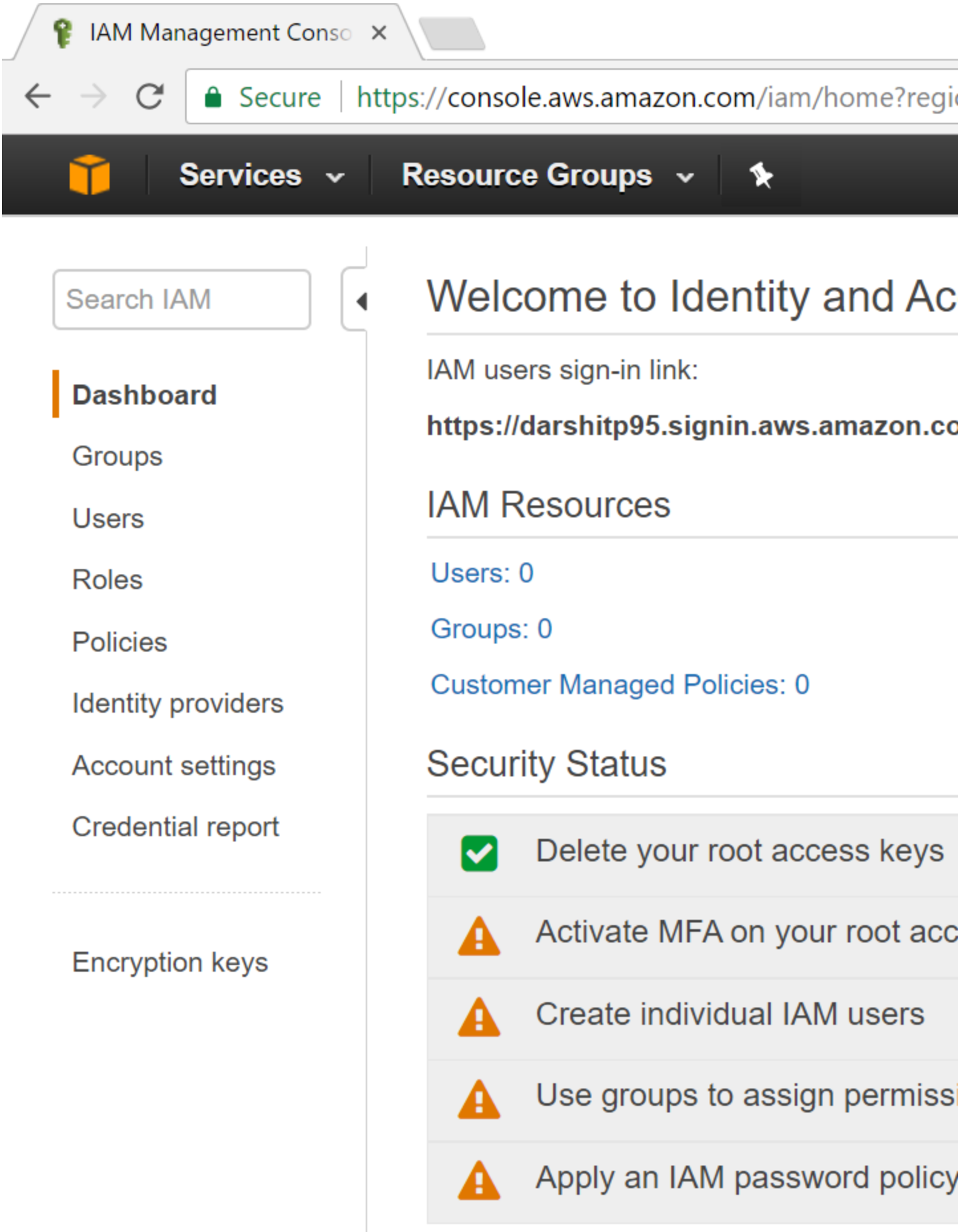
- IAM allows you to manage users and their level of access to the AWS console. It is important to understand IAM and how it works, both for exam and for administering a company's AWS account in real life.

What does IAM give you ?

- Centralized control of your AWS account
- Shared access to your AWS account
- Granular permissions
- Identity Federation (means we can connect IAM to active directory, FB, LinkedIN,etc)
- Multifactor Authentication
- Provide temporary access for users/devices and services where necessary
- Allows you to set up your own password rotation policy
- Integrates with many different AWS services
- Supports PCI DSS compliance ????????

Critical Terms :

- Users - End Users (think people)
- Groups - A collection of users under one set of permissions (finance group, IT group,etc)
- Roles - You create roles and can then assign them to AWS resources. (e.g. you create VM/EC2 instance and you might give a role in order to access S3, and that instance can write directly into S3 and no need to set passwords or anything.)
- Policies - A document that defines one (or more permissions). You apply/attach policies to users/group/role.


IAM Management Conso
Secure
https://console.aws.amazon.com/iam/home?regi
Services
Resource Groups
Search IAM
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys
Welcome to Identity and Ac
IAM users sign-in link:
https://darshitp95.signin.aws.amazon.co
IAM Resources
Users: 0
Groups: 0
Customer Managed Policies: 0
Security Status
Delete your root access keys
Activate MFA on your root acc
Create individual IAM users
Use groups to assign permissi
Apply an IAM password policy

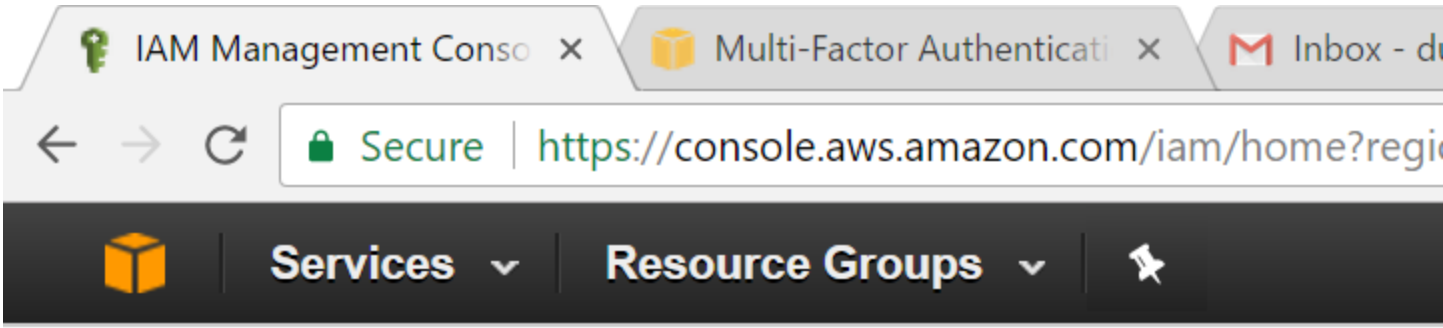
- Activite MFA on your root account :

MFA : Multi-factor authentication. Root account is simply the email address we use to sign up. So as we are signed up as a root account, we have access of deploying 20 VMs, and so on and other unlimited things.

Now as an organization I don't want my all employees to have same access. Say Human resources department should have only access as a read files only on S3 cloud. So what Amazon recommends by this service IAM is you login to root once or twice when you need but create number of users in AWS account and setup permissions

Coming back to our point, we need to do this because incase if anyone finds our username and password and it will not have access to the root unless it has **this** physical device.

- Create Individual IAM users



Set user details

You can add multiple users at once with the same access type and permi

User name* Megaranger

Dp

Add another user

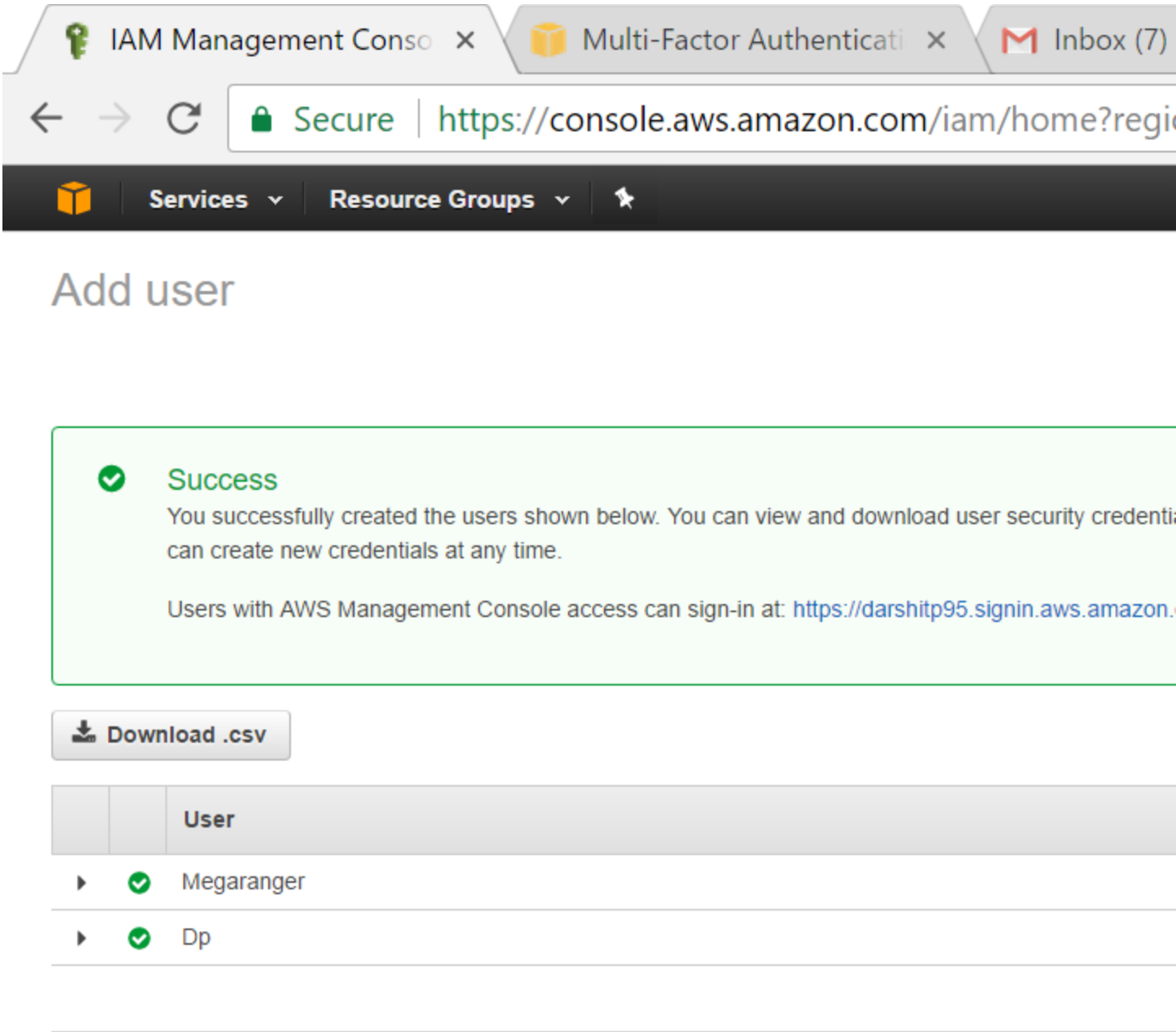
Select AWS access type

Select how these users will access AWS. Access keys and autogenerate

Access type* **Programmatic acce**
Enables an **access k**
tools.

AWS Management C
Enables a **password**

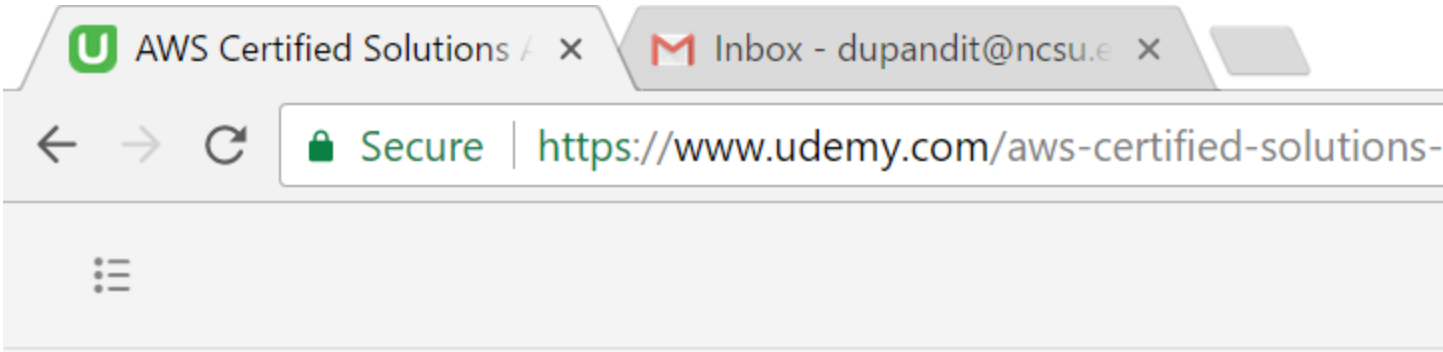
Access Type : Console access means the way it is showing on image right now. Console to add user, grant access,etc. Programmatic access means access by using AWS API, CLI or other development tools.


IAM Management Conso
Multi-Factor Authenticati
Inbox (7)
Secure
https://console.aws.amazon.com/iam/home?regi
Services
Resource Groups
Add user
Success
You successfully created the users shown below. You can view and download user security credentia
can create new credentials at any time.
Users with AWS Management Console access can sign-in at: https://darshitp95.signin.aws.amazon.
Download .csv
User
Megaranger
Dp

Group name - sys-admin, Policy type- admin

Create a billing alarm --- sends you email alerts when you have spent more than 10$ of access per month.

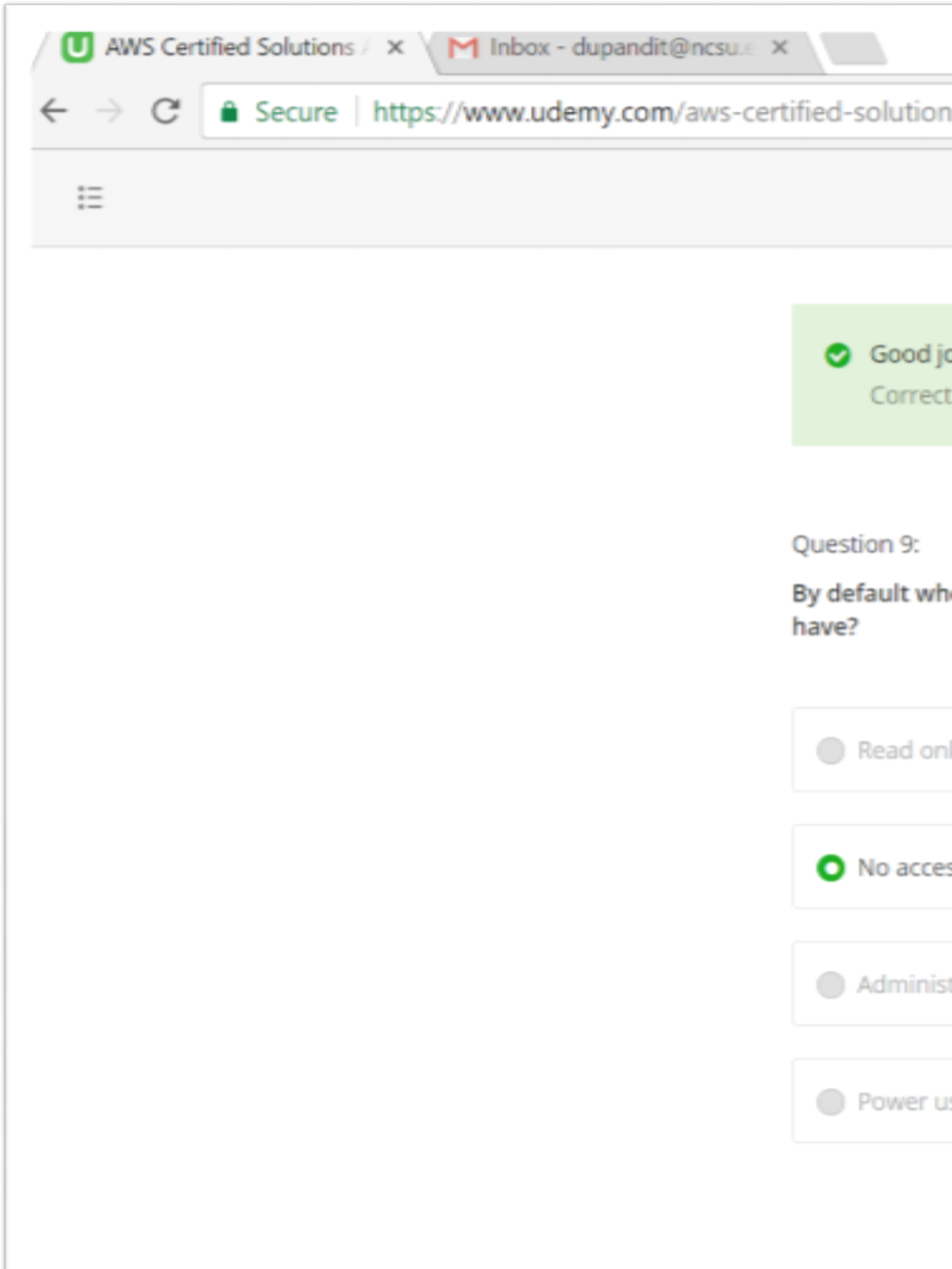
- IAM is universal. It does not apply to regions at this time
- Root account has complete admin access by default. It has administrator access
- New users have NO permissions when first created
- New users are assigned 'Access key ID and Secret Access Keys' when first created
- These are not the same as a password, and you cannot use the Access Key ID and Secret Access key to LOGIN to the console. You can use this to access AWS via the APIs and command Line however.
- If we lose them, we need to regenerate them.
- Always setup Multifactor Authentication on your root account
- You can create and customize your own password rotation policies
- Power users cannot manage groups and user with IAM
- Power users have access to all AWS services except for management of groups and users within IAM.
- IAM settings are set globally. If you shift your organizations account, it will not affect IAM configurations
- New client considering move to AWS services (do not have account yet). First thing company should do is setup account using their company's email address.



Question 7:

You are a security staff who has sta AWS console. You the secret access administrators ar and their access k cannot sign in. Wh

- You have no must apply t
- Your user is network. Thi
- You have no they will not
- You cannot Key, instead this passwo


AWS Certified Solutions
Inbox - dupandit@ncsu.
Secure
https://www.udemy.com/aws-certified-solution
Good jo
Correct
Question 9:
By default wh
have?
Read onl
No acces
Administ
Power us