How to Remove (Demote) a Domain Controller in Active Directory

https://woshub.com/remove-domain-controller-active-directory/

Removing an Active Directory Domain Controller and ADDS Role (Step-by-Step)

If you are going to decommission one of your AD domain controllers (common DC or read-only domain controller – RODC), you have to take some preparatory steps before demoting your domain controller to a member server and removing the Active Directory Domain Services (ADDS) role.

1. Check the state of your domain controller, Active Directory, and replication. There is a separate article on how to check a domain controller's health and replication in AD using `dcdiag`, `repadmin`, and PowerShell scripts. Fix the issues if found. To display a list of errors on a specific domain controller, run the following command: `dcdiag.exe /s:mun-dc03 /q`
2. Make sure that the AD FSMO roles are not running on the domain controller: `netdom query fsmo` Image not found or type unknown check fsmo role owners in actove directory If needed, move the FSMO roles to another DC.
3. Make sure that the DHCP server role is not running on the domain controller. If it is, migrate it to another server;
4. Change DNS settings for the DHCP scopes that are assigning IP addresses to the clients. Change the configuration of the DHCP scopes so that they assign a different DNS server address (wait for the IP lease time to expire so that all clients get new DNS server settings). You can display a list of DNS servers set for all zones (*DNS Servers Option 006*) on a server using the following PowerShell command (learn more about how to manage

DHCP in Windows Server using PowerShell): `Get-DhcpServerv4Scope -ComputerName mun-dhcp.woshub.com| Get-DhcpServerv4OptionValue | Where-Object {$_.OptionID -like 6} | FT Value`

5. Some clients may be manually set to use a DNS server on the DC (network devices, servers, printers, scanners, etc.). You need to find such devices and reconfigure them to another DNS server. It is easier to find such devices accessing your DNS server by its logs.

   Here is a detailed article: How to Audit Client DNS Queries in Windows Server;
6. If a Certificate Authority role is running on the domain controller, migrate it to another server;
7. If other services (like a KMS server, Radius/NPS, WSUS, etc.) are running on the domain controller, decide whether you want to move them to other hosts;
8. Use the `Test-ADDSDomainControllerUninstallation` cmdlet to make sure if there are any dependencies or issues you may come across when removing a DC. If the cmdlet returns *Success*, you may move on. Test-ADDSDomainControllerUninstallation

You are now ready to demote the domain controller to a member server. Prior to Windows Server 201, the **dcpromo** command was used for this. In modern Windows Server editions, this tool is deprecated and is not recommended to be used.

You can demote your domain controller using the **Server Manager**. Open Server Manager -> Remote Roles and Features -> uncheck **Active Directory Domain Services** in the Server Roles section.

Removing Active Directory Domain Services using Server Manager

Click **Demote this domain controller**.

Demote this domain controller

The Active Directory Domain Services Configuration Wizard appears. **Force the removal of this domain controller** option is used to remove the last domain controller in adomain. **Do not** use it. Later we will delete all DC metadata manually.

In the next screen, check the **Proceed with removal** option.

Force the removal of the Active Directory domain controller

Then set the local server administrator password.

Set local admin password on a demoted DC

Then you just need to click **Demote**.

uninstall domain controller role on windows server

Wait till the domain controller demotion is over. The following message will appear: **Successfully demoted the Active Directory Domain Controller**.

Image not found or type unknown
Successfully demoted the Active Directory Domain Controller

Restart your Windows Server host. Open the Server Manager again to remove the Active Directory Domain Services role.

Image not found or type unknown

When removing the ADDS role, the following components will be removed by default:

- Active Directory Module for Windows PowerShell
- AD DS and AD LDS Tools feature
- Active Directory Administrative Center
- AD DS Snap-ins and Command-line Tools
- DNS Server
- Group Policy Management Console (`gpmc.msc`)

Run the Active Directory Users and Computers console (dsa.msc) and make sure that the domain controller computer account has been removed from the Domain Controllers OU.

You can also uninstall a domain controller using the `Uninstall-ADDSDomainController` PowerShell cmdlet. The command will prompt you to set a local administrator password and confirm the DC demotion.

After the restart, you will just remove the ADDS role using PowerShell:

```
Uninstall-WindowsFeature AD-Domain-Services -IncludeManagementTools
```

Then open the Active Directory Sites and Services (`dssite.msc`) console, find the domain controller site, and its account in the Servers section. Expand the DC, right-click the NTDS Settings, and select **Delete**.

Image not found or type unknown
Delete domain controller account in Active Directory Sites and Services snap-in

Confirm the DC removal by checking **Delete This Domain controller anyway. It is permanently offline and can no longer be removed using the removal wizard**.

Image not found or type unknown
Delete This Domain controller anyway. It is permanently offline and can no longer be removed using

Then delete the server account.

Wait till the AD replication is over and check the domain state using `dcdiag` and `repadmin` commands (described above).

How to Remove a Failed Domain Controller in Active Directory?

If your domain controller has failed (physical server or virtual DC files on storage) and you are not going to restore the DC from the domain controller backup created earlier, you can force delete it.

Important. A domain controller removed in this way should never be brought online.
In Windows Server 2008 R2 or earlier, the `ntdsutil` tool was used to remove a failed domain controller and clear its metadata from AD. In the current Windows Server 2022/2019/2016/2012, you can delete the failed DC and clear its metadata correctly using graphic AD management MMC snap-ins.

Open the ADUC console (`dsa.msc`) and navigate to the **Domain Controllers**. Find your DC account and delete it.

delete domain controller computer account manually

A window to confirm deleting the domain controller appears. Check **Delete this Domain Controller anyway**. Click **Delete**.

confirm domain controller account removal

Active Directory will automatically clear the metadata of the removed DC from the ntds.dit database.

Then delete the domain controller in the AD Sites and Services console as shown above.

And the last step is to remove the domain controller records from the DNS. Open the DNS Manager (`dnsmgmt.msc`).

Remove the server from the Name Servers list in the zone settings.

Removing domain controller records in DNS

Remove static Name Servers (NS) records related to the deleted DC in your DNS zone and `_msdcs`, `_sites`, `_tcp`, `_udp` sections, as well as PTR records in the reverse lookup zone.

Delete Name Server (NS) records of a domain controller

Or use PowerShell to find and remove records in DNS.

Here is a step-by-step guide showing how to uninstall a domain controller or delete a failed DC from Active Directory.

Revision #1
Created 5 January 2024 05:45:49 by ColtM
Updated 7 August 2024 23:24:38 by ColtM