Using Service Principle as AAD User

Last updated by | Hamza Aqel | Mar 8, 2023 at 2:39 AM PST

Using Service Principle as AAD User

We had a current limitation in the implementation of AAD in Azure database for PostgreSQL that the AAD administrator has to be a user and not a service principle or the add user validation will not work . f their admin is a service principal, and they are adding individual users, there is a possible workaround if they are willing to add the user with their OID or appId explicitly. That is, they can do:

set aad_validate_oids_in_tenant = off;

and then:

create role myaaduser with login password 'aadOidorAppIdHere' in role azure_ad_user;

There are two downsides here:

The admin user has to provide the AAD OID because the PostgreSQL server does not look it up. You do this by using the syntax: "create role xxx with login password 'aadOidHere' in role azure_ad_user". For users, use the AAD user OID. For applications, use the AAD applicationId/clientId (NOT the service principal ID).

Because the PostgreSQL server also does not look up the object type, it makes an assumption that you are adding an individual (user or application, it doesn't matter). You cannot add an AAD group this way.

Why it’s not supported?

From a technical standpoint, what is happening here is:

Customer acquires access token to sign in to PostgreSQL server with resource=https://ossrdbms-aad.database.windows.net

Customer does "grant azure_ad_user to <role>"

PostgreSQL server acquires access token for AAD Graph API using "on behalf of" flow (OBO). The OBO flow takes the original access token and exchanges it for an access token with resource=https://graph.windows.net.

PostgreSQL server calls Graph API "on behalf of" the PostgreSQL AAD administrator to lookup PostgreSQL AAD role name in customer tenant to get OID and object type (User, Group, or Application). The assumption here is that the PostgreSQL AAD admin user has permissions in the customer tenant to validate the PostgreSQL AAD role name.

PostgreSQL server stores mapping of PostgreSQL AAD role to AAD User, Group, or Application OID.

The limitation occurs in step 3 where AAD OBO flow is only supported for AAD user, not AAD service principals. This is a limitation in AAD that will probably never be lifted.

This limitation can’t be lifted, on flexible servers there will be a different implementation where each server uses a Managed Identity to directly do the AAD user/group/application validation in the customer tenant. Because there is no OBO token flow, there is also no restriction on using service principals as the AAD admin user.

How good have you found this content?

🙂 🙁