

Windows NT Emergency Boot

By Mark E. Donaldson

INTRODUCTION

This document is about disaster recovery for the Windows NT system. It applies to both the server and workstation systems. If you want to learn how you can ultimately protect your system by creating the ultimate Windows NT boot disk, and protect all you data read on. The **boot disk described below** will assist you in restoring your system if you suffer hard disk drive failure on your root system, if you loose or corrupt your system MBR (Master Boot Record), if you loose or corrupt your Master Partition Table, or if you loose or corrupt your MTF (Master File table). The other saved date described, which you will backup on a separate partition on a separate hard disk drive, will assist you in restoring your ERD (Emergency Repair Disk) information and data, and your registry data.

STEP 1: INSTALL A SEPARATE COPY OF WINDOWS NT

Although most of your system can be recovered by the creation of the ultimate boot disk, to be adequately prepared for all disasters (mainly the one of worst case scenario) you should have a second copy of Windows NT (server or workstation) installed on your system. ***This should be installed on a separate hard disk drive from your primary or root system.*** Think about it. If your hard disk drive physically fails, there is very little you can do. However, if you have a separate installation, all system data can be recovered and restored. Step 1 is to then install Windows NT on a separate hard disk drive on the same system. Do this now. You will need the boot information it generates in the following steps. Once you have done this, ***configure your boot.ini file to allow optional booting into this backup system.*** It may save your life.

- Install a second copy of Windows NT (server or workstation) on your system. This should be installed on a separate hard disk drive from your primary or root system.
- Configure your boot.ini file to allow optional booting into this backup system.

STEP 2: CREATE THE ULTIMATE BOOT FLOPPY

1. Format a new floppy disk using Full Format (just to be safe). It is important that you format the floppy on the same computer as you are creating the backup for or it probably won't work. Now open Windows NT Explorer and click on the root folder (usually C:\). It is essential to copy the following files to the floppy disk:

- **Boot.ini**
- **Ntdetect.com**
- **Bootsect.dos (for dual start-up installations)**
- **NTLDR**
- **Ntbootdd.sys (if it's in the root folder, copy it)**

If you don't see these files in your root folder, choose View|Options in Windows NT Explorer. Select the radio button labeled Show All Files. Click Apply and then OK. Now you should see the files. If you don't, press F5 and look again.

Windows NT Emergency Boot

By Mark E. Donaldson

2. Now, here's where the good stuff comes into play. Copy these files to your boot disk as well:
 - **Dskprobe.exe** (from the Windows NT Resource Kit or NT Server CD-ROM).
 - **autoexec.nt**
 - **config.nt**
3. Using **DiskProbe**, backup the MBR for each of the hard disk drives on your system. **Put these files on your boot disk.** Here's how you do this:
 - Open **DiskProbe**. On the Drives menu, click **Physical Drive**. You will see the **Open Physical Drive** dialog box. The **Available Physical Drives** are listed as PhysicalDriven, where n=0 for the first hard disk. If you have more than one hard disk, backup the MBR on each disk since it contains the partition information for that disk.
 - In the **Handle 0** group box, click **Set Active** and click **Close**.
 - On the **Sectors** menu, click **Read** to open the **Sector Range** dialog box. Set **Starting Sector** to 0 and **Number of Sectors** to 1. Click **Read**.
 - On the **File** menu, click **Save As**. Enter the filename, such as **MBRDSK0.dsk**, **MBRDSK1.dsk**, and **MBRDSK2.dsk**. The file extensions will be **.dsk**.
4. Next, format a second floppy disk and backup your partition table to your boot disk. To do this, start **Disk Administrator**, choose **Partition, Configuration, Save**. Insert the second formatted floppy disk into Drive A and click OK. You now have a valid copy of your Master Partition Table. It will be in a file called **system**, and can easily be restored back to your hard disk drive by using the Disk Administrator **partition|restore** function.

Your **ultimate boot disk (actually it's two disks) is now ready to use**. Please note, you have copies of the Master Partition Tables for all your hard disks on both of the boot disks. You may not need the second disk, but it never hurts to have a second backup to the backup. In this case, they were created by two different disk programs. Under any circumstances, you should now be able to boot into your system and make the necessary repairs to the boot sector and boot files.

STEP 3: BACKUP YOUR REGISTRY AND ERD FILES

Despite what you might hear or read, the Windows NT Registry can be backed up. Here's how:

All the Registry files are located in **Winnt\System32\Config**. If you copy this directory to another location (preferably on another drive), you'll have a complete backup. The problem with this is simply that the **Config** folder is likely to be very large and unable to fit on a floppy disk. However, if you have a Zip Drive, a CD Recorder, or some other removable storage device, you can copy the files to that and then keep the disk in a safe place. The files you need for full Registry backup are:

Windows NT Emergency Boot

By Mark E. Donaldson

- AppEvent.Evt
- default
- default.LOG
- default.sav
- sam
- Sam.log
- SecEvent.Evt
- Security
- Security.log
- Software.sav
- SysEvent.Evt
- System
- System.LOG
- System.sav
- Userdiff
- Software
- Software.LOG

These same registry files are also written to the **Winnt\System32\Repair** directory when you run **rdisk /s** (/s = security). If you copy this directory to another location (preferably on another drive), you'll have a complete backup. The nine files you need are:

- autoexec.nt
- config.nt
- default._
- ntuser._
- sam._
- security._
- setup.log
- software._
- system._

If you have a tape drive attached to your NT system, backing up the hive files is easy: Run NT's tape backup program (ntbackup.exe), and select the Backup Local Registry check box in the Backup Information dialog. However, NT Backup is limited: It can back up the Registry of only the local system (you can't use it to back up a computer's Registry over a network), and it backs up only to tape.

If you don't have a tape drive on your local NT system, or if you want to back up the Registry hives of a remote computer, you must use another method--either NT's **rdisk.exe** utility or an NT Resource Kit's backup utilities, **regback.exe** and **regrest.exe**.

Rdisk

If you don't have an NT Resource Kit, you can copy hive files by running **rdisk.exe**, found in your NT system's support directory (\system32). This utility updates repair data on the Emergency Repair Disk, in the **winnt\repair** directory, or both.

Windows NT Emergency Boot

By Mark E. Donaldson

Note that to completely back up the hives, you must run `rdisk.exe` with the `/s` switch, as follows:

rdisk/s

You can think of the `/s` switch as standing for "security"; using `/s` adds the user account information to the Repair disk and the repair directory. If you run `rdisk.exe` without `/s`, the backup doesn't include the SAM and Security files and is thus an incomplete backup of the Registry. For example, if you add users to the account database and then update the Emergency Repair Disk with `rdisk.exe` (without `/s`), those changes won't be added to the repair disk. And, if you delete accounts, you have to re-create them--they can't be recovered from the Repair disk.

regback and regrest

If you have an NT Resource Kit, you can use two of its utilities, **regback.exe** and **regrest.exe**, to back up and restore the Registry. **regback** copies the hive files for `hkey_local_machine` or `hkey_current_user` to a user-defined location, and **regrest** lets you restore some or all of the files as necessary. Using these two utilities is easier than using `rdisk` because you don't have to go through the NT restoration screens to restore the backups.

To use **regback**, enter:

regback <DestinationDirectory>

where `DestinationDirectory` is the name of the directory to which you save the hive files. If you receive an error message stating that a file must be backed up manually, you must save the file to a named file by using the alternative syntax:

regback <filename> <hivetype> <hivename>

where `filename` is the name of the file you're saving the original file to, `hivetype` is the type of hive (`machine` or `users`, the only types you can back up), and `hivename` is the name of one of the hives in either `hkey_local_machine` or `hkey_current_user`. If you're using the manual backup method because you received an error message during the normal backup, `hivename` needs to be the name of the hive that wasn't backed up.

Using **regrest** is somewhat more complicated. The syntax is:

regrest <newDirectory> <saveDirectory>

where `newDirectory` specifies the source of the backed-up hive file that will replace a hive file in the `system32\config` directory, and `saveDirectory` is the location to which you'll copy the old Registry hive files. By default, **regrest** attempts to replace each file in the `system32\config` directory with a like-named file from the backup directory, and copies all the old hive files to the directory you specify. These directories must be on the same volume. For example:

Windows NT Emergency Boot

By Mark E. Donaldson

regrest c:\hivefiles.bku c:\install.sav

copies the files in c:\hivefiles.bku to the system32\config directory and then backs up the files that were in the system32\config directory to c:\install.sav. You reboot the system to activate the changes.

As with regback, a warning appears if there are hives you must restore manually or if errors occur. To restore a file manually (for example, if you saved it to another name using regback), the syntax is a little different. You enter:

regrest <newFilename> <saveFilename> <hivetype> <hivename>

where newFilename is the name and location of the file to be copied to system32\config and renamed, saveFilename is the name and destination of the file to be copied to the backup location, hivetype is machine or users, and hivename is a hive in hkey_local_machine or hkey_current_user. As with regback, you must reboot your system for these changes to occur.

That's all there is to it. You are now prepared for full disaster recovery. You have all the information and all the files you need, plus the means to do so. If you have any questions or feedback, please contact me at markee@ridgecrest.ca.us.