3/29/2021

Hands On Exercise

Chapter 6

Domain Controller and Active Directory Management

(Part2)

El Adel, Taoufik
IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

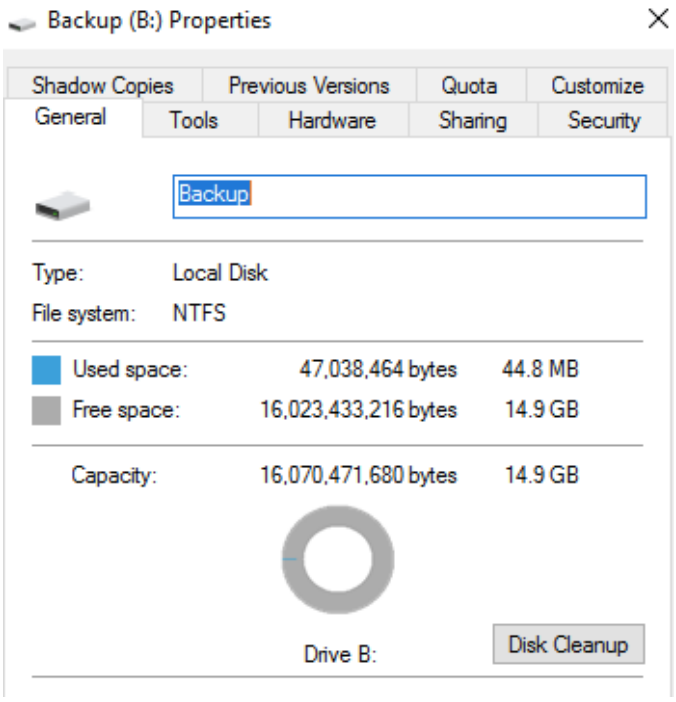
Table 6-1 Activity requirements

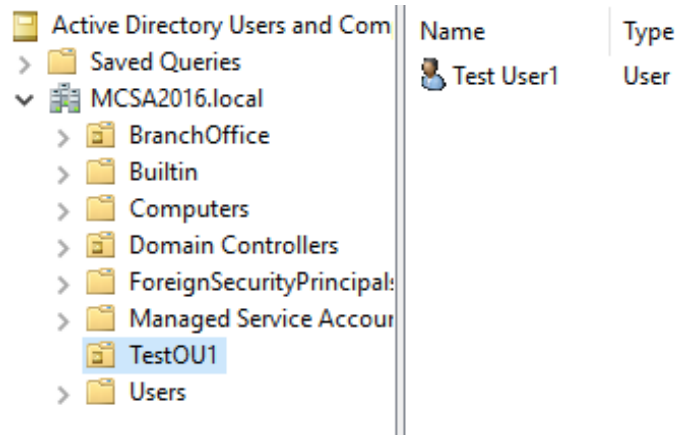
Activity	Requirements	Notes
Activity 6-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1, ServerSA1	
Activity 6-2: Installing an RODC with Staging	ServerDC1, ServerSA1	
Activity 6-3: Configuring the Password Replication Policy	ServerDC1, ServerSA1	
Activity 6-4: Creating a Subnet in Active Directory Sites and Services	ServerDC1	
Activity 6-5: Viewing Site Properties	ServerDC1	
Activity 6-6: Changing an RODC to a Standard DC	ServerDC1, ServerSA1	
Activity 6-7: Transferring FSMO Roles	ServerDC1, ServerSA1	
Activity 6-8: Creating a System State Backup	ServerDC1, ServerSA1	
Activity 6-9: Restoring Active Directory from a System State Backup	ServerDC1, ServerSA1	
Activity 6-10: Restoring Deleted Objects from the Active Directory Recycle Bin	ServerDC1, ServerSA1	
Activity 6-11: Compacting the Active Directory Database	ServerDC1, ServerSA1	

Activity 6-8: Creating a System State Backup

Time Required: 25 minutes or longer
Objective: Create a system state backup.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: In this activity, you create a system state backup, but first you need to install the Windows Server Backup tool. You will store backups on a separate volume from Windows, so you create a new volume on Disk 1 on ServerSA1 for this purpose. Then you create some objects in Active Directory and create the system state backup.

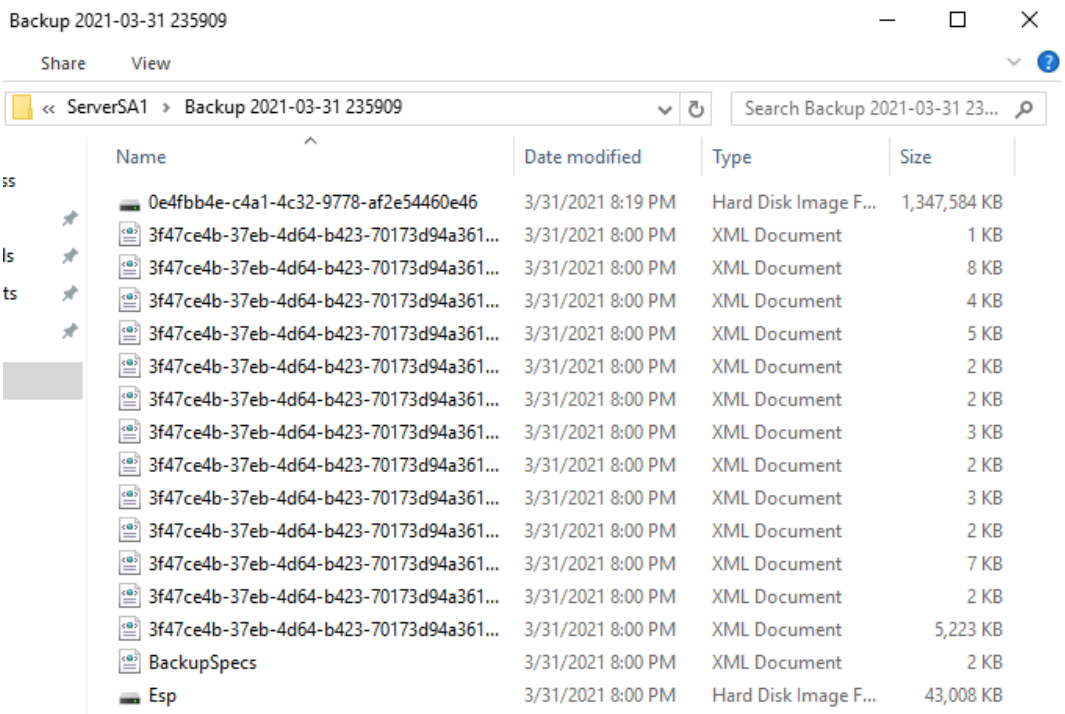
1. On ServerSA1, open Disk Management. Create a 15 GB NTFS volume named **Backup** and assign it drive letter **B** (the backup should take about 12 GB of space). Use the defaults for all other options. Close Disk Management.
2. Open Active Directory Users and Computers. First, you create some objects that you delete in a later activity to test the backup. Right-click the domain object, point to **New**, and click **Organizational Unit**. Type **TestOU1** in the Name text box. Click to clear the **Protect container from accidental deletion** check box. Click **OK**.
3. Create a user in TestOU1 with the full name **Test User1**, the logon name **testuser1**, and the password **Password01**. Set the password to never expire.
4. Open a PowerShell prompt. Type **Install-WindowsFeature Windows-Server-Backup** and press **Enter**.
5. Even though wbadmin isn't a PowerShell cmdlet, you can still run it from PowerShell. Type **wbadmin start systemstatebackup -backuptarget:B:** and press **Enter** to start a system state backup on the B drive.
6. When you're prompted to start the backup operation, type **y** and press **Enter**.
7. The backup must first identify all system state files, and you see progress displays as wbadmin finds the files. When the files have been found, the backup begins. (It might take several minutes.) Progress lines are displayed periodically to show the percentage complete. When the backup is finished, a log of files backed up successfully is created in the C:\Windows\Logs\WindowsServerBackup folder. Close the PowerShell window.
8. To view files in the backup, open File Explorer and navigate to **B:\WindowsImageBackup\ServerSA1**. You see a folder named Backup *DateAndTime* where the backup you created is stored. You also see a folder named Catalog that holds the files composing the catalog of backups.
9. Close File Explorer, but stay signed in for the next activity.

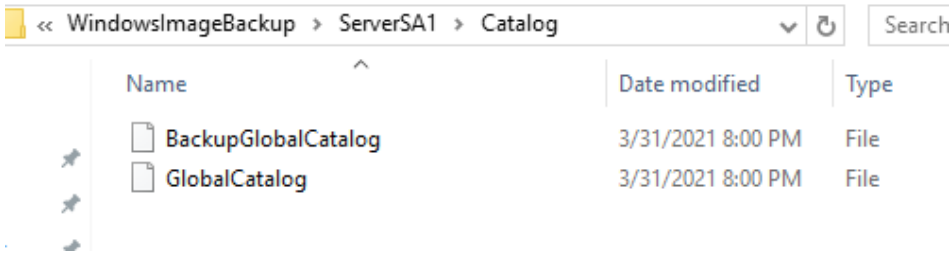





```
PS C:\Users\administrator.MCSA2016> Install-WindowsFeature Windows-Server-Backup

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Windows Server Backup}
```

```
Summary of the backup operation:
--------------------

The backup operation successfully completed.
The backup of the system state successfully completed [4/1/2021 5:56 PM].
Log of files successfully backed up:
C:\Windows\Logs\WindowsServerBackup\Backup-31-03-2021_23-59-09.log

PS C:\Users\administrator.MCSA2016> _
```





Activity 6-9: Restoring Active Directory from a System State Backup

Time Required: 30 minutes or longer
Objective: Restore Active Directory from a backup.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: In this activity, you delete an OU from Active Directory and then perform an authoritative restore on the deleted object.

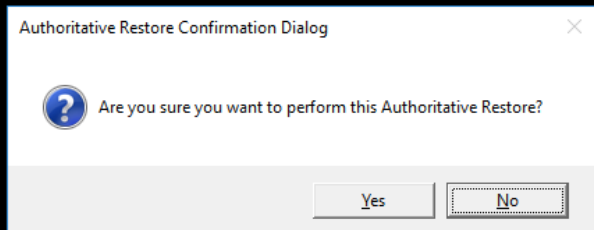
1. On ServerSA1, open Active Directory Users and Computers. Click **TestOU1** and press **Delete**. When prompted to confirm the deletion, click **Yes**.
2. In the Confirm Subtree Deletion message box, click the **Use Delete Subtree server control** check box so that protected objects can be deleted, and then click **Yes**.
3. Now, you'll restore the objects using the backup. To do so, you need to restart ServerSA1 in Directory Services repair mode. Right-click **Start**, click **Run**, type **msconfig**, and press **Enter** to start System Configuration.
4. Click the **Boot** tab. Click the **Safe boot** check box and click **Active Directory repair**. Click **OK**.
5. Click **Restart** to restart ServerSA1 in Safe Mode.
6. Sign in to ServerSA1 using the local administrator account and the DSRM password, which is **Password01**. It might take a while before you see the desktop. "Safe Mode" is displayed in the corners of the desktop.
7. Open a command prompt window. You must get a list of the available backups before you can restore the system state. Type **wbadmin get versions -backuptarget:B:** and press **Enter**. After a short wait, a list of backups is displayed. Make a note of the version identifier of the most recent backup, which is the system state backup you created in the previous activity.
8. To begin the recovery, type **wbadmin start systemstaterecovery -version:*Version* -backuptarget:B:** (replacing `Version` with the version identifier you noted in Step 7) and press **Enter**. When prompted to start the recovery operation, type **y** and press **Enter**. You see a warning about replicated content causing latency or outage issues and are prompted to continue. Type **y** and press **Enter**.
9. The restoration will probably take several minutes. When it's finished, you're prompted to restart. However, don't restart the server because you must first mark deleted objects as authoritative. The prompt doesn't give you the option to enter "n" to prevent a restart, so press **Ctrl+C** to quit `wbadmin`. If this server were the only writeable DC, the next step isn't necessary, but ServerDC1 is also writeable. With a nonauthoritative restore, you would simply restart the server to finish the restoration.
10. Type **ntdsutil** and press **Enter**. Type **activate instance ntds** and press **Enter** to make the Active Directory database the focus of the command. Type **authoritative restore** and press **Enter**. At the authoritative restore prompt, type **restore subtree ou=TestOU1,dc=mcsa2016,dc=local** and press **Enter**. When the Authoritative Restore Confirmation Dialog message box opens, click **Yes**. Type **quit** and press **Enter**, and then type **quit** again and press **Enter**. The `restore` command specifies the object to restore authoritatively. The rest of the Active Directory database is stored nonauthoritatively.
11. Change the boot setting so that ServerSA1 boots normally. Right-click **Start**, click **Run**, type **msconfig**, and press **Enter** to start System Configuration. Click the **Boot** tab. Click to clear the **Safe boot** check box. Click **OK**. Click **Restart** to restart the server.
12. Sign in to ServerSA1 as the domain administrator. The system state recovery performs some final tasks, opens a command prompt window, and displays a "Completed successfully" message. Press **Enter** to continue when prompted.
13. Open Active Directory Users and Computers and click **TestOU1** to verify that the objects have been restored.
14. Close Active Directory Users and Computers and continue to the next activity.

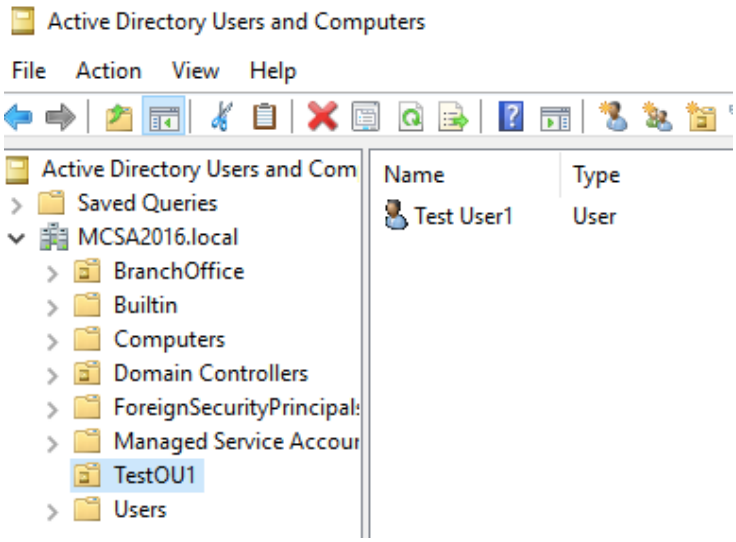
```
C:\Users\Administrator.SERVERSA1>wbadmin get versions -backuptarget:B:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Backup time: 3/31/2021 7:59 PM
Backup target: 1394/USB Disk labeled B:
Version identifier: 03/31/2021-23:59
Can recover: Volume(s), File(s), Application(s), System State
Snapshot ID: {8833f96e-5bba-4080-b9e2-15bc6d3764ac}


C:\Users\Administrator.SERVERSA1>wbadmin start systemstaterecovery -version:03/31/2021-23:59 -backuptarget:B:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Do you want to start the system state recovery operation?
[Y] Yes [N] No y

Note:  The recovery operation will cause all replicated content (replicated
using DFSR or FRS) on the local computer to resynchronize after recovery.
The rise in network traffic due to resynchronization may cause potential
latency or outage issues.
System state recovery cannot be paused or cancelled once it has started.
It will need a restart of the server to complete the recovery operation.

Do you want to continue ?
[Y] Yes [N] No y

Starting a system state recovery operation [4/1/2021 4:23 PM].
```

Safe Mode

```
The recovery of the system state successfully completed [4/1/2021 4:49 PM].
Log of files successfully recovered:
C:\Windows\Logs\WindowsServerBackup\SystemStateRestore-01-04-2021_20-23-52.log

Restart the server to complete the operation.
Note: Please wait while the system state recovery operation attempts to
recover system files. This might take several minutes to complete, depending
on how many files are getting replaced and the server restarts needed during
the process. Do not interrupt this process.

A computer restart is required to complete the system state recovery operation.
Press [Y] to restart the computer now.
[Y] Yes
```

```
C:\Users\Administrator.SERVERSA1.000>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: authoritative restore
authoritative restore: restore subtree ou=TestOU1, dc=mcsa2016, dc=local
Error parsing Input - Invalid Syntax.
authoritative restore: restore subtree ou=TestOU1,dc=mcsa2016,dc=local
```

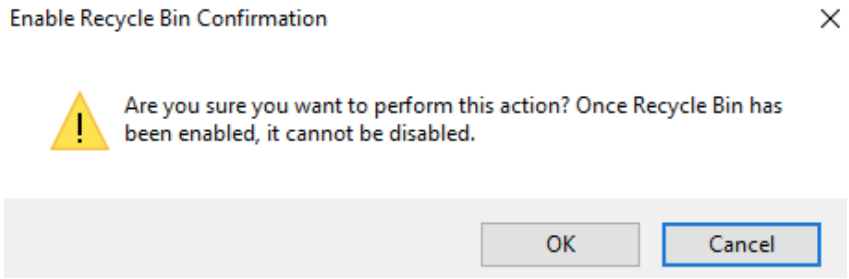


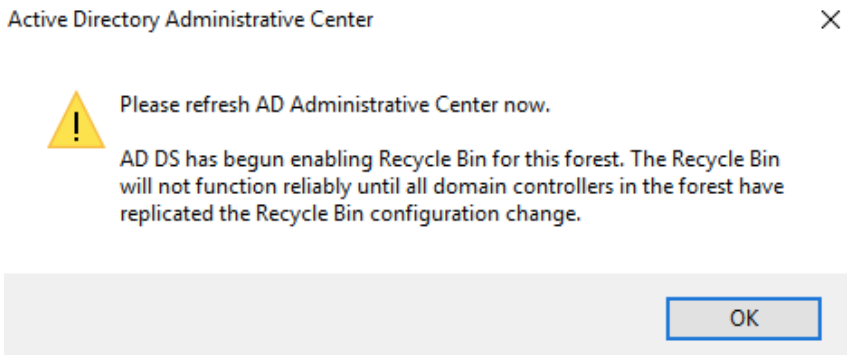


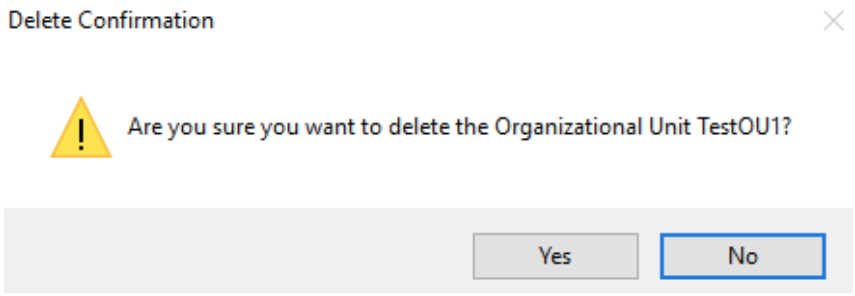
Activity 6-10: Restoring Deleted Objects from the Active Directory Recycle Bin

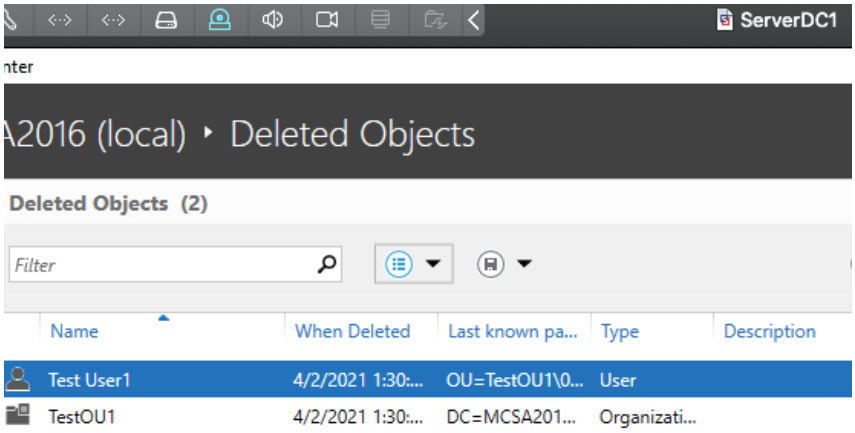
Time Required: 20 minutes
Objective: Restore deleted objects from the Active Directory Recycle Bin.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: You have seen that recovering deleted objects can involve quite a bit of time if the Active Directory Recycle Bin isn't enabled. To make the process easier, you enable and test this feature.

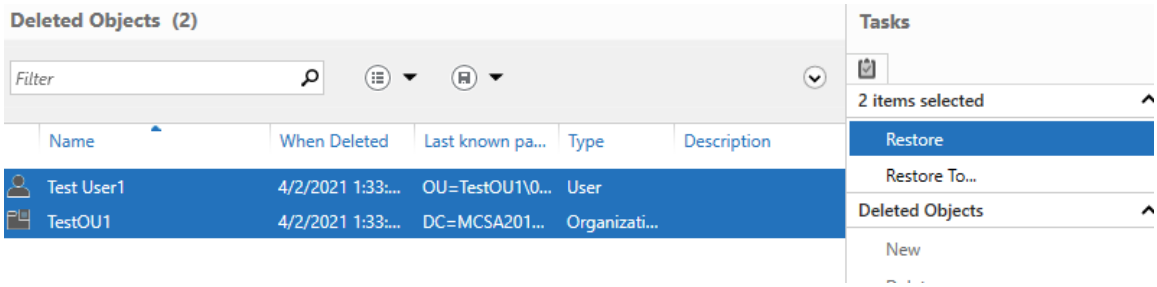
1. On ServerDC1, open Active Directory Administrative Center, and click **MCSA2016 (local)** in the left pane.
2. In the right pane, click **Enable Recycle Bin**. You see a message explaining that the Recycle Bin can't be disabled after it's enabled. Click **OK**. You see a message telling you to refresh the Active Directory Administrative Center now. Click **OK**.
3. Click the **Refresh** icon to refresh Active Directory Administrative Center. You see a new folder named Deleted Objects. Sign in to ServerSA1 as administrator, if necessary. Open Active Directory Administrative Center and click the domain object to verify that the Deleted Objects folder is there. If it is, the Recycle Bin is enabled on both DCs.
4. Now delete some objects. Right-click **TestOU1** and click **Delete**. Click **Yes** to confirm. Click **Use delete subtree server control** and click **Yes**.
5. On ServerDC1, refresh Active Directory Administrative Center and verify that **TestOU1** has been deleted. Double-click the **Deleted Objects** folder. You see TestOU1 and Test User1.
6. To restore both objects, click **Test User1**, hold down the **Ctrl** key, and click **TestOU1** so that both objects are highlighted and then release the **Ctrl** key. In the right pane, click **Restore**.
7. In the left pane, click **MCSA2016 (local)**. Double-click **TestOU1** and verify that Test User1 is also restored.
8. Next, you see how to restore an object with PowerShell. First you need a deleted object, so delete **Test User1** from TestOU1, but don't delete TestOU1 this time.
9. Open a PowerShell prompt. Type **Get-ADObject -Filter {DisplayName -eq "Test User1"} -IncludeDeletedObjects | Restore-ADObject** and press **Enter**.
10. Refresh Active Directory Administrative Center, and you'll see that Test User1 is restored.
11. Close the PowerShell window and Active Directory Administrative Center. Continue to the next activity.

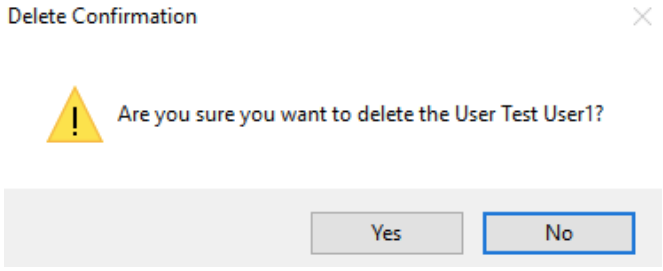




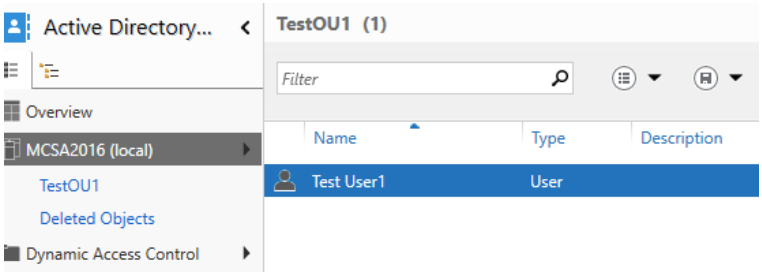









```
PS C:\Users\Administrator> Get-ADObject -Filter {DisplayName -eq "Test User1"} -IncludeDeletedObjects | Restore-ADObject
PS C:\Users\Administrator>
```



Activity 6-11: Compacting the Active Directory Databases

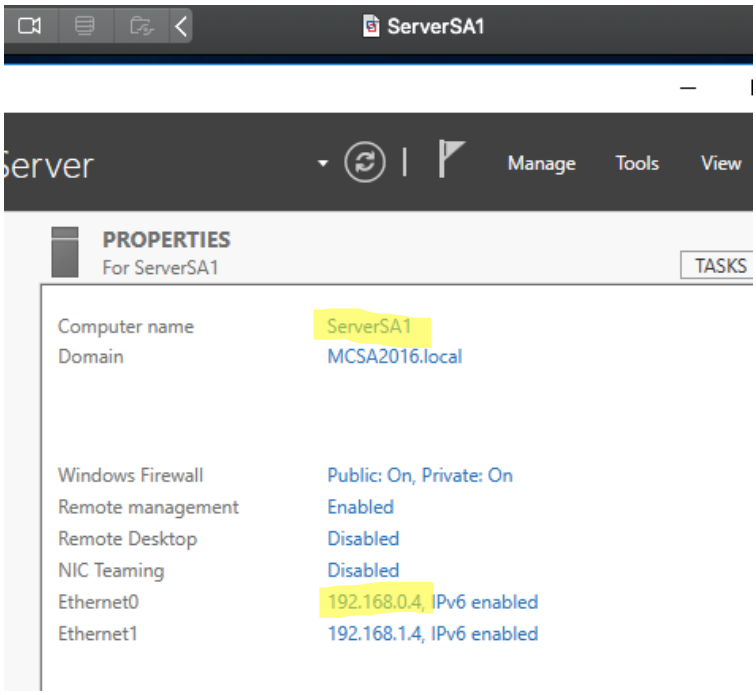
Time Required: 15 minutes
Objective: Compact the Active Directory database.
Required Tools and Equipment: ServerDC1, ServerSA1
Description: In this activity, you compact the Active Directory database. You create folders to hold temporary copies of the database, stop the Active Directory service, and then compact the database with one of the folders you created as the destination. First, you make a copy of the original database in case a problem occurs with compaction, and then you must delete the Active Directory log files and copy the compacted database to replace the original database.

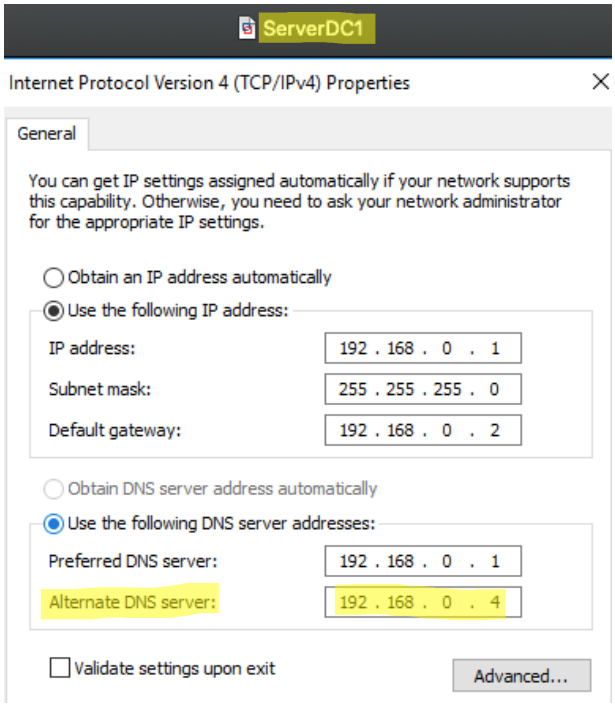
1. On ServerDC1, set the alternate DNS server address in the network connection IP address settings to the address of ServerSA1 (192.168.0.2). This step is done as a precaution. Because DNS doesn't respond to DNS queries while Active Directory is stopped, ServerDC1 might need to contact a DNS server if you have to sign in after Active Directory is stopped. This can happen, for example, if your screen saver comes on and requires a password to access the desktop. When you have finished changing the alternate DNS server address, close any open dialog boxes.
2. Create two folders in the root of the C drive: **tempAD** and **backupAD**.
3. Open a command prompt window. Type **net stop ntds** and press **Enter** to stop the Active Directory service. When prompted to continue, type **y** and press **Enter**.
4. Type the following commands, pressing **Enter** after each one (see Figure 6-18):
   ntdsutil, activate instance ntds
   files
   compact to c:\tempAD

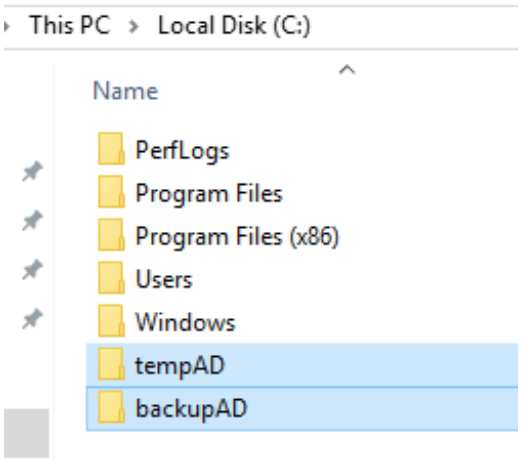
```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: compact to c:\tempAD
Initiating DEFRAGMENTATION mode...
     Source Database: C:\Windows\NTDS\ntds.dit
     Target Database: c:\tempAD\ntds.dit

                Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compaction is successful. You need to:
   copy "c:\tempAD\ntds.dit" "C:\Windows\NTDS\ntds.dit"
and delete the old log files:
   del C:\Windows\NTDS\*.log


file maintenance:
```

Figure 6-18 Compacting the database with `ntdsutil`

5. The Defragmentation Status display shows the progress of compaction. When you see a message stating that you need to copy the new file over the old file and delete the log files, type **quit** and press **Enter**, and then type **quit** and press **Enter** again.
6. To copy the original database file to the backup folder you created, type **copy c:\windows\ntds\ntds.dit c:\backupAD** and press **Enter**.
7. To delete the log files, type **del c:\windows\ntds*.log** and press **Enter**.
8. To copy the compacted database over the original database, type **copy c:\tempAD\ntds.dit c:\windows\ntds\ntds.dit** and press **Enter**. Type **y** and press **Enter** to confirm the copy.
9. Next, to verify the integrity of the new database, type the following commands, pressing **Enter** after each one:
   ntdsutil
   activate instance ntds
   files
   integrity
10. Assuming the integrity check was successful, type **quit** and press **Enter**. If it wasn't successful, copy the backup from C:\backupAD to C:\Windows\Ntds, and attempt the compaction process again, starting with Step 4.
11. To check the semantic database integrity (which is recommended), type **semantic database analysis** and press **Enter**, then type **go fixup**, and press **Enter**. Type **quit** and press **Enter**, and then type **quit** and press **Enter** again.
12. To restart Active Directory, type **net start ntds** and press **Enter**. You can verify a successful startup by checking the most recent events in the event log. Shortly after the service starts, a new event with ID 1000 should be created in the Directory Service log under Applications and Services Logs in Event Viewer, indicating a successful Active Directory start.
13. Close all open windows, and shut down both servers.


ServerSA1
Server
Manage
Tools
View
PROPERTIES
For ServerSA1
TASKS
Computer name
ServerSA1
Domain
MCSA2016.local
Windows Firewall
Public: On, Private: On
Remote management
Enabled
Remote Desktop
Disabled
NIC Teaming
Disabled
Ethernet0
192.168.0.4, IPv6 enabled
Ethernet1
192.168.1.4, IPv6 enabled


ServerDC1
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 1
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 0 . 2
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
192 . 168 . 0 . 1
Alternate DNS server:
192 . 168 . 0 . 4
Validate settings upon exit
Advanced...




```
C:\Users\Administrator>net stop ntds
The following services are dependent on the Active Directory Domain Services service.
Stopping the Active Directory Domain Services service will also stop these services.

   Kerberos Key Distribution Center
   Intersite Messaging
   DNS Server
   DFS Replication

Do you want to continue this operation? (Y/N) [N]: y
.
The Kerberos Key Distribution Center service was stopped successfully.

The Intersite Messaging service is stopping.
The Intersite Messaging service was stopped successfully.

The DNS Server service is stopping.
The DNS Server service was stopped successfully.

.
The DFS Replication service was stopped successfully.

The Active Directory Domain Services service is stopping.
The Active Directory Domain Services service was stopped successfully.
```

```
C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: compact to c:\tempAD
Initiating DEFRAGMENTATION mode...
     Source Database: C:\Windows\NTDS\ntds.dit
     Target Database: c:\tempAD\ntds.dit

                 Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compaction is successful. You need to:
   copy "c:\tempAD\ntds.dit" "C:\Windows\NTDS\ntds.dit"
and delete the old log files:
   del C:\Windows\NTDS\*.log
```

```
C:\Users\Administrator>copy c:\windows\NTDS\ntds.dit c:\backupAD
       1 file(s) copied.

C:\Users\Administrator>del c:\Windows\NTDS\*.log

C:\Users\Administrator>copy c:\tempAD\ntds.dit c:\Windows\NTDS\ntds.dit
Overwrite c:\Windows\NTDS\ntds.dit? (Yes/No/All): y
       1 file(s) copied.

C:\Users\Administrator>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: integrity
Doing Integrity Check for db: C:\Windows\NTDS\ntds.dit.

Checking database integrity.

                    Scanning  Status (% complete)

         0    10   20   30   40   50   60   70   80   90  100
         |----|----|----|----|----|----|----|----|----|----|
         ..................................................


Integrity check successful.

It is recommended you run semantic database analysis
to ensure semantic database consistency as well.
```

```
ntdsutil: semantic database analysis
semantic checker: go fixup
Fixup mode is turned on

Opening DIT database... Done.

Done.

......Done.


Writing summary into log file dsdit.dmp.0
SDs scanned:            118
Records scanned:       3958
Processing records..Done. Elapsed time 1 seconds.

semantic checker: quit
ntdsutil: quit

C:\Users\Administrator>net start ntds
The Active Directory Domain Services service is starting.
The Active Directory Domain Services service was started successfully.
```