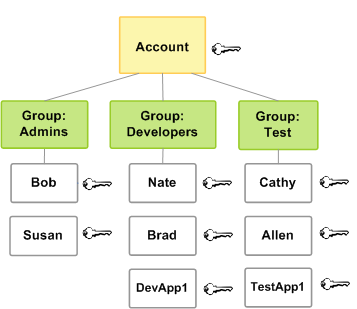


***AWS Identity and Access Management (IAM)***

AWS Identity and Access Management (IAM) enables us to securely control access to AWS services and resources for the users.

Using IAM, we can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to **manage users and user permissions** in AWS. The service is targeted at organizations with **multiple users** or systems in the cloud that use AWS products such as **Amazon EC2**, Amazon **RDS**, and the **AWS Management Console**. With IAM, we can **centrally** manage users, security credentials such as **access keys**, and permissions that control AWS resources for the users.



1.**user**

**An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.**

If you have employees that require access to AWS, don't share root user credentials with them. Instead, create individual IAM users within your account that correspond to users in your organization.

2.**group**

A user group is a collection of IAM users. User groups simplify permissions management by letting you grant, change, and remove permissions for multiple users at once. For example, you can create a user group named "Admins" and give that group administrative permissions. Any user in that group automatically has the permissions that are assigned to the group.

3.**Roles**

A role is an IAM identity that you can create in your account that has specific permissions. An IAM role has some similarities to an IAM user. Roles and users are both AWS identities with permissions policies that determine what the identity can and cannot do in AWS.

4.**policies**

* Permissions let us specify, who has access to AWS resources and which actions they can perform on those resources.
* Every AWS Identity and Access Management (IAM) user starts with no permissions.
* In other words, by default, users can do nothing, not even view their own access keys.
* To give a user permission to do something, we can add the permission to the user (that is, **attach a policy** to the user), or add the user to a group that has the **desired permission**
* {
* "Version": "2012-10-17",
* "Statement": [
* {
* "Action": "ec2:\*",
* "Effect": "Allow",
* "Resource": "\*"
* },
* {
* "Effect": "Allow",
* "Action": "elasticloadbalancing:\*",
* "Resource": "\*"
* },
* {
* "Effect": "Allow",
* "Action": "cloudwatch:\*",
* "Resource": "\*"
* },
* {
* "Effect": "Allow",
* "Action": "autoscaling:\*",
* "Resource": "\*"
* },
* {
* "Effect": "Allow",
* "Action": "iam:CreateServiceLinkedRole",
* "Resource": "\*",
* "Condition": {
* "StringEquals": {
* "iam:AWSServiceName": [
* "autoscaling.amazonaws.com",
* "ec2scheduled.amazonaws.com",
* "elasticloadbalancing.amazonaws.com",
* "spot.amazonaws.com",
* "spotfleet.amazonaws.com",
* "transitgateway.amazonaws.com"
* ]
* }
* }
* }
* ]
* }

***To create IAM user, assign password, change password policy***

* Login to AWS console
* Select security, identity and compliance
* Click IAM service
* From IAM dashboard
* Select group
* Click on new group
* Give the group name
* Click next
* In filter type – EC2F
* Check the box amazon EC2 full access
* Click next
* Click on create group
* Verify
* Create another group
* Click in create group
* Give the full access S3 storage
* In filter type: S3f
* Check the box amazon full access
* Click next
* Click on create group
* Verify
* Attach the policy
* Create the users and join the EC2 admin group and S3 admin group
* Create another user and EC2 full access and S3 full access policy
* Click on IAM dashboard
* Select users
* Click on add users
* Create user ali and join the EC2 admin group
* Select ali
* Access type: AWS management console access
* Dragdown
* Give console custom password
* Click on next permissions
* Under group column
* Select EC2 admin group
* Click on next review
* Verify user details
* Download the .CSV file
* Click on close button
* Again create another user raja
* Join to S3 admin group
* Select user
* Add user
* Username: raja
* Console password: \*\*\*\*
* Drag down
* Click on next permissions
* Select S3 admin permissions
* Click on next review
* Verify user details
* Select user
* Download .CSV file
* Click on close
* Create another user nivas without joining any group
* Attach EC2full access and S3full access policy
* Select user
* Add user
* Username: nivas
* Console password: \*\*\*\*\*
* Drag down
* Click on next permission
* Click on attach existing policies directly box
* Filter type EC2f
* Select amazon EC2full access check box
* Filter type search for S3f
* Select amazon S3full access check box
* Click on next review
* Verify user details
* Download .CSV file
* Click on close
* Verification
* Open web browser
* Type: [**https://123456789.signin.aws.amazon.com/console**](https://123456789.signin.aws.amazon.com/console)
* Click on sign in
* Click on S3 verify access
* Now select EC2 service
* Now he can access

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html>