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:

www.PASSDataCommunitySummit.com/evaluation

Why standardize?

- Protect sensitive data
- Meet industry requirements
- Operational Consistency
- Enable automation through infrastructure as code

Workload Type

- Development
  - Default Compute: Burstable
  - Default Compute size: Standard_B2s
  - High Availability Disabled
- Production
  - Default Compute: General Purpose
  - Default Compute size: Standard_D4ds_V4
  - High Availability (Zonal resiliency) Enabled

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

Recommendation

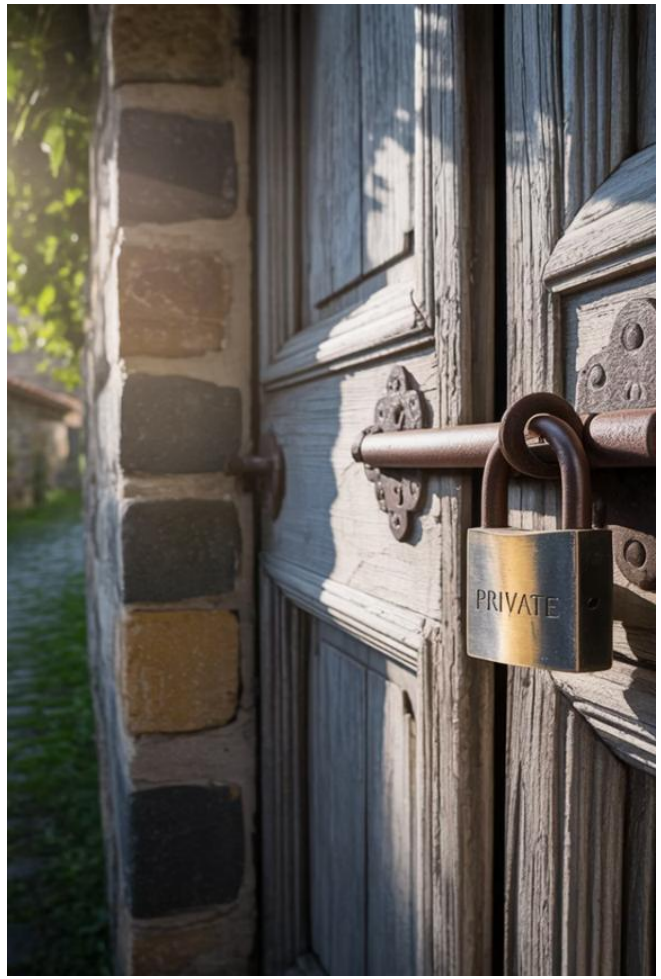
- Development for Non-production workloads
- Production for Production workloads
- Enforce this during deployment using Azure Policy

Authentication method

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

Recommendation

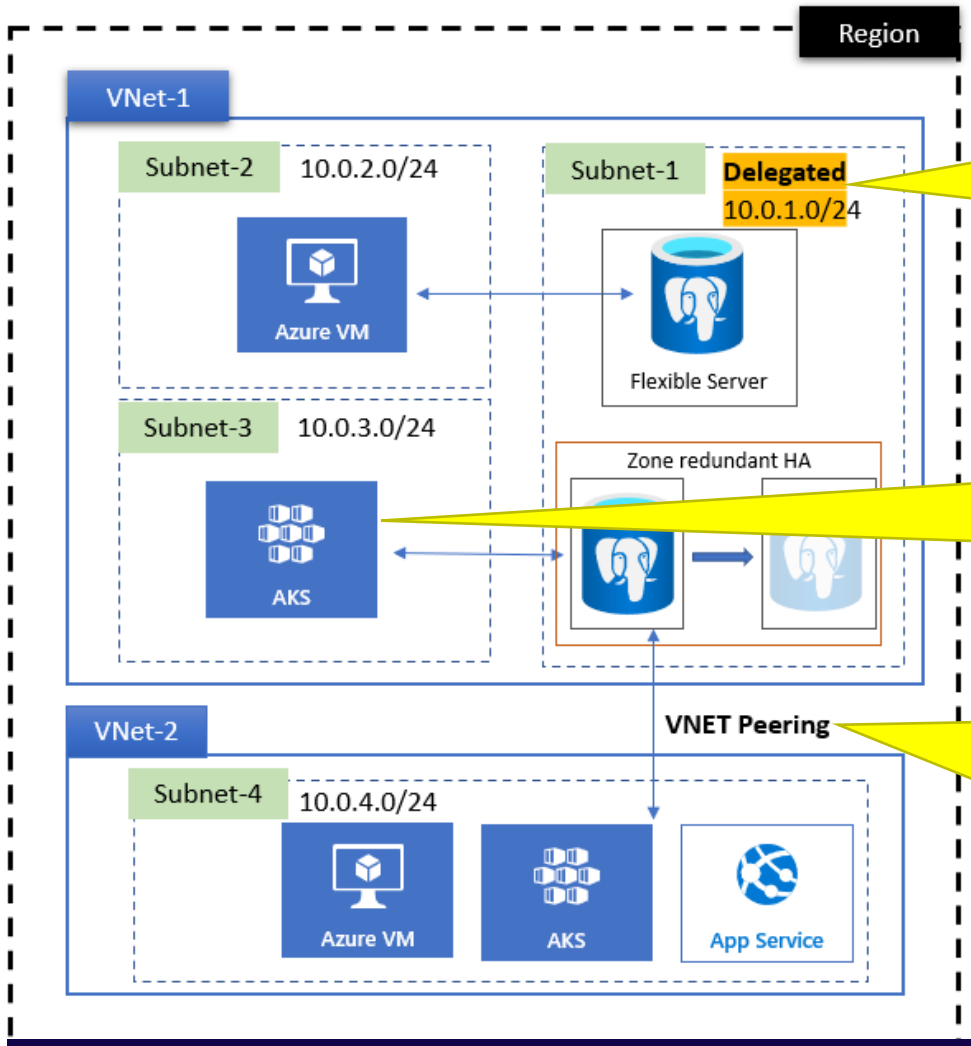
- Use Entra instead of database local authentication
- Disallow the use of local authentication
- If you must use local authentication:
  - Ensure strong password policies
  - Regular password rotation
  - Use SCRAM authentication only
- Azure Policy



Network Connectivity

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

Network Connectivity



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

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

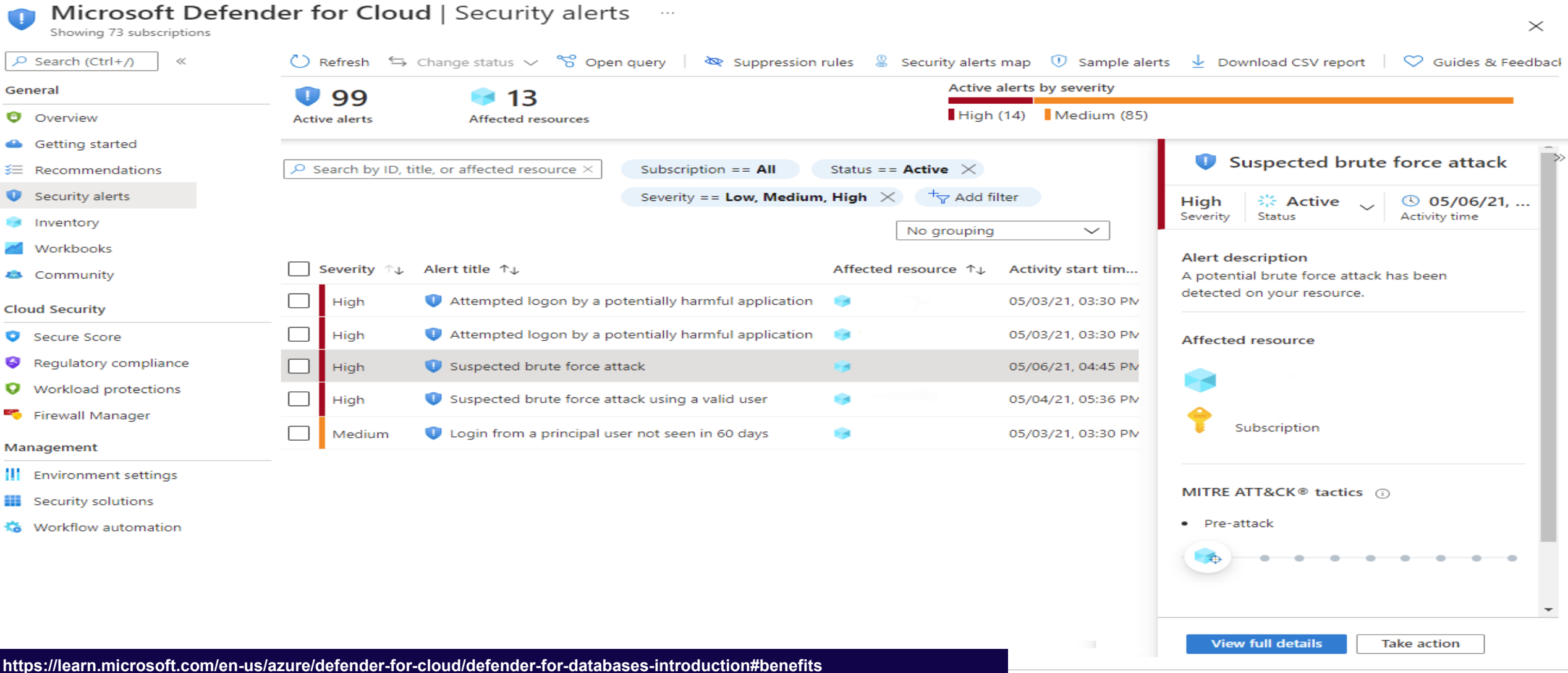
Recommendation

- For production environment
  - Environment
  - ApplicationID
- 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
- Enforce tagging 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

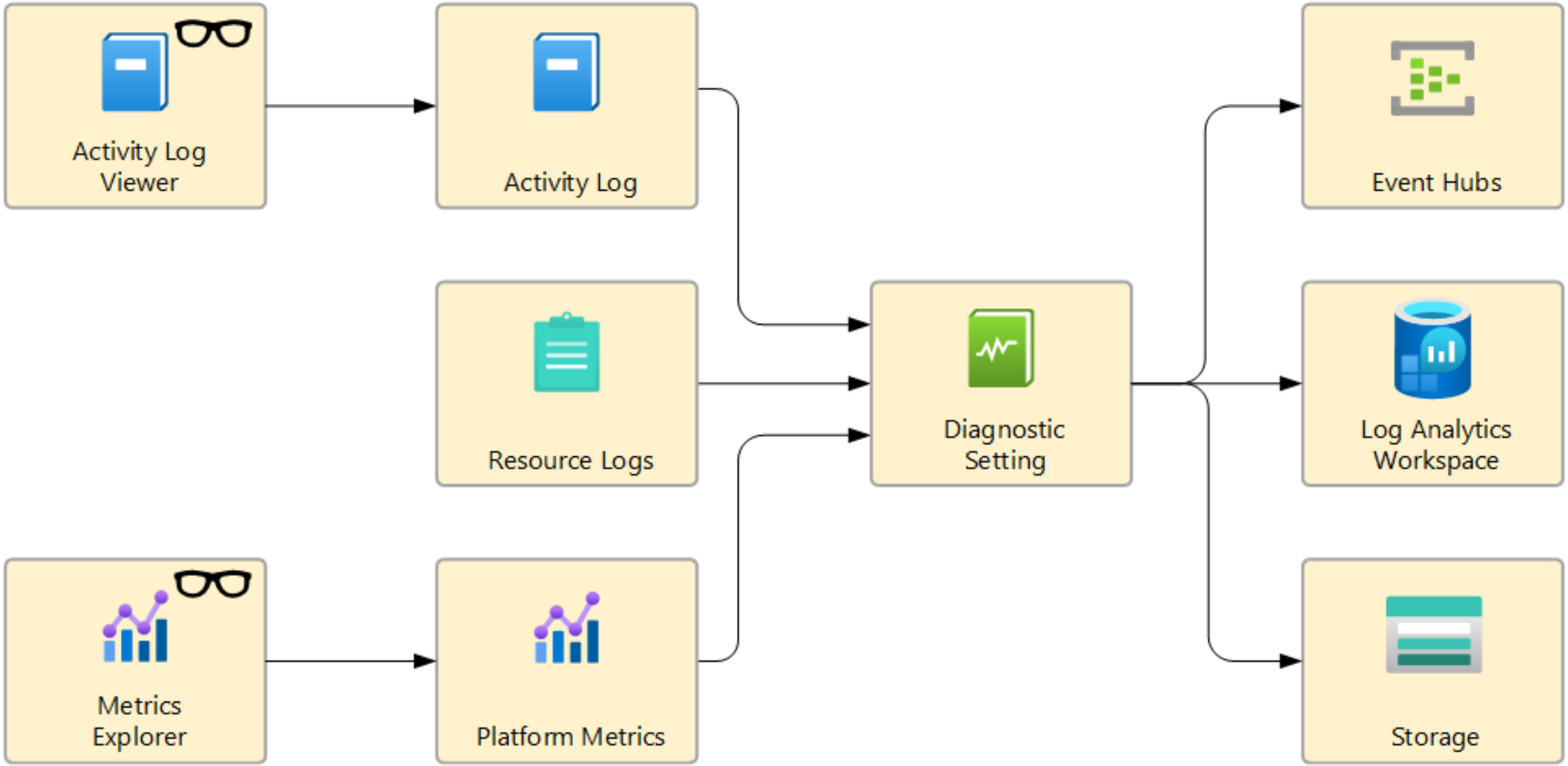
Recommendation

- Enable for all Servers
- Preferable: Enable on Subscription level if possible
- Otherwise: Enable per server during deployment
- Enforce by using Azure policy
- $15/Server/Month

Diagnostics

- Metrics
- Platform logs:
  - Activity log
  - Resource logs

Diagnostics



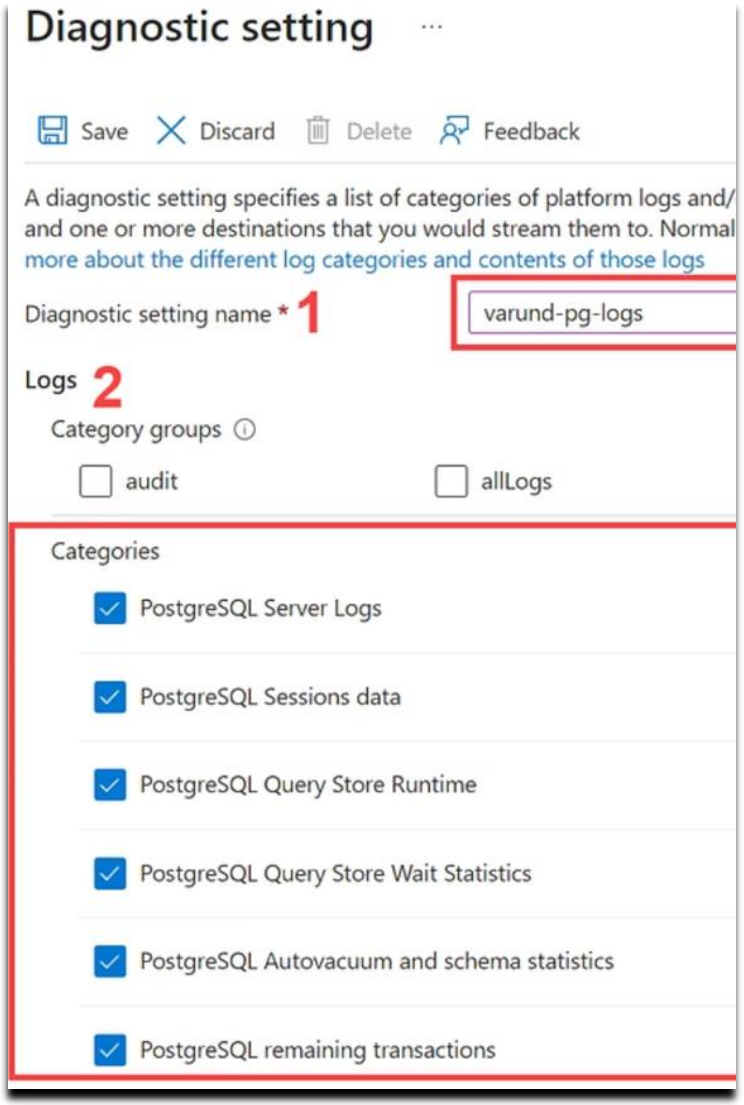
https://learn.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings?WT.mc_id=Portal-Microsoft_Azure_Monitoring&tabs=portal

Diagnostics

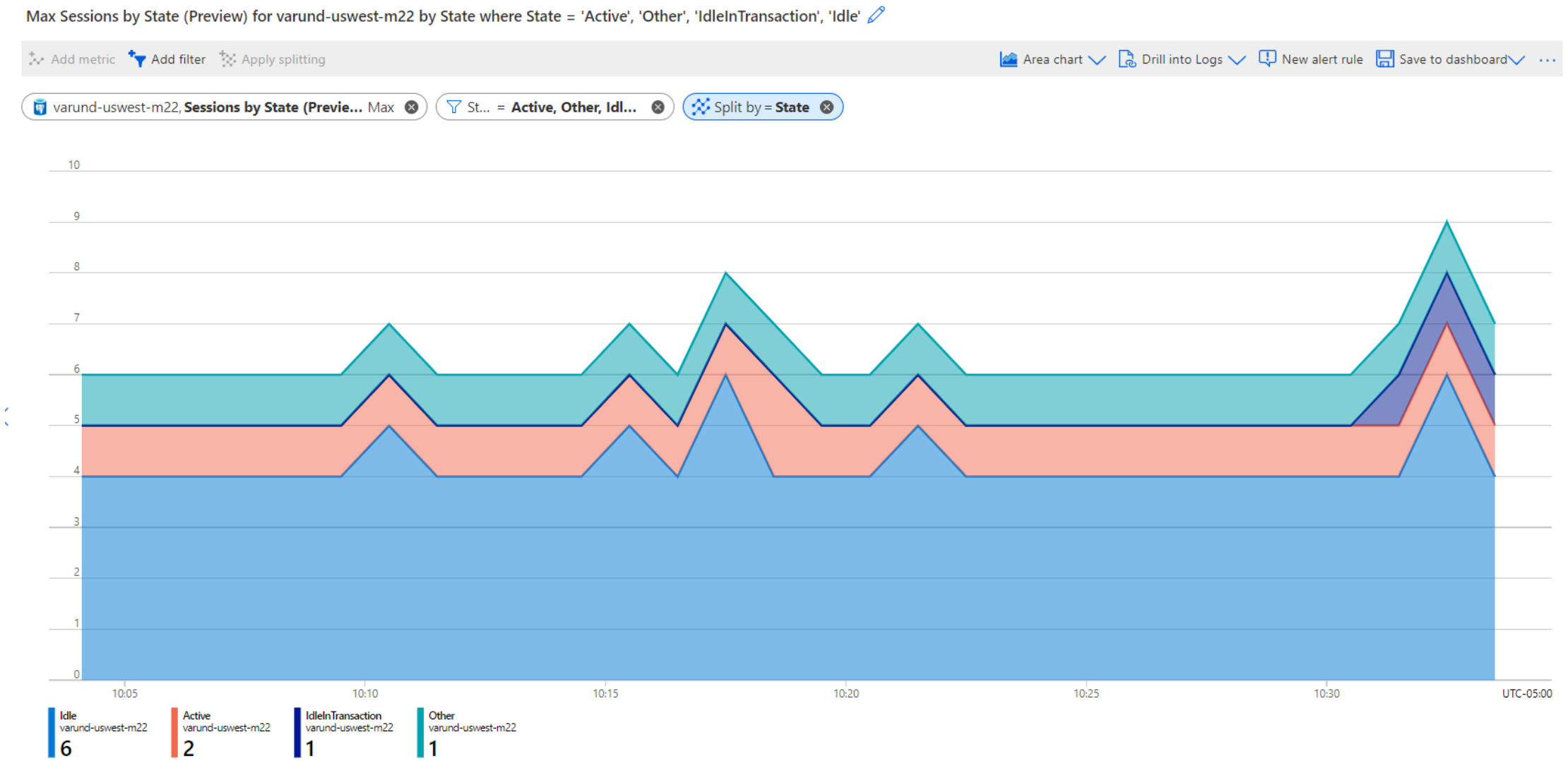
- Log Analytics workspace
  - Query and analyze logs
  - Create alerts
- Azure Storage account (Same region)
  - Archive logs for audit, offline analytics or backup
- Azure Event Hubs
  - Stream logs to custom logging systems
- Partner solutions

Recommendation

- Only collect the categories you require for each service
- You can have multiple Diagnostic setting
- Adjust retention
- Azure policy or function



Enhanced Metrics



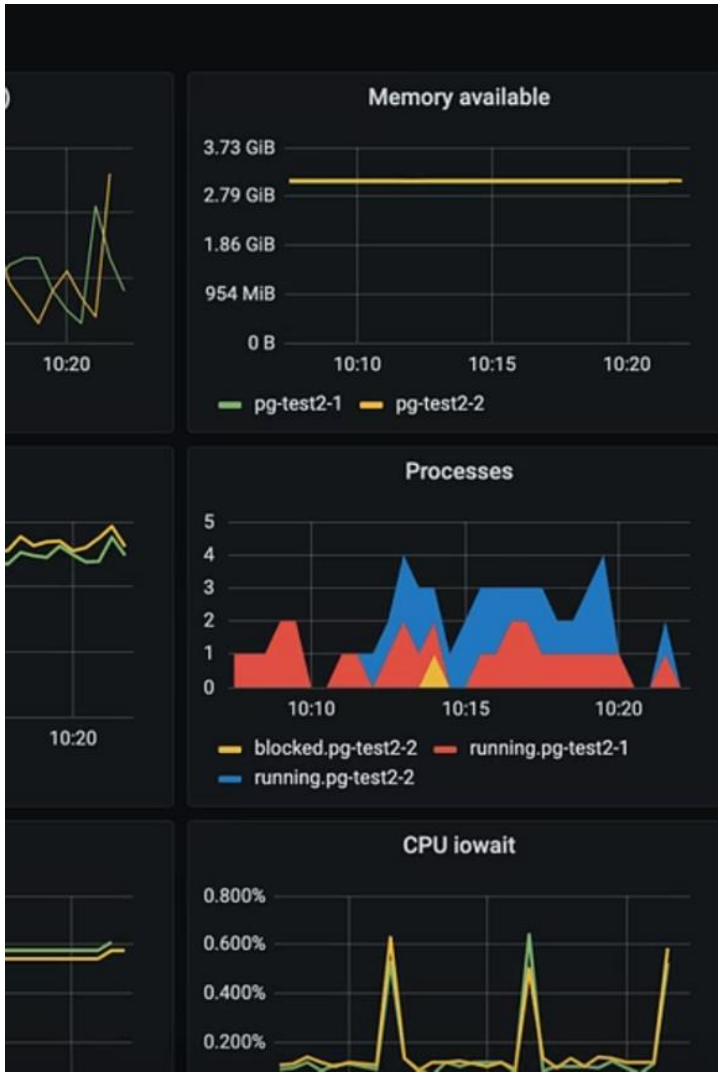
https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-monitoring#enabling-enhanced-metrics

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

Recommendation

- Only on demand

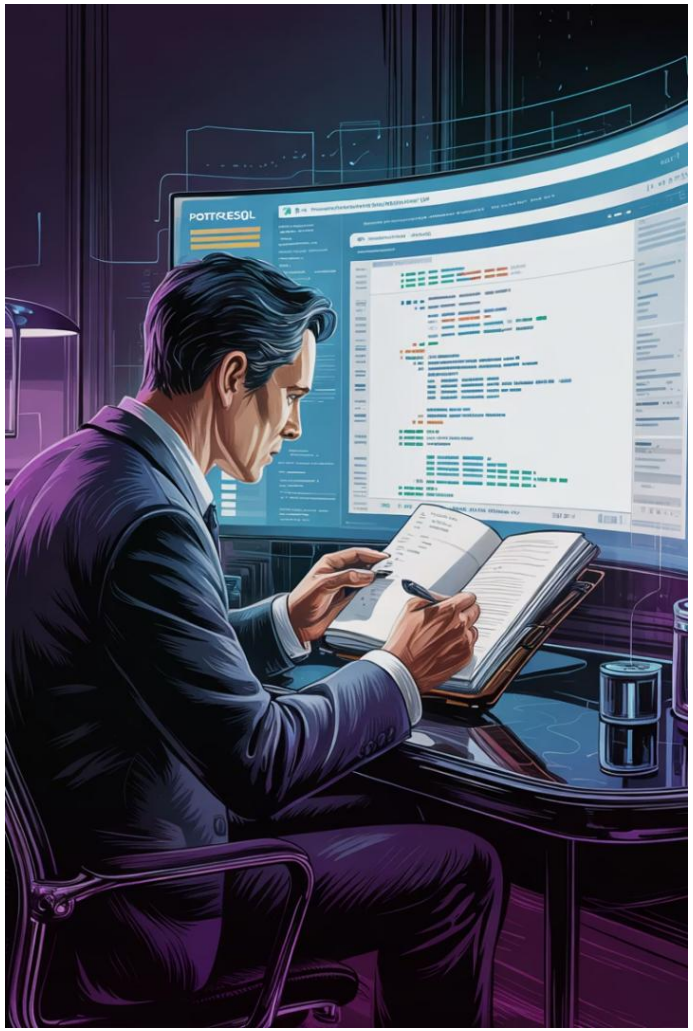


Downloadable Logs

- Download PostgreSQL and upgrade logs
  - Disable by default
  - Server logs
  - Upgrade logs
- Overlap with diagnostics setting

Recommendation

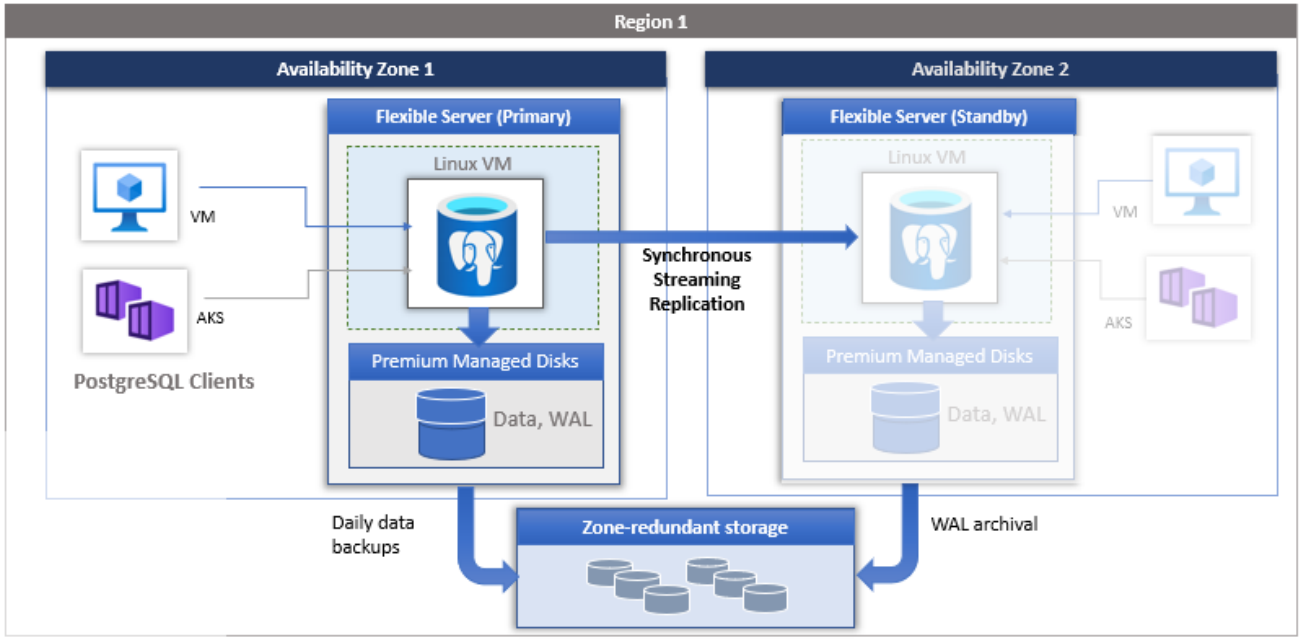
- Setup on demand
- Default three days
- Extend up to seven days

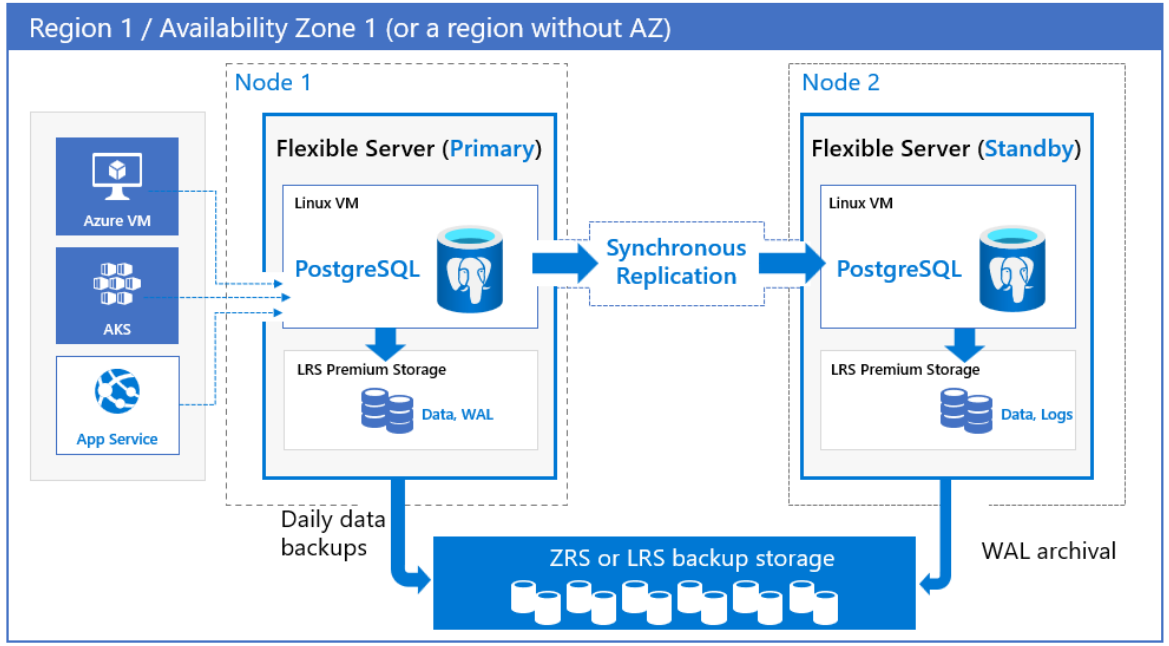


High Availability

- 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

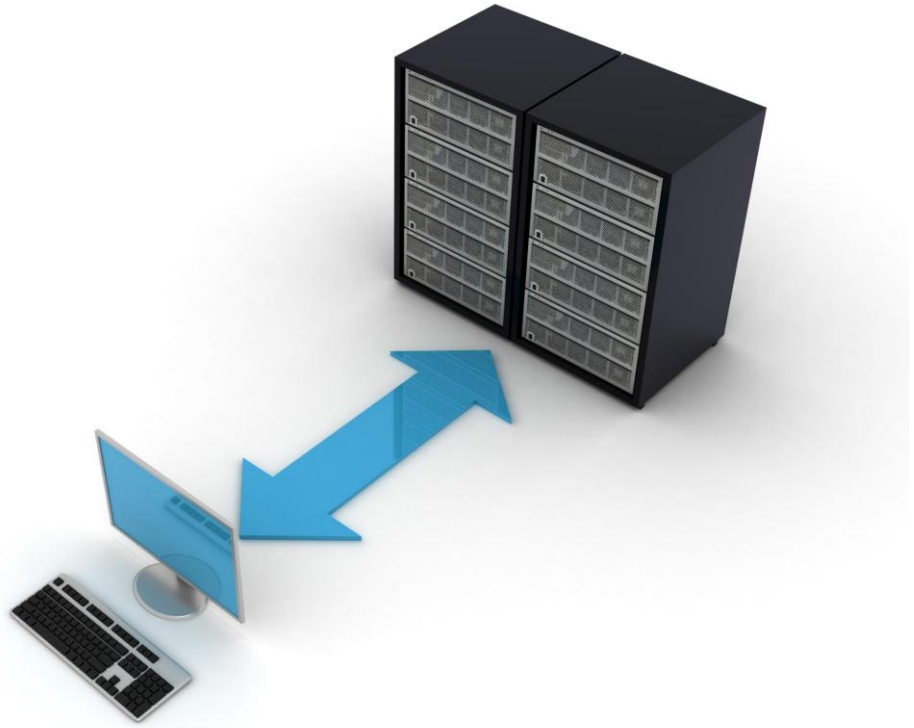
High Availability





Recommendation

- Subjective to your business SLA
- Production: standby replica for automatic failover capability
- Practice failover testing (forced failover)

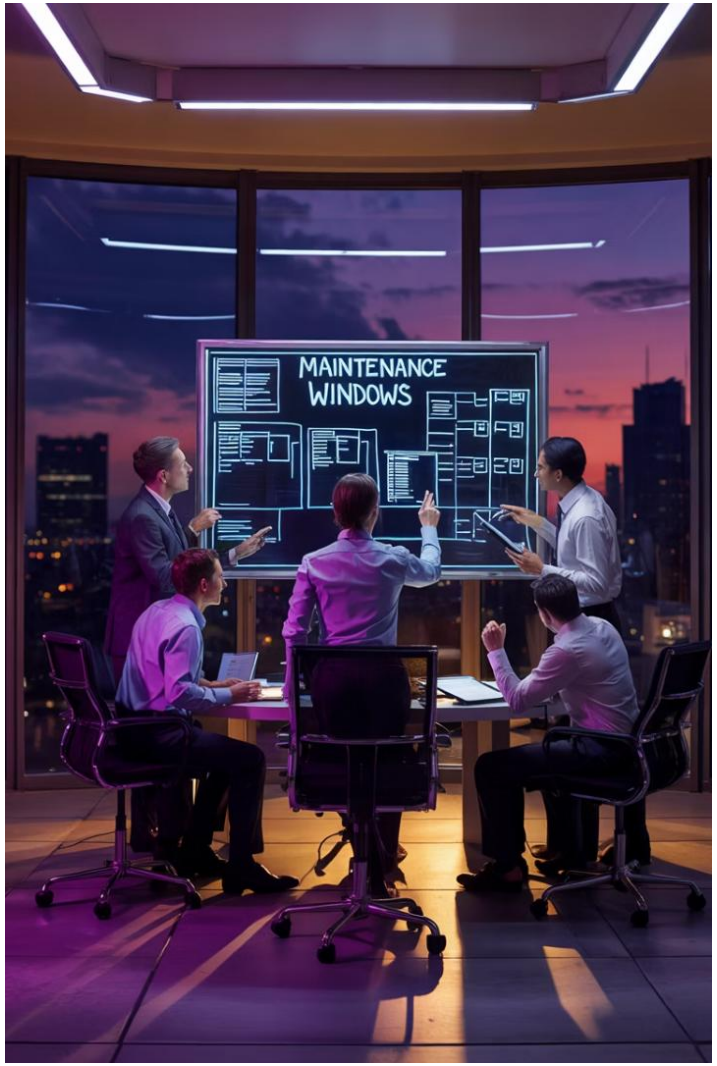


Maintenance

- 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
- Implement custom azure policy or Azure function



Backup Retention (PIT)

- Point-in-time backup: Default is 7 days and 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’
- 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
- Use Azure policy to implement

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

Resource Lock

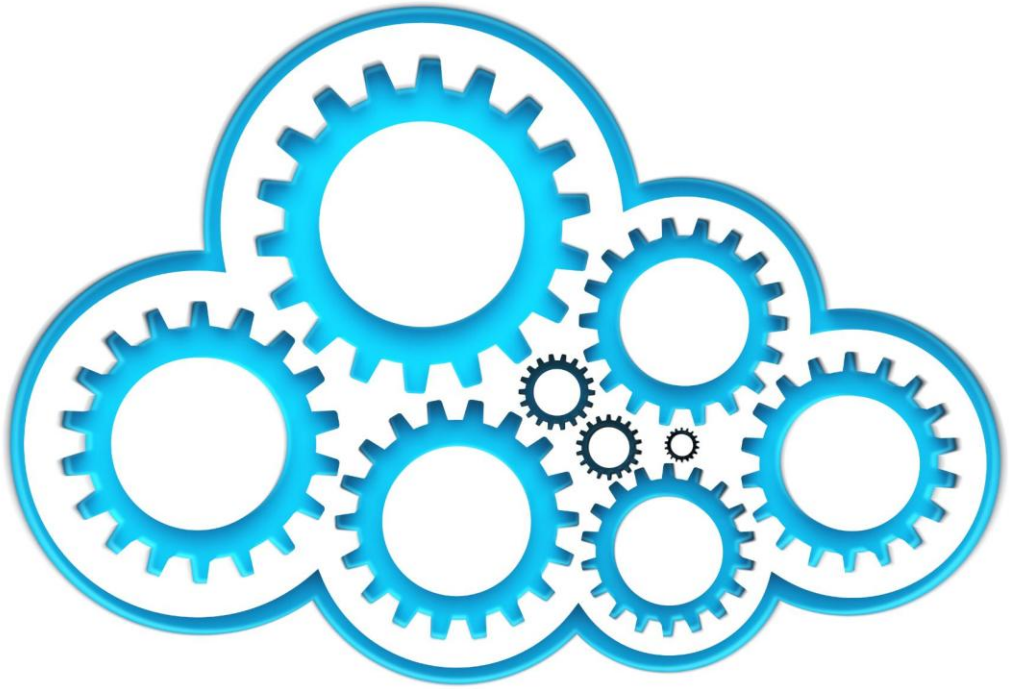
- Delete lock
- Read-only Lock

Recommendation

- Production: Delete lock
- Use Azure policy to implement

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:

www.PASSDataCommunitySummit.com/evaluation

Thank you

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

Taiob Ali

@sqlworldwide

sqlworldwide

https://sqlworldwide.com