Microsoft

Azure Storage

Microsoft Services

Agenda

- Storage Overview
- Storage Services
- Storage Replication
- Storage Security

Azure Storage Overview

- Azure Storage is a scalable, durable, and highly available storage solution.

- Uses an auto-partitioning system that automatically load-balances your data based on traffic.

- Is accessible from anywhere in the world, from any type of application, whether it's running in the cloud, on a desktop, on an on-premises server, or on a mobile or tablet device.

- Supports clients using a diverse set of operating systems (including Windows and Linux) and a variety of programming languages i.e. .NET, Java, Node.js, Python, Ruby, PHP and C++.

Storage Services

Microsoft Services

Azure Storage Accounts

Azure storage provides three types of storage accounts, **General Purpose v1, v2** and **Blob**.

General purpose v1 storage accounts give you access to Blobs, Tables, Queues, Files and Azure virtual machine disks under a single account and has two performance tiers, Standard and Premium:

- **Standard** storage performance tier uses HDD disks and allows you to store Blobs, Tables, Queues, Files and Azure virtual machine disks.
- **Premium** storage performance tier uses SSD disks which currently only supports Azure virtual machine disks.

General purpose v2 storage accounts give you all the features of v1 plus Hot and Cool storage tiers

Blob Storage Accounts are specialized storage accounts for storing unstructured data as blobs in Azure Storage, optimised for block or append blob storage, not page blobs.

Microsoft Confidential

Standard Storage Account

5PB limit per storage account	250 storage accounts per region
Up to 20,000 IOPS Per storage account and Up to 500 IOPS per VHD	Encryption at Rest by default

Microsoft Confidential

Premium Storage Account

| Only supports Locally Redundant Storage (LRS) | Must use B-series, DS-series, DSv2-series, DSv3-series, GS-series, Ls-series, M-series, and Fs-series VMs | Cannot be mapped to a custom domain | Storage analytics not currently supported | No support for Block blobs, Append blobs, Azure Files, Azure Tables or Azure Queues only Page Blobs for Virtual Machines (aka VHD's) |

Microsoft Confidential

Azure Premium Storage Scalability

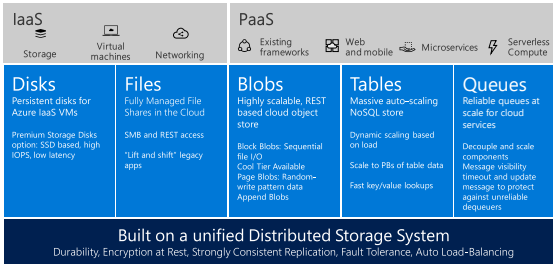| Premium SSD sizes	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	120	240	500	1,100	2,300	5,000	7,500	7,500	16,000	18,000	20,000
Through put per disk	25 MiB/sec	50 MiB/sec	100 MiB/sec	125 MiB/sec	150 MiB/sec	200 MiB/sec	250 MiB/sec	250 MiB/sec	500 MiB/sec	750 MiB/sec	900 MiB/sec

Microsoft Confidential

Azure Storage Services

- An Azure storage account provides the following storage services: Blob storage, Table storage, Queue storage, File storage and Managed Disk storage.

- **Blob Storage** stores **unstructured object data or Blobs** and can be any type of text or binary data, such as a document, media file or VHD.

- **Table Storage** stores structured datasets and is a NoSQL key-attribute data store, which allows for rapid development and fast access to large quantities of data.

- **Queue Storage** provides reliable messaging for workflow processing and for communication between components of cloud services.

- **File Storage** offers shared storage for legacy applications using the standard SMB protocol.

- **Managed Disk Storage** provides persistent VHD disk storage without the overhead of managing a storage account.
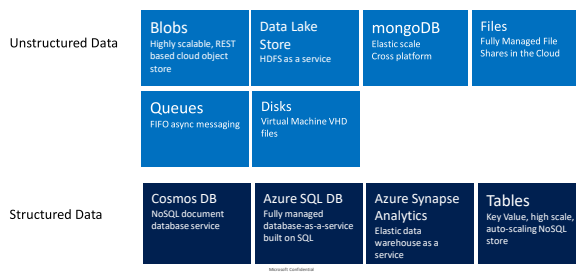
Microsoft Confidential

Azure Storage Services

IaaS

| Storage | Virtual machines | Networking |

PaaS

| Existing frameworks | Web and mobile | Microservices | Serverless Compute |

Disks	Files	Blobs	Tables	Queues
Persistent disks for Azure IaaS VMs	Fully Managed File Shares in the Cloud	Highly scalable, REST based cloud object store	Massive auto-scaling NoSQL store	Reliable queues at scale for cloud services
Premium Storage Disks option: SSD based, high IOPS, low latency	SMB and REST access	Block Blobs: Sequential file I/O	Dynamic scaling based on load	Decouple and scale components
	"Lift and shift" legacy apps	Cool Tier Available	Scale to PBs of table data	Message visibility timeout and update message to protect against unreliable dequeuers
		Page Blobs: Random-write pattern data	Fast key/value lookups	
		Append Blobs		

Built on a unified Distributed Storage System
Durability, Encryption at Rest, Strongly Consistent Replication, Fault Tolerance, Auto Load-Balancing

Azure Storage & Data Services

	Blobs	Data Lake Store	mongoDB	Files
Unstructured Data	Highly scalable, REST based cloud object store	HDFS as a service	Elastic scale Cross platform	Fully Managed File Shares in the Cloud
	Queues	Disks		
	FIFO async messaging	Virtual Machine VHD files		

	Cosmos DB	Azure SQL DB	Azure Synapse Analytics	Tables
Structured Data	NoSQL document database service	Fully managed database-as-a-service built on SQL	Elastic data warehouse as a service	Key Value, high scale, auto-scaling NoSQL store

Microsoft Confidential

Blob Storage

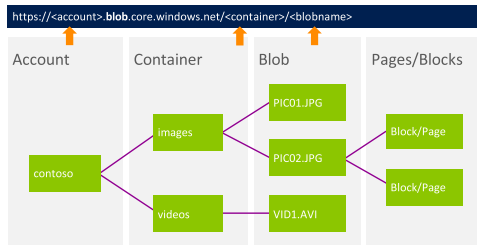|	
Azure Blob storage is a service that stores unstructured data in the cloud as objects or blobs.	Blob storage can store any type of text or binary data, such as a document, media file, or application installer.
Blob storage is also referred to as object storage.	Azure Storage offers three types of blobs: block blobs, page blobs, and append blobs.

Blob Storage Concepts

https://<account>.**blob**.core.windows.net/<container>/<blobname>

Account	Container	Blob	Pages/Blocks

- contoso
- images
- videos
- PIC01.JPG
- PIC02.JPG
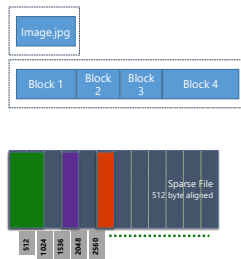- VID1.AVI
- Block/Page
- Block/Page

Microsoft Confidential

Blob Types

- Block blob
  - Targeted at streaming workloads or individual file uploads
  - Each blob consists of a sequence of blocks
  - Each block is identified by a Block ID
  - Size limit of **4.7** TB per blob
  - Optimistic concurrency via Entity Tags (ETags)
  - Optimistic or pessimistic (locking) concurrency via leases
  - Manage leases from Azure portal

- Page blob
  - Targeted at random read/write workloads
  - Each blob consists of an array of pages
    - Each page is identified by its offset from the start of the blob
  - Size limit of **8 TB** per blob
  - Optimistic concurrency via Entity Tags (ETags)
  - Optimistic or pessimistic (locking) concurrency via leases
  - Manage leases from Azure portal

Image.jpg

| Block 1 | Block 2 | Block 3 | Block 4 |

Sparse File
512 byte aligned

512 | 1024 | 1536 | 2048 | 2560

Microsoft Confidential

Blob Types

- Append Blob
  - An append blob is comprised of blocks and is optimized for append operations
  - When you modify an append blob blocks are added to the end of the blob by the Append Block operation
  - Updating or deleting of existing blocks is not supported
  - Does not expose its block IDs
  - Each block in an append blob can be a different size, up to a maximum of 4 MB and can include up to 50,000 blocks
  - The maximum size of an append blob is 4 MB X 50,000 blocks
  - Optimistic concurrency via Entity Tags (ETags)
  - Optimistic or pessimistic (locking) concurrency via leases
  - Manage leases from Azure portal

Microsoft Confidential

Blob Names

https://contoso.blob.core.windows.net/vhds/OSDisk.vhd

Account Name: 3-24 characters, lower case only	Container Name: 3-63 characters, lower case only
Blob Name: 1-1024 characters, case sensitive	Virtual directories within blob namespace

Microsoft Confidential

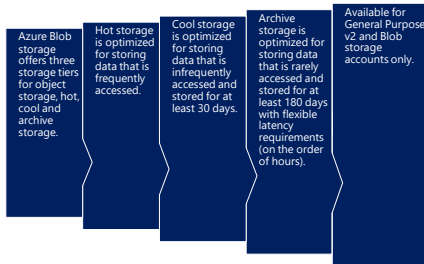## Hot, Cool & Archive Storage Tiers

Azure Blob storage offers three storage tiers for object storage, hot, cool and archive storage.

Hot storage is optimized for storing data that is frequently accessed.

Cool storage is optimized for storing data that is infrequently accessed and stored for at least 30 days.

Archive storage is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Available for General Purpose v2 and Blob storage accounts only.

Microsoft Confidential

Hot, Cool & Archive Storage Tiers

Pricing to match workload
- Hot: Higher storage costs, lower access and transaction costs
- Cool: Lower storage costs, higher access and transaction costs
- Archive: Lowest storage costs, highest access and transaction costs

Switch account tiers as needed
- Charges may apply

Blob REST API

Blob Storage Account – Hot
Data that's in active use

Blob Storage Account – Cool
Short-term backup and disaster recovery datasets

Blob Storage Account – Archive
Long-term backup, secondary backup, and archival datasets
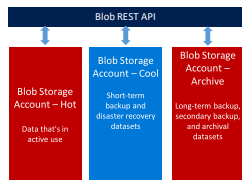
Microsoft Confidential

Pricing and billing

- **Storage costs**: The per-gigabyte cost decreases as the tier gets cooler.

- **Data access costs**: Increase as the tier gets cooler. For data in the cool and archive access tier, you're charged a per-gigabyte data access charge for reads.

- **Transaction costs**: There's a per-transaction charge for all tiers that increases as the tier gets cooler.

- **Geo-Replication data transfer costs**: Applies to accounts with geo-replication configured, including GRS and RA-GRS.

- **Outbound data transfer costs**: Data that is transferred out of an Azure region incur billing for bandwidth usage on a per-gigabyte basis, consistent with general-purpose storage accounts.

- **Changing the access tier**: Will result in tier change charges for access tier inferred blobs stored in the account that don't have an explicit tier set.

Archive Storage Tier

- Intended for data that can tolerate several hours of retrieval latency and will remain in the archive tier for at least 180 days

- Is enabled on a blob and not a container or storage account

- While a blob is in archive storage, it is offline and cannot be read (except the metadata, which is online and available), copied, overwritten, or modified

- You cannot take snapshots of a blob in archive storage

- To read data in archive storage, you must first change the tier of the blob to hot or cool, this process is known as rehydration and can take up to 15 hours to complete

---

Usage Scenarios for Archive Storage Tier

Long-term backup, secondary backup, and archival datasets	Original (raw) data that must be preserved, even after it has been processed into final usable form. (For example, Raw media files after transcoding into other formats)	Compliance and archival data that needs to be stored for a long time and is hardly ever accessed. (For example, Security camera footage, old X-Rays/MRIs for healthcare organizations, audio recordings, and transcripts of customer calls for financial services)

Microsoft Confidential

Storage Tier Comparison

	Premium performance	Hot tier	Cool tier	Archive tier
Availability	99.9%	99.9%	99%	Offline
Availability (RA-GRS reads)	N/A	99.99%	99.9%	Offline
Usage charges	Higher storage costs, lower access and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
Minimum object size	N/A	N/A	N/A	N/A
Minimum storage duration	N/A	N/A	30 days[1]	180 days
Latency (Time to first byte)	Single-digit milliseconds	milliseconds	milliseconds	hours[2]

[1] Objects in the cool tier on GPv2 accounts have a minimum retention duration of 30 days. Blob storage accounts don't have a minimum retention duration for the cool tier.

[2] Archive Storage currently supports 2 rehydrate priorities, High and Standard, that offers different retrieval latencies.

Microsoft Confidential

Soft Delete

- Allows you to recover your data when it is erroneously modified or deleted by an application or other storage account user
- When data is deleted, it transitions to a soft deleted state instead of being permanently erased
- When soft delete is on and you overwrite data, a soft deleted snapshot is generated prior to the data being overwritten
- Currently you can retain soft deleted data for between 1 and 365 days
- Billing based on Undelete Blob transactions at the "Write Operations" rate, not billed for the automatic generation of snapshots
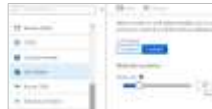
Table Storage

- Azure Table storage is a service that stores large amounts of structured data in the cloud as entities within a table.
- Table storage contains the following components:

URL format: https://<storage account>.table.core.windows.net/<table> to access the tables.

Storage Account: All access to Azure Storage is done through a storage account.

Table: A table is a collection of entities.

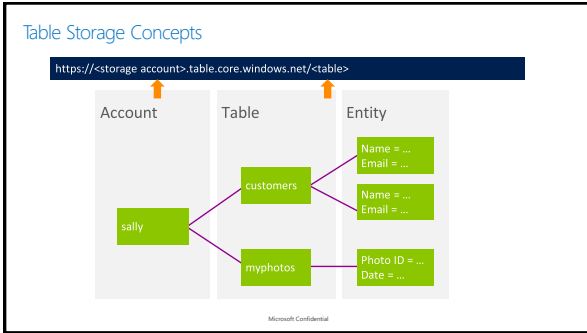Entity: An entity is a set of properties, similar to a database row and can be up to 1MB in size.

Property: A property is a name-value pair and each entity can include up to 252 properties to store data.

Microsoft Confidential

Table Storage Concepts

https://<storage account>.table.core.windows.net/<table>

Account   Table   Entity

sally

customers

myphotos

Name = ...
Email = ...

Name = ...
Email = ...

Photo ID = ...
Date = ...

Microsoft Confidential

Entity Properties

- Entity can have up to 252 properties
  - Up to **1 MB** per entity
- Mandatory Properties for every entity
  - PartitionKey and RowKey (only indexed properties)
    - Uniquely identifies an entity
    - Defines the sort order
  - Timestamp
    - Optimistic concurrency
    - Exposed as an HTTP eTag
- No fixed schema for other properties
  - Each property is stored as a <name, typed value> pair
  - No schema stored for a table
  - Properties can be the standard .NET types
  - String, binary, bool, DateTime, GUID, int, int64, and double2

No Fixed Schema

FIRST	LAST	BIRTHDATE	FAV SPORT
Wade	Wegner	2/2/1981	
Nathan	Totten	3/15/1965	Canoeing
Nick	Harris	May 1, 1976	

Microsoft Confidential

Queue Storage

Azure Queue storage is a service for storing large numbers of messages that can be accessed from anywhere in the world via authenticated calls using HTTP or HTTPS.

A single queue message can be up to 64 KB in size, and a queue can contain millions of messages, up to the total capacity limit of a storage account.

Asynchronous messaging for communication between application components, whether they are running in the cloud, on a desktop, on an on-premises server, or on a mobile device.

Queue Storage

• Queue storage contains the following components:

URL Format	https://<storage account>.queue.core.windows.net/<queue> to access the tables.
Storage Account	All access to Azure Storage is done through a storage account.
Queue	A queue contains a set of messages, all messages must be in a queue and queue names must be all lowercase.
Message	A message, in any format, of up to 64 KB, the maximum time that a message can remain in the queue is 7 days.

Queue Storage Concepts

https://<storage account>.queue.core.windows.net/<queue>

Account

Queue

Images-to-download

myaccount

Images-to-resize

https://myaccount.queue.core.windows.net/images-to-download

Disk Storage

Unmanaged Disks:

This is the initial storage model where you manage the storage accounts that are used to store the VHD files that correspond to your VM disks.

Managed Disks:

This is the new storage model where Microsoft manages the storage accounts that are used to store the VHD files that correspond to your VM disks.

Managed Disks

- What are Azure Managed Disks?
  - Azure Managed Disks are VHD's that are stored in a Microsoft managed storage account.

- Administrators do not have access to the managed disk storage account.

- **Note**: Managed disks are not a replacement for other storage account services i.e. Blobs, Tables & Queues.

Managed Disks Benefits

- Simple and scalable VM deployment
  - Up to 50 000 VM disks of a type in a subscription per region.
  - Up to 1 000 VMs in a virtual machine scale set.
  - No storage account management.

- Better reliability for Availability Sets
  - Ensures that the disks of VMs in an Availability Set are sufficiently isolated from each other to avoid single points of failure.

- Integration with Availability Zones
  - Managed disks supports Availability Zones, which is a high-availability offering that protects your applications from datacenter failures. Azure offers industry best 99.99% VM uptime SLA.

- Better security
  - Use Azure Role-Based Access Control (RBAC) to assign specific permissions for a managed disk to one or more users.
  - Supports granular permissions.

- Supports a read-only shared access signature (SAS)

Managed Disks Performance Tiers

• Managed Disks offers 4 performance tiers:

❶	❷	❸	❹
Ultra disk	Premium (SSD-based)	Standard (SSD-based)	Standard (HDD-based)

Microsoft Confidential
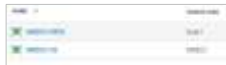
Managed Disks Images & Snapshots

• **Images** is a feature that allows you to capture, in a single image, all managed disks associated with a running VM.
  • You can create an image from your custom VHD in a storage account or directly from a running VM.
• A **Managed Snapshot** is a read-only copy of a managed disk which is stored as a standard managed disk.
  • With snapshots, you can back up your managed disks at any point in time.
  • These snapshots exist independent of the source disk and can be used to create new Managed Disks or attach to a new VM.
• **Azure Backup service** can also be used with Managed Disks to create a backup job with time-based backups, easy VM restoration and backup retention policies.

Microsoft Confidential

Managed Disks Pricing

When using Managed Disks, the following billing considerations apply:

Storage Type	Billing of a managed disk depends on which type of storage you have selected for the disk
Disk Size	Azure maps the provisioned size rounded to the nearest Managed Disks option
Number of transactions	Billed for the number of transactions performed on a standard managed disk
Outbound data transfers	Data going out of Azure data centers incur billing for bandwidth usage
Managed Disk Snapshots (full disk copy)	Snapshots are billed based on the size used

Microsoft Confidential

Managed Disks Migration

• You can migrate to Managed Disks in following scenarios:

Scenario	Article
Convert stand alone VMs and VMs in an availability set to managed disks	Convert VMs to use managed disks
Convert a single VM from classic to Resource Manager on managed disks	Create a VM from a classic VHD
Convert all the VMs in a vNet from classic to Resource Manager on managed disks	Migrate IaaS resources from classic to Resource Manager and then Convert a VM from unmanaged disks to managed disks
Upgrade VMs with standard unmanaged disks to VMs with managed premium disks	First, Convert a Windows virtual machine from unmanaged disks to managed disks. Then Update the storage type of a managed disk.

Microsoft Confidential

Azure Files

• Azure Files offers fully managed file shares in the cloud that are accessible via SMB

• Can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS via the Internet

• Can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used

• Support for file share snapshots (Incremental)

• Maximum of 200 snapshots

Azure Files Benefits

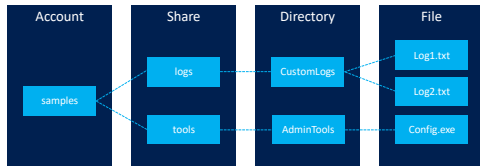|	
Shared access	Using the SMB protocol you can seamlessly replace your on-premises file shares with Azure File shares without worrying about application compatibility.
Fully managed	Azure File shares can be created without the need to manage hardware or an OS.
Scripting and tooling	PowerShell cmdlets and Azure CLI can be used to create, mount, and manage Azure File shares as part of the administration of Azure applications.
Resiliency	Azure Files has been built from the ground up to be always available.
Familiar programmability	Applications running in Azure can access data in the share via file system I/O APIs.

Microsoft Confidential

Azure Files Concepts

- A share can have multiple directories
- All directories and files must be created in a parent share
- An account can contain an unlimited number of shares, and a share can store an unlimited number of files, up to the capacity limits of 100TB

Account	Share	Directory	File
samples	logs	CustomLogs	Log1.txt / Log2.txt
	tools	AdminTools	Config.exe

Microsoft Confidential

Azure Files vs Blobs

Description	Azure Blobs	Azure Files
Durability Options	LRS, ZRS, GRS (and RA-GRS for higher availability)	LRS, GRS
Accessibility	REST APIs	SMB 2.1/3.0 (standard file system APIs) REST APIs
Connectivity	REST – Worldwide	SMB 2.1 - Within region REST – Worldwide
Endpoints	https://myaccount.blob.core.windows.net/mycontainer/myblob	\\myaccount.file.core.windows.net\myshare\myfile.txt https://myaccount.file.core.windows.net/myshare/myfile.txt
Directories	Flat namespace however prefix listing can simulate virtual directories	True directory objects
Case Sensitivity of Names	Case sensitive	Case insensitive, but case preserving
Capacity	Up to 500TB containers	Up to 100TB of files
Throughput	Up to 60 MB/s per blob	Up to 60 MB/s per share
Object size	Up to 4 TB/blob	Up to 1 TB/file
Billed capacity	Based on bytes written	Based on file size

Azure Files vs Disk

Description	Disk	Azure Files
Relationship with Azure VMs	Required for booting (OS Disk)	
Scope	Exclusive/Isolated to a single VM	Shared access across multiple VMs and also on-premises
Snapshots and Copy	Yes	No
Configuration	Configured via portal/Management APIs and available at boot time	Connect after boot (via net use on windows)
Built-in authentication	Built-in authentication	Set up authentication on net use
Cleanup	Resources can be cleaned up with VM if needed	Manually via standard file APIs or REST APIs
Access via REST	Can only access as fixed formatted VHD (single blob) via REST. Files stored in VHD cannot be accessed via REST.	Individual files stored in share are accessible via REST
Max Size	4TB Disk	5TB File Share 1TB file within share
Max 8KB IOps	500 IOps (Basic Storage)	1000 IOps
Throughput	Up to 60 MB/s per Disk	Up to 60 MB/s per File Share

14

Azure Files – Windows Client OS Support

When a client accesses Azure File Storage, the actual SMB version used will depend on the client OS being used.

Azure Files – Linux Client OS Support

- Linux SMB client does not support encryption
- Mounting from Linux in a different region to the Azure File share requires SMB 3.0

Microsoft

Storage Replication

Microsoft Services

Storage Replication

Data in a Microsoft Azure storage account is always replicated to ensure durability and high availability.	Replication copies your data, either within the same data center, or to a second data center, depending on which replication option you choose.	Replication protects your data and preserves your application up-time in the event of transient hardware failures.	If your data is replicated to a second data center, that also protects your data against a catastrophic failure in the primary location.

Storage Replication Terminology

Storage Node	Scale Unit
A storage node is a disk array.	A storage scale unit is a collection of racks of storage nodes.
Fault domain (FD)	Upgrade domain (UD)
is a group of nodes that represent a physical unit of failure and can be considered as nodes belonging to the same physical rack.	is a group of nodes that are upgraded together during the process of a service upgrade or rollout.

Microsoft Confidential

Storage Replication Terminology

Node/Disk Array

Fault Domain/Rack

Upgrade Domain

Scale Unit/Collection of racks of nodes

Microsoft Confidential

Storage Replication Types

Locally redundant storage (LRS)	Zone-redundant storage (ZRS)	Geo-redundant storage (GRS)
Read-access geo-redundant storage (RA-GRS)	Geo-zone-redundant storage (GZRS)	Read-access geo-zone-redundant storage (RA-GZRS)

Microsoft Confidential

Locally Redundant Storage (LRS)

Locally redundant storage (LRS) replicates your data three times within a storage scale unit which is hosted in a datacenter in the region in which you created your storage account.	A write request returns successfully only once it has been written to all three replicas.	These three replicas each reside in separate fault domains and upgrade domains within one storage scale unit to ensure that data is available even if hardware failure impacts a single rack or when nodes are upgraded during a rollout.

Microsoft Confidential

Zone-Redundant Storage (ZRS)

Zone-redundant storage (ZRS) replicates your data synchronously across datacenters within a region, storing three replicas and providing higher durability than LRS.	Data stored in ZRS is durable even if the primary datacenter is unavailable or unrecoverable.	Available for block blobs, non-disk page blobs, files, tables, and queues in general purpose v2 storage accounts.

Microsoft Confidential

Geo-Redundant Storage (GRS)

Geo-redundant storage (GRS) replicates your data to a secondary region that is hundreds of miles away from the primary region.	If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region is not recoverable.	An update is first committed to the primary region, where it is replicated three times, then the update is replicated asynchronously to the secondary region, where it is also replicated three times.	With GRS, both the primary and secondary regions manage replicas across separate fault domains and upgrade domains within a storage scale unit.

Microsoft Confidential

Read-Access Geo-Redundant Storage (RA-GRS)

Read-access Geo-Redundant storage (RA-GRS) provides read-only access to the data in the secondary location, in addition to the replication across two regions provided by GRS.	Secondary endpoint is similar to the primary endpoint, but appends the suffix –secondary to the account name e.g. if your primary endpoint is myaccount.blob.core.win dows.net, then your secondary endpoint is myaccount-secondary.blob.core.win dows.net.	The access keys for your storage account are the same for both the primary and secondary endpoints.

Microsoft Confidential

Geo-zone-redundant storage (GZRS)

Geo-zone-redundant storage (GZRS) = the high availability of zone-redundant storage (ZRS) + protection from regional outages as provided by geo-redundant storage (GRS).	You can continue to read and write data if an availability zone becomes unavailable. And, your data is also durable in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.	Data is first replicated synchronously in the primary region across three availability zones. The data is then replicated asynchronously to a second region that is hundreds of miles away. When the data is written to the secondary region, it's further replicated synchronously three times within that region using LRS.

Microsoft Confidential

Read-access geo-zone-redundant storage (RA-GZRS)

When you enable RA-GZRS for your storage account, your data can be read from the secondary endpoint as well as from the primary endpoint for your storage account.	Secondary endpoint appends the suffix – *secondary* to the account name, e.g., if your primary endpoint for the Blob service is myaccount.blob.core.windows.net, then your secondary endpoint is myaccount-secondary.blob.core.windows.net.	The access keys for your storage account are the same for both the primary and secondary endpoints.

Microsoft

Storage Security

Microsoft Services

Authorizing access to Azure Storage

- The following table describes the options that Azure Storage offers for authorizing access to resources:

	Shared Key (storage account key)	Shared access signature (SAS)	Azure Active Directory (Azure AD)	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Supported
Azure Files (SMB)	Supported	Not supported	Supported, only with AAD Domain Services	Not supported
Azure Files (REST)	Supported	Supported	Not supported	Not supported
Azure Queues	Supported	Supported	Supported	Not supported
Azure Tables	Supported	Supported	Not supported	Not supported

Authorize access to Azure blobs and queues using Azure AD

- Note, Microsoft recommends using Azure AD authorization with your Azure Storage applications when possible.

- Azure Storage defines a set of built-in RBAC roles that encompass common sets of permissions used to access blob and queue data. You can also define custom roles for access to blob and queue data.

- The list describes the levels at which you can scope access to Azure blob and queue resources, starting with the narrowest scope:

  - An individual container.
  - An individual queue.
  - The storage account.
  - The resource group.
  - The subscription.

- Specific Blob or Queue service operations can be authorized via RBAC actions.
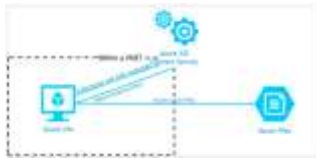

Azure AD Domain Services (DS) integration

- Azure Files supports identity-based authentication over Server Message Block (SMB) through Azure AD DS. This provides RBAC for fine-grained control over a client's access to resources in a storage account.

- Azure Files uses Azure AD Domain Services to support Kerberos authentication with Azure AD credentials from domain-joined VMs.

Shared Access Signatures

- Fine grain access rights to storage entities (blobs/tables etc)

- Sign URL with storage key—permit elevated rights

- Revocation:
  - Use short time periods and re-issue
  - Use container-level policy that can be deleted

- Two broad approaches:
  - Ad hoc
  - Policy-based

Ad Hoc Signatures

- Create short-dated SAS
  - Signedresource Blob or Container
  - AccessPolicy Start, Expiry, and Permissions
  - Signature HMAC-SHA256 of above fields

- Use case
  - Single use URLs
  - For example, provide URL for the client to upload to container

```
        https://...blob.../pics/image.jpg?
 sr=c&st=2009-02-09T08:20Z&se=2009-02-10T08:30Z&sp=w
&sig= dD80ihBh5jfNpymO5Hg1IdiJIEvHcJpCMiCMnN%2fRnbI%3d
```

Microsoft Confidential

Policy-Based Signatures

- Create container-level policy
  - Specify StartTime, ExpiryTime, and Permissions
  - Also created in the Azure Portal
- Create SAS URL
  - Signedresource Blob or Container
  - Signedidentifier optional pointer to container policy
  - Signature HMAC-SHA256 of above fields

```
        https://...blob.../pics/image.jpg?
      sr=c&si=MyUploadPolicyForUserID12345
&sig=dD80ihBh5jfNpymO5Hg1IdiJIEvHcJpCMiCMnN%2fRnbI%3d
```

- Use case
  - Providing revocable permissions to certain users/groups
  - To revoke: Delete or update container policy

Microsoft Confidential

Authorize with Shared Key

- **Use the Shared Key authorization scheme to make requests against the Blob, Queue, and File services.** Shared Key authorization in version 2009-09-19 and later supports an augmented signature string for enhanced security and requires that you update your service to authorize using this augmented signature.

- **Use the Shared Key authorization scheme to make requests against the Table service using the REST API.** Shared Key authorization for the Table service in version 2009-09-19 and later uses the same signature string as in previous versions of the Table service.

- **Use the Shared Key Lite authorization scheme to make requests against the Blob, Queue, Table, and File services.**

  - For version 2009-09-19 and later of the Blob and Queue services, Shared Key Lite authorization supports using a signature string identical to what was supported against Shared Key in previous versions of the Blob and Queue services. You can therefore use Shared Key Lite to make requests against the Blob and Queue services without updating your signature string.
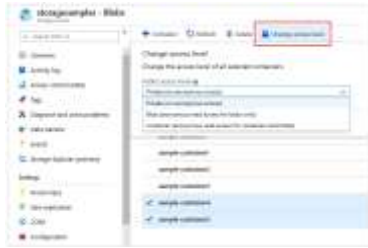
Microsoft Confidential

Grant anonymous users permissions to containers and blobs

- You can configure a container with the following permissions:
  - No public read access.
  - Public read access for blobs only.
  - Public read access for container and its blobs.

Azure Disk Encryption (Encryption at Rest)

- Allows you to encrypt your VM OS and Data disks using Bitlocker technology
- Integrated with Azure Key Vault to store and manage disk encryption keys and secrets
- Ensures that all data on the virtual machine disks are encrypted at rest in your Azure storage account
- Supports BYOK to further safeguard the data encryption key (Passphrase secret) in your key vault

Storage Service Encryption (Encryption at Rest)

- Automatically encrypts your data before persisting it to Azure Storage, and decrypts the data before retrieval
- Enabled for all new and existing storage accounts and cannot be disabled
- Encrypted using 256-bit AES encryption, Microsoft managed keys
- Automatically encrypts data in:
  - Both performance tiers (Standard and Premium)
  - Both deployment models (Azure Resource Manager and classic)
  - All of the Azure Storage services (Blob storage, Queue storage, Table storage, and Azure Files)
- No additional cost

Storage Service Encryption with Customer Managed Keys

- Allows you to specify your own encryption keys

- Create your own encryption keys and store them in a key vault, or you can use Azure Key Vault's APIs to generate encryption keys

- Custom keys give you more flexibility, so that you can create, rotate, disable, and define access controls.

- Custom keys also enable you to audit the encryption keys used to protect your data.

Microsoft Confidential

Storage Account Firewall

- Azure Storage provides a layered security model allowing you to secure your storage accounts to a specific set of networks by means of firewall rules

- When firewall rules are configured, only applications from allowed networks can access a storage account

- When calling from an allowed network, applications continue to require authorization e.g. a valid access key or SAS token to access the storage account

- Must be configured in addition to virtual network service endpoints to allow traffic from a specific virtual network

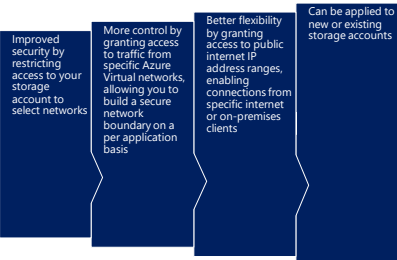## Storage Account Firewall Benefits

Improved security by restricting access to your storage account to select networks

More control by granting access to traffic from specific Azure Virtual networks, allowing you to build a secure network boundary on a per application basis

Better flexibility by granting access to public internet IP address ranges, enabling connections from specific internet or on-premises clients

Can be applied to new or existing storage accounts

Microsoft Confidential

Demo: Create & Explore a storage account & Enable a storage account Firewall

Microsoft

Lab: Implementing Azure Storage

Microsoft Services

Microsoft