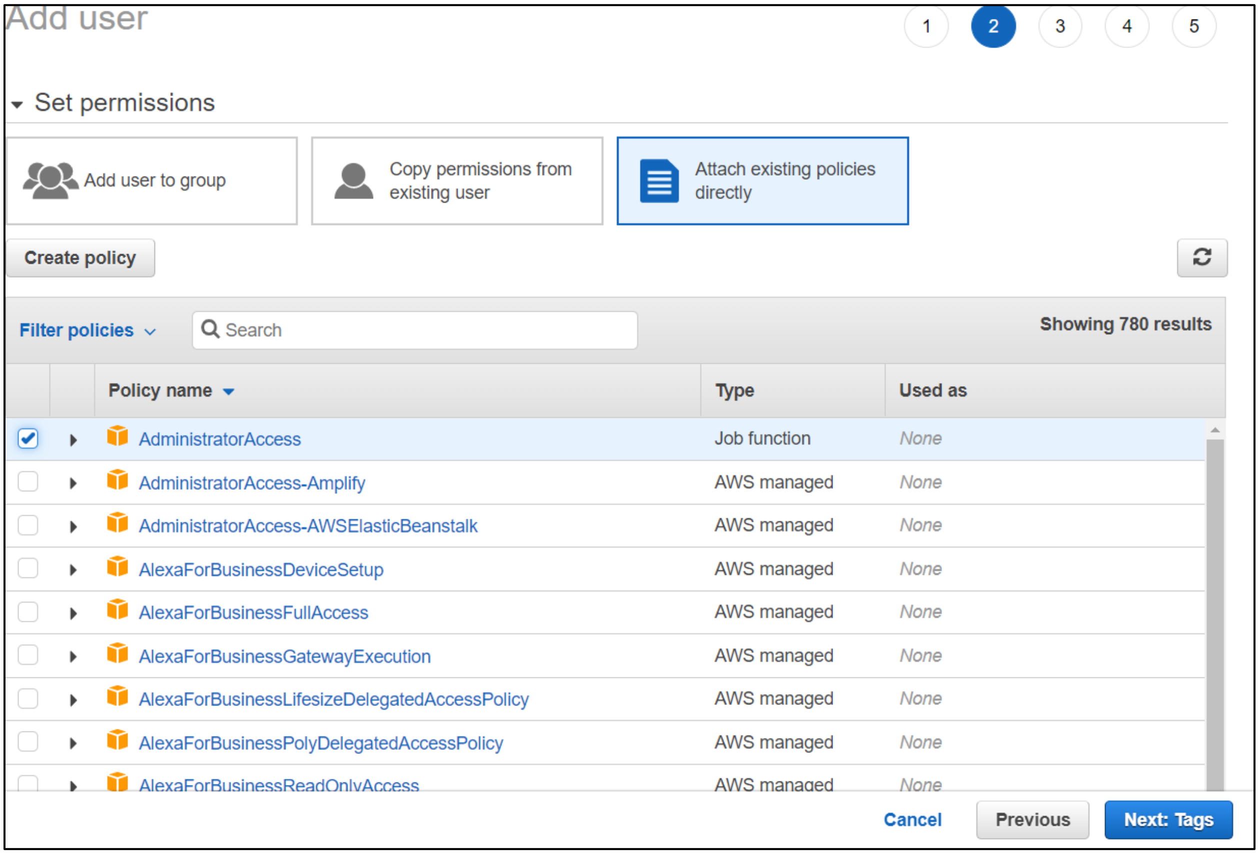
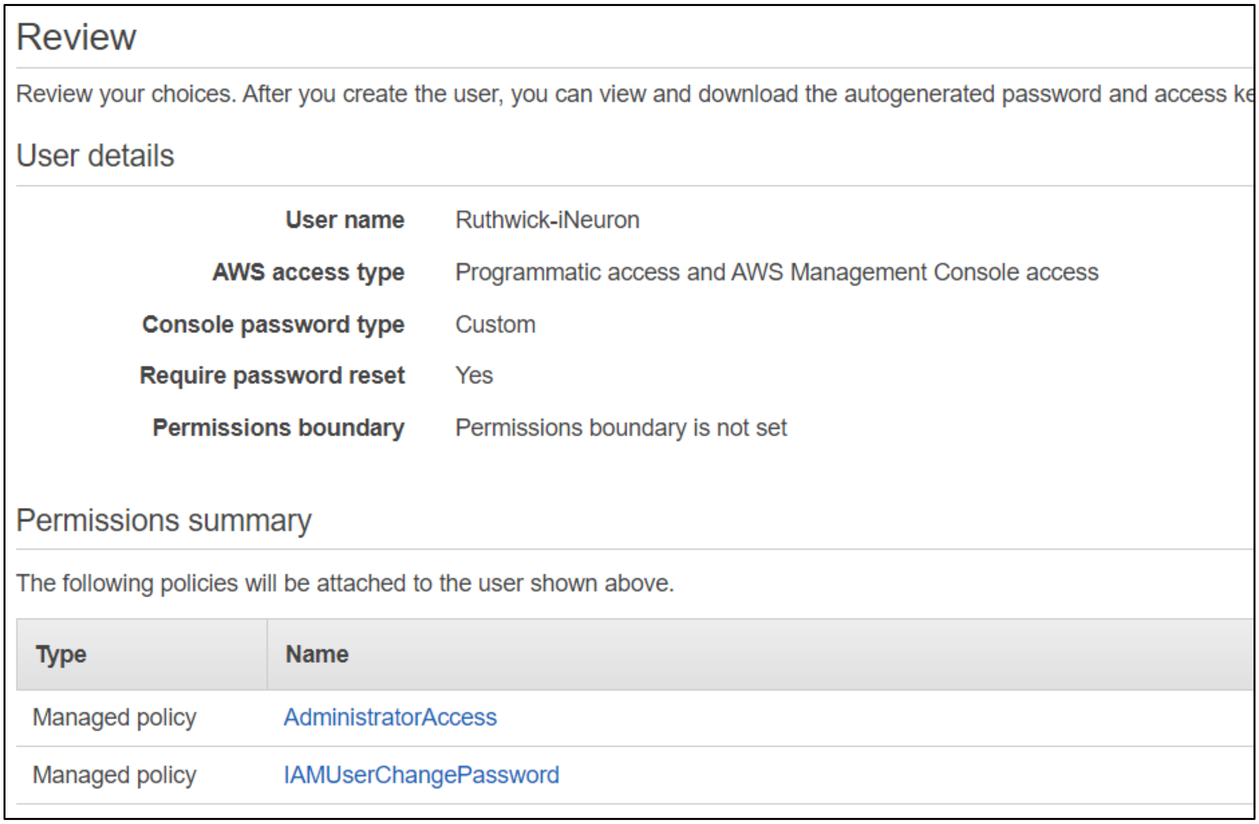
Assignment sheet for IAM

Assignment 1:- Create an IAM user with username ofyour own wish and grantadministrator policy.



		Policy name	Type	Used as
☑	▸	AdministratorAccess	Job function	None
□	▸	AdministratorAccess-Amplify	AWS managed	None
□	▸	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None
□	▸	AlexaForBusinessDeviceSetup	AWS managed	None
□	▸	AlexaForBusinessFullAccess	AWS managed	None
□	▸	AlexaForBusinessGatewayExecution	AWS managed	None
□	▸	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None
□	▸	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
□	▸	AlexaForBusinessReadOnlyAccess	AWS managed	None



Review

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

User details

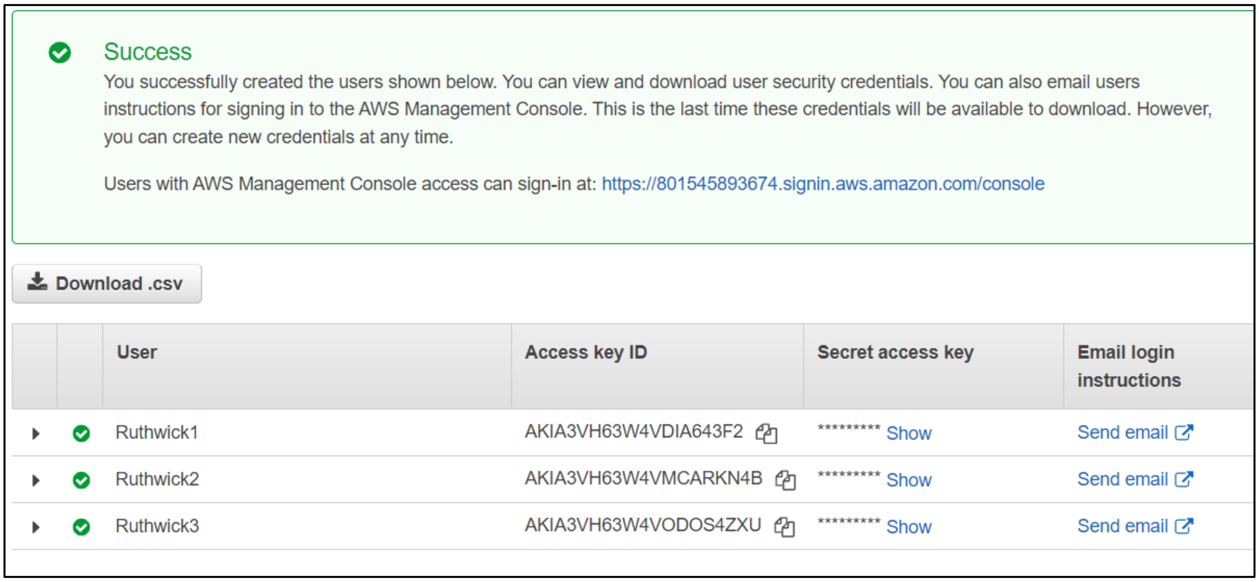
User name	Ruthwick-iNeuron
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess
Managed policy	IAMUserChangePassword

Assignment 2:- Hello students, in this assignmentyou need to prepare adevelopers team of avengers.- Create 3 IAM users of avengers and assign them in developer’s groups withIAM policy.

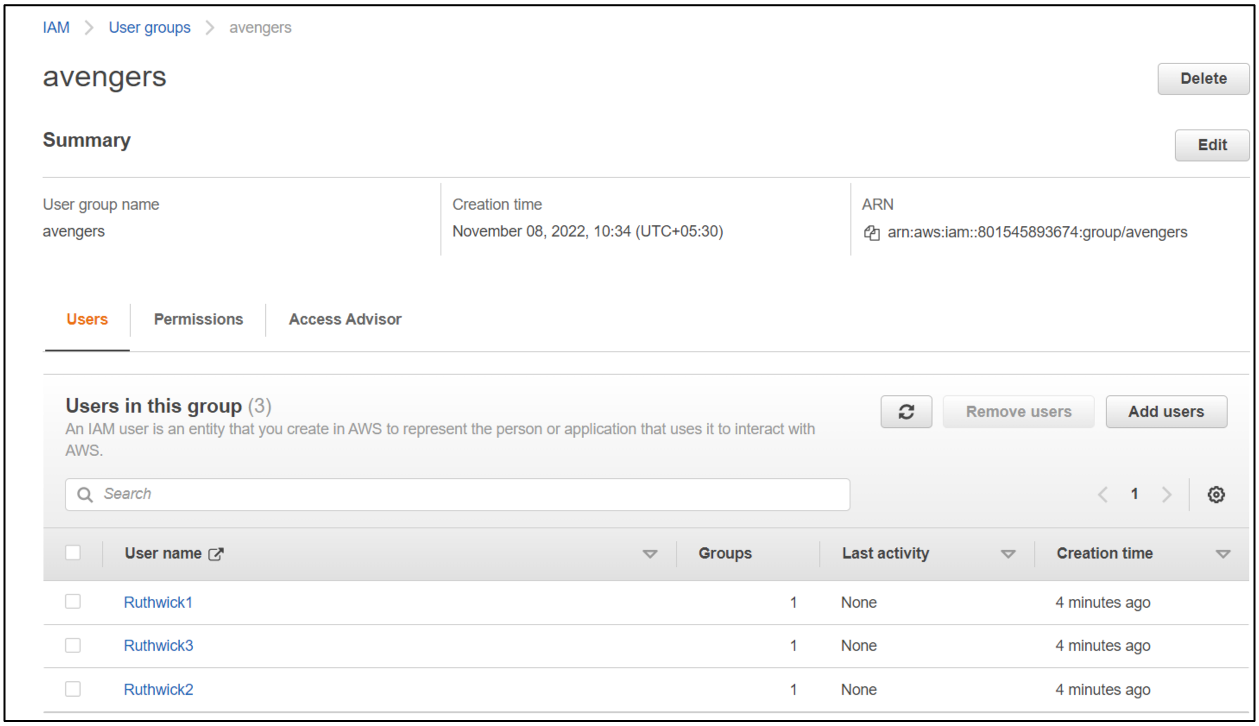


Success

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://801545893674.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Email login instructions
▸	✓	Ruthwick1	AKIA3VH63W4VDIA643F2	********* Show	Send email
▸	✓	Ruthwick2	AKIA3VH63W4VMCARKN4B	********* Show	Send email
▸	✓	Ruthwick3	AKIA3VH63W4VODOS4ZXU	********* Show	Send email



IAM > User groups > avengers

avengers

Summary

User group name
avengers

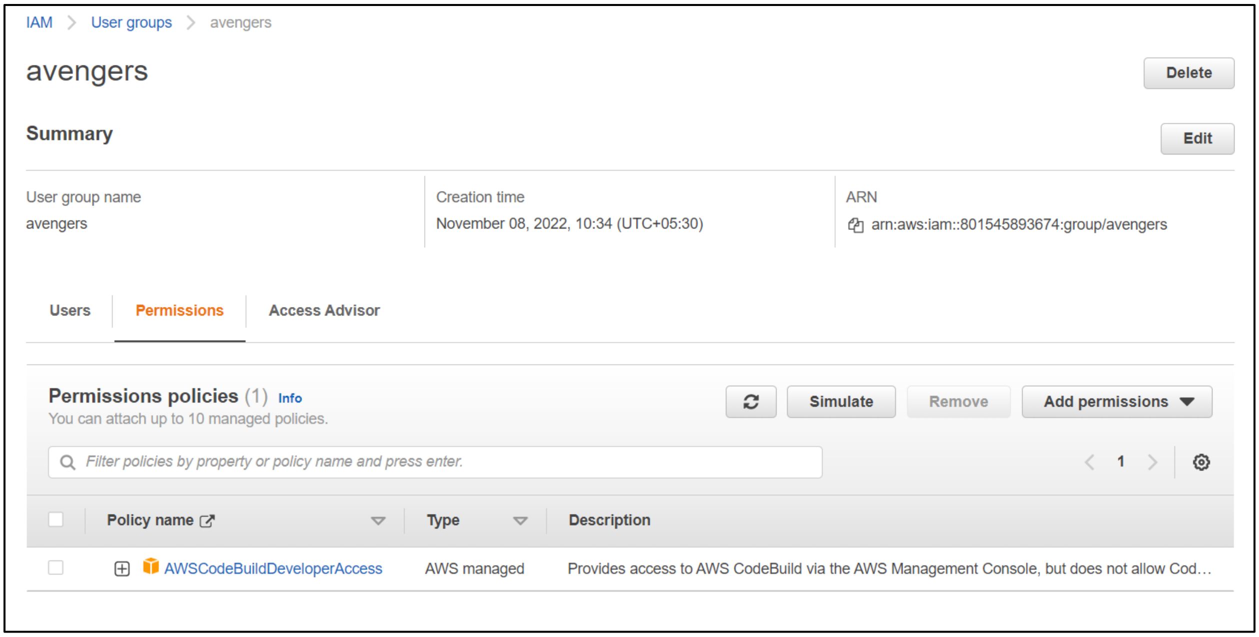
Creation time
November 08, 2022, 10:34 (UTC+05:30)

ARN
arn:aws:iam::801545893674:group/avengers

Users in this group (3)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

□	User name	Groups	Last activity	Creation time
□	Ruthwick1	1	None	4 minutes ago
□	Ruthwick3	1	None	4 minutes ago
□	Ruthwick2	1	None	4 minutes ago


IAM > User groups > avengers
Delete
Edit
Users
Permissions
Access Advisor
Simulate
Remove
Add permissions ▼
Info
Filter policies by property or policy name and press enter.
< 1 >

avengers

Summary

User group name
avengers

Creation time
November 08, 2022, 10:34 (UTC+05:30)

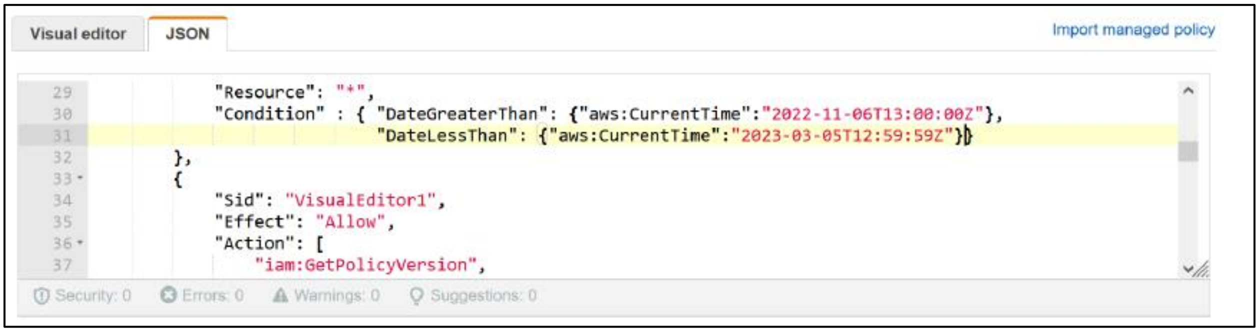
ARN
arn:aws:iam::801545893674:group/avengers

Permissions policies (1)
You can attach up to 10 managed policies.

□	Policy name	Type	Description
□	AWSCodeBuildDeveloperAccess	AWS managed	Provides access to AWS CodeBuild via the AWS Management Console, but does not allow Cod…

Assignment 3:- Define a condition in policy for expirationlike

"DateGreaterThan":{"aws:CurrentTime":"2020-04-01T00:00:00Z"},"DateLessThan":{"aws:CurrentTime":"2020-06-30T23:59:59Z"}Define the span of 4 months as per your wish



```
            "Resource": "*",
            "Condition" : { "DateGreaterThan": {"aws:CurrentTime":"2022-11-06T13:00:00Z"},
                            "DateLessThan": {"aws:CurrentTime":"2023-03-05T12:59:59Z"}}
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
```

Assignment 4:- Prepare 15 authentic MCQ questions related to IAM.

Q1: An explicit Deny in IAM precedes an explicit allow?

Options:

a>True

b>False

Q2: Which of the following sections in a policy specifies the entities to whom access to a resource is granted or denied?

Options:

a>Statement ID

b>Resources

c>Principal

d>Conditions

Q3: Which of the following is not an IAM best practice?

Options:

a>Delete user accounts, not in use

b>Attach policies to individual users

c>Manage permissions by adding users to groups

d>Enable MFA on user accounts

Q4: Which of the following set of credentials are used to log in to AWS programmatically? (Choose two)

Options:

a>Username

b>Access Key

c>Password

d>Secret Key

Q5: Which statement best describes IAM?

Options:

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.

Q6: You have created a new AWS account for your company, and you have also configured multi-factor authentication on the root account. You are about to create your new users. What strategy should you consider in order to ensure that there is good security on this account?

Options:

a> Require users to only be able to log in using biometric authentication.

b> Give all users the same password so that if they forget their password they can just ask their co-workers.

c> Restrict login to the corporate network only.

d> Enact a strong password policy: user passwords must be changed every 45 days, with each password containing a combination of capital letters, lowercase letters, numbers, and special symbols.

Q7: Using SAML (Security Assertion Markup Language 2.0), you can give your federated users single sign-on (SSO) access to the AWS Management Console.

Options:

a> False

b> True

Q8: Which of the following is not a component of IAM?

Options:

a>Roles

b>Users

c>Organizational Units

d>Groups

Q9: A new employee has just started work, and it is your job to give her administrator access to the AWS console. You have given her a username, an access key ID, and a secret access key, and you have generated a password for her. She is now able to log in to the AWS console, but she is unable to interact with any AWS services. What should you do next?

Options:

a>Ensure she is logging in to the AWS console from your corporate network and not the normal internet.

b>Grant her Administrator access by adding her to the Administrators' group.

c>Tell her to log out and try logging back in again.

d>Require multi-factor authentication for her user account.

Q10: Which of the following is not a feature of IAM?

Options:

a>IAM allows you to set up 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 accounts allowing single sign-on.

Q11: You are a security administrator working for a hotel chain. You have a new member of staff who has started as a systems administrator, and she will need full access to the AWS console. You have created the user account and generated the access key id and the secret access key. You have moved this user into the group where the other administrators are, and you have provided the new user with their secret access key and their access key id. However, when she tries to log in to the AWS console, she cannot. Why might that be?

Options:

a>Your user is trying to log in from the AWS console from outside the corporate network. This is not possible.

b>You have not yet activated multi-factor authentication for the user, so by default, they will not be able to log in.

c>You cannot log in to the AWS console using the Access Key ID / Secret Access Key pair. Instead, you must generate a password for the user, and supply the user with this password and your organization's unique AWS console login URL.

d>You have not applied the "log in from console" policy document to the user. You must apply this first so that they can log in.

Q12: You are a developer at a fast-growing start-up. Until now, you have used the root account to log in to the AWS console. However, as you have taken on more staff, you will now need to stop sharing the root account to prevent accidental damage to your AWS infrastructure. What should you do so that everyone can access the AWS resources they need to do their jobs? (Choose 2)

Options:

a>Create individual user accounts with minimum necessary rights and tell the staff to log in to the console using the credentials provided.

b>Give your users the root account credentials so that they can also sign in.

c>Create a customized sign-in link such as "yourcompany.signin.aws.amazon.com/console" for your new users to use to sign in with. d>Create an additional AWS root account for each new user.

Q13: What is an additional way to secure the AWS accounts of both the root account and new users alike?

Options:

a>Implement Multi-Factor Authentication for all accounts.

b>Store the access key id and secret access key of all users in a publicly accessible plain text document on S3 of which only you and members of your organization know the address to.

c>Configure the AWS Console so that you can only log in to it from your internal network IP address range.

d>Configure the AWS Console so that you can only log in to it from a specific IP Address range

Q14: IAM group:

a>Is the 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

Q15: IAM role:

a>Have credentials (password or access keys) associated with it

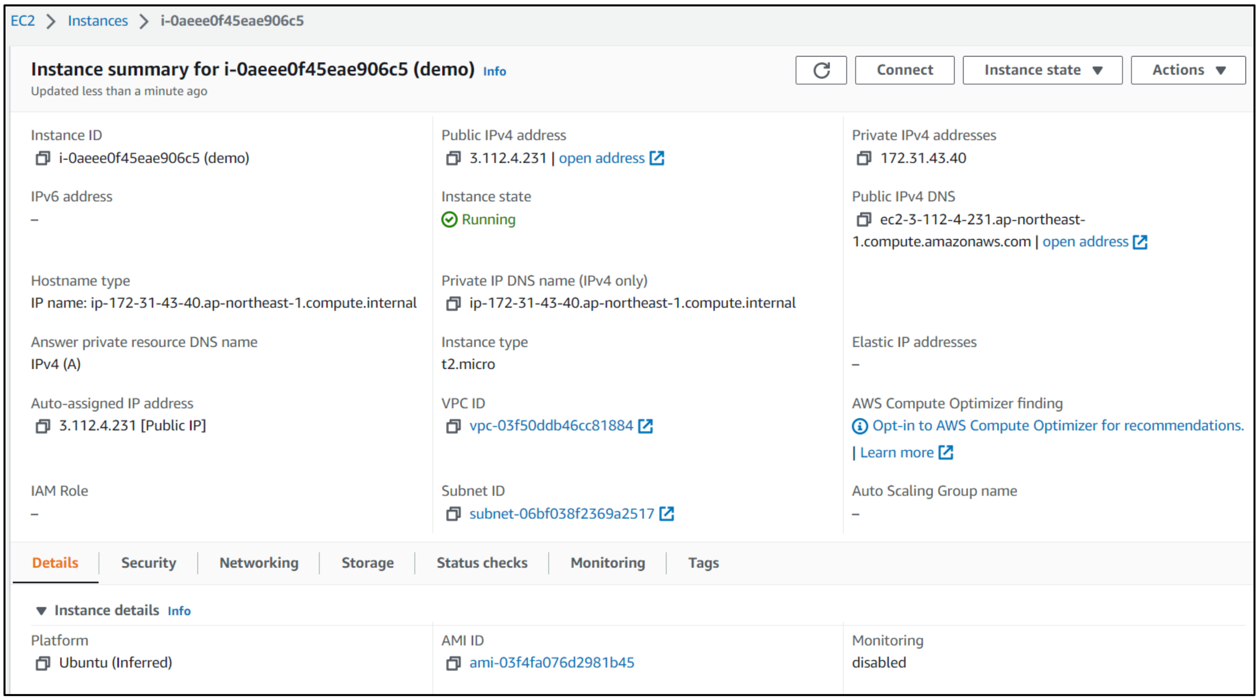
b>Does not have any credentials (password or access keys) associated with it

c>May or may not have credentials (password or access keys) associated with it

d>None of these

Solution of MCQs: 1b-2b-3b-4-5b-6d-7b-8c-9b-10a-11c-12a&c-13a-14b-15b

Assignment 5:- Launch your linux instance in IAMand update your machine.



EC2 > Instances > i-0aeee0f45eae906c5

Instance summary for i-0aeee0f45eae906c5 (demo) Info

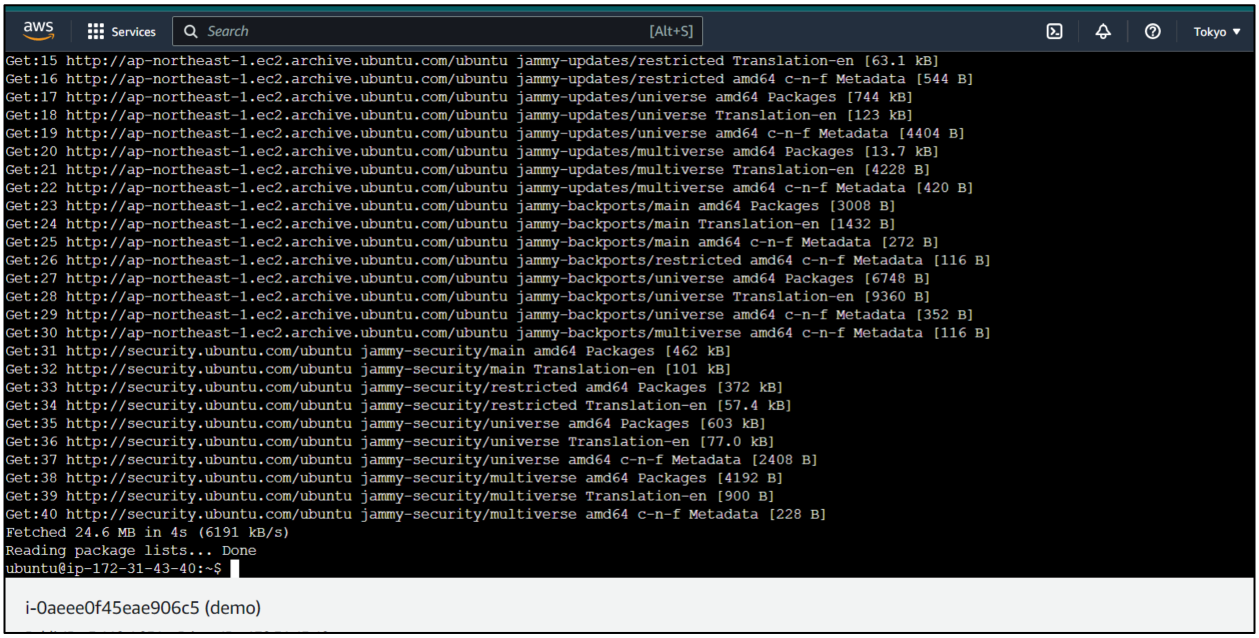
Updated less than a minute ago

Instance ID i-0aeee0f45eae906c5 (demo)	Public IPv4 address 3.112.4.231 | open address	Private IPv4 addresses 172.31.43.40
IPv6 address –	Instance state Running	Public IPv4 DNS ec2-3-112-4-231.ap-northeast-1.compute.amazonaws.com | open address
Hostname type IP name: ip-172-31-43-40.ap-northeast-1.compute.internal	Private IP DNS name (IPv4 only) ip-172-31-43-40.ap-northeast-1.compute.internal	
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	Elastic IP addresses –
Auto-assigned IP address 3.112.4.231 [Public IP]	VPC ID vpc-03f50ddb46cc81884	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. | Learn more
IAM Role –	Subnet ID subnet-06bf038f2369a2517	Auto Scaling Group name –

▼ Instance details Info

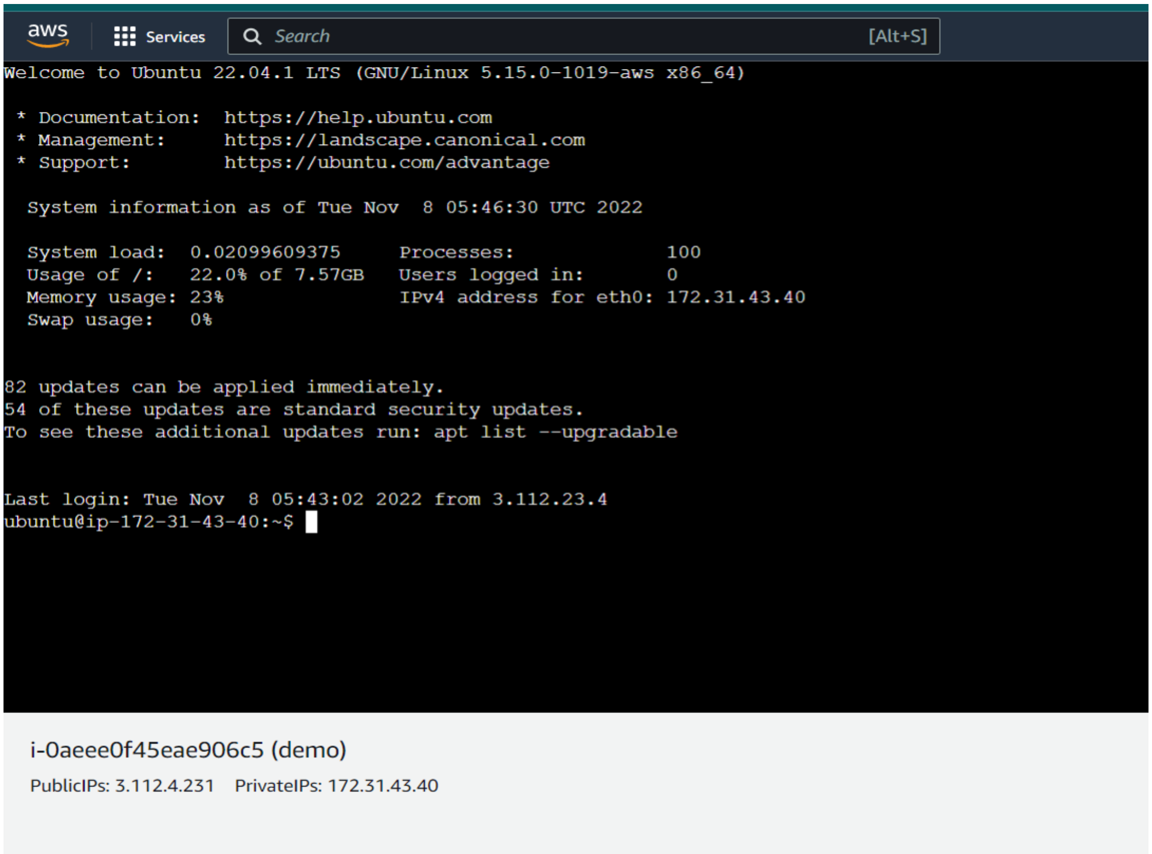
Platform Ubuntu (Inferred)	AMI ID ami-03f4fa076d2981b45	Monitoring disabled

To update we need to use: sudo apt-get update



```
Get:15 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [63.1 kB]
Get:16 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [544 B]
Get:17 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [744 kB]
Get:18 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [123 kB]
Get:19 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [4404 B]
Get:20 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [13.7 kB]
Get:21 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [4228 B]
Get:22 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [420 B]
Get:23 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [3008 B]
Get:24 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [1432 B]
Get:25 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [272 B]
Get:26 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [6748 B]
Get:28 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [9360 B]
Get:29 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [352 B]
Get:30 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [462 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [101 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [372 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [57.4 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [603 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [77.0 kB]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [2408 B]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [4192 B]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/multiverse Translation-en [900 B]
Get:40 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 c-n-f Metadata [228 B]
Fetched 24.6 MB in 4s (6191 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-43-40:~$
```

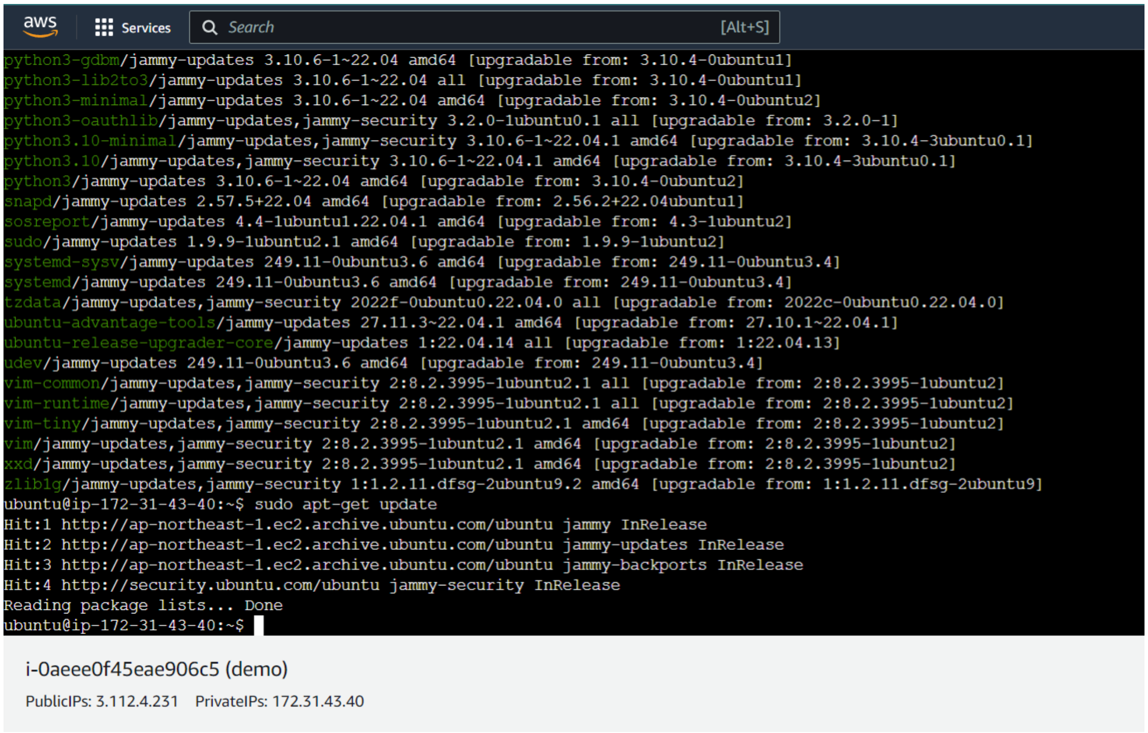
i-0aeee0f45eae906c5 (demo)



```
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1019-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Nov  8 05:46:30 UTC 2022

  System load:  0.02099609375     Processes:             100
  Usage of /:   22.0% of 7.57GB   Users logged in:       0
  Memory usage: 23%               IPv4 address for eth0: 172.31.43.40
  Swap usage:   0%


82 updates can be applied immediately.
54 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Tue Nov  8 05:43:02 2022 from 3.112.23.4
ubuntu@ip-172-31-43-40:~$
```

i-0aeee0f45eae906c5 (demo)

PublicIPs: 3.112.4.231   PrivateIPs: 172.31.43.40



```
python3-gdbm/jammy-updates 3.10.6-1~22.04 amd64 [upgradable from: 3.10.4-0ubuntu1]
python3-lib2to3/jammy-updates 3.10.6-1~22.04 all [upgradable from: 3.10.4-0ubuntu1]
python3-minimal/jammy-updates 3.10.6-1~22.04 amd64 [upgradable from: 3.10.4-0ubuntu2]
python3-oauthlib/jammy-updates,jammy-security 3.2.0-1ubuntu0.1 all [upgradable from: 3.2.0-1]
python3.10-minimal/jammy-updates,jammy-security 3.10.6-1~22.04.1 amd64 [upgradable from: 3.10.4-3ubuntu0.1]
python3.10/jammy-updates,jammy-security 3.10.6-1~22.04.1 amd64 [upgradable from: 3.10.4-3ubuntu0.1]
python3/jammy-updates 3.10.6-1~22.04 amd64 [upgradable from: 3.10.4-0ubuntu2]
snapd/jammy-updates 2.57.5+22.04 amd64 [upgradable from: 2.56.2+22.04ubuntu1]
sosreport/jammy-updates 4.4-1ubuntu1.22.04.1 amd64 [upgradable from: 4.3-1ubuntu2]
sudo/jammy-updates 1.9.9-1ubuntu2.1 amd64 [upgradable from: 1.9.9-1ubuntu2]
systemd-sysv/jammy-updates 249.11-0ubuntu3.6 amd64 [upgradable from: 249.11-0ubuntu3.4]
systemd/jammy-updates 249.11-0ubuntu3.6 amd64 [upgradable from: 249.11-0ubuntu3.4]
tzdata/jammy-updates,jammy-security 2022f-0ubuntu0.22.04.0 all [upgradable from: 2022c-0ubuntu0.22.04.0]
ubuntu-advantage-tools/jammy-updates 27.11.3~22.04.1 amd64 [upgradable from: 27.10.1~22.04.1]
ubuntu-release-upgrader-core/jammy-updates 1:22.04.14 all [upgradable from: 1:22.04.13]
udev/jammy-updates 249.11-0ubuntu3.6 amd64 [upgradable from: 249.11-0ubuntu3.4]
vim-common/jammy-updates,jammy-security 2:8.2.3995-1ubuntu2.1 all [upgradable from: 2:8.2.3995-1ubuntu2]
vim-runtime/jammy-updates,jammy-security 2:8.2.3995-1ubuntu2.1 all [upgradable from: 2:8.2.3995-1ubuntu2]
vim-tiny/jammy-updates,jammy-security 2:8.2.3995-1ubuntu2.1 amd64 [upgradable from: 2:8.2.3995-1ubuntu2]
vim/jammy-updates,jammy-security 2:8.2.3995-1ubuntu2.1 amd64 [upgradable from: 2:8.2.3995-1ubuntu2]
xxd/jammy-updates,jammy-security 2:8.2.3995-1ubuntu2.1 amd64 [upgradable from: 2:8.2.3995-1ubuntu2]
zlib1g/jammy-updates,jammy-security 1:1.2.11.dfsg-2ubuntu9.2 amd64 [upgradable from: 1:1.2.11.dfsg-2ubuntu9]
ubuntu@ip-172-31-43-40:~$ sudo apt-get update
Hit:1 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ap-northeast-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Reading package lists... Done
ubuntu@ip-172-31-43-40:~$
```

i-0aeee0f45eae906c5 (demo)

PublicIPs: 3.112.4.231   PrivateIPs: 172.31.43.40

EC-2 Instance running Linux OS (Ubuntu) in Iam USER created and update successfully.