LDAP-фильтры для поиска в Active Directory

windowsnotes.ru/activedirectory/ldap-filtry-dlya-poiska-obektov-v-active-directory-chast-1

31 декабря 2019 г.

Есть много способов найти что либо в Active Directory, но одним из самых эффективных является использование LDAP-фильтров. Они универсальны и их можно использовать как в командной строке, так и из графической оснастки.

Текстовая форма поисковых LDAP-фильтров определена в RFC 4515. Синтаксис LDAP-фильтра имеет вид:

<Фильтр>=(<Атрибут><оператор сравнения><значение>)

В фильтре могут использоваться следующие операторы сравнения.

Оператор	Значение
=	Равно
>=	Больше или равно
<=	Меньше или равно
~=	Приблизительно равно

Например, следующий фильтр возвращает все объекты, у которых значение атрибута **cn** (common name) равно **Vasya**:

(cn=Vasya)

Для проверки воспользуемся командлетом Get-ADObject с параметром LdapFilter:

```
Get-ADObject -LdapFilter "(cn=Vasya)"
```

```
PS C:\> Get-ADObject -LDAPFilter "(cn=Vasya)"

DistinguishedName                       Name  ObjectClass ObjectGUID
-----------------                       ----  ----------- ----------
CN=Vasya,CN=Computers,DC=test,DC=local Vasya computer    34cb3515-83ad-40a3-8b6b-cb2262234774
CN=Vasya,CN=Users,DC=test,DC=local     Vasya user        c3f5f243-7d80-469e-9158-7174ea8324ea
```

Кстати, вместо имени атрибута можно использовать его идентификатор (Attribute-Id). Например атрибут **cn** имеет Id **2.5.4.3**, соответственно предыдущий фильтр можно изменить следующим образом:

(2.5.4.3=Vasya)

```
PS C:\> Get-ADObject -LDAPFilter "(2.5.4.3=Vasya)"

DistinguishedName                       Name  ObjectClass ObjectGUID
-----------------                       ----  ----------- ----------
CN=Vasya,CN=Computers,DC=test,DC=local Vasya computer    34cb3515-83ad-40a3-8b6b-cb2262234774
CN=Vasya,CN=Users,DC=test,DC=local     Vasya user        c3f5f243-7d80-469e-9158-7174ea8324ea
```

Примечание. Список атрибутов AD с описанием можно найти здесь https://docs.microsoft.com/en-us/windows/win32/adschema/attributes-all.

При наличии нескольких условий поиска фильтры можно комбинировать с помощью логических операторов.

Оператор	Значение
& (И)	Все условия должны быть выполнены
| (ИЛИ)	Любое количество условий может быть соблюдено
! (НЕ)	Условие не должно быть выполнено

В этом случае синтаксис фильтра будет таким:

(<Оператор><Фильтр1><Фильтр2>)

Для примера отберем объекты с **cn** равным **Vasya** и **sn** (surname) равным **Pupkin:**

(&(cn=Vasya)(sn=Pupkin))

```
PS C:\> Get-ADObject -LDAPFilter "(&(cn=Vasya)(sn=Pupkin))"

DistinguishedName                 Name  ObjectClass ObjectGUID
-----------------                 ----  ----------- ----------
CN=Vasya,CN=Users,DC=test,DC=local Vasya user        c3f5f243-7d80-469e-9158-7174ea8324ea
```

Немного изменим задачу и отберем все объекты, у которых или **cn** равно **Vasya** или **sn** равно **Pupkin:**

(|(cn=Vasya)(sn=Pupkin))

```
PS C:\> Get-ADObject -LDAPFilter "(|(cn=Vasya)(sn=Pupkin))"

DistinguishedName                     Name  ObjectClass ObjectGUID
-----------------                     ----  ----------- ----------
CN=Vasya,CN=Computers,DC=test,DC=local Vasya computer    34cb3515-83ad-40a3-8b6b-cb2262234774
CN=Vasya,CN=Users,DC=test,DC=local     Vasya user        c3f5f243-7d80-469e-9158-7174ea8324ea
CN=Fedor,CN=Users,DC=test,DC=local     Fedor user        62f5f17b-b0a8-4245-95fd-4444ad213b31
```

Можно использовать сразу несколько логических операторов в одном фильтре, главное не запутаться в скобках. Составим фильтр, который выдаст объекты с **cn** равно **Vasya** или **sn** равно **Pupkin,** у которых **cn** не равен **Fedor**:

(&(|(cn=Vasya)(sn=Pupkin)(!(cn=Fedor)))

```
PS C:\> Get-ADObject -LDAPFilter "(&(|(cn=Vasya)(sn=Pupkin))(!(cn=Fedor)))"

DistinguishedName                     Name  ObjectClass ObjectGUID
-----------------                     ----  ----------- ----------
CN=Vasya,CN=Computers,DC=test,DC=local Vasya computer    34cb3515-83ad-40a3-8b6b-cb2262234774
CN=Vasya,CN=Users,DC=test,DC=local     Vasya user        c3f5f243-7d80-469e-9158-7174ea8324ea
```

Фильтр по атрибутам objectClass и objectCategory

Как видно из примера, фильтр возвращает нам как объекты пользователей, так и компьютеров. Уточнить параметры поиска можно с помощью атрибутов **objectCategory** и **objectClass**. Оба этих атрибута позволяют задать тип (класс) искомого объекта, однако между ними есть существенное отличие. Атрибут **objectClass** может принимать несколько значений, тогда как **objectCategory** имеет только одно значение, поэтому фильтры с использованием **objectCategory** точнее. Для большей эффективности поиска можно использовать оба этих атрибута. Возможны следующие комбинации.

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

С помощью следующего фильтра отберем всех пользователей с именем Vasya:

(&(objectClass=user)(objectCategory=person)(cn=Vasya))

```
PS C:\> Get-ADObject -LDAPFilter "(&(objectClass=user)(objectCategory=person)(cn=Vasya))"

DistinguishedName                Name  ObjectClass ObjectGUID
-----------------                ----  ----------- ----------
CN=Vasya,CN=Users,DC=test,DC=local Vasya user        c3f5f243-7d80-469e-9158-7174ea8324ea
```

Символы подстановки

При составлении LDAP-фильтра можно пользоваться знаками подстановки (wildcards). Если точнее, то поддерживается всего один подстановочный символ * (звездочка), который может заменять любое количество символов. Так следующий фильтр найдет всех пользователей, у которых имя начинается с буквы V:

(&(objectClass=user)(objectCategory=person)(cn=V*))

```
PS C:\> Get-ADObject -LDAPFilter "(&(objectClass=user)(objectCategory=person)(cn=V*))"

DistinguishedName                  Name   ObjectClass ObjectGUID
-----------------                  ----   ----------- ----------
CN=Vasya,CN=Users,DC=test,DC=local  Vasya  user        c3f5f243-7d80-469e-9158-7174ea8324ea
CN=Victor,CN=Users,DC=test,DC=local Victor user        a2829e7e-7ec7-451e-a945-bf70218a76ea
```

Подстановочные символы очень удобно использовать для проверки наличия значения заданного атрибута. Для примера найдем всех пользователей, у которых заполнен атрибут **mail**:

(&(objectClass=user)(objectCategory=person)(mail=*))

```
PS C:\> Get-ADObject -LDAPFilter "(&(objectClass=user)(objectCategory=person)(mail=*))"

DistinguishedName                 Name  ObjectClass ObjectGUID
-----------------                 ----  ----------- ----------
CN=Fedor,CN=Users,DC=test,DC=local Fedor user        62f5f17b-b0a8-4245-95fd-4444ad213b31
```

В некоторых случаях вместо подстановочных символов можно использовать операторы сравнения **>=** и **<=**. Например с помощью такого фильтра выведем тех пользователей, у которых имя начинается с буквы V и далее по алфавиту (т.е. V,W,X,Y,Z):

(&(objectClass=user)(objectCategory=person)(cn>=V))

```
PS C:\> Get-ADObject -LDAPFilter "(&(objectClass=user)(objectCategory=person)(cn>=V))"

DistinguishedName                  Name   ObjectClass ObjectGUID
-----------------                  ----   ----------- ----------
CN=Vasya,CN=Users,DC=test,DC=local  Vasya  user        c3f5f243-7d80-469e-9158-7174ea8324ea
CN=Victor,CN=Users,DC=test,DC=local Victor user        a2829e7e-7ec7-451e-a945-bf70218a76ea
CN=yulia,CN=Users,DC=test,DC=local  yulia  user        1ff4797b-ab60-4a4a-9d63-8f789651d88d
```

Спец символы

При использовании в LDAP-фильтрах следующих спец. символов они описываются в шестнадцатеричном представлении.

Символ	Представление
*	\2A
&	\26
(	\28
)	\29

<	\3C
>	\3e
=	\3d
~	\7e
\	\5c
/	\2f
|	\7c
Nul	\00

Другими словами, если вы хотите использовать эти символы как обычные текст, то их необходимо заменить на соответствующие коды. Например, ищем группу с экзотическим именем **Users*)**:

(&(objectCategory=group)(cn=Users\2A\29))

Примечание. Закрытые круглые скобки в значении атрибута не требуют использования hex-кодов. К примеру фильтр (cn=Us(e)rs)) является вполне корректным.

```
PS C:\> Get-ADObject -LDAPFilter "(&(objectCategory=group)(cn=Users\2A\29))"

DistinguishedName                   Name    ObjectClass ObjectGUID
-----------------                   ----    ----------- ----------
CN=Users*),CN=Users,DC=test,DC=local Users*) group       e3fa4956-cc94-4620-beae-ffe09f01c783
```

Для начала хватит. А в следующей статье мы копнем поглубже и рассмотрим расширенные фильтры поиска.