Multitier web application built for high availability and disaster recovery on Azure

11/16/2018 • 5 minutes to read • Contributors all

In this article

Relevant use cases
Architecture
Other considerations
Pricing

This example scenario is applicable to any industry that needs to deploy resilient multitier applications built for high availability and disaster recovery. In this scenario, the application consists of three layers.

- Web tier: The top layer including the user interface. This layer parses user interactions and passes the actions to next layer for processing.
- Business tier: Processes the user interactions and makes logical decisions about the next steps. This layer connects the web tier and the data tier.
- Data tier: Stores the application data. Either a database, object storage, or file storage is typically used.

Common application scenarios include any mission-critical application running on Windows or Linux. This can be an off-the-shelf application such as SAP and SharePoint or a custom line-of-business application.

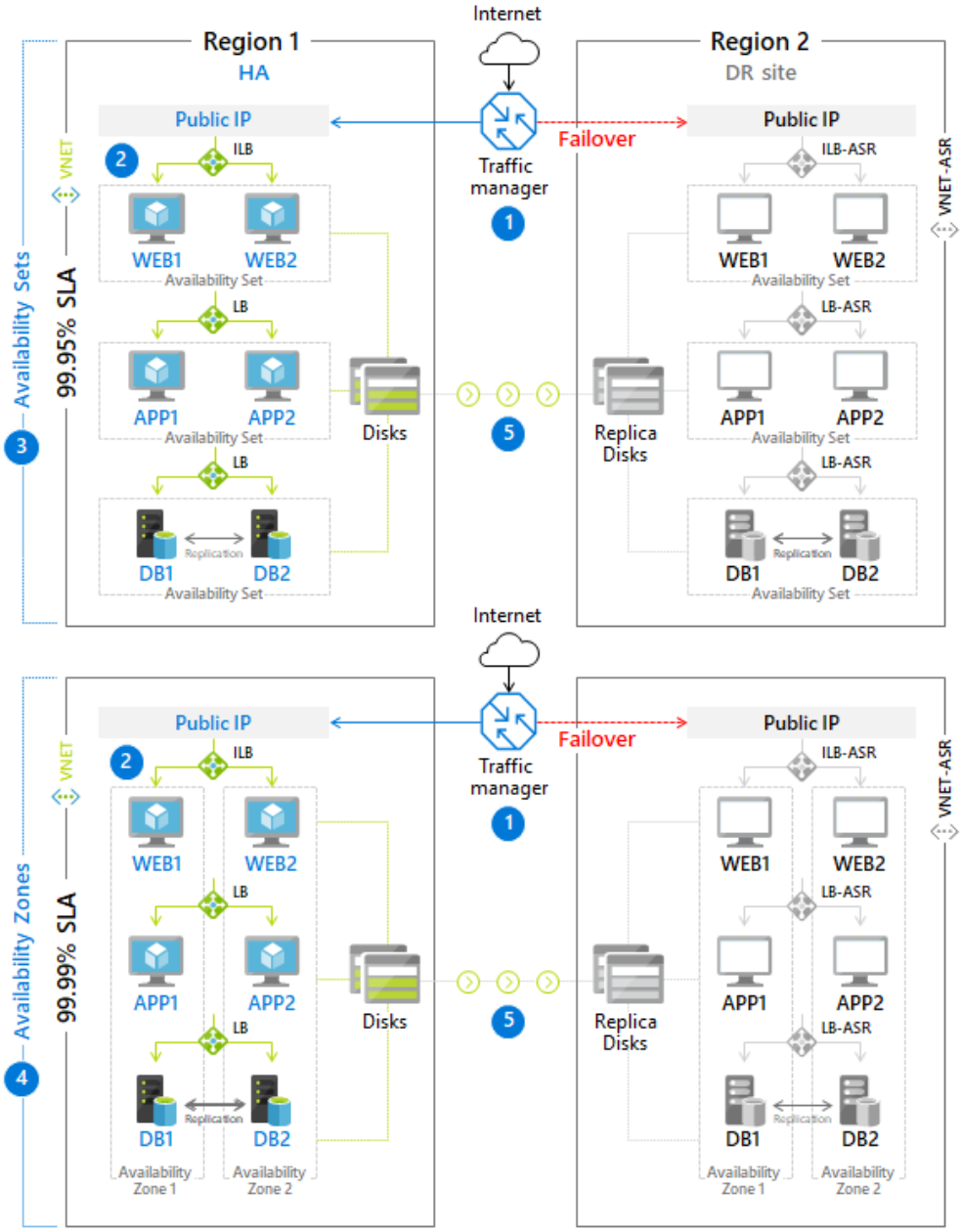
Relevant use cases

Other relevant use cases include:

- Deploying highly resilient applications such as SAP and SharePoint
- Designing a business continuity and disaster recovery plan for line-of-business applications
- Configure disaster recovery and perform related drills for compliance purposes

Architecture

This scenario demonstrates a multitier application that uses ASP.NET and Microsoft SQL Server. In Azure regions that support availability zones, you can deploy your virtual machines (VMs) in a source region across availability zones and replicate the VMs to the target region used for disaster recovery. In Azure regions that don't support availability zones, you can deploy your VMs within an availability set and replicate the VMs to the target region.



- Distribute the VMs in each tier across two availability zones in regions that support zones. In other regions, deploy the VMs in each tier within one availability set.
- The database tier can be configured to use Always On availability groups. With this SQL Server configuration, one primary database within a cluster is configured with up to eight secondary databases. If an issue occurs with the primary database, the cluster fails over to one of the secondary databases, allowing the application to remain available. For more information, see Overview of Always On availability groups for SQL Server.
- For disaster recovery scenarios, you can configure SQL Always On asynchronous native replication to the target region used for disaster recovery. You can also configure Azure Site Recovery replication to the target region if the data change rate is within supported limits of Azure Site Recovery.
- Users access the front-end ASP.NET web tier via the traffic manager endpoint.
- The traffic manager redirects traffic to the primary public IP endpoint in the primary source region.
- The public IP redirects the call to one of the web tier VM instances through a public load balancer. All web tier VM instances are in one subnet.
- From the web tier VM, each call is routed to one of the VM instances in the business tier through an internal load balancer for processing. All business tier VMs are in a separate subnet.
- The operation is processed in the business tier and the ASP.NET application connects to Microsoft SQL Server cluster in a back-end tier via an Azure internal load balancer. These back-end SQL Server instances are in a separate subnet.
- The traffic manager's secondary endpoint is configured as the public IP in the target region used for disaster recovery.

- In the event of a primary region disruption, you invoke Azure Site Recovery failover and the application becomes active in the target region.
- The traffic manager endpoint automatically redirects the client traffic to the public IP in the target region.

Components

- Availability sets ensure that the VMs you deploy on Azure are distributed across multiple isolated hardware nodes in a cluster. If a hardware or software failure occurs within Azure, only a subset of your VMs are affected and your entire solution remains available and operational.
- Availability zones protect your applications and data from datacenter failures. Availability zones are separate physical locations within an Azure region. Each zone consists of one or more datacenters equipped with independent power, cooling, and networking.
- Azure Site Recovery allows you to replicate VMs to another Azure region for business continuity and disaster recovery needs. You can conduct periodic disaster recovery drills to ensure you meet the compliance needs. The VM will be replicated with the specified settings to the selected region so that you can recover your applications in the event of outages in the source region.
- Azure Traffic Manager is a DNS-based traffic load balancer that distributes traffic optimally to services across global Azure regions while providing high availability and responsiveness.
- Azure Load Balancer distributes inbound traffic according to defined rules and health probes. A load balancer provides low latency and high throughput, scaling up to millions of flows for all TCP and UDP applications. A public load balancer is used in this scenario to distribute incoming client traffic to the web tier. An internal load balancer is used in this scenario to distribute traffic from the business tier to the back-end SQL Server cluster.

Alternatives

- Windows can be replaced by other operating systems because nothing in the infrastructure is dependent on the operating system.
- SQL Server for Linux can replace the back-end data store.
- The database can be replaced by any standard database application available.

Other considerations

Scalability

You can add or remove VMs in each tier based on your scaling requirements. Because this scenario uses load balancers, you can add more VMs to a tier without affecting application uptime.

For other scalability topics, see the scalability checklist in the Azure Architecture Center.

Security

All the virtual network traffic into the front-end application tier is protected by network security groups. Rules limit the flow of traffic so that only the front-end application tier VM instances can access the back-end database tier. No outbound internet traffic is allowed from the business tier or database tier. To reduce the attack footprint, no direct remote management ports are open. For more information, see Azure network security groups.

For general guidance on designing secure scenarios, see the Azure Security Documentation.

Pricing

Configuring disaster recovery for Azure VMs using Azure Site Recovery will incur the following charges on an ongoing basis.

- Azure Site Recovery licensing cost per VM.
- Network egress costs to replicate data changes from the source VM disks to another Azure region. Azure Site Recovery uses built-in compression to reduce the data transfer requirements by approximately 50%.
- Storage costs on the recovery site. This is typically the same as the source region storage plus any additional storage needed to maintain the recovery points as snapshots for recovery.

We have provided a sample cost calculator for configuring disaster recovery for a three-tier application using six virtual machines. All of the services are pre-configured in the cost calculator. To see how the pricing would change for your particular use case, change the appropriate variables to estimate the cost.