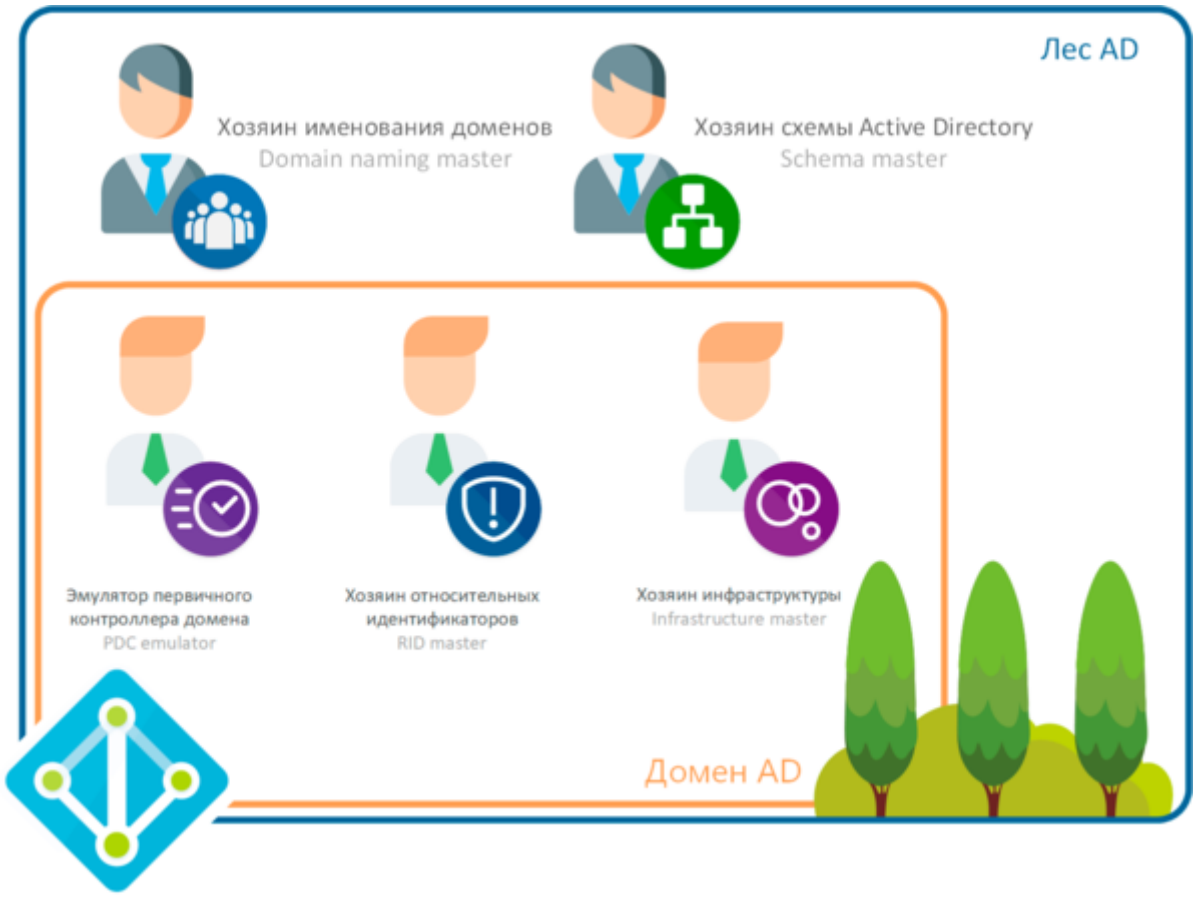
Мифы и легенды Active Directory. Хозяева ролей FSMO

Active Directory, как и любая серьезная система с долгой историей успела приобрести свой фольклор, неотъемлемой частью которого являются мифы и легенды. А одной из самых мифологизированных тем являются **хозяева операций**, они же роли FSMO, большее количество фантазий и суеверий существует разве что на тему равноправия контроллеров домена, но о них мы поговорим в другой раз. Сегодня же попытаемся понять, что делают и чего не делают хозяева операций, для чего они вообще нужны и можно ли жить без них.

Данная статья не ставит цель дать полную и исчерпывающую информацию о ролях FSMO и их хозяевах. Мы коротко рассмотрим основные задачи каждой роли, ее влияние на работоспособность инфраструктуры Active Directory, последствия отказа и дадим основные рекомендации по применению. Ну и попутно разберем некоторые мифы, а также распространенные заблуждения.

Напомним, что существуют пять ролей FSMO: две - уровня леса (уникальны в пределах леса) и три - уровня домена (уникальны для каждого домена). Для лучшей наглядности мы подготовили следующую инфографику, где указали как русские, так и английские названия хозяев:



В одном лесу могут существовать множество доменов и каждый домен будет иметь свой набор хозяев, хозяева леса существуют в единственном экземпляре на весь лес, вот с них мы и начнем.

Хозяин именования доменов (Domain naming master)

Хозяин именования доменов, как следует из его названия, контролирует уникальность доменных имен в пределах леса. На самом деле его обязанности несколько шире и правильно будет говорить о том, что в зону ответственности этого хозяина входит контроль уникальности **контекста имен**, куда кроме собственно имен доменов входят имена **разделов каталогов приложений**, которые также хранят свои данные в базе AD.

Базовые задачи

Задач у этого хозяина немного, но несмотря на то, что все они важные, это разовые и штучные операции. Прежде всего это создание, удаление и переименования доменов, и да, для удаления домена вам тоже нужно получить одобрение от этого хозяина. Следующая задача - это создание и удаление разделов, но это тоже происходит далеко не каждый день. И, наконец, создание и удаление перекрестных ссылок, которые служат для поиска по каталогу, если сервер, к которому мы подключаемся не содержит нужной копии каталога, такие ссылки могут вести за пределы домена и даже за пределы леса.

Никакой уникальной и критичной информации хозяин именования доменов не хранит, в повседневной жизни каталога участия не принимает.

Последствия недоступности

Как следует из основных задач этого хозяина, его наличие или отсутствие для нормальной работы Active Directory некритично, скажем больше - без него можно спокойно жить годами. Фактически он нужен для выполнения очень редких и единичных операций, все что он делает - это выдает разрешения на создание, изменение или удаление объектов контекста имен. А теперь давайте вспомним, как часто вы создаете новые домены и разделы? Во многих случаях только один раз, при создании Active Directory, а про перекрестные ссылки многие и не слышали.

Рекомендации по размещению

Официально Microsoft рекомендует совмещать роль этого хозяина с ролью **хозяина схемы** и размещать их на отдельном контроллере в центре топологии сети, который при этом не будет загружен обработкой логинов и групповых политик. Но с учетом крайне редкой необходимости данного хозяина и некритичности его задач к быстродействию роль можно располагать где угодно, это ни на что не повлияет. На практике хозяином именования доменов становится первый контроллер в структуре AD.

Хозяин схемы Active Directory (Schema Master)

Чтобы понять значение этого хозяина вспомним, что такое **схема Active Directory** - это перечень всех возможных объектов каталога, их полей и атрибутов. Если мы хотим добавить в Active Directory новые объекты или расширить набор реквизитов у существующих - мы изменяем схему. На самом деле изменения схемы происходят достаточно редко: при вводе в домен нового контроллера на более свежей версии ОС и установке ПО, добавляющего в схему свои объекты, например, Exchange.

Схема Active Directory существует в единственном экземпляре, хотя ее копия хранится на каждом контроллере домена и очень важно обеспечить единообразность и предсказуемость этой информации. Если вдруг два контроллера одновременно начнут вносить изменения в схему, то о единообразности можно забыть и пойди еще разберись какие именно изменения правильные. Чтобы этого избежать было решено сделать ответственным за изменение схемы единственный контроллер, с ролью **хозяина схемы**.

Базовые задачи

Задача у хозяина схемы одна - внесение изменений в схему и ее репликацию на другие контроллеры. С внесением изменений понятно, хозяин схемы единственный кто может вносить в нее изменения, а вот репликация заслуживает отдельного пояснения. При изменении схемы каталог переходит в состояние **потери конвергенции**, т.е. обнаружив расхождение в схеме с партнером по репликации

контроллер ее временно приостанавливает и чтобы ее возобновить нужно обновить схему на всех контроллерах, именно этим и занимается данный хозяин, а для ускорения процесса для этого вида репликации применяется нулевая задержка.

Также до сих пор бытует мнение, что изменение схемы можно производить только на хозяине схемы, действительно, когда-то такие требования были, но сейчас это давно не так. Вы можете запустить процесс на любом контроллере или рабочей станции с установленными инструментами администрирования. Утилита сама установит связь с хозяином, и он внесет в схему необходимые изменения.

Второй популярный ужастик - это сложность и высокий риск при обновлении схемы. Общий смысл сводится к тому, что если схему обновили неправильно, не до конца или не на ту версию - то всё, дальше только переустановка Active Directory. На самом деле это не так, завалить каталог при обновлении схемы было возможно в Windows 2000, в более поздних версиях такую возможность исключили.

Следует помнить, что обновление схемы касается только того ПО, для которого мы это обновление делаем, все остальные как работали, так и будут работать, они ничего не знают про новые атрибуты с объектами и знать не хотят. Поэтому, если криво обновили схему - ничего страшного, обновим еще раз.

Последствия недоступности

Исходя из выполняемых задач можем видеть, что хозяин схемы нужен нам только для ее обновления и репликации обновленной схемы на контроллеры, при восстановлении **конвергенции** в каталоге хозяин перестает быть нужен и никак не влияет на его повседневную работу. Никаких уникальных данных он не хранит. Как часто вы вносите изменения в схему? Вряд ли чаще одного раза в несколько лет, вот именно тогда вы в очередной раз вспомните об этом хозяине, в остальных случаях его наличия в каталоге не требуется.

Рекомендации по размещению

Как мы уже писали выше, Microsoft рекомендует размещать **хозяина схемы** вместе с **хозяином именования доменов** на выделенном контроллере без высокой нагрузки в центре топологии. Фактически его размещение особой роли не играет, на практике хозяином схемы становится первый контроллер в каталоге.

Хозяин инфраструктуры (Infrastructure Master)

От ролей уровня леса плавно переходим к ролям уровня домена. **Хозяин инфраструктуры**, пожалуй, самая непонятная роль, вокруг которой хватает домыслов и фантазий, но далеко не все могут четко сказать зачем она нужна и что делает. На самом деле все довольно просто, структура Active Directory предусматривает наличие в одном лесу множества доменов, которые могу образовывать сложные подчиненные структуры и у каждого домена будут свои администраторы и своя зона ответственности. Тем не менее мы можем добавлять в

каталог своего домена объекты из других доменов леса - "иностранцев", но так как мы не можем управлять данным объектом для него создается специальная ссылка - фантом.

Что может быть дальше? Да все что угодно, "иностранный" объект могут изменить, переместить, удалить и за этим всем надо как-то следить, именно эту задачу и выполняет **хозяин инфраструктуры**.

Базовые задачи

Хозяин инфраструктуры периодически (один раз в двое суток) соединяется с ближайшим **глобальным каталогом** и обновляет информацию о фантомных объектах. Что такое глобальный каталог? Это один из контроллеров в текущем домене, который содержит информацию о всех объектах леса.

Вот здесь существуют некоторые тонкости, если хозяин инфраструктуры расположен на глобальном каталоге, то он работать не будет. Таким образом роль вроде бы есть, но на самом деле ее нет.

Но это только цветочки, в ряде ситуаций роль данного хозяина становится чисто номинальной, перечислим их:

- У вас только один домен или нет ссылок на объекты других доменов
- На уровне леса включена **корзина Active Directory**, в этом случае задачи хозяина инфраструктуры будут выполнять все контроллеры домена
- Каждый из контроллеров домена является глобальным каталогом (именно так сейчас рекомендует делать Microsoft)

В общем, получился у нас какой-то хозяин, который и сам себе не хозяин, поэтому надо четко представлять ситуацию и понимать нужна вам эта роль или нет.

Последствия недоступности

Как мы уже выяснили, во многих сценариях роль хозяина инфраструктуры будет сугубо номинальной и нам будет ни горячо, ни холодно от его наличия или отсутствия. Если же данный хозяин действительно нужен, но оказался недоступным, то через некоторое время ваш каталог будет содержать недостоверную информацию об "иностранцах", например, в адресной книге будет продолжать присутствовать удаленный аккаунт. Ничего особо страшного в этом нет, но и приятного мало. А так-как никакой уникальной информации данный хозяин не хранит, то мы всегда можем захватить эту роль любым другим контроллером.

Рекомендации по размещению

Прежде всего нужно действительно убедиться, что вам нужна данная роль. При положительном ответе на данный вопрос рекомендуется размещать ее на отдельном контроллере, который не является глобальным каталогом и иметь не

менее двух глобальных каталогов в составе домена, для того, если один из них окажется недоступен, хозяин смог бы подключиться к второму из них.

Хозяин относительных идентификаторов (RID master)

Любой объект в пределах леса отличается своим уникальным идентификатором - GUID, который позволяет однозначно определить объект даже если мы его переименуем или перенесем в другое расположение. Для объектов, которые могут производить действия над другими объектами используется дополнительный идентификатор безопасности - SID, а сами объекты называются субъектами безопасности (*security principal*).

Классический SID имеет вид:

```
S-1-5-21-1004336348-1177238915-682003330-500
```

Который состоит из:

- Номера редакции, на данный момент существует только одна редакция (1)
- Идентификатора центра выдачи (5, NT Authority)
- Идентификатора домена, уникален для каждого домена в пределах леса (21-1004336348-1177238915-682003330)
- Относительного идентификатора (500, встроенная учетная запись администратора домена)

Как можно заметить, все субъекты в пределах домена будут различаться только номером относительного идентификатора - RID. Существуют зарезервированные диапазоны RID: от 0 до 499 - системные RID, 500-1000 - встроенные субъекты безопасности (например, встроенные группы и учетные записи), начиная с 1001 - свободные RID для создания новых субъектов безопасности.

Кто может создавать новые субъекты безопасности в домене? Любой контроллер и поэтому начинает стоять вопрос обеспечения уникальности выдаваемых RID. Разработчики решили этот вопрос просто и изящно - каждый контроллер получает свой пакет RID и занимается их выдачей самостоятельно. Эти пакеты - пулы выдает специально уполномоченный контроллер - **хозяин относительных идентификаторов**.

Базовые задачи

Основная задача хозяина относительных идентификаторов - это выдача контроллерам домена пулов RID. Каждому обратившемуся контроллеру хозяин выдает пул из 500 RID, когда он заканчивается (остается менее 100), контроллер обращается к хозяину повторно и получает новый пул. Выданный пул сразу считается израсходованным и если получивший его контроллер выйдет из строя, то повторно использовать этот диапазон нельзя.

Дополнительная задача - контроль уникальности RID при переносе субъекта безопасности в другой домен. Хотя GUID объекта не меняется, его SID должен быть изменен и хотя это может сделать любой контроллер домена мы должны убедиться в уникальности присеваемого SID, а что если перенос объекта одновременно начнут два контроллера? Поэтому для данной операции привлекается хозяин RID того домена, в который осуществляется перенос для контроля уникальности SID.

Последствия недоступности

Так как с хозяином RID общаются только контроллеры домена, то никакого влияния на повседневную работу каталога его отсутствие не окажет. Проблемы начнутся тогда, когда контроллеры израсходуют пул RID, а это может случиться очень нескоро, с учетом того, что количество объектов во многих каталогах гораздо меньше пятисот.

Никакой уникальной информации хозяин RID не хранит и для восстановления работоспособности можно просто захватить эту роль другим контроллером.

Рекомендации по размещению

Никаких особых рекомендаций по размещению хозяина RID нет, с точки зрения быстродействия его следует размещать в центре топологии, также желательно чтобы хозяин не был единственным контроллером в сайте Active Directory. По возможности стоит совмещать эту роль вместе с PDC Emulator.

Эмулятор первичного контроллера домена (PDC Emulator)

Самая нагруженная обязанностями роль FSMO. Первоначально была создана для обеспечения совместимости с **доменом NT**, но в наши времена домен NT - это что-то из разряда древних легенд и **эмулятор первичного контроллера домена** занимается совсем другими задачами. И, в отличие от других хозяев, прохлаждаться ему не приходится.

Базовые задачи

Эмулятор PDC является **эталоном времени** для собственного домена, а эмулятор PDC корневого домена также является эталоном для эмуляторов PDC дочерних доменов. Остальные контроллеры домена синхронизируют время с эмулятором PDC, прочие участники домена синхронизируют время с ближайшим контроллером.

Вторая важная задача - это **приоритетная репликация паролей**, после изменения пароля любой контроллер в приоритетном порядке уведомляет об этом эмулятор PDC. Если аутентификация на контроллере не была успешной по причине неверного пароля следующий запрос будет направлен эмулятору, так как он точно знает правильный пароль. При последующей успешной аутентификации об этом снова уведомляется эмулятор PDC, который сбрасывает на ноль количество неудачных попыток входа.

Изменения в пространство имен **Distributed File System (DFS)** и **групповые политики (GPO)** также вносятся на эмуляторе первичного контроллера домена.

Также эмулятор PDC следит за встроенными субъектами безопасности и восстанавливает их при необходимости, скажем, если вы вдруг решите исключить встроенную учетную запись Администратор из группы Администраторы - эмулятор PDC быстро вернет все на место.

Последствия недоступности

Пожалуй, это единственный из хозяев, отсутствие которого можно заметить достаточно быстро. Во-первых прекратится синхронизация времени в домене, каждый контроллер начнет ориентироваться на свои часы и после того, как время разбежится более чем на 5 минут начнутся проблемы со входом в систему.

Если вы используете DFS, то через некоторое время столкнетесь с его неверной работой. А вот изменения в групповые политики внести будет можно, но при этом оснастка попросит вас явно указать контроллер, на котором вы хотите выполнить данную процедуру.

Что касается изменения паролей, то без эмулятора PDC мы можем испытывать проблемы со входом в систему вплоть до блокировки учетной записи до тех пор, пока информация об измененном пароле не будет реплицирована на все контроллеры домена.

А также мы можем творить всякую дичь со встроенными субъектами безопасности и исправить это будет некому.

Для устранения этой ситуации достаточно захватить роль любым другим контроллером.

Рекомендации по размещению

Для эмулятора первичного контроллера домена рекомендуется настроить синхронизацию времени с внешним источником, если он располагается в виртуальной машине, то обязательно следует отключить синхронизацию часов виртуальной машины через гипервизор. В случае переноса или захвата роли эмулятора следует повторно настроить синхронизацию времени с внешним источником.

Как и другие хозяева размещать эмулятор первичного контроллера домена лучше всего в центре топологии, также рекомендуется совмещать эту роль с хозяином RID.