The Active Directory is arguably the most important part of the IT infrastructure. Administrators have to maintain constant vigilance when making any changes to it. Despite this, there can occasions where objects are mistakenly deleted and need to be restored.

In this whitepaper, we will explore some of the different methods you can use to restore deleted objects from the Active Directory Recycle Bin.

Active Directory Recycle Bin

**Recycle Bin**

**Requirement**
To enable this feature, raise the forest functional level of your Active Directory Directory Service (AD DS) or Active Directory Lightweight Directory Service (AD LDS) to Windows Server 2008 R2. It means all domain controllers in AD DS, and all servers hosting AD LDS should be running Windows 2008 R2, Windows Server 2012 or Windows Server 2012 R2.
Enable Active Directory Recycle Bin

**NOTE:** The process to enable the Active Directory Recycle Bin is irreversible.

Execute the following command to enable Active Directory Recycle Bin.

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=www,DC=domain,DC=com' -Scope ForestOrConfigurationSet -Target 'www.domain.com'
```
In Active Directory Administrative Center on Windows Server 2012 and Windows Server 2012 R2, right-click domain name in the left pane and then click “Enable Recycle Bin” command.

It shows the following dialog box, which asks for the user confirmation before enabling the recycle bin.
Figure 3: Seeking user confirmation before enabling Recycle Bin

Click “OK” to proceed. It shows the following dialog box, where the program wants you to refresh the view of Administrative Center.

Figure 4: Enabled the Active Directory Recycle Bin in Windows Server 2012

Execute the following command to check whether Active Directory Recycle Bin is enabled or not.

```
Get-ADOptionalFeature -Filter 'name-like "Recycle Bin Feature"'
```

Figure 5: Check the status of Active Directory Recycle Bin
Active Directory Object Lifecycle

Once Active Directory Recycle Bin is enabled, the lifecycle of Active Directory is changed as displayed in the following picture.

![Diagram of Active Directory Object Lifecycle]

Figure 6: Lifecycle of an Active Directory Object

What happens when an object is deleted?

If Active Directory Recycle Bin is enabled, the following actions are performed on the object when it is deleted from Active Directory.

1. The value of “IsDeleted” is changed to “True.”
2. The value of internal and inaccessible “WhenDeleted” column is changed to “TimeChanged” time stamp of “IsDeleted” attribute.
3. A special value is assigned to Windows security descriptor of the deleted object.
4. The object enters into “logically deleted” state.
5. Relative Distinguished Name (RDN) is changed to an impossible value that cannot be defined by any LDAP program.
6. The object will be moved to “Deleted Objects” container, where it remains until the deleted object lifetime is over.
7. The system preserves all the object’s link-valued and non-linked value attributes.
8. Except the following key attributes, other attributes were deleted.
   a. Object-GUID
   b. Object-SID
   c. Object-Dist-Name
   d. USN
9. After Deleted Object Lifetime (msDS-deletedObjectLifetime) expires, the object turns into a new state: “recycled object.”

10. The recycled object remains in “Deleted Objects” container until the recycled object lifetime expires, which is equal to tombstone lifetime.

11. Most of the attributes, which were retained in “logically deleted” state, are now erased.

12. After the recycled lifetime expires, the garbage collections process starts that physically deletes the object.

You can restore the object when it is in a “logically deleted” state, before the Deleted Object Lifetime (msDS-deletedObjectLifetime) expires, by using Windows PowerShell commands, LDP.exe, AD Administrative Center, or third party tools such as LepideAuditor Suite. The process to restore an object from its tombstone state is termed as “reanimating” the object.

You cannot restore the object when it is in a “recycled” state.

**Test Case**

Suppose you have accidentally deleted an Organizational Unit named “New Test”, which contains the following objects:

1. Three users: User1, User2, User3
2. One contact: User12
3. One computer: P1
4. One Shared folder: Shared

![Figure 7: Sample OU that has been deleted by mistake](image)

WARNING: Please do not delete an organizational unit or object in a live environment to test the commands and operations listed in this article. We have tried these steps in a sample environment.
Perform the following steps to search for the Deleted Objects.

1. Execute the following command at Windows PowerShell on the server computer, where the Organizational Unit and its member objects were removed.

   ```powershell
   Get-ADObject -SearchBase "CN=Deleted Objects,DC=www,DC=domain,DC=com" -
   ldapFilter:"(msDs-lastKnownRDN=OU_NAME)" -IncludeDeletedObjects -
   Properties lastKnownParent
   ```

   ![Figure 8: Command to search for the deleted Organizational Unit](image)

   Replace “OU_NAME” with the relative distinguished name (RDN) of the deleted organizational unit. Similarly, you can replace “domain” with your domain name.

2. Now, copy the displayed value of “Distinguished Name” to trace the member objects of this organizational unit, which were deleted. Execute the following command.

   ```powershell
   Get-ADObject -SearchBase "CN=Deleted Objects,DC=www,DC=domain,DC=com" -
   Filter {lastKnownParent -eq 'OU= OU_NAME\0ADEL:a64811e4-b306-43c0-b50d-645b321eb5d4,CN=Deleted Objects,DC=www,DC=domain,DC=com'} -
   IncludeDeletedObjects -Properties lastKnownParent | ft
   ```

   NOTE: Add double backslashes (\) between the relative distinguished name and new value.
3. You have to restore the deleted organizational unit before restoring its deleted member objects. Execute the following command.

   Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=OU_NAME)" -IncludeDeletedObjects | Restore-ADObject

4. Now, execute the following command to restore all deleted objects, which were member of the already restored Organizational Unit.

   Get-ADObject -SearchBase "CN=Deleted Objects,DC=www,DC=domain,DC=com" -Filter "{lastKnownParent -eq "OU=OU_NAME,DC=www,DC=domain,DC=com"}"  -IncludeDeletedObjects | Restore-ADObject
Perform the following steps.

1. At the RUN or command prompt, type “LDP” and press “Enter” key to access LDP console.
2. On the “Connection” menu, click “Connect” to access the following dialog box.

![Connect dialog box](image)

3. Enter the domain name. The default port is 389.
4. Click “OK” to establish the connection with the domain.
5. On the “Connection” menu, click “Bind” to access the following dialog box.

![Bind dialog box](image)

6. If you are logged on as an administrator, then select “Bind as currently logged on user” option. Else select “Bind with credentials” option, and provide the login credentials of an administrator.
7. Click “OK.”
8. On the “Options” menu, click “Controls” to access the following dialog box.
9. In “Load Predefined” drop-down list, click “Return deleted objects” to access the deleted objects in Active Directory.

10. Click “OK.”

11. On the “View” menu, click “Tree” to access the following dialog box.

12. Enter the following distinguished name in it.

   CN=Deleted Objects,DC=www,DC=domain,dc=com

13. Click “OK” to show the list of deleted objects in the left panel.
14. Perform the following steps for each deleted organizational unit or object.
   a. Right-click the deleted Organizational Unit or object, and click "Modify" command to access the following dialog box.

![Figure 16: Modify dialog box](image_url)
b. Type “isDeleted” in “Edit Entry Attribute” text box. Leave “Values” text box blank.

c. Under “Operation”, click “Delete” option, and then click “Enter.”

d. Type “distinguishedName” name in “Edit Entry Attribute” text box.

e. Type the original distinguished name (DN) of this object or organizational unit:


g. Please make sure that “Extended” check box is selected.

15. You cannot restore the object to its parent Organizational Unit, rather it can be restored only the root of domain, that is, under “www.domain.com”.

16. Once recovered, you have to move the object manually to its earlier parent container.

---

Figure 17: Restoring the deleted Organizational Unit from LDP.exe

a. Click “Enter” and then click “Run” to restore the deleted object.

Repeat the above steps for each deleted object.
Restore Deleted Objects using AD Administrative Center

Perform the following steps to recover the deleted objects in Windows Server 2012 and Windows Server 2012 R2.

1. Start “Active Directory Administrative Center.”
2. If Recycle Bin is enabled, click the domain name and then click “Deleted Objects” in the context menu.
3. It shows “Deleted Objects” container.
4. It is recommended to restore the parent container first before restoring the child objects.

Right-click the container and then click “Restore” to restore the deleted container.

Follow the same step to restore other objects.

Limitations of Native Object Restoration

Recovering or re-animating deleted objects in the Active Directory is a complex process that involves multiple steps. It can often take a lot of time and patience which isn't ideal when dealing with deadlines. The native methods are not completely reliable and currently Windows Server OS offers no way to restore deleted objects if they have entered a “recycled” or “totally deleted” state. There is also no method to revert the value of an object to an earlier state.

LepideAuditor Suite

LepideAuditor Suite is a comprehensive solution that audits, tracks and monitors Active Directory, Group Policy Objects, Exchange Server, SQL Server, SharePoint and File Server. It creates backup snapshots of Active Directory and Group Policy Objects at predefined intervals. The Administrator can use these snapshots to restore deleted objects, even if they have entered into a “recycled” state or physically deleted from Active Directory.

From the LepideAuditor Suite interface, click “Restore” in the “Audit Reports” Tab to start the “Lepide Object Restore Wizard.”
Select the objects you want to restore and click “Next” to proceed. This wizard can restore Deleted Objects and lets you revert the state of modified objects to an earlier date.

**Conclusion**

There are numerous different ways to restore deleted objects using Windows Server Operating System, including authoritative restore, PowerShell commands, LDP.exe and the Active Directory Administrative Center. However, the deleted objects cannot be restored if they have already entered into a “recycled” or “physically deleted” state. In these situations, you can use LepideAuditor Suite to restore the deleted objects from backup snapshots.