# Module 8: Planning and implementing backup and disaster recovery

# Lab A: Implementing Azure Backup and Azure Site Recovery

### Scenario

Adatum wants to evaluate the ability of Azure Backup to protect the content of on-premises computers and Azure IaaS virtual machines. A. Datum Corporation also wants to evaluate Azure Site Recovery for protecting Azure VMs.

### Objectives

At the end of this lab, you will be able to:

* Implement Azure Backup.
* Implement Azure Site Recovery–based protection of Azure VMs

### Lab Setup

Estimated Time: 60 minutes

Virtual machine: **20533E-MIA-CL1**

User name: **Student**

Password: **Pa55w.rd**

## Exercise 1: Protecting data with Azure Backup

### Scenario

Adatum currently uses an on-premises backup solution. As part of your Azure evaluation, you want to test the protection of on-premises master copies of your image files and invoices by backing them up to the cloud. To accomplish this, you intend to use Azure Backup.

The main tasks for this exercise are as follows:

1. Create a recovery services vault
2. Configure the vault for on-premises backup
3. Install and configure the Azure Recovery Services Agent
4. Create a backup schedule
5. Run a backup
6. Perform a restore
7. Disable backups and delete the vault

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

1. In Internet Explorer, open the Azure portal.
2. Create a new recovery services vault with the following settings:

* Name: **vault20533E0801**
* Subscription: the name of your Azure subscription
* Resource group: create a new resource group named **20533E0802-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 Azure portal, in the newly created vault, configure the backup goal with 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. Download the **Microsoft Azure Recovery Services Agent** from the Azure portal and install it on MIA-CL1 with the default settings.
2. Download the vault credentials file from the Azure portal
3. Register MIA-CL1 with the vault. Prior to registration, generate a passphrase and store it in the **F:\Labfiles\Lab08\Starter** folder.
4. At the end of the registration process, start the Azure Backup console and leave it open for the next task.

#### Task 4: Create a backup schedule

1. Use Azure Backup to schedule a daily backup to run at 4:30 AM and protect the following subfolders in the **F:\Labfiles\Lab08\Starter** folder:

* **asset-images**
* **invoices**

1. Keep the default values for the other backup settings.

#### Task 5: Run a backup

1. From the Microsoft Azure Backup console, run an on-demand backup.
2. From the Azure portal, verify that MIA-CL1 is registered with the Recovery Services vault and note the most recent backup items, which should include files and folders on the F: drive.

#### Task 6: Perform a recovery

1. From the Microsoft Azure Backup console, initiate data recovery.
2. From the Recover Data Wizard, mount the backed up volume.
3. Use File Explorer to copy the content of the backed up directories to their original location, overwriting existing data
4. Unmount the backed up volume.

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

1. From the Azure portal, in the Recovery Services vault, delete references to **mia-cl1.**
2. From the Azure portal, delete the Recovery Services vault.

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

### Scenario

Adatum Corporation wants to test a disaster recovery of its Azure-based Azure VMs. As part of Adatum’s evaluation of integration with Microsoft Azure, you have been asked to use Site Recovery to configure the protection of your test Azure VM environment.

The main tasks for this exercise are as follows:

1. Create an Azure Recovery Services vault
2. Configure Azure VM replication
3. Review Azure VM replication settings
4. Disable replication of an Azure VM and delete the Azure Recovery Services vault
5. Remove the lab environment

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

1. On MIA-CL1, from the the Azure portal, create an Azure Recovery Services vault with the following settings:

* Name: **vault20533E0802**
* Subscription: the name of your Azure subscription
* Resource group: **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. On MIA-CL1, in the Azure portal, navigate to the blade of the newly provisioned Azure Recovery Services vault.
2. Enable replication with the following settings:

* Source: **Azure - PREVIEW**
* 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**
* 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. Wait until the replication is enabled. This might take about 15 minutes.

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

1. On MIA-CL1, in the Azure portal, navigate to the replicated item blade representing the Azure VM **20533E0801-vm1**.
2. On the replicated item 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**.
3. 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, disable replication of the Azure VM **20533E0801-vm1**.
2. Wait until the replication is disabled. This might take about 15 minutes.
3. From the Azure portal, delete the Recovery Services vault.

**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. Start **Windows PowerShell** as Administrator and, from the **Administrator: Windows PowerShell** window, run **Remove-20533EEnvironment**.
3. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. If you have multiple Azure subscriptions, select the one you want the script to target.
5. If prompted, specify the current lab number.
6. When prompted for confirmation, type **y**.
7. Start Microsoft Edge, browse to the Azure portal, and sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
8. In the Azure portal, reset the dashboard to the default state.
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.

**Question** Why did the lab not include failover and failback?

**Question** If you wanted to protect Azure VMs that reside behind an Azure load balancer, how would you configure your Site Recovery solution?

©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.