# Lab Answer Key: Module 6: Planning and implementing storage, backup, and recovery services

# Lab: Planning and implementing Azure Storage

## Exercise 1: Creating and configuring Azure Storage

#### Task 1: Create a storage account

1. Ensure that you are signed in to MIA-CL1 as **Student** with the password **Pa$$w0rd** and that the setup script that you ran in the previous demonstration to prepare the environment has completed.
2. Start Internet Explorer, and then browse to **https://portal.azure.com**. When prompted, sign in by using the Microsoft account that is the Service Administrator or Co-Administrator of your Microsoft Azure subscription.
3. On the **Hub** menu, click **New**, and then click **Storage**.
4. In the Data + Storage blade, click **Storage account**.
5. In the Create storage account blade, apply the following settings, and then click **Create**:

* Name: Enter a valid, unique name consisting of between 3 and 24 lower case characters or digits.
* Deployment model: Classic
* Account kind: General purpose
* Performance: Standard
* Replication: Geo-redundant storage (GRS)
* Subscription: *Your Azure subscription*
* Resource group: make sure that **Create new** radio button is selected and then type **Asset-Management** as the name of the *Resource Group*.
* Location: Select the Azure region nearest to you
* Pin to dashboard: Clear the check box

1. At the top of the portal window menu, click the **Notifications** icon, and then wait for the notification that the storage account has been created.
2. On the **Hub** menu, click **More services**, and then click **Storage accounts (classic)**.
3. In the Storage accounts (classic) blade, click the storage account that you just created.
4. In the blade for your storage account, click the **Blobs** tile.
5. In the Blob service blade, click **Container** in the toolbar.
6. In the New container blade, apply the following settings, and then click **Create**:

* Name: **asset-images**
* Access type: **Private**

1. Close the Blob service blade.
2. On the taskbar, right-click **Windows PowerShell**, and then click **Run ISE as Administrator**. Click **Yes** when prompted.
3. In the Windows PowerShell Interactive Scripting Environment (ISE), click **File**, and then click **Open**.
4. In the **Open** dialog box, browse to \*\*D:06\*\*, click **ExampleCommands.ps1**, and then click **Open**.
5. If the Script pane is not visible, on the **View** menu, click **Show Script Pane**.
6. In Windows PowerShell ISE, in the Script pane, type the name of the storage account that you created in the previous task.
7. Leave the Internet Explorer window open. You will use it later in this lab.

#### Task 2: Install AzCopy

1. In Internet Explorer, open a new tab, and then browse to **http://aka.ms/AzCopy**.
2. In the Download and install AzCopy section, click the link to **Download the latest version of AzCopy**.
3. When prompted to run or save the file, click **Run**. Then click **Yes** if prompted to allow the program to make changes to the computer, and then complete the wizard to install AzCopy by using the default installation options.
4. Right-click **Start**, click **System**, and then in the System window, click **Advanced system settings**.
5. In the **System Properties** dialog box, on the **Advanced** tab, click **Environment Variables**.
6. In the **Environment Variables** dialog box, in the **System variables** list, select **Path**, and then click **Edit**.
7. In the **Edit** **environment variable** dialog box, click **New**.
8. In the text box, type \*\*C:Files (x86)SDKs\*, and then click **OK**.
9. In the **Environment Variables** dialog box, click **OK**.
10. In the **System Properties** dialog box, click **OK**, and then close the System window.
11. Right-click **Start**, click **Command Prompt (Admin)**, and then click **Yes** when prompted.
12. At the command prompt, type the following command, and then press Enter:

AzCopy /?

1. View the syntax information that displays. Leave the Command Prompt window open for the next task.

#### Task 3: Use AzCopy to upload blobs

1. In Internet Explorer, on the **Microsoft Azure** tab, in the blade for your storage account, click the **Keys** icon.
2. On the Manage keys blade, click the **Copy** icon next to the primary access key. If prompted to allow access to the Clipboard, click **Allow access**.
3. In the Command Prompt window, enter the following commands to change the current directory context:

D: CD D:\Labfiles\Lab06\Starter

1. Switch to Windows PowerShell ISE.
2. In Windows PowerShell ISE, in the Script pane, locate the following code:

AzCopy /Dest:https://<your storage account>.blob.core.windows.net/asset-images /destkey:<your primary access key> /Source:asset-images

1. Replace < *your storage account*> with your storage account name.
2. Replace with your primary access key.
3. In Windows PowerShell ISE, in the Script pane, select the code that you just edited. Click **Edit**, and then click **Copy**.
4. Switch to the Command Prompt window.
5. In the Command Prompt window, click the control box at the top left of the window, point to **Edit**, click **Paste**, and then press Enter to run the command.
6. Wait for the command to complete, and then view the file transfer information that displays.
7. Close the Command prompt window.

**Result**: At the end of this exercise, you should have created a new Azure storage account with a container named "asset-images."

## Exercise 2: Using Azure File storage

#### Task 1: Create a file share and upload files

1. Switch to Windows PowerShell ISE.
2. Click **File**, and then click **Open**.
3. In the **Open** dialog box, browse to \*\*D:06\*\*, click **FileShare.ps1**, and then click **Open**.
4. In Windows PowerShell ISE, in the command prompt pane, enter the **Get-AzureAccount** command, and then verify that your Microsoft account displays. > **Note:** If your account does not display, enter the **Add-AzureAccount** command, and then sign in by using your Microsoft account.
5. In the script pane, in the *$storageAccountName* variable declaration at the beginning, replace the *<your\_storage\_account\_name>* value with the name of the Azure storage account that you created in the previous task.
6. Review the script, noting that it:

* Declares variables named *$shareName\_ and \_$folderName* for the file share and the folder to create.
* Uses the **Get-AzureStorageKey** cmdlet to retrieve the access key for your storage account.
* Uses the **New-AzureStorageContext** cmdlet to create a storage context that connects to your storage account by using the access key.
* Uses the **New-AzureStorageShare** cmdlet to create a share.
* Uses the **New-AzureStorageDirectory** cmdlet to create a folder in the share.
* Finds the folder where the script is stored, and then declares a variable named *$sourceFolder* that references the invoices subfolder.
* Iterates through the files in the source folder, and then uses the **Set-AzureStorageFileContent** cmdlet to write each file to the folder in the file share.

1. Save the script, and then on the toolbar, click **Run Script**.
2. Observe the script as it runs, and then view the output. When you finish, close Windows PowerShell ISE without saving any changes.

#### Task 2: Access a file share from a VM

1. In Internet Explorer, on the Azure portal, click **Browse**, click **Virtual machines (classic)**, and then in the Virtual machines (classic) blade, click **AdatumSvr1**.
2. In the AdatumSvr1 blade, click **Connect**, and then when prompted to open or save the AdatumSvr1.rdp file, click **Open**.
3. When prompted to connect, click **Connect**, enter the following credentials, and then click **OK**:

* User name: \*\*AdatumSvr1\*
* Password: **Pa$$w0rd123**

1. If prompted to connect again, click **Yes**, and then wait for the remote desktop session to open and initialize. If you are promoted to find PCs, devices, and content on this network, click **No**.
2. When Server Manager starts, on the **Local Server** page, click the status for **IE Enhanced Security Configuration**, select **Off** for Administrators, and then click **OK**.
3. Close Server Manager.
4. In the AdatumSvr1 remote desktop window, switch to the **Start** page, and then click **Internet Explorer**. If prompted to set up Internet Explorer, select **Use recommended security, privacy, and compatibility settings**, and then click **OK**.
5. Browse to **https://portal.azure.com**, and then sign in by using the Microsoft account that is the Service Administrator or Co-Administrator of your Azure subscription.
6. On the **Hub** menu, click **More services**, and then click **Storage accounts (classic)**.
7. In the Storage accounts (classic) blade, click the storage account that you created in the previous exercise, and then in the blade for your storage account, click **Access Keys**.
8. On the Manage Keys blade, click the **Copy** icon next to the primary access key. If prompted to allow access to the Clipboard, click **Allow access**.
9. Right-click **Start**, and then click **Command Prompt (Admin)**.
10. In the Command Prompt window, enter the following command to map a network drive to the assets file share in your Azure storage account. Replace both instances of *storage\_account* with the name of your storage account, and then press Enter:

net use z: \\storage\_account.file.core.windows.net\assets /u:storage\_account

1. When prompted, paste the *access\_key* from the Clipboard (to paste into a Command Prompt window, click the control box at the top left of the window, point to **Edit**, and then click **Paste**).
2. At the command prompt, enter the following command to view the contents of the invoices folder in drive Z, which is now mapped to the assets file share that you created in a previous task:

dir z:\invoices

1. Verify that three invoice files are listed.
2. Close the Command Prompt window and Internet Explorer, and then sign out of the remote desktop session to AdatumSvr1.

**Result**: At the end of this exercise, you should have created a file share named "assets" that contains a folder named "invoices." This folder will contain three invoice documents and will be accessible on the AdatumSvr1 virtual machine (VM).

## Exercise 3: Protecting data with Azure Backup

#### Task 1: Create a backup vault

1. On the MIA-CL1, open Internet Explorer, and then browse to **https://manage.windowsazure.com**.
2. If prompted, sign in by using the Microsoft account that is the Service Administrator or Co-Administrator of your Azure subscription.
3. In the Azure classic portal, click **NEW**, click **DATA SERVICES**, click **RECOVERY SERVICES**, click **BACKUP VAULT**, and then click **QUICK CREATE**.
4. Enter a valid, unique name, select your closest region, and then click **CREATE VAULT**.

#### Task 2: Obtain vault credentials

1. On the Azure classic portal, click **RECOVERY SERVICES** on the **Hub** menu, and then click your new backup vault.
2. On the backup vault **Quick Start** page, click **Download vault credentials**.
3. Click **Save** to download the vault credentials to the Downloads folder.
4. After the credentials download, you will be prompted to open the folder. Click the prompt window.

#### Task 3: Install and configure the Azure Backup agent

1. On the Azure classic portal, on the **Quick Start** page of your backup vault, under Download Azure Backup Agent, click the **Agent forWindows Server or System Center Data Protection Manager or Windows Client** link.
2. When prompted to run or save the file, click **Run**. When prompted to allow the program to make changes, click **Yes**, and then complete the wizard to install the agent. Use the default installation options, and if prompted, choose the option to use Microsoft Update to check for updates.
3. When installation is complete, click **Close**.
4. Minimize all active windows, and then on the desktop, double-click **Microsoft Azure Backup**. When prompted to allow the program to make changes, click **Yes**.
5. In the Microsoft Azure Backup window, in the Actions pane, click **Register Server**.
6. In the Register Server Wizard, on the **Proxy Configuration** page, click **Next**.
7. On the **Vault** **Identification** page, click **Browse**, navigate to the **Downloads** folder, select the credentials that you created earlier, and then click **Open**.
8. On the **Vault Identification** page, click **Next**.
9. On the **Encryption Setting** page, click **Generate Passphrase**, click **Browse**, browse to the **D:06\* folder, and then click** OK\*\*.
10. Click **Register**, and then when registration is complete, click **Close**.
11. Leave Azure Backup open for the next task.

#### Task 4: Create a backup schedule

1. In Azure Backup, in the Actions pane, click **Schedule Backup**.
2. In the Schedule Backup Wizard, on the **Getting started** page, click **Next**.
3. On the **Select Items to Backup** page, click **Add Items**.
4. In the **Select Items** dialog box, expand **D**, expand **Labfiles**, expand **Lab06**, expand **Starter**, select the following folders, and then click **OK**:

* asset-images
* invoices

1. On the **Select Items to Backup** page, click **Next**.
2. On the **Specify Backup** **Schedule** page, 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**.
3. On the **Select Retention Policy** page, accept the defaults, and then click **Next**.
4. On the **Choose Initial Backup type** page, accept the defaults, and then click **Next**.
5. On the **Confirmation** page, click **Finish**. When the backup schedule is created, click **Close**.

#### Task 5: Run a backup

1. In Azure Backup, in the Actions pane, click **Back Up Now**.
2. In the Back Up Now Wizard, on the **Confirmation** page, click **Back Up**.
3. When the backup is complete, click **Close**, and then close Azure Backup.
4. In Internet Explorer, on the Azure portal, on the page for your backup vault, click **REGISTERED ITEMS**.
5. In the **TYPE** drop-down list box, select **Windows server**, click the **check** **mark** on the right side, and then verify that the MIA-CL1 server lists as registered.
6. Click **PROTECTED ITEMS**.
7. In the **TYPE** drop-down list box, select **Files and Folders**, click the **check** **mark** on the right side, and then verify that drive D of MIA-CL1 lists as protected.

#### Task 6: Reset the environment

1. Close all open applications without saving any files.
2. On the taskbar, right-click **Windows PowerShell**, and then click **Run as administrator**. In the **User Account Control** dialog box, click **Yes**.
3. Type the following command, and then press Enter:

Reset-Azure

1. When prompted (twice), sign in by using the Microsoft account that is associated with your Azure subscription.
2. If you have multiple Azure subscriptions, select the one that you want to target with the script.
3. When prompted for confirmation, press Y and press Enter.

**Note:** This script will remove Azure services in your subscription. We therefore recommended that you use an Azure trial pass that was provisioned specifically for this course, and not your own Azure account. The script will take 5-10 minutes to reset your Azure environment, ready for the next lab. The script removes all storage, virtual machines, virtual networks, cloud services, and resource groups. **Note:** **Important**: The script might not be able to access a storage account to delete it (if this occurs, you will see an error). If you find objects remaining after the reset script is complete, you can rerun the **Reset-Azure** script, or you can use the Azure portal and the Azure classic portal to delete all the objects in your Azure subscription manuallyâ€”with the exception of the default directory.

**Result**: At the end of this exercise, you should have created an Azure Backup vault in your subscription, created Azure Backup vault credentials, and installed the Azure Backup agent on the MIA-CL1 lab computer. You should have backed up the contents of the asset-images and invoices folders to the backup vault.

©2016 Microsoft Corporation. All rights reserved.

The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are **not** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.