Connectivity Login Troubleshoot - Single PG Server including AAD

Last updated by | Hamza Aqel | Feb 2, 2022 at 5:34 AM PST

Step 1

The below query will give the error and state for the specific server over the last two hours

```
MonLogin
    | where TIMESTAMP >= ago(2h)
    | where AppTypeName == "Gateway.PG"
    | where SourceMoniker contains "Prod"
    | where event == "process_login_finish" and error != 17830
    | where logical_server_name == "<your_logical_server_name>"
    | extend outcome = iff(is_success == 1, "Success", iff(is_user_error == 1, "User Error", "System Error"))
    | project PreciseTimeStamp, ClusterName, logical_server_name, error, ['state']
, outcome, total_login_time_ms , total_time_ms, SourceMoniker
```

Following are the general error and states that are encountered for PG

AppName	error	state	state name	comments
GW	18456	20	GW_FAIL_CONNECT_TO_POSTGRES	backend is not available
	18456	4	DbUnavailableWinFabLookupFailure	the server is not registered in Winfab. This can simply indicate that the customer has specified the wrong "@server" suffix on the user name in the connection string, or that the server has been deleted or has not yet been created.
	18456	100	SSLNegotiationFailed	server has SSL enforced, but ssl is not specified. This is also the default failure if a failure occurs during the accept phase on the backend.
	18456	101	SSLSecureRedirectFailed	redirected connection does not have ssl enforced
	18456	121	GW_FAIL_SSL_WITH_HOST	SSL handshake from gateway to host failed
	18456	122	VNET_VALIDATION_FAILED	a ipv6 connection failed because of vnet
	40613	16	DbUnavailableProxyConnectionToBackendFailed	gateway cannot start proxy connection to host
Host	40613	12	DbUnavailableFailedToPrepareDuplicatedData	socket duplication failed
Worker	18456	1	RLF_STATE_OUT_OF_MEMORY	Database server is out of memory
	18456	2	RLF_STATE_COULD_NOT_FORK	Cannot fork connection worker--typically due to out of memory
	18456	3	RLF_STATE_TOO_MANY_CONNECTIONS	Server has reached connection limit
	18456	4	RLF_STATE_DB_IN_SHUTDOWN	Server is shutting down--This error occurs if any connection is attempted while the database is shutting down, and it does not necessarily indicate a problem
	18456	5	RLF_STATE_DB_IN_STARTUP	Server is starting up--This error is very common when Instance Agent is connecting to a database that is just starting or restarting, and does not necessarily indicate a problem

	18456	6	RLF_STATE_DB_IN_RECOVERY	Server is performing database recovery--This error can occur during a restart
	18456	7	RLF_STATE_AUTH_FAILED	Authentication failed--user provided a bad user or password
	18456	8	RLF_STATE_FIREWALL_BLOCKED	Firewall blocked--check client IP and firewall rules to see if there is a problem
	18456	9	RLF_STATE_NO_SUCH_DATABASE	Connection parameters specified a database that does not exist on the server
	18456	10	RLF_STATE_BAD_CLIENT_CERT	Cert auth failed because client provided a bad certificate. Azure Sterling does not support cert auth for end users, and this could only happen for Instance Agent or replication. If it does happen, it indicates a problem with how the service has configured the server, and should be forwarded to PostgreSQL DRI
	18456	11	RLF_STATE_CONNECTION_THROTTLE	Connects are throttled due to too many bad password errors
	18456	90	RLF_STATE_AAD_AUTH_FAILED	AAD authentication failed (general). Notify PostgreSQL DRI and OrcasAAD
	18456	91	RLF_STATE_AAD_TENANT_NOT_SET	AAD tenant not set--indicates that AAD admin is not set for the database
	18456	92	RLF_STATE_AAD_ADMIN_NOT_SET	AAD admin not set--indicates that AAD admin is not set for the database
	18456	93	RLF_STATE_AAD_MFA_ENFORCEMENT	Customer attempted to login with a valid AAD access token that does not indicate multi-factor authentication, and multi-factor authentication is enforced for the PostgreSQL user. Customer should acquire another access token, logging in using multiple factors (Windows Hello, phone authentication, etc.) rather than simply AAD user and password.

	18456	94	RLF_STATE_AAD_AUTH_BUF_OVERRUN	Internal error. Report to PostgreSQL DRI and notify OrcasAAD.
	18456	95	RLF_STATE_AAD_TOKEN_TOO_LONG	Customer attempted to login with an access token longer than the current maximum allowed length of 16KB. AAD should never issue an access token longer than 16KB. If this occurs, please assign to PostgreSQL DRI and notify OrcasAAD to evaluate whether the maximum allowed length needs to be increased.
	18456	96	RLF_STATE_AAD_MAPPING_FILE_ERR	Internal error. Report to PostgreSQL DRI and notify OrcasAAD.
	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 signing certificates from AAD. If this error is transient, then it is okay. If it occurs repeatedly, it can indicate a problem with the AAD service, and should be reported to PostgreSQL DRI and OrcasAAD.
	18456	108	AAD_AUTH_EXPIRED	Customer attempted to login with an expired access token. Access tokens are good for up to one hour. Customer should acquire a new access token.
	18456	111	AAD_AUTH_DECODE_FAILED	Customer attempted to login with a malformed access token. We have seen this when the customer made errors attempting to copy/paste the token. Verify that the customer pasted the entire token, and that the pasted token does not contain leading, trailing, or embedded newlines or whitespace
	18456	112	AAD_AUTH_BAD_SIGNATURE	Customer attempted to login with an access token that has a bad signature. If the access token came from AAD, then this can happen if the token

				is over a day old. Access tokens are good for up to one hour. Customer should acquire a new access token.
	18456	113	AAD_AUTH_BAD_HEADER	Customer attempted to login with an access token that does not contain necessary header information. If the access token came from AAD, then notify PostgreSQL DRI and OrcasAAD.
	18456	114	AAD_AUTH_MISSING_OBJECTID	Customer attempted to login with an access token that does not contain necessary claim information. If the access token came from AAD, then notify PostgreSQL DRI and OrcasAAD.
	18456	115	AAD_AUTH_MISSING_ISSUER	Customer attempted to login with an access token that does not contain necessary claim information. If the access token came from AAD, then notify PostgreSQL DRI and OrcasAAD.
	18456	116	AAD_AUTH_BAD_ISSUER	Customer attempted to login with an access token issued for a tenant different than the one configured for the database server. Check AAD tenant in which the access token is issued and tenant of the AAD admin user set on the database.
	18456	117	AAD_AUTH_MISSING_AUDIENCE	Customer attempted to login with an access token that does not contain necessary claim information. If the access token came from AAD, then notify PostgreSQL DRI and OrcasAAD.
	18456	118	AAD_AUTH_BAD_AUDIENCE	Customer attempted to login with an access token issued for a different resource than "ossrdbms-aad". Check to make sure that the access token is issued for the correct "ossrdbms-aad" resource URI in the correct cloud, and not for ARM or other resources.

	18456	121	AAD_AUTH_ALG_NOT_ALLOWED	Customer attempted to login with an access token where the header specifies an unsupported signature algorithm. (AAD for Orcas only supports RSA-based algorithms that are used by AAD.) If the access token came from AAD, then notify PostgreSQL DRI and OrcasAAD.
	18456	126	AAD_AUTH_NOT_VALID_YET	Customer attempted to login with an access token that is not yet valid. If the access token came from AAD, this is highly unlikely. Please notify PostgreSQL DRI and OrcasAAD.
	18456	127	AAD_AUTH_CANNOT_FETCH_TOKEN	Database server could not authenticate with AAD to fetch group information for the access token user. Check for sandbox logs containing " [AADAuthProvider] HTTP bad request". If found, include in incident. If error does not indicate transient failure, then notify PostgreSQL DRI and OrcasAAD.
	18456	134	AAD_AUTH_CANNOT_FETCH_GRAPH_DATA	Database server could not fetch group information for the access token user. Check for sandbox logs containing " [AADAuthProvider] HTTP bad request". If found, include in incident. If error does not indicate transient failure, notify PostgreSQL DRI and OrcasAAD.
	18456	100+	Other AAD errors	Any other error is probably an internal error in the service or some unaccounted for use-case. Please notify PostgreSQL DRI and OrcasAAD.

Step 2

Based on the error and state the appropriate action could be taken as below

ERROR 18456 and STATES 4,100,101

These are user errors and does not indicate a problem with the system.
4 - usually means someone put a bad server name in the connection string
100 and 101 means customer tried connection without SSL but they had enforce SSL set on their server

ERROR 18456, STATE 16

Indicates Gateway could not connect to the host. Follow the following to troubleshoot

a. Look up the host node database is running on by using the following kusto query.
look for the value of NodeName by looking at the Elastic servers and databases view in Xts
b. Get JIT Access to the box
c. Execute "netsat -aon"
d. If netstat shows lot of sockets(Hundreds of sockets) in FIN_WAIT_2 or CLOSE_WAIT then it could be because of socket leak.
Try to kill the process that owns these sockets and see if that resolves issues. If not then last restart would be to restart the node (SOP103 Restarting A Node)
e. If the problem is not with socket leak then please contact Expert Queue for issues.

ERROR 18456, STATE 20

Indicates that backend is not reachable. Use the below queries on sandbox logs

a. Query for Checking for crashing servers .

```
MonRdmsPgSqlSandbox
| where LogicalServerName == "<logicalservername>"
| summarize min(originalEventTimestamp), max(originalEventTimestamp) by ClusterName, NodeName, process_id
| order by min_originalEventTimestamp asc
```

If the server is restarting/crashing continuously then look at the sandbox logs for more error as below

```
MonRdmsPgSqlSandbox
| where TIMESTAMP > ago(30m)
| where LogicalServerName == "<logicalservername>"
| where text !contains "XStore" and text !contains "whitelist"
| project TIMESTAMP, ClusterName, NodeName, process_id, AppName, LogicalServerName, text
| order by TIMESTAMP desc  nulls last
```

Also check the Azure Watson for Dumps Refer: **SOP0006: Search Postgres Dumps.** Please follow up Expert Queue for this issue as restarting will probably not mitigate the issue. You can also search the ICM using server name to see if there is a related issue.

b. Query for checking CPU/Memory usage: This tells you if the server's CPU /Memory is exhausted. If it is really high (over 90%) on a continuous basis then probably that might indicate an overutilized server (or it could be a memory leak as well) . If the server is not currently accepting any more connection, restart the server as a mitigation step. Refer **SOP0007: Restarting or Dumping a process using CAS**. Please follow up with Expert Queue when this is encountered to resolve the issue.

```
MonResourceMetricsProvider
| where TIMESTAMP > ago(2d)
| where LogicalServerName  == "decovoanalyticsprod"
| extend cpu_percentage = (cpu_load/cpu_load_cap)*100, memory_percentage =
(memory_used_mb/memory_used_mb_cap)*100
| project TIMESTAMP, cpu_percentage, memory_percentage, working_set_percent
|render timechart
```

ERROR 18456, STATE 122

If the client receives the error message: "FATAL: Server is not configured to allow ipv6 connections," when attempting to connect from another Azure service, this is almost always because the customer has enabled the Microsoft.Sql endpoint on their service's subnet, which is causing all traffic to flow through a VNET. When such traffic reaches a Basic edition server, it results in this error message.

a. Is the server Basic edition?
b. Is the customer attempting to connect from another Azure Service?
c. Has the customer enabled the Microsoft.Sql endpoint on the service subnet?

There are two possible solutions:

a. Use a GeneralPurpose server instead, and provision VNET access according to this tutorial: https://docs.microsoft.com/en-us/azure/postgresql/howto-manage-vnet-using-portal
b. Alternatively, disable the Microsoft.Sql endpoint on the service subnet so that traffic does not flow through a VNET.

Others PG ERROR states for 18456:

These error states will show in MonLogin entries for AppTypeName Worker.PAL.PG for Standard or GeneralPurpose edition PostgreSQL servers
if the login attempt got to the PostgreSQL server backend.

https://msdata.visualstudio.com/Database%20Systems/_git/orcasql-postgresql-extensions?path=%2Fpostgres%2F9.5.20180228.1%2Fcontent%2Finclude%2Fserver%2Fazure_service_fabric%2Flogging_helpers.h&version=GBmaster

```
#define RLF_ERROR_LOGON_SUCCEEDED       0
#define RLF_ERROR_LOGON_FAILED          18456
#define RLF_STATE_SUCCESS               0
#define RLF_STATE_OUT_OF_MEMORY         1
#define RLF_STATE_COULD_NOT_FORK        2
#define RLF_STATE_TOO_MANY_CONNECTIONS  3
#define RLF_STATE_DB_IN_SHUTDOWN        4
#define RLF_STATE_DB_IN_STARTUP         5
#define RLF_STATE_DB_IN_RECOVERY        6
#define RLF_STATE_AUTH_FAILED           7
#define RLF_STATE_FIREWALL_BLOCKED      8
#define RLF_STATE_NO_SUCH_DATABASE      9
#define RLF_STATE_BAD_CLIENT_CERT       10

#define RLF_STATE_CONNECTION_THROTTLE   11
#define RLF_STATE_AAD_AUTH_FAILED       90
#define RLF_STATE_AAD_TENANT_NOT_SET    91
#define RLF_STATE_AAD_ADMIN_NOT_SET     92
#define RLF_STATE_AAD_MFA_ENFORCEMENT   93
#define RLF_STATE_AAD_AUTH_BUF_OVERRUN  94
#define RLF_STATE_AAD_TOKEN_TOO_LONG    95
#define RLF_STATE_AAD_MAPPING_FILE_ERR  96
```

From <https://msdata.visualstudio.com/Database%20Systems/_git/orcasql-postgresql-extensions?path=%2Fpostgres%2F9.5.20180228.1%2Fcontent%2Finclude%2Fserver%2Fazure_service_fabric%2Flogging_helpers.h&version=GBmaster>

How good have you found this content?