Create AAD user FROM EXTERNAL PROVIDER - TSQL fails

Last updated by | Charlene Wang | Mar 22, 2021 at 1:07 AM PDT

Contents

This TSG applies for Azure SQL Database, Azure SQL Managed Instance, Azure Synapse Analytics

Issue

When the user is trying to execute a T-SQL to add an AAD user to connect to the DB, but the action fails with the following message:
--Msg 33130, Level 16, State 1, Line 2
--Principal 'user@aad.onmicrosoft.com' could not be found or this principal type is not supported.

Mitigation

Please make sure that the user you are trying to add is part of the AAD associated with the SQL Server you are trying this TSQL on. You can validate this by navigating to Azure Portal and verifying if the user exists in the same tenant.

Guest users in AAD

Currently, this operation(create user) is in public preview for guest users in the AAD. As part of this public preview, guest users can be created and connect directly to SQL Database, SQL Managed Instance, or Azure Synapse without the requirement of adding them to an Azure AD group first, and then creating a database user for that Azure AD group.

As part of this feature, you also have the ability to set the Azure AD guest user directly as an AD admin for the Azure SQL logical server. The existing functionality where the guest user can be part of an Azure AD group, and that group can then be set as the Azure AD admin for the Azure SQL logical server is not impacted. Guest users in the database that are a part of an Azure AD group are also not impacted by this change. (More information refer to: https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-guest-users)

Service Principals in AAD

Support for Azure Active Directory (Azure AD) user creation in Azure SQL Database (SQL DB) and Azure Synapse Analytics on behalf of Azure AD applications (service principals) are currently in public preview.

The T-SQL command CREATE USER [Azure_AD_Object] FROM EXTERNAL PROVIDER on behalf of an Azure AD application is now supported for SQL Database and Azure Synapse.

Please be careful about Troubleshooting and limitations for public preview

Classification

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

How good have you found this content?

🙂 🙁