

Обследование MS AD 2003 по горячим следам

Давно этими делами не занимаюсь, различными видами обследований и аудитов, и тут в родственной конторе произошло слияние трех небольших фирм, виной всему нестабильность экономики, в связи с этими событиями понадобилось провести обследование ИТ. В данной заметке речь пойдет только про AD.

Обычно структура документа по обследованию AD содержит следующее:

- Общее описание доменной структуры. Описывается:
 1. Назначение каждого домена.
 2. Схема каждого домена с отражением контроллеров домена по конкретным площадкам/офисам/ЦОДам.
 3. Сводные количественные данные по доменам. Для каждого домена указываются: Дата создания домена; Количество пользовательских ПК; Количество пользователей (Вход за последние 60 дней); Количество контроллеров домена; Общее количество серверов.
 4. Параметры доменов. Для каждого домена указываются: NetBIOS имя домена; Функциональный уровень леса; Функциональный уровень домена; Расположение FSMO ролей.
 5. Параметры контроллеров для каждого домена. Перечень контроллеров с указанием параметров: Тип (физический / виртуальный); IP-адрес; Операционная система; Сервер Глобального каталога.
- Описание доверительных отношений каждого домена. Для каждого домена указываются: Имя домена доверия; Направление доверия; Тип доверия; Дата создания.

- Описание структуры сайтов. Описывается:
 1. Описание сайтов леса. Для каждого сайта указывается: Наименование сайта; IP-сети входящими в сайт; Контроллеры домена сайта.
 2. Описание межсайтовых связей. Указывается: Наименование связи; Сайты; Интервал репликации; Стоимость связи.
- Статистика использования учетных записей. Описывается:
 1. Пользователи. Для каждого домена указываются: Общее кол-во пользователей; Enabled; Disabled; Locked; Password Not Required; Password Does Not Expire; Password Must Change.
 2. Компьютеры. Для каждого домена указываются: Общее кол-во компьютеров; Enabled; Disabled; Inactive; Windows workstations; Windows Servers; Non-Windows Device.
 3. Группы. Для каждого домена указываются: Общее кол-во групп; Built-in; Universal Security; Universal Distribution; Global Security; Global Distribution; Domain Local Security; Domain Local Distribution.
- Описание групповых политик. Детальное обследование за рамками обследования и проводится в рамках аудита GPO. В рамках обследования только статистика по GPO: общее кол-во GPO; перечень объектов GPO, которые не связаны ни с одним контейнером домена; перечень объектов GPO, которые связаны с контейнерами домена, но все связи отключены; перечень пустых объектов GPO, у которых параметры политики не заданы.
- Описание параметров безопасности. Описывается:
 1. Состав привилегированных групп безопасности. Для всех доменов приводится состав привилегированных групп безопасности: Administrators, Enterprise Admins, Domain Admins и Schema Admins.
 2. Политика паролей. Для каждого домена приводится политика паролей определённая в Default Domain Policy: Maximum password age; Minimum password age; Minimum password length; Enforce password history; Password must meet complexity requirements; Store passwords using reversible encryption.
 3. Политика блокировки учётной записи. Для каждого домена приводится политика блокировки учётных записей определённая в Default Domain Policy: Account lockout duration; Account threshold; Reset account lockout counter after.
 4. Описание настроек аудита. Для каждого домена приводятся настройки аудита определённые в Default Domain Policy: Audit account logon events; Audit account management; Audit directory service access; Audit logon events; Audit object access; Audit policy change; Audit privilege use; Audit process tracking; Audit system events.
- Резервное копирование Active Directory. Приводятся параметры Плана резервного копирования Active Directory. Для каждого домена приводится последняя дата резервного копирования одного из контроллеров соответствующего домена (поле службы каталога).

- Правила именования объектов AD. Приводятся действующие правила именования любых объектов ИТ инфраструктуры: учетные записи пользователей; учетные записи компьютеров пользователей; учетные записи серверов; группы (универсальные, глобальные, локальные); сервисные учетные записи; принтера; сайты AD; связи сайтов AD; объекты GPO; и другие.

В данной заметке просто зафиксирую несколько команд/операций, которые использовались при сборе данных Active Directory. Нюанс был в том, что было несколько лесов AD 2003, в которых не допускалось что-либо устанавливать на контроллеры домена, в частности AD Web Services для использования PowerShell, поэтому приходилось обходиться имеющимися утилитами и консолями.

При любом обследовании AD, большими помощниками будут:

Несколько дополнительных команд:

- 1) Получить дату последнего бэкапа каждой партиции AD:

```
repadmin /showbackup domain.ru > .\backup-domain.ru.txt
```

- 2) Получить данные по настроенным доверительным отношениям:

```
netdom query /d:domain.ru trust > .\trusts-nd-domain.ru.txt
```

```
nltest /server:domain.ru /domain_trusts > .\trusts-domain.ru.txt
```

- 3) Получить дату создания домена:

```
adfind.exe -h domain.ru -tdcgt -s Base -b dc=domain,dc=ru whenCreated > .\adcreate-domain.ru.txt
```

- 4) Получить общее кол-во объектов по заданному фильтру (Например, Общее кол-во пользователей; Enabled; Disabled; Locked; Password Not Required; Password Does Not Expire; Password Must Change):

```
adfind -h domain.ru -f "(sAMAccountType=805306368)" -c
```

LDAP запросы можно выполнить несколькими способами, я пользуюсь двумя:

- 1) Используя замечательную утилиту AdFind:

```
adfind -f "тело запроса"
```

- 2) Используя консоль управления AD Users And Computers:

1. В консоли Active Directory Users and Computers правой кнопкой мыши по Вашему домену (**DOMAIN.RU**)
2. В контекстном меню выбираем «Find»
3. В выпадающем списке «Find:» выбираем «Custom Search»

4. Переходим на закладку «Advanced» и пишем/копируем в поле «Enter LDAP query» нужный запрос.

Примеры нескольких LDAP запросов:

LDAP query search по ЮЗЕРАМ

Список всех пользователей:

`(sAMAccountType=805306368)`

Список всех Enabled пользователей:

`(&(sAMAccountType=805306368)(!useraccountcontrol:1.2.840.113556.1.4.803:=2))`

Список всех Disabled пользователей:

`(&(sAMAccountType=805306368)(useraccountcontrol:1.2.840.113556.1.4.803:=2))`

Список всех Locked пользователей:

`(&(sAMAccountType=805306368)
(lockoutTime:1.2.840.113556.1.4.804:=4294967295))`

Список всех пользователей с "Password Does Not Expire":

`(&(sAMAccountType=805306368)
(userAccountControl:1.2.840.113556.1.4.803:=65536))`

Список всех пользователей с "Password Must Change":

`(samAccountType=805306368)(pwdLastSet=0)
(!useraccountcontrol:1.2.840.113556.1.4.803:=2)`

Список всех пользователей с "Password Not Required":

`(samAccountType=805306368)(UserAccountControl:1.2.840.113556.1.4.803:=32)`

Список пользователей выполнявших логон за последние 60 дней:

`(&(sAMAccountType=805306368)(lastlogontimestamp>=1303860960000000000))`

Список пользователей выполнявших логон за последние 90 дней:

`(&(sAMAccountType=805306368)(lastlogontimestamp>=1303601760000000000))`

LDAP query search по ГРУППАМ

Список всех групп:

(objectCategory=group)

Список Built-in групп:

(groupType=-2147483643)

Список Universal Security групп:

(groupType=-2147483640)

Список Universal Distribution групп:

(groupType=8)

Список Global Security групп:

(groupType=-2147483646)

Список Global Distribution групп:

(groupType=2)

Список Domain Local Security групп:

(groupType=-2147483644)

Список Domain Local Distribution групп:

(groupType=4)

LDAP query search по КОМПАМ

Список всех компьютеров:

((&(objectCategory=computer))

Список всех Enabled компьютеров:

((&(objectCategory=computer)(!useraccountcontrol:1.2.840.113556.1.4.803:=2))

Список всех Disabled компьютеров:

((&(objectCategory=computer)(useraccountcontrol:1.2.840.113556.1.4.803:=2))

Список компьютеров неактивных (Inactive) > 180 days:

((&(objectCategory=computer)(pwdLastSet<=130281552000000000))

Список Windows Workstation Enabled:

((&(objectCategory=computer)(!useraccountcontrol:1.2.840.113556.1.4.803:=2)
(operatingSystem=*Windows*)(!operatingSystem=*Server*)))

Список Windows Workstation Disabled:

((&(objectCategory=computer)(useraccountcontrol:1.2.840.113556.1.4.803:=2)
(operatingSystem=*Windows*)(!operatingSystem=*Server*)))

Список Windows Server Enabled:

((&(objectCategory=computer)(!useraccountcontrol:1.2.840.113556.1.4.803:=2)
(operatingSystem=*Server*)))

Список Windows Server Disabled:

((&(objectCategory=computer)(useraccountcontrol:1.2.840.113556.1.4.803:=2)
(operatingSystem=*Server*)))

Список Не Windows компьютеров:

((&(objectCategory=computer)(!operatingSystem=*Windows*)))

Рубрики: Полезности ИТ, ИТ (All).