Network settings, TCP ports and firewalls

Last updated by | Subbu Kandhaswamy | Sep 17, 2020 at 6:25 PM PDT

Contents

- Firewall Related issues
  - Scenarios
- Basics on handling persistent connectivity issues
- Resolution /Mitigation steps
- Root Cause: Azure

Firewall Related issues

Scenarios

If the application persistently fails to connect to Azure SQL Database, it usually indicates an issue with one of the following:

- Firewall configuration. The Azure SQL database or client-side firewall is blocking connections to Azure SQL Database.
- Network reconfiguration on the client side: for example, a new IP address or a proxy server.
- User error: for example, mistyped connection parameters, such as the server name in the connection string.

Basics on handling persistent connectivity issues

Set up firewall rules to allow the client IP address. For temporary testing purposes, set up a firewall rule using 0.0.0.0 as the starting IP address range and using 255.255.255.255 as the ending IP address range. This will open the server to all IP addresses. If this resolves your connectivity issue, remove this rule and create a firewall rule for an appropriately limited IP address or address range.

- On all firewalls between the client and the Internet, make sure that port 1433 is open for outbound connections. Review Configure the Windows Firewall to Allow SQL Server Access and Hybrid Identity Required Ports and Protocols for additional pointers related to additional ports that you need to open for Azure Active Directory authentication.
- Verify your connection string and other connection settings. See the Connection String section in the connectivity issues topic.
- Check service health in the dashboard. If you think there's a regional outage, see Recover from an outage for steps to recover to a new region.

Depending on the configuration at customer end, customer may experience a persistent connection failure where Azure SQL database or client-side firewall is blocking connections .

Resolution /Mitigation steps

Connection to database/server coming from Non-Azure IP and IP address not part of firewall rule then, State 130 error will be encountered. When user connecting to database from Azure service , and Allow Azure Services at the server level is not turned ON then, State 82 will be encountered. In rare cases, user experience firewall errors connecting from Non-Azure Services and IP address is allow listed OR if user connecting from Azure based services and Allow Azure Services is ON. Open ICM incident and engage engineering in a must.

Root Cause: Azure

SQL DB v2\Connectivity\Login Errors\Firewall errors and misconfigurations

How good have you found this content?