REANIMATING DELETED OBJECTS IN ACTIVE DIRECTORY

WHITEPAPER

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

Active Directory Recycle Bin was introduced in Windows Server 2008 R2. By default, this feature is disabled in Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

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.

Before and after enabling Active Directory Recycle Bin

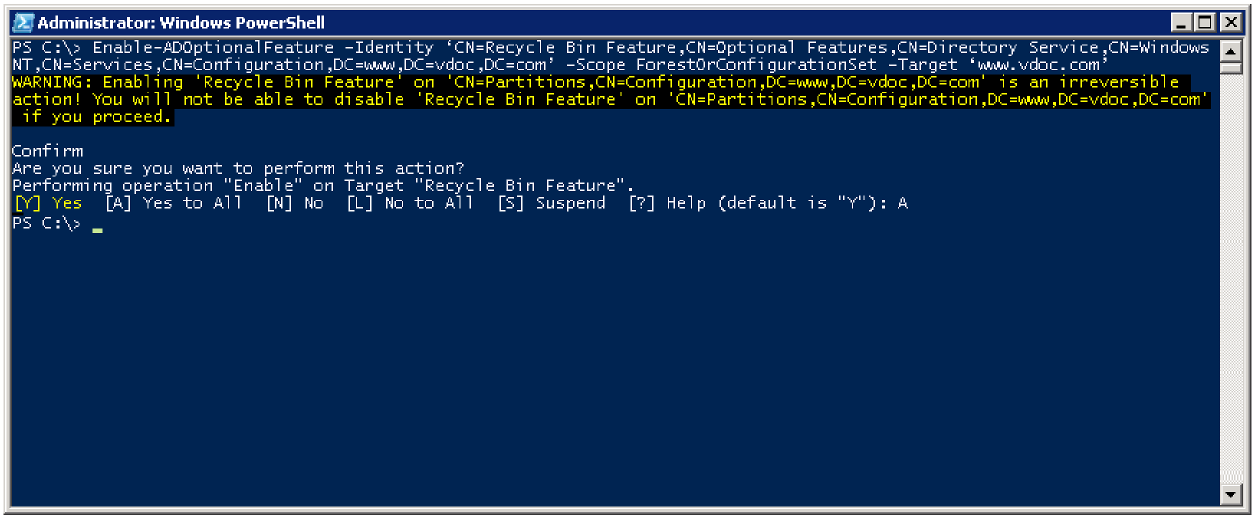
Before	After
Deleted object enters straight into “tombstone” state.	Deleted object enters into “logically deleted” state.
After 60 to 180 days, the “tombstone” lifetime expires and the deleted object is physically erased.	After 60 to 180 days, the deleted object lifetime expires and the deleted object enters into a “recycled” state. After another 60 to 180 days, the “recycled’ object is physically erased.
The deleted Object can be restored from “tombstone” state before the Tombstone Lifetime of 60 days to 180 days expires.	The deleted Object can be restored from “logically deleted” state before Deleted Object Lifetime of 60 days to 180 days expires.
The administrator has to use authoritative restoration, which is a complex process, to restore the deleted object.	The administrator can use Windows PowerShell commands, LDP.exe, and AD Administrative Center to restore the deleted objects. These methods are relatively easy.

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’
```



```
PS C:\> Enable-ADOptionalFeature -Identity ‘CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=www,DC=vdoc,DC=com’ -Scope ForestOrConfigurationSet -Target ‘www.vdoc.com’
WARNING: Enabling 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=www,DC=vdoc,DC=com' is an irreversible
action! You will not be able to disable 'Recycle Bin Feature' on 'CN=Partitions,CN=Configuration,DC=www,DC=vdoc,DC=com'
 if you proceed.

Confirm
Are you sure you want to perform this action?
Performing operation "Enable" on Target "Recycle Bin Feature".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
PS C:\> _
```

Figure 1: Command to enable Active Directory Recycle Bin

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.

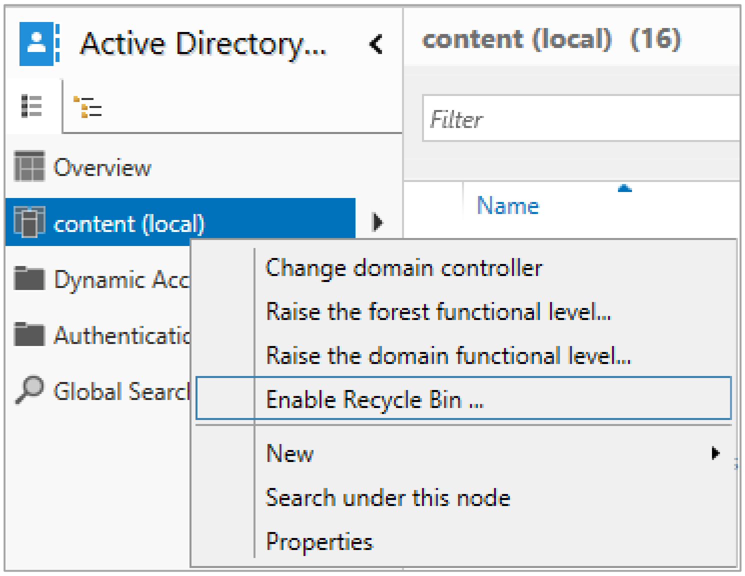
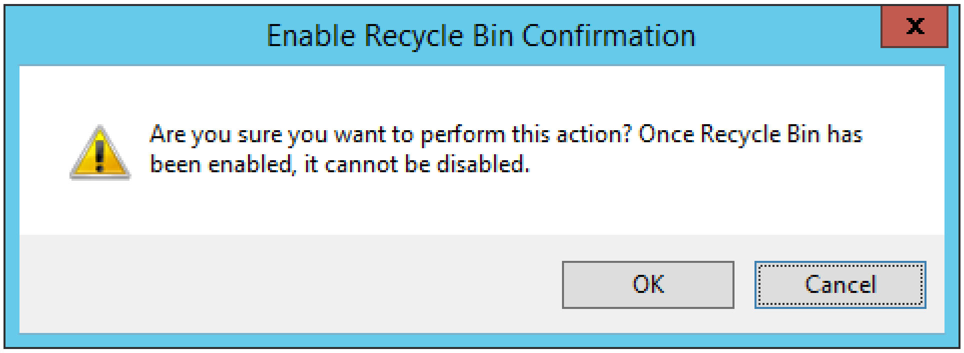


Figure 2: Option to enable Recycle Bin in Windows Server 2012 R2

It shows the following dialog box, which asks for the user confirmation before enabling the recycle bin.

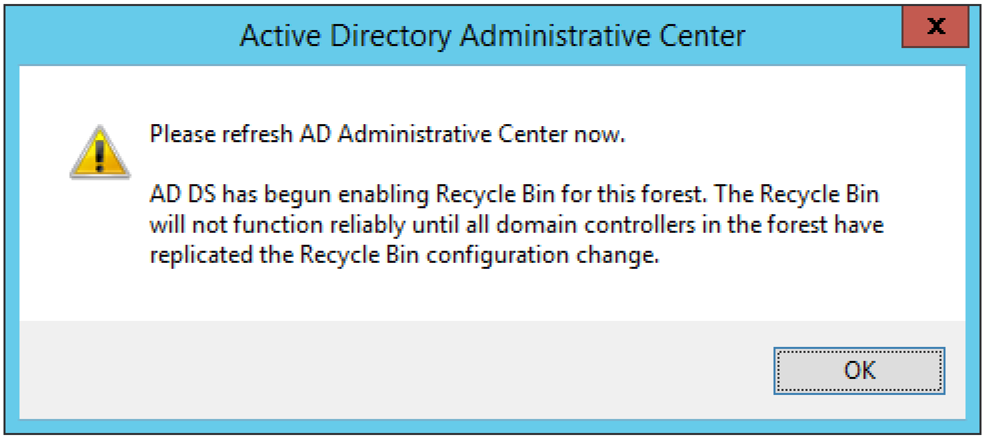


Enable Recycle Bin Confirmation

Are you sure you want to perform this action? Once Recycle Bin has been enabled, it cannot be disabled.

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.



Active Directory Administrative Center

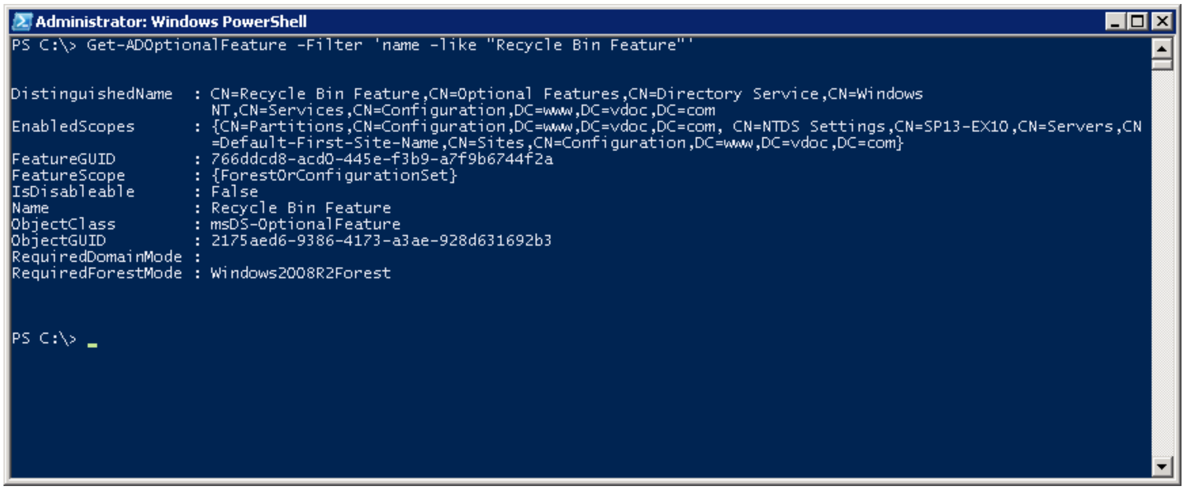
Please refresh AD Administrative Center now.

AD DS has begun enabling Recycle Bin for this forest. The Recycle Bin will not function reliably until all domain controllers in the forest have replicated the Recycle Bin configuration change.

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"'
```



```
PS C:\> Get-ADOptionalFeature -Filter 'name -like "Recycle Bin Feature"'


DistinguishedName  : CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows
                     NT,CN=Services,CN=Configuration,DC=www,DC=vdoc,DC=com
EnabledScopes      : {CN=Partitions,CN=Configuration,DC=www,DC=vdoc,DC=com, CN=NTDS Settings,CN=SP13-EX10,CN=Servers,CN
                     =Default-First-Site-Name,CN=Sites,CN=Configuration,DC=www,DC=vdoc,DC=com}
FeatureGUID        : 766ddcd8-acd0-445e-f3b9-a7f9b6744f2a
FeatureScope       : {ForestOrConfigurationSet}
IsDisableable      : False
Name               : Recycle Bin Feature
ObjectClass        : msDS-OptionalFeature
ObjectGUID         : 2175aed6-9386-4173-a3ae-928d631692b3
RequiredDomainMode :
RequiredForestMode : Windows2008R2Forest



PS C:\> _
```

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.

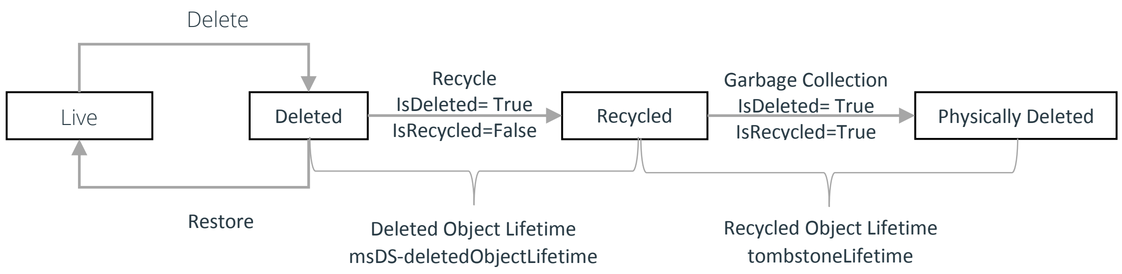


Figure 6: Lifecycle of an Active Directory Object

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.

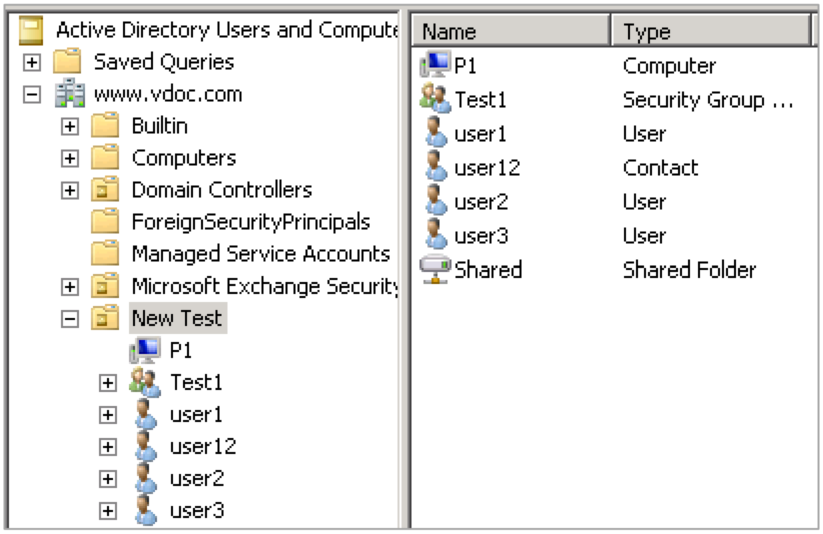
You can restore the object when it is in a “logically deleted” state, before the Deleted Object Lifetime (msDS-deletedObjectLifetime) expires, by using Windows PowerShell commands, LDP.exe, AD Administrative Center, or third party tools such as LepideAuditor Suite. The process to restore an object from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



```
Active Directory Users and Compute
⊞ Saved Queries
⊟ www.vdoc.com
    ⊞ Builtin
    ⊞ Computers
    ⊞ Domain Controllers
      ForeignSecurityPrincipals
      Managed Service Accounts
    ⊞ Microsoft Exchange Security
    ⊟ New Test
          P1
        ⊞ Test1
        ⊞ user1
        ⊞ user12
        ⊞ user2
        ⊞ user3
```

Name	Type
P1	Computer
Test1	Security Group ...
user1	User
user12	Contact
user2	User
user3	User
Shared	Shared Folder

Figure 7: Sample OU that has been deleted by mistake

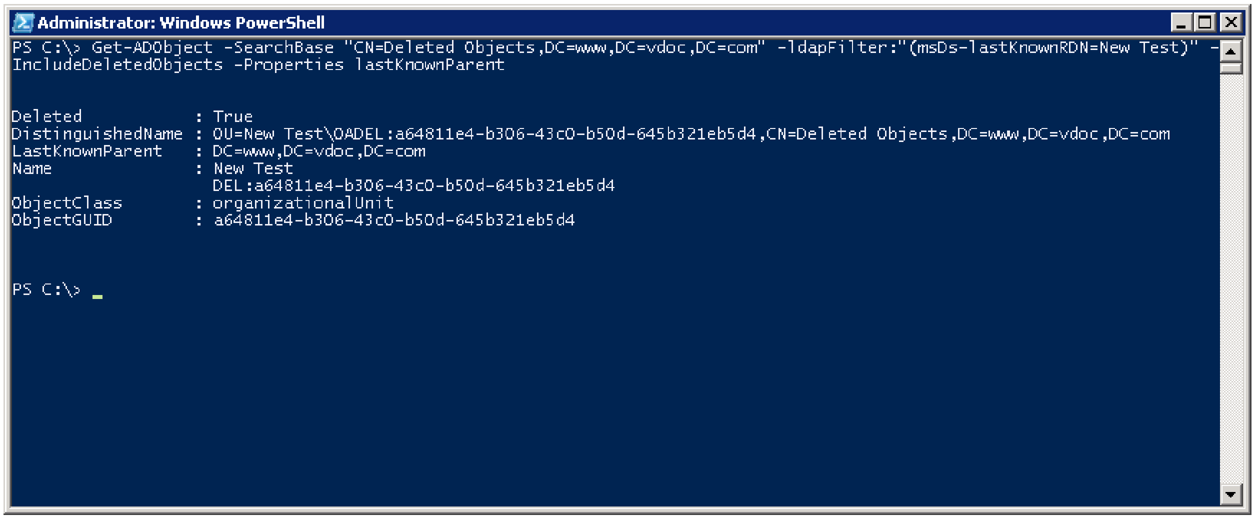
WARNING: Please do not delete an organizational unit or object in a live environment to test the commands and operations listed in this article. We have tried these steps in a sample environment.

Restore Deleted Objects using Windows PowerShell

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.

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

   ```
   PS C:\> Get-ADObject -SearchBase "CN=Deleted Objects,DC=www,DC=vdoc,DC=com" -ldapFilter:"(msDs-lastKnownRDN=New Test)" -
   IncludeDeletedObjects -Properties lastKnownParent


   Deleted           : True
   DistinguishedName : OU=New Test\0ADEL:a64811e4-b306-43c0-b50d-645b321eb5d4,CN=Deleted Objects,DC=www,DC=vdoc,DC=com
   LastKnownParent   : DC=www,DC=vdoc,DC=com
   Name              : New Test
                       DEL:a64811e4-b306-43c0-b50d-645b321eb5d4
   ObjectClass       : organizationalUnit
   ObjectGUID        : a64811e4-b306-43c0-b50d-645b321eb5d4



   PS C:\> _
   ```

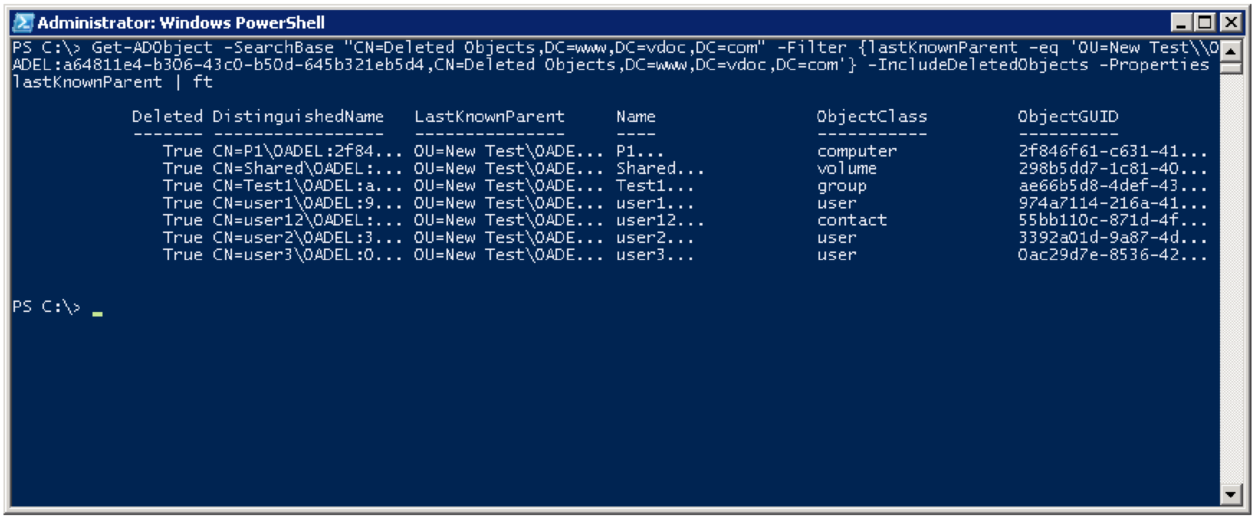
   Figure 8: Command to search for the deleted Organizational Unit

   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.

   ```
   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.



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

            Deleted DistinguishedName   LastKnownParent     Name                ObjectClass         ObjectGUID
            ------- -----------------   ---------------     ----                -----------         ----------
               True CN=P1\0ADEL:2f84... OU=New Test\0ADE... P1...               computer            2f846f61-c631-41...
               True CN=Shared\0ADEL:... OU=New Test\0ADE... Shared...           volume              298b5dd7-1c81-40...
               True CN=Test1\0ADEL:a... OU=New Test\0ADE... Test1...            group               ae66b5d8-4def-43...
               True CN=user1\0ADEL:9... OU=New Test\0ADE... user1...            user                974a7114-216a-41...
               True CN=user12\0ADEL:... OU=New Test\0ADE... user12...           contact             55bb110c-871d-4f...
               True CN=user2\0ADEL:3... OU=New Test\0ADE... user2...            user                3392a01d-9a87-4d...
               True CN=user3\0ADEL:0... OU=New Test\0ADE... user3...            user                0ac29d7e-8536-42...


PS C:\> _
```

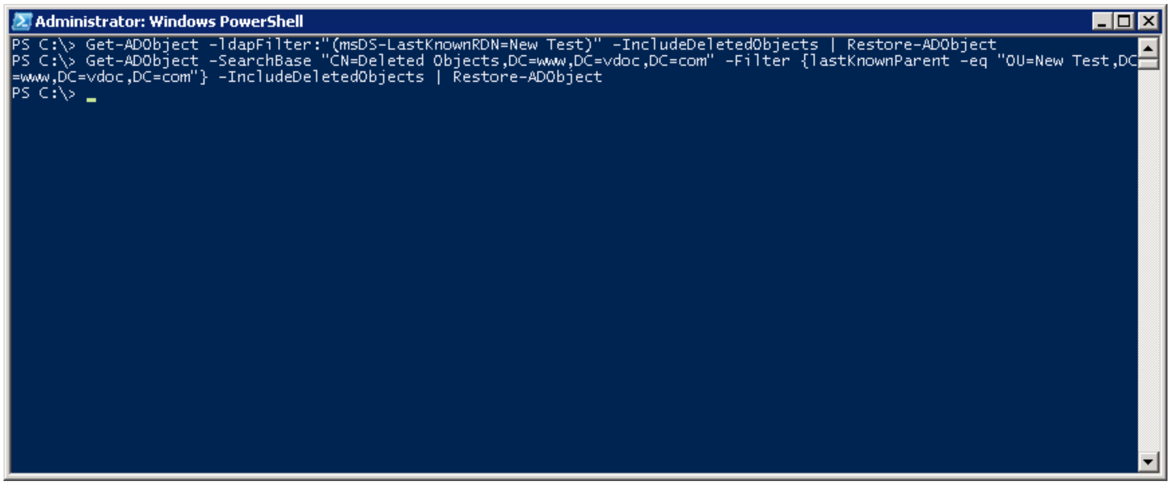
Figure 9: Command to display the list of deleted objects in the deleted organizational unit

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
```



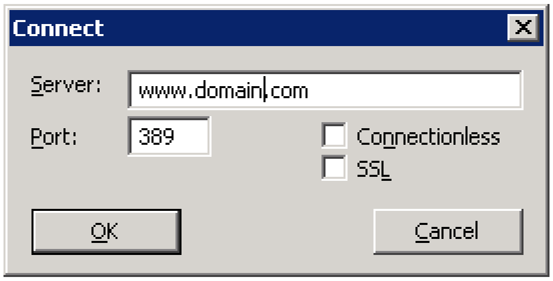
```
PS C:\> Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=New Test)" -IncludeDeletedObjects | Restore-ADObject
PS C:\> Get-ADObject -SearchBase "CN=Deleted Objects,DC=www,DC=vdoc,DC=com" -Filter {lastKnownParent -eq "OU=New Test,DC
=www,DC=vdoc,DC=com"} -IncludeDeletedObjects | Restore-ADObject
PS C:\> _
```

Figure 10: Command to restore all deleted objects of which parent is the specified Organizational Unit's name

Restore Deleted Objects using LDP.exe

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.



Server: www.domain.com

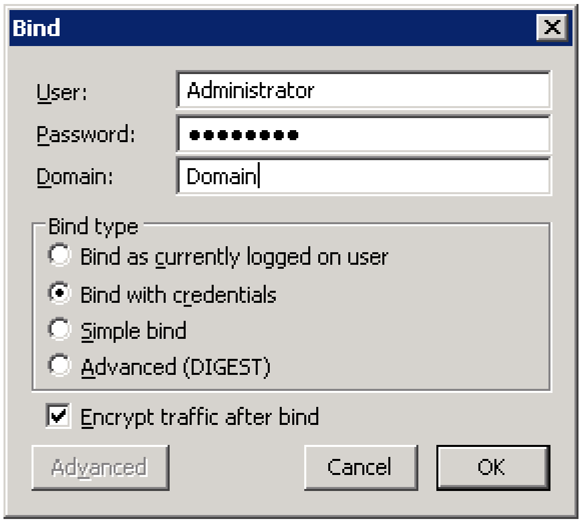
Port: 389

□ Connectionless

□ SSL

Figure 11: “Connect” dialog box

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.



User: Administrator

Password: ●●●●●●●●●

Domain: Domain

Bind type

○ Bind as currently logged on user

● Bind with credentials

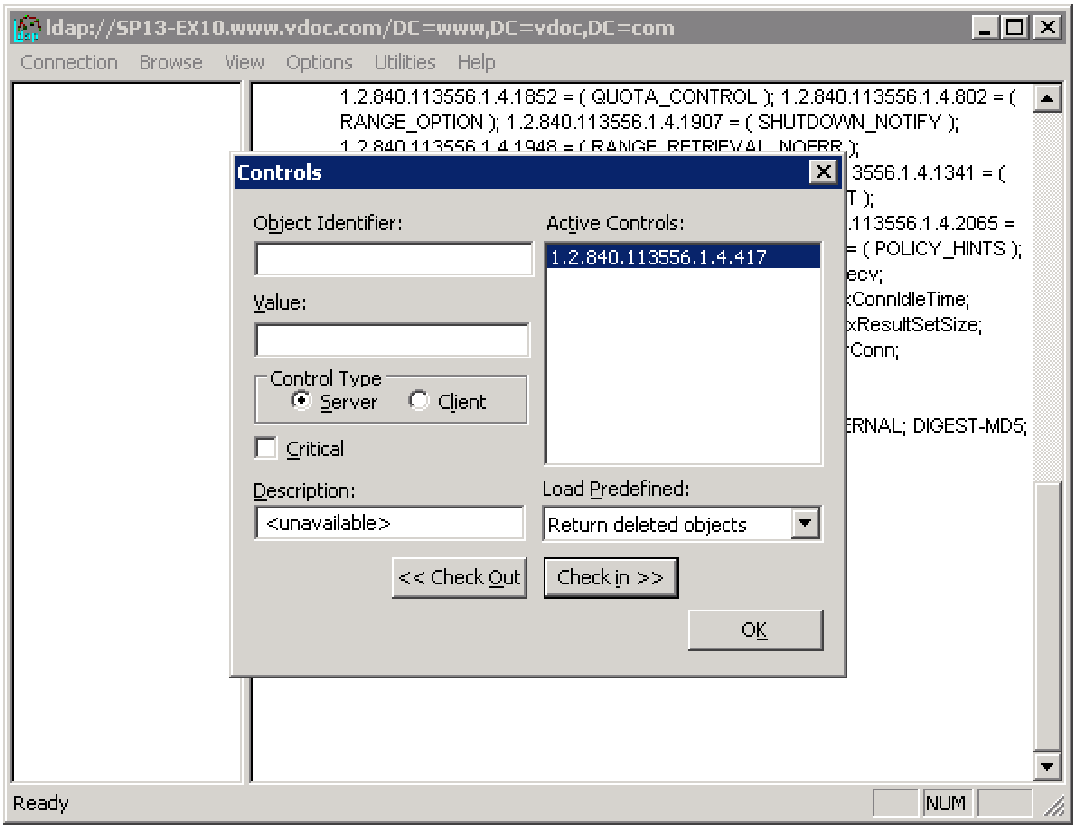
○ Simple bind

○ Advanced (DIGEST)

☑ Encrypt traffic after bind

Figure 12:”Bind” dialog box

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.



```
1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = (
RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY );
1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR );
3556.1.4.1341 = (
T );
.113556.1.4.2065 =
= ( POLICY_HINTS );
ecv;
ConnIdleTime;
xResultSetSize;
Conn;

ERNAL; DIGEST-MD5;
```

Object Identifier:

Value:

Control Type ● Server ○ Client

□ Critical

Description: <unavailable>

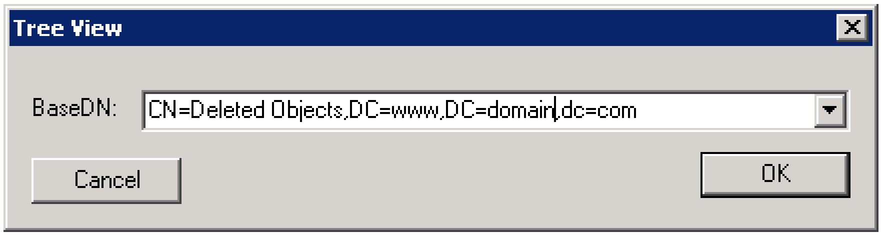
Active Controls: 1.2.840.113556.1.4.417

Load Predefined: Return deleted objects

Figure 13: "Controls" 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.

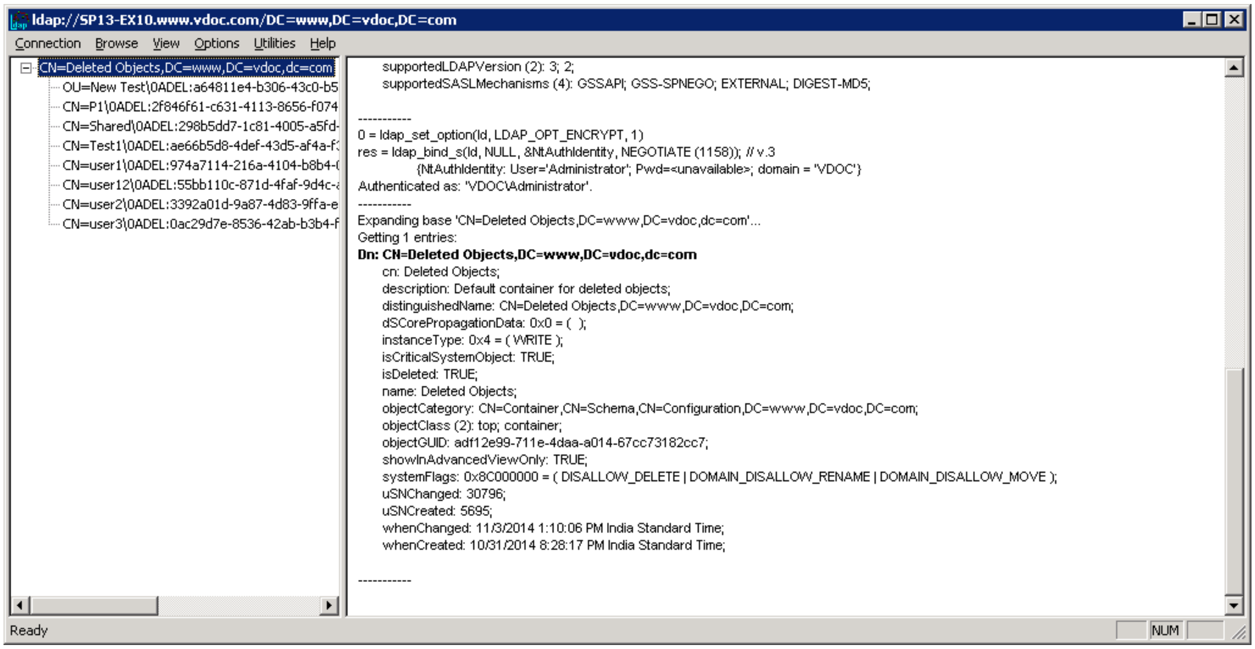
    `CN=Deleted Objects,DC=www,DC=domain,dc=com`



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

Figure 14: Tree view dialog box

13. Click "OK" to show the list of deleted objects in the left panel.



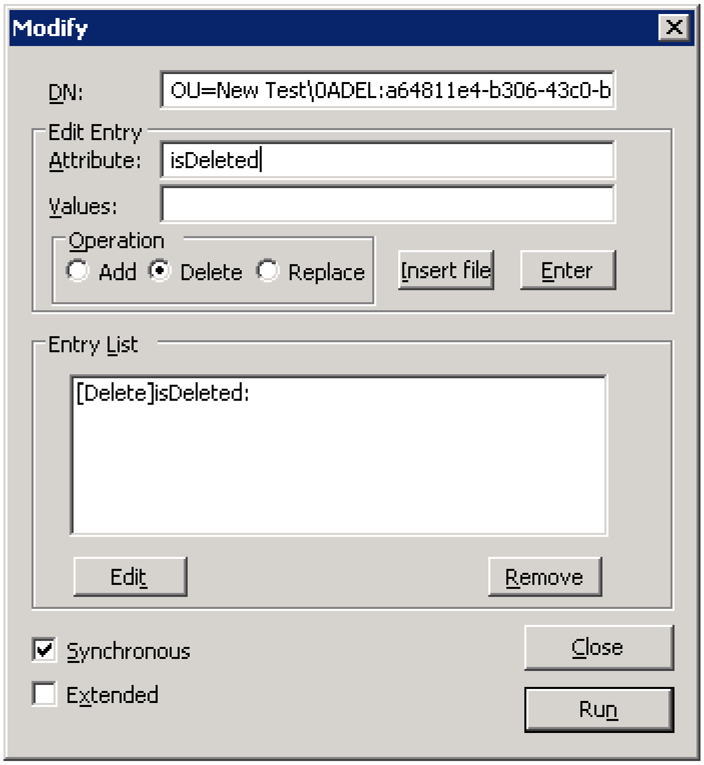
```
CN=Deleted Objects,DC=www,DC=vdoc,dc=com
    OU=New Test\0ADEL:a64811e4-b306-43c0-b5
    CN=P1\0ADEL:2f846f61-c631-4113-8656-f074
    CN=Shared\0ADEL:298b5dd7-1c81-4005-a5fd-
    CN=Test1\0ADEL:ae66b5d8-4def-43d5-af4a-f
    CN=user1\0ADEL:974a7114-216a-4104-b8b4-(
    CN=user12\0ADEL:55bb110c-871d-4faf-9d4c-
    CN=user2\0ADEL:3392a01d-9a87-4d83-9ffa-e
    CN=user3\0ADEL:0ac29d7e-8536-42ab-b3b4-f
```

```
      supportedLDAPVersion (2): 3; 2;
      supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
0 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 1)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, NEGOTIATE (1158)); // v.3
            {NtAuthIdentity: User='Administrator'; Pwd=<unavailable>; domain = 'VDOC'}
Authenticated as: 'VDOC\Administrator'.
-----------
Expanding base 'CN=Deleted Objects,DC=www,DC=vdoc,dc=com'...
Getting 1 entries:
Dn: CN=Deleted Objects,DC=www,DC=vdoc,dc=com
      cn: Deleted Objects;
      description: Default container for deleted objects;
      distinguishedName: CN=Deleted Objects,DC=www,DC=vdoc,DC=com;
      dSCorePropagationData: 0x0 = (  );
      instanceType: 0x4 = ( WRITE );
      isCriticalSystemObject: TRUE;
      isDeleted: TRUE;
      name: Deleted Objects;
      objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=www,DC=vdoc,DC=com;
      objectClass (2): top; container;
      objectGUID: adf12e99-711e-4daa-a014-67cc73182cc7;
      showInAdvancedViewOnly: TRUE;
      systemFlags: 0x8C000000 = ( DISALLOW_DELETE | DOMAIN_DISALLOW_RENAME | DOMAIN_DISALLOW_MOVE );
      uSNChanged: 30796;
      uSNCreated: 5695;
      whenChanged: 11/3/2014 1:10:06 PM India Standard Time;
      whenCreated: 10/31/2014 8:28:17 PM India Standard Time;

-----------
```

Figure 15: Displaying the list of the deleted objects

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.



DN: OU=New Test\0ADEL:a64811e4-b306-43c0-b

Attribute: isDeleted

Values:

○ Add ● Delete ○ Replace

[Delete]isDeleted:

☑ Synchronous

☐ Extended

Figure 16: Modify dialog box

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:

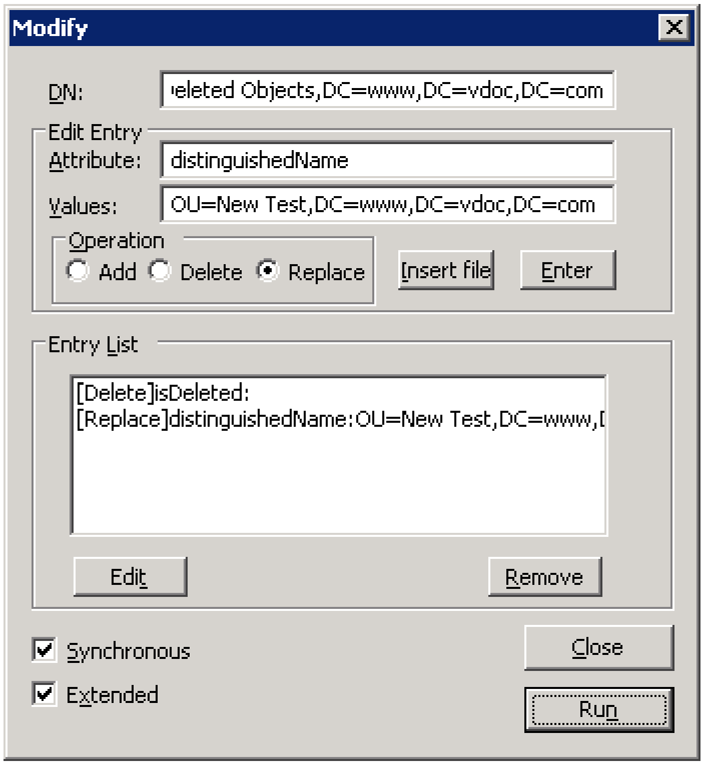
```
CN=”New Test”,DC=”www”,DC=”Domain”,DC=”com”
```

f. Under “Operation”, click “Replace” option.

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.



Modify

DN: ›eleted Objects,DC=www,DC=vdoc,DC=com

Edit Entry

Attribute: distinguishedName

Values: OU=New Test,DC=www,DC=vdoc,DC=com

Operation

○ Add ○ Delete ● Replace

Entry List

[Delete]isDeleted:
[Replace]distinguishedName:OU=New Test,DC=www,[

☑ Synchronous

☑ Extended

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.

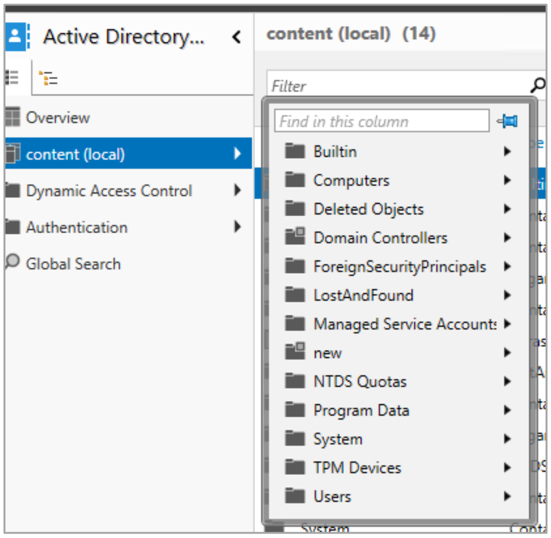
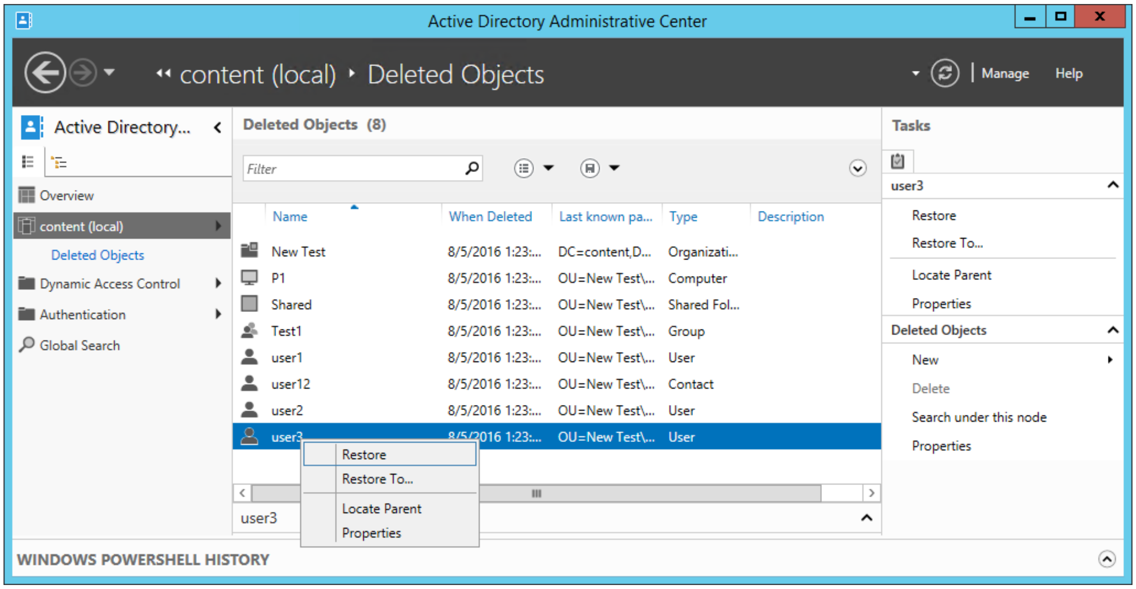


Figure 18: Option to view Deleted Objects container

3. It shows "Deleted Objects" container.



Deleted Objects (8)

Name	When Deleted	Last known pa...	Type	Description
New Test	8/5/2016 1:23:...	DC=content,D...	Organizati...	
P1	8/5/2016 1:23:...	OU=New Test\...	Computer	
Shared	8/5/2016 1:23:...	OU=New Test\...	Shared Fol...	
Test1	8/5/2016 1:23:...	OU=New Test\...	Group	
user1	8/5/2016 1:23:...	OU=New Test\...	User	
user12	8/5/2016 1:23:...	OU=New Test\...	Contact	
user2	8/5/2016 1:23:...	OU=New Test\...	User	
user3	8/5/2016 1:23:...	OU=New Test\...	User	

Figure 19: Deleted Objects Container in AD Administrative Center

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.

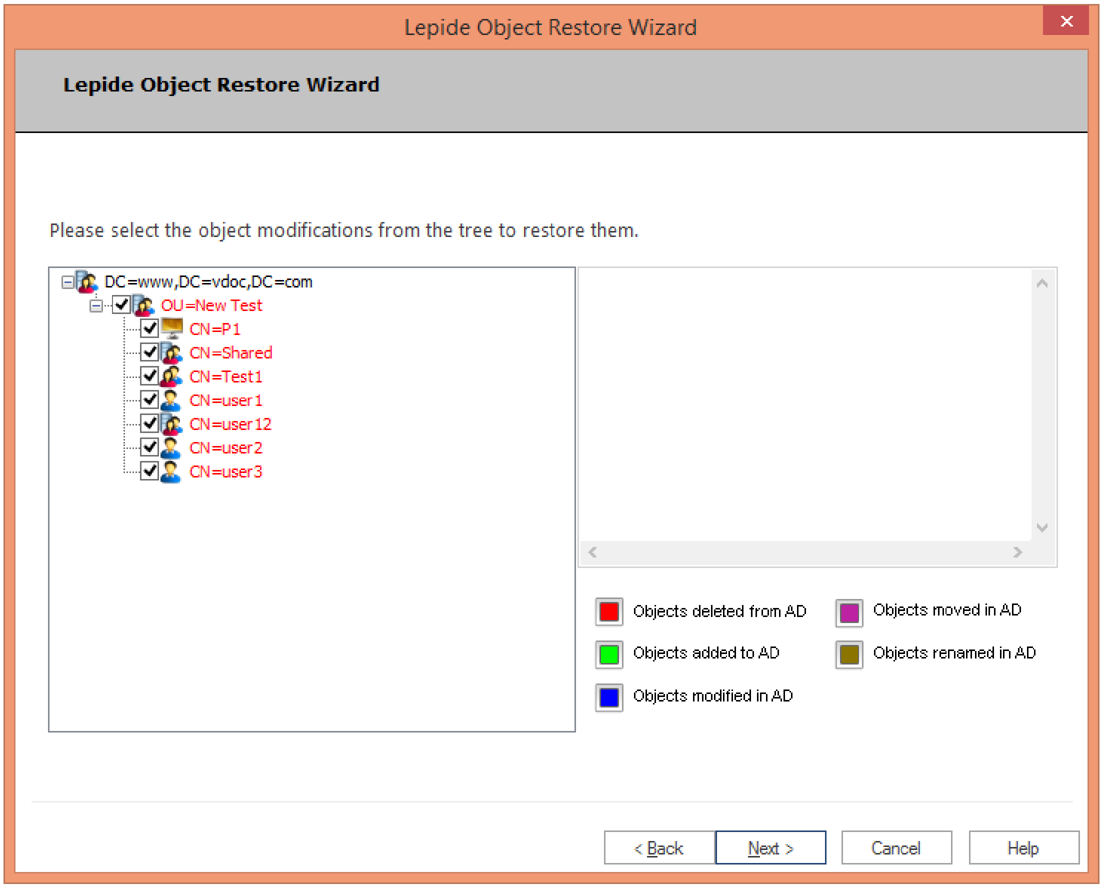
Limitations of Native Object Restoration

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.”



Lepide Object Restore Wizard

Lepide Object Restore Wizard

Please select the object modifications from the tree to restore them.

- DC=www,DC=vdoc,DC=com
  - ☑ OU=New Test
    - ☑ CN=P1
    - ☑ CN=Shared
    - ☑ CN=Test1
    - ☑ CN=user1
    - ☑ CN=user12
    - ☑ CN=user2
    - ☑ CN=user3

🟥 Objects deleted from AD 🟪 Objects moved in AD

🟩 Objects added to AD 🟫 Objects renamed in AD

🟦 Objects modified in AD

Figure 20: Restore the Deleted Objects using LepideAuditor Suite

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.