Change the 'life cycle' of tombstone objects in Active Directory

In the previous article, I showed you how to recover deleted components in Active Directory, which are related to the lifecycle properties of tombstone objects. Technically this lifetime must be set longer than the fixed latency between domain controllers. Period of cycles between x & a times

TipsMake.com - In the previous article , we showed you how to recover deleted components in Active Directory, which is related to the life cycle properties of tombstone objects. Technically this lifetime must be set longer than the fixed latency between domain controllers. The period of time between **tombstone** removals must be at least equal to the maximum delay when the process spreads through the **forest** layer. Because the 'validity' period of the tombstone life cycle is based on when the object was actually deleted, not the time the server received the specific tombstone signal through the replication process, and all the **tombstone** of 1 objects are collected on multiple servers at the same time. If the tombstone has not been replicated on a specific **Domain Controller** , that DC will not record the process of deleting the corresponding data. And this is also the main reason why we cannot restore the **Domain Controller** from any backup that is older than the **lifetime** of the **tombstone** .

By default, the **Active Directory** lifetime tombstone time is 60 days, and users can completely change depending on their needs. Specifically, the tombstoneLifetime attribute of the **CN** object **= Directory Service** in the configuration phase must be changed, and this object is fixed at:

cn = Directory Service, cn = Windows NT, cn = Services, cn = Configuration, dc =

Note that the longer this lifetime, the greater the percentage of deleted objects left in the system directory when disconnecting the DC than it is to remove it completely from the DC online. In addition, the lifetime of the tombstone will not change automatically when the user updates Windows Server 2003 to **SP1** , but can be done manually later. The new forest layers that come with **Windows Server 2003 SP1** will have a default lifetime parameter of 180 days.

You can check the default lifetime attribute with the command:

```
dsquery * "cn = Directory Service, cn = Windows NT, cn = Services, cn = Configura
```

In fact, there are many ways to change this parameter, and the simplest way is to use **ADSIEdit** .

Method 1: use ADSIEdit:

This is part of the **Windows 2003 Support Tools,** and if you want to use **ADSIEdit** , you must install **Support tools** directly on the computer or **Domain Controller** . In addition, to complete the steps below, the account in use must be a member of the **Enterprise Admins** group **.**

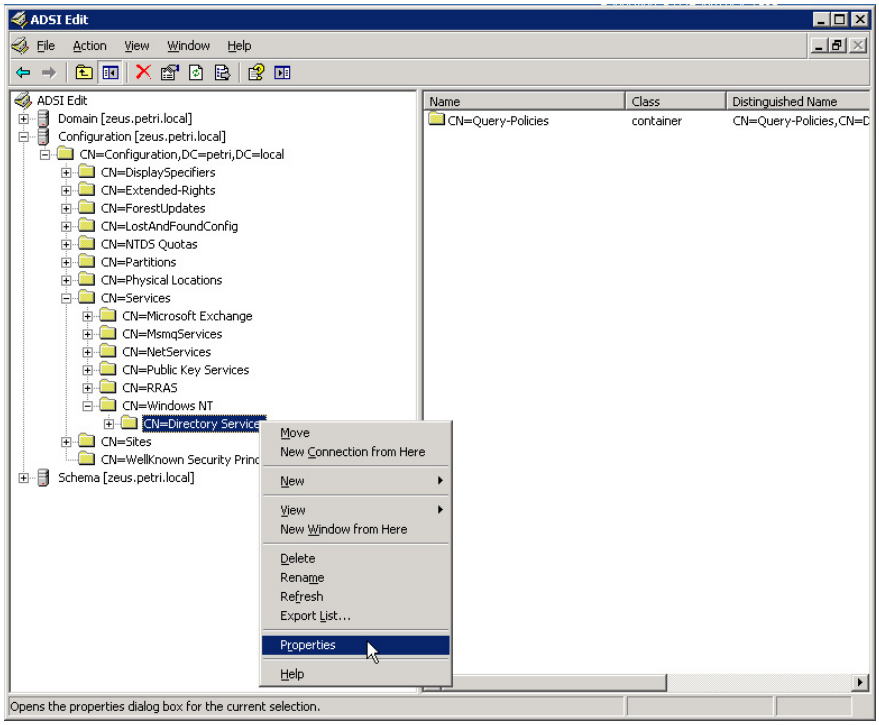
To view or change the attribute value section with **ADSIEdit** , type **ADSIEdit.msc** in the **Run field** and type **Enter** . Then move to:

cn = Directory Service, cn = Windows NT, cn = Services, cn = Configuration, dc =

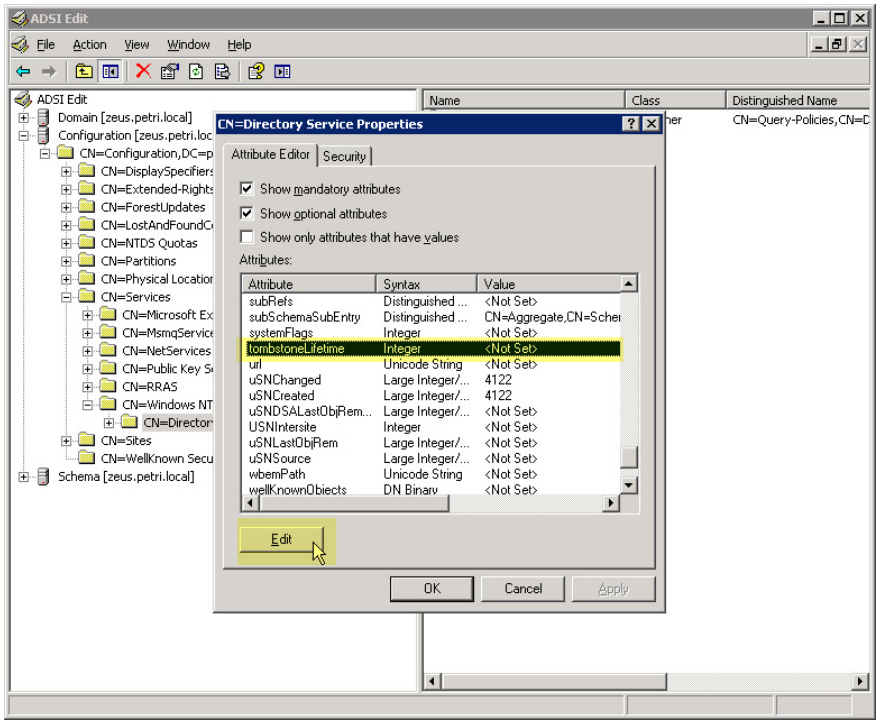
with the **ForestRootDN** is the **Distinguished Name** of the **Active Directory Forest Root** domain. For example, if your domain name is *kuku.co.il* , the **DN** section will be:

DC = kuku, DC = co, DC = il

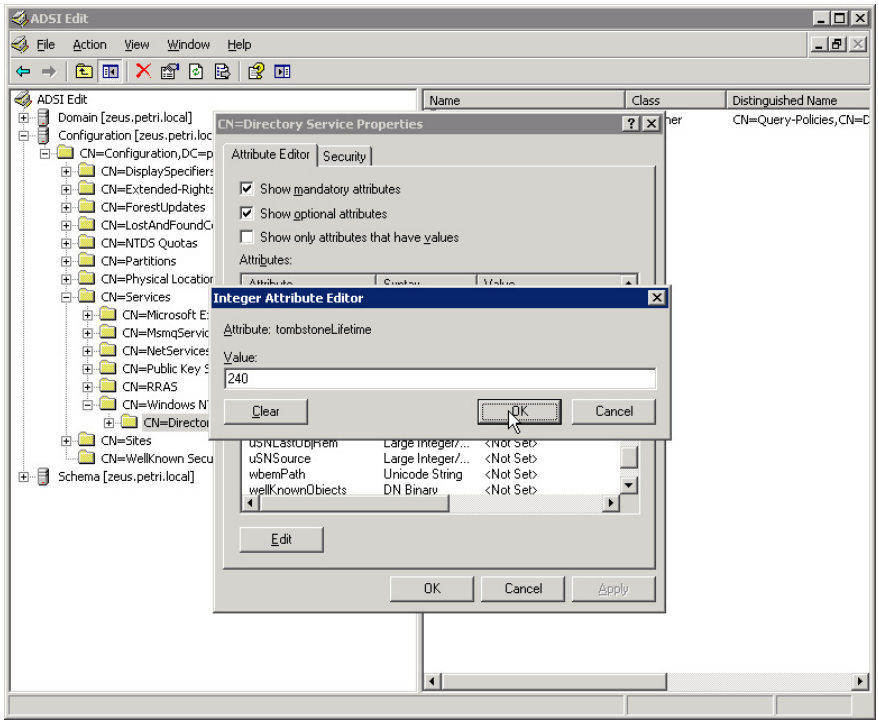
Right-click and select **Properties** :



In the **Properties** window displayed, scroll down to the **tombstoneLifetime** section, click **Edit** :



Change the required **Tombstone Lifetime Period** parameter then click **OK** :



Click **OK** and close **ADSIEdit** again. When we see properties on the *cn = Directory Service section, cn = Windows NT, cn = Services, cn = Configuration* , if no value is set, it means that the default value is valid. And any value the user enters into the Edit Attribute box replaces the default parameter when pressing the **Set** button.

Method 2: use LDIF file:

First, open **Notepad** and create a text file with the content:

```
dn: cn = Directory Service, cn = Windows NT, cn = Services, cn = Configuration,
```

Note that you must not forget the **-** in the last line. With the **Distinguished Name** is the **Active Directory Forest Root** domain **.** For example, if the domain name is *kuku.co.il* , the **DN** part will be:

DC = kuku, DC = co, DC = il

Then, save this file to **tombstoneLifetime.ldf** . Open **Command Prompt** and type the command:

Ldifde –I –f {path to tombstoneLifetime.ldf} file

Quite simple and easy, wish you success!

You finished reading the article "**Change the 'life cycle' of tombstone objects in Active Directory**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.