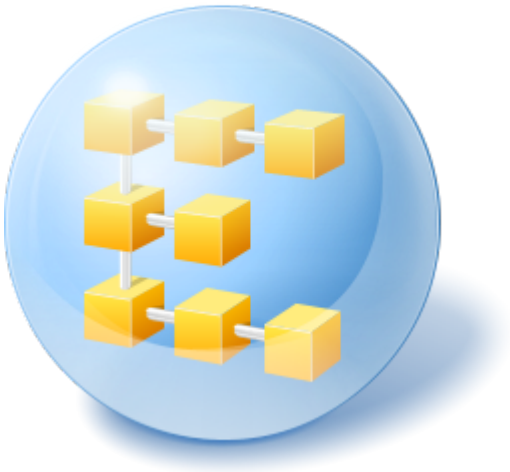

Acronis® Backup & Recovery ® 10 Advanced Server Virtual Edition

Update 5

Command-Line Reference

Table of contents

1 Command-line mode and scripting in Windows

Acronis Backup & Recovery 10 supports the command-line mode and enables backup automation by executing XML scripts.

Acronis Backup & Recovery 10 uses the Acronis True Image Echo command line utility with the following additions:

1. Ability to use the before/after data capture commands.
2. Ability to use the VSS support option.
3. Ability to check for a license on the license server with the /ls_check command.
4. Ability to use file exclusion at disk backup.
5. Ability to export archives and backups.

The rest of the commands and options are exactly the same. For this reason, the command line reference uses the terminology accepted in Acronis True Image Echo.

The command line logs are saved in the old (Echo) format and cannot be converted to Acronis Backup & Recovery 10 logs.

Command line mode limitations

The command-line mode functionality is somewhat more limited than the GUI mode. You will not be able to perform:

- recovery of a system volume
- operations that require a user interaction, such as inserting removable media (CD, DVD or tape). The operation fails if there is no media in the drive or the inserted media is full.

These operations only can be done through the GUI.

Scripting is intended only for backup.

1.1 Agent for Windows command-line utility

An administrator might need a console interface in some situations. Acronis Backup & Recovery 10 supports this mode with trueimagecmd.exe utility. The file is located in the folder where Acronis Backup & Recovery 10 Agent for Windows has been installed, by default it is C:\Program Files\Acronis\BackupAndRecovery.

This utility is also available when operating under the PE-based bootable media.

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:[file name] /password:[password] /crypt:[AES128|AES192|AES256] /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /incremental /differential /compression:[0…9] /split:[size in MB] /oss_numbers /progress:[on|off] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/harddisk:[disk number] /partition:[partition number] /file_partition:[partition letter] /raw /exclude_names:[names] /exclude_masks:[masks] /exclude_system /exclude_hidden /before:[pre-data capture command] /after:[post-data capture command] /use_vss
filebackup Backs up specified files and folders	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /crypt:[AES128|AES192|AES256] /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /incremental /differential /compression:[0…9] /split:[size in MB] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/include:[names] /exclude_names:[names] /exclude_masks:[masks] /exclude_system /exclude_hidden /before:[pre-data capture command] /after:[post-data capture command] /use_vss

deploy Restores disks and partitions, except for the MBR, from an image	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /oss_numbers /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/file_partition:[partition letter] /harddisk:[disk number] /partition:[partition number] /target_harddisk:[disk number] /target_partition:[partition number] /start:[start sector] /size:[partition size in sectors] /fat16_32 /type:[active|primary|logical] /preserve_mbr **When using the Acronis Universal Restore option:** /ur_path:[path] /ur_username:[user] /ur_password:[pwd] /ur_driver:[inf-filename]
deploy_mbr Restores the MBR from a disk or partition image	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/harddisk:[disk number] /target_harddisk:[disk number]
filerestore Restores files and folders from a file archive	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name] /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /reboot /later /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/target_folder:[target folder] /overwrite:[older|never|always] /restore_security:[on|off] /original_date:[on|off] /include:[names]
verify Verifies the archive data integrity	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name]	folder_name:[path] no_subdir

	/password:[password] /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	
pit_info Displays the numbered list of backups, contained in the specified archive	/filename:[file name] /password:[password] /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password]	
consolidate Creates a consistent copy of the archive which will contain only the specified backups	/include_pits:[pits numbers] /filename:[file name] /password:[password] /ftp_user:[username] /ftp_password:[password] /reboot /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/target_filename:[file name] /net_src_user:[username] /net_src_password:[password] /net_user:[username] /net_password:[password]
export Creates a copy of an archive or a self-sufficient part copy of an archive in the location you specify	/vault:[path] /arc:[archive name] /arc_id:[archive id] /include_pits:[pits numbers] /password:[password] /ftp_user:[username] /ftp_password:[password] /progress:[on|off] /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/net_src_user:[username] /net_src_password:[password] /ftp_src_user:[username] /ftp_src_password:[password] /target_vault:[target path] /target_arc:[target archive name] /net_user:[username] /net_password:[password]
convert Converts an image to virtual disk format for using with a virtual machine	/filename:[file name] /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password] /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/target_filename:[file name] /harddisk:[disk number] /vm_type:[vmware|esx|microsoft|parallels] /ur /ur_path:[path]
list	/password:[password]	/filename:[file name]

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.	/index:N /asz:[number of archive] /net_user:[username] /net_password:[password] /ftp_user:[username] /ftp_password:[password]	/vault:[path] /arc:[archive name] /arc_id:[archive id]
explore Connects an image as a virtual drive	/vault:[path] /arc:[archive name] /arc_id:[archive id] /filename:[file name]* /password:[password] /asz:[number of archive] /index:N /net_user:[username] /net_password:[password] /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent *for a split image, the name of the last created file	/partition:[partition number] /letter:X
unplug Disconnects the image connected as a virtual drive		/letter:X /letter:all
asz_create Creates the Acronis Secure Zone on the selected drive	/password:[password] /oss_numbers /reboot /later /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	/harddisk:X /partition:[partition number] /size:[ASZ size in sectors|unallocated]
asz_content Displays the Acronis Secure Zone size, free space and contents	/password:[password]	

asz_files Displays the Acronis Secure Zone size, free space and contents using the generated file names	/password:[password]	
asz_delete_files Deletes the most recent backup in the archive located in the Acronis Secure Zone	/filename:[file name] /password:[password] /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /silent	
asz_delete Deletes the Acronis Secure Zone	/password:[password] /oss_numbers /reboot /later /log:[file name] /log_net_user:[remote user] /log_net_password:[password] /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	/reboot /later /silent	/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		

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

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

*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 options are specified, the **arc_id** option is used.

filename:[file name]

a) Backup file name, if the archive location is other than ASZ.

b) Archive name, when restoring or deleting files from ASZ. Can be obtained with asz_files.

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

password:[password]

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

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

asz:[number of archive]

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

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

index:N

N = Number of the backup in an archive:

- 1 = basic full backup

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

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

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

include_pits:[pits numbers]

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

```
/include_pits:2,4,5
```

The "0" value means the last backup in the archive, for example:

```
/include_pits:0
```

If not specified the whole archive is selected.

net_user:[username]

Specify a user name for network drive access.

net_password:[password]

Specify a password for network drive access.

ftp_user:[username]

Specify a user name for access to an FTP server.

ftp_password:[password]

Specify a password for access to an FTP server.

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. 9) 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 just as ascending numbers. This means that primary partitions have numbers 1-1, 1-2, 1-3, 1-4; logical partitions numbers start with 1-5. For example, if the disk has one primary and two logical partitions, their numbers can appear as follows:

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

or

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

reboot

Reboot the machine before the operation (if required) or after the operation is completed.

Use this option when performing the following operations that require a reboot: recovering locked files, creating/deleting Acronis Secure Zone on a system disk, cloning a system disk. The machine will be rebooted automatically. To postpone the operation until a user reboots the system manually, add the **/later** option. With this option, the operation will be performed after the user initiates a reboot.

The **/reboot** option can be used with operations that do not necessarily require a reboot. Examples of such operations are: recovery under bootable media, recovering files that are not locked by the operating system, archives validation, and most types of backup. In those cases a reboot will be performed after the operation is completed. The **/later** option is not necessary.

The following table summarizes the software behavior with and without the **/reboot** and **/later** options.

	Reboot is necessary	Reboot is not required
/reboot /later	Reboot before operation (postponed)	Reboot after operation
/reboot	Reboot before operation	Reboot after operation
no option	No reboot, operation fails	No reboot, operation succeeds

later

Postpone the reboot until a user restarts the system manually. The option is used with the **/reboot** option in the following operations that require a reboot: recovering locked files, creating/deleting Acronis Secure Zone on a system disk, cloning a system disk.

log:[file name]

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

log_net_user:[remote user]

If the log file is created on a network share, include the user name for logon to the share.

log_net_password:[password]

If the log file is created on a network share, include the password for logon to the share.

silent

Suppresses the command's output.

progress:[on | off]

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

1.1.3 Specific options

1.1.3.1 create

harddisk:[disk number]

Specifies the hard disks to include into the image file. The list of available hard disks is provided by the /list command. An image may contain data of more than one hard disk. In that case, separate disk numbers by commas, e.g.:

```
/harddisk:1,3
```

By specifying

```
/harddisk:DYN
```

you will back up all dynamic volumes present in the system.

partition:[partition number]

Specifies the partitions to include into the image file. The list of available partitions is provided by **/list**. Partition numbers are specified as **<disk number>-<partition number>**, e.g.:

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

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/partition:DYN1,DYN2
```

Both basic partitions and dynamic volumes can be specified by their letters, for example:

```
/partition:"C"
```

Mixed notation is also acceptable, for example:

```
/partition:1-1,"D"
```

file_partition:[partition letter]

Specifies the partition where the image file will be stored (by letter or number). This option is used with **filename:[file_name]**. In that case the file name must be specified without a drive letter or root folder. For example:

```
/file_partition:D /filename:”\1.tib”
```

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/file_partition:DYN1 /filename:”\1.tib”
```

raw

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

progress:[on | off]

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

exclude_names:[names]

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

```
/exclude_names:E:\MyProject\111.doc,E:\MyProject\Old
```

exclude_masks:[masks]

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

exclude_hidden

Excludes all hidden files from the backup.

before:[pre-data capture command]

Enables to define the command to be automatically executed before data capture at the beginning of the backup procedure. For example:

```
/before:"net stop MSSQLSERVER"
```

after:[post-data capture command]

Enables to define the command to be automatically executed after data capture at the beginning of the backup procedure. For example:

```
/after:"net start MSSQLSERVER"
```

use_vss

Notifies the VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications, in particular, completion of all database transactions, at the moment of taking the data snapshot. The data consistency, in turn, ensures that the application will be recovered in the correct state and become operational immediately after recovery.

1.1.3.2 filebackup

include:[names]

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

```
/include:E:\Workarea\MyProject
```

exclude_names:[names]

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

```
/exclude_names:E:\MyProject\111.doc,E:\MyProject\Old
```

exclude_masks:[masks]

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

exclude_system

Excludes all system files from the backup.

exclude_hidden

Excludes all hidden files from the backup.

before:[pre-data capture command]

Enables to define the command to be automatically executed before data capture at the beginning of the backup procedure. For example:

```
/before:"net stop MSSQLSERVER"
```

after:[post-data capture command]

Enables to define the command to be automatically executed after data capture at the beginning of the backup procedure. For example:

```
/after:"net start MSSQLSERVER"
```

use_vss

Notifies the VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications, in particular, completion of all database transactions, at the moment of taking the data snapshot. The data consistency, in turn, ensures that the application will be recovered in the correct state and become operational immediately after recovery.

1.1.3.3 deploy

file_partition:[partition letter]

Specifies the partition where the image file will be stored (by letter or number). This option is used with **filename:[file_name]**. In that case the file name must be specified without a drive letter or root folder. For example:

```
/file_partition:D /filename:”\1.tib”
```

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/file_partition:DYN1 /filename:”\1.tib”
```

harddisk:[disk number]

Specifies the basic hard disks to restore.

partition:[partition number]

Specifies the partitions to restore.

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/partition:DYN1
```

target_harddisk:[disk number]

Specifies the hard disk number where the image will be restored.

By specifying

```
/target_harddisk:DYN
```

you will select unallocated space on all dynamic disks that are present in the system.

target_partition:[partition number]

Specifies the target partition number for restoring a partition over the existing one. If the option is not specified, the program assumes that the target partition number is the same as the partition number specified with the /partition option.

Dynamic volumes are specified with the prefix DYN, e.g.:

```
/target_partition:DYN1
```

start:[start sector]

Sets the start sector for restoring a partition to the hard disk unallocated space.

size:[partition size in sectors]

Sets the new partition size (in sectors).

fat16_32

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

type:[active | primary | logical]

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

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

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

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

preserve_mbr

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

Options specific for Universal Restore

The following options are available when using the Universal Restore add-on to Acronis Backup & Recovery 10.

ur_path:[path]

Specifies using Acronis Universal Restore and the path to the drivers storage.

ur_username:[username]

Specifies using Acronis Universal Restore and a user name.

When getting access to a place located on the remote computer, the *username* depends on the service which is used to get access to the remote resource. E.g. if the remote resource is a shared folder located on a workgroup computer, the *username* must contain the remote computer name ("Computer_name\User_name"). If the resource is located on an FTP-server the computer name is not required. When the target and local computer are members of different domains, the *username* must contain the name of the domain the target computer is the member of (e.g. "Domain_name\User_name").

ur_password:[pwd]

Specifies using Acronis Universal Restore and a password associated with the **ur_username** option value.

ur_driver:[inf-filename]

Specifies using Acronis Universal Restore and the mass-storage driver to be installed.

1.1.3.4 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.

1.1.3.5 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:D:\MyFolder1,D:\MyFolder2\file_1.exe
```

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

1.1.3.6 verify

folder_name:[path]

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

For example:

```
/folder_name:D:\MyFolder
```

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. 18) option.

no_subdir

This option is used together with the **/folder_name** (p. 18) option. Prohibits verification of archives stored in the subfolders of the specified folder.

For example:

```
/folder_name:D:\MyBackups /no_subdir
```

If the option 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.

net_src_user:[username]

Specifies the user name for logon to the network share to access the source archive.

net_src_password:[password]

Specifies the *password* for logon to the network share to access the source archive.

net_user:[username]

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

net_password:[password]

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

1.1.3.8 export

net_src_user:[username]

Specifies the user name for logon to the network share to access the source archive.

net_src_password:[password]

Specifies the *password* for logon to the network share to access the source archive.

ftp_src_user:[username]

Specifies the user name for logon to the FTP/SFTP server to access the source archive.

ftp_src_password:[password]

Specifies the password for logon to the FTP/SFTP server to access the source archive.

target_vault:[target path]

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

The following target locations are supported:

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

target_arc:[target archive name]

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

net_user:[username]

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

net_password:[password]

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

1.1.3.9 convert

target_filename:[file name]

Specifies the path to and name of the virtual disk file to be created. The file extension corresponds to the type of virtual machine to which the virtual disk will be added:

- VMware virtual machine - **.vmdk**
- MS virtual machine and Citrix XenServer - **.vhd**
- Parallels virtual machine - **.hdd**.

harddisk:[disk number]

Specifies the hard disks to convert by numbers. For each disk, a separate virtual disk will be created.

By specifying

```
/harddisk:DYN
```

you will convert all dynamic volumes that are present in the system.

vm_type:[vmware|esx|Microsoft|parallels]

The type of virtual machine to which the virtual disk will be added.

ur

Use when converting the image of a disk, containing Windows, and the resulting virtual disk is supposed to be bootable. With this key, the program will add drivers, necessary for the virtual machine type selected with the **vm_type** key, to the resulting virtual disk. If the image was taken from a virtual machine of the same type, normally the key is not needed.

Drivers for the virtual machine reside in the storage, defined by the registry key *HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\UniversalRestore\DriversPackPath*. In case the storage has been moved, please change the key or use the command **ur_path:[path]**.

ur_path:[path]

The same as **ur** with custom path to the virtual machine drivers storage.

1.1.3.10 list

filename:[file name]

With this option, the image contents are displayed.

When listing image contents, the partition numbers may not coincide with those in the drives/partitions list, if the image does not contain all the disk partitions. For example, if the image contains partitions 2-3 and 2-5, they will be listed as 2-1 and 2-2.

If the **deploy /partition** command cannot find a partition in the image by its physical number, use the **partition:<number in the image> /target_partition:<physical number of the target partition>** keys. For the above example, to restore partition 2-5 to its original place use:

```
/partition:2-2 /target_partition:2-5
```

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

vault:[path]

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

The following locations are supported:

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

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

arc:[archive name]

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

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

arc_id:[archive id]

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

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

1.1.3.11 explore

partition:[partition number]

Specifies a list of partitions to be mounted as virtual drives. Without this option, all partitions stored in the image will be mounted.

To obtain the partition number for this option, list the image contents with the **/list/filename** command and use the number from the Idx column.

letter:X

Assigns letters to the mounted drives. This option is used with the **partition** option only.

1.1.3.12 unplug

letter:X

Specifies the virtual drive to be disconnected by letter.

letter:all

Disconnects all virtual drives.

1.1.3.13 asz_create

harddisk:X

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

partition:[partition number]

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

size:[ASZ size in sectors | unallocated]

Sets the Acronis Secure Zone size (in sectors).

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

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

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

1.1.3.14 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.

1.1.3.15 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.exe usage examples

1.1.4.1 Image disks and partitions

- The following command will create an image named 1.tib of partitions 2-1 and 1-3:

```
trueimagecmd /create /filename:"C:\Test\1.tib" /partition:2-1,1-3
```

  The image will be saved to the C:\Test\ folder.

- The following command will create an image of partitions 2-1 and 1-3 in the Acronis Secure Zone:

```
trueimagecmd /create /asz /partition:2-1,1-3
```

- The following command will create an image named 1.tib of partitions 2-1 and 1-3:

```
trueimagecmd /create /filename:"\Test\1.tib" /partition:2-1,1-3
/file_partition:3-1
```

  The image will be saved in the folder \Test on partition 3-1.

- The following command will append an incremental image to the image named 1.tib of hard disk 2:

```
trueimagecmd /create /filename:"C:\Test\1.tib" /password:qwerty
/harddisk:2 /reboot /raw /incremental /compression:5 /split:640
/progress:off
```

  The image will be saved to C:\Test\ folder, protected with password "qwerty", split into 640-MB parts, and contain all cluster data. Image compression level is 5. The server will be rebooted after the operation is completed.

- The following command will create an image of partition 2-1 named arc.tib in the shared folder \\server1\folder:

```
trueimagecmd /create /partition:2-1 /filename:\\server1\folder\arc.tib
/net_user:user1 /net_password:pw1 /log:\\server2\dir\log1.log
/log_net_user:user2 /log_net_password:pw2
```

  The operation log file log1.log will be saved on another share \\server2\dir\. Credentials for both shares are provided.

- The following command will create an image of partition 2-1 in the archive.tib file located on the FTP server:

```
trueimagecmd /create /partition:2-1 /filename:ftp://server/folder/archive.tib
/ftp_user:usr1 /ftp_password:pswd1
```

1.1.4.2 Restore disks and partitions

- The following command will restore partition 2-1 from image 1.tib to the original location:

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1
```

- The following command will restore hard disk 2 from image 1.tib, protected with password 'qwerty', to the original hard disk:

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /password:qwerty
/harddisk:2
```

- The following command will restore partition 2-1, stored in image 1.tib, to partition 1-1:

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1
/target_partition:1-1
```

- The following command will restore partition 2-1, stored in image 1.tib, to hard disk 3:

```
trueimagecmd /deploy /filename:"C:\Test\1.tib" /partition:2-1
/target_harddisk:3 /start:63 /size:64000 /type:logical
```

  A new logical partition will be created on disk 3 starting from sector 63. The partition will occupy about 64000 sectors—the exact size will depend on disk geometry and the type of the file system.

- The following command will restore partition 1-1, stored in image Server30Cdrive.tib, protected with password '123qwe', to partition 2-1. The restored partition will be of the active type:

```
trueimagecmd /deploy /filename:z:\Server30Cdrive.tib /partition:1-1
/target_partition:2-1 /type:active /password:123qwe
```

- The following command will restore the MBR from the image of hard disk 1 to the same hard disk 1. The image is contained in the 3rd backup created in archive number 2, located in Acronis Secure Zone that is protected with password 'pswd':

```
trueimagecmd /deploy_mbr /harddisk:1 /asz:2 /index:3 /password:pswd
```

- The following command will restore the MBR from the image of hard disk 1 to hard disk 2. The image is contained in the arc.tib file located on the FTP server:

```
trueimagecmd /deploy_mbr /harddisk:1 /target_harddisk:2
/filename:ftp://server/folder/arc.tib /ftp_user:fuser
/ftp_password:fpswd
```

1.1.4.3 Back up files

- The following command will back up files from the MyProject folder residing in D:\Workarea, except for files in the Old subfolder and hidden files, to the Myproject.tib file and save this file in the E:\Backups folder:

```
trueimagecmd /filebackup /filename:E:\Backups\Myproject.tib
/include:D:\Workarea\MyProject /exclude_names: D:\Workarea\MyProject\Old
/exclude_hidden
```

1.1.4.4 Restore files

- The following command will restore all files from E:\Backups\Myproject.tib to the original folder and assign the files the original date and time:

```
trueimagecmd /filerestore /filename:E:\Backups\Myproject.tib
/original_date
```

Since the /overwrite option is not specified, the latest file modifications will be replaced with the original ones.

1.1.4.5 Consolidate backups

- The following command will display the numbered list of backups, contained in the archive Kons.tib residing on the network share \\smbsrv\Archives\:

```
trueimagecmd /pit_info /filename:\\smbsrv\Archives\Kons.tib
```

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /pit_info
/filename:\\srv\elenel\kons.tib
Pit number: 1
   type: image; kind: base; date: 6/27/2009 11:39:10 AM
Pit number: 2
   type: image; kind: incremental; date: 6/27/2009 11:43:13 AM
Pit number: 3
   type: image; kind: incremental; date: 6/27/2009 11:44:04 AM
Pit number: 4
   type: image; kind: incremental; date: 6/27/2009 11:48:22 AM
Pit number: 5
   type: image; kind: incremental; date: 6/27/2009 11:50:32 AM

Operation has succeeded.
```

- The following command will create on disk D: an archive consisting of three files Kons_new.tib, (pit 2 of the archive \\smbsrv\Archives\Kons.tib, former \\smbsrv\Archives\Kons2.tib) Kons_new2.tib (pit 4, former \\smbsrv\Archives\Kons4.tib) and Kons_new3.tib (pit 5, former \\smbsrv\Archives\Kons5.tib):

```
trueimagecmd /consolidate /filename:\\smbsrv\Archives\Kons.tib
/target_filename:D:\Kons_new.tib /include_pits:2,4,5
```

1.1.4.6 Export backups

- The following command will export 3 backups (pits) from the archive (Archive 1) located in *D:\Backups* to the new archive (Archive 2) on the FTP server (Server22/Vault3):

```
trueimagecmd /export /vault:D:\Backups /arc:"Archive 1" /include_pits:2,4,5
/target_vault:ftp://Server22/Vault3 /target_arc:"Archive 2"
/ftp_user:"user" /ftp_password:"password" /progress:on
```

- The following command will export 2 backups (pits) from the archive (Archive 1) located in managed vault "Vault1" to the new archive (Archive 2) on the network share (Server15\Backups):

```
trueimagecmd /export /vault:bsp://StorageNode/Vault1 /arc:"Archive 1"
/include_pits:2,3
/net_src_user:"user" /net_src_password:"password"
/target_vault:\\Server15\Backups\
/target_arc:"Archive 2" /net_user:"user" /net_password:"password" /progress:on
```

1.1.4.7 Convert an image to virtual disk

- The following command will convert images of disks 1 and 3, contained in the file C:\MyBackup.tib, to the virtual disks C:\MyHDD.vmdk and C:\MyHDD2.vmdk for using with VMware type virtual machines:

```
trueimagecmd /convert /filename:C:\MyBackup.tib
/target_filename:C:\MyHDD.vmdk /vm_type:vmware /harddisk:1,3
```

1.1.4.8 List

- The following command will list available partitions:

```
trueimagecmd /list
```

- The following command will list contents of the latest image located in Acronis Secure Zone:

```
trueimagecmd /list /asz
```

- The following command will list contents of the specified image:

```
trueimagecmd /list /filename:"C:\My Folder\Backup.tib"
```

- The following command will list all archives and their UUID's in the specified location:

```
trueimagecmd /list /vault:D:Backups
```

- The following command will list all backups of the specified archive:

```
trueimagecmd /list /vault:D:Backups /arc:"Archive 1"
```

1.1.4.9 Check for assigned licenses

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

```
trueimagecmd /ls_check
```

The result is a list of used licenses for the local machine in the following format:

```
SKU | (trial)/empty | valid/invalid
```

The empty "trial" field means that a standard license is assigned to this machine.

Example:

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

1.1.4.10 Acronis Secure Zone: managing backups by archive numbers

- The following command will list the Acronis Secure Zone size, free space and contents:

```
trueimagecmd /asz_content
```

Assume that the contents of Acronis Secure Zone are as follows:

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /asz_content
ASZ size: 34.439 GB
ASZ free space: 34.409 GB
ARCHIVE number: 1
         index: 1; type: file, base; creation time: 4/2/2009 3:52 PM
ARCHIVE number: 2
         index: 1; type: file, base; creation time: 4/2/2009 4:04 PM
         index: 2; type: file, incremental; creation time: 4/4/2009 6:31 PM
         index: 3; type: file, incremental; creation time: 4/4/2009 6:32 PM
```

In our example, the Acronis Secure Zone contains two archives. The older archive #1 consists of one full (base) file-level backup created on **4/2/2009 at 3:52**. The second archive contains a base file-level backup with two increments. You can restore data from any backup as follows:

```
trueimagecmd /filerestore /asz:2 /index:2 /target_folder:e:
```

This will restore files and folders from the backup created on **4/4/2009 at 6:31 PM** with their original paths to the root of partition E.

```
trueimage /list /filename:asz://2 /index:3 /password:aszpw
```

which is equal to:

```
trueimagecmd /list /asz:2 /index:3 /password:aszpw
```

This will list content of the 3rd backup created in archive number 2, located in Acronis Secure Zone that is protected with password 'aszpw'.

1.1.4.11 Acronis Secure Zone: managing backups by file names

- The following command will list the Acronis Secure Zone size, free space and contents using generated filenames:

  ```
  trueimagecmd /asz_files /password:aszpw
  ```

Assume that the contents of Acronis Secure Zone are as follows:

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /asz_files
/password: aaa
ASZ size: 5.387 GB
ASZ free space: 4.363 GB
FILE name: AAA2.TIB; size: 56414317 byte
     type: image, base; creation time: 2/16/2009 3:43:34 PM
     type: image, incremental; creation time: 4/25/2009 11:44:47 AM
FILE name: FAAA.TIB; size: 3125550 byte
     type: file, base; creation time: 8/22/2009 12:28:40 PM
FILE name: FAAB2.TIB; size: 5147 byte
     type: file, base; creation time: 8/14/2009 2:17:45 PM
     type: file, incremental; creation time: 8/15/2009 2:19:43 AM
```

In our example, the Acronis Secure Zone contains three archives.

Archive AAA2 (2 stands for the number of backups in the archive) consists of:

- full (base) image backup created on **2/16/2009 at 3:43**
- incremental backup created on **4/25/2009 at 11:44**.

Archive FAAA (F means that this is a file-level archive) contains one base file-level backup.

Archive FAAB2 (B means that this is the second file-level archive in the zone) consists of:

- full (base) file-level backup created on **8/14/2009 at 2:17**
- incremental backup created on **8/15/2009 at 2:19**.

  ```
  trueimagecmd /filerestore /filename:asz://FAAA /target_folder:e:
  /password:aszpw
  ```

This will restore files and folders with their original paths from the sole base backup FAAA to the root of partition E.

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /filerestore
/filename:asz://FAAA /target_folder:e: /password:aaa
[########################################] 100%

Operation has succeeded.
```

1.1.4.12 Acronis Secure Zone: deleting backups

- The following command will delete the most recent backup in the FAAB archive:

```
trueimagecmd /asz_delete_files /password:aszpw /filename:FAAB.tib
```

Assume, the contents of Acronis Secure Zone are as follows:

```
C:\Program Files\Acronis\BackupAndRecovery>trueimagecmd /asz_files
/password: aaa
ASZ size: 5.387 GB
ASZ free space: 4.363 GB
FILE name: AAA2.TIB; size: 56414317 byte
     type: image, base; creation time: 2/16/2009 3:43:34 PM
     type: image, incremental; creation time: 4/25/2009 11:44:47 AM
FILE name: FAAA.TIB; size: 3125550 byte
     type: file, base; creation time: 8/22/2009 12:28:40 PM
FILE name: FAAB2.TIB; size: 5147 byte
     type: file, base; creation time: 8/14/2009 2:17:45 PM
     type: file, incremental; creation time: 8/15/2009 2:19:43 AM
```

The above command will delete the incremental backup created on 8/15/2009 at 2:19.

The next execution of the same command will delete the base FAAB backup. By continuing with the FAAA and AAA names, you can clear the Acronis Secure Zone except for the last remaining base backup that cannot be deleted.

1.1.4.13 Clone

- The following command will clone hard disk 2 to hard disk 3:

```
trueimagecmd /clone /harddisk:2 /target_harddisk:3
```

1.1.4.14 Explore image

- The following command will connect all images, stored in file mybackup.tib on the network drive, as virtual drives:

```
trueimagecmd /explore /filename:\\myserver\backup\mybackup.tib
/net_user:john /net_password:qwerty
```

1.2 Storage node command-line utility

The **StorageNodeCmd** command-line utility provides tools to view and export the archives stored in centralized managed vaults, and to import archives to such vaults.

This utility runs only on a machine where a storage node is installed, and works only with the centralized vaults managed by that storage node—called the *local* storage node in this section.

Unlike the **trueimagecmd** utility, which provides similar functionality, the **StorageNodeCmd** utility does not require the agent to be installed on the machine.

1.2.1 Supported commands

The **StorageNodeCmd** utility has the following format:

```
StorageNodeCmd /command /option1 /option2 ...
```

Commands may be accompanied with options.

Command	Mandatory options	Other options
list Lists the contents of a centralized managed vault or of an archive stored in it	**/vault:***Managed_Vault*	Either **/arc:***Archive_Name* or **/arc id:***Archive_UUID* **/password:***Password* **/credentials:***User_Name***:***Password*
export Exports an archive (or one or more backups stored in it) from a centralized managed vault to a local or network folder	**/vault:***Managed_Vault* Either **/arc:***Archive_Name* or **/arc id:***Archive_UUID* **/target_vault:***Folder_Name*	**/include_pits:***Backup_Numbers_List* **/password:***Password* **/credentials:***User_Name***:***Password* **/target_arc:***Archive_Name* **/target_credentials:***User_Name***:***Password* **/progress:**{**on**|**off**} **/log:***Log_File_Name* **/log_net_user:***User_Name* **/log_net_password:***Password*
import Imports an archive from a local or network folder to a centralized managed vault	**/vault:***Folder_Name* Either **/arc:***Archive_Name* or **/arc id:***Archive_UUID* **/target_vault:***Managed_Vault*	**/password:***Password* **/credentials:***User_Name***:***Password* **/target_credentials:***User_Name***:***Password* **/progress:**{**on**|**off**} **/log:***Log_File_Name* **/log_net_user:***User_Name* **/log_net_password:***Password*
help Shows usage information	None	None

1.2.2 Options

This section lists the options used by the **StorageNodeCmd** command-line utility.

1.2.2.1 arc and arc_id

The **arc** option specifies the name of the archive—for example: **/arc:"My Archive"**

If the vault contains more than one archive with this name, the utility uses the first such archive it finds—not necessarily the oldest or newest one. When there are several archives with the same name, consider using the **arc_id** option instead.

The **arc_id** option specifies the Universally Unique Identifier (UUID) of the archive—for example: **/arc_id:183DE307-BC97-45CE-9AF7-60945A568BE8**

To view the UUIDs of the archives stored in a managed vault, use the **list** command—for example:

```
StorageNodeCmd /list /vault:"bsp://My Storage Node/MyVault"
```

Specify only one of these options. If both are specified, the **arc_id** option is used.

1.2.2.2 credentials

Specifies the user name and password to access the location (a managed vault or a folder) whose name is given by the **vault** option—for example: **/credentials:"MyDomain\User A":"My PassWd123"**

1.2.2.3 include_pits

For the archive whose name is given by the **arc** or **arc_id** option, specifies the list of backups (sometimes called pits) that you want to export—for example: **/include_pits:0,4,5**

The number **0** identifies the newest backup in the archive.

Use commas to separate the backup numbers. To view the list of backup numbers for an archive, use the **list** command—for example:

```
StorageNodeCmd /list /arc:"My Archive" /vault:"bsp://My Node/My Vault"
```

Without this option, the utility exports the entire archive.

For details on how backups are exported, see the "Exporting archives and backups" section in the User's Guide.

1.2.2.4 log

Specifies the name of the file where to save the log of the current operation—for example: **/log:"\\Server\Share\Exporting Log.txt"**

If you want to create the file on a network share, use the **log_net_user** and **log_net_password** options to specify access credentials to it.

Without the **log** option, the log is not created.

1.2.2.5 log_net_password

Specifies the password for the user whose name is given by the **log_net_user** option—for example: **/log_net_password:"My PassWd123"**

1.2.2.6 log_net_user

Specifies access credentials to the file whose name is given by **log**—for example: **/log_net_user:"User A"**

1.2.2.7 password

Specifies the password for a password-protected archive whose name is given by **arc** or **arc_id**—for example: **/password:"My PassWd123"**

This option is ignored if the archive is not password-protected.

1.2.2.8 progress

Specifies whether to show (**/progress:on**) or hide (**/progress:off**) the progress of an exporting or importing operation.

Without this option, the progress is shown.

1.2.2.9 target_arc

Specifies the name of the exported archive—for example: **/target_arc:"Exported Archive"**

Without this option, the exported archive will have the same name as the original archive.

1.2.2.10 target_credentials

Specifies the user name and password to access the location (a managed vault or a folder) whose name is given by the **target_vault** option—for example: **/target_credentials:"MyDomain\User A":"My PassWd123"**

1.2.2.11 target_vault

When used with the **export** command, specifies the local or network folder where you want to export the archive—for example: **/target_vault:\\Server\Share**

When used with the **import** command, specifies the centralized managed vault where you want to place the imported archive. The vault has to be managed by the local storage node. The vault name is given as a Uniform Resource Identifier (URI)—for example: **/target_vault:"bsp://My Storage Node/MyVault"**

1.2.2.12 vault

When used with the **list** command, specifies the centralized managed vault whose archives (or the contents of an individual archive) you want to list.

When used with the **export** command, specifies the centralized managed vault that contains the archive to export.

In either of these cases, the vault has to be managed by the local storage node. The vault name is given as a Uniform Resource Identifier (URI)—for example: **/vault:"bsp://My Storage Node/MyVault"**

When used with the **import** command, specifies the local or network folder that contains the archive to import—for example: **/vault:\\Server\Share**

1.2.3 Examples

These examples assume the following:

- You are running the **StorageNodeCmd** utility on a machine where a storage node is installed.
- The name of the storage node is **My Node**.
- The storage node manages a centralized vault whose name is **My Vault**.

Listing the vault's archives

The following command shows the list of archives that are stored in the vault.

```
StorageNodeCmd /list /vault:"bsp://My Node/My Vault"
```

The output will look similar to this:

```
Archive name: My Archive

type: image; owner: domain/sample_user; machine: sample-comp; date: 6/27/2009
11:39:10 AM; used_space: 1000000000; id: 183DE307-BC97-45CE-9AF7-60945A568BE8

Archive name: My new Archive

type: file; owner: domain/sample_user; machine: sample-comp; date: 6/27/2009
11:50:10 AM; used_space: 2000000000; id: 283DE307-BC97-45CE-9AF7-60945A568BE8

Archive name: The last Archive

type: image; owner: domain/sample_user; machine: sample-comp; date: 6/29/2009
11:20:10 AM; used_space: 3000000000; id: 383DE307-BC97-45CE-9AF7-60945A568BE8
```

Listing the backups of an archive

The following command shows the list of backups that are contained in the **My Archive** archive. The archive is specified here by its Universally Unique Identifier (UUID) instead of its name—see the output in the previous example.

```
StorageNodeCmd /list /vault:"bsp://My Node/My Vault" /arc_id:183DE307-BC97-
45CE-9AF7-60945A568BE8
```

The output will look similar to this:

```
Pit number: 1

type: image; kind: full; date: 6/27/2009 11:39:10 AM

Pit number: 2

type: image; kind: incremental; date: 6/27/2009 11:43:13 AM

Pit number: 5

type: image; kind: incremental; date: 6/28/2009 11:12:19 AM
```

The pit number identifies a backup within the archive. By using pit numbers, you can export individual backups of an archive instead of exporting it as a whole.

Exporting an archive

The following command exports the **My Archive** archive to the **C:\Archives** folder.

```
StorageNodeCmd /export /vault:"bsp://My Node/My Vault" /arc:"My Archive"
/target_vault:"C:\Archives"
```

Exporting the newest backup of an archive

The following command exports the newest backup of the **My Archive** archive. Such backup is identified by the pit number **0** in addition to its own pit number. The exported backup is saved in the **C:\Archives** folder in the **Exported Archive** archive.

```
StorageNodeCmd /export /vault:"bsp://My Node/My Vault" /arc:"My Archive"
/include_pits:0 /target_vault:"C:\Archives" /target_arc:"Exported Archive"
```

Importing an archive

The following command imports the **Archive 1** archive from the **C:\Archives** folder to the vault.

```
StorageNodeCmd /import /vault:"C:\Archives" /arc:"Archive 1"
/target_vault:"bsp://My Node/My Vault"
```

1.2.4 Exporting vaults and importing multiple archives

To export all archives stored in a managed vault or to import all archives from a folder to a managed vault, you can use the scripts that are provided with Acronis Backup & Recovery 10 Storage Node.

The scripts are located in the folder where the storage node is installed—by default, C:\Program Files\Acronis\StorageNode.

Password-protected archives will be skipped during export or import.

To export all archives from a managed vault to a folder

1. Go to the folder containing the scripts.
2. Run the **VaultExport.js** script as follows, specifying the vault whose archives you want to export, and the local or network folder where to export them to:

```
cscript.exe VaultExport.js /source_vault:"bsp://My Node/My Vault"
/target_vault:"C:\Archives"
```

To import all archives from a folder to a managed vault

1. Go to the folder containing the scripts.
2. Run the **VaultImport.js** script as follows, specifying the local or network folder from which you want to import the archives, and the managed vault where to import them to:

```
cscript.exe VaultImport.js /source_folder:"C:\Archives" /target_vault:"bsp://My
Node/My Vault"
```

Script options

The options of the **VaultExport.js** script are: **source_vault**, **source_credentials**, **target_vault**, and **target_credentials**.

The options of the **VaultImport.js** script are: **source_folder**, **source_credentials**, **target_vault**, and **target_credentials**.

For either script, these options are equivalent respectively to the **vault**, **credentials**, **target_vault**, and **target_credentials** options of the **StorageNodeCmd** utility.

1.3 Scripting

Scripting is intended only for backup.

1.3.1 Script execution parameters

Scripts are executed by the **TrueImageTerminal.exe** utility located in the Acronis Backup & Recovery 10 installation folder (i.e. C:\Program Files\Acronis\BackupAndRecovery). This utility is also used to monitor backup progress.

TrueImageTerminal execution parameters:

```
TrueImageTerminal.exe [arguments]
```

Arguments include the following:

/help – outputs help information about TrueImageTerminal.exe parameters.

/progress – outputs the progress of backup operations run either from Acronis Backup & Recovery 10 graphics user interface, or from the script.

/execute: [script file name] – executes a script. If there are several scripts to be executed, they are queued. An example for executing MyBackup.tis script:

```
TrueImageTerminal.exe /execute:C:\MyBackup.tis
```

/nowait – an optional script execution argument. Enables to terminate TrueImageTerminal before backup is finished. Example:

```
TrueImageTerminal /execute:C:\MyBackup.tis /nowait
```

*By pressing **Ctrl+C** you can forcibly turn off backup progress output and switch TrueImageTerminal to a background operation.*

*You can terminate the backup operation executed by TrueImageTerminal by pressing **Ctrl+B**.*

1.3.2 Script structure

Scripts are written in the XML language and you can use the following tags:

- Source (p. 34)
- Target (p. 34)
- Options (p. 34)

1.3.2.1 Source

Specifies the partitions or disks to be imaged. Letters assigned to partitions must be used without a colon. Disk numbers correspond to their system numbers. To create images of several partitions or disks, use the SOURCE tag for each of them, e.g.:

```
<source letter =”C” />
<source letter =”D” />
<source disk =”1” />
<source disk =”2” />
```

1.3.2.2 Target

Specifies the name and the location of an image file, e.g.:

```
<target file=“E:\Mybackup2.tib” username=”username” password=”password” />
```

username and **password** parameters are optional. They are used to access networked resources.

As a target for the image files you can indicate a CD-R/RW or tape drive.

1.3.2.3 Options

This tag can be used with a number of additional parameters:

Compression

specifies the backup compression level. Can be **None, Normal, High, Maximum**.

Incremental

specifies whether you need to create an incremental image file. If equal to ”false” (or “0”), a complete image file will be created. If there is already a file with the specified name, it will be replaced without warnings. If equal to “true” (or “1”) and there is already a file with the specified name, an incremental image will be created. Otherwise the program will create a complete image file. The default value for this parameter is “true”.

Description

adds a description to an image file. The comment must be a single string (though its length is not limited.)

Split

splits a large image file into a number of smaller files of the specified size, which can be provided in bytes, kilobytes, megabytes, etc.

Password

adds password protection to an image file.

1.3.3 Script usage examples

The following example illustrates the usage of a script to back up two partitions (logical drives), C and F. **mybackup2.tib** is specified as an incremental image file. High compression level is selected and the image will be split into 650-MB parts for recording to CD-R/RW media. Password protection will also be added. The entire script must be located between the **<backup>** and **</backup>** tags.

```
<? xml version="1.0" encoding="utf-8" ?>
<backup>
<source letter ="c" />
<source letter ="f" />
<target file="e:\mybackup2.tib" />
<options compression="high" incremental="true" description="this is my backup"
 split="650 Mb" password="" />
</backup>
```

The script for backing up to tape (tapeN specifies the tape numbers):

```
<? xml version="1.0" encoding="utf-8" ?>
<backup>
<source letter =”c” />
<source letter ="f" />
<target cdrw="\taperecorder\\\.\tape0|||” />
<target cdrw="\taperecorder\\\.\tape1|||” />
<options compression="high" incremental="true"
 description="this is my backup" />
</backup>
```

2 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.

2.1 Backup, restore and other operations (trueimagecmd)

2.1.1 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		

2.1.2 Common options

2.1.2.1 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
```

2.1.2.2 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. 9) 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.

2.1.2.3 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.

2.1.3 Specific options

2.1.3.1 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.

2.1.3.2 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.

2.1.3.3 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.

2.1.3.4 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.

2.1.3.5 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.

2.1.3.6 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. 47) option.

no_subdir

This option is used together with the **/folder_name** (p. 18) 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.

2.1.3.7 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.

2.1.3.8 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.

2.1.3.9 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.

2.1.3.10 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.

2.1.3.11 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.

2.1.3.12 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.

2.1.4 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
```

2.2 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.

2.3 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]
```

2.3.1 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.

2.3.2 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
```