Neha T Mathew
A069
apsara

Date:

CLOUD COMPUTING PRACTICAL - 3

Identity Access Managment

1. Users: A user is an individual identity that can be authenticated and authorized to interact with cloud services. Users represent human or non-human entities such as employees, applications or devices.

Users account: each user has a unique account that has been granted permissions to perform actions on cloud resources. Their permissions are usually defined by policies.

Credentials: Users are given credentials to authenticate their identity when accessing the cloud environment.

Groups

A group in IAM is a collection of users. Groups simplify the managment of permission by allowing you to assign permissions to a group rather than to each individual user. Permissions assigned to a group automatically apply to all users within that group. This helps in managing access for multiplying access for multiple users who need similar permissions.

Examples of groups:

Admin group: Users in this group might have full access to all resources.

Developers group: Users in this group might have access to development resources but not production resources.

2. IAM

Identity and Access managment is a critical framework in cloud computing & entreprise environments that governs how users access resources. It involves managing the identities of users, controling their access to resources and enforcing security policies to protect sensitive data.

Page No.:

Date:

* Core concepts of IAM

Users: individuals that need access to resources.

Groups: collection of users that share common needs.

Roles: Roles are used to define a set of permissions that can be assumed by users or services. Roles are typically used to grant temporary access to specific resources

After a user is set up in IAM, they use their sign in credentials to authenticate with AWS. Authentication is provided by matching the sign-in credentials to a principal trusted by AWS account. Next, a request is made to grant the principal access to resources. Access is granted in response to an authorization request if the user has been given permission to the resource. Once authorized the principal can take action or perform operations on resources in AWS account. IAM achieves high availability by replacing data across multiple servers with amazons data centers around the world.

3) Role of IAM

1) Identity managment

User identification: IAM ensures that each user is uniquely identified within a system.

User lifecycle managment: It manages the entire lifecycle of a user's identity from creation and managment to eventual deactivation when access is no longer needed.

Authentication: IAM controls the authentication process, ensuring that users are who they claim to be before granting access.

2) Access Managment.

Authorization: IAM determine what resources a user can can access and what actions they can perform based on their roles & permissions

Multi-factor Authentication: IAM often implements MFA, requiring users to provide two or more verification factors to gain access, enhancing security.

3) Compliance and Security

Regulatory Compliance: IAM helps organizations meet compliance requirments by ensuring proper access controls which is critical for regulations like GDPR, HIPAA & SOX.

Risk Managment: IAM reduces the risk of unauthorized access, inside threats & data breaches by ensuring that only authorized users have access to sensitive resources.

4) User Experience.

Single Sign-in: IAM often includes SSO, allowing users to access multiple applications with a single set of credentials, improving user experience.

Self Service Capabilities: Users can manage their own credentials such as resseting passwords or managing multifactor authentication methods.