



Microsoft Cloud Workshop

Business continuity and disaster recovery
Hands-on lab step-by-step

March 2018

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of manufacturers, products, or URLs are provided for informational purposes only, and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links may be provided to third-party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

© 2018 Microsoft Corporation. All rights reserved.

Microsoft and the trademarks listed at <https://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/Usage/General.aspx> are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

Contents

Business continuity and disaster recovery hands-on lab step-by-step	1
Abstract and learning objectives.....	1
Overview.....	1
Solution architecture	2
Environment: On-premises (migrate to Azure).....	2
Environment: Azure IaaS (failover region to region).....	3
Environment: Azure PaaS (high-available with seamless failover)	4
Requirements.....	4
Before the hands-on lab.....	5
Task 1: Create a virtual machine to execute the lab.....	5
Task 2: Download hands-on lab step by step support files to LABVM.....	8
Task 3: Install SQL Server Express on LABVM	8
Task 4: Create the resource groups	10
Exercise 1: Deploy Azure environments.....	13
Task 1: Deploy Azure IaaS.....	13
Task 2: Deploy on-premises environment.....	14
Task 3: Deploy Azure PaaS environment	16
Exercise 2: Configure BCDR services	18
Task 1: Create Azure recovery services vault.....	18
Task 2: Deploy Azure automation.....	18
Exercise 3: Configure environments for failover	29
Task 1: Configure on-premises to Azure IaaS failover for migration	29
Task 2: Configure IaaS SQL Always On availability groups for region to region failover	50
Task 3: Configure IaaS for region to region failover	78
Task 4: Configure PaaS for region to region failover	87
Exercise 4: Simulate failovers	110
Task 1: Failover Azure IaaS region to region	110
Task 2: Migrate the on-premises VM to Azure IaaS.....	118
Task 3: Failover and fallback Azure PaaS	123
Task 4: Fallback Azure IaaS region to region	130
After the hands-on lab.....	140
Task 1: Disable replication in the recovery services vault	140
Task 2: Delete all BCDR resource groups	141

Business continuity and disaster recovery hands-on lab step-by-step

Abstract and learning objectives

In this workshop, the student will gain experience designing solutions using Azure business continuity and disaster recovery (BCDR) technologies. Three different types of environments will be examined. The first will consist of on-premises VMs running applications that will be migrated to Azure IaaS. Next, Azure IaaS applications that need to be failed over from either on-premises to Azure or between two Azure Regions. Finally, the use of automated failover technologies built into Azure PaaS services App Service and SQL Database will be used for PaaS applications.

Learning Objectives:

- Understanding the different use cases for implementing Azure Site Recovery (ASR), for on-premises VM migration to Azure IaaS
- Determine how to leverage various Azure technologies together to build a complex and robust IaaS BCDR plan this consists of using Azure Site Recovery, Azure Automation, Traffic Manager and SQL Server Always On Availability Groups (VMs), to failover and fallback an Azure IaaS IIS application and database from one Azure Region to another
- Design for high-availability and using BCDR techniques with Azure PaaS including Traffic Manager, SQL Database Failover Groups with Azure App Services

Overview

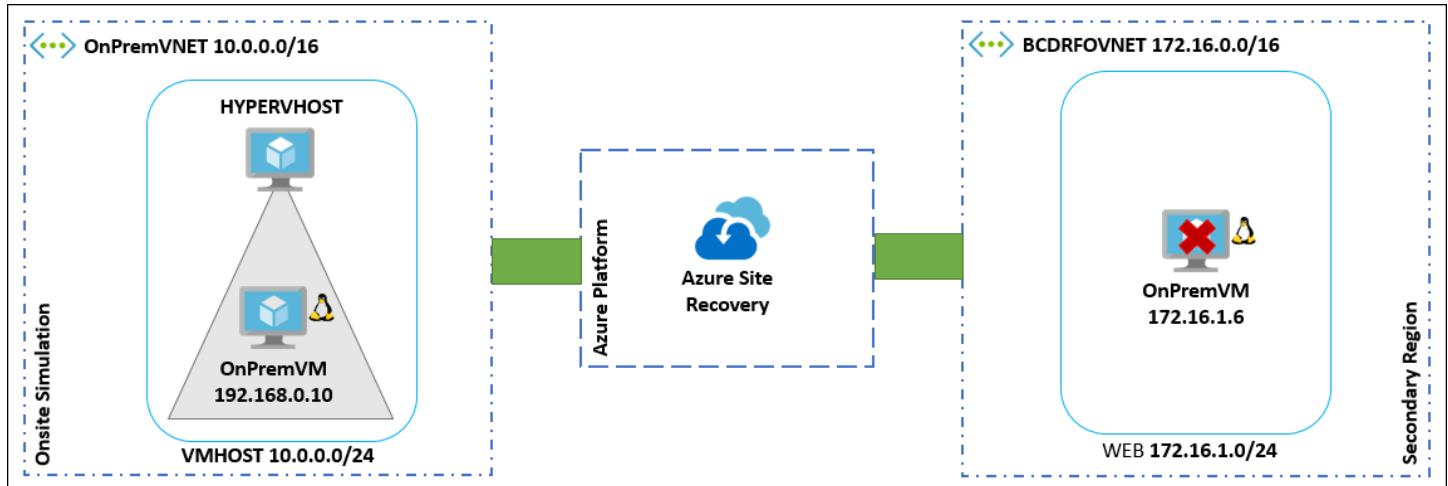
In this hands-on lab (HOL), attendees will implement three different environments and use Azure BCDR technologies to achieve three distinct goals for each environment type. These will include a migration to Azure, Azure region to region failover using Azure Site Recovery (ASR) and a PaaS implementation using BCDR technologies to ensure high availability of an application.

Solution architecture

Below are diagrams of the solution architecture you will build in this lab. Please study this carefully, so you understand the whole of the solution as you are working on the various components.

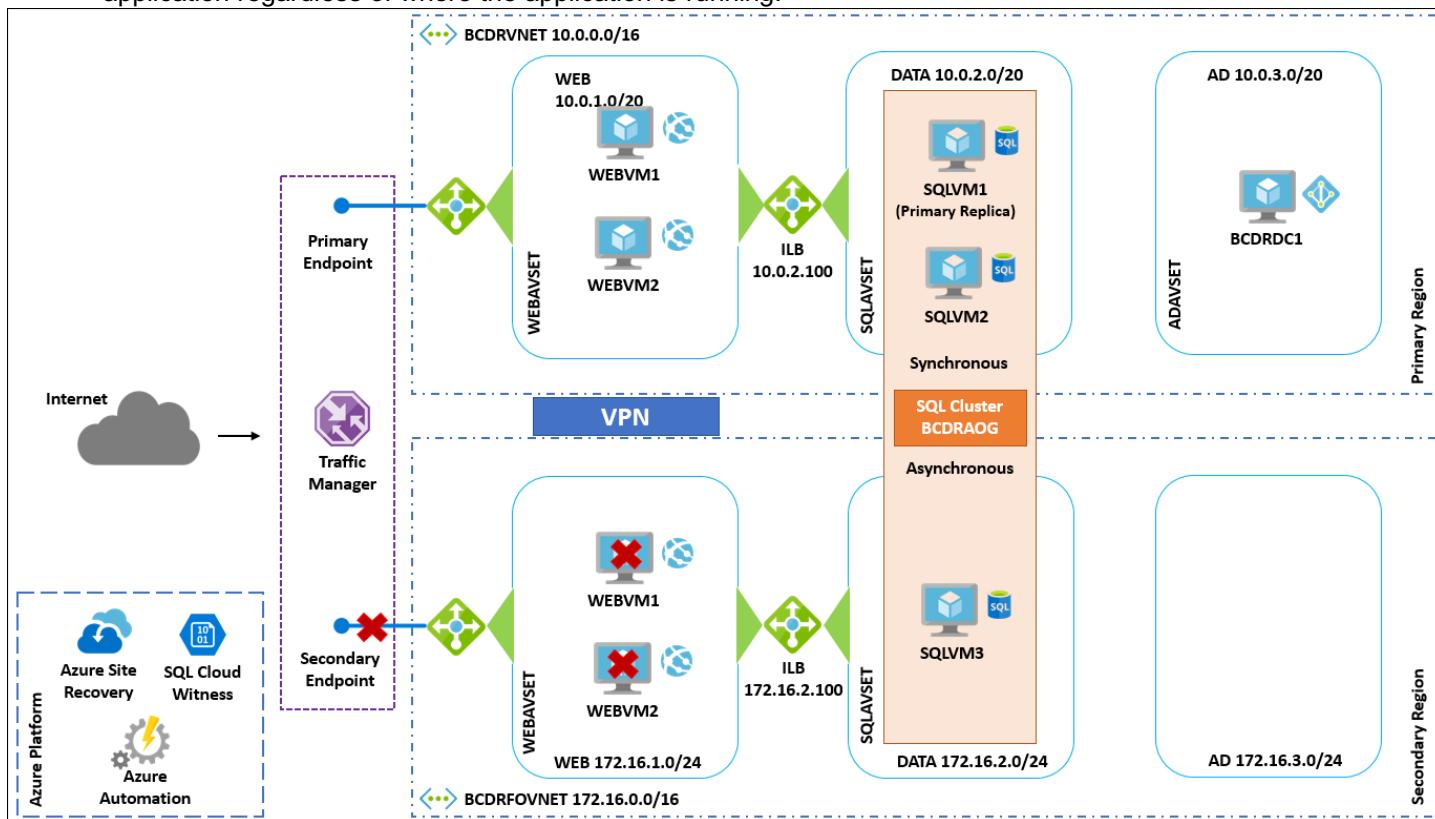
Environment: On-premises (migrate to Azure)

- **Background:** This environment will deploy a Hyper-V Host that will host a Linux VM to simulate a Linux, Apache, PHP and MySQL (LAMP), based web application deployed into an on-premises datacenter on a single VM
- **Goal using Azure BCDR:** Your goal for this environment will be to migrate this application to Azure IaaS with a one-direction failover



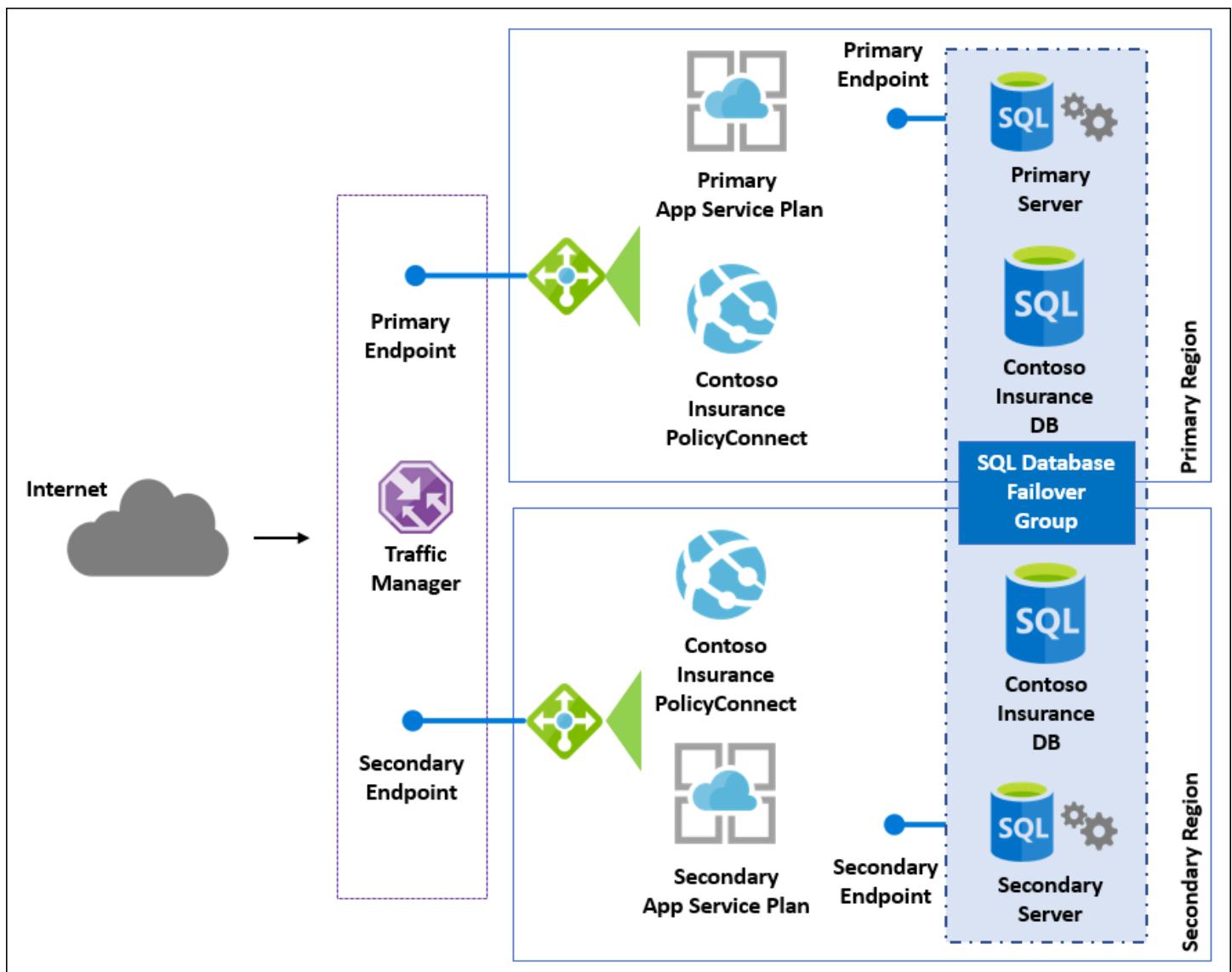
Environment: Azure IaaS (failover region to region)

- Background:** This environment will consist of two Virtual Networks deployed to your Primary and Secondary site with an AD Domain, IIS Web Servers and Microsoft SQL Servers that you will configure into a SQL Always On Availability Group
- Goal using Azure BCDR:** Your goal for this environment is to have the ability to have a one-click failover process using Azure Site Recovery in either direction. The users will have one URL that they will use to connect to your application regardless of where the application is running.



Environment: Azure PaaS (high-availability with seamless failover)

- **Background:** This environment will deploy an Azure Web App and Azure SQL Server in both the Primary and Secondary locations. You will configure SQL Database Failover groups to allow for seamless failover of the database.
- **Goal using Azure BCDR:** Your goal for this environment is never to have the users experience any downtime if issues arise with your Web App or the SQL Database. The users will have one URL that they will use to connect to your application regardless of where the application or database is running.



Requirements

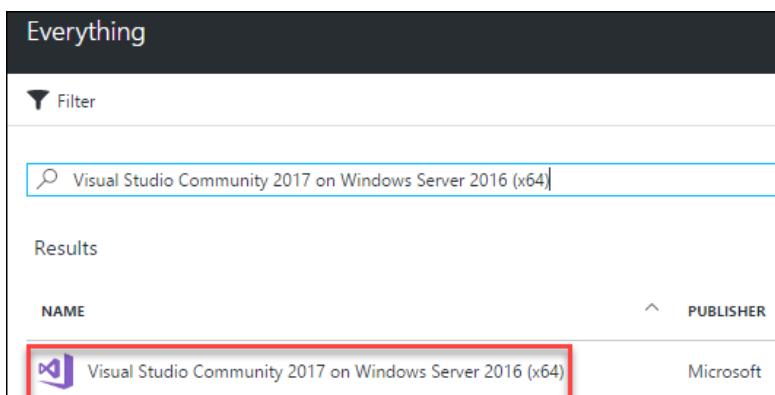
1. Azure Subscription with full access to the environment

Before the hands-on lab

Duration: 20 minutes

Task 1: Create a virtual machine to execute the lab

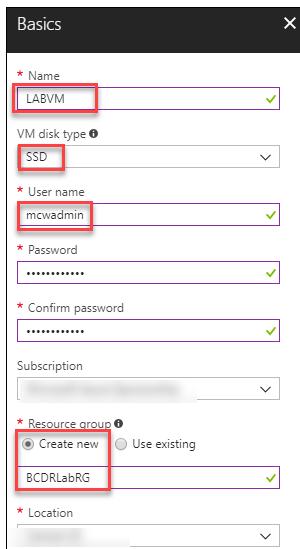
1. Launch a browser and navigate to the Azure Global portal at <https://portal.azure.com>. Once prompted, login with your Microsoft Azure credentials. If prompted, choose whether your account is an organization account or just a Microsoft Account.
2. Select **+NEW**, and in the search box enter in **Visual Studio Community 2017 on Windows Server 2016 (x64)** and press Enter. Select the Visual Studio Community 2017 image running on Windows Server 2016 and with the latest update.
3. In the returned search results select the image name



The screenshot shows the Azure portal search interface. At the top, there's a dark header bar with the word 'Everything' and a 'Filter' button. Below it is a search bar containing the query 'Visual Studio Community 2017 on Windows Server 2016 (x64)'. Underneath the search bar is a 'Results' section with two columns: 'NAME' and 'PUBLISHER'. A single result is listed: 'Visual Studio Community 2017 on Windows Server 2016 (x64)' by Microsoft. This result is highlighted with a red rectangular box.

4. Select **Create**
5. Set the following configuration on the Basics tab and select **OK**
 - a. **Name:** LABVM
 - b. **VM disk type:** SSD
 - c. **User name:** mcwadmin
 - d. **Password:** demo@pass123
 - e. **Subscription:** If you have multiple subscriptions choose the subscription to execute your labs in.
 - f. **Resource Group:** BCDRLabRG

- g. **Location:** Choose the closest Azure region to you



6. Choose the **D2S_V3 Standard** instance size on the Size blade.

Note: If the Azure Subscription you are using has limits on the number of cores you may wish to choose DS1_V2.

7. On the **Settings** blade accept the defaults and select **OK**



8. Select **Summary** blade select **Create**

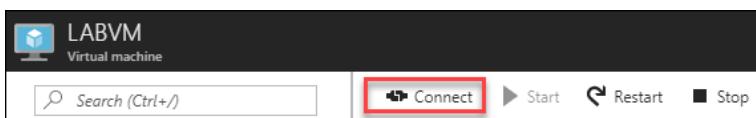


9. Accept the remaining default values on the Settings blade and select **OK**. On the Summary page, select **Create**. The deployment should begin provisioning. It may take 10+ minutes for the virtual machine to complete provisioning.



Note: Please wait for the LABVM to be provisioned prior to moving to the next step.

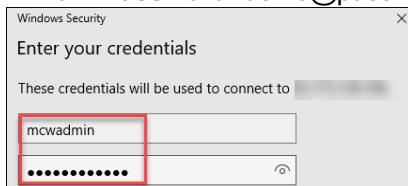
10. Move back to the Portal page on your local machine and wait for **LABVM** to show the Status of **Running**. Select **Connect** to establish a new Remote Desktop Session



11. Depending on your remote desktop protocol client and browser configuration you will either be prompted to open an RDP file, or you will need to download it and then open it separately to connect

12. Log in with the credentials specified during creation:

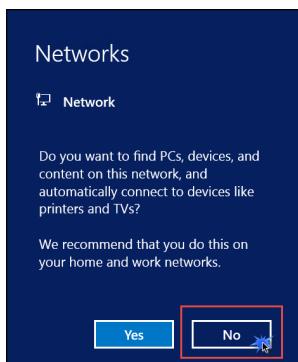
- a. **User:** mcwadmin
- b. **Password:** demo@pass123



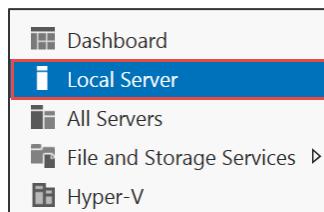
13. You will be presented with a Remote Desktop Connection warning because of a certificate trust issue. Select **Yes** to continue with the connection.



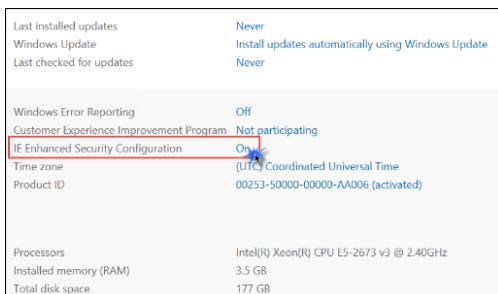
14. When logging on for the first time you will see a prompt on the right asking about network discovery. Select **No**.



15. Notice that Server Manager opens by default. On the left, select **Local Server**.



16. On the right side of the pane, select **On** for **IE Enhanced Security Configuration**



17. Change Administrators to Off and select OK



Task 2: Download hands-on lab step by step support files to LABVM

- After the reboot has completed, download the zipped Hands-on Lab Step by Step student files by clicking on this link:

<https://www.dropbox.com/s/sx91sjcn63t980j/StudentFiles.zip?dl=1>

- Extract the downloaded files into the directory C:\HOL

Task 3: Install SQL Server Express on LABVM

- From within LABVM open Internet Explorer and browse to the following URL:

<https://www.microsoft.com/en-US/sql-server/sql-server-downloads>

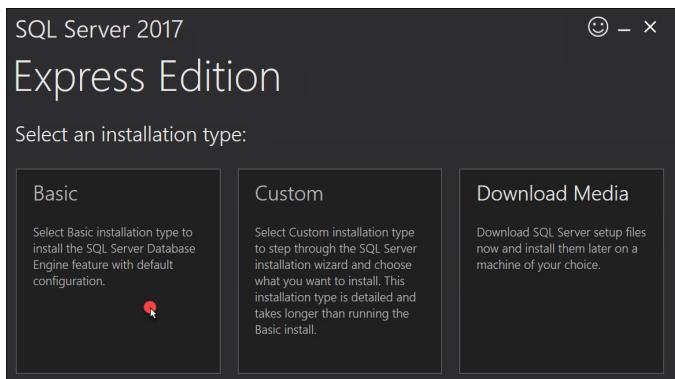
- Click **Download now** under the Express edition



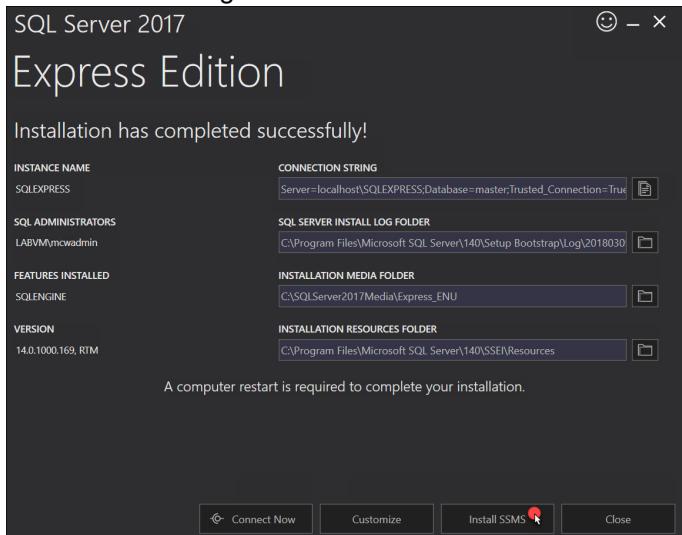
- Click **Run**



- When the installer starts, click **Basic**



5. Accept the other defaults in the install wizard until SQL starts to install
6. Once the install completes, click the **Install SSMS** button. This will webpage where you can download and install SQL Server Management Studio.



7. Click the **Download SQL Server Management Studio 17.X** link. When prompted click **Run**.

Download SQL Server Management Studio (SSMS)

02/21/2018 • 5 minutes to read • Contributors all

THIS TOPIC APPLIES TO: SQL Server Azure SQL Database Azure SQL Data Warehouse Data Warehouse

SSMS is an integrated environment for managing any SQL infrastructure, from SQL Server to SQL Data. SSMS provides tools to configure, monitor, and administer instances of SQL. Use SSMS to deploy, mon and upgrade the data-tier components used by your applications, as well as build queries and scripts.

Use SQL Server Management Studio (SSMS) to query, design, and manage your databases and data warehouses, wherever they are - on your local computer, or in the cloud.

SSMS is free!

SSMS 17.x is the latest generation of *SQL Server Management Studio* and provides support for SQL Server 2017.

[Download SQL Server Management Studio 17.5](#)

8. Click **Install**



9. Click **Close**

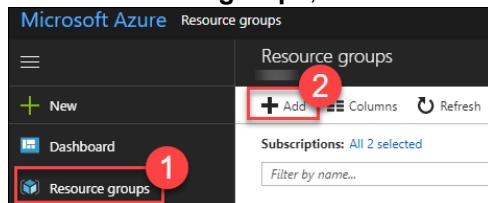
Task 4: Create the resource groups

In this task, you will select a **Primary** and **Secondary** Azure Region that will be used for the remainder of the HOL. The **Primary** region should be able to support V3 virtual machine sizes, and then you should select the **Secondary** region based on the region pair assigned by Microsoft. Use the Products available by region webpage to determine your **Primary** site: <https://azure.microsoft.com/en-us/regions/services/>. Once you have selected the Primary site, then review the BCDR page to find your Primary Site's Region Pair: <https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions>.

Note: The examples in this HOL Guide use these regions: **Primary**: East US 2 and **Secondary**: Central US.

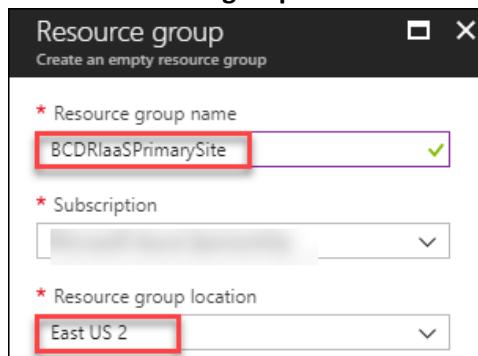
1. From the **LABVM**, open Internet Explorer and connect to the Azure portal at: <https://portal.azure.com>

2. Select **Resource groups**, the select **+Add**



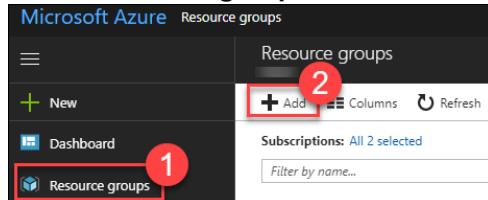
3. Complete the **Resource group** blade using the following inputs and select **Create**

- Resource group name:** BCDRlaaSPPrimarySite
- Subscription:** Select your Subscription
- Resource group location:** Select a Region for the Primary location.



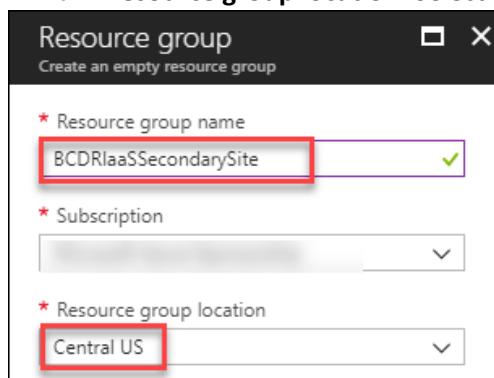
Note: It's very important for you to use these exact names. Changing the names of the Resource groups will impact the HOL setup and could cause you to not be able to complete the lab.

4. Select **Resource groups**, the select **+Add**



5. Complete the **Resource group** blade using the following inputs and select **Create**

- Resource group name:** BCDRlaaSSecondarySite
- Subscription:** Select your Subscription
- Resource group location:** Select a Region for the Secondary location



6. Continue to add resource groups to support the HOL

Resource Group Name	Location
BCDAzureAutomation	Any available site other than your Primary or Secondary
BCDAzureSiteRecovery	Secondary
BCDROnPremPrimarySite	Primary
BCDRPaaSPPrimarySite	Primary
BCDRPaaSSecondarySite	Secondary

7. Once all the resource groups have been created, you should review all the resource groups for this HOL. **It is critical to ensure that the spelling is correct and that they are in the correct Azure Regions (Primary or Secondary).**

Note: If for some reason there is an error, you should delete the resource group with the error and recreate it.

Resource Group Name	Location
BCDAzureAutomation	Any available site other than your Primary or Secondary
BCDAzureSiteRecovery	Secondary
BCDRIaaSPPrimarySite	Primary
BCDRIaaSSecondarySite	Secondary
BCDROnPremPrimarySite	Primary
BCDRPaaSPPrimarySite	Primary
BCDRPaaSSecondarySite	Secondary

8. Here is the Azure Portal with each of the resource groups created in the correct Azure Region

NAME	LOCATION
BCDAzureAutomation	East US 2
BCDAzureSiteRecovery	Central US
BCDRIaaSPPrimarySite	East US 2
BCDRIaaSSecondarySite	Central US
BCDRLabRG	Central US
BCDROnPremPrimarySite	East US 2
BCDRPaaSPPrimarySite	East US 2
BCDRPaaSSecondarySite	Central US

You should follow all steps provided *before* attending the Hands-on lab.

Exercise 1: Deploy Azure environments

Duration: 15 minutes (Deployments can take as long as 75 minutes)

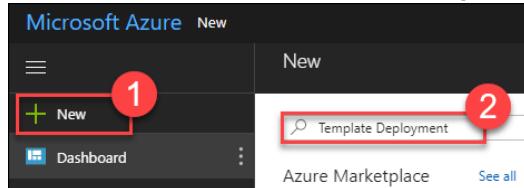
In this exercise, you will use Azure ARM Templates to deploy the following environments that will be used in this HOL:

- **Azure IaaS:** This environment will consist of two Virtual Networks deployed to your Primary and Secondary site with an AD Domain, IIS Web Servers and Microsoft SQL Servers that you will configure into a SQL Always On Availability Group
- **On-premises:** This environment will deploy a Hyper-V Host that will host a Linux VM to simulate a web application deployed into on-premises datacenter on a single VM. Your goal for this environment will be to migrate this application to Azure IaaS with a one-direction failover
- **Azure PaaS:** This environment will deploy an Azure Web App and Azure SQL Server in both the Primary and Secondary locations

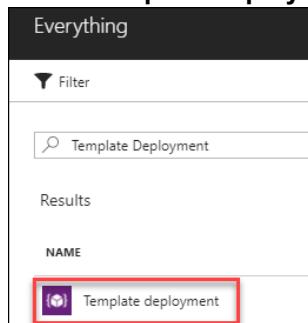
Task 1: Deploy Azure IaaS

1. From the **LABVM**, open Internet Explorer and connect to the Azure portal at: <https://portal.azure.com>

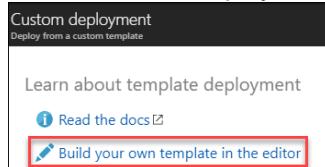
2. Select **+New** and then search for **Template Deployment**



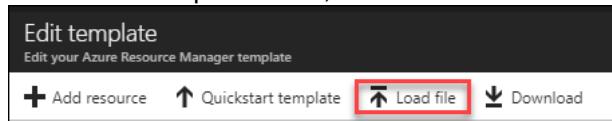
3. Select **Template deployment** and then **Create**



4. On the Custom deployment blade, select **Build your own template in the editor**

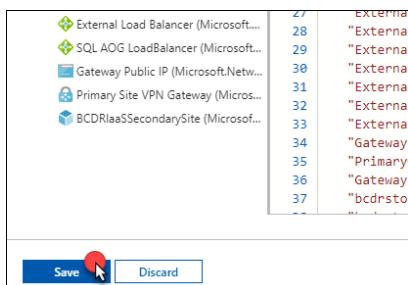


5. On the Edit template blade, select **Load file**

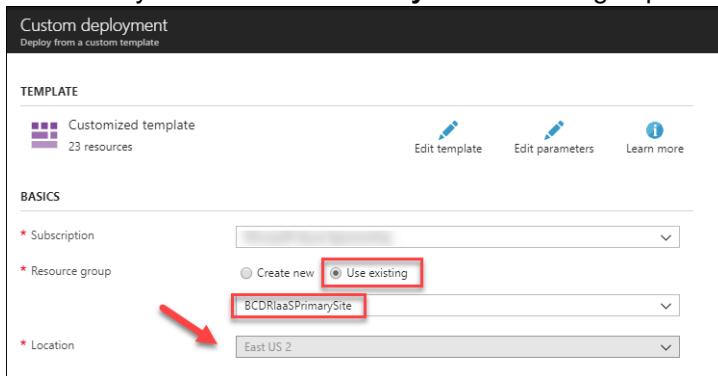


6. From the **C:\HOL\Deployments** directory locate the **BCDRIaaSPrimarySite.json** file and select **Open**

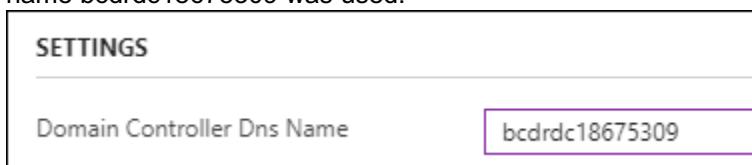
7. This will load the template into the Azure portal. Select **Save**.



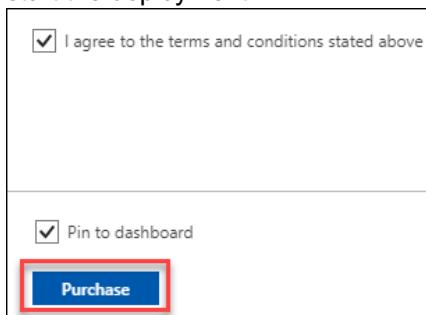
- On the Custom deployment blade, next to **Resource group** select **Use existing** and then select your **BCDR IaaS Primary Site** resource group. Notice how the template picked the deployment region based on the location of your **BCDR IaaS Primary Site** resource group. Make sure that this is your **Primary** region.



- Next, update the **Domain Controller DNS Name** in the **Settings** area. This will be the DNS name for the Active Directory Domain controller that will be your jump box into the IaaS environment. The name will need to be lowercase and 3-24 characters consisting of letters & numbers and be unique to all of Azure. In the example the name bcdrdc18675309 was used.



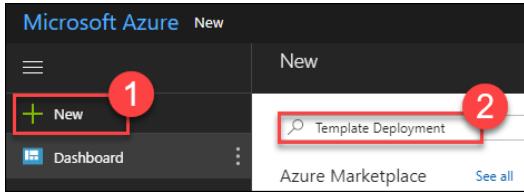
- Finally, select **I agree to the terms and conditions stated above** and **Pin to dashboard**. Select **Purchase** to start the deployment.



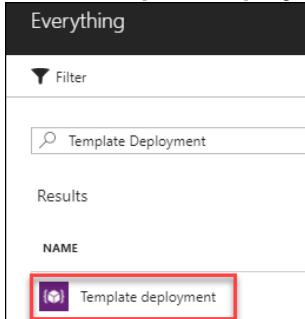
Note: This deployment will take at least 60 minutes, but you can continue to the next task.

Task 2: Deploy on-premises environment

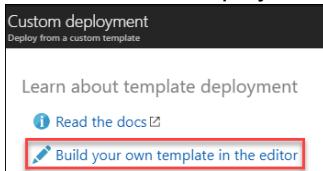
- From the **LABVM**, open Internet Explorer and connect to the Azure portal at: <https://portal.azure.com>
- Select **+New** and then search for **Template Deployment**



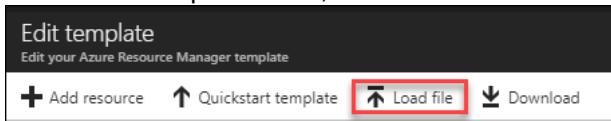
3. Select **Template deployment** and then **Create**



4. On the Custom deployment blade, select **Build your own template in the editor**



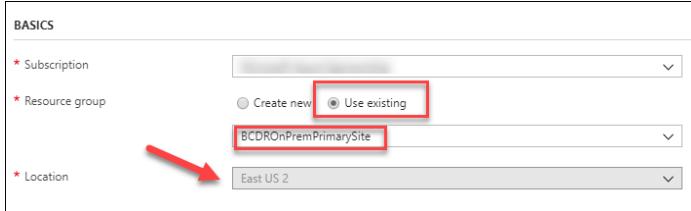
5. On the Edit template blade, select **Load file**



6. From the **C:\HOL\Deployments** directory locate the **BCDROnPremPrimarySite.json** file and select **Open**

7. This will load the template into the Azure portal. Select **Save**

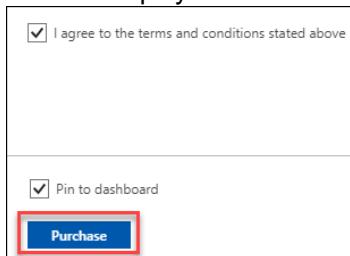
8. On the Custom deployment blade, next to **Resource group** select **Use existing** and then select your **BCDROnPremPrimarySite** resource group. Notice how the template picked the deployment region based on the location of your **BCDROnPremPrimarySite** resource group. Make sure that this is your **Primary** region.



9. Next, update the **Hyper-V Host DNS Name** in the **Settings** area. This will be the DNS name for the Hyper-V Host that will you will use for this simulated on-premises environment. The name will need to be lowercase and 3-24 characters consisting of letters & numbers and be unique to all of Azure. In the example, the name **hypervhost8675309** was used.



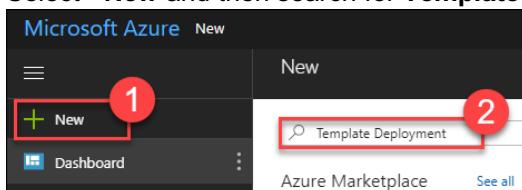
10. Finally, select **I agree to the terms and conditions stated above** and **Pin to dashboard**. Select **Purchase** to start the deployment.



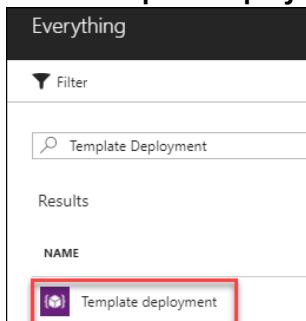
Note: This deployment will take at least 20 minutes, but you can continue to the next task.

Task 3: Deploy Azure PaaS environment

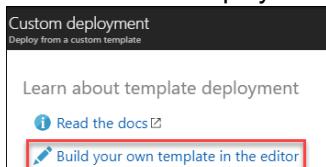
- From the **LABVM**, open Internet Explorer and connect to the Azure portal at <https://portal.azure.com>
- Select **+New** and then search for **Template Deployment**



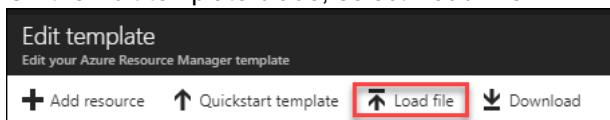
- Select **Template deployment** and then **Create**



- On the Custom deployment blade, select **Build your own template in the editor**

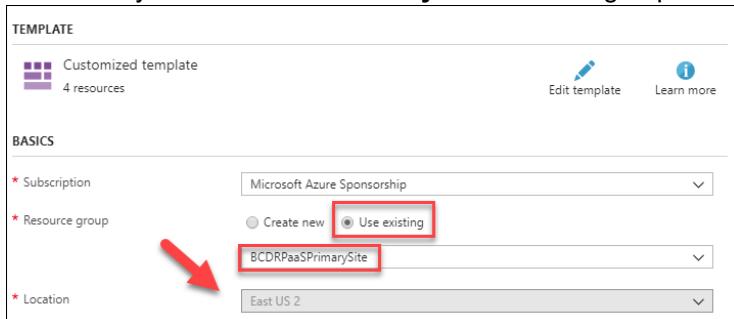


- On the Edit template blade, select **Load file**

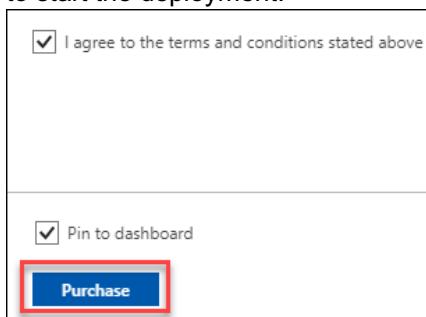


- From the **C:\HOL\Deployments** directory locate the **BCDRPaaSPrimarySite.json** file and select **Open**
- This will load the template into the Azure portal. Select **Save**.

8. On the Custom deployment blade, next to **Resource group** select **Use existing** and then select your **BCDRPaaSPrimarySite** resource group. Notice how the template picked the deployment region based on the location of your **BCDRPaaSPrimarySite** resource group. Make sure that this is your **Primary** region.



9. Finally, select the **I agree to the terms and conditions stated above** and **Pin to dashboard**. Select **Purchase** to start the deployment.

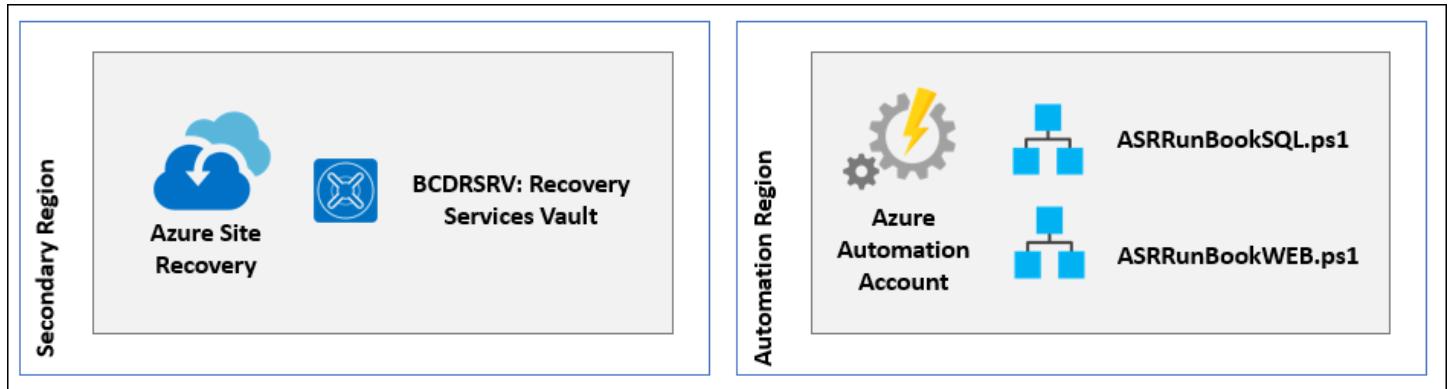


Note: This deployment will take at least 10 minutes, but you can continue to the next task.

Exercise 2: Configure BCDR services

Duration: 30 minutes

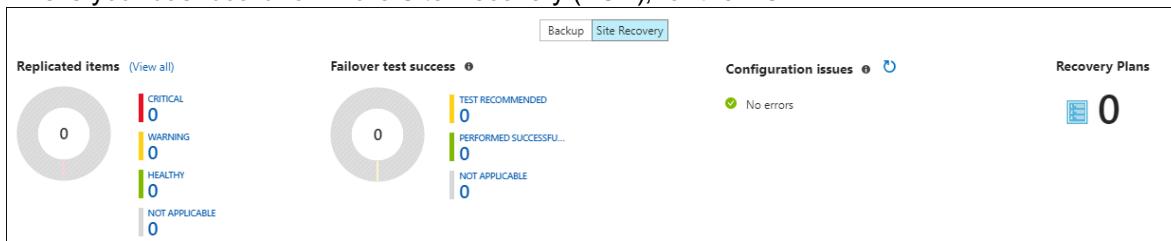
In this exercise, you will create and configure the services that will make it possible to failover both the on-premises and Azure IaaS environments. These will include a Recovery Services Vault used for Azure Site Recovery and an Azure Automation account.



Task 1: Create Azure recovery services vault

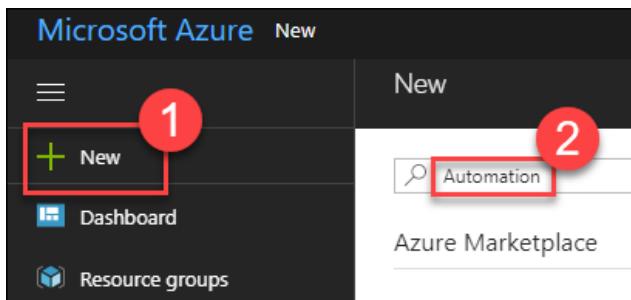
1. Using the **LABVM** connect to the Azure portal using your web browser at <https://portal.azure.com>
2. Select **+New, Monitoring + Management** and then **Backup and Site Recovery (OMS)**
3. Complete the **Recovery Services vault** blade using the following inputs, then select **Create**
 - a. **Name:** BCDRRSV
 - b. **Resource Group:** Use existing / BCDRAzureSiteRecovery
 - c. **Location:** Secondary Site (should be automatically selected based on your resource group)
4. Once the **BCDRRSV** Recovery Service Vault has been created, open it in the Azure portal. Toggle the switch that selects Backup / Site Recovery

5. This is your dashboard for Azure Site Recovery (ASR), for the HOL

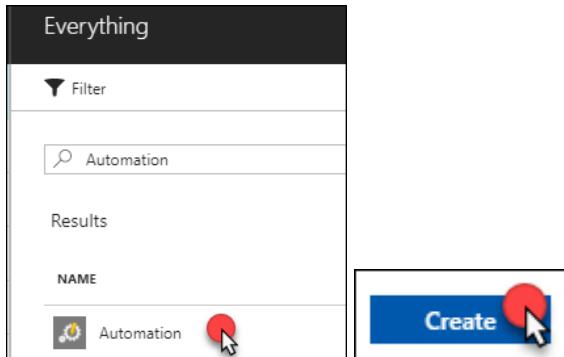


Task 2: Deploy Azure automation

1. Open the Azure portal at: <https://portal.azure.com>
2. Select **+New** and then enter **Automation** in the search box



3. Select **Automation** and then **Create**



4. Complete the **Add Automation Account** blade using the following inputs and then select **Create**:

- Name:** Enter a Globally unique name starting with BCDR
- Resource group:** Use existing / BCDRAzureAutomation
- Location:** Select a site in your Area, but NOT your Primary Site
- Create Azure Run As account:** Yes

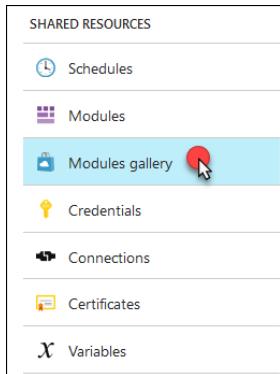
A screenshot of the 'Add Automation Account' blade. It contains several input fields:

- * Name: bcdrautomation
- * Subscription: (dropdown menu)
- * Resource group:
 - Create new
 - Use existingBCDRAzureAutomation
- * Location: South Central US
- * Create Azure Run As account:
 - Yes
 - No

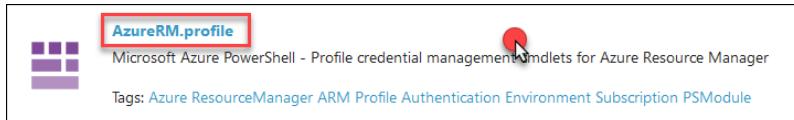
A red callout bubble points to the 'Location' field with the text 'NOT Primary Site'.

Note: Azure Automation accounts are only allowed to be created in certain Azure regions, but they can act on any region in Azure (except Government, China or Germany). It is not a requirement to have your Azure Automation account in the same region as the **BCDRAzureAutomation** resource group but **CANNOT** be in your primary site.

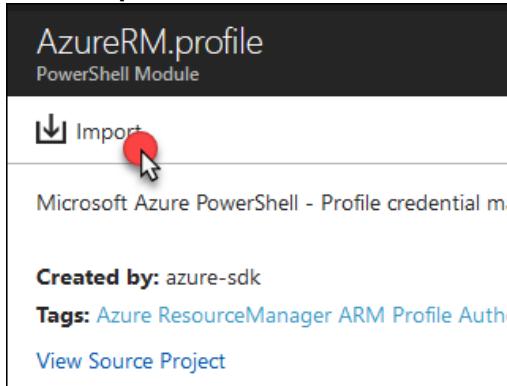
- Once the Azure automation account has been created open the account and select **Modules gallery** under **Shared Resources**



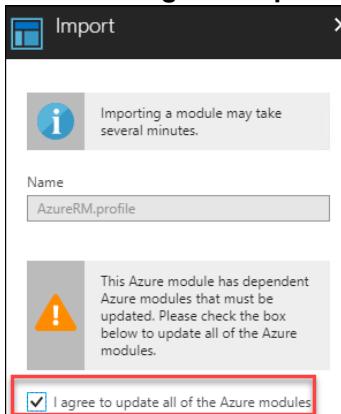
- When the Modules load, scroll down and locate and select **AzureRM.Profile**



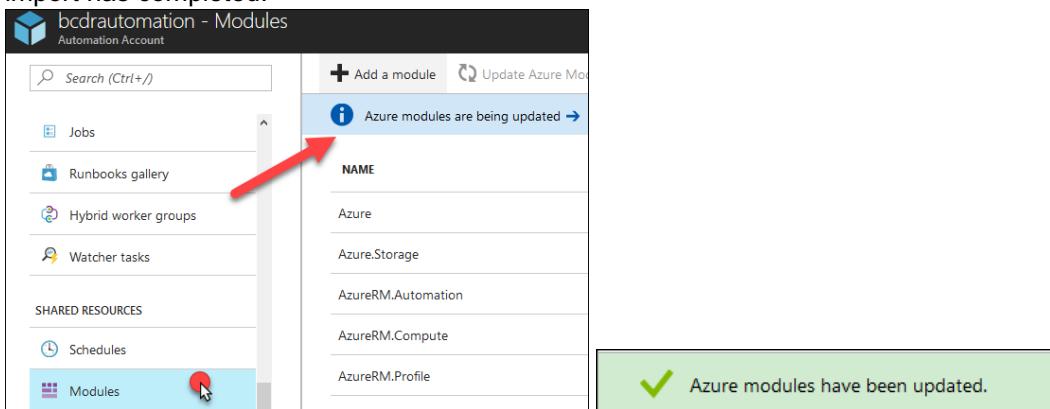
- Select **Import**



8. Select the **I agree to update all of the Azure modules** and then select **OK**



9. It will take a few minutes to update the modules. Select **Modules** under Shared Resources, and you can wait the import has completed.

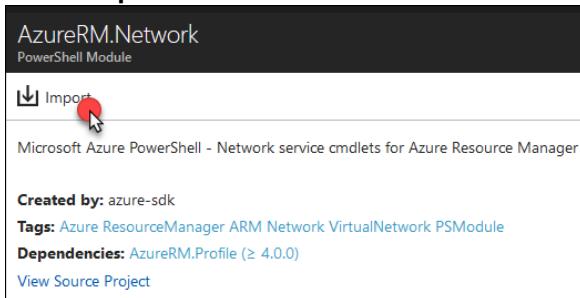


10. Select back to **Modules Gallery**

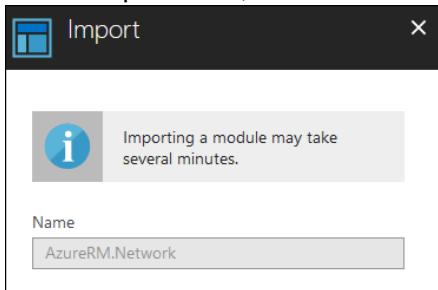
11. When the Modules load, scroll down and locate and select **AzureRM.Network**



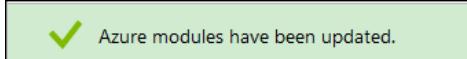
12. Select **Import**



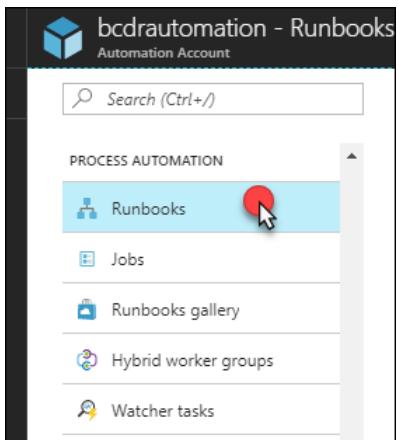
13. On the Import blade, select **OK**



14. The portal will begin the import process, but should only take about a minute



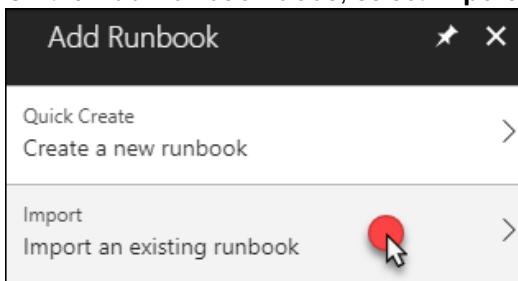
15. Next select **Runbooks**



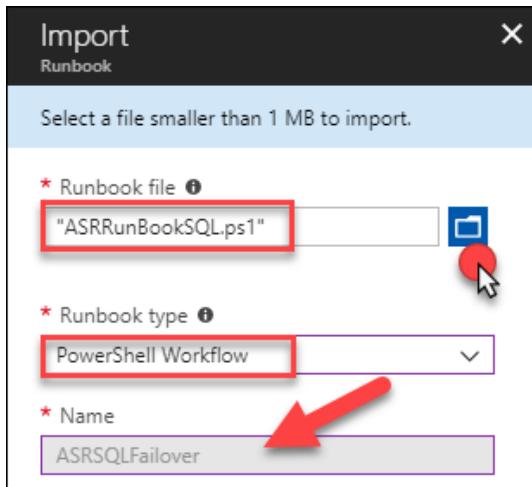
16. Select **+Add a runbook**



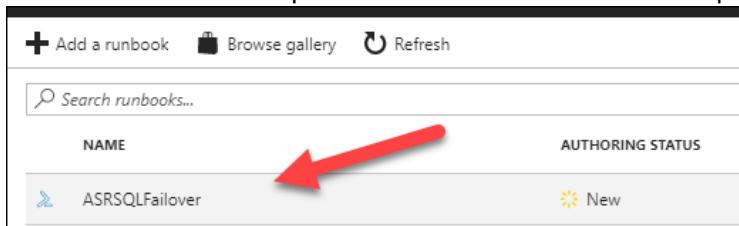
17. On the **Add Runbook** blade, select **Import an existing runbook**



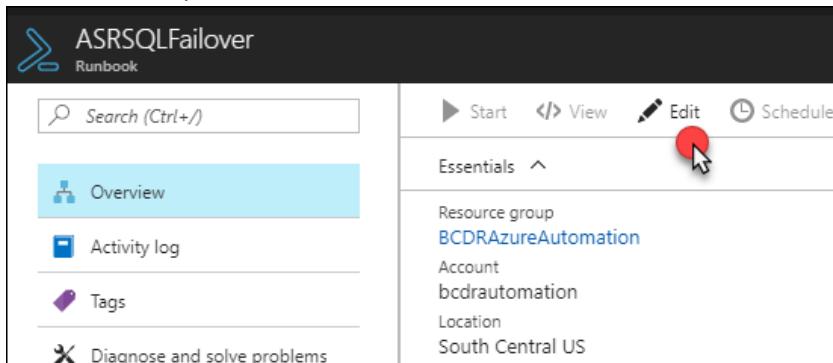
18. Select the **Folder** icon on the Import blade and select the file **ASRRunbookSQL.ps1** from the C:\HOL\Deployments directory on the **LABVM**. The Runbook type should default to **PowerShell Workflow**. Notice that the Name can't be changed. This is the name of the Workflow inside of the Runbook script. Select **Create**.



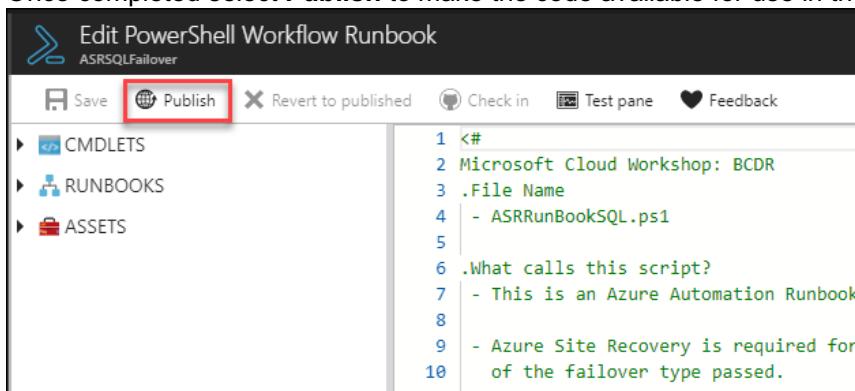
19. Once the Runbook is imported select **ASRSQFailover** to open the runbook



20. On the **ASRSQFailover** Runbook blade select **Edit**



21. The PowerShell runbook will load. If you wish, you can review the comments to better understand the runbook. Once completed select **Publish** to make the code available for use in the portal.



```

1 <#
2 Microsoft Cloud Workshop: BCDR
3 .File Name
4 - ASRRunBookSQL.ps1
5
6 .What calls this script?
7 - This is an Azure Automation Runbook
8
9 - Azure Site Recovery is required for
10 of the failover type passed.
11

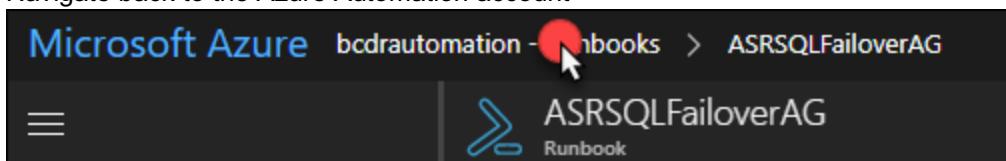
```

Note: You might notice the Test Pane link. This script can't be tested from here as there are more configurations required, and it relies of being called by Azure Site Recovery to feed its variables.

22. Select **Yes**, to configure that this Runbook will be published



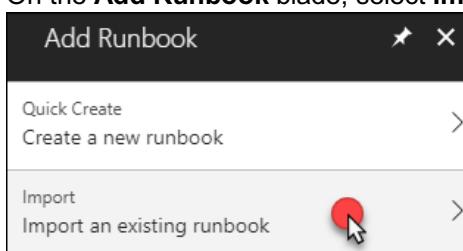
23. Navigate back to the Azure Automation account



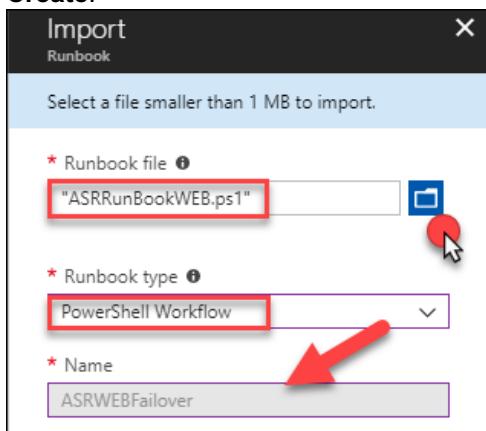
24. Select **+Add a runbook**



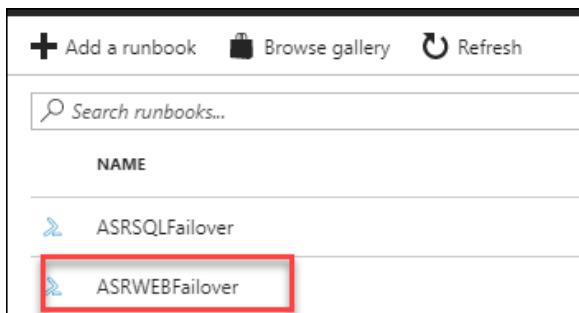
25. On the **Add Runbook** blade, select **Import an existing runbook**



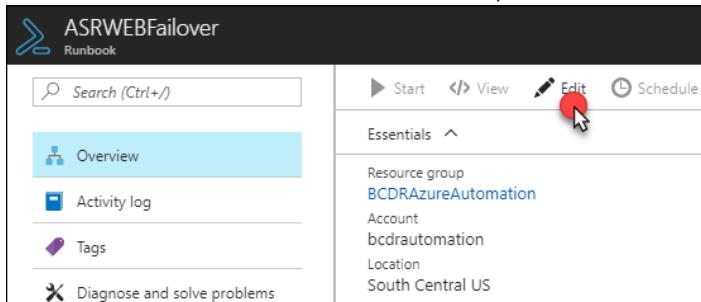
26. Select the Folder icon on the Import blade and select the file **ASRRunbookWEB.ps1** from the **C:\HOL\Deployments** directory on the **LABVM**. The Runbook type should default to **PowerShell Workflow**. Notice that the Name can't be changed. This is the name of the Workflow inside of the Runbook script. Select **Create**.



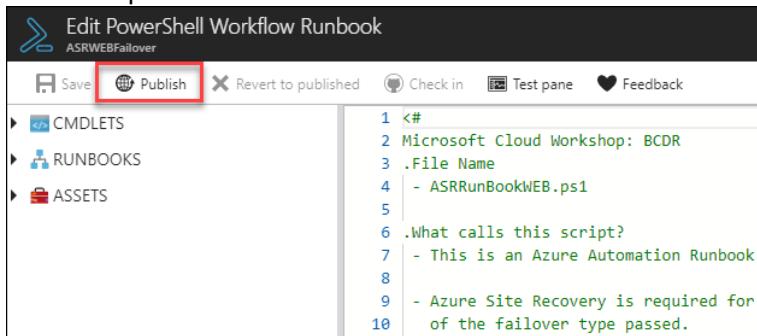
27. Once the Runbook is imported select **ASRWebFailover** to open the runbook



28. On the **ASRWebFailover** Runbook blade, select **Edit**



29. The PowerShell runbook will load. If you wish, you can review the comments to better understand the runbook. Once completed select **Publish** to make the code available for use in the portal.



```
1 <#
2 Microsoft Cloud Workshop: BCDR
3 .File Name
4 - ASRRunBookWEB.ps1
5
6 .What calls this script?
7 - This is an Azure Automation Runbook
8
9 - Azure Site Recovery is required for
10 of the failover type passed.
```

30. Select **Yes**, to configure that this Runbook will be published



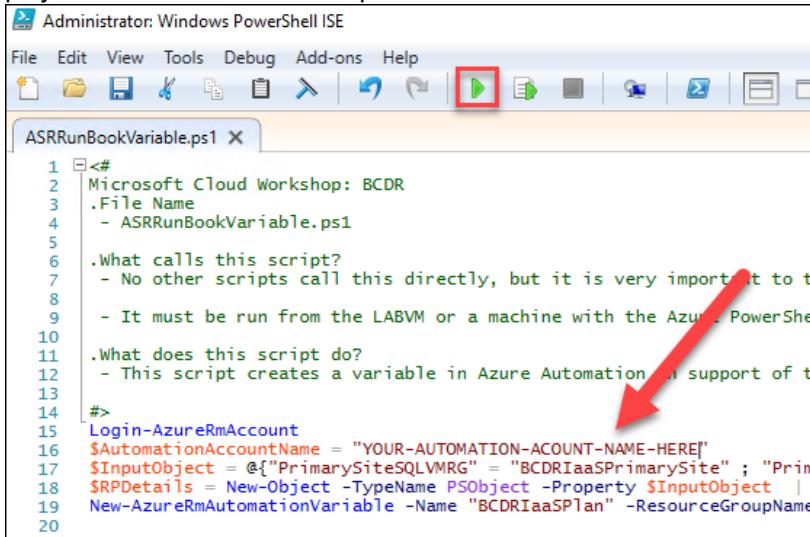
31. Navigate back to **Runbooks**, make sure that both Runbooks show as “**Published**”

NAME	AUTHORING STATUS
ASRSQFailover	✓ Published
ASRWEBFailover	✓ Published

32. From **LABVM**, select **Start** and select **PowerShell ISE** (make sure to right-click and run as Administrator)



33. Open the file **C:\HOL\Deployments\ASRRunBookVariable.ps1**. Review the script and then select the green play button to execute the script. You will need to authenticate to Azure.



```

1 <#
2 Microsoft Cloud Workshop: BCDR
3 .File Name
4 - ASRRunBookVariable.ps1
5
6 .What calls this script?
7 - No other scripts call this directly, but it is very important to t
8
9 - It must be run from the LABVM or a machine with the Azure PowerShell
10
11 .What does this script do?
12 - This script creates a variable in Azure Automation in support of t
13
14 #>
15 Login-AzureRmAccount
16 $AutomationAccountName = "YOUR-AUTOMATION-ACCOUNT-NAME-HERE"
17 $InputObject = @{
        "PrimarySiteSQLVMRG" = "BCDRIaaSPrimarySite" ;
        "Prim
18 $RPDetails = New-Object -TypeName PSObject -Property $InputObject |
19 New-AzureRmAutomationVariable -Name "BCDRIaaSPlan" -ResourceGroupName
20

```

Note: If you are using an account that has multiple subscriptions you may need to change the context of your login. You can comment the **Login-AzureRmAccount** command in the script and complete the login and the use the **Get-AzureRmSubscription** and **Select-AzureRmSubscription** cmdlets to create the proper context for this HOL. For help, you can review this article: <https://docs.microsoft.com/en-us/powershell/azure/authenticate-azureps?view=azurermps-5.1.1> & <https://docs.microsoft.com/en-us/powershell/azure/manage-subscriptions-azureps?view=azurermps-5.1.1>

34. Once the script has run, you will see the following output from PowerShell ISE. This script created a variable that will be used with the PowerShell Runbook in Azure Automation to help with the Failover and Failback of the Azure IaaS environment.

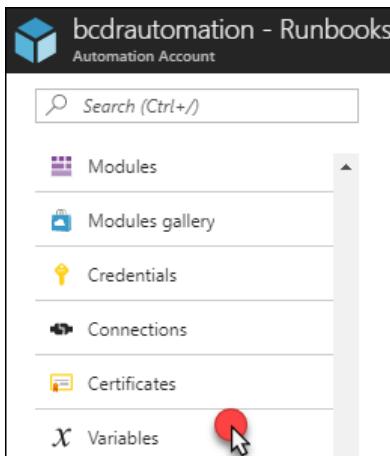


```

Value : {
    "SecondarySitePath": "SQLSERVER:\\\\Sq1\\\\SQLVM3\\\\DEFAULT\\\\AvailabilityGroups\\\\BCDRAOG",
    "PrimarySitePath": "SQLSERVER:\\\\Sq1\\\\SQLVM1\\\\DEFAULT\\\\AvailabilityGroups\\\\BCDRAOG",
    "SecondarySiteSQLVMRG": "BCDRIaaSSecondarySite",
    "PrimarySiteSQLVMName": "SQLVM1",
    "SecondarySiteSQLVMName": "SQLVM3",
    "PrimarySiteSQLVMRG": "BCDRIaaSPrimarySite"
}
Encrypted : False
ResourceGroupName : BCDAzureAutomation
AutomationAccountName : bcdrautomation
Name : BCDRIaaSPlan

```

35. Move back to the Azure portal and locate the **Azure Automation** account. Select the **Variables** link in the **Shared Resources** section.



36. Notice that the variable **BCDRIaaSPlan** has been created. This variable will be used along with ASR to orchestrate part of the failover.

The screenshot shows the 'Variables' section of an Azure Automation account. On the left, there's a sidebar with 'Search (Ctrl+ /)', 'Modules', 'Modules gallery', and 'Credentials'. The main area has a header with '+ Add a variable' and 'Refresh'. Below is a table with one row, where a red arrow points to the 'NAME' column containing 'BCDRIaaSPlan'.

NAME
BCDRIaaSPlan

Note: When you configure the ASR Recovery Plan for the IaaS deployment you will use the SQL Runbook as a Pre-Failover Action and the Web Runbook as a Post-Failover action. They will run both ways and have been written to take the “Direction,” of the failover into account when running.

Exercise 3: Configure environments for failover

Duration: 90 minutes

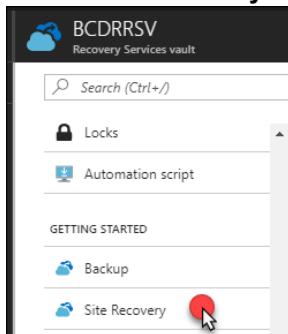
In this exercise, you will configure the three environments to use BCDR technologies found in Azure. Each environment has unique configurations that must be completed to ensure their availability in the event of a disaster.

Note: Make sure prior to starting each task that the deployment that you started in Exercise 1 has completed for each as you come to that task. This can be determined, but reviewing the deployments for each Resource group in the Azure portal. If it says Succeeded, then you can begin the task.

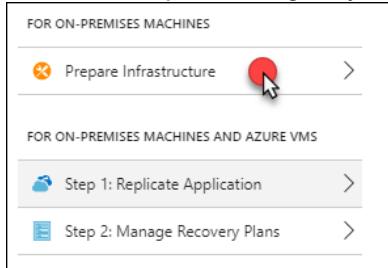
Task 1: Configure on-premises to Azure IaaS failover for migration

In this task, the **OnPremVM** will be configured to replicate to Azure and be ready to failover to the **BCDRIaaSSecondarySite**. This will consist of configuring your Hyper-V host with the ASR provider and then enabling replication of the VM to the Recovery Service Vault.

1. From the Azure portal, open the **BCDRRSV** Recovery Services Vault located in the **BCDRAzureSiteRecovery** resource group
2. Select **Site Recovery** in the **Getting Started** area of **BCDRRSV** blade



3. Next, select **Prepare Infrastructure** in the **For On-Premises Machines** section. This will start you down a path of various steps to configure your VM that is running on Hyper-V on-premises to be replicated to Azure.



4. On **Step 1 Protection Goal** select the following inputs and then select **OK**:
- Where are your machines located?**: On-premises
 - Where do you want to replicate your machines to?**: To Azure
 - Are your machines virtualized?**: Yes, with Hyper-V (your VM is running as a nested VM in Azure)
 - Are you using System Center VMM to manage your Hyper-V hosts?**: No

Protection goal
BCDRRSV

* Where are your machines located?
On-premises

* Where do you want to replicate your machines to?
To Azure

* Are your machines virtualized?
Yes, with Hyper-V

* Are you using System Center VMM to manage your Hyper-V hosts?
No

5. On **Step 2 Deployment planning** select the following inputs and then select **OK**:
- Have you completed deployment planning: **Yes, I have done it**

Note: You can read more about planning an ASR to deployment here:
<https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-hyper-v-deployment-planner>

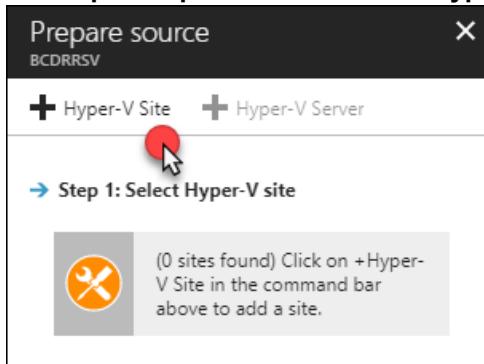
Deployment planning
BCDRRSV

Site Recovery performs optimally when sufficient network bandwidth and storage are provisioned. Allocating insufficient capacity can lead to replication issues.

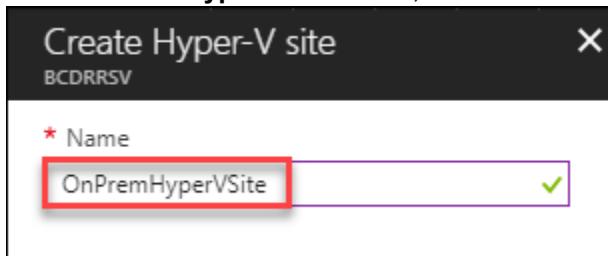
Download and run the deployment planner to accurately estimate network bandwidth, storage and other requirements to meet your replication needs. [Learn more](#)

* Have you completed deployment planning?
Yes, I have done it

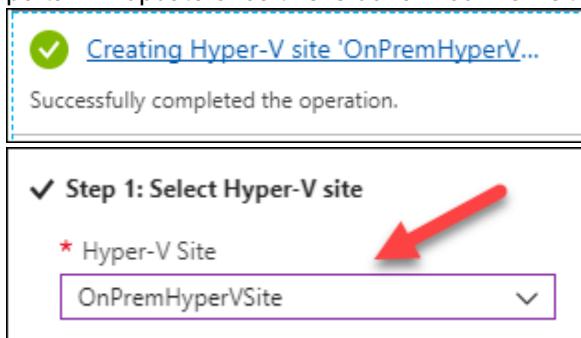
6. On Step 3 Prepare source select +Hyper-V Site



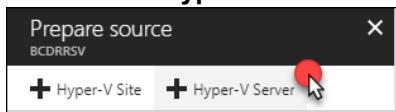
7. On the Create Hyper-V site blade, enter the name: **OnPremHyperVSite** and select **OK**



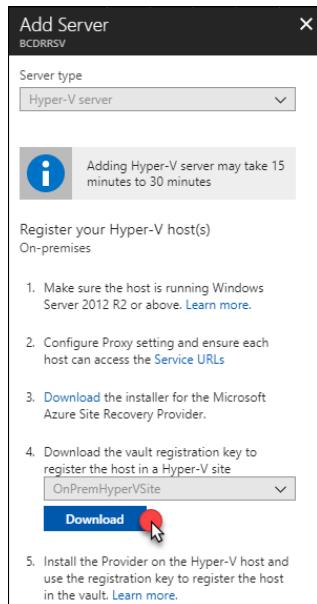
8. The portal will deploy the site providing you notifications. Wait for the creation process to complete, and the ASR portal will update once this is done. Your new site is now shown under **Step 1: Select Hyper-V site**.



9. Next select +Hyper-V Server

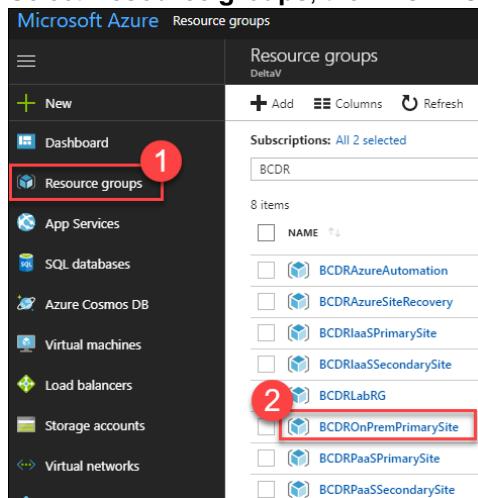


10. A new blade will appear. You will need to download the vault registration key to register the host in the Hyper-V site of ASR. Select the Download button which will save the file to your Downloads folder on the **LABVM**.



11. Open a **NEW** tab in your web browser and connect again to the Azure Portal at <https://portal.azure.com>

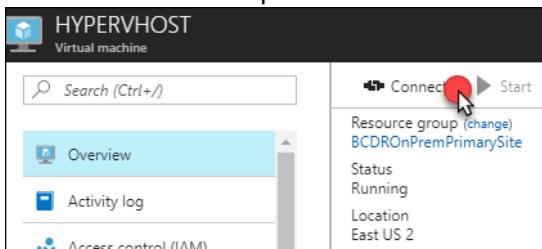
12. Select **Resource groups**, then **BCDROnPremPrimarySite**



13. Locate and select on the **HYPERVERHOST** VM object



14. Select Connect and open the RDP file that is downloaded



15. Enter the credentials for the VM:

- b. **User Name:** mcwadmin
- c. **Password:** demo@pass123

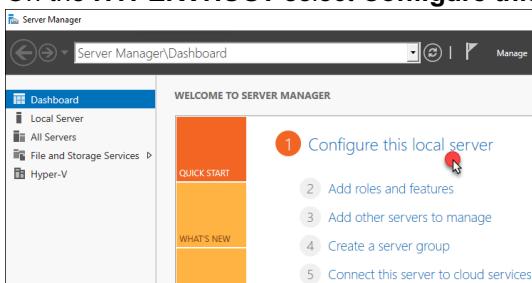
16. You will be prompted with a warning about a certificate. Select **Yes** to connection (you can always select yes to these prompts during this HOL).



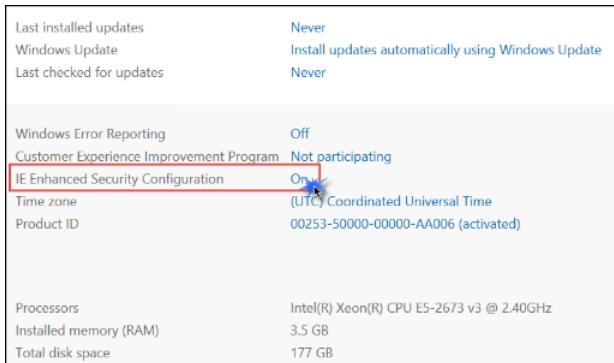
17. Select **Yes**, on the Networks prompt



18. On the **HYPERVHOST** select **Configure this local server** in the Server Manager Dashboard



19. On the right side of the pane, select **On** by **IE Enhanced Security Configuration**.



20. Change to **Off** for Administrators and select **OK**

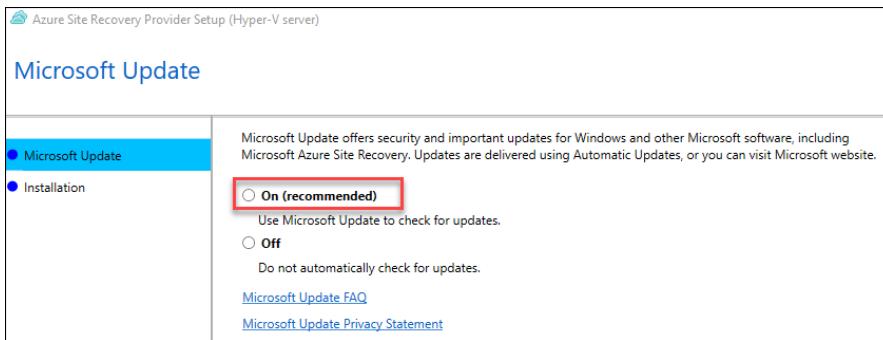
21. Open Internet Explorer on **HYPERVERHOST** and browse to the following URL. This will download the Azure Site Recovery Provider for Hyper-V

`http://aka.ms/downloadaddr_cus`

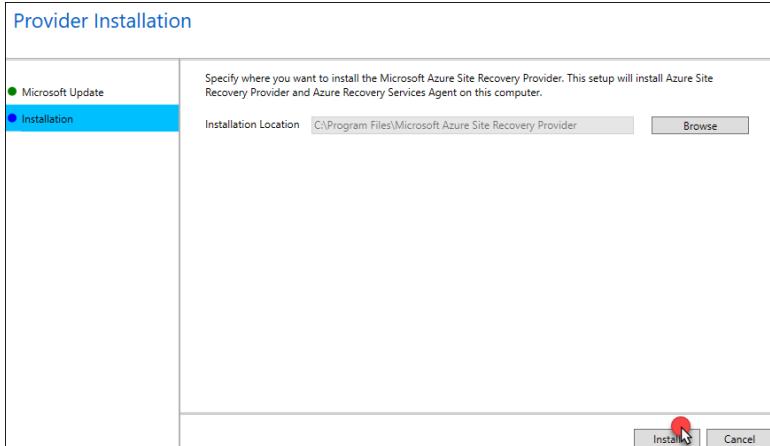
22. Select **Run**



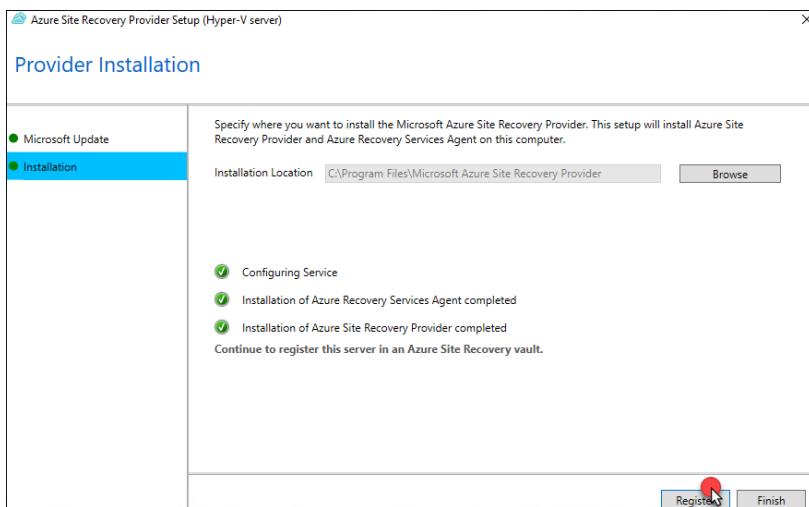
23. Select **On** and then **Next**



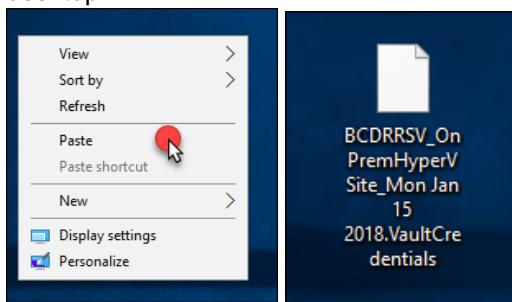
24. Select **Install** on the Provider Installation screen



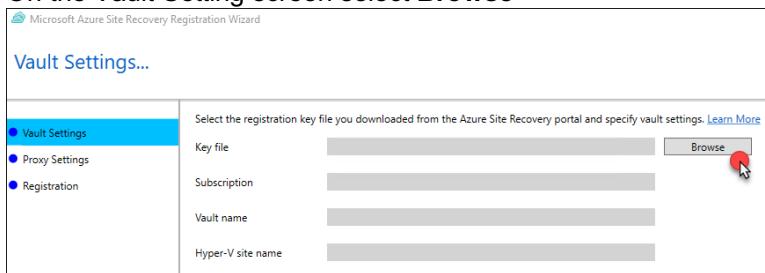
25. Once the Provider has been installed you will come to a screen that will request for you **Register** or **Finish**. Select **Register**.



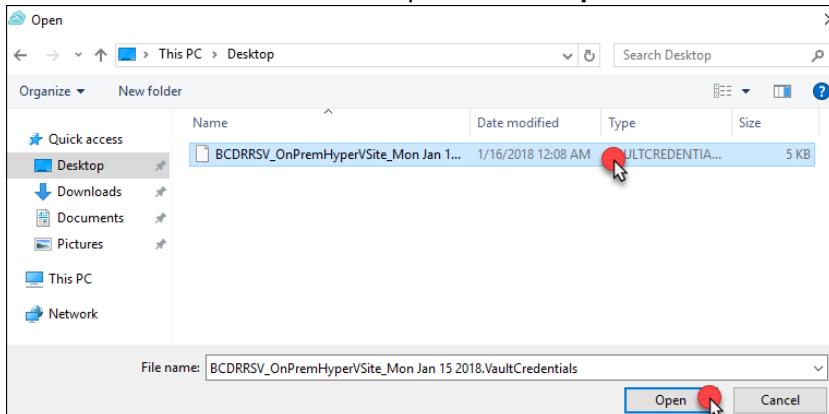
26. Minimize your Remote Desktop window and locate the vault registration key which is in the **Downloads** directory of your **LABVM**. Right-click the file and copy it. Move back to your **HYPERVERHOST** and paste the file to the desktop.



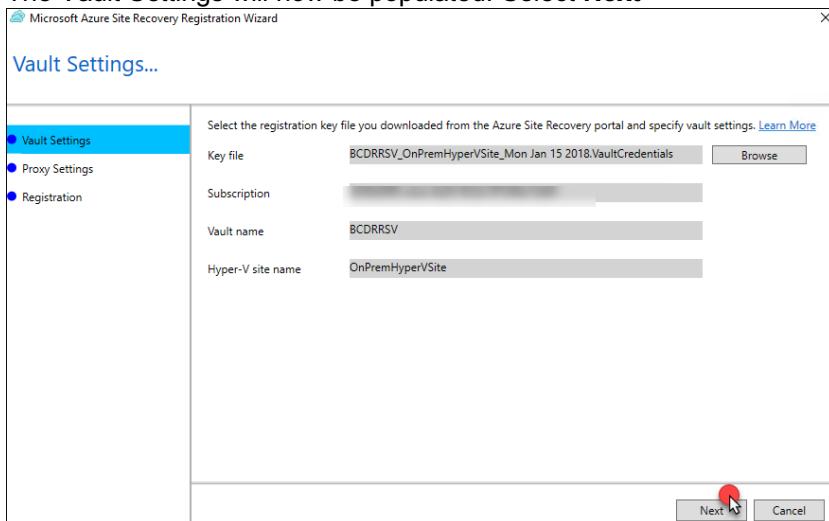
27. On the Vault Setting screen select **Browse**



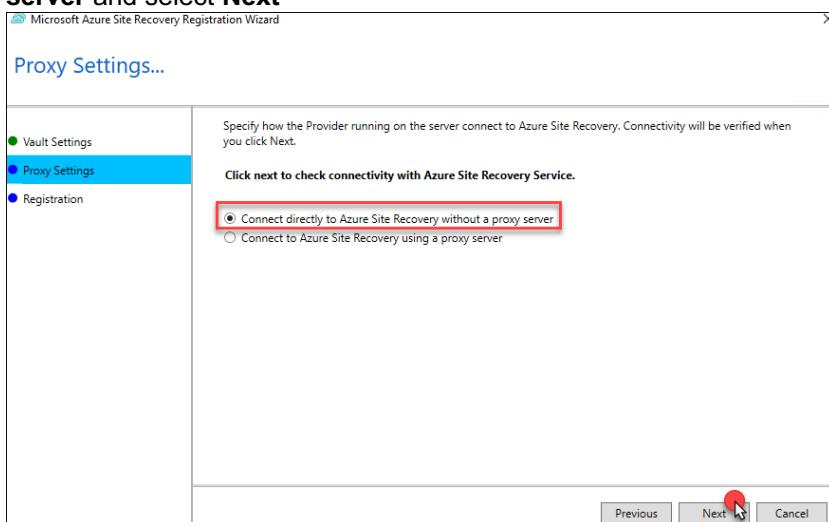
28. Locate the Vault file on the desktop and select Open



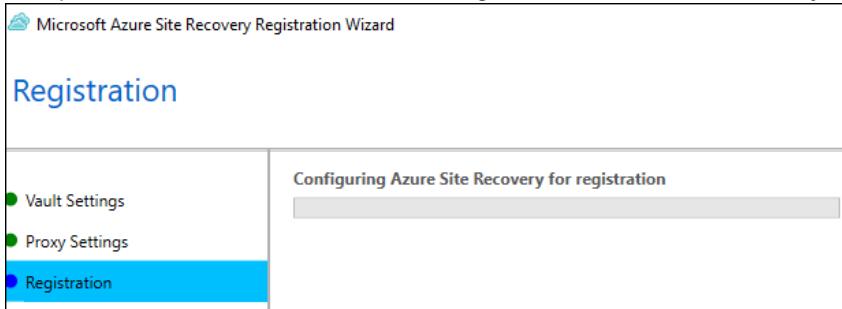
29. The Vault Settings will now be populated. Select Next



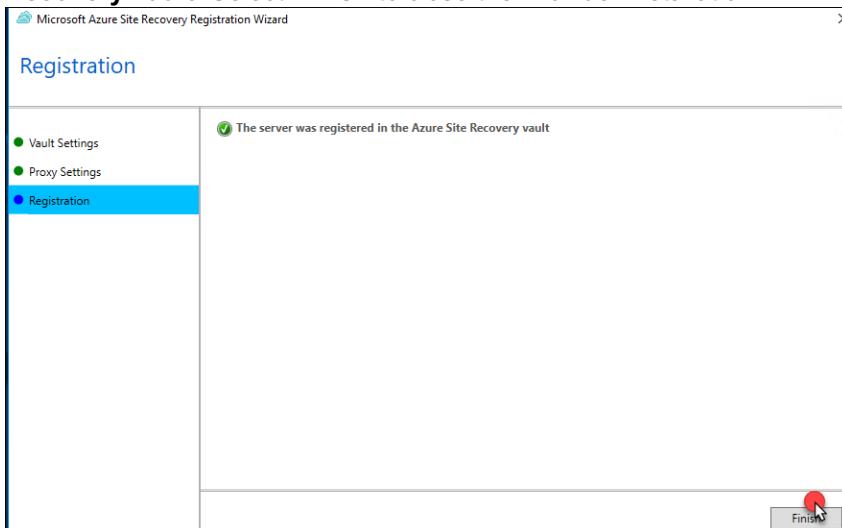
30. On the Proxy settings screen retain the settings Connect directly to Azure Site Recovery without a proxy server and select Next



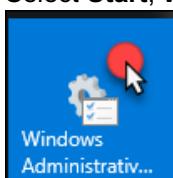
31. The provider will then connect and configure the Azure Site Recovery registration for the Hyper-V Server.



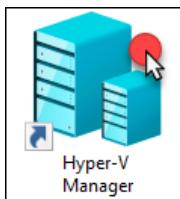
32. After a few minutes, the wizard will be complete with the message **The Server was registered in the Azure Site Recovery vault**. Select **Finish** to close the Provider installation.



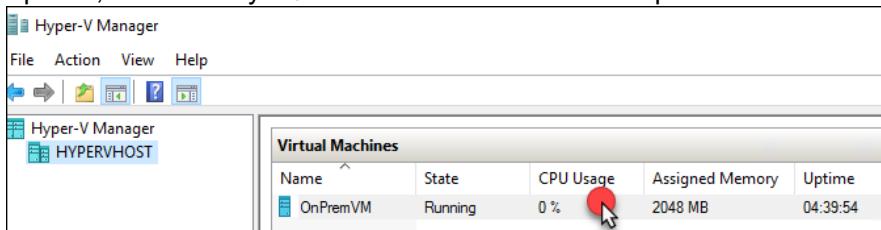
33. Select **Start**, **Windows Administrative Tools**



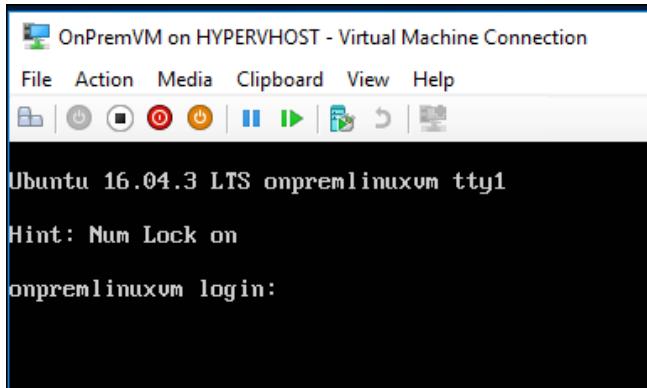
34. Locate then double-click the **Hyper-V Manager**



35. When the Hyper-V Manager opens select the Server name in the left pane and then you will see that the **OnPremVM** virtual machine is running on your **HYPERVERHOST**. This is an Ubuntu 16.04.3 LTS server running Apache, PHP and MySQL. Double-click on the VM to open.



36. The console for the **OnPremVM** will load. Press **Enter** to get a login prompt.



37. Login to the VM using the following credentials:

- User Name:** mcwadmin
- Password:** demo@pass123

38. Once logged in enter a few commands and notice that you can get to the internet and that the **local IP address of the VM is currently 192.168.0.10**

```
ping 8.8.8.8 -c 4
ifconfig
```

```
mcwadmin@onpremlinuxvm:~$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=5.86 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=6.35 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=5.98 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=52 time=6.28 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 5.861/6.121/6.357/0.220 ms
mcwadmin@onpremlinuxvm:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:15:5d:00:04:01
          inet addr:192.168.0.10  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe00:401/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:104552 errors:0 dropped:231 overruns:0 frame:0
            TX packets:3474 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:15540271 (155.4 MB)  TX bytes:254369 (254.3 KB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:65536  Metric:1
            RX packets:224 errors:0 dropped:0 overruns:0 frame:0
            TX packets:224 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:51841 (51.8 KB)  TX bytes:51841 (51.8 KB)

mcwadmin@onpremlinuxvm:~$ _
```

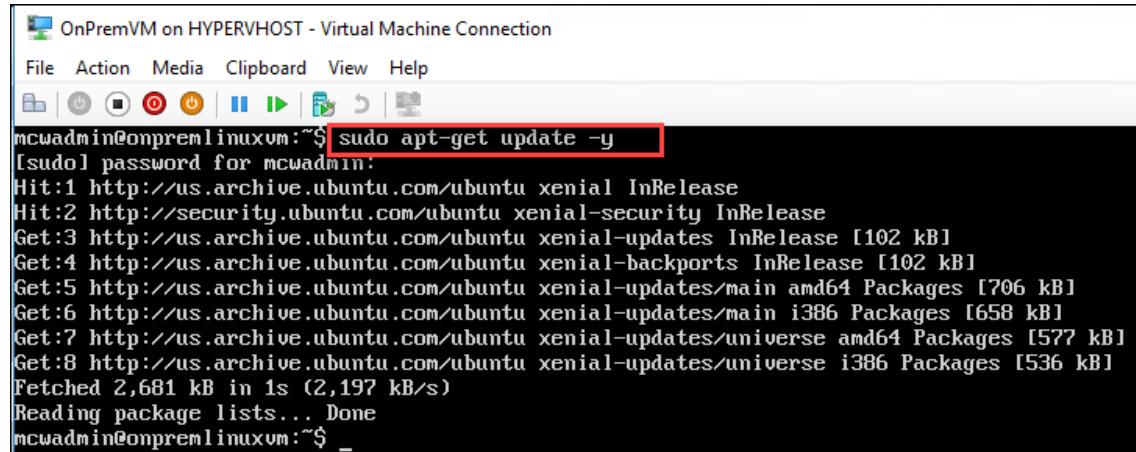
39. Open Internet Explorer on **HYPERVHOST** and browse to the following URL of the **OnPremVM**. This is very simple PHP application running on the **OnPremVM** connected to the MySQL Server that is running locally on the VM. This is to simulate an application is that running on one VM in the on-premises data center.

```
http://192.168.0.10/bcdr.php
```



40. From the command prompt of the **OnPremVM** update the OS with the latest patches by using the following command. You will need to enter the password again.

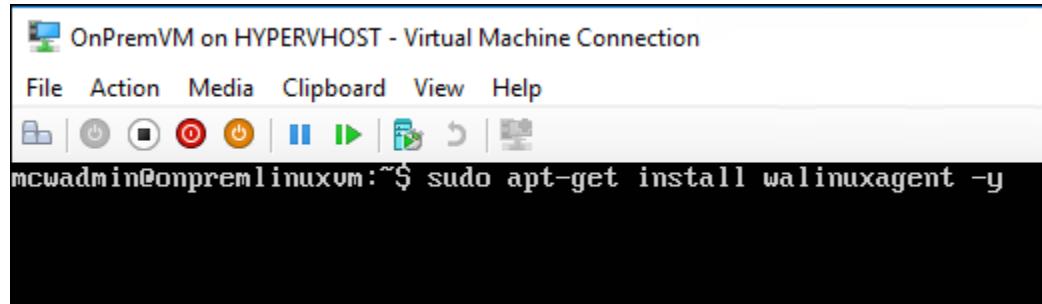
```
sudo apt-get update -y
```



```
OnPremVM on HYPERVHOST - Virtual Machine Connection
File Action Media Clipboard View Help
mcwadmin@Onpremlinuxvm:~$ sudo apt-get update -y
[sudo] password for mcwadmin:
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Hit:2 http://security.ubuntu.com/ubuntu xenial-security InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [706 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [658 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packages [577 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages [536 kB]
Fetched 2,681 kB in 1s (2,197 kB/s)
Reading package lists... Done
mcwadmin@Onpremlinuxvm:~$ _
```

41. After the updates complete, install the Azure Guest Agent for Linux on the VM using the following commands

```
sudo apt-get install walinuxagent -y
```



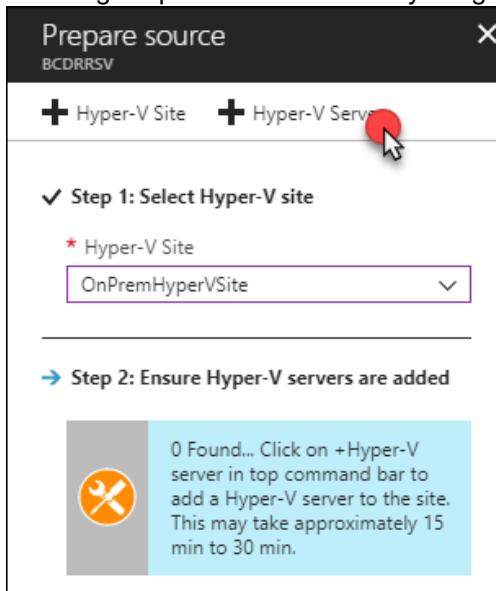
```
OnPremVM on HYPERVHOST - Virtual Machine Connection
File Action Media Clipboard View Help
mcwadmin@Onpremlinuxvm:~$ sudo apt-get install walinuxagent -y
```

Note: You may see some errors, but this is normal behavior since the VM now thinks it should be in Azure.

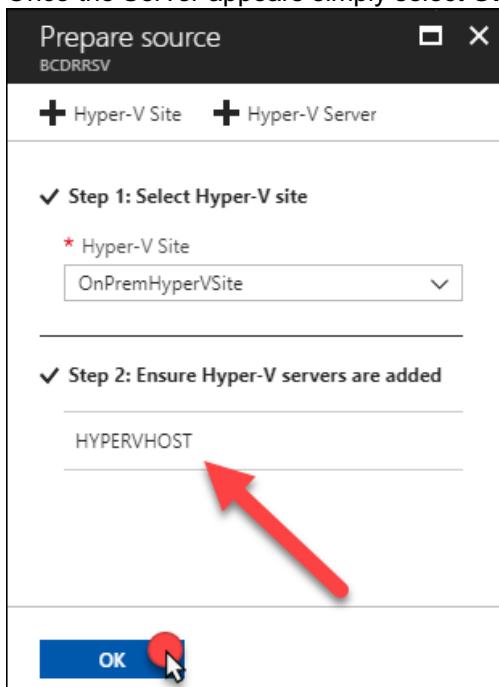
42. Enter exit to log out of the **OnPremVM**

43. Sign out of **HYPERVHOST** and return to the Azure portal running on your **LABVM**

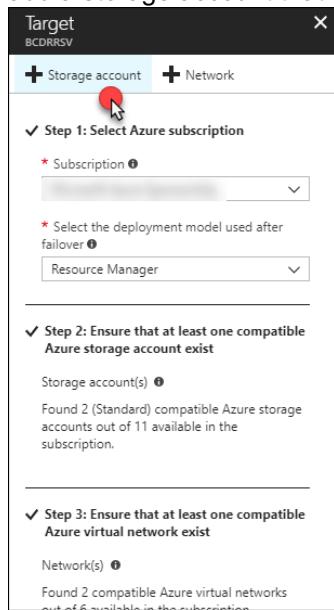
44. You will need to Return to the Prepare Source screen and select **+Hyper-V Server**. Notice the warning that it could take up to 30 mins for this server to appear, but in practice you should cancel out of this window by selecting Step 2 and then answer yes again with **I have done it** to the question of Deployment planning.



45. Once the Server appears simply select **OK**

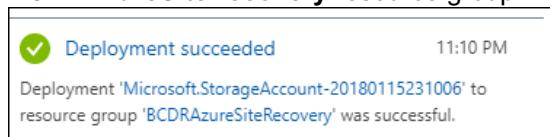


46. On **Step 4 Target Prepare** review the screen to better understand the various steps. Select **+Storage account** to add a storage account that will be used for the **OnPremVM** when it is failed over to Azure.

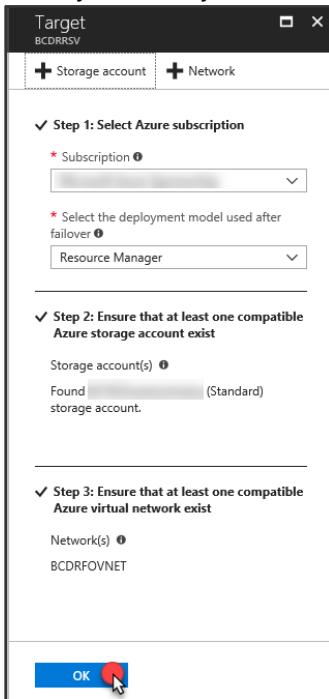


47. Select **Create New** and provide a unique name for your storage account containing the name of the VM **OnPremVM** with added characters to make it unique. Also, select the Premium tier for the storage account and select **OK**.

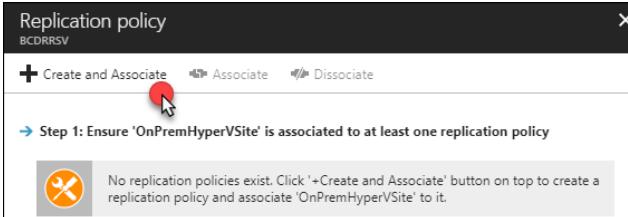
48. The portal will submit a deployment, and you must wait until this completes. It will be created in the **BCDRAzureSiteRecovery** resource group.



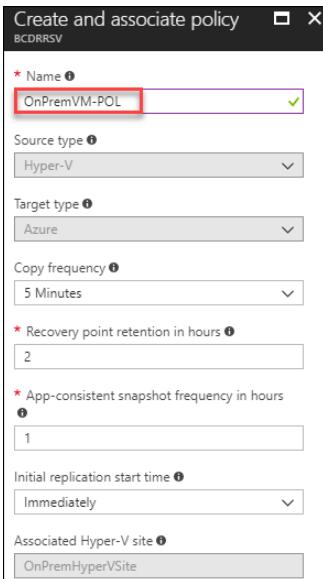
49. You will be failing the **OnPremVM** into the **Secondary** site that was deployed with your IaaS installation, so as a result you already have a Virtual Network created. Select **OK** on the Target blade to continue.



50. On Step 5: Replication settings screen you will select the **+Create and Associate** to a **Replication policy**



51. Enter the Name: **OnPremVM-POL**, review the settings that you can configure and then select **OK**



52. Azure will run a deployment and start the process of creating and then associating the Hyper-V Site with the replication policy

→ Step 1: Ensure 'OnPremHyperVSite' is associated to at least one replication policy

* Replication policy ⓘ
Select

*** Creating replication policy (View job in progress)

⌚ Waiting for replication policy creation. Association will start automatically.

→ Step 1: Ensure 'OnPremHyperVSite' is associated to at least one replication policy

* Replication policy ⓘ
OnPremVM-POL

✔ Successfully created replication policy (View job)

*** Associating 'OnPremHyperVSite' to replication policy (View job in progress)

Note: This will take a couple of minutes to complete. Please wait until this completes prior to moving on.

Once complete select **OK**

Replication policy
BCDRRSV

+ Create and Associate Associate Dissociate

✓ Step 1: Ensure 'OnPremHyperVSite' is associated to at least one replication policy

* Replication policy ⓘ
OnPremVM-POL

✔ Successfully created replication policy (View job)

✔ Successfully associated 'OnPremHyperVSite' to replication policy (View job)

OK

53. Select **OK** again, and the process for adding the Hyper-V Server to the Recovery Services Vault will be complete

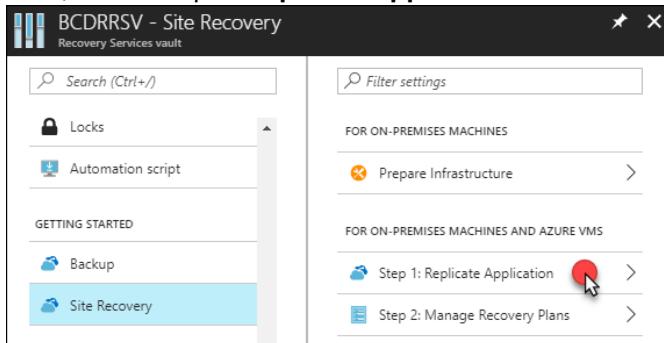
Prepare infrastructure
BCDRRSV

These are long running tasks done on-premises.

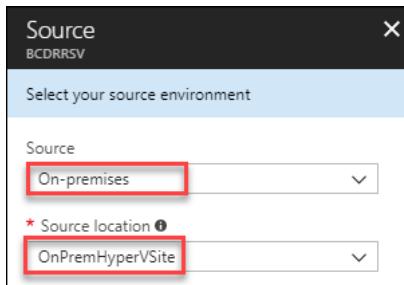
1	Protection goal Hyper-V VMs to Azure	✔
2	Deployment planning I have done it	✔
3	Source OnPremHyperVSite	✔
4	Target Azure	✔
5	Replication settings OnPremVM-POL	✔

OK

54. Next, select Step 1: **Replicate Application**

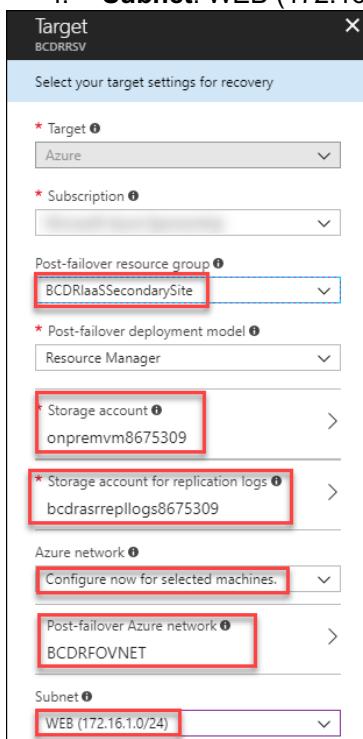


55. On the Source blade select: Source: **On-premises** and Source location: **OnPremHyperVSite** and select **OK**.

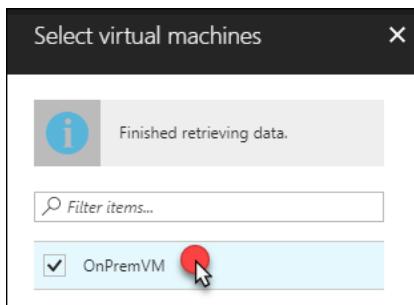


56. Complete the Target blade using the following inputs:

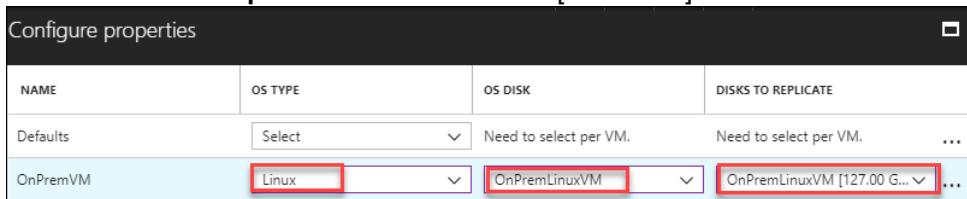
- Post-failover resource group:** BCDRlaaSSecondarySite
- Storage Account:** Select the account you just created (onpremvm8675309)
- Storage Account for replication logs:** create a new one using the prefix bcdrasreplogs
- Azure network:** configure now for selected machines
- Post-failover Azure network:** BCDRFOVNET
- Subnet:** WEB (172.16.1.0/24)



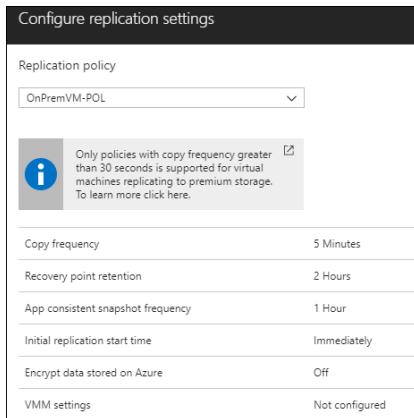
57. Next on the **Select virtual machines** select **OnPremVM** and then select **OK**



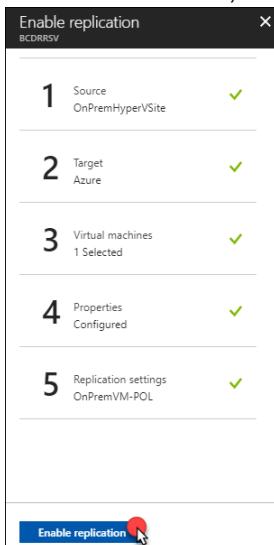
58. Complete the **OnPremVM** selections of the **Configure properties** blade using these inputs and then select **OK**
- OS Type:** Linux
 - OS Disk:** OnPremLinuxVM
 - Disks to Replicate:** OnPremLinuxVM [127.00GB]



59. On the **Configure replication settings** blade review the selections and notice that the **OnPremVM-POL** that you created has been selected. Select **OK**.



60. On the final screen, select **Enable replication**



61. The deployment will be submitted. You can select **Jobs**, Site Recovery Jobs to review the process

Name	Status	Type	Item
Enable replication	In progress	Protected item	OnPremVM
Associate replication policy	Successful	Replication policy	OnPremVM-POL
Create replication policy	Successful	Replication policy	OnPremVM-POL
Register the Azure Site Recove...	Successful	Server	HYPERVHOST
Create a site	Successful	Server	OnPremHyperVSite

62. After a few minutes, the Enable replication will move to Successful. Select **Overview** on the **BCDRRSV**, and you should now see that there is 1 Healthy Replicated Item.

Replicated items (View all)

- CRITICAL: 0
- WARNING: 0
- HEALTHY: 1**
- NOT APPLICABLE: 0

63. Select **Healthy 1** and you will see the replicated items list. Notice it shows that the VM is healthy, but the replication has just started, so it shows **0% synchronized**. It will take a few minutes for the VM to replicate.

The screenshot shows a table titled 'Replicated items' with one item listed:

NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION
OnPremVM	Healthy	0% synchronized	OnPremHyperVSite

A red arrow points to the '0% synchronized' status.

64. Select **OnPremVM**. Review the Replication details for **OnPremVM**. Once the VM has replicated the selections across the top menu bar of the dashboard will allow you to work with this VM.

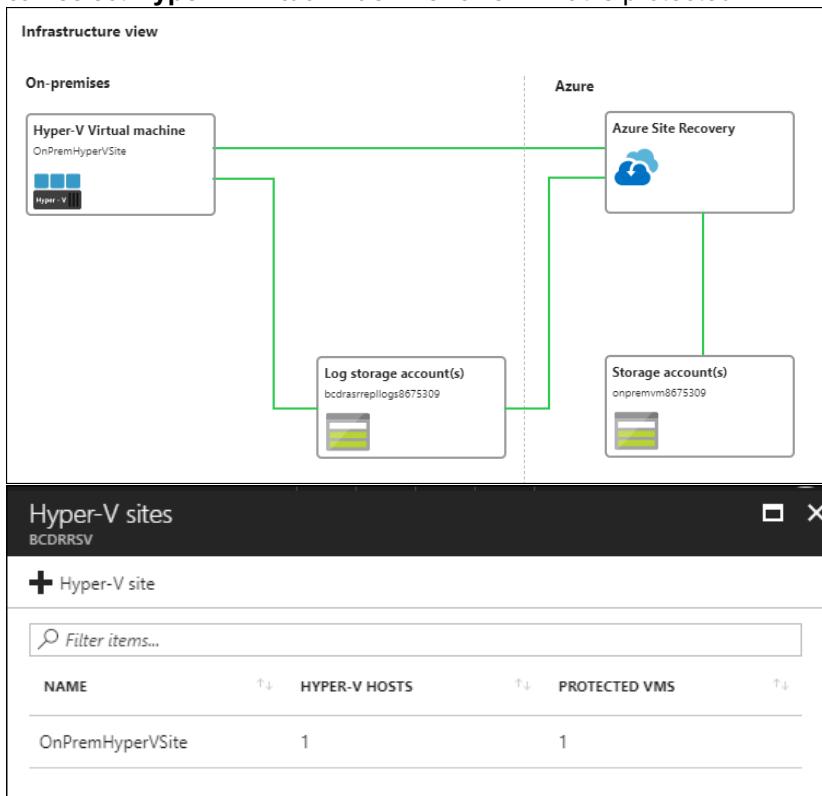
The screenshot shows the 'OnPremVM' dashboard under the 'Replicated items' section. The 'Overview' tab is selected. In the 'Health and status' section, the 'Status' is listed as 'Protected'.

Replication Health	Status	Latest available recovery points
Healthy	Protected	Crash-consistent App-consistent

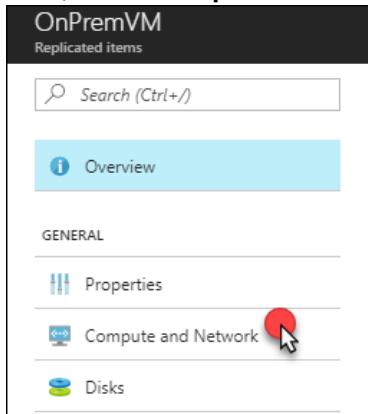
A red arrow points to the 'Protected' status.

Note: It will take about 15 minutes for the VM to replicate, so you can move on and come back to review the environment later.

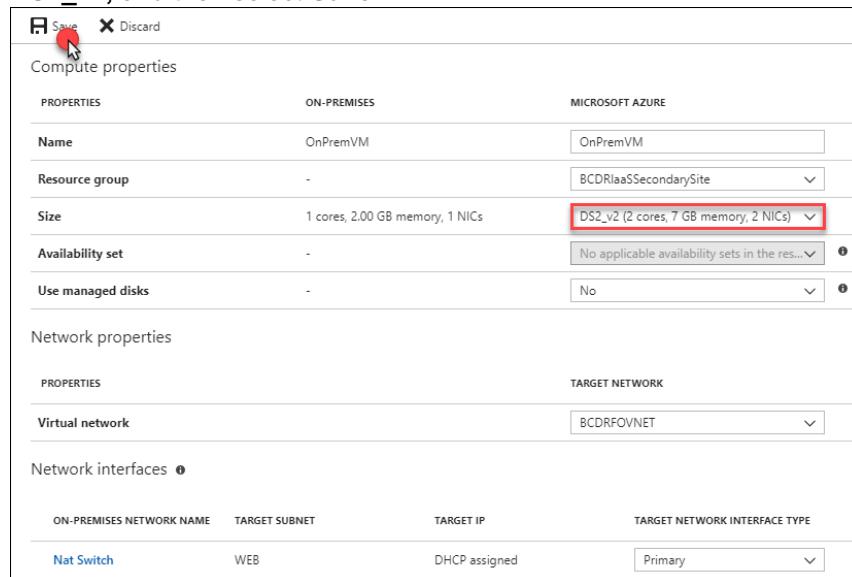
65. Scroll down and review the Infrastructure view of the BCDR environment you have created for **OnPremVM**. You can select **Hyper-V Virtual Machine** review what is protected.



66. Next, select **Compute and Network**



67. Details of the VM will be shown, and you can make configuration changes. Change the **Size** of the VM to **DS2_v2**, and then select **Save**.

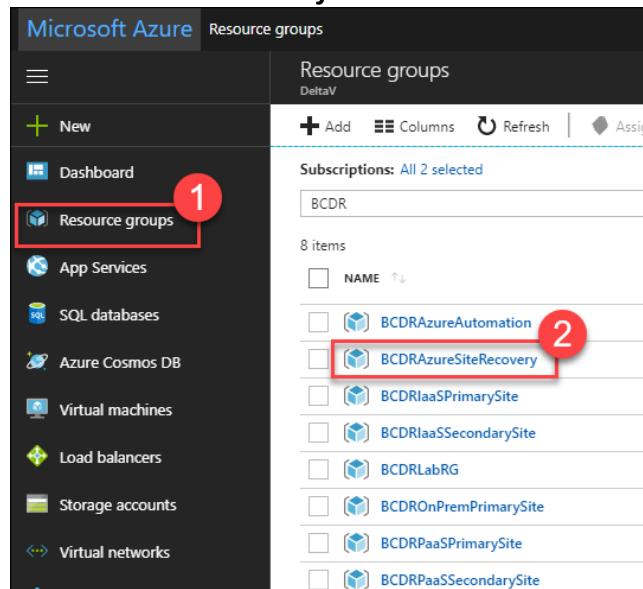


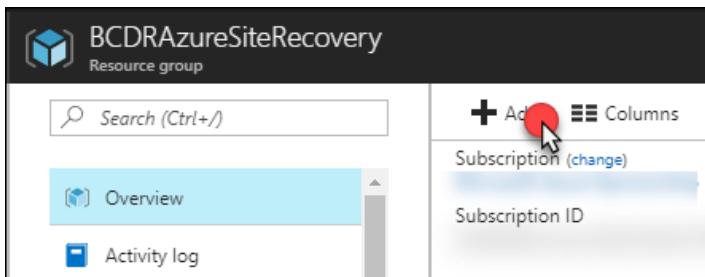
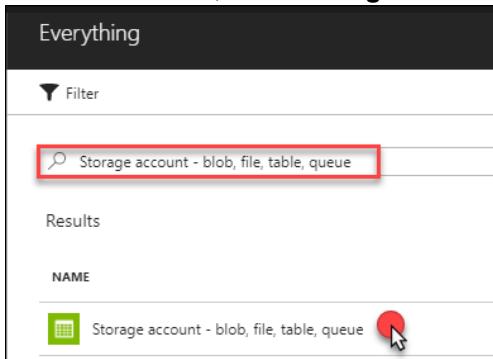
Note: It could take a few minutes for these screens to populate, so be patient. You can come back to this step later to adjust the size if you wish.

Task 2: Configure IaaS SQL Always On availability groups for region to region failover

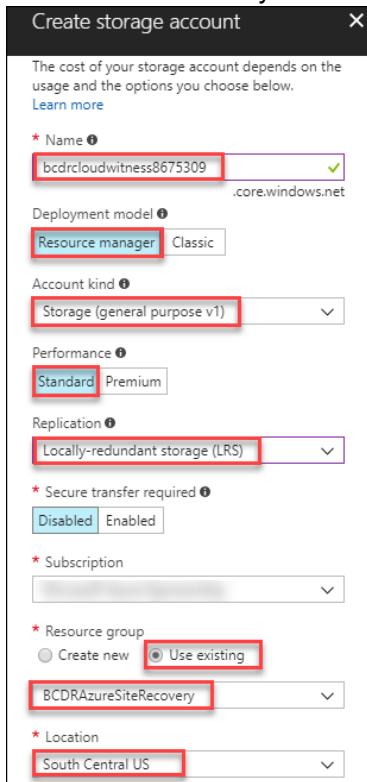
In this task, you will build a Windows Failover Cluster and configure SQL Always On Availability Groups. This will be in place to ensure that if there is an issue in the **Primary** site in Azure you can failover to the **Secondary** site and have access to the data for the application. You will also configure the Traffic Manager to ensure that the Web Application will always answer to the same DNS name even when it is failed over to the **Secondary** site.

- From the **LABVM** navigate to the Azure Portal, and navigate to **Resource Groups** and then **BCDRAzureSiteRecovery**

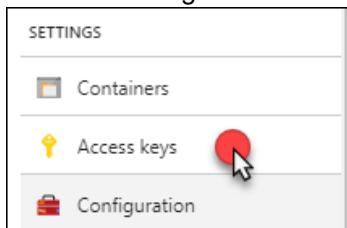


2. Select **+Add**3. In the Search box, enter **Storage Account**, and then select **Storage account – blob, file, table, queue**4. Select **Create**

5. Complete the **Create storage account** blade using the following details, then select **Create**:
- Name:** Unique name starting with bcdrcloudwitnessxxx
 - Deployment model:** Resource manager
 - Account kind:** Storage (general purpose v1)
 - Performance:** Standard
 - Replication:** Locally-redundant storage (LRS)
 - Access tier:** Hot
 - Resource group:** Use existing / BCDRAzureSiteRecovery
 - Location:** any location in your area that is NOT your Primary or Secondary Site



6. Once the storage account is created, locate and select **Access keys** under **Settings**



7. Copy the name of the account and the first access key to notepad and save the file as **C:\HOL\Deployments\CloudWitness.txt** on your LABVM

The screenshot shows the Azure Storage account keys page with the account name 'bcdrcloudwitness8675309' and two keys listed. The first key is selected, and a 'Click to copy' button is highlighted with a red circle. Below, a Notepad window titled 'CloudWitness - Notepad' contains the account name and the copied key.

NAME	KEY
key1	+SSECv1PiSgoeyU6WGNIO3XYQOAIi1rcSgxpTN6...
key2	Veg9ZLYpd3CE4uJ852GM9uLuWBa3jbsi3Ud6DEL...

CloudWitness - Notepad

File Edit Format View Help

Account Name:

bcdrcloudwitness8675309

KEY1:

+SSECv1PiSgoeyU6WGNIO3XYQOAIi1rcSgxpTN62++o/...

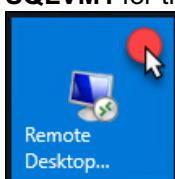
8. From the **LABVM**, connect to the Azure portal and locate the **BCDRaaSPrimarySite**

The screenshot shows the Azure Resource groups page. A red circle labeled '1' highlights the 'Resource groups' link in the left sidebar. Another red circle labeled '2' highlights the 'BCDRaaSPrimarySite' resource group in the list of items.

9. Select **BCDRDC1** and then select **Connect**

The screenshot shows the Azure Virtual machine details page for 'BCDRDC1'. A red circle highlights the 'Connect' button in the top right corner. The 'Overview' tab is selected in the left navigation pane.

10. Once in the RDP session to **BCDRDC1**, select **Start** and then **Remote Desktop**. You will need to connect to **SQLVM1** for the next steps

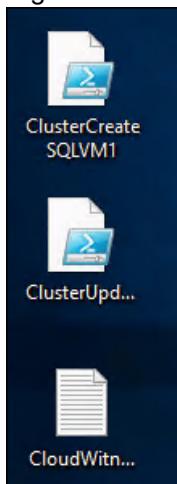


11. Connect to **SQLVM1** using the following credentials:

- User Name:** CONTOSO\mcwadmin
- Password:** demo@pass123



12. Minimize your Remote Desktop window and locate three files: **ClusterCreateSQLVM1.ps1**, **ClusterUpdateSQLVM1.ps1** and **CloudWitness.txt** in the **C:\HOL\Deployments** directory of your **LABVM**. Right-click the files and copy them, then move back to your **SQLVM1** and **paste the files to the desktop**.



13. On **SQLVM1**, select Start and then select **PowerShell ISE**



14. Open the **ClusterCreateSQLVM1.ps1** in the PowerShell ISE window. Then select the **green play button**. This script will create the Windows Failover Cluster and add all the SQL VMs as nodes in the cluster. It will also assign a static IP address of 10.0.2.99 to the new Cluster named **AOGCLUSTER**.

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
ClusterCreateSQLVM1.ps1 X
1 <#
2 Microsoft Cloud Workshop: BCDR
3 .File Name
4 - ClusterCreateSQLVM1.ps1
5
6 .What calls this script?
7 - This is run manually on SQLVM1 create the Windows Failover Cluster
8
9
10 .What does this script do?
11 - The Result will be a Cluster Named AOGCLUSTER running on the 10.0.2.99 IP
12 with the hostname of AOGCLUSTER.CONTOSO.COM.
13
14 - Azure Site Recovery is required for this to function properly as it relies
15 of the failover type passed.
16
17 - Two Cluster Networks will be created Cluster Network 1 (10.0.2.0/24) and
18
19 New-Cluster -Name AOGCLUSTER -Node SQLVM1,SQLVM2 -StaticAddress 10.0.2.99
20 Add-ClusterNode -Name SQLVM3

```

PS C:\Users\mcwadmin> C:\Users\mcwadmin\Desktop\ClusterCreateSQLVM1.ps1
WARNING: There were issues while creating the clustered role that may prevent the cluster from functioning correctly.
WARNING: Report file location: C:\Windows\cluster\Reports>Create Cluster

Name

AOGCLUSTER

Note: It is possible to use a wizard for this task, but the resulting cluster will require additional configuration to set the static IP address in Azure.

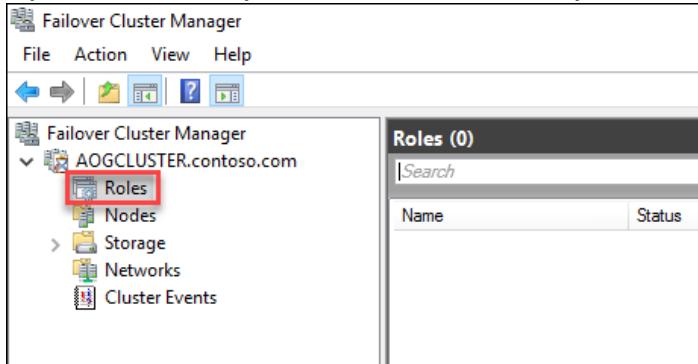
15. After the cluster has been created, select **Start** and then **Windows Administrative Tools**. Locate and open the **Failover Cluster Manager**.



16. When the cluster opens, select **Nodes** and the SQL Server VMs will show as nodes of the cluster and show their status as **Up**

Name	Status	Assigned Vote	Current Vote
SQLVM1	Up	1	1
SQLVM2	Up	1	1
SQLVM3	Up	1	1

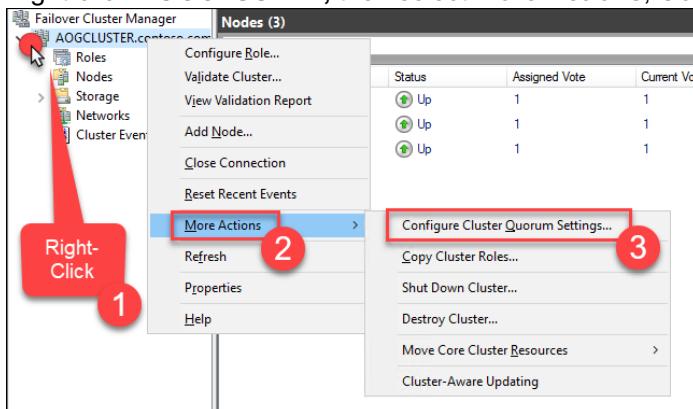
17. If you select **Roles**, you will notice there currently there aren't any roles assigned to the cluster



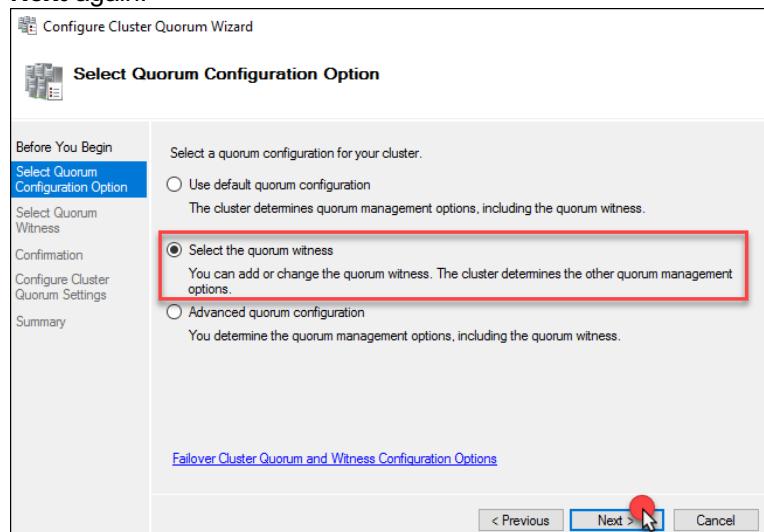
18. Select Networks, and you will see two networks: **Cluster Network 1** and **Cluster Network 2**. Both should show the status of **Up**. If you navigate through to the networks, you will see their IP address spaces, and on the lower tab you can select **Network Connections** and review the nodes.

This screenshot shows the Failover Cluster Manager interface. The 'AOGCLUSTER.contoso.com' node's 'Networks' child node is selected, indicated by a red box. The main pane shows a table titled 'Networks (2)' with two entries: 'Cluster Network 1' and 'Cluster Network 2', both marked as 'Up'. A red arrow points to the 'Status' column of the first entry. Below this, a larger window titled 'Cluster Network 1' displays network details for two nodes: 'SQLVM1' and 'SQLVM2'. Each node has an associated IP V4 Address: 10.0.2.4 and 10.0.2.5 respectively, both marked as 'Up'.

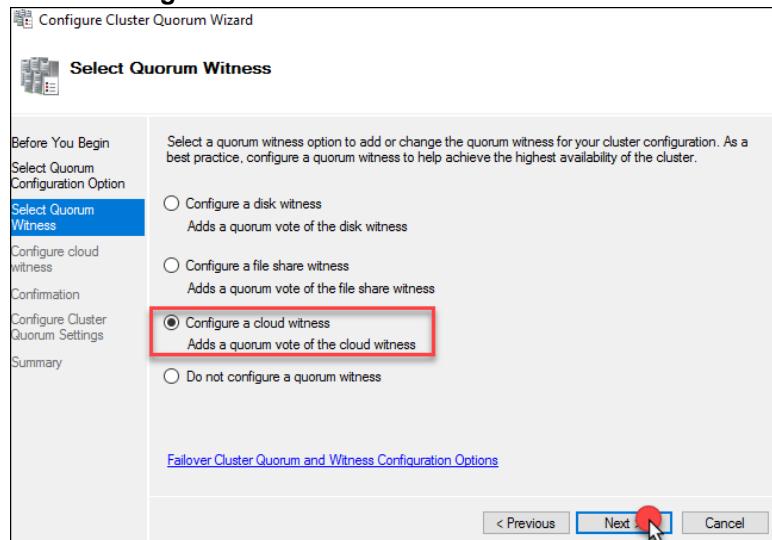
19. Right-click **AOGCLUSTER**, then select **More Actions**, **Configure Cluster Quorum Settings**



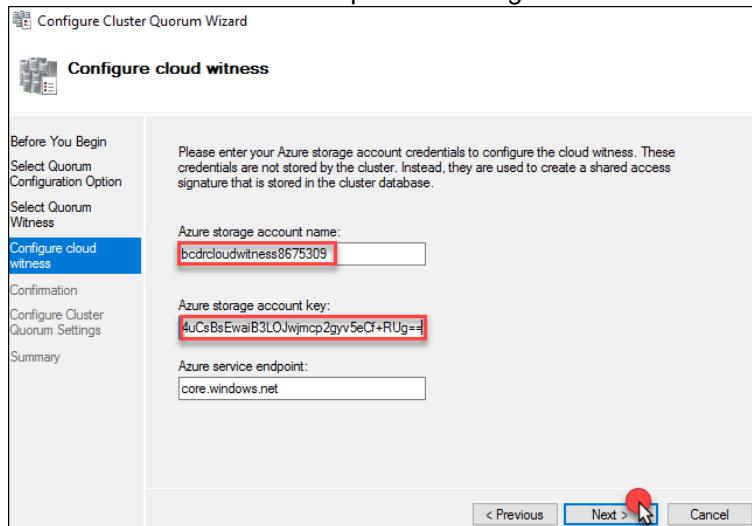
20. On the **Configure Cluster Quorum Wizard** select **Next**, then select **Select the quorum witness**. Then select **Next again**.



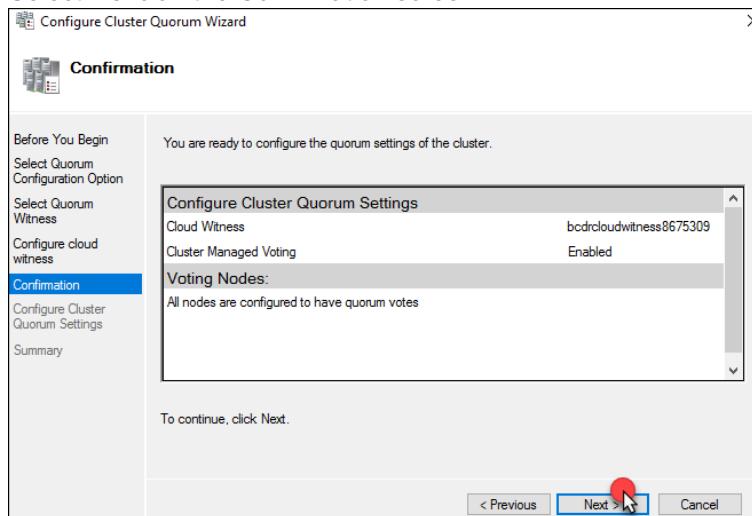
21. Select **Configure a cloud witness**

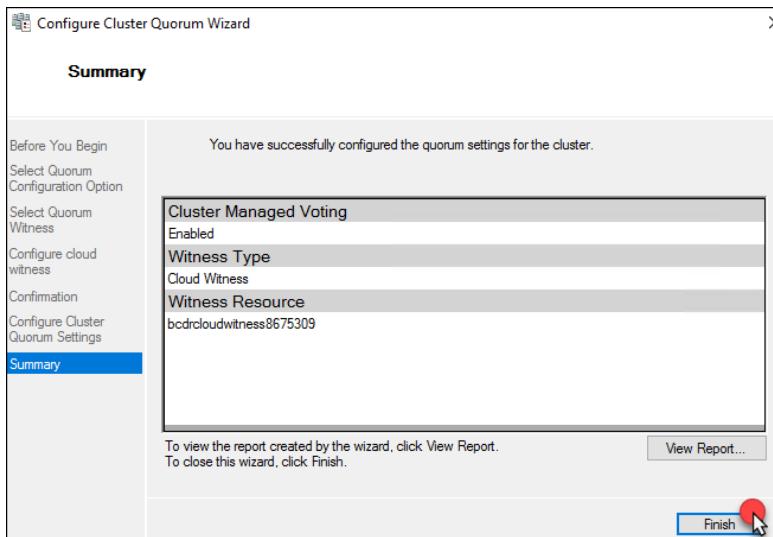


22. Open the **CloudWitness.txt** file on the desktop of **SQLVM1** and copy the **Storage account name** and **KEY1**.
Leave the Azure Service endpoint as configured. Then select **Next**.

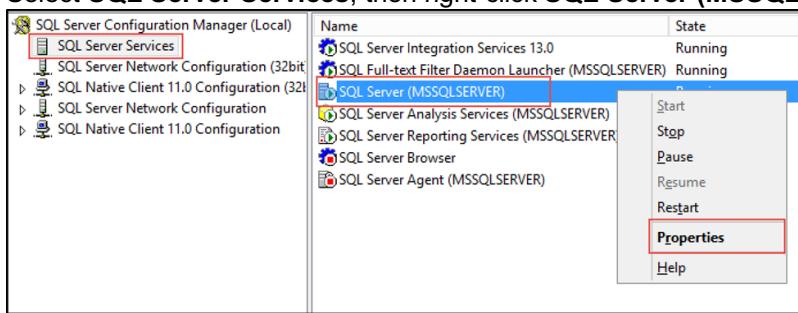


23. Select **Next** on the Confirmation screen

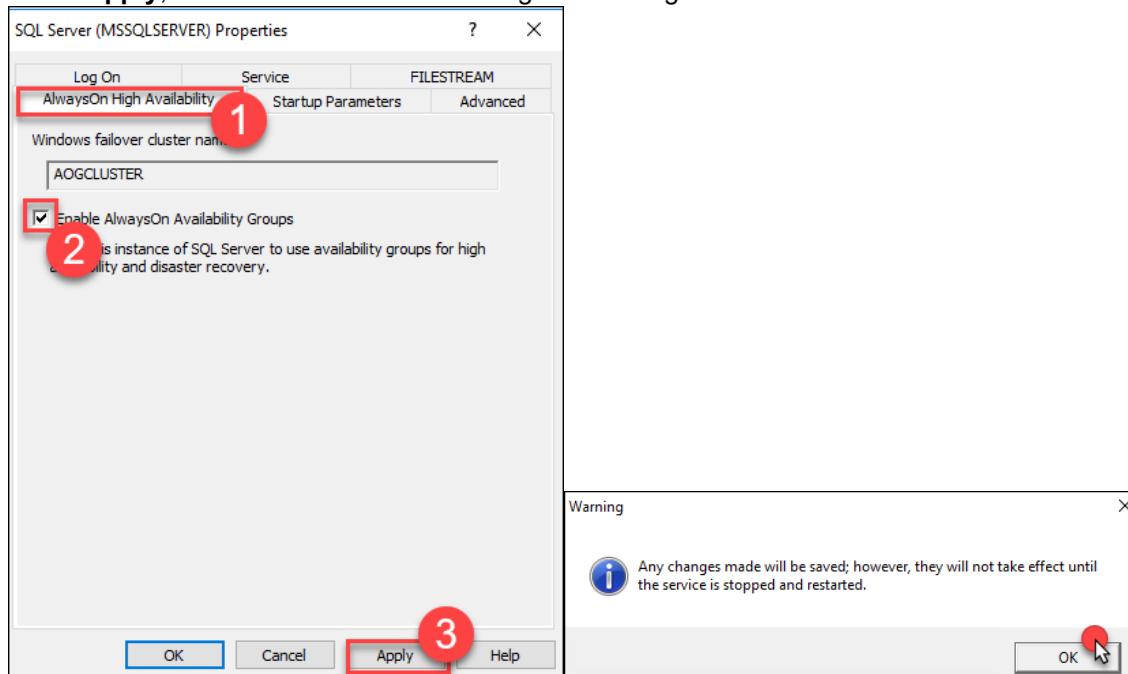


24. Select **Finish**

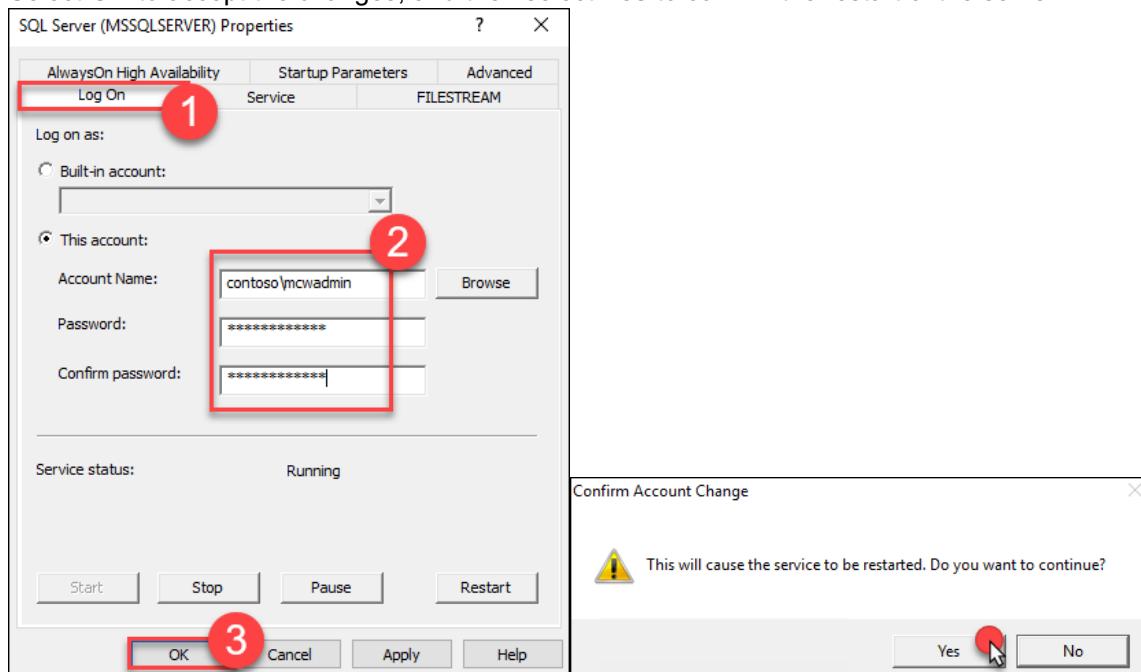
25. Select the name of the Cluster again and the **Cloud Witness** should now appear in the **Cluster Resources**. It's important to always use a third datacenter, in your case here a third Azure Region to be your Cloud Witness.

26. Select **Start** and Launch **SQL Server 2017 Configuration Manager**27. Select **SQL Server Services**, then right-click **SQL Server (MSSQLSERVER)** and select **Properties**

28. Select the **AlwaysOn High Availability** tab and check the box for **Enable AlwaysOn Availability Groups**, then select **Apply**, then select **OK** on the message that changes won't take effect until after the server is restarted



29. On the **Log On** tab. Change the service account to **contoso\mcwadmin**, with the password **demo@pass123**. Select **OK** to accept the changes, and then select **Yes** to confirm the restart of the server.



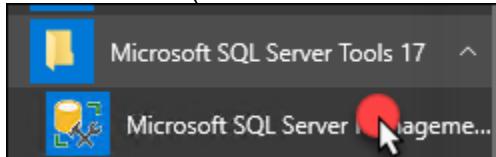
30. Open a new Remote desktop session (this can be done from within SQLVM1), and repeat these steps to **Enable SQL Always On** and change the User name to **contoso\mcwadmin** on each of the other nodes **SQLVM2**, and **SQLVM3**. Make sure that you have restarted the SQL Service on each node prior to moving to the next node.

Note: If you get confused what server you are on open a command prompt and simply enter the command `hostname`.

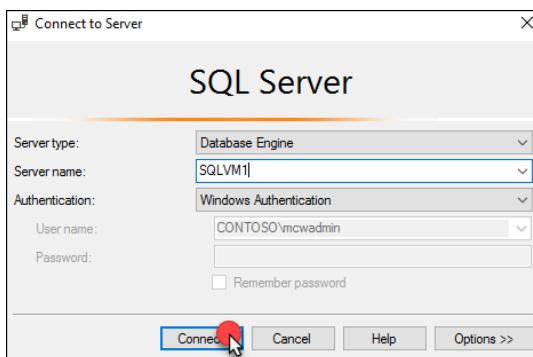
31. After you have completed the process on each SQLVM Node, reconnect to **SQLVM1** using Remote Desktop

Note: Remember that you must use the BCDRDC1 VM as your jumpbox to get into the environment. You can use the Azure portal to connect to BCDRDC1 and then use Remote desktop form there to SQLVM1.

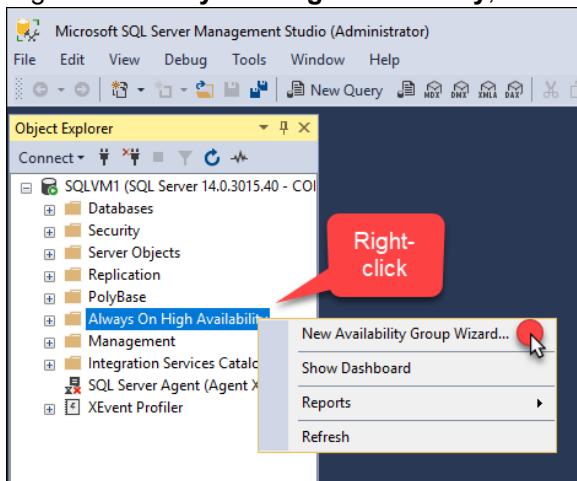
32. Use the Start menu to launch **Microsoft SQL Server Management Studio 17** and connect to the local instance of SQL Server. (Located in the Microsoft SQL Server Tools 17 folder)

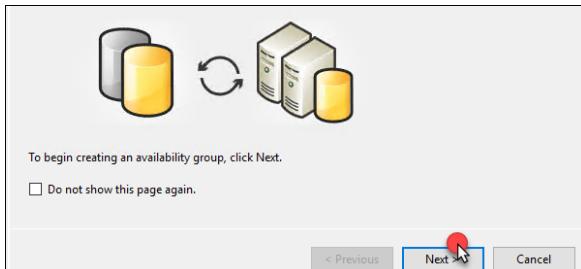
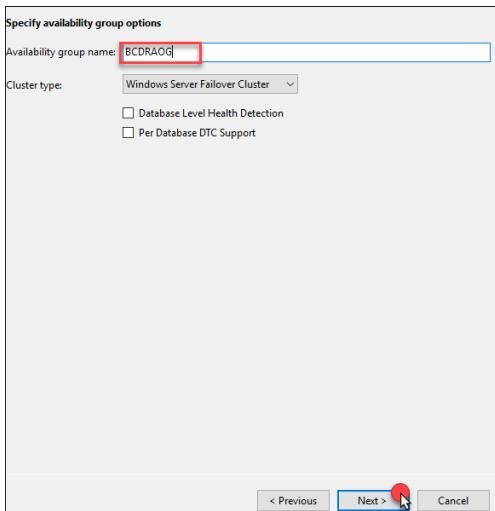
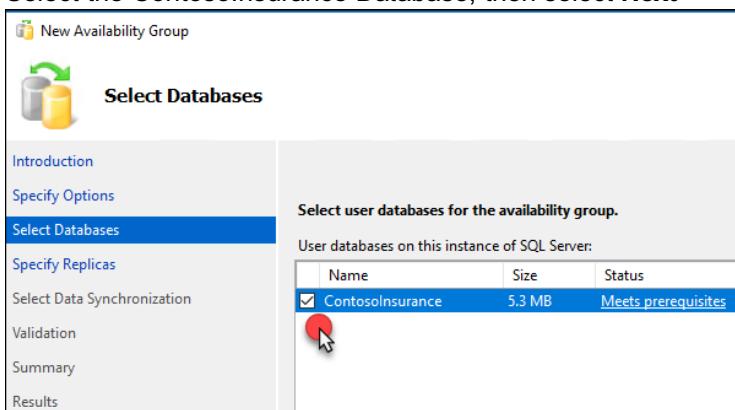
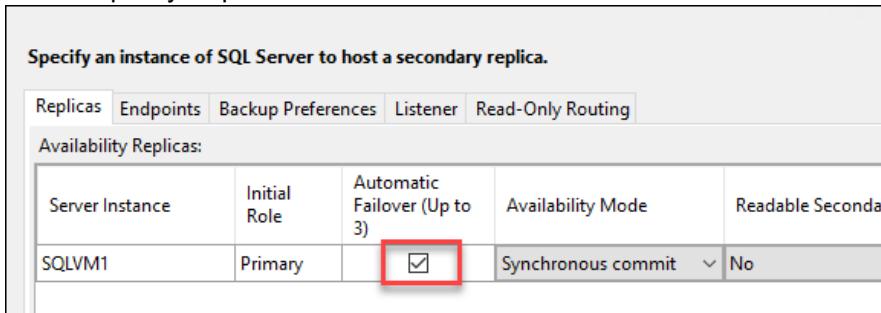


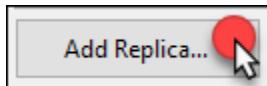
33. Select **Connect** to Sign On to **SQLVM1**



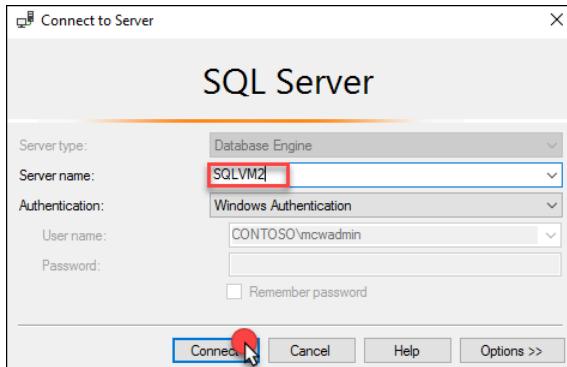
34. Right-click **Always On High Availability**, then select **New Availability Group Wizard**



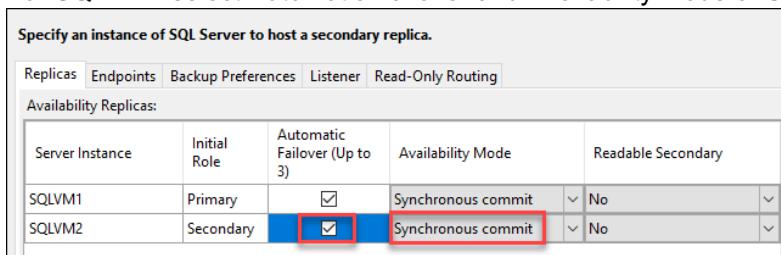
35. Select **Next** on the Wizard36. Provide the name **BCDRAOG** for the **Availability group name**, then select **Next**37. Select the ContosoInsurance Database, then select **Next**38. On the Specify Replicas screen next to **SQLVM1** select **Automatic Failover**39. Select **Add Replica**



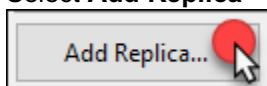
40. On the Connect to Server enter the Server Name of **SQLVM2** and select **Connect**



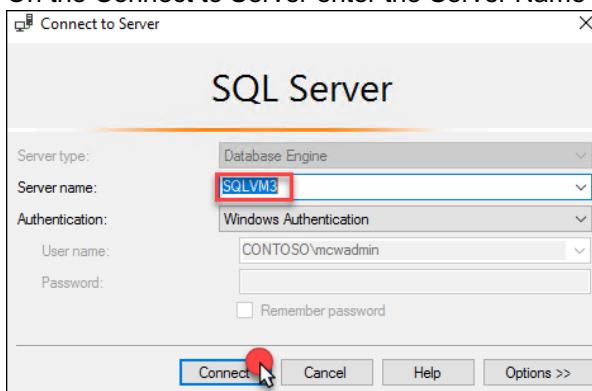
41. For **SQLVM2** select Automatic Failover and Availability Mode of Synchronous commit



42. Select **Add Replica**



43. On the Connect to Server enter the Server Name of **SQLVM3** and select **Connect**



44. At this point, the wizard should resemble the following:

Server Instance	Initial Role	Automatic Failover (Up to 3)	Availability Mode	Readable Secondary
SQLVM1	Primary	<input checked="" type="checkbox"/>	Synchronous commit	No
SQLVM2	Secondary	<input checked="" type="checkbox"/>	Synchronous commit	No
SQLVM3	Secondary	<input type="checkbox"/>	Asynchronous commit	No

45. Select Endpoints and review these that the wizard has created

Server Name	Endpoint URL	Port Number
SQLVM1	TCP://SQLVM1.contoso.com:5022	5022
SQLVM2	TCP://SQLVM2.contoso.com:5022	5022
SQLVM3	TCP://SQLVM3.contoso.com:5022	5022

46. Next, select Listener. Then select the **Create an availability group listener**

Specify an instance of SQL Server to host a secondary replica.

Replicas Endpoints Backup Preferences Listener Read-Only Routing

Specify your preference for an availability group listener that will provide a client connection point:

Do not create an availability group listener now
You can create the listener later using the Add Availability Listener dialog.

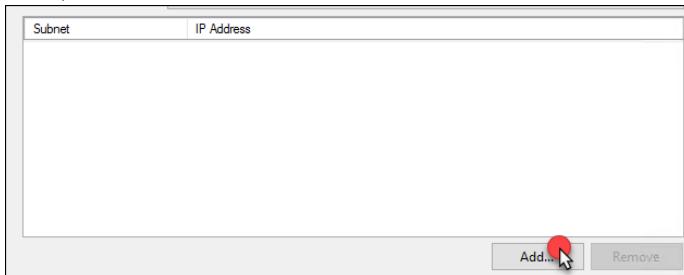
Create an availability group listener
Specify your listener preferences for this availability group.

47. Add the following details:

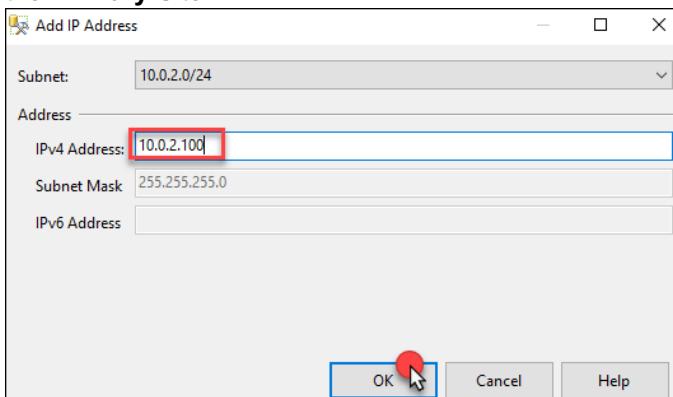
- c. **Listener DNS Name:** BCDRAOG
- d. **Port:** 1433
- e. **Network Mode:** Static IP

Listener DNS Name:	BCDRAOG
Port:	1433
Network Mode:	Static IP

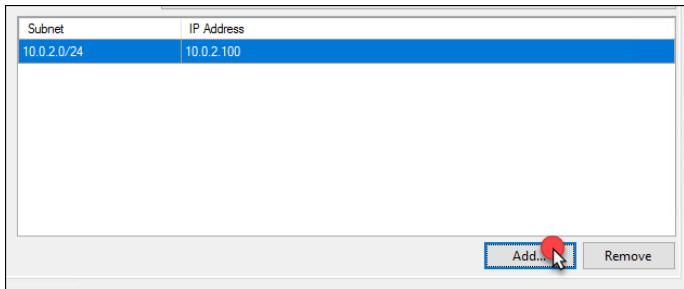
48. Next, select Add



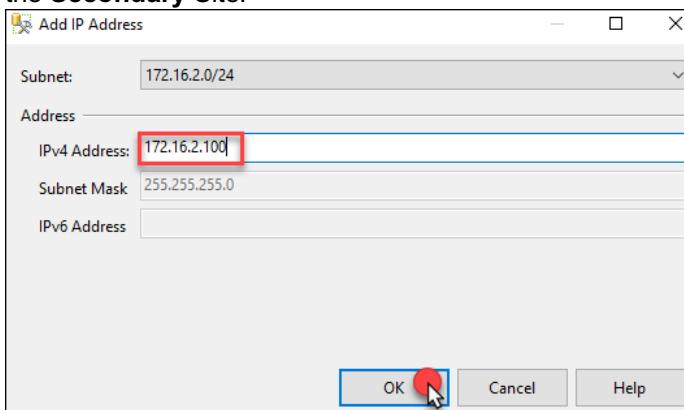
49. Select the Subnet of **10.0.2.0/24** and then add IPv4 **10.0.2.100** and select **OK**. This is the IP address of the Internal Load Balancer that is in front of the **SQLVM1** and **SQLVM2** in the **BCDRVNET Data** Subnet running in the **Primary Site**.

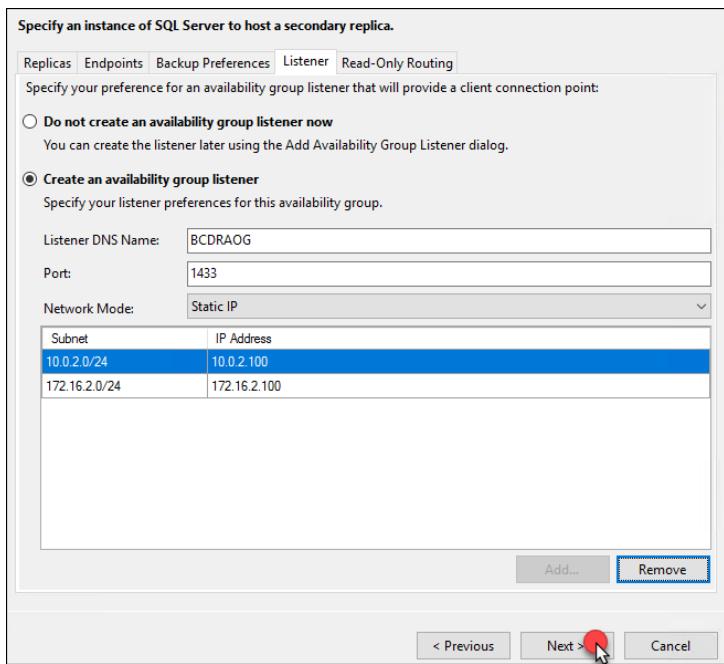


50. Select Add

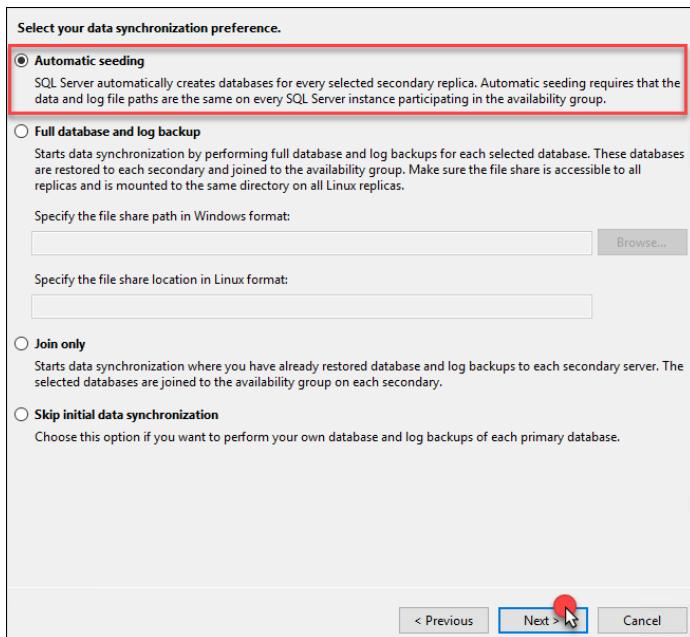


51. Select the Subnet of **172.16.2.0/24** and then add IPv4 **172.16.2.100** and select **OK**. This is the IP address of the Internal Load Balancer that is in front of the **SQLVM3** and **SQLVM4** in the **BCDRFOVNET Data** Subnet running in the **Secondary Site**.

52. Select **Next**



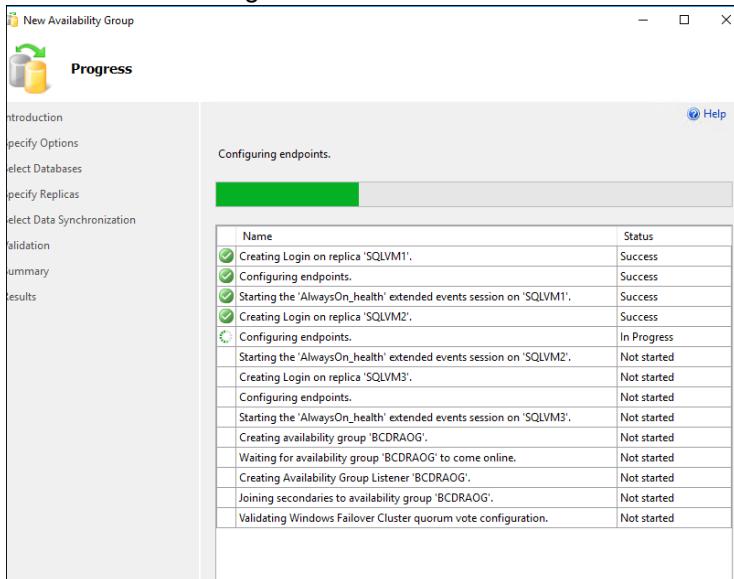
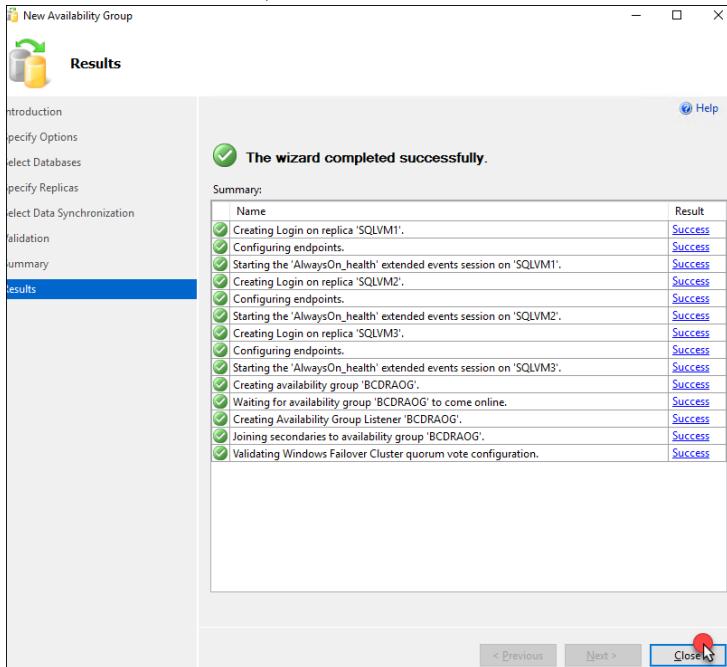
53. On the Select Initial Data Synchronization screen, make sure that **Automatic seeding** is selected and select **Next**



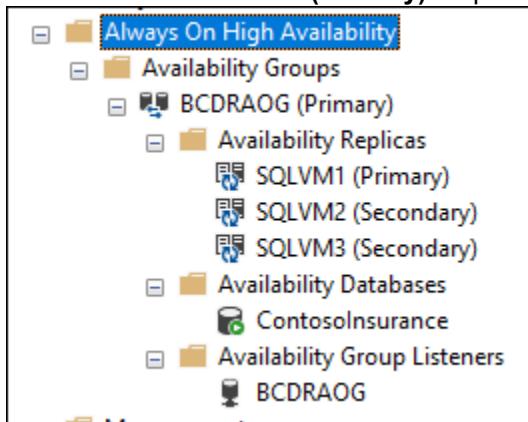
54. On the Validation screen, you should see all green. Select **Next**

Name	Result
Checking for free disk space on the server instance that hosts secondary replica SQLVM2	Success
Checking if the selected databases already exist on the server instance that hosts secondary replica S...	Success
Checking for the existence of the database files on the server instance that hosts secondary	Success
Checking for compatibility of the database file locations on the server instance that hosts replica SQL...	Success
Checking for free disk space on the server instance that hosts secondary replica SQLVM3	Success
Checking if the selected databases already exist on the server instance that hosts secondary replica S...	Success
Checking for the existence of the database files on the server instance that hosts secondary	Success
Checking for compatibility of the database file locations on the server instance that hosts replica SQL...	Success
Checking for free disk space on the server instance that hosts secondary replica SQLVM4	Success
Checking if the selected databases already exist on the server instance that hosts secondary replica S...	Success
Checking for the existence of the database files on the server instance that hosts secondary	Success
Checking for compatibility of the database file locations on the server instance that hosts replica SQL...	Success
Checking whether the endpoint is encrypted using a compatible algorithm	Success
Checking replica availability mode	Success
Checking the listener configuration	Success

55. On the Summary page select **Finish**

56. The wizard will configure the AOG**57. Once the AOG is built, select Close**

58. Move back to **SQL Management Studio** on **SQLVM1** and open the **Always On High Availability** and then select on the **BCDRAOG (Primary)**. Expand the areas and review them.



59. Right-click **BCDRAOG (Primary)** and then **Show Dashboard**. You should see that all the nodes have been added and are now “Green”.

Right-Click

Show Dashboard

BCDRAOG:SQLVM1

BCDRAOG: hosted by SQLVM1 (Replica role: Primary)

Availability group state: Healthy

Primary instance: SQLVM1

Failover mode: Automatic

Cluster state: AOGCLUSTER (Normal Quorum)

Cluster type: Windows Server Failover Cluster

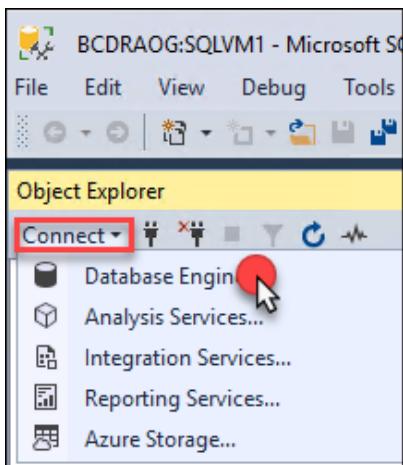
Availability replica:

Name	Role	Availability Mode	Failover Mode	Seeding Mode	Synchronization State	Issues
SQLVM1	Primary	Synchronous co...	Automatic	Automatic	Synchronized	
SQLVM2	Second...	Synchronous co...	Automatic	Automatic	Synchronized	
SQLVM3	Second...	Asynchronous co...	Manual	Automatic	Synchronizing	

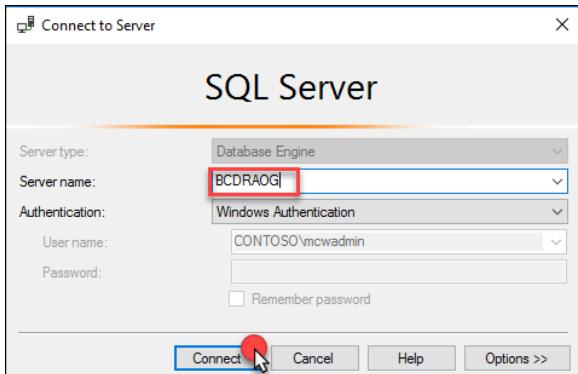
Group by ▾

Name	Replica	Synchronization State	Failover Readi...	Issues
SQLVM1	SQLVM1	Synchronized	No Data Loss	
SQLVM2	SQLVM2	Synchronized	No Data Loss	
SQLVM3	SQLVM3	Synchronizing	Data Loss	
ContosoInsurance	SQLVM1	Synchronized	No Data Loss	
ContosoInsurance	SQLVM2	Synchronized	No Data Loss	
ContosoInsurance	SQLVM3	Synchronizing	Data Loss	

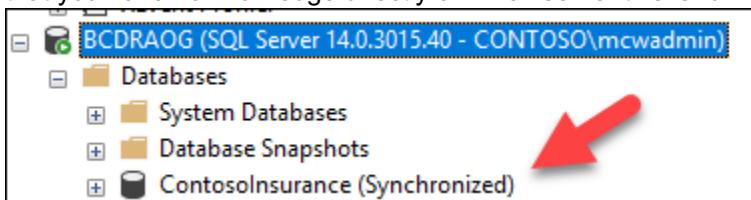
60. Next, select **Connect** and then **Database Engine** in SQL Management Studio



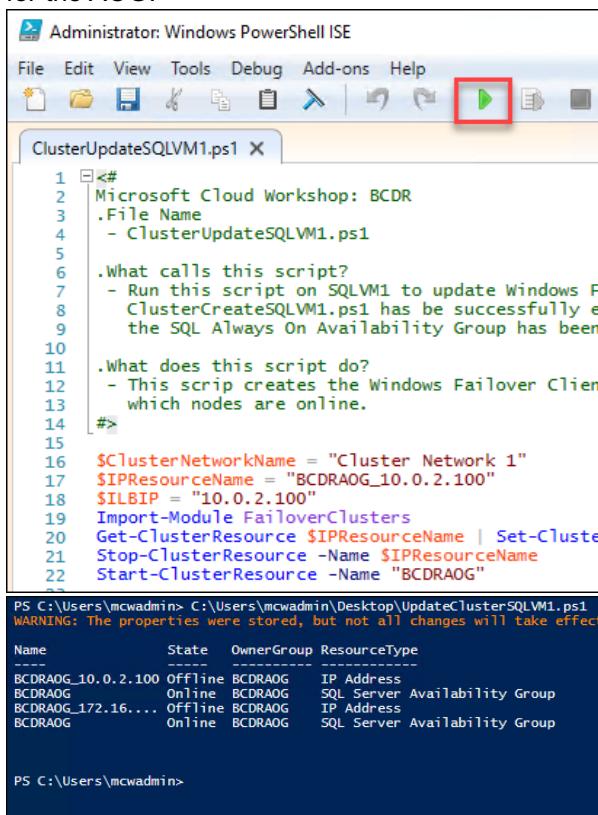
61. Enter **BCDRAOG** as the Server Name. This will be connected to the listener of the group that you created.



62. Once connected to the **BCDRAOG** you can select **Databases** and will be able to see the database there. Notice that you have no knowledge directly of which server this is running on.



63. Move back to PowerShell ISE on **SQLVM1** and open the PowerShell script named **ClusterUpdateSQLVM1.ps1**. Select the **Play** button. This will update the Failover cluster with the IP Addresses of the Listener that you created for the AOG.



```

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help
[File] [Open] [Save] [Run] [Stop] [Exit] [Redo] [Undo] [Copy] [Paste] [Find] [Replace] [Select All] [Run] [Stop] [Exit]
ClusterUpdateSQLVM1.ps1 x

1 <#
2 Microsoft Cloud Workshop: BCDR
3 .File Name
4   - ClusterUpdateSQLVM1.ps1
5
6 .What calls this script?
7   - Run this script on SQLVM1 to update Windows F
8     ClusterCreatesQLVM1.ps1 has been successfully e
9       the SQL Always On Availability Group has been
10
11 .What does this script do?
12   - This script creates the Windows Failover Client
13     which nodes are online.
14 #>
15
16 $ClusterNetworkName = "Cluster Network 1"
17 $IPResourceName = "BCDRAOG_10.0.2.100"
18 $ILBIP = "10.0.2.100"
19 Import-Module FailoverClusters
20 Get-ClusterResource $IPResourceName | Set-Cluste
21 Stop-ClusterResource -Name $IPResourceName
22 Start-ClusterResource -Name "BCDRAOG"
23

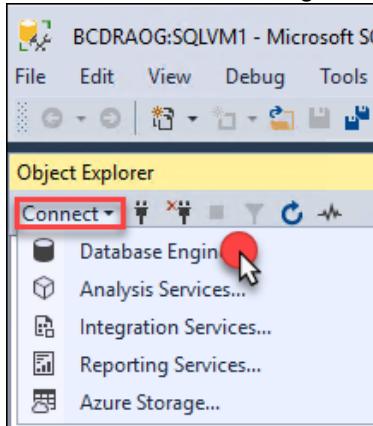
PS C:\Users\mcwadmin> C:\Users\mcwadmin\Desktop\UpdateClusterSQLVM1.ps1
WARNING: The properties were stored, but not all changes will take effect

Name          State    OwnerGroup ResourceType
----          ----    -----      -----
BCDRAOG_10.0.2.100 Offline  BCDRAOG  IP Address
BCDRAOG      Online   BCDRAOG  SQL Server Availability Group
BCDRAOG_172.16.... Offline  BCDRAOG  IP Address
BCDRAOG      Online   BCDRAOG  SQL Server Availability Group

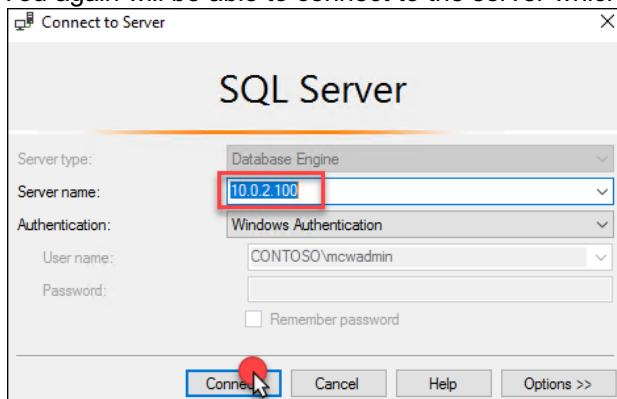
PS C:\Users\mcwadmin>

```

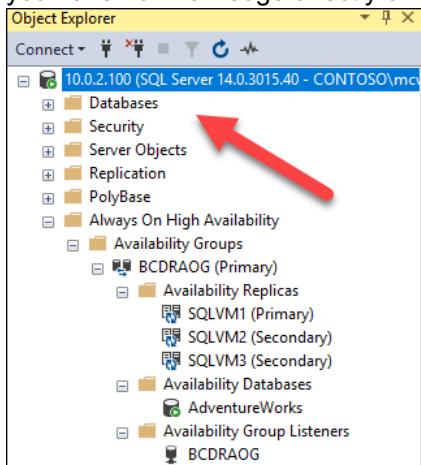
64. Move back to SQL Management Studio and select **Connect** and then **Database Engine**



65. This time put in the IP address of the Internal Load balancer of the **Primary** Site AOG Load Balancer: **10.0.2.100**. You again will be able to connect to the server which is up and running as the master.

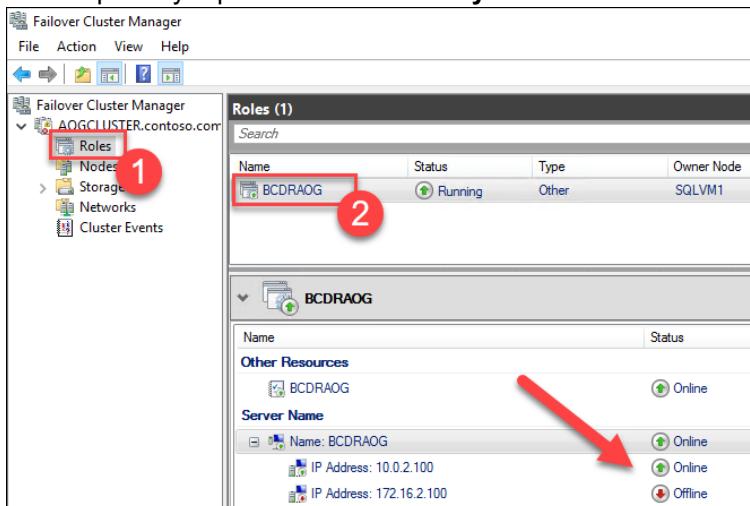


66. Once connected to **10.0.2.100** you can select **Databases** and will be able to see the database there. Notice that you have no knowledge directly of which server this is running on.



Note: It could take a minute to connect the first time as this is going through the Azure Internal Load Balancer.

67. Move back to Failover Cluster Manager on **SQLVM1**, and you can review the IP Addresses that were added by selecting Roles and **BCDRAOG** and viewing the Resources. Notice how the **10.0.2.100** is Online since the current primary replica is on the **Primary Site**.



68. Now that the AOG is up and running online the Contoso Insurance Web Application should be available. Minimize the RDP window and from the **LABVM** open the Azure portal and navigate to the resource group **BCDRIaaSPrimarySite**. Select **WWWEXTLB-PIP** which is the Public IP address for the external load balancer **WWWEXTLB** in front of **WEBVM1** and **WEBVM2** in your Primary region.



69. Locate the DNS name address and copy it to your clipboard

A screenshot of the Azure portal showing the 'WWWEXTLB-PIP' resource details. The 'DNS name' field is highlighted with a red arrow.

70. Open a new tab in the browser and navigate to the DNS name. The **Contoso Insurance PolicyConnect** application should load in your browser. Select the **Current Policy Offerings** button to check for database connectivity.

A screenshot of a web browser showing the 'Contoso Insurance PolicyConnect' homepage. The 'Current Policy Offerings' button is highlighted with a red arrow.

71. If you can see the offerings, then the application is able to access the database. You can also go back to the home page and interact with the application including adding, editing or deleting data.

Name	Description	DefaultDeductible	DefaultOutOfPocketMax	Action
Bronze	Basic coverage	1000.00	3000.00	Edit Details Delete
Silver	Basic+ coverage	800.00	2500.00	Edit Details Delete
Gold	Advanced coverage	500.00	2000.00	Edit Details Delete
Platinum	Extensive coverage	250.00	1000.00	Edit Details Delete

Note: If you see the following screen shot then something is not configured correctly with your environment. The connection string of the application is configured to use the name of **bcdraog.contoso.com** which is the name for the SQL AOG listener. This configuration is part of the connection string located in the **web.config** file which is on **WEBVM1** and **WEBVM2** in the **C:\Inetpub\wwwroot** directory. If you for some reason you named something incorrectly you can make a change to this file and then **iisreset /restart** from the command line on the WEBVMs.

Error.
An error occurred while processing your request.

72. Once you have verified that the application is up and running, you will need to build a Traffic Manager to direct traffic to the edge of your Primary and Secondary Site. Select **+NEW, Networking** then **Traffic Manager profile** in the Azure portal.

1. Click the 'New' button in the left sidebar.

2. In the Azure Marketplace search results, click on the 'Networking' category.

3. Click on the 'Traffic Manager profile' item.

73. Complete the **Create Traffic Manager profile** using the following inputs, then select **Create**:

- Name:** unique name all lowercase using bcdriaasxxx
- Routing method:** Priority
- Resource group:** Use existing / BCDRlaasPrimarySite
- Location:** automatically assigned based on the BCDRlaasSPrimarySite

The screenshot shows the 'Create Traffic Manager profile' dialog box. The 'Name' field contains 'bcdriaas8675309'. The 'Routing method' dropdown is set to 'Priority'. Under 'Resource group', the 'Use existing' radio button is selected, and 'BCDRlaasSPrimarySite' is chosen from the dropdown. The 'Resource group location' dropdown is set to 'East US 2'.

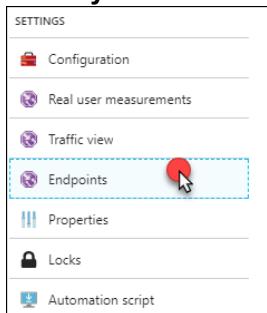
74. Once the Traffic Manager profile is created, open it in the Azure portal. Notice the DNS name. This is the URL that you will use to connect to the application. Once configured this DNS name will always respond and doesn't matter if the IaaS application is running normally in the **Primary site** or failed over to the **Secondary site**.

The screenshot shows the Azure portal's 'Overview' tab for the Traffic Manager profile 'bcdriaas8675309'. The 'DNS name' field is highlighted with a red arrow and contains the value 'http://bcdriaas8675309.trafficmanager.net'. Other visible details include the resource group 'BCDRlaasSPrimarySite', status 'Enabled', and monitor status 'Inactive'.

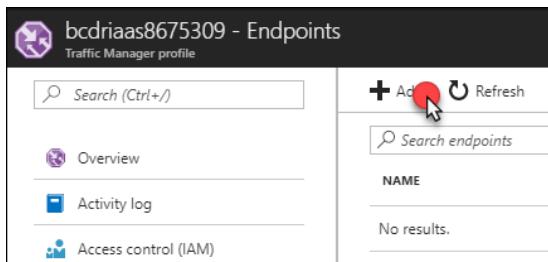
75. Select **Configuration** and review the configurations

The screenshot shows the 'Configuration' page in the Azure portal. The left sidebar under 'SETTINGS' has a list of options: Configuration (highlighted with a red circle), Real user measurements, Traffic view, Endpoints, Properties, Locks, and Automation script.

76. Next select **Endpoints**. This is where you will configure the two external load balancers that are located your **Primary** and **Secondary** sites

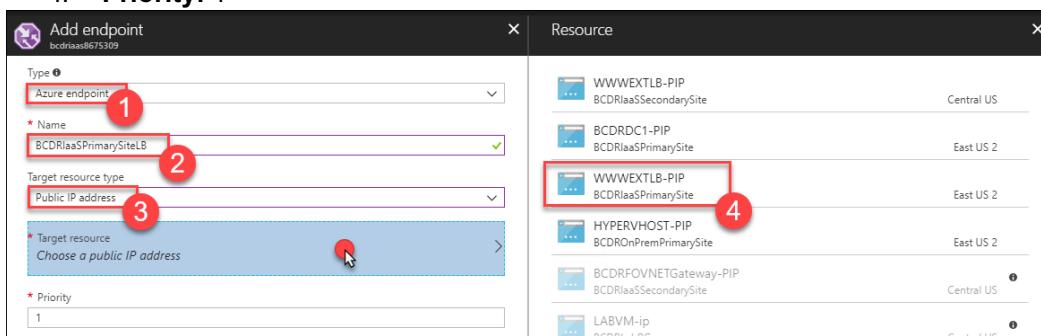


77. Select **+Add**

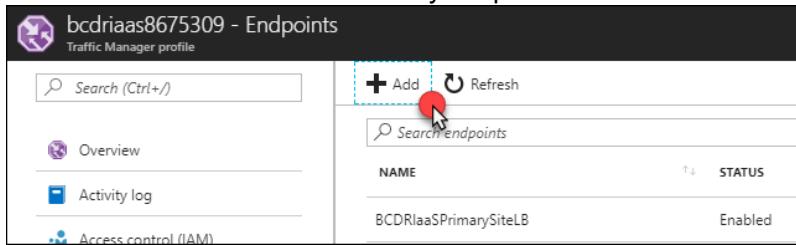


78. Complete the **Add endpoint** using the following inputs and then select **OK**:

- Type:** Azure endpoint
- Name:** BCDRlaaSPPrimarySiteLB
- Target resource type:** Public IP address
- Target resource:** Choose a public IP address
- Resource:** WWWEXTLB-PIP in the BCDRlaaSPPrimarySite
- Priority:** 1



79. Select **+Add**. Notice that the Primary endpoint was created as “**Enabled**”



80. Complete the **Add endpoint** using the following inputs and then select **OK**:

- Type:** Azure endpoint
- Name:** BCDRlaaSSecondarySiteLB
- Target resource type:** Public IP address
- Target resource:** Choose a public IP address
- Resource:** WWWEXTLB-PIP in the BCDRlaaSSecondarySite
- Priority:** 2

81. Once the second endpoint has been added, select **Overview**. Notice that the Primary endpoint is set to **Priority 1**. This means that traffic will always be directed to the **Primary** site unless it is down. The Traffic Manager will monitor the Endpoints, and if the **Primary** site moves to a **Monitor Status** of **Degraded**, then the Traffic Manager will direct traffic to the **Secondary** site. The current **Monitor Status** shows that the **Primary** site is **Online** and the Secondary site is **Degraded**. During a failover using ASR, the **Primary** site will move to **Degraded**, and the **Secondary** will move to **Online**. This will allow for traffic to flow to the failed over IaaS infrastructure now running at the **Secondary** site. This will, of course, revert during the failback to the **Primary** site.

NAME	STATUS	MONITOR STATUS	TYPE	PRIORITY
BCDRlaaSPrimarySiteLB	Enabled	Online	Azure endpoint	1
BCDRlaaSSecondarySiteLB	Enabled	Degraded	Azure endpoint	2

Note: All of this is automatic and easily configured with a vanity domain by adding a C NAME record in DNS to point to the DNS name of the Traffic Manager. This would allow for a site like www.contoso.com to resolve to the DNS name of the traffic manager. The users will never know that the site is failed over or failed back.

82. Select the DNS name of the Traffic manager the Policy Connect web application will load. This is connecting to the **WWWEXTLB** External Load Balancer that is in front of **WEBVM1** and **WEBVM2** running in the **Primary Site** in **BCDRiaasPrimarySite** resource group and connecting to the SQL Always On Listener at the same location.

The screenshot shows the Azure portal's Resource group blade for 'BCDRiaasPrimarySite'. Under the 'DNS name' section, the URL 'http://bcdriias8675309.trafficmanager.net' is listed. A red arrow points to this URL. Below it, the status is shown as 'Degraded'.

The screenshot shows a web browser window titled 'Home Page - Policy Con'. The address bar contains the URL 'bcdriias8675309.trafficmanager.net'. A red arrow points to the address bar. The page itself displays the 'Contoso Insurance Policy Connect' logo and a 'Welcome to the Policy Management System' message.

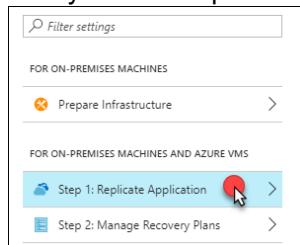
Task 3: Configure IaaS for region to region failover

In this task the WEBVM1 and WEBVM2 will be configured to replicate from the Primary Site to the Secondary site to support an Azure region to region failover. This will consist of configuring the VMs to replicate and integrating with the Azure Automation to failover the SQL Always On group from the Primary Site to the Secondary. Once the failover is complete the website will again answer to the Traffic Manager DNS name.

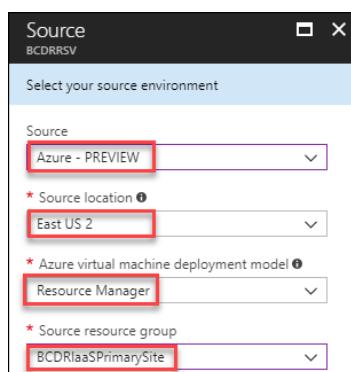
- From the Azure portal on **LABVM**, open the **BCDRRSV** Recovery Services Vault located in the **BCDRAzureSiteRecovery** resource group.
- Select **Site Recovery** in the **Getting Started** area of **BCDRRSV** blade

The screenshot shows the 'BCDRRSV Recovery Services vault' blade. In the 'GETTING STARTED' section, the 'Site Recovery' option is highlighted with a red arrow pointing to it.

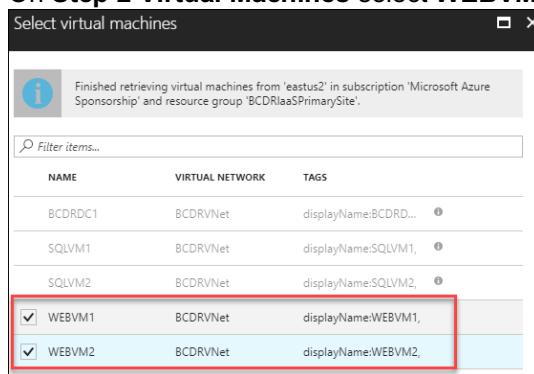
3. Next, select **Step 1: Replicate Application** in the **For On-Premises Machines and Azure VMs** section. This will start you down a path of various steps to configure your WEBVMs that are running on Azure at your Primary Site.



4. On **Step 1 Source** select the following inputs and then select **OK**:
- Source:** Azure-PREVIEW
 - Source Location:** Your Primary Region
 - Azure virtual machine deployment model:** Resource Manager
 - Source resource group:** BCDRlaaSPPrimarySite



5. On **Step 2 Virtual Machines** select **WEBVM1** and **WEBVM2** and select **OK**



6. On the **Configure settings** blade, first select the **Target location** as your **Secondary Site Azure Region**



7. Select **Customize**

* Target location ⓘ
Central US

Resource group, Network, Storage and Availability sets **Customize**

By default Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets as below. Click 'Customize' above to change the configuration. The resources created are appended with "asr" suffix.

8. Update the rest of the blade using the following inputs and the select **OK**:

- Target resource group:** BCDRlaaSSecondarySite
- Target virtual network:** BCDRFOVNET
- Target storage:** accept the new account
- Target storage:** accept the new account
- Target Availability Set:** WEBAVSET

General settings

Target resource group
BCDRlaaSSecondarySite

Target virtual network
BCDRFOVNET

VM settings

VM NAME	SOURCE STORAGE	TARGET STORAGE	CACHE STORAGE	TARGET AVAILABILITY SET
WEBVM1	bcdrstorageasedyfizo7bpc [Premium...]	(new) bcdrstorageasedyfizoasr... ▾	(new) bcdrstorageasedcacheasr... ▾	WEBAVSET
WEBVM2	bcdrstorageasedyfizo7bpc [Premium...]	(new) bcdrstorageasedyfizoasr... ▾	(new) bcdrstorageasedcacheasr... ▾	WEBAVSET

Note: Double check these selections. They are critical to your Failover.

9. Then select **Create target resources**

Configure settings

* Target location ⓘ
Central US

Resource group, Network, Storage and Availability sets **Customize**

By default Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets as below. Click 'Customize' above to change the configuration. The resources created are appended with "asr" suffix.

Target resource group ⓘ
BCDRlaaSSecondarySite

Target virtual network ⓘ
BCDRFOVNET

Cache storage accounts ⓘ
(new) bcdrstorageasedcacheasr

Target storage accounts ⓘ
(new) bcdrstorageasedyfizoasr

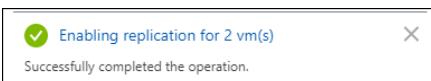
Target availability sets ⓘ
webavset

Create target resources

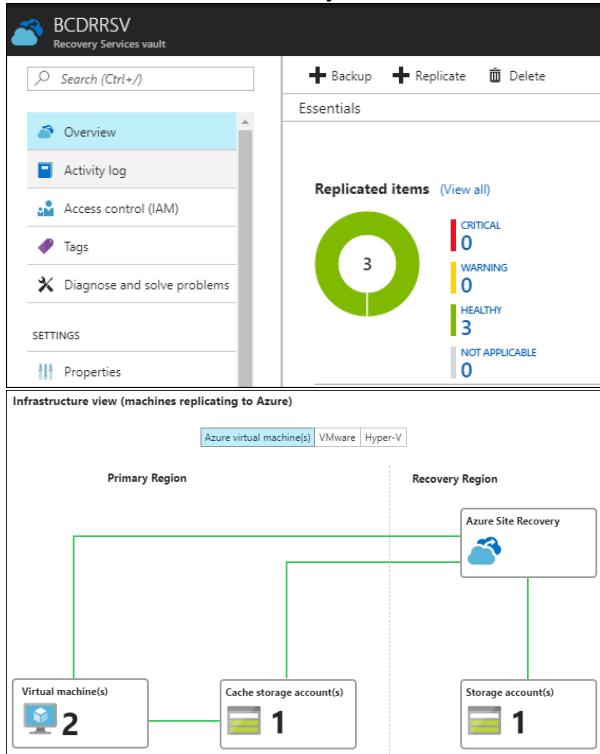
10. Then select **Enable replication**

Enable replication

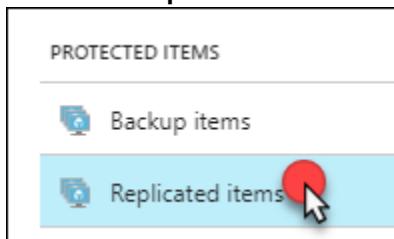
11. The Azure portal will start the deployment. This will take about 10 minutes to complete and you will receive a notification once it has



12. Select back to the Recovery Services Vault **BCDRRSV** and you will now see that 3 items are replicated



13. Select the **Replicated Items** link under **Protected Items**



14. You should see three items: **OnPremVM**, **WEBVM1** and **WEBVM2**. The **OnPremVM** will show as protected and the others may still need to synchronize a bit more

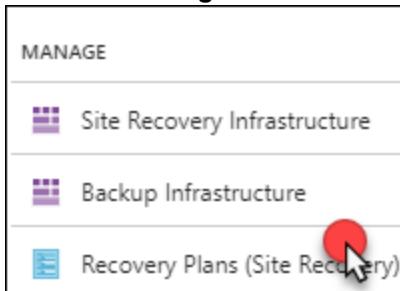
NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION
WEBVM1	Healthy	93% synchronized	East US 2
WEBVM2	Healthy	93% synchronized	East US 2
OnPremVM	Healthy	Protected	OnPremHyperVSite

15. Once **WEBVM1** and **WEBVM2** have reached Protected status, you can move on to the next step

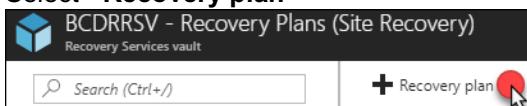
NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION
WEBVM1	Healthy	Protected	East US 2
WEBVM2	Healthy	Protected	East US 2

Note: It can take up to 30 minutes for this action to complete.

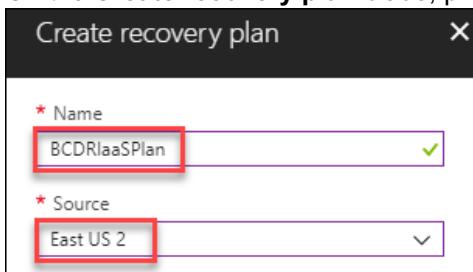
16. Under the **Manage** area select **Recovery Plans (Site Recovery)**



17. Select **+Recovery plan**

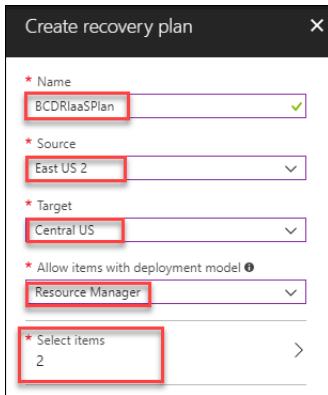


18. On the **Create recovery plan** blade, provide the Name: **BCDRIaaSPlan** and Source: select your **Primary site**



19. Complete the rest of the blade using the following inputs and then select **OK**:

- Target:** Secondary region
- Allow items with deployment model:** Resource Manager
- Select Items:** Select WEBVM1 and WEBVM2



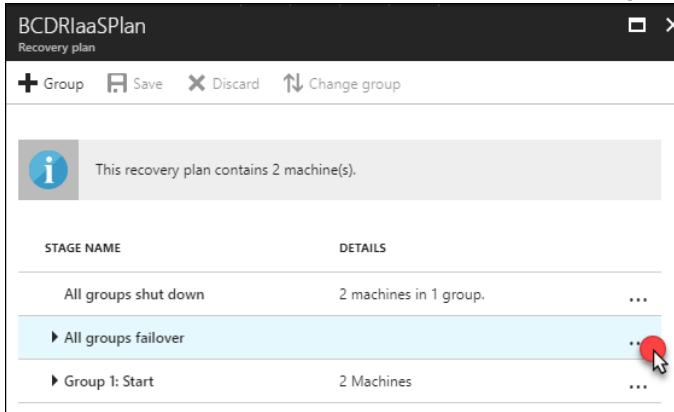
20. After a moment the **BCDRaaSPlan** Recovery plan will appear, select it to review

NAME	SOURCE	TARGET
BCDRaaSPlan	East US 2	Central US

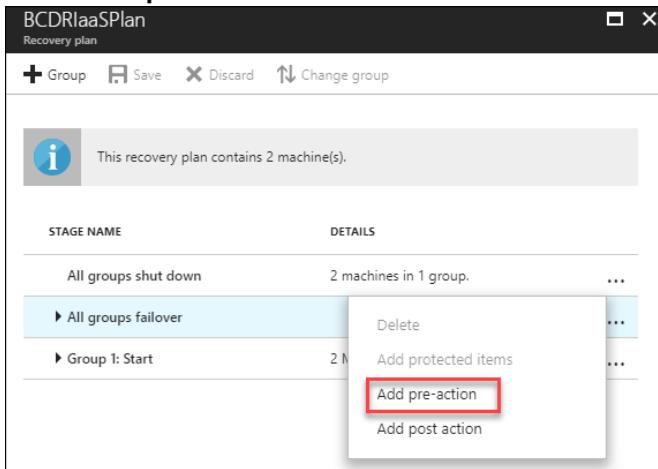
21. When the **BCDRaaSPlan** loads notice that it shows **2 VMs in the Source** which is your **Primary Site**. Then select **Customize**.

Source	Target
2	0

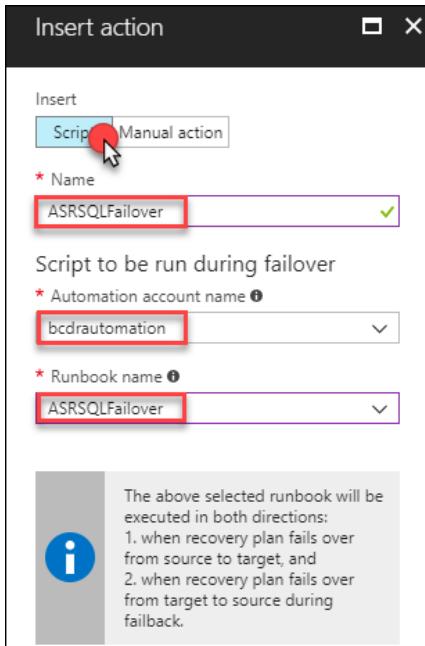
22. Once the **BCDRIaaSPlan** blade loads, select the **ellipse** next to **All groups failover**



23. Select **Add pre-action**



24. On the **Insert action** blade, select **Script** and then provide the name: **ASRSQFailover**. Ensure that your Azure Automation account is selected and then chose the Runbook name: **ASRSQFailover**. Select **OK**.



25. Once the **BCDRIaaSPlan** blade loads, select the **ellipse** next to **Group 1: Start**

BCDRlaaSPlan
Recovery plan

+ Group Save Discard Change group

You have unsaved changes.

This recovery plan contains 2 machine(s).

STAGE NAME	DETAILS
All groups shut down	2 machines in 1 group.
>All groups failover: Pre-steps	1 Step
Script: ASRSQFailover	Script
All groups failover	
Group 1: Start	2 Machines

26. Select Add post action

BCDRlaaSPlan
Recovery plan

+ Group Save Discard Change group

You have unsaved changes.

This recovery plan contains 2 machine(s).

STAGE NAME	DETAILS
All groups shut down	2 machines in 1 group.
All groups failover: Pre-steps	1 Step
Script: ASRSQFailover	Script
All groups failover	
Group 1: Start	2 Machines

...

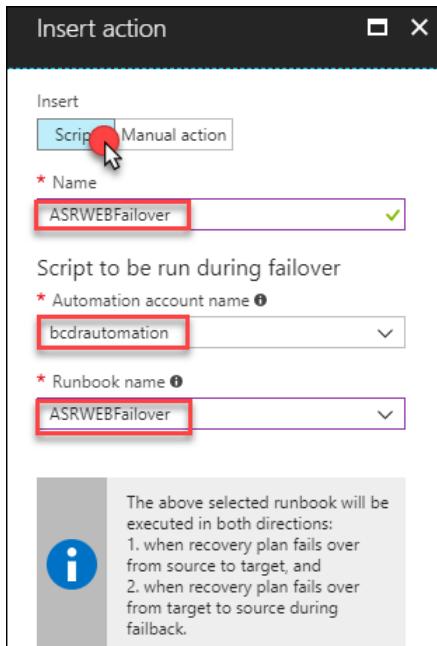
Delete

Add protected items

Add pre-action

Add post action

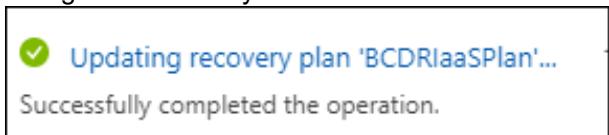
27. On the **Insert action** blade, select **Script** and then provide the name: **ASRWEBFailover**. Ensure that your Azure Automation account is selected and then chose the Runbook name: **ASRWEBFailover**. Select **OK**.



28. Make sure that your **Pre-steps** are running under **All groups failover** and the **Post-steps** are running under the **Group1: Start**. Select **Save**.

STAGE NAME	DETAILS
All groups shut down	2 machines in 1 group.
All groups failover: Pre-steps	1 Step
Script: ASRSQFailover	Script
All groups failover	
Machines	2 Machines
WEBVM1	Machine
WEBVM2	Machine
Replication groups	
Group 1: Start	2 Machines
WEBVMI	Machine
WEBVM2	Machine
Group 1: Post-steps	
Script: ASRWEBFailover	Script

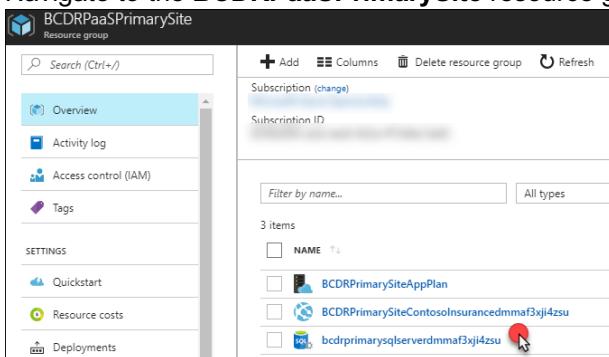
29. After a minute, the portal will provide a successful update notification. This means that your machines are fully configured and ready to Failover and Back between the **Primary** and **Secondary** regions.



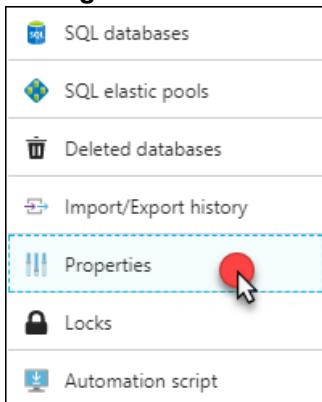
Task 4: Configure PaaS for region to region failover

In this task you will deploy the website to App Services using Visual Studio, migrate a database to Azure SQL Database and configure it for high-availability using an Azure SQL Database Failover Group. The Traffic Manager will be used to direct traffic to the closest front end to the user. If there is a failover of the database it will happen transparently, and the users will never know there was an outage. There is no reconfiguration required for this to function properly.

1. From the **LABVM**, open the Azure portal at: <https://portal.azure.com>
2. Navigate to the **BCDRPaaSPPrimarySite** resource group. Select the SQL Server resource



3. This server will host your SQL Database for the Contoso Insurance Web App. Select **Properties** under the **Settings** area.



4. Copy the name of the SQL Server to notepad. Also, notice that the Server Admin Login is the same. Save this file as **C:\HOL\Deployments\SQLSERVER.txt**. Navigate to this folder using Windows Explorer and right-click and copy the file to your clipboard.

bcdrprimarysqlserverdmmaf3xji4zsu - Properties

STATUS Available

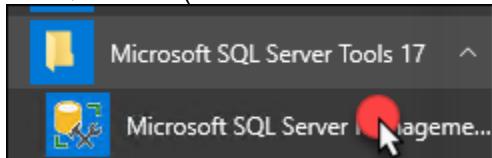
SERVER NAME bcdrprimarysqlserverdmmaf3xji4zsu.database.windows.net

LOCATION East US 2

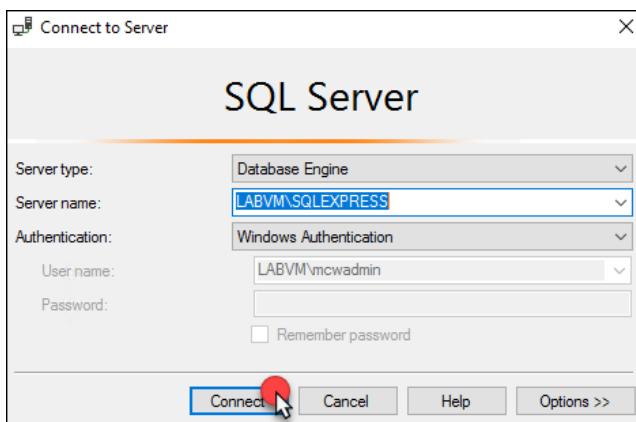
SERVER ADMIN LOGIN mcwadmin

SQL SERVER NAME
bcdrprimarysqlserverdmmaf3xji4zsu.database.windows.net

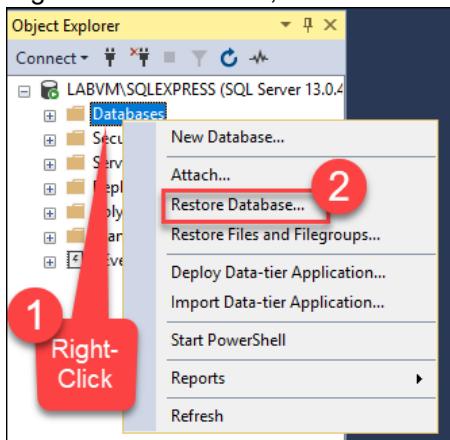
5. Use the Start menu to launch **Microsoft SQL Server Management Studio 17** and connect to the local instance of SQL Server (Located in the Microsoft SQL Server Tools 17 folder)



6. Select **Connect** to Sign On to the Local **SQLEXPRESS** on LABVM



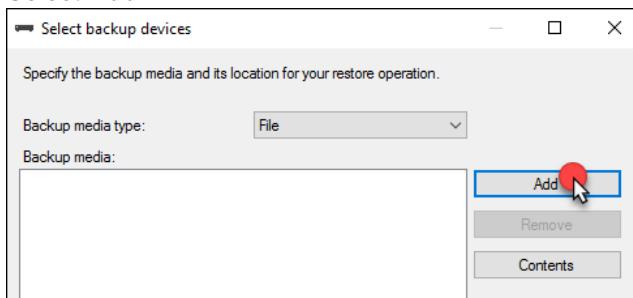
7. Right-click **Databases**, then select **Restore Database**



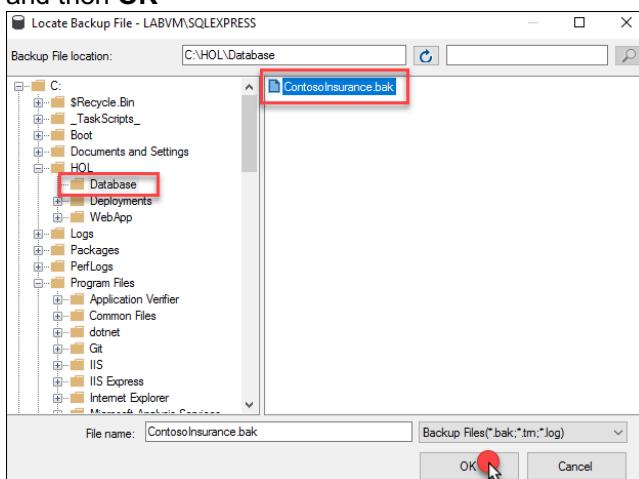
8. Select **Device** and then the **Ellipse**

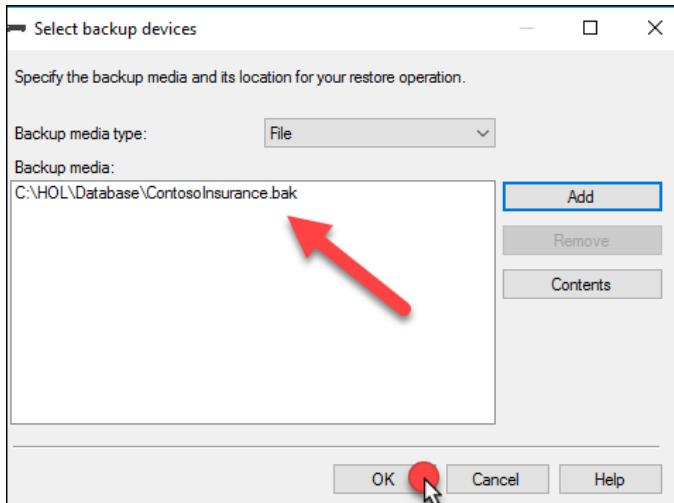
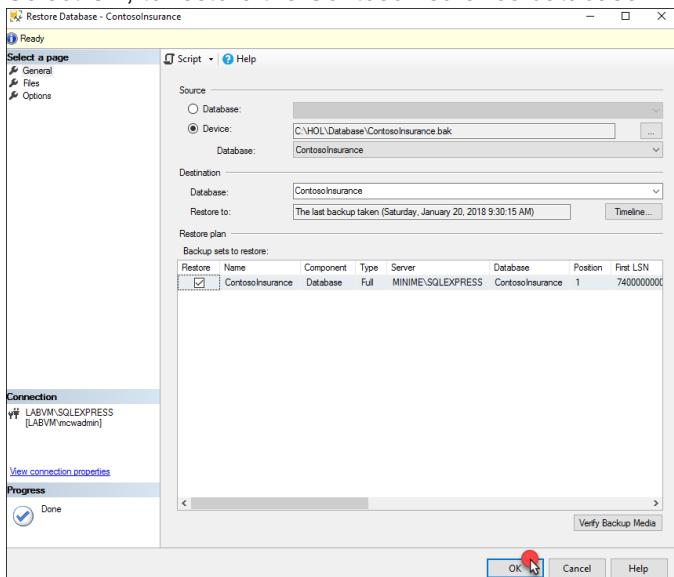
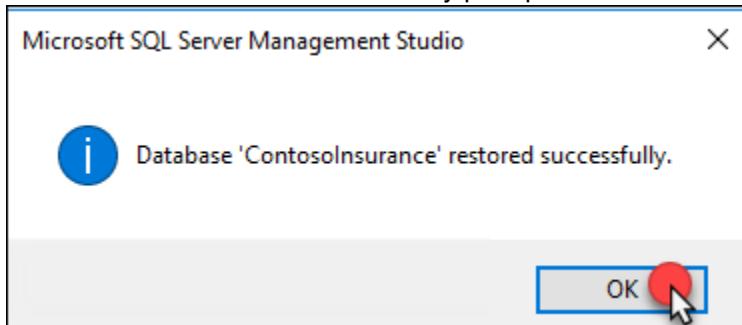


9. Select **Add**

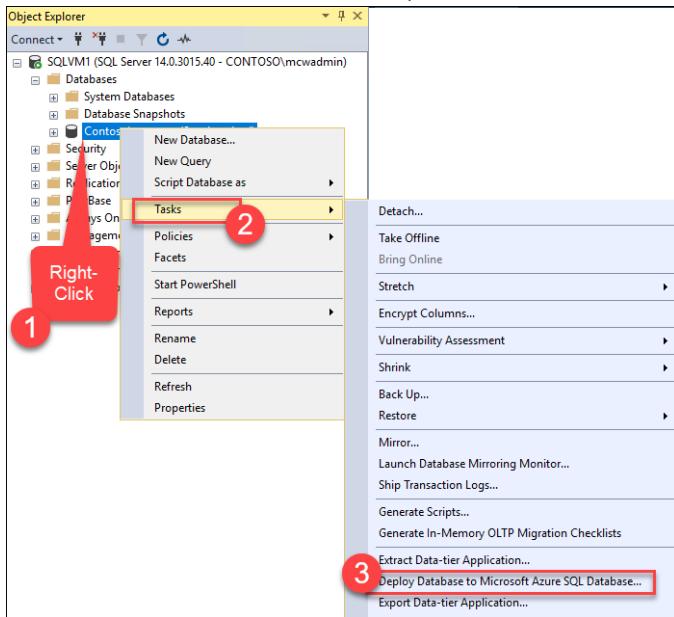


10. Navigate the folder menu and locate the C:\HOL\Database folder and then select on **ContosoInsurance.bak** and then **OK**

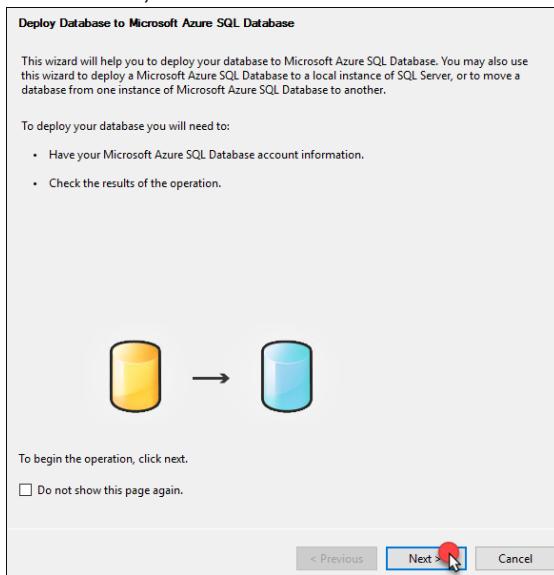


11. Select OK**12. Select OK, to restore the ContosoInsurance database****13. Select OK at the restored successfully prompt**

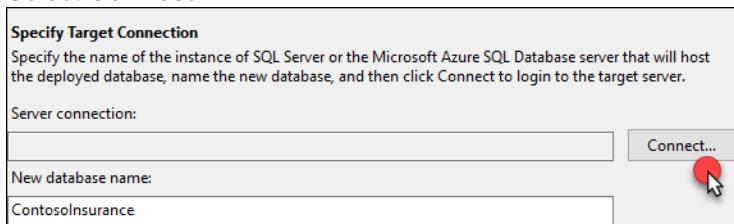
14. Expand Databases and then right-click on the ContosoInsurance database, select Tasks, then Deploy Database to Microsoft Azure SQL Database



15. Select Next, on the Introduction screen

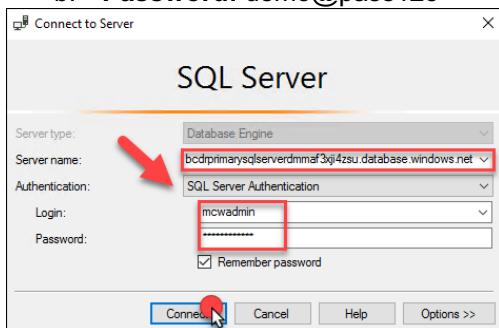


16. Select Connect



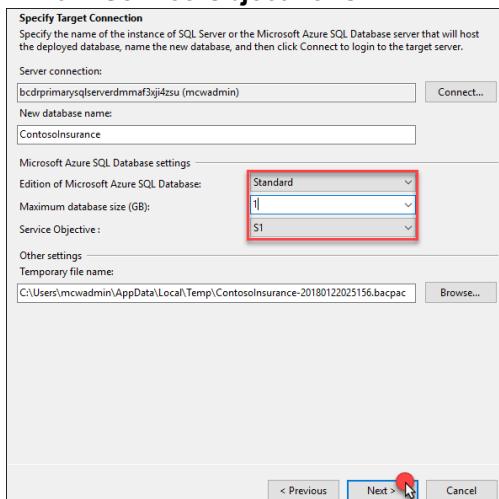
17. In the **Connect to SQL Server** screen, copy the name of your Azure SQL Server from the **SQLSERVER.TXT**. Change the Authentication to **SQL Server Authentication** and enter the credentials for the server then select **Connect**.

- Login:** mcwadmin
- Password:** demo@pass123

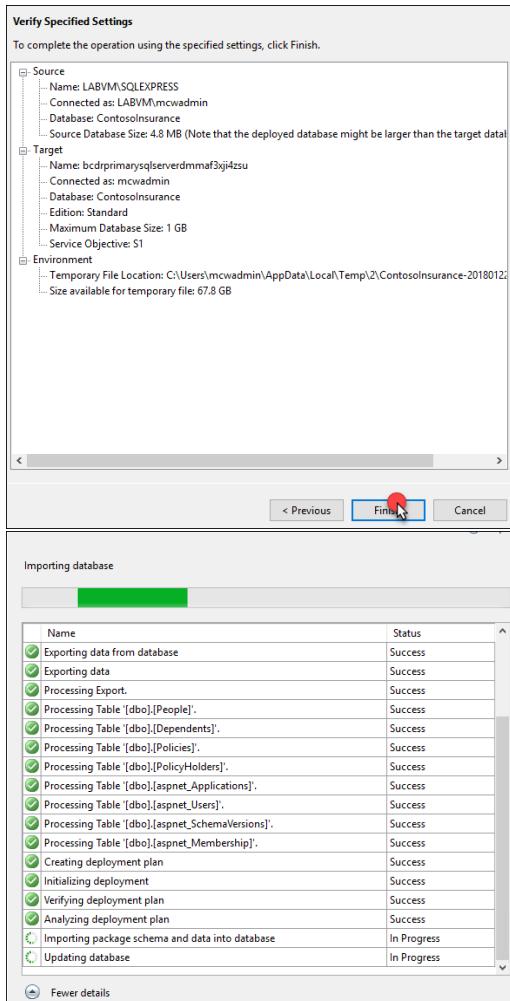


18. Update the remainder of the Deployment Settings screen using these inputs and then select **Next**:

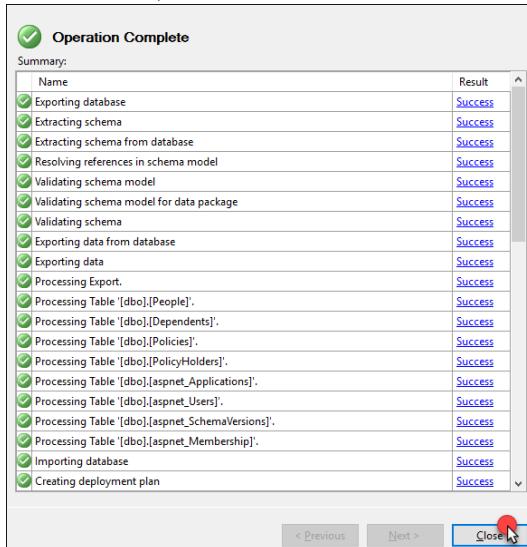
- Edition of Azure SQL database:** Standard
- Maximum database size (GB):** 1
- Service Objective:** S1



19. Select **Finish and allow the Database to be migrated to Azure**



20. Select **Close, once the database has been migrated to Azure SQL Database**



21. Move back to the Azure portal on **LABVM**. Open the **BCDRPaaSPrimarySite** resource group and notice that there is a new SQL Database called **ContosoInsurance**

BCDRPaaSPrimarySite
Resource group

Search (Ctrl+ /)

Subscription (change) Subscription ID

Overview Activity log Access control (IAM) Tags

SETTINGS Quickstart Resource costs Deployments Policies

NAME ↑

- BCDRPrimarySiteAppPlan
- BCDRPrimarySiteContosoInsuredmmaf3xji4zsu
- bcdrprimarysqlserverdmmaf3xji4zsu
- ContosoInsurance**

22. Select **ContosoInsurance** to open the resource then select **Show database connection strings**

Resource group (change) BCDRPaaSPrimarySite	Server name bcdrprimarysqlserverdmmaf3xji4zsu.database.windows.net
Status Online	Elastic database pool No elastic pool
Location East US 2	Connection strings Show database connection strings

23. Select the **Copy to clipboard** link to capture the connection string and then paste it to your **SQLSERVER.TXT** file

ADO.NET JDBC ODBC PHP

ADO.NET (SQL authentication)

Copied

[your_username];Password=[
[your_password];MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;

SQL SERVER - Notepad

File Edit Format View Help

SQL SERVER NAME
bcdrprimarysqlserverdmmaf3xji4zsu.database.windows.net

ContosoInsurance Connection string

Server=tcp:bcdrprimarysqlserverdmmaf3xji4zsu.database.windows.net

24. In the Azure portal, move back to the **BCDRPaaSPrimarySite** resource group and then select the **SQL Server** resource

The screenshot shows the Azure portal's resource group overview for 'BCDRPaaSPrimarySite'. On the left, a sidebar lists options like Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, and Policies. The main pane displays a list of resources under '4 items'. One resource, 'bcdrprimarysqlserverdmmaf3xji4zsu', is highlighted with a red box.

25. Under **Settings**, select **Failover groups**

The screenshot shows the 'bcdrprimarysqlserverdmmaf3xji4zsu' SQL server settings page. The left sidebar includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Quick start', 'Firewall / Virtual Networks ...', and 'Failover groups'. The 'Failover groups' option is highlighted with a red box.

26. Select **+Add group**

The screenshot shows the 'Failover groups' creation page for the 'bcdrprimarysqlserverdmmaf3xji4zsu' SQL server. The top bar shows the title 'bcdrprimarysqlserverdmmaf3xji4zsu - Failover groups'. The left sidebar has the same options as the previous screenshot. The main area contains a 'NAME' input field and a note 'Failover group are a SQL serv'. A large red circle highlights the '+Add group' button.

27. Complete the **Failover group** blade using these inputs and then select **Create**:

- Failover group name:** enter a lowercase unique name 3-24 characters using bcdrpasfogxxx
- Secondary Server:** select the secondary SQL Server from your BCDRPaasSecondarySite
- Database within the group:** Contosolnsurnace

Failover group		Databases for failover group
Create a failover group to automatically failover databases in it. * Failover group name: bcdrpasfog8675309 * Secondary server: bcdrsecondarysqlserverfcumtoavifg6		Select all Filter items... NAME Contosolnsurnace
Read/Write failover policy: Automatic Read/Write grace period (hours): 1 hours		Summary Databases on secondary (excluding ones in Elastic Pools) Elastic Pools on secondary server
Database within the group Select databases to add		Monthly cost

28. The portal will submit a deployment

*** Deployment in progress...

Deployment to resource group 'BCDRPaasPrimarySite' is in progress.

29. The portal will update once the Failover group has been deployed. Select the **group**

Failover group are a SQL server feature designed to automatically manage replication, connectivity and failover between primary and secondary servers.		
NAME	PRIMARY SERVER	PARTNER SECONDARY SERVER
bcdrpasfog8675309	bcdrprimarysqlserverdmmaf3xj4zsu	bcdrsecondarysqlserverfcumtoavifg6

30. The Failover group (FOG) portal will appear. Copy the name of the Listener endpoint to your clipboard and then copy this to your **SQLSERVER.TXT** file.

The screenshot shows the Failover Group (FOG) portal interface. At the top, there's a navigation bar with 'Save', 'Discard', 'Add databases', 'Edit configuration', 'Remove databases', 'Failover', 'Forced Failover', and 'Delete' buttons. Below the navigation bar, there are tabs for 'Configuration details', 'Databases within group', 'Databases selected to be added (0)', and 'Databases selected for removal (0)'. The main area features a world map with a connection line between two locations. Below the map is a table with the following data:

SERVER	ROLE	READ/WRITE FAILOVER POLICY	GRACE PERIOD
bcdrprimarysqlserverdmmaf3xji4zs (East U...)	Primary	Automatic	1 hours
bcdrsecondarysqlserverfcumtoavifg6 (Cen...	Secondary		

Below the table, there are sections for 'Read/write listener endpoint' and 'Read-only listener endpoint'. The 'Read/write listener endpoint' section contains the endpoint 'bcdrpassfog8675309.database.windows.net' with a copy icon. The 'Read-only listener endpoint' section contains the endpoint 'bcdrpassfog8675309.secondary.database.windows.net' with a copy icon. At the bottom, there's a 'SQLSERVER - Notepad' window showing the following text:

```
SQL SERVER NAME  
bcdrprimarysqlserverdmmaf3xji4zs.database.windows.net  
  
FOG LISTNER ENDPOINT  
bcdrpassfog8675309.database.windows.net  
  
ContosoInsurance Connection string  
  
Server=tcp:bcdrprimarysqlserverdmmaf3xji4zs.database.windows.net
```

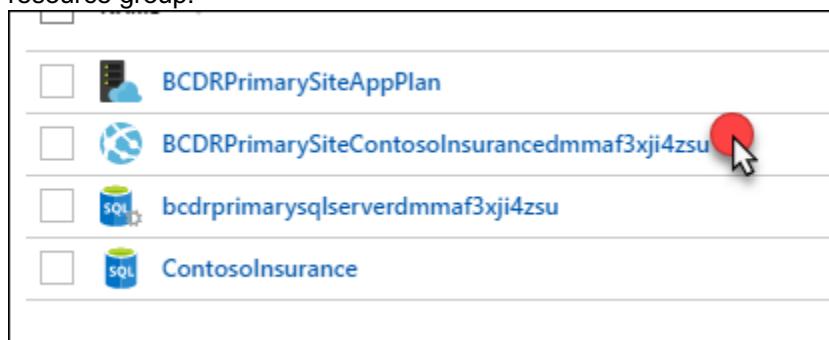
A red arrow points to the 'bcdrpassfog8675309.database.windows.net' entry in the 'FOG LISTNER ENDPOINT' section of the Notepad window.

31. In the **SQLSERVER.TXT** file, update the server name in the connection string with the name of the FOG listener endpoint. Also, change the user name and password to the credentials for the SQL Server:
- Username:** mcwadmin
 - Password:** demo@pass123

BEFORE	Server=tcp:bcdrprimarysqlserverdmmaf3xji4zsu.database.windows.net,1433
AFTER	Server=tcp:bcdrpassfog8675309.database.windows.net,1433;Initial Catalog

BEFORE	User ID={your_username};Password={your_password};MultipleAct
AFTER	User ID=mcwadmin;Password=demo@pass123;MultipleAct

32. The new connection string will be used for the Web App. This will ensure that when the SQL Database is failed over that the server is always pointing to the Failover group. Open the Web App in the **BCDRPaaSPrimarySite** resource group.



33. Select the **URL**. The empty Web App will appear

Resource group ([change](#))
BCDRPaaSPrimarySite

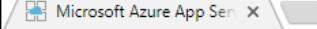
Status
Running

Location
East US 2

OS name
Windows Server 2016

URL
<https://bcdrprimarysitecontosoinsuredmmaf3xji4zsu.azurewebsites.net>

App Service plan/pricing tier
BCDRPrimarySiteAppPlan (Standard: 1 Small)

 Microsoft Azure App Service

Secure | <https://bcdrprimarysitecontosoinsuredmmaf3xji4zsu.azurewebsites.net>

Microsoft Azure

Your App Service app is up and running

Go to your app's [Quick Start](#) guide in the Azure portal to get started or read documentation.

34. Under **Settings**, select **Application Settings**

SETTINGS

-  Application settings
-  Authentication / Authorization
-  Managed service identity
-  Backups
-  Custom domains
-  SSL certificates

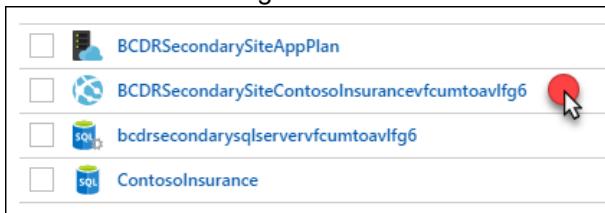
35. Scroll down to the **Connection strings** settings and add a new connection string using the following inputs, then select **Save**.

- Name:** PolicyConnect
- Value:** Paste in the updated string you created with the Failover group name from the SQLSERVER.TXT file

Connection strings	
PolicyConnect	Server=tcp:bcdrpassfog8675309.database.windows.net,143... SQL Database

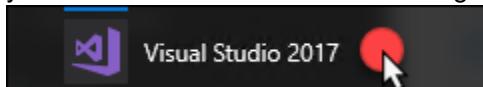
Note: You must use the Name **PolicyConnect**. This is the name that the Application in the source code.

36. Repeat the same procedure on the Web App located in the **BCDRPaaSSecondarySite** resource group using the same connection string:

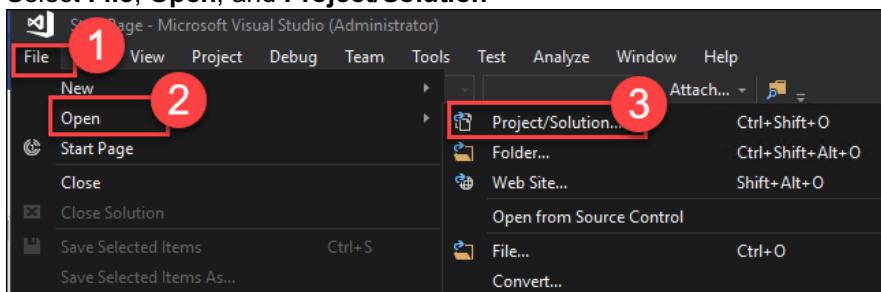


- Name:** PolicyConnect
- Value:** Paste in the updated string you created with the Failover group name from the SQLSERVER.TXT file.

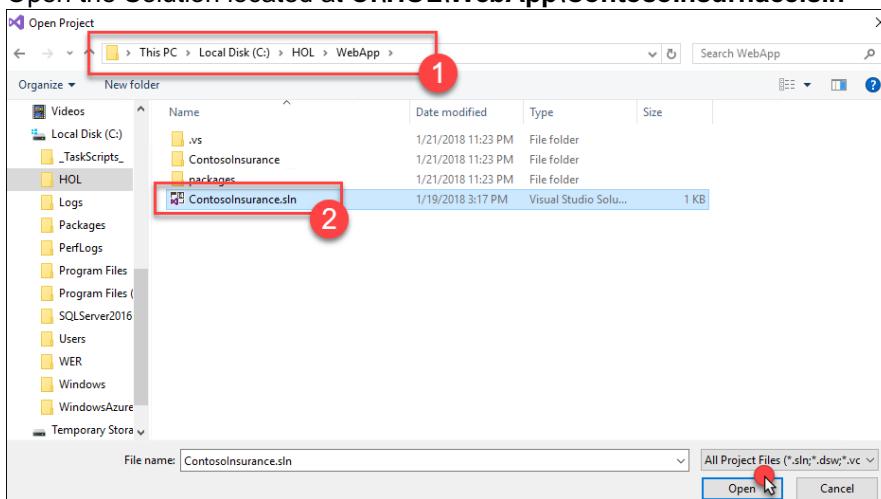
37. On the LABVM open **Visual Studio**. You will be required to login to Visual Studio. If you don't have an account you can create a free account following the prompts.



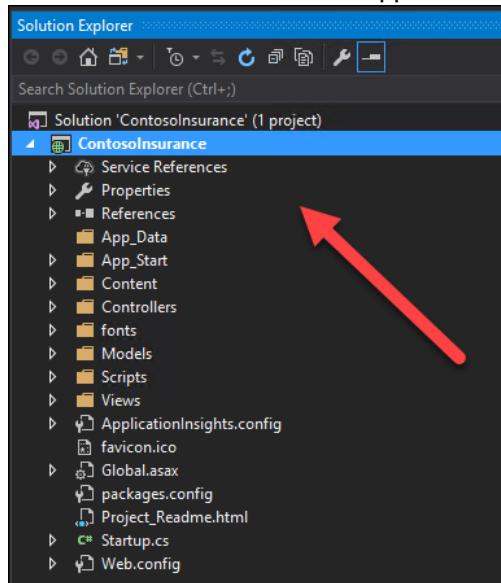
38. Select **File, Open, and Project/Solution**



39. Open the Solution located at **C:\HOL\WebApp\ContosolInsurnace.sln**

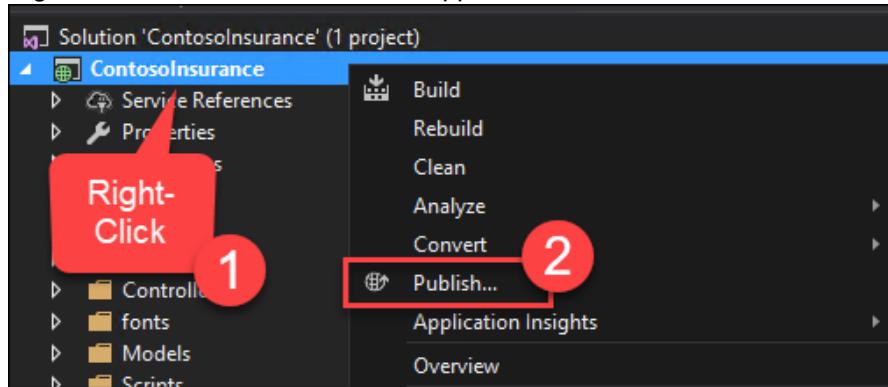


40. Locate the ContosoInsurance application in the Solution Explorer on the right-hand area of Visual Studio

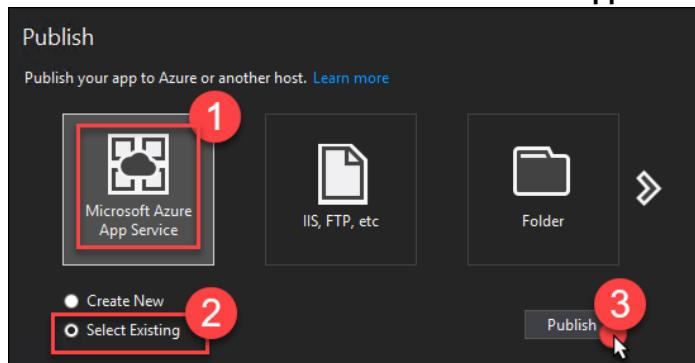


Note: If for some reason the Solution Explorer is not seen you can select **View -> Solution Explorer** on the Menu bar of Visual Studio.

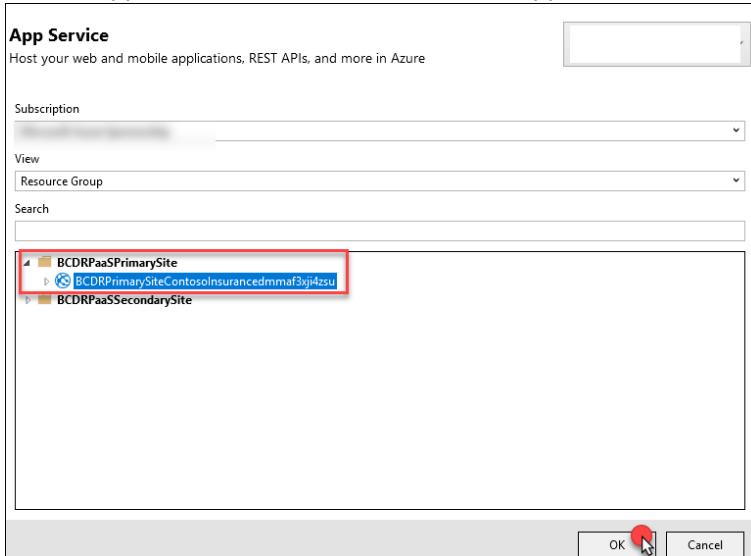
41. Right-click the **ContosoInsurance** Application and select **Publish**



42. On the **Publish** screen select **Microsoft Azure App Service** and then **Select Existing** and finally **Publish**



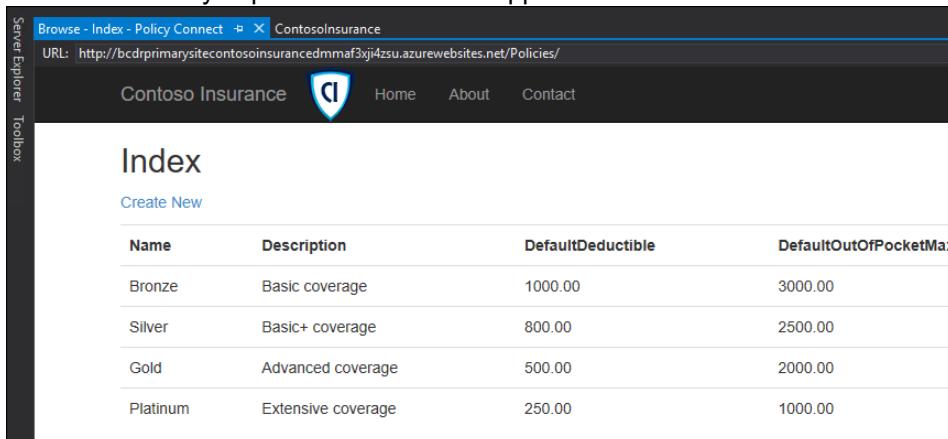
43. On the App Service screen select the Web App under the **BCDRPaaSPrimarySite**. Then select **OK**.



44. Visual Studio will build the app and then publish to your Web App. The browser should open to the application.



45. Select the **Current Policy Offerings** button, and the page should load with data showing. This means that you have successfully implemented the Web App and it has connected to the Failover Group database.



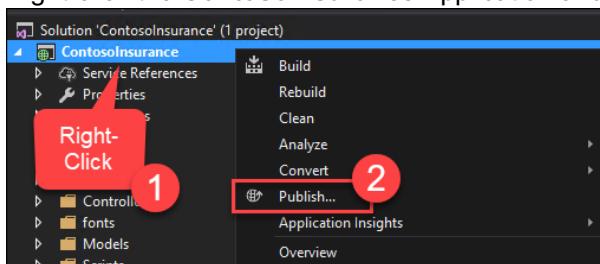
Name	Description	DefaultDeductible	DefaultOutOfPocketMax
Bronze	Basic coverage	1000.00	3000.00
Silver	Basic+ coverage	800.00	2500.00
Gold	Advanced coverage	500.00	2000.00
Platinum	Extensive coverage	250.00	1000.00

46. Close Visual Studio

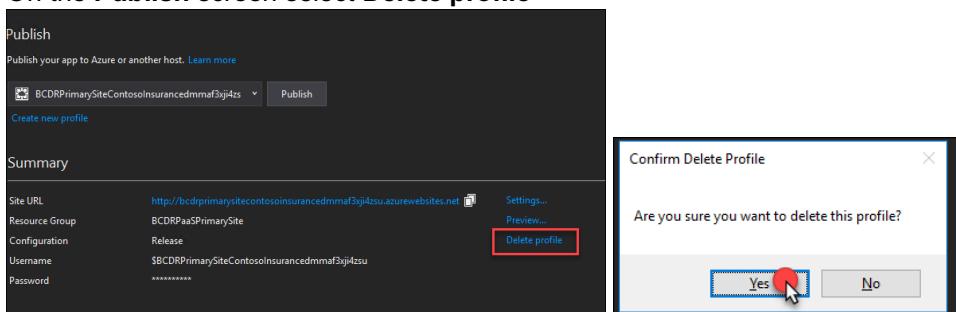
47. Start Visual Studio

48. Re-open the **ContosoInsurance.sln** Solution

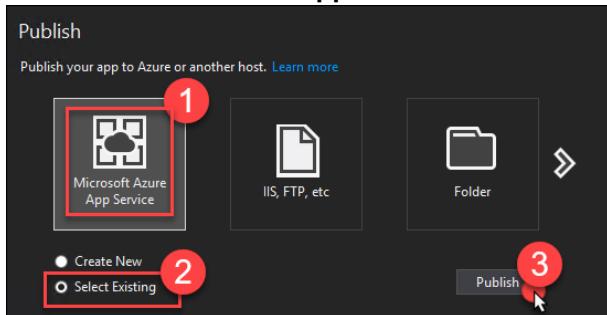
49. Right-click the **ContosoInsurance** Application and select **Publish**



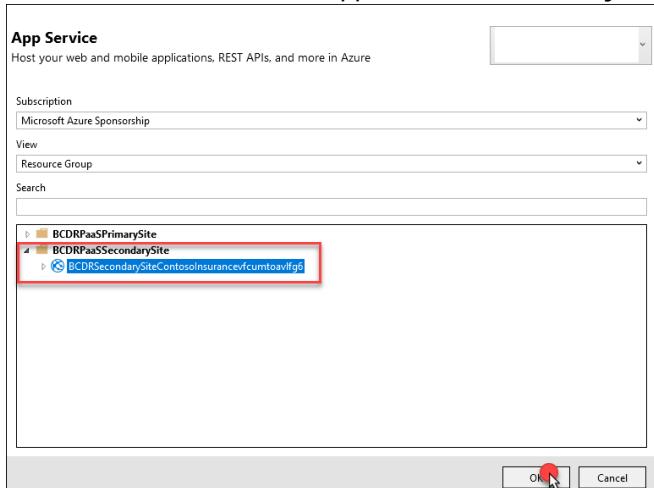
50. On the **Publish** screen select **Delete profile**



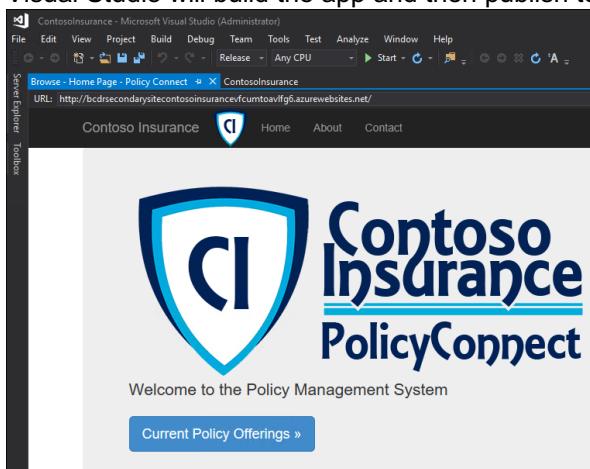
51. Select **Microsoft Azure App Service** and then **Select Existing** and finally **Publish**



52. This time choose the Web App from the **Secondary** Site running in the **BCDRPaaSSecondarySite**. Select OK.



53. Visual Studio will build the app and then publish to your Web App. The browser should open to the application.



54. Select the **Current Policy Offerings** button, and the page should load with data showing. This means that you have successfully implemented the Web App, and it has connected to the Failover Group database.

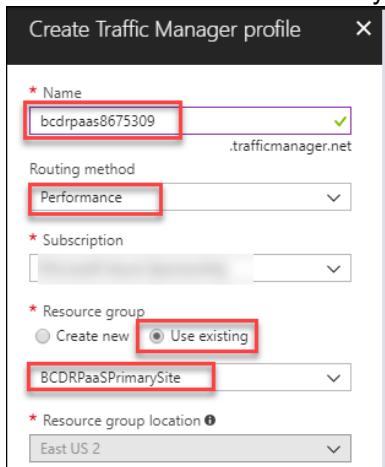
The screenshot shows a Microsoft Visual Studio interface with a browser window titled "ContosoInsurance - Microsoft Visual Studio (Administrator)". The browser URL is "http://bcdrsecondarysitecontosoinsurancefcumtoavlg6.azurewebsites.net/Policies/". The page content is the "Index" of policy offerings for Contoso Insurance, listing five categories: Bronze, Silver, Gold, and Platinum, each with a description and default deductible amount. The page footer includes a copyright notice for 2018.

55. Close Visual Studio and move back to the Azure Portal. The next step will be to deploy a Traffic Manager for this PaaS implementation. Select **+NEW, Networking** then **Traffic Manager profile** in the Azure portal.

The screenshot shows the Azure Portal's left sidebar with a "New" button highlighted by a red circle labeled "1". The main area displays the "Networking" category under the "Azure Marketplace" section, with the "Traffic Manager profile" option highlighted by a red box and red circle labeled "3". Other networking services like Virtual network, Load Balancer, Application Gateway, and Virtual network gateway are also listed.

56. Complete the **Create Traffic Manager profile** using the following inputs, then select **Create**:

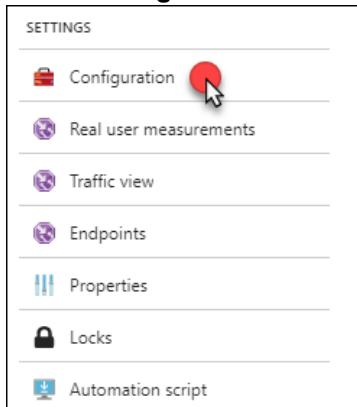
- Name:** unique name all lowercase using bcdrpaa\$xxx
- Routing method:** Performance
- Resource group:** Use existing / BCDRPaa\$PrimarySite
- Location:** automatically assigned based on the BCDRPaa\$PrimarySite



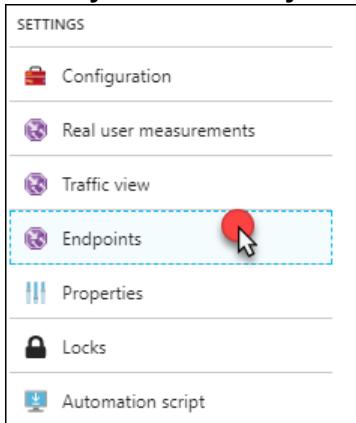
57. Once the Traffic Manager profile is created, open it in the Azure portal. Notice the DNS name. This is the URL that you will use to connect to the application. Once configured this DNS name will always respond and doesn't matter which location is responding or where if the current primary database is located. Since the **Performance** routing method was selected the closest site to the end users will be calculated and they will be sent to that location. If for some reason one of the sites is down the other will service all requests.

Resource group (change) BCDRPaa\$PrimarySite	DNS name http://bcdrpaa\$8675309.trafficmanager.net
Status Enabled	Monitor status Inactive
Subscription name (change)	Routing method Performance
Subscription ID	

58. Select **Configuration** and review the configurations



59. Next select **Endpoints**. This is where you will configure the two external load balancers that are located your **Primary** and **Secondary** sites.



60. Select **+Add**

61. Complete the **Add endpoint** using the following inputs and then select **OK**

62. Complete the **Create Traffic Manager profile** using the following inputs, then select **Create**:

- Name:** unique name all lowercase using bcdrpaaaxxx
- Routing method:** Performance
- Resource group:** Use existing / BCDRPaaSPrimarySite
- Location:** automatically assigned based on the BCDRPaaSPPrimarySite

63. Once the Traffic Manager profile is created, open it in the Azure portal. Notice the DNS name. This is the URL that you will use to connect to the application. Once configured, this DNS name will always respond and doesn't matter which location is responding or where if the current primary database is located. Since the **Performance**

routing method was selected the closest site to the end users will be calculated, and they will be sent to that location. If for some reason one of the sites is down the other will service all requests.

Resource group (change) BCDRPaaSPrimarySite	DNS name http://bcdrpaas8675309.trafficmanager.net
Status Enabled	Monitor status Inactive
Subscription name (change)	Routing method Performance
Subscription ID	

64. Select Configuration and review the configurations

65. Select+Add. Notice that the Primary endpoint was created as “Enabled”

66. Complete the Add endpoint using the following inputs and then select OK:

- Type: Azure endpoint
- Name: BCDRPaSSecondarySite
- Target resource type: App Service
- Target resource: Choose an app service
- Resource: BCDRPrimarySiteContosolsurance... in the BCDRPaasPrimarySite

67. Once the second endpoint has been added select Overview. The Traffic Manager will monitor the Endpoints and if the Primary or Secondary site moves to a Monitor Status of Degraded, then the Traffic Manager will direct traffic only to the other site until the service is restored. The current Monitor Status shows that the Primary site and the Secondary site are Online. If there was an outage at the web layer for one of these sites then the site will move to Degraded, and the other site will service all requests.

NAME	STATUS	MONITOR STATUS	TYPE	LOCATION
BCDRPaaSPrimarySite	Enabled	Online	Azure endpoint	East US 2
BCDRPaaSSecondarySite	Enabled	Online	Azure endpoint	Central US

Note: All of this is automatic and easily configured with a vanity domain by adding a C NAME record in DNS to point to the DNS name of the Traffic manager. This would allow for a site like www.contoso.com to resolve to the DNS name of the traffic manager. The users will never know that the site is failed over or failed back as long as one site is up and the database is active in the Failover group.

68. Select the DNS name of the Traffic manager the Policy Connect web application will load. This is connecting to one of the two Web Apps running in the **Primary Site** or **Secondary Site** and talking to the Azure SQL Database Failover Group primary replica using the SQL FOG Listener.

Resource group (change)
BCDRPaaSPrimarySite
Status
Enabled
Subscription name (change)

DNS name
<http://bcdrpaa8675309.trafficmanager.net>

Monitor status
Online
Routing method
Performance

Contoso Insurance Home About Contact

Welcome to the Policy Management System

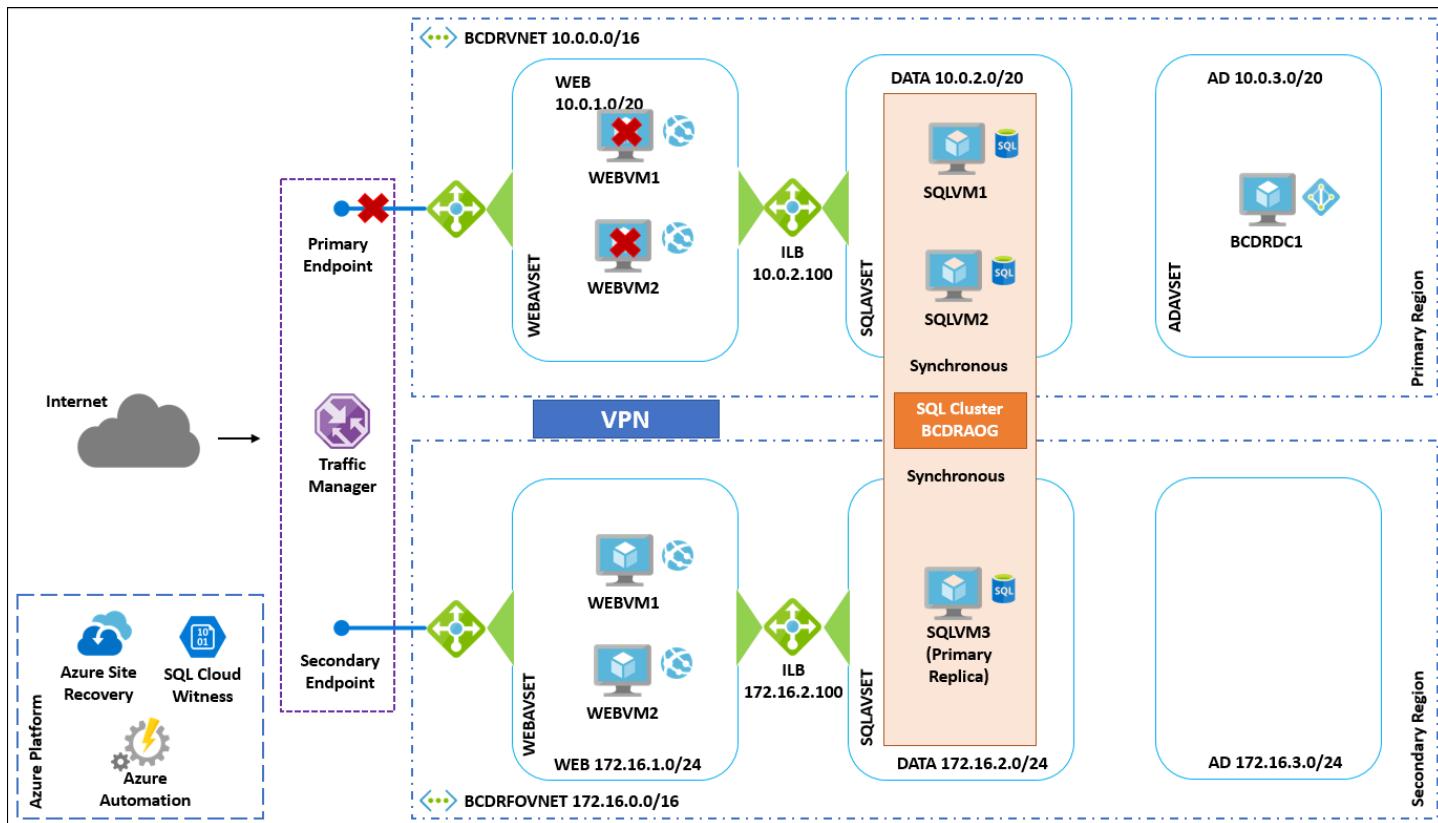
Current Policy Offerings »

Exercise 4: Simulate failovers

Duration: 75 minutes

Now, that your applications have been made ready for high-availability and BCDR you will now simulate their capabilities. First, you will Failover the **Azure IaaS environment** from your **Primary** to **Secondary** Region. Next, you will migrate the **On-Premises** environment to Azure. The **PaaS** environment will be tested to ensure that failing over the database doesn't cause an outage to the application. Finally, you will fallback the Azure IaaS environment from the **Secondary** site to the **Primary** site.

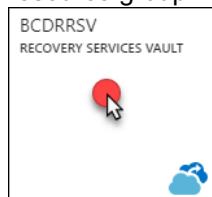
Task 1: Failover Azure IaaS region to region



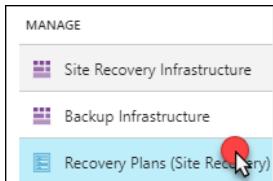
1. Using the Azure portal, open the **BCDRIaaSPrimarySite** resource group. Locate the Traffic Manager DNS URL and select it to ensure that the application is up and running from the Primary Site. Pin the Traffic manager to your dashboard for easy access to this URL or make a favorite in your browser.



2. From the Azure portal, open the **BCDRRSV** Recovery Services Vault located in the **BCDRAzureSiteRecovery** resource group



3. Select **Recovery Plans (Site Recovery)** in the **Manage** area



4. Select BCDRlaaSPlan

NAME	SOURCE	TARGET
BCDRlaaSPlan	East US 2	Central US

5. Select More and then Failover

6. On the warning about No Test Failover, select I understand the risk, Skip test failover

7. Review the Failover direction. Notice that From is the Primary site, and To is the Secondary site. Select OK.

8. After the Failover is initiated close the blade and move to **Jobs, then **Site Recovery Jobs**. Select the **Failover** job to monitor the progress.**

The screenshot shows a table titled "Site Recovery jobs" under the heading "BCDRRSV". The columns are "NAME", "STATUS", "TYPE", and "ITEM". A single row is visible: "Failover" with status "In progress", type "Recovery plan", and item "BCDRIaaSPlan". A red circle highlights the "In progress" status icon.

9. You can monitor the progress of the Failover from here

The screenshot shows the "Properties" section of a Site Recovery Job. It includes fields for "Vault" (BCDRRSV), "Recovery plan" (BCDRIaaSPlan), "Job id" (ca78dd33-bc8e-40d9-ae27-4f76f764869d-2018-01-1), "Source" (East US 2), and "Target" (Central US). Below this is the "Job" section, which lists the status of tasks: "Prerequisites check for the recovery plan" is successful, and "All groups shutdown (1)" and "Shutdown: Group 1 (2)" are both in progress.

Note: Do not make any changes to your VMs in the Azure portal during this process. Allow ASR to take the actions and wait for the failover notification prior to moving on to the next step. You can open another portal view in a new browser tab and review the output of the Azure Automation Jobs, by opening the jobs and selecting Output.

The screenshot shows the output of an Azure Automation job named "ASRSQLFailover" run on 1/19/2018 at 12:34 PM. The output pane displays PowerShell command logs. Key configuration parameters shown include:

```

$PComputerName : localhost
$PSourceJobInstanceId : b9ed0a1-62f3-401f-858c-314ff955c30
$Environment : (AzureCloud, AzureGlobalNetwork)
$Context : Microsoft.Azure.Commands.Profile.Models.PSAzureContext
Selecting Azure subscription...
$PComputerName : localhost
$PSourceJobInstanceId : b9ed0a1-62f3-401f-858c-314ff955c30
$Region : CentralUS
$Environment : AzureCloud
$Subscription : f835e049-cdc4-4a3b-922e-f77346a5a65
$Tenant : a974dc1-2c13-4a4b-91ec-ddeaf6a85e8
Configurations used by this Runbook for the failover...
$SecondarySqlPath : $SQLServer\1\SqL50\W3\Default\AvailabilityGroups\URDB000
$PrimarySqlPath : $SQLServer\1\SqL50\W3\Default\AvailabilityGroups\URDB000
$SecondarySiteQVMName : RDRB000SecondarySite
$PrimarySiteQVMName : SQL01
$SecondarySiteQVMIP : 10.0.0.4
$PrimarySiteQVMPort : 3389
$PComputerName : localhost
$PSourceJobInstanceId : b9ed0a1-62f3-401f-858c-314ff955c30
Determining if Failover or Fallback...

```

10. Once the job has finished, it should show as successful for all tasks

Job	
NAME	STATUS
Prerequisites check for the recovery plan	Successful
▼ All groups shutdown (1)	Successful
Shutdown: Group 1 (2)	Successful
▼ All groups failover: Pre-steps (1)	Successful
Script on recovery side: ASRSQFailover	Successful
▼ Recovery plan failover	Successful
webvm1	Successful
webvm2	Successful
▼ Group 1: Start (2)	Successful
webvm1	Successful
webvm2	Successful
▼ Group 1: Post-steps (1)	Successful
Script on recovery side: ASRWEBFailover	Successful
Finalizing the recovery plan	Successful

11. There is also details of the failover VMs shown. Notice how they are running the **BCDRFOVNET**. This is the failover Virtual Network running in the **Secondary Site**.

Environment Details		
BCDRIaaSPlan		
VIRTUAL MACHINE	NETWORK\SUBNET	RECOVERY POINT
WEBVM1	bcdrfovnet\WEB	1/22/2018, 10:52:12 AM
WEBVM2	bcdrfovnet\WEB	1/22/2018, 10:53:24 AM

12. Select **Resource groups** and select **BCDRIaaSPrimarySite**. Locate the **WEBVM1** in the resource group and select to open.

The screenshot shows the Azure Resource Groups blade for the 'BCDRIaaSPrimarySite' resource group. The left sidebar has 'Overview' selected. The main area displays a list of resources with their names and icons. The 'WEBVM1' resource is highlighted with a red circle around its name.

NAME
WWWEXTLB-PIP
WWWEXTLB
WEBVM2-NIC
WEBVM2
WEBVM1-NIC
WEBVM1

13. Notice that it currently shows as **Status: Stopped (deallocated)**. This shows that failover has stopped the VMs at the **Primary** site.

WEBVM1
Virtual machine

Search (Ctrl+ /) Connect Start Restart Stop

Resource group (change)
BCDRIaaSPrimarySite

Status
Stopped (deallocated)

Activity log

Access control (IAM)

Location
East US 2

Note: Do not select Start! This is a task only for ASR.

14. Move back to the Resource group and select the **WWWEXTLB-PIP** Public IP address. Copy the DNS name and paste it into a new browser tab.

WWWEXTLB-PIP
Public IP address

Search (Ctrl+ /) Associate Dissociate Move Delete

Overview Activity log Access control (IAM) Tags

Resource group (change)
BCDRIaaSPrimarySite

IP address
40.70.6.46

DNS name
bcdrprimarysitelbasedyfizo7bpce.eastus2.cloudapp.azure.com

Associated to
WWWEXTLB

15. The site will be unreachable at the Primary location

16. In the Azure portal, move to the **BCDRIaaSSecondarySite** resource group. Locate the **WEBVM1** in the resource group and select to open.

BCDRIaaSSecondarySite
Resource group

Search (Ctrl+ /) Add Columns Delete reso

Overview Activity log Access control (IAM) Tags

SETTINGS

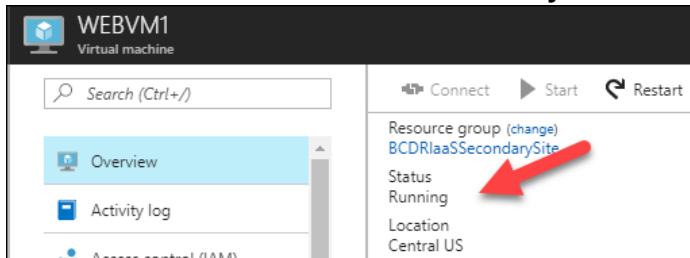
Quickstart Resource costs Deployments Policies Properties

Filter by name...

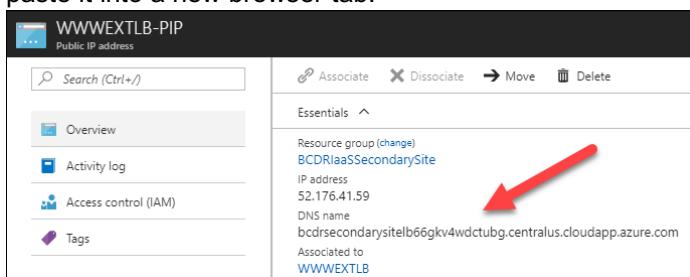
18 items

NAME
WWWEXTLB-PIP
WWWEXTLB
WEBVM249db6bbf-0793-49e
WEBVM
WEBVM1e2333c8e-6837-469f
WEBVM1

17. Take note that the **WEBVM1** in the **Secondary** site is running



18. Move back to the Resource group and select the **WWWEXTLB-PIP** Public IP address. Copy the DNS name and paste it into a new browser tab.



19. The Application running on the WEBVM1 and WEBVM2 is now responding from the **Secondary** Site. Make sure to select the current Policy Offerings to ensure that there is connectivity to the SQL Always On group that was also failed over in the background.

The image contains two screenshots of a web browser displaying the 'Contoso Insurance PolicyConnect' application.

Top Screenshot: Shows the homepage of the application. It features a large blue and white shield logo on the left, followed by the text 'Contoso Insurance PolicyConnect' and 'Welcome to the Policy Management System'. Below this is a blue button labeled 'Current Policy Offerings >'.

Bottom Screenshot: Shows the 'Index' page. At the top, there is a navigation bar with links for 'Home', 'About', and 'Contact'. Below this is a section titled 'Create New'. A table lists four policy offerings:

Name	Description	DefaultDeductible
Bronze	Basic coverage	1000.00
Silver	Basic+ coverage	800.00
Gold	Advanced coverage	500.00
Platinum	Extensive coverage	250.00

20. Using the Azure portal to locate the **BCDRaaS Traffic Manager** profile in the **BCDRaaSPrimarySite** resource group. Notice that the Monitor Status has moved to **Degraded** for the **Primary Site** and moved to **Online** for the **Secondary site**.

NAME	STATUS	MONITOR STATUS	TYPE	PRIORITY
BCDRaaSPrimarySiteB	Enabled	Degraded	Azure endpoint	1
BCDRaaSSecondarySiteLB	Enabled	Online	Azure endpoint	2

21. Select **DNS Name URL**. The site load immediately and is failed over. The users will always be using this DNS URL, so they there is no change in how they access the site even though it is failed over. There **will** be downtime as the failover happens, but once the site is back online the experience for them will be no different than when it is running in the **Primary site**.

Option task: If you wish you can RDP to **SQLVM3** and open the SQL Management Studio to review the Failed over **BCDRAOG**. You will see that **SQLVM3** which is running the **Secondary** site is now the Primary Replica.

22. Now, that you have successfully failed over you need to prep ASR for the Failback. Move back to the **BCDRSRV** Recovery Service Vault using the Azure portal. Select Recovery Plans on the ASR dashboard.

23. The BCDRlaaSPlan will show as **Failover completed**. Select the Plan

NAME	SOURCE	TARGET	CURRENT JOB
BCDRlaaSPlan	East US 2	Central US	Failover completed

24. Notice that now 2 VMs are show in the Target

Source	Target
0	2

25. Select **More**, then select **Re-protect**

- ... More
- Failover
- Re-protect (highlighted)
- Commit
- Delete

26. On the **Re-protect** screen review the configuration and then select **OK**

Re-protect
BCDRlaaSPlan

centralus to eastus2

Resource group, Network, Storage and Availability sets

By default, Site Recovery will pick the original source resource group, virtual network, storage accounts and availability sets above to change the configuration. The resources created are appended with "asr" suffix.

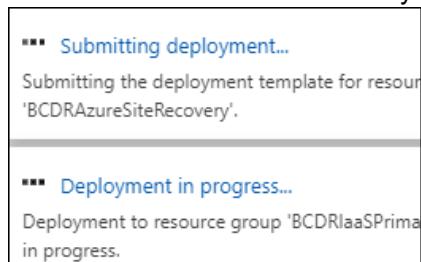
Target resource group BCDRlaaSPrimarySite

Target virtual network BCDRVNet

Target storage accounts (new) bcdrstorageaseasedcacheasr1 bcdrstorageasedyfizo7bpc

Target availability sets WEBAVSET

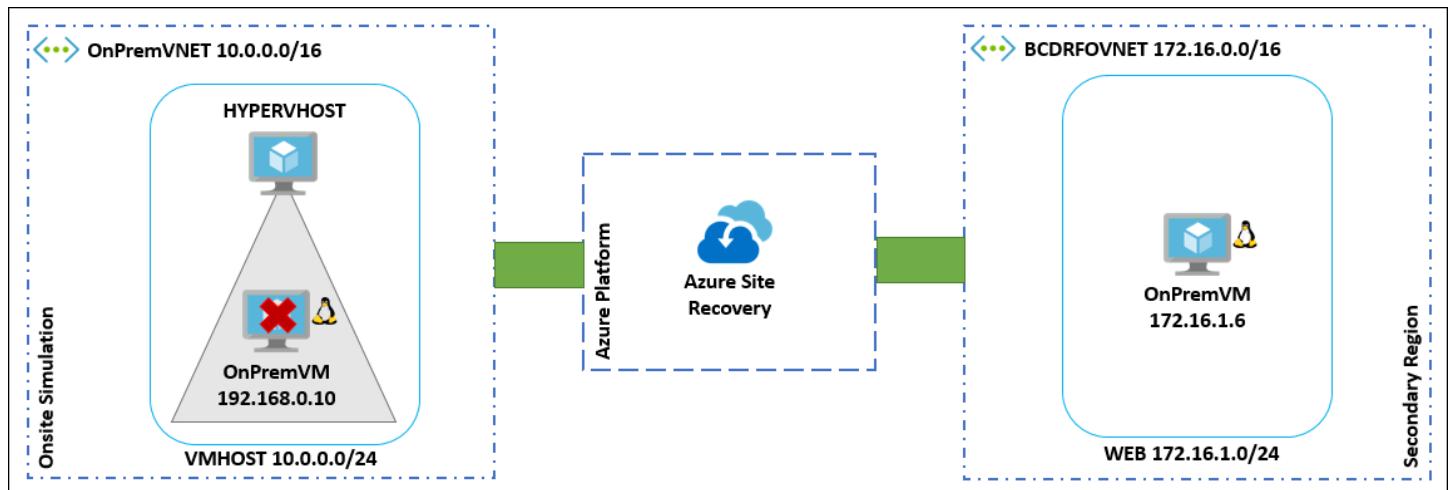
27. The portal will submit a deployment. This process will take some time, by first committing the failover and then synchronizing the WEBVM1 and WEBVM2 back to the Primary Site. Once this process is complete, then you will be able to Fail back to the Primary.



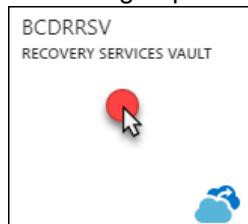
Note: You will perform the Failback later in the HOL, so it is safe to move on to the next task. You can check the status of the Re-protect using the Jobs, Site Recovery Jobs area of the BCDRSRV.

Site Recovery jobs BCDRRSV				
▼ Filter Export jobs				
Filter items...				
NAME	STATUS	TYPE	ITEM	
Reprotect	In progress	Protected item	webvm2	
Reprotect	In progress	Protected item	webvm1	

Task 2: Migrate the on-premises VM to Azure IaaS



- From the Azure portal, open the **BCDRRSV** Recovery Services Vault located in the **BCDRAzureSiteRecovery** resource group



2. Open the **BCDRSRV** and select **Replicated Items** under the **Protected Items** area. Make sure that **OnPremVM** shows up ad **Replication Heath: Healthy**. Select **OnPremVM**.

PROTECTED ITEMS		
Backup items		
Replicated items	Healthy	Protected

3. Right-click **OnPremVM** and then select **Failover**

- OnPremVM Healthy
- Pin to dashboard
- Planned Failover
- Failover**
- Test Failover
- Cleanup test failover
- Change recovery point
- Commit
- Complete Migration
- Reverse replicate
- Resynchronize
- Error Details
- Disable Replication

4. Select you understand the risk without a Test Failover and then on the Failover blade notice that the **From** is **OnPremHyperVSite** and the **To** is **Microsoft Azure**. Select **OK**.

Failover □ X

OnPremVM

Failover direction

From OnPremHyperVSite

To Microsoft Azure

Recovery Point

Choose a recovery point Latest (lowest RPO)

Shut down virtual machine and synchronize the latest data. If you do not select this option, or you select this option and the attempt fails, the latest recovery point will be used.

5. The Azure portal will provide a notification that the Failover is starting

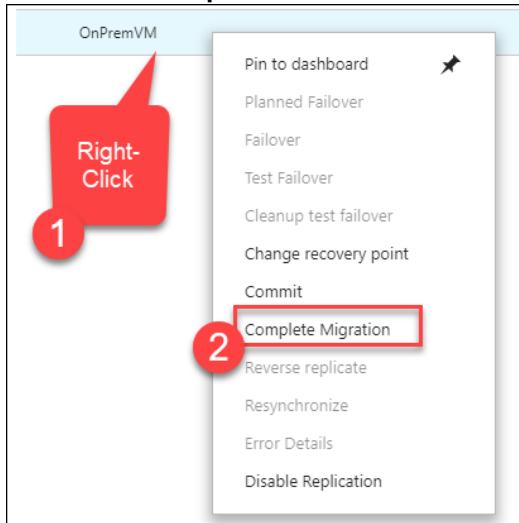
Starting Failover

The operation is in progress.

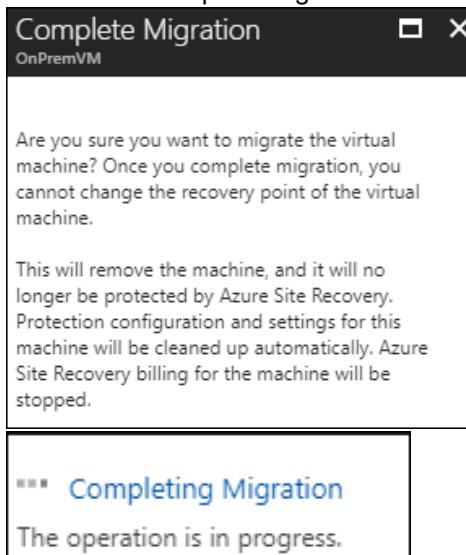
6. Using Jobs, Site Recovery Jobs, you can watch the progress of the failover

Properties	
Vault	BCDRRSV
Protected item	OnPremVM
Job id	4e4007ff-a0cc-4ab6-bc03-b0238ce2f5bc-2018-01-22 19:45:40
Source	OnPremHyperVSite
Target	Microsoft Azure
Job	
NAME	STATUS
Prerequisites check for failover	Successful
Shut down the virtual machine	Successful
Synchronizing the latest changes	Successful
Start failover	In progress
Start the replica virtual machine	

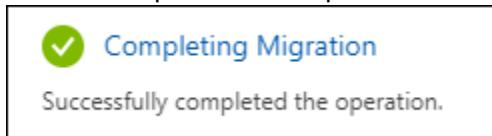
7. Move back to **Replicated Items** in the **BCDRRSV** and right-click **OnPremVM**. Select **Complete Migration**.



8. Review the Complete Migration blade and then select **OK**



9. Wait for this process finish prior to continuing



10. Once the Migration is completed, you can move over to the **BCDRIaaSSecondarySite** Resource group and locate and select the **OnPremVM**.

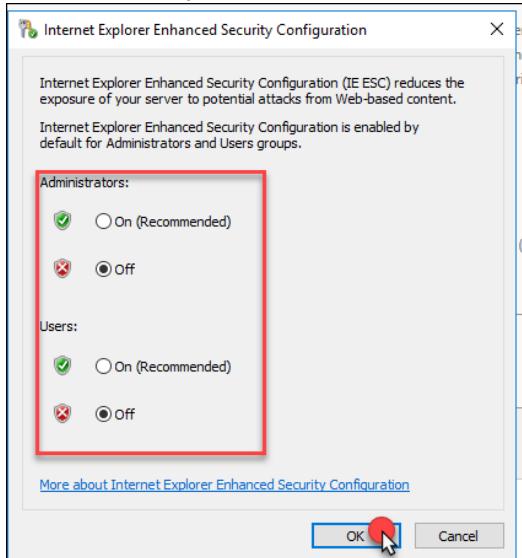
A screenshot of the Azure portal showing the "BCDR IaaS Secondary Site" Resource group. The left sidebar includes "Overview", "Activity log", "Access control (IAM)", and "Tags". Under "SETTINGS", there are "Quickstart", "Resource costs", "Deployments", "Policies", and "Properties". The main pane lists items under "Subscription (internal)" with a "Filter by name..." search bar. A list of 20 items is shown, with "NAME" as the sorting column. The items include "BCDRFOVNET", "BCDRFOVNETGateway-PIP", "BCDRFOVNET-to-BCDRVNET", "BCDRVNETFOGateway", "BCDRVNET-to-BCDRFOVNET", and "OnPremVM". The "OnPremVM" item is highlighted with a red circle at the bottom right.

11. Review the details of the VM. Notice that it is running in the **BCDRFOVNET** virtual network in the **WEB** Subnet

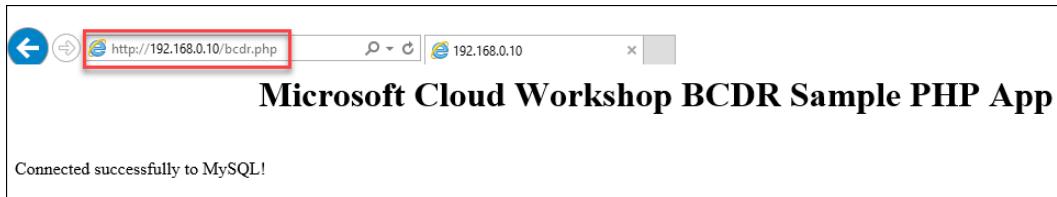
A screenshot of the Azure portal showing the "OnPremVM" Virtual machine details. The left sidebar includes "Overview", "Activity log", "Access control (IAM)", and "Tags". The main pane shows the "Resource group (change)" as "BCDR IaaS Secondary Site". The "Status" is listed as "Running" with a red arrow pointing to it. The "Location" is "Central US". On the right, detailed information is provided: Computer name, Operating system (Linux), Size (Standard D2s v3 (2 vcpus, 8 GB memory)), and Public IP address. A red box highlights the "Virtual network/subnet" field, which is "BCDRFOVNET/WEB".

12. Select the **Networking** link. Notice the IP address of the VM

A screenshot of the Azure portal showing the "OnPremVM - Networking" section. The left sidebar includes "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", and "Networking". The main pane shows the "Network Interface: OnPremVMa6a57ecc-baa8-4959-9d04-0bf17bd48787". It lists the "Virtual network/subnet: BCDRFOVNET/WEB", "Public IP: None", and "Private IP: 172.16.1.6". A red arrow points to the "Private IP: 172.16.1.6" field.

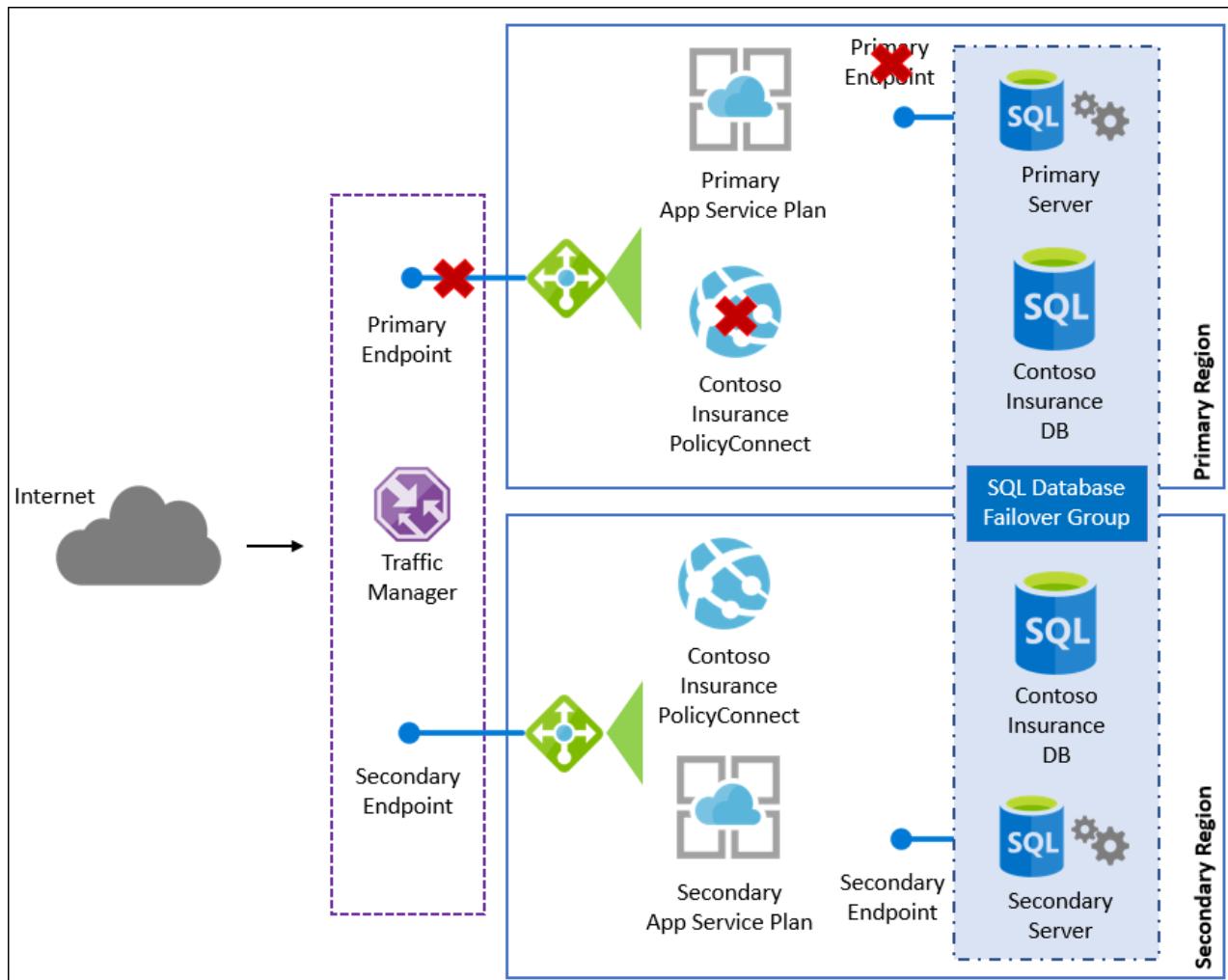
13. Remote desktop into BCDRDC1. Use the Server Manager to disable the IE Enhanced Security Configuration.**14. Point the browser of BCDRDC1 at the IP address of the OnPremVM. And it should load the sample web application**

http://172.16.1.?:/bcdr.php

**15. Your OnPremVM has been successfully migrated to Azure**

Option Task: If you wish you can Remote Desktop back to the HYPERVHOST, and you will see that the migrated VM has shutdown.

Task 3: Failover and failback Azure PaaS



1. Using the Azure portal, open the **BCDRPaaSPrimarySite** resource group. Locate the Traffic Manager profile and then click the URL to ensure that the application is running.



2. Once you are sure that the website is active and connecting to the database, move back to the BCDRPaaSPrimarySite resource group. Select **SQL Server** resource.

The screenshot shows the Azure Resource Group 'BCDRPaaSPrimarySite'. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Quickstart, Resource costs, Deployments, and Policies. Under 'SETTINGS', the 'Failover groups' option is highlighted with a red circle. The main pane displays a table of resources with columns for NAME, TYPE, and STATUS. One row, 'bcdrprimarysqlserverdmmaf3xji4zsu', is selected and highlighted with a red box.

3. Under **Settings**, select **Failover groups**

The screenshot shows the 'bcdrprimarysqlserverdmmaf3xji4zsu' SQL server settings. The left sidebar has links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Quick start, Firewall / Virtual Networks, and Failover groups. The 'Failover groups' link is highlighted with a red circle. The main pane shows a table of databases with columns for DATABASE, STATUS, and PRICING TIER. One database, 'ContosoInsurance', is listed as Online in the Standard S1 tier.

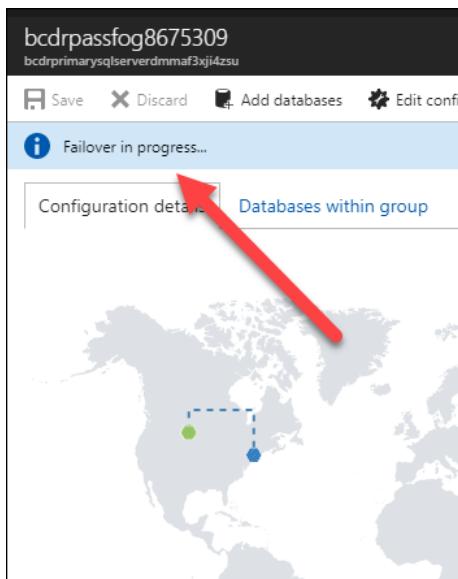
4. Select the **Failover Group**

The screenshot shows the 'bcdrprimarysqlserverdmmaf3xji4zsu - Failover groups' page. The left sidebar has links for Overview, Activity log, Access control (IAM), and Configuration details. The 'bcdrpassfog8675309' failover group is selected and highlighted with a red circle. The main pane shows a table with columns for NAME, PRIMARY SERVER, and SECONDARY SERVER. The 'bcdrpassfog8675309' group is listed under the primary server 'bcdrprimarysqlserverdmmaf3xji4zsu'.

5. Along the top of the page, select the **Failover** button. Then select **Yes** to confirm.

The screenshot shows a confirmation dialog box. It contains a warning message: 'This will switch all secondary databases to the primary role, server, which now becomes primary server.' At the bottom, there are two buttons: 'Yes' (highlighted with a red circle) and 'No'.

6. The portal will notify you of the **Failover in progress**



7. While this is happening move back to your browser tab with the Contoso Insurance application is running on using the PaaS Traffic Manager link. Attempt to use the application. You should see no difference during the failover, but there could be some slowdown in the responses from the web pages that access the database.
8. After a few minutes, move back to the Azure portal to the page where you performed the Failover. You should see that the Failover has completed and the Server running in the Secondary site will now show as the Primary replica. Also, there should be a notification from the Azure portal.

SERVER	ROLE
<input checked="" type="checkbox"/> bcdrsecondarysqlserverfcumtoavlf6 (Central US)	Primary
<input checked="" type="checkbox"/> bcdrprimarysqlserverdmmaf3xji4zsu (East US 2)	Secondary

Failover group failover succeeded 11:13 AM

Failover group failover succeeded for failover group:
bcdrpassfog8675309, old secondary server:
bcdrsecondarysqlserverfcumtoavlf6

A screenshot of the Azure portal showing the results of a failover. The top part is a table with two rows: the first row has a checked checkbox and the server name 'bcdrsecondarysqlserverfcumtoavlf6 (Central US)', labeled 'Primary'; the second row has a checked checkbox and the server name 'bcdrprimarysqlserverdmmaf3xji4zsu (East US 2)', labeled 'Secondary'. The bottom part is a message box with a green checkmark icon. It says 'Failover group failover succeeded' and '11:13 AM'. Below that, it says 'Failover group failover succeeded for failover group:' followed by the old secondary server name 'bcdrpassfog8675309' and the new primary server name 'bcdrsecondarysqlserverfcumtoavlf6'.

9. Next, to simulate a failover of one of the Azure regions you will stop the Primary Web App. Move to the **BCDRPaaSPrimarySite** resource group. Select the **Web App**.

A screenshot of the Azure portal showing the 'BCDRPrimarySite' resource group. The list contains five items: 'bcdrpaaas8675309', 'BCDRPrimarySiteAppPlan', 'BCDRPrimarySiteContosoInsurance' (with a red circle around it), 'bcdrprimarysqlserverdmmaf3xji4zsu', and 'ContosoInsurance'. The 'BCDRPrimarySiteContosoInsurance' item is selected.

10. Select the URL of the **Web App**. The browser should open to the direct link to the Application.

A screenshot showing the details for the 'BCDRPrimarySiteContosoInsurance' web app. It shows the resource group (change) as 'BCDRPaaSPrimarySite', status as 'Running', location as 'East US 2', and the URL as 'https://bcdrprimarysitecontosoinsurance.mmaf3xji4zsu.azurewebsites.net'. Below this, a browser window displays the 'Contoso Insurance' website, showing the 'Contoso Insurance PolicyCon' logo and a 'Welcome to the Policy Management System' message.

11. Back in the Azure portal, select **Stop** to terminate the Web App. Select **Yes** to confirm.

A screenshot of the Azure portal showing the 'BCDRPrimarySiteContosoInsurance' web app details. The 'Stop' button is highlighted with a red circle. Below it, a confirmation dialog box asks 'Are you sure you want to stop BCDRPrimarySiteContosoInsurance.mmaf3xji4zsu?' with 'Yes' and 'No' buttons. The 'Yes' button is also highlighted with a red circle.

12. The Web App will now show as stopped. Select the URL again, and notice that the Web App shows as stopped.

The screenshot shows the Azure portal interface for an App Service named 'BCDRPrimarySiteContosoInsuredmmaf3xji4zsu'. The 'Overview' blade is open, displaying a message: 'Your app is stopped. App Service plan charges still apply.' A red arrow points from this message to the status 'Stopped' listed below it. Below the blade, a browser window shows the URL <https://bcdrprimarysitecontosoinsuredmmaf3xji4zsu.azurewebsites.net>, which displays an 'Unavailable' error page with the message 'Error 403 - This web app is stopped.'

13. Move back to the **BCDRPaaS Traffic Manager** profile and review the **Monitor Status**

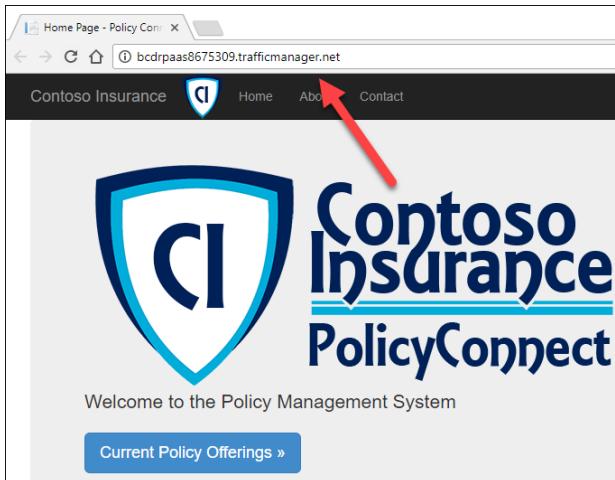
The screenshot shows the Azure portal interface for a Traffic Manager profile named 'bcdrpaaas8675309'. The 'Overview' blade is open, showing the 'Essentials' section with the status 'Enabled'. A red arrow points to the 'MONITOR STATUS' column in the 'Search endpoints' table. The table lists two endpoints: 'BCDRPaaSPrimarySite' with 'MONITOR STATUS' 'Stopped' and 'BCDRPaaSSecondarySite' with 'MONITOR STATUS' 'Online'.

NAME	STATUS	MONITOR STATUS
BCDRPaaSPrimarySite	Enabled	Stopped
BCDRPaaSSecondarySite	Enabled	Online

14. Select the **DNS Name URL**

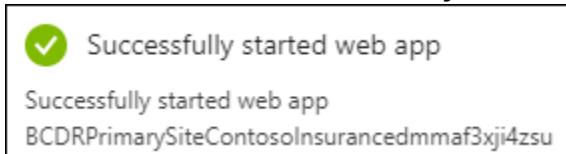
The screenshot shows the 'DNS name' field in the Azure portal, containing the URL <http://bcdrpaaas8675309.trafficmanager.net>. A red circle highlights the URL, and a red arrow points to the 'DNS name' label above it.

15. Notice that the website loads as normal. You can select refresh or F5, and you will always get back to the site.



16. In the current configuration, you are completely failed over to the **Secondary** site. There were no configurations for you to do and this was completely transparent to the user of the application.

17. Move back to the **BCDRPaaSPrimarySite** and start the Web App



18. Open the **BCDRPaaS** Traffic Manager again, and the Monitor Status should show both as Online again

The screenshot shows the Azure portal interface for a Traffic Manager profile named 'BCDRPaaSPrimarySite'. At the top, there are buttons for 'Enable profile', 'Disable profile', 'Refresh', 'Move', and 'Delete profile'. Below this, the 'Essentials' section shows the 'Resource group (change)' as 'BCDRPaaSPrimarySite', 'Status' as 'Enabled', and 'Subscription name (change)' as 'BCDRPaaSPrimarySite'. To the right, it shows the 'DNS name' as 'http://bcdrpaas8675309.trafficmanager.net', 'Monitor status' as 'Online', 'Routing method' as 'Performance', and 'Subscription ID' as 'BCDRPaaSPrimarySite'. Below this, there is a table titled 'Search endpoints' with columns: NAME, STATUS, MONITOR STAT..., TYPE, and LOCATION. The table contains two rows: 'BCDRPaaSPrimarySite' with STATUS 'Enabled' and MONITOR STATUS 'Online', and 'BCDRPaaSSecondarySite' with STATUS 'Enabled' and MONITOR STATUS 'Online'. A red arrow points to the 'MONITOR STAT...' column header.

NAME	STATUS	MONITOR STAT...	TYPE	LOCATION
BCDRPaaSPrimarySite	Enabled	Online	Azure endpoint	East US 2
BCDRPaaSSecondarySite	Enabled	Online	Azure endpoint	Central US

19. Move back to your **BCDRPaaSPrimarySite** resource group and select through to your **SQL Server**. Select the **Failover group**. Select **Failover** and **Confirm**.

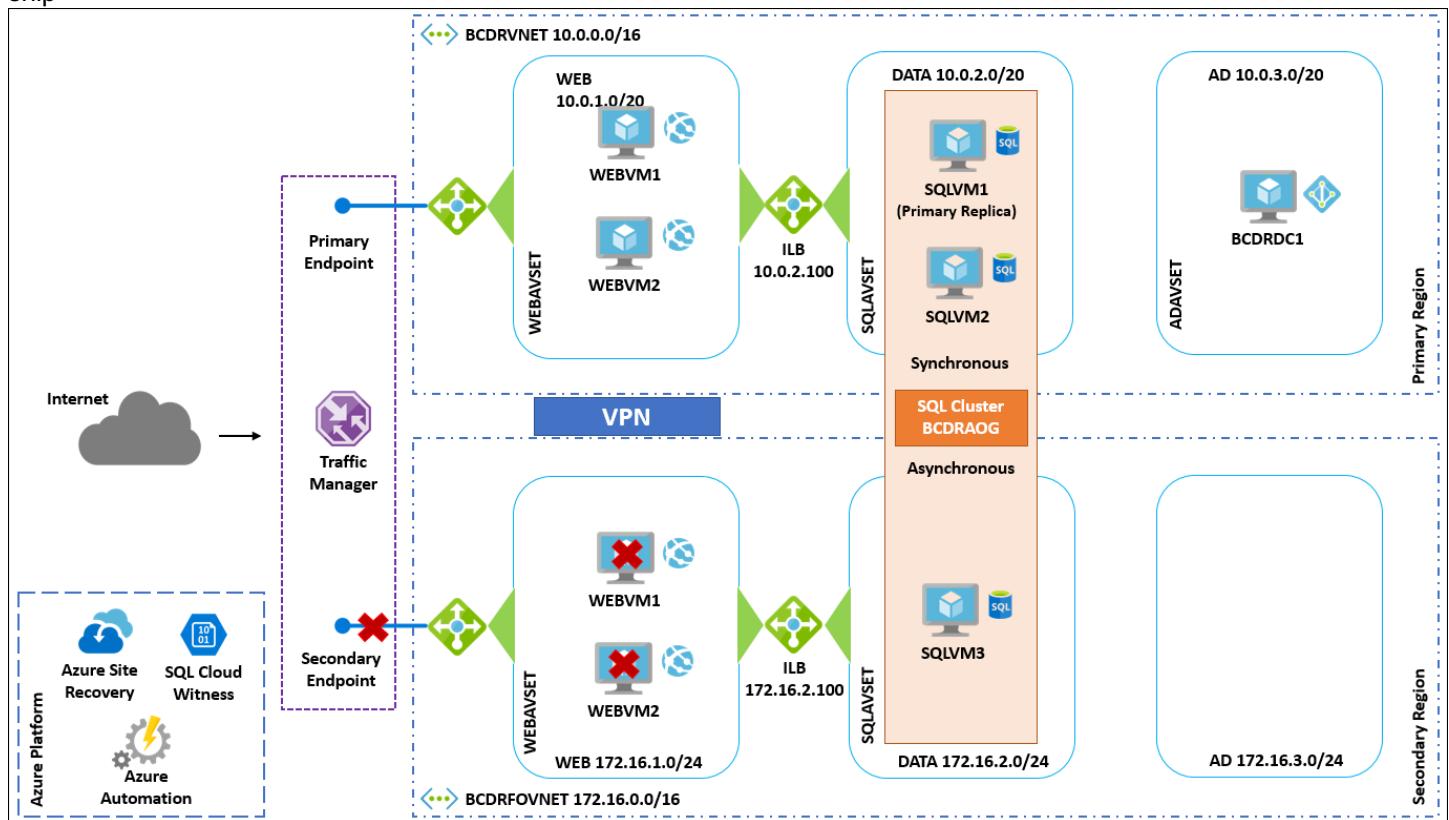


20. Once the Failover back to the **Primary** site is completed, the **SQL Server** in the **Primary** site will show as the **Primary**

SERVER	ROLE
<input checked="" type="checkbox"/> bcdrprimarysqlserverdmmaf3xji4zsu (East US 2)	Primary
<input checked="" type="checkbox"/> bcdrsecondarysqlserverfcumtoavlfq6 (Central US)	Secondary

Task 4: Failback Azure IaaS region to region

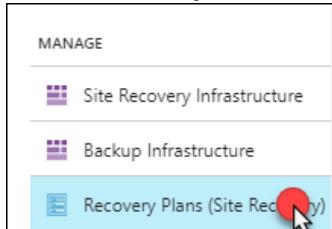
snip



1. Open the **BCDRSRV** and select **Replicated Items** under the **Protected Items** area. Make sure that **WEBVM1** and **WEBVM2** show up ad **Replication Heath: Healthy**.

NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION
WEBVM2	Healthy	Protected	Central US
WEBVM1	Healthy	Protected	Central US
OnPremVM	Healthy	Protected	OnPremHyperVSite

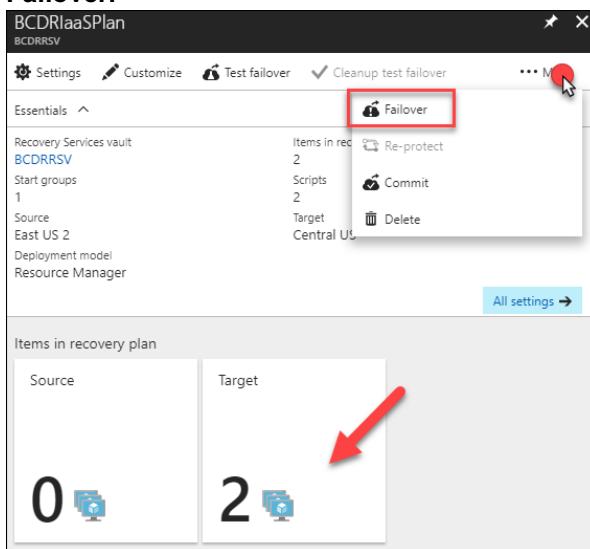
2. Select **Recovery Plans** under the **Manage** area



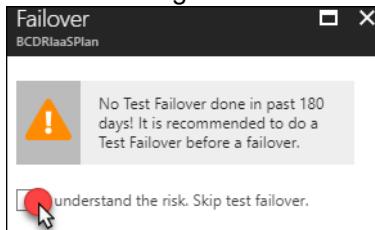
3. Select the **BCDRiaaSPlan**



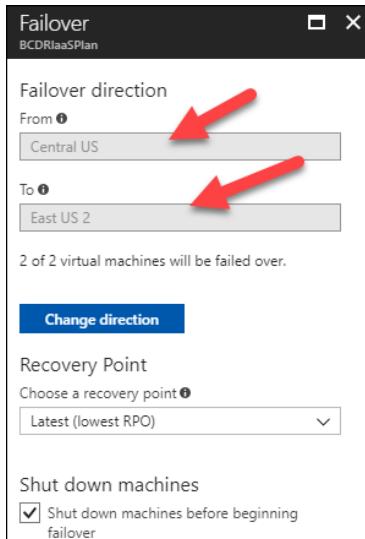
4. Notice that the VMs are still at the Target, since they are Failed over to the Secondary Site. Select **More, Failover**.



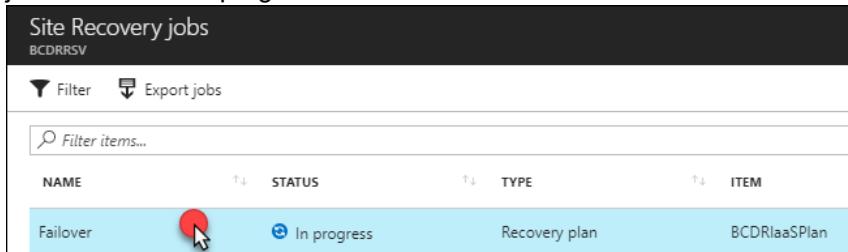
5. On the warning about No Test Failover, select **I understand the risk, Skip test failover**.



6. Review the Failover direction. Notice that **From** is the **Secondary** site and **To** is the **Primary** site. Select **OK**.



7. After the Failover is initiated close the blade and move to **Jobs**, then **Site Recovery Jobs**. Select the **Failover** job to monitor the progress.



8. Once the job has finished, it should show as successful for all tasks

Job	
NAME	STATUS
Prerequisites check for the recovery plan	Successful
▼ All groups shutdown (1)	Successful
Shutdown: Group 1 (2)	Successful
▼ All groups failover: Pre-steps (1)	Successful
Script on recovery side: ASRSQLFailover	Successful
▼ Recovery plan failover	Successful
webvm1	Successful
webvm2	Successful
▼ Group 1: Start (2)	Successful
webvm1	Successful
webvm2	Successful
▼ Group 1: Post-steps (1)	Successful
Script on recovery side: ASRWEBFailover	Successful
Finalizing the recovery plan	Successful

9. There is also details of the failover VMs shown. Notice how they are running the **BCDRVNET**. This is the primary Virtual Network running in the **Primary Site**.

Environment Details	
VIRTUAL MACHINE	NETWORK\SUBNET
WEBVM1	bcdrvnet\WEB
WEBVM2	bcdrvnet\WEB

10. Select Resource groups and select **BCDRiaSSecondarySite**. Locate the **WEBVM1** in the resource group and select to open.

11. Notice that it currently shows as **Status: Stopped (deallocated)**. This shows that failover has stopped the VMs at the **Secondary site**.

Note: Do not select Start! This is a task only for ASR.

12. Move back to the Resource group and select the **WWWEXTLB-PIP** Public IP address. Copy the DNS name and paste it into a new browser tab.

WWWEXTLB-PIP
Public IP address

Search (Ctrl+ /)

Associate Dissociate Move Delete

Overview Activity log Access control (IAM) Tags

Resource group (change) **BCDRIaaSSecondarySite**
IP address 52.176.41.59
DNS name **bcdrsesecondarysitelb66gkv4wdctubg.centralus.cloudapp.azure.com**
Associated to **WWWEXTLB**

13. The site will be unreachable at the **Secondary** location

14. In the Azure portal, move to the **BCDRIaaSPrimarySite** resource group. Locate the **WEBVM1** in the resource group and select to open.

BCDRIaaSPrimarySite
Resource group

Search (Ctrl+ /)

Add Columns Delete resource group Refresh

Overview Activity log Access control (IAM) Tags

SETTINGS Quickstart Resource costs Deployments Policies Properties

Filter by name... All types

28 items

NAME
WWWEXTLB-PIP
WWWEXTLB
WEBVM2-NIC
WEBVM2
WEBVM1-NIC
WEBVM1

15. Take note that the **WEBVM1** in the **Primary** site is running

WEBVM1
Virtual machine

Search (Ctrl+ /)

Connect Start Restart

Resource group (change) **bcdriaspowersite**
Status **Running** Location **East US 2**

Overview Activity log Access control (IAM)

16. Move back to the Resource group and select the **WWWEXTLB-PIP** Public IP address. Copy the DNS name and paste it into a new browser tab.

WWWEXTLB-PIP
Public IP address

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Associate Dissociate Move Delete

Resource group (change) BCDRPrimarySite

IP address 40.70.6.46

DNS name bcdrprimarysitelbasedyfizo7bpc.eastus2.cloudapp.azure.com

Associated to WWWEXTLB

17. The Application running on the **WEBVM1** and **WEBVM2** is now responding from the **Primary** Site. Make sure to select the current **Policy Offerings** to ensure that there is connectivity to the SQL Always On group that was also failed back to primary in the background.

Home Page - Policy Connect

bcdrprimarysitelbasedyfizo7bpc.eastus2.cloudapp.azure.com

Contoso Insurance Home About Contact

Welcome to the Policy Management System

Current Policy Offerings »

Index

Create New

Name	Description	DefaultDeductible
Bronze	Basic coverage	1000.00
Silver	Basic+ coverage	800.00
Gold	Advanced coverage	500.00
Platinum	Extensive coverage	250.00

© 2018 - Contoso Insurance

18. Using the Azure portal, locate the **BCDRaaS Traffic Manager** profile in the **BCDRaaSPrimarySite** resource group. Notice that the Monitor Status has moved to **Degraded** for the **Secondary Site** and moved to **Online** for **Primary** the site.

NAME	STATUS	MONITOR STAT...	TYPE	
BCDRaaSPrimarySiteLB	Enabled	Online	Azure endpoint	1
BCDRaaSSecondarySiteLB	Enabled	Degraded	Azure endpoint	2

19. Select the **DNS Name URL**. The site load immediately and is failed over. The users will always be using this DNS URL, so they there is no change in how they access the site even though it is failed over.

20. Now, that you have successfully failed back you need to prep ASR for the Failover again. Move back to the **BCDRSRV** Recovery Service Vault using the Azure portal. Select Recovery Plans on the ASR dashboard.

21. The BCDRlaaSPlan will show as **Failover completed**. Select the Plan.

The screenshot shows the 'Recovery plans' blade for the BCDRlaaSPlan. It lists one item: 'BCDRlaaSPlan' with a status of 'Failover completed'. A red arrow points to the status indicator.

22. Notice that now 2 VMs are show in the **Source**

23. Select **More**, then select **Re-protect**

The screenshot shows the BCDRlaaSPlan blade. In the top right, there is a 'More' button with a red box around it. Below it, the 'Re-protect' option is highlighted with a red circle and a cursor icon.

24. On the **Re-protect** screen review the configuration and then select **OK**

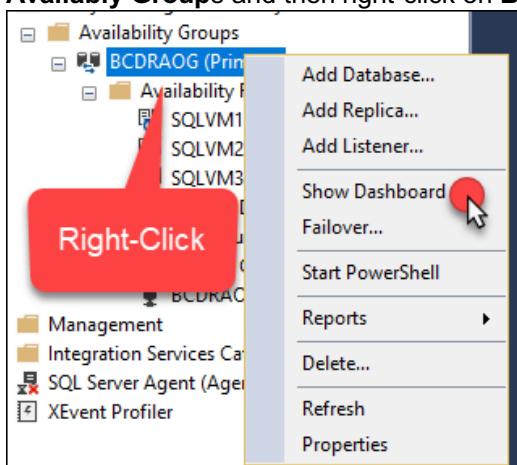
The screenshot shows the 'Re-protect' configuration screen. It displays the target details: 'Target resource group' set to 'BCDRlaaSSecondarySite', 'Target virtual network' set to 'BCDRFOVNET', 'Cache storage accounts' set to 'bcdrstorageasedcacheasr', 'Target storage accounts' set to 'bcdrstorageasedyfzoasr', and 'Target availability sets' set to 'WEBAVSET'. A red box highlights the 'Customize' link at the top right of the configuration area.

25. The portal will submit a deployment. This process will take some time, by first committing the failover and then synchronizing the **WEBVM1** and **WEBVM2** back to the **Primary** Site. Once this process is complete, then you will be able to Fail over from the **Primary** to **Secondary** site from the perspective of ASR.

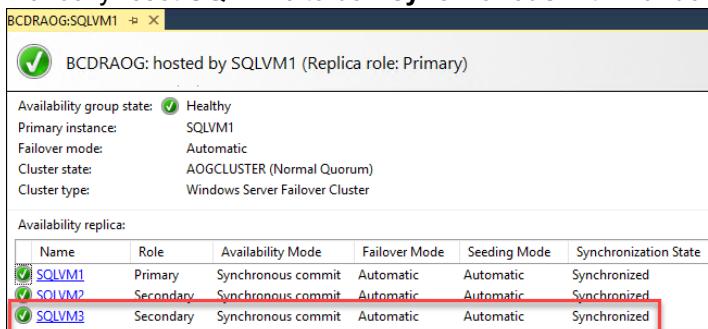
26. Select **Resource groups** in the Azure portal and notice that two new Resource groups have been created with - asr in their names. These are used by ASR for the Failover and Failback, so they should be left in place.

The screenshot shows the 'Resource groups' blade. It lists three resource groups: 'BCDRlaaSPPrimarySite', 'BCDRlaaSPPrimarySite-asr', and 'BCDRlaaSPPrimarySite-asr-1'. A large red arrow points to the 'BCDRlaaSPPrimarySite-asr' group.

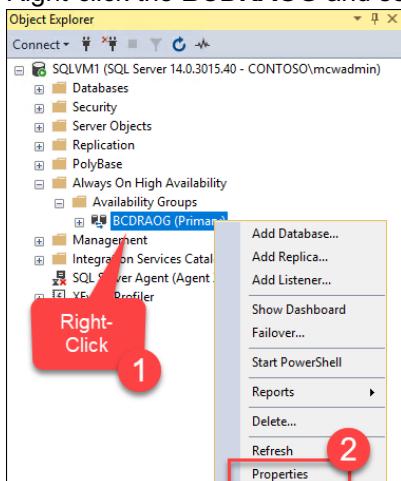
27. Next, you need to reset the SQL AOG environment to ensure a proper failover. To do this open Remote Desktop to **BCDRDC1** and then jump to **SQLVM1** using Remote desktop.
28. Once connected to **SQLVM1** open SQL Management Studio and Connect to **SQLVM1**. Expand the **Always On Available Groups** and then right-click on **BCDRAOG** and then select **Show Dashboard**.



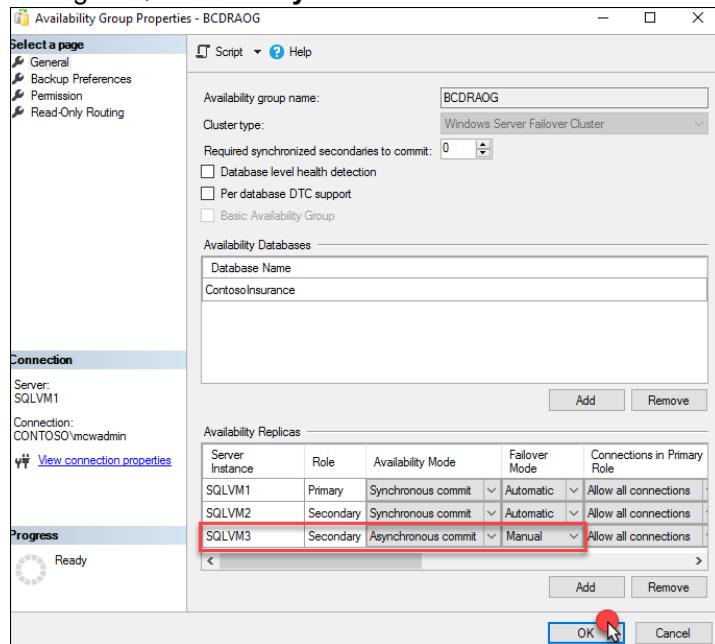
29. Notice that all the Replica partners are now Synchronous Commit with Automatic Failover Mode. You need to manually reset **SQLVM3** to be **Asynchronous** with **Manual Failover**.



30. Right-click the **BCDRAOG** and select **Properties**



31. Change SQLVM3 to Asynchronous and Manual Failover and select OK



32. Show the Availability Group Dashboard again. Notice that they change has been made and that the AOG is now reset.

Name	Role	Availability Mode	Failover Mode	Seeding Mode	Synchronization State
SQLVM1	Primary	Synchronous commit	Automatic	Automatic	Synchronized
SQLVM2	Secondary	Synchronous commit	Automatic	Automatic	Synchronized
SQLVM3	Secondary	Asynchronous commit	Manual	Automatic	Synchronizing

Note: This task could have been done using the Azure Automation script during Failback, but more DBAs would prefer a good clean fallback and then do this manually once they are comfortable with the failback.

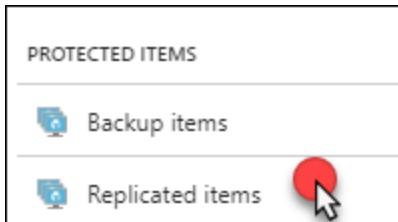
After the hands-on lab

Duration: 15 minutes

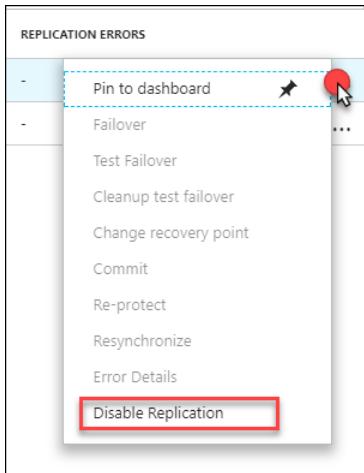
There are many items that were created as a part of this lab, and they should be deleted once you no longer desire to retain the environments.

Task 1: Disable replication in the recovery services vault

1. To clean up the environment, you must first disable the replication of the **WEBVM1**, **WEBVM2** and **OnPremVM** in the **BCDRSRV** Recovery Service Vault. Open **BCDRSRV** in the Azure portal and select **Replicated Items** in the **Protected Items** area.



2. Select the **Ellipse** next to each replicated item and then select **Disable Replication**. On the following screen select **OK**



3. After this process is completed you can move on to the next task

Task 2: Delete all BCDR resource groups

1. Using the Azure Portal delete each of the BCDR Resource Groups that you created

Resource Group Name	Location
BCDRAzureAutomation	Your Location
BCDRAzureSiteRecovery	Secondary
BCDRIaaSPrimarySite	Primary
BCDRIaaSSecondarySite	Secondary
BCDRLabRG	Your Location
BCDROnPremPrimarySite	Primary
BCDROnPremPrimarySite-asr	Primary
BCDROnPremPrimarySite-asr-1	Primary
BCDRPaaSPrimarySite	Primary
BCDRPaaSSecondarySite	Secondary

You should follow all steps provided *after* attending the Hands-on lab.