ERROR: server certificate does not match host name

Last updated by | Daniel Valero | Mar 13, 2023 at 2:34 PM PDT

Contents

Issue

psql: error: connection to server at X.X.X.X", port 5432 failed: server certificate for "xxxxxxxxxx.database.azure.com ☒" (and 2 other names) does not match host name "X.X.X.X"

Investigation/Analysis

When using **sslmode=verify-full** the connections will fail if the server IP Address is used as hostname

> psql: error: connection to server at "10.5.3.4", port 5432 failed: server certificate for "ce73dbb59a96.database.azure.com ☒" (and 2 other names) does not match host name "10.5.3.4"

This is an expected behavior

A similar error can happen in Private Servers if the connections is attempted using the cname of the server, and the cname changed for any reason.

```
daniel              .:~$ nslookup pgdvvr8.postgres.database.azure.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
pgdvvr8.postgres.database.azure.com     canonical name = db1f8b98ef78.pgdvvr8.private.postgres.database.azure.com.
Name:   db1f8b98ef78.pgdvvr8.private.postgres.database.azure.com
Address: 10.5.3.4
```

The cname for the server can change during the server life cycle and the server certificate is not regenerated

One scenario that could cause (but not always) the change of the came is changing the Private DNS Zone for the server

Repro Steps

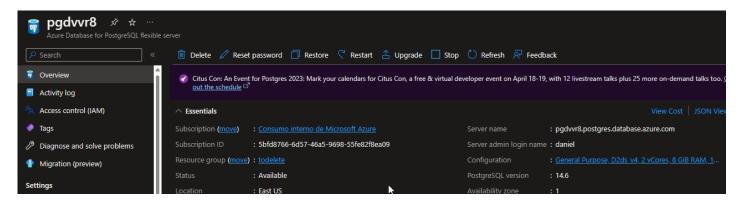This is valid for Private Servers and Public Servers, as shown below:

Public Server

```
daniel@                   :~$ psql "sslmode=verify-full sslrootcert=DigiCertGlobalRootCA.crt.pem host=20.120.52.176 dbname=postgres user=daniel"
psql: error: connection to server at "20.120.52.176", port 5432 failed: server certificate for "cddcab87a5f5.database.azure.com" (and 1 other nam
) does not match host name "20.120.52.176"
```

Private Server

```
daniel@                   :~$ psql "sslmode=verify-full sslrootcert=DigiCertGlobalRootCA.crt.pem host=10.5.3.4 dbname=postgres user=daniel"
psql: error: connection to server at "10.5.3.4", port 5432 failed: server certificate for "ce73dbb59a96.database.azure.com" (and 2 other names
es not match host name "10.5.3.4"
```

Mitigation

1. Connection must be done using the server FQDN

2. Connections is possible the Server IP Address or cnanme (even after it changed) by using any *sslmode* other than *verify-full*, However, we recommend customer to always connect using FQDN instead of server IP Address or cname as they can change during the serve life cycle