**Module 5: Designing and implementing Azure Site Recovery solutions**

**Lab: Implementing protection of on-premises Hyper-V virtual machines in Azure by using Site Recovery**

**Exercise 1: Preparing an Azure subscription for implementing Site Recovery**

**Task 1: Create an Azure virtual network**

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, click **+ Create a resource**.
4. On the **New** blade, click **Networking** and then, click **Virtual network**.
5. On the **Create virtual network** blade, specify the following settings and click **Create**:

* Name: **WinGovm5XX-vnet**
* Address space: **10.5.0.0/20**
* Subscription: select the name of the Azure subscription you will be using in this lab
* Resource group: ensure that the **Create new** option is selected and type **WinGovm5XX-LabRG** as the name of the new resource group
* Location: select the name of any Azure region where you can provision a Recovery Services vault
* Subnet: **subnet-0**
* Address range: **10.5.0.0/24**
* Service endpoints (Preview): **Disabled**
* Pin to dashboard: Leave the checkbox unchecked

1. Do not wait until the virtual network is provisioned. Instead, proceed directly to the next task.

**Task 2: Create an Azure storage account**

1. In the browser window, in the Azure portal, in the hub menu on the left-hand side, click **+ Create a resource**.
2. On the **New** blade, click **Storage** and then click **Storage account - blob, file, table, queue**.
3. On the **Create storage account** blade, specify the following settings, and then click **Create**:

* Name: **wingovm5XXsa** (a unique name between 3 and 24 characters in length, which can include lowercase letters and digits)
* Deployment model: **Resource Manager**
* Account kind: **Storage (general purpose v1)**
* Performance: **Standard**
* Replication: **Locally-redundant storage (LRS)**
* Secure tansfer required: **Disabled**
* Subscription: the same Azure subscription you selected in the previous task
* Resource group: ensure that the **Use existing** option is selected and then select **WinGovm5XX-LabRG** in the drop-down list
* Location: the same Azure region that you selected in the previous task
* Configure virtual networks: **Disabled**
* Pin to dashboard: leave unchecked

1. Wait until the storage account is provisioned before proceeding to the next task.

**Task 3: Create a Recovery Services vault**

1. In the Azure portal, in the hub menu on the left hand side, click **+ Create a resource**.
2. On the **New** blade, click **Monitoring + Management** and then click **Backup and Site Recovery (OMS)**.
3. On the **Recovery Services vault** blade, specify the following settings and then click **Create**:

* Name: **RSWinGovm5XX-vault**
* Subscription: the same Azure subscription you selected in the previous task
* Resource group: ensure that the **Use existing** option is selected and then select **WinGovm5XX-LabRG** in the drop-down list
* Location: the same Azure region that you selected in the previous task
* Pin to dashboard: leave the checkbox unchecked

1. Wait for the vault to be provisioned before proceeding to the next step. This should take less than a minute.

**Task 4: Configure the Recovery Services vault protection goals**

**MUST be done from a server. *Nested Virtualization on Server VM,* then create empty vm in Hyper-V manager named VM1**

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 **RSWinGovm5XX-vault**.
4. On the **RSWinGovm5XX-vault** blade, in the **GETTING STARTED** section, click **Site Recovery**.
5. On the **Site Recovery** blade, click **Prepare Infrastructure**.
6. On the **Protection goal** blade, specify the following settings, and then click **OK**:
7. Where are your virtual machines located?: **On-premises**
8. Where do you want to replicate your machines to?: **To Azure**
9. Are your machines virtualized?: **Yes, with Hyper-V**
10. Are you using System Center VMM to manage your Hyper-V hosts?: **No**
11. On the **Deployment planning** blade, in the **Have you completed deployment planning** drop down list, select **Yes, I have done it**, and then click **OK**.

**Result**: After you completed this exercise, you should have successfully created an Azure virtual network, created an Azure storage account, created a Recovery Services vault, and configured the Recovery Services vault protection goals.

**Exercise 2: Preparing a Hyper-V host for the implementation**

**Task 1: Enable the Windows Update service**

1. On the host computer, right-click **Start**, and then click **Computer Management**.
2. In the **Computer Management** console, expand the **Services and Applications** node, and then click **Services**.
3. In the list of services, right-click **Windows Update**, and then click **Properties**.
4. In the **Windows Update Properties (Local Computer)** dialog box, select **Manual** in the **Startup type** drop-down list, and then click **OK**.
5. Close the **Computer Management** console.

**Task 2: Install the Azure Site Recovery Provider and the Azure Site Recovery Services agent**

1. In the Azure portal, within the Internet Explorer window, on the **Prepare source** blade, click **+ Hyper-V Site**.
2. On the **Create Hyper-V site** blade, type **WinGovm5XX-LabSite**, and then click **OK**.
3. On the **Prepare source** blade, click **+ Hyper-V Server**.
4. On the **Add Server** blade, review the list of steps to add Hyper-V server. Click the **Download** link in step **3. Download the installer for the Microsoft Azure Site Recovery Provider**.
5. When you receive a prompt asking whether to run or save **AzureSiteRecoveryProvider.exe**, click **Run**.
6. In the **Azure Site Recovery Provider Setup (Hyper-V server)** window, on the **Microsoft Update** page, click **Off**, and then click **Next**.
7. On the **Installation** page, accept the default installation location, and then click **Install**.
8. Wait for the installation to complete, and then click **Register**. This will launch the **Microsoft Azure Site Recovery Registration Wizard**.

**Task 3: Register the Hyper-V host with the Recovery Services vault.**

1. Switch to the browser window that is showing the **Add Server** blade in the Azure portal.
2. On the **Add Server** blade, click the **Download** command button in step **4. Download the vault registration key to register the host in a Hyper-V site**. Ensure that **WinGovm5XX-LabSite** appears in the drop-down list.
3. When you receive a prompt asking whether to open or save the vault credentials file, click **Save**.
4. Switch to the **Microsoft Azure Site Recovery Registration Wizard** window.
5. On the **Vault Settings** page, click **Browse** next to the **Key file** entry.
6. In the **Open** dialog box, browse to the **Downloads** folder, click the vault credentials file you just downloaded, and then click **Open**.
7. Click **Next**.
8. On the **Proxy Settings** page, click **Next**.
9. Wait until the registration completes successfully, and then click **Finish**.

**Note:** It might take between 15 and 30 minutes before the Hyper-V server appears in the Azure portal.

1. Switch to the Internet Explorer window, showing the **Add Server** blade in the Azure portal.
2. Close the **Add Server** blade and then close the **Prepare source** blade.
3. In the dialog box displaying the message **Your unsaved edits will be discarded**, click **OK**.
4. Back in the **Prepare infrastructure** blade, click **3 Source Prepare**.
5. On the **Prepare source** blade, verify that **WintellectSRV** is listed under **Step 2: Ensure Hyper-V servers are added**, and then click **OK**. This will automatically display the **Target** blade. If you do not see **WintellectSRV** appearing on the **Prepare source** blade under **Step 2: Ensure Hyper-V servers are added**, wait for five minutes, and then repeat steps 11 to 14.

**Result**: After you completed this exercise, you should have successfully installed the Azure Site Recovery Provider and the Azure Site Recovery Services agent as well as registered the Hyper-V host with the Recovery Services vault.

**Exercise 3: Configuring Site Recovery protection of a Hyper-V virtual machine**

**Task 1: Verify the existence of a Site Recovery target storage account and virtual network**

1. On the host computer, in the Azure portal, on the **Target** blade, verify that your Azure subscription is listed in the **Subscription** drop-down list and that the **Resource Manager** appears in the **Select the deployment model used after failover** drop-down list.
2. Verify that there is a green checkbox next to **Step 2: Ensure that at least one compatible Azure storage account exist**.
3. Verify that there is a green checkbox next to **Step 3: Ensure that at least one compatible Azure virtual network exist**.
4. Click **OK**. This will automatically open the **Replication policy** blade.

**Task 2: Create and associate a Site Recovery replication policy with the Hyper-V host**

1. In the Azure portal, on the **Replication policy** blade, click **+ Create and Associate**.
2. On the **Create and associate policy** blade, specify the following settings, and then click **OK**:
   1. Name: **WinGovm5XX-LabASRPolicy**
   2. Source type: **Hyper-V**
   3. Target type: **Azure**
   4. Copy frequency: **5 minutes**
   5. Recovery point retention in hours: **2**
   6. App-consistent snapshot frequency in hours: **1**
   7. Initial replication start time: choose the time 12 hours ahead of the current time.
   8. Associated Hyper-V site: **WinGovm5XX-LabSite**.
3. Wait for the replication policy to be created and associated with the **WinGovm5XX-LabSite**. After both steps complete successfully, as indicated by two checkmarks in green circles with a white checkmark appearing on the **Replication policy** blade, click **OK**.
4. Back on the **Prepare infrastructure** blade, click **OK**. This will bring you back to the **RSWinGovm5XX-vault - Site Recovery** blade.

**Task 3: Configure and enable virtual machine replication**

1. In the Azure portal, in the Internet Explorer window that is showing the **RSWinGovm5XX-vault - Site Recovery** blade, click **Step 1: Replicate Application**. This will automatically open the **Enable replication** blade and the **Source** blade.
2. On the **Source** blade, ensure that **On premises** appears in the **Source** drop down list and **WinGovm5XX-LabSite** appears in the **Source** drop-down list, and then click **OK**.
3. In the **Target** blade, specify the following settings:
   1. Target: **Azure**
   2. Subscription: the name of your Azure subscription
   3. Post-failover resource group: **WinGovm5XX-LabRG**
   4. Post-failover deployment model: **Resource Manager**
4. Click **Storage account**.
5. On the **Choose storage account** blade, click the storage account you created in the first exercise of this lab.
6. Ensure that **Configure now for selected machines** appears in the **Azure network** drop-down list.
7. Click **Post-failover Azure network**.
8. In the **Choose virtual network** blade, click **WinGovm5XX-vnet**.
9. In the **Subnet** drop-down list, select **subnet-0 (10.5.0.0/24)**.
10. Click **OK**.
11. On the **Select virtual machines** blade, select the checkbox next to the **VM1** entry representing the virtual machine guest on the lab virtual machine, and then click **OK**.
12. On the **Configure properties** blade, in the **Defaults** row, select **Windows** in the **OS TYPE** drop-down list, and then click **OK**.
13. On the **Configure replication settings** blade, verify that the **WinGovm5XX-LabASRPolicy** appears in the **Replication policy** drop-down list, and then click **OK**.
14. Back on the **Enable replication** blade, click **Enable replication**.

**Task 4: Create a recovery plan.**

1. In the Azure portal, in the Internet Explorer window that is showing the **RSWinGovm5XX-vault - Site Recovery** blade, click **Step 2: Manage Recovery Plans**. This will automatically open the **Recovery plans** blade.
2. On the **Recovery plans** blade, click **+ Recovery plan**.
3. On the **Create recovery plan** blade, specify the following settings:
   1. Name: **WinGovm5XX-LabRecoveryPlan**
   2. Source: **WinGovm5XX-LabSite**
   3. Target: **Microsoft Azure**
   4. Allow items with deployment model: **Resource Manager**
4. Click **Select items**.
5. On the **Select items** blade, enable the checkbox next to the **VM1** entry representing the virtual machine guest on the lab virtual machine, and then click **OK**.
6. Back on the **Create recovery plan** blade, click **OK**.
7. Wait for the recovery plan to be created. This should take less than a minute. The new recovery plan should appear on the **Recovery plans** blade.

**Task 5: Identify and delete all lab Azure resources**

1. In the Azure portal, navigate to the **RSWinGovm5XX-vault** blade.
2. In the **PROTECTED ITEMS** section of the **RSWinGovm5XX-vault** blade, click **Replicated items**.
3. On the **Replicated items** blade, click the ellipsis to the right of the **VM1** entry and then, in the drop-down menu, click **Disable Replication**.
4. On the **Disable Replication** blade, in the **Remove replicated items** drop down list, select **Disable replication and remove (Recommended)** and click **OK**. Wait for the operation to complete. This should take less than a minute.
5. Scroll back to the **RSWinGovm5XX-vault** blade.
6. In the **MANAGE** section of the **RSWinGovm5XX-vault** blade, click **Site Recovery Infrastructure**.
7. On the **Site Recovery Infrastructure** blade, click **Hyper-V Hosts**.
8. On the **Servers** blade, click ellipsis to the right of the entry that represents your host computer and then, in the drop-down menu, click **Delete**. When prompted for confirmation, click **OK**.

**Note:** Disregard any error messages indicating that **Deleting Hyper-V server** operation failed.

1. Navigate back to the **RSWinGovm5XX-vault** blade and click **Overview**.
2. On the **RSWinGovm5XX-vault** blade, click **Delete**.
3. When prompted for confirmation, click **Yes**.
4. In the hub menu of the Azure portal, click **Resource groups**.
5. On the **Resource groups** blade, click ellipsis next to the **WinGovm5XX-LabRG** blade and, in the drop-down menu, click **Delete resource group**.
6. On the **Are you sure you want to delete "WinGovm5XX-LabRG"** blade, in the **TYPE THE RESOURCE GROUP NAME** text box, type the name of the resource group, and then click **Delete**.
7. Close all open windows.