Designing a Disaster Recovery Strategy on Microsoft Azure

DETERMINING RECOVERY REQUIREMENTS

Daniel Krzyczkowski

MICROSOFT MVP & SOFTWARE DEVELOPER

@DKrzyczkowski   www.techmindfactory.com

Course Overview

Determining recovery requirements

Working with data backup in Azure

Failure Mode Analysis for Azure applications

Designing a geo-replication strategy

Summary

Module Overview

Design and implement disaster recovery for applications on Azure

Explanation of RTO, RPO, and RLO

Disaster recovery concepts for the popular Azure PaaS services like Azure App Service, Azure SQL, Cosmos DB and Storage Account

Working with the Traffic Manager

Resiliency Checklist for Specific Azure Services

Disaster Recovery (DR)

Describes steps which are done to re-establish availability of the solution after an outage

It refers to restoring systems and data to a previous acceptable state in the event of partial or complete failure due to natural or technical causes
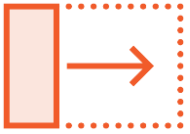
Resiliency

Ability of a system to recover from failures and continue to function

Every technology has its own particular failure modes, which has to be considered when designing and implementing application solution

Important Questions to Ask

How much do we invest in making our application highly available?

How much does potential downtime cost our business?

What are our customer's availability requirements?

How to Implement Resiliency?

Determine subscription and service requirements

Apply Resiliency Strategies

Plan for a usage patterns

Identify a distinct workloads

How to Implement Resiliency?

Operate in the multiple regions

Monitor third-party services

Apply load balancing

Identify possible failure points in the system

Azure Paired Regions

An Azure region is an area within a geography, containing one or more datacenters

Each Azure region is paired with another region within the same geography, together making a regional pair
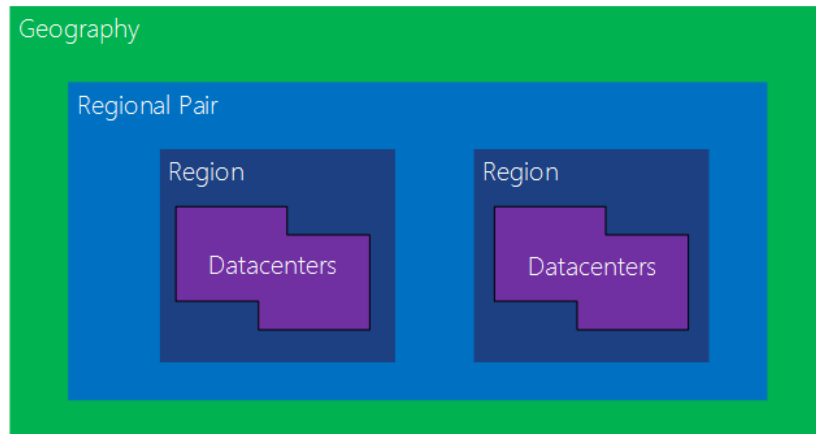
Azure Regional Pairs

Europe

North Europe (Ireland)

Europe

West Europe (Netherlands)

Azure Regional Pairs

Geography	Paired regions	
Asia	East Asia	Southeast Asia
Australia	Australia East	Australia Southeast
Australia	Australia Central	Australia Central 2
Brazil	Brazil South	South Central US
Canada	Canada Central	Canada East
China	China North	China East
China	China North 2	China East 2
Europe	North Europe (Ireland)	West Europe (Netherlands)
France	France Central	France South
Germany	Germany Central	Germany Northeast

Azure Availability Zones
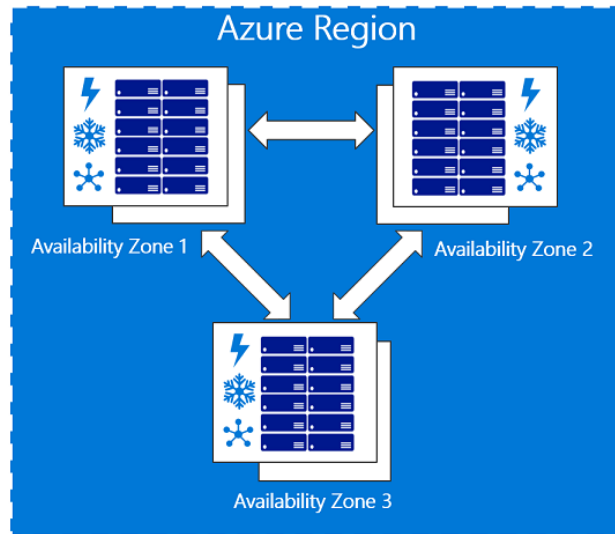
Availability Zones are unique physical locations within an Azure region

To ensure resiliency, there's a minimum of three separate zones in all enabled regions
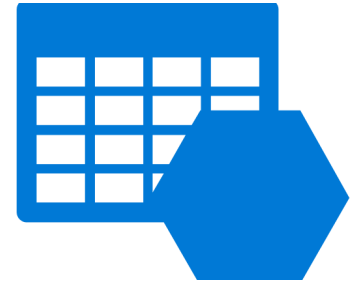
Azure PaaS Services in This Course

Azure Web App (App Service)

Azure SQL Database

Azure Cosmos DB

Azure Storage Account

Azure Web App
(App Service)

HTTP-based service for hosting web applications, REST APIs, and mobile back ends

Multiple languages and frameworks
- ASP .NET
- Java
- PHP

Global scale with high availability

Azure SQL Database

General-purpose relational database, provided as a managed service

Enables processing both relational data and non-relational structures, such as:

- JSON
- XML
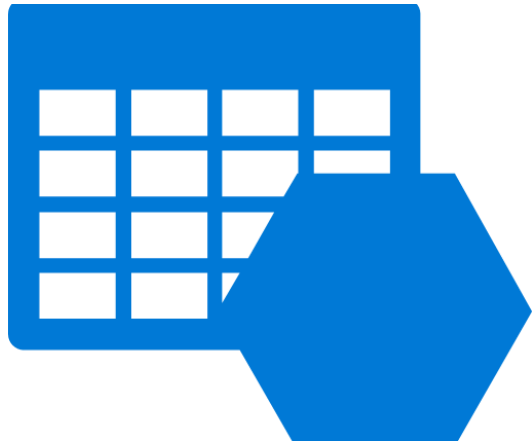
Provides advanced monitoring and troubleshooting features

Azure Cosmos DB

Globally distributed, multi-model database service

Data access through different APIs:
- MongoDB
- SQL

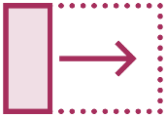**Enables elastically and independently scaling throughput and storage across many of Azure regions worldwide**

Azure Storage Account

Cloud storage solution for modern data storage scenarios

Azure Storage includes these data services:

- Azure Blobs
- Azure Files
- Azure Queues
- Azure Tables

Resiliency Checklist for Azure App Service

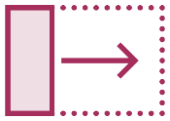Use Standard or Premium tier

Avoid scaling up or down

Create separate App Service plans for production and test

Enable diagnostics logging

Resiliency Checklist for Azure SQL Database

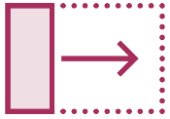Use Standard or Premium tier

Enable SQL Database auditing
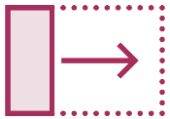
Use Active Geo-Replication

Use point-in-time restore to recover from human error

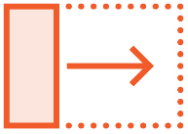# Resiliency Checklist for Azure Cosmos DB

Replicate the database across regions

Optionally enable multi-master (multiple writes regions)

Resiliency Checklist for Azure Storage Account

For application data, use read-access geo-redundant storage

For VM disks, use managed disks

For Queue storage, create a backup queue in another region

# Determine and Document RTO, RPO, and RLO Recovery Requirements

The Recovery Time Objective (RTO)

The duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity

The Recovery Time Objective (RTO)

System Failure

System Recovery

System Recovered
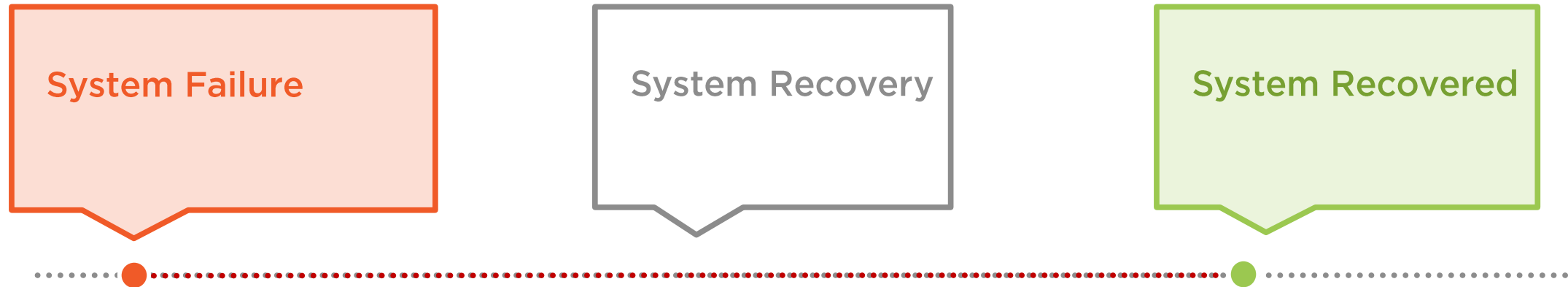
Recovery Point Objective (RPO)

Describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold
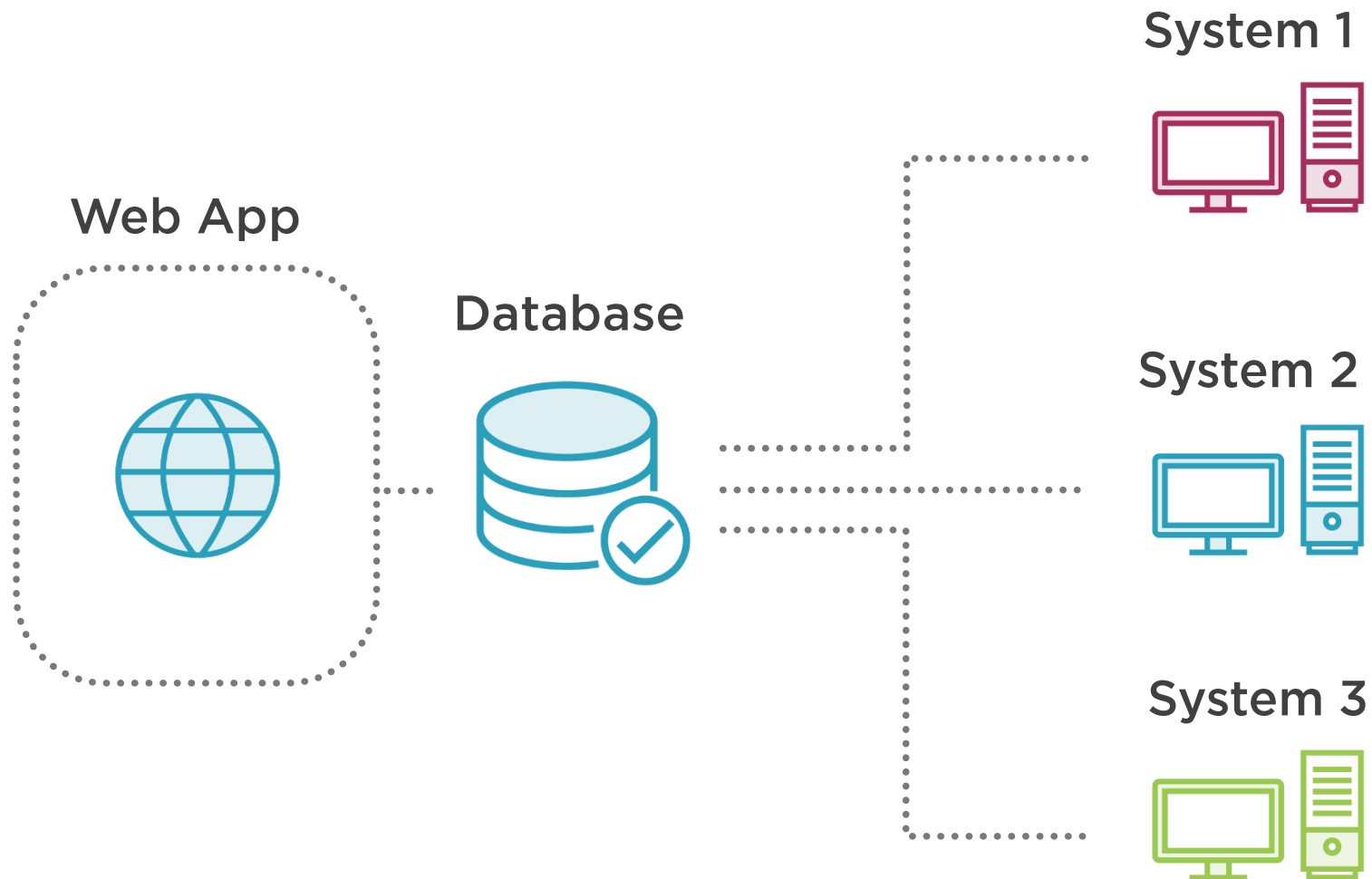
Recovery Level Objective (RLO)

Defines the granularity with which data has to be rocovered. Whether recovery is required for the whole instance, database or set of databases or specific tables

Recovery Level Objective (RLO)

Web App

Database

System 1

System 2

System 3

Backup and Disaster Recovery for Azure Applications

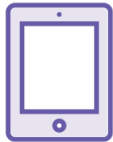Many Azure services include features that support resiliency and availability

Evaluating each service independently is likely to improve disaster recovery plan

Disaster Recovery Plan

Evaluate the business impact of application failures

Automate the process as much as possible

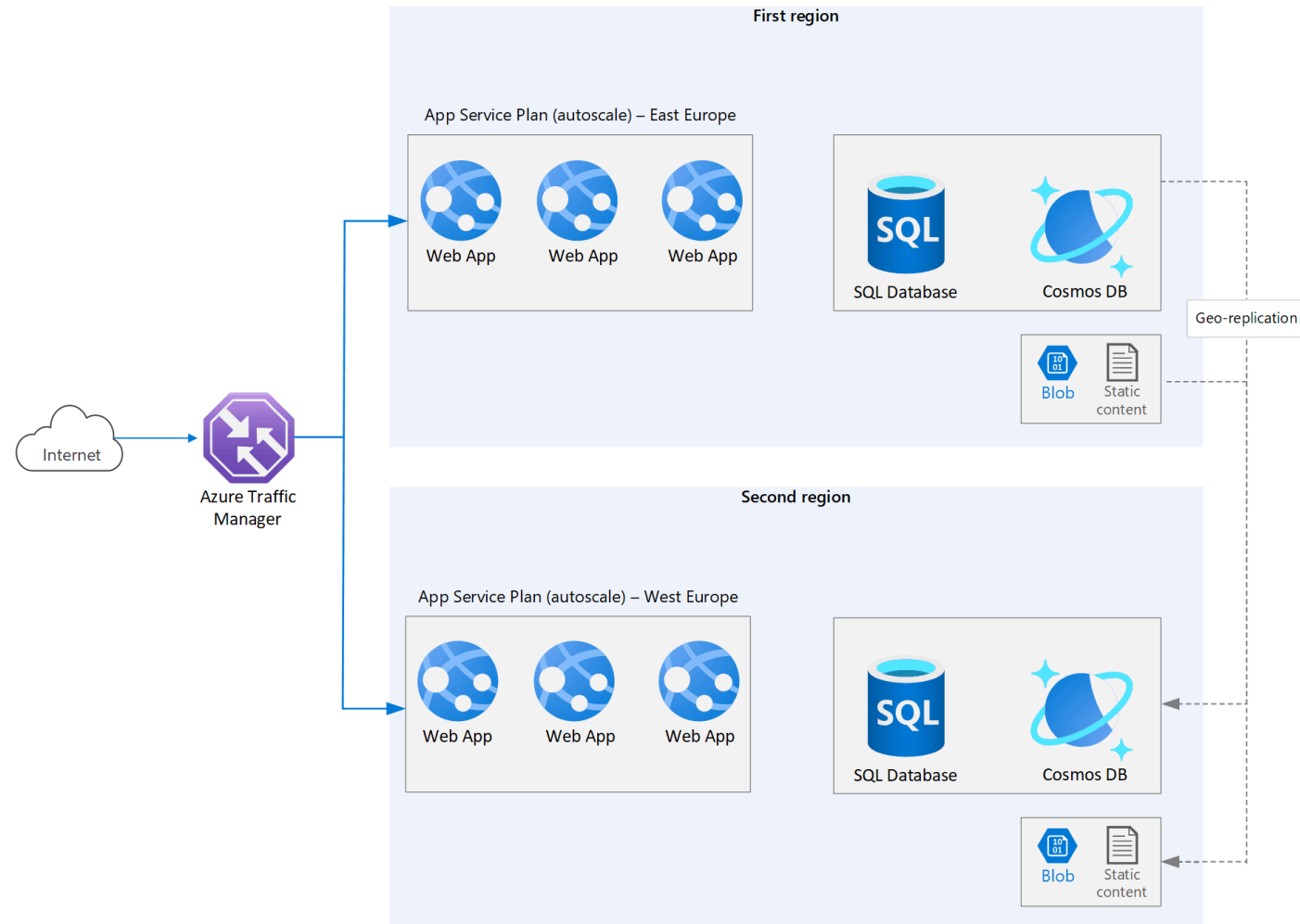Document the process, especially any manual steps
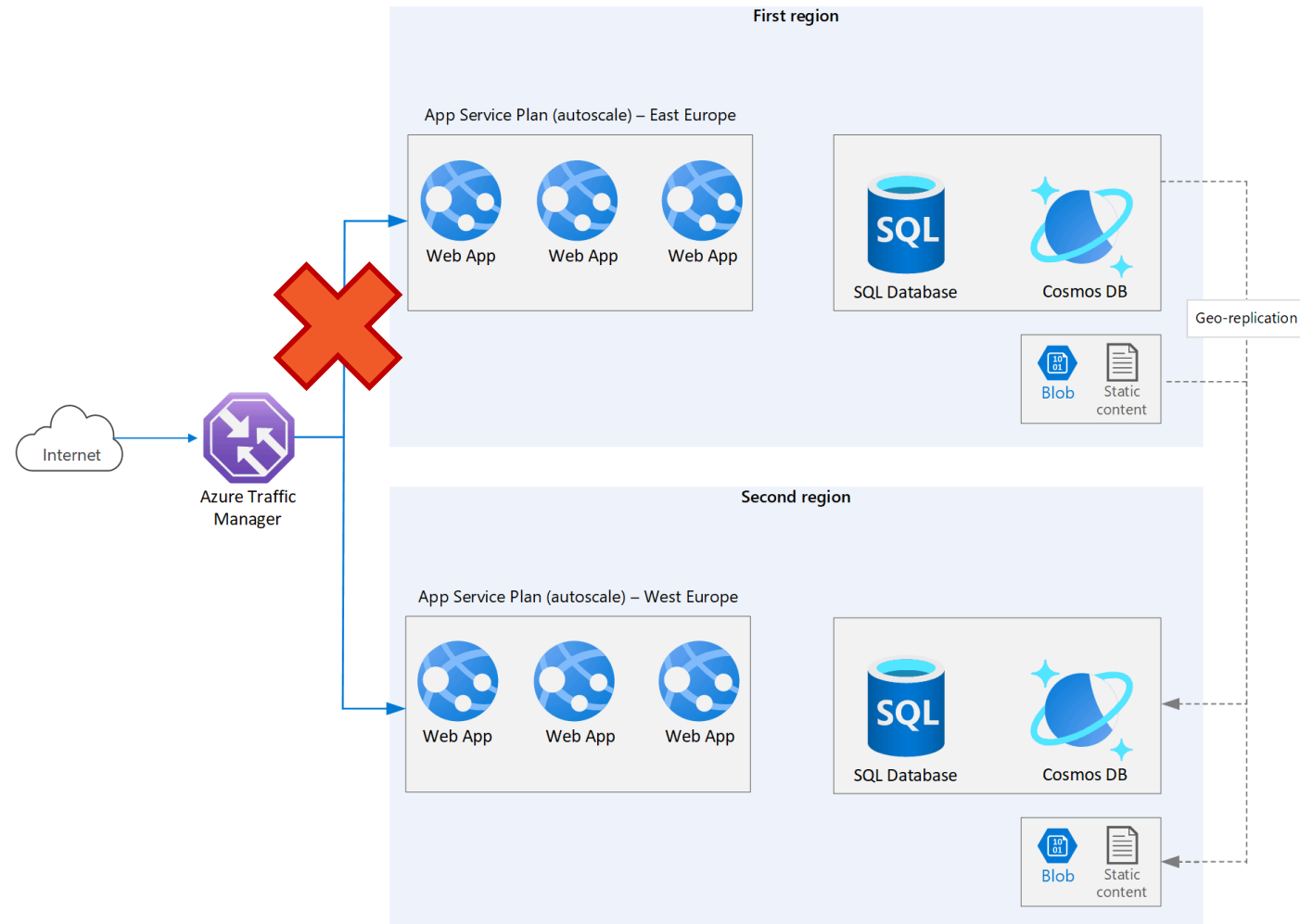
Choose a cross-region recovery architecture

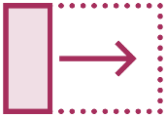Perform regular disaster simulations to validate and improve the plan

Multiple Azure Regions for High Availability

Multiple Azure Regions for High Availability

Data Corruption and Restoration

Backups protect from losing a component of the application because of accidental deletion or data corruption

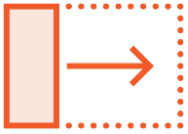The frequency of running the backup process determines the RPO

Azure automatically stores Azure Storage and SQL Database data three times within different fault domains in the same region

 In case data is corrupted or deleted in the primary copy, all the changes replicate to the other copies

High Availability with Azure App Service

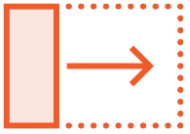Scales out up to 30 virtual machnines (VMs) instances

Standard and Premium tiers support staging slots and automated backups

Provides deployment slots to hold the last-known-good (LKG) deployment. If there is a problem discovered later, there is a quick way to revert to the LKG version

High Availability with Azure Cosmos DB

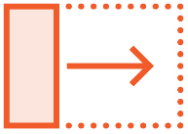Supports geo-replication across regions

Supports multiple write regions (multi-master)

The client SDK automatically sends write requests to the current write region after a failover

High Availability with Azure SQL Database

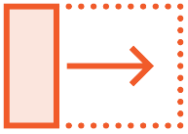Active Geo-Replication enables creating a readable secondary replica in a different region

There can be up to four readable secondary replicas

Fail over to a secondary database if primary database fails or needs to be taken offline

High Availability with Azure Storage Account

Read-access geo-redundant storage (RA-GRS) replicates the data to a secondary region, and provides read-only access from the secondary region
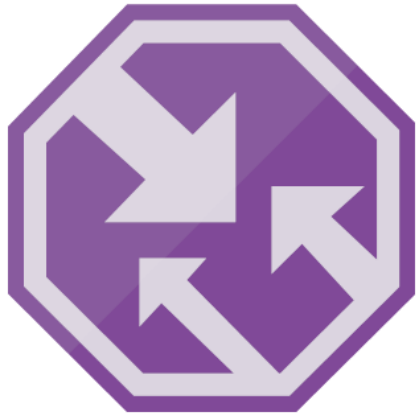
In case of a storage outage in the primary region, the application can read the data from the secondary region

The data in the Microsoft Azure storage account is always replicated to ensure durability and high availability

Azure Traffic Manager

DNS-based traffic load balancer that enables distribution of a traffic optimally to services across global Azure region

Delivers high availability for critical applications by monitoring endpoints and providing automatic failover when an endpoint goes down

Demo

Create and configure Azure Traffic Manager in the Azure portal

- Create a Traffic Manager profile
- Add Traffic Manager endpoints
- Test Traffic Manager profile

Summary

Resiliency Checklist for Specific Azure Services: Azure App Service, Azure SQL, Cosmos DB and Storage Account

Explanation of RTO, RPO, and RLO

Azure Traffic Manager configuration