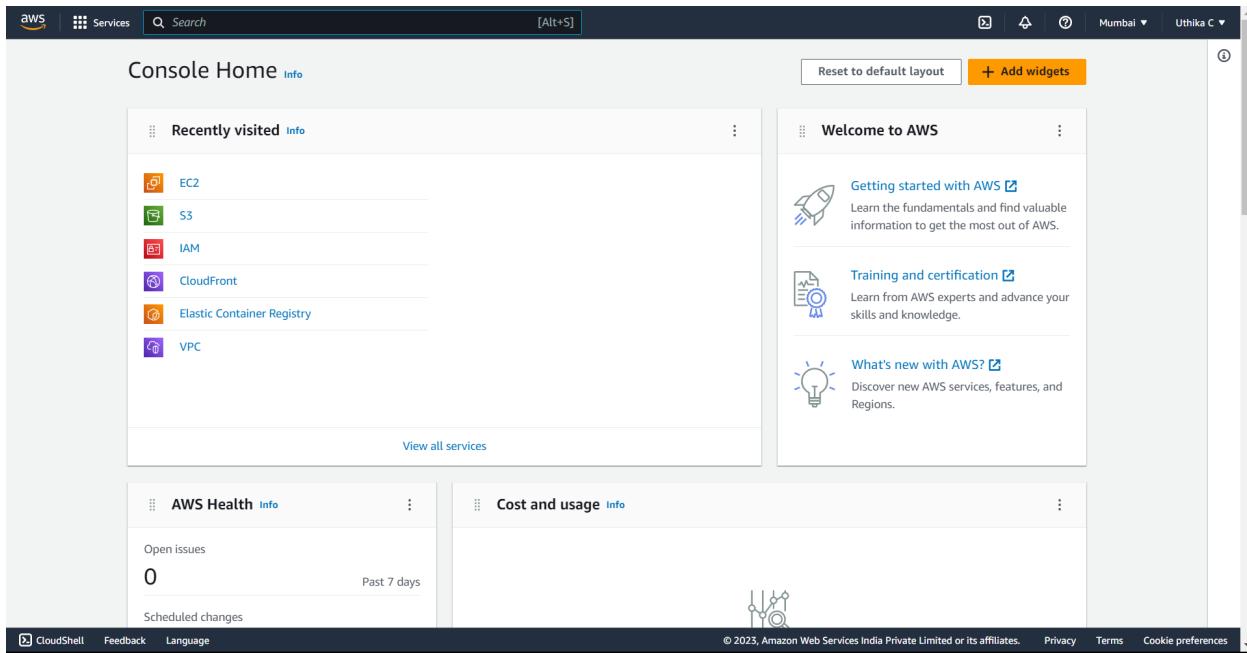


CLOUD COMPUTING

DAY 1

AWS Account Creation

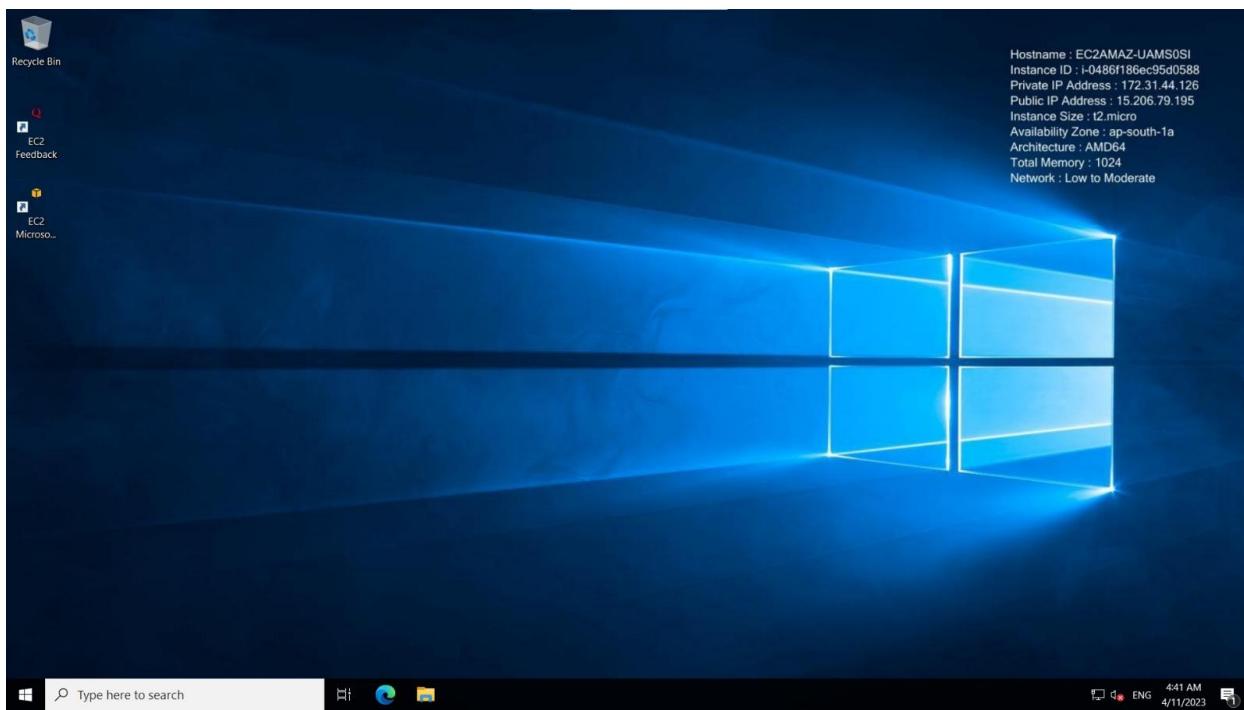


DAY 2

Question 1

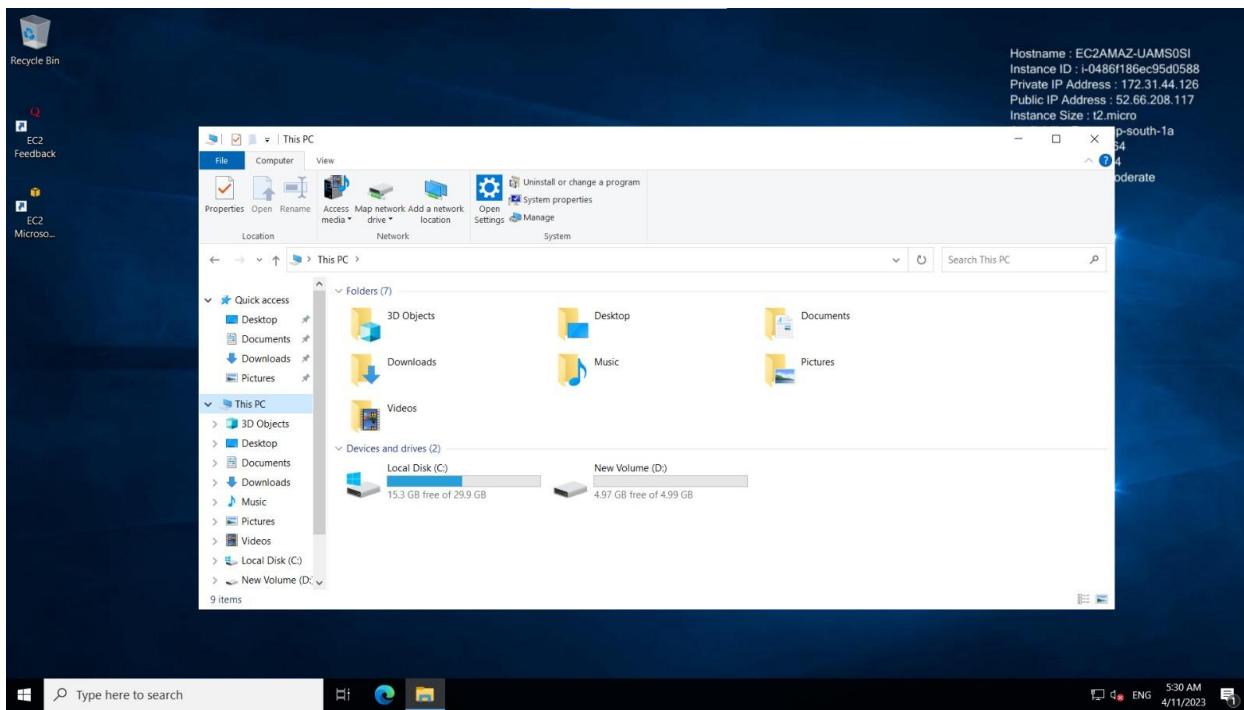
Create a Windows EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.

NAME:UTHIKA C
REG NO:727721EUCS173



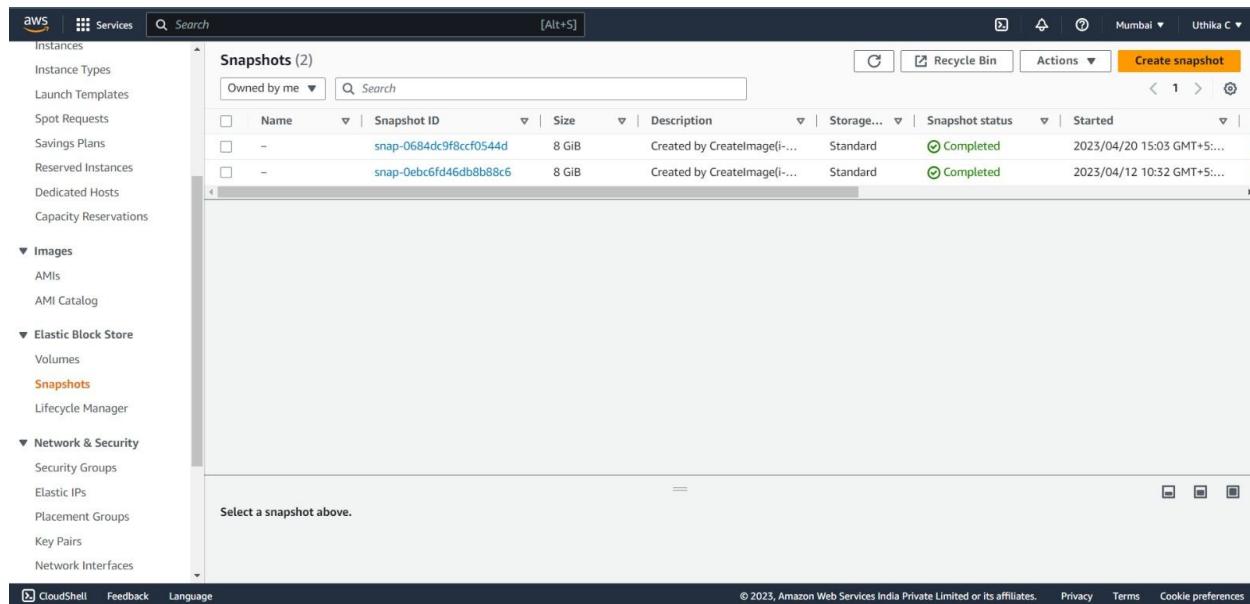
Question 2

Create an EBS volume of 5 GB and attach to a windows EC2 instance and make partition of that EBS volume.



Question 3

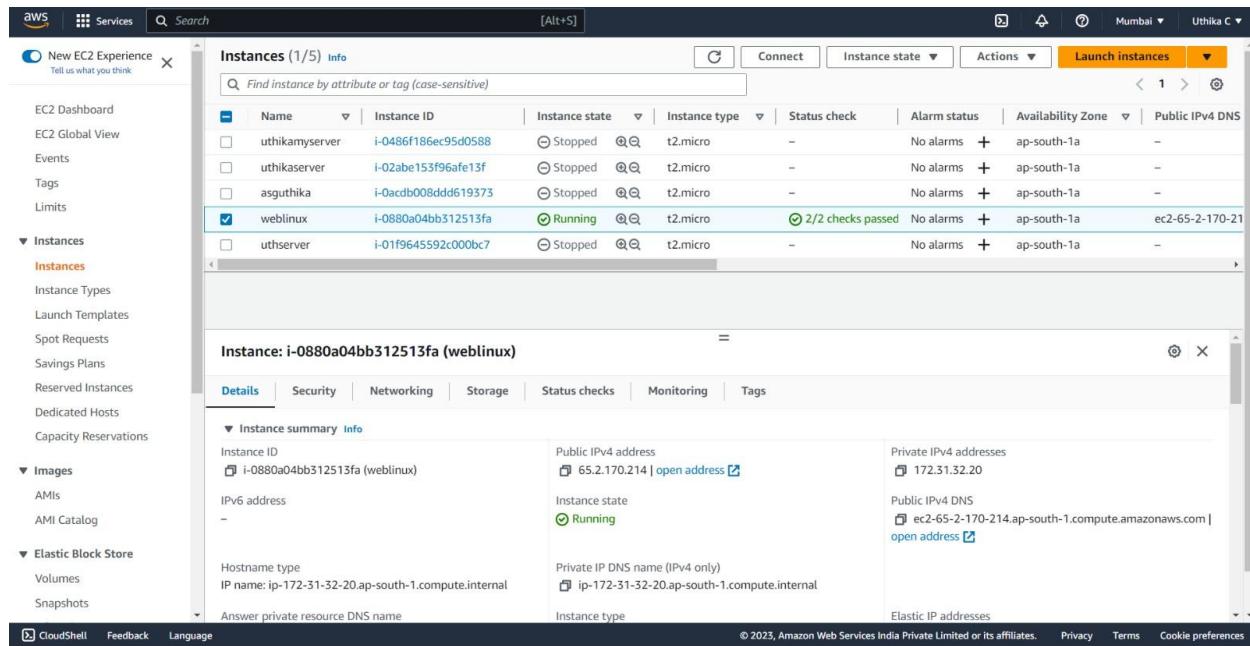
Create some files and folders into 5 GB EBS volume of the previous exercise and take a snapshot of that EBS volume.



The screenshot shows the AWS Management Console with the EBS service selected. The left sidebar lists various services like Instances, Images, and Network & Security. The main pane displays a table of snapshots, each with a checkbox, Name, Snapshot ID, Size, Description, Storage type, Snapshot status, and Start time. Two snapshots are listed under 'Owned by me': 'snap-0684dc9f8ccf0544d' (8 GiB, Standard, Completed, 2023/04/20 15:03 GMT+5...) and 'snap-0ebc6fd46db8b88c6' (8 GiB, Standard, Completed, 2023/04/12 10:32 GMT+5...). Below the table, a message says 'Select a snapshot above.' with three small icons.

Question 4

Create a Linux EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.

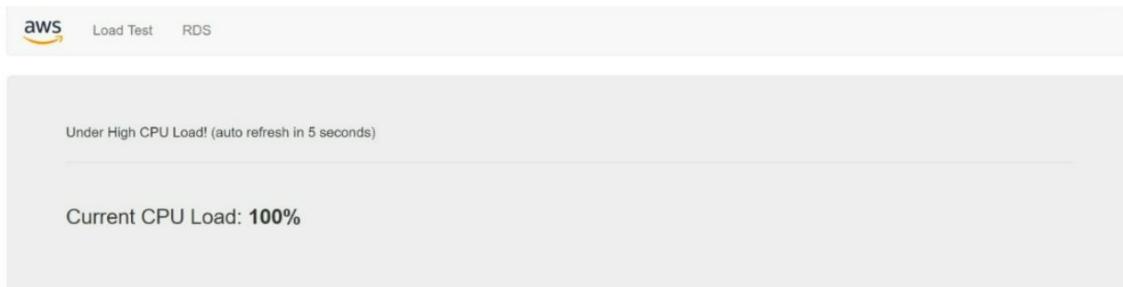


The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar lists various services like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main pane shows a table of instances with columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. One instance, 'weblinux' (Instance ID i-0880a04bb312513fa), is highlighted and shown in more detail below the table. The 'Details' tab is selected, displaying information such as Instance ID (i-0880a04bb312513fa (weblinux)), Public IPv4 address (65.2.170.214), Private IP4 address (172.31.32.20), Public IPv4 DNS (ec2-65-2-170-214.ap-south-1.compute.amazonaws.com), and Private IP DNS name (ip-172-31-32-20.ap-south-1.compute.internal). Other tabs include Security, Networking, Storage, Status checks, Monitoring, and Tags.

It works!

Question 5

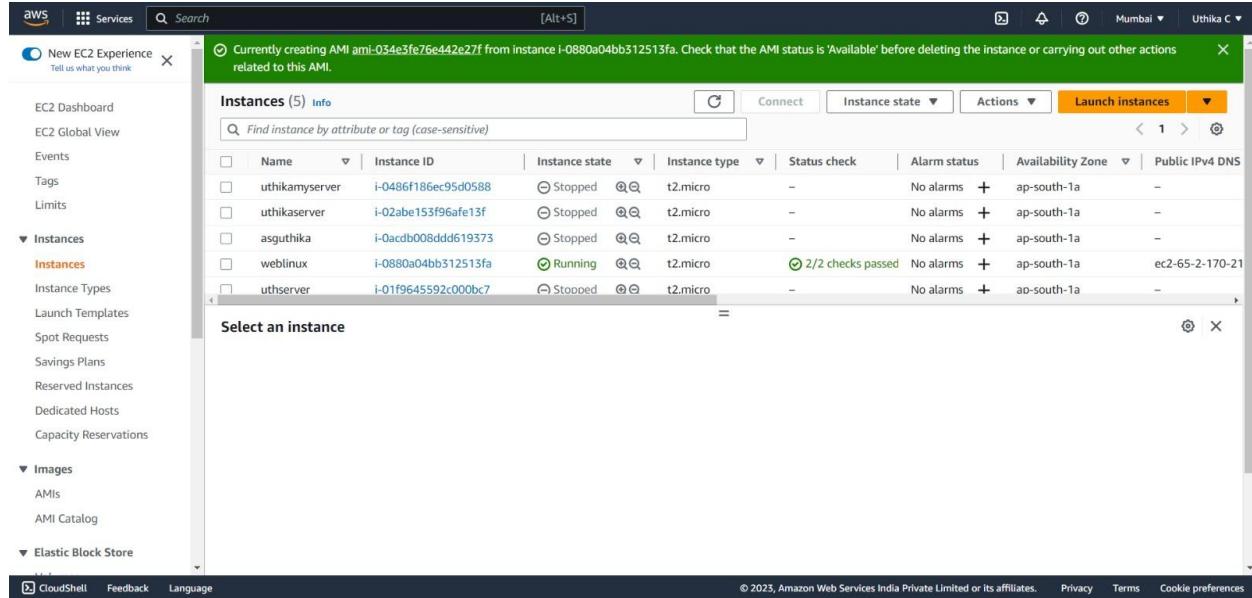
Install, Start and Enable the httpd webservice in that Linux EC2 Instance, then host a static website in EC2.



Question 6

Create Image(MyAMI) of the linux Webserver(from the previous exercise) and launch new EC2 instance from the created Image(MyAMI)

NAME:UTHIKA C
REG NO:727721EUCS173

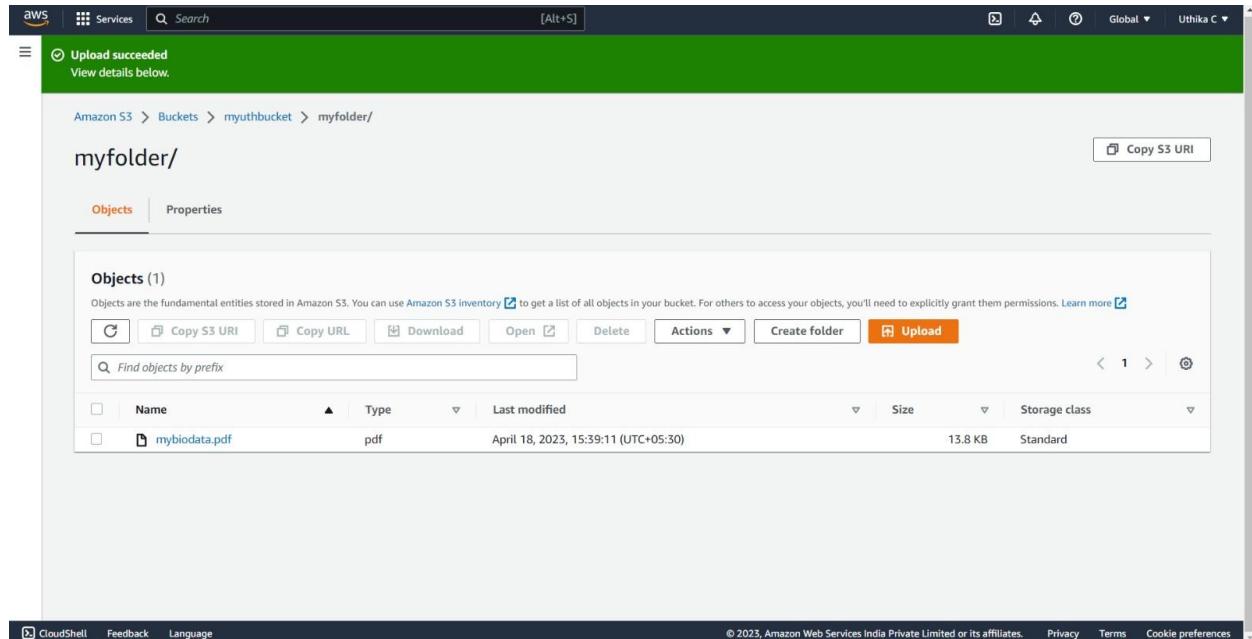


The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with links like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store. The main content area displays a table of instances with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. The instances listed are: uthikamyserv (i-0486f186ec95d0588, Stopped, t2.micro, -), uthikaserver (i-02abe153f96afe13f, Stopped, t2.micro, -), asguthika (i-0acdb008dd619373, Stopped, t2.micro, -), weblinux (i-0880a04bb312513fa, Running, t2.micro, 2/2 checks passed, No alarms, ap-south-1a, ec2-65-2-170-21), and uthserver (i-01f9645592c000bc7, Stopped, t2.micro, -). A green banner at the top indicates "Currently creating AMI ami-034e3fe76e442e27f from instance i-0880a04bb312513fa. Check that the AMI status is 'Available' before deleting the instance or carrying out other actions related to this AMI."

DAY 3

Question 1

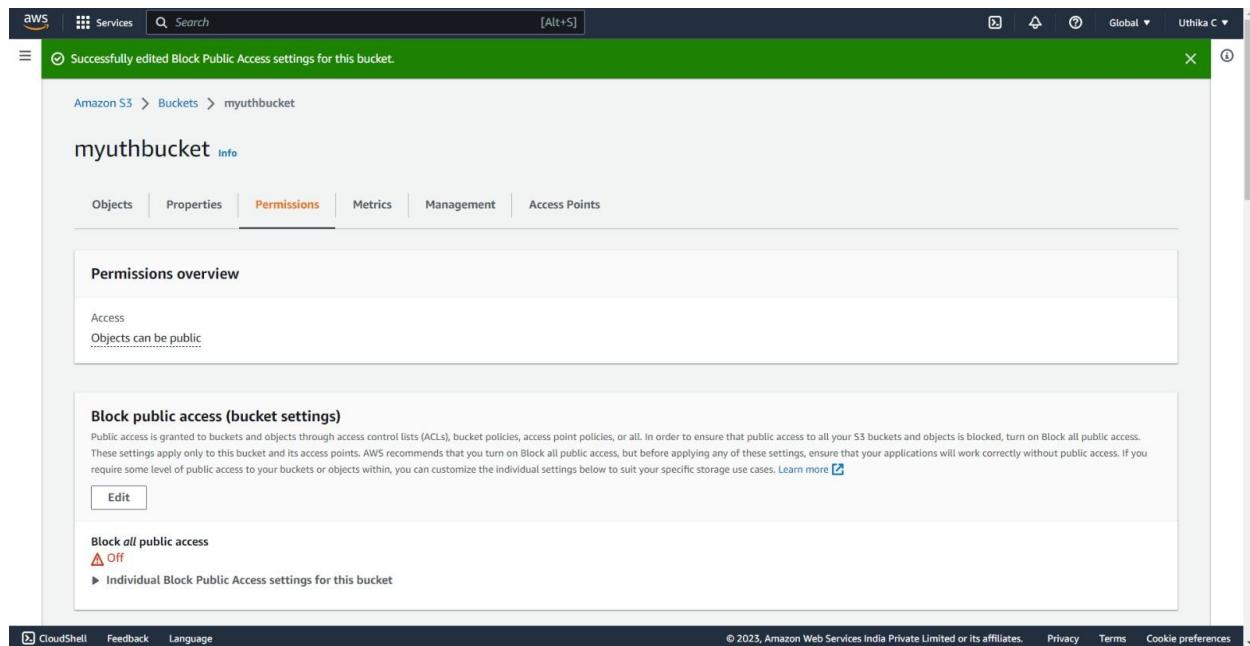
Create a S3 Bucket and create a folder in the bucket and upload a file in the folder.



The screenshot shows the AWS S3 Objects page. The URL is Amazon S3 > Buckets > myuthbucket > myfolder/. A green banner at the top says "Upload succeeded". The main content area shows a table of objects with columns: Name, Type, Last modified, Size, and Storage class. There is one object listed: mybiodata.pdf (pdf, April 18, 2023, 15:39:11 (UTC+05:30), 13.8 KB, Standard). A "Copy S3 URI" button is visible on the right. The top navigation bar includes CloudShell, Feedback, Language, and links for Global, Mumbai, and Uthika C.

Question 2

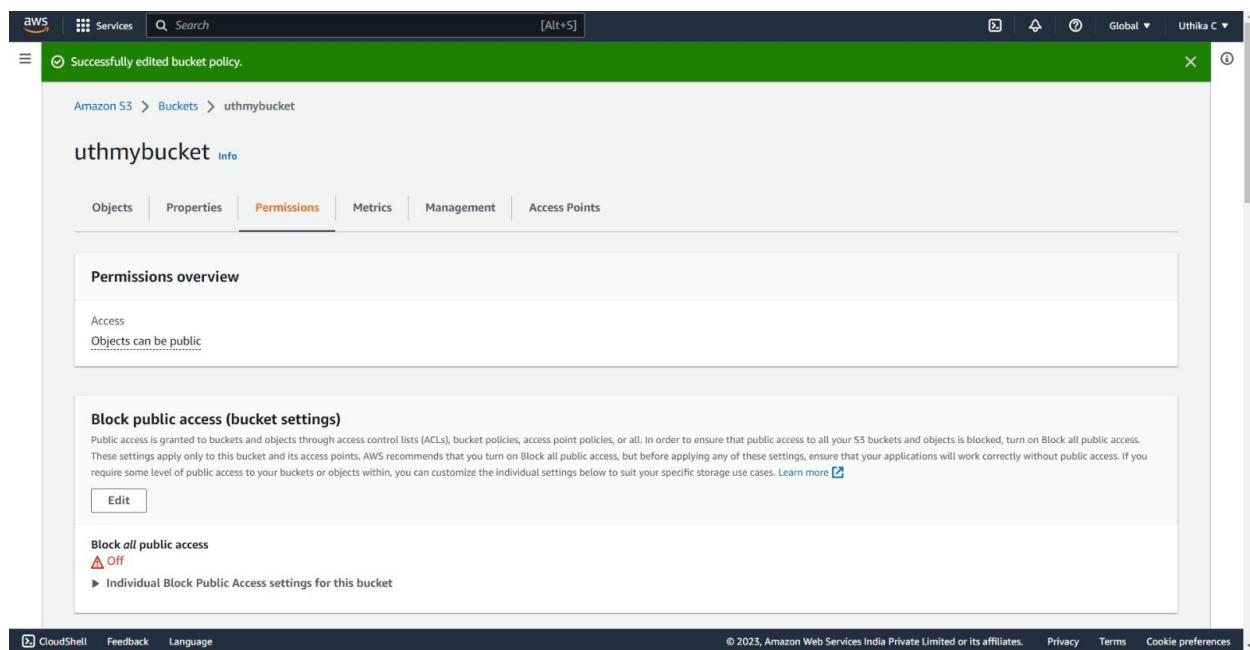
Disable "Block Public Access" for the bucket and enable public read access for a file.



The screenshot shows the AWS S3 Bucket Permissions settings page for the bucket 'myuthbucket'. At the top, a green success message says 'Successfully edited Block Public Access settings for this bucket.' Below the message, the breadcrumb navigation shows 'Amazon S3 > Buckets > myuthbucket'. The main title is 'myuthbucket' with an 'Info' link. The navigation bar includes 'Objects', 'Properties', 'Permissions' (which is highlighted in red), 'Metrics', 'Management', and 'Access Points'. The 'Permissions overview' section shows 'Access' and 'Objects can be public'. The 'Block public access (bucket settings)' section contains a note about public access being granted through various methods like ACLs, bucket policies, and access point policies. It has an 'Edit' button and a status indicator showing 'Off'. A link 'Block all public access' leads to 'Individual Block Public Access settings for this bucket'. At the bottom, there are links for CloudShell, Feedback, Language, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

Question 3

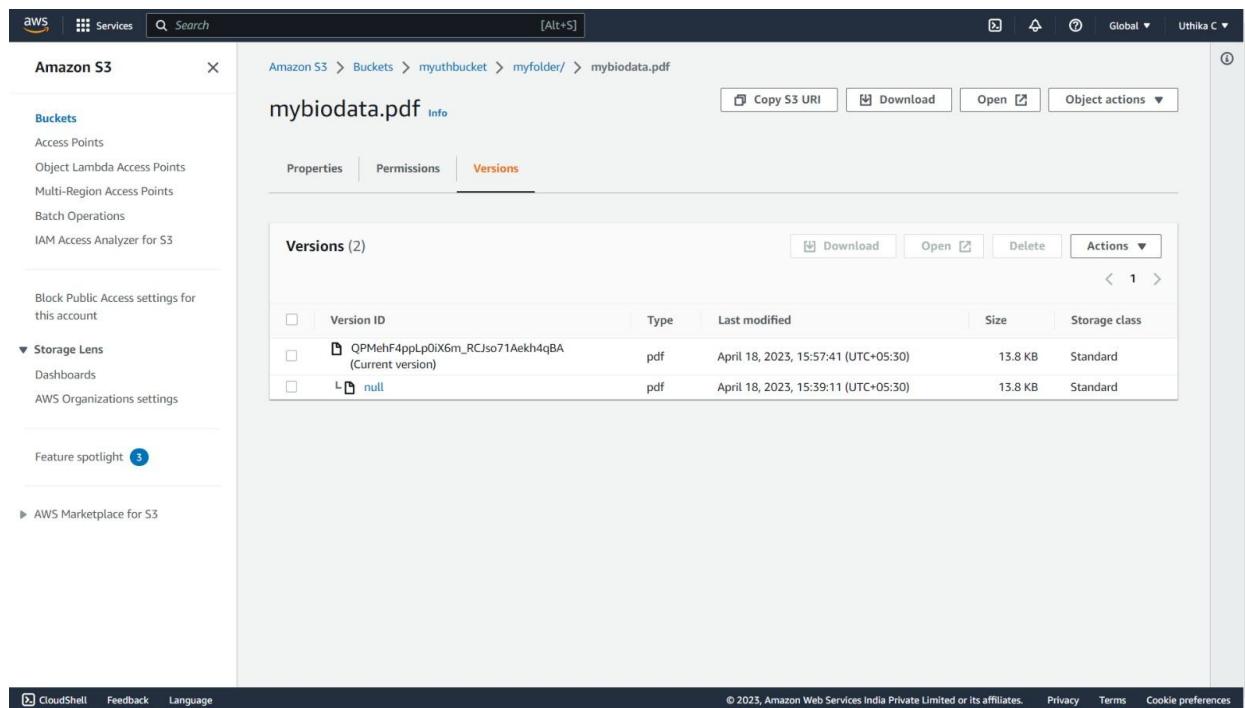
Create a bucket policy which should deny to read objects under a folder of a bucket.



The screenshot shows the AWS S3 Bucket Permissions settings page for the bucket 'uthmybucket'. At the top, a green success message says 'Successfully edited bucket policy.'. Below the message, the breadcrumb navigation shows 'Amazon S3 > Buckets > uthmybucket'. The main title is 'uthmybucket' with an 'Info' link. The navigation bar includes 'Objects', 'Properties', 'Permissions' (which is highlighted in red), 'Metrics', 'Management', and 'Access Points'. The 'Permissions overview' section shows 'Access' and 'Objects can be public'. The 'Block public access (bucket settings)' section contains a note about public access being granted through various methods like ACLs, bucket policies, and access point policies. It has an 'Edit' button and a status indicator showing 'Off'. A link 'Block all public access' leads to 'Individual Block Public Access settings for this bucket'. At the bottom, there are links for CloudShell, Feedback, Language, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

Question 4

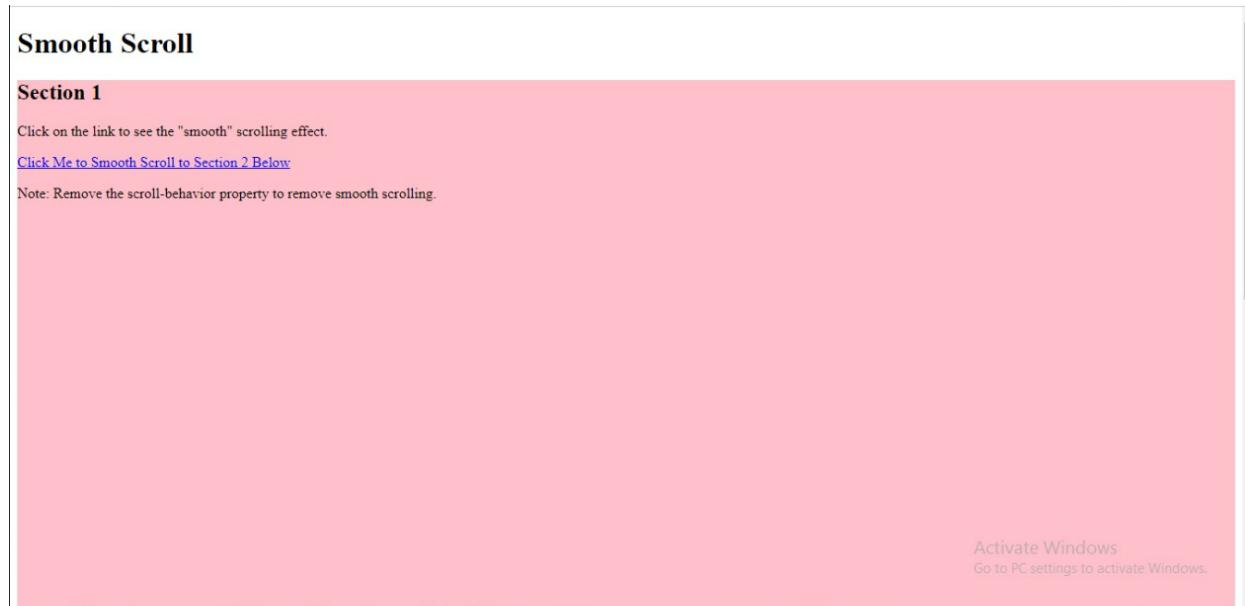
Enable versioning objects for a bucket and upload objects with multiple versions of it.



The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with options like 'Buckets', 'Storage Lens', and 'Feature spotlight'. The main area shows the path 'Amazon S3 > Buckets > myuthbucket > myfolder/ > mybiodata.pdf'. Below this, there are tabs for 'Properties', 'Permissions', and 'Versions'. The 'Versions' tab is active, showing a table with two rows. The columns are 'Version ID', 'Type', 'Last modified', 'Size', and 'Storage class'. The first row is the 'Current version' with Version ID 'QPMehF4ppLp0IX6m_RCJso71Aekh4qBA', Type 'pdf', Last modified 'April 18, 2023, 15:57:41 (UTC+05:30)', Size '13.8 KB', and Storage class 'Standard'. The second row is labeled 'null'.

Question 5

Host a static webpage in a bucket itself by using static website hosting feature of it.

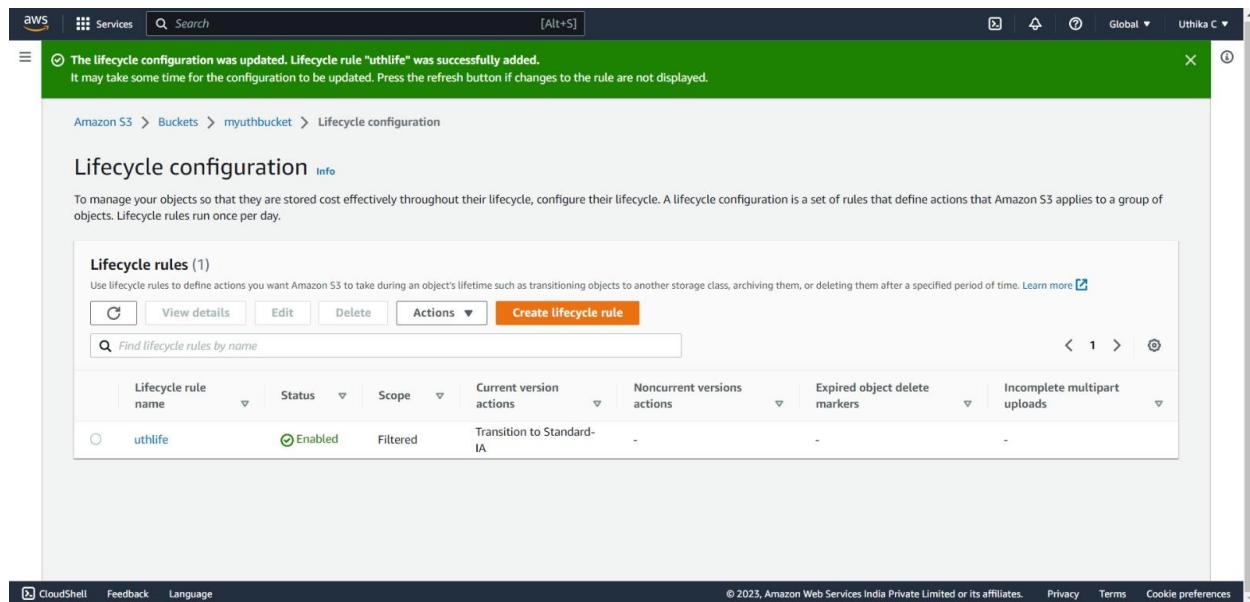


The screenshot shows a static webpage with a pink background. At the top, it says 'Smooth Scroll'. Below that is a section titled 'Section 1' with the text 'Click on the link to see the "smooth" scrolling effect.' followed by a link 'Click Me to Smooth Scroll to Section 2 Below'. Underneath is a note 'Note: Remove the scroll-behavior property to remove smooth scrolling.' In the bottom right corner, there's a watermark that says 'Activate Windows Go to PC settings to activate Windows.'

Question 6

Enable a lifecycle management rule between various storage classes for a S3 bucket.

NAME:UTHIKA C
REG NO:727721EUCS173

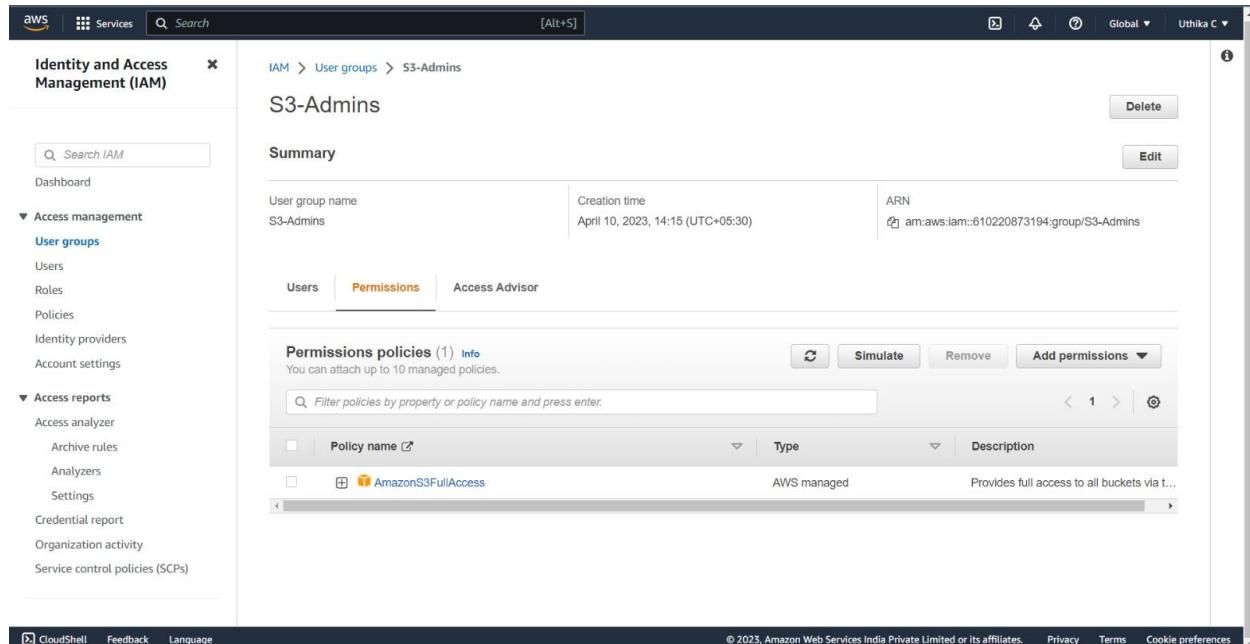


The screenshot shows the AWS S3 Lifecycle configuration page for a bucket named 'myuthbucket'. A green header bar at the top indicates that a lifecycle rule named 'uthlife' was successfully added. Below this, the page displays the 'Lifecycle configuration' section with a table titled 'Lifecycle rules (1)'. The table has columns for Lifecycle rule name, Status, Scope, Current version actions, Noncurrent versions actions, Expired object delete markers, and Incomplete multipart uploads. One rule is listed: 'uthlife' (Enabled, Filtered, Transition to Standard-IA). At the bottom of the page, there are links for CloudShell, Feedback, Language, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

DAY 4

Question 1

Create an IAM group called as 'S3-Admins' with 'AmazonS3FullAccess'.



The screenshot shows the AWS IAM User groups page. On the left, a sidebar menu includes 'Identity and Access Management (IAM)', 'Access management' (with 'User groups' selected), 'Access reports', and other options like 'Archive analyzer', 'Analyzers', and 'Settings'. The main content area shows a group named 'S3-Admins' with a summary table. The 'Permissions' tab is selected, showing one policy attached: 'AmazonS3FullAccess' (AWS managed, provides full access to all buckets via t...). At the bottom, there are links for CloudShell, Feedback, Language, and a footer with copyright information and links for Privacy, Terms, and Cookie preferences.

Question 2

Create an IAM user called as 'S3Admin1' and add it to the 'S3-Admins' group.

S3-Admins

Summary

User group name	Creation time	ARN
S3-Admins	April 10, 2023, 14:15 (UTC+05:30)	arn:aws:iam::610220873194:group/S3-Admins

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.

User name	Groups	Last activity	Creation time
S3Admins1	1	None	1 minute ago

Question 3

Attach an IAM custom policy to the 'S3-Admins' group which should deny to delete objects.

The policy uths3 has been created.

Policies (1068) Info
A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
uths3	Customer managed	None	
AWSHealthFullAccess	AWS managed	None	Allows full access to AWS Health services
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only access to Amazon Glacier
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability to access AWS Marketplace
ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable Client VPN
AWSSSOAdministrator	AWS managed	None	Administrator access to AWS SSO
AWSIoTClickReadOnlyAccess	AWS managed	None	Provides read only access to AWS IoT Click
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only access to Auto Scaling console
AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to Amazon DMS Redshift S3 role
AWSQuickSightListIAM	AWS managed	None	Allow QuickSight to list IAM users
AWSHealthFullAccess	AWS managed	None	Allows full access to AWS Health services

S3-Admins

Summary

User group name: S3-Admins | Creation time: April 10, 2023, 14:15 (UTC+05:30) | ARN: arn:aws:iam::610220873194:group/S3-Admins

Permissions

Permissions policies (2)

Policy name	Type	Description
uths3	Customer managed	
AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...

Question 4

Create an Inline policy for an IAM user and set some permission boundary for that user.

S3Admins1

Summary

ARN: arn:aws:iam::\$10220873194:user/S3Admins1 | Console access: Enabled without MFA | Last console sign-in: Never | Access key 1: Not enabled | Access key 2: Not enabled

Permissions

Permissions policies (4)

Policy name	Type	Attached via
AmazonS3FullAccess	AWS managed	Group S3-Admins
IAMUserChangePassword	AWS managed	Directly
inlinepolicy	Customer inline	Inline
uths3	Customer managed	Group S3-Admins

Permissions boundary (not set)

Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

Question 5

Create an IAM role with 'AmazonS3FullAccess' and attach the role to an EC2 instance.

NAME:UTHIKA C
REG NO:727721EUCS173

The screenshot shows the AWS IAM service interface. In the top left, the 'Identity and Access Management (IAM)' logo is visible. On the left sidebar, under 'Access management', the 'Roles' option is selected. A green notification bar at the top right says 'Role S3AccessRole created.' Below it, the 'Roles (5) Info' section is shown, with a table listing five roles: AWSServiceRoleForAutoScaling, AWSServiceRoleForElasticLoadBalancing, AWSServiceRoleForSupport, AWSServiceRoleForTrustedAdvisor, and S3AccessRole. The S3AccessRole row indicates it is associated with the 'AWS Service: ec2'. At the bottom of the page, there is a 'Roles Anywhere' section.

Question 6

Activate MFA for an IAM user and Set some Password Policies such as 1 uppercase, 1 lowercase etc

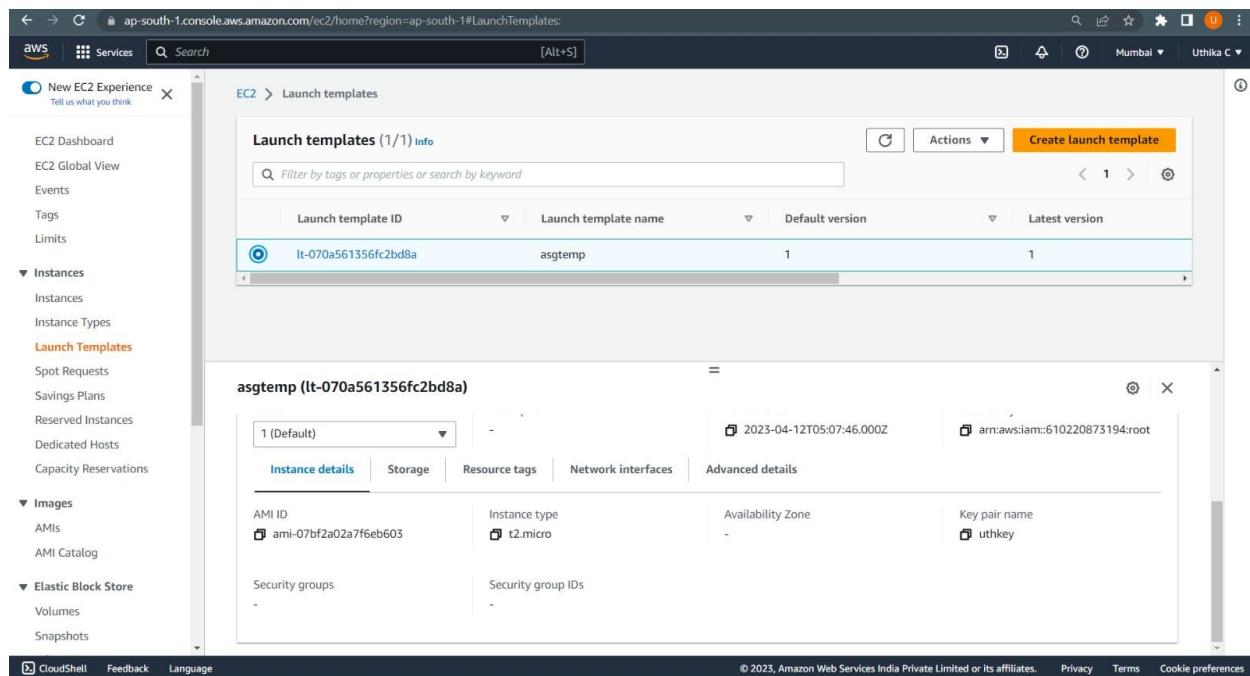
The screenshot shows the AWS IAM service interface. The left sidebar shows the 'Users' option is selected under 'Access management'. A green notification bar at the top right says 'MFA device assigned'. Below it, the 'S3Admins1' user profile is displayed. The 'Summary' section shows ARN (arn:aws:iam::610220873194:user/S3Admins1), Console access (Enabled with MFA), and Access key 1 (Not enabled). The 'Security credentials' tab is selected. The 'Console sign-in' section shows a console sign-in link (<https://610220873194.signin.aws.amazon.com/console>) and a console password (Updated 53 minutes ago (2023-04-20 11:42 GMT+5:30)).

DAY 5

Question 1

Create a launch template with a custom AMI and t2.micro instance type

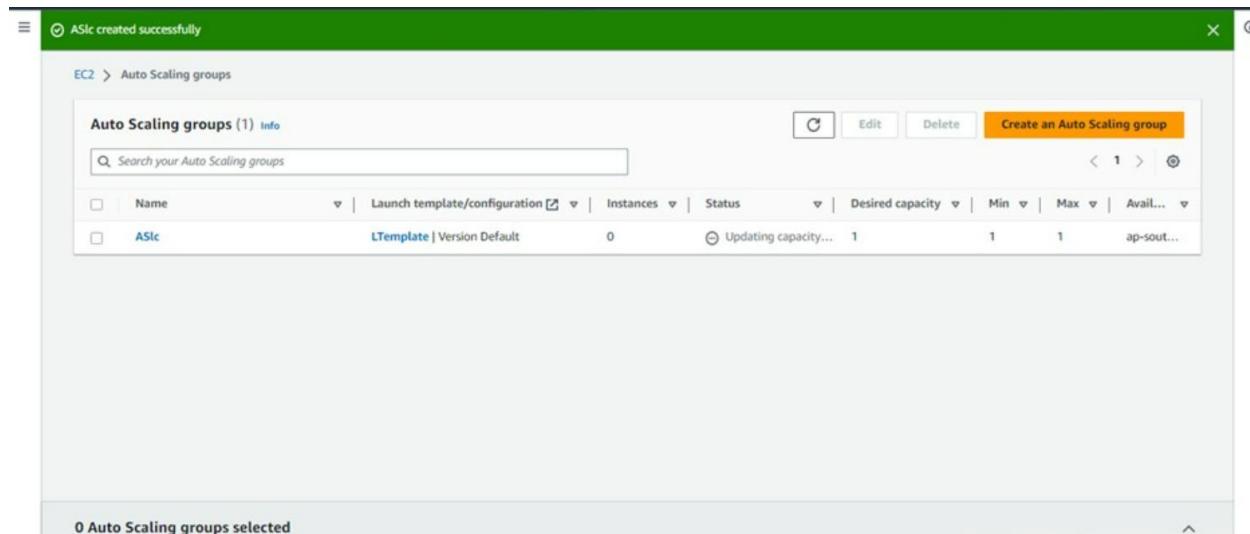
NAME:UTHIKA C
REG NO:727721EUCS173



The screenshot shows the AWS EC2 Launch Templates page. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances, Launch Templates (which is selected), Images, and Elastic Block Store. The main content area displays a table titled "Launch templates (1/1) info". The table has columns for Launch template ID, Launch template name, Default version, and Latest version. A single row is shown: "lt-070a561356fc2bd8a" with "asgtemp" as the name, both default and latest versions are 1. Below this, a detailed view for "asgtemp" is expanded, showing fields for Instance details (AMI ID: ami-07bf2a02a7f6eb603, Instance type: t2.micro, Availability Zone: -), Storage, Resource tags, Network interfaces, and Advanced details. At the bottom of the page, there are links for CloudShell, Feedback, Language, and footer information.

Question 2

Create an autoscaling group with the above-created launch template



The screenshot shows the AWS Auto Scaling groups page. The top bar indicates "ASlc created successfully". The main content area displays a table titled "Auto Scaling groups (1) info". The table has columns for Name, Launch template/configuration, Instances, Status, Desired capacity, Min, Max, and Available. One row is listed: "ASlc" with "LTemplate | Version Default" as the launch template, 0 instances, and a status of "Updating capacity...". At the bottom, it says "0 Auto Scaling groups selected".

DAY 6

1)Create a VPC with multiple subnets(at least 1 subnet in each zone)

The screenshot shows the 'Create VPC workflow' success page in the AWS VPC console. It lists 25 successful steps in a bulleted list, including creating the VPC, endpoint, subnets, internet gateway, route tables, and route table associations. A 'View VPC' button is at the bottom.

Create VPC workflow

Success

Details

- ✓ Create VPC: vpc-04c553d53ffffc5cfe
- ✓ Disable DNS hostnames
- ✓ Disable DNS resolution
- ✓ Verifying VPC creation: vpc-04c553d53ffffc5cfe
- ✓ Create S3 endpoint: vpcce-06e75e1ddd53339d5
- ✓ Create subnet: subnet-00e896cce5058403e5
- ✓ Create subnet: subnet-081c17c41e32c2ff
- ✓ Create subnet: subnet-0572e49373e9b6c656
- ✓ Create subnet: subnet-03e542e332239a4fd
- ✓ Create internet gateway: igw-0495e2613d03d1ea3
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0e0ff357c72859f5c
- ✓ Create route table
- ✓ Associate route table
- ✓ Associate route table
- ✓ Create route table: rtb-0f7d1b77d9ee159d7
- ✓ Associate route table
- ✓ Create route table: rtb-0dd0f3e90d01ae75
- ✓ Associate route table
- ✓ Verifying route table creation
- ✓ Associate S3 endpoint with private subnet route tables: vpcce-06e75e1ddd53339d5

View VPC

2) Make 1 public subnet and 2 private subnets in the created VPC

The screenshot shows the 'Subnets (1/7)' list and a detailed view of a specific subnet. The list shows 7 subnets, including one public and six private subnets. The detailed view for the subnet 'private' shows its configuration: Subnet ID: subnet-0f2808854e26c47fb, Subnet ARN: arn:aws:ec2:us-east-2:610220873194:subnet/subnet-0f2808854e26c47fb, State: Available, IPv4 CIDR: 172.31.32.0/20, Availability Zone: us-east-2c, and Availability Zone ID: use2-az3.

Subnets (1/7)

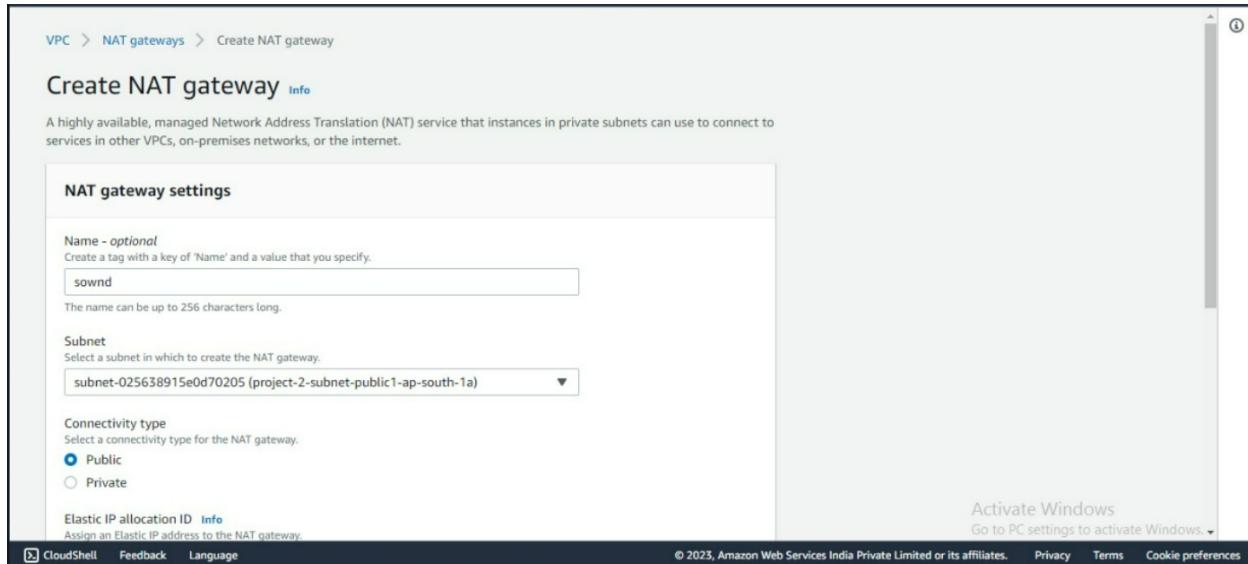
Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
projectcl-subnet-pu...	subnet-0e5951d28cd6445	Available	vpc-0c7572b3302257eb2 pr...	10.0.16.0/20	-
public	subnet-0be4bb0f2950480b0	Available	vpc-0e5298c75e184c354	172.31.16.0/20	-
projectcl-subnet-pr...	subnet-082fae2fde6d80d14	Available	vpc-0c7572b3302257eb2 pr...	10.0.128.0/20	-
projectcl-subnet-pr...	subnet-0b9db3a6e164cb169	Available	vpc-0c7572b3302257eb2 pr...	10.0.144.0/20	-
private	subnet-0eaaeb919de081b	Available	vpc-0e5298c75e184c354	172.31.0.0/20	-
projectcl-subnet-pu...	subnet-0c547fc7ceb51030	Available	vpc-0c7572b3302257eb2 pr...	10.0.0/20	-
private	subnet-0f2808854e26c47fb	Available	vpc-0e5298c75e184c354	172.31.32.0/20	-

subnet-0f2808854e26c47fb / private

Details

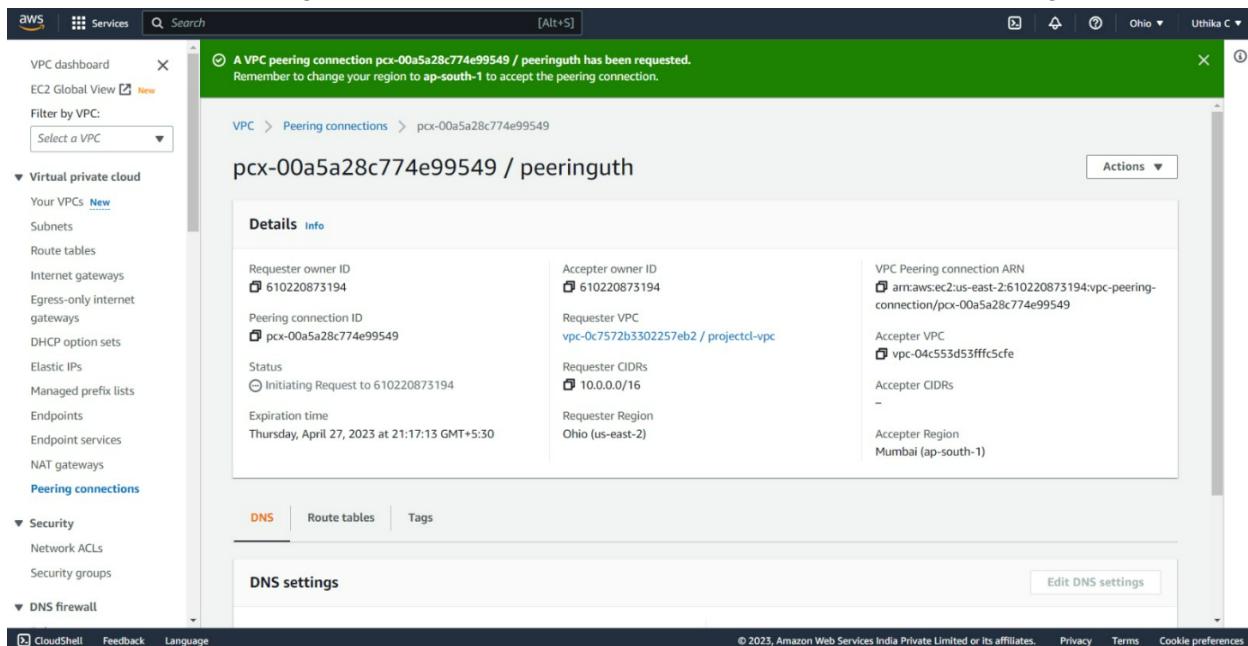
Subnet ID subnet-0f2808854e26c47fb	Subnet ARN arn:aws:ec2:us-east-2:610220873194:subnet/subnet-0f2808854e26c47fb	State Available	IPv4 CIDR 172.31.32.0/20
Available IPv4 addresses 4091		Availability Zone us-east-2c	Availability Zone ID use2-az3

3) Make internet connection using NAT gateway for the 2 private subnets.



The screenshot shows the 'Create NAT gateway' page in the AWS VPC service. The 'NAT gateway settings' section is visible, including fields for 'Name - optional' (containing 'sound'), 'Subnet' (selected as 'subnet-025638915e0d70205 (project-2-subnet-public1-ap-south-1a)'), 'Connectivity type' (set to 'Public'), and 'Elastic IP allocation ID' (info). A status bar at the bottom right indicates 'Activate Windows'.

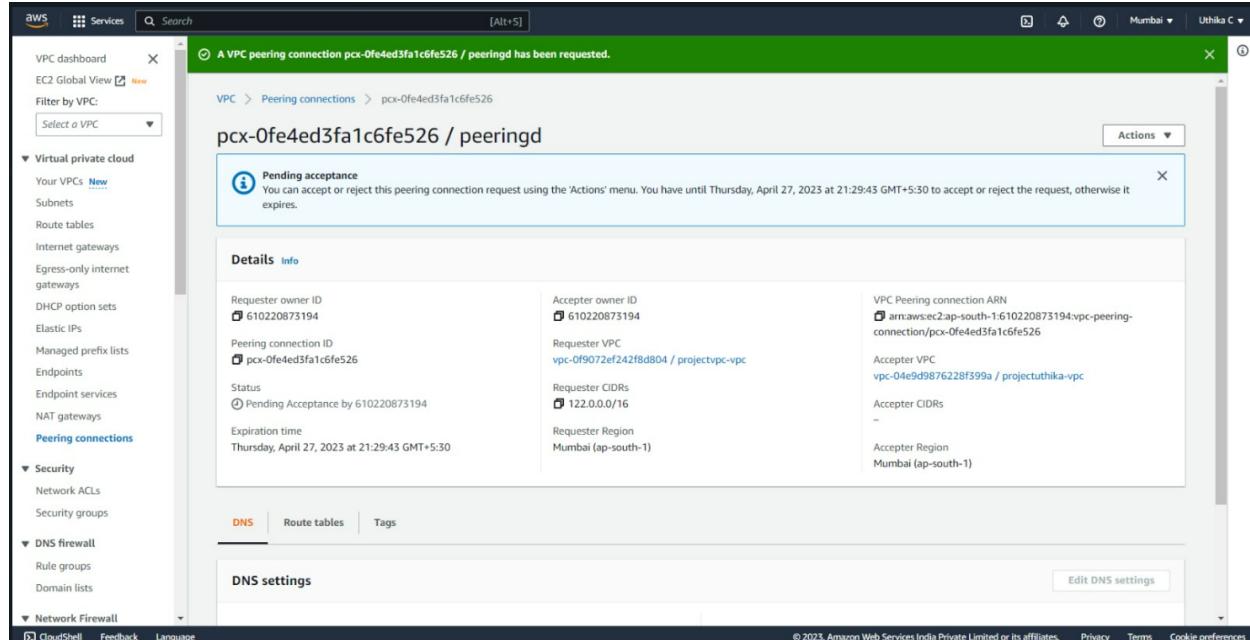
4)Create a VPC peering connection between 2 different VPCs from 2 different regions.



The screenshot shows the 'Peering connections' page in the AWS VPC service. A green banner at the top states 'A VPC peering connection pcv-00a5a28c774e99549 / peerenguth has been requested. Remember to change your region to ap-south-1 to accept the peering connection.' The main table lists the peering connection details, including Requester owner ID (610220873194), Acceptor owner ID (610220873194), Peering connection ID (pcx-00a5a28c774e99549), Requester VPC (vpc-0c7572b3302257eb2 / projectl-vpc), Requester CIDR (10.0.0.0/16), Requester Region (Ohio (us-east-2)), Acceptor VPC (vpc-04c553d53fffc5cf), Acceptor CIDR (10.0.0.0/16), and Acceptor Region (Mumbai (ap-south-1)).

5)Create VPC peering connections for 3 different VPCs from the same region

NAME:UTHIKA C
REG NO:727721EUCS173

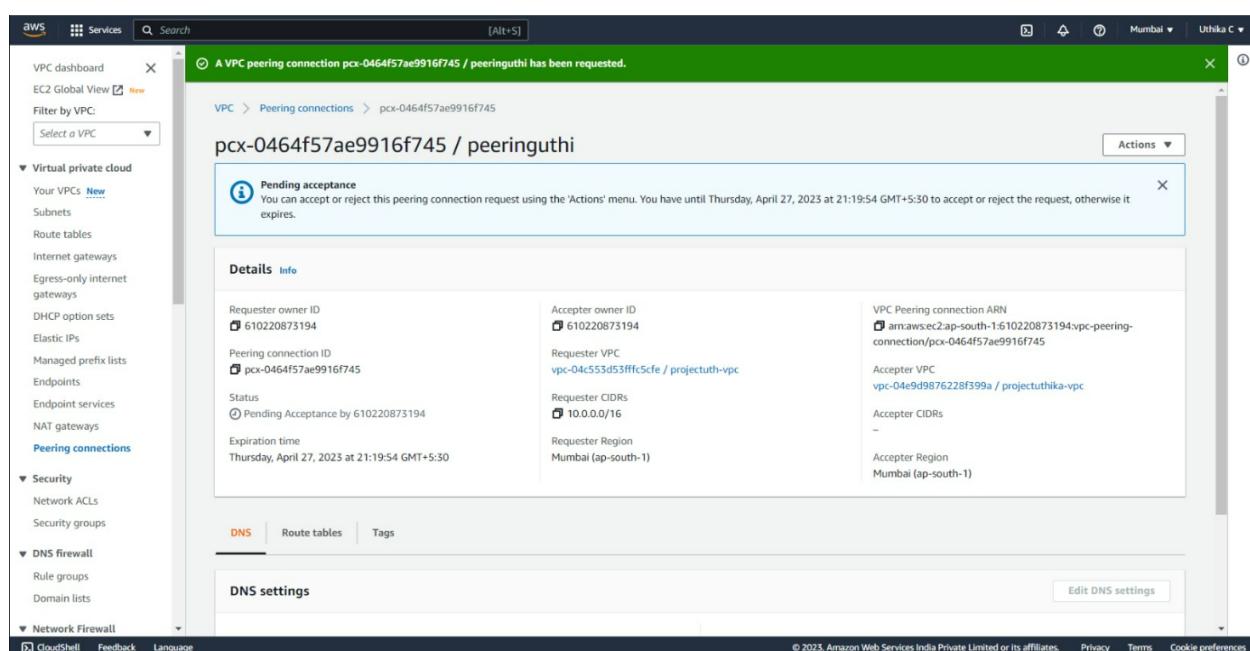


A screenshot of the AWS VPC Peering Connections page showing a pending acceptance request. The peering connection ID is pcv-0fe4ed3fa1c6fe526. The requester is Uthika C (arn:aws:ec2:ap-south-1:610220873194:vpc-peering-connection/pcv-0fe4ed3fa1c6fe526) and the accepter is vpc-04e9d9876228f399a (projectuthika-vpc). Both are located in Mumbai (ap-south-1). The status is Pending Acceptance by 610220873194. The expiration time is Thursday, April 27, 2023 at 21:29:43 GMT+5:30.

Details

Requester owner ID	Acceptor owner ID	VPC Peering connection ARN
610220873194	610220873194	arn:aws:ec2:ap-south-1:610220873194:vpc-peering-connection/pcv-0fe4ed3fa1c6fe526
Peering connection ID	Requester VPC	Acceptor VPC
pcv-0fe4ed3fa1c6fe526	vpc-0f9072ef242f8d804 / projectvpc-vpc	vpc-04e9d9876228f399a / projectuthika-vpc
Status	Requester CIDRs	Acceptor CIDRs
Pending Acceptance by 610220873194	122.0.0.0/16	-
Expiration time	Requester Region	Acceptor Region
Thursday, April 27, 2023 at 21:29:43 GMT+5:30	Mumbai (ap-south-1)	Mumbai (ap-south-1)

DNS settings

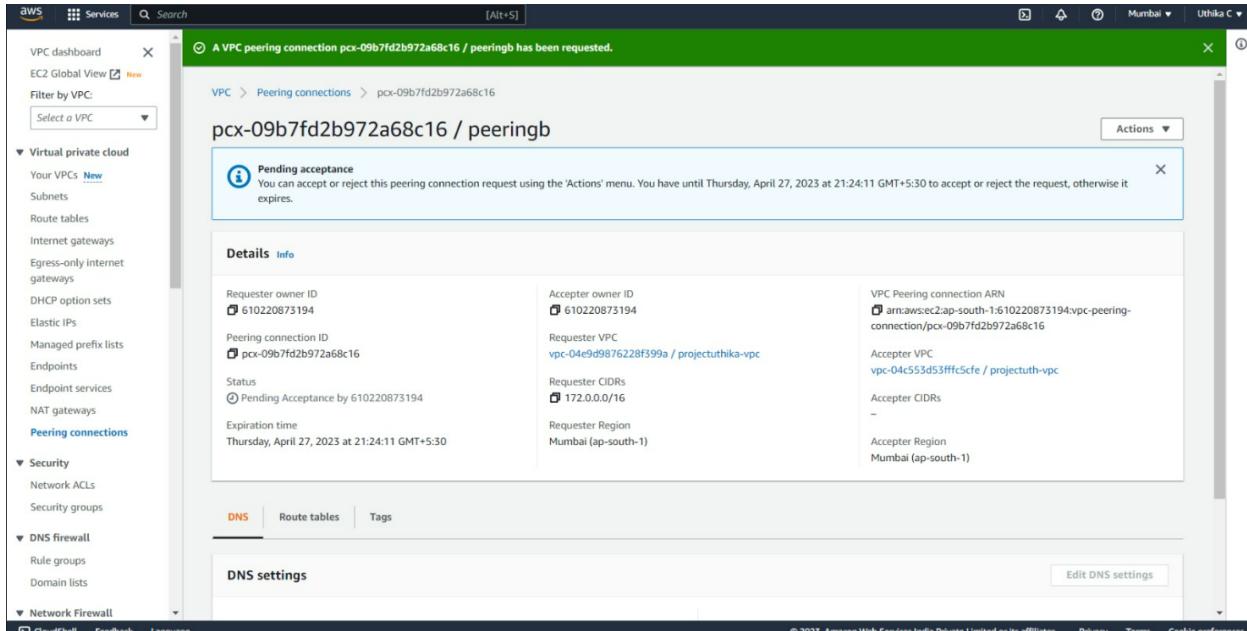


A screenshot of the AWS VPC Peering Connections page showing a pending acceptance request. The peering connection ID is pcv-0464f57ae9916f745. The requester is Uthika C (arn:aws:ec2:ap-south-1:610220873194:vpc-peering-connection/pcv-0464f57ae9916f745) and the accepter is vpc-04e553d53fffc5ce (projectuthika-vpc). Both are located in Mumbai (ap-south-1). The status is Pending Acceptance by 610220873194. The expiration time is Thursday, April 27, 2023 at 21:19:54 GMT+5:30.

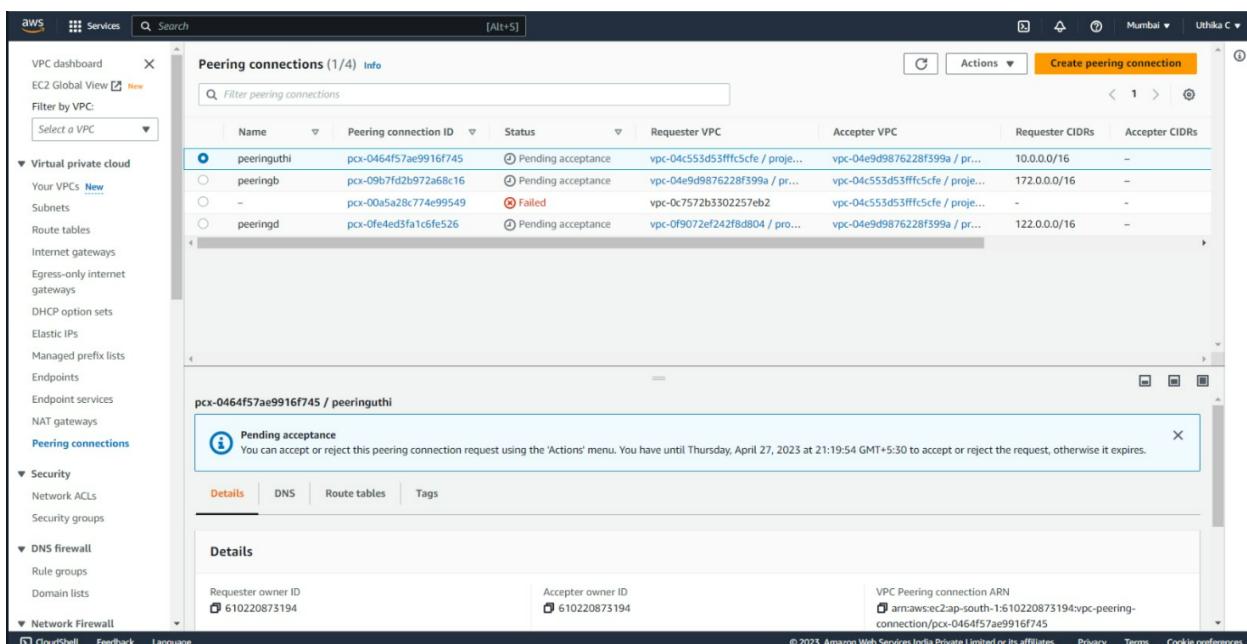
Details

Requester owner ID	Acceptor owner ID	VPC Peering connection ARN
610220873194	610220873194	arn:aws:ec2:ap-south-1:610220873194:vpc-peering-connection/pcv-0464f57ae9916f745
Peering connection ID	Requester VPC	Acceptor VPC
pcv-0464f57ae9916f745	vpc-04e553d53fffc5ce / projectvpc-vpc	vpc-04e553d53fffc5ce / projectuthika-vpc
Status	Requester CIDRs	Acceptor CIDRs
Pending Acceptance by 610220873194	10.0.0.0/16	-
Expiration time	Requester Region	Acceptor Region
Thursday, April 27, 2023 at 21:19:54 GMT+5:30	Mumbai (ap-south-1)	Mumbai (ap-south-1)

DNS settings



A screenshot of the AWS VPC Peering Connections page. A green header bar at the top indicates a 'Pending acceptance' status for a peering connection named 'pcx-09b7fd2b972a68c16'. The main content area shows the details of this connection, including Requester owner ID (610220873194), Acceptor owner ID (610220873194), Peering connection ID (pcx-09b7fd2b972a68c16), Requester VPC (vpc-04e9d9876228f399a / projectuthika-vpc), Acceptor VPC (vpc-04c553d53fffc5cfe / projectuth-vpc), Status (Pending Acceptance by 610220873194), Requester CIDRs (172.0.0.0/16), Acceptor CIDRs (empty), Requester Region (Mumbai (ap-south-1)), and Acceptor Region (Mumbai (ap-south-1)). Below this, there are tabs for DNS, Route tables, and Tags, with the DNS tab currently selected. A 'DNS settings' section is visible.



A screenshot of the AWS VPC Peering Connections page showing a list of four peering connections. The table includes columns for Name, Peering connection ID, Status, Requester VPC, Acceptor VPC, Requester CIDRs, and Acceptor CIDRs. The connections are:

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
peeringuthi	pcx-0464f57ae9916f745	Pending acceptance	vpc-04c553d53fffc5cfe / proj...	vpc-04e9d9876228f399a / pr...	10.0.0.0/16	-
peeringb	pcx-09b7fd2b972a68c16	Pending acceptance	vpc-04e9d9876228f399a / pr...	vpc-04c553d53fffc5cfe / proj...	172.0.0.0/16	-
-	pcx-00a5a28c774e99549	Failed	vpc-0c7572b3302257eb2	vpc-04c553d53fffc5cfe / proj...	-	-
peeringd	pcx-0fe4ed3fa1c6fe526	Pending acceptance	vpc-0f9072ef242f8d804 / pr...	vpc-04e9d9876228f399a / pr...	122.0.0.0/16	-

Below the table, a specific peering connection ('pcx-0464f57ae9916f745 / peeringuthi') is selected, showing its pending acceptance status and details. The 'Details' tab is selected, displaying the same information as the main connection details above.

6)Create VPC peering connections for 3 different VPCs from the same region

NAME:UTHIKA C
REG NO:727721EUCS173

The screenshot shows the AWS VPC Network ACLs interface. The top navigation bar includes the AWS logo, Services, a search bar, and user information for "Uthika C". A green banner at the top right indicates: "You have successfully updated inbound rules for acl-009d4f3494eb57817". The left sidebar has sections for Virtual private cloud (Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections), Security (Network ACLs, Security groups), and DNS firewall. The main content area shows the details for Network ACL ID "acl-009d4f3494eb57817", which is associated with 4 subnets, is the Default, and is linked to VPC ID "vpc-0c572b3302257eb2 / project-1-vpc". Below this, tabs for Inbound rules, Outbound rules, Subnet associations, and Tags are visible. A message says "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button. The Inbound rules section shows a table with one row:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
98	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Deny

At the bottom, there are links for CloudShell, Feedback, Language, and a footer note: "© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences".