

PROJECT 1:

VPC peering

Ss1: VPCs list

Your VPCs (3) Info

Filter VPCs

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	vpc2	vpc-095edde339592eabd	Available	172.16.0.0/16	-
<input type="checkbox"/>	vpc1	vpc-00290035555412e7c	Available	172.19.0.0/16	-
<input type="checkbox"/>	-	vpc-b62083dd	Available	172.31.0.0/16	-

Select a VPC above

Ss2: igw list

Internet gateways (3) Info

Filter internet gateways

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input type="checkbox"/>	igw2	igw-0cc71565bc8580b77	Attached	vpc-095edde339592eabd vpc2
<input type="checkbox"/>	igw1	igw-0e365325c84fd5c49	Attached	vpc-00290035555412e7c vpc1
<input type="checkbox"/>	-	igw-6b216d03	Attached	vpc-b62083dd

Select an internet gateway above

Ss3: edit route list

Learn with LetsUpgrade - Online | Assignment - Google Drive | Route Tables | VPC Management | +

amazon.com

Services

New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs **New**

Subnets

Route Tables

Internet Gateways **New**

Egress Only Internet Gateways **New**

DHCP Options Sets **New**

Elastic IPs **New**

Managed Prefix Lists **New**

Endpoints

Endpoint Services

NAT Gateways **New**

Create route table Actions

Filter by tags and attributes or search by keyword

1 to 5 of 5

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
	rtb-04d4c265b20433524	-	-	No	vpc-095edde339592eabd...
route1	rtb-053c5f640020dda4e	-	-	Yes	vpc-00290035555412e7c...
route2	rtb-06d498950d0650f81	-	-	Yes	vpc-095edde339592eabd...

Route Table: rtb-053c5f640020dda4e

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
172.19.0.0/16	local	active	No
0.0.0.0/0	igw-0e365325c84fd5c49	active	No
172.16.0.0/16	pcx-0bed46cdec7842b4f	active	No

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

Learn with LetsUpgrade - Online | Assignment - Google Drive | Route Tables | VPC Management | +

amazon.com

Services

New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs **New**

Subnets

Route Tables

Internet Gateways **New**

Egress Only Internet Gateways **New**

DHCP Options Sets **New**

Elastic IPs **New**

Managed Prefix Lists **New**

Endpoints

Endpoint Services

NAT Gateways **New**

Create route table Actions

Filter by tags and attributes or search by keyword

1 to 5 of 5

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
	rtb-04d4c265b20433524	-	-	No	vpc-095edde339592eabd...
route1	rtb-053c5f640020dda4e	-	-	Yes	vpc-00290035555412e7c...
route2	rtb-06d498950d0650f81	-	-	Yes	vpc-095edde339592eabd...

Route Table: rtb-06d498950d0650f81

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

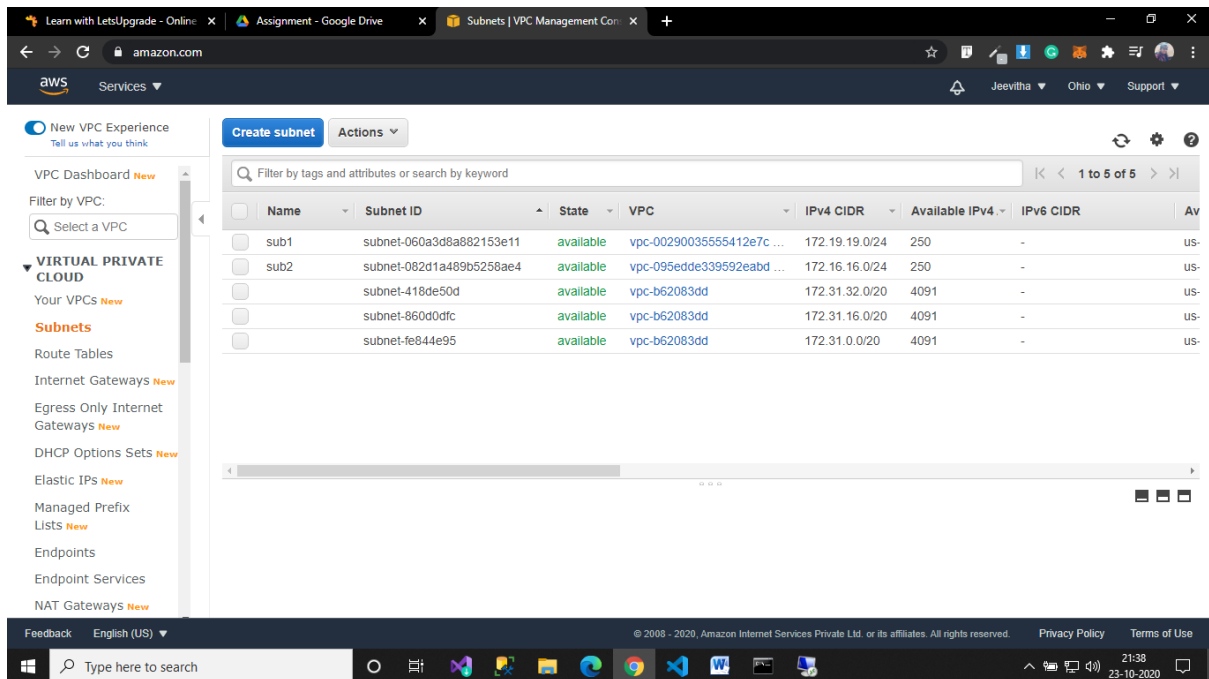
Destination	Target	Status	Propagated
172.16.0.0/16	local	active	No
0.0.0.0/0	igw-0cc71565bc8580b77	active	No
172.19.0.0/16	pcx-0bed46cdec7842b4f	active	No

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

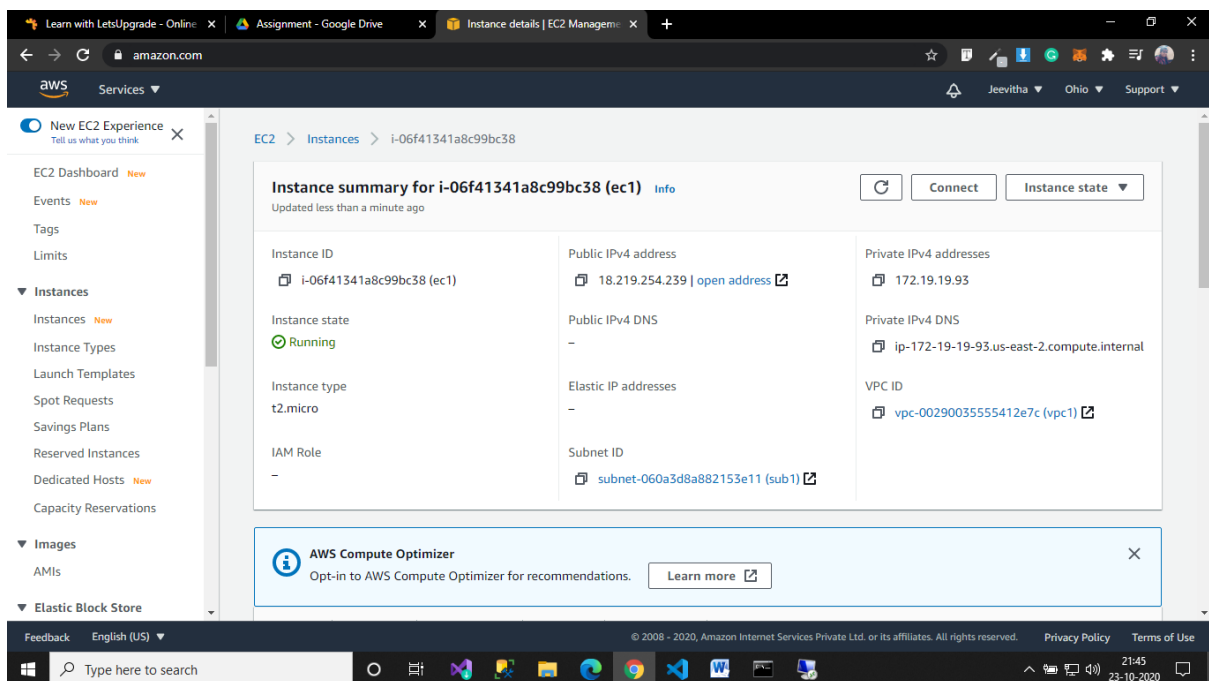
Ss4: subnet list



The screenshot shows the AWS Management Console interface for the 'Subnets | VPC Management Console'. The left sidebar contains the 'VIRTUAL PRIVATE CLOUD' section with options like 'Your VPCs', 'Subnets', 'Route Tables', 'Internet Gateways', 'Egress Only Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Managed Prefix Lists', 'Endpoints', 'Endpoint Services', and 'NAT Gateways'. The main content area displays a table of subnets with columns: Name, Subnet ID, State, VPC, IPv4 CIDR, Available IPv4, IPv6 CIDR, and Availability Zone. The table lists five subnets, all in an 'available' state, associated with VPC 'vpc-00290035555412e7c'.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone
sub1	subnet-060a3d8a882153e11	available	vpc-00290035555412e7c	172.19.19.0/24	250	-	us-east-2a
sub2	subnet-082d1a489b5258ae4	available	vpc-095edde339592eabd	172.16.16.0/24	250	-	us-east-2a
	subnet-418de50d	available	vpc-b62083dd	172.31.32.0/20	4091	-	us-east-2a
	subnet-860d0dfc	available	vpc-b62083dd	172.31.16.0/20	4091	-	us-east-2a
	subnet-fe844e95	available	vpc-b62083dd	172.31.0.0/20	4091	-	us-east-2a

Ss5: instance details



The screenshot shows the 'Instance details | EC2 Management Console' page for instance 'i-06f41341a8c99bc38'. The left sidebar shows the 'EC2 Dashboard' with sections for 'Events', 'Tags', 'Limits', 'Instances', 'Images', and 'Elastic Block Store'. The main content area displays the 'Instance summary for i-06f41341a8c99bc38 (ec1)'. The instance is in a 'Running' state, of type 't2.micro', and has an IAM Role of '-'. It is associated with Subnet ID 'subnet-060a3d8a882153e11 (sub1)'. The summary also shows the Public IPv4 address '18.219.254.239', Private IPv4 address '172.19.19.93', and VPC ID 'vpc-00290035555412e7c (vpc1)'. An 'AWS Compute Optimizer' banner is visible at the bottom.

Instance ID	Public IPv4 address	Private IPv4 addresses
i-06f41341a8c99bc38 (ec1)	18.219.254.239 open address	172.19.19.93

Instance state	Public IPv4 DNS	Private IPv4 DNS
Running	-	ip-172-19-19-93.us-east-2.compute.internal

Instance type	Elastic IP addresses	VPC ID
t2.micro	-	vpc-00290035555412e7c (vpc1)

IAM Role	Subnet ID
-	subnet-060a3d8a882153e11 (sub1)

Learn with LetsUpgrade - Online x Assignment - Google Drive x Instance details | EC2 Managem x +

amazon.com

Services

New EC2 Experience Tell us what you think

EC2 Dashboard **New**

Events **New**

Tags

Limits

▼ Instances

Instances **New**

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts **New**

Capacity Reservations

▼ Images

AMIs

▼ Elastic Block Store

EC2 > Instances > i-004f3e13ec11abbcbb

Instance summary for i-004f3e13ec11abbcbb (ec2) Info

Updated less than a minute ago

Instance ID: i-004f3e13ec11abbcbb (ec2)

Public IPv4 address: 18.191.245.140 | [open address](#)

Private IPv4 addresses: 172.16.16.83

Instance state: **Running**

Public IPv4 DNS: -

Private IPv4 DNS: ip-172-16-16-83.us-east-2.compute.internal

Instance type: t2.micro

Elastic IP addresses: -

VPC ID: vpc-095edde339592eabd (vpc2)

IAM Role: -

Subnet ID: subnet-082d1a489b5258ae4 (sub2)

AWS Compute Optimizer

Loading Compute Optimizer recommendations...

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

21:44 23-10-2020

Ss6: success public, rto private IP

Recycle Bin Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 18.191.245.140

Pinging 18.191.245.140 with 32 bytes of data:
Reply from 18.191.245.140: bytes=32 time<1ms TTL=127
Reply from 18.191.245.140: bytes=32 time<1ms TTL=127
Reply from 18.191.245.140: bytes=32 time<1ms TTL=127
Reply from 18.191.245.140: bytes=32 time<1ms TTL=127

EC2 Feedback

EC2 Micros... Ping statistics for 18.191.245.140:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 172.16.16.83

Pinging 172.16.16.83 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.16.83:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 172.16.16.83

Pinging 172.16.16.83 with 32 bytes of data:

Hostname: EC2AMAZ-EAOP97F
Instance ID: i-06f41341a8c99bc38
Public IP Address: 18.219.254.239
Private IP Address: 172.19.19.93
Instance Size: t2.micro
Availability Zone: us-east-2c
Architecture: AMD64
Total Memory: 1024 MB
Network Performance: Low to Moderate

4:02 PM 10/23/2020

Ss7: peering with req and acceptor

The screenshot shows the AWS Management Console interface. On the left, the navigation menu is visible with categories like 'New VPC Experience', 'SECURITY', and 'VIRTUAL PRIVATE'. The main content area displays the 'Peering Connections' page. A table lists the peering connections, with one entry 'mypeer1' in an 'Active' state. Below the table, the details for the selected peering connection 'pcx-0bed46cdec7842b4f' are shown, including tabs for Description, DNS, Route Tables, and Tags. The details section provides information about the Requester VPC and the Acceptor VPC, including their IDs, regions, and owners.

Name	Peering Connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs	Requester VPC ID
mypeer1	pcx-0bed46cdec7...	Active	vpc-095edde3395...	vpc-00290035555...	172.16.0.0/16	172.19.0.0/16	409578...

Peering Connection: pcx-0bed46cdec7842b4f

Field	Value
Requester VPC owner	409578114950
Requester VPC ID	vpc-095edde339592eabd
Requester VPC Region	Ohio (us-east-2)
Acceptor VPC owner	409578114950
Acceptor VPC ID	vpc-00290035555412e7c
Acceptor VPC Region	Ohio (us-east-2)

Ss8: success for private

The screenshot shows a Windows desktop environment. A command prompt window is open, displaying the results of a ping command to the IP address 172.16.16.83. The output shows that the ping was successful, with 4 packets sent and 4 received, resulting in 0% loss. The taskbar at the bottom shows several icons, including the Start button, a search bar, and various application icons. The system tray in the bottom right corner displays the date and time as 4:02 PM on 10/23/2020.

```
Request timed out.

Ping statistics for 172.16.16.83:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 172.16.16.83

Pinging 172.16.16.83 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

C:\Users\Administrator>ping 172.16.16.83

Ping statistics for 172.16.16.83:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Administrator>ping 172.16.16.83

Pinging 172.16.16.83 with 32 bytes of data:
Reply from 172.16.16.83: bytes=32 time<1ms TTL=128
Reply from 172.16.16.83: bytes=32 time<1ms TTL=128
Reply from 172.16.16.83: bytes=32 time<1ms TTL=128
Reply from 172.16.16.83: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.16.83:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>
```

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 interface. The left sidebar contains the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Users, Roles, Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, and Organization activity. The main content area displays the 'Summary' page for user 'sharve'. The user's details include: User ARN (arn:aws:iam::409578114950:user/sharve), Path (/), and Creation time (2020-10-22 21:52 UTC+0530). Below the summary, there are tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor. The 'Permissions' tab is active, showing 'Permissions policies (1 policy applied)'. A table lists the policy 'IAMUserChangePassword' as an 'AWS managed policy'. There is also a section for 'Permissions boundary (not set)'.

Task 2: Creating users without the IAM password policy.

Ss2: user summary with all tab information

The screenshot shows the AWS IAM console interface for user 'anu'. The left sidebar is the same as in the previous screenshot. The main content area displays the 'Summary' page for user 'anu'. The user's details include: User ARN (arn:aws:iam::409578114950:user/anu), Path (/), and Creation time (2020-10-22 23:51 UTC+0530). Below the summary, there are tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor. The 'Permissions' tab is active, showing 'Permissions policies'. A blue box with an information icon contains the text 'Get started with permissions' and '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 is also a section for 'Permissions boundary (not set)'.

Task 3: Create a user with S3 full access

Ss3: User 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, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, and Organization activity. The main content area displays the 'Summary' for a user named 'janu'. The user's details are: User ARN: am:aws:iam::409578114950:user/janu, Path: /, and Creation time: 2020-10-22 23:54 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)'. A table lists the attached policies: 'AmazonS3FullAccess' (AWS managed policy). There is also a section for 'Permissions boundary (not set)'.

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy

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. The main content area displays the 'Summary' for a group named 'Testing'. The group's details are: Group ARN: am:aws:iam::409578114950:group/Testing, Users (in this group): 4, Path: /, and Creation Time: 2020-10-22 22:53 UTC+0530. Below this, there are tabs for Users, Permissions, and Access Advisor. The 'Permissions' tab is active, showing 'Managed Policies'. A table lists the attached policies: 'AmazonEC2FullAccess'. There is also a section for 'Inline Policies'.

Policy Name	Actions
AmazonEC2FullAccess	Show Policy Detach Policy Simulate Policy

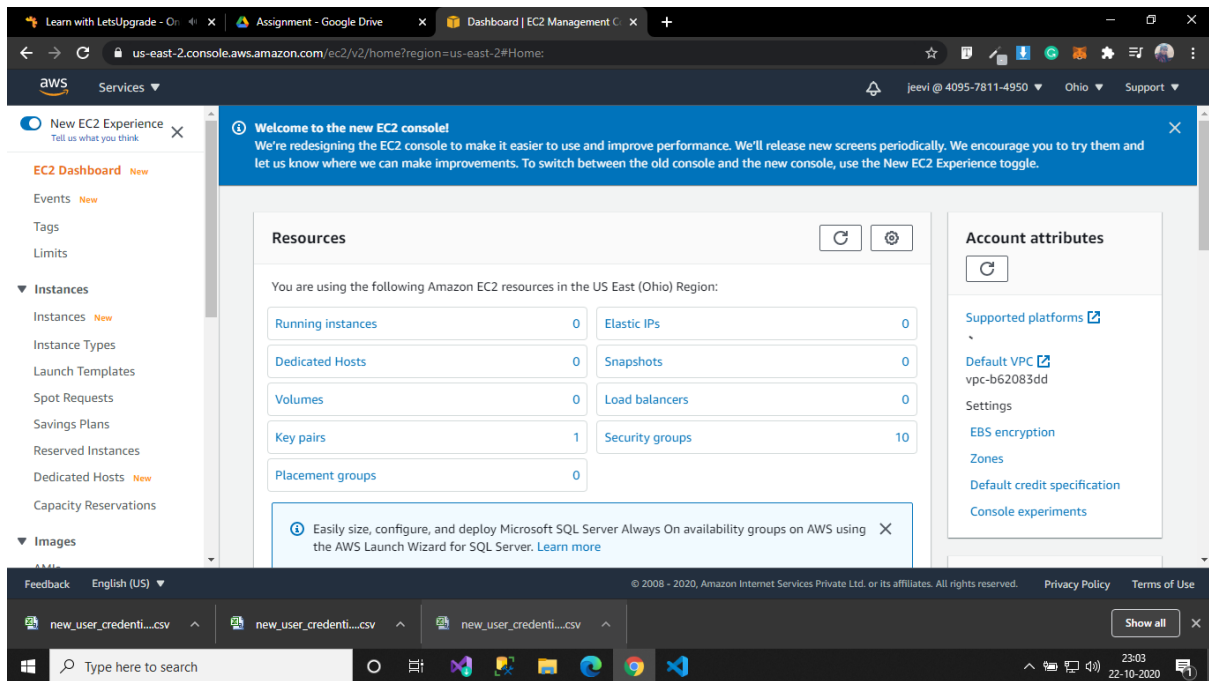
Task 5: Add user to a group and check if user policy and the group policy is reflecting on the user

Ss5: user summary with permissions

The screenshot shows the AWS IAM console 'Summary' page for a user. The user's ARN is 'arn:aws:iam::409578114950:user/jeevi', the path is '/', and the creation time is '2020-10-22 22:44 UTC+0530'. The 'Permissions' tab is selected, showing 'Permissions policies (2 policies applied)'. There are two policies: 'AmazonS3FullAccess' (AWS managed policy) and 'AmazonEC2FullAccess' (AWS managed policy from group 'Testing'). The 'Add permissions' button is visible. The left sidebar shows the 'Users' link under 'Access management'. The bottom of the screen shows a Windows taskbar with various application icons.

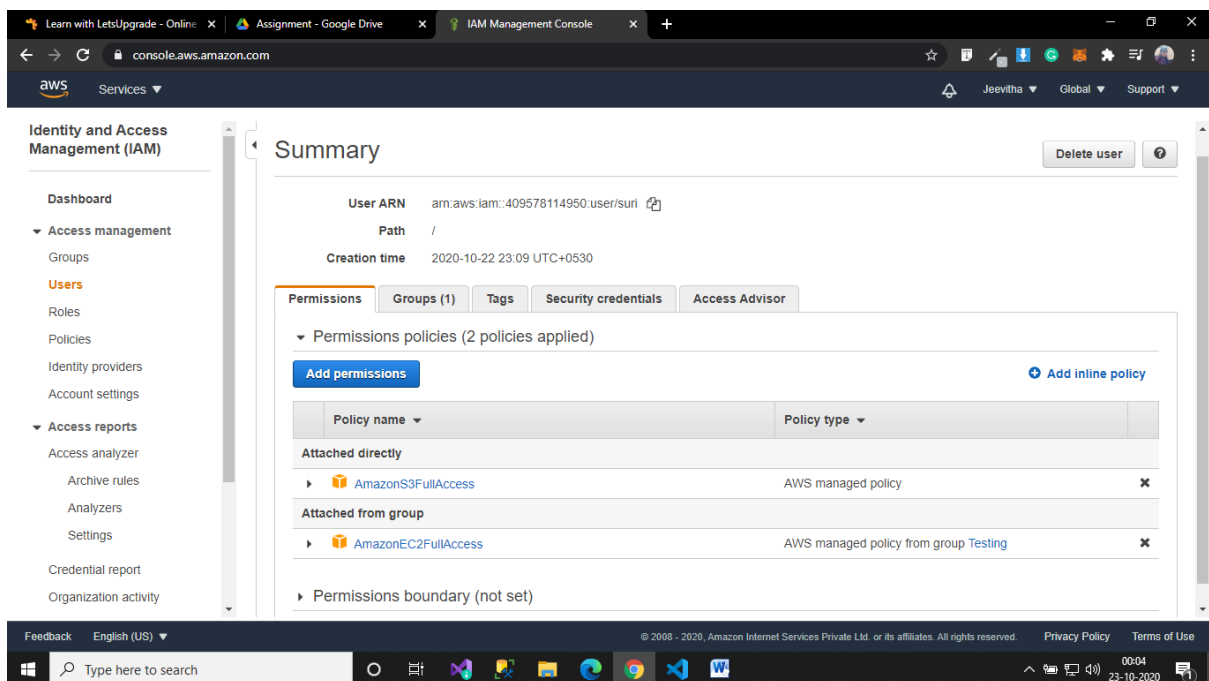
Ss6: login as this user show that this policy is in effect

The screenshot shows the AWS S3 console. A message at the top states: 'We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. Switch to the new console.' Below this, the 'S3 buckets' section shows a search bar and a dropdown for 'All access types'. A large blue box in the center says 'You do not have any buckets. Here is how to get started with Amazon S3.' The left sidebar shows the 'Buckets' link. The bottom of the screen shows a Windows taskbar with various application icons.

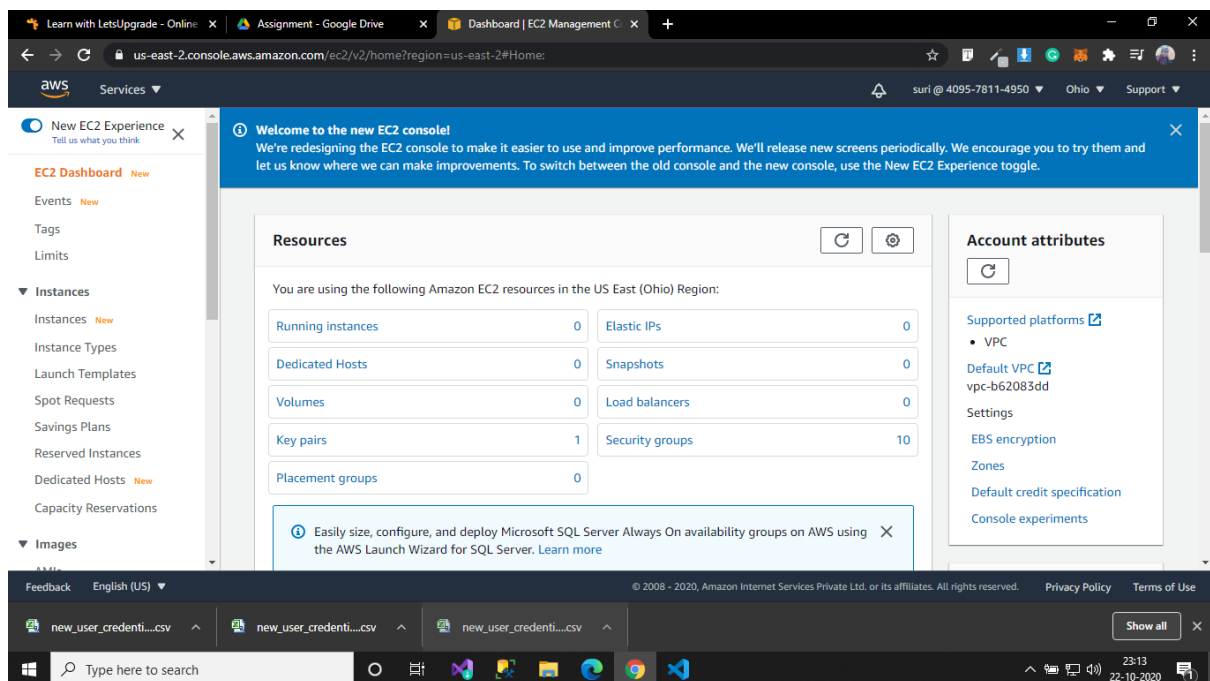
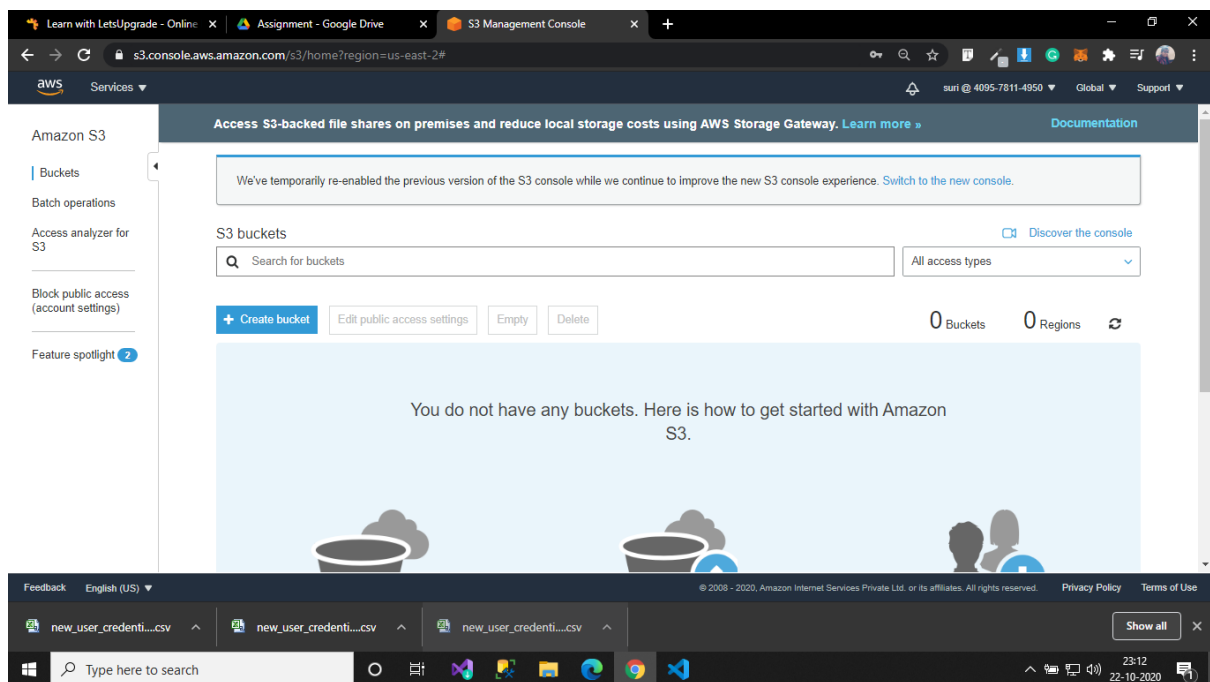


Task 6: Copy policies from the existing user

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



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

Task 8: setting a password policy

The screenshot shows the 'Set password policy' page in the AWS IAM console. The page title is 'Set password policy'. Below the title, there is a description: 'A password policy is a set of rules that define complexity requirements and mandatory rotation periods for your IAM users' passwords. [Learn more](#)'. The section 'Select your account password policy requirements:' contains several checkboxes and input fields. The 'Enforce minimum password length' checkbox is checked, with a value of '9' characters. Other checked requirements include: '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 (!@#\$%^&*()_+-=[]{}|')', and 'Enable password expiration'. The 'Expire passwords in' field is set to '90' day(s). The 'Allow users to change their own password' checkbox is also checked. At the bottom right, there are 'Cancel' and 'Save changes' buttons.

Ss9: password policy screen

The screenshot shows the 'Password policy' screen in the AWS IAM console. A green notification box at the top states 'Password policy updated.' with a close button. Below this, there is a description: 'A password policy is a set of rules that define the type of password an IAM user can set. [Learn more](#)'. The section 'Password policy' states 'This AWS account uses a password policy'. A list of requirements is displayed: 'Minimum password length is 9 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 (!@#\$%^&*()_+-=[]{}|')', 'Password expires in 90 day(s)', 'Allow users to change their own password', and 'Remember last 2 password(s) and prevent reuse'. At the bottom, there are 'Change password policy' and 'Delete password policy' buttons. The left sidebar shows the 'Identity and Access Management (IAM)' menu with 'Account settings' highlighted. The bottom of the screen shows the Windows taskbar with the time 23:27 on 22-10-2020.

Ss10: login as the user and show password incompatibility error

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 a special character and a digit

Require password reset ☒ User must create a new password at next sign-in

* Required

Cancel Next: Permissions

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

new_user_credenti...csv new_user_credenti...csv new_user_credenti...csv Show all

Type here to search

23:28 22-10-2020

Task 9: Enabling MFA and using an MFA device

Ss11: enable MFA

Set up virtual MFA device

✓ You have successfully assigned virtual MFA
This virtual MFA will be required during sign-in.

Close

Use MFA to increase the security of your AWS environments. Signing in to MFA-protected accounts requires a user name, password, and an authentication code from an MFA device.

Device type	Serial number	Actions
Virtual	arn:aws:iam::409578114950:mfa/root-account-mfa-device	Manage

Access keys (access key ID and secret access key)

CloudFront key pairs

X.509 certificate

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

new_user_credenti...csv new_user_credenti...csv new_user_credenti...csv Show all

Type here to search

23:39 22-10-2020

Ss12: login screen for MFA

Learn with LetsUpgrade - O... X | Assignment - Google Drive X | Amazon Web Services Sign-In X +

signin.aws.amazon.com

aws

Multi-factor authentication

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.

Email address: gytha98@gmail.com

MFA code

Submit

[Troubleshoot MFA](#)

[Cancel](#)

Amazon Aurora Serverless

Automatically starts, scales, and shuts down your database

aws

new_user_credenti...csv ^ new_user_credenti...csv ^ new_user_credenti...csv ^ Show all X

Type here to search

23:42 22-10-2020