Error 18456, State 15 - AAD Login failure and AAD Administrative units

Last updated by | Vitor Tomaz | Oct 18, 2022 at 3:49 AM PDT

Contents

Issue

Customer fails to login to Azure SQL with AAD user

```
===================================
Cannot connect to weeu-s03-tst-sqlsv-01.database.windows.net.
===================================
Login failed for user 'user@domain.net'. (.Net SqlClient Data Provider)
------------------------------
Server Name: xxxxxx.tr605.westeurope1-a.worker.database.windows.net,11019
Error Number: 18456
Severity: 14
State: 1
Line Number: 65536
------------------------------
Program Location:
   at System.Data.SqlClient.SqlInternalConnectionTds..ctor(DbConnectionPoolIdentity identity, SqlConnectionStr
   at System.Data.SqlClient.SqlConnectionFactory.CreateConnection(DbConnectionOptions options, DbConnectionPoo
   at System.Data.ProviderBase.DbConnectionFactory.CreateNonPooledConnection(DbConnection owningConnection, Db
```

Troubleshoot

Using Azure support center

We don't have insight for this issue in Azure support center. Please follow below steps to further identify this issue.

Using Kusto

MonLogin will show error 18456 / 15

```
let ServerName = "ServerName";
MonLogin
| where TIMESTAMP >= ago(1d)
| where logical_server_name =~ ServerName
| where event == "process_login_finish"
| where is_success == 0
| extend AADUser = iif( fedauth_adal_workflow > 0 or fedauth_library_type > 0, "AAD" , "SQL")
| extend ProxyOrRedirect = iif( result == "e_crContinueSameState", "Proxy" , "Redirect")
| extend fedauth_library_type_desc =
case (
fedauth_library_type == 0, "SQL Auth",
fedauth_library_type == 2, "Token Based",
fedauth_library_type == 3 and fedauth_adal_workflow == 1, "AAD Password",
fedauth_library_type == 3 and fedauth_adal_workflow == 2, "AAD Integrated",
fedauth_library_type == 3 and fedauth_adal_workflow == 3, "AAD Universal MFA",
fedauth_library_type == 4, "Windows Auth",
strcat(tostring(fedauth_library_type) , "-" , tostring(fedauth_adal_workflow))
)
| project PreciseTimeStamp, logical_server_name, database_name, MachineName , package, event, is_success, is_u
        application_name, driver_name, ProxyOrRedirect, AADUser, fedauth_library_type_desc, total_time_ms, mes
```

MonFedAuthTicketService shows "fedauth_ticket_service_success"

```
MonFedAuthTicketService
| where TIMESTAMP >= ago(1d)
| where sql_connection_id =~ "1F2E08D8-3748-4510-A8E1-A430ADE88166"
```

MonAzureActivDirService will show error_state "46" = AADGraphGroupLookupFailed. If you see other error_state, please refer to MonAzureActivDirService

```
let ServerName = "ServerName";
MonAzureActivDirService
| where TIMESTAMP >= ago(1d)
| where LogicalServerName =~ ServerName
| project sql_connection_id , event, connection_type,operation_type, error_code , error_state , error_message
```

When client tries to authenticate to SQL using AAD and have more than 150/200 groups the auth token will not list the group names and will use Graph API (An URL that SQL will query to list all groups that is part of)

https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-saml-tokens "If the number of groups the user is in goes over a limit (150 for SAML, 200 for JWT) then an overage claim will be added the claim sources pointing at the Graph endpoint containing the list of groups for the user."

Token Sample

```
"_claim_names": {
  "groups": "src1"
},

"_claim_sources": {
  "src1": {
    "endpoint": "https://graph.windows.net/a6b169f1-592b-4329-8f33-8db8903003c7/users/6d8ab668-0d7e-47f0-aa1
```


The AAD engineer identified that it was failing to use API "ListMemberAdministrativeUnits"

RCA Template

Root Cause Our first party SQL Service is still unable to list members of Administrative Unit (a preview feature of Azure AD).

Mitigation Initial workaround was to decrease the number of groups the user is member of, so SQL does not need to perform group lookup. Final solution is to remove affected users from Administrative Unit so SQL service is able to perform group lookup properly.

Additional Information For more information, you can refer to https://docs.microsoft.com/en-us/azure/active-directory/develop/reference-saml-tokens https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-administrative-units

Internal Reference (don't share with customer)

CASE 120032624001681 https://portal.microsofticm.com/imp/v3/incidents/details/183092893/home

Classification

Cases resolved by this TSG should be coded to the following root cause:
Root Cause: Azure SQL DB v2\Connectivity\Login Errors\Other

How good have you found this content?