AAD - FAQs

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

Frequently asked Questions - AAD

[Question] What about SPN's for Azure SQL DB

[Inputs] In Azure Active Directory there is a tenant called as infrastructure tenant, They have exposed first party service principle via this tenant. Azure SQL DB registers to this tenant as a whole service. During the registration the SPN is registered for the whole Azue DB Service. Once this registration is complete the SPN's gets mirrored to all Customer tenants. So there is no concept of dropping and creating back the SPN every time any SQL Server Service gets restarted.

[Question] How does AAD and On-Premise AD work with each other

[Inputs] AD DirSync implementation along with ADFS will be setup, Where in except the password all other metadata about the objects will be synchronized continuously between the two. During this setup there is an Exchange of certificates that happen. Any communication between the 2 is encrypted and decrypted using the certificates that got exchanged during the setup. This is how signature validation happens to understand that the Token is from a reliable party.

[Question] How does Azure SQL DB validate the JWT received from the client that Azure AD provided.

[Inputs] There is a huge validation process in place , Look at the above diagram about JWT validation to get more details. Before this validation can start the JWT is encrypted and Azure SQL DB will have a public key provided by AAD (This is a common key across all tenants). Azure SQL DB caches this Public key and once its receives a JWT it uses this Public key to decrypt the JWT and then follows up with the validation process. In case if the cached key is invalid it once again requests a valid key and proceeds ahead.

[Question] What is the easiest way to understand if i have to start troubleshooting at Azure SQL DB Layer or Client Side.

[Inputs] If customer is reporting an error just look at the error message , if the Error Number and State is 0 that means this error is not raised by Azure SQL DB Engine and this will make it clear that it’s a client side error.

[Question] How does sp_reset_connection impact the performance

[Inputs] During sp_reset_connection --> The TDS REST Bit is set --> This enforces the login structure to be refreshed but the structure is kept intact --> For the next login attempt the token that is present in SQL Address space is reused and the security information is re-populated into the login structure --> in case the token has expired the connection will be closed and the connection is terminated.

There is no token renewal concept present in the feature today , A retry attempt for connection has to be made. As per the connectivity team's recommendations we encourage customers to close and open a new connection instead providing feature for re-using the same connection for this reason renewal has not been implemented.

[Question] What about Token Expiration

[Inputs] Today in Azure SQL DB the JWT token received is only valid for 1hr , If a connection attempt is made after the token has expired the connection attempt would fail. The customer needs to implement retry logic to connect again.

[Question] How does this feature impact the performance during login

[Inputs] As by this time you understand the different layers that are being involved apart from traditional SQL server authentication , For sure there will be certain delay's when compared against the SQL server authentication process. This feature is being released to enhance customer with central Credential management capabilities and not targeted towards providing similar performance experience similar to SQL Server authentication.

How good have you found this content?

☺ ☹