Lab 7 Active Directory Maintenance

Part 1 Creating and mounting AD SnapShots

1. Log on to DC2
2. Open an elevated command prompt
3. Type **ntdsutil**
4. Type **activate instance ntds**
5. Type **snapshot**
6. Type **create**

View the snapshots by typing the following command

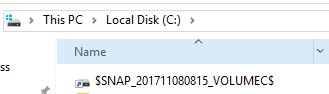
1. **list all**

|  |
| --- |
| **Screenshot the list all command that shows snapshots** |

1. Type **mount 1**

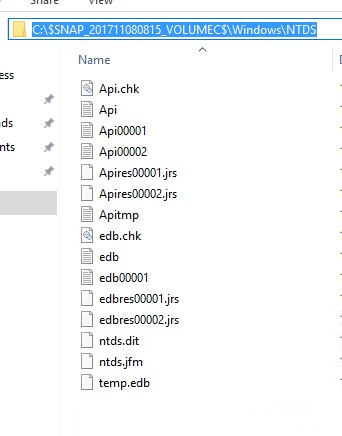
You should receive a message showing that the snapshot is mounted and the location of the mounted snapshot

1. Type **quit** and then **quit** again to exit the ntdsutil
2. From file explorer Navigate to the C:\You should see the mounted volume here



1. Navigate into this VolumeWindowsNTDS

You should see the ntds.dit file which is a copy of the database.

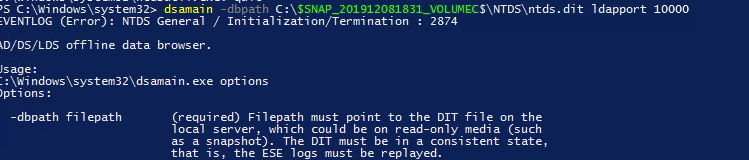


The snapshot is mounted but it cannot be accessed via

directory tools until it is hosted. This can be accomplished using the dsamain command

1. From a command prompt type, the following (Note you will need to **change the path to match your path from the previous steps.**

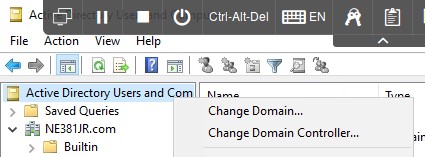
**dsamain -dbpath "C:\$SNAP\_201811101730\_VOLUMEC$\Windows\NTDS\ntds.dit" ldapport 10000**

**Error:**

You should get a message stating the Active Directory Domain

Services startup complete

1. Make sure you leave this window open
2. Launch ADUC and in the left pane right click and select change domain controller

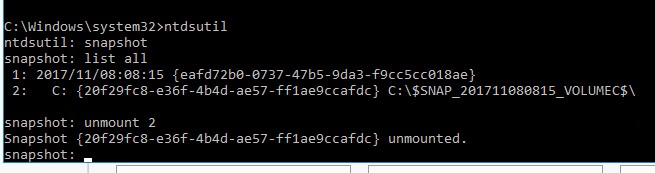


1. Select the This domain Controller or AD LDS instance option and then click in the list box below where it reads

<Type a Directory Server name[:port] here>

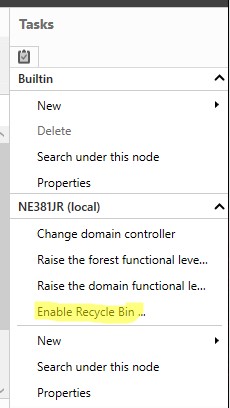
1. Type localhost:10000 and press Enter
2. When the Status reads “Online,” the server is connected and recognized. Click OK.
3. You can now browse the snapshot of the directory try it out.
4. Close out of ADUC
5. Open the command prompt where you have dsamain running and press Ctrl+C you should get a message stating Active Directory Domain Services was shut down successfully
6. Type **ntdsutil** and press Enter 22. Type **snapshot** and press Enter.

23. Type **unmount 2** and press Enter



Part 2 AD Recycle Bin

* 1. From the Start Menu launch Server Manager.
  2. Select Tools > Active Directory Administrative Center.
  3. On the left-hand navigation pane select the domain you want to enable Recycle Bin for.
  4. On the right-hand Tasks pane, click Enable Recycle Bin



* 1. Browse to a user, right-click it, and select Delete.
  2. Click Yes to Confirm
  3. Browse to the Deleted Objects container to see the deleted object.

|  |
| --- |
| **Screenshot the deleted user in the Recycle bin** |

* 1. Right Click on in and select Restore

Part 3 ADDS Services

One of the best troubleshooting and error fixing tasks you can do for ADDS is to restart the service. This will fix the service or point to the issue in the event log. Also, AD is a database, if performance is slow then it may be due to fragmentation.

* 1. From the Start Menu launch Server Manager
  2. Select Tools > Services
  3. Right-click the service Active Directory Domain Services and select Stop
  4. A dialog appears warning you of dependent services that must also be stopped. Click Yes

Take extra note of these services. These services are all critical to ADDS

* 1. Launch a command prompt.
  2. Type **ntdsutil** and press Enter.
  3. At the **ntdsutil** prompt type activate instance ntds and press Enter.
  4. At the **ntdsutil** prompt type files and press Enter.
  5. At the files prompt type **compact** to C:\defrag and press Enter.
  6. Once the operation completes, **review the instructions** for copying the ntds.dit file and deleting log files. (Do not actually take the steps to use the defragmented copy.

|  |
| --- |
| **Screenshot the defrag screen** |

* 1. Make sure that ADDS is started again before proceeding

Part 4 Setting Time from an external source

ADDS keeping time is critical to replication and overall directory health. The ability to access resources i.e Shares, logon servers is severely impacted if time is off in the environment. Please read the following [https://docs.microsoft.com/en-us/windowsserver/identity/ad-ds/get-started/windows-time-service/howthe-windows-time-service-works](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/windows-time-service/how-the-windows-time-service-works)

This will provide you with a very detailed explaniation of how time service works in AD. In a nutshell the PDC emulator is the time source for the domain. Other DC’s will get their time from the PDC emulator and clients will get there time from the closest DC.

1. Open a command prompt on DC2 (This should be your PDC emulator) and issue the following comamnd **w32tm /config /manualpeerlist:"tick.usno.navy.mil "**

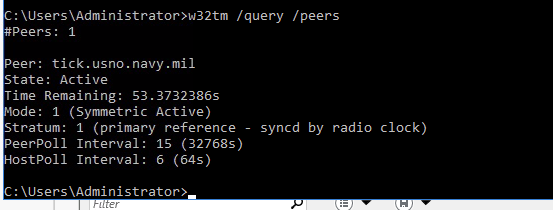
**/syncfromflags:manual /reliable:yes /update**

You should receive a message stating the command completed successfully.

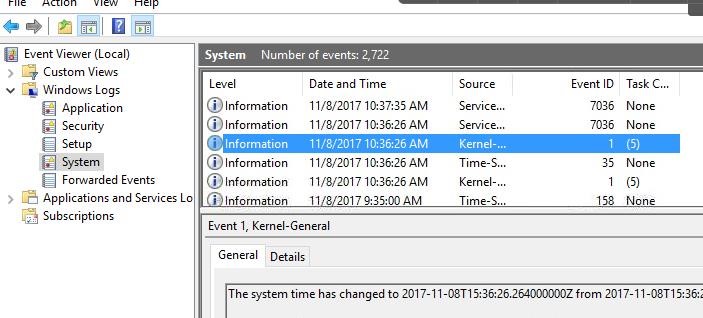
1. Type **w32tm /query /peers**

You should see that the peer is set to tick.usno.navy.mil

**Screenshot the time peer for submission to canvas\***



1. Type **w32tm /resync**
2. Open Event Viewer and in the system log locate the 1 and 35 event ID This shows that the system is syncing its time

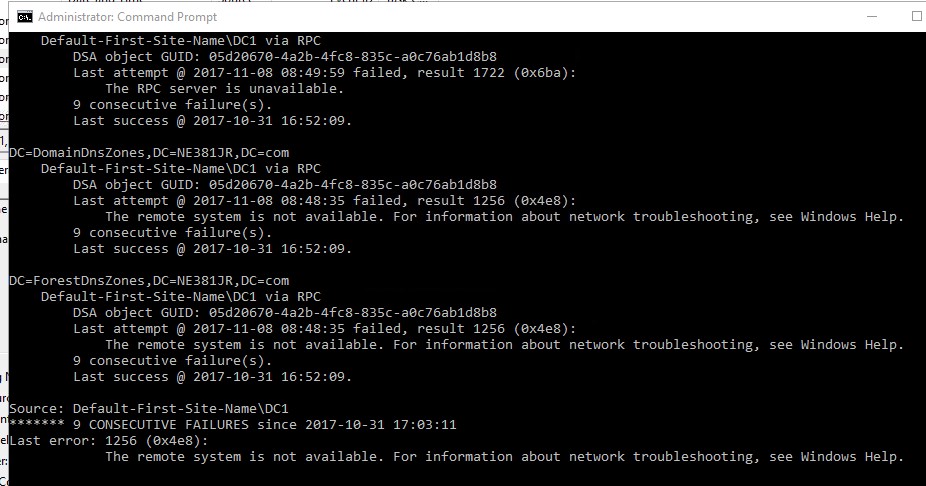


**Continued on next page…..**

Part 5 Monitoring and Managing Replication

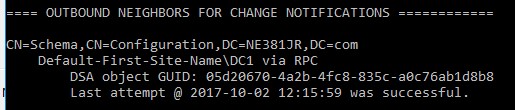
1. Open a command prompt
2. Type **repadmin /showrepl**

The command will give a report on replication issues if any are detected. Here is a screenshot (See below) of what this looks like. In the screenshot my DC1 is offline so it is not available for replication.

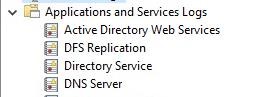


In a multiple DC environment, it can be difficult to detect errors. To see what DC the current DC is setup to replicate to we can issue the following command.

1. Type **repadmin /showrepl /repsto**



1. While troubleshooting ADDS you can use the repadmin and the Event viewer to identify the problem. A majority of the time the fix and the problem is detailed in the event viewer.
2. Open Event Viewer on DC2
3. Navigate to Applications and Services Logs then expand out to see the following



1. These logs contain all the information about the current state of ADDS as a whole. Navigating these logs will provide you with the information needed to fix any issue with AD

|  |
| --- |
| Screenshot an Event showing an entry from the repadmin command: |