VNET - Virtual Network integration and failover groups

Last updated by | Vitor Tomaz | Aug 5, 2020 at 12:40 PM PDT

Contents

Update: 2018-07-17

Update from Subbu:

Engineering recently made change to **block** creating a Failover group if customer is using VNET (and vice versa) as those two features are not currently supported **together**.

An update to online document (Azure docs) is required and currently in progress for customer awareness. In meantime if you have related case(s), please let customer know it's not supported and share RCA.

RCA : *"The failover groups were never supported with virtual network firewall rules due to connectivity problems that may occur once customer perform a failover of a Failover Group. We have recently realized that we are not disallowing customers to create such configurations and therefore blocked it with the recent deployment. We are in process of updating our documentation and we are also working on fixing it, but no ETA for a fix is known yet."*

vNet Integration and failover group are not compatible

~~**Short summary: vNet integration and failover group are compatible**~~ **~~features and can work together.~~**

Explanation

When using vNet integration this **actually just configure firewall access** from that subnet on a vNet to the Azure SQL DB.

On top of that it register endpoint in the vNet so traffic can be captured and reroute accordingly

Behavior from client resource inside of the vNet:

- The client VM on the vNet will use the regular public IP of the Azure SQL DB to connect.

(ping will be translated to the public IP address on the VM within the vNet)

- From network perspective (network trace) the traffic will be targeted to the public IP of the Azure SQL DB (this is true for MySQL and PGSQL as well, as for now *this* is not

implemented for them so in case of vnet integration connection to MySQL and PGSQL will fail)

- The traffic will be captured by the endpoint on that vnet and will be handled internally within Azure infrastructure without actually going out to the public internet.
- This is the "magic" with vNet integration

Behavior from Azure SQL:

- Client can / cannot connect based on firewall rules
- When client is in allowed subnet he will be able to connect
- SQL server will see that the client is connected with the vNet IP address as the source

This can be confirmed by querying: select * from sys.dm_exec_connections

Behavior when using failover group with vNet integration:

First, we need to ask about the scenario when this is applicable, when DB is failing over between regions what is the chances for the application to be still active in the original location

(this is still possibility, I already had a case with this scenario)

When using failover group listener, we still accessing the public IP of the FG endpoint name, and the traffic will be handled by the vNet endpoint so we can get access to the destination server via FG endpoint name.

Since vnet integration is applicable only on the same region, this will work only for that region, so once failover occur, the secondary region will treat the original region as any other client, therefore in order to connect the client should be configured with his public IP on the secondary server.

If the application is failing over to the other region as well, it can have vNet integration in the secondary region so it can continue working after app + db has been failed over to the secondary region.

Remember that from SQL DB perspective this is no more than just a firewall rule.

Thanks to @Matteo Teruzzi and @Jose Manuel Jurado Diaz for helping me with this case.

Written by Yochanan Rachamim (yocr)

How good have you found this content?