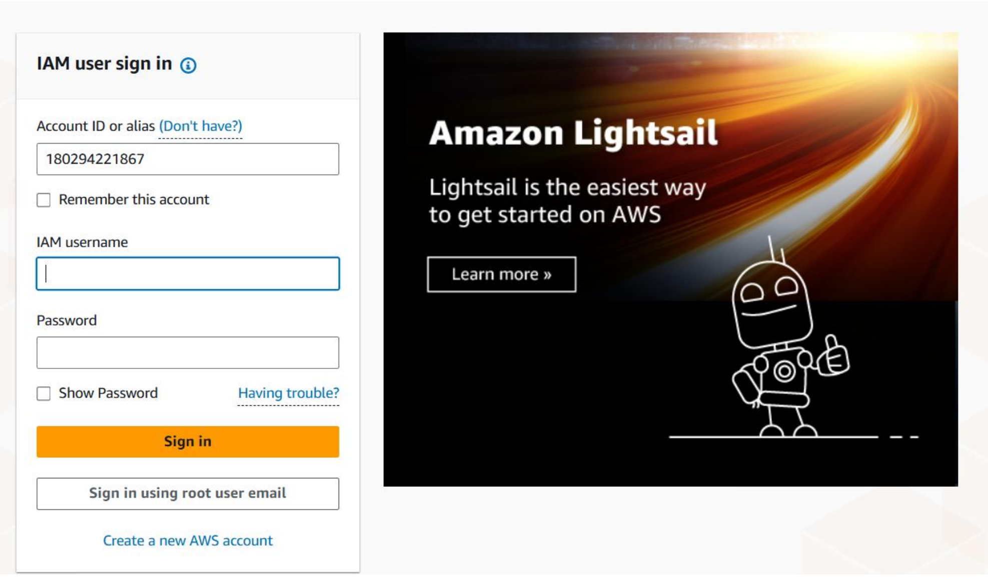
Assignment 2

1) Create a new IAM user , Enable MFA , create sign in password at sign in , grant user admin Permission ?

⇨ Go to aws console login > select sign in using root user email > and login has root user



IAM user sign in

Account ID or alias (Don't have?)

180294221867

□ Remember this account

IAM username

Password

□ Show Password

Having trouble?

Sign in
Sign in using root user email
Create a new AWS account
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »

⇨ Then go to IAM > under Access Management select Users

# Enabling MFA

⇨ In IAM dashboard enable MFA

⇨ If all the options gets positive then your MFA is enabled using you respective authenticaton

# Creating IAM user

⇨ Go to user section in acess management and select create user

⇨ Name the user

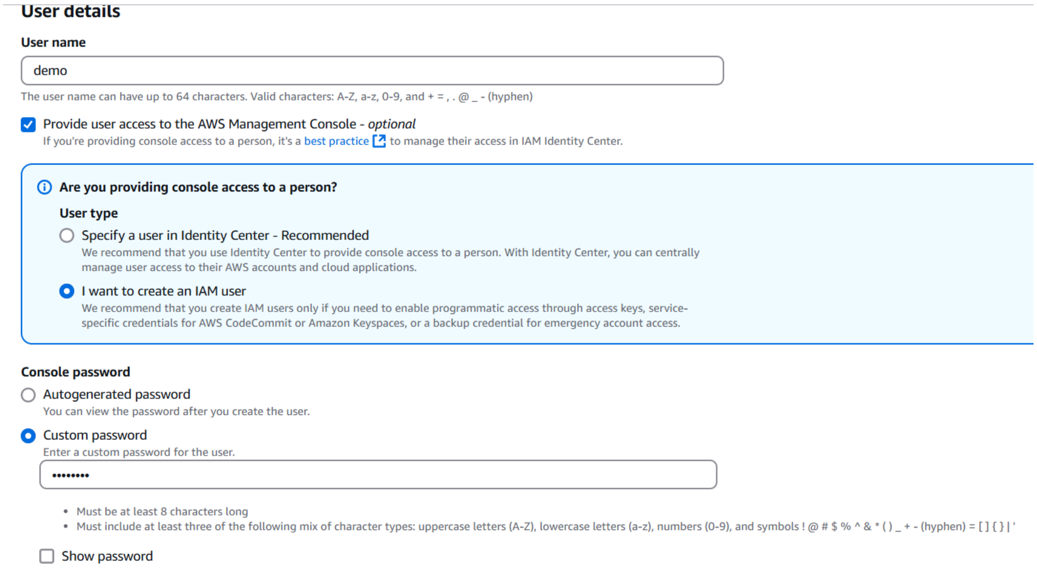
Assignment 2

⇨ Select provide user access to the AWS Management console

⇨ Now, select " I want to create IAM"

⇨ Give you custom name

⇨ Then click next



User details

User name

demo

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☑ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

ⓘ **Are you providing console access to a person?**

User type

○ Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

● I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

○ Autogenerated password
You can view the password after you create the user.

● Custom password
Enter a custom password for the user.

••••••••

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # $ % ^ & * ( ) _ + - (hyphen) = [ ] { } | '

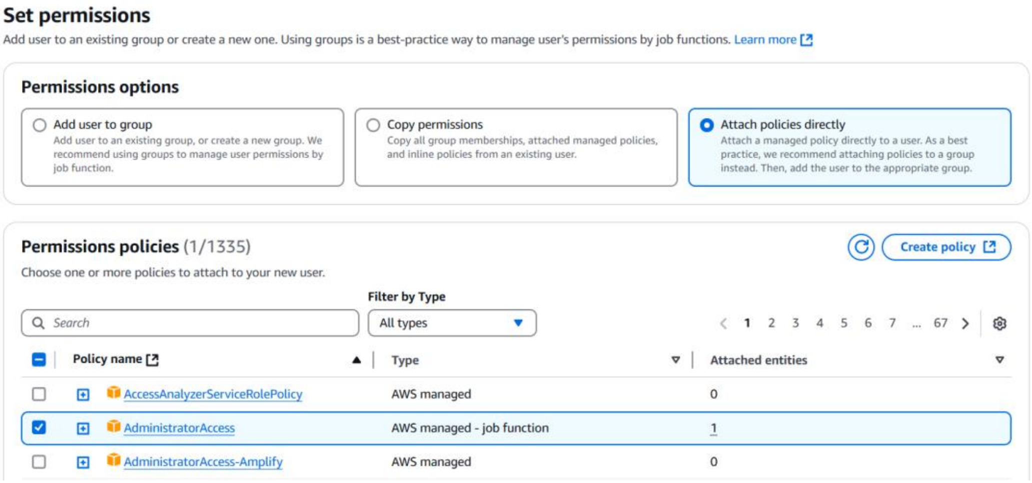
□ Show password

⇨ Under set permissions:

- Select "Attach policies directly"

# granting user admin Permission to the user

- Under permission policies select "Administrator Accesss"



Set permissions

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

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1335)

Choose one or more policies to attach to your new user.

Filter by Type: All types

	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0
☑	AdministratorAccess	AWS managed - job function	1
□	AdministratorAccess-Amplify	AWS managed	0

Assignment 2

⇨ Now select create to create user

# creating sign in password at sign in

⇨ Now, login using your user_name , and custom password and then reset your new permanent password