****

**SQL server Always On Reporting Feature**

Date: 25 Aug 2021

Author: Raunak Sharma

For further information please contact:

[R.sharma@projectobjects.com](mailto:R.sharma@projectobjects.com)  
[www.projectobjects.com](http://www.projectobjects.com)

© 2021 Project Objects Ltd

© 2021 Project Objects Ltd

© 2021 Project Objects Ltd

© 2021 Project Objects Ltd

Contents

[SQL Server Always On Reporting Feature 1](file:///C:/Users/POI/Desktop/Document%20For%20SQL%20Always%20On%20Group.docx#_Toc80779464)

[Prerequisites for creating availability groups on SQL Server on Azure Virtual Machines 3](#_Toc80779465)

1. [Create a resource group 4](#_Toc80779466)

[1.1 Create the network and subnet 4](#_Toc80779467)

[1.2 Create availability sets 5](#_Toc80779468)

[2. Create domain controllers 6](#_Toc80779469)

[**2.1 Configure the domain controller** 7](#_Toc80779470)

[**Note the IP address of the primary domain controller** 8](#_Toc80779471)

[**2.1.1 Configure the virtual network DNS** 8](#_Toc80779472)

[**2.2 Configure the second domain controller** 9](#_Toc80779473)

[**2.2.1 Add the private IP address to the second domain controller to the VPN DNS Server** 10](#_Toc80779474)

[**2.2.3** **Grant the required permissions to the installation account** 11](#_Toc80779475)

[3 Create SQL Server VMs 11](#_Toc80779476)

[**3.1 Create and configure the SQL Server VMs** 12](#_Toc80779477)

[**3.1.1 Join the servers to the domain** 13](#_Toc80779478)

[3.1.2 Add accounts 13](#_Toc80779479)

[**3.1.3 Add the Corp\Install user as an administrator on each cluster VM** 13](#_Toc80779480)

[**3.1.4 Create a sign-in on each SQL Server VM for the installation account** 14](#_Toc80779481)

[**3.1.5 Set the SQL Server service accounts** 15](#_Toc80779482)

[3.1.6 Add Failover Clustering features to both SQL Server VMs 15](#_Toc80779483)

[**3.1.7 Open a TCP port in the firewall** 15](#_Toc80779484)

[3.1.8 Create the cluster 16](#_Toc80779485)

[**Set the Windows server failover cluster IP address** 16](#_Toc80779486)

[**3.1.9 Add the other SQL Server to cluster** 17](#_Toc80779487)

[**3.1.10 Add a cluster quorum file share** 17](#_Toc80779488)

[**3.1.11 Configure the cluster quorum** 18](#_Toc80779489)

[3.1.12 Enable availability groups 18](#_Toc80779490)

[Create a backup share 19](#_Toc80779491)

[Take a full and Transactional backup of the database 19](#_Toc80779492)

[**3.1.13 Create the availability group:** 19](#_Toc80779493)

[4.Create an Azure load balancer 20](#_Toc80779494)

[**4.1 Add a backend pool for the availability group listener** 20](#_Toc80779495)

[**Set the probe** 21](#_Toc80779496)

[**4.2 Set the load balancing rules** 21](#_Toc80779497)

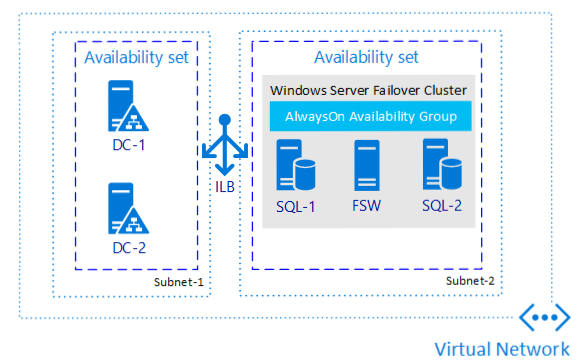
[**4.3 Add the cluster core IP address for the Windows Server Failover Cluster (WSFC)** 22](#_Toc80779498)

[4.4 Configure the listener 24](#_Toc80779499)

[4.5 In SQL Server Set listener port 26](#_Toc80779500)

**Prerequisites for creating availability groups on SQL Server on Azure Virtual Machines**

The following diagram illustrates what you build in the tutorial.



## **1.Create a resource group**

1. Sign into the azure Portal
2. Select **+** to create a new object in the portal.
3. Type **resource group** in the **Marketplace** search window.
4. Select **Resource group**.
5. Select **Create**.
6. Under **Resource group name**, type a name for the resource group. For example, type **sql-ha-rg**.
7. If you have multiple Azure subscriptions, verify that the subscription is the Azure subscription that you want to create the availability group in.
8. Select a location. The location is the Azure region where you want to create the availability group. This article builds all resources in one Azure location.
9. Verify that **Pin to dashboard** is checked. This optional setting places a shortcut for the resource group on the Azure portal dashboard.
10. Select **Create** to create the resource group.

## **1.1 Create the network and subnet**

The next step is to create the networks and subnet in the Azure resource group.

The solution uses one virtual network and one subnet. The [Virtual network overview](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview) provides more information about networks in Azure.

To create the virtual network in the Azure portal:

1. In your resource group, select **+ Add**.
2. Search for **virtual network**.
3. Select **Virtual network**.
4. On the **Virtual network**, select the **Resource Manager** deployment model, and then select **Create**.

The following table shows the settings for the virtual network:

|  | |
| --- | --- |
| **Field** | **Value** |
| **Name** | autoHAVNET |
| **Address space** | 10.0.0.0/16 |
| **Subnet name** | Admin |
| **Subnet address range** | 10.0.0.0/24, 10.0.1.0/24 |
| **Subscription** | Specify the subscription that you intend to use. **Subscription** is blank if you only have one subscription. |
| **Resource group** | Choose **Use existing** and pick the name of the resource group. |
| **Location** | Specify the Azure location. |

Your address space and subnet address range might be different from the table. Depending on your subscription, the portal suggests an available address space and corresponding subnet address range. If no sufficient address space is available, use a different subscription.

The example uses the subnet name **Admin**. This subnet is for the domain controllers and SQL-subnet for SQL Server VMs.

1. Select **Create**.

## **1.2 Create availability sets**

You need two availability sets. One is for the domain controllers. The second is for the SQL Server VMs.

To create an availability set, go to the resource group and select **Add**. Filter the results by typing **availability set**. Select **Availability Set** in the results, and then select **Create**.

Configure two availability sets according to the parameters in the following table:

| **CREATE AVAILABILITY SETS** | | |
| --- | --- | --- |
| **Field** | **Domain controller availability set** | **SQL Server availability set** |
| **Name** | Domainavailabilityset | sqlavailabilityset |
| **Resource group** | SQL-HA-RG | SQL-HA-RG |
| **Fault domains** | 3 | 3 |
| **Update domains** | 5 | 3 |

## **2. Create domain controllers**

After you've created the network, subnet, and availability sets, you're ready to create the virtual machines for the domain controllers.

Create virtual machines for the domain controllers

To create and configure the domain controllers, return to the **SQL-HA-RG** resource group.

1. Select **Add**.
2. Type **Windows Server 2016 Datacenter**.
3. Select **Windows Server 2016 Datacenter**. In **Windows Server 2016 Datacenter**, verify that the deployment model is **Resource Manager**, and then select **Create**.

Repeat the preceding steps to create two virtual machines. Name the two virtual machines:

* ad-primary-dc
* ad-secondary-dc

The following table shows the settings for these two machines:

|  | |
| --- | --- |
| **Field** | **Value** |
| **Name** | First domain controller: *ad-primary-dc*. Second domain controller *ad-secondary-dc*. |
| **VM disk type** | SSD |
| **User name** | DomainAdmin |
| **Password** | Contoso!0000 |
| **Subscription** | *Your subscription* |
| **Resource group** | SQL-HA-RG |
| **Location** | *Your location* |
| **Size** | DS1\_V2 |
| **Storage** | **Use managed disks** - **Yes** |
| **Virtual network** | autoHAVNET |
| **Subnet** | admin |
| **Public IP address** | *Same name as the VM* |
| **Network security group** | *Same name as the VM* |
| **Availability set** | adavailabilityset **Fault domains**:2 **Update domains**:2 |
| **Diagnostics** | Enabled |
| **Diagnostics storage account** | *Automatically created* |

### **2.1 Configure the domain controller**

In the following steps, configure the **ad-primary-dc** machine as a domain controller for corp.contoso.com.

1. In the portal, open the **SQL-HA-RG** resource group and select the **ad-primary-dc** machine. On **ad-primary-dc**, select **Connect** to open an RDP file for remote desktop access.
2. Sign in with your configured administrator account (**\DomainAdmin**) and password (**Contoso!0000**).
3. By default, the **Server Manager** dashboard should be displayed.
4. Select the **Add roles and features** link on the dashboard.
5. Select **Next** until you get to the **Server Roles** section.
6. Select the **Active Directory Domain Services** and **DNS Server** roles. When you're prompted, add any additional features that are required by these roles.
7. Select **Next** until you reach the **Confirmation** section. Select the **Restart the destination server automatically if required** check box.
8. Select **Install**.
9. After the features finish installing, return to the **Server Manager** dashboard.
10. Select the new **AD DS** option on the left-hand pane.
11. Select the **More** link on the yellow warning bar.
12. In the **Action** column of the **All Server Task Details** dialog, select **Promote this server to a domain controller**.
13. In the **Active Directory Domain Services Configuration Wizard**, use the following values:

|  | |
| --- | --- |
| **Page** | **Setting** |
| **Deployment Configuration** | **Add a new forest** **Root domain name** = corp.contoso.com |
| **Domain Controller Options** | **DSRM Password** = Contoso!0000 **Confirm Password** = Contoso!0000 |

1. Select **Next** to go through the other pages in the wizard. On the **Prerequisites Check** page, verify that you see the following message: **All prerequisite checks passed successfully**. You can review any applicable warning messages, but it's possible to continue with the installation.
2. Select **Install**. The **ad-primary-dc** virtual machine automatically reboots.

### **Note the IP address of the primary domain controller**

Use the primary domain controller for DNS. Note the primary domain controller IP address.

One way to get the primary domain controller IP address is through the Azure portal.

1. On the Azure portal, open the resource group.
2. Select the primary domain controller.
3. On the primary domain controller, select **Network interfaces**.

### **2.1.1 Configure the virtual network DNS**

After you create the first domain controller and enable DNS on the first server, configure the virtual network to use this server for DNS.

1. In the Azure portal, select on the virtual network.
2. Under **Settings**, select **DNS Server**.
3. Select **Custom**, and type the private IP address of the primary domain controller.
4. Select **Save**

### **2.2 Configure the second domain controller**

After the primary domain controller reboots, you can configure the second domain controller. This optional step is for high availability. Follow these steps to configure the second domain controller:

1. In the portal, open the **SQL-HA-RG** resource group and select the **ad-secondary-dc** machine. On **ad-secondary-dc**, select **Connect** to open an RDP file for remote desktop access.
2. Sign in to the VM by using your configured administrator account (**BUILTIN\DomainAdmin**) and password (**Contoso!0000**).
3. Change the preferred DNS server address to the address of the domain controller.
4. In **Network and Sharing Center**, select the network interface.
5. Select **Properties**.
6. Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.
7. Select **Use the following DNS server addresses** and then specify the address of the primary domain controller in **Preferred DNS server**.
8. Select **OK**, and then **Close** to commit the changes. You are now able to join the VM to **corp.contoso.com**.
9. From the remote desktop to the secondary domain controller, open **Server Manager Dashboard**.
10. Select the **Add roles and features** link on the dashboard.
11. Select **Next** until you get to the **Server Roles** section.
12. Select the **Active Directory Domain Services** and **DNS Server** roles. When you're prompted, add any additional features that are required by these roles.
13. After the features finish installing, return to the **Server Manager** dashboard.
14. Select the new **AD DS** option on the left-hand pane.
15. Select the **More** link on the yellow warning bar.
16. In the **Action** column of the **All Server Task Details** dialog, select **Promote this server to a domain controller**.
17. Under **Deployment Configuration**, select **Add a domain controller to an existing domain**.
18. Click **Select**.
19. Connect by using the administrator account (**CORP.CONTOSO.COM\domainadmin**) and password (**Contoso!0000**).
20. In **Select a domain from the forest**, choose your domain and then select **OK**.
21. In **Domain Controller Options**, use the default values and set a DSRM password.
22. Select **Next** until the dialog reaches the **Prerequisites** check. Then select **Install**.

After the server finishes the configuration changes, restart the server.

### **2.2.1 Add the private IP address to the second domain controller to the VPN DNS Server**

In the Azure portal, under virtual network, change the DNS Server to include the IP address of the secondary domain controller. This setting allows the DNS service redundancy.

Configure the domain accounts

In the next steps, you configure the Active Directory accounts. The following table shows the accounts:

| **CONFIGURE THE DOMAIN ACCOUNTS** | | | |
| --- | --- | --- | --- |
|  | **Installation account** | **sqlserver-0 SQL Server and SQL Agent Service account** | **sqlserver-1 SQL Server and SQL Agent Service account** |
| **First Name** | Install | SQLSvc1 | SQLSvc2 |
| **User SamAccountName** | Install | SQLSvc1 | SQLSvc2 |

Use the following steps to create each account.

1. Sign in to the **ad-primary-dc** machine.
2. In **Server Manager**, select **Tools**, and then select **Active Directory Administrative Center**.
3. Select **corp (local)** from the left pane.
4. On the right **Tasks** pane, select **New**, and then select **User**.
5. Select **OK** to create the user.
6. Repeat the preceding steps for each of the three accounts.

### **Grant the required permissions to the installation account**

1. In the **Active Directory Administrative Center**, select **corp (local)** in the left pane. Then in the right-hand **Tasks** pane, select **Properties**.
2. Select **Extensions**, and then select the **Advanced** button on the **Security** tab.
3. In the **Advanced Security Settings for corp** dialog, select **Add**.
4. Click **Select a principal**, search for **CORP\Install**, and then select **OK**.
5. Select the **Read all properties** check box.
6. Select the **Create Computer objects** check box.
7. elect **OK**, and then select **OK** again. Close the **corp** properties window.

Now that you've finished configuring Active Directory and the user objects, create two SQL Server VMs and a witness server VM. Then join all three to the domain.

## **3 Create SQL Server VMs**

Create three additional virtual machines. The solution requires two virtual machines with SQL Server instances. A third virtual machine will function as a witness. Windows Server 2016 can use as cloud witness.

### **3.1 Create and configure the SQL Server VMs**

| **Page** | **VM1** | **VM2** | **VM3** |
| --- | --- | --- | --- |
| Select the appropriate gallery item | **Windows Server 2016 Datacenter** | **SQL Server 2016 SP1 Enterprise on Windows Server 2016** | **SQL Server 2016 SP1 Enterprise on Windows Server 2016** |
| Virtual machine configuration **Basics** | **Name** = cluster-fsw **User Name** = DomainAdmin **Password** = Contoso!0000 **Subscription** = Your subscription **Resource group** = SQL-HA-RG **Location** = Your Azure location | **Name** = sqlserver-0 **User Name** = DomainAdmin **Password** = Contoso!0000 **Subscription** = Your subscription **Resource group** = SQL-HA-RG **Location** = Your Azure location | **Name** = sqlserver-1 **User Name** = DomainAdmin **Password** = Contoso!0000 **Subscription** = Your subscription **Resource group** = SQL-HA-RG **Location** = Your Azure location |
| Virtual machine configuration **Size** | **SIZE** = DS1\_V2 (1 vCPU, 3.5 GB) | **SIZE** = DS2\_V2 (2 vCPUs, 7 GB) The size must support SSD storage (Premium disk support. )) | **SIZE** = DS2\_V2 (2 vCPUs, 7 GB) |
| Virtual machine configuration **Settings** | **Storage**: Use managed disks. **Virtual network** = autoHAVNET **Subnet** = sqlsubnet(10.1.1.0/24) **Public IP address** automatically generated. **Network security group** = None **Monitoring Diagnostics** = Enabled **Diagnostics storage account** = Use an automatically generated storage account **Availability set** = sqlAvailabilitySet | **Storage**: Use managed disks. **Virtual network** = autoHAVNET **Subnet** = sqlsubnet(10.1.1.0/24) **Public IP address** automatically generated. **Network security group** = None **Monitoring Diagnostics** = Enabled **Diagnostics storage account** = Use an automatically generated storage account **Availability set** = sqlAvailabilitySet | **Storage**: Use managed disks. **Virtual network** = autoHAVNET **Subnet** = sqlsubnet(10.1.1.0/24) **Public IP address** automatically generated. **Network security group** = None **Monitoring Diagnostics** = Enabled **Diagnostics storage account** = Use an automatically generated storage account **Availability set** = sqlAvailabilitySet |
| Virtual machine configuration **SQL Server settings** | Not applicable | **SQL connectivity** = Private (within Virtual Network) **Port** = 1433 **SQL Authentication** = Disable **Storage configuration** = General **Automated patching** = Sunday at 2:00 **Automated backup** = Disabled **Azure Key Vault integration** = Disabled | **SQL connectivity** = Private (within Virtual Network) **Port** = 1433 **SQL Authentication** = Disable **Storage configuration** = General **Automated patching** = Sunday at 2:00 **Automated backup** = Disabled **Azure Key Vault integration** = Disabled |

After the three VMs are fully provisioned, you need to join them to the **corp.contoso.com** domain and grant CORP\Install administrative rights to the machines.

### **3.1.1 Join the servers to the domain**

You're now able to join the VMs to **corp.contoso.com**. Do the following steps for both the SQL Server VMs and the file share witness server:

1. Remotely connect to the virtual machine with **BUILTIN\DomainAdmin**.
2. In **Server Manager**, select **Local Server**.
3. Select the **WORKGROUP** link.
4. In the **Computer Name** section, select **Change**.
5. Select the **Domain** check box and type **corp.contoso.com** in the text box. Select **OK**.
6. In the **Windows Security** popup dialog, specify the credentials for the default domain administrator account (**CORP\DomainAdmin**) and the password (**Contoso!0000**).
7. When you see the "Welcome to the corp.contoso.com domain" message, select **OK**.
8. Select **Close**, and then select **Restart Now** in the popup dialog.

## **3.1.2 Add accounts**

Add the installation account as an administrator on each VM, grant permission to the installation account and local accounts within SQL Server, and update the SQL Server service account.

### **3.1.3 Add the Corp\Install user as an administrator on each cluster VM**

After each virtual machine restarts as a member of the domain, add **CORP\Install** as a member of the local administrators group.

1. Wait until the VM is restarted, then launch the RDP file again from the primary domain controller to sign in to **sqlserver-0** by using the **CORP\DomainAdmin** account.
2. In **Server Manager**, select **Tools**, and then select **Computer Management**.
3. In the **Computer Management** window, expand **Local Users and Groups**, and then select **Groups**.
4. Double-click the **Administrators** group.
5. In the **Administrators Properties** dialog, select the **Add** button.
6. Enter the user **CORP\Install**, and then select **OK**.
7. Select **OK** to close the **Administrator Properties** dialog.
8. Repeat the previous steps on **sqlserver-1** and **cluster-fsw**.

### **3.1.4 Create a sign-in on each SQL Server VM for the installation account**

Use the installation account (CORP\install) to configure the availability group. This account needs to be a member of the **sysadmin** fixed server role on each SQL Server VM. The following steps create a sign-in for the installation account:

1. Connect to the server through the Remote Desktop Protocol (RDP) by using the <MachineName>\DomainAdmin account.
2. Open SQL Server Management Studio and connect to the local instance of SQL Server.
3. In **Object Explorer**, select **Security**.
4. Right-click **Logins**. Select **New Login**.
5. In **Login - New**, select **Search**.
6. Select **Locations**.
7. Enter the domain administrator network credentials.
8. Use the installation account (CORP\install).
9. Set the sign-in to be a member of the **sysadmin** fixed server role.
10. Select **OK**.

Repeat the preceding steps on the other SQL Server VM.

To create an account for the system account and grant appropriate permissions, complete the following steps on each SQL Server instance:

Grant the following permissions to [NT AUTHORITY\SYSTEM] on each SQL Server instance:

* ALTER ANY AVAILABILITY GROUP
* CONNECT SQL
* VIEW SERVER STATE

The following script grants these permissions:

RANT ALTER ANY AVAILABILITY GROUP TO [NT AUTHORITY\SYSTEM]

GO

GRANT CONNECT SQL TO [NT AUTHORITY\SYSTEM]

GO

GRANT VIEW SERVER STATE TO [NT AUTHORITY\SYSTEM]

GO

### **3.1.5 Set the SQL Server service accounts**

On each SQL Server VM, set the SQL Server service account. Use the accounts that you created when you configured the domain accounts.

1. Open **SQL Server Configuration Manager**.
2. Right-click the SQL Server service, and then select **Properties**.
3. Set the account and password.
4. Repeat these steps on the other SQL Server VM.

For SQL Server availability groups, each SQL Server VM needs to run as a domain account.

## **3.1.6 Add Failover Clustering features to both SQL Server VMs**

To add Failover Clustering features, do the following steps on both SQL Server VMs:

1. Connect to the SQL Server virtual machine through the Remote Desktop Protocol (RDP) by using the CORP\install account. Open **Server Manager Dashboard**.
2. Select the **Add roles and features** link on the dashboard.
3. Select **Next** until you get to the **Server Features** section.
4. In **Features**, select **Failover Clustering**.
5. Add any additional required features.
6. Select **Install** to add the features.

Repeat the steps on the other SQL Server VM.

### **3.1.7 Open a TCP port in the firewall**

1. On the first SQL Server **Start** screen, launch **Windows Firewall with Advanced Security**.
2. On the left pane, select **Inbound Rules**. On the right pane, select **New Rule**.
3. For **Rule Type**, choose **Port**.
4. For the port, specify **TCP** and type the appropriate port numbers
5. Select **Next**.
6. On the **Action** page, keep **Allow the connection** selected, and then select **Next**.
7. On the **Profile** page, accept the default settings, and then select **Next**.
8. On the **Name** page, specify a rule name (such as **Azure LB Probe**) in the **Name** text box, and then select **Finish**.

Repeat these steps on the second SQL Server VM.

## **3.1.8 Create the cluster**

After the prerequisites are completed, the first step is to create a Windows Server Failover Cluster that includes two SQL Severs and a witness server.

1. Use Remote Desktop Protocol (RDP) to connect to the first SQL Server. Use a domain account that is an administrator on both SQL Servers and the witness server.
2. n the **Server Manager** dashboard, select **Tools**, and then select **Failover Cluster Manager**.
3. In the left pane, right-click **Failover Cluster Manager**, and then select **Create a Cluster**.
4. In the Create Cluster Wizard, create a one-node cluster by stepping through the pages with the settings in the following table:

| **Page** | **Settings** |
| --- | --- |
| Before You Begin | Use defaults |
| Select Servers | Type the first SQL Server name in **Enter server name** and select **Add**. |
| Validation Warning | Select **No. I do not require support from Microsoft for this cluster, and therefore do not want to run the validation tests. When I select Next, continue Creating the cluster**. |
| Access Point for Administering the Cluster | Type a cluster name, for example **SQLAGCluster1** in **Cluster Name**. |
| Confirmation | Use defaults unless you are using Storage Spaces. See the note following this table. |

### **Set the Windows server failover cluster IP address**

1. In **Failover Cluster Manager**, scroll down to **Cluster Core Resources** and expand the cluster details. You should see both the **Name** and the **IP Address** resources in the **Failed** state. The IP address resource cannot be brought online because the cluster is assigned the same IP address as the machine itself, therefore it is a duplicate address.
2. Right-click the failed **IP Address** resource, and then select **Properties**.
3. elect **Static IP Address** and specify an available address from the same subnet as your virtual machines.
4. In the **Cluster Core Resources** section, right-click cluster name and select **Bring Online**. Wait until both resources are online. When the cluster name resource comes online, it updates the domain controller (DC) server with a new Active Directory (AD) computer account. Use this AD account to run the availability group clustered service later.

### **3.1.9 Add the other SQL Server to cluster**

Add the other SQL Server to the cluster.

1. In the browser tree, right-click the cluster and select **Add Node**.
2. In the **Add Node Wizard**, select **Next**. In the **Select Servers** page, add the second SQL Server. Type the server name in **Enter server name** and then select **Add**. When you are done, select **Next**.
3. In the **Validation Warning** page, select **No** (in a production scenario you should perform the validation tests). Then, select **Next**.
4. In the **Confirmation** page if you are using Storage Spaces, clear the checkbox labeled **Add all eligible storage to the cluster.**
5. Select **Next**.
6. Select **Finish**.

Failover Cluster Manager shows that your cluster has a new node and lists it in the **Nodes** container.

1. Log out of the remote desktop session.

### **3.1.10 Add a cluster quorum file share**

In this example, the Windows cluster uses a file share to create a cluster quorum. This tutorial uses a Node and File Share Majority quorum.

1. Connect to the file share witness member server with a remote desktop session.
2. On **Server Manager**, select **Tools**. Open **Computer Management**.
3. Select **Shared Folders**.
4. Right-click **Shares** and select **New Share...**.

Use **Create a Shared Folder Wizard** to create a share.

1. On **Folder Path**, select **Browse** and locate or create a path for the shared folder. Select **Next**.
2. In **Name, Description, and Settings** verify the share name and path. Select **Next**.
3. On **Shared Folder Permissions** set **Customize permissions**. Select **Custom...**.
4. On **Customize Permissions**, select **Add...**.
5. Make sure that the account used to create the cluster has full control.
6. Select **OK**.
7. In **Shared Folder Permissions**, select **Finish**. Select **Finish** again.
8. Log out of the server

### **3.1.11 Configure the cluster quorum**

Next, set the cluster quorum.

1. Connect to the first cluster node with remote desktop.
2. In **Failover Cluster Manager**, right-click the cluster, point to **More Actions**, and select **Configure Cluster Quorum Settings...**.
3. In **Configure Cluster Quorum Wizard**, select **Next**.
4. In **Select Quorum Configuration Option**, choose **Select the quorum witness**, and select **Next**.
5. On **Select Quorum Witness**, select **Configure a file share witness**.
6. On **Configure File Share Witness**, type the path for the share you created. Select **Next**.
7. Verify the settings on **Confirmation**. Select **Next**.
8. Select **Finish**.

The cluster core resources are configured with a file share witness.

## **3.1.12 Enable availability groups**

Next, enable the **Always On availability groups** feature. Do these steps on both SQL Servers.

1. From the **Start** screen, launch **SQL Server Configuration Manager**.
2. In the browser tree, select **SQL Server Services**, then right-click the **SQL Server (MSSQLSERVER)** service and select **Properties**.
3. Select the **AlwaysOn High Availability** tab, then select **Enable AlwaysOn availability groups**, as follows:
4. elect **Apply**. Select **OK** in the pop-up dialog.
5. Restart the SQL Server service.

Repeat these steps on the other SQL Server.

### Create a backup share

1. On the first SQL Server in **Server Manager**, select **Tools**. Open **Computer Management**.
2. Select **Shared Folders**.
3. Right-click **Shares**, and select **New Share...**.

Use **Create a Shared Folder Wizard** to create a share.

4. On **Folder Path**, select **Browse** and locate or create a path for the database backup shared folder. Select **Next**.

5.In **Name, Description, and Settings** verify the share name and path. Select **Next**.

6.On **Shared Folder Permissions** set **Customize permissions**. Select **Custom...**.

7.On **Customize Permissions**, select **Add...**.

8.Make sure that the SQL Server and SQL Server Agent service accounts for both servers have full control.

9.Select **OK**.

10.In **Shared Folder Permissions**, select **Finish**. Select **Finish** again.

### Take a full and Transactional backup of the database

### **3.1.13 Create the availability group:**

1. On remote desktop session to the first SQL Server. In **Object Explorer** in SSMS, right-click **AlwaysOn High Availability** and select **New availability group Wizard**.
2. In the **Introduction** page, select **Next**. In the **Specify availability group Name** page, type a name for the availability group in **Availability group name**. For example, **AG1**. Select **Next**.
3. In the **Select Databases** page, select your database, and then select **Next**.
4. In the **Specify Replicas** page, select **Add Replica**.
5. The **Connect to Server** dialog pops up. Type the name of the second server in **Server name**. Select **Connect**.
6. Select **Endpoints** to see the database mirroring endpoint for this availability group. Use the same port that you used when you set the Firewall rule
7. In the **Select Initial Data Synchronization** page, select **Full** and specify a shared network location In the example it was, **\\<First SQL Server>\Shared\**. Select **Next**.
8. In the **Validation** page, select **Next**.
9. In the **Summary** page, select **Finish**, then wait while the wizard configures the new availability group. In the **Progress** page, you can select **More details** to view the detailed progress. Once the wizard is finished, inspect the **Results** page to verify that the availability group is successfully created.
10. Select **Close** to exit the wizard.

## **4.Create an Azure load balancer**

1. In the Azure portal, go to the resource group where your SQL Servers are and select **+ Add**.
2. Search for **Load Balancer**. Choose the load balancer published by Microsoft
3. Select **Create**.
4. Configure the following parameters for the load balancer.

|  | |
| --- | --- |
| **Setting** | **Field** |
| **Name** | Use a text name for the load balancer, for example **sqlLB**. |
| **Type** | Internal |
| **Virtual network** | Use the name of the Azure virtual network. |
| **Subnet** | Use the name of the subnet that the virtual machine is in. |
| **IP address assignment** | Static |
| **IP address** | Use an available address from subnet. Use this address for your availability group listener. Note that this is different from your cluster IP address. |
| **Subscription** | Use the same subscription as the virtual machine. |
| **Location** | Use the same location as the virtual machine. |

1. Select **Create**, to create the load balancer.

### **4.1 Add a backend pool for the availability group listener**

1. In the Azure portal, go to your availability group. You might need to refresh the view to see the newly created load balancer
2. elect the load balancer, select **Backend pools**, and select **+Add**.
3. Type a name for the backend pool.
4. Associate the backend pool with the availability set that contains the VMs.
5. Under **Target network IP configurations**, check **VIRTUAL MACHINE** and choose both of the virtual machines that will host availability group replicas. Do not include the file share witness server.
6. Select **OK** to create the backend pool
7. Select the load balancer, choose **Health probes**, and then select **+Add**.
8. Set the listener health probe as follows:

| **Set the probe** | | |
| --- | --- | --- |
| **Setting** | **Description** | **Example** |
| **Name** | Text | SQLAlwaysOnEndPointProbe |
| **Protocol** | Choose TCP | TCP |
| **Port** | Any unused port | 59999 |
| **Interval** | The amount of time between probe attempts in seconds | 5 |
| **Unhealthy threshold** | The number of consecutive probe failures that must occur for a virtual machine to be considered unhealthy | 2 |

1. Select **OK** to set the health probe.

### **4.2 Set the load balancing rules**

1. Select the load balancer, choose **Load balancing rules**, and select **+Add**.
2. Set the listener load balancing rules as follows
3. Select **OK** to set the listener load balancing rules

|  | | |
| --- | --- | --- |
| **Setting** | **Description** | **Example** |
| **Name** | Text | SQLAlwaysOnEndPointListener |
| **Frontend IP address** | Choose an address | Use the address that you created when you created the load balancer. |
| **Protocol** | Choose TCP | TCP |
| **Port** | Use the port for the availability group listener | 1433 |
| **Backend Port** | This field is not used when Floating IP is set for direct server return | 1433 |
| **Probe** | The name you specified for the probe | SQLAlwaysOnEndPointProbe |
| **Session Persistence** | Drop down list | **None** |
| **Idle Timeout** | Minutes to keep a TCP connection open | 4 |
| **Floating IP (direct server return)** |  | Enabled |

### **4.3 Add the cluster core IP address for the Windows Server Failover Cluster (WSFC)**

The WSFC IP address also needs to be on the load balancer.

1. In the Azure portal, go to the same Azure load balancer. Select **Frontend IP configuration** and select **+Add**. Use the IP Address you configured for the WSFC in the cluster core resources. Set the IP address as static.
2. On the load balancer, select **Health probes**, and then select **+Add**.
3. Set the WSFC cluster core IP address health probe as follows:

|  | | |
| --- | --- | --- |
| **Setting** | **Description** | **Example** |
| **Name** | Text | WSFCEndPointProbe |
| **Protocol** | Choose TCP | TCP |
| **Port** | Any unused port | 58888 |
| **Interval** | The amount of time between probe attempts in seconds | 5 |
| **Unhealthy threshold** | The number of consecutive probe failures that must occur for a virtual machine to be considered unhealthy | 2 |

1. Select **OK** to set the health probe.
2. Set the load balancing rules. Select **Load balancing rules**, and select **+Add**.
3. Set the cluster core IP address load balancing rules as follows.

| **Setting** | **Description** | **Example** |
| --- | --- | --- |
| **Name** | Text | WSFCEndPoint |
| **Frontend IP address** | Choose an address | Use the address that you created when you configured the WSFC IP address. This is different from the listener IP address |
| **Protocol** | Choose TCP | TCP |
| **Port** | Use the port for the cluster IP address. This is an available port that is not used for the listener probe port. | 58888 |
| **Backend Port** | This field is not used when Floating IP is set for direct server return | 58888 |
| **Probe** | The name you specified for the probe | WSFCEndPointProbe |
| **Session Persistence** | Drop down list | **None** |
| **Idle Timeout** | Minutes to keep a TCP connection open | 4 |
| **Floating IP (direct server return)** |  | Enabled |

1. Select **OK** to set the load balancing rules.

## **4.4 Configure the listener**

The next thing to do is to configure an availability group listener on the failover cluster

The availability group listener is an IP address and network name that the SQL Server availability group listens on. To create the availability group listener, do the following:

1. Get the name of the cluster network resource.

a. Use RDP to connect to the Azure virtual machine that hosts the primary replica.

b. Open Failover Cluster Manager.

c. Select the **Networks** node, and note the cluster network name. Use this name in the $ClusterNetworkName variable in the PowerShell script. In the following image the cluster network name is **Cluster Network 1**:

2. Add the client access point.  
The client access point is the network name that applications use to connect to the databases in an availability group. Create the client access point in Failover Cluster Manager.

a. Expand the cluster name, and then click **Roles**.

b. In the **Roles** pane, right-click the availability group name, and then select **Add Resource** > **Client Access Point**.

* 1. n the **Name** box, create a name for this new listener. The name for the new listener is the network name that applications use to connect to databases in the SQL Server availability group.
  2. To finish creating the listener, click **Next** twice, and then click **Finish**. Do not bring the listener or resource online at this point.

1. Take the availability group cluster role offline. In **Failover Cluster Manager** under **Roles**, right-click the role, and select **Stop Role**.
2. Configure the IP resource for the availability group.

a. Click the **Resources** tab, and then expand the client access point you created.  
The client access point is offline.

b. Right-click the IP resource, and then click properties. Note the name of the IP address, and use it in the $IPResourceName variable in the PowerShell script.

c. Under **IP Address**, click **Static IP Address**. Set the IP address as the same address that you used when you set the load balancer address on the Azure portal.

5. Make the SQL Server availability group resource dependent on the client access point.

a. In Failover Cluster Manager, click **Roles**, and then click your availability group.

b. On the **Resources** tab, under **Other Resources**, right-click the availability resource group, and then click **Properties**.

c. On the dependencies tab, add the name of the client access point (the listener) resource.

d. Click OK

6. Make the client access point resource dependent on the IP address.

a. In Failover Cluster Manager, click **Roles**, and then click your availability group.

b. On the **Resources** tab, right-click the client access point resource under **Server Name**, and then click **Properties**.

c. Click the **Dependencies** tab. Verify that the IP address is a dependency. If it is not, set a dependency on the IP address. If there are multiple resources listed, verify that the IP addresses have OR, not AND, dependencies. Click **OK**.

**4.5 Set the cluster parameters in PowerShell.**

a. Copy the following PowerShell script to one of your SQL Server instances. Update the variables for your environment.

* $ListenerILBIP is the IP address that you created on the Azure load balancer for the availability group listener.
* $ListenerProbePort is the port you configured on the Azure load balancer for the availability group listener.

b. Set the cluster parameters by running the PowerShell script on one of the cluster nodes.

1. Bring the availability group cluster role online. In **Failover Cluster Manager** under **Roles**, right click the role, and select **Start Role**.

If necessary, repeat the steps above to set the cluster parameters for the WSFC cluster IP address.

1. Get the IP address name of the WSFC Cluster IP address. In **Failover Cluster Manager** under **Cluster Core Resources**, locate **Server Name**.
2. Right-click **IP Address**, and select **Properties**.
3. Copy the **Name** of the IP address. It may be Cluster IP Address.
4. Set the cluster parameters in PowerShell.

a. Copy the following PowerShell script to one of your SQL Server instances. Update the variables for your environment.

* + $ClusterCoreIP is the IP address that you created on the Azure load balancer for the WSFC core cluster resource. It is different from the IP address for the availability group listener.
  + $ClusterProbePort is the port you configured on the Azure load balancer for the WSFC health probe. It is different from the probe for the availability group listener.

  b. Set the cluster parameters by running the PowerShell script on one of the cluster nodes.

## 4.5 **In SQL Server** **Set listener port**

Management Studio, set the listener port.

1. Launch SQL Server Management Studio and connect to the primary replica.
2. Navigate to **AlwaysOn High Availability** > **availability groups** > **availability group Listeners**.
3. You should now see the listener name that you created in Failover Cluster Manager. Right-click the listener name and select **Properties**.
4. In the **Port** box, specify the port number for the availability group listener. 1433 is the default. Select **OK**.

You now have a SQL Server availability group in Azure virtual machines running in Resource Manager mode.