

How to Find and Remove Lingered Objects in Active Directory

Gary Olsen

Some of the biggest annoyances for any Active Directory administrator are odd little things called lingering objects. These have existed since Windows 2000 Server and will probably never go away completely, although Microsoft has worked to give us some great tools to get rid of them and protect our domain controllers.

While there are already some good articles out there describing lingering objects, I'd like to put my own spin on the issue based on experiences I've had with them. I still find many Active Directory admins who either don't understand what lingering objects are or don't know what to do about them. Put simply, a lingering object is any Active Directory object that has been deleted, but gets reanimated when a DC has not replicated the change during the domain's tombstone lifetime period.

In other words, when an Active Directory object is deleted, it still exists in the AD as a tombstone. This form of the object contains only the mandatory attributes and is moved into the Deleted Objects container. The contents of the Deleted Objects container can be seen using the LDP.exe tool from the Windows Server 2003 Support Tools. Once the object is tombstoned, it will remain in this condition until the tombstone lifetime period expires (which is 60 days by default). At that point, the garbage collection process will purge it from the Active Directory.

Now suppose you have a Global Catalog server in a remote office in Brazil that has not been available on the network for the 60-day tombstone lifetime period. This could be due to maintenance, a network outage, a hardware failures, etc. that prevents the Global Catalog from replicating with the other DCs.

So let's say you have a multiple domain forest and 100 users were deleted from the United Kingdom domain while the Brazil DC was off the network. Finally, the Brazil Global Catalog comes back online and starts replicating, but since it did not replicate the deletion of those 100 user objects which have now been purged from Active Directory, it thinks that those objects need to be replicated to its partners. So now the partners replicate the objects and those 100 accounts are alive again – sort of. Since the Brazil Global Catalog contains a read-only copy of the United Kingdom domain, it replicates read-only copies of those objects.

In this condition you will see all sorts of anomalies. You may have deleted an account called RBrown several months ago and now another person joins the company with a similar name. You try to create the RBrown account and will get an error saying it already exists. You may also see inconsistencies in the Active Directory such as two copies of an object (a lingering version and a recreated version), or you may see different objects in a user interface depending on which Global Catalog/domain controller you query. You could even get conflicting objects and find that email has failed due to inconsistencies in the Global Address List (GAL).

Preventing Lingered Objects

Of course, it's most desirable to prevent lingering objects from being created in the first place. There is a registry key called StrictReplicationConsistency -- which we'll refer to as Strict Mode -- that will protect a DC from lingering objects:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters  
ValueName = Strict Replication Consistency  
Data Type = Reg_DWORD  
Value Data = 1 = Strict 0=Loose
```

If this value is set to 1, it will prevent a partner from replicating lingering objects to the DC it is defined on. Thus, if every domain controller has Strict Mode enabled, they are protected from lingering objects

How to Find and Remove Lingered Objects in Active Directory

Gary Olsen

being propagated to them. If the value is set to 0, however, it is said to be in Loose Mode, and will allow the lingering objects to be propagated.

Now in Windows 2000 Server, the default value for StrictReplicationConsistency is loose consistency. This is important to note because if you have a domain that was upgraded to Windows Server 2003 from Windows 2000 and this key remained in the default Loose Mode, the domain will remain in loose mode. On the other hand, if you install a clean Windows Server 2003 domain, without upgrading from Windows 2000 Server, it will be in Strict Mode by default.

I've worked with a few organizations that suffered lingering objects because they had not taken the time to check this registry key. Again, you should always define the StrictReplicationConsistency key =1 in normal operations. It should only be set to 0 during removal of lingering objects.

Also, when Strict Mode is enabled on say DC1, and DC2 attempts to replicate an object that has been deleted on DC1, replication will be disabled between DC1 and DC2. Not just replication of the object either -- all replication between the two DCs.

Determining the Existence of Lingered Objects in the Domain

Various events will either indicate the existence of Active Directory lingering objects, or will warn that they may exist. There are several events that might be logged in the Directory Service event.

Event ID 1864

This event will indicate if there are lingering objects. Note that it contains a count of how many DCs have not replicated in a day, week, month, two months, or the tombstone lifetime. The last entry is important. Unfortunately, the event will not tell us the name of the domain controller that hasn't replicated in the tombstone lifetime.

Source NTDS Replication

Event ID 1864

User NT AUTHORITY\ANONYMOUS LOGON

This is the replication status for the following directory partition on the local domain controller.

Directory partition:

DC=DomainDnsZones,DC=corp,DC=com

The local domain controller has not recently received replication information from a number of domain controllers. The count of domain controllers is shown, divided into the following intervals.

More than 24 hours:

2

More than a week:

2

More than one month:

1

More than two months:

1

More than a tombstone lifetime:

1

Tombstone lifetime (days):

60

How to Find and Remove Lingered Objects in Active Directory

Gary Olsen

Event 2042 (Error) -- Source: NTDS Replication

This identifies that strict replication is enabled, the "source DC" has not replicated in tombstone lifetime days and is attempting to replicate, thus replication has been disabled from the source. The event provides the GUID of the source in the format of the CName (alias) DNS record: 982a942e-40e4-4e3c-8609-bae0cfd2affb._msdcs.corp.net. The friendly name of the domain controller can easily be found by looking at the Alias records in the _msdcs zone in the DNS snap-in.

Event ID 1388 (Error) – Source: NTDS Replication

Description: Another domain controller (DC) has attempted to replicate into this DC an object which is not present in the local Active Directory database. The object may have been deleted and already garbage collected (a tombstone lifetime or more has past since the object was deleted) on this DC.

Event 1988 (Error) -- Source: NTDS Replication

Description: Active Directory Replication encountered the existence of objects in the following partition that have been deleted from the local domain controllers (DCs) Active Directory database. This event is being logged because the source DC contains a lingering object which does not exist on the local DCs Active Directory database.

Source DC (Transport-specific network address):
4a8717eb-8e58-456c-995a-c92e4add7e8e._msdcs.Corp.com

Since these are logged individually on each domain controller, you can use a tool like Microsoft EventComb, which is part of the Account Lockout tools download. Events 1864 and 1862 indicate the existence of lingering objects.

If you run the command Repadmin /showrepl when replication has been disabled due to strict consistency, you will see verbiage such as:

```
==== INBOUND NEIGHBORS =====
```

```
DC=Wtec,DC=adapps,DC=hp,DC=com  
  Bracknell\GSE-EXCH3 via RPC  
    DC object GUID: 00b71e7b-46e3-4b2e-8eef-c05f08d2ab82
```

```
***** 753 CONSECUTIVE FAILURES since 2008-12-15 11:52:10
```

```
Last error: 8614 (0x21a6):
```

```
  The Active Directory cannot replicate with this server because the time  
  since the last replication with this server has exceeded the tombstone lifetime.
```

From the error here, it is pretty obvious that the domain controller is being protected from an out-of-date DC. As part of regular Active Directory health maintenance, it's a good idea to run the following command manually or by script:

```
Repadmin/replsum /bysrc /bydest /sort:delta
```

```
Source DC largest delta fails/total %% error  
WTEC-DC2 >60 days      105 /105    100 (1722)The RPC server...  
WTEC-DC1 41m:26s      0/20       0  
GSE-EXCH3 08m:59s     0/6        0  
WTEC-DC6 08m:34s     0/6        0
```

How to Find and Remove Lingered Objects in Active Directory

Gary Olsen

In this output, we can see how long it has been since each of the other DCs have replicated with the one on which the command has been run. Of course the red flag is WTEC-DC2 that tells us it hasn't replicated to our target DC for more than 60 days (tombstone lifetime).

The action that should be taken in this instance is to NOT fix it. Luckily, it is not replicating or we would have the danger of lingering objects coming to our source DC if strict consistency is not enabled. The resolution for WTEC-DC1 is to remove it from the network, manually demote it, clean up the server object in Active Directory, wait for replication and re-promote it.

Removing Active Directory Lingered Objects

If you have found the events and errors noted above, the lingering objects need to be cleaned up. You can refer to the Microsoft articles in the box to the right for more details, but here is the quick version.

The first step is to set the StrictReplicationConsistency registry value =1 (Strict), if it isn't already set. Be sure to check it – don't assume you know what it is. Use the Repadmin command to set this value on all DCs:

```
repadmin /regkey DC_LIST +strict
```

Simply add the DCs to be affected in the DC_List argument.

In the Windows Server 2003 SP1 (and later) Support Tools, the Repadmin tool has a nice switch called \RemoveLingeredObjects:

```
/removelingeredobjects [/ADVISORY_MODE]
```

This is a general lingering object purge. The arguments are:

```
Dest_DC_List - list of DCs to operate on  
Source DC GUID - the DSA GUID of a reliable DC (preferably the PDC)  
NC - Naming context of the domain the lingering objects exist in.  
/ADVISORY_MODE - identifies what will happen when you execute the command for real.
```

So a sample command would be:

```
C:\>Repadmin /removeLingeredObjects wtec-dc1 f5cc63b8-cdc1-4d43-8709-22b0e07b48d1  
dc=wtec,dc=adapps,dc=hp,dc=com
```

```
RemoveLingeredObjects sucessfull on wtec-dc1.
```

After running the Repadmin command, check the event log for the events noted previously to ensure the lingering objects are removed.

Obviously for a single domain forest with a few DCs, it will be pretty easy to find the warning signs and run the Repadmin command to remove the lingering objects. In a large forest with multiple domains, however, it isn't so easy. For instance, the lingering objects may only exist on some subset of DCs in the forest. This command would need to be run for every naming context in the forest.

In an upcoming article, I will describe some advanced techniques for finding and removing lingering objects in large, multi-domain forests, including some advanced commands and scripting methods.