

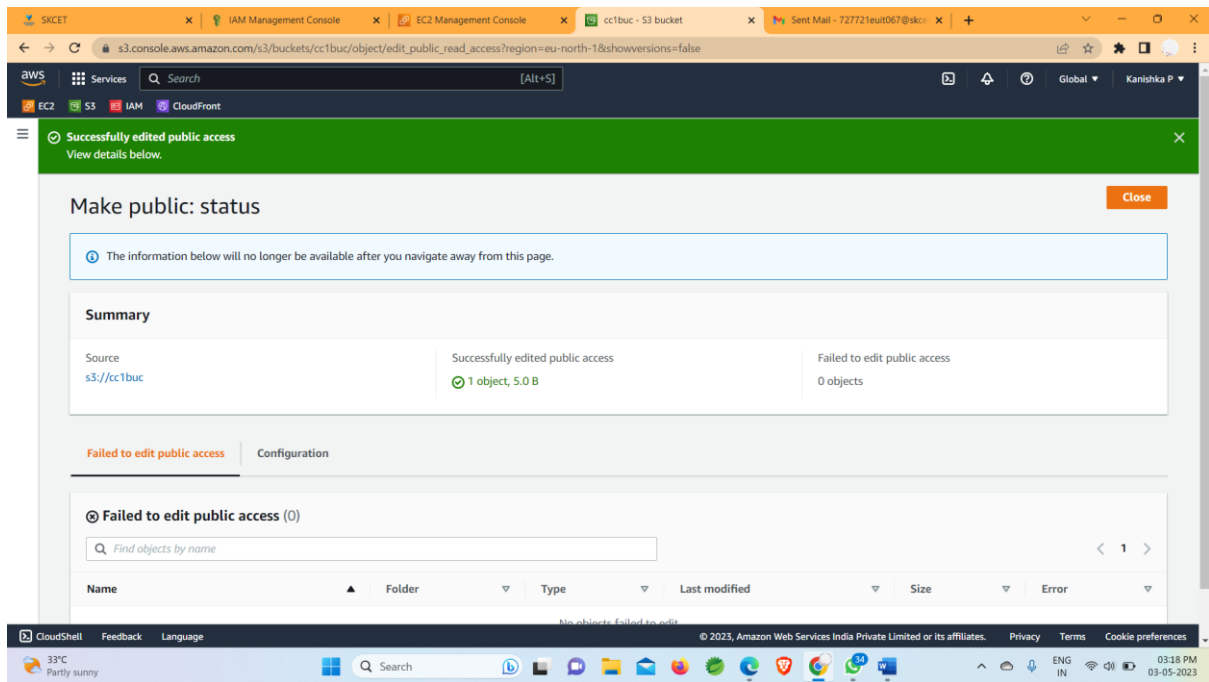
1)023\_SKCET\_Cloud\_CC1Time:30 minutesMarks: 17Q3. Create a S3 bucket for the following requirementsCreate a new S3 bucket in the region of "Stockholm".(4 Marks)Make the bucket accessible to everyone(publicly) via Bucket ACL.(4 Marks)Upload a text file in the name of 'accounts.txt'. (5Marks)Make the object 'accounts.txt' file accessible to everyone(publicly).(4 Marks)

Sol:

The first screenshot shows the 'Create bucket' page in the AWS Management Console. The 'Bucket name' is 'bucket\_cc' and the 'AWS Region' is 'EU (Stockholm) eu-north-1'. Under 'Object Ownership', 'ACLs enabled' is selected. A warning message states: 'We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.'

The second screenshot shows the 'cc1buc' bucket page. The 'Objects (1)' section displays a table with one object:

	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	accounts.txt	txt	May 3, 2023, 15:16:55 (UTC+05:30)	5.0 B	Standard



2)2023\_SKCET\_Cloud\_CC1Time:30 minutesMarks: 17Q2. 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 name of the IAM user should be 'Network-L1-User1'. (4 Marks) The 'AmazonVPCReadOnlyAccess' policy should be attached. (4 Marks) The 'AWSNetworkManagerReadOnlyAccess' policy should be attached. (5 Marks)

Sol:

The image displays two screenshots of the AWS IAM Management Console, showing the configuration of the 'Network-L1-Team' user group.

**Top Screenshot: Users in the group**

- Summary:** User group name: Network-L1-Team, Creation time: May 03, 2023, 15:36 (UTC+05:30), ARN: am:aws:iam::874646025163:group/Network-L1-Team.
- Users in this group (1):** A table showing one user, 'Network-L1-User1', with 1 group, no last activity, and created 7 minutes ago.

**Bottom Screenshot: Permissions policies**

- Summary:** Same as the top screenshot.
- Permissions policies (2):** A table showing two policies attached to the group: 'AmazonVPCReadOnlyAccess' and 'AWSNetworkManagerReadOnlyAccess', both AWS managed.

3)2023\_SKCET\_Cloud\_CC1Time:30 minutesMarks: 16Q1. 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 puttyremote connection.(4 Marks)Allow HTTP traffic from the internet for reaching website requests.(4 Marks)

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:v=3,\$case=tags:true%5Cclient:false,\$regex=tags:false%5Cclient:false

EC2 S3 IAM CloudFront

New EC2 Experience

EC2 Dashboard  
EC2 Global View  
Events  
Limits

Instances

Instances

Instance Types  
Launch Templates  
Spot Requests  
Savings Plans  
Reserved Instances  
Dedicated Hosts  
Scheduled Instances  
Capacity Reservations

Images

AMIs  
AMI Catalog

Elastic Block Store

CloudShell Feedback Language

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

33°C Partly sunny

Find instance by attribute or tag (case-sensitive)

Connect Instance state Actions Launch instances

	Name	Instance ID	Instance state	Instance type	Availability Zone	Key name	Launch time
<input type="checkbox"/>	ser	i-08e7574ed67b1eecc	Terminated	t2.micro	us-east-1d	ke	2023/05/02 19:40 GMT+5:30
<input type="checkbox"/>	ec2usecase1	i-025ab7ee573bc212b	Running	t2.micro	us-east-1c	ec2usecase1	2023/05/03 15:27 GMT+5:30
<input type="checkbox"/>	ec2usecase1	i-0255844445fac9df6	Terminated	t2.micro	us-east-1c	ec2usecase1	2023/05/03 15:39 GMT+5:30

Select an instance

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

EC2 S3 IAM CloudFront

Subnet info

No preference (Default subnet in any availability zone)

Auto-assign public IP info

Enable

Firewall (security groups) info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-3' with the following rules:

☒ Allow SSH traffic from Anywhere (0.0.0.0/0)

☒ Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Configure storage info Advanced

Summary

Number of instances info 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.0.2...read more ami-02396cdd13e9a1257

Virtual server type (instance type) t2.micro

Firewall (security group) New security group

Storage (volumes) 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the

Cancel Launch instance Review commands

CloudShell Feedback Language

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

33°C Partly sunny