TNGS Learning Solutions
AWS Solutions Architect
Online Course
AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM)

- AWS Identity and Access Management (IAM) is a service provided by Amazon Web Services (AWS) that allows you to manage access to AWS resources securely. IAM enables you to control who can access your AWS resources and what actions they can perform.

AWS Identity and Access Management (IAM)

- **Users**: IAM allows you to create and manage IAM users. These are individual AWS accounts that are associated with people or applications that need access to AWS resources. Each user has a unique set of security credentials.
- **Groups**: You can organize IAM users into groups, which simplifies access management. Instead of applying policies to individual users, you can apply them to groups, making it easier to grant or deny permissions to multiple users at once.

AWS Identity and Access Management (IAM)

- **Roles**: IAM roles are a way to grant permissions to AWS resources. Unlike users and groups, roles are not associated with specific identities. Instead, roles are assumed by AWS services, applications, or EC2 instances, allowing them to access resources securely.
- **Policies**: IAM policies are JSON documents that define permissions. You can attach policies to users, groups, or roles to specify what actions they can perform on which resources. AWS provides predefined policies, and you can create custom policies to meet your specific requirements.

AWS Identity and Access Management (IAM)

- **Access Control Lists (ACLs)**: IAM allows you to define and manage ACLs that specify which actions are allowed or denied on your resources. ACLs are associated with S3 buckets and objects.
- **Multi-Factor Authentication (MFA)**: IAM supports MFA, which adds an extra layer of security to IAM users' sign-in process. Users need to provide a time-based one-time password (TOTP) in addition to their regular credentials.

AWS Identity and Access Management (IAM)

- **Identity Federation**: IAM supports identity federation, allowing you to grant temporary access to your AWS resources to users from external identity providers, such as Active Directory or SAML-based providers.
- **Access Keys**: IAM users can have access keys, which consist of an access key ID and a secret access key. These keys are used for programmatic access to AWS resources via the AWS Command Line Interface (CLI), SDKs, or scripts.

AWS Identity and Access Management (IAM)

- **Resource-Level Permissions**: IAM allows you to define fine-grained permissions at the resource level. For example, you can specify which S3 buckets and objects a user can access.
- **AWS Organizations**: IAM can be used in conjunction with AWS Organizations to manage access to multiple AWS accounts within an organization. You can set up cross-account access and permissions within an organization.

AWS Identity and Access Management (IAM)

- **Logging and Monitoring**: You can enable AWS CloudTrail to log all IAM actions for auditing purposes. AWS also provides IAM Access Analyzer to help you identify unintended resource access.
- **Password Policies**: You can define password policies to enforce password complexity and rotation rules for IAM users.

AWS Identity and Access Management (IAM)

- AWS IAM is a critical component of AWS security, helping you enforce the principle of least privilege, manage access effectively, and maintain a secure environment for your AWS resources.
- Properly configuring IAM is essential for securing your AWS infrastructure and data.