The target principal name is incorrect

Last updated by | Vitor Tomaz | Feb 24, 2023 at 3:30 AM PST

Contents

Issue

Customer gets error "The target principal name is incorrect" while trying to connect to SQL MI.

Connection to database X failed (error -2146893022, state 0): A connection was successfully established with the server, but then an error occurred during the log in process. (provider: SSL Provider, error: 0 - The target principal name is incorrect.)

Investigation/Analysis

A few reasons that can cause this problem:

- **Customer is using a custom DNS name**
  Customer should be able to connect when the checkbox "Trust server certificate" is checked.
  However, not all drivers support the "Trust server certificate" option. Some drivers, like the OLE DB driver since v19.0 is supporting hostNameInCertificate option which the customer can try to specify so the certificate validation is performed.

- **Customer is connecting to the wrong IP Address**
  Wrong DNS configuration or cached results may direct the connection to the wrong IP address (wrong Virtual Cluster) and certificate validation will fail because the dns_zone is different. Use Azure SQL Connectivity Checker to help confirm the cause (RemoteCertificateNameMismatch) :

```
$parameters = @{
    # Supports Single, Elastic Pools and Managed Instance (please provide FQDN, MI public endpoint is
    # Supports Azure Synapse / Azure SQL Data Warehouse (*.sql.azuresynapse.net / *.database.windows.n
    # Supports Public Cloud (*.database.windows.net), Azure China (*.database.chinacloudapi.cn), Azure
    Server = 'mi43.public.e7b0d5db2d92.database.windows.net,3342' # or any other supported FQDN
    Database = ''  # Set the name of the database you wish to test. 'master' will be used by default i
```

```
Advanced connectivity policy tests (please wait):
[2022.07.26 10:00:10.5669] Connect initiated (attempt # 1).
[2022.07.26 10:00:10.5685]   DNS resolution took 0 ms, (20.216.148.25)
[2022.07.26 10:00:10.6090]   TCP connection open
[2022.07.26 10:00:10.6090]    Local endpoint is 192.168.1.65:1187
[2022.07.26 10:00:10.6090]    Remote endpoint is 20.216.148.25:3342

[2022.07.26 10:00:10.6095]  Building PreLogin message.
[2022.07.26 10:00:10.6115]   Adding PreLogin option Encryption [EncryptOff].
[2022.07.26 10:00:10.6115]   Adding PreLogin option TraceID
[2022.07.26 10:00:10.6120]    ConnectionID: 36D62006-1383-408F-8F6E-0EC5CADE0F8C
[2022.07.26 10:00:10.6120]    ActivityID: ED16284E-85AB-4ABC-B0B3-A242FB630CA9
[2022.07.26 10:00:10.6120]    ActivitySequence: 0
[2022.07.26 10:00:10.6120]   Adding PreLogin message terminator.
[2022.07.26 10:00:10.6159]  PreLogin message sent.

[2022.07.26 10:00:10.6164]  Waiting for PreLogin response.
[2022.07.26 10:00:10.6552]   Server requires encryption, enabling encryption.
[2022.07.26 10:00:10.6572]   Opening a new SslStream.
[2022.07.26 10:00:10.6576]   Trying to authenticate using Default, Tls11, Tls12:
[2022.07.26 10:00:11.0693]    Certificate error: RemoteCertificateNameMismatch
[2022.07.26 10:00:11.0723]    Cert details:
[2022.07.26 10:00:11.0723]     issued to CN=0d67f5456c3d.database.windows.net
[2022.07.26 10:00:11.0723]     valid from 5/25/2022 12:43:57 PM until 5/25/2023 12:43:57 PM
[2022.07.26 10:00:11.0723]     issued from CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US
[2022.07.26 10:00:11.0723]    Cert details:
[2022.07.26 10:00:11.0723]     issued to CN=Microsoft RSA TLS CA 01, O=Microsoft Corporation, C=US
[2022.07.26 10:00:11.0723]     valid from 7/22/2020 12:00:00 AM until 10/8/2024 8:00:00 AM
[2022.07.26 10:00:11.0723]     issued from CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
[2022.07.26 10:00:11.0723]    Cert details:
[2022.07.26 10:00:11.0723]     issued to CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
[2022.07.26 10:00:11.0723]     valid from 5/12/2000 7:46:00 PM until 5/13/2025 12:59:00 AM
[2022.07.26 10:00:11.0723]     issued from CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
[2022.07.26 10:00:11.0743] Exception:
[2022.07.26 10:00:11.0743] The remote certificate is invalid according to the validation procedure.
[2022.07.26 10:00:11.0758]  Disconnect initiated.
[2022.07.26 10:00:11.0758]  Disconnect done.
```

Mitigation

- If customer is using a custom DNS name, check "Trust server certificate" and/or use a driver that supports hostNameInCertificate.
- If customer is connecting to the wrong IP Address, the DNS resolution needs to be fixed.

How good have you found this content?