Fails due to grant role using service principals

Last updated by | Marlon Jin | Apr 28, 2022 at 5:45 AM PDT

Contents

- Issue
- Analysis
- Conclusion

Issue

Customer connect to the database using Service Principal and then tried to grant an user to the azure_ad_user role, it will fail.

1. To use the service principal to connect to the database, you can follow the guidance here.

   ```
    az login --service-principal -u xx -p=xxx --tenant xxx  az account get-access-token --resource-type oss-
   rdbms  set pgpassword=<token obtained above>  psql "host=xxx.postgres.database.azure.com port=5432
   dbname=postgres user=aad_group@xxx"
   ```

2. After login successfully, we can reproduce the issue using the command below.

   ```
   SET aad_validate_oids_in_tenant = off;

   GRANT azure_ad_user to aad_user
   ```

   The error message is <must have admin option on role "azure_ad_user" and "an unexpected error occurred while trying to validate user". >

3. However, if he connect to the database using an individual AD user, the same step would work.

Analysis

1. Customer actually is trying to do use the step to map number AAD user to the PostgreSQL Role authenticating as SP.

   If customer is attempting to use the "GRANT azure_ad_user to <user Name>;" command as defined below in this documentation:

   These commands will not work if the AAD_Admin is a SP or MI, at least not now. A SP or MI AAD Admin does not have sufficient privileges to use these calls. That is By Design currently. Please note these statements are for special cases and not a general situation.

```
 *Migrating existing PostgreSQL users to Azure AD-based authentication*  *You can enable Azure AD authentication
for existing users. There are two cases to consider:*

 *Case 1: PostgreSQL username matches the Azure AD User Principal Name*  *In the unlikely case that your
existing users already match the Azure AD user names, you can grant the azure_ad_user role to them in order to
enable them for Azure AD authentication:*
```

SQL *GRANT azure_ad_user TO "existinguser@yourtenant.onmicrosoft.com";* *They will now be able to sign in with Azure AD credentials instead of using their previously configured PostgreSQL user password.*

Case 2: PostgreSQL username is different than the Azure AD User Principal Name *If a PostgreSQL user either does not exist in Azure AD or has a different username, you can use Azure AD groups to authenticate as this PostgreSQL user. You can migrate existing Azure Database for PostgreSQL users to Azure AD by creating an Azure AD group with a name that matches the PostgreSQL user, and then granting role azure_ad_user to the existing PostgreSQL user:*

SQL *GRANT azure_ad_user TO "DBReadUser";* *This assumes you have created a group "DBReadUser" in your Azure AD. Users belonging to that group will now be able to sign in to the database as this user.*

Conclusion

We can use this syntax to resolve the issue.

CREATE ROLE aad_user@domain.com WITH LOGIN PASSWORD 'CLIENT_ID' IN ROLE azure_ad_user;

This is documented here as syntax for managed identity but is applicable to user AAD objects as well

https://docs.microsoft.com/en-us/azure/postgresql/howto-connect-with-managed-identity#creating-a-postgresql-user-for-your-managed-identity

How good have you found this content?

🙂 🙁