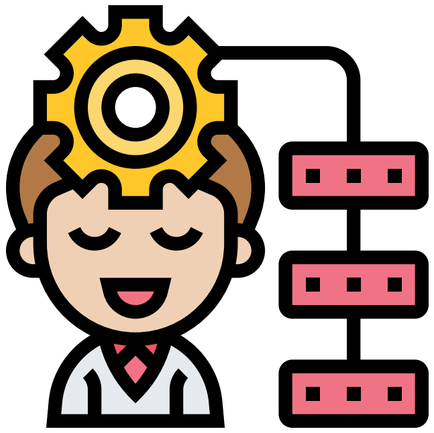
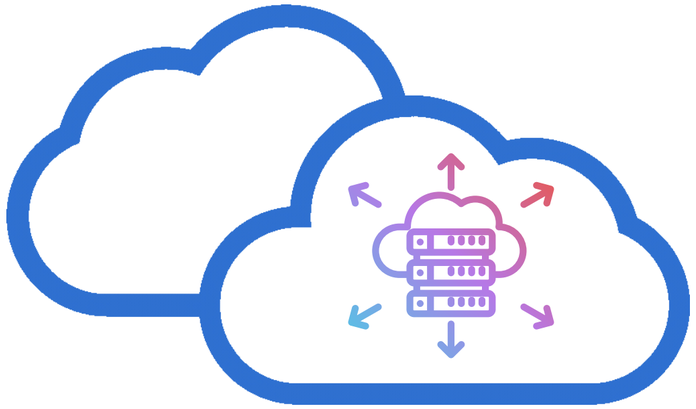
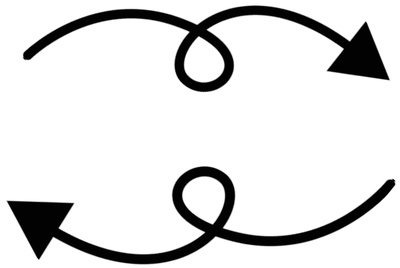


AWS Identity and Access Management (IAM)

Lets understand what is IAM



Agenda



1. Introduction to IAM
2. Benifits and Components of IAM
3. Create Users, Groups, Roles, and Policies in IAM
4. Programmatically working with Users, Groups, Roles, and Policies
5. Create customer-managed policies
6. MFA, Password policy setup, Setup Credentials
7. Real-world example, MCQ and Interview Questions, Work Culture.

Much More . . .

AWS Identity and Access Management (IAM)

Securely manage identities and access to AWS services and resources

- **Set and manage guardrails and fine-grained access controls for your workforce and workloads**
- **Manage identities across single AWS accounts or centrally connect identities to multiple AWS accounts.**
- **Grant temporary security credentials for workloads that access your AWS resources.**
- **Continually analyze access to right-size permissions on the journey to least privilege.**

With AWS Identity and Access Management (IAM), you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.

- **Before AWS or IAM, passwords were often shared in corporate environments in a very insecure manner: over the phone or through email. Often only one admin password existed, which was commonly stored in a set location, or there was only one person who could reset it, and you needed to call the person to ask for the admin password over the phone. That was not secure at all, because anybody could walk by and eavesdrop and then walk away with the password and access to your system and information.**

- **IAM is a feature of your AWS account offered at no additional charge. You will be charged only for the use of other AWS services by your users. To get started using IAM, or if you have already registered with AWS, go to the AWS Management Console and get started with these IAM Best Practices.**

What are the benefits of IAM?

- Improved security.
- Information sharing.
- Ease of use.
- Productivity gains.
- Reduced IT Costs.

Components of IAM

- **Users**

An IAM user is an identity with an associated credential and permissions attached to it. This could be an actual person who is a user, or it could be an application that is a user.

- **Groups**

A collection of IAM users is an IAM group. You can use IAM groups to specify permissions for multiple users so that any permissions applied to the group are applied to the individual users in that group as well. Managing groups is quite easy. You set permissions for the group, and those permissions are automatically applied to all the users in the group.

- **Policies**

An IAM policy sets permission and controls access to AWS resources. Policies are stored in AWS as JSON documents. Permissions specify who has access to the resources and what actions they can perform.

- **Roles**

An IAM role is a set of permissions that define what actions are allowed and denied by an entity in the AWS console. It is similar to a user in that it can be accessed by any type of entity (an individual or AWS service). Role permissions are temporary credentials.

Components of IAM

IAM Users

An Individual who has set of permissions is an ***IAM User***

Users have credentials to make API calls in order to communicate with AWS resources

IAM Groups

A Collection of IAM users is called as ***IAM Groups***

All the IAM users in a group can access the permissions assigned to that group

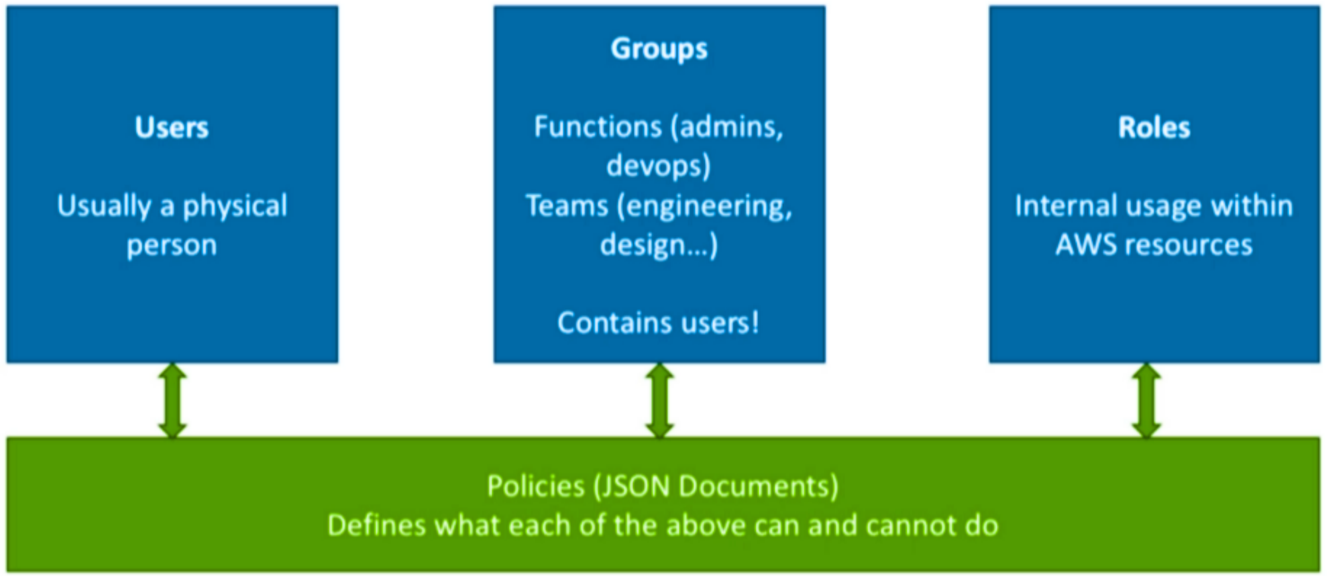
IAM Policies

IAM Policies Specifies those permissions that you want to acquire

IAM Roles

IAM Roles define set of permissions for making AWS service requests

IAM Roles are basically assigned to the applications



Creating IAM users (console)

1. **Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.**
2. **In the navigation pane, choose Users and then choose Add users.**
3. **Type the user name for the new user. This is the sign-in name for AWS. If you want to add multiple users, choose to Add another user for each additional user and type their user names. You can add up to 10 users at one time.**
4. **Select the type of access this set of users will have. You can select programmatic access, access to the AWS Management Console, or both.**
5. **Select Programmatic access if the users require access to the API, AWS CLI, or Tools for Windows PowerShell. This creates an access key for each new user. You can view or download the access keys when you get to the Final page.**
6. **Select AWS Management Console access if the users require access to the AWS Management Console. This creates a password for each new user.**
7. **For the Console password, choose one of the following:**
8. **Autogenerated password. Each user gets a randomly generated password that meets the account password policy. You can view or download the passwords when you get to the Final page.**
9. **Custom password. Each user is assigned the password that you type in the box.**
10. **(Optional) We recommend that you select Require password reset to ensure that users are forced to change their password the first time they sign in.**
11. **Choose Next: Permissions, Choose Next: Tags, Choose Next: Review, Create user.**

Creating an IAM role (console)

1. **Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.**
2. **In the navigation pane of the console, choose Roles and then choose to Create role.**
3. **Choose AWS account role type.**
4. **To create a role for your account, choose This account. To create a role for another account, choose Another AWS account and enter the Account ID to which you want to grant access to your resources.**
5. **The administrator of the specified account can grant permission to assume this role to any IAM user in that account. To do this, the administrator attaches a policy to the user or a group that grants permission for the sts: AssumeRole action. That policy must specify the role's ARN as the Resource.**
6. **If you are granting permissions to users from an account that you do not control, and the users will assume this role programmatically, select Require external ID.**
7. **If you want to restrict the role to users who sign in with multi-factor authentication (MFA), select Require MFA.**
8. **IAM includes a list of the AWS-managed and customer-managed policies in your account. Select the policy to use for the permissions policy or choose Create a policy to open a new browser tab and create a new policy from scratch. Choose Next.**
9. **Review the role and then choose Create role.**

This Slide is to provide the commands for using IAM Role and Access Keys I'm Linux Machine and also for installing AWS CLI.

Configure AWS CLI on another machine/ec2 machine

sudo su

apt-get update

apt-get install awscli

aws configure

{here we need to enter the access key and secret key and region}

Enter and try to access the buckets

aws s3 ls

aws s3 mb newbucketname

aws s3 rb newbucketname

aws iam list-users

NOTE: If you want to use role no need to use aws configure and access key and also secret key

Please make sure about the permissions before you perform any command on AWS cli

Please wait for 10sec after applying new policies or after making any change in policy

Creating IAM user groups

1. **Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.**
2. **In the navigation pane, choose User groups and then choose Create group.**
3. **For the User group name, type the name of the group.**
4. **In the list of users, select the check box for each user that you want to add to the group.**
5. **In the list of policies, select the check box for each policy that you want to apply to all members of the group.**
6. **Choose Create group.**

Creating IAM policies

1. **Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.**
2. **In the navigation pane on the left, choose Policies.**
3. **Choose to Create policy.**
4. **On the Visual editor tab, choose Choose a service and then choose an AWS service. You can use the search box at the top to limit the results in the list of services. You can choose only one service within a visual editor permission block. To grant access to more than one service, add multiple permission blocks by choosing Add additional permissions.**
5. **For Actions, choose the actions to add to the policy. You can choose actions in the following ways:**
6. **Select the check box for all actions.**
7. **Choose to add actions to type the name of a specific action. You can use wildcards (*) to specify multiple actions.**
8. **When you are finished, choose Next: Tags, When you are finished, choose Next: Review.**
9. **Review the policy summary to make sure that you have granted the intended permissions, and then choose Create policy to save your new policy.**

Create Customer Managed Policies

1. **Sign in to the IAM console at https://console.aws.amazon.com/iam/ with your user that has administrator permissions.**
2. **In the navigation pane, choose Policies.**
3. **In the content pane, choose Create policy**
4. **Choose the JSON tab and copy the text from the following JSON policy document. Paste this text into the JSON text box.**
5. **Resolve any security warnings, errors, or general warnings generated during policy validation, and then choose Review policy**
6. **On the Review page, type UsersReadOnlyAccessToIAMConsole for the policy name. Review the policy Summary to see the permissions granted by your policy, and then choose Create policy to save your work.**

MFA, Password policy setup, Setup Credentials

1. **Sign in to the AWS Management Console.**
2. **On the right side of the navigation bar, choose your account name, and choose My Security Credentials. If necessary, choose Continue to Security Credentials. Then expand the Multi-Factor Authentication (MFA) section on the page.**
3. **Choose Activate MFA.**
4. **In the wizard, choose Virtual MFA device, and then choose Continue.**
5. **IAM generates and displays configuration information for the virtual MFA device, including a QR code graphic.**
6. **Open the virtual MFA app on the device.**
7. **The easiest way to configure the app is to use the app to scan the QR code.**
8. **The device starts generating six-digit numbers.**
9. **In the Manage MFA Device wizard, in the MFA Code 1 box, enter the six-digit number that's currently displayed by the MFA device. Wait up to 30 seconds for the device to generate a new number, and then type the new six-digit number into the MFA Code 2 box.**
10. **Choose Assign MFA, and then choose Finish. The device is ready for use with AWS**

MCQ

1. Which of these is Identity in IAM?

(a) Users
(b) Groups
(c) Roles
(d) All of these*

2. IAM group Means?

(a) Is same as IAM users
(b) Can be used to specify permissions for a collection of users
(c) Is truly an identity
(d) All of these*

3. Which of the following is not a component of IAM?

a. Roles
b. Users
c. Organizational Units*
d. Groups

MCQ

Which statement best describes IAM?

a. IAM stands for Improvised Application Management, and it allows you to deploy and manage applications in the AWS Cloud.

b. IAM allows you to manage users, groups, roles, and their corresponding level of access to the AWS Platform.*

c. IAM allows you to manage users' passwords only. AWS staff must create new users for your organization. This is done by raising a ticket.

d. IAM allows you to manage permissions for AWS resources only.

Which of the following is not a feature of IAM?

a. IAM allows you to setup biometric authentication so that no passwords are required.*

b. IAM offers fine-grained access control to AWS resources.

c. IAM offers centralized control of your AWS account.

d. IAM integrates with existing active directory account allowing single sign-on.

A _____ is a document that provides a formal statement of one or more permissions.

a. Group
b. Policy*
c. Role
d. User

Interview Questions

1) What is AWS IAM?
The Amazon Web Services Identity and Access Management service is like a security guard at the door to Amazon Web Services. This is where Azure Services and its environment are authenticated and authorized. The basic building blocks of AWS IAM are IAM roles, IAM users, groups and policies.

2) What is an Identity?
An Identity is something that can be authenticated.

3) Define AWS IAM roles.
An IAM role is a temporary way to access permissions through your identity.

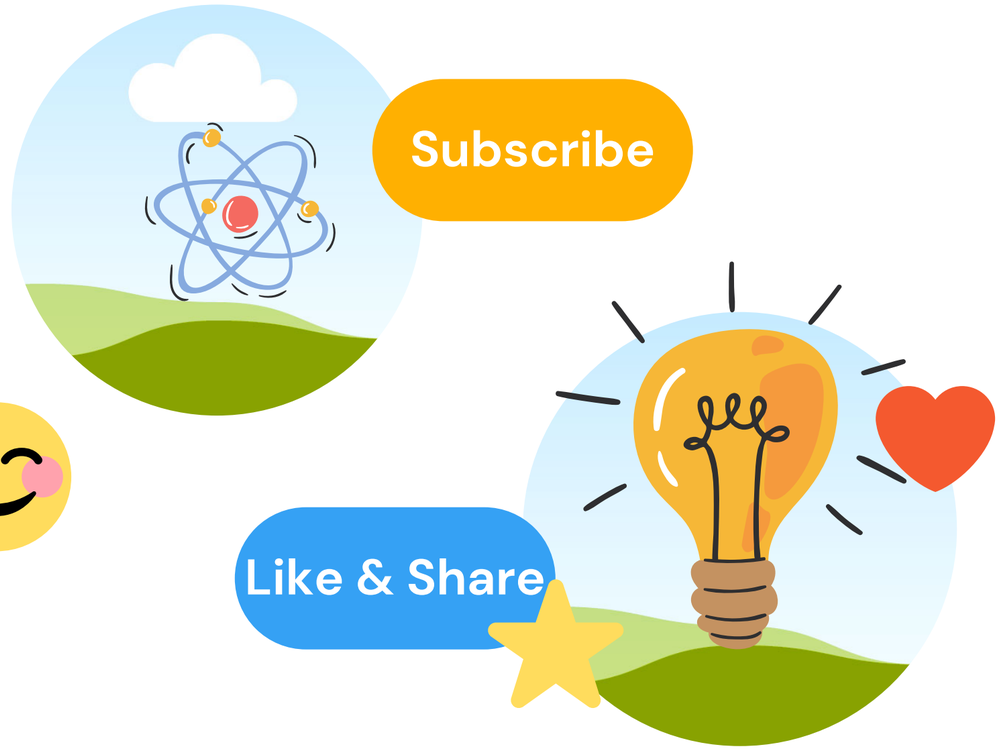
4) What is a Root user?
The Root User is the Owner Account (administrator) that is created when the AWS Account is created. By default, it has access to all AWS services and resources. It is not possible for IAM Policies to explicitly deny this user access to AWS services or resources.

Work Etiquette

- Don’t Interrupt Meetings
- Don’t Interrupt Conversations
- Use Wisdom When Communicating
- Respond to Emails
- Offer to Help Others
- Don’t Play Loud Music
- Greet others politely

THANKYOU

The End



- Hope you like the presentation and the explanation.

- Have more questions? Please reach out to us

Cloud Computing in Telugu