Storage Accounts Set Up

Blob storage is highly scalable, secure, and cost-efficient. It is used for storing unstructured data like images, videos, backups, logs, or large text files. Blobs is what we will use within Azure for storing data and will be a means of connecting to CSU environment.

A high level overview of the relationship of storage accounts and blobs is available in figure 1.

A blue rectangle with black background

Description automatically generated

The proposed solution uses several storage accounts which each are independent of one another. The access is to each be governed by Intra Role-Based Access Control (RBAC) a system that controls access to Azure resources by allocating particular roles to users, groups, or applications. Most of these roles are built into Azure (<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage>).

Admin permissions will be granted the contributor role, allowing them to read/write/delete from the storage account. The developers will be given the role of read/write for storage accounts, this is a custom role and will have to be created.

The following Storage Accounts are to be created:

1. sa

saetf stands for storage account electronic file transfer. It will be used for getting blobs from Azure to. The files will remain available for 30 days after which they would be deleted.

1. sa

This has a couple of containers within it.

* 1. Pki (Public Key Infrastructure) holds the certificates and key files used to build the infrastructure.
  2. Keys

The public keys generated for accessing virtual machines.

1. sa

This contains the keys container which will hold the public keys for accessing virtual machines.

1. sa

This will hold the gitlab backups and will hold them for 30 days.