Lab: Implement Azure Site Recovery between Azure regions

All tasks in this lab are performed from the Azure portal

Lab files:

- **Labfiles\Module_07\Azure_Site_Recovery_Between_Regions\az-101-01_azuredeploy.json**
- **Labfiles\Module_07\Azure_Site_Recovery_Between_Regions\az-101-01_azuredeploy.parameters.json**

Scenario

Adatum Corporation wants to implement Azure Site Recovery to facilitate migration and protection of Azure VMs between regions

Objectives

After completing this lab, you will be able to:

- Implement Azure Site Recovery Vault
- Configure replication of Azure VMs between Azure regions by using Azure Site Recovery

Exercise 1: Implement prerequisites for migration of Azure VMs by using Azure Site Recovery

The main tasks for this exercise are as follows:

1. Deploy an Azure VM to be migrated by using an Azure Resource Manager template
2. Create an Azure Recovery Services vault

Task 1: Deploy an Azure VM to be migrated by using an Azure Resource Manager template

1. From the lab virtual machine, start Microsoft Edge, browse to the Azure portal at **http://portal.azure.com** and sign in by using a Microsoft account that has the Owner role in the Azure subscription you intend to use in this lab.
2. In the Azure portal, navigate to the **Create a resource** blade.
3. From the **Create a resource** blade, search Azure Marketplace for **Template deployment**.
4. Use the list of search results to navigate to the **Deploy a custom template** blade.
5. On the **Custom deployment** blade, click the **Build your own template in the editor** link. If you do not see this link, click **Edit template** instead.
6. From the **Edit template** blade, load the template file **Labfiles\Module_07\Azure_Site_Recovery_Between_Regions\az-101-01_azuredeploy.json**.

> **Note**: Review the content of the template and note that it defines deployment of an Azure VM hosting Windows Server 2016 Datacenter.

7. Save the template and return to the **Custom deployment** blade.
8. From the **Custom deployment** blade, navigate to the **Edit parameters** blade.
9. From the **Edit parameters** blade, load the parameters file **Labfiles\Module_07\Azure_Site_Recovery_Between_Regions\az-101-01_azuredeploy.parameters.json**.
10. Save the parameters and return to the **Custom deployment** blade.
11. From the **Custom deployment** blade, initiate a template deployment with the following settings:
    - Subscription: the name of the subscription you are using in this lab
    - Resource group: the name of a new resource group **az1010101-RG**
    - Location: the name of the Azure region which is closest to the lab location and where you can provision Azure VMs
    - Vm Name: **az1010101-vm**
    - Admin Username: **Student**
    - Admin Password: **Pa55w.rd1234**
    - Image Publisher: **MicrosoftWindowsServer**
    - Image Offer: **WindowsServer**
    - Image SKU: **2016-Datacenter-Server-Core-smalldisk**
    - Vm Size: **Standard_DS1_v2**

> **Note**: To identify Azure regions where you can provision Azure VMs, refer to **https://azure.microsoft.com/en-us/regions/offers/**
>
> **Note**: Do not wait for the deployment to complete but proceed to the next task. You will use the virtual machine **az1010101-vm** in the second exercise of this lab.

Task 2: Implement an Azure Site Recovery vault

1. In the Azure portal, navigate to the **Create a resource** blade.
2. From the **Create a resource** blade, search Azure Marketplace for **Backup and Site Recovery**.
3. Use the list of search results to navigate to the **Recovery Services vault** blade.
4. Use the **Recovery Services vault** blade, to create a Site Recovery vault with the following settings:
    - Subscription: the same Azure subscription you used in the previous task of this exercise
    - Resource group: the name of a new resource group **az1010102-RG**
    - Vault name: **vaultaz1010102**
    - Region: the name of an Azure region that is available in your subscription and which is different from the region you deployed the Azure VM in the previous task of this exercise.

      Note: Wait for the provisioning to complete. This should take about a minute.

5. In the Azure portal, navigate to the blade of the newly provisioned Azure Recovery Services vault **vaultaz1010102**.
6. From the **vaultaz1010102** blade, navigate to its **Properties** blade and then to the **Security Settings** blade.
7. On the **Security Settings** blade, disable **Soft Delete** and save the change.

Result: After you completed this exercise, you have initiated deployment of an Azure VM by using an Azure Resource Manager template and created an Azure Site Recovery vault that will be used to replicate content of the Azure VM disk files.

Exercise 2: Migrate an Azure VM between Azure regions by using Azure Site Recovery

The main tasks for this exercise are as follows:

1. Configure Azure VM replication
2. Review Azure VM replication settings

Task 1: Configure Azure VM replication

Note: Before you start this task, ensure that the template deployment you started in the first exercise has completed.

1. In the Azure portal, navigate to the blade of the newly provisioned Azure Recovery Services vault **vaultaz1010102**.
2. From the **vaultaz1010102** blade, click **Replicate** and configure the following replication settings:
    - Source: **Azure**
    - Source location: the same Azure region into which you deployed the Azure VM in the previous exercise of this lab
    - Azure virtual machine deployment model: **Resource Manager**
    - Source subscription: the same Azure subscription you used in the previous exercise of this lab
    - Source resource group: **az1010101-RG**
    - Virtual machines: **az1010101-vm**
    - Target location: the name of an **Azure region** that is available in your subscription and which is **different from the region you deployed an Azure VM** in the previous task. If possible, use the same Azure region into which you deployed the Azure Site Recovery vault.
    - Target resource group: **(new) az1010101-RG-asr**
    - Target virtual network: **(new) az1010101-vnet-asr**
    - Cache storage account: accept the default setting
    - Replica managed disks: **(new) 1 premium disk(s), 0 standard disk(s)**
    - Target availability sets: **Not Applicable**
    - Replication policy: the name of a new replication policy **12-hour-retention-policy**
    - Recovery point retention: **12 Hours**
    - App consistent snapshot frequency: **6 Hours**
    - Multi-VM consistency: **No**
3. From the **Configure settings** blade, initiate creation of target resources and wait until you are redirected to the **Enable replication** blade.
4. From the **Enable replication** blade, enable the replication.

Task 2: Review Azure VM replication settings

1. In the Azure portal, navigate to the **vaultaz1010102 - Replicated items** blade.
2. On the **vaultaz1010102 - Replicated items** blade, ensure that there is an entry representing the **az1010101-vm** Azure VM and verify that its **REPLICATION HEALTH** is **Healthy** and that its **STATUS** is **Enabling protection**.

> **Note**: You might need to wait a few minutes until the **az1010101-vm** entry appears on the **vaultaz1010102 - Replicated items** blade.

3. From the **vaultaz1010102 - Replicated items** blade, display the replicated item blade of the **az1010101-vm** Azure VM.
4. On the **az1010101-vm** replicated item blade, review the **Health and status**, **Failover readiness**, **Latest recovery points**, and **Infrastructure view** sections. Note the **Failover** and **Test Failover** toolbar icons.

> **Note**: The remaining steps of this task are optional and not graded.

5. If time permits, wait until the replication status changes to **100% synchronized**. This might take additional 90 minutes.
6. Examine the values of **RPO**, as well as **Crash-consistent** and **App-consistent** recovery points.
7. Perform a test failover to the **az1010101-vnet-asr** virtual network.

Result: After you completed this exercise, you have configured replication of an Azure VM and reviewed Azure VM replication settings.

Exercise 3: Remove lab resources

Task 1: Open Cloud Shell

1. At the top of the portal, click the **Cloud Shell** icon to open the Cloud Shell pane.
2. At the Cloud Shell interface, select **Bash**.
3. At the **Cloud Shell** command prompt, type in the following command and press **Enter** to list all resource groups you created in this lab:

   ShellCopy

```
az group list --query "[?starts_with(name,'az10101')].name" --output tsv
```

4. Verify that the output contains only the resource groups you created in this lab. These groups will be deleted in the next task.

Task 2: Delete resource groups

1. At the **Cloud Shell** command prompt, type in the following command and press **Enter** to delete the resource groups you created in this lab

ShellCopy

```
az group list --query "[?starts_with(name,'az10101')].name" --output tsv |
xargs -L1 bash -c 'az group delete --name $0 --no-wait --yes'
```

Note: If you encounter an error similar to "...cannot perform delete operation because following scope(s) are locked..." then you need to run the following steps to remove the lock on the resource that prevents its deletion:

ShellCopy

```
lockedresource=$(az resource list --resource-group az1010101-RG-asr --
resource-type Microsoft.Compute/disks --query
"[?starts_with(name,'az10101')].name" --output tsv)
az disk revoke-access -n $lockedresource --resource-group az1010101-RG-
asr
lockid=$(az lock show --name ASR-Lock --resource-group az1010101-RG-asr
--resource-type Microsoft.Compute/disks --resource-name $lockedresource
--output tsv --query id)
az lock delete --ids $lockid
az group list --query "[?starts_with(name,'az10101')].name" --output tsv
| xargs -L1 bash -c 'az group delete --name $0 --no-wait --yes'
```

2. Close the **Cloud Shell** prompt at the bottom of the portal.