Domain User is not a valid login or you do not have permission

Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:30 AM PST

Domain User is not a valid login or you do not have permission

Contents

Issue

Unable to add a new AAD user

Error

'Domain\User' is not a valid login or you do not have permission.

Mitigation

Following are the steps you need to follow to add a AAD user:

As an Active Directory admin for an Azure SQL Database server, you or your customer may want to grant existing Azure Active Directory (henceforth known as Directory) Groups or Users the ability to access Azure SQL Databases using their Directory credentials. If said users happen to be a member of a Directory Group that has been designated as the Active Directory admin for the Azure SQL Database server, then these users can access the databases without further effort. If, however, said users are not a part of said group, then user accounts will need to be created via SQL Server Management Studio 2016 (or newer) by the Active Directory admin. To accomplish this:

Log into SQL Server Management Studio 2016 (or newer) using Active Directory Password Authentication for Authentication. The User name MUST contain the full User Principal Name of the Directory account (i.e. alias@domain.com or alias@domain.onmicrosoft.com).

In normal circumstances where Directory credentials are not a factor, an Azure SQL Database server administrator would need to create both a user login and a user (to set permissions). However, since Directory credentials are at play here, the process is unique. In this case, a login does not need to be created, as the logins are pulled from existing Directory Groups and Users. Thus, a user needs to be created in order to establish general access permissions. As Directory Groups and Users can only be added via the Contained Database User model, select the database you want to grant a user access to, and initiate a new query.

Steps

Run the following TSQL command against the database to create the user:

```
CREATE USER [alias@domain.com or alias@domain.onmicrosoft.com] FROM EXTERNAL PROVIDER
```

Once the user has been created, you can assign roles as appropriate via the following TSQL command:

```
EXEC sp_addrolemember '<role>', '<alias@domain.com or="" alias@domain.onmicrosoft.com="">';
```

IMPORTANT: The dbmanager and loginmanager roles cannot be assigned to a user unless the user has been created on the Master. Said roles would then need to be assigned from the Master.

Classification

Root cause Tree - Connectivity/AAD Issue/AAD user Configuration

How good have you found this content?

🙂 🙁