

AAD Login failure - Error -122

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

AAD Login Failure

Contents

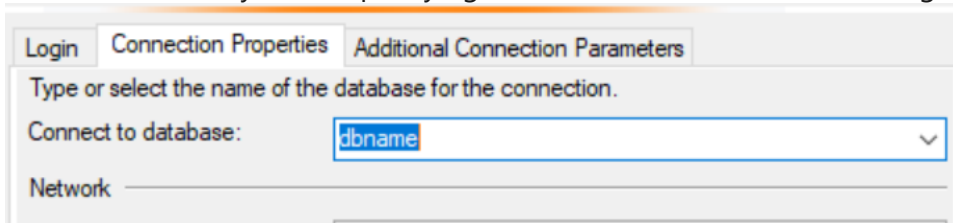
- [AAD Login Failure](#)
 - [Issue](#)
 - [Mitigation](#)
 - [How to debug AAD Token](#)
 - [Classification](#)

Issue

Customer is trying to use SSMS or other SQL tools to connect to Azure SQL DB and are getting the error message "NT AUTHORITY\ANONYMOUS LOGON" message.

Mitigation

1. Please make sure you are specifying a database name in the SSMS Login UI



2. Trying to Login to SQL with AAD user:

Please make sure the user that you are trying to connect with a user who has access to the DB via one of the following methods is added to the DB by using `CREATE USER <USERNAME> FROM EXTERNAL PROVIDER` or is AAD Admin or part of the AAD Admin group set up for the SQL Server (AAD admin will have db_owner on all databases)

Also ensure that the user does not have any DENY CONNECT permissions

Here is how to verify this using DMVs

First check who is the AAD admin from master

```
--master
select name,sid,create_date from sys.database_principals where type='X'
```

in my case this returns

name	sid	create_date
rohitna@microsoft.com	0xE7D524FADC13114BA9BBE170E6BAF626	2016-12-14 20:00:58.367

3. Use this query to look at permissions for individual users at each database


```
SELECT pr.principal_id, pr.name, pr.sid, pr.type_desc,
       pr.authentication_type_desc, pe.state_desc, pe.permission_name
FROM sys.database_principals AS pr
JOIN sys.database_permissions AS pe
      ON pe.grantee_principal_id = pr.principal_id
where pr.type='E' -- Filter for external users
```

Note :- Being a subscription admin does not guarantee that you will have access to the DB. You need to grant access to the user only by the above options. Trying to Login to SQL with imported or guest users in AAD using Universal Authentication: (imported users are users that belong to another AAD and have been invited by the AAD Admin of the tenant associated with the SQL DB) If user is trying to use Universal Authentication to login, they need to specify the TenantID in Connection Properties. (See fig. below). For a guest, you will want to ensure that the TenantID/Domain is the one the guest is apart and not the source of the guest account itself.


4. Trying to Login with MSA(@hotmail.com, @outlok.com etc) user: AAD Integrated/AAD Password Login will fail for MSA users because they need to go through an Interactive login workflow. Please use Universal Authentication for connecting via MSA Users. Also, please make sure you specify the AAD Tenant ID in the Connection Properties.



The screenshot shows the 'SQL Server' 'Connect to Server' dialog box. The 'Connection Properties' tab is active. The 'Connect to database' dropdown is set to 'db1test2'. Under the 'Connection' section, the 'AD domain name or tenant ID' checkbox is checked and circled in red. The text 'febtest.onmicrosoft.com' is entered in the field next to it. Other options visible include 'Encrypt connection' (checked), 'Trust server certificate' (unchecked), and 'Use custom column mapping' (unchecked). The 'Reset All' button is also visible.

5. User is MFA enforced: Please make sure you only use Universal authentication if you are a MFA enabled AAD user, because only this option provides an interactive login protocol.



6. Please make sure that the AAD Admin is correctly setup and is part of the AAD associated with your subscription. AAD Admin for SQL Server does not automatically get updated if you switch out AAD's. You will have to reset your SQL Server Admin if you migrate from 1 AAD to another. This can also cause login failures.
7. If AAD integrated or password are not working, try Universal Authentication in SSMS or trying this code sample (<https://blogs.msdn.microsoft.com/sqlsecurity/2017/08/18/token-based-authentication-including-multi-factor-auth-mfa-for-azure-sql-db-using-azure-active-directory-ad/>  - Please plug in parameters for your application)
8. If the pop-up UI for universal Authentication contains errors – This means probably your machine cannot talk to AAD. Make sure your machine can talk to AAD. You can check this via small telnet command:

```
telnet login.microsoftonline.com 443
```
9. If you can enter your credentials in the pop-up but do not get a token back: This indicates the issue is with AAD not being able to authenticate your credentials. You might want to check your credentials or whether you are a valid user in AAD or reach out to AAD team for support.
10. If you can get a valid token from the service, proceed to next step.

Validate your AAD Token: You can grab the token issued by AAD (see how to grab it in fiddler trace Fiddler trace) and validate
11. if the token issued is legitimate. You can paste your token on <http://jwt.io>  which parses the token. If the token cannot be parsed here, you have probably received a bad token and need to contact AAD support team or fix your code which acquires the token. You can ignore signature validation errors on this site.

Look for the following verifications:
12. Token "aud" is a legitimate url. "aud": <https://database.windows.net/> 
13. Token "sts" is a legitimate url and tenant: "sts": <https://sts.windows.net/72f888ff-77f1-41af-91ab-2d7cd011db47/> 
14. Object Id should not be empty. If oid is absent, please contact AAD team because something is wrong with the token here. Oid should also be a valid GUID. "oid": "5cd2c5dc-0010-0000-cccc-aaacaccab000"
15. Token should contain a valid tenantId. This should be a valid GUID too. "tid": "72f888ff-77f1-41af-91ab-2d7cd011db47",

How to debug AAD Token

16. Grab the AAD issued accesstoken.
17. Open a browser of your choice and go to <https://jwt.io/>  or <http://jwt.ms/> 

18. Paste the token in the following box

Encoded

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjE5OTY0OTUyMjIyLjJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ

Once you paste the token, the right side automatically parses the token. Validate the properties of the token (like expiration time, tenantId, person who this token was issued to). To get precise information on what could potentially be wrong with the token, look for the information in Kusto table MonFedAuthTicketService (details mentioned above)

Classification

Root cause Tree

Connectivity/AAD Issue/AAD user Configuration

How good have you found this content?

