1. **What is CloudTrail in AWS. Why is it used?**

CloudTrail enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage. CloudTrail logs, continuously monitors, and retains account activity related to actions across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

1. **What’s AWS IAM, and why is it used?**
2. AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources. With IAM, you can centrally manage permissions that control which AWS resources users can access. You use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.
3. **What are the key capabilities provided by AWS IAM?**
4. Fine-grained access control. Permissions let you specify and control access to AWS services and resources. ...

Delegate access by using IAM roles. ...

IAM Roles Anywhere. ...

IAM Access Analyzer. ...

Permissions guardrails. ...

Attribute-based access control.

1. **What are the different identities provided by IAM?**
2. An IAM identity provides access to an AWS account. An IAM user group is a collection of IAM users managed as a unit. An IAM identity represents a human user or programmatic workload, and can be authenticated and then authorized to perform actions in AWS. Each IAM identity can be associated with one or more policies.
3. **What is AWS account root user?**
4. One sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account.
5. **What are the some best practice to manage access to AWS resource?**
6. AWS Identity and Access Management Best Practices

Require multi-factor authentication (MFA) ...

Rotate access keys regularly for use cases that require long-term credentials. ...

Safeguard your root user credentials and don't use them for everyday tasks. ...

Set permissions guardrails across multiple accounts.

1. What are the key elements in the JSON scheme of a policy?
2. JSON policy documents are made up of elements. The elements are listed here in the general order you use them in a policy. The order of the elements doesn't matter—for example, the Resource element can come before the Action element. You're not required to specify any Condition elements in the policy. To learn more about the general structure and purpose of a JSON policy document, see [Overview of JSON policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html#access_policies-json).
3. What are the AWS polices?
4. A policy is an object in AWS that, when associated with an entity or resource, defines their permissions. AWS evaluates these policies when a principal, such as a user, makes a request.

Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents.

1. What is AWS IAM Role. IAM User and IAM Policy
2. AWS Identity and Access Management (IAM) roles are entities you create and assign specific permissions to that allow trusted identities such as workforce identities and applications to perform actions in AWS. When your trusted identities assume IAM roles, they are granted only the permissions scoped by those IAM roles.

10.What happens with below policy?

|  |
| --- |
| { |
|  | "Statement":[{ |
|  | "Effect":"Allow", |
|  | "Action":["s3:ListBucket","s3:GetObject","s3:GetObjectVersion"], |
|  | "Resource":["arn:aws:s3:::my\_bucket/\*","arn:aws:s3:::my\_bucket"] |
|  | } |
|  | ], |
|  |  |
|  | "Statement":[{ |
|  | "Effect":"Allow", |
|  | "Action":["s3:ListAllMyBuckets"], |
|  | "Resource":"\*", |
|  | "Condition": {} |
|  | } |
|  | ] |
|  | } |

1. Allow-S3 list, bucket and object in my bucket.

Allow – list bucket all bucket