Configure Active Directory Snapshots

Create a snapshot of AD DS in Windows Server 2012 R2 by using NTDSUTIL.

NTDSUtil in Windows Server 2012 can create and mount snapshots of AD DS.

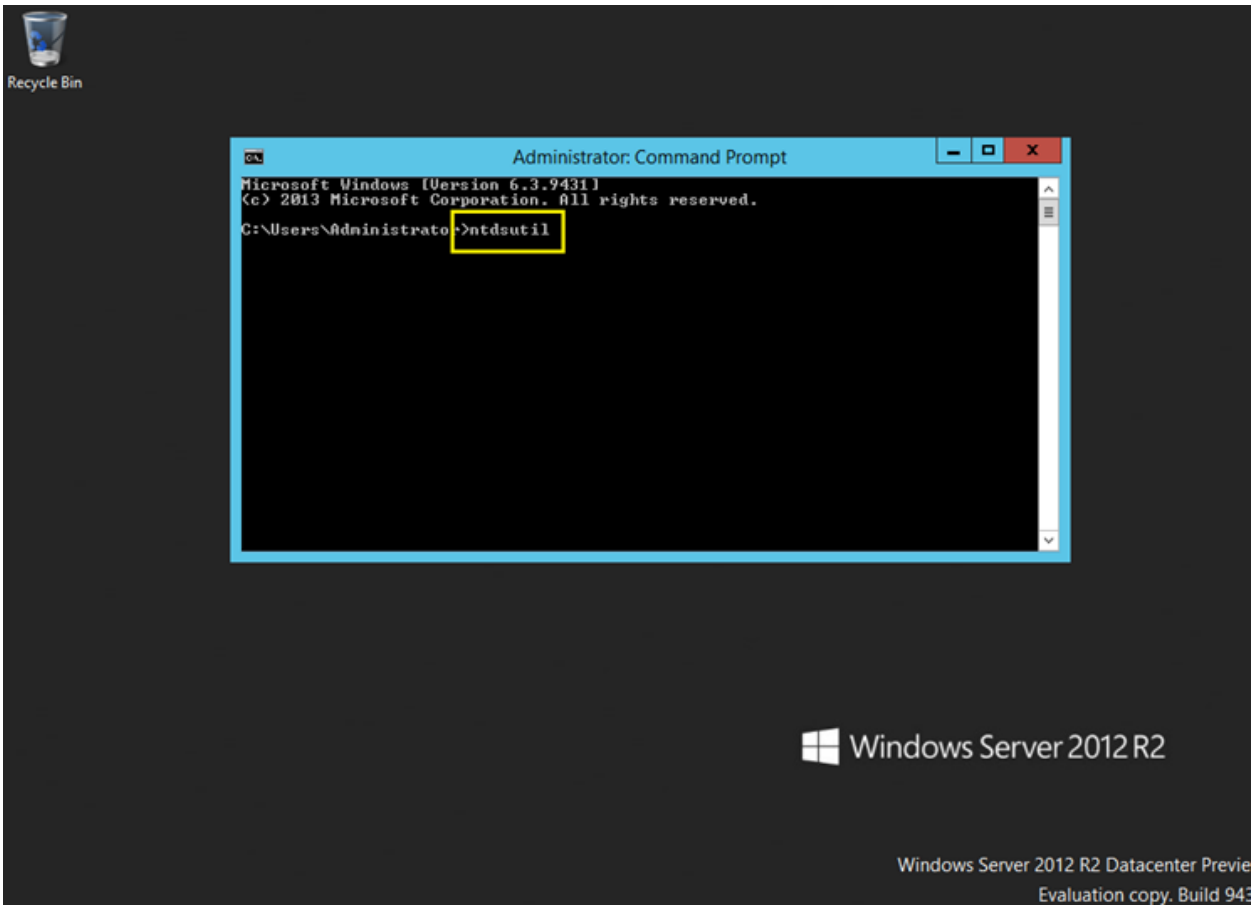
A snapshot is a form of historical backup that captures the exact state of the directory service at the time of the snapshot.

You can use tools to explore the contents of a snapshot to examine the state of the directory service at the time the snapshot was made, or connect to a mounted snapshot with LDIFDE and export a reimport objects into AD DS.

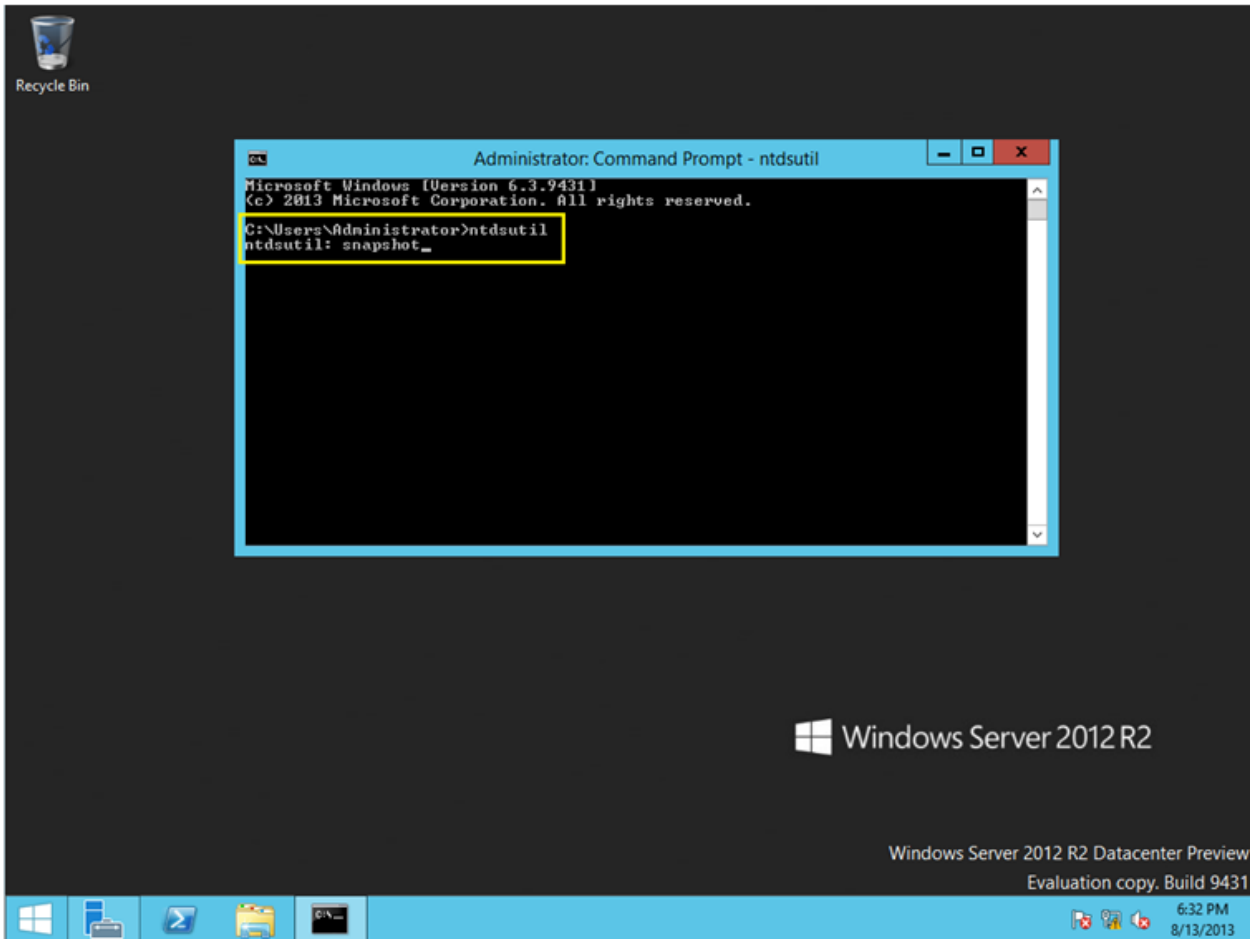
For this short demo, I use my DC01.comsys.local server.

Lets get started…

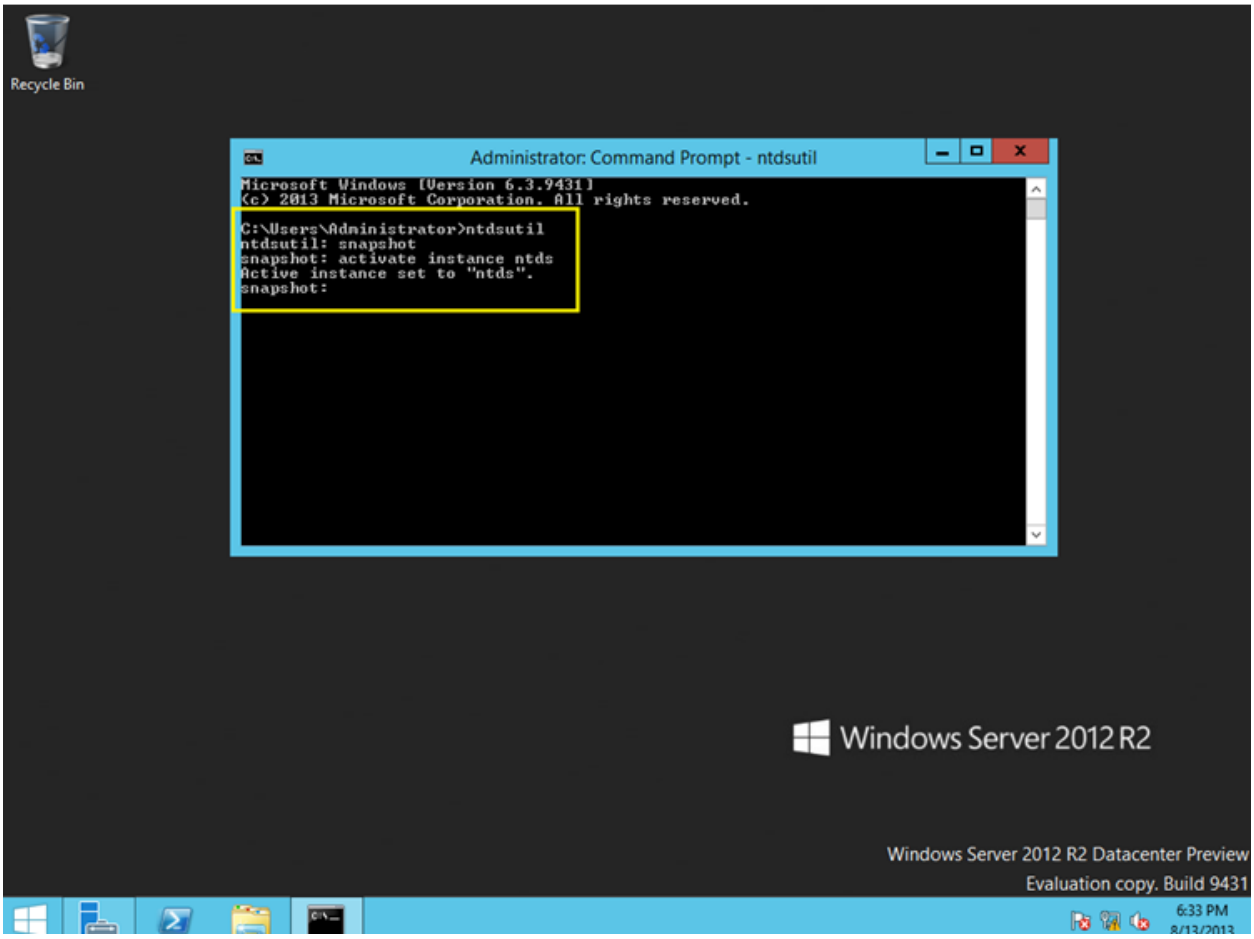
1 – On the domain server, which is my DC01.comsys.local, open command prompt and type **ntdsutil** and press enter…



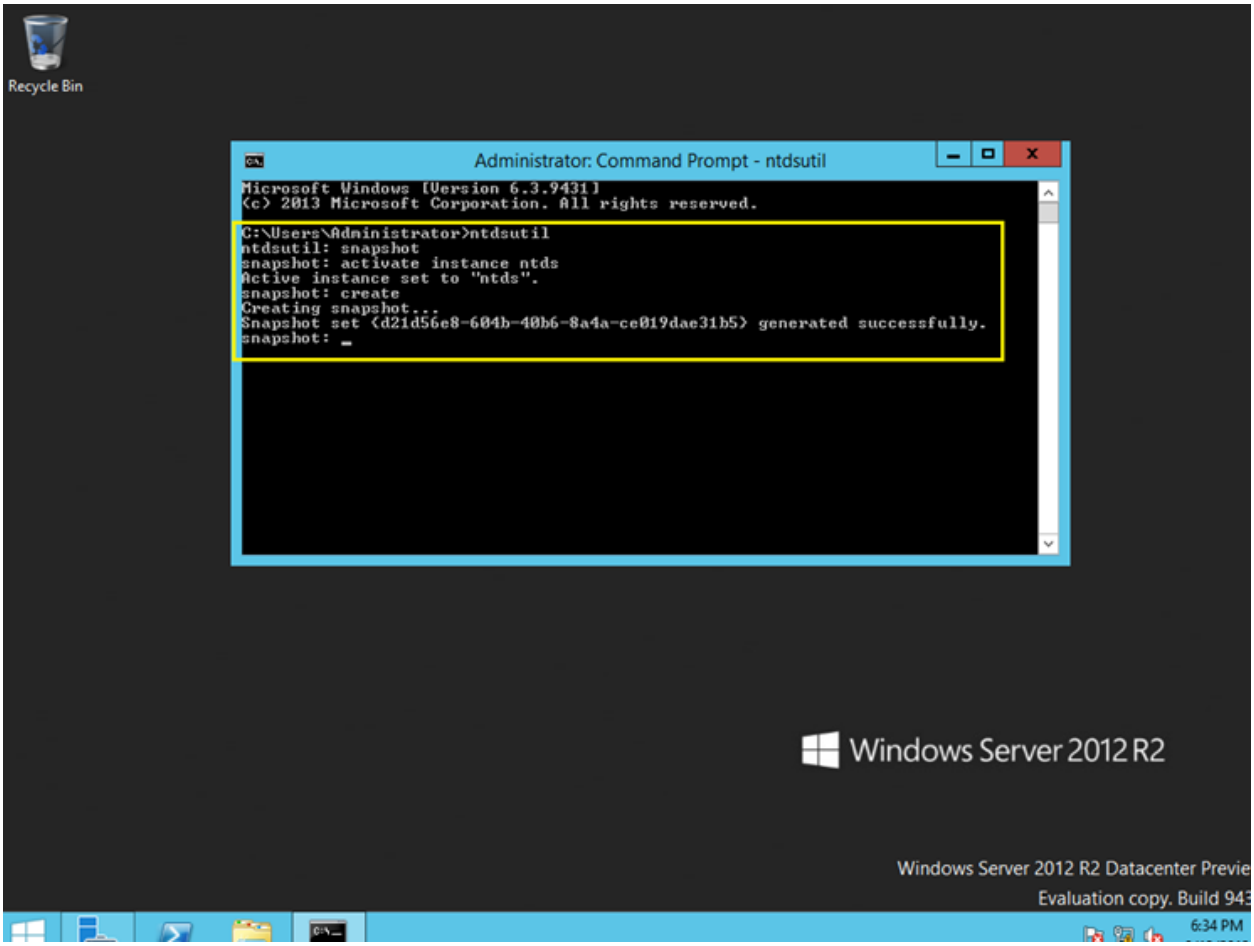
2- Next, type **snapshot** and press enter…



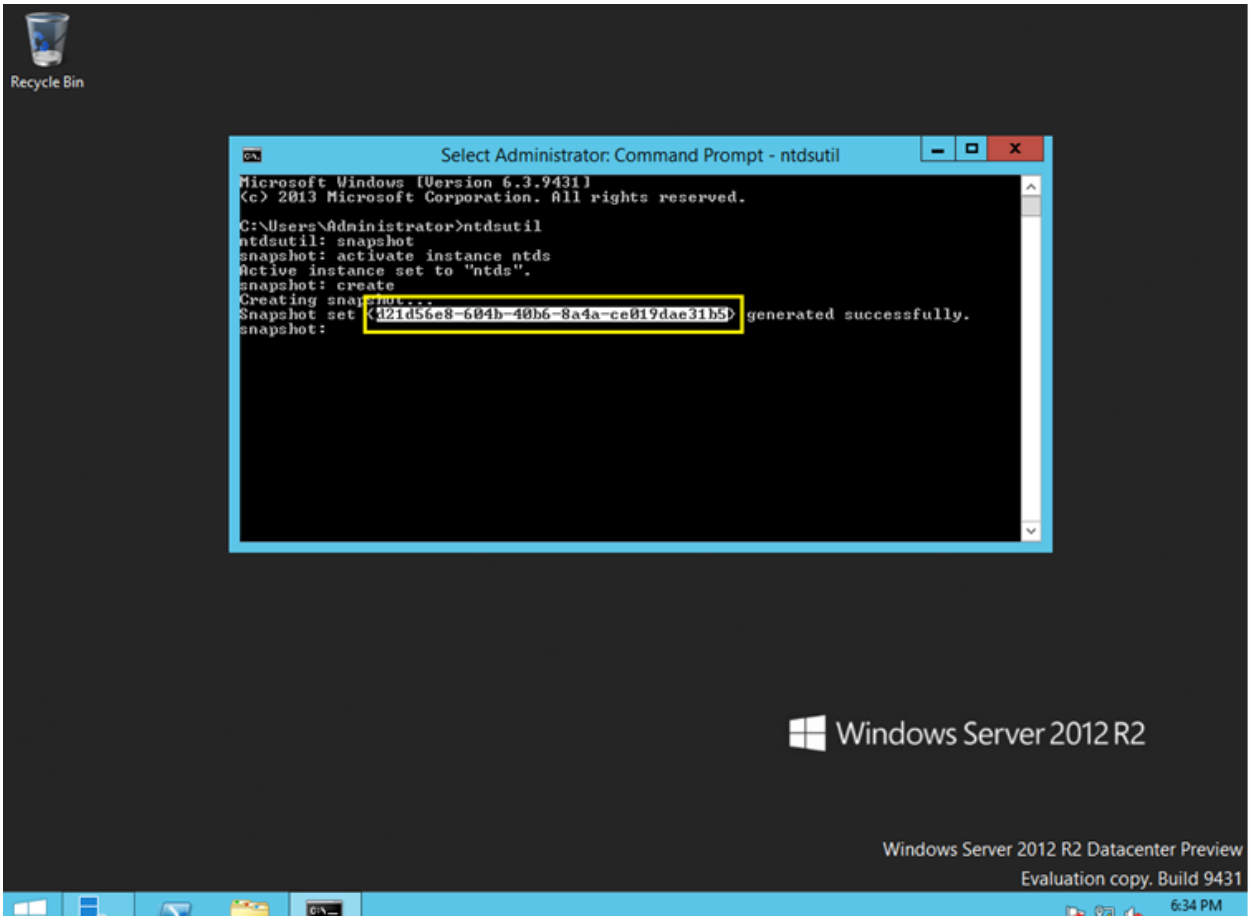
3 – Next, type **activate instance ntds** and press Enter…



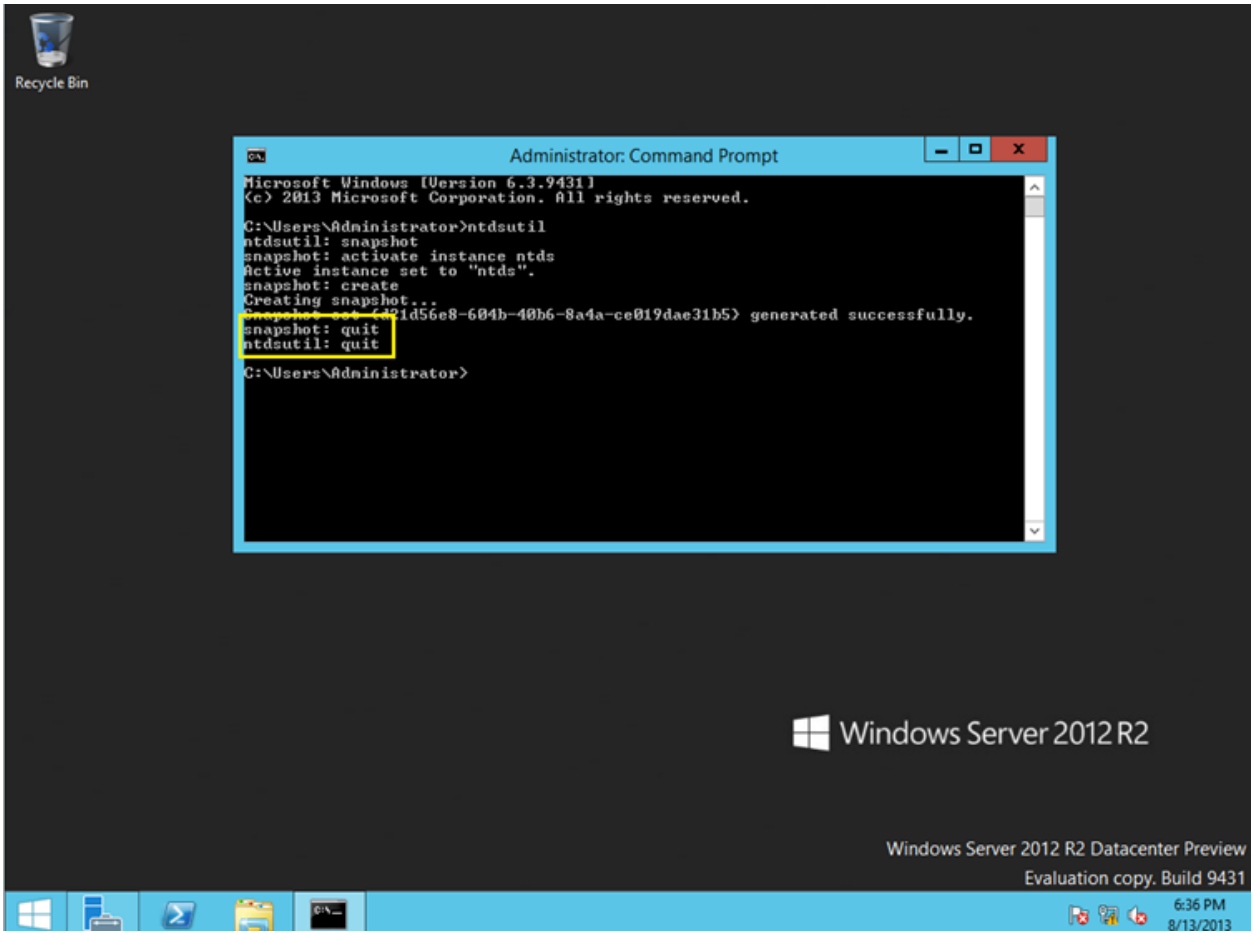
4 – Next, type **create** (this create command is to generate a snapshot of my AD) and press Enter…



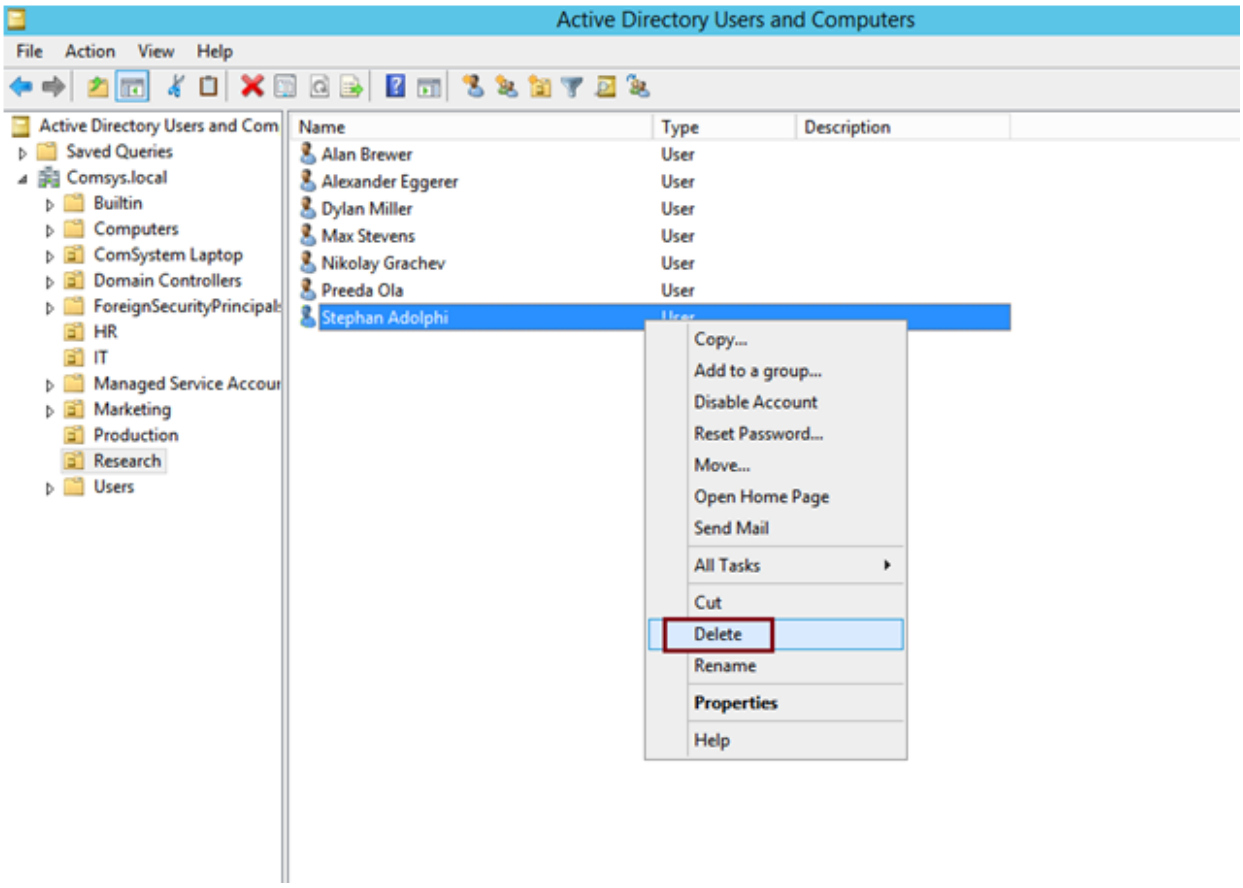
5 – Next, make sure you **copy the copy the GUID** somewhere (highlight the GUID and then copy)…

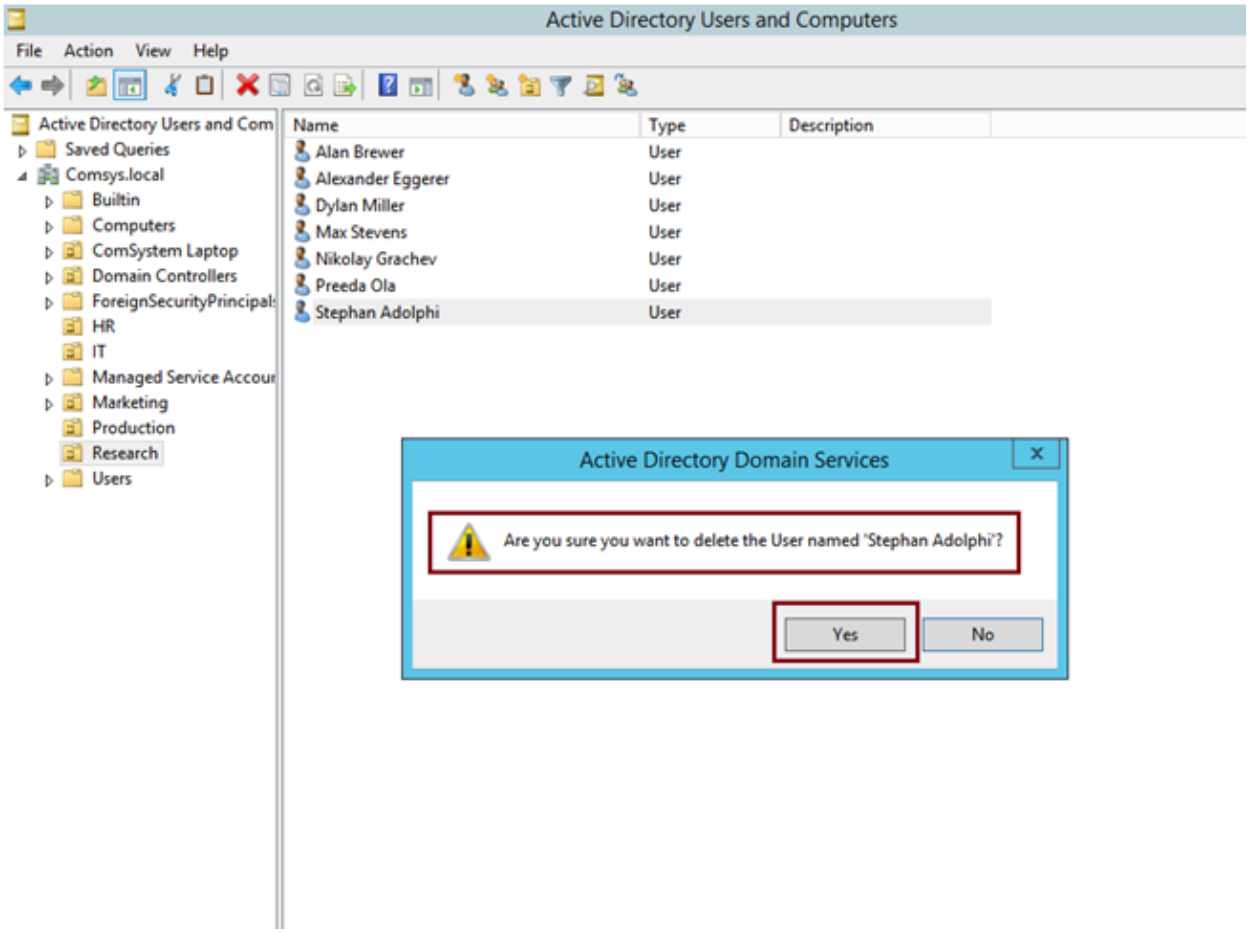


6 – Next, type **quit** 2 times to exit from snapshot…



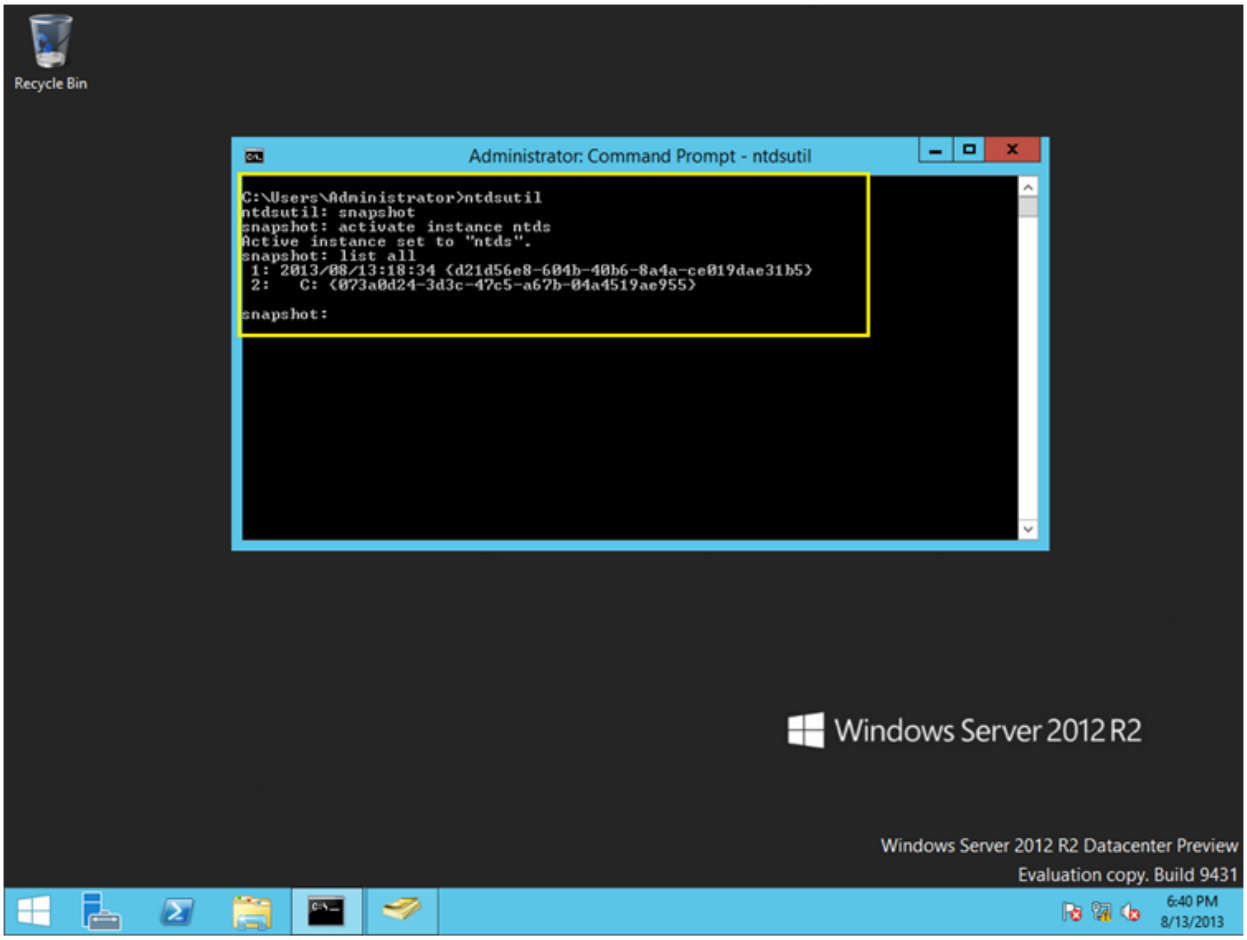
7 – Now, lets **make some change to my ADDS** by deleting 1 of my AD user, for this demo, I choose my user from Research department


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
Comsys.local
Builtin
Computers
ComSystem Laptop
Domain Controllers
ForeignSecurityPrincipals
HR
IT
Managed Service Accour
Marketing
Production
Research
Users
Name
Type
Description
Alan Brewer
User
Alexander Eggerer
User
Dylan Miller
User
Max Stevens
User
Nikolay Grachev
User
Preeda Ola
User
Stephan Adolphi
Copy...
Add to a group...
Disable Account
Reset Password...
Move...
Open Home Page
Send Mail
All Tasks
Cut
Delete
Rename
Properties
Help

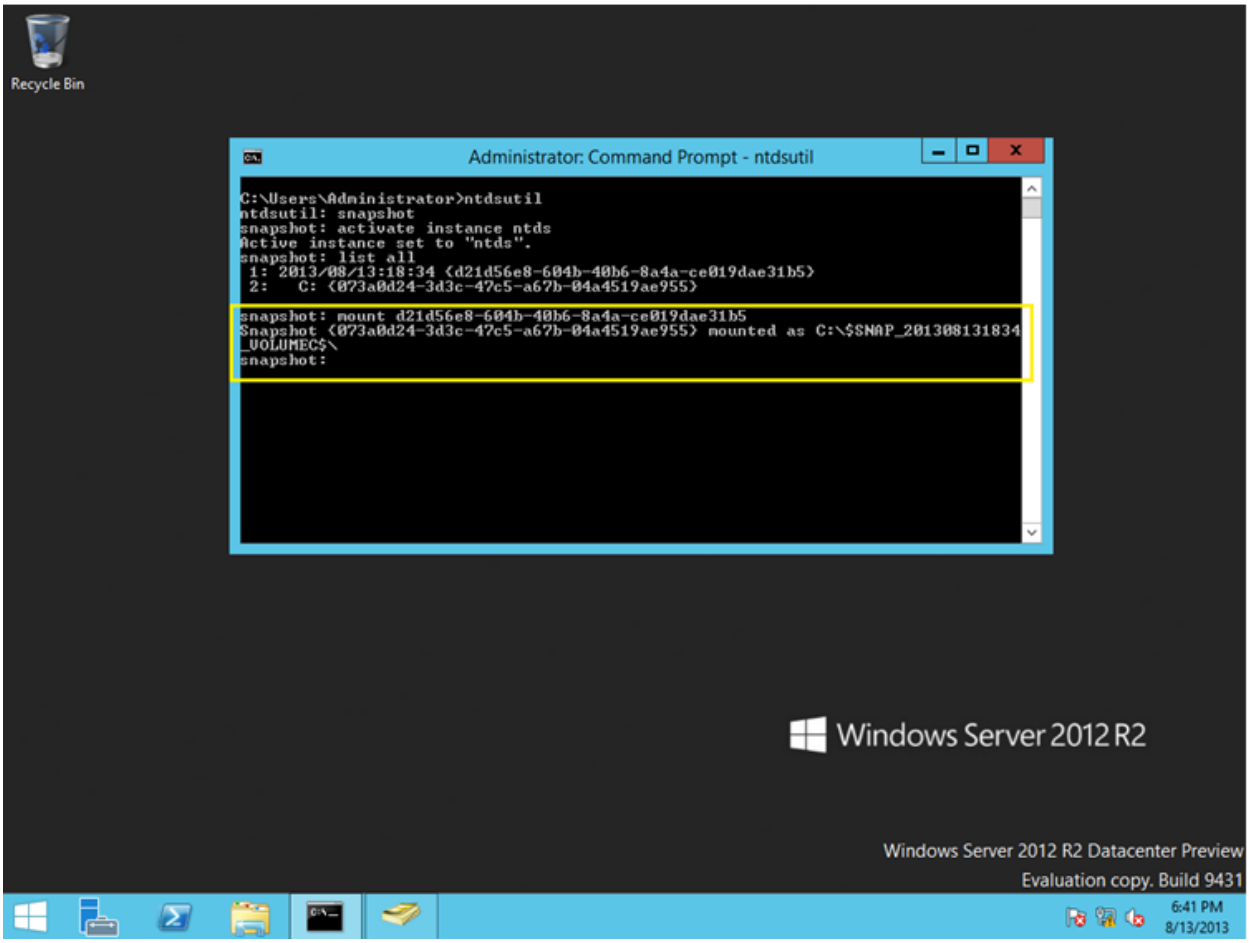


Once you deleted the user, you need to mount an Active Directory snapshot, and create a new instance so that later we can retrieve back the deleted user…

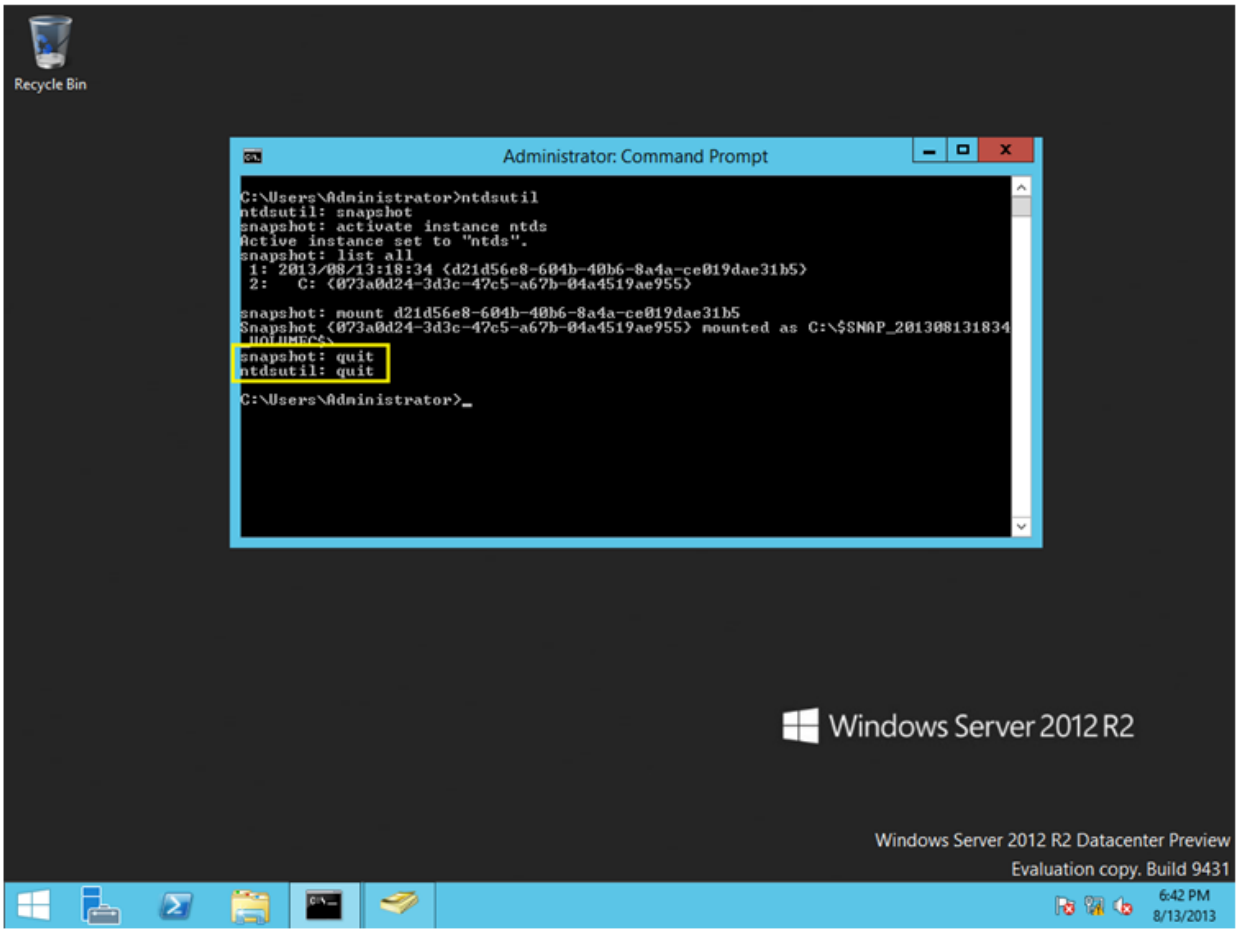
8 – in CMD, type **ntdsutil**, then snapshot, then type **activate instance ntds**, then type **list all** (please refer to the screen shot)…



9 – Next, you need to **mount GUID no** (please refer to my screen shot), type **mount <GUID> no** and press enter…

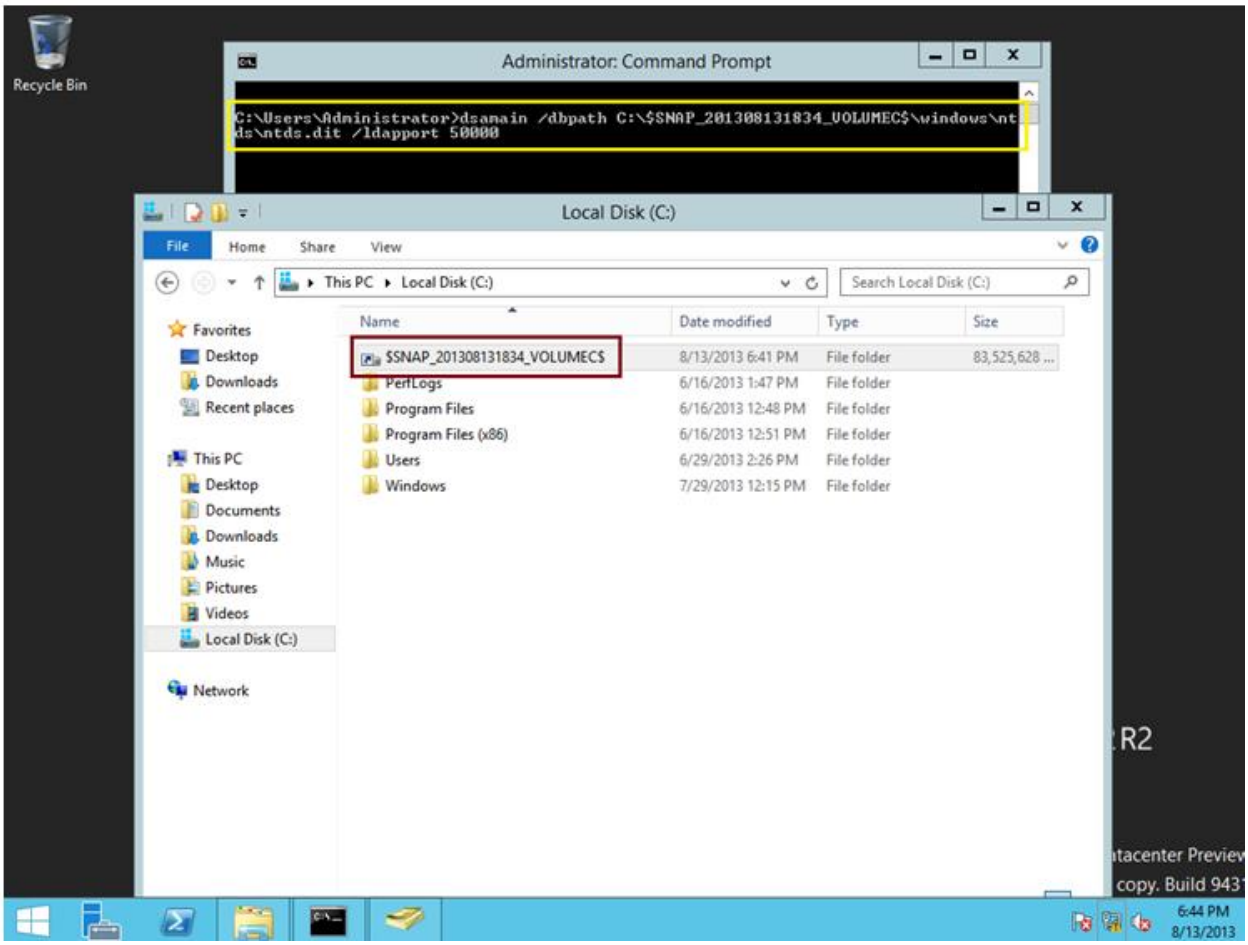


10 – once successful, **exit** the process by typing quit 2 times…



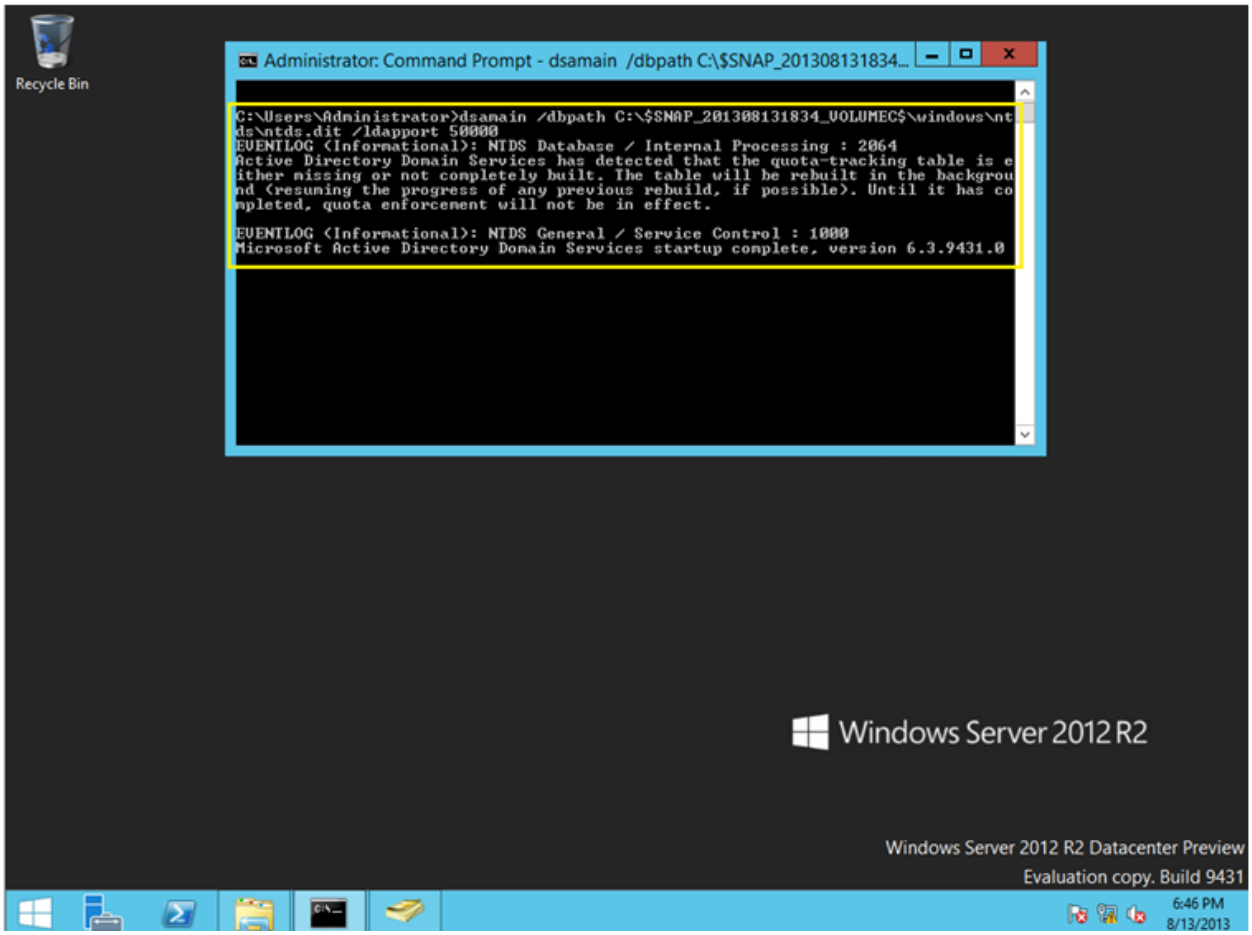
11 – Next, on the CMD, type **dsamain /dbpath C:\$SNAP_datetime_volumec$\windows\ntds\ntds.dit /ldapport 50000**

**** be aware that datetime will be a unique value. There only should be one folder on your C:\ drive with a name that begins with $snap.**

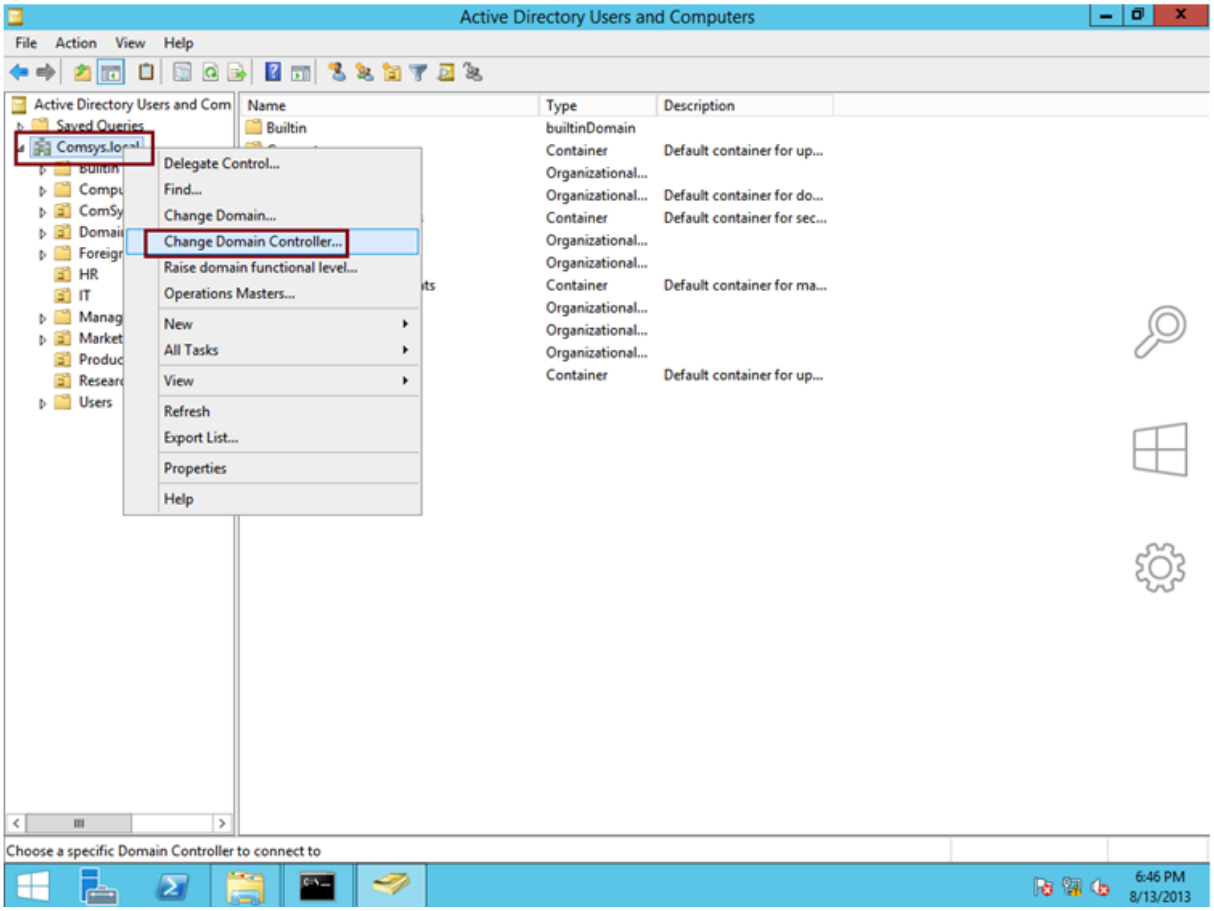


12 – **Leave Dsamain.exe running**, and **do not close the CMD…**

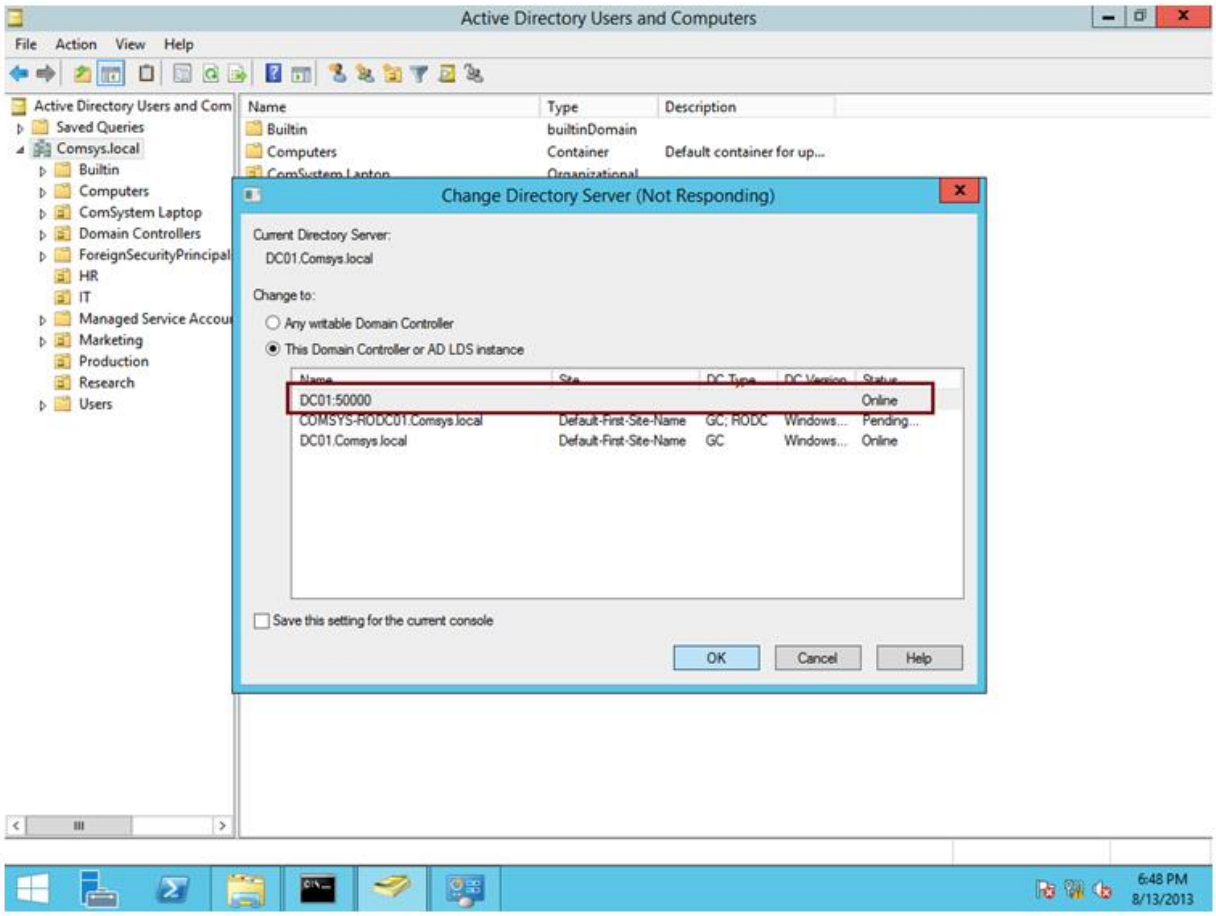
**** A message indicates that Active Directory Domain Services startup is complete…**



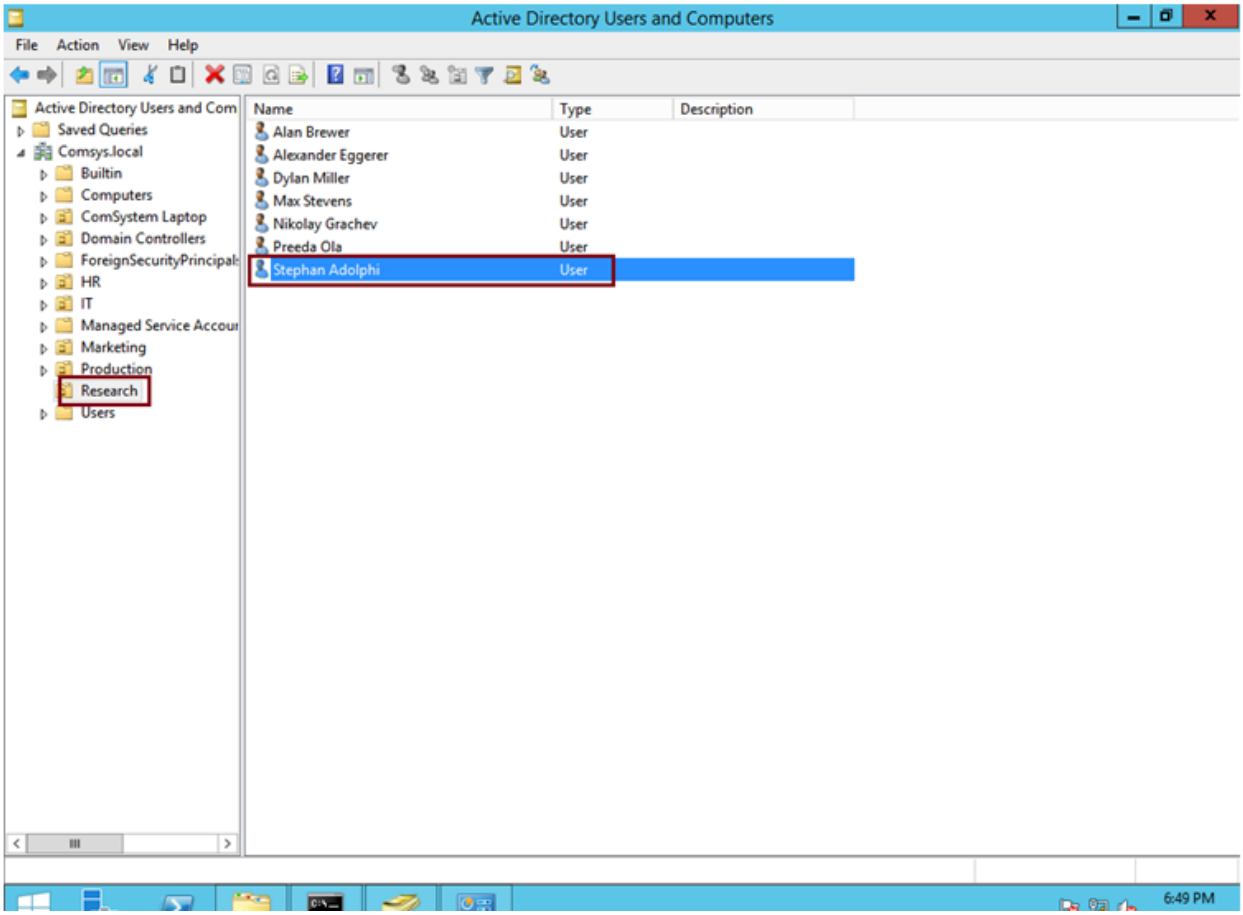
13 – Next, lets explore a snapshot with Active Directory Users and Computers, on the ADUC, **right click Comsys.local** and click **Change Domain Controller**


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
Comsys.local
Builtin
Compu
ComSy
Domai
Foreign
HR
IT
Manag
Market
Produc
Researc
Users
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Name
Type
Description
Builtin
builtinDomain
Container
Default container for up...
Organizational...
Organizational...
Default container for do...
Container
Default container for sec...
Organizational...
Organizational...
Container
Default container for ma...
Organizational...
Organizational...
Organizational...
Container
Default container for up...
Choose a specific Domain Controller to connect to
6:46 PM
8/13/2013

14 – type **DC01:50000 on the <Type a Directory Server name[:port] here>, then click OK…**

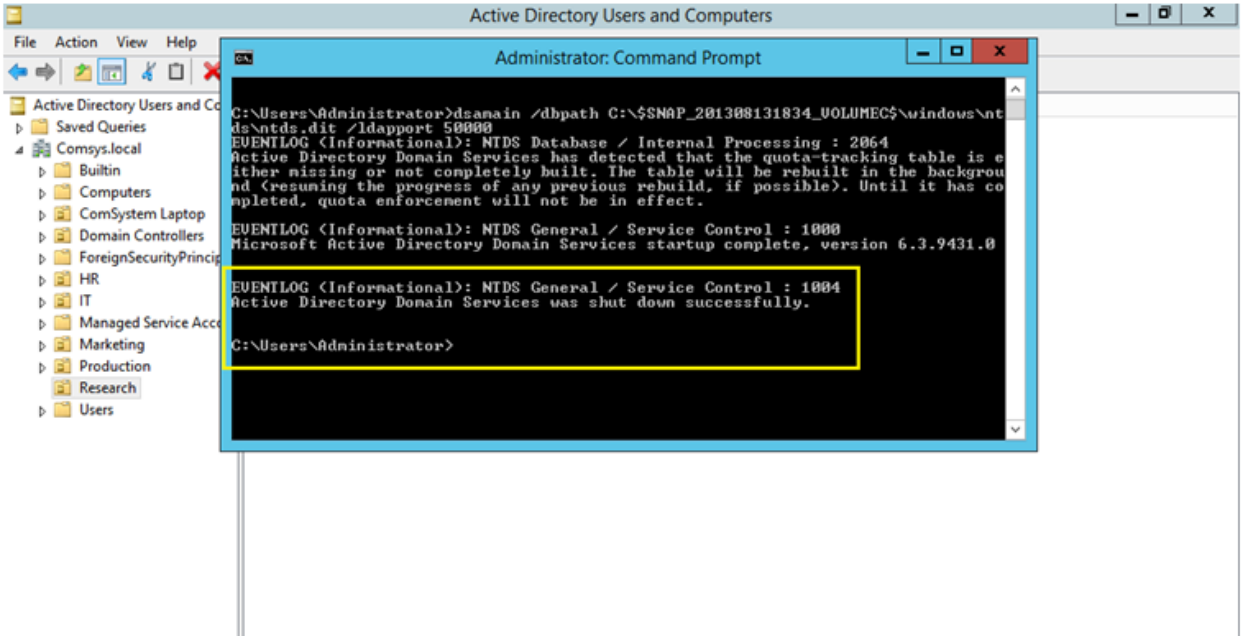


15 – Next, **browse to Research OU** and you will notice that our **deleted user is now back online**



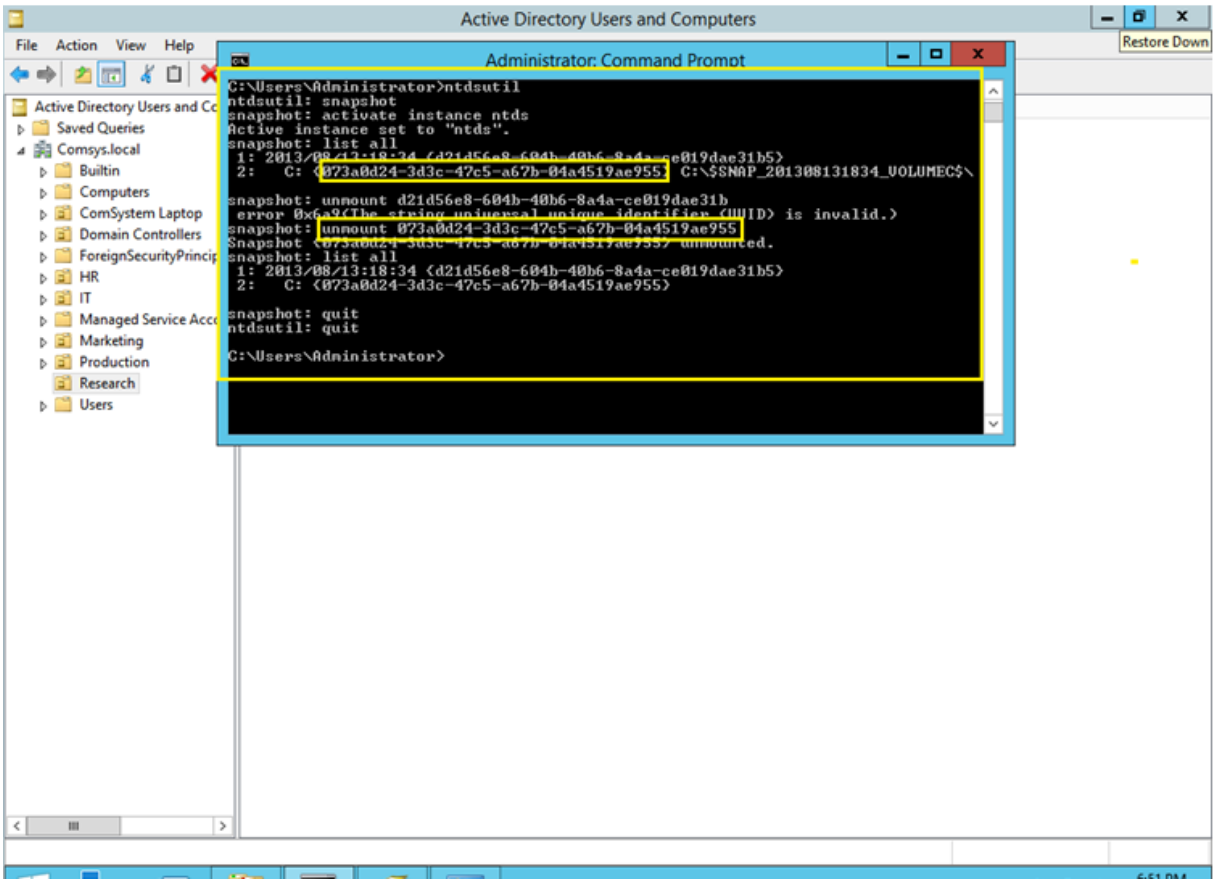
16 – our last step is to **unmount an Active Directory snapshot**…

on the command prompt, press **CTRL+C to stop DSAMain.exe**…



17 – then wrap up the whole process, on the CMD, type :

ntdsutil
snapshot
activate instance ntds
list all
unmount guid (guid is the GUID of the snapshot)
list all
quit
quit


Active Directory Users and Computers
File Action View Help
Restore Down
Active Directory Users and Co
Saved Queries
Comsys.local
Builtin
Computers
ComSystem Laptop
Domain Controllers
ForeignSecurityPrincip
HR
IT
Managed Service Acc
Marketing
Production
Research
Users
Administrator: Command Prompt
C:\Users\Administrator>ntdsutil
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: list all
1: 2013/08/13:18:34 {d21d56e8-604b-40b6-8a4a-ce019dae31b5}
2: C: {073a0d24-3d3c-47c5-a67b-04a4519ae955} C:\$SNAP_201308131834_VOLUMEC$\
snapshot: unmount d21d56e8-604b-40b6-8a4a-ce019dae31b
error 0x6a9(The string universal unique identifier (UUID) is invalid.)
snapshot: unmount 073a0d24-3d3c-47c5-a67b-04a4519ae955
Snapshot {073a0d24-3d3c-47c5-a67b-04a4519ae955} unmounted.
snapshot: list all
1: 2013/08/13:18:34 {d21d56e8-604b-40b6-8a4a-ce019dae31b5}
2: C: {073a0d24-3d3c-47c5-a67b-04a4519ae955}
snapshot: quit
ntdsutil: quit
C:\Users\Administrator>