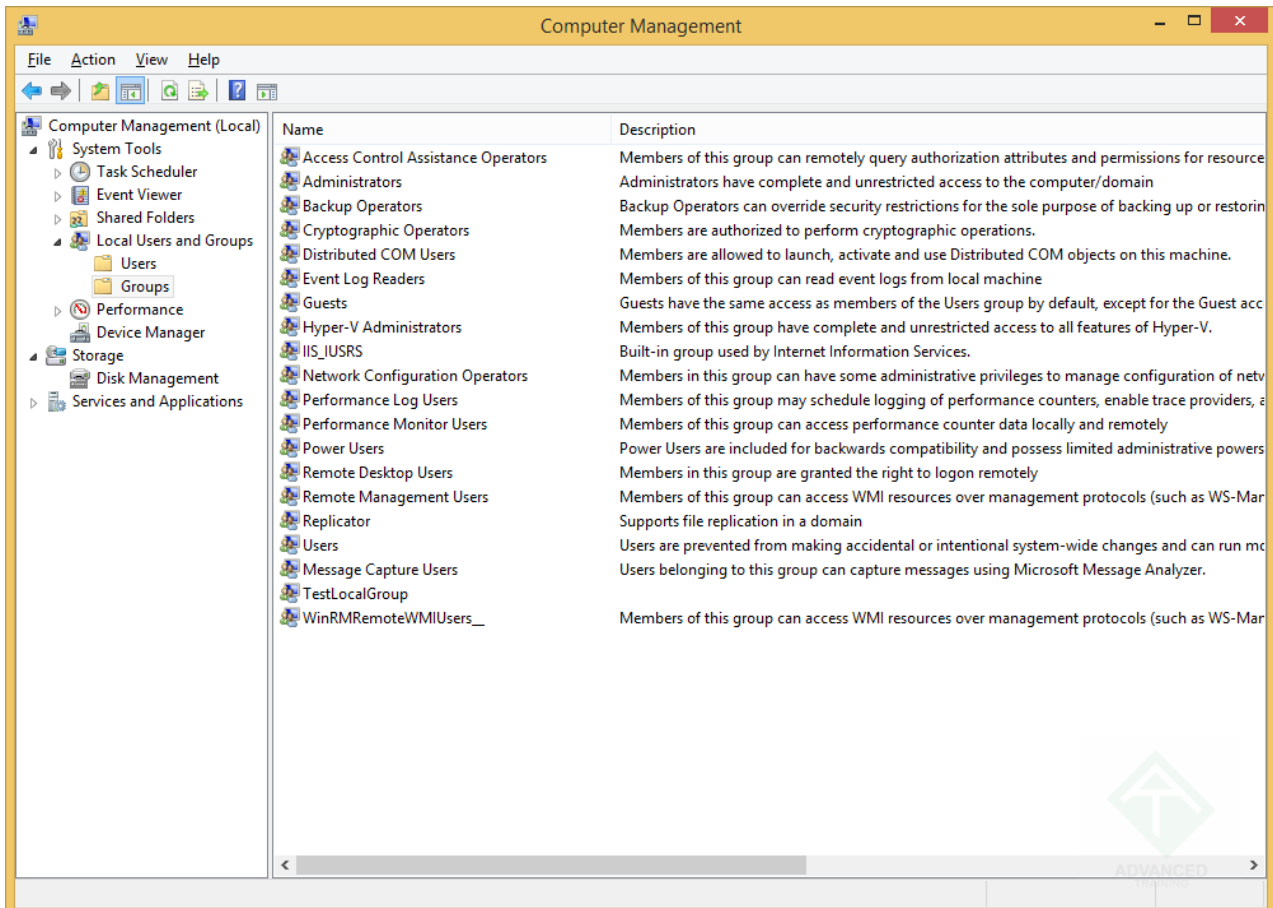


Local и Domain Local, Global и Universal, Security и Distribution - вокруг них много фантазий и мифов. Разбираемся.

 atraining.ru/groups-windows-nt-active-directory-explained

2016-05-04T13:25:44+08:00



Для человека, который сталкивается с многообразием групп в Active Directory, разобраться с ними сходу весьма трудно. Local и Domain Local, Global и Universal, Security и Distribution – всё это осложняется ситуацией “кого в кого можно включать”, и в финале сопровождается выводом “нафиг столько нагородили, уму непостижимо”. Добавляет к этому бардаку сочности то, что в фирменных курсах Microsoft данная тема освещается всё обзорнее и обзорнее – и сводится буквально к паре слайдов “запомните вот эту табличку”, без объяснения причин того, почему всё работает именно так.

Такой подход понятен – задача Microsoft – максимально удешевить чтение курсов, снижая требования по знаниям у [MCT](#), которые обычно сами не могут объяснить, почему с группами в Windows / Active Directory всё сложилось именно так. Нужен меньший уровень знаний, чтобы вслух ртом начитывать сверху вниз слайды – можно меньше платить – ниже расходы – выше прибыль у партнёров Microsoft – больше партнёров – больше прибыли Microsoft. Приводит это к предсказуемому результату – тему “проскакивают” на бегу с логикой “зазубрите табличку, потом

дампс почитаете чуток и проходной балл на экзамене кое-как перевалите, да вообще всё это некритично на самом деле”, а после работают с группами наощупь, а-ля “я на форуме читал, что всё надо делать security global, а у distribution SID’a вообще нет, ко-ко-ко”, ну и с подобными мифами. Табличка “кого в куда включать можно”, будучи не понятой, быстро забывается, а вся тема остаётся мистическим облачком “ой там всё мутно, нереально разобраться, да и не нужно никому”.

Как обычно, у нас подход другой. Разберёмся, что и как с группами. Вам понадобится базовая подготовка на уровне материала курса [Microsoft 20410D](#) – можете [скачать бесплатно его запись](#) у нас и посмотреть, там несложно.

Группы Windows NT и Active Directory – что, зачем, как, почему

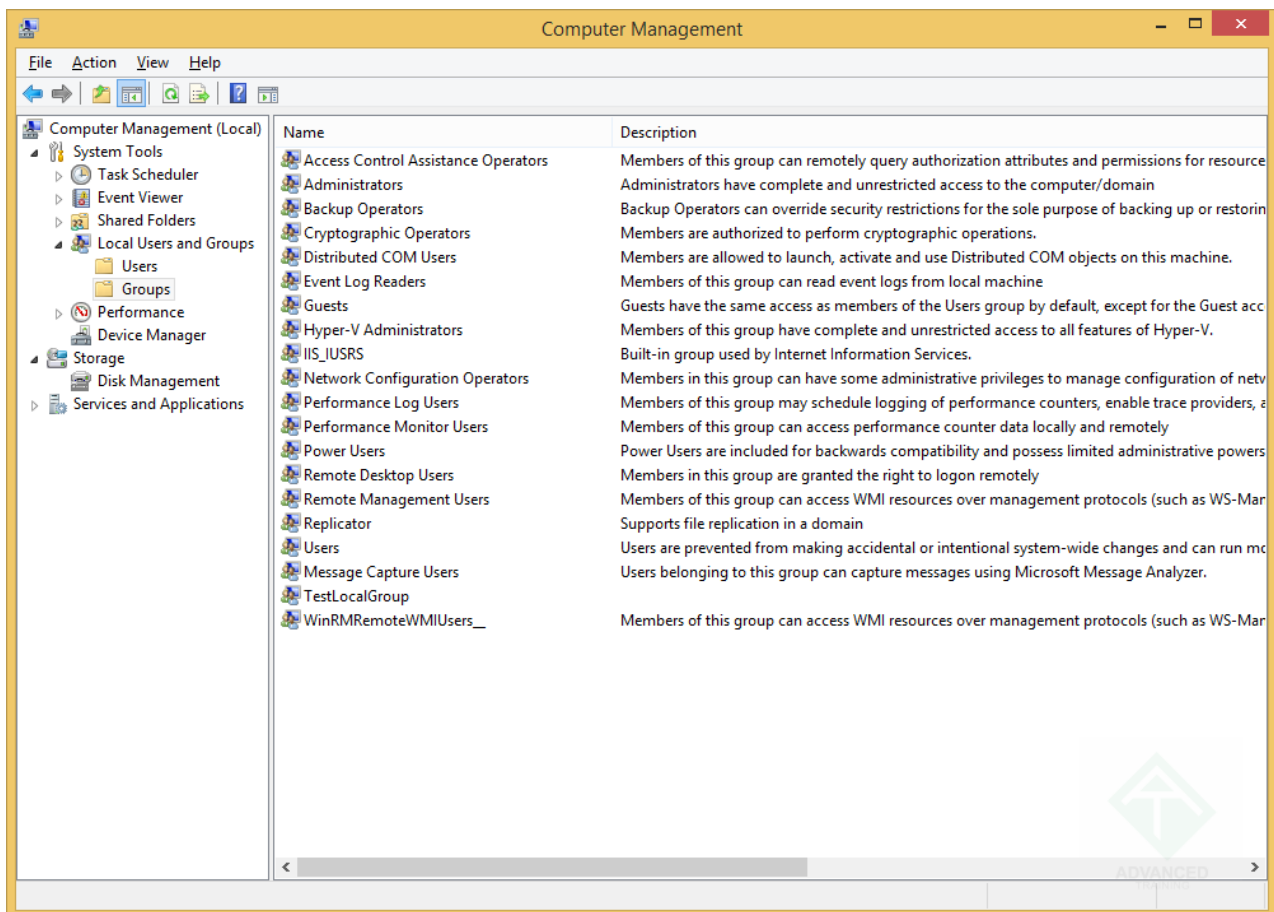
- Часть первая – изначальная ситуация – одиночная система
- Часть вторая – домен Windows NT – появление Domain Local и Security-групп
- Лирическое отступление про максимальное количество групп и прочие технические мелочи
- Поведение системы при переполнении маркера доступа
- Часть третья – лес Active Directory – появление Universal-групп и разделения на Security и Distribution
- Universal-группы и режимы работы домена
- Можно ли жить в лесу Active Directory без Universal-групп, только с Global и Domain Local
- Проблемы масштабирования при использовании только Global и Domain Local
- Domain Local-группы и объекты Active Directory
- Миф про сниженное быстроедействие Universal-групп
- Миф про одинаковость всех групп, потому что их можно друг в друга переключать

Приступим.

Часть первая – изначальная ситуация – одиночная система

Группы, как объекты, являющиеся участниками системы безопасности – т.н. “security principal” – появились в Windows NT изначальным. Так же как и пользователи, группы имеют свой личный и уникальный в пределах системы идентификатор – SID (про них можно поподробнее почитать в [статье про FSMO-роль RID Master](#)).

Однако, даже на единичной системе групп уже есть два вида – это встроенные, например `BUILTIN\Administrators`, и дополнительно созданные – в моём случае это группа `TestLocalGroup` и некоторые другие:



[Локальные группы на Windows 8.1](#)

[\(кликните для увеличения до 1000 px на 715 px\)](#)

Как отличить эти два типа групп? Исключая, конечно, то, что мне было лень писать description к тестовой группе, и она выделяется по этому признаку? Всё просто – у этих двух типов групп разные форматы SID'ов:

```

Administrator: Windows PowerShell

PS C:\Windows\system32> Get-WmiObject -Class Win32_Group | Format-Table -Property Name,SID

Name                               SID
----                               -
Access Control Assistance Operators 5-1-5-32-579
Administrators                      5-1-5-32-544
Backup Operators                    5-1-5-32-551
Cryptographic Operators              5-1-5-32-569
Distributed COM Users                5-1-5-32-562
Event Log Readers                    5-1-5-32-573
Guests                              5-1-5-32-546
Hyper-V Administrators               5-1-5-32-578
IIS_IUSRS                           5-1-5-32-568
Network Configuration Operators      5-1-5-32-556
Performance Log Users                5-1-5-32-559
Performance Monitor Users            5-1-5-32-558
Power Users                          5-1-5-32-547
Remote Desktop Users                 5-1-5-32-555
Remote Management Users              5-1-5-32-580
Replicator                           5-1-5-32-552
Users                               5-1-5-32-545
Message Capture Users                5-1-5-21-3369640497-176770125-935461305-1002
TestLocalGroup                      5-1-5-21-3369640497-176770125-935461305-1003
WinRMRemoteWMIUsers__               5-1-5-21-3369640497-176770125-935461305-1000

PS C:\Windows\system32>

```

[Просмотр SID у локальных групп - разница между builtin и обычными группами](#)

[\(кликните для увеличения до 877 px на 451 px\)](#)

У встроенных это будет **S-1-5-32-abc**, где abc – идентификатор от 500 до 1000 (в теории, в реальности полтыщи встроенных групп в системе нет, их меньше полусотни). У обычных это будет **S-1-5-21-yyy-zzz**, где YYY – это идентификатор системы (его меняет, например, утилита **sysprep**), а ZZZ – это [RID](#).

Встроенные группы будут стоять особняком – они нужны для предоставления прав учётным записям, исключительно – т.е. ни включать их друг в друга (эта операция будет называться **group nesting**), ни включать в них обычные локальные группы будет нельзя. Вы можете убедиться в этом, запросив на локальной системе список тех, кто может быть добавлен во встроенную группу:

Select Users



Select this object type:

Users or Built-in security principals

Object Types...

From this location:

ATRAINING-DEMO

Locations...

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

Days since last logon:

Columns...

Find Now

Stop



OK

Cancel

Search results:

Name	In Folder
Administrator	ATRAINING-DEMO
ALL APPLICATION PACKAGES	
ANONYMOUS LOGON	
Authenticated Users	
BATCH	
CONSOLE LOGON	
CREATOR GROUP	
CREATOR OWNER	
DIALUP	
Everyone	
Guest	ATRAINING-DEMO
INTERACTIVE	
IUSR	
Local account	
Local account and member of Administrators group	
LOCAL SERVICE	
NETWORK	
NETWORK SERVICE	
OWNER RIGHTS	
REMOTE INTERACTIVE LOGON	
Ruslan	ATRAINING-DEMO
SERVICE	
SYSTEM	
TERMINAL SERVER USER	
This Organization Certificate	



В builtin-группу сможем добавить только учётку пользователя или техническую - обычную группу не сможем
(кликните для увеличения до 529 px на 870 px)

Если что, **ATRAINING-DEMO** – это имя локальной машины, это обычная Windows 8.1, разве что на ней заведена учётка пользователя с именем **Ruslan**.

Т.е. задача этих групп – выдавать права тем или иным локальным **пользователям** или обладателям каких-то специфичных SID'ов в nt-маркере доступа – например, logon type'ов типа **NETWORK** или **INTERACTIVE**.

Возможность же создавать свои собственные группы на локальной машине нужна, чтобы предоставлять доступ к ресурсам – например, общим папкам. Вы можете создавать группы, и включать в них пользователей. Ранее, замечу, можно было включать локальные группы в локальные – для этого трюка нужна утилита **net.exe** и её контекст **LOCALGROUP**, но на данный момент этот функционал заблокирован и даже если вы сделаете так на NT 4.0 и проапгрейдите систему до современной версии, то все равно – **lsass** учитывает у локальных пользователей только группы, в которые они включены напрямую, т.е. в маркере доступа других групп не будет.

Зачем же в этой ситуации, когда можно было бы обойтись, по сути, простым критерием “RID меньше тысячи – значит, встроенная группа – а больше – значит, созданная пользователем”, делать разные форматы SID'ов? Нужно это было для того, чтобы обеспечить перенос ACL'ов между системами. Пример – у вас есть внешний диск, отформатированный в NTFS. Вы создаёте там структуру папок и назначаете права – в эту папку можно участникам группы **Administrators**, в эту – обычным **Users**. Если вы перенесёте этот диск на другую систему, то все ACL'ы будут читаемы – потому что SID'ы что **Administrators**, что **Users** – одинаковы у любой NT-системы. Но если вы создадите свою собственную группу, то такого никогда не случится – её SID никогда не совпадёт с SID'ом группы на другой системе, потому что включает компонент **S-1-5-21-уникальный идентификатор системы-RID**. Поэтому если вы создадите у себя локальную группу **Special Secret Administrators**, а на соседней машине создадут **Puny Faggots**, то неприятной ситуации, когда добавляли права доступа для участников первой, а при переносе оказалось, что права доступа появились у второй, т.к. SID'ы совпали – вот такой ситуации не будет в принципе.

У пользователей, замечу, такого разделения нет – они всегда привязаны к идентификатору системы:

```
Administrator: Windows PowerShell

PS C:\Windows\system32> Get-WmiObject -Class Win32_Group | Format-Table -Property Name,SID

Name                SID
----                -
Access Control Assistance Operators S-1-5-32-579
Administrators       S-1-5-32-544
Backup Operators     S-1-5-32-551
Cryptographic Operators S-1-5-32-569
Distributed COM Users S-1-5-32-562
Event Log Readers    S-1-5-32-573
Guests               S-1-5-32-546
Hyper-V Administrators S-1-5-32-578
IIS_IUSRS            S-1-5-32-568
Network Configuration Operators S-1-5-32-556
Performance Log Users S-1-5-32-559
Performance Monitor Users S-1-5-32-558
Power Users          S-1-5-32-547
Remote Desktop Users S-1-5-32-555
Remote Management Users S-1-5-32-580
Replicator           S-1-5-32-552
Users                S-1-5-32-545
Message Capture Users S-1-5-21-3369640497-176770125-935461305-1002
TestLocalGroup       S-1-5-21-3369640497-176770125-935461305-1003
WinRMRemoteWMIUsers__ S-1-5-21-3369640497-176770125-935461305-1000

PS C:\Windows\system32> Get-WmiObject -Class Win32_UserAccount | Format-Table -Property Name,SID

Name                SID
----                -
Administrator       S-1-5-21-3369640497-176770125-935461305-500
Guest                S-1-5-21-3369640497-176770125-935461305-501
Ruslan               S-1-5-21-3369640497-176770125-935461305-1001

PS C:\Windows\system32>
```

[В builtin-группу сможем добавить только учётку пользователя или техническую - обычную группу не сможем](#)
([кликните для увеличения до 877 px на 487 px](#))

Что ж, с локальной системой всё ясно и несложно. Теперь – следующий шаг – появляется домен Windows NT.

Часть вторая – домен Windows NT – появление Domain Local и Security-групп

Работа с группами в одиночной системе – штука простая. Сложности появляются, когда надо создать свой **authentication domain** – т.е. подмножество систем, которые признавали бы не только свои локальные базы security principal'ов (хранящиеся в реестровой ветке **HKLM\SAM\SAM**), но и некую центральную и общую БД учётных записей.

Если вы берёте систему на базе Windows Server и делаете её контроллером домена – т.е. говорите, что теперь её хранилище security principal'ов будет общим, и ему будут доверять другие системы – она понимает возложенную ответственность и решается на апгрейд своего Security Accounts Manager'a. Ведь одно дело, когда предполагается использование базы только на одной системе – а другое дело, когда на нескольких. Плюс, домены могут доверять друг другу через систему domain trust'ов – а, следовательно, надо ещё и учитывать то, что должна обеспечиваться уникальность security principal'ов в пределах произвольного числа доменов.

Если просто взять и сделать общим SAM локальной машины – сразу появятся конфликты тех же builtin-групп; например, как при идентичных SID'ах группы **BUILTIN\Administrators** на всех системах сделать свой SAM доступным для остальных? Что будет обозначать запись в маркере доступа на произвольной, включённой в домен, машине “входит в группу с SID = S-1-5-32-544” – это значит,

что участник локальных Administrators или общих-доменных Administrators? Как решать ситуации с “из соседнего домена придёт группа с таким же SID’ом”? Ситуация требовала и расширения функционала, и введения ограничений – и это произошло.

Было сделано следующее – существующая ситуация со встроенными и обычными группами была усложнена до “Есть два ~~есть~~ вида групп – локальные для этого домена (Domain Local) и глобальные с возможностью ‘выхода наружу’, за пределы домена (Global)”. У Domain Local при этом остаётся разделение на BUILTIN, т.е. встроенных и изначально существующих в домене, и обычных, созданных администраторами. Было два типа групп – стало два с половиной – локальные встроенные, локальные обычные, и глобальные.

Новый тип групп, Global, сразу же был ограничен до “в него могут входить только учётки”. Вложения однотипных групп (т.е. Global в Global) в домене Windows NT не было, поэтому всё, зачем нужны Global-группы – собрать в них ресурсы по какому-либо критерию (например, подразделение организации) и добавить эту группу в чей-нибудь ACL. Например, у папки, или у принтера. У любого объекта NT-системы, в общем. Простой пример – сделать группу BUN, добавить туда учётки всех сотрудников бухгалтерии и выдать этой группе права на папку Otchet2016 на файл-сервере.

Существующий подтип Builtin Local получил ограничение – в силу того, что SID’ы его участников не содержат доменный компонент, групп этого типа не видно при просмотре с рабочих станций и серверов домена. То есть, если в домене есть рабочая станция, и у неё есть своя локальная группа **Administrators**, то конфликт с имеющимися на контроллере домена **BUILTIN\Administrators** разрешается просто – что в локальную группу на этой рабочей станции, что в любой ACL на любом объекте на этой рабочей станции – добавить доменных **BUILTIN\Administrators** не выйдет, их просто не будет видно. Выборка по “потенциально возможным к добавлению” не покажет Builtin Local’ов. Они существуют только на системах, которые разделяют между собой “выросший” локальный SAM самого первого сервера, который стал контроллером этого домена – то есть, на контроллерах домена.

Domain Local же, как наследники “обычных локальных групп”, данного ограничения не имеют – их SID ведь содержит компонент с идентификатором домена – а, следовательно, уникальность в сравнении с локальными группами каждой входящей в домен системы поддерживается. Поэтому вы можете добавить, например, в локальную группу **Administrators** группу из домена, у которой будет тип Domain Local – никакого потенциального конфликта тут не будет. SID’ы этих групп, кстати, не поменялись при превращении сервера в первый контроллер домена в новом домене – поэтому если вы, например, создали локальную группу и выдали ей права на какой-то папке, то после DC promotion эта группа станет Domain Local и все её права сохранятся – ведь SID тот же.

В итоге ситуация стабильна – каждый домен обладает уникальным идентификатором, есть специальный тип групп, у которых в SID'е всегда этот уникальный идентификатор есть (Global). Назначение групп тоже понятно – в Global добавляем учётки с прицелом “им можно хоть где угодно права раздавать, хоть в другом домене”, Domain Local используем для групп-заглушек на ресурсах, вида “SRV1 Buh-Otchet2016 RO” (Read-Only на общей папке \\srv1\BUH\Otchet2016).

Но потребности растут – и ситуация изменяется ещё раз.

Лирическое отступление про максимальное количество групп и прочие технические мелочи

Возможность создавать много групп и делать сложные схемы вложения одних в другие, безусловно, технически ограничена. В части ограничения количества объектов типа “группа” в домене всё упрётся в размер хранилища NTDS в Active Directory, а также в [максимально возможное количество RID'ов в данном домене](#). Оба этих барьера трудно достижимы – наштамповать миллиарды групп всё ж задача не из бытовых. Но есть ограничение, которое достигнуть можно – это вопрос про “во сколько групп может входить пользователь”.

Ответ на этот вопрос, за время развития Active Directory, несколько раз изменялся – давайте разберёмся, почему и как.

Первичное техническое ограничение на количество групп, в которых одновременно может состоять конкретный пользователь, вызвано тем, что при логине с использованием протокола Kerberos (его поддержка появляется в Windows NT 5.0 и в Active Directory с момента её создания) будет необходимо передавать по сети сведения о членстве доменного пользователя в группах. Протокол Kerberos по умолчанию работает с использованием транспортного протокола UDP (впрочем, переключаем на TCP начиная с Windows 2000), и теоретически возможный размер Kerberos-данных – это максимальный размер UDP-датаграммы минус заголовок пакета Kerberos. Получается чуть меньше 64КБ (65.5 тысяч байт). Вычитаем минимальный размер маркера доступа (это 1200 байт – это минимум, размер может быть чуть больше, если будет, например, очень длинный FQDN или UPN/SPN). Получаем примерно 62КБ (где-то 63 тысячи байт). Учитываем, что при работе с веб-сервисами, тем же IIS, использующим при работе метод Negotiate, содержимое токена надо будет передавать по HTTP, в Base64 (т.е. упаковывать всё в 6ти битовые символы). В результате получим уменьшение технологически возможного размера до примерно 47КБ (около 48 тысяч байт). Это, повторюсь, техническое ограничение при условиях:

- Наш Kerberos работает по UDP;
- Мы используем Negotiate в IIS как метод авторизации доменных учётных записей;
- Мы не тюнингуюем Kerberos в плане доп.информации в заголовке и у нас учётка с нормальным именем (или хост с тривиальным по габаритам FQDN);

Поэтому операционная система, в частности встроенный в неё модуль поддержки Kerberos, имеет настройку, ограничивающую максимальный размер содержимого. Исторически этот размер, появившись в Windows 2000, был 8.000. В Windows 2000 Service Pack 2 он стал 12.000, а с Windows Server 2012 – 48.000. Вы можете его поправить, если что, простой настройкой параметра **MaxTokenSize**, который сейчас уже есть в стандартных групповых политиках (я предполагаю, что вы обновляете административные шаблоны у себя в домене):

Set maximum Kerberos SSPI context token buffer size

Set maximum Kerberos SSPI context token buffer size

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options: Maximum size 12000

Help:

This policy setting allows you to set the value returned to applications which request the maximum size of the SSPI context token buffer size.

The size of the context token buffer determines the maximum size of SSPI context tokens an application expects and allocates. Depending upon authentication request processing and group memberships, the buffer might be smaller than the actual size of the SSPI context token.

If you enable this policy setting, the Kerberos client or server uses the configured value, or the locally allowed maximum value, whichever is smaller.

If you disable or do not configure this policy setting, the Kerberos client or server uses the locally configured value or the default value.

Note: This policy setting configures the existing MaxTokenSize registry value in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters, which

OK Cancel Apply

[Размер токена MaxTokenSize](#)

[\(кликните для увеличения до 686 px на 636 px\)](#)

Находится она, если что, в **Computer Configuration \ Policies \ Administrative Templates \ System \ Kerberos**, а называется **Set maximum Kerberos SSPI context token buffer size**. Учитывайте только, что это – именно максимальный размер самого **содержимого** токена, а не токена в смысле “весь керберовский пакет”. Кстати, на KDC – т.е. на всех контроллерах – можно также выставить полезную настройку “журналировать события, когда токен не влез в указанные размеры”:

Warning for large Kerberos tickets

Warning for large Kerberos tickets

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options: Ticket Size Threshold 12000

Help: This policy setting allows you to configure at what size Kerberos tickets will trigger the warning event issued during Kerberos authentication. The ticket size warnings are logged in the System log.

If you enable this policy setting, you can set the threshold limit for Kerberos ticket which trigger the warning events. If set too high, then authentication failures might be occurring even though warning events are not being logged. If set too low, then there will be too many ticket warnings in the log to be useful for analysis. This value should be set to the same value as the Kerberos policy "Set maximum Kerberos SSPI context token buffer size" or the smallest MaxTokenSize used in your environment if you are not configuring using Group Policy.

If you disable or do not configure this policy setting, the threshold value defaults to 12,000 bytes, which is the default Kerberos MaxTokenSize for Windows 7, Windows Server 2008 R2 and prior versions.

OK Cancel Apply

[Журналирование на KDC событий превышения максимального размера Kerberos-токена](#)

[\(кликните для увеличения до 686 px на 636 px\)](#)

Находится она рядом с предыдущей в **Computer Configuration \ Policies \ Administrative Templates \ System \ KDC**, называется **Warning for large Kerberos tickets**.

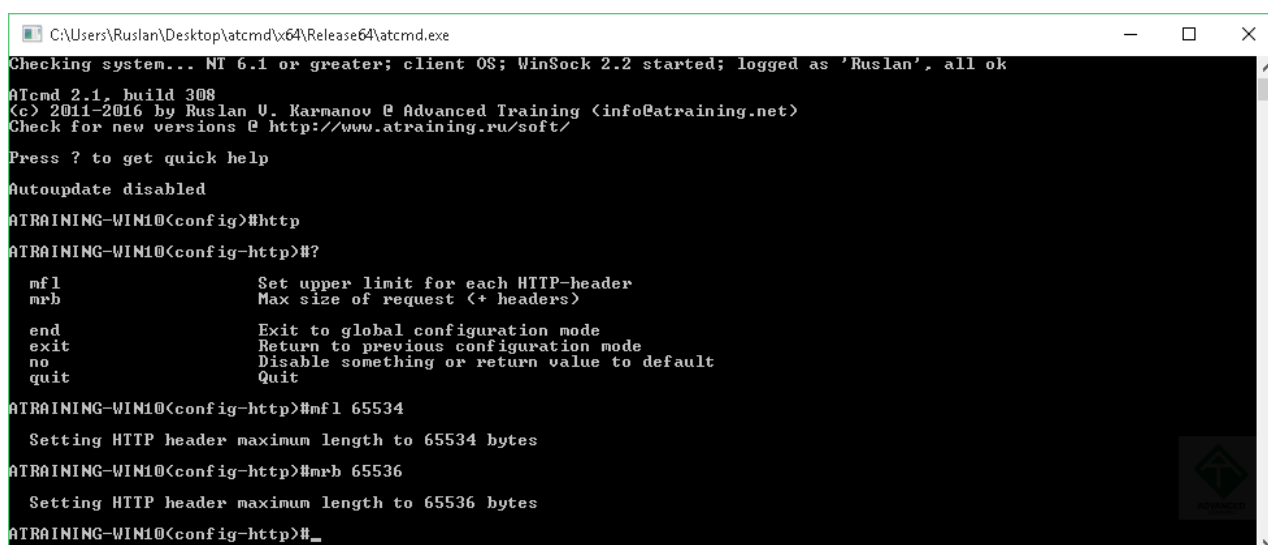
Теперь добрались до связи всего этого с группами. Каждая запись о том, что данный security principal состоит в группе, занимает место. Больше всего места занимает запись о членстве в Domain Local-группе и в Universal-группе из чужого домена (об Universal чуть далее) – 40 байт. Запись о членстве в Global или Universal-группе своего домена занимает 8 байт. Используя эти данные, можно прикинуть, в каком количестве групп может состоять пользователь – это будет или 1200 Domain Local-групп, или 6000 Global-групп, или хз сколько Universal (зависит от того, из того же они домена, что и вы, или нет).

Но это будет ещё не очень точной прикидкой, потому что есть дополнительные факторы, влияющие на содержимое маркера доступа:

- SID History – если учётная запись мигрировала из другого домена, и этот атрибут не пустой, а содержит SID'ы групп из предыдущего домена, то они тоже занимают место в маркере;
- Delegation – если учётка trusted for delegation, то теоретический максимум можно делить пополам, т.к. в маркере будет 2 комплекта SID'ов;

Чтобы не замучаться поддерживать весь этот дремучий лес из различных ситуаций “много групп или не очень”, Microsoft выпустила статью про жёсткое ограничение количества групп до [1.015](#), и посоветовала не превышать число в 1.010 (хотя, как видно из вычислений, количество может быть в разы больше). Ситуация на некоторое время успокоилась – для спокойной работы можно выставить на уровне домена **MaxTokenSize** в 48.000 и не иметь никаких проблем (ещё лучше форсировать Kerberos на TCP-вариант, чтобы не наткнуться на ограничения размера UDP-датаграммы).

Помимо этого, в случае проблем с работой веб-сервисов, возможно, понадобится увеличить максимальный размер одиночного поля в HTTP-заголовке и одиночного запроса. По умолчанию они оба 16К, имеет смысл увеличить их хотя бы до 64К – это решит проблемы с ситуацией “большой маркер доступа и сбой 401.1 при авторизации на IIS” и в подобных:



```

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 308
(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)#http
ATRAINING-WIN10(config-http)#?
  mfl          Set upper limit for each HTTP-header
  mrb          Max size of request (+ headers)
  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-http)#mfl 65534
  Setting HTTP header maximum length to 65534 bytes
ATRAINING-WIN10(config-http)#mrb 65536
  Setting HTTP header maximum length to 65536 bytes
ATRAINING-WIN10(config-http)#_
  
```

[Размер HTTP-заголовка и запроса](#) ([кликните для увеличения до 979 px на 415 px](#))

Данная ситуация была стабильна до Windows Server 2012, в котором появилось сжатие токена – механизм Resource SID Compression.

Идея данного механизма чрезвычайно проста – “давайте от Domain Local-групп передавать только RID'ы”. Данным механизмом можно управлять, включая-выключая его для каждого конкретного DC:

```
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 308
(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)#kerberos kdc
ATRAINING-WIN10(config-k Kerberos-kdc)#?
  backofftime      KDC backoff time
  dontcheckaddr    KDC do not check IP in client's AS_REQ into Caddr field
  fartimeout       Far KDC timeout
  maxreplysize     Max datagram reply size
  neartimeout      Near KDC timeout
  newcontimeout    New connection timeout
  sendretries      KDC retries
  sidcompress      Enable SID compression
  useclientaddr    Add KDC IP in AS_REQ into Caddr field
  waittime        KDC wait time

  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-k Kerberos-kdc)#sidcompress
  Resource SID Compression enabled
ATRAINING-WIN10(config-k Kerberos-kdc)#end
ATRAINING-WIN10(config)#sh kerberos kdc
  Wait time 10 sec
  Backoff time 10 sec
  Send retries count is 3
  KDC timeouts
    far 10 minutes
    near 30 minutes
  KDC use client IP address: Implicitly disabled, and don't check it: Implicitly enabled
  New incoming connections timeout: 10 sec
  Max accepted datagram size: 1465 bytes
  Resource SID Compression: Enabled
ATRAINING-WIN10(config)#_
```

[Настраиваем Resource SID Compression в Windows Server 2012 и старше \(кликните для увеличения до 979 px на 677 px\)](#)

Отключать его вам понадобится разве что в случае проблем с взаимодействием с не-Windows системами, которые не понимают схему сжатия SID'ов.

Технически (я не буду углубляться в дебри кербероса, это чрезвычайно интересная, но масштабная тема) всё реализуется несложно – если KDC поддерживает сжатие, то он проверяет бит **Resource-SID-compression-disabled** в поле **KerbSupportedEncryptionTypes** у своей учётки и у учётной записи **krbtgt**; если нигде этот бит не установлен в единицу, то KDC формирует маркер доступа, заполнив в структуре **KERB_VALIDATION_INFO** поле **ResourceGroupDomainSid** SID'ом текущего домена, и добавляя поле **ResourceGroupIds**, указывающее на массив “укороченных” SID'ов (которые на самом деле просто RID'ы). В финале в поле **ResourceGroupCount** пишется суммарное количество записей, и всё готово.

Использование этого механизма способно очень серьёзно снизить затраты места в токене – вместо 40 байт для Domain Local расход падает примерно до 6 байт на группу, плюс заголовок структуры.

Так что если у вас все DC на базе Windows Server 2012, и вы не выключили этот механизм, то токен будет компактнее.

Что же произойдёт, если всё ж SID'ов групп окажется столько, что они не влезут в маркер доступа?

Поведение системы при переполнении маркера доступа

Начиная с Windows Server 2003, есть “аварийный сценарий работы”, нужный для ситуации “я доблестно добавил единственного администратора в домене в тьму групп, и теперь не могу им залогиниться”. Чтобы спастись в этом случае, надо зайти в режиме “Safe mode with networking” на любой DC, используя **BUILTIN\Administrators** – аварийный сценарий работает только для неё, с RID’ом = 500 – в этом случае в маркер будут добавлены только группы, в которые явно входит эта учётная запись – без вложенных, плюс только BUILTIN и Domain Local. И если групп много даже в этом сценарии, то lsass просто не будет добавлять те из них, которые не влезли – при том, начнёт добавление с:

- Everyone (S-1-1-0)
- BUILTIN\Users (S-1-5-32-545)
- BUILTIN\Administrators (S-1-5-32-544)
- NT AUTHORITY\INTERACTIVE (S-1-5-4)
- NT AUTHORITY\Authenticated Users (S-1-5-11)
- LOCAL (S-1-2-0)
- Domain\Domain Users (S-1-5-21-aaaaaaa-bbbbbbbb-cccccccc-513)
- Domain\Domain Admins (S-1-5-21-aaaaaaa-bbbbbbbb-cccccccc-512)
- NT AUTHORITY\This Organization (S-1-5-15)

Такой маркер сгенерить точно получится и вход администратора в аварийной ситуации работает.

Надеюсь, я не сильно вас запутал, но, в общем, тема “во сколько групп может входить юзер”, как видно, весьма обширная и не ограничивается “в этой версии винды во столько, а в этой – во столько”, как иногда бездумно заучивают на авторизованных курсах Microsoft.

Продолжим про разновидности групп – статья вообще-то именно про это, а не про тонкости реализации Kerberos в современных версиях Windows Server.

Часть третья – лес Active Directory – появление Universal-групп и разделения на Security и Distribution

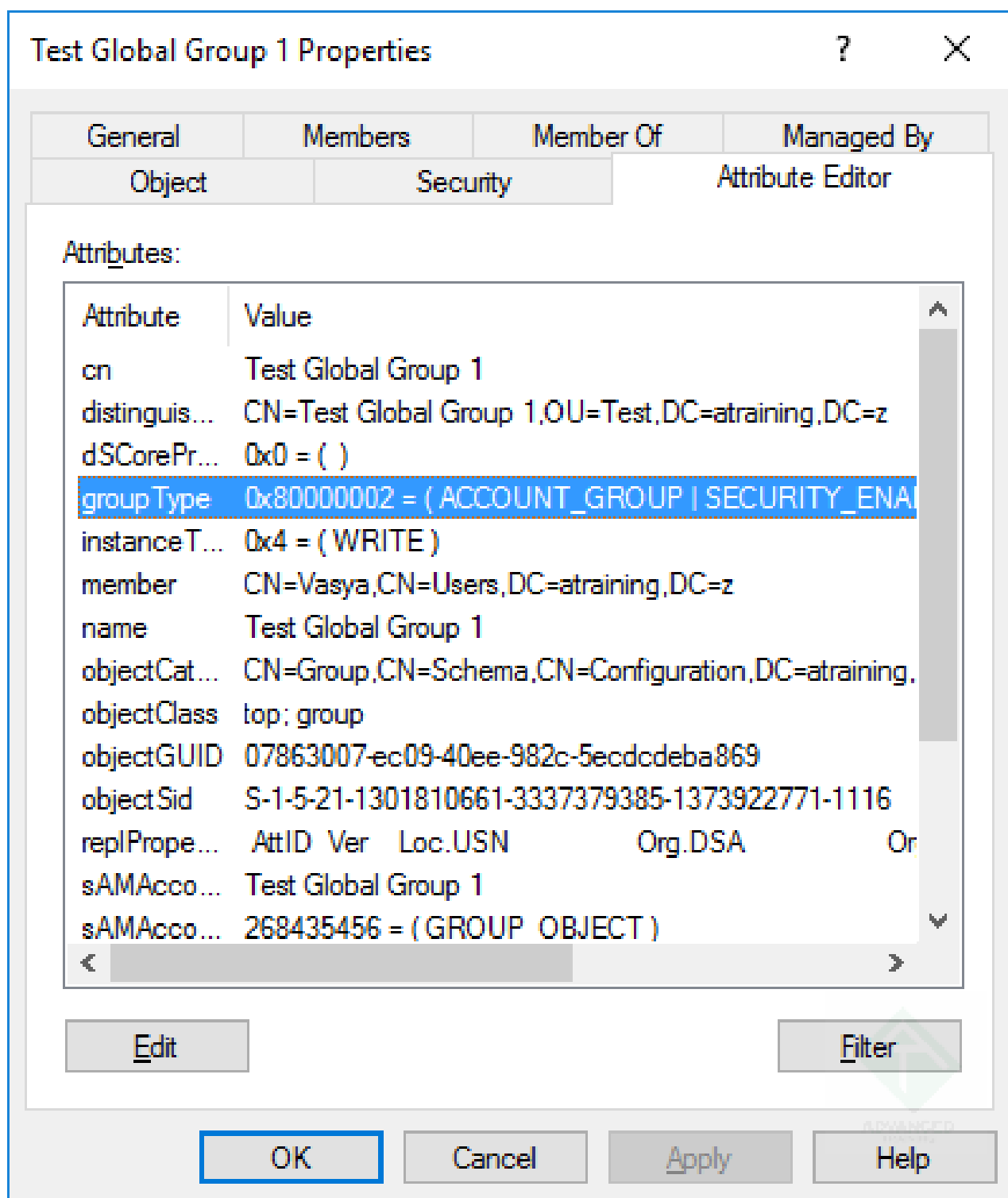
Active Directory добавляет целую пачку нового – теперь вместо одиночных доменов, связанных ниточками-трастами, есть пачки дружественных друг к другу доменов, называемые лесами. Появляется возможность изменять атрибуты объектов, хранимых в Active Directory, и создавать новые типы объектов. Все эти добавления нуждаются в изменениях в работе групп. Первым делом смотрим на новое разделение групп – на Security и Distribution.

Чем отличаются Security и Distribution группы

Миф про “у Distribution-групп нет SID’ов” – один из самых живучих. Его бездумно копируют преподаватели авторизованных курсов Microsoft, ни разу не работавшие с Active Directory в production и просто ни разу не интересовавшиеся, как оно вообще

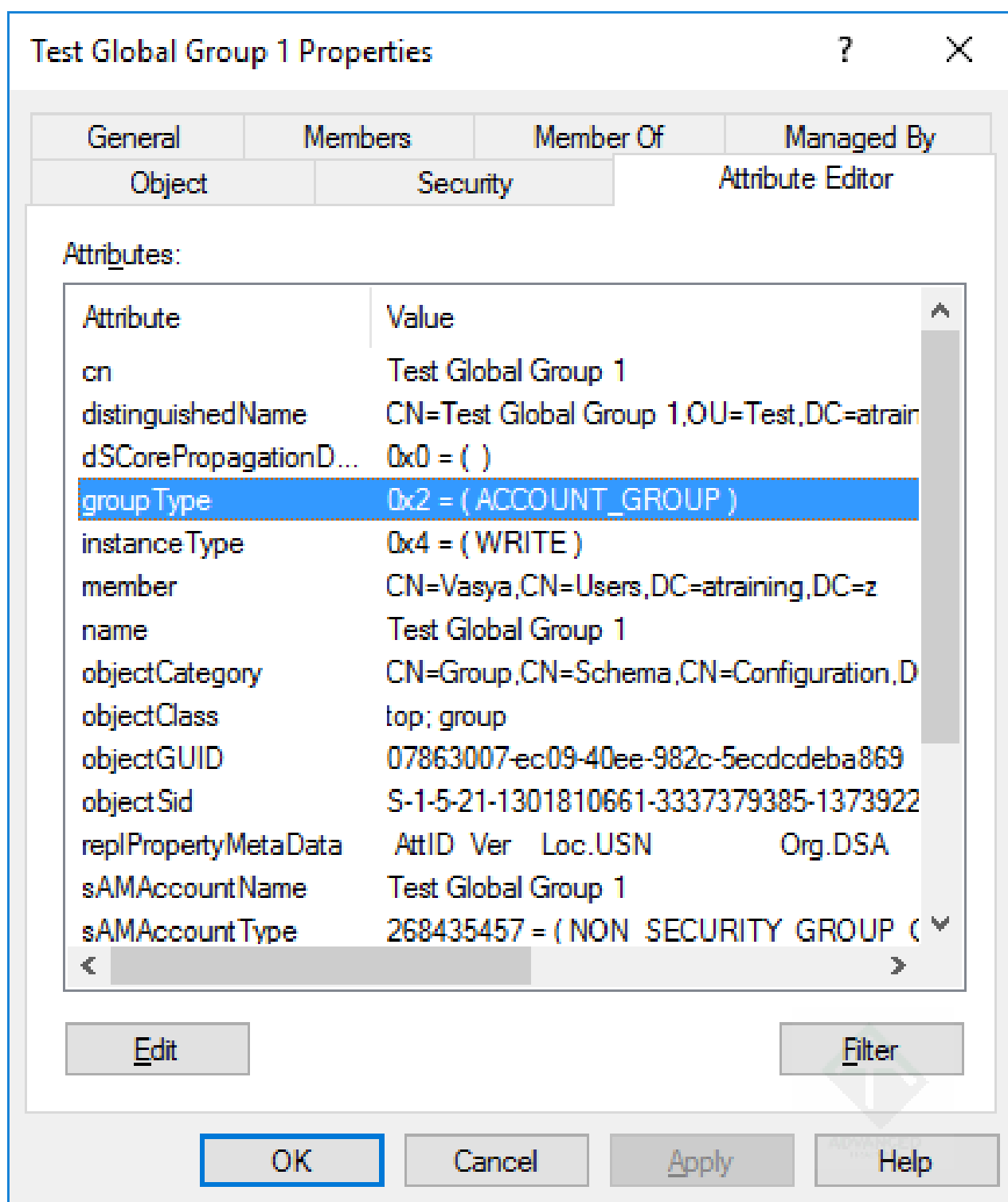
работает. Его копируют расплодившиеся в последнее время “архитекторы”, павшие жертвой подхода работодателей “давайте сисадмина Ваську переименуем в должности, чтобы зарплату не поднимать”. Его озвучивают набранные по критерию “амбициозный туповатый услужливый региональный сисадмин” сотрудники системных интеграторов, потому что “ребята из МС, эксперты, архитекторы, говорили”.

Технически же всё просто – Distribution-группы отличаются от Security (или, если быть точным, Security Enabled) групп одним битом в атрибуте **groupType** – у Security-группы этот атрибут будет содержать бит **SECURITY_ENABLED**:



[У Security-группы этот бит атрибута groupType включен](#)
(кликните для увеличения до 400 px на 473 px)

,а у Distribution – нет:



[У той же самой группы, которую переключили в Distribution-режим, этот бит атрибута groupType сбросился, а SID остался](#)
(кликните для увеличения до 400 px на 473 px)

Вы можете сколько угодно раз переключать группу из Security в Distribution, от этого её SID никуда не девается. Он и не может – ведь SID это атрибут **всего класса объектов group**, а не какого-то их подвида. Поэтому при создании объекта класса **group** SID разово создаётся, а смене типа с Security на Distribution – не

стирается. Поэтому при переключении между Security и Distribution не запрашиваются новые блоки у [RID Master](#)’а – операции “генерация SID для нового security principal” не происходит. Поэтому, если добавить группу в ACL какого-нибудь объекта, а потом переключить её в Distribution, она оттуда никуда не пропадёт – потому что в ACL записывается SID, а он у этой группы один, с рождения, и никак не зависит от типа группы.

Зачем же нужен этот новый тип группы, Distribution?

Этот тип нужен исключительно для вопросов оптимизации быстродействия и обеспечения безопасности. Смысл существования варианта Distribution – это “lite-version” обычной группы. Отсутствие бита **SECURITY_ENABLED** анализируется сервисом **lsass** в момент создания маркера доступа для сеанса пользователя, и доменные группы без этого бита просто не попадают в маркер.

Пример – есть большая фирма, у которой множество тематических групп рассылок. Например, у них внедрено управление проектами, и к каждой задаче привязан список рассылки “кого уведомлять при изменении связанных с задачей документов, или любом другом изменении”. Таких групп, если проектов много, у одного пользователя могут быть тысячи, а то и десятки тысяч. Если этот пользователь, например, является аудитором, которому надо знать про все изменения в ходе работ у N проектов.

Если это реализовывать через простое добавление пользователя во все эти группы, то при его входе – что на локальную рабочую станцию, что по сети – будет формироваться маркер доступа чудовищного размера, набитый SID’ами групп, которые – это ключевое – не применяются для назначения прав, а нужны лишь для упорядочивания списков рассылки. То есть эти группы изначально созданы только для одной задачи – и их никогда не добавят в ACL у общей папки или в локальную группу Administrators.

В результате получается, что при логине пользователя, добавляя SID’ы Distribution-групп, делается куча лишней работы, от этого замедляется вход в систему, а также создаются потенциальные риски безопасности – вдруг кто-то действительно возьмёт и на локальном сервере, где имеет права, добавит в ACL ресурса группу для рассылок? Тогда входящие в неё с одной целью (получать письма) получат совершенно не нужные права.

Добавление бита **SECURITY_ENABLED** решило оба этих вопроса – составляя маркер доступа, **lsass** разбирает вложения групп, и, если видит группу без этого бита – не добавляет её в маркер доступа, и идёт дальше. То есть добавить в ACL у общей папки или куда-либо ещё Distribution-группу можно – просто т.к. её SID не попадает в маркер доступа, то пользователь в неё с точки зрения Active Directory входит, но получить доступ на ресурс, где она в ACL – не может.

В официальной документации Microsoft содержится ошибка – *Distribution groups are not security-enabled, which means that they cannot be listed in discretionary access control lists (DACLS)* – вот никакого *cannot be listed* нет, вы можете проверить это, явно назначив Distribution группу в любой ACL.

Вот и всё. И весь “волшебный механизм”. Поэтому увидите “эксперта-архитектора” с рассказами о том, что у Distribution-групп нет SID’a – смейтесь над ним и унижайте его, обзывайте его дампером и характеризуйте его “знания” “бауманским качеством”. Показывайте ему SID у Distribution-группы, открыв вкладку Attributes, и выкладываете в соц.сети реакцию – будет много просмотров.

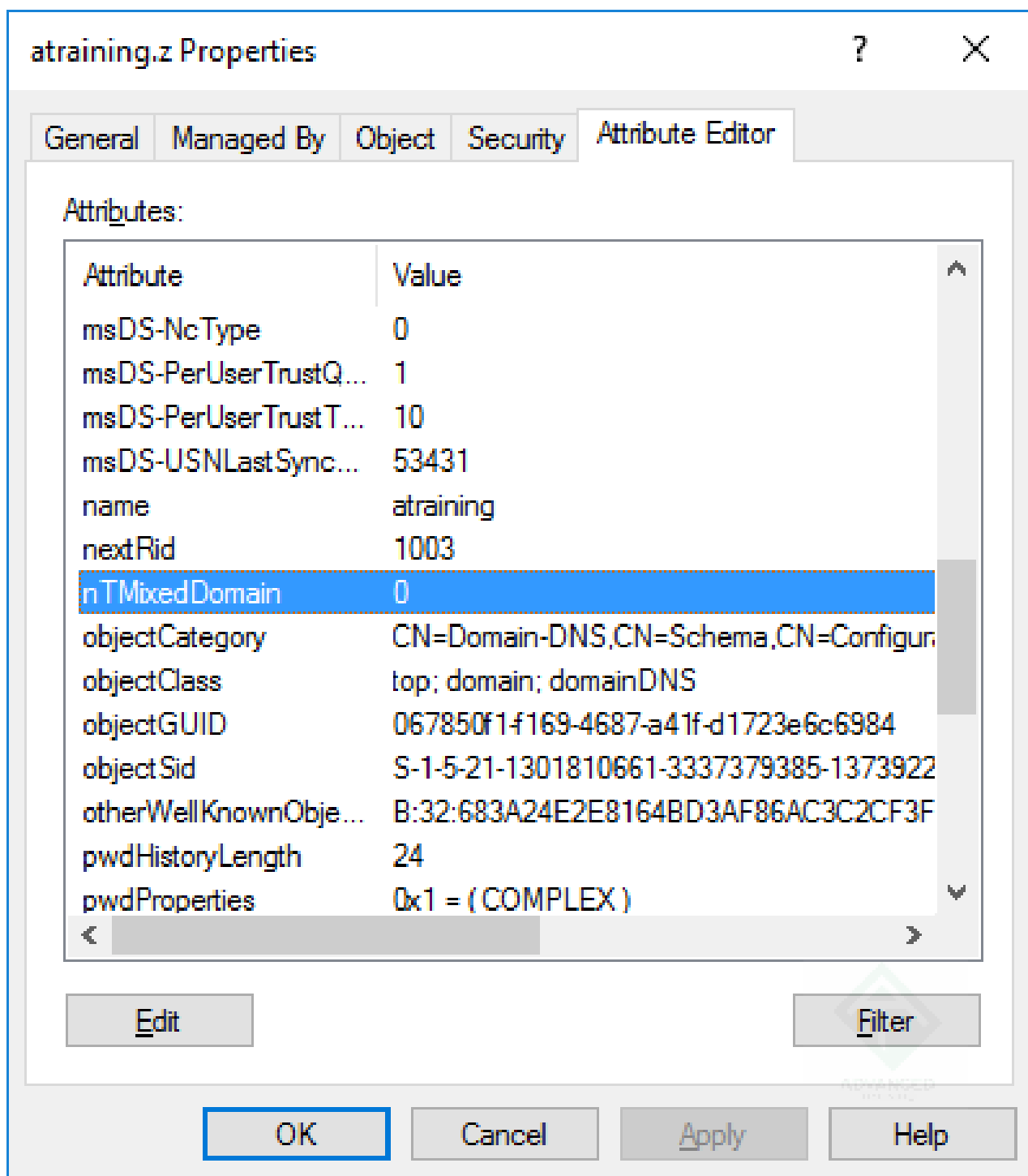
Ну а мы, разобравшись с этим горе-битом, перейдём к новому типу групп – универсальным.

Зачем нужны Universal-группы

Universal-группы и режимы работы домена

Первым делом зафиксируем тот факт, что само по себе появление типа Universal связано с появлением лесов в Active Directory. Universal-группы – новый тип объектов, которого не было в домене Windows NT, поэтому чтобы этот тип групп появился, ваш домен должен быть в “native”-режиме – то есть без включённого признака “работаем в режиме совместимости с доменами Windows NT”. Это просто проверить – у корневого контейнера доменного контекста есть атрибут

nTMixedDomain:



Атрибут nTMixedDomain

(кликните для увеличения до 400 px на 455 px)

Наличие значения **1** у данного атрибута показывает, что домен работает в режиме совместимости с Windows NT – т.е. на владельце FSMO-роли PDC Emulator запущен сервис, который имитирует для старых контроллеров домена Windows NT (т.н. BDC) работу старого PDC. Этот сервис умеет брать содержимое Active Directory и “пережёвывать” его в понятный для Windows NT 4.0-контроллеров формат. Очевидно, что эти контроллеры ничего про Universal-группы не знают, поэтому в режимах работы домена “совместим со старыми Windows NT-системами” универсальную группу вам создать не дадут – ведь неясно, как в этой ситуации отправить BDC-контроллеру содержимое такой группы, или другой группы, в которую включена Universal. Такая ситуация возникнет лишь в двух старых режимах

работы домена Active Directory – **Windows 2000 Mixed** и **Windows 2003 Interim**. Как только вы переключитесь в любой из “native” режимов работы домена – возможность создания Universal-групп появится. Впрочем, натолкнуться сейчас на домен, работающий в одном из этих двух режимов, достаточно сложно. Поэтому далее предполагаем, что у вас домен – как минимум **Windows 2000 Native**.

Итак, зачем же нужны Universal-группы?

Если вы домотали до этого момента, то, пожалуйста, перечитайте верхнюю часть ещё раз – потому что чтобы разово уложить новые сведения в голове, нужно понять всё предыдущее.

Можно ли жить в лесу Active Directory без Universal-групп, только с Global и Domain Local

Начнём с простого – без универсальных групп вполне можно жить. Т.е. Global и Domain Local покрывают все существующие задачи. Глобальные группы, как и было заведено изначально, нужны для консолидации учётных записей – разве что в домене Windows NT нельзя было делать group nesting, т.е. вкладывать глобальную в глобальную, а в Active Directory (речь про Native-режимы) – можно. Вложить в глобальную группу группу из другого домена – что Global, что Domain Local – нельзя, всё, ещё раз повторяюсь, чётко – в глобальные вкладываем учётки из нашего домена и другие глобальные группы только из нашего домена.

Domain Local же наоборот – самый “гостепреимный” вариант – в них можно вкладывать и учётные записи, и глобальные группы из любого доступного через trusts домена. Можно даже другие Domain Local – но, как понятно, только из своего домена – ведь домены в силу ряда ограничений (см. начало статьи) не позволяют друг другу добавлять Domain Local из одного домена в члены Domain Local из другого.

Жить, таким образом, можно – собираем учётки по отделам-задачам в Global (например, в каждом домене делаем группы BUGHALTERIA и MARKETING). Эти группы добавляем в Domain Local’ы с названиями вида “SRV1 BUH-Otchets RO” (которым заранее раздаём соответствующие их названию права – этой, например, на файл-сервере SRV1 на общей папке BUH и подпапке Otchets разрешаем Read Only), и удобно управляем доступами для групп пользователей.

Сразу ответ на типовой вопрос “а можно ли вообще всё глобальными делать?” – в пределах одного домена – да, а как только доменов больше одного, то вы не сможете, “повесив” в ACL ресурса Global-группу, включить в неё Global-группу из другого домена, и придётся использовать “гостепреимную” Domain Local, в которую можно запихнуть кого угодно из какого угодно домена.

Но не всё так однозначно – будут и проблемы.

Проблемы масштабирования при использовании только Global и Domain Local

Так вот, основное веселье с ситуацией “используем только глобальные и домен-локальные” начинается, если доменов в лесу много. Тогда штука с “нельзя засунуть в Global из нашего домена Global из другого” сразу же всплывает. В этом случае, если надо будет создать группу вида “Все сотрудники фин.департаментов”, куда логично добавить группы вида “Accountants”, “Fincontrol”, “Finauditors”, то ничего не получится – технически это не реализуется. В результате Domain Local-группы, висящие на ACL’ах у ресурсов, начнут ощутимо тяжелеть, потому что там надо будет в явном виде перечислять все Global из всех доменов леса. Этот процесс вызовет и замедление обработки, и увеличение сложности обслуживания.

Более того, начнёт появляться проблема с логином. Суть её проста – при входе пользователя с использованием UPN-имени (по факту всегда; просто с UPN-именем нагляднее) DC обращается к GC, чтобы выяснить, что это за пользователь такой. Ведь UPN суффиксы уникальны в пределах леса, а не домена – т.е. у вас может быть лес с 8 доменами, в котором 3 UPN-суффикса, и по “хвосту” имени пользователя сходу сказать “да, он из такого домена” просто нельзя.

Обращаясь к GC, контроллер домена запрашивает вначале “кто это ко мне такой за составлением маркера доступа обратился”, а после, узнав кто это (т.е. получив SID по UPN’у), начинает составлять маркер доступа, вычисляя, в каких группах состоит данная учётная запись. Тонкость в том, что состав групп – т.е. поле **member** у Global и Domain Local, на GC не реплицируется, поэтому получив ссылку вида “Данный пользователь входит в группу X”, контроллер домена находит у себя эту группу, и уже читая domain naming context, а не ответ GC, вычисляет, в какие группы в свою очередь входит она. Этот итеративный процесс “парсинга вложенных групп” вполне будет достаточно ёмким по количеству итераций и общему объёму.

Почему ж так странно сделали, спросите вы – ну т.е. почему на GC не реплицируется атрибут **member** у групп? Тонкость в том, что на момент разработки оригинальной версии Active Directory, в NT 5.0, не было механизма частичной репликации multivalued-атрибутов (т.н. LVR, Linked Value Replication). В результате, если бы у GC кэшировался этот атрибут, то для групп с большим числом участников (тысячи, а то и десятки тысяч), любое изменение приводило бы к запуску полной репликации всех GC леса. То есть ещё раз – есть лес с кучей доменов, в одном из них в одной из групп добавляется один участник – вот если бы GC кэшили **member**, то это заставляло бы все GC леса, во всех доменах, полностью перекопировать этот объект. Эта ситуация уходит с появлением NT 5.2, и уровня леса “Windows Server 2003”, но на момент выхода Active Directory это всё – критично. Каналы слабые (я помню, как регионы реплицировались по диалапу, поверх которого поднимался RRaS’овский VPN, и полоса составляла единицы килобайт), GC не на каждом контроллере (опять же из-за экономии, чтобы меньше репликаций было).

В результате имеем сложную ситуацию – логинящемуся пользователю надо собрать маркер, для этого надо распарсить “матрёшку” из “какая группа в какую вложена”, для этого надо бегать вначале на GC, чтобы узнать, кто логинится, а потом, узнавая

в какие группы он включен, бегать за уточнениями “а кто в эту группу входит” уже на DC.

Всё это решается проще, если добавляется новый тип групп – универсальные.

Состав универсальной группы кэшируется на GC – то есть, обратившись к GC, можно получить из этого запроса список участников данной группы. Сразу, без беготни туда-сюда. Притом на любом GC леса есть все Universal-группы этого леса – поэтому можно, если имеет место вложенность одной в другую, сразу же разрешить это с одним GC – вся информация на нём есть.


Это быстрее – и именно поэтому, к примеру, когда вы читаете документацию на Exchange Server, то можете заметить, что почтовые группы предлагается делать Universal – тогда их быстрее можно “раскрывать” в плане состава, за одно обращение к ближайшему GC.

Да, изменение состава Universal-групп инициирует репликацию во всём лесу (и в том домене, в котором эта группа существует, разумеется) – но всё ж, благодаря LVR-репликации, масштаб не настолько критичен и огромен. Суть в том, что если вы реже меняете состав групп, чем их читаете (так обычно и происходит), то Universal-группы выгодны – трафик репликации растёт мало, на фоне явной экономии времени и трафика на запросах о членстве.

Универсальные группы, подчеркну, будут запрашиваться с GC – поэтому необходимо, чтобы в каждом сайте AD был хотя бы один GC – иначе работать будет, но появится большая задержка от round-trip запросов поверх WAN-каналов между сайтами – именно из-за этого на уровне сайта есть опция “включить на всех DC этого сайта кэширование состава универсальных групп”, понимаемая всеми Windows 2003 Server и более новыми:

NTDS Site Settings Properties

Site Settings | Object | Security | Attribute Editor

 NTDS Site Settings

Description:

Inter-Site Topology Generator

Server:

Site:

Universal Group Membership Caching

☐ Enable Universal Group Membership Caching

Refresh cache from:

[Кэширование состава универсальных групп в сайте Active Directory](#)

([кликните для увеличения до 400 px на 488 px](#))

Эту настройку, как понятно, имеет смысл включать, если теоретически возможна ситуация “в этом сайте не на всех DC есть GC, и есть шанс, что все GC умрут, тогда долго ходить за GC, проще кэш использовать” – если же у вас современная ситуация “каждый DC в сайте – GC”, то эта настройка уже не имеет смысла.

Что же у универсальных групп по части членства? Всё очень хорошо – в универсальную группу могут входить учётки, глобальные группы, и другие универсальные – из любого домена нашего леса. Это очень удобно. Domain Local’ы,

как понятно, не могут – они, находящиеся в других доменах, просто не видны из нашего – впрочем, мы это уже много раз подчеркнули.

Кроме того, универсальные группы из нашего же домена занимают 8 байт в PAC'е (т.е. в итоговом маркере доступа) – это выгодно.

Таким образом, вырисовывается следующая картинка с универсальными группами – они действительно гораздо более просты в части “что в них можно положить” – можно всё, кроме не видимых нами из нашего домена Domain Local'ов других доменов ; плюс запрос у GC состава этих групп делается в одно движение; плюс места в токене занимают мало.

Что ж, давайте теперь немного посуммируем то, что имеется на данный момент.

- В Active Directory есть три типа групп – каждый со своей спецификой;
- У каждого типа есть вариант “с пометкой о не-использовании в составе маркера доступа” – это называется Distribution-группой;
- Разные типы групп занимают разное число байт – некоторые занимают 40 байт, т.е. пишется SID целиком, с доменной частью, некоторые 8 – когда только тип и RID;
- Специфика универсальных групп будет связана в основном с фактом появления леса Active Directory – впрочем, некоторое увеличение скорости работы можно будет получить, заменяя Global на Universal и в сценарии “один домен в лесу”;
- Универсальные группы ускоряют работу только если нет проблем с GC – т.е. он доступен, он в нашем сайте (требуется правильная настройка сайтов и подсетей); при риске потенциальной недоступности можно подстраховаться включением кэширования состава универсальных групп на уровне сайта;

Что ещё можно добавить? По мат.части всё – теперь перейдём к отдельным вопросам и тонкостям.

Тонкость в назначении прав с использованием Domain Local-групп на объекты Active Directory.

Domain Local-группы и объекты Active Directory

В Active Directory, назначая права на объекты, не используйте схему “ACL объекта -> в нём группы-заглушки Domain Local -> в них включаются Universal или Global -> в которые включаются учётные записи”. Почему? Дело в том, что когда пользователь из домена X будет пытаться провести операцию с каким-то объектом Active Directory, подключившись к DC из домена Y (это важно – т.е. у нас лес, много доменов, и есть например лесной раздел Configuration, который есть на всех DC в лесу) – так вот, этот пользователь, когда будет идти проверка “а можно ли ему сделать операцию”, может оказаться в ситуации “на объекте в ACL указана Domain Local группа, но не из домена Y – поэтому данный DC не может её запросить, её состава нет на GC, а контроллер домена, на котором живёт эта группа, не

показывает чужим Domain Local-группы”). В этом случае маркер доступа будет сформирован с ошибкой, без SID’ов таких групп, и пользователь может не получить доступ (или наоборот, ему явно запрещено, а он получит).

Поэтому применяемый для доступа к ресурсам доменных рабочих станций и серверов подход с Domain Local-группами – это одно, а специфика Active Directory, как существующей на нескольких системах-DC с общей базой безопасности – другое.

Миф про сниженное быстродействие Universal-групп

Корни данного мифа, формулируемого как “Universal-группы универсальные, поэтому тормозят”, лежит в советах времён Windows 2000, где вся “тормознутость” сводилась к “часто менять будете состав, и большие группы – значит, большая репликация GC”. По факту и добавление LVR, и рост скорости каналов связи на несколько порядков, этот вопрос полностью убрали. Размеры объектов AD-то не выросли вместе со скоростью каналов – сейчас вопрос “скорость репликации GC” совершенно другую актуальность имеет. Так что используйте Universal-группы смело, они дают явный плюс в скорости при использовании. И не пользуйтесь кэшированием состава Universal-групп на уровне сайта AD, пока нет ситуации “очень далёкий очень медленный филиал, где хотя бы 2 DC, и не все из них GC” – если хотя бы одно из этого не является верным, кэширование просто не нужно.


Производительность дополнительно вырастет, если заменять по возможности Domain Local-группы на Universal (из того же домена) – тогда размер маркера доступа, при прочих равных, уменьшится.

Миф про одинаковость всех групп, потому что их можно друг в друга переключать

Все три типа групп могут превращаться друг в друга – схема достаточно проста, группы Global или Domain Local можно сделать Universal, а Universal – превратить в Global или Domain Local. Т.е. нельзя разве что напрямую Global в Domain Local, надо через превращение в Universal:

Test Universal Group 1 Properties ? X

Object	Security	Attribute Editor	
General	Members	Member Of	Managed By

 Test Universal Group 1

Group name (pre-Windows 2000):

Description:

E-mail:

Group scope

☐ Domain local

☐ Global

☒ Universal

Group type

☒ Security

☐ Distribution

Notes:


OK Cancel Apply Help

[Universal-группу можно сконвертировать что в Global, что в Domain Local](#)
([кликните для увеличения до 400 px на 473 px](#))

Test Global Group 1 Properties

Object Security Attribute Editor

General Members Member Of Managed By

 Test Global Group 1

Group name (pre-Windows 2000):

Description:

E-mail:

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☐ Security

☒ Distribution


Notes:

OK Cancel Apply Help

[Global-группу можно сконвертировать только в Universal](#)
([кликните для увеличения до 400 px на 473 px](#))

Test Domain Local Group 1 Properties

Object	Security	Attribute Editor	
General	Members	Member Of	Managed By

 Test Domain Local Group 1

Group name (pre-Windows 2000):

Description:

E-mail:

Group scope

☒ Domain local

☐ Global

☐ Universal

Group type

☒ Security

☐ Distribution

Notes:

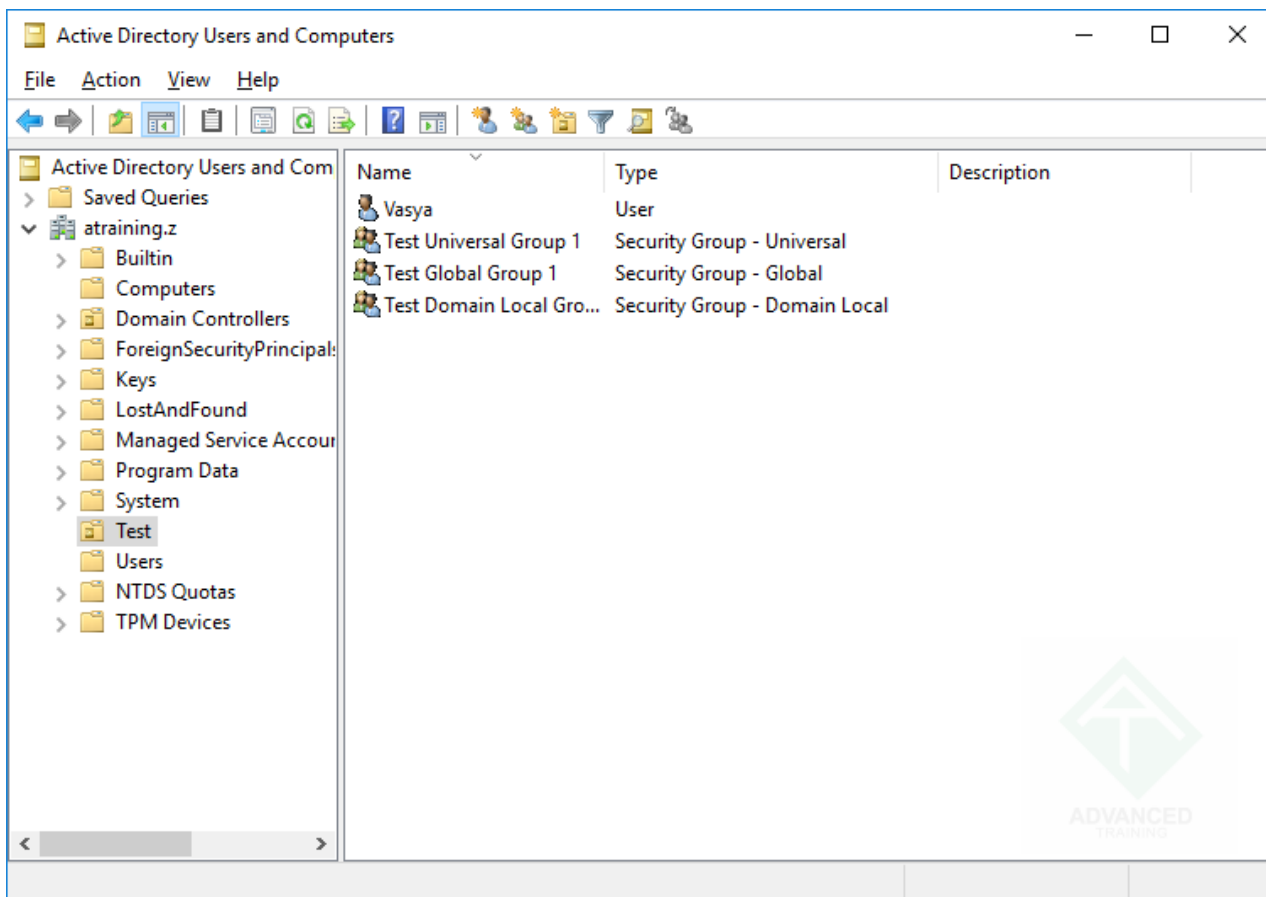
OK Cancel Apply Help

[Domain Local-группу можно сконвертировать только в Universal](#)
[\(кликните для увеличения до 400 px на 473 px\)](#)

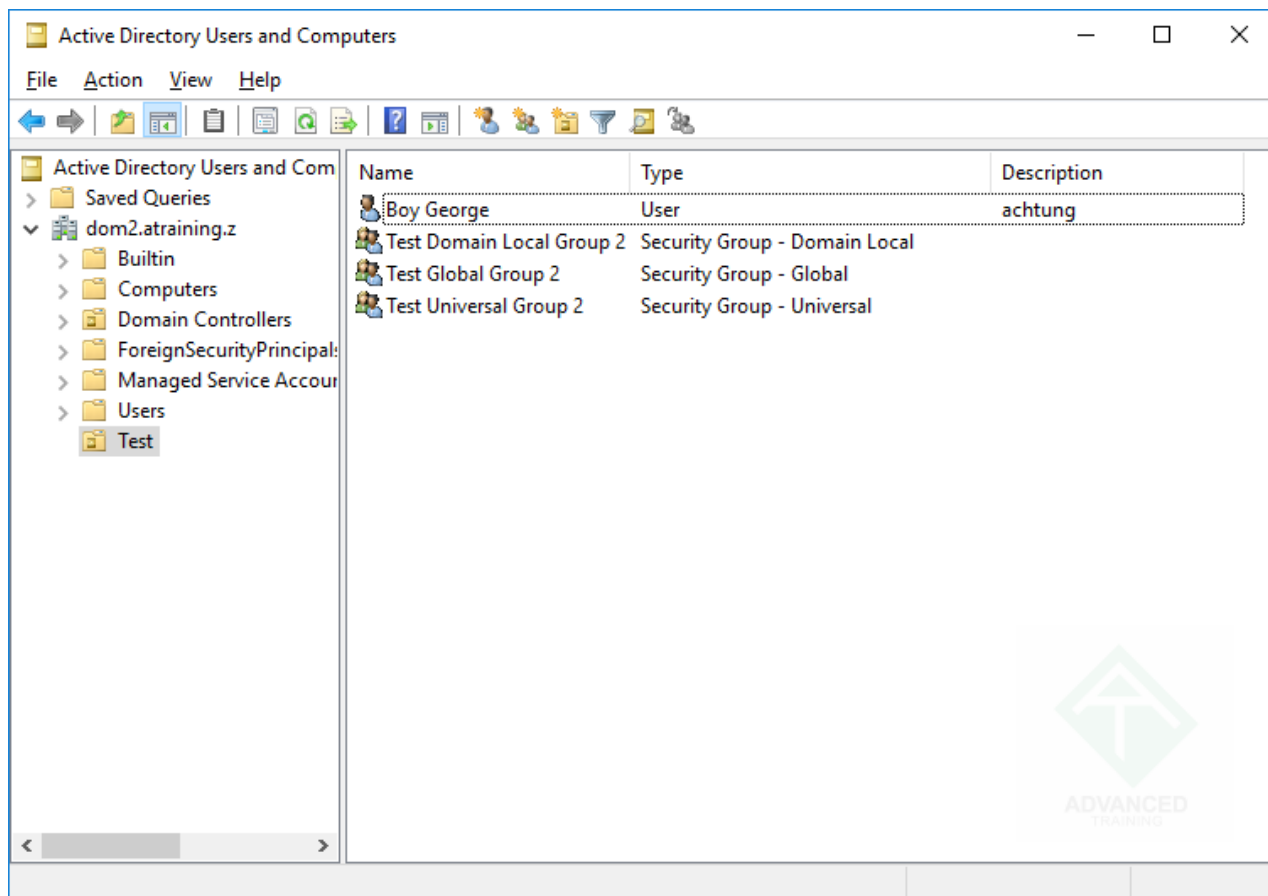
Из-за этого функционала, визуально “простого”, и рождается миф, что “понаделают тут просто так от скуки типов групп, ведь это подтверждается тем, что любую в любую, по сути, можно переделать, и ничего не поменяется”.

Не любую в любую. Исключением будет попытка превратить Domain Local в Universal в ситуации, когда в Domain Local есть foreign security principal.

Проверим на практике. Исходные данные – корневой домен леса **atraining.z** и его дочерний домен с удручающим названием **dom2.atraining.z**. В каждом из доменов создано 3 тестовых группы разных видов и по одному пользователю:

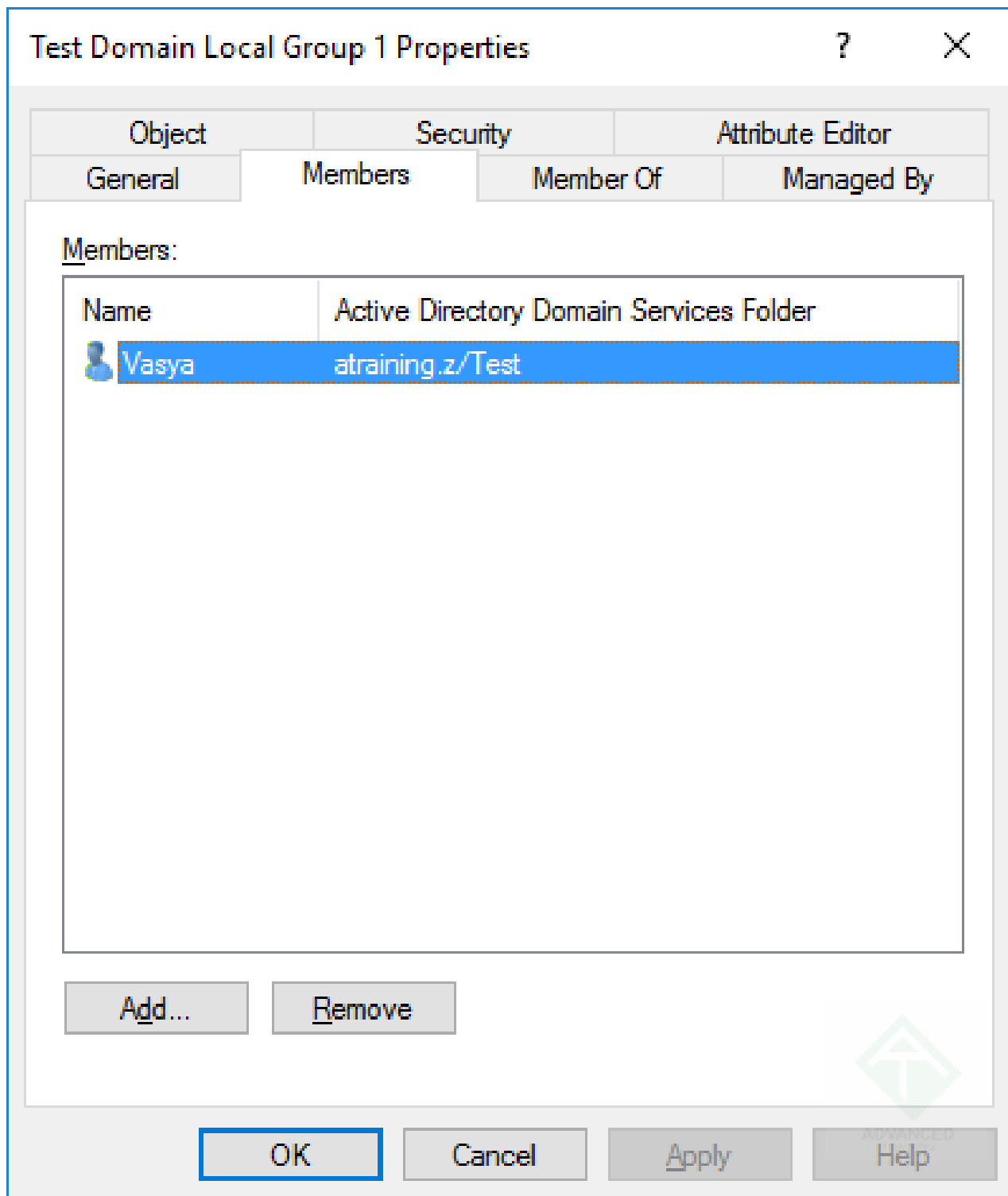


[Тестовый домен atraining.z с тестовыми группами и пользователем](#)
(кликните для увеличения до 754 px на 530 px)



[Тестовый домен dom2.atraining.z с тестовыми группами и пользователем](#)
([кликните для увеличения до 754 px на 530 px](#))

В Domain Local-группе у нас будет одинокий местный участник Vasya:



[Тестовый домен dom2.atrainig.z с тестовыми группами и пользователем](#)
([кликните для увеличения до 400 px на 473 px](#))

Ищем ему компаньона-иностранца из другого домена:

Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
 Users, Service Accounts, Groups, or Other objects Object Types...

From this location:
 dom2.atraining.z Locations...

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts


☐ Non expiring password

Days since last logon:

Columns...











Find Now

Stop



OK Cancel

Search results:

Name	E-Mail Address	Description	In Folder
 Administrator		Built-in account f...	dom2.atraining.z...
 Boy George		achtung	dom2.atraining.z...
 Cloneable Do...		Members of this ...	dom2.atraining.z...
 DefaultAccount		A user account ...	dom2.atraining.z...
 DnsUpdatePr...		DNS clients who...	dom2.atraining.z...
 Domain Admins		Designated admi...	dom2.atraining.z...
 Domain Comp...		All workstations ...	dom2.atraining.z...
 Domain Contr...		All domain contr...	dom2.atraining.z...
 Domain Guests		All domain guests	dom2.atraining.z...
 Domain Users		All domain users	dom2.atraining.z...

[Иностранная учётная запись сразу же чем-то не понравилась Василию \(кликните для увеличения до 515 px на 579 px\)](#)

И получаем сообщение **The following Active Directory Domain Services error occurred: Foreign security principals cannot be members of universal groups.**, или LDAP-ошибку 50 (0x32) от контроллера – **ERROR_NOT_SUPPORTED**.

Так что не всё так однозначно – и преобразование групп из одного вида в другой, хоть и выглядит “тривиальным”, является операцией, при которой проводятся доп.проверки, поэтому никакого “любую в любую можно спокойно, поэтому пофигу на все эти виды групп” не нужно.

Что ж. В общем, всё.

Финал

Я надеюсь, что не очень сильно вас запутал, а даже наоборот – что-то распутал. Впрочем, такие темы проще, конечно же, рассказывать на курсах – так что [заходите](#), у нас интересно. Тема Active Directory – огромна и очень увлекательна.

До встреч!