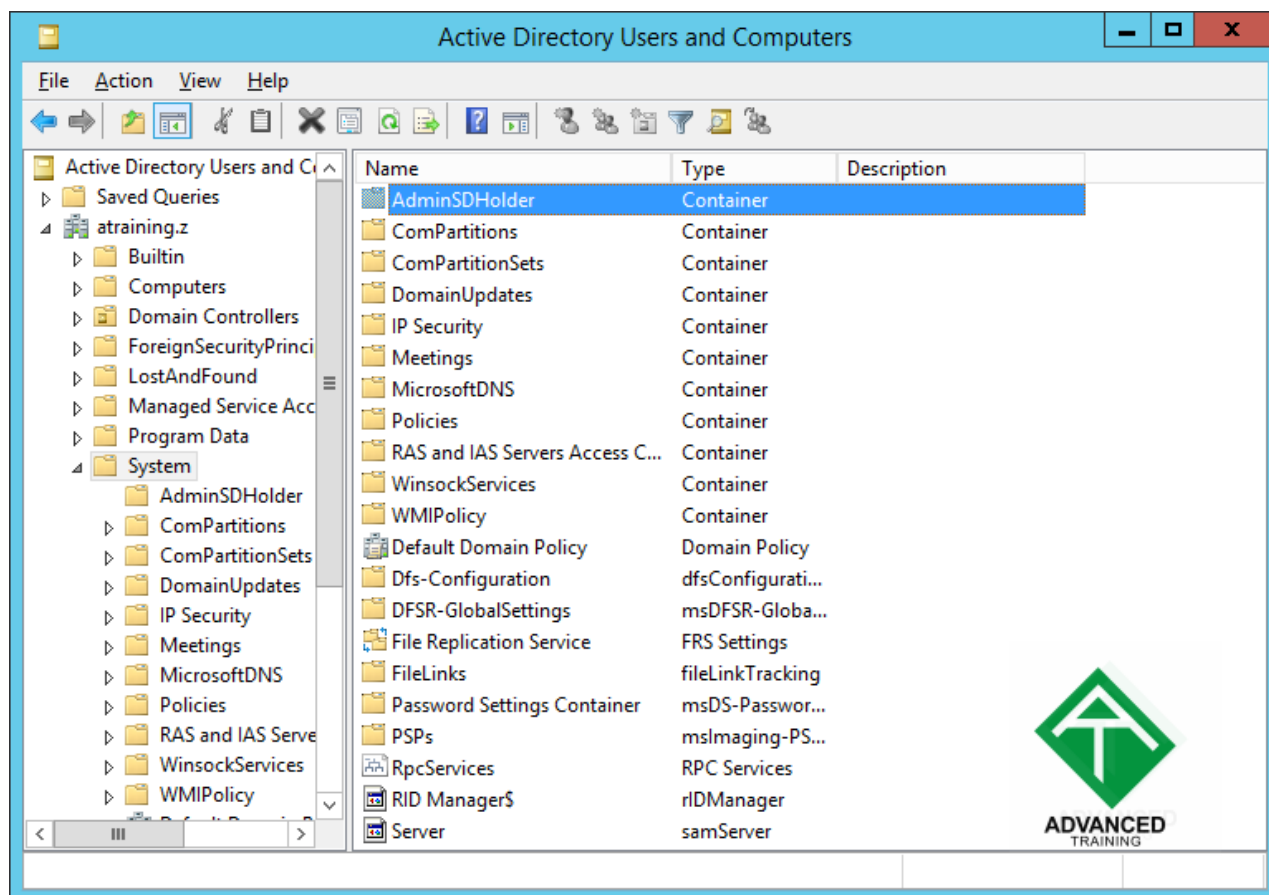


Механизмы SDProp и AdminSDHolder - работа с защищёнными группами Active Directory

 atraining.ru/adminsdholder-protected-groups

2013-10-04T09:01:31+08:00



Привет.

В данной статье я расскажу про мелкую, но интересную функциональную единицу в составе Active Directory – механизм управления безопасностью критических security principal'ов, обычно называемый по ключевому участвующему объекту AdminSDHolder, и использующему SDProp. Рассказ будет про современную реализацию – в Windows Server 2012 R2 / Threshold, ну а детали про предыдущие реализации буду упоминать при необходимости. Для мелкого тюнинга я буду использовать [Atcmd](#).

Работаем с защищёнными группами, SDProp и AdminSDHolder

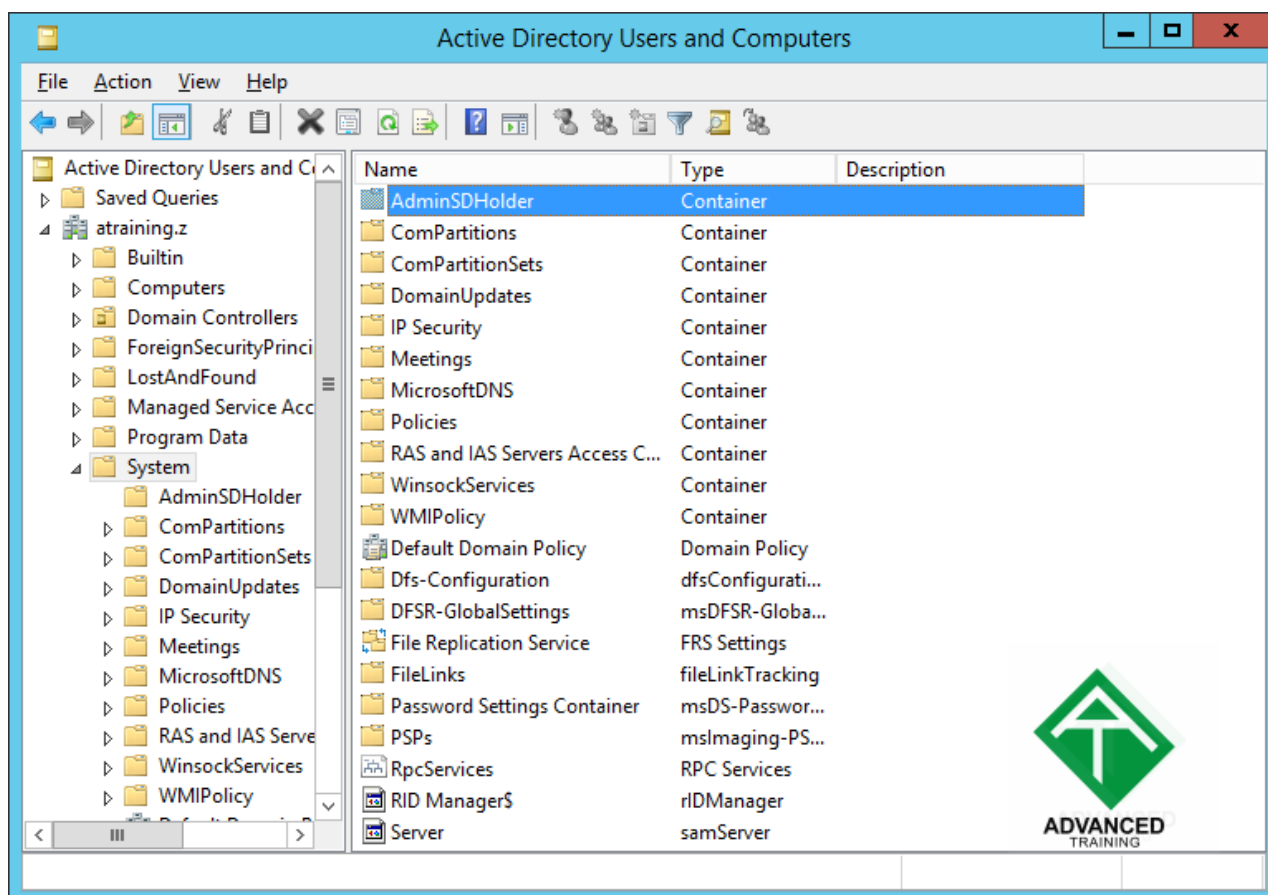
- Что и как делает данный механизм
- Какие группы и учётные записи будут защищаться SDProp / AdminSDHolder?
- Как изменить, какие группы подпадают под око Большого Брата
- Как изменить периодичность запуска SDProp
- Как запустить процесс обработки AdminSDHolder вручную
- Специфика работы с distribution groups

- Что такое orphaned AdminSDHolder objects

Поехали.

Что и как делает данный механизм

Для установки прав в Active Directory используется SDProp (Security Descriptor propagator) – периодически иницилирующийся на контроллерах домена механизм, приводящий в порядок ACL'ы объектов в Active Directory. В нашем случае, для узкоспецифичной задачи управления ACL'ами у критичных security principal'ов, данный механизм запускается на держателе FSMO-роли PDC, и устанавливает ACL'ы у некоторых важных объектов Active Directory в соответствие с образцовым ACL. Этот образцовый ACL, в свою очередь, в каждом домене в лесу Active Directory будет уникальным и будет браться из объекта AdminSDHolder. По сути, данный объект будет нужен только затем, чтобы хранить в своём ACL информацию о настройках безопасности для специфического подмножества security principals, называемых “защищёнными”. В основном это BUILTIN-группы, но будут и учётки пользователей. Сам же объект AdminSDHolder будет располагаться в domain partition, в контейнере System. Вот он:



[Объект AdminSDHolder в Active Directory](#)
[\(кликните для увеличения до 768 px на 537 px\)](#)

Суть работы всего механизма будет достаточно простой. Как упомянуто выше, он будет иметь жёстко прописанный список security principal'ов (разный в зависимости от версии серверной ОС, установленной на DC с ролью PDC Emulator – поэтому

важно, чтобы держатель данной роли был наивысшей доступной версии Windows Server в случае, если в домене есть разные DC), и, с определённой периодичностью (по умолчанию раз в час), будет находить всех security principals, входящих в список защищаемых, и после – выставлять им ACL в соответствии с ACL'ом от объекта AdminSDHolder. Чтобы исключить влияние унаследованных прав, наследование ACL будет выключено – признак отказа от наследования ACL также будет устанавливаться механизмом SDProp.

Зачем это будет нужно?

Первое – это проблема явно объявленных ACE. Ну, к примеру, админ, увольняясь, может напоследок сделать какую-нибудь “приятную мелочь” – например, разрешить любому из **Domain Users** сбрасывать пароль одному из **Account Operators**, а у оных уже прописать такое же право, но на **Enterprise Admins**. Такое вручную вычислить достаточно сложно, да и утомителен такой аудит. Механизм SDProp же делает ACL'ы учётных записей, находящихся в “защищённых группах”, предсказуемыми и страхует от случайного или преднамеренного изменения, решая эту проблему превентивным способом – просто, в нашем примере, при очередном срабатывании скинув ACL у **Account Operators** и **Enterprise Admins** на стандартный.

Второе – учётные записи, входящие в “защищённые группы”, могут быть в любом месте иерархии Active Directory. Соответственно, на них могут действовать унаследованные ACL'ы, которые будут изменять ситуацию с безопасностью критичных учётных записей. Рассматриваемый механизм блокирует наследование ACL'ов для всех целевых учётных записей.

Теперь посмотрим, кто под него подпадает.

Какие группы и учётные записи будут защищаться SDProp / AdminSDHolder?

Простейший критерий для определения того, кто будет жертвами рассматриваемого механизма – это проверка атрибута **adminCount**. Этот атрибут будет равен единице у тех security principal'ов, кто подпадает под SDProp.

Делаем поиск штатным фильтром обычной оснастки Active Directory Users & Computers:

Edit Query

?

x

Name:

AdminSDHolder affected

Description:

Query root:

...\atraining

Browse...


☒ Include subcontainers

Query string:

(&adminCount=1)

Define Query...

OK

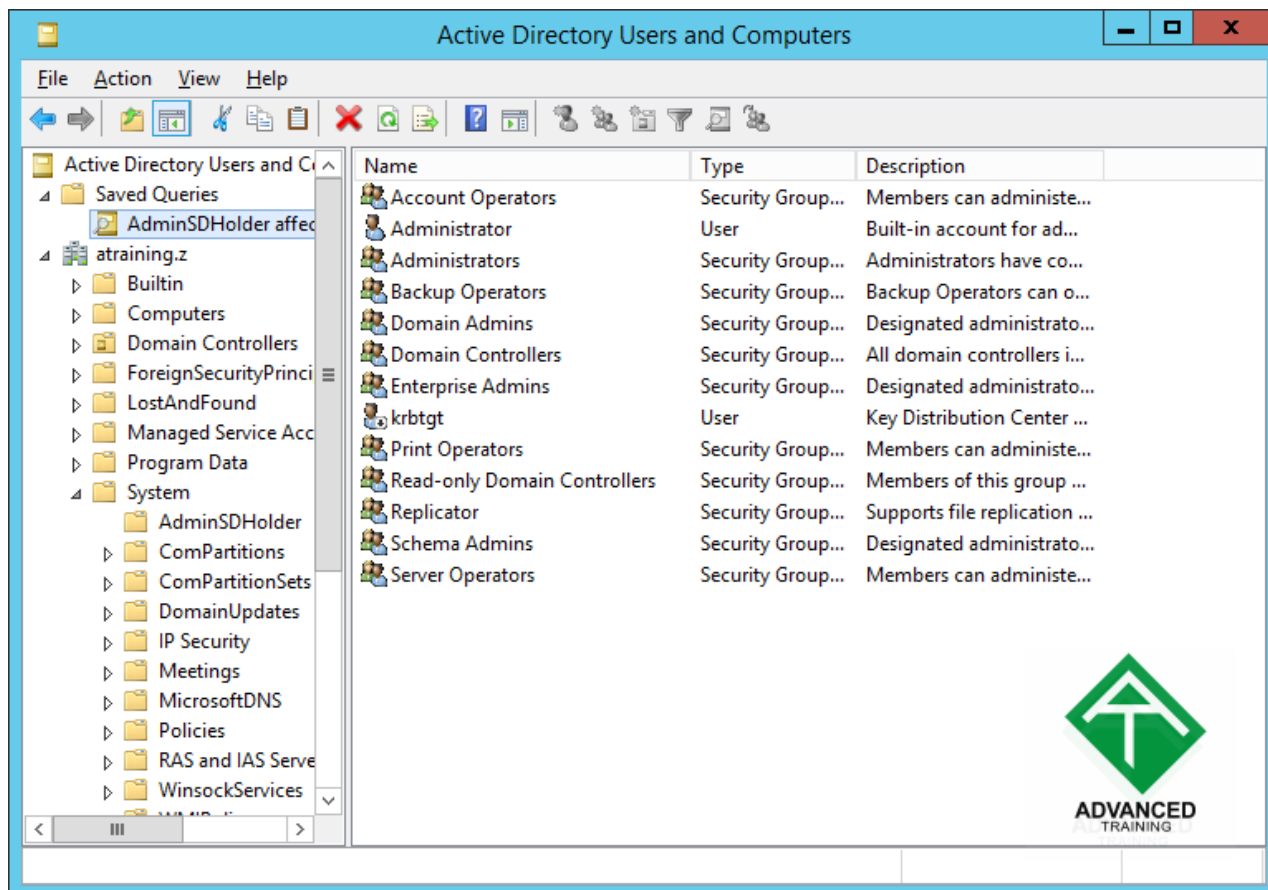


Advanced Search

Cancel

[Фильтр для поиска всех объектов, защищаемых SDProp и AdminSDHolder](#)
(кликните для увеличения до 394 px на 359 px)

Результат:



[Защищаемые SDProp и AdminSDHolder объекты в Windows Server](#) ([кликните для увеличения до 768 px на 537 px](#))

Итак, для Windows Server 2012 R2 это будут:

- Administrator
- krbtgt

Administrators

- Account Operators
- Backup Operators
- Print Operators
- Server Operators

- Domain Admins
- Enterprise Admins
- Schema Admins

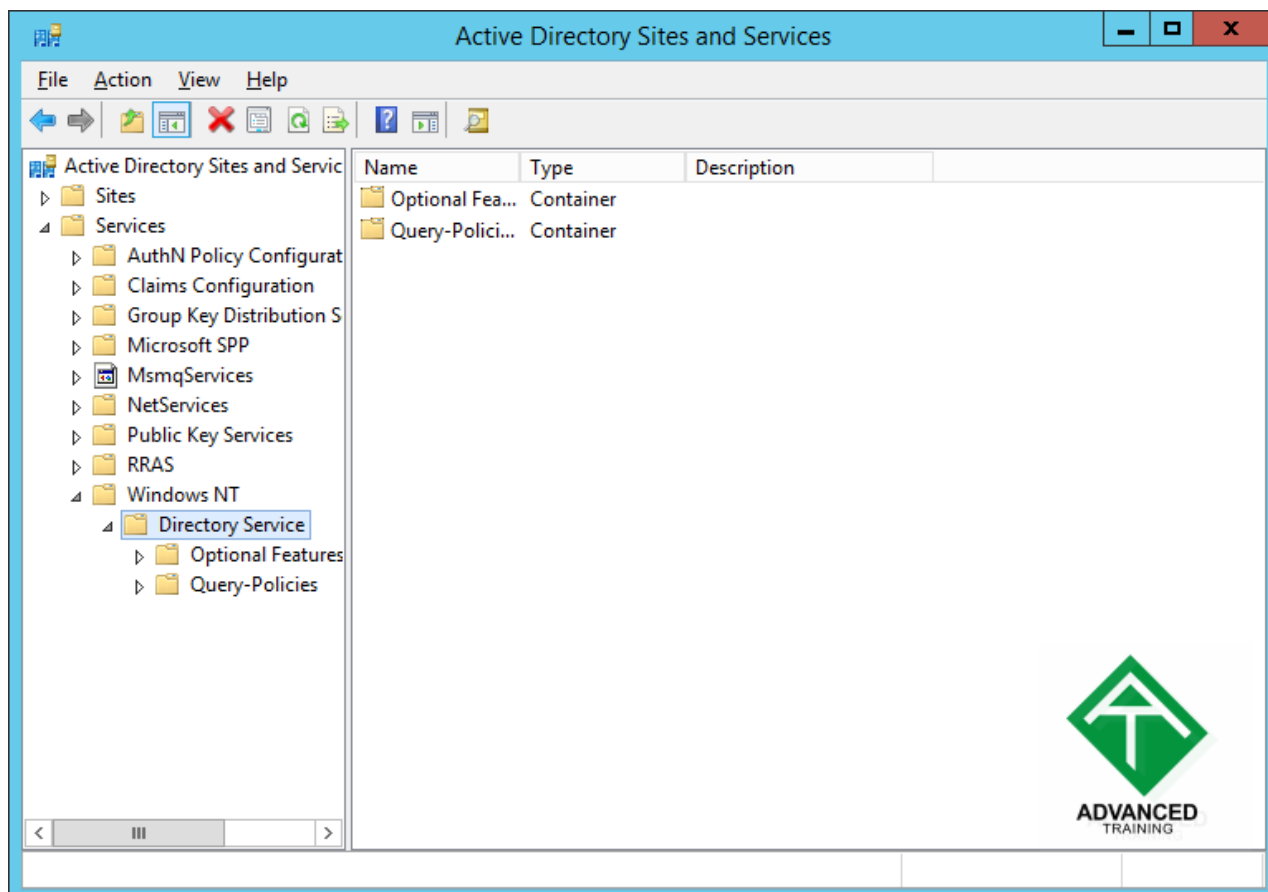
- Domain Controllers
- Read-only Domain Controllers

Replicator

Как изменить, какие группы подпадают под око Большого Брата

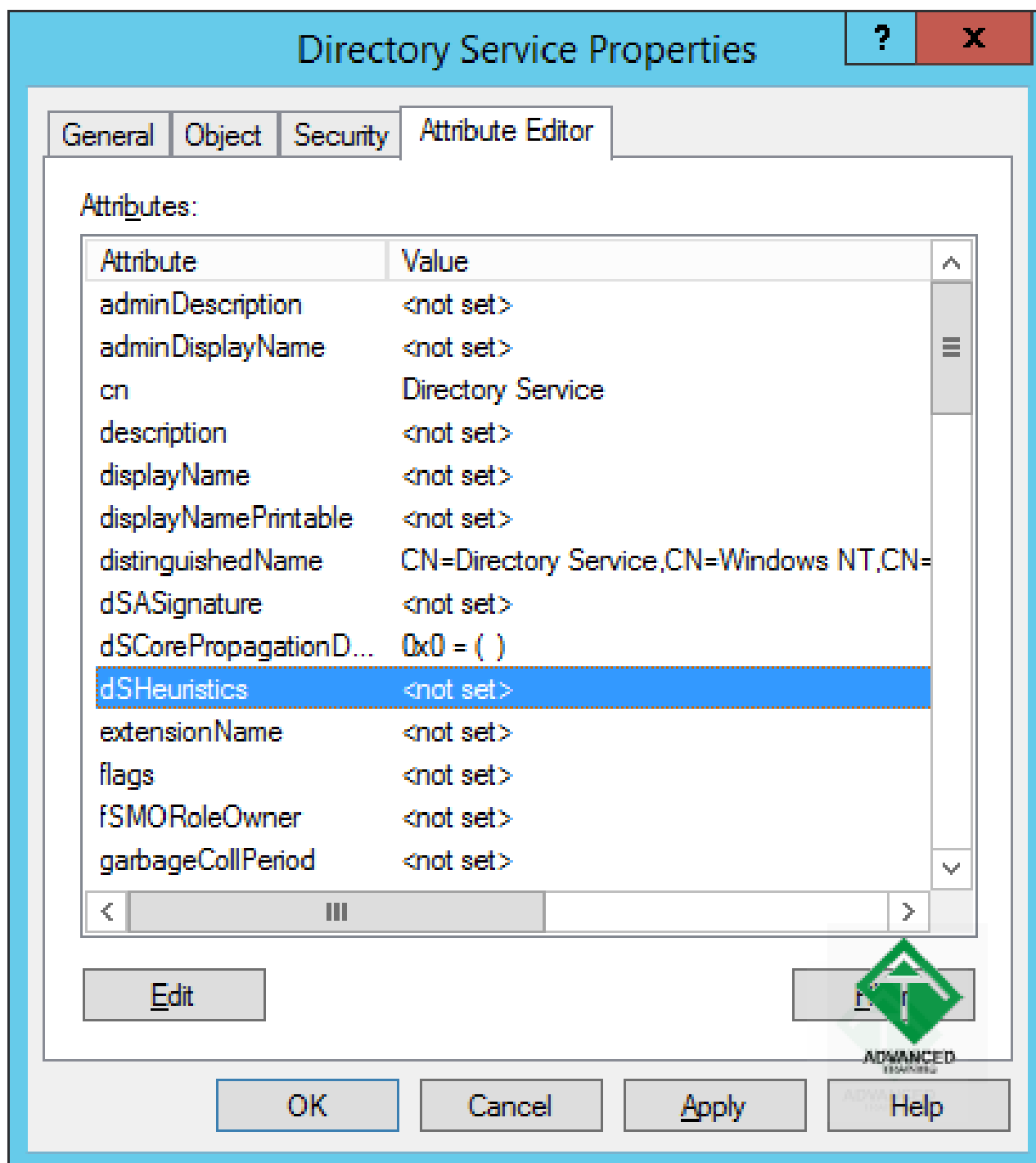
На практике возможна ситуация, когда постоянная “прокатка” ACL’ов для определённых security principals нежелательна. Это частично решаемо следующим образом (частично – потому что вывести из-под этого механизма можно только одну или несколько групп семейства Operators, для других security principals это не получится):

В разделе Configuration есть объект с DN вида **CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=корневой_домен_леса**:



[Объект управления всеми DC в лесу, Directory Service](#)
([кликните для увеличения до 768 px на 537 px](#))

У этого объекта есть замечательный атрибут – **dsHeuristics**:



[Настройка dsHeuristics для управления SDProp](#) ([кликните для увеличения до 414 px на 462 px](#))

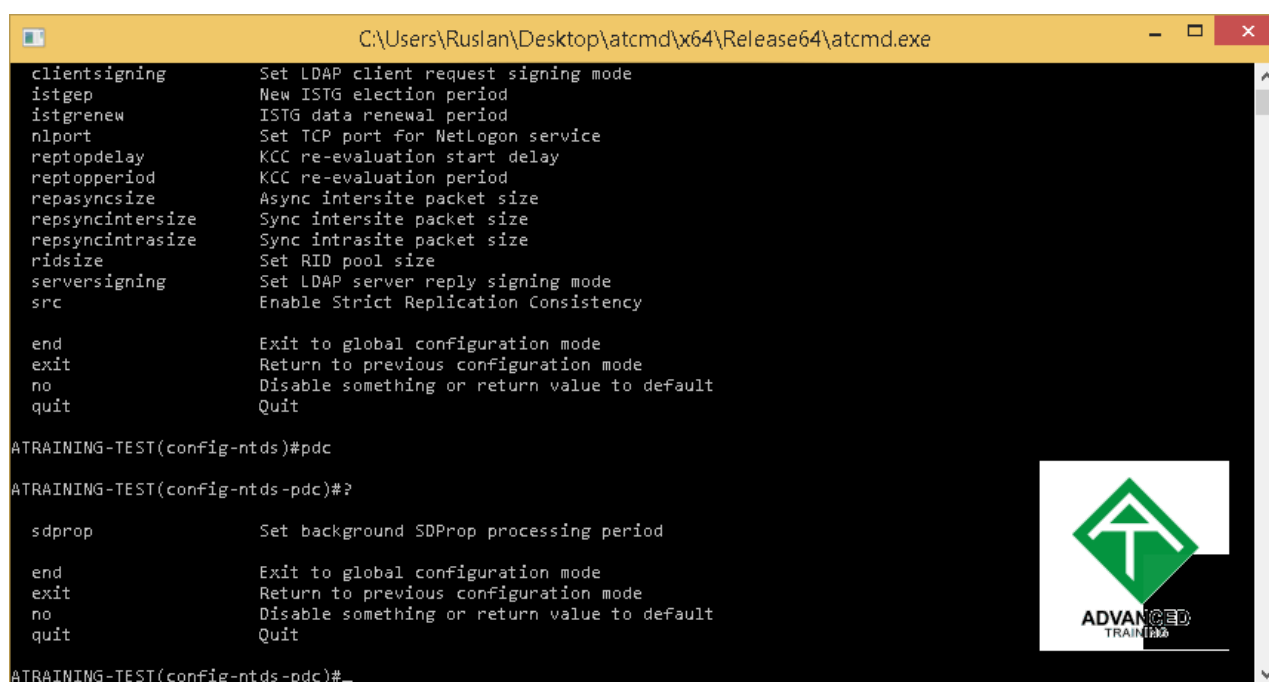
Данный атрибут выглядит как Unicode-строка, где 16й по порядку шестнадцатеричный разряд – это группа из 4х бит, которые, будучи включенными, обозначают:

- Нулевой бит – исключить из процесса **Account Operators**
- Первый бит – исключить из процесса **Server Operators**
- Второй бит – исключить из процесса **Print Operators**
- Третий бит – исключить из процесса **Backup Operators**

То есть, если захотите поправить – подумайте, какие группы хотите исключить, вычислите итоговое значение, откройте данный атрибут (он может выглядеть как-то так: **000000000100000c**) и поправьте. В примере у меня на 16й позиции символ “C”, это значит, что Print Operators (которые 0100) и Backup Operators (которые 1000) исключаются из процесса. Учитывайте, что несмотря на то, что механизм реализуется каждым PDC-эмулятором лично, в своём домене, данная настройка – на уровне леса, и будет учитываться всеми PDC-эмуляторами в лесу. И будьте осторожны – каждый символ в этом поле обозначает настройки какой-либо подсистемы, не заденьте лишнего.

Как изменить периодичность запуска SDProp

Это несложно делается через [Atcmd](#) – надо только зайти в контекст **ntds**, в нём в субконтекст **pdc**, и там есть команда **sdprop**:



```
C:\Users\Ruslan\Desktop\atcmd\x64\Release64\atcmd.exe

clientsigning      Set LDAP client request signing mode
istgep            New ISTG election period
istgrenew          ISTG data renewal period
nlport            Set TCP port for NetLogon service
reptopdelay       KCC re-evaluation start delay
reptopperiod      KCC re-evaluation period
repasynthesize    Async intersite packet size
repasynthesize    Sync intersite packet size
repasynthesize    Sync intrasite packet size
ridsize           Set RID pool size
serversigning     Set LDAP server reply signing mode
src               Enable Strict Replication Consistency

end               Exit to global configuration mode
exit              Return to previous configuration mode
no                Disable something or return value to default
quit              Quit

ATRAINING-TEST(config-ntds)#pdc
ATRAINING-TEST(config-ntds-pdc)#?

sdprop            Set background SDProp processing period
end               Exit to global configuration mode
exit              Return to previous configuration mode
no                Disable something or return value to default
quit              Quit

ATRAINING-TEST(config-ntds-pdc)#
```

[Настройка периодичности запуска SDProp на PDC emulator](#) (кликните для увеличения до 859 px на 454 px)

Понятно, что данная настройка имеет смысл только на DC, держащем FSMO-роль PDC-эмулятора. Да, и после изменения периода надо будет перезапустить службу ADDS – до этого значение не вступит в силу. Диапазон допустимых значений ограничен – не менее 1й минуты и не более 2х часов.

Как запустить процесс обработки AdminSDHolder вручную

Для этого есть только один надёжный способ – вызов на корневом объекте домена **rootDSE** операции **runProtectAdminGroupsTask**. Для этого надо будет запустить утилиту **ldp.exe**, вначале подключиться (сделать **ldap_connect**) к держателю роли PDC-эмулятора, после – подтвердить свои права авторизацией (через **ldap_bind**), ну а после – “заказать” операцию, выбрав в меню Browse->Modify, указав название

‘атрибута’ – **runProtectAdminGroupsTask**, значение = **1**, тип операции **Add**, нажав Enter и после того, как запись добавлена в список поставленных на выполнение операций – нажав Run. Значение **DN** надо оставить пустым.

Modify

DN:

Edit Entry

Atttribute:

Values:

Operation

☒ Add ☐ Delete ☐ Replace

Entry List

☒ Synchronous

☐ Extended

[Запуск SDProp вручную](#)

[\(кликните для увеличения до 344 px на 385 px\)](#)

Примечание: До Windows Server 2008 R2 это делалось так же, но использовалась другая операция – **FixUpInheritance**, и вместо единицы в качестве значения надо было указывать **Yes**.

В общем-то из ключевого это всё. Теперь тонкости.

Специфика работы с distribution groups

Классикой жанра является заблуждение, что “у distribution-групп нет SID’а”. SID есть у всех объектов класса group, потому что данный объект относится к security principal. Если бы у distribution-групп не было SID’а, то тогда, неоднократно переключая тип группы между security и distribution, у группы каждый раз бы создавался новый SID, что, как несложно убедиться, не происходит.

К чему бы я это? К тому, что в маркере доступа SID’ов distribution-групп обычно нет – Isass их туда не добавляет, читая флаг “не-security-enabled-группа” (который, в общем-то, и является основным отличием между distribution и security группами). А вот механизм вычисления перечня security principals, подпадающих под карающий меч AdminSDHolder – добавляет. Говоря проще, если учётная запись X входит в безобидную группу почтовой рассылки “Поздравления к 23 Февраля”, а эта группа входит, допустим, в Backup Operators (бред конечно с практической точки зрения, но вдруг), то все участники списка рассылки будут подпадать под механизм SDProp / AdminSDHolder. Он не различает security/distribution группы.

Обязательно учитывайте это при проектировании механизма защиты учётных записей.

Что такое orphaned AdminSDHolder objects

Когда при очередной “прокатке” домена данным механизмом он находит подпадающую под нужный критерий учётную запись или группу, он [механизм] ставит объекту атрибут **adminCount** в единицу. Что интересно – снимать назад не умеет. Т.е. у не-подпадающих security principal’ов нуль не пишет. Поэтому когда учётная запись, допустим, была участником Domain Admins, а после перестала, на ней сохраняется этот атрибут, и она начинает находиться в интересной ситуации – ACL у неё уже не перезаписывается AdminSDHolder’ом, но наследования нет.

Автоматического исправления этой ситуации нет, убирайте атрибут **adminCount** у экс-админских учётных записей вручную. Для исправления Microsoft предлагает скрипт, доступный [здесь](#).

Выводы

Данный механизм – штука весьма интересная. Надо, по крайней мере, знать как он работает и управляется, чтобы не удивляться самопроизвольному изменению ACL’ов у ряда учётных записей. Модифицировать время применения особо не нужно, КПД этого мероприятия сомнительно.

Удач!