Step-by-step guide to Install an Additional Domain Controller by Using IFM

Teacher's copy

3 Votes

You can create an additional domain controller in a domain by installing Active Directory Domain Services (AD DS) on a server computer. When you are placing the additional domain controller in a remote site, you can install AD DS on the server either before or after you ship it to the remote site, as follows:

- Ship the computer as a workgroup computer, and install AD DS on it in the remote site. If you do not have administrative support in the remote site, enable Remote Desktop on the computer before you ship the computer so that you can perform the installation remotely. In the remote site, you can either:
    - Install AD DS from installation media that has been shipped to the site on removable media.
    - Install AD DS over the network.
- Install AD DS on the server in a hub or staging site, and then ship the installed domain controller to the remote site.

What is tool used to create media (IFM) for an additional domain controller?

- Windows Server 2008 and Windows Server 2008 R2 include an improved version of the Ntdsutil tool that you can use to create installation media for an additional domain controller. You can use **Ntdsutil.exe** to create installation media for additional domain controllers that you are creating in a domain. The IFM method uses the data in the installation media to install AD DS, which eliminates the need to replicate every object from a partner domain controller.

Note:

- Objects that were modified, added, or deleted since the installation media was created must be replicated. If the installation media was created recently, the amount of replication that is required is considerably less than the amount of replication that is required for a regular AD DS installation.

Advantages of using IFM to install a domain controller in a remote site:

- *You can reduce the replication traffic that is initiated during the installation of an additional domain controller in an Active Directory domain. Reducing the replication traffic reduces the time that is necessary to install the additional domain controller.*
- You can install many domain controllers from a single source of installation media.
- You do not have to disconnect a functioning domain controller from the replication topology. Therefore, you can avoid the disadvantages that are associated with a domain controller that does not replicate.
- You can avoid having to either replicate the entire Active Directory replica over a wide area network (WAN) link or disconnect an existing domain controller while it is being shipped to the remote site.
- If you enable Remote Desktop on the server before you ship it, you do not have to employ an administrator with Domain Admins credentials in the remote site. You can also use Remote Server Administration Tools (RSAT) to manage AD DS remotely.

IFM has the following requirements:

- You cannot use IFM to create the first domain controller in a domain. A Windows Server 2008–based domain controller must be running in the domain before you can perform IFM installations.
- The media that you use to create additional domain controllers must be taken from a domain controller in the same domain as the domain of the new domain controller.
- If the domain controller that you are creating is to be a global catalog server, the media for the installation must be created on an existing global catalog server in the domain.
- To install a domain controller that is a Domain Name System (DNS) server, you must create the installation media on a domain controller that is a DNS server in the domain.
- To create installation media for a full (writable) domain controller, you must run the ntdsutil ifm command on a writable domain controller that is running Windows Server 2008 or Windows Server 2008 R2.
- To create installation media for a read-only domain controller (RODC), you can run the **ntdsutil ifm** command on either a writable domain controller or an RODC that runs Windows Server 2008 or Windows Server 2008 R2. For RODC installation media, Ntdsutil removes any cached secrets, such as passwords
- You can use a 32-bit domain controller to generate installation media for a 64-bit domain controller; the reverse is also true. The ability to mix processor types for IFM installations is new in Windows Server 2008 and Windows Server 2008 R2.
- The IFM process creates a temp database in the %TMP% folder. You need at least 110% of the size of the AD DS or AD LDS database free on the drive where the %TMP% folder is in order for the operation to succeed. You can redirect the %TMP% folder to another disk on the server in order to use more space.

Task requirements

The following tools are required to perform the procedures for this task:

- Ntdsutil.exe

- Dcpromo.exe
- Robocopy.exe
- Enable Remote Desktop on the **destination** server

To create installation media for IFM

1. click **Start**. In **Start Search**, type **Command Prompt**.
2. right-click **Command Prompt**, and then click **Run as administrator**
3. At the command prompt, type the following command, and then press ENTER:

Ntdsutil

4. At the ntdsutil prompt, type the following command, and then press ENTER:
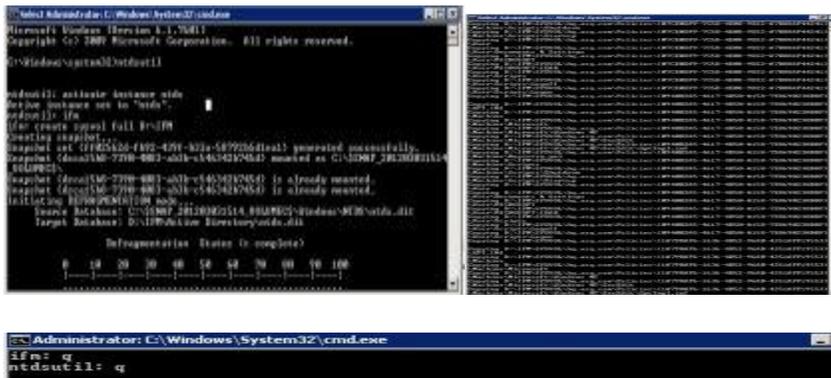
activate instance ntds

5. At   the ntdsutil prompt, type the following command, and then press ENTER:

ifm

6. At the ifm prompt, type the command for the type of installation media that you want to create, and then press ENTER. For example, to create installation media for a writable domain controller with SYSVOL, type the following command:

create sysvol full <Drive>:\<InstallationMediaFolder>

You can save the installation media to a network shared folder or to removable media. The IFM process creates a temp database in the %TMP% folder. You need at least 110% of the size of the AD DS or AD LDS database free on the drive where the %TMP% folder is in order for the operation to succeed. You can redirect the %TMP% folder to another disk on the server in order to use more space.

Important
*If you create installation media with SYSVOL, use **Robocopy.exe**to copy the installation media from where it is saved to the destination domain controller that you want to add to the domain.*

To copy the installation media with SYSVOL to a destination domain controller

1. click **Start**. In **Start   Search**, type **Command Prompt**.
2.   right-click **Command Prompt**, and   then click **Run as administrator**.
3. At the command prompt, type the   following command, and then press ENTER:

robocopy.exe /E /COPYALL \<source location\> \<destination location\>

Example:

robocopy.exe /E /COPYALL c:\InstallationMediaFolder \\RODC01\IFM

Important :
The next steps are required to   change the SYSVOL folder security settings. These steps change the file hash,   which will become the same file hash as in the IFM. If you use DFS   Replication, SYSVOL will keep the presided data only if the file hash on the   source domain controller and the destination server are the same

4. On the destination server, right-click the SYSVOL folder, and then click **Properties**.
5. Click the **Security** tab, and then click **Advanced**.
6. Click the **Auditing** tab, and then click **Edit**.
7. Clear the **Include inheritable auditing entries from this object's parent** check box, and then select it again.
8. Click **Apply**, and then click **OK**.

To install AD DS from IFM media by using the Windows interface:

1. Click **Start**, and then click Server Manager.
2. In Roles Summary, click Add Roles.
3. Review the information on the Before You Begin page, and then click Next.
4. On the Select Server Roles page, click Active Directory Domain Services, and then click Next.
5. Review the information on the Active Directory Domain Services page, and then click Next.
6. On the Confirm Installation Selections page, click Install.
7. On the Installation Results page, click Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
8. Select **Use advanced mode installation**.
9. Select the install from media option and provide the location of the installation media.
10. The **Source Domain Controller** page appears. Click **Let the wizard choose an appropriate domain controller** or click **Use this specific domain controller** to specify a domain controller that you want to provide as a source for replication to create the new domain controller, and then click **Next**. If you do not choose to install from media, all data will be replicated from this source domain controller.
11. After the installation operation completes successfully and the computer is restarted, remove the folder that contains the IFM media from the local disk.
12. On the Operating System Compatibility page, review the warning about the default security settings for Windows Server 2008 domain controllers, and then click Next.
13. Click Existing forest, click Add a domain controller to an existing domain, provide the user name and password for an account that can install the additional domain controller.
14. Select the domain of the new domain controller, and then click Next.
15. Select a site from the list or select the option to install the domain controller in the site that corresponds to its IP address, and then click Next.
16. Make the following selections, and then click Next.
17. type or browse to the volume and folder locations for the database file, the directory service log files, and the SYSVOL files, and then click Next.
18. On the Directory Services Restore Mode Administrator Password page, type and confirm the restore mode password, and then click Next. This password must be used to start AD DS in Directory Services Restore Mode (DSRM) for tasks that must be performed offline.
19. On the Summary page, review your selections. Click Back to change any selections, if necessary.
20. On the Completing the Active Directory Domain Services Installation Wizard page, click Finish.

21. You can select Reboot on completion to have the server restart automatically, or you can restart the server to complete the installation of AD DS when you are prompted to do so.