

# TRACKING A DELETED ACTIVE DIRECTORY OBJECT'S REPLICATION STATUS

Mark E. Donaldson

There are many times when a Windows admin needs to determine when a change -- such as the creation, modification or deletion of an object -- has been replicated throughout the forest. For instance, if you demote a DC or a GC either manually or via DCPromo, you must wait until the deleted server object has replicated to all domain controllers before you re-promote using the same name.

The problem comes if you want to demote the existing DC and re-promote it with the same name and IP address on a different physical computer. When you re-promote the DC or want to promote another machine with the same name and IP address, it will create a new computer account with a new GUID. If you do the new promotion before the first object deletion has replicated to all DCs in the forest, it will cause a great deal of confusion about the status of this object. Some domain controllers will know that the old object is deleted and the new one is now in existence. Some will see the old one but not the new one, and some will see both as valid objects.

This is because of Active Directory replication latency. I have seen cases where adequate time was not allowed before the promotion of the new DC with the same name, and they usually eventually converge and are happy. However, I would recommend waiting long enough for the change to be replicated thru the forest before promoting a new DC with the same name.

The tricky part of this operation is to determine when all the DCs have replicated the deletion. Usually you can just wait overnight to be sure, but there is an easy way to find out using the Repadmin command. Repadmin.exe is part of the Windows Support tools for Windows 2003 Service Pack 1. These support tools are *not* installed automatically by installing SP1. If you have a CD for SP1, they will be on the CD. Also refer to KB 892777. If you have a Windows 2000 environment, then you can install the support tools on a Windows 2003 Server or XP workstation and execute the command.

The general command using the /ShowObjMeta is:

**Repadmin /showObjMeta <DC name > < "DN of computer object">**

In the following example, the *DC HPQNET-DC3* has been demoted and removed. It's Distinguished Name, or DN, is *DC=hpqnet-DC3,DC=hpqnet,DC=cpqcorp,DC=net*.

The command:

```
C:\>repadmin /showobjmeta hpqnet-dc3 "CN=HPQnet-DC3,OU=Domain Controllers  
OU, DC=hpqnet,DC=qttest,DC=cpqcorp,DC=net"
```

Executing the Repadmin command above returned the following table:

# TRACKING A DELETED ACTIVE DIRECTORY OBJECT'S REPLICATION STATUS

Mark E. Donaldson

Loc.USN	Originating DC	Org.USN	Org.Time/Date	Ver	Attribute
=====	=====	=====	=====	====	=====
72830	Dublin\HPQBOX-DC02	68360	2005-07-26 16:28:52	1	objectClass
72878	Roseville\HPQBOX-DC01	72878	2005-07-26 16:31:10	2	cn
72884	Roseville\HPQBOX-DC01	72884	2005-07-26 16:32:01	2	description
624242	Roseville\HPQBOX-DC01	624242	2005-11-03 02:11:42	1	userCertificate
72830	Dublin\HPQBOX-DC02	68360	2005-07-26 16:28:52	1	instanceType
72830	Dublin\HPQBOX-DC02	68360	2005-07-26 16:28:52	1	whenCreated
73146	Alpharetta\HPQBOX-DC03	12290	2005-07-26 17:32:54	2	nTSecurityDescriptor
72878	Dublin\HPQBOX-DC02	68395	2005-07-26 16:30:57	2	name

This command dumps the values of all object attributes *if* it finds the object. If it doesn't find the object, it will return an error:

**DsReplicaGetInfo() failed with status 8333 (0x208d): Directory object not found.**

There is one final option that will allow admins to execute this command on all DCs with one command -- without having to execute it on each DC individually. Using the \* in the DCLIST option executes the command on all DCs – one at a time – and reports if it finds the object. If it returns an error, then the computer object is not in the DC OU because that was the path we are searching for. When all DCs report the error, then we know all of them have moved the old DC computer object into the Deleted Objects folder and it is safe to promote the new computer using the name and IP of the old one.

The command in our example to execute on all DCs would be

```
C:\>repadmin /showobjmeta "*"cn=hpqbox-dc03,ou=domain
controllers,dc=hpqbox,dc=a dapps,dc=hp,dc=com" >objmeta.txt
```

Here, we have redirected the output to a text file, *Objmeta.txt*.

# **TRACKING A DELETED ACTIVE DIRECTORY OBJECT'S REPLICATION STATUS**

**Mark E. Donaldson**

Again, if any of the DCs in the report return attributes for the object, then the deletion has not replicated there yet. If there is an error for each DC in the list, then AD object replication has completed and the new machine can be promoted.