Baltimore root CA change Plan

Last updated by | Lisa Liu | Nov 6, 2020 at 10:34 AM PST

As a part of the Baltimore Root CS retired process , Baltimore Root (SSLAdmin) certificates are being revoked on 10/26, so we will change the root CA of Gateway service for MySQL/PostgreSQL/MariaDB. You remember in the SSL documentations we have a step asking the customer to download a Baltimore CA cert for SSL connections:

PostgreSQL:

https://docs.microsoft.com/en-us/azure/postgresql/concepts-ssl-connection-security

Due to the root CA change, the customer will need to change their root CA to the new one. The rotation process will be.

1. We will send the notification/instruction to all the customer who is using the SSL and ask them to update their application to trust both new and old CA.

2. We will rotate the gateway CA at 10/26. Assuming the customers have all updated their applications, so they won't be broken.

3. After 10/26. The customer can update their application to trust the new CA only, but this is an optional step.

The #1 is currently ongoing, including the email, portal and selfhelp communication, we expected the notification will be sent out in recent days. We also expected to receive related cases/questions when customer see this notification.

The information below contains some canned email notification as part of the customer communications and other FAQs and details that will be useful for us :

Baltimore root CA change Plan

Background

You are receiving this email since you are using Azure Database for PostgreSQL. Azure Database for <engine-name> will be changing the if the client application/driver enabled the will be set to expire starting November 30th 2020 as part of standard maintenance and security best practices for running your database workloads on Azure. This article gives you more details about the upcoming changes, what are the resources getting affected and what are the steps needed to ensure that your application maintains connectivity to your database server. the upcoming changes, what are the resources getting affected and what are the steps needed to ensure that your application maintains connectivity to your database server. gives you more details about the upcoming changes, what are the resources getting affected and what are the steps needed to ensure that your application maintains connectivity to your database server. the upcoming changes, what are the resources getting affected and what are the steps needed to ensure that your application maintains connectivity to your database server.

What update is going to happen?

In some cases, applications use a local certificate file generated from a trusted Certificate Authority (CA) certificate file to connect securely. Currently customers can **only use** the predefined certificate to connect to an Azure Database for PostgreSQL server which is located at https://www.digicert.com/CACerts/BaltimoreCyberTrustRoot.crt.pem. However, Certificate Authority (CA) Browser forum recently published reports of multiple certificates issued by CA vendors that are used by our customers, Microsoft, and the greater technology community that were out-of-compliance with industry standards for publicly trusted CAs. The reports regarding the non-compliant CAs can be found here:

1. Bug 1649951
2. Bug 1650910

As per the industry's compliance requirements, CA vendors began revoking non-compliant CAs and issuing compliant CAs. This requires client application using these certificates re-issued and updated. Since Azure Database for PosrgreSQL leverages one of these non-compliant certificates to validation of client application using SSL, we need to ensure that appropriate actions are taken (described below) to minimize the potential impact to Azure Services.

The new certificate will be used starting December 1st, 2020. If you use full validation of the server certificate you need to update your application configuration before December 1st, 2020.

How do I know if my database is going to be affected?
All application that use SSL/TLS and verify the root certificate need to update the root certificate in order to connect to Azure Database for PostgreSQL. If you are not using SSL/TLS currently, there is no impact to your application availability. You can verify if your client application is trying to use SSL mode with the predefined trusted Certificate Authority (CA) here.
To avoid your application's availability being interrupted due to certificates being unexpectedly revoked, or to update a certificate which has been revoked, please refer to the "**What do I need to do to maintain connectivity"** section.

What do I need to do to maintain connectivity?
To avoid your application's availability being interrupted due to certificates being unexpectedly revoked, or to update a certificate which has been revoked, follow the steps below:

1. Download BaltimoreCyberTrustRoot & DigiCertGlobalRootG2 Root CA from links below:
   - https://www.digicert.com/CACerts/BaltimoreCyberTrustRoot.crt.pem
   - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem
2. Generate a combined CA certificate store with both BaltimoreCyberTrustRoot and DigiCertGlobalRootG2 certificates are included.

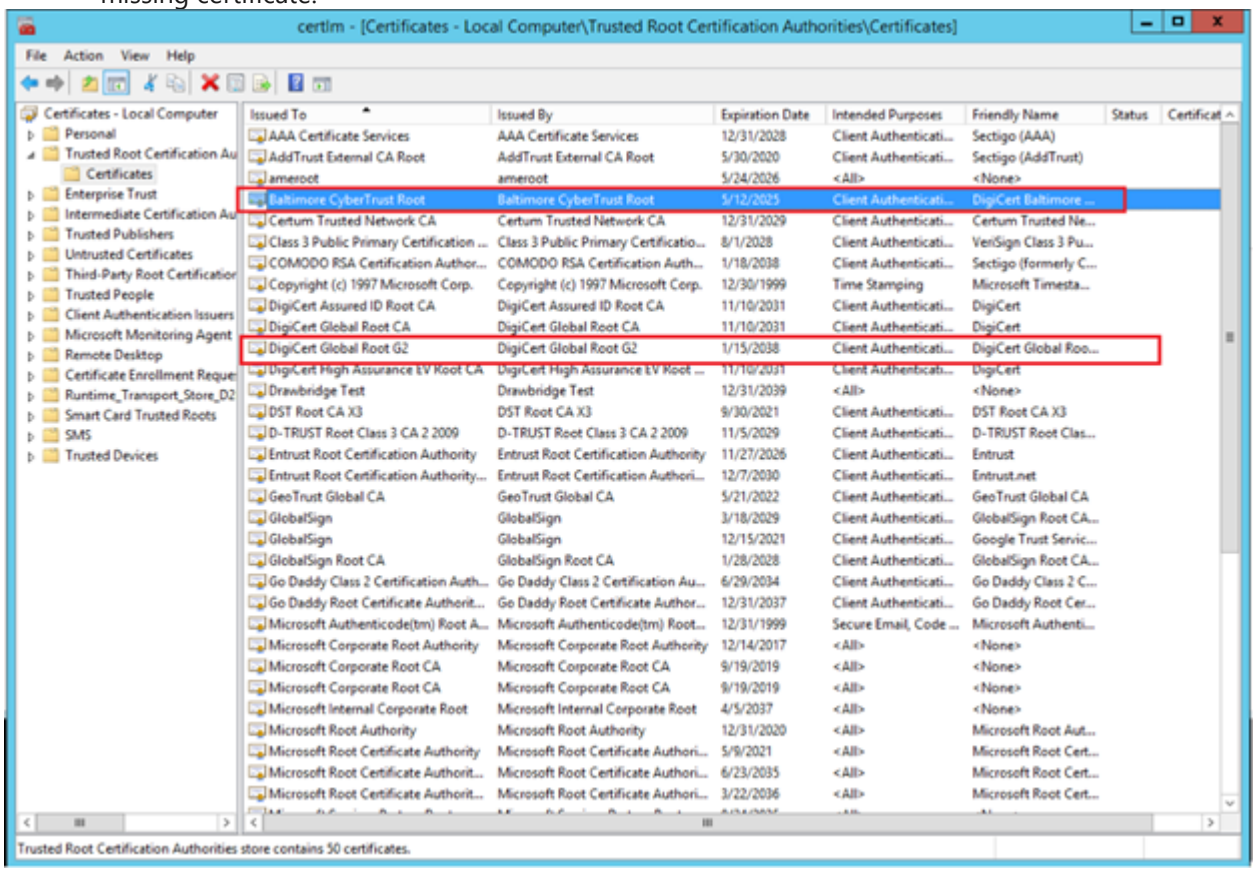
2.1 For Java connector users, execute:

```
keytool -importcert -alias postgresServerCACert  -file D:\BaltimoreCyberTrustRoot.crt.pem  -
keystore truststore -storepass password -noprompt
keytool -importcert -alias postrgresServerCACert2  -file D:\DigiCertGlobalRootG2.crt.pem -
keystore truststore -storepass password  -noprompt
```

Then replace the original keystore file with the new generated one:

```
System.setProperty("javax.net.ssl.trustStore","path_to_truststore_file");
System.setProperty("javax.net.ssl.trustStorePassword","password");
```

2.2 For .NET (e.g npgsql) users, make sure BaltimoreCyberTrustRoot and DigiCertGlobalRootG2 both exist in Windows Certificate Store, Trusted Root Certification Authorities. If any certificates do not exist, please import the missing certificate.



2.3 For other (PostgreSQL Clients) PGadmin/C/C++/Go/Python/Ruby/ ..) users, you can merge 2 CA certificate files like this format below:

-----BEGIN CERTIFICATE-----
(Root CA1: BaltimoreCyberTrustRoot.crt.pem)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Root CA2: DigiCertGlobalRootG2.crt.pem)
-----END CERTIFICATE-----

3. Replace the original root CA pem file with the combined root CA file and restart your application/client.
4. After the new certificate deployed on the server side, you can change your CA pem file to DigiCertGlobalRootG2.crt.pem.

What can be the impact?

If you are using the Azure Database for PostgreSQL issued certificate as documented here, your application's availability might be interrupted since the database will not be reachable. Depending on your application, you may receive a variety of error messages including but not limited to:

1. Invalid certificate/revoked certificate
2. Connection timed out.
3. <Other error if applicable>

FAQ

1. **If I am not using SSL/TLS, do I still need to update the root CA?**

No actions required if you are not using SSL/TLS.

2. **If I am using SSL/TLS, do I need to restart my database server to update the root CA?**

No. You do not need to restart the database server to start using the new Certificate. This is a client-side change and the incoming client connections need to use the new certificate to ensure that they can connect to the database server.

3. **What will happen if I do not update the root certificate before 30th November?**

If you do not update the root certificate before November 30th, 2020, your applications that connect via SSL/TLS and does verification for the root certificate will be unable to communicate to the PostgreSQL database server and application will experience connectivity issues to your PostgreSQL database server.

4. **Do I need to plan a maintenance downtime for this change?**

No. Since the change here is only on the client side to connect to the database server, there is no maintenance downtime needed here for this change.

5. **What if I cannot get a scheduled downtime for this change before Nov 30st?**

6. **If I create a new server after Nov 30th, will I be impacted?**

For server created after Nov 30th, you can use the newly issued Certificate to for your application to connect using SSL.

7. **How often does Microsoft update their certificates or what is the expiry policy?**

8. **If I am using read replicas, do I need to perform this only on master server or all the read replicas?**
9. **Do we have server-side query to determine the client connections coming in using this certificate?**

10. **What if I have further questions?**

If you have questions, get answers from community experts in Microsoft Q&A. If you have a support plan and you need technical help, please contact us.

How good have you found this content?