Module 13: Monitoring, managing, and recovering AD DS

Lab: Recovering objects in AD DS

(VMs: 20742B-LON-DC1)

Exercise 1: Backing up and restoring AD DS

Task 1: Install the Windows Server Backup feature

1. Switch to **LON-DC1**.
2. In **Server Manager**, click **Manage**, and then click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, on the **Before you begin page**, 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, in the **Features** list, select the **Windows Server Backup** check box, and then click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When the installation finishes, click **Close**.
10. Click **Start**, type ***cmd*** and then press Enter.
11. In the **Command Prompt** window, type the following, and then press Enter.

cacls C:\Windows\System32\InputMethod\CHS\chsime.exe /E /P system:R

Note: *This command is only required for the lab environment, and is not part of typical backup procedures.*

12. Close the **Command Prompt** window.

Task 2: Create a scheduled backup

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Windows Server Backup**.
2. In Windows Server Backup, click **Local Backup**, and then click **Backup Schedule**.
3. In the **Backup Schedule Wizard**, on the **Getting Started** page, click **Next**.
4. On the **Select Backup Configuration** page, click **Custom**, and then click **Next**.
5. On the **Select Items for Backup** page, click **Add Items**.
6. In the **Select Items** dialog box, select **Bare metal recovery**, click **OK**, and then click **Next**.
7. On the **Specify Backup Time** page, click **Once a day**.

8. In the **Select time of day** list, select **12:00 am**, and then click **Next**.
9. On the **Specify Destination Type** page, click **Back up to a hard disk that is dedicated for backups (recommended)**, and then click **Next**.
10. On the **Select Destination Disk** page, click **Show All Available Disks**.
11. In the **Show All Available Disks** dialog box, select the **Disk 1** check box, and then click **OK**.
12. On the **Select Destination Disk** page, select the **Disk 1** check box, and then click **Next**.
13. When the **Windows Server Backup** dialog box appears, informing you that all data on the disk will be deleted, click **Yes** to continue.

Note: *You will cancel the process in the next step to avoid formatting drive E.*

14. On the **Confirmation** page, click **Cancel** to avoid formatting drive E.

Task 3: Perform an interactive backup

1. In the **Actions** pane, click **Backup Once**.
2. On the **Backup Options** page, ensure that **Different options** is selected, and then click **Next**.
3. On the **Select Backup Configuration** page, click **Custom**, and then click **Next**.
4. On the **Select Items for Backup** page, click **Add Items**.
5. In the **Select Items** dialog box, click **System state**, and then click **OK**.
6. Click **Advanced Settings**, and then click the **VSS Settings** tab.
7. Click **VSS full Backup**, click **OK**, and then click **Next**.
8. On the **Specify Destination Type** page, click **Next**.
9. On the **Select Backup Destination** page, click **Next**.
10. On the **Confirmation** page, click **Backup**, and then click **Close**.

Note: *The backup will take about 10–15 minutes to complete. After the backup completes, close Windows Server Backup.*

Task 4: Delete an OU

Note: *Wait until the backup completes before proceeding.*

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. On the **Menu** bar, click **View**, and then click **Advanced Features**.
3. In the console tree, expand **Adatum.com**, and then click the **Research**

organizational unit (OU).
4. Right-click **Research**, and then click **Properties**.
5. In the **Research Properties** dialog box, on the **Object** tab, clear the **Protect object from accidental deletion** check box, and then click **OK**.
6. In the navigation pane, right-click **Research**, and then click **Delete**.
7. When a confirmation message appears, click **Yes**.
8. When a warning message appears, click **Yes**.
9. Wait for the deletion to complete.
10. Verify that the Research OU was deleted.

Task 5: Restart in Directory Services Restore Mode (DSRM)

1. On **LON-DC1**, click **Start**, right-click **Windows PowerShell**, and then click **Run as Administrator**.
2. In the Windows PowerShell command-line interface, at the command prompt, type the following command, and then press Enter:

bcdedit /set safeboot dsrepair

3. At the command prompt, type the following command, and then press Enter:

shutdown /t 0 /r

Task 6: Restore System state data

1. Sign in to **LON-DC1** as **Administrator** with the password **Pa55w.rd**.
2. Click **Start**, right-click **Windows PowerShell**, click **More**, and then click **Run as Administrator**.
3. At the **Windows PowerShell** command prompt, type the following command, and then press Enter:

wbadmin get versions -backuptarget:E: -machine:LON-DC1

Note the version identifier that the command returns.
4. At the command prompt, type the following command, where *version* is the number that you recorded in the previous step, and then press Enter:

wbadmin start systemstaterecovery -version:<version> -backuptarget:E: -machine:LONDC1

For example: ***wbadmin start systemstaterecovery -version:01/22/2011-10:37 -backuptarget:E: -machine:LON-DC1***

5. Type ***Y***, and then press Enter.
6. Type ***Y***, and then press Enter.

Note: *The restoration will take about 30–35 minutes. Depending on the host machine, it could take up to an hour.*

7. When prompted to restart, type ***Y***, and then press Enter.

Task 7: Mark restored information as authoritative

1. Sign in to **LON-DC1** as **Administrator** with the password **Pa55w.rd**.
2. When prompted, press Enter.
3. Click **Start**, right-click **Windows PowerShell**, point to **More** and then click **Run as administrator**.
4. At the Windows PowerShell command prompt, type the following command, and then press Enter: ***NtdsUtil.exe***
5. At the command prompt, type the following command, and then press Enter: ***activate instance ntds***
6. At the command prompt, type the following command, and then press Enter: ***authoritative restore***
7. At the command prompt, type the following command, and then press Enter: ***restore subtree "ou=Research,dc=adatum,dc=com"***
8. In the confirmation dialog message box that displays, click **Yes**.
9. Type ***quit***, and then press Enter.
10. Type ***quit***, and then press Enter.
11. At the command prompt, type the following command, and then press Enter: ***bcdedit /deletevalue safeboot***
12. At the command prompt, type the following command, and then press Enter: ***shutdown /t 0 /r***

Task 8: Verify that the data has been restored

1. Wait for **LON-DC1** to restart.
2. Sign in to **LON-DC1** as **Adatum\Administrator** with the password **Pa55w.rd**.
3. In **Server Manager**, from the **Tools** menu, click **Active Directory Users and Computers**.
4. In the console tree, expand **Adatum.com**, and then verify that the **Research** OU is restored. Note that you might have to force a site replication in Active Directory Sites and Services to see the change immediately.

***Results**: After completing this exercise, you should have successfully performed an interactive backup and an authoritative restore of Active Directory Domain System (AD DS).*

Exercise 2: Recovering objects in AD DS

Task 1: Verify requirements for Active Directory Recycle Bin

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Domains and Trusts**.
2. In the **Active Directory Domains and Trusts** console, right-click **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.
3. Confirm that the value of **Current forest functional level** is **Windows Server 2012 R2**, and then click **Cancel**.
4. Close the **Active Directory Domains and Trust** console.

Task 2: Enable the Active Directory Recycle Bin feature

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Module for Windows PowerShell**.
2. At the command prompt, type the following command, and then press Enter:

Enable-ADOptionalFeature –Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=adatum,DC=com' –Scope ForestOrConfigurationSet –Target 'adatum.com'

3. Type ***Y***, and then press Enter.
4. After the command prompt is returned to you, close the **Windows PowerShell** window.

Task 3: Delete objects to simulate accidental deletion

1. In **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. Navigate to the **Sales** OU.
3. Right-click **Abbie Parsons**, and then click **Delete**.
4. In the confirmation window, click **Yes**.
5. Close Active Directory Users and Computers.

Task 4: Perform object restoration with the Active Directory Module for Windows PowerShell

1. In **Server Manager**, click **Tools**, and then click **Active Directory Module for Windows PowerShell**.
2. Type the following command, and then press Enter:
Get-ADObject -Filter {displayName -eq "Abbie Parsons"} -IncludeDeletedObjects | Restore-ADObject
3. Close the **Windows PowerShell** window.

Task 5: Verify object restoration

1. On **LON-DC1**, in **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
2. Make sure that **Abbie Parsons** exists within the Sales OU.

Results*: After completing the exercise, you should have enabled and tested the* ***Active Directory Recycle Bin*** *feature successfully.*

Task 6: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:
1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742B-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.