How to remove data in Active Directory after an unsuccessful domain controller demotion

Article ID : 216498
Last Review : April 25, 2005
Revision : 7.3
This article was previously published under Q216498

SUMMARY

This article describes how to remove data in Active Directory after an unsuccessful domain controller demotion.

Warning If you use the ADSI Edit snap-in, the LDP utility, or any other LDAP version 3 client, and you incorrectly modify the attributes of Active Directory objects, you can cause serious problems. These problems may require you to reinstall Microsoft Windows 2000 Server, Microsoft Windows Server 2003, Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003, or both Windows and Exchange. Microsoft cannot guarantee that problems that occur if you incorrectly modify Active Directory object attributes can be solved. Modify these attributes at your own risk.

The Active Directory Installation Wizard (Dcpromo.exe) is used for promoting a server to a domain controller and for demoting a domain controller to a member server (or to a stand-alone server in a workgroup if the domain controller is the last in the domain). As part of the demotion process, the wizard removes the configuration data for the domain controller from Active Directory. This data takes the form of an NTDS Settings object that exists as a child of the server object in Active Directory Sites and Services.

The information is in the following location in Active Directory:
CN=NTDS Settings,CN=<servername>,CN=Servers,CN=<sitename>,CN=Sites,CN=Configuration,DC=<domain>...
The attributes of the NTDS Settings object include data representing how the domain controller is identified in respect to its replication partners, the naming contexts that are maintained on the machine, whether the domain controller is a global catalog server, and the default query policy. The NTDS Settings object is also a container that may have child objects that represent the domain controller's direct replication partners. This data is required for the domain controller to operate in the environment, but is retired upon demotion.

In the event that the NTDS Settings object is not removed correctly (for example, if the NTDS Settings object is not correctly removed from a demotion attempt), the administrator can use the Ntdsutil.exe utility to manually remove the NTDS Settings object. The following steps list the procedure for removing the NTDS Settings object in Active Directory for a particular domain controller. At each Ntdsutil menu, the administrator can type **help** for more information about the available options.

Caution The administrator must also make sure that replication has occurred since the demotion before manually removing the NTDS Settings object for any server. Using the Ntdsutil utility incorrectly may result in partial or complete loss of Active Directory functionality.

back to the top

Procedure

1. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command**

Prompt.

2. At the command prompt, type **ntdsutil**, and then press ENTER.
3. Type **metadata cleanup**, and then press ENTER. Based on the options given, the administrator can perform the removal, but additional configuration parameters must be specified before the removal can occur.
4. Type **connections** and press ENTER. This menu is used to connect to the specific server where the changes occur. If the currently logged on user does not have administrative permissions, different credentials can be supplied by specifying the credentials to use before making the connection. To do so, type **set creds *DomainNameUserNamePassword***, and then press ENTER. For a null password, type **null** for the password parameter.
5. Type **connect to server *servername***, and then press ENTER. You should receive confirmation that the connection is successfully established. If an error occurs, verify that the domain controller being used in the connection is available and the credentials you supplied have administrative permissions on the server.

   Note If you try to connect to the same server that you want to delete, when you try to delete the server that step 15 refers to, you may receive the following error message:
   Error 2094. The DSA Object cannot be deleted0x2094
6. Type **quit**, and then press ENTER. The **Metadata Cleanup** menu appears.
7. Type **select operation target** and press ENTER.
8. Type **list domains** and press ENTER. A list of domains in the forest is displayed, each with an associated number.
9. Type **select domain *number*** and press ENTER, where *number* is the number associated with the domain the server you are removing is a member of. The domain you select is used to determine if the server being removed is the last domain controller of that domain.
10. Type **list sites** and press ENTER. A list of sites, each with an associated number, is displayed.
11. Type **select site *number*** and press ENTER, where *number* is the number associated with the site the server you are removing is a member of. You should receive a confirmation listing the site and domain you chose.
12. Type **list servers in site** and press ENTER. A list of servers in the site, each with an associated number, is displayed.
13. Type **select server *number***, where *number* is the number associated with the server you want to remove. You receive a confirmation listing the selected server, its Domain Name Server (DNS) host name, and the location of the server's computer account you want to remove.
14. Type **quit** and press ENTER. The **Metadata Cleanup** menu appears.
15. Type **remove selected server** and press ENTER. You should receive confirmation that the removal completed successfully. If you receive the following error message:
    Error 8419 (0x20E3)
    The DSA object could not be found
    the NTDS Settings object may already be removed from Active Directory as the result of another administrator removing the NTDS Settings object, or replication of the successful removal of the object after running the DCPROMO utility.

    Note You may also see this error when you try to bind to the domain controller

that is going to be removed. Ntdsutil has to bind to a domain controller other than the one that is going to be removed with metadata cleanup.

16. Type **quit** at each menu to quit the Ntdsutil utility. You should receive confirmation that the connection disconnected successfully.
17. Remove the cname record in the _msdcs.*root domain of forest* zone in DNS. Assuming that DC is going to be reinstalled and re-promoted, a new NTDS Settings object is created with a new GUID and a matching cname record in DNS. You do not want the DC's that exist to use the old cname record.

    As best practice you should delete the hostname and other DNS records. If the lease time that remains on Dynamic Host Configuration Protocol (DHCP) address assigned to offline server is exceeded then another client can obtain the IP address of the problem DC.

Now that the NTDS Settings object has been deleted, you can delete the computer account, the FRS member object, the cname (or Alias) record in the _msdcs container, the A (or Host) record in DNS, the trustDomain object for a deleted child domain, and the domain controller.

The Adsiedit utility is included with the Windows Support Tools feature in both Windows 2000 Server and Windows Server 2003. To install the Windows Support Tools, following these steps:

- Windows 2000 Server: On the Windows 2000 Server CD, open the Support\Tools folder, double-click **Setup.exe**, and then follow the instructions that appear on the screen.

- Windows Server 2003: On the Windows Server 2003 CD, open the Support\Tools folder, double-click **Suptools.msi**, click **Install**, and then follow the steps in the Windows Support Tools Setup Wizard to complete the installation.

1. Use ADSIEdit to delete the computer account. To do this, follow these steps:
   a. Click **Start**, click **Run**, type **adsiedit.msc** in the **Open** box, and then click **OK**.
   b. Expand the **Domain NC** container.
   c. Expand **DC=*Your Domain Name*, DC=COM, PRI, LOCAL, NET**.
   d. Expand **OU=Domain Controllers**.
   e. Right-click **CN=*domain controller name***, and then click **Delete**.

   If you receive the "DSA object cannot be deleted" error message when you try to delete the object, change the UserAccountControl value. To change the UserAccountControl value, right-click the domain controller in ADSIEdit, and then click **Properties**. Under **Select a property to view**, click **UserAccountControl**. Click **Clear**, change the value to 4096, and then click **Set**. You can now delete the object.

   Note The FRS subscriber object is deleted when the computer object is deleted because it is a child of the computer account.

2. Use ADSIEdit to delete the FRS member object. To do this, follow these steps:
   a. Click **Start**, click **Run**, type **adsiedit.msc** in the **Open** box, and then click **OK**
   b. Expand the **Domain NC** container.

c. Expand **DC=*Your Domain*, DC=COM, PRI, LOCAL, NET**.
d. Expand **CN=System**.
e. Expand **CN=File Replication Service**.
f. Expand **CN=Domain System Volume (SYSVOL share)**.
g. Right-click the domain controller you are removing, and then click **Delete**.

3. In the DNS console, use the DNS MMC to delete the A record in DNS. The A record is also known as the Host record. To delete the A record, right-click the A record, and then click **Delete**. Also delete the cname (also known as the Alias) record in the **_msdcs** container. To do so, expand the **_msdcs** container, right-click the cname, and then click **Delete**.

   Important If this was a DNS server, remove the reference to this DC under the **Name Servers** tab. To do this, in the DNS console, click the domain name under **Forward Lookup Zones**, and then remove this server from the **Name Servers** tab.

   Note If you have reverse lookup zones, also remove the server from these zones.

4. If the deleted computer was the last domain controller in a child domain and the child domain was also deleted, use ADSIEdit to delete the trustDomain object for the child. To do this, follow these steps:
   a. Click **Start**, click **Run**, type **adsiedit.msc** in the **Open** box, and then click **OK**
   b. Expand the **Domain NC** container.
   c. Expand **DC=*Your Domain*, DC=COM, PRI, LOCAL, NET**.
   d. Expand **CN=System**.
   e. Right-click the **Trust Domain** object, and then click **Delete**.

5. Use Active Directory Sites and Services to remove the domain controller. To do this, follow these steps:
   a. Start Active Directory Sites and Services.
   b. Expand **Sites**.
   c. Expand the server's site. The default site is **Default-First-Site-Name**.
   d. Expand **Server**.
   e. Right-click the domain controller, and then click **Delete**.

Also, consider the following:

- If the removed domain controller was a global catalog server, evaluate whether application servers that pointed to the offline global catalog server must be pointed to a live global catalog server.

- If the removed DC was a global catalog server, evaluate whether an additional global catalog must be promoted to the address site, the domain, or the forest global catalog load.

- If the removed DC was a Flexible Single Master Operation (FSMO) role holder, relocate those roles to a live DC.

- If the removed DC was a DNS server, update the DNS client configuration on all member workstations, member servers, and other DCs that might have used this DNS server for name resolution. If it is required, modify the DHCP scope to reflect the removal of the DNS server.

- If the removed DC was a DNS server, update the Forwarder settings and the Delegation settings on any other DNS servers that might have pointed to the removed DC for name resolution.