

Firewall Rules

Last updated by | Lisa Liu | Nov 6, 2020 at 10:34 AM PST

Firewall Rules

Tuesday, February 20, 2018
7:23 PM

Firewalls prevent all access to your database server until you specify which computers have permission. The firewall grants access to the server based on the originating IP address of each request.

To configure a firewall, create firewall rules that specify ranges of acceptable IP addresses. You can create firewall rules at the server level.

Firewall rules: These rules enable clients to access your entire Azure Database for PostgreSQL server, that is, all the databases within the same logical server. Server-level firewall rules can be configured by using the Azure portal or Azure CLI commands. To create server-level firewall rules, you must be the subscription owner or a subscription contributor.

More information: <https://docs.microsoft.com/en-us/azure/postgresql/concepts-firewall-rules>

You need to make sure that you client's IP address is enabled on the firewall rule or if your application is connecting within Azure make sure to set the Allow access to Azure services to on.

Firewall rules can be determined either by whitelisting IP address of the application Or allowing All Azure Services. One more option is to allow

[PostgreSQL VNET support](#)

If the customer did not configure his Firewall correctly he will get Error 8 state 102, this can be checked on ASC or Kusto.

8	102	0	1	COUNT	e_crDisconnect	IPv4 address not in the whitelist.	
---	-----	---	---	-------	----------------	------------------------------------	--

ASC should Show a Critical Insight in case the customer did not setup firewall properly

MySQL CONNECTIVITY ERROR

error(s): Firewall blocked connection (Error Code = 18456, State Code = 102)

MySQL SERVER

MSK

is this insight helpful?

Description

[User Error] Found 3 failed connection attempts (error(s): Firewall blocked connection (Error Code = 18456, State Code = 102)) to MySQL server msk during the period of 09/24/2019 11:17:12 UTC and 09/24/2019 11:18:57 UTC because client's IP is not configured in Firewall.

Impacted Resources

msk

Recommended Action

To fix this issue please ensure client IP address is configured in the firewall of the server.

Customer Ready Content

Copy Content

New Email

Thank you for contacting Microsoft support about your connection issues with Azure Database for MySQL. During our investigation we determined that connections to your database server are failing because the client IP address is not configured as allowed IP address in the firewall of the server.

Recommended Steps

To fix this issue please ensure your client IP address is configured in the firewall of the server. You can refer to this article for assistance with configuring your firewall for your Azure Database for MySQL server.

Recommended Documents

Azure Database for MySQL

MySQL Discussion forum

Links

Internal - Oracle Gateway TSO for Azure CSS engineers

Azure Database for MySQL

Public - MySQL Discussion forum

Insight Investigation Period

From 09/23/2019 12:00:00 to 09/24/2019 12:00:00 (UTC)

Generated On

Sep 24, 2019 5:29:28 AM

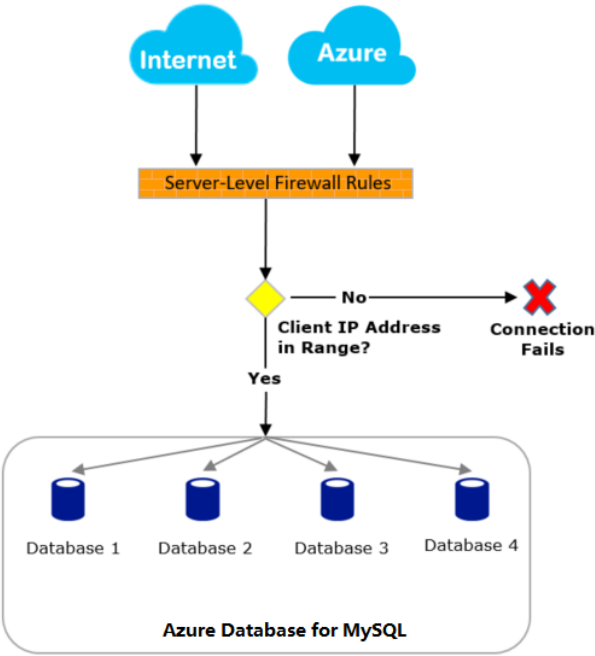
Below is a Kusto Query to check for errors

```
let pg_server_name = "nasetlur";
let start_time = ago(4h);
let end_time = now();
MonLogin
| where logical_server_name == pg_server_name
| where originalEventTimestamp > start_time
| where originalEventTimestamp < end_time
| where AppTypeName contains "Gateway.PG"
| where event contains "process_login_finish" or event contains "proxy_close_connection"
| project originalEventTimestamp , is_success, is_user_error , ['state']
, error, result, logical_server_name, database_name,AppTypeName , connection_id, peer_address , event, process_id , ClusterName
```

Update the server_name, start_time, and end_time with the incident specifics.

https://supportability.visualstudio.com/AzureDBPostgreSQL/_wiki/wikis/AzureDBPostgreSQL/289068/Firewall-Rules

1/2



Created with Microsoft OneNote 2016.

How good have you found this content?

