Azure Storage security

Azure storage security overview

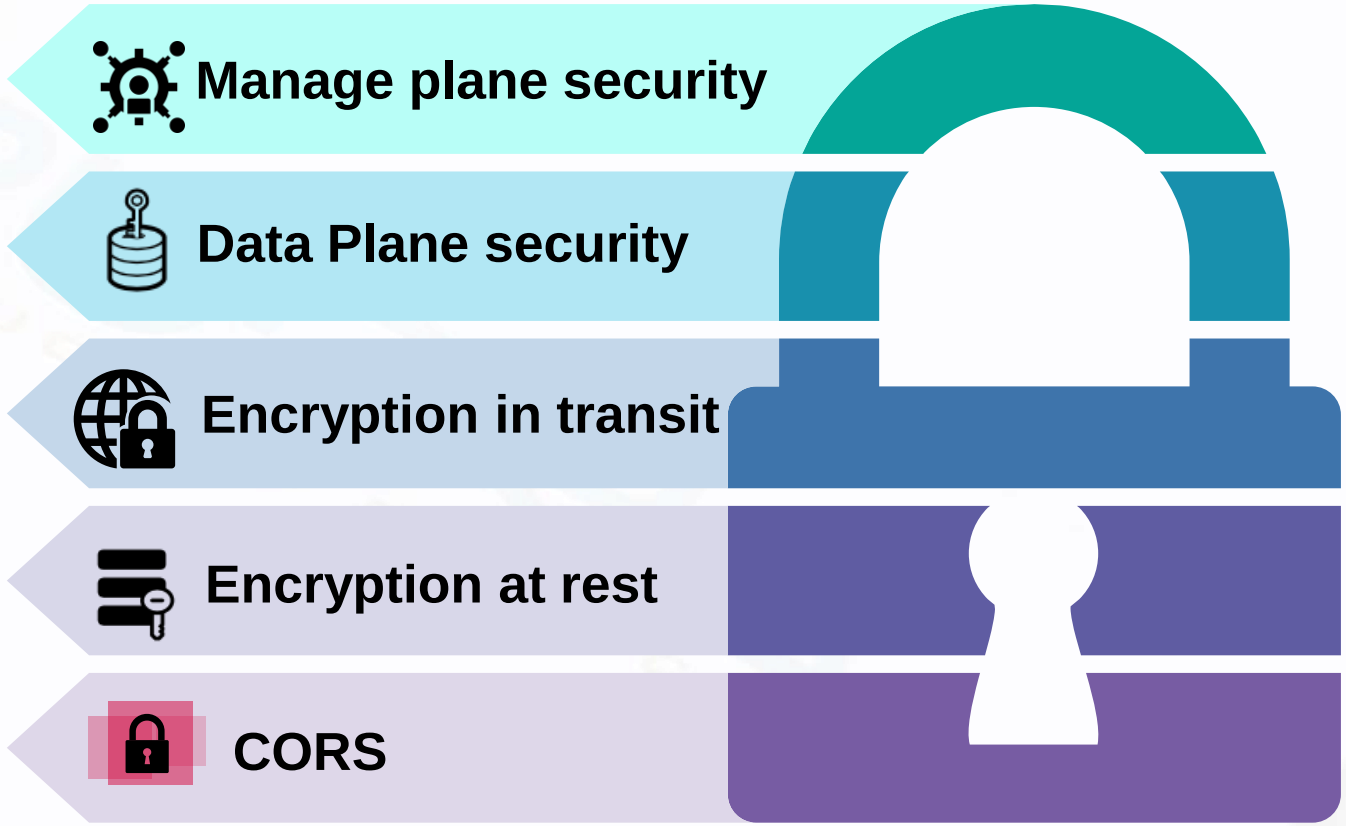
Securing your storage account

Securing access to your data

Encryption in transit

Encryption at rest

Cross Origin Resource Sharing



Management plane security

- Management plane refers to the operations that effect the storage account itself.

- Role Based Access Control
  - Each Azure subscription has an Azure Active Directory. Users, groups and applications from that directory can be granted access to manage resources in the Azure subscription. This is referred as Role Based Access Control.
  - Access is granted by assigning the appropriate RBAC role to users, groups, and applications at the right level. This level can be subscription, resources group and resources.

- Key points to remember
  - When you assign a role, You can control access to operations used to manage the storage account and data objects in the account..
  - Each role has a list of Actions & Not Actions.
  - There are some standard management roles available. For e.g. Owner, Reader, Contributor etc.
  - Data operations roles include Storage blob data reader role etc.

Data plane security

- Data plane security refers to the methods used to secure data objects (blobs, queues, tables and files) within the storage account.

- Three methods for controlling access to data objects

    - Using Azure AD to authorize access to containers and queues (Preview). Azure AD provides advantages over other approaches to authorization, including removing the need to store secrets in your code.
    - Storage account keys
    - Shared Access Signatures

- You can allow public access to your blobs by setting the access level for the container that holds the blob accordingly.

- Storage firewall to restrict access only to known IP address ranges and virtual networks

Encryption in Transit

- Transport level Encryption using HTTPS
  - Always use HTTPS when using REST APIs or accessing objects in storage.
  - If you are using SAS, you can specify that only HTTPS should be used

- Using encryption in transit for Azure file shares
  - SMB2.1 do not support encryption so connections are only allowed within the same region.
  - SMB3.0 supports encryption and cross region access is allowed

- Client side encryption
  - Encrypt the data before being transferred to Azure storage
  - When retrieving the data from Azure, data is decrypted after it is received on the client side.

Encryption at rest

- Client side encryption
  - Encrypt the data before being transferred to Azure storage
  - When retrieving the data from Azure, data is decrypted after it is received on the client side

- Storage Service Encryption (SSE)
  - SSE is enabled for all storage accounts and cannot be disabled
  - SSE automatically encrypts data in all performance tiers (Standard and Premium), all deployment models (Azure Resource Manager and Classic), and all of the Azure Storage services (Blob, Queue, Table, and File).
  - You can use either Microsoft-managed keys or your own custom keys.

- Azure Disk Encryption
  - Encrypt the OS & data disks used by IaaS Virtual Machine
  - You can enable encryption on existing IaaS VMs
  - You can use customer provided encryption keys

Important note: Refer to the link in the resource section of this lecture for comparison between above three encryption types

Cross Origin Resource Sharing

- When a web browser running in one domain makes an HTTP request for a resource from a different domain, this is called a cross-origin HTTP request

- Azure Storage allows you to enable CORS. For each storage account, you can specify domains that can access the resources in that storage account. For example, enable CORS on the mystorage.blob.core.windows.net storage account and configure it to allow access to mywebsite.com

- CORS allows access but does not provide authentication which means you still need to use SAS to access non-public storage resources.

- By default, CORS is disabled on all services.