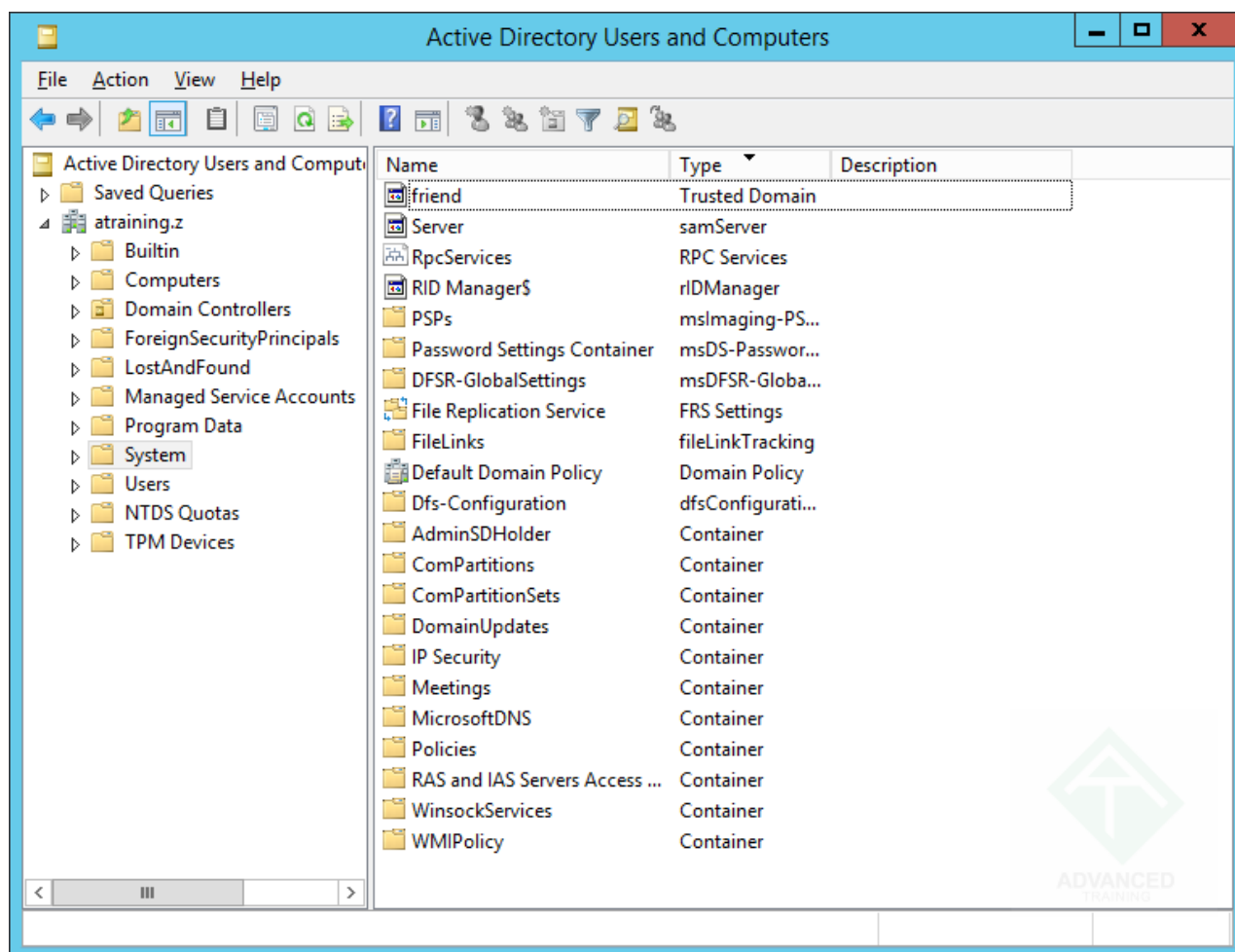


Четыре истории про кастомизацию Active Directory.



Привет.

Кастомизация Active Directory – тема вечная. Вокруг неё накручено много вымыслов, шаманства и прочего, однако тема эта никакого волшебства в себе не содержит. Я это наглядно покажу.

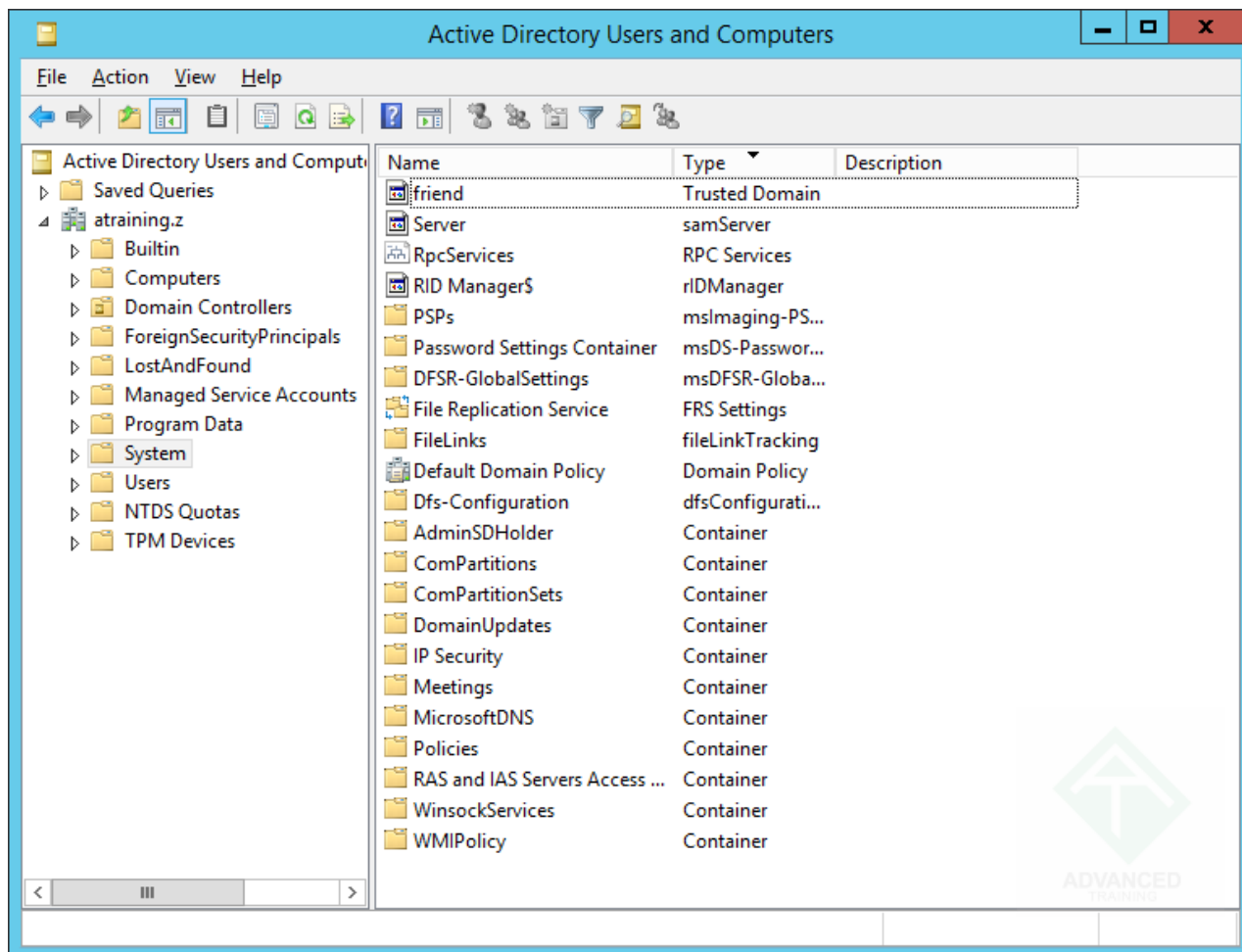
Это обновлённая версия статьи – старая, от 2009 года выпуска, получила новые картинки, сделанные на Windows Server 2012 R2, актуализацию и уточнения. Впрочем, актуализация не особо нужна – всё рассказанное работает и на старых, и на новых ОС.

Начнём.

История первая – Глючные картинки

Однажды к одному CIO пришёл руководитель IT-департамента.

– В Active Directory есть глючные объекты, у которых нет картинки. Вот, смотри:



[У дружественного домена, до которого установлен trust, нет своей картинки \(кликните для увеличения до 768 px на 586 px\)](#)

– Траст до партнёрского домена есть, а судя по картинке – глючный. Люди волнуются, говорят, что надо домен переставлять, наверное.

“Люди не должны волноваться. Чистый разум, по которому бежит рябь мысли о переустановке Active Directory, подобен нечистому разуму, а таких по ТК премии лишают. Нельзя так с людьми.” – подумал CIO.

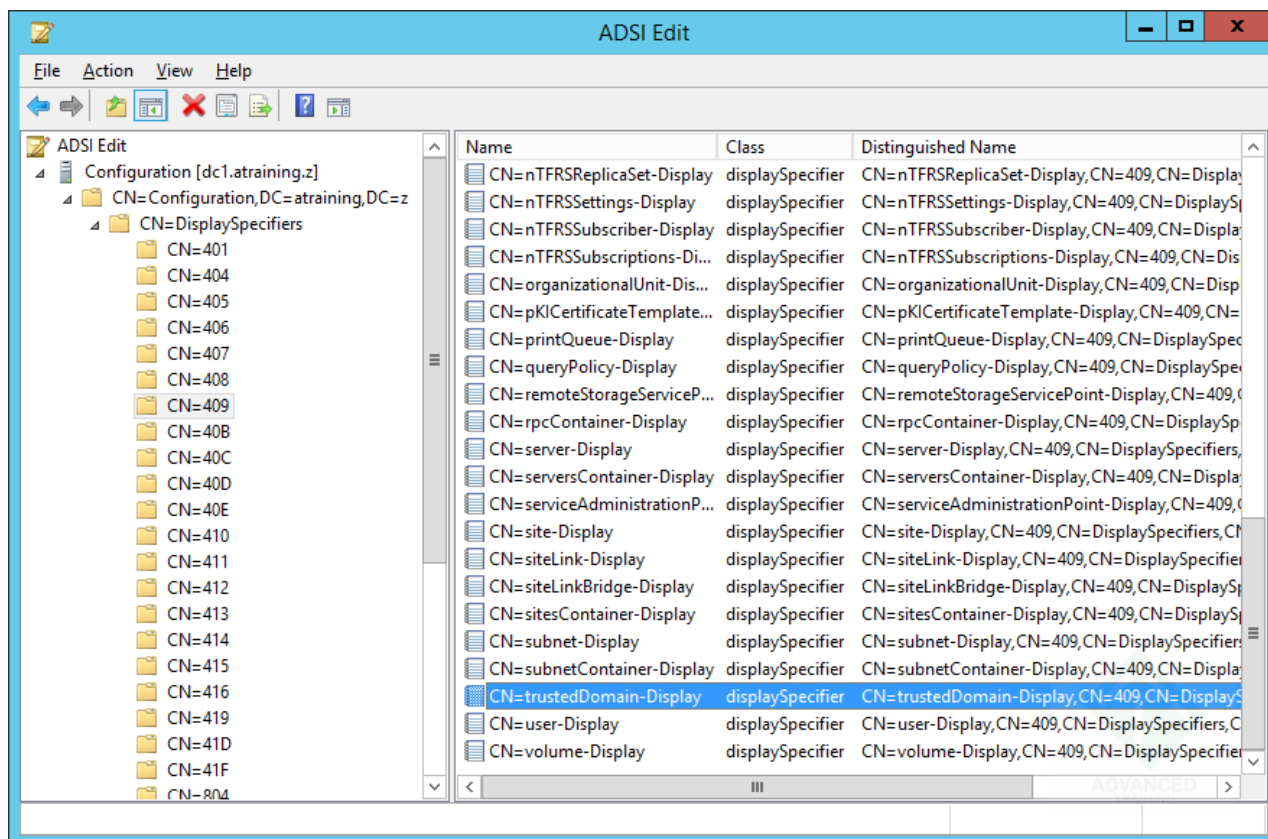
Действуем.

Последовательность действий

Отображение всех объектов в Active Directory предприятия регулируется в контейнере **CN=Display Specifiers,CN=Configuration,DC=доменный контекст**. В нём Вы найдёте отдельные контейнеры, название которых соответствует языковому коду – для английского это будет 409; если хотите, чтобы объекты отображались в разных в плане языков консолях Active Directory по-разному – просто поправьте не в одном, а в нескольких соответствующих контейнерах.

Откуда берётся число 409? Это 1033 в hex-варианте, а справочник по кодам языков Вы можете легко найти, никуда не выходя с локальной машины – откройте ключ реестра **HKLM\SYSTEM\CurrentControlSet\Control\ContentIndex\Language**, там в

каждом разделе будет **Locale**, которое, путём перевода в hex, и даст искомый код. Выглядеть в нашем случае консоль для редактирования этих свойств будет как-то так:



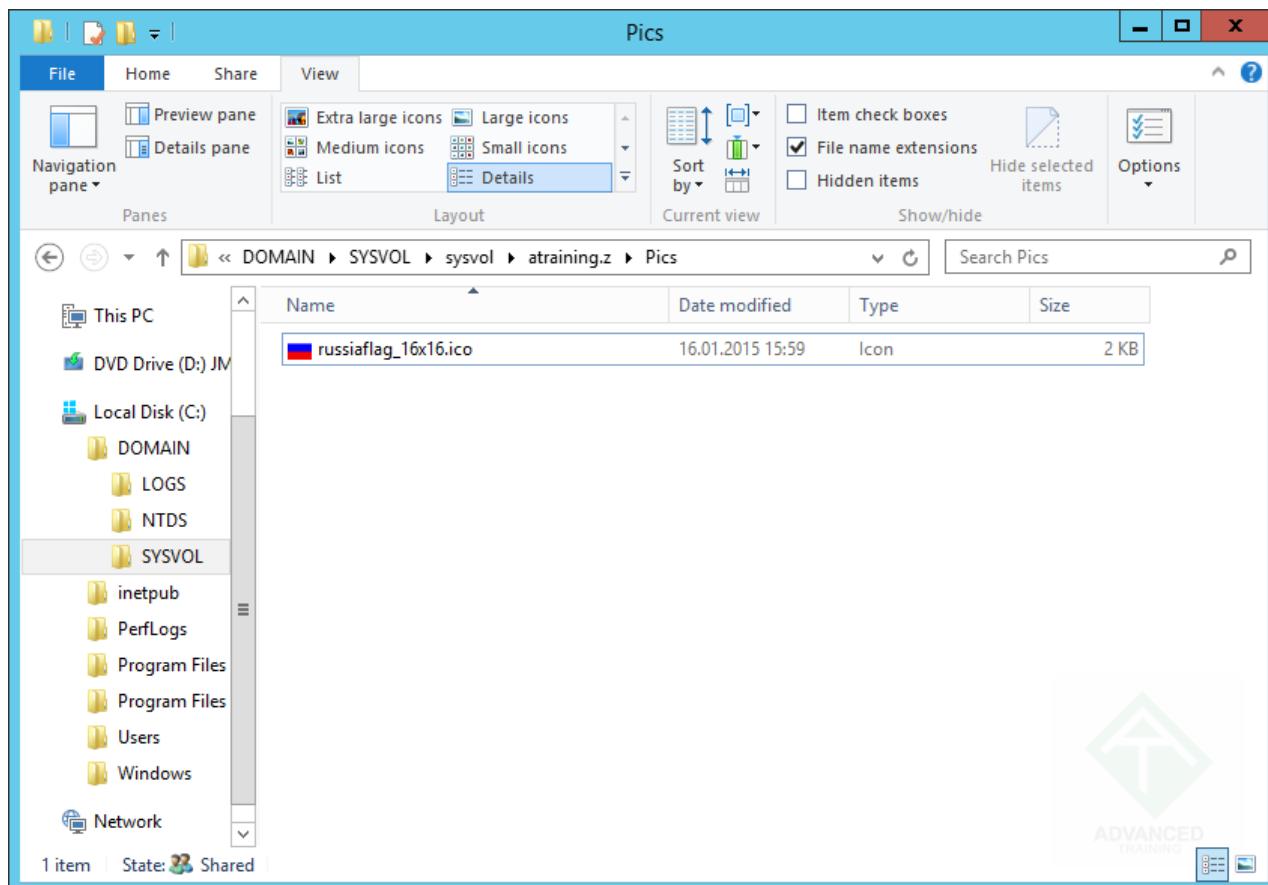
Редактируем картинку для траста Active Directory.

(кликните для увеличения до 881 px на 579 px)

Объект, который мы хотим поправить, имеет класс **trustedDomain-display**. Откроем вкладку **Attribute Editor**, и в ней найдём атрибут **iconPath**. Данный атрибут позволит нам задать до 16 различных картинок, используемых для разных состояний объекта (это надо, если у объекта могут быть разные состояния – у пользователя, например, разные картинки, когда он в обычном состоянии или в Disabled). Стандартных состояний будет три:

- Нуль – картинка по-умолчанию, если у объекта нет состояний, или “closed”, если объект, допустим, контейнер
- Единица – “opened”, если объект, допустим, контейнер
- Двойка – объект отключён, флаг “disabled”

Нам будет нужна нулевая, т.к. у этого типа объектов нет разных визуальных состояний при просмотре консоли ADUC. Картинку, которую мы поставим, заранее выложим в папку **\\FQDN домена\SYSVOL\FQDN домена\Pics** – этим мы решим вопрос с автоматической репликацией картинки на все контроллеры домена, да и подгружаться она будет с ближайшего, что тоже плюс. Для изготовления картинки в формате *.ico используем ресурс [ConvertICO](#). Вот что получится:



[Подготовка картинки для отрисовки объекта trust в Active Directory.](#)
([кликните для увеличения до 846 px на 588 px](#))

Теперь редактируем атрибут **iconPath**:

Multi-valued String Editor

Attribute: iconPath

Value to add:

Add

Values:

0,\\atraining.z\\SYSVOL\\atraining.z\\Pics\\russiaflag_

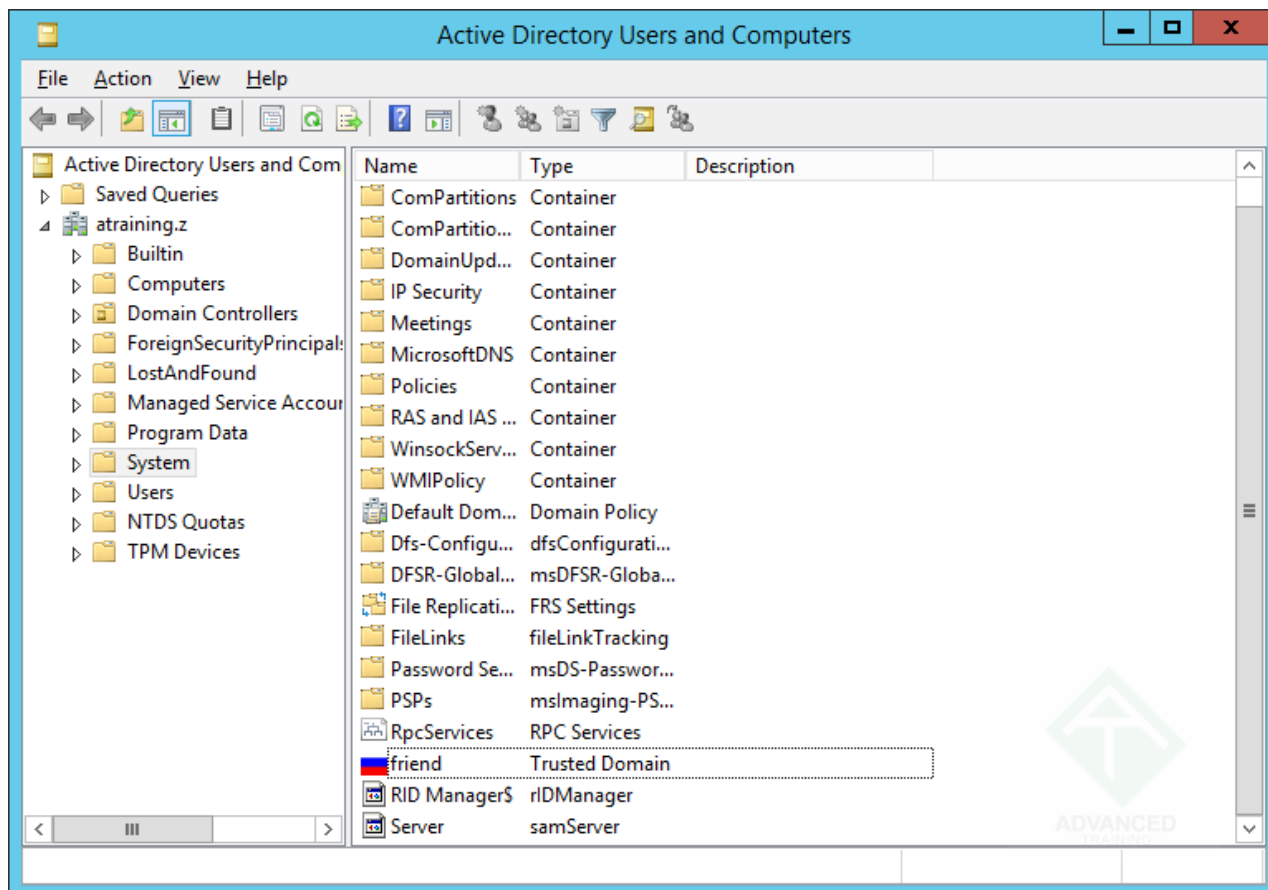
Remove

< ||| >

OK Cancel

[Меняем атрибут iconPath для дефолтной иконки объекта в Active Directory](#)
([кликните для увеличения до 376 px на 393 px](#))

Результат будет таким:



[Корректное отображение траста в Active Directory.](#)

[\(кликните для увеличения до 768 px на 537 px\)](#)

Теперь у этого типа объектов своя, хорошо заметная картинка. Она будет автоматически появляться в любой консоли Active Directory Users & Computers, братья с ближайшего DC. Ничего дописывать не надо, никаких хаков не делается, всё штатно, централизованно и удобно. Переустановка “глучного домена” отменяется.

История вторая – Как Вася в алкоголе запутался

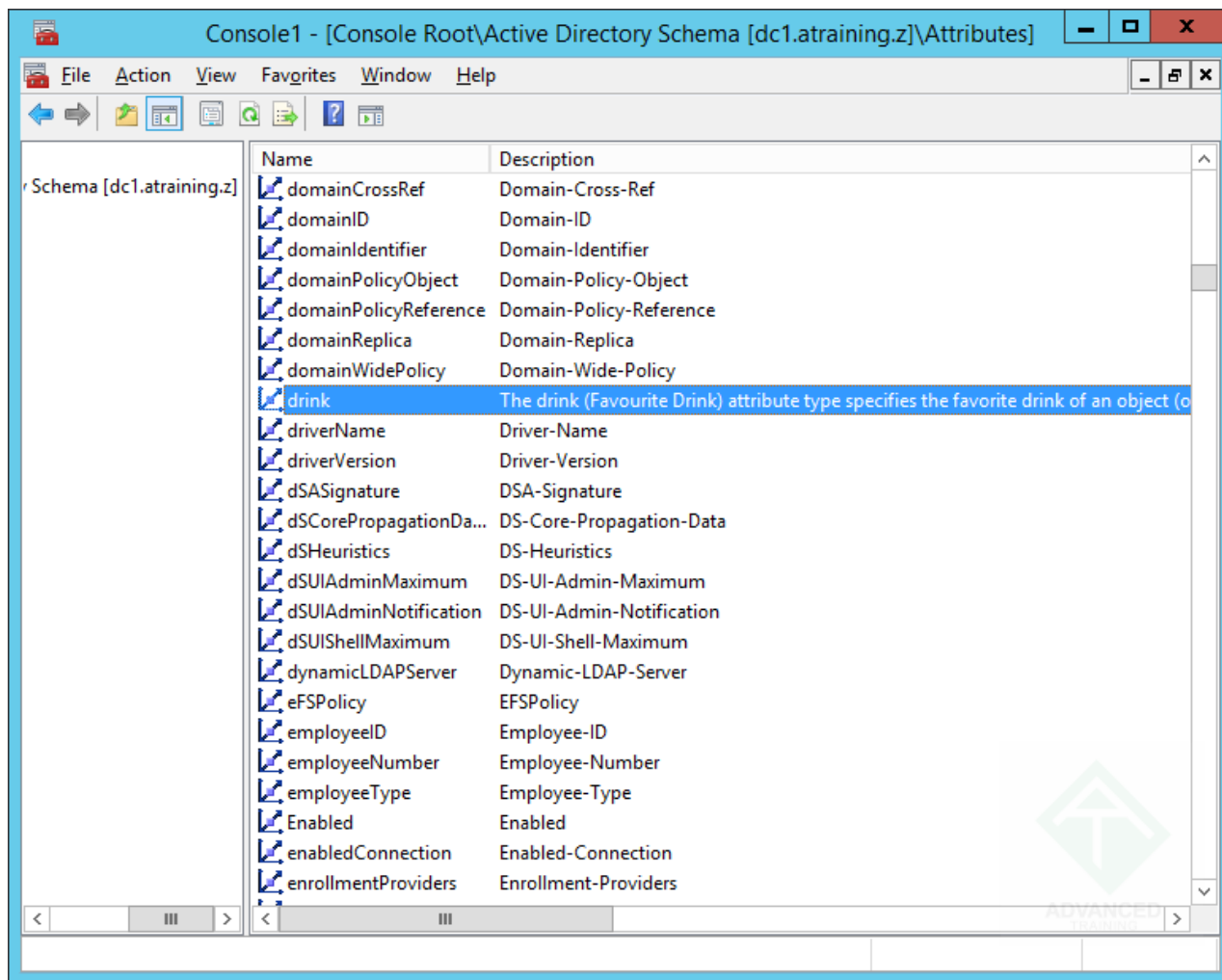
Однажды к одному CIO пришёл руководитель IT-департамента.

- Помнишь Васю, которому мы обещали проставиться?
- Конечно помню.
- Вот и я помню. А если забудем? Надо как-то сделать так, чтобы такое не забылось. Иначе мы потеряем лицо.
- Ты не поверишь – но это – встроенная возможность Active Directory

Действуем.

Последовательность действий

В схеме Active Directory есть штатный атрибут **drink** – его описание выглядит как *“The drink (Favourite Drink) attribute type specifies the favorite drink of an object (or person)”*.

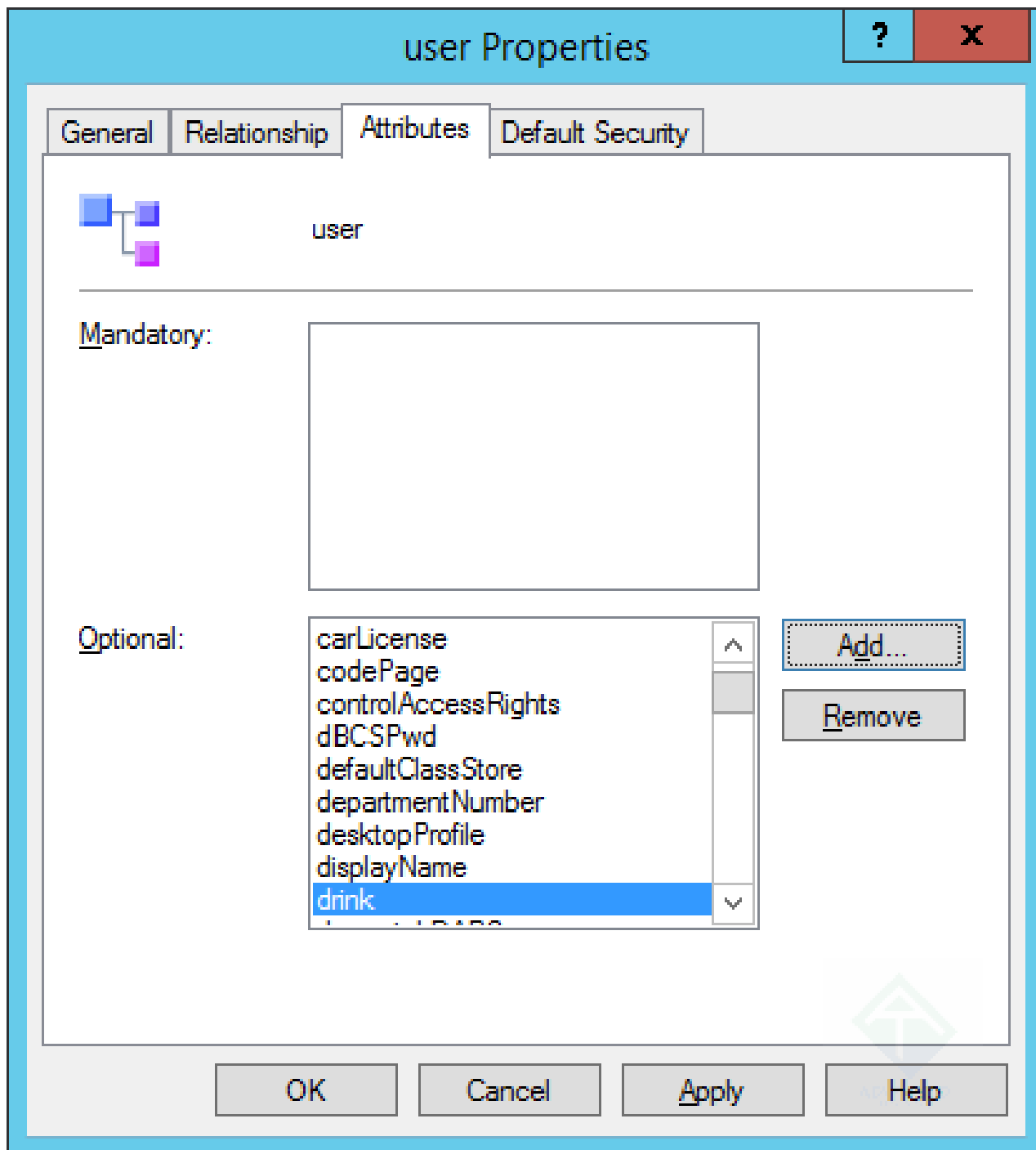


Марка выпивки - штатный атрибут Active Directory.

(кликните для увеличения до 773 px на 615 px)

Это пачка текстовых строк в Unicode, которая благоразумно не добавлена в объект **user** по умолчанию. Мы её добавим – сделать это несложно:

- Зарегистрируем оснастку для редактирования схемы Active Directory – выполнив команду **regsvr32 schmmgmt.dll** (не забудем, что для данного внесения изменений в \CLSID надо быть членом группы локальных администраторов или обладать аналогичными правами на ветку реестра)
- Откроем новый экземпляр **mmc**, добавим туда оснастку Active Directory Schema, и найдём там в контейнере **Classes** класс **user**
- Далее на вкладке **Attributes** добавим данный атрибут к пользователю

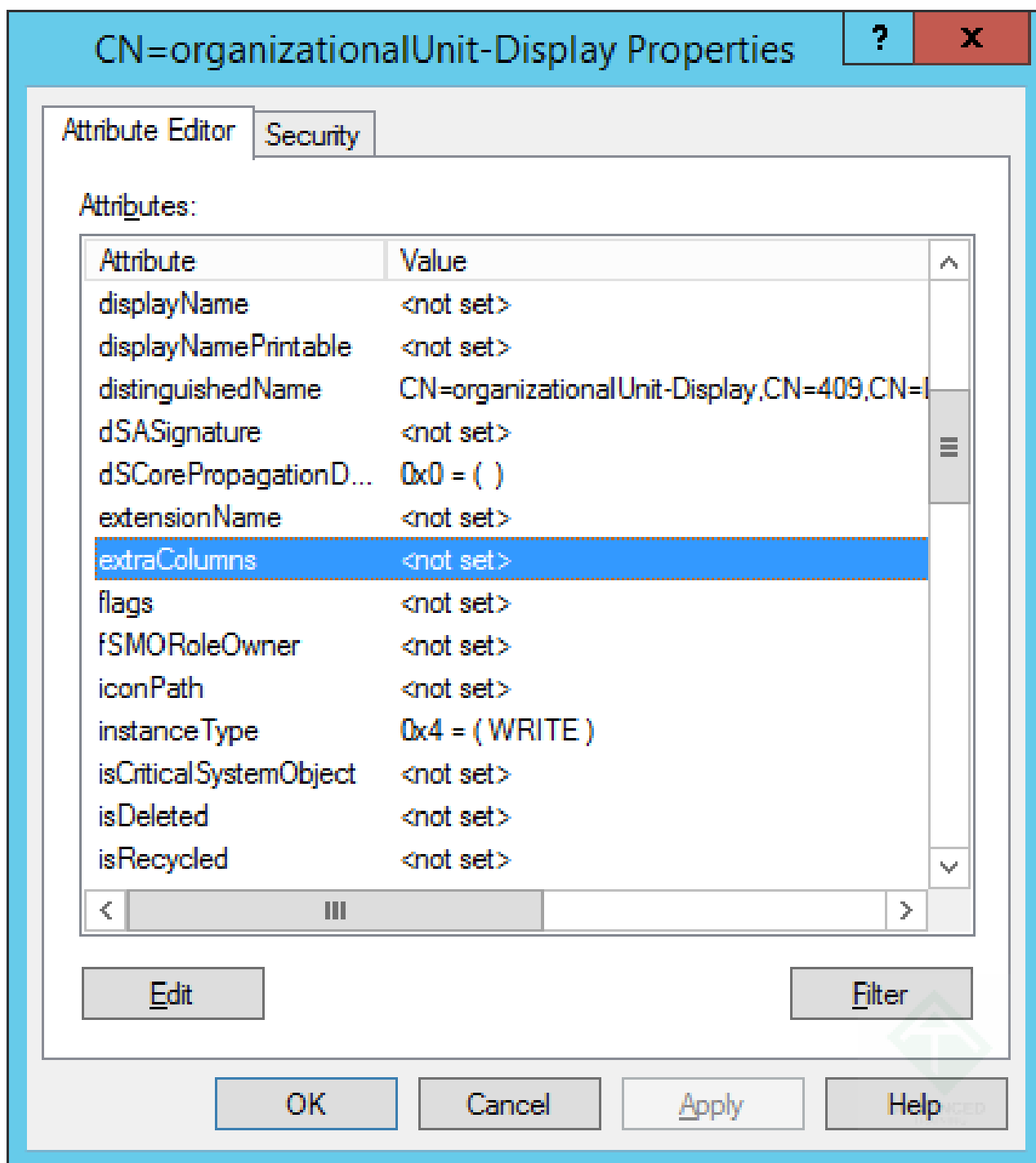


[Добавляем атрибут drink к классу user в Active Directory.](#)

[\(кликните для увеличения до 414 px на 457 px\)](#)

Закроем оснастку Active Directory Schema, т.к. она нам больше не понадобится, и откроем ADSI, чтобы теперь добавить этот замечательный атрибут в GUI оснастки Active Directory Users & Computers. Путь наш будет лежать туда же, куда и в прошлой истории – в контейнер **CN=код языка,CN=Display**

Specifiers,CN=Configuration в лесу Active Directory. Мы выберем тот тип контейнеров, при просмотре которых у нашего пользователя должны выводиться дополнительные атрибуты – например, OU. Раз OU, то называться объект будет **organizationalUnit-Display**, а интересоваться нас в нём будет атрибут **extraColumns**:



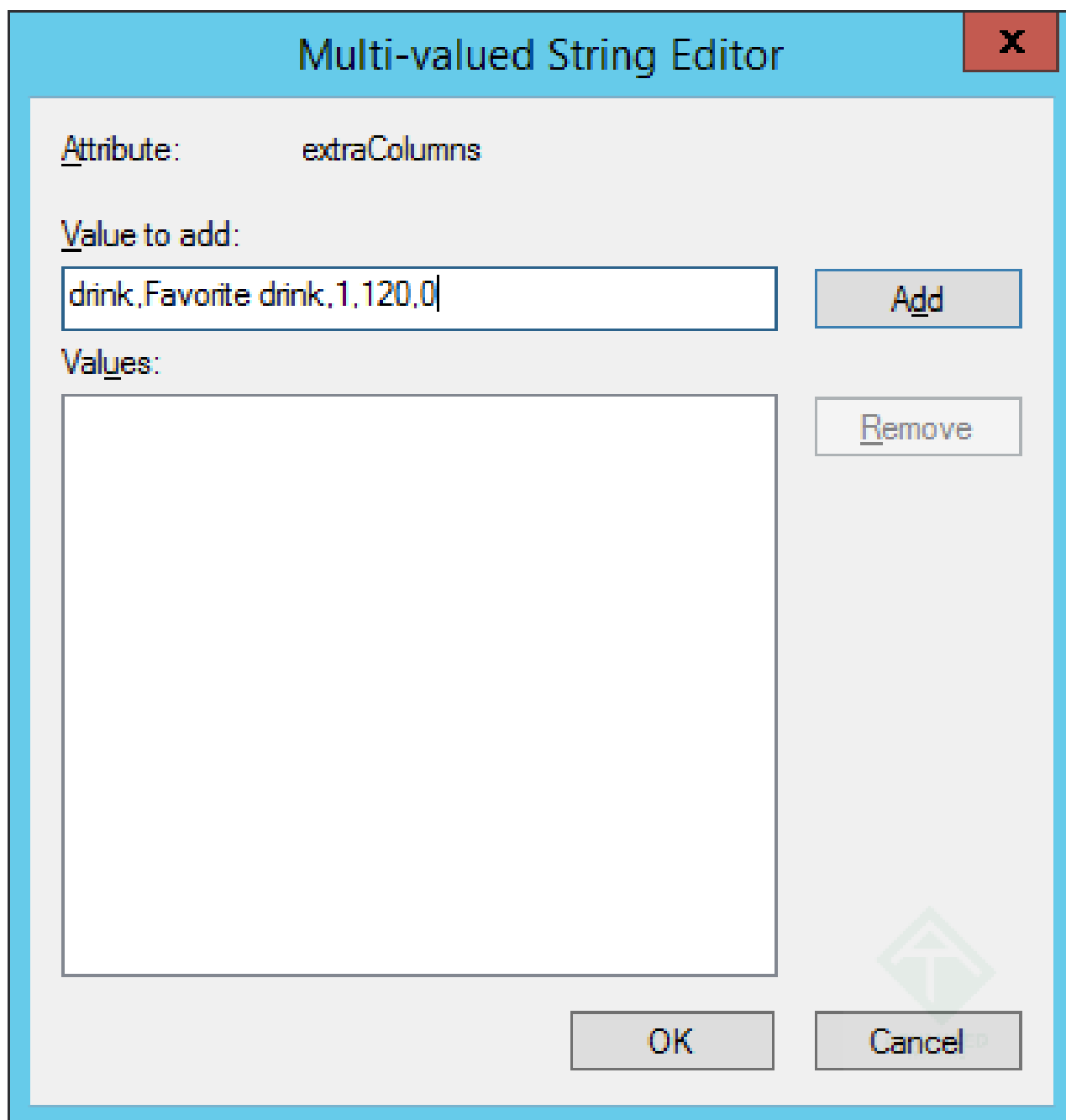
[Добавление новой колонки в отображение объекта user в Active Directory.](#)
(кликните для увеличения до 414 px на 462 px)

Кстати, если нам хочется, чтобы колонка отображалась вообще везде, где не указано какие колонки отрисовывать, надо взять объект **default-Display**.

Формат строки, описывающей дополнительную колонку, достаточно прост:

- Название атрибута
- Заголовок колонки с атрибутом
- Будет ли отображаться по умолчанию (мы поставим единицу)
- Стартовая ширина колонки в пикселях (если поставить -1, будет подобрана автоматически, мы поставим 120 пикселей)
- Зарезервированное на будущее значение, пока что ноль

Таких строк, как понятно, можно добавить несколько – всё зависит от того, что Вам конкретно надо отображать в первую очередь. Это удобнее, чем каждый раз кликать на пользователя, чтобы просмотреть нужный атрибут, отсутствующий в консоли Active Directory Users & Computers по умолчанию. В нашем случае всё будет выглядеть вот так:



Multi-valued String Editor

Atttribute: extraColumns

Value to add:

drink, Favorite drink, 1, 120, 0

Add

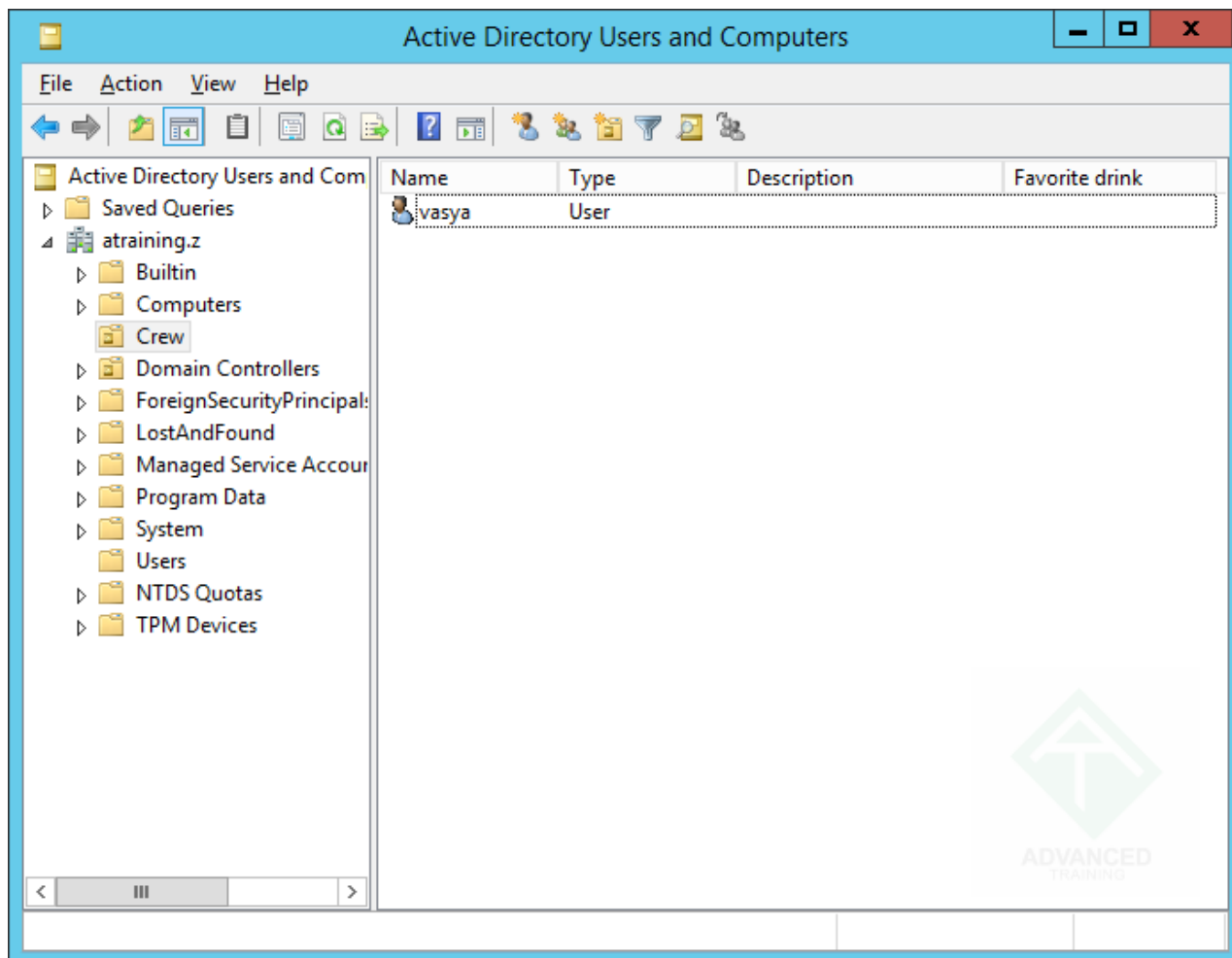
Values:

Remove

OK Cancel

[Дополнительная колонка с нужным атрибутом в Active Directory](#)
(кликните для увеличения до 376 px на 393 px)

А результат будет такой:



[Пользователь в Active Directory с информацией о предпочитаемой выпивке](#)
(кликните для увеличения до 694 px на 537 px)

Как понятно, и тип родительского контейнера, и тип объекта, и атрибут можно менять произвольно – плюсом будет то, что это не потребует никакой модификации стандартной консоли и будет сразу работать “из коробки” во всей организации. Редактировать атрибут можно произвольными методами – через вкладку Attribute Editor, через PowerShell – на выбор.

История третья – Как Все правозащитники помогали

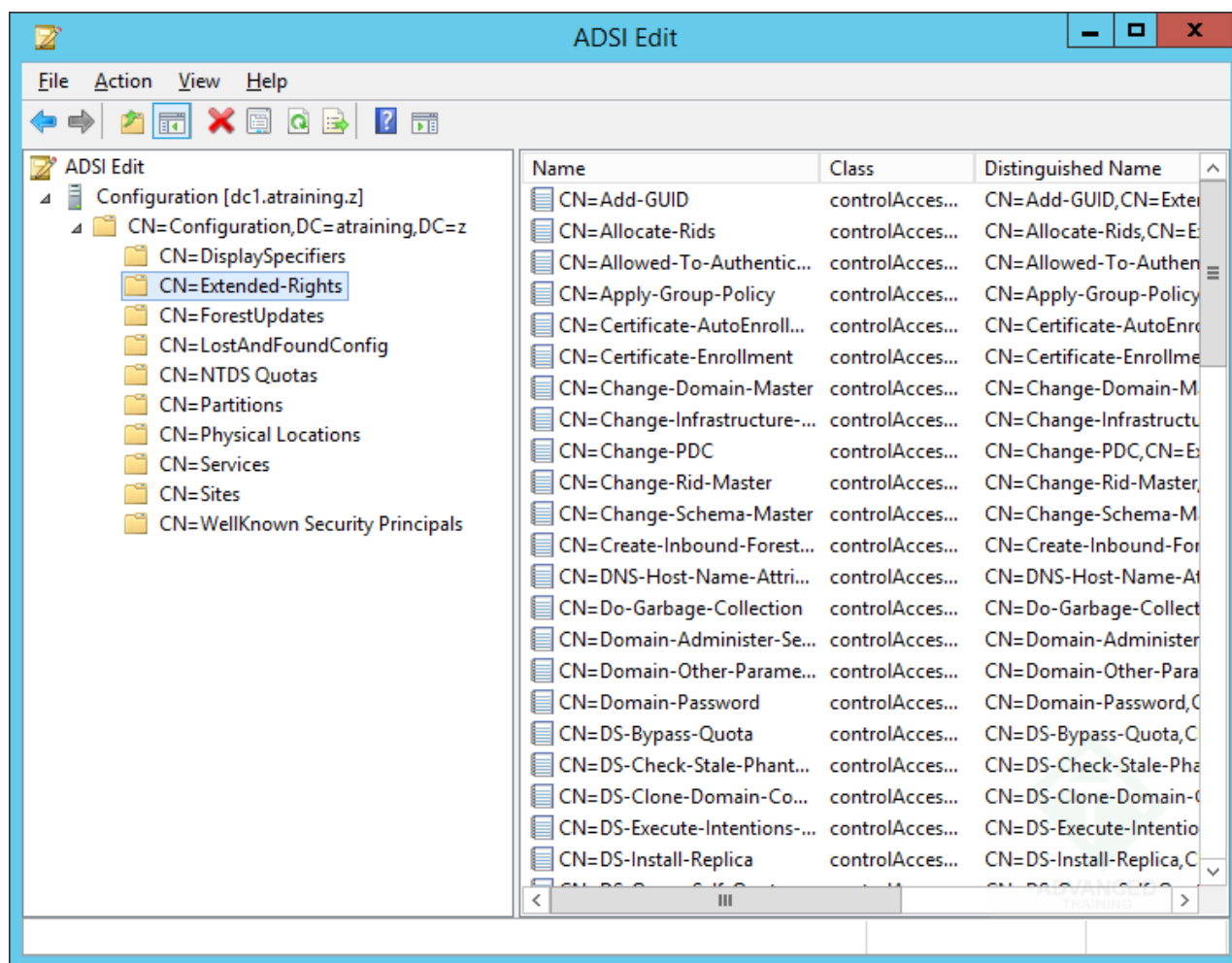
Однажды к одному CIO пришёл руководитель IT-департамента.

- Слышал вчера вопли у sales’ов. Михась орал на какого-то своего, мол, “Какое ты имеешь право пить на работе, скотина?”
- Да, работать в такой ситуации невозможно. Ведь администратору Active Directory непонятно по учётной записи пользователя, имеет ли он право пить на работе или нет. Отсюда непонимание, а это – корень всех бед в коллективе. Надо исправлять.

Действительно, надо что-то делать.

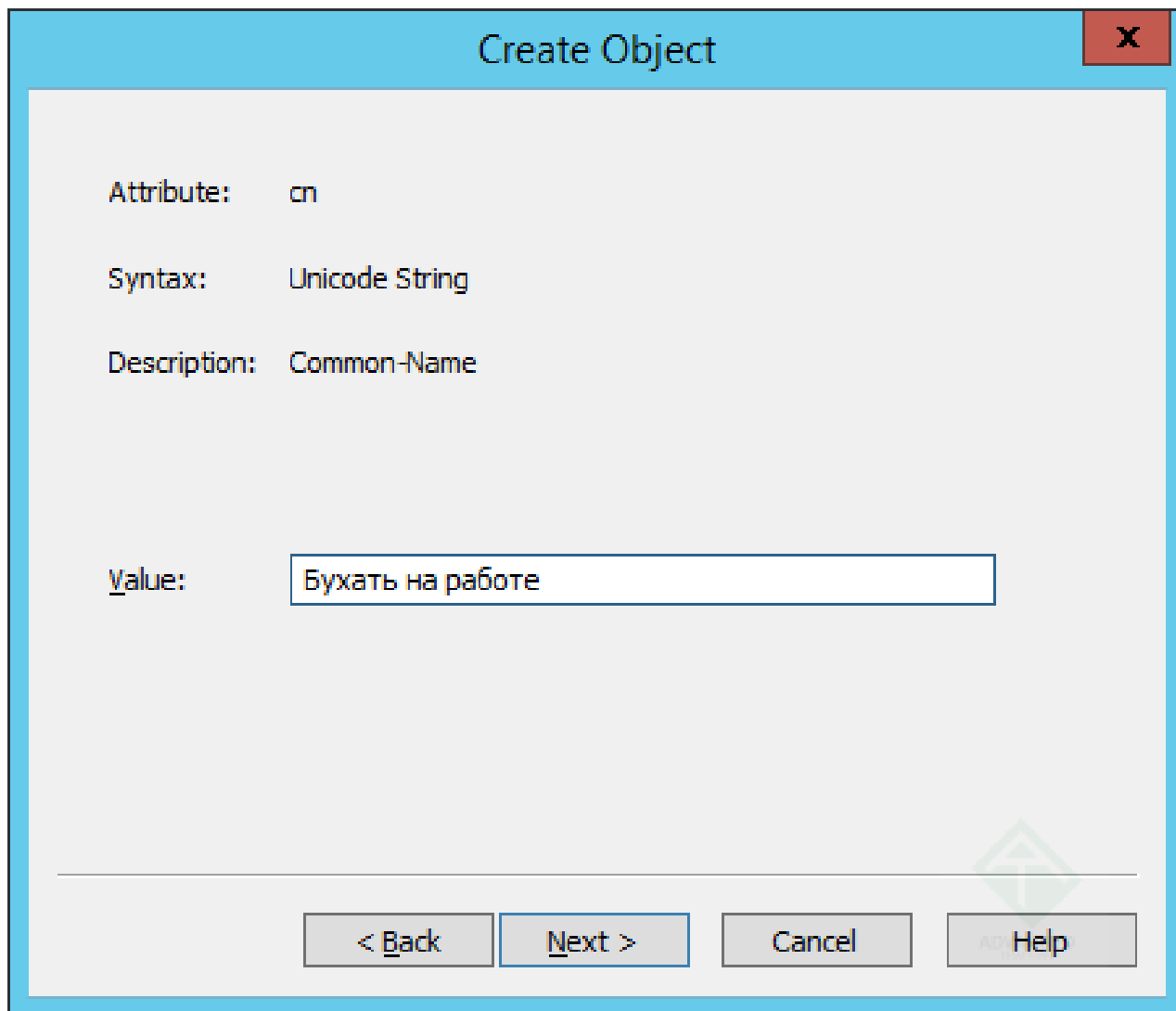
Последовательность действий

Типы прав в Active Directory – динамическая структура, поэтому мы добавим нужное нам право. Откроем ADSI и зайдём в контейнер **CN=Extended-Rights,CN=Configuration** в нашем лесу Active Directory.



[Список дополнительных прав в Active Directory](#)
([кликните для увеличения до 748 px на 579 px](#))

Мы создадим новый пустой экземпляр объекта класса **controlAccessRight** и назовём его предсказуемо:

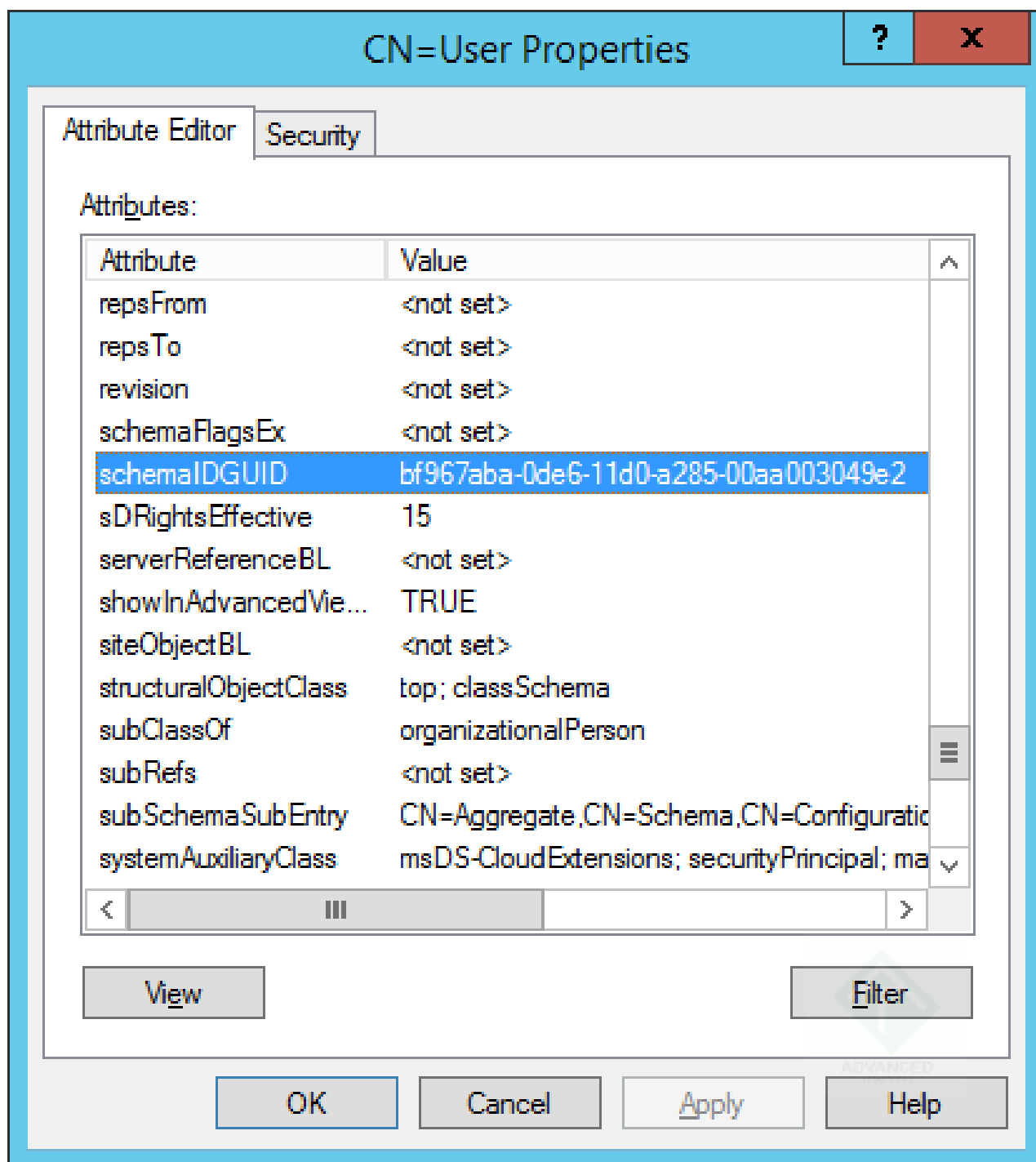


[Дополнительное право сотрудника, официально прописанное в Active Directory. \(кликните для увеличения до 451 px на 385 px\)](#)

Какие же нам надо будет задать атрибуты, чтобы всё заработало? Их не очень много.

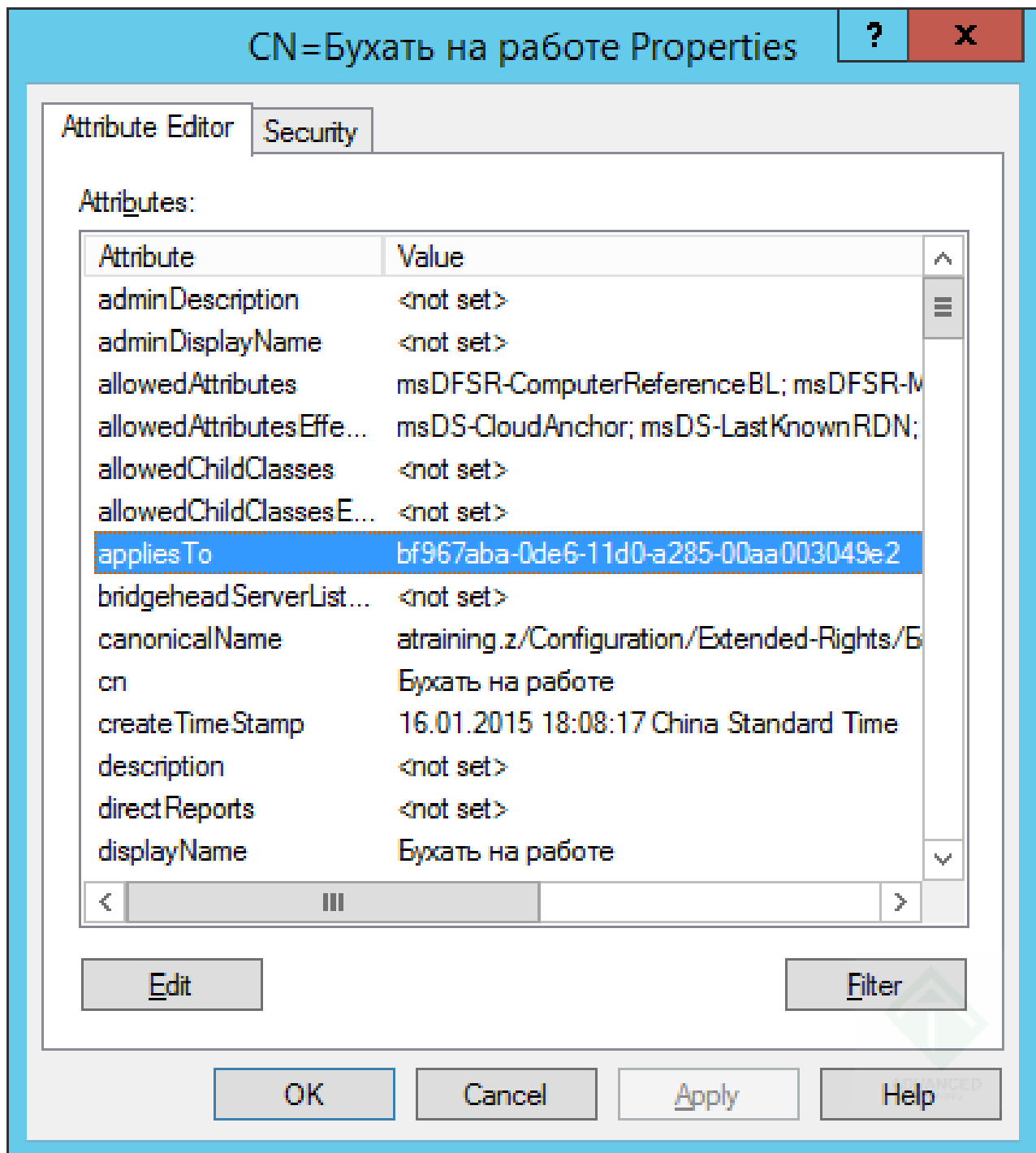
Настройка атрибутов у нового типа прав пользователя

Мы хотим, чтобы это право было у пользователя – открываем ADSI, зацепляемся за схему, находим там **classSchema** с названием **User**, и копируем у него атрибут **schemaIDGUID**:



[Атрибут, который мы укажем в appliesTo для связи нового типа права в Active Directory и объекта, на котором это право может применяться \(кликните для увеличения до 414 px на 462 px\)](#)

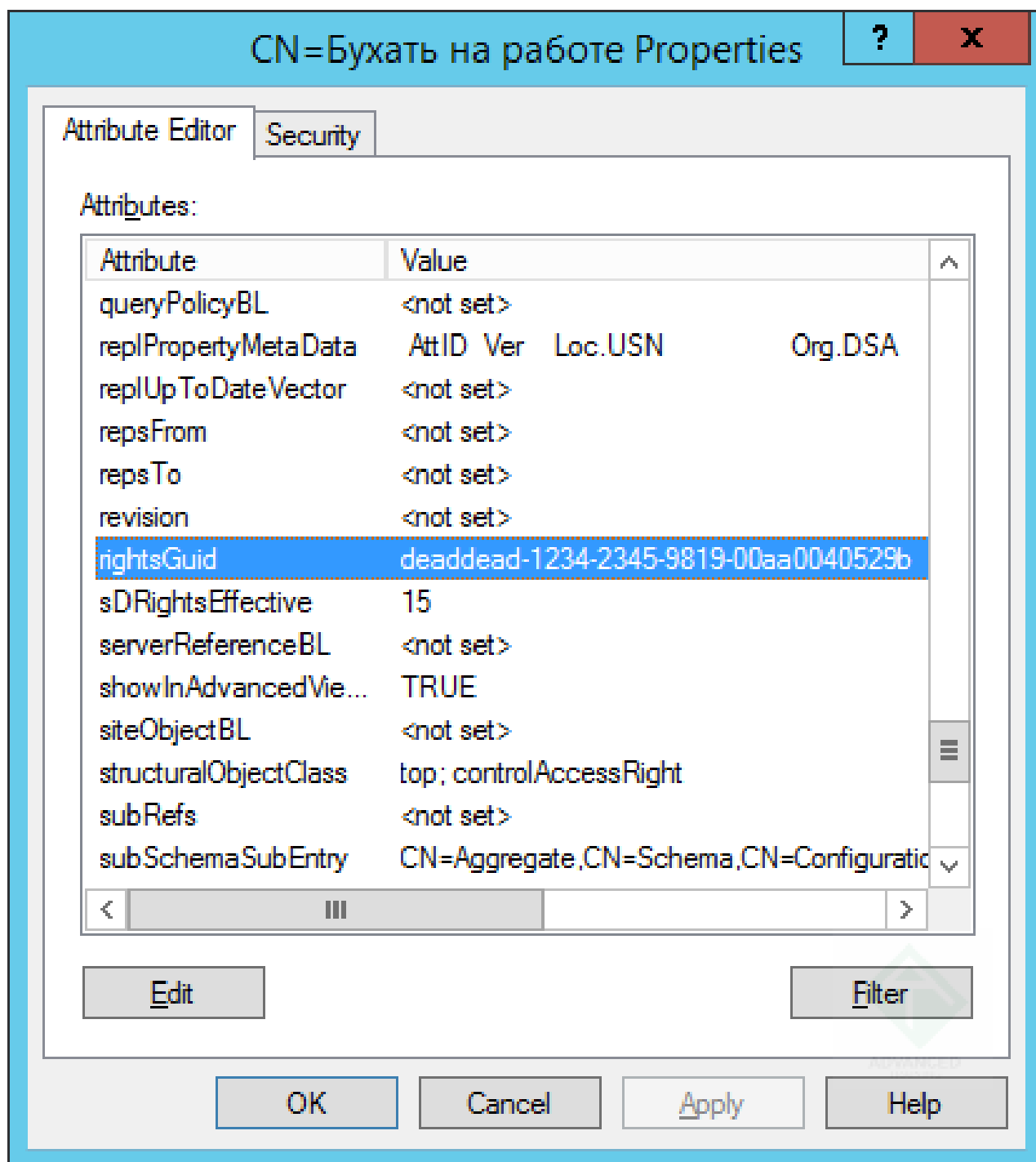
Этот GUID будет **bf967aba-0de6-11d0-a285-00aa003049e2**; мы добавим его в атрибут **appliesTo** у нашего нового типа прав:



[Выдача пользователю в Active Directory права бухать на работе](#)
(кликните для увеличения до 414 px на 462 px)

Объекта класса “пользователь” хватит – нам же не нужно, чтобы контроллер домена имел право бухать на работе.

Теперь добавляем читаемое имя у атрибута – в атрибут **displayName** нам надо будет добавить то, что будет выводиться при просмотре ACL штатными средствами – т.е. “человеческое” название этого права.



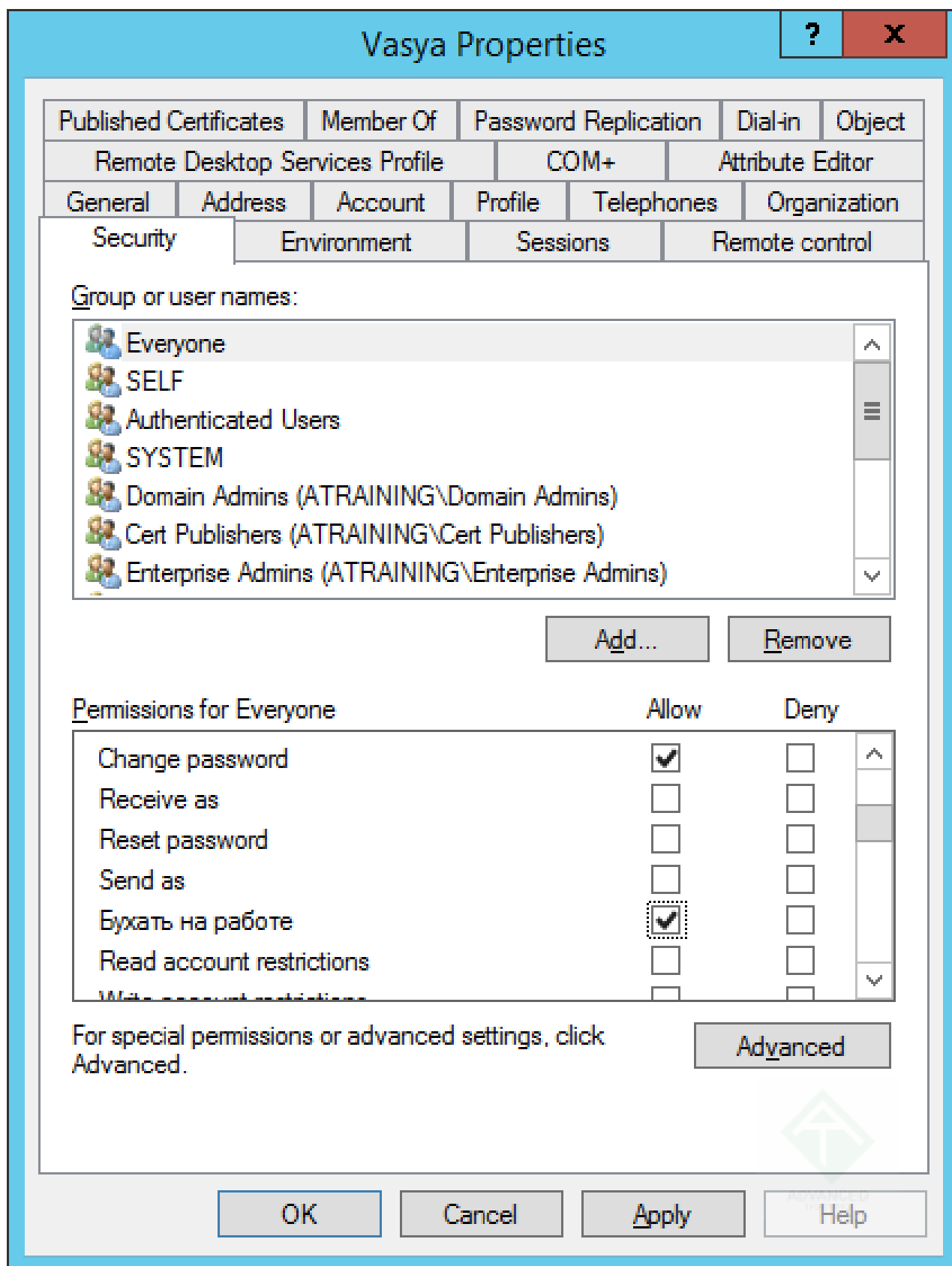
[Алкоголь - нейротоксин. Это знает даже GUID в Active Directory.](#)

[\(кликните для увеличения до 414 px на 462 px\)](#)

По GUID'у хорошо заметно, что бухать – вредно для здоровья.

Осталось только сказать, что это всё может работать – для этого в атрибут **validAccesses** запишем 0x100 (десятичное число 256) – это включит 9й бит (ADS_RIGHT_DS_CONTROL_ACCESS) в поле, отвечающем за “где это право показывать в диалогах по редактированию ACL’ов”, и мы наконец-то увидим плоды нашей работы.

Сделали? Смотрим.



[У пользователя Василия появились уникальные права](#)
[\(кликните для увеличения до 425 px на 563 px\)](#)

Теперь сотрудника Василия никто не упрекнёт, что он не может бухать на работе – может. Ну, а какое применение такой возможности он найдёт, да и Вы – тут уж сами думайте.

История четвертая – Родная сеть родного предприятия

Однажды к одному CIO пришёл руководитель IT-департамента.

- Никто не любит сотрудников техподдержки так, как люблю их я. Их, этих воинов переднего края, этот штрафбат духа и знаний, этот...
- Ты по делу, наверное?
- Да, есть косяк. Состоит он в том, что людям неудобно понимать, когда доменная машина “увидела сетку”, а когда – нет. Просветлённые понимают, а у остальных столько духовности, что их предположения “видит комп доменную сетку или вроде нет” заставляют меня потерять веру в человечество. А ведь без веры нельзя жить.
- Понимаю. Устроит ли ситуация, когда факт нахождения в доменной сети будет идентифицироваться путём отображения на сетевом интерфейсе логотипа фирмы с соответствующей подписью?
- Вполне.

Действительно, так будет удобнее. Делаем.

Последовательность действий

В момент, когда Windows подключается к новой сети, пользователю предлагается выбор – домашняя ли это сеть, рабочая или “внешняя”-гостевая. В зависимости от того, что выберет пользователь, будут установлены настройки общего доступа, а также ряд других параметров. Во что ткнёт пользователь – неизвестно. Отсюда “Подключение по локальной сети 5” с картинкой домика, а впоследствии – вагон разных сетей с жуткими именами и невнятными задачами – поди вспомни, откуда это подключение номер пять взялось – то ли когда в Макдоналдсе сидел, то ли когда дома роутер купил и в него переподключился. Для сотрудников техподдержки же крайне желательно, чтобы можно было задать вопрос “В какой Вы сейчас сети?” и получить относительно вменяемый ответ.

Для начала мы возьмём откуда-нибудь иконку с логотипом нашей организации. Ей хватит размера 64×64 пикселя. Я буду использовать этот файл для примера:



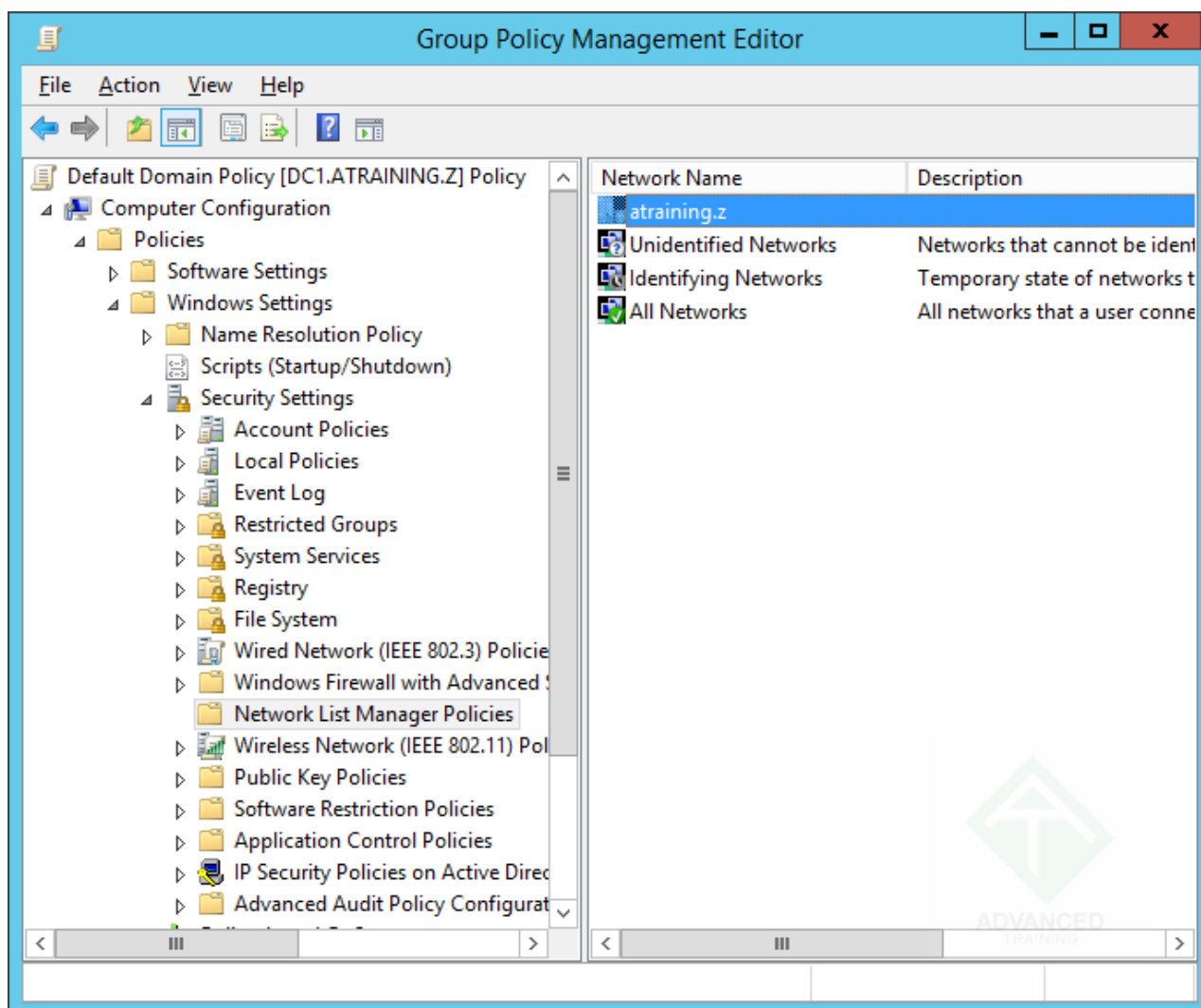
[Логотип Advanced Training](#)

[\(кликните для увеличения до 300 px на 300 px\)](#)

Теперь можно открыть объект групповой политики, действующий на доменные компьютеры, на которых нужно изменить отображение и логику определения сетей, и зайти там в следующий раздел:

Computer Configuration / Policies / Windows Settings / Security Settings / Network List Manager Policies

Так как я редактирую политики с контроллера домена, который уже находится в домене (что, в общем-то, логично), то картинка будет выглядеть примерно так:



[Список доступных сетей](#)

[\(кликните для увеличения до 686 px на 572 px\)](#)

Три строчки из четырёх – это Unidentified Networks, Identifying Networks, All Networks – стандартные, а четвёртая – мой тестовый домен **atrainig.z**. Для начала, поменяем настройки для стандартных объектов.

Настройки для Unidentified Networks

Здесь будет две настройки – Location Type и User Permissions. Первая будет обозначать то, как будет трактоваться местоположение для неизвестных сетей – как частная сеть (Private), общедоступная (Public) либо отдаваться на откуп локальному пользователю (т.е. у него при подключении новой сети будет то самое окно с выбором из 3х вариантов типов сетей – домашней, предприятия или общедоступной). Мы выставим их так – Location Type сделаем **Public**, а пользователю запретим менять тип Unidentified сети (**User cannot change location**). Это отсекает ситуации, когда пользователь неверно определит тип сети (допустим, в кафе поставит сеть как домашнюю), что ощутимо снизит уровень безопасности (например, появится возможность обнаружения других устройств, да и возможности в плане общего доступа к ресурсам, которые никак не нужны в сети кафе).

Настройки для Identifying Networks

Это те сети, которые находятся “в процессе” идентификации. Визуально это рисуется анимацией на иконке подключения, занимает обычно некоторое количество секунд. Настройка здесь одна – “как трактовать тип сети, находящейся в этой фазе”. Почему она важна? Потому что если пользователь хоть раз выбирал вручную тип новой сети, добрая операционная система дала ему возможность выставить галку вида “... И все дальнейшие новые сети считать такими же, как ты выбрал сейчас”. Это уязвимость, потому что ситуация может быть простой – человек дома поставил новый роутер, ОС повторно “нашла” локальную сеть, предложила выбрать – человек выбрал, что сеть доверенная, домашняя, и нажал галку “больше меня не спрашивай, остальные неизвестные сети такие же”. В результате, когда он пойдёт в кафе, где есть Wifi, у него сеть, будучи в процессе Identifying, будет трактоваться как домашняя, давая излишние возможности его соседям по IP-диапазону.

Мы выставим этот параметр как **Public** – т.е. любая сеть, которая “в процессе определения”, будет по определению общедоступной, внешней, и к ней будут применяться максимальные ограничения по совместной работе и доступу к соседским ресурсам.

Настройки для All Networks

Это общие настройки для всех сетей. Логика их действия простая – если что-то не зафиксировано администратором, то это можно изменять пользователю. Так как речь идёт о рабочей системе, то такие настройки неправильные. Мы явно определим сеть предприятия, если надо – так же, через политики, раздадим настройки беспроводных сетей. Пользователю не нужно ничего менять. Соответственно, мы выставляем следующие настройки:

All Networks Properties

User Permissions

These permissions control if users can change the network name, location, or icon.

Network name

- ☐ Not configured
- ☐ User can change name
- ☒ User cannot change name

Network location

- ☐ Not configured
- ☐ User can change location
- ☒ User cannot change location

Network icon

- ☐ Not configured
- ☐ User can change icon
- ☒ User cannot change icon

OK Cancel Apply

[Хорошие и безопасные настройки All Networks](#)
(кликните для увеличения до 414 px на 462 px)

Теперь пришла очередь настроить отображение и настройки нашей, доменной сети.

Настройки для родной сети предприятия

Их будет четыре, и они будут распределены по двум вкладкам. Можно будет задать картинку, имя сети, и права пользователей на смену картинки и имени. Права мы, конечно, отнимем, а название сети и картинку сменим:

atraining.z Properties

Network Name

Network Icon

A network name identifies a network.

Name

☐ Not configured

☒ Name

Сеть Advanced Training

User permissions

☐ Not configured

☐ User can change name

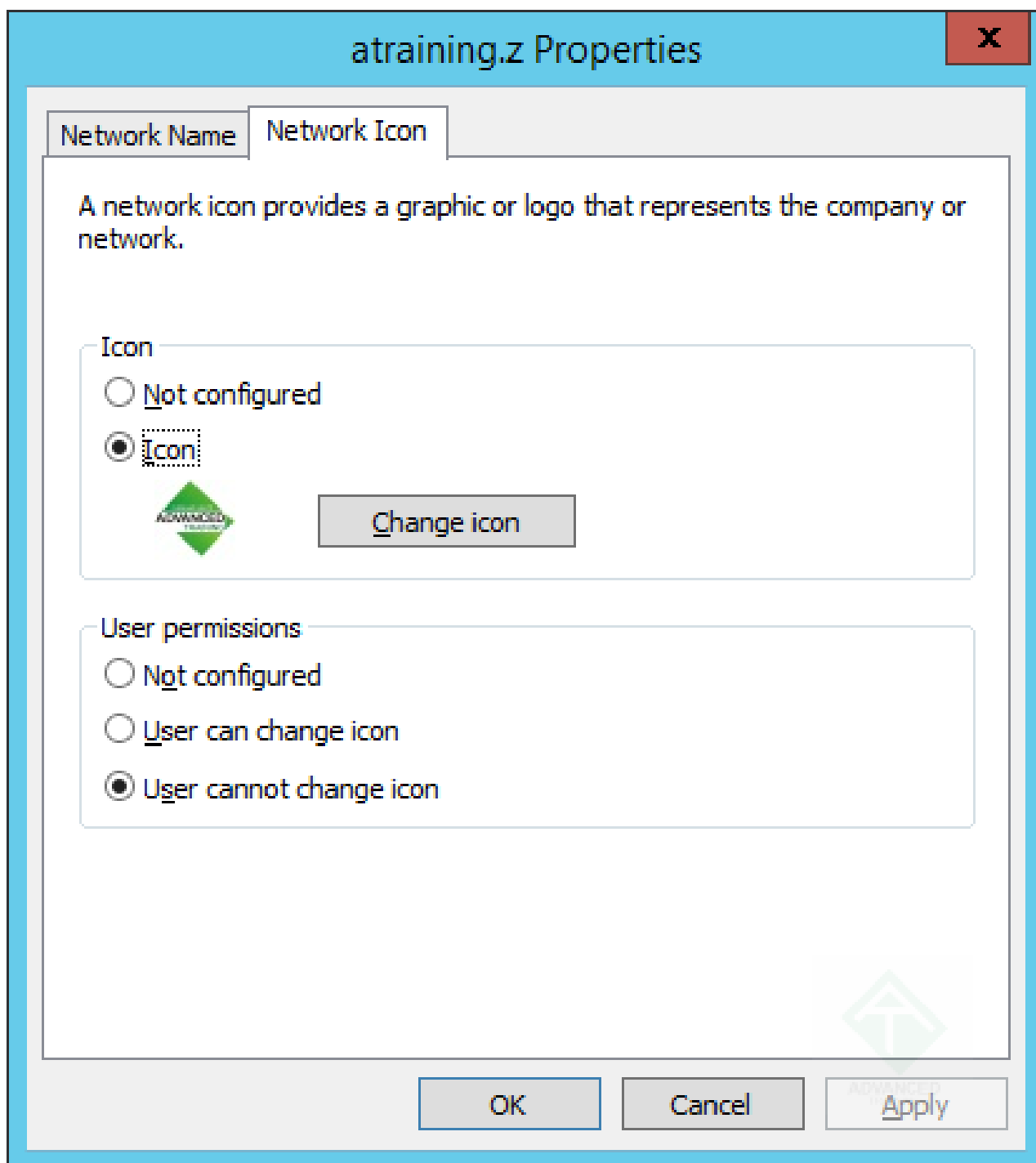
☒ User cannot change name

OK

Cancel

Apply

[Задаём личное имя для доменной сети](#)
([кликните для увеличения до 414 px на 462 px](#))



[Задаём личную картинку для доменной сети](#)
(кликните для увеличения до 414 px на 462 px)

Важный момент – картинку мы будем хранить в SYSVOL'е и задавать её местоположение тоже через UNC. Поэтому наши доменные рабочие станции будут забирать картинку с ближайшего SYSVOL, реплицироваться она будет автоматически, и её не надо будет куда копировать вручную.

В результате этих действий повысилась безопасность – пользователь не может объявить все сети домашними и таким образом ослабить защиту своего хоста. Мелочь, никакого шаманства и кодинга, а из таких мелочей состоит то, что с точки зрения ряда восточных практик отличает работу от искусства. ActiveDirectory-до лучше, чем ActiveDirectory-дзюцу.

Выводы

Задача “сделать Active Directory чуть менее формальной и дефолтной” решена – это лишь часть возможностей, которые предоставляет Active Directory – их масса. Главное – [знания](#).

Удач.