



Azure Storage Account:

tutto quello che avresti voluto sapere, ma non hai mai chiesto !!



Massimo Bonanni

Senior Technical Trainer @ Microsoft





What is an Azure Storage Account?

Core Concept

A Storage Account is the **top-level namespace** in Azure for all storage services.

It provides a unique namespace accessible via HTTP/HTTPS from anywhere in the world.

Every object stored in Azure has an address including the unique account name.

Unique Namespace

Account name forms the base URL:
`accountname.blob.core.windows.net`

Subscription Scoped

Created within an Azure subscription and Resource Group for billing & management

Account Types

Standard (GPv2),
Premium Block Blob,
Premium File Shares,
Premium Page Blobs

Region Bound

Created in a specific Azure region; data stays local unless replication is configured



Performance Tiers



Standard

General Purpose v2

HDD / Magnetic

- Backed by magnetic disk drives (HDD)
- Supports all 4 storage services: Blob, File, Queue, Table
- Lower cost per GB — ideal for bulk/warm data
- Redundancy: LRS, GRS, ZRS, GZRS
- Max throughput: ~60 Gbps per account
- Best for: backups, archives, general workloads

VS



Premium

High Performance

NVMe / SSD

- Backed by solid-state drives (NVMe SSD)
- Three sub-types: Block Blob, File Shares, Page Blobs
- Consistent low-latency (single-digit milliseconds)
- Redundancy: LRS or ZRS only
- Max throughput: up to 200 Gbps per account
- Best for: databases, interactive apps, AI/ML workloads

The 4 Core Storage Services



Blob Storage

Object storage for unstructured data: text, binary, images, videos, backups.

USE CASES

- Log files & backups
- Streaming media
- Static web content
- Data lakes (ADLS Gen2)



Azure Files

Fully managed file shares via SMB 3.0 and NFS 4.1 protocols.

USE CASES

- Lift & shift applications
- Dev/Test shared storage
- Containerized workloads
- Replace on-prem file servers



Queue Storage

Reliable messaging for async communication between app components.

USE CASES

- Decoupled microservices
- Task queuing & scheduling
- Event-driven workflows
- Up to 64 KB per message



Table Storage

NoSQL key-value store for semi-structured data at massive scale.

USE CASES

- Structured non-relational data
- IoT telemetry data
- User and session data
- Cost-effective vs Cosmos DB



Availability & Built-in Replication



LRS

3 copies

Locally Redundant Storage

Single datacenter

3 synchronous copies within one datacenter. Protects against hardware failures. Lowest cost option.

ZRS

3 copies

Zone Redundant Storage

3 Availability Zones

3 synchronous copies across 3 AZs in same region. Protects against datacenter outages.

GRS

6 copies

Geo Redundant Storage

LRS + 2nd region

LRS + async replication to secondary region. RA-GRS option enables read access to secondary.

GZRS

6 copies

Geo-Zone Redundant Storage

ZRS + 2nd region

ZRS in primary + async replication to secondary region. Highest durability and availability.

RA- prefix (RA-GRS, RA-GZRS) enables read access to the secondary region at all times, not just during failover and increase the availability.

Encryption



At Rest (SSE)

AES-256 bit • Always enabled

Storage Service Encryption (SSE) automatically encrypts all data before persisting using AES-256. Enabled by default and cannot be disabled.



In Transit

TLS 1.2+ • HTTPS enforced

HTTPS is enforced by default (Secure Transfer Required). TLS 1.2 minimum is recommended. HTTP access can be blocked at account level.



Key Management

Microsoft keys or CMK via Key Vault

Choose Microsoft-managed keys (default) or Customer-managed keys (CMK) stored in Azure Key Vault for full control of the encryption lifecycle.



Infrastructure Encryption

Double encryption • Compliance use

Optional second encryption layer at the infrastructure level. Data is encrypted twice with two different algorithms for highest regulatory compliance.





Access to Storage



Connection String

Combines account name and master key into a single string for easy SDK usage.

✓ ADVANTAGES

- Simple for dev/test scenarios
- Widely supported by all SDKs

⚠ CONSIDERATIONS

- Exposes master account key
- No granular permissions
- Rotate keys carefully



RBAC (Entra ID)

Assign roles (Storage Blob Data Reader, Contributor etc.) to identities via Azure Active Directory.

✓ ADVANTAGES

- Identity-based, no shared secrets
- Principle of least privilege
- Full audit logs via Entra ID
- Fine-grained permissions

⚠ CONSIDERATIONS

- Requires AAD configuration
- Permission propagation ~5 min



Shared Access Signature (SAS)

Signed URI granting limited, time-bound access to specific resources without exposing the master key.

✓ ADVANTAGES

- Fine-grained permissions
- Time-limited expiry
- No master key exposure

⚠ CONSIDERATIONS

- Hard to revoke (use Stored Access Policy)
- Token lifecycle management needed

Data Protection

Soft Delete for Blobs

Retains deleted blobs for a configurable period (1–365 days). Marked as deleted but restorable. Protects against accidental deletions and overwrites.

Soft Delete for Containers

Same as blob soft delete but at container level. Entire containers and all their contents can be recovered within the retention window.

Blob Versioning

Automatically saves previous versions on every write. Each version has a unique ID. Restore, list, or delete specific versions independently.

Point-in-Time Restore

Restore block blobs to a previous state within a retention period. Works at container level. Requires soft delete + versioning + change feed enabled.

Immutability Policies (WORM)

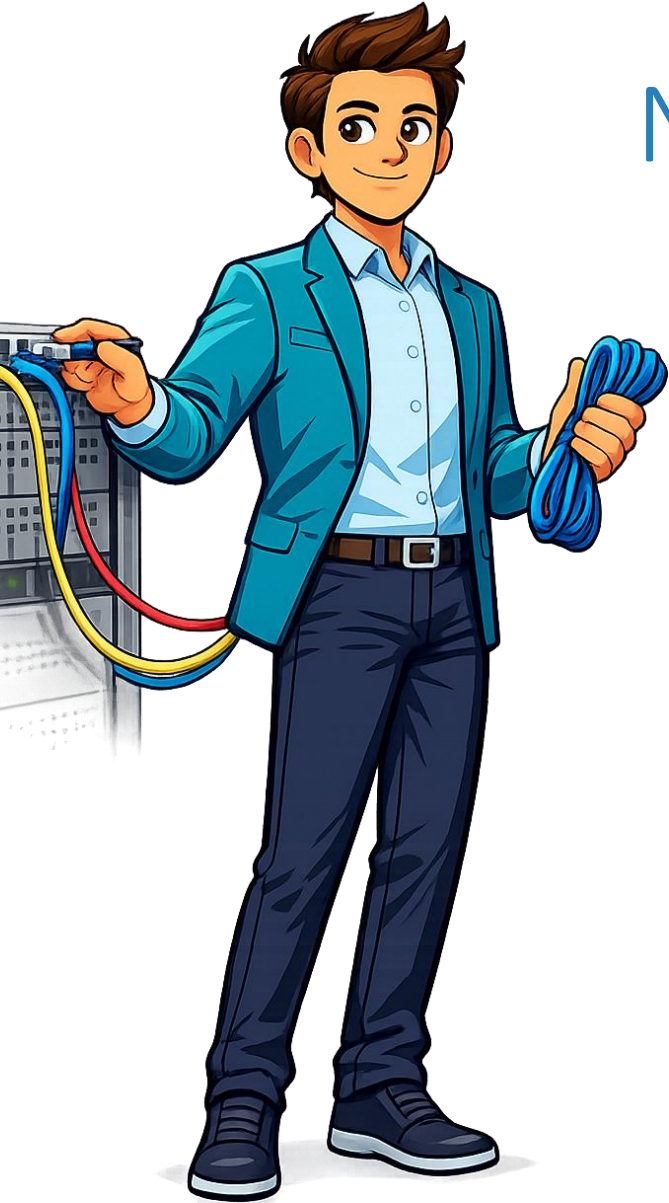
Write Once, Read Many policy. Prevents blobs from being modified or deleted. Supports time-based retention and legal holds for regulatory compliance.

Azure Backup for Blobs

Operational backup via Azure Backup Center. Continuous backup with point-in-time recovery. Supports central management and policy-based scheduling.



Networking & Access Control



Public Endpoint

- ✓ **Accessible from the internet**
Default endpoint for all storage accounts
- ✓ **IP Firewall Rules**
Restrict to specific public IPs or IP ranges
- ✓ **Virtual Network Rules**
Allow specific VNets and subnets via Service Endpoint
- ✓ **All networks (default)**
Allows any client with valid credentials to connect
- ✓ **Selected networks**
Restrict to whitelisted IPs and VNets only
- ✓ **Disabled**
Block all public access (Private Endpoint only)

Private Connectivity

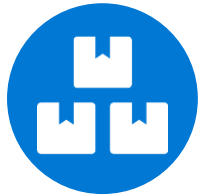
Service Endpoints

- Extends VNet identity to the storage over Azure backbone
- Traffic stays on Microsoft backbone (not public internet)
- Configured at subnet level — no additional cost
- Storage account still has public IP but restricted to VNet

Private Endpoints

- Injects a private NIC into your VNet with a private IP address
- Fully removes public endpoint exposure from internet
- DNS resolves storage account to private IP via Private DNS Zone
- Charged per endpoint and per GB of data processed

Blob Storage — Typologies of Blobs



Block Blob

Most Common

Max Size

~190.7 TiB

Block/Page Size

**Up to 4,000
MiB/block**

- Text and binary files
- Images, video, audio
- Log files and backups
- Data lake workloads (ADLS Gen2)
- Most common blob type



Append Blob

Append-Only

Max Size

~195 GiB

Block/Page Size

**Up to 4
MiB/block**

- Application log files
- Audit trail data streams
- Streaming data ingestion
- IoT diagnostic logs



Page Blob

Random R/W

Max Size

8 TiB

Block/Page Size

512-byte pages

- Azure VM OS and data disks
- VHD/VHDX disk images
- Database files (SQL, Oracle)
- Random access workloads





Blob Storage — Access Tiers

 Hot	 Cool	 Cold	 Archive
Storage: \$\$\$	Storage: \$\$	Storage: \$	Storage: ¢
Access: \$	Access: \$\$	Access: \$\$\$	Access: \$\$\$\$
Latency: Milliseconds	Latency: Milliseconds	Latency: Milliseconds	Latency: Hours (rehydrate)
Min Retain: No minimum	Min Retain: 30 days min	Min Retain: 90 days min	Min Retain: 180 days min
<i>Active data, frequently read content, websites and apps</i>	<i>Short-term backups, disaster recovery, older datasets</i>	<i>Long-term backups, compliance data, rarely accessed archives</i>	<i>Raw data, regulatory archives, long-term cold storage</i>

Storage Cost: High → Low | Access Cost: Low → High | Tiers set at account level (default) or per-blob | Early deletion fees apply

Blob Storage - Metadata & Tag Indexes

Blob Metadata

Key-Value pairs

Up to 8 KB per blob, arbitrary name/value pairs

Not indexed

Cannot be used for filtering or querying blobs

Custom properties

Store application-specific metadata with the blob

Set via API/SDK

Set at upload time or updated independently later

System metadata

Content-Type, ETag, Last-Modified, Content-Length

User-defined

Arbitrary custom key=value pairs (lowercase keys required)

Blob Index Tags

Indexed key-value pairs

Up to 10 tags per blob, fully indexed and queryable

Cross-container search

Filter blobs across entire storage account by tag value

Queryable with OData

Use filter expressions to find blobs matching conditions

Lifecycle management

Use blob tags as conditions in lifecycle policy rules

Billing applies

Charged per tag stored and per query operation executed

Tag Query Example

```
"Project" = 'Finance'  
AND "Status" = 'Processed'  
AND "Year" >= '2024'
```



Blob Storage - Other Notable Features



Lifecycle Management

Automate tier transitions and deletions: move blobs Hot→Cool→Cold→Archive or delete after N days. Filter by prefix, tags, or blob type.



Object Replication

Async replication of block blobs between storage accounts (same or different regions). Useful for geo-distribution and latency reduction.



Blob Inventory

Scheduled reports (daily/weekly) listing all blobs with properties, metadata, and tags. Output as CSV or Parquet. Great for compliance and auditing.



Static Website Hosting

Serve static content directly from Blob Storage via \$web container. Integrate with Azure CDN for global distribution and custom domains.



Azure Data Lake Gen2

Hierarchical namespace on top of Blob Storage. Adds directory semantics, POSIX-compliant ACLs, and optimized analytics performance.



Change Feed

Ordered, durable log of all create, modify, and delete blob events. Used for point-in-time restore and event-driven processing. Stored as Avro files.



Azure CDN Integration

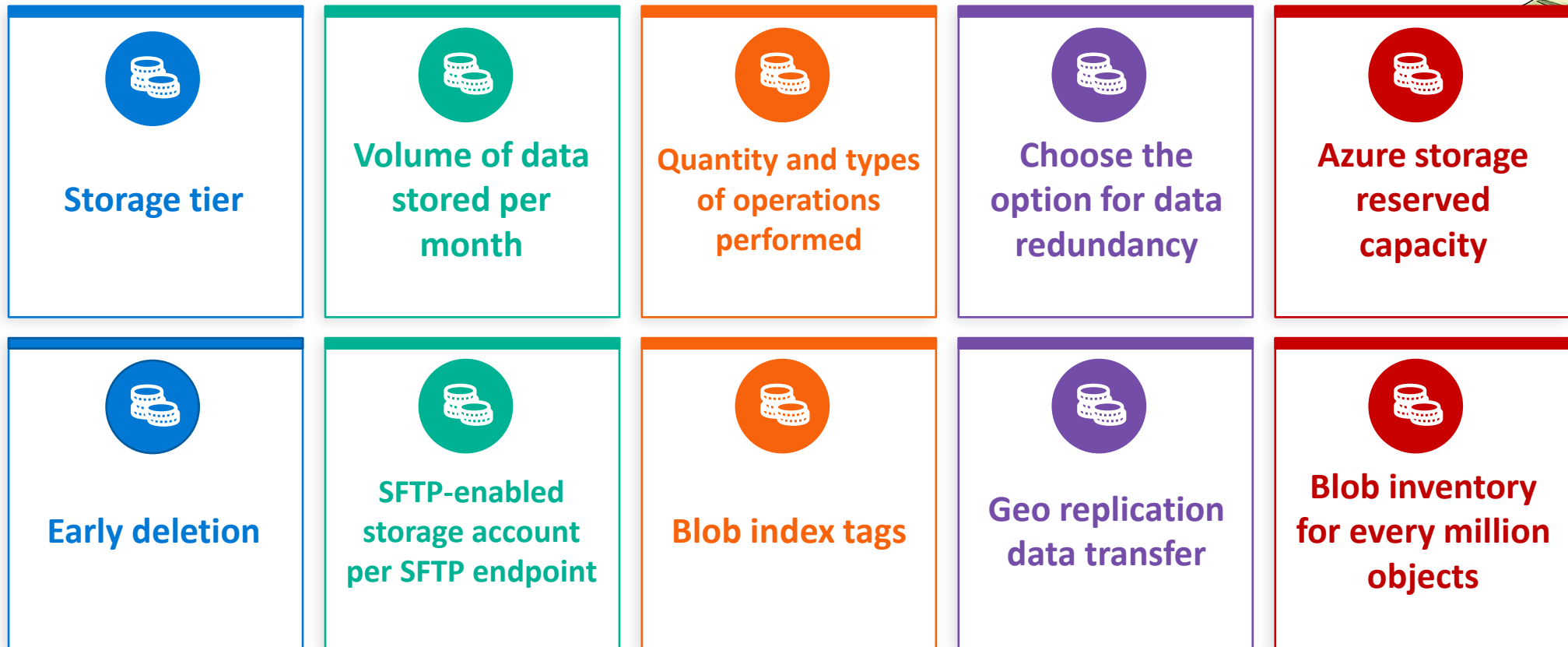
Cache blob content at global edge nodes to reduce latency. Supports custom domains, HTTPS, and cache rules via Microsoft, Verizon, or Akamai CDN.



Immutable Storage (WORM)

Write Once, Read Many compliance. Time-based retention policies and legal holds prevent modification/deletion. For regulatory requirements.

Demystifying Azure Blob Storage Cost



PayslipsManager



DEMO

Payslips Manager Requirements



- Web Application:
 - Each Employee enter with his/her account
 - Can see the list of all his/her payslips
 - Can download a single payslip
- Payslips are PDF files
- We want to optimize management
- We want to optimize costs
- We want to have the best SLA with a single region
- Each employee can see only his/her payslips

Payslips Manager Solution



- Performance Tier: Standard
- Storage Service: Blob Storage
- Replication: ZRS
- Structure: One container for each user (providing access with Entra ID)
- Cost Optimization: Payslips for the last year in Hot, the next five years in Cool, and then Cold. Archive for employees who no longer work for the company.

Any Questions?



Massimo Bonanni

Senior Technical Trainer

massimo.bonanni@microsoft.com

[@massimobonanni](#)



