Azure Active Directory integrated authentication

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

Contents

Issue

Azure SQL team gets several cases related to Azure Active Directory Integrated Authentication. Below are some sanity checks to help identify the issue in a more timely fashion before we reach out to Azure Active Directory team for a collaboration.

Investigation/Analysis

1. Confirm if customer is connecting from a federated domain (e.g. ADFS), or a managed domain that is configured for seamless single sign-on (SSSO) for pass-through (PTA) and password hash authentication (PHA). Those are the only use cases which are supported for integrated authentication.

2. Collect a Fiddler trace to see if the client application is receiving an Access Token

3. Confirm the ADAL (Azure Active Directory Authentication Library for SQL Server) version that the customer is using to attempt a connection. To check the version used by the client tool/application the following PowerShell cmdlets can be used when executed from the client machine attempting the connection

```
$keys = "SOFTWARE\Microsoft\MSADALSQL", "SOFTWARE\WOW6432Node\Microsoft\MSADALSQL"
foreach ($key in $keys) {
    if (Test-Path -Path "HKLM:\$key") {
        $file = Get-ItemProperty -Path "HKLM:\$key" | Select-Object -ExpandProperty TargetDir
        if (Test-Path -Path $file) {
            Get-Item -Path $file | Select-Object -Property Name -ExpandProperty VersionInfo
        }
        else {
            Write-Warning -Message "File $file doesn't exist"
        }
    }
    else {
        Write-Warning -Message "Registry key HKLM:\$key doesn't exist"
    }
}
```

The script above shows the version for the x64 and x86 versions.

Mitigation

If the output of the property "FileName" returned by the PowerShell cmdlet above is ADALSQL.dll (legacy library) then proceed to check if the the latest library ADAL.dll is installed on the customer's computer.

The location of ADAL.dll is C:\Windows\SysWOW64\adal.dll for x86 (32 bit applications) and C:\Windows\System32\adal.dll for x64 (64 bit applications)

If ADAL.dll is not installed on the client computer check how to install ADAL

If ADAL.dll is installed but the registry key is pointing to ADALSQL.dll you can ask customer to manually change the registry value to point to ADAL.dll instead.

Open the registry (regedit.exe) and change the value of the key **TargetDir** to *C:\Windows\SysWOW64\adal.dll* on the location *HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSADALSQL* for 32 bit applications and **TargetDir** to *C:\Windows\System32\adal.dll* on the location *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSADALSQL* for 64 bit applications.

Note: A very common error observed in several cases is "AdalException: Integrated Windows authentication supported only in federation flow." This error mainly happens when the client application is loading the legacy dll of ADAL

If the issue is not related to ADAL and customer is not able to connect from a federated domain or a managed domain configured for SSSO open a collaboration with the appropriate team (ADFS or AAD) as this would be an issue outside the scope of Azure SQL DB/MI.

Public Doc Reference

Active Directory integrated authentication

Azure Active Directory Seamless Single Sign-On

Manage and customize Active Directory Federation Services by using Azure AD Connect

Internal Reference

Migrate applications to the Microsoft Authentication Library (MSAL)

Root Cause Classification

Root cause Tree - Connectivity/AAD Issue/Other Client Configuration

How good have you found this content?

🙂 🙁