Windows Server 2012 AD Backup and Disaster Recovery Procedures

Peter Van Keymeulen, 2013
EDE Consulting
ICT Infrastructure Architect

Version: 1.2
1. Contents

1. CONTENTS ......................................................................................................................... 2
2. CONTACT INFORMATION ............................................................................................... 4
3. VERSION CONTROL ......................................................................................................... 5
4. TERMS AND ABBREVIATIONS .......................................................................................... 5
5. INTRODUCTION ............................................................................................................... 6
6. SCOPE ............................................................................................................................... 6
7. AGREEMENTS .................................................................................................................... 6
8. ACTIVE DIRECTORY CONTENT BACKUP AND RESTORE METHODS ........................................ 7
  8.1 System State Backup ..................................................................................................... 7
    8.1.1 Why, despite the Recycle Bin Feature? ................................................................. 7
    8.1.2 Backup Modes ....................................................................................................... 8
    8.1.3 Backup Targets ..................................................................................................... 8
    8.1.4 Backup Versioning .............................................................................................. 8
  8.2 Active Directory Recycle Bin ....................................................................................... 9
  8.3 Active Directory Snapshot Backups ........................................................................... 11
  8.4 Tombstone Reanimation ............................................................................................ 11
  8.5 Virtual Machine Snap Shots ..................................................................................... 11
9. INSTALLING AND CONFIGURING BACKUPS .................................................................. 12
  9.1 System State Backup ................................................................................................. 12
  9.2 Snapshot Backups ..................................................................................................... 13
    9.2.1 Manual Snapshots ............................................................................................. 13
    9.2.2 Scheduled Snapshots ....................................................................................... 14
  9.3 Enable Active Directory Recycle Bin ........................................................................ 14
  9.4 Configuring Garbage collection process .................................................................... 15
    9.4.1 Without Recycle Bin ....................................................................................... 15
    9.4.2 With Recycle Bin ............................................................................................ 16
10. WHEN TO RESTORE ........................................................................................................ 16
11. WHERE TO RESTORE .................................................................................................... 17
12. COMMON TASKS ............................................................................................................. 17
    12.1 Remove Domain Controller from DNS .................................................................. 17
    12.2 Remove Domain Controller from Active Directory .............................................. 17
    12.3 Change the Active Directory Restore Mode (DSRM) Administrator Password .... 19
    12.4 Restore your Backups files to restore from .......................................................... 19
    12.5 How to Disable Initial Replication .......................................................................... 20
    12.6 Verification of a Successful Restore ....................................................................... 21
    12.7 Verification of a Successful Backup ....................................................................... 21
13. ACTIVE DIRECTORY CONTENT RECOVERY ................................................................... 21
    13.1 Overview ................................................................................................................. 21
      13.1.1 Authoritative Restore ...................................................................................... 22
      13.1.2 Non-Authoritative Restore .............................................................................. 22
    13.2 Recovery through System State Backup .................................................................. 22
      13.2.1 Non-Authoritative Restore .............................................................................. 22
      13.2.2 Authoritative Restore .................................................................................... 23
    13.3 Recovery through tombstone object reanimation .................................................... 25
      13.3.1 Authoritative Restore through LDP.exe ......................................................... 25
      13.3.2 Authoritative Restore through ADRestore.exe ............................................. 26
    13.4 Active Directory Recovery through Snapshots ....................................................... 27
    13.5 Active Directory Restore through Recycle Bin ...................................................... 28
      13.5.1 Restore Through AD Administrative Center ................................................. 28
      13.5.2 Restore Through Power Shell ....................................................................... 28
    13.6 Restoring Back-Links ............................................................................................. 30
      13.6.1 Restore group memberships through NTDSUTIL and LDIFF ...................... 30
      13.6.2 Restore security principals two times ............................................................ 31
14. ENTIRE DOMAIN CONTROLLER RECOVERY ............................................................ 31

2/46
2. Contact Information

“IT” doesn’t matter
Even in our fast growing world of technology, IT became a commodity the same way as electricity did. It’s not the software, hardware or technologies that will make the difference, but the way how you design, implement, maintain and use it. Speaking personally, as an architect, software, hardware and technology “as such” are not that important. They are only a way to create a stable, reliable and secure IT infrastructure to meet all your business and technical needs. Cost reductions, flexibility and future scalability are key words in every project I’m involved with.

EDE Consulting
EDE Consulting was formed in 2006. Though a young company, all our IT professionals are senior consultants with 10 to 20 years of experience in IT business. EDE Consulting has extensive experience with everything related to enterprise system management, network management, system migration and integration, and this at consultancy, architectural and implementation level.
While you take care of your core business, EDE Consulting looks after your IT infrastructure. We think beyond the technical aspects of IT. If, for example, we design a disaster recovery procedure, this procedure includes all documentation, personal procedures, access lists, and so on.
Among our current customers you will find: Fortis, Dexia, ING, Oleon, AGF, KUL, Vodafone Germany, RIZIV, Besix, ...

EDE Consulting bvba
Beverstraat 19
9500 Geraardsbergen
BE-0881.137.013
www.edeconsulting.be

Peter Van Keymeulen
ICT Infrastructure Architect
peter.vankeymeulen@edeconsulting.be
+32 (0)473 98 62 99

http://www.linkedin.com/pub/peter-van-keymeulen/3/531/783
3. Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Status</th>
<th>Date</th>
<th>Authors</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>Initial</td>
<td>17.09.2012</td>
<td>Van Keymeulen Peter</td>
<td></td>
</tr>
<tr>
<td>V1.1</td>
<td>Update</td>
<td>15.04.2013</td>
<td>Van Keymeulen Peter</td>
<td></td>
</tr>
<tr>
<td>V2.2</td>
<td>Update</td>
<td>17.12.2013</td>
<td>Van Keymeulen Peter</td>
<td></td>
</tr>
</tbody>
</table>

4. Terms and Abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>BIA</td>
<td>Business Impact Analysis</td>
</tr>
<tr>
<td>ADDS</td>
<td>Active Directory Domain Services</td>
</tr>
<tr>
<td>VSS</td>
<td>Volume Shadow Copy</td>
</tr>
<tr>
<td>MOSS</td>
<td>Microsoft Office SharePoint Server</td>
</tr>
<tr>
<td>SCCM</td>
<td>System Center Configuration Manager</td>
</tr>
<tr>
<td>SCOM</td>
<td>System Center Operations Manager</td>
</tr>
<tr>
<td>EPO</td>
<td>ePolicy Orchestrator</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>IPV6</td>
<td>IP version 6</td>
</tr>
<tr>
<td>RPC</td>
<td>Remote Procedure Call</td>
</tr>
<tr>
<td>WINS</td>
<td>Windows Name Service</td>
</tr>
<tr>
<td>NTDS</td>
<td>NT Directory Service - Active Directory database</td>
</tr>
<tr>
<td>DFSR</td>
<td>Distributed File System Replication</td>
</tr>
<tr>
<td>UNC</td>
<td>Universal Naming Convention (path)</td>
</tr>
<tr>
<td>SRV</td>
<td>DNS server record</td>
</tr>
<tr>
<td>CNAME</td>
<td>DNS canonical name record</td>
</tr>
<tr>
<td>FSMO</td>
<td>Flexible Single Master Operation</td>
</tr>
<tr>
<td>PDC</td>
<td>Primary Domain Controller Master</td>
</tr>
<tr>
<td>RID</td>
<td>Relative ID Master</td>
</tr>
<tr>
<td>INFR</td>
<td>Infrastructure master</td>
</tr>
<tr>
<td>GC</td>
<td>Global Catalog</td>
</tr>
<tr>
<td>SCHEM</td>
<td>Schema Master</td>
</tr>
<tr>
<td>DOM</td>
<td>Domain Naming Master</td>
</tr>
<tr>
<td>NT5DS</td>
<td>Windows Time Protocol</td>
</tr>
</tbody>
</table>
5. Introduction

It must be somewhere in the late nineties, after struggling with Windows NT 4 domains for years, that I became involved with the Windows 2000 Academy developed and organized @ Digital. The very first impressions about Active Directory caused me to fell of my chair several times a day, surprised that I was about this technology. Although Windows 2003 and 2008 were necessary and useful releases, I waited till Windows 2012 to get exactly the same wow feeling as fifteen years ago while discovering all new Windows Server 2012 features.

Yet, Active Directory, still is a core infrastructure layer in your organization, storing all enterprise wide user and computer accounts, your Exchange and mailbox configurations, Lync related objects, SCCM and SCOM objects, AD integrated DNS ... and used as authentication and authorization service.

Active Directory became so important and mission critical for your business that it forces you to understand, implement and test efficient and reliable backup and disaster recovery procedures.

This document deals with Active Directory related backup and disaster recovery aspects as they exists in the Server 2012 RTM, build 9200 release.

6. Scope

This document tackles all possible scenarios, mechanisms and techniques related to Active Directory Backup and Disaster Recovery.

V1 version contained the following items:

- Active Directory Content Backup and Restore through System State
- Active Directory Content Backup and Restore through Tombstone Reanimation
- Active Directory Content Backup and Restore through the recycle bin
- Active Directory Content Backup and Restore through snapshot
- Active Directory Domain Controller Backup and Restore through Virtual Machine Snap Shot
- SYSVOL restore
- FSMO roles restore
- Restore an Entire Forest
- Restore an Entire Domain

7. Agreements

All Windows Power Shell commands using in this document are written down as:

```
Add-WindowsFeature windows-server-backup -IncludeAllFeature
```

All Windows Command Line Commands are written down as:

```
Wbadmin enable backup -addtarget:<target> -schedule:21:00 -systemstate -quiet
```
8. Active Directory Content backup and restore methods

There are several methods for Active Directory and domain controller backup and Recovery:

- Through System State
- Through the recycle bin
- Through snapshot backups
- Through Tombstone Reanimation
- Through Virtual Machine Snap Shot

8.1 System State Backup

As from Windows Server 2008, the OS includes a new backup application named Windows Server Backup. Windows Server Backup replaces the good old NTBACKUP.EXE and is not installed by default. You must install it by using the Add Features option in Server Manager before you can use the Wbadmin.exe command-line tool or Windows Server Backup on the Administrative Tools menu. In Windows Server 2012, the system components that make up system state data depend on the server roles that are installed on the computer.

The system state data includes at least the following data, plus additional data, depending on the server roles that are installed:

- Registry
- COM+ Class Registration database
- Boot files
- Active Directory Certificate Services (AD CS) database
- Active Directory database (Ntds.dit)
- SYSVOL directory
- Cluster service information
- Microsoft Internet Information Services (IIS) metadirectory
- System files that are under Windows Resource Protection
- Active Directory Federation Services
- ...

When you use Windows Server Backup to back up the critical volumes on a domain controller, the backup includes all data that resides on the volumes that include the following:

- The volume that hosts the boot files, which consist of the Bootmgr file and the Boot Configuration Data (BCD) store
- The volume that hosts the Windows operating system and the registry
- The volume that hosts the SYSVOL tree
- The volume that hosts the Active Directory database (Ntds.dit)
- The volume that hosts the Active Directory database log files

8.1.1 Why, despite the Recycle Bin Feature?

Did you ever try the new Recycle bin feature in Windows 2012? Just right-click the deleted object and select restore. Simpler, easier or faster object recovery isn’t possible. So, why should I still make System State Backups and consume storage space for my backup files? It’s because you can run into situations where the recycle bin isn’t reachable:

- To use the recycle bin, you need to be able to log on to the domain. This isn’t possible when you lost the entire domain.
When someone deletes group memberships without deleting the accounts and groups involved, only a system state restore can be used to restore the memberships. Membership deletions “as such” are not stored in the deleted objects because they aren’t objects, they are only attributes. Deleting group memberships only updates attributes.

Imaging someone only changes a huge amount of attributes and objects in your AD without deleting anything. Only a System State restore can be used to recover.

8.1.2 Backup Modes

- Manual backup
  A member of the Administrators group or the or Backup Operators group can initiate a manual backup by using Server Backup or the Wbadmin.exe command-line tool each time that a backup is needed.

- Scheduled backup
  A member of the Administrators group can use the Windows Server Backup or the Wbadmin.exe command-line tool to schedule backups. The scheduled backups must be made on a local, physical drive that does not host any critical volumes or on any remote share. Allowing backing up onto system critical volumes can no longer be forced through registry settings as it was in Windows 2008 and 2008R2. Wbadmin scheduled backups can have local disks as well as a remote share as backup target.

8.1.3 Backup Targets

Windows Server 2012 supports the following backup Targets for System State Backups:

- All Windows 2012 volume types are supported: NTFS and ReFS.
- UNC path to the local server, even if it’s a shared folder on a critical disk, which is, of course, not a good idea. This is a VSS Copy Backup by default.
- UNC path to remote server. This is a VSS Copy Backup by default.
- Local Non-Critical Volume. Any local connected disk can be used to store system states backups as long the volume is not part of the systems state backup. The volume can be created on top of a physical local disk or on top of a storage pool. This is a VSS Copy Backup by default.
- Local Critical Volumes. This is no longer supported, even if you add the AllowSSBToAnyVolume parameter to the registry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wbengine\SystemStateBackup
Name: AllowSSBToAnyVolume
Data type: DWORD
Value data: 1
```

For more information about this Windows Server 2008 and 2008R2 parameter, please refer to: [http://support.microsoft.com/kb/944530](http://support.microsoft.com/kb/944530)

8.1.4 Backup Versioning

Depending on the commands used to schedule the backup job or the backup target location, backups are made differently:
Except from the first backup, System State backups are by default always differential.

A scheduled System State backup to an UNC path is always differential and only the latest version can be viewed and restored. So, no versioning on UNC path based System State Backups. The backup target folder will be renamed every time a new backup starts.

A manual started System State backup to an UNC path is always differential and only the latest version can be viewed and restored. So, no versioning. The backup target folder will be renamed every time a new backup starts.

A scheduled System State backup to a local non-critical volume is always differential, only one backup target folder exists but versioning is enabled. The backup target folder name contains the last backup date. The folder will be automatically renamed with each backup.

A Manual started System State backup to a local non-critical volume is always differential by default, only one backup target folder exists but versioning is enabled. The backup target folder name contains the last backup date. The folder will be automatically renamed with each backup.

Versioning is only possible with local volume targets.

A manual full backup (-vssful -allcritical) is never possible, regardless the target type (UNC or Volume)

Although “–vssful” forces a full backup, only the delta’s are written down to disk. What actually happen is that VSS updates each file’s history to reflect that is was backed up.

### Differential and Full Backup Target

<table>
<thead>
<tr>
<th>Backup Target</th>
<th>Scheduled</th>
<th>Manual</th>
<th>Scheduled</th>
<th>Manual</th>
<th>Versioning</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNC Path</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>X</td>
<td>NO</td>
</tr>
<tr>
<td>Local Disk</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>X</td>
<td>YES</td>
</tr>
</tbody>
</table>

#### 8.2 Active Directory Recycle Bin

Active Directory Recycle Bin helps minimize directory service downtime by enhancing your ability to preserve and restore accidentally deleted Active Directory objects without restoring Active Directory data from backups, restarting Active Directory Domain Services (AD DS), or rebooting domain controllers.

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion. For example, restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains.

When Active Directory Recycle Bin has not been enabled, objects are stripped down and marked Tombstoned. The Garbage collection process will delete these objects when the Tombstone Life Time has been expired.

![Diagram](image)

**Fig. 1** without Recycle Bin

When the Active Directory Recycle Bin has been enabled, deleted object are no longer tombstoned but they receive a “Deleted” status. In this status, all attributes are preserved. Objects are in the Recycled status when the deleted life time expires. In this status, most of the attributes are stripped of and lost. This is the equivalent state of a tombstoned object in Windows 2003. The garbage collection process physically deletes the object from the AD database when the Recycled Life Time has been expired.

Both life time parameters are configurable.

![Diagram](image)

**Fig. 2** with Recycle Bin

**Using the recycling bin to restore deleted objects, please keep in mind that:**

- You can’t restore objects from which the parent object has been deleted. If you delete an OU, together with all child objects (user objects for example), it’s not possible to restore the user accounts without first restoring the OU (the user account object parent), unless you restore the object into another location.
- Using the Active Directory Administrative Center, you can restore an object to any location into your directory, regardless the object’s original location.

---

1 Source: Microsoft Technet

2 Source: Microsoft Technet
Using the Active Directory Administrative Center, you can select multiple objects to restore at once, but child objects are not restored automatically if you only select the parent OU object. You have to select the child objects as well.

You cannot use the recycle bin to restore group memberships should someone only deletes or change group memberships without deleting the users or groups involved.

8.3 Active Directory Snapshot Backups

As from Windows Server 2008, a new feature has been added allowing administrators to create snapshots of the Active Directory database for offline use. With AD snapshots you can mount a backup of AD DS under a different set of ports and have read-only access to your backups through LDAP. There are quite a few scenarios for using AD snapshots. For example, if someone has changed properties of AD objects and you need to revert to their previous values, you can mount a copy of a previous snapshot to an alternate port and easily export the required attributes for every object that was changed. These values can then be imported into the running instance of AD DS. You can also restore deleted objects or simply view objects for diagnostic purposes.

AD snapshots, when mounted and connected to, allow you to see how the AD Database looked like at the moment of the snapshot creation, what objects existed and other type of information. However, out of the box, it does not allow you to move or copy items or information from the snapshot to the live database. In order to do that you will need to manually export the relevant objects or attributes from the snapshot, and manually import them back to the live AD database.

Active Directory Snapshots are not created to use as a real restore mechanism. It’s more a way to find differences in Active Directory over time without the need to reboot a domain controller into the AD restore mode and restore the entire or parts of the database authoritatively.

8.4 Tombstone Reanimation

All previous backup and restore methods are using backups or snapshots to start from. But what are the possibilities when there are no backups at all and the recycle bin has not been enabled yet? A deleted Active Directory object isn’t physically deleted from the database, it’s just Tombstoned, moved to the Deleted Items container in AD and hidden from any tool or MMC snap-in. In opposite to the AD recycle bin, not all object attributes are preserved, some of them were deleted when Tombstoned.

Tombstone reanimation changes the deleted objects attributes directly in the AD database and isn’t something you should do often, it’s really a worst case scenario.

8.5 Virtual Machine Snap Shots

Domain controllers use USNs together with the invocation IDs to track updates that must be replicated between replication partners in an Active Directory forest. Source domain controllers use USNs to determine what changes have already been received by the destination domain controller that is requesting changes. Destination domain controllers use USNs to determine what changes should be requested from source domain controllers. The invocation ID identifies the version or the instantiation of the Active Directory database that is running on a given domain controller. When Active Directory is restored on a domain controller by using the APIs and methods that Microsoft has designed and tested, the invocation ID is correctly reset on the restored domain controller. Domain controllers in the forest receive notification of the invocation reset. Therefore, they adjust their high watermark values accordingly.
Microsoft does not support any other process that takes a snapshot of the elements of a Windows Server 2003, 2008 and 2008R2 Active Directory domain controller's system state and copies elements of that system state to an operating system image. Unless an administrator intervenes, such processes cause a USN rollback. This USN rollback causes the direct and transitive replication partners of an incorrectly restored domain controller to have inconsistent objects in their Active Directory databases.

As from Windows Server 2012, Microsoft introduces a new mechanism to protect the Active Directory against an USN rollback, when restoring virtual server snapshots outside the control of the OS, by meaning of a new attributed on the domain controller computer account object: msDS-GenerationId, called the VM-Generation Id.

**VM-Generation ID**

Virtualized domain controller cloning relies on the hypervisor platform to expose an identifier called VM-Generation ID to detect creation of a virtual machine. AD DS initially stores the value of this identifier in its database during domain controller promotion. When the virtual machine boots up, the current value of the VM-Generation ID from the virtual machine is compared against the value in the database. If the two values are different, the domain controller resets the Invocation ID and discards the RID pool, thereby preventing USN re-use or the potential creation of duplicate security-principals.

At the time of writing, only Windows 2012 Hyper-V supports the VM-Generation ID and domain controller snapshot restores from within the hypervisor.

*For more information about USN rollback:*
[http://support.microsoft.com/kb/875495](http://support.microsoft.com/kb/875495)

*For more information about domain controller virtualization architecture:*

### 9. Installing and Configuring Backups

#### 9.1 System State Backup

The Windows Server 2012 Backup features are not installed by default.

**To install the Windows Backup features:**

- Logon to the system with at least domain controller local administrator privileges
- From the Power Shell prompt, execute the following commands:
  ```
  add-windowsfeature windows-server-backup -includeallsubfeature
  [enter]
  ```

**To Remove the Windows Backup features from the server:**

- Logon to the system with at least domain controller local administrator privileges
- From the Power Shell prompt, execute the following commands:
  ```
  remove-windowsfeature windows-server-backup [enter]
  ```

**To schedule the System State Backup:**

- Logon to the system with at least domain controller local administrator privileges
- From the command prompt, execute the following command:
**Wbadmin enable backup -addtarget:<target> -schedule:21:00 –systemstate –quiet**

- The above command is enough to create a reliable and useful backup of Active Directory. However, it’s possible to schedule a FULL system (VSS Full Backup) system state backup that can be used in case of a full bare metal restore. To schedule, from the command prompt, run the following command:

  **Wbadmin enable backup -addtarget:<target> -schedule:21:00 –systemstate –quiet –allcritical -vssfull**

To create a manual one shot System State Backup:

- Logon to the system with at least domain controller local administrator privileges
- From the command prompt, execute the following command:

  **Wbadmin start systemstatebackup –backuptarget :<drive> -quiet**

- The –vssfull and –allcritical Wbadmin parameters are not supported with the start systemstatebackup command.

To find out all System State Backups stored on your domain controller:

- Logon to the system with at least domain controller local administrator privileges
- From the command prompt, execute the following command:

  **Wbadmin get versions**

To get the status or a view of the running System State Backup:

- Logon to the system with at least domain controller local administrator privileges
- From the command prompt, execute the following command:

  **Wbadmin get status**

### 9.2 Snapshot Backups

Active Directory Snapshots are made through NTDSUtil. NTDSUtil can be used to create a one-time Snapshot backup of your Active Directory as well as a scheduled Snapshot backup mechanism.

#### 9.2.1 Manual Snapshots

To manually create and view Active Directory Snapshots:

- Logon to the system with at least domain controller local administrator privileges
- From the command prompt, start **NTDSUtil**
- To activate the current instance of NTDS, type: **Activate Instance NTDS**
- Enter: **snapshot** to change to the snapshot part of NTDSUtil
- Enter: **create** to create a snapshot
- Enter: **list all** to view all current snapshots. This command does not only list the snapshots made by NTDSUtil, but all snapshots, those made by your system state backups too.
9.2.2 Scheduled Snapshots

NTDSUtil can be used in an automated way of working by putting all commands on one single command line. This command line can be scheduled through the Windows OS build-in scheduling service.

To launch a snapshot with a one step, one line command:

- Logon to the system with at least domain controller local administrator privileges
- From the command prompt, initiate the following command:

`ntdsutil snapshot "activate instance ntds" create quit quit`

9.3 Enable Active Directory Recycle Bin

First, to be able to enable and use the Active Directory Recycle Bin, your Forest and Domain Functional level should be at least Windows Server 2008 R2 level. Be aware that with Windows Server 2008, you can roll back the forest and domain functional level elevation as long as you didn’t enable the Recycle Bin. This feature will be disabled when the Recycle Bin becomes active.

Second, be aware that enabling the recycle bin is an irreversible operation. Once enabled, you can never disable it again.

You must prepare the forest and the domain before enabling the Active Directory Recycle Bin if you upgraded an existing pre-Windows 2008 R2 operating system to Windows 2008 R2 or Windows 2012. Prepare the forest by executing the `adprep /forestprep` on the Schema Master. Prepare the domain by executing the `adprep /domainprep /gpprep` on the infrastructure master. And finally, upgrade both, the domain and functional level to at least Windows Server 2008 R2.

To enable the Active Directory Recycle Bin through Active Directory Administrative Center:

- Open the Active Directory Administrative Center
- From the right pane, select Enable Recycle Bin

To enable the Active Directory Recycle Bin through Power Shell:

- From the Administrative Tools, start the Active Directory Module for Windows PowerShell
- Execute the following command:

```
Import-module ActiveDirectory
Enable-ADOptionalFeature -Identity <ADOptionalFeature> -Scope <ADOptionalFeatureScope> -Target <ADEntity>
```

Where `<ADOptionalFeature>` is the DN of the option you want to enable, `<ADOptionalFeatureScope>` is the scope: domain or forest, `<ADEntity>` is the name of the domain or forest

For example:

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=edeconsulting,DC=local' -Scope Forest -Target 'edeconsulting.local'
```
9.4 Configuring Garbage collection process

Deleted objects are not physically removed from the ADS database. They are marked as deleted and physically removed from the database by the garbage collection process after a well-defined set of time frames. As mentioned in 8.2 Active Directory Recycle Bin, the garbage collection process time frames depends on whether you use the Recycle Bin or not.

Garbage collection time frames are very important. As a general rule, you always should have at least one ADS system state backup younger than the Tombstone lifetime.

9.4.1 Without Recycle Bin

In this situation, only the Tombstone Life Time can be configured. The Tombstone Life Time is a forest wide setting in the configuration naming context of Active Directory.

- In Windows Server 2000, 2003 and 2003 R2, the Tombstone Lifetime is 60 days by default when the tombstoneLifetime value is “<not set>”. Microsoft recommends setting the tombstoneLifetime manually to 180 days when upgrading from Windows Server 2000, 2003 and 2003 R2.
- In Windows Server 2003 SP1, 2003 SP2, 2008 and 2008 R2 the Tombstone Lifetime is 180 days by default when the tombstoneLifetime value is “<not set>”.
- In a new deployed Windows 2012 forest, the tombstoneLifetime attribute is explicitly set to 180 days by default.

To change the Tombstone Life Time via ADSIedit:

- Open a new ADSIedit mmc console
- Connect to the configuration naming context
- Navigate to cn=directory service,cn=windows nt,cn=services,cn=configuration
- Right click on the cn=Directory Service and select properties
- Navigate to the tombstoneLifetime attribute
- Add the number of days

To change the Tombstone lifetime by using the Set-ADObject cmdlet

- Open the Active Directory Module for Windows PowerShell running in an Administrator security context.
- Type the following command:

```
Set-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=<…>,DC=<…>" -Partition "CN=Configuration, DC=<…>,DC=<…>" -Replace:@{"tombstoneLifetime" = <value>}
```

Where D"C=<…>“ contains the domain name and “<value>” contains the number of days.

To get the Tombstone lifetime using Power Shell

- Open the Active Directory Module for Windows PowerShell running in an Administrator security context.
- Type the following command:
9.4.2 With Recycle Bin

With the Recycle Bin enabled, two different time settings can be configured: the Deleted Object Lifetime and the Recycled Object Lifetime.

The deleted object lifetime is represented by the value of the msDS-deletedObjectLifetime attribute. The recycled object lifetime is represented by the value of the legacy tombstoneLifetime attribute. In Windows 2012, by default, msDS-deletedObjectLifetime is set to <not set>. When msDS-deletedObjectLifetime is set to null, the deleted object lifetime is set to the value of the recycled object lifetime. By default, the recycled object lifetime, which is stored in the tombstoneLifetime attribute, is set to 180.

Please refer to “9.4.1. Without Recycle Bin” to know how to configure the tombstone lifetime.

To change the deleted object lifetime by using the Set-ADObject cmdlet

- Open the Active Directory Module for Windows PowerShell running in an Administrator security context.
- Type the following command:

```
Set-ADObject -Identity "CN=Directory Service,CN=Windows NT, CN=Services, CN=Configuration, DC=<...>,DC=<...>" -Partition "CN=Configuration, DC=<...>,DC=<...>" -Properties @{ "msDS-deletedObjectLifetime" = <value> }
```

Where D"C=<...>" contains the domain name and “<value>” contains the number of days.

10. When to Restore

When an object is deleted in Windows 2012, the DC from which the object was deleted informs the other DCs in the environment about the deletion by replicating what is known as a tombstone (if the recycle bin isn’t enabled) or Deleted (with recycle bin).

A tombstone or deleted object is a representation of an object that has been deleted from the directory. The tombstone object is removed by the garbage collection processes, based on the tombstone lifetime setting, which by default is set to 180 days by default in Windows 2012. A Deleted object will be recycled after the “Recycle object lifetime”, which is by default equal to the tombstone lifetime, or 180 days in Windows 2012.

A backup older than the tombstone lifetime set in Active Directory is not considered to be a good backup.

Active Directory protects itself from restoring data older than the tombstone lifetime. For example, let’s assume that we have a user object that is backed up. If after the backup the object is deleted, a replication operation is performed to the other DCs and the object is replicated in the form of a tombstone. After 180 days, all the DCs remove the tombstone as part of the garbage collection process. This is a process routinely performed by DCs to clean up their copy of the database.

If you attempt to restore the deleted object after 180 days, the object cannot be replicated to the other DCs in the domain because it has a USN that is older than the level required to trigger
replication. And the other DCs cannot inform the restored DC that the object was deleted, so the result is an inconsistent directory.

11. Where to Restore

Never restore a system state from ServerA on hardware ServerB while ServerA is still up and running. The system state restore will restore the registry from the original server which causes duplicate names on the network. Moreover, you’ll end-up with a domain with two identical domain controllers, same names, same GUIDs and same connection objects. This causes the NTDS service to exclude both, the original and the restored server, from AD replication.

Since the system state contains drivers for network and Raid controller hardware, never restore a system state backup on servers with other hardware than the original server.

Never restore a system state backup which is older than the tombstone lifetime because this can create lingering objects. Linger objects can occur if a domain controller does not replicate for an interval of time that is longer than the tombstone lifetime (TSL). The domain controller then reconnects to the replication topology. Objects that are deleted from the Active Directory service when the domain controller is offline can remain on the domain controller as lingering objects.

For more information about lingering objects:
http://support.microsoft.com/kb/910205

12. Common Tasks

This part of the document contains tasks which are used in almost every type of restore. References to these tasks are made throughout the document.

12.1 Remove Domain Controller from DNS

All DNS records are removed from DNS automatically when demoting a domain controller. This is not the case should the domain controller goes down and never come back on line. To recover from this situation, all A, PTR, SRV and CNAME records should be deleted from DNS.

Ask your local DNS team to remove the domain controller from DNS. Remind them that they have to:

- Delete the A and PTR record form the DNS zone for which this server was a Domain Controller.
- Delete the A record for the domain for which this server was a Domain controller.
- Delete all SRV records for the domain controller in his own zone and the zone of the root domain.
- Delete the CNAME record for the domain controller.
- Delete the A record from the gc._msdcs.<FQDN> DNS zone of the root domain if the domain controller was a global catalog.

12.2 Remove Domain Controller from Active Directory

During this process, you have to know the name of two servers, the server you want to remove, and the Domain Controller (from the same domain) from which you want to remove this server.

To remove a Domain Controller from Active Directory:
Start, on the command prompt on a remaining domain controller, `ntdsutil`. Type, without the quotes: "m c" and press return to enter the meta cleanup part of ntdsutil. Type: "c" and press return to enter the connection part. Type: "Connect to server <servername>" where the server name is the name of the remaining domain controller, not the name of the server you have to remove from the directory. Type: "Q" (and return) to leave the connection part. Type: "s o t" to enter the “Select Operation Target” part of ntdsutil Type: "list sites" to get all existing sites for the forest Type: "select site <number>" Where the number should be the number of the site on which the “to be removed” server is located. Type: "list domains in site" to get all domains on that site. Type: "select domain<number>" where the number should be the number of the domain for which the “to be removed” server was a domain controller. Type: "list servers for domain in site" to get all domain controllers for the selected domain on the selected site. Type: "select server <number>" where the number should be the number of the “to be removed” server Type: “Q” to leave the “select operation target” part of ntdsutil. Type: “remove selected server”. Confirm the deletion of the server from Active Directory. Close ntdsutil

Depending of the situation from which you want to recover from, the tools to use might be different.

When there are still other domain controllers of the same domain active:

- Open the MMC “Active Directory Site and Services Settings” snap-in and select the site from which you deleted the domain controller.
- Select the “to be removed” server and delete this object from AD.
- On each server, remove all connection objects coming from the removed server.
- Open the MMC “Active Directory Users and Computers” snap-in and select the domain from which you removed the server.
- From the View menu, select “Advanced Features”.
- In right pane, navigate to the “System” container
- Select the “DFSR-GlobalSettings” container
- Select the “Domain System Volume” container
- Select the “Topology” container and be sure that the removed server doesn’t have an object in this container. If it does, remove it.
- Return to the root of the domain.
- Remove the domain controller’s computer account from the “Domain Controller” container (if it still exists).
- If MOM has been used to monitor Active Directory, Remove the domain controller’s account from “MOMLatencyMonitors”.
- If SCOM has been used to monitor Active Directory, Remove the domain controller’s account from “OpsMgrLatencyMonitors”.

If you’re working on the last remaining domain controller, use ADSI Edit:

- Start MMC and open the ADSI snap-in
Windows Server 2012 AD Backup and Disaster Recovery Procedures

- From the left pane, right click on “ADSI Edit”, select “connect to”
- In the computer part of the window, enter the domain name for which the DC serves as a domain controller and select OK.
- In right pane, navigate to the “System” container.
- Select the “DFSR-GlobalSettings” container.
- Select the “Domain System Volume” container.
- Select the “Topology” container and be sure that the removed server doesn’t have an object in this container. If it does, remove it.
- Return to the root of the domain.
- Remove the domain controller’s computer account from the “Domain Controller” OU (if it still exists).
- If MOM has been used to monitor Active Directory, Remove the domain controller’s account from “MOMLatencyMonitors”.
- If SCOM has been used to monitor Active Directory, Remove the domain controller’s account from “OpsMgrLatencyMonitors”.
- From the left pane, right click on “ADSI Edit”, select “connect to”
- In the “Select the well-known naming context” part of the window, select “Configuration” and OK.
- In the right pane, navigate to the “sites” container.
- Select the site of the domain controller you want to remove.
- Select “servers” container.
- Select the DC name of the DC you want to remove.
- Select “NTDS Settings” container.
- Delete all connection objects from this container, if any.
- Move back one level (up) to the “NTDS Settings” container and delete the “NTDS Settings” container.
- Move back one level (up) to the domain controller container for the DC you want to remove and delete the domain controller (despite the warning).
- Close ADSI edit.

12.3 Change the Active Directory Restore Mode (DSRM) Administrator Password

Change Directory Services Restore Mode Administrator password if you don’t know it. Every domain administrator can change the DSRM Administrator Password. This account and password can only be used on a Domain Controller booted in the “Active Directory Restore mode”.

To change the password:

- Start, on the command prompt, ntdsutil
- Type, without the quotes: “set dsrm password” and press return to enter the DSRM part of ntdsutil.
- Type: “Reset Password on server <servername>”, where servername is the name of the Domain Controller on which we have to perform an AD recovery operation.
- Enter the new administrator password.
- Confirm the new administrator password.
- Close ntdsutil.

12.4 Restore your Backups files to restore from

Backups are created using Windows Backup and stored locally on the domain controller. Offsite backups of these Windows Backup backup files should be made as well, for DRP reasons.
Imagine that you have only one domain controller, which is not preferable, on which you make Windows Backup based system state backups stored on a local hard drive. This hard drive, in turn, has been backed up with a third party product (think about BackupExec or Tivoli ...) to maintain backups of our VSS backup volume offsite.

Some disaster happens and you install new server hardware to be restored as the original domain controller somewhere on another location. How should you proceed when you recovered your backup files from your third party backup system onto the local hard drive of your new installed server? Your server will not be aware of these backups since they were not created on that server. There is a great change that Windows Backup is not even installed.

**To make the backups accessible for Windows Backup:**

- Install Windows Backup, reconstruct the backup catalog using the wbadmin command and recover your system state
  - To restore the catalog
    ```
    Wbadmin restore catalog –backuptarget:<location>
    ```
  - To get version from which you want to restore
    ```
    Wbadmin get versions
    ```

For the Catalog process to be successful, the path to the backup files should start at the level where WindowsImageBackup is in the path. If you copy the backup files to a local attached disk, the structure should be as follows:

```
<localdrive>:\WindowsImageBackup<computername>\...
```

This will not work:

```
c:\serverbackups\win2k8<computername>\...
```

### 12.5 How to Disable Initial Replication

A domain controller from a domain with more than one domain controller only advertise himself as being a domain controller when he was able to perform a first initial replication with another domain controller at boot time.

If this is the first domain controller and it is a Windows 2012 operating system. Then you need to add a registry key to avoid AD DS being unavailable until it has completed replication of a writeable directory.

Create the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\NTDS\Parameters\
Name: Repl Perform Initial Synchronizations
Data type: DWORD
Value data: 0
```

After the forest is recovered completely, you must reset the value of this entry to 1, which requires a domain controller that restarts and holds operations master roles to have successful AD DS inbound and outbound replication with its known replica partners before it advertises itself as domain controller and starts providing services to clients.
12.6 Verification of a Successful Restore
To verify the success of a restore, use the following basic tests:

- Reboot in normal mode. If the domain controller is able to successfully boot into normal mode, it means that the directory is able to successfully initialize. Especially if it wasn’t able to do so before it was rebooted.
- Check if both, the NETLOGON and SYSVOL share are created. If so, the SYSVOL was successfully published to the other domain controllers.
- Check the Directory Service Event log for any messages.
- Check if the domain controller is able to replicate with its neighbors.
- Check if the domain controller is able to authenticate with its neighbors.

A very useful toll to verify AD replication status can be downloaded from Microsoft.

**Microsoft Active Directory Replication Status Tool**

12.7 Verification of a Successful Backup
System restores are as good as your backups. Using Repadmin, you can get the information about the most recent backup made into your forest, for each of the name spaces. On the command prompt (any DC in the forest), start the following command:

```
Repadmin /showbackup
```

13. Active Directory Content Recovery
13.1 Overview
The only circumstances in which you should have to recover the content of the directory is when someone, accidentally or on purpose, deleted parts from the directory or when a failing procedure made incorrect changes.

**There are five Replication Naming Contexts in Active Directory:**

- Domain naming context
- Configuration Naming Context
- Schema Naming Context
- Global Catalog
- Application Partition

Domain, Configuration and Application Partitions replication context are restorable through the System State restore and Snap Shot restore. Global Catalog recovery is possible by restoring the AD, but not really necessary. It’s not possible to restore the Schema Naming Context unless you destroy your entire forest and restore one domain controller of the root domain, deletes all other domain controllers and restage them ad additional domain controller in your restored forest.

**When restoring AD, two possible types of restore exist:**

- Authoritative restore
- Non-Authoritative
13.1.1 Authoritative Restore

An authoritative restore is, in essence, an extension of the non-authoritative restore process. That is, it requires all the steps of a non-authoritative restore before it can be initiated. The authoritative restore distinguishing characteristic is that it increments the version number of an entire directory, a sub tree, or individual objects (provided that they are leaf objects) to mark them as authoritative in the directory.

As with a non-authoritative restore, once a DC is back online, it contacts its replication partner(s) to see what has changed since the last backup. But because the version number of the object(s) restored is higher than the existing instances of those objects held on replication partner(s), the objects on the restored DC appear to be more recent and, therefore, must be replicated out to the rest of the DCs within the environment. (By default, version numbers are incremented by 100,000 under the authoritative restore process.)

Because of this, the authoritative restoration method is typically used when human error is involved, such as when an administrator has accidentally deleted an OU.

Unlike a non-authoritative restore, an authoritative restore requires the use of a separate application: NTDSUTIL.

An authoritative restore does not overwrite new objects created after the backup occurred. An authoritative restore can be carried out only on objects from the configuration and domain contexts. The authoritative restore of schema components is not supported, unless you remove all exiting domain controllers in the forest and restore an older version.

13.1.2 Non-Authoritative Restore

Non-authoritative restore is the default method for the restoration of Active Directory, and is used for the majority of restore operations. Using this method, the settings and entries that existed in the Domain, Schema, Configuration, and (optionally) Global Catalog naming contexts maintain the version number they had at the time of backup.

After a non-authoritative restore, the DC is updated using normal replication techniques. That is, if the version number of an object is less than the same object’s version number stored by its replication partner(s) (indicating the object has changed since it was last backed up), the object on the restored server is updated. This ensures an up-to-date version of the database.

Keep in mind that when a non-authoritative restore restores an object that has been deleted in the time between the backup and the restore, the object will be restored but deleted again by the replication once the restored domain controller becomes online. This because the deleted object is not physically deleted, but marked as being deleted on all remaining domain controllers.

13.2 Recovery through System State Backup

13.2.1 Non-Authoritative Restore

To restore the entire AD or parts of it non-authoritatively:

- Be sure you know the Active Directory Restore Mode Administrator Password. If not, please refer to: 12.2. Change the Active Directory Restore Mode (DSRM) Administrator Password
- To boot an existing domain controller, or new staged Windows 2012 server into the “Active Directory Restore Mode”: 
- Logon to the system using an account with at least local administrative rights
- From the command prompt, execute the following task:
  
  \textit{Bcdedit /set safeboot dsrepair}

- Reboot the server
- Logon to the system using the DSRM account and password
- Start a command prompt
- On the command prompt, execute the following command:

  \textit{wbadmin get versions}

  \textit{wbadmin start systemstaterecovery –version:<version> -quiet}

  \text{example: wbadmin start systemstaterecovery –version:07/27/2010-09:25 –quiet}

- Once the SystemState restore has been finished, select \textit{Y} to reboot the system
- Logon to the system using the DSRM account and password
- Wait till the restore process has been finished.
- To disable the “Active Directory Restore Mode” boot option, execute the following command on the command prompt:

  \textit{Bcdedit /deletevalue safeboot}

- Reboot the System

13.2.2 Authoritative Restore

Restoring Active Directory content authoritatively follows the same process as a non-authoritatively restore plus some additional tasks.

To restore the Domain Naming Context or parts of it authoritatively:

- Be sure you know the Active Directory Restore Mode Administrator Password. If not, please refer to: \textit{12.3. Change the Active Directory Restore Mode (DSRM) Administrator Password}
- To boot an existing domain controller, or new staged Windows 2012 server into the “Active Directory Restore Mode”:

  - Logon to the system using an account with at least local administrative rights
  - From the command prompt, execute the following task:
    \textit{Bcdedit /set safeboot dsrepair}
  - Reboot the server

  - Logon to the system using the DSRM account and password
  - Start a command prompt
  - On the command prompt, execute the following command:

    \textit{wbadmin get versions}
Once the SystemState restore has been finished, select **Y** to reboot the system
Logon to the system using the DSRM account and password
Wait till the restore process has been finished.
From the command prompt, start ntdsutil and execute all of the following commands:

- **Activate instance ntds**
- **Authoritative Restore**
  - To restore one object: **Restore Object “<distinguished name>”**
  - To restore object and all child objects: **Restore Subtree “<distinguished name>”**
- Select Yes to restore the object Authoritatively
- **Q** to exit
- **Q** to close ntdsutil
- To disable the “**Active Directory Restore Mode**” boot option, execute the following command on the command prompt:

  ```
  Bcdedit /deletevalue safeboot
  ```

- Reboot the System

**<Distinguished name>**
The distinguished name is unambiguous (identifies one object only) and unique (no other object in the directory has this name). By using the full path to an object, including the object name and all parent objects to the root of the domain, the distinguished name uniquely and unambiguously identifies an object within a domain hierarchy. It contains sufficient information for an LDAP client to retrieve the object's information from the directory.

For example, a user named James Smith works in the marketing department of a company as a promotions coordinator. Therefore, his user account is created in an organizational unit that stores the accounts for marketing department employees who are engaged in promotional activities. James Smith's user identifier is JSmith, and he works in the North American branch of the company.

The root domain of the company is reskit.com, and the local domain is noam.reskit.com. The diagram illustrates the components that make up the distinguished name of the user object JSmith in the noam.reskit.com domain.
13.3 Recovery through tombstone object reanimation

The domain naming context contains all users, groups, computers and other objects. Tombstone object reanimation is always an authoritative restore. There are two feasible methods for tombstone reanimation:

- Through LDP.exe
- Through ADRestore.exe

13.3.1 Authoritative Restore through LDP.exe

Tombstone objects are invisible through normal Active Directory Operations. With LDP and special LDAP search operations, tombstone objects can be found in AD.

To find tombstones:

- Start, on the command prompt, **ldp.exe**
- From the **Connection** menu, select **connect**
- Specify the domain controller **name**
- From the **connection** menu, select **bind**
- Select the **method** to get validated against the domain controller
- From the **Browse** menu, select **search**
- enter **cn=deleted Items**, followed by your base DN. For example **cn=deleted objects,dc=be,dc=edeconsulting,dc=local**
- From the **scope** part, select **subtree**
- Select **options**
- On the new window, from the **Search Call Type**, select **Extended**
- Select **controls**
- On the new window, from the **Load Predefined** part, select **Return Deleted Objects**
- Select **OK**
- Select **OK**
- Select **Run**
- The result should be something as follows

---

3 Figure comes from Microsoft Technet
To reanimate tombstones:

- **Copy** the entire DN of the tombstone object
- From the **Browse** menu, select **modify**
- Enter the entire DN of the deleted object into the **DN** part
- In the **Edit Entry Attribute**, add **isDeleted**
- Leave the **Values** field blank
- From the **operation** part, select **Delete**
- Select the **Enter button**
- In the **Edit Entry Attribute**, add **distinguishedName**
- In the **values** field, enter the **original DN** of the object to restore
- From the **Operation** part, select **Replace**
- Select the **Enter button**
- Enable the **Extended** option
- Select **Run**

### 13.3.2 Authoritative Restore through ADRestore.exe

Although it isn’t that difficult to reanimate deleted objects, it’s not a user friendly method. People from Sysinternals (a Microsoft company now) developed a tool named ADRestore. The command line version can be downloaded from:

To find tombstones:
- Start, on the command prompt, `AdRestore.exe`
- This lists all deleted objects

To reanimate tombstones:
- Start, on the command prompt, `AdRestore.exe -r`
- Select Yes on the object to restore

### 13.4 Active Directory Recovery through Snapshots

This is not the most recommended way to restore objects from Active Directory. It’s more intended to find content differences in Active Directory over time without the need to fully restore a Domain Controller.

Snapshots can’t be used to recover objects, you need to mount a snapshot, export your objects, mount the NTDS instance and import your objects.

To mount snapshots:
- Start, on the command prompt: `ntdsutil`
- First you need to mount a snapshot. Enter `snapshot`
- Enter `List All` and decide up on which snapshot you want to use to recover from
- Enter `mount <snapshot number>`
  - You can mount as many snapshots you want.
- You should be able to find the mounted snapshot as a shortcut on the C: drive. When you open it, you should find a full copy of your entire system. It’s even possible to copy files from the mounted snapshot.
- You can leave ntdsutil

In order to connect to the AD snapshot you’ve mounted you will need to use the DSAMAIN command. DSAMAIN is a command-line tool that is built into Windows Server 2012. It is available if you have the Active Directory Domain Services or Active Directory Lightweight Directory Services server role installed.

After using DSAMAIN to expose the information inside the AD snapshot, you can use any GUI tool that can connect to the specified port, tools such as Active Directory Users and Computers (DSA.msc), ADSIEDIT.msc, LDP.exe or others. You can also connect to it by using command line tools such as LDIFDE or CSVDE, tools that allow you to export information from that database.

To list AD content through the snapshots using DSAMAIN:
- First find the exact path of the NTDSD database file in the file structure of the mounted snapshot. So search for the file named: ntds.dit.
- First you need to mount a snapshot. Enter the following command on the command line:

  ```
  dsamain -dbpath <path>\ntds.dit -ldapport <portnumber>
  ```

  For example:
  ```
  dsamain -dbpath c:\$SNAP_20112041648_VOLUMEC\windows\NTDS\ntds.dit –ldapport 22222
  ```
- Open the ADSI MMC snap-in
- Select Connect to
Select Advanced
Enter the LDAP port you specified with the DSAMAIN command
Select OK, Select OK
You’re now connected to the mounted Active Directory with the content at the time the snapshot backup took place. You can use any LDAP aware tool to connect, browse and export the content.
To disconnect from the DSAMAIN from the database, press CTRL+C on the command prompt where you mounted the database.

Export and import Active Directory Objects
LDIFDE and CSVDE are tools that can be used to export and import Active Directory objects. You use these tools to connect to your mounted AD snapshot backup to search for and export objects. The exports you created are used later to import these objects in a real life Active Directory.

For more information related to LDIFDE and CSVDE, please refer to:

To dismount snapshots:
- Start, on the command prompt: ntdsutil.
- First you need to mount a snapshot. Enter snapshot
- Enter List All and decide up on which snapshot you want to use to recover from
- Enter unmount <snapshot number>
  You can unmout version after version.
- The snapshot folder on the hard drive should be disappeared.
  You can leave ntdsutil

13.5 Active Directory Restore through Recycle Bin
This is, from an Active Directory Backup and Disaster Recovery perspective, the new feature with the most added value. Restoring an object was never and shall never be easier as it has been implemented in the Active Directory Administrative Center in Windows 2012. Just right-click and select restore. Easy and fast.

This feature is only available when the domain and forest functional level are at least on Windows Server 2008 R2 and the recycle bin has been enabled.

13.5.1 Restore Through AD Administrative Center

To restore an object through the AD Administrative Center:
- Open the Active Directory Administrative Center
- In the left pane, navigate to Deleted Objects
- From the right pane, select all deleted objects you want to restore, right-click and select restore.

13.5.2 Restore Through Power Shell
You can use PowerShell commands to restore objects based on queries if there are too many deleted objects in the recycle bin, making it hard to find the necessary objects.
You need to know the ObjectGUID of the deleted object in order to be able to recover the Active Directory object through the recycle bin.

The Get-ADObject and Restore-ADObject are PowerShell commands that can be used on a Windows 2008 domain without the recycle bin being enabled. The difference is that the deleted objects in the domain without the recycle bin are being stripped off. After the restore, much of their attributes are empty. Attributes are not stripped of when the recycle bin has been enabled.

To find all deleted Active Directory Objects

- Open the Active Directory Module for Windows PowerShell running in an Administrator security context.
- Execute the following command to find all deleted objects and all it attributes:
  
  ```powershell
  Get-ADObject -filter 'isdeleted -eq True -and name -ne "Deleted Objects"' -includeDeletedObjects -property *
  ```

- Execute the following command to find all deleted objects and only list its ObjectGUID:
  
  ```powershell
  Get-ADObject -filter 'isdeleted -eq True -and name -ne "Deleted Objects"' -includeDeletedObjects -property objectGUID
  ```

- Or when you need particular attributes only, for example:
  
  ```powershell
  Get-ADObject -filter 'isdeleted -eq True -and name -ne "Deleted Objects"' -includeDeletedObjects -property objectGUID, distinguishedname, samaccountname
  ```

- To find all deleted objects deleted after a particular date:
  
  ```powershell
  $changeddate = new-object datetime(2011,3,21,18,00,00) [enter] Get-ADObject -filter 'whenchanged -gt $changeddate -and isdeleted -eq True' -includeDeletedObjects
  ```

- To find a deleted OU:
  
  ```powershell
  Get-ADObject -filter 'isdeleted -eq True -and msds:lastknownrdn -eq "<OU name>" -and lastknownparent -eq "<FQDN of parent>"' -includeDeletedObjects
  ```

- To find a deleted objects underneath a particular OU:
  
  ```powershell
  Get-ADObject -filter 'isdeleted -eq True -and lastknownparent -eq "<FQDN OU>"' -includeDeletedObjects
  ```

You can now restore the deleted object once you found the ObjectGUID of the object you want to restore.

To restore deleted Active Directory Objects

- Open the Active Directory Module for Windows PowerShell running in an Administrator security context.
- Execute the following command to restore a single deleted object:
  
  ```powershell
  restore-ADObject -identity <identity>
  ```

  Where <identity> represents the ObjectGUID attributed of the deleted object.

  For example:
  
  ```powershell
  restore-adobject -identity 99a536bb-8430-4732-9b52-78c621905ff0
  ```

- You can restore multiple objects at the same time. Actually, you can recover every object or group of objects listed through one of your Get_ADObe object commands, simply by adding the outcome to the restore-ADObject as in the following examples:
13.6 Restoring Back-Links

Restoring all back-links is only necessary when groups or users were deleted from a domain while they were member of groups of other domains.

Restoring back-links is not needed when the following is true:

- Your DC’s are running at least “Windows Server 2003 SP1, 2008, 2008 R2, 2012” and the forest operates at least at the “Windows Server 2003 Forest Functional Level”.
- Only users are deleted, or only groups are deleted, never both at the same time
- The deleted users and groups are in the same domain

In variations of this scenario, user accounts, computer accounts, or security groups may have been deleted individually or in some combination. In all these cases, authoritatively restore those objects that were inadvertently deleted.

Some deleted objects require more work to be restored. These objects include objects such as user accounts that contain attributes that are back links of the attributes of other objects. Two of these attributes are managedBy andmemberOf.

There are three methods:

- Restore the deleted user accounts, and then add the restored users back to their groups by using Ntdsutil.exe
- Restore the deleted user accounts, and then add the restored users back to their groups using a script.
- Authoritatively restore the deleted user accounts and the deleted users' security groups two times.

13.6.1 Restore group memberships through NTDSUTIL and LDIFF

For each user that you restore, at least two files are generated. These files have the following format:

ar_YYYYMMDD-HHMMSS_objects.txt
This file contains a list of the authoritatively restored objects. Use this file with the ntdsutil authoritative restore “create ldif file from” command in any other domain in the forest where the user was a member of Domain Local groups.

ar_YYYYMMDD-HHMMSS_links_usn.loc.ldf
If you perform the auth restore on a global catalog, one of these files is generated for every domain in the forest. This file contains a script that you can use with the Ldifde.exe utility. The
script restores the backlinks for the restored objects. In the user’s home domain, the script restores all the group memberships for the restored users. In all other domains in the forest where the user has group membership, the script restores only universal and global group memberships. The script does not restore any Domain Local group memberships. These memberships are not tracked by a global catalog.

**To restore the back-links:**

- Disconnect the computer from the network.
- Reboot the DC in normal “Active Directory Mode”
- Disable all inbound replication by launching the following command:

  ```
  repadmin /options <recovery dc name> +DISABLE_INBOUND_REPL
  ```

- Type the following command to push the auth-restored objects to all the cross-site replica domain controllers in the domain and to all the global catalogs in the forest:

  ```
  repadmin /syncall /d /e /P <recovery dc> <Naming Context> /e
  ```

- Type the following command to restore the users’ group memberships using LDIFF:

  ```
  ldifde -i -f ar_YYYYMMDD-HHMMSS_links_usn.loc.ldf
  ```

- Enable inbound replication:

  ```
  repadmin /options <recovery dc name> -DISABLE_INBOUND_REPL
  ```

### 13.6.2 Restore security principals two times

**To restore all security principals twice:**

- Authoritatively restore all deleted user accounts and all security groups, for more information please refer to: 13.1.1. Authoritative Restore
- Reboot the system in normal Active Directory operation mode
- Wait for the end-to-end replication of the restored users and of the security groups to all the domain controllers in the deleted user's domain and to the forest's global catalog domain controllers.
- Repeat step 1,2 and 3 once again.
- If the deleted users were members of security groups in other domains, authoritatively restore all the security groups that the deleted users were members of in those domains. Or, if system state backups are current, authoritatively restore all the security groups in those domains.

### 14. Entire Domain Controller Recovery

What if you lose an entire domain controller? Depending on other services hosted on this server, think about Exchange, file and print services, websites ... it might be necessary to recover the domain controller from systems state backup rather than just adding another new domain controller to the domain. So, you have two options:

- Cleanup AD, install a new server with the same name and perform a DCPROMO
- Install a new server and restore the system state backup
14.1 Without System State Recovery

When you just lost a domain controller and have enough remaining domain controllers in the same domain, just clean-up Active Directory, reinstall the domain controller on new hardware and perform a DCPROMO to promote the server to domain controller.

**Clean up Active Directory:**

- Using ntdsutil, remove all but the restored domain controller for the restored domain from the domain. The goal is to end up with a domain in which only the recovered domain controller remains for the recovered domain. When using ntdsutil, connect to the recovered domain controller.
- Keep in mind that the domain is not reachable. This means that the MMC snap in “Active Directory Users and Computers” would not work. So use ADSI editor to remove objects from the AD.
- To remove a DC from Active Directory, please refer to: **12.2. Remove Domain Controller from Active Directory**
- Unless you plan to use the same names as the original servers, start cleaning out DNS for each domain controller removed from the domain. For more information, please refer to: **12.1. Remove Domain Controller from DNS**

You can now safely install a new server using the same SAMAccountName and promote it to domain controller.

14.2 Through System State Recovery

It’s not necessary the clean-up Active Directory or DNS when you want to restore an entire domain controller from System State backup.

**To recover the system state:**

- Restage a computer on equivalent hardware and equivalent number of partitions as the original failed domain controller.
- Perform an authoritative System State restore. For more information please refer to: **13.1.1. Authoritative Restore**
- Be sure that all domain wide FSMO roles are now maintained on the recovered domain controller. To seize the FSMO roles, refer to: **17. FSMO Roles Recovery**.
- Reboot the system
- Validate the successful restore, please refer to: **12.6. Verification of a Successful Restore**.

15. Entire Domain Recovery

This procedure is only valid if the domain doesn’t exist anymore, that is, there are no domain controllers anymore. This procedure is not intended to be followed blindly. By this I mean, exceptions within the steps to take can occur as this is a very complex procedure. It depends on the FSMO role distribution, SYSVOL content, .....

**To recover an entire domain:**

- Remove all remaining domain controllers for the failed domain
- Cleanup Active Directory and DNS
- Stage a new server and restore the system state backup
Stage additional domain controllers

**Remove all remaining Domain Controllers**
If any, power down all existing domain controllers for the domain to recover. Be sure they never come back on line.

To clean up Active Directory:

- Using ntdsutil, remove all but the restored domain controller for the restored domain from the domain. The goal is to end up with a domain in which only the recovered domain controller remains for the recovered domain. When using ntdsutil, connect to the recovered domain controller.
- Keep in mind that the domain is not reachable. This means that the MMC snap in “Active Directory Users and Computers” would not work. So use ADSI editor to remove objects from the AD.
- To remove a DC from Active Directory, please refer to: **12.2. Remove Domain Controller from Active Directory**
- Unless you plan to use the same names as the original servers, start cleaning out DNS for each domain controller removed from the domain. For more information, please refer to: **12.1. Remove Domain Controller from DNS**

To recover the system state:

- Restage a computer on equivalent hardware and equivalent number of partitions as the original failed domain controller.
- Perform an authoritative System State restore. For more information please refer to: **13.1.1. Authoritative Restore**
- Be sure that all domain wide FSMO roles are now maintained on the recovered domain controller. To seize the FSMO roles, refer to: **17. FSMO Roles Recovery.**
- Reboot the system
- Validate the successful restore, please refer to: **12.6. Verification of a Successful Restore.**

Add Additional domain controllers:

- Add additional domain controllers through normal staging procedures using the most recent domain controller profile.

16. **Entire Forest Recovery**
Restoring an entire forest is much easier than it looks like. You only have to respect the order of all steps to take to get the forest up and running again.

Although the AD schema can’t be restores as such, when restoring a root domain controller, the schema will be restored in the state it was at the last backup, meaning that all schema extensions made are restored to.

These are the most important rules to follow:

- Always start from the root domain down to the child domains following the domain hierarchy
- Restore only one domain controller from each domain
• Clean out all other domain controllers in the restored domain, before starting the restore of the next domain
• To speed up the recovery, and to avoid all manual DNS changes, use the same IP address and hostname as the original DC.

To recover an entire forest:

• Remove all remaining domain controllers for the failed forest
• Cleanup Active Directory and DNS
• For each domain in the forest, stage a new server and restore the system state backup
• For each domain in the forest, stage additional domain controllers

Remove all remaining Domain Controllers
If any, power down all existing domain controllers for the all domains in the forest to recover. Be sure they never come back on line.

To clean up Active Directory:

• Using ntdsutil, remove all but the restored domain controller for each restored domain in the forest. The goal is to end up with a domain in which only the recovered domain controller remains for the recovered domain. When using ntdsutil, connect to the recovered domain controller.
• Keep in mind that the domain is not reachable. This means that the MMC snap in “Active Directory Users and Computers” would not work. So use ADSI editor to remove objects from the AD.
• To remove a DC from Active Directory, please refer to: 12.2. Remove Domain Controller from Active Directory
• Unless you plan to use the same names as the original servers, start cleaning out DNS for each domain controller removed from the domain. For more information, please refer to: 12.1. Remove Domain Controller from DNS

To recover the system state:

• For each domain in the forest, restage a computer on equivalent hardware and equivalent number of partitions as the original failed domain controllers.
• For one domain controller of each domain in the forest, perform an authoritative System State restore. For more information please refer to: 13.1.1. Authoritative Restore
  Be sure that all domain and forest wide FSMO roles are now maintained on the recovered on the correct domain controller. To seize the FSMO roles, refer to: 17. FSMO Roles Recovery.
• Reboot the systems
• Validate the successful restore, please refer to: 12.6. Verification of a Successful Restore

Add Additional domain controllers:

• For each domain in the forest, add additional domain controllers through normal staging procedures using the most recent domain controller profile.
17. FSMO Roles Recovery

17.1 Overview

In a Windows NT4 domain, only the PDC holds an updatable copy of the User Account Database. All other domain controllers have only read-only replicas of the PDC.

In Windows 2008, all domain controllers are maintaining an updatable copy of the Active Directory. However, not all attributes or objects are updatable on every domain controller. Some are; such as the Schema can only be updated on one single DC in the entire forest, others are done on one single DC in each domain, whatever the number of domains there are.

To avoid some unsolvable replication conflicts if the same object was modified on two different domain controllers at the same time, 5 different roles are maintained throughout the infrastructure:

<table>
<thead>
<tr>
<th>Role</th>
<th>Scope</th>
<th>Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema Master</td>
<td>Forest</td>
<td>Modifies the Schema</td>
</tr>
<tr>
<td>Domain Naming Master</td>
<td>Forest</td>
<td>Makes changes to the forest-wide domain name space of the directory</td>
</tr>
<tr>
<td>RID Master</td>
<td>Domain</td>
<td>Processes RID Pool requests from all DC’s within a given domain</td>
</tr>
<tr>
<td>PDC Emulator</td>
<td>Domain</td>
<td>Synchronize time in an enterprise. Account lockout is processed on the PDC emulator. Password changes performed by other DC’s in the domain are replicated preferentially to the PDC emulator.</td>
</tr>
<tr>
<td>Infrastructure Master</td>
<td>Domain</td>
<td>The infrastructure FSMO role holder is the DC responsible for updating an object's SID and distinguished name in a cross-domain object reference.</td>
</tr>
</tbody>
</table>

Recovering or Seizing an FSMO Role

Seizing, or forcing transfer, as it is sometimes called, is a process carried out without the cooperation of the original role holder. In other words, when the original role holder has suffered a disaster, you can seize the role, forcing it to be moved to another DC within the domain/forest.

Although the process required to seize an FSMO role is similar to the process used for all five roles, the issues associated with FSMO seizure differ.

Recovering the Schema Master

The primary consideration is the permanence of the outage. Because of the chance of duplicate schema changes being propagated throughout the environment, a seizure of the schema master role should be carried out only if the failed role holder will never come back online.
Because of the infrequent requirement for a schema master role and the implications of a seizure, you can usually live with the outage during the period of time it takes to restore the DC holding the role. However, if you require the immediate use of the schema master role or if the original role holder will never be brought back into the Windows 2012 environment, a seizure can be carried out.

**Recovering the Domain Naming Master**
The primary consideration is the permanence of the outage. Because of the chance of duplicate domain naming changes being propagated throughout the environment, a seizure of the domain naming master role should be carried out only if the failed role holder will never come back online.

Because of the infrequent requirement for a domain naming master role and the implications of a seizure, you can usually live with the outage during the period of time it takes to restore the DC holding the role. However, if you require the immediate use of the domain naming master role or if the original role holder will never be brought back into the Windows 2012 environment, a seizure can be carried out.

**Recovering the RID Master**
Consider carefully before you decide to perform a seizure on an RID master. Because of the risk of duplicate RIDs on the network, the sever that originally housed the RID master role should never come back online.

**Recovering the PDC Emulator**
Because the role of the PDC emulator is not quite as critical as those previously mentioned, the act of seizing the role does not have the ramifications of the others. If you choose to seize the PDC emulator role, you do not need to completely rebuild the original role holder before it can participate in the Windows 2012 environment again.

As a result, the decision to seize the PDC emulator role has fewer implications to your environment and is generally considered a standard practice in the event of a PDC emulator failure, particularly in a mixed mode environment.

The only real issue to consider is whether you are functioning in a mixed mode environment with NT 4.0 BDCs. For the BDCs to be aware of the changes, a full synchronization of the BUILTIN database with the new PDC emulator will occur.

**Recovering a Global Catalog**
This is not necessary when all domain controllers through the forest are Global Catalog. If not, just enable the GC role on another remaining domain controller.

**Recovering the Infrastructure Master**
This is not necessary when all domain controllers through the forest are Global Catalog. If not, simply seize the Infrastructure Master role to another remaining domain controller.

### 17.2 How to find the existing FSMO role holders

Every domain control should know what domain controller own what FSMO roles.

**To find all the FSMO roles the local domain controller knows about:**

- Start, on the command prompt on a remaining domain controller, `ntdsutil`
- Type, without the quotes: "roles” and press return to enter the “FSMO Maintenance” part of ntdsutil
- Type “Connections”
- Type “Connect to server <local dc name>”
• Type “q”
• Type “Select Operation Target”
• Type “List roles for connected server”

17.3 How to Seize a Role

To seize a role:

• Start, on the command prompt on a remaining domain controller, ntdsutil
• Type, without the quotes: “roles” and press return to enter the “FSMO Maintenance” part of ntdsutil
• Type “Connections”
• Type “Connect to server <local dc name>”
• Type “q”
• Type: “seize <role>”, where the role could be one of the following:
  • PDC
  • Domain naming master
  • Infrastructure master
  • RID Master
  • Schema master
 • Type: “Select Operation Target”
• Type: “List roles for connected server” to be sure all seized roles are now on your domain controller
• Close ntdsutil
• Restart the netlogon service

17.4 How to Move a Role

To move a role:

• Start, on the command prompt on a remaining domain controller, ntdsutil
• Type, without the quotes: “roles” and press return to enter the “FSMO Maintenance” part of ntdsutil
• Type “Connections”
• Type “Connect to server <local dc name>”
• Type “q”
• Type: “Transfer <role>”, where the role could be one of the following:
  • PDC
  • Domain naming master
  • Infrastructure master
  • RID Master
  • Schema master
• Type: “Select Operation Target”
• Type: “List roles for connected server” to be sure all seized roles are now on your domain controller
• Close ntdsutil
• Restart the netlogon service
18. SYSVOL Recovery

18.1 Overview

Although you should only authoritatively restore the SYSVOL together with the authoritative restore of Active Directory, it’s possible (not recommended) to restore the SYSVOL authoritatively, but independently from the AD restore. Keep in mind that GPO settings are stored on both, Active directory database and the SYSVOL, and that these two have to be in sync with each other at any moment in time.

It’s only possible to restore the content of the SYSVOL share and the NETLOGON share. If someone deleted the entire SYSVOL directory, restore will be successful, but SYSVOL and NETLOGON replication won’t work.

SYSVOL Replication has been changed in Windows 2008

If the domain’s functional level is Windows Server 2008 and the domain has undergone SYSVOL migration, DFSR will be used to replicate the SYSVOL folder. If the first domain controller in the domain was promoted directly into the Windows Server 2008 functional level, DFSR is automatically used for SYSVOL replication. In such cases, there is no need for migration of SYSVOL replication from FRS to DFSR. If the domain was upgraded to Windows Server 2008 functional level, FRS is used for SYSVOL replication until the migration process from FRS to DFSR is complete.

18.2 Authoritative SYSVOL Restore Trough System State Backup

To restore SYSVOL authoritatively:

- Be sure you know the Active Directory Restore Mode Administrator Password. If not, please refer to: 12.3. Change the Active Directory Restore Mode (DSRM) Administrator Password
- To boot an existing domain controller, or new staged Windows 2012 server into the “Active Directory Restore Mode”:
  - Logon to the system using an account with at least local administrative rights
  - From the command prompt, execute the following task:
    
    Bcedit /set safeboot dsrepair
  - Reboot the server
  - Logon to the system using the DSRM account and password
  - Start a command prompt
  - On the command prompt, execute the following command
    - wbadmin /get versions
    - wbadmin start systemstaterecovery –versions:<version> -quiet -authsysvol
    
    Example:
  - Once the SystemState recstore has been finished, select “Y” to reboot the system
  - Logon to the system using the DSRM account and password
  - Wait till the restore process has been finished.
At this point, SYSVOL has been restored authoritatively through NTDS. You now have the possibility to authoritatively restore the Active Directory as well. Skip the next step if you don’t want the restore AD.

From the command prompt, start ntdsutil and execute all of the following commands:

- `Activate instance ntds`
- `Authoritative Restore`
- `Restore Object <distinguished name>`
- `Q` to exit
- `Q` to close ntdsutil

To disable the “Active Directory Restore Mode” boot option, execute the following command on the command prompt:

- `Bcdedit /deletevalue safeboot`

Reboot the System

18.3 How to force an Authoritative and Non-Authoritative Synchronization for DFSR Replicated SYSVOL

This part is an extract from the following Microsoft Document:
http://support.microsoft.com/kb/2218556

As from Windows Server 2008, natively installed, SYSVOL replication will take place by meaning of DFSR instead of FRS. You want to force the non-authoritative synchronization of SYSVOL on a domain controller. In the File Replication Service (FRS), this was controlled through the D2 and D4 data values for the Burflags registry values, but these values do not exist for the Distributed File System Replication (DFSR) service. You cannot use the DFS Management snap-in (Dfsmgmt.msc) or the Dfsradmin.exe command-line tool to achieve this. Unlike custom DFSR replicated folders, SYSVOL is intentionally protected from any editing through its management interfaces to prevent accidents.

How to perform a non-authoritative synchronization of DFSR-replicated SYSVOL (like "D2" for FRS)

- In the ADSIEDIT.MSC tool modify the following distinguished name (DN) value and attribute on each of the domain controllers that you want to make non-authoritative:

  CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain>
  msDFSR-Enabled=FALSE

- Force Active Directory replication throughout the domain. This can be accomplice by using the following command: `repadmin /syncall /e`

- Run the following command from an elevated command prompt on the same servers that you set as non-authoritative: `DFSRDIA POL LAB`
- You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated.

- On the same DN from Step 1, set:
  
  msDFSR-Enabled=TRUE

- Force Active Directory replication throughout the domain. This can be accomplice by using the following command: `repadmin /syncall /e`

- Run the following command from an elevated command prompt on the same servers that you set as non-authoritative: `DFSRTDIAG POLLAD`

- You will see Event ID 4614 and 4604 in the DFSR event log indicating SYSVOL has been initialized. That domain controller has now done a “D2” of SYSVOL.

### How to perform an authoritative synchronization of DFSR-replicated SYSVOL (like "D4" for FRS)

- In the ADSIEDIT.MSC tool, modify the following DN and two attributes on the domain controller you want to make authoritative (prefferrably the PDC Emulator, which is usually the most up to date for SYSVOL contents):

  CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<the server name>,OU=Domain Controllers,DC=<domain>

  msDFSR-Enabled=FALSE
  msDFSR-options=1

- Modify the following DN and single attribute on all other domain controllers in that domain:

  CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<each other server name>,OU=Domain Controllers,DC=<domain>

  msDFSR-Enabled=FALSE

- Force Active Directory replication throughout the domain. This can be accomplice by using the following command: `repadmin /syncall /e`

- Start the DFSR service set as authoritative

- You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated.

- On the same DN from Step 1, set: msDFSR-Enabled=TRUE

- Force Active Directory replication throughout the domain. This can be accomplice by using the following command: `repadmin /syncall /e`

- Run the following command from an elevated command prompt on the same server that you set as authoritative: `DFSRTDIAG POLLAD`

- You will see Event ID 4602 in the DFSR event log indicating SYSVOL has been initialized. That domain controller has now done a “D4” of SYSVOL.
Start the DFSR service on the other non-authoritative DCs. You will see Event ID 4114 in the DFSR event log indicating SYSVOL is no longer being replicated on each of them.

Modify the following DN and single attribute on all other domain controllers in that domain:

\[
\text{CN=SYSVOL Subscription,CN=Domain System Volume,CN=DFSR-LocalSettings,CN=<each other server name>,OU=Domain Controllers,DC=<domain>}
\]

msDFSR-Enabled=TRUE

Run the following command from an elevated command prompt on all non-authoritative DCs (i.e. all but the formerly authoritative one): DFSRDIA P POLLAD

19. Active Directory Database Operations

19.1 Repairing a corrupted Database

There are several possibilities to recover from a corrupted Active Directory Database:

- Demote the domain controller, delete all database files and promote the computer back to domain controller
- Non-authoritative restore of the entire database from backup
- Using NTDSUTIL, perform a database repair by compacting the database

NTDSUTIL can be used to compact the Active Directory database to another location followed by a copy and overwrites of the original database file with the new compacted database file:

- On the domain controller, start a command prompt
- on the command prompt, execute the following command:
  \[
  \text{net stop NTDS}
  \]
- Select “Y” to stop all dependency services
- From the command prompt, start nt dsutil
- Select Activate instance nd ts
- Select “Files”
- Create a compacted copy of the current database onto another location by using the command: compact to d: \\
- From another command prompt, copy the new compacted database file to it original location (overwrite the original database file): copy D:\ntds.dit E:\NTDS_AD\ntds.dit
- From the NTDSUTIL command, start a checksum and be sure that there are no corruptions found. The AD database must be restored when any corruption occurs at this point of the repair operation. This means that the corruptions are too complex to solve with the compact command.
20. Recovering Individual Group Policy Objects

GPO’s are restored entirely with an authoritative system state restore. Both parts of the GPO’s, the AD and the SYSVOL part are restored together.

The following GPO restore operations are based upon a manual export-import mechanism used to backup, restore and even distribute GPO’s to other forests and/or domains.

20.1 Rollback GPO update

To rollback a GPO update or to restore some settings in a GPO:

- Select the GPO in the Group Policy Management console
- Right-click and choose ‘Import Settings...’
- Choose the latest backup from the individual GPO backup folder
- Complete the import settings wizard

20.2 Restore one or more GPOs

To restore one or more deleted GPOs:

- Select the ‘Group Policy Objects’ container within the Group Policy Management console
- Right-click and choose ‘Manage Backups...’
- Browse to the folder that contains all GPO backups for that domain
- Select one or more GPOs to restore
- Click on ‘Restore’ within the Manage Backups dialog box.
- For each restored GPO, open the report file (.html) from the backup folder and recreate the reported links when needed.

---

Applies to event:

<table>
<thead>
<tr>
<th>Event Type:</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Source:</td>
<td>NTDS ISAM</td>
</tr>
<tr>
<td>Event Category:</td>
<td>Database Page Cache</td>
</tr>
<tr>
<td>Event ID:</td>
<td>474</td>
</tr>
<tr>
<td>Date:</td>
<td>21/09/2009</td>
</tr>
<tr>
<td>Time:</td>
<td>13:06:02</td>
</tr>
<tr>
<td>User:</td>
<td>N/A</td>
</tr>
<tr>
<td>Computer:</td>
<td>&lt;servername&gt;</td>
</tr>
<tr>
<td>Description:</td>
<td>NTDS (420) NTDS: The database page read from the file “e:\NTDS_AD\ntds.dit” at offset 1557479424 (0x000000005cd54000) for 8192 (0x00002000) bytes failed verification due to a page checksum mismatch. The expected checksum was 2951061134 (0xfafe59e8e) and the actual checksum was 2951061135 (0xfafe59e8f). The read operation will fail with error -1018 (0xfffffc06). If this condition persists then please restore the database from a previous backup. This problem is likely due to faulty hardware. Please contact your hardware vendor for further assistance diagnosing the problem.</td>
</tr>
</tbody>
</table>
21. Fast Disaster Recovery from Delayed Replicated Site

21.1 Introduction

Today, between sites, replication happens immediately. This means that changes to AD are replicated to each Domain Controller in the domain almost in real time. But, errors, corruptions and accidentally object deletions are replicated in real time too. If we change the replication schedule to 24 hours, that is; one replication every 24 hour, we do have 24 hours to detect corruptions, procedural or human errors causing the Active Directory to become unavailable. Should this happen, the Delayed Replicated site can then be used to recover very fast from a totally lost domain on another site.

21.2 Recover a domain on another site

To recover a domain on from another “Delayed Replicated site“:

- On a domain controller on the Delayed Replication Site, start a command prompt
- On the command prompt, execute the following command
  ```
  net stop NTDS
  ```
- Select “Y” to stop all dependency services
- From the command prompt, start `ntdsutil` and execute all of the following commands:
  ```
  Activate instance ntds
  Authoritative Restore
  Restore Object <distinguished name>
  Q to exit
  Q to close ntdsutil
  ```
- Reboot the System

22. Active Directory Site Disaster Recovery Procedures

22.1 Introduction

By design, Active Directory Services are built to be always available; even should we encounter the outage of an entire site.

The KCC service running on each domain controller recalculates and rebuilds the entire replication topology every 15 minutes, if necessary. The replication topology will be dynamically changed should one or more domain controllers, site links or entire sites become unavailable. This makes ADS less vulnerable to network issues or Domain Controller hardware issues.

22.2 RTO and RPO Times

**RTO Defined**

The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for users’ representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. The RTO attaches to the business process and not the resources required supporting the process.

---

The RTO and the results of the Business Impact Analysis (BIA) in its entirety provide the basis for identifying and analysing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs. The "O" in RTO stands for objective, not mandate. In reality, strategy is often selected that will not meet the RTO. In this instance the RTO will not be met but should still remain an objective of future strategy revision.

RPO Defined

The Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours.

Example: If there is a complete replication at 10:00 am and the system dies at 11:59 am without a new replication, the loss of the data written between 10:00 am and 11:59 am will not be recovered from the replica. This amount of time data has been lost has been deemed acceptable because of the 2 hour RPO. This is the case even if it takes an additional 3 hours to get the site back into production (although these three hours may form part of the Recovery Time Objective). The production will continue from the point in time of 10:00 am. All data in between will have to be manually recovered through other means.

22.3 When to go into DRP mode

Putting ADS into DRP mode has a huge impact on the way to return back to normal operational level. ADS have 5 different FSMO roles which are unique through the domain or even through the forest. The original domain controller providing one or more of these roles may never be put back on line once the roles, he maintained before the disaster, are moved to a DC on another site. Moving a FSMO role to the DRP site causes the original role holder to be reinstalled afterwards. ADS, on the other hand, can life for a short time without having the FSMO roles available. So deciding when to go into DRP mode is a crucial choice between a time consuming DRP or facing some issues caused by missing FSMO roles.

**ADS should go into DRP mode only:**

- When one more sites are down. A “site”, from and Active Directory point of view is not the same a physical building our site. A site in ADS is a collection of networks in which all servers are fully connected to each other through fast network links.
- When the site outage will be longer than 8 hours.

22.4 Putting ADS into Disaster Recovery Mode

**We’re facing the following issues should we lose a site:**

- The remaining domain controllers will be much more called by clients and users for authentication and authorization operations. This will slow down the reaction time of these domain controllers.
- ADS have 5 different FSMO roles, which are unique through the domain or the forest. It would be possible that some of these roles become unavailable since they are on the failing site.

---

To address one or both above issues:

- Some manual interventions in both cases.
- Install additional domain controllers on the remaining sites
- Move all failed roles to domain controllers on the remaining sites

22.5 Common tasks when going into DR mode

Once the DRP has been started all of the following manual interventions have to be initiated:

- Shutdown all domain controllers on the remaining site (if she still exists)
- The DNS team should, for each domain controller on the failing site:
  - Remove the A and PTR record for the server name from the DNS
  - Remove the A record for the domain for the server from the DNS
  - Remove all SRV records for the server from the DNS

22.6 Installing additional domain controllers

Keep in mind that new domain controllers should have write access to all _zones of his own domain and some _zones of the forest root domain. So please inform the DNS people to grant the new server all necessary rights. They know exactly what rights.

22.7 Move all FSMO roles

To know which roles are missing or which role exists on which server, please refer to 17.2. How to find the existing FSMO role holders

For more information about how to move a role, please refer to: 17.4. How to Move a Role

For more information about how to seize a role, please refer to: 17.3. How to Seize an FSMO Role

22.8 How to move back to the original operation level

This part describes how we can switch over from DRP mode back to normal operations mode, meaning that the site failed is back online.

- Be sure all domain controllers have the necessary rights to update and or create their SRV records in the DNS. Be sure the A and the PTR record for the servers exists and that their A record also exist on the domain record.
- Power on all domain controllers which did not have any FSMO role before the DRP started.
- Verify if, after the boot, all necessary SRV records for each server exists. To do, log onto the server and launch the “CheckDNS.exe” tool.
- Ask the DNS people to force a full regeneration of all zones and force a full replication to each secondary DNS server.
- Reinstall all domain controllers which maintained a FSMO role before the DRP started.
- Verify if, after the boot, all necessary SRV records for the reinstalled server exists. To do, log onto the server and launch the “CheckDNS.exe” tool.
- Ask the DNS people to force a full regeneration of all zones and force a full replication to each secondary DNS server.
- Move all FSMO roles to their original server. For more information, please refer to: 17.4. How to Move a Role
23. Useful Links

AD DS Backup and Recovery Step-by-Step Guide

Active Directory Recycle Bin Step-by-Step Guide

Active Directory Snapshot, new feature in Windows 2008

More information about restoring deleted objects using ADRestore can be found @:
http://support.microsoft.com/?kbid=840001

How to force an authoritative and non-authoritative synchronization for DFSR-replicated SYSVOL (like "D4/D2" for FRS)
http://support.microsoft.com/kb/2218556

Backing Up and Restoring an FRS-Replicated SYSVOL Folder

Active Directory Backup and Restore in Windows Server 2008

Bare Metal server recovery
http://searchsystemschannel.techtarget.com/generic/0,295582,sid99_gci1514371,00.html

Active Directory Recycle Bin Step-by-Step

Windows Server 2012 Documentation

How to detect and recover from USN Roll Back
http://support.microsoft.com/kb/875495

All about lingering objects
http://support.microsoft.com/kb/910205/en-us