Lab 17

Maintaining Active directory

This lab contains the following exercises and activities:

|  |  |
| --- | --- |
| Exercise 17.1 | Backing Up System State |
| Exercise 17.2 | Restoring the System State |
| Exercise 17.3 | Using an Active Directory Snapshot |
| Exercise 17.4 | Restoring a Deleted Object Using the Active Directory Recycle Bin |
| Exercise 17.5 | Managing the Active Directory Database |
| Lab Challenge | Removing Server02 from Active Directory |

BEFORE YOU BEGIN

The lab environment consists of student workstations connected to a local area network, along with a server that functions as the domain controller for a domain called *contoso.com*. The computers required for this lab are listed in Table 17-1.

Table 17-1

Computers Required for Lab 17

|  |  |  |
| --- | --- | --- |
| Computer | Operating System | Computer Name |
| Server (VM 1) | Windows Server 2012 | RWDC01 |
| Server (VM 2) | Windows Server 2012 | Server01 |
| Server (VM 3) | Windows Server 2012 | Server02 |

In addition to the computers, you also require the software listed in Table 17-2 to complete Lab 17.

Table 17-2

Software Required for Lab 17

|  |  |
| --- | --- |
| Software | Location |
| Lab 17 student worksheet | Lab17\_worksheet.rtf (provided by instructor) |

Working with Lab Worksheets

Each lab in this manual requires that you answer questions, take screen shots, and perform other activities that you will document in a worksheet named for the lab, such as Lab17\_worksheet.rtf. You will find these worksheets on the book companion site. It is recommended that you use a USB flash drive to store your worksheets, so you can submit them to your instructor for review. As you perform the exercises in each lab, open the appropriate worksheet file using WordPad, fill in the required information, and save the file to your flash drive.

After completing this lab, you will be able to:

* Back up the System State including Active Directory
* Perform an Active Directory restore
* Configure Active Directory snapshots
* Restore a Deleted Object using the Active Directory Recycle Bin
* Perform Active Directory maintenance

Estimated lab time: 130 minutes

|  |  |
| --- | --- |
| Exercise 17.1 | Backing Up System State |
| Overview | As a system administrator, it is important to have good backups. Therefore, during this exercise, you use Windows Server Backup to back up the system state of Server01, which includes the Active Directory. |
| Completion time | 30 minutes |

**Mindset Question: What is the system state and how does it relate to Active Directory?**

# Installing Windows Server Backup

|  |  |
| --- | --- |
| Question 1 | What is the best method for disaster recovery? |

**1.** Log in to Server01 as the **Contoso\administrator** using the password of **Password01** and **restart** the Virtual Machine. When Server01 restarts, log in as **Contoso\administrator** using the password of **Password01**. The Server Manager console opens.

**2.** On Server Manager, click Manage and click Add Roles and Features.

**3.** When the Add Roles and Features Wizard starts, click Next.

**4.** On the Select installation type page, click Next.

**5.** On the Select destination server page, click Next.

**6.** On the Select server roles page, click Next.

**7.** On the Select features page, click to select the Windows Server Backup and click Next.

**8.** On the Confirm installation selections page, click Install.

**9.** When the installation is complete, click Close.

# Performing a Back Up of the System State

1. Log in to RWDC01 as the **Contoso\Administrator** user account. The Server Manager console opens.
2. On RWDC01, open File Explorer and create a **C:\BAK** folder.
3. Right-click the BAK folder and click Properties.
4. When the Properties dialog box opens, click the Sharing tab.
5. Click Advanced Sharing.
6. When the Advanced Sharing dialog box opens, click Share this folder. Click Permissions. Click to select the Allow Change permission for Everyone. Click OK to close the Permissions for BAK dialog box. Click OK to close the Advanced Sharing dialog box.
7. Click Close to close the Properties dialog box.
8. Restart Server01 and Log in as the **Contoso\administrator** user account, using the password of **Password01**.
9. On Server Manager, click Tools > Windows Server Backup. The Windows Server Backup console opens.
10. Click Local Backup in the left pane.
11. Under Actions, click Backup Once.
12. When the Backup Once Wizard starts, click Different Options and click Next.
13. On the Select Backup Configuration page, click Custom and click Next.
14. On the Select Items for Backup page, click Add Items. The Select Items dialog box opens as shown in Figure 17-1.

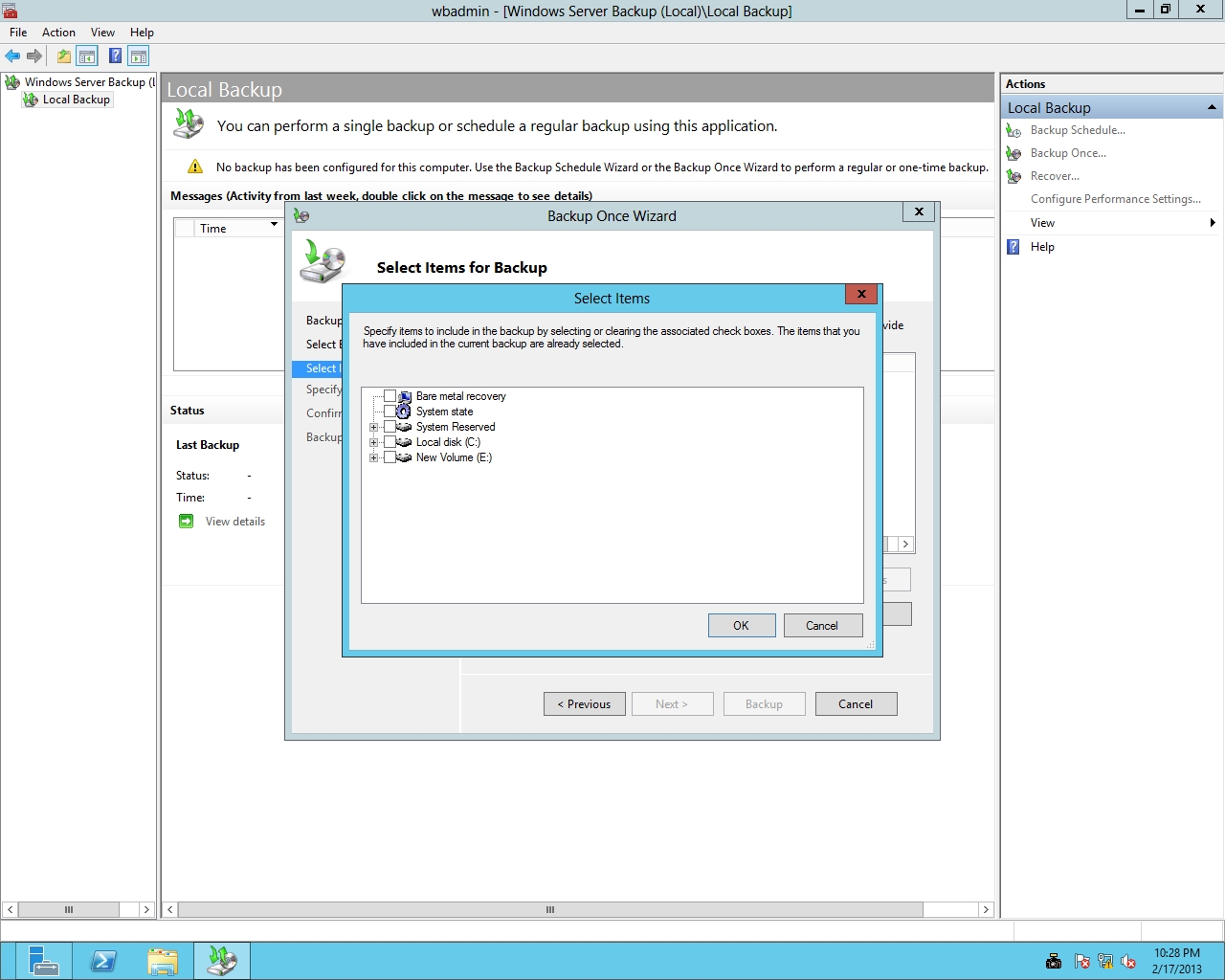


Figure 17-1

Selecting items for backup

1. Select System state and click OK.
2. On the Select Items for Backup page, click Next.
3. On the Specify Destination Type page, select Remote shared folder. Click Next.
4. On the Specify Remote Folder page, type **\\RWDC01\BAK** and click Next.
5. On the Confirmation page, click Backup. The backups will take a few minutes.
6. When the backup is completed, take a screen shot of the Backup Once Wizard window by pressing Alt+Prt Scr and then paste it into your Lab17\_worksheet file in the page provided by pressing Ctrl+V.
7. Click Close.

End of exercise. You can leave the windows open for the next exercise.

|  |  |  |
| --- | --- | --- |
| Exercise 17.2 | | Restoring the System State |
| Overview | In the previous exercise, you performed a backup. During this exercise, you perform a restore of the system state. However, before you perform the final reboot, you make an OU as authoritative so that the OU will not be overwritten by other domain controllers. | |
| Completion time | 30 minutes | |

**Mindset Question: When you need to restore Active Directory, what are the two types of restores and how do they differ?**

**1.** On a physical server, you would normally press F8 during reboot. However, because you are running on a virtual environment on Server01, right-click Start, select Run, and then enter msconfig.exe, opening System Configuration. Click the Boot tab, click to select Safe boot, and select Active Directory repair. Click OK. Then restart the computer.

**2.** Log in as the local administrator (DSRM), **Server01\Administrator**, using the password of **Password01**.

**3.** On Server01, using Server Manager, click Tools > Windows Server Backup. The Windows Server Backup console opens.

**4.** Click Local Backup. Under Actions, click Recover.

**5.** When the Recovery Wizard starts, select *A backup stored on another location* and click Next.

**6.** On the Specify Location Type page, click Remote shared folder and click Next.

**7.** On the Specify Remote Folder page, type **\\RWDC01\BAK** and click Next.

**8.** On the Select Backup Date page, select today’s date of the backup that you want to restore from and click Next.

**9.** On the Select Recovery Type page, click System state. Click Next.

**10.** On the Select Location for System State Recovery page, you do not have to select Perform an authoritative restore of Active Directory files. Instead use the ntdsutil command to specify what is authoritative. Click Next.

**11.** When the warning appears that this recovery option will cause all replicated content on the local server to re-synchronize after recovery, click OK.

**12.** When you are prompted to continue, click OK.

**13.** On the Confirmation page, select Automatically reboot the sever to complete the recovery process. Click Recover.

**14.** When you are prompted to continue again, click Yes. The restore will take some time.

**15.** When Server01 reboots, log in to as the local administrator (DSRM), **Server01\Administrator**, using the password **Password01**.

**16.** When a cmd.exe window opens, indicating that the restore was complete, press the Enter key.

**17.** Right-click the Start Menu button and select Command Prompt (Admin). The command prompt window opens.

**18.** Execute the ntdsutil command.

**19.** From the ntdsutil prompt, execute the flowing command:

activate instance NTDS

**20.** At the ntdsutil prompt, execute the following command:

authoritative restore

**21.** To mark the Service Accounts OU to be restored with an authoritative restore, execute the following command:

restore subtree “OU=Service Accounts,DC=contoso,DC=com”

**22.** When the Authoritative Restore Confirmation dialog box opens, click Yes to perform the authoritative restore. When the record or records have been updated, the names of the back-link files are displayed.

**23.** Take a screen shot of the ntdsutil Command Prompt window by pressing Alt+Prt Scr and then paste it into your Lab17\_worksheet file in the page provided by pressing Ctrl+V.

**24.** Execute the quit command twice to get back to the command prompt.

**25.** Open System Configuration by executing msconfig.exe. Click the Boot tab, deselect the Safe boot option, and click OK. When it asks you to restart, click Restart.

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 17.3 | Using an Active Directory Snapshot |
| Overview | In this exercise, you create a snapshot of Active Directory. You then mount and access the snapshot. |
| Completion time | 20 minutes |

**Mindset Question: Active Directory has the ability to create snapshots. How can snapshots be used and what are their limits?**

**1.** Log in to Server01 as the **Contoso\Administrator** user account. The Server Manager console opens.

**2.** Right-click the Start button and select Command Prompt (Admin). The command prompt window opens.

**3.** At the command prompt, execute the ntdsutil command.

**4.** At the ntdsutil prompt, execute the snapshot command.

**5.** At the snapshot prompt, execute the activate instance ntds command.

**6.** Execute the create command.

|  |  |
| --- | --- |
| Question 2 | What is the Guid (without the braces ({})) of the snapshot created? |

**7.** To return a list of all snapshots, at the snapshot prompt, execute the list all command.

**8.** Execute the mount {GUID} command, where GUID is the one that you recorded.

**9.** Take a screen shot of the ntdsutil Command Prompt window by pressing Alt+Prt Scr and then paste it into your Lab17\_worksheet file in the page provided by pressing Ctrl+V.

**10.** Execute the quit command twice to exit ntdsutil.

**11.** To mount the snapshot, execute the following command:

dsamain -dbpath c:\$snap\_datetime\_volumec$\windows\ntds\ntds.dit

-ldapport 5000

You need to specify the date-time when you performed the mount command. The port number, 5000, can be any open and unique TCP port number (see Figure 17-2).

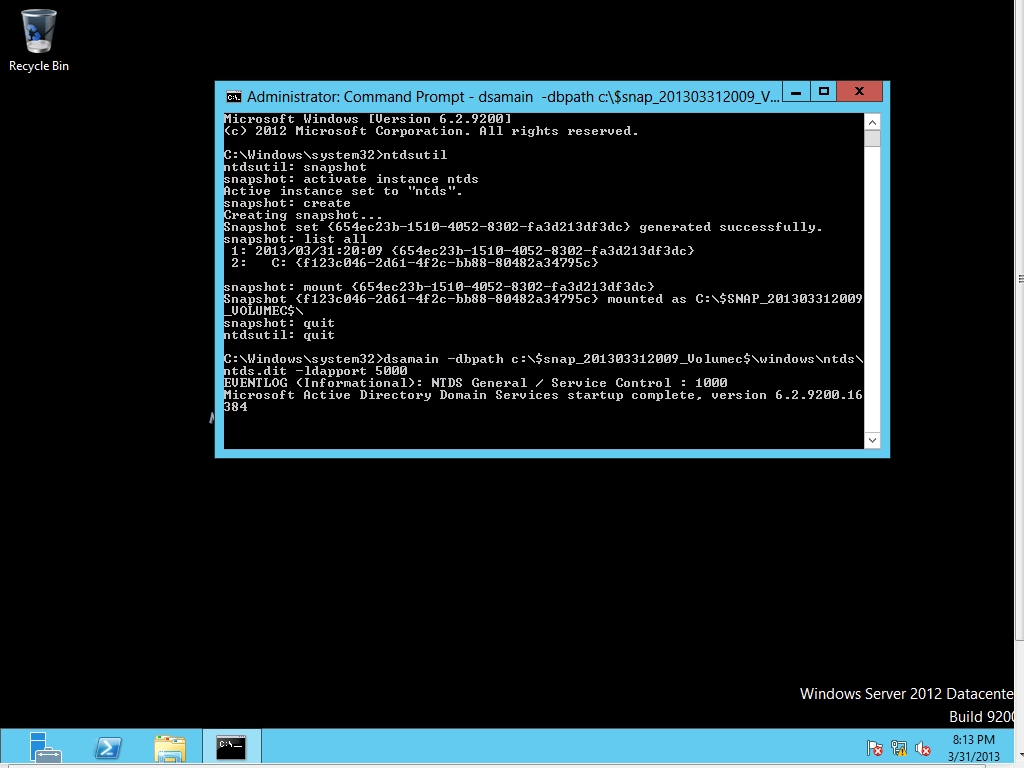


Figure 17-2

Mounting a snapshot

**12.** A message indicates that Active Directory Domain Services startup is complete. Do not close the command prompt window and leave the command you just ran, dsamain.exe, running while you continue to the next step.

**13.** Using Server Manager, click Tools > Active Directory Users and Computers. The Active Directory Users and Computers console opens.

**14.** Right-click the contoso.com, and then click Change Domain Controller. The Change Directory Server dialog box appears.

**15.** Click <Type a Directory Server name[:port] here>, type **Server01.contoso.com:5000**, and press Enter.

**16.** Click OK. You are now viewing the users and computers that are stored in the snapshot.

**17.** Switch to the command prompt in which the snapshot is mounted.

**18.** Press Ctrl+C to stop DSAMain.exe.

**19.** Execute the ntdsutil command.

**20.** Execute the activate instance ntds command.

**21.** Execute the snapshot command.

**22.** Type **unmount <GUID>**, where GUID is the GUID of the snapshot, and then press Enter.

**23.** Execute the list all command.

**24.** Because the snapshot is the first entry in the list, execute the following command:

delete 1

**25.** Execute the quit command twice.

**26.** Take a screen shot of the ntdsutil Command Prompt window by pressing Alt+Prt Scr and then paste it into your Lab17\_worksheet file in the page provided by pressing Ctrl+V.

**27.** Close the command prompt window and the Active Directory Users and Computers console.

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 17.4 | Restoring a Deleted Object Using the Recycle Bin |
| Overview | During this exercise, you activate the Active Directory Recycle Bin. You then delete an object and restore the object from the Recycle Bin. |
| Completion time | 10 minutes |

**Mindset Question: Explain how the Active Directory Recycle Bin works.**

**1.** On RWDC01, using Server Manager, click Tools > Active Directory Administrative Center. The Active Directory Administrative Center opens.

**2.** Click contoso (local), as shown in Figure 17-3.

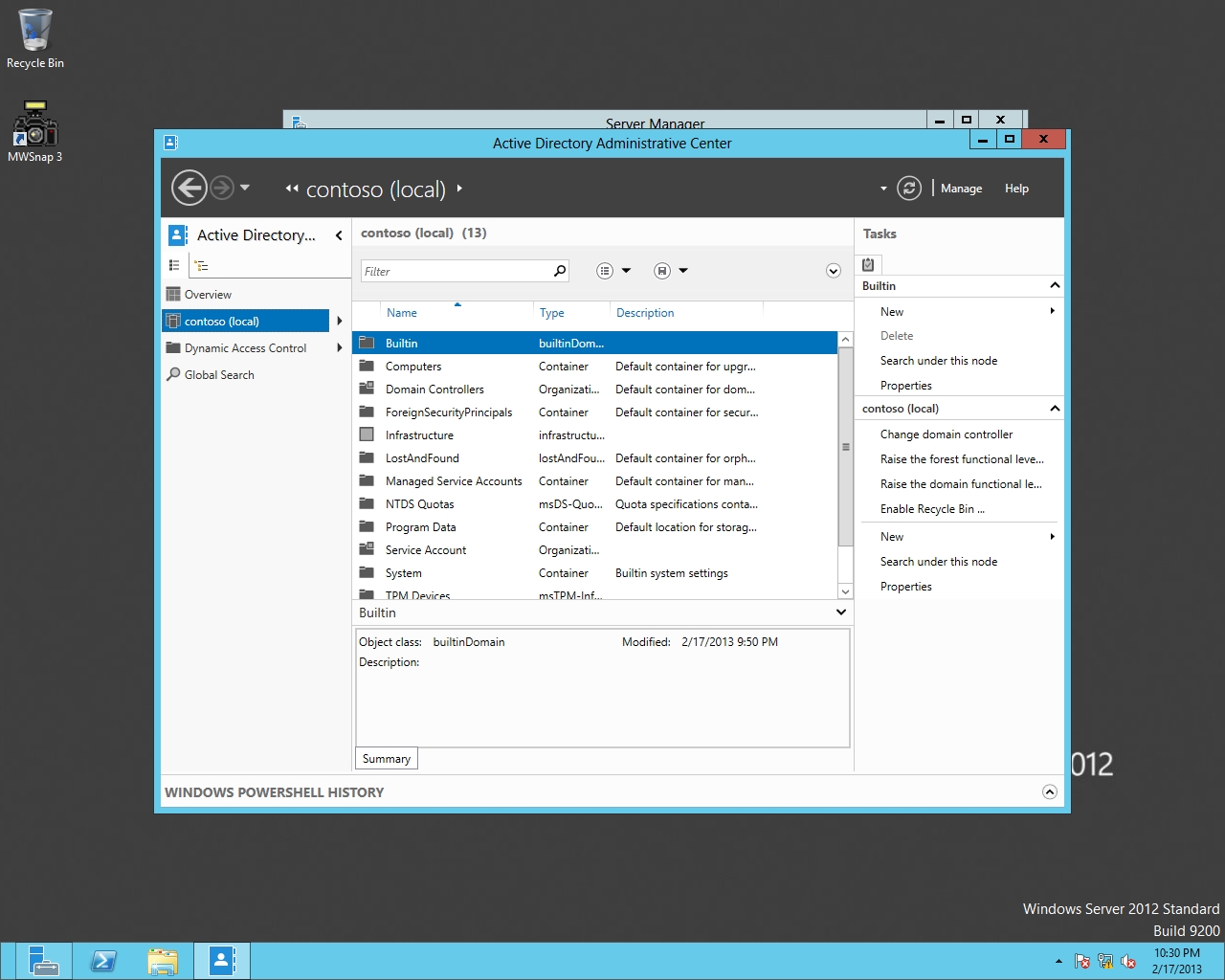


Figure 17-3

Managing the contoso domain with Active Directory Administrator Center

**3.** In the right pane, click Enable Recycle Bin. When it says that once the Recycle Bin has been enabled, it cannot be disabled and asks if you want to continue, click OK.

**4.** When is says to refresh the AD Administrative Center now, click OK.

**5.** Press the F5 key on the keyboard to refresh the Active Directory Administrative Center.

**6.** Using Server Manager, open Active Directory Users and Computers.

**7.** Expand contoso.com and click Service Accounts.

**8.** Delete the App1Service account. Click Yes to continue.

**9.** Close Active Directory Users and Computers.

**10.** Go back to the Active Directory Administrative Center.

**11.** Click the small arrow next to the domain and select Deleted Objects. If the App1Service account does not show in the Deleted Objects folder, press the F5 key to refresh.

**12.** Take a screen shot of the Active Directory Administrative Center window by pressing Alt+Prt Scr and then paste it into your Lab17\_worksheet file in the page provided by pressing Ctrl+V.

**13.** Right-click App1Service and click Restore.

**14.** Close Active Directory Administrative Center.

|  |  |
| --- | --- |
| Question 3 | What other method could used to activate the Active Directory Recycle Bin? |

**15.** Confirm that the App1Service account has been restored to Service Accounts OU.

End of exercise. You can leave the windows open for the next exercise.

|  |  |
| --- | --- |
| Exercise 17.5 | Managing the Active Directory Database |
| Overview | From time to time, you should perform maintenance on the Active Directory Database. Therefore, during this exercise, you compact the database and perform an integrity check on the database. |
| Completion time | 20 minutes |

**Mindset Question: Why does maintenance have to be done on Active Directory?**

**1.** On Server01, using Server Manager, click Tools > Services. The Services console opens.

**2.** Right-click the Active Directory Domain Services service and click Stop. When it asks if you want to stop other services, click Yes.

**3.** Right-click the Start button and select Command Prompt (Admin). The command prompt window opens.

**4.** Execute the ntdsutil command.

**5.** At the ntdsutil prompt, execute the activate instance NTDS command.

**6.** Execute the files command.

**7.** At the file maintenance prompt, execute the compact to C:\ command. The database is compacted.

**8.** Take a screen shot of the ntdsutil Command Prompt window by pressing Alt+Prt Scr and then paste it into your Lab17\_worksheet file in the page provided by pressing Ctrl+V.

**9.** To check the integrity of the offline database, execute the integrity command.

**10.** At the file maintenance prompt, execute the quit command.

**11.** To perform a semantic database consistency check, execute the semantic database analysis command.

**12.** At the semantic checker prompt, execute the go command.

**13.** Execute the quit command twice.

**14.** Copy the ntds.dit file from the C:\ folder to the C:\Windows\NTDS folder.

**15.** Close the command prompt.

**16.** Go back to the Services console. Right-click the Active Directory Domain Services service and click Start.

**17.** Close the Services console.

Lab REview Questions

|  |  |
| --- | --- |
| **Completion time** | **10 minutes** |

**1.** In Exercise 17.1, what did you use to back up the System State?

**2.** In Exercise 17.2, what type of restore will have changes overwritten by the current Active Directory?

**3.** In Exercise 17.2, when you restore from backup and you want to make sure that the restored objects in Active Directory do not get removed automatically by Active Directory because they were deleted in the past, what type of of restore must be done?

**4.** In Exercise 17.2, what tool allowed you to choose selected objects as authoritative restore?

**5.** In Exercise 17.3, what command did you use to create the Active Directory snapshot?

**6.** In Exercise 17.4, what did you use to enable the Active Directory Recycle Bin?

**7.** In Exercise 17.5, what program allowed you to compress the Active Directory database?

|  |  |
| --- | --- |
| Lab Challenge | Remove Server02 from Active Directory |
| Overview | To complete this challenge, you will remove a domain controller from Active Directory. |
| Completion time | 10 minutes |

In Hyper V, you decide to shut down Server02 because it has been giving you problems that you cannot recover from. Assuming the Server02 is not available, how would you remove Server02 from Active Directory?

Write out the steps you performed to complete the challenge.

End of lab. You can log off or start a different lab. If you want to restart this lab, you’ll need to click the End Lab button in order for the lab to be reset.