✅ Assignment 1: AWS Account Creation and Budget Configuration

1. **Q:** Why is it important to configure a budget in AWS?
   A: To track and control spending, avoid bill shocks, and receive alerts when usage exceeds thresholds.

2. **Q:** What is the difference between budget alert and cost explorer?
   A: Budget alert notifies when spending reaches a set limit, while cost explorer analyzes past and current usage trends.

3. **Q:** Can you set a budget on service-level spending (e.g., EC2)?
   A: Yes, budgets can be scoped to individual services like EC2, S3, etc.

4. **Q:** What is the use of the free tier alert?
   A: To notify users before they exceed the AWS Free Tier usage limits.

5. **Q:** Can a budget stop service usage?
   A: No, it only provides alerts, not enforcement.

6. **Q:** What is AWS Billing Dashboard used for?
   A: To view usage, set budgets, and monitor costs in a centralized interface.

7. **Q:** Is billing region-specific?
   A: No, billing is consolidated across all regions.

8. **Q:** How often are budget notifications sent?
   A: Generally, within a few hours of threshold being crossed.

9. **Q:** What are the three types of budgets?
   A: Cost budget, usage budget, and reservation budget.

10. **Q:** Can budgets be shared across accounts?
    A: Yes, using AWS Organizations with consolidated billing.

✅ Assignment 2: Enable Multi-Factor Authentication (MFA) in AWS

1. **Q:** Why is MFA important for AWS accounts?
   A: It adds an extra layer of security beyond just the password.

2. **Q:** What types of MFA devices does AWS support?
   A: Virtual MFA, hardware MFA, and U2F security keys.

3. **Q:** What happens if the MFA device is lost?
   A: Admin can reset it or open a support ticket for root account recovery.

4. **Q:** What is TOTP in MFA?
   A: Time-based One-Time Passwords used in virtual MFA apps.

5. **Q:** Can MFA be enforced via IAM policies?
   A: Yes, using policy conditions like `aws:MultiFactorAuthPresent`.

6. **Q:** Does enabling MFA affect CLI access?
   A: Yes, users need session tokens obtained via MFA.

7. **Q:** Can MFA be disabled once set?
   A: Yes, but it's not recommended for security reasons.

8. **Q:** Is MFA mandatory for all AWS accounts?
   A: No, but it's highly recommended, especially for root users.

9. **Q:** What is the difference between root and IAM user MFA?
   A: Root user MFA secures the full account; IAM user MFA secures only the individual identity.

10. **Q:** Can you assign the same MFA device to multiple users?
    A: No, each user should have a unique device.

✅ Assignment 3: IAM User Creation with Full S3 Access

1. **Q:** Why create IAM users instead of using the root user?
   A: For security and access control using least privilege.

2. **Q:** How do you give an IAM user full S3 access?
   A: Attach the `AmazonS3FullAccess` policy.

3. **Q:** What is the principle of least privilege?
   A: Giving only the minimum required permissions.

4. **Q:** Can IAM users be restricted to a specific bucket?
   A: Yes, using custom policies with specific bucket names.

5. **Q:** What are IAM groups?
   A: Collections of IAM users with shared policies.

6. **Q:** What is an access key in IAM?
   A: A credential for programmatic access via CLI/SDK.

7. **Q:** Can IAM users be given temporary credentials?
   A: Yes, via STS (Security Token Service).

8. **Q:** What is the benefit of using IAM policies?
   A: They offer fine-grained control over AWS services.

9. **Q:** Can you audit IAM user actions?
   A: Yes, using AWS CloudTrail.

10. **Q:** How do you revoke S3 access for a user?
    A: Remove or modify the attached policy.

✅ Assignment 4: Private Bucket and Presigned URL

1. **Q:** What makes an S3 bucket private?
   A: Blocked public access settings and restrictive policies.

2. **Q:** How does a presigned URL work?
   A: It temporarily grants access via a signed link.

3. **Q:** What is the advantage of using a presigned URL?
   A: Secure, time-limited access without making data public.

4. **Q:** Can presigned URLs be used for uploads?
   A: Yes, for PUT operations as well.

5. **Q:** Who can generate presigned URLs?
   A: IAM users or roles with sufficient permissions.

6. **Q:** What happens if a presigned URL expires?
   A: Access is denied automatically.

7. **Q:** Is a private bucket accessible via CLI?
   A: Yes, with valid credentials and permissions.

8. **Q:** Can presigned URLs be reused?
   A: Only until they expire.

9. **Q:** How can you track presigned URL usage?
   A: Enable S3 access logs or CloudTrail.

10. **Q:** Are presigned URLs secure?
    A: Yes, if shared properly and expiration is short.

✅ Assignment 5: Public Bucket in AWS and Public File Access

1. **Q:** What makes an S3 bucket public?
   A: A bucket policy or ACL that grants access to `Principal: *`.

2. **Q:** Why would you make a bucket public?
   A: To serve files openly, like for public websites or media downloads.

3. **Q:** What is the security risk of a public bucket?
   A: Unauthorized access, data leakage, or modification if permissions are too broad.

4. **Q:** How can you allow read-only public access?
   A: Use a bucket policy that permits `s3:GetObject` to everyone.

5. **Q:** What does "Block Public Access" setting do?
   A: Prevents all public access regardless of other permissions.

6. **Q:** Can you make only one file public in a private bucket?
   A: Yes, by setting a public object ACL or specific policy.

7. **Q:** How do you know if a file is publicly accessible?
   A: Try accessing its URL or use S3's "object overview" access permissions.

8. **Q:** Can a bucket be partially public?
   A: Yes, if only some objects or prefixes are exposed.

9. **Q:** Is it recommended to make buckets public?
   A: Not unless necessary—prefer presigned URLs or CloudFront.

10. **Q:** How do you revoke public access?
    A: Remove public bucket policies or enable "Block All Public Access".

✅ Assignment 6: Uploading a Static Website to Amazon S3

1. **Q:** Why use S3 for static website hosting?
   A: It's cost-effective, scalable, and requires no servers.

2. **Q:** What types of content can be hosted?
   A: HTML, CSS, JS, images, and static assets.

3. **Q:** What is the role of `index.html` and `error.html`?
   A: They serve as the default home and error pages.

4. **Q:** Do you need a public bucket for static sites?
   A: Yes, or use CloudFront with an origin access control.

5. **Q:** Can S3 host dynamic websites?
   A: No, only static content is supported.

6. **Q:** What is the website endpoint format?
   A: `http://bucket-name.s3-website-region.amazonaws.com`

7. **Q:** Does S3 support HTTPS for static sites?
   A: Only via CloudFront, not directly.

8. **Q:** How do you improve performance?
   A: Use CloudFront for caching and distribution.

9. **Q:** Can you use a custom domain?
   A: Yes, with Route 53 and S3/CloudFront configuration.

10. **Q:** What permissions are required for public access?
    A: `s3:GetObject` for all users on the relevant objects.

✅ Assignment 7: Uploading a Static Website to Amazon EC2

1. **Q:** What server is commonly used for hosting static files on EC2?
   A: Apache or Nginx.

2. **Q:** Why use EC2 instead of S3 for static sites?
   A: For more control or if dynamic features are expected later.

3. **Q:** What port needs to be open for web access?
   A: Port 80 for HTTP, 443 for HTTPS.

4. **Q:** Can you host multiple websites on a single EC2?
   A: Yes, using virtual hosts in Apache/Nginx.

5. **Q:** How do you make your site visible to the public?
   A: Attach a security group allowing inbound HTTP traffic.

6. **Q:** Do you need to keep the EC2 instance running?
   A: Yes, unless using auto-stop/start or Lambda alternatives.

7. **Q:** What is the default web directory in Apache?
   A: `/var/www/html`

8. **Q:** Can you host a site using only IP?
   A: Yes, though using a domain is better for users and HTTPS.

9. **Q:** What happens if the EC2 instance restarts?
   A: Data is lost unless stored persistently or backed up.

10. **Q:** How do you serve files securely?
    A: Use HTTPS via SSL/TLS with proper configuration.

✅ Assignment 8: Local Project Deployment to GitHub and Vice Versa

1. **Q:** What tool is used to push local projects to GitHub?
   A: Git CLI (`git push`, `git pull`, etc.)

2. **Q:** What is a remote in Git?
   A: A link to the GitHub repository (typically named `origin`).

3. **Q:** What is the purpose of `.gitignore`?
   A: To exclude files/folders from being pushed (e.g., secrets, node_modules).

4. **Q:** How do you clone a project from GitHub?
   A: Use `git clone <repo_url>`.

5. **Q:** Can you deploy to GitHub without Git CLI?
   A: Yes, using GitHub Desktop or GitHub Web UI.

6. **Q:** What is version control?
   A: Tracking and managing code changes over time.

7. **Q:** How do you undo a pushed commit?
   A: Use `git revert` or force push with caution.

8. **Q:** What is the use of branches?
   A: To work on features independently without affecting main code.

9. **Q:** Can GitHub be used for deployment automation?
   A: Yes, using GitHub Actions.

10. **Q:** What is the default branch name in new repos?
    A: `main` (previously `master`).

✅ Assignment 9: Deploy a Project from GitHub to EC2

1. **Q:** How do you get code from GitHub to EC2?
   A: Clone the repo on the EC2 instance using `git clone`.

2. **Q:** What credentials are needed?
   A: GitHub credentials or an access token for private repos.

3. **Q:** How do you keep the code updated?
   A: Pull latest changes with `git pull`.

4. **Q:** Where is the project stored after cloning?
   A: In the directory where the clone command is run.

5. **Q:** Do you need Git installed on EC2?
   A: Yes, if you're using the CLI method.

6. **Q:** How do you automate the deployment?
   A: Use user data scripts or CI/CD pipelines.

7. **Q:** What happens if a repo is private?
   A: You need an access token or SSH key to access it.

8. **Q:** Can deployment be part of EC2 launch?
   A: Yes, using the user data feature.

9. **Q:** What is the benefit of GitHub deployment?
   A: Fast, version-controlled deployment.

10. **Q:** How do you serve the deployed app?
    A: Use Apache/Nginx or run a Node/Python server.

✅ Assignment 10: Deploy from GitHub with New Security Group and User Data

1. **Q:** What is a security group in AWS?
   A: A virtual firewall controlling traffic to EC2.

2. **Q:** Why create a new security group?
   A: To define custom rules for a new project.

3. **Q:** What is user data in EC2?
   A: Startup script that runs during instance boot.

4. **Q:** What is installed via user data usually?
   A: Git, Node.js, Nginx, or code deployments.

5. **Q:** Can user data include Git commands?
   A: Yes, to automate project cloning and setup.

6. **Q:** What permissions should the security group have?
   A: Inbound: port 22 (SSH), 80/443 (web access); Outbound: open.

7. **Q:** Can user data fail silently?
   A: Yes—logs are in `/var/log/cloud-init.log`.

8. **Q:** How do you test if user data ran successfully?
   A: Check the web app or inspect instance logs.

9. **Q:** Can user data be re-run?
   A: Not by default; requires re-launch or manual run.

10. **Q:** Why combine security group and user data?
    A: For secure and automated deployment setup.

✅ Assignment 11: Build Scaling Plans on EC2

1. **Q:** What is EC2 Auto Scaling?
   A: Automatically adds/removes instances based on load.

2. **Q:** What is a scaling plan?
   A: A configuration for managing scale-out/in policies.

3. **Q:** What triggers scaling?
   A: Metrics like CPU usage, network in/out, etc.

4. **Q:** What are the scaling types?
   A: Manual, scheduled, and dynamic (based on metrics).

5. **Q:** What is the benefit of auto scaling?
   A: Cost savings and performance optimization.

6. **Q:** Can scaling be region-specific?
   A: Yes, scaling applies to instances in a region.

7. **Q:** What happens if demand spikes suddenly?
   A: New instances are launched automatically if configured.

8. **Q:** Can you limit the max instances?
   A: Yes, set max capacity in the scaling group.

9. **Q:** What is the role of launch template?
   A: Defines how new instances are created (AMI, type, key).

10. **Q:** How is load balanced in scaling?
    A: Use an Elastic Load Balancer (ELB).

✅ Assignment 12: Deploy and Run the Project in AWS Without Using the Port

1. **Q:** Why avoid using a port in the project URL?
   A: For cleaner URLs and better compatibility with HTTP standards.

2. **Q:** What is the default HTTP port?
   A: Port 80 for HTTP and 443 for HTTPS.

3. **Q:** How can we map a non-standard port to port 80?
   A: Use a reverse proxy like Nginx or Apache.

4. **Q:** What AWS service helps with port forwarding?
   A: Application Load Balancer (ALB) or using Nginx on EC2.

5. **Q:** How can a Node.js app run without specifying the port in the browser?
   A: Run the app on port 80 or behind a reverse proxy listening on port 80.

6. **Q:** What is a reverse proxy?
   A: A server that forwards client requests to backend applications.

7. **Q:** Why use port 443?
   A: For secure HTTPS communication.

8. **Q:** What issues arise from using non-standard ports?
   A: Firewalls may block them; users need to specify port manually.

9. **Q:** What's the solution to serve multiple apps on the same port?
   A: Use virtual hosts or reverse proxy routing based on domain/path.

10. **Q:** Can S3 static hosting help avoid port usage?
    A: Yes, for static sites—it serves content on default ports via its endpoint.

✅ Assignment 13: Create a WorkMail for Your Organization

1. **Q:** What is AWS WorkMail?
   A: A secure, managed business email and calendaring service.

2. **Q:** Why use WorkMail over Gmail or Outlook?
   A: Integrated with AWS services, better security control, and hosted in your AWS region.

3. **Q:** What domain is used if you don't have a custom one?
   A: AWS provides a temporary domain for testing.

4. **Q:** How do you send/receive emails in WorkMail?
   A: Via its web client or email clients using SMTP/IMAP/ActiveSync.

5. **Q:** Can WorkMail integrate with Route 53?
   A: Yes, for DNS validation and routing.

6. **Q:** What is the storage limit in WorkMail?
   A: Each user gets 50 GB of mailbox storage.

7. **Q:** Can you create groups and aliases in WorkMail?
   A: Yes, for better user and team management.

8. **Q:** What AWS service is WorkMail backed by for directory?
   A: AWS Directory Service.

9. **Q:** Is WorkMail accessible programmatically?
   A: Yes, via SDK or SMTP APIs.

10. **Q:** Can WorkMail use encryption?
    A: Yes, messages are encrypted at rest and in transit.

✅ Assignment 14: Create an Elastic IP for an Instance

1. **Q:** What is an Elastic IP?
   A: A static, public IPv4 address that you can associate with EC2.

2. **Q:** Why use an Elastic IP instead of default public IP?
   A: Because default IPs change on reboot; Elastic IP remains constant.

3. **Q:** How many Elastic IPs can you have by default?
   A: 5 per region.

4. **Q:** What happens to Elastic IPs when an instance is terminated?
   A: The association breaks, but the IP remains allocated to your account.

5. **Q:** Is there a cost for Elastic IPs?
   A: Free when associated with a running instance; charged when idle.

6. **Q:** Can you transfer an Elastic IP across regions?
   A: No, Elastic IPs are region-specific.

7. **Q:** What is a potential risk of Elastic IPs?
   A: If leaked, they can expose your instance to attacks.

8. **Q:** How do you release an Elastic IP?
   A: Unassociate it and then release from the EC2 dashboard.

9. **Q:** Can you associate an Elastic IP with multiple instances?
   A: No, only one at a time.

10. **Q:** How is DNS affected by Elastic IP?
    A: You can map a domain to the Elastic IP using Route 53 or another DNS provider.

✅ Assignment 15: Create Serverless Computing Using AWS Lambda

1. **Q:** What is AWS Lambda?
   A: A serverless compute service that runs code in response to events.

2. **Q:** What languages does Lambda support?
   A: Node.js, Python, Java, Go, C#, Ruby, and custom runtimes.

3. **Q:** What is the max execution time for a Lambda function?
   A: 15 minutes.

4. **Q:** What triggers can invoke a Lambda function?
   A: API Gateway, S3, CloudWatch, DynamoDB, etc.

5. **Q:** Does Lambda require server provisioning?
   A: No, it's fully managed by AWS.

6. **Q:** What is a cold start in Lambda?
   A: Delay on first invocation due to environment setup.

7. **Q:** How is Lambda billed?
   A: Based on request count and execution time (GB-seconds).

8. **Q:** Can Lambda access other AWS services?
   A: Yes, with proper IAM roles.

9. **Q:** What's the maximum memory for Lambda?
   A: 10 GB.

10. **Q:** How do you deploy code to Lambda?
    A: Upload ZIP, use inline editor, or deploy via CI/CD pipelines or AWS CLI.

✅ 1. What is Cloud Computing?

A: Cloud computing is the delivery of computing services—such as servers, storage, databases, networking, software, analytics, and intelligence—over the internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

✅ 2. What are the main service models in Cloud Computing?

A:

- **IaaS (Infrastructure as a Service):** Virtual machines, storage, networks.
- **PaaS (Platform as a Service):** Runtime environments, development tools.
- **SaaS (Software as a Service):** Ready-to-use software accessed online.

✅ 3. What are the types of Cloud deployment models?

A:

- **Public Cloud:** Resources shared and managed by third-party providers (e.g., AWS).
- **Private Cloud:** Used by a single organization.
- **Hybrid Cloud:** Combines public and private cloud infrastructures.
- **Community Cloud:** Shared among several organizations with similar requirements.

✅ 4. What is elasticity in cloud computing?

A: Elasticity refers to the ability of a cloud system to dynamically scale resources up or down based on demand.

✅ 5. What is the difference between scalability and elasticity?

A:

- **Scalability** is the ability to handle increasing workloads by adding resources.
- **Elasticity** is the ability to automatically allocate or deallocate resources as needed.

✅ 6. What is virtualization?

A: Virtualization is the creation of virtual instances of resources like servers or storage, allowing multiple virtual machines to run on a single physical machine.

✅ 7. Name common hypervisors used in cloud environments.

A: VMware ESXi, Microsoft Hyper-V, KVM, Xen, and Oracle VirtualBox.

✅ 8. What is multi-tenancy in cloud computing?

A: Multi-tenancy allows multiple users (tenants) to share the same cloud infrastructure securely and efficiently.

✅ 9. What are the key characteristics of cloud computing as per NIST?

A:

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured service

✅ 10. What is cloud bursting?

A: Cloud bursting allows an application to run in a private cloud and "burst" into a public cloud when the demand for computing capacity spikes.

✅ 11. What are some examples of IaaS providers?

A: AWS EC2, Google Compute Engine, Microsoft Azure Virtual Machines.

✅ 12. What are the benefits of cloud computing?

A:

- Cost efficiency
- Flexibility and scalability
- High availability and disaster recovery
- Reduced IT management effort
- Global accessibility

✅ 13. What is serverless computing?

A: A cloud model where developers write code without managing servers; the cloud provider automatically handles infrastructure (e.g., AWS Lambda, Azure Functions).

✅ 14. What are cloud storage types?

A:

- **Object Storage:** S3, Blob
- **Block Storage:** EBS
- **File Storage:** EFS, FSx

✅ 15. How is data secured in the cloud?

A:

- Encryption (at rest and in transit)
- IAM and access control policies
- Firewalls and VPCs
- Backup and disaster recovery mechanisms

✅ 16. What is a Virtual Private Cloud (VPC)?

A: A VPC is a logically isolated section of the cloud where you can define and control a virtual network.

✅ 17. What are cloud-native applications?

A: Applications built specifically for cloud environments using microservices, containers, and DevOps practices.

✅ 18. What is a Content Delivery Network (CDN)?

A: A CDN is a network of servers distributed geographically to deliver content faster by caching it closer to users.

✅ 19. What is Identity and Access Management (IAM)?

A: IAM is a framework that ensures only authorized users can access specific resources in the cloud environment.

✅ 20. What is a Service Level Agreement (SLA) in cloud computing?

A: An SLA is a formal agreement between a cloud provider and a user that defines the expected level of service (uptime, response time, etc.).

✅ 21. What is the role of an API Gateway in cloud architecture?

A: An API Gateway acts as a reverse proxy that routes client requests to appropriate backend services, manages traffic, handles authentication, and provides additional services like rate limiting and logging.

✅ 22. What is the concept of "pay-as-you-go" in cloud computing?

A: "Pay-as-you-go" refers to the billing model where users pay only for the resources they use, such as storage, computing power, and bandwidth, without upfront commitments or long-term contracts.

✅ 23. What is the difference between private cloud and public cloud?

A:

- **Private Cloud:** Owned and operated by a single organization, offers more control and security.
- **Public Cloud:** Managed by third-party providers, resources are shared across organizations, and it is more cost-effective but with less control.

✅ 24. What is a cloud service broker?

A: A cloud service broker is an intermediary entity that manages cloud service offerings, helps businesses choose appropriate cloud services, and integrates multi-cloud environments for optimized usage.

✅ 25. What is cloud security posture management (CSPM)?

A: CSPM is a set of practices and tools that help ensure that cloud environments are configured securely, monitoring and identifying risks and compliance violations.

✅ 26. What are the benefits of using a hybrid cloud model?

A:

- Provides flexibility by combining the best of private and public clouds.

- Offers scalability of public cloud with the security and control of a private cloud.
- Helps in disaster recovery and workload balancing.

✅ 27. What is the role of a load balancer in cloud computing?

A: A load balancer distributes incoming network traffic across multiple servers to ensure no single server is overwhelmed, improving performance and ensuring high availability.

✅ 28. What is a cloud service provider (CSP)?

A: A Cloud Service Provider is a company that provides cloud computing services, including infrastructure, platform, and software. Examples include AWS, Microsoft Azure, and Google Cloud.

✅ 29. What is the concept of "fault tolerance" in cloud computing?

A: Fault tolerance refers to the ability of a system to continue functioning properly even in the event of hardware or software failures. In cloud computing, it often involves redundancy and failover mechanisms.

✅ 30. What is the difference between containerization and virtualization?

A:

- **Virtualization:** Creates multiple virtual machines, each with its own operating system.
- **Containerization:** Runs applications in isolated environments (containers) without the need for separate operating systems, leading to more lightweight and efficient use of resources.