partition set primary may remain inactive.

If the type is not specified, the program tries to keep the target partition type. If the target partition is active, the restored partition is set active. If the target partition is primary, and there are other primary partitions on the disk, one of them will be set active, while the restored partition becomes primary. If no other primary partitions remain on the disk, the restored partition is set active.

When restoring a partition on unallocated space, the program extracts the partition type from the image. For the primary partition, the type will be set as follows:

- if the target disk is the 1st according to BIOS and it has no other primary partitions, the restored partition will be set active
- if the target disk is the 1st according to BIOS and there are other primary partitions on it, the restored partition will be set logical
- if the target disk is not the 1st, the restored partition will be set logical.

preserve_mbr

When restoring a partition over an existing one, the target partition is deleted from the disk along with its entry in the target disk MBR. Then, with the **preserve_mbr** option, the restored partition's entry will occupy the upper empty position in the target disk MBR. Thus, the target disk MBR is preserved. If not specified, the restored partition's entry will occupy the same position as in the source disk MBR saved in the image. If the position is not empty, the existing entry will be moved to another position.

1.1.3.4 filerestore

target_folder:[target folder]

Specifies a folder where folders/files will be restored (a target folder). If not specified, the original path is re-created from the archive.

overwrite:[older | never | always]

This option allows you to keep useful data changes made since the backup being restored was done. Choose what to do if the target folder contains a file with the same name as in the archive:

- *older* – this will give priority to the most recent file modification, whether it be in the archive or on the disk.
- *never* – this will give the file on the hard disk unconditional priority over the archived file.
- *always* – this will give the archived file unconditional priority over the file on the hard disk.

If not specified, the files on the disk will always be replaced with the archived files.

restore_security:[on | off]

Specifies whether to restore files' security attributes (default) or whether the files will inherit the security settings of the folder where they will be restored.

original_date:[on | off]

Specifies whether to restore files' original date and time from the archive or whether to assign the current date and time to the restored files. If not specified, the current date is assigned.

include:[names]

Specifies the files and folders to restore from the file backup (comma separated).

For example:

```
--include:'/home/bot/file1.i686,/home/bot/MyProject'
```

If not specified, all contents of the file backup are restored.

1.1.3.5 deploy_mbr

harddisk:[disk number]

Specifies the basic hard disk to restore the MBR from.

target_harddisk:[disk number]

Specifies the target hard disk where the MBR will be deployed to.

1.1.3.6 verify

folder_name:[path]

Specifies a path to the local folder that contains archives to verify.

For example:

```
--folder_name:'/home/bot/MyProject'
```

By default, all archives stored in the folder and its subfolders will be verified. To exclude the subfolders from verification, add the **--no_subdir** (p. 14) option.

no_subdir

This option is used together with the **/folder_name** option. Prohibits verification of archives stored in the subfolders of the specified folder.

For example:

```
--folder_name:'/home/bot/MyProject' --no_subdir
```

If the option is not specified, all archives stored in the parent folder and its subfolders will be verified.

1.1.3.7 consolidate

target_filename:[file name]

Specifies the path to and name of the archive copy to be created. If there are two or more backups (pits) in the copy, numbers will be added to their names.

1.1.3.8 export

target_vault:[target path]

Specifies a path to the target location to export the archive to.

The following target locations are supported:

- Local folders and unmanaged vaults, e.g.: --`vault:/folder`, or --`vault:"/Folder 1"`
- Managed vaults (for advanced product editions only), e.g.: --`vault:bsp://StorageNode/VaultName`
- Network folders, e.g.: --`vault:smb://Server/Share/`
- FTP and SFTP, e.g.: --`vault:ftp://ServerA/Folder1`
- CD, DVD – with the path specified as a local path, e.g.: --`vault:/mnt/cdrom`
- Acronis Secure Zone, e.g.: --`vault:atis:///asz`
- Tapes, e.g.: --vault:atis:///tape?0
- Unmanaged vaults are specified by their path. For example, if a vault is located in a folder, specify the path to that folder.

target_arc:[target archive name]

The name of the target archive. Has to be unique within the target folder. If there is an archive with the same name, the operation will fail.

1.1.3.9 list

filename:[filename]

With this option, the image contents are 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 the **--partition:<number in the image> --target_partition:<physical number of the target partition>** keys. For the above example, to restore partition 2-5 to its original place use:

```
--partition:2-2 --target partition:2-5
```

If the **vault** option is specified the **filename** option is ignored.

vault:[path]

Specifies a path to the location whose archives you want to list. Along with archive names, it lists Universally Unique Identifiers (UUID) that are used with the **arc_id** option.

The following locations are supported:

- Local folders, e.g.: --`vault:/folder`, or --`vault:"/Folder 1"`
- Network folders, e.g.: --`vault:smb://Server/Share/`
- Managed vaults (for advanced product editions only), e.g.: --`vault:bsp://StorageNode/VaultName`
- FTP and SFTP, e.g.: --`vault:ftp://ServerA/Folder1`
- CD, DVD – with the path specified as a local path, e.g.: --`vault:/mnt/cdrom`
- Acronis Secure Zone, e.g.: --`vault:atis:///asz`
- Tapes, e.g.: --`vault:atis:///tape?0`
- Unmanaged vaults are specified by their path. For example, if a vault is located in a folder, specify the path to that folder.

If the **vault** option is specified the **filename** option is ignored.

arc:[archive name]

Used in combination with the **vault** option. Lists all backups contained in the archive.

If not specified, the **arc_id** option is used. If both the **arc** and **arc_id** options are specified, the **arc_id** option is used.

arc_id:[archive id]

Used in combination with the **vault** option. Lists all backups of the selected archive.

If not specified, the **arc** option is used. If both the **arc** and **arc_id** options are specified, the **arc_id** option is used.

1.1.3.10 asz_create

password:[password]

a) Password for the archive, if the archive location is other than ASZ.

b) Password for the ASZ, if archive location is ASZ.

harddisk:X

Specifies the hard disk number where the Acronis Secure Zone will be created.

partition:[partition number]

Specifies partitions from which free space will be taken for Acronis Secure Zone.

size:[ASZ size in sectors | unallocated]

Sets the Acronis Secure Zone size (in sectors).

If not specified, the size is set as an average between the maximal (unallocated space plus free space on all partitions selected with the **partition** option) and minimal (about 35MB) values.

Either way, the program will first use the unallocated space. If there is not enough unallocated space, the selected partitions will be decreased. Resizing of locked partitions requires a reboot.

With “unallocated”, the zone will use all unallocated space on the disk. Partitions will be moved, if necessary, but not resized. Moving of locked partitions requires a reboot. The **partition** option is ignored.

1.1.3.11 asz_delete

partition:[partition number]

Specifies partitions to which free space will be added after the Acronis Secure Zone is deleted. If you specify several partitions, the space will be distributed proportionally based on each partition’s size.

1.1.3.12 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.

1.1.4 trueimagecmd usage examples

- The following command will list available partitions:

```
trueimagecmd --list
```

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

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

- The following command will check if there are licenses assigned to the local machine on the license server:

```
trueimagecmd --ls_check
```

  The result is a list of used licenses. For example:

```
Acronis Backup & Recovery 10 Advanced Server     (trial)      invalid
Acronis Backup & Recovery 10 Advanced Server           valid
```

- The following command will create an image named backup.tib of partition 1-1:

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

- The following command will create an incremental image of the above partition:

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

- The following command will create an image of partition 1-1 in the Acronis Secure Zone:

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

- The following command will create an image of an MD device (which may reside on two or more partitions):

```
trueimagecmd --partition:dyn1 --filename:backup.tib --create
```

- This will restore a partition from backup.tib:

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

- The following command will restore an MD device from backup.tib:

```
trueimagecmd --partition:dyn1 --filename:backup.tib --restore
```

- The following command will back up the folder /usr/kerberos/lib to the FTP server location:

```
trueimagecmd --filebackup --include:'/usr/kerberos/lib' \
--filename:ftp://myftp.com/Backup/MyLib.tib --ftp_user:usr1 \
--ftp_password:passw1
```

- The following command will back up the folder /bin to the shared folder on host1 and create the operation log in the shared folder on host2:

```
trueimagecmd --filebackup --include:’/bin' \
--filename:smb://username1:password1@host1/dir/MyBin.tib \
--log:smb://username2:password2@host2/dir/Mylog1.log
```

- The following command will list backups, contained in the archive /usr/backups/backups.tib, with their pit numbers. This command is designed to obtain pit numbers for consolidation:

```
trueimagecmd --pit_info --filename:/usr/backups/backups.tib
```

  The list will look like the following:

```
Pit number: 1
  type: file; kind: base; date: 10/18/07 2:45:02 PM
Pit number: 2
  type: file; kind: incremental; date: 10/18/07 2:47:38 PM
Pit number: 3
  type: file; kind: incremental; date: 10/18/07 2:49:58 PM
```

- The following command will create in the folder /usr/backups an archive consisting of two files: kons.tib, (pit 2 of the archive /usr/backups/backups.tib) and kons2.tib (pit 3 of the archive /usr/backups/backups.tib). Therefore, the 'kons' archive is a copy of the 'backups' archive without pit 1. Use this command to get rid of backups that you no longer need, while keeping the archive:

```
trueimagecmd --consolidate --filename:/usr/backups/backups.tib \
--include_pits:2,3 --target_filename:/usr/backups/kons.tib
```

- The following command will restore the MBR from partition image D1 to the hard disk 1:

```
trueimagecmd --deploy_mbr --filename:/usr/backups/D1.tib --harddisk:1
```

- The following command will export the "archive1" archive from the root folder to the new archive named "archive2" in the "exported" folder:

```
trueimagecmd --export --vault:/ --arc:archive1 --target_vault:/exported \
--target_arc:archive2
```

- The following command will export the "archive1" archive from managed vault "vault10" to the network share:

```
trueimagecmd --export --vault:bsp://StorageNode/vault10 --arc:archive1 \
--net_src_user:username --net_src_password:password \
--target_vault:smb://server/exported --target_arc:archive2 \
--net_user:username --net_password:password
```

- The following command will export the "archive1" archive from the network share to the "exported" folder:

```
trueimagecmd --export --vault:smb://server/backups/ --arc:archive1 \
--target_vault:/exported --target_arc:archive2 --net_src_user:username \
--net_src_password:password
```

1.2 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 the **--list** command 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 the name and path of the image.

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 set up their own backup schedule. For more information, see Help on the **cron** service.

1.3 Restoring files with trueimagemnt

The **trueimagemnt** tool is designed to restore files from partition/disk images. It mounts Acronis Backup & Recovery 10 archives as if they were kernel space block devices. The program implements the user level part of the user mode block device service of Acronis Backup & Recovery 10. The majority of the 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]
```

1.3.1 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 the **-f|--filename** option into the folder specified by the **mountpoint** option. The partition index should be specified by the **-i|--index** option. Image file contents (partitions and their indices) may be listed by the **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 the successive images is missing, mounting is impossible.

-u|--umount mountpoint

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

-s|--stop pid

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

-o|--loop

A test command. Mounts a file, specified in the **-f|--filename** option, containing a valid Linux filesystem, as if it were an Acronis Backup & Recovery 10 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 Network File System (NFS) and Samba network access. To access an 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
```

The hostname may be specified with the username and password as: username:password@hostname, unless the user name or password contains the @ or / symbols.

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

1.3.2 Trueimagemnt usage examples

- The following command will list the mounted archives:

```
trueimagemnt --list
```

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

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

- The following command will unmount a partition mounted at /mnt/backup:

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