lab: title: '10 - Implement Data Protection' module: 'Module 10 - Data Protection'

Lab 10 - Backup virtual machines

Student lab manual

Lab scenario

You have been tasked with evaluating the use of Azure Recovery Services for backup and restore of files hosted on Azure virtual machines and on-premises computers. In addition, you want to identify methods of protecting data stored in the Recovery Services vault from accidental or malicious data loss.

Objectives

In this lab, you will:

- Task 1: Provision the lab environment
- Task 2: Create a Recovery Services vault
- Task 3: Implement Azure virtual machine-level backup
- Task 4: Implement File and Folder backup
- Task 5: Perform file recovery by using Azure Recovery Services agent
- Task 6: Perform file recovery by using Azure virtual machine snapshots (optional)
- Task 7: Review the Azure Recovery Services soft delete functionality (optional)

Estimated timing: 50 minutes

Instructions

Exercise 1

Task 1: Provision the lab environment

In this task, you will deploy two virtual machines that will be used to test different backup scenarios.

1. Sign in to the Azure portal.
2. In the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
3. If prompted to select either **Bash** or **PowerShell**, select **PowerShell**.

   Note: If this is the first time you are starting **Cloud Shell** and you are presented with the **You have no storage mounted** message, select the subscription you are using in this lab, and click **Create storage**.
4. In the toolbar of the Cloud Shell pane, click the **Upload/Download files** icon, in the drop-down menu, click **Upload** and upload the files **\Allfiles\Labs\10\az104-10-vms-template.json** and **\Allfiles\Labs\10\az104-10-vms-parameters.json** into the Cloud Shell home directory.
5. From the Cloud Shell pane, run the following to create the resource group that will be hosting the virtual machines (replace the `[Azure_region]` placeholder with the name of an Azure region where you intend to deploy Azure virtual machines):

```
$location = '[Azure_region]'

$rgName = 'az104-10-rg0'

New-AzResourceGroup -Name $rgName -Location $location
```

6. From the Cloud Shell pane, run the following to create the first virtual network and deploy a virtual machine into it by using the template and parameter files you uploaded:

```
New-AzResourceGroupDeployment `
   -ResourceGroupName $rgName `
   -TemplateFile $HOME/az104-10-vms-template.json `
   -TemplateParameterFile $HOME/az104-10-vms-parameters.json `
   -AsJob
```

7. Minimize Cloud Shell (but do not close it).

   Note: Do not wait for the deployment to complete but instead proceed to the next task. The deployment should take about 5 minutes.

Task 2: Create a Recovery Services vault

In this task, you will create a recovery services vault.

1. In the Azure portal, search for and select **Recovery Services vaults** and, on the **Recovery Services vaults** blade, click **+ Add**.
2. On the **Create Recovery Services vault** blade, specify the following settings:

Settings	Value
Subscription	the name of the Azure subscription you are using in this lab
Resource group	the name of a new resource group **az104-10-rg1**
Name	**az104-10-rsv1**
Region	the name of a region where you deployed the two virtual machines in the previous task

   Note: Make sure that you specify the same region into which you deployed virtual machines in the previous task.

3. Click **Review + Create** and then click **Create**.

   Note: Wait for the deployment to complete. The deployment should take less than 1 minute.

4. When the deployment is completed, click **Go to Resource**.
5. On the **az104-10-rsv1** Recovery Services vault blade, in the **Settings** section, click **Properties**.
6. On the **az104-10-rsv1 - Properties** blade, click the **Update** link under **Backup Configuration** label.
7. On the **Backup Configuration** blade, note that you can set the **Storage replication type** to either **Locally-redundant** or **Geo-redundant**. Leave the default setting of **Geo-redundant** in place and close the blade.

   Note: This setting can be configured only if there are no existing backup items.

8. Back on the **az104-10-rsv1 - Properties** blade, click the **Update** link under **Security Settings** label.
9. On the **Security Settings** blade, note that **Soft Delete (For Azure Virtual Machines)** is **Enabled**.
10. Close the **Security Settings** blade and, back on the **az104-10-rsv1** Recovery Services vault blade, click **Overview**.

Task 3: Implement Azure virtual machine-level backup

In this task, you will implement Azure virtual-machine level backup.

Note: Before you start this task, make sure that the deployment you initiated in the first task of this lab has successfully completed.

1. On the **az104-10-rsv1** Recovery Services vault blade, click **+ Backup**.
2. On the **Backup Goal** blade, specify the folowing settings:

Settings	Value
Where is your workload running?	**Azure**
What do you want to backup?	**Virtual machine**

3. On the **Backup Goal** blade, click **Backup**.
4. On the **Backup policy**, review the **DefaultPolicy** settings and select **Create a new policy**.
5. Define a new backup policy with the following settings (leave others with their default values):

Setting	Value
Policy name	**az104-10-backup-policy**
Frequency	**Daily**
Time	**12:00 AM**
Timezone	the name of your local time zone
Retain instant recovery snapshot(s) for	**2** Days(s)

6. Click **OK** to create the policy and then, in the **Virtual Machines** section, select **Add**.
7. On the **Select virtual machines** blade, select **az-104-10-vm0**, click **OK**, and, back on the **Backup** blade, click **Enable backup**.

   Note: Wait for the backup to be enabled. This should take about 2 minutes.
8. Navigate back to the **az104-10-rsv1** Recovery Services vault blade, in the **Protected items** section, click **Backup items**, and then click the **Azure virtual machines** entry.
9. On the **Backup Items (Azure Virtual Machine)** blade of **az104-10-vm0**, review the values of the **Backup Pre-Check** and **Last Backup Status** entries, and click the **az104-10-vm0** entry.
10. On the **az104-10-vm0** Backup Item blade, click **Backup now**, accept the default value in the **Retain Backup Till** drop-down list, and click **OK**.

    Note: Do not wait for the backup to complete but instead proceed to the next task.

Task 4: Implement File and Folder backup

In this task, you will implement file and folder backup by using Azure Recovery Services.

1. In the Azure portal, search for and select **Virtual machines**, and on the **Virtual machines** blade, click **az104-10-vm1**.
2. On the **az104-10-vm1** blade, click **Connect**, in the drop-down menu, click **RDP**, on the **Connect with RDP** blade, click **Download RDP File** and follow the prompts to start the Remote Desktop session.

   Note: This step refers to connecting via Remote Desktop from a Windows computer. On a Mac, you can use Remote Desktop Client from the Mac App Store and on Linux computers you can use an open source RDP client software.

   Note: You can ignore any warning prompts when connecting to the target virtual machines.
3. When prompted, sign in by using the **Student** username and **Pa55w.rd1234** password.
4. Within the Remote Desktop session to the **az104-10-vm1** Azure virtual machine, in the **Server Manager** window, click **Local Server**, click **IE Enhanced Security Configuration** and turn it **Off** for Administrators.
5. Within the Remote Desktop session to the **az104-10-vm1** Azure virtual machine, start Internet Explorer, browse to the Azure portal, and sign in using your credentials.

6. In the Azure portal, search for and select **Recovery Services vaults** and, on the **Recovery Services vaults**, click **az104-10-rsv1**.
7. On the **az104-10-rsv1** Recovery Services vault blade, click **+ Backup**.
8. On the **Backup Goal** blade, specify the following settings:

Settings	Value
Where is your workload running?	**On-premises**
What do you want to backup?	**Files and folders**

   Note: Even though the virtual machine you are using in this task is running in Azure, you can leverage it to evaluate the backup capabilities applicable to any on-premises computer running Windows Server operating system.

9. On the **Backup Goal** blade, click **Prepare infrastructure**.
10. On the **Prepare infrastructure** blade, click the **Download Agent for Windows Server or Windows Client** link.
11. When prompted, click **Run** to start installation of **MARSAgentInstaller.exe** with the default settings.

    Note: On the **Microsoft Update Opt-In** page of the **Microsoft Azure Recovery Services Agent Setup Wizard**, select the **I do not want to use Microsoft Update** installation option.

12. On the **Installation** page of the **Microsoft Azure Recovery Services Agent Setup Wizard**, click **Proceed to Registration**. This will start **Register Server Wizard**.
13. Switch to the Internet Explorer window displaying the Azure portal, on the **Prepare infrastructure** blade, select the checkbox **Already downloaded or using the latest Recovery Server Agent**, and click **Download**.
14. When prompted, whether to open or save the vault credentials file, click **Save**. This will save the vault credentials file to the local Downloads folder.
15. Switch back to the **Register Server Wizard** window and, on the **Vault Identification** page, click **Browse**.
16. In the **Select Vault Credentials** dialog box, browse to the **Downloads** folder, click the vault credentials file you downloaded, and click **Open**.
17. Back on the **Vault Identification** page, click **Next**.
18. On the **Encryption Setting** page of the **Register Server Wizard**, click **Generate Passphrase**.
19. On the **Encryption Setting** page of the **Register Server Wizard**, click the **Browse** button next to the **Enter a location to save the passphrase** drop-down list.
20. In the **Browse For Folder** dialog box, select the **Documents** folder and click **OK**.
21. Click **Finish**, review the **Microsoft Azure Backup** warning and click **Yes**, and wait for the registration to complete.

    Note: In a production environment, you should store the passphrase file in a secure location other than the server being backed up.

22. On the **Server Registration** page of the **Register Server Wizard**, review the warning regarding the location of the passphrase file, ensure that the **Launch Microsoft Azure Recovery Services Agent** checkbox is selected and click **Close**. This will automatically open the **Microsoft Azure Backup** console.
23. In the **Microsoft Azure Backup** console, in the **Actions** pane, click **Schedule Backup**.
24. In the **Schedule Backup Wizard**, on the **Getting started** page, click **Next**.
25. On the **Select Items to Backup** page, click **Add Items**.
26. In the **Select Items** dialog box, expand **C:\Windows\System32\drivers\etc**, select **hosts**, and then click **OK**:
27. On the **Select Items to Backup** page, click **Next**.

28. On the **Specify Backup Schedule** page, ensure that the **Day** option is selected, in the first drop-down list box below the **At following times (Maximum allowed is three times a day)** box, select **4:30 AM**, and then click **Next**.
29. On the **Select Retention Policy** page, accept the defaults, and then click **Next**.
30. On the **Choose Initial Backup type** page, accept the defaults, and then click **Next**.
31. On the **Confirmation** page, click **Finish**. When the backup schedule is created, click **Close**.
32. In the **Microsoft Azure Backup** console, in the Actions pane, click **Back Up Now**.

    Note: The option to run backup on demand becomes available once you create a scheduled backup.
33. In the Back Up Now Wizard, on the **Select Backup Item** page, ensure that the **Files and Folders** option is selected and click **Next**.
34. On the **Retain Backup Till** page, accept the default setting and click **Next**.
35. On the **Confirmation** page, click **Back Up**.
36. When the backup is complete, click **Close**, and then close Microsoft Azure Backup.
37. Switch to the Internet Explorer window displaying the Azure portal, navigate back to the Recovery Services vault blade and click **Backup items**.
38. On the **az104-10-rsv1 - Backup items** blade, click **Azure Backup Agent**.
39. On the **Backup Items (Azure Backup Agent)** blade, verify that there is an entry referencing the **C:** drive of **az104-10-vm1.**.

Task 5: Perform file recovery by using Azure Recovery Services agent (optional)

In this task, you will perform file restore by using Azure Recovery Services agent.

1. Within the Remote Desktop session to **az104-10-vm1**, open File Explorer, navigate to the **C:\Windows\System32\drivers\etc** folder and delete the **hosts** file.
2. Switch to the Microsoft Azure Backup window and click **Recover data**. This will start **Recover Data Wizard**.
3. On the **Getting Started** page of **Recover Data Wizard**, ensue that **This server (az104-10-vm1.)** option is selected and click **Next**.
4. On the **Select Recovery Mode** page, ensure that **Individual files and folders** option is selected, and click **Next**.
5. On the **Select Volume and Date** page, in the **Select the volume** drop down list, select **C:**, accept the default selection of the available backup, and click **Mount**.

    Note: Wait for the mount operation to complete. This might take about 2 minutes.
6. On the **Browse And Recover Files** page, note the drive letter of the recovery volume and review the tip regarding the use of robocopy.
7. Click **Start**, expand the **Windows System** folder, and click **Command Prompt**.
8. From the Command Prompt, run the following to copy the restore the **hosts** file to the original location (replace `[recovery_volume]` with the drive letter of the recovery volume you identified earlier):

    ```
    robocopy [recovery_volume]:\Windows\System32\drivers\etc C:\Windows\system32\drivers\etc hosts /r:1 /w:1
    ```
9. Switch back to the **Recover Data Wizard** and, on the **Browse and Recover Files**, click **Unmount** and, when prompted to confirm, click **Yes**.
10. Terminate the Remote Desktop session.

Task 6: Perform file recovery by using Azure virtual machine snapshots (optional)

In this task, you will restore a file from the Azure virtual machine-level snapshot-based backup.

1. Switch to the browser window running on your lab computer and displaying the Azure portal.
2. In the Azure portal, search for and select **Virtual machines**, and on the **Virtual machines** blade, click **az104-10-vm0**.

3. On the **az104-10-vm0** blade, click **Connect**, in the drop-down menu, click **RDP**, on the **Connect with RDP** blade, click **Download RDP File** and follow the prompts to start the Remote Desktop session.

   Note: This step refers to connecting via Remote Desktop from a Windows computer. On a Mac, you can use Remote Desktop Client from the Mac App Store and on Linux computers you can use an open source RDP client software.

   Note: You can ignore any warning prompts when connecting to the target virtual machines.

4. When prompted, sign in by using the **Student** username and **Pa55w.rd1234** password.

5. Within the Remote Desktop session to the **az104-10-vm0** Azure virtual machine, in the **Server Manager** window, click **Local Server**, click **IE Enhanced Security Configuration** and turn it **Off** for Administrators.

6. Within the Remote Desktop session to the **az104-10-vm0**, click **Start**, expand the **Windows System** folder, and click **Command Prompt**.

7. From the Command Prompt, run the following to delete the **hosts** file:

   ```
   del C:\Windows\system32\drivers\etc\hosts
   ```

   Note: You will restore this file from the Azure virtual machine-level snapshot-based backup later in this task.

8. Within the Remote Desktop session to the **az104-10-vm0** Azure virtual machine, start Internet Explorer, browse to the Azure portal, and sign in using your credentials.

9. In the Azure portal, search for and select **Recovery Services vaults** and, on the **Recovery Services vaults**, click **az104-10-rsv1**.

10. On the **az104-10-rsv1** Recovery Services vault blade, in the **Protected items** section, click **Backup items**.

11. On the **az104-10-rsv1 - Backup items** blade, click **Azure Virtual Machine**.

12. On the **Backup Items (Azure Virtual Machine)** blade, click **az104-10-vm0**.

13. On the **az104-10-vm0** Backup Item blade, click **File Recovery**.

    Note: You have the option of running recovery shortly after backup starts based on the application consistent snapshot.

14. On the **File Recovery** blade, accept the default recovery point and click **Download Executable**.

    Note: The script mounts the disks from the selected recovery point as local drives within the operating system from which the script is run.

15. Click **Download** and, when prompted whether to run or save **IaaSVMILRExeForWindows.exe**, click **Save**.

16. Start File Explorer, navigate to the **Downloads** folder, right-click the newly downloaded file, select **Properties** in the right-click menu, in the **Properties** dialog box, select the **Unblock** checkbox, and click **OK**.

17. Back in the File Explorer window, double-click the newly downloaded file.

18. When prompted to provide the password from the portal, copy the password from the **Password to run the script** text box on the **File Recovery** blade, paste it at the Command Prompt, and press **Enter**.

    Note: This will open a Windows PowerShell window displaying the progress of the mount.

    Note: If you receive an error message at this point, refresh the Internet Explorer window and repeat the last three steps.

19. Wait for the mount process to complete, review the informational messages in the Windows PowerShell window, note the drive letter assigned to the volume hosting **Windows**, and start File Explorer.

20. In File Explorer, navigate to the drive letter hosting the snapshot of the operating system volume you identified in the previous step and review its content.

21. Switch to the **Command Prompt** window.

22. From the Command Prompt, run the following to copy the restore the **hosts** file to the original location (replace `[os_volume]` with the drive letter of the operating system volume you identified earlier):

```
robocopy [os_volume]:\Windows\System32\drivers\etc C:\Windows\system32\drivers\etc hosts /r:1 /w:1
```

23. Switch back to the **File Recovery** blade in the Azure portal and click **Unmount Disks**.
24. Terminate the Remote Desktop session.

Task 7: Review the Azure Recovery Services soft delete functionality

1. On the lab computer, in the Azure portal, search for and select **Recovery Services vaults** and, on the **Recovery Services vaults**, click **az104-10-rsv1**.
2. On the **az104-10-rsv1** Recovery Services vault blade, in the **Protected items** section, click **Backup items**.
3. On the **az104-10-rsv1 - Backup items** blade, click **Azure Backup Agent**.
4. On the **Backup Items (Azure Backup Agent)** blade, click the entry representing the backup of **az104-10-vm1**.
5. On the **C:\ on az104-10-vm1.** blade, click the **az104-10-vm1.** link.
6. On the **az104-10-vm1.** Protected Servers blade, click **Delete**.
7. On the **Delete** blade, specify the following settings.

Settings	Value
TYPE THE SERVER NAME	**az104-10-vm1.**
Reason	**Recycling Dev/Test server**
Comments	**az104 10 lab**

Note: Make sure to include the trailing period when typing the server name

8. Enable the checkbox next to the label **There is backup data of 1 backup items associated with this server.I understand that clicking "Confirm" will permanently delete all the cloud backup data. This action cannot be undone. An alert may be sent to the administrators of this subscription notifying them of this deletion** and click **Delete**.
9. Navigate back to the **az104-10-rsv1 - Backup items** blade and click **Azure Virtual Machines**.
10. On the **az104-10-rsv1 - Backup items** blade, click **Azure Virtual Machine**.
11. On the **Backup Items (Azure Virtual Machine)** blade, click **az104-10-vm0**.
12. On the **az104-10-vm0** Backup Item blade, click **Stop backup**.
13. On the **Stop backup** blade, select **Delete Backup Data**, specify the following settings and click **Stop backup**:

Settings	Value
Type the name of Backup item	**az104-10-vm0**
Reason	**Others**
Comments	**az104 10 lab**

14. Navigate back to the **az104-10-rsv1 - Backup items** blade and click **Refresh**.

Note: The **Azure Virtual Machine** entry is still lists **1** backup item.

15. Click the **Azure Virtual Machine** entry and, on the **Backup Items (Azure Virtual Machine)** blade, click the **az104-10-vm0** entry.
16. On the **az104-10-vm0** Backup Item blade, note that you have the option to **Undelete** the deleted backup.

Note: This functionality is provided by the soft-delete feature, which is, by default, enabled for Azure virtual machine backups.

17. Navigate back to the **az104-10-rsv1** Recovery Services vault blade, and in the **Settings** section, click **Properties**.

18. On the **az104-10-rsv1 - Properties** blade, click the **Update** link under **Security Settings** label.
19. On the **Security Settings** blade, Disable **Soft Delete (For Azure Virtual Machines)** and click **Save**.

    Note: This will not affect items already in soft delete state.
20. Close the **Security Settings** blade and, back on the **az104-10-rsv1** Recovery Services vault blade, click **Overview**.
21. Navigate back to the **az104-10-vm0** Backup Item blade and click **Undelete**.
22. On the **Undelete az104-10-vm0** blade, click **Undelete**.
23. Wait for the undelete operation to complete, refresh the browser page, if needed, navigate back to the **az104-10-vm0** Backup Item blade, and click **Delete backup data**.
24. On the **Delete Backup Data** blade, specify the following settings and click **Delete**:

Settings	Value
Type the name of Backup item	**az104-10-vm0**
Reason	**Others**
Comments	**az104 10 lab**

Clean up resources

Note: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges.

1. In the Azure portal, open the **PowerShell** session within the **Cloud Shell** pane.
2. List all resource groups created throughout the labs of this module by running the following command:

```
Get-AzResourceGroup -Name 'az104-10*'
```

3. Delete all resource groups you created throughout the labs of this module by running the following command:

```
Get-AzResourceGroup -Name 'az104-10*' | Remove-AzResourceGroup -Force -AsJob
```

Note: Optionally, you might consider deleting the auto-generated resource group with the prefix **AzureBackupRG_** (there is no additional charge associated with its existence).

Note: The command executes asynchronously (as determined by the -AsJob parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.

Review

In this lab, you have:

- Provisioned the lab environment
- Created a Recovery Services vault
- Implemented Azure virtual machine-level backup
- Implemented File and Folder backup
- Performed file recovery by using Azure Recovery Services agent
- Performed file recovery by using Azure virtual machine snapshots
- Reviewed the Azure Recovery Services soft delete functionality