Kaseya 2

Backup

User Guide

Version 7.0

English

September 3, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Backup Overview

Backup

Backup (KBU) provides real-time automated disk backup, disk imaging, file level backup and bare-metal restore for Windows servers and workstations.

Automation, superior performance, ease of use and security are the cornerstone features of **Backup**. Unlike conventional file-based back-up products, **Backup** creates an image of the entire system state, including operating system, user settings, applications and data. Applications and servers are always available since the backup process does not require system downtime.

Once a backup is created, **Offsite Replication** *(page 7)* ensures that image and folder backups are immediately and automatically transferred and stored safely away from the business location. This process is completely automated and eliminates the need for a person to remember to take backup media, such as tapes, home or drop them off at a location for storage.

Data can be recovered quickly and easily with **Backup**. Whether it is a simple need to recover a few files, restore a system from a crash or recover systems from bare-metal in the event of a disaster, **Backup** provides IT Managed Service Providers and IT users with the most comprehensive, reliable, and cost effective server and workstation protection.

Fully Automated Real-Time Backup

- No user intervention required
- No system downtime required
- Schedule full and incremental imaging
- Schedule folder and file backups
- All processes are automated and occur when scheduled

Complete Disk Imaging

- Sector level backup
- Multiple partitions
- Full and incremental images provides for granular restoration points and reduced file size transfer for offsite replication
- Complete data protection of all programs, settings, configuration, system and user data

Fully Automated Offsite Replication

- Scheduled time periods
- Occurs automatically without user intervention
- No downtime required
- No tapes or other media to transport
- Synthetic backups on offsite servers
- Supports synthetic encrypted backups of folder and files.

Fast and Easy Recovery

- Granular date selection for recovery
- Remotely mount drive volumes
- Complete system image restoration
- Drag and drop restoration of folders and files
- Bare-metal image restoration
- Minimizes downtime

Flexible Configuration and Control

- Configure globally, by group, OS type, etc.
- Granular by server or workstation
- Scheduled and unattended backup and file restoration
- Remote and automated deployment
- No need to physically visit the server or workstation or customer site
- No additional hardware or software is required

Note: *See* **System Requirements** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm).*

Functions	Description
Backup Status	Displays the status of scheduled backups for any machine.
Schedule Volumes	Schedules backups for selected hard disk volumes on any managed machine.
Pre/Post Procedure	Specifies a procedure to run before and/or after Volume Backup
Schedule Folders	Schedules backups for individual folders.
Backup Sets	Displays a list of the current backup sets you have stored, for both volumes and folders.
Backup Logs	Displays the logs generated by every backup action.
Explore Volumes	Mounts a backup as a new drive letter on the managed machine.
Explore Folders	Copies the folder backup to the managed machine.
Verify Images	Verifies any volume or folder backup image.
Image to VM	Converts an existing backup file to one of three types of virtual machine file formats: Virtual PC, VMware and ESX
Auto Recovery	Selects a volume backup image to automatically restore to a selected machine. Requires the machine can still boot and the agent can communicate with the server.
CD Recovery	Boots the managed machine from a CD and then automatically restore a selected volume backup image.
Universal Restore	Provides instructions for creating a boot CD and restoring a backup image manually by walking through a wizard.
Offsite Servers	Specifies a machine to act as an offsite server and receive files from a local server.
Local Servers	Specifies a machine to act as a local server and send files to an offsite server.
Offsite Alert	Generates alerts when a local server fails to connect to an offsite server.
Schedule Transfer	Sets up a day by day schedule for each local server to push files to an offsite server.
Install/Remove	Installs and uninstall the backup driver and software on any managed machine.
Image Location	Sets the path to the backup storage location.
Image Password	Lists the passwords used to protect backup images and enables image encryption.
Folder Backup	Specifies a list of folders to backup during Schedule Folders.

Backup Alert	Activates/deactivates alerts associated with backup events.
Compression	Sets compression level used by both volume and folder backups.
Max File Size	Sets a maximum file size used for backup images. Images larger than this maximum are broken into multiple files.
Max Log Age	Sets the maximum number of days to save backup log data.
Secure Zone	Installs a secure zone to support Auto Recovery.

Backup Module Requirements

Kaseya Server

- The Backup 7.0 module requires VSA 7.0.

Requirements for Each Managed Machine

- 512 MB of RAM
- 2.3 GB of free disk space
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1

Note: See general **System Requirements** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/reqs/index.asp#home.htm).*

Uninstalling Other Backup Products

If other backup products are installed on a managed machine, this may cause problems with **Backup**. Uninstall other backup products before backing up volumes and folders using **Backup**. A warning message displays on the Backup Status page if other backup products are installed.

Volume Backups vs Folder Backups

When you perform a backup using Schedule Folders, only the data, along with the folder tree, is compressed and stored.

Backing up disks and partitions is performed in a different way: **Schedule Volumes** stores a sector-by-sector snapshot of the disk, which includes the operating system, registry, drivers, software applications and data files, as well as system areas hidden from the user. This procedure is called **creating a disk image**, and the resulting backup archive is often called a disk/partition image.

Only those hard disk parts that contain data are stored. Further, it does not back up swap file information. This reduces image size and speeds up image creation and restoration.

Partition Backups

You can backup individual drive letters (partitions) or entire disk drives.

A partition image includes all files and folders independent of their attributes (including hidden and system files), boot record, FAT (file allocation table), root and the zero track of the hard disk with master boot record (MBR).

A disk image includes images of all disk partitions as well as the zero track with master boot record (MBR). To **ensure recovery from complete disk failure**, you should backup entire disk drives. Only by backing up entire disks **will you capture hidden recovery partitions** that may have been installed by your PC system vendor.

> **Note:** Only 1 disk/partition can be restored at a time.

Full Backups, Incremental and Differential Backups

Full backups take significant time to complete compared with incremental or differential backups. To save time and disk space, schedule full backups to run less frequently than incremental or differential backups. Typically full backups are scheduled once per week or once per month, while incremental or differential backups run daily. All files required for a full backup, including all incremental or differential backups, are saved together in a backup set. You may save any number of full backup sets you wish.

Verification of Backups

Verification spot checks that backups are completed and can be used to restore from successfully. Verification does *not* involve comparing the backup to the original source files, so any other machine with an agent can be used to perform the verification of the backup file so long as the machine has read access to the image location. Successful backups may fail to verify if the backup image file was not copied successfully to the Image Location path. This problem typically only occurs in slow or unreliable networks. On slow networks, consider selecting the **Verify Backup** option in Schedule Volumes and Schedule Folders to verify the backup every time.

Hidden Preferences

Alt+clicking the Synthetic Full backup  icon *in the header panel* of Schedule Volumes or Schedule Folders displays five tabs of preferences that can be applied individually to each machine.

Synthetic Full tab

- **When performing synthetic full backups -** If **synthetic full backups** *(page 9)* are being used on a KBU managed machine and the Image Location or Offsite Servers' local directory is a UNC path, such as `\\server\share`, *then* `Copy the Files Locally First` *is enabled by default instead of* `Access the Network Directly`. To use this robust consolidation option effectively, appropriate hard disk space is required on the managed machine. See the Kaseya **knowledge base** *(https://helpdesk.kaseya.com/entries/35940987)* for more information.

- **Run synthetic full backups <N> time(s) until successful** - Sets the **Synthetic Full Attempts** count for synthetic full backups.
- **Retry after <N> days(s)** - Sets the **Retry after (days)** count.

Installer tab

- **Max Number of Concurrent Downloads** - Sets the maximum number of concurrent downloads.

Offsite Replication tab

- **Verification method used to check Offsite data integrity** - Selects the verification method used to check offsite data integrity.
  - `Quickest File Verification using File Size and Last Modified Time`
  - `Quick File Verification with SHA-1 Hash for Partial Files only`
  - `File Verification with SHA-1 Hash for Partial Files and Complete Files`

Diagnostics tab

- **Run AcronisInfo on selected machines** - Runs *AcronisInfo* on selected machines. *AcronisInfo* is a utility that automatically gathers User Rights Assignment list, Windows Event Log, Msinfo32, Acronis registry keys, Acronis logs, Acronis Scheduler report, Acronis Disks Report and list of user's Active Directory groups. This information is placed inside a `AcronisInfo.zip` file. The `AcronisInfo.zip` file can then be downloaded from a link that displays in the **Acronis Link Info** column of selected machines.

> **Note:** Creating the `AcronisInfo.zip` file displays progress bars and other programs on the user's desktop momentarily. You may wish to get the user's approval before running this process.

Backup Options tab

- **Use multivolume snapshot option** - This option applies only to machines with VSS for Volume Backup and only to the Schedule Volumes page. If checked, snapshots of all volumes being backed up are created simultaneously. Use this option to create a time-consistent backup of data spanning multiple volumes, for instance, database files. If unchecked, volume snapshots are taken one after the other. Backups of data spanning several volumes may not consistent.

Dynamic Disks

Dynamic storage involves dividing a physical disk into multiple volumes or combining a physical disk with other physical disks to form volumes that are greater in size than any one physical disk. A traditional disk volume is called a "basic" disk volume. **Backup** supports the following basic and dynamic backup and restore combinations:

- backup basic disks
- backup dynamic disks
- restore basic volumes to basic disks
- restore basic volumes to dynamic disks
- restore dynamic volumes to basic disks
- restore dynamic volumes to dynamic disks

> **Note:** While Universal Restore supports restoration of dynamic disks to similar hardware, it does not support restoration of dynamics disks to different hardware platforms that require new drivers. To restore to different hardware platforms, you must restore the dynamic disk backup to a basic disk.

Disk-Based Backups of Dynamic and GPT Disks

Backup clients ABR10 and ABR11 support disk-based backups of Dynamic and GPT disks. Previous to ABR10, only **partition-based backups** *(page 4)* were supported for these types of disks. Restoring disk-based backups of Dynamic and GPT disks requires Universal Restore. AutoRecovery and CD Recovery of Dynamic and GPT Disks are not supported. ABR11 also supports EFI-based systems, where Windows is installed on a GPT volume (partition style is GPT).

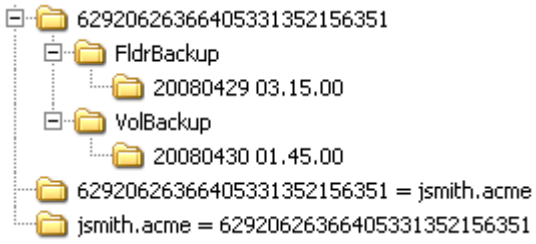
> **Note:** Acronis clients prior to ABR11 do not support EFI-based systems. If Windows is installed on a GPT volume, the restored system will only be boot-able if it is backed up and restored using ABR11. For more information, see the Acronis **KB article** *(http://kb.acronis.com/content/5684)*.

Backup Folder Structure

Separate Image Location paths may be specified for volume and folder backups. Volume backups and folder backups are saved as full backup sets. Each backup set gets its own folder. Backup files have a `*.tib` extension.

Backup folders are organized by the GUID used to uniquely identify each machine ID. By using the GUID instead of the machine ID, renaming the machine ID or assigning the machine ID to a different group does not cause the backup to become unavailable.

Two extra, empty, folders in the same backup image location folder identify the machine ID associated with each GUID. For instance, if you have a machine ID named `jsmith.acme` and its GUID is `629206263664053313521563 51` then folders might be organized as follows in the image location folder:



The first folder contains the backups. The second empty folder identifies the machine ID for a GUID. The third empty folder identifies the GUID for a machine ID. If you have backups for many machine IDs all stored in the same image location folder, you can use either of the two empty cross-reference folders to identify the appropriate GUID backup folder, either by machine ID or by GUID.

Backing Up the Kaseya Server

Do not attempt to backup the Kaseya Server using **Backup** while the Kaseya Server is running, even if VSS is enabled. Doing so can cause problems when the VSA attempts to write information about the backup to a database that is being backed up. Kaseya Server data is backed up automatically each time a database maintenance cycle is run. Database maintenance cycle frequency is set using the **Run database backup / maintenance every <N> Days @ <Time>** option in System > Server Management > **Configure** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#248.htm)*. You can use Schedule Folders to backup the folder containing the Kaseya database backup files.

For maximum flexibility and resiliency when using **Backup** backups of Kaseya-related files, Kaseya recommends that you configure a **Folder Backup** to back up the following folders on your Kaseya Server in addition to any other backups that you run on the server:

```
C:\<KaseyaInstallDirectory>\UserProfiles
```

```
C:\<KaseyaInstallDirectory>\WebPages\ManagedFiles
C:\<KaseyaInstallDirectory>\WebPages\banner\default\images\new
C:\<KaseyaInstallDirectory>\WebPages\compact\default\images\new
C:\<KaseyaInstallDirectory>\WebPages\themes\default\images\new
C:\<KaseyaInstallDirectory>\WebPages\Access
```

Confirm that the **Schedule Folders** schedule does not coincide with the Kaseya database backup configured on the System > Server Management > **Configure** page, and that the folder you have configured as the backup folder on the Kaseya Server is included in folders in the **Folder Backup**.

You should not attempt to stop SQL services or Kaseya Server services while running any **Backup** backup of your Kaseya Server, as Kaseya requires write access to the SQL database in order to update the backup results.

Note: See **Kaseya Server Setup** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/install/index.asp#home.htm)*.

Kaseya Backup Local UI

A **Kaseya Backup Local UI** installs in the background on each end-point that has the backup client installed. With this version you can:

- Verify folder and volume backup.
- Mount volume backups that you wish to restore from.
- Restore all files from a folder backup.
- Convert volume backups to a virtual hard disk.

The **Kaseya Backup Local UI** is typically located:

- On 32-bit machines at `c:\Program Files\Kaseya\<VSA_ID>\Backup\KaseyaBackupLocalUI.exe`
- On 64-bit machines at `c:\Program Files (x86)\Kaseya\<VSA_ID>\Backup\KaseyaBackupLocalUI.exe`

The `<VSA_ID>` is a unique identifier that correlates to your VSA. There is also a shortcut in the Acronis folder to this path.

Offsite Replication

Offsite replication safely and securely transfers backup images from a LAN to a remote location. Offsite replication transfers all *changes* to files and sub-directories in a Local Server directory to a specified Offsite Server directory.

- File transfers are scheduled using Schedule Transfer.
- Image Location directories should be defined as subdirectories of a local server directory to be included in these transfers.
- The Offsite Alert page creates an alert when a specified local server can not connect to its offsite server.
- Offsite replication supports the use of **Synthetic Full Backups** *(page 9)*.

Offsite Server Configuration

Any machine ID may act as an offsite server. You may also have as many offsite servers as you like. Offsite server configuration examples include:

- **One global offsite server** - A local server at each managed LAN pushes data to the global offsite server.

- **Multiple offsite servers** - Several local servers are assigned to each offsite server. Multiple offsite servers are used to balance the load.
- **Cross offsite servers** - Supports offsite replication for companies with multiple locations. For example, two company sites each act as the offsite server location for the other company site.

Local Servers

The Local Servers page defines the machine ID and directory on the local LAN used to transfer all new files to an Offsite Server. Offsite replication transfers all *changes* to files and sub-directories in the local server directory to a specified offsite server directory. File transfers are scheduled using Schedule Transfer. Image Location directories should be defined as subdirectories of a **Local Server** directory to be included in these transfers.

For each local server specify:

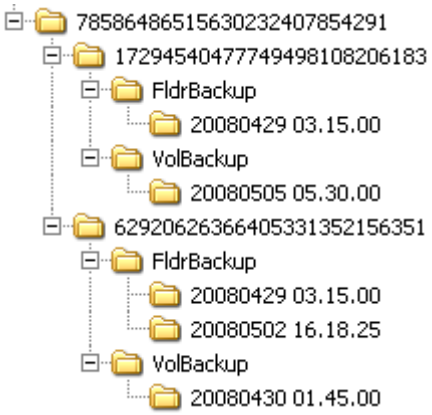
- The offsite server to push files to.
- The local directory path to push to the offsite server.
- Optional bandwidth limit.

The local server directory can be a UNC path pointing to a directory on a network file share. *Do not specify a local server directory using a mapped drive.* The local server must have a **credential** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#352.htm)* set in order to access the network.

> **Note:** Offsite replication is designed specifically for replication of backup sets created using Kaseya **Backup**. Replication of other file types or folders is *not* supported.

Offsite Folder Structure

The offsite server stores data received from local servers in the directory specified. The top level GUID folder is the GUID of the local server the data is coming from. Second level GUID folders are the GUIDs of the machine IDs being backed up. The following diagram illustrates a typical offsite server directory structure.



File Transfers

Only file changes are pushed to the offsite server. Broken file transfers are automatically restarted at the point left off. Restarting the file transfer from the beginning is not required. Offsite replication uses the same communications technology used in agent/server communications. All traffic is 256-bit encrypted.

Using the Same Machine for the Local Server and Offsite Server

You may assign the offsite server to be the same machine as the local server, but note the following:

- You'll need to open a port just to replicate across drives, whereas other replication tools can do so locally.
- The files aren't copied offsite. You'll lose the disaster recovery benefit of an offsite backup.

Setting the Name/IP Address and Port

Select a target machine with an agent that will act as the offsite server. The offsite server is always running and listens for connections from local servers using any TCP port you specify. The port cannot be used by any other application. Try using 9721 as it is similar to the agent check-in port. Offsite server ports are restricted to between 1024 and 49151.

Note: Avoid ports 9876 or 9877 if using Backup client v10.x or higher. These ports are used by Acronis Backup & Recovery components and will conflict with Offsite Replication services.

You must specify a DNS name or IP address that can be resolved from the local server. Typically, this is the *external* name/IP address of the gateway/firewall/router used by the target machine. Configure **port range forwarding** on your gateway/firewall/router to direct requests for port 9721—or whatever port number you've chosen—to the internal IP address of the machine ID acting as the offsite server.

Note: The offsite server must have a **credential** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#352.htm)* set to access the network directory receiving data transfers.

Testing the Offsite Configuration

Once you have configured the offsite server, check pending procedures on the offsite server machine:

1. Click the or or icon.
2. Click the **Live Connect** *(http://help.kaseya.com/webhelp/EN/VSA/7000000/index.asp#4796.htm)* > Agent Data > Pending Procedures tab.
3. Ensure the `Start Offsite Server` procedure ran successfully.

Try to connect to the offsite server component using Telnet. In the command below replace the string `your.offsiteServer.com` with your Name/IP address. Replace `9721` with the port number you are using.

```
telnet your.offsiteServer.com 9721
```

If the connection is successful you should only see a blinking cursor. Once you can verify the offsite server is ready, You can configure the local servers.

Synthetic Full Backups

A synthetic full backup is created by consolidating existing incremental or differential backups with the previous full backup image. This is sometimes called an 'Incremental Forever Backup'. Unlike traditional full backups, synthetic full backups are not transferred from the local server to the offsite server. Instead, after the *first* full backup is transferred, only the incremental or differential files are transferred to the offsite server. A synthetic backup component on the offsite server recreates the next full synthetic backup in parallel with the local server. This eliminates the need to transfer full backups between the local server and offsite server. With synthetic full backups, bandwidth requirements for transferring full backups are eliminated, but the offsite server's access to its own file server may need to be enhanced to handle the processing of its synthetic full backups.

If synthetic full backups are being used on a KBU managed machine and the Image Location or Offsite Servers' local directory is a UNC path, such as `\\server\share`, then **Copy the Files Locally First** is enabled by default instead of **Access the Network Directly**. To use this robust consolidation option effectively, appropriate hard disk space is required on the managed machine. For more information, see the Kaseya **knowledge base** *(https://helpdesk.kaseya.com/entries/33899557)*.

Note: See **Offsite Replication** *(page 7)*.

Configuring synthetic full backups involves the following steps:

These first three steps apply to ANY Offsite Server.

1. Install an agent on a local server. Typically the backup image locations of machine IDs being backed up point to the local server.

   > **Note:** You do not have to install the *backup client* to either a local server or an offsite server.

2. Install an agent on the offsite server.
3. Define a machine ID as an offsite server using Backup > Offsite Servers.

   These steps apply to Offsite Servers using Synthetic Full Backups.

4. Click the **Schedule Install** hyperlink on the Backup > **Offsite Servers** page for the machine ID you want to schedule synthetic support on. A dialog box displays. Schedule the installation of synthetic support components to the offsite server.
5. When using Backup > Schedule Volumes or Schedule Folders to create backups for machine IDs, ensure the **Synthetic Full** checkbox is checked. These are machine IDs that store backups on local servers that transfer backups to the offsite server you defined above.
6. Check the progress of scheduled synthetic backups using the Backup Status page. The **Offsite Server Status** and **Local Server Status** sections on this page display a **Synthetic Backups Queued** column. The columns displays counts for each machine ID with synthetic backups scheduled. Click the link to display a window showing the queue status of each synthetic full backup.

Index