



Building a resilient IaaS architecture

Hands-on lab step-by-step

May 2022

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.

© 2022 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 property of their respective owners.

Contents

- [Building a resilient IaaS architecture hands-on lab step-by-step](#)
 - [Abstract and learning objectives](#)
 - [Overview](#)
 - [Solution architecture](#)
 - [Requirements](#)
 - [Help references](#)
 - [Exercise 1: Enable High Availability for the Contoso application](#)
 - [Task 1: Deploy HA resources](#)

- Task 2: Configure HA for the Domain Controller tier
- Task 3: Configure HA for the SQL Server tier
- Task 4: Configure HA for the Web tier
- Exercise 2: Enable Disaster Recovery for the Contoso application
 - Task 1: Deploy DR resources
 - Task 2: Inspect DR for the Domain Controller tier
 - Task 3: Configure DR for the SQL Server tier
 - Task 4: Configure DR for the Web tier
 - Task 5: Configure a public endpoint using Azure Front Door
- Exercise 3: Enable Backup for the Contoso application
 - Task 1: Create the Azure Backup resources
 - Task 2: Enable Backup for the Web tier
 - Task 3: Enable Backup for the SQL Server tier
- Exercise 4: Validate resiliency
 - Task 1: Validate High Availability
 - Task 2: Validate Disaster Recovery - Failover IaaS region to region
 - Task 3: Validate Disaster Recovery - Fallback IaaS region to region
 - Task 4: Validate VM Backup
 - Task 5: Validate SQL Backup
- After the hands-on lab
 - Task 1: Delete the lab resources

Building a resilient IaaS architecture hands-on lab step-by-step

Abstract and learning objectives

In this hands-on lab, you will deploy a pre-configured IaaS environment and then redesign and update it to account for resiliency and high availability. Throughout the hands-on lab, you will use various configuration options and services to help build a resilient architecture.

At the end of the lab, you will be better able to design and use availability zones, SQL Server Always On Availability Groups, Azure Site Recovery, Azure Backup, and Azure Front Door to implement a fully resilient IaaS application. The training includes content on high availability, disaster recovery, as well as knowledge of how to back up the databases and virtual machines.

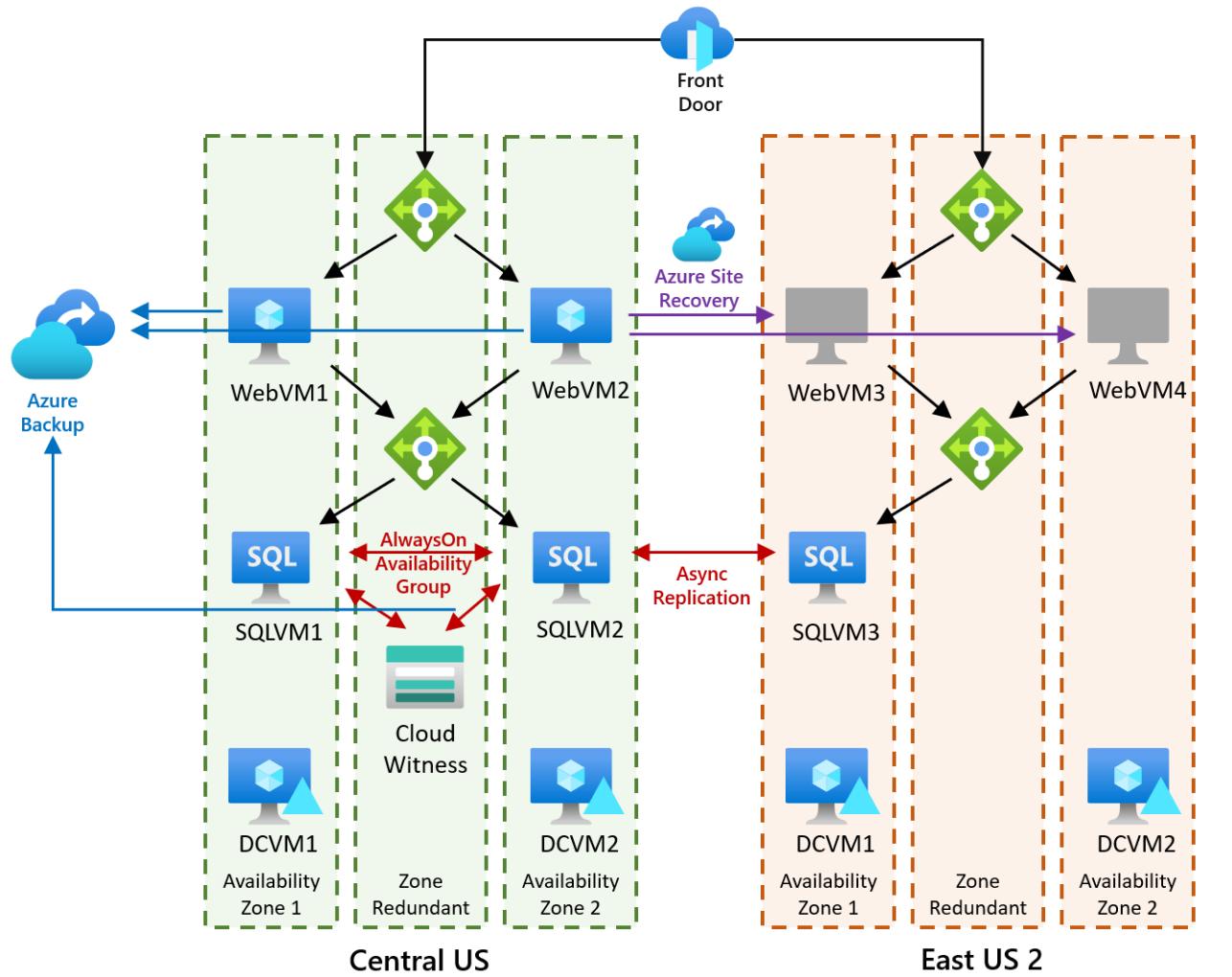
Overview

Contoso has asked you to deploy their infrastructure in a resilient manner to ensure their infrastructure will be available for their users and gain an SLA from Microsoft.

Solution architecture

The following diagram shows the highly resilient application architecture you will build in this lab. Starting with just WebVM1, SQLVM1 and DCVM1, you will first build out a fully-redundant, high-availability

environment in Central US. You will then extend this environment to a disaster recovery site in East US 2 and add a backup solution for both the web tier and database tier.



Requirements

Complete the steps given in the [Before the HOL - Building a resilient IaaS architecture](#) guide before starting this lab.

Help references

Description	Links
Azure Resiliency Overview	https://azure.microsoft.com/features/resiliency/
Always-On Availability Groups	https://docs.microsoft.com/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server?view=sql-server-2017
SQL Server Backup in Azure VMs	https://docs.microsoft.com/azure/backup/backup-azure-sql-database

Azure Backup

<https://azure.microsoft.com/services/backup/>

Azure Site
Recovery

<https://docs.microsoft.com/en-us/azure/site-recovery/>

Exercise 1: Enable High Availability for the Contoso application

Duration: 60 minutes

The Contoso application has been deployed to the Central US region. This initial deployment does not have any redundancy - it uses a single web VM, a single database VM, and a single domain controller VM.

In this exercise, you will convert this deployment into a highly-availability architecture by adding redundancy to each tier.

Task 1: Deploy HA resources

In this task, you will deploy additional web, database, and domain controller VMs.

A template will be used to save time. You will configure each tier in subsequent exercises in this lab.

1. Select the **Deploy to Azure** button below to open the Azure portal and launch the template deployment for the additional infrastructure components that will be used to enable high availability for the Contoso application. Log in to the Azure portal using your subscription credentials.



Deploy to Azure

2. Complete the Custom deployment blade as follows:

- Resource Group: **ContosoRG1** (existing)
- Location: Location close to you. This will be your primary location.

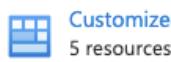
Select **Review + Create** and then **Create** to deploy resources.

Custom deployment

Deploy from a custom template

[Basics](#) [Review + create](#)

Template



[Customized template](#) ↗
5 resources

[Edit template](#)

[Edit parameters](#)

[Visualize](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

ContosoRG1

[Create new](#)

Instance details

Region * ⓘ

(US) East US 2

Sku Size VM ⓘ

D2s_v3

Admin Username ⓘ

demouser

Admin Password ⓘ

Domain Name ⓘ

contoso.com

Existing DNS Server ⓘ

10.0.3.100

Base Uri

<https://raw.githubusercontent.com/microsoft/MCW-Building-a-resilie...>

Resource Folder

master/Hands-on%20lab/Resources/

[Review + create](#)

< Previous

Next : Review + create >

3. While you wait for the HA resources to deploy, review the template contents. You can review the template by navigating to the **ContosoRG1** resource group, selecting **Deployments** in the resource group left-nav, and selecting any of the deployments, followed by **template**.

```

1  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
2  "contentVersion": "1.0.0.0",
3  "parameters": {
4      "sk1Elephant": {
5          "defaultValue": "D2s_v3",
6          "allowedValues": [
7              "D2s_v3",
8              "D2s_v5",
9              "DC2s_v3"
10         ],
11         "type": "string",
12         "metadata": {
13             "description": "Size of Virtual Machines to use"
14         }
15     },
16     "adminUsername": {
17         "defaultValue": "demouser",
18         "type": "String",
19     }
20 }

```

The template contains five child templates, containing the various resources required for:

- The ADVM2 virtual machine, which will be a second Domain Controller.
- The SQLVM2 virtual machine, which will be a second SQL Server.
- The WebVM2 virtual machine, which will be a second web server.
- Two load balancers, one for the web tier and one for the SQL tier.
- The virtual network with the proper DNS configuration in place.

4. You can check the HA resource deployment status by navigating to the **ContosoRG1** resource group, selecting **Deployments** in the resource group left-nav, and checking the status of the deployments. Make sure the deployment status is **Succeeded** for all templates before proceeding to the next task.

<input type="checkbox"/> Deployment name	Status	Last modified	Duration
<input type="checkbox"/> VirtualNetworkWithDNS	Succeeded	5/3/2022, 3:09:27 PM	6 seconds
<input type="checkbox"/> WebVM2	Succeeded	5/3/2022, 3:12:47 PM	9 minutes 48 seconds
<input type="checkbox"/> SQLVM2	Succeeded	5/3/2022, 3:11:04 PM	8 minutes 6 seconds
<input type="checkbox"/> ADVM2	Succeeded	5/3/2022, 3:09:12 PM	6 minutes 13 seconds
<input type="checkbox"/> LoadBalancers	Succeeded	5/3/2022, 3:03:03 PM	5 seconds
<input type="checkbox"/> Microsoft.Template-20220503150252	Succeeded	5/3/2022, 3:12:58 PM	10 minutes 3 seconds
<input type="checkbox"/> WebVM1	Succeeded	5/3/2022, 2:53:19 PM	8 minutes 12 seconds
<input type="checkbox"/> Bastion	Succeeded	5/3/2022, 2:50:17 PM	5 minutes 11 seconds
<input type="checkbox"/> SQLVM1	Succeeded	5/3/2022, 2:54:00 PM	8 minutes 53 seconds
<input type="checkbox"/> ADVM1	Succeeded	5/3/2022, 2:44:31 PM	7 minutes 22 seconds
<input type="checkbox"/> VirtualNetwork	Succeeded	5/3/2022, 2:37:03 PM	12 seconds
<input type="checkbox"/> Microsoft.Template-20220503143646	Succeeded	5/3/2022, 2:54:06 PM	17 minutes 19 seconds

Task 2: Configure HA for the Domain Controller tier

In this task, you will reboot all the virtual machines to ensure they receive the updated DNS settings.

When using a domain controller VM in Azure, other VMs in the virtual network must be configured to use the domain controller as their DNS server. This is achieved with the DNS settings in the virtual network. These settings are then picked up by the VMs when they reboot or renew their DHCP lease.

The initial deployment included a first domain controller VM, **ADVM1**, with static private IP address **10.95.3.100**. The initial deployment also configured this IP address in the VNet DNS settings.

The HA resources template has added a second domain controller, **ADVM2**. The static private IP address should be **10.95.3.101**. This server has already been promoted to be a domain controller using a CustomScriptExtension (you can review this script if you like, you'll find it linked from the ADVM2 deployment template). The template also updated the DNS setting on the virtual network to include the IP address of the second domain controller.

In this task, you will reboot all the servers to ensure they have the latest DNS settings.

1. Restart the **ADVM1** and **ADVM2** virtual machines in the **ContosoRG1** resource group, so they pick up the new DNS server settings.
2. Wait for a minute or two for the domain controller VMs to boot fully, then restart the **WebVM1**, **WebVM2**, **SQLVM1**, and **SQLVM2** virtual machines, so they also pick up the new DNS server settings.

Task 3: Configure HA for the SQL Server tier

In this task, you will build a Windows Failover Cluster and configure SQL Always On Availability Groups to create a high-availability database tier.

1. From the Azure portal home page, select **+ Create a resource**. Select **Storage account**.
2. Complete the **Create storage account** form using the following details:
 - **Resource group:** Use existing / ContosoRG1
 - **Storage account name:** Unique name starting with **contososqlwitness**
 - **Location:** Any location in your area that is **NOT** your Primary or Secondary site, for example **West US 3**.
 - **Performance:** Standard
 - **Replication:** Zone-redundant storage (ZRS)
 - **Access tier (default):** Hot

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *

Resource group *

[Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

Performance ⓘ *

Standard: Recommended for most scenarios (general-purpose v2 account)
 Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ *

[Review + create](#)

< Previous

Next : Advanced >

3. Switch to the **Advanced** tab. Change the **Minimum TLS version** to **Version 1.0**. Then select **Review + Create**, followed by **Create**.

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations

Enable blob public access

Enable storage account key access

Default to Azure Active Directory authorization in the Azure portal

Minimum TLS version ▼

Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). [Learn more](#)

Enable hierarchical namespace

Blob storage

Enable SFTP (preview)

To enable SFTP, 'hierarchical namespace' must be enabled.

Enable network file system v3

< Previous

Next : Networking >

Note: To promote the use of the latest and most secure standards, by default, Azure storage accounts require TLS version 1.2. This storage account will be used as a Cloud Witness for our SQL Server cluster. SQL Server requires TLS version 1.0 for the Cloud Witness.

- Once the storage account is created, navigate to the storage account blade. Select **Access keys** under **Security + networking**. Toggle the **Show/Hide keys button** (Shown as hide keys in the screenshot), copy the **storage account name** and the **first access key**, and paste them into your text editor of choice - you will need these values later.

contososqlwitness53 | Access keys

Storage account

Search (Cmd+ /) Hide keys Set rotation reminder Refresh

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account. [Learn more about managing storage account access keys](#)

Storage account name: contososqlwitness53

key1 Rotate key
Last rotated: 5/3/2022 (0 days ago)
Key: jderV6... (highlighted with a red box)

Connection string: ...ountKe... (highlighted with a red box)

key2 Rotate key
Last rotated: 5/3/2022 (0 days ago)
Key: vt4/0Q... (highlighted with a red box)

Connection string: ...ountKe... (highlighted with a red box)

Containers, File shares, Queues, Tables, Networking, Azure CDN, Shared access signature, Encryption

5. Return to the Azure portal and navigate to the **ContosoSQLLBPrimary** load balancer blade. Select **Backend pools** and open **BackEndPool1**.

ContosoSQLLBPrimary | Backend pools

Load balancer

Search (Cmd+ /) Add Refresh Give feedback

Filter by name... Backend pool == all

Group by Backend pool

Backend pool	Resource Name
BackEndPool1	BackEndPool1 (highlighted with a red box)

Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems

Settings

Frontend IP configuration, Backend pools (highlighted with a red box), Health probes, Load balancing rules

6. In the **BackendPool1** blade, select **+ Add** and choose the two SQL VMs. Select **Add** to close. Select **Save** to add these SQL VMs to **BackEndPool1**.

Add virtual machines to backend pool

BackEndPool1

ContosoSQLLBPrimary

 IPv4 IPv6

Virtual machines

You can only attach virtual machines in All IP configurations must be on the same virtual network.

+ Add**X Remove**

Virtual machine ↑↓

No virtual machines selected

Virtual machine scale sets

Virtual Machine Scale Sets must be in the same location (Basic/Standard) as the Load Balancer.

<input type="checkbox"/>	Virtual machine	Resource group	IP Configuration	Availability set	Tags
<input type="checkbox"/>	webvm2	contosorg1	ipconfig1 (10.0.1.5)	-	-
<input type="checkbox"/>	advm2	contosorg1	ipconfig1 (10.0.3.101)	-	-
<input checked="" type="checkbox"/>	sqlvm2	contosorg1	ipconfig1 (10.0.2.5)	-	-
<input checked="" type="checkbox"/>	sqlvm1	contosorg1	ipconfig1 (10.0.2.4)	-	-
<input type="checkbox"/>	advm1	contosorg1	ipconfig1 (10.0.3.100)	-	-
<input type="checkbox"/>	webvm1	contosorg1	ipconfig1 (10.0.1.4)	-	-

Save
Cancel
Give feedback

3

Note: The load-balancing rule in the load balancer has been created with **Floating IP (direct server return)** enabled. This is important when using the Azure load balancer for SQL Server AlwaysOn Availability Groups.

7. From the Azure portal, navigate to the **SQLVM1** virtual machine. Select **Connect**, then choose **Bastion**.

Home >

SQLVM1 Virtual machine

Search (Cmd+ /)

Connect ▾

Start | Restart | Stop

Overview | Activity log | Access control (IAM) | Tags | Diagnose and solve problems | Settings

RDP | SSH | **Bastion**

Location: East US 2 (Zone 1) | Subscription (move): Demo Creation | Subscription ID: e223f1b3-d19b-4cfa-98e9-... | Availability zone: 1

8. Connect to the machine using the following credentials:

- **Username:** adadmin@contoso.ins
- **Password:** Demo!pass123

PROFESSEUR : M.DA ROS

◆ 11 / 137 ◆

BTS SIO BORDEAUX - LYCÉE GUSTAVE EIFFEL

Note: When using Azure Bastion to connect to a VM using domain credentials, the username must be specified in the format `user@domain-fqdn` and **not** in the format `domain\user`.

Home > SQLVM1

SQLVM1 | Bastion Virtual machine

Search (Cmd+ /) Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Connection Settings

Open in new window

Username * `demouser@contoso.com`

Password * `*****`

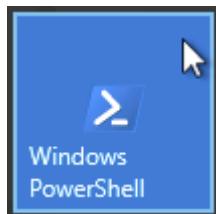
Show Connect

Azure Bastion protects your virtual machines by providing lightweight, browser-based connectivity without the need to expose them through public IP addresses. Deploying will automatically create a Bastion host on a subnet in your virtual network. [Learn more](#)

Using Bastion: **PrimaryBastion**, Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

9. On **SQLVM1**, select **Start** and then choose **Windows PowerShell**.



10. Copy and paste the following command into PowerShell and execute it. This 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 **10.95.2.99** to the new Cluster named **sqlAlwaysOn**.

```
New-Cluster -Name sqlAlwaysOn -Node SQLVM1,SQLVM2 -StaticAddress  
10.22.2.99
```

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

```
PS C:\Users\demouser.CONTOSO> New-Cluster -Name AOGCLUSTER -Node SQLVM1,SQLVM2 -StaticAddress 10.0.2.99  
WARNING: There were issues while creating the clustered role that may prevent it from starting. For more information  
view the report file below.  
WARNING: Report file location: C:\Windows\cluster\Reports\Create Cluster Wizard AOGCLUSTER on 2022.05.03 At  
20.48.22.htm
```

Name

AOGCLUSTER

```
PS C:\Users\demouser.CONTOSO>
```

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.

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



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

A screenshot of the Failover Cluster Manager application. The left navigation pane shows a tree structure with 'AOGCLUSTER.contoso.com' expanded, showing 'Roles', 'Nodes', 'Storage', 'Networks', and 'Cluster Events'. The 'Nodes' item is selected and highlighted with a red box. The main pane is titled 'Nodes (2)' and contains a table with two rows. The table has columns for Name, Status, Assigned Vote, and Current Vote. The data is as follows:

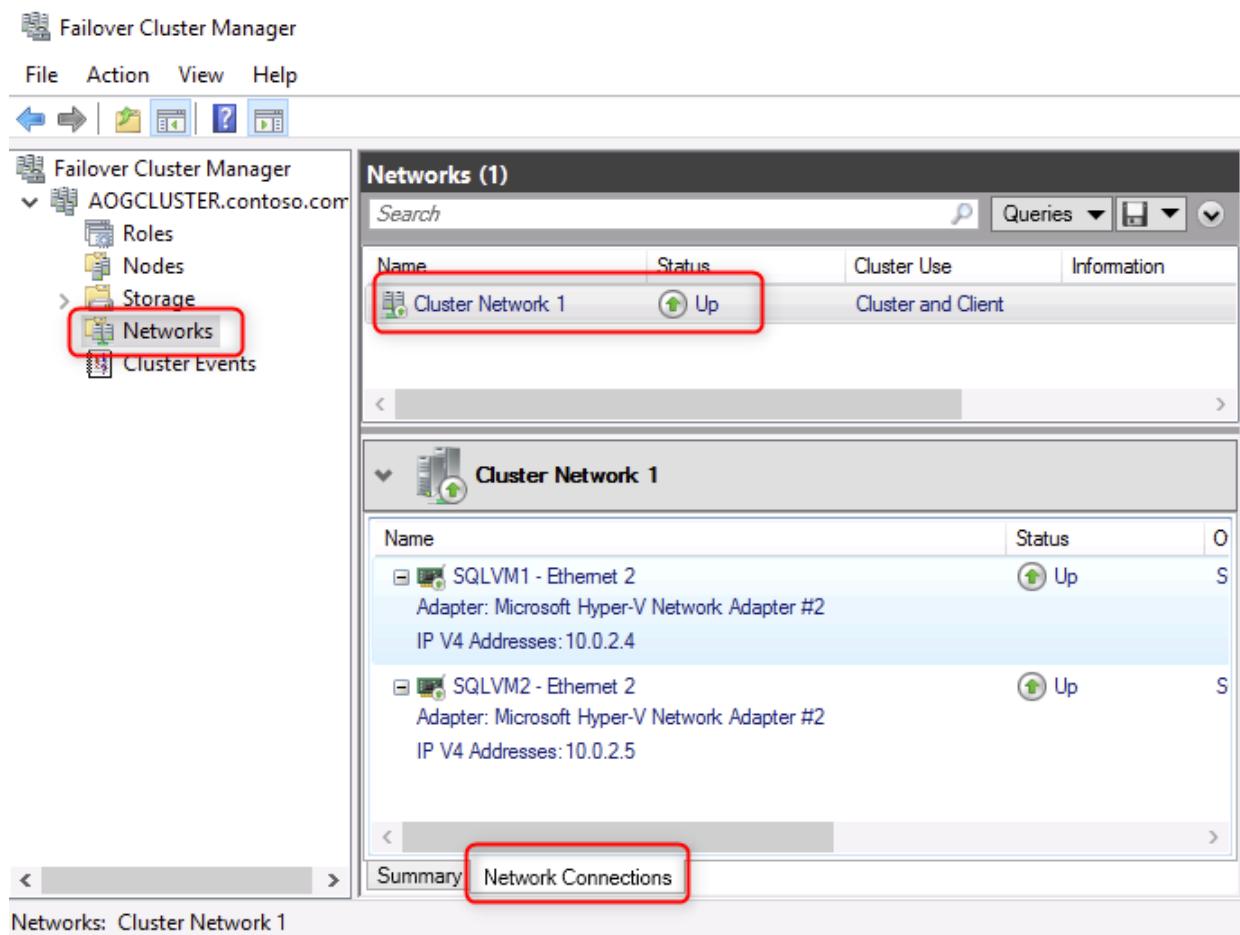
Name	Status	Assigned Vote	Current Vote
SQLVM1	Up	1	1
SQLVM2	Up	1	0

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

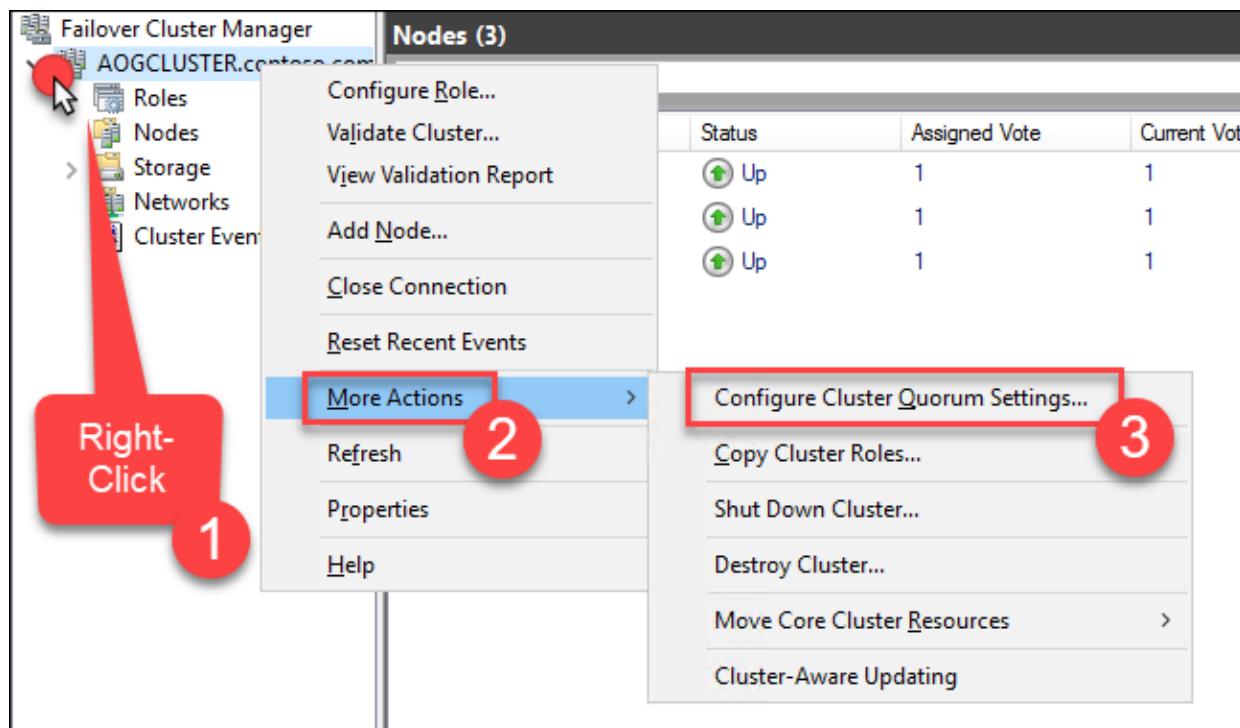
A screenshot of the Failover Cluster Manager application. The left navigation pane shows a tree structure with 'AOGCLUSTER.contoso.com' expanded, showing 'Roles', 'Nodes', 'Storage', 'Networks', and 'Cluster Events'. The 'Roles' item is selected and highlighted with a red box. The main pane is titled 'Roles (0)' and contains a table with no data.

Name	Status	Type	Owner Node

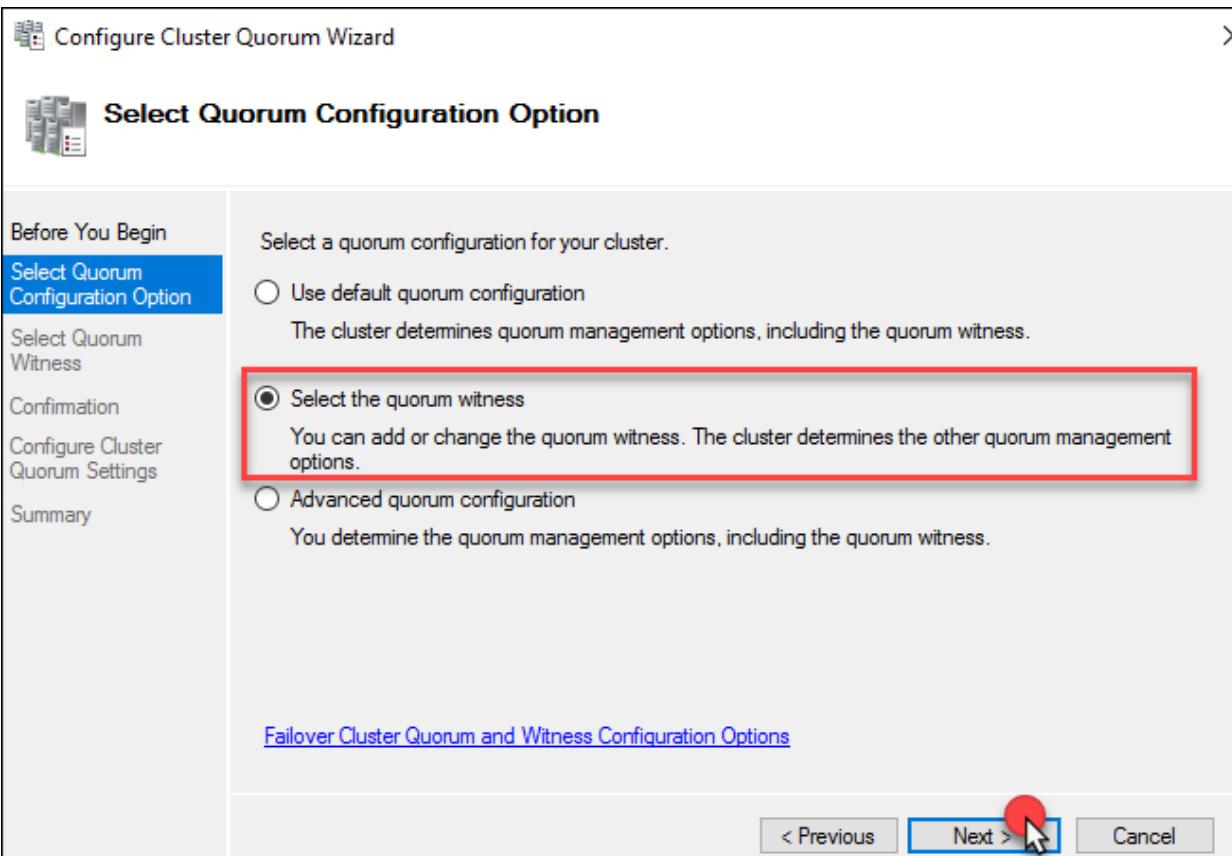
14. Select Networks, and you will see **Cluster Network 1** with status **Up**. If you navigate to the network, you will see the IP address space, and on the lower tab, you can select **Network Connections** and review the nodes.



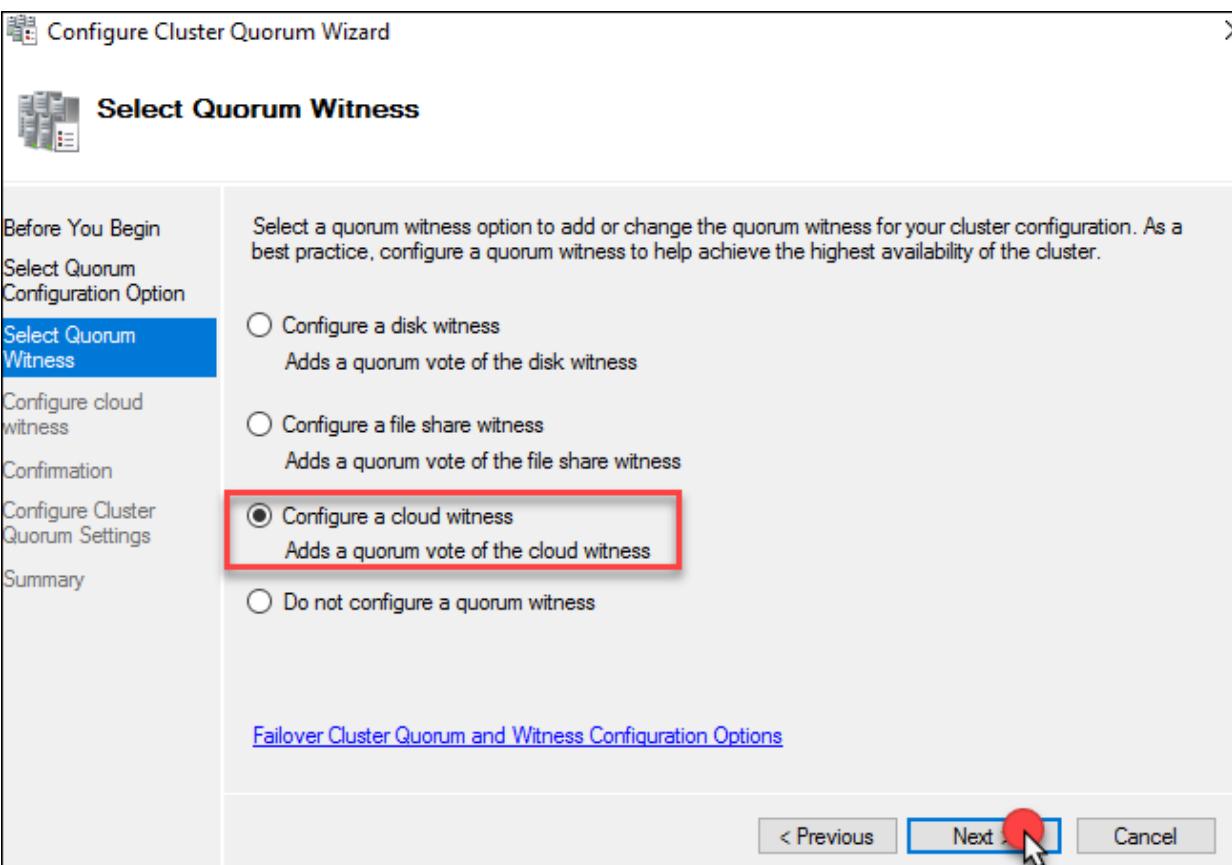
15. Right-click **sqlAlwaysOn**, then select **More Actions**, **Configure Cluster Quorum Settings**.



16. On **Before you Begin** in the wizard, select **Next**. Then choose **Select the quorum witness**. Then, select **Next** again.



17. Select **Configure a cloud witness** and **Next**.



18. Copy the **storage account name** and **storage account key** values you noted earlier and paste them into their respective fields on the form. Leave the Azure Service endpoint as configured. Then, select **Next**.

Configure Cluster Quorum Wizard

X

Configure cloud witness

Before You Begin

Select Quorum Configuration Option

Select Quorum Witness

Configure cloud witness

Confirmation

Configure Cluster Quorum Settings

Summary

Please enter your Azure storage account credentials to configure the cloud witness. These credentials are not stored by the cluster. Instead, they are used to create a shared access signature that is stored in the cluster database.

Azure storage account name:

contososqlwitness49

Azure storage account key:

I0yaQlpkQ6J4SkZbLINLNhMmTaRNcw==

Azure service endpoint:

core.windows.net

< Previous

Next >

Cancel

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

Configure Cluster Quorum Wizard

X

Confirmation

Before You Begin

Select Quorum Configuration Option

Select Quorum Witness

Configure cloud witness

Confirmation

Configure Cluster Quorum Settings

Summary

You are ready to configure the quorum settings of the cluster.

Configure Cluster Quorum Settings

Cloud Witness bcdrcloudwitness8675309

Cluster Managed Voting Enabled

Voting Nodes:

All nodes are configured to have quorum votes

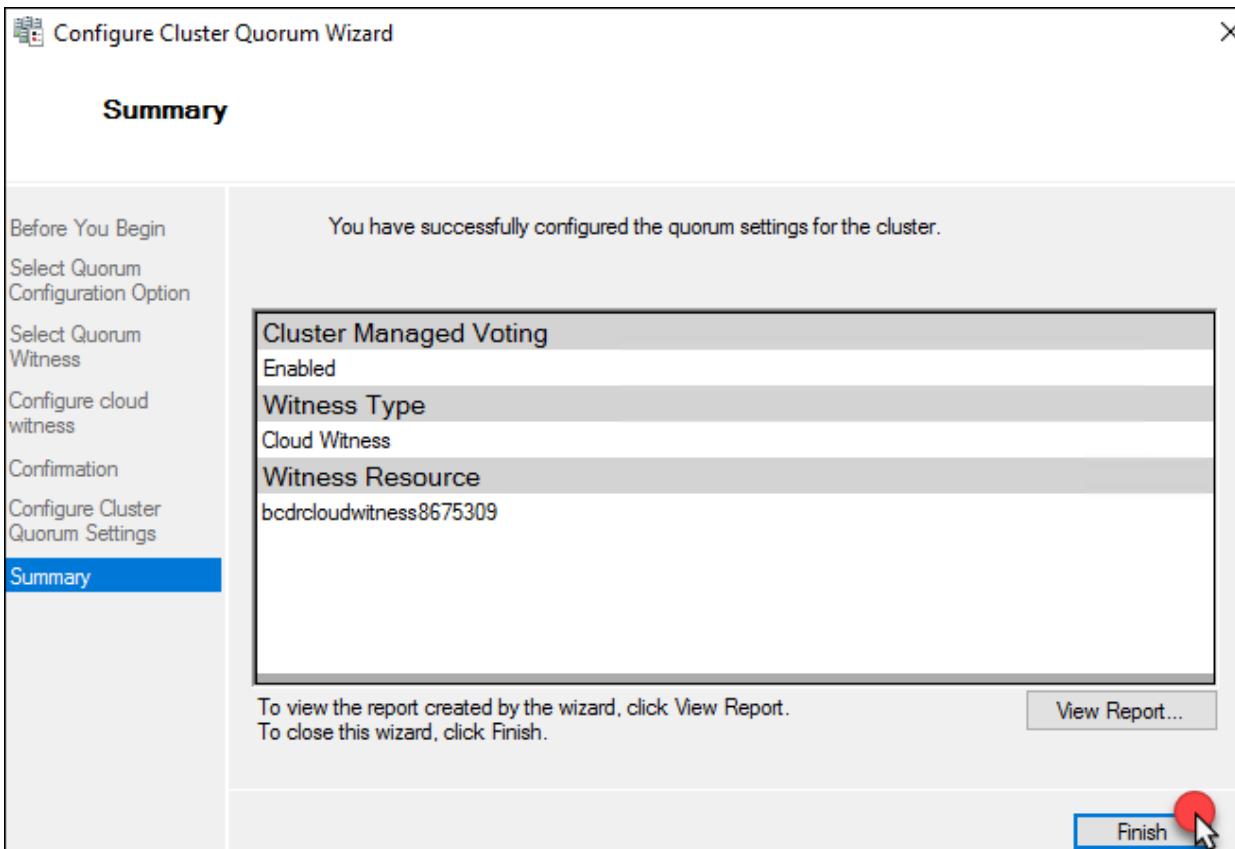
To continue, click Next.

< Previous

Next >

Cancel

20. Select **Finish**.



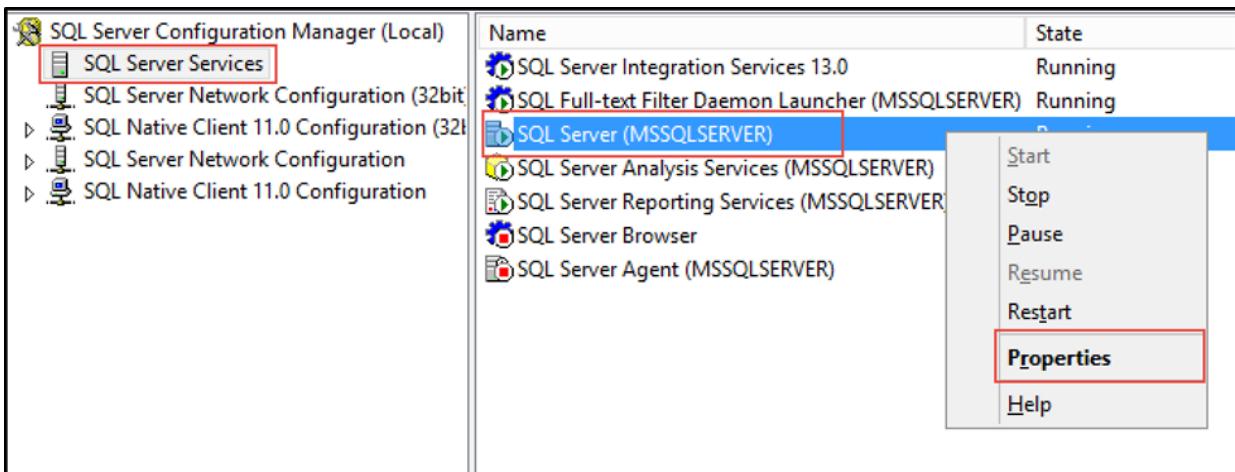
21. Select the name of the Cluster again, and the **Cloud Witness** should now appear in the **Cluster Resources**. It is important to always use a third data center; in your case, a third Azure Region is used for your Cloud Witness.



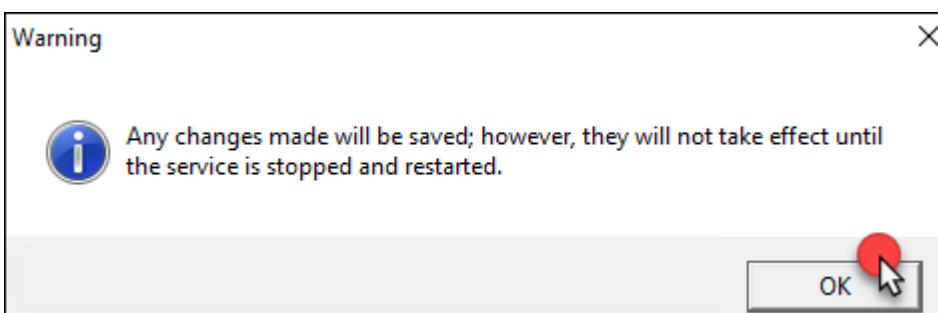
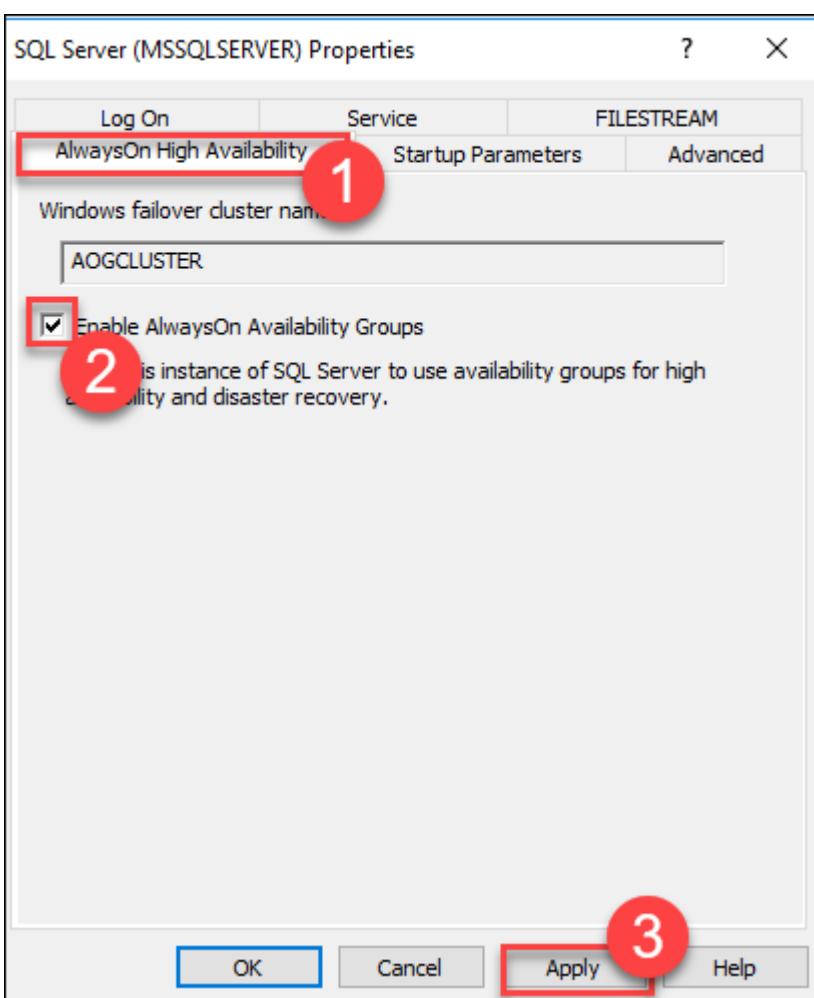
22. Select **Start** and launch **SQL Server 2017 Configuration Manager**.



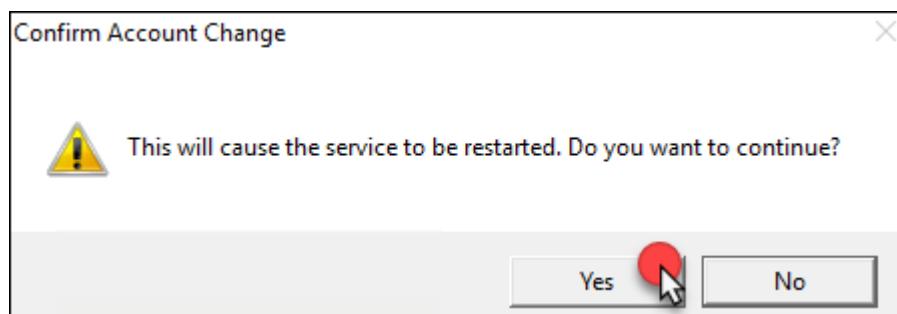
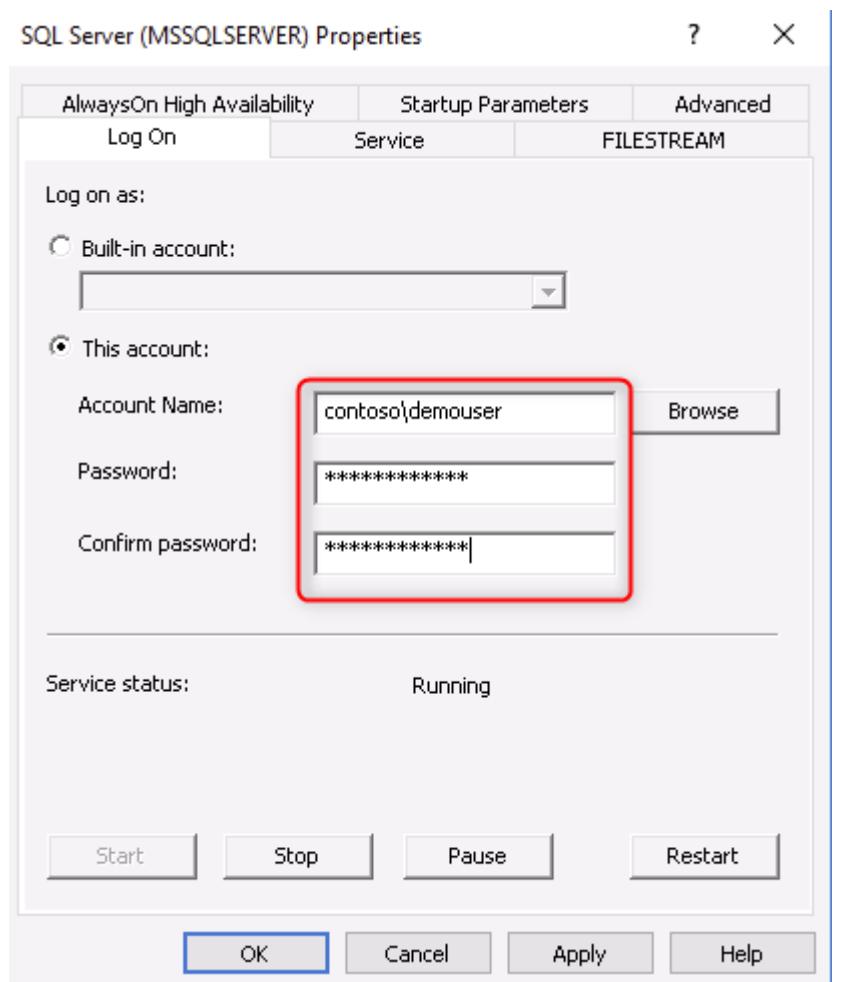
23. Select **SQL Server Services**, then right-click **SQL Server (MSSQLSERVER)** and select **Properties**.



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

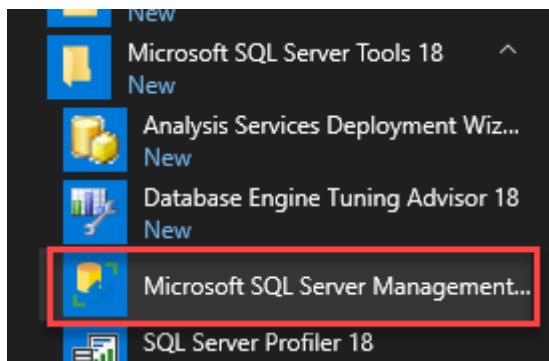


25. On the **Log On** tab, change the service account to **contoso\adadmin** with the password **Demo!pass123**. Select **OK** to accept the changes, and then select **Yes** to confirm the restart of the server.

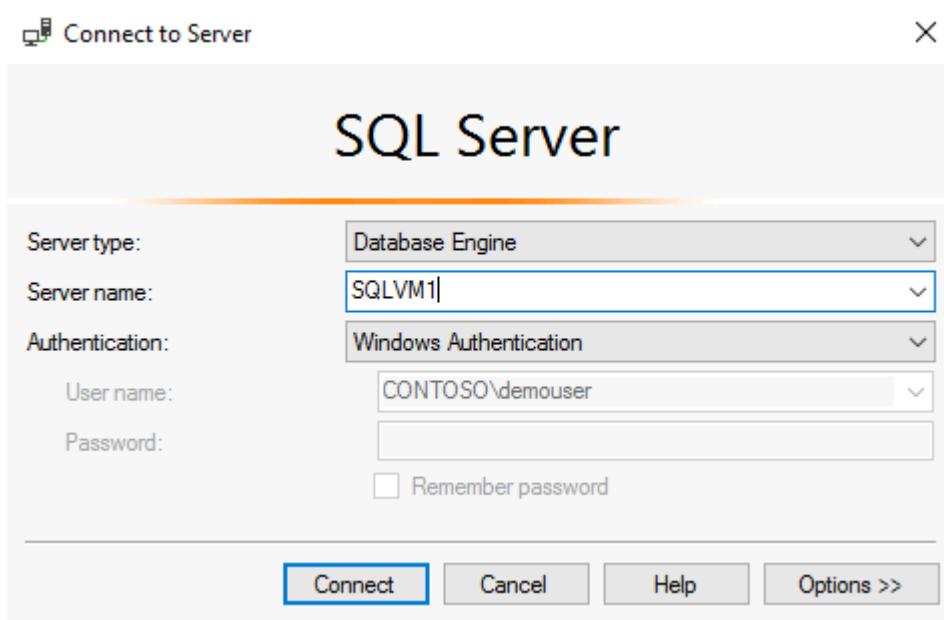


26. Return to the Azure portal and open a new Azure Bastion session to **SQLVM2**. Launch **SQL Server 2017 Configuration Manager** and repeat the steps above to **Enable SQL AlwaysOn** and change the **Log On** username. Make sure that you have restarted the SQL Service.

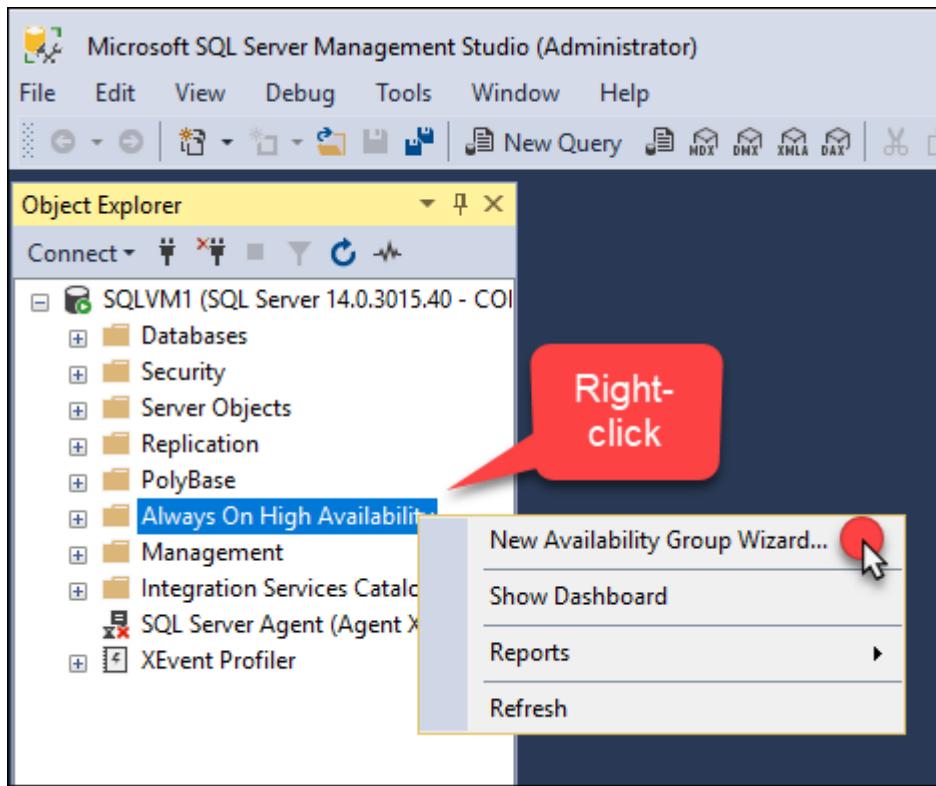
27. Return to your session with **SQLVM1**. Use the Start menu to launch **Microsoft SQL Server Management Studio 18** and connect to the local instance of SQL Server. (Located in the Microsoft SQL Server Tools folder).



28. Select **Connect** to sign on to **SQLVM1**. **Note:** The username for your lab should show **CONTOSO\adadmin**.



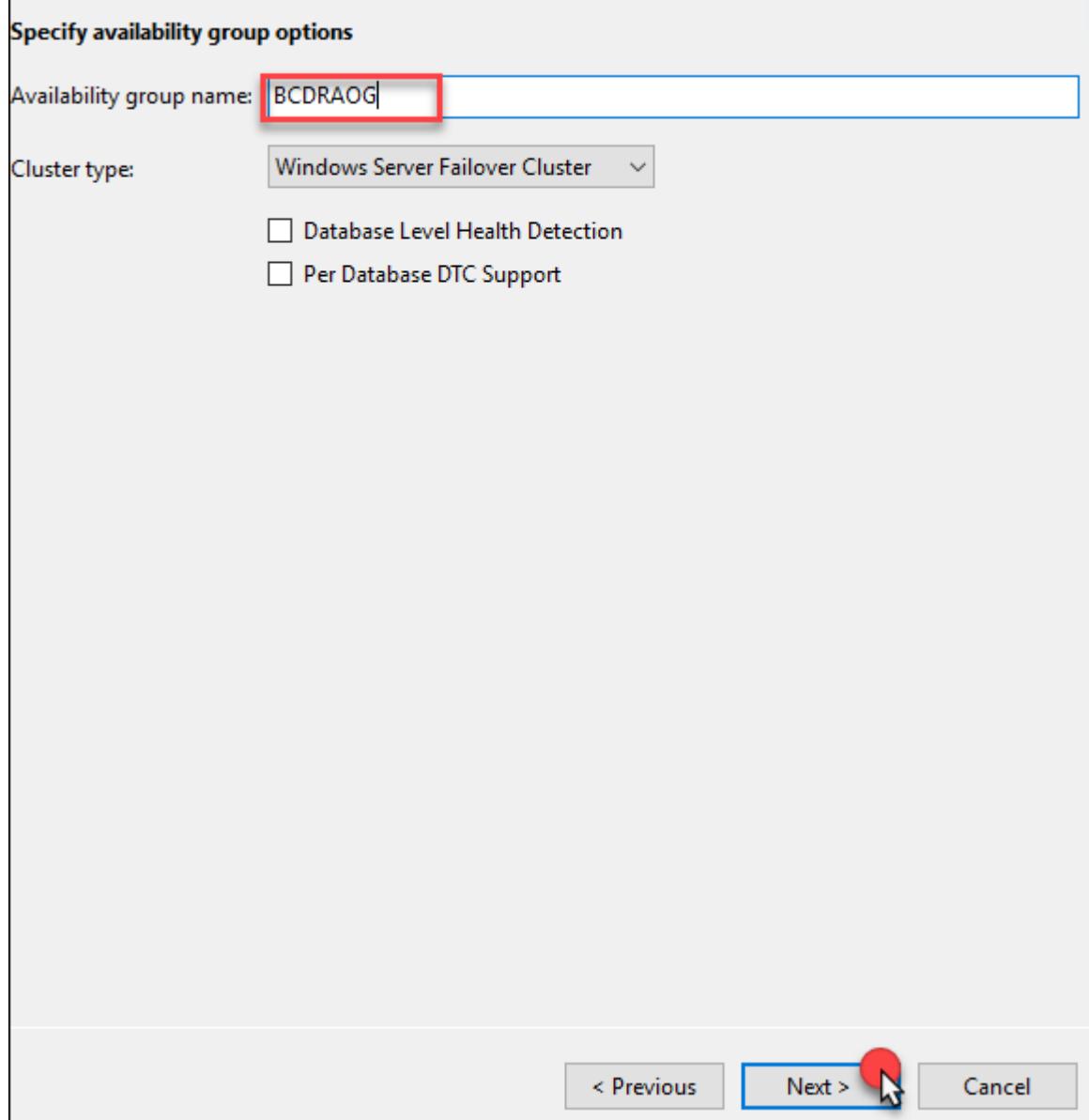
29. Right-click **Always On High Availability**, then select **New Availability Group Wizard**.



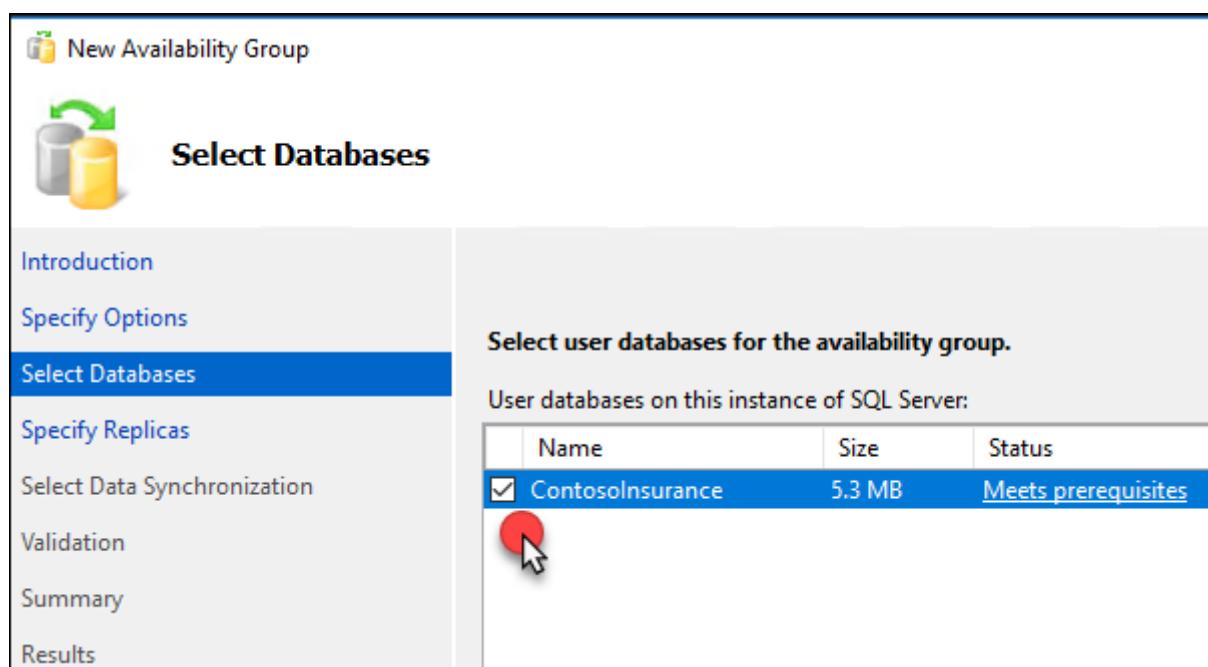
30. Select **Next** on the Wizard.



31. Provide the name **BCDRAOG** for the **Availability group name**, then select **Next**.



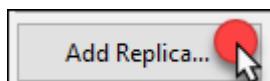
32. Select the **ContosoInsurance Database**, then select **Next**.



33. On the **Specify Replicas** screen next to **SQLVM1**, select **Automatic Failover**.

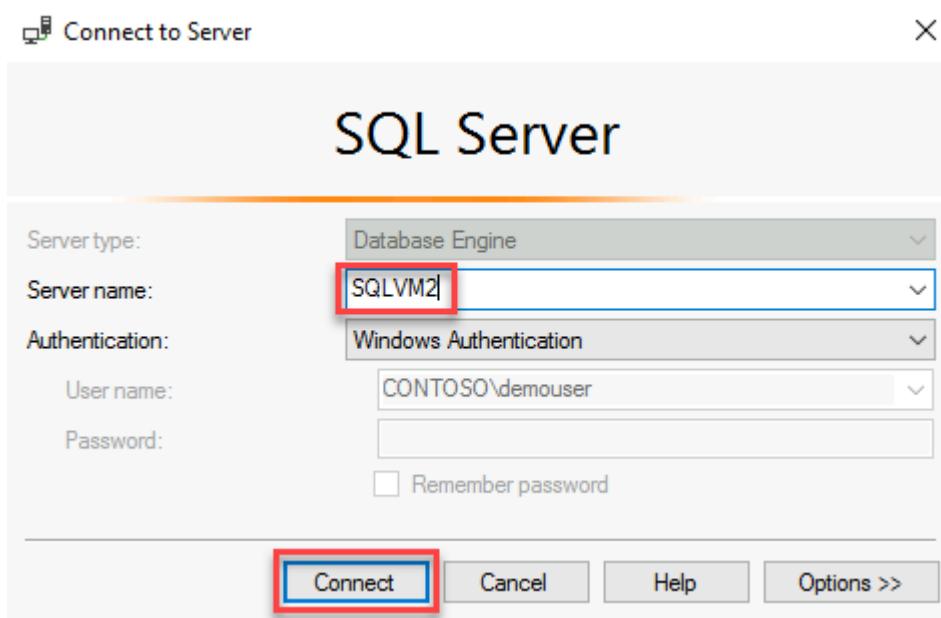
Server Instance	Initial Role	Automatic Failover (Up to 3)	Availability Mode	Readable Secondary
SQLVM1	Primary	<input checked="" type="checkbox"/>	Synchronous commit	No

34. Select **Add Replica**.



35. On the **Connect to Server** dialog box, enter the Server Name of **SQLVM2** and select **Connect**.

Note: The username for your lab should show **CONTOSO\adadmin**.



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

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"/>	<input checked="" type="checkbox"/>	Synchronous commit

37. Select **Endpoints** and review these that the wizard has created.

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

Replicas Endpoints Backup Preferences Listener Read-Only Routing

Endpoint values:

Server Name	Endpoint URL	Port Number	End Nar
SQLVM1	TCP://SQLVM1.contoso.com:5022	5022	Had
SQLVM2	TCP://SQLVM2.contoso.com:5022	5022	Had

38. 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.

39. Add the following details:

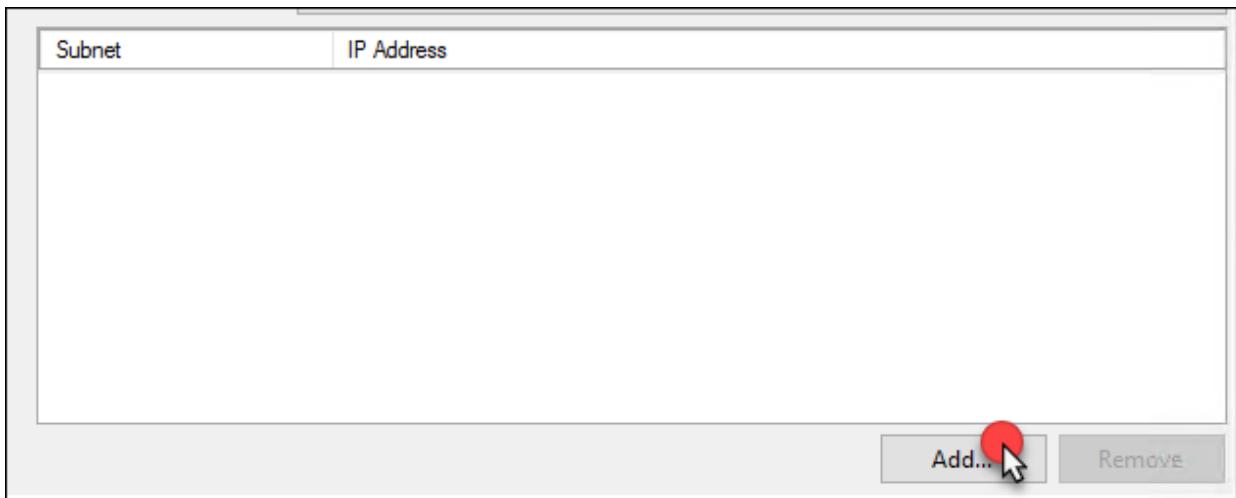
- **Listener DNS Name:** BCDRAOG
- **Port:** 1433
- **Network Mode:** Static IP

Listener DNS Name: BCDRAOG

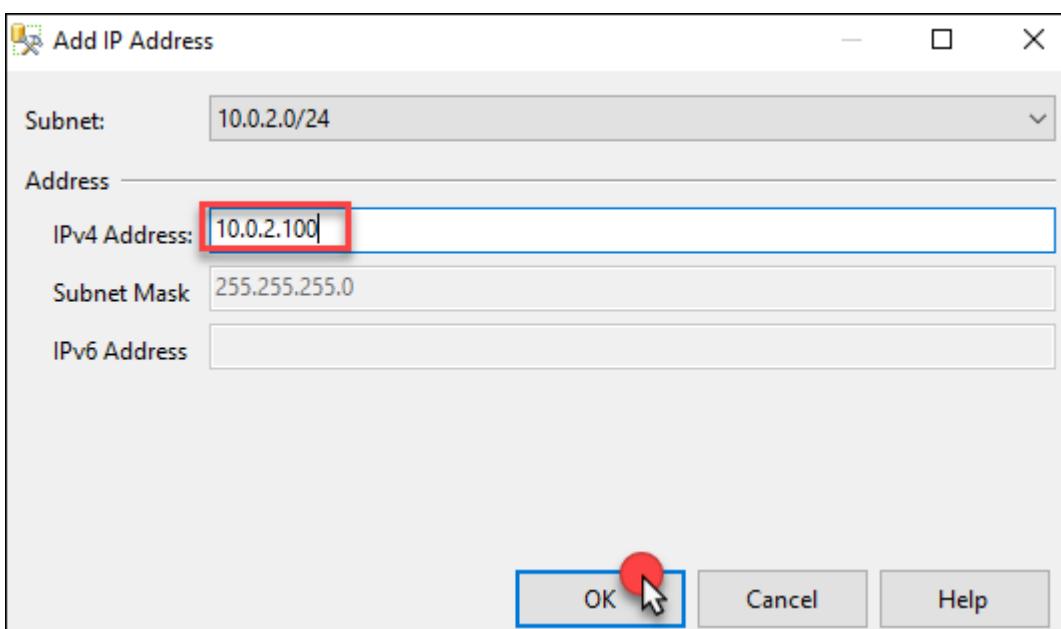
Port: 1433

Network Mode: Static IP

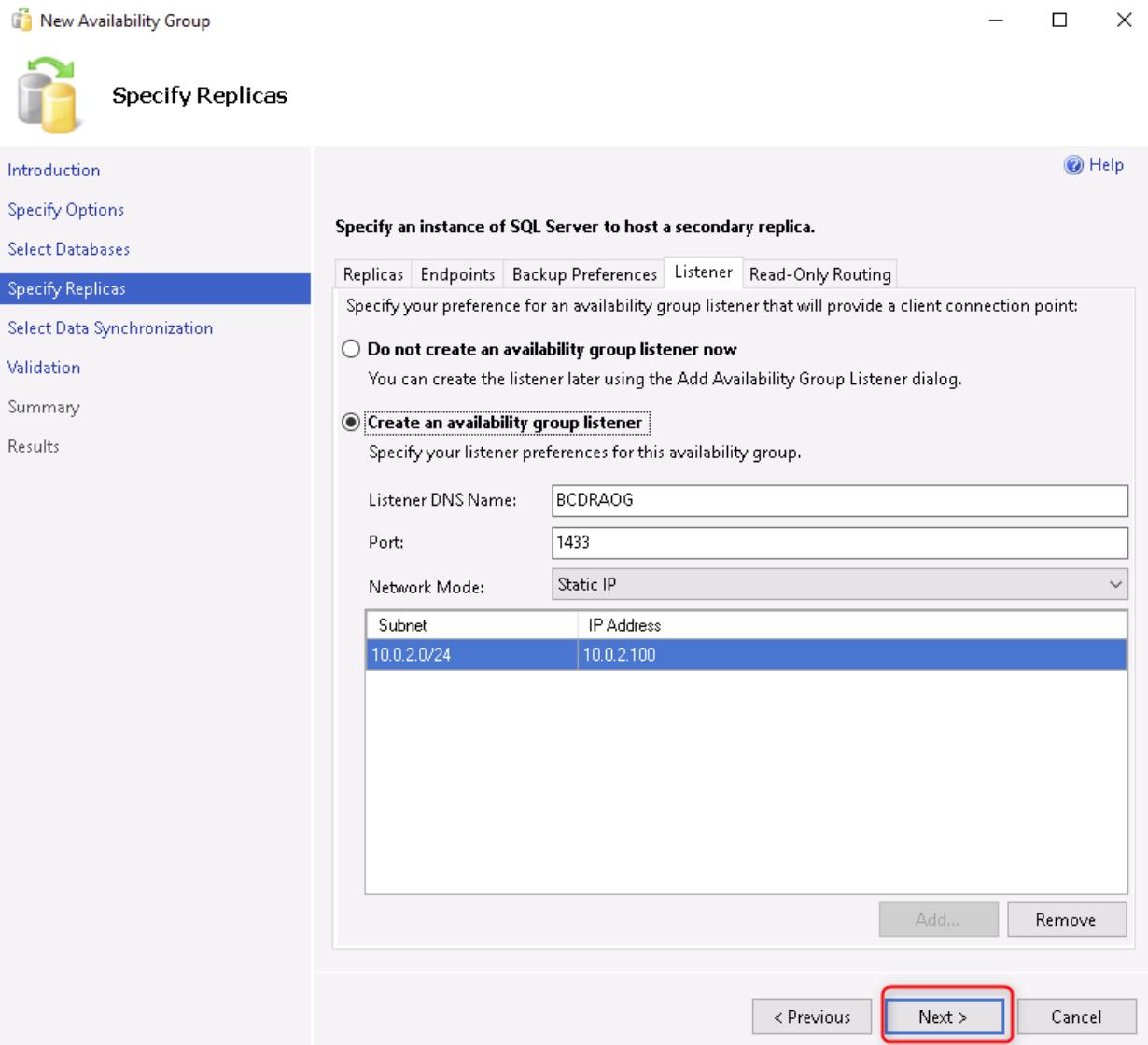
40. Next, select **Add**.



41. Select the Subnet of **10.95.2.0/24** and then add IPv4 **10.95.2.100** and select **OK**. This is the IP address of the Internal Load Balancer that is in front of the **SQLVM1** and **SQLVM2** in the **Data** subnet running in the **Primary** Site.



42. Select **Next**.



43. On the **Select Initial Data Synchronization** screen, ensure that **Automatic seeding** is selected and select **Next**.

Select your data synchronization preference.

Automatic seeding

SQL Server automatically creates databases for every selected secondary replica. Automatic seeding requires that the data and log file paths are the same on every SQL Server instance participating in the availability group.

Full database and log backup

Starts data synchronization by performing full database and log backups for each selected database. These databases are restored to each secondary and joined to the availability group. Make sure the file share is accessible to all replicas and is mounted to the same directory on all Linux replicas.

Specify the file share path in Windows format:

 Browse...

Specify the file share location in Linux format:

Join only

Starts data synchronization where you have already restored database and log backups to each secondary server. The selected databases are joined to the availability group on each secondary.

Skip initial data synchronization

Choose this option if you want to perform your own database and log backups of each primary database.

< Previous

Next > 

Cancel

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



Validation

Introduction

[Help](#)

Specify Options

Select Databases

Specify Replicas

Select Data Synchronization

Validation

Summary

Results

Results of availability group validation.

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 second..	Success
Checking for the existence of the database files on the server instance that hosts seconda..	Success
Checking for compatibility of the database file locations on the server instance that host..	Success
Checking whether the endpoint is encrypted using a compatible algorithm	Success
Checking replica availability mode	Success
Checking the listener configuration	Success

[Re-run Validation](#)[< Previous](#)[Next >](#)[Cancel](#)

45. On the Summary page, select **Finish**.

Verify the choices made in this wizard.

Click Finish to perform the following actions:

The screenshot shows the 'Review' step of the SQL Server Availability Group Wizard. It displays a tree view of configuration settings:

- Availability group: BCDRAOG**
 - Primary replica: SQLVM1
 - Cluster type: Windows Server Failover Cluster
 - Availability group listener: BCDRAOG
 - Automated backup preference: Secondary
 - Database health trigger: False
 - Required synchronized secondaries to commit: 0
 - Per database DTC support enabled: False
- Databases**
 - AdventureWorks (207.0 MB)
- Initial data synchronization: Automatic Seeding**
- Replicas**
 - Server instance name: SQLVM1**
 - Role: Primary
 - Availability mode: Synchronous commit
 - Failover mode: Manual
 - Readable secondary: No
 - Read-only routing URL:
 - Read-only routing list:
 - Automated backup priority: 50
 - Endpoint: Hadr_endpoint**
 - URL: TCP://SQLVM1.contoso.com:5022
 - Encrypted: Yes
 - Service account: contoso\mcwadmin

At the bottom right, there are buttons for **< Previous**, **Finish** (which has a red circle over it), and **Cancel**. A **Script** button is also present.

46. Once the AOG is built, check that each task was successful and select **Close**.

New Availability Group

Results

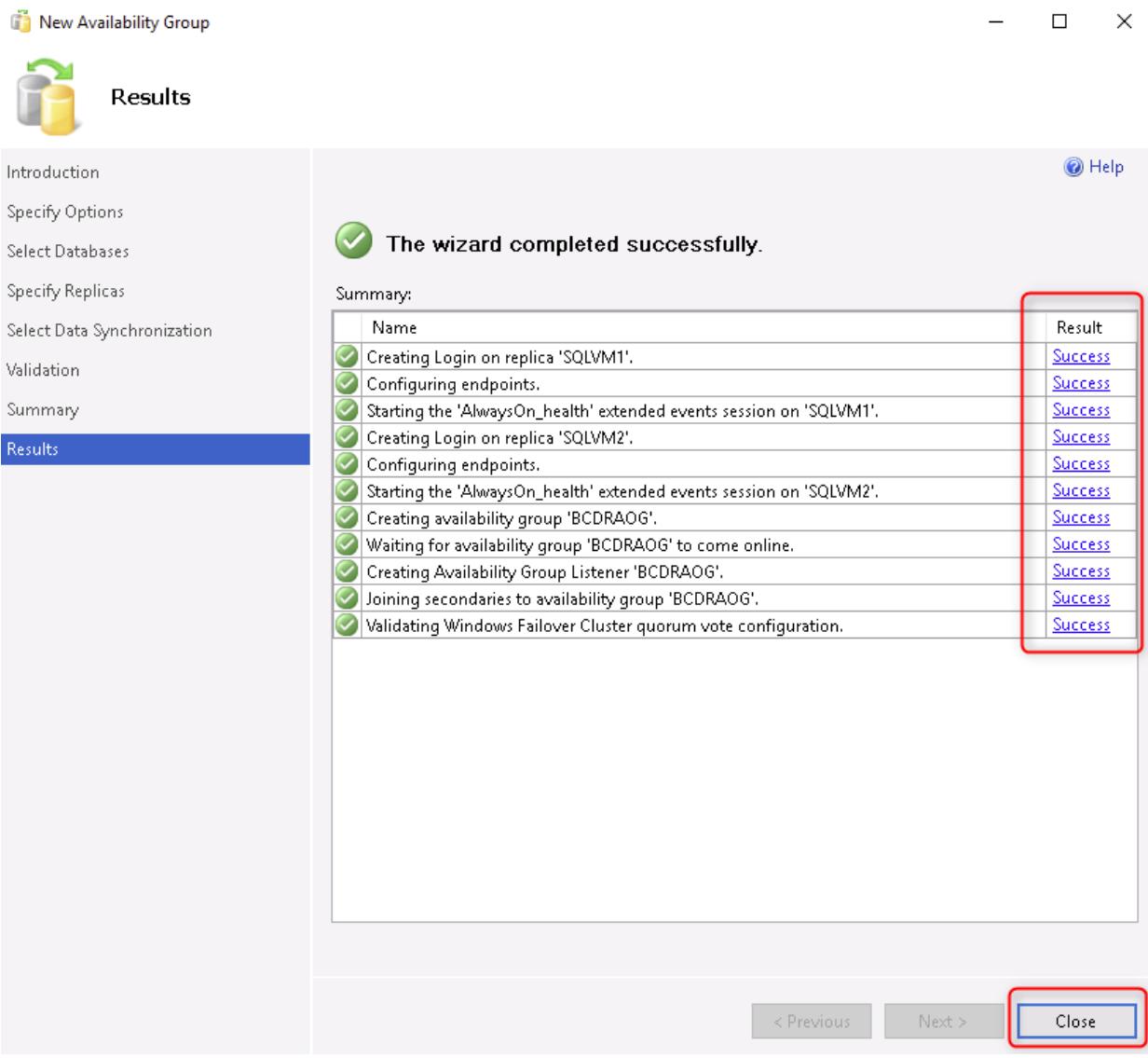
Introduction
Specify Options
Select Databases
Specify Replicas
Select Data Synchronization
Validation
Summary
Results

The wizard completed successfully.

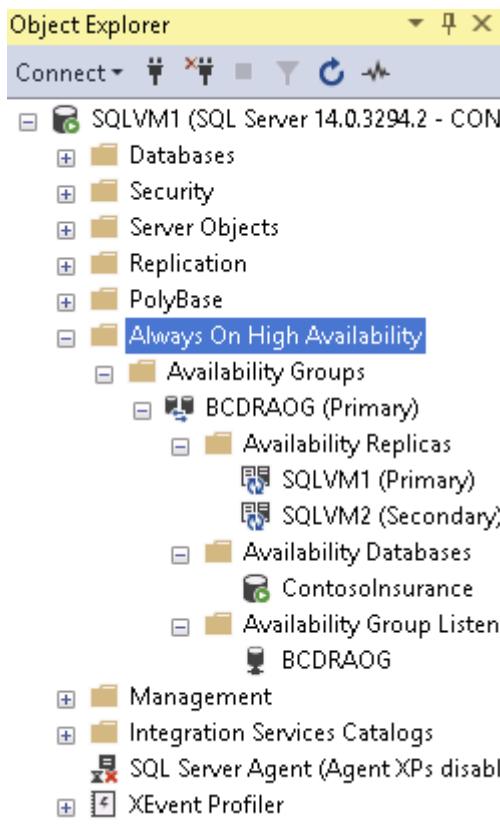
Summary:

Name	Result
Creating Login on replica 'SQLVM1'.	Success
Configuring endpoints.	Success
Starting the 'AlwaysOn_health' extended events session on 'SQLVM1'.	Success
Creating Login on replica 'SQLVM2'.	Success
Configuring endpoints.	Success
Starting the 'AlwaysOn_health' extended events session on 'SQLVM2'.	Success
Creating availability group 'BCDRAOG'.	Success
Waiting for availability group 'BCDRAOG' to come online.	Success
Creating Availability Group Listener 'BCDRAOG'.	Success
Joining secondaries to availability group 'BCDRAOG'.	Success
Validating Windows Failover Cluster quorum vote configuration.	Success

< Previous Next > **Close**



47. Move back to **SQL Management Studio** on **SQLVM1** and expand the **Always On High Availability** item in the tree view. Under Availability Groups, expand the **BCDRAOG (Primary)** item.



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

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

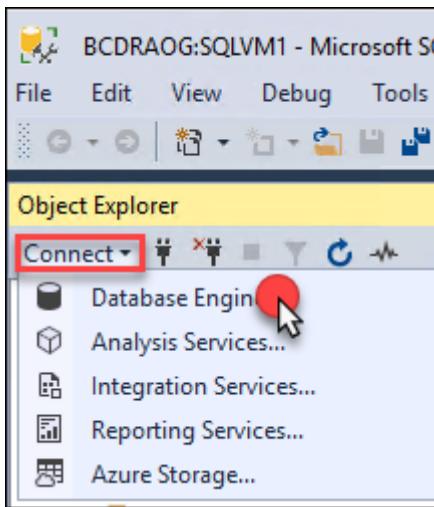
Availability replica:

Name	Role	Availability Mode	Failover Mode	Seeding Mode	Synchronization State	Issues
SQLVM1	Primary	Synchronous co...	Automatic	Automatic	Synchronized	
SQLVM2	Secon...	Synchronous co...	Automatic	Automatic	Synchronized	

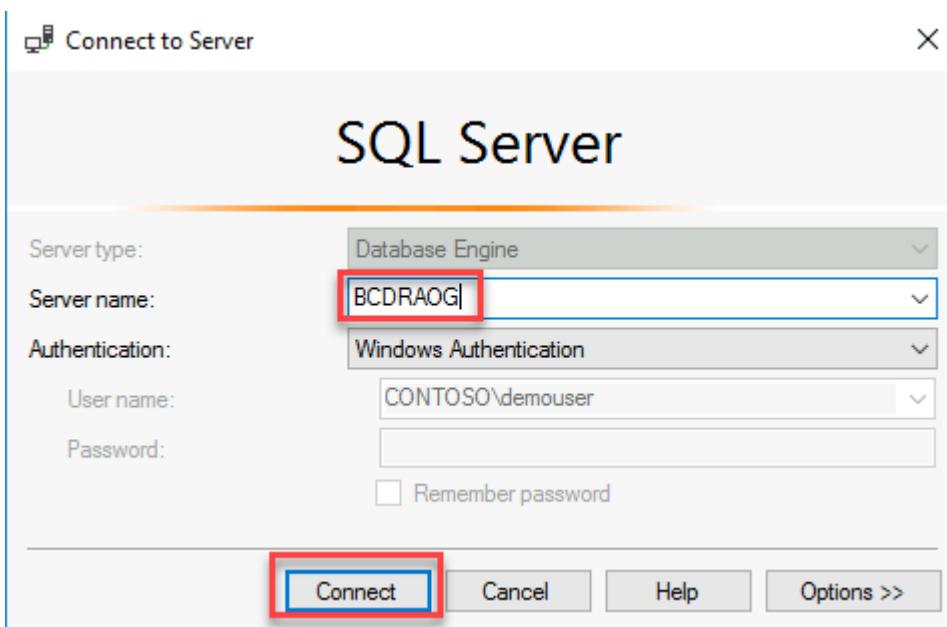
Group by ▾

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

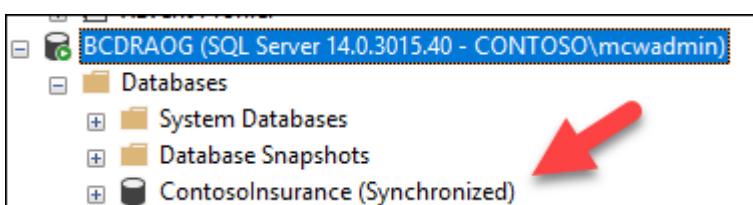
49. Next, select **Connect** and then **Database Engine** in SQL Management Studio.



50. Enter **BCDRAOG** as the Server Name. This will be connected to the listener of the group that you created. **Note:** The username for your lab should show **CONTOSO\adadmin**.



51. Once connected to the **BCDRAOG**, you can select **Databases** and will be able to see the database there. Notice that you do not know directly which server this is running on.



52. Move back to **PowerShell** on **SQLVM1**. Open a new file, paste in the following script, and select the **Play** button. This will update the Failover cluster with the IP address of the Listener that you created for the AOG.

```
$ClusterNetworkName = "Cluster Network 1"
$IPResourceName = "BCDRAOG_10.95.2.100"
$ILBIP = "10.22.2.100"
```

```

Import-Module FailoverClusters
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
@{ "Address" = "$ILBIP"; "ProbePort" = "59999"; "SubnetMask" = "255.255.255.255"; "Network" = "$ClusterNetworkName"; "EnableDhcp" = 0}
Stop-ClusterResource -Name $IPResourceName
Start-ClusterResource -Name "BCDRAOG"

```

```

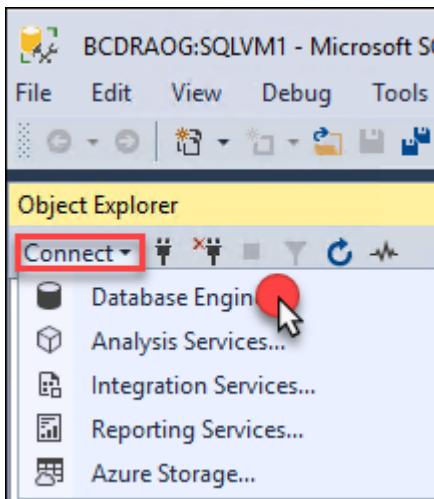
PS C:\Users\demouser.CONTOSO> $ClusterNetworkName = "Cluster Network 1"
>> $IPResourceName = "BCDRAOG_10.0.2.100"
>> $ILBIP = "10.0.2.100"
>> Import-Module FailoverClusters
>> Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple @{ "Address" = "$ILBIP"; "ProbePort" = "59999"; "SubnetMask" = "255.255.255.255"; "Network" = "$ClusterNetworkName"; "EnableDhcp" = 0}
>> Stop-ClusterResource -Name $IPResourceName
>> Start-ClusterResource -Name "BCDRAOG"
WARNING: The properties were stored, but not all changes will take effect until BCDRAOG_10.0.2.100 is taken offline and then online again.

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

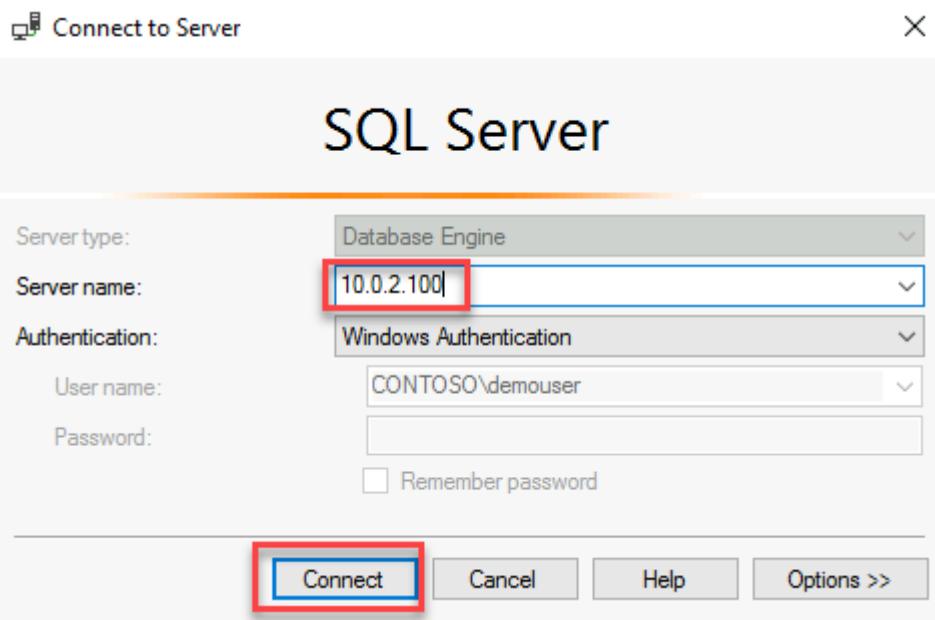
PS C:\Users\demouser.CONTOSO>

```

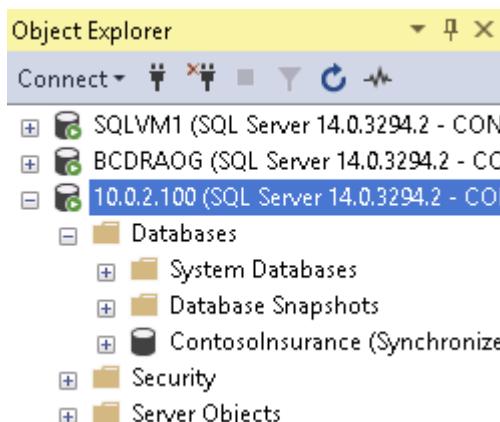
53. Move back to SQL Management Studio, select **Connect**, and then **Database Engine**.



54. This time, put the following into the IP address of the Internal Load balancer of the **Primary** Site AOG Load Balancer: **10.95.2.100**. You again will be able to connect to the server, which is up and running as the master. **Note:** The username for your lab should show **CONTOSO\adadmin**.

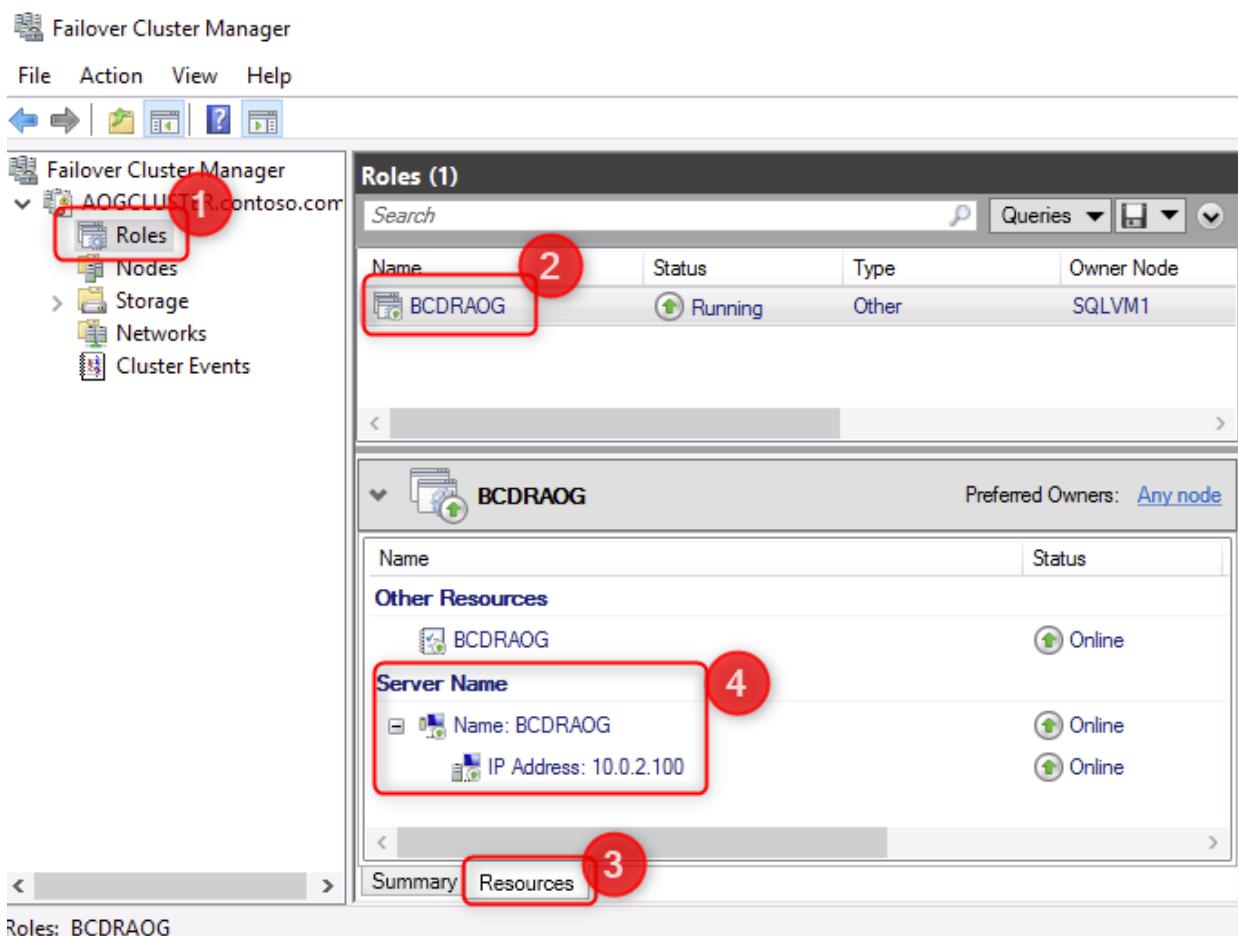


55. Once connected to **10.95.2.100**, you can select **Databases** and will be able to see the database there. Notice that you do not know directly which server this is running on.



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

56. 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 **10.95.2.100** is Online.



You have now successfully set up the SQL Server VMs to use Always On Availability Groups with a Cloud Witness storage account located in another region.

Task 4: Configure HA for the Web tier

In this task, you will configure a high-availability web tier. This comprises two web server VMs, which you will locate behind an Azure load balancer. You will also configure the VMs to access the database using the Always On Availability Group endpoint you created earlier.

1. In the Azure portal, navigate to **WebVM1**, select **Connect** followed by **Bastion**, and connect to the VM using the following credentials:

- **Username:** adadmin@contoso.ins
- **Password:** Demo!pass123

2. In **WebVM1**, open Windows Explorer, navigate to **C:\inetpub\wwwroot** and open the **Web.config** file using Notepad.

Note: If the **Web.config** change does not run, go to **Start**, **Run** and type **iisreset /restart** from command line.

3. In the **Web.config** file, locate the **<ConnectionStrings>** element and replace **SQLVM1** with **BCDRAOG** in the data source. Remember to **Save** the file.

```

Web - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8"?>
<!--
For more information on how to configure your ASP.NET application, please visit
http://go.microsoft.com/fwlink/?LinkId=301880
-->
<configuration>
  <configSections>
    <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSection, EntityFr
      <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237
    </configSections>
    <connectionStrings>
      <add name="DefaultConnection" connectionString="data source= \SQLEXPRESS;initial catalog=ContosoInsurance;per
        <add name="PolicyConnect" connectionString="data source=BCDRAOG.contoso.com;initial catalog=ContosoInsurance;
    </connectionStrings>
    <appSettings>
      <add key="webpages:Version" value="3.0.0.0" />

```

4. Repeat the above steps to make the same change on **WebVM2**.

5. Return to the Azure portal and navigate to the **ContosoWebLBPrimary** load balancer blade. Select **Backend pools** and open **BackEndPool1**.

The screenshot shows the Azure portal interface for managing a load balancer named 'ContosoWebLBPrimary'. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Frontend IP configuration, Backend pools (which is selected and highlighted with a red box), Health probes, and Load balancing rules. The main content area displays the 'Backend pools' blade. At the top, there is a search bar, an 'Add' button, a 'Refresh' button, and a 'Give feedback' link. Below the search bar is a 'Filter by name...' input field and a dropdown menu set to 'Backend pool == all'. The main table lists a single entry under 'Backend pool': 'BackEndPool1'. This entry is also highlighted with a red box. The table has columns for 'Backend pool' and 'Resource Name'.

6. In the **BackendPool1** blade, select **VNet1 (ContosoRG1)** as the Virtual network. Then select **+ Add** and select the two web VMs. Select **Save**.

BackEndPool1

ContosoWebLBPrimary

Name: BackEndPool1 1

Virtual network *: VNet1 (ContosoRG1) 1

Backend Pool Configuration:

- NIC
- IP Address

IP Version:

- IPv4
- IPv6

Virtual machines

You can only attach virtual machines in eastus2 that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

2 + Add X Remove

<input type="checkbox"/> Virtual machine ↑↓	IP Configuration ↑↓	Availability set ↑↓
<input type="checkbox"/> WebVM1	ipconfig1 (10.0.1.4)	-
<input type="checkbox"/> WebVM2	ipconfig1 (10.0.1.5)	-

Virtual machine scale sets

Virtual Machine Scale Sets must be in same location as Load Balancer. Only IP configurations that have the same SKU (Basic/Standard) as the Load Balancer can be selected. All of the IP configurations have to be in the same Virtual Network.

3 i No virtual machine scale set is found in eastus2 that matches the above criteria

Virtual machine scale set Save Cancel Give feedback

7. You will now check that the Contoso sample application is working when accessed through the load-balancer. In the Azure portal, navigate to the **ContosoWebLBPrimaryIP** resource. This is the public IP address attached to the web tier load balancer front end. Copy the **DNS name** to the clipboard.

4 ContosoWebLBPrimaryIP Public IP address

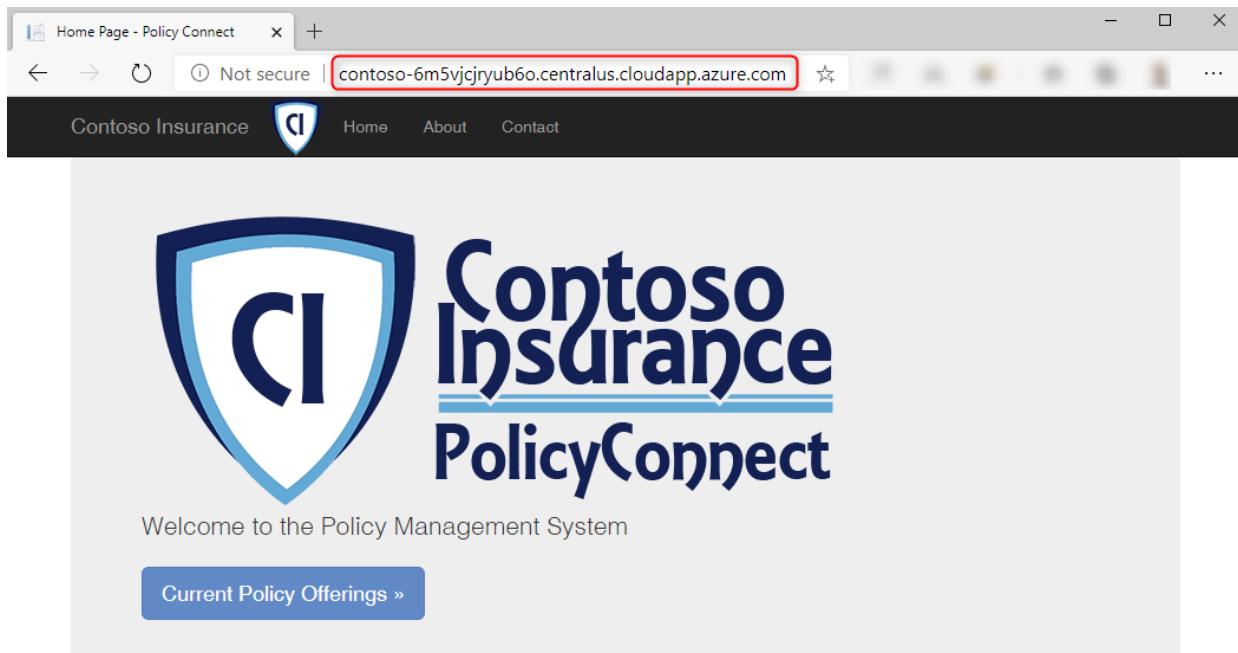
Search (Cmd+ /) Associate Dissociate Move Delete Refresh

Overview Associate Dissociate Move Delete Refresh

Essentials

Resource group (move) : ContosoRG1	SKU : Standard
Location : East US 2 (Zone 1, 2, 3)	Tier : Regional
Subscription (move) : Demo Creation	IP address : 20.96.144.96
Subscription ID : e223f1b3-d19b-4cfa-98e9-bc9be62717bc	DNS name : contoso-2uy3.eastus2.cloudapp.azure.com Copy to clipboard
	Associated to : ContosoWebLBPrimary

8. Open a new browser tab and paste the DNS name. The Contoso Insurance sample app is shown.



Note: You will test the HA capabilities later in the lab.

Exercise 2: Enable Disaster Recovery for the Contoso application

Duration: 90 minutes

In this exercise, you will enable a secondary DR site in East US 2. This site will support each tier of the Contoso application, using a different technology in each case. The DR approach is summarized in the following table.

Tier	DR Strategy
Web	Failover using Azure Site Recovery
SQL	Secondary SQL Always On Availability Group replica, with asynchronous replication. Failover steps are integrated into Azure Site Recovery using Azure Automation.
AD	Active-active domain controllers

Task 1: Deploy DR resources

In this task, you will deploy the resources used by the DR environment. First, you will deploy a template to create the network and virtual machines. You will then manually deploy the Recovery Services Vault and Azure Automation account that Azure Site Recovery uses.

1. In a new browser tab, navigate to **https://shell.azure.com**. You will be redirected to **https://portal.azure.com/#cloudshell** automatically. Open a **PowerShell** session, and create a Cloud Shell storage account if prompted to do so.

2. Update the **-Location** parameter in each of the commands below to be a different location than **ContosoRG11**. Execute the commands. These commands will create the DR resource group and deploy the DR resources.

You can proceed to the following tasks while the template deployment is in progress.

```
New-AzResourceGroup -Name 'ContosoRG2' -Location 'East US 2'

New-AzSubscriptionDeployment -Name 'Contoso-IaaS-DR' ` 
    -TemplateUri 'https://raw.githubusercontent.com/yungchou/bcdr/main/'
```

Hands-on%20lab/Resources/templates/contoso-iaas-dr.json`
`-Location 'East US 2'
`
`

> ****Note**:** If your deployment fails with an error *``The requested size for resource '<resourceID>' is currently not available``*, add the parameter `-skuSizeVM 'D2s_v5'` to the end of the `New-AzSubscriptionDeployment` and rerun the command:

```
```powershell
Only run this command if the previous deployment failed with an error that
size was not available
New-AzSubscriptionDeployment -Name 'Contoso-IaaS-DR-SKU' `
 -TemplateUri 'https://raw.githubusercontent.com/yungchou/bcdr/main/'
```

Hands-on%20lab/Resources/templates/contoso-iaas-dr.json`  
`-Location 'East US 2' -skuSizeVM 'D2s\_v5'  
`  
`

3. Take a few minutes to review the template while it deploys. Navigate to the Azure portal home page, select **Subscriptions**, then **Deployments** to review the template and deployment progress. Note that the template includes:

- A DR virtual network, which is connected using VNet peering to the existing virtual network.
- Two additional domain controller VMs, **ADVM3** and **ADVM4**.
- An additional SQL Server VM, **SQLVM3**.
- Azure Bastion, to enable VM access.

The screenshot shows the Azure portal interface. On the left, the 'Resource groups' blade is open, displaying two resource groups: 'ContosoRG1' and 'ContosoRG2'. 'ContosoRG2' is selected and highlighted with a red box. On the right, the 'ContosoRG2 | Deployments' blade is open, showing a list of deployments. Each deployment entry includes a checkbox, the deployment name, and its status. A red box highlights the 'Status' column, which shows all entries as 'Succeeded' with green checkmarks. The deployment names listed are: SQLVM3, VirtualNetworkSecondaryWithSecondary..., ADVM3, ADVM4, VirtualNetworkSecondaryWithPrimaryDNS, VNet2-to-VNet1-deploy, LoadBalancersSecondary, Bastion, and VirtualNetworkSecondary.

Deployment name	Status
SQLVM3	Succeeded
VirtualNetworkSecondaryWithSecondary...	Succeeded
ADVM3	Succeeded
ADVM4	Succeeded
VirtualNetworkSecondaryWithPrimaryDNS	Succeeded
VNet2-to-VNet1-deploy	Succeeded
LoadBalancersSecondary	Succeeded
Bastion	Succeeded
VirtualNetworkSecondary	Succeeded

Next, you will create the Recovery Services Vault used to replicate the Web tier VMs and orchestrate the cross-site failover.

4. From the Azure portal, select **+Create a resource**, search for and select **Backup and Site Recovery**, and select **Create**.
5. Complete the **Recovery Services Vault** blade using the following inputs, then select **Review and Create**, followed by **Create**:

- **Resource Group:** ContosoRG2
- **Name:** **BCDRRSV**
- **Location:** East US 2 (*your secondary region*)

# Create Recovery Services vault

Preview

\* Basics Tags Review + create

## Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription \* ⓘ



Resource group \* ⓘ

 ContosoRG2

1

[Create new](#)



## Instance Details

Vault name \* ⓘ

 BCDRRSV

2

Region \* ⓘ

 East US 2

3

[Review + create](#)

4

[Next: Tags](#)

- Once the **BCDRRSV** Recovery Service Vault has been created, open it in the Azure portal and select the **Site Recovery** tab.

## Essentials

[Overview](#) [Backup](#)

[Site Recovery](#)

- This is your dashboard for Azure Site Recovery (ASR).

Essentials

JSON View

Overview Backup Site Recovery

Replication health ([View all VMs](#)) Failover health ⓘ Configuration issues ⓘ Recovery Plans

**0** Critical 0 Healthy 0 Warning 0 Not Applicable... **0** Critical 0 Healthy 0 Warning 0 Not applicable... **0** No errors 0

Recovery Plan	Count
LabVM	0

**Important:** Next, you will set up the Azure Automation account that will be used to automate certain failover and fallback tasks. This will require several PowerShell scripts to be imported as Azure Automation runbooks. **Be sure to execute the following steps from the LabVM since that is where the scripts are located.**

8. From the Azure portal, select **+Create a resource**, followed by **IT & Management Tools**, then **Automation**.
9. Complete the **Add Automation Account** blade using the following inputs and then select **Review + Create** followed by **Create**:

- **Name:** Enter a Globally unique name starting with **BCDR**.
- **Resource group:** Use existing / **ContosoRG2**
- **Location:** Any region that support automation **except for** your primary region.

Home > Create a resource >

## Create an Automation Account

Basics Advanced Networking Tags Review + Create

Create an Automation Account to hold the Automation runbooks & configuration used for automating operations and management tasks around Azure and non-Azure resources. You could execute cloud jobs in a serverless environment or use hybrid jobs on your compute via Azure Virtual machines or Arc-enabled servers. [Learn more](#)

Subscription \* ⓘ

Resource group \* ⓘ

ContosoRG2

[Create new](#)

### Instance Details

Automation account name \* ⓘ

BCDRContoso22

Region \* ⓘ

West US 2

**Review + Create**

Previous

Next

**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 required to have your Azure Automation account in the same region as the failover resources, but it **CANNOT** be in your primary region.

10. Once the Azure automation account has been created, select **Run as accounts** under **Account Settings**. Then, select **Create** under **Azure Run as Account**.

**BCDRContoso22 | Run as accounts**

Automation Account

- Search (Cmd+ /)
- Schedules
- Modules
- Python packages
- Credentials
- Connections
- Certificates
- Variables

**Related Resources**

- Linked workspace
- Event grid
- Start/Stop VM

**Account Settings**

- Properties
- Networking
- Keys
- Pricing
- Source control
- Run as accounts** (highlighted with red box 1)
- Identity

We recommend using Managed Identities for the Automation accounts instead of using Runas. Managed  
Read here on how to use Managed Identities.

Run As accounts in Azure Automation are used to provide authentication for managing resources in Azure with the documentation below to learn more about Run As accounts.

Create a Run As account  
Permissions required to configure Run As accounts  
Permissions required to configure Classic Run As accounts  
Limit Run As accounts permissions  
Extend Run As accounts permissions to other subscriptions  
Resolve incomplete Run As accounts  
Renew self-signed certificate of Run As accounts

+ Azure Run As Account ⓘ  
**Create** (highlighted with red box 2)

+ Azure Classic Run As Account ⓘ  
**Create**

11. Select Create. Once the deployment has finished, you'll have a new Azure Run As Account listed with an expiration date.

**BCDRContoso22 | Run as accounts**

Automation Account

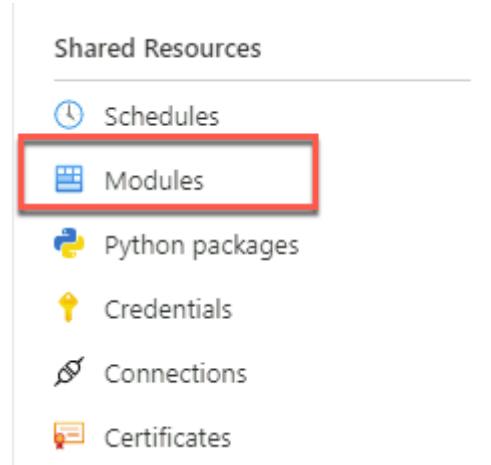
Run As accounts in Azure Automation are used to provide authentication for managing resources in Azure with the documentation below to learn more about Run As accounts.

Create a Run As account  
Permissions required to configure Run As accounts  
Permissions required to configure Classic Run As accounts  
Limit Run As accounts permissions  
Extend Run As accounts permissions to other subscriptions  
Resolve incomplete Run As accounts  
Renew self-signed certificate of Run As accounts

**Azure Run As Account** ⓘ  
Expires 5/9/2023, 8:00 PM (highlighted with red box)

+ Azure Classic Run As Account ⓘ  
**Create**

12. Open the account and select **Modules** under **Shared Resources**.



13. When the Modules load, search for and select **Az.Accounts**, then select **Import**, then **OK**.

The screenshot shows the details for the **Az.Accounts** module:

- Az.Accounts**
- Description: Microsoft Azure PowerShell - Accounts credential management cmdlets for Azure Resource Manager in Windows PowerShell and PowerShell Core.
- Version: Cr 15
- Tags: Azure ResourceManager ARM Accounts Authentication Environment Subscription PSModule PSEdition\_Core PSEdition/Desktop

**Az.Accounts**

PowerShell Module

**Import** (highlighted with a red box)

14. It will take a few minutes to import the module. From the Recovery Services Vault blade, select **Modules** to view the current status and **Refresh** to monitor progress.

The screenshot shows the 'BC DR Contoso49 | Modules' blade:

- BC DR Contoso49 | Modules**
- Automation Account
- Search (Ctrl+ /) and Refresh buttons (highlighted with a red box)
- Shared Resources menu (Schedules, Modules, Modules gallery, Python 2 packages)
- Table of modules:
 

Name	Last modified	Status	Version
AuditPolicyDsc	5/13/2020, 11:33 AM	Available	1.1.0.0
<b>Az.Accounts</b>	6/25/2020, 4:41 PM	Importing	1.0.0
Azure	5/13/2020, 11:22 AM	Available	1.0.3
Azure Storage	5/13/2020, 11:22 AM	Available	1.0.3

15. Once the **Az.Accounts** module has been imported; repeat the above steps to import the **Az.Network** and **Az.Compute** modules.

16. Next, navigate back to the **Azure Automation Account** blade and select **Runbooks**, then select **Import a runbook**.

The screenshot shows the 'Runbooks' section of the Azure Automation blade. On the left, there's a navigation menu with 'Update management' and 'Process Automation' sections. Under 'Process Automation', the 'Runbooks' item is highlighted with a red box and the number 1. On the right, there's a search bar and a 'Create a runbook' button. Below that is another search bar and an 'Import a runbook' button, which is also highlighted with a red box and the number 2. A table lists three runbooks: 'AzureAutomationTutorial...', 'AzureAutomationTutorial...', and 'AzureAutomationTutorial...'. All three are marked as 'Published'.

Name	Authoring status
AzureAutomationTutorial...	✓ Published
AzureAutomationTutorial...	✓ Published
AzureAutomationTutorial...	✓ Published

**Note:** You must be connected to the **LABVM** to complete the next steps.

17. Select the **Folder** icon on the Import blade and select the file **ASRRunbookSQL.ps1** from the **C:\HOL\** directory on the **LABVM**. Set the Runbook type to **PowerShell Workflow**. Update the name to **ASRSQFailover**. This is the name of the Workflow inside the Runbook script. Leave everything else set to the default. Select **Import**.

**Import a runbook** ...

Upload a runbook file \* ⓘ

Browse for file  
 Browse from gallery

Runbook file \* ⓘ

"ASRRunBookSQL.ps1" 

1

Name \* ⓘ

ASRSQFailover 

2

Runbook type \* ⓘ

PowerShell Workflow 

3

Runtime version \* ⓘ

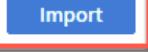
5.1 

Description

 The workflow name in the script must match the runbook name in the textbox "Name" for PowerShell Workflow type

 During runbook execution, PowerShell modules targeting 5.1 runtime version will be used. Please make sure the required PowerShell modules are present in 5.1 runtime version.

4

**Import**  Cancel

18. Once the Runbook is imported, the runbook editor will load. You can review the comments to understand the runbook better if you wish. Once you are ready, select **Publish**, followed by **Yes** at the confirmation prompt. This makes the runbook available for use.

## Edit PowerShell Workflow Runbook

ASRSQFailover

Save  Publish Revert to published Test pane Feedback

> CMDLETS

> RUNBOOKS

> ASSETS

1	<#
2	Microsoft Cloud Workshop: BCDR
3	.File Name
4	- ASRRunBookSQL.ps1
5	

19. Repeat the above steps to import and publish the **ASRRunbookWEB.ps1** runbook. Name this runbook **ASRWEBFailover**.

20. . Navigate back to **Runbooks**, and make sure that both Runbooks show as **Published**.

NAME	AUTHORING STATUS
ASRSQFailover	✓ Published
ASRWEBFailover	✓ Published

**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.

Next, you will create a variable in Azure Automation that contains settings (such as resource group names and VM names) that describe your environment. This information is required by the runbooks you imported. Using variables allows you to avoid hard-coding this information in the runbooks themselves.

21. In your Azure Automation account, select **Variables**, then **Add a variable**.

The screenshot shows the 'Variables' blade for the 'BCDRContoso49' automation account. The left sidebar has tabs for 'Connections', 'Certificates', and 'Variables', with 'Variables' being the active tab and highlighted by a red box. The main area has a search bar, a 'Refresh' button, and a 'Search variables...' input field. Below is a table with columns 'Name' and 'Type', showing the message 'No variables found.' A red box highlights the 'Add a variable' button at the top right of the main area.

22. In the **New Variable** blade, enter **BCDRIaaSPlan** as the variable name. The variable type should be **String**. Paste the following into the variable **Value**, then select **Create**.

```
{
 "PrimarySiteRG": "ContosoRG1",
 "PrimarySiteSQLVM1Name": "SQLVM1",
 "PrimarySiteSQLVM2Name": "SQLVM2",
 "PrimarySiteSQLPath": "SQLSERVER:\\Sql\\SQLVM1\\DEFAULT\\AvailabilityGroups\\BCDRAOG",
 "PrimarySiteVNetName": "VNet1",
 "PrimarySiteWebSubnetName": "Apps",
 "PrimarySiteWebLBName": "ContosoWebLBPrimary",
 "SecondarySiteRG": "ContosoRG2",
 "SecondarySiteSQLVMName": "SQLVM3",
 "SecondarySiteSQLPath": "SQLSERVER:\\Sql\\SQLVM3\\DEFAULT\\AvailabilityGroups\\BCDRAOG",
 "SecondarySiteVNetName": "VNet2",
```

```

 "SecondarySiteWebSubnetName": "Apps",
 "SecondarySiteWebLBName": "ContosoWebLBSecondary"
 }

```

**New Variable**

Name \*

Description

Type ⓘ

Value \*

```
{
 "PrimarySiteRG": "ContosoRG1",
 "PrimarySiteSQLVMName":
 "SQLVM1",
 "PrimarySiteSQLPath":
 "SQLSERVER:\Sql\SQLVM1\DEFAULT\AvailabilityGroups\BCDRAOG",
```

Encrypted \*

Yes
  No

---

**Create**

23. Notice that the variable **BCDRiaaSPlan** has been created.

**BCDRContoso49 | Variables**

Automation Account

Name	Type	Value
BCDRiaaSPlan	String	{ "PrimarySiteRG": "Contoso..."}

Search (Ctrl+ /)
+ Add a variable
 ↻ Refresh

🔑 Credentials
 🔗 Connections
 📜 Certificates
 fx Variables

24. Before continuing, check that the template deployment you started at the beginning of this task has been completed successfully. Then, from the Azure portal home page, select **Subscriptions**, select your subscription, then select **Deployments**.

Deployment name	Status	Last modified	Duration
Peering	Succeeded	6/26/2020, 7:34:52 AM	37 seconds
Contoso-IaaS-DR	Succeeded	6/26/2020, 7:53:09 AM	19 minutes 16 seconds

## Task 2: Inspect DR for the Domain Controller tier

The failover site in East US 2 has been deployed with two additional domain controllers, **ADVM3** and **ADVM4**. These are integrated with the existing `contoso.ins` domain hosted on **ADVM1** and **ADVM2** in the primary site. They run in a fully active-active configuration (therefore, no failover is required for this tier).

The configuration of these domain controllers is fully automatic. In this task, you will simply review the rest of the configuration to confirm everything is as it should be.

1. From the Azure portal home page, select **Subscriptions**, choose your subscription, select **Deployments**, then open the **Contoso-IaaS-DR** deployment used for the DR site.

Deployment name	Status
Peering	Succeeded
Contoso-IaaS-DR	Succeeded

2. Select **Template** and review the template contents. Note the use of `dependsOn` to carefully control the deployment sequence. The resources are deployed as follows:

- The VNet2 virtual network is created.
- VNet2 is peered with VNet1. This peering creates connectivity between the two networks.
- The DNS settings in VNet2 are updated to point to the domain controllers in VNet1.

- The new domain controllers, **ADVM3** and **ADVM4**, are deployed to VNet2 with static private IP addresses. A custom script extension is used to configure these VMs as domain controllers.
- The DNS settings in VNet2 are then updated to point to these new domain controllers.
- Other VMs (such as **SQLVM3**) are now able to be deployed.

**Contoso-IaaS-DR | Template**

Deployment

Search (Ctrl+ /) Download Add to library (preview)

Overview Inputs Outputs **Template**

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Define resources and configurable input parameters and deploy with script or code. [Learn more about template deployment.](#)

Include parameters ⓘ

Template Parameters Scripts

Parameters (5) Variables (3) Resources (9)

VirtualNetworkSecondary (Microsoft.Resources/deployments) Peering (Microsoft.Resources/deployments) VirtualNetworkSecondaryWithPrimaryDNS (Microsoft.Resources/deployments) **ADVM3** (Microsoft.Resources/deployments) **ADVM4** (Microsoft.Resources/deployments) VirtualNetworkSecondaryWithSecondaryDNS (Microsoft.Resources/deployments) LoadBalancersSecondary (Microsoft.Resources/deployments) SQLVM3 (Microsoft.Resources/deployments) Bastion (Microsoft.Resources/deployments)

```

46 "resources": [
47 {
48 "type": "Microsoft.Resources/deployments",
49 "apiVersion": "2019-10-01",
50 "name": "VirtualNetworkSecondary",
51 "dependsOn": [],
52 "properties": {
53 "mode": "Incremental",
54 "templateLink": {
55 "uri": "[concat(variables('baseUri'), 'templates/vnet-dr.json')]",
56 "contentVersion": "1.0.0.0"
57 },
58 "parameters": {
59 "VNetName": {
60 "value": "[variables('vnetNameSecondary')]"
61 }
62 }
63 },
64 "resourceGroup": "[parameters"

```

3. Navigate to the **ContosoRG2** resource group. Inspect network interface (NIC) resources for the **ADVM3** and **ADVM4** VMs to confirm their network settings include the static private IP addresses **10.102.3.100** and **10.102.3.101**, respectively.

**ADVM3NIC** IP configurations ...

Network Interface

Search (Ctrl+ /) Add Save Discard Refresh

Overview Activity log Access control (IAM) Tags

Settings **IP configurations** DNS servers Network security group Properties Locks

IP forwarding settings IP forwarding Enabled

Virtual network VNet2

IP configurations Subnet \*

Identity (10.1.3.0/24)

Name	IP Version	Type	Private IP address	Public IP address
ipconfig1	IPv4	Primary	10.1.3.100 (Static)	-

4. Navigate to the **VNet2** virtual network. Select **DNS servers** and confirm that the IP addresses for **ADVM3** and **ADVM4** are configured.

The screenshot shows the 'DNS servers' section of the VNet2 virtual network settings. The 'Custom' option is selected, and two IP addresses, 10.1.3.100 and 10.1.3.101, are listed. The 'Add DNS server' button is visible.

5. Select **Peerings** and confirm that the network is peered with VNet1.

The screenshot shows the 'Peerings' section of the VNet2 virtual network settings. A connection named 'VNet2-to-VNet1' is listed as 'Connected' to 'VNet1'. The 'Add' and 'Refresh' buttons are also visible.

### Task 3: Configure DR for the SQL Server tier

This task will extend the SQL Server Always On Availability Group you created earlier to include **SQLVM3** as an asynchronous replica running in the DR site.

This task comprises the following steps:

- Add SQLVM3 to the load-balancer backend pool in the DR site.
- Add SQLVM3 to the existing Windows Server Failover Cluster.
- Enable AlwaysOn and set the domain login credentials on SQLVM3.
- Update the Availability Group Listener to include the SQLVM3 IP address.
- Add SQLVM3 as an asynchronous replica in the existing Always On Availability Group.
- Update the failover cluster with the Listener IP address.

1. Return to the Azure portal and navigate to the **ContosoSQLBSecondary** load balancer blade in **ContosoRG2**. Select **Backend pools** and open **BackEndPool1**. Note that the pool is connected to the **VNet2** virtual network. Select **+ Add**.

## BackEndPool1

ContosoSQLLBSecondary

Name BackEndPool1

Virtual network ⓘ VNet2 (ContosoRG2)

Backend Pool Configuration  NIC  
 IP Address

IP Version  IPv4  
 IPv6

### Virtual machines

You can only attach virtual machines in westus2 that have a standard SKU public IP configuration or no public IP configuration. All IP configurations must be on the same virtual network.

+ Add

X Remove

Virtual machine ↑↓

IP Configuration ↑↓

Availability set ↑↓

No virtual machines selected

### Virtual machine scale sets

Virtual Machine Scale Sets must be in same location as Load Balancer. Only IP configurations that have the same SKU (Basic/Standard) as the Load Balancer can be selected. All of the IP configurations have to be in the same Virtual Network.

i No virtual machine scale set is found in westus2 that matches the above criteria

Virtual machine scale set

IP address

▼	▼	▼
---	---	---

Used by

Save

Cancel

Give feedback

2. Select **SQLVM3**. Select **Add**. Select **Save** on **BackEndPool1** to save changes.

## Add virtual machines to backend pool

**!** You can only attach virtual machines that are in the same location and on the same virtual network as the loadbalancer. Virtual machines must have a standard SKU public IP or no public IP.

<input type="checkbox"/> Virtual machine ↑↓	Resource group ↑↓	IP Configuration ↑↓	Availability set ↑↓	Tags
<input checked="" type="checkbox"/> sqlvm3	contosorg2	ipconfig1 (10.1.2.4)	-	-
<input type="checkbox"/> advm3	contosorg2	ipconfig1 (10.1.3.100)	-	-
<input type="checkbox"/> advm4	contosorg2	ipconfig1 (10.1.3.101)	-	-

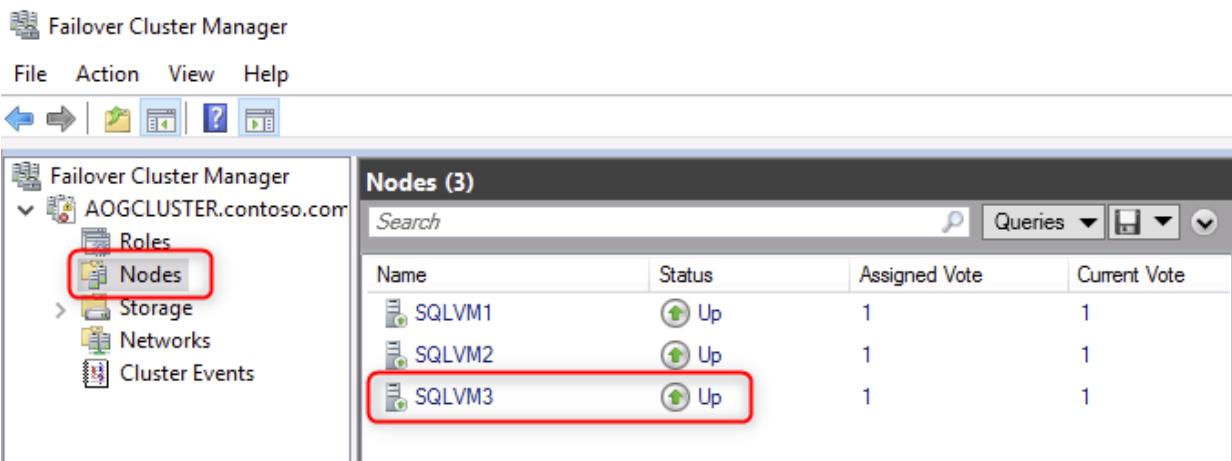
Add Cancel

**Note:** For this lab, the DR site is configured with a single SQL Server VM. Using a load balancer is therefore not strictly required. However, it allows the DR site to be extended to include its own HA cluster if needed.

3. Return to your browser tab containing your Bastion session with **SQLVM1**. (If you have closed the tab, reconnect using Azure Bastion with username `adadmin@contoso.ins` and password `Demo!pass123`.)
4. On **SQLVM1**, use **Windows PowerShell** to execute the following command. This command will add **SQLVM3** as a node in the existing Windows Server Failover Cluster.

```
Add-ClusterNode -Name SQLVM3
```

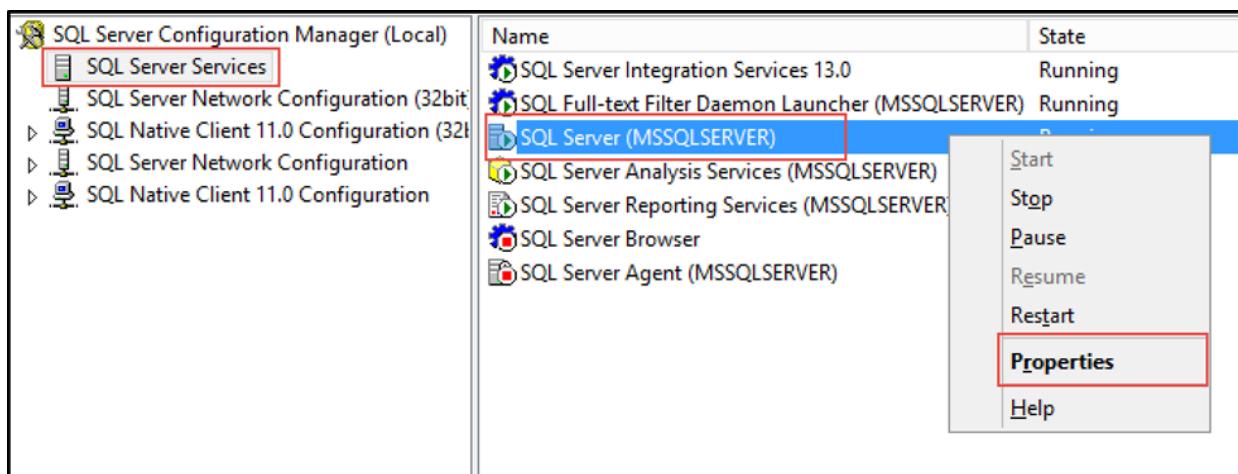
5. Select **Start** and then **Windows Administrative Tools**. Locate and open the **Failover Cluster Manager**. Expand the **sqlAlwaysOn** and select **Nodes**. Note that SQLVM3 is now included in the list, with the status **Up**.



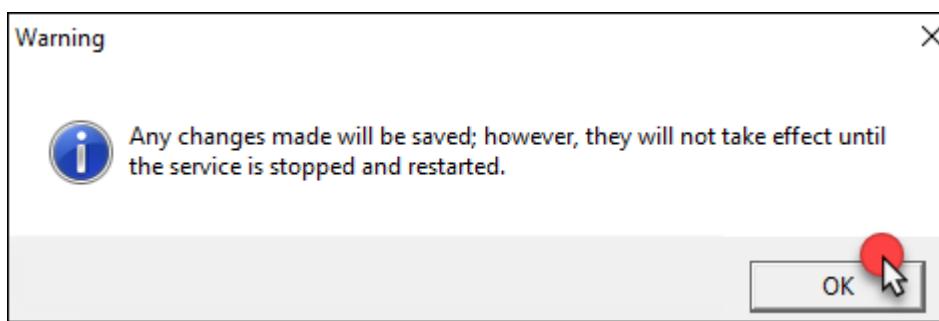
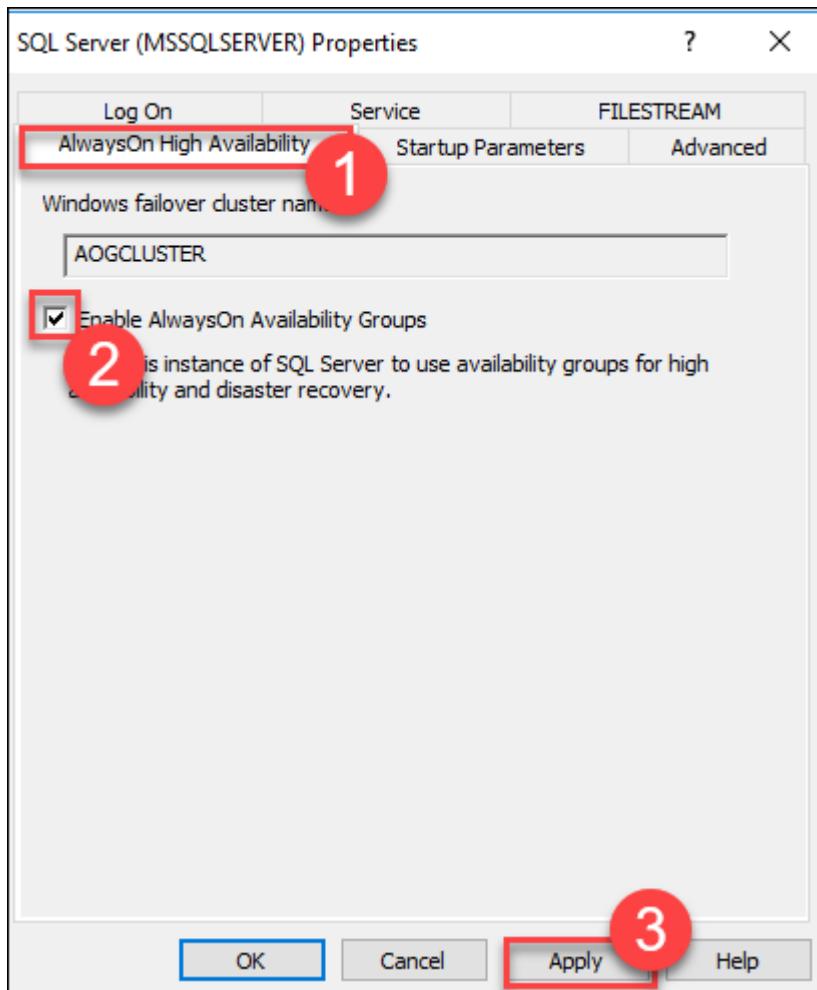
6. Return to the Azure portal. Locate **SQLVM3**, and connect to the VM using Azure Bastion with the username `adadmin@contoso.ins` and the password `Demo!pass123`.
7. On **SQLVM3**, select **Start** and launch **SQL Server 2017 Configuration Manager**.



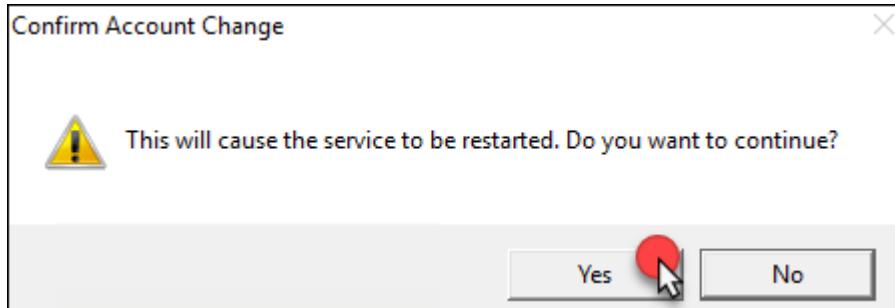
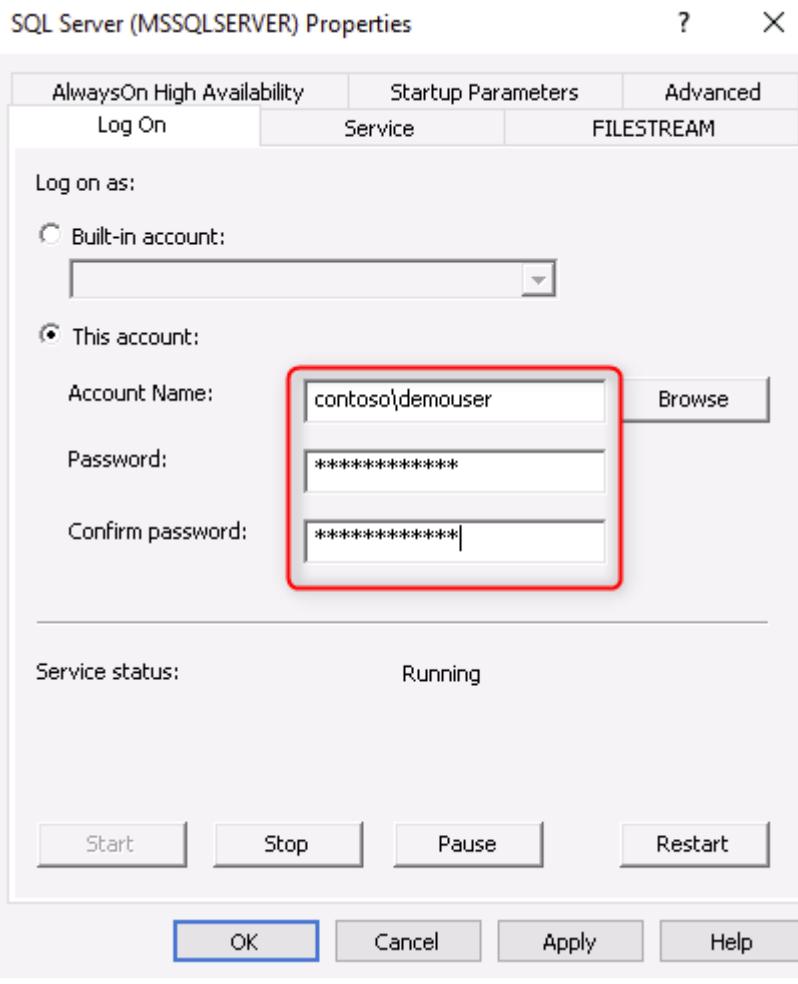
8. Select **SQL Server Services**, then right-click **SQL Server (MSSQLSERVER)** and select **Properties**.



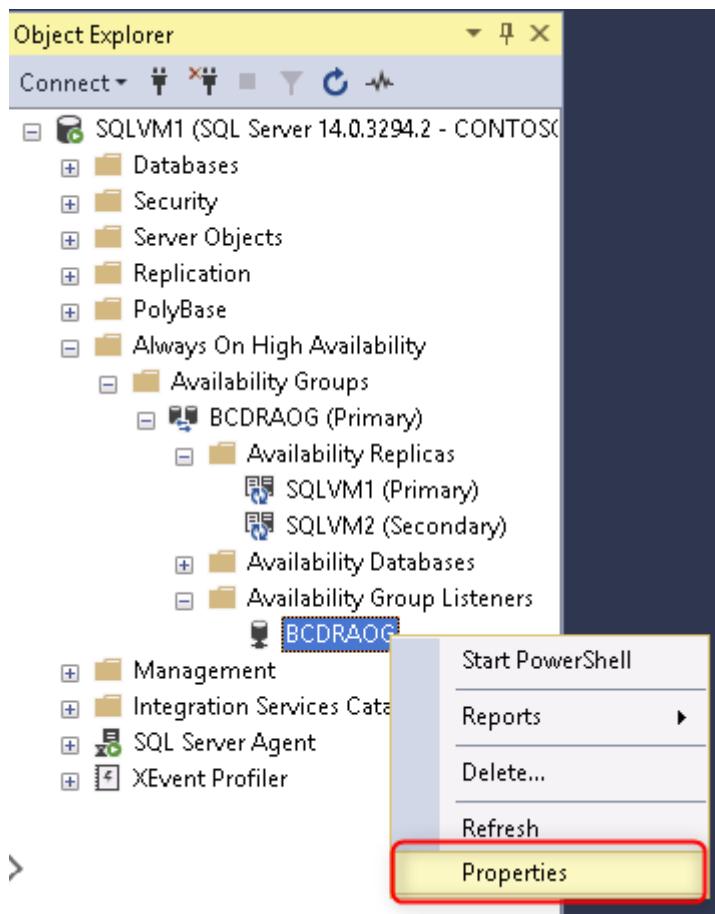
9. Select the **AlwaysOn High Availability** tab and check the box for **Enable AlwaysOn Availability Groups**. Select **Apply** and then select **OK** on the message that notifies you that changes won't take effect until after the server is restarted.



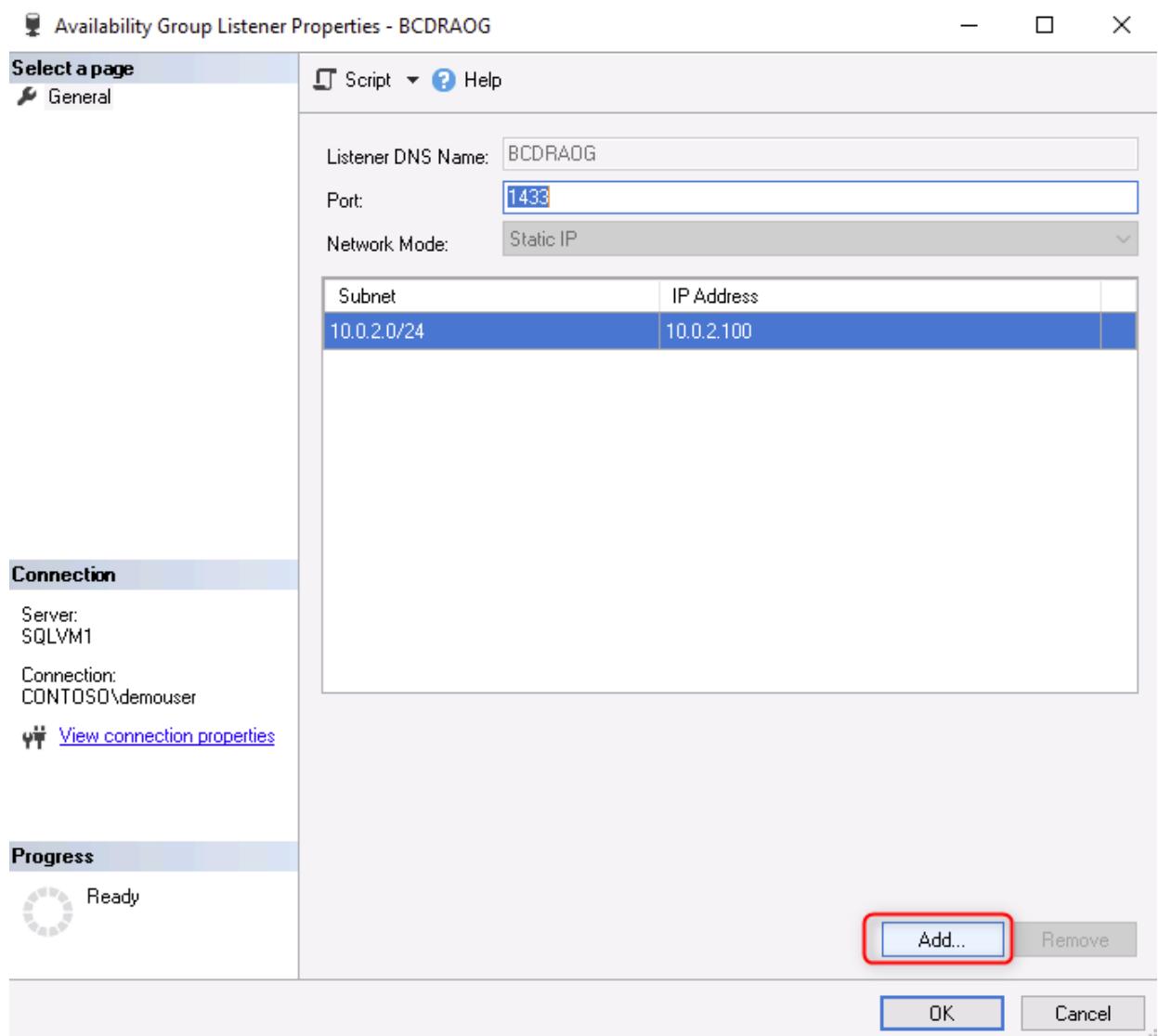
10. On the **Log On** tab, change the service account to **contoso\adadmin** with the password **Demo!pass123**. Select **OK** to accept the changes, and then select **Yes** to confirm the restart of the server.



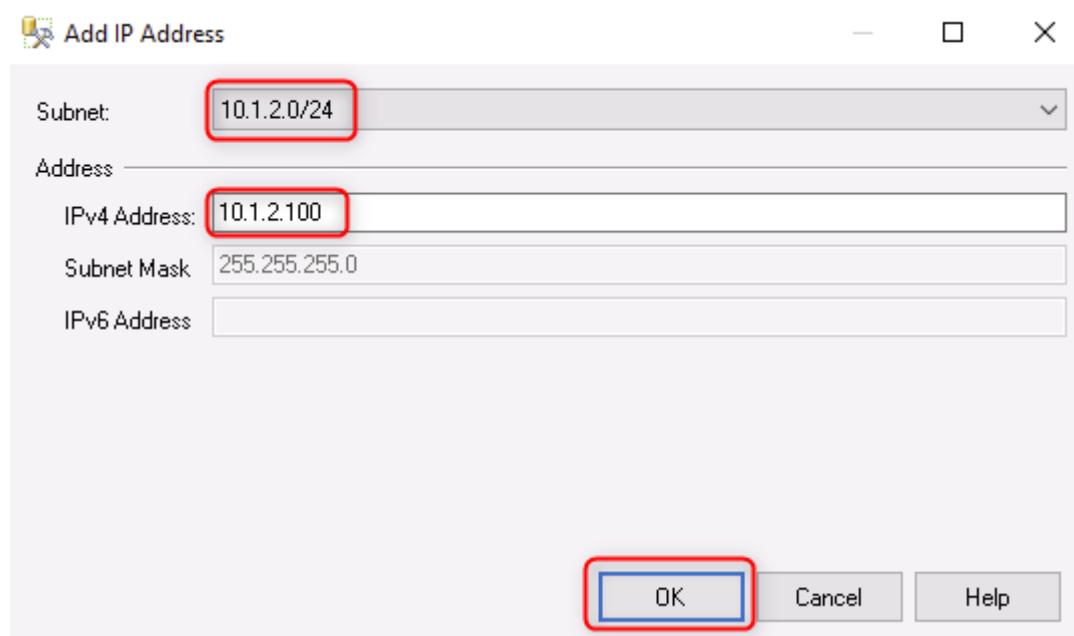
11. Return to your session with **SQLVM1**. Open **Microsoft SQL Server Management Studio 18** and connect to the local instance of SQL Server.
12. Expand the **Always On High Availability** node. Under **Availability Group Listeners**, right-click on **BCDRAOG** and select **Properties**.



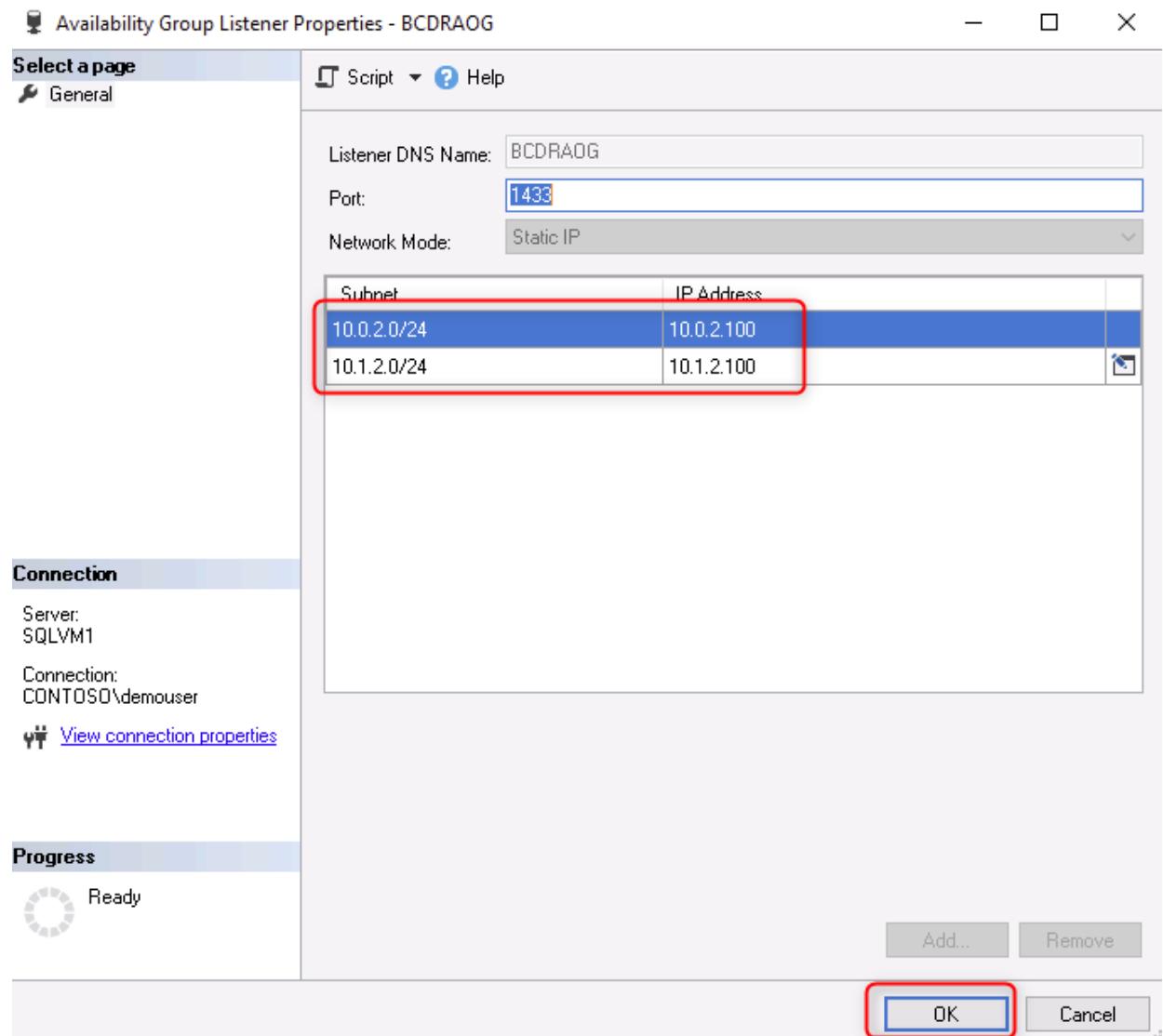
13. On the BCDRAOG Listener properties dialog, select **Add**.



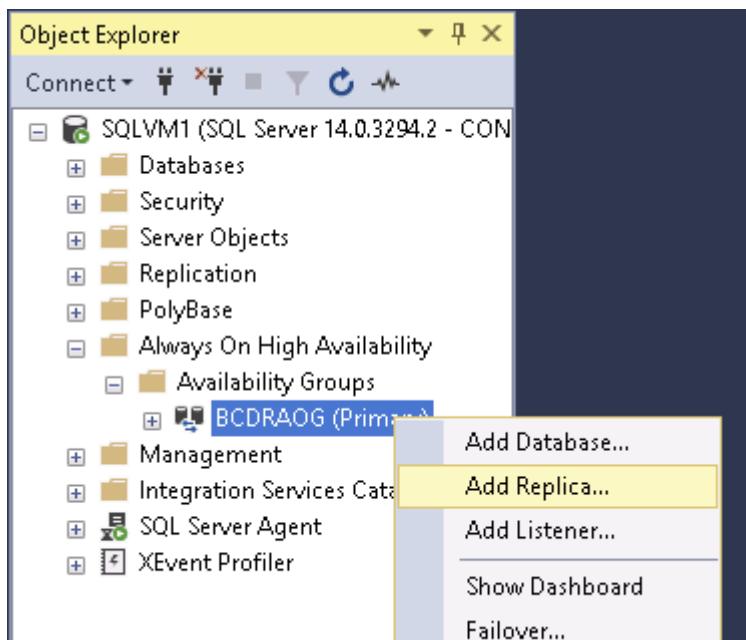
14. On the Add IP Address dialog, check the subnet is **10.102.2.0** (this is the Data subnet in VNet2). Enter the IP address **10.102.2.100** (this is the frontend IP of the SQL load balancer in VNet2). Select **OK**.



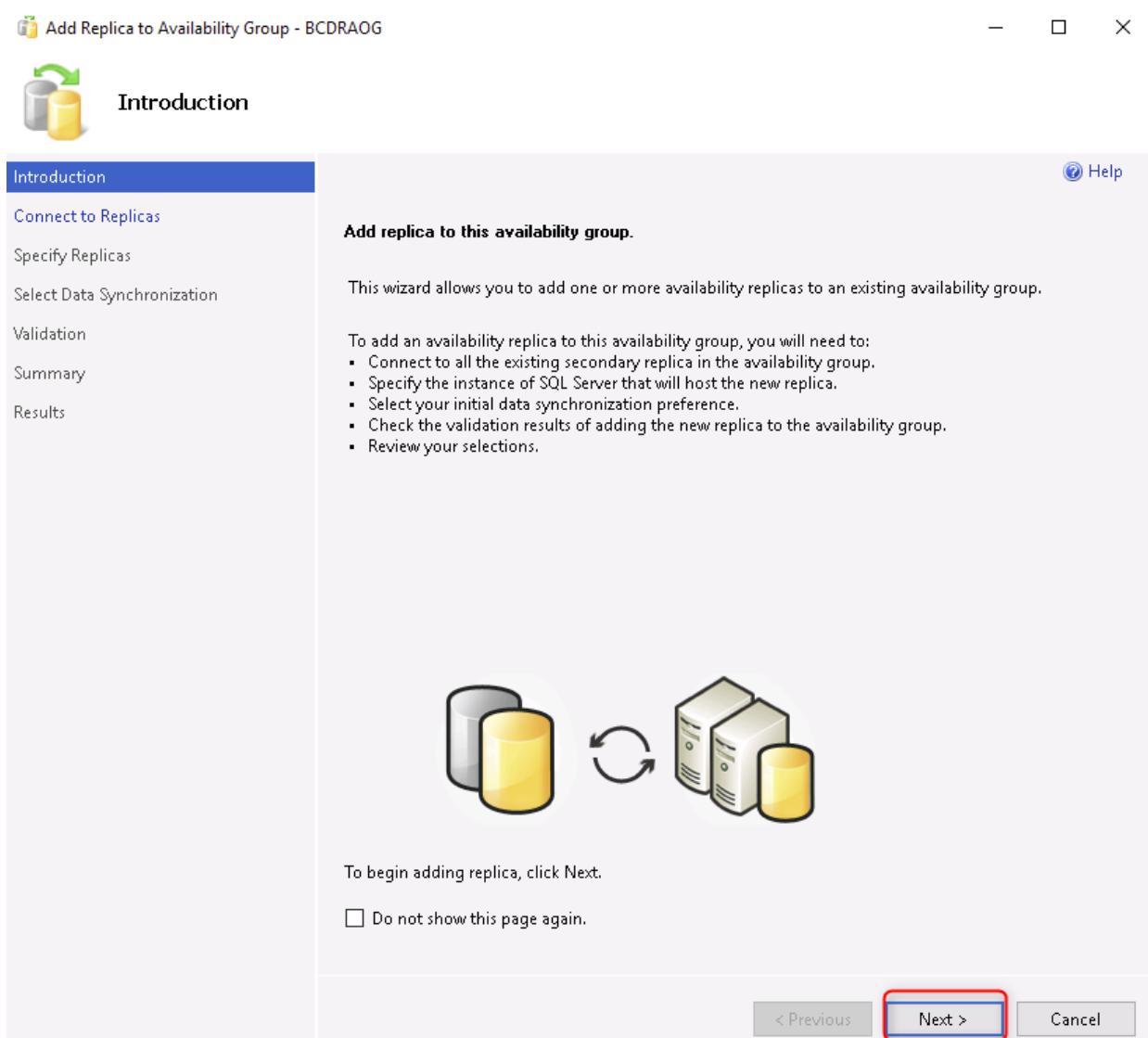
15. Two IP addresses should be shown on the BCDRAOG Listener properties dialog. Select **OK** to close the dialog and commit the change.



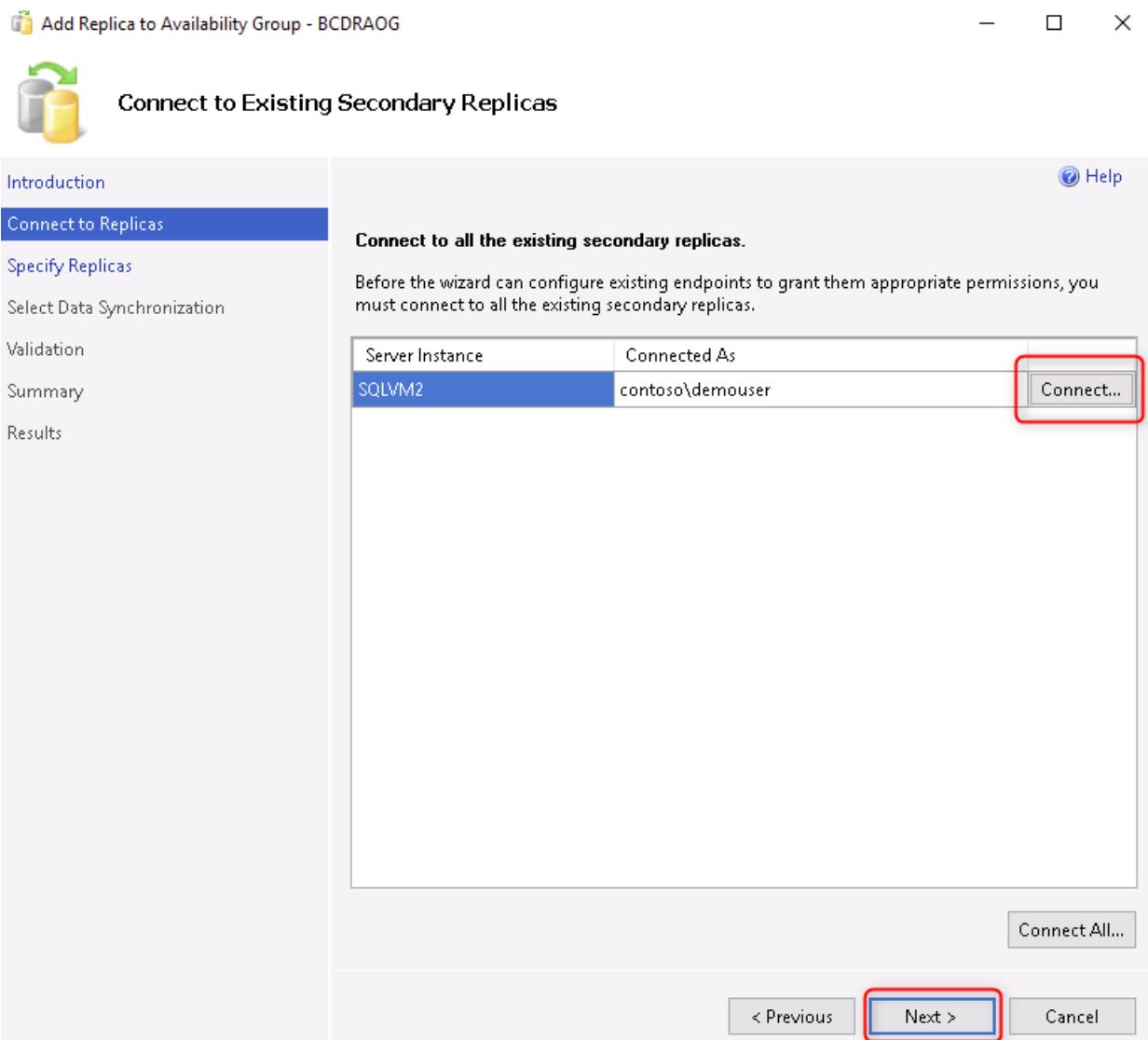
16. Under **Availability Groups**, right-click on **BCDRAOG (Primary)** and select **Add Replica..** to open the Add Replica wizard.



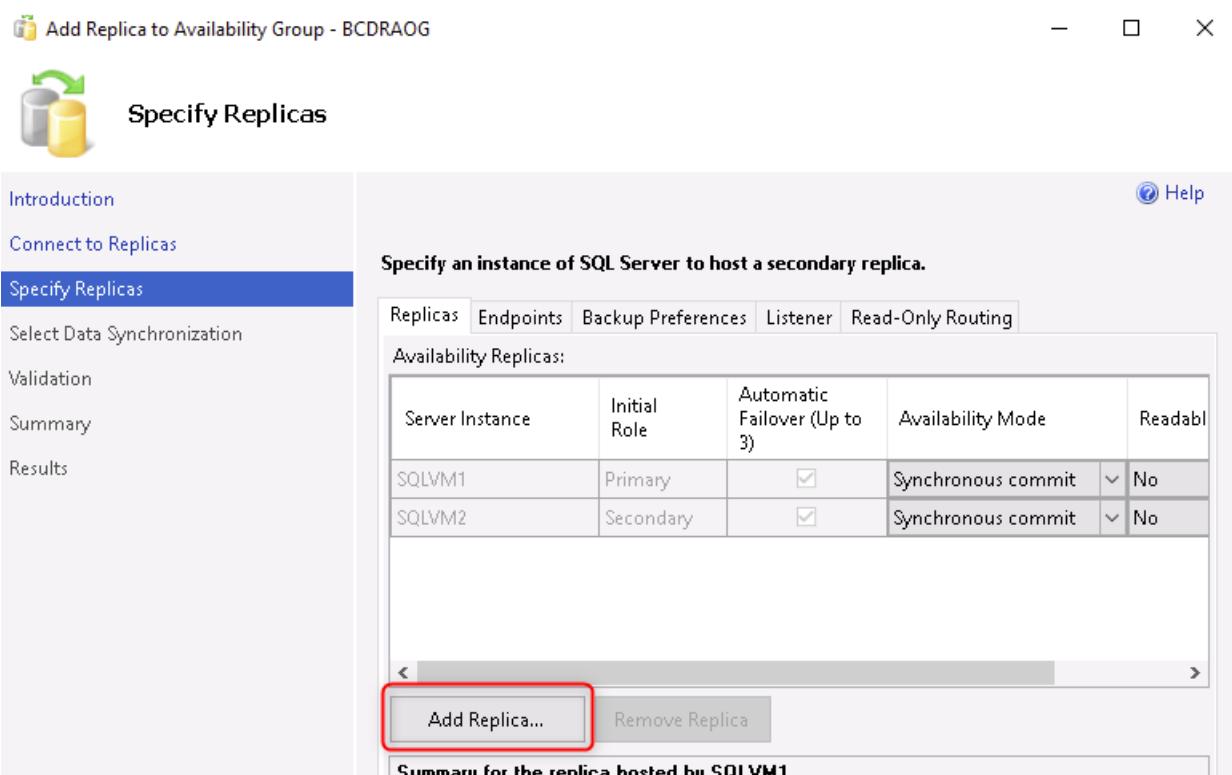
17. Select **Next** on the wizard.



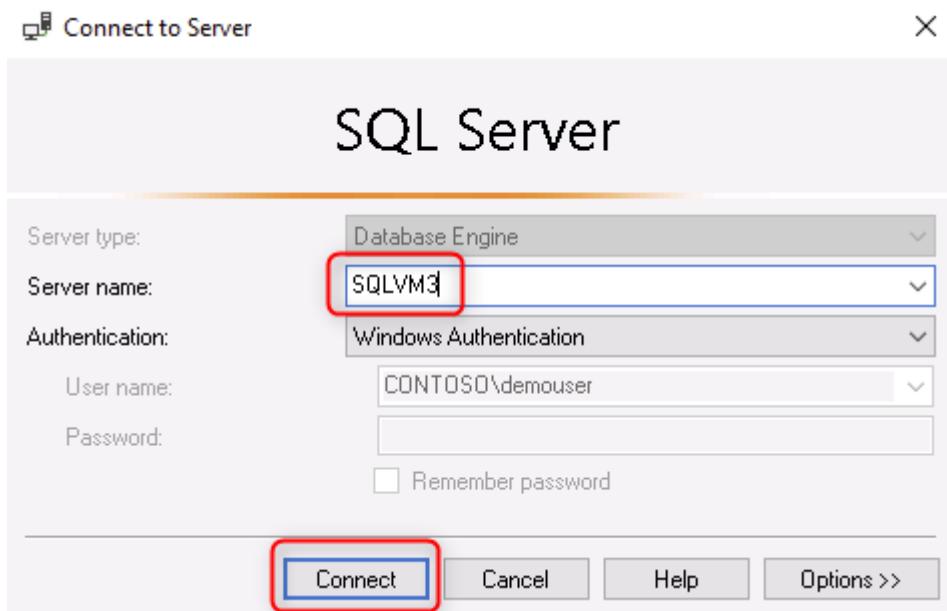
18. Select **Connect** to connect to SQLVM2, then **Connect** again on the 'Connect to Server' prompt.  
Then select **Next**.



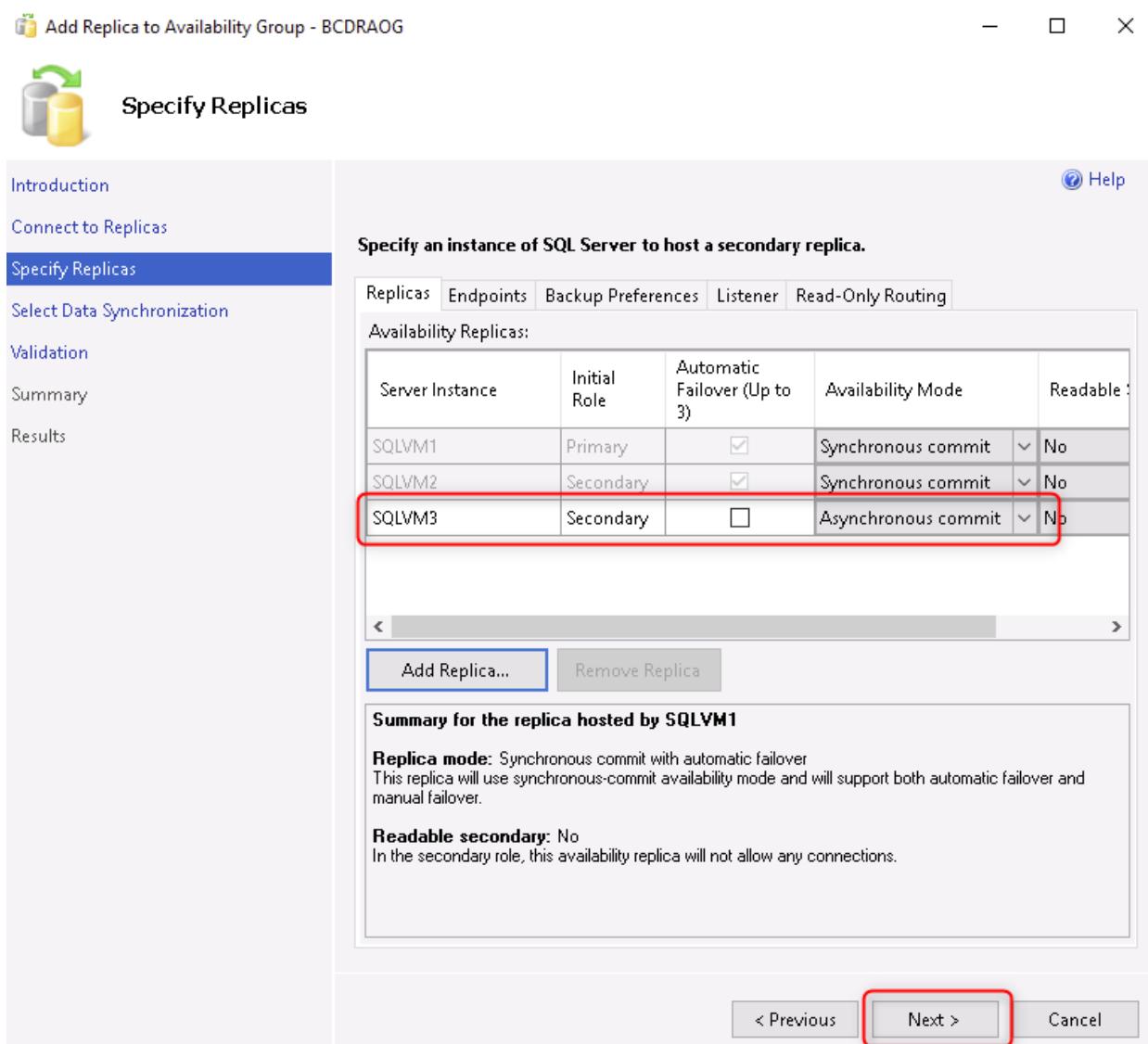
19. On the **Specify Replicas** page, select **Add Replica....**



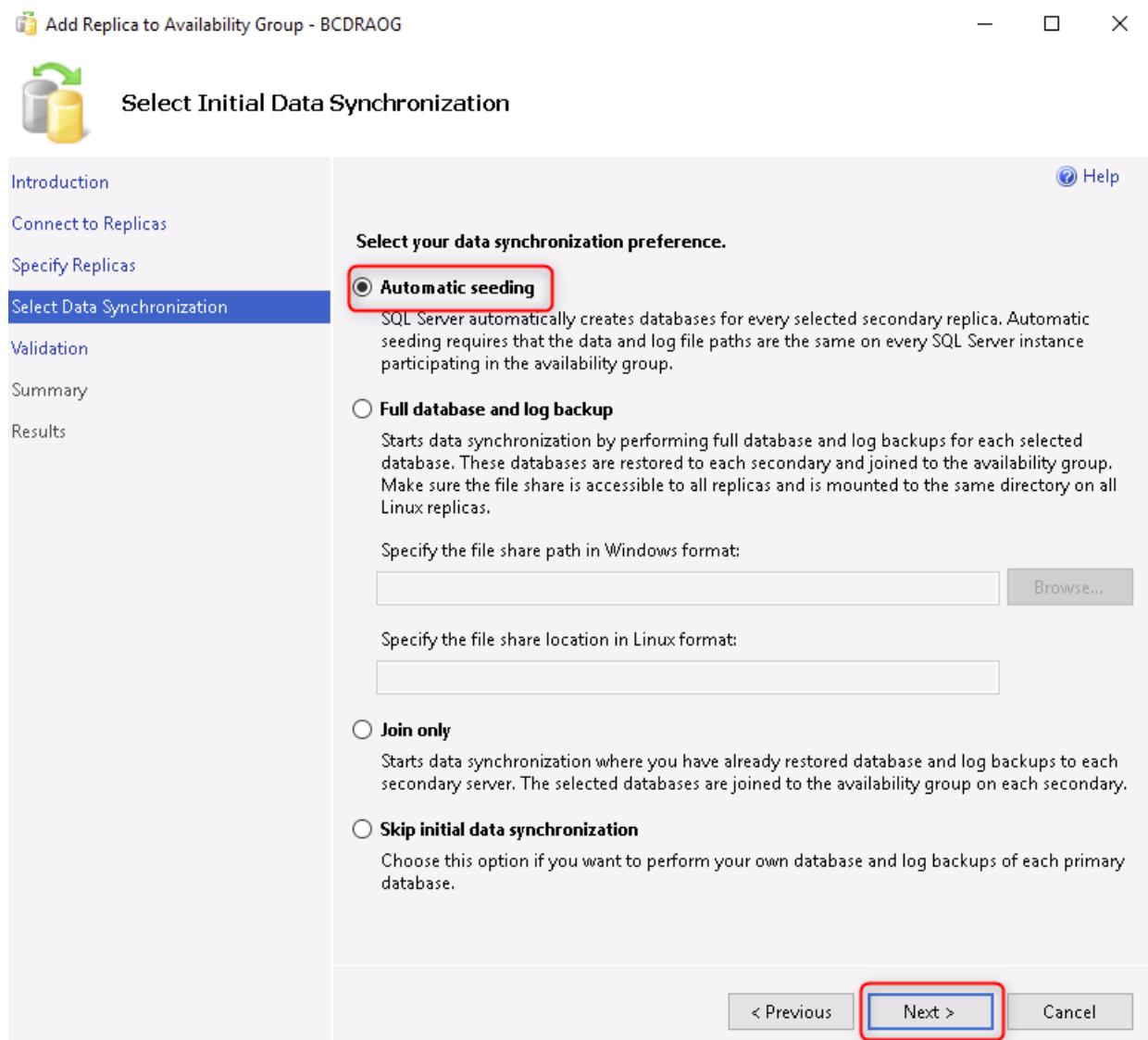
20. On the **Connect to Server** dialog box, enter the Server Name of **SQLVM3** and select **Connect**.



21. For **SQLVM3**, leave the default settings of 'Asynchronous commit' with 'Automatic Failover' disabled. Select **Next**.



22. On the **Select Data Synchronization** page, ensure that **Automatic seeding** is selected and select **Next**.



23. On the **Validation** screen, you should see all green, except for a warning for 'Checking the listener configuration'. The listener configuration warning will be addressed later. Select **Next**.

Add Replica to Availability Group - BCDRAOG

## Validation

Introduction  
Connect to Replicas  
Specify Replicas  
Select Data Synchronization  
**Validation**  
Summary  
Results

Help

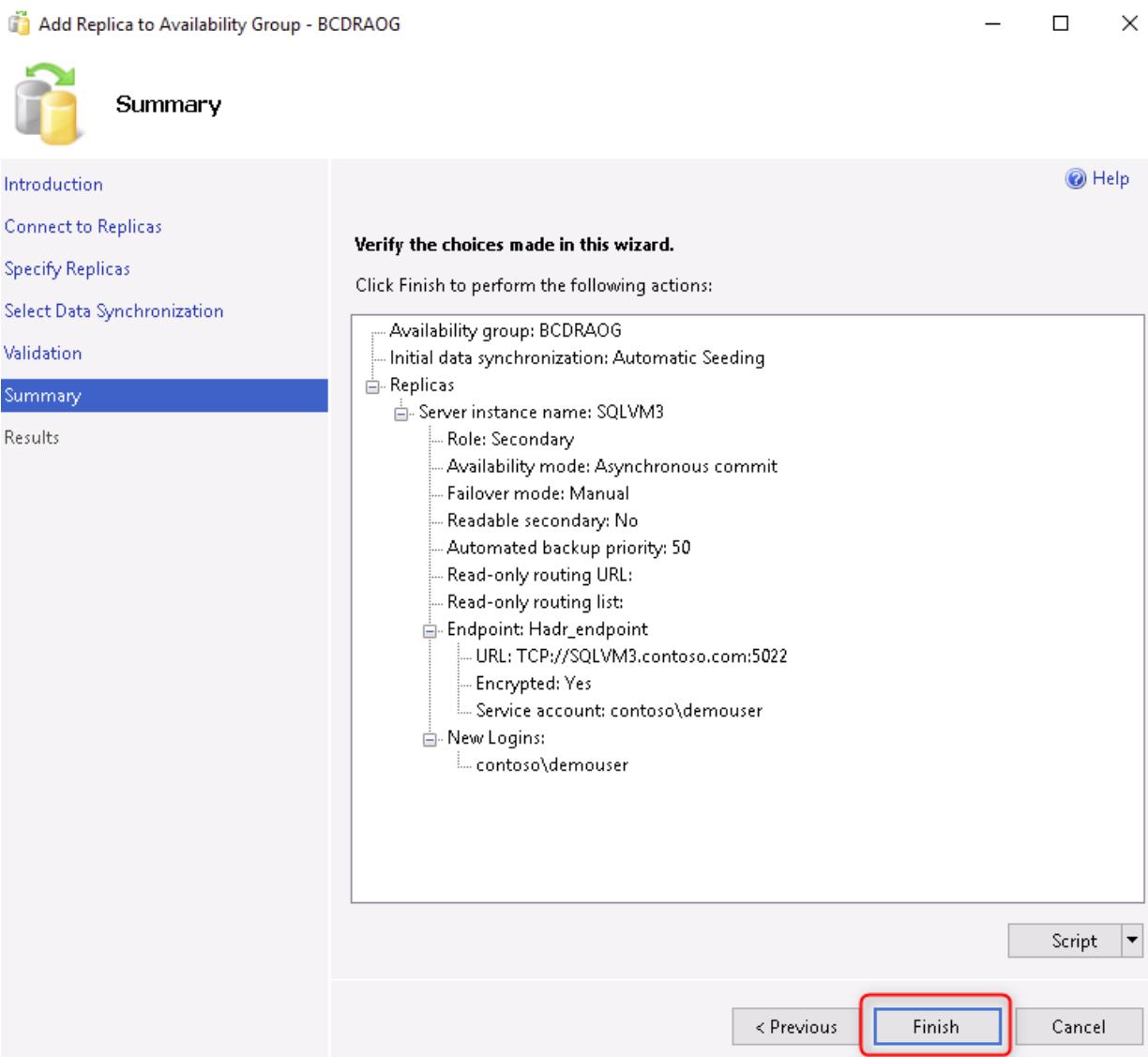
**Results of availability group validation.**

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

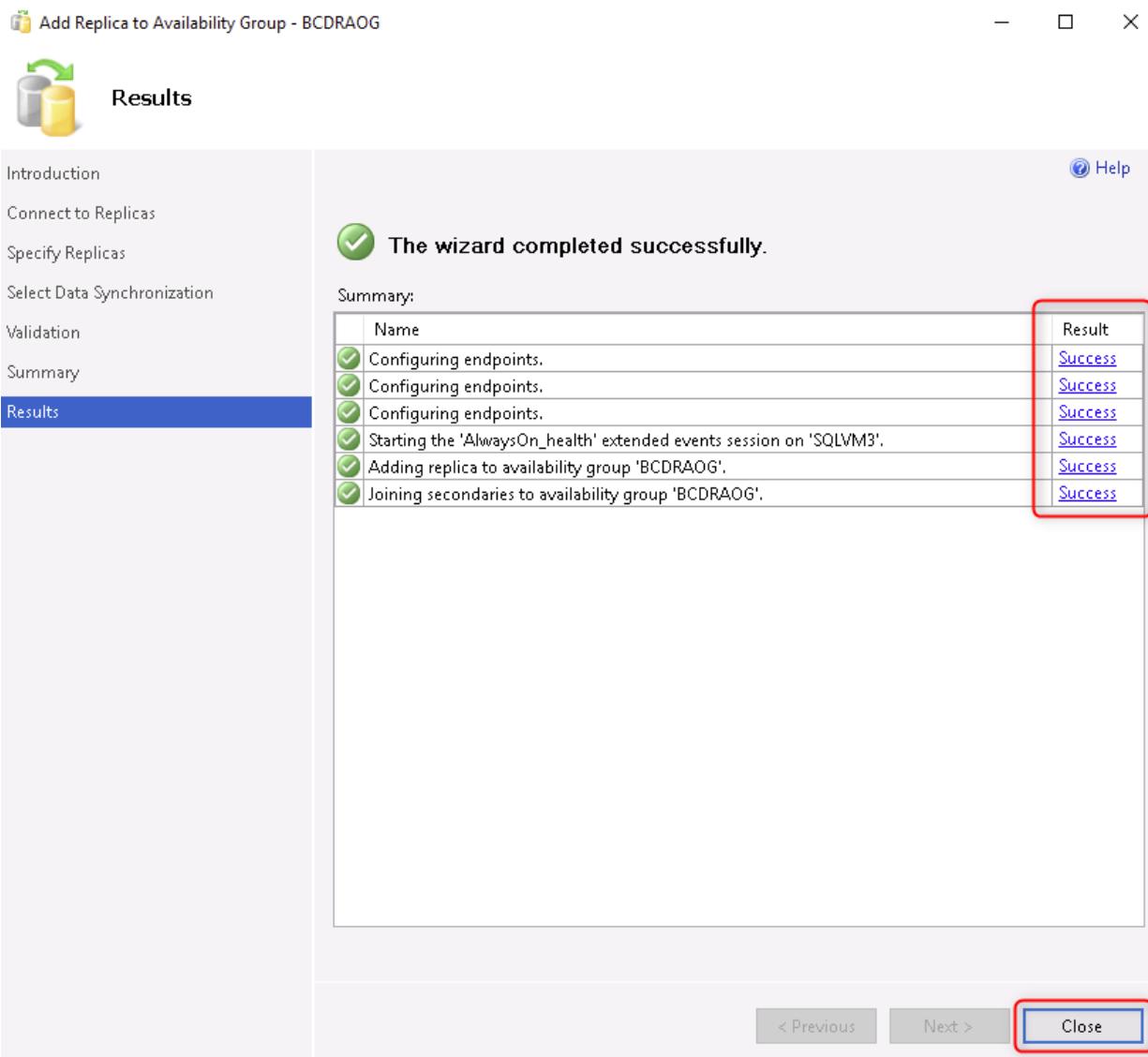
Re-run Validation

< Previous Next > Cancel

24. On the Summary page, select **Finish**.



25. Once the AOG is built, check that each task was successful and select **Close**.



26. Under Availability Groups, right-click **BCDRAOG (Primary)** and then select **Show Dashboard**. You should see that the **SQLVM3** node has been added and is synchronizing.

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
<span style="color: green;">✓</span> SQLVM1	Primary	Synchronous co...	Automatic	Automatic	Synchronized	
<span style="color: green;">✓</span> SQLVM2	Second...	Synchronous co...	Automatic	Automatic	Synchronized	
<span style="color: green;">✓</span> SQLVM3	Second...	Asynchronous co...	Manual	Automatic	Synchronizing	

Group by ▾

Name	Replica	Synchronization State	Failover Readi...	Issues
SQLVM1				
<span style="color: green;">✓</span> ContosoInsurance	SQLVM1	Synchronized	No Data Loss	
SQLVM2				
<span style="color: green;">✓</span> ContosoInsurance	SQLVM2	Synchronized	No Data Loss	
<span style="color: green;">✓</span> SQLVM3				
<span style="color: green;">✓</span> ContosoInsurance	SQLVM3	Synchronizing	Data Loss	

27. Move back to **PowerShell** on **SQLVM1**. Paste in the following script, and press **Return**. This script will update the Failover cluster with the new Listener IP address you created.

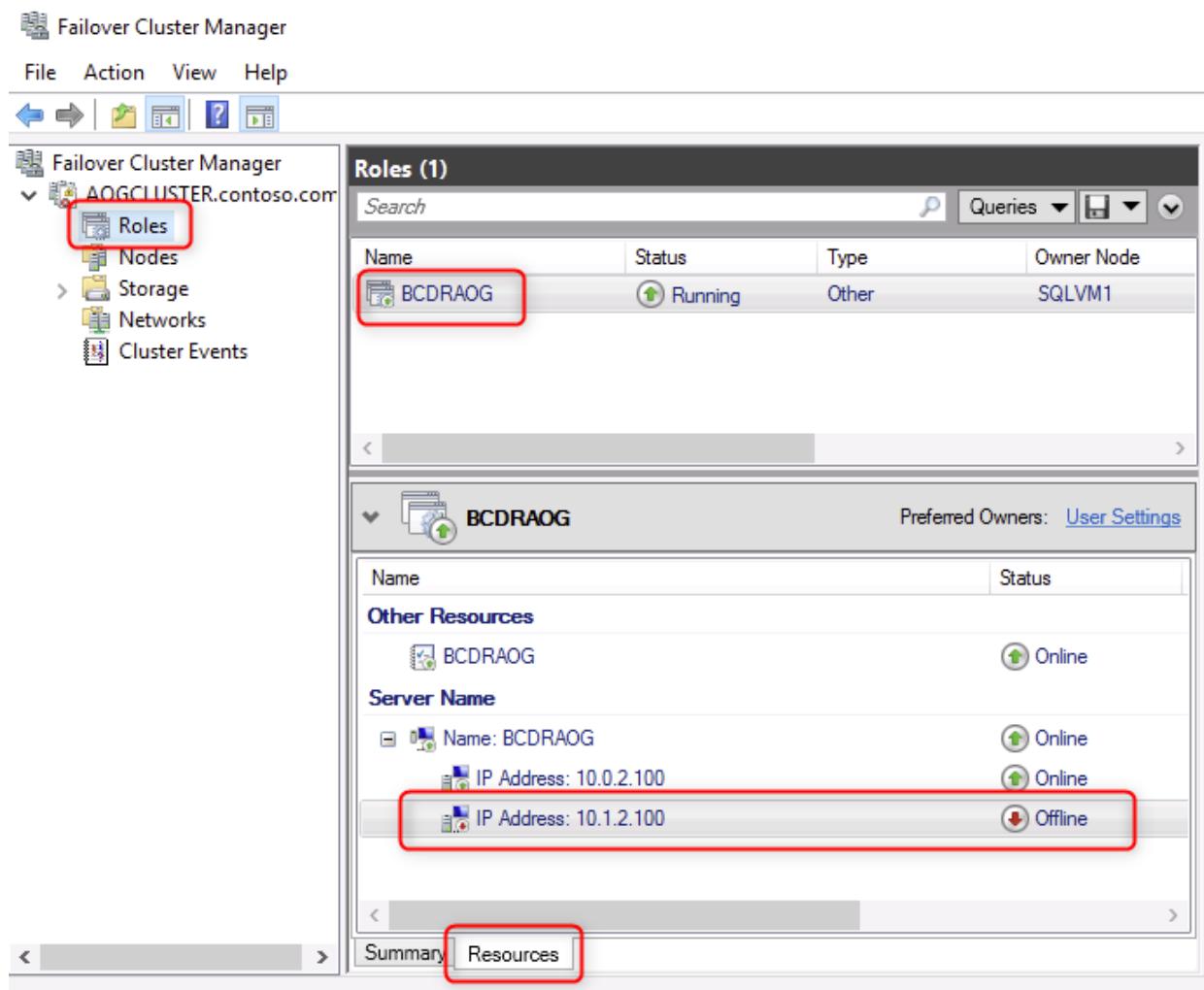
```
$ClusterNetworkName = "Cluster Network 2"
$IPResourceName = "BCDRAOG_10.102.2.100"
$ILBIP = "10.33.2.100"
Import-Module FailoverClusters
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple
@{ "Address"="$ILBIP"; "ProbePort"="59999"; "SubnetMask"="255.255.255.255"; "Network"="$ClusterNetworkName"; "EnableDhcp"=0}
Stop-ClusterResource -Name $IPResourceName
Start-ClusterResource -Name "BCDRAOG"
```

```
PS C:\Users\demouser.CONTOSO> $ClusterNetworkName = "Cluster Network 2"
>> $IPResourceName = "BCDRAOG_10.1.2.100"
>> $ILBIP = "10.1.2.100"
>> Import-Module FailoverClusters
>> Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple @{ "Address"="$ILBIP"; "ProbePort"="59999"; "SubnetMask"="255.255.255.255"; "Network"="$ClusterNetworkName"; "EnableDhcp"=0}
>> Stop-ClusterResource -Name $IPResourceName
>> Start-ClusterResource -Name "BCDRAOG"

Name State OwnerGroup ResourceType
---- ---- ----- -----
BCDRAOG_10.1.2.100 Offline BCDRAOG IP Address
BCDRAOG Online BCDRAOG SQL Server Availability Group

PS C:\Users\demouser.CONTOSO>
```

28. Move back to Failover Cluster Manager on **SQLVM1**, select **Roles**, then **BCDRAOG**. Notice how the **Resources** tab shows that the new IP address **10.102.2.100** has been added and is currently Offline.



#### Task 4: Configure DR for the Web tier

In this task, you will configure DR for the Contoso application web tier.

The DR solution for the web tier uses Azure Site Recovery to continually replicate the primary site web tier VMs to Azure storage. During failover, the replicated data is used to create new VMs in the DR site, which is pre-configured with the virtual network and web-tier load balancer.

Custom scripts in Azure Automation are called by Azure Site recovery to add the recovered web VMs to the load balancer and failover the SQL Server.

1. From the Azure portal on **LABVM**, open the **BCDRRSV** Recovery Services Vault located in the **ContosoRG2** resource group.
2. Under **Getting Started**, select **Site Recovery**. Next, select **Step 1: Enable replication** in the **For On-Premises Machines and Azure VMs** section.

3. On **Step 1 - Source**, select the following inputs and then select **Next**:

- o **Source Location:** Central US (or what you select as your Primary region)
- o **Azure virtual machine deployment model:** Resource Manager
- o **Source resource group:** ContosoRG1
- o **Disaster Recovery between Availability Zones?:** No (this option is for DR between availability zones *within* a region)

## Enable replication

4. On **Step 2 - Virtual Machines**, select **WebVM1** and **WebVM2** and then select **Next**.

## Enable replication ...

Source    2 Virtual machines    3 Replication settings

Unable to view / select your VMs? Click [here](#) to know why.

Filter items...

Name	Virtual network	Tags
<input type="checkbox"/> ADVM1	VNet1	
<input type="checkbox"/> ADVM2	VNet1	
<input type="checkbox"/> SQLVM1	VNet1	
<input type="checkbox"/> SQLVM2	VNet1	
<input checked="" type="checkbox"/> WebVM1	VNet1	
<input checked="" type="checkbox"/> WebVM2	VNet1	

Selected machines: 2

Previous    **Next**

5. On the **Replication settings** tab, select the **Target location** as **East US 2** (or what you selected as your secondary site Azure region). Then, in the 'Resource group, Network, Storage and Availability' section, select **Customize**.

## Enable replication ...

✓ Source   ✓ Virtual machines   **Replication settings**

Target location \* ⓘ  
East US 2

Target subscription ⓘ Customize  
Microsoft Azure Sponsorship

**⚠** If you are choosing General Purpose v2 storage accounts, ensure that operations and data transfer prices are understood clearly before you proceed. [Learn more](#)

Resource group, Network, Storage and Availability ⓘ 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. All newly created resources except disks are appended with the suffix "asr". Disks are appended with the suffix "asrreplica".

<b>Target resource group</b> ⓘ (new) ContosoRG2-asr	<b>Target virtual network</b> ⓘ (new) VNet1-asr
<b>Cache storage accounts</b> ⓘ (new) a9vbjy3bcdrrsvasrcache	<b>Replica managed disks</b> ⓘ (new) 2 premium disk(s), 0 standard disk(s)
<b>Target availability sets</b> ⓘ Not Applicable	<b>Target availability zones</b> ⓘ 1 2

Target proximity placement groups ⓘ

Previous   **Enable replication**

6. Update the blade using the following:

- **Target resource group:** ContosoRG2
- **Target virtual network:** VNet2

Review the settings for each VM, keeping their default values. Then select **OK**.

## Customize target settings

X

**i** By default, Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network, managed disks and availability sets. You can change the settings below.

General settings

Target resource group  
ContosoRG2

Target virtual network ⓘ  
VNet2

VM settings

VM Name	Source managed disk	Replica managed disk	Cache storage	Disk to replicate	Target availability type
▼ 1 (Availability zone)	[Premium SSD] WebVM1OS...	(new) [Premium SSD]...	(new) tuh5lzbcdrrsva...	<input checked="" type="checkbox"/> include	zone 1
▼ 2 (Availability zone)	[Premium SSD] WebVM2OS...	(new) [Premium SSD]...	(new) tuh5lzbcdrrsva...	<input checked="" type="checkbox"/> include	zone 2

OK

**Note:** Double check these selections; they are **critical** to your on-premise to Azure failover.

- Under 'Replication Policy', review the default policy but do not make any changes.

## Enable replication

<b>Target resource group</b> ⓘ	<b>Target virtual network</b> ⓘ
ContosoRG2	VNet2
<b>Cache storage accounts</b> ⓘ	<b>Replica managed disks</b> ⓘ
(new) yb3jh0bcdrrsvasrcache	(new) 2 premium disk(s), 0 standard disk(s)
<b>Target availability sets</b> ⓘ	<b>Target availability zones</b> ⓘ
Not Applicable	1 2
<b>Target proximity placement group</b> ⓘ	
Not Applicable	

### Capacity Reservation Settings

Reserve a capacity at the destination location - West US 2

[Why to reserve capacity at the destination location?](#)

Capacity Reservation Groups ⓘ Assigned for 0 out of 2 machines  
[View or Edit Capacity Reservation group assignment](#)

### Replication Policy [Customize](#)

**Name:** 24-hour-retention-policy  
**Recovery point retention:** 1 day(s)  
**App consistent snapshot frequency:** 0 hour(s)  
**Replication group:** None

Extension settings

[+] Show details

- Under 'Extension settings', select **[+] Show details**. Change the **Automation Account** to use your existing Automation Account.

Extension settings [\[-\] Hide details](#)

**Update settings**

Allow ASR to manage

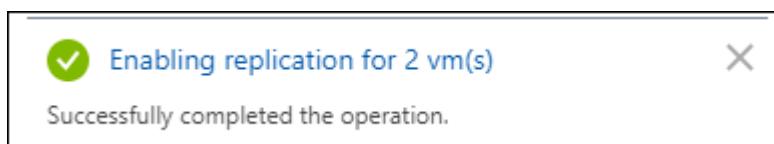
**Automation account**

BCDRContoso49

- Next, select **Enable replication**.



- The Azure portal will start the deployment. This deployment will take approximately 10 minutes to complete. Wait for replication to complete before moving to the next step.



11. The **BCDRRSV** blade should still have the **Site Recovery** option (under 'Getting started') selected.

Select **Step 2: Manage Recovery Plans**.

The screenshot shows the Azure Site Recovery blade for the BCDRRSV vault. The left sidebar has a red box around the 'Site Recovery' link under 'Getting started'. A red circle with '1' is on the 'Site Recovery' link, and another red circle with '2' is on the 'Manage recovery plans' link below it. The main content area is titled 'Protect your infrastructure for disaster recovery' and shows three options: 'Azure virtual machines', 'VMware machines to Azure', and 'Hyper-V machines to Azure'. Each option has a corresponding icon and a brief description. At the bottom, there are links for 'Protect your Hyper-V machines by replicating to' and 'Helpful links'.

12. Select **+Recovery plan**.

## Recovery plans

BCDRRSV

**+ Recovery plan**

**Filter items...**

Name	↑↓	Source
------	----	--------

To failover virtual machines individually, !

13. Fill in the **Create recovery plan** blade as follows:

- **Name:** BCDRlaaSPlan
- **Source:** Central US (*This is your primary region.*)
- **Target:** East US 2 (*This is your secondary region.*)
- **Allow items with deployment model:** Resource Manager
- **Select Items:** Select **WebVM1** and **WebVM2**.

## Create recovery plan

Up to 100 protected instances can be added to recovery plan. [Learn more](#)

Name \*

Source \*

Select this check box if you would like to failover machines across regions.

Target \*

Allow items with deployment model \* ⓘ

Selected items.  
2

**Create**

**Note:** It is **critical** to use the correct recovery plan name **BCDRIaaSPlan**. This plan name must match the name of the Azure Automation variable you created in the first task in this exercise.

14. Select **Create** to create the recovery plan. After a moment, the **BCDRIaaSPlan** Recovery plan will appear. Select it to review.

## Recovery plans

BCDRRSV

+ Recovery plan

Filter items...

Name	Source	Target
BCDRIaaSPlan	Central US	East US 2

15. When the **BCDRIaaSPlan** loads **notice**, it shows **2 VMs in the Source**, which is your **Primary Site**.
16. You will now customize the recovery plan to trigger the SQL failover and configure the web tier load-balancer during the failover process; select **Customize**.

17. Once the **BCDRiaasPlan** blade loads, select the **ellipsis** next to **All groups failover**, then select **Add pre-action** from the context menu.

Stage name	Details	
All groups shut down	2 machines in 1 group.	...
> All groups failover		...
> Group 1: Start	2 Machines	

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

**Note:** If nothing happens, select the **X** in the upper right corner and select **OK** when asked about discarding your changes. You will notice that the script is still added to the recovery plan.

## Insert action ...

Insert

**Script** Manual action

Name \*

ASRSQFailover

Script to be run during failover

Automation account name \* ⓘ

BCDRContoso22

Runbook name \* ⓘ

ASRSQFailover

**i** The above selected runbook will be executed in both directions:  
1. when recovery plan fails over from source to target, and  
2. when recovery plan fails over from target to source during failback.

OK

**Note:** As noted on the 'Insert action' blade, the ASRSQFailover runbook will be executed on both failover and failback. The runbook has been written to support both scenarios.

19. Once the **BCDRIaaSPlan** blade loads, select the **ellipsis** next to **Group 1: Start**, then select **Add post action** from the context menu.

## BCDRiaaSPlan

Recovery plan

+ Group Save Discard

Change group

i You have unsaved changes.

This recovery plan contains 2 machine(s). Up to 100 protected instances can be added to recovery plan. [Learn more.](#)

Stage name	Details	...
All groups shut down	2 machines in 1 group.	...
>All groups failover: Pre-steps	1 Step	...
Script: ASRSQLFailover	Script	...
> All groups failover		...
> Group 1: Start	2 Machines	<span style="border: 1px solid #0070C0; padding: 5px;">Delete</span> <span style="border: 1px solid #0070C0; padding: 5px;">Add protected items</span> <span style="border: 1px solid #0070C0; padding: 5px;">Add pre-action</span> <span style="border: 2px solid red; padding: 5px;">Add post action</span>

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

**Note:** If nothing happens, select the **X** in the upper right corner and select **OK** when asked about discarding your changes. You'll notice that the script is still added to the recovery plan.

## Insert action

Insert

Script    Manual action

Name \*

ASRWebFailover

Script to be run during failover

Automation account name \* ⓘ

BCDRContoso22

Runbook name \* ⓘ

ASRWEBFailover

**i** The above selected runbook will be executed in both directions:  
1. when recovery plan fails over from source to target, and  
2. when recovery plan fails over from target to source during failback.

**OK**

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

# BCDRIaaSPlan

Recovery plan

+ Group Save Discard Change group

i You have unsaved changes.

This recovery plan contains 2 machine(s). Up to 100 protected instances can be added to recovery plan. [Learn more.](#)

Stage name	Details	...
All groups shut down	2 machines in 1 group.	...
▼ All groups failover: Pre-steps	1 Step	...
Script: ASRSQLFailover	Script	...
> All groups failover		...
> Group 1: Start	2 Machines	...
▼ Group 1: Post-steps	1 Step	...
Script: ASRWEBFailover	Script	...

22. After a minute, the portal will provide a successful update notification. This means that your recovery plan is fully configured and ready to failover and back between the primary and secondary regions.

✓ Updating recovery plan 'BCDRIaaSPlan'...  
Successfully completed the operation.

23. Return to the Recovery Services Vault **BCDRRSV** blade and select the **Replicated Items** link under **Protected Items**. You should see **WebVM1** and **WebVM2**. The Replication Health should be **Healthy**. The Status will show the replication progress. Once both VMs show status **Protected** replication is complete, you will be able to test the failover.

The screenshot shows the Azure Recovery Services vault interface for 'BCDRRSV'. On the left, a navigation pane includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Identity, Private endpoint connections, Properties, Locks), Getting started (Backup, Site Recovery), Protected items (Backup items, Replicated items), and Replicated items. The 'Replicated items' link is highlighted with a red box. The main content area displays a table with columns for Name, Replication Health, and Status. Two rows are present: one for 'WebVM1' (Healthy, 90% Synchronized) and one for 'WebVM2' (Healthy, 93% Synchronized). A message at the top right indicates 'Finished loading data from service.'

Name	Replication Health	Status
WebVM1	Healthy	90% Synchronized
WebVM2	Healthy	93% Synchronized

**Note:** It can take up to 30 minutes for the replication to complete.

## Task 5: Configure a public endpoint using Azure Front Door

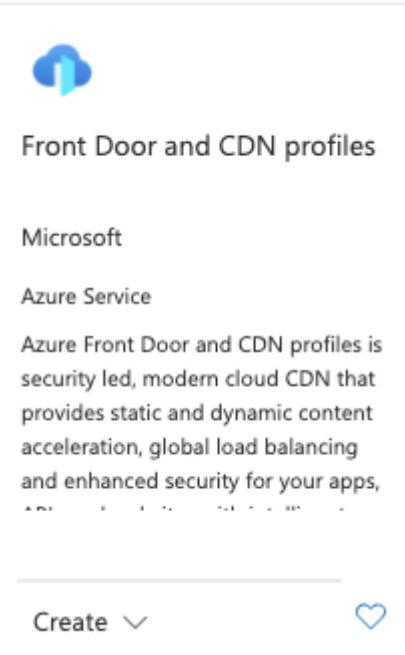
There is just one step remaining to complete your DR environment. After a failover to the DR site, the IP address for the Contoso application (the web-tier load balancer frontend IP address) will change. Therefore, users need to be directed to the failover IP address.

The redirection to the failover IP address can be achieved in either of two ways:

- Update the DNS record for the user endpoint to point to the new IP address. This update can be implemented using Azure Traffic Manager.
- Direct users to a proxy service and have that service forward traffic to the currently active endpoint. Azure Front Door provides such a service.

In this task, you will use the Front Door approach to configure a highly available endpoint that directs traffic to your primary or secondary site, depending on which site is currently available.

1. You will now build a Front Door to direct traffic to your Primary and Secondary Sites. From the Azure portal, select **+Create a resource**, then search for and select **Front Door and CDN profiles**. Select **Create**.



2. Select **Azure Front Door** and **Custom create**. Then select **Continue to create a Front Door**.

# Compare offerings

Microsoft Azure

Choose between Azure Front Door and other offerings.

## Azure Front Door

Azure Front Door is a secure cloud CDN which provides static and dynamic content acceleration, global load balancing and protection of your apps, APIs and websites with intelligent threat protection.

## Explore other offerings

See offerings for our Azure Front Door (classic) and Azure CDN Standard from Microsoft (classic), along with our partner offerings.

Choose between Azure Front Door options

## Quick create

Get started with a simplified web application deployment using default settings.

Define one endpoint with one origin and one WAF policy to get your front door up and running quickly.

Configure advanced settings and add endpoints as your needs evolve.

## Custom create

Leverage powerful configuration options to deploy a custom solution.

Design an endpoint with multiple domains and origin groups. Define routes to connect them, and add

Add endpoints to scale your deployment as your needs evolve.

**Continue to create a Front Door**

3. Complete the **Basics** tab of the **Create a Front Door** blade using the following inputs, then select **Next: Secrets >**.

- **Resource group:** Use existing / **ContosoRG1**
- **Location:** Automatically assigned based on the region of **ContosoRG1**.
- **Profile name:** ContosoFD1

- **Tier:** Standard

## Create a front door profile

Microsoft Azure

\* Basics    Secrets    \* Endpoint    Tags    Review + create

Azure Front Door is a modern application delivery network platform providing a secure, scalable CDN, dynamic site acceleration, and global HTTP(s) load balancing for your global web applications. [Learn more](#)

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*

ContosoRG1

[Create new](#)

Resource group location

East US 2

---

Profile details

Name \*

ContosoFD1

Tier \*

Standard  
 Content delivery optimized

Premium  
 Security optimized

---

[Review + create](#)

[< Previous](#)

Next: Secrets >

[Automation options](#)

4. Select **Next: Endpoint >**.

5. Select **Add an endpoint** to set the hostname of Front Door. In the **Add an endpoint** pane, enter the following values, then select **Add**:

- **Endpoint name:** contosoiaas
- **Status:** Leave **Enable this endpoint** selected.

# Add an endpoint

X

Microsoft Azure

The endpoint name specifies a desired subdomain on Front Door's default domain (i.e. .z01.azurefd.net) to route traffic from that host via Front Door. You can optionally onboard custom domains as well. [Learn more ↗](#)

Endpoint name \*

 contosoiaas

Endpoint hostname

contosoiaas-b8cyachmbfake6f2.z01.azurefd.net

Status  Enable this endpoint

**Add**

**Cancel**

## 6. Under **Routes** select + Add a route.

Create a front door profile ...

Microsoft Azure

\* Basics   Secrets   **\* Endpoint**   Tags   Review + create

Add an endpoint to get started. Add domains and create origin groups, then define routes to connect your domains and origin groups. Add security rules to complete your front door configuration. Later, you will be able to add endpoints and reuse your domains, origin groups, rule sets and WAF policies across endpoints in your front door profile. [Learn more ↗](#)

Routes	Domains	Origin group	Status	Provisioning state	+ Add a route	Security policy	+ Add a policy	Domain state
No results.						No results.		

## 7. Select **Add a new origin group**.

# Add a route

Microsoft Azure

A route maps your domains and matching URL path patterns to a specific origin group. [Learn more](#)

Name \*

ContosoRoute

Endpoint

contosoiaas-b8cyachmbfake6f2.z01.azurefd.net

Domains

Domains \*

contosoiaas-b8cyachmbfake6f2.z01.azurefd.net

[Add a new domain](#)

Patterns to match ⓘ

/\*

/path

Accepted protocols \*

HTTP only

Redirect

Redirect all traffic to use HTTPS

Origin group

Origin group \*

[Add a new origin group](#)

Origin path

Forwarding protocol \*

HTTP only

8. Give the new origin group the name of **ContosoOrigins**.

9. Select + **Add an origin**.

# Add an origin group

X

Microsoft Azure

An origin group is a set of origins to which Front Door load balances your client requests.

[Learn more ↗](#)

Name \*

ContosoOrigins



## Origins

Origins are the application servers where Front Door will route your client requests. Utilize any publically accessible application server, including App Service, Traffic Manager, Private Link, and many others. [Learn more ↗](#)

Add an origin

10. For adding an origin, use the following values. Leave all other values set to their default. Then select Add.

- Name: **ContosoWebPrimary**
- Origin type: Public IP Address
- Host name: ContosoWebLBPrimaryIP
- Priority: 1

# Add an origin

X

Microsoft Azure

Origins are your application servers. Front door will route your client requests to origins, based on the type, ports, priority, and weight you specify here. [Learn more](#)

← [Go back to origin group](#)

Name *	ContosoWeb ✓
Origin type *	Public IP Address ✓
Host name *	ContosoWebLBPrimaryIP ✓
Origin host header	20.96.144.96 ✓
Certificate subject name validation ⓘ	<input checked="" type="checkbox"/> Enable the validation
HTTP port *	80
HTTPS port *	443
Priority *	1 ✓
Weight *	1000
Status	<input checked="" type="checkbox"/> Enable this origin

**Add**

**Cancel**

11. Repeat step 10 and change the values to the following.

- Name: ContosoWebSecondary
- Origin type: Public IP Address
- Host name: ContosoWebLBSecondaryIP
- Priority: 2

12. Update **Interval (in seconds)** to 30. Click Add

# Add an origin group

X

Microsoft Azure

An origin group is a set of origins to which Front Door load balances your client requests.

[Learn more ↗](#)

Name \*

ContosoOrigins ✓

## Origins

Origins are the application servers where Front Door will route your client requests. Utilize any publicly accessible application server, including App Service, Traffic Manager, Private Link, and many others. [Learn more ↗](#)

+ Add an origin

Origin host name	Status	Priority	Weight	...
20.96.144.96	✓ Enabled	1	1000	...
20.69.189.42	✓ Enabled	2	1000	...

Session affinity

Enable session affinity

## Health probes

If enabled, front door will send periodic requests to each of your origins to determine their proximity and health for load balancing purposes. [Learn more ↗](#)

Status ⓘ

Enable health probes

Path \*

/

Protocol \* ⓘ

HTTP

HTTPS

Probe method \*

HEAD

Interval (in seconds) \* ⓘ

30

seconds ✓

## Load balancing

Configure the load balancing settings to define what sample set we need to use to call the backend as healthy or unhealthy. The latency sensitivity with value zero (0) means always send it to the fastest available backend, else Front Door will round robin traffic between the fastest and the next fastest backends within the configured latency sensitivity.

Add

Cancel

13. Enter the following values in **Add a route**. Leave all other values as default. Select **Add**.

- **Name:** ContosoRoute
- **Accepted protocols:** HTTP only
- **Redirect:** Uncheck **Redirect all traffic to use HTTPS.**
- **Origin group:** Ensure **ContosoOrigins** is selected.
- **Forwarding protocol:** HTTP only

## Add a route

Microsoft Azure

A route maps your domains and matching URL path patterns to a specific origin group. [Learn more](#)

**Name \***  ContosoRoute

**Endpoint**

**Domains**

**Domains \***  [Add a new domain](#)

**Patterns to match**

**Accepted protocols \***  HTTP only

**Redirect**  Redirect all traffic to use HTTPS

**Origin group**

**Origin group \***  [Add a new origin group](#) ContosoOrigins

**Origin path**

**Forwarding protocol \***  HTTP only  HTTPS only  Match incoming request

**Caching**  Enable caching

**Rules**

Add Cancel

14. Select **Review + Create**. Once validation has been completed, select **Create** to provision the Front Door service.

## Create a front door profile ...

Microsoft Azure

\*Basics   Secrets   \*Endpoint   Tags   Review + create

Add an endpoint to get started. Add domains and create origin groups, then define routes to connect your domains and origin groups. Add security rules to complete your front door configurations and WAF policies across endpoints in your front door profile. [Learn more](#)

The screenshot shows the 'Routes' section of the Azure Front Door configuration. A single route, 'ContosoRoute', is listed. It points to the domain 'contosoiaas-b8cyachmbfake6f2.z01.azurefd.net' and the origin group 'ContosoOrigins'. The route is marked as 'Enabled'. The 'Review + create' button at the bottom left is highlighted with a red box.

Routes ↑↓	Domains ↑↓	Origin group ↑↓	Status ↑↓	Provisioning state ↑↓
ContosoRoute	1 selected	ContosoOrigins	Enabled	...
contosoiaas-b8cyachmbfake6f2.z...				

Review + create   < Previous   Next: Tags >   Automation options

15. Navigate to the Azure Front Door resource. Select the **Frontend host** URL of Azure Front Door, and the Policy Connect web application will load. The web application is routing through the **ContosoWebLBPrimary** External Load Balancer configured in front of **WEBVM1** and **WEBVM2** running in the **Primary** Site in **ContosoRG1** resource group and connecting to the SQL AlwaysOn Listener at the same location.

**ContosoFD1** ...

Front Door and CDN profiles

Search (Cmd+/) Purge cache Origin response timeout Delete Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings

- Front Door manager
- Domains
- Origin groups
- Rule set
- Security policies
- Optimizations
- Secrets
- Properties
- Locks

**Essentials**

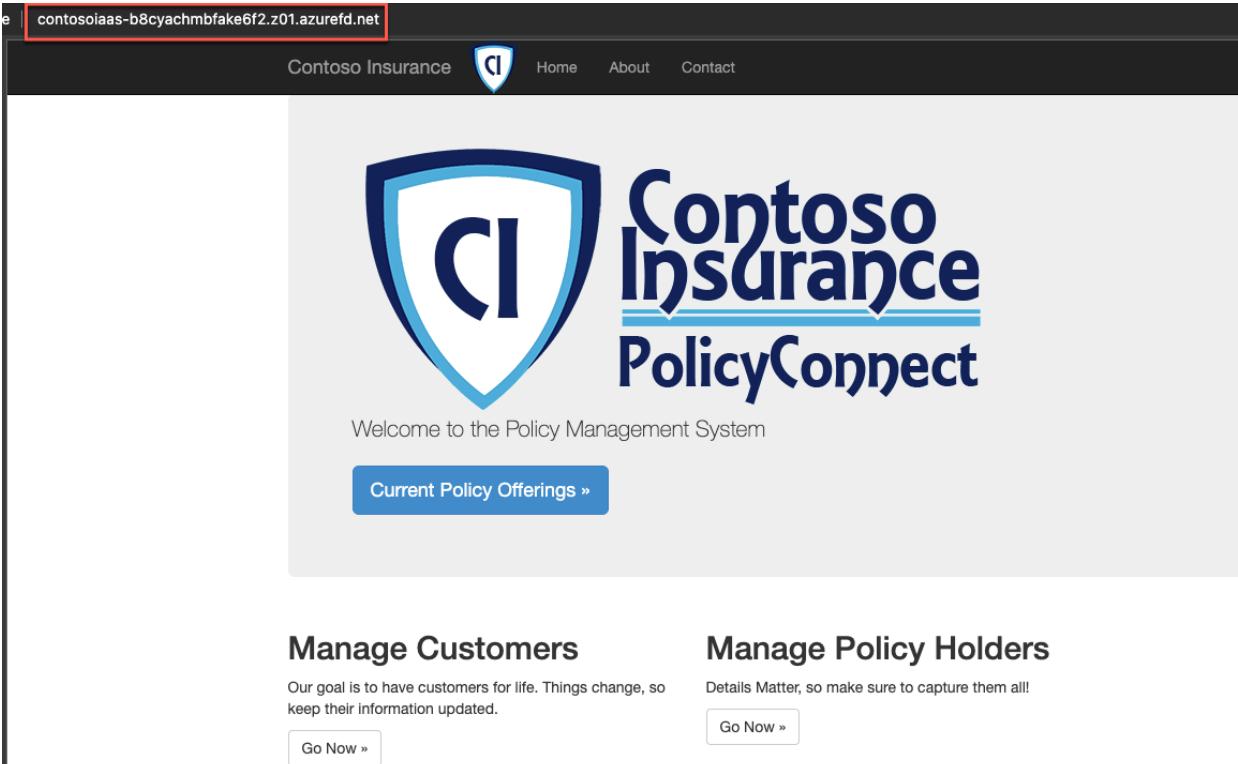
Resource group ([move](#)) : [ContosoRG1](#)  
 Status : Active  
 Location : Global  
 Subscription ([move](#)) : [Demo Creation](#)  
 Subscription ID : e223f1b3-d19b-4cfa-98e9-bc9be62717bc  
 Tags ([edit](#)) : [Click here to add tags](#)

**Properties** Monitoring

**Endpoints**

Endpoint hostname : [contosoiaas-b8cyachmbfake6f2.z01.azurefd.net](#) (Provision succeeded, Enabled)

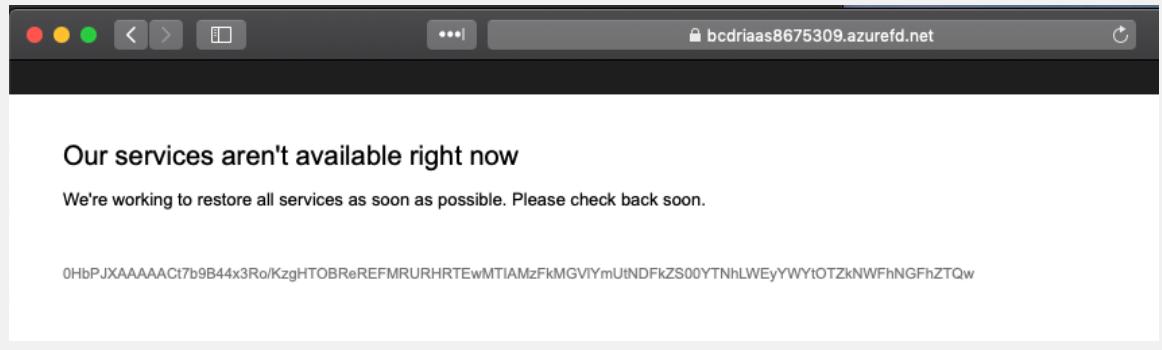
**Security policy**



**Note:** Be sure to use **HTTP** to access the Azure Front Door **frontend host** URL. The lab configurations only support HTTP for Front Door since WebVM1 and WebVM2 are only set up for HTTP support, not HTTPS (no SSL\TLS).

**Note:** If you get an "Our services aren't available right now" error (or a 404-type error) accessing the web application, then continue with the lab and come back to this later. Sometime this can take a ~10 minutes for the routing rules to publish before it's "live".

If you continue to have this issue beyond 15 minutes, ensure that you are using the correct backend host header (Step 5) and using HTTP for both the routing rules and the health probes of the backend pools. (Step 4).



## Exercise 3: Enable Backup for the Contoso application

Duration: 30 minutes

In this exercise, you will use Azure Backup to enable backup for the Contoso application. You will configure backup for the web tier VMs and the SQL Server database.

### Task 1: Create the Azure Backup resources

Azure Backup and Azure Site Recovery are implemented using the same Azure resource type, the Recovery Services Vault. However, for Azure Backup, the vault must be deployed to the same region as the resources being protected; in this case, the primary site is in Central US. In contrast, for Azure Site Recovery, the vault was deployed to the secondary region. In this task, you will create the vault in the primary region for use by Azure Backup.

1. From the Azure portal, select **+Create a resource**, search for and select **Backup and Site Recovery**, and select **Create**.

The screenshot shows the Azure portal interface for creating a new resource. The path is Home > Create a resource > Marketplace > Backup and Site Recovery. The 'Backup and Site Recovery' blade is displayed, showing a Microsoft logo, a 3.8 rating (578 reviews), and a 'Plan' dropdown set to 'Backup and Site Recovery'. A large blue 'Create' button is prominently displayed at the bottom of the blade, with a red box drawn around it to indicate it as the next step.

2. Complete the **Recovery Services Vault** blade using the following inputs, then select **Review and Create**, followed by **Create**:
- A disaster recovery and data protection strategy keeps your business running when unexpected events occur.
- The Backup service is Microsoft's born in the cloud backup solution to backup data that's located on-premises and in Azure. It replaces your existing on-premises or offsite backup solution with a reliable, secure and cost competitive cloud backup solution. It also provides the flexibility of protecting your assets running in the cloud. You can backup Windows Servers, Windows Clients, Hyper-V VMs, Microsoft workloads, Azure Virtual Machines (Windows and Linux) with its in-built resilience and high SLAs. [Learn more](#).
- The Site Recovery service ensures your servers, virtual machines, and apps are resilient by replicating them so that when disasters and outages occur you can easily fail over to your replicated environment and continue working. When services are resumed you simply failback to your primary location with uninterrupted access. Site Recovery helps protect a wide range of Microsoft and third-party workloads. [Learn more](#).

2. Complete the **Recovery Services Vault** blade using the following inputs, then select **Review and Create**, followed by **Create**:

- **Resource Group:** ContosoRG1
- **Name:** BackupRSV
- **Location:** *your primary region*

\* Basics Tags Review + create

### Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription \* ⓘ

Resource group \* ⓘ  1

### Instance Details

Vault name \* ⓘ  2

Region \* ⓘ  3

Review + create

4

Next: Tags

3. Once the deployment completes, navigate to the **BackupRSV** resource and select **Properties**.

# BackupRSV | Properties

Recovery Services vault

Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

### Settings

- Identity
- Private endpoint connections
- Properties**
- Locks
- Export template

### Getting started

- Backup
- Site Recovery

### Protected items

- Backup items
- Replicated items

### Manage

- Backup policies
- Backup Infrastructure

Status  
Active

Location  
Central US

Subscription Name  
Visual Studio Enterprise – MPN

Subscription Id  
41811f87-4f0d-44d0-bec9-a9b162257403

Resource group  
ContosoRG1

Diagnostics Settings  
[Update](#)

---

BACKUP

Backup Configuration  
[Update](#)

Security Settings  
[Update](#)

Security PIN  
[Generate](#)

- Under **Backup Configuration**, select **Update**. In the Backup Configuration blade, check that the storage replication type is set to **Geo-redundant** and set the Cross-Region Restore option to **Enable** then **Save** your changes and close the Backup Configuration panel.



## Backup Configuration

X

3

Save

Discard

Storage replication type

Locally-redundant   Zone-redundant

Geo-redundant

1

- i** This option cannot be changed after protecting items. Geo-Redundant Storage (GRS) provides a higher level of data availability than Zonal-Redundant Storage and Local-Redundant Storage. Zonal -Redundant Storage helps to replicate the data in the availability zones of the same region. Review the trade-offs between lower cost and higher cost availability [here](#).

Cross Region Restore

Enable

Disable

Note:

2

- This allows you to **restore in the secondary region** for both BCDR drills and outage scenarios.
- This is **available for Azure Virtual Machines** and SQL/SAP HANA databases running inside Azure VMs in this vault. No support for classic VMs.
- Cross Region Restore is currently **non-reversible** storage property.

Learn more about [Cross Region Restore](#) and [pricing impact](#).

**Note:** This enables backups from the primary site to be restored in the DR site if required.

5. Still in the BackupRSV Properties blade, under **Security Settings**, select **Update**. Under Soft Delete, select **Disabled**, then **Save** your changes and close the Security Settings panel.

# Security Settings

X

BackupRSV

2

 Save

 Discard

- i** If you have enabled [Azure multi-factor authentication](#), you will be required to additionally authenticate using another device (for example, a mobile phone) while signing in to the Azure portal.

## Soft Delete (For workloads running in Azure)

Enable this setting to protect backup data for Azure VM, SQL Server in Azure VM and SAP HANA in Azure VM from accidental deletes. [Learn More](#)

Enable

Disabled

1

**!** All Future deletes will be immediate and will not have soft delete protection. [Learn more](#).

This action will not impact items already in soft deleted state. If you wish to delete these permanently with immediate effect please refer to the documentation. [Learn more](#).

## Security Features (For workloads running on-premises)

Enable this setting to protect hybrid backups against accidental deletes and add additional layer of authentication for critical operations. Refer [this](#) link for minimum agent version requirement to enable this setting. [Learn more](#).

Enabled

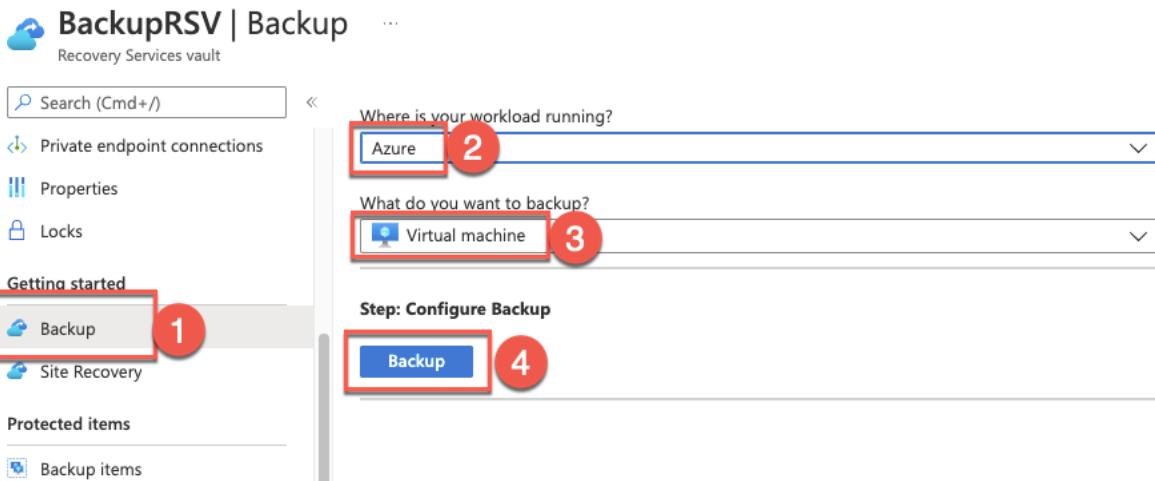
Disable

**Note:** In a production environment, you should leave Soft Delete enabled. However, it is better to disable this feature for this lab since leaving it enabled makes it more difficult to clean up your lab resources once the lab is complete.

## Task 2: Enable Backup for the Web tier

In this task, you will configure Azure Backup for the Web tier virtual machines. Of course, if the Web VMs are stateless, backup may not be required, so long as the VM image and/or application installation are protected.

- From the **BackupRSV** Recovery Services vault blade, under 'Getting Started', select **Backup**. Under 'Where is your workload running?', select **Azure**. Under 'What do you want to backup?', select **Virtual machine**. Then select **Backup**.



2. On the 'Configure Backup' blade, Leave **Standard** selected and select **Create a new policy** and fill in the Create Policy blade as follows:

- **Policy name:** WebVMPolicy
- **Backup schedule:** Daily, 9:00 PM, UTC
- **Retain instant recovery snapshots for:** 2 day(s)
- **Retention of daily backup point:** Enabled, 180 days
- **Retention of weekly backup point:** Enabled, Sunday, 12 weeks
- **Retention of monthly backup point:** Enabled, First Sunday, 24 months
- **Retention of yearly backup point:** Enabled, day-based, January 1, 5 years
- **Azure Backup Resource Group:** ContosoBackupRG

When finished, select **OK**.

## Create policy

X

Azure Virtual Machine

Policy name ⓘ

WebVMPolicy ✓

Backup schedule

Frequency \*

Daily

Time \*

9:00 PM

Timezone \*

(UTC) Coordinated Universal Time

Instant Restore ⓘ

Retain instant recovery snapshot(s) for

2

Day(s) ⓘ

Retention range

Retention of daily backup point

At

For

9:00 PM

180

Day(s)

Retention of weekly backup point

On \*

At

For

Sunday

9:00 PM

12

Week(s)

Retention of monthly backup point

Week Based  Day Based

On \*

Day \*

At

For

First

Sunday

9:00 PM

24

Month(s)

Retention of yearly backup point

Week Based  Day Based

In \*

On \*

At

For

January

1

9:00 PM

5

Year(s)

**i** Azure Backup service creates a separate resource group to store the instant recovery points of managed virtual machines. The default naming format of resource group created by Azure Backup service is AzureBackupRG\_(Geo)\_n. It is optional to customize the name as per your requirement. [Learn More](#)

Azure Backup Resource Group (Optional) ⓘ

ContosoBackupRG ✓

n

Suffix (Optional)

OK

3. On the 'Backup' blade, under 'Virtual Machines', select **Add**. Select the **WebVM1** and **WebVM2** virtual machines, then **OK**.

**Backup**

BackupRSV

**Policy**

(new) WebVMPolicy

[Create a new policy](#)**BACKUP FREQUENCY**

Daily at 9:00 AM UTC

**Instant Restore**

Retain instant recovery snapshot(s) for 2 day(s)

**RETENTION RANGE****Retention of daily backup point**

Retain backup taken every day at 9:00 AM for 180 Day(s)

**Retention of weekly backup point**

Retain backup taken every week on Sunday at 9:00 AM for 12 Week(s)

**Retention of monthly backup point**

Retain backup taken every month on First Sunday at 9:00 AM for 24 Month(s)

**Retention of yearly backup point**

Retain backup taken every year in January on 1 at 9:00 AM for 5 Year(s)

**Virtual Machines**

Virtual machine name	Resource Group
No Virtual Machines Selected	
<a href="#">Add</a>	

1

[Enable Backup](#)

**Select virtual machines**

<input type="text"/> Filter items ...		
	Virtual machine name	Resource Group
<input type="checkbox"/>	ADVM1	ContosoRG1
<input type="checkbox"/>	ADVM2	ContosoRG1
<input type="checkbox"/>	SQLVM1	ContosoRG1
<input type="checkbox"/>	SQLVM2	ContosoRG1
<input checked="" type="checkbox"/>	WebVM1	ContosoRG1
<input checked="" type="checkbox"/>	WebVM2	ContosoRG1

2

OK

4. Select **Enable Backup** and wait for the deployment to complete.

 Deployment succeeded 10:32 AM

Deployment '[ConfigureProtection-2020529103053](#)' to  
resource group '[ContosoRG1](#)' was successful.

5. From the **BackupRSV** Recovery Services vault blade, under 'Protected items', select **Backup items**.

The blade should show 2 Azure VMs protected.

**BackupRSV | Backup items**

Recovery Services vault

Search (Ctrl+ /) Refresh

Export template

Primary Region Secondary Region

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	2
SAP HANA in Azure VM	0
SQL in Azure VM	0
Azure Storage (Azure Files)	0
DPM	0
Azure Backup Server	0
Azure Backup Agent	0

Getting started

Backup

Site Recovery

Protected items

Backup items (selected)

Replicated items

Manage

Backup policies

6. Select **Azure Virtual Machine**. The 'Backup Items (Azure Virtual Machine' blade loads, listing **WebVM1** and **WebVM2**). In both cases, the 'Last Backup Status' is 'Warning (Initial backup pending)'.

Backup Items (Azure Virtual Machine)

BackupRSV

Refresh Add Filter

Fetching data from service completed.

Name	Resource Group	Backup Pre-Check	Last Backup Status	Latest restore point
WebVM1	ContosoRG1	Passed	Warning(Initial backup pending)	...
WebVM2	ContosoRG1	Passed	Warning(Initial backup pending)	...

7. Select **View details** for **WebVM1** to open the 'WebVM1' backup status blade. Select **Backup now**, leave the default backup retention and select **OK**.

**WebVM1**

**Backup now** | Restore VM | File Recovery | Stop backup | Resume backup | Delete backup data | Restore to Secondary Region | Undelete

For backups, try our new Backup Center. It offers Azure Backup customers a unified view of Recovery Services Vaults used for backup in Azure. It also provides improved sorting and filtering along with new governance.

**Essentials**

Recovery services vault : [BackupRSV](#)

Subscription (move) : [REDACTED]

Subscription ID : [REDACTED]

Alerts (in last 24 hours) : [View alerts](#)

Jobs (in last 24 hours) : [View jobs](#)

Backup Pre-Check : Passed

Last backup status : Warning (Initial backup pending)

Backup policy : [WebVMPolicy](#)

Oldest restore point : -

**Restore points**

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, as well as archive, [click here](#).

Long term retention points can be moved to vault-archive. To move all 'recommended recovery points' to vault-archive tier, [click here](#).

CRASH CONSISTENT	APPLICATION CONSISTENT	FILE-SYSTEM CONSISTENT	Time ↑↓	Consistency	Recovery type
0	0	0			

No restore points available.

## Backup Now

WebVM1

Retain Backup Till [\(i\)](#)



**OK**

**Note:** The backup policy created earlier determines the retention period for scheduled backups. For on-demand backups, the retention period is specified separately.

8. Close the WebVM1 backup status blade. Then, repeat the above step to trigger an on-demand backup for **WebVM2**.
9. From the **BackupRSV** Recovery Services vault blade, under 'Monitoring', select **Backup Jobs** to load the Backup Jobs blade. This blade shows the current status of each backup job. The blade should show two completed jobs (configuring backup for WebVM1 and WebVM2) and two in-progress jobs (backup for WebVM1 and WebVM2).

**BackupRSV | Backup Jobs**

Recovery Services vault

Protected items

- Backup items
- Replicated items

Manage

- Backup policies
- Backup Infrastructure
- Site Recovery infrastructure
- Recovery Plans (Site Recovery)
- Backup Reports

Monitoring

- Alerts
- Metrics
- Diagnostic settings
- Logs
- Backup Jobs** (highlighted with a red box)
- Site Recovery jobs
- Backup Alerts
- Site Recovery events

Filtered by: Item Type - All, Operation - All, Status - All, Start Time - 5/9/2022, 5:17:15 PM, End Time - 5/10/2022, 5:17:15 PM

For backups, try our new Backup Center. It offers Azure Backup customers a unified view of Recovery Services Vaults used for backup the new experience.

All data fetched from the service.

Filter items ...

Workload name ↑	Operation	Status	Type
webvm2	Backup	In progress	Azure Virtual machine
webvm1	Backup	In progress	Azure Virtual machine
webvm1	Configure backup	Completed	Azure Virtual machine
webvm2	Configure backup	Completed	Azure Virtual machine

< Previous Page 1 of 1 Next >

10. Select **View Details** for **WebVM1** to open the backup job view. This backup job view shows the detailed status of the tasks within the backup job.

## Backup

webvm1

Refresh Cancel Deploy Template Feedback

### Job details

VM Name	webvm1
Recovery Point Expiry Time in UTC	6/9/2022 9:16:32 PM
Activity ID	eaa10f8b-ff32-48e9-9367-602fd2ae104b

### Sub tasks

Name	Status
Take Snapshot	In progress
Transfer data to vault	Not started

**Note:** To restore from a backup, it suffices that the 'Take Snapshot' task is complete. Transferring the data to the vault does not need to be complete since recent backups can be restored from the snapshot.

You can proceed to the next task without waiting for the backup jobs to complete.

### Task 3: Enable Backup for the SQL Server tier

In this task, you will configure backup for the SQL Server database.

There are two approaches to backup for SQL Server running on Azure VMs. One uses native SQL managed backup to Azure storage. The other uses Azure Backup. For this lab, you will use Azure Backup.

Before enabling Azure Backup, you will first register the SQL Server VMs with the SQL VM resource provider. This resource provider installs the **SqllaaSExtension** onto the virtual machine. Azure Backup uses this extension to configure the **NT SERVICE\AzureWLBackupPluginSvc** account with the necessary permissions to discover databases on the virtual machine.

1. In a new browser tab, navigate to <https://shell.azure.com> and open a **PowerShell** session.
2. Unless you have done so previously, you will need to register your Azure subscription to use the **Microsoft.SqlVirtualMachine** resource provider. In the Cloud Shell window, execute the following command:

```
Register-AzResourceProvider -ProviderNamespace
Microsoft.SqlVirtualMachine
```

```
PS /> Register-AzResourceProvider -ProviderNamespace Microsoft.SqlVirtualMachine
ProviderNamespace : Microsoft.SqlVirtualMachine
RegistrationState : Registering
ResourceTypes : {SqlVirtualMachineGroups, SqlVirtualMachines, SqlVirtualMachineGroups/AvailabilityGroupListeners, operations...}
Locations : {West Central US, Brazil South, West Europe, Australia Central...}
```

**Note:** It may take several minutes to register the resource provider. Wait until the registration is complete before proceeding to the next step. You can check the registration status using **Get-AzResourceProvider -ProviderNamespace Microsoft.SqlVirtualMachine**.

3. Register **SQLVM1** with the resource provider by executing the following command in the Cloud Shell window. Ensure that **-Location** matches the location SQLVM1 is deployed.

```
New-AzSqlVM -Name 'SQLVM1' -ResourceGroupName 'ContosoRG1' -
SqlManagementType Full -Location 'Central US' -LicenseType PAYG
```

```
PS /> New-AzSqlVM -Name 'SQLVM1' -ResourceGroupName 'ContosoRG1' -SqlManagementType Full -Location 'Central US' -LicenseType PAYG
Name ResourceGroupName LicenseType Sku Offer SqlManagementType
---- ----- ----- ----- ----- -----
SQLVM1 ContosoRG1 PAYG Developer SQL2017-WS2016 Full
```

**Note:** This will register the resource provider using the **Full** management mode. This change causes the SQL service to restart, which may impact production applications. To avoid this restart in production environments, you can alternatively register the resource provider in **LightWeight** mode and upgrade later during a scheduled maintenance window.

4. Register **SQLVM2** and **SQLVM3** with the resource provider using the following commands. Ensure you specify the correct locations.

```
New-AzSqlVM -Name 'SQLVM2' -ResourceGroupName 'ContosoRG1' -
SqlManagementType Full -Location 'Central US' -LicenseType PAYG
New-AzSqlVM -Name 'SQLVM3' -ResourceGroupName 'ContosoRG2' -
SqlManagementType Full -Location 'East US 2' -LicenseType PAYG
```

**Note:** This lab uses SQL Server under a 'Developer' tier license. When using SQL Server in production at the 'Standard' or 'Enterprise' tier, you can specify **DR** as the license type for failover servers (each full-price server includes a license for 1 DR server). The DR license type reduces your licensing cost significantly. Check the SQL Server licensing documentation for full details.

5. In the Azure portal, navigate to the **ContosoRG1** resource group. In addition to the SQLVM1 and SQLVM2 virtual machines, there are now parallel SQLVM1 and SQLVM2 resources of type 'SQL virtual machine'. These additional resources provide additional management capabilities for SQL Server in Azure virtual machines.

<input type="checkbox"/> Name ↑↓	Type ↑↓
<input type="checkbox"/> PrimaryBastionIP	Public IP address
<input type="checkbox"/> SQLVM1	Virtual machine
<input type="checkbox"/> SQLVM1	SQL virtual machine
<input type="checkbox"/> SQLVM1DataDisk1	Disk
<input type="checkbox"/> SQLVM1NIC	Network interface
<input type="checkbox"/> SQLVM1OSDisk	Disk
<input type="checkbox"/> SQLVM2	Virtual machine
<input type="checkbox"/> SQLVM2	SQL virtual machine
<input type="checkbox"/> SQLVM2DataDisk1	Disk

6. Select the **SQLVM1** virtual machine (the standard VM resource, not the SQL virtual machine resource). Then select **Extensions**. Note that the **SqllaaSExtension** has been installed on the virtual machine.

The screenshot shows the Azure portal's Extensions blade for a virtual machine named SQLVM1. The left sidebar lists options like Size, Security, Advisor recommendations, Extensions (which is selected and highlighted with a red box), Continuous delivery, and Availability + scaling. The main area displays a table of installed extensions:

Name	Type	Version	Status	...
InstallDB	Microsoft.Compute.CustomScriptExtension	1.*	Provisioning succeeded	...
JoinDomain	Microsoft.Compute.JsonADDomainExtension	1.*	Provisioning succeeded	...
SqllaaSExtension	Microsoft.SqlServer.Management.SqllaaSAgent	2.*	Provisioning succeeded	...

With the SQL virtual machine resources created and the SQL IaaS extension installed, you can now configure Azure Backup for virtual machines.

7. In the Azure portal, navigate to the **BackupRSV** Recovery Services Vault resource in **ContosoRG1**. Under 'Getting started', select **Backup**. Under 'Where is your workload running?', select **Azure**. Under 'What do you want to backup?', select **SQL Server in Azure VM**. Then select **Start Discovery**.

The screenshot shows the Azure portal's Backup blade for the BackupRSV Recovery Services Vault. The left sidebar shows options like Settings, Identity, Private endpoint connections, Properties, Locks, Getting started (with Backup selected and highlighted with a red box, labeled 1), Site Recovery, Protected items (Backup items, Replicated items), and Manage.

The main area is divided into two steps:

- Step 1: Discover DBs in VMs**: It asks "Where is your workload running?" (Azure is selected and highlighted with a red box, labeled 2) and "What do you want to backup?" (SQL Server in Azure VM is selected and highlighted with a red box, labeled 3). A message says "(No DBs discovered) Click 'Start Discovery' to discover databases and validate backup permissions".
- Step 2: Configure Backup**: It says "Complete previous step".

A prominent blue button labeled "Start Discovery" is highlighted with a red box and labeled 4.

8. In the 'Select Virtual Machines' blade, select **SQLVM1** and **SQLVM2**, then select **Discover DBs**.

## Select Virtual Machines

X



For AlwaysOn clusters, ensure that all the nodes(VMs) of the cluster in the same Geo are selected. Selected nodes (VMs) will be registered to the vault

Filter items...

VIRTUAL MACHINE NAME	RESOURCE GROUP	↑↓
<input type="checkbox"/> ADVM1	ContosoRG1	
<input type="checkbox"/> ADVM2	ContosoRG1	
<input checked="" type="checkbox"/> SQLVM1	ContosoRG1	
<input checked="" type="checkbox"/> SQLVM2	ContosoRG1	
<input type="checkbox"/> WebVM1	ContosoRG1	
<input type="checkbox"/> WebVM2	ContosoRG1	

Selected Virtual Machines

>

2

Azure Backup will need SQL sysadmin privilege for doing backups. It will create NT Service\AzureWLBackupPluginSvc account on the selected VMs which needs to be added to SQL login and given SQL sysadmin privilege. In case of a SQL Marketplace VM, Azure Backup will invoke SQL IaaS extension to automatically get required permissions. [Learn More](#)

**Discover DBs**

9. This will trigger a deployment. Wait for the deployment to complete (this may take several minutes).



Deployment succeeded

X

Deployment '[RegisterProtectableContainers-2020529115610](#)' to resource group '[ContosoRG1](#)' was successful.

10. On the 'BackupRSV' blade, select **Configure Backup**.

BackupRSV | Backup

Recovery Services vault

Search (Cmd+/)

Settings

- Identity
- Private endpoint connections
- Properties
- Locks

Getting started

- Backup**
- Site Recovery

Protected items

- Backup items
- Replicated items

Manage

Where is your workload running? Azure

What do you want to backup? SQL Server in Azure VM

**Step 1: Discover DBs in VMs**

(No DBs discovered) Click 'Start Discovery' to discover databases and validate backup permissions

**Start Discovery**

**Step 2: Configure Backup**

**Configure Backup**

11. On the 'Backup' blade, select **Add**.

Configure Backup

Backup policy \* ⓘ

HourlyLogBackup

Create a new policy

Policy Details

Full Backup

**Backup Frequency**  
Daily at 3:30 AM UTC

Retention of daily backup point  
Retain backup taken every day at 3:30 AM for 30 Day(s)

Log Backup

**Backup Frequency**  
Every 1 hour(s)

**Retained for**  
30 days

Log backup for DBs in simple recovery model will be skipped.

SQL Databases

Database	Instance or AlwaysOn AG
No items selected for backup	

**Add**

12. On the 'Select items to backup' blade, select the > icon next to the **BCDRAOG\BCDRAOG** entry to show the databases. Note that the ContosoInsurance database is listed. Change the **AutoProtect** setting for BCDRAOG to **ON**, then select **OK**.

## Select items to backup

Refresh Rediscover DBs

To discover more SQL servers go back to Start Discovery

Filter items...

INSTANCE or AlwaysOn AG

	AUTOPROTECT
<input checked="" type="checkbox"/> <b>BCDRAOG\BCDRAOG</b>	ON
<input checked="" type="checkbox"/> ContosoInsurance	OFF
> <input type="checkbox"/> <a href="#">sqlvm1.contoso.com\MSSQLSERVER</a>	OFF
> <input type="checkbox"/> <a href="#">sqlvm2.contoso.com\MSSQLSERVER</a>	OFF

Selected Items ([View items](#))  
0 individual database(s), 1 instance(s)/availability group(s) with auto-protect

**OK**

**Note:** Using AutoProtect backups up the current database and any future databases on this Always On Availability Group.

**Note:** You may also want to backup system databases on each of the SQL Servers.

13. On the 'Backup' blade, note that **BCDRAOG\BCDRAOG** is now listed for backup. Leave the policy as the default **HourlyLogBackup** policy. Select **Enable Backup** and wait for the deployment to complete.

## Configure Backup

BackupRSV

**Retention of daily backup point**

Retain backup taken every day at 6:30 AM for 30 Day(s)

Log Backup

**Backup Frequency**

Every 1 hour(s)

**Retained for**

30 days

**i** Log backup for DBs in simple recovery model will be skipped.

SQL Databases

Database

**BCDRAOG\BCDRAOG**

Add

Instance or AlwaysOn AG

**Enable backup**

14. In the **BackupRSV** Recovery Service Vault, navigate to the **Backup Jobs** view. You should see a backup configuration job in progress for the ContosoInsurance database. (If this job does not show immediately, wait a minute and select **Refresh**.)

The screenshot shows the 'BackupRSV | Backup Jobs' page. On the left, a navigation menu includes 'Protected items', 'Manage', 'Monitoring', 'Logs' (with 'Backup Jobs' highlighted), and 'Automation'. The main area displays a table of backup jobs:

Workload name	Operation	Status	Type
ContosoInsurance	Configure backup	<span style="color: blue;">In progress</span>	Azure Workload
SQLVM1	Register	<span style="color: green;">Completed</span>	Azure Workload
SQLVM2	Register	<span style="color: green;">Completed</span>	Azure Workload
webvm2	Backup	<span style="color: green;">Completed</span>	Azure Virtual machine
webvm1	Backup	<span style="color: green;">Completed</span>	Azure Virtual machine
webvm1	Configure backup	<span style="color: green;">Completed</span>	Azure Virtual machine
webvm2	Configure backup	<span style="color: green;">Completed</span>	Azure Virtual machine

At the bottom, there are navigation buttons: < Previous, Page 1 of 1, Next >.

15. Wait for the backup configuration job to complete. Use the **Refresh** button to monitor progress. The configuration job will take several minutes.

16. Select **Backup items**, then select **SQL in Azure VM**.

The screenshot shows the 'BackupRSV | Backup items' page. On the left, a navigation menu includes 'Locks', 'Export template', 'Getting started' (with 'Backup' and 'Site Recovery' listed), 'Protected items' (with 'Backup items' highlighted), and 'Manage'.

In the main area, a table shows backup management types and their counts:

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	2
<span style="border: 2px solid red; padding: 2px;">SQL in Azure VM</span>	1
SAP HANA in Azure VM	0
Azure Storage (Azure Files)	0
DPM	0
Azure Backup Server	0
Azure Backup Agent	0

17. From the backup items list, note that the **contosoinsurance** database has status **Warning (Initial backup pending)**.

## Backup Items (SQL in Azure VM)

BackupRSV

X

⟳ Refresh + Add

With Backup center, you can view all your SQLDataBases items across vaults, subscriptions and regions in a single pane of glass. Click here to use the new experience. →

✓ All data fetched from the service.

Filter items ...				
Database ↑↓	Instance or AlwaysOn ... ↑↓	Type ↑↓	Backup Status	Details
ContosoInsurance	contoso.com\BCDRAOG	Always on AG	<span>⚠ Warning (Initial backup pending)</span>	<span>View details</span>
< Previous	Page	1	of 1	Next >

18. Select **View details** on the **contosoinsurance** database and select **Backup now**

ContosoInsurance

Backup Item

Backup now Restore Restore to secondary region Stop backup Delete backup data

^ Essentials

Recovery services vault : [BackupRSV](#)

19. Review the default backup settings, then select **OK** to start the backup.

## Backup Now

ContosoInsurance

### Backup Type

Full



### Compression ⓘ

Enable

Disable

**OK**

20. The backup process starts. You can monitor progress from the **Backup Job** pane.

Workload name	Operation	Status	Type
ContosoInsurance [BCDRAOG...]	Backup (Full)	<span>In progress</span>	Azure Workload
ContosoInsurance	Configure backup	<span>Completed</span>	Azure Workload
SQLVM1	Register	<span>Completed</span>	Azure Workload
SQLVM2	Register	<span>Completed</span>	Azure Workload
webvm2	Backup	<span>Completed</span>	Azure Virtual machine
webvm1	Backup	<span>Completed</span>	Azure Virtual machine
webvm1	Configure backup	<span>Completed</span>	Azure Virtual machine
webvm2	Configure backup	<span>Completed</span>	Azure Virtual machine

**Note:** You can continue to the next step in the lab without waiting for the backup job to complete.

## Exercise 4: Validate resiliency

Duration: 90 minutes

This exercise will validate the high availability, disaster recovery, and backup solutions you have implemented in the earlier lab exercises.

### Task 1: Validate High Availability

In this task, we will validate high availability for both the Web and SQL tiers.

1. In the Azure portal, open the **ContosoRG1** resource group. Select the public IP address for the web tier load-balancer, **ContosoWebLBPrimary**. Select the **Overview** tab, copy the DNS name to the clipboard, and navigate to it in a different browser tab.
2. The Contoso application should load in your browser tab. Select **Current Policy Offerings** to view the policy list - this shows the database is accessible. As an additional check, edit an existing policy and save your changes to show that the database is writable.
3. Open an Azure Bastion session with **SQLVM1** (with username `adadmin@contoso.ins` and password `Demo!pass123`). Open **SQL Server Management Studio** and connect to **SQLVM1** using Windows Authentication. Locate the BCDRAOG availability group, right-click and select **Show Dashboard**. Note that the dashboard shows **SQLVM1** as the primary replica.



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	Secondary	Synchronous co...	Automatic	Automatic	Synchronized	
✓	SQLVM3	Secondary	Asynchronous co...	Manual	Automatic	Synchronizing	

4. Using the Azure portal, stop both **WebVM1** and **SQLVM1**. Wait a minute for the VMs to stop.

5. Refresh the browser tab with the Contoso application. The application still works. Confirm again that the database is writable by changing one of the policies.

6. Open an Azure Bastion session with **SQLVM2** (with username `adadmin@contoso.ins` and password `Demo!pass123`). Open **SQL Server Management Studio** and connect to **SQLVM2** using Windows Authentication. Locate the BCDRAOG availability group, right-click and select **Show Dashboard**. Note that the dashboard shows **SQLVM2** as the primary replica, and there is a critical warning about **SQLVM1** not being available.



BCDRAOG: hosted by SQLVM2 (Replica role: Primary)

Availability group state: Critical --- Critical (1), Warnings (3)

Primary instance: SQLVM2

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	Secon...	Synchronous co...	Automatic	Automatic	Not Synchronizing	<span style="border: 2px solid red; padding: 2px;">Critical ...</span>
✓	SQLVM2	Primary	Synchronous co...	Automatic	Automatic	Synchronized	
✓	SQLVM3	Secon...	Asynchronous co...	Manual	Automatic	Synchronizing	

7. Restart **WebVM1** and **SQLVM1**. **Wait a full two minutes** for the VMs to start - **this is important**; we don't want to test simultaneous failover of SQLVM1 and SQLVM2 at this stage. Then stop **WebVM2** and **SQLVM2**.

8. Refresh the blade with the Contoso application. The application still works. Confirm again that the database is writable by changing one of the policies.

9. Re-open an Azure Bastion session with **SQLVM1** (with username `adadmin@contoso.ins` and password `Demo!pass123`). Open **SQL Server Management Studio** and connect to **SQLVM1** using Windows Authentication. Locate the BCDRAOG availability group, right-click and select **Show Dashboard**.

**Dashboard.** Note that the dashboard shows **SQLVM1** as the primary replica, and there is a critical warning about **SQLVM2** not being available.

BCDRAOG: hosted by SQLVM1 (Replica role: Primary)

Availability group state: **Critical --- Critical (1), Warnings (3)**

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	Not Synchronizing	<b>Critical ...</b>
SQLVM3	Second...	Asynchronous co...	Manual	Automatic	Synchronizing	

#### 10. Re-start **SQLVM2** and **WebVM2**.

#### Task 2: Validate Disaster Recovery - Failover IaaS region to region

In this task, you will validate the failover of the Contoso application from Central US to East US 2. The failover is orchestrated by Azure Site Recovery using the recovery plan you configured earlier. It includes the failover of both the web tier (creating new Web VMs from the replicated data) and the SQL Server tier (failure to the SQLVM3 asynchronous replica). The failover process is fully automated, with custom steps implemented using Azure Automation runbooks triggered by the Recovery Plan.

1. Using the Azure portal, open the **ContosoRG1** resource group. Navigate to the Front Door resource, locate Frontend Host URL, and open it in a new browser tab. Navigate to it to ensure that the application is up and running from the Primary Site.

Frontend host : <https://bcdriaas8675309.azurefd.net>

Keep this browser tab open; you will return to it later in the lab.

2. From a new browser tab, open the Azure portal, then navigate to the **BCDRRSV** Recovery Services Vault located in the **ContosoRG2** resource group.
3. Select **Recovery Plans (Site Recovery)** in the **Manage** area, then select **BCDRIaaSPlan**.

# BCDRRSV | Recovery Plans (Site Recovery)

Recovery Services vault

Search (Cmd+/)

Protected items

- Backup items
- Replicated items

Manage

- Backup policies
- Backup Infrastructure
- Site Recovery infrastructure
- Recovery Plans (Site Recovery) **Recovery Plans (Site Recovery)**
- Backup Reports

+ Recovery plan

Filter items...

Name	Source
BCDRlaaSPlan	East US 2

#### 4. Select **Failover**.

bcdriaasplan ...

BCD RSSV

Search (Cmd+/)

Customize Test failover Cleanup test failover Failover Re-protect Commit Delete

Overview

General

Items in recovery plan

Recovery Services vault bcdrrsv Start groups 1 Source East US 2 Deployment model Resource Manager

Items in recovery plan  
2 Scripts 2 Target West US 2

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

## Failover

BCDRlaaSPlan

**!** No Test Failover done in past 180 days! It is recommended to do a Test Failover before a failover.

I understand the risk. Skip test failover.

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

## Failover

X

BCDRlaaSPlan

### Failover direction

From ⓘ

East US 2

To ⓘ

West US 2

2 of 2 virtual machines will be failed over.

**Change direction**

### Recovery Point

Choose a recovery point ⓘ

Latest processed (low RTO)

▼

### Shut down machines

Shut down machines before beginning failover

**OK**

- After the Failover is initiated, close the Failover blade and navigate to **Site Recovery Jobs**. Select the **Failover** job to monitor the progress.

**BCD RSSV | Site Recovery jobs**

Recovery Services vault

Search (Cmd+ /) Filter Export jobs

Filter items...

Name	Status	Type
Failover	In progress	Recovery plan
Save a recovery plan	Successful	Recovery plan
Finalize protection on the recovery ...	Successful	Protected item
Finalize protection on the primary v...	Successful	Protected item

Alerts Metrics Diagnostic settings Logs Backup Jobs Site Recovery jobs Backup Alerts

- You can monitor the progress of the Failover from this panel.

**Failover** ...  
Site Recovery Job

Export job Cancel Environment Details

Properties

Vault	bcdrrsv
Recovery plan	BCDRlaaSPlan
Job id	781dd22f-ec40-4602-bac1-2b0b3be8c20e-2022-05-11T01:34:08Z-lbz ActivityId: dff9052f-4

Job

Name	Status
Prerequisites check for the recovery plan	Successful
> All groups shutdown (1)	Successful
> All groups failover: Pre-steps (1)	In progress
> Recovery plan failover	
> Group 1: Start (2)	
> Group 1: Post-steps (1)	
Finalizing the recovery plan	

**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 before 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.

**ASRSQFailover 6/29/2020, 10:15 PM**

Job

Resume Stop || Suspend Refresh

Id : c4de535a-c6a0-4ce2-ac08-a97016b577db	Created : 6/29/2020, 10:15:31 PM
Status : Completed	Last Update : 6/29/2020, 10:17:33 PM
Ran ... : Azure	Runbook : ASRSQFailover
Ran ... : User	Source snaps... : <a href="#">View source snapshot</a>

Input Output Errors Warnings All Logs Exception

Errors	Warnings
0 !	0 !

- Once the Failover job has finished, it should show as *Successful* for all tasks. The failover job may take more than 15 minutes.

**Failover**

Site Recovery Job

Export job Environment Details

Properties

Vault	bcdrrs
Recovery plan	BCDRlaaSPlan
Job id	3b6cae8f-08d9-4bd4-b7f3-331dfa78731e-2020-06-29T22:19:00Z-lbz ActivityId: 58e2d1f7-...

Job

Name	Status	Start time	Duration
Prerequisites check for the recovery plan	Successful	6/29/2020, 11:19:04 ...	00:00:08
> All groups shutdown (1)	Successful	6/29/2020, 11:19:13 ...	00:01:02
> All groups failover: Pre-steps (1)	Successful	6/29/2020, 11:20:15 ...	00:04:03
> Recovery plan failover	Successful	6/29/2020, 11:24:19 ...	00:01:43
> Group 1: Start (2)	Successful	6/29/2020, 11:26:02 ...	00:00:34
> Group 1: Post-steps (1)	Successful	6/29/2020, 11:26:37 ...	00:03:03
Finalizing the recovery plan	Successful	6/29/2020, 11:29:41 ...	00:00:00

10. Select **Resource groups** and select **ContosoRG1**. Open **WebVM1** and notice that it currently shows as **Status: Stopped (deallocated)**. This shows that failover automation has stopped the VMs at the **Primary** site.

**WebVM1**

Virtual machine

Search (Ctrl+ /) Connect Start Restart Stop Capture Delete

Overview	Resource group (change) : ContosoRG1
Activity log	Status : Stopped (deallocated)
Access control (IAM)	Location : Central US (Zone 1)
Tags	Subscription (change) :

**Note:** Do not select Start! The VM will be restarted automatically by ASR during failback.

11. Move back to the Resource group and select the **ContosoWebLBPrimaryIP** Public IP address. Copy the DNS name and paste it into a new browser tab. The website will be unreachable at the Primary location since the Web VMs at this location have been stopped by ASR during failover.
12. In the Azure portal, move to the **ContosoRG2** resource group. Locate the **WebVM1** in the resource group and select to open. Notice that **WebVM1** is running on the **Secondary** site.

13. Move back to the **ContosoRG2** resource group and select the **ContosoWebLBSecondaryIP** Public IP address. Copy the DNS name and paste it into a new browser tab. The Contoso application is now responding from the **Secondary** site. Make sure to select the current Policy Offerings to ensure connectivity to the SQL Always-On group that was also failed over in the background.
14. Return to the browser tab pointing to the Contoso application at the Front Door URL. Refresh the page. The site loads immediately from the DR site. Web site users accessing the service via Front Door are automatically routed to the currently available site, so 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, their experience will be no different from when it is running in the **Primary** site.

**Optional task:** You can log in to **SQLVM3** and open the SQL Management Studio to review the Failed over **BCDRAOG**. You will see that **SQLVM3**, which is running in the **Secondary** site, is now the Primary Replica.

15. Now that you have successfully tested failover, you need to configure ASR for fallback. Move back to the **BCDRSRV** Recovery Service Vault using the Azure portal. Select **Recovery Plans** on the ASR dashboard. The **BCDRIaaSPlan** will show as **Failover completed**.

16. Select the BCDRlaaSPlan plan. Notice that two (2) VMs are now shown in the **Target** tile.

17. Select **Re-protect**.

18. On the **Re-protect** screen, review the configuration and select **OK**.

## Re-protect

X

BCDRlaaSPlan

Resource group, Network, Storage and Availability  [Customize](#)

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

### Target resource group

ContosoRG1

### Cache storage accounts

aq51mtbcdrrsasrcache

### Target virtual network

VNet1

### Replica managed disks

(new) 2 premium disk(s), 0 standard disk(s)

### Target availability zones

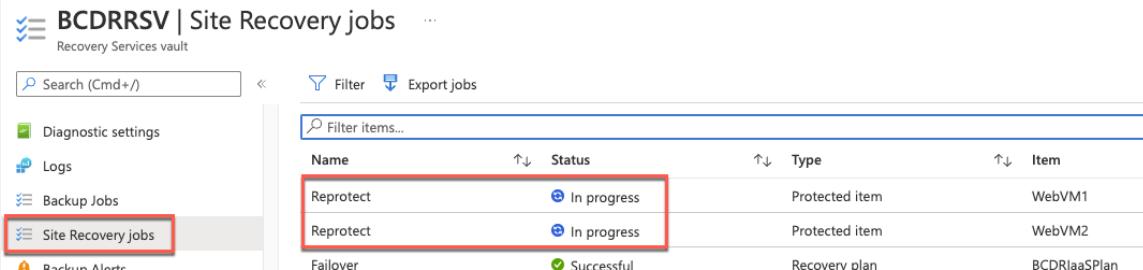
1

2

**OK**

19. The portal will submit a deployment. This process will take up to 30 minutes to commit the failover and then synchronize WebVM1 and WebVM2 with the Recovery Services Vault. Once this process is complete, you will be able to failback to the primary site.

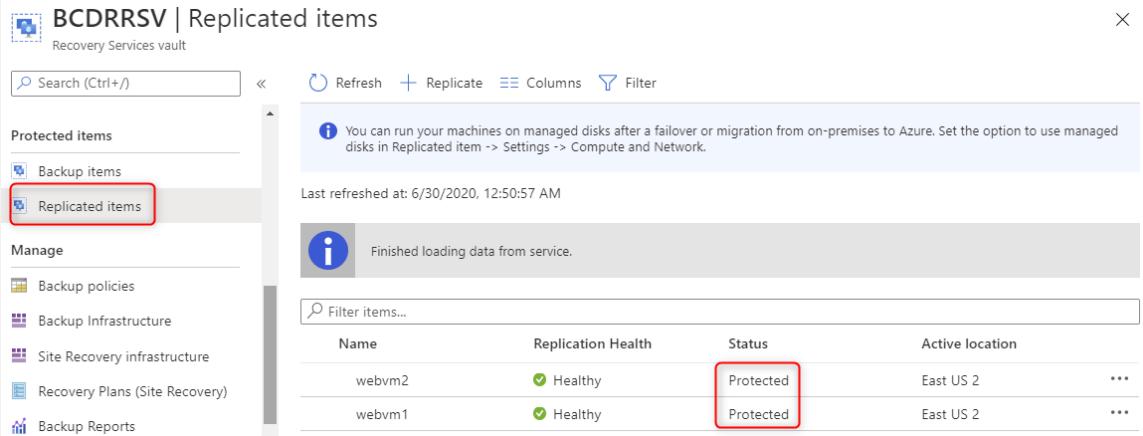
**Note:** You need to wait for the re-protect process to complete before continuing with the failback. You can check the status of the Re-protect using the Site Recovery Jobs area of the BCDRSRV.



The screenshot shows the 'Site Recovery jobs' blade under the 'BCDRRSV | Site Recovery jobs' section. On the left, there's a navigation menu with 'Site Recovery jobs' highlighted. The main area displays a table with the following data:

Name	Status	Type	Item
Reprotect	In progress	Protected item	WebVM1
Reprotect	In progress	Protected item	WebVM2
Failover	Successful	Recovery plan	BCDRlaaSPlan

Once the jobs are completed, move to the **Replicated items** blade and wait for the **Status** to show as **Protected**. This status shows the data synchronization is complete, and the Web VMs are ready to failback.



The screenshot shows the 'Replicated items' blade under the 'BCDRRSV | Replicated items' section. On the left, there's a navigation menu with 'Replicated items' highlighted. The main area displays a table with the following data:

Name	Replication Health	Status	Active location
webvm2	Healthy	Protected	East US 2
webvm1	Healthy	Protected	East US 2

## Task 3: Validate Disaster Recovery - Failback IaaS region to region

In this task, you will failback the Contoso application from the DR site in your secondary region back to the primary site (your primary region).

1. Still in the **BCDRRSV** Recovery Services vault, select **Recovery Plans** and re-open the **BCDRIaaSPlan**. Notice that the VMs are still at the Target since they failed over to the secondary site.
2. Select **Failover**. At the warning about No Test Failover, select **I understand the risk, Skip test failover**. Notice that **From** is the **Secondary** site and **To** is the **Primary** site. Select **OK**.

## Failover

BCDRIaaSPlan

Failover direction

From ⓘ	East US 2
To ⓘ	Central US

2 of 2 virtual machines will be failed over.

**Change direction**

Recovery Point

Choose a recovery point ⓘ

Latest processed (low RTO) ▾

Shut down machines

Shut down machines before beginning failover

**OK**

3. After the Failover is initiated, close the blade and select **Site Recovery Jobs**, then select the **Failover** job to monitor the progress. Once the job has finished, it should show as successful for all tasks.

**Failover** ...

Site Recovery Job

Export job Environment Details

**Properties**

Vault	bcdrrsv
Recovery plan	BCDRIaaSPlan
Job id	a1c0c195-bbbd-4343-a4d0-ee1683aae2a1-2022-05-11T02:43:14Z-lbz ActivityId: a409bd28-9356-4918-be2b-2... <a href="#">Copy</a>

**Job**

Name	Status	Start time	Duration
Prerequisites check for the recovery plan	Successful	5/10/2022, 10:43:16 PM	00:00:04
> All groups shutdown (1)	Successful	5/10/2022, 10:43:20 PM	00:00:31
> All groups failover: Pre-steps (1)	Successful	5/10/2022, 10:43:52 PM	00:02:12
> Recovery plan failover	Successful	5/10/2022, 10:46:04 PM	00:01:46
> Group 1: Start (2)	Successful	5/10/2022, 10:47:51 PM	00:00:39
> Group 1: Post-steps (1)	Successful	5/10/2022, 10:48:30 PM	00:01:11
Finalizing the recovery plan	Successful	5/10/2022, 10:49:41 PM	00:00:00

4. Confirm that the Contoso application is once again accessible via the **ContosoWebLBPrimaryIP** public IP address and is **not** available at the **ContosoWebLBSecondaryIP** address. This test shows it has returned to the primary site. Open the **Current Policy Offerings** and edit a policy to confirm database access.

**Note:** If you get an "Our services aren't available right now" error (or a 404-type error) accessing the web application, verify that you are utilizing the **ContosoWebLBPrimaryIP**. If it does not come up within ~10 minutes, verify that the backend system is responding.

5. Confirm that the Contoso application is also available via the Front Door URL.
6. 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 and open the **BCDRIaaSPlan**.
7. Notice that now 2 VMs are shown in the **Source**. Select **Re-protect**, review the configuration, and select **OK**.

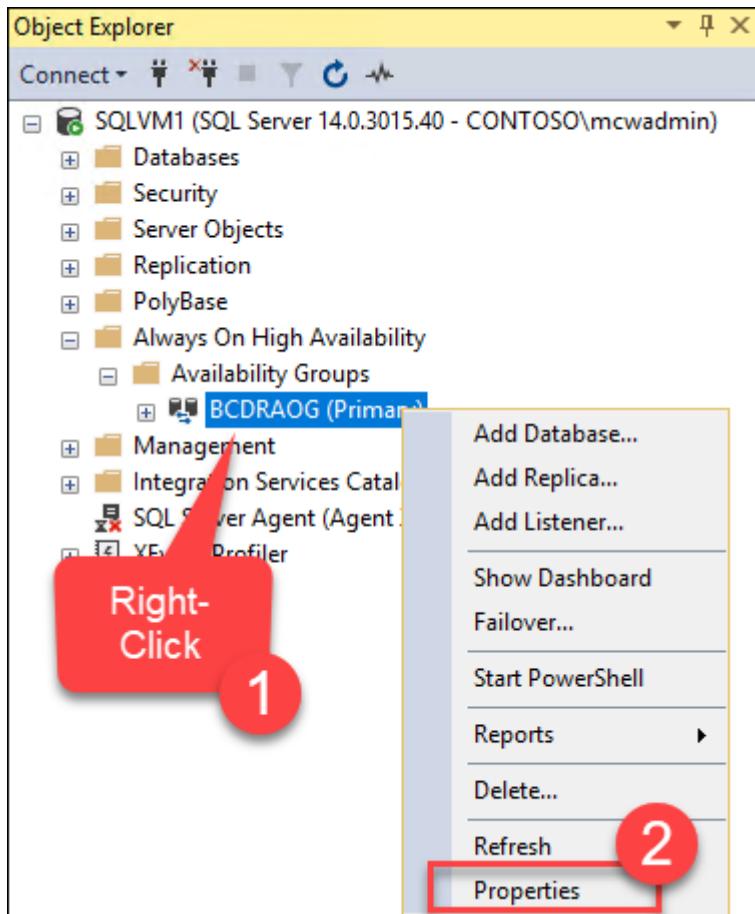
The screenshot shows the Azure Recovery Services vault interface for 'bcdriaasplan'. The top navigation bar includes 'Customize', 'Test failover', 'Cleanup test failover', 'Failover', 'Re-protect' (which is highlighted with a red box), 'Commit', and 'Delete'. Below the navigation is a 'General' section with 'Overview' selected. It displays details about the vault: 'bcdrssv' as the Recovery Services vault, '1' Start groups, 'Source East US 2', 'Deployment model Resource Manager', and 'Items in recovery plan' with '2' Source and '0' Target. A large box highlights the 'Items in recovery plan' section, specifically the 'Source' count of '2'.

8. As previously, the portal will submit a deployment. This process will take some time. You can proceed with the lab without waiting.
9. Next, you need to reset the SQL Always On Availability Group environment to ensure a proper failover. Use Azure Bastion to connect to **SQLVM1** with username `adadmin@contoso.ins` and password `Demo!pass123`.
10. Once connected to **SQLVM1**, open SQL Server Management Studio and Connect to **SQLVM1**. Expand the **Always On Availability Groups** and then right-click on **BCDRAOG** and select **Show Dashboard**.
11. 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**.

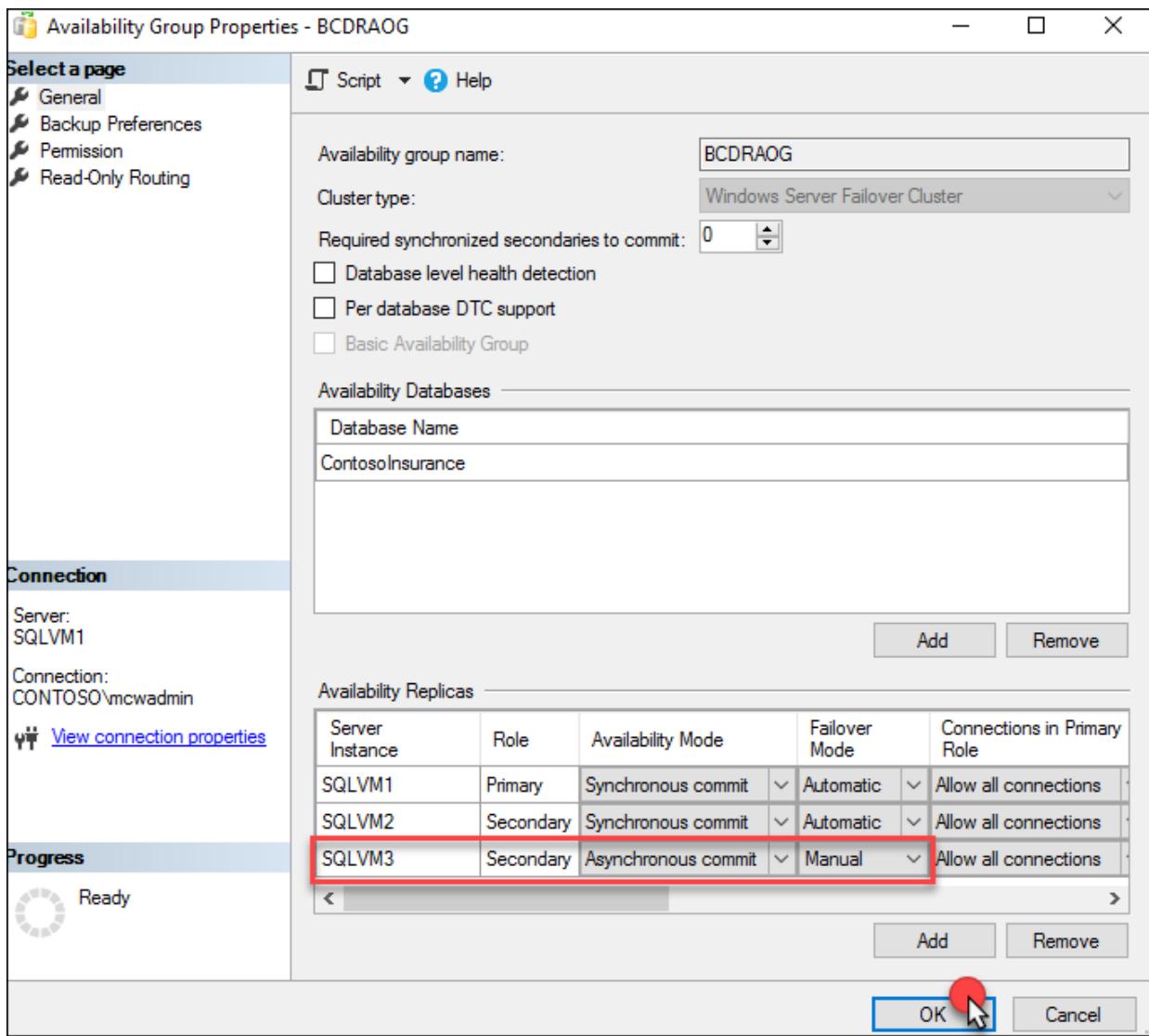
The screenshot shows the 'BCDRAOG:SQLVM1' dashboard in SQL Server Management Studio. At the top, it says 'BCDRAOG: hosted by SQLVM1 (Replica role: Primary)'. Below that, the 'Availability group state' is listed as 'Healthy'. The primary instance is 'SQLVM1' and the failover mode is 'Automatic'. The cluster state is 'AOGLCLUSTER (Normal Quorum)' and the cluster type is 'Windows Server Failover Cluster'. Under 'Availability replica:', there is a table with the following data:

Name	Role	Availability Mode	Failover Mode	Seeding Mode	Synchronization State
<a href="#">SQLVM1</a>	Primary	Synchronous commit	Automatic	Automatic	Synchronized
<a href="#">SQLVM2</a>	Secondary	Synchronous commit	Automatic	Automatic	Synchronized
<a href="#">SQLVM3</a>	Secondary	Synchronous commit	Automatic	Automatic	Synchronized

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



13. Change **SQLVM3** to **Asynchronous** and **Manual Failover** and select **OK**.



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

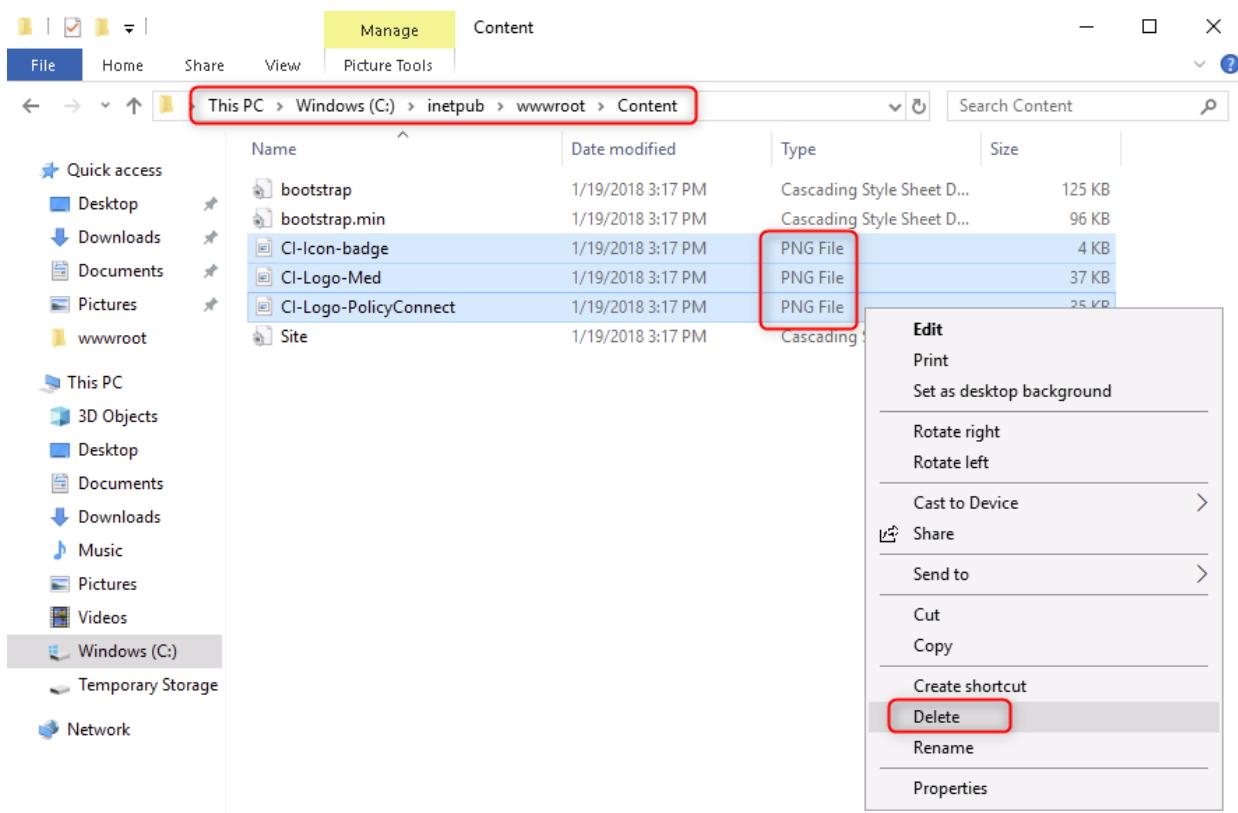
Name	Role	Availability Mode	Failover Mode	Seeding Mode	Synchronization State
SQLVM1	Primary	Synchronous commit	Automatic	Automatic	Synchronized
SQLVM2	Secondary	Synchronous commit	Automatic	Automatic	Synchronized
SQLVM3	Secondary	Asynchronous commit	Manual	Automatic	Synchronizing

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

## Task 4: Validate VM Backup

In this task, you will validate the backup for the Contoso application WebVMs. You will do this by removing several image files from **WebVM1**, breaking the Contoso application. You will then restore the VM from backup.

1. From the Azure portal, locate and shut down **WebVM2**. This forces all traffic to be served by **WebVM1**, making the backup/restore verification easier.
2. Navigate to **WebVM1** and connect to the VM using Azure Bastion, using username `adadmin@contoso.ins` and password `Demo!pass123`.
3. Open Windows Explorer and navigate to the `C:\inetpub\wwwroot\Content` folder. Select the three `.PNG` files and delete them.



4. In the Azure portal, locate the **ContosoWebLBPrimaryIP** public IP address in **ContosoRG1**. Copy the DNS name and open it in a new browser tab. Hold down **CTRL** and refresh the browser to reload the page without using your local browser cache. The Contoso application should be shown with images missing.



Welcome to the Policy Management System

[Current Policy Offerings »](#)

## Manage Customers

Our goal is to have customers for life. Things change, so keep their information updated.

[Go Now »](#)

## Manage Policy Holders

Details Matter, so make sure to capture them all!

[Go Now »](#)

© 2020 - Contoso Insurance

5. To restore WebVM1 from backup, Azure Backup requires that a 'staging' storage account be available. To create this account, in the Azure portal, select + **Create a resource**, then search for and select **Storage account**. Select **Create**.
6. Complete the 'Create storage account' form as follows, then select **Review + Create** followed by **Create**.
  - **Resource group:** ContosoRG1
  - **Storage account name:** Unique name starting with **backupstaging**.
  - **Location:** *your primary region*
  - **Performance:** Standard
  - **Replication:** Locally-redundant storage (LRS)

## Create a storage account ...

Basics   Advanced   Networking   Data protection   Encryption   Tags   Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

### Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \*

Resource group \*

 ContosoRG1 [Create new](#)

### Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ \*

 backupstaging09  

Region ⓘ \*

 (US) East US 2  

Performance ⓘ \*

Standard: Recommended for most scenarios (general-purpose v2 account)

Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ \*

 Locally-redundant storage (LRS)

**Review + create**

< Previous

Next : Advanced >

7. Before restoring a VM, the existing VM must be shut down. Use the Azure portal to shut down **WebVM1**.

**Note:** since WebVM2 is also shut down, this will break the Contoso application. In a real-world scenario, you would keep WebVM2 running while restoring WebVM1.

8. In the Azure portal, navigate to the **BackupRSV** Recovery Services Vault. Under 'Protected Items', select **Backup items**, then select **Azure Virtual Machine**.

 **BackupRSV | Backup items**

Recovery Services vault

Search (Ctrl+ /) Refresh

Getting started

- Backup
- Site Recovery

Protected items

- Backup items** (highlighted)
- Replicated items

Manage

- Backup policies
- Backup Infrastructure

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	2
SQL in Azure VM	1
SAP HANA in Azure VM	0
Azure Storage (Azure Files)	0
DPM	0
Azure Backup Server	0
Azure Backup Agent	0

9. On the Backup items page, select **View details** for **WebVM1**. On the **WebVM1** page, select **RestoreVM**.

 **WebVM1**  
Backup Item

Backup now **Restore VM** (highlighted) File Recovery Stop backup Resume backup Delete

Alerts and Jobs	Backup status
<a href="#">View all Alerts (last 24 hours)</a>	Backup Pre-Check  Passed
<a href="#">View all Jobs (last 24 hours)</a>	Last backup status  Success 6/30/2020, 10:08:11 AM

10. Complete the Restore Virtual Machine page as follows, then select **Restore**.

- **Restore point:** Select the most recent restore point.
- **Restore Configuration:** Replace existing
- **Staging Location:** Choose the storage account you created earlier, starting with **backupstaging**.

## Restore Virtual Machine

webvm1

Restore allows you to restore VM/disks from a selected Restore Point.

Restore point \*

5/10/2022, 5:16:39 PM

Select

Data Store

Snapshot and Vault-Standard

### Restore Configuration

Create new

Replace existing

*The disk(s) from the selected restore point will replace the disk(s) in your existing VM. [Learn more about In-Place Restore.](#)*

Restore Type ⓘ

Replace Disk(s)

Staging Location \* ⓘ

backupstaging09 (StandardLRS)



[Can't find your storage account?](#)

*The identities listed here are based on the MSI configurations in the corresponding Recovery services vault. [Learn more.](#)*

Identities ⓘ

Disabled

**Restore**

11. In the **BackupRSV** vault, navigate to the **Backup Jobs** view. Note that two new jobs are shown as 'In progress', one to take a backup of the VM and a second to restore the VM.

## BackupRSV | Backup Jobs

Recovery Services vault

- Search (Cmd+ /)
- Backup Infrastructure
- Site Recovery infrastructure
- Recovery Plans (Site Recovery)
- Backup Reports

### Monitoring

- Alerts
- Metrics
- Diagnostic settings
- Logs
- Backup Jobs**
- Site Recovery jobs
- Backup Alerts

Filtered by: Item Type - All, Operation - All, Status - All, Start Time - 5/9/2022, 11:17:05 PM, End Time - 5/10/2022, 11:17:05 PM

*For backups, try our new Backup Center. It offers Azure Backup customers a unified view of Recovery Services Vaults used for back get the new experience.*

All data fetched from the service.

[Filter items ...](#)

Workload name ↑↓	Operation	Status	Type
webvm1	Backup	<i>In progress</i>	Azure Virtual machine
webvm1	Restore	<i>In progress</i>	Azure Virtual machine
ContosoInsurance [BCDRAOG....]	Backup (Full)	<i>Completed</i>	Azure Workload

12. It will take several minutes for the VM to be restored. Wait for the restore to complete before proceeding with the lab.

13. Once the restore operation is complete, navigate to the **WebVM1** blade in the Azure portal and **Start** the VM.

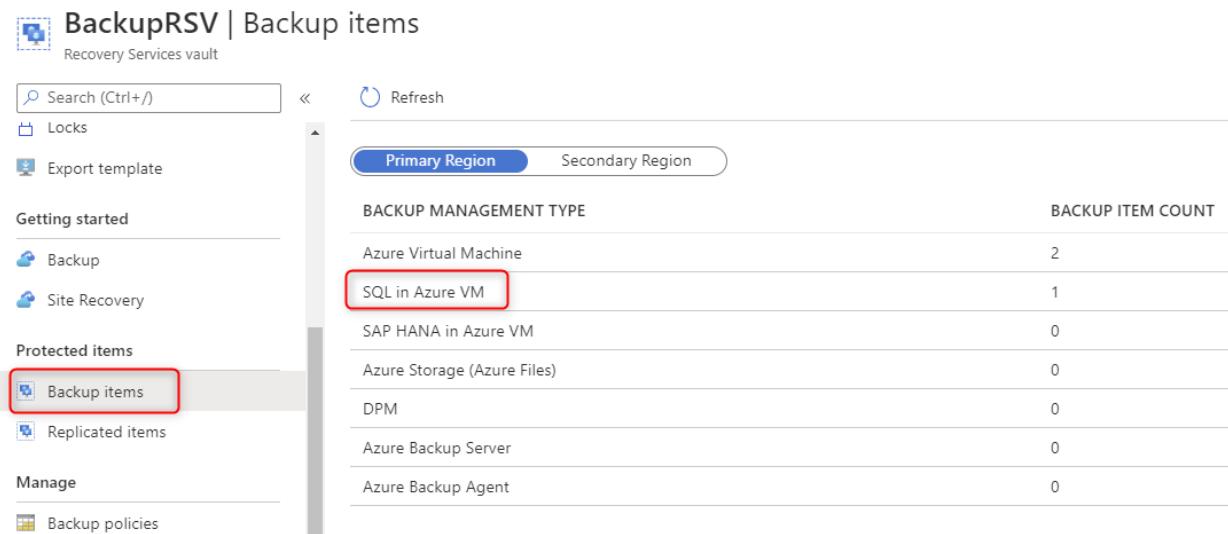
14. Wait for the VM to start, then return to your browser tab showing the Contoso application with missing images. Hold down **CTRL** and select **Refresh** to reload the page. The application is displayed with the images restored, showing the restore from backup has been successful. (As an optional step, you can also open a Bastion connection to the VM and check the deleted .PNG files have been restored.)

15. Start **WebVM2**.

## Task 5: Validate SQL Backup

In this task, you will validate the ability to restore the Contoso application database from Azure Backup.

1. In the Azure portal, navigate to the **BackupRSV** in **ContosoRG1**. Under 'Protected items', select **Backup items**, then select **SQL in Azure VM**.

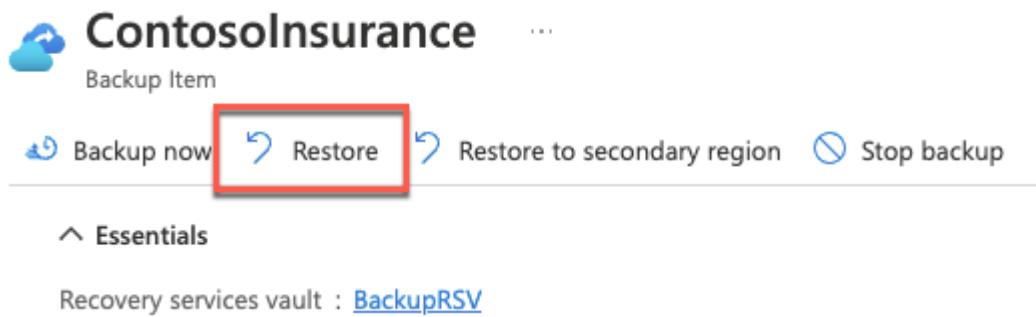


The screenshot shows the 'BackupRSV | Backup items' page. On the left, there's a sidebar with 'Getting started' (Backup, Site Recovery), 'Protected items' (Backup items, Replicated items), 'Manage' (Backup policies), and 'Recovery Services vault'. The 'Protected items' section is expanded, and 'Backup items' is highlighted with a red box. The main area shows a table of backup management types and their counts:

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	2
<b>SQL in Azure VM</b>	1
SAP HANA in Azure VM	0
Azure Storage (Azure Files)	0
DPM	0
Azure Backup Server	0
Azure Backup Agent	0

2. From the backup items list, select **View details** for the **contosoinsurance** database.

3. From the **contosoinsurance** blade, select **Restore**.



The screenshot shows the 'ContosoInsurance' blade. At the top, there's a cloud icon and the text 'Backup Item'. Below that are buttons for 'Backup now', 'Restore' (highlighted with a red box), 'Restore to secondary region', and 'Stop backup'. Underneath these buttons is a section titled '^ Essentials'. At the bottom, it says 'Recovery services vault : [BackupRSV](#)'.

4. Review the default settings on the **Restore** blade. By default, the backup will be restored to a new database alongside the existing database on SQLVM1.

# Restore

## Where and how to Restore?

Alternate Location

Overwrite DB

Restore as files



If you don't see your SQL Server in the below list go to 'Getting Started' > 'Backup' > 'Start Discovery'

Server ([Can't find Server?](#)) \*

sqlvm1.contoso.com



SQLVM1

Instance \*

MSSQLSERVER



Restored DB Name \*

contosoinsurance\_restored\_7\_1\_2020\_1642



Overwrite if the DB with same name already exists on selected SQL instance

Restore Point

No Restore Point Selected

Select

**Note:** For an Always On Availability Group backup, the option to overwrite the existing database is not available. You must restore to a parallel location.

5. Select the option to choose your Restore Point. On the 'Select restore point' blade, explore the restore options. Note how the log-based option offers a point-in-time restore, whereas the full & differential option provides backup based on the backup schedule.

Choose any restore point and select **OK**.

# Select restore point

X

Logs (Point in Time)

Full & Differential

Restores corresponding full, differential and log backups with minimal RTO



Log based restore is available from 6/30/2020, 19:33:19 . To restore from older or Full & Differential backup, click on Full & Differential above.

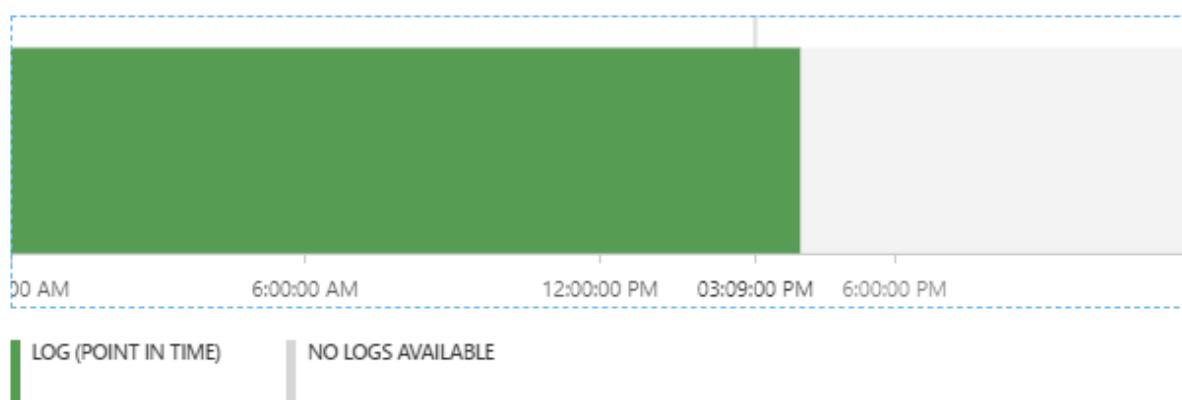
Restore Date/Time

07/01/2020



1:45:04 PM

Local Time (UTC+0100)



## Select restore point

X

Start Time

06/01/2020



4:45:59 PM

End Time

07/01/2020



4:45:59 PM

Refresh

Logs (Point in Time)

Full & Differential

Filtered for last 30 days

Time	Type
6/30/2020, 7:33:19 PM	Full Backup
6/30/2020, 7:05:32 PM	Full Backup

6. Under 'Advanced Configuration', select **Configure**. Review the settings but don't change anything.  
Select **OK** to accept the default configuration
7. Select **OK** to start the restore process.
8. Navigate to the **Backup Jobs** view. The ContosoInsurance job is 'In progress'. Use the **Refresh** button to monitor the progress and wait for the job to complete.

BackupRSV | Backup Jobs

Recovery Services vault

Search (Cmd+ /) Choose columns Filter Export jobs Refresh Feedback View jobs in secondary region

Filtered by: Item Type - All, Operation - All, Status - All, Start Time - 5/9/2022, 11:50:41 PM, End Time - 5/10/2022, 11:50:41 PM

For backups, try our new Backup Center. It offers Azure Backup customers a unified view of Recovery Services Vaults used for backups. Get the new experience.

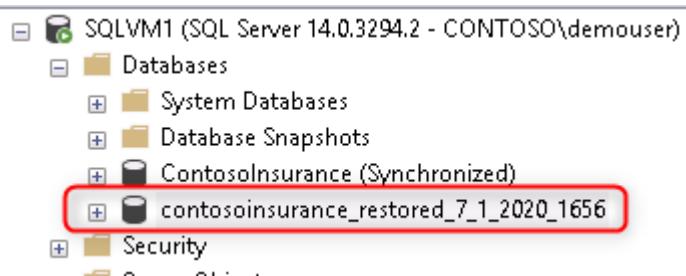
All data fetched from the service.

Filter items ...

Workload name	Operation	Status	Type
ContosoInsurance [BCDRAOG....]	Restore	In progress	Azure Workload

9. Navigate to **SQLVM1** and connect to the VM using Azure Bastion, using username **adadmin@contoso.ins** and password **Demo!pass123**.
10. On SQLVM1, open **SQL Server Management Studio** and connect to SQLVM1.

11. Note that the restored database is present alongside the production database on the server.



**Note:** You can now either copy data from the restored database to the production database or add this database to the Always On Availability Group and switch the Web tier to use the restored database.

## After the hands-on lab

### Task 1: Delete the lab resources

1. Within the Azure portal, select Resource Groups on the left navigation.
2. To delete the Recovery Services Vaults, you will first need to open the vaults, disable all VM backup and replication and delete any backup and replicated data.
3. Delete each of the resource groups created in this lab by selecting them, followed by the **Delete resource group** button. You will need to confirm the name of the resource group to delete.

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