Target principal name is incorrect using private link

Last updated by | Holger Linke | Feb 28, 2023 at 1:08 AM PST

Contents

You can find a much more detailed description in Sergio Fonseca's public troubleshooting article at Azure SQL DB Private Link / Private Endpoint - Connectivity Troubleshooting. This Wiki article documents the specific error "The target principal name is incorrect".

Issue

The customer has configured a private link endpoint for their Azure SQL Database and is trying to access it through their Azure VNet. They have disabled the public endpoint, but they can't connect to SQL anymore after that.

The application reports the following error:

> A connection was successfully established with the server, but then an error occurred during the login process.
> (provider: SSL Provider, error: 0 - The target principal name is incorrect.) (.Net SqlClient Data Provider)

Investigation

When checking the connection string that was used by the application, it turned out that the customer has configured either the private IP address of the SQL server, or has used the private link routing name. Neither is supported though.

If you try to connect using the private endpoint IP address, you are going to get an error like this:

```
============================
Cannot connect to 10.0.1.4.
============================
A connection was successfully established with the server, but then an error occurred during the login process
(provider: SSL Provider, error: 0 - The target principal name is incorrect.) (.Net SqlClient Data Provider)
------------------------------
Server Name: 10.0.1.4
Error Number: -2146893022
Severity: 20
State: 0
```

Similarly, if you use the private link routing name instead of the FQDN, you are going to get an error like this:

```
============================================================
Cannot connect to servername.privatelink.database.windows.net.
============================================================
A connection was successfully established with the server, but then an error occurred during the login process
(provider: SSL Provider, error: 0 - The target principal name is incorrect.) (.Net SqlClient Data Provider)
------------------------------
Server Name: servername.privatelink.database.windows.net
Error Number: -2146893022
Severity: 20
State: 0
```

The same error pattern will occur if you have configured a different DNS name for the SQL server, e.g. in a private DNS zone, and are then trying to connect to that custom name instead of the FQDN.

Mitigation

1. You must use the FQDN of the SQL server `servername.database.windows.net` to connect to Azure SQL Database.

   Any login attempts made directly to the IP address or using the private link FQDN (`servername.privatelink.database.windows.net`) will fail. This behavior is by design, because the private endpoint routes traffic to the SQL Gateway in the region, and the correct FQDN needs to be specified for logins to succeed. If the correct FQDN information of the registered server name isn't provided, the gateway routing won't succeed and the connection will fail.

2. If you are already using the FQDN `servername.database.windows.net` but still getting the error, then there might be something wrong with the DNS routing or the traffic routing from application to target. In this case, use the Azure SQL Connectivity Checker to test the network traffic from the source to the FQDN of the SQL server. There is a good chance that the DNS routing into the Azure VNet is misconfigured, or that a part of the traffic gets blocked by the customer firewall or their Azure Virtual Network Appliance.

3. If the customer is using a custom DNS name, they should be able to connect if the connection option "Trust server certificate" is enabled. However, not all drivers support the "Trust server certificate" option. Some drivers are supporting the "hostNameInCertificate" option which the customer can try to specify so that certificate validation is performed. See the related article on Managed Instance.

More Information

Lesson Learned #141 approaches the topic from a different angle:

Our customer tried to connect using the FQDN of their private link endpoint - `servername.privatelink.database.windows.net` and our customer got the error: Error 0 - The target principal name is incorrect. Why?

Here we have two issues to explain:

- First of all, when you created a private link there is not needed to connect to the server using the FQDN private link, basically, you need to pay attention in how you have created the private link. If you enabled the Private DNS for a specific VNET and Subnet, you are going to have a new entry in your DNS with the new IP resolution of you Azure SQL Database `servername.database.windows.net`. If you didn't enable this private DNS or you didn't allow to update the DNS entry, the resolution will be the public IP. For this reason, it is very important to know this first thing. Please, always check the DNS resolution when you have enable a private endpoint.
- Second, when you establish the connection to Azure SQL Database, in order to encrypt the data, our gateway encryt this using the certificate that we have for the domain `*.database.windows.net`. For this reason, if you tried to connect `servername.privatelink.database.windows.net` you are going to have this error message about "Error 0 - The target principal name is incorrect" if you want to skip this validation, basically you need to specify in your connection string the parameter "Trust Server Certificate" and you would be able to connect. But, my recomendation is always use the `servername.database.windows.net` and configure correctly your DNS to prevent any additional problem.

Public Doc Reference

- Azure SQL DB Private Link / Private Endpoint - Connectivity Troubleshooting
- Azure Private Link for Azure SQL Database and Azure Synapse Analytics
- Check connectivity using SQL Server Management Studio (SSMS)
- DNS configuration scenarios

Root Cause Classification

Cases resolved by this TSG should be coded to the following root cause:

Root Cause: Azure SQL v3\Connectivity\Login Errors\Other

How good have you found this content?