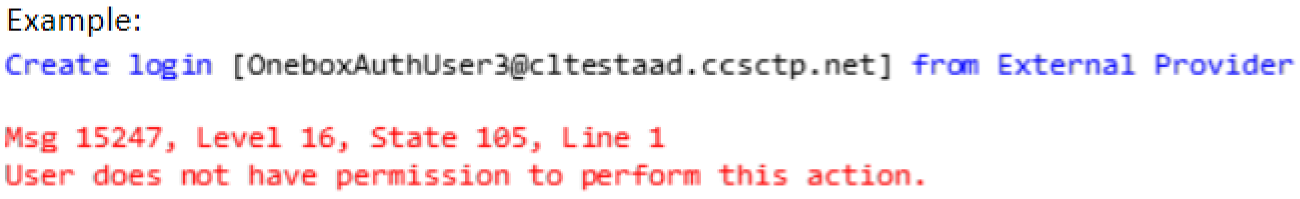
Creating an AAD login but it fails with “insufficient permission”

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:34 AM PDT

Contents

Issue



Example:

```
Create login [OneboxAuthUser3@cltestaad.ccsctp.net] from External Provider

Msg 15247, Level 16, State 105, Line 1
User does not have permission to perform this action.
```

Scenario #1

The customer must have an AAD admin configured and must be logged in as an admin to create an AAD login or a user who has the permission of the login manager. If the customer has an AAD admin configured, please refer to Scenario 2. If Admin is not configured, please share the document to configure an AAD admin for the SQL DB.

Note: A SQL user or SQL admin would not be able to create AAD logins. Only an AAD Admin or an AAD user who has login manager permission can create AAD logins.

Scenario #2

The customer has set up AAD admin but wants an AAD user who is not an admin to be able to create logins.

Solution: This can be achieved by an AAD admin who needs to perform the below steps:

- AAD Admin in master DB
- Create login <new user> from external provider
- Create user <new user> from LOGIN <new user>
- Alter role [loginmanager] add member [<new user>]

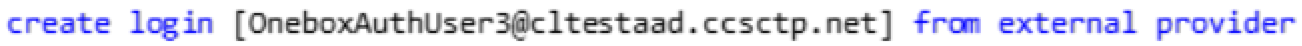
The new user will now have the permission to run the command

- Create login <new user> from external provider

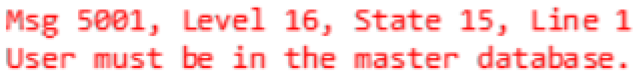
Scenario #3

The customer is trying to run Create Login <new_user> from external provider in a User DB.

Example:



```
create login [OneboxAuthUser3@cltestaad.ccsctp.net] from external provider
```



```
Msg 5001, Level 16, State 15, Line 1
User must be in the master database.
```

Customer can only create AAD logins : create login <new_user> from external provider in logical master database . They can create users based on login at the UserDatabase using

the DDL: Create user [new_user] from Login [new_user] given the AAD login already has been created at the logical master database

Root Cause (optional)

Detailed information/background that may be useful but isn’t strictly required for troubleshooting. Often these are the “verbose” details that one usually doesn’t need

Public Doc Reference (optional)

https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell#provision-azure-ad-admin-sql-database

Internal Reference (optional)

This may include links to architecture, training material, etc. that are helpful for understanding the steps given above.

Root Cause Classification

Security/AAD/AADLogins/Error/Failed

How good have you found this content?