Q1.
Your company wants to allow a new developer to log in to the AWS Management Console but restrict them from accessing billing information. Which is the BEST way to achieve this?

a) Share the root account credentials with the developer.
b) Create an IAM user for the developer and attach a policy denying billing access.
c) Add the developer to the Administrators group.
d) Enable MFA for the root account and share it with the developer.

Q2.
A team wants to centrally manage user permissions for a group of developers working on the same project. Instead of assigning policies individually to each user, which IAM construct should you use?

a) IAM Roles
b) IAM Groups
c) Service-linked roles
d) Access keys

Q3.
Your security team requires all administrators to use MFA when signing in. One admin complains that they cannot access AWS CLI after MFA is enabled. What is the most likely reason?

a) MFA is not supported in the AWS CLI.
b) The admin needs to configure a session token using aws sts get-session-token.
c) The admin should disable MFA when using the CLI.
d) The admin must log in with the root account.

Q4.
You attach the following policy to an IAM user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": "s3:DeleteObject",
    "Resource": "*"
  }
 ]
}
```

What is the result when the user tries to delete an S3 object?

a) Allowed because "Allow" overrides "Deny".
b) Denied because explicit deny always takes precedence.
c) Allowed only if the object is encrypted.
d) Depends on bucket policy.

Q5.
A startup is setting up AWS for the first time. Which of the following is considered an IAM best practice?

a) Use the root account for daily operations.
b) Assign least privilege permissions to IAM users and roles.
c) Store long-term AWS access keys in your application code.
d) Disable logging to reduce costs.

Q6.
Under the AWS Shared Responsibility Model, who is responsible for **configuring IAM policies** to restrict user access?

a) AWS
b) The customer
c) AWS Support
d) Third-party auditors

Q7.
Your company has created an IAM role that grants S3 read-only access. The security team requires that developers must also use MFA when accessing the AWS Console. Which two steps must you take to comply?

a) Attach a policy requiring MFA to the role.
b) Configure MFA on the root account.
c) Enable MFA for developer IAM users.
d) Assign IAM users to the IAM role.

Q8.
A developer left your company, but their IAM user account is still active. What is the MOST secure step to take immediately?

a) Disable their password only.
b) Remove them from all IAM groups.
c) Delete their IAM user account.
d) Rotate their access keys.

Q9.
An intern needs **temporary** access to Amazon S3 for two weeks. Which approach is the MOST secure?

a) Create an IAM user with permanent credentials and delete later.
b) Share the root user's access keys with the intern.
c) Assign an IAM role with a session duration controlled by STS.
d) Give the intern access through an IAM group with full S3 access.

Q10.
During a compliance audit, the team asks who is responsible for patching the underlying host operating systems of EC2 instances. What should you answer?

a) AWS
b) The customer
c) Shared between AWS and the customer
d) Depends on the EC2 instance type

Q11.
Your company uses an application running on EC2 that needs to access an S3 bucket securely. What is the BEST way to configure access?

a) Store AWS access keys in the application code.
b) Use an IAM role attached to the EC2 instance.
c) Generate long-term credentials for the application.
d) Share the root account keys with the application.

Q12.
A junior admin accidentally attached the **AdministratorAccess** policy to all IAM users. What is the most immediate security risk?

a) Billing will be disabled.
b) Users can bypass MFA.
c) Every user has full access to all AWS resources.
d) Logging will be turned off automatically.

Q13.
Your team wants to ensure that sensitive AWS accounts cannot be compromised by password-only authentication. What should you implement?

a) Access keys
b) IAM roles
c) Multi-factor Authentication (MFA)
d) Bucket policies

Q14.
Which of the following is **AWS's responsibility** under the shared responsibility model?

a) Configuring security groups
b) Encrypting data at rest in EBS (if enabled by the user)
c) Physical security of data centers
d) Managing IAM policies

Q15.
A finance team member needs access to download AWS billing reports only. Which is the BEST way to configure this?

a) Attach BillingFullAccess policy to their IAM user.
b) Attach a custom policy allowing only billing actions.
c) Add them to the Administrators group.
d) Give them the root account credentials.

Q16.
Which IAM entity is designed to be assumed temporarily by AWS services such as Lambda or EC2?

a) IAM Group
b) IAM Role
c) IAM User
d) Resource Policy

Q17.
Your company enforces password rotation every 90 days. Which IAM feature can enforce this automatically?

a) IAM roles
b) IAM password policies
c) IAM groups
d) MFA

Q18.
An IAM user tries to access S3 but receives an "Access Denied" error even though their policy allows access. What could be the reason?

a) IAM policy evaluation is case sensitive.
b) An explicit deny is set in a bucket policy.
c) S3 does not support IAM policies.
d) The user must use MFA for S3 access.

Q19.
An auditor requests proof that no one is using the AWS root account for daily tasks. Which service should you check?

a) AWS Config
b) CloudTrail
c) Trusted Advisor
d) GuardDuty

Q20.
Your DevOps team wants to automate user provisioning. Which AWS feature is best suited for automatically creating and managing IAM users and groups?

a) AWS CloudFormation
b) AWS Inspector
c) AWS Secrets Manager
d) Amazon Macie

Q21.
A new IAM role was created but cannot be assumed by an EC2 instance. What is the most likely cause?

a) The role does not have MFA enabled.
b) The instance profile was not attached to the EC2 instance.
c) The IAM role is in the wrong AWS Region.
d) IAM roles cannot be used with EC2.

Q22.
Who is responsible for ensuring that IAM users follow the principle of least privilege?

a) AWS
b) The customer
c) AWS Support
d) Third-party providers

Q23.
You want to prevent accidental deletion of production resources. Which IAM strategy is most effective?

a) Attach AdministratorAccess to all users but enable MFA.
b) Apply an explicit deny on delete actions in a policy.
c) Use the root account for sensitive operations only.
d) Use IAM groups with ReadOnlyAccess.

Q24.
Your company requires that all access to AWS Management Console be logged and reviewed periodically. Which service provides this functionality?

a) AWS Shield
b) AWS Config
c) AWS CloudTrail
d) Amazon GuardDuty

Q25.
An organization wants to give its developers programmatic access to AWS using CLI but NOT Management Console access. Which is the best way to achieve this?

a) Create an IAM user with only an access key and secret key.
b) Create an IAM role with console access.
c) Give them the root account's credentials.
d) Attach the AdministratorAccess policy to their account.