Prepare Active Directory for site publishing

09/22/2019 • 4 minutes to read •

In this article

Applies to: Configuration Manager (current branch)

When you extend the Active Directory schema for Configuration Manager, you introduce new structures to Active Directory that are used by Configuration Manager sites to publish key information in a secure location where clients can easily access it.

It's a good idea to use Configuration Manager with an extended Active Directory schema when you manage on-premises clients. An extended schema can simplify the process of deploying and setting up clients. An extended schema also lets clients efficiently locate resources like content servers and additional services that the different Configuration Manager site system roles provide.

- If you're not familiar with what extended schema provides for a Configuration Manager deployment, you can read about Schema extensions for Configuration Manager to help you make this decision.

- When you don't use an extended schema, you can set up other methods like DNS and WINS to locate services and site system servers. These methods of service location require additional configurations and are not the preferred method for service location by clients. To learn more, read Understand how clients find site resources and services for Configuration Manager,

- If your Active Directory schema was extended for Configuration Manager 2007 or System Center 2012 Configuration Manager, then you don't need to do more. The schema extensions are unchanged and will already be in place.

Extending the schema is a one-time action for any forest. To extend, and then use the extended Active Directory schema, follow these steps:

Step 1. Extend the schema

To extend the schema for Configuration Manager:

- Use an account that is a member of the Schema Admins security group.
- Be signed in to the schema master domain controller.
- Run the **Extadsch.exe** tool, or use the LDIFDE command-line utility with the **ConfigMgr_ad_schema.ldf** file. Both the tool and file are in the **SMSSETUP\BIN\X64** folder on the Configuration Manager installation media.

Option A: Use Extadsch.exe

1. Run **extadsch.exe** to add the new classes and attributes to the Active Directory schema.

   > **Tip**
   >
   > Run this tool from a command line to view feedback while it runs.

2. Verify that the schema extension was successful by reviewing extadsch.log in the root of the system drive.

Option B: Use the LDIF file

1. Edit the **ConfigMgr_ad_schema.ldf** file to define the Active Directory root domain that you want to extend:

   - Replace all instances of the text, **DC=x**, in the file with the full name of the domain to extend.
   - For example, if the full name of the domain to extend is named widgets.microsoft.com, change all instances of DC=x in the file to **DC=widgets, DC=microsoft, DC=com**.

2. Use the LDIFDE command-line utility to import the contents of the **ConfigMgr_ad_schema.ldf** file to Active Directory Domain Services:

   - For example, the following command line imports the schema extensions to Active Directory Domain Services, turns on verbose logging, and creates a log file during the import process: **ldifde -i -f ConfigMgr_ad_schema.ldf -v -j <location to store log file>**.

3. To verify that the schema extension was successful, review a log file created by the command line used in the previous step.

Step 2. Create the System Management container and grant sites permissions to the container

After you extend the schema, you must create a container named **System Management** in Active Directory Domain Services (AD DS):

- You create this container one time in each domain that has a primary or secondary site that will publish data to Active Directory.
- For each container, you grant permissions to the computer account of each primary and secondary site server that will publish data to that domain. Each account needs **Full Control** to the container with the advanced permission, **Apply onto**, equal to **This object and all descendant objects**.

To add the container

1. Use an account that has the **Create All Child Objects** permission on the **System** container in Active Directory Domain Services.
2. Run **ADSI Edit** (adsiedit.msc), and connect to the site server's domain.
3. Create the container:
   - Expand **Domain** <computer fully qualified domain name>, expand <distinguished name>, right-click **CN=System**, choose **New**, and then choose **Object**.
   - In the **Create Object** dialog box, choose **Container**, and then choose **Next**.
   - In the **Value** box, enter **System Management**, and then choose **Next**.
4. Assign permissions:

   ⓘ **Note**

> If you prefer, you can use other tools like the Active Directory Users and Computers administrative tool (dsa.msc) to add permissions to the container.

- Right-click **CN=System Management**, and then choose **Properties**.
- Choose the **Security** tab, choose **Add**, and then add the site server computer account with the **Full Control** permission.
- Choose **Advanced**, choose the site server's computer account, and then choose **Edit**.
- In the **Apply onto** list, choose **This object and all descendant objects**.

5. Choose **OK** to close the console and save the configuration.

Step 3. Set up sites to publish to Active Directory Domain Services

After the container is set up, permissions are granted, and you have installed a Configuration Manager primary site, you can set up that site to publish data to Active Directory.

For more about publishing, see Publish site data for Configuration Manager.

Is this page helpful?

Yes No