

WINDOWS SERVER HACKS™

*100 Industrial-Strength
Tips & Tools*

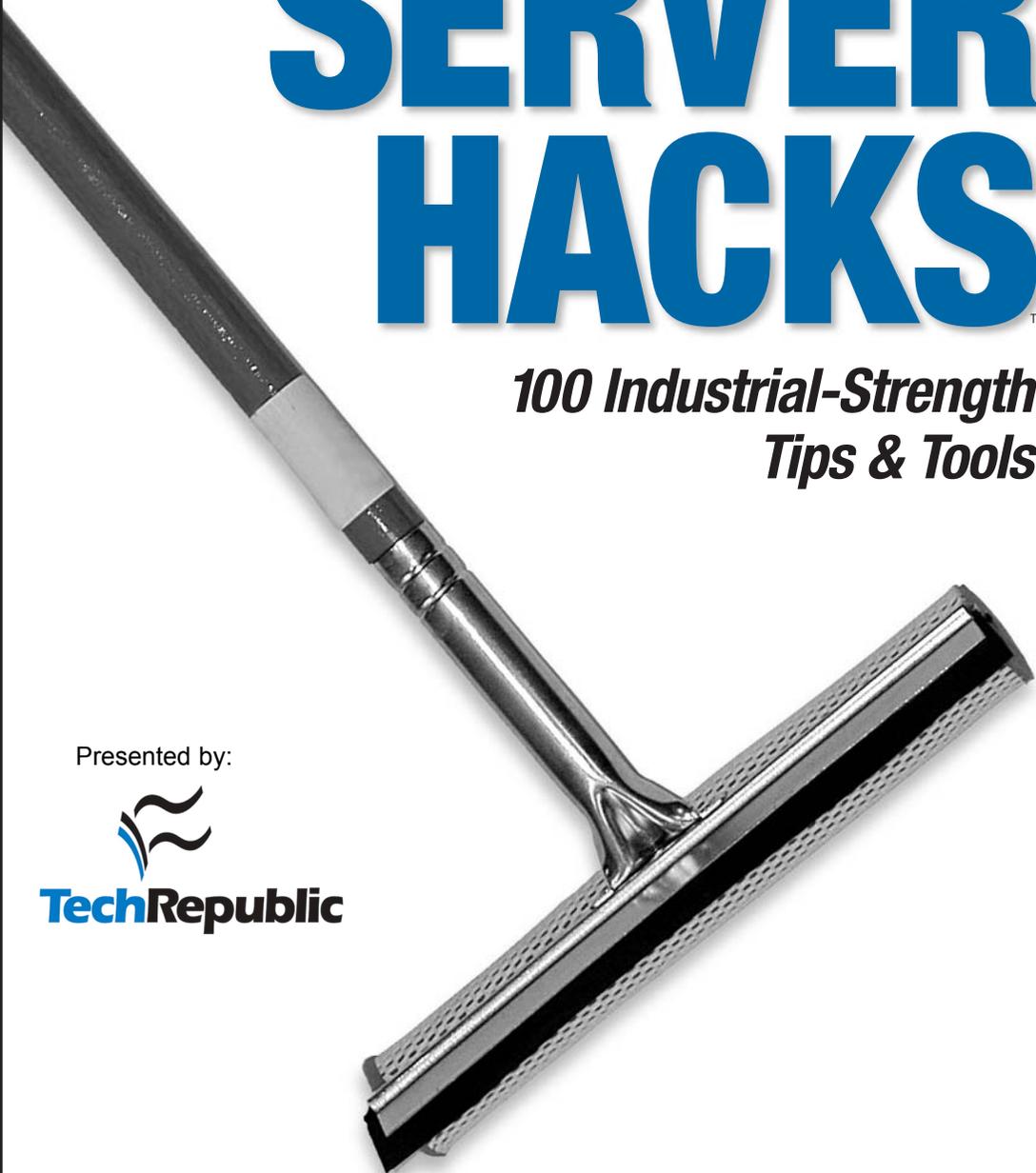
Presented by:



TechRepublic

O'REILLY®

Mitch Tulloch



HACK
#98

Recover with Automated System Recovery

Automated System Recovery (ASR) is a new feature of Windows Server 2003 that makes recovering from a disaster a whole lot easier.

Rebuilding a server after a disaster is generally not a trivial task. The process usually involves reinstalling Windows from scratch, reconfiguring disk partitions to the exact configuration they had before the failure, and then restoring the system volumes, boot volumes, and all your data volumes. The process is not especially complicated, but it takes a considerable amount of time to do it right, usually with significant involvement of the administrator along the way.

With Windows Server 2003, however, things have suddenly gotten much easier. Automated System Recovery (ASR), a new feature included in the Backup utility, greatly simplifies the process of recovering a server that won't boot because of severe problems with the system/boot volume, such as Registry corruption. By automating the process of restoring a failed server, ASR saves you time and reduces the chances for making mistakes. ASR is an essential part of the [Recovery Roadmap \[Hack #99\]](#) for troubleshooting problems that might happen to Windows servers, and this hack leads you through the process step by step. I'll also clarify how best to use this feature and how to resolve problems that can arise.

ASR Backup

The simplest way to back up your system with ASR is to use the Backup or Restore Wizard that starts by default when you select Accessories → System Tools → Backup. Simply start the wizard, select “Back up files and settings,” and choose the option to back up “All information on this computer.” Then, specify the remaining backup job parameters as usual. The result is that all information on your hard drives is backed up, including the boot, system, and data volumes. Later, should a disaster occur, you can restore your system by using the ASR restore process to the exact configuration it had earlier.

The backup is done by using shadow copies [\[Hack #95\]](#) to ensure that any open files on the system and boot volumes are properly backed up. Note, however, that this applies mainly to the system and boot volumes, which are critical for successful ASR backup. While shadow copies are also used to back up data volumes, these shadow copies are deleted afterward unless you've specifically enabled shadow copies on these volumes to help protect users' work from accidental loss or damage.

Recover with Automated System Recovery

An alternative method for performing ASR backup is to start Backup and switch to Advanced Mode. Then, under the Welcome tab (Figure 10-9), select the Automated System Recovery Wizard button. This wizard lets you back up only information on your system and boot volumes that is critical to restore your system; it does not back up any data volumes, which are usually best left for your regular backup program to handle anyway.

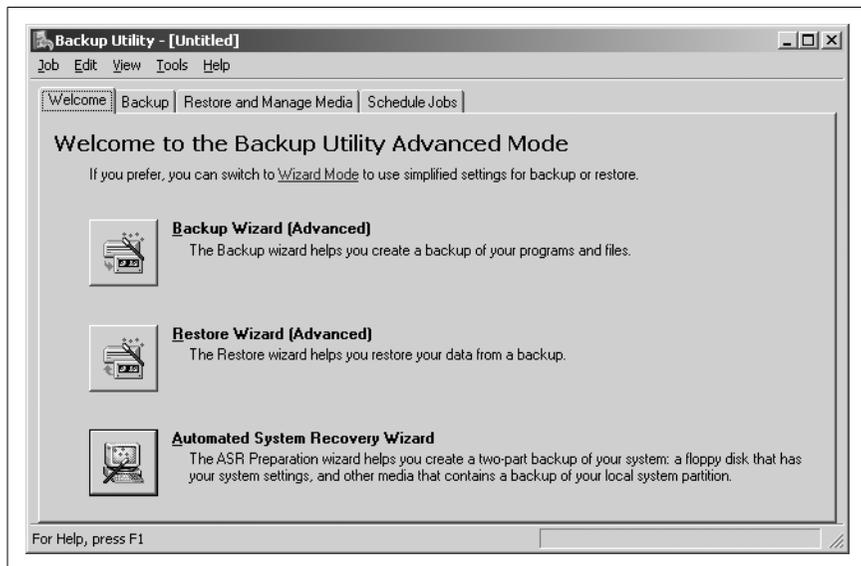


Figure 10-9. Starting the Automated System Recovery Wizard

During the ASR backup process, you're asked to insert a blank, formatted floppy to create a system recovery disk (commonly called an ASR floppy). This floppy is critical to the ASR restore process, so it's worth digging a little deeper into how it's used. The ASR backup process saves two files onto your floppy: the ASR state file (*asr.sif*), which contains information about the disk signatures and configuration of disk volumes on your machine, and *asrnpn.sif*, which contains information about different Plug and Play devices on your system. These two files are critical for the recovery of your system, because they connect the underlying hardware configuration with the operating system above it. As we'll see in a moment, you need to insert this floppy at the beginning of the ASR restore, in order to rebuild the disk subsystem and hardware configuration of your system before restoring the contents of the system and boot volumes.

What if you have no floppy disk drive on your machine? Fortunately, you can still use ASR to back up your system, but it's a bit of a workaround. During the ASR backup process copies of these *asr.sif* and *asrnpn.sif* files are

also saved in the `%SystemRoot%\Repair` folder on your server. So, when you receive a prompt at the end of the backup process to insert a floppy, simply ignore the prompt and instead copy `asr.sif` and `asrnpn.sif` from `Repair` to a network share on another server (one that has a floppy disk drive installed). Then, copy the files from the share on that server to a blank floppy you insert into its drive, and you now have a working ASR floppy for your backup. Then, go buy a USB external floppy drive, because you'll need it if you ever have to rebuild your original server from the backup set you created. In other words, you can perform ASR backup without a floppy, but you cannot perform an ASR restore without one.

What if you lose your ASR floppy? Well, the procedure just described will work in this case too. Just insert a new blank, formatted floppy into your server and copy `asr.sif` and `asrnpn.sif` from the `Repair` directory to the floppy. Note that these files must be located in the root folder on the floppy for the restore process to work, so use a separate floppy for each ASR backup; don't try to combine several ASR backups in different folders on one floppy.

However, since the `Repair` directory is located on the boot volume of the system itself, if your system volume is toast, then so is your `Repair` directory and the files within it. So, what if you've lost your ASR floppy and the `Repair` directory is gone with your hard drive? There's still a workaround that can save your bacon: use the Backup utility on a different machine to open the backup catalog for the ASR backup set you want to restore, expand the `%SystemRoot%\Repair` directory on the boot volume, select `asr.sif` and `asrnpn.sif` as the files you want to restore, insert a blank floppy, and restore these two files to the root of the floppy. Presto! You now have a recovered ASR floppy you can use to initiate a restore.

ASR Restore

The ASR restore process in a nutshell is as follows: first, the disk configurations are restored; then, your system and boot volumes are formatted; and, finally, a bare-bones version of Windows is installed that starts Backup and rebuilds your system and boot volumes from your ASR backup set stored on tape media.



Note that *your system and boot volumes are formatted*. Clearly, using the ASR restore process should be considered a last-ditch effort, to be used only when everything else fails. See “Recovery Roadmap” [Hack #99] for information on how to choose between the various recovery options for Windows servers.

Using ASR restore. Let's look at a restore in more detail. First, make sure you have your ASR floppy, tape backup media, and original installation files for Windows Server 2003 (i.e., the product CD). If you have any mass storage controllers on your server that require an updated driver to replace the one on the product CD, be sure to have this handy as well.

Also—and this might be important—be sure to back up any data files or folders located on your system or boot volumes. Since ASR reformats these volumes, anything other than the Windows operating system files that are located on these volumes might be lost. Mind you, best practice is to never store data files on these volumes—you should store them on separate volumes instead—so if you've been following this practice you have nothing to worry about, right? Note that I said *might* be lost, not *will* be lost. While Windows documentation says that non-operating system files stored on system/boot volumes won't be restored by ASR, my own experience is that they are restored sometimes and other times not. So, just to be safe, back up these volumes separately using normal backup procedures so you can later restore any missing data files.

Now, insert your product CD and boot from your CD-ROM drive (press the appropriate key to do this if required). Press F6 when prompted if you have an updated device driver for your mass storage device. Then, press F2 when text-mode setup prompts you to perform ASR restore, and insert the ASR floppy when asked to do so. The recovery process will rebuild the disk signatures and partition table, reformat the system/boot volumes, copy installation files, and begin installing Windows. A short while into the installation of Windows, the Automated System Recovery Wizard screen will ask you to specify the location of the tape backup media where your ASR backup is located. Once you specify this, the recovery process continues and it's considerably faster than the Windows installation process itself, which is nice. Be sure not to interrupt this process; otherwise, you'll have an incomplete and nonfunctional server. Once the restore process is finished, the logon screen appears and you're done.

That is, you're done unless your system was totally fried and you have to rebuild it from scratch—in which case, you have to complete the procedure by restoring any data volumes on your server from your regular backup sets.

Here's one more thing that's helpful, but not documented. Running the ASR restore process also creates a *setup.log* file that identifies the system and boot volumes, checksums for kernel files, the directory where Windows is installed, and the device drivers loaded during setup. A copy of this file is placed in `%SystemRoot%\Repair` and also another one is placed on the ASR floppy itself, which is handy for verifying the details of the restore process. Print that log and keep a record of it for troubleshooting purposes later.

Hacking the restore. If your original machine is *really* toast, you can use ASR to restore to a different machine. However, to do this, you must ensure that the hardware on your new system is identical to your original (toasted) system, with the exception of the video card, network card, and hard disks, which can be different brands or types. Concerning hard disks, however, make sure the number of hard drives in your new system is equal to or greater than the number of hard drives on the old system, and also make sure that the storage capacity of each drive is the same or larger than drives on your old system.

If you're using ASR to restore a failed server to another system with hardware that does differ significantly from the old one, there's a workaround: you can hack the *asr.sif* file to make the ASR restore process install additional device drivers (or any other kinds of files) that might be needed by the text-mode setup process to install Windows successfully and complete the recovery.

The *asr.sif* file is a text file with different sections, identified by brackets:

```
[VERSION]
Signature="$Windows NT$"
ASR-Version="1.0"

[SYSTEMS]
1="SRV230","x86","5.2","C:\WINDOWS",1,0x00020112,"360 0 -60 0-10-0-5 2:00:00.0 0-4-0-1 2:00:00.0","Central Standard Time","Central Daylight Time"

[BUSES]
1=1,3

[DISKS.MBR]
1=1,1,1,0xdbe3dbe3,512,63,255,16514064
```

By adding an additional [InstallFiles] section, you can specify additional files that need to be copied to the machine during text-mode setup. For example, adding the following section will cause the driver file *MyDriver.sys* to be copied from the root of the floppy disk that has the volume label *My Drivers* to the %SystemRoot%\System32\Drivers folder on the machine:

```
[InstallFiles]
1=1,"My Drivers","Floppy","%SystemRoot%\System32\Drivers\MyDriver.sys","My Company Name",0x00000001
```

During text-mode setup, a prompt will ask you to insert the floppy disk that has the driver file for *My Company Name*, and the 0x00000001 flag indicates that this prompt will always appear. Other flags can also be used, including 0x00000006, which indicates that ASR recovery can't proceed unless you load the specified driver file; 0x00000010, which indicates that any existing copy of *MyDriver.sys* should be overwritten by the new file; and 0x00000020, which prompts before overwriting an existing version of the file.

Using this hack, you can customize the ASR restore process to make it successful, even if there are some hardware differences between the original machine and the new one.

Using ASR

Finally, many administrators don't understand *when* to use ASR to back up the system and when they should just use regular backups. You should back up your system anytime you change your hardware or operating system configuration. Examples of such changes might include upgrading to a new version of the operating system, installing service packs or hotfixes, adding new disk storage or changing the partition layout of your volumes, switching from basic to dynamic storage, installing a new Windows component or service, installing and configuring a third-party application, installing new hardware or upgrading device drivers, and so on.

Doesn't this sound suspiciously like the instructions for creating the old Emergency Repair Disk (ERD) on Windows NT/2000? Yes, though ASR is a far more powerful feature than the ERD. Since it backs up the System State and Registry on your machine, it does include similar functionality to the ERD, including saving a copy of your Registry hives in the *Repair* folder. But while the ERD could be used only to replace corrupt or missing system files or Registry hives, ASR is a complete system-recovery feature that does everything the ERD did and more—automatically.

You don't need to use ASR for backup when your system is tuned and running perfectly and only user data files are being created, modified, or deleted on your server. If you've properly partitioned your system so that all user data files are on data volumes separate from the boot and system volumes, then you can simply back up these data volumes on a daily basis to ensure nothing is lost in the case of a disaster. But if you change your basic operating system or underlying hardware in a significant way, use Backup to create a new ASR backup set so that you can recover your system to its current state, should massive failure occur.

This material has been adapted from *Windows Server Hacks* by Mitch Tulloch, published by O'Reilly Media, Inc. Copyright O'Reilly Media, Inc., 2004. All rights reserved. To purchase this or other O'Reilly publications, [click here](#).

Additional resources

- Sign up for the [Windows 2000 Server newsletter](#)
- Sign up for the [Windows Server 2003 newsletter](#)
- See all of [TechRepublic's newsletter offerings](#)
- [Ten great Windows Server hacks](#) (TechRepublic)
- [From its help desk calls, Microsoft reports top 10 security errors](#) (TechRepublic)
- [Active Directory: Lock it down in 10 steps](#) (TechRepublic)