

## Re: removing Windows 2008 DC after demotion, time for ntdsutil

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2009-05/msg00944](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2009-05/msg00944)

---

- *From:* "Edward Ray" <[hunglikethor@xxxxxxxxxxxxx](mailto:hunglikethor@xxxxxxxxxxxxx)>
  - *Date:* Wed, 20 May 2009 21:52:39 -0700
- 

Thanks ACE! Was able to solve the problem myself by going into "adsiedit" and making the changes, then doing a "net stop ntds && net start ntds" on both Windows 2008 DCs. Windows 2003 DC had to do a reboot; no ntds service and manually stop and restarting did not have an effect.

Yes I used the aforementioned KB article to remove the CA then put it back on after DC demotion.

Edward W. Ray

"Ace Fekay [Microsoft Certified Trainer]" <[aceman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:aceman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message [news:u7pPl2Z2JHA.5244@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:u7pPl2Z2JHA.5244@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)

"Edward Ray" <[hunglikethor@xxxxxxxxxxxxx](mailto:hunglikethor@xxxxxxxxxxxxx)> wrote in message [news:3C37A4A9-E62F-47EA-BEAB-FE175823370D@xxxxxxxxxxxxxxxxxxxx](mailto:news:3C37A4A9-E62F-47EA-BEAB-FE175823370D@xxxxxxxxxxxxxxxxxxxx)

Looks like I will have to put in some time answering other peoples questions; this my third in last week or so :)

REcently demoted a Windows 2008 x64 Enterprise DC to a member server. It was also an enterprise subordinate CA so first I backed up private key, database and registry settings of the CA. Then I removed the Active Directory Services (had to do this before DC demotion). Then I used "dcpromo" to demote the DC, followed by then removal "Active Directory Domain Services" and "DNS Server" in the "Server Manager." Then I added back the Active Directory Certificate Services and imported the private key, database and registry settings.

All appeared to be working fine, except that all of my clients still continue to try to get Kerberos tickets from the demoted DC (I use "tcpdump" on a SPAN switch port to observe this). In addition the demoted DC is still listed in the "Active Directory Sites and Services" and attempts to remove it fail due to lack of permissions. This is despite the fact I am logged in as an Enterprise Admin and the Enterprise Admin has the "Full Control" under the Security tab of the demoted DC in sites and services.

The recently added DC (also a Windows 2008 x64 Enterprise system has the following error in the Directory Service Event log (Event ID 1568, repeated 3 times in same time period):

Re: removing Windows 2008 DC after demotion, time for ntdsutil

None of the directory servers in the following site that replicate the following directory partition are configured to use the following transport, even though the site itself is configured to allow replication over this transport.

Site:

CN=Orange,CN=Sites,CN=Configuration,DC=mmicmanhomenet,DC=local

Directory partition:

CN=Configuration,DC=mmicmanhomenet,DC=local

Transport:

CN=SMTP,CN=Inter-Site

Transports,CN=Sites,CN=Configuration,DC=mmicmanhomenet,DC=local

User Action

- Configure the site to not allow replication using this transport by modifying the appropriate siteLink objects.
- Enable one or more directory servers to use this transport. For the SMTP transport, this requires installation of the SMTP service and configuration of the mailAddress attribute on the corresponding Server object.

All of my domain controllers ( 2 Windows 2008 Enterprise, 1 Windows 2003 R2 SP 2 Enterprise, Windows 2003 native AD domain/forest) are in different sites, have the SMTP service installed and have a rule allowing them to replicate via SMTP. This is by choice; I have found it to be a more secure as well as robust way to replicate across geographically dispersed sites.

Suspect it is time to use ntdsutil to clean up the AD and fix these issues. Been awhile since I have messed around with ntdsutil so if someone can point to of give me a step by step much appreciated. Main goal is to get old demoted DC records out of the AD and be able to remove the server from Sites and Services. I also do not seem to have permissions to remove the site link and recreate, which was the first thing I tried.

Thanks in advance!

Edward Ray  
CISSP, GCIA, GCIH, MCSE+Security  
Netsec Consulting

Here you go, Edward!

How to remove data in Active Directory after an unsuccessful domain controller demotion  
<http://support.microsoft.com/?id=216498>

Also, I'm not sure if it was clear, but did you uninstall/remove the CA before demotion or at least remove it's reference as a subordinate out of the Forest? If so, curious which KB did you follow? Was it the following

Re: removing Windows 2008 DC after demotion, time for ntdsutil

Re: removing Windows 2008 DC after demotion, time for ntdsutil

KB?

How to decommission a Windows enterprise certification authority and how to remove all related objects from Windows Server 2003 and from Windows Server 2000 (same for 2008)

<http://support.microsoft.com/kb/889250>

--

Ace

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSA Messaging, MCT

Microsoft Certified Trainer

aceman@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

For urgent issues, you may want to contact Microsoft PSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

"Efficiency is doing things right; effectiveness is doing the right things." – Peter F. Drucker

<http://twitter.com/acefekay>

.