Connectivity - Check if client uses proxy or redirect

Last updated by | Vitor Tomaz | Jun 8, 2022 at 5:32 AM PDT

Contents

Connectivity - Check if a client application uses proxy or redirect

This article provides you with several methods to identify if a client application is using the Proxy or Redirect connection policy. It applies to both Azure SQL Database and Managed Instance.

Quick summary on Proxy vs. Redirect:

- Proxy means that all database traffic runs over destination port 1433 on the Azure gateway
- Redirect means that the application will use as a destination port within the range between 11000 and 12000; the initial connection handshake will still use port 1433.
- If you are using Private Link, the connection will use Proxy even if you have configured a default connection policy of Redirect. This might change in the future.

Check from the client side

These steps can be run by a customer on their application environment.

TCPView

Download TCPView from sysinternals and open it on the platform where the client application is executing. It will show you information similar to the following - using SQL Server Management Studio as an example:

Example 1 - collected on an Azure VM

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
spoolsv.exe	3100	TCPV6	[0:0:0:0:0:0:0:0]	49669	[0:0:0:0:0:0:0:0]	0	LISTENING
Ssms.exe	6224	TCP	10.11.2.6	50079	10.11.1.250	1433	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50088	10.11.1.250	1433	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50284	52.236.184.6	11035	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50288	52.236.184.6	11035	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50294	104.40.168.110	11041	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50296	52.236.184.6	11035	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50297	64.4.54.254	443	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50301	52.178.21.132	11034	ESTABLISHED
Ssms.exe	6224	TCP	10.11.2.6	50303	52.236.184.6	11035	ESTABLISHED
svchost.exe	692	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING

Check the `Remote Port` column - the lines with port 1433 are for a Managed Instance that is running in the same VNet as the client VM, whereas the lines with ports 11034/11035/11041 are for Azure SQL Databases in the West Europe region. The MI connections are using Proxy, the SQL Database connections are using Redirect.

Example 2 - collected on an on-premise VM

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
sqlbrowser.exe	2500	UDP	0.0.0.0	1434	*	*	
sqlbrowser.exe	2500	UDPV6	[0:0:0:0:0:0:0:0]	1434	*	*	
sqlceip.exe	3984	TCP	10.190.65.48	60828	10.190.65.48	2516	ESTABLISHED
sqlservr.exe	3828	TCP	0.0.0.0	2516	0.0.0.0	0	LISTENING
sqlservr.exe	3828	TCP	10.190.65.48	2516	10.190.65.48	60828	ESTABLISHED
sqlservr.exe	3828	TCP	127.0.0.1	57614	0.0.0.0	0	LISTENING
sqlservr.exe	3828	TCPV6	[0:0:0:0:0:0:0:0]	2516	[0:0:0:0:0:0:0:0]	0	LISTENING
sqlservr.exe	3828	TCPV6	[0:0:0:0:0:0:0:1]	57614	[0:0:0:0:0:0:0:0]	0	LISTENING
Ssms.exe	10788	TCP	10.190.65.48	49172	20.224.105.73	3342	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	59333	20.224.105.73	3342	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	61400	20.224.105.73	3342	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	60773	52.236.184.6	11035	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	60845	52.178.21.132	11034	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	60847	52.236.184.6	11035	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	60849	104.40.168.110	11041	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	60851	52.236.184.6	11035	ESTABLISHED
Ssms.exe	10788	TCP	10.190.65.48	60871	20.224.105.73	3342	ESTABLISHED
svchost.exe	872	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING

On the `Remote Port` column, the lines with ports 11034/11035/11041 are again for Azure SQL Databases in the West Europe region. The lines with port 3342 are for the same Managed Instance but using the public endpoint - note how the TCP address is different from Example 1.
Above the SSMS entries, you can also see the connections from a locally-installed SQL Server instance.

NETSTAT

Open an elevated command prompt (admin privileges) and execute `netstat -anob`. It will return information similar to TCPView, but without having to download any software. The output is unsorted and not as nice though:

```
C:\WINDOWS\system32>netstat -anob

Active Connections

  Proto  Local Address          Foreign Address        State           PID
(...)
  TCP    10.11.2.6:50079        10.11.1.250:1433       ESTABLISHED     6224
 [Ssms.exe]
  TCP    10.11.2.6:50088        10.11.1.250:1433       ESTABLISHED     6224
 [Ssms.exe]
  TCP    10.11.2.6:50250        52.167.107.67:443      ESTABLISHED     3572
 [HealthService.exe]
  TCP    10.11.2.6:50282        20.150.74.100:443      ESTABLISHED     3688
 [WindowsAzureGuestAgent.exe]
  TCP    10.11.2.6:50284        52.236.184.6:11035     ESTABLISHED     6224
 [Ssms.exe]
  TCP    10.11.2.6:50288        52.236.184.6:11035     TIME_WAIT       0
  TCP    10.11.2.6:50294        104.40.168.110:11041   ESTABLISHED     6224
 [Ssms.exe]
  TCP    10.11.2.6:50296        52.236.184.6:11035     TIME_WAIT       0
  TCP    10.11.2.6:50301        52.178.21.132:11034    ESTABLISHED     6224
 [Ssms.exe]
  TCP    10.11.2.6:50303        52.236.184.6:11035     ESTABLISHED     6224
 [Ssms.exe]
(...)
```

Check from the backend telemetry

Either check the ASC Troubleshooter or run the following Kusto query for the server and database:

```
let startTime = datetime(2022-06-03 12:00:00);
let endTime = datetime(2022-06-03 14:00:00);
let srv = "servername";
let db = "databasename";
MonLogin
| where TIMESTAMP >= startTime and TIMESTAMP <= endTime
| where logical_server_name =~ srv and database_name =~ db
| where event =~ "process_login_finish"
//| where is_success == 0 or total_time_ms > 14000
| extend ProxyOrRedirect = iif( result =~ "e_crContinue", "Redirect", iif( result =~ "e_crContinueSameState",
| project originalEventTimestamp, type, event, error, state, is_user_error, is_success, os_error, sni_error, s
| limit 3000
| order by originalEventTimestamp asc
```

You can see the connection policy on the `result` colum: "e_crContinue" means Redirect and "e_crContinueSameState" means Proxy.

More Information

Detailed description of the connection policy:
[Azure SQL Database connectivity architecture]
[Connection policy]

[Gateway IP addresses]

Blog article with a link to a connectivity PowerShell script:
[Lesson Learned #203: How can I know that my connection is using Redirect connectivity policy?]

How good have you found this content?