AAD authentication for Guest(slash)External user account

Last updated by | Balaji Barmavat | Nov 30, 2020 at 11:20 PM PST

Contents

Issue

You were trying to connect to Azure SQL database using **aaa@companyxyz.com** and fails with the following error.

Msg 33130, Level 16, State 1, Line 1

Principal 'aaaa@companyxyz.com' could not be found or this principal type is not supported.

You have observed that only in-cloud accounts in AAD can connect, such as **John.Doe@companyxyzservices.onmicrosoft.com**;

any accounts **@companyxyz.com** have issue in making successful connection

Investigation/Analysis

Upon our checks from the backend, the account **John.Doe@companyxyz.com** is **Guest/External** User account in the directory (companyxyzservices.onmicrosoft.com)

When External user accounts are added on to your Azure Active Directory (companyxyzservices.onmicrosoft.com), despite having the same login name that derives from their source directory, they are stored in the target directory with a different UserPrincipalName (UPN). Consider the above example – the UPN in the source directory would be as follows:

aaa@companyxyz.com, but the UPN in AAD for the object would be:

John.Doe_companyxyz.com#EXT#@companyxyzservices.onmicrosoft.com

Fiddler trance analysis reported:

The client application (SQL MANAGEMENT STUDIO) tried accessing a resource which is protected by Azure AD (In your case it is a Azure SQL DB- https://database.windows.net/) using the <Active Directory – Universal > method.

Since it's an protected resource of AAD, the request has been redirected to Azure AD for authentication , so that the AAD can verify the user identity and provide an access token for the target resource (https://database.windows.net/), Wherein you have supplied the UPN of the user (John.Doe@companyxyz.com)

which is external to your Azure AD directory (B2B- Guest user), based on the user principal name input AAD has done a realm discovery on the user domain and redirected the user back to his identity provider for authentication which is a secure auth(idp) in your case (http://ssoidp.companyxyz.com) , the identity provider has successfully authenticated the user against the claims provider probably Active directory and issued a SAML token to Azure AD and Azure AD has transformed that token to a token (Access/ID Token) which could be recognized by the target resource (Azure SQL DB- https://database.windows.net/).

I see from the logs that AAD has issued the access token for the target resource (as pasted below)

Now it is an client application's (SQL MANAGEMENT STUDIO) responsibility to use the access token to be able to access/connect with target resource in question (Azure SQL DB), which I do not see happening from the logs.

ID_Token:


```
{"typ":"JWT","alg":"none"}

{
    "aud": "a94f9c62-97fe-4d19-b06d-472bed8d2bcf",
    "iss": "https://sts.windows.net/141f0f15-43fe-42df-b979-02251d5bc73c/",
    "iat": 1536945232,
    "nbf": 1536945232,
    "exp": 1536949132,
    "amr": [
        "pwd"
    ],
    "family_name": "Doe",
    "given_name": "John",
    "ipaddr": "13.66.221.120",
    "name": "John Doe",
    "oid": "40531648-4055-4875-8047-cf5a4776b4d0",
    "onprem_sid": "S-1-5-21-606747145-1060284298-839522115-178106",
    "sub": "0XFVHylgTRtqCqb2PILu_6VZxBmG_tj9u3hS8o4KBrE",
    "tid": "141f0f15-43fe-42df-b979-02251d5bc73c",
    "unique_name": "John.Doe@companyxyz.com",
    "upn": "John.Doe@companyxyz.com",
    "ver": "1.0"
}
```


Notice the application is SQL SSMS.

Mitigation

For such external user, it is not supported directly from TSQL create user.

Put external user into AAD group, Execute TSQL "create user [the AAD group containing external user] from external user"

Then try to login using John.Doe@companyxyz.com.

https://portal.microsofticm.com/imp/v3/incidents/details/83878819/home

Also:

Add B2B collaboration guest users without an invitation

https://docs.microsoft.com/en-us/azure/active-directory/b2b/add-user-without-invite

Classification

Root cause Tree - Security/User issue/error/Uncoded

How good have you found this content?