

Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller

This article was previously published under Q255504

Article ID	: 255504
Last Review	: October 31, 2006
Revision	: 7.1

On This Page

[SUMMARY](#)

[MORE INFORMATION](#)

[Transfer FSMO roles](#)

[Seize FSMO roles](#)

SUMMARY

This article describes how to use the Ntdsutil.exe utility to transfer or to seize Flexible Single Master Operations (FSMO) roles.

MORE INFORMATION

Certain domain and enterprise-wide operations that are not good for multi-master updates are performed by a single domain controller in an Active Directory domain or forest. The domain controllers that are assigned to perform these unique operations are called operations masters or FSMO role holders.

The following list describes the 5 unique FSMO roles in an Active Directory forest and the dependent operations that they perform:

- Schema master - The Schema master role is forest-wide and there is one for each forest. This role is required to extend the schema of an Active Directory forest or to run the **adprep /domainprep** command.
- Domain naming master - The Domain naming master role is forest-wide and there is one for each forest. This role is required to add or remove domains or application partitions to or from a forest.
- RID master - The RID master role is domain-wide and there is one for each domain. This role is required to allocate the RID pool so that new or existing domain controllers can create user accounts, computer accounts or security groups.
- PDC emulator - The PDC emulator role is domain-wide and there is one for each domain. This role is required for the domain controller that sends database updates to Windows NT backup domain controllers. The domain controller that owns this role is also targeted by certain administration tools and updates to user account and computer account passwords.
- Infrastructure master - The Infrastructure master role is domain-wide and there is one for each domain. This role is required for domain controllers to run the **adprep /forestprep** command successfully and to update SID attributes and distinguished name attributes for objects that are referenced across domains.

The Active Directory Installation Wizard (Dcpromo.exe) assigns all 5 FSMO roles to the first domain controller in the forest root domain. The first domain controller in each new child or tree domain is assigned the three domain-wide roles. Domain controllers continue to own FSMO roles until they are reassigned by using one of the following methods:

- An administrator reassigns the role by using a GUI administrative tool.
- An administrator reassigns the role by using the **ntdsutil /roles** command.
- An administrator gracefully demotes a role-holding domain controller by using the Active Directory Installation Wizard. This wizard reassigns any locally-held roles to an existing domain controller in the forest. Demotions that are performed by using the **dcpromo /forceremoval** command leave FSMO roles in an invalid state until they are reassigned by an administrator.

We recommend that you transfer FSMO roles in the following scenarios:

- The current role holder is operational and can be accessed on the network by the new FSMO owner.
- You are gracefully demoting a domain controller that currently owns FSMO roles that you want to assign to a specific domain controller in your Active Directory forest.
- The domain controller that currently owns FSMO roles is being taken offline for scheduled maintenance and you need specific FSMO roles to be assigned to a "live" domain controller. This may be required to perform operations that connect to the FSMO owner. This would be especially true for the PDC Emulator role but less true for the RID master role, the Domain naming master role and the Schema master roles.

We recommend that you seize FSMO roles in the following scenarios:

- The current role holder is experiencing an operational error that prevents an FSMO-dependent

operation from completing successfully and that role cannot be transferred.

- A domain controller that owns an FSMO role is force-demoted by using the **dcpromo /forceremoval** command.
- The operating system on the computer that originally owned a specific role no longer exists or has been reinstalled.

As replication occurs, non-FSMO domain controllers in the domain or forest gain full knowledge of changes that are made by FSMO-holding domain controllers. If you must transfer a role, the best candidate domain controller is one that is in the appropriate domain that last inbound-replicated, or recently inbound-replicated a writable copy of the "FSMO partition" from the existing role holder. For example, the Schema master role-holder has a distinguished name path of CN=schema,CN=configuration,dc=<forest root domain>, and this means that roles reside in and are replicated as part of the CN=schema partition. If the domain controller that holds the Schema master role experiences a hardware or software failure, a good candidate role-holder would be a domain controller in the root domain and in the same Active Directory site as the current owner. Domain controllers in the same Active Directory site perform inbound replication every 5 minutes or 15 seconds.

The partition for each FSMO role is in the following list:

FSMO role	Partition
Schema	CN=Schema,CN=configuration,DC=<forest root domain>
Domain Naming Master	CN=configuration,DC=<forest root domain>
PDC	DC=<domain>
RID	DC=<domain>
Infrastructure	DC=<domain>

A domain controller whose FSMO roles have been seized should not be permitted to communicate with existing domain controllers in the forest. In this scenario, you should either format the hard disk and reinstall the operating system on such domain controllers or forcibly demote such domain controllers on a private network and then remove their metadata on a surviving domain controller in the forest by using the **ntdsutil /metadata cleanup** command. The risk of introducing a former FSMO role holder whose role has been seized into the forest is that the original role holder may continue to operate as before until it inbound-replicates knowledge of the role seizure. Known risks of two domain controllers owning the same FSMO roles include creating security principals that have overlapping RID pools, and other problems.

Transfer FSMO roles

To transfer the FSMO roles by using the Ntdsutil utility, follow these steps:

1. Log on to a Windows 2000 Server-based or Windows Server 2003-based member computer or domain controller that is located in the forest where FSMO roles are being transferred. We recommend that you log on to the domain controller that you are assigning FSMO roles to. The logged-on user should be a member of the Enterprise Administrators group to transfer Schema master or Domain naming master roles, or a member of the Domain Administrators group of the domain where the PDC emulator, RID master and the Infrastructure master roles are being transferred.
2. Click **Start**, click **Run**, type **ntdsutil** in the **Open** box, and then click **OK**.
3. Type **roles**, and then press ENTER.

Note To see a list of available commands at any one of the prompts in the Ntdsutil utility, type **?**, and then press ENTER.

4. Type **connections**, and then press ENTER.
5. Type **connect to server *servername***, and then press ENTER, where *servername* is the name of the domain controller you want to assign the FSMO role to.
6. At the **server connections** prompt, type **q**, and then press ENTER.
7. Type **transfer *role***, where *role* is the role that you want to transfer. For a list of roles that you can transfer, type **?** at the **fsmo maintenance** prompt, and then press ENTER, or see the list of roles at the start of this article. For example, to transfer the RID master role, type **transfer rid master**. The one exception is for the PDC emulator role, whose syntax is **transfer pdc**, not **transfer pdc emulator**.
8. At the **fsmo maintenance** prompt, type **q**, and then press ENTER to gain access to the **ntdsutil** prompt. Type **q**, and then press ENTER to quit the Ntdsutil utility.

Seize FSMO roles

To seize the FSMO roles by using the Ntdsutil utility, follow these steps:

1. Log on to a Windows 2000 Server-based or Windows Server 2003-based member computer or domain controller that is located in the forest where FSMO roles are being seized. We recommend that you log on to the domain controller that you are assigning FSMO roles to. The logged-on user should be a member of the Enterprise Administrators group to transfer schema or domain naming master roles, or a member of the Domain Administrators group of the domain where the PDC emulator, RID master and the Infrastructure master roles are being transferred.
2. Click **Start**, click **Run**, type **ntdsutil** in the **Open** box, and then click **OK**.
3. Type **roles**, and then press ENTER.
4. Type **connections**, and then press ENTER.
5. Type **connect to server *servername***, and then press ENTER, where *servername* is the name of the domain controller that you want to assign the FSMO role to.
6. At the **server connections** prompt, type **q**, and then press ENTER.
7. Type **seize *role***, where *role* is the role that you want to seize. For a list of roles that you can seize, type **?** at the **fsmo maintenance** prompt, and then press ENTER, or see the list of roles at the start of this article. For example, to seize the RID master role, type **seize rid master**. The one exception is for the PDC emulator role, whose syntax is **seize pdc**, not **seize pdc emulator**.
8. At the **fsmo maintenance** prompt, type **q**, and then press ENTER to gain access to the **ntdsutil** prompt. Type **q**, and then press ENTER to quit the Ntdsutil utility.

Notes

- Under typical conditions, all five roles must be assigned to "live" domain controllers in the forest. If a domain controller that owns a FSMO role is taken out of service before its roles are transferred, you must seize all roles to an appropriate and healthy domain controller. We recommend that you only seize all roles when the other domain controller is not returning to the domain. If it is possible, fix the broken domain controller that is assigned the FSMO roles. You should determine which roles are to be on which remaining domain controllers so that all five roles are assigned to a single domain controller. For more information about FSMO role placement, click the following article number to view the article in the Microsoft Knowledge Base:
[223346](http://support.microsoft.com/kb/223346/) (<http://support.microsoft.com/kb/223346/>) FSMO placement and optimization on Windows 2000 domain controllers
- If the domain controller that formerly held any FSMO role is not present in the domain and if it has had its roles seized by using the steps in this article, remove it from the Active Directory by following the procedure that is outlined in the following Microsoft Knowledge Base article:
[216498](http://support.microsoft.com/kb/216498/) (<http://support.microsoft.com/kb/216498/>) How to remove data in active directory after an unsuccessful domain controller demotion
- Removing domain controller metadata with the Windows 2000 version or the Windows Server 2003 build 3790 version of the **ntdsutil /metadata cleanup** command does not relocate FSMO roles that are assigned to live domain controllers. The Windows Server 2003 Service Pack 1 (SP1) version of the Ntdsutil utility automates this task and removes additional elements of domain controller metadata.
- Some customers prefer not to restore system state backups of FSMO role-holders in case the role has been reassigned since the backup was made.
- Do not put the Infrastructure master role on the same domain controller as the global catalog server. If the Infrastructure master runs on a global catalog server it stops updating object information because it does not contain any references to objects that it does not hold. This is because a global catalog server holds a partial replica of every object in the forest.

To test whether a domain controller is also a global catalog server:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Sites and Services**.
2. Double-click **Sites** in the left pane, and then locate the appropriate site or click **Default-first-site-name** if no other sites are available.
3. Open the Servers folder, and then click the domain controller.
4. In the domain controller's folder, double-click **NTDS Settings**.
5. On the **Action** menu, click **Properties**.
6. On the **General** tab, view the **Global Catalog** check box to see if it is selected.

For more information about FSMO roles, click the following article numbers to view the articles in the Microsoft Knowledge Base:

[197132](http://support.microsoft.com/kb/197132/) (http://support.microsoft.com/kb/197132/) Windows 2000 Active Directory FSMO roles

[223787](http://support.microsoft.com/kb/223787/) (http://support.microsoft.com/kb/223787/) Flexible Single Master Operation transfer and seizure process

APPLIES TO

- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

Keywords: kbhowto KB255504

©2007 Microsoft Corporation. Tutti i diritti sono riservati.