DATE: / /
PAGE:

→ Name: Siddhant Shukla ; A067; 860623000038

Q1 Users and groups

USERS:

→ In cloud computing, users are individuals entities that require access to cloud resource and services. Users can be human individuals or non-human entities (such as applications or services). Each user has a unique identity and is authenticated through credentials like username, passwords, API keys, or certificates. Users are assigned permissions that define what actions they can perform within the cloud environment.

Key aspects of Users:

- Identity Management: Ensures each user has a unique identity.
- Authentication: Verifies user identity through methods like passwords or multi-factor authentication.
- Authorization: Determines what actions a user can perform based on permissions.
- Types: End users, service accounts, administrators and external users.

Groups:

→ Groups in cloud computing are collections of users who share similar roles or access needs. Groups simplify permission management by allowing administrators to assign permissions and policies collectively rather than individually. This approach especially useful in large organization, where managing individual user permission can be complex.

Key aspects of groups:

- Role-based Access control: Assigns permissions based on roles to enhance security and reduce administrative tasks.
- Policy Enforcement: Ensures consistent application of security policies across all groups members.
- Scalability: Facilities management of permissions for large number of users.
- Types: Security groups, resource groups and user groups.

2) Identity and Access Management (IAM)

→ Identity and access management (IAM) is a combination of policies of techologies that allows organisations to identify users and provide the right form of access as and when required. There has been a burst in the market with new applications and the requirements for an organisation

DATE: / /
PAGE:

to use these applications has increased drastically. The services and resources you want to access can be specified is IAM. IAM doesn't provide any replica or backup. IAM can be used for many purpose such as, if one want's to control access of individual & group access for your AWS resources. With IAM policies, managing permissions to your workforce and systems to ensure least privilege permissions becomes easier. The AWS IAM is a global services.

→ Components of identity and access management (IAM) user:

1) Row
2) Groups
3) Policies.

→ IAM

1
2
3

3. IAM roles:

→ A role is a set of permissions that grant access to actions and resources in AWS. These permissions are attached to the role, not to an IAM user or a group.

→ An IAM user can use a role in the same AWS account or a different account.

DATE: / /
PAGE:

→ An IAM user is similar to an IAM user, role is also an AWS identity with permission policies that determine what the identity can & cannot do in AWS.

→ A role is a not uniquely associated with a single person; it can be used by anyone who needs it.

→ A role does not have long term security credential i.e. password or security key. ~~instead~~ instead if the user uses a role, temporarily security credentials are created & provided to the user.

→ You can use the roles to delegate access to ~~users~~ users, applications or services that generally do not have access to your AWS account / resources.