Module 12 Lab 1: Protecting Hyper-V VMs by using Azure Site Recovery

Exercise 1: Preparing the Azure Environment for Azure Site Recovery

ASR helps keep your business apps up and running during planned and unplanned outages. ASR manages and orchestrates disaster recovery of on-premises machines and Azure virtual machines (VMs), including replication, failover, and recovery.

In this practice, you will:

- Verify that your Azure account has replication permissions.
- Create an Azure storage account. Images of replicated machines are stored in it.
- Create a Recovery Services vault. A vault holds metadata and configuration information for VMs, and other replication components.
- Set up an Azure network. When Azure VMs are created after failover, they're joined to this Azure network.

Task 1: Verify account permissions

You already have an Azure Subscription and you're the administrator of your subscription. If were not the subscription administrator, work with the administrator to assign the permissions you need. To enable replication for a new virtual machine, you must have permission to:

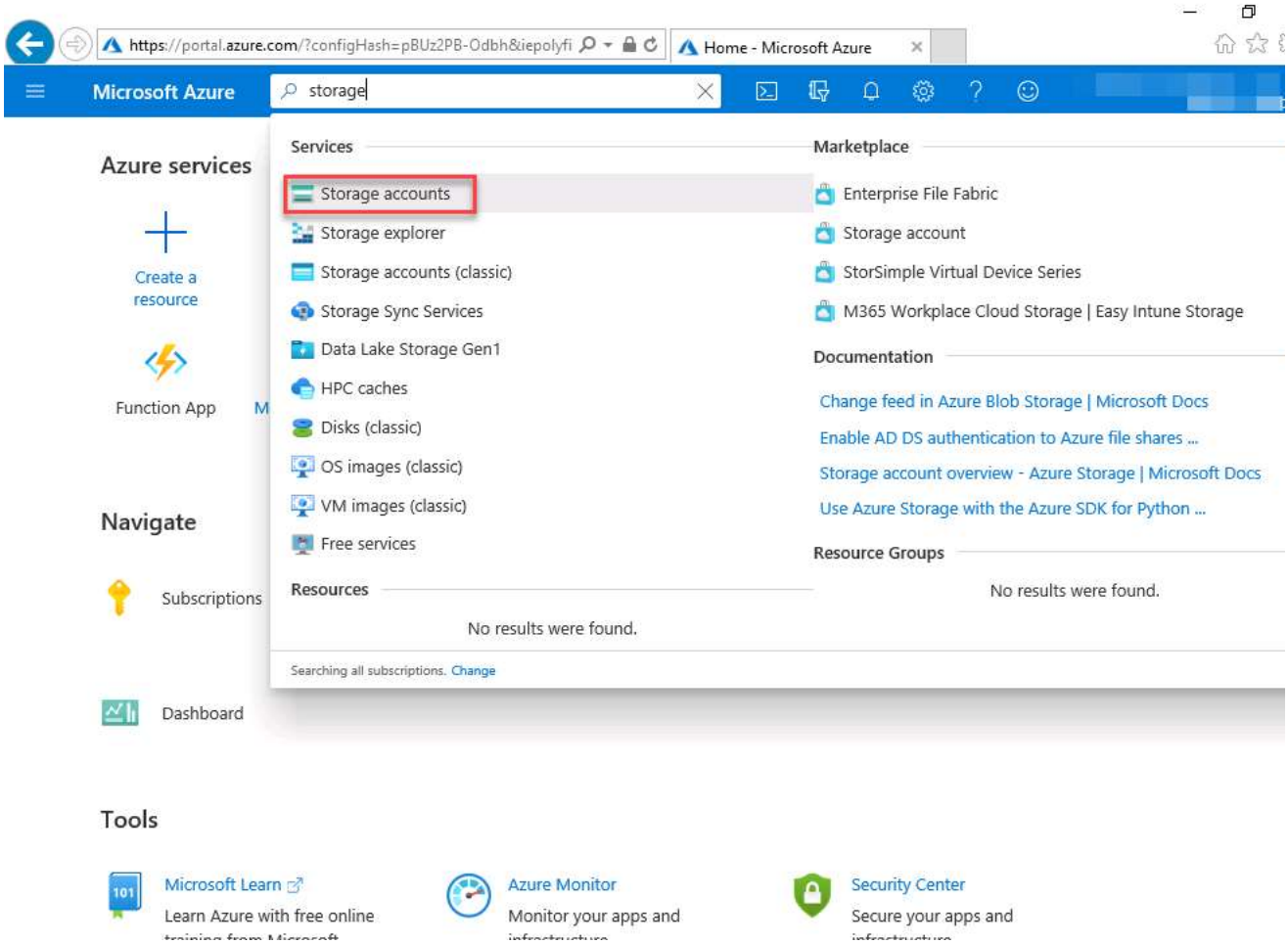
- Create a VM in the selected resource group.
- Create a VM in the selected virtual network.
- Write to the selected storage account.

To complete these tasks your account should be assigned the Virtual Machine Contributor built-in role. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor build-in role.

Task 2: Create a storage account

Images of replicated machines are held in Azure storage. Azure VMs are created from the storage when you fail over from on-premises to Azure. The storage account must be in the same region as the Recovery Services vault. We're using **EastUS** in this task.

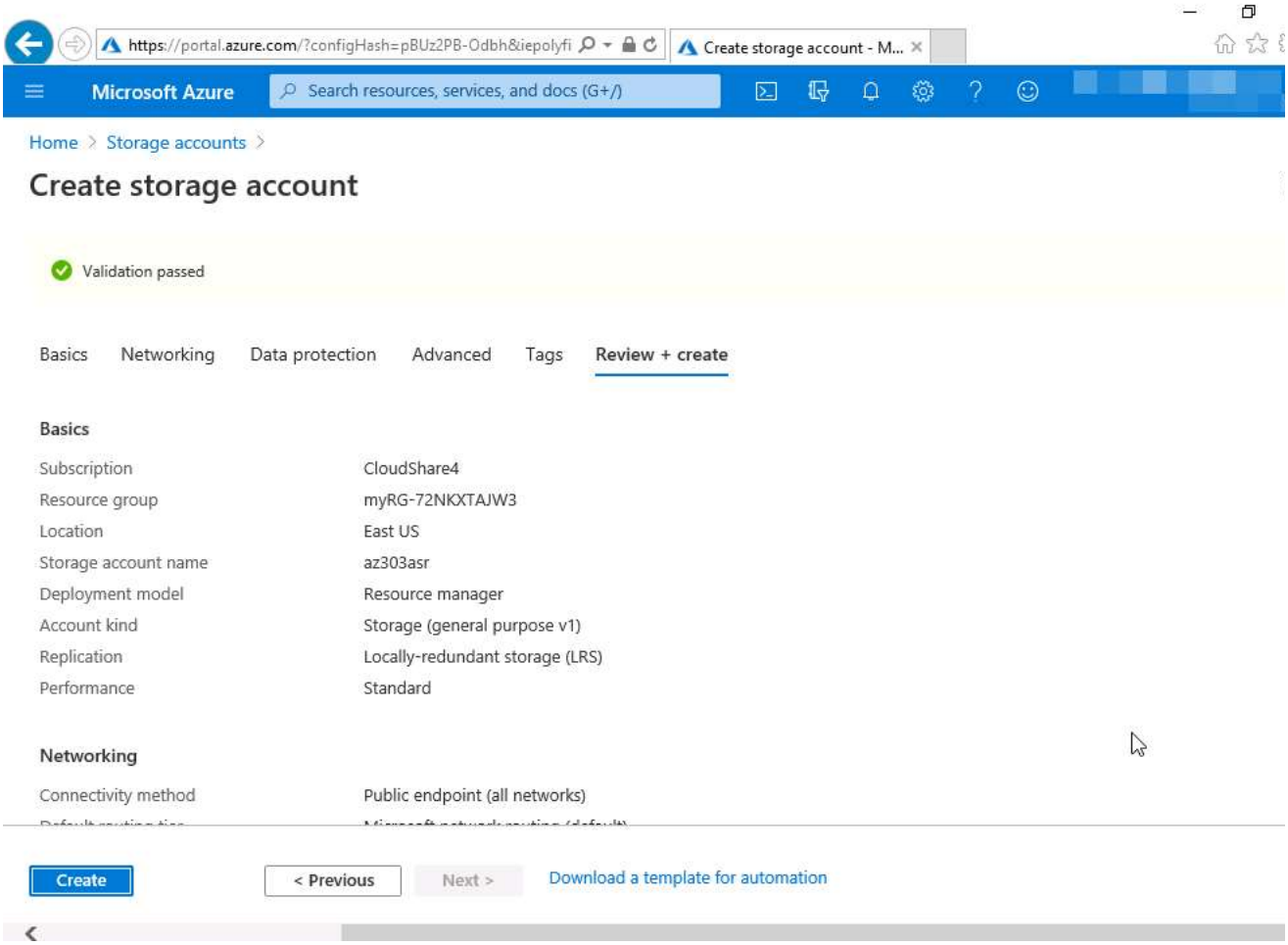
- [ ] 1. On **LON-HV1** virtual machine and send the **CTRL+ALT+DEL** command. Login using the username **Administrator** and password **Pa55w.rd**
- [ ] 2. Open a browser and navigate to the **Azure Portal** **https://portal.azure.com** and login with username **sheikhnasirLJTC0@gdcs4.com** and password **exIIPgiecfNyVk3R**
- [ ] 3. Search for and select **Storage accounts**.



- [ ] 4. Select + **Create**.
- [ ] 5. On **Create storage account** blade under **Resource Group** select **myRG-T17DSTITVP**.
- [ ] 6. Scroll down to the Storage account name field and enter a name for the account. *The name you select must be unique within Azure and be between 3 and 24 characters, with numbers and lowercase letters only.*
- [ ] 7. In **Region**, select **East US**.
- [ ] 8. In **Performance**, select **Standard**
- [ ] 9. In **Redundancy**, select **Locally-redundant storage (LRS)**
- [ ] 10. In the **Data Protection** tab uncheck the below options:

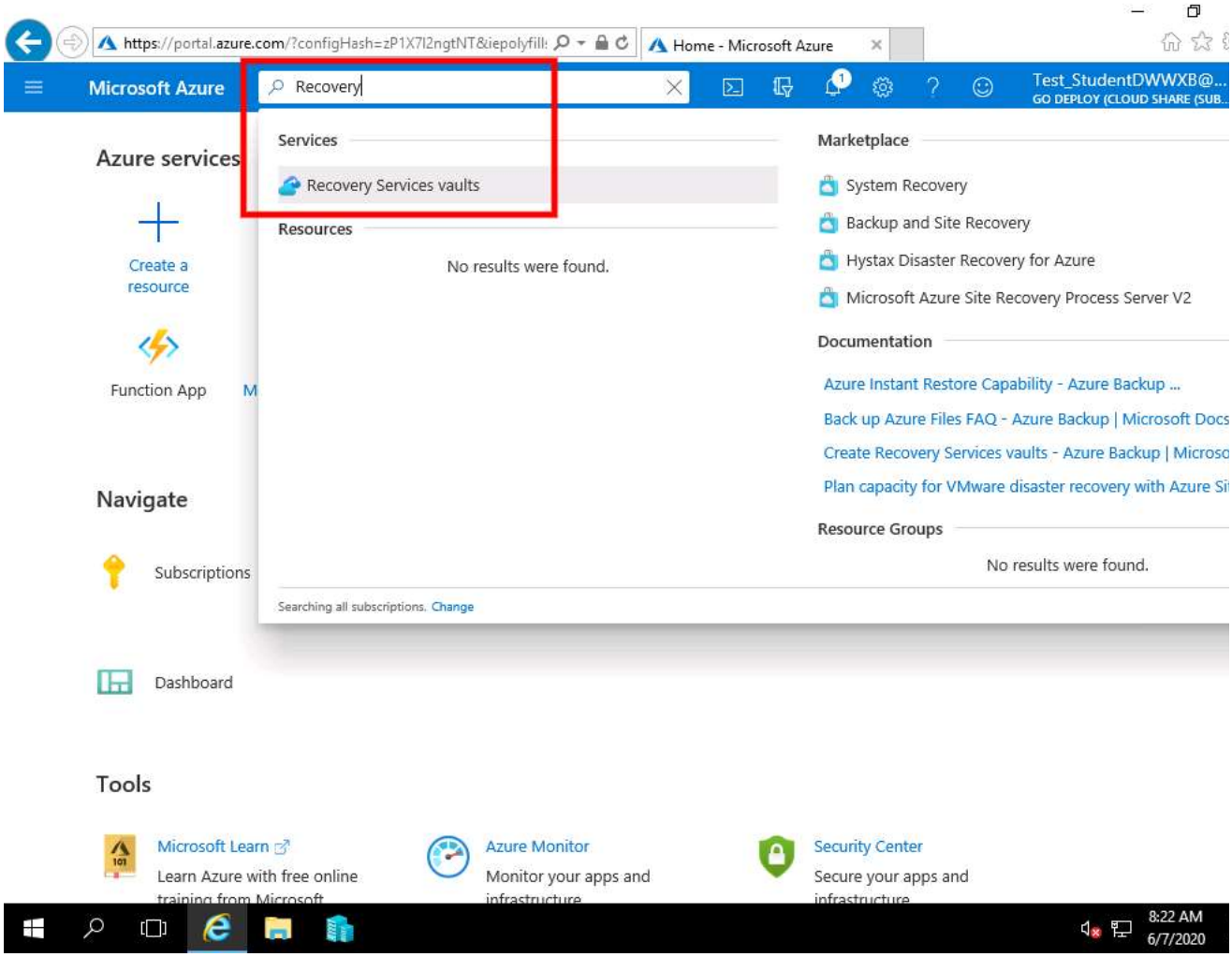
    - **Enable Soft Delete for Blobs**
    - **Enable Soft Delete for Containers**
    - **Enable Soft Delete for File shares**

- [ ] 9. Select **Review + Create**.
- [ ] 10. On the Validation screen click **Create**.

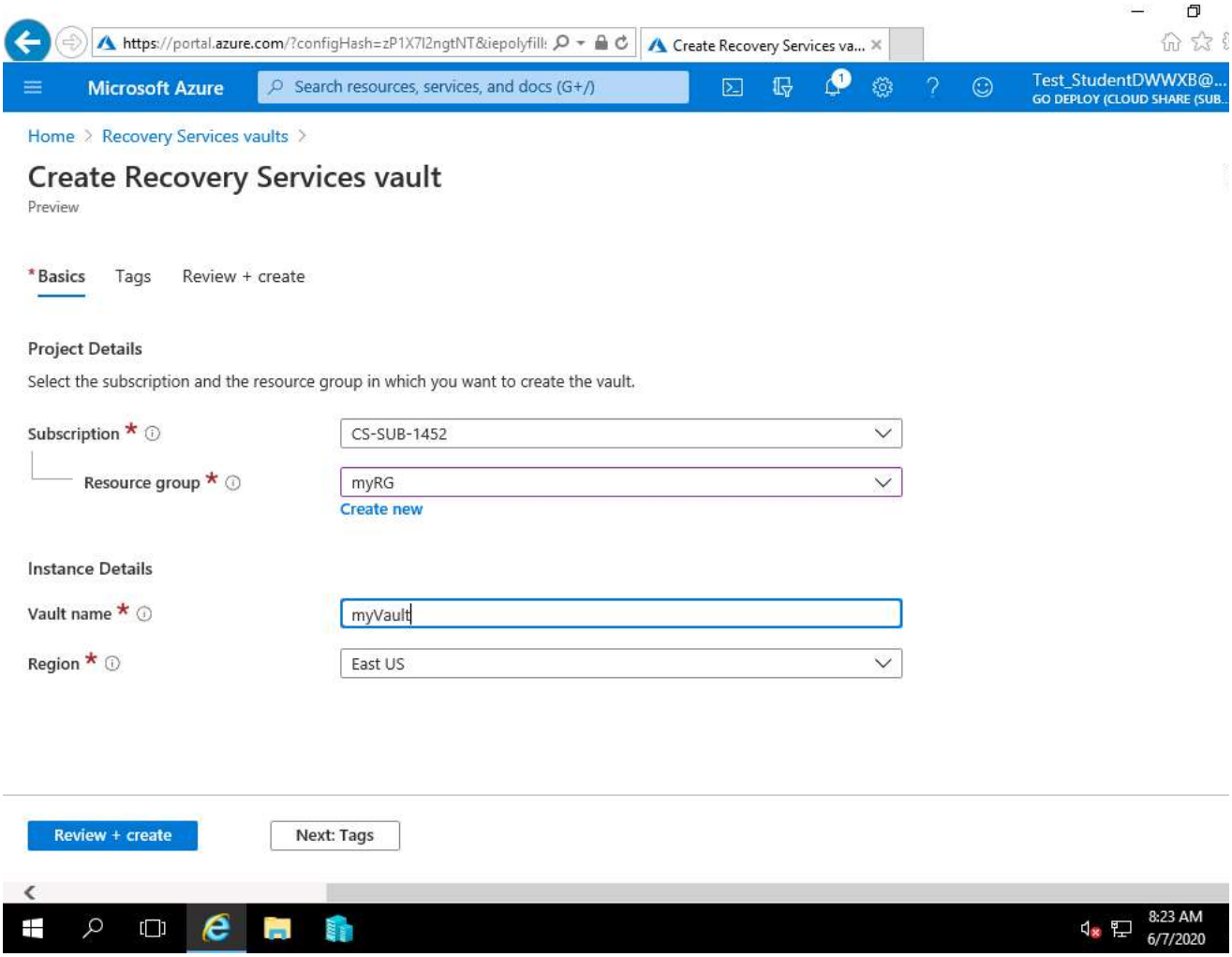


Task 3: Create a Recovery Services vault

- [ ] 1. In the Azure portal, search for and select **Recovery Services vaults**.



- [ ] 2. Click + **Create**.
- [ ] 3. In **Resource group**, select **myRG-T17DSTITVP**
- [ ] 4. In **Name**, enter a friendly name of myVault to identify the vault.
- [ ] 5. In **Location** select **East US**.

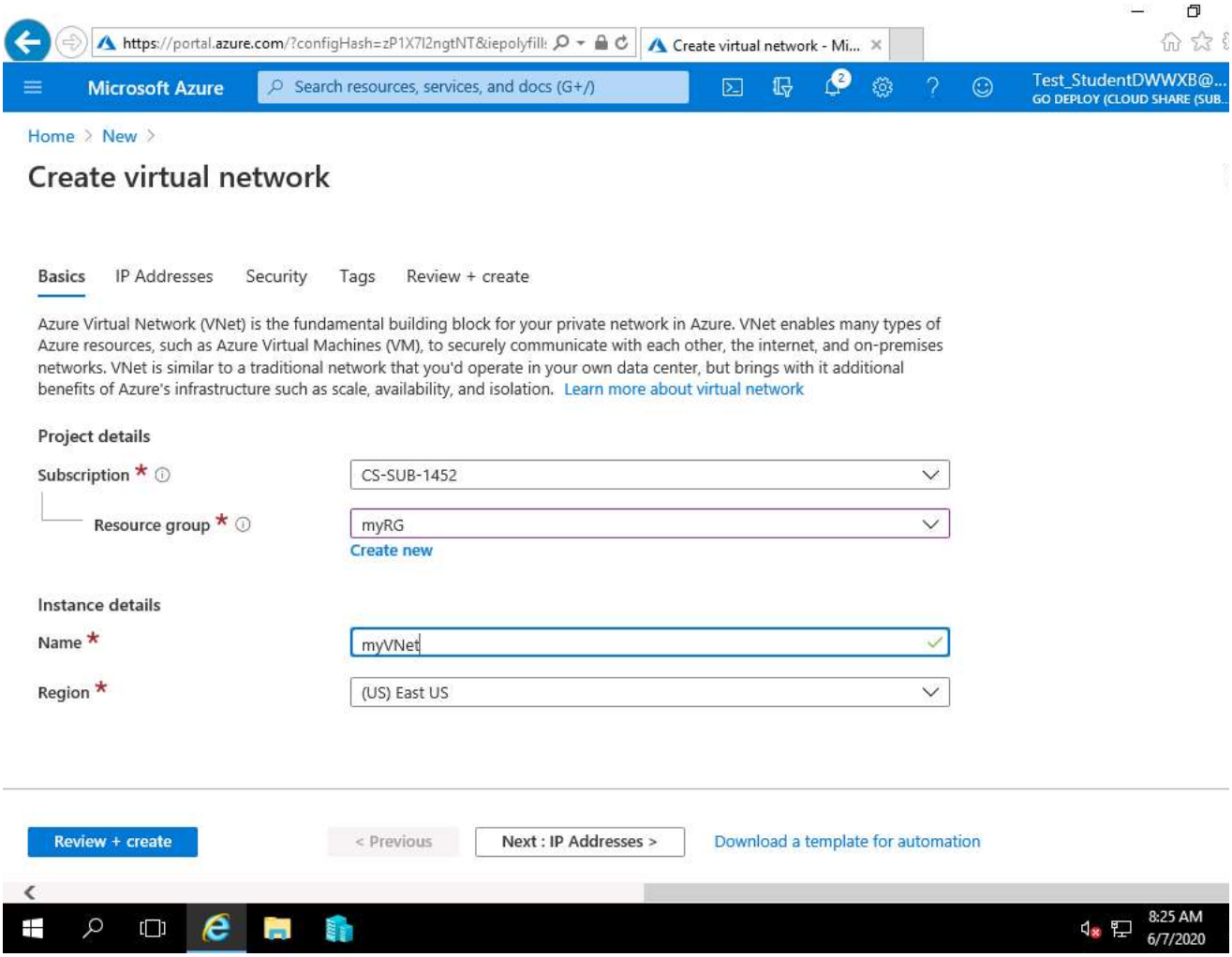


- [ ] 6. Click **Review + create** then select **Create**.

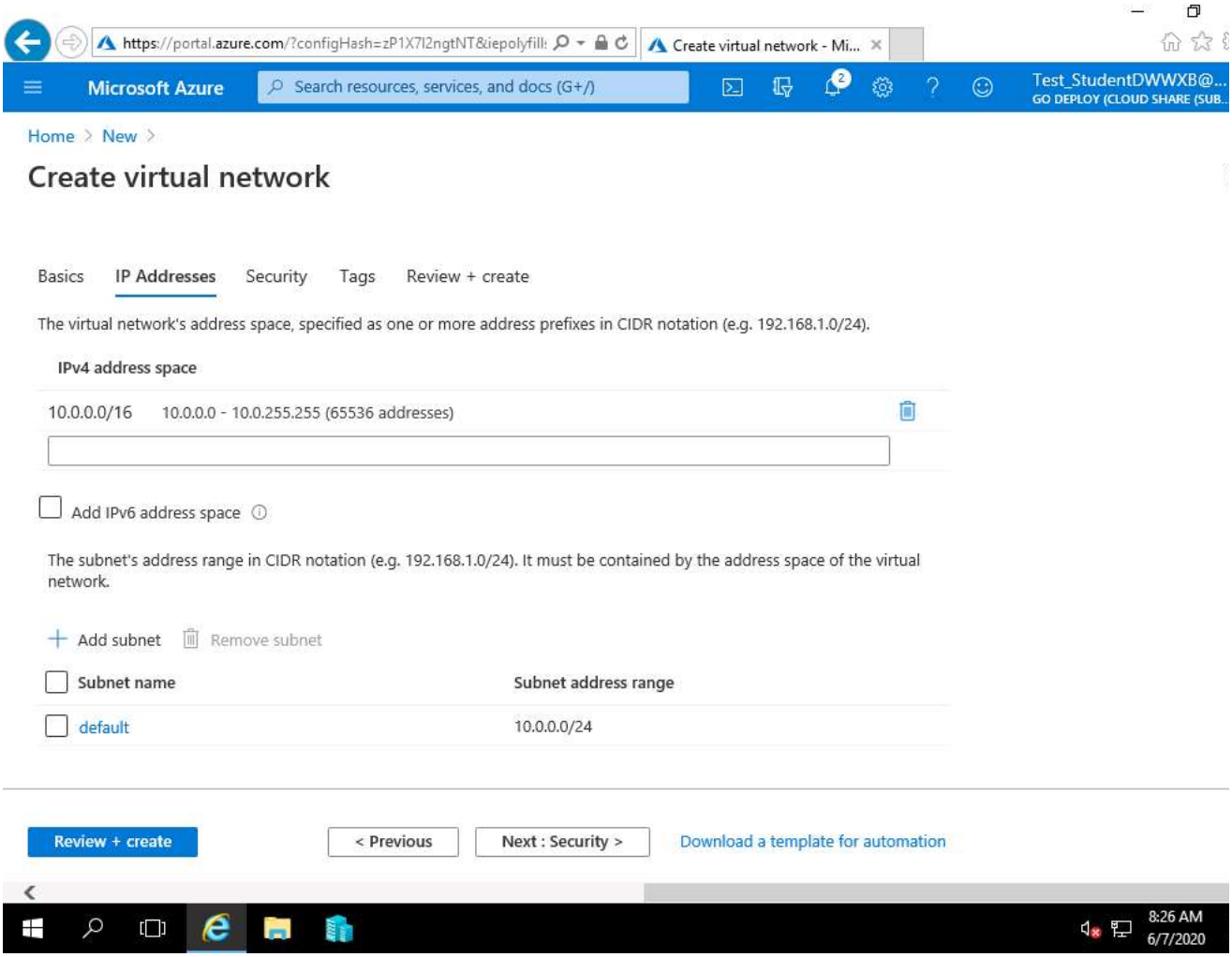
Task 4: Set up an Azure network

When Azure VMs are created from storage after failover, they're joined to this network.

- [ ] 1. In the Azure portal, select **Create a resource** > **Networking** > **Virtual network**.
- [ ] 2. Select **+Create**
- [ ] 3. In **Subscription**, select your subscription.
- [ ] 4. Select the resource group **myRG-T17DSTITVP**
- [ ] 5. In **Name**, enter myVNet
- [ ] 6. In **Location**, select **East US**. The network must be in the same region as the Recovery Services vault.



- [ ] 7. Select the **IP Addresses** tab.
- [ ] 8. In **Address range**, enter the range for the network 10.0.0.0/16.
- [ ] 9. In **Subnet**, enter the range for the subnet 10.0.0.0/24.



10. Click **Review + create** then click **Create**.

> ⚠ The virtual network takes a few seconds to create.

Task 5: Prepare to connect to Azure VMs after failover

> ⚠ **Note**: These steps have already been carried out in the lab environment for you and no configuration is necessary, this section is informational.

During a failover scenario you may want to connect to your replicated on-premises network.

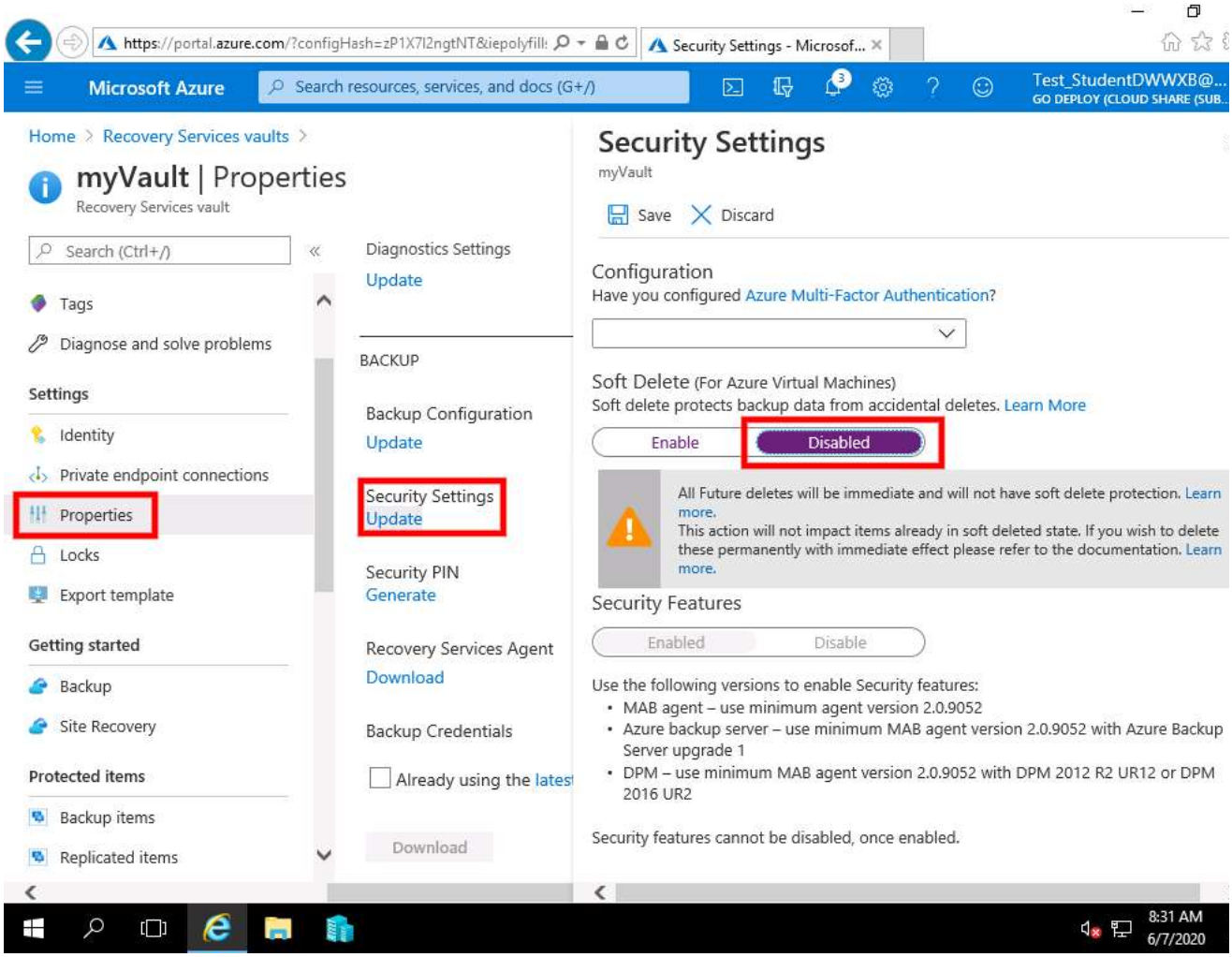
To connect to Windows VMs using RDP after failover, allow access as follows:

- To access over the internet, enable RDP on the on-premises VM before failover. Make sure that TCP, and UDP rules are added for the Public profile, and that RDP is allowed in Windows Firewall > Allowed Apps for all profiles.
- To access over site-to-site VPN, enable RDP on the on-premises machine. RDP should be allowed in the Windows Firewall -> Allowed apps and features for Domain and Private networks. Check that the operating system's SAN policy is set to OnlineAll. Learn more. There should be no Windows updates pending on the VM when you trigger a failover. If there are, you won't be able to log in to the virtual machine until the update completes.
- On the Windows Azure VM after failover, check Boot diagnostics to view a screenshot of the VM. If you can't connect, check that the VM is running and review these troubleshooting tips.

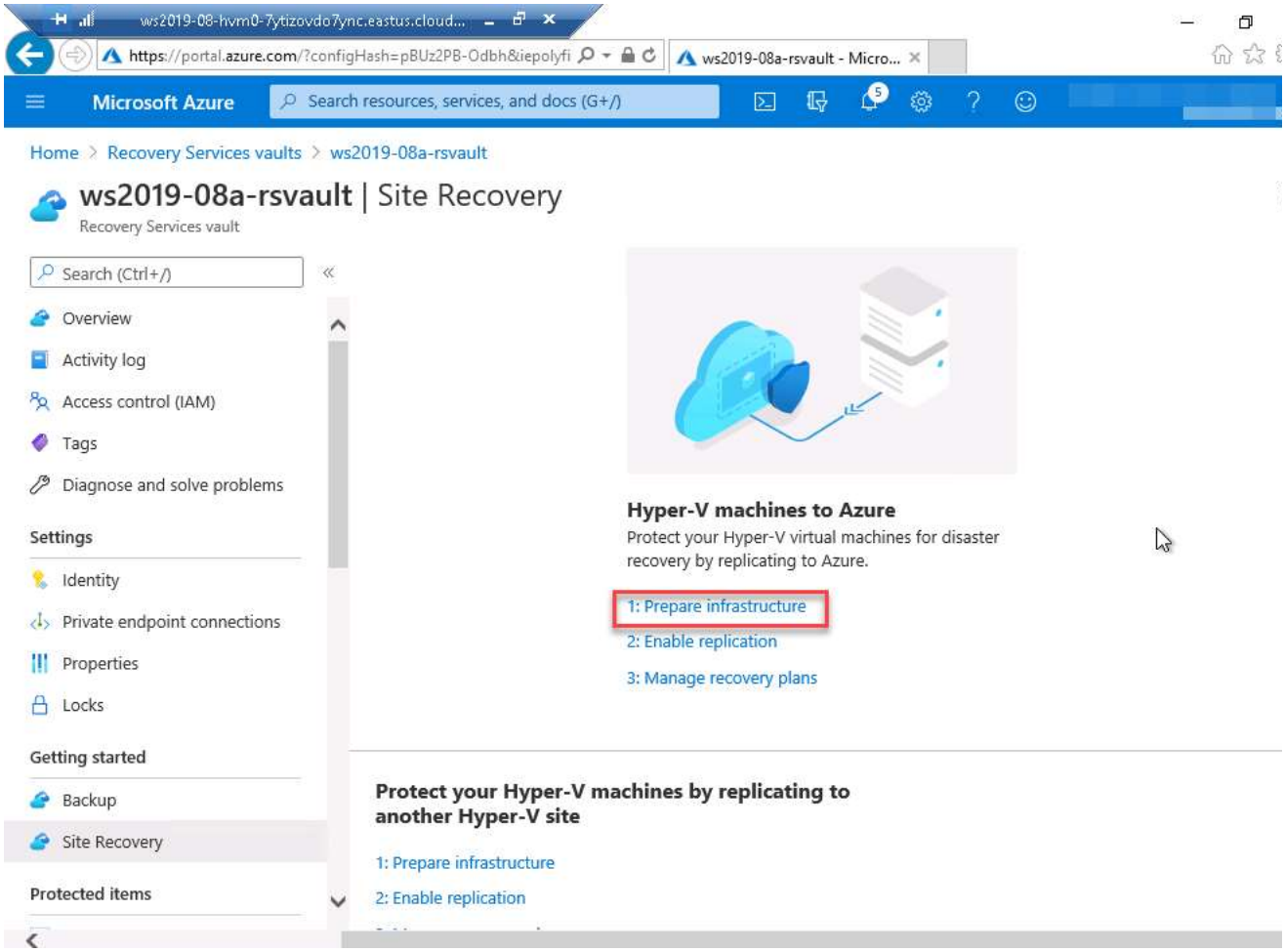
Exercise 2: Set up disaster recovery of on-premises Hyper-V VMs to Azure

Task 1: Select a replication goal

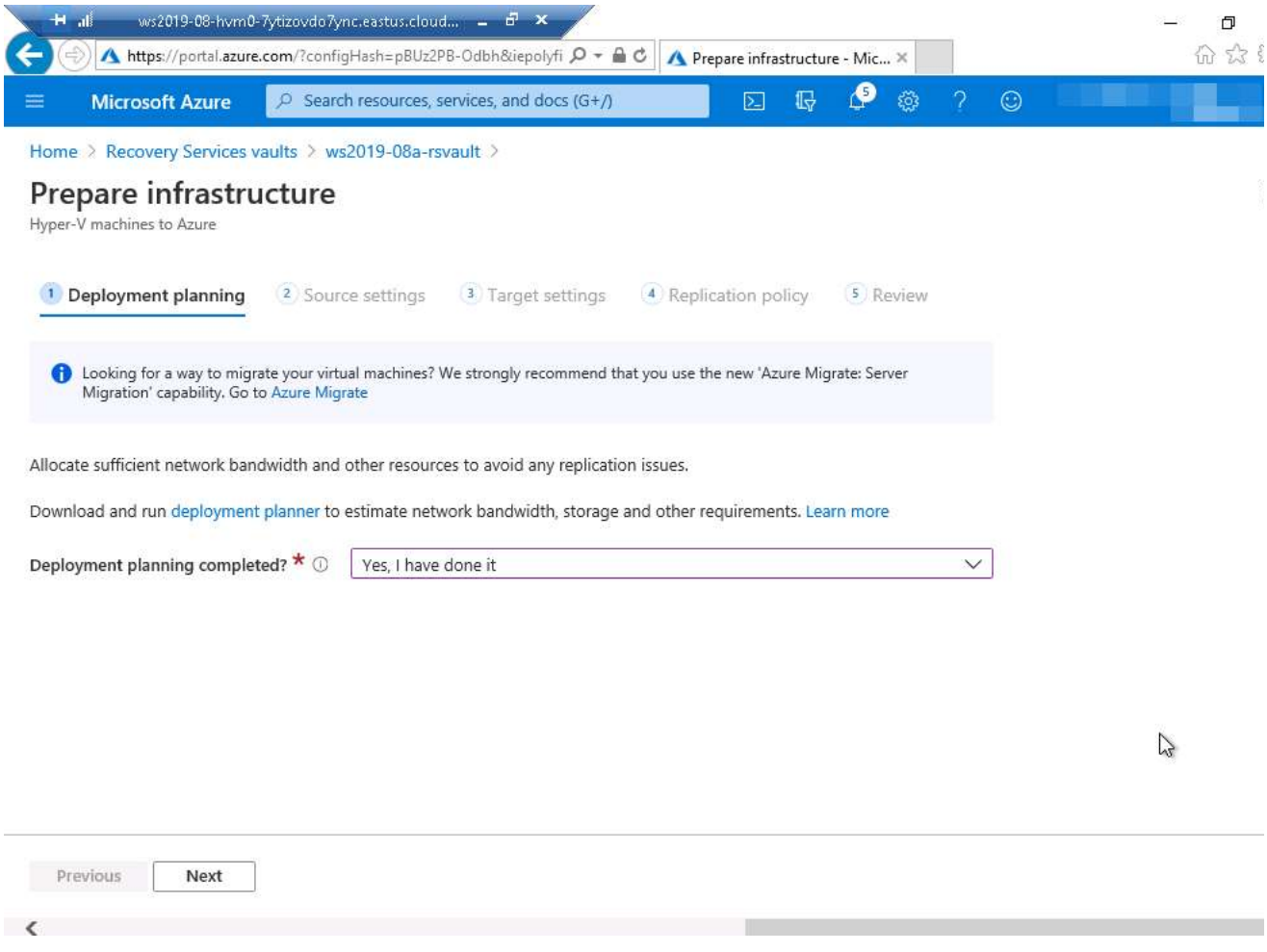
1. In the Azure portal, select **All Services** > **Recovery Services vaults**, select the vault that was prepared in the previous task, **myVault**.
2. On the Recovery Services vault blade, select **Settings** -> **Properties**.
3. In the properties pane, select **Security Settings** -> **Update**.
4. In the security settings pane, under **Soft Delete**, select **Disabled**.



- [ ] 5. Click **Save**
- [ ] 6. On the **MyVault** blade, in the vertical menu, in the **Getting started** section, select **Site Recovery**
- [ ] 7. On the **MyVault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **1. Prepare infrastructure**.



- [ ] 8. On the **Deployment planning** tab of the **Prepare infrastructure** blade, in the **Deployment planning completed?** drop-down list, select **Yes, I have done it** and select **Next**.

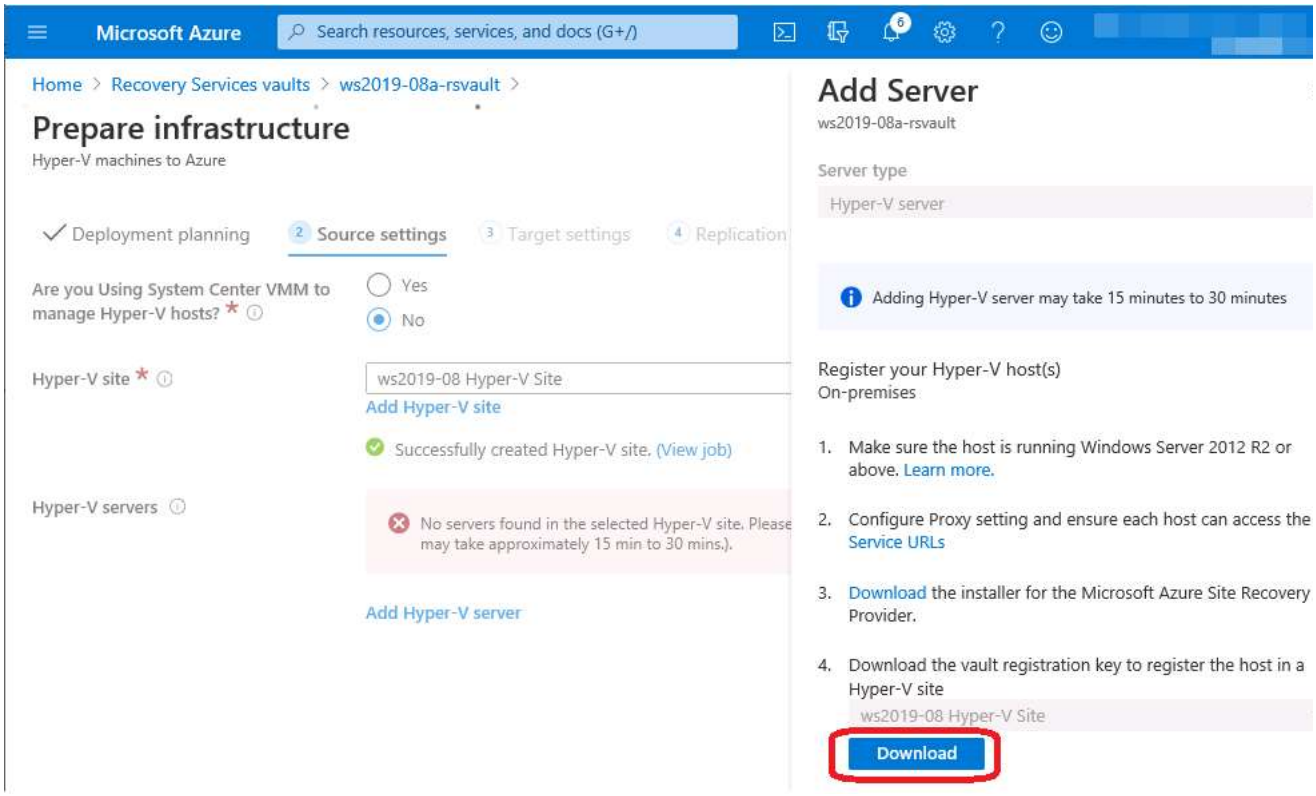


9. On the **Source settings** tab of the **Prepare infrastructure** blade, next to the **Are you Using System Center VMM to manage Hyper-V hosts** label, select the **No** option.

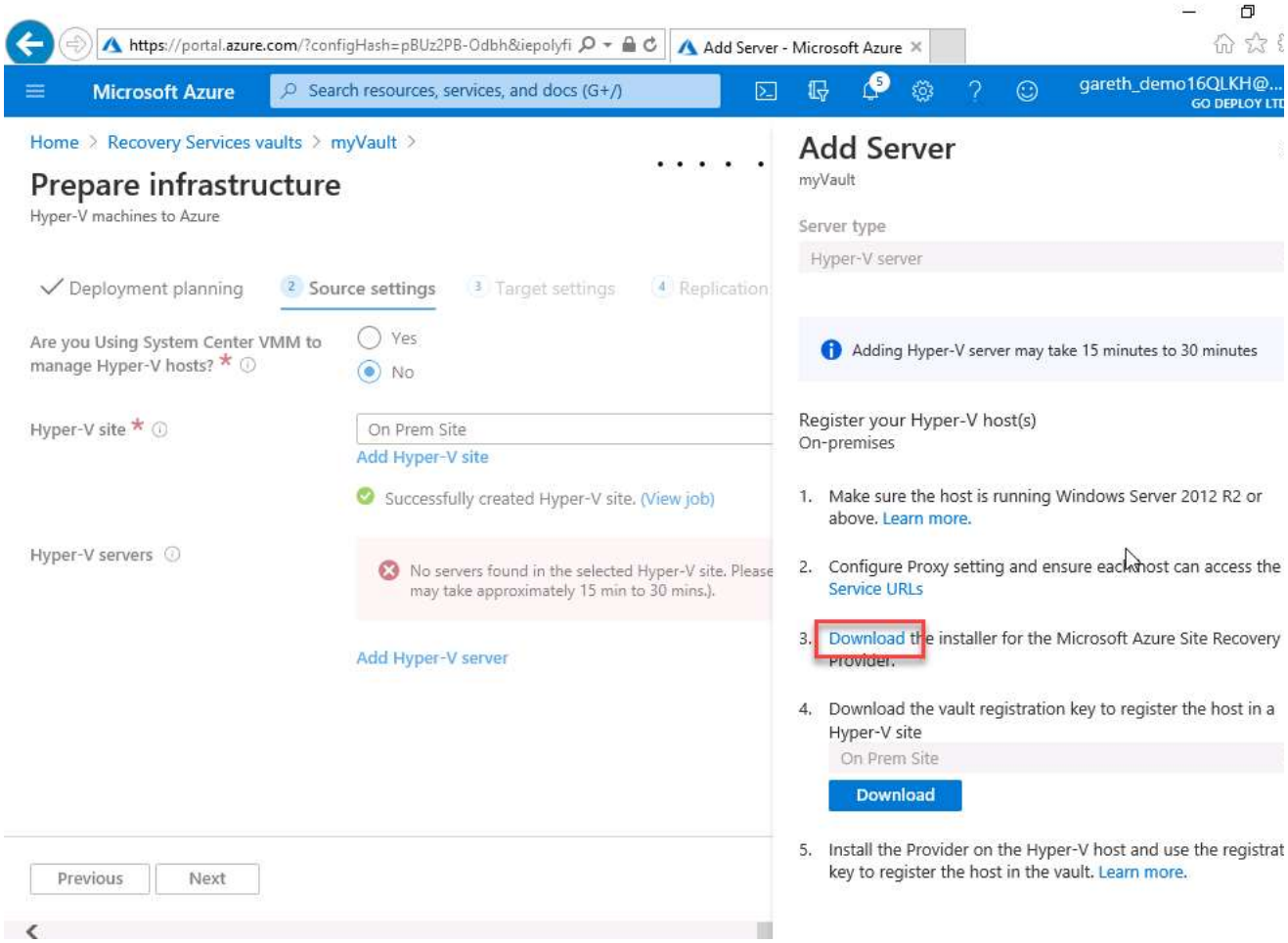
10. On the **Source settings** tab of the **Prepare infrastructure** blade, select the **Add Hyper-V site** link, on the **Create Hyper-V Site** blade, in the **Name** text box, enter OnPremsite and select **OK**:

11. On the **Source settings** tab of the **Prepare infrastructure** blade, select the **Add Hyper-V server** link.

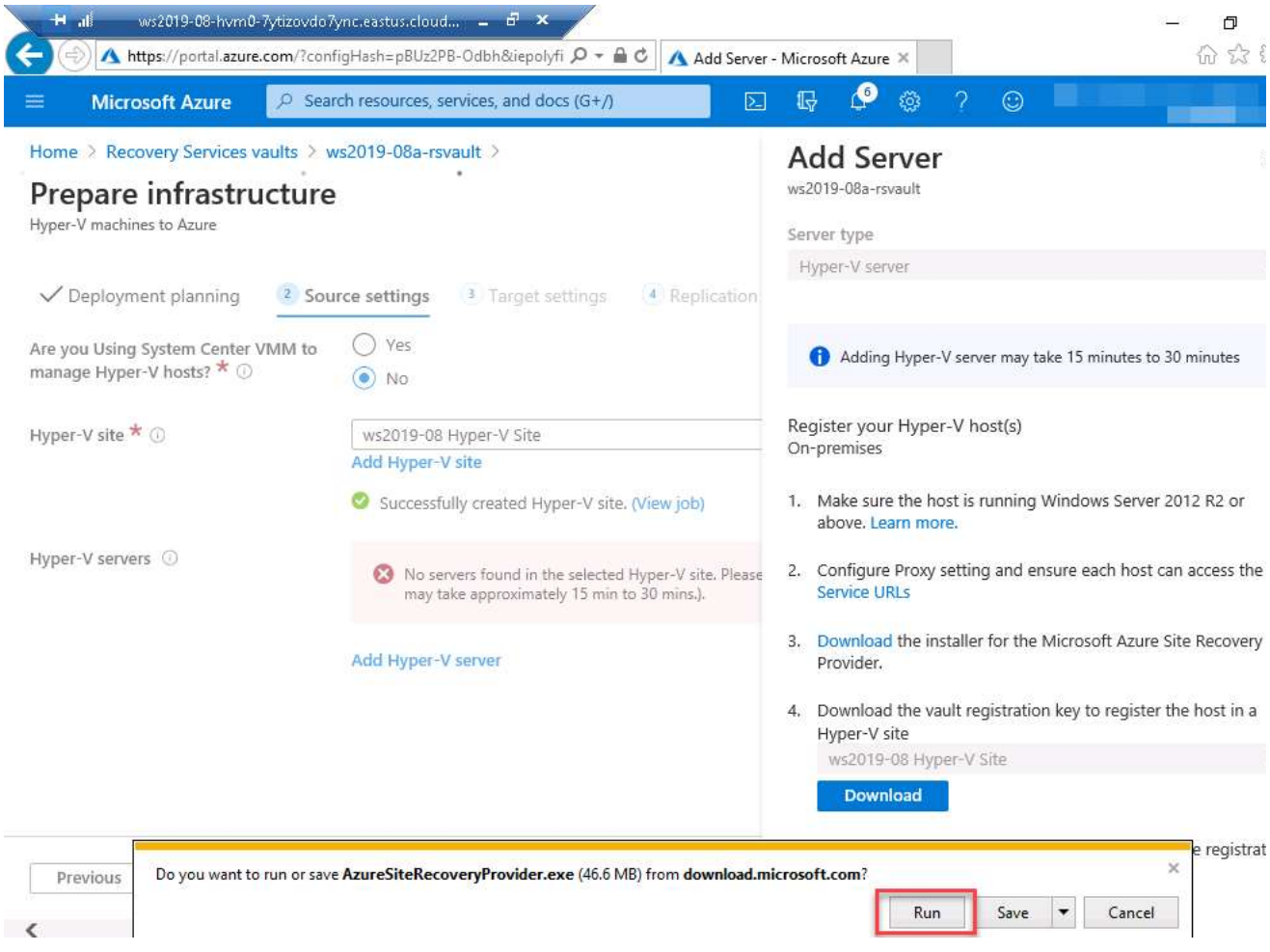
12. On the **Add Server** blade, select the **Download** link in step 4 to download the vault credentials file.



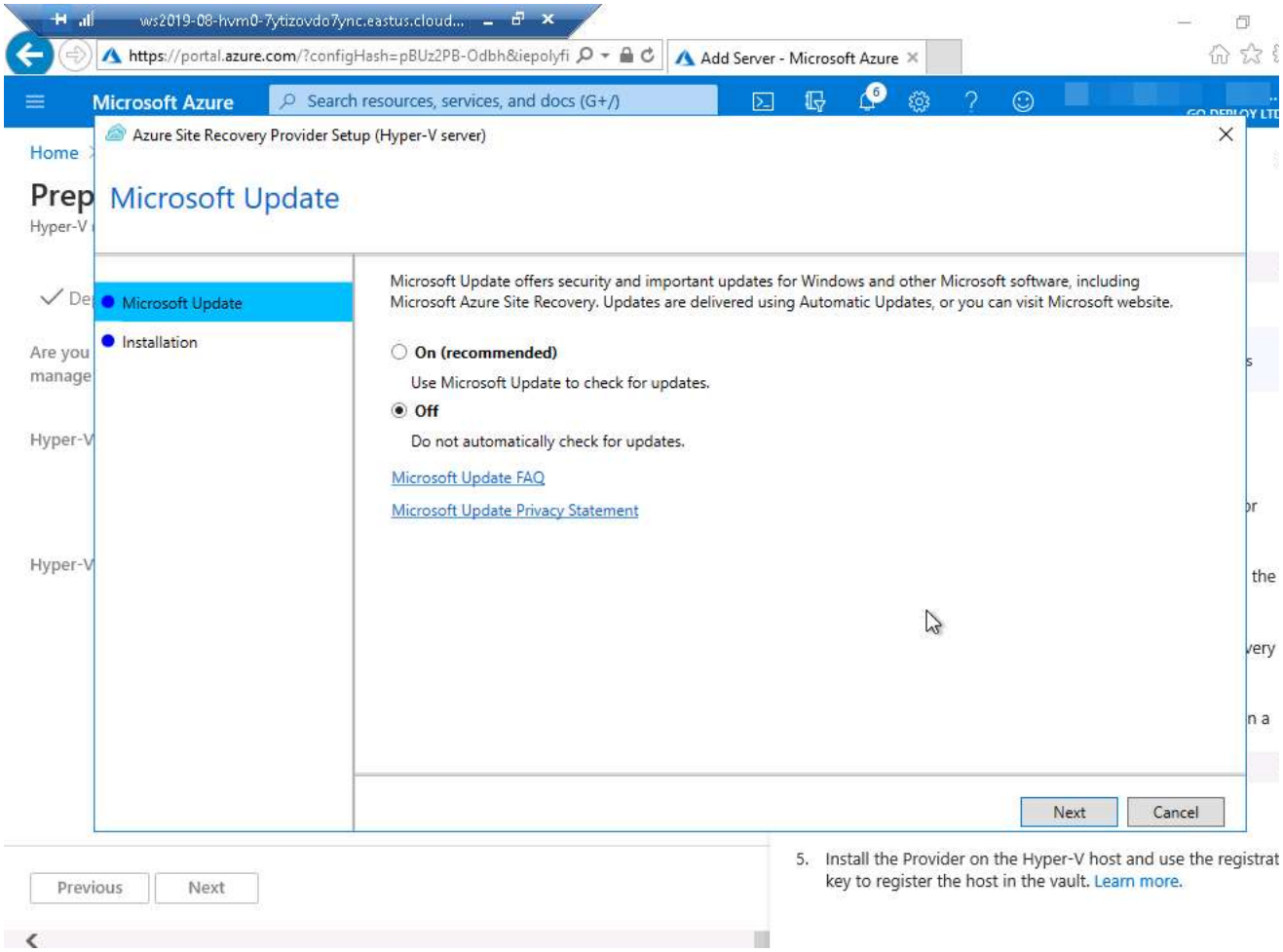
13. On the **Add Server** blade, select the **Download** link in step 3 of the procedure for adding on-premises Hyper-V hosts in order to download the Microsoft Azure Site Recovery Provider.



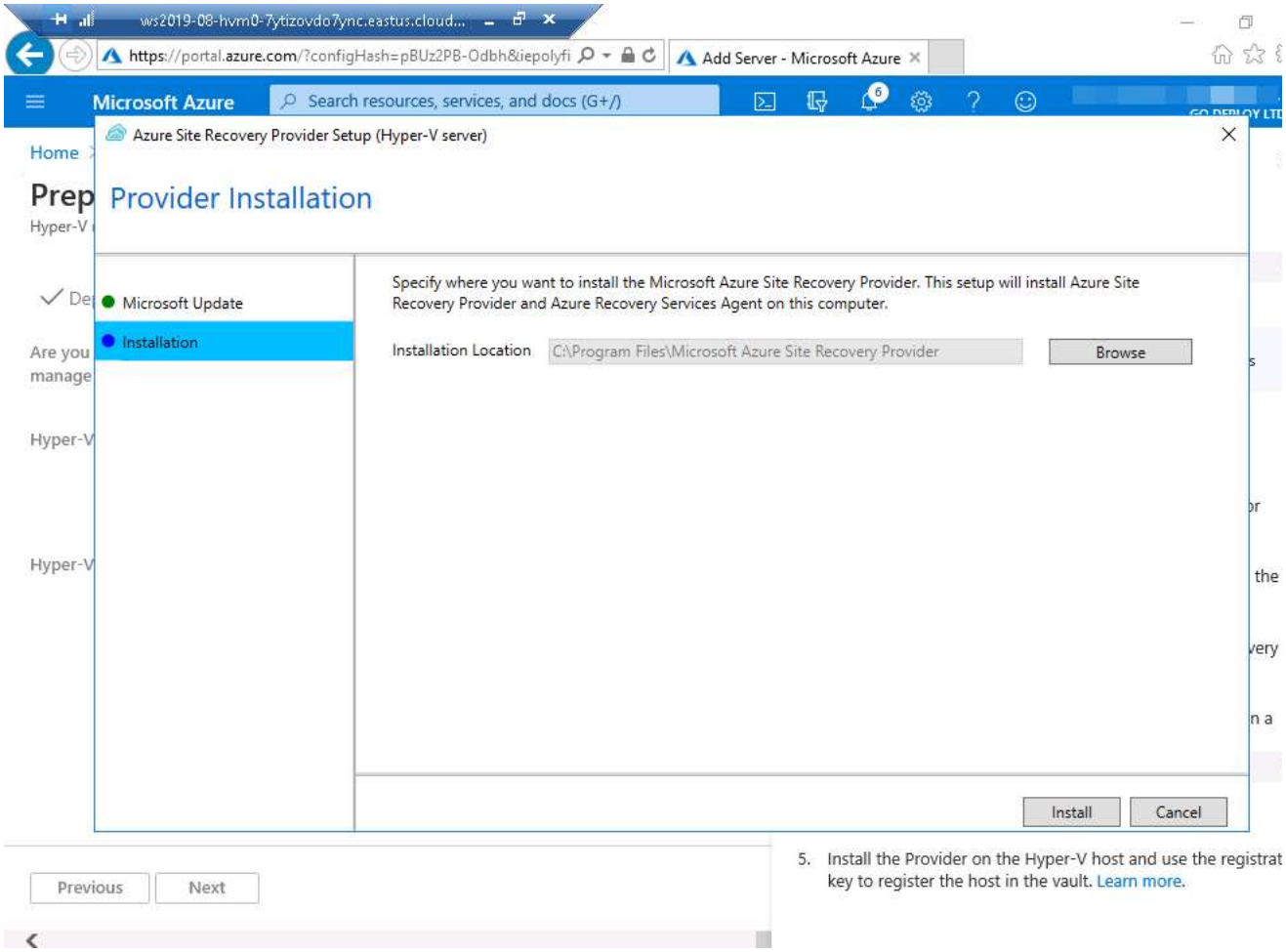
☐ 14. When prompted, in the browser window, select **Run** to launch **AzureSiteRecoveryProvider.exe**. This will start the **Azure Site Recovery Provider Setup (Hyper-V server)** wizard.



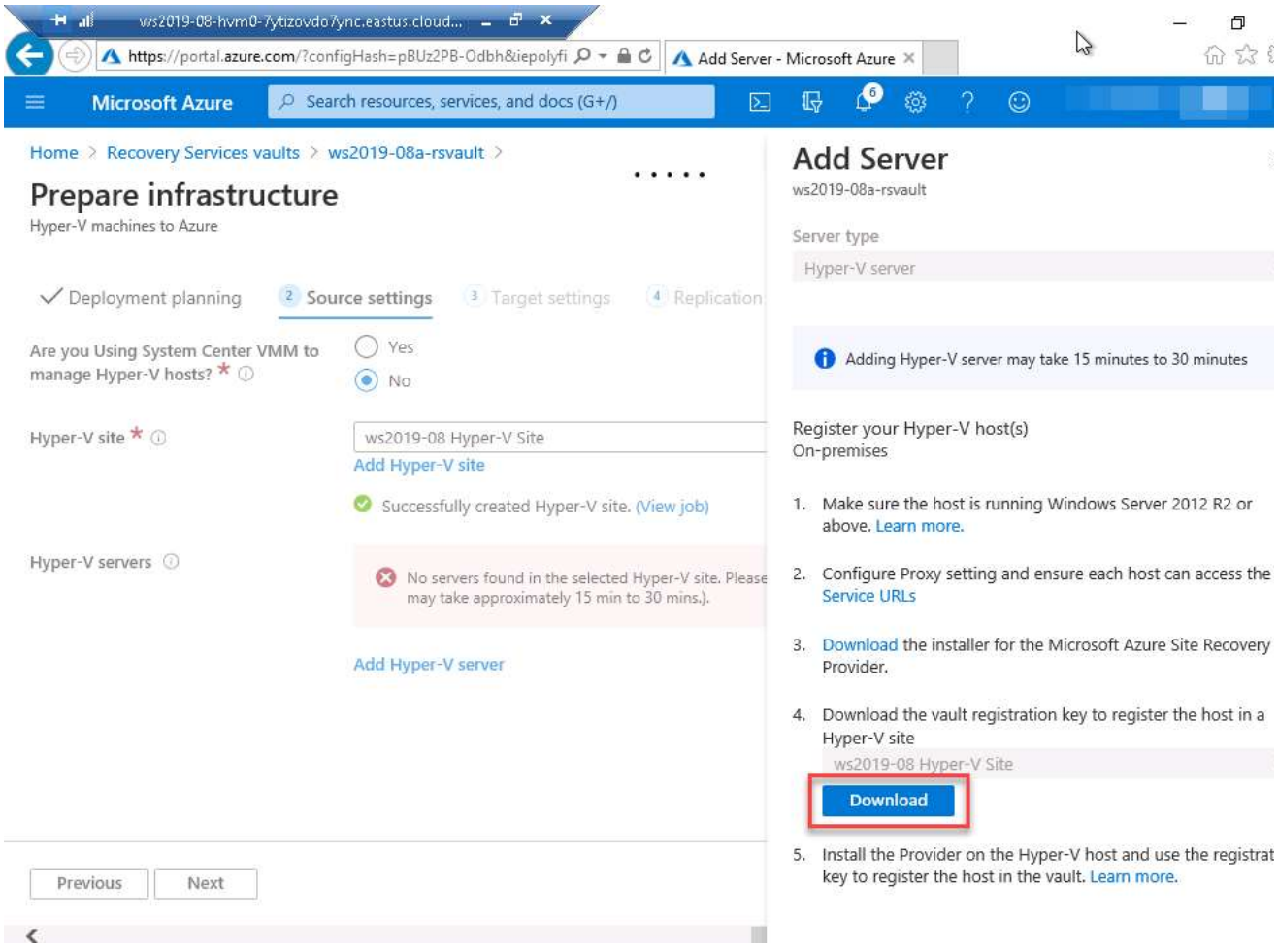
☐ 15. On the **Microsoft Update** page, select **Off** and select **Next**.



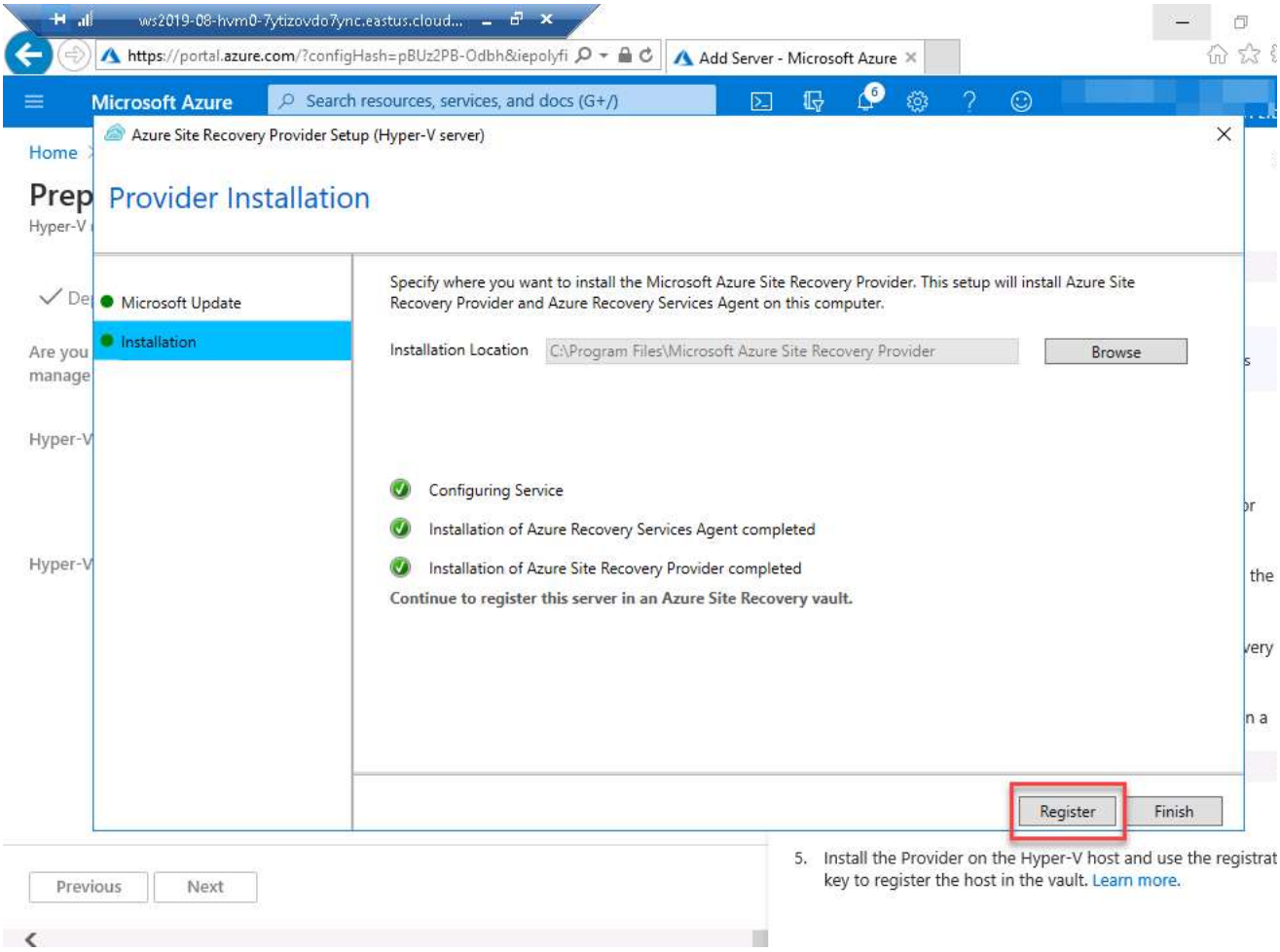
☐ 16. On the **Provider installation** page, select **Install**.



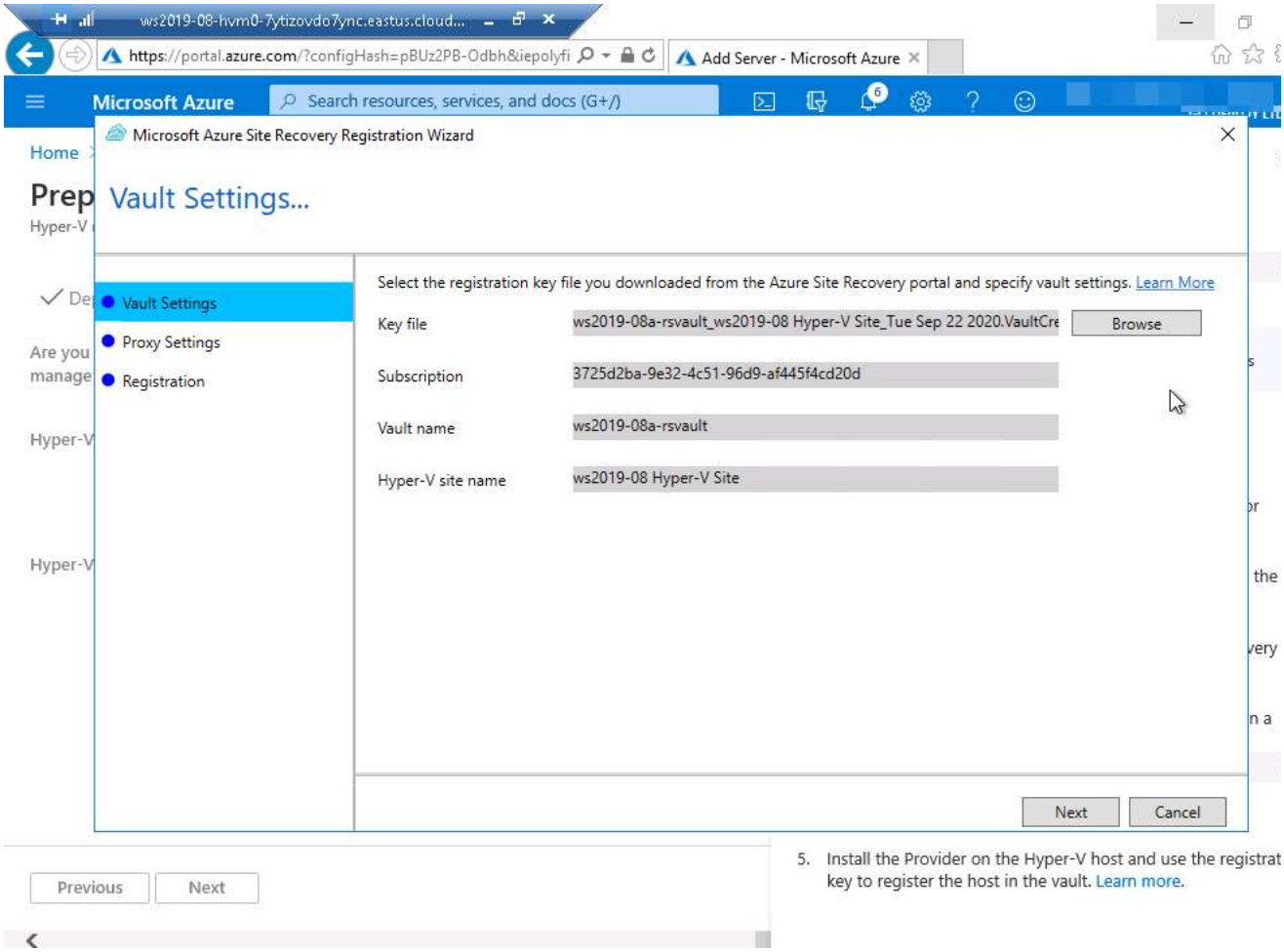
☐ 17. Switch to the Azure portal and, on the **Add Server** blade, select the **Download** button in step 4 of the procedure for registering on-premises Hyper-V hosts in order to download the vault registration key. When prompted, select **Save** to save the vault credentials file in the **Downloads** folder.



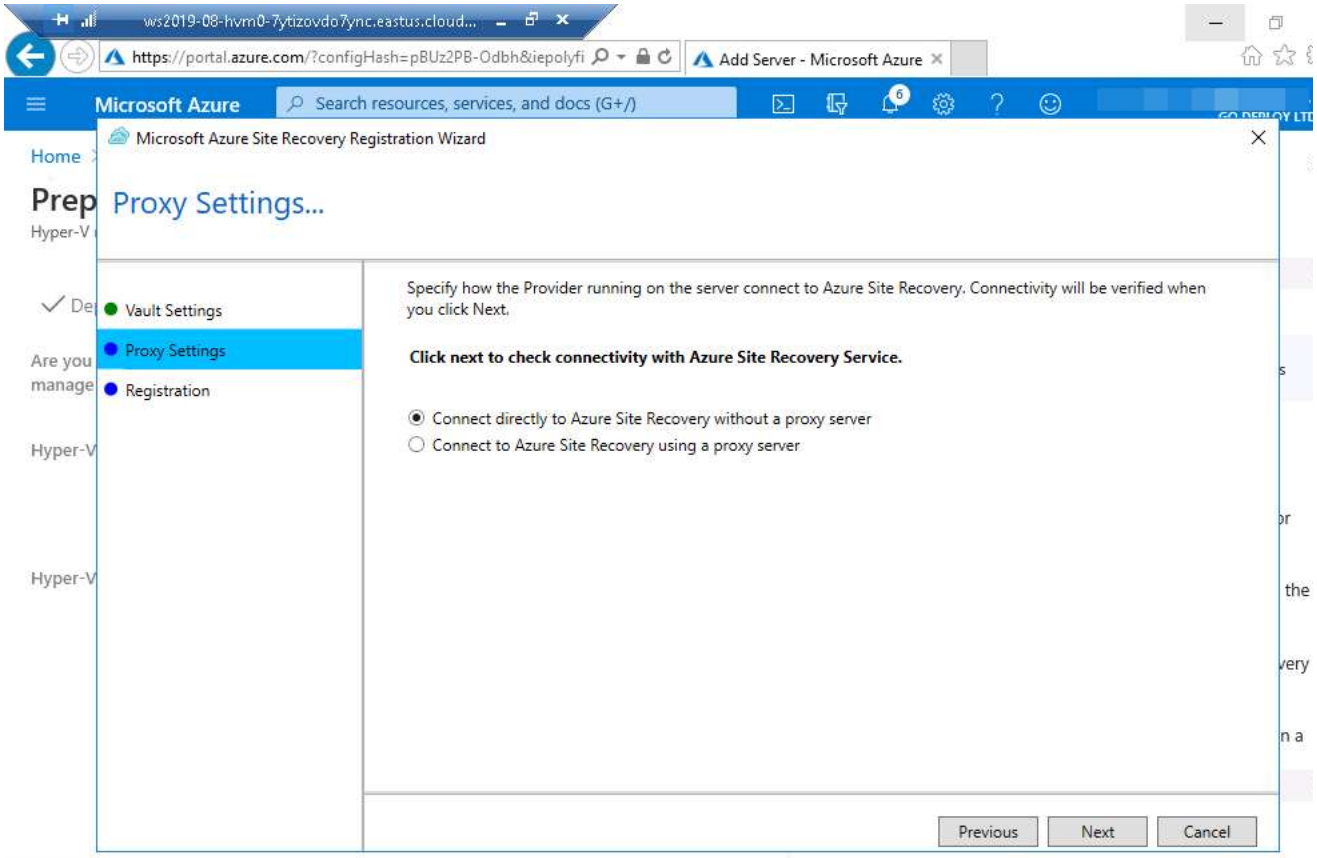
☐ 18. Switch to the **Provider installation** wizard window and select **Register**. This will start the **Microsoft Azure Site Recovery Registration Wizard**.



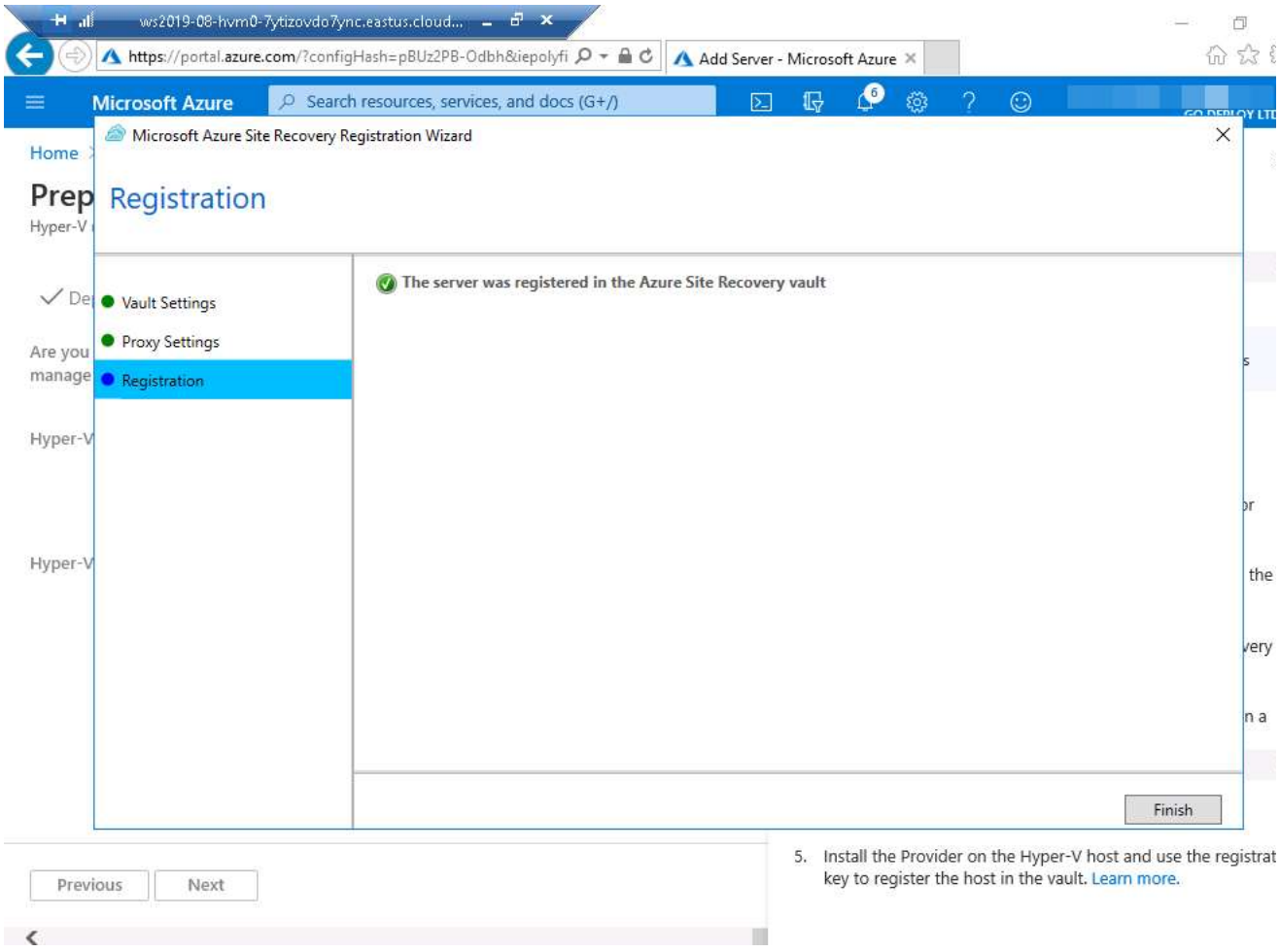
☐ 19. On the **Vault Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Browse**, in the **Open** window, navigate to the **Downloads** folder, select the vault credentials file, and select **Open**.



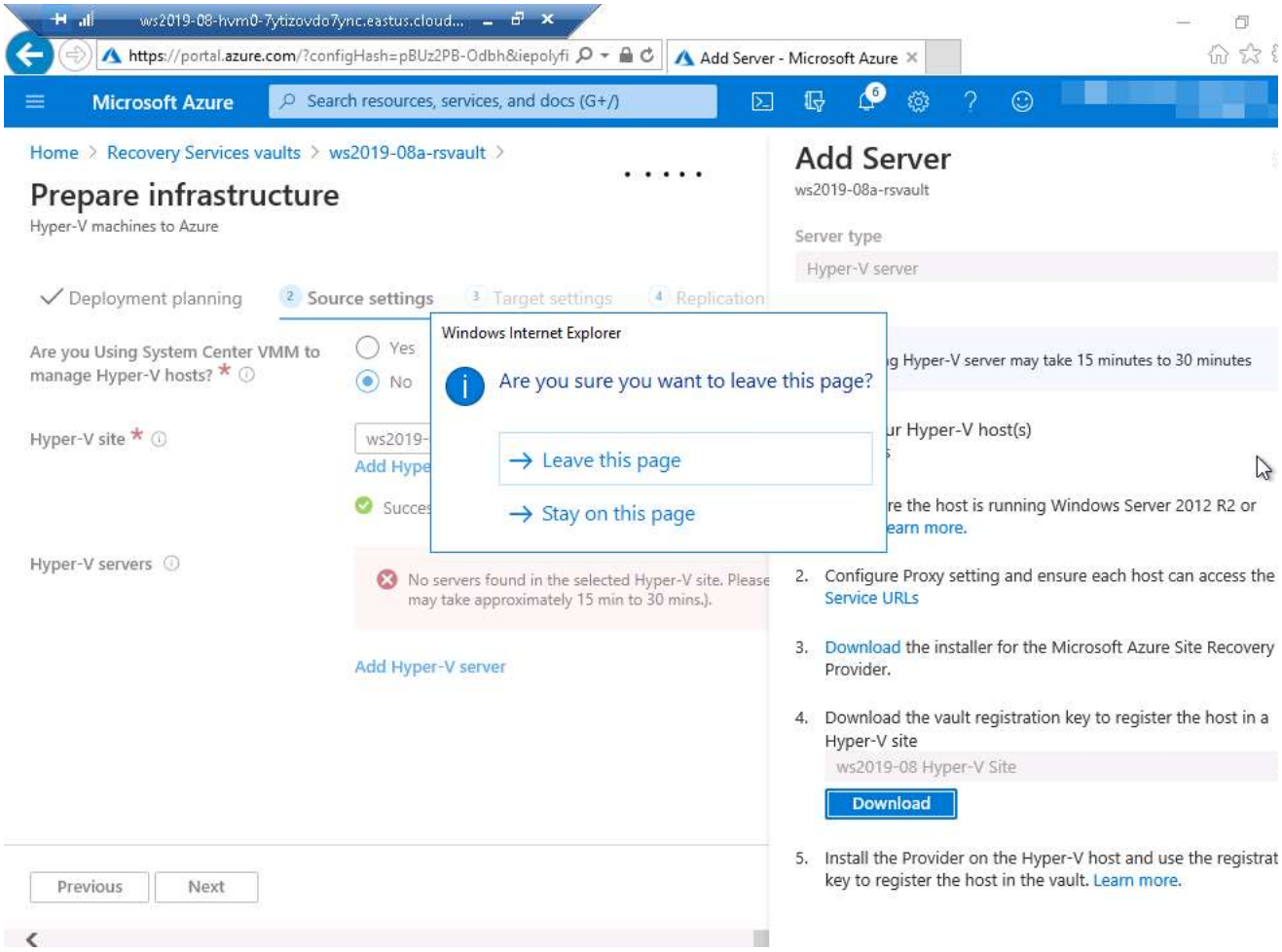
- [ ] 20. Back on the **Vault Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Next**.
- [ ] 21. On the **Proxy Settings** page of the **Microsoft Azure Site Recovery Registration Wizard**, accept the default settings and select **Next**.



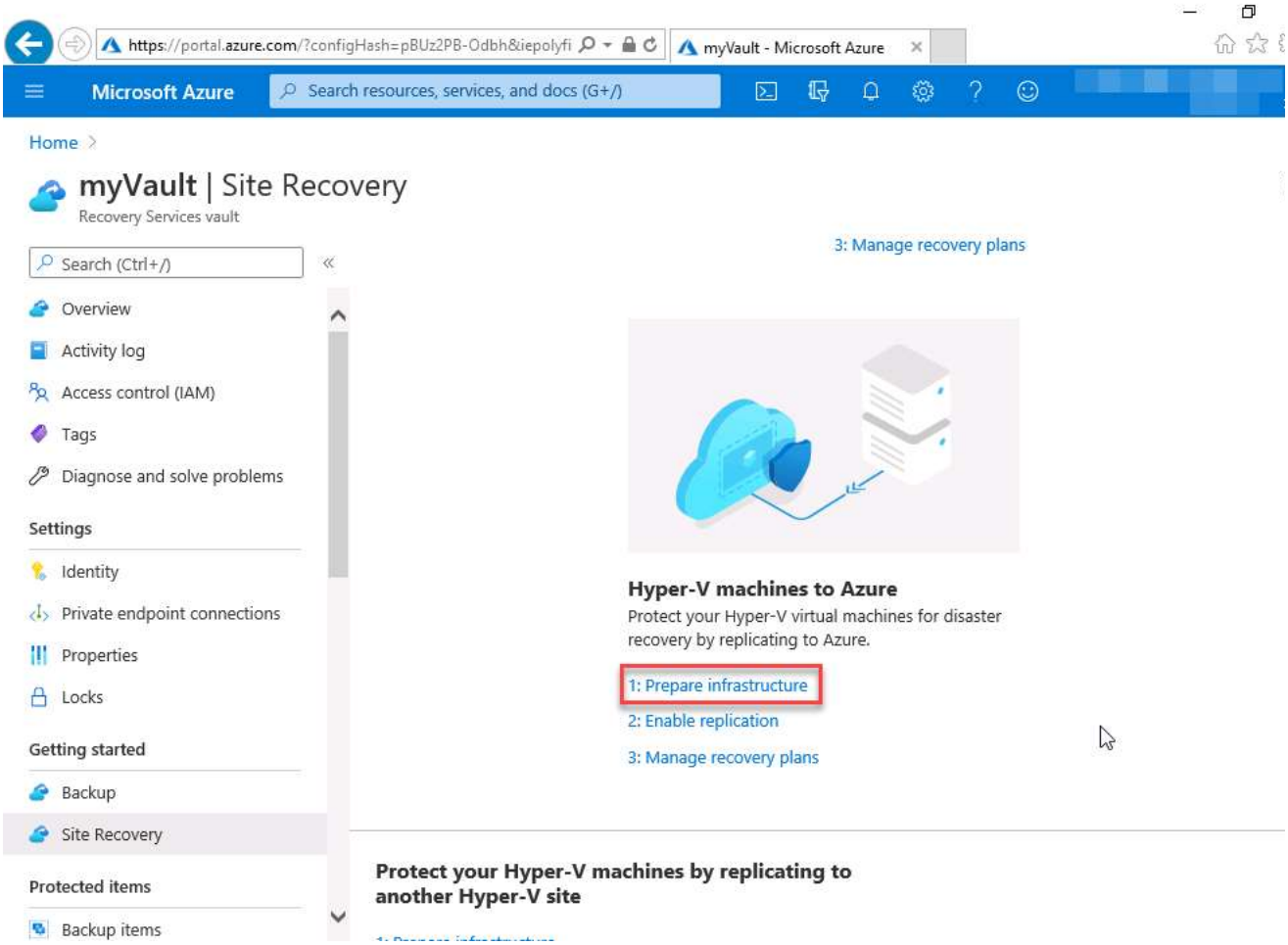
☐ 22. On the **Registration** page of the **Microsoft Azure Site Recovery Registration Wizard**, select **Finish**.



☐ 23. Switch back to the browser window displaying the Azure portal and refresh the page. When prompted, select **Leave this page**.



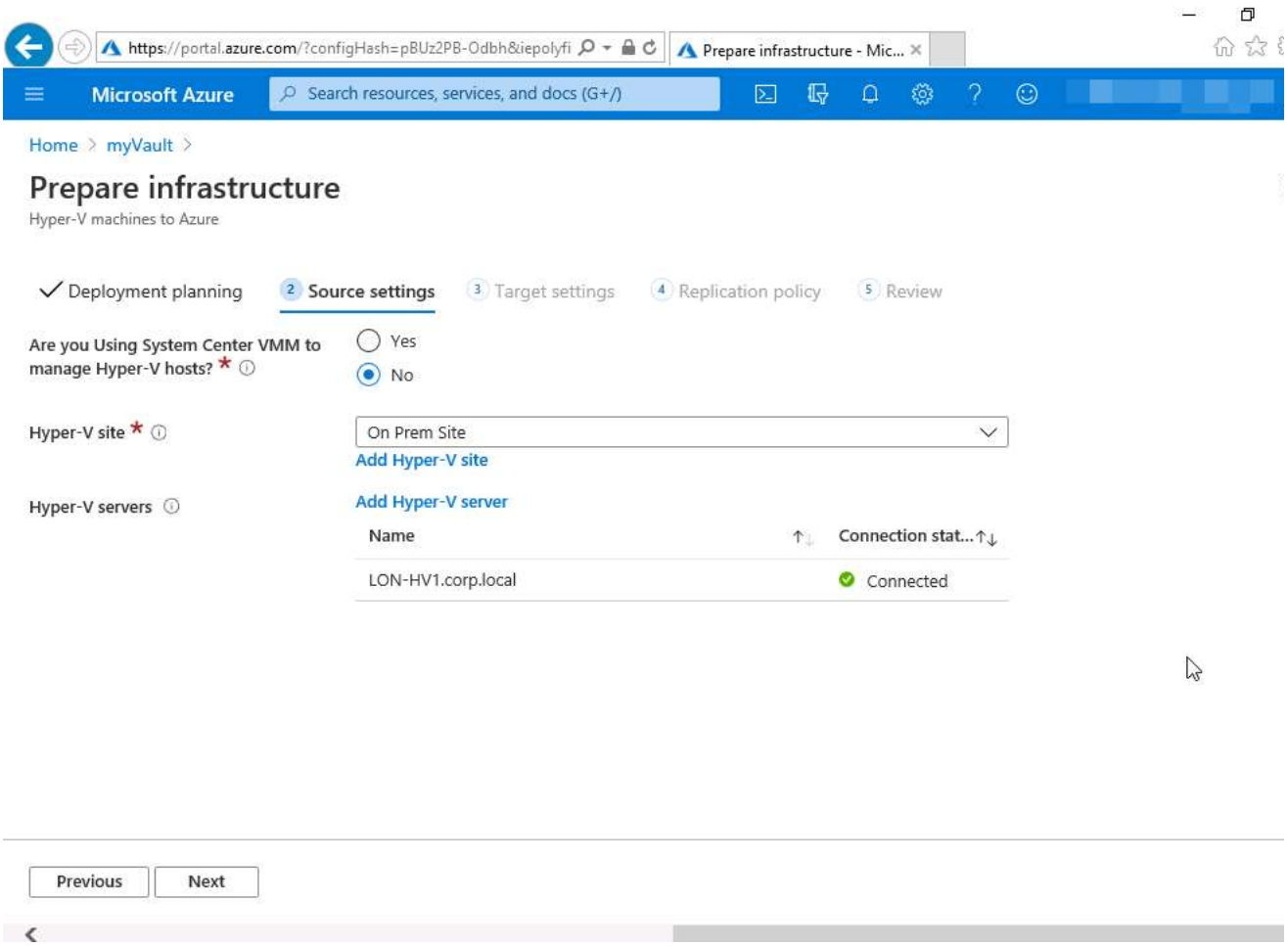
☐ 24. Back on the **myVault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **1. Prepare infrastructure**.



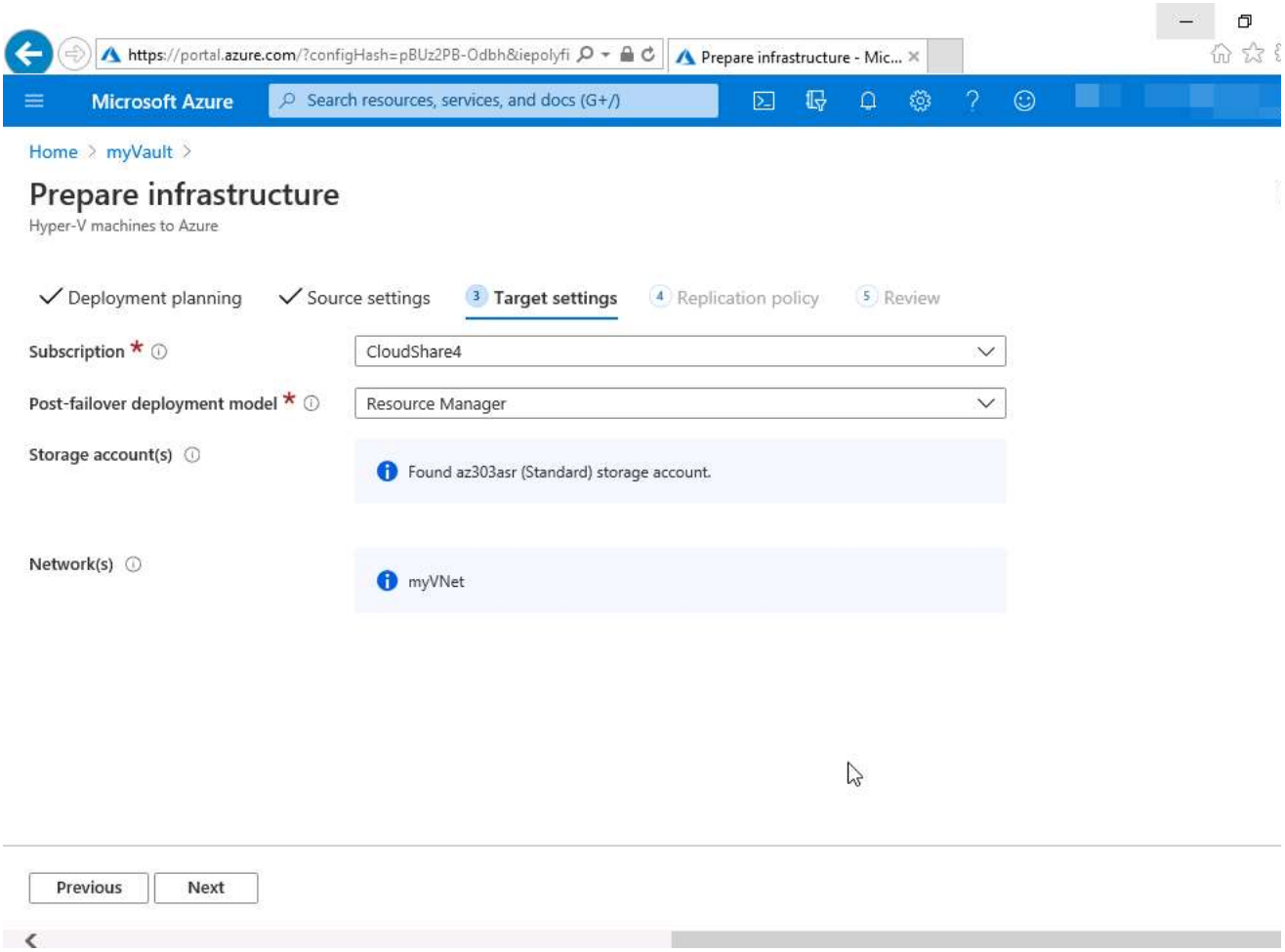
- [ ] 25. On the **Deployment planning** tab of the **Prepare infrastructure** blade, in the **Deployment planning completed?** drop-down list, select **Yes, I have done it** and select **Next**.

- [ ] 26. On the **Source settings** tab of the **Prepare infrastructure** blade, next to the **Are you Using System Center VMM to manage Hyper-V hosts** label, select the **No** option.

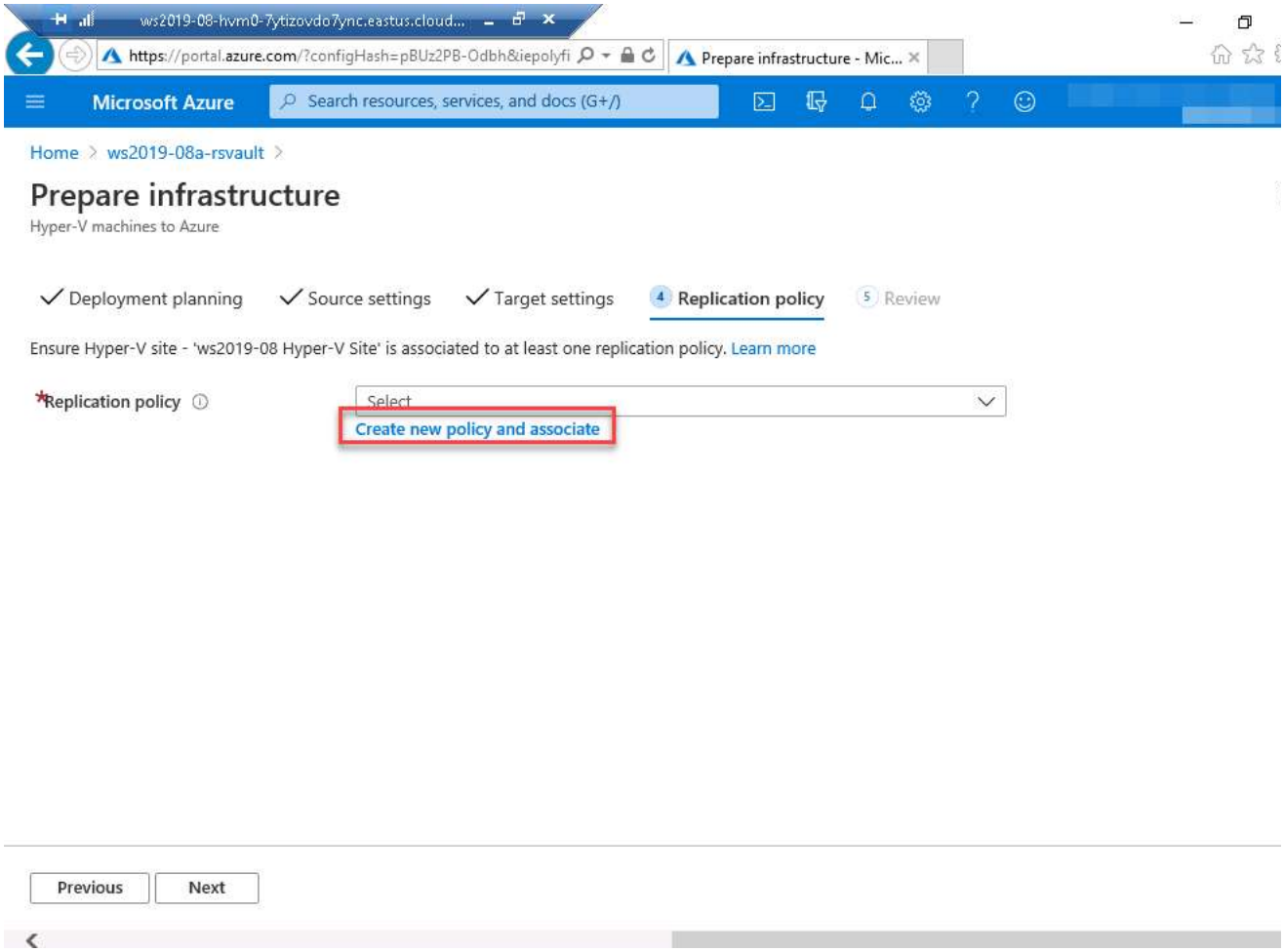
- [ ] 27. Verify that the **Hyper-V site** and **Hyper-V servers** settings are set correctly and select **Next**.



☐ 28. On the **Target settings** tab of the **Prepare infrastructure** blade, accept the default settings and select **Next**.



- [ ] 29. On the **Replication policy** tab of the **Prepare infrastructure** blade, select **Create new policy and associate**.



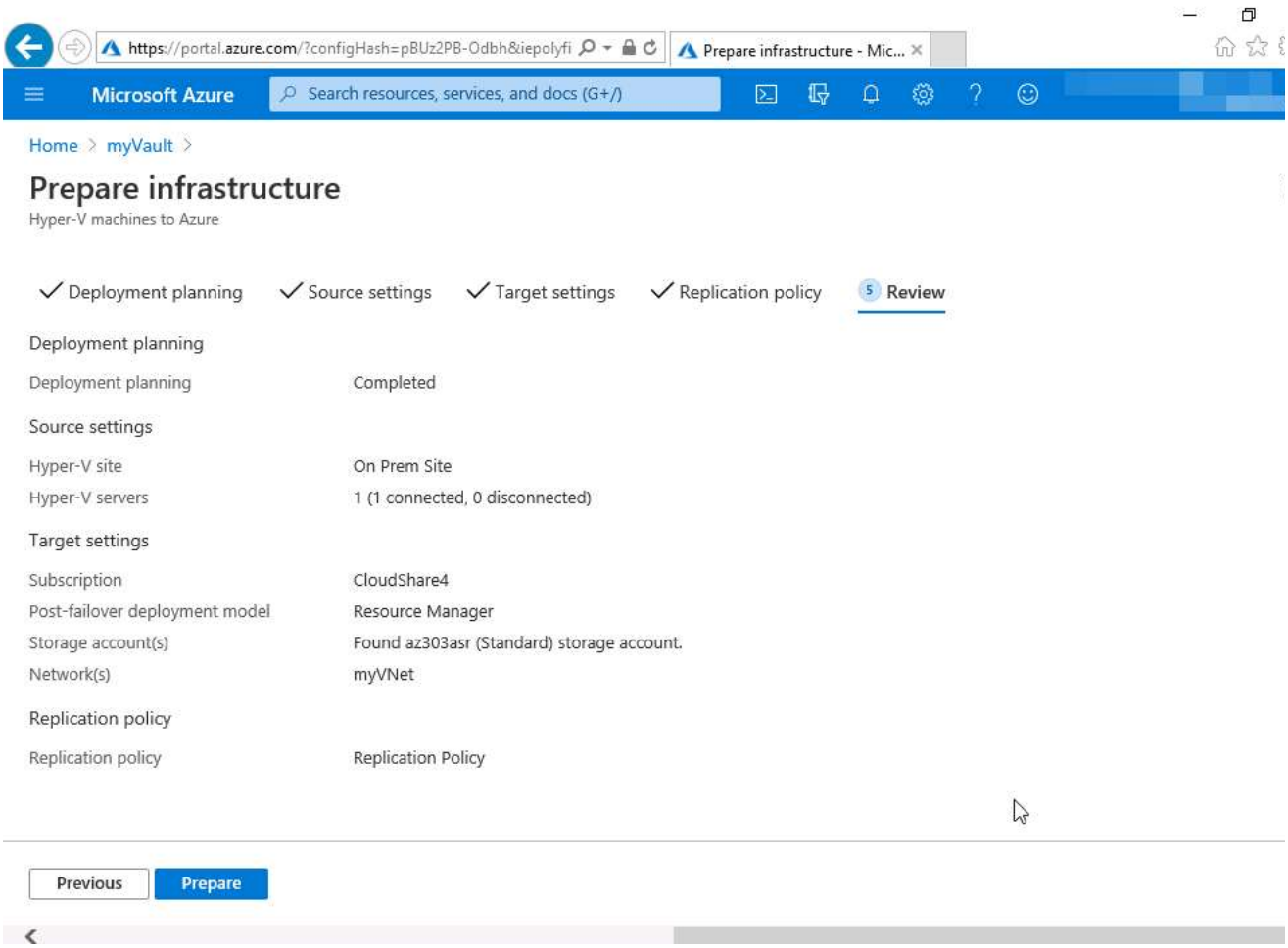
- [ ] 30. On the **Create and associate policy** blade, specify the following settings (leave others with their default values) and select **OK**:

Table 11: Policy settings

Setting	Value
Name	replicationpolicy
Copy frequency	**30 seconds**

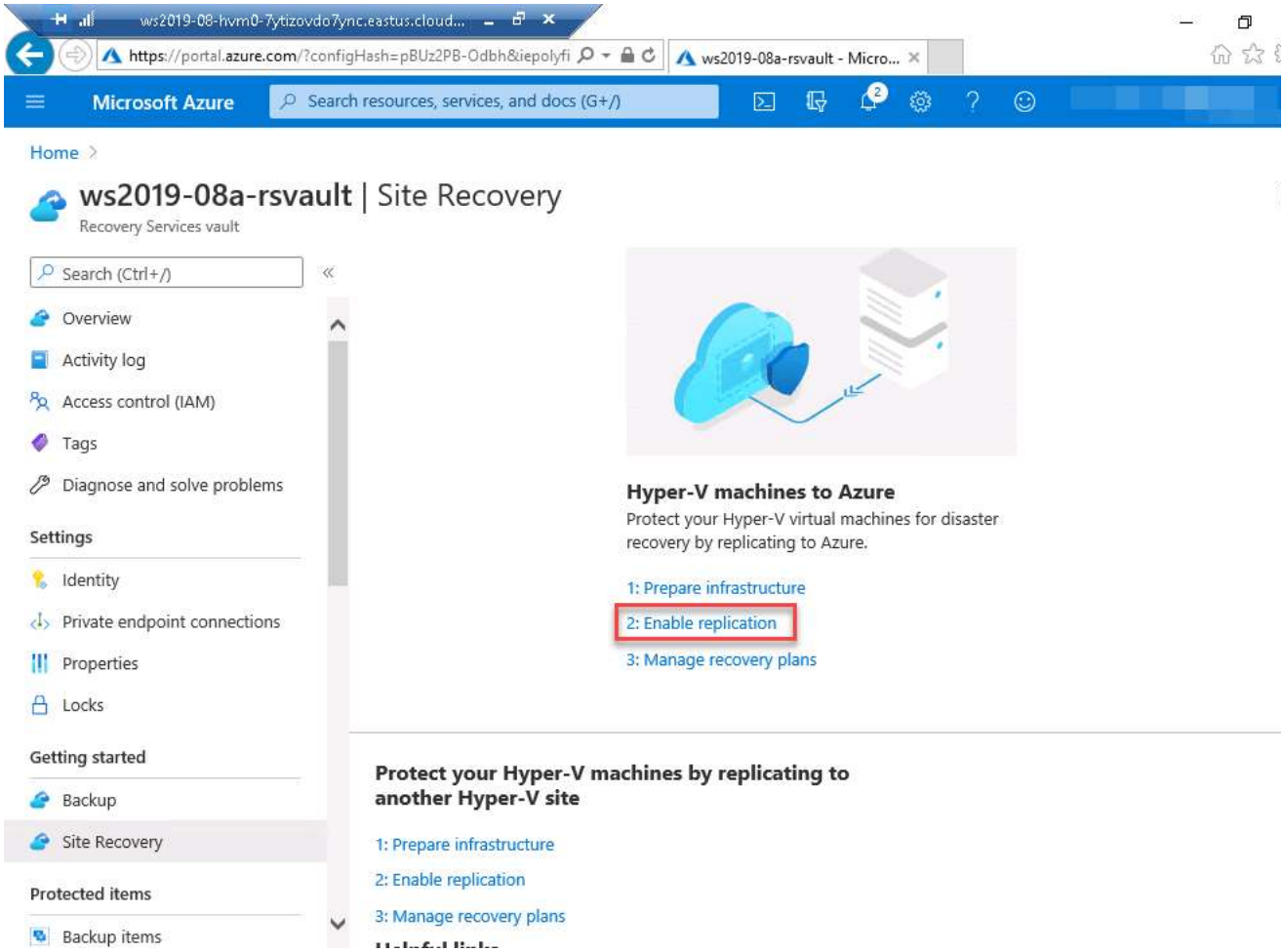
- [ ] 31. Back on the **Replication policy** tab of the **Prepare infrastructure** blade, wait until the site has been associated with the policy and select **Next**.

- [ ] 32. On the **Review** tab of the **Prepare infrastructure** blade, select **Prepare**



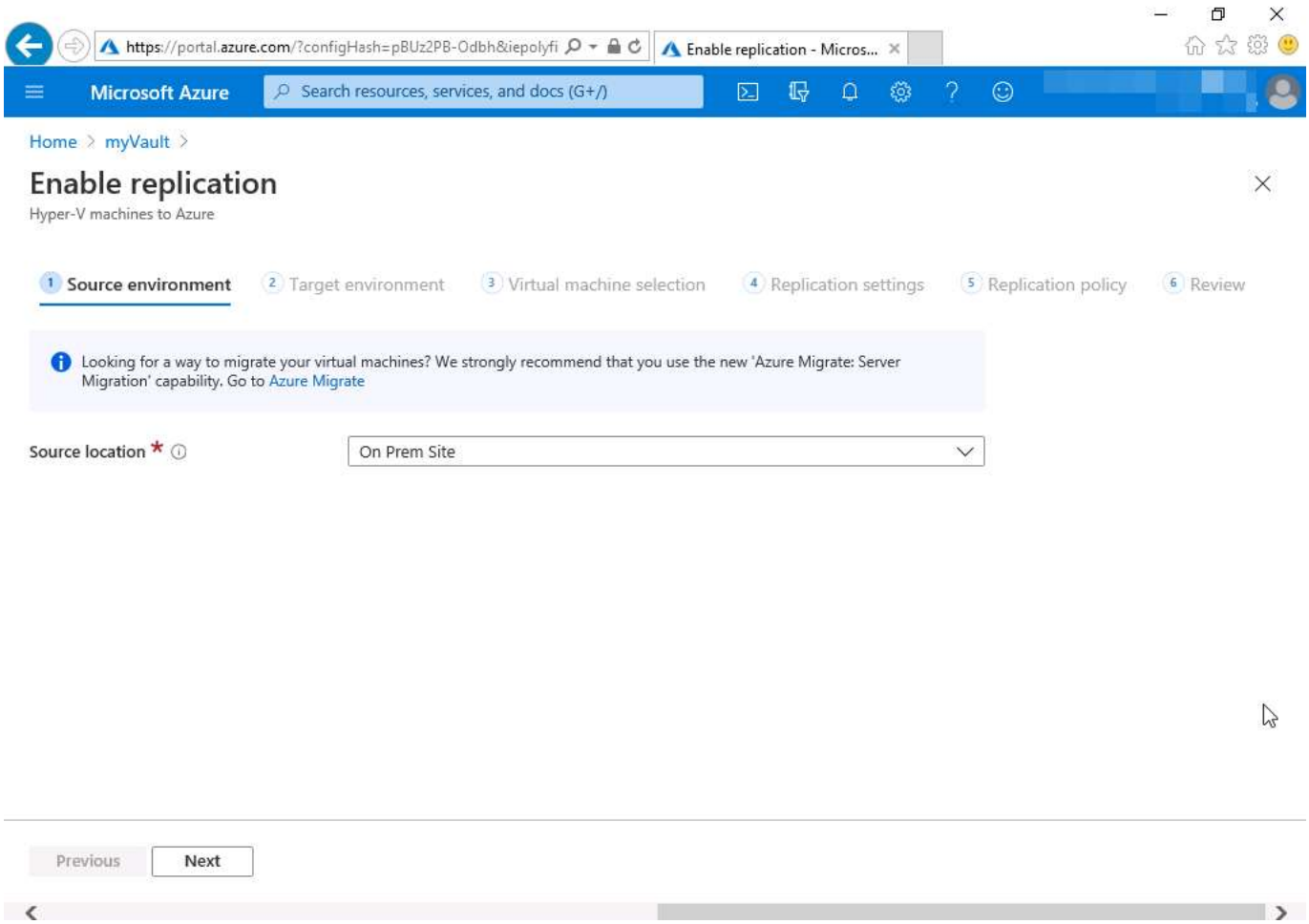
Task 2: Enable replication of a Hyper-V virtual machine

- [ ] 1. In the Azure portal, on the **ws2019-08a-rsvault | Site Recovery** blade, in the **Hyper-V machines to Azure** section, select **2. Enable replication**.



- [ ] 2. On the **Source environment** tab of the **Enable replication** blade, in the **Source location** drop-down list, select **On Prem site** and select **Next**.

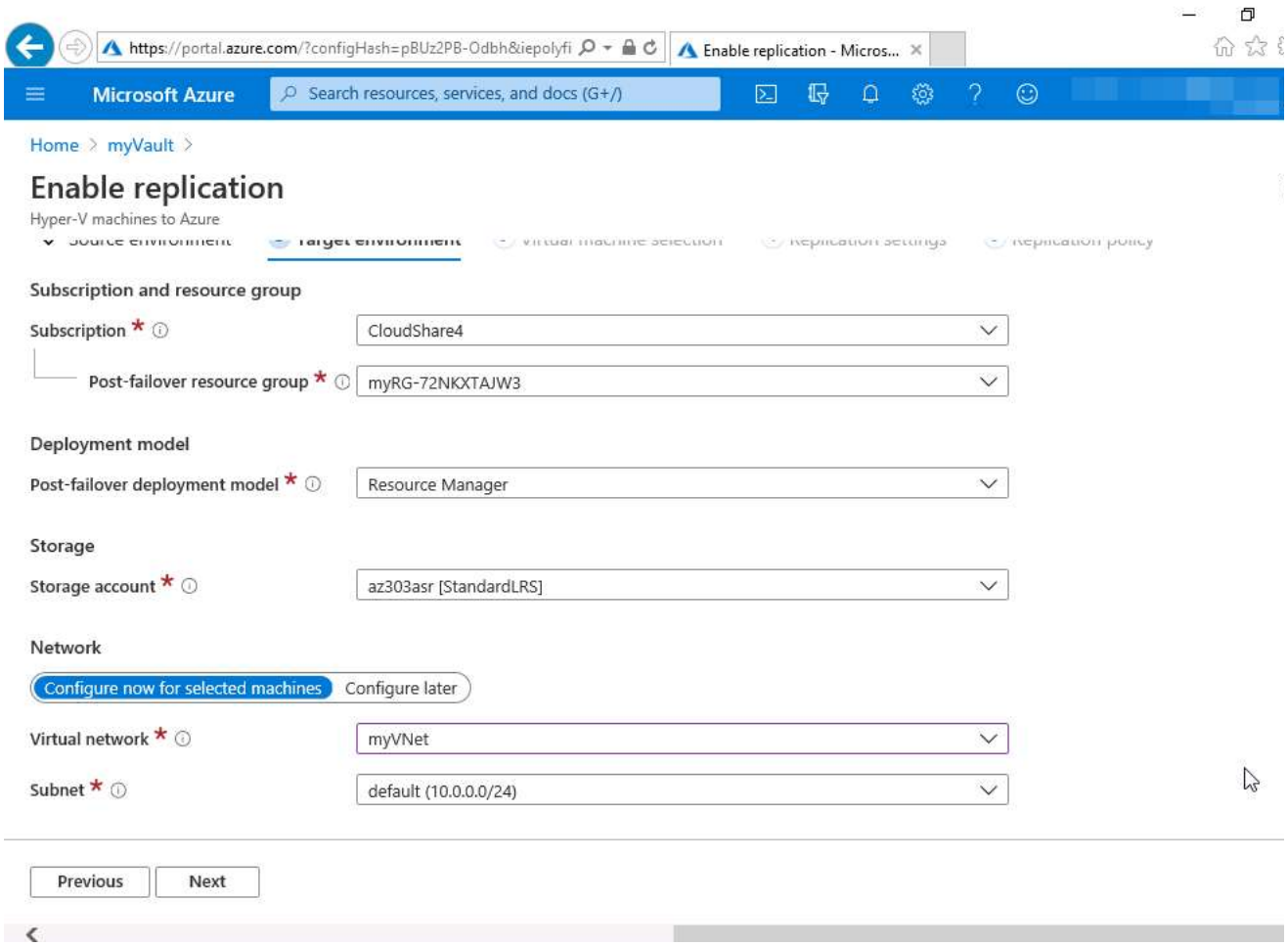
> ⚠ If the **Onpremsite** option does not appear, Please refresh your browser.



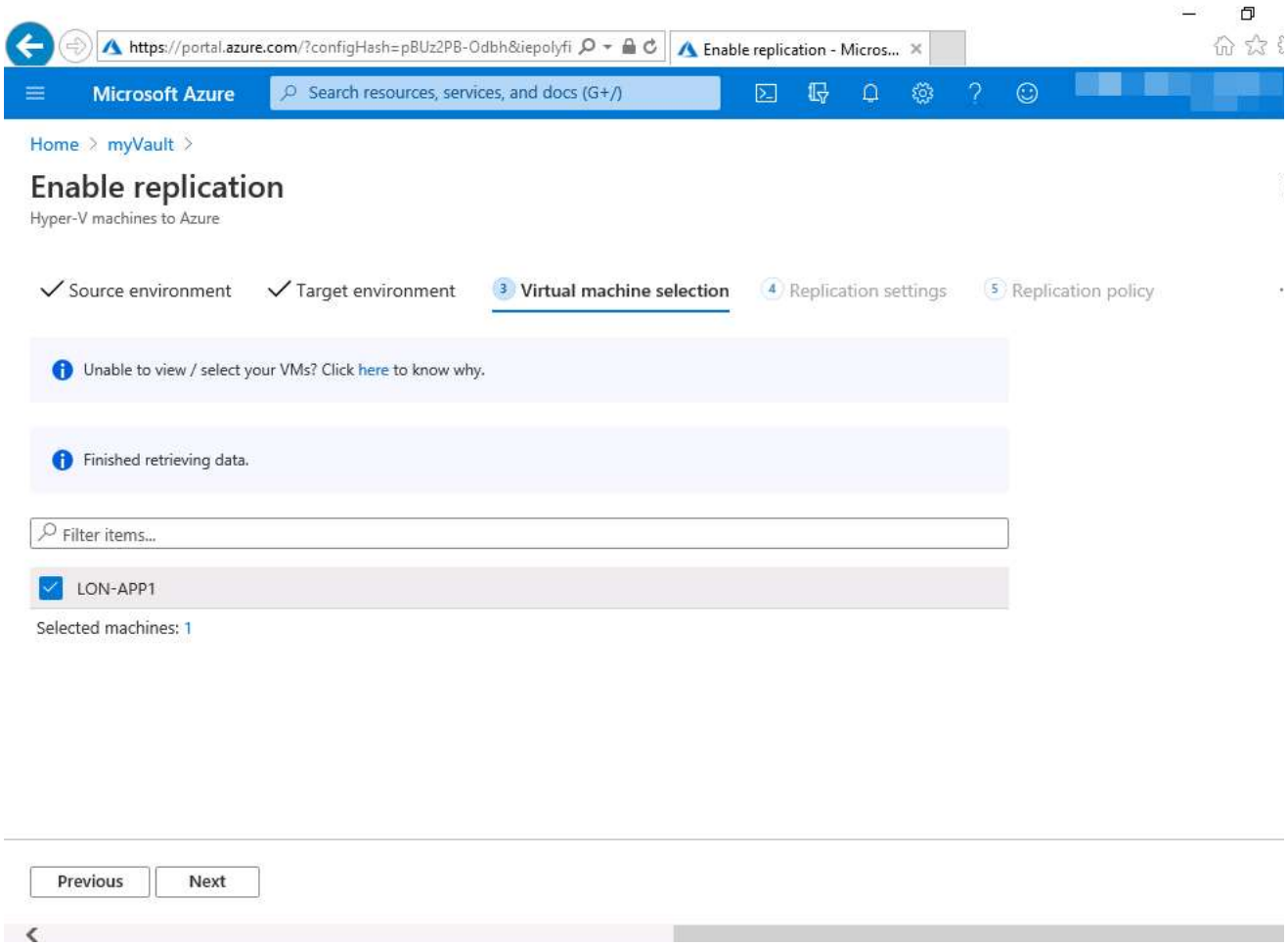
- [ ] 1. On the **Target environment** tab of the **Enable replication** blade, specify the following settings (leave others with their default values) and select **Next**:

Table 12: Target environment settings

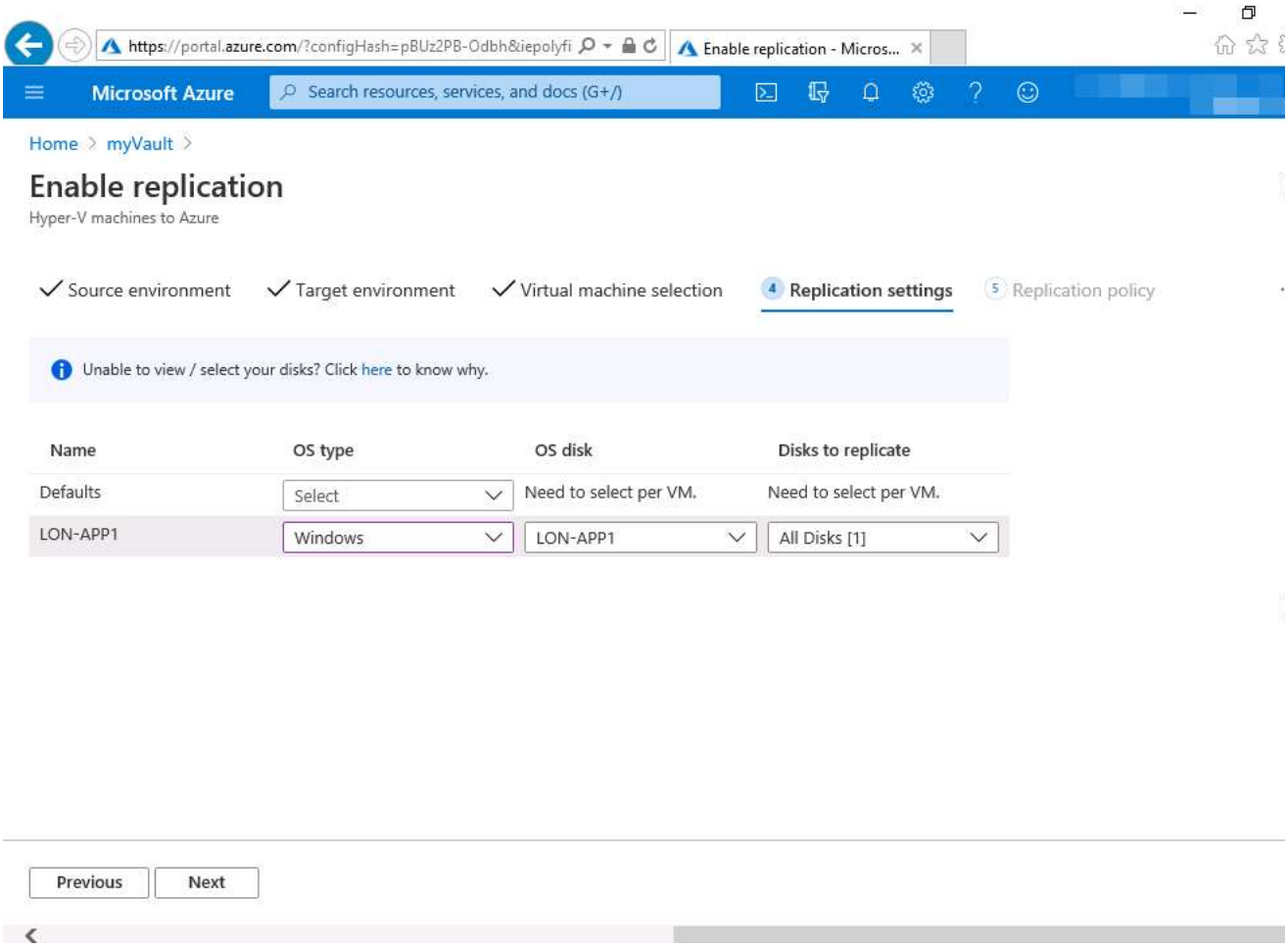
Setting	Value
Subscription	**CloudShare4**
Post-failover resource group	**myRG-T17DSTITVP**
Post-failover deployment model	**Resource Manager**
Storage account	**the name of the storage account you created in the first task of this exercise**
Azure network	**Configure now for selected machines**
Virtual network	**myVNet**
Subnet	default **(10.0.0.0/24)**



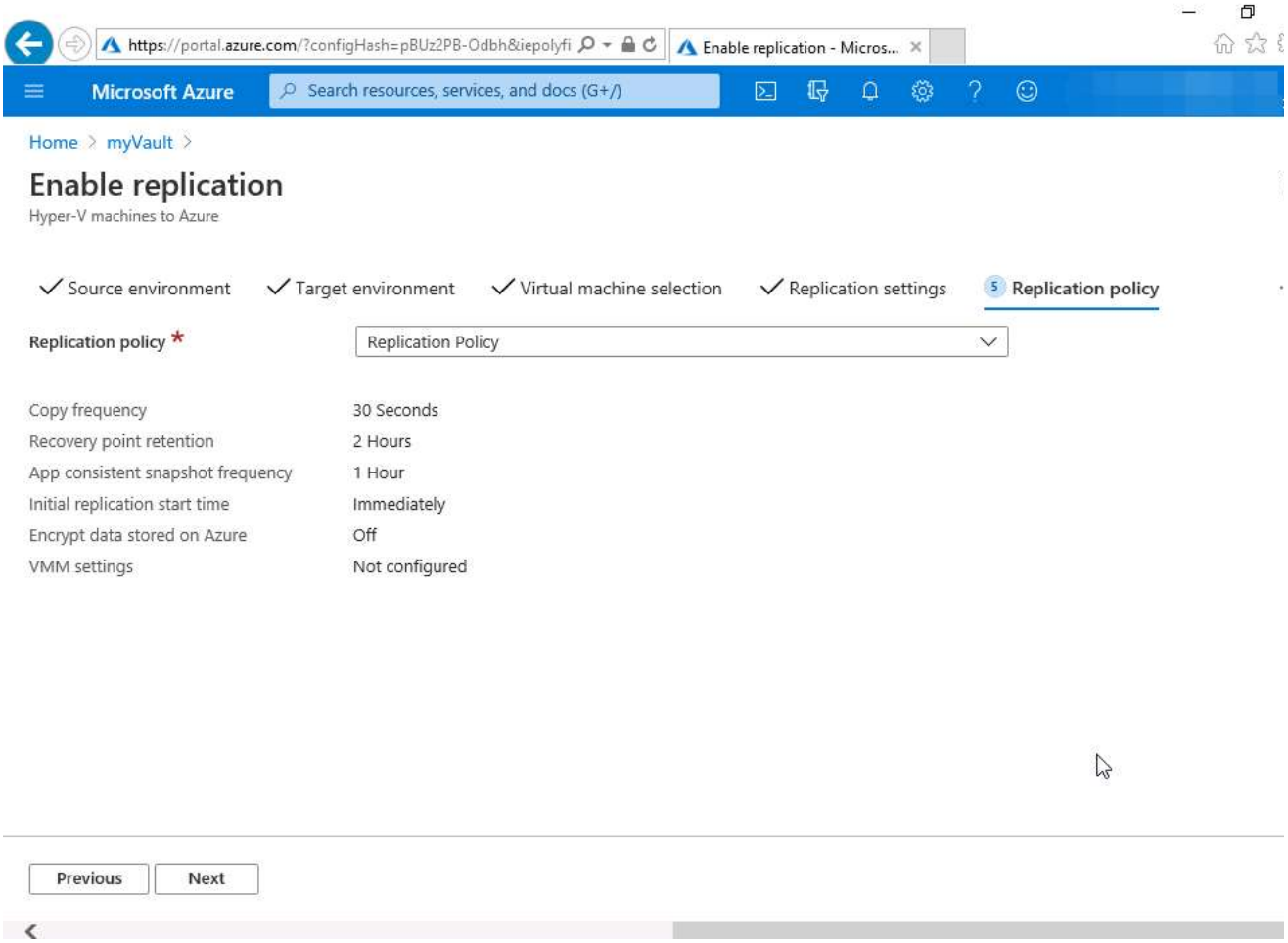
2. On the **Virtual machine selection** tab of the **Enable replication** blade, select the **LON-APP1** checkbox and select **Next**.



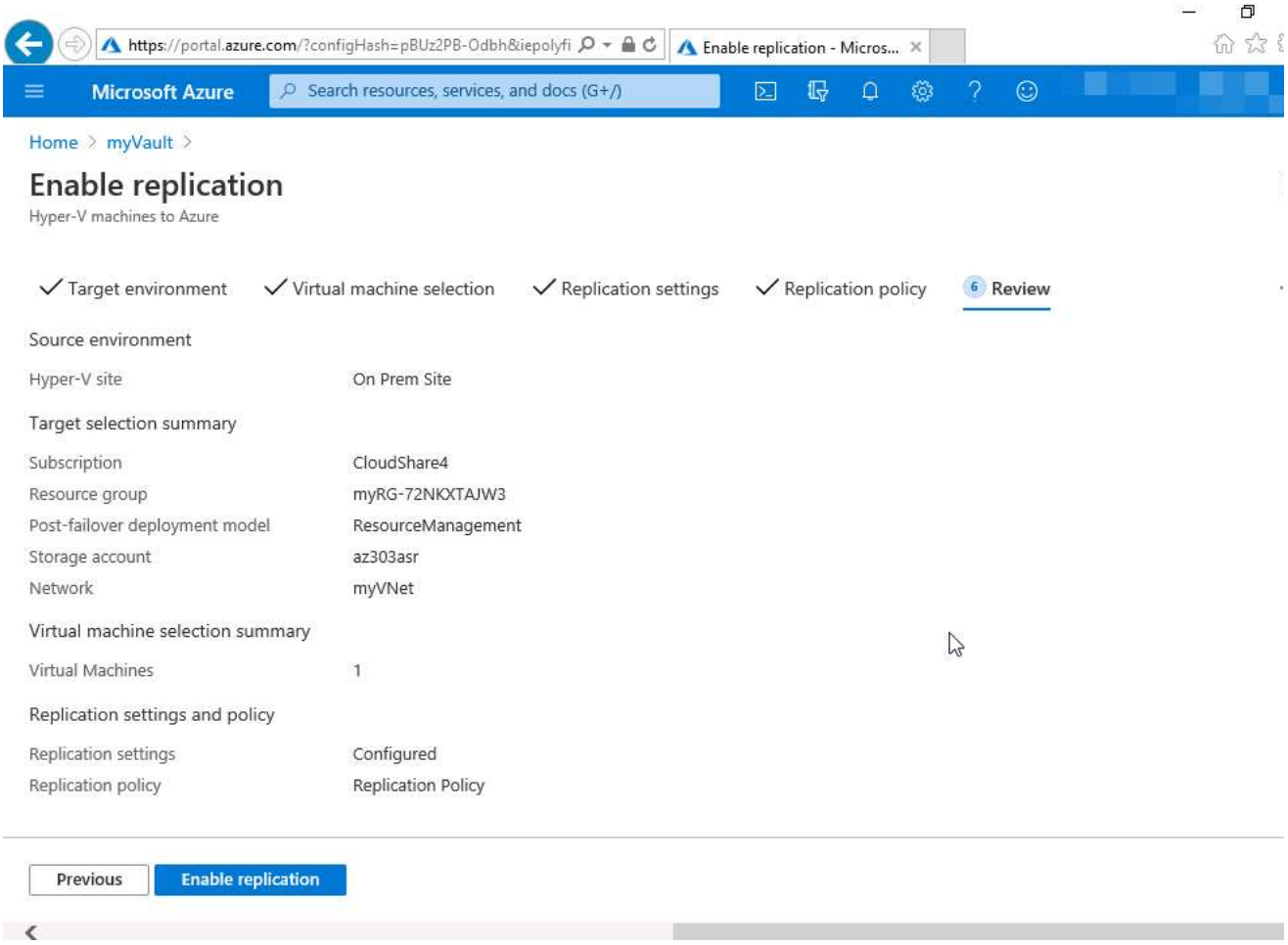
☐ 3. On the **Replication settings** tab of the **Enable replication** blade, in the **Defaults** row and **OS type** column, select **Windows** from the drop-down list and select **Next**.



☐ 4. On the **Replication policy** tab of the **Enable replication** blade, accept the default settings and select **Next**.

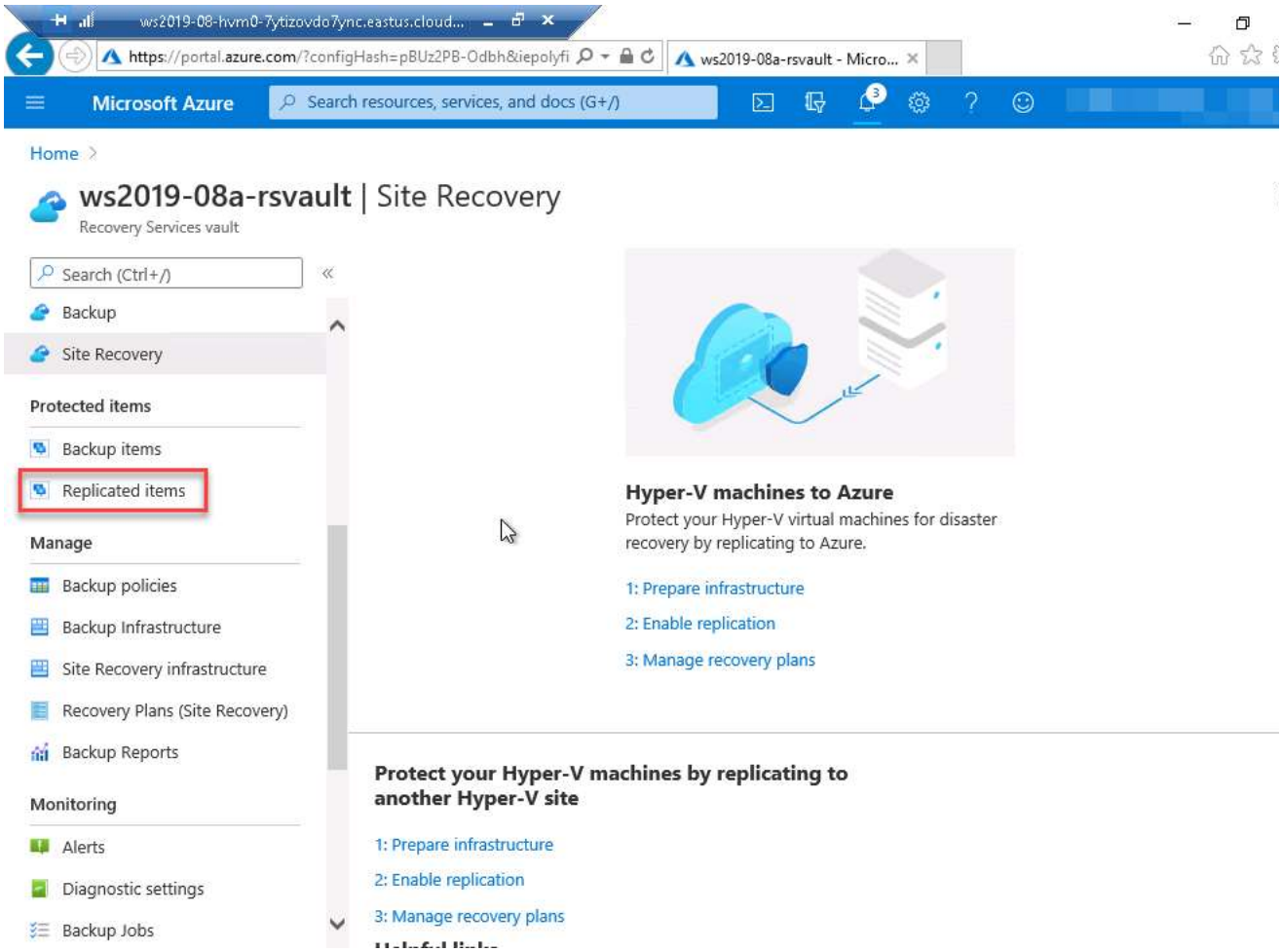


☐ 5. On the **Review** tab of the **Enable replication** blade, select **Enable replication**.



Task 3: Review Azure VM replication settings

- [ ] 1. In the Azure portal, back on the **myVault | Site Recovery** blade, in the vertical menu, select **Replicated items**.



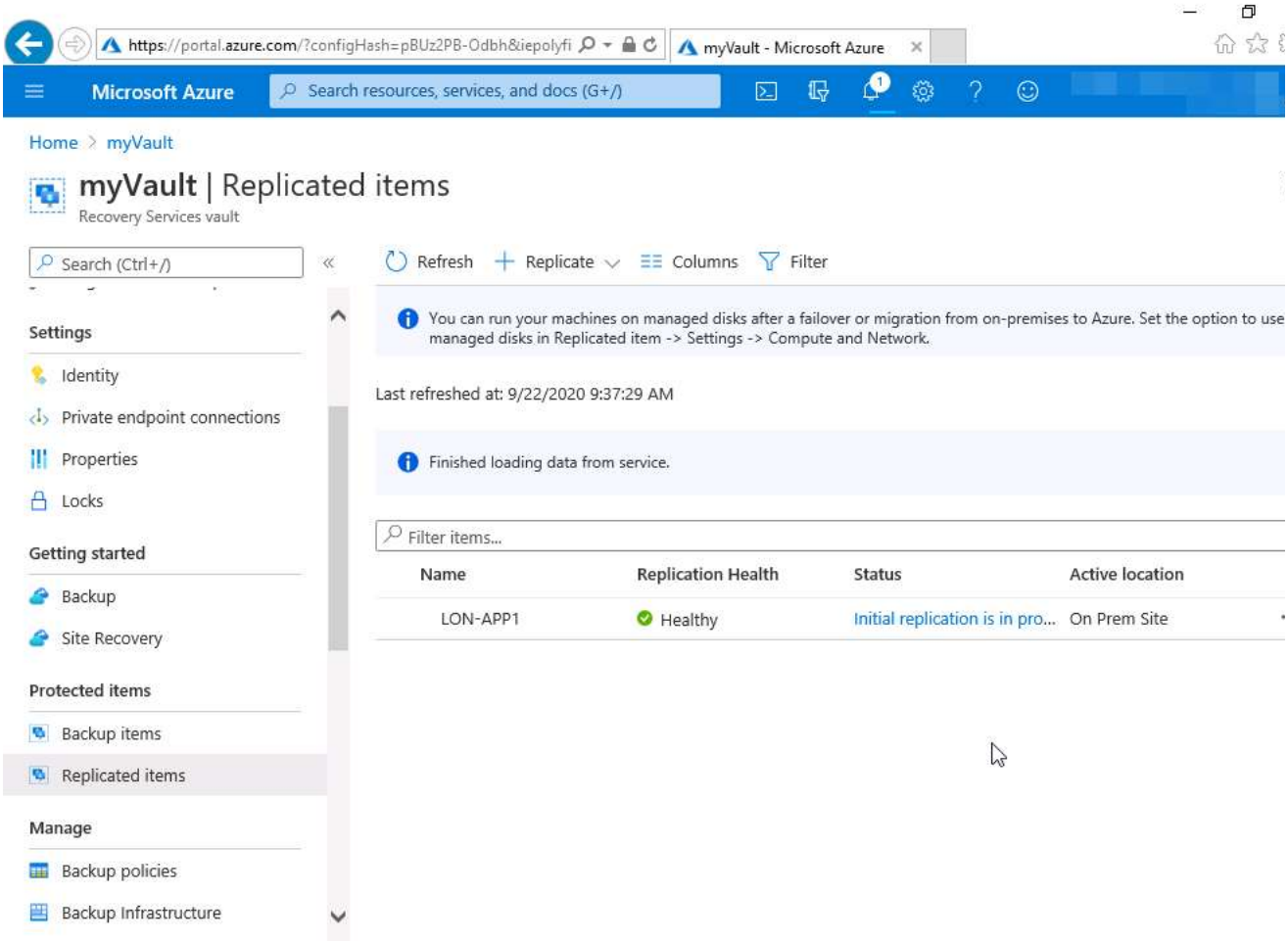
- [ ] 2. On the **myVault | Replicated items** blade, ensure that there is an entry representing the **LON-APP1** virtual machine and verify that its **Replication Health** is listed as **Healthy** and that its **Status** is listed as either **Enabling protection**, **Waiting for first recovery point**, or displaying a current percentage of synchronization progress.

> ⚠ **Note:** You might need to wait a few minutes until the **LON-APP1** entry appears on the **myVault | Replicated items** blade.

- [ ] 3. On the **myVault | Replicated items** blade, select the **LON-APP1** entry.

- [ ] 4. On the **LON-APP1** replicated items blade, review the **Health and status**, **Failover readiness**, **Latest recovery points**, and **Infrastructure view** sections. Note the **Planned Failover**, **Failover** and **Test Failover** toolbar icons.

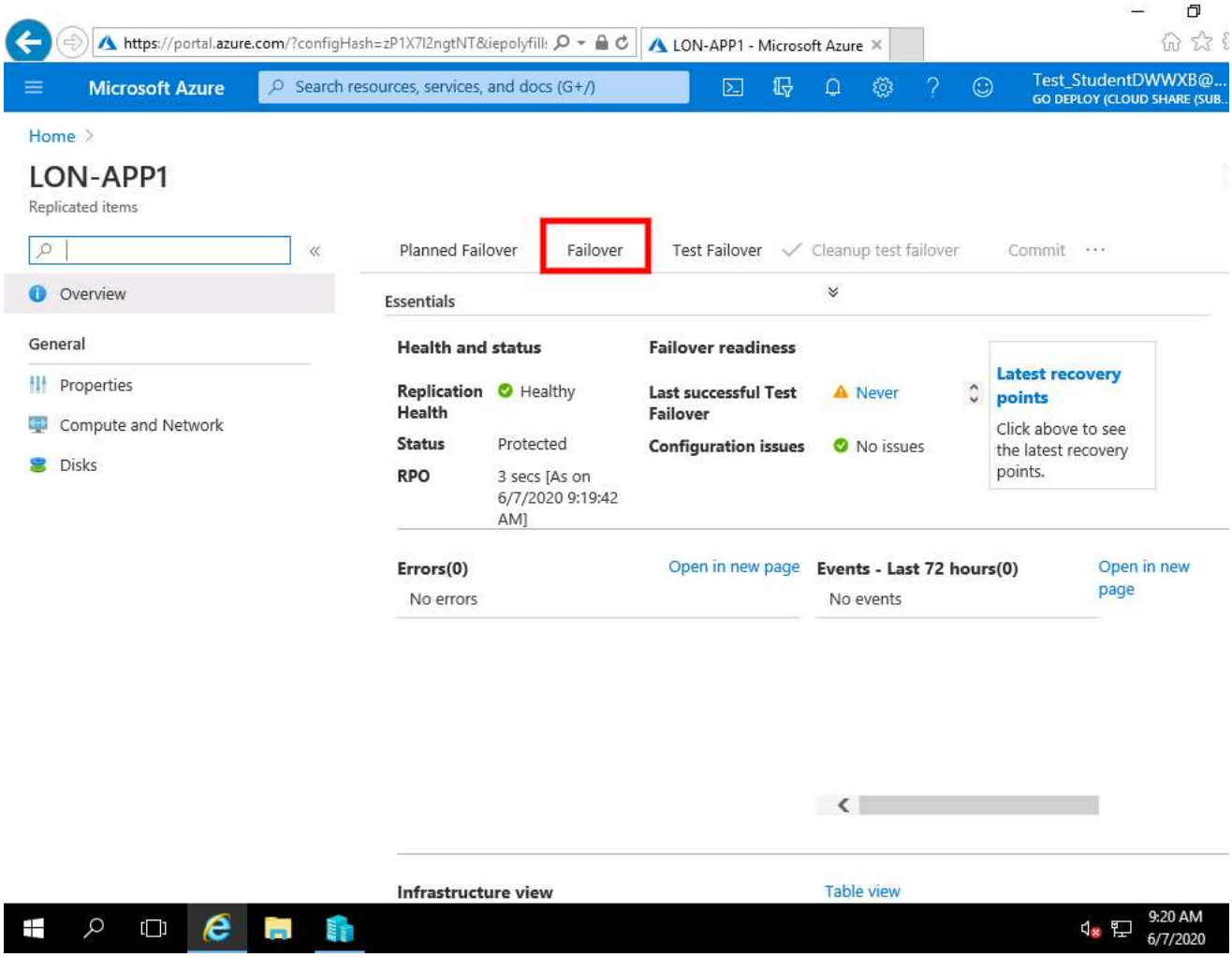
> ⚠ **Note:** Wait until the status changes to **Protected**. This might take additional 15-20 minutes. You will need to refresh the browser page for the status to be updated.



- [ ] 5. On the **LON-APP1** replicated items blade, select **Latest recovery points** and review **Latest crash-consistent** and **Latest app-consistent** recovery points.
- [ ] 6. On LON-HV1, in the browser window displaying the Azure portal, on the **LON-APP1** replicated items blade click **Compute and Network**.
- [ ] 7. Click **Edit** then change the VM size to **D2s_v3** and click **Save**.

Task 4: Failover to Azure

- [ ] 1. In **Protected items** > **Replicated items**, click **LON-APP1** > **Failover**.



2. Click **I understand the risk. Skip test failover** check box.

> ⚠ **Note**: In a real world environment you would test the failover to ensure it would be success in the event of a disaster.

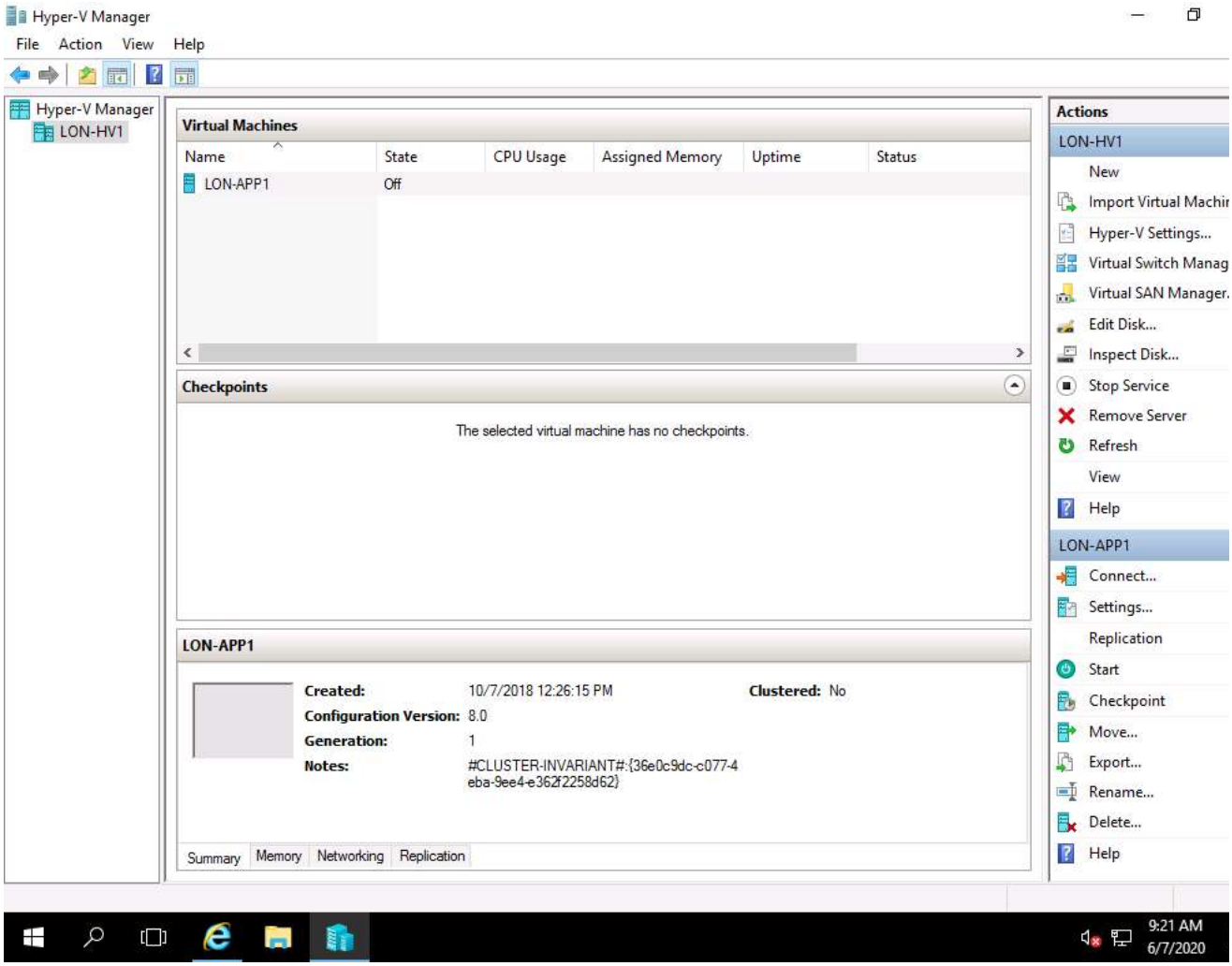
3. In **Failover**, select the **Latest processed (low RTO)** recovery point.

4. Select **Shut down machine before beginning failover** and click **OK**.

> ⚠ **Note**: Site Recovery attempts to do a shutdown of source VMs before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.

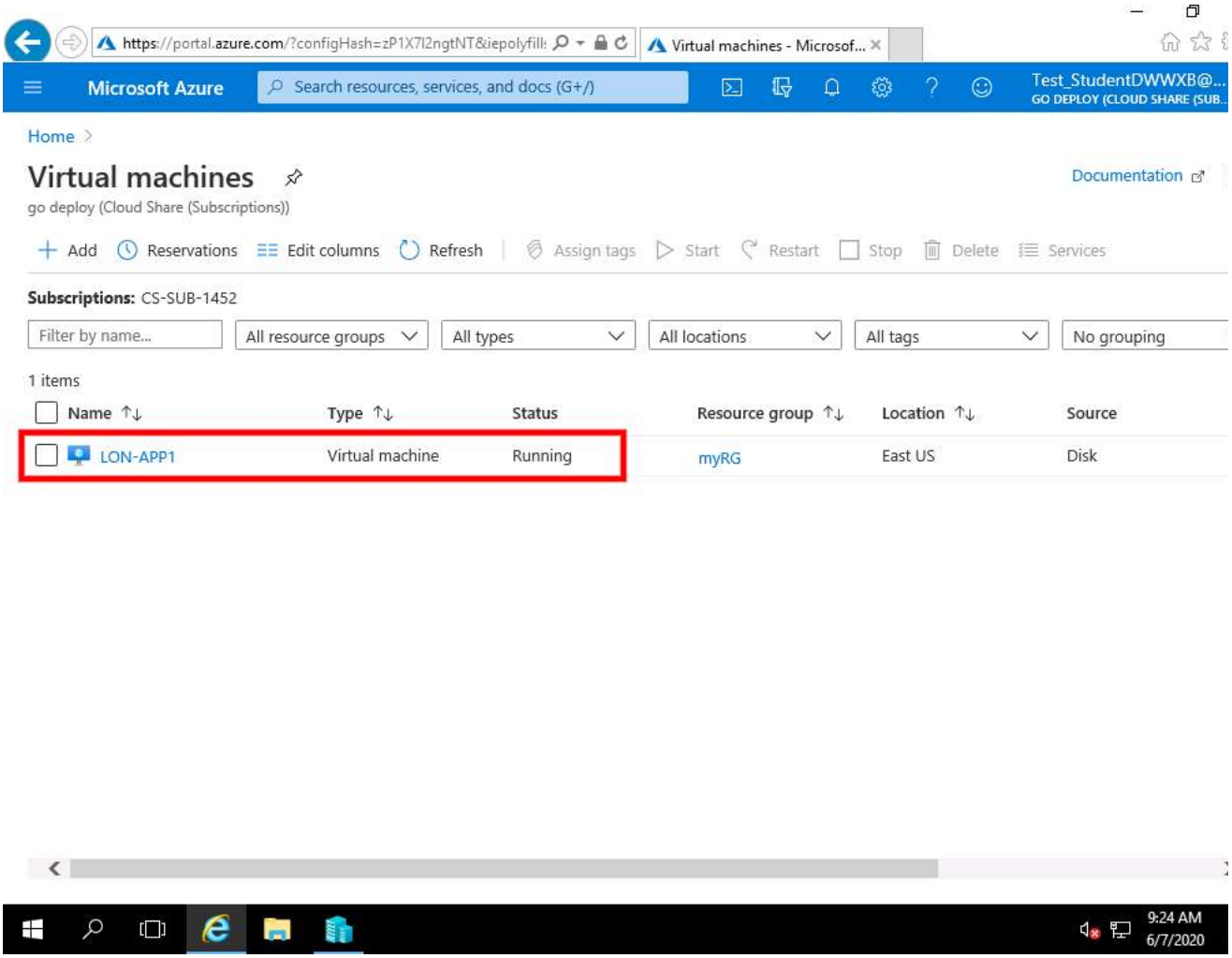
> ⚠ **Note**: Never cancel a **Failover in progress**: If you cancel in progress, failover stops, but the VM won't replicate again.

5. Open Hyper-V manager and after a short period you will see the virtual machine is shutdown.

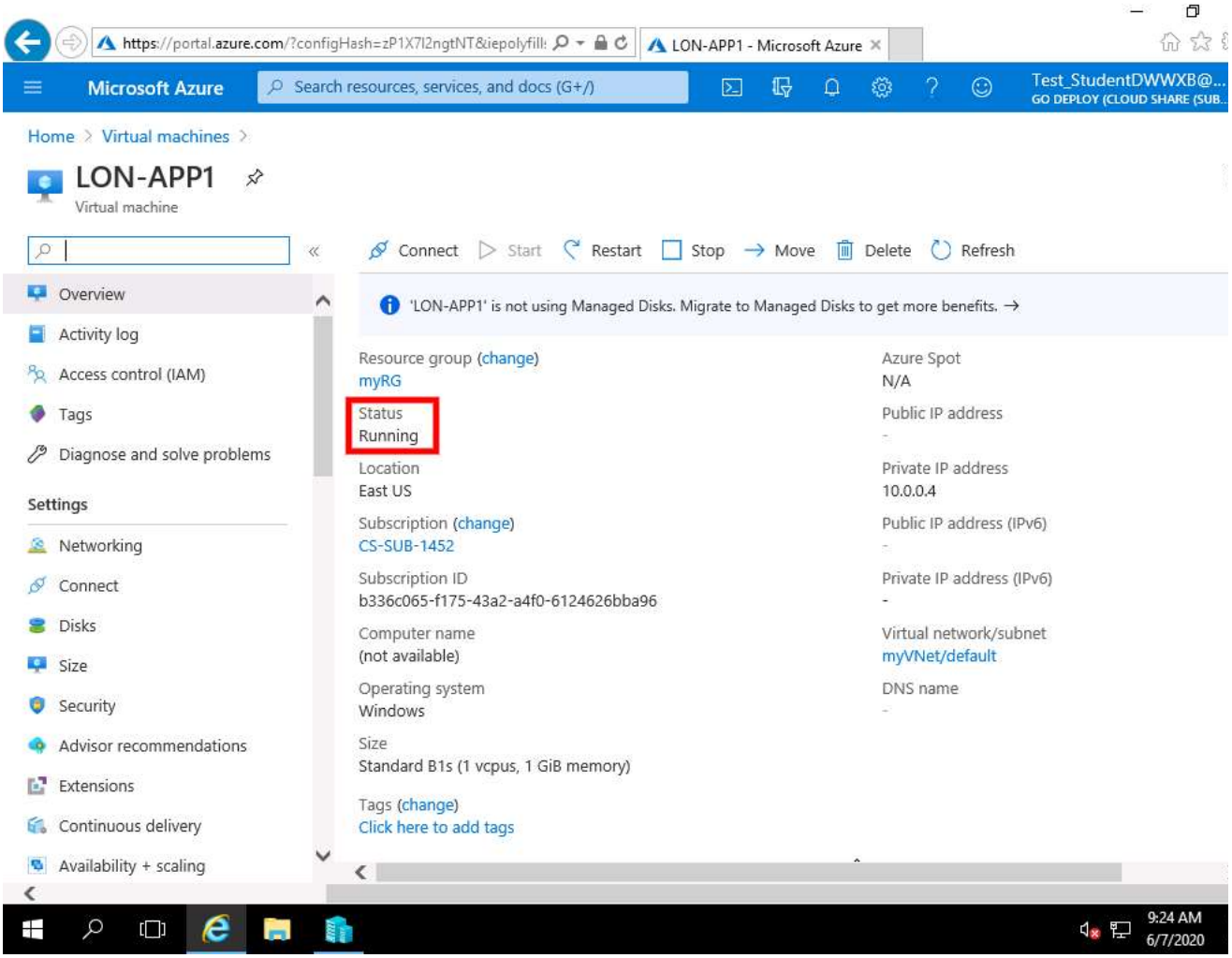


Task 5: Verify the failover to Azure

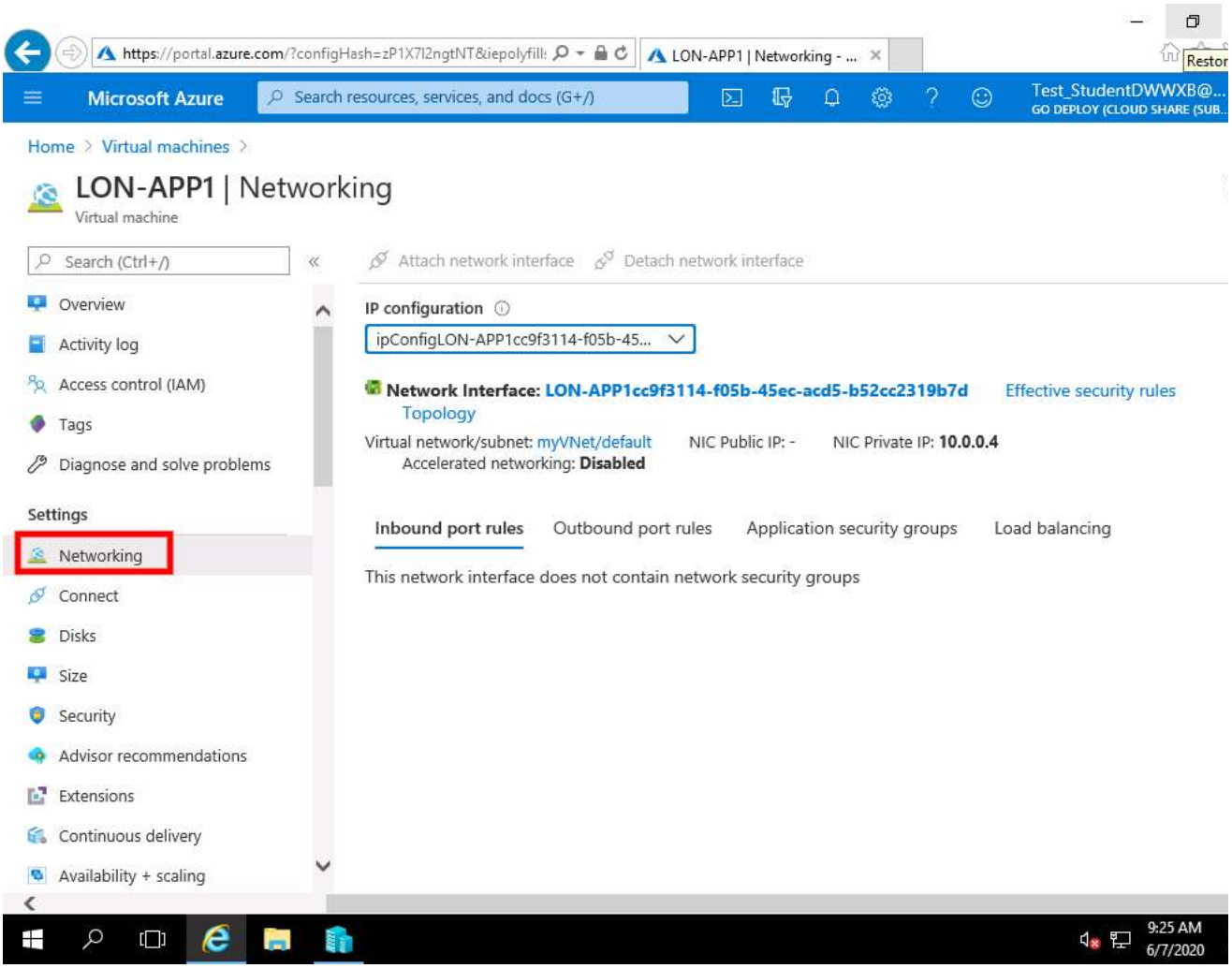
- [ ] 1. In the **Azure Portal** click **Virtual Machines** and select **LON-APP1**.



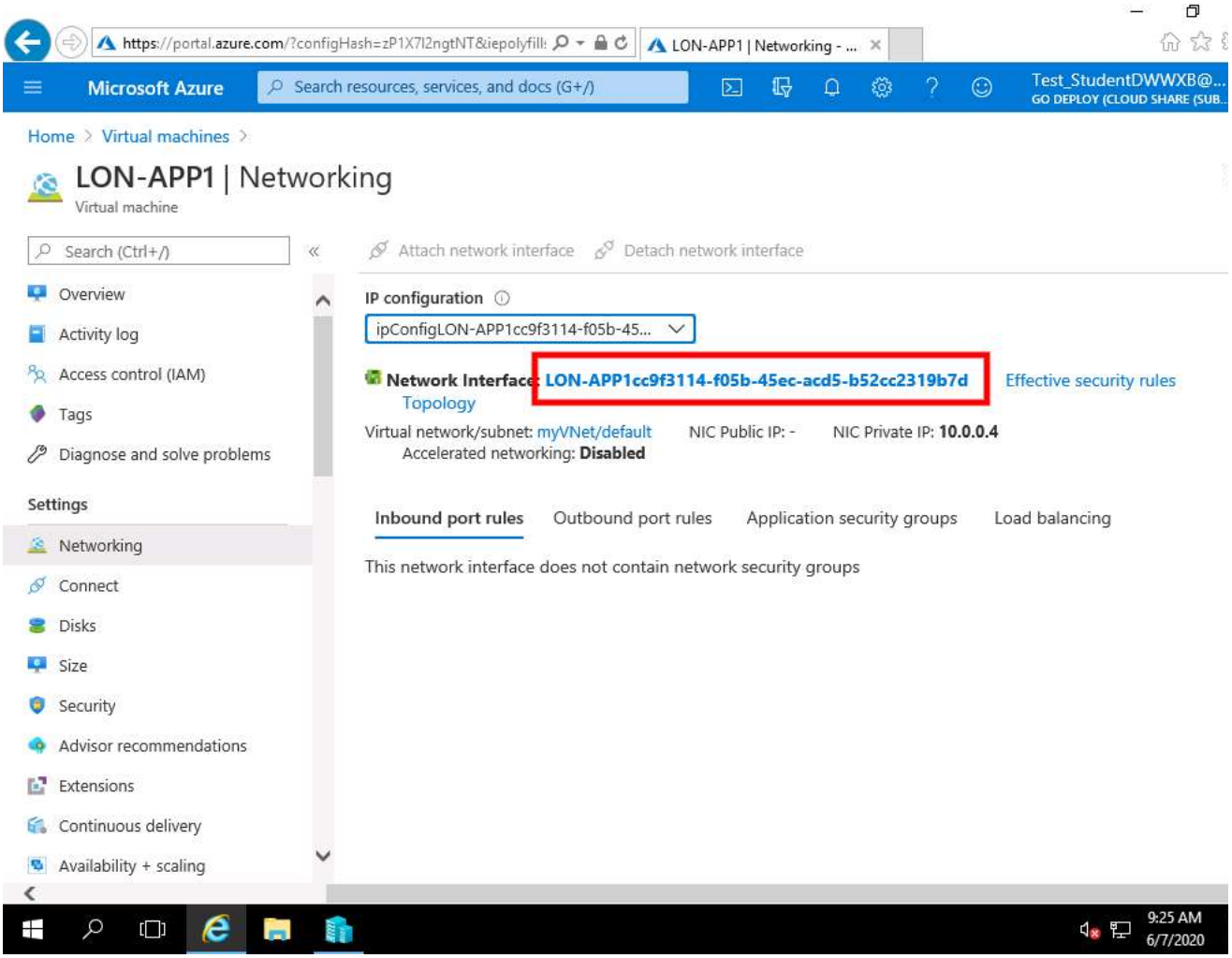
☐ 2. On the overview blade note that the Virtual Machine is running.



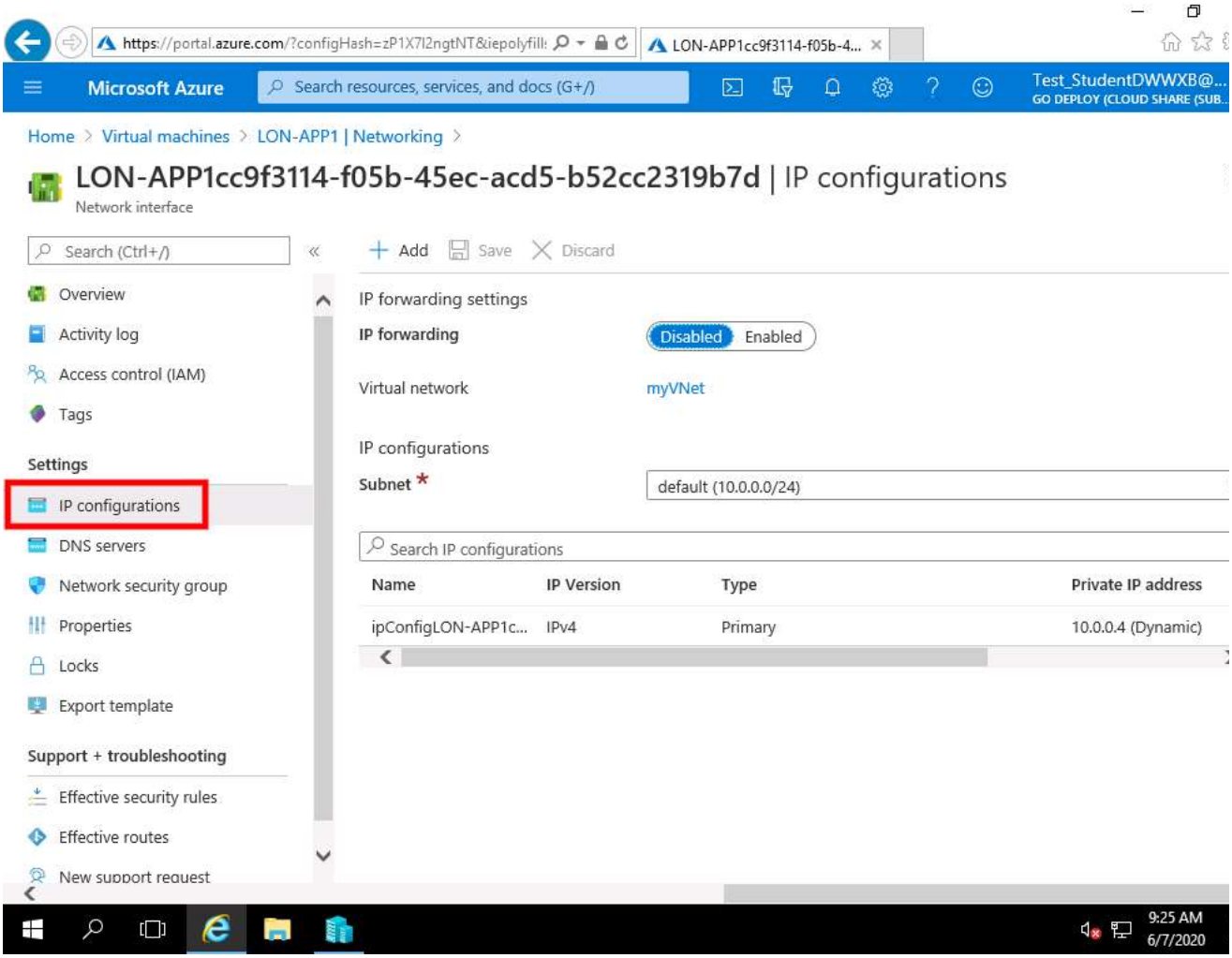
☐ 3. Click Networking. Notice that the Virtual Machine now has an IP Address from the Virtual Network you created in an earlier task.



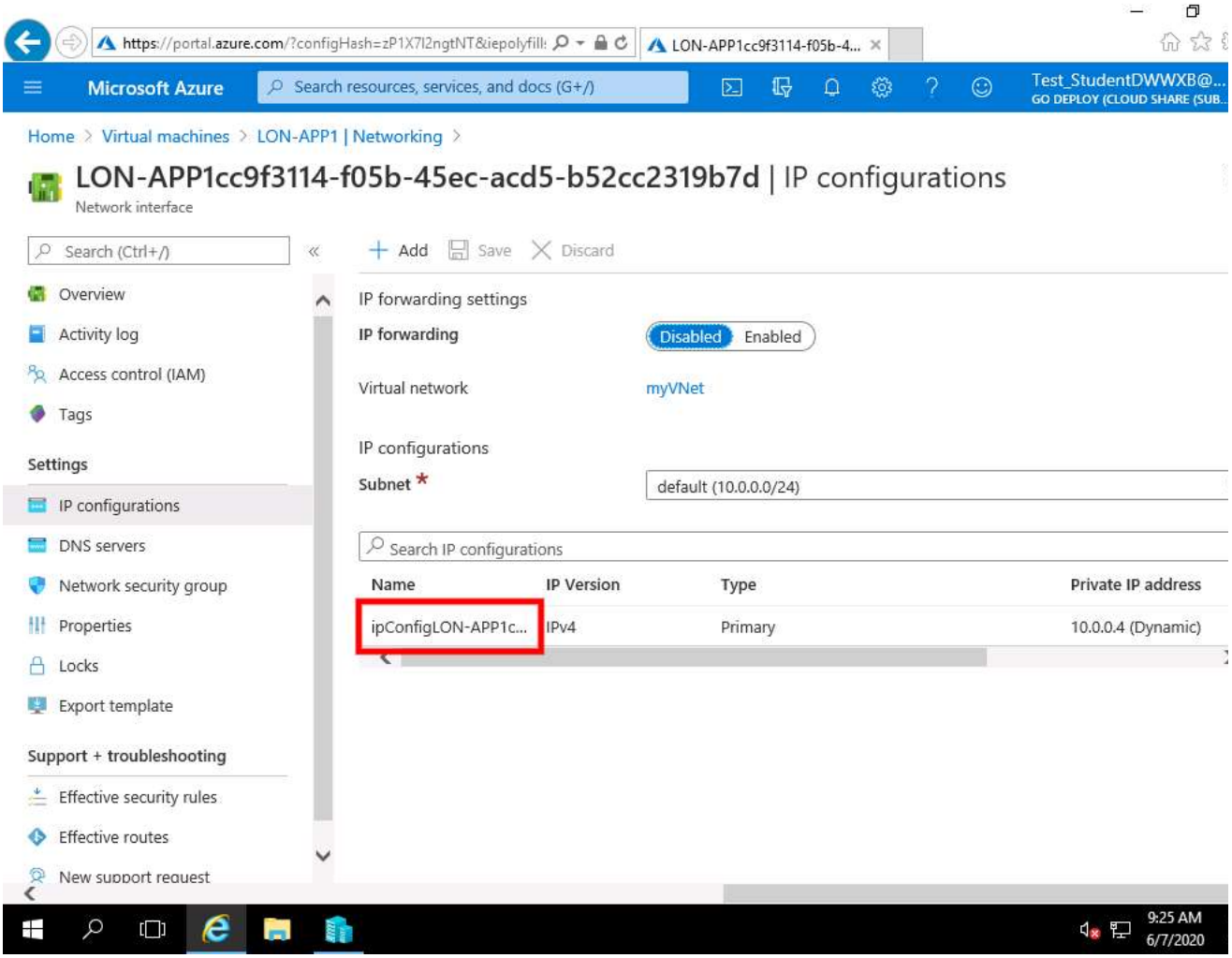
- [ ] 4. Click on the **Network Interface**.



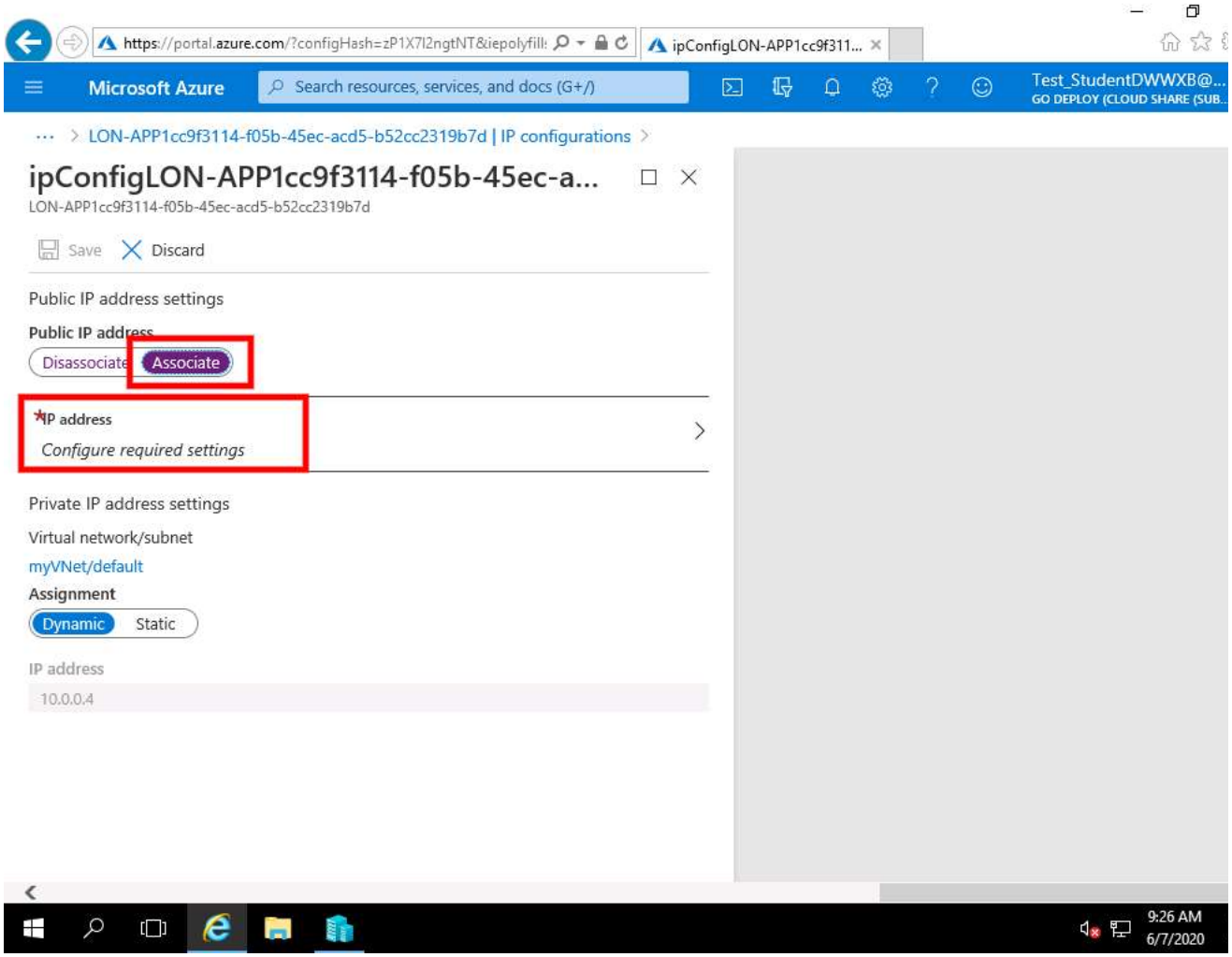
☐ 5. Click **IP Configurations**.



☐ 6. Click on **ipConfig1**.

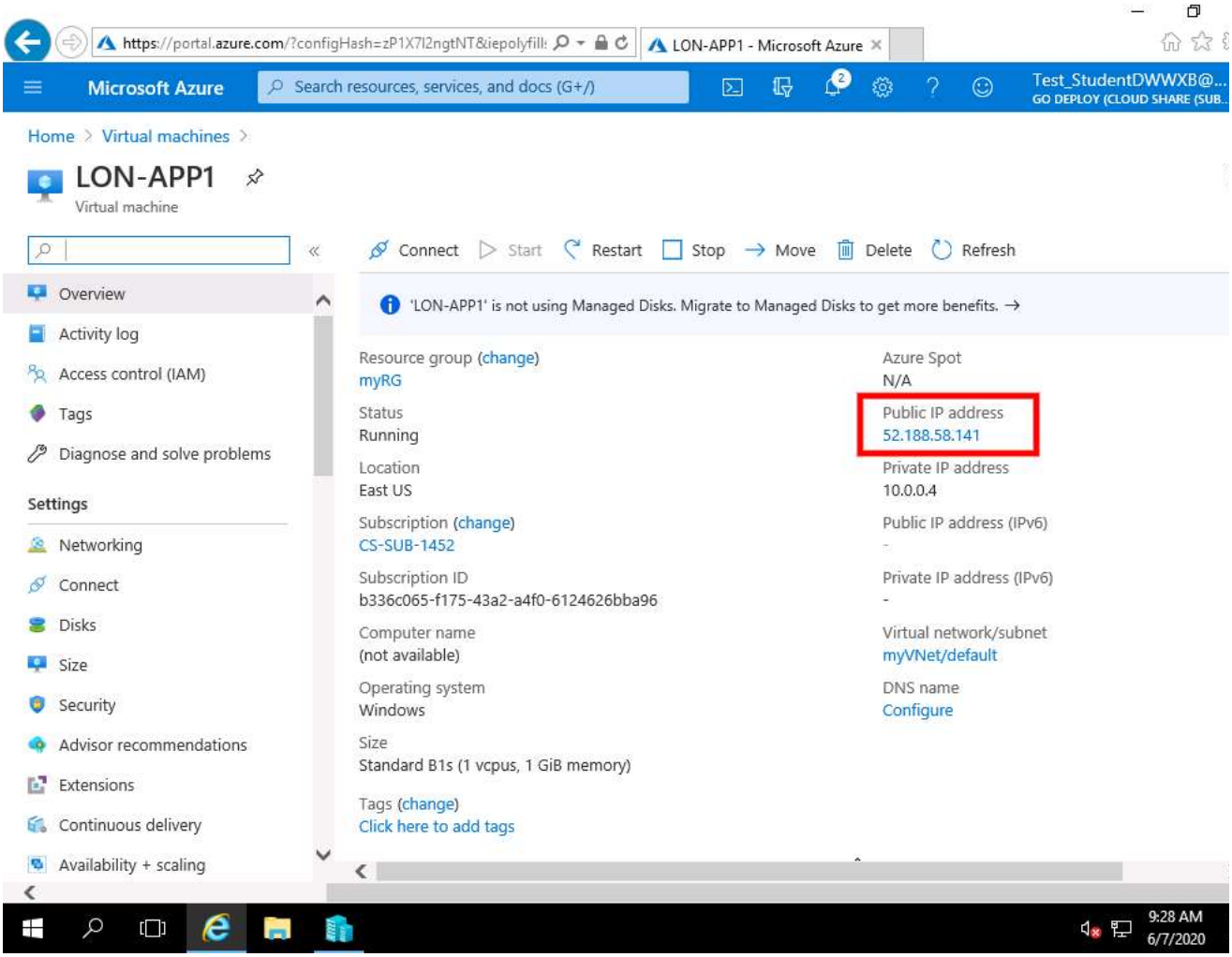


- [ ] 7. On the Public IP Address click **Associate** and then click **Create New** and Enter a name for your public IP Address. Click **Ok**. This will create a new Public IP and allocated it to the Network Interface of the Virtual Machine.



- [ ] 8. Click **Save** and wait for the deployment to complete.

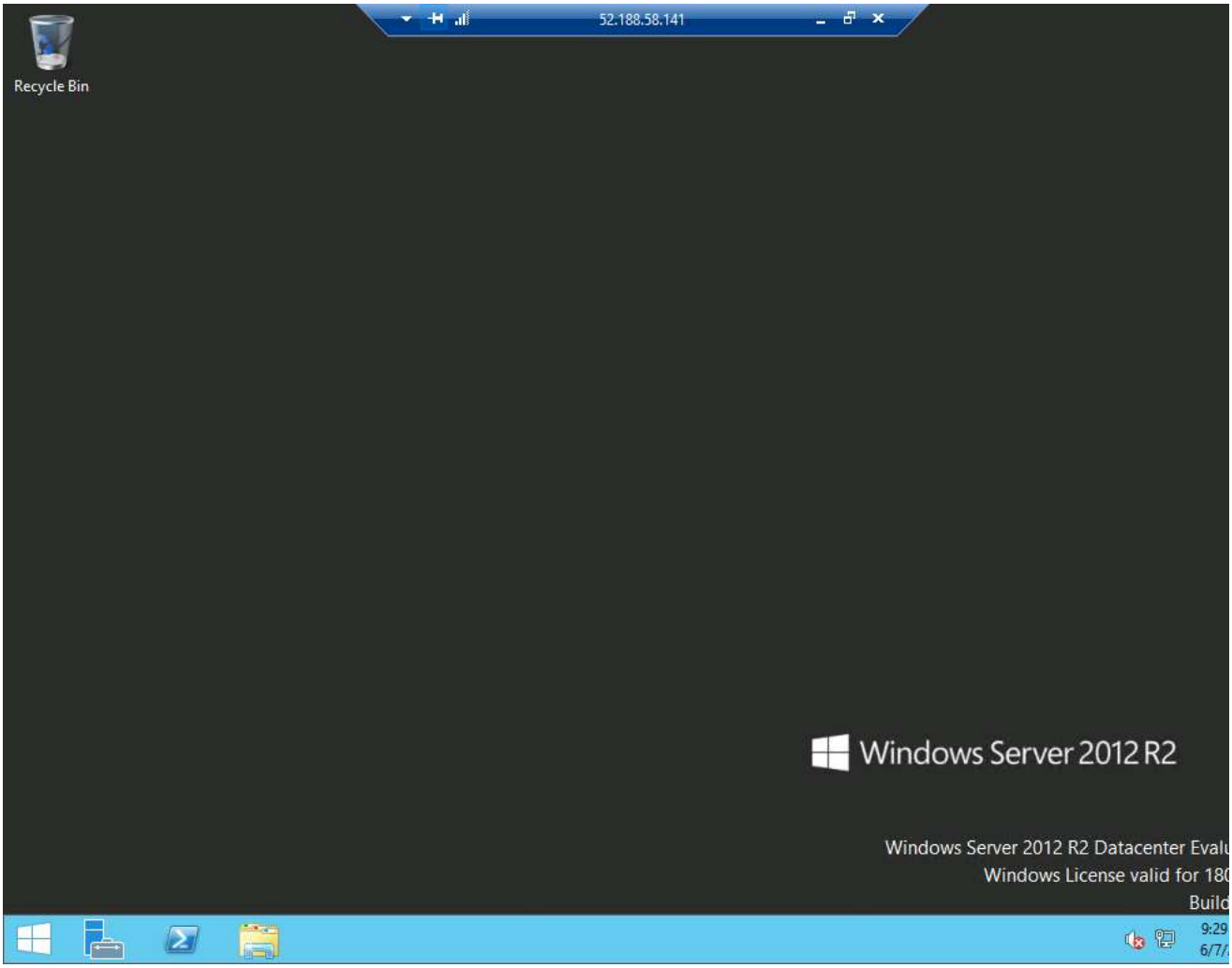
- [ ] 9. Navigate back to the **Virtual Machine** blade and notice the Virtual Machine now as a Public IP Address.



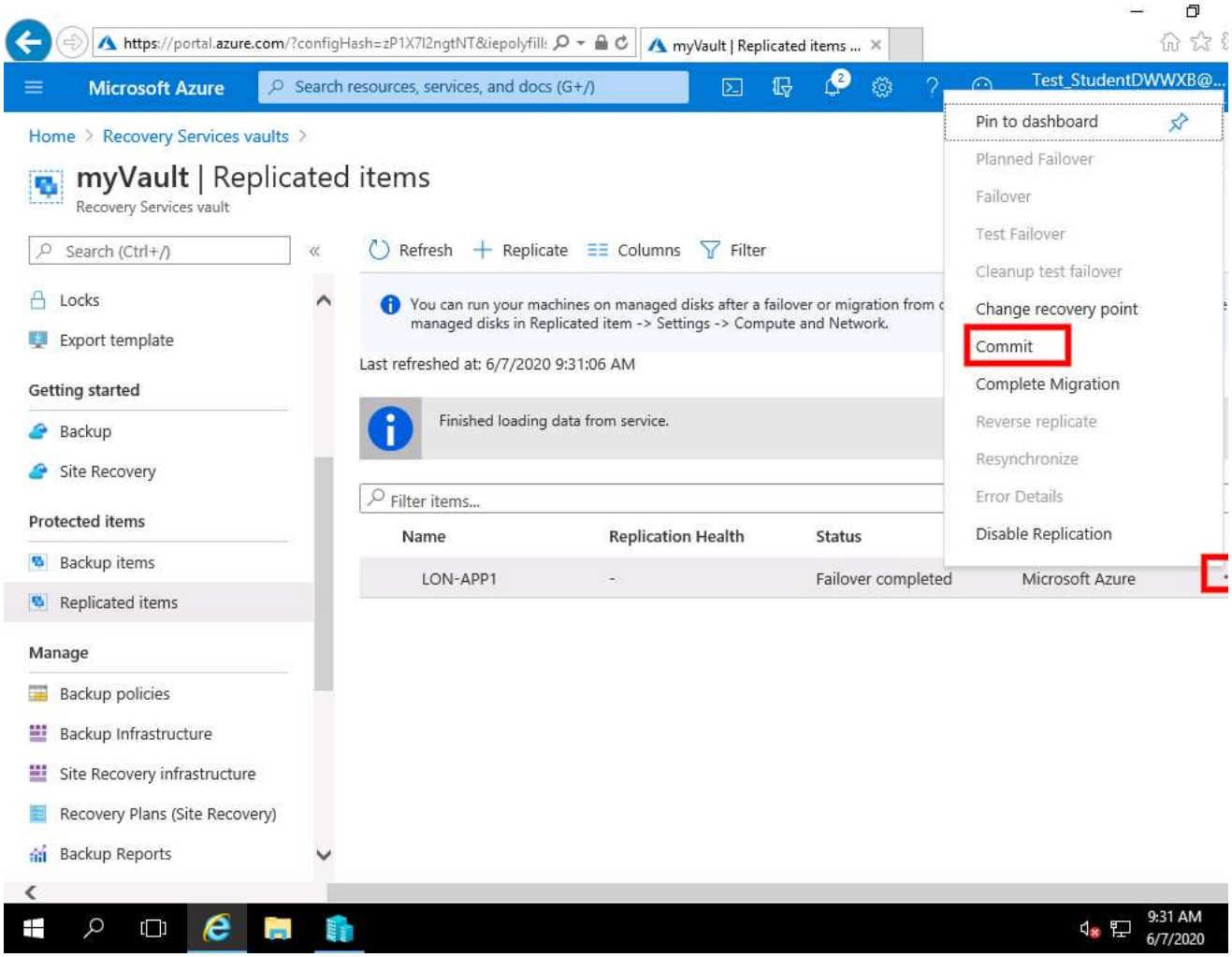
- [ ] 10. Click **Connect** > **RDP** and download and open the RDP file and click Connect.

- [ ] 11. Login with the following credentials:

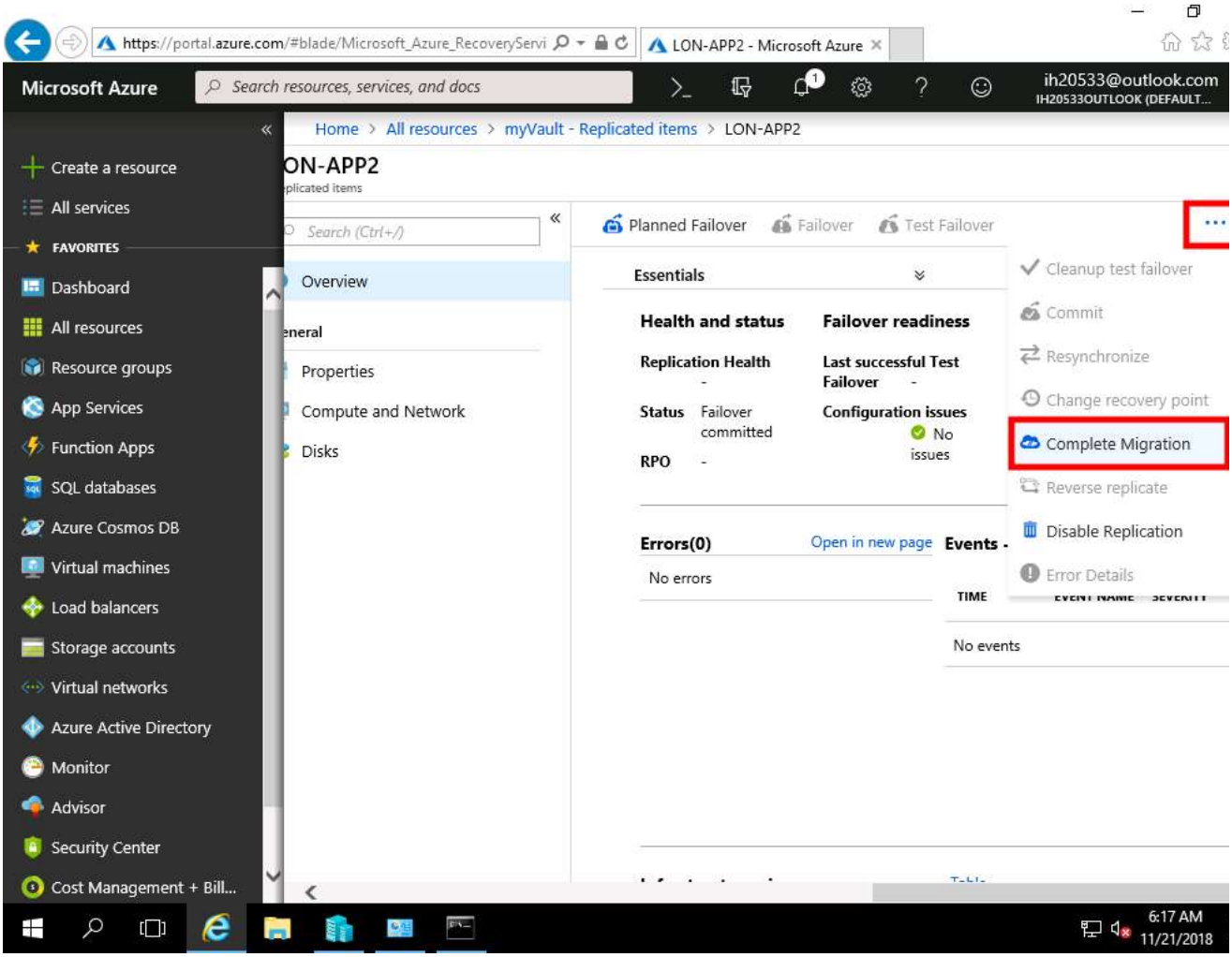
  - **Username**: .\administrator
  - **Password**: Pa55w.rd



- [ ] 1. Exit the Virtual Machine RDP connection.
- [ ] 2. Nagivate back to your **Recovery Services vault** > **Replicated Items**
- [ ] 3. Click **...More** and click **Commit** and then click **OK**. It deletes all the available recovery points.



- [ ] 4. Click **...More** and then click **Complete Migration** then click **OK**.



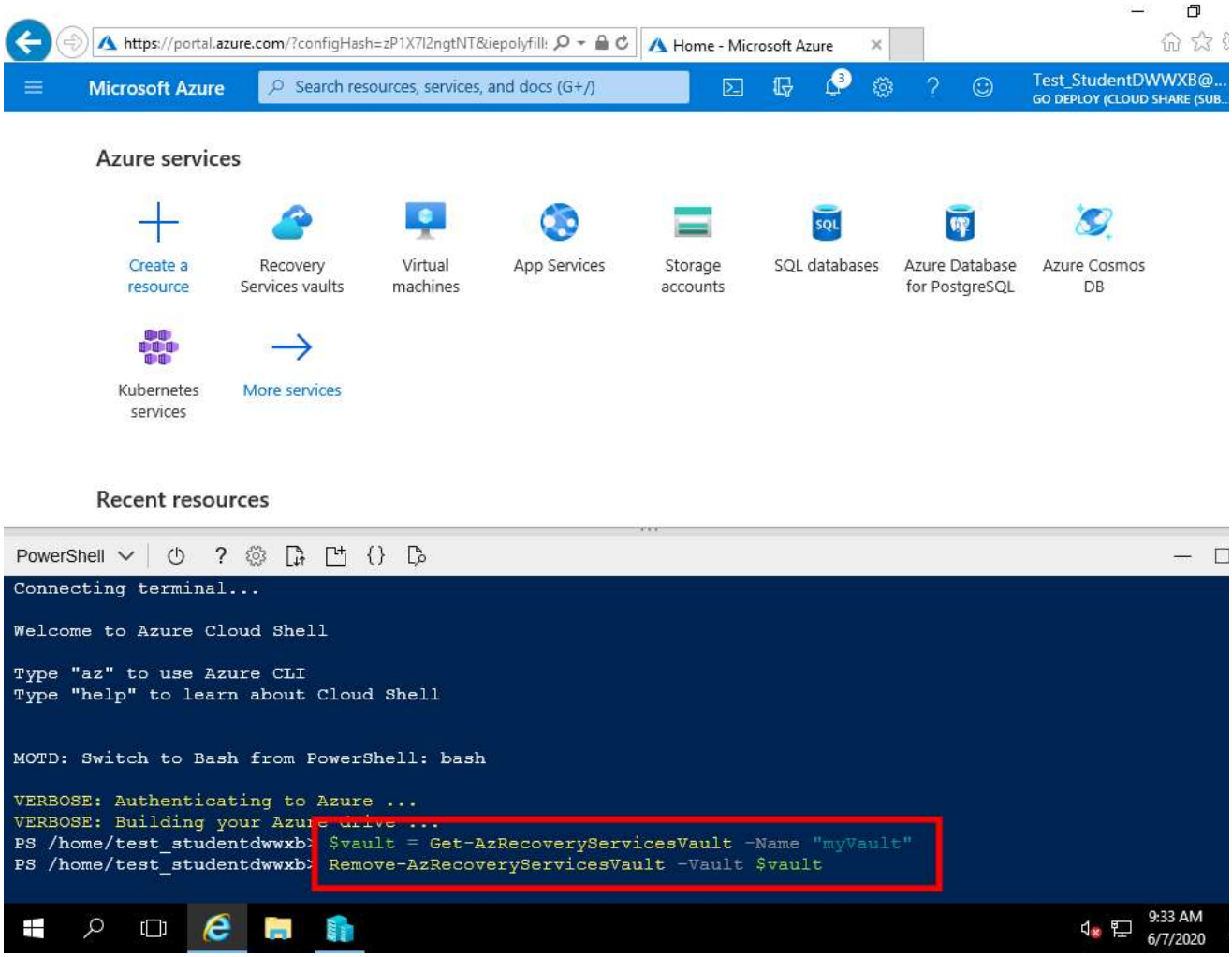
- [ ] 5. Wait for the commit task to complete.

Task 6: Clean up the environment.

- [ ] 1. Open the Cloud Shell PowerShell and type the following command:

```
$vault = Get-AzRecoveryServicesVault -Name "myVault"
```

```
Remove-AzRecoveryServicesVault -Vault $vault
```



- [ ] 2. Close the Cloud Shell and delete any remaining Resource Groups from the Azure Portal.

✓ **Results** : You have now completed this lab.