PASS Data Community Summit

Host redgate

Best Practices and Compliance for Azure Database for PostgreSQL

Taiob Ali

He/Him

Database Solutions Manager

GMO LLC

Taiob Ali

He/Him

Database Solutions Manager
GMO LLC

I am a Microsoft Data Platform MVP with over 19 years of experience designing and implementing data solutions across finance, e-commerce, and healthcare. My expertise encompasses the Microsoft Data Platform, MongoDB, Azure AI, and Python, enabling data-driven innovation.

As a community advocate, I've presented at over 100 events worldwide, including SQL Saturdays, Data Saturdays, and international conferences. I founded the Database Professionals Virtual Meetup Group, serve on the New England SQL Server User Group, and the SQL Saturday boards.

@sqlworldwide

sqlworldwide

https://sqlworldwide.com

Your feedback is important to us

Evaluate this session at:

passdatacommunitysummit.com/evaluations

Why Standardize?

- Protect sensitive data
- Meet industry requirements
- Operational Consistency
- Enable automation through Infrastructure as Code (IaC)

Workload Type

- Dev/Test Default
  - Compute: Burstable
  - Compute size: Standard_B2s
  - Does not support High Availability
- Production Default
  - Compute: General Purpose
  - Compute size: Standard_D4ds_V4
  - High Availability (Zonal resiliency) Enabled with fallback unchecked

The Burstable compute tier is optimized for dev/test workloads. For production use, we recommend General Purpose or Memory Optimized tiers

Recommendation

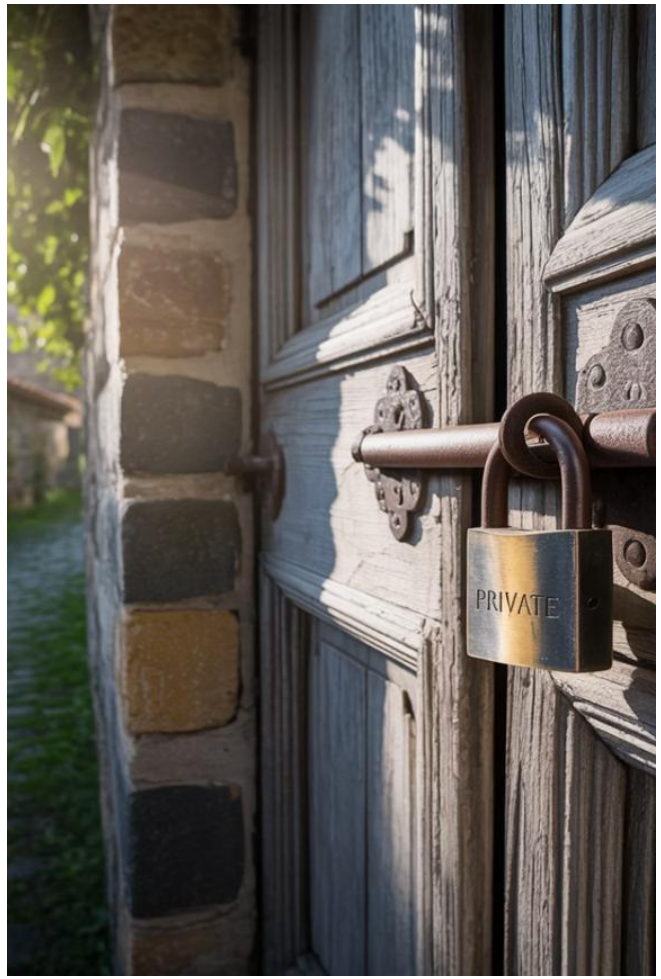
- Dev/Test for Non-production workloads
- Production for Production workloads
- Enforce this during deployment using Azure Policy

Authentication Method

- PostgreSQL authentication only
- Microsoft Entra authentication only
- PostgreSQL and Microsoft Entra authentication (Default)

Recommendation

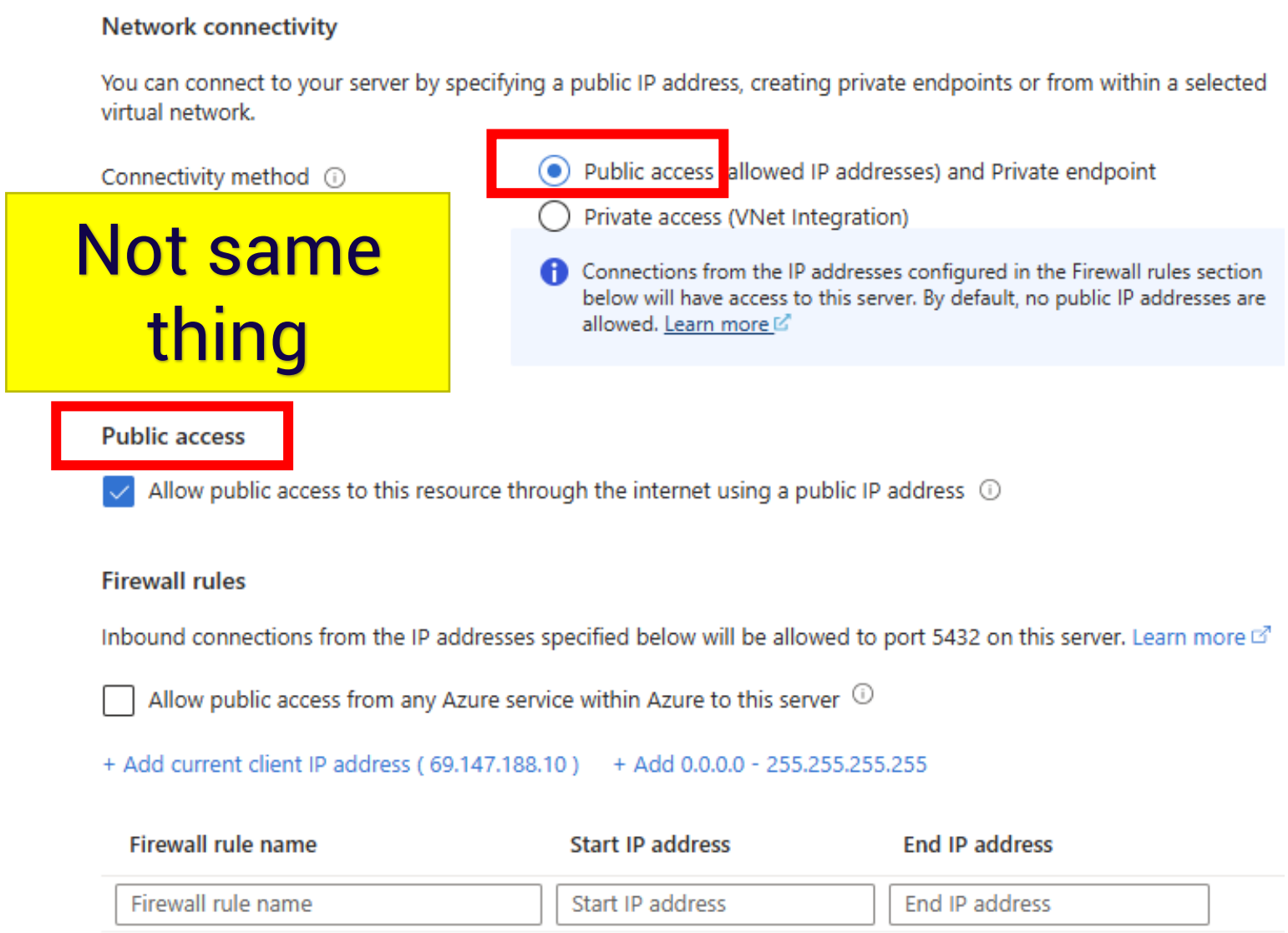
- Use “Microsoft Entra authentication only”
- Use managed identities for secure application access
- If you must use local authentication:
  - Ensure strong password policies
  - Regular password rotation
  - Use SCRAM authentication only
- Achieve compliance with Azure Policy



Network Connectivity

- Public access (allowed IP addresses) and Private endpoint
  - Enable public access
    - Configure firewall rules
    - Allow access from Azure Services
  - Disable public access
    - Create private endpoint (PE) as Connectivity is only possible via PE
- Private access with (VNET Integration)
  - Azure Private DNS integration

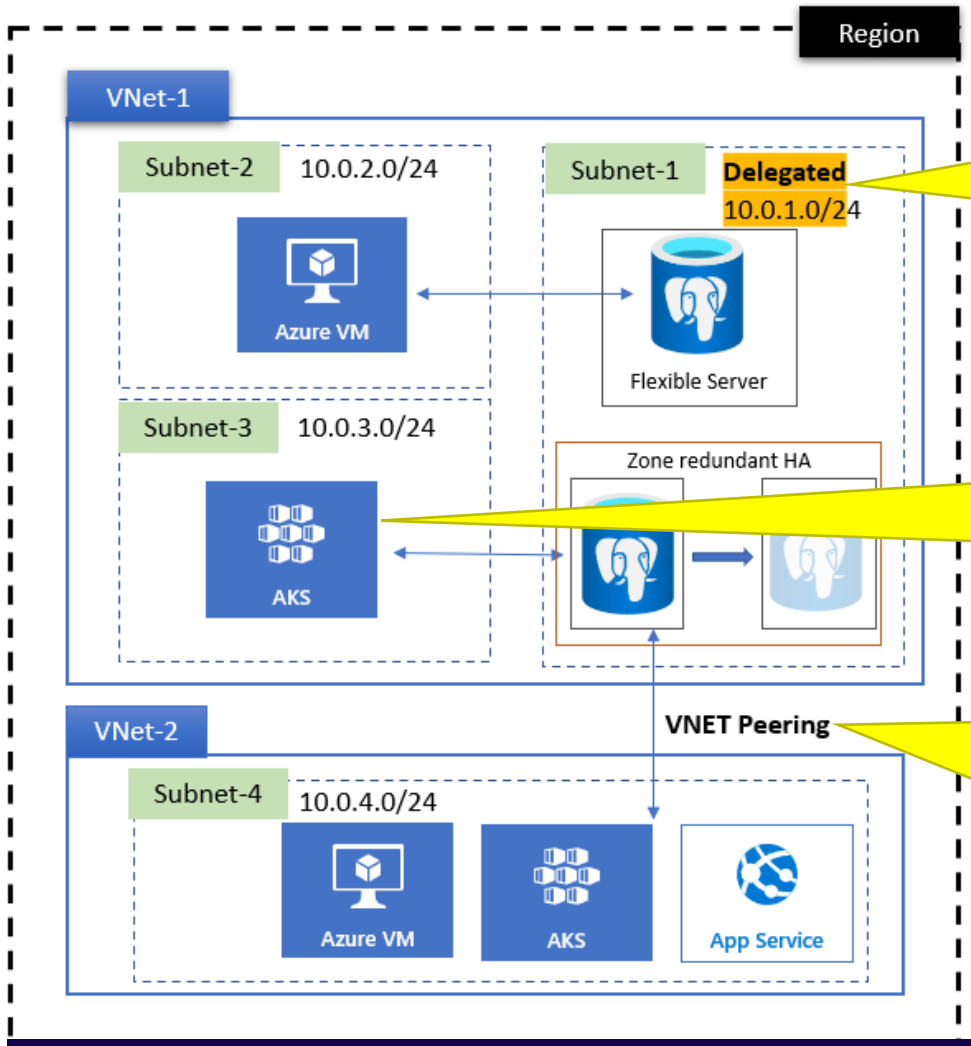
Public Access



Public Access

Network connectivity				
	Connectivity method	Select **Public access (allowed IP addresses) and Private endpoint**, for the sake of simplicity.	Possible values are **Public access (allowed IP addresses) and Private endpoint** and **Private access (VNET Integration)**. For more information, see Networking overview for Azure Database for PostgreSQL with public access and Network with private access for Azure Database for PostgreSQL.	Can't be changed after instance is created.
Public access				
	Allow public access to this resource through the internet using a public IP address	Enable the checkbox.	By enabling this checkbox, you can configure firewall rules to control the IP address ranges from where clients can connect to your instance through the public endpoint. For more information, see Networking overview for Azure Database for PostgreSQL with public access	Can be changed after instance is created.

Private Access



PostgreSQL flexible server instances are injected into subnet 10.0.1.0/24 of the VNet-1 virtual network

Applications that are deployed on different subnets within the same virtual network can access Azure Database for PostgreSQL flexible server instances directly

Applications that are deployed on a different virtual network (VNet-2) don't have direct access to Azure Database for PostgreSQL flexible server instances. You have to perform virtual network peering for a Private DNS zone before they can access the flexible server instance

https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-networking-private#private-access-virtual-network-integration

Recommendation

- Public access (allowed IP addresses) and Private endpoint
- Disable public access
- Connectivity is only possible via private endpoints
- Achieve compliance with Azure Policy

Tags

- Cost Management
  - Determine cost allocation needs
- Establish governance boundaries
- Automation
  - Identify operational and compliance requirements

Tags

- Resources do not inherit tags from RG or subscription
- Not every Azure resource supports tags
- Case sensitivity in tags
  - Tag names (keys) are case insensitive, but tag values are case-sensitive

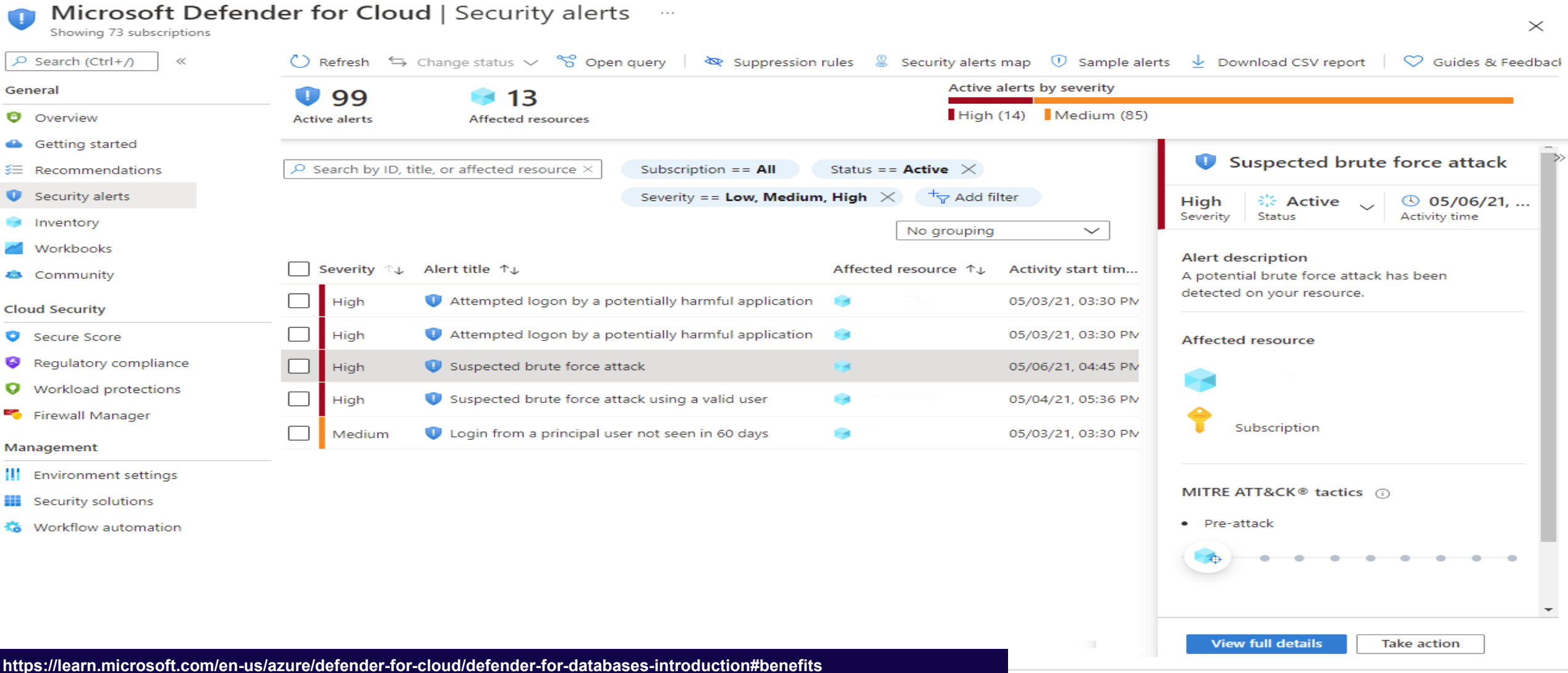
Recommendation

- Must have tags
  - Environment
  - ApplicationID
  - Create date
- Do not add sensitive values to tags
- Apply consistent letter case for tag values
  - Use lowercase for tag names (keys)
- Multi-Region Operations include tags to indicate region
- Achieve compliance with Azure Policy

Defender for Cloud

- Detects anomalous database access
  - Suspected brute force attack
  - Login from a principal user not seen in 60 days
  - Log on from an unusual Azure Data Center
- Detects anomalous query patterns
- Detects suspicious database activities
  - Legitimate user accessing a SQL server from a breached computer

Defender for Cloud



https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-databases-introduction#benefits

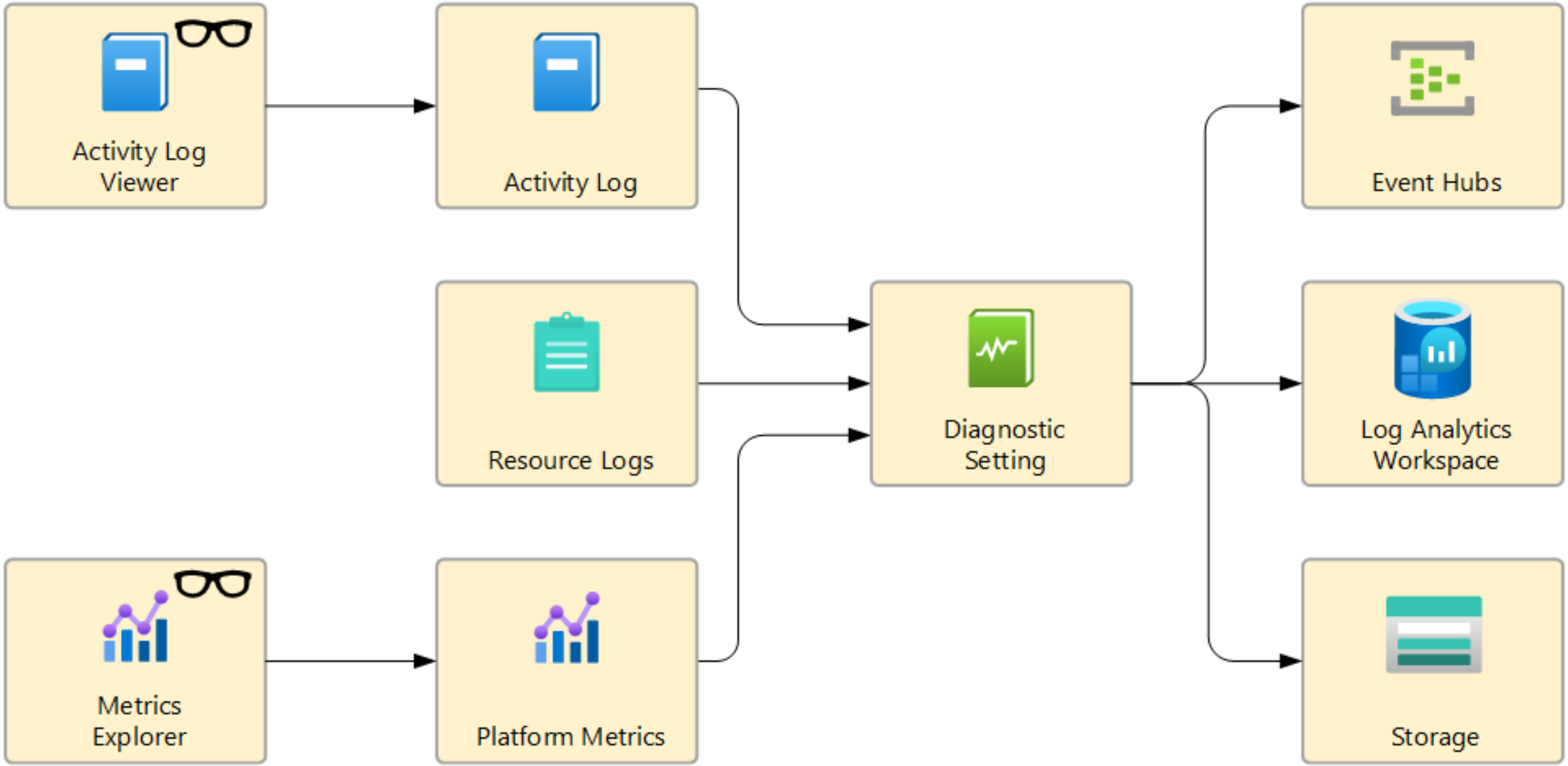
Recommendation

- Enable for all Servers
- Preferable: Enable on Subscription level if possible
- Otherwise: Enable per server during deployment
- $15/Server/Month
- Achieve compliance with Azure Policy

Diagnostics

- Server Logs
- Sessions data
- Query Store Runtime
- Query Store Wait Statistics
- Autovacuum and schema statistics
- PostgreSQL remaining transactions
- All Metrics

Diagnostics



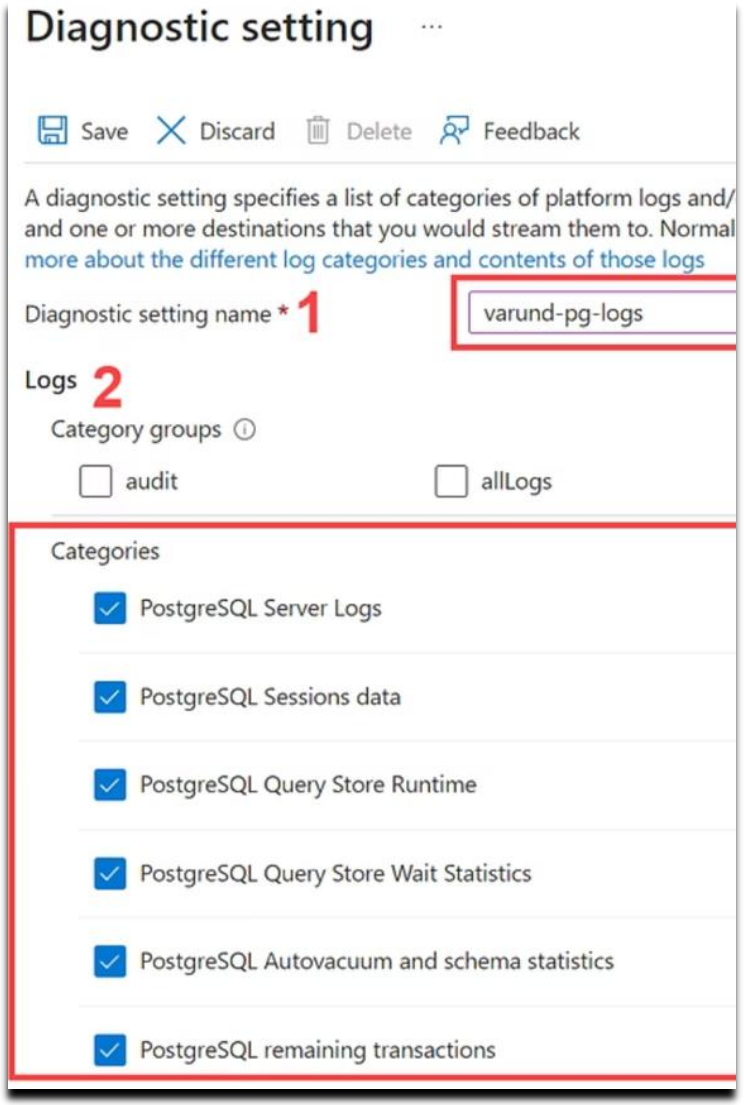
https://learn.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings?WT.mc_id=Portal-Microsoft_Azure_Monitoring&tabs=portal

Diagnostics: Destination

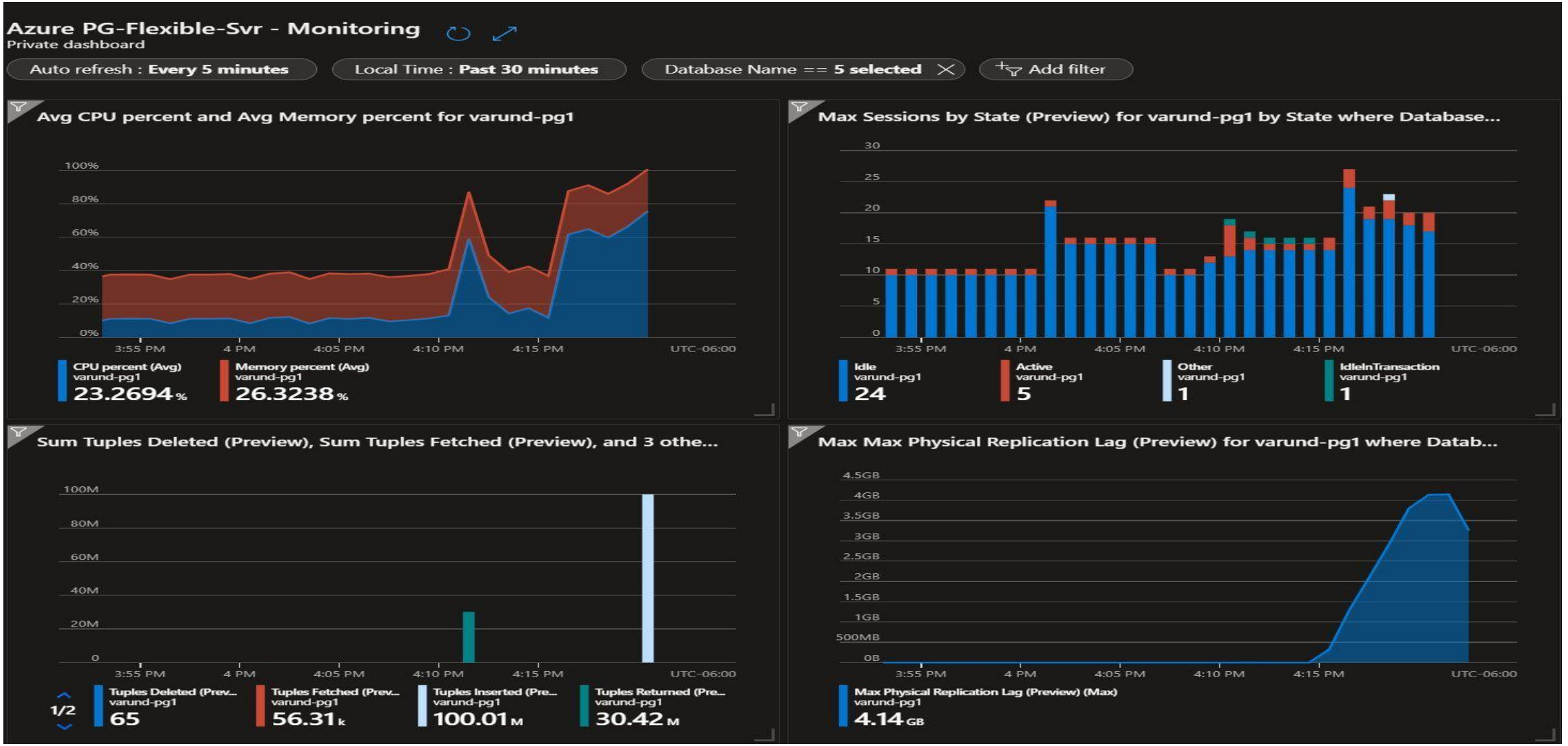
- Log Analytics workspace
  - Query and analyze logs
  - Create alerts
- Azure Storage account (Same region)
  - Archive logs for audit, offline analytics or backup
- Azure Event Hubs
  - Stream logs to custom logging systems
- Partner solutions

Recommendation

- Only collect the categories you require for each service
- You can have multiple Diagnostic setting
- Adjust retention
- Achieve compliance with Azure Policy



More Metrics



https://techcommunity.microsoft.com/blog/adforpostgresql/enhanced-monitoring-metrics-for-azure-postgres-flexible-server/3711774

Enhanced Metrics

- Get fine-grained monitoring and alerting on databases
- Some enhanced metrics include a Dimension parameter
- Categories
  - Activity
  - Database
  - Logical replication
  - Replication
  - Saturation
  - Traffic

Autovacuum Metrics

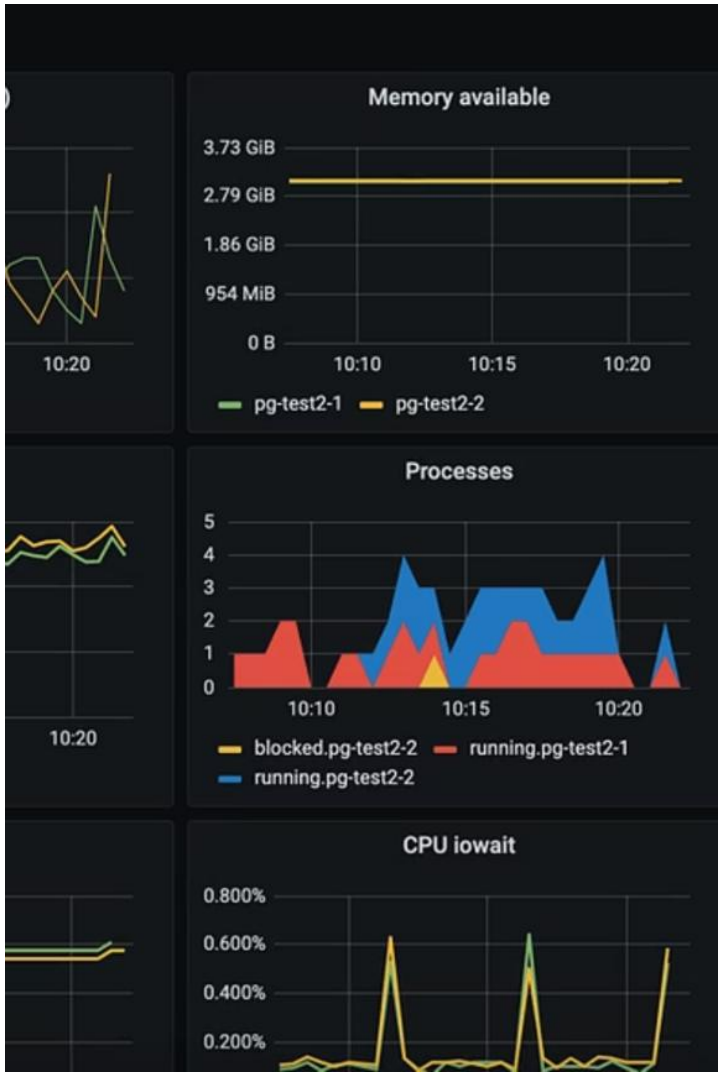
- Disabled by default.
- To enable set the server parameter metrics.autovacuum_diagnostics to ON

PgBouncer Metrics

- Disabled by default.
- Feature is enabled via the server parameter
  - pgbouncer.enabled
  - metrics parameter metrics.pgbouncer_diagnostics is enabled
- These parameters are dynamic and don't require an instance restart

Recommendation

- Enhanced Metrics
  - Only on demand
- Autovacuum Metrics
  - On for all Production systems
- PgBouncer Metics
  - Only on Busy or high-concurrency systems

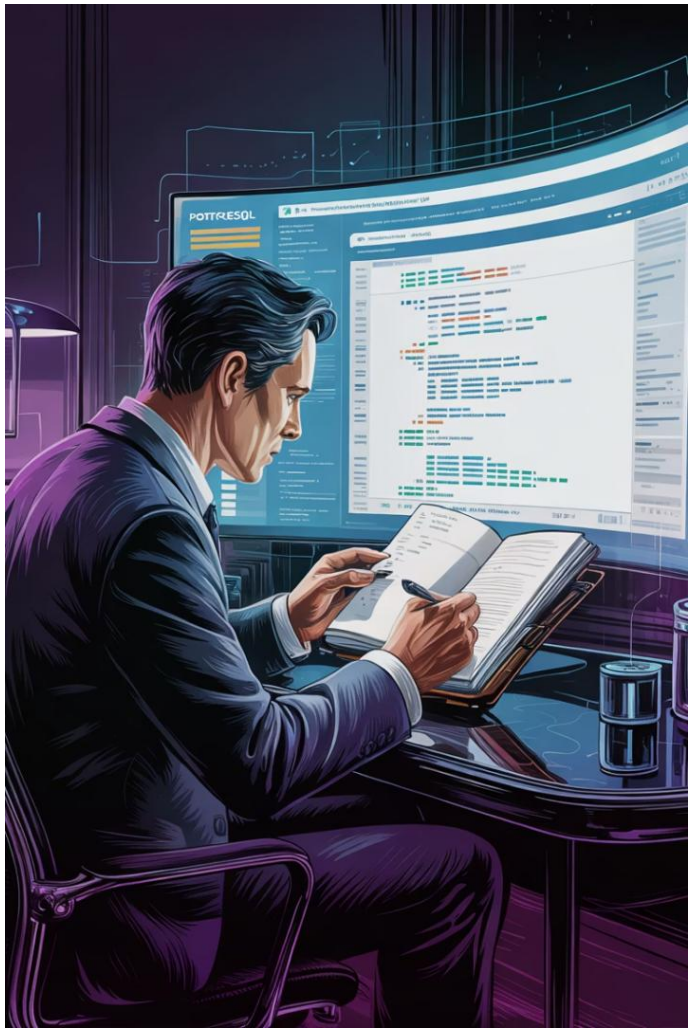


Downloadable Logs

- Capturing logs for download is disabled by default
- Server logs
- Upgrade logs
- Overlap with diagnostics setting (Server logs)

Recommendation

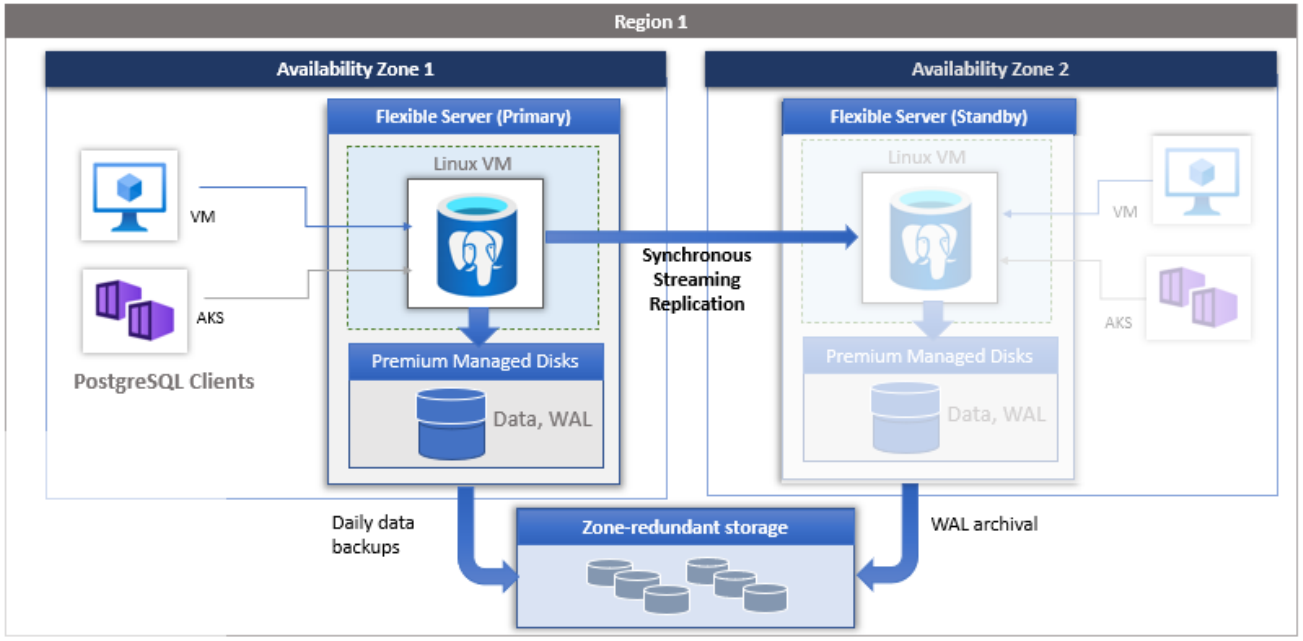
- Setup on demand
- Default three days
- Extend up to seven days

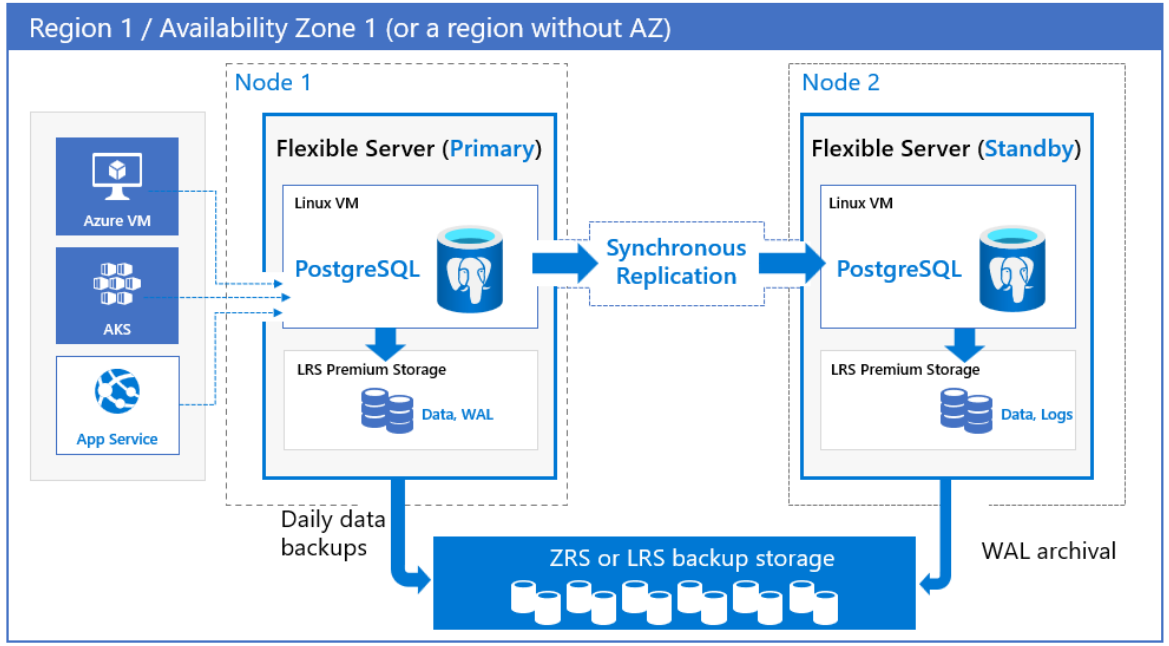


High Availability

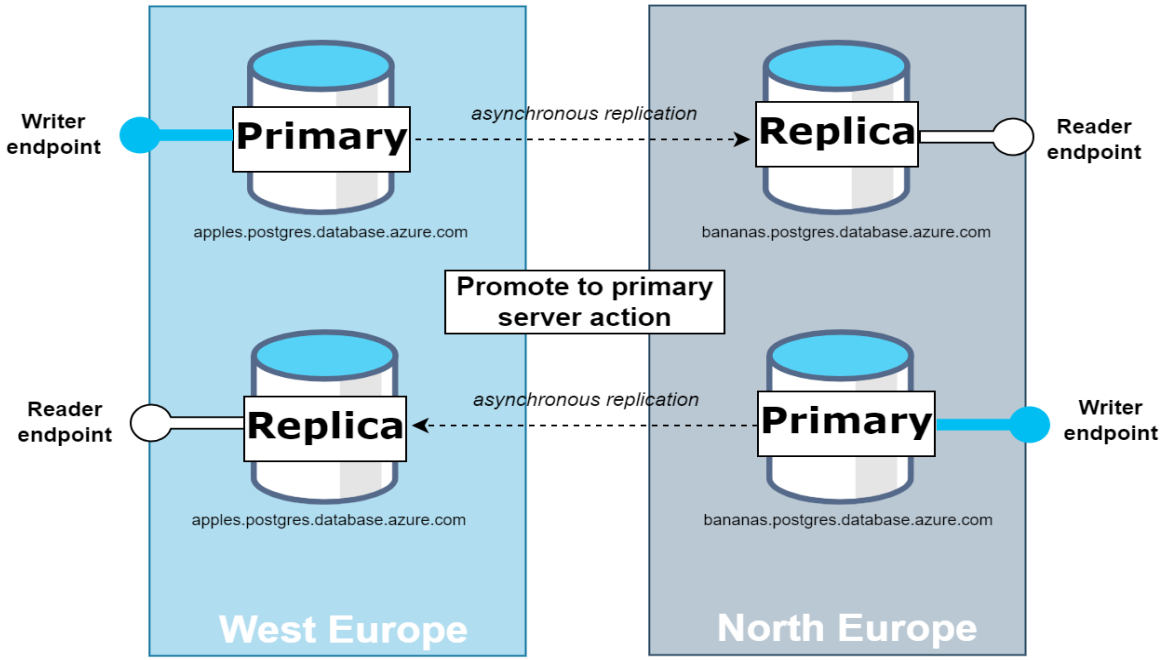
- High availability limitations
- Availability zone support
  - Zone-redundant with fallback
  - Zonal
- Cross-region disaster recovery and business continuity
  - Geo-redundant backup and restore
  - Read replicas

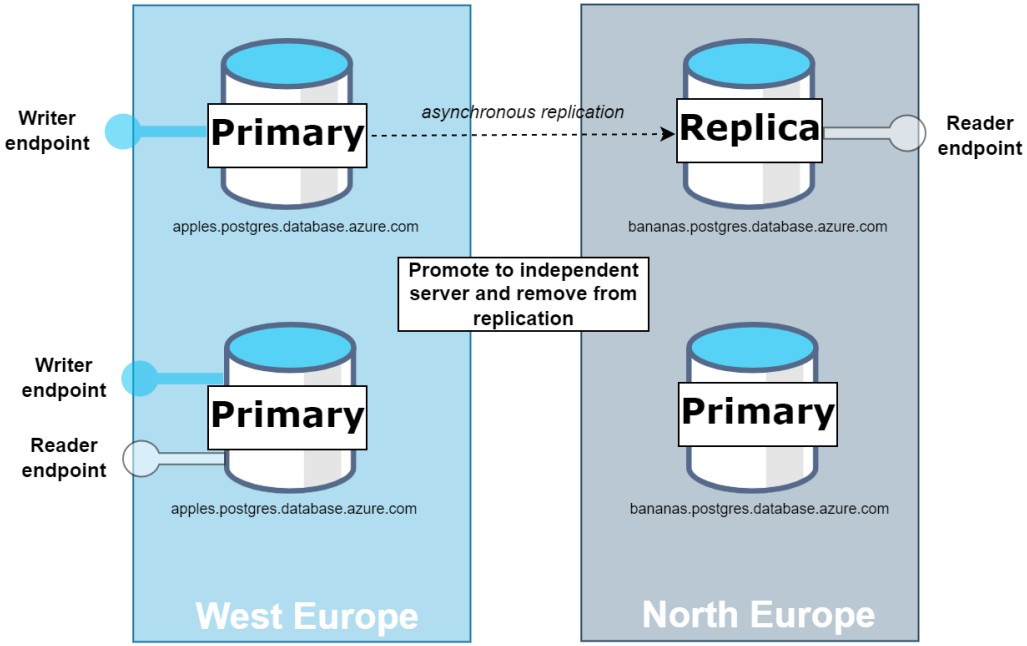
High Availability: Zone





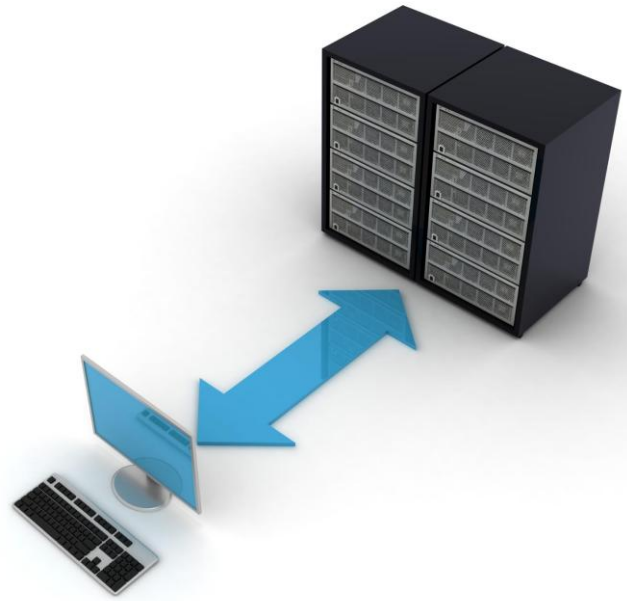
High Availability: Promote





Recommendation

- Subjective to your business SLA
- Production: standby replica to promote as Primary
- The promote operation doesn't carry over specific configurations and parameters
- Practice failover testing
- Achieve compliance with Azure function

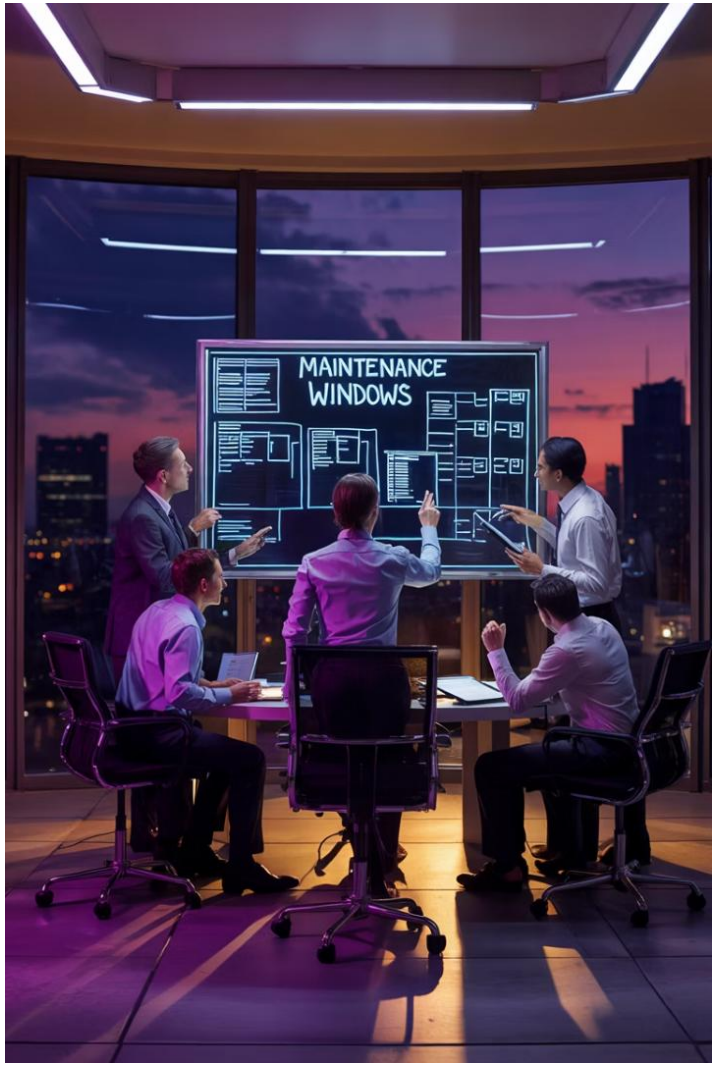


Maintenance Schedule

- System-managed schedule
  - Any day between 11pm and 7am
- Custom schedule
  - You can pick a day of the week and time
- Excluding emergencies, maintenance occurs once every 30 days

Recommendation

- Production: Custom schedule
- Non-production: System-managed schedule
- Achieve compliance with Azure Policy



Backup Retention (PIT)

- Point-in-time backup: Default is 7 days
- Can be extended up to 35 days
- On-demand backup
  - Not supported with burstable tier
  - Not supported with SSDv2
  - Maximum of 7 copies within the retention period

Backup Retention (LTR)

- Must use azure backup service and backup vault
- Up to 10 years
- Currently available ‘Restore as Files’ using storage container
- Future plan ‘Restore as Server’
- Cannot select individual databases
- Maximum database size 1 TiB
- Do not support tables containing a row with a BYTEA length exceeding 500 MB

Backup Redundancy

- Zone redundancy is default
- You can configure geo-redundant storage for backup only during server creation
  - You can restore it to a geo-paired region
- After a server is provisioned, you can't change the backup storage redundancy option

Recommendation

- Agree with system owners about requirements before deploying
- Understands your retention requirement
- Practice frequent restore
- Achieve compliance with Azure function

Storage

- Premium SSD V2 is in Preview and not available in all regions
- When storage usage reaches >95% or <=5 GiB, whichever is more, the server switches to read-only mode
- Note that storage cannot be scaled down once the server is created

Storage Autogrow

- Storage autogrow
  - Prevents a server from running out of storage and becoming read-only
  - More than 1TiB: smaller of 64TiB or 10%
  - Less than 1TiB: smaller of 64TiB or 20%
  - Premium SSD always doubles the disk size
  - Not supported with Premium SSD V2
- Premium SSD V2(preview) supports more granular disk size

Recommendation

- Turn off auto-growth
- Setup alert: information, high and critical for available free space
- Achieve compliance with Azure Policy

Intelligent Performance

- Query Performance Insight
  - Long running queries
  - Wait statistics
  - Top queries by calls
  - Top queries by data usage
  - Top queries by IOPS
  - Top queries by temporary files

Intelligent Performance

- Index tuning
  - CREATE INDEX recommendations
  - Drop duplicate indexes
  - Drop unused indexes

Intelligent Performance

- Prerequisites
  - Query Store is enabled on your database
  - Query Store Wait Sampling is enabled
  - Diagnostics turned on with:
    - Sessions data
    - Query Store Runtime
    - Query Store Wait Statistics

Recommendation

- Query Performance Insight
  - Turn on for all production cluster
- Index tuning
  - Enabled to only emit recommendation*

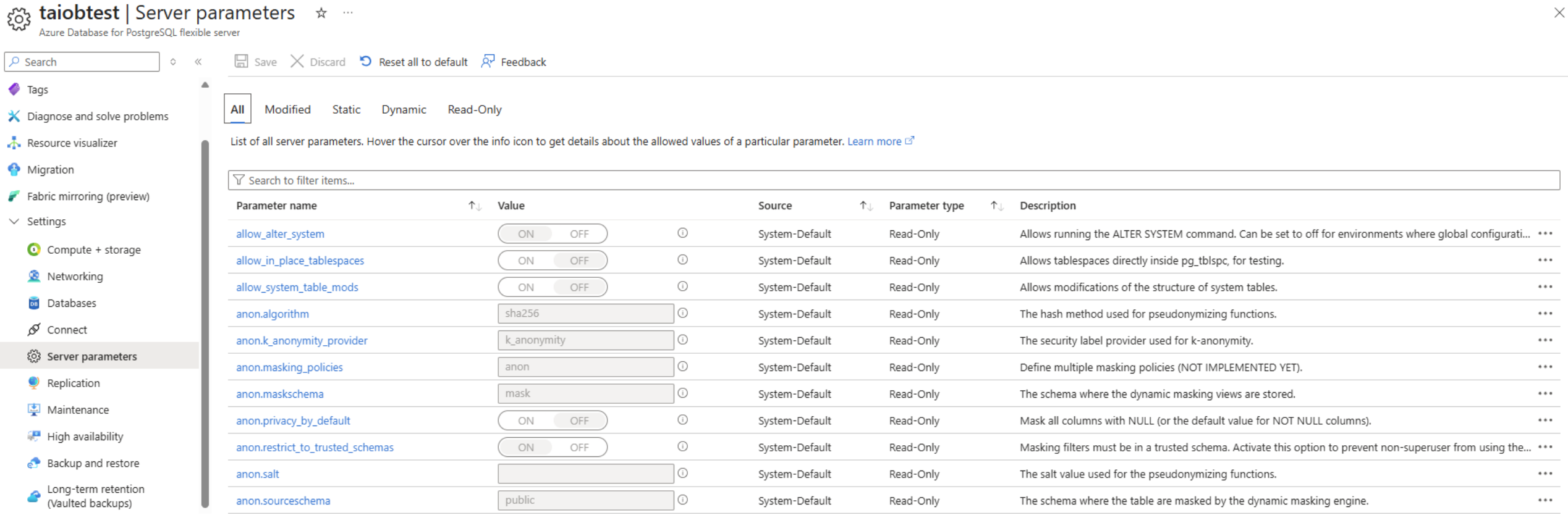
Resource Lock

- Delete lock
- Read-only lock

Recommendation

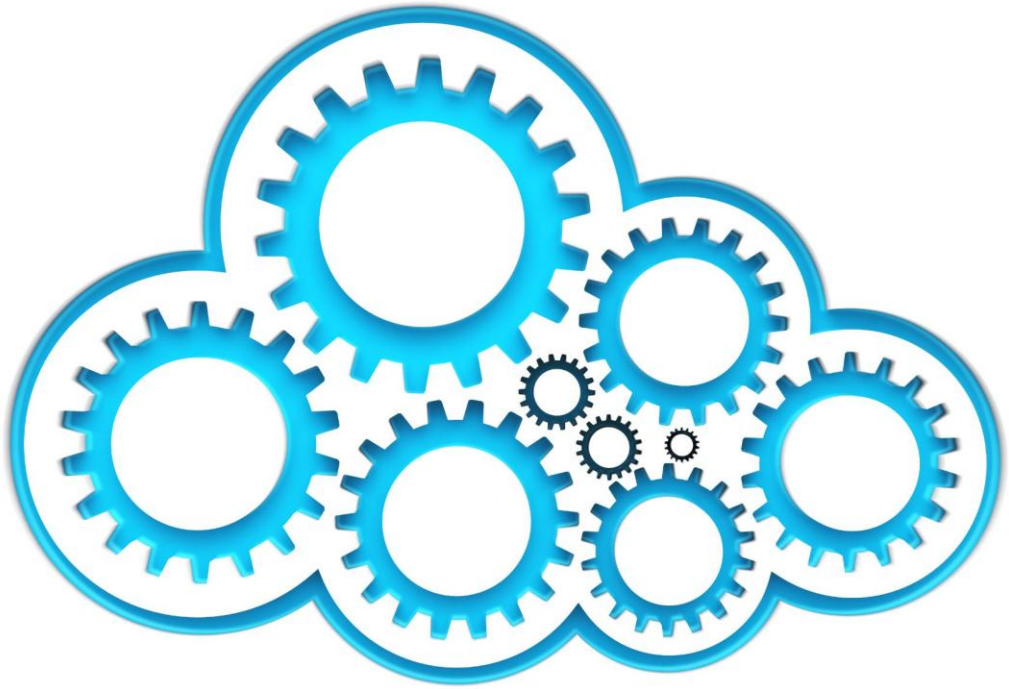
- Production: Delete lock
- Achieve compliance with Azure Policy

Server Parameters



Key Implementation

- Azure Policy Enforcement
- Production vs Non-Production Controls
- Mandatory Security Items
- Customization via Azure Functions



PASS
Data Community Summit
Host redgate

I'm a Community Expert at PASS Summit 2025!

Book a Meeting

PASS
Data Community Summit

Your feedback is important to us

Evaluate this session at:

passdatacommunitysummit.com/evaluations

Thank you

Reach out to me with questions/comments.
You are guaranteed an answer!

Taiob Ali

@sqlworldwide

sqlworldwide

https://sqlworldwide.com