Active Directory: Использование LDAP-фильтров (ru-RU)

LDAP-фильтры используются для получения данных из Active Directory, например, в сценариях на PowerShell и VBScript. LDAP-фильтры используются в командах adfind и dsquery. Командлеты PowerShell Get-ADUser, Get-ADGroup, Get-ADComputer и Get-ADObject используют LDAP-фильтры, если указать параметр LDAPFilter

Table of Contents

Условия LDAP

Фильтр определяет необходимые условия для включения объекта в результат запроса. LDAP-фильтр может содержать одно или более условий. Результат условия - "Истина" или "Ложь". Общий вид фильтра

```
(<Атрибут AD><оператор сравнения><значение>)
```

<Атрибут AD> - LDAP-имя атрибута AD. Операторы сравнения

Оператор	Значение
=	Равенство
>=	Больше или равно
<=	Меньше или равно

Операторы "<" и ">" не поддерживаются. Также поддерживается оператор "~=" (приблизительное равенство), но в Active Directory он не находит своего применения. Элемент "<значение>" - значение атрибута AD. Значение не чувствительно к регистру и не должно быть заключено в кавычки. Символ шаблона "*" допустим всегда, кроме случаев. когда <Атрибут AD> - атрибут DN (уникальное имя), например distinguishedName, manager, directReports, member и memberOf. Если атрибут DN, то допустим только оператор равенства и необходимо указать полное уникальное имя значения (или "*" для объектов с любым значением атрибута). DN не нужно заключать в круглые скобки. Если атрибут принимает несколько значений, то условие выполняется при выполнении условия фильтра любым значением. Пример

```
(cn=Василий Пупкин)
```

Данный фильтр возвращает все объекты с CN (общее имя) равным строке "Василий Пупкин".
Условия фильтра могут быть объединены следующими операторами.

Орератор	Значение
&	И, все условия должны быть выполнены
|	ИЛИ, любое количество условий может быть соблюдено
!	НЕТ, условие не должно быть соблюдено

Пример. cn должно быть "Василий Пупкин" или givenName равно "Василий", sn равно "Пупкин":

(|(cn=Василий Пупкин)(&(givenName=Василий)(sn=Пупкин)))

Условия могут заключаться в скобки, но нужно их корректно закрывать.

Специальные символы

Спецификация LDAP-фильтра присваивает специальное значение следующим символам:

* ( ) \ NUL

Символ NUL это ASCII 00. В LDAP-фильтрах данные символы описываются как "\" с последующим шестнадцатеричным (Hex) представлением символа.

Character	Hex Representation
*	\2A
(	\28
)	\29
\	\5C
Nul	\0

Для поиска объектов с общим именем "Василий Вася*) Пупкин", LDAP-фильтр имеет вид:

(cn=Василий Вася\2A\29 Пупкин)

Закрытые круглые скобки не требуют использования кодов, например условие (cn=Василий(Вася)Пупкин) является корректным. Также не отображаемые или символы других алфавитов должны быть заменены кодами. Пример кодов и символов:

Символ	Шестнадцатеричное представление
á	\E1
é	\E9
í	\ED
ó	\F3
ú	\FA
ñ	\F1

Фильтрация по атрибутам objectCategory и objectClass

При фильтрации по атрибуту класса objectCategory, LDAP производит преобразование значения для более удобного составления фильтров. objectCategory - атрибут DN, например "cn=person,cn=Schema,cn=Configuration,dc=MyDomain,dc=com". Возможное условие фильтра

```
(objectCategory=cn=person,cn=Schema,cn=Configuration,dc=MyDomain,dc=com)
```

Active Directory позволяет использовать следующее короткое написание

(objectCategory=person)

Таблица комбинаций objectCategory и objectClass

objectCategory	**objectClass**	**Результат**
person	user	Пользователи
person		Пользователи и контакты
person	contact	Контакты
	user	Пользователи и компьютеры
computer		Компьютеры
user		Пользователи и контакты
	contact	Контакты
	computer	Компьютеры
	person	пользователи, компьютеры и контакты
contact		Пользователи и контакты
group		Группы
	group	Группы
person	organizationalPerson	Пользователи и контакты
	organizationalPerson	Пользователи, компьютеры и контакты
organizationalPerson		Пользователи и контакты

Нужно использовать фильтры, наиболее точно описывающие желаемый результат. Когда приходится выбирать между использованием objectCategory и objectClass, предпочтительно objectCategory, т.к. objectCategory принимает только одно значение и индексируется, а objectClass - много значений и не индексируется в Windows Server до 2008. Фильтрация с использованием objectCategory эффективнее аналогичной, но основанной на objectClass. Контроллеры домена на Windows Server 2008 индексируют objectClass. Этим можно воспользоваться, когда все контроллеры используют Windows Server 2008 или же при явном указании контроллера домена на Windows Server 2008 при запросе.

Примеры

Запрос	**LDAP-фильтр**
Все пользователи	(&(objectCategory=person)(objectClass=user))
Все пользователи (прим. 1)	(sAMAccountType=805306368)
Все компьютеры	(objectCategory=computer)
Все контакты	(objectClass=contact)
Все группы	(objectCategory=group)
Все организационные подразделения	(objectCategory=organizationalUnit)
Все контейнеры	(objectCategory=container)
Все встроенные контейнеры	(objectCategory=builtinDomain)
Все домены	(objectCategory=domain)
Компьютеры без описания	(&(objectCategory=computer)(!description=*))
Группы с описанием	(&(objectCategory=group)(description=*))
Пользователи с cn начитающимися на "Вас"	(&(objectCategory=person)(objectClass=user) (cn=Вас*))
Объекты с описанием "Отдел IT Ижевск\Казань" (прим. 2)	(description=Отдел IT Ижевск\5CКазань)
Группы с cn начинающимся на "Test" или "Admin"	(&(objectCategory=group(|(cn=Test*)(cn=Admin*)))
Все пользователи с заполненными именем и фамилией.	(&(objectCategory=person)(objectClass=user) (givenName=*)(sn=*))
Все пользователи с указанным e-mail	(&(objectCategory=person)(objectClass=user) (|(proxyAddresses=*:jsmith@company.com) (mail=jsmith@company.com)))
Объекты с общим именем "Василий * Пупкин" (прим. 3)	(cn=Василий \2A Пупкин)
Объекты с sAMAccountName, начинающимся на "x", "y", или "z"	(sAMAccountName>=x)
Объекты с sAMAccountName начинающимся с "a" или цифры или символа, кроме "$"	(&(sAMAccountName<=a)(!sAMAccountName=$*))
пользователи с установленным параметром "Срок действия пароля не ограничен" (прим. 4)	(&(objectCategory=person)(objectClass=user) (userAccountControl:1.2.840.113556.1.4.803:=65536))
Все отключенные пользователи (прим. 4)	(&(objectCategory=person)(objectClass=user) (userAccountControl:1.2.840.113556.1.4.803:=2))
Все включенные пользователи (прим. 4)	(&(objectCategory=person)(objectClass=user) (!userAccountControl:1.2.840.113556.1.4.803:=2))
Пользователи, не требующие паролей (прим. 4)	(&(objectCategory=person)(objectClass=user) (userAccountControl:1.2.840.113556.1.4.803:=32))
Пользователи с включенным параметром "Без	(&(objectCategory=person)(objectClass=user)

предварительной проверки подлинности Kerberos"	(userAccountControl:1.2.840.113556.1.4.803:=4194304))
Пользователи с неограниченным сроком действия учетной записи (прим. 5)	(&(objectCategory=person)(objectClass=user) (|(accountExpires=0) (accountExpires=9223372036854775807)))
Учетные записи, доверенные для делегирования	(userAccountControl:1.2.840.113556.1.4.803:=524288)
Чувствительные и недоверенные для делегирования учетные записи	(userAccountControl:1.2.840.113556.1.4.803:=1048574)
Все группы распространения (прим. 4, 15)	(&(objectCategory=group) (!groupType:1.2.840.113556.1.4.803:=2147483648))
Все группы безопасности (прим. 4)	(groupType:1.2.840.113556.1.4.803:=2147483648)
Все встроенные группы (прим. 4, 16)	(groupType:1.2.840.113556.1.4.803:=1)
Все глобальные группы (прим. 4)	(groupType:1.2.840.113556.1.4.803:=2)
Все локальные в домене группы (прим. 4)	(groupType:1.2.840.113556.1.4.803:=4)
Все универсальные группы (прим. 4)	(groupType:1.2.840.113556.1.4.803:=8)
Все глобальные группы безопасности (прим. 17)	(groupType=-2147483646)
Все универсальные группы безопасности (прим. 17)	(groupType=-2147483640)
Все локальные в домене группы безопасности (прим. 17)	(groupType=-2147483644)
Все глобальные группы распространения	(groupType=2)
Все объекты с имемем участника-службы	(servicePrincipalName=*)
Пользователи с параметром "Разрешить доступ" на вкладке "Входящие звонки" (прим. 6)	(&(objectCategory=person)(objectClass=user) (msNPAllowDialin=TRUE))
Группы, созданные после 1 марта 2011	(&(objectCategory=group) (whenCreated>=20110301000000.0Z))
Пользователи, обязанные изменить свой пароль при следующем входе в систему	(&(objectCategory=person)(objectClass=user) (pwdLastSet=0))
Пользователи, сменившие свои пароли после 15.04.2011 (прим. 7)	(&(objectCategory=person)(objectClass=user) (pwdLastSet>=129473172000000000))
Пользовали с "основной" группой, отличающейся от "Пользователи домена"	(&(objectCategory=person)(objectClass=user) (!primaryGroupID=513))
Компьютеры с "основной" группой "Контроллеры домена"	(&(objectCategory=computer)(primaryGroupID=515))
Объект с GUID "90395FB99AB51B4A9E9686C66CB18D99" (прим. 8)	(objectGUID=\90\39\5F\B9\9A\B5\1B\4A\9E\96 \86\C6\6C\B1\8D\99)
Объект с SID "S-1-5-21-73586283-152049171 -839522115-1111" (прим. 9)	(objectSID=S-1-5-21-73586283-152049171 -839522115-1111)
Объект с SID "010500000000000515 0000006BD662041316100943170A3257040000" (прим. 9)	(objectSID=\01\05\00\00\00\00\00\05\15 \00\00\00\6B\D6\62\04\13\16\10\09\43\17\0A\32 \57\04\00\00)
Компьютеры, не являющиеся контроллерами домена (прим. 4)	(&(objectCategory=computer) (!userAccountControl:1.2.840.113556.1.4.803:=8192))
Все контроллеры домена (прим. 4)	(&(objectCategory=computer) (userAccountControl:1.2.840.113556.1.4.803:=8192))
Все контроллеры домена (прим. 14)	(primaryGroupID=516)
Все компьютеры с Windows Server	(&(objectCategory=computer) (operatingSystem=*server*))
Все компьютеры с Windows Server, исключая контроллеры домена (прим. 4)	(&(objectCategory=computer) (operatingSystem=*server*) (!userAccountControl:1.2.840.113556.1.4.803:=8192))
Прямые члены группы	(memberOf=cn=Test,ou=East,dc=Domain,dc=com)
Пользователя - не прямые члены указанной группы	(&(objectCategory=person)(objectClass=user) (!memberOf=cn=Test,ou=East,dc=Domain,dc=com))
Группы с указанным прямым членом	(member=cn=Jim Smith,ou=West, dc=Domain,dc=com)
Все члены группы, включая вложенность групп (прим. 10)	(memberOf:1.2.840.113556.1.4.1941:= cn=Test,ou=East,dc=Domain,dc=com)
все группы, членом которых является указанный пользователь, учитывая вложенность групп (прим. 10)	(member:1.2.840.113556.1.4.1941:= cn=Jim Smith,ou=West,dc=Domain,dc=com)
Объекты с givenName "Василий*" и sn "Пупкин*", или cn "Василий Пупкин*" (прим. 11)	(anr=Василий Пупкин*)
Атрибуты контейнера "Schema", реплицируемые в глобальный каталог (прим. 6, 12)	(&(objectCategory=attributeSchema) (isMemberOfPartialAttributeSet=TRUE))
Атрибуты схемы, не реплицируемые на другие контроллеры домена (прим. 4, 12)	(&(objectCategory=attributeSchema) (systemFlags:1.2.840.113556.1.4.803:=1))
Все связи сайтов в контейнере configuration (Note 13)	(objectClass=siteLink)
Объекты nTDSDSA связаные с глобальными каталогами. Позволяет определить контроллеры домена с глобальным каталогом. (Note 4)	(&(objectCategory=nTDSDSA) (options:1.2.840.113556.1.4.803:=1))
Объект nTDSDSA связанный с ролью PDC-эмулятора. Позволяет определить контроллер домена с FSMO-ролью PDC-эмулятор (прим. 18).	(&(objectClass=domainDNS)(fSMORoleOwner=*))
Объект nTDSDSA связанный с ролью Владелец относительных идентификаторов. Позволяет определить контроллер домена с FSMO-ролью Владелец относительных идентификаторов (прим. 18).	(&(objectClass=rIDManager)(fSMORoleOwner=*))
Объект nTDSDSA связанный с ролью владелец инфраструктуры. Позволяет определить контроллер	(&(objectClass=infrastructureUpdate) (fSMORoleOwner=*))

домена с FSMO-ролью владелец инфраструктуры (прим. 18).	
Объект nTDSDSA связанный с ролью владелец доменных имен. Позволяет определить контроллер домена с FSMO-ролью владелец доменных имен(прим. 18).	(&(objectClass=crossRefContainer)(fSMORoleOwner=*))
Объект nTDSDSA связанный с ролью владелец схемы. Позволяет определить контроллер домена с FSMO-ролью владелец схемы (прим. 18).	(&(objectClass=dMD)(fSMORoleOwner=*))
Все серверы Exchange в контейнере Configuration (прим. 13)	(objectCategory=msExchExchangeServer)
Объекты, защищенные AdminSDHolder	(adminCount=1)
Все отношения доверия	(objectClass=trustedDomain)
Все объекты групповой политики	(objectCategory=groupPolicyContainer)
Все контроллеры домена, доступные только для чтения (прим. 4)	(userAccountControl:1.2.840.113556.1.4.803:=67

Примечания

1. Фильтр `(sAMAccountType=805306368)` более эффективен для объектов "пользователь"
2. Обратный слеш должен быть заменен на `\5C`
3. Астериск `"*"` должен быть заменена на `\2A`
4. Строка `1.2.840.113556.1.4.803` указывает `LDAP_MATCHING_RULE_BIT_AND`. Обозначает побитовое "И" атрибута флага, например userAccounControl, groupType или systemFlags и битовая маска (2, 32, 65536). Условие возвращает "Истину", когда побитовое "И" значения атрибута и битовой маски не равно нулю, что указывает на установку бита.
5. Атрибут accountExpires имеет тип Integer8, 64-битное значение, представляющее дату в UTC - количество интервалов в 100 наносекунд, начиная с 12:00 01.01.1601. Если срок действия учетной записи не ограничен, то атрибут accountExpires равен 0 или 2^63-1 (9,223,372,036,854,775,807 - наибольшее Interger64 число), оба значат "никогда".
6. При фильтрации атрибутов типа Boolean (булевые), например msNPAllowDialin или isMemberOfPartialAttributeSet, значения TRUE и FALSE должны быть введены в верхнем регистре.
7. Атрибут pwdLastSet имеет тип Integer8.
8. Байтовые массивы, например objectGUID, могут быть представлены как последовательность исключаемых шестнадцатеричных байтов. GUID `{b95f3990-b59a-4a1b-9e96-86c66cb18d99}` имеет hex-представление `90395fb99ab51b4a9e9686c66cb18d99`". Порядок первых восьми байтов изменен.
9. objectSID хранится как байтовый массив. Можно указывать как десятичный формат `S-1-5-21-73586283-152049171-839522115-1111` или шестнадцатеричное представление, где каждый байт исключен `\01\05\00\00\00\00\00\05\15\00\00\00\6B\D6\62\04\13\16\10\09\43\17\0A\32\57\04\00\00`", что позже можно использовать в VBScript.
10. Строка `1.2.840.113556.1.4.1941`указывает `LDAP_MATCHING_RULE_IN_CHAIN`. Применимо только к DN-атрибутам. Это расширенный оператор совпадения, проходящий по цепи наследования к корню до тех пор, пока не найдет совпадение. Выявляет вложенность групп. Доступен на контроллерах домена с Windows Server 2003 SP2 и более поздних версий.
11. Строка "anr" обозначает "неоднозначное разрешение имен" (Ambiguous Name Resolution). Подробнее здесь http://www.rlmueller.net/AmbiguousNameResolution.htm
12. Для запросов к атрибутам схемы нужно использовать поиск по контейнеру Schema, например `cn=Schema,cn=Configuration,dc=MyDomain,dc=com`.
13. Для запросов к атрибутам конфигурации нужно использовать поиск по контейнеру Configuration, например `cn=Configuration,dc=MyDomain,dc=com`.
14. Основной группой для контроллеров домена должна быть "Контроллеры домена" с известным RID, равным 516.
15. Многие LDAP-фильтры различных типов групп AD могут использовать атрибут groupType и опускать условие (objectCategory=group), т.к. только группы имеют атрибут groupType. Например, фильтр (groupType=2) вернет все глобальные группы распространения. При использовании оператора "НЕТ", например (!groupType:1.2.840.113556.1.4.803:=2147483648) для групп распространения (группы, не являющиеся группами безопасности) вернет все объекты без атрибута groupType. Таким образом, нужно использовать дополнительное условие (objectCategory=group).
16. Может показаться, что LDAP-фильтр для встроенных групп безопасности может быть (groupType=2147483649) или (groupType=-2147483643). т.к. побитовое "ИЛИ" между 2147483648 (маска групп безопасности) и 1 (маска встроенных групп) даст обозначенный результат. Однако результат фильтра будет пустым, т.к. встроенные группы являются локальными в домене.Нужно применить "ИЛИ" между полученными значениями и "4" (маска локальных в домене групп). Результат (2147483643 ИЛИ 1 ИЛИ 4) = 2147483653, после вычитания 2^32 станет -2147483643. Можно использовать как (groupType=2147483653), так и (groupType=-2147483643) для получения встроенных локальных в домене групп безопасности. Однако, проще использовать фильтр по условию (groupType:1.2.840.113556.1.4.803:=1).
17. Атрибуты userAccountControl и groupType принимают целочисленные 32-битные значения, т.е. от -2^31 до 2^31 - 1 или от -2147483648 до 2147483647. Значения, назначенные этим атрибутам будут результатом побитового "ИЛИ" указанной маски для каждого значения. Например, значение groupType для для универсальной группы безопасности определяется применением "ИЛИ" к маске универсальной группы 8 и и группы безопасности 2147483648. Результат (8 ИЛИ 2147483648) равен 2147483656. Данное значение превышает допустимое для целочисленного 32-битного значения, поэтому оно обращается в отцательно число. 2147483656 становится -2147483640. Правило сделующее - если целочисленное 32-битное поле превышает 2^31-1, то нужно вычесть из него 2^32 (4294967296). Таким образом groupType для универсальной грппы безопасности становится 2147967296 - 4294967296 = -2147483640. Это значение можно увидеть через "редактирование ADSI". Предпочтительно использование менно отрицательного значения, что является требованием для VBScript, т.к. его побитовые операторы могут обрабатывать только целочисленные 32-битные значения.
18. Существует 5 FSMO ролей. Для эмулятора PDC, владельца относительных эмуляторов и владельца инфраструктуры нужно опрашивать домен. Для владельца схемы нужно опрашивать контейнер schema, например cn=Schema,cn=Configuration,dc=MyDomain,dc=com. Для владельца доменных имен нужно опрашивать контейнер configuration, например cn=Configuration,dc=MyDomain,dc=com. В любом случае запрос вернет объекта типа nTDSDSA. Родитель данного объекта будет иметь относительное уникальное имя, указывающее на контроллер домена. Родительский объект имеет атрибут dnsHostName равный DNS-имени контроллера домена с требуемой FSMO-ролью.