FSMO-роли, или, как их ещё называют, мастера Active Directory - это контроллеры домена, наделённые специфичными полномочиями.

atraining.ru/active-directory-fsmo-roles

2013-10-05T07:15:33+08:00

Эта статья написана достаточно давно Николаем Кутявиным и перенесена с нашего предыдущего хостинга с некоторыми потерями, поэтому краткая и не очень полная. Сейчас я пишу статьи про каждую из FSMO-ролей отдельно – например, про RID Master. Они более наполнены информацией и актуализированы, чем эта – имеет смысл зайти к нам в раздел Knowledge Base и посмотреть их там.
Ruslan V. Karmanov.

Введение

В жизни каждого системного администратора наступает момент, когда ему приходится лихорадочно вспоминать, какая роль на каком контроллере домена развернута, а главное, какая за что отвечает. Как правило, это сценарии обновления, миграции или аварийного восстановления.

По долгу службы регулярно приходится сталкиваться с большим разнообразием фантазий и суеверий на тему равноправности контроллеров домена (“начиная с Windows 2000”), интересных предположений о работе, например, роли Infrastructure Master, поэтому прояснить ситуацию раз и навсегда крайне желательно.

Итак. Все мы знаем, что ролей FSMO (Flexible Single Master Operation) в Active Directory встречается аж пять штук. Это:

- Schema Master

- Domain Naming Master
- Infrastructure Master
- RID Master
- PDC Emulator

Каждая из них сейчас будет рассмотрена подробнее. Поехали!

Schema Master

(отдельная статья тут – Schema Master)

В каждом лесу Active Directory есть не более одного хозяина схемы (Schema Master). Именно он отвечает за внесение изменений в раздел Schema, где находятся описания всех классов и атрибутов Active Directory.

Располагаться данная роль может на любом контроллере домена в пределах леса. Если вдруг ей случится оказаться на сервере с ОС Windows 2000, считайте, что вам повезло – вы сможете запретить ее изменение галочкой в настройках. В Windows 2003 эту галочку декомиссовали, т.к. польза от нее неизмерима.

Хорошая роль, простая и нужная.

Domain Naming Master

(отдельная статья тут – Domain Naming Master)

Следующая роль лесного уровня – хозяин именования доменов. Как понятно из определения “лесной”, этого товарища в лесу также не более одного.

Domain Naming Master отвечает за операции, связанные с именами доменов Active Directory. Но не только. Зон ответственности у него четыре:

- Добавление и удаление доменов в пределах леса
- Создание и удаление разделов (application directory partitions)
- Создание и удаление перекрестных ссылок (crossRef)
- Одобрение переименования домена

Пройдемся по каждой чуть подробнее.

Добавление и удаление доменов

Добавлять и удалять домены позволяется только контроллеру с ролью Domain Naming Master. Этот контроллер бдительно следит, чтобы добавляемый домен имел уникальное в пределах леса NETBIOS-имя. Если Naming Master недоступен, на попытках изменить число доменов в лесу можно ставить крест.

Нужно отметить, что проверять уникальность FQDN-имени нового домена на специально отведенном контроллере смысла нет, проще запросить информацию из DNS.

Создание и удаление разделов

В Windows 2003 появилась возможность создавать обособленные разделы, или, как их еще называют, партиции. Партиции используются для хранения в AD произвольных данных. Самый яркий пример использования партиций – хранение данных для DNS-серверов в партициях *ForestDnsZones* и *DomainDnsZones*.

Стоит ли говорить, что управление партициями при недоступном DNM невозможно? Хотя… Да, возможен вариант, когда доступный Domain Naming Master хостится на сервере с ОС Windows 2000, тогда о партициях речи тоже не будет.

Создание и удаление перекрестных ссылок

Перекрестные ссылки используются для поиска по каталогу в том случае, если сервер, к которому подключен клиент, не содержит нужной копии каталога; причем ссылаться можно даже на домены вне леса, при условии их доступности. Хранятся перекрестные ссылки (объекты класса *crossRef*) в контейнере *Partitions* раздела *Configuration*, и только Domain Naming Master имеет право в этом контейнере хозяйничать. Понятно, что читать содержимое контейнера может любой контроллер, благо раздел *Configuration* один для всего леса, но вот изменять его содержимое может лишь один.

Очевидно, что недоступность контроллера с ролью Domain Naming Master опечалит администратора, желающего создать новую перекрестную ссылку, или удалить ненужную.

Одобрение переименования домена

В процессе переименования домена основная утилита этого действа (rendom.exe) составляет скрипт с инструкциями, которые должны будут выполниться в процессе переименования. Все инструкции проверяются, после чего скрипт помещается в атрибут *msDS-UpdateScript* контейнера *Partitions* раздела *Configuration*. Помимо этого, значения атрибута *msDS-DnsRootAlias* для каждого объекта класса *crossRef* устанавливаются в соответствии с новой моделью именования доменов. Поскольку право менять содержимое *crossRefContainer* есть только у контроллера с ролью Domain Naming Master, то очевидно, что проверку инструкций и запись атрибутов выполняет именно он.

Если при проверке скрипта обнаружатся ошибки, или новый лес окажется некошерным, или выявятся пересечения имен между доменами старого и нового лесов, весь процесс переименования будет остановлен.

Пожалуй, Domain Naming Master – единственная роль, без которой можно безболезненно жить годами. Но, разумеется, лучше, когда всё работает.

Infrastructure Master

(отдельная статья тут – Infrastructure Master)

В случаях, когда наш домен содержит ссылки на объекты из других доменов или лесов, возможны разные интересные ситуации. Например, переименование объекта, или перенос объекта в другой OU в пределах домена, или перенос объекта в другой домен. В первых двух случаях меняется DN, в третьем – DN и SID. В результате таких изменений найти объект по нашей ссылке станет невозможно. Последствия навскидку – устаревание информации в адресной книге, отказ внешнему пользователю в доступе к ресурсам нашего домена, и так далее. Infrastructure Master как раз и предназначен для разгребания таких интересных ситуаций.

Дело в том, что в Active Directory есть три основных атрибута уникальности объекта – GUID, SID (у Security Principal'ов), и distinguished name (DN). Сервер с ролью IM отвечает за обновление так называемых "фантомных записей" (Phantom Records), содержащих GUID, SID и DN не-местных объектов. Он старательно проверяет, не изменилось ли чего важного, и при необходимости обновляет информацию в своем домене. Проверка заключается в поиске объектов *не*родного домена по GUID – как по единственному категорически неизменному атрибуту.

~~Причем, совершенно неважно, идет речь о разных доменах одного леса, или о разных лесах. Возможна ситуация, когда домен в лесу один, но он имеет доверительные отношения с другим доменом. Здесь тоже найдется работа для хозяина инфраструктуры.~~

Роль IM отслеживает изменения в текущем лесу. Доверие между доменами других лесов и сопутствующие объекты – не его зона ответственности.

RID Master

(отдельная статья тут – RID Master)

В жизни каждого домена возникает момент, когда создается первая учетная запись. У кого-то такая потребность возникает сразу, кто-то приходит к ней со временем. Но рано или поздно учетные записи возникают абсолютно в любом домене. И у каждой учетной записи (пользователя, компьютера, группы, TDO) должен быть уникальный идентификатор безопасности (SID) – он будет служить великой задаче разграничения доступа. Поэтому было бы неплохо понять, как формируется данный идентификатор, и при чем тут RID Master.

Воспользуемся тайным знанием Майкрософт. Любой доменный идентификатор безопасности состоит из нескольких частей.

SID: S-1-5-Y1-Y2-Y3-Y4. Здесь:

Элемент SID	Описание
S-1	SID ревизии 1. В настоящее время используется только эта ревизия.
5	Обозначает, кем был выдан SID. 5 означает NT Authority. Однако, так называемые well-known SIDs могут в данной части иметь 0, 1, и некоторые другие значения для обозначения своей “well-known’ости”.
Y1-Y2-Y3	Идентификатор домена, к которому относится учетная запись. Одинаковый для всех объектов security principal в пределах данного домена.
Y4	Относительный идентификатор (Relative ID, RID), относящийся к конкретной учетной записи. Подставляется из пула относительных идентификаторов (RID Pool) домена в момент создания учетной записи.

Так вот. Контроллер домена с ролью RID Master отвечает за выделение последовательности уникальных RID’ов каждому контроллеру домена в своем домене, а также за корректность перемещения объектов из одного домена в другой. У контроллеров домена есть общий пул относительных идентификаторов, из которого каждому контроллеру выделяется пачка “примерно” по 500 штук. Когда число выделенных контроллеру RID’ов подходит к концу (становится меньше 100), он запрашивает новую пачку. Разумеется, число выдаваемых RID и порог запроса можно при желании менять.

В действительности же всё не совсем так, как на самом деле :) Выдаются не сами идентификаторы, а ссылки на них. Для каждого контроллера домена – своя ссылка, которая, к тому же, хранится в его собственном контейнере. Поэтому, если мы вдруг удаляем контроллер домена из Active Directory вручную, может возникнуть нехорошая ситуация, когда при создании учетных записей (пользователя, компьютера, группы, TDO) будут использоваться уже выданные RID, что, в свою очередь, приведет к увлекательнейшему траблшутингу.

Не будем забывать и про перемещение объектов между доменами. Именно RID Master следит за тем, чтобы в каждый момент времени каждый объект перемещался только в один домен. Иначе возможна крайне нездоровая ситуация, когда в двух доменах будет два объекта с одинаковым GUID. Траблшутинг подобной ситуации грозит быть не менее увлекательным, чем ловля дублирующихся SID.

Если RID Master не будет доступен, то после истощения запаса свободных RID создать новую учетную запись (пользователя, компьютера, группы, TDO*) станет невозможно. А заодно не удастся провести миграцию объектов из текущего домена в другой.

—

** TDO – Trusted Domain Object. Создаётся при настройке доверительных отношений.*

PDC Emulator

Третья и последняя FSMO-роль уровня домена – Primary Domain Controller (PDC) Emulator. Пожалуй, самая нагруженная обязанностями.

ДОМЕН ACTIVE DIRECTORY

Сервер с ролью PDC Emulator служит великой задаче обеспечения совместимости с предыдущими версиями Windows. Но не только, и, в последнее время, не столько. Для начала неплохо бы вспомнить, чем занимался PDC в Windows NT 4.0 и 3.51:

Обработка операции “смена пароля” для пользователей и компьютеров

Репликация обновлений на BDC (Backup Domain Controller)

Обозреватель сети (Domain Master Browser)

В смешанной среде, в которой встречаются клиенты Windows NT4.0, Windows 95 и Windows 98 (без установленного клиента Active Directory) и контроллеры домена pre-Windows2000, всем вышеперечисленным занимается как раз PDC Emulator. Только он и только для них.

Когда же все клиенты обновляются до Windows 2000 и выше (либо когда на Windows NT4/95/98 ставится клиент Active Directory), наступает счастье:

Клиенты меняют пароли при помощи первого попавшегося контроллера домена

Запросы на репликацию от BDC перестают отнимать время в силу полного своего отсутствия

Клиенты ищут сетевые ресурсы в AD, и не зависят более от обозревателя сети (эх, как всё хорошо в technet)

После перехода всей инфраструктуры на Windows 2000 и старше, контроллер домена с ролью PDC Emulator причиняет пользу так:

Пароль, измененный любым другим контроллером домена, отправляется на PDC Emulator высокоприоритетной репликацией

Если аутентификация на любом другом контроллере домена не была успешной с признаком “неверный пароль”, запрос повторяется на эмуляторе PDC. Понятно, что, в случае только что произошедшей смены пароля, уж этот-то запрос будет успешным

При успешной аутентификации учетной записи сразу после неудачной попытки, эмулятор PDC о ней уведомляется и сбрасывает счетчик неудачных попыток в ноль. Сущий позитив для пользователя, часто забывающего свой пароль

Здесь важно заметить, что, даже в случае недоступности эмулятора PDC, информация об изменении пароля всё равно расползется по домену. Да, возможны некоторые сложности, пока идет репликация, но, в принципе, ничего страшного.

WELL KNOWN SECURITY PRINCIPALS

В Active Directory есть такая замечательная штука, как Well Known Security Principals. Это всяческие Local Service, Network Service, Digest Authentication, и т.п. Несложно догадаться, что управление ими всеми (начиная с Windows 2003) осуществляется как раз контроллером домена с ролью PDC Emulator. Конкретно, эмулятор PDC после апгрейда (или переноса данной роли) на более новую версию Windows обновляет содержимое контейнера “CN=WellKnown Security Principals,CN=Configuration,DC=*YourDomain*”. В этот же момент происходит создание недостающих well-known и built-in групп, а также обновление членства в них.

ADMINSDHOLDER

Следующая нужная фича – AdminSDHolder, владелец административных дескрипторов безопасности. AdminSDHolder защищает административные группы от изменений. Если дескриптор безопасности в какой-либо административной учетной записи не соответствует представлениям AdminSDHolder’a, этот дескриптор будет обновлен в соответствии с его (AdminSDHolder’a) понятиями. К примеру, если исключить well-known пользователя Administrator из группы Builtin\Administrators, AdminSDHolder вернет его на место.

Да, AdminSDHolder, как понятно, выполняется именно на контроллере домена с ролью эмулятора PDC.

DNS

Только для PDC Emulator в DNS регистрируется SRV-запись вида _ldap._tcp.pdc._msdcs.DnsDomainName, она позволяет клиентам быстренько найти сервер эмуляции PDC.

DFS

Изменения, вносимые в пространство имен Distributed File System (DFS), вносятся на контроллере домена с ролью PDC Emulator. Корневые серверы DFS периодически запрашивают с эмулятора PDC обновленные метаданные, сохраняя их у себя в памяти. Очевидно, что недоступность эмулятора PDC влечет за собой неверную работу DFS.

ГРУППОВЫЕ ПОЛИТИКИ

Редактор групповых политик по умолчанию соединяется с сервером PDC Emulator, и изменения политик происходят на нем же. Если PDC Emulator недоступен, тогда редактор ГП не постесняется спросить у администратора, к какому контроллеру домена подключиться.

ВРЕМЯ

Да, по умолчанию именно сервер PDC Emulator является для клиентов сервером точного времени в домене. А эмулятор PDC корневого домена в лесу является по умолчанию сервером точного времени для эмуляторов PDC в дочерних доменах.