

Azure Site Recovery

Contents

Azure to Azure Site Recovery with ASR.....	2
Before you Begin	2
Create a IaaS Web Server	2
Build the VM	2
Install and Configure IIS	3
Modify the NSG	3
Confirm Web Traffic	4
Create a vault	4
Enable replication	4
Select the source	4
Track Replication	5
Run a Test Failover Disaster Recovery Drill	6

Azure to Azure Site Recovery with ASR

In this lab you will create a VM in Azure, install IIS, enable replications, and with time permitting failover the VM to a different Azure region.

Before you Begin

If you are using a Microsoft Azure subscription that was provided to you by Microsoft, you are limited to a specific set of Microsoft Azure regions that you can use. **Please use either the East US, South Central US, West Europe, Southeast Asia, West US 2, or West Central US locations.**

Your subscription doesn't support virtual machine creation in West US. Choose a different location. Supported locations are: East US, South Central US, West Europe, Southeast Asia, West US 2, West Central US.
[Learn more](#)

Otherwise you will receive the following error in the portal if you select an unsupported region and attempt to build anything in Microsoft Azure.

Create a IaaS Web Server

Build the VM

1. Return to the Azure portal and click the **Create a Resource** button (the Plus) found on the upper left-hand corner of the Azure portal.
2. Select **Compute** from the **New** blade, then select **Windows Server 2016 Datacenter**.
3. Fill out the virtual machine **Basics** form and click **OK**:
 - a. **Subscription:** Azure Pass
 - b. **Resource Group:** *(Create New)* EastWebServers
 - c. **Name:** Webby
 - d. **Region:** East US
 - e. **Size:** Standard DS1v2
 - i. Is the 'Standard DS1v2 sku is not available in your selected region, select a VM with the lowest cost and at least 1 CPU and 3.5GB RAM (the options will vary based upon your subscription type).
 - f. Under **Administrator Account**
 - i. **Username:** WebAdmin
 - ii. **Password:** Complex.Password
 - g. Under **Inbound Port Rule**
 - i. **Public inbound ports:** Allow selected ports
 - ii. **Select inbound ports:** RDP (3389)
4. Click **Next : Disks >**
5. On the Disks settings blade
 - a. **OS disk type:** standard HDD

- b. Open **Advanced** settings and select **No** under **Use managed disks**. Keep the other settings as defaults.
6. Click **Review + Create** and then select **Create** to start the virtual machine deployment.
7. To monitor deployment status, click the "Deploying Windows Server 2016 Datacenter" tile. The VM can be found on the Azure portal dashboard, or by selecting **Virtual Machines** from the left-hand menu. It should take less than 10 minutes to spin up the VM.
8. When the VM has been created, the status changes from **Creating** to **Running**.

Install and Configure IIS

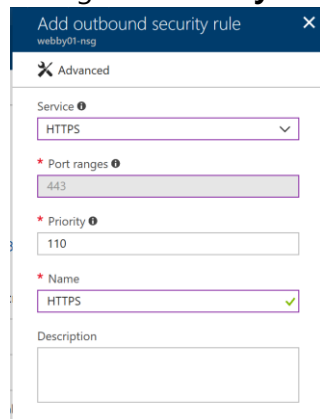
1. Connect to the Webby VM and logon as webby\WebAdmin.
2. When prompted, click **No** on the Networks blade.
3. Within Server Manager, select **Add Role and Features** under **Manage**.
4. Click **Next** three times.
5. On the Select server roles screen, select **Web Server (IIS)**, then **Add Features**, then **Next** four times. Click **Install** and then **Close** when installation completes.
6. Click on **Tools** then **Internet Information Servers (IIS) Manager**.
7. Expand **Webby** until you can select the **Default Web Site**. Right click on **Default Web Site** and choose **Explore**.
8. Start Notepad as an Admin
9. Modify the iisstart.html file with notepad and change <title>IIS Windows Server</title> to <title>Webby</title>. Save and close the file.

Modify the NSG

Ports 80 443 are not allowed through the default Network Security Group. You will need to open these ports.

1. In the Azure Portal click **Resource Groups** then **EastWebServers**.
2. Click on the **Webby-nsg**.
3. Under Setting, select **Inbound security rules** then **+Add**.
4. Enter the following and click **OK**:
 - a. Destination port ranges: 80
 - b. Protocol: TCP
 - c. Name: HTTPIn
5. Under Setting, select **Outbound security rules** then **+Add**.
6. Enter the following and click **OK**:
 - a. Destination port ranges: 80
 - b. Protocol: TCP
 - c. Name: HTTPOut
7. Select **Outbound security rules** then **+Add**
 - a. Click the **Basic** button if it is present
 - b. Under **Service** Select **HTTPS**

c. Change the **Priority** to **110**



Confirm Web Traffic

1. In the Azure Portal click **Resource Groups** then **EastWebServers**.
2. Click on the Webby VM and copy the Public IP address.
3. With a browser surf to this public IP address to confirm you are hitting your IIS server and web traffic is coming through. The name in the browser tab should be **Webby IIS Server**.

Create a vault

Create the vault in an approved region, except the source region.

- 1) On the Portal blade menu, click **All services** and in the all services search box, type **Recovery Services** and click **Recovery Services vaults**.
- 2) On the **Recovery Services vaults** menu, click **Add**.
- 3) The Recovery Services vault blade opens, enter the following:
 - a. **Name:** WestDRVault
 - b. **Subscription:** Azure Pass
 - c. **Resource group:** Create New *DRaaSWest*
 - d. **Location:** West US 2
- 4) At the bottom of the Recovery Services vault blade, click **Create**.

Enable replication

Select the source

- 1) In the Azure Portal click **Resource Groups** then **DRaaSWest**.
- 2) Click on **WestDRVault** and then **+Replicate**.
- 3) In **Source**, enter the following and Click **OK**:
 - a. **Source:** Azure
 - b. **Source location:** East US
 - c. **Azure virtual machine deployment model:** Resource Manager
 - d. **Source resource group:** EastWebServers
- 4) On the **Select Virtual Machines Blade** select **Webby** and click **OK**.

- 5) On the Configure settings blade set the **Target Location** to **West US 2** and click **Create target resources**.
- 6) Once validation completes, click **Enable Replication**.

Track Replication

You can track replication status the following:

1. In the Azure Portal under your recovery vault, choose **Monitoring > Site Recovery Jobs**. Monitor the Site Recovery job.

Depending on the size of the source VM you chose Error ID 150050 may occur (The Completed with information message). The means the source VM size is not available in the target geo. You may need to update the target VM's size prior to failover if desired.

Site Recovery jobs

WestDRVault

Filter


Export jobs

Filter items...

NAME	STATUS	TYPE	ITEM	START TIME	DURATION
Enable replication	Completed with information	Protected item	webby	1/6/2018 12:40:08 PM	00:08:10
Associate replication policy	Successful	Replication policy	24-hour-retention-policy	1/6/2018 12:38:45 PM	00:01:09
Associate replication policy	Successful	Replication policy	24-hour-retention-policy	1/6/2018 12:37:23 PM	00:01:08
Map Networks	Successful	Network	eastwebservers-vnet-asr	1/6/2018 12:37:18 PM	00:00:03
Create protection container	Successful	Cloud	asr-a2a-default-westus2-cont...	1/6/2018 12:36:45 PM	00:00:00
Map Networks	Successful	Network	eastwebservers-vnet	1/6/2018 12:36:45 PM	00:00:03
Create a site	Successful	Server	asr-a2a-default-westus2	1/6/2018 12:35:38 PM	00:01:04
Create protection container	Successful	Cloud	asr-a2a-default-eastus-contai...	1/6/2018 12:35:38 PM	00:00:00
Create a site	Successful	Server	asr-a2a-default-eastus	1/6/2018 12:34:31 PM	00:01:05
Create replication policy	Successful	Replication policy	24-hour-retention-policy	1/6/2018 12:34:30 PM	00:00:01

2. Once Enable Replication is complete, in the Azure Portal click **Protected Items > Replicated Items** to examine the synchronization status of the VM. Hit Refresh to monitor replication status. It may take 15-30 minutes to replicate the VM, so now is an appropriate time to take a break.

Last refreshed at: 1/6/2018 1:09:44 PM

 Finished loading data from service.

Filter items...			
NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION
Webby	Healthy	Protected	East US

Until the VM is 100% synchronized and Protected, a test failover is not possible. It may take several hours for your VM to replicate in a production environment.

Run a Test Failover Disaster Recovery Drill

Before you run a test failover, verify the VM properties to make sure everything's as expected. Access the VM properties in **Replicated items**. The **Essentials** blade shows information about machines settings and status.

Search (Ctrl+ /)

Overview

GENERAL

Properties

Compute and Network

Disks

Failover Test Failover Cleanup test failover

Essentials ^

Recovery Services vault
WestDRVault

Active location
East US

Replication policy
24-hour-retention-policy

Target location
West US 2

Operating system
Windows

Target resource group
EastWebServers-asr

Protected disks
1


Target storage account
eastwebserverdisks2asr

Target size
Standard_G1

Target network
eastwebserver-vnet-asr

Replication

Health	Events
Replication health Healthy	0
Status Protected	
RPO 56 seconds [As on 1/6/201...	
Latest Recovery Points	
Crash-consistent 1/6/2018, 9:19:31 AM	
App-consistent 1/6/2018, 8:06:34 AM	



A test failover executes a failover but does not make the secondary VM active. A drill validates your replication strategy without data loss or downtime and doesn't affect your production environment.

1. Click the VM **Test Failover** icon.
2. In **Test Failover**, select **Latest (lowest RPO)** as the recovery point to use for the failover. Note the following:
 - a. **Latest (lowest RPO)**: Fails the VM over with the current state of the VM but requires some processing time.
 - b. **Latest processed (low RTO)**: Fails the VM over to the latest recovery point that was processed by the Site Recovery service. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO (Recovery Time Objective)
 - c. **Latest app-consistent**: This option fails over all VMs to the latest app-consistent recovery point. The time stamp is shown.
 - d. **Custom**: Use this option to fail over to a specific recovery point. This option is useful for performing a test failover.
3. Select **EastWebServers-vnet-asr** as the target Azure virtual network to which Azure VMs in the secondary region will be connected after the failover occurs.
4. To start the failover, click **OK**. To track progress, click the VM to open its properties or the alert in the Notifications window. Lastly, you can click the **Test Failover** job in the vault name > **Monitoring** > **Site Recovery jobs**.
5. After the failover finishes (Start the virtual machine is successful), the replica Azure VM appears in the Azure portal > **Virtual Machines**. Make sure that the VM is running, sized appropriately, and connected to the appropriate network.

The screenshot shows the 'Virtual machines' page in the Azure portal. At the top, there's a header with 'Virtual machines' and 'ppesa2outlook (Default Directory)'. Below the header is a toolbar with icons for '+ Add', 'Columns', 'Refresh', 'Assign Tags', 'Start', 'Restart', 'Stop', and 'Delete'. A filter bar shows 'Subscriptions: Azure Pass' and a search box 'Filter by name...'. Below the filter bar, it says '2 items'. The table has columns: NAME, TYPE, STATUS, RESOURCE GROUP, LOCATION, MAINTENANCE, and SUBSCRIPTION. There are two rows: 'Webby' (Virtual machine, EastWebServers, East US, Azure Pass) and 'Webby-test' (Virtual machine, EastWebServers-asr, West US 2, Azure Pass).

NAME	TYPE	STATUS	RESOURCE GROUP	LOCATION	MAINTENANCE	SUBSCRIPTION
Webby	Virtual machine		EastWebServers	East US		Azure Pass
Webby-test	Virtual machine		EastWebServers-asr	West US 2		Azure Pass

6. To delete the VMs that were created during the test failover, in your vault under **Protected Items > Replicated items**, select your VM and then click the Content Menu (the three buttons on the right) and choose **Cleanup test failover**. In **Notes**, record and save any observations associated with the test failover. Click the box for **Testing is complete** and click **Ok**.

If you don't delete the failover VM, the VM will continue to run and increase your Azure consumption.