**Postgres connection Using User Managed Identity**

These are the steps that we have followed :

(These are all in the Azure Environment).

1. create a Resource group .

2.create a virtual machine of ubuntu. And install postgres in that vm.

3. create a postgres flexible server Azure AD authentication enabled and add user having AD

account and set the Fire wall rules to allow to public access.

4. create a managed identity and assign it to the VM so that we can have the client id.

5. login to vm and try to connect to postgres using

psql"host= port=5432 dbname=postgres user=<server login name> sslmode=require".

6. now we have to create a role for the Azure AD admin but for that we need to generate a token using

1. az account get-access-token --resources https://ossrdbms-aad.database.windows.net -o json in the cloud shell and save the token
2. now use psql"host= port=5432 dbname=postgres user=<azure ad name> sslmode=require" in the VM and provide that token as
3. export PGPASSWORD=<access token>

7. SET aad\_validate\_oids\_in\_tenant = off;

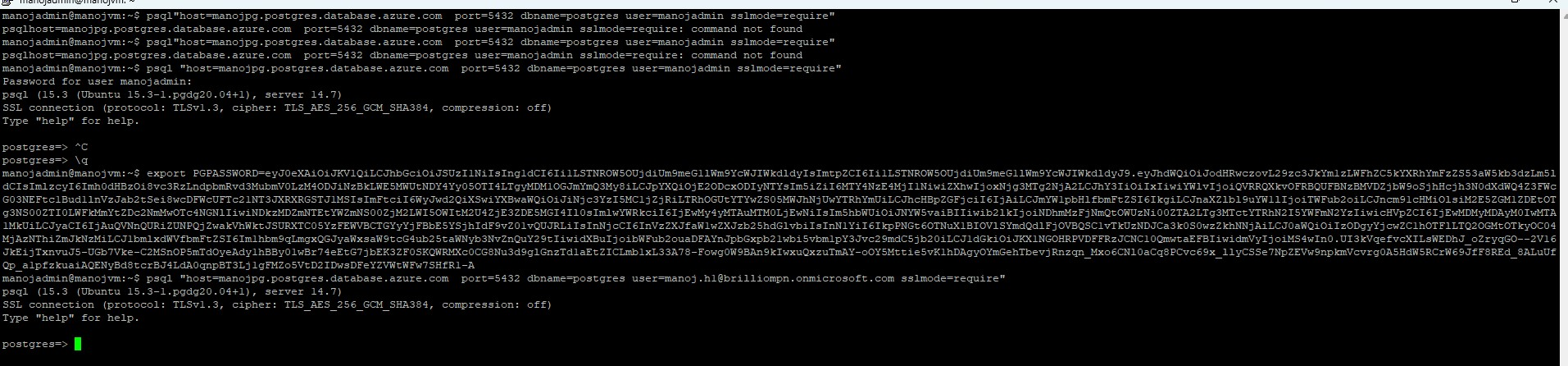
8. CREATE ROLE <managed identity name> WITH LOGIN PASSWORD "CLIENT ID in managed section of VM" IN ROLE azure\_ad\_user;

9.curl'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https%3A%2F%2Fmanagement.azure.com%2F' -H Metadata:true -s to get the token.

10.export PGPASSWORD=<access token that we got>

11. psql"host= port=5432 dbname=postgres user=<azure ad name> sslmode=require"

12. In case you want to remove the role DROP ROLE <managed identity name>.



A picture containing text, screenshot, font

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

