PostgreSQL AAD connectivity

Last updated by | Hamza Aqel | Mar 8, 2023 at 2:39 AM PST

If the server is General Purpose or Memory Optimized edition first by checking the MonLogin table to determine if there is an AAD error state, and what that state indicates:
Use a query similar to this:

```
MonLogin
| where logical_server_name == "serverName"
| where AppTypeName == "Worker.PAL.PG"
| where event == "process_login_finish"
| where is_success == false
| project originalEventTimestamp, ClusterName, NodeName, event, connection_id, application_name, result, error, ['state']
```

Check especially for the following error states:

- 7 or 90 which could mean that the user does not exist in the DB
- 91 which indicates that AAD is not configured on the server
- 108 or 112 which indicate that the access token is expired
- 111 which indicates that the access token is corrupted, perhaps due to embedded newlines, truncation or other

Error	State	reason	Action
18456	90	RLF_STATE_AAD_AUTH_FAILED	AAD authentication failed (general). Notify Po
18456	91	RLF_STATE_AAD_TENANT_NOT_SET	AAD tenant not set--indicates that AAD adm
18456	92	RLF_STATE_AAD_ADMIN_NOT_SET	AAD admin not set--indicates that AAD admi
18456	93	RLF_STATE_AAD_MFA_ENFORCEMENT	Customer attempted to login with a valid AA authentication, and multi-factor authenticatic should acquire another access token, logging authentication, etc.) rather than simply AAD u
18456	94	RLF_STATE_AAD_AUTH_BUF_OVERRUN	Internal error. Report to PostgreSQL DRI and
18456	95	RLF_STATE_AAD_TOKEN_TOO_LONG	Customer attempted to login with an access length of 16KB. AAD should never issue an ac assign to PostgreSQL DRI and notify OrcasAA needs to be increased.
18456	96	RLF_STATE_AAD_MAPPING_FILE_ERR	Internal error. Report to PostgreSQL DRI and
18456	101	AAD_AUTH_NO_MEMORY	Server is out of memory
18456	103	AAD_AUTH_CANNOT_FETCH_FEDERATION_METADATA	Error fetching federation metadata to acquire transient, then it is okay. If it occurs repeated and should be reported to PostgreSQL DRI ar
18456	108	AAD_AUTH_EXPIRED	Customer attempted to login with an expired hour. Customer should acquire a new access
18456	111	AAD_AUTH_DECODE_FAILED	Customer attempted to login with a malform customer made errors attempting to copy/pa entire token, and that the pasted token does or whitespace
18456	112	AAD_AUTH_BAD_SIGNATURE	Customer attempted to login with an access came from AAD, then this can happen if the t up to one hour. Customer should acquire a n
18456	113	AAD_AUTH_BAD_HEADER	Customer attempted to login with an access information. If the access token came from A
18456	114	AAD_AUTH_MISSING_OBJECTID	Customer attempted to login with an access information. If the access token came from A
18456	115	AAD_AUTH_MISSING_ISSUER	Customer attempted to login with an access information. If the access token came from A
18456	116	AAD_AUTH_BAD_ISSUER	Customer attempted to login with an access configured for the database server. Check AA tenant of the AAD admin user set on the data
18456	117	AAD_AUTH_MISSING_AUDIENCE	Customer attempted to login with an access information. If the access token came from A
18456	118	AAD_AUTH_BAD_AUDIENCE	Customer attempted to login with an access "ossrdbms-aad". Check to make sure that the aad" resource URI in the correct cloud, and n
18456	121	AAD_AUTH_ALG_NOT_ALLOWED	Customer attempted to login with an access signature algorithm. (AAD for Orcas only sup If the access token came from AAD, then not
18456	126	AAD_AUTH_NOT_VALID_YET	Customer attempted to login with an access from AAD, this is highly unlikely. Please notify
18456	127	AAD_AUTH_CANNOT_FETCH_TOKEN	Database server could not authenticate with user. Check for sandbox logs containing "[AA in incident. If error does not indicate transien
18456	134	AAD_AUTH_CANNOT_FETCH_GRAPH_DATA	Database server could not fetch group inforn logs containing "[AADAuthProvider] HTTP ba not indicate transient failure, notify PostgreS(
18456	100+	Other AAD errors	Any other error is probably an internal error i Please notify PostgreSQL DRI and OrcasAAD.

If the issue is that the tenant is not set (91), confirm that AAD is configured on the server by checking the CMS elastic_server_external_admins table for the server in the adhoccmsquery XTS view, or other similar view such as CMS browser:

Is AAD Enabled?

SELECT s.name, a.state, a.tenant_id, a.external_admin_login_name, a.external_admin_login_sid, is_admin_persisted from
dbo.elastic_server_external_admins a
inner join dbo.elastic_servers s
on s.elastic_server_id = a.elastic_server_id
where s.name = 'serverName'

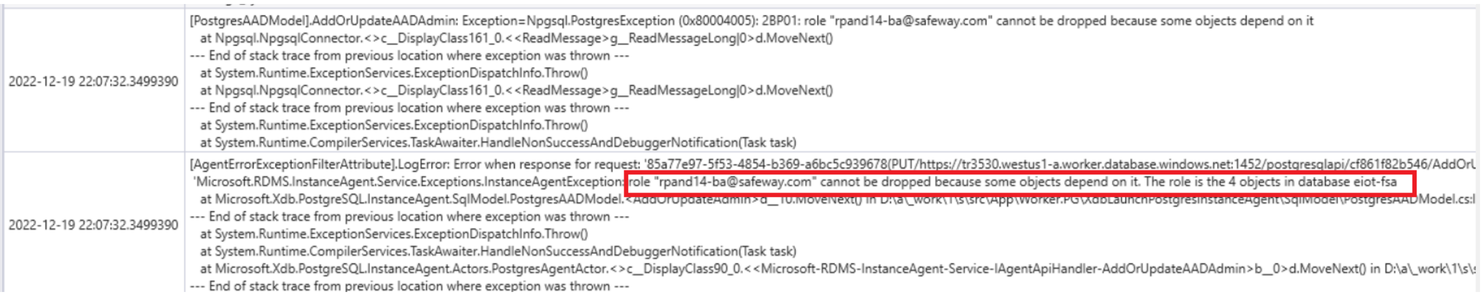
Query results will indicate if AAD is configured (row returned in Ready state with is_admin_persisted == true), along with the tenant ID, PostgreSQL user name, and AAD SID (either user OID or group OID from the AAD tenant).

If a customer is getting errors while attempting to create AAD users in their AAD-enabled PostgreSQL server, the first step is to look at the client error message.

If it says that an unexpected error occurred, then look at sandbox logs to see if there is an error message from AAD:

```
let pg_server_name = "pgservername";
let begin_time = ago(1d);
let finish_time = now();
MonRdmsInstanceAgent
| where LogicalServerName == pg_server_name
| where originalEventTimestamp > begin_time
| where originalEventTimestamp < finish_time
| where message_systemmetadata contains "PostgresAADModel"
| project originalEventTimestamp, process_id, message_systemmetadata
```

We can see the below error message:



```
2022-12-19 22:07:32.3499390  [PostgresAADModel].AddOrUpdateAADAdmin: Exception=Npgsql.PostgresException (0x80004005): 2BP01: role "rpand14-ba@safeway.com" cannot be dropped because some objects depend on it
                                at Npgsql.NpgsqlConnector.<>c__DisplayClass161_0.<<ReadMessage>g__ReadMessageLong|0>d.MoveNext()
                             --- End of stack trace from previous location where exception was thrown ---
                                at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
                                at Npgsql.NpgsqlConnector.<>c__DisplayClass161_0.<<ReadMessage>g__ReadMessageLong|0>d.MoveNext()
                             --- End of stack trace from previous location where exception was thrown ---
                                at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
                                at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
2022-12-19 22:07:32.3499390  [AgentErrorExceptionFilterAttribute].LogError: Error when response for request: '85a77e97-5f53-4854-b369-a6bc5c939678(PUT/https://tr3530.westus1-a.worker.database.windows.net:1452/postgresqlapi/cf861f82b546/AddOrU
                              'Microsoft.RDMS.InstanceAgent.Service.Exceptions.InstanceAgentException: role "rpand14-ba@safeway.com" cannot be dropped because some objects depend on it. The role is the 4 objects in database eiot-fsa
                                at Microsoft.Xdb.PostgreSQL.InstanceAgent.SqlModel.PostgresAADModel.<AddOrUpdateAdmin>d__10.MoveNext() in D:\a\_work\1\s\src\App\Worker.PG\XdbLaunchPostgresInstanceAgent\SqlModel\PostgresAADModel.cs:l
                             --- End of stack trace from previous location where exception was thrown ---
                                at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
                                at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
                                at Microsoft.Xdb.PostgreSQL.InstanceAgent.Actors.PostgresAgentActor.<>c__DisplayClass90_0.<<Microsoft-RDMS-InstanceAgent-Service-IAgentApiHandler-AddOrUpdateAADAdmin>b__0>d.MoveNext() in D:\a\_work\1\s\s
                             --- End of stack trace from previous location where exception was thrown ---
```

and refer to TSG Can’t remove Azure Active directory admin to remove these dependencies from the customer side.

If the error says something about an access token could not be acquired on behalf of a service principal, then the error is likely that the customer has signed in using an application token (not AAD user) as the server AAD admin. This is not supported because AAD cannot acquire tokens on behalf of a service principal.

The workaround for the above issue is for the customer to disable OID validation, and perform the user management operation specifying the OID themselves (rather than having AAD look up the OID). For AAD users or applications:

- set aad_validate_oids_in_tenant = off;
- create role "aadUserOrAppRole" with login password '<aadOidInTenant>' in role azure_ad_user;

For AAD groups:

- set aad_validate_oids_in_tenant = off;
- create role "aadGroupRole" with login password 'G<aadOidInTenant>' in role azure_ad_user;

Note that the "G" prefix is only needed when aad_validate_oids_in_tenant is off. Otherwise, the server will look up the OID in AAD, and can determine whether it is a group or not.

If the error is not something that occurred in AAD itself, then it might help to see all AAD log messages from the server:

```
MonRdmsPgSqlSandbox
| where LogicalServerName == "serverName"
| where text contains "[AAD"
| project originalEventTimestamp, ClusterName, NodeName, text
```

For errors other than BadRequest, the log will still show the HTTP error code. "NotFound (404)" indicates a user error, while "InternalError (5xx)" indicates an outage in AAD itself.for more details about how to configure AAD in Azure Database for PostgreSQL please refer to our documentation