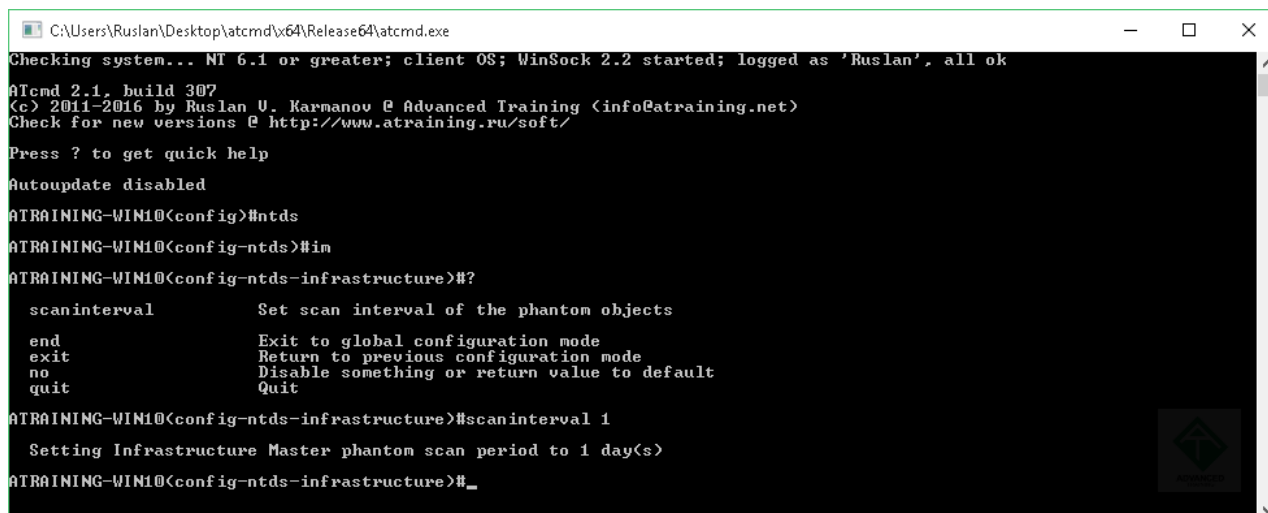


FSMO-роль Infrastructure Master - пожалуй, самая редко изучаемая и понимаемая. Разбираемся детально.

 atrain.ru/active-directory-fsmo-infrastructure-master

2016-05-02T05:37:54+08:00



```
C:\Users\Ruslan\Desktop\atcmd\x64\Release64\atcmd.exe
Checking system... NT 6.1 or greater; client OS; WinSock 2.2 started; logged as 'Ruslan', all ok
ATcmd 2.1, build 307
(c) 2011-2016 by Ruslan U. Karmanov @ Advanced Training (info@atrain.ru)
Check for new versions @ http://www.atrain.ru/soft/
Press ? to get quick help
Autoupdate disabled
ATRAINING-WIN10(config)#ntds
ATRAINING-WIN10(config-ntds)#in
ATRAINING-WIN10(config-ntds-infrastructure)#?
  scaninterval      Set scan interval of the phantom objects
  end               Exit to global configuration mode
  exit              Return to previous configuration mode
  no                Disable something or return value to default
  quit              Quit
ATRAINING-WIN10(config-ntds-infrastructure)#scaninterval 1
  Setting Infrastructure Master phantom scan period to 1 day(s)
ATRAINING-WIN10(config-ntds-infrastructure)#_
```

Привет.

Продолжаем цикл статей про FSMO-роли в Active Directory. На очереди – IM, он же Infrastructure Master. Классический “вопрос на тройку” на собеседовании системного инженера – “что эта роль вообще делает, вкратце?” – хотя, при текущих тенденциях, уже, наверное, на четвёрку. Больно уж сильно окрепли и углубились знания у инженеров в последнее время, да.

Предварительная диспозиция такая же – знание материала работы Active Directory на уровне курса [Microsoft 20410](#), больше – лучше.

Infrastructure Master

- Зачем нужен Infrastructure Master
- Как работает Infrastructure Master
- Что не делает Infrastructure Master
- Как перенести владельца FSMO-роли Infrastructure Master?
- Где хранится информация, кто сейчас Infrastructure Master?
- Где располагать владельца FSMO-роли Infrastructure Master?
- Как повысить надёжность работы Infrastructure Master?
- Как повысить безопасность работы Infrastructure Master?
- “Если Infrastructure Master упал то всё”
- Зависит ли скорость работы доменов и репликации от расположения Infrastructure Master?
- Нужен ли Infrastructure Master’у отдельный бэкап?

Начнём.

Вместо предисловия про Infrastructure Master

Внимание!

Тонкость в том, что сейчас часть статьи про то, где располагать Infrastructure Master'a, не нужна. Процитирую MSDN:

When the Recycle Bin optional feature is enabled, every DC is responsible for updating its cross-domain object references in the event that the referenced object is moved, renamed, or deleted. In this case, there are no tasks associated with the Infrastructure FSMO role, and **it is not important which domain controller owns the Infrastructure Master role.**

То есть, при включённом на уровне леса Active Directory Recycle Bin'е, каждый DC сам решает все задачи, которые решал владелец FSMO-роли Infrastructure Master, поэтому роль, фактически, становится декоративной. **Именно роль, а не функционал проверки и обновления cross-domain object references.** Поэтому дальше в статье мы рассматриваем вариант, когда в лесу выключен Active Directory Recycle Bin. Что, впрочем, никак не уменьшает необходимости понимать данный функционал – т.е. задачи-то не деваются никуда, просто их теперь делают все DC, а не один специально выбранный.

Зачем нужен Infrastructure Master

Во времена доменов Windows NT всё было хорошо и просто – домены были каждый за себя, никакого леса, как объединения нескольких доменов по критерию “общий каталог объектов и общая конфигурация” не было. Вопросы перемещения объектов из домена в домен решались той же утилитой ADMT, и дело было несложным – и объектов поменьше (универсальных групп, например, нет), и логика их взаимодействия попроще (вложения групп, например, тоже нет), и идентификация у security principal'ов простая – SID да и всё, никакого GUID. Благодать.

Но появляется Active Directory, а с ней и понятие леса доменов. Вместо единого подхода к ситуации “один домен дружит с другим” получается несколько вариантов, от “домен дружит внутри леса с соседом, сидящим на одной ветке одного дерева” и “домен дружит внутри леса с соседом, сидящим на другом дереве, а то и в другом лесу” до “домен дружит с чем-то внешним и лишь напоминающим домен”.

В результате возникает совершенно новый класс ситуаций, вызванный тем, что у произвольно выбранного контроллера домена в домене А есть задача по хранению и отображению данных не только объектов из домена А, но и некоторых “иностраных” объектов из других доменов. Например, в списке членов группы в домене А могут быть участники из домена В. И в силу того, что репликация доменного раздела у домена А никак не пересекается с такой же репликацией у домена В, т.е. прямого и непрерывного обмена данными о всех security principals у

всех связанных доменов нет (можно прикинуть потенциальный масштаб такой мета-репликации), нужен какой-то механизм “контроля за иностранцами”. Если этого не делать, то возможны ситуации:

- В составе группы домена А есть учётка User из домена В. Её переименовали в родном домене – как домен А узнает про это событие? Получается, он будет отображать устаревшую информацию;
- В составе группы домена А есть учётка User из домена В. Её удалили в родном домене – как домен А узнает про это событие? Получается, он будет отображать несуществующего члена группы;
- В составе группы домена А есть учётка User из домена В. Её перенесли в домен С – как домен А узнает про это событие? Получается, он будет отображать неверную информацию об учётной записи;

Ситуация ещё более запутывается со схемами “В группу DomainA\Group1 входит группа DomainB\Group2, которая входит в DomainA\Group3”. Поэтому задача “регулярный контроль над состоянием иностранных учёток” – актуальна.

Оговоримся – актуальна она, как понятно, в ситуации, когда доменов больше одного. Если у вас лес с одним доменом, у которого нет trust’ов до других доменов, то смысла в этом контроле нет, т.к. нет “иностранцев”.

В итоге, основной задачей владельца FSMO-роли Infrastructure Master, говоря кратко, будет отслеживание изменения статусов у таких объектов. Технически каждый такой “иностранный security principal” будет представлен т.н. “phantom object” – специфичным объектом-ссылкой. Эти объекты используются в нашем сценарии как “минимальный комплект данных, чтобы добавить в список группы объект, не имея описания этого объекта локально”. Они не доступны для просмотра через обычный интерфейс Active Directory – вы видите в качестве, например, “участника локальной группы, но из другого домена” как раз phantom object, собранный на основании частичного списка атрибутов security principal’a. Эти объекты не будут реплицироваться между контроллерами в рамках стандартной репликации domain NC, хотя будут храниться в той же NTDS-базе, что и другие объекты Active Directory.

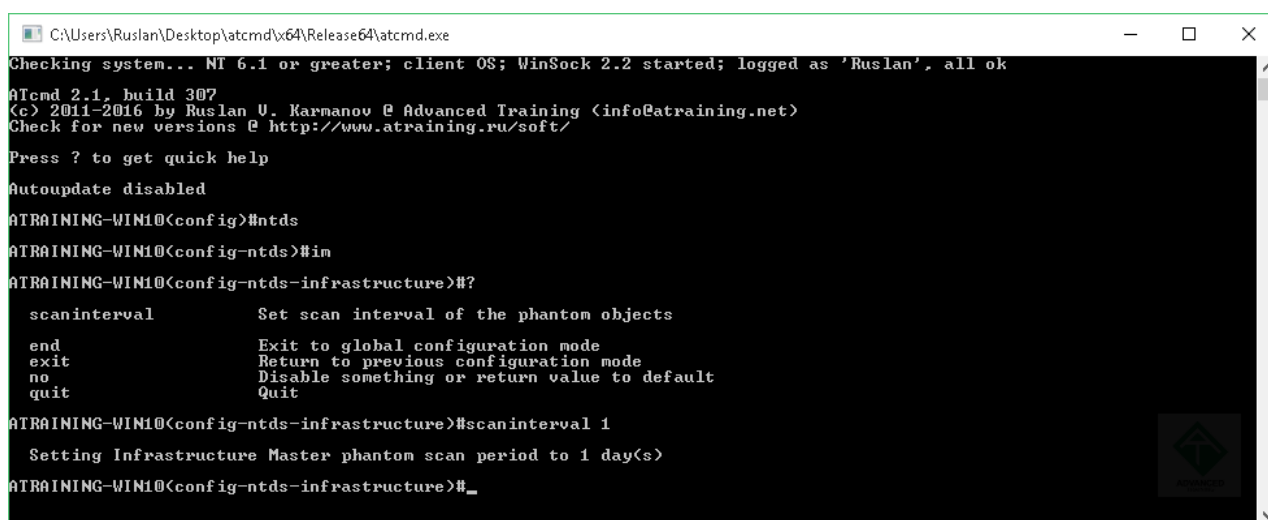
Пример – если у вас есть DomainA\Group1, в которую входит или группа DomainB\Group2, или пользователь DomainB\User2 – без разницы, для любого такого “иностранного” объекта в списке членов группы будет ссылка на phantom object – локальную табличку которых и будет обновлять Infrastructure Master. У каждого такого объекта будет фиксироваться три идентификатора – DN (которое надо проверять, потому что оно меняется при переименовании или перемещении security principal’a внутри домена), SID (который надо проверять, потому что он меняется при перемещении security principal’a из одного домена в другой в пределах леса) и GUID (который, к счастью, у объектов не меняется, и как раз по нему и можно найти новоперемещённый-переименованный объект).

Перейдём к механизму работы владельца FSMO-роли Infrastructure Master.

Как работает Infrastructure Master

Infrastructure Master будет периодически (по умолчанию раз в 2 суток) подключаться к ближайшему GC и, используя GUID-ы phantom object'ов, смотреть – не поменялось ли что в DN'ах и SID'ах отслеживаемых объектов? Для подключения будет использоваться именно GC, а не DC, потому что у GC точно есть вся нужная (в плане атрибутов) информация о всех security principal'ах леса, поэтому чтобы не бегать лично по всем доменам, разумнее подключаться к GC.

Данный промежуток можно изменять; он считается в днях, поэтому в плане “ускорения обработки изменений Infrastructure Master'ом” вы можете удвоить скорость, выставив не 2, а 1 сутки:



```
C:\Users\Ruslan\Desktop\atcmd\x64\Release64\atcmd.exe
Checking system... NT 6.1 or greater; client OS; WinSock 2.2 started; logged as 'Ruslan', all ok
ATcmd 2.1, build 307
(c) 2011-2016 by Ruslan U. Karmanov @ Advanced Training <info@atraining.net>
Check for new versions @ http://www.atraining.ru/soft/

Press ? to get quick help
Autoupdate disabled
ATRaining-WIN10(config)#ntds
ATRaining-WIN10(config-ntds)#in
ATRaining-WIN10(config-ntds-infrastructure)#?

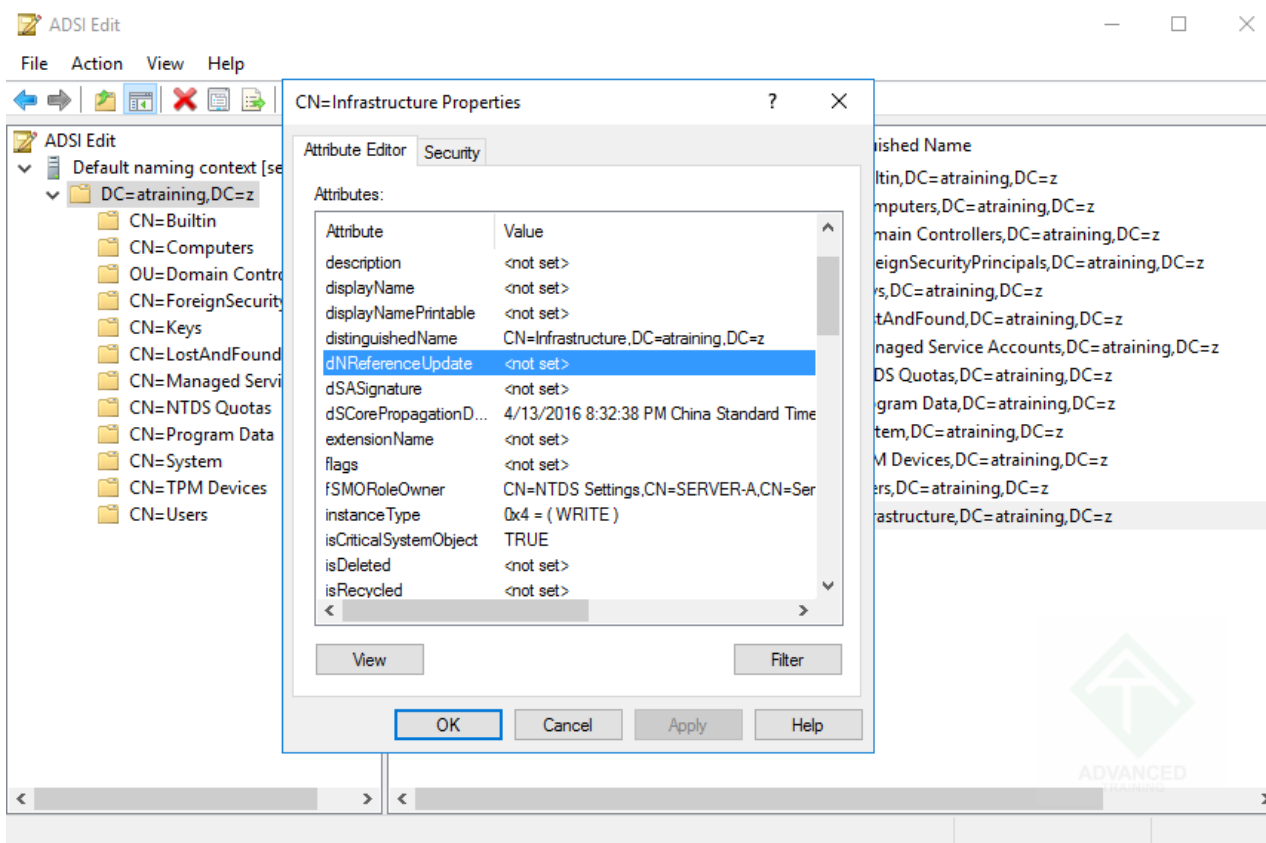
scaninterval      Set scan interval of the phantom objects
end                Exit to global configuration mode
exit               Return to previous configuration mode
no                 Disable something or return value to default
quit              Quit

ATRaining-WIN10(config-ntds-infrastructure)#scaninterval 1
Setting Infrastructure Master phantom scan period to 1 day(s)
ATRaining-WIN10(config-ntds-infrastructure)#_
```

[Изменяем периодичность проверки phantom объектов у Infrastructure Master \(кликните для увеличения до 979 px на 394 px\)](#)

Этот параметр имеет значение только на DC, который держит FSMO-роль Infrastructure Master – на других он будет игнорироваться.

Просмотрев табличку всех зарегистрированных в родном домене “иностранцев” и проверив, поменялись ли у кого имена-адреса-явки, а также вычеркнув выбывших по причине смерти (т.е. GUID не найден среди живых – значит, объект из другого домена удалили, такое тоже может быть), Infrastructure Master делает в своей локальной domain partition своего домена соответствующие изменения, после чего засыпает до следующего периода работы. Изменения, сделанные им, разнесутся по домену обычной репликацией. По сути, данные изменения будут состоять в создании объекта типа **infrastructureUpdate** в контейнере **CN=Infrastructure** и – что удивительно – немедленным переводом его в “удалённые”. Труп объекта, по старой традиции Microsoft'овской репликации, ещё с NBNS/WINS-серверов, будет реплицирован на все другие DC в этом домене, которые займутся некромантией – гаданием на мощах объекта, изучая атрибут **dnReferenceUpdate** (он будет содержать новый DN, который поменяется в части RDN, если объект переименован, или в части DN-суффикса, если перемещён).



[Корневой объект CN=Infrastructure, в котором создаются одиночные infrastructureUpdate](#)

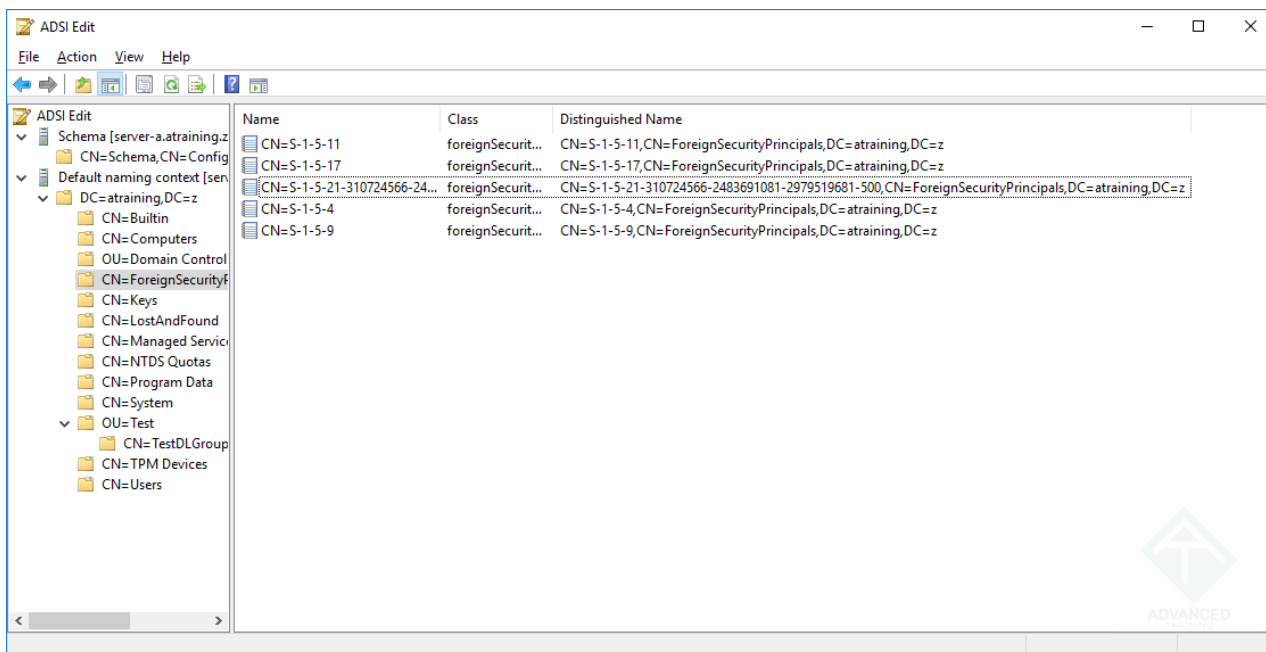
[\(кликните для увеличения до 858 px на 571 px\)](#)

Важные выводы – табличка с phantom object’ами – у каждого DC в домене, а не только у Infrastructure Master. И обновляется она ими на основании информации, полученной из репликации доменного раздела, а не какой-то отдельной, особой репликацией таблиц с phantom object’ами. Теперь чуть-чуть про то, что похоже на “характерные для задач Infrastructure Master действия”, но они не являются.

Что не делает Infrastructure Master

Ситуация с “Мы в домене А добавили в группу учётку из домена В, нашего же леса – подробная информация про неё есть на любом GC в нашем лесу, а мы лишь сделали у себя ссылочку, создав phantom object”, в которой в каждом домене и нужен Infrastructure Master, чтобы как-то централизовать вопрос обновления таблички этих phantom object’ов рассмотрена – но есть ситуация сложнее. Когда “Мы в домене А добавили в группу учётку из домена В, который вообще в другом лесу”.

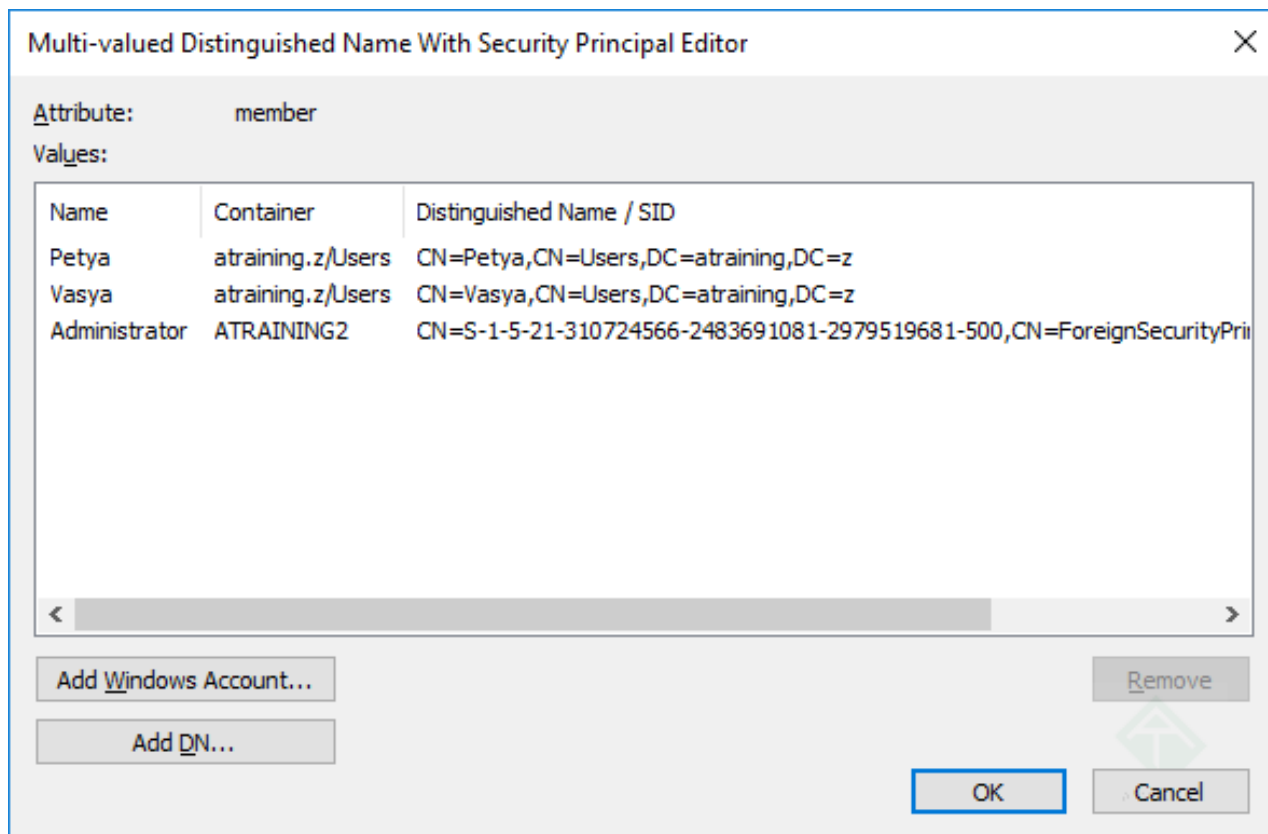
В этом случае Infrastructure Master не работает, работает другой механизм. Он для начала “легализует” этого FPO (foreign principal object) в вашем домене, путём добавления объекта в контейнер **CN=ForeignSecurityPrincipals**:



[Контейнер CN=ForeignSecurityPrincipals, в котором создаются записи про каждого security principal не из нашего леса Active Directory](#)
[\(кликните для увеличения до 1118 px на 572 px\)](#)

(Хорошо видно, что запись про “зарегистрированного в нашем домене иностранца” состоит из его SID’а в оригинальном домене и DN-суффикса контейнера **CN=ForeignSecurityPrincipals**) – а после в локальную группу уже будет добавляться ссылка на эту запись.

Вот так выглядит ситуация “В группу **TestDLGroup** в домене **atraining.z** добавили местных пользователей **Vasya** и **Petya**, а также учётку **Administrator** из доверенного леса **atraining2.z**:



[Чужой среди своих](#)

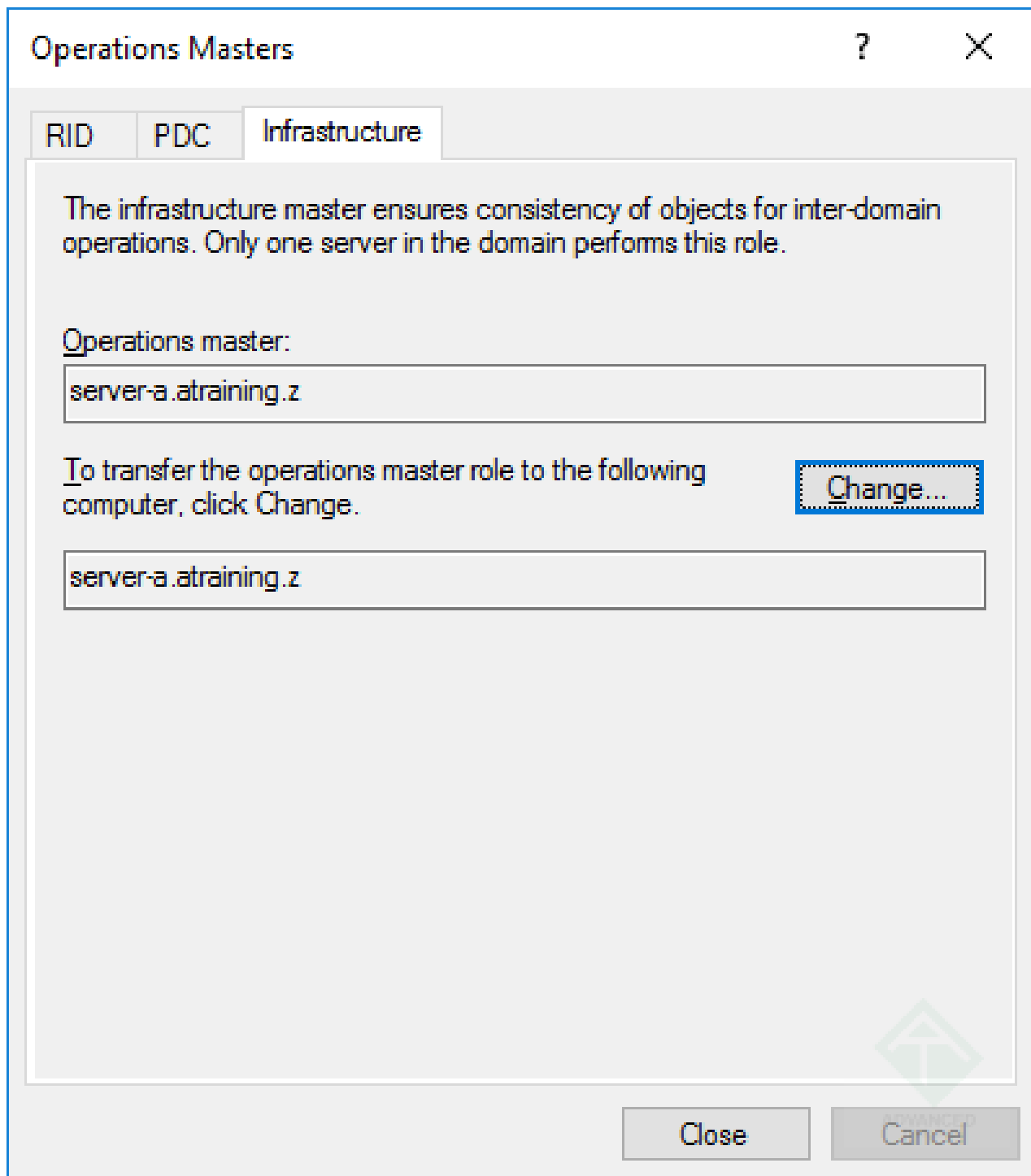
[\(кликните для увеличения до 590 px на 386 px\)](#)

Говоря проще, всё будет привязано к SID'у этого security principal'a на момент добавления, и изменения (например, переименование) отслеживаться будут, но не FSMO-ролью Infrastructure Master.

Ну, а теперь, так как с функционалом разобрались, и единственную настройку тоже увидели, перейдём к типовым вопросам по FSMO-ролям.

Как перенести владельца FSMO-роли Infrastructure Master?

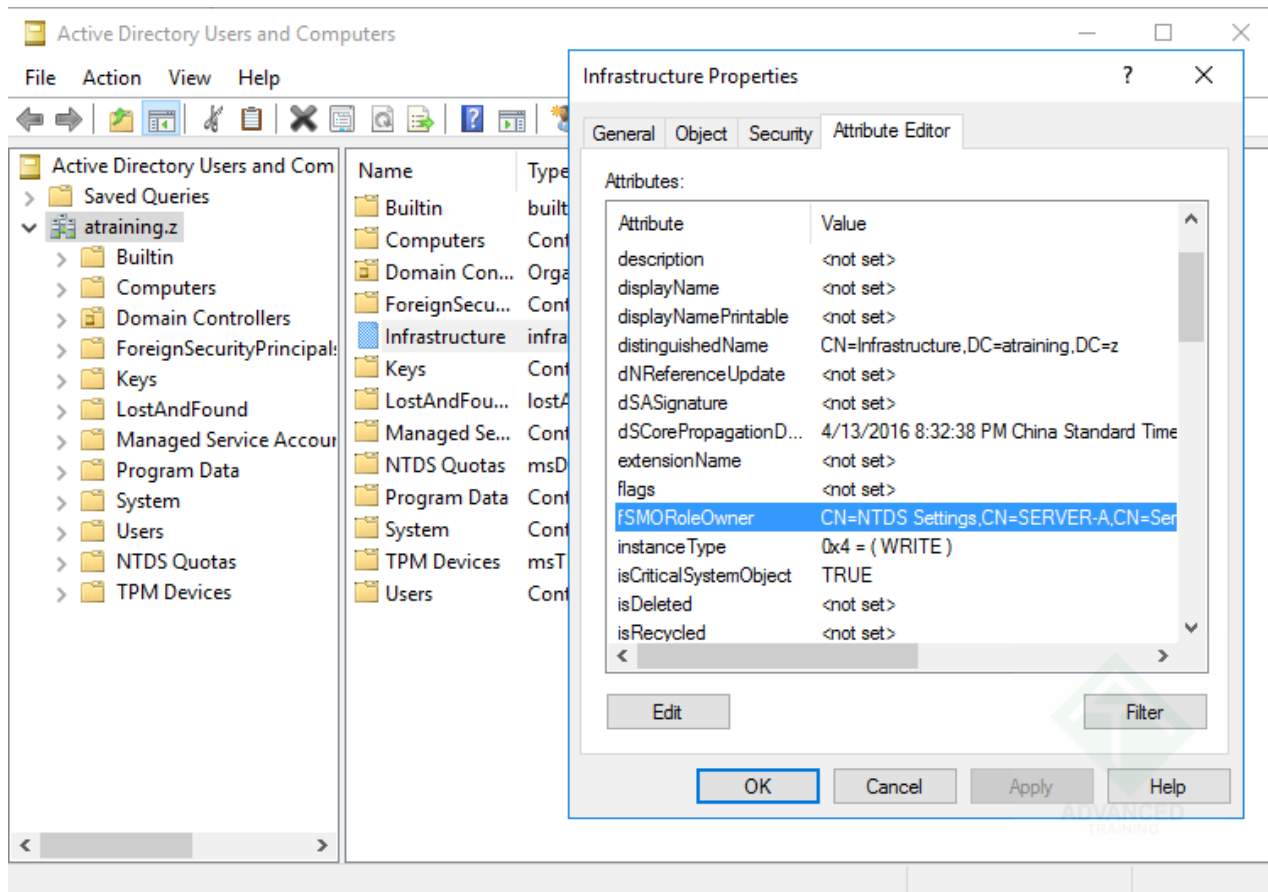
Изначально Infrastructure Master'ом назначается первый DC в первом домене леса – это штатно изменяемо как утилитой ntdsutil, так и через оснастку Active Directory Users and Computers. Открываем оснастку, далее – правой кнопкой по корню домена и выбираем Operations Masters:



[Перенос роли Infrastructure Master](#)
([кликните для увеличения до 400 px на 455 px](#))

Где хранится информация, кто сейчас Infrastructure Master?

Данные о том, кто сейчас в домене держит FSMO-роль Infrastructure Master, содержатся в атрибуте **fSMORoleOwner** объекта **CN=Infrastructure**, находящегося в корне доменного NC:



[Как определить, кто сейчас Infrastructure Master в домене](#)
(кликните для увеличения до 752 px на 529 px)

Где располагать владельца FSMO-роли Infrastructure Master?

С данной ролью связано специфичное требование по расположению – владелец FSMO-роли не должен находиться на DC, на котором работает GC. Если это требование не соблюдается, в логи периодически пишется ошибка номер 1419. Суть конфликта проста – Infrastructure Master забывает на выполнение служебных обязанностей по походу к GC за новостями про phantom object'ы, если сам является GC. Безусловно, эта проблема легко игнорируется что в ситуации “один лес, один домен”, что в ситуации “несколько доменов, но работаем по NT 4.0-стилю – просто логинимся на сервисы другого домена в нашем лесу местными учётками”, что в ситуации “несколько отдельных лесов в организации, чтобы максимальный уровень безопасности и изоляции” – но по сути, она есть, и игнорировать её можно стало только после выхода NT 6.1, когда появился Active Directory Recycle Bin. Если ваша ситуация подпадает под “нет возможности включить Active Directory Recycle Bin на уровне леса”, то вам надо при поиске правильного расположения Infrastructure Master учитывать, что лучший выход – это отдельный DC без функции GC. Проще всего – дополнительный в каком-то сайте в центре топологии, чтобы пара GC была рядом с ним в его же сайте.

Как повысить надёжность работы Infrastructure Master?

Разве что предоставить ему, как написано в совете выше, как минимум 2 GC в его сайте – чтобы при отказе одного на момент наступления времени “пора проверять phantom object’ы” был доступен другой.

Как повысить безопасность работы Infrastructure Master?

Тут вопрос сложный, потому что его работой никак особо не поуправлять, за исключением единственной настройки. В общем, не давать никому лишних административных прав.

“Если Infrastructure Master упал то всё”

Благодаря тому, что процентов этак 100% сдававших MCSE по дампам, или купившим этот статус в центрах тестирования при авторизованных учебных центрах (или, как это популярно, в специальных “внутренних” центрах тестирования у крупных системных интеграторов), просто не понимают, что делает эта FSMO-роль, то рождаются мистические мифы “если IM в дауне, то в домене вся инфраструктура по сути не работает”. Детали “всей инфраструктуры, которая не работает” обычно скрываются и заменяются томно-мудрым взглядом с прищуром аля “кто в теме, тот понимает”.

По факту же в куче ситуаций – что “один лес с одним доменом”, что “включили Active Directory Recycle Bin”, данная роль вообще не работает. В случае же, если с IM реально проблемы, всё фиксируется достаточно просто – выбирается и поднимается новый. Время на это есть приличное – по умолчанию он пробегает таблицу раз в 2 суток.

Зависит ли скорость работы доменов и репликации от расположения Infrastructure Master?

Нет. Чисто в теории, можно сделать очень большие группы с кучей “иностранных” участников, и расположить Infrastructure Master’а в дальнем-дальнем сайте, чтобы он добирался до ближайшего GC на вертолёте, а после – на собачьей упряжке, но ситуация эта исключительно синтетическая.

Нужен ли Infrastructure Master’у отдельный бэкап?

Нечего бэкапить – таблицы phantom object’ов, как и написано выше, несмотря на распространяемые мифы, есть у каждого DC – просто IM тот, кто их регулярно просматривает на предмет соответствия реальной обстановке. У данного владельца FSMO-роли нет локально хранимой уникальной информации.

В заключение

С инфраструктурным мастером всё тоже несложно – так что надеюсь, что ещё часть фантазий и мистификаций уступила свой участок фронта знаниям.

До встречи!