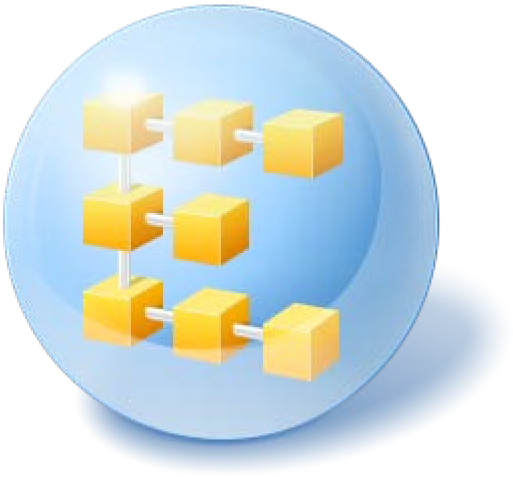
Acronis

COMPUTE WITH CONFIDENCE

WWW.ACRONIS.COM



Active Directory backup and restore with Acronis Backup & Recovery 10

Table of Contents

1. Introduction

Microsoft Active Directory is a central component of the Windows platform, which can be found in any size of Windows environment. Active Directory contains critical information, availability of which is important for businesses to operate.

This white paper is created to enable system administrators to implement their own recovery solution for Active Directory using Acronis Backup & Recovery 10 software.

2. Backup and Recovery overview

Microsoft Active Directory (AD) services use a database located on the file system of a domain controller. If more than one domain controller is available, the information stored in the database is constantly replicated between multiple domain controllers.

A Windows component called Volume Shadow Copy Service (VSS) is used to create a consistent copy of the AD database.

Active Directory recovery scenarios may consist of recovery of a crashed domain controller, recovery of a corrupted AD database, and restoring of accidentally deleted or modified AD records. Required operations and tools may vary depending on the type of information that needs to be restored, and availability of other domain controllers.

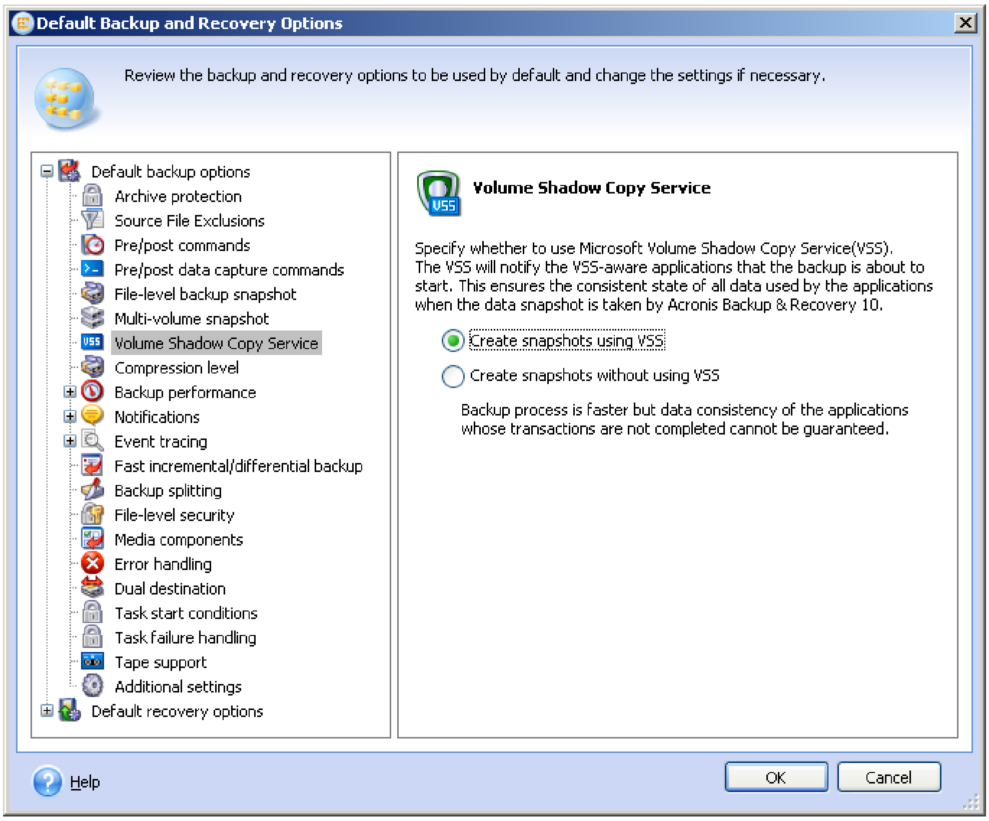
3. Active Directory backup

In Windows (including Windows 2003 and Windows 2008), the Active Directory database is typically located in the **%systemroot%\NTDS** folder (such as C:\Windows\NTDS) of a domain controller. While this location is used by default, it is configurable. The **Ntdsutil** command-line utility may help you to find the current location. Note that the database and the transaction logs may be stored on different volumes, so be sure both are included in the backup.

Because Active Directory service is almost always running, VSS should be used to ensure consistency of the files after the backup. Without VSS, the files would be in a so-called crash-consistent state – that is, after the restore, the system would be in the same state as if the power were disconnected at the moment when backup began.

While such backup is good enough for most applications, databases (including the Active Directory database) may not be able to start from a crash-consistent state, and would require manual recovery.

To avoid that, make sure the **Create snapshots using VSS** option is selected in the backup settings when creating a backup of a domain controller:



Review the backup and recovery options to be used by default and change the settings if necessary.

Volume Shadow Copy Service

Specify whether to use Microsoft Volume Shadow Copy Service(VSS). The VSS will notify the VSS-aware applications that the backup is about to start. This ensures the consistent state of all data used by the applications when the data snapshot is taken by Acronis Backup & Recovery 10.

● Create snapshots using VSS

○ Create snapshots without using VSS

Backup process is faster but data consistency of the applications whose transactions are not completed cannot be guaranteed.

***Note:** This option is not selected by default, so be sure to select it.*

Once you have a full backup of your domain controller, the backup stores the information that is required to later restore your Active Directory.

The next question is how often you need to back up the domain controller. Microsoft recommends performing at least two backups within the tombstone lifetime – which is, depending on the version of the operating system, where your domain has been created, 60 or 180 days. We'll discuss the tombstone lifetime and its impact on the ability to restore later in this document – but as a bare minimum, back up at least monthly.

To summarize, the following needs to be done in order to perform complete Active Directory database backup:

- Make sure that at least one of your domain controllers is backed up.
- Make sure that your most up-to-date backup of the domain controller is not older than half of the tombstone lifetime (not older than 30 days in most cases). It doesn't matter if the latest backup is full or incremental – you can perform successful restore from either. You just have to have one.
- Create a backup immediately in any of the following events, as the existing backups may become not good enough for successful restore:
    - Active Directory database and/or log have been moved to a different location.
    - An operating system on the domain controller is upgraded, or a service pack is installed.
    - A hotfix that changes the AD database is installed.
    - The tombstone lifetime is changed administratively.

- Make sure that the Active Directory database folder is included into the backup. The easiest way to do this is to create a full image backup of your system drive, and drives where AD database and transaction logs are located.
- Make sure that files making up the AD database (.dit, .chk, .log files) are not in the exclusion list.
- Make sure that the **Create snapshots using VSS** option is selected for the backup.

4. Active Directory recovery

As mentioned above, the AD recovery would differ, depending on what type of recovery is required. Moreover, in some cases you even don't need to touch your domain controller backup – all the information required for the recovery is already available.

In order to cover major AD recovery scenarios, let's consider the following disaster scenarios:

- Domain controller is lost, other domain controllers are available.
- All domain controllers are lost (or there was only one).
- Active Directory database is corrupted and AD service doesn't start.
- Certain information is accidentally deleted from the Active Directory.

4.1. Domain Controller restore (other DCs are available)

When one of the domain controllers is lost, the AD service is still available. Therefore, other domain controllers will contain data which is more up-to-date than the data in the backup. For example, if a user account has been created in the AD after the backup was taken, the backup won't contain this account.

Thus, we want to perform a recovery which will not affect the current state of the Active Directory – this operation is called nonauthoritative restore.

Active Directory records are constantly replicated between the domain controllers. At any given moment, the same record may contain a certain value on one domain controller, and a different value on another. To prevent conflicts and loss of information, AD uses incrementing versions (called Update Sequence Number – USN) attached to every AD object. USNs are used to determine the direction of replication – records with greatest USN are considered as most up-to-date, and replicated to other servers.

During nonauthoritative restore, the AD is restored from the database with the original USN stored in the backup.

Live domain controllers cannot have AD records with a USN that is smaller than the one contained in the backup – since a USN is always increasing in value. Thus, the AD records from the backup have little value during such restore – more up-to-date records from other domain controllers will overwrite them during the replication.

Moreover, it is not mandatory to restore AD in this recovery scenario at all. To restore the domain controller functionality, it is sufficient to re-create the domain controller itself (using the **dcpromo.exe** tool). Once replication completes, the domain controller will be up and running again.

To summarize, the following steps should be completed in order to restore a domain controller when other DCs are available:

1. Restore the domain controller from the backup using bare-metal restore.
2. Reboot the domain controller. Make sure the Active Directory service has started successfully.

No other steps are required. Replicating of AD records will be performed automatically.

So what if the only backup available is older than the tombstone lifetime? If it includes the operating system, it still may be restored. The AD database from the backup, however, cannot be used. The tombstone objects are used during the replication – namely, object deletion is replicated through replication of tombstones. Thus, if the backup is older than the tombstone lifetime, proper replication will be impossible. If you don't have a newer backup, recreation of the DC becomes the only possible way to recover.

4.2. Domain Controller restore (no other DCs are available)

If all domain controllers are lost (or there was only one DC in the domain, which has crashed), the AD service is down. Unless the DC may be recovered by other means (without using backup), the most up-to-date information available is the one stored in the backup.

Therefore, nonauthoritative restore de facto becomes authoritative: the objects restored from backup (and their USNs) are the newest available. Other than that, the restore looks similar to the previous scenario, with the exception that recreation of the AD is not an option anymore, since all the information will be lost, and even a backup with an expired tombstone lifetime can be used – although the information loss will be very significant in this case.

To summarize, the following steps should be completed when restoring the last/the only domain controller:

1. Make sure the newest available backup is used for restore. This is especially important, since all the information created since the last backup will be lost. If your domain has only one domain controller, it is a good idea to create a backup at least daily.
2. Restore the domain controller from the backup using bare-metal restore.
3. Reboot the computer. Make sure the Active Directory service has started successfully.

4.3. Active Directory database restore

If the AD database gets corrupted (on the file level, rather than on the AD logic/schema level) and AD service on a domain controller refuses to start or crashes, several things may be done that do not involve restoring data from the backup.

If other domain controllers are available, this domain controller may be demoted and then promoted again using the **dcpromo.exe** tool. During this procedure, the data will be replicated and the AD database will be recovered. The complexity of the entire procedure depends on whether the domain controller is still able to start in normal mode. If it is, you can simply use the **dcpromo /forceremoval** command to remove AD service from the computer. If it is not, a more complex procedure is required – detailed instructions can be found in Microsoft KB articles http://support.microsoft.com/kb/332199/ and http://support.microsoft.com/kb/258062.

If no other domain controllers are available, the data needs to be restored from a backup. One of the ways to do this is to restore the domain controller completely – like in the scenario described in

"Domain Controller restore (no other DCs are available) (p. 6)". This method guarantees complete recovery, and it is reasonable to use it if the domain controller has no other valuable data but the Active Directory itself, or other valuable data is easy to save (e.g. located on another volume that doesn't need to be restored).

Another way is to recover the AD database alone.

The AD database consists of the following files:

1. **NTDS.dit** (database file)
2. **Edb.chk** (checkpoint file)
3. **Edb*.log** (transaction logs)
4. **Res1.log** and **Res2.log** (reserve transaction logs)

By default, these files are located in the **%systemroot%\NTDS** folder – however, the location is configurable, so be sure to check this. Also, if any changes have been made to the GPO, the SYSVOL system volume (**%systemroot%\SYSVOL**) needs to be restored as well.

The entire process will look like this:

1. If no other DCs are available, make sure the newest available backup is used for restore. This is especially important, since all the information created since the last backup will be lost.
2. Reboot the domain controller into Directory Services Restore mode.
3. Create a copy of your AD database files.
4. Restore the files from the backup (use file level restore from an image-level backup to accomplish that).
5. Reboot the computer. Make sure the Active Directory service has started successfully.

4.4. Recovery of accidentally deleted information

An example of accidentally deleted information includes an unintentionally deleted user or computer account.

There are two different ways how such modification may be rolled back.

First, the most obvious method is to restore the AD database from the backup. If you have only one domain controller (and thus any restore becomes authoritative), be ready to lose any changes made since the last backup when using this method. Availability of other domain controllers will give you a bit more flexibility. To perform authoritative restore of certain entries only, perform the following steps:

1. Similarly to the steps from the previous scenario, reboot the domain controller into the Directory Service Restore mode, and perform restore of the AD database.
2. Without rebooting the computer, run **ntdsutil** and type **authoritative restore** in its command prompt.
3. Type the corresponding **restore** command, such as **restore subtree** or **restore object** to perform authoritative restore of the required object (refer to **ntdsutil** documentation for more information). To restore the entire database, use **restore database**.

4. Reboot the computer. Make sure the Active Directory service has started successfully, and the restored object becomes available.

Another way to restore accidentally deleted object is by using tombstones. In AD, any deleted object is retained for a period of time (called tombstone lifetime, as discussed above). This period is, by default, at least 60 days. That means that any object, even though deleted from AD, will remain in its database for at least 60 days before it will be finally erased.

Using this method, the backups are not used, and AD remains available during the recovery – there is no need to reboot a domain controller. There are several tools that perform such recovery; many of them are available for free. For example, a command line tool from Windows Sysinternals called **adrestore** can browse and restore deleted objects. Another example is a freeware tool from MVP Guy Teverovsky called **ADRestore.NET**. This tool has a graphical user interface and may be easier to use. For more information, please refer to the documentation supplied with the appropriate tools.

5. Summary

Acronis Backup & Recovery 10 is a powerful backup and recovery solution, which may efficiently protect any Windows server, including Active Directory servers/domain controllers. Image-level backup technology implemented in the product allows efficient recovery of many databases, including Microsoft Active Directory.