Clean Up Server Metadata

This is the guide to use when a Domain Controller (DC) crashes and cannot be removed from the domain using normal DCPromo removal method.

Domain Controller Decommission

1. Use this first to clean up the metadata
2. Clean/Purge from Sites & Services
3. Clean/Purge from AD Users & Computers
4. Clean/Purge from DNS
5. Clean/Purge from ADSI (&(Name=RHSC-44-VSRV01*))
    1. ADSI purge

c:\>ntdsutil

ntdsutil:

ntdsutil: metadata cleanup

metadata cleanup: connections

server connections: connect to server <YourGoodServerHere>

server connections: q

metadata cleanup: select operation target

select operation target: list domains

Found 1 domain(s)

select operation target: Select domain 0 <or appropriate>

blah blah

select operation target: list sites

blah blah

select operation target: select site <site number>

blah blah

select operation target: list servers in site

Found 2 server(s)

0- probably old

1 - probably new

select operation target: select server <numberhere>

select operation target: q

metadata cleanup: remove selected server

Clean Up Server Metadata

Updated: November 1, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

Metadata cleanup is a required procedure after a forced removal of Active Directory Domain Services (AD DS). You perform metadata cleanup on a domain controller in the domain of the domain controller that you forcibly removed. Metadata cleanup removes data from AD DS that identifies a domain controller to the replication system. Metadata cleanup also removes File Replication Service (FRS) and Distributed File System (DFS) Replication connections and attempts to transfer or seize any operations master (also known as flexible single master operations or FSMO) roles that the retired domain controller holds.

You can clean up server metadata by using the following:

- Clean up server metadata by using GUI tools
- Clean up server metadata using the command line
- Clean up server metadata by using a script

Image not found or type unknown

Note

If you receive an “Access is denied” error when you use any of these methods to perform metadata cleanup, make sure that the computer object and the NTDS Settings object for the domain controller are not protected against accidental deletion. To verify this right-click the computer object or the NTDS Settings object, click Properties, click Object, and clear the Protect object from accidental deletion check box. In Active Directory Users and Computers, the Object tab of an object appears if you click View and then click Advanced Features.

Clean up server metadata by using GUI tools

When you use Remote Server Administration Tools (RSAT) or the Active Directory Users and Computers console (Dsa.msc) that is included with Windows Server 2008 or Windows Server 2008 R2 to delete a domain controller computer account from the Domain Controllers organizational unit (OU), the cleanup of server metadata is performed automatically. Previously, you had to perform a separate metadata cleanup procedure.

You can also use the Active Directory Sites and Services console (Dssite.msc) to delete a domain controller’s computer account, which also completes metadata cleanup automatically. However, Active Directory Sites and Services removes the metadata automatically only when you first delete the NTDS Settings object below the computer account in Dssite.msc.

As long as you are using the Windows Server 2008, Windows Server 2008 R2, or RSAT versions of Dsa.msc or Dssite.msc, you can clean up metadata automatically for domain controllers running earlier versions of Windows operating systems.

Membership in Domain Admins, or equivalent, is the minimum required to complete these procedures. Review details about using the appropriate accounts and group memberships at Local and Domain Default Groups (http://go.microsoft.com/fwlink/?LinkId=83477).

To clean up server metadata by using Active Directory Users and Computers

1. Open Active Directory Users and Computers: On the Start menu, point to Administrative Tools, and then click Active Directory Users and Computers.
2. If you have identified replication partners in preparation for this procedure and if you are not connected to a replication partner of the removed domain controller whose metadata you are cleaning up, right-click Active Directory Users and Computers <DomainControllerName>, and then click Change Domain Controller. Click the name of the domain controller from which you want to remove the metadata, and then click OK.
3. Expand the domain of the domain controller that was forcibly removed, and then click Domain Controllers.
4. In the details pane, right-click the computer object of the domain controller whose metadata you want to clean up, and then click Delete.
5. Metadata Cleanup in ADUC

Image not found or type unknown

5. In the Active Directory Domain Services dialog box, click Yes to confirm the computer object deletion.
6. In the Deleting Domain Controller dialog box, select This Domain Controller is permanently offline and can no longer be demoted using the Active Directory Domain Services Installation Wizard (DCPROMO), and then click Delete.
7. DC offline in AD Users and Computers
   7. If the domain controller is a global catalog server, in the Delete Domain Controller dialog box, click Yes to continue with the deletion.
   8. If the domain controller currently holds one or more operations master roles, click OK to move the role or roles to the domain controller that is shown. You cannot change this domain controller. If you want to move the role to a different domain controller, you must move the role after you complete the server metadata cleanup procedure.

To clean up server metadata by using Active Directory Sites and Services

1. Open Active Directory Sites and Services: On the Start menu, point to Administrative Tools, and then click Active Directory Sites and Services.
2. If you have identified replication partners in preparation for this procedure and if you are not connected to a replication partner of the removed domain controller whose metadata you are cleaning up, right-click Active Directory Users and Computers <DomainControllerName>, and then click Change Domain Controller. Click the name of the domain controller from which you want to remove the metadata, and then click OK.
3. Expand the site of the domain controller that was forcibly removed, expand Servers, expand the name of the domain controller, right-click the NTDS Settings object, and then click Delete.

Metadata Cleanup in AD Sites and Services
4. In the Active Directory Domain Services dialog box, click Yes to confirm the NTDS Settings deletion.
5. In the Deleting Domain Controller dialog box, select This Domain Controller is permanently offline and can no longer be demoted using the Active Directory Domain Services Installation Wizard (DCPROMO), and then click Delete.

DC offline in AD Users and Computers
6. If the domain controller is a global catalog server, in the Delete Domain Controller dialog box, click Yes to continue with the deletion.
7. If the domain controller currently holds one or more operations master roles, click OK to move the role or roles to the domain controller that is shown.
8. Right-click the domain controller that was forcibly removed, and then click Delete.

DC Deletion in AD Sites and Services
9. In the Active Directory Domain Services dialog box, click Yes to confirm the domain controller deletion.

Clean up server metadata using the command line

As an alternative, you can clean up metadata by using Ntdsutil.exe, a command-line tool that is installed automatically on all domain controllers and servers that have Active Directory Lightweight Directory Services (AD LDS) installed. Ntdsutil.exe is also available on computers that have RSAT installed.

To clean up server metadata by using Ntdsutil

1. Open a command prompt as an administrator: On the Start menu, right-click Command Prompt, and then click Run as administrator. If the User Account Control dialog box appears, provide Enterprise Admins credentials, if required, and then click Continue.
2. At the command prompt, type the following command, and then press ENTER:
   ntdsutil
3. At the ntdsutil: prompt, type the following command, and then press ENTER:
   metadata cleanup
4. At the metadata cleanup: prompt, type the following command, and then press ENTER:
   remove selected server <ServerName>
   Or
   remove selected server <ServerName1> on <ServerName2>

Value	Description
ntdsutil: metadata cleanup	Initiates removal of objects that refer to a decommissioned domain controller.
remove selected server	Removes objects for a specified, decommissioned domain controller from a specified server.
<ServerName> or <ServerName1>	The distinguished name of the domain controller whose metadata you want to remove, in the form cn=ServerName,cn=Servers,cn=SiteName,cn=Sites,cn=Configuration,dc=ForestRootDomain. If you specify only one server name, the objects are removed from the current domain controller.
on <ServerName2>	Specifies removing server metadata on <ServerName2>, the Domain Name System (DNS) name of the domain controller to which you want to connect. If you have identified replication partners in preparation for this procedure, specify a domain controller that is a replication partner of the removed domain controller.

5. In Server Remove Configuration Dialog, review the information and warning, and then click Yes to remove the server object and metadata.
   At this point, Ntdsutil confirms that the domain controller was removed successfully. If you receive an error message that indicates that the object cannot be found, the domain controller might have been removed earlier.
6. At the metadata cleanup: and ntdsutil: prompts, type quit, and then press ENTER.

7. To confirm removal of the domain controller:
   Open Active Directory Users and Computers. In the domain of the removed domain controller, click Domain Controllers. In the details pane, an object for the domain controller that you removed should not appear.
   Open Active Directory Sites and Services. Navigate to the Servers container and confirm that the server object for the domain controller that you removed does not contain an NTDS Settings object. If no child objects appear below the server object, you can delete the server object. If a child object appears, do not delete the server object because another application is using the object.

Clean up server metadata by using a script

Another option for cleaning up server metadata is to use a script. For information about using a script to clean up metadata, see Remove Active Directory Domain Controller Metadata (http://go.microsoft.com/fwlink/?LinkID=123599).

Machine generated alternative text:
News Windows
Virtualization
Cloud Computing Of
Dcpromo process will still find the old object and therefore w'll refuse to re-create the objects
In the event that the NTDS Settings object is not removed correctly you can use the Ntdsutil.ex
NTDS Settings object.
If you eve the new domain controller the same name as the failed computer, then you need p
to clean up metadata, which removes the NT DS Settings Object Of the failed domain controller
controller a different name, then you need to perform all three procedures: clean up
Object from the site, and remove the computer Object from the domain controllers container.
You will need the following tool: Ntdsutil.exe, Active Directory Sites and Services, Active Direct(
Also, make sure that you use an account that is a member of the Enterprise Admins universal
Caution: Using the Ntdsutil utility incorrectly may result in partial or complete loss of Active Di
To clean up metadata
1. At the command line, type Ntdsutil and press ENTER.
2 ntdsutil
2. At the Ntdsutil: prompt, type metadata cleanup and press Enter.
ntdsutil: metadata cleanup
2 metadata cleanu
3. At the metadata cleanup: prompt, type connections and press Enter.
metadata cleanup: connections
2 server connections
4. At the server connections: prompt, type connect to server gervername, where «serverna
(any functional domain controller in the same domain) from which you plan to clean up the
controller. Press Enter.
Machine generated alternative text:
News
server connections.
Windows

Virtualization
Cloud Computing
Of
Note: Windows Server 2003 Service Pack 1 eliminates the need for the above step.
Type qu 't and press Enter to return you to the metadata cleanup: prompt.
5.
server connections: q
2 metadata cl eanu
Type select operation target and press Enter.
6.
metadata cleanup: Select operation target
2 select operation target
Type list domains and press Enter. This lists all domains in the forest with a number associi
7.
1 select operation target: list domains
Found 1 domain(s)
Ø - DC—dpetri , DC—net
select o eration tar et
4
. Type select domain where is the number corresponding to the dorm
8
was located. Press Enter.
I select operation targe
Select domain
NO current site
Domain - DC.dpetri , DC.net
4
NO current server
NO current Naming Context
6 select 0 ration tar e t
Type list sites and press Enter.
9.
1 select operation target: List sites
Found 1 site(s)
Ø CN—Defoult-Fi rst-Site-Name , CN—Si tes , CN—Configuration, DC—dpetri , DC—net
4
select o ration tar et
Type select site where refers to the number of the site in which the
10.
member. Press Enter.
Machine generated alternative text:
News
4 No current server
No current Naming Context
6 select operation target
Windows
Virtualization

Cloud Computing
Of
11. Type list servers in site and press Enter. This will list all servers in that site with a correspon
I select operation target
List serwers in site
2 Found 2 server(s)
ø — CN—SERVER2øø , CN—Servers , CN—Sites , CN—Configuration, DC—dpetri ,
CN—SERVERIW , CN—Servers , CN—De fault-Fi r s , CN—Sites , CN—Confi on, DC—dpetri , DC:
5 select 0 ration tar et
12. Type select server qurnbep and press Enter, where c:numbep refers to the domain contr
1 select operation target: Select server
CN—Defou1 t -Fi rst-Si te-Name , CN—Si tes , CN—Configuration , DC—dpetri , DC—net
Domain - DC-dpetri DC-net
4 Server CN—SERVER2ØØ , CN—Servers , DC—dpetr
DSA object - CN—NTDS Settings,
DNS host name
server2ØØ. dpetri net
Computer object
CN-SERVER2ØØ , OU—Domain Control lers , DC—dpetri
8 No current Naming Context
g select o ration tar et
13. Type qu.t and press Enter. The Metadata cleanup menu is displayed.
I select operation target
2 metadata cleanu
14. Type remove selected server and press Enter.
You will receive a warning message. Read it, and if you agree, press Yes.
Machine generated alternative text:
News
metadata cleanup: Remove selected server
Windows
Virtualization
Cloud Computing
solarwtnds
Of
" CN—SERVER2Øø , CN—Servers , CN—Defaul t -F i rst-Si te- Name , CN—Si tes , CN—Configurati on
, DC—dpetri , DC—net
3 metadata cleanu
At this point, Active Directory confirms that the domain controller was removed successfully. If
object could not be found, Active Directory might have already removed from the domain conl
15. Type qu.t, and press Enter until you return to the command prompt.
To remove the failed server object from the sites
16. In Active Directory Sites and Services, expand the appropriate site.
17. Delete the server Object associated with the failed domain controller.
To remove the failed server object from the domain controllers container
18. In Active Directory Users and Computers, expand the domain controllers container.
19. Delete the computer object associated with the failed domain controller.
Machine generated alternative text:

News Windows
Virtualization
Cloud Computing Of
article, would you...) Select "This DC is permanently offline..."
and click on the Delete button
21. AD will display another confirmation window. If you're sure that you want to delete the failE
To remove the failed server object from DNS
22. In the DNS snap-in, expand the zone that is related to the domain from where the server h,
23. Remove the CNAME record in the msdcs.root domain of forest zone in DNS. You should al
other DNS records.
24. If you have reverse lookup zones, also remove the server from these zones.
Other considerations
Also, consider the following:
• If the removed domain controller was a global catalog server, evaluate whether application
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 catalo
address site, the domain, or the forest global catalog load.
• If the removed DC was a Flexible Single Master Operation (FSMO) role holder, relocate thos
• If the removed DC was a DNS server, update the DNS client configuration on all member w
and other DCs that might have used this DNS server for name resolution. If it is required,
the removal of the DNS server.

Revision #1
Created 23 December 2023 00:10:26 by ColtM
Updated 13 June 2024 01:28:01 by ColtM