

# Gateway Upgrades

Last updated by | Vitor Tomaz | Dec 14, 2021 at 10:58 AM PST

## Gateway Upgrades

Tuesday, June 25, 2019  
10:50 AM

### Who is this change impacting?

All Azure SQL Database ( singleton-all SLOs, pools, DW) servers that rely on Gateway(CRs)

### What is changing? <INTERNAL ONLY>

Gen3 machines are being decommissioned across Azure and being replaced with Gen5 hardware which has much better hardware specs. As part of this we need to replace Gen3 CRs w

### How will the change be communicated to customers?

1. Update our IP address list with all the addresses available in each region.
2. Update release notes with why we are decommissioning the primary IP address and mitigation steps.
3. CXP shall email and portal toast customers by ~~subscription /region~~.

All these actions were done by 10/1/2019 and our aim is to start migration for external customers the week of 10/14

### Who will be impacted? i.e. what types of support cases to expect & their mitigation ?

This change will not impact any in-flight transactions or availability for your database. We shall gradually move traffic away from decommissioned Gateway to one of the other Gateway without impacting any existing connections that may still be using the decommissioned gateway. Any new connections will be serviced by one of the other Gateways.

### Errors customer may receive post migration -

#### Error #1

For example, if customer has firewall rules on-premises that depend on IP address of a specific Gateway or if customer is using a custom DNS server that resolves to a specific Gat this error message to be returned when a connection is attempted.

*"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 SQL Server is configured to allow remote connections."*

#### Mitigation for Error#1:-

We recommend that you allow outbound traffic to IP addresses for all the [Azure SQL Database gateway IP addresses](#) in the region on TCP port 1433, and port range 1100 firewall device. For more information on port ranges, see [Connection policy](#).

#### What to do if mitigation does not work?

Allow\_listing all IP addresses per our docs shall take care of Expected Error #1 . If that still does not work, engage Azure Networking team to look at why traffic may not be reach

#### Error #2

For customer using Microsoft JDBC driver lesser than V4.0, they can expect the following error

"A connection was successfully established with the server, but then an error occurred during the pre-login handshake. (provider: SSL Provider, error: 0 - The certificate's CN name passed value.)"

**Mitigation for Error #2** :- Ensure that the hostNameInCertificate property is set to \*.database.windows.net. For more information on how to set the hostNameInCertificate prop [with SSL Encryption](#).

Run the Kusto Query [<HERE>](#) to confirm driver version in use.

*(This should be a minority i.e. we only saw one customer when we did this in Australia data center. For this error confirm which version of JDBC the customer is using and suggest t latest version or implement the mitigation. If neither works then open an ICM with the Gateway team.)*

### How to check Control Ring / Gateway IP/ Connectivity

**<INTERNAL ONLY> - The goal of this migration is to decommission the Gen-3 hardware and migrate the traffic to new gen-5 hardware. The gateway nodes in CR1 are the or hardware and post migration this will change. You can do Nslookup on customer's server to confirm the CR location .**

**Using NSLookup.exe** (To find the control ring and Gateway IP)

```
C:\Users\subbuk>nslookup seahawks.database.windows.net
Server: DNV6Anycast1.corp.microsoft.com
Address: 2001:4898::1050:1050
```

Non-authoritative answer:

```
Name: cr2.centralus1-a.control.database.windows.net
Address: 13.67.215.62
Aliases: seahawks.database.windows.net
        dataslice2.centralus.database.windows.net
```

**Using PSping.exe (Check GW IP you are connecting to and successful connections)**

Post migration, this may fail for customer if they hardcode old (gen-3) Gateway IP's on the client FW rule. Mitigation is to update their FW rule with new.

```
C:\pstools>psping seahawks.database.windows.net:1433
```

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility  
Copyright (C) 2012-2016 Mark Russinovich  
Sysinternals - [www.sysinternals.com](http://www.sysinternals.com)

```
TCP connect to 13.67.215.62:1433:
5 iterations (warmup 1) ping test:
Connecting to 13.67.215.62:1433 (warmup): from 172.30.172.127:1778: 42.50ms
Connecting to 13.67.215.62:1433: from 172.30.172.127:1779: 43.55ms
Connecting to 13.67.215.62:1433: from 172.30.172.127:1780: 42.71ms
Connecting to 13.67.215.62:1433: from 172.30.172.127:1782: 42.90ms
Connecting to 13.67.215.62:1433: from 172.30.172.127:1783: 42.94ms
```

**Variation of the above problem statement:-**

CVS has multiple Prod and Dev environments in each region. How can they confirm that all IP addresses are reachable from their clients?

I suggested that they can do Psping to all the IP addresses in a region like this

```
psping 104.42.238.205:1433
```

PsPing v2.10 - PsPing - ping, latency, bandwidth measurement utility  
Copyright (C) 2012-2016 Mark Russinovich  
Sysinternals - [www.sysinternals.com](http://www.sysinternals.com)

```
TCP connect to 104.42.238.205:1433:
5 iterations (warmup 1) ping test:
Connecting to 104.42.238.205:1433 (warmup): from 100.64.135.245:58330: 61.21ms
Connecting to 104.42.238.205:1433: from 100.64.135.245:58331: 32.16ms
```

**Azure SQL DB Connectivity Checker tool**

In addition, please use the connectivity check tool [Azure SQL DB Connectivity Checker](#) to test connectivity to all the SQL DB gateways existing on the region where th located.

**ASC Insight - (Pending Prod)**

(ASC diagnostics will match customer subscription/resource (server) to confirm and generate the insight ONLY for the impacted customer's resource. )

Step 1 : Check if ASC generated insight for this customer resource. If GW migration insight not generated for this resource, then the issue is not related to GW Migration.

**Sample insight**

SQL DATABASE  
Server migrated to different IP

SQL SERVER DATABASE  
LIBRARY

Is this insight helpful? 🗲️ 🗲️

**Description**

Server seahawks has migrated to a new control ring on 2019-10-03 08:21:39.797. Hence the FQDN seahawks.database.windows.net now resolves to a different Gateway IP address. Customers may experience connectivity issues under one/more of the following conditions:

- If they hard code any of the old IP address list of gateway IP addresses as part of their outgoing firewall rules on their client machines or on-premises firewall.
- If they have any subnets using Microsoft.Sql as a Service Endpoint but cannot communicate with the Gateway IP address?
- If they have any clients connecting with old/legacy JDBC drivers (Microsoft JDBC Version (4.0, JTD5)?

**Impacted Resources**

Library

**Recommended Action**

Server seahawks has migrated to a new control ring on 2019-10-03 08:21:39.797, please review the [login trend \(SQL Troubleshooter -> Connectivity -> Summary -> Login Trend Summary\)](#) for post migration successful connections to this server seahawks.

If successful connections were noticed after the migration time 2019-10-03 08:21:39.797, then issue is NOT related to Gateway Migration. Please continue investigating the ticket by following standard troubleshooting steps to handle customer's connectivity issue.

However, if NO successful connections noticed after migration, follow the below steps depending to help customer depending on the condition(s) applicable:

1. If customer hard code any of the old IP address list of gateway IP addresses as part of their outgoing firewall rules on their client machines or on-premises firewall.  
Solution: Allow outbound traffic to IP addresses for all the Azure SQL Database gateway IP addresses in the region on TCP port 1433, and port range 11000-11999 on their firewall configuration.
2. Have any subnets using Microsoft.Sql as Service Endpoint but cannot communicate with the Gateway IP addresses?  
Solution: Customers may choose to put restrictive NSG rules on the subnet (or on an Azure VM within the subnet) and only open traffic to, say CR1, on ports 1433, 11000-11999; in which case their connections would be blocked by NSG if we move them to CR2/CR3 since they are on a different IP address. The customer needs to update their NSGs with this new IP address.
3. Connecting with Old/Legacy JDBC Driver  
Solution: Ensure that the hostNameInCertificate property is set to \*.database.windows.net. For more information on how to set the hostNameInCertificate property, see [Connecting with SSL Encryption](#).  
Run the Kusto query from TSG Link to confirm the JDBC driver version in use and recommend customer to update their driver version to JDBC 4.0.

Please use this TSG for additional information related to gateway migration and for using tools to confirm the control ring and server availability to help customer(s)

If the above recommendations doesn't help resolve the issue, reach out to Product group via bridge on active ICM Incident 14773730. Also update this ICM with the ongoing support ticket.

**Customer Ready Content**

[Copy Content](#) [New Email](#)

Between 2019-10-07 18:50:00 UTC and 2019-10-08 19:10:00 UTC, server seahawks was unreachable, and issue is related to recent migration of traffic connections to newer gateways in this region. This migration will change the public IP address that DNS resolves for database Library on server seahawks.

For further information, please refer to the documentation present in the link below.

**Recommended Steps**

- Retry connecting to the database after a few minutes
- Ensure that you do not have any outgoing firewall rules restrictions in your environment

**Recommended Documents**

- Gateway Migration to new hardware

**Links**

ICM 149773730: Gateway Migration Active bridge  
Gateway Migration to new hardware  
Connection policy for Azure SQL Database  
Azure SQL Database gateway IP Addresses  
Psping tool

**Generated On**

Oct 11, 2019 3:40:50 PM

Step 2 : If insight generated for customer's resource, follow the Recommended Action to assist customer.

Ensure to check Migrated timestamp and review post migration login trend for customer resource. (SQL Troubleshooter -> Connectivity-> Summary -> Login Trend graph). connection noticed after migration, then the issue is not related to GW migration.

OR

If for some reason, troubleshooter is slow or not able to get the login trend from connectivity please use the kusto query to check the login trend.

MonLogin

```
| where logical_server_name =~ {ServerName} and database_name =~ "DatabaseName"
| where TIMESTAMP >= (use the migrated_datetime - from the ASC Insight)
| extend logical_server_name = tolower(logical_server_name), database_name = tolower(database_name)
| where event=="process_login_finish"
| summarize sum_nb_connection_accept_finish= sum(iff(is_success == 1 and (package=="sqlserver" or package=="mpdw"), 1 , 0))
, sum_nb_connection_accept_only = toint(0)
, sum_nb_connection_accept_failure = toint(0)
, sum_nb_connection_accept_failure_finish = sum(iff(is_success == 0 and is_user_error == 1, 1 , 0))
, sum_nb_connection_accept_failure_finish_is_system_error = sum(iff(is_success == 0 and is_user_error == 0, 1 , 0))
by TIMESTAMP, logical_server_name, database_name //bin = 60
| extend total_succeed = sum_nb_connection_accept_finish
| extend total_failures_system_error = sum_nb_connection_accept_only + sum_nb_connection_accept_failure + sum_nb_connection_accept_failure_finish_is_system_err
| extend total_failures_user_error = sum_nb_connection_accept_failure_finish
| extend total_logins = total_succeed + total_failures_system_error + total_failures_user_error
| project TIMESTAMP,
['Total Logins']=total_logins,
['Failed Logins Due to System Error']=total_failures_system_error,
['Failed Logins Due to User Error']=total_failures_user_error
| sort by TIMESTAMP asc
| render timechart
//QueryName:'Login Trend'
```

Step 3: Depending on customers scenario listed in CSS Ready content follow the recommendations to help customer.

In addition, make use of NSLookup and PSPing tools to confirm the CR location GW IP and Connectivity for customer.

**How good have you found this content?**



-