

## ASSIGNMENT – DAY 7&amp;8

## PROJECT 1:

VPC peering

Ss1: VPCs list

**Your VPCs (3)**

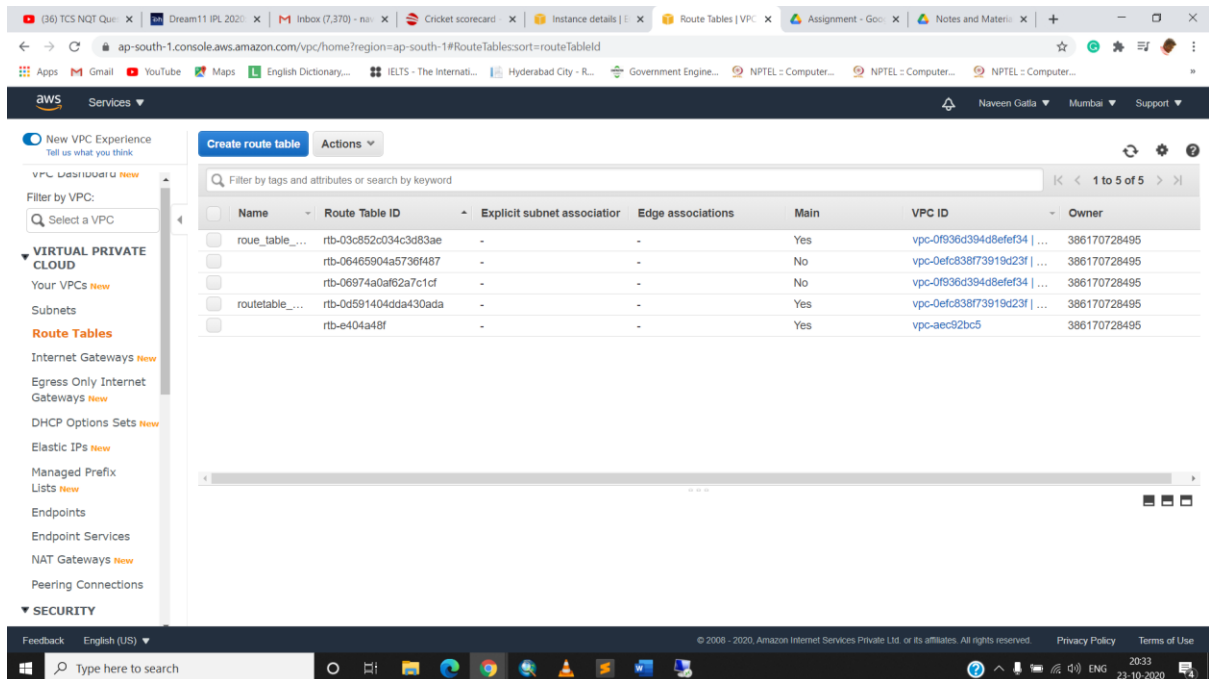
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
-	vpc-aec92bc5	Available	172.31.0.0/16	-
vpc_day7_1	vpc-0f936d394d8ef34	Available	172.19.0.0/16	-
vpc_day7_2	vpc-0efc838f73919d23f	Available	172.16.0.0/16	-

Ss2: igw list

**Internet gateways (3)**

Name	Internet gateway ID	State	VPC ID	Owner
gateway_day7_1	igw-00ee3cccb69996c45	Attached	vpc-0f936d394d8ef34   vpc_day7_1	386170728495
gateway_day7_2	igw-0d54abb6cc728af32	Attached	vpc-0efc838f73919d23f   vpc_day7_2	386170728495
-	igw-3c4cf054	Attached	vpc-aec92bc5	386170728495

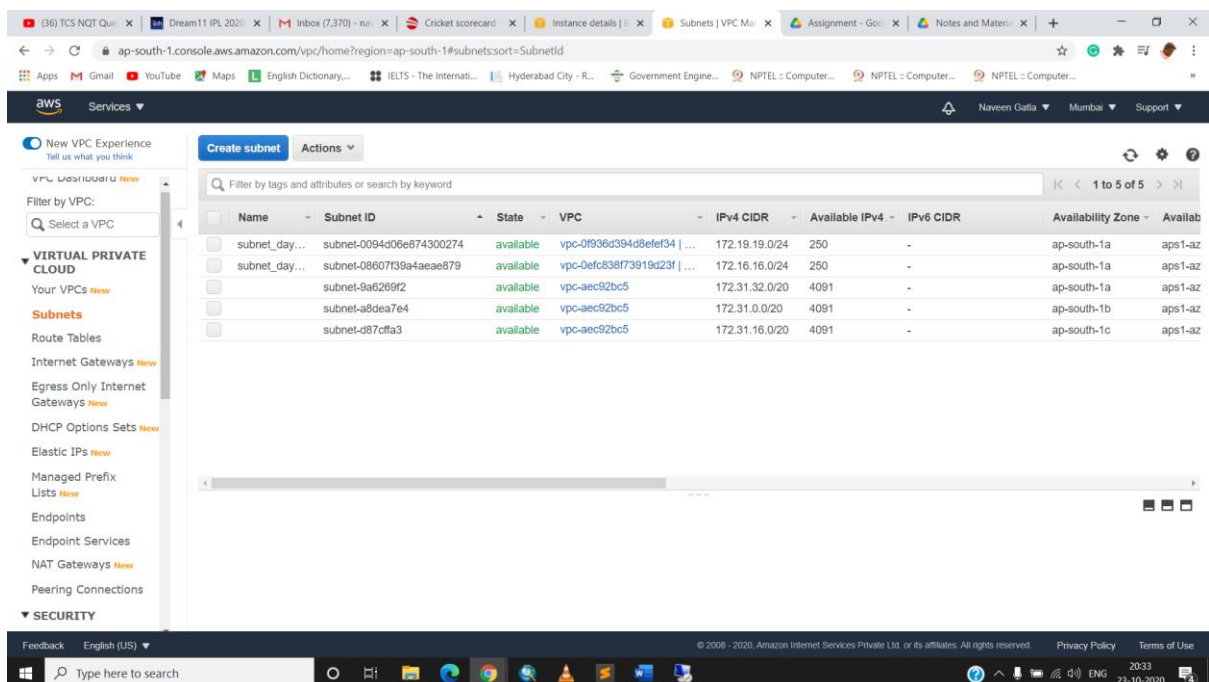
## Ss3: edit route list



Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
route_table_...	rtb-03c852c034c3d83ae	-	-	Yes	vpc-0f936d394d8efef34   ...	386170728495
rtb-06465904a5736f487	-	-	-	No	vpc-0efc838f73919d23f   ...	386170728495
rtb-06974a0af62a7c1cf	-	-	-	No	vpc-0f936d394d8efef34   ...	386170728495
route_table_...	rtb-0d591404dda430ada	-	-	Yes	vpc-0efc838f73919d23f   ...	386170728495
rtb-e404a48f	-	-	-	Yes	vpc-aec92bc5	386170728495

## Ss4: subnet list



Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availab
subnet_day...	subnet-0094d06e874300274	available	vpc-0f936d394d8efef34   ...	172.19.19.0/24	250	-	ap-south-1a	aps1-az
subnet_day...	subnet-08607f39a4aeae879	available	vpc-0efc838f73919d23f   ...	172.16.16.0/24	250	-	ap-south-1a	aps1-az
subnet-9a6269f2	-	available	vpc-aec92bc5	172.31.32.0/20	4091	-	ap-south-1a	aps1-az
subnet-a8dea7e4	-	available	vpc-aec92bc5	172.31.0.0/20	4091	-	ap-south-1b	aps1-az
subnet-d97cfa3	-	available	vpc-aec92bc5	172.31.16.0/20	4091	-	ap-south-1c	aps1-az

## Ss5: instance details

The image displays two screenshots of the AWS Management Console, specifically the EC2 Instance Details page. Both screenshots show the 'Instance summary' for a running EC2 instance in the 'ap-south-1' region.

**Top Screenshot: Instance i-0c634cff577a96eb5 (VPC day7\_2)**

Instance ID	Public IPv4 address	Private IPv4 address
i-0c634cff577a96eb5 (VPC day7_2)	13.233.132.118   <a href="#">open address</a>	172.16.16.115

Instance state: **Running**

Instance type: t2.micro

IAM Role: -

Subnet ID: subnet-08607f39a4ae879 (subnet\_day7\_2)

VPC ID: vpc-0efc838f73919d23f (vpc\_day7\_2)

Private IPv4 DNS: ip-172-16-16-115.ap-south-1.compute.internal

**AWS Compute Optimizer**  
Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)

**Bottom Screenshot: Instance i-0da0992eec593c565 (For VPC day7)**

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0da0992eec593c565 (For VPC day7)	15.206.168.116   <a href="#">open address</a>	172.19.19.230

Instance state: **Running**

Instance type: t2.micro

IAM Role: -

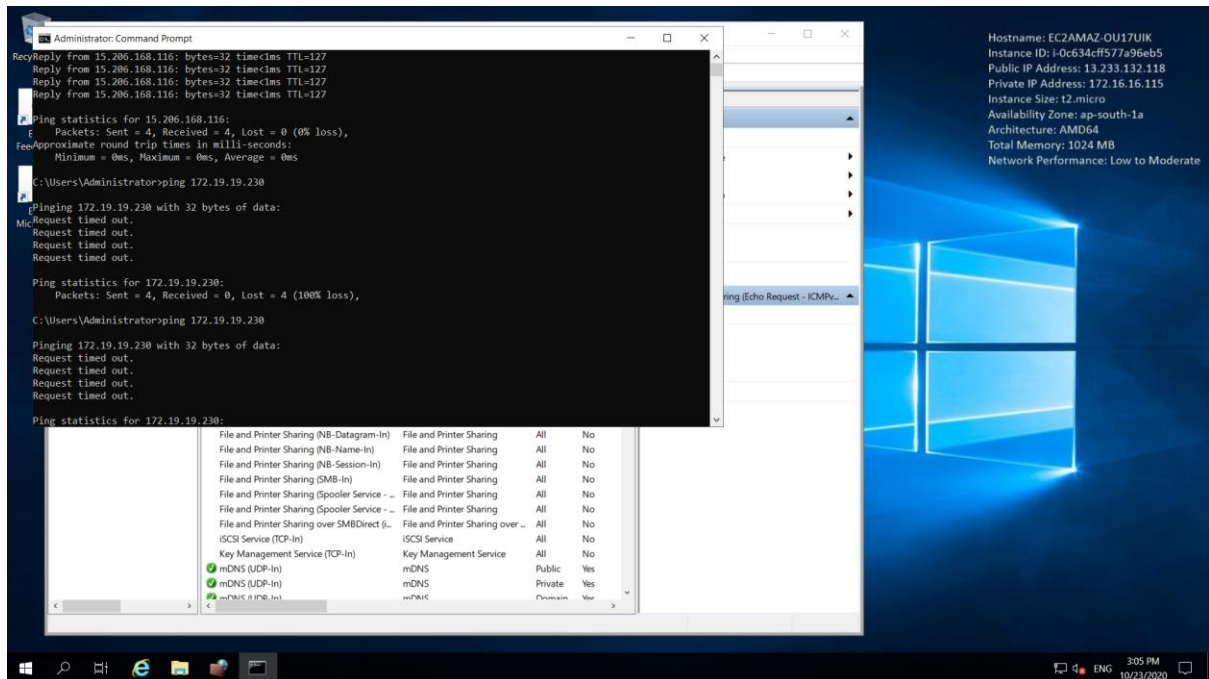
Subnet ID: subnet-0094d06e874300274 (subnet\_day7\_1)

VPC ID: vpc-0f936d394d8efef34 (vpc\_day7\_1)

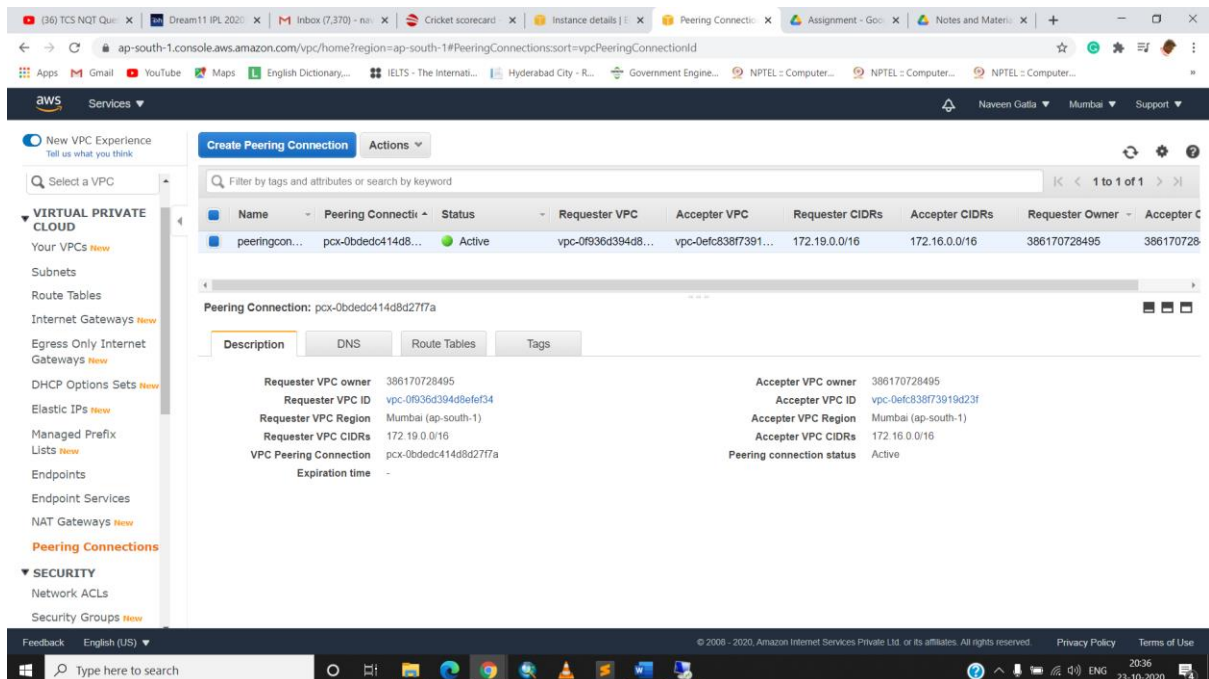
Private IPv4 DNS: ip-172-19-19-230.ap-south-1.compute.internal

**AWS Compute Optimizer**  
Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)

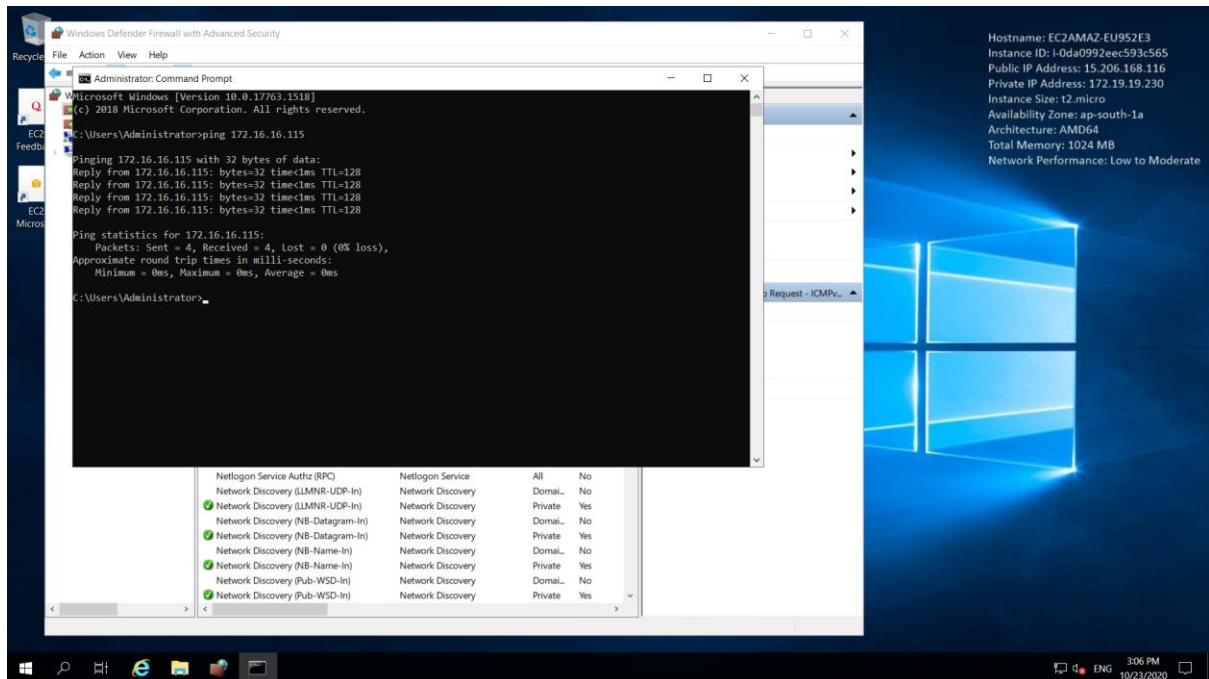
## Ss6: success public, rto private IP



## Ss7: peering with req and acceptor



## Ss8: success for private



## Project 2:

### IAM

Task 1: Creating users without permissions-IAM password policy check.

Ss1: user summary with all tab information

The screenshot shows the AWS IAM console 'Change password' page for user 'user\_1'. The page is titled 'You must change your password to continue'. It displays the AWS account ID '386170728495' and the IAM user name 'user\_1'. There are three input fields: 'Old password', 'New password', and 'Retype new password'. A 'Confirm password change' button is at the bottom. A link 'Steps to using root user email' is also visible. The page footer shows the language set to 'English' and the copyright notice 'Terms of Use Privacy Policy © 1996-2020, Amazon Web Services, Inc. or its affiliates.'

User1 With no permissions.

The screenshot shows the AWS Management Console 'EC2 Dashboard' for user 'user\_1'. The dashboard displays a 'Welcome to the new EC2 console!' message. The 'Resources' section shows a table of EC2 resources in the Asia Pacific (Mumbai) Region, including Instances, Elastic IPs, Dedicated Hosts, Snapshots, Volumes, Key pairs, Security groups, Placement groups, Load balancers, and Running instances. All resources show an 'API Error' status. The 'Account attributes' section lists various settings like Supported platforms, Default VPC, Settings, EBS encryption, Zones, Default credit specification, and Console experiments. The 'Explore AWS' section provides information about Launch Custom AMIs with Fast Snapshot Restore (FSR). The dashboard also includes a 'Launch instance' button and a 'Service health' section.

## Task 2: Creating users without the IAM password policy.

### Ss2: user summary with all tab information

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area displays the 'Summary' page for 'user\_2'. It shows the User ARN as 'am:aws.iam::386170728495:user/user\_2', Path as '/', and Creation time as '2020-10-23 20:51 UTC+0530'. Below this, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing 'Permissions policies' with a message: 'Get started with permissions. This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. Learn more'. There are buttons for 'Add permissions' and 'Add inline policy'. A 'Permissions boundary (not set)' section is also visible. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 20:52 on 23-10-2020.

## Task 3: Create a user with S3 full access

### Ss3: User summary

The screenshot shows the AWS IAM console interface for 'user\_3'. The left sidebar is the same as in the previous screenshot. The main content area displays the 'Summary' page for 'user\_3'. It shows the User ARN as 'am:aws.iam::386170728495:user/user\_3', Path as '/', and Creation time as '2020-10-23 20:53 UTC+0530'. Below this, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing 'Permissions policies (1 policy applied)'. There is a button for 'Add permissions' and a link for 'Add inline policy'. A table lists the attached policies: 'Attached directly' with 'AmazonS3FullAccess' (AWS managed policy). A 'Permissions boundary (not set)' section is also visible. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 20:53 on 23-10-2020.



## Task4: Create a group with ec2 full access

### Ss4: group summary

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Groups, Users, Roles, Policies, etc. The main content area displays the 'Summary' tab for the 'jakeballs' group. The summary includes the Group ARN (am:aws.iam::386170728495:group/jakeballs), the number of users (3), the path (/), and the creation time (2020-10-23 20:55 UTC+0530). Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Permissions' tab is active, showing 'Managed Policies' and 'Inline Policies'. Under 'Managed Policies', it lists 'AmazonEC2FullAccess' with actions 'Show Policy', 'Detach Policy', and 'Simulate Policy'.

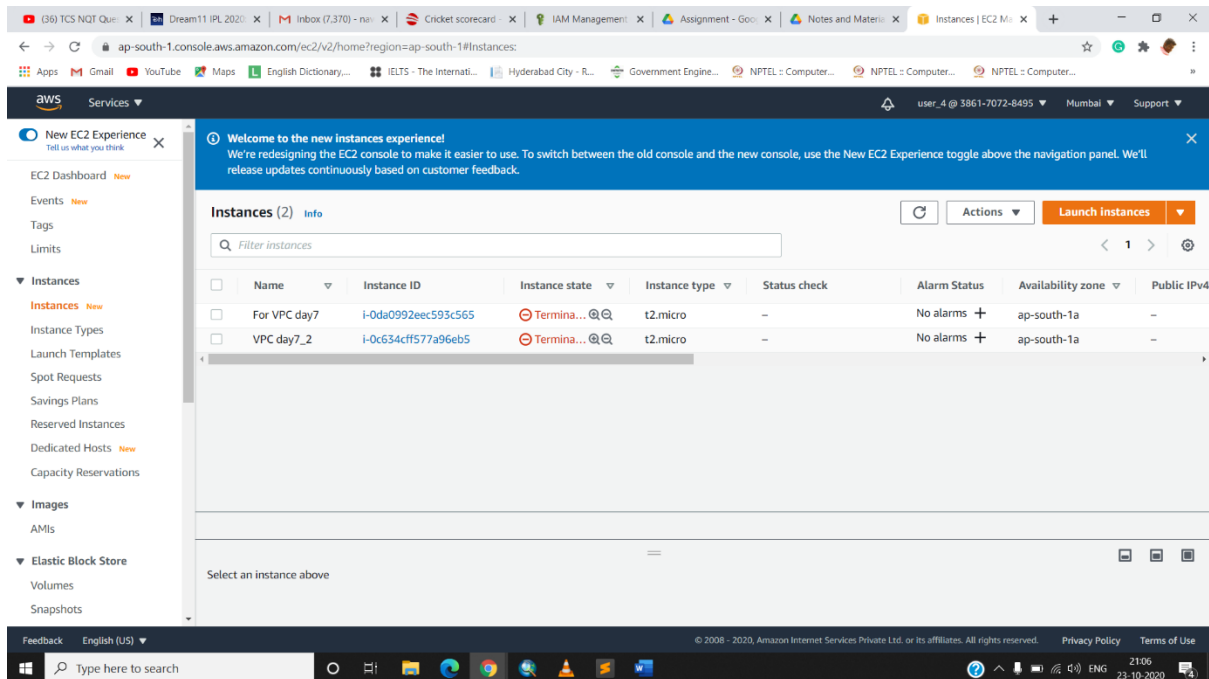
## Task 5: Add user to a group and check if user policy and the group policy is reflecting on the user

### Ss5: user summary with permissions

The screenshot shows the AWS IAM console interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu. The main content area displays the 'Summary' tab for the 'user\_4' user. The summary includes the User ARN (am:aws.iam::386170728495:user/user\_4), the path (/), and the creation time (2020-10-23 21:02 UTC+0530). Below the summary, there are tabs for 'Permissions', 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing 'Permissions policies (2 policies applied)'. It lists 'AmazonS3FullAccess' and 'AmazonEC2FullAccess' as attached policies. The 'Groups (1)' tab is also visible, showing the 'jakeballs' group.

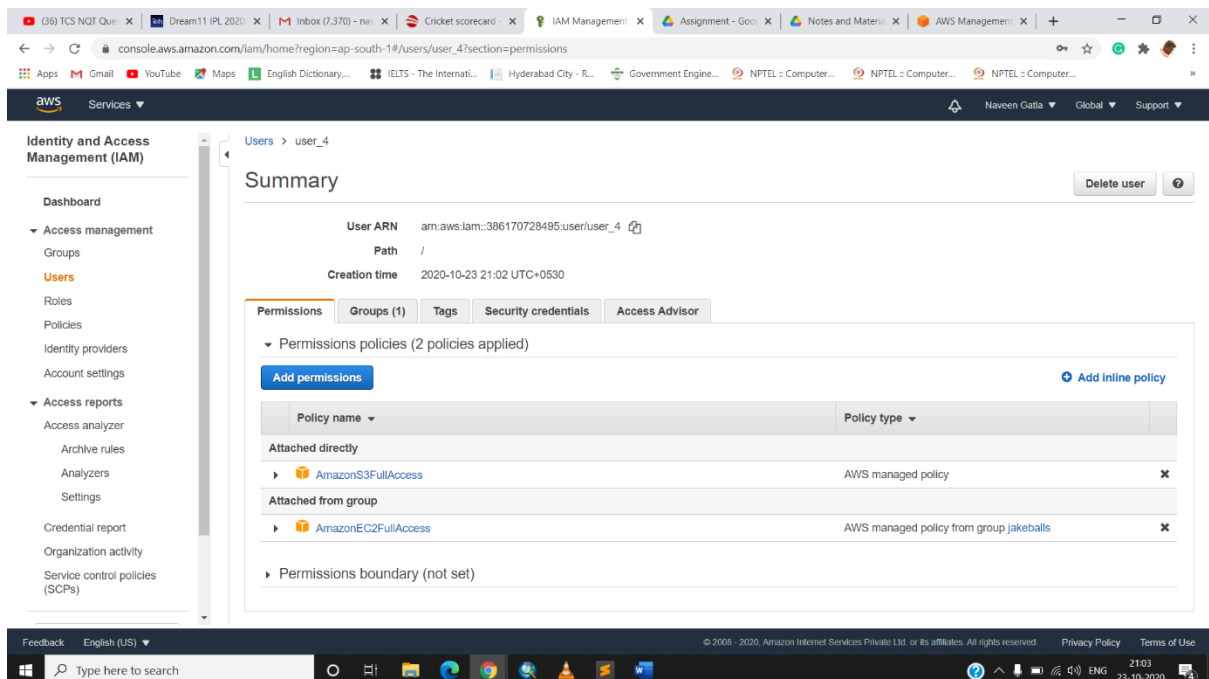


## Ss6: login as this user show that this policy is in effect



## Task 6: Copy policies from the existing user

## Ss7: attach user summary of the user from which you create a new user



## Ss8: login as this user show that this policy is in effect

The screenshot shows the AWS Management Console for the 'ap-south-1' region. The left sidebar contains navigation options like 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances', 'Images', and 'Elastic Block Store'. The main content area shows the 'Instances (2)' page with a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv4
For VPC day7	i-0da0992e0c593c565	Terminated	t2.micro	—	No alarms	ap-south-1a	—
VPC day7_2	i-0c634c0f577a96eb5	Terminated	t2.micro	—	No alarms	ap-south-1a	—

## Task 7: Add user to a group in the process of creating a user

The screenshot shows the 'Add user' page in the AWS IAM console. The 'Set permissions' section has three options: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly'. The 'Add user to group' option is selected. Below this, a table shows the group 'jakeballs' with the attached policy 'AmazonEC2FullAccess'.

Group	Attached policies
<input checked="" type="checkbox"/> jakeballs	AmazonEC2FullAccess

## Task8: setting a password policy

### Ss9: password policy screen

**Set password policy**

A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. [Learn more](#)

**Select your account password policy requirements:**

- ☒ Enforce minimum password length
 

8 characters
- ☒ Require at least one uppercase letter from Latin alphabet (A-Z)
- ☒ Require at least one lowercase letter from Latin alphabet (a-z)
- ☒ Require at least one number
- ☒ Require at least one non-alphanumeric character (! @ # \$ % ^ & \* ( ) \_ + = [ ] { } | ' )
- ☒ Enable password expiration
 

Expire passwords in 90 day(s)
- ☒ Password expiration requires administrator reset
- ☒ Allow users to change their own password
- ☒ Prevent password reuse
 

Remember 5 password(s)

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

### Ss10: login as the user and show password incompatibility error

**User name\*** RAVI

[Add another user](#)

**Select AWS access type**

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

**Access type\***

- ☒ **Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

**Console password\***

- ☐ Autogenerated password
- ☒ Custom password

\*\*\*\*\*

☐ Show password

The password does not conform to the account password policy:

- it must contain at least 15 characters

\* Required

[Cancel](#) [Next: Permissions](#)

## Task 9: Enabling MFA and using an MFA device

### Ss11: enable MFA

The screenshot shows the AWS IAM console 'Your Security Credentials' page. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Groups, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, and Service control policies (SCPs). The main content area is titled 'Your Security Credentials' and includes instructions on managing credentials. It features expandable sections for Password, Multi-factor authentication (MFA), Access keys, CloudFront key pairs, X.509 certificate, and Account identifiers. The MFA section is expanded, showing a table with one entry: a Virtual device with serial number 'arn:aws:iam::386170728495:mfa/root-account-mfa-device' and a 'Manage' link. The bottom of the page shows the Windows taskbar with the time 21:13 on 23-10-2020.

### Ss12: login screen for MFA

The screenshot shows the AWS Multi-factor authentication login screen. The page has the AWS logo at the top left. The main heading is 'Multi-factor authentication'. Below it, text states: 'Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.' The email address 'naveengata96@gmail.com' is displayed. There is a text input field for the 'MFA code' and a blue 'Submit' button. Below the button are links for 'Troubleshoot MFA' and 'Cancel'. On the right side, there is a large graphic with the text 'Migrate with AWS' and 'Reduce cost and gain business agility', along with a 'START YOUR JOURNEY' button and a diagram of interconnected cubes and gears. At the bottom, there is a section titled 'About Amazon.com Sign In' with a paragraph of text. The Windows taskbar at the bottom shows the time 21:14 on 23-10-2020.