

Public_Preview_Enrollment_process_and_Public_Docs

Last updated by | Lisa Liu | Nov 6, 2020 at 10:35 AM PST

Contents

- [Issue](#)
- [More Information](#)
 - [CSS procedure to onboard customers](#)
- [Public Doc Reference](#)
 - [Azure Database for PostgreSQL Single server data encrypti...](#)
 - [Data encryption for Azure Database for PostgreSQL Single ...](#)
 - [Data encryption for Azure Database for PostgreSQL Single ...](#)
 - [Validating data encryption for Azure Database for PostgreS...](#)
 - [Azure Database for MySQL data encryption with a custom...](#)
 - [Data encryption for Azure Database for MySQL by using th...](#)
 - [Data encryption for Azure Database for MySQL by using th...](#)
 - [Enable BYOK using ARM Template](#)
 - [Azure Key Vault Analytics solution in Azure Monitor](#)

Issue

Customer wants to be enrolled for the Public Preview for BYOK (PostgreSQL (Single Server) and MySQL. This is available for PFS Servers only if customer wants to enable this on existing Servers

You can check in the ASC if it is PFS Server

Q

Case OverviewCustomerToolsResource ExplorerTenant ExplorerAppLens

Drag a column header and drop it here to group by that column	
PropertyName	PropertyValue
<div></div>	
> Elastic Server Edition	MemoryOptimized
> Sandbox Package Version	13.1.20200308.2-orcshr-35d4a50c
> Memory Limit (GB)	320
> Storage Host Name	file.bn8prdstf01a.store.core.windows.net
> Storage Type	Premium File Share
> Storage Tier, MBPS	
> IOPS Limit	6000
> Storage Limit (MB)	2048000
> <u>BYOK Enabled</u>	-1
> <u>Double/Additional Infrastructure-encryption Enabled</u>	0
> Enable Storage Auto Grow	1
> Enable SSL Enforcement	
> Blob Storage Account Name	
> Full Blob Storage Account Name	
> Blob Storage Container Name	

More Information

This is currently not available for Citus Hyperscale or MariaDB

CSS procedure to onboard customers

The customer can send a request with his subscription to AskAzureDBforPostgreSQL@service.microsoft.com or we can send the same to "Manish Kumar manishku@microsoft.com" to onboard the customer

The Public Preview is expected to go live on June 7th

1. If you receive a request from your customer Send the onboarding instructions to the customer: [Customer-facing onboarding instructions for BYOK](#)

2. **Request approval to whitelist**

Request enrollment from engineering

Request enrollment from the engineering team by following these steps:

- Create ICM for engineering using this template: <https://icm.ad.msft.net/imp/v3/incidents/create?tmpl=74k2v3>
 - ☑
 - This template will help providing the following information in the request:
 - Subscription ID
 - Region(s) where they plan to
 - Please note that providing Regions where they are deployed will expedite whitelisting.
 - Severity of the incident: 3 (**never a Sev2**)
 - Customer SLA impact: Yes (this is CRI - Customer Raised Incident)
 - Cloud instance: chose Public (assumed EA subscriptions are in the public cloud)
 - Click on the next
 - Optionally: Fill out optional details
 - Submit the request
 - Record the ICM request number generated by the system in the service desk
- Please inform in an email TO: **manishku** and **sarora**, and CC AskAzureDBforPostgreSQL@service.microsoft.com asking for PG enrollment approval. Please include customer name and subscription ID , ICM Number in the email.
- Wait for confirmation from engineering that this customer has been whitelisted
 - **Yes:** Check if the engineering has successfully whitelisted the customer through watching the ICM request. If yes, proceed onto the next step.
 - **No response:** Please do not reach out to engineering directly via email or through Teams for a follow up. Please use ICM exclusively to communicate the status of whitelisting with engineering until the process is completed.

3. **Send acceptance to the customer**

- Send the acceptance instructions to the customer: [Get-started-with-BYOK-public-preview](#)

4. **Close the case**

- Check with the customer if they are happy?
- Need help with troubleshooting issues?
 - Follow the troubleshooting guides available in this section.

- Close the request

Public Doc Reference

Azure Database for PostgreSQL Single server data encryption with a customer-managed key

<https://docs.microsoft.com/en-us/azure/postgresql/concepts-data-encryption-postgresql#restore-and-replicate-with-a-customers-managed-key-in-key-vault> 

Data encryption for Azure Database for PostgreSQL Single server by using the Azure portal

<https://docs.microsoft.com/en-us/azure/postgresql/howto-data-encryption-portal> 

Data encryption for Azure Database for PostgreSQL Single server by using the Azure CLI

<https://docs.microsoft.com/en-us/azure/postgresql/howto-data-encryption-cli> 

Validating data encryption for Azure Database for PostgreSQL

<https://docs.microsoft.com/en-us/azure/postgresql/howto-data-encryption-validation> 

Azure Database for MySQL data encryption with a customer-managed key

<https://docs.microsoft.com/en-us/azure/mysql/concepts-data-encryption-mysql> 

Data encryption for Azure Database for MySQL by using the Azure portal

<https://docs.microsoft.com/en-us/azure/mysql/howto-data-encryption-portal> 

Data encryption for Azure Database for MySQL by using the Azure CLI

<https://docs.microsoft.com/en-us/azure/mysql/howto-data-encryption-cli> 

Enable BYOK using ARM Template

<https://docs.microsoft.com/en-us/azure/postgresql/howto-data-encryption-cli#using-an-azure-resource-manager-template-to-enable-data-encryption> 

Azure Key Vault Analytics solution in Azure Monitor

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/azure-key-vault> 

How good have you found this content?

