Realtime publishers
"Leading the Conversation"

The Essentials Series

Active Directory 2008 Operations

sponsored by
SCRIPTLOGIC

by Greg Shields

Copyright Statement

Understanding Active Directory Recovery in Windows Server 2008

The deceptive ease of backing up Windows' Active Directory (AD) has often lulled Windows administrators into believing that its restoration is similarly easy. Although native tools such as NTBackup and the new Windows Server Backup available in Windows Server 2008 make the backup process relatively easy, the process to restore individual objects remains somewhat complex.

Thankfully, while individual object restores remain a multi-step process, Windows Server 2008 includes new tools that ease the task of completing a bare-metal recovery of a failed domain controller. Using Windows Server 2008's combination of Windows Server Backup and Windows Complete PC Restore, the process to resurrect a failed domain controller has now become fairly trivial.

This white paper will discuss the processes needed to properly backup and restore individual Active Directory objects as well as entire DC's once they have been upgraded to Windows Server 2008. It will provide specific guidance and step-by-step instructions to assist you the administrator with understanding and best completing this critical recovery task.

Backing Up AD

In order to back up AD, the Windows Server Backup feature must first be installed to the domain controller of interest. In contrast to the NTBackup tool used in previous versions, the Windows Server Backup feature is not installed by default. To install the feature and prepare it for first use, launch Server Manager, right-click the Features node, and select Add Features. Select the check box next to Windows Server Backup Features, and click Next, Install to install the feature.

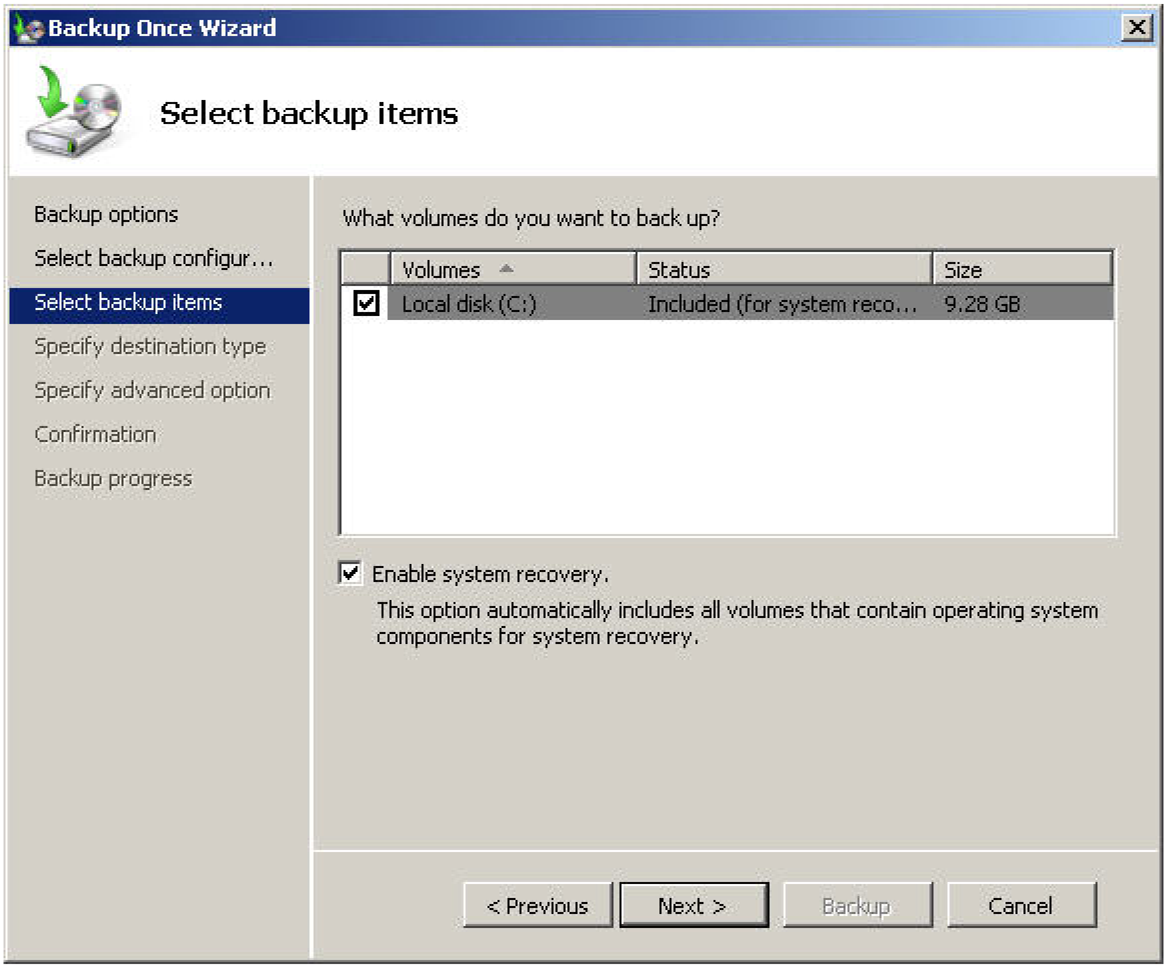
✎ Another available feature selection is Command-line Tools. These tools are useful for scripting or creating batch files to initiate backup or restore operations and are necessary to complete the System State restore necessary to restore individual AD objects.

In Windows Server 2003 as well as earlier versions, backing up AD was done via a backup of the System State. Backing up the System State of a domain controller captured the proper components to ensure AD could be restored successfully onto the same computer. The problem with System State backups was that they did not capture the entire composition of the domain controller. Instead, only a small portion of the server—such as boot files, registry, and COM+ class registrations—were captured to the backup in addition to AD's NTDS database and the SYSVOL. Because of this shortcoming, restoring a failed domain controller meant rebuilding a new server instance, upgrading that instance to the same service pack and patch level, and restoring the System State over the top of the core installation. This mechanism for completing a restoration required less storage space for backups but a longer amount of time required to complete a restore as well as a reduced chance of a successful restore.

With Windows Server 2008, System State backups are deprecated in favor of what are called critical volumes. Critical volumes are those volumes that are required to recover the AD. They include the operating system (OS) files, the registry, the NTDS database and log files, and the SYSVOL. The critical volumes required to be backed up can be as few as a single volume in the case where all AD components are installed to the same drive, or they can be multiple volumes if AD components were separated at installation to different drives.

To back up AD, launch Server Manager and navigate to the Storage | Windows Server Backup node. Select Backup Once to begin a single backup instance. You will need to answer questions in the following screens of the Backup Once Wizard:

- *Backup options*—If options have been previously selected for the Backup Schedule Wizard, those options will be selected here. Otherwise, choose *Different options* to select a new set of options.
- *Select backup configuration*—The option to back up the *Full server* is provided as well as a Custom option to select volumes of interest. When selecting volumes to back up, ensure that all critical volumes are selected.
- *Select backup items*—If the Custom option was selected in the previous screen, the screen shown in Figure 1 enables the selection of volumes to back up. A check box is also available to *Enable system recovery*. This check box must be selected in order to perform a bare-metal restore.
- *Specify destination type*—Backed up data can be stored either to an available local drive or to a remote shared folder. Backups cannot be stored to critical volumes, but it is possible to back up full volumes to DVD media. As a workaround, it is possible to store backups to a shared folder on the local machine by referring to the full shared folder path on the local machine.
- *Specify remote folder* or *Specify backup destination*—Depending on the selection in the previous screen, one of these two options will be displayed. Select either an available local drive or a remote folder. If you select a remote folder, you are given the option to select privilege inheritance on the target folder.
- *Specify advanced configuration*—In this screen, VSS backup behavior is determined, which configures the backup to retain or clear application log files as well as update file backup history. This selection is important when other backup products are being used to back up applications.
- *Confirmation*—Click Backup to start the backup.



Select backup items

What volumes do you want to back up?

☑	Volumes	Status	Size
☑	Local disk (C:)	Included (for system reco...	9.28 GB

☑ Enable system recovery.

This option automatically includes all volumes that contain operating system components for system recovery.

Figure 1: Configuring the volumes to back up in the Backup Once Wizard.

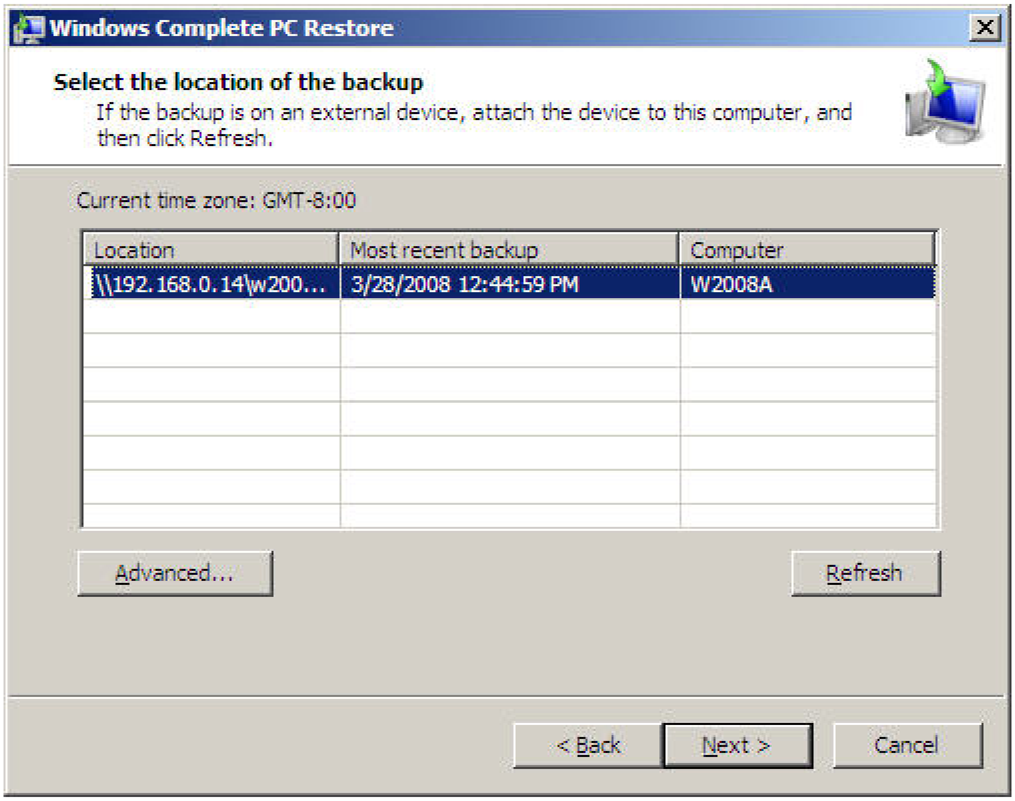
Full Server Recovery of a Domain Controller

In Windows 2003 and earlier, the native Windows restoration process required the installation of an OS prior to starting a restore. This added time and complexity to the restoration process. With Windows Server 2008, once a domain controller backup has been completed, it is then possible to restore that domain controller directly onto bare metal. The target computer need not be the exact same computer as the source of the backup, but it must have the exact same hardware composition.

This capability for bare-metal restoration speeds the restoration process while providing a greater assurance of a successful restore. It relies on the use of Windows Server 2008's pre-installation environment. WinPE natively includes many of the necessary networking and storage drivers as well as a graphical OS to assist with the restoration process.

To complete a bare-metal domain controller restoration, boot the target server with the Windows Server 2008 media DVD, and click Next when prompted. In the resulting screen, click the link titled *Repair your computer*, and then Next at the following screen. When the System Recovery Options screen appears, select Windows Complete PC Restore. The system will attempt to scan the local machine's drives for a current backup. If backup files are stored elsewhere on the network, click Cancel. In the resulting *Restore your entire computer from backup* wizard, select *Restore a different backup*, and click Next.

WinPE includes a set of common network drives that function with many network cards. Because of this native support, it is possible to connect WinPE to Windows shares elsewhere on the network that contain backup files. In the screen titled *Select the location of the backup*, click Advanced, and select *Search for a backup on the network*. Choose Yes when asked to verify that the network is a trusted network. In the resulting box, enter the full path to the network share containing the backup of interest. Figure 2 shows an example of the dialog box that appears when the wizard successfully connects to remote backup files.



Windows Complete PC Restore

Select the location of the backup

If the backup is on an external device, attach the device to this computer, and then click Refresh.

Current time zone: GMT-8:00

Location	Most recent backup	Computer
\\192.168.0.14\w200...	3/28/2008 12:44:59 PM	W2008A

Figure 2: Windows Complete PC Restore successfully connecting to a remote share for backup files.

Select the location of the backup, and click Next. In the screen that follows, select the backup of interest in that location, and click Next again. The resulting screen provides the ability to exclude disks from the restore, install any necessary storage drivers, restart the computer after the restore, and complete automatic checking and updating of disk error information. Click Next, then Finish to start the restoration.

> Be aware that the target disk must be at least as big as the source disk. This is a requirement even if the backup file size is smaller than the total size of the disk. If the target disk is larger than the source disk, a volume will be created on the target disk during restoration that is equal to the original size of the source disk. Using Disk Management, it is possible to later extend the volume to consume the extra space if desired.

Restoring Deleted AD Objects

In the introduction to this paper, it was mentioned that the process to restore deleted AD objects remains complex even upon the upgrade to Windows Server 2008. Such remains the case because much of the process of completing an object restoration in Windows Server 2008 is effectively the same as in previous OS versions.

To begin the process, you will need to reboot the server into Directory Services Restore Mode (DSRM) and complete a non-authoritative restore of AD. To boot into DSRM, hit F8 during the initial boot cycle. In the resulting screen, select Directory Services Restore Mode, and hit the Enter key. After the machine boots into DSRM, login with *.\administrator* as the username along with the DSRM password.

Although System State backups are deprecated in Windows Server 2008, System State restores are still used for restoring objects in AD. System State restores are supported only through the Windows Server Backup command-line tool wbadmin. Two steps are necessary. The first step identifies the correct backup from which to restore data. The second step begins the non-authoritative restore. The first step is shown below:

```
wbadmin get versions –backuptarget:<targetDrive>:
-machine:<backupComputerName>
```

In this step, <*targetDrive*> identifies the location where the backup media is currently stored, while <*backupComputerName*> identifies the name of the computer where you want to recover the backup. Listing 1 shows an example of a result from running this command.

```
C:\Users\Administrator>wbadmin get versions -backuptarget:\\SRV1\share
-machine:w2008a

wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Backup time: 3/28/2008 2:44 PM
Backup target: Network Share labeled \\SRV1\share
Version identifier: 03/28/2008-20:44
Can Recover: Volume(s), File(s), Application(s), Bare Metal Recovery,
System State

C:\Users\Administrator>
```

Listing 1: The result from running the **get versions** ***switch of the*** **wbadmin** ***command.***

The version identifier previously shown is needed for input into the second command. In Listing 1, the version identifier is shown as *03/28/2008-20:44*. This string is used to replace *<version>* in the command below:

```
wbadmin start systemstaterecovery –version:<MM/DD/YYYY-HH:MM>
–backuptarget:<targetDrive>: -machine:<backupComputerName>
```

The values of *<targetDrive>* and *<backupComputerName>* remain the same as for the previous command. After running this command, hit the Y key to start the System State recovery operation.

Once this is complete, restart the server into normal mode. To complete the restore of the deleted object, an authoritative restore is required. This process is completely unchanged from Windows Server 2003, so for more information about the process of completing an authoritative restore, consult http://go.microsoft.com/fwlink/?LinkId=68564.

Locating Deleted Objects with DSAMAIN

A complexity with the object restore process is that the commands to complete the process require the distinguished name of each deleted object. One of the major pain points with using the Windows native tools in restoring deleted AD objects is locating exactly what has been deleted and determining their distinguished names.

The good news is that a new feature has been added to Windows Server 2008 that indirectly assists with this process. The DSAMAIN tool enables the creation and later mounting of AD database snapshots in parallel with the currently running instance. This parallel instance is then compared with the current instance to locate the deleted object as well as its distinguished name. The snapshots are not so much backups that can be restored. Rather, they are view-only representations of the database that are mounted as AD Lightweight Directory Services partitions using the NTDSUTIL command.

Before a snapshot can be mounted, it must first be created. To create a snapshot, use the command:

```
Ntdsutil snapshot “activate instance ntds” create quit quit
```

Among other information, the output of this command will be a GUID that is used to identify the partition when later mounted. If you need to list the available snapshot GUIDs, use the command:

```
Ntdsutil snapshot “list all” quit quit
```

To mount a previously created snapshot, replace <GUID> in the following command with the GUID of your snapshot of interest:

```
Ntdsutil snapshot “mount <GUID>” quit quit
```

The result of this command will look similar to Listing 2. Note in Listing 2 the location in which the snapshot has been mounted within the file system. This information is used in the next step.

```
C:\Users\Administrator>ntdsutil snapshot “mount {837e3bbc-dd34-2fed-
8cb6-88832ef7658c}” quit quit

ntdsutil: snapshot
snapshot: mount {837e3bbc-dd34-2fed-8cb6-88832ef7658c}
Snapshot {837e3bbc-dd34-2fed-8cb6-88832ef7658c} mounted as
C:\$SNAP_200803281403_VOLUMEC$\
snapshot: quit
ntdsutil: quit

C:\Users\Administrator>
```

Listing 2: The result from mounting an AD snapshot using NTDSUTIL.

Once the snapshot is mounted, the DSAMAIN tool can be used to start the mounted snapshot as a parallel AD instance. Do this with the following command:

```
DSAMAIN –dbpath {pathToMountedAd}\WINDOWS\NTDS\ntds.dit –ldapport
{newLdapPort}
```

In this command, you will need to replace {pathToMountedAd} with the path shown in Listing 2. In the example there, the path is C:\$SNAP_200803281403_VOLUMEC$\. You will also need to replace {newLdapPort} with an available network port that is not currently in use. Typically, a very high numbered port is used, such as 41000.

Upon starting the mounted snapshot, the snapshot operates much like a running instance of AD. You can use AD manipulation tools such as LDP to search within the snapshot to locate information about deleted entries. This information becomes useful in completing the authoritative restore step in the AD restore process.

Recovery Knowledge Is as Important as Backup Knowledge

Although some of the processes for completing AD backups and restores have become easier, others remain complex and involve plenty of command-line experience. Being aware of the success of backups and knowing the restore process is critical to getting your Windows domain back online after an accidental deletion incident occurs. The information presented here provides a good start towards assisting you with that critical restoration knowledge and experience.