Ermanno Goletto - Microsoft MVP Directory Services - MCITP - MCSA
Mario Serra - MVP Directory Services - MCITP - MCDST

Gestione AD Recycle Bin in Windows Server 2012

Introduzione

In Windows Server 2008 R2 è stata introdotta la funzionalità Active Directory Recycle Bin che permette di ripristinare oggetti di Active Directory eliminati per errore come ad esempio Account Utente, Gruppi o intere Organizational Unit (per approfondire i dettagli di questa nuova funzionalità si veda Novità di Servizi di dominio Active Directory: Cestino per Active Directory.

Con Windows Server 2012 è stata resa disponibile all'interno dell'Active Directory Administration Center la possibilità di gestire l'Active Directory Recycle Bin mediante GUI e non sono tramite PowerShell come avviene in Windows Server 2008 R2.

In questo articolo vedremo come gestire i vari aspetti dell'Active Directory Recycle Bin sia tramite GUI che tramite PowerShell dal momento che entrambi gli approcci nonostante consentano di fatto di eseguire le stesse operazioni vanno a coprire esigenze di amministrazione diverse. La GUI aumenta la produttività di operazioni da eseguire saltuariamente, mentre PowerShell consente di automatizzare processi ripetitivi o massivi.

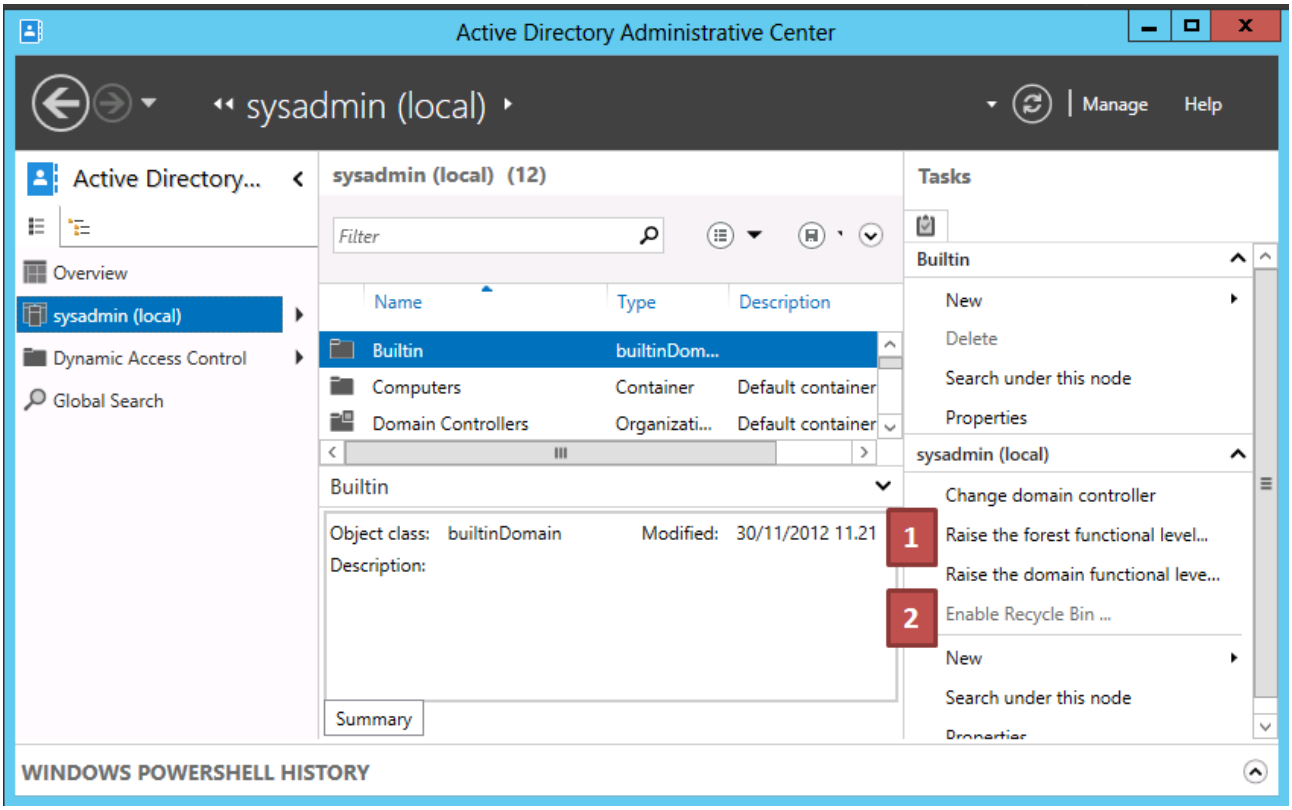
Argomenti

Abilitazione dell'Active Directory Recycle Bin 2
Modifica Deleted e Recycled object lifetime 3
Restore di oggetti Active Directory cancellati 5
Eliminazione di oggetti dall'Active Directory Recycle Bin 7
Conclusioni 7

Abilitazione dell'Active Directory Recycle Bin

Per poter abilitare l'Active Directory Recycle Bin è necessario che il livello funzionale della foresta di Active Directory sia almeno Windows 2008 R2 (questo significa che tutti Domani Controller della foresta devono essere Windows Server 2008 R2 o successivi).

E' possibile sia elevare il livello funzionale della foresta che abilitare l'Active Directory Recycle Bin mediante **Active Directory Administration Center** (ADAC dsac.exe), l'attivazione di questa funzionalità non è disattivabile.



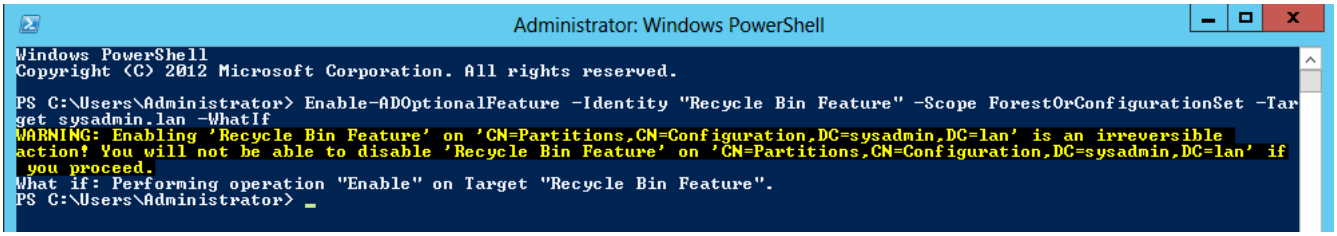
Analogamente è possibile eseguire entrambe le operazioni tramite **PowerShell**, di seguito i comandi per il controllo e l'elevazione del livello funzionale di foresta e di dominio (per cmdlets relativi ad Active Directory si veda Active Directory Cmdlets in Windows PowerShell.

```
#Verifica del livello funzionale della foresta corrente
(Get-ADForest).ForestMode

#Verifica livello funzionale del dominio corrente
(Get-ADDomain).DomainMode

#Verifica del livello funzionale di tutti i domini della foresta corrente
(Get-ADForest).Domains | Get-ADDomain | Select DomainMode, DNSRoot

#Raise livello funzionale della foresta di esempio sysadmin.lan a Windows 2008 R2 o Windows 2012
Set-ADForestMode -Identity <sysadmin.lan>- ForestMode Windows2008R2Forest
Set-ADForestMode -Identity < sysadmin.lan >- ForestMode Windows2012Forest
```

Di seguito invece i comandi per la verifica e l'abilitazione della funzionalità Active Directory Recycle Bin.

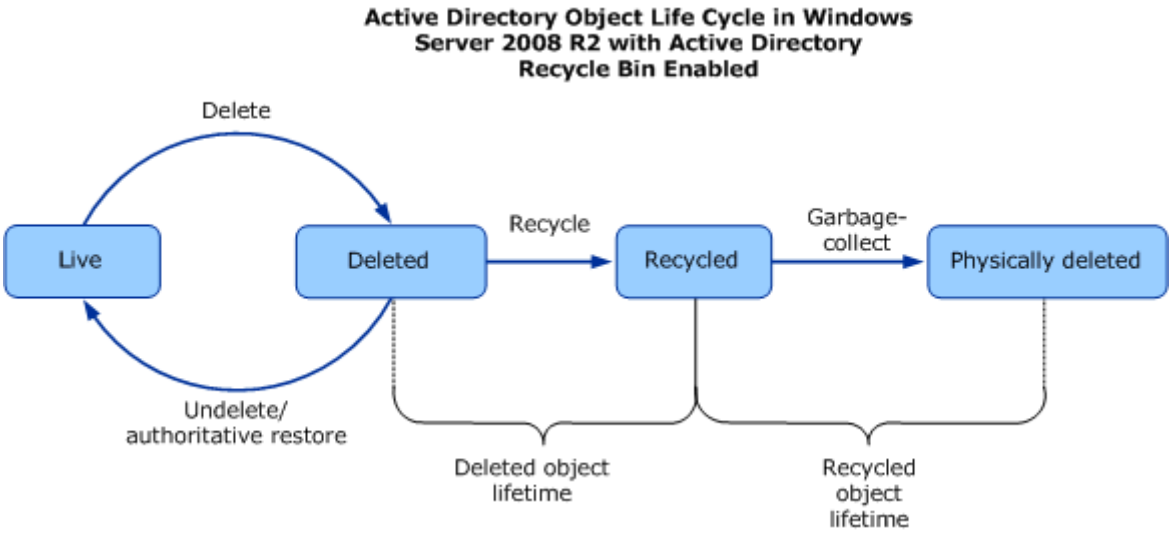
```
#Verifica abilitazione AD Recycle Bin nella foresta corrente.
#L'AD Recycle Bin fa parte delle optional features di AD.
#Al momento esiste solo una optional feature ovvero l'AD Recycle Bin.
#Il cmdlet Get-ADOptionanFeature elenca le optional features di AD e gli scope su cui sono abilitate.
#La funzionalità è disabilitata se non sono riportati scope su cui è abilitata.
Get-ADOptionalFeature -Filter * | Select Name, EnabledScopes

#Abilitazione AD Recycle Bin
Enable-ADOptionalFeature -Identity "Recycle Bin Feature" -Scope ForestOrConfigurationSet -Target <Forest FQDN>
```

A titolo d'informazione si noti che i cmdlet **PowerShell** ammettono il parametro **-WhatIf** che non esegue il comando, ma visualizza solo i cambiamenti che verrebbero eseguiti. Ad esempio utilizzando il parametro WhatIf nel comando per l'abilitazione dell'AD Recycle Bin verrà riportato che la funzionalità non è disabilitabile.



Modifica Deleted e Recycled object lifetime

Una volta abilitato l'Active Directory Recycle Bin il ciclo di vita di un oggetto cancellato in Active Directory è suddiviso in due fasi.



La prima fase è quella in cui l'oggetto passa nello stato di **Deleted** la cui durata è definita mediante l'attributo di foresta **msDS-deletedObjectLifetime**, in questa fase l'oggetto cancellato può essere recuperato tramite la funzionalità dell'Active Directory recycle Bin senza perdere alcun attributo.

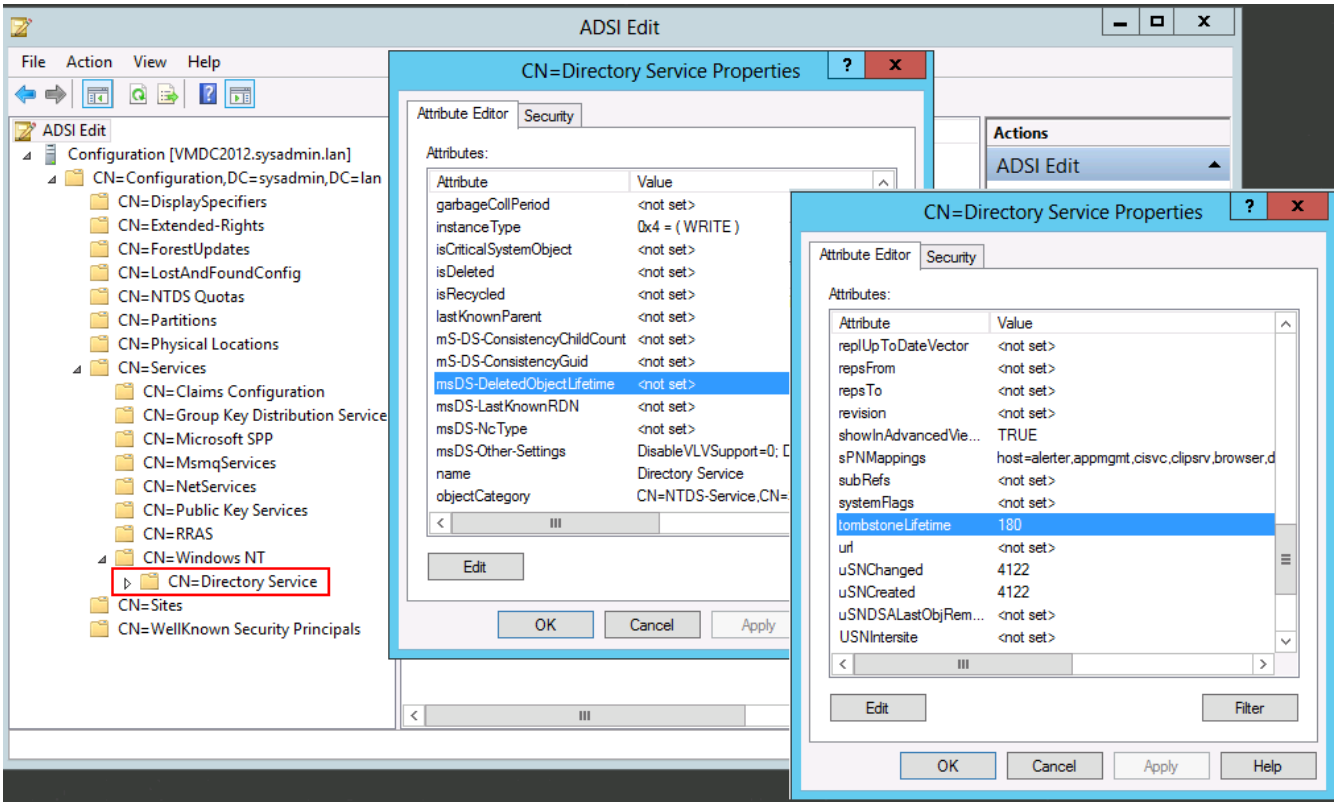
La seconda fase è quella in cui l'oggetto passa nello stato di **Recycled** la cui durata è definita mediante l'attributo di foresta **tombstoneLifetime**, in questa fase l'oggetto cancellato può ancora essere recuperato mediante *Ldp.exe*, *ADRestore* o Ripristino autorevole di AD (utilizzando *NTDSUTIL*), ma perde gli attributi di collegamento e la maggior parte degli altri attributi (tranne quelli con searchFlags = 0x8 nello schema). Di fatto questa fase dal punto di vista dello stato degli oggetti cancellati e delle possibilità del loro recupero coincide alla fase di Tumbstoned presente

quanto la funzionalità di Active Directory Recycle Bin non è abilitata. Per I dettagli sulle procedure di ripristino di oggetti Recycled o Tombstoned si veda How to restore deleted user accounts and their group memberships in Active Directory.

Per default l'attributo **msDS-deletedObjectLifetime** è impostato a NULL quindi la durata del **Deleted Object lifetime** viene determinato dal valore dell'attributo **tombstoneLifetime**. e quindi coincide con il **Recycled Object lifetime**.

L'attributo **tombstoneLifetime** per default è impostato a 180 è quindi la durata del **Recycled Object lifetime** assume il valore di 180 giorni e per quanto detto prima se l'attributo **msDS-deletedObjectLifetime** non è stato impostato anche la durata del **Deleted Object lifetime** sarà di 180 giorni.

E' possibile visualizzare e modificare gli attributi **msDS-deletedObjectLifetime** e **tombstoneLifetime** tramite GUI utilizzando **ADSI Edit** impostando le proprietà dell'oggetto Directory Service nella partizione *Configuration* del Database di Active Directory.



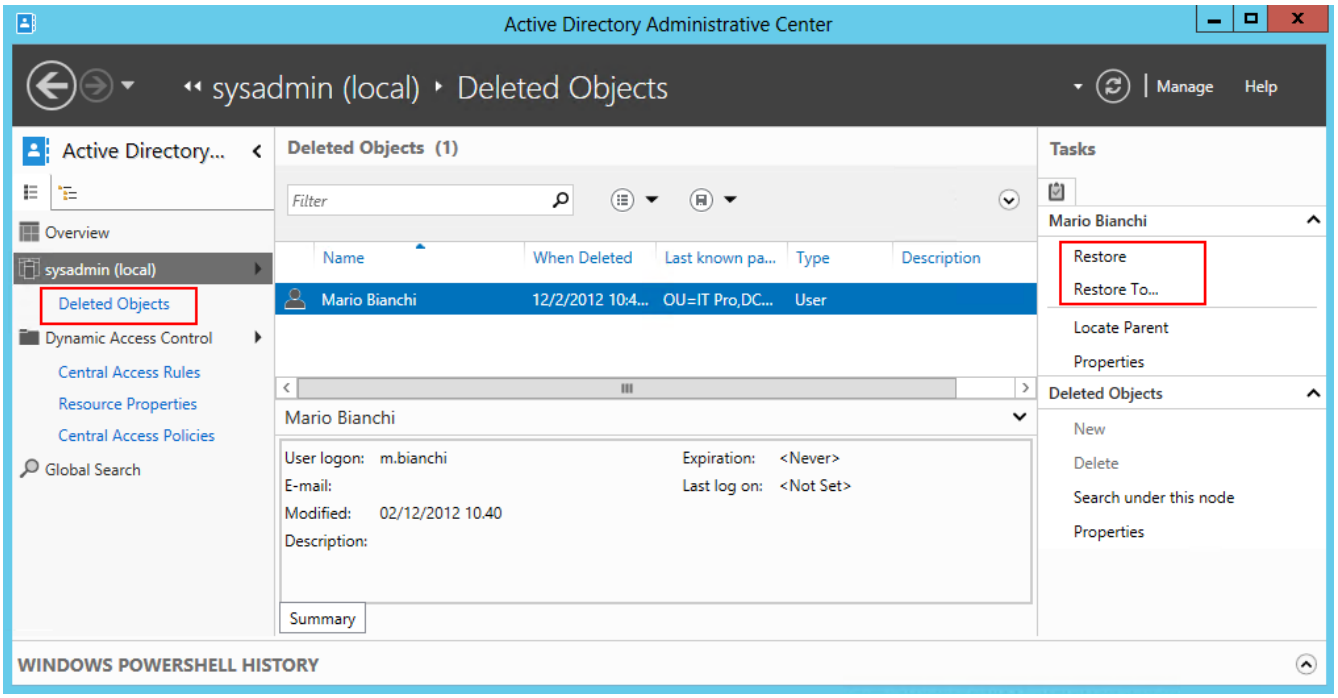
In alternativa è possibile utilizzare **PowerShell** per visualizzare e impostare gli attributi di foresta **msDS-deletedObjectLifetime** e **tombstoneLifetime**.

```
#Verifica abilitazione AD Recycle Bin nella foresta corrente.
#L'AD Recycle Bin fa parte delle optional features di AD.
#Al momento esiste solo una optional feature ovvero l'AD Recycle Bin.
#Il cmdlet Get-ADOptionanFeature elenca le optional features di AD e gli scope su cui sono abilitate.
#La funzionalità è disabilitata se non sono riportati scope su cui è abilitata.
Get-ADOptionalFeature -Filter * | Select Name, EnabledScopes
```

Restore di oggetti Active Directory cancellati

Come spiegato precedentemente gli oggetti Active Directory eliminati possono essere ripristinati tramite **Active Directory Administration Center** sino a quando tali oggetti si trovano nello stato di Deleted ovvero durante il loro **Deleted Object lifetime**.

La GUI offerta da tramite **Active Directory Administration Center** consenti di visualizzare gli oggetti eliminati all'interno del contatiner **Deleted Objects** e di recuperarli nella stessa posizione in cui si trovavano o in una Organizational Unit differente. Tramite l'opzione *Locate Parent* è anche possibile individuare il container che conteneva gli oggetti eliminati, mentre la data *Modified* indica di fatto la data di eliminazione dell'oggetto.



Le funzionalità di ripristino sono anche disponibili tramite **PowerShell** che può tornare utile nel caso di ripristino massivo di oggetti cancellati per errore. Di seguito alcuni esempi di visualizzazione e ripristino di oggetti Active Directory mediante l'uso dei cmdlet PowerShell.

```
#Elenco oggetti nel container Deleted Objects
Get-ADObject -Filter {isDeleted -eq $true} -IncludeDeletedObjects

#Elenco account utenti in stato Deleted
Get-ADObject -Filter {isDeleted -eq $true -and ObjectClass -eq "user"} -IncludeDeletedObjects

#Restore singolo account utente
#Metodo 1: basato su attributo isDeleted
Get-ADObject -Filter {sAMAccountName -eq "m.bianchi" -and isDeleted -eq $true} -IncludeDeletedObjects | Restore-ADObject

#Restore singolo account utente
#Metodo 2: basato su ricerca nel container Deleted Object del dominio di esempio sysadmin.lan
Get-ADObject -SearchBase "CN=Deleted Objects,DC=sysadmin,DC=lan" -Filter {sAMAccountName -eq "m.bianchi"} -IncludeDeletedObjects | Restore-ADObject
```

Tramite **Powershell** diventa semplice anche eseguire query più complesse come ad esempio trovare gli account utente eliminati dopo una certa data visualizzando il parent container.

```
#Elenco oggetti eliminati dopo una certa data
#con visualizzazione del parent container (lastKnownParent) e della data di eliminazione (whenChanged)
$DeletedDate=Get-Date("3/12/2012")
Get-ADObject -Filter {whenChanged -gt $DeletedDate -and isDeleted -eq $true} -IncludeDeletedObjects -Properties lastKnownParent, whenChanged
```

Per una maggiore leggibilità dei dati ottenuti dalla query è anche possibile visualizzare i dati in formato tabellare.

```
#Elenco oggetti eliminati dopo una certa data in formato tabellare
#con visualizzazione del Nome, Parent container (lastKnownParent) e data di eliminazione (whenChanged)
$DeletedDate=Get-Date("3/12/2012")
Get-ADObject -Filter {whenChanged -gt $DeletedDate -and isDeleted -eq $true} -IncludeDeletedObjects -Properties lastKnownParent, whenChanged | Format-Table -Wrap -Autosize Property Name, lastKnownParent, whenChanged
```

Estendendo gli esempi proposti è possibile gestire anche situazioni più complesse come il ripristino massivo e il ripristino in posizione diversa.

```
#Restore di un gruppo di utenti che contengono la parola bianchi nel Display Name
#Metodo 1: basato su attributo isDeleted
Get-ADObject -Filter {Name -Like "*bianchi*" -and isDeleted -eq $true} -IncludeDeletedObjects | Restore-ADObject

#Restore di un gruppo di utenti che contengono la parola bianchi nel Display Name
#Metodo 2: basato su ricerca nel container Deleted Object del dominio di esempio sysadmin.lan
Get-ADObject -SearchBase "CN=Deleted Objects,DC=sysadmin,DC=lan" -Filter {Name -Like "*bianchi*" -and isDeleted -eq $true} -IncludeDeletedObjects | Restore-ADObject

#Restore singolo account utente in una specifica Organizational Unit del dominio di esempio
#Metodo 1: basato su attributo isDeleted
Get-ADObject -Filter {sAMAccountName -eq "m.bianchi" -and isDeleted -eq $true} -IncludeDeletedObjects | Restore-ADObject -TargetPath "OU=ITStaff,DC=sysadmin,DC=lan"

#Restore singolo account utente in una specifica Organizational Unit del dominio di esempio sysadmin.lan
# Metodo 2: basato su ricerca nel container Deleted Object del dominio di esempio sysadmin.lan
Get-ADObject -Filter {sAMAccountName -eq "m.bianchi" -and isDeleted -eq $true} -IncludeDeletedObjects | Restore-ADObject -TargetPath "OU=ITStaff,DC=sysadmin,DC=lan"
```

Eliminazione di oggetti dall'Active Directory Recycle Bin

Può accadere che dopo un certo numero di eliminazioni di oggetti il container Deleted Objects diventa "affollato" di oggetti che non si intenderà mai ripristinare, quindi potrebbe essere desiderabile eliminare tali oggetti dall'Active Directory Recycle Bin per evitare confusioni.

La funzionalità di eliminazione di oggetti Deleted tramite la GUI di **Active Directory Administration Center** non è disponibile, ma occorre utilizzare **ldp.exe** come illustrato nel seguente Appendix A: Additional Active Directory Recycle Bin Tasks - Manually recycling a deleted Active Directory object.

Un'altra alternativa per eliminare gli oggetti Deleted, rendendoli quindi Recycled, è quella di utilizzare PowerShell.

```
#Eliminazione singolo oggetto deleted
#Metodo 1: basato su attributo isDeleted
Get-ADObject -Filter {sAMAccountName -eq "m.bianchi" -and isDeleted -eq $true} -IncludeDeletedObjects | Remove-ADObject

#Eliminazione singolo oggetto deleted
#Metodo 2: basato su ricerca nel container Deleted Object del dominio di esempio sysadmin.lan
Get-ADObject -SearchBase "CN=Deleted Objects,DC=sysadmin,DC=lan" -Filter {sAMAccountName -eq "m.bianchi"} -IncludeDeletedObjects | Remove-ADObject

#Eliminazione di tutti gli oggetti deleted senza richiesta di conferma
#nel container Deleted Object del dominio di esempio sysadmin.lan
Get-ADObject -SearchBase "CN=Deleted Objects,DC=sysadmin,DC=lan" -Filter {DistinguishedName -ne "CN=Deleted Objects,DC=sysadmin,DC=lan"} -IncludeDeletedObjects | Remove-ADObject -Confirm:$false
```

Conclusioni

L'Active Directory Recycle Bin permette di risolvere velocemente problemi legati ad erronee eliminazioni di oggetti Active Directory e la dualità dell'approccio tramite la GUI di **Active Directory Administration Center** oppure mediante i cmdlets **PowerShell** di Active Directory rende estremamente duttile la gestione di questa funzionalità.

Inoltre è possibile anche delegare la gestione dell'Active Directory Recycle Bin come illustrato nel seguente Appendix A: Additional Active Directory Recycle Bin Tasks - Delegating Active Directory Recycle Bin operations, ma soprattutto non bisogna dimenticare anche la possibilità di potere eseguire auditing delle modifiche apportate agli oggetti di Active Directory. Con Windows Server 2008 è stata infatti introdotta la sottocategoria di policies di audit *Directory Service Changes,* a riguardo si vedano Audit Directory Service Changes e AD DS Auditing Step-by-Step Guide.