Directory Backup and Restore

Overview

Active Directory is backed up as part of system state, a collection of system components that depend on each other. You must backup and restore system state components together.

Components that comprise the system state on a domain controller include:

- **System Start-up Files (boot files).** These are the files required for Windows Server to start.
- **System registry.**
- **Class registration database of Component Services.** The Component Object Model (COM) is a binary standard for writing component software in a distributed systems environment.
- **SYSVOL.** The system volume provides a default Active Directory location for files that must be shared for common access throughout a domain. The SYSVOL folder on a domain controller contains:
    - NETLOGON shared folders. These usually host user logon scripts and Group Policy objects (GPOs) for non-Windows 2000based network clients.
    - User logon scripts for Windows 2000 Professionalbased clients and clients that are running Windows 95, Windows 98, or Windows NT 4.0.
    - Windows 2000 GPOs.
    - File system junctions.
    - File Replication service (FRS) staging directories and files that are required to be available and synchronized between domain controllers.
- **Active Directory.** Active Directory includes:
    - Ntds.dit: The Active Directory database.
    - Edb.chk: The checkpoint file.
    - Edb*.log: The transaction logs, each 10 megabytes (MB) in size.
    - Res1.log and Res2.log: Reserved transaction logs.

General Guidelines for Backup

The backup tool in Windows Server supports multiple types of backup: *normal*, *copy*, *incremental*, *differential*, and *daily*. However, because Active Directory is backed up as part of system state, the only type of backup available for Active Directory is *normal*. A normal backup creates a backup of the entire system state while the domain controller is online. In addition, the backup tool marks each file as a backed up file, which clears the archive attribute of the file.

Considerations for ensuring a good backup

To ensure a successful restore from backup, you must know what defines a *good backup*.

Which domain controllers to back up

At a minimum, back up two domain controllers in each domain, one of which should be an operations master role holder (excluding the relative ID (RID) master, which should not be restored). Note that backup data from a domain controller can only be used to restore that domain controller. You cannot use a backup of one domain controller to restore another.

Contents

A good backup includes at least the system state and the contents of the system disk. Backing up the system disk ensures that all the required system files and folders are present so you can successfully restore the data.

Age

A backup that is older than the tombstone lifetime set in Active Directory is not a good backup. At a minimum, perform at least two backups within the tombstone lifetime. The default tombstone lifetime is 60 days. Active Directory incorporates the tombstone lifetime into the backup and restore process as a means of protecting itself from inconsistent data.

Deleting an object from Active Directory is a two-step process. When an object is deleted in Active Directory, the object gets converted into a tombstone, which is then replicated to the other domain controllers in the environment to inform them of the deletion. Active Directory purges the tombstone when the tombstone lifetime is reached.

If you restore a domain controller to a state prior to the deletion of an object, and the tombstone for that object is not replicated to the restored domain controller before the tombstone expires, the object remains present only on the restored domain controller, resulting in inconsistent data. Thus, you must restore the domain controller prior to expiration of the tombstone, and allow inbound replication from a domain controller containing the tombstone to complete prior to expiration of the tombstone.

Active Directory protects itself from restoring data older than the tombstone lifetime by disallowing the restore. As a result, the useful life of a backup is equivalent to the tombstone lifetime setting for the enterprise.

How to Select the Appropriate Restore Method

You select the appropriate restore method by considering:

- Circumstances and characteristics of the failure. The two major categories of failure, from an Active Directory perspective, are Active Directory data corruption and hardware failure. Active Directory data corruption occurs when the directory contains corrupt data that has been replicated to all domain controllers or when a large portion of the Active Directory hierarchy has been changed accidentally (such as deletion of an OU) and this change has replicated to other domain controllers.
- Roles and functions of the failed server.

Non-authoritative restore of Active Directory

A non-authoritative restore returns the domain controller to its state at the time of backup, then allows normal replication to overwrite that state with any changes that have occurred after the backup was taken. After you restore the system state, the domain controller queries its replication partners. The replication partners replicate any changes to the restored domain controller, ensuring that the domain controller has an accurate and updated copy of the Active Directory database.

Non-authoritative restore is the default method for restoring Active Directory, and you will use it in most situations that result from Active Directory data loss or corruption. To perform a non-authoritative restore, you must be able to start the domain controller in Directory Services Restore Mode.

Non-authoritative restore of SYSVOL

When you non-authoritatively restore the SYSVOL, the local copy of SYSVOL on the restored domain controller is compared with that of its replication partners. After the domain controller restarts, it contacts its replication partners, compares SYSVOL information, and replicate the any necessary changes, bringing it up-to-date with the other domain controllers within the domain.

Perform a non-authoritative restore of SYSVOL if at least one other functioning domain controller exists in the domain. This is the default method for restoring SYSVOL and occurs automatically if you perform a non-authoritative restore of the Active Directory.

If no other functioning domain controller exists in the domain, then perform a primary restore of the SYSVOL. A primary restore builds a new File Replication service (FRS) database by loading the data present under SYSVOL on the local domain controller. This method is the same as a non-authoritative restore, except that the SYSVOL is marked primary.

Authoritative restore of Active Directory

An authoritative restore is an extension of the non-authoritative restore process. You must perform the steps of a non-authoritative restore before you can perform an authoritative restore. The main difference is that an authoritative restore has the ability to increment the version number of the attributes of all objects in an entire directory, all objects in a subtree, or an individual object (provided that it is a leaf object) to make it authoritative in the directory. Restore the smallest unit necessary, for example, do not restore the entire directory in order to restore a single subtree.

As with a non-authoritative restore, after a domain controller is back online, it will contact its replication partners to determine any changes since the time of the last backup. However, because the version number of the object attributes that you want to be authoritative will be higher than the existing version numbers of the attribute held on replication partners, the object on the restored domain controller will appear to be more recent and therefore will be replicated out to the rest of the domain controllers within the environment.

Unlike a non-authoritative restore, an authoritative restore requires the use of a separate tool, Ntdsutil.exe. No backup utilities— including the Windows 2000 Server system tools— can perform an authoritative restore.

An authoritative restore will not overwrite new objects that have been created after the backup was taken. You can authoritatively restore only objects from the configuration and domain-naming contexts. Authoritative restores of schema-naming contexts are not supported.

Perform an authoritative restore when human error is involved, such as when an administrator accidentally deletes a number of objects and that change replicates to the other domain controllers and you cannot easily recreate the objects. To perform an authoritative restore, you must start the domain controller in Directory Services Restore Mode.

Authoritative restore of SYSVOL

By authoritatively restoring the SYSVOL, you are specifying that the copy of SYSVOL that is restored from backup is authoritative for the domain. After the necessary configurations have been made, Active Directory marks the local SYSVOL as authoritative and it is replicated to the other domain controllers within the domain.

The authoritative restore of SYSVOL does not occur automatically after an authoritative restore of Active Directory. Additional steps are required.

As with Active Directory authoritative restore, you typically perform an authoritative restore of SYSVOL when human error is involved and the error has replicated to other domain controllers. For example, you might perform an authoritative restore of SYSVOL if an administrator has accidentally deleted an object that resides in SYSVOL, such as a Group Policy object.

Recover a domain controller through reinstallation

To recover a domain controller through reinstallation, you do not restore the system state from backup media; instead, you reinstall Windows, install Active Directory, and allow replication partners to bring the recovered domain controller up to date.

Recovering a domain controller through reinstallation can quickly return the computer to service if the following conditions exist:

- A domain controller has failed and you cannot restart in Directory Services Restore mode. If failure was caused by a hardware failure, you have resolved the hardware problem (for example, by replacing the disk).
- There are other domain controllers in the domain, to serve as replication partners.
- The computer is functioning only as a domain controller (it does not run other server services such as Exchange), and it does not contain other data that needs to be recovered from a backup.

Restore a domain controller through reinstallation and restore from backup

This method involves first reinstalling Windows 2000, to enable you to start in Directory Services Restore Mode. During the Windows 2000 Server setup process, you will obtain more information about the nature of the failure and you can then determine whether you can reinstall Windows 2000 Server into the same partition as it was previously installed or whether you will need to re-partition the drive. After you successfully reinstall Windows 2000, you can start in Directory Services Restore Mode and perform a normal non-authoritative restore from backup media.

Restore a domain controller through reinstallation and restore the system state from backup if the following conditions exist:

- A domain controller has failed and you cannot restart in Directory Services Restore mode. If failure was caused by a hardware failure, you have resolved the hardware problem (for example, by replacing the disk).
- You have the following information about the failed domain controller:
    - Disk configuration. You need a record of the volumes and sizes of the disks and partitions. You use this information to recreate the disk configuration in the case of a complete disk failure. You must recreate all disk configurations prior to restoring system state. Failure to recreate all disk configurations can cause the restore process to fail and can prevent you from starting the domain controller following the restore.
    - Computer name. You need the computer name to restore a domain controller of the same name and avoid changing client configuration settings.
    - Domain membership. You must know the domain name because even if the computer name does not change, you might need to re-establish a new computer account.
    - Local Administrator password. You must know the local computer's Administrator password that was used when the backup was created. Without it, you will not be able to log on to the computer to establish a domain account for the computer after you restore it. If you are not part of the domain, you will not be able to log on by using a domain account, even if you are a domain administrator. The local Administrator password is also required to restore the system state on a domain controller.

- The domain controller is running other server services such as Exchange, or contains other data you must restore from a backup.
- You have a good backup, made within the tombstone lifetime.

Backup and Restore Tasks and Procedures

Table 1.8 shows the tasks and procedures for backup and restore.

Table 1.8 Backup and Restore Tasks and Procedures

Tasks	Procedures	Tools	Frequency
Back up Active Directory and associated components.	• Back up system state on a domain controller. • Back up system state and system disk on a domain controller.	• NTBackup.exe	At least twice within the tombstone lifetime
Perform a non-authoritative restore.	• Restart the domain controller in Directory Services Restore Mode (locally or remotely). • Restore from backup media. • Verify Active Directory restore.	• NTBackup.exe • Ntdsutil.exe • Event Viewer • Repadmin.exe	As needed
Perform an authoritative restore of a subtree or leaf object.	• Restart in Directory Services Restore Mode. • Restore from backup media for authoritative restore. • Restore system state to an alternate location. • Perform authoritative restore of the subtree or leaf object. • Restart in normal mode. • Restore applicable portion of SYSVOL from alternate location. • Verify Active Directory restore.	• NTBackup.exe • Ntdsutil.exe • Event Viewer • Repadmin.exe	As needed
Perform an authoritative restore of the entire directory.	• Restart in Directory Services Restore Mode. • Restore from backup media for authoritative restore. • Restore system state to an alternate location. • Restore the database. • Restart in normal mode. • Copy SYSVOL from alternate location.	• NTBackup.exe • Ntdsutil.exe • Event Viewer • Repadmin.exe	As needed

	• Verify Active Directory restore.		
Recover a domain controller through reinstallation.	• Clean up metadata. • Install Windows 2000 Server. • Install Active Directory.	• Ntdsutil.exe • Active Directory Sites and Services • Active Directory Users and Computers • Dcpromo.exe	As needed
Restore a domain controller through reinstallation and subsequent restore from backup.	• Install Windows 2000 Server on the same drive letter and partition as before the failure, partitioning the drive if necessary. • Restore from backup media (non-authoritative restore). • Verify Active Directory restore.	• NTBackup.exe	As needed

Reference:

http://technet.microsoft.com/en-us/library/bb727048%28d=printer%29.aspx