Secure Document Management System

Project Overview

The **Secure Document Management System** is designed to demonstrate various **Azure Blob Storage configurations, security measures, and access control mechanisms**. This project showcases different real-world storage scenarios, each tailored to meet specific security, availability, and access requirements.

Purpose & Objectives

The primary goal of this project is to configure and secure **Azure Blob Storage** to accommodate different organizational needs. By setting up three distinct storage accounts with unique access and security levels, the project aims to:

- **Showcase public and private access configurations**
- **Implement lifecycle management for cost optimization**
- **Enhance security using SAS, RBAC, Private Endpoints, and Encryption**
- **Ensure data availability through redundancy and replication**
- **Protect data integrity using immutability, soft delete, and versioning**

Storage 1: Public Access with Lifecycle Management

Scenario:

This storage is designed for an organization that allows customers to access its blobs from anywhere on the internet. The focus is on **public accessibility, cost management, and controlled access using SAS**.

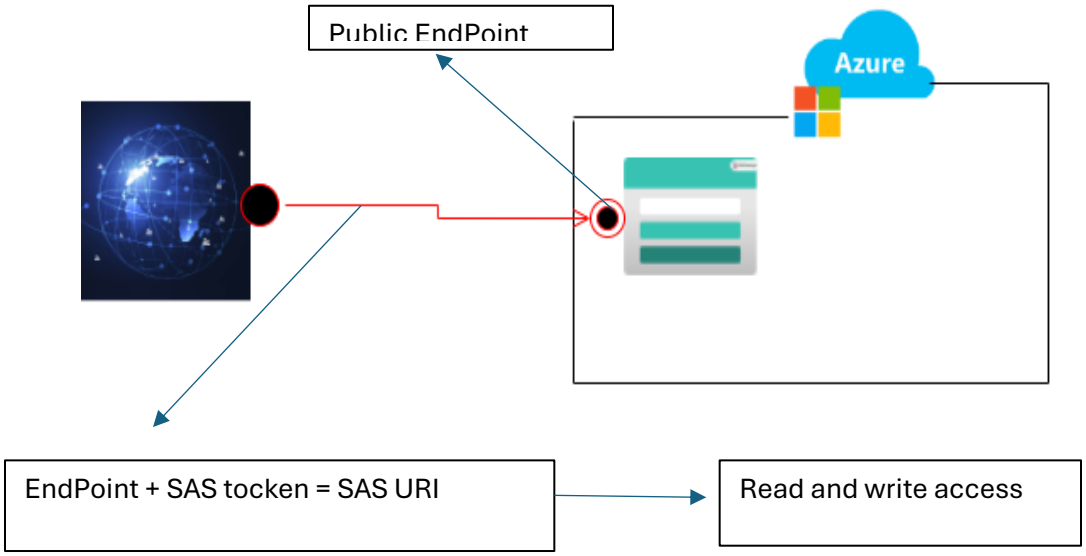
Configuration:

- **Public Access Level:** *Container* (Allows public read access to blobs within the container). To list blobs in this container we have to use Azure storage client libraries or REST APIs.

- **Access Control:** *SAS (Shared Access Signature) at the account level. This is the way to give restricted access for clients, for this storage account, the only permission configured in SAS is read and write access. The user can write on this storage account using Azure storage explorer. The client is only able to access the storage for specified time.*
- **Security Measures:** No sensitive data, so basic security configurations are applied. Azure by default encrypt data at rest before it would be written using platform-managed key called Advanced Encryption Standard (AES)-256
- **Data Redundancy:** *Locally Redundant Storage (LRS)* to ensure durability within a single region.
- **Cost Optimization:** *Lifecycle Management* configured to automatically delete infrequently accessed files. Policies are set to manage the life cycle of blobs with in the container.

Key Features Implemented:

✅ Public access at the container level ✅ SAS token for controlled access ✅ Lifecycle policy to manage data retention ✅ LRS for basic redundancy



Storage 2: Restricted Access with Enhanced Security

Scenario:

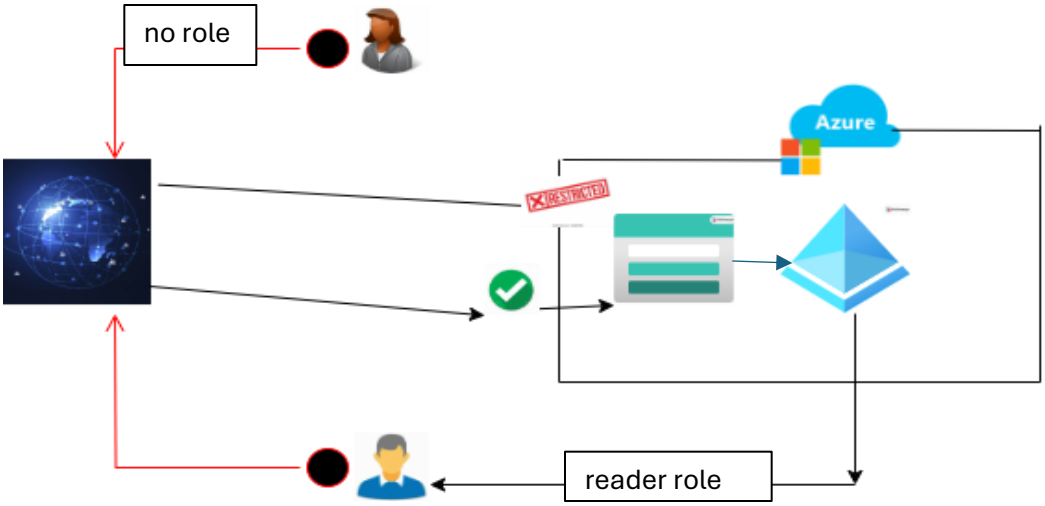
This storage is for an organization that requires **RBAC-based controlled access while still being publicly available**. Anonymous access is **completely restricted**, and security is strengthened using **immutability policies and object replication**.

Configuration:

- **Public Access Level:** *Private* (No anonymous access, only authenticated users). To access the storage account users must determine who they are. Users only with the right credential can access the storage.
- **Access Control:** *RBAC (Role-Based Access Control) for authorized clients. The user may have reader role, means they are able to read the account even if anonymous access is disabled.*
- **Security Measures:**
    - *Immutability Policy with Legal Hold* to prevent data modification/deletion
    - *Soft Delete* enabled to recover accidentally deleted blobs. Users are able to recover data with in the specified period of time.
- **Data Availability:** *Object Replication* to enhance storage resilience. It also enhance performance since users can access blobs from the region where they are closest to. Unlike redundancy options, it give read and write access.

Key Features Implemented:

✅ Private access level with RBAC authentication ✅ Legal Hold Immutability Policy for data protection ✅ Soft Delete to prevent permanent data loss ✅ Object Replication for high availability



Storage 3: High-Security, Private Access with Strong Encryption

Scenario:

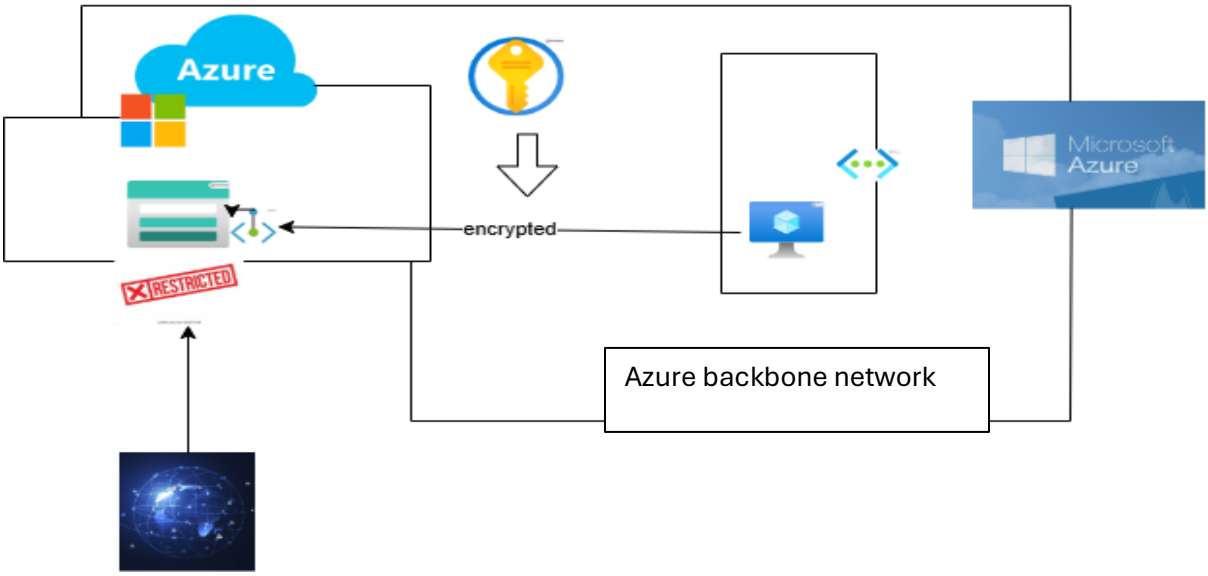
This storage is designed for an organization that requires **strict access control, enhanced encryption, and high availability**. The storage account is completely **private**, and only resources within a virtual network can access it.

Configuration:

- **Public Access Level:** *Disabled* (Only private endpoint access allowed)
- **Access Control:** *Private Endpoint with Virtual Network Integration, Therefore the storage account is accessible only by services found on the virtual network which is linked with the private end point of the storage account. Any type of request from the internet through public endpoint will be restricted.*
- **Security Measures:**
  - *Customer-Managed Keys (CMK)* for full control over encryption
  - *Blob Versioning* to maintain previous versions of modified/deleted blobs
- **Performance & Availability:**
  - *Hot Access Tier* for frequent data access
  - *RA-GRS (Read-Access Geo-Redundant Storage)* for cross-region replication
- **Restricted Client Access:** *SAS tokens configured with precise permissions*

Key Features Implemented:

✅ Private Endpoint for secure virtual network access ✅ Customer-Managed Keys for encryption control ✅ Blob Versioning to retain previous data versions ✅ Hot Access Tier for optimal performance ✅ RA-GRS for high availability and disaster recovery



Conclusion

This project successfully implements **secure, scalable, and highly available blob storage solutions** tailored for different organizational needs. By configuring public and private access, lifecycle management, security policies, and redundancy strategies, it provides a comprehensive demonstration of **Azure Blob Storage best practices**.

Key Learnings & Takeaways:

🔹 Understanding and implementing **public vs. private storage access** 🔹 Utilizing **SAS tokens, RBAC, and Private Endpoints** for secure access control 🔹 Leveraging **encryption strategies** such as Microsoft-managed and customer-managed keys 🔹 Implementing **data protection mechanisms** including immutability, soft delete, and

versioning 🔹 Enhancing **performance and availability** using replication and optimized access tiers

This **Secure Document Management System** is a robust showcase of **Azure Blob Storage capabilities**, demonstrating real-world applications of **storage security, management, and optimization**. 🚀

Contributor: Abinet Degefa