Active Directory: DSQUERY Commands

DSQUERY Commands to query AD objects:-

1. How to find all members for a particular group.

```
dsget group "<DN of the group>" -members
```

a. How to find all groups for a particular member (including nested groups)

```
dsget user "<DN of the user>" -memberof -expand
dsquery user -samid "username" | dsget user -memberof -expand
```

b. Get the Groups name form Users container

```
dsquery group -o rdn cn=users,dc=contoso,dc=com
```

C. Get the members from a Group

```
dsquery group -samid "CS_CLUB_ACCOUNTS" | dsget group -members -expand  | dsget user -samid
```

2. How to find memberof , lastlogontimestamp , homemta(Mail server) , Samaccountname & so on(Repadmin /sho

```
dsquery * "<DN>" -scope base -attr lastlogontimestamp memberoff
```

```
repadmin /showattr <DCNAME> <"DN"> /attrs:lastlogon,homemta,whencreated,lastlogontimestamp,samaccountname
```

3. How to modify user last name.

```
dsmod user <dn> -ln "<last name>"
```

4. How to find memberof , lastlogontimestamp , homemta(Mail server) , Samaccountname & so on for "n" number

Create a batch file(for /f "eol= tokens=* delims= usebackq" %%x in (%1) do dsquery * %%x -scope base -attr sAMAccount lastlogontimestamp mail homeMTA memberof) e.g ds.bat

Create a text file (All users DN e.g:dn.txt)

Open cmd & run ds.bat dn.txt >> c:\attr.txt

5. How to find DN for n number of computers

```
for /f %%x in (%1) do dsquery computer -name %%x
```

(Create a batch file with line & create a txt file computer.txt

open cmd >>>>>>batchfile computer.txt >> c:\dn.txt

6. Find Subnet with associated site.

```
dsquery subnet -name <CIDR> | dsget subnet
```

8.How to find disabled users

```
dsquery user "dc=ssig,dc=com" -disabled
```

```
dsquery * -filter "(&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2))"
```

9. How to find OS?

```
dsquery * <"DN"> -scope base -attr operatingSystem
```

10. How to find site ?

```
dsquery site -name * -limit 0
```

```
dsquery server -s <server> | dsget server -site
```

11. How to get tombstonelifetime ?

```
dsquery * "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=yourdomain,DC=com" -scope base
```

13. How to find mail box?

```
dsquery * -filter "samaccountname=biswajit" -attr homemdb
```

14. How to find the GCs?

```
DsQuery Server -domain contoso.com -isgc
```

15.How to find all the active users?

```
dsquery * -filter "(&(objectCategory=person)(objectClass=user)(!userAccountControl:1.2.840.113556.1.4.803:=2))"
```

16.How to find users logon name by their mail address for bulk users?

For Single user

```
dsquery * domainroot -filter "(&(objectCategory=Person)(objectClass=User)(mail=e-mailaddress))" -attr name
```

For bulk users

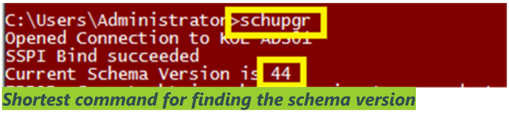
```
for /f %%x in (%1) do dsquery * domainroot -filter "(&(objectcategory=person)(objectclass=user)(mail=%%x))" -attr name
```

17. How to find Schema version?

```
dsquery * cn=schema,cn=configuration,dc=domainname,dc=local -scope base -attr objectVersion
```

or

schupgr



```
C:\Users\Administrator>schupgr
Opened Connection to KOL AD301
SSPI Bind succeeded
Current Schema Version is 44
```

Shortest command for finding the schema version

18. How to find Site name by server name ?

```
dsquery server -name test1 | dsget server -site
```

```
dsquery server -name (provide the server name for DN) | dsget server -site
```

19. How to find all groups of a user is memberof without the DN's?

```
dsquery user -samid anthony | dsget user -memberof | dsget group -samid
```

```
dsquery user -samid (provide the samaccount name of the user) | dsget user -memberof | dsget group -samid
```

20. How to find all groups if a computer account without giving the DN's ?

```
dsquery computer -name test1 | dsget computer -memberof | dsget group -samid
```

21. How to find PDC role holder for the existing domain ?

```
dsquery server -hasfsmo PDC
```

22. How to find Infrastructure Master role holder existing domain ?

```
dsquery server -hasfsmo INFR
```

23. How to find RID master role holder for existing domain ?

```
dsquery server -hasfsmo RID
```

24. How to find Schema master role holder in a Forest ?

```
dsquery server -forest -hasfsmo Schema
```

25. How to find Domain Naming Master in a Forest ?

```
dsquery server -forest -hasfsmo Name
```

26. How to find if the Domain Controller is a Global Catalog (GC) or not ?

```
dsquery server -name test1 | dsget server -isgc
```

27. How to find subnet with associated site.

```
dsquery subnet -name 10.222.88.0/25 | dsget subnet
```

28. How to find SID of a user?

```
dsquery user -samid <bbiswas> | dsget user -sid
dsquery * -filter (samaccountname=santhosh) – attr sid
```

29. How to find sIDHisotry of a user?

```
Dsquery * -filter (samaccoutname=santhosh) – attr siDhistory
```

30. How to find enabled computer accounts in an OU?

```
dsquery computer OU=Test,DC=sivarajan,DC=com -limit 5000 | dsget computer -dn -disabled | find /i " no"
```

31. How to count enabled computer accounts in an OU?

```
dsquery computer OU=Test,DC=sivarajan,DC=com -limit 5000 | dsget computer -dn -disabled | find /c /i " no"
```

32. How to find all members for a OU.

```
dsquery user ou=targetOU,dc=domain,dc=com
```

33. How to find all groups for a OU.

```
dsquery group ou=targetOU,dc=domain,dc=com
```

34. To get the members status from the active directory group

```
dsquery group -samid “Group Pre-Win2k Name” | dsget group -members | dsget user -disabled -display
```

35.Command to find all the subnets for the given site

```
dsquery subnet -o rdn -site <site name>
```

36. Command to find all DCs in the given site

```
>>dsquery server -o rdn -site <site name>
```

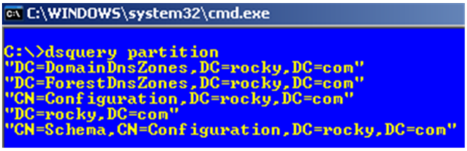
37. Command to find all DCs in the Forest

```
>>dsquery server -o rdn -forest
```

38. To list the distinguished names of all directory partitions in the current forest

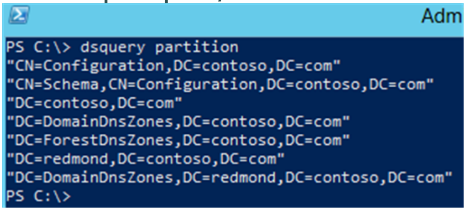
```
>>dsquery partition
```

Below example for single domain



```
C:\>dsquery partition
"DC=DomainDnsZones,DC=rocky,DC=com"
"DC=ForestDnsZones,DC=rocky,DC=com"
"CN=Configuration,DC=rocky,DC=com"
"DC=rocky,DC=com"
"CN=Schema,CN=Configuration,DC=rocky,DC=com"
```

Below example for parent/child domain



```
PS C:\> dsquery partition
"CN=Configuration,DC=contoso,DC=com"
"CN=Schema,CN=Configuration,DC=contoso,DC=com"
"DC=contoso,DC=com"
"DC=DomainDnsZones,DC=contoso,DC=com"
"DC=ForestDnsZones,DC=contoso,DC=com"
"DC=redmond,DC=contoso,DC=com"
"DC=DomainDnsZones,DC=redmond,DC=contoso,DC=com"
PS C:\>
```

39. To find all contacts in the organizational unit (OU)

dsquery contact OU=Sales,DC=Contoso,DC=Com

40. To list the relative distinguished names of all sites that are defined in the directory

dsquery site -limit 0

41. List of all users with primary group "Domain Users"

dsquery * -filter "(primaryGroupID=513)" -limit 0

(**You can change the "primaryGroupID" as per your requirement**)

513:Domain Users
514:Domain Guests
515:Domain Computers
516:Domain Controllers

42. How to find all attributes for all users?

Dsquery * -limit 0 -filter "&(objectClass=User)(objectCategory=Person)" -attr * >>output123.txt

43. Show How Many Times wrong Password has been entered on a specified domain controller.

dsquery * -filter "(sAMAccountName=jsmith)" -s MyServer -attr givenName sn badPwdCount

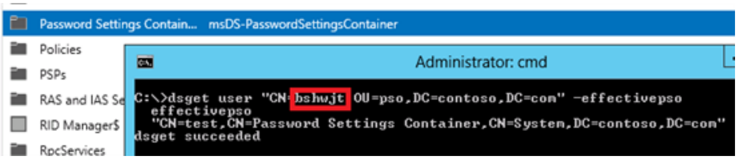
The badPwdCount attribute is not replicated, so a different value is saved for each user on each domain controller.

44.Expire use account.
dsquery * "dc=contoso,dc=com" -filter "(&(objectCategory=Person)(objectClass=User)(!accountExpires=0)(!accountExpires=
sAMAccountname displayName

Fine Granted Password Policy
45. **How to find the 'PSO Applies to'**
i)dsget user <user DN> -effectivepso

Example:

C:\>**dsget user "CN=bshwjt,OU=pso,DC=contoso,DC=com" -effectivepso**
effectivepso
"CN=test,CN=Password Settings Container,CN=System,DC=contoso,DC=com"
dsget succeeded
("bshwjt" is the user and test is the "PSO" also see the below snap)



```
C:\>dsget user "CN=bshwjt OU=pso,DC=contoso,DC=com" -effectivepso
  effectivepso
  "CN=test,CN=Password Settings Container,CN=System,DC=contoso,DC=com"
dsget succeeded
```

ii) **How to find the PSO settings**

C:\>dsquery * "<CN=your pso name>,CN=Password Settings Container,CN=System,DC=contoso,DC=com" -scope base -attr *

46. Find out Account Expiry date

dsquery user -name * -limit 0 | dsget user -samid -acctexpires

47.This example displays all attributes of the contoso.com domain object
dsquery * -filter (dc=contoso) -attr *

48.*This complex example displays the names of all attributes (150) that Windows Server 2003 replicates to Global Catalog serv*
ensure that you typed TRUE in capital letters
>**dsquery * cn=Schema,cn=Configuration,dc=contoso,dc=com -filter "(&(objectCategory=attributeSchema)(isMem**
0 -attr name

49. How to get all samaacount name ?
dsquery user -o rdn -limit 0

50.The command displays the DNS host name, the site name, and whether the server is Global Catalog (GC) server for each
dsquery server | dsget server -dnsname -site -isgc

Get all the servers in the forest

dsquery server -forest -limit 0 | dsget server -dnsname -site -isgc

51.The dsget command displays properties of users or other objects. In this example, it displays the 6 groups that explicitly

Note: The -memberof -expand combination recursively expands the list of groups of which the user is a member. In this exa
because Domain Users is a member of the Users group.
dsget user cn=Administrator,cn=Users,dc=contoso,dc=com -memberof

52.The output of the dsquery command can be used as input for the dsget command by using a pipe (|). In this example, t
(SID) of each user is displayed.
dsquery user | dsget user -samid -sid -limit 0 >> c:\Allusers-samid-sid.txt

53. How to find ***RODC ?***

```
dsquery server -isreadonly
```

Dsqury for exchange server

54. How to find the Schema Version for Exchange Servers.

dsquery * CN=ms-Exch-Schema-Version-Pt,cn=schema,cn=configuration,dc=domain,dc=local -scope base -attr ran

55.How to find lastLogonTimestamp for all users for a domain

dsquery * -filter "&(objectClass=person)(objectCategory=user)" -attr cn lastLogonTimestamp -limit 0

56. Inactive users are go to disable state

dsquery * <ou> -filter "(&(objectCategory=Person)(objectClass=User)(!accountExpires=0)(!accountExpires=9223372036854

57.ADDS existing connection point objects

dsquery * forestroot -filter (objectclass=serviceconnectionpoint)

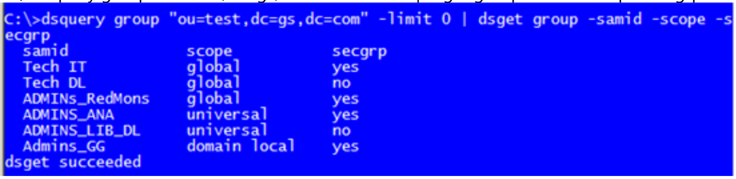
58. Find all Hyper-V hosts in your forest

```
C:\>dsquery * forestroot -filter "&(cn=Microsoft Hyper-V)(objectCategory=serviceconnectionpoint)" 
```

```
59. Find all windows virtual machine in your forest
```

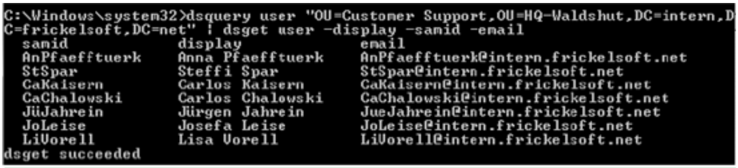
```
C:\>dsquery * forestroot -filter "&(cn=windows virtual machine)(objectCategory=serviceconnectionpo
```

60.Extract the all groups from an OU with Group Scope & Group Type. Find the below snap for your reference.
C:\>dsquery group "ou=test,dc=gs,dc=com" -limit 0 | dsget group -samid -scope -secgrp

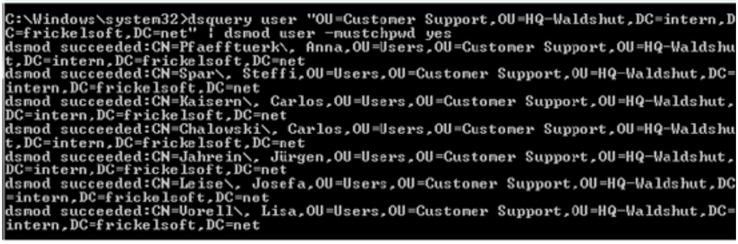


```
C:\>dsquery group "ou=test,dc=gs,dc=com" -limit 0 | dsget group -samid -scope -s
ecgrp
  samid               scope             secgrp
  Tech IT             global            yes
  Tech DL             global            no
  ADMINS_RedMons      global            yes
  ADMINS_ANA          universal         yes
  ADMINS_LIB_DL       universal         no
  Admins_GG           domain local      yes
dsget succeeded
```

61.The below example displays a list of users from the OU "Customer Support",
can then be forwarded to dsget that can provide detailed information about objects.
In the example, the requested user list is headed by the pipe symbol after dsget that
-outputs then the sAMAccountName for all users and email address.
If we wanted to carry out modifications to the information returned by DSQuery user list,
we could send the result to dsmod, which for us is making changes to all users.
In below snap shows the change in the command ensures that all users of DSQuery
-user list must change their passwords at next logon.



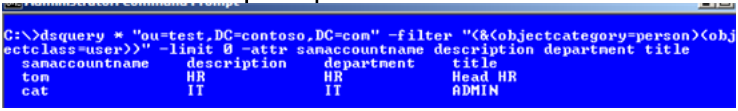
```
C:\Windows\system32>dsquery user "OU=Customer Support,OU=HQ-Waldshut,DC=intern,D
C=frickelsoft,DC=net" | dsget user -display -samid -email
  samid            display            email
  AnPfaefftuerk    Anna Pfaefftuerk   AnPfaefftuerk@intern.frickelsoft.net
  StSpar           Steffi Spar        StSpar@intern.frickelsoft.net
  CaKaisern        Carlos Kaisern     CaKaisern@intern.frickelsoft.net
  CaChalowski      Carlos Chalowski   CaChalowski@intern.frickelsoft.net
  JüJahrein        Jürgen Jahrein     JueJahrein@intern.frickelsoft.net
  JoLeise          Josefa Leise       JoLeise@intern.frickelsoft.net
  LiVorell         Lisa Vorell        LiVorell@intern.frickelsoft.net
dsget succeeded
```



```
C:\Windows\system32>dsquery user "OU=Customer Support,OU=HQ-Waldshut,DC=intern,D
C=frickelsoft,DC=net" | dsmod user -mustchpwd yes
dsmod succeeded:CN=Pfaefftuerk\, Anna,OU=Users,OU=Customer Support,OU=HQ-Waldshu
t,DC=intern,DC=frickelsoft,DC=net
dsmod succeeded:CN=Spar\, Steffi,OU=Users,OU=Customer Support,OU=HQ-Waldshut,DC=
intern,DC=frickelsoft,DC=net
dsmod succeeded:CN=Kaisern\, Carlos,OU=Users,OU=Customer Support,OU=HQ-Waldshut,
DC=intern,DC=frickelsoft,DC=net
dsmod succeeded:CN=Chalowski\, Carlos,OU=Users,OU=Customer Support,OU=HQ-Waldshu
t,DC=intern,DC=frickelsoft,DC=net
dsmod succeeded:CN=Jahrein\, Jürgen,OU=Users,OU=Customer Support,OU=HQ-Waldshut,
DC=intern,DC=frickelsoft,DC=net
dsmod succeeded:CN=Leise\, Josefa,OU=Users,OU=Customer Support,OU=HQ-Waldshut,DC
=intern,DC=frickelsoft,DC=net
dsmod succeeded:CN=Vorell\, Lisa,OU=Users,OU=Customer Support,OU=HQ-Waldshut,DC=
intern,DC=frickelsoft,DC=net
```

Another way to get the user attributes from an OU. Find the below snap & dsquery for that.
C:\>dsquery * "ou=test,DC=contoso,DC=com" -filter "(&(objectcategory=person)(objectclass=user))" -limit 0

-attr samaccountname description department title



```
C:\>dsquery * "ou=test,DC=contoso,DC=com" -filter "(&(objectcategory=person)(obj
ectclass=user))" -limit 0 -attr samaccountname description department title
  samaccountname     description     department     title
  tom                HR              HR             Head HR
  cat                IT              IT             ADMIN
```

62.retrieve the DN of all users in the domain that are not direct members of a specified group
>>dsquery * -filter "(&(objectCategory=person)(objectClass=user)(!(memberOf=Groupname,ou=West, dc=Contoso,dc=com))) -limit 0 > NotInGroup.txt

63. How to open DSQUERY GUI Window
rundll32 dsquery,OpenQueryWindow

DNS application partition

64. How to find the DNS servers from DomainDNSZones & ForestDNSzones

```
C:\>dsquery * DC=DomainDnsZones,DC=contoso,DC=com -scope base -attr msDs-masteredBy
C:\>dsquery * DC=forestDnsZones,DC=contoso,DC=com -scope base -attr msDs-masteredBy
```

65.Finding the Functional Levels of Active Directory

```
dsquery * "DC=contoso,DC=com" -scope base -attr msDS-Behavior-Version ntMixedDomain
```

```
0, 0         Windows 2000 Native domain Level
0, 1         Windows 2000 Mixed domain Level
2, 0         Windows 2003 Domain Level
3, 0         Windows 2008 Domain Level
4, 0         Windows 2008 R2 Domain Level
```

66. Find the object for DES-Only-Encryption

```
dsquery * -filter "(UserAccountControl:1.2.840.113556.1.4.803:=2097152)"
```

67. Find the DNS servers from all the DNS partitions.

```
dsquery * "CN=Configuration,DC=contoso,DC=com" -filter "(&(objectClass=crossRef)(objectCategory=crossRef)(syst
```

Using LDAP Filter.

68. How to find particular user attribute using LDAP Filter?

```
C:\>dsquery * -filter (samaccountname=biz) -attr name whenchanged

  name    whenchanged

  biz     01/03/2014 07:02:14
```

69. How to find all disabled users.

```
PS C:\> dsquery * -filter ("&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.8

"CN=Guest,CN=Users,DC=Rocky,DC=com"

"CN=krbtgt,CN=Users,DC=Rocky,DC=com"
```

70. How to find Forestprep , domainprep & RodcPrep is done or not?

```
    C:\>dsquery * CN=ActiveDirectoryUpdate,CN=ForestUpdates,cn=configuration,dc=msft
,dc=net -scope base -attr revision
 revision
 5


C:\>dsquery * CN=ActiveDirectoryRodcUpdate,CN=ForestUpdates,cn=configuration,dc=
msft,dc=net -scope base -attr revision
 revision
 2
```

More on Active Directory: LDAP Syntax Filters

http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx

---

For more switch see the below link.

http://technet.microsoft.com/en-us/library/cc732535.aspx

::::::::::See the below link for custom filters::::::::

http://www.rlmueller.net/ADOSearchTips.htm

Find the Blogs for more DSQUERY, those are very helpful and effective.

http://social.technet.microsoft.com/wiki/contents/articles/3537.aspx
http://social.technet.microsoft.com/Forums/en-AU/winserverDS/thread/bf5bce23-c1d5-43ac-a47f-8a0585792903

Technet Link
http://technet.microsoft.com/en-us/library/cc754232%28WS.10%29.aspx#BKMK_examplesDSQuery

DSQuery, And Then Some
http://mcpmag.com/articles/2007/08/01/dsquery-and-then-some.aspx

---

Regards
Biswajit Biswas
My Blogs | TechnetWiki Ninja