Azure AD - DDL Extension for Create USER - Private preview

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:34 AM PDT

Contents

Issue

The customer is not able to create a new Azure Active Directory user because the username is non-unique. This issue may occur primarily for service principals as well as AAD groups (for AD synchronized with AAD)

Investigation/Analysis

The customer will receive the following error message when executing the command - CREATE USER <user_name> FROM EXTERNAL PROVIDER

Msg 33131, Level 16, State 1, Line 4 Principal 'myapp' has a duplicate display name. Make the display name unique in Azure Active Directory and execute this statement again.

Mitigation

DDL syntax extension – in yellow

```
CREATE USER [AAD_principal_name | group_name | user_name ]
    FROM EXTERNAL PROVIDER [WITH OBJECT_ID='ObjectID']
```

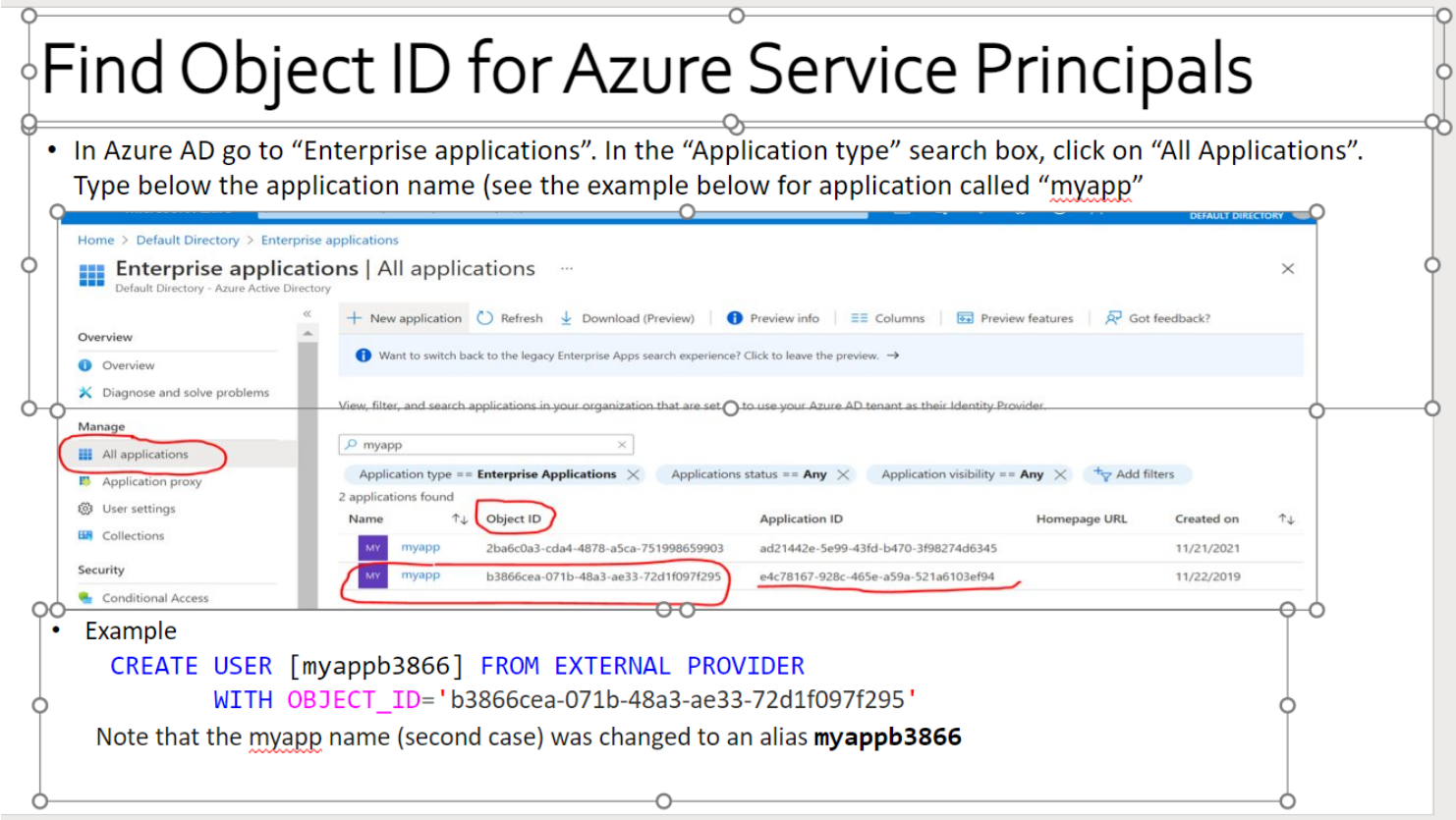
Arguments

```
WITH OBJECT_ID='ObjectID’
Specifies the Azure AD ObjectID. In case the Object_ID is specified the AAD_principal_name is not required
and a different  user_name (an alias)  can be provided. The user_name must be a unique name
in the   sys.database_principals.
```

Remarks

The specified ObjectID must exist in Azure AD where the Azure SQL resides

Double-check that the ObjectID in the AAD corresponds to the right AAD principal name



This option allows to create a user in Azure SQL that do not have to represent the Azure_Active_Directory_principal name.It is required in the case of creating AAD users in Azure SQL with AAD principal names that are not unique in AAD

Most of non-unique display names in Azure AD are related to service principles. In rare situations an Azure AD display name for group's name may not be unique as well. All Azure AD user display names are unique.

For service principals, the new user SID stored in the metadata can be converted back to Application ID and not to Object ID

Permissions

No new permissions are required.

RCA Template (optional)

N\A

Internal Information (optional)

This is currently in private preview and the remaining details will be published and informed accordingly. During the private preview, PG PM will be working with customers for onboarding.

Please contact SQLAADFeedback@microsoft.com for any further information.

Public Doc Reference (optional)

https://docs.microsoft.com/en-us/sql/t-sql/statements/create-user-transact-sql?view=azuresqldb-mi-current

Internal Reference (optional)

https://microsoft.sharepoint.com/:p:/r/teams/sqlsecurity/_layouts/15/Doc.aspx?sourcedoc={959A2EE3-F5EB-4F97-8C57-49213EB490BF}&file=CreateUserWithObjectID.CSS.presentation.pptx&wdLOR=cFF265BDC-DFB6-4DEF-8B84-9AA446C03541&action=edit&mobileredirect=true&share=IQHjLpqV6_WXT4xXSSE-tJC_AT3tYETxR15ELpL-AKa4FAM

Root Cause Classification

N\A

How good have you found this content?