Error 40615 Cannot open server requested by the login IP not allowed

Last updated by | Holger Linke | Feb 10, 2023 at 4:53 AM PST

Cannot open server requested by the login - IP address {address} is not allowed

Issue

Connections to Azure SQL Database are failing with the following error message:

> Error 40615
> Cannot open server '<servername>' requested by the login. Client with IP address 'xxx:xxx:xxx:xxx' is not allowed to access the server. To enable access, use the Windows Azure Management Portal or run sp_set_firewall_rule on the master database to create a firewall rule for this IP address or address range. It may take up to five minutes for this change to take effect.

Investigation / Analysis

The error occurs because the IP address returned in the error message is blocked by the SQL server and database firewall.

Mitigation

You can allow access in several ways:

- Use the SQL Azure Portal (SQL Server -> Security -> Firewalls and Virtual networks) to create a server-level firewall rule.
- Run sp_set_firewall_rule on the `master` database to create a firewall rule for this IP address or address range.
- Run sp_set_database_firewall_rule on the user database to create a firewall rule for this IP address or address range.

It may take up to five minutes for this change to take effect.

More Information

In Azure SQL Database service, a connection attempt from the internet and Azure must pass through the firewalls before they reach your server or database. There are two types of firewall rules:

- **Server level firewall rules**: These rules enable clients to access your entire server, that is, all the databases managed by the server. The rules are stored in the `master` database. You can have a maximum of 128 server-level IP firewall rules for a server. If you have the "Allow Azure services and resources to access this server" setting enabled, this counts as a single firewall rule for the server. These can be managed using Azure Portal, PowerShell, Azure CLI, T-SQL, Rest-API.

  To improve performance, server-level IP firewall rules are temporarily cached at the database level. To refresh the cache, see DBCC FLUSHAUTHCACHE.

- **Allow Azure services and resources to access this server**: When set to "Yes", other resources within the Azure boundary, for example an Azure Virtual Machine, can access SQL Database. Here the boundary refers to the cloud environment. Thus, for regional cloud, it is limited to azure resources inside the regional cloud.

- **Database level firewall rules**: These rules enable clients to access certain (secure) databases. You create the rules for each database (including the master database), and they're stored in the individual database.

  It is recommended to use database-level IP firewall rules whenever possible. This practice enhances security and makes your database more portable. These can be managed only using T-SQL:

  - sys.database_firewall_rules
  - sp_set_database_firewall_rule
  - sp_delete_database_firewall_rule

  See Server-level versus database-level IP firewall rules to understand the difference between server level and database level firewall rules.
  If you are seeing that the firewall rules are not behaving as expected, please follow Troubleshoot the database firewall.

- **SNAT ports**: Azure uses source network address translation (SNAT) and a Load Balancer (not exposed to customers) to communicate with end points outside Azure in the public IP address space. Often times we notice customer whitelist incorrect IP address/subnet ranges instead of public_ip of the client/server to allow access in SQL Server/DB firewall rules and get error. To handle this, check sys.firewall rules from customer end, and also check the incoming connections for that impacted server from our telemetry (Monlogin - Peer address has the last octet masked, but can still match the first 3 octets) and ensure customer is not whitelisting incorrect address. For more information please refer Outbound connections.

Public Doc reference

- Create and manage firewall rules
- Virtual network endpoints
- PowerShell create virtual service endpoint

Classification

Root Cause: Azure SQL DB v3\Connectivity\Login Errors\Firewall errors and misconfigurations

How good have you found this content?

🙂 🙁