

2023_SKCET_Cloud_CC1

Time: 30 minutes

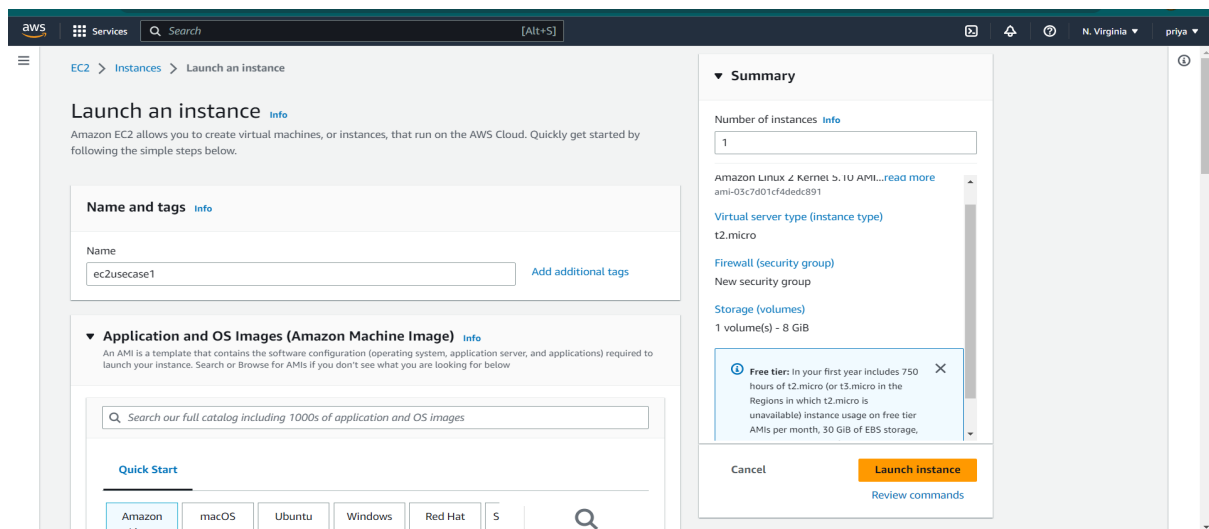
Marks: 16

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)



aws

Services

Search

[Alt+S]

N. Virginia

pritya

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows pricing: 0.0162 USD per Hour

On-Demand SUSE pricing: 0.0116 USD per Hour

On-Demand RHEL pricing: 0.0716 USD per Hour

On-Demand Linux pricing: 0.0116 USD per Hour

Free tier eligible

All generations

Compare instance types

Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

ec2usecase1

Create new key pair

Network settings

Edit

Network

vpc-07e299f67c3956678

Subnet

No preference (Default subnet in any availability zone)

Auto-assign public IP

Enable

Summary

Number of instances

1

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-03c7d01cf4dedc891

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 Standard or subitile t3 instances.)

Cancel

Launch instance

Review commands

aws

Services

Search

[Alt+S]

N. Virginia

pritya

New EC2 Experience

Tell us what you think

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

Instances (1)

Info

Find instance by attribute or tag (case-sensitive)

ec2usecase1

i-096c61d450c3d384e

Running

t2.micro

2/2 checks passed

No alarms

us-east-1c

ec2-18-232-180-

Select an instance

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

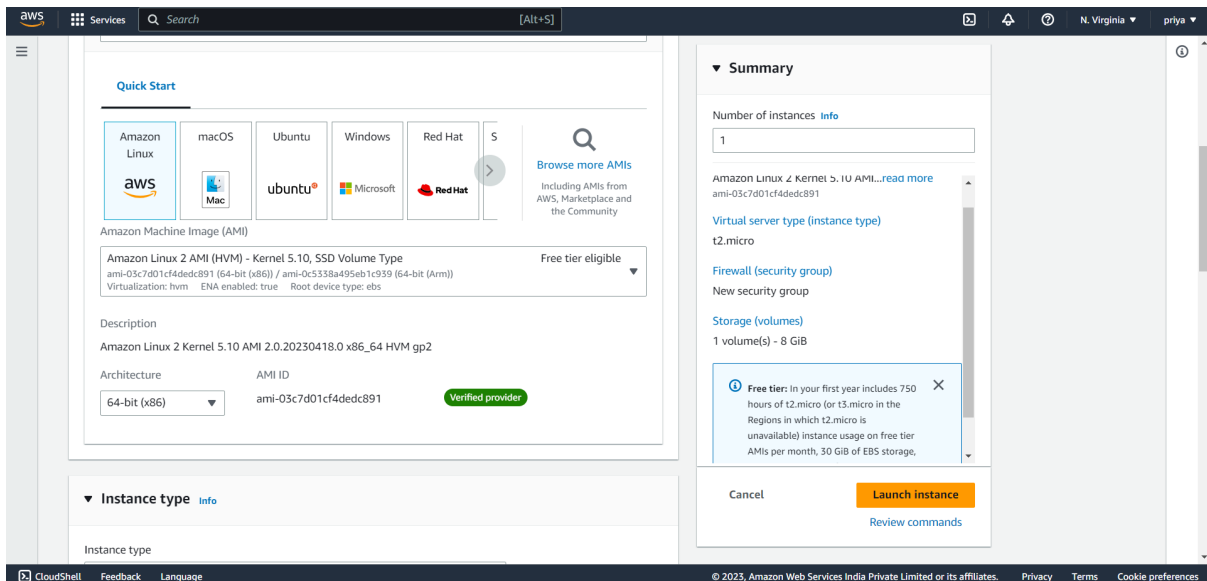
Privacy

Terms

Cookie preferences

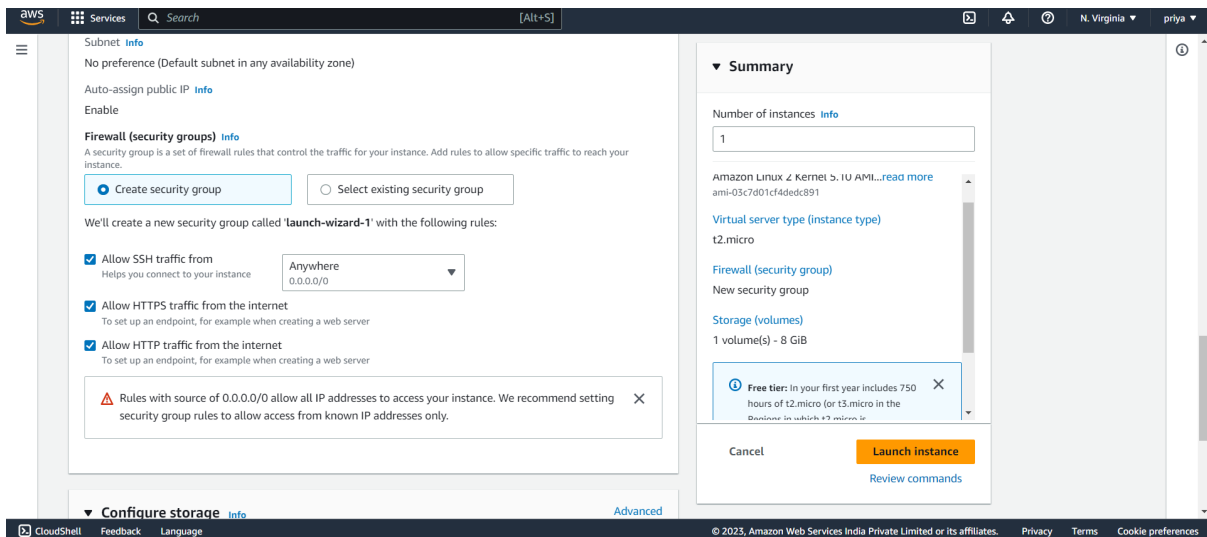
EC2 instance AMI should be "Amazon Linux 2".

(4 Marks)



(4 Marks)

Allow SSH traffic for taking putty remote connection.



Allow HTTP traffic from the internet for reaching website requests.

(4 Marks)

aws

Services

Search

[Alt+S]

N. Virginia

priya

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-1' with the following rules:

Allow SSH traffic from

Helps you connect to your instance

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

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-03c7d01cf4dedc891

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 Standard tier) which is 99 minutes for

Cancel

Launch instance

Review commands

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

2023_SKCET_Cloud_CC1

Time: 30 minutes

Marks: 17

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 displays the AWS IAM console interface. The left-hand navigation pane is open, showing the 'Identity and Access Management (IAM)' section. Under 'Access management', the 'User groups' link is selected. The main content area shows the configuration for the 'Network-L1-Team' group. The 'Summary' tab is active, displaying the group's details: 'User group name' is 'Network-L1-Team', 'Creation time' is 'April 26, 2023, 10:21 (UTC+05:30)', and 'ARN' is 'arn:aws:iam::833781727798:group/Network-L1-Team'. Below the summary, the 'Users' tab is selected, showing a list of users in the group. There is one user, 'Network-L1-User', with a 'Last activity' of 'None' and a 'Creation time' of '1 minute ago'. The console header shows the AWS logo, 'Services' menu, a search bar, and the user's profile 'priya'.

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: April 26, 2023, 10:21 (UTC+05:30)

ARN: arn:aws:iam::833781727798: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-User	1	None	1 minute ago

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

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

(4 Marks)

The screenshot shows the AWS IAM Management Console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, and Access reports. The main content area displays the details for a user named 'Network-L1-User'. The 'Summary' section shows the user's ARN, console access status, and access keys. The 'Permissions policies' section shows a list of policies attached to the user, including 'AmazonVPCFullAccess'.

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-User [Delete]

Summary

ARN arn:aws:iam::833781727798:user/Network-L1-User	Console access Disabled	Access key 1 Not enabled
Created May 03, 2023, 15:44 (UTC+05:30)	Last console sign-in -	Access key 2 Not enabled

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

Find policies

Policy name	Type	Attached via
AmazonVPCFullAccess	AWS managed	Group Network-L1-Team

The 'AmazonVPCReadOnlyAccess' policy should be attached.
(4 Marks)

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links for Identity and Access Management (IAM), Access management, Access reports, and Credential report. The main content area displays the 'Network-L1-Team' user group details, including its name, creation time, and ARN. The 'Permissions' tab is active, showing a list of attached policies. Only the 'AmazonVPCFullAccess' policy is currently attached.

Policy name	Type	Description
AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC vi

The 'AWSNetworkManagerReadOnlyAccess' policy should be attached.
(5 Marks)

This screenshot shows the same AWS IAM console interface as the previous one, but with an additional policy attached to the 'Network-L1-Team' user group. The 'Permissions' tab now shows two policies: 'AmazonVPCFullAccess' and 'AWSNetworkManagerReadOnlyAccess'.

Policy name	Type	Description
AmazonVPCFullAccess	AWS managed	Provides full access to Amazon VPC vi
AWSNetworkManagerReadOnlyAccess	AWS managed	Provides read only access to Amazon .

aws

Services

Search

[Alt+S]

Global

priya

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

Analzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > User groups > Network-L1-Team

Network-L1-Team

Delete

Edit

Summary

User group name

Creation time

ARN

Network-L1-Team

April 26, 2023, 10:21 (UTC+05:30)

arn:aws:iam::833781727798:group/Network-L1-Team

Users

Permissions

Access Advisor

Permissions policies (2)

info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

< 1 >

Policy name

Type

Description

AmazonVPCReadOnlyAccess

AWS managed

Provides read only access to Amazon ...

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

2023_SKCET_Cloud_CC1

Time: 30 minutes

Marks: 17

Q3.

Create a S3 bucket for the following requirements

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

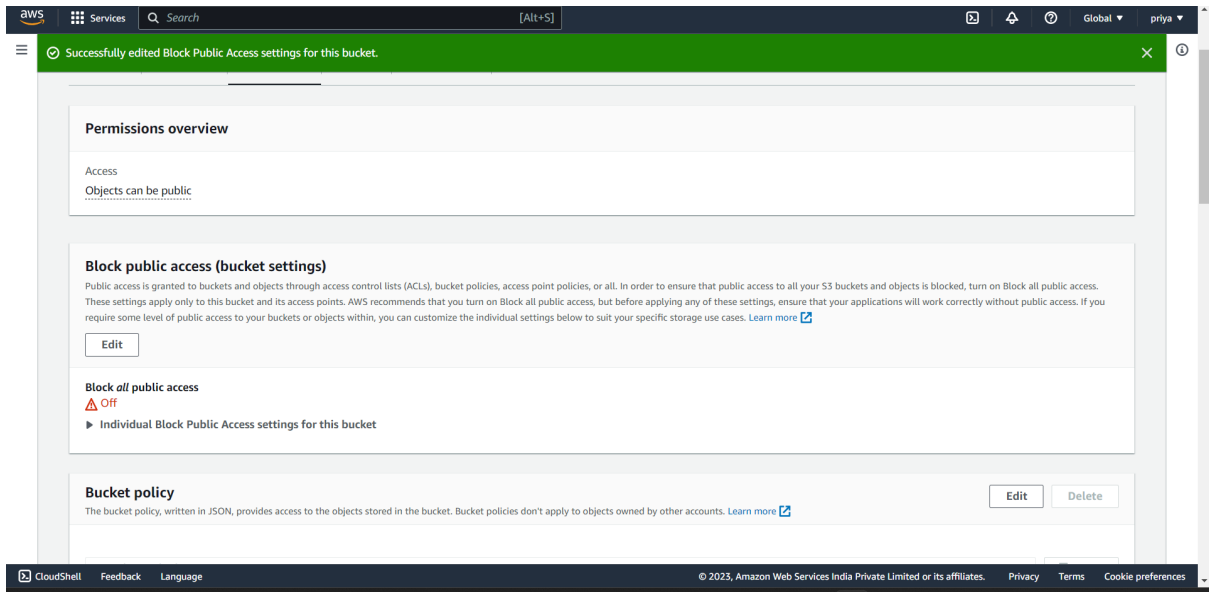
(4 Marks)

The screenshot shows the AWS S3 console interface. A green notification banner at the top states "Successfully created bucket 'cc116'" with a "View details" button. The left sidebar contains navigation links for Buckets, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens, Dashboards, AWS Organizations settings, Feature spotlight, and AWS Marketplace for S3. The main content area displays the "Buckets (3)" list. A table lists the buckets with columns for Name, AWS Region, Access, and Creation date.

Name	AWS Region	Access	Creation date
cc116	EU (Stockholm) eu-north-1	Objects can be public	May 3, 2023, 16:02:20 (UTC+05:30)
linuximg	Asia Pacific (Mumbai) ap-south-1	Public	April 25, 2023, 14:38:51 (UTC+05:30)
virtualbucket116	Asia Pacific (Mumbai) ap-south-1	Public	April 28, 2023, 10:00:58 (UTC+05:30)

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

(4 Marks)



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

(5 Marks)

aws

Services

Search

[Alt+S]

Global

priya

Upload succeeded

View details below.

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

Summary

Destination

s3://cc116

Succeeded

1 file, 2.0 B (100.00%)

Failed

0 files, 0 B (0%)

Files and folders

Configuration

Files and folders (1 Total, 2.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
accounts.txt	-	text/plain	2.0 B	Succeeded	-

CloudShell

Feedback

Language

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

32°C

Partly sunny

Search

16:04

03-05-2023

aws

Services

Search

[Alt+S]

Global

priya

Successfully edited bucket policy.

Amazon S3

Buckets

cc116

cc116

Info

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Permissions overview

Access

Public

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

Off

cc116 - S3 bucket

cc116 - S3 bucket

Untitled document - Google Do...

+

s3.console.aws.amazon.com/s3/buckets/cc116?region=eu-north-1&tab=objects

aws

Services

Search

[Alt+S]

Global

priva

Amazon S3 > Buckets > cc116

cc116

Info

Publicly accessible

Objects

Properties

Permissions

Metrics

Management

Access Points

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 Inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Refresh

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

Show versions

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	accounts.txt	txt	May 3, 2023, 16:04:11 (UTC+05:30)	2.0 B	Standard

https://s3.console.aws.amazon.com/s3/#

© 2023, Amazon Web Services India Private Limited or its affiliates.

Privacy

Terms

Cookie preferences

31°C

Partly sunny

Search

16:07

03-05-2023