# Module 8: Planning and implementing backup and disaster recovery

# Lab: Implementing Azure Backup and Azure Site Recovery

## Exercise 1: Protecting data with Azure Backup

#### Task 1: Create a recovery services vault

1. On MIA-CL1, in the Azure portal displayed in Microsoft Edge, in the hub menu, click **+ Create resource**, on the **New** blade, click **Storage**, and, on the **Storage** blade, click **Backup and Site Recovery (OMS)**.
2. On the **Recovery Services vault** blade, specify the following settings and click **Create**:

* Name: **vault20533E0801**
* Subscription: the name of your Azure subscription
* Resource group: ensure that **Use existing** is selected and, in the textbox below, type **20533E0801-LabRG**
* Location: the same Azure region that you chose when running the provisioning script at the beginning of this module

1. Wait until the vault is provisioned.

#### Task 2: Configure the vault for on-premises backup

1. In the hub menu, click **All services**. In the search text box, type **Recovery Services vaults** and, in the list of results, click **Recovery Services vaults**.
2. On the **Recovery Services vaults** blade, click **vault20533E0801**.
3. On the **vault20533E0801** blade, click **+ Backup**.
4. On the **Backup goal** blade, specify the following settings:

* Where is your workload running?: **On-premises**
* What do you want to back up?: **Files and folders**

1. Click **Prepare Infrastructure**.

#### Task 3: Install and configure the Azure Recovery Services Agent

1. In the Azure portal, on the **Prepare infrastructure** blade, click the **Download Agent for Windows Server or Windows Client** link.
2. When prompted whether to save or run **MARSAgentInstaller.exe**, click **Run**.
3. If prompted, in the **User Access Control** dialog box, click **Yes**. This will start **Microsoft Azure Recovery Services Agent Setup Wizard**.
4. On the **Installation Settings** page of the **Microsoft Azure Recovery Services Agent Setup Wizard**, click **Next**.
5. On the **Proxy Configuration** page of the **Microsoft Azure Recovery Services Agent Setup Wizard**, click **Next**.
6. On the **Installation** page of the **Microsoft Azure Recovery Services Agent Setup Wizard**, click **Install**.
7. Click **Proceed to Registration**. This will start **Register Server Wizard**.
8. Switch to Microsoft Edge displaying the Azure portal and, on the **Prepare infrastructure** blade, select the checkbox **Already downloaded or using the latest Recovery Services Agent** and click **Download**.
9. When prompted, click **Save**. This will save the vault credentials file to your Downloads folder.
10. Switch back to the **Register Server Wizard** and, on the **Vault Identification** page, click **Browse**.
11. In the **Select Vault Credentials** dialog box, browse to the **Downloads** folder, click the **.VaultCredentials** file you downloaded, and click **Open**.
12. Click **Next**.
13. On the **Encryption Setting** page of the **Register Server Wizard**, click **Generate Passphrase**.
14. On the **Encryption Setting** page of the **Register Server Wizard**, next to the **Enter a location to save the passphrase**, click **Browse**.
15. In the **Browse For Folder** dialog box, navigate to **F:\Labfiles\Lab08\Starter\** and click **OK**.
16. Click **Finish** and wait for the registration to complete.
17. On the **Server Registration** page of the **Register Server Wizard**, ensure that the **Launch Microsoft Azure Recovery Services Agent** checkbox is selected and click **Close**. This will automatically open the **Microsoft Azure Backup** console.

#### Task 4: Create a backup schedule

1. In the **Microsoft Azure Backup** console, 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 **F:\Labfiles\Lab08\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, 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**.
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 the **Microsoft Azure Backup** console, 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 Microsoft Azure Backup.
4. Switch to the Azure portal, navigate back to the Recovery Services vault blade and click **Backup items**.
5. On the **Backup items** blade, click **Azure Backup Agent**.
6. On the **Backup Items (Azure Backup Agent)** blade, verify that there is an entry referencing the **F:\** drive of **mia-cl1.**.

#### Task 6: Perform a recovery

1. In the **Microsoft Azure Backup** console, in the Actions pane, click **Recover Data**.
2. In the Recover Data Wizard, on the **Getting Started** page, ensure that the option **This server (mia-cl1.)** is selected and click **Next**.
3. On the **Select Recovery Mode** page, ensure that the **Individual files and folder** option is selected and click **Next**.
4. On the **Select Volume and Data** page, in the **Select the volume** drop-down list, select the **F:\** entry. Next pick the newly created backup and click **Mount**.
5. Wait until the backup is mounted on the local computer.
6. On the **Browse and Recover Files** page, click **Browse**. This will automatically open File Explorer showing the content of the mounted volume containing backed up data.
7. Navigate through the mounted volume in the File Explorer window and verify that it contains the backup of the **asset-images** and **invoices** directories. Copy the content of directories to ther original location, overwriting existing content.
8. Close File Explorer.
9. Switch to the **Browse and Recover Files** of the **Recover Data Wizard** and click **Unmount**. When prompted to confirm, click **Yes**.

#### Task 7: Disable backups and delete the Azure Recovery Services vault

1. Switch to the Azure portal and, on the Recovery Services vault blade, in the **MANAGE** section, click **Backup Infrastructure**.
2. On the **vault20533E0801 - Backup infrastructure** blade, click **Protected Servers**.
3. On the **PROTECTED SERVERS** blade, the click **Azure Backup Agent** entry.
4. On the **Protected Servers (Azure Backup Agent)** blade, click **MIA-CL1.**.
5. On the **MIA-CL1.** blade, click **Delete**.
6. On the **Delete** blade, in the **TYPE THE SERVER NAME** text box, type **MIA-CL1.** and click **Delete**.

* **Note**: Make sure to use upper case and don't forget to add the dot at the end of the server name.

1. Navigate back to the Resource Group **20533E0801-LabRG** blade
2. Right Click the vault name **vault20533E0801** then Click **Delete**. When prompted to confirm, click **Yes**.

* **Note**: You must ensure that the backup item is deleted first before you can delete the vault.

## Exercise 2: Implementing protection of Azure VMs by using Azure Site Recovery

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

1. On MIA-CL1, in the Azure portal, in the hub menu, click **+ Create resource**, on the **New** blade, click **Storage**, and, on the **Storage** blade, click **Backup and Site Recovery (OMS)**.
2. On the **Recovery Services vault** blade, specify the following settings and click **Create**:

* Name: **vault20533E0802**
* Subscription: the same Azure region that you chose when running the provisioning script at the beginning of this module
* Resource group: ensure that **Create new** is selected and, in the textbox below, type **20533E0802-LabRG**
* Location: an Azure region **different** from the one you chose when running the provisioning script at the beginning of this module

1. Wait until the vault is provisioned.

#### Task 2: Configure Azure VM replication

1. In the hub menu, click **All services**. In the search text box, type **Recovery Services vaults** and, in the list of results, click **Recovery Services vaults**.
2. On the **Recovery Services vaults** blade, click **vault20533E0802**.
3. On the **vault20533E0802** blade, click **+ Replicate**.
4. On the **Source** blade, specify the following settings and click **OK**:

* Source: **Azure**
* Source location: the same Azure region that you chose when running the provisioning script at the beginning of this module
* Azure virtual machine deployment model: **Resource Manager**
* Source resource group: **20533E0801-LabRG**

1. On the **Select virtual machines** blade, select the checkbox next to the **20533E0801-vm1** entry and click **OK**.
2. On the **Configure settings** blade, set the target location to the location of the Recovery Services vault **vault20533E0802**.
3. Click the **Customize** link next to the **Resource group, Network, Storage, and Availability sets** label.
4. On the **Customize target settings** blade, review the following settings without making any changes and click **OK**.

* Target resource group
* Target virtual network
* Cache storage
* Replica managed disks

1. Click the **Customize** link next to the **Replication policy** label.
2. On the **Configure replication settings** blade, configure the following settings and click **OK**:

* Replication policy: **Create new**
* Name: **12-hour-retention-policy**
* Recovery point retention: **12 Hours**
* App consistent snapshot frequency: **6 Hours**
* Multi-VM consistency: **No**

1. Back on the **Configure settings** blade, click the **Show details** link next to the **Extension settings** label and verify that **Update settings** are set to **Allow ASR to manage**.
2. Click **Create target resources**.
3. Wait for the target resources to be created. This might take a few minutes.
4. On the **Enable replication** blade, click **Enable replication**.
5. Wait until the replication is enabled. This might take about 15 minutes.

#### Task 3: Review Azure VM replication settings

1. In the Azure portal, on the Recovery Services vault blade, in the **PROTECTED ITEMS** section, click **Replicated items**.
2. In the list of replicated items, click the entry representing **20533E0801-vm1**.
3. On the **20533E0801-vm1** blade, review the **Health and status**, **Latest available recovery points**, and **Failover readiness** sections. Note the **Failover** and **Test Failover** entries in the toolbar. Scroll down to the **Infrastructure view**.
4. If time permits, wait until the status of the Azure VM changes to **Protected**. This might take additional 15-20 minutes. At that point, examine the values of **RPO**, as well as **Crash-consistent** and **App-consistent** recovery points.

#### Task 4: Disable replication of an Azure VM and delete the Azure Recovery Services vault

1. In the Azure portal, on the Recovery Services vault blade, on the **20533E0801-vm1** blade, click **Disable Replication**.
2. On the **Disable Replication** blade, click **I am doing a proof of concept (POC) or trial with Azure Site Recovery**, select the option indicating whether you are likely to use Azure Site Recovery in the future, and then click **OK**.
3. Wait until the replication is disabled. This might take about 15 minutes.
4. Navigate back to the recovery services vault blade and click **Overview**.
5. Click **Delete**. When prompted to confirm, click **Yes**.

**Note**: You must ensure that the replicated item is removed first before you can delete the vault.

#### Task 5: Remove the lab environment

1. On MIA-CL1, close all open windows without saving any files.
2. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Run as Administrator**. In the User Account Control dialog box, click **Yes**.
3. Type the following command, and then press **Enter**:

Remove-20533EEnvironment

1. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
2. If you have multiple Azure subscriptions, select the one you want the script to target.
3. If prompted, specify the current lab number.
4. When prompted for confirmation, type **y**.
5. Start Microsoft Edge, browse to the Azure portal at [**https://portal.azure.com**](https://portal.azure.com), and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
6. In the Azure portal, on Dashboard, click **Edit**.
7. Right-click unoccupied area of the dashboard and, in the right-click menu, click **Reset to default state**. When prompted to confirm, click **Yes**.
8. Click **Done customizing**.
9. Close all open windows.

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