Practical-3 Identity Access Management

Anshika Sharma

86062300034

A061

Users and Groups in Cloud Computing

In cloud computing, **Users** and **Groups** are essential for managing access and ensuring the security of resources.

- **Users**: Users represent individual identities within a cloud environment, such as employees, administrators, or even applications. Each user is given a unique set of credentials to access resources in the cloud. This can include username-password combinations or more secure options like multi-factor authentication (MFA) and access keys. Each user typically has defined permissions that specify which resources they can interact with and what actions they are allowed to perform.
- **Groups**: Groups are collections of users with similar access requirements, organized to simplify permission management. By assigning permissions to a group instead of individual users, it becomes easier to manage access for multiple users at once. For example, all members of a "Developers" group might need access to application databases, while a "Finance" group may only need access to billing information. Any user added to a group inherits that group’s permissions, making access control more scalable and manageable.

IAM (Identity and Access Management)

Identity and Access Management (IAM) is a foundational cloud service for managing secure access to cloud resources. IAM solutions, such as AWS IAM, Azure Active Directory, and Google Cloud IAM, allow organizations to define and enforce policies that control who can access specific resources and what they can do with those resources.

Key Components of IAM:

1. **Users**: Individual accounts with permissions to access cloud resources.
2. **Groups**: Collections of users that simplify access management by sharing permissions.
3. **Roles**: Entities that grant temporary access permissions to users or services, often assigned to applications or virtual machines that need to access resources.
4. **Policies**: JSON-based documents that specify permissions, describing which actions are allowed or denied for users, groups, and roles.

IAM helps enforce the principle of least privilege, ensuring users and services only have the minimum access required to perform their tasks.

Role of IAM in Cloud Computing

IAM plays a central role in securing cloud resources by managing and controlling access based on user needs and organizational policies.

1. **Access Control and Management**:
   - IAM enables administrators to define access controls at a fine-grained level. It specifies which users or groups have access to which resources and what actions they can perform. This helps ensure that only authorized users can access sensitive resources, enhancing the security posture of the cloud environment.
2. **Authentication and Authorization**:
   - IAM provides mechanisms for verifying user identities (authentication) and determining what users are allowed to do (authorization). This can involve the use of usernames, passwords, access keys, and MFA to strengthen authentication. Authorization ensures users can only perform tasks they're permitted to, according to the organization's security policies.
3. **Assigning Roles for Secure Access**:
   - IAM roles are used to provide temporary permissions, ideal for scenarios where users or applications only need limited access for a short duration. For example, a cloud application can assume a role to access a storage service (such as an S3 bucket in AWS), rather than relying on long-term credentials. Roles are frequently used to enable secure interactions between cloud services and components.
4. **Policy Management and Enforcement**:
   - IAM policies define who can access resources and how. These policies support a least-privilege approach, meaning users or applications only receive permissions that are absolutely necessary. This helps prevent unauthorized data access and enhances security by minimizing exposure to sensitive data.
5. **Audit and Compliance**:
   - IAM integrates with monitoring and logging services to provide audit trails of user actions. This capability is crucial for compliance, allowing organizations to verify access, track actions, and ensure adherence to security standards. For example, using services like AWS CloudTrail alongside IAM provides comprehensive logging of IAM user activities.