**Lecture Notes for AWS Developer**

**Module-3**

**Amazon S3**

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. This means customers of all sizes and industries can use it to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements. Amazon S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world.

**Benefits**

**Industry-leading performance, scalability, availability, and durability**

Scale your storage resources up and down to meet fluctuating demands, without upfront investments or resource procurement cycles. Amazon S3 is designed for 99.999999999% (11 9’s) of data durability because it automatically creates and stores copies of all S3 objects across multiple systems. This means your data is available when needed and protected against failures, errors, and threats.

**Wide range of cost-effective storage classes**

Save costs without sacrificing performance by storing data across the S3 Storage Classes, which support different data access levels at corresponding rates. You can use S3 Storage Class Analysis to discover data that should move to a lower-cost storage class based on access patterns, and configure an S3 Lifecycle policy to execute the transfer. You can also store data with changing or unknown access patterns in S3 Intelligent-Tiering, which tiers objects based on changing access patterns and automatically delivers cost savings.

**Unmatched security, compliance, and audit capabilities**

Store your data in Amazon S3 and secure it from unauthorized access with encryption features and access management tools. S3 is the only object storage service that allows you to block public access to all of your objects at the bucket or the account level with S3 Block Public Access. S3 maintains compliance programs, such as PCI-DSS, HIPAA/HITECH, FedRAMP, EU Data Protection Directive, and FISMA, to help you meet regulatory requirements.

**Easily manage data and access controls**

S3 gives you robust capabilities to manage access, cost, replication, and data protection. S3 Access Points make it easy to manage data access with specific permissions for your applications using a shared data set. S3 Replication manages data replication within the region or to other regions. S3 Batch Operations helps manage large scale changes across billions of objects.

**Query-in-place services for analytics**

Run big data analytics across your S3 objects (and other data sets in AWS) with our query-in-place services. Use Amazon Athena to query S3 data with standard SQL expressions and Amazon Redshift Spectrum to analyze data that is stored across your AWS data warehouses and S3 resources. You can also use S3 Select to retrieve subsets of object data, instead of the entire object, and improve query performance by up to 400%.

**Most supported cloud storage service**

Store and protect your data in Amazon S3 by working with a partner from the AWS Partner Network (APN) — the largest community of technology and consulting cloud services providers. The APN recognizes migration partners that transfer data to Amazon S3 and storage partners that offer S3-integrated solutions for primary storage, backup and restore, archive, and disaster recovery.

**Bucket policy**

S3 bucket policies specify what actions are allowed or denied for which principals on the bucket that the bucket policy is attached to. A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates.

**What is a bucket in AWS?**

An Amazon S3 bucket is a public cloud storage resource available in Amazon Web Services' (AWS) Simple Storage Service (S3), an object storage offering. Amazon S3 buckets, which are similar to file folders, store objects, which consist of data and its descriptive metadata.

**Amazon Athena**

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.

Athena is easy to use. Simply point to your data in Amazon S3, define the schema, and start querying using standard SQL. Most results are delivered within seconds. With Athena, there’s no need for complex ETL jobs to prepare your data for analysis. This makes it easy for anyone with SQL skills to quickly analyze large-scale datasets.

**Amazon CloudFront**

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment.

CloudFront offers the most advanced security capabilities, including field level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall and Route 53 to protect against multiple types of attacks including network and application layer DDoS attacks. These services co-reside at edge networking locations – globally scaled and connected via the AWS network backbone – providing a more secure, performant, and available experience for your users.

**Benefits**

**Global Scaled Network for Fast Content Delivery**

Amazon CloudFront is massively scaled and globally distributed. The CloudFront network has 225+ points of presence (PoPs) that are interconnected via the AWS backbone delivering ultra-low latency performance and high availability to your end users. Amazon CloudFront automatically maps network conditions and intelligently routes your user’s traffic to the most performant AWS edge location to serve up cached or dynamic content.

**Security at the Edge**

Amazon CloudFront is a highly secure CDN that provides both network and application level protection. All your CloudFront distributions are defended by default against the most frequently occurring network and transport layer DDoS attacks that target your websites or applications with AWS Shield Standard. To defend against more complex attacks, you can add a flexible, layered security perimeter by integrating CloudFront with AWS Shield Advanced and AWS Web Application Firewall (WAF).

**Highly Programmable and Secure Edge Computing**

Amazon CloudFront offers the programmable and secure edge CDN computing capabilities through AWS Lambda@Edge. For application logic customizations at the edge, Lambda@Edge provides you a general-purpose compute runtime feature for computationally intensive operations such as dynamic origin load-balancing, custom bot-management, or building serverless origins.

**Deep Integration with AWS**

Amazon CloudFront is integrated with AWS services such as Amazon S3, Amazon EC2, Elastic Load Balancing, Amazon Route 53, and AWS Elemental Media Services for easy set-up. As a developer, you can use the AWS management console or familiar developer tools such as CloudFormation templates, the AWS Cloud Development Kit, and APIs. CloudFront’s integration with Amazon Cloudwatch and Kinesis offers real-time observability through metrics and logs.

**Cost-Effective**

Amazon CloudFront offers cost-effective content-delivery globally. Integrated with AWS, there are no transfer fees for origin fetches from any AWS origin and AWS Certificate Manager (ACM) offers custom TLS certificates, at no charge.