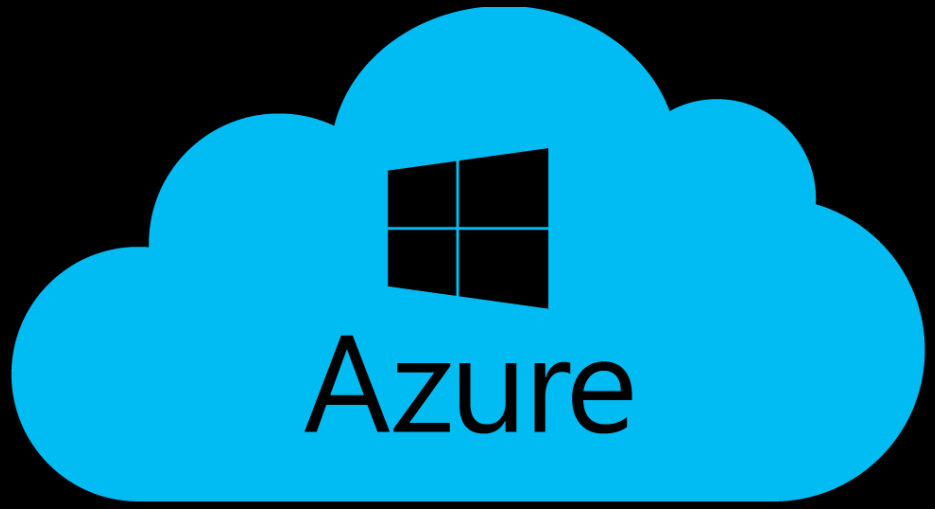

Azure

Storage Account

Data Security

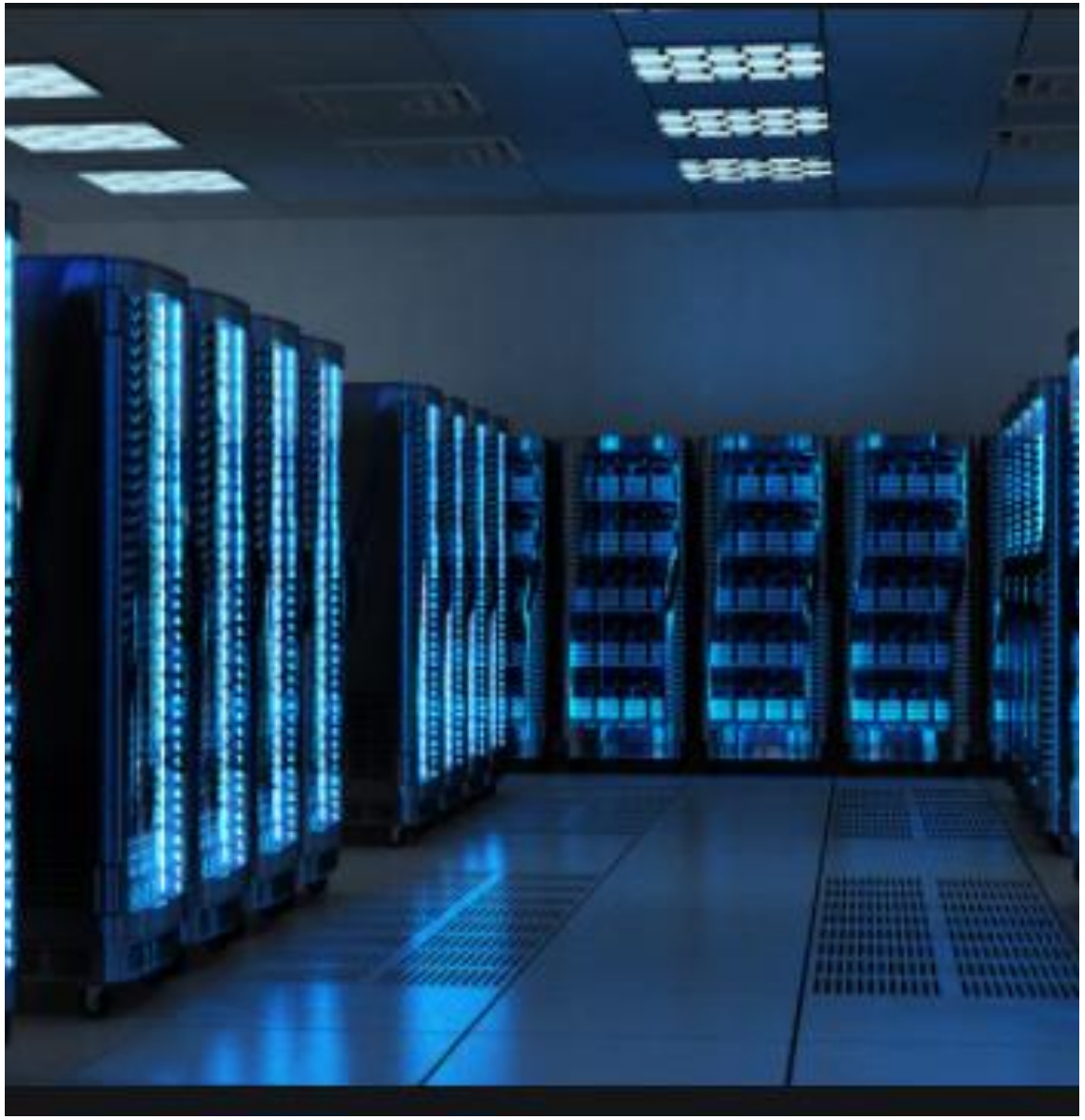
Manage Data

Manage Access

Data Replication

Microsoft Azure Storage

Storage



WannaCry ransomware attack

From Wikipedia, the free encyclopedia

The **WannaCry ransomware attack** was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.[*citation needed*] It propagated through EternalBlue, an exploit discovered by the United States National Security Agency (NSA) for older Windows systems. EternalBlue was stolen and leaked by a group called The Shadow Brokers at least a year prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. These patches are imperative to an organization's cyber-security but many were not applied because of needing 24/7 operation, risking having applications that used to work break, inconvenience, or other reasons.

The attack was halted within a few days of its discovery due to emergency patches released by Microsoft and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.

In December 2017, the United States, United Kingdom and Australia formally asserted that North Korea was behind the attack.[5]

A new variant of WannaCry forced Taiwan Semiconductor Manufacturing Company (TSMC) to temporarily shut down several of its chip-fabrication factories in August 2018. The virus spread to 10,000 machines in TSMC's most advanced facilities.[6]

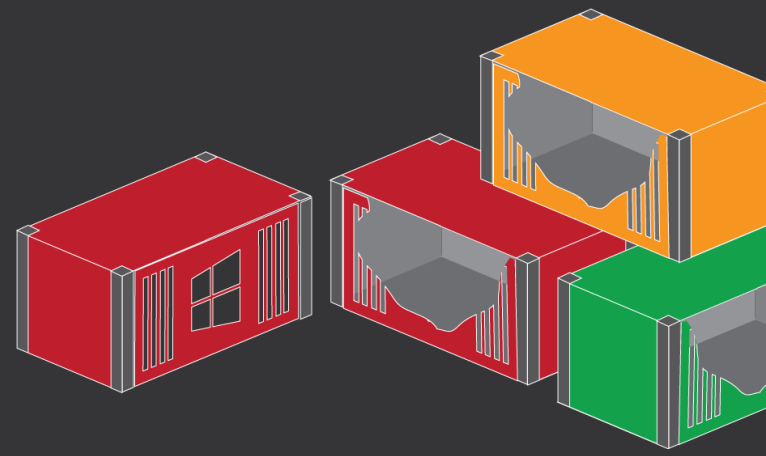
WannaCry ransomware attack

Screenshot of the ransom note left on an infected system

Date	12 May 2017 – 15 May 2017 (initial outbreak)[1]
Duration	4 days
Location	Worldwide
Also known as	Transformations: Wanna → Wana Cryptor → Crypt0r Cryptor → Decryptor Cryptor → Crypt → Cry Addition of "2.0"

Choosing right storage is important

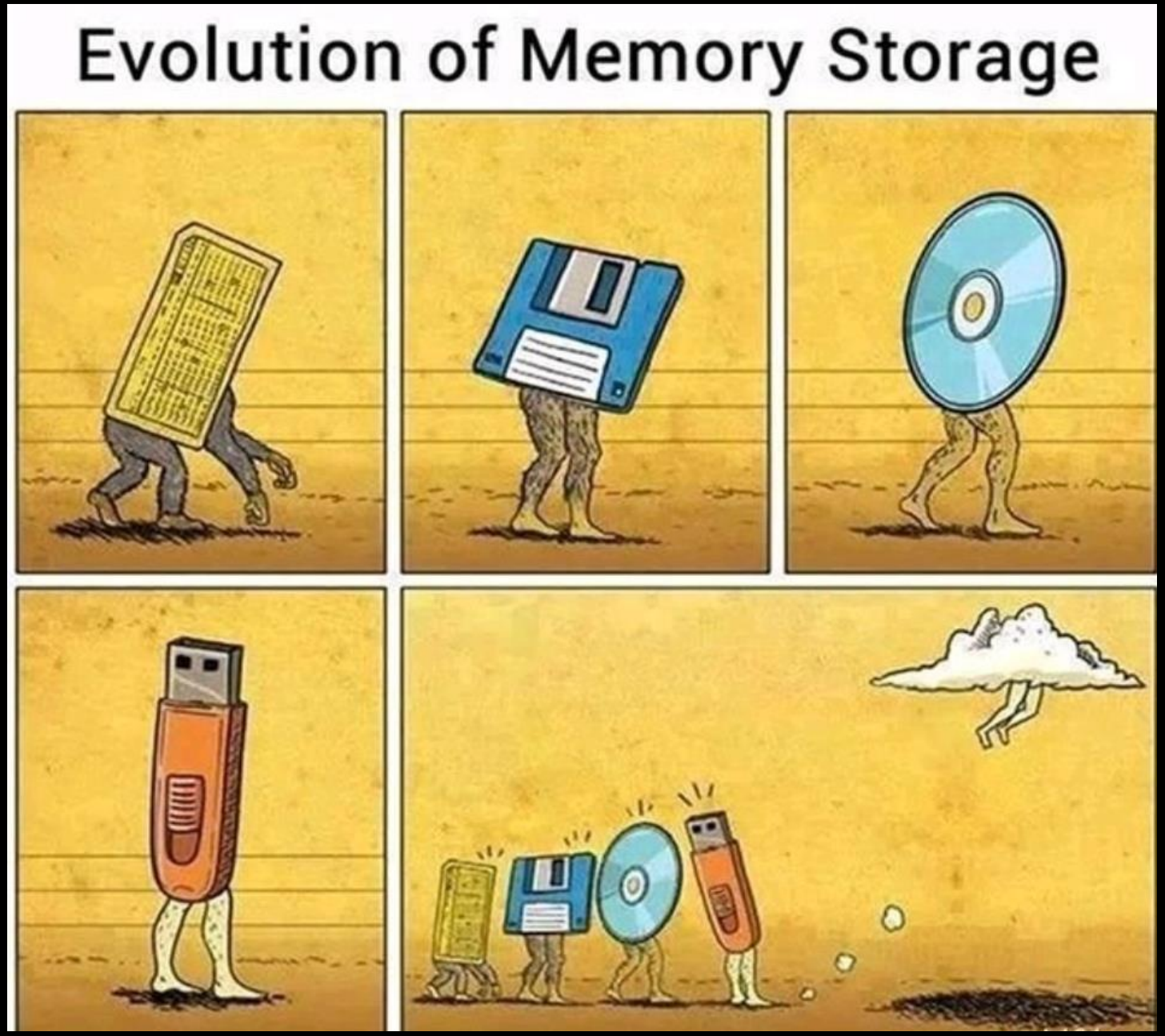
- Cost
- Customer Experience
- Reliability
- Availability

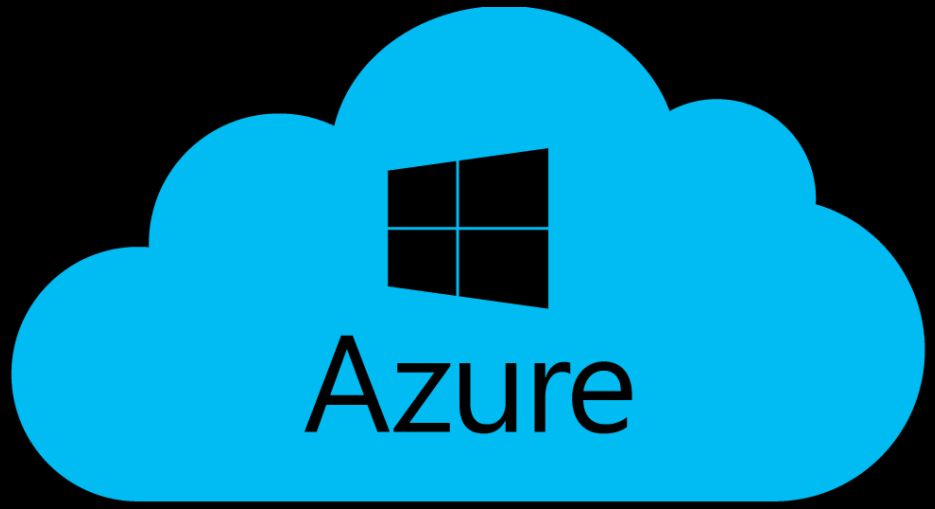


Choose the Right Azure Region f

azure.microsoft.com/en-in/global-infrastructure/geographies/

Azure geographies | Overview | Geographies | Choose your region | Customer stories | New regions | Contact | Free account


Evolution of Memory Storage


Azure


Data is The New Oil

Types of Data

STRUCTURED DATA

SEMI-STRUCTURED DATA

UNSTRUCTURED DATA

Types of Data

Structured Data

Structured data is data that adheres to a schema, so all of the data has the same fields or properties.

Example: A database table

Sr. Number	Emplyee Name	Monthly Salary
1	Vijay	$30,000
2	Pooja	$30,000
3	Mark	$50,000
4	James	$15,000

Types of Data

Semi-structured Data

Semi-structured data doesn't fit neatly into tables, rows, and columns. Instead, semi-structured data uses *tags* or *keys* that organize and provide a hierarchy for the data.

Example: JSON file, XML file

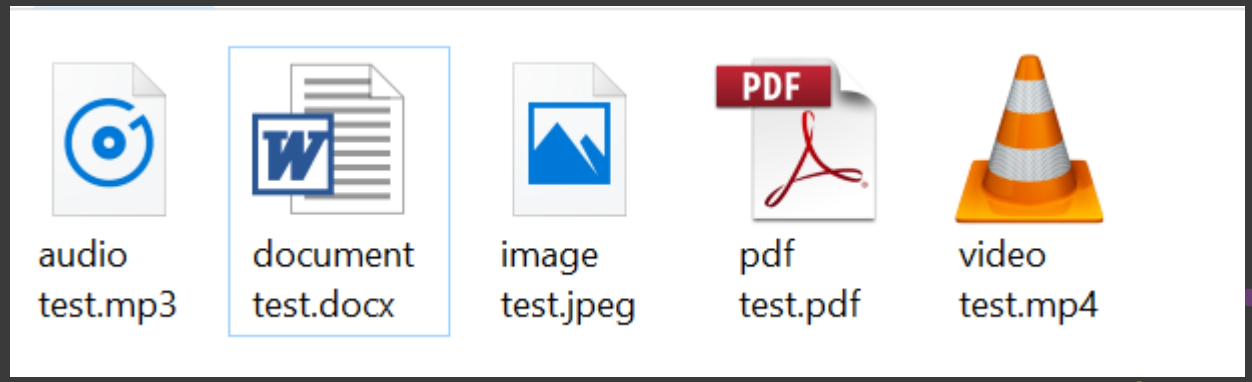
```
student_certifications = @{
                "Student1" = @("AZ-900", "AZ-103");

                "Student2" = @("ITIL 4 Foundation", "AZ-900");

                "Student3" = @("AWS Solution Architect");

                "Student4" = @("AZ-900", "AZ-103", "AZ-200", "AZ-300")
            }
```

Types of Data

Unstructured Data

Unstructured data encompasses data that has no designated structure to it. This lack of structure also means that there are no restrictions on the kinds of data it can hold.

Example: email, video file, pdf



Example

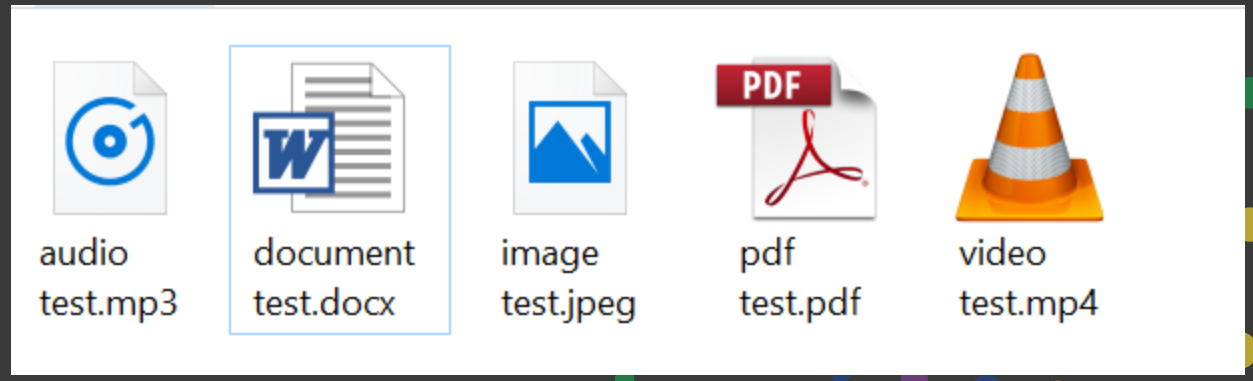
Structured data

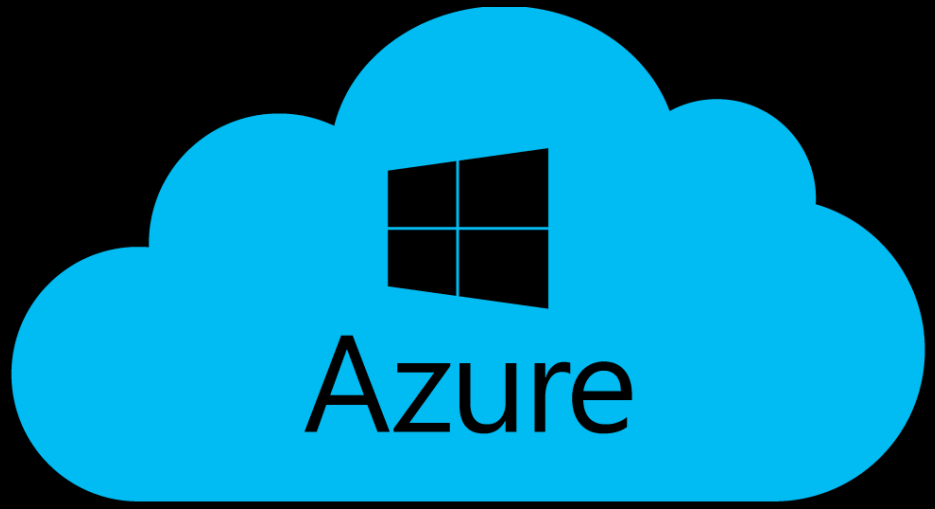
Sr. Number	Emplyee Name	Monthly Salary
1	Vijay	$30,000
2	Pooja	$30,000
3	Mark	$50,000
4	James	$15,000

Semi-Structured data

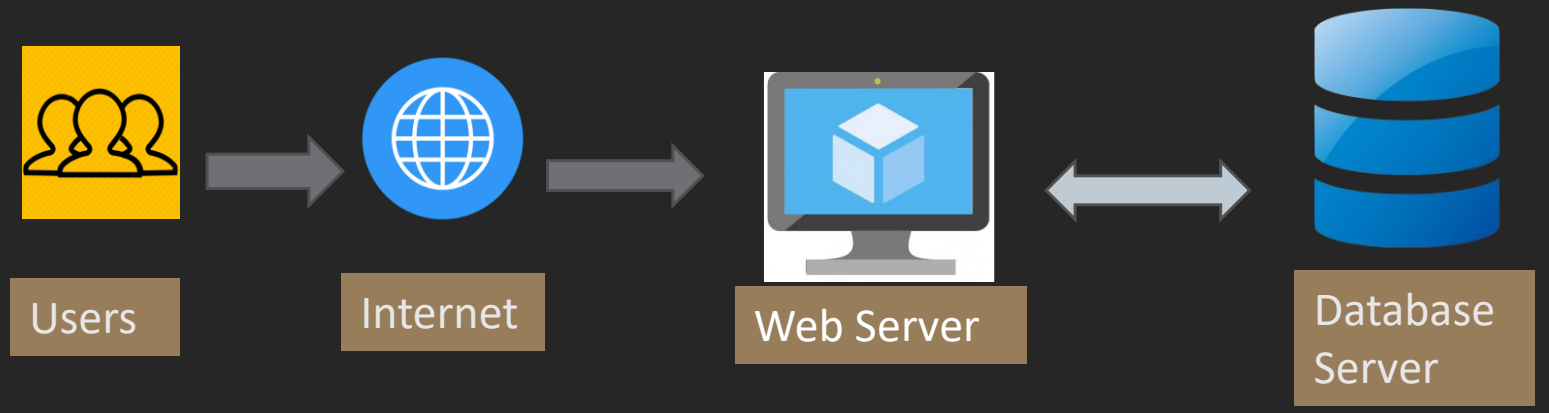
```
student_certifications = @{
                "Student1" = @("AZ-900", "AZ-103");

                "Student2" = @("ITIL 4 Foundation", "AZ-900");

                "Student3" = @("AWS Solution Architect");

                "Student4" = @("AZ-900", "AZ-103", "AZ-200", "AZ-300")
            }
```

Un-Structured data

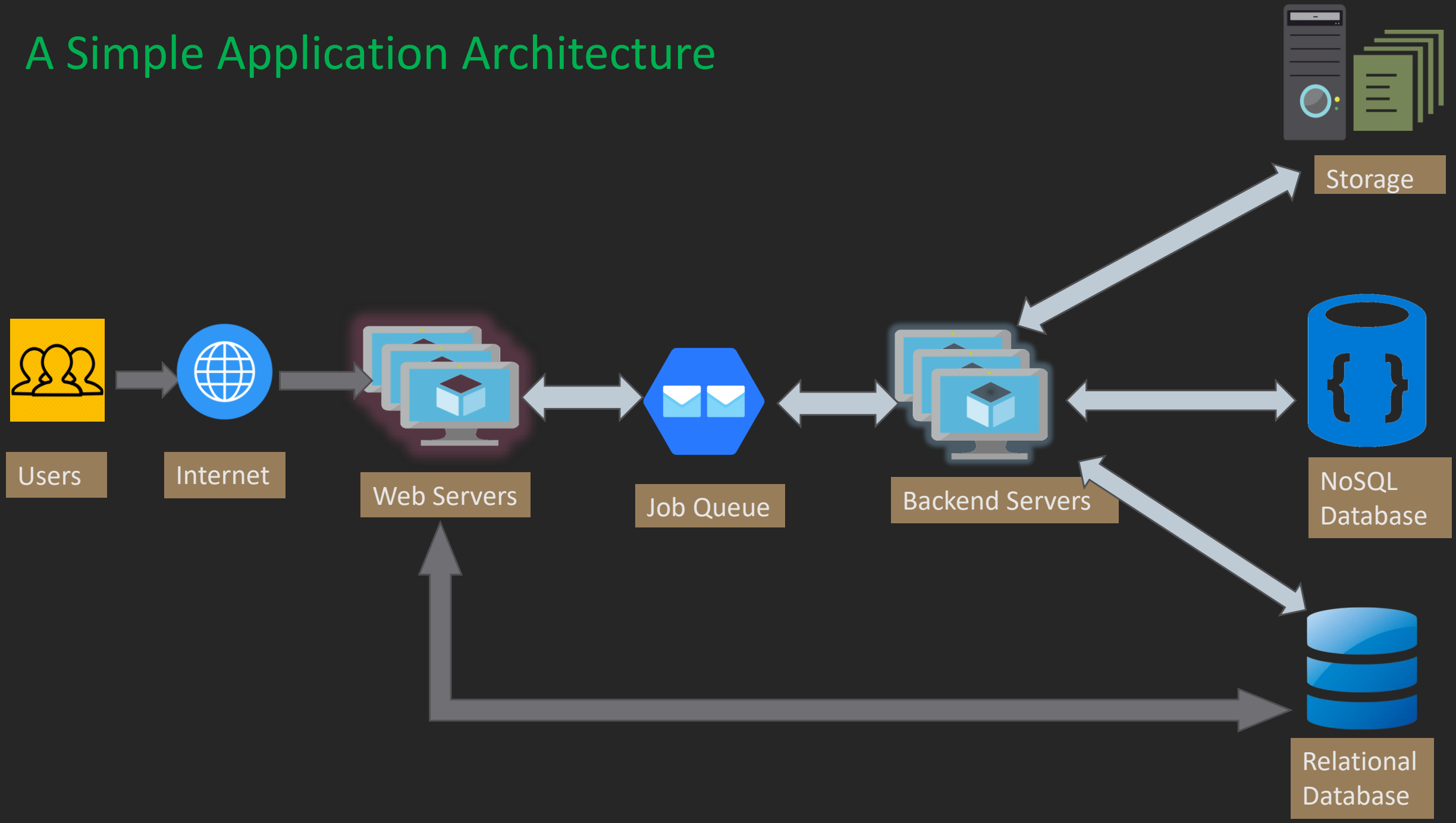



Azure

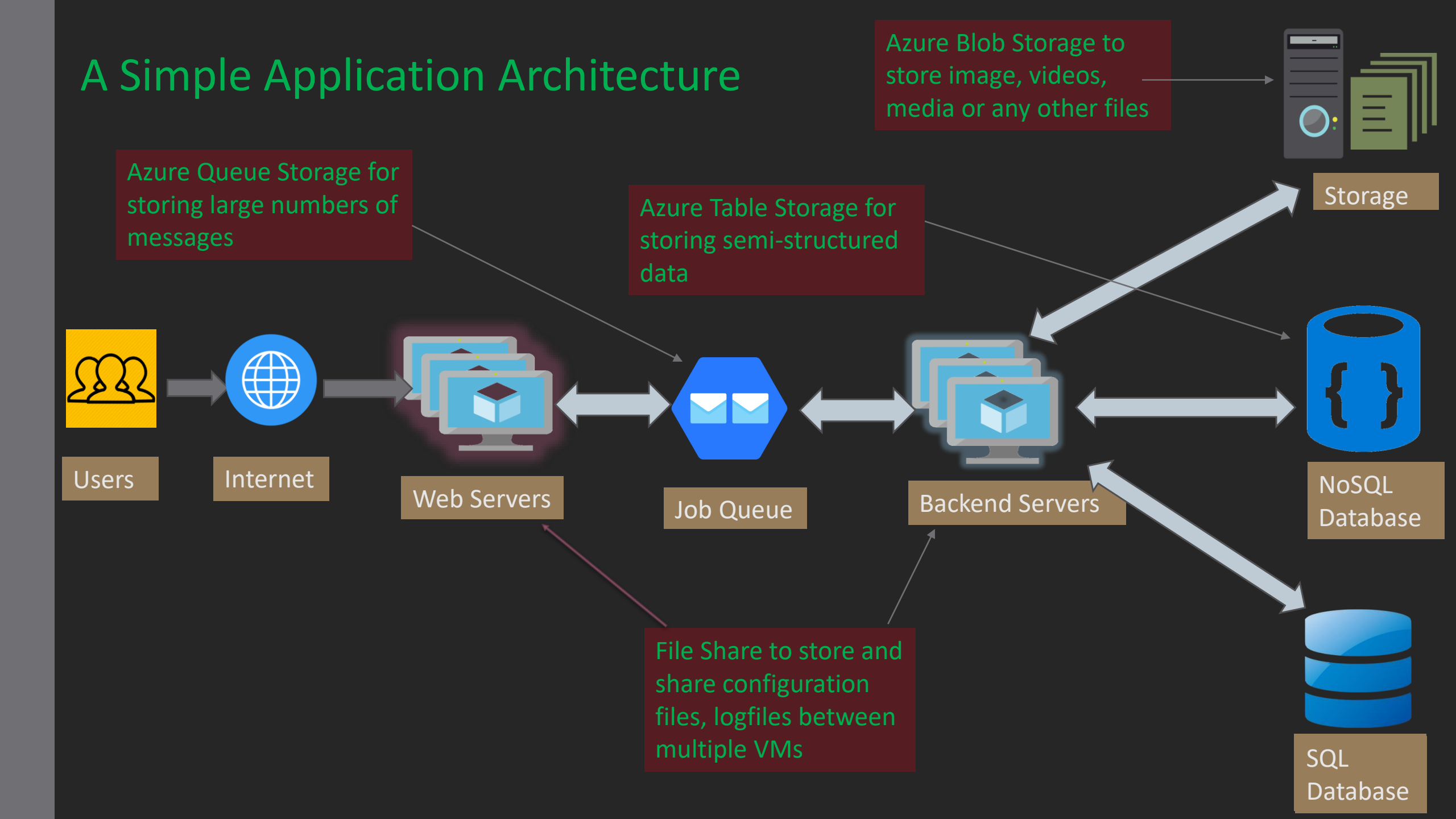
A Simple Application Architecture



A Simple Application Architecture

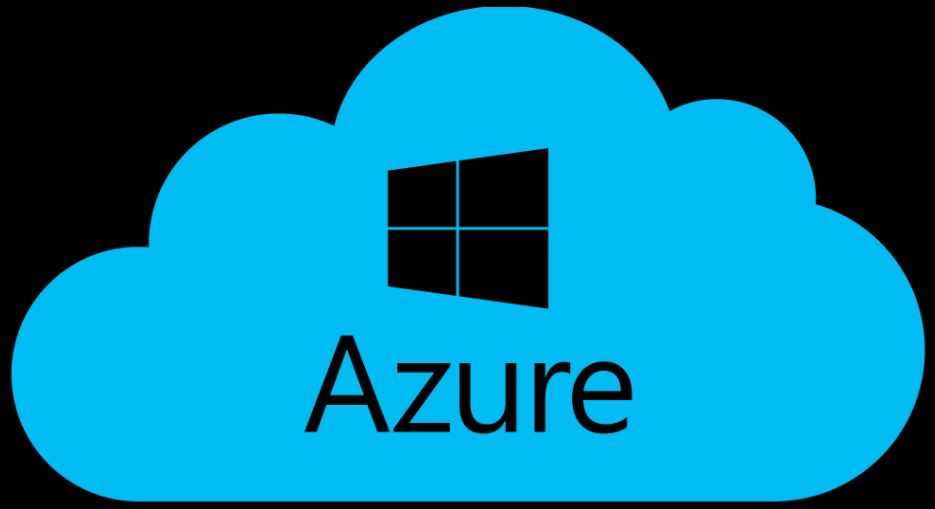


A Simple Application Architecture



Get Your Inspiration Within

THE COFFEE BREAK


Azure

Microsoft Azure Storage

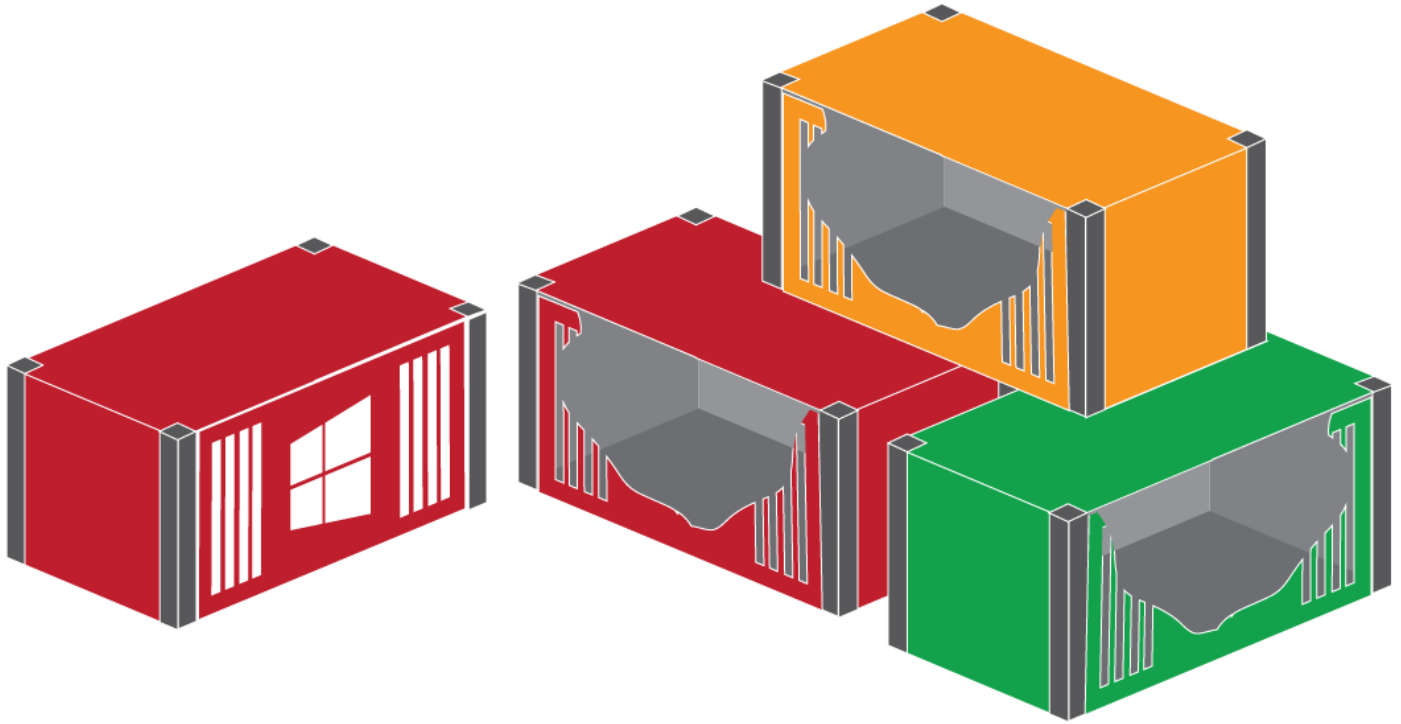
Storage Account

Manage Data

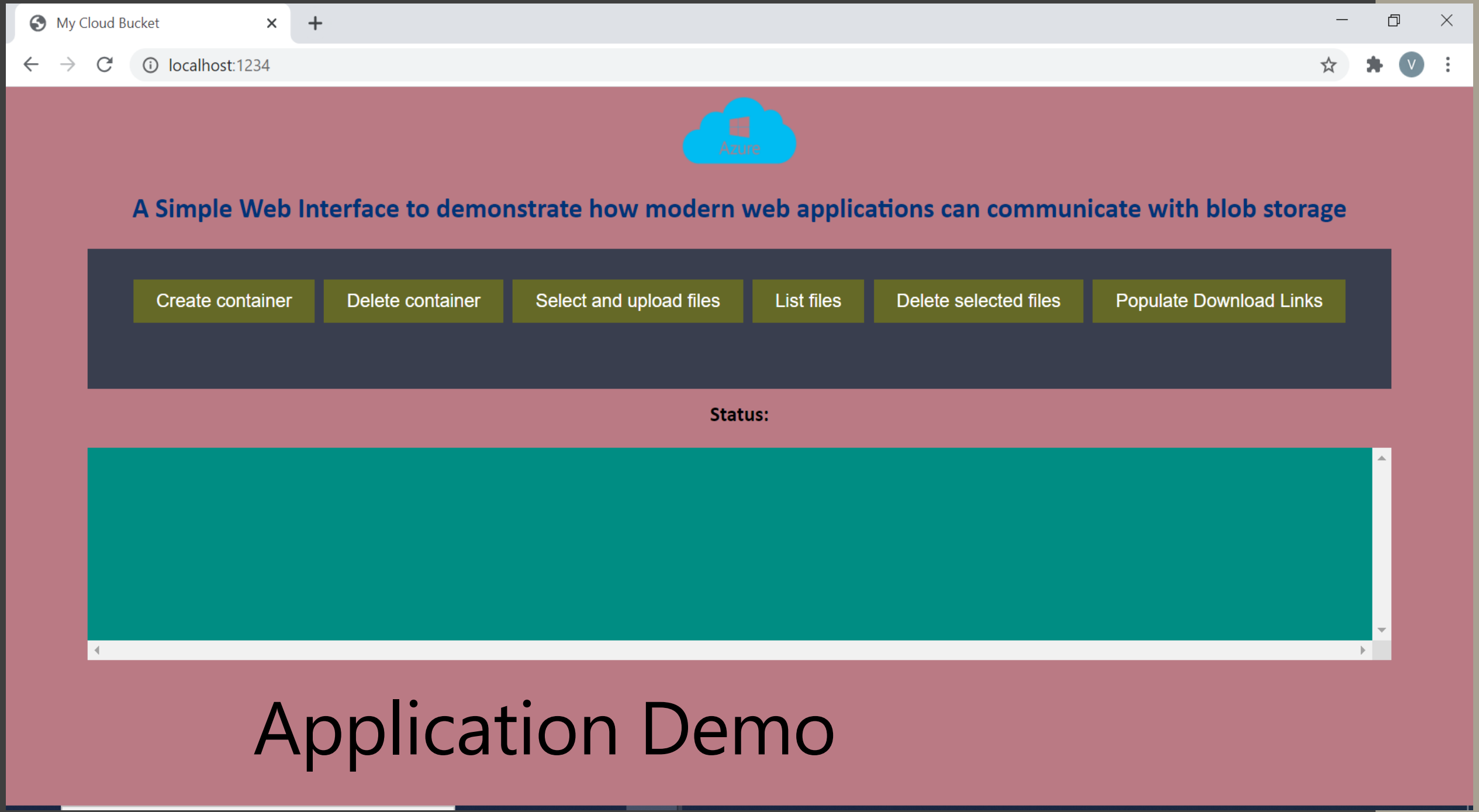
Data Security

Data Replication

Manage Access



An interesting Application demo to grab attention and connect the lessons to knowledge with real world



Application Demo

History [edit]

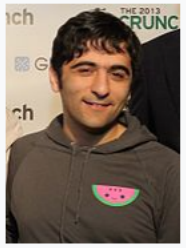
See also: Timeline of Dropbox

Dropbox founder Drew Houston conceived the Dropbox concept after repeatedly forgetting his USB flash drive while he was a student at MIT. In a 2009 "Meet the Team" post on the Dropbox blog, he wrote that existing services at the time "suffered problems with Internet latency, large files, bugs, or just made me think too much". He began making something for his personal use, but then realized that it could benefit others with the same problems.[16]

Houston founded Evenflow, Inc. in May 2007[17] as the company behind Dropbox, and shortly thereafter secured seed funding from Y Combinator.[18] Dropbox was officially launched at 2008's TechCrunch Disrupt, an annual technology conference.[19] Owing to trademark disputes between Proxy, Inc. and Evenflow, Dropbox's official domain name was "*get*dropbox.com" until October 2009, when it acquired its current domain, "dropbox.com".[19] In October 2009, Evenflow, Inc. was renamed to Dropbox, Inc.[17]

In an interview with *TechCrunch*'s "Founder Stories" in October 2011, Houston explained that a demo video was released during Dropbox's early days, with one viewer being Arash Ferdowsi. Ferdowsi was "so impressed" that they formed a partnership. In regards to competition, Houston stated that "It is easy for me to explain the idea, it is actually really hard to do it."[20]

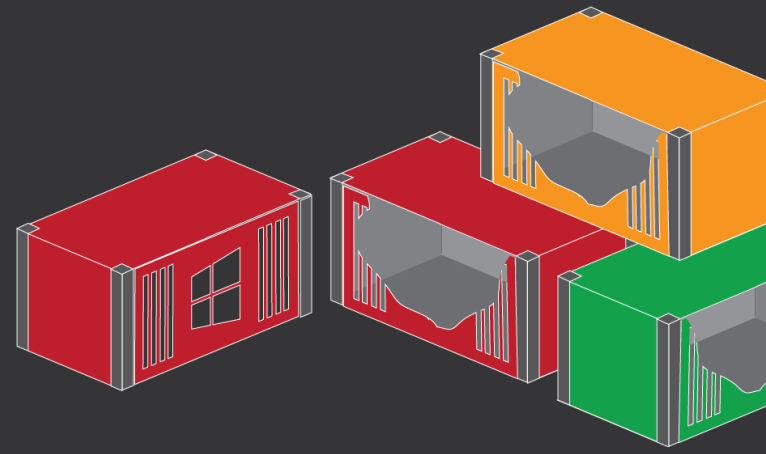
Dropbox founder Drew Houston



Dropbox founder Arash Ferdowsi

What is Azure Storage?

Azure Storage is the modern-day solution to all storage problems. Its storage capacity is limitless, virtually. Being a pay-as-you-go model, it gives you the flexibility of paying only for what you have used.



Priorities while selecting your storage

01

Enabling remote Work from Home

02

Securing your organization

03

Enabling business continuity & DR

04

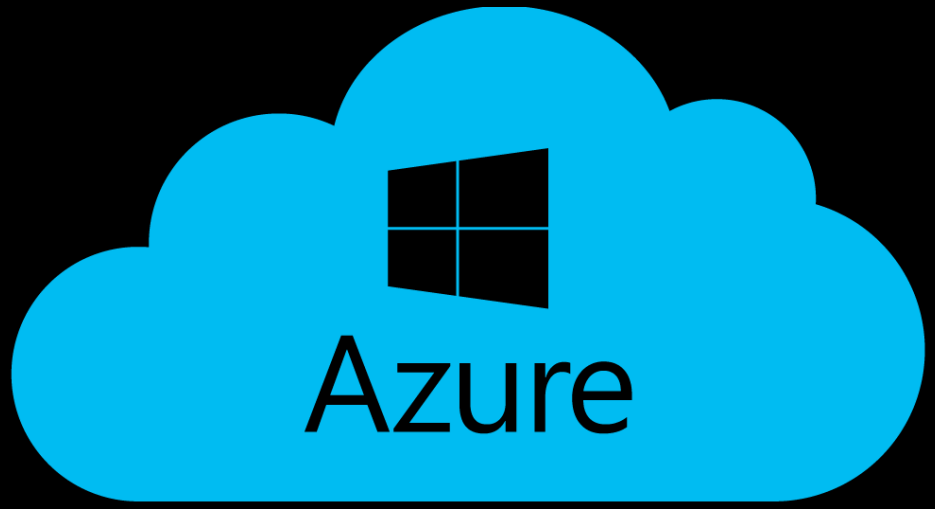
Accelerating migration to the cloud

05

Optimizing Cost

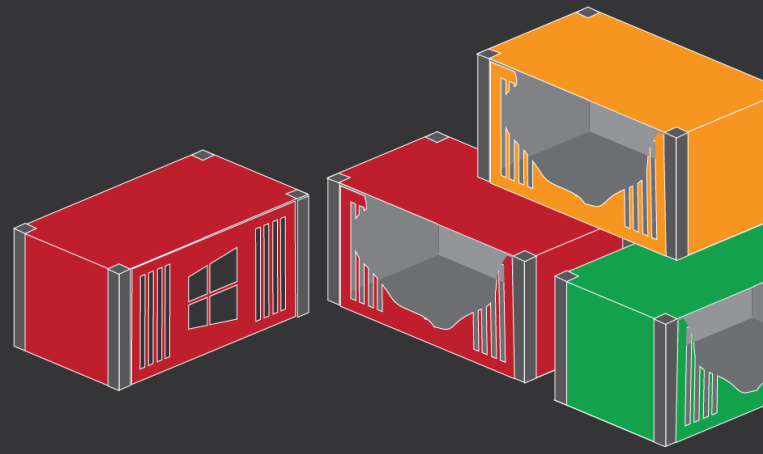
Why Azure Storage?

- ✓ Durable & High Available
- ✓ Secure
- ✓ Scalable
- ✓ Managed
- ✓ Accessible


Azure

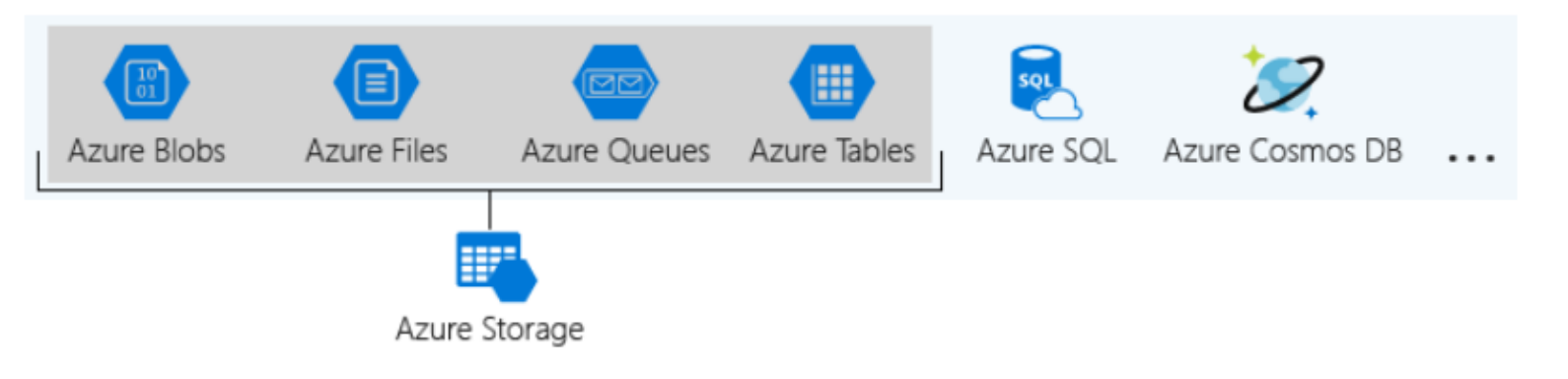
Azure Data Storage

Most organizations have diverse requirements for their cloud-hosted data. For example, storing data in a specific region, or needing separate billing for different data categories. Azure storage accounts let you formalize these types of policies and apply them to your Azure data.



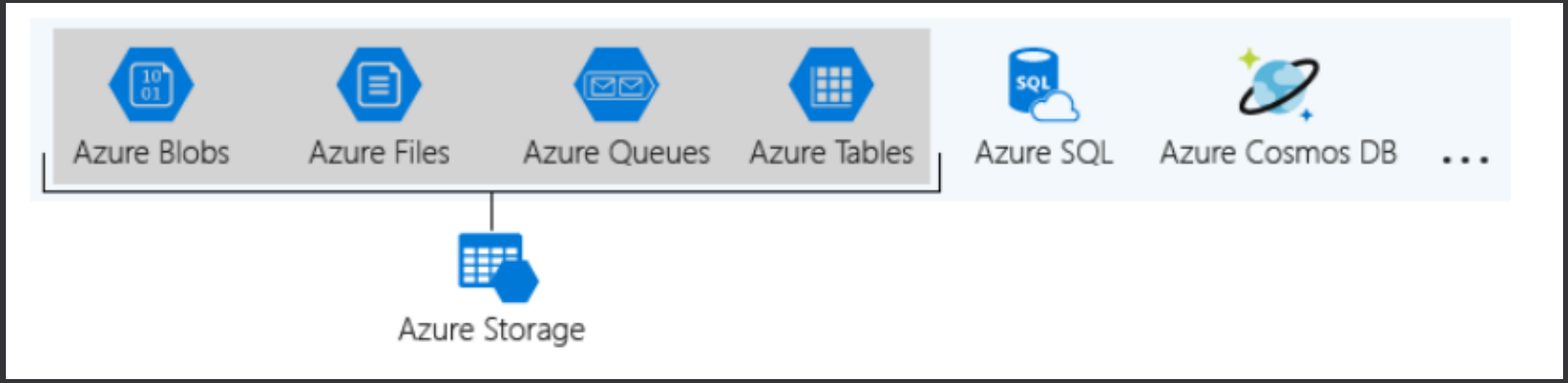
What is a storage account?

A storage account is a container that groups a set of Azure Storage services together.



Why storage account?

- Combining data services into a storage account lets you manage them as a group.
- The settings you specify when you create the account, or any that you change after creation, are applied to everything in the account.
- Deleting the storage account deletes all of the data stored inside it.



Microsoft Azure Storage

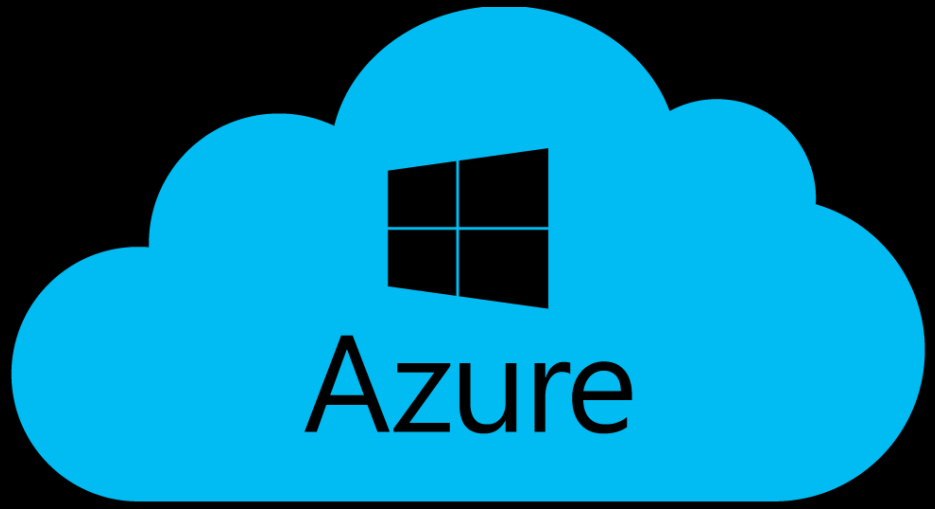
Storage Account

Manage Data

Data Security

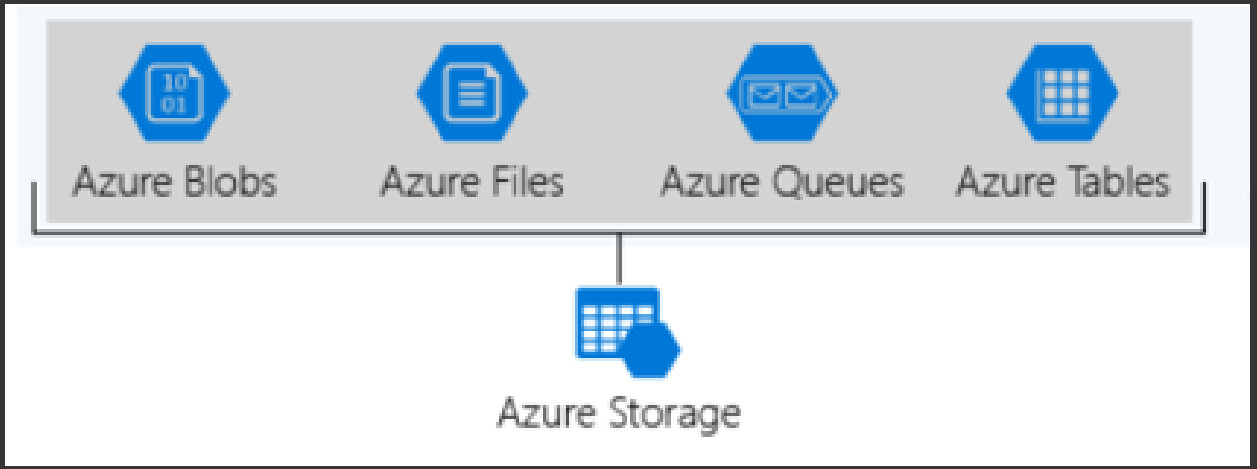
Data Replication

Manage Access

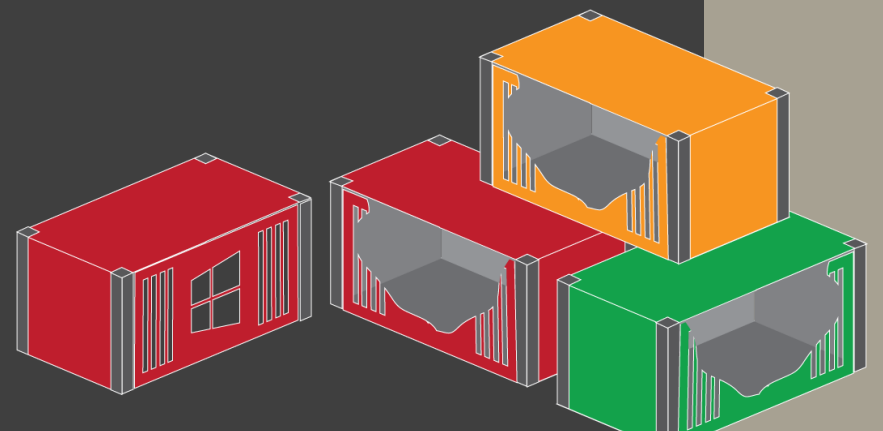

Azure

What is a storage account?

A storage account is a container that groups a set of Azure Storage services together.



How many storage accounts are needed?

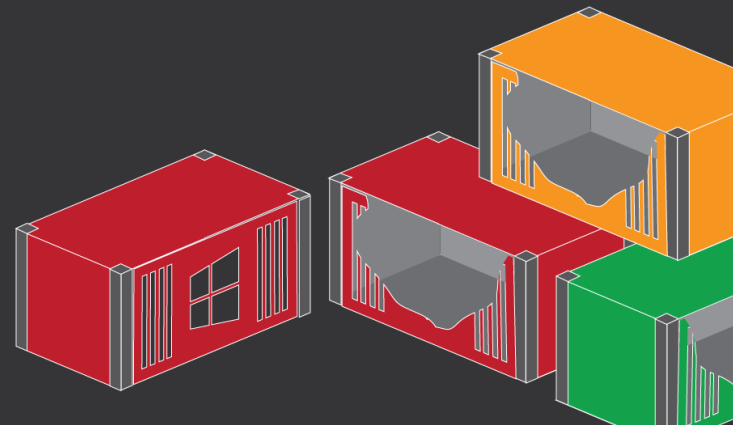


Azure Storage Account

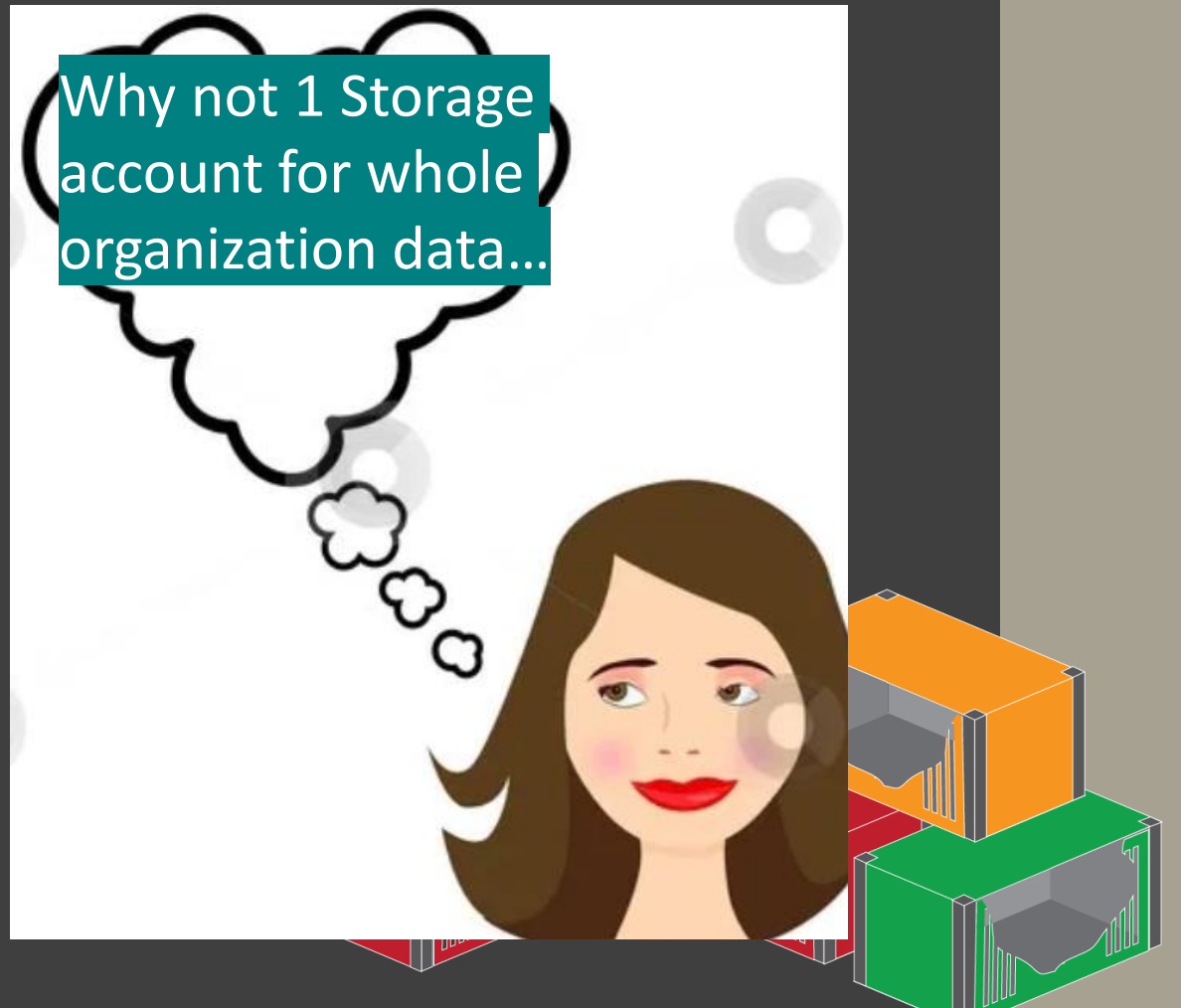
If we just create One storage account and store all our data inside it?

- How much cost customer ABC added on project's storage cost in the last quarter?

- Give full access to user XYZ for his project1_container but make sure he doesn't get any access to any other data.



How many storage accounts?



Azure Storage Account

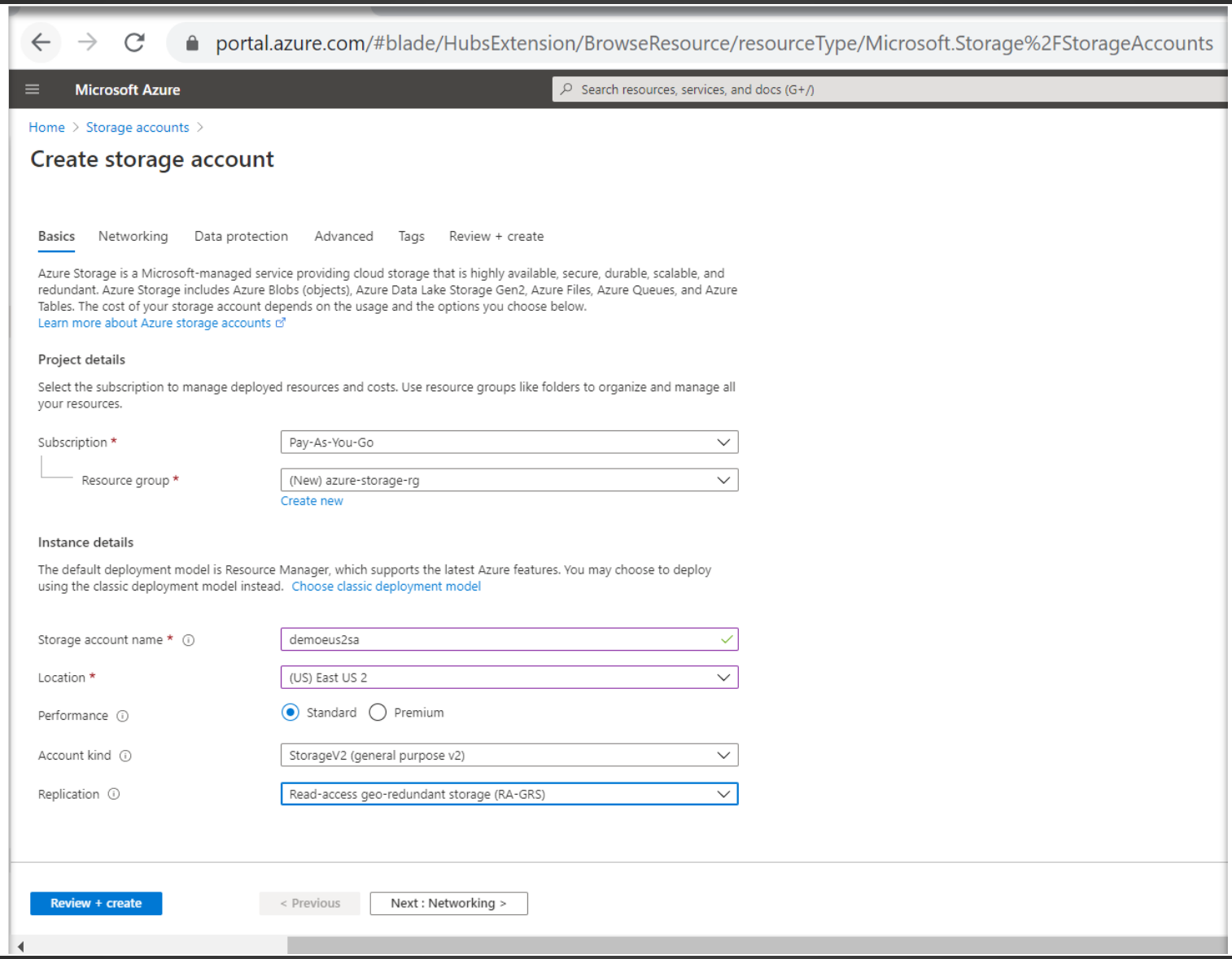
How many storage accounts do you need, depends on

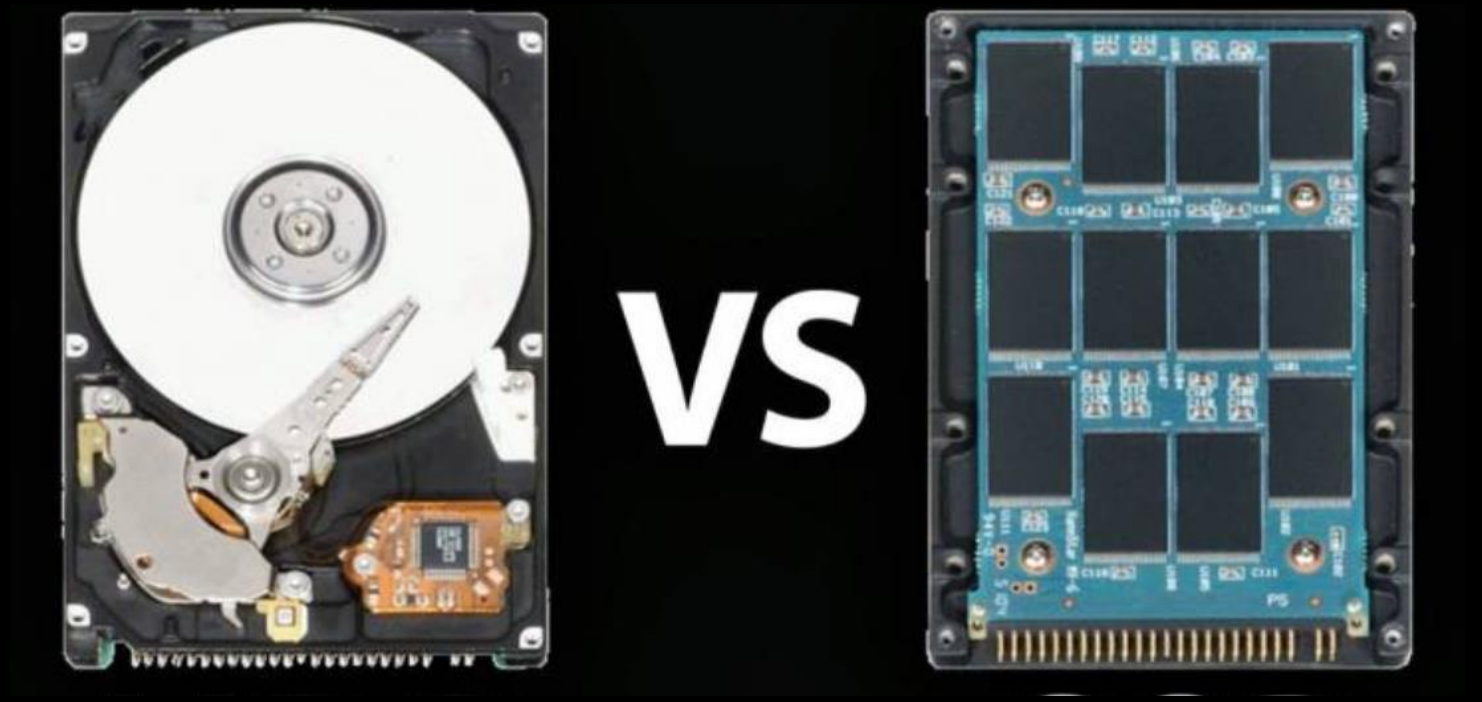
- Data diversity
- Cost sensitivity
- Management overhead

And they reached to solution, both are different though ☺

Core Storage Services

- ✓ Blobs
- ✓ Files
- ✓ Queue
- ✓ Table
- ✓ Disk


portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Storage%2FStorageAccounts
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Storage accounts >
Create storage account
Basics
Networking
Data protection
Advanced
Tags
Review + create
Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below.
Learn more about Azure storage accounts
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Pay-As-You-Go
Resource group *
(New) azure-storage-rg
Create new
Instance details
The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. Choose classic deployment model
Storage account name *
demoeus2sa
Location *
(US) East US 2
Performance
Standard
Premium
Account kind
StorageV2 (general purpose v2)
Replication
Read-access geo-redundant storage (RA-GRS)
Review + create
< Previous
Next : Networking >



Storage Account Performance

Standard storage accounts are backed by magnetic drives and provide the lowest cost per GB. They're best for applications that require bulk storage or where data is accessed infrequently.

Premium storage accounts are backed by solid state drives and offer consistent, low-latency performance. They can only be used with Azure virtual machine disks, and are best for I/O-intensive applications, like databases.

Account Kind

Storage account kind is a set of policies that determine which data services you can include in the account and the pricing of those services. There are three kinds of storage accounts:

- StorageV2 (general purpose v2): the current offering that supports all storage types and all of the latest features
- Storage (general purpose v1): a legacy kind that supports all storage types but may not support all features
- Blob storage: a legacy kind that allows only block blobs and append blobs

Microsoft recommends that you use the General-purpose v2 option for new storage accounts.

Account Kind

Storage account type	Supported services	Supported performance tiers	Supported access tiers	Replication options	Deployment model [1]	Encryption [2]
General-purpose V2	Blob, File, Queue, Table, Disk, and Data Lake Gen2 [6]	Standard, Premium [5]	Hot, Cool, Archive [3]	LRS, GRS, RA-GRS, ZRS, GZRS (preview), RA-GZRS (preview) [4]	Resource Manager	Encrypted
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium [5]	N/A	LRS, GRS, RA-GRS	Resource Manager, Classic	Encrypted
BlockBlobStorage	Blob (block blobs and append blobs only)	Premium	N/A	LRS, ZRS [4]	Resource Manager	Encrypted
FileStorage	File only	Premium	N/A	LRS, ZRS [4]	Resource Manager	Encrypted
BlobStorage	Blob (block blobs and append blobs only)	Standard	Hot, Cool, Archive [3]	LRS, GRS, RA-GRS	Resource Manager	Encrypted

Home > Storage accounts >

Create storage account

Basics | Networking | Data protection | Advanced | Tags | Review + create

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method *

- (•) Public endpoint (all networks)
- ( ) Public endpoint (selected networks)
- ( ) Private endpoint

ⓘ All networks will be able to access this storage account.
Learn more about connectivity methods

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference * ⓘ

- (•) Microsoft network routing (default)
- ( ) Internet routing

Home > Storage accounts >

Create storage account

Basics | Networking | **Data protection** | Advanced | Tags | Review + create

Recovery

When point-in-time restore is enabled, versioning, blob change feed and blob soft delete are also enabled. The retention periods for each of these features must be greater than that of point-in-time restore, if applicable. Learn more

☑ **Turn on point-in-time restore for containers**

Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. Learn more

Set the maximum restore point (days ago) ⓘ 6

☑ **Turn on soft delete for blobs**

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Learn more

Keep deleted blobs for (in days) ⓘ 7

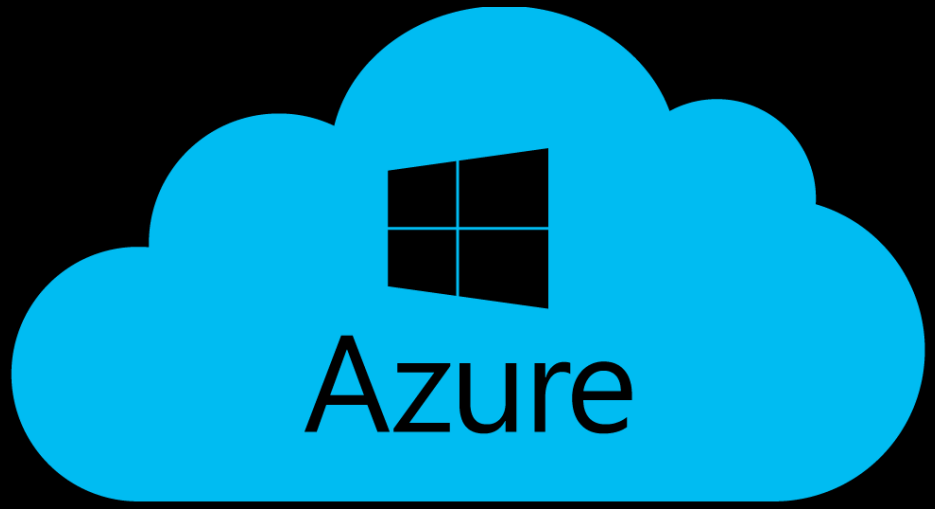
☐ **Turn on soft delete for containers**

Soft delete enables you to recover containers that were previously marked for deletion. Learn more

ⓘ **Sign up is required on a per-subscription basis to use container soft delete.** Sign up for container soft delete

☐ **Turn on soft delete for file shares**

Soft delete enables you to recover file shares that were previously marked for deletion. Learn more


Azure

Storage Account

Data Security

Manage Data

Manage Access

Data Replication

Microsoft Azure Storage

Problem Statement

You're an admin for a music streaming service. Your organization uses Azure Storage to store the music files.

Uptime is important to you and your users. If your audio files aren't available, you might lose subscribers to another service.

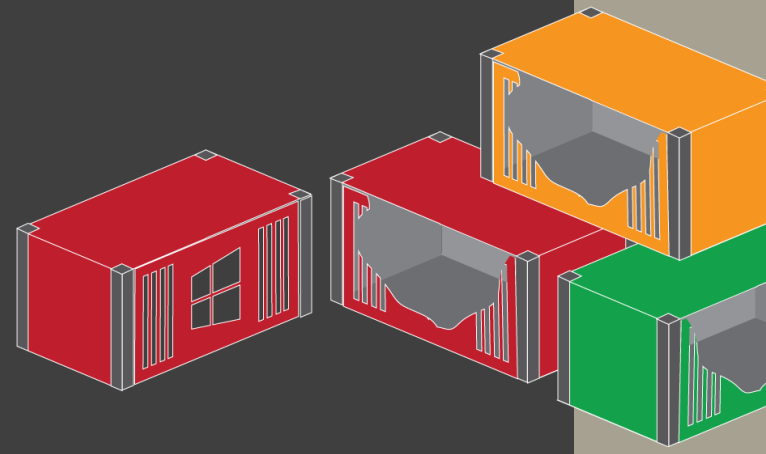
How do you plan to protect your organization from **region-wide outage and practice a storage failover.**


PROBLEM
SOLUTION

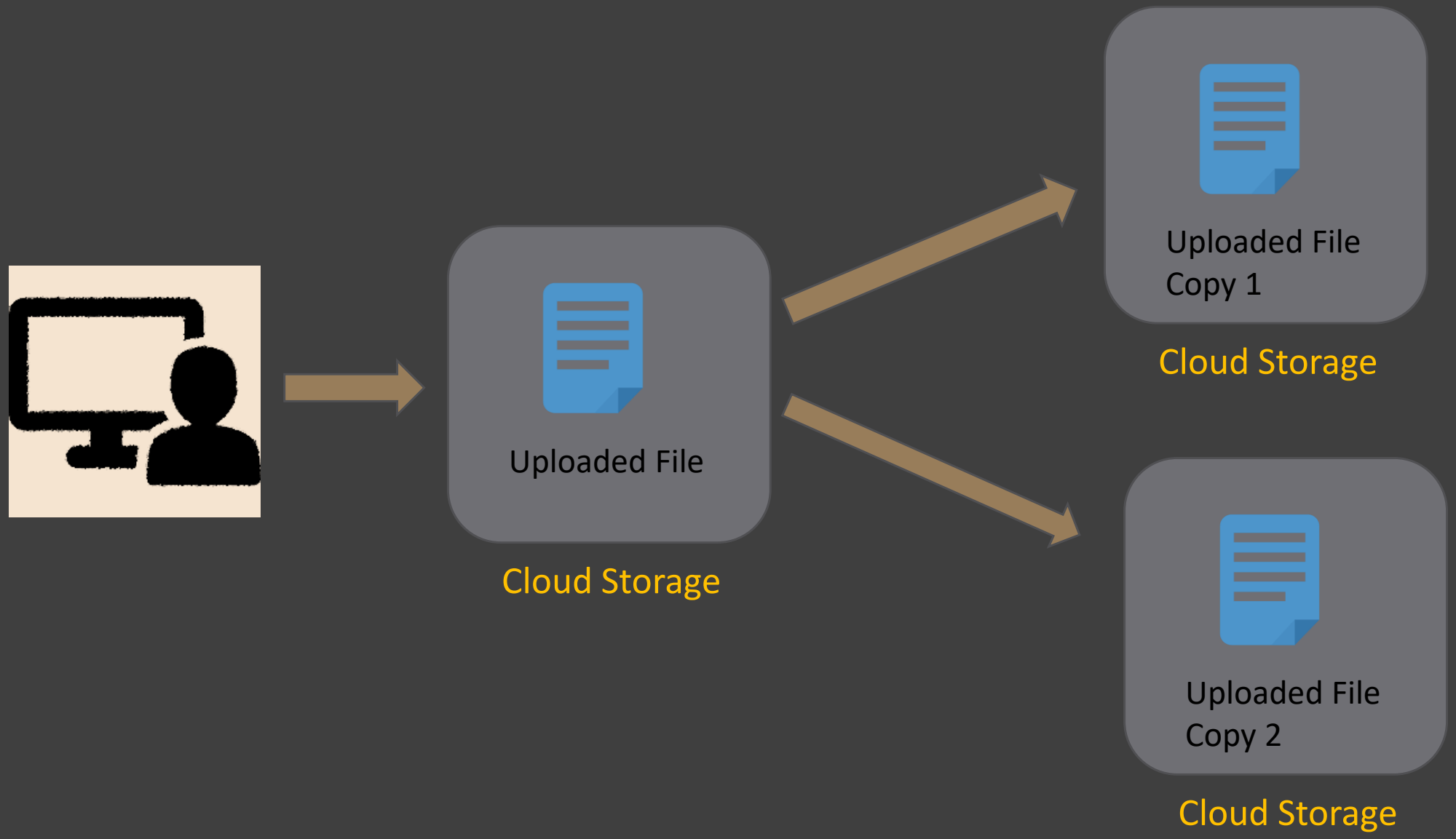
Azure Storage Redundancy

Azure Storage always stores multiple copies of your data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters.

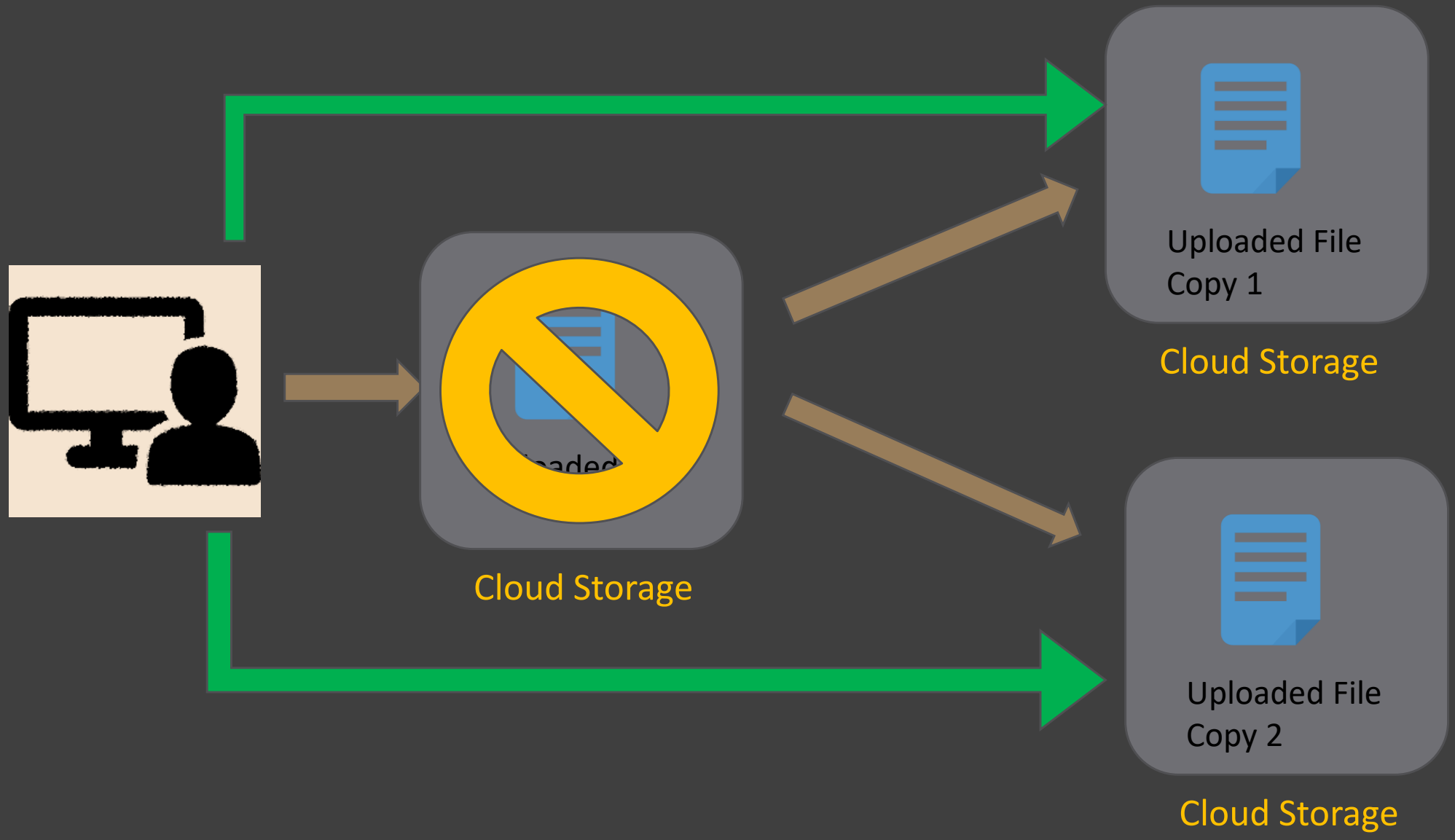
Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.



Azure Storage Redundancy



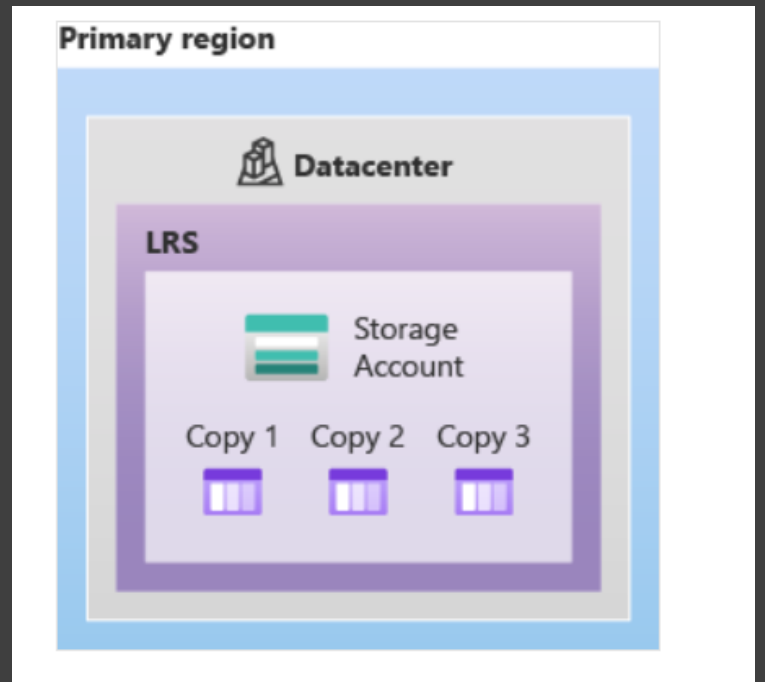
Azure Storage Redundancy



Azure Storage Redundancy

Locally redundant storage

Locally redundant storage (LRS) copies your data three times across separate racks of hardware in a datacenter, inside one region. Even if there's a hardware failure, or if maintenance work is happening in the datacenter, this replication type ensures data is available for use.



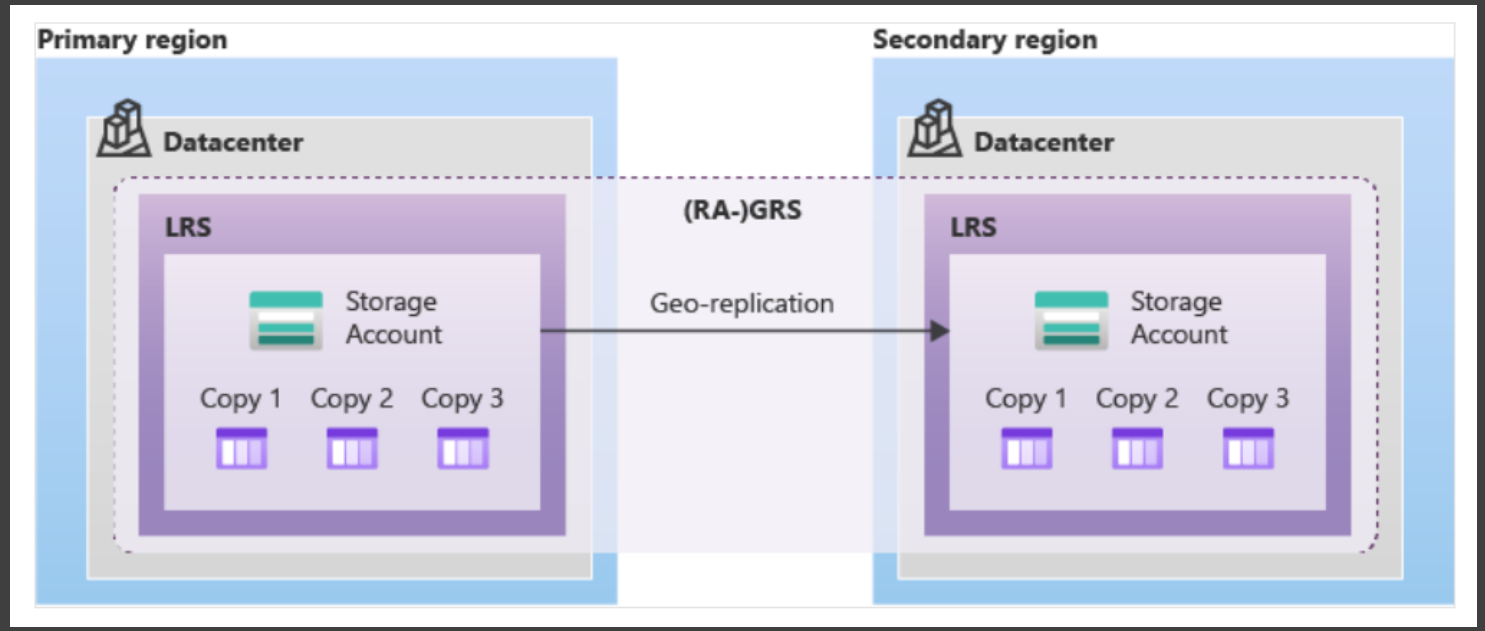
LRS doesn't protect you from a datacenter-wide outage. If the datacenter goes down, you could lose your data.

Azure Storage Redundancy

Geographically redundant storage

With geographically redundant storage (GRS), your data is copied three times within one region, and three times in a secondary region that's paired with it.

This way, if your primary region is experiencing an outage, your secondary region is available for use.



Azure Storage Redundancy

Read-access geo-redundant storage

With GRS, your secondary region isn't available for read access until the primary region fails.

If you want to read from the secondary region, even if the primary region hasn't failed, use RA-GRS for your replication type.

Azure Storage Redundancy

Zone-redundant storage

Zone-redundant storage (ZRS) copies your data in three storage clusters in a single region. Each cluster is in a different physical location and is considered as a single availability zone. Each cluster uses its own separate utilities for things like networking and power.

If one datacenter is experiencing outage, your data remains

accessible from another availability zone in the same Azure region.

Because all availability zones are in a single region, ZRS can't protect your data from a regional level outage

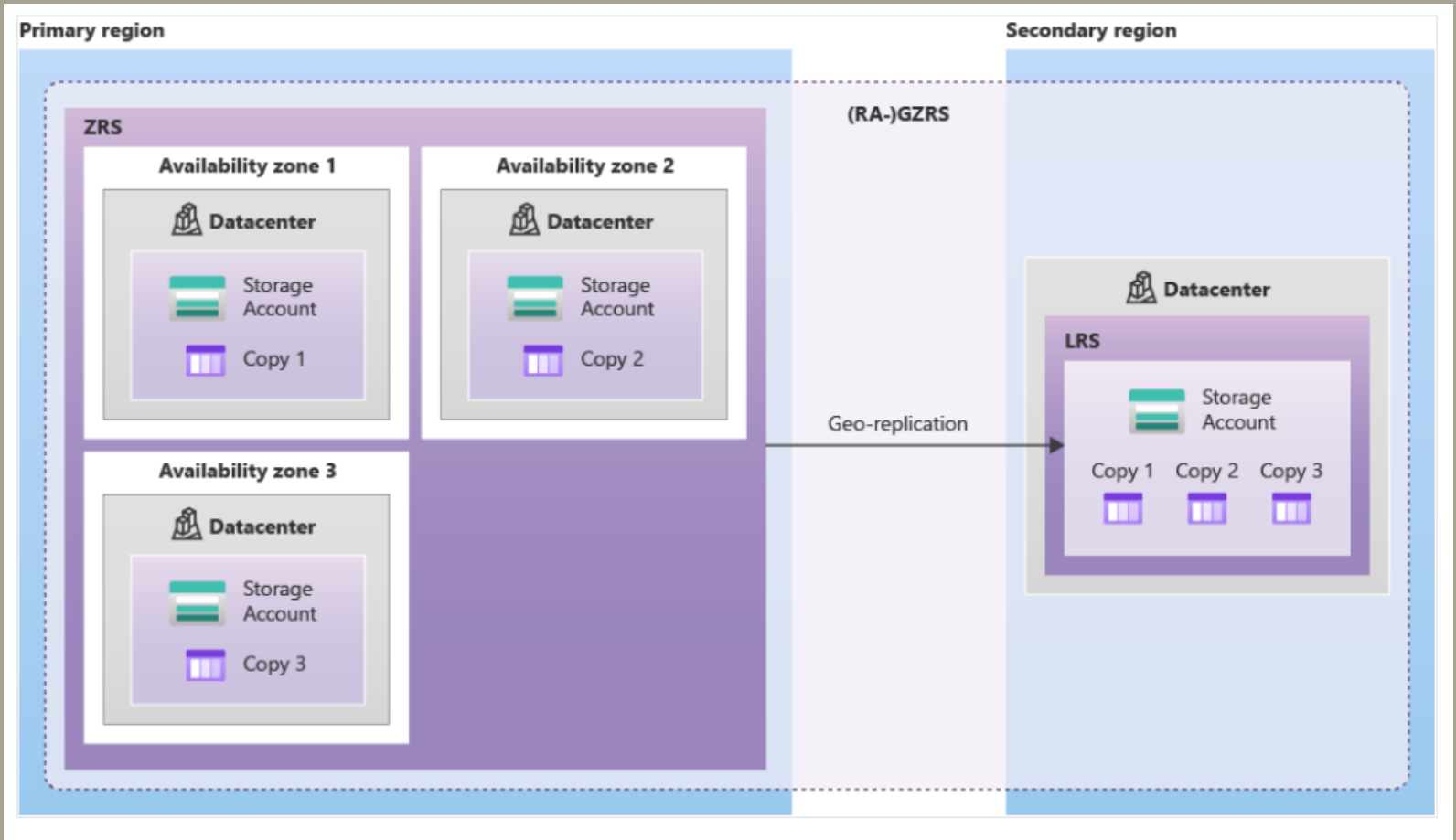
Zone-redundant storage

Azure Storage Redundancy

Geo-zone-redundant storage

Geo-zone-redundant storage (GZRS) combines the high availability benefits of ZRS with GRS. With this replication type, your data is copied across three availability zones in one region.

Data is also replicated three times to another secondary region that's paired with it. This way, your zone-redundant data is also secure from regional level outage.



Geo-zone Redundant Storage

Azure Storage Redundancy

Read-access geo-zone-redundant storage

Read-access geo-zone-redundant storage (RA-GZRS) uses the same replication method as GZRS but lets you read from the secondary region. If you want to read the data that's replicated to the secondary region, even if your primary isn't experiencing downtime, use RA-GZRS for your replication type.

Azure Storage Redundancy

Paired regions

A paired region is where an Azure region is paired with another in the same geographical location to protect against regional outage. Paired regions are used with GRS and GZRS replication types.

Use cases for each replication type

The following table summarizes how many copies you get with each replication type and when you should use it.

Replication type	Copies	Use case
LRS	3	Data remains highly available, but for compliance reasons, isn't allowed to leave the local datacenter.
GRS	6	App has access to the data, even if an entire region has an outage.
RA-GRS	6	App reads from multiple geographical locations, so you can serve users from a location that's closer to them.
ZRS	3	Need redundancy in multiple physical locations, but because of compliance, data isn't allowed to leave a region.
GZRS	6	App can access data, even if the primary region has failed, and your secondary region has a datacenter that's experiencing an outage. But you don't want to read from the secondary region unless the primary region is down.
RA-GZRS	6	Regularly read data from your secondary region, perhaps to serve users from a location closer to them, even if a datacenter is up in your primary region.

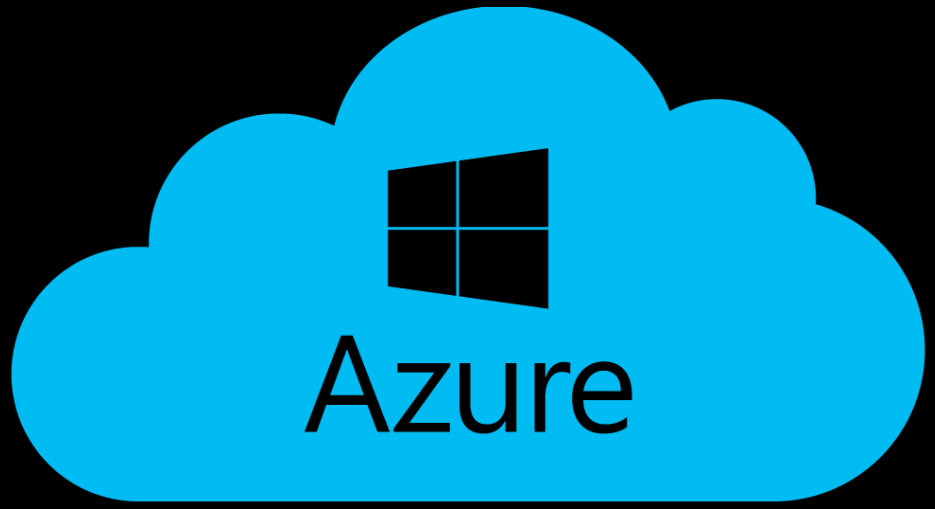
Azure Storage Redundancy

Locally redundant storage (LRS)	Keeps multiple copies of your data in one data center. It provides 99.99% (eleven 9s) durability over a given year.
Zone redundant storage (ZRS)	Keeps multiple copies of your data in different data centers in different regions. It provides 99.99% (twelve 9s) durability.
Geo-redundant storage (GRS)	Holds multiple copies of your data in one region and replicates the data to the second region, asynchronously. The durability is sixteen 9s.
Read-access geo-redundant storage (RA-GRS)	Allows read access from the second region, which is used for GRS, and the read availability is 99.99% and durability is sixteen 9s.

Azure Storage Redundancy

Exercise to check your knowledge

https://docs.microsoft.com/en-us/learn/modules/provide-disaster-recovery-replicate-storage-data/6-knowledge-check


Azure

Microsoft Azure Storage

Storage Account

Manage Data

Data Security

Data Replication

Manage Access

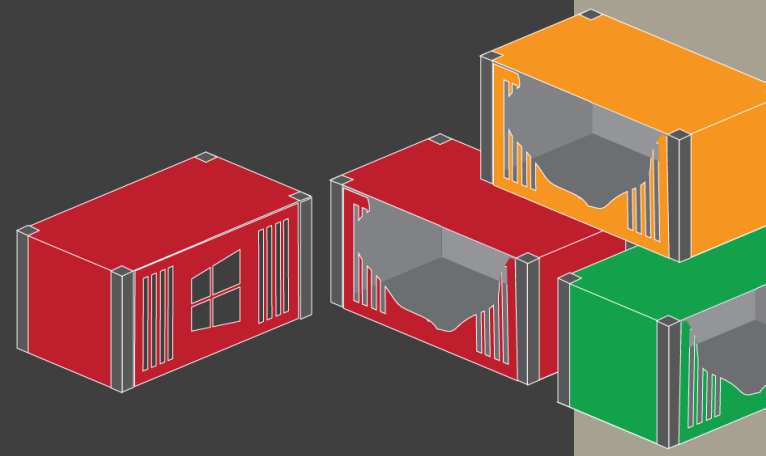
Storage Account Keys

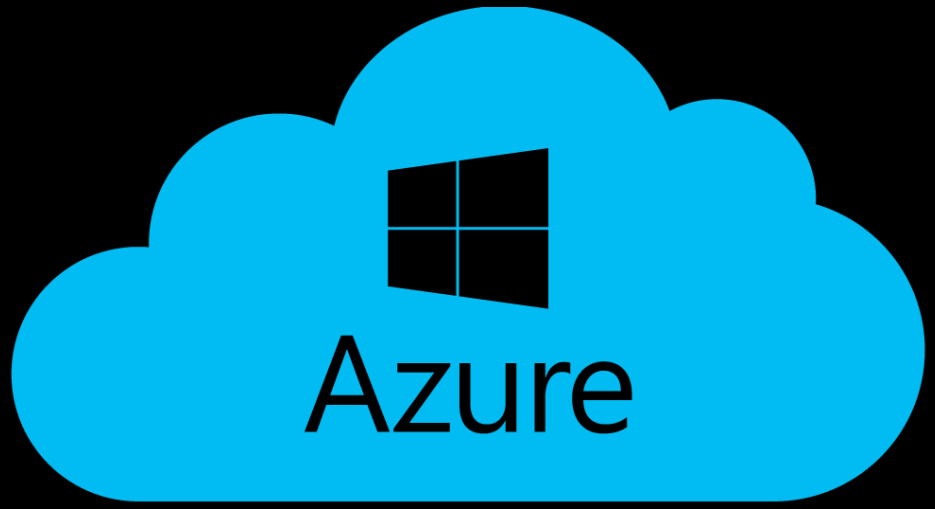
Shared keys are called storage account keys. Azure creates two of these keys (primary and secondary) for each storage account you create. The keys give access to everything in the account.

- For security reasons, you might regenerate keys periodically.
- If someone hacks into an application and gets the key that was hard-coded or saved in a configuration file, regenerate the key. The compromised key can give the hacker full access to your storage account.
- If your team is using a Storage Explorer application that keeps the storage account key, and one of the team members leaves, regenerate the key. Otherwise, the application will continue to work, giving the former team member access to your storage account.

Shared Access Signatures

For untrusted clients, use a shared access signature (SAS). A shared access signature is a string that contains a security token that can be attached to a URI. Use a shared access signature to delegate access to storage objects and specify constraints, such as the permissions and the time range of access




Azure

Blob Storage

- Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data. It has no restrictions on the kinds of data it can hold.

- You can use Blob Storage to expose data publicly to the world, or to store application data privately.

- The blob service includes:
  - Blobs, which are the data objects of any type
  - Containers, which wrap multiple blobs together
  - Azure storage account, which contains all of your Azure storage data objects

Blob Storage

Blob storage is ideal for:

- 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, and archiving
- Storing data for analysis by an on-premises or Azure-hosted service

Blob Categories

Block blobs: These are blobs that are intended to store discrete objects such as images, log files and more. Block blobs can store data up to ~5TB, or 50,000 blocks of up to 100MB each.

Page blobs: These are optimized for random read and write operations and can grow up to 8TB in size. Within the page blob category, Azure offers two types of storage: standard and premium. The latter is the most ideal for virtual machine (VM) storage disks (including the operating system disk).

Append Blobs: Optimized for append scenarios like log storage, append blogs are composed of several blocks of different sizes — up to a maximum of 4MB. Each append blob can hold up to 50,000 blocks, therefore allowing each append blob to grow up to 200GB.

Blob Storage Tiers

Hot Access Tier: Out of the three options, the hot access tier is the most optimized for data that is accessed frequently. It offers the lowest access (read-write) cost, but the highest storage cost.

Cool Access Tier: This option is better suited for use cases where data will remain stored for at least 30 days and is not accessed frequently. Compared to hot access tiers, this tier offers lower storage costs and higher access costs.

Archive Access Tier: Archive storage is designed for data that doesn’t need to be accessed immediately. This tier offers higher data retrieval costs, and also higher data access latency. It is designed for use cases where data will be stored for more than 180 days and is rarely accessed.

https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

/azure/security/fundamentals/physical-security

Physical security

Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft understands the importance of protecting your data, and is committed to helping secure the datacenters that contain your data. We have an entire division at Microsoft devoted to designing, building, and operating the physical facilities supporting Azure. This team is invested in maintaining state-of-the-art physical security.

Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor. Layers of physical security are:

- **Access request and approval.** You must request access prior to arriving at the datacenter. You're required to provide a valid business justification for your visit, such as compliance or auditing purposes. All requests are approved on a need-to-access basis by Microsoft employees. A need-to-access basis helps keep the number of individuals needed to complete a task in the datacenters to the bare minimum. After Microsoft grants permission, an individual only has access to the discrete area of the datacenter required, based on the approved business justification. Permissions are limited to a certain period of time, and then expire.

- **Facility's perimeter.** When you arrive at a datacenter, you're required to go through a well-defined access point. Typically, tall fences made of steel and concrete encompass every inch of the perimeter. There are cameras around the datacenters, with a security team monitoring their videos at all times.

- **Building entrance.** The datacenter entrance is staffed with professional security officers who have undergone rigorous training and background checks. These security officers also routinely patrol the datacenter, and monitor the videos of cameras inside the datacenter at all times.

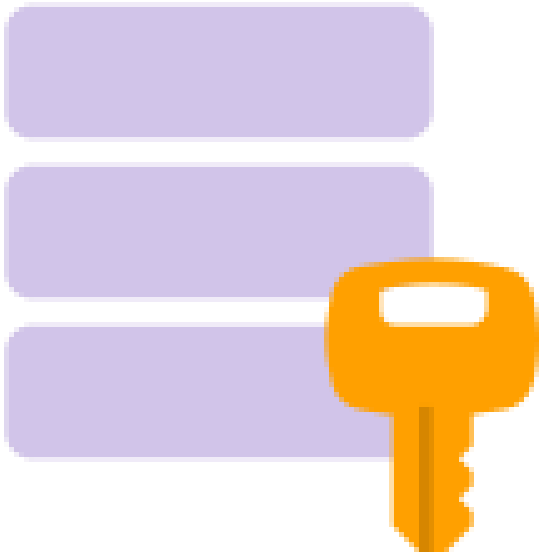
- **Inside the building.** After you enter the building, you must pass two-factor authentication with biometrics to continue moving through the datacenter. If your identity is validated, you can enter only the portion of the datacenter that you have approved access to. You can stay there only for the duration of the time approved.

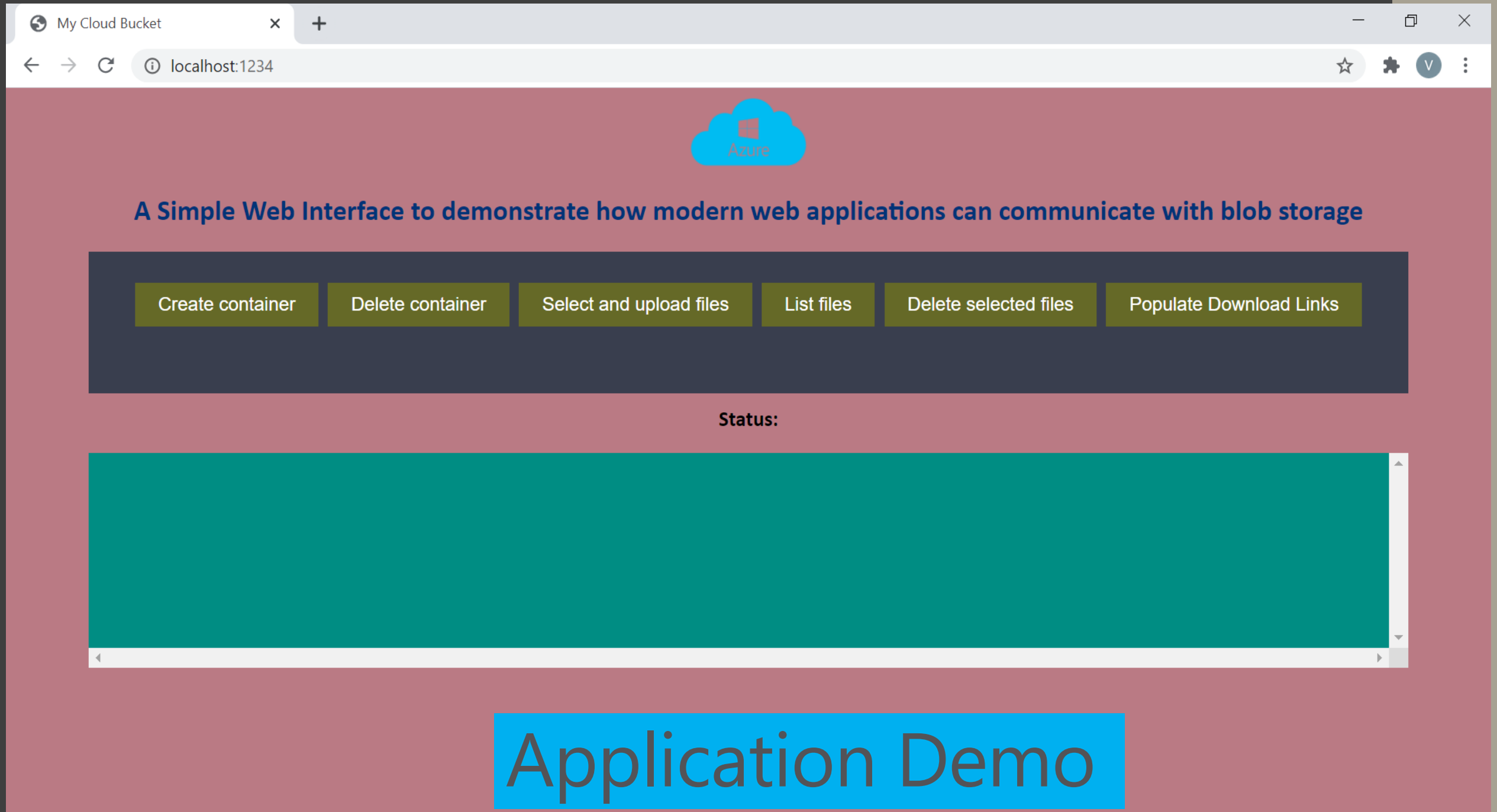
- **Datacenter floor.** You are only allowed onto the floor that you're approved to enter. You are required to pass a full body metal detection screening. To reduce the risk of unauthorized data entering or leaving the datacenter without our knowledge, only approved devices can make their way into the datacenter floor. Additionally, video cameras monitor the front and back of every server rack. When you exit the datacenter floor, you again must pass through full body metal detection screening. To leave the datacenter, you're required to pass through an additional security scan.

Microsoft requires visitors to surrender badges upon departure from any Microsoft facility.

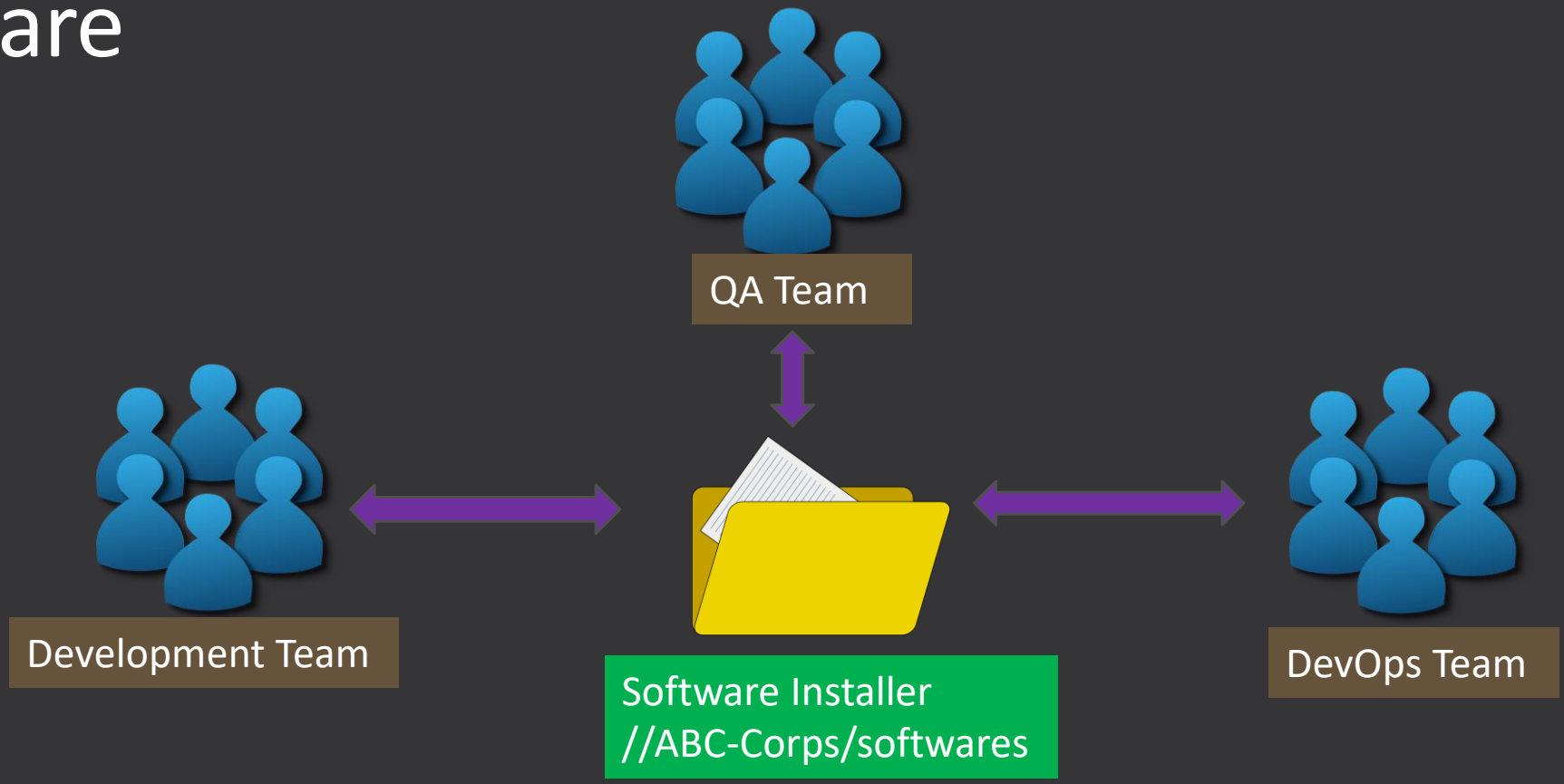
Encryption at Rest

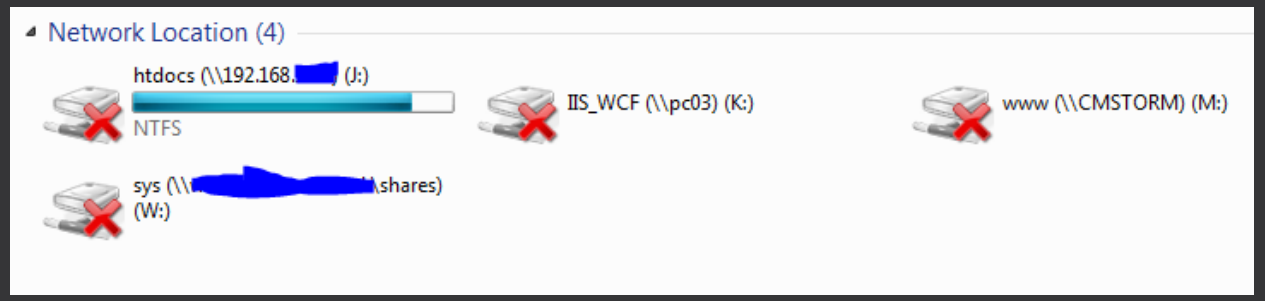
- All data written to Azure Storage is automatically encrypted by **Storage Service Encryption** (SSE)
- SSE automatically encrypts data when writing it to Azure Storage.
- When you read data from Azure Storage, Azure Storage decrypts the data before returning it.
- This process incurs no additional charges and doesn't degrade performance. It can't be disabled.




My Cloud Bucket
localhost:1234
Azure
A Simple Web Interface to demonstrate how modern web applications can communicate with blob storage
Create container
Delete container
Select and upload files
List files
Delete selected files
Populate Download Links
Status:
Application Demo

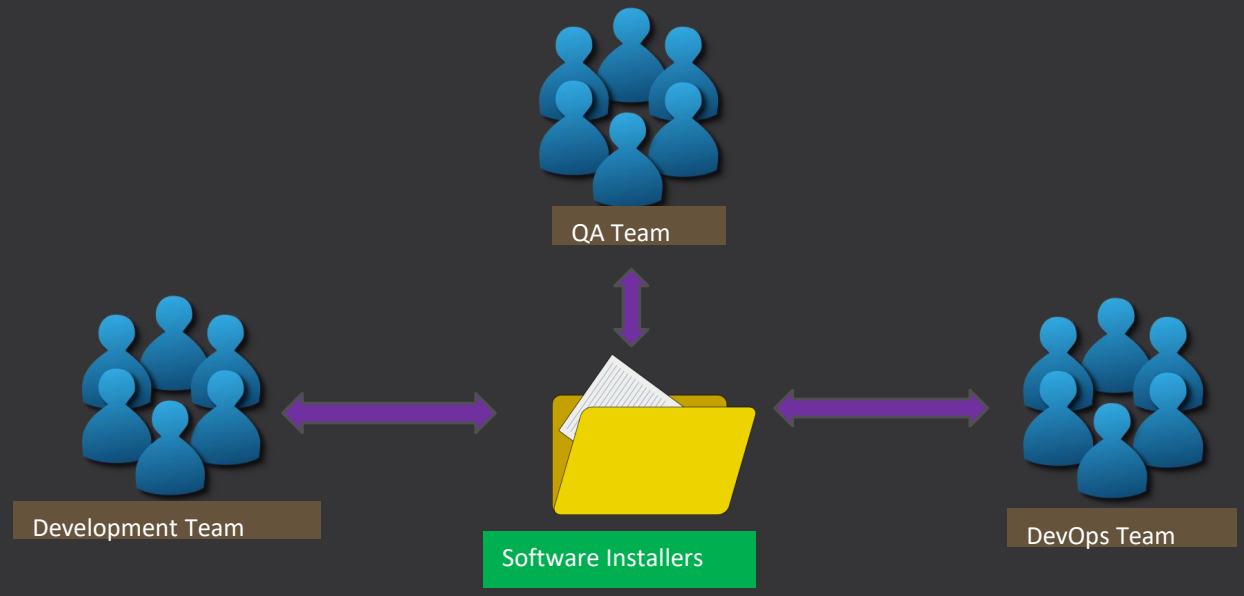
File Share





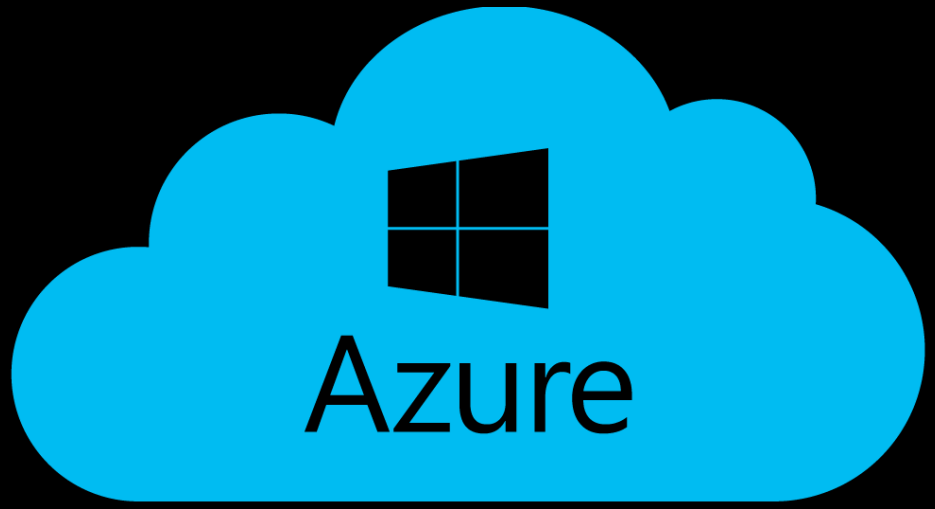
Azure Files

Azure Files provides a cloud-based file share for storing and sharing files. You then access these files from applications hosted in Azure App Service, an Azure VM, or an on-premises machine.



Azure Files

- Azure Files stores and shares file access between applications and systems in a secure and failure-resilient manner.
- Azure Files enables you to set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol.
- Multiple VMs can share the same files with both read and write access.
- One can access the files from anywhere in the world using a URL that points to the file and includes a shared access signature (SAS) token.


Azure

How to mount Azure File Share

Azure Files

File shares can be used for many **common scenarios**:

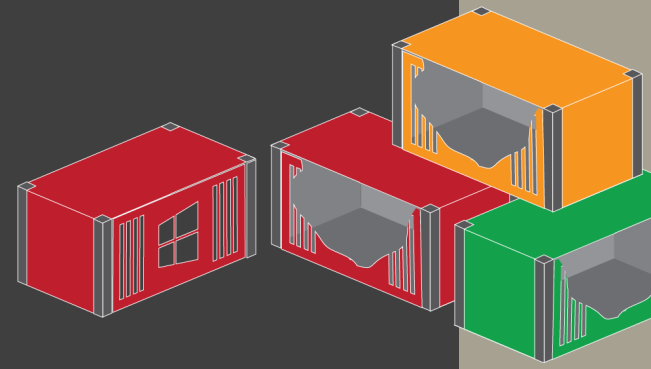
- Many on-premises applications use file shares. This feature makes it easier to migrate those applications that share data to Azure.
- Configuration files can be stored on a file share and accessed from multiple VMs.
- Resource logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analyzed later.

Azure Files – Storage Tiers

To allow you to tailor your shares to the performance and price requirements of your scenario, Azure Files offers four different tiers :

Premium: Premium file shares are backed by solid-state drives (SSDs) and provide consistent high performance and low latency.

Transaction optimized: Transaction optimized file shares enable transaction heavy workloads that don't need the latency offered by premium file shares.



Hot: Hot file shares offer storage optimized for general purpose file sharing scenarios such as team shares. This uses standard storage hardware backed by HDDs.

Cool: Cool file shares offer cost-efficient storage optimized for online archive storage scenarios. This uses standard storage hardware backed by HDDs.

Queue Storage

The Azure Queue service is used to store and retrieve messages. Queue messages can be up to 64 KB in size, and a queue can contain millions of messages. Queues are generally used to store lists of messages to be processed asynchronously.

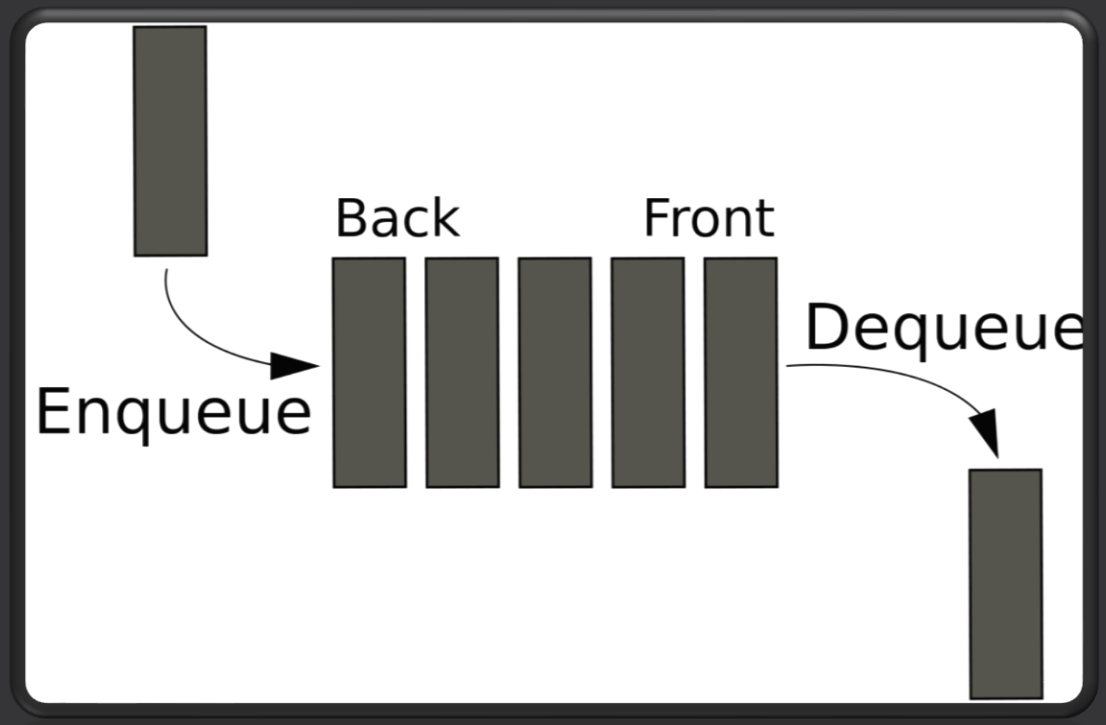


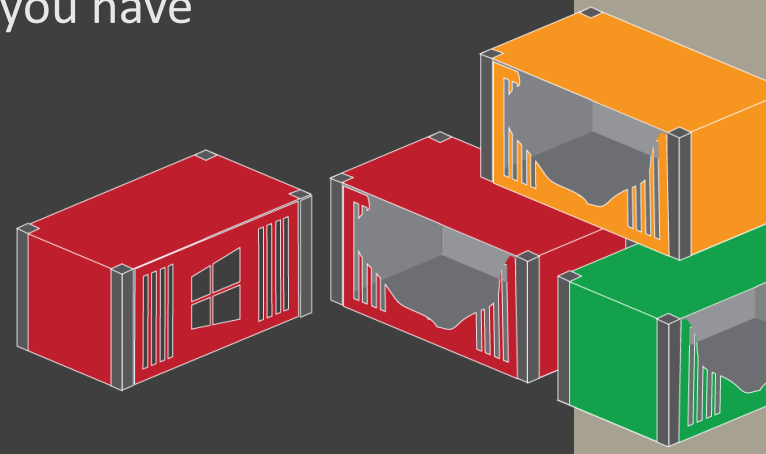
Table Storage

Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schema-less design. Because Table storage is schema-less, it's easy to adapt your data as the needs of your application evolve.

Disk storage

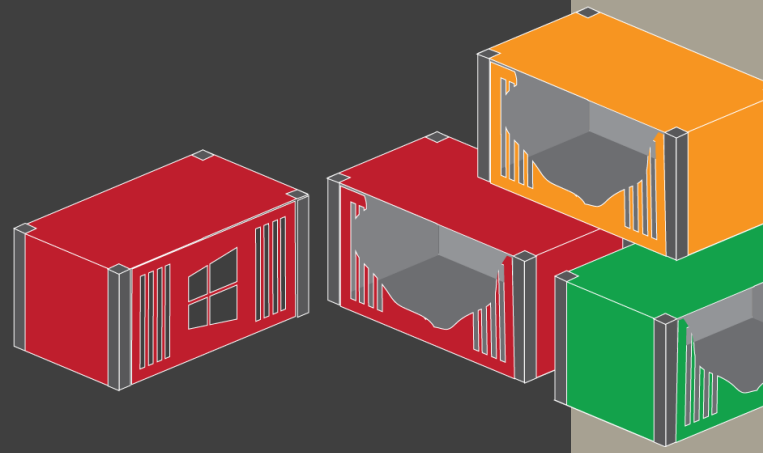
An Azure managed disk is a virtual hard disk (VHD). You can think of it like a physical disk in an on-premises server but, virtualized. Azure-managed disks are stored as page blobs, which are a random IO storage object in Azure.

We call a managed disk 'managed' because it is an abstraction over page blobs, blob containers, and Azure storage accounts. With managed disks, all you have to do is provision the disk, and Azure takes care of the rest.



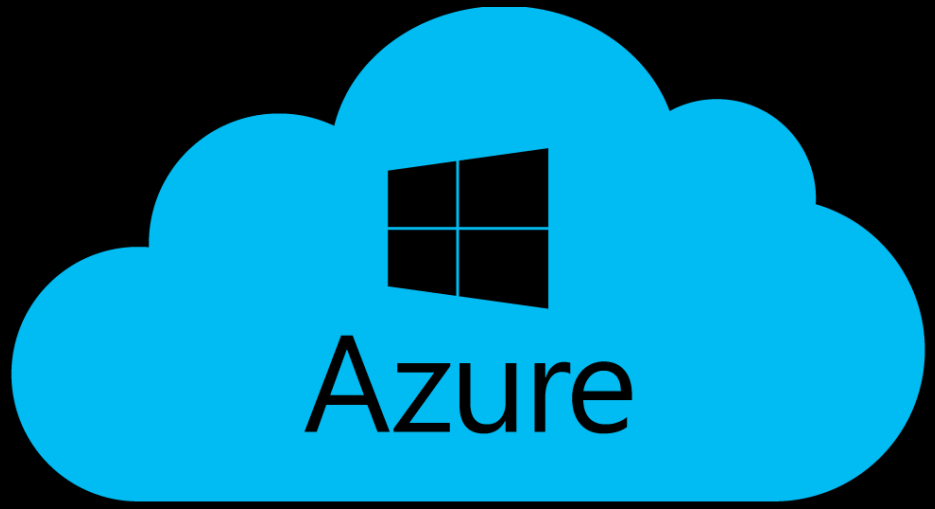
Disk storage

- ✓ Disk storage provides disks for virtual machines, applications, and other services to access and use as they need
- ✓ A disk can be attached to only 1 VM at a time
- ✓ **Persistent, highly-secure, cost-effective SSD option**
- ✓ lift and shift of applications that read and write data to persistent disks



Different ways to connect to your storage account

- Add resources by using Azure Active Directory (Azure AD)
- Use a connection string
- Use a shared access signature URI
- Use a name and key
- Attach to a local emulator
- Attach to Azure Cosmos DB through a connection string
- Attach to Azure Data Lake by using a URI


Azure

PowerShell interaction with Azure Storage

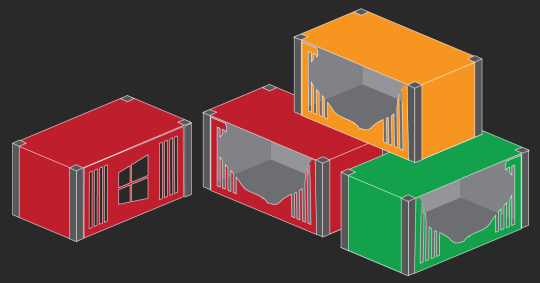
Agenda:

- Basic of Az.Storage module
- Create a new storage account using PowerShell
- Storage Context
- Operations related to Container
- Operations related to Blobs
- Perform Cleanup

Download and install Az module in your PowerShell

```
Install-Module -Name Az -AllowClobber
```

AzCopy



AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

1.) Download & extract azcopy

2.) Set Environment Variables

3.) azcopy login --tenant-id <<your_tenant_id>>

4.) Perform Various Copy Operations

Azure Storage Explorer

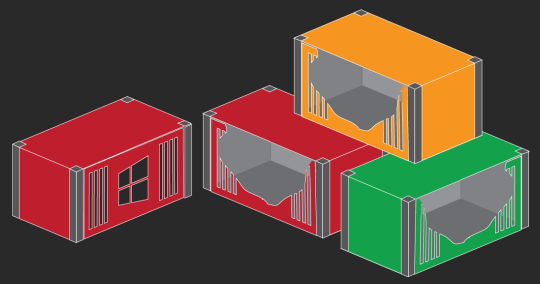
Storage Explorer is a GUI application developed by Microsoft to simplify access to, and the management of, data stored in Azure storage accounts. Storage Explorer is available on Windows, macOS, and Linux.

Some of the benefits of using Storage Explorer are:

- It's easy to connect to and manage multiple storage accounts.
- The interface lets you connect to Azure Cosmos DB and Data Lake.
- You can also use the interface to update and view entities in your storage accounts.
- Storage Explorer is free to download and use.


Thank You

Problem Statement



- You're an administrator for an architecture firm. The firm stores computer-aided design (CAD) files locally on a Windows Server file share. These CAD files are so large that your on-premises file share is nearly at capacity.

- The organization needs quick access to the CAD files that are used most frequently. The system can tolerate some network latency for the files that are used less frequently

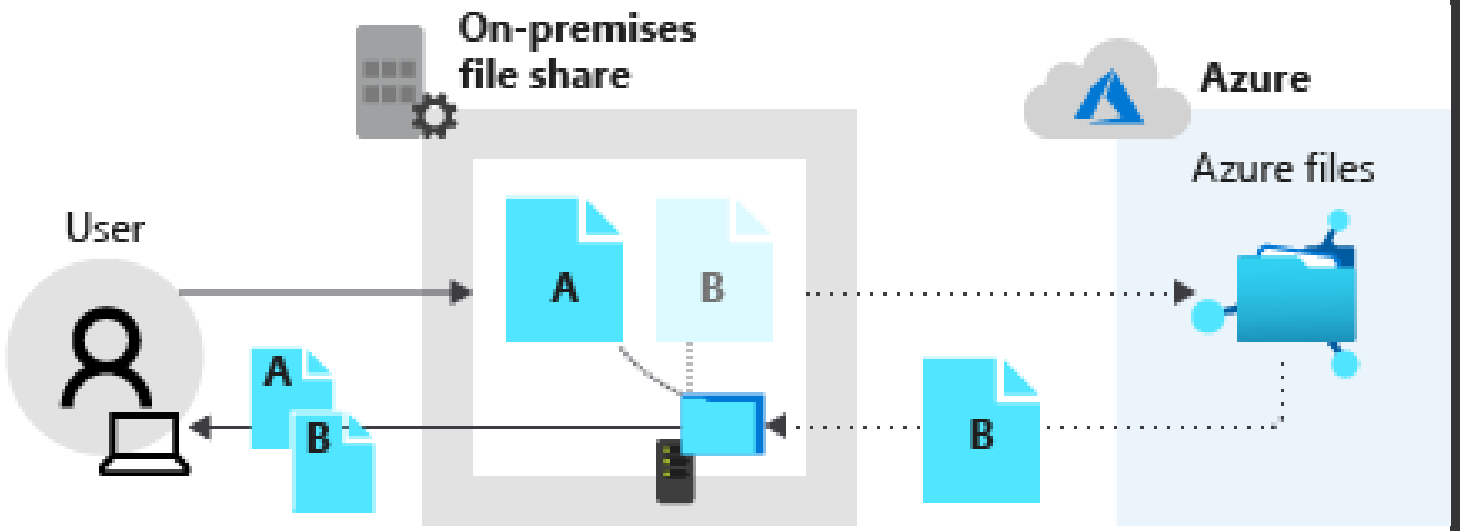

PROBLEM
SOLUTION

Azure File Sync

- Azure File Sync allows you to extend your on-premises file shares into Azure.
- It works with your existing on-premises file shares to expand your storage capacity and provide redundancy in the cloud. It requires Windows Server 2012 R2 or later.
- You can access your on-premises file share with any supported file sharing protocol that Windows Server supports, like SMB, NFS, or FTPS.
- https://docs.microsoft.com/en-us/learn/modules/extend-share-capacity-with-azure-file-sync/

Azure File Sync

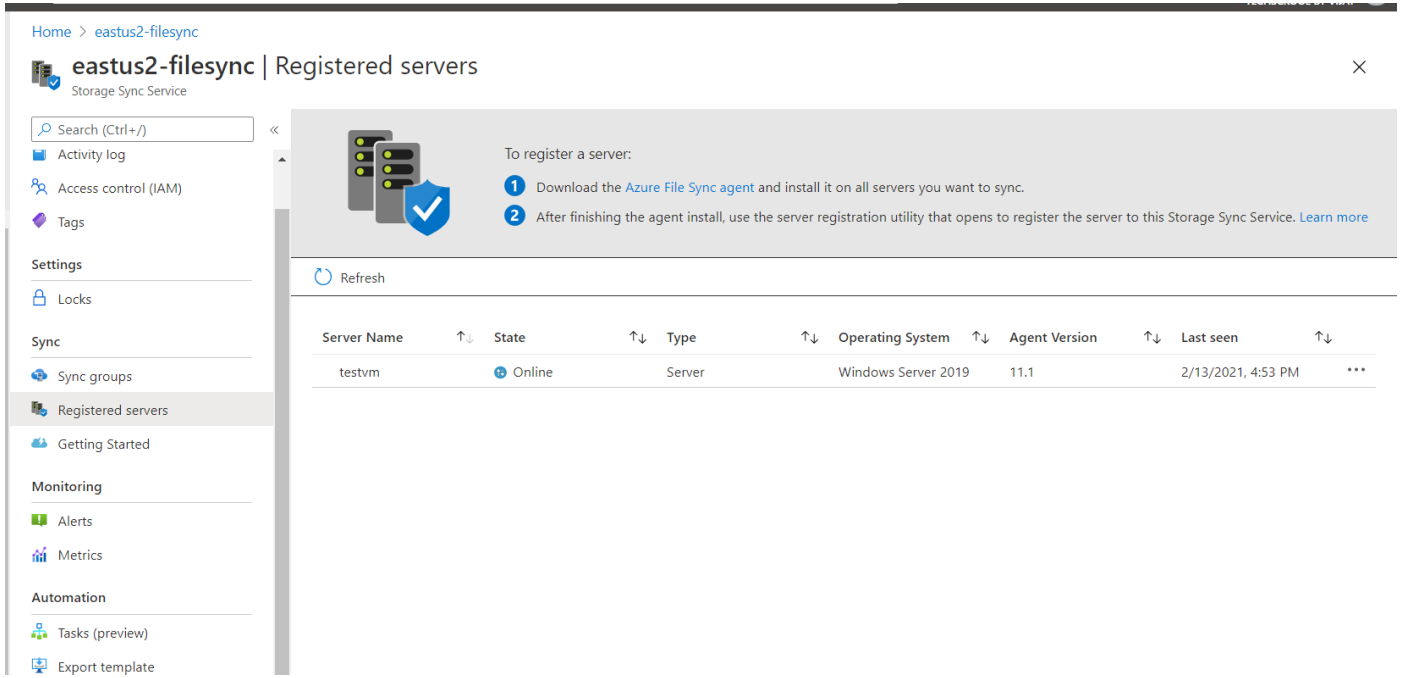
Azure File Sync uses your on-premises file server as a local cache for your Azure file share.



Azure File Sync

Registered Server

- A registered server represents the trust relationship between the on-premises server and the Storage Sync Service.
- You can register multiple servers to the Storage Sync Service. But a server can be registered with only one Storage Sync Service at a time.



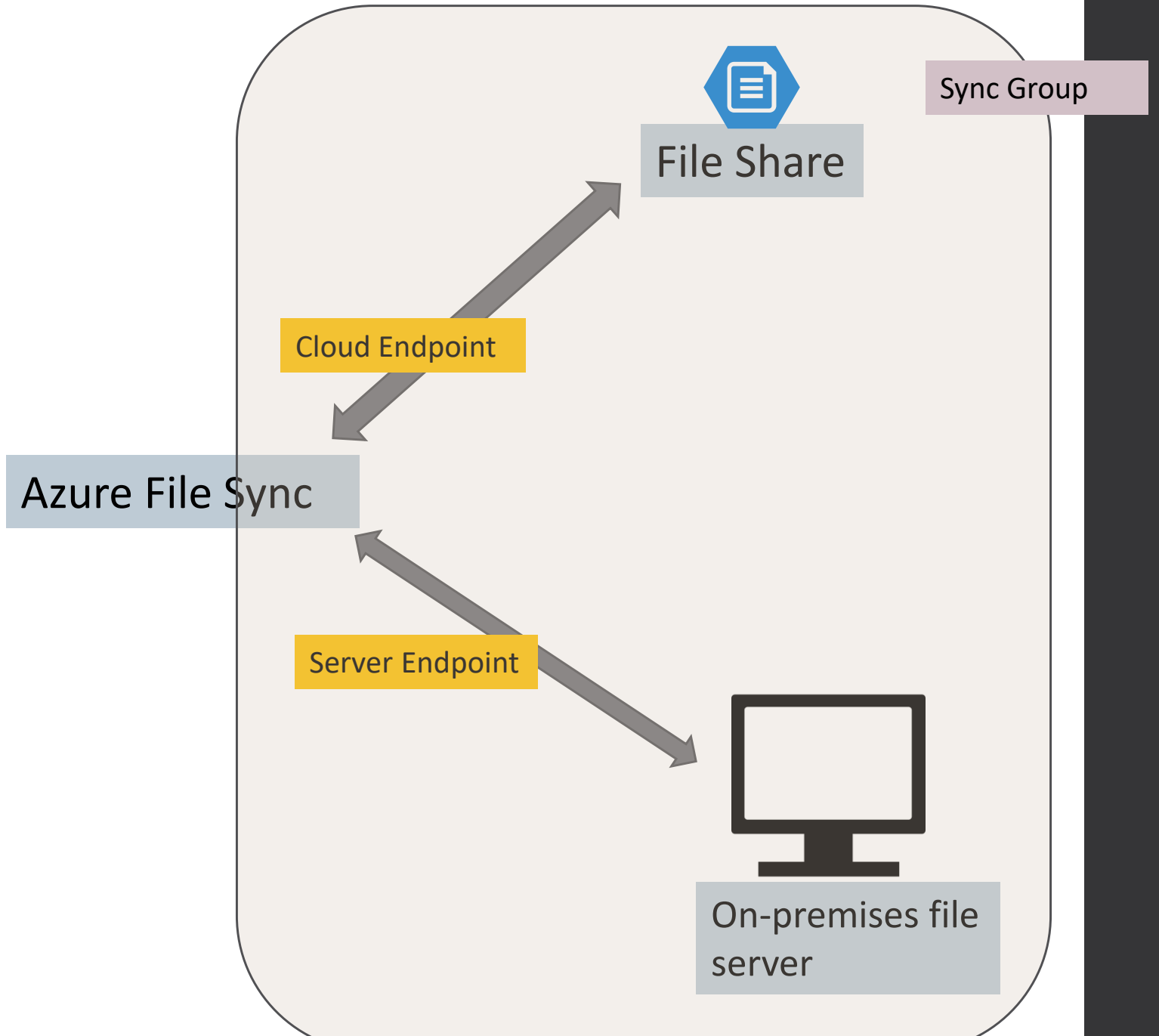
Azure File Sync

File Share

Azure File Sync

On-premises file server

Azure File Sync



Azure File Sync

A sync group outlines the replication topology for a set of files or folders. All endpoints located in the same sync group are kept in sync with each other.

Server endpoint represents a specific location on a registered server, like a folder on a local disk. Multiple server endpoints can exist on the same volume if their paths don't overlap.

Cloud endpoint is the Azure file share that's part of a sync group. The whole file share syncs and can be a member of only one cloud endpoint. An Azure file share can be a member of only one sync group at a time.

Azure Files Storage

Q) The manufacturing company's finance department wants to control how the data is being transferred to Azure Files. They want a graphical tool to manage the process, but they don't want to use the Azure portal. What tool do you recommend they use?

- ✓Azure Data Box
- ✓Robocopy
- ✓Azure Storage Explorer

Check your knowledge Azure Files Sync

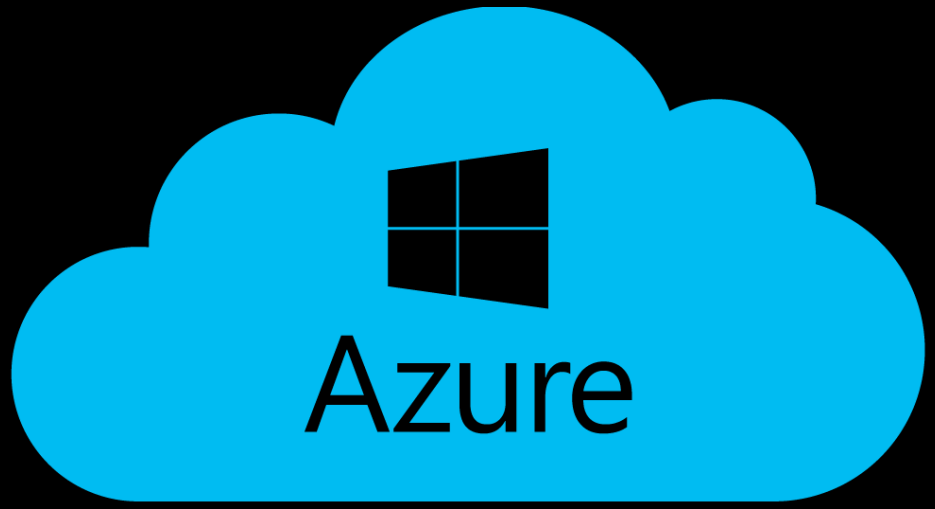
You've been asked by a local manufacturing company that runs dedicated software in their warehouse to keep track of stock. The software needs to run on machines in the warehouse, but the management team wants to access the output from the head office. The limited bandwidth available in the warehouse caused them problems in the past when they tried to use cloud-based solutions. You recommend that they use Azure Files. Which is the best method to sync the files with the cloud?

A.) Create an Azure Files share and directly mount shares on the machines in the warehouse.

B.) Use a machine in the warehouse to host a file share, install Azure File Sync, and share a drive with the rest of the warehouse.

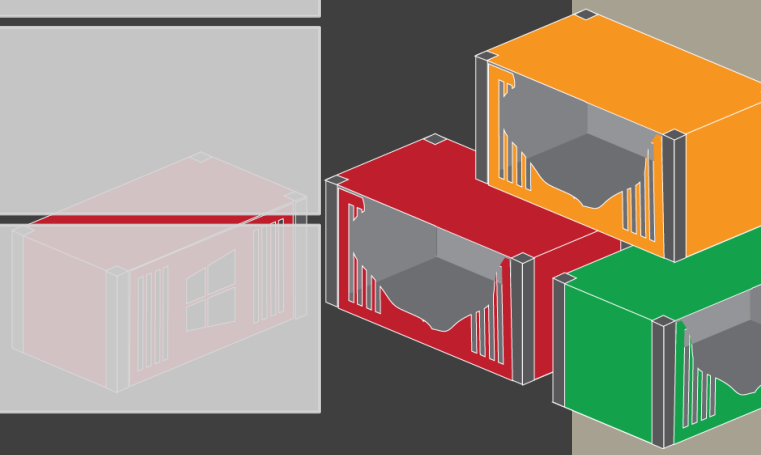
C.) Install Azure File Sync on every machine in the warehouse and head office.

Answer: B


Azure

Azure Storage : Security Features

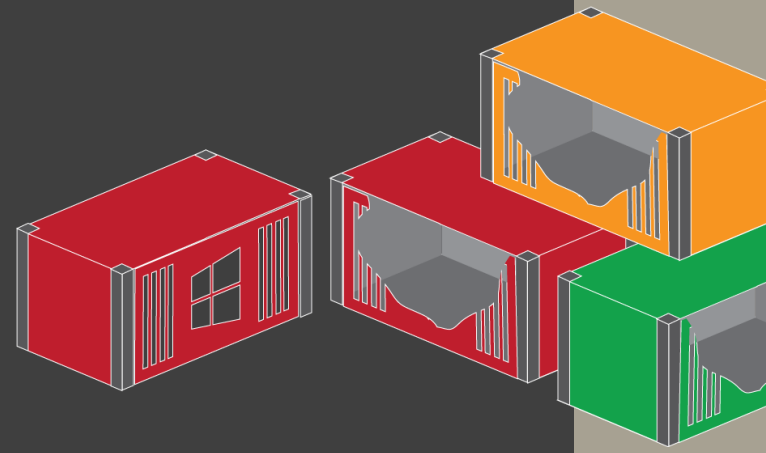
Protect	Protect the data at rest
Protect	Protect the data in transit
Support	Support browser cross-domain access
Control	Control who can access data
Audit	Audit storage access



Azure Files Storage: Security Options

https://docs.microsoft.com/en-us/learn/modules/store-and-share-with-azure-files/5-secure-azure-files

Secure Az Files



Encryption at Rest

All data written to Azure Storage is automatically encrypted by Storage Service Encryption (SSE) with a 256-bit Advanced Encryption Standard (AES) cipher, and is FIPS 140-2 compliant.

SSE automatically encrypts data when writing it to Azure Storage.

When you read data from Azure Storage, Azure Storage decrypts the data before returning it. This process incurs no additional charges and doesn't degrade performance. It can't be disabled.

~~For virtual machines (VMs), Azure lets you encrypt virtual hard disks (VHDs) by using Azure Disk Encryption. This encryption uses BitLocker for Windows images, and it uses dm-crypt for Linux.~~

Encryption in Transit

Keep your data secure by enabling transport-level security between Azure and the client. Always use HTTPS to secure communication over the public internet.

When you call the REST APIs to access objects in storage accounts, you can enforce the use of HTTPS by requiring secure transfer for the storage account. After you enable secure transfer, connections that use HTTP will be refused.

This flag will also enforce secure transfer over SMB by requiring SMB 3.0 for all file share mounts.

Role-Based Access Control

Azure Storage supports Azure Active Directory and role-based access control (RBAC) for both resource management and data operations.

To security principals, you can assign RBAC roles that are scoped to the storage account. Use Active Directory to authorize resource management operations, such as configuration. Active Directory is supported for data operations on Blob and Queue storage.

To a security principal or a managed identity for Azure resources, you can assign RBAC roles that are scoped to a subscription, a resource group, a storage account, or an individual container or queue.

CORS Support

Contoso stores several website asset types in Azure Storage. These types include images and videos. To secure browser apps, Contoso locks GET requests down to specific domains.

Azure Storage supports cross-domain access through cross-origin resource sharing (CORS). CORS uses HTTP headers so that a web application at one domain can access resources from a server at a different domain. By using CORS, web apps ensure that they load only authorized content from authorized sources.

CORS support is an optional flag you can enable on Storage accounts. The flag adds the appropriate headers when you use HTTP GET requests to retrieve resources from the Storage account.

Auditing Access

Auditing is another part of controlling access. You can audit Azure Storage access by using the built-in Storage Analytics service.

Storage Analytics logs every operation in real time, and you can search the Storage Analytics logs for specific requests. Filter based on the authentication mechanism, the success of the operation, or the resource that was accessed.

Azure Storage Security

https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations

Check your knowledge

https://docs.microsoft.com/en-us/learn/modules/secure-azure-storage-account/8-summary

Azure Storage Monitoring

Azure Blob storage creates monitoring data by using Azure Monitor, which is a full stack monitoring service in Azure.

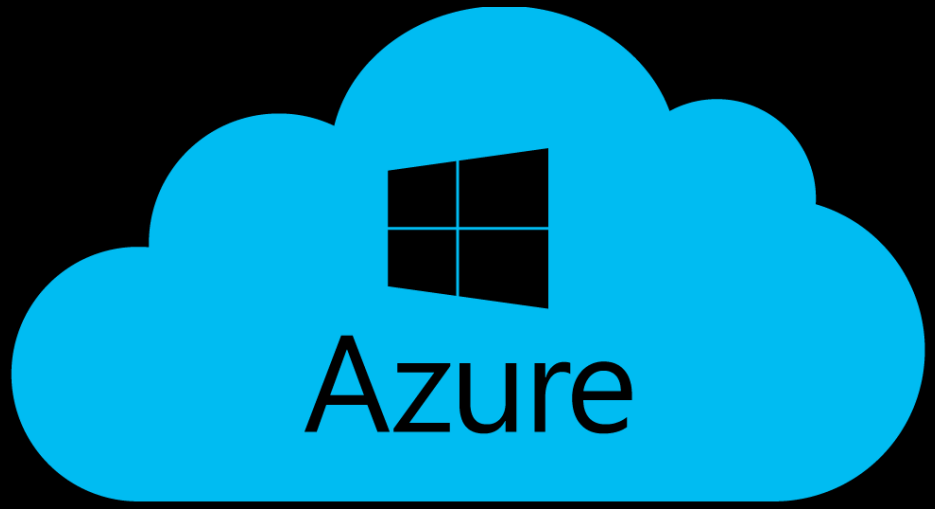
Azure Monitor provides a complete set of features to monitor your Azure resources and resources in other clouds and on-premises.

https://docs.microsoft.com/en-us/azure/storage/blobs/monitor-blob-storage?tabs=azure-portal

Data Protection

Recommendation	Comments
Use the Azure Resource Manager deployment model	Create new storage accounts using the Azure Resource Manager deployment model for important security enhancements, including superior Azure role-based access control (Azure RBAC) and auditing, Resource Manager-based deployment and governance, access to managed identities, access to Azure Key Vault for secrets, and Azure AD-based authentication and authorization for access to Azure Storage data and resources. If possible, migrate existing storage accounts that use the classic deployment model to use Azure Resource Manager. For more information about Azure Resource Manager, see Azure Resource Manager overview.
Enable Azure Defender for all of your storage accounts	Azure Defender for Azure Storage provides an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit storage accounts. Security alerts are triggered in Azure Security Center when anomalies in activity occur and are also sent via email to subscription administrators, with details of suspicious activity and recommendations on how to investigate and remediate threats. For more information, see Configure Azure Defender for Azure Storage.
Turn on soft delete for blob data	Soft delete enables you to recover blob data after it has been deleted. For more information on soft delete, see Soft delete for Azure Storage blobs.
Lock storage account to prevent accidental deletion	You can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying it. For more information, see Lock resources to prevent unexpected changes.
Store business-critical data in immutable blobs	Configure legal holds and time-based retention policies to store blob data in a WORM (Write Once, Read Many) state. Blobs stored immutably can be read, but cannot be modified or deleted for the duration of the retention interval. For more information, see Store business-critical blob data with immutable storage.
Limit shared access signature (SAS) tokens to HTTPS connections only	Requiring HTTPS when a client uses a SAS token to access blob data helps to minimize the risk of eavesdropping. For more information, see Grant limited access to Azure Storage resources using shared access signatures (SAS).

‘’Who so ever has come to this world, will surely go one day. This is the process of life.”



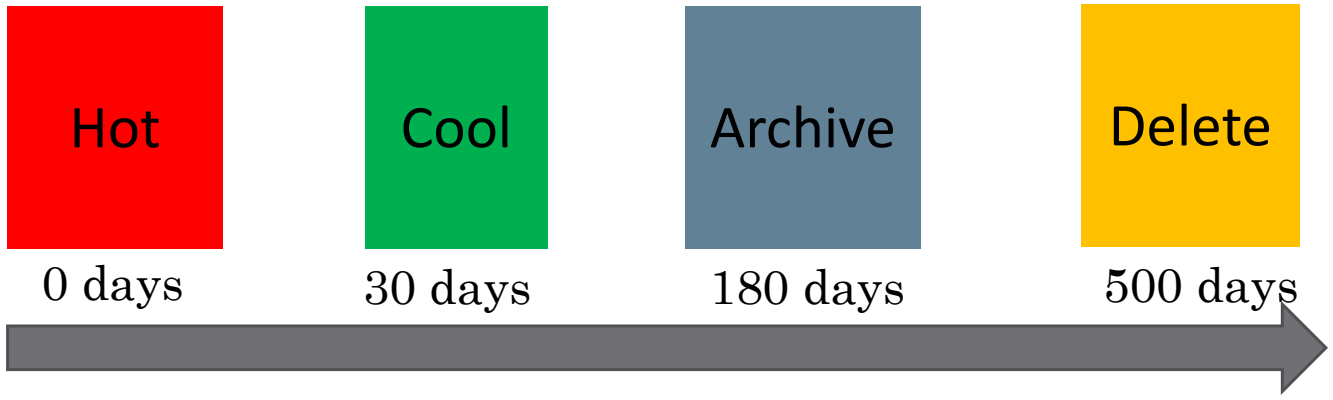
“Everything has a lifecycle. You have to believe it’s going to change.”

Data Lifecycle

Lifecycle Management

Azure Blob Storage lifecycle management offers a rich, rule-based policy for GPv2 and blob storage accounts.

Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle.



Azure Blob Storage Life Cycle Management

Lifecycle Management

The lifecycle management policy lets you:

- Transition blobs from cool to hot immediately if accessed to optimize for performance
- Transition blobs, blob versions, and blob snapshots to a cooler storage tier (hot to cool, hot to archive, or cool to archive) if not accessed or modified for a period of time to optimize for cost
- Delete blobs, blob versions, and blob snapshots at the end of their lifecycles
- Define rules to be run once per day at the storage account level
- Apply rules to containers or a subset of blobs (using name prefixes or blob index tags as filters)

Thank You