Restore deleted components in Active Directory

In essence, Active Directory is a 'massive' database based on a hierarchical architecture, which contains complete information about network systems such as computers, servers, user accounts, and user groups. ... The main purpose of Active Directory is to provide and ensure the validation of all accounts in the system ...

TipsMake.com - In essence, Active Directory is a 'massive' database based on a hierarchical architecture, which contains complete information about network systems such as computers, servers, user accounts. , group of users . The main purpose of Active Directory is to provide and ensure the validation of all accounts in the system. And the 'daily' work of Active Directory is to create, manage, move, edit, delete . many different related objects . And the **Active Directory** database is stored at the **Domain Controller** (aka **DC**), in a file called **NTDS.DIT.**

When deleting a certain object in **Active Directory** , the administrator must be absolutely careful, because if it is mistaken in this phase, their system will be greatly affected, and more other components will be available. related may not be recoverable. For **Windows 2000 Server** and **Windows Server 2003** operating systems, we can do this via **NTBACKUP** and **System State** . In the following article, we will introduce you to some basic operations that can be applied in situations of mistakenly deleting data in Active Directory.

How does 'Active Directory' deal with deleted components?

When any object is deleted from **Active Directory** , it is in fact not, but simply a markup so that the memo system will do this in the next session. Technically, **Active Directory** often uses replication models with the main function being ' *multi-master loose consistency with convergence* '. Changes can be made on any forest in the forest layer, and those changes will in turn be replicated across the entire **forest** . Therefore, objects deleted in this environment are not simply removed from the system in the usual way.

Markers used for objects in **AD** are called **tombstone** . A **tombstone is** actually an object with the **IsDeleted** attribute set to **True** , and that attribute specifies the object that has been deleted but has not been removed from the system, just like deleting a normal data file. The corresponding **Directory services** will proceed to move these **tombstone-** marked objects to the **Deleted Objects** archive, they will continue to "exist" until the process of collecting and processing the redundant file mode removed from the system. This process will work 12 hours each time in default mode on each DC. In addition, the duration of tombstone objects that existed before being removed is **60** days for **Windows 2000/2003 Active Directory** , or **180** days for **Windows Server 2003 SP1 Active Directory** (in default mode). On the other hand, the 'life cycle' of **tombstone** must be established longer than the data deletion process to ensure that the same application with many objects is replicated on other **DCs** .

With the above characteristics, we can see that deleting data here is merely changing the properties of any object, including:

- Set **IsDeleted** to **True** .

- Change the **WhenDeleted** column to **IsDeleted** in the **TimeChanged** section of **metadata** .

- Set the security level of **Windows NT** to a certain value.

- Change **Relative Distinguished Name - RDN** to 1 value cannot be set by **LDAP** application.

- 'Quit' all unnecessary properties at this time by **Active Directory** , some important attributes below have been hard-coded for use in this process such as: **Object-GUID, Object-SID, Object-Dist-Name and USN.**

Besides, you need to understand the difference between recovering an object that has been completely removed from the database, and the non-existence of that object, not just **tombstone** objects and How to recover **tombstone** . Restoring any tombstone object from an **Active Directory** database is often called **reanimation** - and here is the main topic of our article today.

On the other hand, **tombstone** of any object will ignore many technical properties at the same time, we must also note that if you choose to delete user or group accounts, you must also restore the **Membership** group and the properties. The computer is interconnected, you will definitely need to use it in many later sessions. However, one of the **Active Directory features** that was added in **Windows Server 2003 Service Pack 1** is **Directory Service Backup Reminders** . And with this **Reminder** application, every 1 new notification message (for example, ID 2089), the system will provide backup capabilities for each partition of the **Directory** that **DC** stores, which includes partitions. **Directory** application and Active Directory Application Mode - ADAM. If you have experienced a half-life of the **tombstone** that the corresponding partition has not yet been backed up, this will be recorded in the **Directory Service** logs and continue with the daily work until it is completed.

Method to recover deleted components in Active Directory:

In fact, there are several ways we can do this for **Active Directory,** including free or paid tools. However, before embarking on the main job, please back up the entire status of the system, to minimize the possible risk ratio, mainly **System State** , including **Registry** , **COM + Class Registration Database, System Boot Files, certificates from Certificate Server (if installed), Cluster database, NTDS.DIT ??file and SYSVOL directory.**

Restore from previous backup:

Recovering data from the most recent **System State** backup is not really straightforward, and in fact this is not really a data recovery process, but just a retrieval of deleted files. However, since this is done by **NTBACKUP** and the **System State** backup is related to turning off **DC** and rebooting via **DS Restore Mode** , this mechanism will be the only way to recover data. does not affect **DC** operation.

Use LDP.EXE:

As mentioned in the previous section of the article, objects deleted in the **Active Directory** still don't really "disappear" from the system, but they are only marked as **tombstone** in a certain amount of time, possibly 60 or 180 days depending on the operating system managing DC.

Use ADRestore.net:

This is a tool completed by Guy Teverovsky with an easy feature to help users recover deleted AD objects. Some of the main functions of this utility:

- Search for **tombstone**

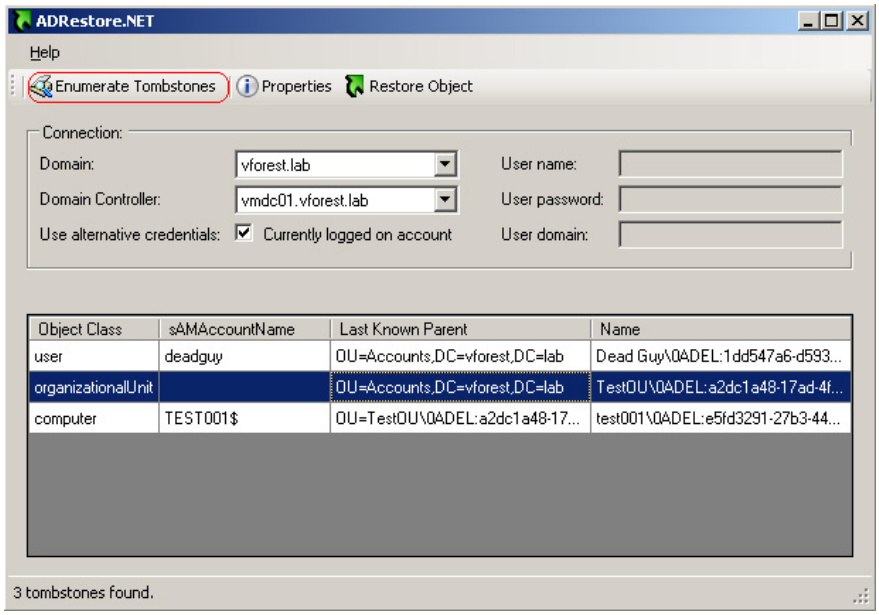
- Assign exactly the **domain controllers** in the system

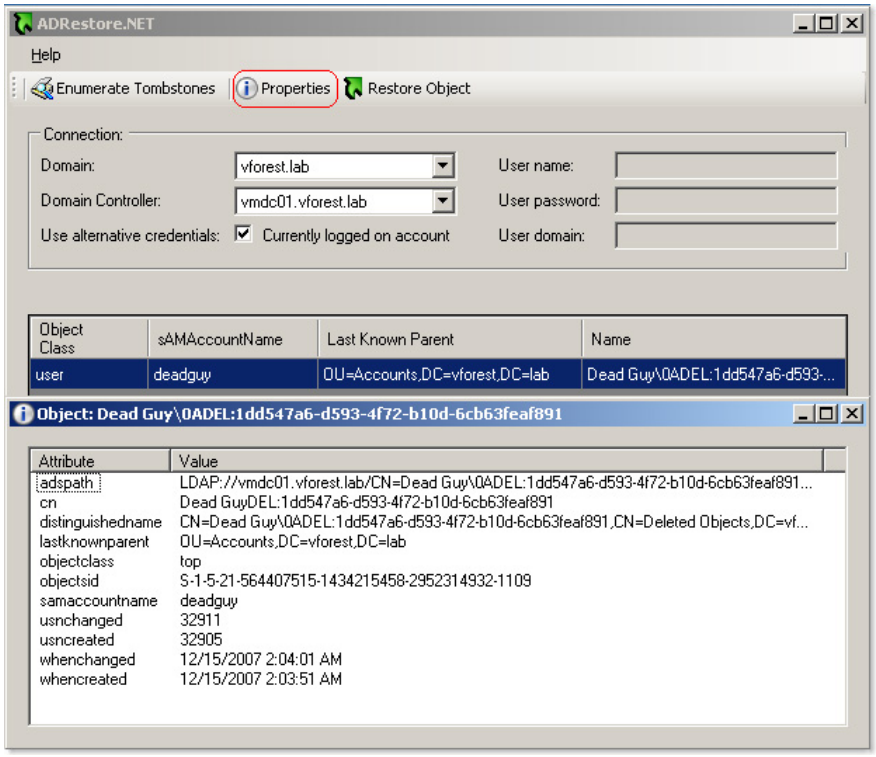
- Can be used with alternative identification information

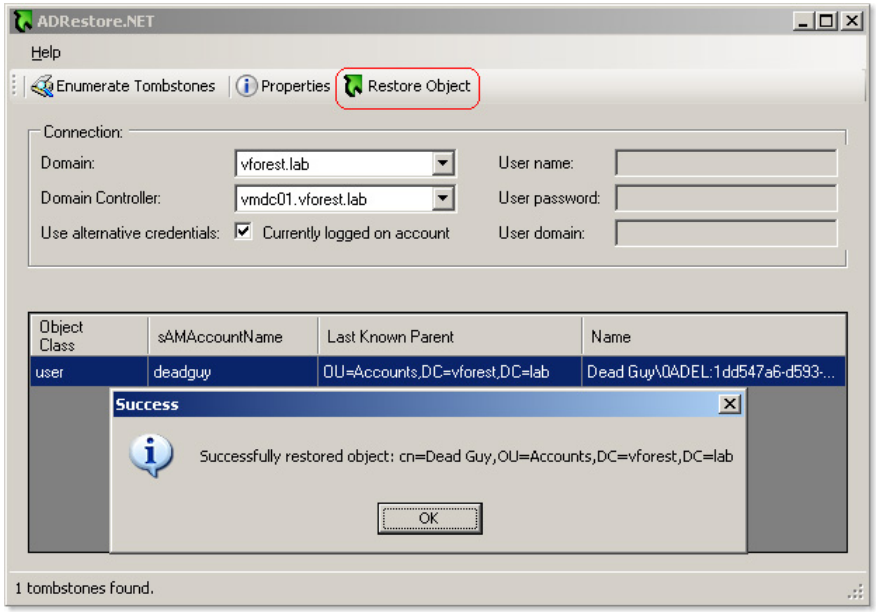
- Restore **User / Computer / OU / Container**

- Additional preview feature - **Preview** the technical properties of **tombstone**

Some pictures of **ADRestore.net** 's main **console:**







Use Microsoft ADRestore:

In addition, you can consult and use Microsoft's free **ADRestore** tool, with a command-line console - **Command Prompt** . When booting, the system will ask you to select the appropriate object to restore, then select **NO** at each question displayed next.

To add the correct option to this recovery process, we can add parameters to the back of the main command structure. For example:

adrestore -r daniel

This command will search all objects with the name *daniel* . The *-r* parameter will 'force' the system to display questions with each recovery. Besides, all objects that match the search request will be automatically restored. In default mode (no parameters), all **tombstone** objects will be listed and restored.

However, you should note that the deleted components will no longer be a member of any fixed **Organizational Unit - OU** . At the same time, recovery in this way will also remove the automatic restore function through the corresponding **OU** , which will have to be done manually.

Use Quest Object Restore for Active Directory:

Quest Software - one of the leading market leaders, provides a solution for managing applications, databases and **Windows** operating systems. Besides, a tool with a graphical interface makes it easy for **Microsoft Active Directory administrators** to recover deleted objects with the **Tombstone Reanimation** feature of **Windows Server 2003** . The advantage of using this tool is that users can completely do it via the online method, not having to restart the **Domain Controller,** adding and completing many features in searching, listing and restoring. **Active Directory** object **.**

Restoring one or more components in **Active Directory** may cause some downtime in the system. Object Restore is a completely free application that allows users to view and browse tombstoned objects in Active Directory and new components deleted with **Microsoft** 's **Tombstone Reanimation** in **Windows Server 2003** . When downloading the **Freeware** version, the key uses the 6-month software that has been built into it. And users will have to re-register on the manufacturer's homepage after 6 months if they want to use it again.

Good luck!