Configuring or using failover groups

Last updated by | Vitor Tomaz | Nov 24, 2021 at 2:51 AM PST

Contents

Self-help content presented in Azure Portal

(This content was shown to the customer during case submission. It's also visible on 'Diagnose and solve problems' blade.)

Resolve issues when configuring or using failover groups

You can use auto-failover groups to enable transparent and coordinated failover of multiple databases in Azure SQL Managed Instance.

The auto-failover group must be configured on the primary instance and auto-failover group will connect the primary instance to the secondary instance in a different Azure region. All databases in the instance will be replicated to the secondary instance.

Long running or failed create failover group operation

If creating the failover group is a taking a long time, an error may already have been detected. To check for error messages:

1. Go to the resource group on Azure Portal.
2. Select **Deployments**.
3. Find the related deployment and select it via the link available in the deployment name.
4. Find the resource with type Microsoft.Sql/locations/instanceFailoverGroups and select **Operation details**.
5. Investigate the status message for more details.

Create the geo-secondary managed instance

To ensure non-interrupted connectivity to the primary SQL Managed Instance after failover, both the primary and secondary instances must be in the same DNS zone.

DNS zone is a property of a SQL Managed Instance and underlying virtual cluster, and its ID is included in the host name address. The zone ID is generated as a random string when the first SQL Managed Instance is created in each VNet and the same ID is assigned to all other instances in the same subnet. Once assigned, the DNS zone cannot be modified. SQL Managed Instances included in the same failover group must share the DNS zone.

Do this by specifying an optional parameter during creation. If you are using PowerShell or the REST API, the name of the optional parameter is DNSZonePartner. The name of the corresponding optional field in the Azure portal is Primary Managed Instance.

The first managed instance created in a subnet determines the DNS zone for all subsequent instances in the same subnet. This usually means that the secondary instance needs to be created in an empty subnet so the same DNS zone as primary can be specified.

If the managed instance you plan to use as secondary is dimmed in Azure portal, it's likely using a different DNS zone.

Enabling geo-replication between managed instance virtual networks

When you set up a failover group between primary and secondary SQL Managed Instances in two different regions, each instance is isolated using an independent virtual network. To allow replication traffic between these VNets, make sure these prerequisites are met:

- The two SQL Managed Instance VNets cannot have overlapping IP addresses.
- The secondary SQL Managed Instance is configured with the same DNS zone ID as the primary.
- The two instances of SQL Managed Instance need to be in different Azure regions.
- The two instances of SQL Managed Instance need to be the same service tier, and have the same storage size.
- Your secondary instance of SQL Managed Instance must be empty (no user databases).
- The virtual networks used by the instances of SQL Managed Instance are connected through Global VNet Peering, VPN Gateway or Express Route.
  Note: Global VNet Peering is only supported for SQL Managed Instances created in empty subnets after 9/22/2020, as well for all the subsequent managed instances created in those subnets. To be able to use global virtual network peering for SQL managed instances from virtual clusters created before the announcement date, consider configuring a non-default maintenance window on the instances, as it will move the instances into new virtual clusters that support global virtual network peering.
- Network Security Groups (NSG) are set up such that ports 5022, and the range 11000-11999, are open inbound and outbound for connections from the subnet of the other managed instance. This allows replication traffic between the instances. When two virtual networks connect through an on-premises network, make sure there is no firewall rule blocking ports 5022, and 11000-11999.

For a detailed tutorial on how to add a managed instance to a failover group, see:

- Tutorial using Azure portal
- Tutortial using PowerShell

Common errors the first time you configure failover group

Replication to the partner managed instance could not be established. Verify that connectivity between the Virtual Networks of the primary and secondary managed servers has been established correctly according to guidelines

Verify that the NSG, firewall, and VNet connectivity are set up correctly.

Unable to select secondary managed instance when adding failover group on Azure portal

This is usually caused by a DNS zone ID mismatch. Make sure that you deploy the secondary managed instance under same DNS zone ID, by following Create a secondary managed instance.

Create a failover group between managed instances in different subscriptions

You can create a failover group between SQL Managed Instances in two different subscriptions if they are associated to the same Azure Active Directory Tenant. Azure portal does not support the creation of failover groups across different subscriptions, use PowerShell or REST API.

Manage failover to secondary instance

The failover group will manage the failover of all the databases in the SQL Managed Instance. When a group is created, each database in the instance will be automatically geo-replicated to the secondary SQL Managed Instance. You can't use failover groups to initiate a partial failover of a subset of the databases.

For the existing failover groups across different subscriptions and/or resource groups, failover can't be initiated manually via portal from the primary SQL Managed Instance. Instead, initiate it from the geo-secondary instance.

Read-write and read-only listeners

Read-write and read-only listeners are DNS CNAME records that point to the current primary's URL and secondary's URL. They are created automatically when the failover group is created and allow the workloads to transparently reconnect to the new primary/secondary when they change after failover.

- The DNS CNAME record for the read-write listener URL is formed as `<fog-name>.<zone_id>.database.windows.net`
- The DNS CNAME record for the read-only listener URL is formed as `<fog-name>.secondary.<zone_id>.database.windows.net`

Resources

- Best practices for configuring auto-failover group in Managed Instance
- Enabling geo-replication between managed instances and their VNets

How good have you found this content?

🙂 🙁