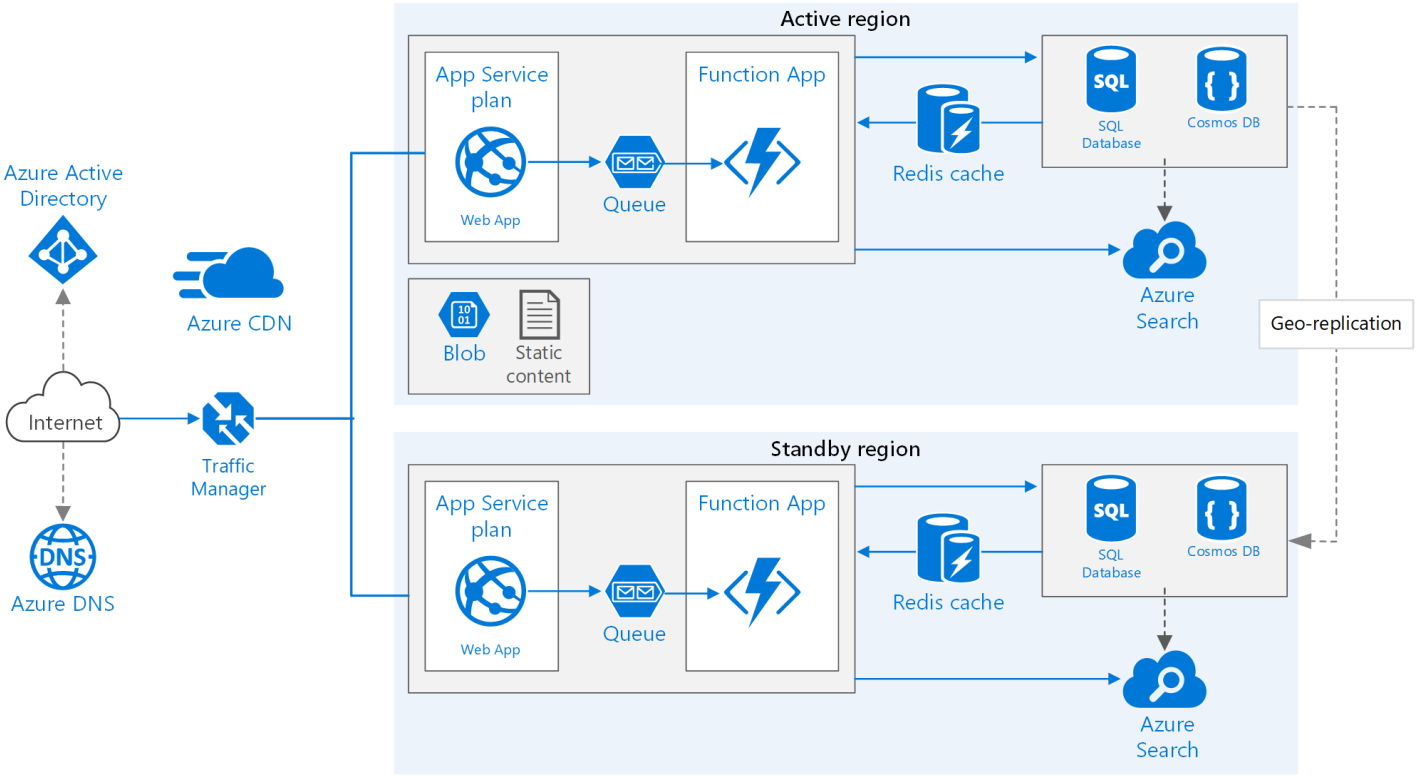
Run a web application in multiple Azure regions for high availability

10/25/2018 • 8 minutes to read • Contributors all

In this article

This reference architecture shows how to run an Azure App Service application in multiple regions to achieve high availability.



Download a Visio file of this architecture.

Architecture

This architecture builds on the one shown in Improve scalability in a web application. The main differences are:

- **Primary and secondary regions**. This architecture uses two regions to achieve higher availability. The application is deployed to each region. During normal operations, network traffic is routed to the primary region. If the primary region becomes unavailable, traffic is routed to the secondary region.
- **Azure DNS**. Azure DNS is a hosting service for DNS domains, providing name resolution using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

- **Azure Traffic Manager**. Traffic Manager routes incoming requests to the primary region. If the application running that region becomes unavailable, Traffic Manager fails over to the secondary region.
- **Geo-replication** of SQL Database and Cosmos DB.

A multi-region architecture can provide higher availability than deploying to a single region. If a regional outage affects the primary region, you can use Traffic Manager to fail over to the secondary region. This architecture can also help if an individual subsystem of the application fails.

There are several general approaches to achieving high availability across regions:

- Active/passive with hot standby. Traffic goes to one region, while the other waits on hot standby. Hot standby means the VMs in the secondary region are allocated and running at all times.
- Active/passive with cold standby. Traffic goes to one region, while the other waits on cold standby. Cold standby means the VMs in the secondary region are not allocated until needed for failover. This approach costs less to run, but will generally take longer to come online during a failure.
- Active/active. Both regions are active, and requests are load balanced between them. If one region becomes unavailable, it is taken out of rotation.

This reference architecture focuses on active/passive with hot standby, using Traffic Manager for failover.

Recommendations

Your requirements might differ from the architecture described here. Use the recommendations in this section as a starting point.

Regional pairing

Each Azure region is paired with another region within the same geography. In general, choose regions from the same regional pair (for example, East US 2 and Central US). Benefits of doing so include:

- If there is a broad outage, recovery of at least one region out of every pair is prioritized.
- Planned Azure system updates are rolled out to paired regions sequentially to minimize possible downtime.
- In most cases, regional pairs reside within the same geography to meet data residency requirements.

However, make sure that both regions support all of the Azure services needed for your application. See Services by region. For more information about regional pairs, see Business continuity and disaster recovery (BCDR): Azure Paired Regions.

Resource groups

Consider placing the primary region, secondary region, and Traffic Manager into separate resource groups. This lets you manage the resources deployed to each region as a single collection.

Traffic Manager configuration

Routing. Traffic Manager supports several routing algorithms. For the scenario described in this article, use *priority* routing (formerly called *failover* routing). With this setting, Traffic Manager sends all requests to the primary region unless the endpoint for that region becomes unreachable. At that point, it automatically fails over to the secondary region. See Configure Failover routing method.

Health probe. Traffic Manager uses an HTTP (or HTTPS) probe to monitor the availability of each endpoint. The probe gives Traffic Manager a pass/fail test for failing over to the secondary region. It works by sending a request to a specified URL path. If it gets a non-200 response within a timeout period, the probe fails. After four failed requests, Traffic Manager marks the endpoint as degraded and fails over to the other endpoint. For details, see Traffic Manager endpoint monitoring and failover.

As a best practice, create a health probe endpoint that reports the overall health of the application and use this endpoint for the health probe. The endpoint should check critical dependencies such as the App Service apps, storage queue, and SQL Database. Otherwise, the probe might report a healthy endpoint when critical parts of the application are actually failing.

On the other hand, don't use the health probe to check lower priority services. For example, if an email service goes down the application can switch to a second provider or just send emails later. This is not a high enough priority to cause the application to fail over. For more information, see the Health Endpoint Monitoring pattern.

SQL Database

Use Active Geo-Replication to create a readable secondary replica in a different region. You can have up to four readable secondary replicas. Fail over to a secondary database if your primary database fails or needs to be taken offline. Active Geo-Replication can be configured for any database in any elastic database pool.

Cosmos DB

Cosmos DB supports geo-replication across regions with multi-master (multiple write regions). Alternatively, you can designate one region as the writable region and the others as read-only replicas. If there is a regional outage, you can fail over by selecting another region to be the write region. The client SDK automatically sends write requests to the current write region, so you don't need to update the client configuration after a failover. For more information, see Global data distribution with Azure Cosmos DB.

> **Note**
>
> All of the replicas belong to the same resource group.

Storage

For Azure Storage, use read-access geo-redundant storage (RA-GRS). With RA-GRS storage, the data is replicated to a secondary region. You have read-only access to the data in the secondary region through a separate endpoint. If there is a regional outage or disaster, the Azure Storage team might decide to perform a geo-failover to the secondary region. There is no customer action required for this failover.

For Queue storage, create a backup queue in the secondary region. During failover, the app can use the backup queue until the primary region becomes available again. That way, the application can still process new requests.

Availability considerations - Traffic Manager

Traffic Manager automatically fails over if the primary region becomes unavailable. When Traffic Manager fails over, there is a period of time when clients cannot reach the application. The duration is affected by the following factors:

- The health probe must detect that the primary datacenter has become unreachable.
- Domain name service (DNS) servers must update the cached DNS records for the IP address, which depends on the DNS time-to-live (TTL). The default TTL is 300 seconds (5 minutes), but you can configure this value when you create the Traffic Manager profile.

For details, see About Traffic Manager Monitoring.

Traffic Manager is a possible failure point in the system. If the service fails, clients cannot access your application during the downtime. Review the Traffic Manager service level agreement (SLA) and determine whether using Traffic Manager alone meets your business requirements for high availability. If not, consider adding another traffic management solution as a fallback. If the Azure Traffic Manager service fails, change your canonical name (CNAME) records in DNS

to point to the other traffic management service. This step must be performed manually, and your application will be unavailable until the DNS changes are propagated.

Availability Considerations - SQL Database

The recovery point objective (RPO) and estimated recovery time (ERT) for SQL Database are documented in Overview of business continuity with Azure SQL Database.

Availability Considerations - Storage

RA-GRS storage provides durable storage, but it's important to understand what can happen during an outage:

- If a storage outage occurs, there will be a period of time when you don't have write-access to the data. You can still read from the secondary endpoint during the outage.
- If a regional outage or disaster affects the primary location and the data there cannot be recovered, the Azure Storage team may decide to perform a geo-failover to the secondary region.
- Data replication to the secondary region is performed asynchronously. Therefore, if a geo-failover is performed, some data loss is possible if the data can't be recovered from the primary region.
- Transient failures, such as a network outage, will not trigger a storage failover. Design your application to be resilient to transient failures. Possible mitigations:
  - Read from the secondary region.
  - Temporarily switch to another storage account for new write operations (for example, to queue messages).
  - Copy data from the secondary region to another storage account.
  - Provide reduced functionality until the system fails back.

For more information, see What to do if an Azure Storage outage occurs.

Manageability Considerations - Traffic Manager

If Traffic Manager fails over, we recommend performing a manual failback rather than implementing an automatic failback. Otherwise, you can create a situation where the application flips back and forth between regions. Verify that all application subsystems are healthy before failing back.

Note that Traffic Manager automatically fails back by default. To prevent this, manually lower the priority of the primary region after a failover event. For example, suppose the primary region is priority 1 and the secondary is priority 2. After a failover, set the primary region to priority 3, to prevent automatic failback. When you are ready to switch back, update the priority to 1.

The following commands update the priority.

PowerShell

PowerShell Copy

```
$endpoint = Get-AzureRmTrafficManagerEndpoint -Name <endpoint> -ProfileName <profile> -Re-
sourceGroupName <resource-group> -Type AzureEndpoints
$endpoint.Priority = 3
Set-AzureRmTrafficManagerEndpoint -TrafficManagerEndpoint $endpoint
```

For more information, see Azure Traffic Manager Cmdlets.

Azure CLI

Azure CLI | Copy

```
az network traffic-manager endpoint update --resource-group <resource-group> --profile-name
<profile> \
    --name <endpoint-name> --type azureEndpoints --priority 3
```

Manageability Considerations - SQL Database

If the primary database fails, perform a manual failover to the secondary database. See Restore an Azure SQL Database or failover to a secondary. The secondary database remains read-only until you fail over.