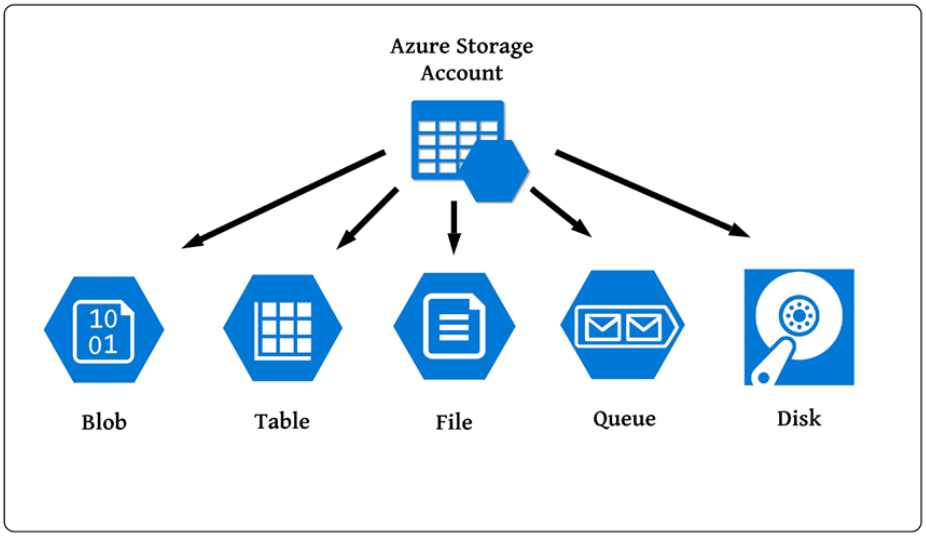
Data and Application in Cloud Security

What is a Storage Account?

All your data items are stored in an Azure storage account: blobs, file shares, queues, tables, and discs. The storage account creates a unique namespace for your Azure Storage data that can be accessed through HTTP or HTTPS from anywhere in the world. Your storage account's data is long-lasting and highly available, as well as safe and enormously expandable.



Source: www.partech.nl

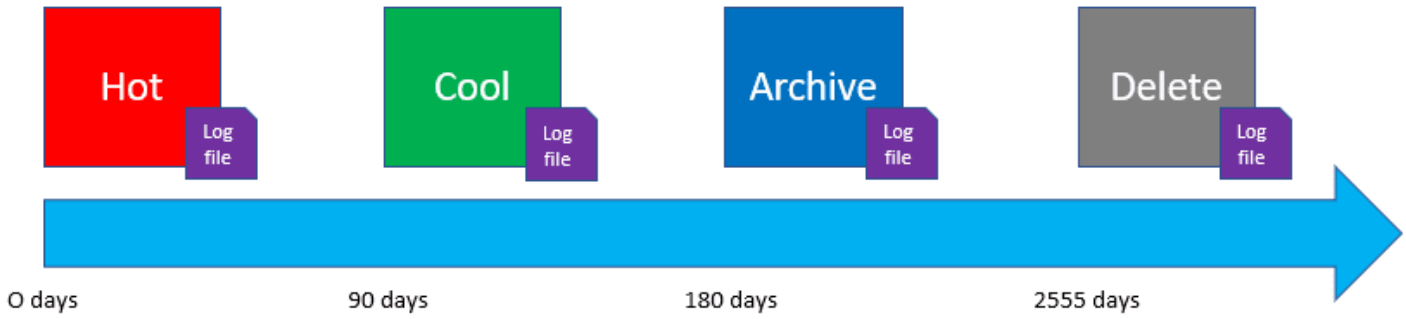
Q1. What do you mean by blobs, file share, queues, table and discs?

- **Blob:** The term "blob" is an acronym for "binary large object." Blobs are large, unstructured files such as photos, video, music files, backup files, and so on. It's a text and binary data object store with huge scalability. Data Lake Storage Gen2 also provides support for big data analytics.
- **Azure Files:** provides fully managed cloud file shares that can be accessed via the industry-standard Server Message Block (SMB) or Network File System (NFS) protocols. Cloud and on-premises deployments can both mount Azure Files file shares at the same time.
- **Azure Queue:** Storage is a service for storing large numbers of messages. Authenticated HTTP or HTTPS calls allow you to access messages from anywhere in the world.
- **Azure Table:** A NoSQL store for schemaless storage of structured data.
- **Azure Disk:** Block-level storage volumes for Azure VMs.

>Know more about Storage Account

Access Tiers

The amount of data saved in the cloud is growing at an exponential rate. To keep expenses down as your storage needs grow, it's a good idea to arrange your data by how often it'll be accessed and how long it'll be kept. Different access tiers are available in Azure storage, allowing you to store your blob data in the most cost-effective way possible based on how it will be used. The following are the Azure Storage access tiers:

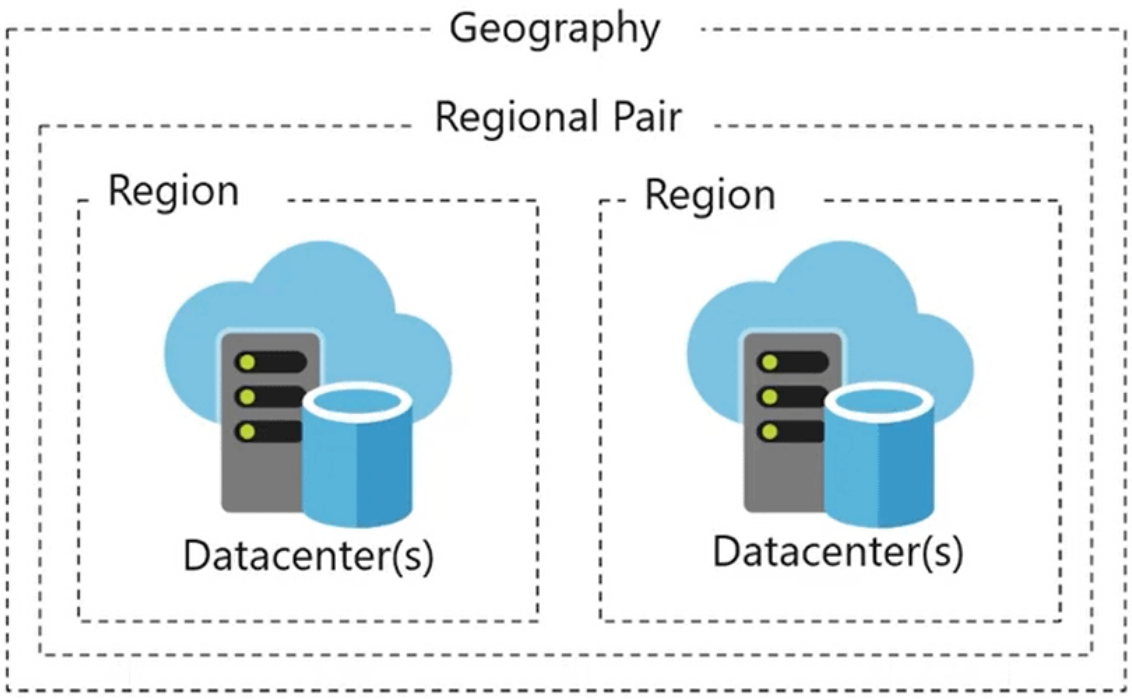


Source: Medium

- **Hot tier:** An online layer designed for storing data that is regularly accessed or updated. The storage costs at the hot tier are the highest, but the access costs are the lowest.
- **Cool tier:** An online layer designed for storing data that is accessed or modified seldom. The data in the cool tier should be kept for at least 30 days. In comparison to the hot tier, the cool tier has reduced storage costs but greater access expenses.
- **Archive tier:** Offline tier for archiving data that is rarely accessed and has variable latency requirements on the order of hours. The data in the archive tier should be kept for at least 180 days.

Data Sovereignty

Data sovereignty refers to the necessity that data be subject to the laws of the country in which it is gathered or processed and remain within its boundaries. These regulations have existed in many nations for decades, and new privacy legislation, such as the GDPR, are just increasing their prominence. Countries such as Russia, China, Germany, France, Indonesia, and Vietnam, to name a few, mandate that individuals' data be maintained on physical servers within their borders.



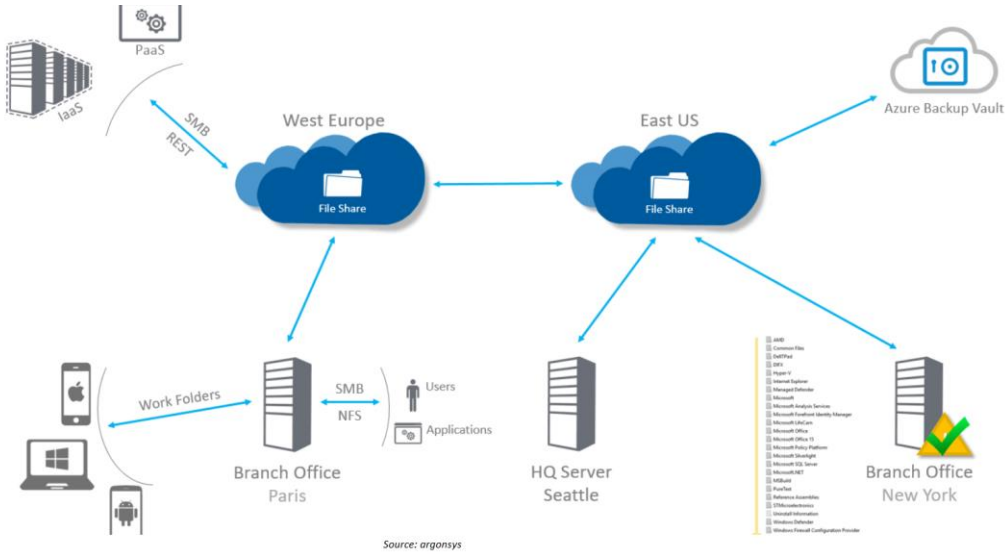
Source: Microsoft

Azure has more global regions than any other cloud provider, giving you the scalability and data residency options you need to bring your apps closer to your global users and well as maintain Data Sovereignty.

Q2. What storage redundancy options does Azure Files support?
Ans. Currently, Azure Files supports locally redundant storage (LRS), zone redundant storage (ZRS), geo-redundant storage (GRS), and geo-zone-redundant storage (GZRS). Azure Files premium tier currently only supports LRS and ZRS.

File Sync

With Azure File Sync, shares can be replicated on-premises or on Azure and accessed via SMB or NFS shares on Windows Server.



Azure File Sync is useful in instances when data must be accessed and edited from a location other than an Azure datacenter, such as a branch office. Data can be replicated between different Windows Server endpoints, for example, between branch offices. Windows Server becomes a rapid cache of your Azure file sharing with Azure File Sync. To access your data locally, you can use any protocol supported by Windows Server, including SMB, NFS, and FTPS. You can have as many caches as you want anywhere on the planet.

Azure File Sync enables organizations to:

- Centralize file services in Azure storage
- Cache data in multiple places for fast, local performance
- Eliminate DR and local backup

Q3. Is Azure File Sync compatible with geo-redundant storage?

Ans. Yes, both locally redundant storage (LRS) and geo-redundant storage are supported by Azure Files (GRS). If you failover a storage account across paired regions from a GRS-enabled account, Microsoft suggests treating the new region as a data backup only. The new primary region is not automatically synced by Azure File Sync.

Azure Storage Access

Every request made against the secure resources must be authorized. The authorization ensures that the resources in your storage account are accessed only when you want them to be accessed and only by trusted apps or users, as it may contain data like credit card information.

We have different options for authorizing access to Azure Storage, for example, Azure AD. Azure Storage provides integration with Azure AD for identity-based authorization of requests to the blob and queue services. A brief picture of which authentication method is supported by which storage type is given below:

Storage	Storage Account Shared Key	Shared access signature	Azure Active Directory	Active Directory Domain Services (on-prem AADS)	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Not supported	Supported
Azure Files (SMB)	Supported	Not supported	Supported, only with Azure AD Domain Services	Supported, credentials must be synced to Azure AD	Not supported
Azure Files (REST)	Supported	Supported	Not supported	Not supported	Not supported

Source: Microsoft

What is Region Pairing?

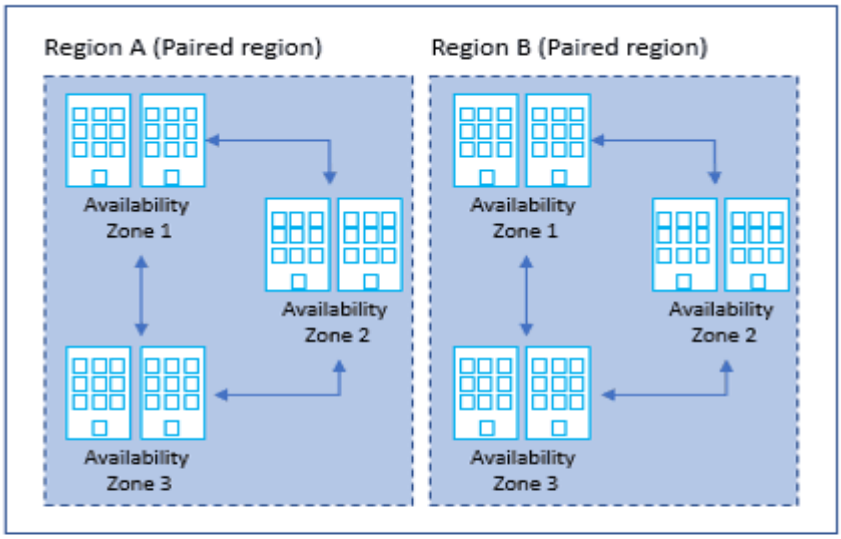
The reason I start here is that Azure contains a feature that's unique among the large three cloud providers. It's the concept of "region pairing." Region pairing is that the relationship between two Azure regions within an identical geographical area to supply geographically redundant solutions. Azure's paired regions are prewired with high bandwidth connectivity between them.

Azure operates in several geographies worldwide, and within given geography or geopolitical boundary, each region is deployed together with another paired region. Some exceptions exist, like Brazil, which is paired with South Central US, but these are edge cases. So, for instance, in the US, Microsoft pairs Virginia (called East US 2) with Iowa (called Central US). So, if you're in East US 2 and a disaster recovery (DR) failover has to occur, you're still within inexpensive proximity to your secondary region and warranted of a high level of service from a latency perspective. Contrast this with the first Virginia region, East US, which pairs with West US (California), and you're faced with a far higher latency should your environment have to failover.

Region Pairs

- Each Azure region pairs with another region within the same geography, together making a regional pair.
- Azure serializes platform updates so only one region is updated at a time.
- Azure Regions in a Pair have direct connections that bring additional benefits to use them together.
- Each Azure Region in a pair is always located greater than 300 miles apart when possible.
- **Examples of region pairs** are West US paired with East US, South-East Asia paired with East Asia.

Data Residency Boundary (Azure Reginal Pairs in geography)



Primary	Secondary
West US	East US
North Europe	West Europe
Southeast Asia	East Asia

Examples of region pairs