Restoring deleted Active Directory objects

Introduction

Active Directory provides a very helpful feature to reanimate deleted objects. Depending on your domain functional level, you can restore only a set of basic attributes or with enabled optional feature “the Active Directory Recycle-Bin” most of them.

This Howto covers the restore with and without enabled AD Recycle-Bin.

Currently there are some pitfalls, caused by some known issues. Make sure that you read them, if you were pointed to them.

Some background information

General information

Whenever an Active Directory object is deleted, it is moved into a hidden container, named „Deleted Objects (CN=Deleted Objects, DC=samdom, DC=example, DC=com). Objects in that container remain there for a configurable period of time. After that period, they are finally removed from the directory by the garbage collection.

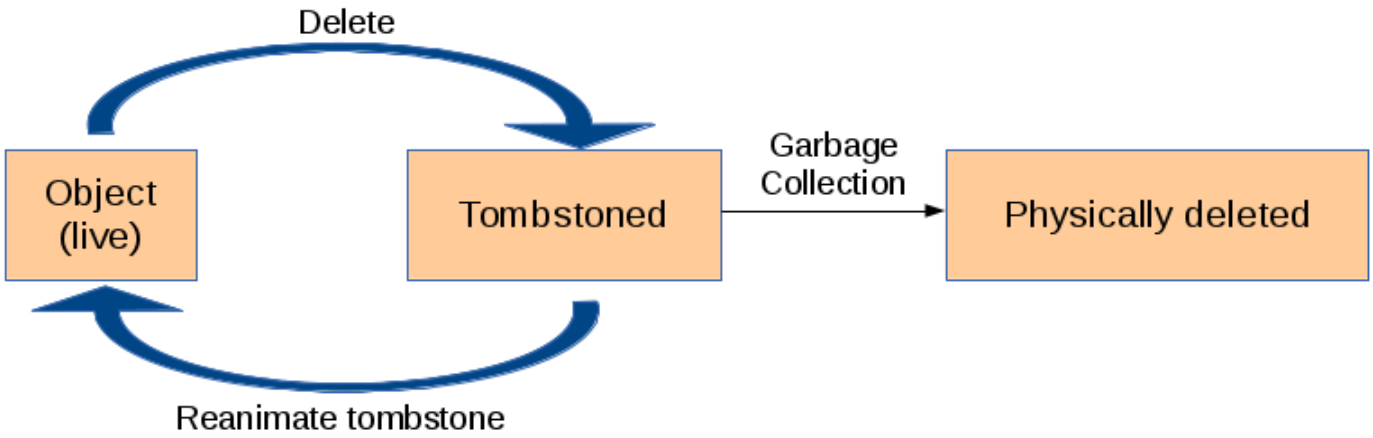
States of a deleted object

There are two states for objects in the Deleted Objects container:

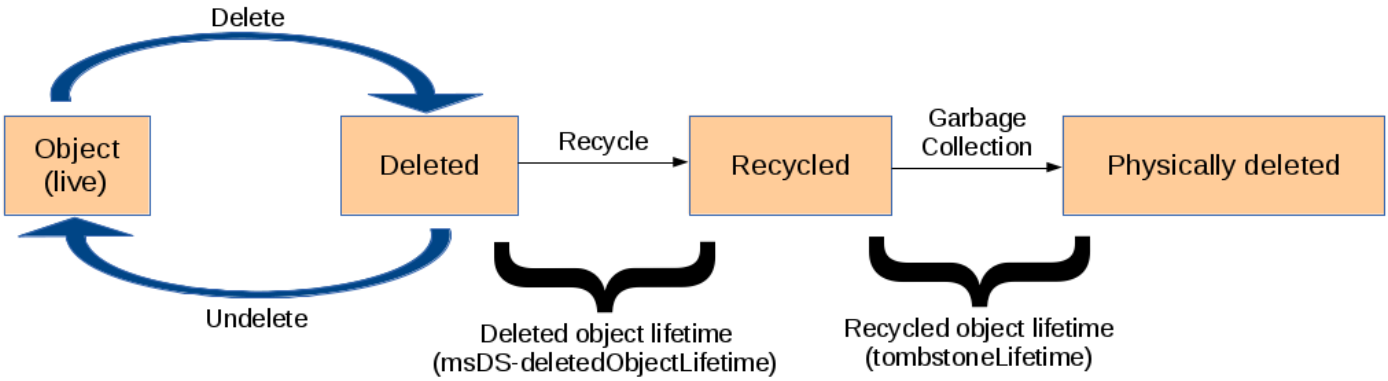
- “**Deleted**”: Objects in that state can be restored for the configured amount of days. The number of attributes which can be restored depends on the AD Recycle-Bin feature. If it has been enabled much more information is kept in place for an eventual recovery.
- “**Recycled**”: Objects in that state can't be restored and are only kept for replicating the deletion.

Active Directory object lifecycle

Object lifecycle with AD Recycle-Bin disabled



Object lifecycle with AD Recycle-Bin enabled



What can/can't be recovered?

- If you haven't enabled the AD Recycle-Bin, only some general attributes, like cn, objectSid, objectGUID, etc. of an object are kept in the Deleted Objects container. But with enabled AD Recycle-Bin, most of the attributes are preserved and can be restored.
- Active Directory doesn't save forward and backward-linked attributes in the tombstones. This means, if you delete e. g. an user account, that the “member” attribute in groups, the account belonged to, and the memberOf attributes in the account object itself, will be lost on deletion.
- Deleted objects from the naming context “configuration” can't be restored.

AD Recycle Bin

Preconditions

- All Domain Controllers in your Active Directory forest are running Windows Server >= 2008r2 or Samba >= 4.0.
- Domain functional level >= 2008r2. See the Raising the functional levels for further information.

Enabling the AD Recycle-Bin

On a Samba DC

Run the following script on a Samba DC to enable the AD Recycle-Bin. It can be found in the Samba sources.

```
# **source4/scripting/bin/enablerecyclebin /usr/local/samba/private/sam.ldb**
Recycle Bin feature enabled
```

Hint: You have to specify the path to the sam.ldb! You can't use a "ldap://URL" here.

On a Windows DC

See the known issue Windows tools for enabling the AD Recycle-Bin don't work.

Reanimating deleted objects

On a Samba DC

The steps to restore do not differ, regardless if you have the AD Recycle-Bin enabled or not.

If you are running a multi DC environment and have the AD Recycle-Bin enabled, see the known issue Multi-DC environment: Deleted objects are recycled too fast.

- Find out the DN of the object in the Deleted Objects container. The following example searches for the DN of an object, whose CN was "demoAccount", before it got deleted:

```
 # ldbsearch -H ldap://localhost -Uadministrator --show-deleted
cn=demoAccount\\0ADEL:
```

```
 Password for [REDTIC\administrator]:
 ...
 dn: CN=demoAccount\0ADEL:b57e14a1-70e9-47e7-9095-7000b0445e16,CN=Deleted
Objects,DC=redtic,DC=uclv,DC=cu
 lastKnownParent: CN=Users,DC=redtic,DC=uclv,DC=cu
 msDS-LastKnownRDN: demoAccount
 ...
```

Your search result will also contain the last known parent object and the attribute msDS-LastKnownRDN, which was the old CN.

- Move the object back to it's last known container (lastKnownParent: CN=Users,DC=redtic,DC=uclv,DC=cu) with its old CN (msDS-LastKnownRDN: demoaccount):

```
 # ldbrename -H ldap://localhost -Uadministrator
CN=demoAccount\0ADEL:b57e14a1-70e9-47e7-9095-7000b0445e16,CN=Deleted
Objects,DC=redtic,DC=uclv,DC=cu"
cn=demoAccount,cn=Users,dc=redtic,dc=uclv,dc=cu"
 Password for [REDTIC\administrator]:
 Renamed 1 record
```

- Edit the renamed object:

```
 # ldbedit -H ldap://localhost -Uadministrator --show-deleted -b
"cn=demoAccount,cn=users,dc=redtic,dc=uclv,dc=cu"
# editing 1 records
# record 1
dn: CN=demoAccount,CN=Users,DC=redtic,DC=uclv,DC=cu
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=samba,DC=example,DC=com     <--- add
this attribute (adapt your realm)
sn: demoAccount
givenName: Demo
instanceType: 4
whenCreated: 20140125214758.0Z
displayName: Demo demoAccount
uSNCreated: 4043
objectGUID: b58f0760-b786-434c-86da-4e0be3c9c039
badPwdCount: 0
codePage: 0
countryCode: 0
homeDirectory: \\DC1\home\demoAccount
homeDrive: H:
badPasswordTime: 0
```

```
lastLogoff: 0
lastLogon: 0
scriptPath: logonscript.bat
primaryGroupID: 513
profilePath: \\DC1\Profiles\demoAccount
objectSid: S-1-5-21-3134998938-619743855-3616620706-1127
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: demoAccount
userPrincipalName: demoAccount@samdom.example.com
mail: demoAccount.Demo@samdom.example.com
pwdLastSet: 130351600780000000
userAccountControl: 512
isDeleted: TRUE                                          <--- remove this
attribute
lastKnownParent: CN=Users,DC=samdom,DC=example,DC=com    <--- remove this
attribute
msDS-LastKnownRDN: demoAccount                           <--- remove this
attribute
cn: demoAccount
name: demoAccount
whenChanged: 20140125231002.0Z
uSNChanged: 4052
distinguishedName: CN=demoAccount,CN=Users,DC=samdom,DC=example,DC=com
```

Through Windows

See the known issue Windows tools for enabling the AD Recycle-Bin don't work.

Changing the defaults for msDS-deletedObjectLifetime and tombstoneLifetime

---

- *msDS-deletedObjectLifetime*: Only configurable, if the AD Recycle-Bin is enabled. The attribute contains the number of days, objects can be restored with most of their attributes.
- *tombstoneLifetime*: Number of days, objects stay in the directory until they are finally removed by the garbage collector. During that time, only a limited set of attributes can be recovered.

See the states of a deleted objects, where these attributes take place.

You can use ldbedit to add/change this values:

```
 # ldbedit -H ldap://localhost -Uadministrator -s base -b "CN=Directory
Service,CN=Windows NT,CN=Services,CN=Configuration,DC=redtic,DC=uclv,DC=cu"
 Password for [REDITC\administrator]:
```

The tombstone lifetime is determined by the value of the tombstoneLifetime attribute. The deleted object lifetime is determined by the value of the msDS-deletedObjectLifetime attribute. By default, tombstoneLifetime is set to null. When tombstoneLifetime is set to null, the tombstone lifetime defaults to 60 days (hard-coded in the system). By default, msDS-deletedObjectLifetime is also set to null. When msDS-deletedObjectLifetime is set to null, the deleted object lifetime is set to the value of the tombstone lifetime. (Source: http://technet.microsoft.com/en-us/library/dd392260%28v=ws.10%29.aspx)

Please be aware of to large lifetimes, as they may cause big AD databases!

Known issues

If you are affected by one or more of the listed known issues, add yourself to the bug report(s), to stay informed about the progress. And of course, any help to get the problems fixed is welcome.

Windows tools for enabling the AD Recycle-Bin don't work

Bug #10371

Currently it's not possible to use Windows tools (like ldp.exe) to enable the the AD Recycle-Bin. The reason is, that Samba currently uses a different operation in background to modify/rename objects.

As a workaround enable the optional feature through Samba.

Windows tools for restoring deleted objects don't work

Bug #10371

Currently it's not possible to use Windows tools (like ldp.exe) to restore deleted objects. The reason is, that Samba currently uses a different operation in background to modify/rename objects.

As a workaround restore deleted objects manually through Samba.

Multi-DC environment: Deleted objects are recycled too fast

Bug #10403

If you have the AD Recycle-Bin feature enabled and run multiple DCs, you may encounter that deleted objects are getting recycled too fast (with the next replication). This leads to the fact, that you can't restore them with the above commands any more, as recycled objects are already waiting for being removed by the garbage collector. If you add “- -show-recycled” to the commands, it may be possible, but be warned about possible unknown side-effects, if you reanimate recycled objects!

Single DC environments are not affected and can use the AD Recycle-Bin without that limitation.

Further documentation about the Active Directory Recycle-Bin

- MS TechNet: Scenario Overview for Restoring Deleted Active Directory Objects.
- MS TechNet: Possible Issues When Restoring Attributes Used by Directory-Enabled Applications.
- MS TechNet: Reanimating Active Directory Tombstone Objects.