SSL SYSCALL error EOF

Last updated by | Hamza Aqel | Jan 9, 2023 at 1:45 AM PST

The error message "SSL SYSCALL error EOF detected," usually indicates a connection error. This error can be related to resource consumption, query time-out, PostgreSQL disk issues, network interruptions, server crash, or other failures.

Common causes and solutions

Potential cause	Solution
Server is under heavy memory usage	The most common cause of this error is when the system runs out of memory. Verify from our Memory TSG. Also, check resource usage on the application end. If the server resources or application resources are maxed out, it will most likely result in this error message.
Server is down	One cause could be if your database server is down. Check our Availability TSG to confimr if the server was not available for some time.
High CPU usage	High CPU usage can lead to connection issues. If it is nearing 100%, then it might be cause of this issue, you can check our CPU TSG to check why CPU is nearing 100% and how to check the cause of that.
You are writing to the database server	Check your Postgres server logs. If you're seeing block-write messages before or after this error message in the logs, it's likely a storage issue. PostgreSQL storage engine reports this error when it's trying to read at or past end-of-file (EOF), or a partial block written at end of file due to which the PostgreSQL storage engine was attempting to read these blocks to insert new rows (tuples) into. Run a Vacuum Full on the table that you're writing to resolve this error message.
Queries are timing out	The EOF detected error can occur if the client thinks the TCP connection is still up, but the server has already hung up. The client then starts sending a query down the pipe and when it does, it notices the connection is broken, resulting in a sudden EOF. Try setting or changing timeout parameters and optimize the query if possible.
Unused or inactive replication slots	Check if there is any Inactive replication slots through our TSG Inactive replication slot to see if you have any inactive replication slots. Replication slots are created to hold transaction-related information on the source server for clients to consume. The server will keep write-ahead log (WAL) files and other transaction-snapshot related files around without cleaning them up until the information is consumed from the server and the slot LSN moves forward. Any unused slots can result in a buildup of files. These files start causing checkpoint issues since checkpoint has to process these files. The long checkpoint can lead to long recovery and result in this error message.