Connectivity - SQL DB connection Policy

Last updated by | Charlene Wang | Mar 14, 2021 at 8:18 PM PDT

Contents

Connectivity - SQL DB connection Policy

Policy

Azure SQL Database supports the following three options for the connection policy setting of a SQL Database server:

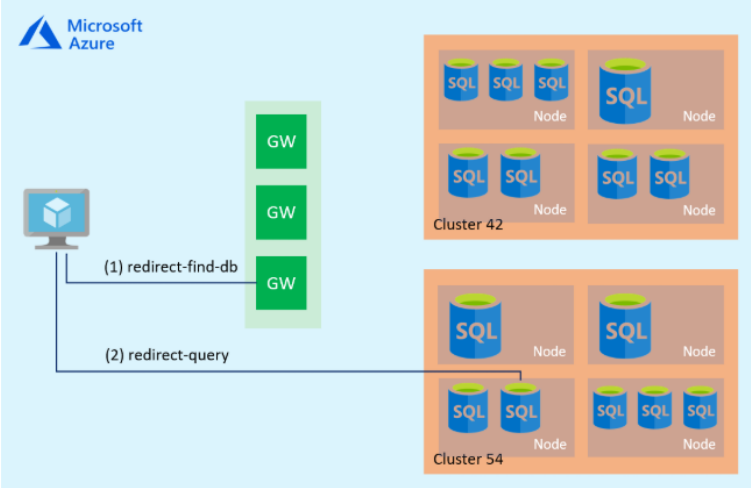
- **Redirect (recommended):** Clients establish connections directly to the node hosting the database, leading to reduced latency and improved throughout. For connections to use this mode clients need to
- Allow inbound and outbound communication from the client to all Azure IP addresses in the region on ports in the range of 11000 11999.
- Allow inbound and outbound communication from the client to Azure SQL Database gateway IP addresses on port 1433.
- **Proxy:** In this mode, all connections are proxied via the Azure SQL Database gateways, leading to increased latency and reduced throughout. For connections to use this mode clients need to allow inbound and outbound communication from the client to Azure SQL Database gateway IP addresses on port 1433.
- **Default:** This is the connection policy in effect on all servers after creation unless you explicitly alter the connection policy to either Proxy or Redirect. The default policy is Redirect for all client connections originating inside of Azure (e.g. from an Azure Virtual Machine) and Proxy for all client connections originating outside (e.g. connections from your local workstation).

We highly recommend the Redirect connection policy over the Proxy connection policy for the lowest latency and highest throughput. However, you will need to meet the additional requirements for allowing network traffic as outlined above. If the client is an Azure Virtual Machine you can accomplish this using Network Security Groups (NSG) with service tags. If the client is connecting from a workstation on-premises then you may need to work with your network admin to allow network traffic through your corporate firewall.

Connecting to Azure Database from within Azure services

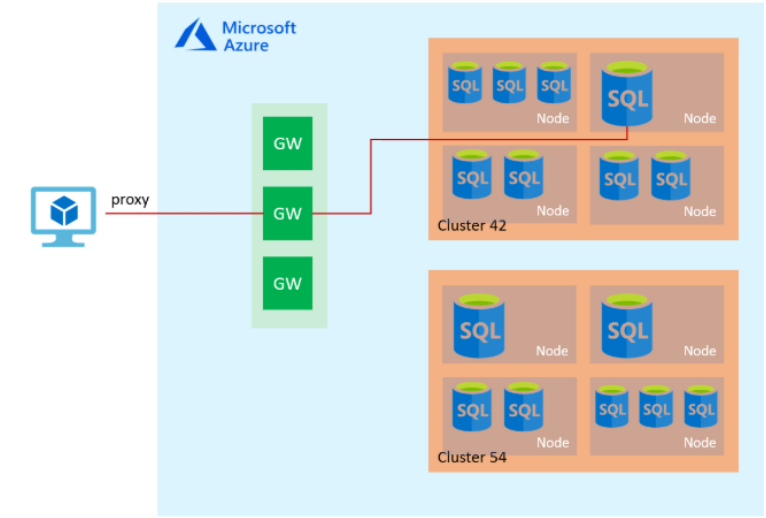
If you are connecting from within Azure your connections have a connection policy of Redirect by default. A policy of Redirect means that after the TCP session is established to the Azure SQL database, the client session is then redirected to the right database cluster with a change to the destination virtual IP from that of the Azure

SQL Database gateway to that of the cluster. Thereafter, all subsequent packets flow directly to the cluster, bypassing the Azure SQL Database gateway. The following diagram illustrates this traffic flow.



Connecting to Azure Database from Outside

If you are connecting from outside Azure, your connections have a connection policy of Proxy by default. A policy of Proxy means that the TCP session is established via the Azure SQL Database gateway and all subsequent packets flow via the gateway. The following diagram illustrates this traffic flow.



Check connection policy from backend

We can check connection policy used by client from MonLogin. Check logins on the Gateway, the “result” column will tell you if redirection is used (value **e_crContinue**), or not (value **e_crContinueSameState**) for proxy.

```
MonLogin
| where originalEventTimestamp > ago(2d)
| where (logical_server_name =~ "{ServerName}" ) and database_name =~ "{DatabaseName}
| where event == "process_login_finish"
| where AppName == "Gateway"
| summarize count() by result, driver_name
```

Public doc Reference

- <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-connectivity-architecture>

How good have you found this content?