Azure SQL Database Business Continuity

Jes Chapman (she/her)

- Cloud Solution Architect @ Microsoft
- Based in Louisville, KY
- Runner
- Foodie

/grrlgeek.bsky.social
Jes Schultz
grrlgeek

Data is the most important asset for most organizations

- If they lose access to their data, or the data itself, they lose business
- One way to mitigate this threat is through a business continuity plan

What's Business Continuity?

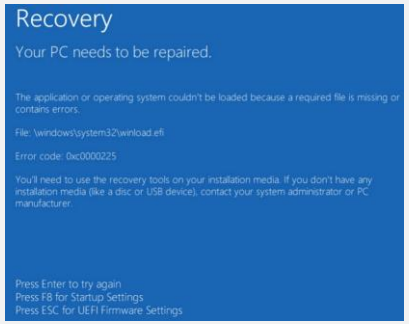
- "A process-driven approach to maintaining operations in the event of an unplanned disruption."

What does business continuity encompass?

Data Entry Error

Data inserted, updated, or deleted by mistake

Equipment Failures



Hardware failures in datacenters

Natural Disaster

Datacenter availability affected due to a natural disaster

Software Upgrades

Continuous software deployments

Core concepts

Backups

- A database backup is a transactionally-consistent record of the database at a point in time

Restores

- A database restore takes a backup and recreates the database as of a point in time

HA (High Availability)

- Recovering data within the same data center or region

DR (Disaster Recovery)

- Recovering data in a secondary data center or region

In the on-premises SQL Server world…

- DBAs set up backup jobs
- Hopefully they test restores
- They may set up Windows Server Failover Clustering (WSFC) with SQL Server Failover Cluster Instances (FCI) (shared storage), or Always On Availability Groups (AGs) (separate storage) for HA.
- They may set up Availability Groups or Log Shipping for DR.

That's a lot of work

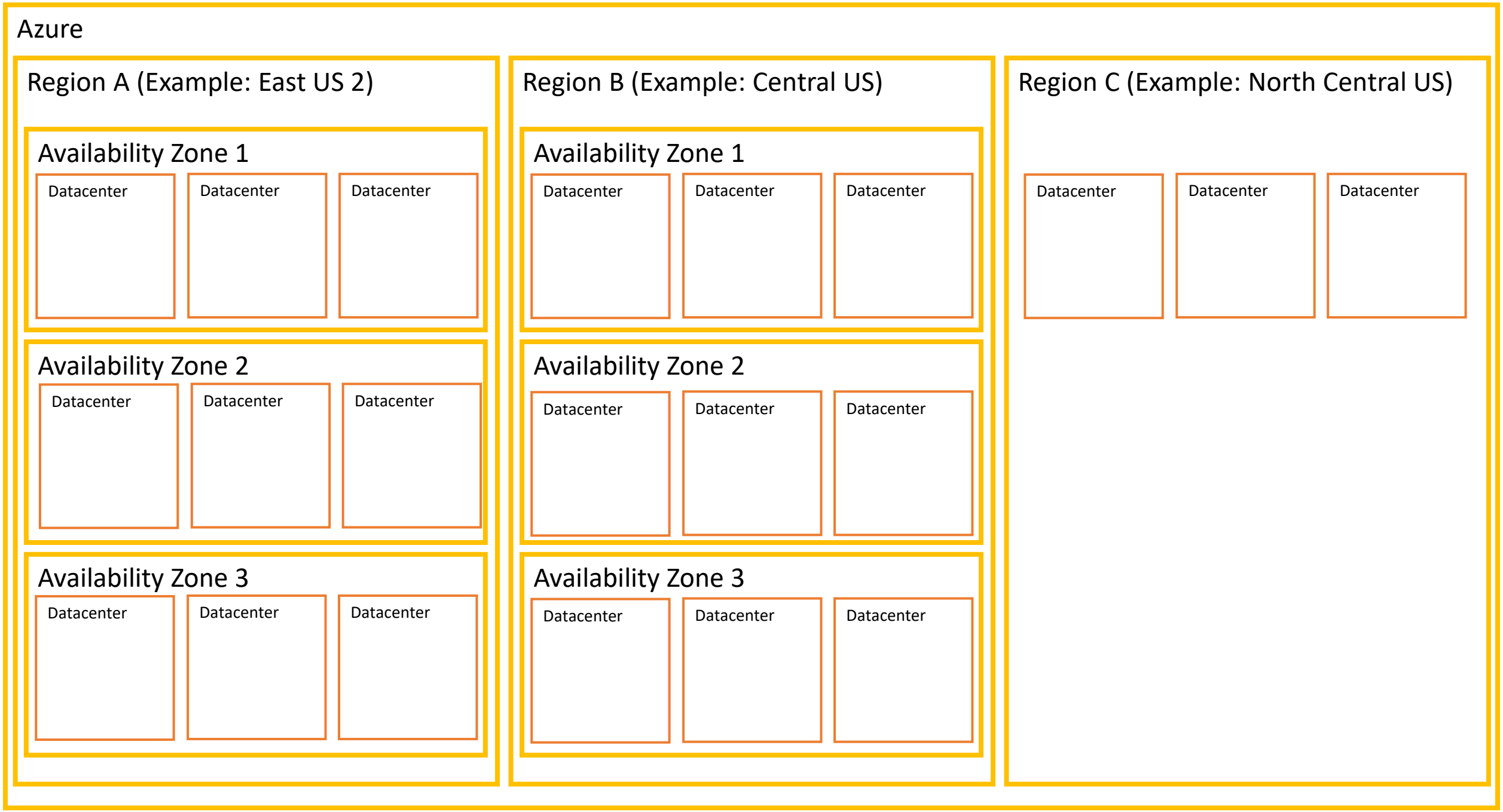
...especially when a company has hundreds of SQL Server instances!

Azure makes it easier!

Azure SQL Database does heavy lifting for the DBA

Azure architecture

First, a look at Azure architectural concepts


Azure
Region A (Example: East US 2)
Availability Zone 1
Datacenter
Datacenter
Datacenter
Availability Zone 2
Datacenter
Datacenter
Datacenter
Availability Zone 3
Datacenter
Datacenter
Datacenter
Region B (Example: Central US)
Availability Zone 1
Datacenter
Datacenter
Datacenter
Availability Zone 2
Datacenter
Datacenter
Datacenter
Availability Zone 3
Datacenter
Datacenter
Datacenter
Region C (Example: North Central US)
Datacenter
Datacenter
Datacenter

Backups

The first line of defense for any database

Fundamentals

- **General Purpose & Business Critical**
  - Full (.bak) and transaction log (.trn) backups.
  - Stored in a Microsoft-owned, Microsoft-managed container.
    - Data exports managed via .bacpac
  - If you delete the server, all backups are deleted and can't be recovered
    - Use Locks to prevent resource deletion
    - Store backups using long-term retention

- **Hyperscale**
  - File snapshots + log backups
  - Stored in a Microsoft-owned, Microsoft-managed container
    - Data exports managed via .bacpac
  - If you delete the server, all backups are deleted and can't be recovered
    - Use Locks to prevent resource deletion
    - Store backups using long-term retention
  - Can’t modify backup storage redundancy after creation

Frequency

- **General Purpose & Business Critical**
  - Full backup every week
  - Differential backups every 12 or 24 hours
  - Transaction log backups approximately every 10 minutes - based on compute size and database activity

- **Hyperscale**
  - Storage snapshots of data files are taken regularly
  - Transaction logs taken regularly

Retention

Short-term

- Minimum 1 day
- Maximum 35 days
- Default 7 days

Long-term

- Up to 10 years
- Backups stored in a different container, tied to the subscription.
  - Can use to recover from a deleted server.
  - Additional protection if data is compromised.
- Stores the weekly full backup - you pick one per week, per month, or per year.

Redundancy

Local (LRS)

- Copies backups synchronously three times within a single physical location in the primary region.

Zone (ZRS)

- Copies backups synchronously across three availability zones in the primary region.

Geo (GRS)

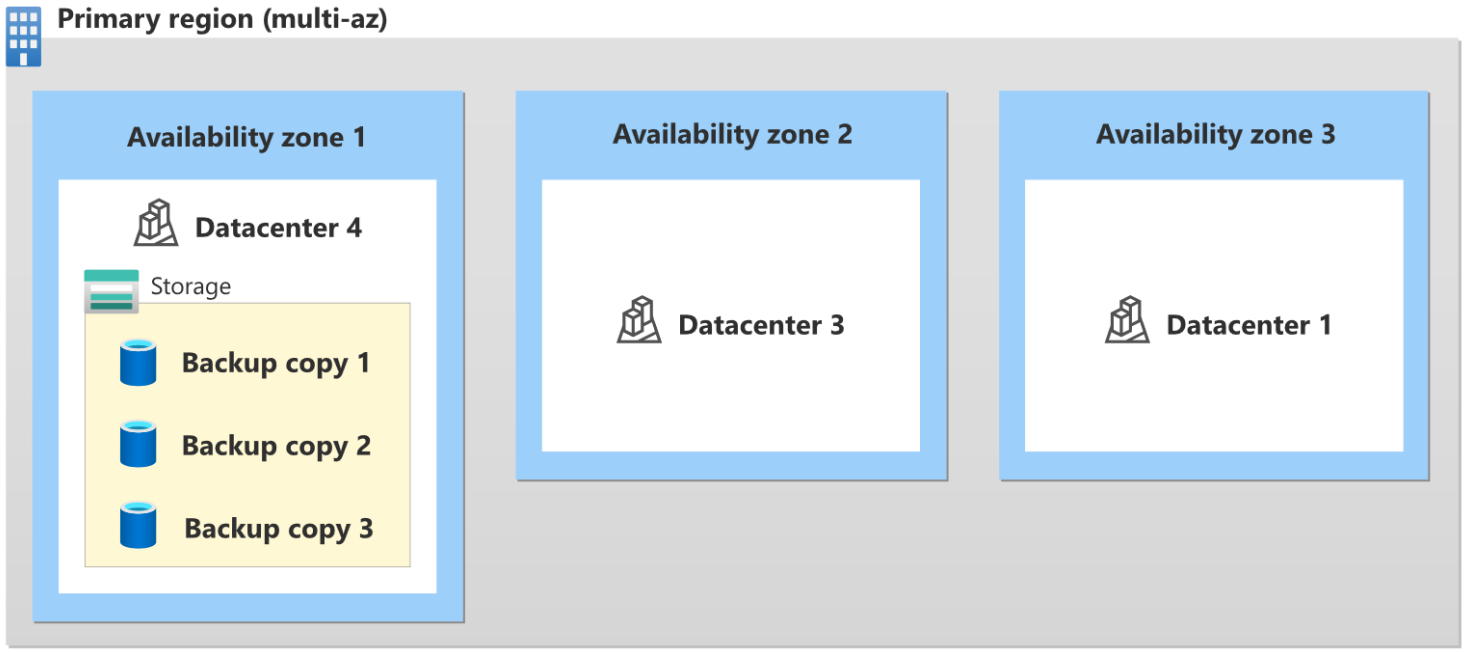
- Copies backups synchronously three times within a single physical location in the primary region by using LRS.
- Copies backups asynchronously three times to a single physical location in the paired secondary region.

Geo-zone (GZRS) (Hyperscale only)

- Copies backups synchronously across three AZs in the primary region.
- Copies backups asynchronously to a single physical location in the paired secondary region.

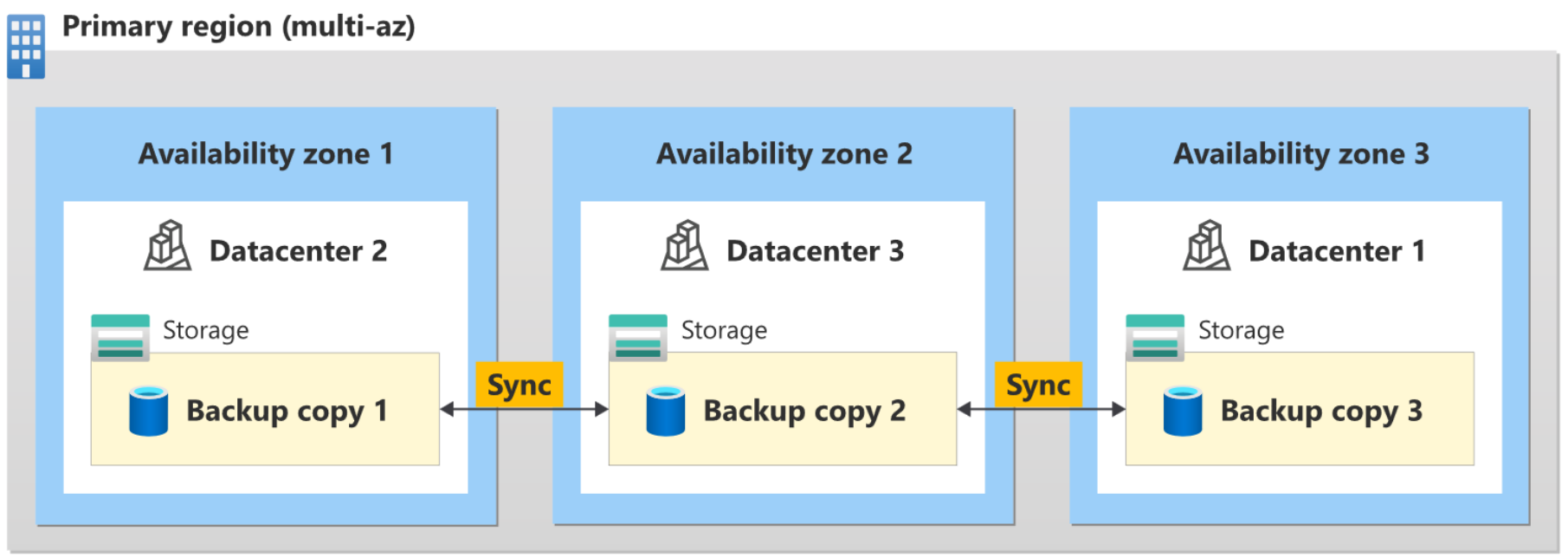
LRS

Copies backups synchronously three times within a single physical location in the primary region.



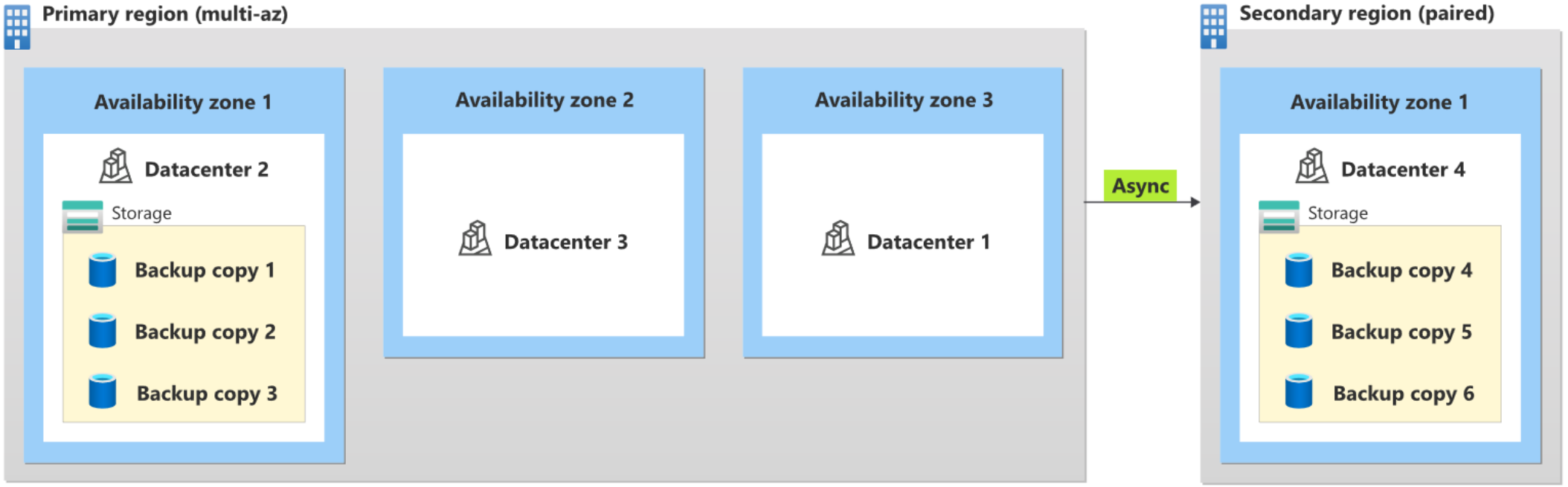
ZRS

Copies backups synchronously across three availability zones in the primary region.



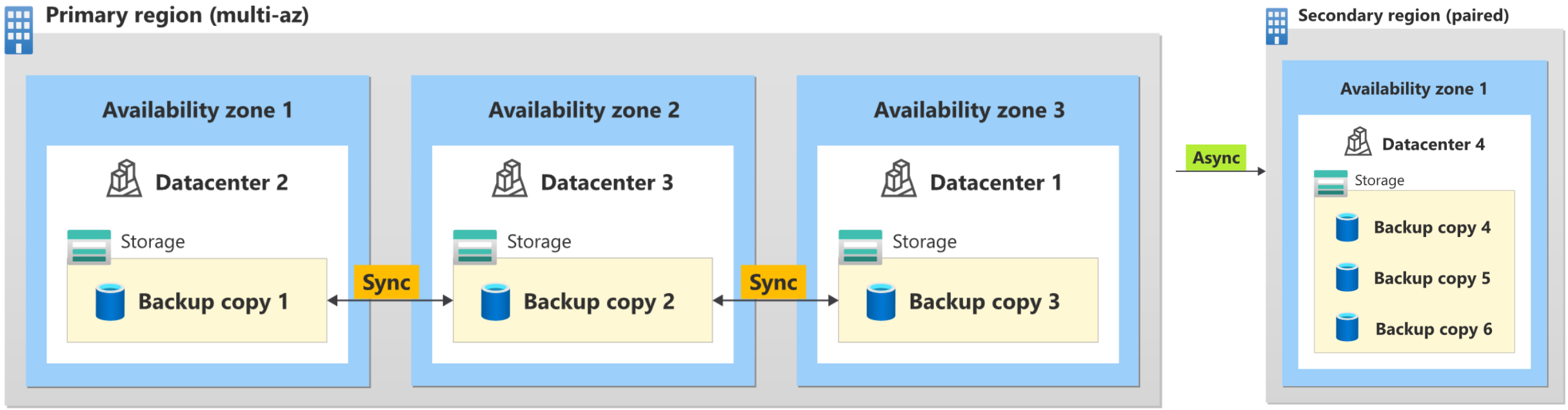
GRS

Copies backups synchronously three times within a single physical location in the primary region by using LRS.
Copies backups asynchronously three times to a single physical location in the paired secondary region.

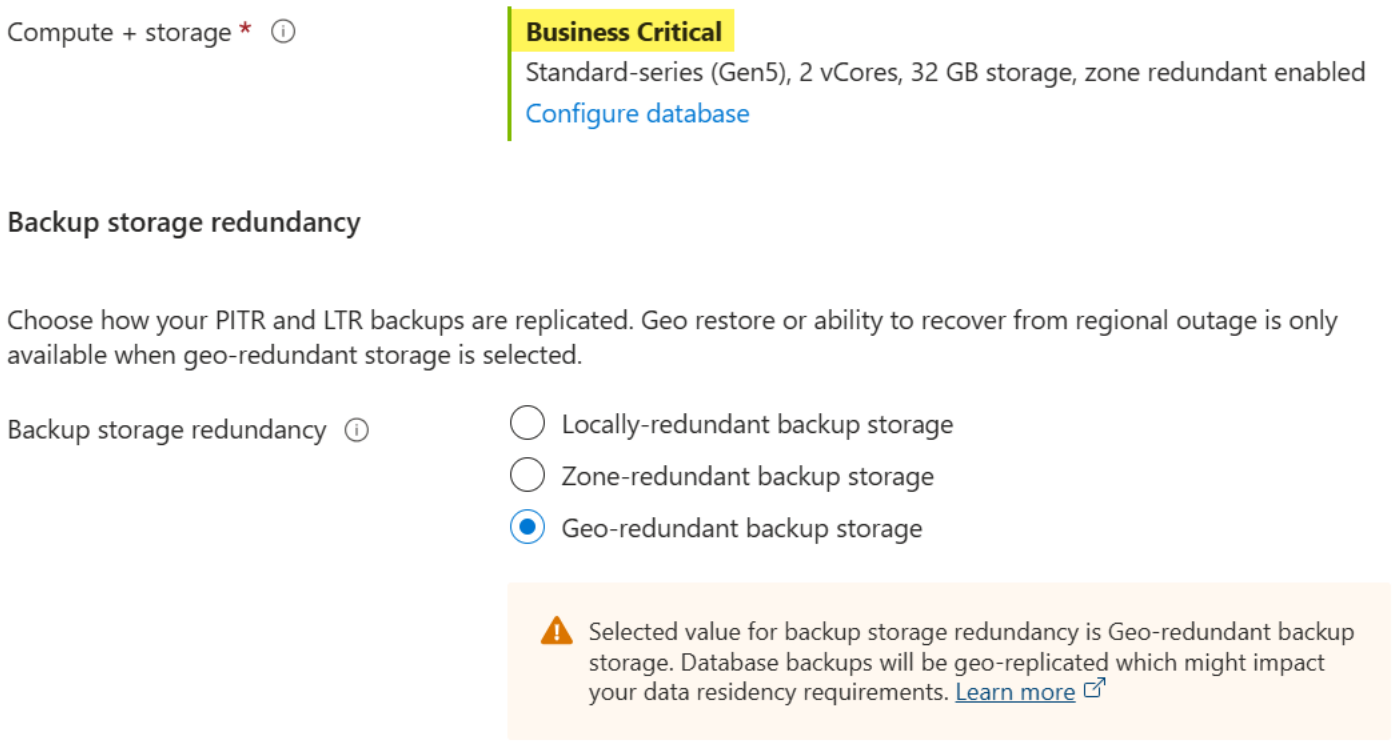


GZRS (Hyperscale only)

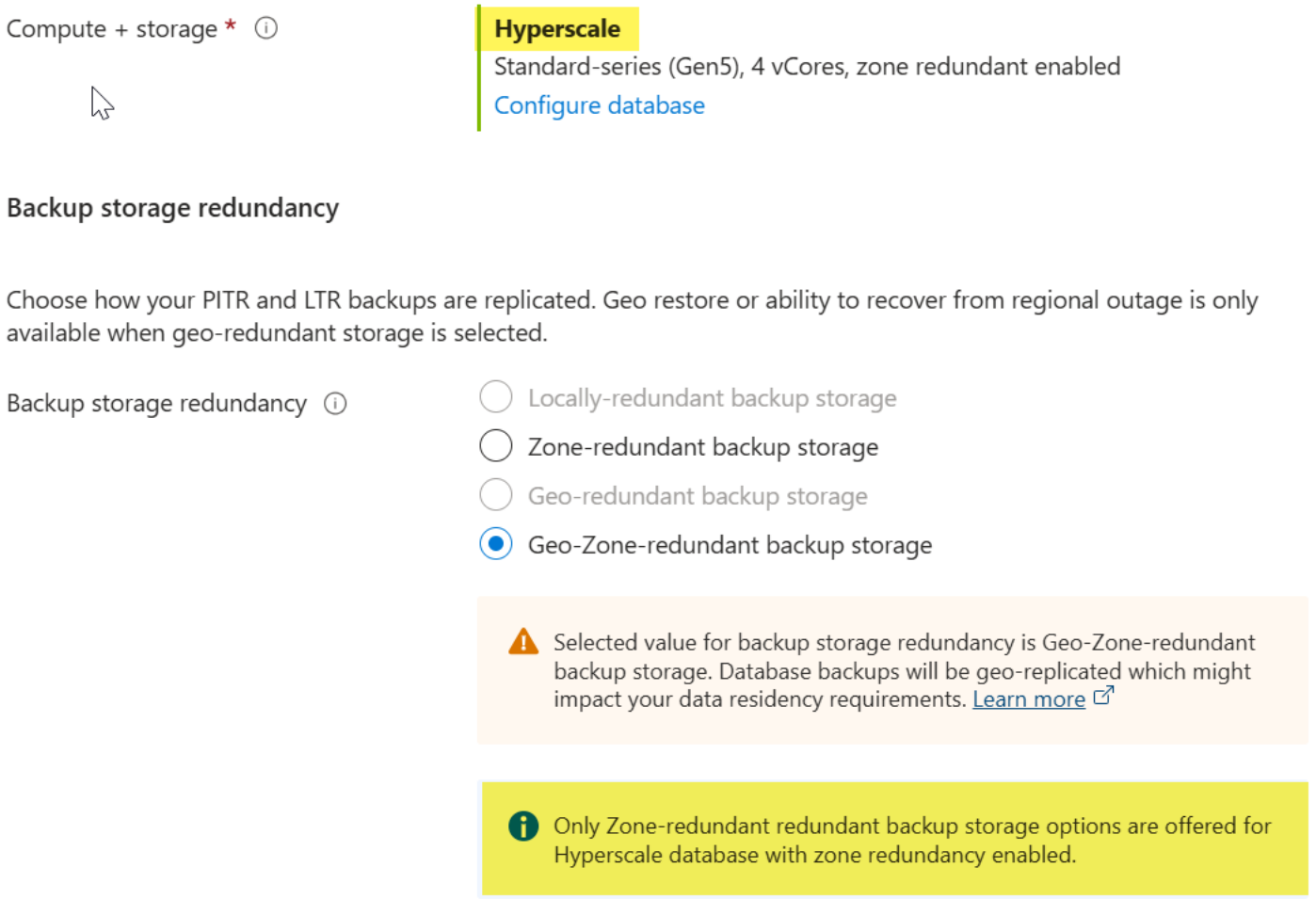
Copies backups synchronously across three AZs in the primary region.
Copies backups asynchronously to a single physical location in the paired secondary region.



Selecting backup redundancy - GP/BC



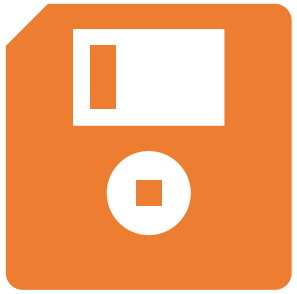
Selecting backup redundancy - Hyperscale



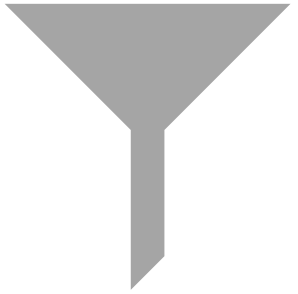
Recovery

A backup is only good if it can be restored!

Restores



Easy button - no more figuring out which series of backups to restore



Go to portal, PowerShell, or CLI and specify the name of the database and the day and time to restore to

Restore scenarios

- Restore existing database to point in time (PITR) - same region, same server, new name.
- Restore deleted database to point in time - same region, same server, same name.
- Restore deleted database to another geographic region - only available for databases configured with GRS or GZRS - different server, same name.
- Restore database from specific long-term backup - different server, same or different name.

Hot tip

- Many factors affect recovery time
  - Size of the database (GB/TB)
  - Compute size of the database (vCores, storage)
  - Number of transaction logs involved
  - Amount of activity that needs to be replayed to recover to the restore point
  - Network bandwidth if the restore is to a different region
  - Number of concurrent restore requests that are processed in the target region
- When restoring, create the new database with more compute than needed.
- When restore is finished, scale to the desired size.

Demo

Point-in-time restore

PowerShell

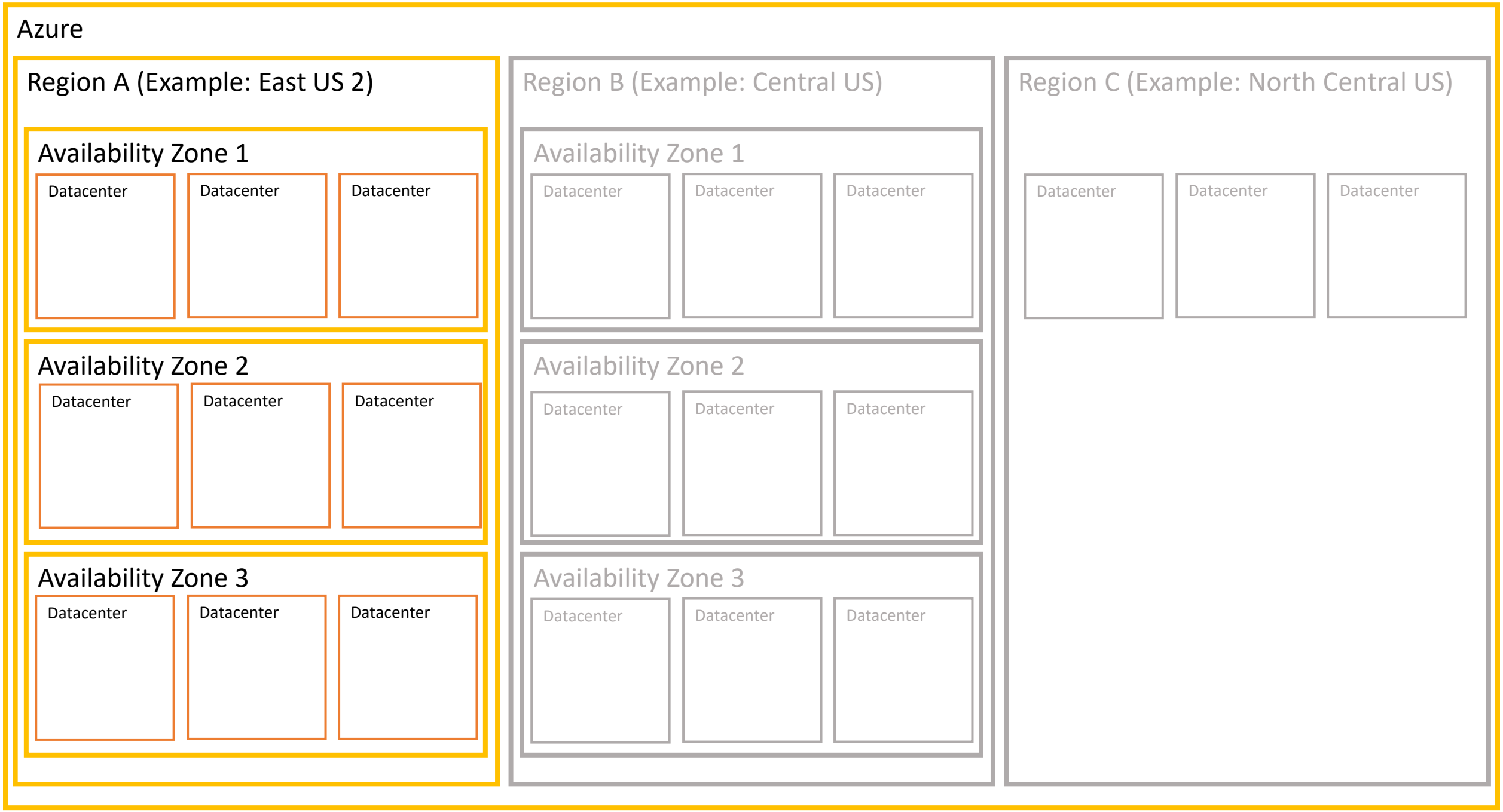
```
$Database = Get-AzSqlDatabase -ResourceGroupName "acmedevus" `
    -ServerName "sql049eastus2" `
    -DatabaseName "WideWorldImporters"
Restore-AzSqlDatabase -FromPointInTimeBackup `
    -PointInTime "2024-07-29T15:00:00Z" `
    -ResourceGroupName $Database.ResourceGroupName `
    -ServerName $Database.ServerName `
    -TargetDatabaseName "WideWorldImporters_20240729" `
    -ResourceId $Database.ResourceID
```

CLI

```
az sql db restore --dest-name WideWorldImporters_20240729 `
    --edition GeneralPurpose `
    --name WideWorldImporters `
    --resource-group acmedevus `
    --server sql049eastus2 `
    --subscription acme_subscription `
    --time "2024-07-29T15:00:00"
```

High Availability

Built in – DBAs don’t customize in Azure


Azure
Region A (Example: East US 2)
Availability Zone 1
Datacenter
Datacenter
Datacenter
Availability Zone 2
Datacenter
Datacenter
Datacenter
Availability Zone 3
Datacenter
Datacenter
Datacenter
Region B (Example: Central US)
Availability Zone 1
Datacenter
Datacenter
Datacenter
Availability Zone 2
Datacenter
Datacenter
Datacenter
Availability Zone 3
Datacenter
Datacenter
Datacenter
Region C (Example: North Central US)
Datacenter
Datacenter
Datacenter

High availability (HA) is built in

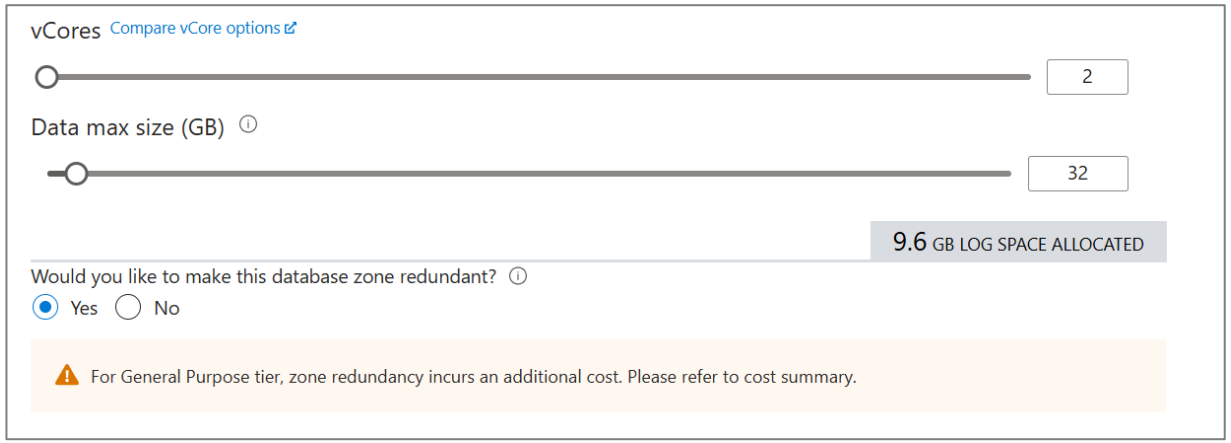
- Different tiers have different architectures

Availability Zones

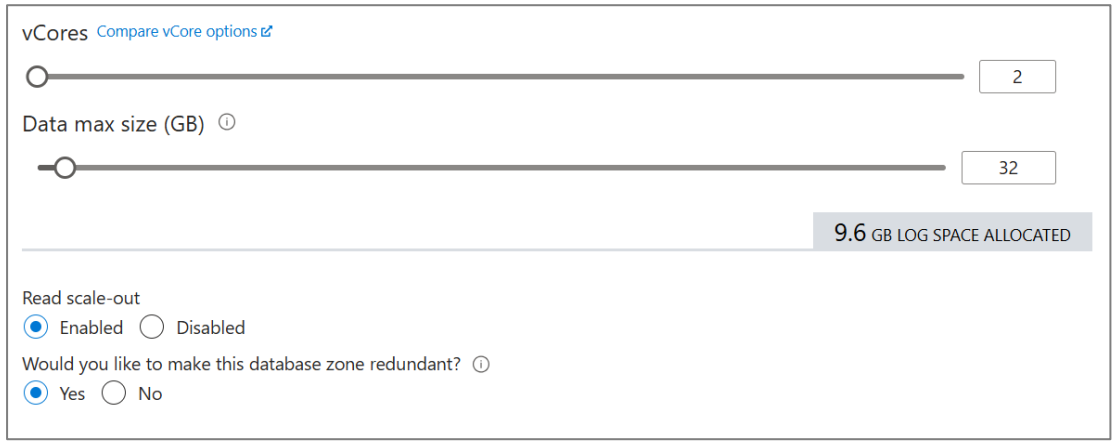
- By default, all compute nodes and data storage are provisioned in the same datacenter in one region
- Availability Zones allow the compute and storage to be provisioned across multiple data centers in the same region
  - Reduces single point of failure during an outage or disaster
  - Helps companies that need to follow data residency laws achieve HA and some level of DR without going outside of their boundaries

Enable AZs during creation

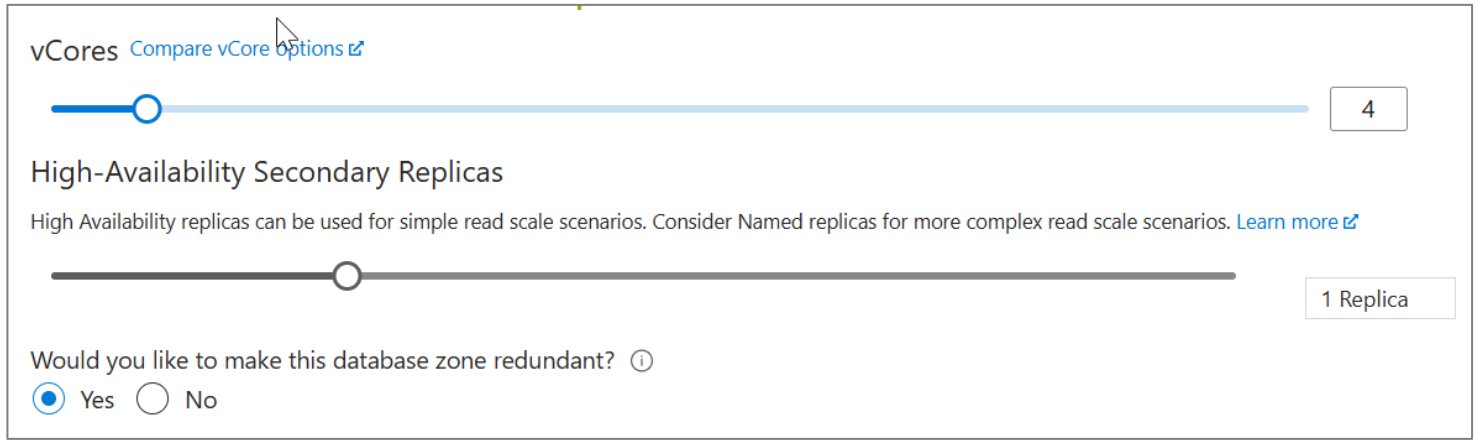
GP



BC

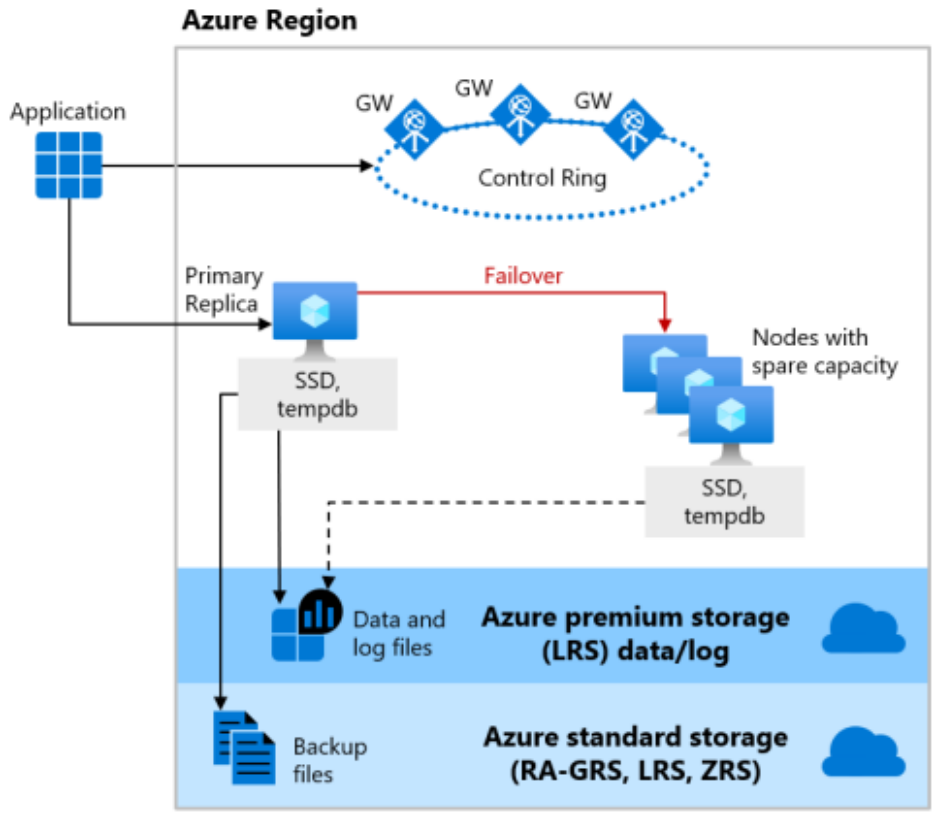


Hyperscale



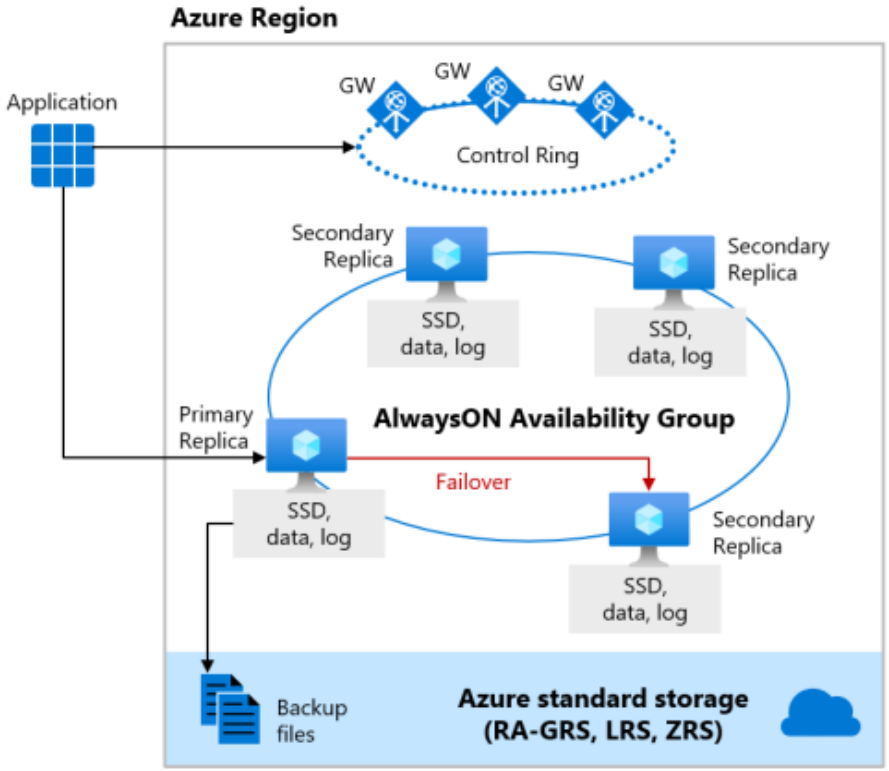
General Purpose

- Separate compute and storage
- The high availability is at the storage level
- During failover, a new stateless compute replica is created and data and log files are attached to it
- Slower failover because the new compute node must start the sqlservr.exe process with a cold cache
- No readable secondary



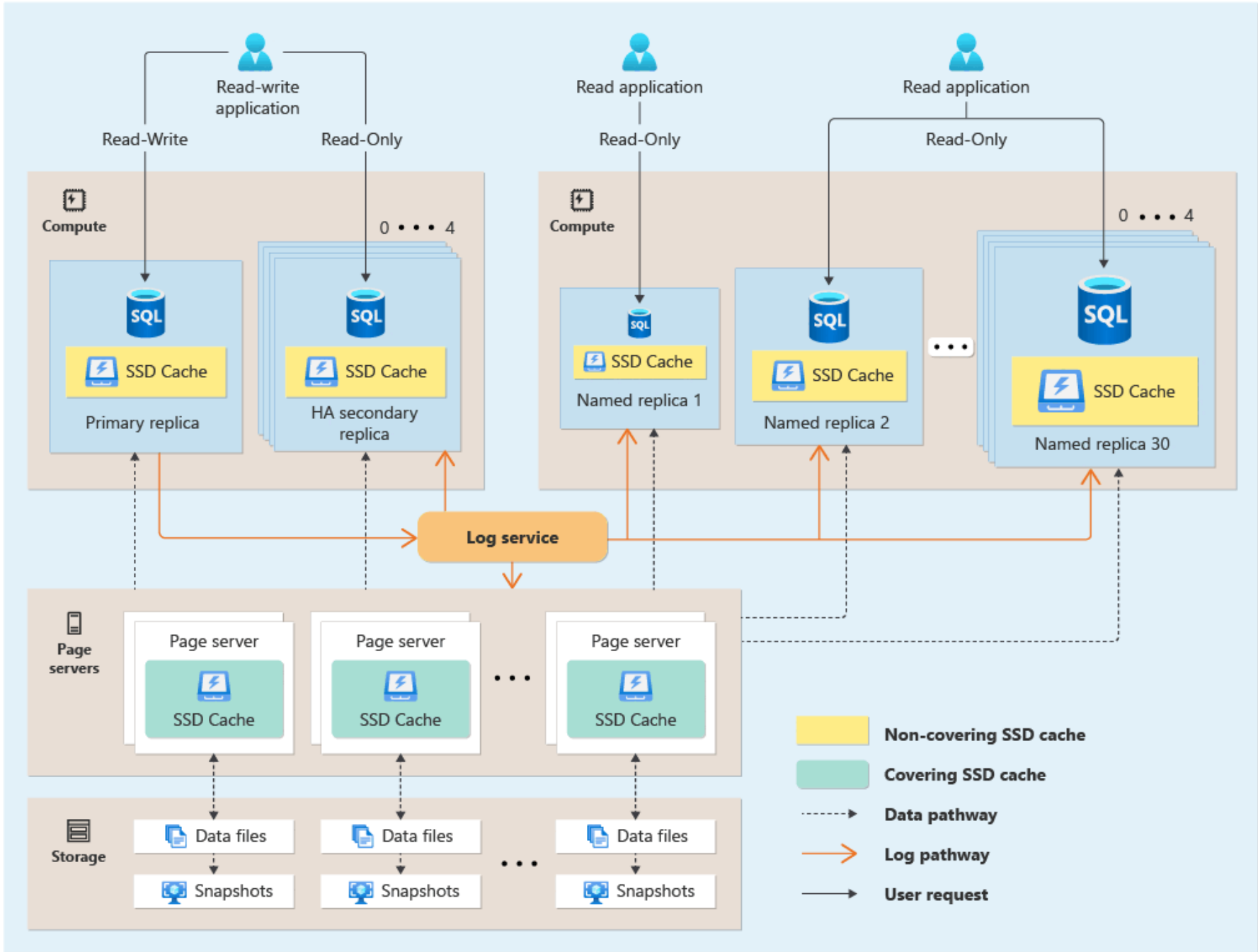
Business Critical

- Integrated compute and local SSD storage in a cluster
- At least three nodes exist in the same region
- During failover, primary fails over to a fully-synchronized secondary
- Faster failover because compute is already provisioned, and data is in sync
- Readable secondaries!
- Does this sound like an Always On availability group? It is!



Hyperscale

- 4 layers of redundancy
- Compute
  - Can have multiple nodes as failover targets
- Page Server storage
  - Every page server has an active-active paired server
- Transaction Log storage
  - Uses Azure Storage for availability and redundancy
- Database file storage
  - Uses Azure Storage for availability and redundancy


Region 1
Read-write application
Read-Write
Read-Only
Read application
Read-Only
Read application
Read-Only
Compute
0 • • • 4
SQL
SSD Cache
Primary replica
HA secondary replica
Named replica 1
Named replica 2
Named replica 30
Log service
Page servers
Page server
Storage
Data files
Snapshots
Non-covering SSD cache
Covering SSD cache
Data pathway
Log pathway
User request

What else DBAs and devs need to know

The database **can** and **will be** failed over automatically between HA replicas for patching and maintenance.

All apps need to have retry logic built in.

Disaster Recovery

Customers can configure this!

Three options

Feature	Geo-replicated backups	Active geo-replication	Failover group
Automatic failover	No	No	Yes
User must update connection string after failover	Yes	Yes	No
Can be in non-paired region	No	Yes	Yes
One or many databases	One	One	One or many
Set up at which level?	Database	Database	Server

Restore geo-replicated backup

Backup redundancy of GRS or GZRS (HS only) must be selected

Restore will be to last point of most recently replicated backup file

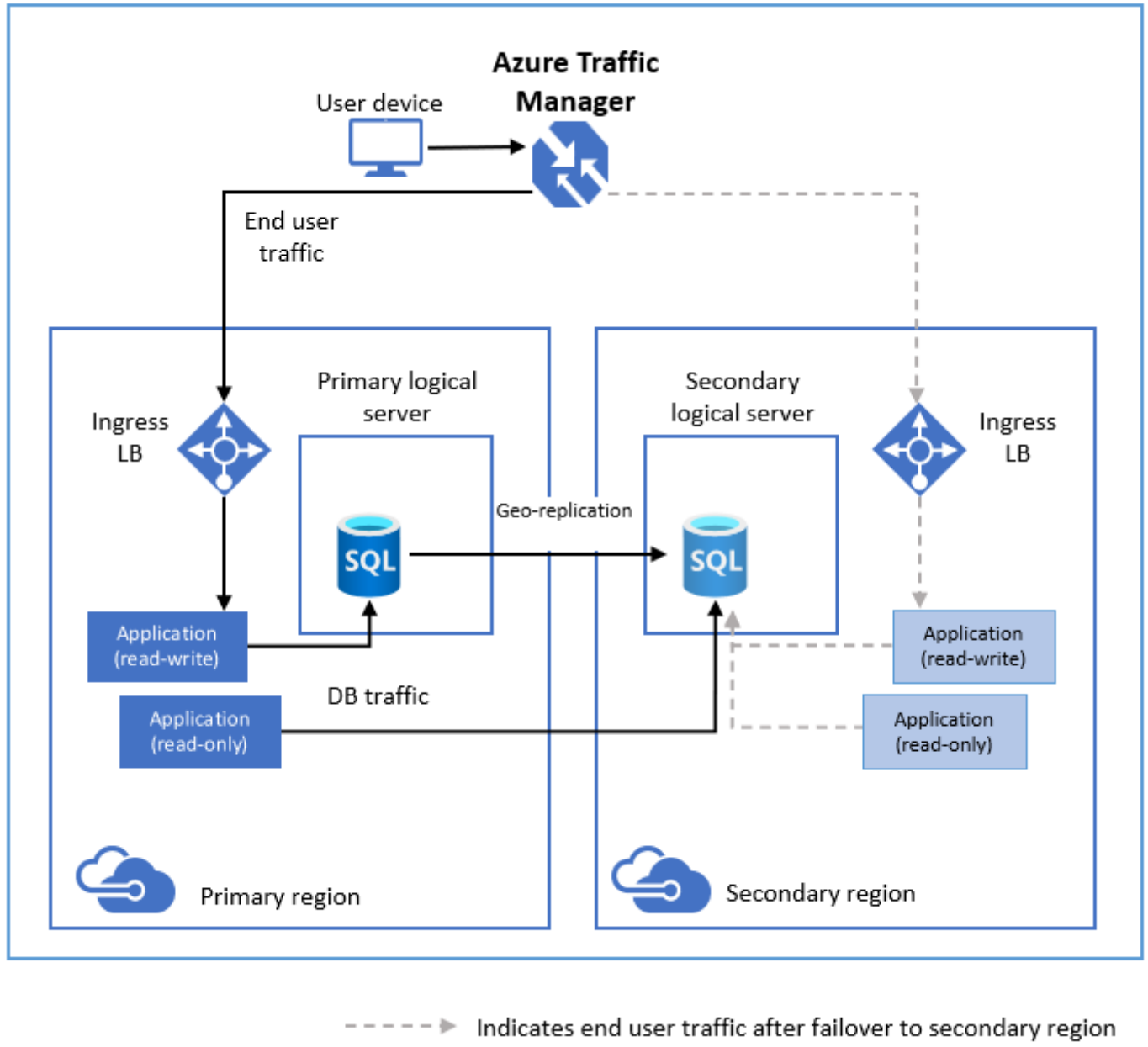
RPO - up to 1 hour

RTO - usually takes less than 12 hours but could take longer, depending on size and activity - in a regional outage, the paired region will have more activity

Portal, PowerShell, CLI, REST API

Active geo-replication

- Set up at SQL Database level – one database at a time
- Create up to four readable secondary databases in different region(s)
- Asynchronous replication from primary to secondaries
- Failover: manual
- On failover, update application connection string to new server name


Azure Traffic Manager
User device
End user traffic
Ingress LB
Primary logical server
SQL
Geo-replication
Secondary logical server
SQL
Ingress LB
Application (read-write)
Application (read-only)
DB traffic
Application (read-write)
Application (read-only)
Primary region
Secondary region
Indicates end user traffic after failover to secondary region

Search (Ctrl+/)

Data management

Replicas

Sync to other databases

Integrations

Create replica | Refresh | Feedback

Geo replicas for your database[illegible] listed
center outage. Learn more

Name | Server | [illegible]te

No replicas found

Database details

Enter required settings for this database, including picking a logical server and configuring the compute and storage resources

Database name: ap1

Server *: testsyncserver (Japan East)
Create new

Region: Japan East

Want to use SQL elastic pool? ○ Yes ◉ No

Compute + storage *:
General Purpose
Gen5, 2 vCores, 32 GB storage, zone redundant disabled
Configure database

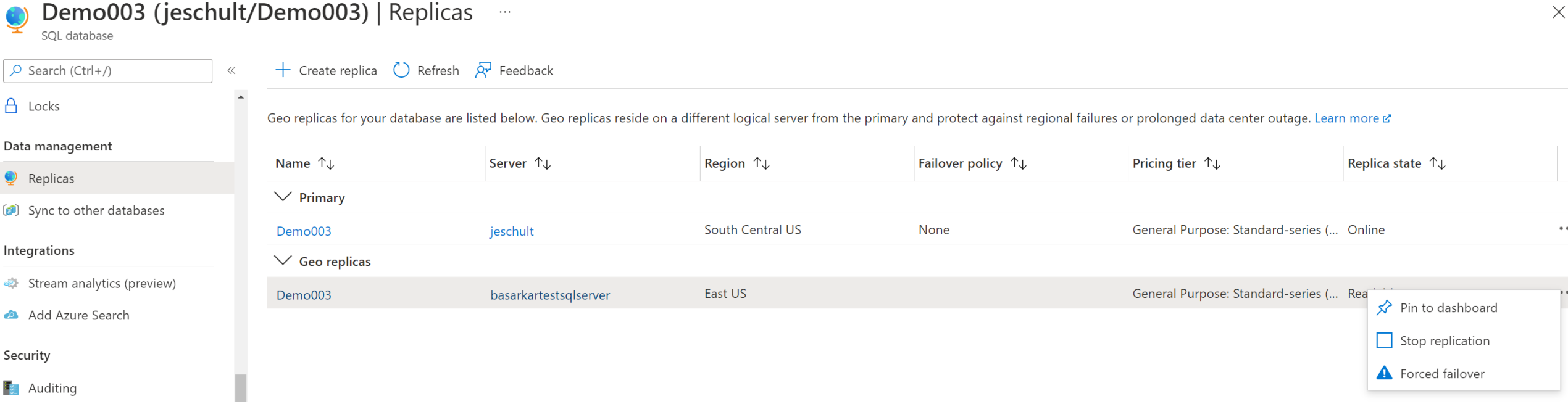
Backup storage redundancy

Choose how your PITR and LTR backups are replicated. Geo restore or ability to recover from regional outage is only available when geo-redundant storage is selected.

The default backup storage redundancy setting is taken from the setting of the source.

Backup storage redundancy:
○ Locally-redundant backup storage
○ Zone-redundant backup storage
◉ Geo-redundant backup storage

⚠ Selected value for backup storage redundancy is Geo-redundant backup storage. Database backups will be geo-replicated which might impact your data residency requirements. Learn more


Demo003 (jeschult/Demo003) | Replicas
SQL database
Search (Ctrl+/)
Locks
Data management
Replicas
Sync to other databases
Integrations
Stream analytics (preview)
Add Azure Search
Security
Auditing
Create replica
Refresh
Feedback
Geo replicas for your database are listed below. Geo replicas reside on a different logical server from the primary and protect against regional failures or prolonged data center outage. Learn more
Name
Server
Region
Failover policy
Pricing tier
Replica state
Primary
Demo003
jeschult
South Central US
None
General Purpose: Standard-series (...
Online
Geo replicas
Demo003
basarkartestsqlserver
East US
General Purpose: Standard-series (...
Pin to dashboard
Stop replication
Forced failover

Why choose active geo-replication?

The app has one database

The app can benefit from one or more readable secondary replicas

The RTO is high enough to allow for manual failover to the replica and time to update the connection string

Demo

Active geo-replication

Failover groups

- Abstraction of geo-replication
- Set up at SQL *server* level!
- One or more databases in a group
- Readable secondaries behind a load balancer with a listener
- Can have a read-write listener or read-only listener
- Failover: automatic or manual
- On failover, if application is directed to listener name, no need to update connection string

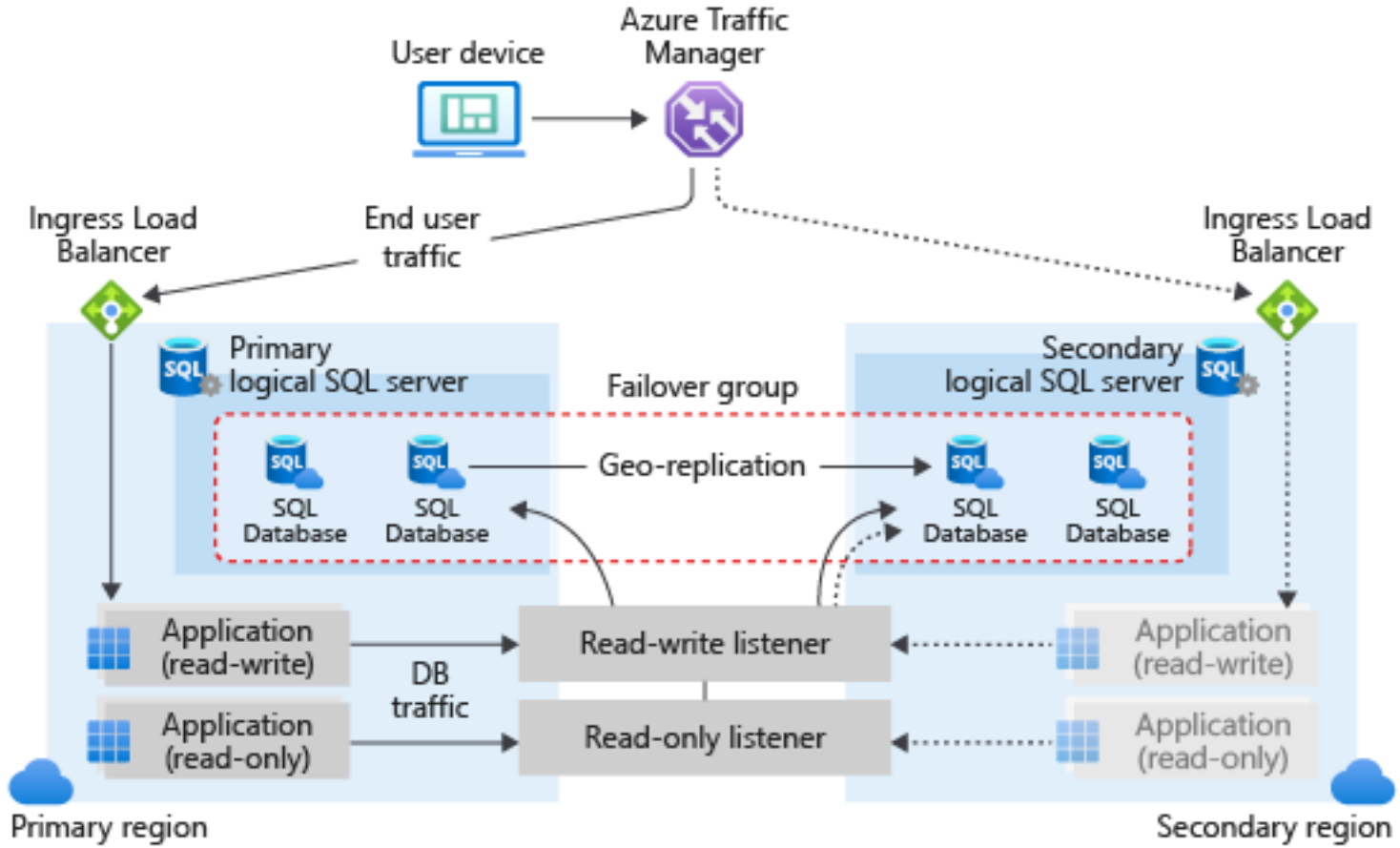
Failover policy

Customer managed failover policy (recommended)

- One or more databases in a failover group is impacted by an outage and become unavailable. You can choose to fail over.

Microsoft managed failover policy

- Azure Service fabric detects failure that cannot be mitigated by the built-in high availability infrastructure due to the scale of the impact.
- With **GracePeriodWithDataLossHours**, you can control how long the system waits before initiating the failover that is likely to result in data loss.
  - Failover only occurs after minimum grace period has expired – **minimum 1 hour.**
- When these conditions are met, the Azure SQL service initiates forced failovers for all failover groups in the region that have the failover policy set to Microsoft managed.
- Read Only Listener disabled after failover by default to avoid performance impact on the new primary, but you can change it by configuring the **AllowReadOnlyFailoverToPrimary** property.


User device
Azure Traffic Manager
Ingress Load Balancer
End user traffic
Ingress Load Balancer
Primary logical SQL server
Failover group
Secondary logical SQL server
Geo-replication
SQL Database
SQL Database
SQL Database
SQL Database
Application (read-write)
Application (read-only)
DB traffic
Read-write listener
Read-only listener
Application (read-write)
Application (read-only)
Primary region
Secondary region

jeschult | Failover groups

SQL server

Search (Ctrl+/)

- SQL elastic pools
- DTU quota
- Properties
- Locks

Data management

- Backups
- Deleted databases
- Failover groups

Add group | Refresh

Failover group are a SQL server feature designed to automatically manage replication, connectivity and failover of a set of databases.

Name	Primary server	Secondary server	Read/Write failover poli...	Grace Period (minutes)	Database count

Failover group

Create a failover group to automatically failover databases in it.

Failover group name *

fogdemo001

.database.windows.net

Server *

basarkartestsqlserver

Create new

Read/Write failover policy

Automatic

Read/Write grace period (hours)

1 hours

Database within the group

2 databases selected

4 databases eligible

Configure database

fogdemo001

jeschult

Save | Discard | Add databases | Edit configuration | Remove databases | Failover | Forced Failover | Delete

Configuration details | Databases within group | Databases selected to be added (0) | Databases selected for removal (0)

	Server	Role	Read/Write failover policy	Grace period
	jeschult (South Central US)	Primary	Automatic	1 hours
	basarkartestsqlserver (East US)	Secondary		

Read/write listener endpoint

fogdemo001.database.windows.net

Read-only listener endpoint

fogdemo001.secondary.database.windows.net

Why choose failover groups?

App has multiple databases that need to fail over together

The RTO is low enough that failover must be automatic and the connection string can’t be updated manually

Demo

Failover groups

Recap

Backups

- Azure SQL Database automatically takes backups
- Backups can be stored in multiple regions

Restores

- Azure SQL Database restores are simple – provide the date and time you want to restore to

HA (High Availability)

- HA is built into every tier of Azure SQL Database

DR (Disaster Recovery)

- Geo-replicated backups
- Active geo-replication for a single database
- Failover groups at the SQL server level for multiple databases

Questions?

Resources

- Automatic, geo-redundant backups - Azure SQL Database
- Automatic, geo-redundant backups - Azure SQL Managed Instance
- Restore a database from a backup - Azure SQL Database
- Restore a database from a backup - Azure SQL Managed Instance
- Availability through local and zone redundancy - Azure SQL Database
- Availability through local and zone redundancy - Azure SQL Managed Instance
- Active geo-replication - Azure SQL Database
- Auto-failover groups overview & best practices - Azure SQL Database
- Failover groups overview & best practices - Azure SQL Managed Instance
- Disaster recovery drills - Azure SQL Database
- Disaster recovery drills - Azure SQL Managed Instance