Windows Server 2008 R2 introduced Active Directory Recycle Bin, a Windows PowerShell–based feature that allowed you to restore objects deleted from the Active Directory Domain Services database. Windows Server 2012 brings this functionality of Active Directory Recycle Bin to Active Directory Administrative Center, the graphical tool for managing Active Directory Domain Services that also first appeared in Windows Server 2008 R2.

This section covers the following topics:

 Enable Active Directory Recycle Bin

- Use Active Directory Recycle Bin to restore deleted objects
- Set the deleted object lifetime in a domain

Restoring deleted objects in Active Directory

Before Windows Server 2008 R2, there were just two methods you could use to restore an object that had accidentally been deleted from Active Directory Domain Services: You could perform an authoritative restore with the Ntdsutil command-line utility, or you could use a procedure called tombstone reanimation. Both of these methods, however, had significant drawbacks. With Ntdsutil, the drawbacks were that you first had to boot the domain controller into Directory Services Restore Mode (making the domain controller temporarily unavailable to clients on the network) and that you could only restore deleted objects that you had previously backed up. With tombstone reanimation, the drawbacks were that it was a complicated procedure and it couldn't be relied on to restore an object's group memberships.

For more information about performing an authoritative restore with Ntdsutil, visit *http://technet.microsoft.com/en-us/library/cc755296(v=WS.10).aspx*. For more information about reanimating tombstoned objects, visit *http://technet.microsoft.com/en-us/magazine/2007.09.tombstones.aspx*.

Active Directory Recycle Bin

Windows Server 2008 R2 and Windows Server 2012 have removed these drawbacks with Active Directory Recycle Bin. With Active Directory Recycle Bin, you don't have to take the domain controller offline to restore a deleted object, and the original group memberships of the deleted objects are preserved when you restore them.

Windows Server 2008 R2 introduced Active Directory Recycle Bin in a Windows PowerShell-only mode. Windows Server 2012 makes this new feature more accessible by bringing its functionality to the graphical Active Directory Administrative Center tool. For the exam, you need to know how to enable and use Active Directory Recycle Bin in both Windows PowerShell and Active Directory Administrative Center.

ENABLING ACTIVE DIRECTORY RECYCLE BIN

For the exam and the real world, remember that the Active Directory Recycle Bin is not enabled by default. You can use Active Directory Recycle Bin to restore only those objects that have been deleted after the feature is enabled. Objects you deleted before then can be restored only through authoritative restore or tombstone reanimation.

To enable Active Directory Recycle Bin in Windows PowerShell, first make sure that all domain controllers in the domain are running Windows Server 2008 R2 or Windows Server 2012. In addition, the functional level of your forest must be set to Windows Server 2008 R2 or higher. You can use the Get-ADForest cmdlet to check the functional level of your forest:

```
Get-ADForest ForestName
```

If you need to raise the functional level of the forest, you can use the Set-ADForestMode cmdlet with the following syntax:

```
Set-ADForestMode -Identity ForestName -ForestMode Windows2008R2Forest
```

Once your environment meets the prerequisites of Active Directory Recycle Bin, you can enable the feature by using the following Windows PowerShell command:

```
Enable-ADOptionalFeature 'Recycle Bin Feature' -scope ForestOrConfigurationSet -target DomainName -server DomainControllerName
```

To enable Active Directory Recycle Bin in the graphical user interface (GUI) in Windows Server 2012, open Active Directory Administrative Center from the Tools menu in Server Manager. Then, in Active Directory Administrative Center, right-click the domain icon in the console tree and select Enable Recycle Bin from the shortcut menu, as shown in Figure 8-9.

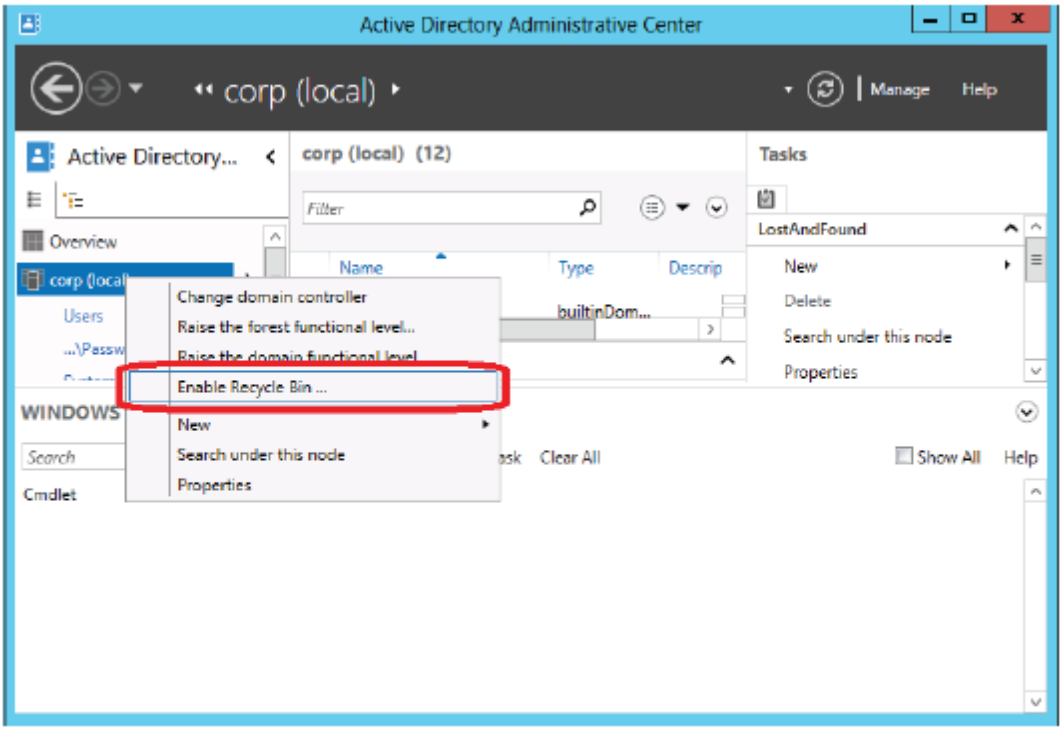

FIGURE 8-9 Enabling Active Directory Recycle Bin in Windows Server 2012.

Enabling Active Directory Recycle Bin is irreversible. In some environments, allowing administrators to see previously deleted objects might be undesirable. Consequently, you should make sure that Active Directory Recycle Bin is compatible with your organization's security policy before enabling the feature.

RESTORING DELETED OBJECTS IN ACTIVE DIRECTORY ADMINISTRATIVE CENTER

A new Deleted Objects container appears in Active Directory Administrative Center at the root of the domain container after you enable Active Directory Recycle Bin, as shown in Figure 8-10. Objects that you delete appear in this container for a period of time called the deleted object lifetime, which is 180 days by default.

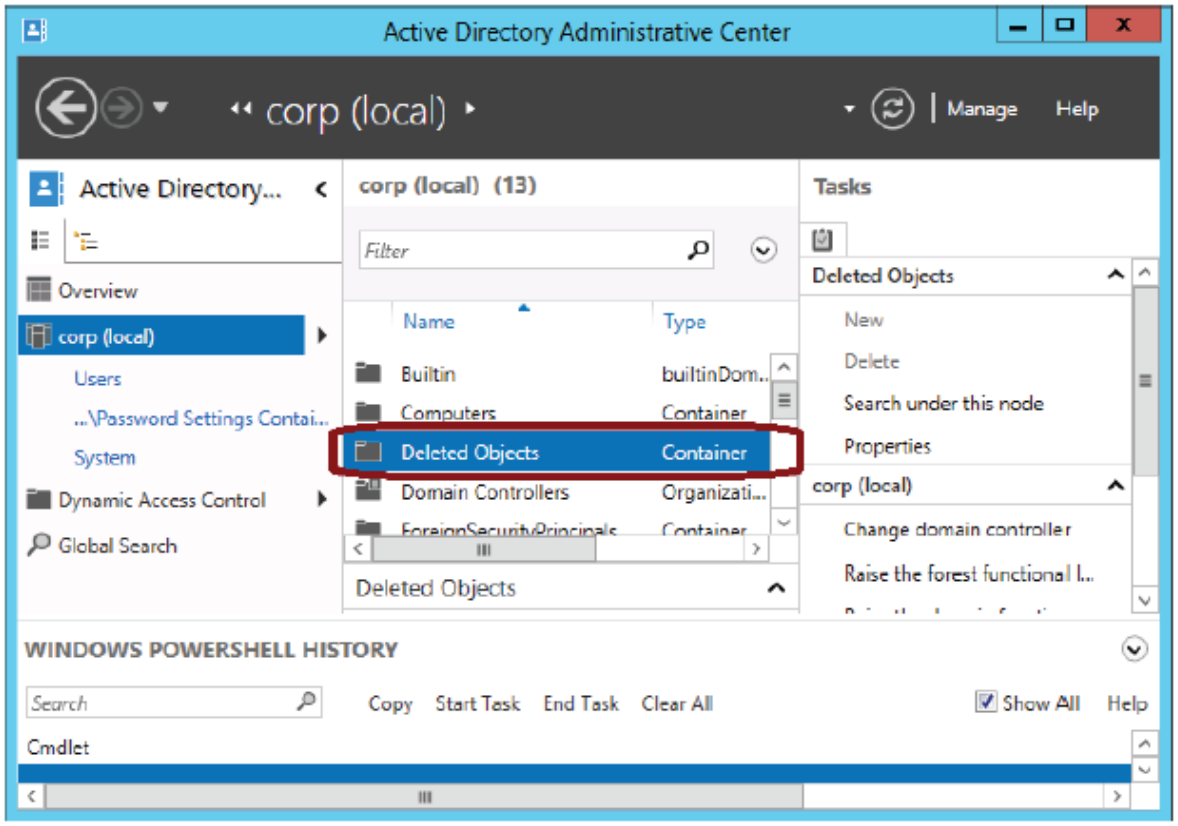

FIGURE 8-10 A Deleted Objects container appears after you enable Active Directory Recycle Bin.

Restoring an object in the GUI is simple—so simple, in fact, that it might be challenging for the exam writers to think up hard enough questions about restoring objects from the GUI. To restore the object to its last known parent container, just right-click the object and select Restore from the shortcut menu, as shown in Figure 8-11.

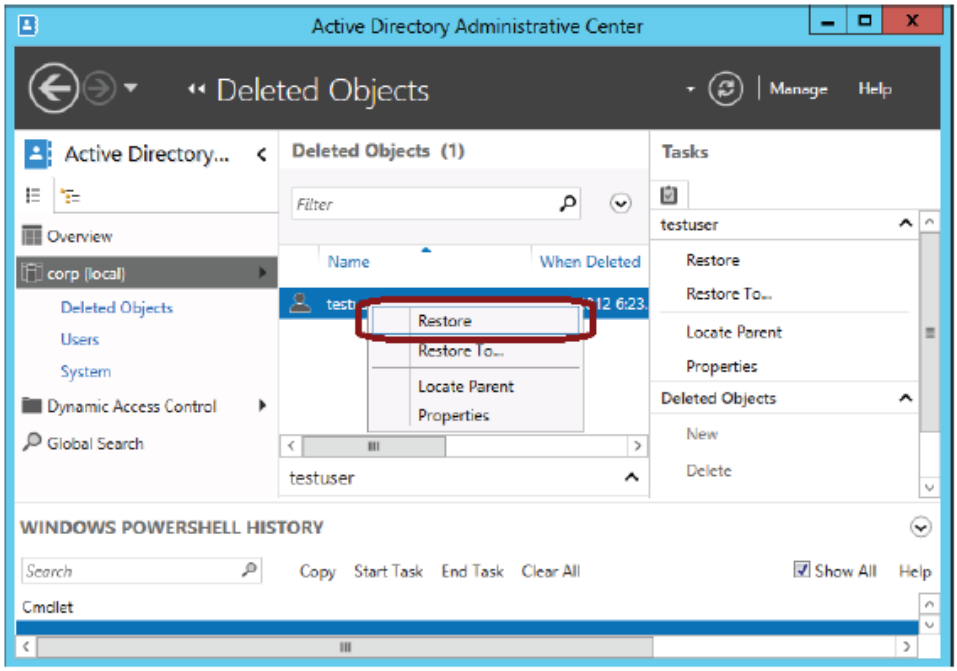

FIGURE 8-11 Restoring a deleted object in Active Directory.

To restore an object to a different container, select Restore To and select the new container in which you want the object to appear. The Locate Parent option opens the former parent container in the console.

One potential complication in restoring an object might occur if you have deleted both the container and the object. In this case, you need to restore the parent before the child object, or choose to restore the object to another container.

RESTORING DELETED OBJECTS IN WINDOWS POWERSHELL

To restore a deleted object in Windows PowerShell, first use the Get-ADObject cmdlet with the -Filter and -IncludeDeletedObjects switches, and then pipe the result to the Restore-ADObject cmdlet. For example, to restore a deleted user with the display name "Mary," type the following command at an elevated Windows PowerShell prompt:

```
Get-ADObject -Filter {DisplayName -eq "Mary"} -IncludeDeletedObjects | Restore-ADObject
```

Here's another example: To restore a user whose canonical name (CN) is like "Jorge," type the following:

```
Get-ADObject -Filter {CN -like "Jorge"} -IncludeDeletedObjects | Restore-ADObject
```

In the real world, it doesn't make much sense to restore a deleted object by using Windows PowerShell if you don't have to. However, don't be surprised if the Windows PowerShell method of Active Directory Recycle Bin still appears on the exam.

MORE INFO **For more information about how to use Get-ADObject, visit** ***http://technet.microsoft.com/en-us/library/ee617198.aspx.***

DELETED OBJECT LIFETIME

By default, you have only 180 days to restore an object after it is deleted. This period is known as the deleted object lifetime and is governed by the msDS-DeletedObjectLifetime attribute assigned to the domain. To change the value of this attribute, use the Set-ADObject cmdlet in the following manner:

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

Replace *DC=<mydomain>,DC=<com>* with the appropriate forest root domain name of your Active Directory environment, and replace *<value>* with the new value of the deleted object lifetime.

For example, to set the deleted object lifetime to 365 days, run the following command:

```
Set-ADObject -Identity "CN=Directory Service,CN=Windows
NT,CN=Services,CN=Configuration,DC=contoso,DC=com" -Partition
"CN=Configuration,DC=contoso,DC=com" -Replace:@{"msDS-DeletedObjectLifetime" = 365}
```

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of the chapter.

1. You are a network administrator for Contoso.com. You have learned that a user account was accidentally deleted from the Contoso.com Active Directory domain. The domain controllers in your network are all running Windows Server 2012. Active Directory Recycle Bin is not yet enabled.

You want to restore the deleted user account without taking any domain controller offline. What should you do?

A. Perform an authoritative restore of the deleted user account with the Ntdsutil utility.

B. Reanimate the tombstone of the deleted object.

C. Enable Active Directory Recycle Bin, and use Active Directory Administrative Center to restore the object.

D. Enable Active Directory Recycle Bin, and use Windows PowerShell to restore the object.

2. You are a network administrator for Contoso.com. You have learned that a user account for a user named Dan Park was accidentally deleted from the Contoso.com Active Directory domain. The domain controllers in your network are all running Windows Server 2012. Active Directory Recycle Bin was enabled at the time the object was deleted.

You want to restore the deleted user account without taking any domain controller offline. What should you do?
A. Restore the object from the Deleted Objects container in Active Directory Administrative Center.

B. Perform an authoritative restore using the Ntdsutil utility.

C. Reanimate the tombstone of the deleted object.

D. Run the following command:

```
Get-ADObject -Filter {displayName -eq "Dan Park"} | Restore-ADObject
```

3. You are a network administrator for Adatum.com. You have learned that all 10 user accounts in the Finance department were accidentally deleted from the Adatum.com Active Directory domain. The domain controllers in your network are all running Windows Server 2012. Active Directory Recycle Bin was enabled at the time the user accounts were deleted.

   You attempt to restore the deleted user accounts in Active Directory Administrative Center, but you receive errors indicating that objects' parent is deleted.

   You want to restore the deleted user accounts. What should you do?

   A. Use the Set-ADObject cmdlet to extend the deleted object lifetime in the domain.

   B. Re-create the parent organizational unit of the user accounts and then restore the user accounts.

   C. Restore the parent organizational unit of the user accounts and then restore the user accounts.

   D. Restart a domain controller in Directory Services Restore Mode, and perform an authoritative restore of the deleted user accounts.