18c Active Directory Password Authentication Fails With ORA-28276 for Client Connections Below 12c (Doc ID 2472256.1)

In this Document

APPLIES TO:

Oracle Database - Enterprise Edition - Version 18.1.0.0.0 and later
JDBC - Version 11.1.0.6 to 12.1.0.2.0 [Release 11.1 to 12.1]
Information in this document applies to any platform.

SYMPTOMS

Version 18c of the database introduces the ability to authenticate incoming connections using Active Directory without EUS (Enterprise User Security) or some other intermediate directory service, as discussed here in the following documentation:

Release 18 Security Guide
Chapter 5: Configuring Centrally Managed Users with Microsoft Active Directory
Section: About Configuring Password Authentication for Centrally Managed Users

There are 3 authentication methods that can be configured: Password authentication; Kerberos authentication; or SSL authentication.

When using password authentication, 12.2.0.1 client connections, such as the 12.2.0.1 JDBC driver, is able to connect to the 18.x database.
However, when connecting using an older client connection, such as 11.2.0.4, the connection fails with the following error:

ORA-28276: Invalid ORACLE password attribute

CHANGES

CAUSE

Older client connections need to be added to the Active Directory group ORA_VFR_11G.

This is discussed in the following documentation:

Release 18 Security Guide
Chapter 5: Configuring Centrally Managed Users with Microsoft Active Directory
Section: About Configuring Password Authentication for Centrally Managed Users

"To maintain backward compatibility (if your site requires it), the Oracle filter can generate password verifiers to work

with Oracle Database clients for releases 11g, 12c, and 18c. The Oracle password filter uses Active Directory groups named ORA_VFR_MD5 (for WebDAV), ORA_VFR_11G (for release 11g) and ORA_VFR_12C (for releases 12c and 18c) to determine which Oracle Database password verifiers to generate. These groups must be created in Active Directory for the Oracle password verifiers to be generated for group member users. These are separate groups that dictate which specific verifiers should be generated for the Active Directory users. For example, if ten directory users need to log in to a newly created Oracle Database release 18c database that only communicated with Oracle Database release 18c and 12c clients, then an Active Directory group ORA_VFR_12C will have ten Active Directory users as members. The Oracle filter will only generate 12C verifiers for these ten Active Directory users when they change passwords with Active Directory (18c verifiers are the same as 12c verifiers)."

NOTE: This is not confined to JDBC connections; the documentation specifies that any type of incoming client connection should adhere to these guidelines.

SOLUTION

For older client connections, add the user to the Active Directory group ORA_VFR_11G.