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

On This Page

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

Back to the top

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

Использование средства Ntdsutil.exe для получения и передачи ролей FSMO контроллеру домена

На этой странице

В статье приведены указания по получению и передаче ролей FSMO (Flexible Single Master Operations) с помощью средства Ntdsutil.exe.

Перейти к началу страницы

Дополнительная информация

Некоторые операции уровня домена или предприятия, для которых не может выполняться обновление с несколькими хозяевами, выполняются одним контроллером домена в рамках домена или леса Active Directory. Контроллеры домена, назначенные для выполнения таких особых операций, называются хозяевами операций или обладателями ролей FSMO.
Ниже перечислены 5 особых ролей FSMO, существующих в лесу Active Directory, и специальные операции, выполняемые обладателями этих ролей.

- Хозяин схемы. Роль хозяина схемы — это роль уровня леса. В каждом лесу существует один хозяин схемы. Эта роль необходима для расширения схемы леса Active Directory или для выполнения команды **adprep /domainprep**.
- Хозяин именования домена. Роль хозяина именования домена — это роль уровня леса. В каждом лесу существует один хозяин именования домена. Эта роль необходима для добавления или удаления доменов или разделов приложений в лесу.

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

- Хозяин RID. Роль хозяина RID — это роль уровня домена. В каждом домене существует один хозяин RID. Эта роль необходима для выделения идентификаторов RID, которые необходимы новым или существующим контроллерам доменов учетных записей пользователей, учетных записей компьютеров, а также групп безопасности.
- Эмулятор PDC. Роль эмулятора PDC — это роль уровня домена. В каждом домене существует один эмулятор PDC. Эта роль необходима для контроллера домена, отправляющего обновления базы данных резервным контроллерам домена Windows NT. Контроллер домена, владеющий этой ролью, также используется некоторыми средствами администрирования и получает обновления паролей учетных записей пользователей и компьютеров.
- Хозяин инфраструктуры. Роль хозяина инфраструктуры — это роль уровня домена. В каждом домене существует один хозяин инфраструктуры. Эта роль необходима контроллерам доменов для успешного выполнения команды **adprep /forestprep**, а также для обновления атрибутов идентификаторов безопасности (SID) и различающихся атрибутов имен для объектов, на которые указывают междоменные ссылки.

Мастер установки Active Directory (Dcpromo.exe) назначает все 5 ролей FSMO первому контроллеру домена в корневом домене леса. При создании дочерних доменов 3 роли уровня домена назначаются первому контроллеру домена в каждом дочернем домене. Контроллеры домена владеют ролями FSMO, пока эти роли не будут переданы другим контроллерам доменов одним из следующих методов.

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

- Администратор переназначает роль с помощью средства администрирования с графическим интерфейсом.
- Администратор переназначает роль, выполняя команду **ntdsutil /roles**.
- Администратор в штатном порядке понижает роль контроллера домена, являющегося хранителем роли, с помощью мастера установки Active Directory. При этом роли, которыми обладал текущий контроллер домена, мастер переназначает существующим контроллерам домена в лесу. Если для понижения роли контроллера домена использовалась команда **dcpromo /forceremoval**, то роли FSMO будут находиться в недопустимом состоянии, пока администратор не выполнит переназначение ролей вручную.

Корпорация Майкрософт рекомендует использовать передачу ролей FSMO в следующих случаях.

- Текущий обладатель роли работает надлежащим образом и доступен по сети новому обладателю роли FSMO.
- Администратор в штатном порядке понижает роль контроллера домена, являющегося обладателем ролей FSMO, которые следует назначить определенному контроллеру домена в лесу Active Directory.
- Контроллер домена, являющийся обладателем ролей FSMO, необходимо отключить для выполнения профилактических работ, а его роли должны быть назначены работающему контроллеру домена. Это может потребоваться для выполнения операций, относящихся к данному владельцу ролей FSMO. Это особенно

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 mean 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-

необходимо при отключении эмулятора PDC. Временное отключение хозяина RID, хозяина именования домена и хозяина схемы в меньшей степени сказывается на работе.

Корпорация Майкрософт рекомендует использовать получение ролей FSMO в следующих случаях.

- В работе текущего обладателя роли FSMO возникли сбои, которые препятствуют успешному выполнению функций, присущих данной роли, и не дают выполнить передачу роли.
- Роль контроллера домена, являвшегося обладателем роли FSMO, была принудительно понижена с помощью команды **dcpromo /forceremoval**.
- На компьютере, являвшемся обладателем роли FSMO, переустановлена или не загружается операционная система.

В процессе репликации сведения об изменениях, выполненных обладателями ролей FSMO, передаются всем не являющимся обладателями ролей FSMO контроллерам домена в лесу или в домене. При выборе контроллера домена, которому следует передать роль FSMO, рекомендуется выбирать контроллер, который расположен в соответствующем домене и последним (или в числе последних) выполнил входящую репликацию доступной для записи копии «раздела FSMO» с текущим обладателем данной роли. Например, хозяин схемы имеет различающееся имя пути CN=schema,CN=configuration,dc=<корневой_домен_леса>. Это означает, что роли хранятся и реплицируются в составе раздела CN=schema. Если на контроллере домена, являющемся хозяином схемы, возникает программный или аппаратный сбой, рекомендуется назначить эту роль контроллеру

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.

Back to the top

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**

домена, расположенному в том же корневом домене и в том же узле Active Directory, что и исходный хозяин схемы. Контроллеры домена, находящиеся в пределах одного узла Active Directory, выполняют входящую репликацию каждые 5 минут или 15 секунд.

Ниже перечислены разделы, используемые ролями FSMO.

Роль FSMO	Раздел
Схема	CN=Schema,CN=configuration,DC=<корневой_домен_леса>
Хозяин именования домена	CN=configuration,DC=<корневой_домен_леса>
Эмулятор PDC	DC=<домен>
Хозяин RID	DC=<домен>
Хозяин инфраструктуры	DC=<домен>

После получения роли FSMO контроллер домена, ранее являвшийся обладателем этой роли, не должен обмениваться данными с другими контроллерами домена в лесу. На таком контроллере домена необходимо отформатировать жесткий диск и переустановить операционную систему или принудительно понизить роль данного контроллера домена в изолированной сети и удалить метаданные этого контроллера домена с других контроллеров домена в лесу с помощью команды **ntdsutil /metadata cleanup**. Включение в сеть обладателя роли FSMO, роль которого была получена другим компьютером, может привести к тому, что до получения сведений о получении роли при входящей репликации данный контроллер домена продолжит функционировать в качестве хозяина операций. Наличие двух компьютеров, исполняющих одну роль FSMO, может привести к созданию участников безопасности, обладающих перекрывающимися пулами идентификаторов RID, а также к возникновению других проблем.

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.

Back to the top

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.

Перейти к началу страницы

Передача ролей FSMO

Для передачи ролей FSMO с помощью средства Ntdsutil выполните следующие действия.

1. Войдите в систему на рядовом сервере или контроллере домена под управлением Windows 2000 Server или Windows Server 2003, расположенном в том лесу, в котором следует выполнить передачу ролей FSMO. Рекомендуется войти в систему на контроллере домена, которому назначаются роли FSMO. Для передачи роли хозяина схемы или хозяина именования домена необходимо войти в систему с учетной записью, являющейся членом группы «Администраторы предприятия». Для передачи роли эмулятора PDC, хозяина RID или хозяина инфраструктуры необходимо войти в систему с учетной записью, являющейся членом группы «Администраторы домена».
2. Нажмите кнопку **Пуск**, выберите пункт **Выполнить**, введите в поле **Открыть** команду **ntdsutil** и нажмите кнопку **OK**.
3. Введите строку **roles** и нажмите клавишу ВВОД.

   Примечание.. На любом этапе использования средства Ntdsutil для просмотра доступных команд следует ввести символ **?** и нажать клавишу ВВОД.
4. Введите строку **connections** и нажмите клавишу ВВОД.
5. Введите команду **connect to server *имя_сервера*** и нажмите клавишу ВВОД. *Имя_сервера* — это имя контроллера домена, которому назначается роль FSMO.
6. В ответ на приглашение **server connections** введите **q** и нажмите

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 FSMO placement and optimization on Windows 2000 domain controllers

- If the domain controller that formerly held any FSMO role is not

клавишу ВВОД.

7. Введите команду **transfer *роль***, где *роль* — роль, которую требуется передать. Чтобы определить роли, которые могут быть переданы, ознакомьтесь со списком ролей в начале данной статьи или введите команду **?** после появления запроса **fsmo maintenance** и нажмите клавишу ВВОД. Например, для передачи роли хозяина RID введите команду **transfer rid master**. Единственным исключением является передача роли эмулятора PDC — для передачи данной роли необходимо использовать команду **transfer pdc** (а не **transfer pdc emulator**).
8. После появления запроса **fsmo maintenance** введите **q** и нажмите клавишу ВВОД, чтобы вернуться в обычный режим средства **ntdsutil**. Для завершения работы средства Ntdsutil введите команду **q** и нажмите клавишу ВВОД.

Перейти к началу страницы

Получение ролей FSMO

Для получения ролей FSMO с помощью средства Ntdsutil выполните следующие действия.

1. Войдите в систему на рядовом сервере или контроллере домена под управлением Windows 2000 Server или Windows Server 2003, расположенном в том лесу, в котором следует выполнить получение ролей FSMO. Рекомендуется войти в систему на контроллере домена, которому назначаются роли FSMO. Для получения роли хозяина схемы или хозяина именования домена необходимо войти в систему с учетной записью, являющейся членом группы «Администраторы предприятия». Для получения роли эмулятора

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 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**.

PDC, хозяина RID или хозяина инфраструктуры необходимо войти в систему с учетной записью, являющейся членом группы «Администраторы домена».

2. Нажмите кнопку **Пуск**, выберите пункт **Выполнить**, введите в поле **Открыть** команду **ntdsutil** и нажмите кнопку **OK**.
3. Введите строку **roles** и нажмите клавишу ВВОД.
4. Введите строку **connections** и нажмите клавишу ВВОД.
5. Введите команду **connect to server *имя_сервера*** и нажмите клавишу ВВОД. *Имя_сервера* — это имя контроллера домена, которому назначается роль FSMO.
6. В ответ на приглашение **server connections** введите **q** и нажмите клавишу ВВОД.
7. Введите команду **seize *роль***, где *роль* — роль, которую требуется получить. Чтобы определить роли, которые могут быть получены, ознакомьтесь со списком ролей в начале данной статьи или введите команду **?** после появления запроса **fsmo maintenance** и нажмите клавишу ВВОД. Например, для получения роли хозяина RID введите команду **seize rid master**. Единственным исключением является получение роли эмулятора PDC — для получения данной роли необходимо использовать команду **seize pdc** (а не **seize pdc emulator**).
8. После появления запроса **fsmo maintenance** введите **q** и нажмите клавишу ВВОД, чтобы вернуться в обычный режим средства **ntdsutil**. Для завершения работы средства Ntdsutil введите команду **q** и нажмите клавишу ВВОД.

Примечания

- В обычной ситуации все пять ролей должны быть назначены действующим контроллерам домена в лесу. Если контроллер

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.

домена, которому назначены роли FSMO, отключается до передачи ролей, необходимо выполнить получение этих ролей и назначить их работающим контроллерам домена. Корпорация Майкрософт рекомендует выполнять получение ролей только в тех случаях, когда исходный обладатель ролей больше не будет работать в домене. Если возможно, восстановите работоспособность вышедшего из строя контроллера домена, которому назначены роли FSMO. Выберите контроллер домена для каждой роли таким образом, чтобы все роли оказались на одном сервере. Для получения дополнительных сведений о размещении ролей FSMO щелкните следующий номер статьи базы знаний Майкрософт:

223346 Расположение и оптимизация ролей FSMO на контроллерах домена под управлением Windows 2000

o Если контроллер домена, ранее исполнявший какую-либо роль FSMO, отсутствует в домене, а его роли были получены в соответствии с приведенными в этой статье указаниями, удалите данный контроллер из Active Directory. Для этого выполните процедуру, описанную в следующей статье базы знаний Майкрософт:

216498 Удаление данных из Active Directory после неудачного понижения роли контроллера домена

o При удалении метаданных контроллера домена с помощью команды **ntdsutil /metadata cleanup** (версия для Windows

2000 или для Windows Server 2003, сборка 3790) роли FSMO, назначенные работающим контроллерам доменов, не передаются другим контроллерам домена. Версия средства Ntdsutil, входящая в состав Windows Server 2003 с пакетом обновления 1 (SP1), автоматизирует выполнение этой задачи и удаляет дополнительные элементы метаданных контроллера домена.

- Некоторые администраторы предпочитают не восстанавливать состояние системы на контроллерах домена, являющихся обладателями ролей FSMO, если соответствующая роль была передана после архивирования состояния системы.
- Не назначайте роль хозяина инфраструктуры контроллеру домена, являющемуся сервером глобального каталога, поскольку в этом случае хозяин инфраструктуры не будет обновлять сведения об объектах, так как он не содержит ссылки на объекты, которые не хранит. Причина такого поведения заключается в том, что сервер глобального каталога хранит частичные реплики всех объектов в лесу.

Чтобы проверить, является ли контроллер домена сервером глобального каталога, выполните следующие действия.

1. Нажмите кнопку **Пуск** и выберите последовательно пункты **Программы**, **Администрирование** и **Active Directory - сайты и службы**.
2. Дважды щелкните узел **Сайты** в левой панели и найдите соответствующий сайт или, если другие сайты отсутствуют, выберите вариант **Default-first-site-name**.

	3.Откройте папку «Серверы» и выделите требуемый контроллер домена. 4.В папке контроллера домена дважды щелкните элемент **Параметры NTDS**. 5.В меню **Действие** выберите команду **Свойства**. 6.Перейдите на вкладку **Общие** и проверьте, установлен ли флажок **Глобальный каталог**.