PW SKILLS | DevOps and Cloud Computing

AWS IAM, Security & EC2

Objective

- Understand AWS IAM concepts, including users, groups, roles, and policies.
- Learn about AWS security services for encryption, certificates, and firewalls.
- Explore Amazon EC2 instance types, launch options, and AMIs.
- Configure Auto Scaling and Elastic Load Balancing (ELB) fc high availability.
- Get an overview of serverless computing (FaaS) and AWS Lambda.

PW SKILLS

Explaining what IAM is and why it’s crucial for AWS security.

Let’s see

IAM (Identity and Access Management) is an AWS service that controls who can access what in your AWS environment.

It is crucial for AWS security because it:

- Manages user access
- Implements least privilege
- Enables secure authentication
- Audits activity

PW SKILLS

Discussing IAM users, groups, and roles, and their differences.

Let’s discuss

IAM Users, Groups, and Roles are key components in AWS IAM for managing access:

- Users: Individual identities (e.g., a person or app) with credentials to access AWS services.
- Groups: Collections of users with shared permissions for easier management.
- Roles: Identities with specific permissions that can be assumed temporarily by users, AWS services, or external identities.

Let’s discuss

Key Differences:

- Users have long-term credentials; roles use temporary credentials.
- Groups are used to organize users; roles are used to delegate access.
- Roles are ideal for cross-account access and AWS service access.

Pop Quiz

Q. Which of the following best describes an IAM user in AWS?

A

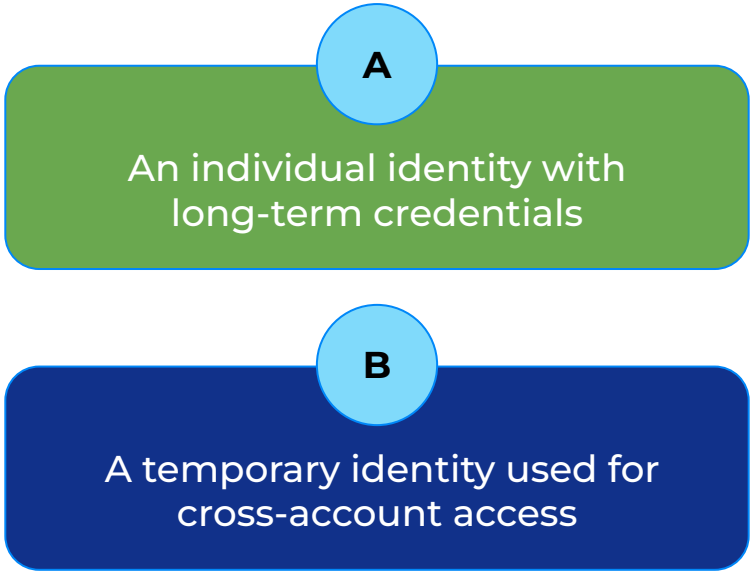
An individual identity with long-term credentials

B

A temporary identity used for cross-account access

Pop Quiz

Q. Which of the following best describes an IAM user in AWS?



PW SKILLS

Demonstrating IAM policies and how to attach them to users or roles.

Let’s do it

IAM policies are JSON documents that define permissions (allow or deny) for AWS actions on resources.

Example Policy (Read-only access to S3):

```json
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::example-bucket/*"
  }]
}
```

Let’s do it

How to Attach a Policy:

1. To a user or role via console:

- Go to IAM > Users/Roles
- Select the user/role
- Click Add permissions > Attach policies directly
- Choose a policy (e.g., AmazonS3ReadOnlyAccess) and confirm

2. Using AWS CLI:

```
aws iam attach-user-policy \
  --user-name Alice \
  --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
```

PW SKILLS

Explaining why MFA adds an extra layer of security to AWS accounts.

Let’s see

This extra layer of security is crucial because:

- Even if an attacker obtains a user's password, they cannot access the account without the second factor.
- It reduces the risk of unauthorized access from phishing, credential leaks, or brute-force attacks.
- MFA is especially important for high-privilege accounts like root users or IAM users with administrative access.

PW SKILLS

Discussing best practices for managing IAM access keys securely.

Let’s discuss

- Avoid using root access keys – create IAM users instead.
- Rotate access keys regularly to reduce risk from compromised keys.
- Use IAM roles with temporary credentials instead of long-term keys when possible.
- Never hard-code access keys in code; use environment variables or AWS credentials file.
- Delete unused keys immediately.
- Monitor key usage with AWS CloudTrail and IAM Access Analyzer.

PW SKILLS

Demonstrating enabling MFA for an IAM user and generating access keys.

Let’s do it

1. Enable MFA (via AWS Console):

- Go to IAM > Users > [User Name]
- Select Security credentials
- Under Multi-factor authentication (MFA), click Assign MFA device
- Choose Virtual MFA device, scan QR code using an authenticator app, and enter the two codes to verify

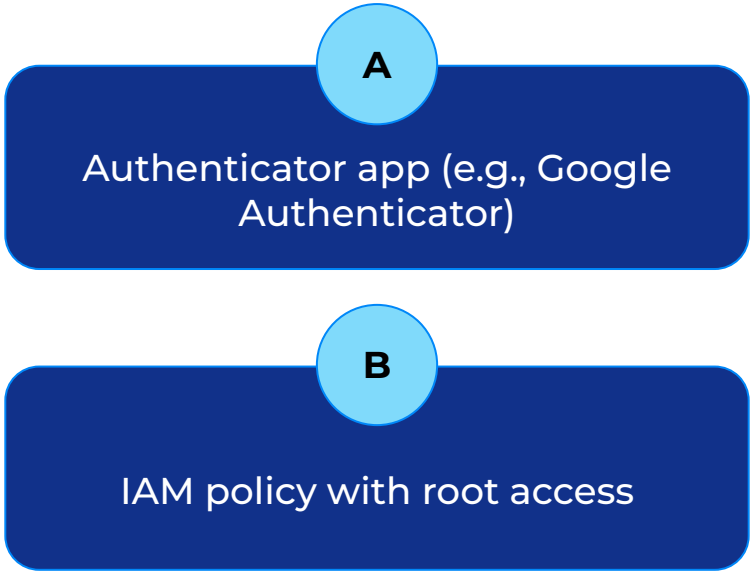
Let’s do it

2. Generate Access Keys:

- In the same Security credentials tab, go to Access keys
- Click Create access key
- Download the keys or copy them securely (they're shown only once)

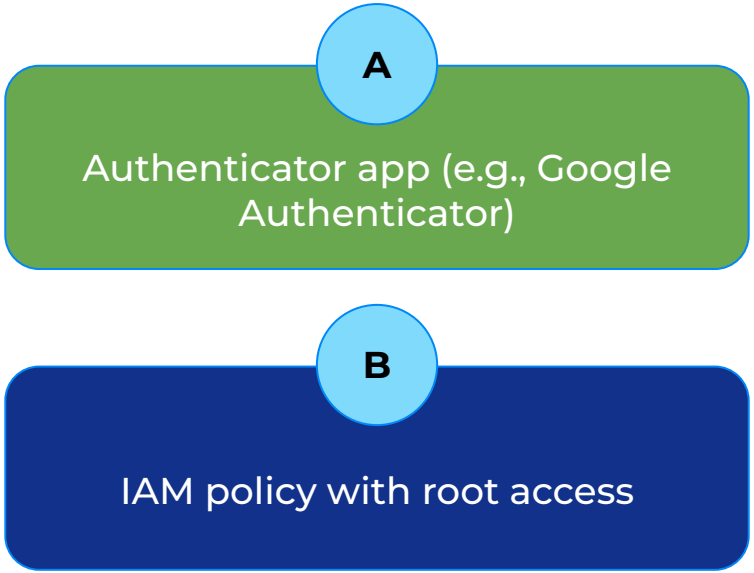
Pop Quiz

Q. Which of the following is required to enable virtual MFA for an IAM user?



Pop Quiz

Q. Which of the following is required to enable virtual MFA for an IAM user?



PW SKILLS

Explaining the role of AWS Key Management Service (KMS) in encryption and security.

Let’s see

AWS Key Management Service (KMS) helps you create, manage, and control encryption keys to protect your data.

Key roles of KMS:

- Encrypts data at rest and in transit using customer-managed keys.
- Manages key lifecycle securely (creation, rotation, deletion).
- Integrates with AWS services like S3, EBS, and RDS for seamless encryption.
- Enforces access control using IAM and key policies.

PW SKILLS

Discussing AWS Certificate Manager (ACM) for managing SSL/TLS certificates.

Let’s discuss

AWS Certificate Manager (ACM) helps you provision, manage, and deploy SSL/TLS certificates for securing websites and applications.

Key features:

- Automatic certificate renewal
- Free public certificates for use with services like CloudFront, ELB, and API Gateway
- Simplifies HTTPS setup without manual certificate handling
- Supports private certificates via ACM Private CA

PW SKILLS

Explaining AWS Web Application Firewall (WAF) for protecting web applications.

Let’s see

AWS Web Application Firewall (WAF) protects web applications by filtering and monitoring HTTP/HTTPS traffic.

Key features:

- Blocks common threats like SQL injection and XSS
- Lets you set custom rules to allow, block, or count requests
- Integrates with services like CloudFront, ALB, and API Gateway
- Helps prevent DDoS attacks and unwanted bots

Pop Quiz

Q. What is the primary function of AWS WAF?

A

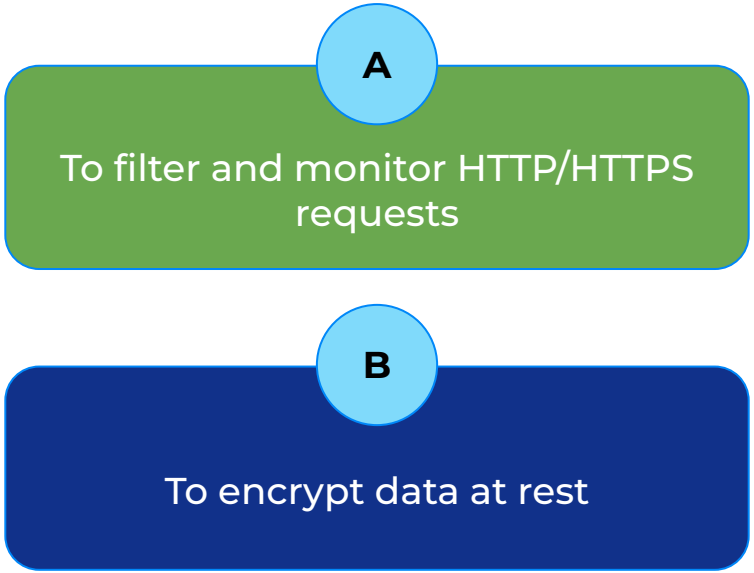
To filter and monitor HTTP/HTTPS requests

B

To encrypt data at rest

Pop Quiz

Q. What is the primary function of AWS WAF?



Take A 5-Minute Break!

- Stretch and relax
- Hydrate
- Clear your mind
- Be back in 5 minutes

PW SKILLS

Explaining what EC2 is and when to use it for compute workloads.

Let’s see

Amazon EC2 (Elastic Compute Cloud) is a service that provides resizable virtual servers in the cloud to run applications.

Use EC2 when you need:

- Full control over the operating system and software
- Custom configurations for CPU, memory, and storage
- Scalable compute power for web apps, batch jobs, or development environments

PW SKILLS

Discussing EC2 instance types and their use cases (General Purpose, Compute-Optimized, Memory-Optimized).

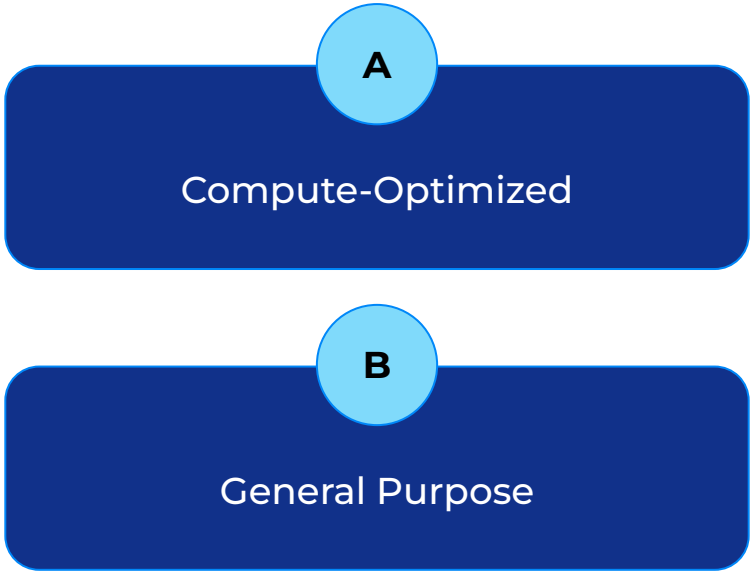
Let’s discuss

EC2 instance types and use cases:

- General Purpose (e.g., t3, m5): Balanced CPU, memory, and networking — great for web servers, small databases, and development environments.
- Compute-Optimized (e.g., c5, c6g): High CPU performance — ideal for batch processing, high-performance web servers, and scientific modeling.
- Memory-Optimized (e.g., r5, x1e): Large memory capacity — best for in-memory databases, real-time big data analytics, and caching.

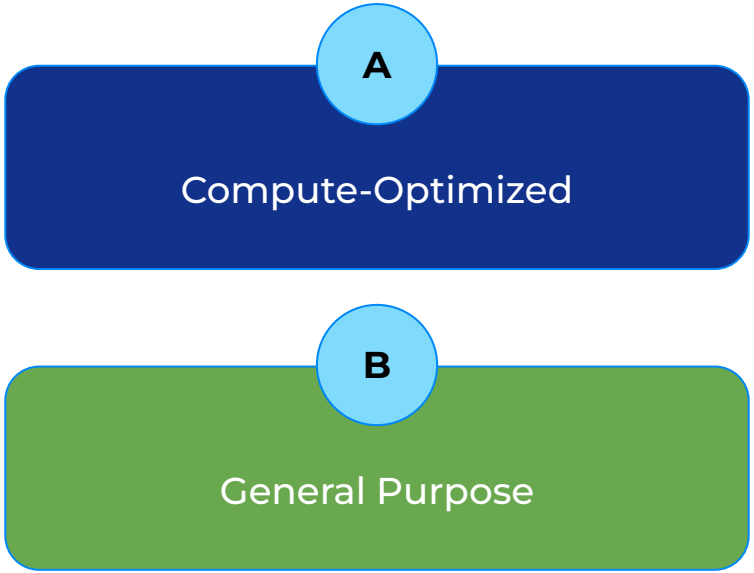
Pop Quiz

Q Which EC2 instance type is best suited for a balanced workload such as web servers and development environments?



Pop Quiz

Q Which EC2 instance type is best suited for a balanced workload such as web servers and development environments?



PW SKILLS

Demonstrating how to launch an EC2 instance using AWS Console and AWS CLI.

Let’s do it

To launch an EC2 instance:

Using AWS Console:

1. Go to EC2 Dashboard

2. Click Launch instance

3. Choose:

- Name, AMI (e.g., Amazon Linux)
- Instance type (e.g., t2.micro)
- Key pair
- Security group (allow SSH/HTTP)

4. Click Launch instance

PW SKILLS

Explaining Amazon Machine Images (AMIs) and how to create custom AMIs.

Let’s see

Amazon Machine Images (AMIs) are pre-configured templates used to launch EC2 instances. They include an OS, software, and settings.

To create a custom AMI:

- Launch and configure an EC2 instance.
- Go to EC2 Console > Instances.
- Select the instance → Actions > Image and templates > Create image.
- Name the image and click Create image.

Pop Quiz

Q. How can you create a custom AMI from an EC2 instance?

A

Create an image from a running EC2 instance

B

Take a CloudTrail snapshot

Pop Quiz

Q. How can you create a custom AMI from an EC2 instance?

A

Create an image from a running EC2 instance

B

Take a CloudTrail snapshot

PW SKILLS

Explaining Auto Scaling Groups (ASG) and how they adjust EC2 instances dynamically.

Let’s see

Auto Scaling Groups (ASG) automatically add or remove EC2 instances based on demand.

Key Features:

- Maintain desired instance count
- Scale out/in using policies (e.g., CPU > 70%)
- Improve availability and reduce costs

How it works:

1. Define launch template, min/max/desired capacity
2. Set scaling policies (e.g., target tracking)
3. ASG monitors metrics and adjusts instances dynamically

Pop Quiz

Q. What is the primary function of an Auto Scaling Group (ASG) in AWS?

A

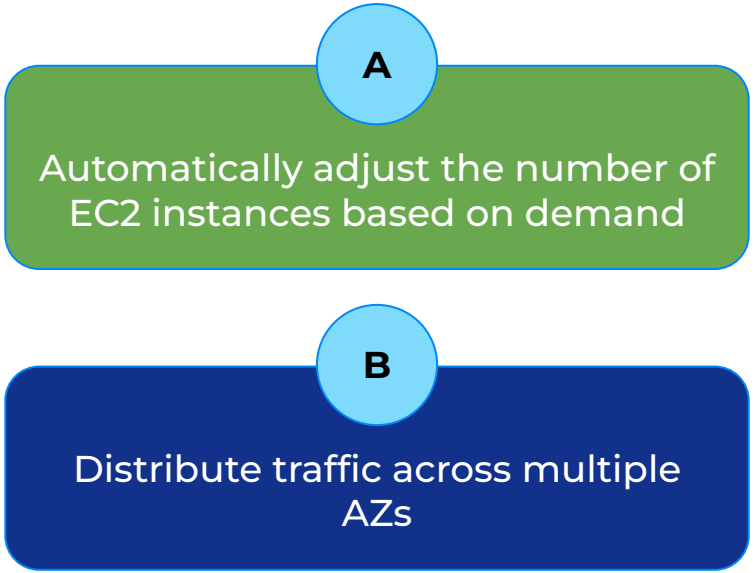
Automatically adjust the number of EC2 instances based on demand

B

Distribute traffic across multiple AZs

Pop Quiz

Q. What is the primary function of an Auto Scaling Group (ASG) in AWS?



PW SKILLS

Discussing Elastic Load Balancer (ELB) types (ALB, NLB, CLB) and when to use them.

Let’s discuss

Elastic Load Balancer (ELB) distributes incoming traffic across multiple EC2 instances.

Types and Use Cases:

ALB (Application Load Balancer):

- Layer 7 (HTTP/HTTPS)
- Use for web apps, microservices, path-based or host-based routing

NLB (Network Load Balancer):

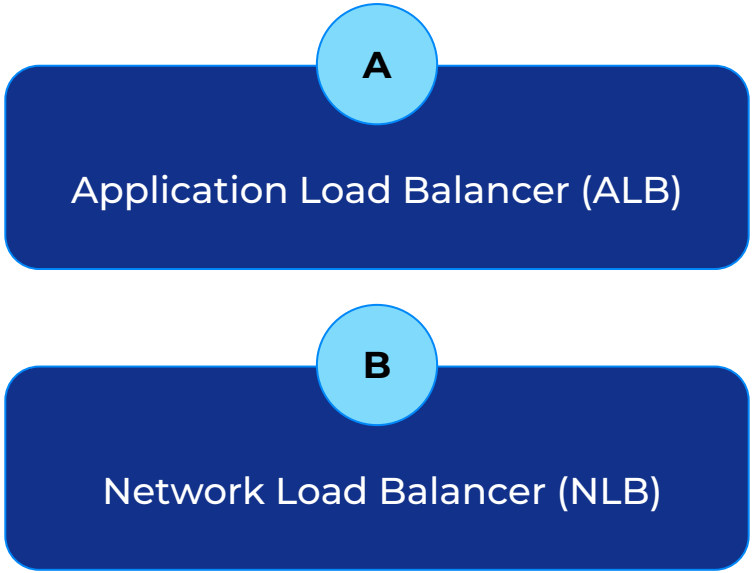
- Layer 4 (TCP/UDP)
- Use for high performance, low latency, or static IP needs

CLB (Classic Load Balancer):

- Legacy, Layer 4 & 7
- Use only for legacy apps; newer workloads should use ALB or NLB

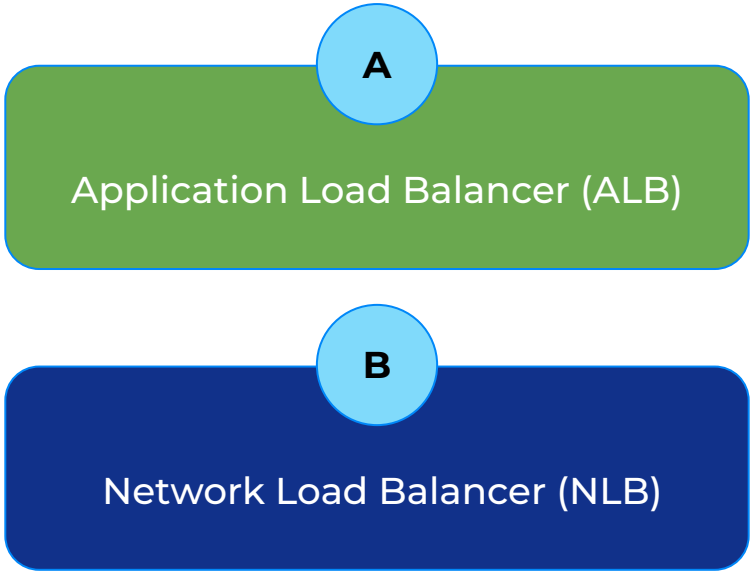
Pop Quiz

Q. Which ELB type is best suited for load balancing HTTP and HTTPS traffic with advanced routing features?



Pop Quiz

Q. Which ELB type is best suited for load balancing HTTP and HTTPS traffic with advanced routing features?



PW SKILLS

Demonstrating how to attach an EC2 instance to an ELB for load balancing.

Let’s do it

Using AWS Console:

- Go to EC2 > Load Balancers
- Select your Load Balancer
- Under Target Groups, select or create one
- Click Targets > Edit
- Register EC2 instances, then click Include as pending and Save

Using AWS CLI:

```
aws elbv2 register-targets \
  --target-group-arn arn:aws:elasticloadbalancing:... \
  --targets Id=i-0123456789abcdef0
```

PW SKILLS

Explaining Function-as-a-Service (FaaS) and how it eliminates the need for managing servers.

Let’s see

Function-as-a-Service (FaaS) lets you run code in response to events without managing servers.

Key benefits:

- You write and upload functions, not full apps
- No server provisioning or scaling needed
- Pay only for execution time

Example: AWS Lambda

- Triggers on events (e.g., S3 upload, API call)
- Automatically scales and handles infrastructure

PW SKILLS

Discussing the benefits of AWS Lambda for event-driven workloads.

Let’s discuss

AWS Lambda is ideal for event-driven workloads because it:

- Auto-scales instantly with demand
- Runs code only when triggered (e.g., S3 uploads, API calls)
- Reduces costs — you pay only for execution time
- Eliminates server management
- Integrates easily with many AWS services

PW SKILLS

Comparing EC2 vs. Lambda vs. Containers for different use cases.

Let’s discuss

Feature	EC2	Lambda	Containers (ECS/EKS)
Use Case	Full control, long-running apps	Event-driven, short tasks	Microservices, scalable workloads
Management	You manage servers	Fully managed, no servers	Partial management (or full with Fargate)
Scalability	Manual or auto scaling	Auto-scales instantly	Scalable with orchestration
Cost	Pay for uptime	Pay per request/runtime	Pay per container/task/runtime

PW SKILLS

Time for case study!

Important

- Complete the post-class assessment
- Complete assignments (if any)
- Practice the concepts and techniques taught in this sessio
- Review your lecture notes
- Note down questions and queries regarding this session ar
  consult the teaching assistants

Thanks !