

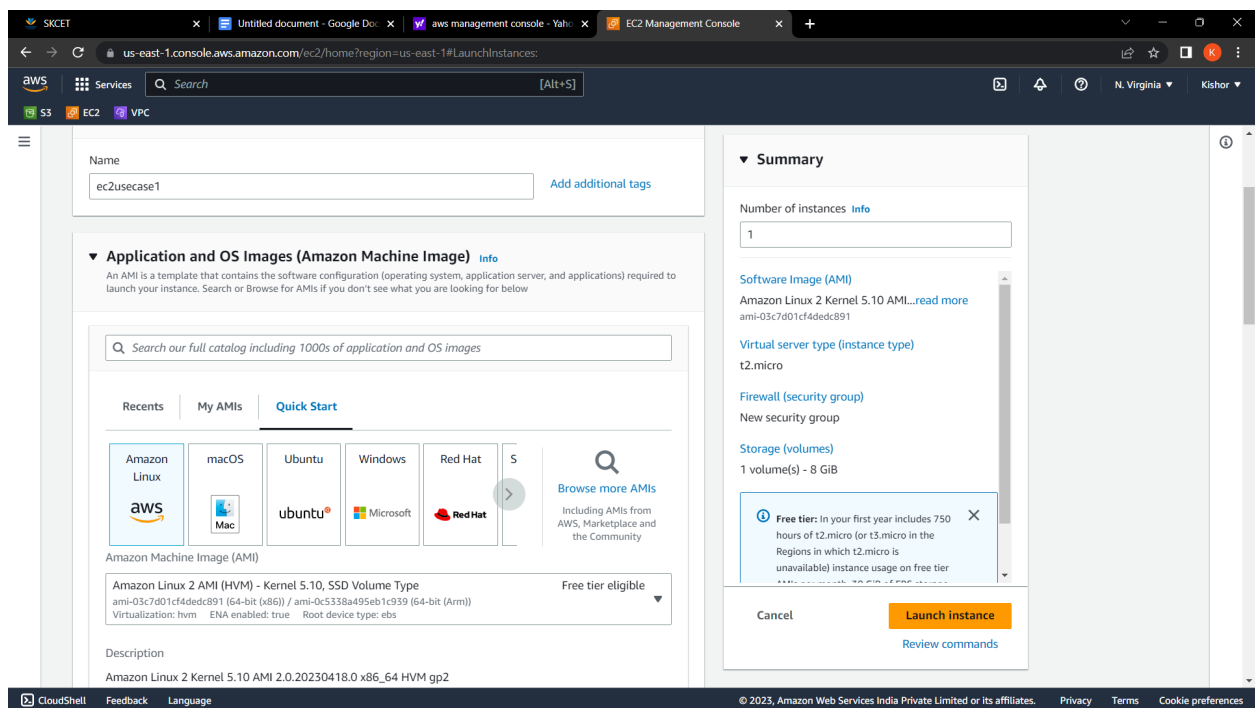
Cloud Computing

1.

Q1.

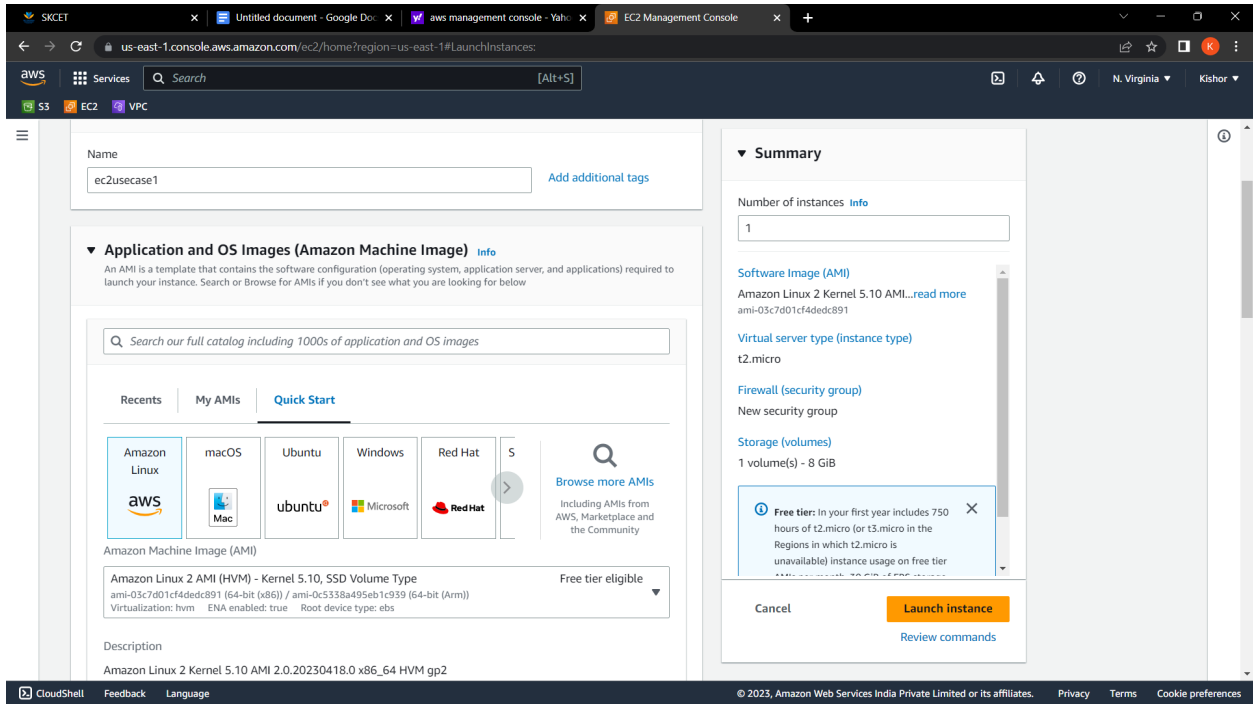
Create an EC2 Instance in the us-east-1 region with the following requirements.

Give the Name tag of both EC2 instance & keypair as "ec2usecase1"(Name).
(4 Marks)

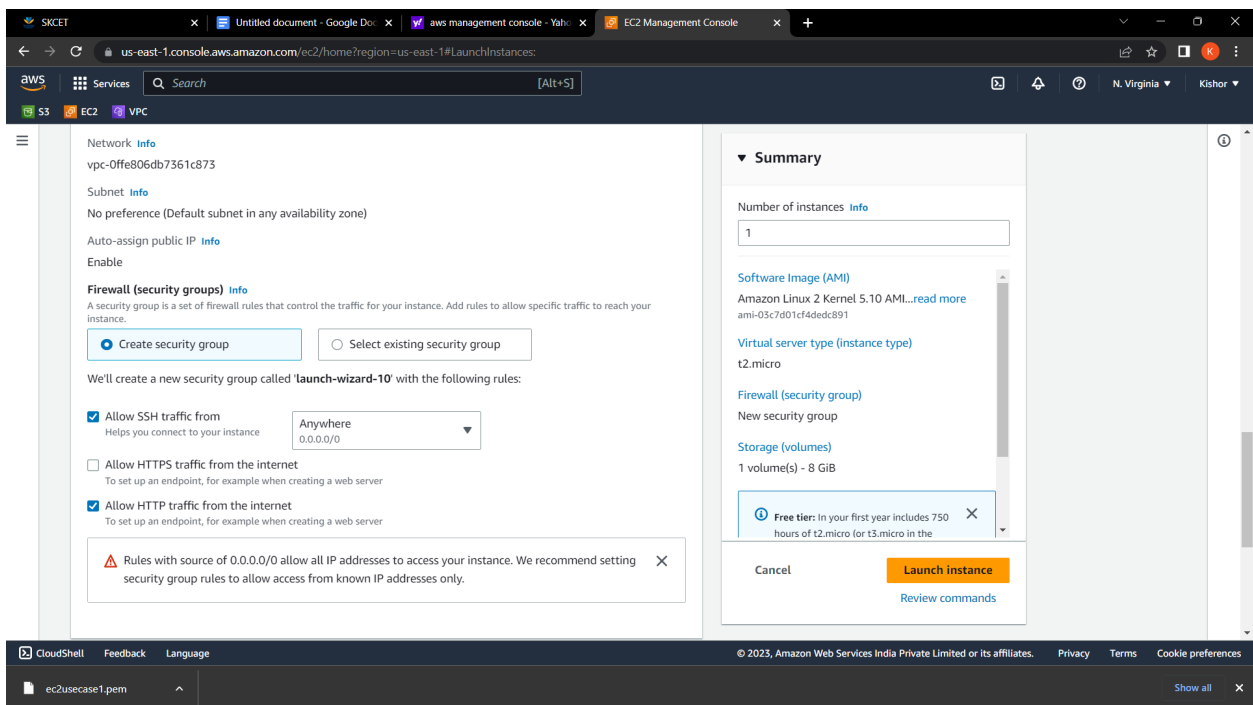


EC2 instance AMI should be "Amazon Linux 2".

(4 Marks)

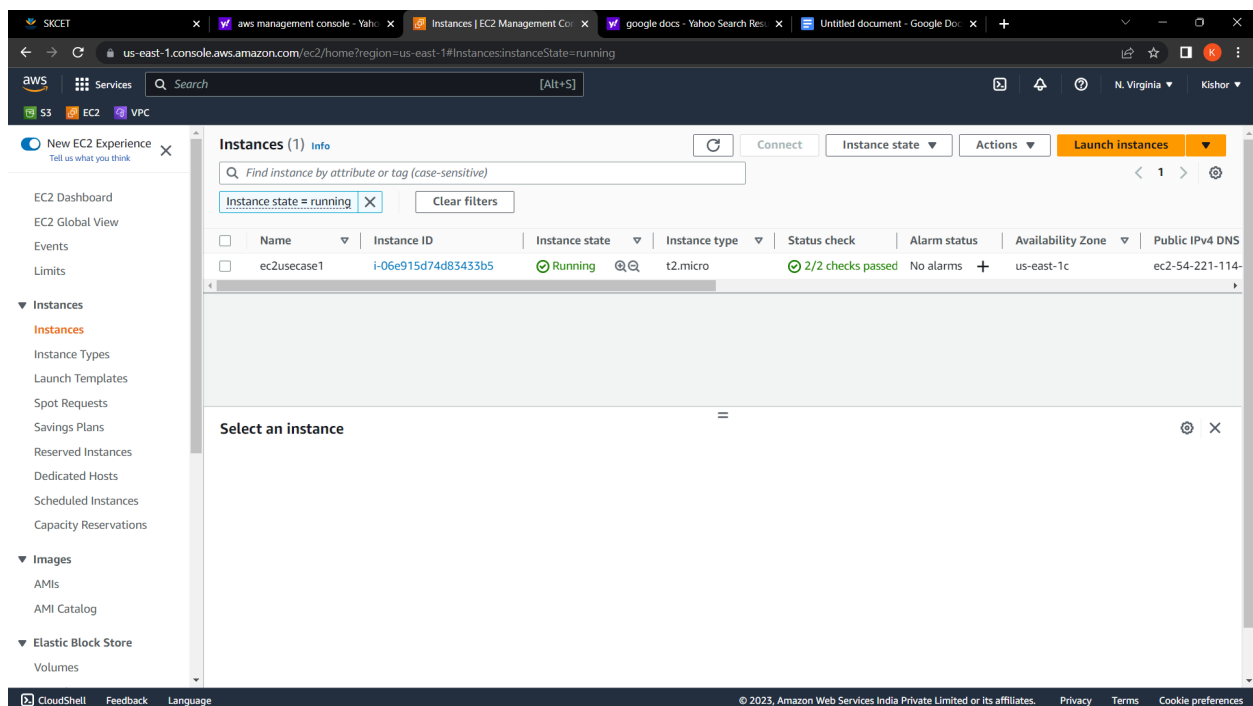
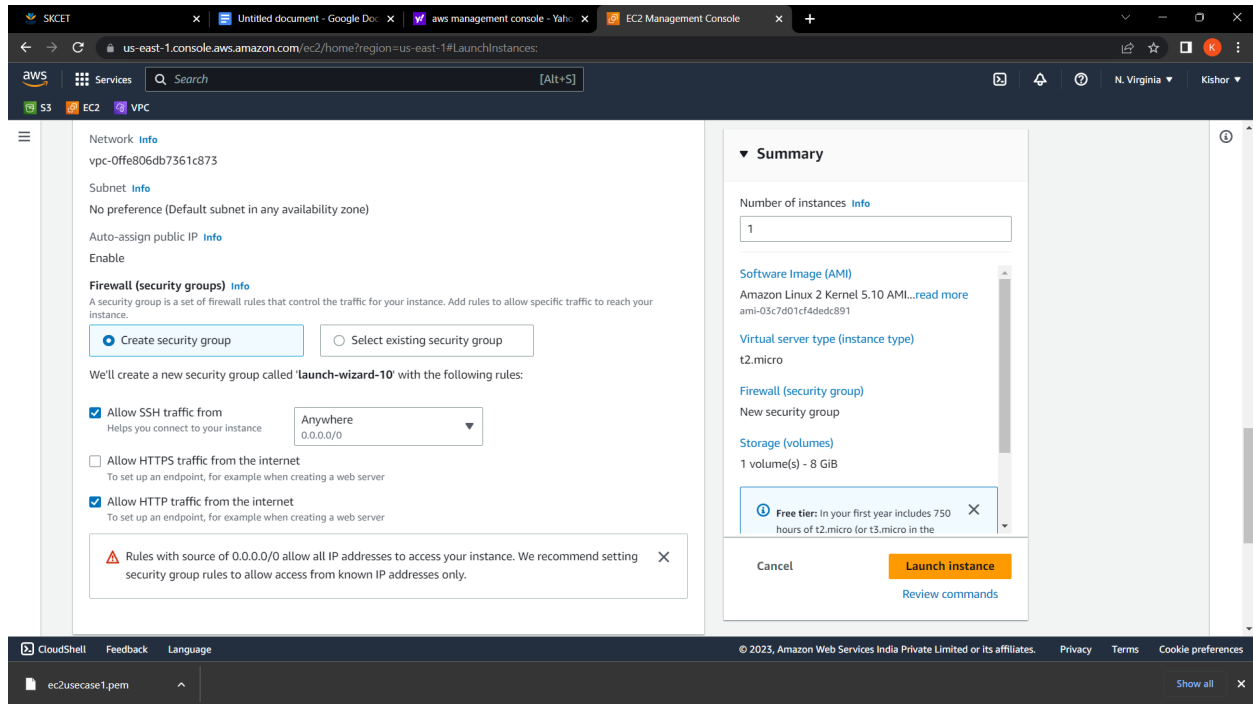


Allow SSH traffic for taking putty remote connection.
(4 Marks)



Allow HTTP traffic from the internet for reaching website requests.

(4 Marks)



2.

Q2.

Create an IAM group called 'Network-L1-Team' with 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess' policies, then add an IAM user called 'Network-L1-User1' to the group.

The name of the IAM group should be 'Network-L1-Team'.

(4 Marks)

The screenshot shows the AWS IAM console interface. The left sidebar contains the navigation menu with 'User groups' selected under 'Access management'. The main content area displays the 'User groups' page with a table listing existing groups. The table has columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. Two groups are listed: 'Network-L1-Team' and 's3-Admins'. The 'Network-L1-Team' group has 1 user and 'Defined' permissions, created 5 minutes ago. The 's3-Admins' group has 1 user and 'Defined' permissions, created 6 days ago. The top of the console shows the AWS logo and navigation tabs for various services like S3, EC2, and VPC.

Group name	Users	Permissions	Creation time
Network-L1-Team	1	Defined	5 minutes ago
s3-Admins	1	Defined	6 days ago

The name of the IAM user should be 'Network-L1-User1'.

(4 Marks)

Screenshot of the AWS IAM console showing the 'Network-L1-Team' user group details. The 'Users' tab is selected, showing one user: 'Network-L1-User1'. The 'Policies attached to this user group' section is visible at the top.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Network-L1-Team

Summary

User group name: Network-L1-Team

Creation time: May 03, 2023, 15:47 (UTC+05:30)

ARN: arn:aws:iam::324871465713:group/Network-L1-Team

Users | Permissions | Access Advisor

Users in this group (1)

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

Search

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	Network-L1-User1	1	None	2 minutes ago

https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

The 'AmazonVPCReadOnlyAccess' policy should be attached.

(4 Marks)

Screenshot of the AWS IAM console showing the 'Network-L1-Team' user group details. The 'Permissions' tab is selected, showing two policies attached: 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess'.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Network-L1-Team

Summary

User group name: Network-L1-Team

Creation time: May 03, 2023, 15:47 (UTC+05:30)

ARN: arn:aws:iam::324871465713:group/Network-L1-Team

Users | **Permissions** | Access Advisor

Permissions policies (2)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon .
<input type="checkbox"/>	AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon .

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

The 'AWSNetworkManagerReadOnlyAccess' policy should be attached.

(5 Marks)

The screenshot shows the AWS IAM console for the 'Network-L1-Team' user group. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Service control policies (SCPs). The main content area shows the 'Network-L1-Team' user group details, including its creation time (May 03, 2023, 15:47 UTC+05:30) and ARN. The 'Permissions' tab is active, showing two attached policies: 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess'. The 'AWSNetworkManagerReadOnlyAccess' policy is highlighted, indicating it is the one to be attached.

Policy name	Type	Description
AmazonVPCReadOnlyAccess	AWS managed	Provides read only access to Amazon .
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon .

The screenshot shows the AWS IAM console for the 'User groups' list. The left sidebar contains the 'Identity and Access Management (IAM)' menu. The main content area shows the 'User groups' list, which includes the 'Network-L1-Team' and 's3-Admins' groups. The 'Network-L1-Team' group is highlighted, showing it has 1 user and is 'Defined'.

Group name	Users	Permissions	Creation time
Network-L1-Team	1	Defined	5 minutes ago
s3-Admins	1	Defined	6 days ago

3.

Q3.

Create a S3 bucket for the following requirements

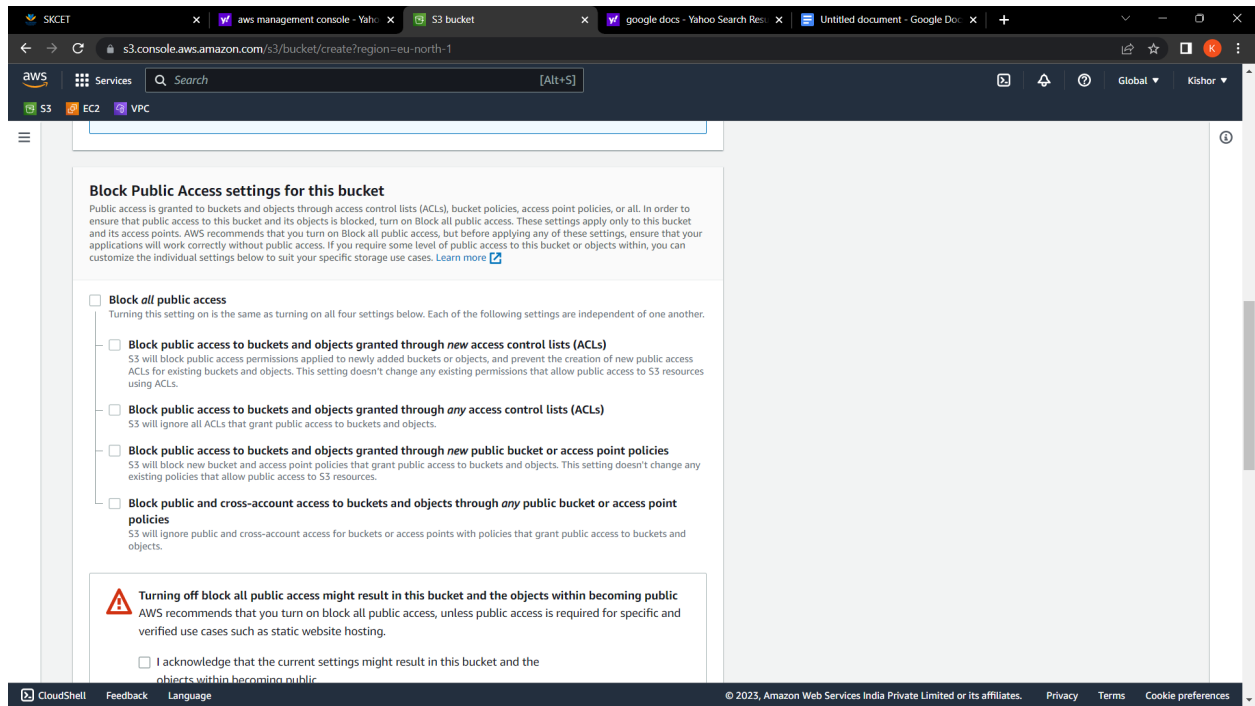
Create a new S3 bucket in the region of "Stockholm".

(4 Marks)

The screenshot shows the AWS Management Console interface for creating a new S3 bucket. The browser address bar indicates the URL is `s3.console.aws.amazon.com/s3/bucket/create?region=eu-north-1`. The console header shows the AWS logo and navigation tabs for S3, EC2, and VPC. The main content area is titled 'Create bucket' with an 'Info' link. Below the title, it states 'Buckets are containers for data stored in S3. [Learn more](#)'. The 'General configuration' section contains a 'Bucket name' input field with the value 'kenniel', a note that the name must be globally unique and cannot contain spaces or uppercase letters, and an 'AWS Region' dropdown menu set to 'EU (Stockholm) eu-north-1'. There is also an optional section to 'Copy settings from existing bucket' with a 'Choose bucket' button. The 'Object Ownership' section explains that it controls ownership and ACLs, with two options: 'ACLs disabled (recommended)' and 'ACLs enabled'. The 'ACLs enabled' option is selected, indicating that objects can be owned by other AWS accounts and accessed via ACLs. The footer of the console shows 'CloudShell', 'Feedback', 'Language', and copyright information for 2023.

Make the bucket accessible to everyone(publicly) via Bucket ACL.

(4 Marks)



Upload a text file in the name of 'accounts.txt'.

(5 Marks)

Browser tabs: SKCET, aws management console, S3 Management Console, google docs - Yahoo, Untitled document - , text about cloud computing, What is cloud computing.

URL: s3.console.aws.amazon.com/s3/upload/kennie?region=eu-north-1

Services: S3, EC2, VPC

Upload succeeded
View details below.

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination s3://kennie	Succeeded 1 file, 2.2 KB (100.00%)	Failed 0 files, 0 B (0%)
----------------------------	---------------------------------------	-----------------------------

Files and folders | Configuration

Files and folders (1 Total, 2.2 KB)

Find by name

Name	Folder	Type	Size	Status	Error
accounts.txt	-	text/plain	2.2 KB	Succeeded	-

CloudShell | Feedback | Language | © 2023, Amazon Web Services India Private Limited or its affiliates. | Privacy | Terms | Cookie preferences

Make the object 'accounts.txt' file accessible to everyone(publicly).
(4 Marks)

