

Private Link TSG

Last updated by | Hamza Aqel | Feb 11, 2022 at 8:41 AM PST

Demo Video : <https://msit.microsoftstream.com/video/464232f8-23f1-4b10-9de9-2f6fae9cc1d5>

CSS Mentoring session :

[Microsoft Stream](#)

Documentation :

[Private Link for Azure Database for PostgreSQL Single server](#) (Web view)

[Private Link documentation](#)

[Private Link](#)

Blogs :

PostgreSQL :

<https://techcommunity.microsoft.com/t5/azure-database-for-postgresql/introducing-private-link-for-azure-database-for-postgresql/ba-p/1088068>

<https://techcommunity.microsoft.com/t5/azure-database-for-postgresql/using-private-link-and-point-to-site-gateway-for-secure-on/ba-p/1108165>

ARM Templates :

PostgreSQL :

<https://github.com/Azure/azure-postgresql/tree/master/arm-templates/ExampleWithPrivateLink/ExistingServerAndVnet>

<https://github.com/Azure/azure-postgresql/tree/master/arm-templates/ExampleWithPrivateLink/NewServerAndVnet>

With respect to issues for the customer, There are 2 possible categories : Provisioning issues, Login issues

Provisioning issues

The customer is not able to provision a private endpoint successfully for an elastic server.

Provisioning involves communication between Orcas RP and Network RP. So the issue might be on either side.

To detect issues on Network RP side, follow this TSG :

https://dev.azure.com/msazure/AzureWiki/_wiki/wikis/AzureWiki.wiki/21697/-Private-Endpoint-Internal-Server-Error

To detect issues on Orcas RP side, first check the state of PEC in CMS table elastic_server_private_endpoint_connections :

```
select A.name, A.state, A.elastic_server_edition, B.* from dbo.elastic_server_private_endpoint_connections B inner join
dbo.elastic_servers A on A.elastic_server_id = B.elastic_server_id where A.name = '<SERVERNAME>'
```

Check the last_exception column to detect if there are any exceptions.

Check list of operations for the server :

MonManagementOperations

| where operation_type contains "ElasticServerPrivateEndpointConnection"

| where operation_parameters contains "<SERVERNAME>"

Get connection_name from CMS table dbo.elastic_server_private_endpoint_connections and query MonManagement and don't hesitate to file an ICM if this is the case :

MonManagement

```
| where keys ends with '<connection_name>'
| project originalEventTimestamp, state_machine_type, old_state, new_state, keys
```

In some cases the Azure Database for PostgreSQL and the VNet-subnet are in different subscriptions. In these cases you must ensure the following configurations: Make sure that both the subscription has the Microsoft.DBforPostgreSQL resource provider registered. For more information refer resource-manager-registration

Login Issues :

Find the app name of the server and use SFE to check fabric properties. Verify such an entry exists

"InterfaceEndpointsProfiles" :

fabric/Worker.PAL.PG/e8aae6811bce	InterfaceEndpointsProfiles	6/21/2019 12:57:07 AM	0x3c496e74657266616365456e64706f696e747350726666696c65733e0d0a20203c496e74657266616365456e64706f696e747350726666696c65204e616d653d2272616d7065
fabric/Worker.PAL.PG/e8aae6811bce	IsInCreate	6/21/2019	0x460061006c0073006500

Find if logins are successful in MonLogin and make sure the customer can resolve the private link FQDN using nslookup :

```
nslookup mydemopostgresserver.privatelink.postgres.database.azure.com.
```

You'll receive a message similar to this:

```
Azure PowerShell

Server: Unknown
Address: 168.63.129.16
Non-authoritative answer:
Name: mydemopostgresserver.privatelink.postgres.database.azure.com
Address: 10.1.3.4
```

MonLogin

```
| where event == "process_login_finish"
| where LogicalServerName == "<SERVERNAME>"
```

Execute: [\[Web\]](#) [\[Desktop\]](#) [\[Web \(Lens\)\]](#) [\[Desktop \(SAW\)\]](#) <https://sqlazurescus2.kustomfa.windows.net/sqlazure1>

MonLogin

```
| where TIMESTAMP > ago(2d)
| where logical_server_name contains "pgservername" and database_name == "postgres" and
is_vnet_private_access_address == 1
```

Check logs around incoming vnet v2 packet in sandbox logs :

MonRdmsPgSqlSandbox

```
| where LogicalServerName == "pgservername"
| where text contains "[vnet] Incoming vnet v2 packet"
```

for more details about the setup , please refer to our public

[documentation](#)