Risk Assessment

Name: Kantha Sishanth S

Reg No: 212222100020

Aim

To perform an asset-oriented risk assessment of cloud storage assets including:

- AWS Elastic Block Store (EBS)
- AWS Elastic File System (EFS)
- Azure Files (File Storage)

Pre-requisites

1. Background

Cloud storage services offer flexible, scalable options for storing data. However, each storage type brings distinct security risks and configurations. This experiment focuses on identifying assets and performing a detailed risk assessment based on:

- Confidentiality, Integrity, and Availability (CIA)
- Access control
- Encryption
- Auditing capabilities

2. Tools Required

- AWS Console with EC2, EBS, and EFS access
- Azure Portal with Storage Account access
- IAM credentials with sufficient permissions
- Risk Assessment Template (provided)
- Internet browser
- Microsoft Excel or Google Sheets for tabulating findings

Procedure

Part A: Identifying AWS Storage Assets

Step 1: Login to AWS Console

- Go to: https://aws.amazon.com/console
- Log in using IAM or root credentials

Step 2: Identify EBS Volumes

- Navigate to: `EC2 > Volumes (under Elastic Block Store)`
- Record the following:
  - Volume ID
  - Size and Type (e.g., gp2, io1)
  - Availability Zone
  - Attached instance (if any)
  - Encryption status
  - Tags

Step 3: Identify EFS File Systems

- Go to: `EFS > File systems`
- Record:
  - File system ID and name
  - Mount targets (AZs)
  - Throughput mode (bursting/provisioned)
  - Performance mode
  - Lifecycle policy
  - Encryption at rest status

Part B: Identifying Azure File Storage Assets

Step 4: Login to Azure Portal

- Go to: https://portal.azure.com
- Log in using credentials with access to storage accounts

Step 5: View File Shares

- Navigate to: `Storage Accounts > Choose Account > File Shares`
- Record:
  - Name
  - Quota (in GB)
  - Used space
  - Protocol (SMB/NFS)
  - Authentication method (SAS Tokens, Azure AD, Shared Keys)
  - Snapshot policies

Risk Assessment Methodology

Use the following **CIA-based asset-oriented checklist** for each asset:

Criteria	Description
Confidentiality	Encryption, authentication, access control
Integrity	Data consistency, snapshot support, checksums
Availability	Multi-AZ, redundancy, auto-scaling
Access Control	IAM, Security Groups, ACLs
Encryption	At-rest and in-transit encryption
Auditing	CloudTrail, logs, alerts

Sample Output Table

Cloud Provider	Asset Type	Asset ID	Encrypted	Access Control	Risk Level	Comments
AWS	EBS Volume	vol-abc	Yes	IAM Policy	Medium	Used by EC2
AWS	EFS	fs-xyz	Yes	Security Group	Low	Multi-AZ mount

Cloud Provider	Asset Type	Asset ID	Encrypted	Access Control	Risk Level	Comments
Azure	File Share	datafiles	Yes	Shared Key	Medium	Quota 1TB

Result

All active cloud storage assets across AWS and Azure have been identified and assessed for security posture based on CIA principles, access control, encryption, and risk level.