[Oracle] Troubleshoot SSL handshake failure

Last updated by | Xing Wei | Apr 17, 2022 at 8:53 PM PDT

Contents

Issue Description

When following ADF doc 'To use TLS' section on setting up SSL/TLS connection, getting SSL handshake failure when connecting to Oracle DB via Oracle connector on SHIR in test connection, preview data and copy scenarios. Error message is like below,

```
[ODBC Oracle Wire Protocol driver]SSL Handshake Failure reason [Unknown SSL Error]
```

Prerequisite

Please refer to this training session for ramping up basic knowledge on SSL/TLS connection.

Troubleshooting

The general idea is to narrow down the connectivity issue (driver, VM, network, Oralce server, etc.) and identify the culprit.

1. EncryptionMethod = 1 means data sent between the driver and Oracle server is encrypted using the TLS/SSL protocols. But in order to take effect, make sure it is supported/enabled by Oracle as well, otherwise the connection fails and the driver returns SSL handshake error.
    - The Oracle server settings related with TLS/SSL are specified in Sqlnet.ora file. Customer should reach out Oracle DBA for double checking the configured settings.

2. Check whether service logon account of the SHIR such as NT SERVICE\DIAHostService has read access to the trust store file.
    - monitor tool (https://docs.microsoft.com/en-us/sysinternals/downloads/procmon) will help provide more details about file path and permissions

3. If the above was checked and the issue persists, then collect netmon trace from the SHIR machine to determine the stage of the failure. i.e. From the client/server comms flow image in the training session video.

4. Check if customer is using proxy or any firewalls - that could potentially block connectivity

5. Use other client tool (such as SQL plus) to test connectivity from the same VM to the server, this also helps to validate the certificate and reveal if there was mis-configuration in the linked service properties.

6. If SHIR is on Azure VM deployed with Vnet peering, review NSG and ensure connectivity access is not blocked.

7. If the above options could not help, involve CSS AAD SSL expert for further review.

8. If issue persists, try out reproducing in your lab environment and check with Progress team to work together.