Create SQL Database

Microsoft

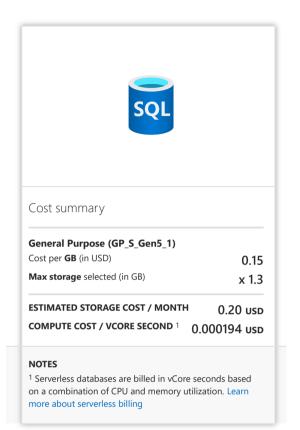
Basics Networking Security Additional settings Tags Review + create Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'cloud-sql-server' and all databases it manages. Learn more **Network connectivity** Choose an option for configuring connectivity to your server via public endpoint or private endpoint. Choosing no access creates with defaults and you can configure connection method after server creation. Learn more No access Connectivity method * (i) Public endpoint Private endpoint Firewall rules Setting 'Allow Azure services and resources to access this server' to Yes allows communications from all resources inside the Azure boundary, that may or may not be part of your subscription. Learn more Setting 'Add current client IP address' to Yes will add an entry for your client IP address to the server firewall. Allow Azure services and resources to No Yes access this server * Add current client IP address * No Yes

Connection policy

Configure how clients communicate with your SQL database server. Learn more

Connection policy ①

- Default Uses Redirect policy for all client connections originating inside of Azure (except Private Endpoint connections) and Proxy for all client connections originating outside Azure
- Proxy All connections are proxied via the Azure SQL Database gateways
- Redirect Clients establish connections directly to the node hosting the database



Encrypted connections

This server supports encrypted connections using Transport Layer Security (TLS). For information on TLS version and certificates, refer to connecting with TLS/SSL. Learn more

Minimum TLS version

TLS 1.2

Review + create

< Previous

Next : Security >