## ****Lecture Notes for AWS Developer****

## ****Module I****

**AWS Identity and Access Management (IAM)**

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

IAM is a feature of your AWS account offered at no additional charge. You will be charged only for use of other AWS services by your users.

**Use cases**

**Fine-grained access control to AWS resources**

IAM enables your users to control access to AWS service APIs and to specific resources. IAM also enables you to add specific conditions such as time of day to control how a user can use AWS, their originating IP address, whether they are using SSL, or whether they have authenticated with a multi-factor authentication device.

**Multi-factor authentication for highly privileged users**

Protect your AWS environment by using AWS MFA, a security feature available at no extra cost that augments user name and password credentials. MFA requires users to prove physical possession of a hardware MFA token or MFA-enabled mobile device by providing a valid MFA code.

**Analyze access**

IAM helps you analyze access across your AWS environment. Your security teams and administrators can quickly validate that your policies only provide the intended public and cross-account access to your resources. You can also easily identify and refine your policies to allow access to only the services being used. This helps you to better adhere to the principle of least privilege.

**Integrate with your corporate directory**

IAM can be used to grant your employees and applications federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation).

**Elastic Load Balancing**

Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, Lambda functions, and virtual appliances. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers four types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault tolerant.

**Types**

**Application Load Balancer**

Application Load Balancer is best suited for load balancing of HTTP and HTTPS traffic and provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers. Application Load Balancer routes traffic to targets within Amazon VPC based on the content of the request.

**Network Load Balancer**

Network Load Balancer is best suited for load balancing of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Transport Layer Security (TLS) traffic where extreme performance is required. Network Load Balancer routes traffic to targets within Amazon VPC and is capable of handling millions of requests per second while maintaining ultra-low latencies.

**Gateway Load Balancer**

Gateway Load Balancer makes it easy to deploy, scale, and run third-party virtual networking appliances. Providing load balancing and auto scaling for fleets of third-party appliances, Gateway Load Balancer is transparent to the source and destination of traffic. This capability makes it well suited for working with third-party appliances for security, network analytics, and other use cases.

**Classic Load Balancer**

Classic Load Balancer provides basic load balancing across multiple Amazon EC2 instances and operates at both the request level and the connection level. Classic Load Balancer is intended for applications that were built within the EC2-Classic network. A Classic Load Balancer makes routing decisions at either the transport layer (TCP/SSL) or the application layer (HTTP/HTTPS). Classic Load Balancers currently require a fixed relationship between the load balancer port and the container instance port.

**Benefits**

**Highly availability and elasticity**

Elastic Load Balancing is part of the AWS network, with native awareness of failure boundaries like AZs to keep your applications available across a region, without requiring Global Server Load Balancing (GSLB). ELB is also a fully managed service, meaning you can focus on delivering applications and not installing fleets of load balancers. Capacity is automatically added and removed based on the utilization of the underlying application servers.

**Security**

Elastic Load Balancing works with Amazon Virtual Private Cloud (VPC) to provide robust security features, including integrated certificate management, user-authentication, and SSL/TLS decryption. Together, they give you the flexibility to centrally manage TLS settings and offload CPU intensive workloads from your applications. ALB also supports integration with AWS WAF, adding a level of protection before bad actors reach the application. Further, S2N and HTTP Guardian have been developed as Open Source solutions to reduce the potential for HTTP-based attacks.

**Feature breadth**

Elastic Load Balancing offers the breadth of features needed by businesses of all sizes, while delivering them in an AWS-native experience. Elastic Load Balancing includes support for features needed in container-based workloads, including HTTP/2, gRPC, TLS offload, advanced rule-based routing, and integration with container services as an ingress controller. ALB provides customers with a native HTTP endpoint for calling Lambda functions, removing the dependency on other solutions. Further, Gateway Load Balancer creates one gateway for routing traffic through fleets of third-party appliances.

**Robust monitoring & visibility**

Elastic Load Balancing allows you to monitor the health of your applications and their performance in real time with Amazon CloudWatch metrics, logging, and request tracing. This improves visibility into the behavior of your applications, uncovering issues and identifying performance bottlenecks in your application stack. ELB helps ensure compliance with application Service Level Agreements (SLAs).

**Integration and global reach**

As a native AWS service, ELB is tightly integrated with other AWS services like EC2, ECS/EKS, Global Accelerator and operational tools such as AWS CloudFormation and AWS Billing. Across the Amazon Global Infrastructure and customer data centers with AWS Outposts and on-premises target support, ELB is available everywhere you run your AWS workloads.

**Use cases**

**Migrating to AWS**

ELB supports the load balancing capabilities critical for you to migrate to AWS. ELB is well positioned to load balance both traditional as well as cloud native applications with auto scaling capabilities that eliminate the guess work in capacity planning. ELB is easy to configure and use, which makes your migration experience simple. The managed experience of ELB means that you can focus on the most critical part of a successful migration - migrating applications - instead of configuring load balancers. ELB also integrates well with the common management tools that you are familiar with such as Terraform and Ansible.

**Modernizing applications with serverless and containers**

Organizations need to build applications faster than ever, with a combination of modular architecture patterns, serverless operational models, and agile developer processes. ELB adapts to these modern applications and their changing load without customer intervention, scaling out while still only charging for usage. Customers building serverless applications using Lambda can leverage ALB to provide a native HTTP-based endpoint, without requiring complex configurations or using an API gateway. ELB also includes support for containers and container orchestration using Kubernetes, providing load balancing between clients and applications as well as service to service communication.

**Building a hybrid cloud**

Elastic Load Balancing offers the ability to load balance across AWS and on-premises resources, using a single load balancer. You can achieve this by registering all of your resources to the same target group and associating the target group with a load balancer. Alternatively, you can use DNS-based weighted load balancing across AWS and on-premises resources across two load balancers, with one load balancer for AWS and another for on-premises resources.

**Scaling third-party virtual appliances**

When migrating to the cloud, some customers look to retain their existing appliances, and the skills and processes they have built around them. Using Gateway Load Balancer, customers deploy appliances from their preferred vendor while taking advantage of the scale and flexibility of running in the cloud.

**AWS Auto Scaling**

AWS Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Using AWS Auto Scaling, it’s easy to setup application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources including Amazon EC2 instances and Spot Fleets, Amazon ECS tasks, Amazon DynamoDB tables and indexes, and Amazon Aurora Replicas. AWS Auto Scaling makes scaling simple with recommendations that allow you to optimize performance, costs, or balance between them. If you’re already using Amazon EC2 Auto Scaling to dynamically scale your Amazon EC2 instances, you can now combine it with AWS Auto Scaling to scale additional resources for other AWS services. With AWS Auto Scaling, your applications always have the right resources at the right time.

**Benefits**

**SETUP SCALING QUICKLY**

AWS Auto Scaling lets you set target utilization levels for multiple resources in a single, intuitive interface. You can quickly see the average utilization of all of your scalable resources without having to navigate to other consoles. For example, if your application uses Amazon EC2 and Amazon DynamoDB, you can use AWS Auto Scaling to manage resource provisioning for all of the EC2 Auto Scaling groups and database tables in your application.

**MAKE SMART SCALING DECISIONS**

AWS Auto Scaling lets you build scaling plans that automate how groups of different resources respond to changes in demand. You can optimize availability, costs, or a balance of both. AWS Auto Scaling automatically creates all of the scaling policies and sets targets for you based on your preference. AWS Auto Scaling monitors your application and automatically adds or removes capacity from your resource groups in real-time as demands change.

**AUTOMATICALLY MAINTAIN PERFORMANCE**

Using AWS Auto Scaling, you maintain optimal application performance and availability, even when workloads are periodic, unpredictable, or continuously changing. AWS Auto Scaling continually monitors your applications to make sure that they are operating at your desired performance levels. When demand spikes, AWS Auto Scaling automatically increases the capacity of constrained resources so you maintain a high quality of service.

**PAY ONLY FOR WHAT YOU NEED**

AWS Auto Scaling can help you optimize your utilization and cost efficiencies when consuming AWS services so you only pay for the resources you actually need. When demand drops, AWS Auto Scaling will automatically remove any excess resource capacity so you avoid overspending. AWS Auto Scaling is free to use, and allows you to optimize the costs of your AWS environment.

**How it works**

## aws-auto-scaling-how-it-works-diagram

## Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) is an easy to use, high-performance, block-storage service designed for use with Amazon Elastic Compute Cloud (EC2) for both throughput and transaction intensive workloads at any scale. A broad range of workloads, such as relational and non-relational databases, enterprise applications, containerized applications, big data analytics engines, file systems, and media workflows are widely deployed on Amazon EBS. You can choose from six different volume types to balance optimal price and performance. You can achieve single-digit-millisecond latency for high-performance database workloads such as SAP HANA or gigabyte per second throughput for large, sequential workloads such as Hadoop. You can change volume types, tune performance, or increase volume size without disrupting your critical applications, so you have cost-effective storage when you need it. Designed for mission-critical systems, EBS volumes are replicated within an Availability Zone (AZ) and can easily scale to petabytes of data. Also, you can use EBS Snapshots with automated lifecycle policies to back up your volumes in Amazon S3, while ensuring geographic protection of your data and business continuity.

**Benefits**

**Performance for any workload**

EBS volumes are performant for your most demanding workloads, including mission-critical applications such as SAP, Oracle, and Microsoft products. SSD-backed options include a volume designed for high performance applications and a general-purpose volume that offers strong price/performance for most workloads. Customers who want to drive higher performance can attach their EBS volumes to Amazon EC2 R5b instances to get up to 60 Gbps bandwidth and 260K IOPS (input/output operations per second) of performance, the fastest block storage performance on EC2. For large, sequential workloads such as big data analytics engines, log processing, and data warehousing, customers can use HDD-backed volumes. Use Fast Snapshot Restore (FSR) to instantly receive full performance when creating an EBS volume from a snapshot.

**Highly available and durable**

Amazon EBS architecture offers reliability for mission-critical applications. EBS volumes are designed to protect against failures by replicating within the Availability Zone (AZ), offering 99.999% availability. EBS offers a high-durability volume (io2) for customers that need 99.999% durability, especially for their business-critical applications. All other EBS volumes are designed to deliver 99.8% - 99.9% durability. For simple and robust backup, use EBS Snapshots with Amazon Data Lifecycle Manager (DLM) policies to automate snapshot management.

**Cost-effective**

EBS offers six different volumes at various price points and performance benchmarks, enabling you to optimize costs and invest in a precise level of storage for your application needs. Options range from highly-cost-effective, dollar-per-gigabyte volumes to high-performance volumes with high IOPS and high throughput designed for mission-critical workloads. With up to a 20% lower price point per GB than gp2, gp3 volumes provide you with high-performance SSD storage and the ability to provision more IOPS without adding more storage capacity. Additionally, EBS offers backups using EBS Snapshots that are incremental and save on storage costs by not duplicating data.

**Easy to Use**

Amazon EBS volumes are easy to create, use, encrypt, and protect. Elastic Volumes capability allows you to increase storage, tune performance up and down, and change volume types without any disruption to your workloads. EBS Snapshots allow you to easily take backups of your volumes for geographic protection of your data. Data Lifecycle Manager (DLM) is an easy-to-use tool for automating snapshot management without any additional overhead or cost.

**Virtually unlimited scale**

Amazon EBS enables you to increase storage without any disruption to your critical workloads, build applications that require as little as a single GB of storage, or scale up to petabytes of data — all in just a few clicks. Snapshots can be used to quickly restore new volumes across a region's Availability Zones, enabling rapid scale.

**Secure**

EBS is built to be secure for data compliance. Newly-created EBS volumes can be encrypted by default with a single setting in your account. EBS volumes support encryption of data at rest, data in transit, and all volume backups. EBS encryption is supported by all volume types, includes built-in key management infrastructure, and has zero impact on performance.

**Amazon Elastic File System (Amazon EFS)**

Amazon Elastic File System (Amazon EFS) provides a simple, serverless, set-and-forget, elastic file system that lets you share file data without provisioning or managing storage. It can be used with AWS Cloud services and on-premises resources, and is built to scale on demand to petabytes without disrupting applications. With Amazon EFS, you can grow and shrink your file systems automatically as you add and remove files, eliminating the need to provision and manage capacity to accommodate growth.

Amazon EFS offers you the choice of creating file systems using Standard or One Zone storage classes. Standard storage classes store data within and across multiple availability zones (AZ). One Zone storage classes store data redundantly within a single AZ, at a 47% lower price compared to file systems using Standard storage classes, for workloads that don’t require multi-AZ resilience.

Amazon EFS offers four storage classes: two Standard storage classes, Amazon EFS Standard and Amazon EFS Standard-Infrequent Access (EFS Standard-IA), and two One Zone storage classes, Amazon EFS One Zone, and Amazon EFS One Zone-Infrequent Access (EFS One Zone-IA).

Amazon EFS is designed to provide massively parallel shared access to thousands of Amazon EC2 instances, and AWS containers and serverless compute services including Amazon Elastic Container Service (ECS), Amazon Elastic Kubernetes Service (EKS), AWS Fargate, and AWS Lambda, enabling your applications to achieve high levels of aggregate throughput and IOPS with consistent low latencies.

**Benefits**

* POSIX-compliant shared file storage
* Scalable performance
* Dynamic elasticity
* Fully managed
* Cost-effective
* Security and compliance

**Amazon Relational Database Service (Amazon RDS)**

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security and compatibility they need.

Amazon RDS is available on several database instance types - optimized for memory, performance or I/O - and provides you with six familiar database engines to choose from, including Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server.

**Benefits**

**Easy to administer**

Amazon RDS makes it easy to go from project conception to deployment. Use the Amazon RDS Management Console, the AWS RDS Command-Line Interface, or simple API calls to access the capabilities of a production-ready relational database in minutes. No need for infrastructure provisioning, and no need for installing and maintaining database software.

**Highly scalable**

You can scale your database's compute and storage resources with only a few mouse clicks or an API call, often with no downtime. Many Amazon RDS engine types allow you to launch one or more Read Replicas to offload read traffic from your primary database instance.

**Available and durable**

Amazon RDS runs on the same highly reliable infrastructure used by other Amazon Web Services. When you provision a Multi-AZ DB Instance, Amazon RDS synchronously replicates the data to a standby instance in a different Availability Zone (AZ). Amazon RDS has many other features that enhance reliability for critical production databases, including automated backups, database snapshots, and automatic host replacement.

**Fast**

Amazon RDS supports the most demanding database applications. You can choose between two SSD-backed storage options: one optimized for high-performance OLTP applications, and the other for cost-effective general-purpose use. In addition, Amazon Aurora provides performance on par with commercial databases at 1/10th the cost.

**Secure**

Amazon RDS makes it easy to control network access to your database. Amazon RDS also lets you run your database instances in Amazon Virtual Private Cloud (Amazon VPC), which enables you to isolate your database instances and to connect to your existing IT infrastructure through an industry-standard encrypted IPsec VPN. Many Amazon RDS engine types offer encryption at rest and encryption in transit.

**Inexpensive**

You pay very low rates and only for the resources you actually consume. In addition, you benefit from the option of On-Demand pricing with no up-front or long-term commitments, or even lower hourly rates via our Reserved Instance pricing.

**Use cases**

**Web and mobile applications**

Web and mobile applications that are built to operate at very large scale need a database with high throughput, massive storage scalability, and high availability. Amazon RDS fulfills the needs of such highly demanding applications with room for future growth. Since Amazon RDS does not have any licensing constraints, it perfectly fits the variable usage pattern of these applications.

Airbnb chose Amazon RDS because it simplifies much of the time-consuming administrative tasks typically associated with databases. Airbnb uses Multi-Availability Zone (Multi-AZ) deployment to further automate its database replication and augment data durability. Airbnb was able to complete its entire database migration to Amazon RDS with only 15 minutes of downtime.

**Ecommerce applications**

Amazon RDS offers small and large ecommerce businesses a flexible, secured, highly scalable, and low-cost database solution for online sales and retailing. Amazon RDS provides a managed database offering helping ecommerce companies meet PCI compliance and focus on building high quality customer experiences without worrying about managing the underlying database.

To avoid the complexities of building a new production database from scratch, Instacart turned to Amazon RDS for their new same-day grocery delivery service. The company can now add millions of new items to its database every month and its engineering team can focus on developing new features and improving the overall customer experience.

**Mobile and online games**

Mobile and Online games need a database platform with high throughput and availability. Amazon RDS manages the database infrastructure so game developers don’t have to worry about provisioning, scaling, or monitoring database servers. Amazon RDS provides familiar database engines that can rapidly grow capacity to meet user demand.

Bandai Namco Studios uses Amazon RDS to provide better performance, lower costs, better security, and greater availability for their arcade, social and mobile games. Bandai Namco saw the benefit in terms of reductions in overhead, especially when it came to adding, modifying, and removing server resources.

**Amazon Aurora**

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases.

Amazon Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases. It provides the security, availability, and reliability of commercial databases at 1/10th the cost. Amazon Aurora is fully managed by Amazon Relational Database Service (RDS), which automates time-consuming administration tasks like hardware provisioning, database setup, patching, and backups.

Amazon Aurora features a distributed, fault-tolerant, self-healing storage system that auto-scales up to 128TB per database instance. It delivers high performance and availability with up to 15 low-latency read replicas, point-in-time recovery, continuous backup to Amazon S3, and replication across three Availability Zones (AZs).

**Benefits**

* High Performance and Scalability
* High Availability and Durability
* Highly Secure
* MySQL and PostgreSQL Compatible
* Fully Managed
* Migration Support

**Use cases**

* Enterprise Applications
* Software as a Service (SaaS) Applications
* Web and Mobile Gaming

**Amazon ElastiCache**

Amazon ElastiCache allows you to seamlessly set up, run, and scale popular open-source compatible in-memory data stores in the cloud. Build data-intensive apps or boost the performance of your existing databases by retrieving data from high throughput and low latency in-memory data stores. Amazon ElastiCache is a popular choice for real-time use cases like Caching, Session Stores, Gaming, Geospatial Services, Real-Time Analytics, and Queuing.

Amazon ElastiCache offers fully managed Redis, voted the most loved database by developers in the Stack Overflow 2020 Developer Survey, and Memcached for your most demanding applications that require sub-millisecond response times.

**Benefits**

**Extreme performance**

Amazon ElastiCache works as an in-memory data store and cache to support the most demanding applications requiring sub-millisecond response times. By utilizing an end-to-end optimized stack running on customer dedicated nodes, Amazon ElastiCache provides secure, blazing fast performance.

**Fully managed**

You no longer need to perform management tasks such as hardware provisioning, software patching, setup, configuration, monitoring, failure recovery, and backups. ElastiCache continuously monitors your clusters to keep your workloads up and running so that you can focus on higher value application development.

**Scalable**

Amazon ElastiCache can scale-out, scale-in, and scale-up to meet fluctuating application demands. Write and memory scaling is supported with sharding. Replicas provide read scaling.

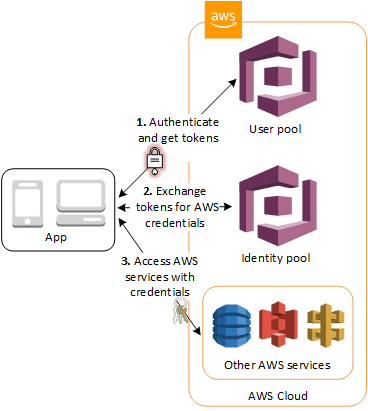
## ****Module VII****

**Amazon Cognito**

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps.Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.   The two main components of Amazon Cognito are user pools and identity pools. User pools are user directories that provide sign-up and sign-in options for your app users. Identity pools enable you to grant your users access to other AWS services. You can use identity pools and user pools separately or together.

**An Amazon Cognito user pool and identity pool used together**

1. In the first step your app user signs in through a user pool and receives user pool tokens after a successful authentication.
2. Next, your app exchanges the user pool tokens for AWS credentials through an identity pool.
3. Finally, your app user can then use those AWS credentials to access other AWS services such as Amazon S3 or DynamoDB.



## Features of Amazon Cognito

**User pools**

A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito, or federate through a third-party identity provider (IdP). Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.

User pools provide:

* Sign-up and sign-in services.
* A built-in, customizable web UI to sign in users.
* Social sign-in with Facebook, Google, Login with Amazon, and Sign in with Apple, and through SAML and OIDC identity providers from your user pool.
* User directory management and user profiles.
* Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
* Customized workflows and user migration through AWS Lambda triggers.

**Identity pools**

With an identity pool, your users can obtain temporary AWS credentials to access AWS services, such as Amazon S3 and DynamoDB. Identity pools support anonymous guest users, as well as the following identity providers that you can use to authenticate users for identity pools:

* Amazon Cognito user pools
* Social sign-in with Facebook, Google, Login with Amazon, and Sign in with Apple
* OpenID Connect (OIDC) providers
* SAML identity providers
* Developer authenticated identities

To save user profile information, your identity pool needs to be integrated with a user pool.

**AWS Key Management Service (KMS)**

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

**Benefits**

**Fully managed**

You control access to your encrypted data by defining permissions to use keys while AWS KMS enforces your permissions and handles the durability and physical security of your keys.

**Centralized key management**

AWS KMS presents a single control point to manage keys and define policies consistently across integrated AWS services and your own applications. You can easily create, import, rotate, delete, and manage permissions on keys from the AWS Management Console or by using the AWS SDK or CLI.

**Manage encryption for AWS services**

AWS KMS is integrated with AWS services to simplify using your keys to encrypt data across your AWS workloads. You choose the level of access control that you need, including the ability to share encrypted resources between accounts and services. KMS logs all use of keys to AWS CloudTrail to give you an independent view of who accessed your encrypted data, including AWS services using them on your behalf.

**Encrypt data in your applications**

AWS KMS is integrated with the AWS Encryption SDK to enable you to used KMS-protected data encryption keys to encrypt locally within your applications. Using simple APIs you can also build encryption and key management into your own applications wherever they run.

**Digitally sign data**

AWS KMS enables you to perform digital signing operations using asymmetric key pairs to ensure the integrity of your data. Recipients of digitally signed data can verify the signatures whether they have an AWS account or not.

**Low cost**

There is no commitment and no upfront charges to use AWS KMS. You only pay US $1/month to store any key that you create. AWS managed keys that are created on your behalf by AWS services are free to store. You are charged per-request when you use or manage your keys beyond the free tier.

**Secure**

AWS KMS uses hardware security modules (HSMs) that have been validated under FIPS 140-2, or are in the process of being validated, to generate and protect keys. Your keys are only used inside these devices and can never leave them unencrypted. KMS keys are never shared outside the AWS region in which they were created.

**Compliance**

The security and quality controls in AWS KMS have been certified under multiple compliance schemes to simplify your own compliance obligations. AWS KMS provides the option to store your keys in single-tenant HSMs in AWS CloudHSM instances that you control.

**Built-in auditing**

AWS KMS is integrated with AWS CloudTrail to record all API requests, including key management actions and usage of your keys. Logging API requests helps you manage risk, meet compliance requirements and conduct forensic analysis.