Active Directory Database Mounting Tool (AD DS and AD LDS Snapshots)

Windows Server 2008 introduces a new feature that allows you to create and view snapshots of data that is stored in AD DS and AD LDS. The Active Directory database mounting tool (Dsamain.exe) was referred to as Snapshot Viewer and Active Directory data mining tool during the beta releases of Windows Server 2008.

Microsoft states that the Active Directory database mounting tool is useful to simplify the forest recovery process and to audit modified and deleted objects. These are two very useful reasons to learn more about the Active Directory mounting tool. What follows is a step-by-step on how to use the Active Directory database mounting tool.

Overview of the Active Directory Database Mounting Tool

It is important to note that the Active Directory database mounting tool is built into Windows Server 2008 and can be used for AD DS and AD LDS. There are essentially three tools you will leverage when using the Active Directory database mounting tool:

- **Ntdsutil snapshot** is a new operation that allows you to create, delete, list, mount, and unmount snapshots of AD DS and AD LDS data.
- Dsamain.exe allows you to expose snapshots as LDAP servers.
- LDP and Active Directory Users and Computers allow you to view the data within a snapshot.

It is also important to note that by default, only members of the Enterprise Admins and Domain Admins groups can view data stored within snapshots. However, Dsamain.exe does allow you to allow non-administrators to access data that is stored in a snapshot.

Another great feature of the tool is that the permissions within the data itself are enforced. So, for example, if a group has been denied the ability to read data on user accounts in a particular OU in your AD DS domain, that same group will be denied the ability to read these user accounts in the snapshot, even if you use Dsamain.exe to grant them access to the snapshot.

This new feature is not fool proof though. Data can be copied from one forest to another forest, and then the data can be exploited. As a result, you need to ensure you properly secure the snapshot files and do not rely solely on the AD DS or AD LDS permissions.

Step-by-Step Guide to Using the Active Directory Database Mounting Tool

The steps required to use the Active Directory Database Mounting Tool include the following:

1. Manually or automatically create a snapshot of your AD DS or AD LDS database.
2. Mount the snapshot.
3. Expose the snapshot as an LDAP server.
4. Connect to the snapshot.
5. View data in the snapshot.

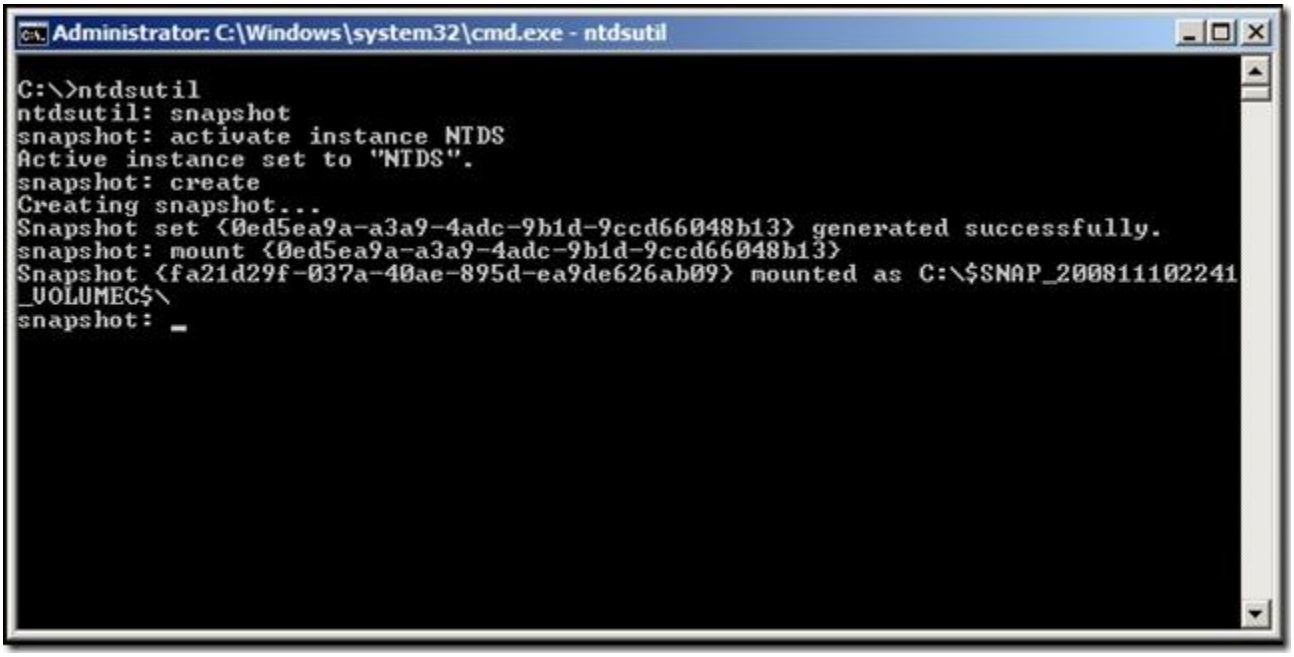
The steps that follow are specific to AD DS. The steps required for AD LDS are very similar and can be found here: http://technet.microsoft.com/en-us/library/cc753609.aspx.

Create a Snapshot of Active Directory Domain Services

As previously mentioned, a snapshot can be created manually or it can be scheduled by using Task Scheduler in Windows Server 2008. I will cover the steps for both below. It is my recommendation that you schedule a regular task that creates snapshots of your AD DS domain.

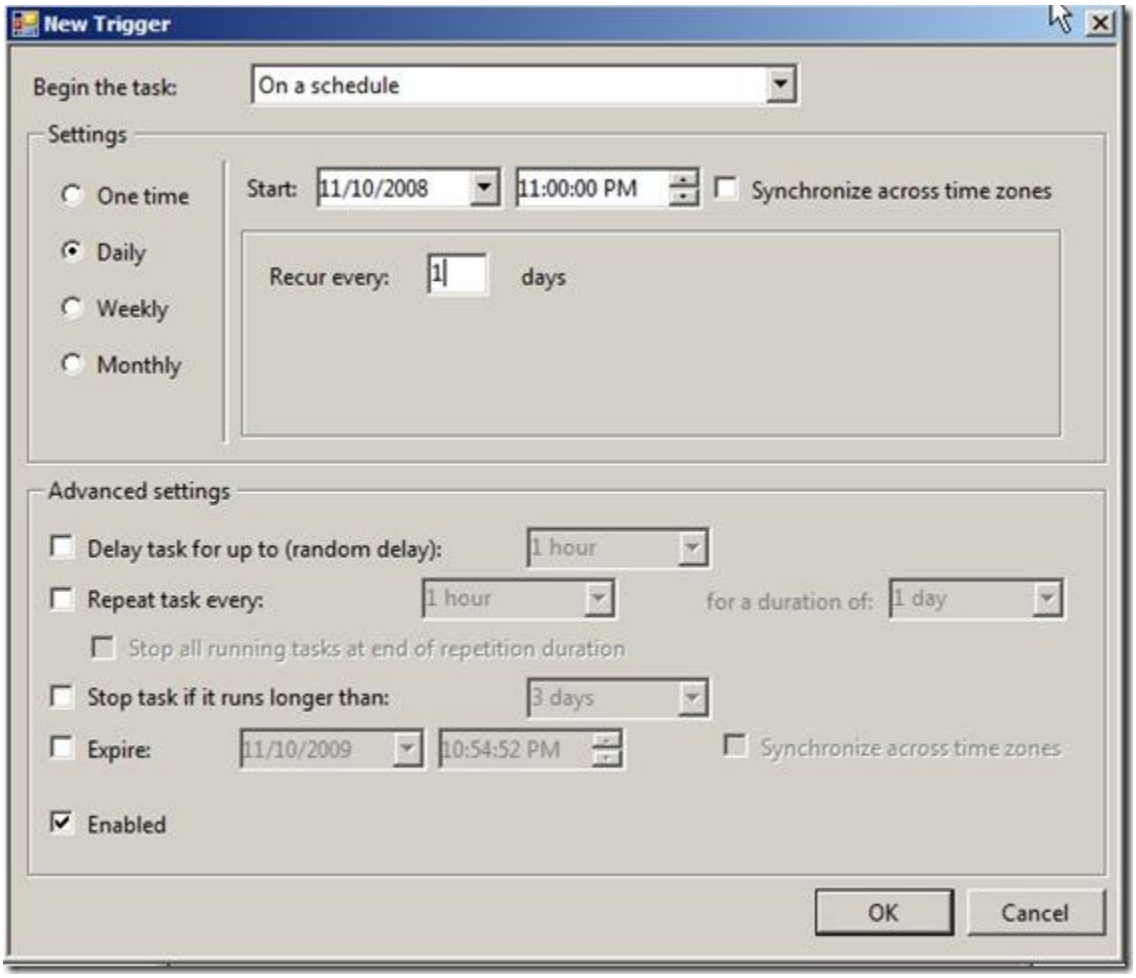
Manually Create a Snapshot

1. Logon to a Windows Server 2008 domain controller.
2. Click **Start**, and then click **Command Prompt**.
3. In the Command Prompt window, type **ntdsutil**, and then hit **Enter**.
4. At the ntdsutil prompt, type **snapshot**, and then hit **Enter**.
5. At the snapshot prompt, type **activate instance NTDS**, and then hit **Enter**.
6. At the snapshot prompt, type **create**, and then hit **Enter**.
7. Record the GUID that is returned by the above command.



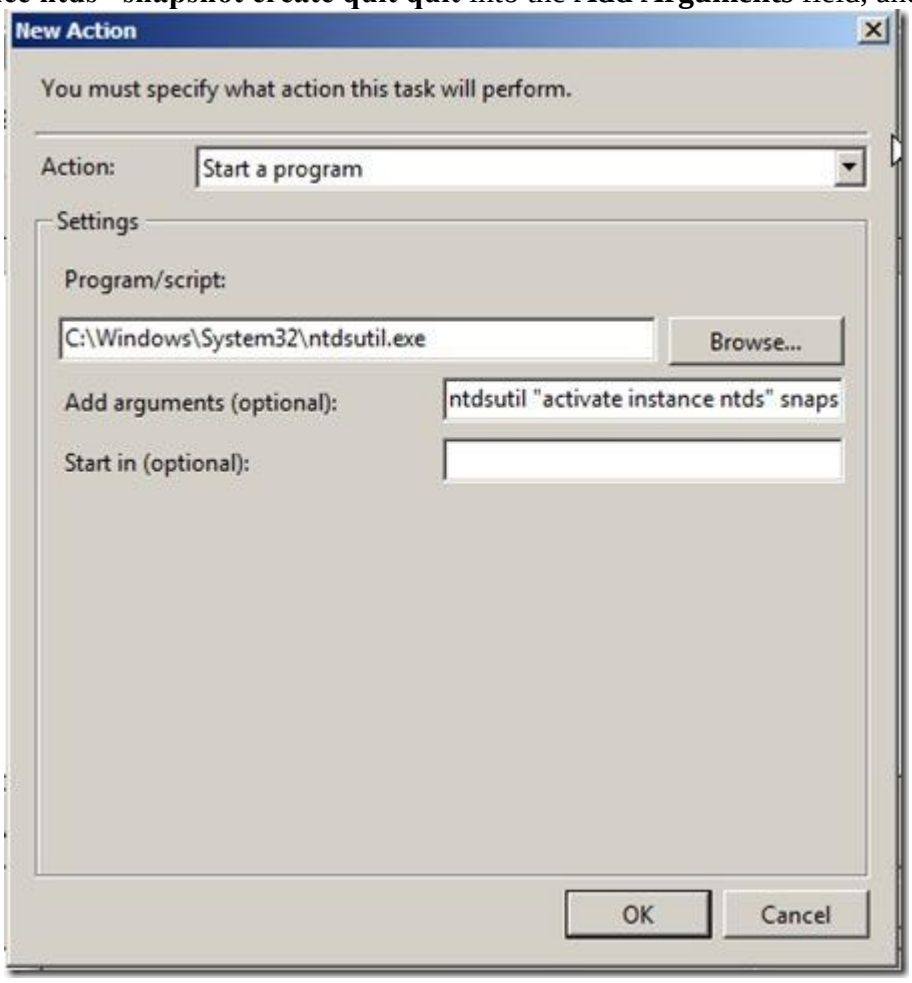
Schedule a Task to Create a Snapshot

1. Logon to a Windows Server 2008 domain controller.
2. Click **Start**, click **Administrative Tools**, and then click **Task Scheduler**.
3. On the **Action** menu in Task Scheduler, click **Create Task**.
4. On the **General** tab of the **Create Task Wizard**, type a name for the task into the **Name** field.
5. On the **Triggers** tab of the Create Task Wizard, click **New**.
6. On the **New Trigger** window, define a trigger for the task, and then click **OK**.



7. On the **Action** tab, click **New**.
8. On the **New Task** window, ensure **Start a program** is selected from the drop-down, type **C:\Windows\System32\ntdsutil.exe** into the **Program/Script:** field, and type **ntdsutil**

“activate instance ntds” snapshot create quit quit into the **Add Arguments** field, and then click **OK**.



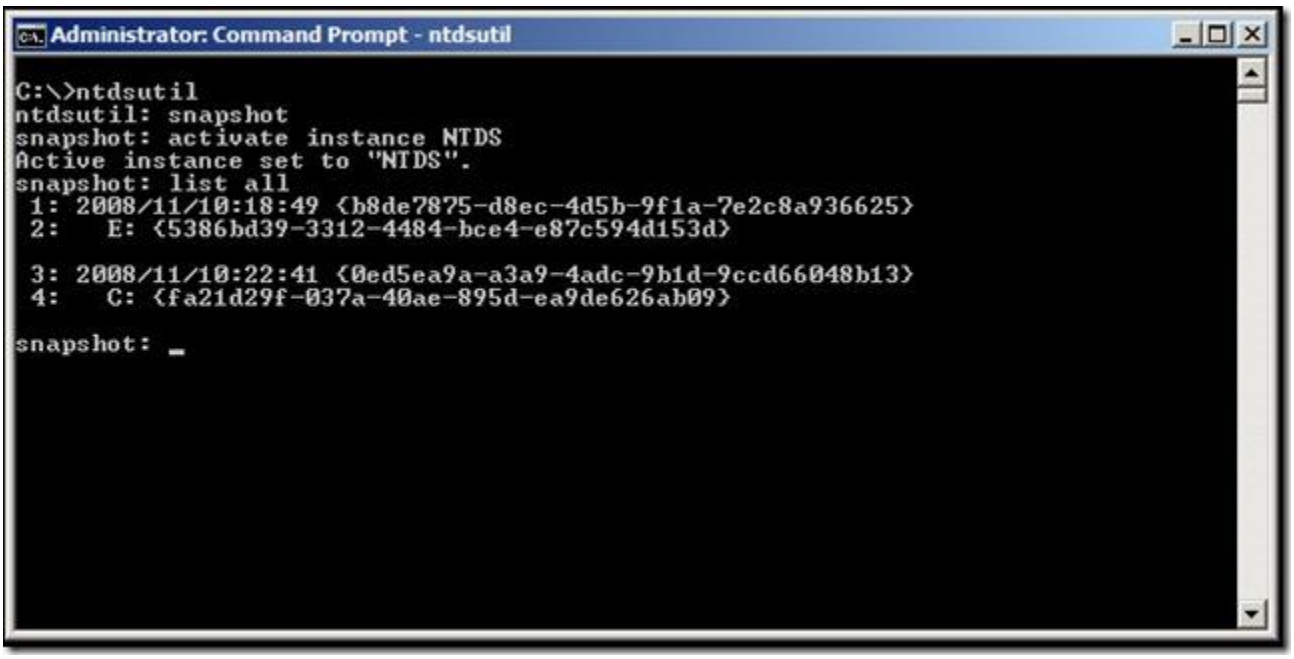
9. Click **OK** on the Create Task Wizard.

Mount the Snapshot

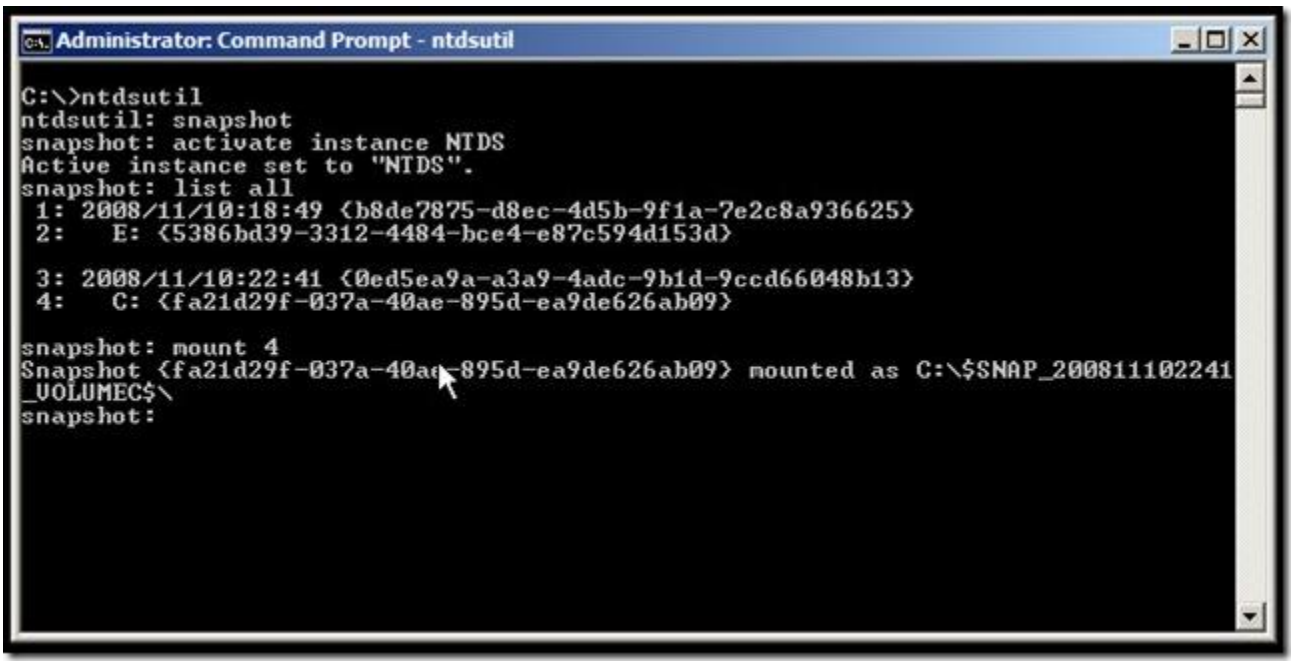
NOTE: When a snapshot is manually created, it is automatically mounted. Therefore, if you manually created the snapshot, you can skip these steps.

1. Logon to a Windows Server 2008 domain controller.
2. Click **Start**, and then click **Command Prompt**.
3. In the Command Prompt window, type **ntdsutil**, and then hit **Enter**.
4. At the ntdsutil prompt, type **snapshot**, and then hit **Enter**.
5. At the snapshot prompt, type **activate instance NTDS**, and then hit **Enter.**

6. At the snapshot prompt, type **list all**, and then hit **Enter**.



7. The snapshot is item 4 above.
8. At the snapshot prompt, type **mount 4**, and then hit **Enter**.

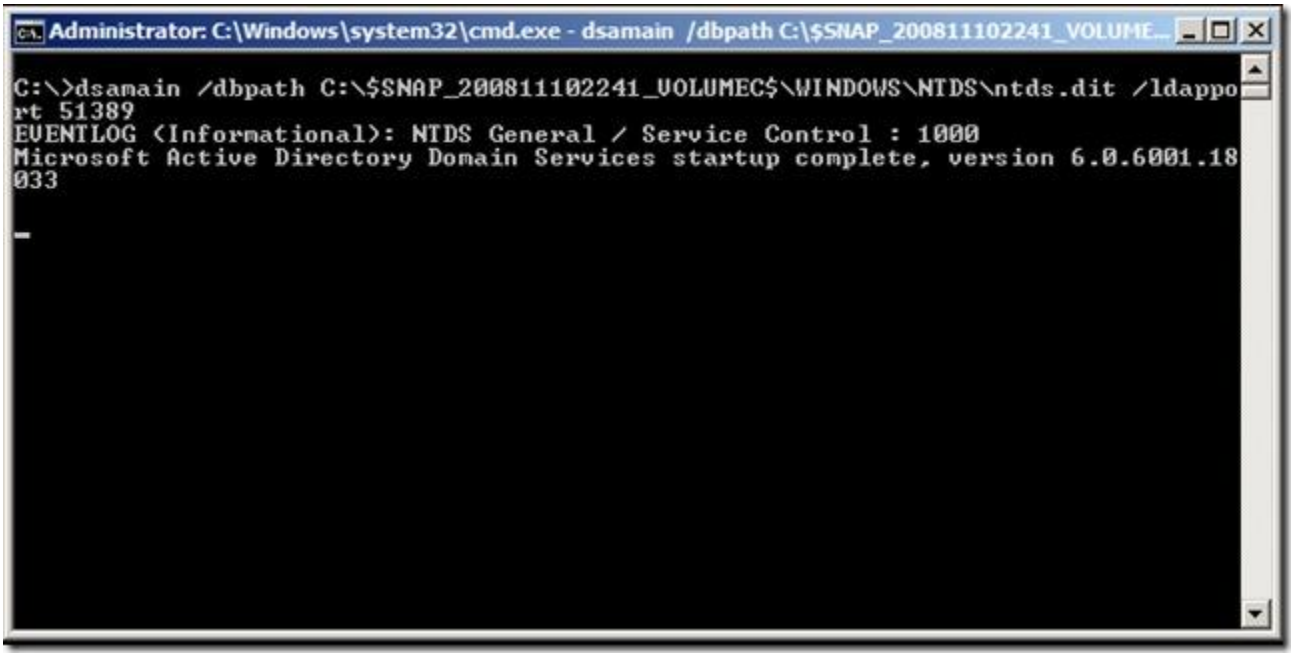


9. If the mounting was successful, you will see Snapshot *{GUID}* mounted as *PATH*, where *{GUID}* is the GUID that corresponds to the snapshot, and *PATH* is the path where the snapshot was mounted.
10. Record the path.

Expose the Snapshot as an LDAP Server

Now that the snapshot has been created and mounted, you need to expose the snapshot as an LDAP server so that data can be read from it. By exposing the snapshot as an LDAP server, users can connect to it by using the native Windows LDAP tools, such as LDP.exe and Active Directory Users and Computers.

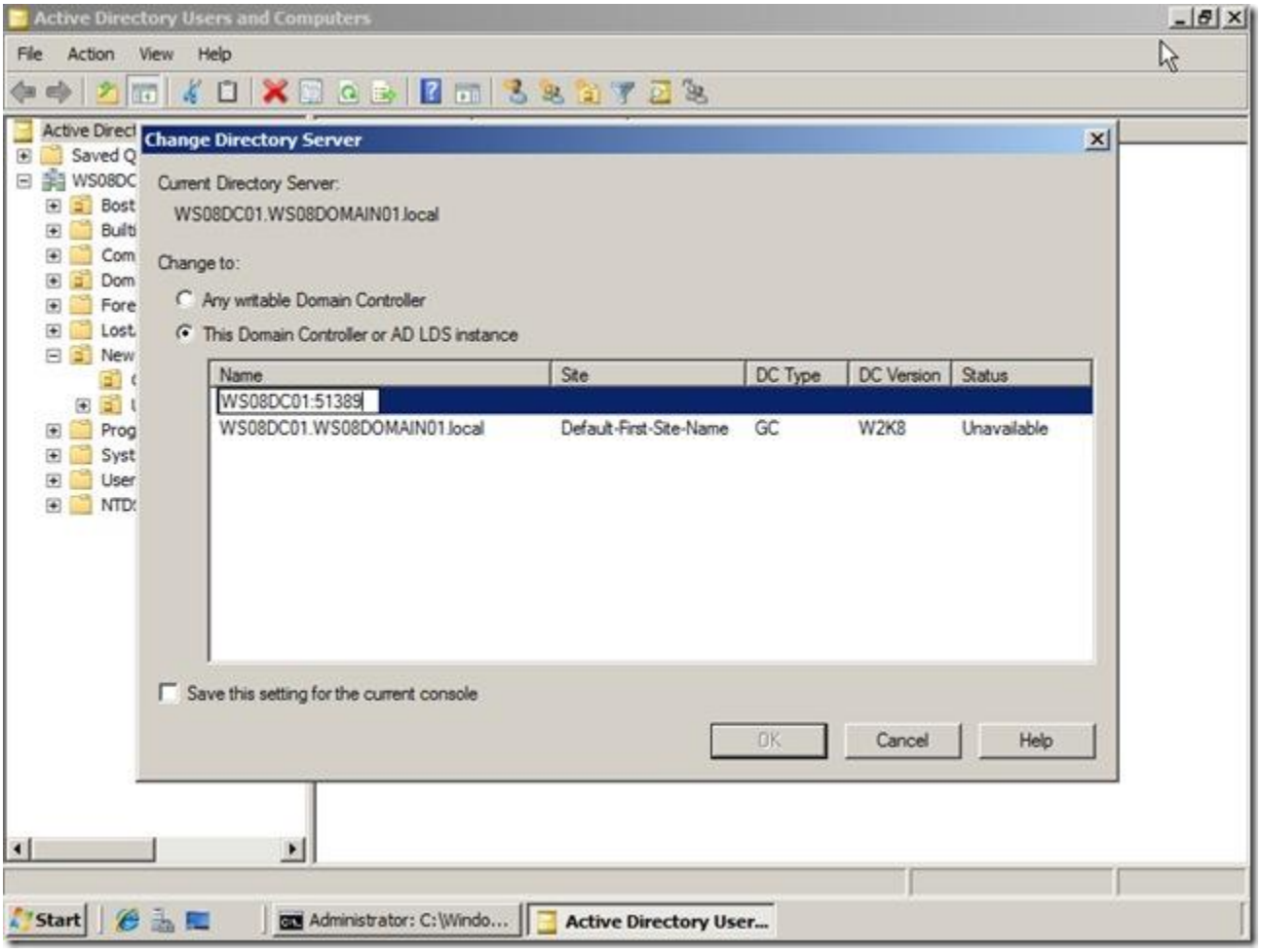
1. Logon to a Windows Server 2008 domain controller.
2. Click **Start**, and then click **Command Prompt**.
3. In the Command Prompt window, type dsamain /dbpath C:\$SNAP_200811102241_VOLUMEC$\WINDOWS\NTDS\ntds.dit /ldapport 51389, and then hit **Enter**.
    - **/dbpath C:\$SNAP_200811102241_VOLUMEC$\WINDOWS\NTDS\ntds.dit** represents the path to the snapshot, which was recorded in step 10 above.
    - **/ldapport 51389** represents the LDAP port to use. It is important that 389 not be used on a domain controller.
4. "Microsoft Active Directory Domain Services startup complete" will appear in the Command Prompt window after running the above command. This means the snapshot is exposed as an LDAP server, and you can proceed to access data on it. NOTE: Do not close the Command Prompt window or the snapshot will no longer be exposed as an LDAP server.



Connect to the Snapshot

You can connect to the snapshot by using any LDAP tool. In this example, I will use the Active Directory Users and Computers console to connect to the snapshot.

1. Log on to a domain controller or a member computer that has Windows Server 2008 Remote Server Administration Tools (RSAT) installed.
2. Click **Start**, **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, right-click on the Active Directory Users and Computers node, and then click **Change Domain Controller**.
4. On the **Change Directory Server** window, click **<Type a Domain Controller name or an IP Address here>**, and type the name and port number of the server where the snapshot is exposed on.



View Data in the Snapshot

To view data in the snapshot, Find the object (user, computer, group, contact, OU, etc.) you want to view, and view the object as you would view live AD DS objects.