Postgres Connectivity Errors

Last updated by | Lisa Liu | Nov 6, 2020 at 10:34 AM PST

Errors

Error	State	Reason	Action
17830	*	Connection Timed out	Can happen for any reason. Transfer to connectivity queue
17832	126	Invalid Startup Packet	Something is missing from the startup packet. Customer should get an e
18456	4	Server name not found in startup packet	Ask customer to make sure username is "<User>@<Server>"

18456	20	Backend Unavailable	This one is most likely not a connectivity problem.
			1. First, check the # of restarts.
			2. Check the sandbox for any errors that could signal unavailability.
			3. It could just be that the PG or SBS recovery time is long. Run the foll
			<pre>MonRdmsPgSqlSandbox
			| where LogicalServerName == "toruscap"
			| where text contains "PostgresLauncher: ShutdownWithSF
			  or text contains "SqlSocketDuplicateProvider::DB engi
			  or text contains "Parallel redo is started for databa
			  or text contains "Parallel redo is shutdown for datab
			  or text contains "Recovery completed for database SBS
			  or text contains "LOG: database system was not prope
			  or text contains "LOG: redo starts at"
			  or text contains "LOG: redo done at"
			  or text contains "LOG: checkpoint starting: end-of-r
			  or text contains "LOG: database startup complete in"
			  or text contains "LOG: database system is ready to a
			  or tolower(text) contains "role" and tolower(text) cc
			on"
			| order by originalEventTimestamp asc
			| project originalEventTimestamp, NodeName, process_id,</pre>
			4. If you find nothing and the backend looks completely healthy, transf

18456	100	SSL Connection Enforced	Psql has behavior where a connection that fails with SSL is retried witho "sslmode=require". If you see this error, it's most likely just a retry. The for failure.
18456	101	SSL Secure Redirection Failed	If redirection is selected (which only Adobe has) and needs to be secure thrown. Exceedingly rare.
18456	121	GW SSL Handshake With Host Failed	Transfer to Connectivity Queue
18456	122	VNET Validation Failed	Could be a VNET Firewall rule, a client attempting to connect to a basic provide the error message they are getting on their console or in their lc
18456	123	Connection throttle due to memory	If you see this consistently, there should be a corresponding error in the the memory limit. However, these occasionally pop up as a 1-off error ir happens, but those can be ignored.
18456	124		Null pointer dereference error. Transfer to Naveen Setlur
18456	125	Invalid Startup Packet Length	The length of the startup packet is too little
18456	126	Invalid Startup Packet	The packet is malformed
18456	127	Too many clients	There are too many clients attempting to connection to Postgres. The cu existing clients to close. Look into connection pooling.
40532	4	Server Lookup Failed	This error means the user is attempting to connect to a server that does this isn't the case, it may be an SLB issue - One possibility is TSG: SNAT P If not, transfer to connectivity queue.

| 40613 | 16 | ProxyConnectionToBackendFailed | The Gateway was unable to connect to the Host. Take the connection_id below, and see if the connection was received by the Host. Note it down |

For General Purpose and Memory Optimized edition servers, there can also be entries for Worker.PAL.PG:

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.

If a combination is not on this chart, please transfer to the PG Connectivity Queue. Please look for the majority error when deciding which action to take. If a server is down, you will see different error and state combinations as the connection fails at different points. 18456,20 is the best indicator of a backend problem.

Steps

1. Start by running the query below for the window of time the incident existed. Update the server_name, start_time, and end_time with the incident specifics.

```
let pg_server_name = "nasetlur";
let begin_time = ago(4h);
let finish_time = now();
MonLogin
| where logical_server_name == pg_server_name
| where originalEventTimestamp > begin_time
| where originalEventTimestamp < finish_time
```

```
| where AppTypeName endswith ".PG"
| where event contains "process_login_finish"
| summarize count() by logical_server_name, error, ['state']
```

Similar query also available at:

https://msdata.visualstudio.com/Database%20Systems/_git/orcasql-fabric?
path=%2Fkusto_queries%2Fqueries%2Findependent%2Flogin_errors_and_states.txt&version=GBmaster
Please consider keeping both semantically equivalent.

  2. Take note of the most frequent errors and states and check the table above and take the appropriate action.

Connection ID query for (40613, 16)

```
let connectionid = 'test';
MonLogin
| where connection_id == connectionid
| project originalEventTimestamp , is_success, is_user_error , ['state']
, error, result, logical_server_name, database_name,AppTypeName , connection_id, peer_address , even
t, process_id , ClusterName
| order by originalEventTimestamp asc
```

If we do not notice any failures in MonLogin for the given server for all apptypes I.e. Gateway.PG, Host.PG and
Worker.PAL.PG , it could be related to SLB SNAT port exhaustion. Please refer to TSG SNAT port exhaution (Web view)

How good have you found this content?