Cannot open server y requested by the login (Error 40532 or 40615)

Last updated by | Peter Hewitt | Mar 8, 2023 at 5:20 AM PST

Contents

Issue

When trying to logon to SQL Server error 40532 or error 40615 occurs.

1. `Cannot open server {servername} requested by the login.... The login failed. (Microsoft SQL Server, Error: 40532)`

2. `Cannot open server {servername} requested by the login.... IP address {address} is not allowed (Microsoft SQL Server, Error: 40615)`

Error 40532 - Cannot open server {servername} requested by the login.... The login failed.

This error code can be generated by SQL Server or the Azure Gateway. It occurs for a number of reasons, such as connecting from a subnet where VNet service endpoints are enabled, but the VNet rules aren't set correctly. Also when an incorrect "gateway IP address" due to stale/misconfigured DNS records is used, or when the login username is an email address or contains the @ symbol. It can be related to a gateway issue, however this is a less common cause.

Troubleshooting error 40532

The following Kusto query returns 40532 errors for the specified server:

```
let ServerName = "";
MonLogin
| where TIMESTAMP >= ago(1d)
| where event == "process_login_finish"
| where error == '40532'
| where logical_server_name =~ ServerName or LogicalServerName =~ ServerName
| project PreciseTimeStamp, logical_server_name, database_name, MachineName
, package, event, is_user_error, error, state, peer_address, is_vnet_address, application_name, connection_id
```

If you obtain a ConnectionId, like when using [Azure SQL Connectivity Checker](#), you can view the telemetry using:

```
MonLogin
| where connection_peer_id =~ 'put customer connectionId here'
```

1. SQL Server

This issue is usually originated by one of the following:

- Aiming to connect to SQL DB, customer enabled Microsoft.Sql in the subnet but forgot to add the virtual network rule for the originating subnet in the **Firewalls and virtual networks** settings on the server.
- Aiming to connect to other services (like Azure Database for MySQL), customer didn't realized that SQL DB would also be impacted.

See Error 40532 State 150

2. Gateway

Gateway is responsible for resolving physical location of a customer's database given server name and database name which user is using to connect.

If the error is coming from gateway package, it means that either something is wrong internally while trying to resolve it or, most likely, the server does not exist in that gateway. Please note that each region can have multiple "gateway IP addresses" (control rings), and that each server will belong to one of those control ring.

Error 40532 is usually related to one of the following scenarios:

- When a log-in name includes an At symbol (@), SQL treats the domain (for example, mydomain.com ☐ in user@mydomain.com) as a server. This results in a log-in failure after lookup. This is by design. If the username includes @, see Handling Error 40532 ☐.
- Customers trying to connect to the wrong "gateway IP address" due to stale/misconfigured DNS records.

Error 40615 - Cannot open server {servername} requested by the login…. IP address {address} is not allowed

This error is commonly caused by required ports not enabled, problems with network address translation (NAT) of IP addresses and internet connections using dynamic IP addressing.

1. Required ports not enabled

1. If connecting from outside Azure services (for example, from a local network), create a firewall exception on your computer for TCP Port 1433 to access the Azure SQL Database.
2. When connecting from Azure services (such as, Azure-VM or Azure-Web App connecting to SQL Database), you might need to open additional ports. See, Ports beyond 1433 for ADO.NET 4.5 and Azure SQL Database ☐.

2. Connection fails after allowing the IP address

Due to NAT, the IP address used by your computer to connect to SQL Database might be different than the IP address in your computer IP configuration settings. To view the IP address to connect to Azure and help fix this issue:

1. Sign in to the Azure portal.

2. Go to the **Configure** tab on the server that hosts your database. The Current Client IP Address is in the **Allowed IP Addresses** section.

3. Select **Add** or **Allow Azure services and resources to access this server**.

3. Dynamic IPs

If you have an internet connection using dynamic IP addressing and cannot get through the firewall:

1. Ask your internet service provider for the IP address range assigned to your client computers that access the server.

2. Add that IP address range (subnet) as an IP firewall rule.

Public Doc References

- [Create and manage firewall rules](#) ⧉
- [PowerShell create virtual service endpoint](#) ⧉

Root Cause Classification

Cases resolved by this TSG should be coded to the one of the following root causes:
Azure SQL v3\Connectivity\Login Errors
Azure SQL v3\Connectivity\Configuration request
Azure SQL v3\Connectivity\Gateway failures
Azure SQL v3\Connectivity\How-to/advisory

How good have you found this content?