**Module 4: Azure Storage types and capabilities**

**Lab B: Implementing the Azure Recovery Services agent-based backups**

**Exercise 1: Preparing your Azure subscription for implementing Azure Backup**

**Task 1: Create an Azure Recovery Services vault**

1. In the browser, browse to the Azure portal at <http://portal.azure.us>
2. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
3. In the Azure portal, in the hub menu on the left hand side, click **+ Create a resource**.
4. On the **New** blade, click **Monitoring + Management** and then click **Backup and Site Recovery (OMS)**.
5. On the **Recovery Services vault** blade, specify the following settings and then click **Create**:

* Name: **RSWinGov4bXX-vault**
* Subscription: select the name of the Azure subscription you will be using in this lab
* Resource group: click **Create new** and type **WinGov4bXX-LabRG** as the name of the new resource group
* Location: select any Azure region where you can create a recovery services vault, preferably close to the lab location
* Pin to dashboard: leave the checkbox unchecked

1. Wait for the vault to be provisioned.

**Task 2: Configure backup redundancy**

1. In the Azure portal, in the hub menu, click **All services**.
2. In the service menu, in the **Filter** text box, type **Recovery Services vaults** and then, in the list of results, click **Recovery Services vaults**.
3. On the **Recovery Services vaults** blade, click **RSWinGov4bXX-vault**.
4. On the **RSWinGov4bXX-vault** blade, in the **MANAGE** section, click **Backup Infrastructure**.
5. On the **RSWinGov4bXX-vault - Backup Infrastructure** blade, click **Backup Configuration**.
6. On the **Backup Configuration** blade, click **Locally-redundant**.
7. Click **Save**.

**Result**: After you completed this exercise, you should have successfully created and configured the Azure Recovery Services vault.

**Exercise 2: Configuring an on-premises computer for Azure Recovery Services agent-based backups**

**Task 1: Download the Azure Recovery Services agent**

1. In the Azure portal, navigate to the **RSWinGov4bXX-vault** blade.
2. In the **GETTING STARTED** section, click **Backup**.
3. In the **Where is your workload running?** drop-down list, click **On-Premises**.
4. In the **What do you want to backup?** drop-down list, click **Files and folders**.
5. Click **Prepare Infrastructure**.
6. On the **Prepare infrastructure** blade, click the **Download Agent for Windows Server or Windows Client** link.
7. When you receive a prompt to choose whether to run or save the **MARSAgentInstaller.exe** file, click **Save**.

**Task 2: Install the Azure Recovery Services agent**

1. In the browser window displaying the Azure portal, in the notification bar at the bottom of the window, click **Open folder**.
2. In the File Explorer, in the **Downloads** folder, double-click **MARSAgentInstaller** file. This will launch the **Microsoft Azure Recovery Services Agent Setup Wizard**.
3. If prompted by User Account Control, click **Yes**.
4. On the **Installation Settings** page of the wizard, accept the default settings, and then click **Next**.
5. On the **Proxy Configuration** page of the wizard, accept the default settings, and then click **Next**.
6. On the **Microsoft Update Opt-in** page, select **I do not want to use Windows Update**, and click **Next**.
7. On the **Installation** page of the wizard, click **Install**.
8. After the installation completes, on the **Installation** page of the **Microsoft Azure Recovery Services Agent** **Setup** **Wizard**, click **Proceed to Registration**. This will launch the **Register Server Wizard**.

**Task 3: Download vault credentials and register Recovery Services agent with the vault**

1. Switch to the browser window that displays the Azure portal.
2. On the **Prepare infrastructure** blade, select the checkbox labeled **Already downloaded or using the latest Recovery Services Agent** and then click **Download**.
3. When prompted whether to open or save a file with the extension **.VaultCredentials**, click **Save**.
4. Switch to the **Register Server Wizard**.
5. On the **Vault Identification** page of the wizard, click **Browse**.
6. In the **Select Vault Credentials** window, browse to the **Downloads** folder, click the file with the extension **.VaultCredentials**, and then click **Open**.
7. Wait for the vault credentials validation to complete, and then click **Next**.
8. On the **Encryption Setting** page of the wizard, click **Generate Passphrase**.
9. Click **Browse** button next to the **Enter a location to save the passphrase** text box.
10. In the **Browse For Folder** dialog box, navigate to the **C:\Test** folder, and then click **OK**.
11. Click **Finish**.
12. Wait for the registration to complete. Ensure that the **Launch Microsoft Azure Recovery Services Agent** check box is selected, and then click **Close**. This will open the **Microsoft Azure Backup** window.

**Task 4: Configure throttling options**

1. In the **Microsoft Azure Backup** window, in the **Actions** pane, click **Change Properties**.
2. In the **Microsoft Azure Backup Properties** window, click the **Throttling** tab.
3. Click the **Enable internet bandwidth usage throttling for backup operations** **and then click** **OK**.
4. In the **Microsoft Azure Backup** dialog box, click **OK**.

**Note:** Note that you have the options of adjusting the bandwidth and the definition of what constitutes work and nonwork hours.

**Result**: After you completed this exercise, you should have successfully installed and configured Azure Recovery Services agent on your lab virtual machine and registered it with Azure Recovery Services vault.

**Exercise 3: Testing the backup of the virtual machine files and folders**

**Task 1: Configure a backup schedule**

1. In the **Microsoft Azure Backup** window, in the **Actions** pane, click **Schedule Backup**. This launches the **Schedule Backup Wizard**.
2. On the **Getting started** page of the wizard, click **Next**.
3. On the **Select Items to Backup** page of the wizard, click **Add Items**.
4. In the **Select Items** dialog box, navigate to the **C:\Windows\System32\drivers\etc** folder, and then click the check box next to the **hosts** entry. Ensure that this is the only item selected, and then click **OK**.
5. On the **Select Items to Backup** page of the wizard, click **Next**.
6. On the **Specify Backup Schedule (Files and Folders)** page of the wizard, change the entry in the first drop-down list to **11:00 PM**, and then click **Next**.
7. On the **Select Retention Policy (Files and Folders)** page of the wizard, accept the default settings, and then click **Next**.
8. On the **Choose Initial Backup Type (Files and Folders)** page of the wizard, ensure that the **Automatically over the network** option is selected, and then click **Next**.
9. On the **Confirmation** page of the wizard, click **Finish**.
10. On the **Modify Backup Progress** page of the wizard, click **Close**.

**Task 2: Perform a manual backup**

1. In the **Microsoft Azure Backup** window, in the **Actions** pane, click **Back Up Now**. This launches the **Back Up Now Wizard**.
2. On the **Confirmation** page of the wizard, click **Back Up**. Notice that you can change the properties of the server settings, but not the list of backup items.
3. On the **Backup Progress** page of the wizard, monitor the status of the backup process. After it completes, click **Close**.

**Result**: After completing this exercise, you should have successfully tested backup of files by using the Azure Recovery Services agent.

**Exercise 4: Testing a restore of the virtual machine files and folders**

**Task 1: Perform a restore**

1. In the **Microsoft Azure Backup** window, in the **Actions** pane, click **Recover Data**. This launches the **Recover Data Wizard**.
2. On the **Getting Started** page of the wizard, ensure that the **This server** **(*your pc name*)** option is selected, and then click **Next**.
3. On the **Select Recovery Mode** page of the wizard, ensure that the **Individual files and folders** option is selected, and then click **Next**.
4. On the **Select Volume and Date** page of the wizard, click the **C:\** entry in the **Select the volume** drop-down list and click **Mount**. Since there is only a single backup, the date of the backup is automatically selected.
5. On the **Browse and Recover Files** page, note that the recovery volume has been mounted as the **E:\** drive and click **Browse**. This will open a File Explorer window.
6. In the File Explorer window, navigate to the **Windows\System32\drivers\etc** folder, right-click the **hosts** file, and, in the right-click menu, click **Copy**
7. In the File Explorer window, right-click the **Documents** folder and, in the right-click menu, click **Paste**.
8. Switch back to the **Browse and Recover Files** of the **Recover Data Wizard** and click **Unmount**.
9. When prompted, in the **Confirm Recovery Volume Unmount** dialog box, click **Yes**.
10. Back in the **Microsoft Azure Backup** window, verify that the recovery job is marked as completed.

**Task 2: Identify and delete all lab Azure resources**

1. Switch to the Internet Explorer window that displays the Azure portal.
2. In the Azure portal, scroll to the **RSWinGov4bXX-vault** blade.
3. In the **MANAGE** section of the **RSWinGov4bXX-vault** blade, click **Backup Infrastructure**.
4. On the **RSWinGov4bXX-vault - Backup Infrastructure** blade, click **Protected Servers**.
5. On the **Protected Servers** blade, click **Azure Backup Agent**.
6. On the **Protected Servers (Azure Backup Agent)** blade, click the entry representing your lab computer.
7. On the **your computer name** blade, click **Delete**.
8. On the **Delete** blade, in the **TYPE THE SERVER NAME** text box, type **your computer name.** and then click **Delete**.

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

1. Navigate to the **RSWinGov4bXX-vault** blade and click **Overview**.
2. Click **Delete**.
3. When prompted for confirmation, click **Yes**.
4. In the hub menu, click **Resource groups**.
5. On the **Resource groups** blade, click **WinGov4bXX-LabRG**.
6. On the **WinGov4bXX-LabRG** blade, click **Delete**.
7. On the **Are you sure you want to delete "WinGov4bXX-LabRG"** blade, in the **TYPE THE RESOURCE GROUP NAME** box, type the name of the resource group, and then click **Delete**.
8. Perform steps 13-15 for the **StoreXXRG** you made in **Lab A** of this module.
9. Close all open windows.