Lab Reports - Ishmael GYAMFI

Lab 1 Report: Storage Classes & Lifecycle Policies

What worked as expected?

- Bucket creation in eu-west-1 was straightforward
- Uploading objects with different storage classes functioned correctly
- Lifecycle rule creation successfully configured automatic transitions
- Cost differences between storage classes were clearly visible in the pricing calculator

What was challenging?

- Understanding the minimum duration requirements for each storage class
- Calculating the break-even point for when Standard-IA becomes cost-effective
- Comprehending the complexity of retrieval costs for infrequently accessed storage

Real-world application:

- **Log Management:** Implement lifecycle policies to automatically transition application logs from Standard to IA after 30 days, then to Glacier after 90 days
- **Backup Strategy:** Use intelligent tiering for unknown access patterns, Standard-IA for monthly reports, and Glacier for long-term compliance data
- **Media Assets:** Transition large media files to cheaper storage classes based on access patterns

Cost implications observed:

- Standard-IA provides 45% cost savings for storage but adds retrieval costs
- Intelligent-Tiering adds $0.0025/1000 objects monitoring fee but optimizes automatically
- Glacier Deep Archive offers 75% cost savings but requires 12-hour retrieval time

Lab 2 Report: Versioning & MFA Delete

What worked as expected?

- Versioning enabled seamlessly during bucket creation
- Multiple versions of the same object were created and managed properly
- Delete markers functioned as expected, preserving underlying object versions
- Version restoration worked without data loss

What was challenging?

- Understanding the difference between delete markers and permanent deletion
- Grasping the security implications of MFA Delete
- Managing storage costs with multiple versions accumulating

Real-world application:

- **Document Management:** Enable versioning for critical business documents to prevent accidental data loss
- **Code Repositories:** Use versioning for configuration files and deployment artifacts
- **Compliance:** Implement MFA Delete for regulatory requirements in financial or healthcare industries

Cost implications observed:

- Each version consumes storage space and incurs separate charges
- Delete markers don't consume storage but count toward object count
- Version management requires governance policies to prevent cost accumulation

Lab 3 Report: Cross-Region Replication (CRR)

What worked as expected?

- CRR setup between eu-west-1 and eu-central-1 worked smoothly
- Objects replicated automatically within 2-3 minutes
- Storage class transitions were applied correctly at destination
- IAM role permissions functioned properly

What was challenging?

- Understanding replication timing and eventual consistency
- Configuring proper IAM permissions for cross-region access
- Managing costs with data transfer between regions

Real-world application:

- **Disaster Recovery:** Replicate critical data across regions for business continuity
- **Compliance:** Meet data residency requirements by replicating to specific regions
- **Performance:** Reduce latency by having data closer to global users
- **Backup Strategy:** Create geographically distributed backups for enhanced protection

Cost implications observed:

- Data transfer costs apply for cross-region replication
- Destination storage costs based on configured storage class
- Request charges for replication API calls
- Monitoring and management overhead costs

Lab 1 Assessment:

Q1: What happens to an object's cost when it transitions from Standard to Standard-IA?

- **Answer:** The storage cost decreases from $0.023/GB to $0.0125/GB per month, but retrieval costs are introduced. Standard-IA has a minimum storage duration of 30 days and minimum object size of 128KB. Objects accessed frequently may cost more due to retrieval fees.

Q2: Can you transition directly from Standard to Glacier Deep Archive? Why/why not?

- **Answer:** No, you cannot transition directly from Standard to Glacier Deep Archive. AWS requires objects to remain in Standard-IA for at least 30 days before transitioning to Glacier storage classes. This ensures objects aren't immediately moved to long-term archival storage.

Q3: What's the minimum duration an object must stay in Standard-IA?

- **Answer:** Objects must remain in Standard-IA for a minimum of 30 days. If deleted or transitioned before 30 days, you're still charged for the full 30-day period.

Lab 2 Assessment:

Q1: What happens to previous versions when you upload a new version of an object?

- **Answer:** Previous versions are preserved and remain accessible. The new version becomes the "current" version, but all historical versions maintain their unique version IDs and can be downloaded, restored, or managed independently.

Q2: How do you permanently delete a specific version of an object?

- **Answer:** Toggle "Show versions" in the S3 console, select the specific version you want to delete, and choose "Delete". This permanently removes that version. Alternatively, use AWS CLI with the version ID specified.

Q3: Why can only the root user enable MFA Delete?

- **Answer:** MFA Delete provides an additional security layer for critical operations. Only the root user can enable it because root users have the highest level of account access and are responsible for account-wide security policies. This prevents unauthorized users from modifying this critical security feature.

Lab 3 Assessment:

Q1: What are the prerequisites for setting up CRR?

- **Answer:**
  - Versioning must be enabled on both source and destination buckets
  - Source and destination buckets must be in different AWS regions

    - IAM role with appropriate permissions for replication
    - Unique bucket names in different regions

Q2: Do delete markers get replicated by default?

- **Answer:** No, delete markers are not replicated by default. This behavior can be configured in the replication rule settings. When disabled, deleting an object in the source bucket won't delete it in the destination bucket, providing additional data protection.

Q3: Can you replicate to a bucket in the same region?

- **Answer:** No, Cross-Region Replication (CRR) requires buckets to be in different AWS regions. For same-region replication, you would use Same-Region Replication (SRR), which has similar configuration but different use cases.