

Azure Talk – Azure Storage

Niraj Kumar

Lead Azure Architect, MCT(Microsoft Certified Trainer)



Agenda

Azure Storage

- Azure Storage Overview
- Types of Storage Account and performance tiers
- Storage Replication Scope
- Types of Storage
- Managed VM disk
- Securing Storage
 - SSE(Storage Service Encryption)
 - ADE(Azure Disk Encryption)
 - SAS Signature
 - Secure Transfer required
- Storage Access Tools
- Azure Storage Demo



Azure Storage Overview

Storage for Virtual Machines	<div>Disks "Persistent block storage for Azure IaaS VMs"</div>	<div>Files "Fully Managed File Shares in the Cloud"</div>	
Unstructured Data	<div>Blobs "Highly scalable, REST based cloud object store"</div>	<div>Data Lake Store "HDFS as a service"</div>	
Structured Data	<div>Tables "Key Value, high scale, auto-scaling NoSQL store"</div>	<div>DocumentDB "NoSQL document database service"</div>	<div>Azure SQL DB "Fully managed database-as-a-service built on SQL"</div>

- **Azure Storage** is a service that you can use to store **files, messages, tables** and other types of information.
- Azure storage is also used by **IaaS virtual machines**, and PaaS cloud services.
- All Storage services can be accessed using a REST API.
- You can conceptually think of Azure storage in three areas:
 - Storage for Virtual Machines
 - Unstructured Data storage
 - Structured Data storage.
- What is Storage account? An **Azure storage account** provides a unique namespace to store and access your Azure Storage data objects.



Storage Account

There are two kinds of Storage accounts:

- **General Purpose Storage Account:** A general-purpose storage account gives you access to Azure Storage services such as **Tables, Queues, Files, Blobs** and **Azure virtual machine disks** under a single account. It has two performance tiers:
 - **Standard storage performance tier** which allows you to store **Tables, Queues, Files, Blobs** and Azure virtual machine disks. It's backed by magnetic drives (**HDD**) and provide the lowest cost per GB.
 - **Premium storage performance tier** which currently only supports Azure virtual machine disks. It is backed by solid state drives (**SSD**) and offer consistent low-latency performance.
- **Blob Storage Account:** is a specialized storage account for storing your unstructured data as blobs (objects) in Azure Storage. Blob storage has two tiers:
 - A **Hot** access tier which indicates that the objects in the storage account will be more frequently accessed. This allows you to store data at a lower access cost.
 - A **Cool** access tier which indicates that the objects in the storage account will be less frequently accessed. This allows you to store data at a lower data storage cost.



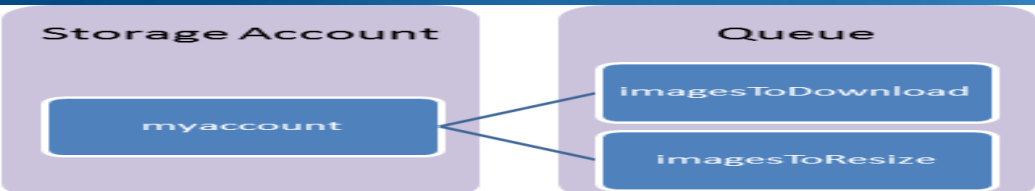
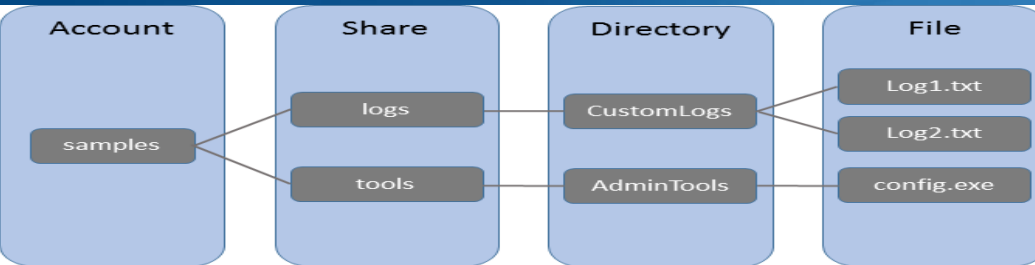
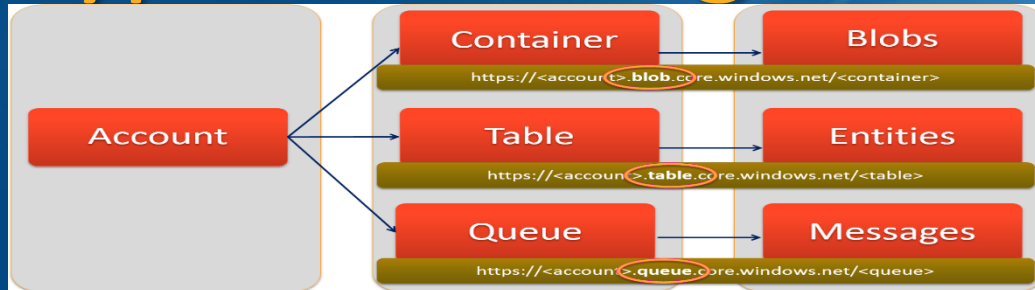
Storage Replication Option

- The data in your Microsoft Azure storage account is always replicated to ensure durability and high availability.
- When you create a storage account, you have four replication options. **LRS, ZRS, GRS, RA-GRS**
- You can switch from LRS to GRS or RA-GRS but **ZRS can't be converted**.

Replication Option	Number of copies	Strategy
Locally redundant storage (LRS)	Maintains three copies of your data.	Data is replicated three time within a single facility in a single region.
Zone-redundant storage (ZRS)	Maintains three copies of your data.	Data is replicated three times across two to three facilities, either within a single region or across two regions.
Geo-redundant storage (GRS)	Maintains six copies of your data.	Data is replicated three times within the primary region, and is also replicated three times in a secondary region hundreds of miles away from the primary region.
Read access geo-redundant storage (RA-GRS) (Default)	Maintains six copies of your data.	Data is replicated to a secondary geographic location, and also provides read access to your data in the secondary location.



Types of Storage



Azure Storage is comprised of four primary types of storage services:

- **Blobs:** Azure Blob storage also called **Object Storage** is a service that stores **unstructured data** in the cloud as objects/blobs. It offers three types of blobs:
 - **Block blobs:** Ideal for storing text or binary files, such as documents and media files.
 - **Append blobs:** Similar to block blobs in that they are made up of blocks, but they are optimized for append operations, so they are useful for **logging scenarios**.
 - **Page blobs:** can be up to 4 TB in size, and are more efficient for frequent read/write operations. **Azure Virtual Machines use page blobs as OS and data disks.**
- **Files:** File storage offers shared storage for applications using the standard SMB 3.0 protocol. Tables
- **Queues:** It 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**. Common use cases are:
 - Creating a backlog of work to process asynchronously
 - Passing messages from an Azure Web role to an Azure Worker role
- **Table:** Azure tables are ideal for storing structured, non-relational data. It can be thought as spreadsheet of information where there is no linkage or relationship (joins) between the information.



Managed Disk, Security and Access Tools

Managed Disk:

- Azure Managed Disks simplifies disk management for Azure IaaS VMs by **managing the storage accounts** associated with the VM disks.
- It is designed for 99.999% availability.
- Managed Disks allow you to create up to **10,000 VM disks** in a subscription.
- Managed Disks provides better reliability for Availability Set by automatically placing the disks in **different** storage scale units (**stamps**).
- Billing for managed disks depends on the provisioned size of the disk and not the actual consumption.

Security:

- **SSE(Storage Service Encryption)**: Azure SSE provides encryption-at-rest and safeguard your data to meet your organizational security and compliance commitments. Any new data written to existing storage account are automatically encrypted-at-rest with keys managed by Microsoft.
- **ADE(Azure Disk Encryption)**: ADE allows you to encrypt the **OS and Data disks** used by an IaaS Virtual Machine. For Windows, the drives are encrypted using **BitLocker** encryption technology. For Linux, the disks are encrypted using the **DM-Crypt** technology. This is integrated with **Azure Key Vault**.
- **Secure access to your data**. There are two methods for controlling access to your data objects: Using **Storage Account Keys** and **Shared Access Signatures** to grant access to specific data objects for a **specific amount of time**.
- **Secure Transfer Required**: The "**Secure transfer required**" option enhances the security of your storage account by only allowing requests to the storage account from secure connections. For example, when calling REST APIs to access your storage account, you must connect using **HTTPS**. Any requests using HTTP are rejected.

Access Tools:

- **PowerShell**: PowerShell offers storage cmdlets to work with Azure Storage.
- **Azure Storage Explorer**: It is a standalone app from Microsoft that allows you to easily work with Azure Storage data on Windows, macOS and Linux.
- **Azcopy**: AzCopy is a Windows command-line utility designed for copying data to and from Microsoft Azure Blob, File, and Table storage.



Azure Storage account configuration *demo*

Niraj Kumar

Lead Azure Architect, MCT(Microsoft Certified Trainer)

