WSA - HW – 13 :

2. Install Active Directory Recycle Bin feature. Demostrate how to restore deleted objects. Provide some steps and screenshots (or video).

Applies To: Windows Server 2008 R2

Install and Enable Active Directory Recycle Bin feature with Windows PowerShell:

On the Schema Master Domain Controller, run Start / Administrative Tools / Active Directory Module for Windows PowerShell.
N.B. Replace yourdomain.com with your own Active Directory domain name !!!

Type in the following command:

Enable-ADOptionalFeature –Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=yourdomain,DC=com' –Scope ForestOrConfigurationSet –Target 'yourdomain.com'

You will get a warning which you will need to confirm stating that enabling the Recycle Bin Feature is irreversible.
That's it! The recycle bin will now begin capturing deletions of objects which will allow you to later restore them to their original or alternate location.

Install and Enable Active Directory Recycle Bin feature with Ldp.exe:

1. To open Ldp.exe, click Start, click Run, and then type ldp.exe.

2. To connect and bind to the server that hosts the forest root domain of your AD DS environment, under Connection, click Connect, and then click Bind.

3. Click View, click Tree, in BaseDN, select the configuration directory partition, and then click OK.

4. In the console tree, double-click the distinguished name of the configuration directory partition, and then navigate to the CN=Partitions container.

5. Right-click the CN=Partitions container's distinguished name, and then click Modify.

6. In the Modify dialog box, make sure that the DN box is empty.

7. In the Modify dialog box, in Edit Entry Attribute, type enableOptionalFeature.

8. In the Modify dialog box, in Values, type **CN=Partitions,CN=Configuration,DC=mydomain,DC=com:766ddcd8-acd0-445e-f3b9-a7f9b6744f2a**.

Replace **mydomain** and **com** with the appropriate forest root domain name of your **AD DS** environment.

NOTE:
766ddcd8-acd0-445e-f3b9-a7f9b6744f2a is the Active Directory Recycle Bin globally unique identifier (**GUID**).
To verify the Active Directory Recycle Bin GUID, navigate to the **CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=mydomain,DC=com** container (replace **mydomain** and **com** with the appropriate forest root domain name of **your AD DS environment**), and in the details pane, locate the value of the msDS-OptionalFeatureGUID attribute.

9. In the Modify dialog box, under Operation click Add, click Enter, and then click Run.

10. To verify that Active Directory Recycle Bin is enabled, navigate to the CN=Partitions container.
In the details pane, locate the **msDS-EnabledFeature** attribute, and confirm that its value is set to **CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=mydomain,DC=com,** where **mydomain** and **com** represent the appropriate forest root domain name of **your AD DS environment**.

How to restore deleted objects with Ldp.exe:

1. Open Ldp.exe from an elevated command prompt. Open a command prompt (Cmd.exe) as an administrator.
To open a command prompt as an administrator, click Start. In Start Search, type Command Prompt. At the top of the Start menu, right-click Command Prompt, and then click Run as administrator.
If the User Account Control dialog box appears, enter the appropriate credentials (if requested), confirm that the action it displays is what you want, and then click Continue.

2. To connect and bind to the server that hosts the forest root domain of your AD DS environment, under Connections, click Connect, and then click Bind.

3. On the Options menu, click Controls.

4. In the Controls dialog box, expand the Load Predefined drop-down list, click Return Deleted Objects, and then click OK.

5. In the console tree, navigate to the CN=Deleted Objects container.

6. Locate and right-click the deleted Active Directory object that you want to restore, and then click Modify.

7. In the Modify dialog box:

a. In Edit Entry Attribute, type isDeleted.

b. Leave the Values box empty.

c. Under Operation, click Delete, and then click Enter.

d. In Edit Entry Attribute, type distinguishedName.

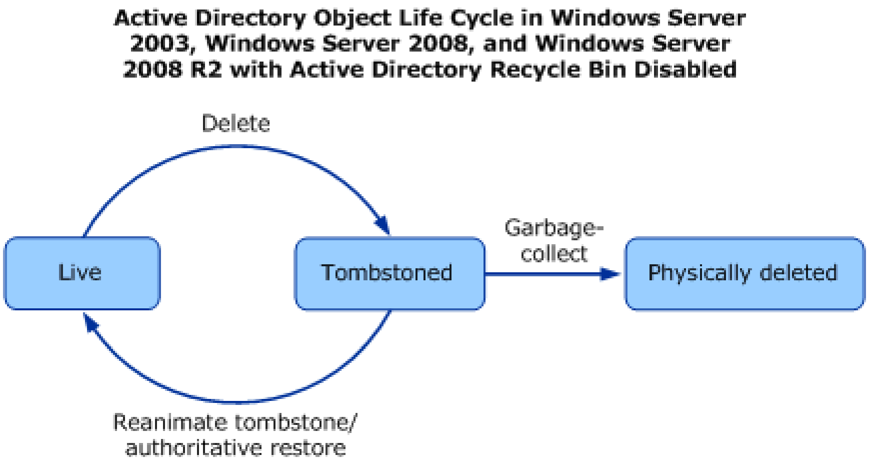
e. In Values, type the original distinguished name (also known as DN) of this Active Directory object.

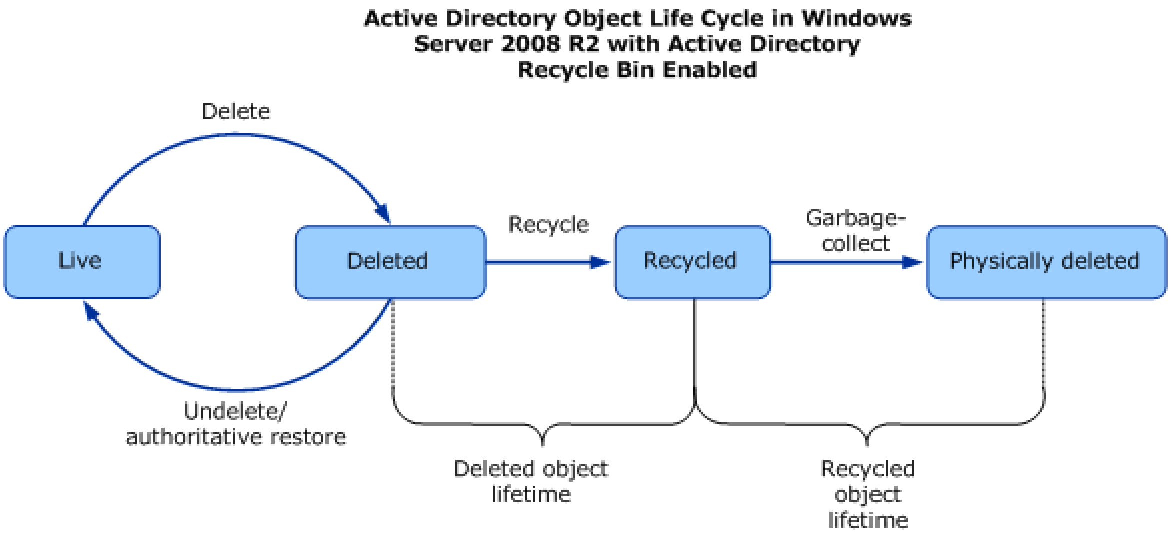
f. Under Operation, click Replace.

g. Make sure that the Extended check box is selected, click Enter, and then click Run.

NOTE:
When you delete or recover an Active Directory object with link-valued attributes, AD DS must process the object's link value table to maintain referential integrity on the linked attribute's values.
Because deleting or recovering an Active Directory object results in modifications to the object's link value table, if you attempt to delete or recover an object during its ongoing link-value-table processing time, the operation will be blocked.
For example, if you use the Active Directory Recycle Bin to recover a deleted object with a large number of link-valued attributes (for example, a group object with 10 million users) immediately after it was deleted (or anytime throughout the duration of its link-value-table processing), the object recovery will be blocked.
(If you are using **Ldp.exe** to perform the recovery, you might see the following error message: "**Error 0x2093 The operation cannot continue because the object is in the process of being removed**.")

Some Graphics:


Active Directory Object Life Cycle in Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 with Active Directory Recycle Bin Disabled
Delete
Live
Tombstoned
Garbage-collect
Physically deleted
Reanimate tombstone/ authoritative restore


Active Directory Object Life Cycle in Windows Server 2008 R2 with Active Directory Recycle Bin Enabled
Delete
Live
Deleted
Recycle
Recycled
Garbage-collect
Physically deleted
Undelete/ authoritative restore
Deleted object lifetime
Recycled object lifetime

info:
http://technet.microsoft.com/en-us/library/dd379481%28WS.10%29.aspx

http://technet.microsoft.com/en-us/library/dd379509%28v=ws.10%29.aspx

more info:
http://technet.microsoft.com/en-us/library/dd379542%28v=ws.10%29.aspx

http://sharepointgeorge.com/2010/enabling-active-directory-recycle-bin-feature-windows-2008-r2