Domain Controller Recovery

How to Backup and Restore Active Directory

Backing up Windows 2000 Active Directory requires special care and precautions beyond what a normal backup might require. The issues are further complicated if you are targeting dissimilar hardware, for a useful How-To please refer to:
http://wwwbrainbuz.org/techinfo/win2ksystate.pdf.

Step 1: How to Backup a Domain Controller using NTBackup

Prior to Service Pack 2, there was a bug affecting restoration of system state. Before backing up install at least Service Pack 2 on your Domain Controllers.

It is necessary to backup the entire System or boot volume(s), and System State, which is a separate checkoff in NTBackup.

Some files typically fail to be backed up, you need to review the log to see what they were. Some files like individual's settings are non-criticial and you can safely ignore them. The WINS database always fails to backup, if you will need to restore the existing WINS database then stop the WINS service prior to backing up the server and restart it when you are done.

Step 2: Restoring the First Domain Controller from Backup

When there are no other active Domain Controllers for a Domain Available, it is necessary to perform a "Primary Restore", marking that Server's version of SYSVOL as authoritative. This is not nearly as drastic as an "Authoritative Restore" which will cause one server's version of the Directory to overwrite all of the other replicas.

Primary Restore is fairly simple, follow the regular restore procedure below, when the Advanced options become available during the restore process, check the box for "Primary Restore".

Step 3: Restoring a Domain Controller from Backup

Install the same version of Windows 2000 Server (Server, Advanced Server, etc.) as is on the Domain Controller you are restoring.

Restart the target in Directory Services Restore mode. Start NTBackup and retrieve the catalog for the backup. Check off to restore the C Drive and system state (and any other volumes you need to restore). In options, elect to "Overwrite all files". You will be restoring to the "Same Location".

When you begin to backup and a dialog box with a button for "Advanced" appears, click it and check that the appropriate boxes are checked. If this is the first Domain Controller (see step 2)

check Primary Restore, otherwise do not check this box. You will want to: Restore Security, Restore Junction Points, and Preserve Volume Mount Points.

Step 4: Starting a Restored Domain Controller

If the restore was "Primary", the Domain Controller should come up (after considerable delay to restore network connections) as a fully functional DC. You can quickly test by typing "net share" at a command prompt to see the SYSVOL is being shared.

A regular (non-authoritative) restore may need a bit of a kick.

You can restart in Directory Services restore mode and run NTDSUTIL which will allow you to verify the directory and perform a recovery of the database. You should not perform an Authoritative restore unless there is a specific reason, and especially if a primary restore has already succeeded.

The best kick may be to manually share the sysvol with the command "net share sysvol=c:\winnt\sysvol". You will get an error, but with luck it is now actually sharing SYSVOL and NETLOGON.

The final test is logging a user on to a connected workstation (which you may first need to join to the domain), success means you have both a functioning Domain Controller and Global Catalog.

Step 5: Post Restore

Un-restored Domain Controllers

The Domain Controllers, which you have not elected to restore, will remain until you go to lengths to delete them. First you will need to delete all references from Active Directory Sites and Services to those DCs. A reference may be hidden within a site's own NTDS object. Then you must wait for replication before you can delete them from the Domain Controllers container in Active Directory Users and Computers. Even after this is done, the purged DCs may not be entirely gone. Use NTDSUtil to view information, and use its Metadata Cleanup feature.

Roles and Global Catalogs

You will need to check the positioning of Operations Master Roles and Global Catalogs. Remember that Infrastructure Master should not be placed on a Global Catalog. Seize roles from servers you won't be restoring. Make sure all workstations can reach at least one global catalog.

WINS and DNS

If WINS has trouble starting you will need to delete all files from C:\WINNT\SYSTEM32\WINS, then restart the service. If DNS Servers are not restored then recursive queries to DNS will fail making the snap in for DNS think the server has failed. The only solution would be to purge DNS of all old records.

Authoritative Restore

An Authoritative restore operation would be necessary when it is necessary to revert the entire Domain and Directory to an earlier state from a backup. Restore the backup either normally as

above or with “Primary” selected. Reboot the machine in directory services restore mode. Use NTDSUtil to perform the authoritative restore. Reboot the computer on the network in place of the original machine being replaced. The other Domain Controllers will synchronize to the Authoritative machine through the replication process. Records which have been added, will be deleted, records which were deleted or changed, will revert to their former state.

Known Issues

DNS Must Be Installed

Before restoring your Domain Controller, you must install the DNS component. If DNS is not installed, it will not work after the restore.

Replacing a Domain Controller

It is preferable to demote a Domain Controller prior to replacement. If this is done successfully, you need only to install Server + Service Pack and run DCPROMO. You can even give the new DC the same name if the old is permanently removed from the Network.

Restoring a Forest

When restoring a forest, whether one domain or several you need to meet several requirements. You need at least one Global Catalog (which can be for the entire forest), and at least one Domain Controller from each Domain. All roles must be present for the Forest and each Domain. Your order of restore should be dictated by number of roles held. In a multi-domain forest you would start by restoring the role holding DCs of the parent domain (which will hold the forest-wide roles) and then seizing any roles held by non-restored DCs, then work your way down the pyramid.

Time Synchronization

When you restore your Domain, time synchronization may suffer. The DC which holds PDC Emulator is also the default time-source for the domain, the PDCE for the root Domain is the master time-source for the child domains. If any servers had been directed through "net time set sntp" to non-synchronized or unavailable time sources, Active Directory will develop severe problems as the clocks separate. Synchronize the Root Domain PDCE to a reliable time-source and do not set time-sources on other servers so they will all go with the PDCE.

Revision History

Authored June 4, 2001 by John Karr with assistance from Tom Creegan.

Minor formatting and content revisions September 5, 2002 by John Karr.