Active Directory backup and restore with Acronis Backup & Recovery 11

Technical white paper

Applies to the following editions:

- þ Advanced Server
- þ Virtual Edition
- þ Advanced Server SBS Edition
- o Advanced Workstation
- o Server for Linux
- þ Server for Windows
- o Workstation

Table of contents

1 Introduction

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

This white paper provides information to enable system administrators to implement their own recovery solutions for Active Directory by using the Acronis Backup & Recovery 11 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 include the recovery of a crashed domain controller, recovery of a corrupted AD database, and restoring accidentally deleted or modified AD objects. The required operations and tools may vary depending on the type of information that needs to be restored, and the availability of other domain controllers.

3 Active Directory backup

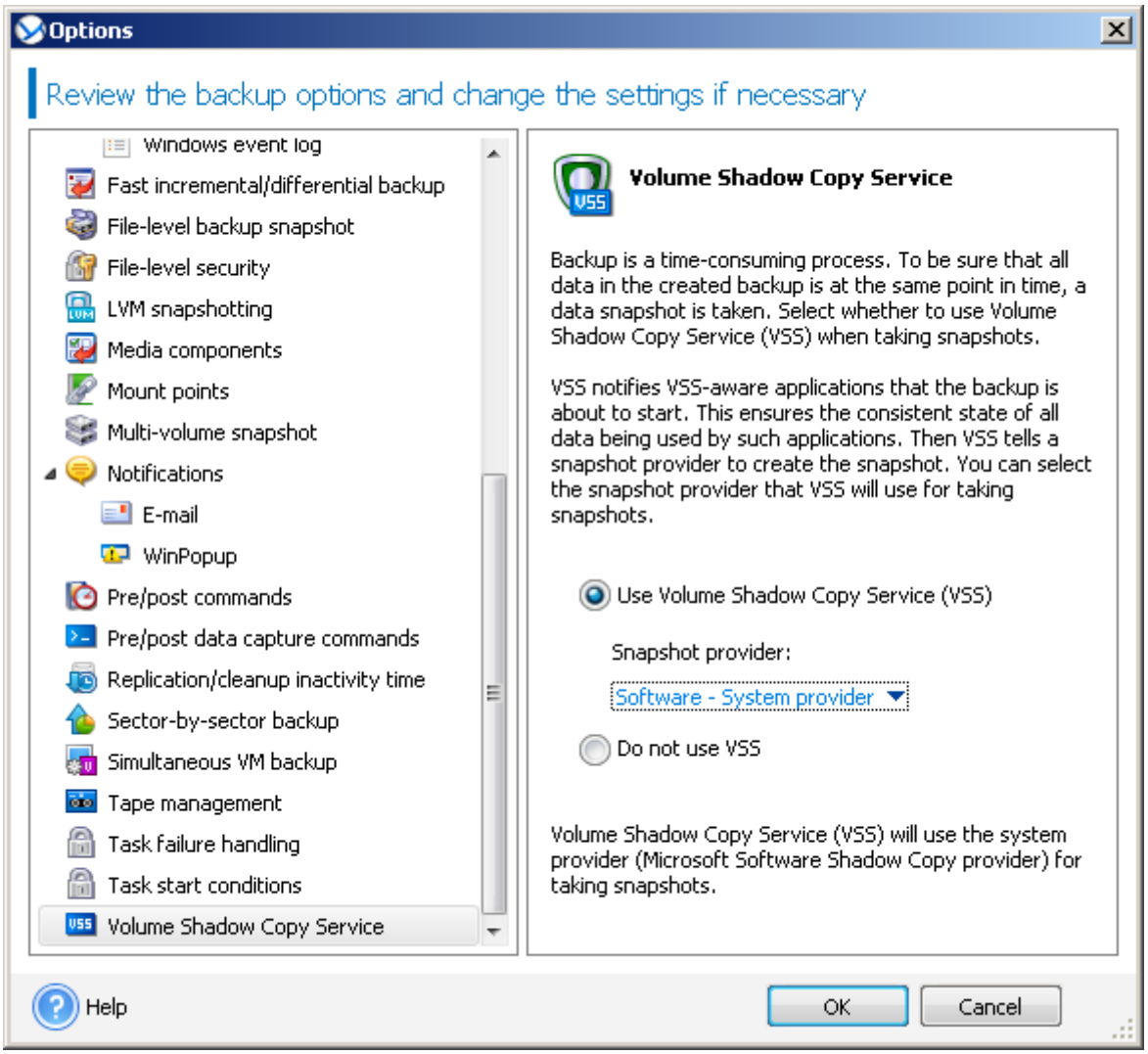
In Windows (including Windows 2003 and Windows 2008), the Active Directory database is typically located in the **%systemroot%\NTDS** folder (such as C:\Windows\NTDS) of a domain controller. While this location is used by default, it is configurable. The **Ntdsutil** command-line utility may help you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

We recommend that you back up the domain controller's system volume, boot volume, and the volumes where the AD database and transaction logs are located. The resulting backup will contain all the information required to recover the domain controller to bare metal and restore your Active Directory.

Because the Active Directory service is almost always running, Volume Shadow Copy Service (VSS) should be used to ensure consistency of the files in 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 backups are good enough for most applications, databases (including the Active Directory database) may not be able to start from a crash-consistent state and could require manual recovery.

To avoid that, make sure the **Use Volume Shadow Copy Service (VSS)** option is selected in the backup options when creating a backup of a domain controller. In **Snapshot provider**, select **Software - System provider**. Acronis Backup & Recovery 11 will use the Microsoft Software Shadow Copy provider. This ensures that the Active Directory database is backed up in a consistent state.



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. However, as a bare minimum, back up at least monthly.

To summarize, the following needs to be done in order to perform a 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. In most cases, the tombstone lifetime is 60 days, so the backup must be not older than 30 days. It doesn't matter if the latest backup is full or incremental – you can perform a successful restore from either one.

- Create a backup immediately upon any of the following events, as a successful restore of the Active Directory from the existing backups may be impossible:
  - Active Directory database and/or log were moved to a different location.
  - An operating system on the domain controller was upgraded, or a service pack was installed.
  - A hotfix that changes the AD database was installed.
  - The tombstone lifetime was changed administratively.
- Make sure that files making up the AD database (.dit, .chk, .log files) are not in the exclusion list.
- Make sure that the **Use Volume Shadow Copy Service (VSS)** option is selected for the backup.

4 Active Directory recovery

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

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

- A domain controller is lost but other domain controllers are still available. See "Domain Controller restore (other DCs are available)" (p. 5).
- All domain controllers are lost (or there was only one). See "Domain Controller restore (no other DCs are available)" (p. 7).
- Active Directory database is corrupted and the AD service doesn't start. See "Active Directory database restore" (p. 7).
- Certain information is accidentally deleted from the Active Directory. See "Restoring accidentally deleted information" (p. 8).

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.

About replication of Active Directory data

Active Directory data is constantly replicated between the domain controllers. At any given moment, the same Active Directory object may have a newer version on one domain controller and an older version on another. To prevent conflicts and loss of information, Active Directory tracks object versions on each domain controller and replaces the outdated versions with the up-to-date version.

Thus, the AD objects from the backup have little value – more up-to-date objects from other domain controllers will overwrite them during the replication.

Steps to perform

When other DCs are available, you can perform nonauthoritative restore of a lost domain controller in either of the following ways:

- *Recover a domain controller* from a backup.
- *Recreate a domain controller* by installing the operating system and making the computer a new domain controller (using the **dcpromo.exe** tool).

Both operations are followed by automatic replication. Replication makes the domain controller database up-to-date. Just make sure the Active Directory service has started successfully. Once replication completes, the domain controller will be up and running again.

Recovery vs. re-creation

Recreation does not require having a backup. Recovery is normally faster than recreation but it is not possible in the following cases:

- All available backups are older than the tombstone lifetime. Tombstones are used during replication to ensure that an object deleted on one domain controller becomes deleted on other domain controllers. Thus, proper replication is not possible after the tombstones have been deleted.
- The domain controller held a Flexible Single Master Operations (FSMO) role, and you have assigned that role to a different domain controller (seized the role). In this case, restoring the domain controller would lead to two domain controllers holding the same FSMO role within the domain and cause a conflict.

Recreating a domain controller that holds a FSMO role

Some domain controllers hold unique roles known as Flexible Single Master Operations (FSMO) roles or operations manager roles. A domain controller can hold multiple FSMO roles. However, two domain controllers within the same domain cannot hold the same FSMO role. Some FSMO roles must be held by a single domain controller within the whole collection of domains known as a forest. For the description of FSMO roles and their scopes (domain-wide or forest-wide), see Microsoft Help and Support article http://support.microsoft.com/kb/324801.

Before recreating a domain controller that held the PDC Emulator role, you must seize that role. Otherwise, you will not be able to add the recreated domain controller to the domain. After recreating the domain controller, you can transfer this role back. For information about how to seize and transfer FSMO roles, see Microsoft Help and Support article http://support.microsoft.com/kb/255504.

To view which FSMO roles are assigned to which domain controller, you can connect to any live domain controller by using the **ntdsutil.exe** tool as described in Microsoft Help and Support article http://support.microsoft.com/kb/234790. Follow the steps in the "Using the NTDSUTIL Tool" section of that article:

- For the Windows 2000 Server and Windows Server 2003 operating systems, follow all steps as they are given.
- For the Windows Server 2008 operating systems, in the step asking you to type **domain management**, type **roles** instead. Follow other steps as they are given.

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 and this DC has crashed), the AD service is down. Therefore, nonauthoritative restore de facto becomes authoritative: the objects restored from backup are the newest available. Replication of AD data cannot take place since there are no live DCs. This means that:

- Changes to AD that occurred after the backup had been made, will be lost.
- Recreation of the DC is not an option.
- Even a backup with an expired tombstone lifetime can be used.

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

1. Make sure the newest available backup is used for recovery. 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. Recover the domain controller from the backup.
3. Reboot the computer. Make sure the Active Directory service has started successfully.

4.3 Active Directory database restore

If the AD database becomes corrupted on the file level rather than on the AD logic/schema level, there are several solutions 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 Help and Support 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 way to do this is to restore the domain controller completely. The procedure is similar to the scenario described in “Domain Controller restore (no other DCs are available)” (p. 7). This method guarantees complete recovery and is reasonable to use if the domain controller has no other valuable data but the Active Directory itself or if the 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 to restore with the newest available backup. This is especially important, since all the information created after 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 restore from a disk-level backup to accomplish that).
5. Reboot the computer. Make sure the Active Directory service has started successfully.

4.4 Restoring accidentally deleted information

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

There are two different ways to roll back such modification.

Restoring the entire database

The most obvious method is to restore the AD database from the backup. As in the previous scenario, reboot the domain controller into the Directory Services Restore mode and restore the AD database.

If you have only one domain controller (and thus any restore becomes authoritative), be ready to lose any changes made after the last backup when using this method.

The availability of other domain controllers enables you to perform authoritative restore of certain objects only. Other objects will be replicated from other controllers when you reboot the controller in the normal mode. This way, you will restore the unintentionally deleted objects and keep the other objects up-to-date. Having restored the AD database from the backup, be sure to perform the following steps:

1. Without rebooting the computer, run **ntdsutil** and type **authoritative restore** in its command prompt.
2. 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**.
3. Reboot the computer. Make sure the Active Directory service has started successfully and that the restored object becomes available.

Using tombstones

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