Unable to connect using an Azure AD User account

Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:30 AM PST

Unable to connect using an AAD

Contents

Issue

Issue connecting to Azure SQL Database usingActive Directory user account.

Mitigation

Obtain Fiddler traces

1. Download Fiddler from here https://www.telerik.com/download/fiddler

> **(*) Disclaimer: use of this tool is a recommendation to help troubleshoot and is not administered by Microsoft. Please use at your own risk.**

2. Install Fiddler and add a root certificate.

3. Setup a “Fiddler Trace” with “Decrypt HTTPS Traffic” option checked in [Tools->Options->HTTPS].

4. Launch SSMS

5. Login with an Azure AD credential

6. Stop capture in Fiddler traces

Debug Fiddler Trace?

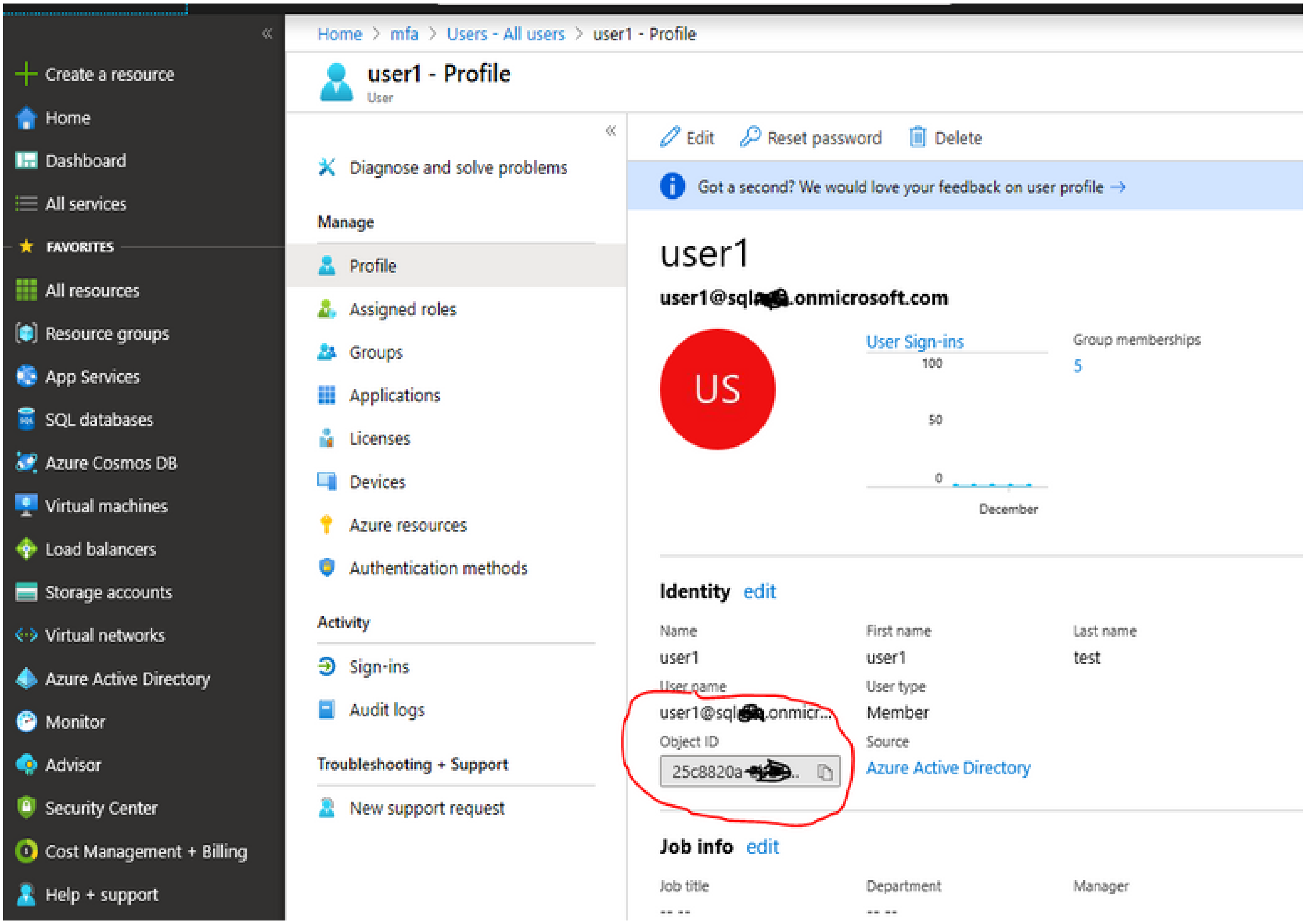
1. Open the Fiddler trace.
2. Look for a call to Host “**windows.net**” or “**login.microsoftonline.com**” in the left pane.
3. Select the frame and look to the right. The upper panel contains the request. You can expand the request by clicking on “**Raw**” and view the request packet being sent to Azure AD.
4. Look for the corresponding response value. The responses from Azure AD are usually very specific and will help guide the customer on what is missing in the authentication request (e.g. "error":"interaction_required","error_description: **AADSTS50079**. The user is required to use multi-factor authentication......).
5. If the Fiddler trace contains a “**seemingly legitimate**” access token, copy the token from the trace and debug it. Please note that a valid token could reveal user information and is a subject for the privacy compliance, therefore before debugging it wait for the token to expire. If needed, before sharing this token with support team to continue working on the problem, make sure that the token does not contain relevant user information.

Debug Azure AD Token

1. Copy the Azure AD access token.
2. Open a browser of your choice and go to https://jwt.io/
   > **(*) Disclaimer: this is only a recommendation and opening this link is not required nor owned by Microsoft.**
3. Paste the token in the following box:
4. This will display ObjectID and groups information.
   1. Use ObjectID if a user is individually added to the server, or
   2. Use Guids in groups if a user is logged in as a member of the group.

Obtain an ObjectID of the user or group trying to login.

This information can be obtained from the Azure AD portal for a user or group
(see a screenshot below, indicating in red an Azure AD ObjectID: 25c8820a-xxxx-xxxx-xxxx-fe2fd9**14e144** for user1@sqlxxx.onmicrosoft.com)



user1 - Profile

User

Got a second? We would love your feedback on user profile →

user1

user1@sql[redacted].onmicrosoft.com

Identity edit

Name	First name	Last name
user1	user1	test

User name: user1@sql[redacted].onmicr...

User type: Member

Object ID: 25c8820a-[redacted]..

Source: Azure Active Directory

Job info edit

Job title	Department	Manager
-- --	-- --	

Obtain a SID from Azure SQL DB

Login to a database and execute a SELECT statement from sys.database_principals to find the right SID for a given

Azure AD user or a group.

Using the example above for Azure AD user1@sqlxxx.onmicrosoft.com, the following SID is derived from the below SELECT statement

```
select name, type, type_desc, SID from sys.database_principals where name='user1@sqlxxx.onmicrosoft.com'
```

Output

name	type	type_desc	SID
user1@sqlxxx.onmicrosoft.com	E	EXTERNAL_USER	0x0XXXXXXXXXFE2FD9**14E144**

Compare the ObjectID and SID

The last six digits for these two should match. If not, there’s is a mismatch between a user registered in Azure AD and an Azure AD user created in SQL DB. This mismatch has to be resolved.

Based on the example above for user1@sqlxxx.onmicrosoft.com, the last 6 digits for the **ObjectID** in Azure AD, and the last six digits for the **SID** match and represent the same user (see the 6 digits **14E144** indicated in **BOLD**).

Public Doc Reference

https://techcommunity.microsoft.com/t5/Azure-SQL-Database/Troubleshooting-problems-related-to-Azure-AD-authentication-with/ba-p/1062991
https://azure.microsoft.com/en-us/blog/sql-azure-and-session-tracing-id/

Classification

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

How good have you found this content?

🙂 🙁