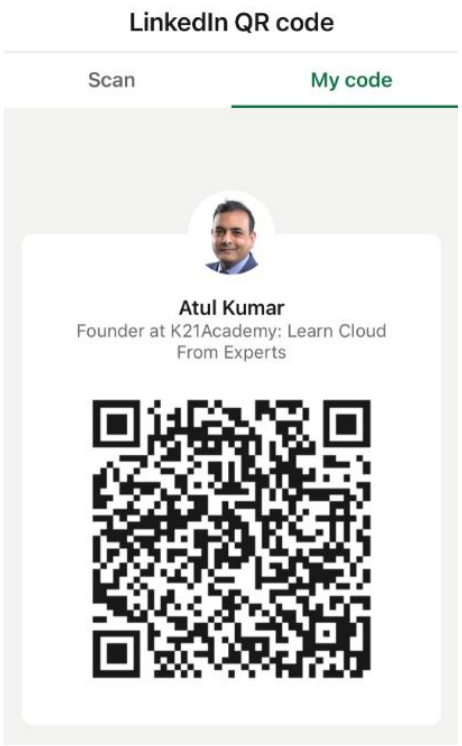
K21Academy
Learn Cloud from Experts

amazon web services

Security Management In AWS

Atul Kumar



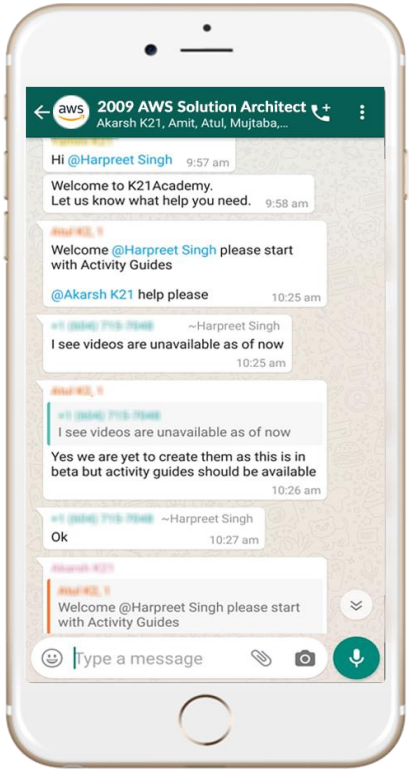
- Author & Cloud Architect
- 21+ Years working in IT & Certified Cloud Architect
- Helped **8500+ individuals** to learn Cloud & Cloud Native

WhatsApp & Ticketing System

K21Academy
Learn Cloud from Experts

support@k21academy.com

zendesk



Module Agenda

Agenda: Module

- Shared Responsibility Model
- AWS Identity & Access Management
- IAM Components
- IAM Federation
- Best Practices for IAM
- IAM Delegation And Audit
- Identity and Credit Management
- AWS Cognito
- AWS WAF, Shield & GuardDuty
- AWS KMS
- Accessing Billing
- AWS Alerts

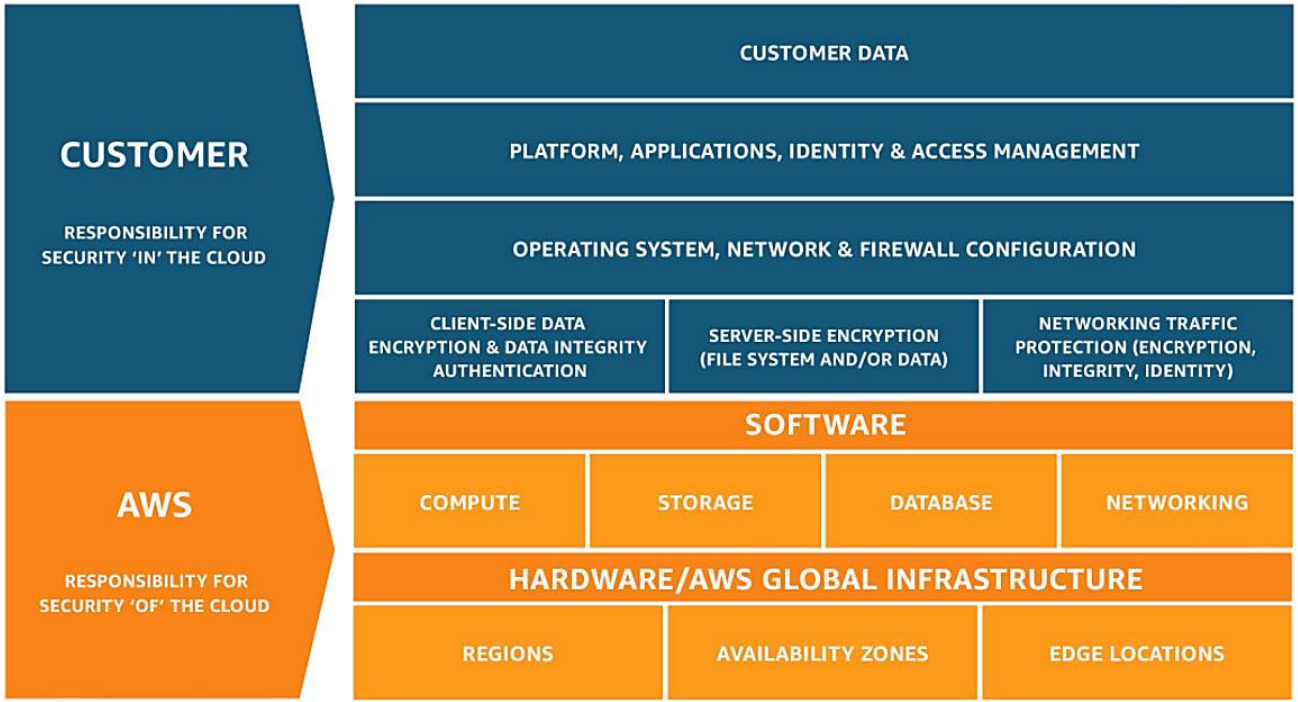
Shared Responsibility Model

Shared Responsibility Model

K21Academy
Learn Cloud from Experts

- AWS responsibility - Security of the Cloud
  - Protecting infrastructure (hardware, software, facilities, and networking) that all of the AWS services.
  - Managed services like S3, DynamoDB, RDS etc
- Customer responsibility - Security in the Cloud
  - For EC2 instance, customer is responsible for management of the guest OS (including security patches and updates), firewall & network configuration, IAM etc.

Shared Responsibility Model



K21Academy
Learn Cloud from Experts

Identity & Access Management

AWS IAM

- IAM is a preventative security control.
- It can create and manage AWS users and groups and use permissions to allow and deny access to AWS resources
- IAM deals with 4 terms such as users, groups, Roles and Policies.
- It controls both centralized and fine grained-API resources plus management console.

Why Use IAM?

K21Academy
Learn Cloud from Experts

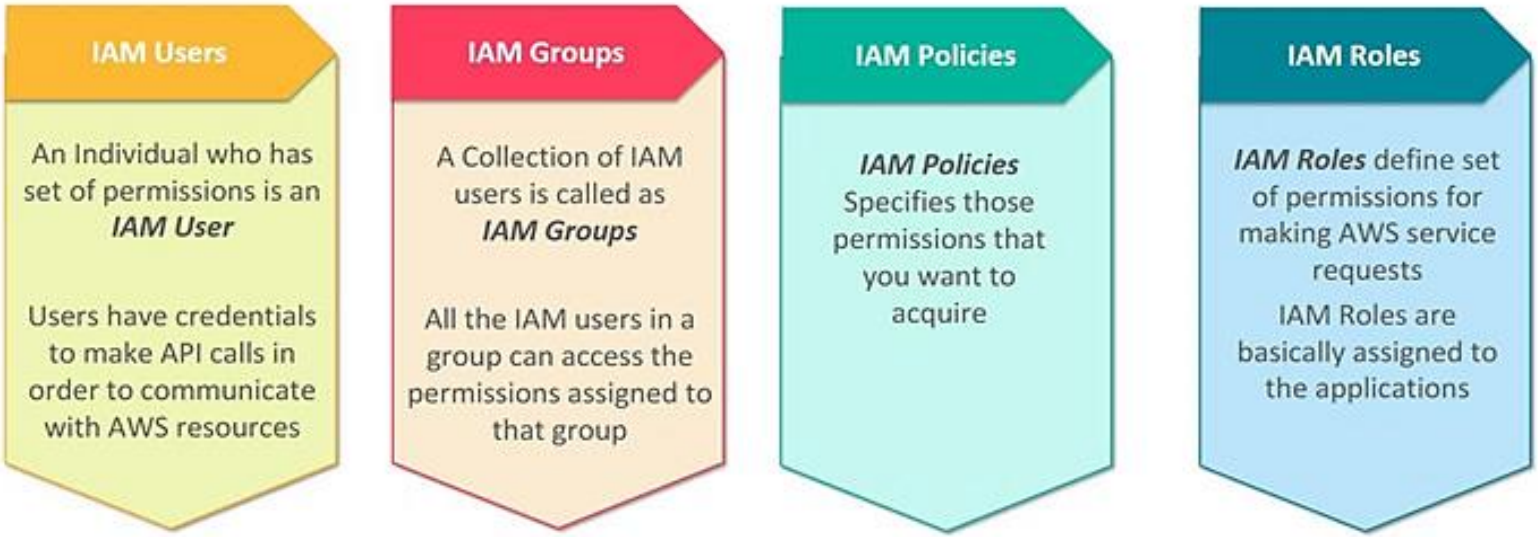
- You can specify permissions to control which operations a user or role can perform on AWS resources
- IAM service provides access to the AWS Management Console, AWS API, and AWS Command-Line Interface (CLI)

Note: IAM does ***not*** provide authentication for your OS or application

K21Academy
Learn Cloud from Experts

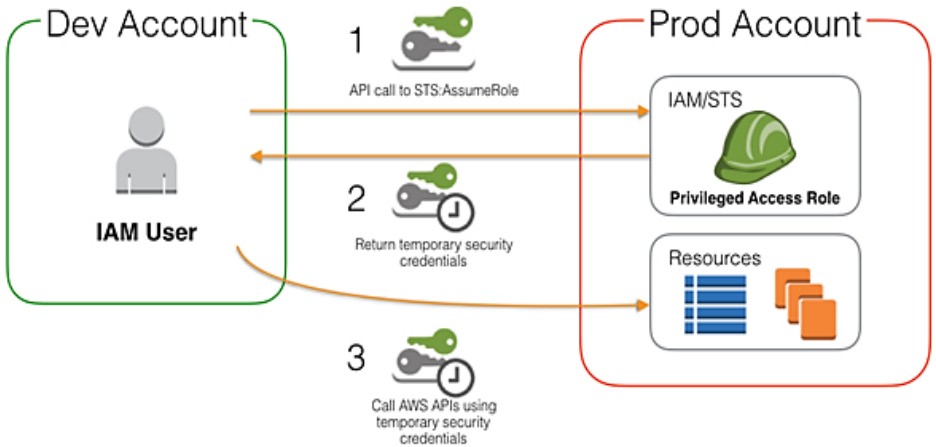
IAM Components

IAM Components



IAM Users

- IAM users can be an individual, system, or application requiring access to AWS services
- A user account consists of a unique name and security credentials such as a password, access key, and/or multi-factor authentication (MFA)
- IAM users only need passwords when they access the AWS Management Console



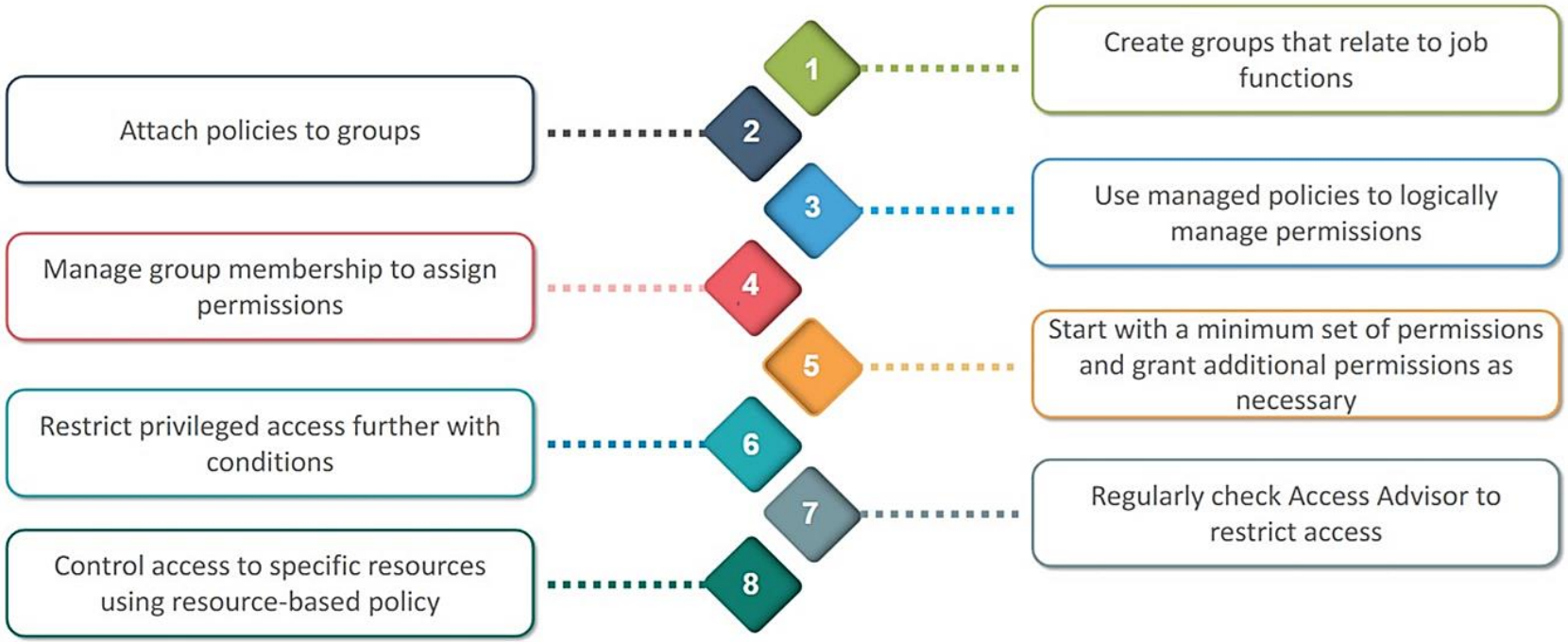
IAM Groups

K21Academy
Learn Cloud from Experts

- IAM Groups are a way to assign permissions to logical and functional units of your organization
- IAM groups are a tool to help with operational efficiency
  - Easy to change permissions as individuals change teams (portable)
  - Bulk permissions management (scalable)
- A group can contain many users, and a user can belong to multiple groups.
- Groups can't be nested; they can contain only users, not other groups.

Why Should We use Groups?

How To Manage Permissions With Groups?



IAM Policies

K21Academy
Learn Cloud from Experts

- IAM policies are JSON-based statements that define access control and permissions.
- IAM policies can be “inline” or “managed” and can be attached to a user or a group
- Inline policies - policies that you create and manage, and that are embedded directly into a single user, group, or role.
- Managed policies - standalone policies that you can manage separately from the IAM users, groups, or roles to which they are attached.
  - AWS managed policies
  - Customer managed policies

Elements of An IAM Policy

K21Academy
Learn Cloud from Experts

- Version – Specifies current version of the policy language.
- Statement – Contain array of elements.
- Effect – Whether the statement will result in an allow or an explicit deny.
- Action – Describes the specific action or actions that will be allowed or denied.
- Resource – Specifies the object or objects that the statement covers.
- Principal – Principal element specifies the identity.

Elements of IAM Policy - Example

K21Academy
Learn Cloud from Experts

- Sample JSON

```
{
  "Version": "2012-10-18",
  "Statement":{
    "Effect": "Allow",
    "Action": "s3:ListBucket",
   "Resource":"arn:aws:s3:::example_bucket"
  }
}
```

IAM Roles

K21Academy
Learn Cloud from Experts

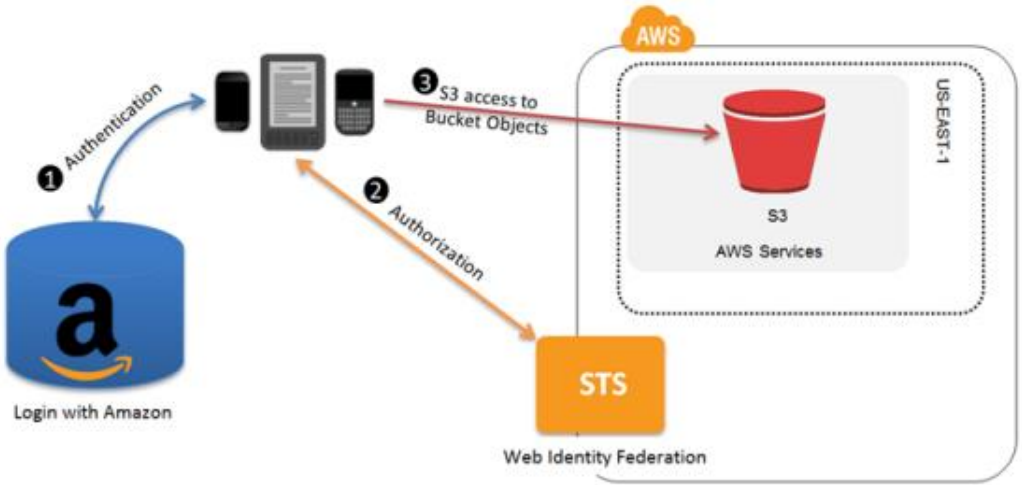
- An IAM role is like a user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.
- You can authorize roles to be assumed by humans, Amazon EC2 instances, custom code, or other AWS services for specific access to services.
- Roles do not have standard long-term credentials such as password or access keys associated to it, instead when you assume a role, it provides you with temporary security credentials for your role session.

K21Academy
Learn Cloud from Experts

IAM Federation

IAM Federation

- Big enterprises usually integrate their own repository of users with IAM.
- This way, one can login into AWS using their company credentials.
- Identity Federation uses the SAML standard (Active Directory).



K21Academy
Learn Cloud from Experts

IAM
Best Practices

IAM Best Practices

- Lock away your AWS account (root) access keys
- Create individual IAM users
- Use groups to assign permissions to IAM users
- Grant least privilege
- Configure a strong policy for your users
- Enable MFA for privileged users

IAM Best Practices

- Use roles for applications that run on Amazon EC2 instances
- Delegate by using roles instead of by sharing credentials
- Rotate credentials regularly
- Remove unnecessary credentials
- Use policy conditions for extra security
- Monitor activity in your AWS Account

IAM Best Practices

K21Academy
Learn Cloud from Experts

Grant Least Privileges

This reduces the chances of more people committing the mistakes and provides a good granular control

Manage permission with Groups

It is one of the simple and efficient medium to provide access or to deny access to multiple users at a time

Restrict privileged access further with conditions

It provides additional security, hence reduces the chances of accidentally performing privileged actions

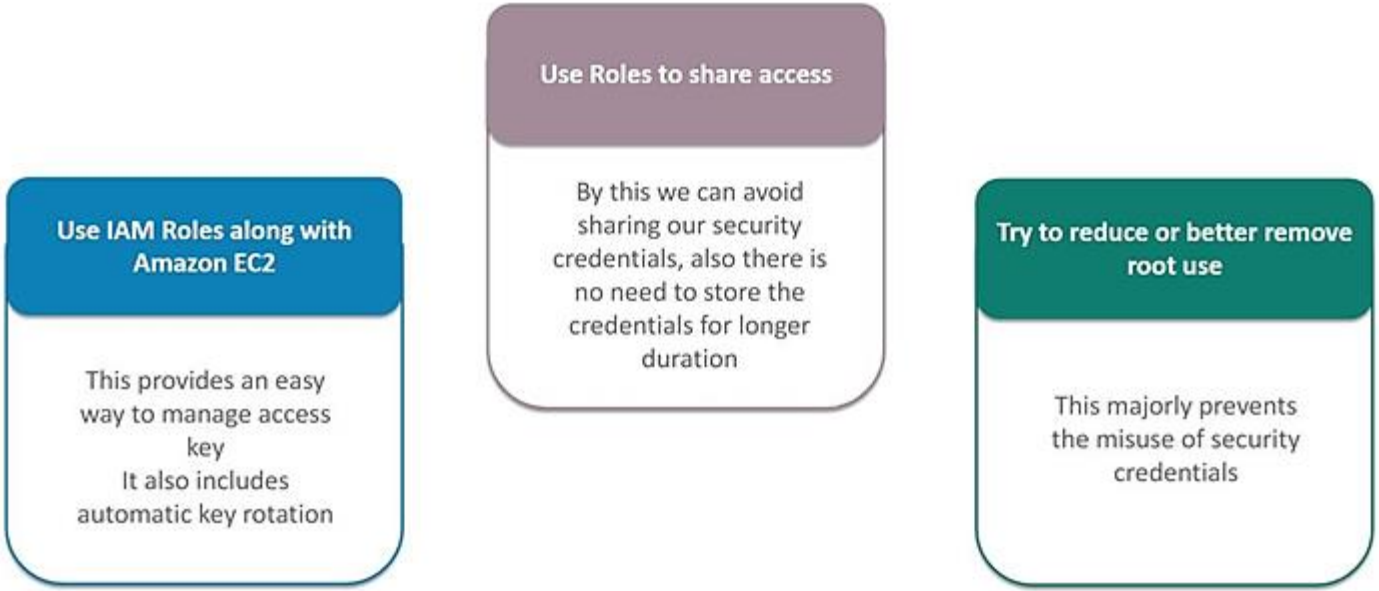
Always enable AWS CloudTrail to be aware of API call logs

This provides a clear view of all your user activity by recording all API calls done to an S3 bucket

K21Academy
Learn Cloud from Experts

IAM
Delegation And Audit

Delegation And Audit



K21Academy
Learn Cloud from Experts

Identity and Credit Management

Identity and Credit Management

K21Academy
Learn Cloud from Experts

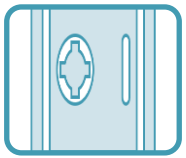
- Why Create Individual user

Benefits	How to Do it
Unique set of credential Individual permission Granular control Easy to revoke access	Create IAM user for yourself Create individual users for others

- Why configure a Strong Password Policy

Benefits	How to Do it
Ensures your user and data are protected Easy to enforce password complexity requirements Increase account resilience against brute force login attempts	Requires password expiration of 90 days Requires complex password Required password rotation policy

Identity and Credit Management



Enabling credential rotation for IAM users (Enable access key rotation sample policy) policy.

The Root account holder as well as IAM users in the account should regularly change their passwords and access keys to analyze if a password or access key is compromised without owners knowledge.

For this you can even set password policies and determine the duration of credentials validity to use resources

K21Academy
Learn Cloud from Experts

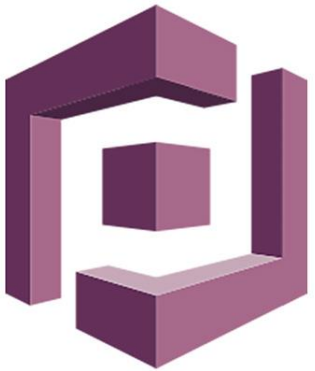
AWS Cognito

Amazon Cognito

- Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps.

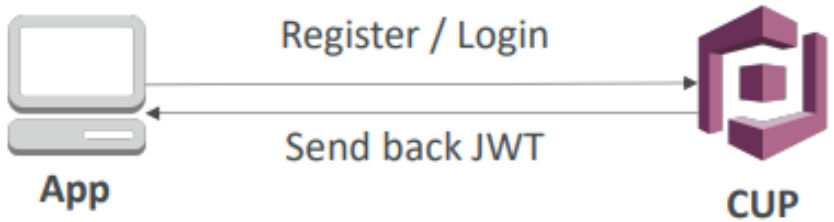
- There are Two main components of Amazon Cognito:

  - User Pools
  - Identity Pools



AWS Cognito User Pools (CUP)

- Create a serverless database of user for your mobile apps
- Simple login: Username (or email) / password combination
- Possibility to verify emails / phone numbers and add MFA
- Can enable Federated Identities (Facebook, Google, SAML)
- Sends back a JSON Web Tokens (JWT)
- Can be integrated with API Gateway for authentication

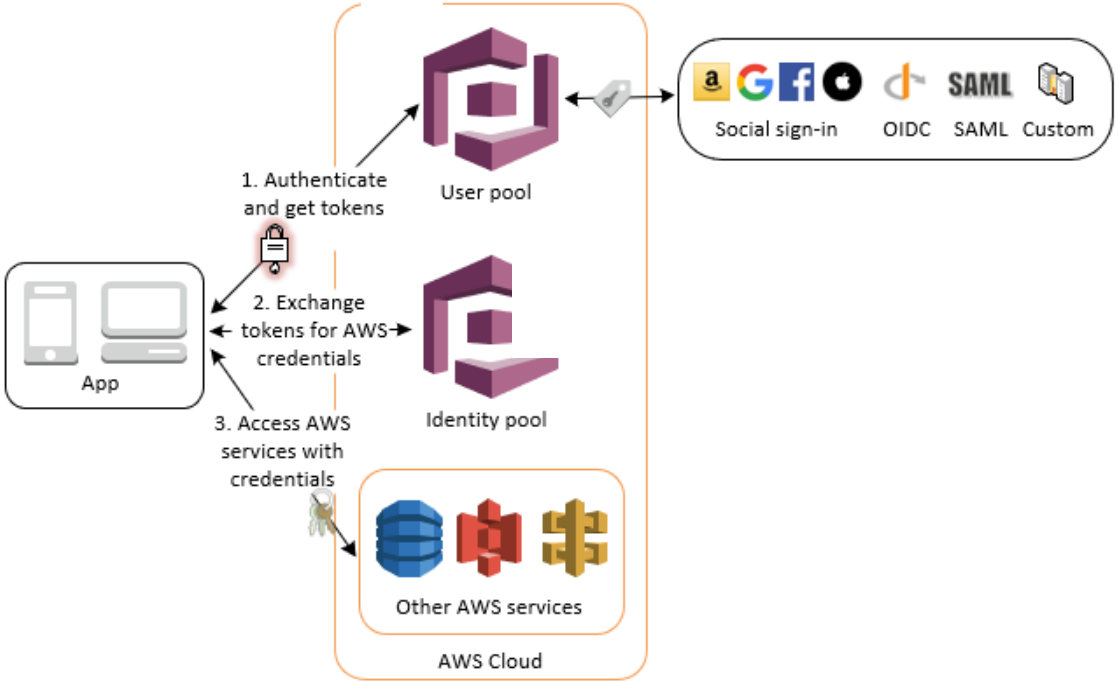


AWS Cognito – Identity Pools

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:

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

AWS Cognito – Identity Pools



K21Academy
Learn Cloud from Experts

AWS WAF, Shield & GuardDuty

Web Application Firewall (WAF)

K21Academy
Learn Cloud from Experts

WAF

WAF protects your web applications that you deliver through ELB and CloudFront from ***attacks*** by allowing you to configure rules that allows, blocks or monitor web requests based on the ***condition you define***

It protects from
SQL injection
Cross-Site Scripting (XSS)
user-agents, bad bots, or ***content scrapers by blacklisting the IPs***

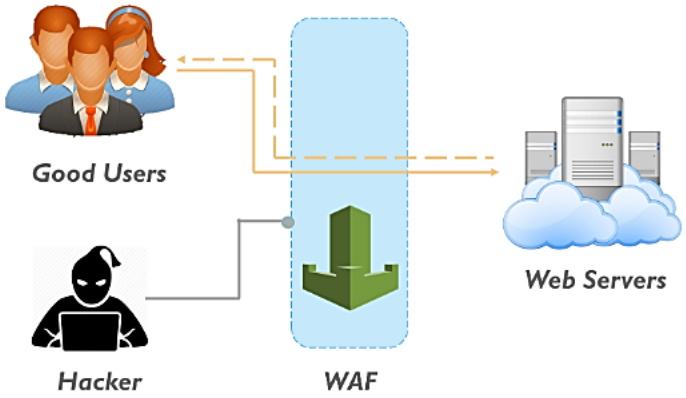


Fig: Working Of WAF

How AWS WAF Works?

K21Academy
Learn Cloud from Experts

To control web requests you can use WAF ACLs (web access control list), rules, and rules groups.

Every rule includes a statement that-

- Defines the **criteria** for inspecting web requests
- Specifies an action to be taken if a web request meets the criteria (allow, block or count)

Rules

- **IP address** that requests originate from
- **Strings** that appear in the web request
- **Country of origin** of the request
- Presence of **malicious code** or scripts

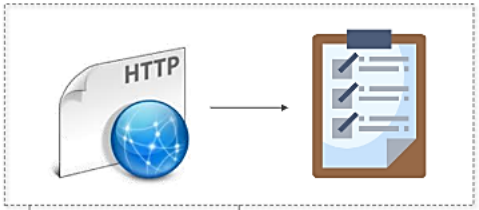
You can **combine multiple statements** in a rule using **logical statements** like AND, OR, and NOT.

Example:

- ✓ The requests come from 190.2.45.43
- ✓ Presence of malicious SQL code

Both these conditions need to be satisfied for the rule to be passed

How AWS WAF Works? Cont.



WAF compares the web request with the rules in WAF ACL in the order they are listed.

Match Occurs

- **Allow matching request**
- **Block matching requests**
- **Count matching requests**

- When there is a match, WAF executes actions – allow, block or count
- Does not proceed to evaluate with other rules that come after matching one (if any).

No Match Occurs

Default Action - determines how AWS WAF handles web requests that don't match any rules in the web ACL (allow or block).

AWS Shield

K21Academy
Learn Cloud from Experts

AWS Shield is a managed ***Distributed Denial of Service (DDoS) protection service*** that protects applications running on AWS infrastructure. It has two levels of protection -

1.AWS Shield Standard :

- It protects most common network and transport layer **DDoS attacks**
- Offers **automated mitigation techniques** that are **applied inline** to your applications
- All these features are provided by AWS Shield Standard at no additional cost

2. AWS Shield Advanced:

- It is a paid service that provides enhanced protection for applications running on EC2, ELB, CloudFront, and Route 53
- Offers real-time visibility into attacks, and integration with AWS WAF, a web application firewall
- Engage 24x7 DDoS Response Team (DRT) to manage and mitigate your application layer from DDoS attacks

Benefits of AWS Shield

Seamless integration and deployment with other AWS services. No routing changes are required.

Customizable protection. You can choose the resources that you want to protect

Cost efficient and customers get "**DDoS cost protection for scaling**" feature

Automatic **network flow monitoring, inline mitigation,** provides advanced DDoS **attack visibility** and insights

AWS GuardDuty

K21Academy
Learn Cloud from Experts

AWS GurardDuty is an intelligent threat detection service that continuously monitors for any malicious activity to protect customers' AWS accounts and workloads.

Enable Guard Duty

Without any additional security software or infrastructure to deploy or manage, you can **monitor all your AWS accounts with few clicks.**

Continuously Analyze

Automatically analyses network and account activity to detect the unauthorized and unexpected activity in your AWS account.

CloudTrail Flow Logs
VPC Flow Logs
DNS Logs

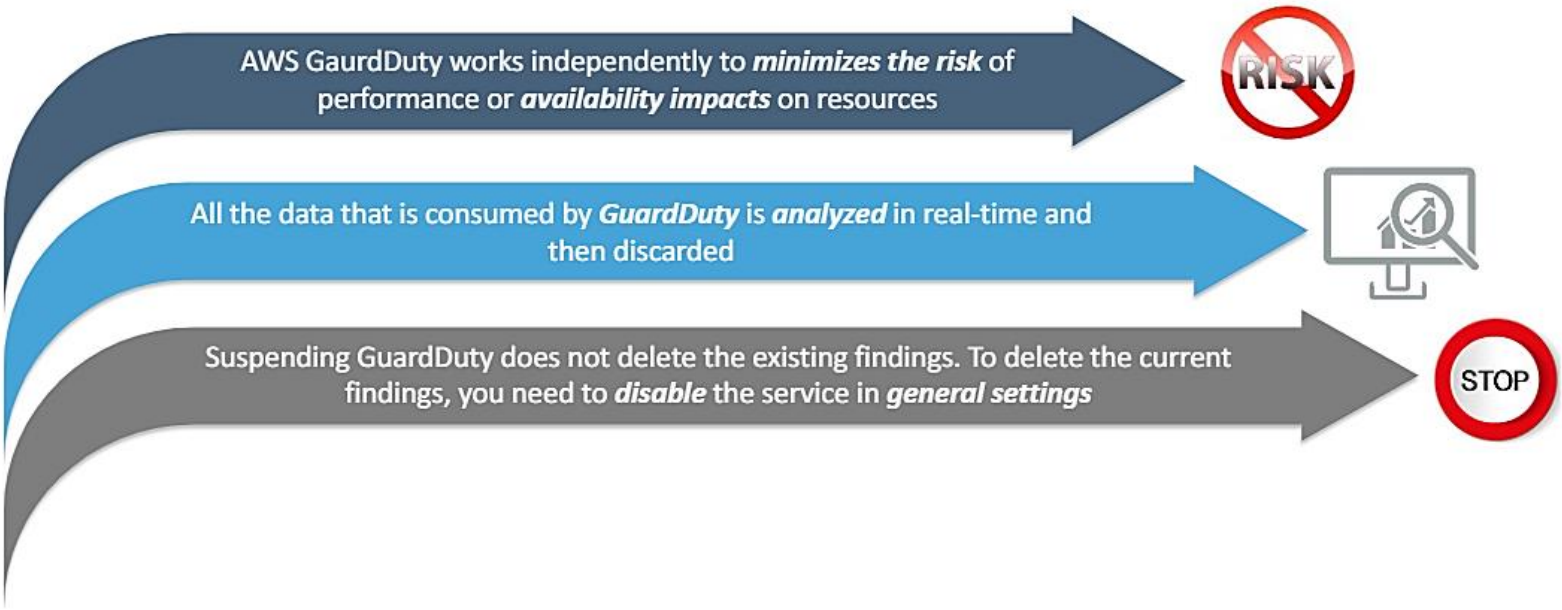
Intelligently detect threats

Guard Duty combines manged **rule-sets, threat intelligence, third party intelligence partners and ML** to detect malicious or unauthorized behavior.

Take Action

Review the detailed findings, integrate into e**vent management or trigger AWS Lambda** to automate the prevention.

Key Points of AWS GuardDuty



K21Academy
Learn Cloud from Experts

AWS Key Management Service (KMS)

Key Management Service KMS

K21Academy
Learn Cloud from Experts

- 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.

Key Management Service KMS

K21Academy
Learn Cloud from Experts

KMS is a managed encryption service that enables user to easily encrypt user data

- Creates keys with unique alias and description KMS
- Allows to Import your own keys
- Defines which IAM users and roles can manage keys
- Defines which IAM users and roles can use keys to encrypt and decrypt data
- Disable and enable keys as per requirement
- Audit use of keys by inspecting logs in AWS CloudTrail
- It provides a highly available key storage, management, and auditing solution for you to encrypt your data across AWS services

Who Can Use KMS?

Developers who need to ***encrypt data*** in their applications can use the ***AWS SDKs with AWS KMS support*** to easily use and protect encryption keys

For a ***scalable*** key management infrastructure ***IT Administrators*** can use AWS KMS to ***reduce*** their licensing ***costs*** and ***operational burden***

In case, of ***data security*** for regulatory or compliance purposes, you can use ***AWS KMS*** to ***verify data encryption*** across the application where it is used and stored

Benefits Of KMS

K21Academy
Learn Cloud from Experts

- **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.

- **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.

- **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.

Benefits Of KMS

K21Academy
Learn Cloud from Experts

- **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.

- **Compliance :** The security and quality controls in AWS KMS have been certified under multiple compliance schemes to simplify your own compliance obligations.

- **Manage encryption for AWS services :** AWS KMS is integrated with AWS services to simplify using your keys to encrypt data across your AWS workloads.

- **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.

Protecting Data Using Encryption

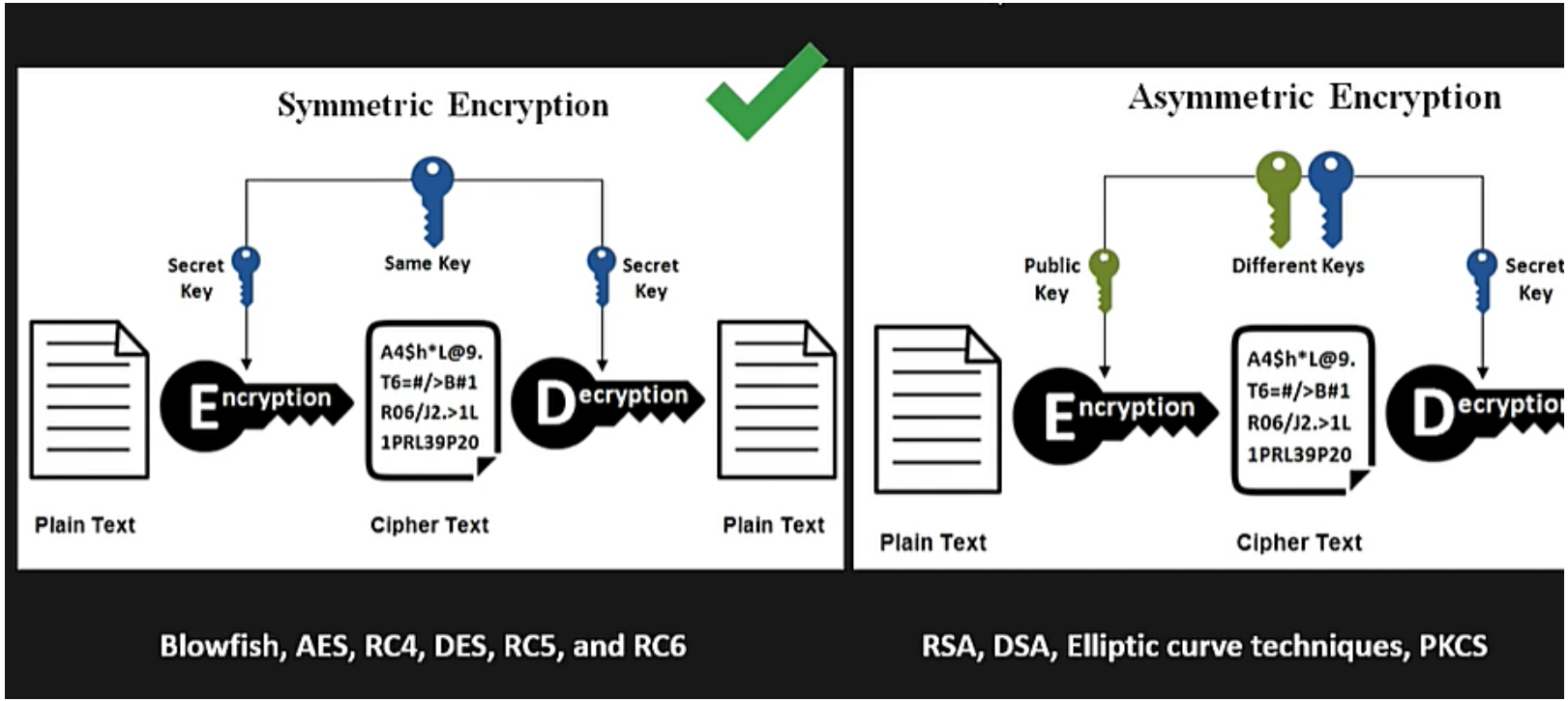
K21Academy
Learn Cloud from Experts

- Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit using Secure Socket Layer/Transport Layer Security (SSL/TLS) or client-side encryption. You have the following options for protecting data at rest in Amazon S3:

- **Server-Side Encryption** – Request Amazon S3 to encrypt your object before saving it on disks in its data centers and then decrypt it when you download the objects.

- **Client-Side Encryption** – Encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Protecting Data Using Encryption



Types of Keys In AWS

- AWS Managed keys
- Customer Managed Keys

Type of CMK	Can view CMK metadata	Can manage CMK	Used only for my AWS account	Automatic rotation
Customer managed CMK	Yes	Yes	Yes	Optional. Every 365 days (1 year).
AWS managed CMK	Yes	No	Yes	Required. Every 1095 days (3 years).
AWS owned CMK	No	No	No	Varies

Types of Keys

K21Academy
Learn Cloud from Experts

- Master Keys : is a logical representation of a master key. The CMK includes metadata, such as the key ID, creation date, description, and key state. The CMK also contains the key material used to encrypt and decrypt data. AWS KMS supports symmetric and asymmetric CMKs. A *symmetric CMK* represents a 256-bit key that is used for encryption and decryption

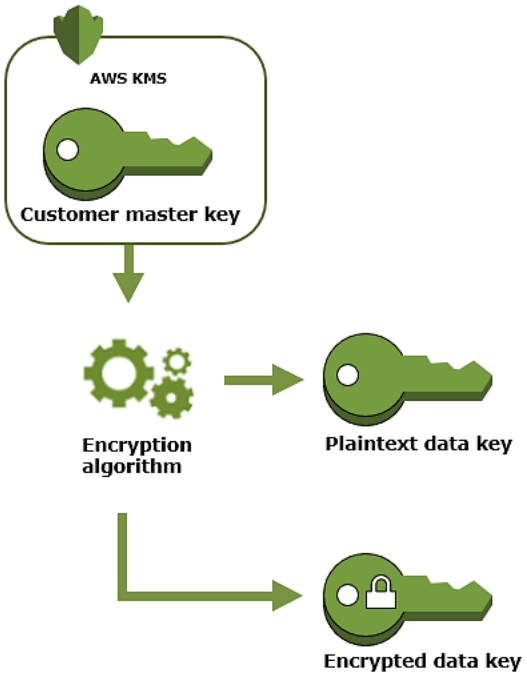
- Data Keys : *Data keys* are encryption keys that you can use to encrypt data, including large amounts of data and other data encryption keys.

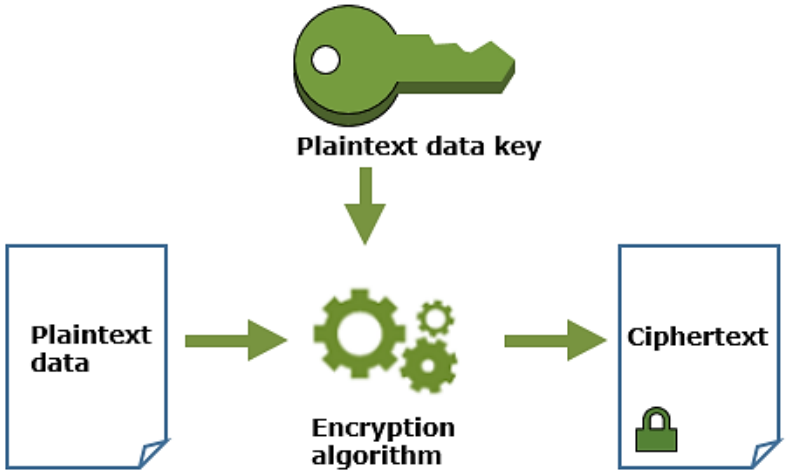
Types of Keys

AWS KMS supports three types of CMKs: customer managed CMKs, AWS managed CMKs, and AWS owned CMKs.

Type of CMK	Can view CMK metadata	Can manage CMK	Used only for my AWS account	Automatic rotation
Customer managed CMK	Yes	Yes	Yes	Optional. Every 365 days (1 year).
AWS managed CMK	Yes	No	Yes	Required. Every 1095 days (3 years).
AWS owned CMK	No	No	No	Varies

Types of Keys



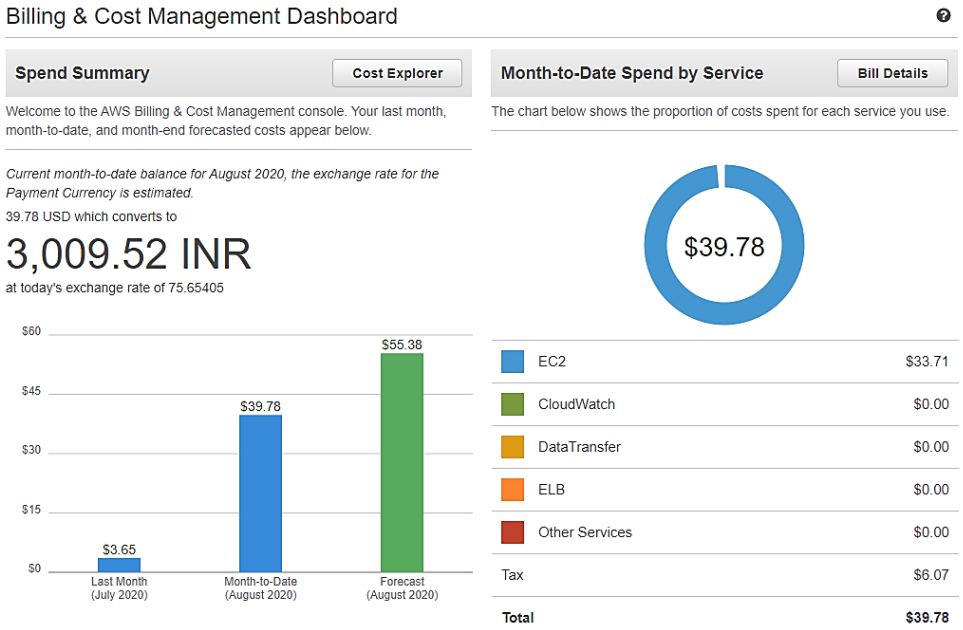


K21Academy
Learn Cloud from Experts

Accessing Billing

AWS Billings

- AWS Billing is the service that you use to pay your AWS bill, monitor your usage, and analyze and control your costs.
- AWS automatically charges the credit card or debit card that you provided when you signed up for a new account with AWS. Charges appear on your monthly card bill.



K21Academy
Learn Cloud from Experts

AWS Alerts

What Are AWS Alerts?

- AWS allows you to ***create an alarm*** for your estimated charges
- Enable ***Billing Alert*** before creating alarm
- Helps you ***monitor*** your estimated AWS charges
- Helps you to create an alarm using ***Billing metric data***

Lab Exercises

AWS Identity and Access Management (IAM)

- Steps to create IAM users, groups, policy
- Setting an account password policy for IAM users
- Creating a role
- Multi-Factor authentication on root account

Contents

Lab Exercises

IAM Power User

- Steps to create AWS IAM Power User
- Test Access For IAM
- Test Other AWS Service Access

Contents

Lab Exercises

K21Academy
Learn Cloud from Experts

AWS Key Management Service (KMS)

- Steps to create AWS KMS Key & Use in S3
- Assign KMS Keys to Other AWS Services

Contents

Certification Sample Quiz

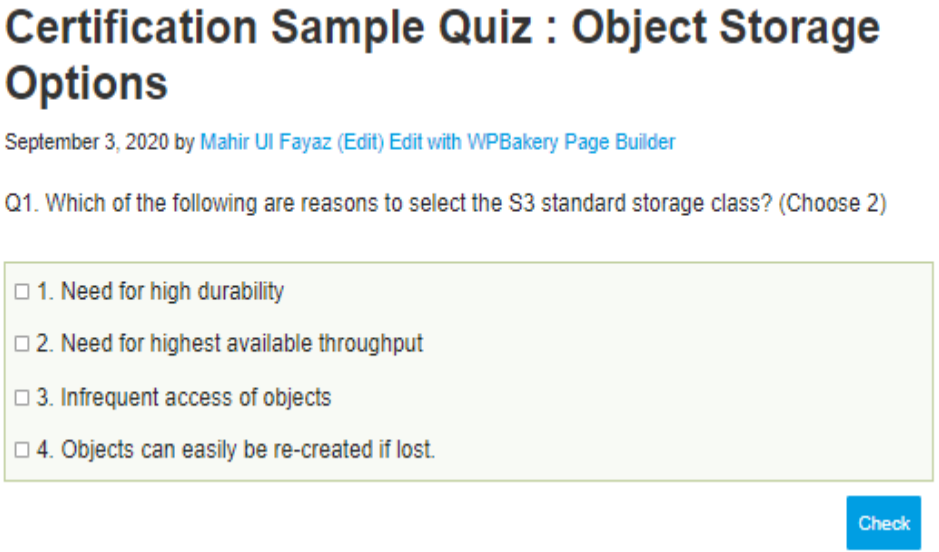
K21Academy
Learn Cloud from Experts

Quiz Section

Check out some sample exam certification quiz questions Under Module 3

Navigation

https://k21academy.com/awssaquizm03



Quiz

K21Academy
Learn Cloud from Experts

You have been tasked with replacing a legacy LDAP directory server that manages users, groups, and permissions with a cloud-based solution in order to reduce maintenance costs for the current directory server. What AWS service should you investigate?

A. IAM
B. Cognito
C. AWS Organizations
D. AWS Directory Server

Answer: A.
Explanation: IAM is the best option for handling users, groups, and permissions within AWS.

Quiz

K21Academy
Learn Cloud from Experts

You are tasked with improving security at an organization that has recently begun using the cloud. It has five developers, a financial manager, and two support engineers. Currently, all eight staff are using the AWS root user for their account. What changes would you make to improve security? (Choose two.)

A. Get all the users to download the AWS CLI and change the root password.
B. Create a new IAM user for each of the eight staff members and provide credentials to each user.
C. Put the five developers in the Power Users group, the financial manager in the Billing group, and the support engineers in the Support User group.
D. Create a new group with access to the IAM service and ensure that at least one developer is in that group.

Answer : B, C

Explanation: The biggest issue here is that all the users are using the root account, meaning there's a shared password and that users have far more permissions than they should. These can both be addressed by creating new IAM users for each user (B) and putting those users in predefined groups according to their job function (C). Developers don't need access to IAM in general, so D is incorrect, and while changing the root password is a good idea, A is also incorrect because a financial manager (and possibly support engineers) may not need the AWS CLI as their access mechanism.

Find Us

https://www.facebook.com/K21Academy

http://twitter.com/k21Academy

https://www.linkedin.com/company/k21academy

https://www.youtube.com/k21academy

https://www.instagram.com/k21academy