

# CLOUD COMPUTING

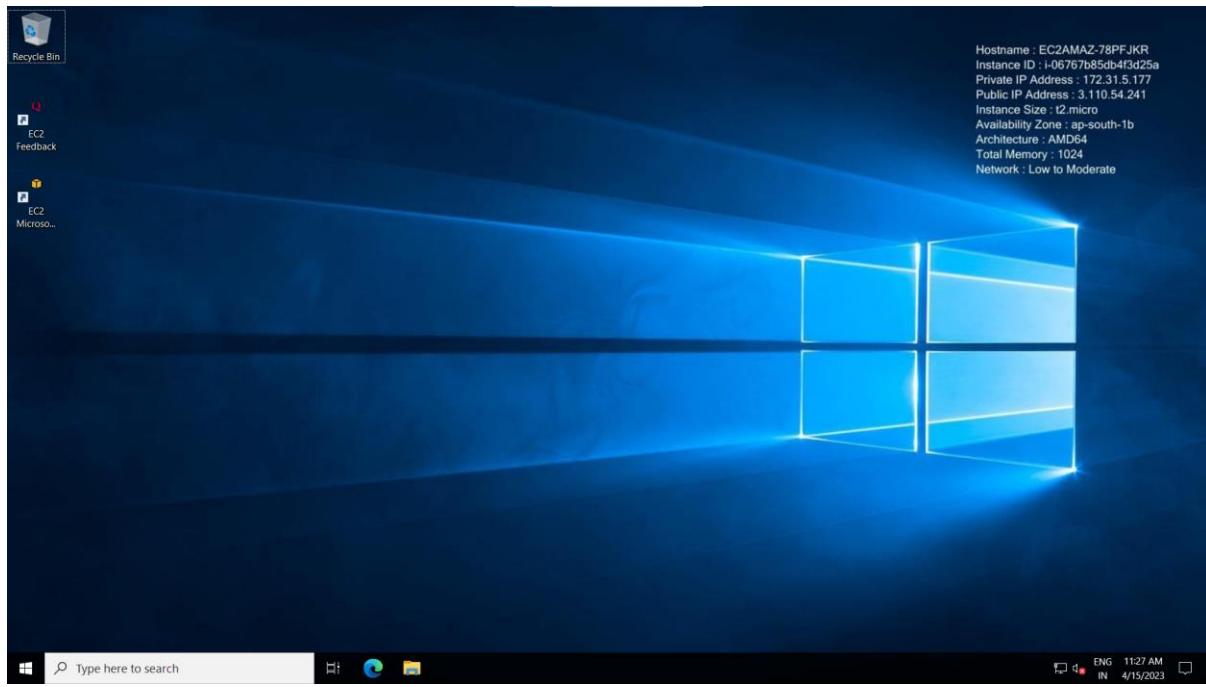
**NAME:** SUBIKSHA KR

**ROLL NO:** 727721eucs154

## DAY 2

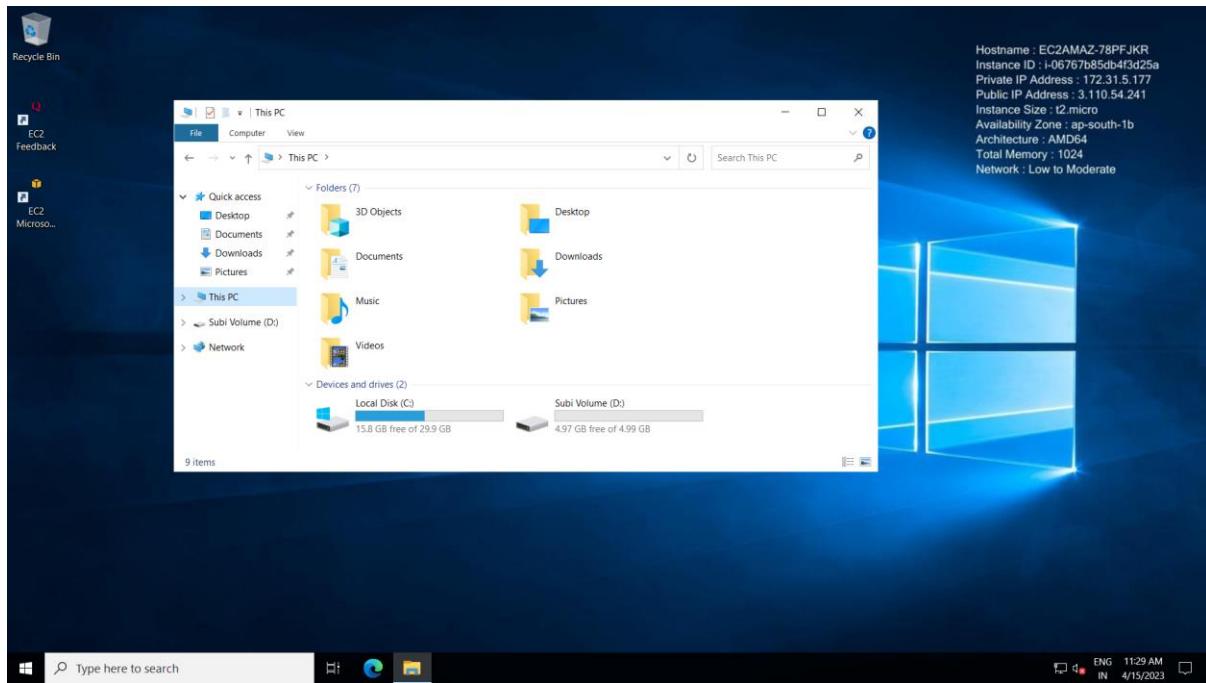
- 1) Create a Windows EC2 instance with t2.micro Instance and show the remote connection of that EC2 Instance.

The screenshot shows the AWS EC2 Instance Details page. The instance ID is i-06767b85db4f3d25a, labeled as SubiWindowsServer. The instance state is Stopped. The instance type is t2.micro, running on a VPC with ID vpc-08f216c0a68454ecd. It is associated with a subnet ID subnet-03f070a381f9dbfc5. The platform is windows, and the AMI ID is ami-09461328af8fbcb9c. The public IPv4 address is 172.31.5.177, and the private IP DNS name is ip-172-31-5-177.ap-south-1.compute.internal. The instance was updated less than a minute ago.

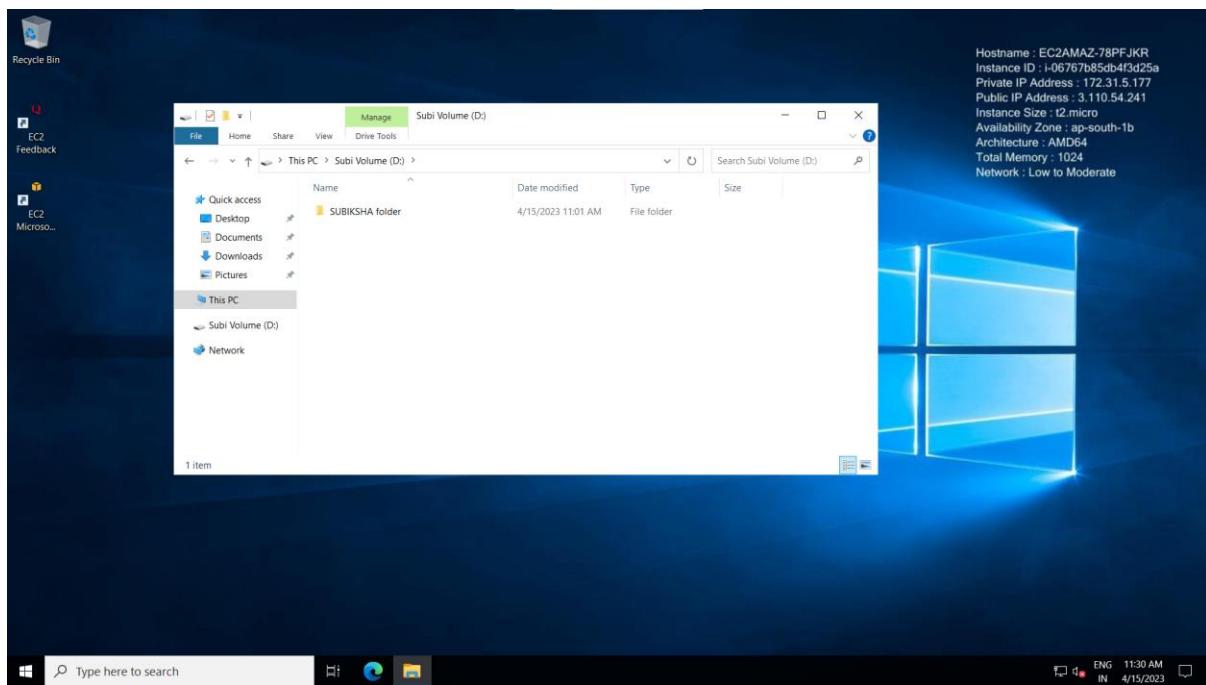


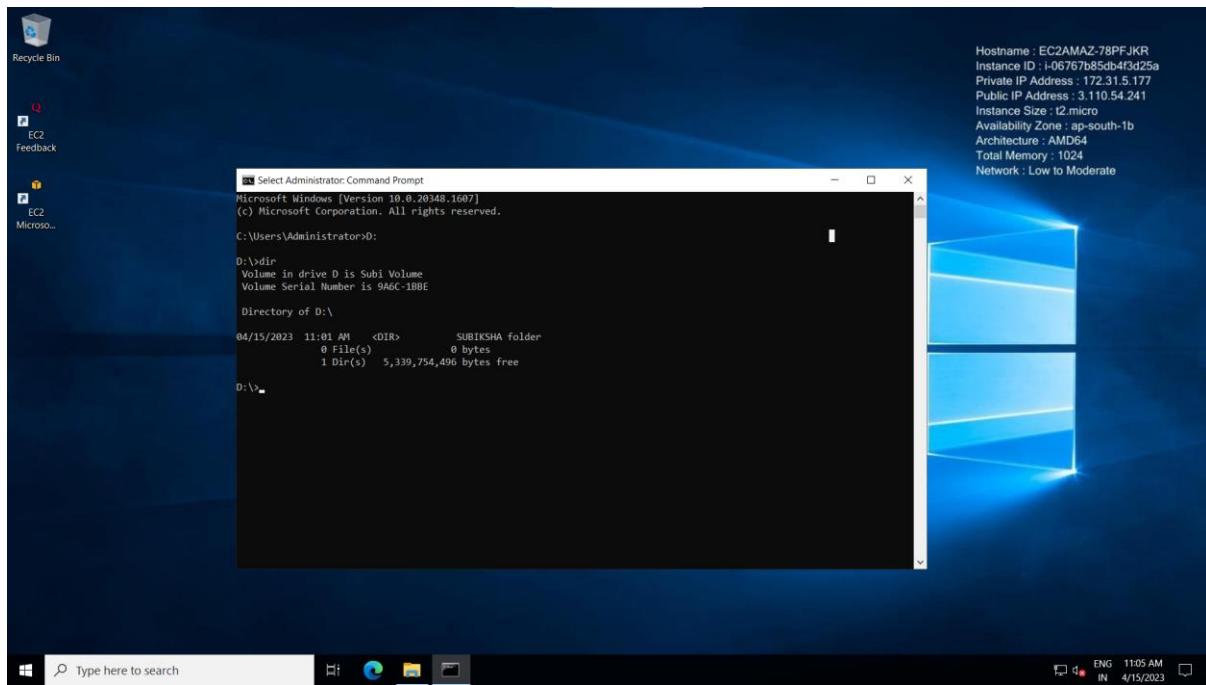
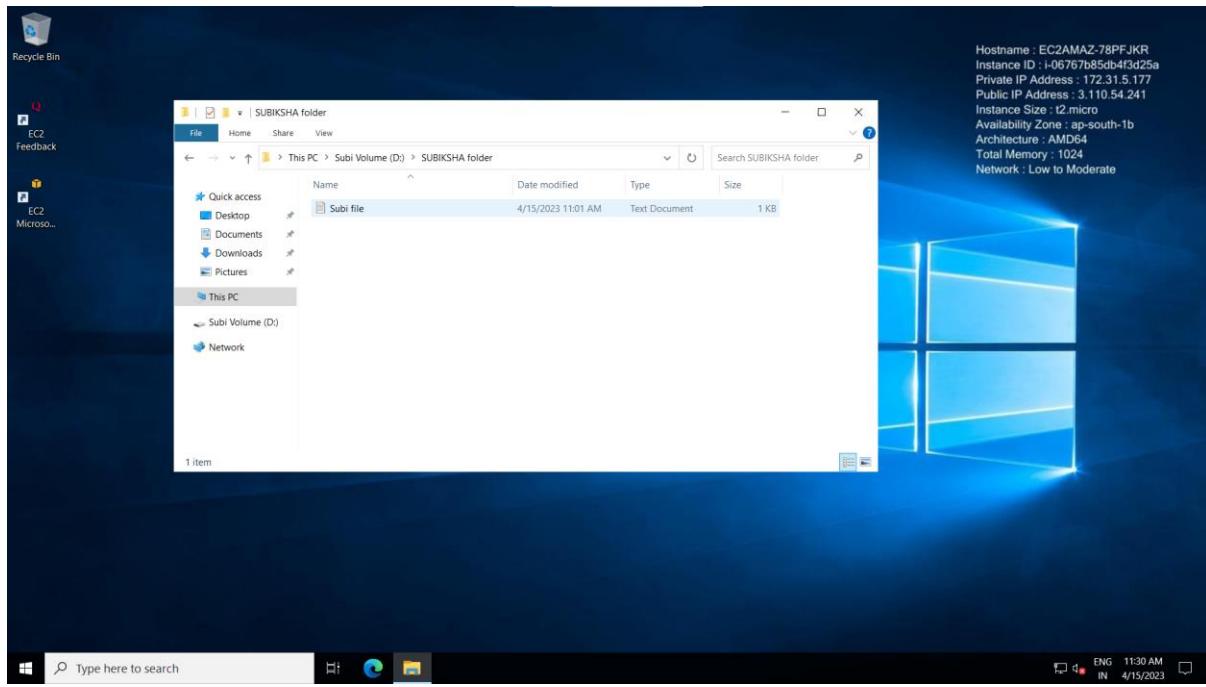
2) Create an EBS volume of 5 GB and attach to a windows EC2 instance and make partition of that EBS volume.

A screenshot of the AWS CloudWatch Metrics interface. The main view shows a line chart titled "CPU Usage" with data points for "SubiWindowsServer" over a period from April 11, 2023, to April 15, 2023. The chart shows a single data series with values ranging from approximately 10% to 20%. Below the chart, there is a table with metrics like "CPU Utilization", "CPU Queue Length", and "CPU Swap Cache". On the left side, there is a navigation pane with links to "Metrics Home", "Metrics Overview", "Metrics Data", "Metrics Insights", and "Metrics Metrics Insights".



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





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

Instance summary for i-0d4aae9a3c4792ac7 (SubiLinuxServer) [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0d4aae9a3c4792ac7 (SubiLinuxServer)	13.232.191.27   <a href="#">open address</a>	172.31.10.200
IPv6 address	-	Public IPv4 DNS
Hostname type	Running	e2-15-232-191-27.ap-south-1.compute.amazonaws.com   <a href="#">open address</a>
IP name: ip-172-31-10-200.ap-south-1.compute.internal		Elastic IP addresses
Answer private resource DNS name	t2.micro	-
IPv4 (A)	VPC ID	AWS Compute Optimizer finding
Auto-assigned IP address	vpc-08f216c0a68454ecd	Opt-in to AWS Compute Optimizer for recommendations.
13.232.191.27 [Public IP]	Subnet ID	Learn more
IAM Role	subnet-03f070a381f9dbfc5	Auto Scaling Group name
-		-
IMDSv2		
Required		

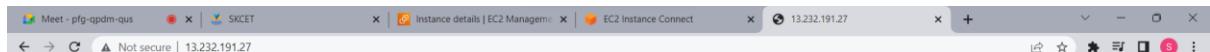
[Details](#) [Security](#) [Networking](#) [Storage](#) [Status checks](#) [Monitoring](#) [Tags](#)

```
A newer release of "Amazon Linux" is available.  
Version 2023.0.20230329:  
Run "/usr/bin/dnf check-release-update" for full release and version update info  
Amazon Linux 2023  
https://aws.amazon.com/linux/amazon-linux-2023  
Last login: Sat Apr 15 11:17:53 2023 from 152.58.222.182  
[ec2-user@ip-172-31-10-200 ~]$
```

i-0d4aae9a3c4792ac7 (SubiLinuxServer)

Public IPs: 13.232.191.27 Private IPs: 172.31.10.200

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



It works!

---

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

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
SubiLinuxServer	i-0d4aae9a3c4792ac7	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b	ec2-13-232-191-
SubiWindowsS...	i-06767bb5d4f3d25a	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b	ec2-3-110-54-24
ASG-Subi	i-0add25986a11b4596	Stopped	t2.micro	-	No alarms	ap-south-1a	-

The screenshot shows the AWS EC2 "Launch an instance" success page. At the top, there are three tabs: "Meet - pfq-qpdm-eus", "SKCET", and "Launch an instance | EC2 Manager". The main content area has a dark header with "Success" and "Successfully initiated launch of instance (i-0e0987aafa9098fc3)". Below this is a "Launch log" button. A "Next Steps" section follows, featuring a search bar and a numbered list from 1 to 6. The steps include: "Create billing and free tier usage alerts", "Connect to your instance", "Connect an RDS database", "Create EBS snapshot policy", "Manage detailed monitoring", "Create Load Balancer", "Create AWS budget", and "Manage CloudWatch alarms". The bottom of the page includes links for "CloudShell", "Feedback", "Language", and copyright information: "© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences".

## DAY 3

- 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 Management Console. A green success message at the top states: "Successfully created bucket 'shbucket'. To upload files and folders, or to configure additional bucket settings choose View details." The left sidebar shows navigation options like Buckets, Access Points, and Storage Lens. The main area displays an "Account snapshot" with a "Buckets" table. The table has columns for Name, AWS Region, Access, and Creation date. It shows one entry: "shbucket" (AWS Region: ap-south-1, Access: Private, Creation date: Loading buckets).

The screenshot shows the AWS S3 Management Console with the path "Amazon S3 > Buckets > shbucket". A green success message at the top states: "Successfully created folder 'SHfolder'. Operation successfully completed." The main area shows the "Objects (1)" section. It displays a single object named "SHfolder/" with a "Folder" type. The table has columns for Name, Type, Last modified, Size, and Storage class. The "Actions" dropdown menu includes options like Copy S3 URI, Copy URL, Download, Open, Delete, Create folder, and Upload.

The screenshot shows the AWS S3 Management Console with a successful upload message: "Upload succeeded". The summary table indicates 1 file uploaded successfully (Succeeded) and 0 files failed. The "Files and folders" tab is selected, showing a single file named "first day.txt" with a size of 367.0 B and a status of "Succeeded".

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

The screenshot shows the AWS S3 Management Console with a success message: "Successfully created bucket 'sh2bucket'". The "Buckets" section lists three buckets: "sh2bucket", "shbucket", and "subikr". The "sh2bucket" bucket has its "Block Public Access settings for this account" option disabled, indicated by a green checkmark icon. The "shbucket" and "subikr" buckets have their "Block Public Access settings for this account" options enabled, indicated by a red warning triangle icon.

Amazon S3 > Buckets > sh2bucket

sh2bucket Info

Permissions overview

Access  
Objects can be 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

Individual Block Public Access settings for this bucket

Upload succeeded

View details below.

Upload: status

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

Summary

Destination	Succeeded	Failed
s3://sh2bucket/sh2folder/	1 file, 367.0 B (100.00%)	0 files, 0 B (0%)

Files and folders (1 Total, 367.0 B)

Name	Folder	Type	Size	Status	Error
first day.txt	-	text/plain	367.0 B	Succeeded	-

Google Me x SKCET x AWS # 015 x sh2bucket x Access com x Creating o x Launch an x what is aci x Bucket poli x sis in public x +

s3.console.aws.amazon.com/s3/buckets/sh2bucket/object/edit\_acl?region=ap-south-1&prefix=sh2folder/first+day.txt

AWS Services Search [Alt+S]

Amazon S3 > Buckets > sh2bucket > sh2folder/ > first day.txt > Edit access control list

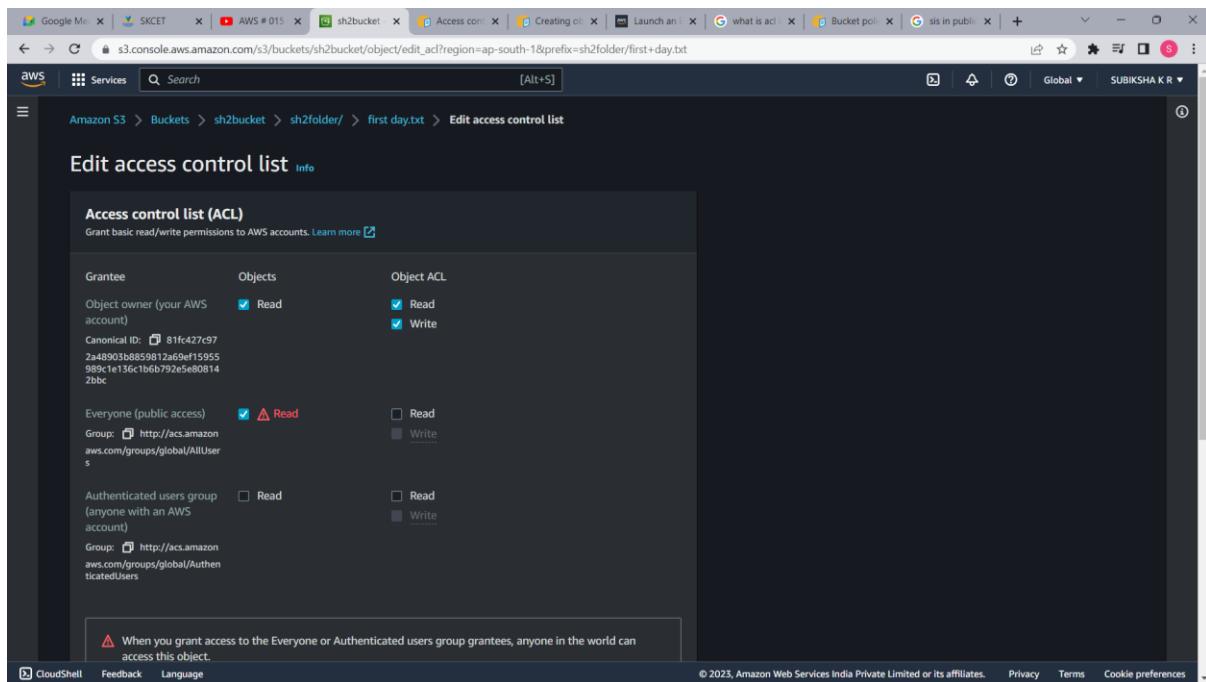
### Edit access control list Info

**Access control list (ACL)**  
Grant basic read/write permissions to AWS accounts. Learn more ?

Grantee	Objects	Object ACL
Object owner (your AWS account)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	
Canonical ID: 81fc427c972a48903b8859812a69ef15955989c1e156c1b6b792e5e808142bbc		
Everyone (public access)	<input checked="" type="checkbox"/> <small>⚠ Read</small> Group: http://acs.amazonaws.com/groups/global/AllUsers	<input type="checkbox"/> Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account)	<input type="checkbox"/> Read Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input type="checkbox"/> Read <input type="checkbox"/> Write

⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.

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



The screenshot shows the 'Edit access control list' page for the file 'first day.txt'. It displays the ACL configuration with three entries: 'Object owner (your AWS account)' with 'Read' and 'Write' checked, 'Everyone (public access)' with 'Read' checked, and 'Authenticated users group (anyone with an AWS account)' with 'Read' checked. A note at the bottom states: '⚠ When you grant access to the Everyone or Authenticated users group grantees, anyone in the world can access this object.'

Google Me x SKCET x AWS # 015 x Access com x Creating o x Launch an x what is aci x Bucket poli x sis in public x +

s3.console.aws.amazon.com/s3/object/sh2bucket?region=ap-south-1&prefix=sh2folder%2Ffirst+day.txt&tab=permissions

AWS Services Search [Alt+S]

Amazon S3 > Buckets > sh2bucket > sh2folder/ > first day.txt

### first day.txt Info

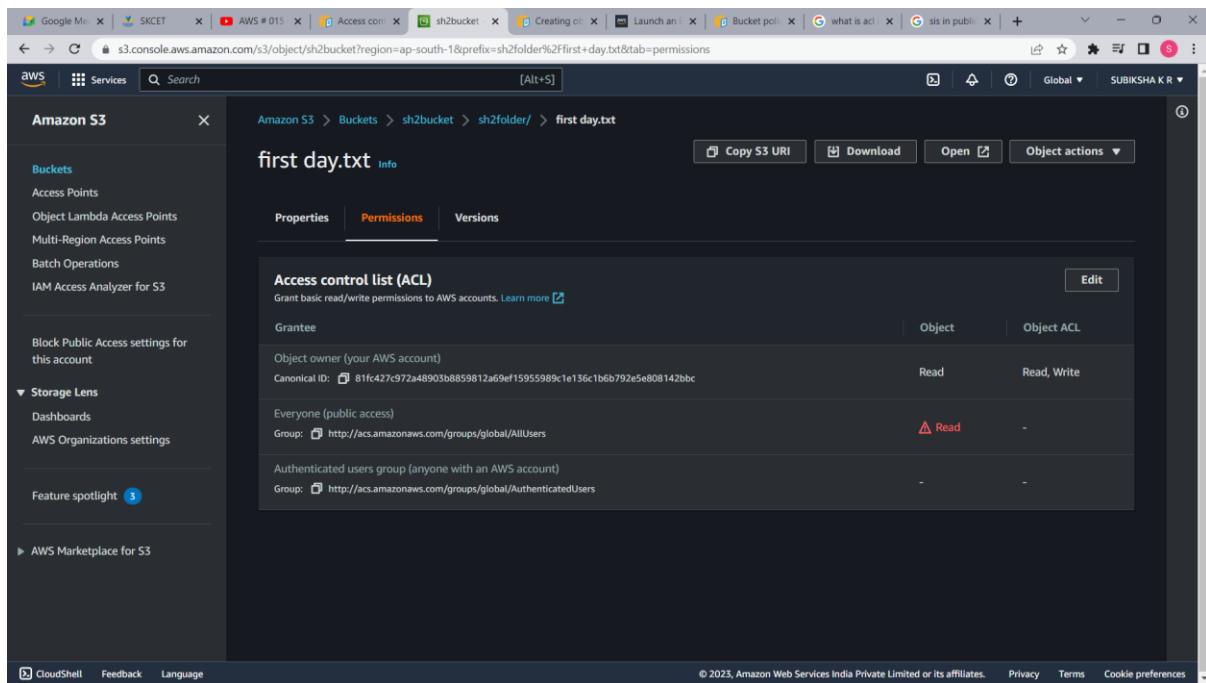
Copy S3 URI Download Open ⚡ Object actions ▾

**Properties** **Permissions** **Versions**

**Access control list (ACL)**  
Grant basic read/write permissions to AWS accounts. Learn more ?

Grantee	Object	Object ACL
Object owner (your AWS account)	Read	Read, Write
Canonical ID: 81fc427c972a48903b8859812a69ef15955989c1e156c1b6b792e5e808142bbc		
Everyone (public access)	<small>⚠ Read</small>	-
Authenticated users group (anyone with an AWS account)	-	-

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



The screenshot shows the 'Permissions' tab for the file 'first day.txt'. It displays the ACL configuration with three entries: 'Object owner (your AWS account)' with 'Read' and 'Write' checked, 'Everyone (public access)' with 'Read' checked, and 'Authenticated users group (anyone with an AWS account)' with 'Read' checked. The 'Edit' button is visible in the top right corner of the ACL table.

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

The screenshot shows the AWS S3 Bucket Policy editor. At the top, a green success message says "Successfully edited bucket policy." Below it, there's a section for "Block all public access" which is currently "Off". The main area displays a JSON-based bucket policy:

```
{
  "Version": "2012-10-17",
  "Id": "Policy1681563908529",
  "Statement": [
    {
      "Sid": "Stmt1681563907080",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::shbucket/*"
    }
  ]
}
```

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

The screenshot shows the AWS S3 Bucket creation confirmation page. A green message at the top says "Successfully created bucket 'sh3bucket369'". Below it, there's an "Account snapshot" section and a table of buckets. The table has columns for Name, AWS Region, Access, and Creation date. A progress bar at the bottom indicates "Loading buckets".

Name	AWS Region	Access	Creation date
Loading buckets			

Objects (3)

Name	Type	Version ID	Last modified	Size	Storage class
mybiodata.pdf	pdf	BDFD8ukeoJA8Ycp2EW.xFcJxoiZv6PW	April 17, 2023, 17:03:09 (UTC+05:30)	30.3 KB	Standard
mybiodata.pdf	pdf	HNsDwg3f77cvYcKk4rcPSA_fmjKY6	April 17, 2023, 17:02:28 (UTC+05:30)	30.3 KB	Standard
mybiodata.pdf	pdf	rdeXk75bG1aGtrij1hZXFaXCIQaSpM	April 17, 2023, 17:01:36 (UTC+05:30)	30.3 KB	Standard

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

Static website hosting in a bucket



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

The lifecycle configuration was updated. Lifecycle rule "rule1SH" was successfully added.  
It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed.

Amazon S3 > Buckets > sh3bucket369 > Lifecycle configuration

Lifecycle configuration [Info](#)

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

**Lifecycle rules (1)**

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

<a href="#">View details</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Actions ▾</a>	<a href="#">Create lifecycle rule</a>
<input type="button" value="G"/> <a href="#">Find lifecycle rules by name</a>				
<a href="#">Lifecycle rule name</a>	<a href="#">Status</a>	<a href="#">Scope</a>	<a href="#">Current version actions</a>	<a href="#">Noncurrent versions actions</a>
rule1SH	<span>Enabled</span>	Filtered	Transition to Standard-IA	-

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

## DAY 4

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

The screenshot shows the AWS IAM Management Console. In the top right corner, there is a green banner that says "S3-Admins user group created." Below this, the main interface shows the "User groups" section. There is a table with four rows:

Group name	Users	Permissions	Creation time
admin	>Loading	>Loading	6 days ago
S3-Admins	>Loading	Defined	Now
secops	>Loading	>Loading	5 days ago

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

The screenshot shows the AWS IAM Management Console. In the top right corner, there is a green banner that says "User created successfully". Below this, the main interface shows the "Create user" step. On the left, there is a sidebar with steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The current step is Step 4. The main area is titled "Retrieve password" and contains the following information:

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

**Console sign-in details**

Console sign-in URL	<a href="https://605266716064.signin.aws.amazon.com/console">https://605266716064.signin.aws.amazon.com/console</a>	Email sign-in instructions
User name	S3Admin1	
Console password	***** Show	

At the bottom right, there are two buttons: "Download .csv file" and "Return to users list".

The screenshot shows the AWS IAM Management Console. A green success message at the top states "User created successfully" and "You can view and download the user's password and email instructions for signing in to the AWS Management Console." Below this, the "Users" section displays five users: S3Admin1, subi, subiks, SUBIKSHA.K.R, and SubikshaKithuvaRamkumar. The table includes columns for User name, Groups, Last activity, MFA, Password age, and Active key age.

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

The screenshot shows the AWS IAM Management Console on the "Policies" page. A green success message at the top states "The policy SHpolicy has been created." The table lists various policies, including the newly created "SHpolicy".

Policy name	Type	Used as	Description
SHpolicy	Customer managed	None	
AWSDirectConnectReadOnlyAccess	AWS managed	None	Provides read only
AmazonGlacierReadOnlyAccess	AWS managed	None	Provides read only
AWSMarketplaceFullAccess	AWS managed	None	Provides the ability
ClientVPNServiceRolePolicy	AWS managed	None	Policy to enable AW
AWSSSOAdministrator	AWS managed	None	Administrator acc
AWSToT1ClickReadOnlyAccess	AWS managed	None	Provides read-only
AutoScalingConsoleReadOnlyAccess	AWS managed	None	Provides read-only
AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to
AWSSQuickSightListIAM	AWS managed	None	Allow QuickSight to
AmazonSQSFullAccess	AWS managed	None	Allows full access to

The screenshot shows the AWS IAM Management Console. On the left, a sidebar navigation includes 'Identity and Access Management (IAM)', 'Access management' (with 'User groups' selected), 'Access reports', and other options like 'Archive rules' and 'Settings'. The main content area displays the 'S3-Admins' user group under 'User groups'. It shows the group's name, creation time (April 16, 2023, 13:44 UTC+05:30), and ARN (arn:aws:iam::605266716064:group/S3-Admins). Below this, there are tabs for 'Users', 'Permissions' (which is selected), and 'Access Advisor'. Under 'Permissions policies (2)', it lists two policies: 'SHpolicy' (Customer managed) and 'AmazonS3FullAccess' (AWS managed). Both policies have a status of 'Enabled without MFA'. At the bottom, there are links for 'CloudShell', 'Feedback', and 'Language', along with a copyright notice for 2023 and links for 'Privacy', 'Terms', and 'Cookie preferences'.

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

The screenshot shows the AWS IAM Management Console. The sidebar navigation is identical to the previous screen. The main content area displays the 'S3Admin1' user under 'Users'. It shows the user's ARN (arn:awsiam:605266716064:user/S3Admin1), creation date (April 16, 2023, 13:47 UTC+05:30), and console access status ('Enabled without MFA'). Below this, there are tabs for 'Permissions' (selected), 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor'. Under 'Permissions policies (4)', it lists four policies: 'AmazonS3FullAccess' (Attached via Group S3-Admins), 'IAMUserChangePassword' (Attached directly), 'SHpolicy' (Attached via Group S3-Admins), and 'SHuserpolicy' (Attached inline). All policies have a status of 'Enabled without MFA'. At the bottom, there are links for 'CloudShell', 'Feedback', and 'Language', along with a copyright notice for 2023 and links for 'Privacy', 'Terms', and 'Cookie preferences'.

S3Admin1

ARN: arn:aws:iam::605266716064:user/S3Admin1

Console access: Enabled without MFA

Created: April 16, 2023, 13:47 (UTC+05:30)

Last console sign-in: Never

Access key 1: Enabled without MFA

Access key 2: Not enabled

Permissions policies (4):

- AmazonS3FullAccess (AWS managed, Attached via Group S3-Admins)
- IAMUserChangePassword (AWS managed, Directly)
- IAMFullAccess (AWS managed, Attached via Group S3-Admins)
- IAMUserChangePassword (AWS managed, Attached via Group S3-Admins)

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

Role iamrole created.

Roles (4) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

View role

Create role

Search

Role name	Trusted entities	Last activity
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	3 days ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
iamrole	AWS Service: ec2	-

Roles Anywhere

Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

The screenshot shows the AWS EC2 Management Console. A modal window titled "Successfully attached iamrole to instance i-06767b85db4f3d25a" is displayed over the main "Instances" list. The main list shows three instances: SubiLinuxServer, SubiWindowsS..., and ASG-Subi, all in the "Stopped" state. The left sidebar includes sections for EC2 Dashboard, 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 (Volumes, Snapshots). The bottom of the screen includes CloudShell, Feedback, Language, and copyright information for 2023.

## 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 Management Console. It displays the "Security credentials" tab for the "S3Admin1" user under the "Users" section. The summary table shows the following details:

ARN	Console access	Access key 1
arn:aws:iam::605266716064:user/S3Admin1	Enabled with MFA	Not enabled
Created April 16, 2023, 13:47 (UTC+05:30)	Last console sign-in Never	Access key 2 Not enabled

The "Console sign-in" section shows a "Manage console access" button and a link to https://605266716064.siginin.aws.amazon.com/console. The bottom of the screen includes CloudShell, Feedback, Language, and copyright information for 2023.

IAM Management Console

Identity and Access Management (IAM)

MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

Console sign-in

Console sign-in link: https://605266716064.signin.aws.amazon.com/console

Console password: Updated 38 minutes ago (2023-04-16 13:47 GMT+5:30)

Last console sign-in: Never

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more

Remove Resync Assign MFA device

Device type	Identifier	Created on
Virtual	arn:aws:iam::605266716064:mfa/subikshadevice	Now

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Create access key

CloudShell Feedback Language

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

IAM Management Console

Identity and Access Management (IAM)

Account settings

Password requirements for IAM users are updated.

IAM > Account Settings

Account settings info

Password policy info

Configure the password requirements for the IAM users.

Edit

This AWS account uses the following custom password policy:

Password minimum length: 8 characters

Other requirements:

- Never expire password

Password strength:

- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)

Security Token Service (STS) info

STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.

Session Tokens from the STS endpoints

AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS endpoints, no action is required. Session tokens from the global STS endpoint (<https://sts.amazonaws.com>) are valid only in AWS Regions that are enabled by default.

CloudShell Feedback Language

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

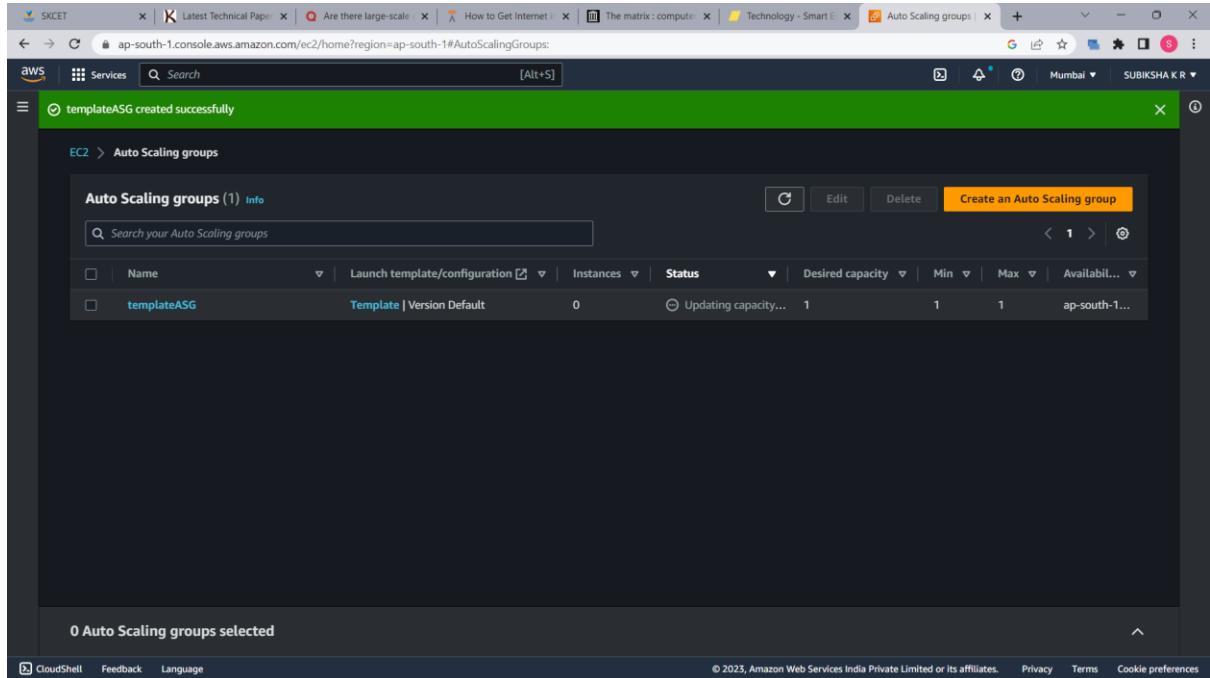
## Day5

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

The screenshot shows the AWS EC2 'Create launch template' success page. At the top, there is a success message: 'Successfully created Template (lt-0ad8d414f30f93fd8)'. Below this, there is a 'Actions log' section. Under 'Next steps', there are several options: 'Launch an instance', 'Launch instance from this template', 'Create an Auto Scaling group from your template', 'Amazon EC2 Auto Scaling helps maintain application availability and allows you to scale your Amazon EC2 capacity up or down automatically according to conditions you define. You can use Auto Scaling to help ensure that you are running your desired number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.', 'Create Auto Scaling group', 'Create Spot Fleet', and 'Create Spot Fleet'. At the bottom right, there is a 'View launch templates' button.

The screenshot shows the AWS EC2 'Template (lt-0ad8d414f30f93fd8)' details page. On the left, there is a navigation sidebar with 'New EC2 Experience' selected. The main content area shows 'Launch template details' for the template ID 'lt-0ad8d414f30f93fd8'. It includes fields for 'Launch template name' (Template), 'Default version' (1), and 'Owner' (arn:aws:iam::605266716064:root). Below this, there is a 'Launch template version details' section for version 1 (Default). This section includes tabs for 'Details', 'Versions', and 'Template tags'. The 'Details' tab shows 'Version' (1), 'Description' (empty), 'Date created' (2023-04-16T16:09:16.000Z), and 'Created by' (arn:aws:iam::605266716064:root). The 'Instance details' tab shows 'AMI ID' (ami-0cf6131382b6722a6), 'Instance type' (t2.micro), 'Availability Zone' (empty), and 'Key pair name' (SubiWinKeyPair). The 'Storage', 'Resource tags', 'Network interfaces', and 'Advanced details' tabs are also present but show empty or default values.

2) Create an autoscaling group with the above-created launch template



The screenshot shows the AWS EC2 Auto Scaling groups page. At the top, there is a green success message: "templateASG created successfully". Below this, the page title is "Auto Scaling groups (1) [Info](#)". A search bar is present. The main table has columns: Name, Launch template/configuration, Instances, Status, Desired capacity, Min, Max, and Available. One row is shown for "templateASG", which is associated with the "Template | Version Default" launch configuration, has 0 instances, and is in an "Updating capacity..." status. The "Desired capacity" is set to 1, and the "Min" and "Max" values are also 1. The "Available" column shows "ap-south-1...". At the bottom left, it says "0 Auto Scaling groups selected". The bottom navigation bar includes links for CloudShell, Feedback, Language, and cookie preferences.

## Day6

1) Create a vpc with multiple subnets(atleast 1 subnet in each zone)

The screenshot shows the AWS VPC Details page for a VPC named 'vpc-0b56db9d6dcc4b49c'. The VPC ID is 'vpc-0b56db9d6dcc4b49c'. The State is 'Available'. The DHCP option set is 'dopt-0fee67ade3352e89f'. The Main route table is 'rtb-0ac4610eb82cb73'. The IPv6 pool is '-' and the Owner ID is '605266716064'. The DNS hostnames are 'Disabled' and DNS resolution is 'Enabled'. The Main network ACL is 'acl-08921e028cdc58382'. The Network Address Usage metrics are 'Disabled'. The Route 53 Resolver DNS Firewall rule groups are '-'. The Resource map, CIDRs, Flow logs, and Tags tabs are visible at the bottom.

The screenshot shows the AWS Subnets page. A success message says 'You have successfully created 1 subnet: subnet-0fd6e543b443005f'. The Subnets table shows one entry: 'shsubnet1' with Subnet ID 'subnet-0fd6e543b443005f', State 'Available', VPC 'vpc-0b56db9d6dcc4b49c | shvpc', IPv4 CIDR '10.0.0.0/24', IPv6 CIDR '—', Available IPv4 addresses '251', Availability Zone 'ap-south-1a', and Availability Zone ID 'ap-s1-az1'. The 'Actions' button and 'Create subnet' button are visible at the top right. The left sidebar includes options like VPC dashboard, EC2 Global View, Filter by VPC, and various VPC and Security settings.

You have successfully created 1 subnet: subnet-05c8073a32b89a804

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
shsubnet2	subnet-05c8073a32b89a804	Available	vpc-0b56db9e6dc4b4fc   shvpc	10.0.2.0/24	-	251	ap-south-1b	aps1-az3

Select a subnet

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

You have successfully created 1 subnet: subnet-0884ba6b2ad5b1b6d

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
shsubnet3	subnet-0884ba6b2ad5b1b6d	Available	vpc-0b56db9e6dc4b4fc   shvpc	10.0.3.0/24	-	251	ap-south-1c	aps1-az2

Select a subnet

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

The screenshot shows the AWS VPC Subnets page. On the left, a sidebar lists various VPC-related services like EC2 Global View, Subnets, Route tables, Internet gateways, etc. The main content area displays a table of subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
shubnet2	subnet-05d075a12b89e204	Available	vpc-0b56d89f0dc4b49c	10.0.2.0/24	-	251	ap-south-1a	apst1-a2
shubnet3	subnet-0884bd9272d5116d	Available	vpc-0b56d89f0dc4b49c	10.0.3.0/24	-	251	ap-south-1c	apst1-a2
shubnet1	subnet-0f65c543b443005f	Available	vpc-0b56d89f0dc4b49c	10.0.1.0/24	-	251	ap-south-1a	apst1-a2

A modal window titled "Select a subnet" is open at the bottom, listing the same three subnets.

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

The screenshot shows the AWS VPC Subnets page. The sidebar is identical to the previous one. The main content area displays a table of subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
shpct-subnet-prv1	subnet-080c11f1ec1a3	Available	vpc-061218084b7c53cbc	10.0.128.0/20	-	4091	ap-south-1a	apst1-a2
shpct-subnet-pub1	subnet-0d35e1837f7f9820	Available	vpc-061218084b7c53cbc	10.0.16.0/20	-	4091	ap-south-1b	apst1-a2
shpct-subnet-pub2	subnet-0488f1c124f7746	Available	vpc-061218084b7c53cbc	10.0.0.0/20	-	4091	ap-south-1a	apst1-a2
shpct-subnet-prv2	subnet-0090f2e61555cc05	Available	vpc-061218084b7c53cbc	10.0.144.0/20	-	4091	ap-south-1b	apst1-a2

A modal window titled "Select a subnet" is open at the bottom, listing the same four subnets.

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

**NAT gateway ID:** nat-0b3f85bd3b0cca675

**Connectivity type:** Public

**Primary public IPv4 address:** -

**Primary private IPv4 address:** -

**Subnet:** subnet-0fd2e5b7051a9d8d / shnat-subnet-private1-ap-south-1a

**State:** Pending

**Created:** Thursday, April 20, 2023 at 12:29:43 GMT+5:30

**State message:** Info

**Actions:** Edit, Delete

**NAT gateway ID:** nat-0def4ecfdec0cb40d

**Connectivity type:** Public

**Primary public IPv4 address:** -

**Primary private IPv4 address:** -

**Subnet:** subnet-0bb9af4fc52e2bceb / shnat-subnet-private2-ap-south-1b

**State:** Pending

**Created:** Thursday, April 20, 2023 at 12:30:23 GMT+5:30

**State message:** Info

**Actions:** Edit, Delete

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

The screenshot shows the AWS VPC Peering Connections page in the us-east-1 region. A green banner at the top indicates that a peering connection has been requested. The main table displays the details of the peering connection:

Details		Info	
Requester owner ID	<a href="#">605266716064</a>	Acceptor owner ID	<a href="#">605266716064</a>
Peering connection ID	<a href="#">pxc-077c8d68576e040fe</a>	Requester VPC	<a href="#">vpc-054d137800daec2c9 / shvpc-vir</a>
Status	<a href="#">Initiating Request to 605266716064</a>	Requester CIDR	<a href="#">172.0.0.0/16</a>
Expiration time	Thursday, April 27, 2023 at 12:04:19 GMT+5:30	Requester Region	N. Virginia (us-east-1)
		VPC Peering connection ARN	<a href="#">arn:aws:ec2:us-east-1:605266716064:vpc-peering-connection/pxc-077c8d68576e040fe</a>
		Acceptor VPC	<a href="#">vpc-061218084b7c53cbc</a>
		Acceptor CIDRs	-
		Acceptor Region	Mumbai (ap-south-1)

Below the table, there are tabs for DNS and Route tables, and a DNS settings section with an 'Edit DNS settings' button.

The screenshot shows the AWS VPC Peering Connections page in the ap-south-1 region. A green banner at the top indicates that the peering connection has been established. The main table displays the details of the peering connection:

Details		Info	
Requester owner ID	<a href="#">605356716064</a>	Acceptor owner ID	<a href="#">605266716064</a>
Peering connection ID	<a href="#">pxc-077c8d68576e040fe</a>	Requester VPC	<a href="#">vpc-054d137800daec2c9</a>
Status	<a href="#">Provisioning</a>	Requester CIDR	<a href="#">172.0.0.0/16</a>
Expiration time	-	Requester Region	N. Virginia (us-east-1)
		VPC Peering connection ARN	<a href="#">arn:aws:ec2:ap-south-1:605356716064:vpc-peering-connection/pxc-077c8d68576e040fe</a>
		Acceptor VPC	<a href="#">vpc-061218084b7c53cbc / shvpc1-vpc</a>
		Acceptor CIDRs	<a href="#">10.0.0.0/16</a>
		Acceptor Region	Mumbai (ap-south-1)

Below the table, there are tabs for DNS and Route tables, and a DNS settings section. It also includes sections for Requester VPC and Acceptor VPC settings, both of which have 'Allow requester VPC to resolve DNS of hosts in requester VPC to private IP addresses' options set to 'Disabled'.

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

Screenshot of the AWS VPC Peering Connections page (ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#PeeringConnections). The page shows a table of existing peering connections:

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDR...	Acceptor CIDR...	Requester owner ID	Acceptor owner ID
-	pxc-0a2887d7b6092177	Active	vpc-0458894680ab728d9	vpc-0b8f58224bdfa14 / ...	172.0.0.0/16	10.0.0.0/16	605266716064	605266716064
-	pxc-0772d868576e640fe	Deleted	vpc-0546137800acec9	vpc-06121808407c53dc	-	-	605266716064	605266716064
-	pxc-0d8eb4ba8cb3d1e9b	Failed	vpc-04167649645234f4	vpc-06121808407c53dc	-	-	605266716064	605266716064
-	pxc-03fcfa256cf0e495	Failed	vpc-04167649645234f4	vpc-06121808407c53dc	-	-	605266716064	605266716064
-	pxc-0c161fd5d25eb20	Failed	vpc-091685909c973d1	vpc-06121808407c53dc	-	-	605266716064	605266716064
sh-sh1	pxc-0a92615e41ee87410	Active	vpc-0a56d9b986cc4b40fc / sh...	vpc-0a720452ac50a7c / sh...	10.0.0.0/16	172.0.0.0/16	605266716064	605266716064

The status bar at the top indicates: "Your VPC peering connection (pxc-0a92615e41ee87410 / sh-sh1) has been established. To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables." A "Create peering connection" button is visible.

Screenshot of the AWS VPC Peering Connections page (ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#PeeringConnections). The page shows a table of existing peering connections:

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDR...	Acceptor CIDR...	Requester owner ID	Acceptor owner ID
-	pxc-0772d868576e640fe	Deleted	vpc-0546137800acec9	vpc-06121808407c53dc	-	-	605266716064	605266716064
-	pxc-03fcfa256cf0e495	Failed	vpc-04167649645234f4	vpc-06121808407c53dc	-	-	605266716064	605266716064
-	pxc-0d8eb4ba8cb3d1e9b	Failed	vpc-04167649645234f4	vpc-06121808407c53dc	-	-	605266716064	605266716064
-	pxc-0c161fd5d25eb20	Failed	vpc-091685909c973d1	vpc-06121808407c53dc	-	-	605266716064	605266716064
-	pxc-0a3887d7b6092177	Active	vpc-0458894680ab728d9	vpc-0b8f58224bdfa14 / ...	172.0.0.0/16	10.0.0.0/16	605266716064	605266716064
sh-sh1	pxc-0a92615e41ee87410	Active	vpc-0a56d9b986cc4b40fc / sh...	vpc-0a720452ac50a7c / sh...	10.0.0.0/16	172.0.0.0/16	605266716064	605266716064
sh-sh2	pxc-0b41554646234d8	Active	vpc-0458894680ab728d9	vpc-0a720452ac50a7c / sh...	10.0.0.0/16	169.0.0.0/16	605266716064	605266716064

The status bar at the top indicates: "Your VPC peering connection (pxc-0b41554646234d8 / sh-sh2) has been established. To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables." A "Create peering connection" button is visible.

Your VPC peering connection (pe-077e16d05b0f7e2dfe / sh1-sh2) has been established.

To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. [Info](#)

[Modify my route tables now](#)

**Peering connections (8)** [Info](#)

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDR...	Acceptor CIDRs	Requester owner ID	Acceptor owner ID
-	pe-077e16d05b0f7e2dfe	Deleted	vpc-054c157b000000000000000000000000	vpc-0612180940755chr	-	-	605366716064	605366716064
-	pe-07361f1eda75eb020	Failed	vpc-0916680909a973d1	vpc-0612180840753d0k	-	-	605366716064	605366716064
-	pe-05edeb404b5d1a9b6	Failed	vpc-041676966523d4f4	vpc-0612180840753dc	-	-	605366716064	605366716064
-	pe-02887cd160921177	Active	vpc-04588948067238f9	vpc-0612180840753dh	172.0.0.0/16	10.0.0.0/16	605366716064	605366716064
-	pe-03fcfa26c70d6495	Failed	vpc-041676966523d4f4	vpc-0612180840753dc	-	-	605366716064	605366716064
sh1-sh1	pe-082615e41ee7410	Active	vpc-03565d9866a4b49r	vpc-03720452a3097c	10.0.0.0/16	172.0.0.0/16	605366716064	605366716064
sh1-sh2	pe-08c415464462aa4d0	Active	vpc-03565d9866a4b49r	vpc-03720452a3097c	10.0.0.0/16	169.0.0.0/16	605366716064	605366716064
sh1-sh2	pe-0debb70d097f72dfe	Active	vpc-03720452a3097c	vpc-03720452a3097c	172.0.0.0/16	169.0.0.0/16	605366716064	605366716064

Select a peering connection above

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

## 6) Add security rules in the VPC's NACL which should deny RDP, SSH from the public network

[Edit inbound rules](#)

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
99	SSH (22)	TCP (6)	22	0.0.0.0/0	Deny
98	RDP (3389)	TCP (6)	3389	0.0.0.0/0	Deny
1	All traffic	All	All	0.0.0.0/0	Deny

[Add new rule](#) [Sort by rule number](#)

[Cancel](#) [Preview changes](#) [Save changes](#)

© 2023, Amazon Web Services India Private Limited or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)