

# RECOVERING ACTIVE DIRECTORY DELETED OBJECTS

Mark E. Donaldson

## Scope

Windows 2003 provides a means to recover and reanimate deleted objects in Active Directory.

## Background

When an object is deleted in Active Directory, it is really just "tombstoned." That is, the object and its mandatory attributes are moved to the Deleted Objects folder. Every 15 minutes, the Garbage Collector checks to see if the object's Tombstone Lifetime has expired. The Tombstone Lifetime is the period of time the object can remain in the Deleted Objects folder before it is purged from the database. This is 60 days by default, but this may be changed. If the Tombstone Lifetime has expired, the Garbage Collector purges the object from AD.

The Tombstone Lifetime can be changed by using the **ADSIEdit** tool. Go to *cn=directory Service,cn=windowsNT,cn=services,cn=configuration,dc=company,dc=com*. Right click on the CN=Directory Service folder and select Properties. Find Tombstone Lifetime in the attribute list, click the Edit button and enter the number of days in the value field.

## Procedure

If an Active Directory object is deleted mistakenly, you could do an authoritative restore of that object, or you can use a much quicker method using the LDP.exe tool to recover it:

1. Open the LDP.exe tool, which is part of the Windows Support Tools on the Server CD. Connect to a DC and Bind (authenticate).
2. Expose the Deleted Objects folder. By default, this folder is not visible. To see it in the LDP tool, go to the Options Menu on the LDP toolbar, and select Controls. In the Controls dialog, in the Load Predefined field, select Return Deleted Objects in the drop down list..
3. Go to View–Tree in the LDP toolbar, and enter the forest DN in the dialog box. If you connected to a root DC, just hit OK. If you already had the View-Tree going, you'll need to do a View-Tree again to refresh it.
4. The Deleted Objects folder should now be visible. Expand the folder to see all tombstoned objects.

Now that you have the Deleted Objects folder displayed, let's reanimate an object. In the following example, we have a user, Bob Smith, who was deleted from *CN=Users,dc=test,dc=bandwidthco,dc=com*. In the Deleted Objects folder expanded, see the deleted user Bob Smith. Note the *\0ADEL:* in the name. All deleted users are flagged with this. Note also that one of the attributes on Bob Smith is the *isDeleted* attribute, which is set to True. This attribute only exists on deleted users, making it easy to find them with an LDAP search. To reanimate Bob Smith, do the following:

1. Right click on the user in the left pane of LDP and select Modify.
2. In the Modify dialog, the long DN of the deleted user is in the DN field at the top.
3. In the Edit Entry Attribute field, enter *isDeleted*.

# RECOVERING ACTIVE DIRECTORY DELETED OBJECTS

Mark E. Donaldson

4. In the Operation area of the dialog, click the Delete radio button, then hit the Enter button. This will put *[Delete]isDeleted* in the "Entry List" field. This will remove the *isDeleted* attribute, but we have to fix the DN and get the object out of the Deleted Objects folder.
5. In the right pane, the user attributes are still visible. Find the *lastKnownParent* attribute, and select the distinguished name text. In this case the *lastKnownParent* is *CN=Users,DC=Qtest,DC=cpqcorp,DC=net*. This is the location of the user when it was deleted.
6. In the Edit Entry Attribute field, enter *distinguishedName*.
7. In the Values field, paste the *lastKnownParent* text. Then add the rest of the DN as needed for the object. In our example, we have to add *CN=Bob Smith*, (don't forget the comma). Note that this puts the user object back where it came from. You could modify the DN to put the object somewhere else. For instance we could specify *OU=OU,CN=Bob Smith,DC=test,DC=bandwidthco,DC=com* to put Bob Smith in the correct OU.
8. In the Operation area of the dialog, select the Replace radio button, and then hit the Enter button. Note that if you mess up, you can delete any of the entries in the Entry List with the Remove button, and try it again.
9. Make sure the Synchronous and Extended boxes at the bottom of the dialog are checked and then hit the Run button. You should get a message indicating success. If you get an error in this operation, such as "unwilling to perform," check the entries in the Edit Entry list -- you probably have a Delete where it should be Replace, or vice-versa. Note that the user was reanimated but came back as disabled. Also note that like any tombstoned object, it doesn't come back with all the attributes, including group membership. This will have to be restored manually (or script).

Obviously, this method would be too laborious to do a hundred or so deleted users (authoritative restore could be used for that task), but to recover a few objects, this method is quick and easy.