Amazon Web Services

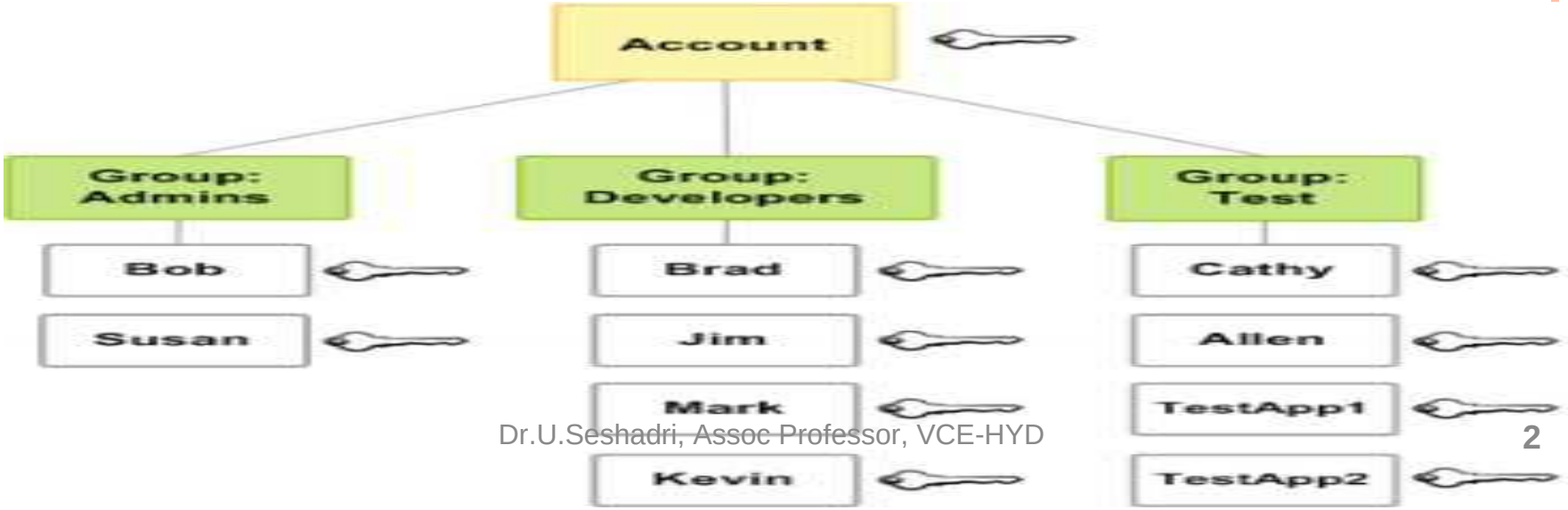
Identity & Access Management

Dr.U.Seshadri, Assoc Professor, VCE-HYD

IDENTITY & ACCESS MANAGEMENT - IAM

- AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. IAM can also keep our account credentials private.

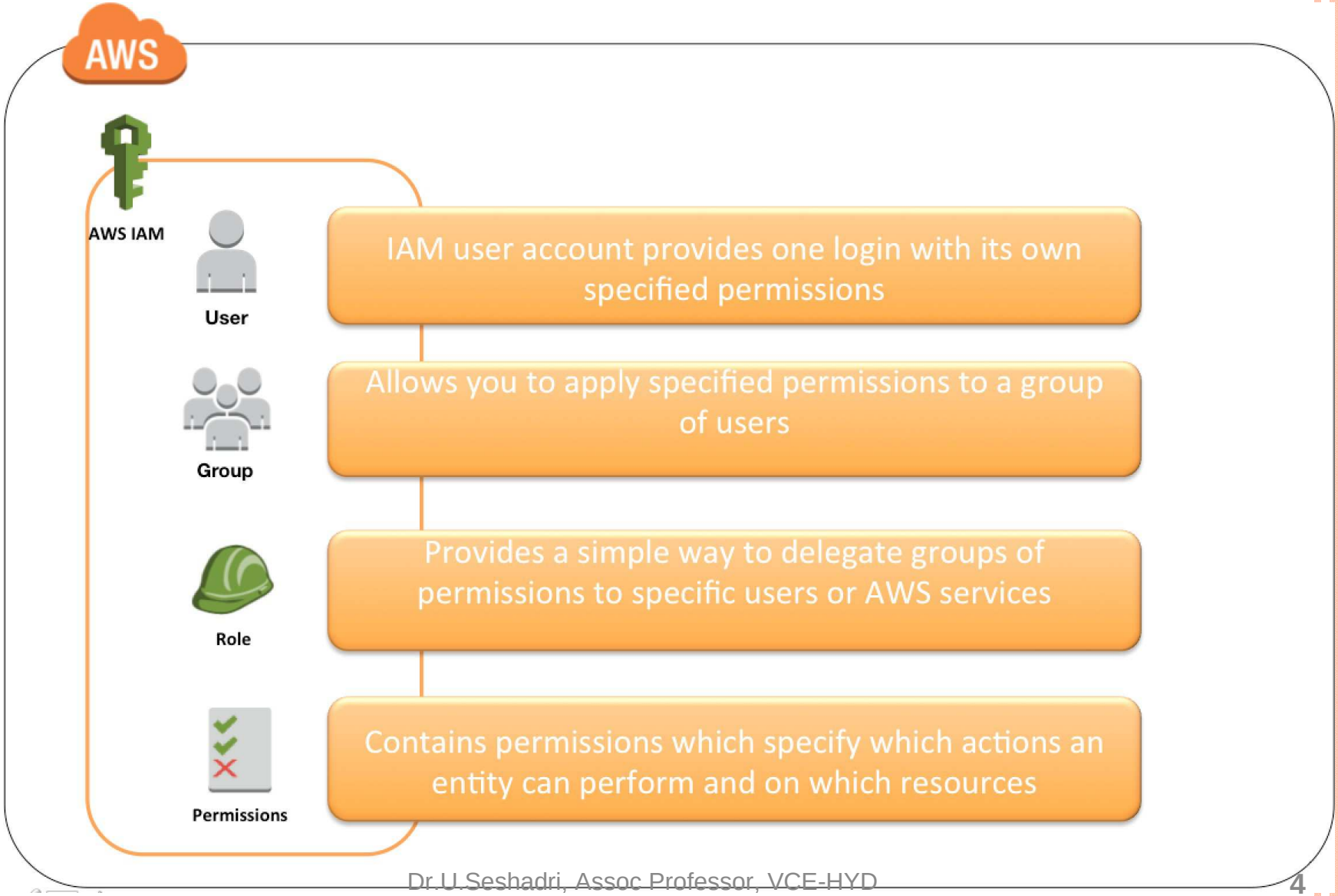
- When we first create an AWS account, it has complete access to all AWS services. This identity is called the AWS



IAM - FEATURES

- **Shared access to the AWS account**: The main feature of IAM is that it allows you to create separate usernames and passwords for individual users or resources and delegate access.
- **Multifactor authentication (MFA)**: IAM supports MFA, in which users provide their username and password plus a one-time password from their phone a randomly generated number used as an additional authentication factor.
- **Identity Federation**: If the user is already authenticated, such as through a Facebook or Google account, IAM can be made to trust that authentication method and then allow access based on it.
- **Free to use**: There is no additional charge for IAM security. There is no additional charge for creating additional users, groups or policies.
- **Password policy**: The IAM password policy allows you to reset a password or rotate passwords remotely.
- **Granular permissions**: Each user can be granted with different set granular permissions as required to perform their job

IAM - Important Terms



IAM - Types of Account in AWS

- Root User
- IAM User

- **Root User**

- Root Account Credentials are the email address and password with which we sign in into the AWS account
- Root Credentials has full unrestricted access to AWS account including the account security credentials which include sensitive information
- An Administrator account can be created for all the activities which too has full access to the AWS account except the accounts security credentials, billing information and ability to change password

IAM - Types of Account in AWS

- IAM User

- IAM user represents the person or service who uses the access to interact with AWS.
- IAM user starts with no permissions and is not authorized to perform any AWS actions on any AWS resources and should be granted permissions as per the job function requirement.
- Each IAM user is associated with one and only one AWS account.
- IAM User cannot be renamed from AWS management console and has to be done from CLI or SDK tools.

IAM – CREATE

- Create Two IAM user.
- One user will access only EC2 Machines & Second user will access only S3 Buckets.
- Go to IAM
- Click on Users
- Click on Add Users
- Enter the user name

IAM – CREATE

- Select AWS Access Type.

- We can connect our AWS account with 2 ways.
- Console Access (Graphical Access)
- Command Line Interface (CLI)

- Select custom password & enter the password

- Uncheck require password reset

- Click on Next: Permissions

IAM – CREATE

- Click on Attach existing policies directly
- Search the EC2 full Access policy
- Select the policy
- Click on Next: Tags
- Click on Next: Review
- Click on Create user
- Create Another User Given S3 Full Access

IAM – LOGIN

- Note down the console ID of your root user
- Go to the AWS URL
- Select IAM User
- Enter the Account ID (Console ID)
- Click on Next
- Enter IAM user name & password
- Click on Sign In
- Change the Password

Amazon Web Services

Groups & Attach Policies

Dr.U.Seshadri, Assoc Professor, VCE-HYD

GROUPS & ATTACH POLICIES

- An IAM Group is a collection of users. Group specifies the permission for a collection of users, and it also makes it possible to manage the permissions easily for those users.
- Following are some important characteristics of user groups:
- A user group can contain many users, and a user can belong to multiple user groups.
- User groups can't be nested; they can contain only users, not other user groups.
- There is no default user group that automatically includes all users in the AWS account. If you want to have a user group like that, you must create it and assign each new user to it.
- Default Quota is 300 Groups For an AWS Account & Max quota is 500 Groups

GROUPS & ATTACH POLICIES

- Go to IAM
- Click on User groups
- Click on Create Group
- Enter the name of the group
- Attach Permission policies
- Search S3Full Access
- Click on Create Group

GROUPS & ATTACH POLICIES

- Create new user with Group
- Select AWS Access Type
- Enter password
- Click on Next: Permissions
- Select Add user to group
- Click on Add: Tags
- Click on Create User
- Login with User
- Check the S3 Bucket

GROUPS & ATTACH POLICIES

- **Remove User & Add User in Group**
- Create One more Group
- Attach Permissions Policies
- Search EC2 Read only
- Create Group
- Open First Group
- Select the user

GROUPS & ATTACH POLICIES

- Click on Remove users
- Open Second Group
- Click on Add Users
- Select the user & Click on Add users
- Now check group

Amazon Web Services

Custom Policies

Dr.U.Seshadri, Assoc Professor, VCE-HYD

CUSTOM POLICIES

- Go to IAM
- Click on Policies
- Click on create policy
- Select Service (IAM)
- Select actions
- Select resources as All Resources

CUSTOM POLICIES

- Click on Next: tags
- Click on Next: Review
- Enter the Name of our policy
- Click on Create policy
- Create user using our policy
- Now login with user

Amazon Web Services

Password Policy

Dr.U.Seshadri, Assoc Professor, VCE-HYD

PASSWORD POLICY

- We can set a custom password policy on our AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. The IAM password policy does not apply to the AWS account root user password.

- **Default Password Policy for IAM Users**

- If an administrator does not set a custom password policy, IAM user passwords must meet the default AWS password policy. The default password policy enforces the following conditions:

- Minimum password length of 8 characters and a maximum length of 128 characters.
- Minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * ( ) _ + - = [ ] { } | ' symbols.
- Not be identical to your AWS account name or email address

PASSWORD POLICY - CUSTOM

- When we configure a custom password policy for your account, we can specify the following conditions:

- Password minimum length: We can specify a minimum of 6 characters and a maximum of 128 characters.
- Password strength: You can select any of the following check boxes to define
  - the strength of your IAM user passwords:
    - Require at least one uppercase letter from Latin alphabet (A–Z) Require at least one lowercase letter from Latin alphabet (a–z)
    - Require at least one number
    - Require at least one non alphanumeric character ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
- Password Expiration: Require users to change the password after some days

PASSWORD POLICY

- Go to IAM
- Click on Account Settings
- Click on Change
- We can check the boxes as per our requirement, we need to apply the password policy.
- Click on save changes

Dr.U.Seshadri, Assoc Professor, VCE-HYD

Amazon Web Services

Security Token Service

Identity Federation

Authentication

Dr.U.Seshadri, Assoc Professor, VCE-HYD

MULTI-FACTOR AUTHENTICATION – MFA

- AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of our user name and password.

- We can enable MFA for our AWS account (Root Account) and for individual IAM users we have created under our account.

MFA - Devices options

- **Virtual MFA Devices**: Applications for your smartphone can be installed from the application store that is specific to your phone type. The following lists some applications for different smartphone types.

- Google Authenticator
- Twilio Authy 2-Factor Authentication
- Duo Mobile
- LastPass Authenticator
- Microsoft Authenticator

MFA - Devices options

- **U2F Security Key:** AWS supports U2F security key as a MFA device for accessing the AWS Management Console using certain web browsers.
- Yubikey
- Other Hardware MFA Device
- Gemalto

MFA – Root User

- Download the mobile App (Authy)
- Go to Security Credentials
- Go to Multi Factor Authentication
- Click on Activate MFA
- Select the Device (Virtual MFA Device)
- Click on Continue

MFA – Root User

- Click on Show QR Code
- Click on plus button in mobile App
- Enter Backup Password in mobile App
- Click on Scan code from mobile App
- Click on Enable Password in mobile App
- Click on Save

MFA – Root User

- System will generate the Code in mobile App
- Enter the code in AWS
- After few Seconds new password will generate in mobile App
- Enter the Second Code
- Click on Assign MFA
- Now try to Login with AWS Account

MFA – IAM User

- Create IAM User
- Click on username
- Go to Security Credentials
- Click on Manage for MFA Device
- Select the Type & Click on Continue
- Click on Show QR Code

MFA – IAM User

- Click on Add Account in mobile App
- Scan QR Code from mobile App
- Save on save in mobile APP
- Password will generate in mobile App
- Click on Assign MFA
- Check our IAM User
- Try to login IAM user