

Error: 10060 - The server was not found or was not accessible

Last updated by | Vitor Tomaz | Dec 6, 2021 at 1:17 PM PST

Contents

- [Issue](#)
- [Investigation/Analysis](#)
 - [Connecting via VPN \(private endpoint\)](#)
 - [Connecting via Public Endpoint](#)

Issue

A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: TCP provider, error: 0 - A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.) (Microsoft SQL Server, Error: 10060)


Investigation/Analysis





Connecting via VPN (private endpoint)

SQL Managed Instance is placed inside the Azure virtual network and a subnet that is dedicated to managed instances. This deployment provides you with a secure private IP address. You can connect to SQL Managed Instance via private endpoint if you are connecting from one of the following:

- Machine inside the same virtual network
- Machine in a peered virtual network
- Machine that is network-connected by VPN or Azure ExpressRoute


If you are trying to connect via private endpoint, review the following:

- The host name is valid and port used for the connection is 1433, format is tcp:<mi_name>.<dns_zone>.database.windows.net,1433
- The Network Security Groups (NSG) on the managed instance subnet allows access on port 1433.
- If you are unable to connect from an Azure hosted client (like an Azure virtual machine), check if you have a Network Security Group set on the client subnet that might be blocking outbound access on port 1433.
- If the [connection type](#)  is **Redirect**:






- Ensure the Network Security Groups (NSG) on the managed instance subnet allows access on ports **11000-11999**.
- If you are unable to connect from an Azure hosted client (like an Azure virtual machine), check if you have a Network Security Group set on the client subnet that might be blocking *outbound* access on ports **11000-11999**.
- Any networking device used (like firewalls, NVAs) does not block the traffic mentioned above.
- Routing is properly configured, and asymmetric routing is avoided. A route with the [0.0.0.0/0 address prefix](#)  instructs Azure how to route traffic destined for an IP address that is not within the address prefix of any other route in a subnet's route table. When a subnet is created, Azure creates a default route to the 0.0.0.0/0 address prefix, with the **Internet** next hop type. Check if this route was overridden. See the details about impact of changes on this default route at [0.0.0.0/0 address prefix](#) .
- If you are using virtual network peering between different regions, verify that **global virtual network peering** is supported. See more at [Connect inside a different VNet](#) .
- If you are using peering via VPN gateway, make sure that the two virtual networks are properly peered. See more at [Connect with VNet peering](#) .

Learn more about how to [connect your application to Azure SQL Managed Instance](#) .

Connecting via Public Endpoint

If the machine does not have virtual network access to managed instance, you can use [public endpoint](#)  for data access to your managed instance from outside the virtual network. For example, this allows access from multi-tenant Azure services like Power BI, Azure App Service, or an on-premises network, via a public endpoint.

If you are trying to connect via public endpoint, review the following:

- You have [public endpoint enabled](#) .
- You have [allowed public endpoint traffic on the network security_group](#) .
- The [host name contains ".public."](#)  and that port used in the connection string is **3342**, format is `<mi_name>.public.<dns_zone>.database.windows.net,3342`
- Network traffic to this endpoint and port is allowed from the source and any networking appliances you may have (firewalls, etc.).
- Routing is properly configured, and asymmetric routing is avoided. A route with the [0.0.0.0/0 address prefix](#)  instructs Azure how to route traffic destined for an IP address that is not within the address prefix of any other route in a subnet's route table. When a subnet is created, Azure creates a default route to the 0.0.0.0/0 address prefix, with the **Internet** next hop type. Check if this route was overridden. See the details about impact of changes on this default route at [0.0.0.0/0 address prefix](#) .

How good have you found this content?

