AWS Security Workshop – Part #1

10-Aug-2024

Online meetup

Raji Krishnamoorthy

What is Cloud Security?

Lock and Key in the Sky

What is Cloud Security?

"Seamless Protection, Everywhere"

Whether you’re managing a small app or a vast enterprise, AWS Security integrates protection at every level of your cloud infrastructure.

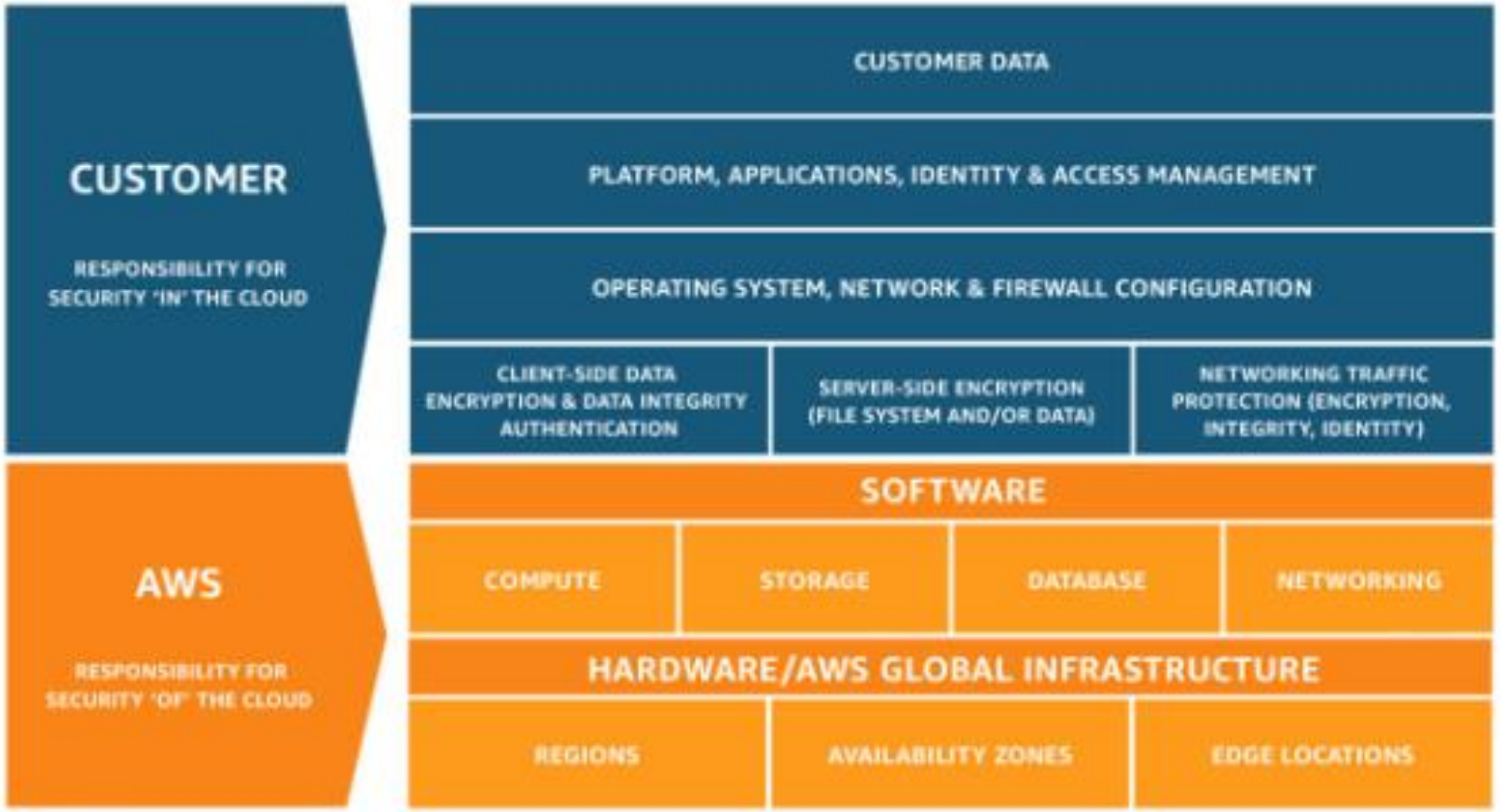
"Proactive, Not Reactive"

AWS Security is designed to anticipate threats before they become a problem, offering peace of mind in a complex digital world.

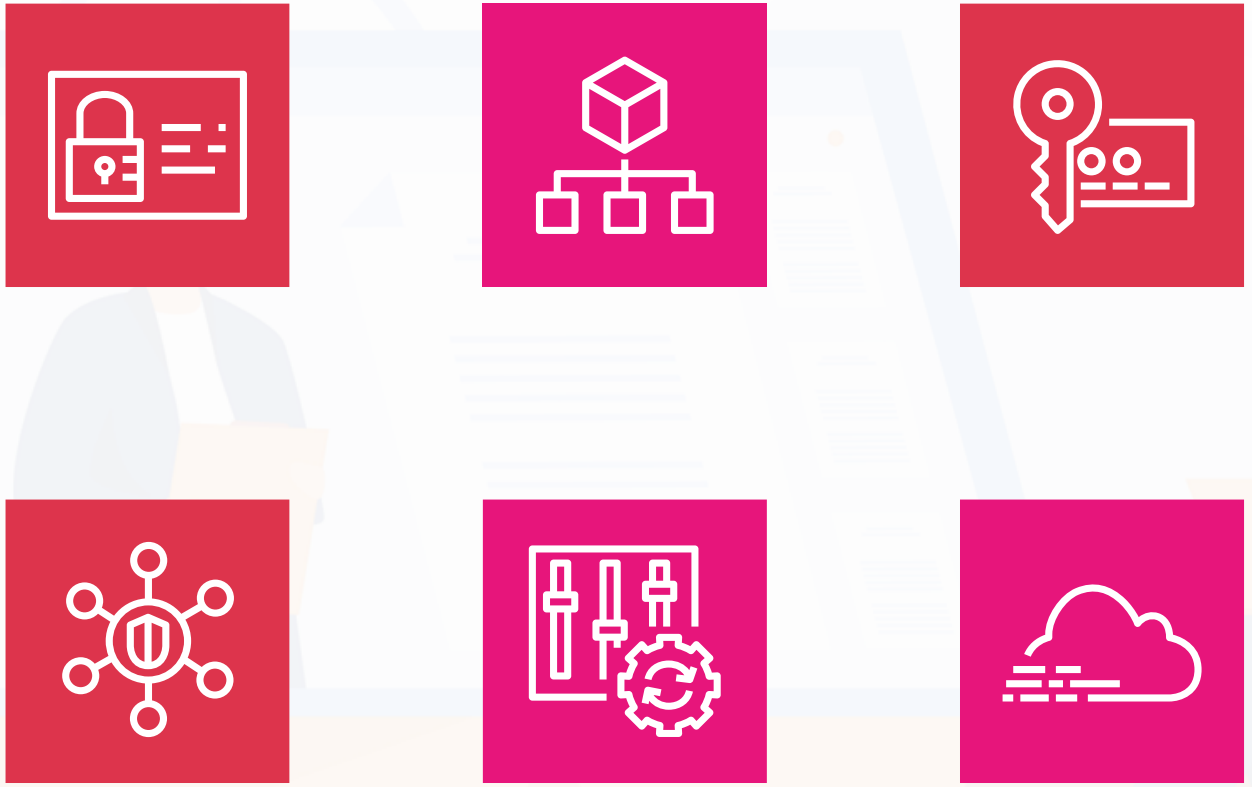
"Customizable Defense"

You’re in control with AWS Security—tailor your security measures to fit your unique needs, ensuring the best defense for your cloud.

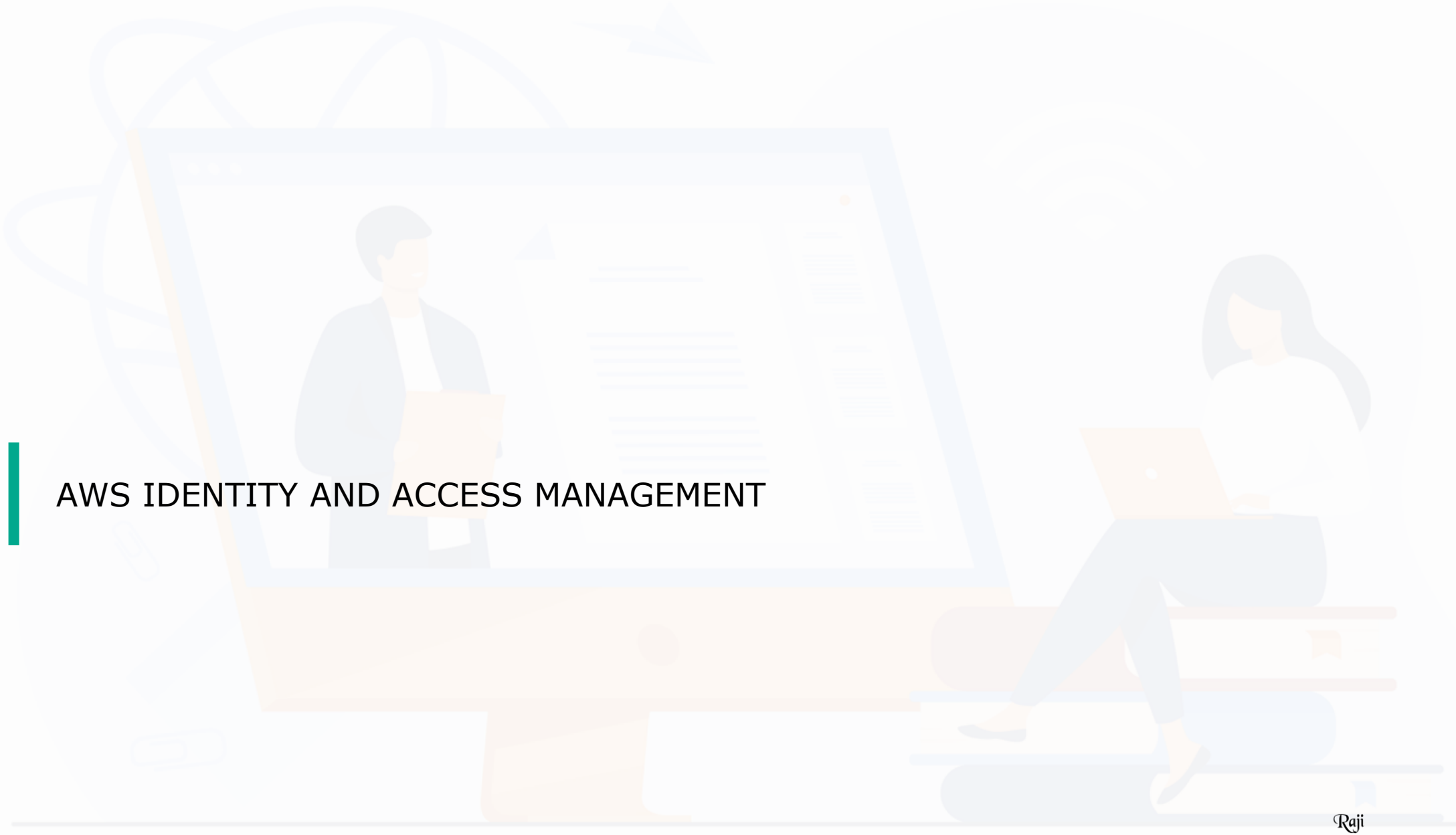
AWS shared security responsibility model



Protecting Your Gateway to the Cloud



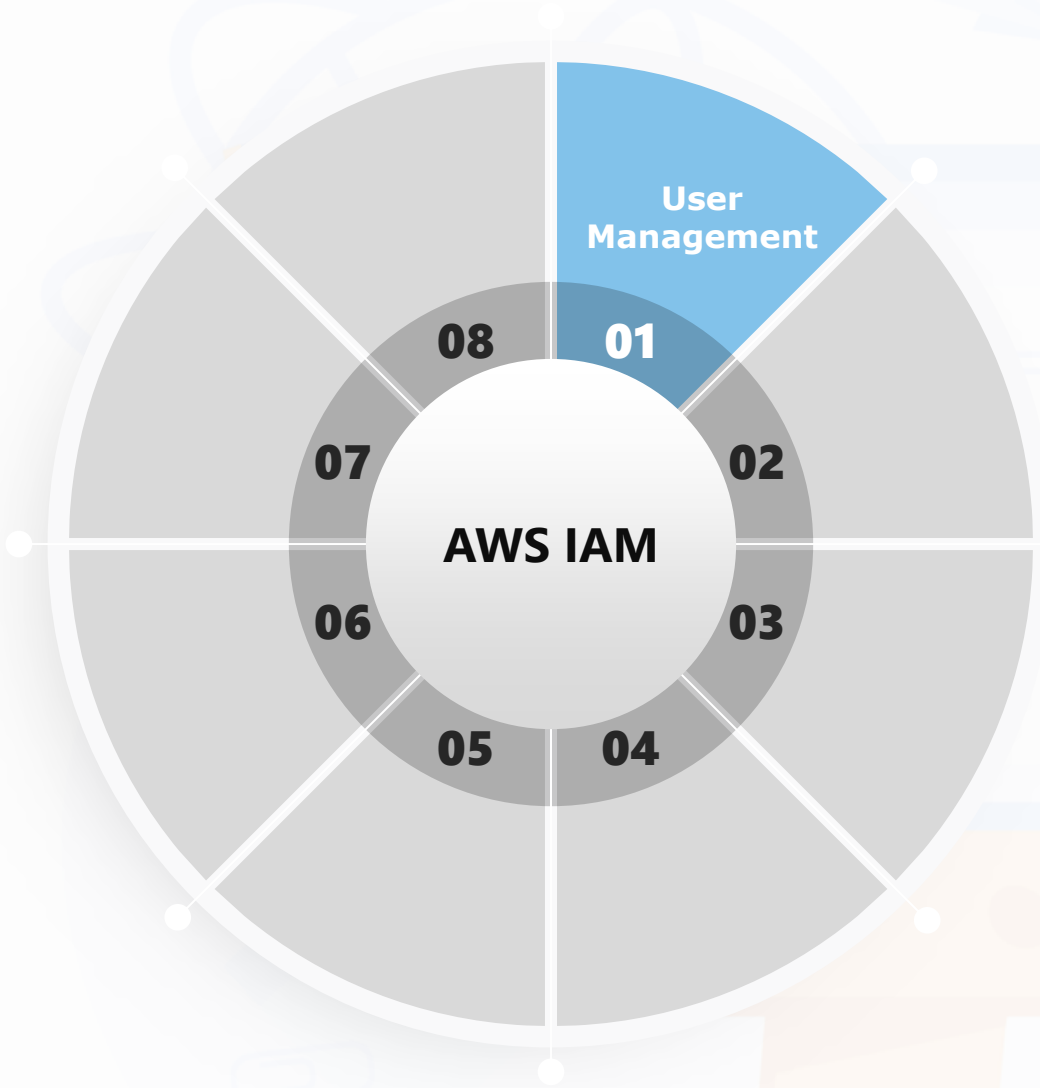
And many many more ….



AWS IDENTITY AND ACCESS MANAGEMENT

AWS IAM - The Foundation of AWS Security

AWS IAM - User Management



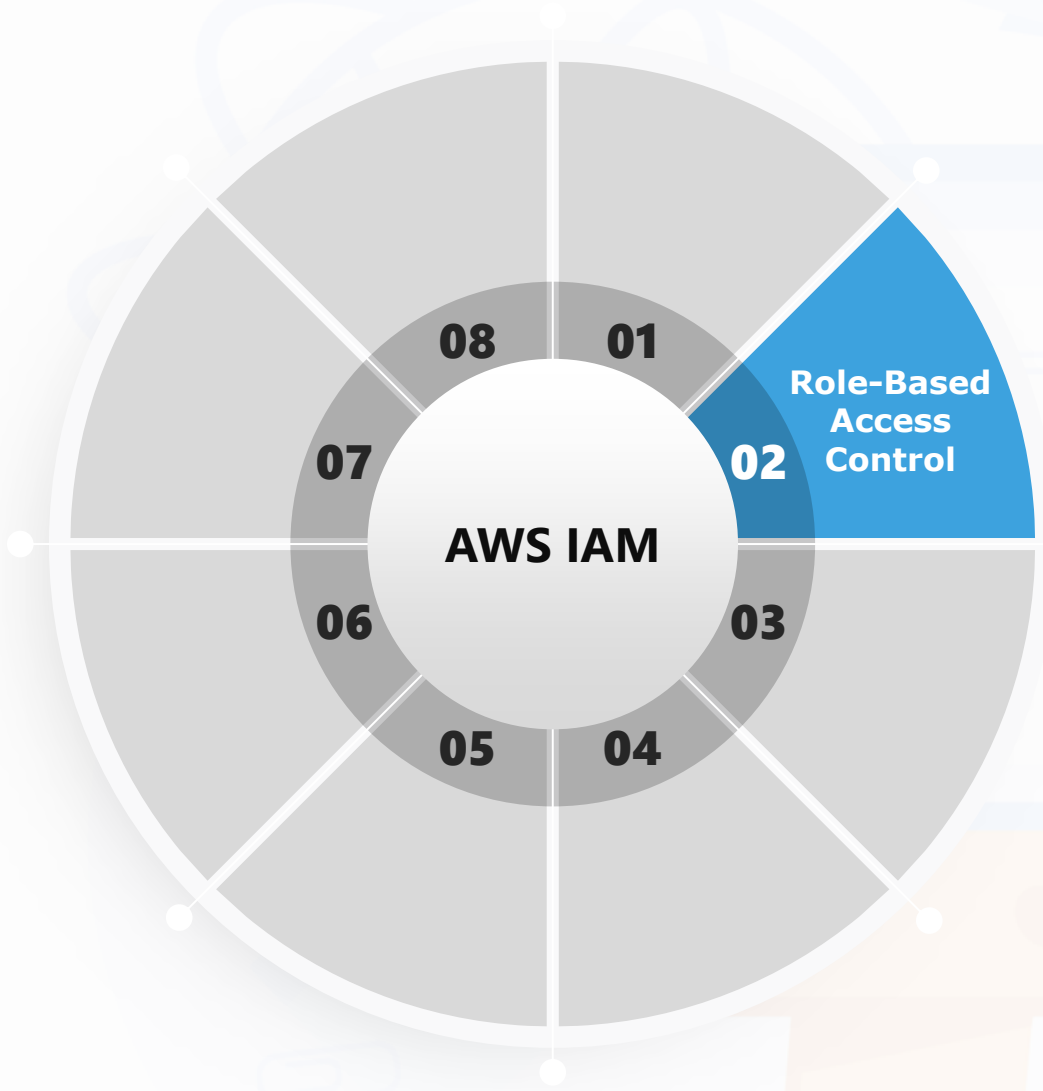
Create and Manage Users

- IAM allows you to create individual user accounts for people or applications that need access to your AWS environment.
- Each user can be assigned unique security credentials (e.g., access keys, passwords) for authentication.

Groups for Simplified Management

- You can organize users into groups and attach permissions to these groups, making it easier to manage access for multiple users with similar roles.

AWS IAM - Role-Based Access Control



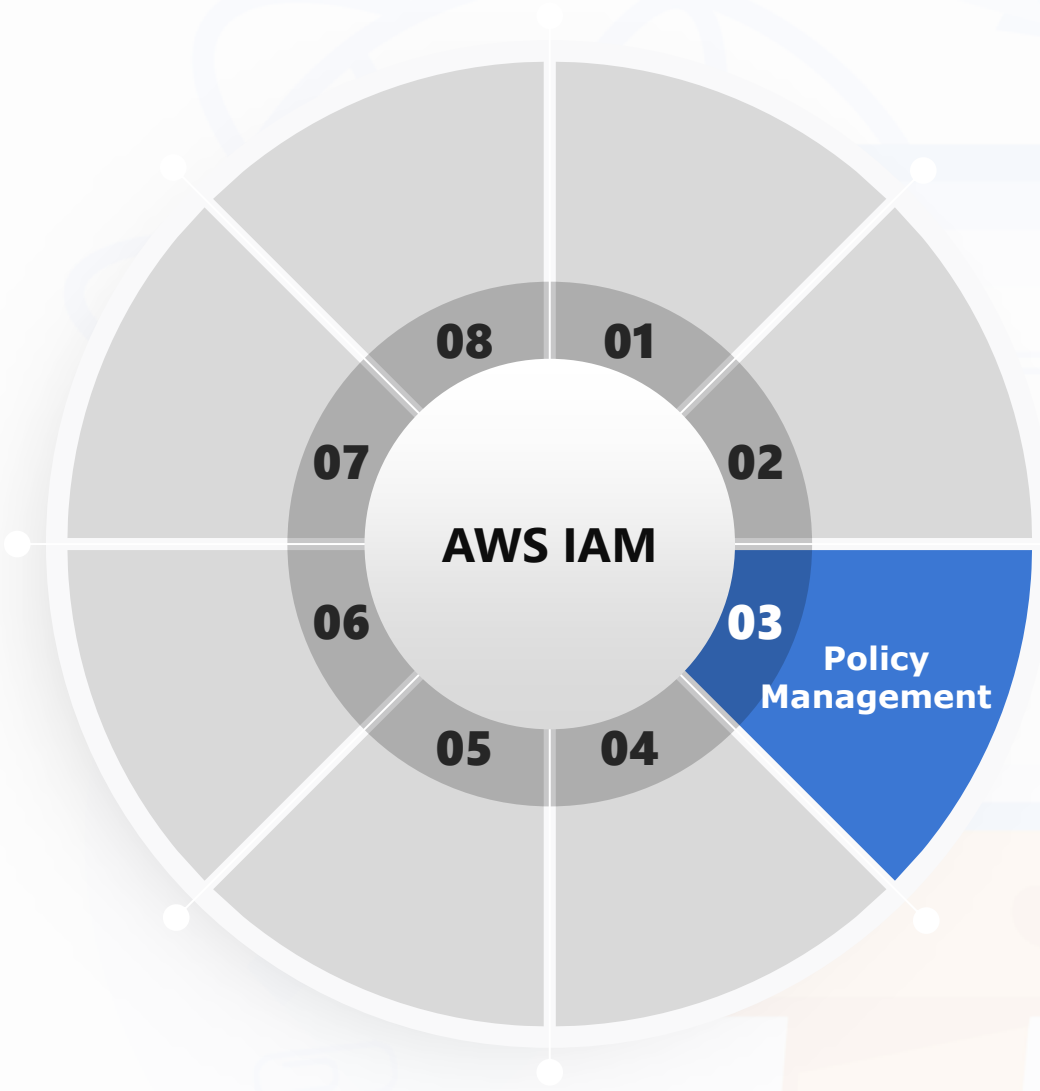
IAM Roles

- IAM Roles enable you to grant temporary access to resources without sharing long-term credentials, ideal for applications or services needing access.
- Roles can be assumed by trusted entities like users, applications, or other AWS services.

Cross-Account Access

- IAM roles also facilitate secure access between AWS accounts, enabling a user or service in one account to access resources in another account without sharing credentials.

AWS IAM - Policy Management



Policies

- IAM policies are JSON documents that define permissions. They specify what actions are allowed or denied on specific resources.
- Policies can be attached to users, groups, or roles, and they can be managed centrally to enforce consistent access controls.

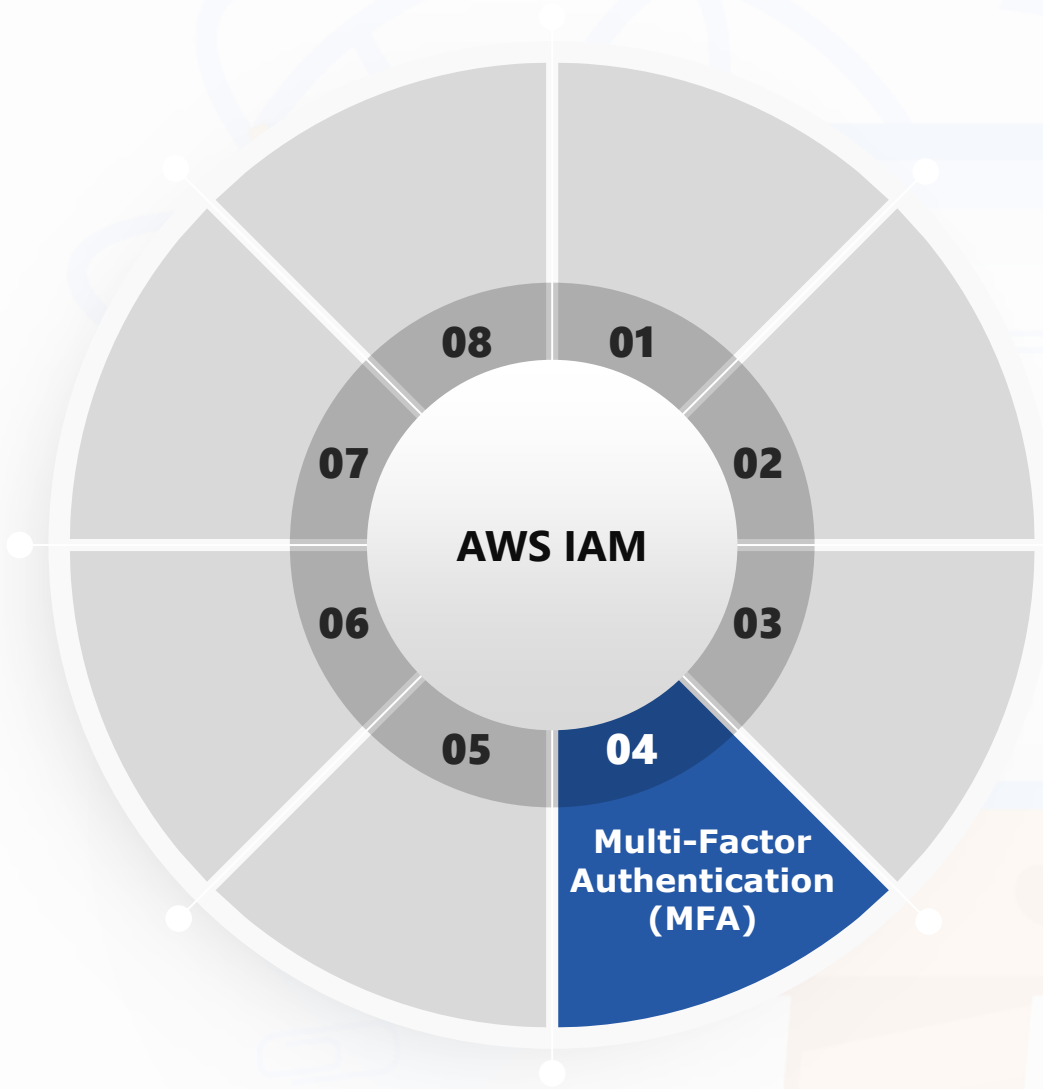
Managed Policies

- AWS provides pre-built managed policies that simplify granting permissions for common use cases, ensuring best practices without needing to write complex policy documents.

Custom Policies

- Users can create custom policies tailored to specific needs, allowing fine-grained control over what actions can be performed on AWS resources.

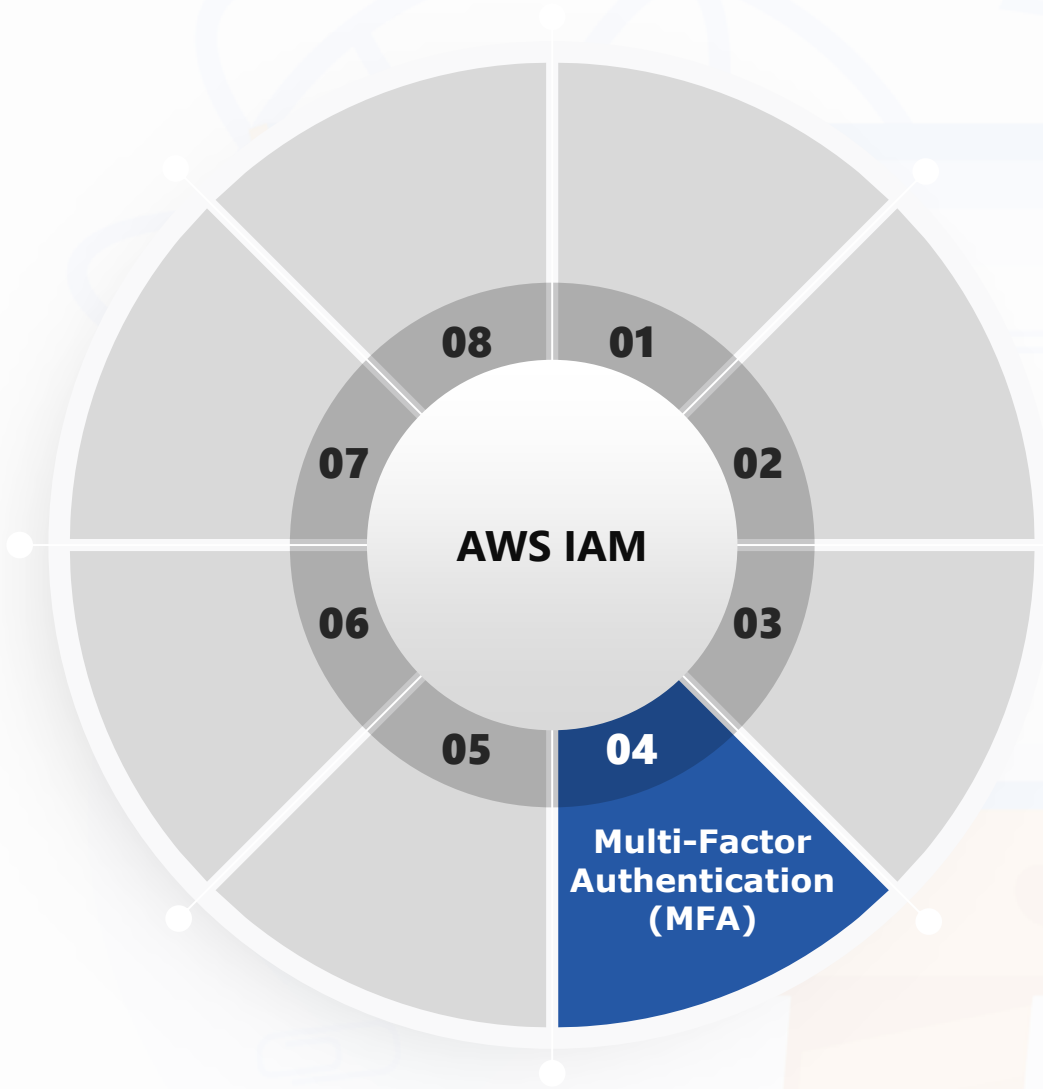
AWS IAM - Multi-Factor Authentication (MFA)



Enhanced Security

- MFA adds an additional layer of security by requiring users to provide a second form of authentication (e.g., a one-time code generated by a device) in addition to their password.
- IAM supports MFA for both root and IAM user accounts, significantly reducing the risk of unauthorized access.

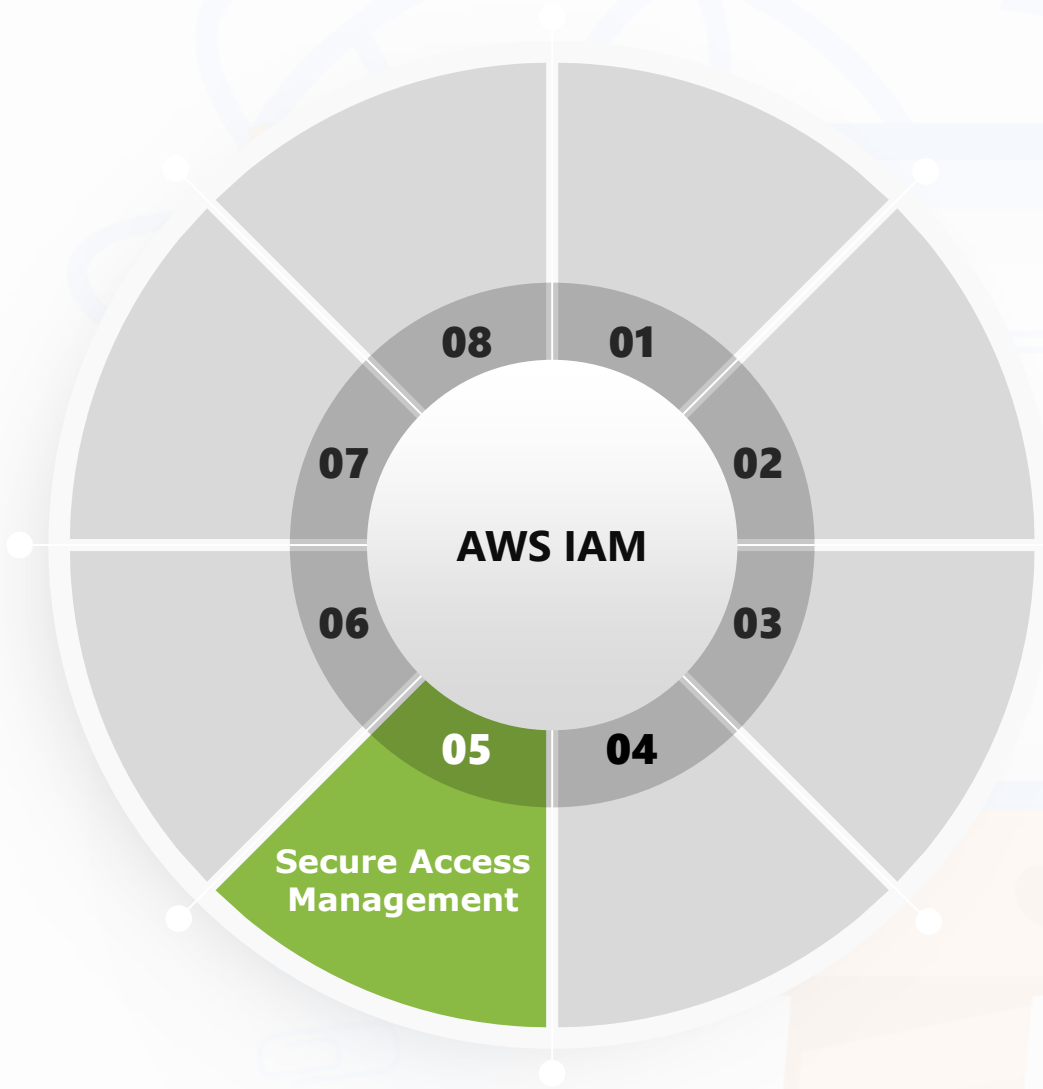
AWS IAM - Multi-Factor Authentication (MFA)



Enhanced Security

- MFA adds an additional layer of security by requiring users to provide a second form of authentication (e.g., a one-time code generated by a device) in addition to their password.
- IAM supports MFA for both root and IAM user accounts, significantly reducing the risk of unauthorized access.

AWS IAM - Secure Access Management



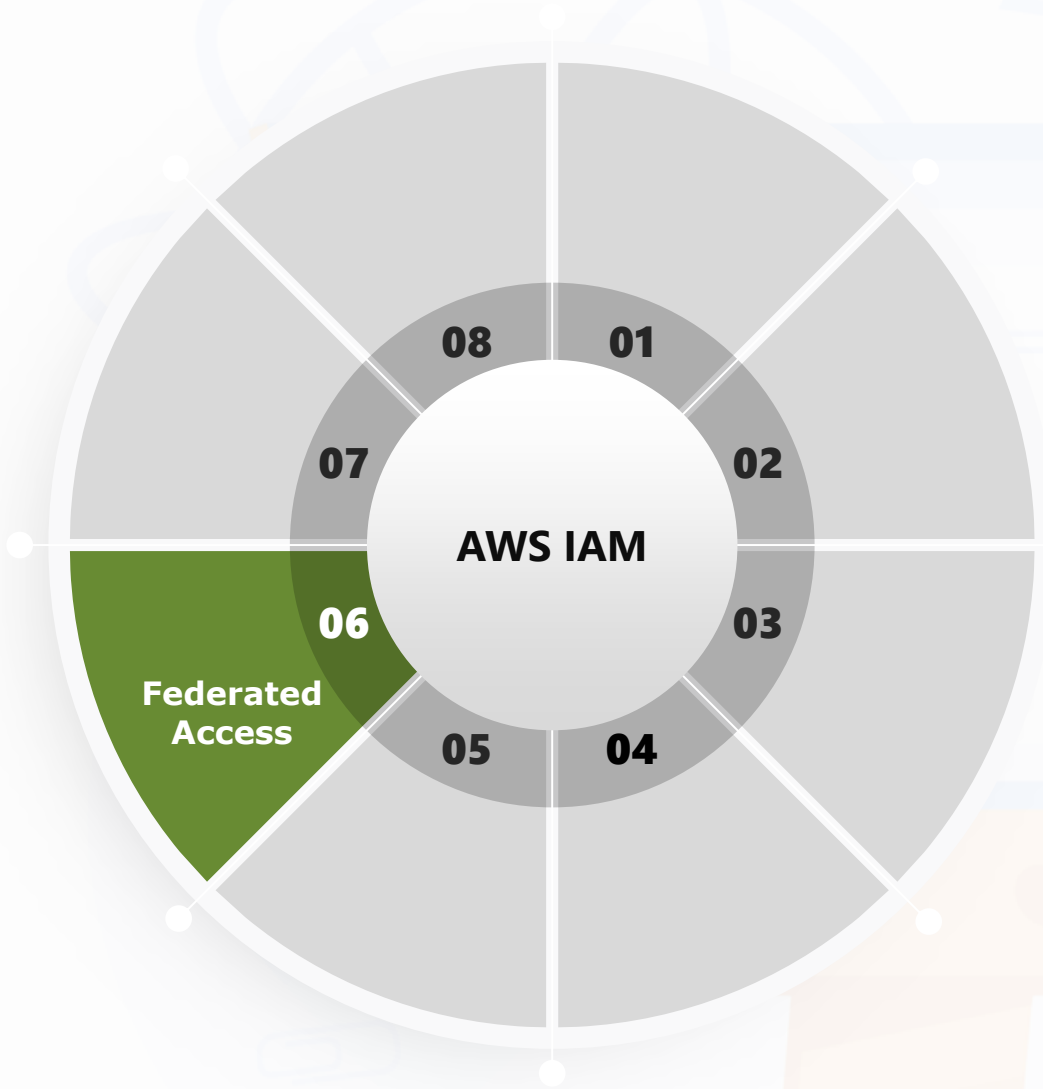
Access Analyzer

- IAM Access Analyzer helps identify resources in your account that are shared with external entities, ensuring that your policies grant the intended level of access.
- It continuously monitors your environment and alerts you to any potential unintended access.

Service-Linked Roles

- AWS services like Amazon EC2 or AWS Lambda can use service-linked roles to access other AWS resources securely on your behalf, minimizing the need for manual access configuration.

AWS IAM - Federated Access



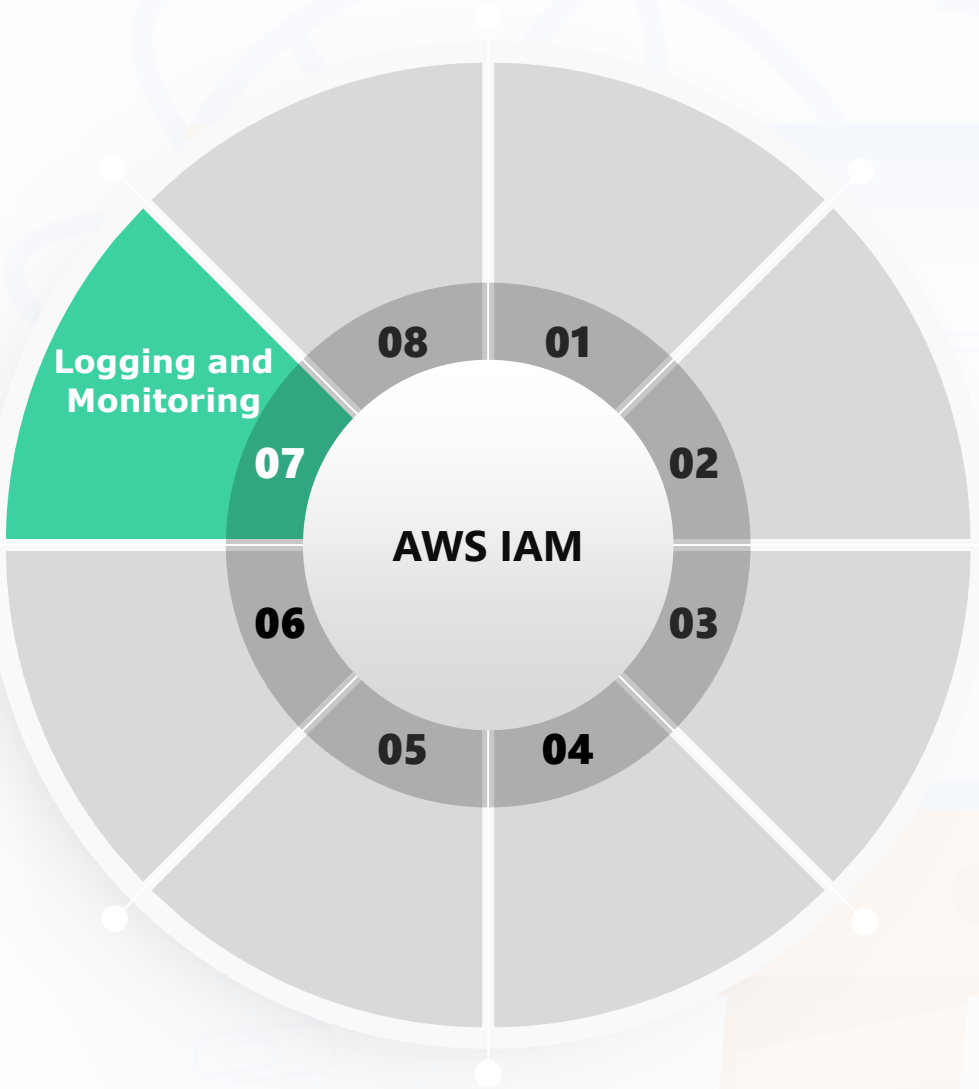
Single Sign-On (SSO)

- IAM supports federated access using identity providers like SAML 2.0 or OpenID Connect, enabling users to log in to AWS using corporate credentials without creating separate IAM users.
- This feature simplifies access management in environments where users already authenticate through a central identity provider.

Temporary Security Credentials

- Federated users or AWS STS (Security Token Service) can provide temporary security credentials, granting limited-time access to AWS resources, reducing the exposure of long-term credentials.

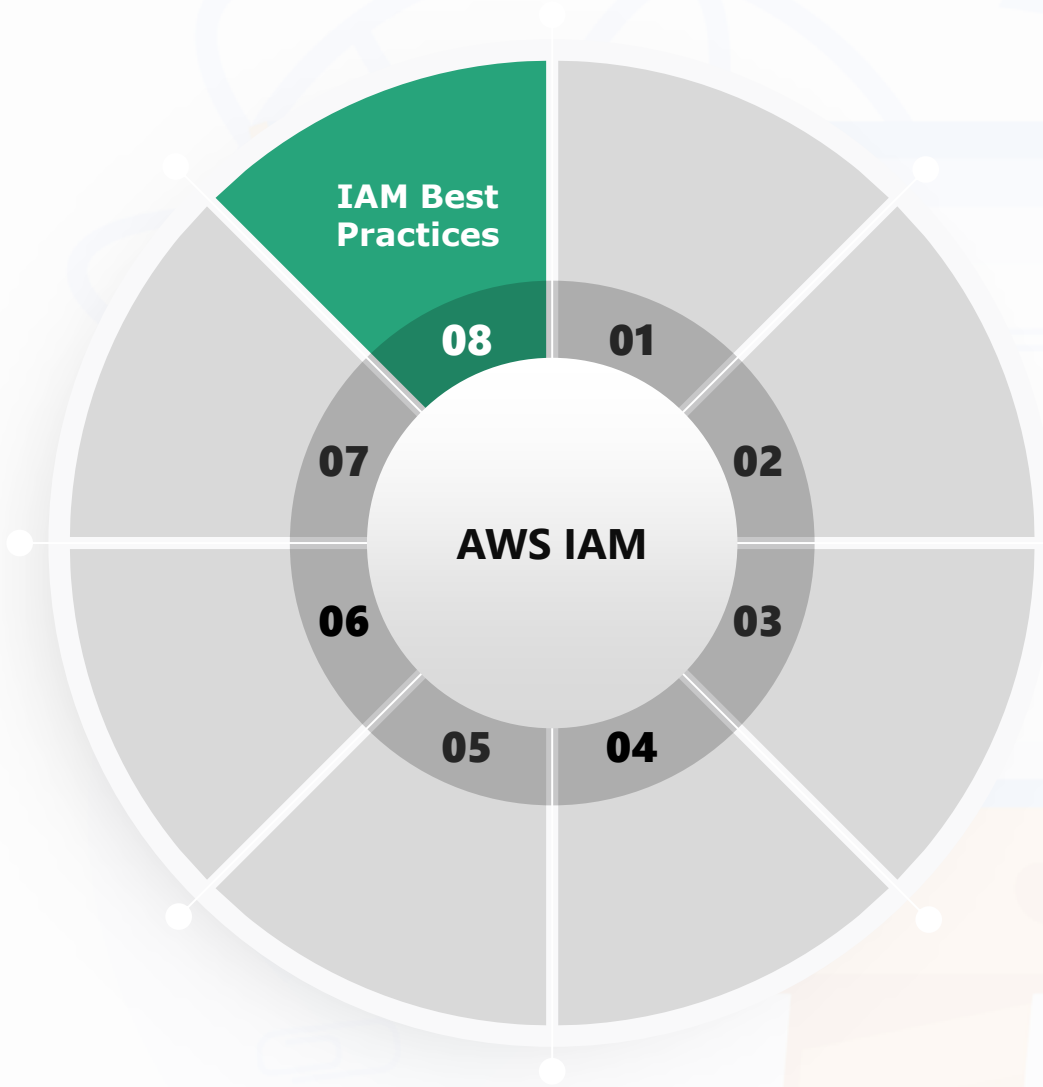
AWS IAM - Logging and Monitoring



CloudTrail Integration

- AWS CloudTrail records IAM API calls, providing a detailed log of all actions taken by users, roles, and services, which is crucial for auditing and compliance.
- Monitor IAM activities to detect potential security incidents or misconfigurations.

AWS IAM - IAM Best Practices



Principle of Least Privilege:

- Always grant the minimal level of access required for users to perform their tasks, reducing the risk of accidental or malicious actions.

Regularly Rotate Credentials:

- Enforce regular rotation of access keys and passwords to minimize the risk of compromised credentials.

Audit and Review:

- Regularly review IAM policies, roles, and permissions to ensure they align with current security requirements and business needs.

GIT REPO

GitHub repo

THANK YOU