## How to restore deleted user accounts and their group memberships in Active Directory (840001.KB.EN-US.1.0)

Discusses how to recover from the accidental deletion of users and their group memberships in Active Directory.

Database: Content Maintenance Bug number: 19777

## SUMMARY

*You can use two methods to restore deleted user accounts, computer accounts, and security groups. These objects are known collectively as security principals. In both methods, you authoritatively restore the deleted objects, and then you restore group membership information for the deleted security principals. When you restore a deleted object, you must restore the former values of the* ***member*** *and* ***memberOf*** *attributes in the affected security principal. The two methods are:*

* *Method 1: Restore the deleted user accounts, and then add the restored users back to their groups*
* *Method 2: Authoritatively restore the deleted user accounts and the deleted users' security groups two times*

*Method 1 provides a better experience for domain users and administrators because it preserves the additions to security groups that were made between the time of the last system state backup and the time the deletion occurred. In method 2, instead of making individual adjustments to security principals, you roll back security group memberships to their state at the time of the last backup.  
  
If you do not have a valid backup of the system state, and the domain where the deletion occurred contains Windows Server 2003-based domain controllers, you can manually or programmatically recover the deleted objects. You can also use the Repadmin utility to determine when and where a user was deleted.   
  
Most large-scale deletions are accidental. Microsoft recommends that you take several steps to prevent others from deleting objects in bulk.*

## MORE INFORMATION

This step-by-step article discusses how to restore user accounts, computer accounts, and their group memberships after they have been deleted from Active Directory. In variations of this scenario, user accounts, computer accounts, or security groups may have been deleted individually or in some combination. In all these cases, the same initial steps apply--you authoritatively restore, or *auth restore*, those objects that were inadvertently deleted. Some deleted objects require additional work to be restored. These objects include objects such as user accounts that contain attributes that are back links of the attributes of other objects. Two of these attributes are **managedBy** and **memberOf**.  
  
When you add security principals such as a user account, a security group, or a computer account to a security group, you make the following changes in Active Directory:

1. The name of the security principal is added to the **member** attribute of each security group.
2. For each security group that the user, the computer, or the security group is a member of, a back link is added to the security principal's **memberOf** attribute.

Similarly, when a user, a computer, or a group is deleted from Active Directory, the following actions occur:

1. The deleted security principal is moved into the deleted objects container.
2. A number of attribute values, including the **memberOf** attribute, are stripped from the deleted security principal.
3. Deleted security principals are removed from any security groups that they were a member of. In other words, the deleted security principals are removed from each security group's **member** attribute.

When you recover deleted security principals and restore their group memberships, the key point to remember is that each security principal must exist in Active Directory before you restore its group membership. (The member may be a user, a computer, or another security group.) To restate this rule more broadly, an object that contains attributes whose values are back links must exist in Active Directory before the object that contains that forward link can be restored or modified.  
  
Although this article focuses on how to recover deleted user accounts and their memberships in security groups, its concepts apply equally to other object deletions. This article's concepts apply equally to deleted objects whose attribute values use forward links and back links to other objects in Active Directory.  
  
You can use either of two methods to recover security principals. When you use method 1, you leave in place all security principals that were added to any security group across the forest, and you add only security principals that were deleted from their respective domains back to their security groups. For example, you make a system state backup, add a user to a security group, and then restore the system state backup. When you use method 1, you preserve any users who were added to security groups that contain deleted users between the dates that the system state backup was created and the date that the backup was restored. When you use method 2, you roll back security group memberships for all the security groups that contain deleted users to their state at the time that the system state backup was made.

### Method 1: Restore the deleted user accounts, and then add the restored users back to their groups

When you use this method, you perform the following high-level steps:

1. Check to see if a global catalog in the user's domain has not replicated in the deletion, and then prevent that global catalog from replicating. If there is no latent global catalog, locate the most current system state backup of a global catalog domain controller in the deleted user's home domain.
2. Auth restore all the deleted user accounts, and then permit end-to-end replication of those user accounts.
3. Add all the restored users back to all the groups in all the domains that the user accounts were a member of before they were deleted.

To use method 1, follow this procedure:

1. Check to see whether there is a global catalog domain controller in the deleted user's home domain that has not replicated any part of the deletion.  
     
   **Note** Focus on the global catalogs that have the least frequent replication schedules.  
     
   If one or more of these global catalogs exist, use the Repadmin.exe command-line tool to immediately disable inbound replication. To do this, follow these steps:   
     
   1. Click **Start**, and then click **Run**.
   2. Type **cmd** in the **Open** box, and then click **OK**.
   3. Type the following command at the command prompt, and then press ENTER:

**repadmin /options *<recovery dc name>* +DISABLE\_INBOUND\_REPL**

**Note** If you cannot issue the Repadmin command immediately, remove all network connectivity from the latent global catalog until you can use Repadmin to disable inbound replication, and then immediately return network connectivity.

This domain controller will be referred to as the recovery domain controller. If there is no such global catalog, go to step 2.

1. Decide whether additions, deletions, and changes to user accounts, computer accounts, and security groups must be temporarily stopped until all the recovery steps have been completed.  
     
   To maintain the most flexible recovery path, temporarily stop making changes to the following items. Changes include password resets by domain users, help desk administrators, and administrators in the domain where the deletion occurred, in addition to group membership changes in the deleted users' groups. Consider halting additions, deletions, and modifications to the following items:   
     
   1. User accounts and attributes on user accounts
   2. Computer accounts and attributes on computer accounts
   3. Service accounts
   4. Security groups

It is best to stop making changes to security groups in the forest if all the following statements are true:

* 1. You are using method 1 to auth restore deleted users or computer accounts by their domain name (dn) path.
  2. The deletion has replicated to all the domain controllers in the forest except the latent recovery domain controller.
  3. You are not auth restoring security groups or their parent containers.

If you are auth restoring security groups or organizational unit (OU) containers that host security groups or user accounts, temporarily stop all these changes.  
  
Notify administrators and help desk administrators in the appropriate domains in addition to domain users in the domain where the deletion occurred about stopping these changes.

1. Create a new system state backup in the domain where the deletion occurred. You can use this backup if you have to roll back your changes.  
     
   **Note** If system state backups are current up to the point of the deletion, skip this step and go to step 4.  
     
   If you identified a recovery domain controller in step 1, back up its system state now.  
     
   If all the global catalogs located in the domain where the deletion occurred replicated in the deletion, back up the system state of a global catalog in the domain where the deletion occurred.  
     
   When you create a backup, you can return the recovery domain controller back to its current state and perform your recovery plan again if your first try is not successful.
2. If you cannot find a latent global catalog domain controller in the domain where the user deletion occurred, find the most recent system state backup of a global catalog domain controller in that domain. This system state backup should contain the deleted objects. Use this domain controller as the recovery domain controller.  
     
   Only restorations of the global catalog domain controllers in the user's domain contain global and universal group membership information for security groups that reside in external domains. If there is no system state backup of a global catalog domain controller in the domain where users were deleted, you cannot use the **memberOf** attribute on restored user accounts to determine global or universal group membership or to recover membership in external domains. Additionally, it is a good idea to find the most recent system state backup of a non-global catalog domain controller.
3. If you know the password for the offline administrator account, start the recovery domain controller in Dsrepair mode. If you do not know the password for the offline administrator account, reset the password while the recovery domain controller is still in normal Active Directory mode.  
     
   You can use the **setpwd** command-line tool to reset the password on domain controllers that are running Microsoft Windows 2000 Service Pack 2 (SP2) and later while they are in online Active Directory mode.  
     
   **Note** Microsoft no longer supports Windows 2000 SP2. Install the most recent Windows 2000 service pack to obtain this functionality.

For additional information about changing the Recovery Console administrator password, click the following article number to view the article in the Microsoft Knowledge Base:

239803.KB.[LN] How to change the Recovery Console administrator password on a domain controller

Administrators of Windows Server 2003 domain controllers can use the **set dsrm password** command in the **Ntdsutil** command-line tool to reset the password for the offline administrator account.

For additional information about how to reset the Directory Services Restore Mode administrator account, click the following article number to view the article in the Microsoft Knowledge Base:

322672.KB.[LN] HOW TO: Reset the Directory Services Restore Mode administrator account password in Windows Server 2003

1. Press F8 during the startup process to start the recovery domain controller in Dsrepair mode. Log on to the console of the recovery domain controller with the offline administrator account. If you reset the password in step 5, use the new password.  
     
   If the recovery domain controller is a latent global catalog domain controller, do not restore the system state. Go to step 7.  
     
   If you are creating the recovery domain controller by using a system state backup, restore the most current system state backup that was made on the recovery domain controller now.
2. Auth restore the deleted user accounts, the deleted computer accounts, or the deleted security groups.  
     
   **Note** The terms *auth restore* and *authoritative restore* refer to the process of using the **authoritative restore** command in the **Ntdsutil** command-line tool to increment the version numbers of specific objects or of specific containers and all their subordinate objects. As soon as end-to-end replication occurs, the targeted objects in the recovery domain controller's local copy of Active Directory become authoritative on all the domain controllers that share that partition. An authoritative restoration is different from a system state restoration. A system state restoration populates the restored domain controller's local copy of Active Directory with the versions of the objects at the time that the system state backup was made.

For additional information about auth restoring a domain controller, click the following article number to view the article in the Microsoft Knowledge Base:

241594.KB.[LN] HOW TO: Perform an authoritative restore to a domain controller in Windows 2000

Authoritative restorations are performed with the **Ntdsutil** command-line tool and refer to the domain name (dn) path of the deleted users or of the containers that host the deleted users.   
  
When you auth restore, use domain name (dn) paths that are as low in the domain tree as they have to be to avoid reverting objects that are not related to the deletion. These objects may include objects that were modified after the system state backup was made.  
  
Auth restore deleted users in the following order:

* 1. Auth restore the domain name (dn) path for each deleted user account, computer account, or security group.  
       
     Authoritative restorations of specific objects take longer but are less destructive than authoritative restorations of a whole subtree. Auth restore the lowest common parent container that holds the deleted objects.  
       
     **Ntdsutil** uses the following syntax:

ntdsutil "authoritative restore" "restore object *<object DN path>*" q q

For example, to auth restore the deleted user *JohnDoe* in the *Mayberry* OU of the *Contoso.com* domain, use the following command:

ntdsutil "authoritative restore" "restore object cn=JohnDoe,ou=Mayberry,dc=contoso,dc=com" q q

To auth restore the deleted security group *ContosoPrintAccess* in the *Mayberry* OU of the *Contoso.com* domain, use the following command:

ntdsutil "authoritative restore" "restore object cn=ContosoPrintAccess,ou=Mayberry,dc=contoso,dc=com" q q

**Important** The use of quotes is required.

* 1. Auth restore only the OU or Common-Name (CN) containers that host the deleted user accounts or groups.  
       
     Authoritative restorations of a whole subtree are valid when the OU that is targeted by the **ntdsutil "authoritative restore"** command contains the overwhelming majority of the objects that you are trying to auth restore. Ideally, the targeted OU contains all the objects that you are trying to auth restore.  
       
     An authoritative restoration on an OU subtree restores all the attributes and objects that reside in the container. Any changes that were made up to the time that a system state backup is restored are rolled back to their values at the time of the backup. With user accounts, computer accounts, and security groups, this rollback may mean the loss of the most recent changes to passwords, to the home directory, to the profile path, to location and to contact info, to group membership, and to any security descriptors that are defined on those objects and attributes.  
       
     **Ntdsutil** uses the following syntax:

ntdsutil "authoritative restore" "restore subtree *<container DN path>*" q q

For example, to auth restore the *Mayberry* OU of the *Contoso.com* domain, use the following command:

ntdsutil "authoritative restore" "restore subtree ou=Mayberry, dc=contoso,dc=com" q q

**Note** Repeat this step for each peer OU that hosts deleted users or groups.  
  
**Important** When you restore a subordinate object of an OU, all the deleted parent containers of the deleted subordinate objects must be explicitly auth restored.

1. If deleted objects were recovered on the recovery domain controller because of a system state restore, remove all the network cables that provide network connectivity to all the other domain controllers in the forest.
2. Restart the recovery domain controller in normal Active Directory mode.
3. Type the following command to disable inbound replication to the recovery domain controller:

**repadmin /options *<recovery dc name>* +DISABLE\_INBOUND\_REPL**

Enable network connectivity back to the recovery domain controller whose system state was restored.

1. Outbound-replicate the auth-restored objects from the recovery domain controller to the domain controllers in the domain and in the forest.  
     
   While inbound replication to the recovery domain controller remains disabled, type the following command to push the auth-restored objects to all the cross-site replica domain controllers in the domain and to all the global catalogs in the forest:

**repadmin /syncall /d /e /P *<recovery dc>***

If all the following statements are true, group membership links are rebuilt with the restoration and the replication of the deleted user accounts. Go to step 14.  
  
**Note** If one or more of the following statements is not true, go to step 12.

* 1. Your forest is running at the Windows Server 2003 forest functional level or at the Windows Server 2003 Interim forest functional level.
  2. Only user accounts or computer accounts were deleted, and not security groups.
  3. The deleted users were added to security groups in all the domains in the forest after the forest was transitioned to Windows Server 2003 forest functional level.

1. Determine which security groups the deleted users were members of, and then add them to those groups.  
     
   **Note** Before you can add users to groups, the users who you auth restored in step 7 and who you outbound-replicated in step 11 must have replicated to the domain controllers in the referenced domain controller's domain and to all the global catalog domain controllers in the forest.  
     
   If you have deployed a group-provisioning utility to re-populate membership for security groups, use that utility now to restore deleted users to the security groups that they were members of before they were deleted. Do this after all the direct and transitive domain controllers in the forest's domain and global catalog servers have inbound-replicated the auth-restored users and any restored containers.  
     
   If you do not have such a utility, the Ldifde.exe command-line tool and the Groupadd.exe command-line tool can automate this task for you when they are run on the recovery domain controller. These tools are available from Microsoft Product Support Services. In this scenario, Ldifde.exe creates an LDAP Data Interchange Format (LDIF) information file that contains the names of the user accounts and their security groups, starting at an OU container that the administrator specifies. Groupadd.exe then reads the **memberOf** attribute for each user account that is listed in the .ldf file, and then generates separate and unique LDIF information for each domain in the forest. This LDIF information contains the names of the security groups that the deleted users have to be added back to so that their group memberships can be restored. Follow these steps for this phase of the recovery.   
     
   1. Log on to the recovery domain controller's console by using a user account that is a member of the domain administrator's security group.
   2. Use the **Ldifde** command to dump the names of the formerly deleted user accounts and their **memberOf** attributes, starting at the topmost OU container where the deletion occurred. The **Ldifde** command uses the following syntax:

ldifde -d *<dn path of container that hosts deleted users>* -r "(objectClass=user)" -l memberof -p subtree -f user\_membership\_after\_restore.ldf

Use the following syntax if deleted computer accounts were added to security groups:

ldifde -d *<dn path of container that hosts deleted users>* -r "(objectClass=computer)" -l memberof -p subtree -f computer\_membership\_after\_restore.ldf

* 1. Run the **Groupadd** command to build additional .ldf files that contain the names of domains and the names of global and universal security groups that the deleted users were a member of. The Groupadd command uses the following syntax:

Groupadd /*after\_restore* users\_membership\_after\_restore.ldf

Repeat this command if deleted computer accounts were added to security groups.

* 1. Import each Groupadd\_*fully.qualified.domainname*.ldf file that you created in step 12c to a single global catalog domain controller that corresponds with each domain's .ldf file. Use the following Ldifde syntax:

Ldifde –i –k –f Groupadd\_*<fully.qualified.domain.name>*.ldf

Run the .ldf file for the domain that the users were deleted from on any domain controller except the recovery domain controller.

* 1. On the console of each domain controller that is used to import the Groupadd\_*<fully.qualified.domain.name>*.ldf file for a particular domain, outbound-replicate the group membership additions to the other domain controllers in the domain and to the global catalog domain controllers in the forest by using the following command:

**repadmin /syncall /d /e /P *<recovery dc>***

1. Enable inbound replication to the recovery domain controller by using the following command:

**repadmin /options *<recovery dc name>* -DISABLE\_INBOUND\_REPL**

1. If deleted users were added to local groups in external domains, do one of the following:   
     
   1. Manually add the deleted users back to those groups.
   2. Restore the system state and auth restore each of the local security groups that contains the deleted users.
2. Verify group membership in the recovery domain controller's domain and in global catalogs in other domains.
3. Make a new system state backup of domain controllers in the recovery domain controller's domain.
4. Notify all the forest administrators, delegated administrators, help desk administrators in the forest, and users in the domain that the user restore is complete.  
     
   Help desk administrators may have to reset the passwords of auth-restored user accounts and computer accounts whose domain password changed after the restored system was made.  
     
   Users who changed their passwords after the system state backup was made will find that their most recent password no longer works. Have such users try to log on by using their previous passwords if they know them. Otherwise, help desk administrators must reset the password and select the **user must change password at next logon** check box, preferably on a domain controller in the same Active Directory site as the user is located in.

### Method 2: Authoritatively restore the deleted users and the deleted users' security groups two times

When you use this method, you perform the following high-level steps:

1. Check to see if a global catalog in the user's domain has not replicated in the deletion, and then prevent that domain controller from inbound-replicating the deletion. If there is no latent global catalog, locate the most current system state backup of a global catalog domain controller in the deleted user's home domain.
2. Authoritatively restore all deleted user accounts and all security groups in the deleted user's domain.
3. Wait for the end-to-end replication of the restored users and of the security groups to all the domain controllers in the deleted user's domain and to the forest's global catalog domain controllers.
4. Repeat steps 2 and 3 to authoritatively restore deleted users and security groups. (You restore the system state only one time.)
5. If the deleted users were members of security groups in other domains, authoritatively restore all the security groups that the deleted users were members of in those domains. Or, if system state backups are current, authoritatively restore all the security groups in those domains.

To satisfy the requirement that deleted group members must be restored before security groups to fix up group membership links, you restore both object types two times in this method. The first restoration puts all the user accounts and group accounts in place, and the second restoration restores deleted groups and repairs the group membership information, including membership information for nested groups.  
  
To use method 2, follow this procedure:

1. Check to see whether a global catalog domain controller exists in the deleted users home domain and has not replicated in any part of the deletion.  
     
   **Note** Focus on global catalogs in the domain that has the least frequent replication schedules. If these domain controllers exist, use the Repadmin.exe command-line tool to immediately disable inbound replication. To do this, follow these steps:   
     
   1. Click **Start**, and then click **Run**.
   2. Type **command** in the **Open** box, and then click **OK**.
   3. Type **repadmin /options *<recovery dc name>* +DISABLE\_INBOUND\_REPL** at the command prompt, and then press ENTER.  
        
      **Note** If you cannot issue the Repadmin command immediately, remove all network connectivity from the domain controller until you can use Repadmin to disable inbound replication, and then immediately return network connectivity.

This domain controller will be referred to as the recovery domain controller.

1. Avoid making additions, deletions, and changes to the following items until all the recovery steps have been completed. Changes include password resets by domain users, help desk administrators, and administrators in the domain where the deletion occurred, in addition to group membership changes in the deleted users' groups.   
     
   1. User accounts and attributes on user accounts
   2. Computer accounts and attributes on computer accounts
   3. Service accounts
   4. Security groups  
        
      **Note** Especially avoid changes to group membership for users, computers, groups, and service accounts in the forest where the deletion occurred.
   5. Notify all the forest administrators, the delegated administrators, and the help desk administrators in the forest of the temporary stand-down.

This stand-down is required in method 2 because you are authoritatively restoring all the deleted users' security groups. Therefore, any changes that are made to groups after the date of system state backup are lost.

1. Create a new system state backup in the domain where the deletion occurred. You can use this backup if you have to roll back your changes.  
     
   **Note** If your system state backups are current up to the time that the deletion occurred, skip this step and go to step 4.  
     
   If you identified a recovery domain controller in step 1, back up its system state now.  
     
   If all the global catalogs that are located in the domain where the deletion occurred replicated the deletion, back up the system state of a global catalog in the domain where the deletion occurred.  
     
   When you create a backup, you can return the recovery domain controller back to its current state and perform your recovery plan again if your first try is not successful.
2. If you cannot find a latent global catalog domain controller in the domain where the user deletion occurred, find the most recent system state backup of a global catalog domain controller in that domain. This system state backup should contain the deleted objects. Use this domain controller as the recovery domain controller.  
     
   Only databases of the global catalog domain controllers in the user's domain contain group membership information for external domains in the forest. If there is no system state backup of a global catalog domain controller in the domain where users were deleted, you cannot use the **memberOf** attribute on restored user accounts to determine global or universal group membership or to recover membership in external domains. Go to the next step. If there is an external record of group membership in external domains, add the restored users to security groups in those domains after the user accounts have been restored.
3. If you know the password for the offline administrator account, start the recovery domain controller in Dsrepair mode. If you do not know the password for the offline administrator account, reset the password while the recovery domain controller is still in normal Active Directory mode.  
     
   You can use the **setpwd** command-line tool to reset the password on domain controllers that are running Microsoft Windows 2000 Service Pack 2 (SP2) and later while they are in online Active Directory mode.  
     
   **Note** Microsoft no longer supports Windows 2000 SP2. Install the most recent Windows 2000 service pack to obtain this functionality.

For additional information about changing the Recovery Console administrator password, click the following article number to view the article in the Microsoft Knowledge Base:

239803.KB.[LN] How to change the Recovery Console administrator password on a domain controller

Administrators of Windows Server 2003 domain controllers can use the **set dsrm password** command in the **Ntdsutil** command-line tool to reset the password for the offline administrator account.

For additional information about how to reset the Directory Services Restore Mode administrator account, click the following article number to view the article in the Microsoft Knowledge Base:

322672.KB.[LN] HOW TO: Reset the Directory Services Restore Mode administrator account password in Windows Server 2003

1. Press F8 during the startup process to start the recovery domain controller in Dsrepair mode. Log on to the console of the recovery domain controller with the offline administrator account. If you reset the password in step 5, use the new password.  
     
   If the recovery domain controller is a latent global catalog domain controller, do not restore the system state. Go directly to step 7.  
     
   If you are creating the recovery domain controller by using a system state backup, restore the most current system state backup that was made on the recovery domain controller that contains the deleted objects now.
2. Auth restore the deleted user accounts, the deleted computer accounts, or the deleted security groups.  
     
   **Note** The terms *auth restore* and *authoritative restore* refer to the process of using the **authoritative restore** command in the **Ntdsutil** command-line tool to increment the version numbers of specific objects or of specific containers and all their subordinate objects. As soon as end-to-end replication occurs, the targeted objects in the recovery domain controller's local copy of Active Directory become authoritative on all the domain controllers that share that partition. An authoritative restoration is different from a system state restoration. A system state restoration populates the restored domain controller's local copy of Active Directory with the versions of the objects at the time that the system state backup was made.

For additional information about auth restoring a domain controller, click the following article number to view the article in the Microsoft Knowledge Base:

241594.KB.[LN] HOW TO: Perform an authoritative restore to a domain controller in Windows 2000

Authoritative restorations are performed with the **Ntdsutil** command-line tool by referencing the domain name (dn) path of the deleted users or of the containers that host the deleted users.   
  
When you auth restore, use domain name (dn) paths that are as low in the domain tree as they have to be to avoid reverting objects that are not related to the deletion. These objects may include objects that were modified after the system state backup was made.  
  
Auth restore deleted users in the following order:

* 1. Auth restore the domain name (dn) path for each deleted user account, computer account, or deleted security group.  
       
     Authoritative restorations of specific objects take longer but are less destructive than authoritative restorations of a whole subtree. Auth restore the lowest common parent container that holds the deleted objects.  
       
     **Ntdsutil** uses the following syntax:

ntdsutil "authoritative restore" "restore object *<object DN path>*" q q

For example, to auth restore the deleted user *JohnDoe* in the *Mayberry* OU of the *Contoso.com* domain, use the following command:

ntdsutil "authoritative restore" "restore object cn=JohnDoe,ou=Mayberry,dc=contoso,dc=com" q q

To auth restore the deleted security group *ContosoPrintAccess* in the *Mayberry* OU of the *Contoso.com* domain, use the following command:

ntdsutil "authoritative restore" "restore object cn=ContosoPrintAccess,ou=Mayberry,dc=contoso,dc=com" q q

**Important** The use of quotes is required.  
  
By using this Ntdsutil format, you can also automate the authoritative restoration of many objects in a batch file or a script.

* 1. Auth restore only the OU or Common-Name (CN) containers that host the deleted user accounts or groups.  
       
     Authoritative restorations of a whole subtree are valid when the OU that is targeted by the **Ntdsutil Authoritative restore** command contains the overwhelming majority of the objects that you are trying to auth restore. Ideally, the targeted OU contains all the objects that you are trying to auth restore.  
       
     An authoritative restore on an OU subtree restores all the attributes and objects that reside in the container. Any changes that were made up to the time that a system state backup is restored are rolled back to their values at the time of the backup. With user accounts, computer accounts, and security groups, this rollback may mean the loss of the most recent changes to passwords, to the home directory, to the profile path, to location and to contact info, to group membership, and to any security descriptors that are defined on those objects and attributes.  
       
     **Ntdsutil** uses the following syntax:

ntdsutil "authoritative restore" "restore subtree *<container DN path>*" q q

For example, to auth restore the *Mayberry* OU of the *Contoso.com* domain, use the following command:

ntdsutil "authoritative restore" "restore subtree ou=Mayberry,dc=contoso,dc=com" q q

**Note** Repeat this step for each peer OU that hosts deleted users or groups.  
  
**Important** When you restore a subordinate object of an OU, all the parent containers of the deleted subordinate objects must be explicitly auth restored.

1. Restart the recovery domain controller in normal Active Directory mode.
2. Outbound-replicate the authoritatively restored objects from the recovery domain controller to the domain controllers in the domain and in the forest.  
     
   While inbound replication to the recovery domain controller remains disabled, type the following command to push the authoritatively restored objects to all the cross-site replica domain controllers in the domain and to global catalogs in the forest:

**repadmin /syncall /d /e /P *<recovery dc>***

After all the direct and transitive domain controllers in the forest's domain and global catalog servers have replicated in the authoritatively restored users and any restored containers, go to step 11.  
  
If all the following statements are true, group membership links are rebuilt with the restoration of the deleted user accounts. Go to step 13.

* 1. Your forest is running at the Windows Server 2003 forest functional level or at the Windows Server 2003 interim forest functional level.
  2. Only security groups were not deleted.
  3. All the deleted users were added to all the security groups in all the domains in the forest.

Consider using the Repadmin command to accelerate the outbound replication of users from the restored domain controller.  
  
If groups were also deleted, or if you cannot guarantee that all the deleted users were added to all the security groups after the transition to the Windows Server 2003 interim or forest functional level, go to step 12.

1. Repeat steps 7, 8, and 9 without restoring the system state, and then go to step 11.
2. If deleted users were added to local groups in external domains, do one of the following:
   1. Manually add the deleted users back to those groups.
   2. Restore the system state and auth restore each of the local security groups that contains the deleted users.
3. Verify group membership in the recovery domain controller's domain and in global catalogs in other domains.
4. Use the following command to disable inbound replication to the recovery domain controller:

**repadmin /options *recovery dc name* -DISABLE\_INBOUND\_REPL**

1. Make a new system state backup of domain controllers in the recovery domain controller's domain and global catalogs in other domains in the forest.
2. Notify all the forest administrators, the delegated administrators, the help desk administrators in the forest, and the users in the domain that the user restore is complete.  
     
   Help desk administrators may have to reset the passwords of auth restored user accounts and computer accounts whose domain password changed after the restored system was made.  
     
   Users who changed their passwords after the system state backup was made will find that their most recent password no longer works. Have such users try to log on by using their previous passwords if they know them. Otherwise, help desk administrators must reset the password with the **user must change password at next logon** check box checked, preferably on a domain controller in the same Active Directory site as the user is located in.

### How to recover deleted users on a Windows Server 2003 domain controller when you do not have a valid system state backup

If you lack current system state backups in a domain where user accounts or security groups were deleted, and the deletion occurred in domains that contain Windows Server 2003 domain controllers, follow these steps to manually reanimate deleted objects from the deleted objects container:

1. Follow the steps in the "How to manually undelete objects in the deleted objects container" section to reanimate deleted users, computers, groups, or all of these.
2. Use Active Directory Users and Computers to change the account from disabled to enabled. (The account appears in the original OU.)
3. Use the bulk reset features in the Windows Server 2003 version of Active Directory Users and Computers to perform bulk resets on the "password must change at next logon" policy setting, on the home directory, on the profile path, and on group membership for the deleted account as required. You can also use a programmatic equivalent of these features.
4. If Microsoft Exchange 2000 or later was used, repair the Exchange mailbox for the deleted user.
5. If Exchange 2000 or later was used, reassociate the deleted user with the Exchange mailbox.
6. Verify that the recovered user can log on and access local directories, shared directories, and files.

You can automate some or all of these recovery steps by using the following methods:

* Write a script that automates the manual recovery steps that are listed in step 1. When you write such a script, consider scoping the deleted object by date, time, and last known parent container, and then automating the reanimation of the deleted object. To automate the reanimation, change the **isDeleted** attribute from TRUE to FALSE, and change the relative distinguished name to the value that is defined either in the **lastKnownParent** attribute or in a new OU or common name (CN) container that is specified by the administrator. (The relative distinguished name is also known as the RDN.)
* Obtain a non-Microsoft program that supports the reanimation of deleted objects on Windows Server 2003 domain controllers. One such utility is AdRestore. AdRestore uses the Windows Server 2003 undelete primitives to undelete objects individually. Aelita Software Corporation and Commvault Systems also offer products that support undelete functionality on Windows Server 2003-based domain controllers.  
    
  To obtain AdRestore, visit the following non-Microsoft Web site:

<http://www.sysinternals.com/ntw2k/source/misc.shtml#adrestore>

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

### How to manually undelete objects in a deleted object's container

To manually undelete objects in a deleted object's container, follow these steps:

1. Click **Start**, click **Run**, and then type **ldp.exe**.  
     
   **Note** If the Ldp utility is not installed, install the support tools from the Windows Server 2003 installation CD.
2. Use the **Connection** menu in Ldp to perform the connect operations and the bind operations to a Windows Server 2003 domain controller.  
     
   Specify domain administrator credentials during the bind operation.
3. On the **Options** menu, click **Controls**.
4. In the **Load Predefined** list, click **Return Deleted Objects**.   
     
   **Note** The **1.2.840.113556.1.4.417** control moves to the **Active Controls** window.
5. Under **Control Type**, click **Server**, and the click **OK**.
6. On the **View** menu, click **Tree**, type the distinguished name path of the deleted objects container in the domain where the deletion occurred, and then click **OK**.  
     
   **Note** The distinguished name path is also known as the DN path. For example, if the deletion occurred in the contoso.com domain, the DN path would be the following path:

cn=deletedObjects,dc=contoso,dc=com

1. In the left pane, double-click the deleted objects container.
2. Double-click the object that you want to undelete or to reanimate.
3. Right-click the object that you want to reanimate, and then click Modify.  
     
   Change the value for the **isDeleted** attribute and the DN path in a single Lightweight Directory Access Protocol (LDAP) modify operation. To configure the **Modify** dialog, follow these steps:
   1. In the **Edit Entry Attribute** box, type **isDeleted**.  
        
      Leave the **Value** box blank.
   2. Click the **Delete** option button, and then click **Enter** to make the first of two entries in the **Entry List** dialog.  
        
      **Important** Do not click **Run**.
   3. In the **Attribute** box, type **distinguishedName**.
   4. In the **Values** box, type the new DN path of the reanimated object.  
        
      For example, to reanimate the JohnDoe user account to the Mayberry OU, use the following DN path:

**cn=*JohnDoe*,ou=*Mayberry*,dc=*contoso*,dc=*com***

**Note** If you want to reanimate a deleted object to its original container, append the value of the deleted object's **lastKnownParent** attribute to its CN value, and then paste the full DN path in the **Values** box.

* 1. In the **Operation** box, click **REPLACE**.
  2. Click **ENTER**.
  3. Click to select the **Synchronous** check box.
  4. Click to select the **Extended** check box.
  5. Click **RUN**.

1. After you reanimate the objects, click **Options**, click **Controls**, click to clear **Return Deleted Objects**, and then click **OK**.  
     
   When you clear Return Deleted Objects, you remove the **Return Deleted Objects** control (1.2.840.1138556.1.4.417) from the Active Controls list.
2. Reset user account passwords, profiles, home directories and group memberships for the deleted users.  
     
   When the object was deleted, all the attribute values except **SID**, **ObjectGUID**, **LastKnownParent** and **SAMAccountName** were stripped.
3. Enable the reanimated account in Active Directory Users and Computers.  
     
   **Note** The reanimated object has the same primary SID as it had before the deletion, but the object must be added again to the same security groups to have the same level of access to resources. The first release of Windows Server 2003 does not preserve the **sIDHistory** attribute on reanimated user accounts, computer accounts, and security groups. In a future Windows Server 2003 service pack, domain controllers will preserve the **sIDHistory** attribute for security principals that are deleted after the service pack is installed.
4. Remove Microsoft Exchange attributes and reconnect the user to the Exchange mailbox.  
     
   **Note** The reanimation of deleted objects is supported when the deletion occurs on a Windows Server 2003 domain controller. The reanimation of deleted objects is not supported when the deletion occurs on a Windows 2000 domain controller that is subsequently upgraded to Windows Server 2003.  
     
   **Note** If the deletion occurs on a Windows 2000 domain controller in the domain, the **lastParentOf** attribute is not populated on Windows Server 2003 domain controllers.

### How to determine when and where a deletion occurred

When users are deleted because of a bulk deletion, you may want to learn where the deletion originated. To do so, follow these steps:

1. If auditing has been correctly configured to track the deletion of organizational unit (OU) containers or of subordinate objects, use a utility that searches the security event log of domain controllers in the domain where the deletion occurred. One such utility that searches event logs on a scoped set of domain controllers is the EventCombMT utility. EventCombMT is part of the Windows Server 2003 Resource Kit Tools tool set.  
     
   For additional information about how to obtain the Windows Server 2003 Resource Kit Tools tools set, visit the following Microsoft Web page:

<http://www.microsoft.com/windows/reskits/default.asp>

1. Follow steps 1 to 7 in the "How to manually undelete objects in a deleted object's container" section to locate deleted security principals. If a tree was deleted, follow these steps to locate a parent container of the deleted object.
2. Copy the value of the **objectGUID** attribute to the Windows clipboard.  
     
   You can paste this value when you enter the Repadmin command in step 4.
3. Type the following command:

**repadmin /showmeta *<GUID=objectguid>***

.For example, if the objectGUID of the deleted object or container is 791273b2-eba7-4285-a117-aa804ea76e95, type the following command:

**repadmin /showmeta GUID= 791273b2-eba7-4285-a117-aa804ea76e95**

1. In the Repadmin command output, find the originating date, time and domain controller for the **isDeleted** attribute. For example, information for the **isDeleted** attribute appears in the fifth line of the following sample output:
2. Loc.USN Originating DC Org.USN Org.Time/Date Ver Attribute
3. -----------------------------------------------------------------------------------------------
4. 134759 Default-First-Site-Name\NA-DC1 134759 2004-03-15 17:41:20 1 objectClass
5. 134760 Default-First-Site-Name\NA-DC1 134760 2004-03-15 17:41:22 2 ou
6. 134759 Default-First-Site-Name\NA-DC1 134759 2004-03-15 17:41:20 1 instanceType
7. 134759 Default-First-Site-Name\NA-DC1 134759 2004-03-15 17:41:20 1 whenCreated
8. 134760 Default-First-Site-Name\NA-DC1 134760 2004-03-15 17:41:22 1 isDeleted
9. 134759 Default-First-Site-Name\NA-DC1 134759 2004-03-15 17:41:20 1 nTSecurityDescriptor
10. 134760 Default-First-Site-Name\NA-DC1 134760 2004-03-15 17:41:22 2 name
11. 134760 Default-First-Site-Name\NA-DC1 134760 2004-03-15 17:41:22 1 lastKnownParent

134760 Default-First-Site-Name\NA-DC1 134760 2004-03-15 17:41:22 2 objectCategory

1. If the name of the originating domain controller in the second column of the output appears as a 32-character alpha-numeric GUID, use the Ping command to resolve the GUID to the IP address and the name of the domain controller that originated the deletion. The Ping command uses the following syntax:

ping –a *<originating DC GUID>*.\_msdomain controllers.*<fully qualified path for forest root domain*>

**Note** The "-a" option is case sensitive. Use the fully qualified domain name of the forest root domain regardless of the domain that the originating domain controller resides in.  
  
For example, if the originating domain controller resided in any domain in the Contoso.com forest and had a GUID of 644eb7e7-1566-4f29-a778-4b487637564b, type the following command:

**ping –a 644eb7e7-1566-4f29-a778-4b487637564b.\_msdomain controllers.contoso.com**

The output returned by this command is similar to the following:

Pinging na-dc1.contoso.com [65.53.65.101] with 32 bytes of data:

Reply from 65.53.65.101: bytes=32 time<1ms TTL=128

Reply from 65.53.65.101: bytes=32 time<1ms TTL=128

Reply from 65.53.65.101: bytes=32 time<1ms TTL=128

Reply from 65.53.65.101: bytes=32 time<1ms TTL=128

1. View the security log of the domain controller that originated the deletion on or about the time that was indicated in the output of the Repadmin command in step 5.  
     
   Give consideration to time skews and time zone changes between the computers that were used to arrive at this point. If delete auditing is enabled for OU containers or for the deleted objects, pay attention to the relevant audit events. If auditing is not enabled, pay attention to users who had the permissions to delete OU containers or the subordinate objects in them, and that also had authenticated against the originating domain controller in the time before the deletion.

### How to minimize the impact of bulk deletions in the future

The keys to minimizing the impact of the bulk deletion of users, of computers, and of security groups are to make sure that you have up-to-date system state backups, to tightly control access to privileged user accounts, to tightly control what those accounts can do, and finally, to practice recovery from bulk deletions.  
  
System state changes occur every day. These changes may include password resets on user accounts and on computer accounts in addition to group membership changes and other attribute changes on user accounts, on computer accounts, and on security groups. If your hardware fails, your software fails, or your site experiences another disaster, you will want to restore the backups that were made after each significant set of changes in each Active Directory domain and site in the forest. If you do not maintain current backups, you may lose data or may have to roll back restored objects.   
  
Microsoft recommends that you take the following steps to prevent bulk deletions:

1. Do not share the password for the built-in administrator accounts or permit common administrative user accounts to be shared. If the password for the built-in administrator account is known, change the password and define an internal process that discourages its use. Audit events for shared user accounts make it impossible to determine the identity of the user who is making changes in Active Directory. Therefore, the use of shared user accounts must be discouraged.
2. It is very rare that user accounts, computer accounts, and security groups are intentionally deleted. This is especially true of tree deletions. Disassociate the ability of service and delegated administrators to delete these objects from the ability to create and to manage user accounts, computer accounts, security groups, OU containers, and their attributes. Grant only the most privileged user accounts or security groups the right to perform tree deletes. These privileged user accounts may include enterprise administrators.
3. Grant delegated administrators access only to the class of object that those administrators are permitted to manage. For example, it is better if a help desk administrator whose primary job is to modify properties on user accounts does not have permissions to create and to delete computer accounts, security groups, or OU containers. This restriction also applies to delete permissions for the administrators of other specific object classes.
4. Experiment with audit settings to track delete operations in a lab domain. After you are comfortable with the results, apply your best solution to the production domain.
5. Wholesale access-control and audit changes on containers that host tens of thousands of objects can make the Active Directory database grow significantly, especially in Windows 2000 domains. Use a test domain that mirrors the production domain to evaluate potential changes to free disk space. Check the hard disk drive volumes that host the Ntds.dit files and the log files of domain controllers in the production domain for free disk space. Avoid setting access-control and audit changes on the domain network controller head. Making these changes would needlessly apply to all the objects of all the classes in all the containers in the partition. For example, avoid making changes to Domain Name System (DNS) and digital linear tape (DLT) record registration in the CN=SYSTEM folder of the domain partition.
6. Use the best-practice OU structure to separate user accounts, computer accounts, security groups, and service accounts in their own organizational unit. When you use such a structure, you can apply discretionary access control lists (DACLs) to objects of a single class for delegated administration, and you make it possible for objects to be restored according to object class if they have to be restored. The best-practice OU structure is discussed in the "Creating an Organizational Unit Design" section of the *Best Practice Active Directory Design for Managing Windows Networks* white paper. To obtain this white paper, visit the following Microsoft Web site:

<http://www.microsoft.com/technet/prodtechnol/ad/windows2000/plan/bpaddsgn.asp>

1. Test bulk deletions in a lab environment that mirrors your production domain. Choose the recovery method that makes sense to you, and then customize it to your organization. You may want to identify the following:
   * The names of the domain controllers in each domain that is regularly backed up
   * Where backup images are stored  
       
     Ideally, these images are stored on an extra hard disk that is local to a global catalog in each domain in the forest.
   * Which members of the help desk organization to contact
   * The best way to make that contact
2. Most of the bulk deletions of user accounts, of computer accounts, and of security groups that Microsoft sees are accidental. Discuss this scenario with your IT staff, and develop an internal action plan. At first, focus on early detection and on returning functionality to your domain users and to your business as quickly as possible.

### Tools and scripts that may help you recover from bulk deletions

The Groupadd.exe command-line utility reads the **memberOf** attribute on a collection of users in an OU and builds an .ldf file that adds each restored user account to the security groups in each domain in the forest.   
  
Groupadd.exe automatically discovers the domains and security groups that deleted users were members of and adds them back to those groups. This process is explained in more detail in step 11 of method 1.  
  
Groupadd.exe runs on the following domain controllers:

* Windows Server 2003 domain controllers
* Windows 2000 domain controllers that have the .NET 1.1 framework installed

Groupadd.exe uses the following syntax:

groupadd /*after\_restore ldf\_file* [/*before\_restore ldf\_file*]

Here, *ldf\_file* represents the name of the .ldf file to be used with the previous argument, *after\_restore* represents the user file data source, and *before\_restore* represents the user data from the production environment. (The user file data source is the good user data.)  
  
To obtain Groupadd.exe, contact Microsoft Product Support Services.

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, regarding the performance or reliability of these products.

Groupadd.exe is available on the following Microsoft internal shares:

[\\Efleis\Pub\Groupadd](file:///\\Efleis\Pub\Groupadd)

[\\Lcpssds\Tools\Ad\Groupadd](file:///\\Lcpssds\Tools\Ad\Groupadd)

[\\Ncpssds\Tools\Ad\Groupadd](file:///\\Ncpssds\Tools\Ad\Groupadd)

Groupadd.exe may be given to customers free of charge.  
  
Step 12 in the "How to manually undelete objects in a deleted object's container" section says "Windows Server 2003 does not preserve the **sIDHistory** attribute on reanimated user and computer accounts or security groups." To see if this has changed in Windows Server 2003 SP1, check the status of Windows OS bug 91567.  
  
**Note** The Windows Server 2003 Active Directory Deployment training material covers these steps in more detail. The relevant section is "Student Manual Part Two Module 9: Active Directory Replication." There is also a known issue about the reanimation of domain local groups. See service request number SRZ030915000296 and the 830769 hotfix for more information. (Knowledge Base article 830769 is not yet published.)

### Other scripts

After the authoritative domain controller has been unplugged from the network, and before the computer is started in Active Directory Restore mode, you can run the following script to create a list of users:

List.vbs

--------

Set strOU = GetObject("LDAP://localhost/ou=layer two,ou=layer one,ou=test,dc=i,dc=j,dc=com")

strOU.Filter = Array("user")

For Each Member in strOU

Wscript.Echo Chr(92) & Chr(34) & member.distinguishedname & Chr(92) & Chr(34)

Next

**Note** Make sure that you change the organizational unit path in the first line to point to the path that contains the users and groups to be restored.   
  
You can also use this script to create a list of either users or groups. To create a list of groups, change the filter in the second line to the following:

oU.Filter=Array("group")

To run this script and save the output to a text file, type the following command at the command prompt. Run this command in the same folder as the script:

**cscript //nologo list.vbs > users.txt**

After you have created the list of users and the list of groups, you can use the following script. This script uses the Ntdsutil utility to auth restore each entry.

Authrest.cmd

------------

@echo off

ntdsutil "popups off" "authoritative restore" "restore subtree %1" quit quit

To run this script for every entry in the list of users or the list of groups, use the **for** command to read each entry in the list and pass it to the batch file. To do this, type the following command at the command line. Create these files in the same folder as the two text files that you created earlier.

for /f "tokens=\*" %i in (users.txt) do authrest %i

This command loops through each line of the text file and authoritatively restores the user.

### Future enhancements

Do not share the following information outside Microsoft. To improve the process of recovering users who are deleted in bulk, the Microsoft product group is working on the following enhancements:

1. For Windows Server 2003 SP1 and Windows 2000 SP5, the product group plans to modify the Ntdsutil utility to automate some of the steps that are suggested in this article. One goal is to free the customer from having to restart a domain controller in isolation.  
     
   For additional information, visit the following internal Microsoft Web sites:

<http://bugcheck/default.asp?URL=/Bugs/WindowsSE/41474.asp>

<http://bugcheck/default.asp?URL=/Bugs/WindowsSE/57636.asp>

1. In the next version of Windows Server 2003, the product group plans to change the way Active Directory stores and replicates links. After this change is implemented, administrators will only have to auth restore deleted objects in their host domains. Windows will automate the task of restoring links for all deleted objects, including group membership in all domains in the forest. This feature will require that linked values are defined after the forest functional level has been changed to the Windows Server 2003 forest functional level. For example, users must be added to groups after this change has been made to the forest functional level. If this change is not implemented in the next version of Windows Server 2003, it will be implemented in the Longhorn release of Active Directory.
2. The product group will try to add a functionality to the Recycle Bin in Longhorn. When this functionality is implemented, all a deleted object's attributes and all the values of these attributes are preserved when objects are moved into the deleted objects container. (Currently, only some attributes are preserved when objects are moved into the deleted objects container.) The user interface of the Recycle Bin will also be improved so that administrators can move objects from the deleted objects container back to their original OU containers. The goal of this functionality is that administrators no longer have to restore a system state backup to recover objects that are deleted by accident.

These changes must be approved by the war team of the Windows Sustained Engineering (WinSE) group before they can be implemented.