Replicating Directory Changes permission - Windows Server

By kaushika-msft

Archived: 2026-04-05 16:10:55 UTC

This article describes how to grant the "Replicating Directory Changes" permission for the Microsoft Metadirectory Services ADMA service account.

Original KB number: 303972

Summary

When discovering objects in Active Directory using the Active Directory management agent (ADMA), the account that is specified for connecting to Active Directory must either have Domain Administrative permissions, belong to the Domain Administrators group, or be explicitly granted Replicating Directory Changes permissions for every domain of the forest that this management agent accesses. This article describes how to explicitly a grant a user account the Replicating Directory Changes permissions on a domain.

Note

In Windows Server 2003, the name of this permission changed to "Replicate Directory Changes."

More information

The Replicating Directory Changes permission, known as the Replicate Directory Changes permission in Windows Server 2003, is an Access Control Entry (ACE) on each domain naming context. You can assign this permission by using the ACL editor or the Adsiedit support tool in Windows 2000.

Setting permissions by using the ACL editor

1. Open the **Active Directory Users and Computers** snap-in
2. On the **View** menu, click **Advanced Features**.
3. Right-click the domain object, such as "`company.com`", and then click **Properties**.
4. On the **Security** tab, if the desired user account is not listed, click **Add**; if the desired user account is listed, proceed to step 7.
5. In the **Select Users, Computers, or Groups** dialog box, select the desired user account, and then click **Add**.
6. Click **OK** to return to the **Properties** dialog box.
7. Click the desired user account.
8. Click to select the **Replicating Directory Changes** check box from the list.
9. Click **Apply**, and then click **OK**.
10. Close the snap-in.

Setting permissions by using Adsiedit

Warning

Using Adsiedit incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Adsiedit can be solved. Use Adsiedit at your own risk.

1. Install the Windows 2000 Support tools if they have not already been installed.
2. Run Adsiedit.msc as an administrator of the domain. Expand the Domain Naming Context (Domain NC) node. This node contains an object that begins with "DC=" and reflects the correct domain name. Right-click this object, and then click **Properties**.
3. Click the **Security** tab.
4. If the desired user account is not listed, click **Add**, otherwise proceed to step 8.
5. In the **Select Users, Computers, or Groups** dialog box, select the desired user account, and then click **Add**.
6. Click **OK** to return to the **Properties** dialog box.
7. Click **Apply**, and then click **OK**.
8. Select the desired user account
9. Click to select the **Replicating Directory Changes** check box.
10. Click **Apply**, and then click **OK**.
11. Close the snap-in.

Note

Using either method, setting the Replicating Directory Changes permission for each domain within your forest enables the discovery of objects in the domain within the Active Directory forest. However, enabling discovery of the connected directory does not imply that other operations can be performed.

To create, modify, and delete objects within Active Directory using a non-administrative account, you may need to add additional permissions as appropriate. For example, for Microsoft Metadirectory Services (MMS) to create new user objects in an Organizational Unit (OU) or container, the account that is being used must be explicitly granted the Create All Child Objects permission, as the Replicating Directory Changes permission is not sufficient to allow the creation of objects.

In a similar fashion, the deletion of objects requires the Delete All Child Objects permission.

It is possible that there are limitations on other operations, such as attribute flow, depending on the specific security settings that are assigned to the object in question, and whether or not inheritance is a factor.
