

Random connectivity failure due to firewall issue in Managed VNet IR

Contents

- Not applicable any more, please don't use this
- Issue description:
- Root cause analysis:
- Temp Solution:

****Not applicable any more, please don't use this ****

Issue description:

Customer pipelines were randomly failing with error:

Sample failure in Sql: Source=Microsoft.DataTransfer.ClientLibrary,"Type=System.Data.SqlClient.SqlException,Message=Cannot open server 'sr-col-dev-we-sql' requested by the login. Client with IP address '**20.76.4.235**' is not allowed to access the server. To enable access, use the Windows Azure Management Portal or run sp_set_firewall_rule on the master database to create a firewall rule for this IP address or address range. It may take up to five minutes for this change to take effect.

Sample failure in Azure Sql: [Source=.Net](#) SqlClient Data Provider,SqlErrorNumber=47073,Class=14,ErrorCode=-2146232060,State=1,Errors=[{Class=14,Number=47073,State=1,Message=Reason: An instance-specific error occurred while establishing a connection to SQL Server. Connection was denied since Deny Public Network Access is set to Yes (<https://docs.microsoft.com/azure/azure-sql/database/connectivity-settings#deny-public-network-access>). To connect to this server, use the Private Endpoint from inside your virtual network (<https://docs.microsoft.com/azure/sql-database/sql-database-private-endpoint-overview#how-to-set-up-private-link-for-azure-sql-database>),}]

Sample failure in Storage:

type=System.Net.WebException,Message=Unable to connect to the remote server,Source=System,"Type=System.Net.Sockets.SocketException,Message=A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond **20.38.109.130**:443

Sample failure in KeyVault:

Status code 403, {"error":{"code":"Forbidden","message":"Client address is not authorized and caller is not a trusted service.\r\nClient address: **40.118.57.136**\r\nCaller: appid=af3511f2-3ed7-4e71-b8e4-01d4ce15b7d5;oid=328ce99e-aeaa-4784-bf9c-fd7f912dde58;iss=<https://sts.windows.net/ce4a1124-ed6b-4c9c-8413-6225f4e91136/\r\nVault:> CREDTKV-api;location=westeurope","innererror":{"code":"ForbiddenByFirewall"}}}

Customer pipeline is running using Managed VNet IR, and customer has setup Managed Private Endpoint for the data store, but the failure still complains that some IP is not in the firewall.

Root cause analysis:

VNet team confirmed it's a issue on their side: <https://portal.microsofticm.com/imp/v3/incidents/details/230167694/home>

Temp Solution:

For Copy activity, set retry on the activity. For Non-Copy activity, including Pipeline/External activity, suggest customer to stop queueing any more pipeline/external activities for the next TTL time(default is 60minutes), and start new activity after the TTL time.

How good have you found this content?

