Connection resets for large data sets forcibly closed connection

Last updated by | Peter Hewitt | Mar 29, 2023 at 10:48 PM PDT

Contents

Issue

The error "An existing connection was forcibly closed by the remote host" may occur when the client is in the middle of retrieving large result sets.

Typical scenarios include:

- Running replication from on-premise to Azure SQL Database
- Running queries from SSMS on-premise connecting to Azure SQL Database

Note that this is depending on the size of the result sets, not on the idle connection timeout of 30 minutes. Idle connections is a separate issue.

Investigation / Analysis

This issue occurs because of a defect or limitation in our gateway proxy code. The Gateway PG team is working to identify the root cause and provide fix. There is no clear plan or time frame for the fix though.

See the following items to distinguish this issue from other causes:

- Gateway reset connections idle for 30m to check the symptoms of the idle connection timeout scenario.
- Dropped connections, Communication link failure, Connection resets for similar symptoms.

Mitigation

The issue can be avoided and worked around by using the redirect connection policy instead of proxy. Redirect is the default behaviour for connections from within Azure, for example Azure VMs, Web or Worker roles, Websites.

The customer can check the current setting and change to redirect through the Azure portal, PowerShell, or Azure CLI. See Change the connection policy ↗ for the steps. An earlier version of this article suggested that CSS should change it; this is strongly advised against though as it can break general database connectivity for the customer.

Connection policy lists some prerequisites and limitations for using redirect:

- Clients need to allow outbound communication from the client to all Azure SQL IP addresses in the region on ports in the range of 11000 to 11999. Use the Service Tags for SQL to make this easier to manage.
- Clients need to allow outbound communication from the client to Azure SQL Database gateway IP addresses on port 1433.
- If the client is an Azure Virtual Machine, you can accomplish this using Network Security Groups (NSG) with service tags.
- If the client is connecting from a workstation on-premises then you may need to work with the customer's network admin to allow network traffic through your corporate firewall.
- Connections to private endpoint only support Proxy as the connection policy.

Classification

Root Cause: Azure SQL v3/Connectivity/Disconnects/Idle session disconnected

How good have you found this content?

🙂 🙁