

# [TSG - FSPG] HA Server is in read-only error due to custom DNS entry not update

Last updated by | Dufred Odige | Mar 13, 2023 at 12:03 PM PDT

---

## Issue Scope

Customer may report that their query failed to execute write transactions (CRUD) to PostgreSQL flexible server databases: server is in read-only mode.

- Applies for server deployed with VNET integration and HA enabled.

## Product

Azure Database for PostgreSQL Flexible server.

## Investigation/Analysis

- Have the customer share the result of NS Lookup with screenshot and compare the IP address returned with the one listed for the server A record under their private DNS zone.
- Go to XTS Double check if the server has HA enabled. \_If yes, keep reading. \_
- Use XTS view "orcasbreadth servers.xts\_" to check the role of the original server (the name they can see on azure portal) which should be shown as "Primary".
- If searching the server's name return two records, one with the server and another one with extra letter after the serve name.
- And If you see the original server name is listed as the "standby" server:
  - Then, there was probably a failover where the former standby server had taken over and became primary which will cause the old primary to become standby and set to ready-only.
  - What is also happening on the background is that. On the private DNS zone the server was configured with, there will be an automated task triggered to perform an update of the A record for that server to point to the IP address of the server running as the primary.
  - Customer has no idea about this mechanism.
- So, on their side they may not focus on this change on the Private DNS zone, if they were using the private IP to connect to the server, this where they will start to get the read-only error.
  - Or if they have custom A DNS record that is pointing to the server private IP address so when connecting over VPN they could easily resolve the server's name.

## USE CASE

- Customer may have created an entry on their customer DNS server that points to the original IP address or the primary, and everything should be working so far, it is like using directly the IP address.
- Later on, if an unplanned or planned failover occurs, primary server IP will change, and Azure DNS will update the record for the serve with new IP but customer DNS server will remain with the IP they setup manually.
- So, when they try to run any write transaction, "read only" error message they will because the IP they had setup in their DNS server is no longer the primary.

## Mitigation

- Review the Azure private DNS zone configured with flexible server and check if the A record is there and what IP it is pointing to.
- They can update their own DNS record to point to same IP that is listed on the Azure private DNS zone.
- But Customer should never use private IP of server to connect, especially when they have HA enabled.
- They should use [DNS Forwarder](#) ☑. Same thing applies if they are making connection from outside of azure like from their on-premises network over the VPN to Azure, this way all connection will be always sent to the primary server.