



ActiveImage™ PROTECTOR

Server
SBS
Desktop
Personal
Cluster



Best practices

Content

- 1 Prepare your system for reliable backup and/or vStandby machine
- 2 Installing, Updating and Uninstalling ActiveImage Protector
- 3 Installation/uninstallation Troubleshoot
- 4 Windows BE Recovery Environment Troubleshoot
- 5 Tips for setting up ActiveImage Protector
- 6 Tips for setting up backup jobs
- 7 Tips for lost backup schedules or lost settings
- 8 Performance tuning and VSS Troubleshoot



1 Prepare your system for reliable backup and/or vStandby machine

Windows update

Make sure all Windows updates have been applied and the machine is restarted before beginning installation.

Event logs

Make sure you have no Windows event log entries with VSS, NTFS or disk warnings/errors.

RAID and hard drive

Check your source RAID volumes and hard drives using disk verification tools (i.e. S.M.A.R.T. values and others).

Backup target / Storage device

Use a disk verification tool to check your backup targets are working and error free (i.e. S.M.A.R.T. values and others).

Antivirus

After installation:

1. To use Activelmage Protector backup functionality, create an exception, or create a whitelist, for the file called "AipCopyWLH64.exe" in the real-time scanner of your Antivirus as Activelmage Protector uses this file to run backups. Depending of the OS you are running the file may have a different name such as "AipCopy...".

To use vStandby, do similar procedure for "SbyCopyWLH64.exe" file. Depending of the OS you are running the file may have a different name such as "SbyCopy...".

Note: These files can always be found in Activelmage Protector's installation folder (i.e. C:\Program Files (x86)\NetJapan\ActiveImage Protector ...).

2. Create an exception, or create a whitelist for "Scheduler.exe" and "AipService.exe" process and service in the real-time scanner of your Antivirus.
3. When using Activelmage Protector to run backups, add the following two drivers to the whitelist of your Antivirus:
C:\Windows\System32\drivers\aip2.sys - (used for mounting)
C:\Windows\System32\drivers\aiptrack.sys - (incremental tracker)

When using Activelmage Protector to create a vStandby machine, add the following two drivers to the whitelist of your Antivirus:

C:\Windows\SysWOW64\drivers\vstor2-mntapi10-shared.sys or
C:\Windows\System32\drivers\vstor2-mntapi10-shared.sys - (used for mounting)
C:\Windows\System32\drivers\abytrack.sys - (incremental tracker)

4. When using Activelmage Protector to run backups, exclude the "\$AIPMAP.CBT" file from your antivirus (or add it to its whitelist). This bitmap file is created on all disks / volumes to track changed sectors for incremental backup snapshots.

When using Activelmage Protector to create vStandby machine, exclude the "\$ABYMAP.CBT" file from your antivirus (or add it to its whitelist). This bitmap file is created on all disks / volumes to track changed sectors for incremental vStandby snapshots.

5. Make sure you have completely uninstalled and removed any previously installed VSS-based backup software. You also need to check that you do not have any applications or 3rd party VSS provider from the previous backup solution that remain even after uninstallation.

2 Installing, Updating and Uninstalling Activelmage Protector

Installation

When installing Activelmage Protector we recommend you always use the Custom installation option. Custom installation allows you to select the modules to be installed. Install at least the Activelmage Protector installer on the machine to protect. In regards to ImageBoot and ImageCenter installers, the best recommendation is to install them on a separate machine of the network, with access to the backup storage device, although it's possible to install them on as many machines as you want, included the protected machine.

To make full use of Activelmage Protector you need to install all of the modules.

Check also our [ImageBoot Best Practice](#).

Upgrade

When upgrading Activelmage Protector we recommend you use the Custom installation option. Custom installation allows you to select the modules to be installed. Check the Installation section of this guide for more information.

Uninstall

If you opt to uninstall Activelmage Protector you have the option to keep your configuration settings including backup jobs, log files and more. You will be prompted to choose which, if any settings, you would like to keep.

3 Installation/uninstallation Troubleshoot

1. If the installation succeeded but you get an error message like "...msvcp120.dll or msvcrt120.dll missing..." when you try to launch the software, it means the Microsoft Visual C++ Redistributable Packages have failed to install.
 - 1.1 Navigate to Activelmage Protector's installation folder (i.e. C:\Program Files (x86)\NetJapan\ActiveImage Protector ...) and run "vcredist_x86.exe", "vcredist_x64.exe" and "vcredist_x64_2008SP1.exe".
 - 1.2 If you get the dialog window to repair the installation, follow the wizard.
 - 1.3 If you get the dialog windows to install, run the setup normally.
 - 1.4 In most cases a system restart is required to apply the changes.

2. When facing other problems installing or uninstalling NetJapan's products, use Microsoft's PsExec tool as follows:
 - 2.1 Download PsExec (included in the PSTools Suite):
<http://technet.microsoft.com/en-us/sysinternals/bb897553>
 - 2.2 Extract PsExec.exe from the PSTools.zip file to your C:\ root drive
 - 2.3 Run cmd.exe as Administrator
 - 2.4 Execute the following command in the Run prompt:
C:\psexec.exe -i -s "C:\Windows\system32\cmd.exe"
and click on "Agree" after the Window prompt
 - 2.5 Download the latest NetJapan software from <http://download.netjapan.eu>
 - 2.6 Extract the setup files to your C:\ root drive
 - 2.7 Now use the PsExec command prompt window (that we already started) and run the specific setup file, example: C:\Setup_ActiveImage_Protector_(5.0.1.4417).exe
3. If you are unable to uninstall the software for some unknown reason (uninstaller missing), or if you have a failed installation, you can do the following:
 - 3.1 Install the 3rd party unzip tool 7-zip (freeware: <https://www.7-zip.org>).
 - 3.2 Start the 7-zip application and select the ActiveImage Protector setup file.
 - 3.3 Extract the content of the setup file into a new folder. You only need the file "uninstaller.exe".
 - 3.4 Copy the "uninstaller.exe" file and paste it into the ActiveImage Protector Installation folder (i.e. C:\Program Files (x86)\NetJapan\ActiveImage Protector ...\).
 - 3.5 Execute the newly copied uninstaller.exe application to uninstall the software.
4. **Installing and activating ActiveImage Protector on virtual environments**

Most OEM/ROK Windows licences require a modification of the virtual guest configuration in order for the virtual guest to bypass a BIOS lock or hardware lock and use this branded Windows licence. Using ActiveImage Protector Virtual licences (Virtual - Single, Virtual - Cloud, Virtual - Unlimited) require to recognise the system as a virtual environment. This can cause issues when the configuration is not properly set.

 - 4.1 VMware ESXi
 - 4.1.1 Use vSphere Client / vSphere Web Client and choose the virtual guest.
 - 4.1.1 Click on "Edit Settings" > "Virtual Machine Properties" > "Options" > "General" > "Configuration Parameters" and add the line `smbios.addHostVendor = "TRUE"` in the virtual guest configuration file, to use OEM/ROK Windows licence and the NetJapan virtual licence on the same system.

Don't use `SMBIOS.reflectHost = "TRUE"` and `SMBIOS.noOEMstrings = "TRUE"` in this scenario.
 - 4.2 Microsoft Hyper-V
No change required.

4 Windows BE Recovery Environment Troubleshoot

If you get a DISM error when creating your Windows Boot Environment:

1. Execute the following command from the command prompt as Administrator on Windows Server 2008 R2 / Windows 7 and older:
`DISM /Cleanup-Wim`
2. Execute the following command from the command prompt as Administrator on Windows Server 2012 / Windows 8 and newer:
`DISM /Cleanup-Mountpoints`
3. Check the afterwards the following registry entries:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WIMMount\Mounted Images`
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\WIMMount`
If you have old orphaned registry keys, delete them manually.
4. The system requires a reboot to apply the changes.
5. After reboot, delete the content of the following path:
`C:\Windows\Temp`
6. Run the AIPBE builder again to create your ActiveImage Protector WinPE Recovery Environment.

5 Tips for setting up ActiveImage Protector

Performance

1. Start ActiveImage Protector and go to "Preferences → General".
2. Make sure "Default Performance" is set to Fast / 100%.

Backup storage device

1. Start ActiveImage Protector and go to "Preferences → General".
2. If your backup target is located on the network tick the box "Use network write caching". If you are backing up to locally attached disks, do not tick this box.

Deduplication

1. Start ActiveImage Protector and go to "Preferences → Deduplication".
2. Make sure "Auto-switch from default to an alternative folder" and "Continue operation without (Standard) compression" are ticked.

Default temporary file folder

Note: By default ActiveImage Protector uses the Windows Temp folder (`C:\Windows\temp`) to temporarily store the deduplication table files. To speed up backup creation, or have less I/O impact on the source disks, you can move this folder to another location such as a separate disk which is not included in the backup, or on a network share, an attached SSD drive or other disk based device. The deduplication table files do not require redundancy, they only need fast drives as they are deleted after each backup job is run.

6 Tips for setting up backup jobs

Source

We recommend you back up all your drive(s).

If you only decide to backup the C: volume, you may not backup the boot partition or other important hidden system partitions.

However, if you want to exclude partitions, you can select only the volumes to backup.

Important: If you have an application server with databases and your database and/or logs are on separate disks, do NOT create a single backup job for each individual partition. Instead, create one single backup job which contains all of the partitions or entire disks together in one backup job.

Destination – Options

- We recommend you to untick the “Separate image file for each disk” box. This will give you the best result especially when using deduplication.
- By default deduplication level 2 is selected. It gives you the best compromise between backup size, backup windows and system load. To achieve the highest compression rate, choose deduplication level 1. If you want to increase backup speed, choose deduplication level 3 instead.



WARNING: Never change the deduplication level once a backup file is created! This will corrupt the backup image. If you want to change to another deduplication level, you must create a new full base backup image file.

- Image protection: setup backup password and/or encryption
 - **Password:** Simple password protection without encryption: Offers extremely low impact on the system load and backup windows, but images are only protected with a password.



WARNING: Do not lose your password. You will need it for verification, consolidation, and restore processes and our technicians will not be able to help you if you do lose your password. We do not have a master password!

- **Encryption:** we recommend you to use AES256, although additional CPU usage may be required. If you are experiencing general performance issues with your source machine, we recommend you use Common Compression which uses fast LZ4 algorithm at the expense of requiring more storage space.

Destination – Options

- Enable “Verify backup image upon completion” if you want ActiveImage Protector to verify the entire image file once the backup file is created. Verification is performed sector by sector. We recommend you to verify images after creation.

Notes:

- This process may take some time to complete
- This feature can be also used by the dedicated add-on ImageCenter with a separate image verify task. We recommend you this option.

- We do not recommend that you enable “Ignore bad sectors” by default as you will never be able to tell if the source disk(s) are faulty. This option should only be used in an emergency to create a last backup before a disk fails completely.
- If you are encountering performance issues on network shares and have already enabled the “Use network write caching” option, you may want to try enabling the “Split Image into ... MB files” option using 4096 or 8192 as the MB value.
- Enable “Create MD5 file for image” to use hash value calculation for MD5 file verification.

Schedule

- Backup execution should never start precisely on the hour, ie: begin at 06:15 and end at 20:15. This avoids conflict with a lot of daily or weekly maintenance tasks performed by different applications; they usually take place on the hour.
- If you are using another tool to create backups or make VSS dumps, make sure you never execute one of these at the same time as ActiveImage Protector is performing a backup.
- Execution priority:
 - You usually can choose use the Maximum Execution priority option for the Full (Base) backups if you have scheduled them out of working hours.
 - Keep a medium Execution priority for incremental backups, although you can adjust it to lower priority if you face performance issues.
- Post-backup Process: ImageCheck:
For an automatic image chain boot verification, use the “ImageCheck”, also called “BootCheck” feature. Click on “Unconfigured” and thich the box “Enable BootCheck”. This will require an enabled Hyper-V role or an installed Oracle VirtualBox on the machine.

Note: This feature can be also used by ImageCenter with a separate “ImageBootTest” task.

- Enable Reconcile Image:
This option is enabled by default: when ActiveImage Protector detects one or more dependent incremental files that are no longer accessible (for various reasons) it will find the last usable incremental file and create a synthetic differential calculation and inserts it as a regular incremental into the incremental chain while also removing the remaining usable incremental files. This ensure the backup job can continue.
If you untick the “Reconcile image” box: when ActiveImage Protector detects a missing incremental it will create a new base full image and start a new backup chain. This option is recommend if you are replicating your backup chain to another location, to prevent the already replicated chain to be overwritten by the repaired chain.
- Enable Retention policy:
Specify the number of image set (a set includes a full backup and its dependant incrementals) you want to keep, i.e. delete old image set to control storage space.
 - *Example 1:* If you create a new full base image every Sunday with incremental images scheduled for every 15 minutes, Monday to Friday from 06:15 to 20:15 PM, choosing 1 image set means you will only ever have one week of backups on your backup target. If you choose to retain 4 image sets, it would keep 4 weeks of backups.
 - *Example 2:* If you create a full base backup every night at 22:00, from Monday to Friday, with no incremental backups and with retention set to 5, you would keep 5 days of backups on your backup target. If you choose 15, you would keep 15 days of backups.

7 Tips for lost backup schedules or lost settings

Corrupt schedule / Task already exists message

If your backup job disappeared or if you can't create a new backup job, you will get an error message: "corrupt schedule" / "task already exists". How to solve it:

1. Navigate to ActiveImage Protector's installation folder (i.e. C:\Program Files (x86)\NetJapan\ActiveImage Protector ...\) and check the subfolders "Schedules" and "Profiles". The software stores in this folders the backup task and backup schedule as XML files.
2. You now have two possible solutions:
 - 2.1 Delete the XML files in both subfolders and restart the ActiveImage Protector service under Windows services (AipService.exe) to be able to create new backup jobs.
 - 2.2 Mount a previous image backup from the specific machine and copy & paste these XML files from the mounted image to the local path and overwrite the existing files. Restart the ActiveImage Protector service under Windows services (AipService.exe) and the backup job will be fine again.

Settings not saved or not applied

Your main configuration file may be broken. How to solve it:

1. Navigate to ActiveImage Protector's installation folder (i.e. C:\Program Files (x86)\NetJapan\ActiveImage Protector ...\). There is a file called "aip.ini" this file stores all main settings of the software.
2. You now have two possible solutions:
 - 2.1 Delete the "aip.ini" file and open the ActiveImage Protector setup file like explained at point 3 here in the document to catch a default "aip.ini" file. Overwrite this default "aip.ini" file with the local broken one and restart ActiveImage Protector service under Windows services (AipService.exe). Set your settings again.
 - 2.2 Mount a previous image backup from the specific machine and copy & paste the "aip.ini" file from the mounted image to the local path. Overwrite it.
 - 2.3 Restart the ActiveImage Protector service under Windows services (AipService.exe) and settings will be fine again.

8 Performance tuning and VSS Troubleshoot

Delete old / unused shadow copies

1. Run the command prompt as Administrator.
2. Run "vssadmin delete shadows /all" and select "yes" to delete all.
3. Run "set DEVMGR_SHOW_NONPRESENT_DEVICES=1"
4. Run "devmgmt.msc" to open the Device Manager with the option to show non present devices.
5. Select "View > Show hidden devices" from the Device Manager.

6. Scroll down until you see "Storage volume shadow copies" in the list. Under "Storage volume shadow copies" a listing called "Generic volume shadow copies" will be shown. The icons next to them will be greyed-out.
7. Remove these items one at a time by right-clicking each item and choosing uninstall, or select the item and press DEL and afterwards press ENTER. Repeat this process until all the greyed-out devices are removed.
8. Go to "Storage volumes" and delete all the greyed-out instances of "Generic volume" in the list.

How to increase shadow copy space

In this example we will increase the shadow copy space on C: to 10 GB. A minimum of 1 GB is required on volumes larger than 1 GB. On volumes smaller than 1 GB, a minimum of 350 MB is required.

1. Open the command prompt as Administrator
2. Type the following: `vssadmin Resize ShadowStorage /For=C: /On=C: /MaxSize=10GB`
3. To increase to the maximum permissible size type:
`vssadmin Resize shadowstorage /For=C: /On=C: /MaxSize=UNBOUNDED`
4. We recommend to set the shadow copy space between 10 to 15% of the total volume size. If you have enough free space and you have very large data, you can also set it to unbounded.

Note: If the command prompt commands does not work, you need to change the values over Windows user interface.

5. Go to the local Windows file explorer with all disks shown. Right click any disk and choose "Configure Shadow Copies". On older server operating systems, this may instead be a tab in "Properties".
6. In the Shadow Copies utility: Select the volume C: , click "Settings...", in the "Maximum size" box, increase the limit and press "Ok".

Memory performance tuning for VSS snapshots

1. Run the command prompt as Administrator.
2. Run "regedit" Go to this path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management`
3. Change the following values (if some do not exist, create a new DWORD 32-bit value like the name of the list of the values).
4. Change "PagedPoolSize" to `ffffffff` (hexadecimal)
5. Change "PoolUsageMaximum" to 60 (decimal)
6. Change "SessionPoolSize" to 48 (decimal)
7. Change "SessionViewSize" to 68 (decimal) The following changes apply on this path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters`
8. Change the following values (if some do not exist, create a new DWORD 32-bit value like the name of the list of the values).
9. Change "Size" to 3 (decimal)
10. Change "IRPStackSize" to 24 (decimal)
11. The following changes apply on this path: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\SPP\CreateTimeout`
12. Change value of `CreateTimeout` to 12000000 (decimal)
13. If the key `CreateTimeout` does not exist, create a new DWORD 32-bit value.

Memory performance tuning for VSS snapshots – HYPER-V

For Hyper-V hosts, the following can help to improve Hyper-V VM VSS backup timeout.

1. Run the command prompt as Administrator.
2. Run “regedit”
3. Go to this path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization
4. Change the following value (if it not exist, create a new DWORD 32-bit value like the name of the value). Change “VssRevertTimeout” to 360 (decimal)

Apply important VSS patches

Windows Server 2003: <https://www.microsoft.com/en-us/download/details.aspx?id=11896>

Windows Server 2003 x64: <https://www.microsoft.com/en-us/download/details.aspx?id=9386>

Windows Vista / Server 2008 install latest rollup update patches.

Windows Vista / Server 2008 with 4KB drives or 4KB virtual disks apply this patches: <https://support.microsoft.com/kb/2553708> <https://support.microsoft.com/kb/2470478>

Windows 7 / Server 2008 R2 install latest rollup update patches.

Windows 8 / Server 2012 and newer, install latest rollup update patches.

Pagefile performance changes

Go to Computer → right click → Properties → Advanced System Settings → Performance → Advanced → edit. Change to a fixed size, by default use memory in MB x 1.5. Choose user defined > initial size XXX MB and maximum size XXX MB.

Repair VSS framework

Only use the steps below if all other attempts to repair the VSS framework have failed.. .

These instructions are for 32-bit and 64-bit machines to re-register the VSS framework. You may see some errors, but this can be safely ignored as depending on the system not all modules may be installed. Copy these commands into an empty Windows Notepad and save the file with a batch file extension (*.bat):

```
cd /d %windir%\system32
Net stop vss
Net stop swprv
regsvr32 ole32.dll
regsvr32 vss_ps.dll
Vssvc /Register
regsvr32 /i swprv.dll
regsvr32 /i eventcls.dll
regsvr32 es.dll
regsvr32 stdprov.dll
regsvr32 vssui.dll
regsvr32 msxml.dll
regsvr32 msxml3.dll
regsvr32 msxml4.dll
regsvr32 Vssapi.dll
regsvr32 Vssui.dll
net start vss
net start swprv
```

For 64-bit systems only, add these instructions in addition to the ones above to your batch file:

```
Net stop vss
Net stop swprv
regsvr32.exe /i %windir%\system32\eventcls.dll
regsvr32.exe /i %windir%\system32\swprv.dll
regsvr32.exe %windir%\system32\vssui.dll
regsvr32.exe %windir%\SysWOW64\vss_ps.dll
regsvr32.exe %windir%\SysWOW64\msxml.dll
regsvr32.exe %windir%\SysWOW64\msxml2.dll
regsvr32.exe %windir%\SysWOW64\msxml3.dll
regsvr32.exe %windir%\SysWOW64\msxml4.dll
regsvr32.exe %windir%\SysWOW64\ole32.dll
regsvr32.exe %windir%\SysWOW64\oleaut32.dll
regsvr32.exe %windir%\SysWOW64\es.dll
regsvr32.exe %windir%\SysWOW64\comsvcs.dll
vssvc /register
net start swprv
net start vss
net stop winmgmt
regsvr32 wmiutils.dll
net start winmgmt
```

Run the command prompt as Administrator and execute the created batch file, we recommend to reboot the system afterwards.

Performance tuning of ActiveImage Protector

There are different ways to increase backup speed.

Modify the configuration file "aip.ini" from ActiveImage Protector. This file is always located in ActiveImage Protector's installation folder (i.e. C:\Program Files (x86)\NetJapan\ActiveImage Protector ...\).

Open the "aip.ini" file and scroll down to [aipcopy].

You will see some lines with different values, don't change them.

Add the following lines:

```
io_buffer_size=10240
```

This will result in a higher write buffer.

```
backup_read_buffer_size=10240
```

This will result in a higher read buffer.

This both settings should be tried first. If you still want increase backup speed you can go forward and add the following lines:

```
threadcount=4
```

Default is 0 (will calculate the pipeline thread number by number of CPU Cores), it can also specify the thread number. In the above example we would use 4 cores, in some cases it's recommend to use less threads than the CPU can offer.

```
local_io_flag_non_cache=0
```

Default is 1, you can also try to use local cache with set to 0 and this might can help under circumstances.

After your changes at "aip.ini" you need to restart the ActiveImage Protector service under Windows services (AipService.exe) to get applied.