Error: 0 - The specified network name is no longer available

Last updated by | Vitor Tomaz | Dec 15, 2021 at 2:31 AM PST

Contents

- Issue
- Investigation/Analysis
- Mitigation
- Classification

Issue

Our customer is connecting from OnPremise to Azure Managed Instance using ExpressRoute and they got the following error:

```
TITLE: Connect to Server
------------------------------
Can not connect to xxxx.xxxx.database.windows.net
------------------------------
ADDITIONAL INFORMATION:
A connection was successfully established with the server, but then an error occurred during the login process
```

However, within Azure our customer is able to connect to this Managed Instance and other services like SQL Server on Virtual Machine our customer is able without problems.

Investigation/Analysis

As our customer was using SQL SERVER 2008 Management Studio. But, my suggestion is to use the latest version, because SQL Server 2008 Management Studio reported other errors.

Using MonLogin we found this information:

user_error	error	tds_version	total_time_ms	enqueue_time_ms	netwrite_time_ms	netread_time_ms	ssl_t
1	17830	0	5880	0	0	5880	
1	17830	0	5403	0	0	5403	
1	17830	0	5738	0	0	5738	
1	17830	0	5556	0	0	5556	

In the network trace we found that after 5 seconds the MI reset the connection.

Use [Azure SQL Connectivity Checker]

Alternatively:
We took the network trace using the following statements using Windows Command Prompt with Administrator permissions:

Start the process: **netsh trace start capture=yes packettruncatebytes=512 tracefile=%temp%\%computername%_nettrace.etl maxsize=400 filemode=circular overwrite=yes report=no**

Reproduce the issue.

Stop the process: **netsh trace stop**

Right click on any column header and select 'Group' to create a grouping.

MessageNumber	Timestamp	TimeDelta	EventRec	EventRecor	Module	Summary	SourceAddress	SourcePort	Destination	DestinationPort
878	2019-03-07T12:32:25.3966185		4	1840	TCP	Flags: CE....S., SrcPort: 63238, Dst…	10.200.128.128	63238	10.36.191.62	TDS(1433)
888	2019-03-07T12:32:25.4523315	0,0557130	0	0	TCP	Flags: ...A..S., SrcPort: TDS(1433),…	10.36.191.62	TDS(1433)	10.200.128.128	63238
889	2019-03-07T12:32:25.4523993	0,0000678	0	0	TCP	Flags: ...A...., SrcPort: 63238, Dst…	10.200.128.128	63238	10.36.191.62	TDS(1433)
890	2019-03-07T12:32:25.4525739	0,0001746	7360	7684	TDS	PreLogin, Status: EndOfMessage, Leng…	10.200.128.128	63238	10.36.191.62	TDS(1433)
918	2019-03-07T12:32:25.7526969	0,3001230	0	0	TCP	Flags: ...AP..., SrcPort: 63238, Dst…	10.200.128.128	63238	10.36.191.62	TDS(1433)
957	2019-03-07T12:32:26.3477568	0,5950599	0	0	TCP	Flags: ...AP..., SrcPort: 63238, Dst…	10.200.128.128	63238	10.36.191.62	TDS(1433)
1051	2019-03-07T12:32:27.5508301	1,2030733	0	0	TCP	Flags: ...AP..., SrcPort: 63238, Dst…	10.200.128.128	63238	10.36.191.62	TDS(1433)
1233	2019-03-07T12:32:29.9549441	2,4041140	0	0	TCP	Flags: ...AP..., SrcPort: 63238, Dst…	10.200.128.128	63238	10.36.191.62	TDS(1433)
1264	2019-03-07T12:32:30.6626042	0,7076601	0	0	TCP	Flags: ...A.R.., SrcPort: TDS(1433),…	10.36.191.62	TDS(1433)	10.200.128.128	63238

Based on several documentation, if after the Pre-Login we don't receive or the connection takes more than 5 seconds independent on the timeout of the connection the connection will be discarded by MI.

Working with our customer and Networking team we found

"

It looks like in addition to there being an ExpressRoute, there is also a Palo Alto NVA that is configured to inspect the north/south traffic between on-prem and Azure. The route table on the ExR Gateway subnet routes 10.36.0.0/18 (SQL MI VNET) through this NVA at 10.36.56.252. On other subnets in this SQL MI VNET, there's a UDR to route 0.0.0.0/0, 10.36.16.0/21, and 10.35.20.0/22 through the NVA at IP 10.36.55.252. They also have BGP Route Propagation disabled, so routes from the ExpressRoute will not be learned in the VNET. Therefore all that traffic for on-prem will be routed to the Palo Alto NVA due to the 0.0.0.0/0 route.

On the SQL MI subnet, they only have a 0.0.0.0/0 route with next hop internet, and BGP Route Propagation is not disabled.

As a result they have asymmetric routing. Inbound traffic over the ExpressRoute will be routed through the Palo Alto NVA, but return traffic will not. The first packet from on-prem would unlikely be a problem since it's a new connection. The return traffic will not be a problem, since we do not track connections on the ExpressRoute and just forward everything. However, the 2ndpacket from on-prem would be out of order when it hits the Palo Alto, and the Palo Alto would likely drop it or encounter delays in processing.

I recommend two steps for the customer.

First, on the SQL MI route table SQLPaaS-PRE-TRutas, fix the route to on-prem so that it routes through the NVA. That is, change the 0.0.0.0/0 route to next hop Virtual Appliance 10.36.55.252 and disable BGP Route Propagation. Alternatively, for testing they can simply disable BGP route propagation and route only

10.200.128.0/23 through Virtual Appliance 10.36.55.252 to reduce impact. This is a recommended solution, as it is likely to be the intended configuration.

If this does not resolve the issue, we will want to remove the Palo Alto NVA from the equation to further scope it to the NVA or the ExpressRoute circuit. To do this we would revert changes to SQLPaaS-PRE-TRutas route table to enable BGP Route Propagation and remove the Virtual Appliance routes. We would also add a route to the SUEZSpain-ER-TRutas route table in subscription *Input Subscription Id*. The route will be for prefix 10.36.191.0/26 to route to next hop VNET Local.

If we still encounter issues with the Palo Alto NVA removed from the equation, we know the issues is on-premises, on the ExpressRoute circuit, in our SDN, or on the SQL MI."

Mitigation

Disable BGP route propagation and route only 10.200.128.0/23 through Virtual Appliance 10.36.55.252 to reduce impact. Our customer was able to connect.

Classification

Root cause tree:

How good have you found this content?