AAD Group on Master

Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:41 AM PST

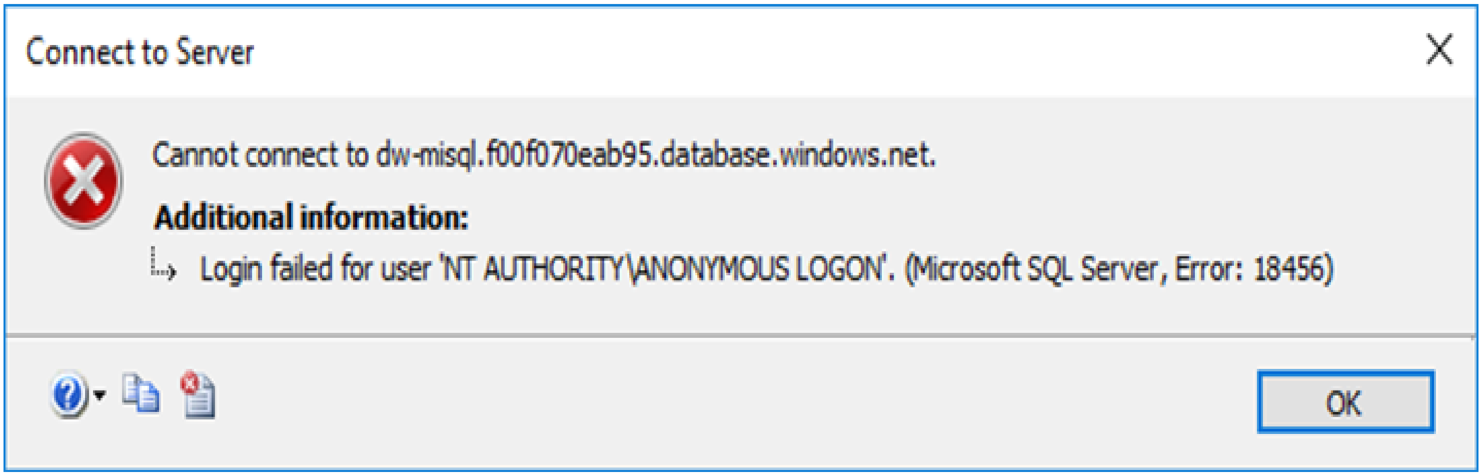
Contents

Issue

Logging into Master or database fails as AD Auth (username / password) when user was added as a member of a group however would work fine when added on their own as an individual account in the database.

From PG:
Azure SQL we support AAD auth where AAD can be based on various topologies, one of those being federated domain.

Checking AD Explorer in ASC showed the Group and the User as a member of that Group. When adding an AD Group our customer could create the account in Master and the user database with CREATE LOGIN [group] FROM EXTERNAL PROVIDER as one would expect. When logging in Fiddler shows the token passed successfully. However Login would fail with:



Connect to Server

Cannot connect to dw-misql.f00f070eab95.database.windows.net.

Additional information:

Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'. (Microsoft SQL Server, Error: 18456)

We would see in MonLogin SNI_CONSUMER_ERRORS 18456 State 62 to match with the above timestamp

Mitigation

This is a known issue with master DB and security groups. We do not support standalone database principals for AAD groups in master database. We do support database principals for AAD groups that are mapped to AAD server principals (CREATE USER FROM LOGIN statement). To work around this issue, customer may:

1. Create database users with individual AAD accounts in master database, and with AAD group in other databases

2. Create AAD server principals (in public preview) based on this AAD group:

```
CREATE LOGIN [group] FROM EXTERNAL PROVIDER
```

optionally, the customer may create a database principal for this server principal, in case any database-level permission needs to be granted in master DB:

```
CREATE USER [group] FROM LOGIN
```

Classification

Root cause tree:

How good have you found this content?

🙂 🙁