

Msg 2760: The specified schema name user@domain.xyz either does not exist or you do not have permissions to use it

Last updated by | Radhika Shah | May 30, 2022 at 4:55 PM PDT

Contents

- [Msg 2760: The specified schema name user@domain.xyz e...](#)
- [Issue](#)
- [Investigation/Analysis](#)
- [Mitigation](#)
- [Internal Reference](#)
- [Classification](#)

Msg 2760: The specified schema name user@domain.xyz either does not exist or you do not have permissions to use it

Tuesday, April 23, 2019

11:39 AM

Issue

Today I bumped into a pretty interesting case where the customer had setup their MI correctly, by granting it AAD read access and everything was properly set.

The user had mapped an AAD group as the MI AAD Admin and when attempting to create a new role or schema logged in as the AAD user, it failed with this error:

```
Msg 2760, Level 16, State 1, Line 3
The specified schema name "user@domain.xyz" either does not exist or you do not have permission to
Msg 2759, Level 16, State 0, Line 3
CREATE SCHEMA failed due to previous errors.
```

Error message: "Msg 2760, Level 16, State 1, Line 3

The specified schema name [user@domain.xyz](#) either does not exist or you do not have permissions to use it.

Msg 2759, Level 16, State 0, Line 3

CREATE SCHEMA failed due to previous errors".

Investigation/Analysis

Basically, the CREATE SCHEMA failed because CREATE SCHEMA is an atomic clause. This meaning that if something prior to this fails, the CREATE SCHEMA will fail.

Upon investigating a bit more I found this: <https://docs.microsoft.com/en-us/sql/t-sql/statements/create-schema-transact-sql?view=sql-server-2017#remarks>

Note:

The implicit creation of an Azure Active Directory user is not possible on SQL Database. Since creating an Azure AD user from external provider must check the users status in the AAD, creating the user will fail with error 2760: The specified schema name "<user_name@domain>" either does not exist or you do not have permission to use it. And then error 2759: CREATE SCHEMA failed due to previous errors. To work around these errors, create the Azure AD user from external provider first and then rerun the statement creating the object."

This is a known limitation to Managed Instance.

So, more in detail, the authenticated user is a member of the AAD group and does not have a direct mapping to the database principals (it's authenticated in indirect way though group membership, which may in general case resolve to multiple groups).

When creating a new schema, SQL server attempts to configure an owner for this new schema, but it fails to resolve the account in the database principals (DMV: sys.database_principals) and tries to create an implicit user for this AAD account.

Implicit user creation is not currently supported for AAD accounts, so this error message is thrown.

Mitigation

The mitigation is to manually create a database principal for AAD account through CREATE USER statement.

```
"CREATE USER [user@domain.xyz] FROM EXTERNAL PROVIDER;"
```

Retry the command and it should work.

Internal Reference

IcM link for more references if needed: <https://icm.ad.msft.net/imp/v3/incidents/details/116580414/home>

Classification

Root cause tree:

How good have you found this content?

