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

https://support.microsoft.com/en-us/help/216498/how-to-remove-data-in-active-directory-after-an-unsuccessful-domain-co

Applies to: Microsoft Windows Server 2003 Standard Edition (32-bit x86)Microsoft Windows Server 2003 Enterprise Edition (32-bit x86)Microsoft Windows Server 2003 Datacenter Edition (32-bit x86) More

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.

If the NTDS Settings object is removed incorrectly (for example, if the NTDS Settings object is removed incorrectly from a demotion attempt), the administrator can manually remove the metadata for a server object. In Windows Server 2008, and Windows Server 2008 R2, the administrator can remove the metadata for a server object by removing the server object in the Active Directory Users and Computers snap-in.

In Windows Server 2003 and Windows 2000 Server, 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.

Windows Server 2003 Service Pack 1 (SP1) or later service packs – Enhanced version of Ntdsutil.exe

The version of Ntdsutil.exe that is included with Service Pack 1 or later service packs for Windows Server 2003 has been enhanced to make the metadata cleanup process complete. The Ntdsutil.exe version that is included with SP1 or later service packs does the following when metadata cleanup is run:

- Removes the NTDSA or NTDS Setting subject.
- Removes inbound AD connection objects that existing destination DCs use to replicate from the source DC being deleted .
- Removes the computer account .

- Removes FRS member object.
- Removes FRS subscriber objects.
- Tries to seize flexible single operations master roles (also known as flexible single master operations or FSMO) held by the DC that are being removed .

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.

Procedure 1: Windows Server 2003 SP1 or later service packs only

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 this, 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 whether 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, appears.
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 System (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, 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.

Error 8419 (0x20E3)
The DSA object could not be found

Note You may also see this error when you try to bind to the domain controller that will be removed. Ntdsutil has to bind to a domain controller other than the one that will be removed with metadata cleanup.

16. Type quit, and then press ENTER at each menu 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 will 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 DCs that exist to use the old cname record.

    As best practice, you should delete the host name 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.
18. 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 record in the _msdcs container. To do this, expand the **_msdcs** container, right-click **cname**, and then click **Delete**.

    Important If this is 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.
19. If the deleted computer is 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:
    1. Click **Start**, click **Run**, type adsiedit.msc, and then click **OK**
    2. Expand the **Domain NC** container.
    3. Expand **DC=Your Domain, DC=COM, PRI, LOCAL, NET**.
    4. Expand **CN=System**.
    5. Right-click the **Trust Domain** object, and then click **Delete**.
20. Use Active Directory Sites and Services to remove the domain controller. To do this, follow these steps:
    1. Start Active Directory Sites and Services.
    2. Expand **Sites**.
    3. Expand the server's site. The default site is Default-First-Site-Name.
    4. Expand **Server**.
    5. Right-click the domain controller, and then click **Delete**.
21. When you use DFS Replication in Windows Server 2008 and in later versions, the current version of Ntdsutil.exe does not clean up the DFS Replication object. In this case, you can use Adsiedit.msc to correct the DFS Replication objects for Active Directory Domain Services (AD DS) manually. To do this, follow these steps:

    1. Logon a domain controller as a domain administrator in the affected domain.
    2. Start Adsiedit.msc.
    3. Connect to the default naming context.
    4. Locate the following DFS Replication topology container:

       CN=Topology,CN=Domain System Volume,CN=DFSR-Globalsettings,CN=System,DC=Your Domain,DC=Domain Suffix

    5. Delete the msDFSR-Member CN object that has the old computer name.

Procedure 2: Windows 2000 (All versions) Windows Server 2003 RTM

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 you make the connection. To do this, 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 whether 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 System (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 you run the Dcpromo utility.

    Note You may also see this error when you try to bind to the domain controller that will be removed. Ntdsutil has to bind to a domain controller other than the one that will 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 will be reinstalled and re-promoted, a new NTDS Settings object is created by using 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.

Note You do not need to manually remove the FRS member object in Windows Server 2003 RTM because the Ntdsutil.exe utility has already removed the FRS member object when you run the utility. Additionaly, the metadata of the computer account cannot be removed if the computer account of the DC contains another leaf object. For example, Remote Installation Services (RIS) might be installed on the DC.

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:
    1. Click **Start**, click **Run**, type adsiedit.msc in the **Open** box, and then click **OK**.
    2. Expand the **Domain NC** container.
    3. Expand **DC=Your Domain Name, DC=COM, PRI, LOCAL, NET**.
    4. Expand **OU=Domain Controllers**.
    5. 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:
    1. Click **Start**, click **Run**, type adsiedit.msc in the **Open** box, and then click **OK**
    2. Expand the **Domain NC** container.
    3. Expand **DC=Your Domain, DC=COM, PRI, LOCAL, NET**.
    4. Expand **CN=System**.
    5. Expand **CN=File Replication Service**.
    6. Expand **CN=Domain System Volume (SYSVOL share)**.
    7. 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, right-click the domain name under Forward Lookup Zones, click **Properties**, and then remove this server from the Name Serverstab.

   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:
   1. Click **Start**, click **Run**, type adsiedit.msc in the **Open** box, and then click **OK**
   2. Expand the **Domain NC** container.
   3. Expand **DC=Your Domain, DC=COM, PRI, LOCAL, NET**.
   4. Expand **CN=System**.
   5. 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:
   1. Start Active Directory Sites and Services.
   2. Expand **Sites**.
   3. Expand the server's site. The default site is **Default-First-Site-Name**.
   4. Expand **Server**.
   5. Right-click the domain controller, and then click Delete.

Advanced optional syntax with the SP1 or later versions of Ntdsutil.exe

Windows Server 2003 SP1 introduced a new syntax that can be used. By using the new syntax, it is no longer required to bind to the DS and select your operation target. To use the new syntax, you must know or obtain the DN of the NTDS settings object of the server that is being demoted. To use the new syntax for metadata cleanup, follow these steps:

1. Run ntdsutil.
2. Switch to the metadata cleanup prompt.
3. Run the following command

   remove selected server <DN of the server object in the config container>

   An example of this command is as follows.

   Note The following is one line but has been wrapped.

   Remove selected server
   cn=servername,cn=servers,cn=sitename,cn=sites,cn=configuration,dc=<forest_root_domain>

4. Remove the cname record in the _msdcs.root domain of forest zone in DNS. Assuming that DC will be reinstalled and re-promoted, a new NTDS Settings object is created by using a new GUID and a matching cname record in DNS. You do not want the DCs that exist to use the old cname record.

   As best practice, you should delete the host name and other DNS records. If the lease time that remains on Dynamic Host Configuration Protocol (DHCP) address assigned to offline server is exceeded, another client can obtain the IP address of the problem DC.
5. 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:

1. Click **Start**, click **Run**, type adsiedit.msc, and then click **OK**.
2. Expand the **Domain NC** container.
3. Expand **DC=Your Domain Name, DC=COM, PRI, LOCAL, NET**.
4. Expand **CN=System**.
5. Right-click the **Trust Domain** object,, and then click **Delete**.

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

More Information

For more information about how to forcefully demote a Windows Server 2003 or Windows 2000 domain controller, click the following article number to view the article in the Microsoft Knowledge Base:

332199 Domain controllers do not demote gracefully when you use the Active Directory Installation Wizard to force demotion in Windows Server 2003 and in Windows 2000 Server

Determine the DN of the server

There are several ways to obtain the DN of the server object that is to be removed. The following example uses Ldp.exe. To obtain the DN by using Ldp.exe, follow these steps:

1. Run LDP.
2. Bind to rootDSE.
3. Select View\tree. Base DN should be cn=configuration,dc=rootdomain,dc=<suffix>.
4. Expand **Sites**.
5. Expand the site where the server object resides.
6. Expand **Servers**.
7. Expand the server that you are removing.
8. Look for a line on the right hand side that starts with DN.
9. Copy whole line excluding the DN.

    Example snip of the first part of the LDP spew:

```
Expanding base 'CN=DC1,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=corp,DC=com'...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn: CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=com”

What you would copy would be

"CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=corp,DC=com"
```

For more information, click the following article number to view the article in the Microsoft Knowledge Base:

887424 "DsRemoveDsDomainW error 0x2015" error message when you use Ntdsutil to try to remove metadata for a domain controller that was removed from your network in Windows Server 2003