FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Department of Computer Engineering

Course, Subject & Experiment Details

Practical No:	
Title:	To study and implement Identity and Access Management (IAM) practices on AWS/Azure cloud
Name of the Student:	Warren Fernandes
Roll No:	8940
Date of Performance:	11/04/2022
Date of Submission:	11/04/2022

Evaluation:

Sr. No.	Rubric	Grade
1	On time submission/completion (2)	
2	Preparedness (2)	
3	Skill (4)	
4	Output (2)	

Signature of the Teacher

AWS IAM

aws

Sign in as IAM user

Account ID (12 digits) or account alias

276776383994

IAM user name

Vinyas-Kulal

Password

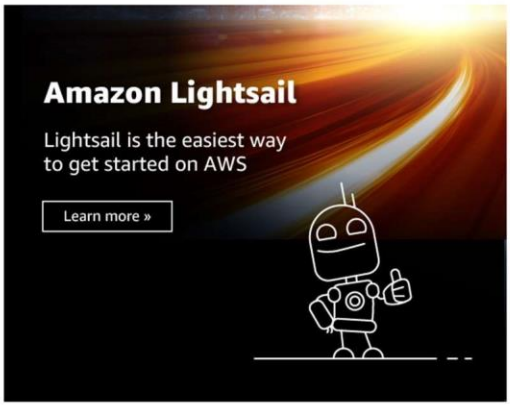
••••••••••••••••

☐ Remember this account

Sign in

Sign in using root user email

Forgot password?



English

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | Global ▾ | Abhi Gupta ▾

Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://276776383994.signin.aws.amazon.com/console

Download .csv

	User	Email login instructions
▸	Vinyas-Kulal	Send email

Close

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | Global ▾ | Abhi Gupta ▾

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	Vinyas-Kulal
AWS access type	AWS Management Console access - with a password
Console password type	Custom
Require password reset	No
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	group_test

Tags

Cancel | Previous | Create user

Set permissions

Add user to group | Copy permissions from existing user | Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

Create group | Refresh

Search | Showing 1 result

Group	Attached policies
group_test	AdministratorAccess

Set permissions boundary

Cancel | Previous | Next: Tags

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*
- [ ] **Access key - Programmatic access** — Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- [x] **Password - AWS Management Console access** — Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*
- ( ) Autogenerated password
- (•) Custom password

••••••••••••••••

[ ] Show password

Require password reset [ ] User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required | Cancel | Next: Permissions

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

aws Services Search for services, features, blogs, docs, and more [Alt+S] Global Abhi Gupta

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* Vinyas-Kulal

Add another user

Select AWS access type

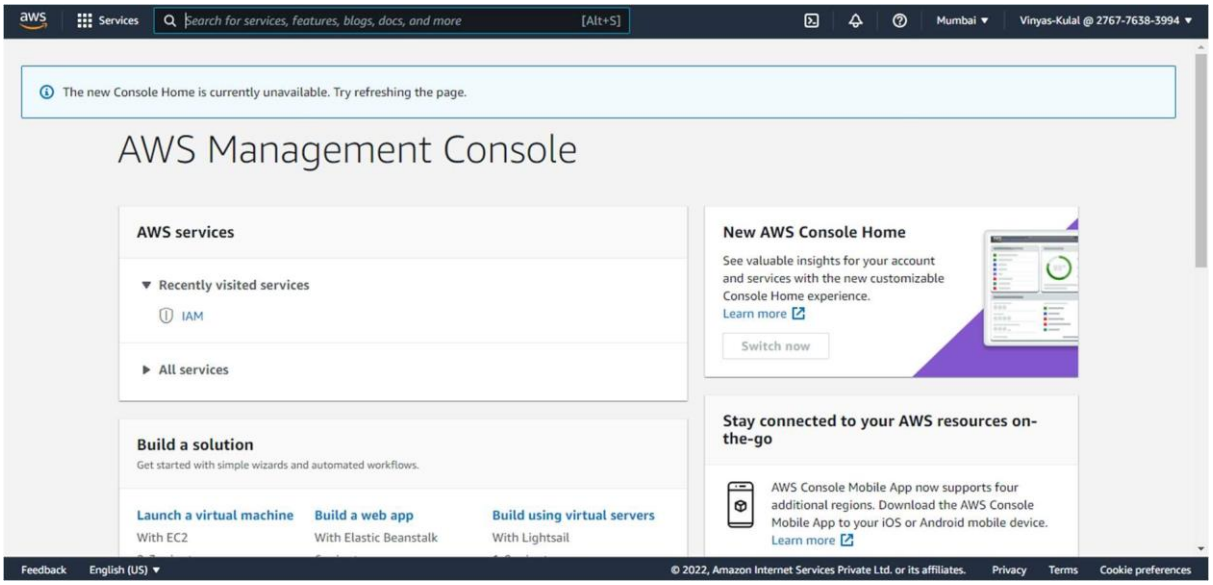
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type*
- [ ] **Access key - Programmatic access** — Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- [x] **Password - AWS Management Console access** — Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*
- (•) Autogenerated password
- ( ) Custom password

* Required | Cancel | Next: Permissions

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Mumbai
Vinyas-Kulal @ 2767-7638-3994
The new Console Home is currently unavailable. Try refreshing the page.
AWS Management Console
AWS services
Recently visited services
IAM
All services
New AWS Console Home
See valuable insights for your account and services with the new customizable Console Home experience.
Learn more
Switch now
Build a solution
Get started with simple wizards and automated workflows.
Launch a virtual machine
With EC2
Build a web app
With Elastic Beanstalk
Build using virtual servers
With Lightsail
Stay connected to your AWS resources on-the-go
AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device.
Learn more
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences

AWS VPC

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | Mumbai | Vinyas-Kulal @ 2767-7638-3994

IPv6 CIDR block Info

- No IPv6 CIDR block
- IPAM-allocated IPv6 CIDR block
- Amazon-provided IPv6 CIDR block
- IPv6 CIDR owned by me

Tenancy Info

Default

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	aws-vpc	Remove

Add new tag

You can add 49 more tags.

Cancel | Create VPC

Feedback | English (US) | © 2022, Amazon Internet Services Private Ltd. or its affiliates. | Privacy | Terms | Cookie preferences

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | Mumbai | Vinyas-Kulal @ 2767-7638-3994

VPC > Your VPCs > Create VPC

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or create VPC, subnets, etc.

- VPC only
- VPC, subnets, etc.

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

aws-vpc

IPv4 CIDR block Info

- IPv4 CIDR manual input
- IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block Info

aws | Services | Search for services, features, blogs, docs, and more [Alt+S] | Mumbai | Vinyas-Kulal @ 2767-7638-3994

New VPC Experience

Tell us what you think

- VPC Dashboard
- EC2 Global View New

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints New
- Endpoint Services
- NAT Gateways

You successfully created vpc-0ef035dc17bb4bb3e / aws-vpc

VPC > Your VPCs > vpc-0ef035dc17bb4bb3e

vpc-0ef035dc17bb4bb3e / aws-vpc

Actions

Details Info

VPC ID vpc-0ef035dc17bb4bb3e	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-082731ecc8bd6d430	Main route table rtb-09cfe9a843907eb3c	Main network ACL acl-0a38d9c9c50d5abc9
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool Amazon Associated	IPv6 CIDR 2406:da1a:72e:9f00::/56 Associated
Route 53 Resolver DNS Firewall rule groups -	Owner ID 276776383994		

Feedback | English (US) | © 2022, Amazon Internet Services Private Ltd. or its affiliates. | Privacy | Terms | Cookie preferences

Experiment 4: Amazon Web Services IAM Post Lab Questions

Q1. What is AWS Identity and Access Management (IAM)?

AWS Identity and Access Management (IAM) provides fine-grained access control across all of AWS. With IAM, you can specify who can access which services and resources, and under which conditions. With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.

Q2. What problems does IAM solve?

A robust IAM solution can ease management pains, streamline provisioning and deprovisioning, and boost user productivity, while lowering costs, reducing demands on IT, and providing the enterprise with comprehensive data to assist in complying with regulatory standards. In addition, enterprises can ensure security by deploying solutions with strong multifactor authentication, while eliminating user frustration by delivering seamless access to cloud-based applications through SSO. Furthermore, as identity and access management become increasingly complex, the ability to create policies based on granular, contextual information will become more and more important. IAM solutions that can collect and make decisions based on user identity, location, device, and the requested resource will allow enterprises to deliver quick access to bona fide employees, partners, contractors, or guests—and easily revoke or deny privileges to unauthorized users.

Q3. How are IAM users managed?

Manage IAM users and their access—You can create users in IAM, assign them individual security credentials (such as access keys, passwords, and multi-factor authentication devices), or request temporary security credentials to provide users access to AWS services and resources.

Q4. What kinds of security credentials can IAM users have?

AWS Identity and Access Management (IAM) lets you manage several types of long-term security credentials for IAM users:

- Passwords – Used to sign in to secure AWS pages, such as the AWS Management Console and the AWS Discussion Forums.
- Access keys – Used to make programmatic calls to AWS from the AWS APIs, AWS CLI, AWS SDKs, or AWS Tools for Windows PowerShell.
- Amazon CloudFront key pairs – Used for CloudFront to create signed URLs.
- SSH public keys – Used to authenticate to AWS CodeCommit repositories. IAM also lets you grant users temporary security credentials with a defined expiration for access to your AWS resources. For example, temporary access is useful when:
- Creating a mobile app with third-party sign-in.
- Creating a mobile app with custom authentication.
- Using your organization's authentication system to grant access to AWS resources.
- Using your organization's authentication system and SAML to grant access to AWS resources.
- Using web-based Single Sign-On (SSO) to the AWS Management Console.
- Delegating API access to third parties to access resources in your account or in another account you own.