

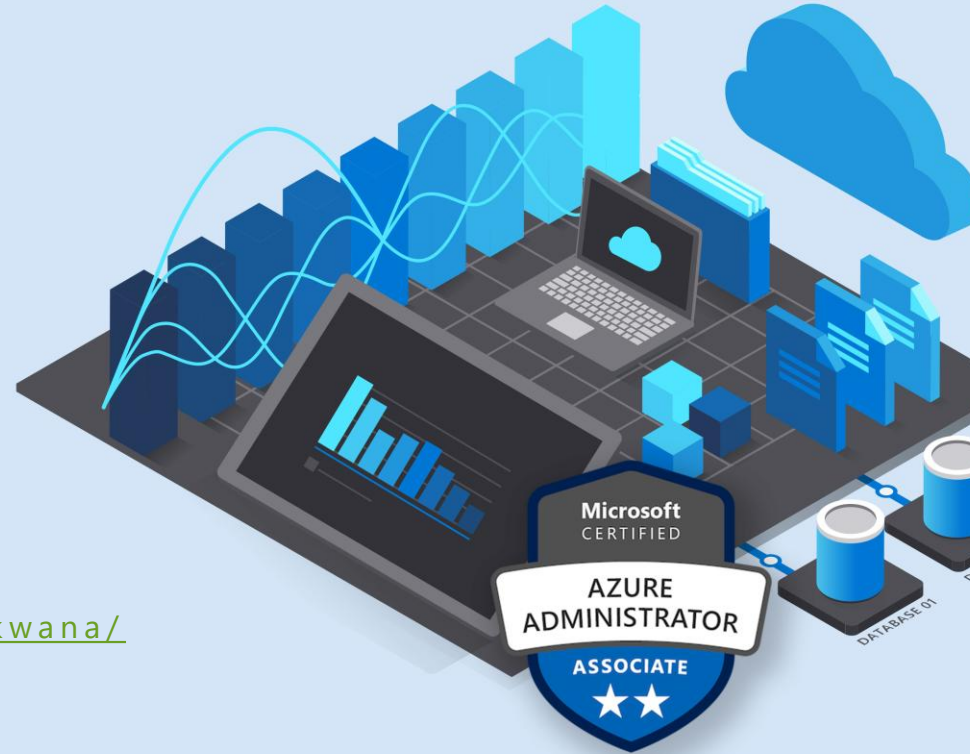
Microsoft Azure Administrator

Maruti Makwana

MCT Corporate Trainer

<https://www.linkedin.com/in/marutimakwana/>

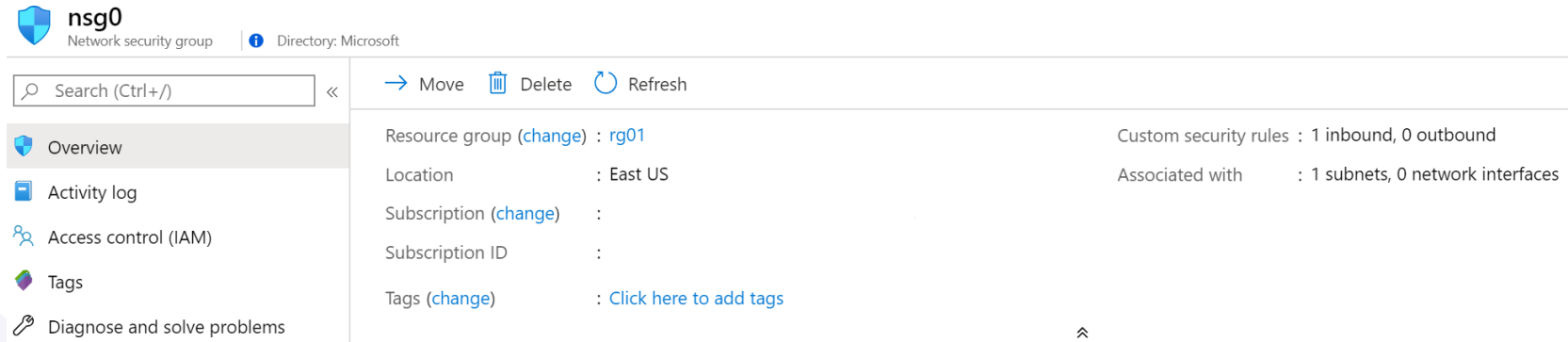
11th June 2025



Configure Network Security Groups (NSGs)



Implement Network Security Groups



The screenshot displays the Azure portal interface for a Network Security Group (nsg0). The left sidebar contains navigation links: Overview (selected), Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area shows the following details:

- Resource group (change): rg01
- Location: East US
- Subscription (change):
- Subscription ID:
- Tags (change): [Click here to add tags](#)

Summary statistics are displayed on the right:

- Custom security rules: 1 inbound, 0 outbound
- Associated with: 1 subnets, 0 network interfaces

Limits network traffic to resources in a virtual network

Lists the security rules that allow or deny inbound or outbound network traffic

Associated to a subnet or a network interface

Can be associated multiple times

Determine NSG Rules

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	 RDP_Inbound	3389	Any	Any	Any	 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow
65500	DenyAllInBound	Any	Any	Any	Any	 Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

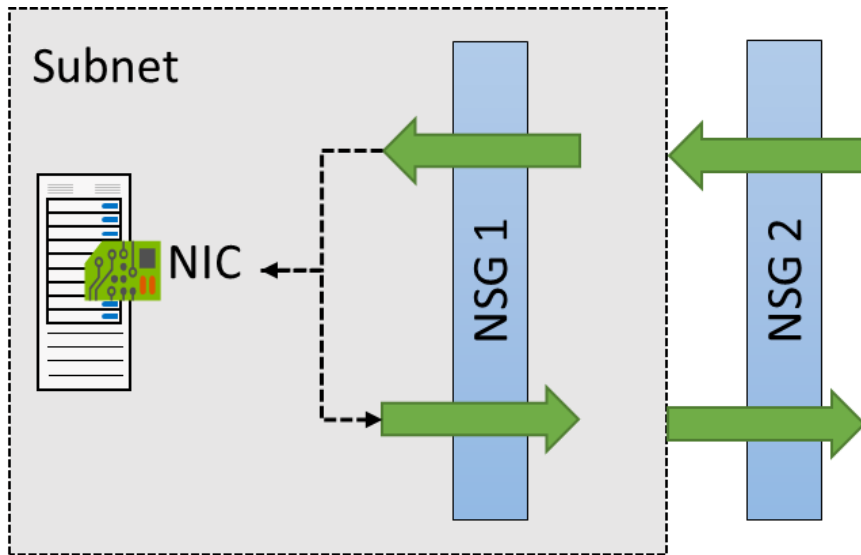
There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

Determine NSG Effective Rules

NSGs are evaluated independently for the subnet and NIC

An “allow” rule must exist at both levels for traffic to be admitted

Use the Effective Rules link if you are not sure which security rules are being applied



 **Network Interface:** [vm01990](#)

[Effective security rules](#)

[Topology](#)

Virtual network/subnet: [vnet01/subnet0](#)

NIC Public IP: -

NIC Private IP: **10.1.0.4**

Accelerated networking: **Disabled**

Create NSG rules

Source (Any, IP addresses, My IP address, service tags, and application security group)

Destination (Any, IP addresses, service tag, and application security group)

Service (HTTPS, SSH, RDP, DNS, POP3, custom, ...)

Priority – The lower the number, the higher the priority



Add inbound security rule

nsgtest

Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

8080

Protocol

☒ Any ☐ UDP
☐ TCP ☐ ICMPv4

Action

☒ Allow ☐ Deny

Priority * ⓘ

100

Name *

AllowAnyCustom8080Inbound

Introduction to Azure Load Balancer

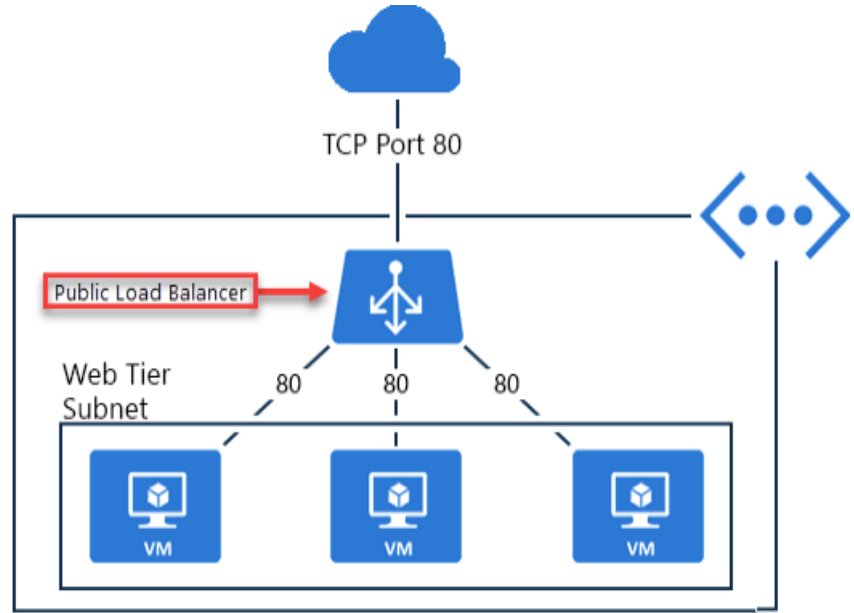


Choose a Load Balancer Solution

Feature	Application Gateway	Front Door	Load Balancer	Traffic Manager
Usage	Optimize delivery from application server farms while increasing application security with web application firewall.	Scalable, security-enhanced delivery point for global, micro service-based web applications.	Balance inbound and outbound connections and requests to your applications or server endpoints.	Distribute traffic to services across global Azure regions, while providing high availability and responsiveness.
Protocols	HTTP, HTTPS, HTTP2	HTTP, HTTPS, HTTP2	TCP, UDP	Any
Private (regional)	Yes		Yes	
Global		Yes		Yes
Env	Azure, non-Azure cloud, on premises	Azure, non-Azure cloud, on premises	Azure	Azure, non-Azure cloud, on premises
Security	WAF	WAF, NSG	NSG	

Implement a Public Load Balancer

- Maps public IP addresses and port number of incoming traffic to the VM's private IP address and port number, and vice versa
- Apply load balancing rules to distribute traffic across VMs or services

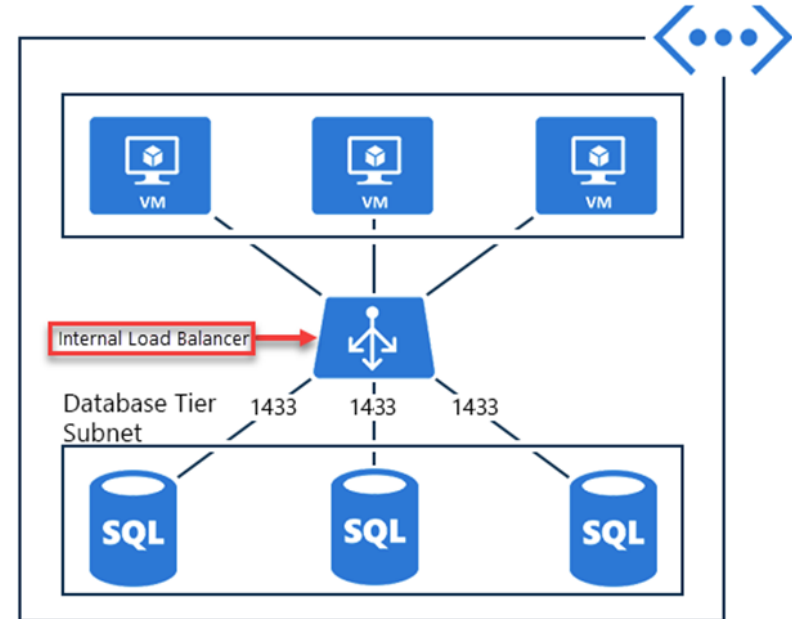


Implement an Internal Load Balancer

Directs traffic only to resources inside a virtual network or that use a VPN to access Azure infrastructure

Frontend IP addresses and virtual networks are never directly exposed to an internet endpoint

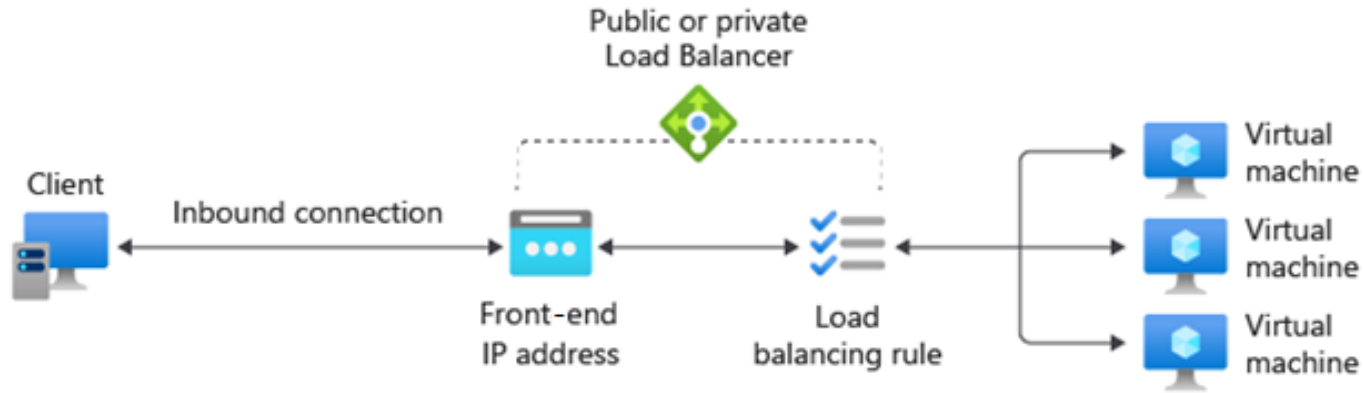
Enables load balancing within a virtual network, for cross-premises virtual networks, for multi-tier applications, and for line-of-business applications



Determine Load Balancer SKUs

Feature	Basic SKU	Standard SKU
Backend pool size	300 IP configurations, single availability set	Up to 5000 instances
Health probes	TCP, HTTP	TCP, HTTP, HTTPS
Availability zones	Not available	Zone-redundant and zonal frontends for inbound and outbound traffic
Multiple frontends	Inbound only	Inbound and outbound
Secure by default	By default, open to the internet	Closed to inbound connections unless opened by NSGs
SLA	Not available	99.99%

Create load balancer rules



Maps a frontend IP and port combination to a set of backend pool and port combination

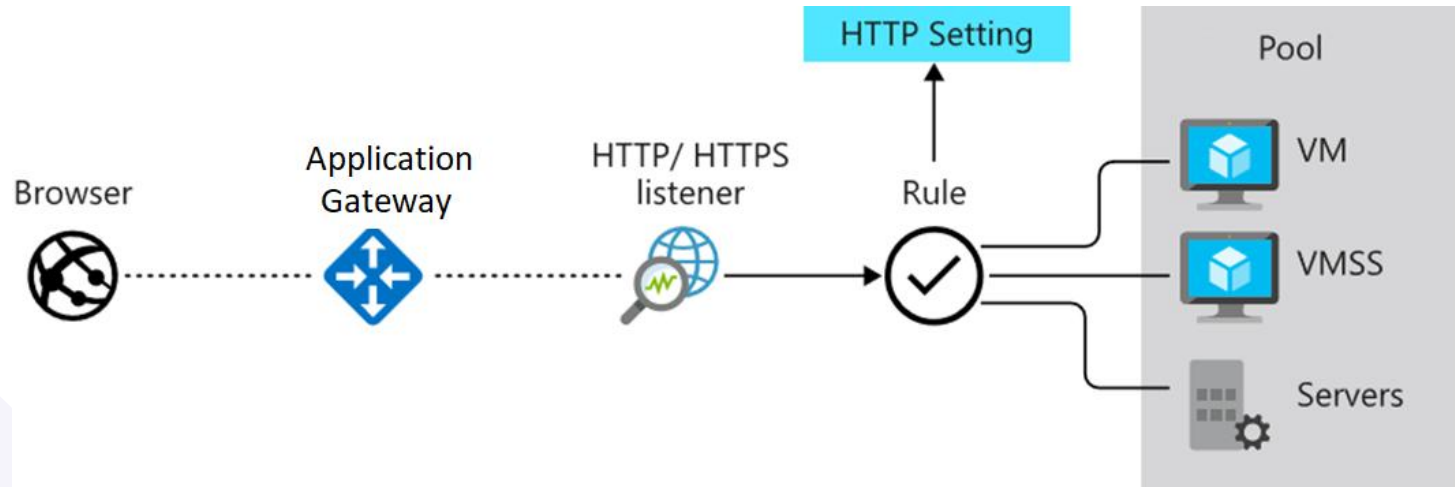
Rules can be combined with NAT rules

A NAT rule is explicitly attached to a VM (or network interface) to complete the path to the target

Introduction to Azure Application Gateway



Implement Application Gateway



Manages web app requests

Routes traffic to a pool of web servers based on the URL of a request

The web servers can be Azure virtual machines, Azure virtual machine scale sets, Azure App Service, and even on-premises servers

Host your domain on Azure DNS



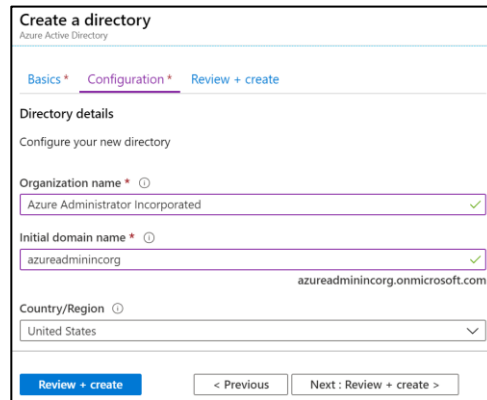
What is Azure DNS?

When you create a new tenant, a new default domain is created

The domain has initial domain name in the form *domainname.onmicrosoft.com*

You can add a custom domain name

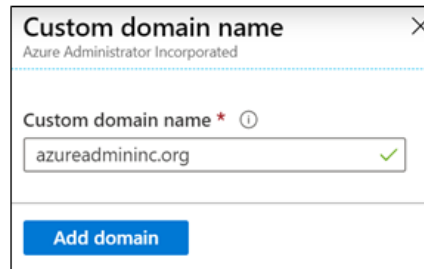
After the custom name is added it must be verified – this demonstrates ownership of the domain



The screenshot shows the 'Create a directory' form in the Azure Active Directory portal. The 'Configuration' tab is selected. The form includes the following fields:

- Organization name ***: Azure Administrator Incorporated (with a green checkmark)
- Initial domain name ***: azureadminincorg (with a green checkmark). The default domain `azureadminincorg.onmicrosoft.com` is displayed below the input.
- Country/Region**: United States (selected from a dropdown menu).

Navigation buttons at the bottom include 'Review + create' (highlighted in blue), '< Previous', and 'Next : Review + create >'.



The screenshot shows the 'Custom domain name' form in the Azure Active Directory portal. The form includes the following fields:

- Custom domain name ***: azureadmininc.org (with a green checkmark).

An 'Add domain' button is located at the bottom of the form.

Configure Azure DNS to host your domain

A DNS zone hosts the DNS records for a domain

Where multiple zones share the same name, each instance is assigned different name server addresses

Root/Parent domain is registered at the registrar and pointed to Azure NS

Create DNS zone



Basics

Tags

Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more.](#)

Project details

Subscription *

MSDN Platforms Subscription

Resource group *

rg-dns

[Create new](#)

Instance details

Name *

azureadmininc.org



Resource group location ⓘ

East US

Review + create


Previous

Next : Tags >

[Download a template for automation](#)

Verify delegation of domain name services

- When delegating a domain to Azure DNS, you must use the name server names provided by Azure DNS – use all four
- Once the DNS zone is created, update the parent registrar
- For child zones, register the NS records in the parent domain

 **azureadmininc.org**
DNS zone

[+ Record set](#) [→ Move](#) [🗑 Delete zone](#) [🔄 Refresh](#)

Resource group ([change](#))
[rg-dns](#)

Subscription ([change](#))
[MSDN Platforms Subscription](#)

Subscription ID

Name server 1
ns1-02.azure-dns.com.

Name server 2
ns2-02.azure-dns.net.

Name server 3
ns3-02.azure-dns.org.

Name server 4
ns4-02.azure-dns.info.

Tags ([change](#))
[Click here to add tags](#)

Dynamically resolve resource name by using alias record

A record set is a collection of records in a zone that have the same name and are the same type

You can add up to 20 records to any record set

A record set cannot contain two identical records

Changing the drop-down Type, changes the information required

×

Add record set

azureadmininc.org

Name

helloworld

✓

.azureadmininc.org

Type

A

▼

Alias record set ⓘ

☐ Yes ☒ No

TTL *

1

TTL unit

Hours

▼

IP address

0.0.0.0

...

Configure a private DNS zone

Use your own custom domain names

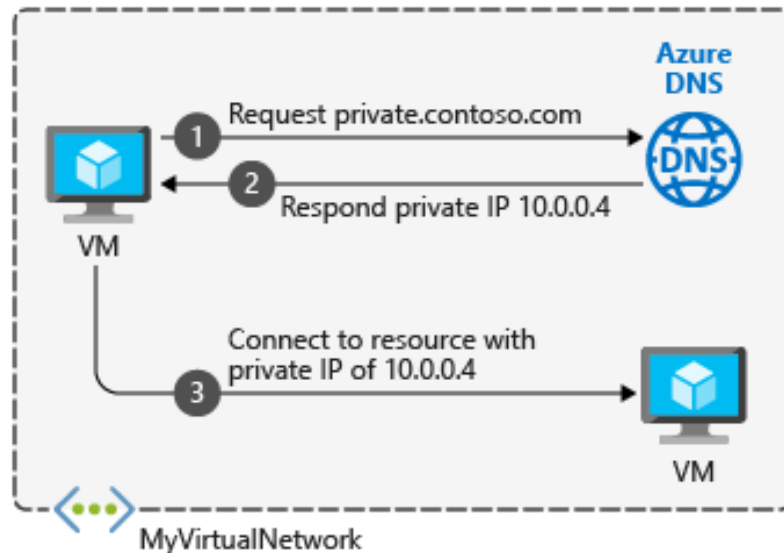
Provides name resolution for VMs within a VNet and between VNets

Automatic hostname record management

Removes the need for custom DNS solutions

Use all common DNS records types

Available in all Azure regions



Configure Storage Accounts



Explore Azure Storage Services

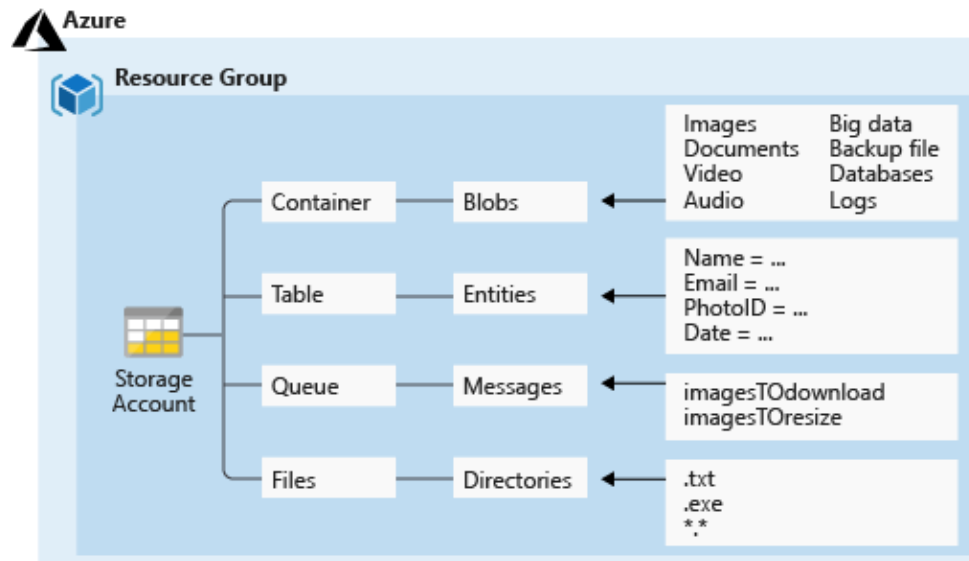
A service that you can use to store files, messages, tables, and other types of information

Azure Containers: A massively scalable object store for text and binary data

Azure Tables: Ideal for storing structured, non-relational data

Azure Queues: A messaging store for reliable messaging between application components

Azure Files: Managed file shares for cloud or on-premises deployments



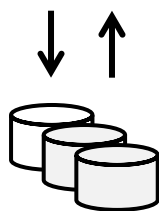
Determine Storage Account Kinds

All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest

Storage Account	Recommended usage
Standard general-purpose v2	Most scenarios including Blob, File, Queue, Table, and Data Lake Storage.
Premium block blobs	Block blob scenarios with high transactions rates, or scenarios that use smaller objects or require consistently low storage latency.
Premium file shares	Enterprise or high-performance file share applications.
Premium page blobs	Premium high-performance page blob scenarios.

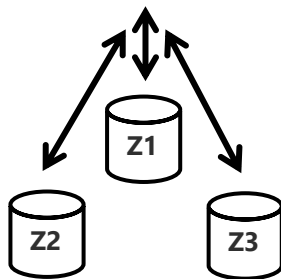
Determine Replication Strategies (1 of 2)

Single region



LRS

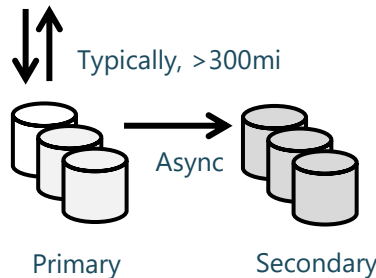
- Three replicas, one region
- Protects against disk, node, rack failures
- Write is acknowledged when all replicas are committed
- Superior to dual-parity RAID



ZRS

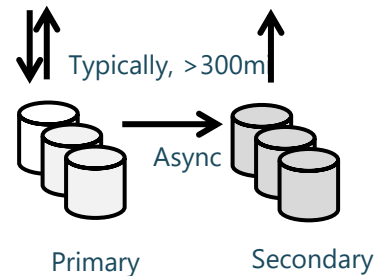
- Three replicas, three zones, one region
- Protects against disk, node, rack, and zone failures
- Synchronous writes to all three zones

Multiple regions



GRS

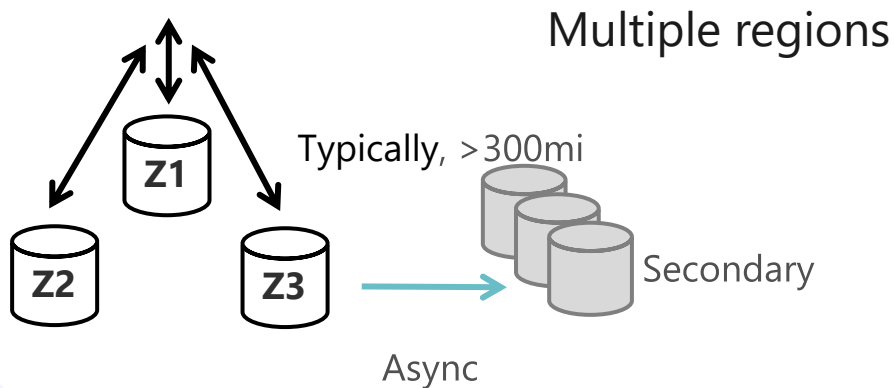
- Six replicas, two regions (three per region)
- Protects against major regional disasters
- Asynchronous copy to secondary



RA-GRS

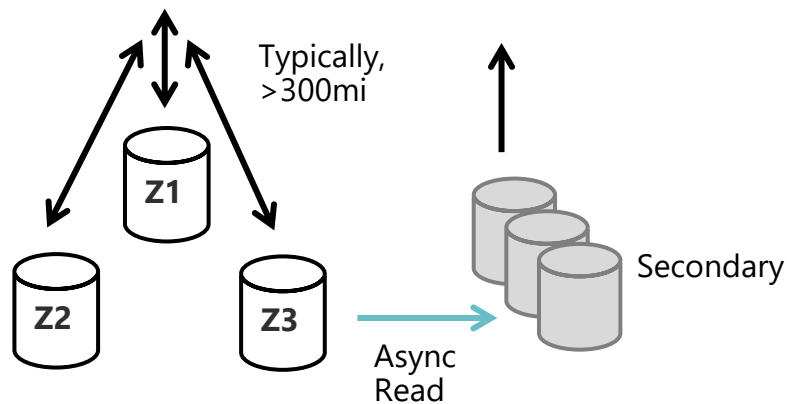
- GRS + read access to secondary
- Separate secondary endpoint
- Recovery point objective (RPO) delay to secondary can be queried

Determine Replication Strategies (2 of 2)



GZRS

- Six replicas, 3+1 zones, two regions
- Protects against disk, node, rack, zone, and region failures
- Synchronous writes to all three zones and asynchronous copy to secondary



RA-GZRS

- GZRS + read access to secondary
- Separate secondary endpoint
- RPO delay to secondary can be queried

Access Storage

Every object has a unique URL address – based on account name and storage type

Container service: `https://mystorageaccount.blob.core.windows.net`

Table service: `https://mystorageaccount.table.core.windows.net`

Queue service: `https://mystorageaccount.queue.core.windows.net`

File service: `https://mystorageaccount.file.core.windows.net`

- If you prefer you can configure a custom domain name

CNAME record	Target
blobs.contoso.com	contosoblobs.blob.core.windows.net

Secure Storage Endpoints

Firewalls and Virtual Networks restrict access to the Storage Account from specific Subnets on Virtual Networks or public IP's

Subnets and Virtual Networks must exist in the same Azure Region or Region Pair as the Storage Account

Firewalls and virtual networks

Custom domain



Save



Discard



Refresh

Public network access



Enabled from all networks



Enabled from selected virtual networks and IP addresses



Disabled



All networks, including the internet, can access this storage account. [Learn more](#)

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference ⓘ



Microsoft network routing



Internet routing



The current combination of storage account kind, performance, replication, and location does not support network routing.

Configure Blob Storage



Implement Blob Storage

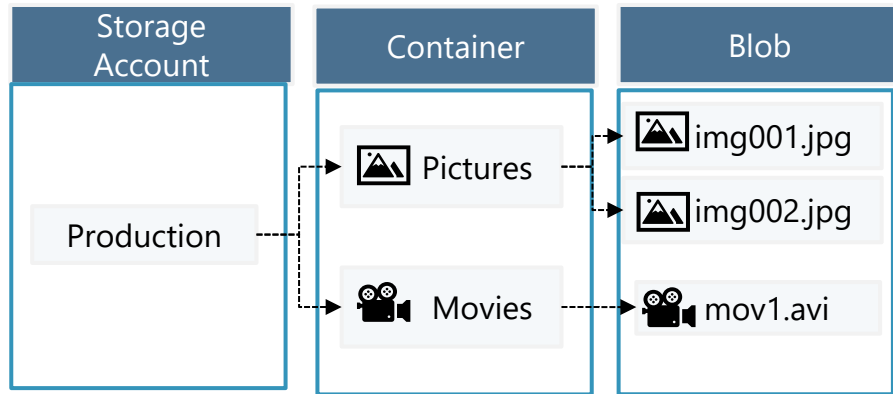
Stores unstructured data in the cloud

Can store any type of text or binary data

Also referred to as *object storage*

Common uses:

- Serving images or documents directly to a browser
- Storing files for distributed access
- Streaming video and audio
- Storing data for backup and restore, disaster recovery, archiving
- Storing data for analysis by an on-premises or Azure-hosted service



Create Blob Containers

All blobs must be in a container

Accounts have unlimited containers

Containers can have unlimited blobs

Restrict access using the public access level

 Container  Change access level  Refresh |  Delete

New container

Name *

container01

Public access level ⓘ

Private (no anonymous access)

Private (no anonymous access)

Blob (anonymous read access for blobs only)

Container (anonymous read access for containers and blobs)

OK

Cancel

Create Blob Access Tiers

Hot tier – Data that is accessed or modified frequently

Cool tier – Data that is infrequently accessed or modified and stored for at least 30 days

Cold tier – Data that is infrequently accessed or modified and stored for at least 90 days

Archive – Data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days

Change tier



infoicon.jpg

Optimize storage costs by placing your data in the appropriate access tier. [Learn more](#)

Access tier

Hot (Inferred)

Hot (Inferred)

Cool

Cold

Archive

Add Blob Lifecycle Management Rules

Transitioning of blobs to a cooler storage tier to optimize for performance and cost

Delete blobs at the end of their lifecycle

Apply rules to filtered paths in the Storage Account

Add a rule ...

✓ Details 2 Base blobs 3 Filter set

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If

Base blobs were *

☒ Last modified

☐ Created

More than (days ago) *

Enter a value

Then

Delete the blob

Move to cool storage

For infrequently accessed data that you want to keep on cool storage for at least 30 days.

Move to cold storage

For rarely accessed data that you want to keep for at least 90 days.

Move to archive storage

Use if you don't need online access and want to keep the object for 180 days or longer.

Delete the blob

Deletes the object per the specified conditions.

Determine Blob Object Replication

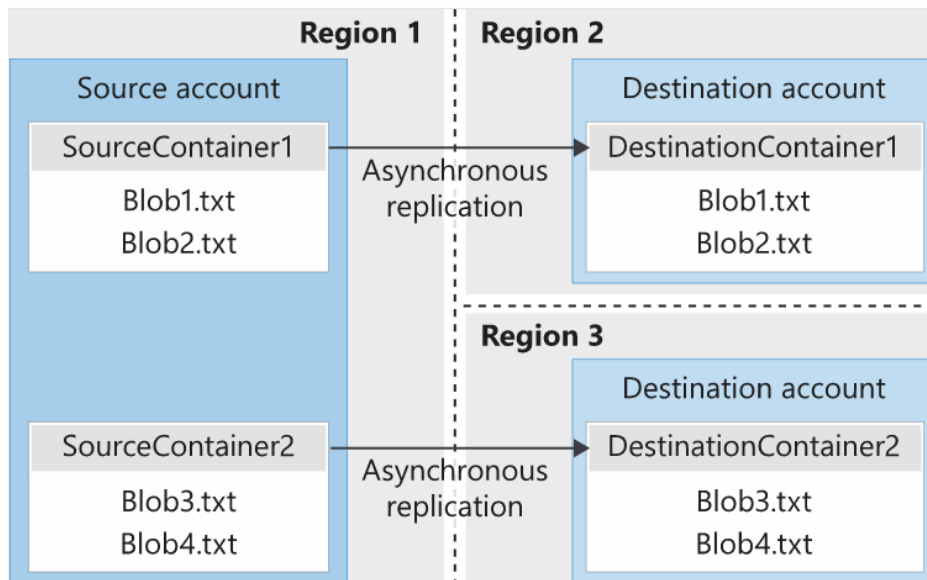
Asynchronous to any other Region

Minimizes latency for read requests

Increases efficiency for compute workloads

Optimizes data distribution

Optimizes costs



Configure Storage Security



Review Storage Security Strategies



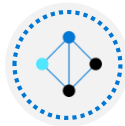
Storage Service Encryption



Shared Access Signatures – delegated access



Authentication with Entra ID and RBAC



Shared Key – encrypted signature string



Client-side encryption, HTTPS, and SMB 3.0 for data in transit



Anonymous access to containers and blobs



Azure disk encryption

Create Shared Access Signatures

Provides delegated access to resources

Grants access to clients without sharing your storage account keys

The account SAS delegates access to resources in one or more of the storage services

The service SAS delegates access to a resource in just one of the storage services

Signing method ⓘ

☒ Account key ☐ User delegation key

Signing key ⓘ

Key 1 ▼

Permissions * ⓘ

Read ▼

Start and expiry date/time ⓘ

Start

02/01/2021 

(UTC-08:00) Coordinated Universal Time-08 ▼

Expiry

02/02/2021 

(UTC-08:00) Coordinated Universal Time-08 ▼

Allowed IP addresses ⓘ

for example, 168.1.5.65 or 168.1.5.65-168.1....

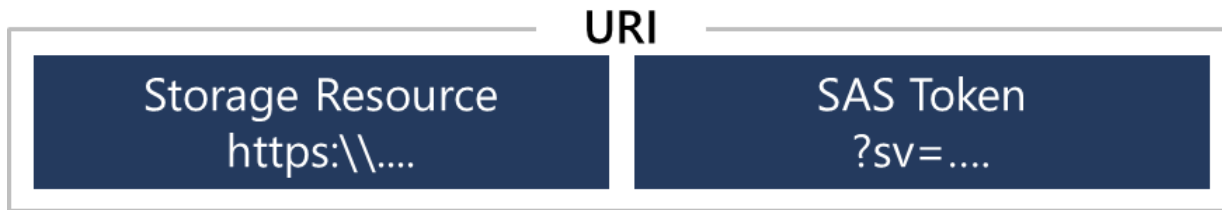
Allowed protocols ⓘ

☒ HTTPS ☐ HTTP

[Generate SAS token and URL](#)

Identify URI and SAS Parameters

- A SAS is a signed URI that points to one or more storage resources
- Consists of a storage resource URI and the SAS token



`https://myaccount.blob.core.windows.net/?sp=r&st=2020-05-11T18:31:43Z&se=2020-05-12T02:31:43Z&spr=https&sv=2019-10-10&sr=b&sig=j0qABJZHfUVEBQ3yVn7kWICKl00sxCiK1rzEchfAz8U%3D`

Includes parameters for resource URI, storage services version, services, resource types, start time, expiry time, resource, permissions, IP range, protocol, signature

Determine Storage Service Encryption

You can use your own key (next topic)

Protects your data for security and compliance

Automatically encrypts and decrypts your data

Encrypted through 256-bit AES encryption

Is enabled for all new and existing storage accounts and cannot be disabled

Is transparent to users

Encryption

 Save  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data in the storage account is encrypted using Microsoft Managed Keys. You may choose to bring your own key.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn More about Azure Storage Encryption](#) 

Encryption type

- ☒ Microsoft Managed Keys
- ☐ Customer Managed Keys

Create Customer Managed Keys

Use the Azure Key Vault to manage your encryption keys


Create your own encryption keys and store them in a key vault

Use Azure Key Vault's APIs to generate encryption keys

Custom keys give you more flexibility and control

Encryption type

- ☐ Microsoft Managed Keys
- ☒ Customer Managed Keys

i The storage account named 'storage987123' will be granted access to the selected key vault. Both soft delete and purge protection will be enabled on the key vault and cannot be disabled. [Learn more about customer managed keys](#) 

Encryption key

- ☐ Enter key URI
- ☒ Select from Key vault

Key vault and key *

Key vault: keyvault987123

Key: storagekey

[Select a key vault and key](#)