

Azure Database for PostgreSQL 15: Essential Standards for Compliance and Security

Standards for secure and compliant PostgreSQL deployments in Azure





Taiob Ali

Database Solutions Manager @ GMO | Microsoft MVP | Global Data Solutions Leader | Cloud & Al Advocate

Let's connect and collaborate:

- Iinkedin.com/in/sqlworldwide
- sqlworldwide.com
- taiob@sqlworldwide.com
- @sqlworldwide.bsky.social













Agenda

6

Why Standardize?

The importance of consistent PostgreSQL configurations

Essential Standards Key requirements for compliance and security

Implementation Approaches Practical deployment using Azure Policy and automation



Why Standardize?

> Enhanced Security

Protect sensitive data



Regulatory Compliance

Meet industry requirements



Operational Consistency

Reduce configuration drift



Automation Friendly

Enable infrastructure as code



Login

Login

Secure Your Infrastructure

Real-time insights and control for your critical systems.

Request demo



N =

Workload Type

Development

For non-production servers

Production

Customizable

Can modify compute, storage, HA from default

For all production servers

Workload Type: Standards

Standard

- Development for non-prod
- Production for all production servers

Implementation

- Preferable: Enforce during creation
- Azure Policy will work





Workload Type: Learn More

•	

Documentation

Microsoft Learn guides

Compute and Storage Concepts



Sample Policies

Ready-to-use templates

Server Creation Quickstart Guide

Tags



Required tags: ApplicationId, Environment

Tags: Standards

P

 \bigcirc

Required Tags

ApplicationId and Environment

逊

Enforcement

Azure Policy for compliance

Reporting

Resource organization and billing



Tags: Learn More





Maintenance Schedule



Custom schedule

Maintenance Schedule: Standards

Environment	Recommended Setting
Non-production	System-managed
Production	Custom schedule
Implementation	Azure Policy





Maintenance Schedule: Learn More

Documentation

Comprehensive guide

View documentation

Minimum between system and custom

Days

Learn about windows

Typical maintenance duration



Minutes

Read about impact

Backup Retention





Backup Retention: Standards

Standard

- Non-Production: \bullet Zero retention
- Production: Based on ulletrequirements
- Consider compliance ulletneeds

Implementation

- **Azure Policy** •
- **Azure Functions**

821-000

70.1007

2933076

90:007

Database Backup Retention Timeline



Backup Retention: Learn More



Documentation

Bcø

Comprehensive guide

View documentation

Policy Templates Enforcement examples Explore templates



Backup Redundancy

Zone-redundant

Default if region supports

Locally redundant

Default if zone not supported

Geo-redundant

Only at server creation



Azure PostgreSQL **Backup Redundancy**

Locally Redundant

Geo Redundant

Backup Redundancy: Standards



Configuration Geo-redundant ONLY at creation time



Backup Redundancy: Learn More







Resource Lock

Delete Lock

Prevents accidental deletion

Read-only Lock

Prevents modifications

Resource Lock: Standards

Production Requirement Mandatory for all production DBs

Implementation

Azure Policy enforcement

 \Rightarrow

ഫ

Exception Process

Documented approval workflow



Resource Lock: Learn More





Documentation

Official Microsoft guidance

View documentation



ARM Templates Deployment examples Explore templates

Compute Tier



General Purpose

Balanced CPU/memory ratio



Memory Optimized

Higher memory-to-CPU ratio



Burstable

- No zone redundancy •
- No read replicas ullet

Not recommended for production

Compute Tier: Standards

Standard

- No Burstable tier for ullet**Production Workload**
 - Lacks zone redundancy ullet
 - No read replica ulletsupport

Implementation

- **Azure Policy** •
- Audit non-compliant •
 - servers

General Purpose

Azure Database for PostgreSQL **Compute Tiers**



Memory Optimizred



Compute Tier: Learn More

3

Compute Tiers

Burstable, General Purpose, Memory Optimized

96

Max vCores

Available in General Purpose and Memory

Optimized tier

Available in General Purpose and Memory

Compute options in Azure Database for PostgreSQL flexible server

672

Max Memory (GB)

Optimized tier

S Everscale

4,00

Sdutions

Storage Auto-growth

34.90

200

Automatic Scaling

Grows as needed



Configurable

On or Off

000

Monitoring

Track growth patterns

 \bigotimes Scalability Security

Automated Database Growth

66.00		
	6,00	7
		20.700**
	ZEĽ	



Cost Optimization

Storage Auto-growth: Standards





Storage Auto-growth: Learn More

Þ

Documentation

Official guidance

View documentation

Storage options

Storage configuration guide

(+-

Monitoring

Storage used

Monitoring resources

\mathbf{D}

Enhanced Metrics



Enhanced metrics provide deeper insights for production environments

Enhanced Metrics: Standards

Standard

- On for production
- Optional for non-production

Implementation

- Azure Policy
- Azure Functions



Enhanced Metrics: Learn More

Enabling Enhanced Metrics

Step-by-step guide for activating enhanced monitoring

View documentation

Available Metrics

Complete list of metrics available for PostgreSQL

View documentation

Visualization Tools

visualize metric data

View documentation

- How to create dashboards and

Diagnostic Settings

Azure diagnostic settings enable monitoring and analysis of your PostgreSQL server operations

Data Collection

Configure which server logs and metrics to capture for analysis and compliance

Destination Options

Send data to Log Analytics, Storage Account, or Event Hub for flexible processing

Retention Control

Set appropriate retention periods for historical data based on your requirements

Diagn	ostic sett
Save	× Discard
A diagnosti and one or more about	c setting specifie more destination t the different log
Diagnostic	setting name *
Logs 2 Category	groups ① udit
Categorie	es
	PostgreSQL Serve
	PostgreSQL Sessi
<u>~</u>	PostgreSQL Quer
~	PostgreSQL Quer
<u>~</u>	PostgreSQL Auto
	PostgreSQL rema



er Logs

ions data

ry Store Runtime

ry Store Wait Statistics

ovacuum and schema statistics

aining transactions

Diagnostic Settings: Standards





0 Descent Br Descent Bill Distance Bill Distance Bill Distance	Advertise Accessed	process processing to the same relation of		
	ALLA Address (Andress Address (Andress (Andress Address (Andress Address (Andress (Andress Address (Andress (Andress (Andress Address (Andress (Andress (Andress (Andress Address (Andress (Andres	215 MB 1984	Proper Bana Para Unione Annual	
	Inits inclustication and an analysis of the second	n Distant Shapel Data Race Malates S (12) Dist data sejatar dES Methoda PAC gas a hasal sejatar dES distant setatu (14) distant setatu (14) distant setatu (14) distant setatu (14) distant setatu (14) distant setatu (14)	regenere Tonoscources ne Detadoun or Welgene Near and mar Insigni & 19 y here Promotionary Near and real-responde & 10 y here anno real near-responde table i in the anno real performant table i in the anno performant table in the	Maria Balanta Salanta Maria Maria Maria Maria Maria Maria Maria Maria Maria Balanta Maria Balanta Maria Balanta Maria Balanta

Diagnostic Settings: Learn More

$\left(\right)$	~~~	
	<u>Selys</u>	
	U	

Configuration Guide

Official documentation



Analysis Resources

Monitoring and tuning



Server Logs



- Server logs capture detailed insights about the activities that run on your servers.
- You can use major version upgrade logs to troubleshoot errors that might occur during an attempt to upgrade your server to a higher major version of PostgreSQL.

O. Bea

A Sia

B Pox

8 kve

Server Logs: Standards

Enable for Production

- Default retention is 3 days
- Can adjust between 1 and 7 days
- Can download by time and log type
- Readable with most text editors

		Postg	reS	QI
x	S.	moing kurret	ior.at	πho
		Ailoce	R¢.	8,2
IS	*	H6.00		
ocs				
sus		9.00		
			-	
		-		
		Innarnee	ed Repa	vtiba
		\$4,0312		-
оте		\$4,0313		3

PostgreSQL Log Monitoring

Log			BY Patues 2milit	anone
dicon:clors				
1210 0.45	11565		Me	SSSCOS
			295 fontarikt oversit dits	
			- 4,401912	+
/		0	EVOTERO HOLOL DIGRHOS	
			+ \$11, 20912	+
			ET-ROMERCEARING REFORMER	90 .
			4,7332	+
ms		\$61 72%	Omnano A 212	2
agentications	#1501263 20111501W0	4111		
37N 🖗	-\$23,3995	\$.274	*312	



Server Logs: Learn More



Configuration Guide

Official documentation



Download Steps

How to Download Logs



High Availability



These components form the foundation of our PostgreSQL high availability architecture, ensuring business continuity and minimal downtime.

High Availability: Standards



Read Replicas for high traffic

Geo-redundant backups or Bring up Read Replica as Primary



High Availability: Learn More

Availability Zone Support

Deploy across multiple zones for 99.99% uptime and protection against datacenter failures. Standby is automatically provisioned in a different zone.

Performance Considerations

Zone-redundant configurations may experience slightly higher latency (typically 1-2 ms) due to cross-zone data synchronization.

Learn more

Disaster recovery in multi-region geography

Learn more

Learn more

Geo-redundant backup and restore

Authentication Mode



Entra Authentication

Preferred authentication

PostgreSQL Authentication

 \mathcal{L}

Only by exception



Authentication Mode: Standards





Authentication Mode: Learn More



Official guidance on Entra ID authentication

Configuration

Step-by-step setup instructions

Security Benefits

 \mathcal{S}

Enhanced protection features





Private Endpoint







Enhanced Security

Minimize risk of data breaches

Data Protection

Access from approved VNets

Regulatory Compliance Data isolated from public internet

Private Endpoint: Standards

Standard

- Mandatory for all servers •
- Public access disabled ullet

Implementation

- **Azure Policy** •
- **Enforce during creation** •
- Audit existing servers •



Private Endpoint: Learn More

Documentation

Official guidance on <u>private</u> endpoints

Configuration

♥,7J ©∮

Step-by-step setup instructions



Defender for Cloud

Defender for Cloud

Threat Protection

Detect unusual access

Suspicious Activity

Identify security gaps

Investigate and mitigation Recommendations

Actionable guidance

	-	
		8.
: !!!!!!!!!!		8.
:	*	9.0
		8
•	-	
	*	
: .	-	
	*	10

Defender for Cloud: Standards



Coverage

Required for all databases

\$15

Cost

Monthly per server

24/7

Monitoring

Continuous protection

Defender for Cloud

100% Coverage

24/7Monitoring

Automated Response



Defender for Cloud: Learn More



Official guidance on Microsoft Defender for Cloud

Configuration

2

3

Setup instructions for **Defender for Cloud**

Monitoring

Alert management in <u>Security Operations</u>



Implementation Approaches







Thank You!



LinkedIn

linkedin.com/in/sqlworldwide

Blog

sqlworldwide.com

Email



Bluesky

@sqlworldwide.bsky.social

GitHub

github.com/sqlworldwide

Questions?

taiob@sqlworldwide.com

Happy to discuss further