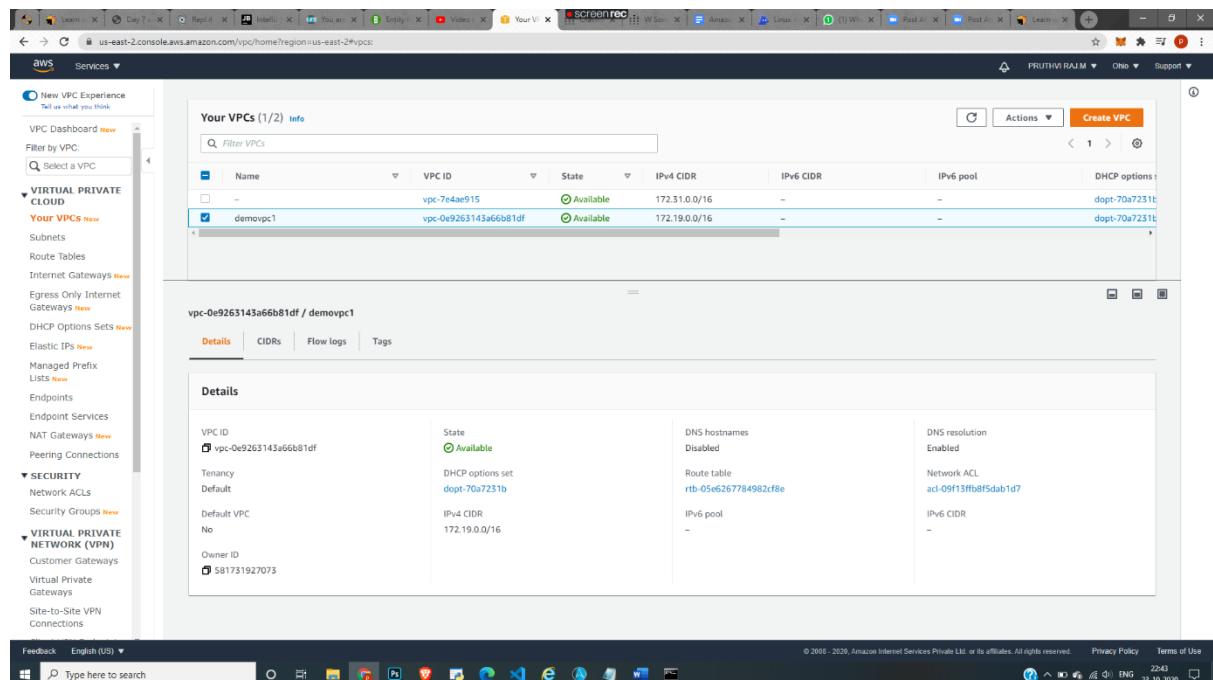


# AWS ASSIGNMENT 7 AND 8

## PROJECT 1: VPC PEERING

### TASK 1: VPCS LIST



Your VPCs (1/2) Info

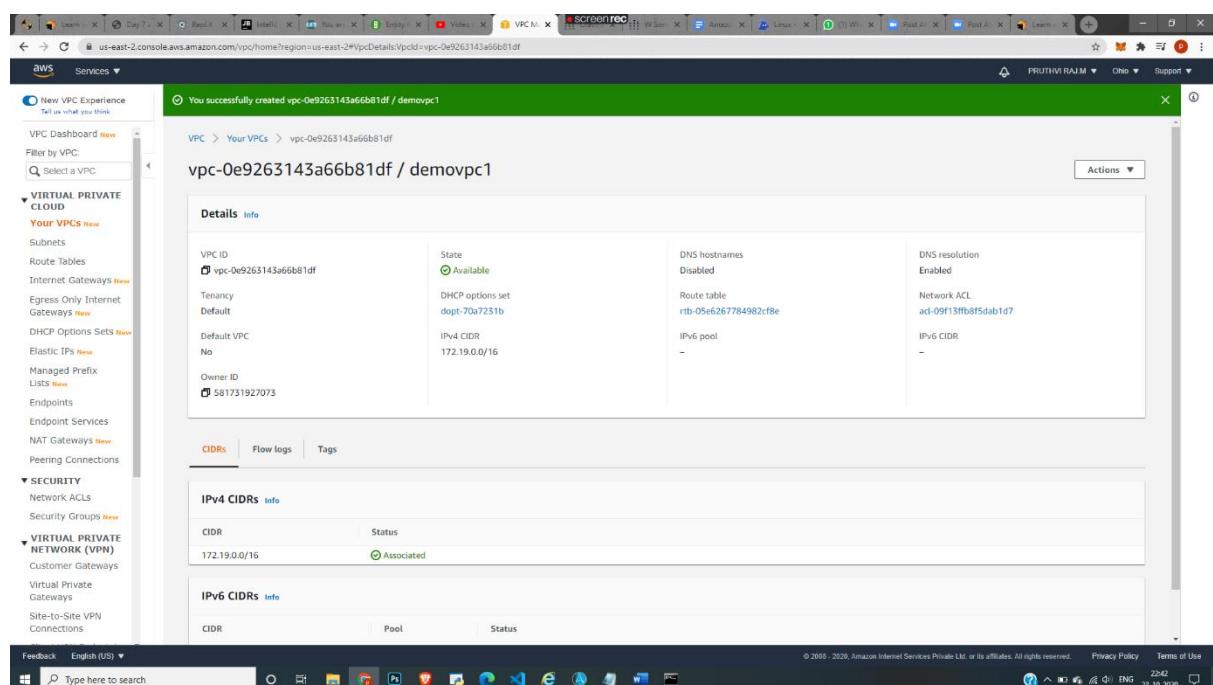
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options
vpc-7e4ae915	Available	172.31.0.0/16	-	-	dopt-70a7231b	
<b>demovpc1</b>	<b>vpc-0e9263143a66b81df</b>	<b>Available</b>	<b>172.19.0.0/16</b>	-	-	<b>dopt-70a7231b</b>

**vpc-0e9263143a66b81df / demovpc1**

**Details** CIDs Flow logs Tags

**Details**

VPC ID vpc-0e9263143a66b81df	State <b>Available</b>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-70a7231b	Route table rtb-05e6267784982cf8e	Network ACL acl-09f13fb8f5dab1d7
Default VPC No	IPv4 CIDR 172.19.0.0/16	IPv6 pool -	IPv6 CIDR -
Owner ID 581731927073			



You successfully created vpc-0e9263143a66b81df / demovpc1

**vpc-0e9263143a66b81df / demovpc1**

**Details** Info

VPC ID vpc-0e9263143a66b81df	State <b>Available</b>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-70a7231b	Route table rtb-05e6267784982cf8e	Network ACL acl-09f13fb8f5dab1d7
Default VPC No	IPv4 CIDR 172.19.0.0/16	IPv6 pool -	IPv6 CIDR -
Owner ID 581731927073			

**CIDs** Flow logs Tags

**IPv4 CIDs** Info

CIDR	Status
172.19.0.0/16	<b>Associated</b>

**IPv6 CIDs** Info

CIDR	Pool	Status
------	------	--------

Screenshot of the AWS VPC console showing the list of VPCs. The 'demovpc2' VPC is selected.

**Your VPCs (1/3) Info**

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options
vpc-7e4ae915	vpc-0e9263143a66b81df	Available	172.31.0.0/16	-	-	dopt-70a7231t
demovpc1	vpc-003ca47714ab618cc	Available	172.19.0.0/16	-	-	dopt-70a7231t
<b>demovpc2</b>	<b>vpc-003ca47714ab618cc</b>	<b>Available</b>	<b>172.16.0.0/16</b>	<b>-</b>	<b>-</b>	<b>dopt-70a7231t</b>

**vpc-003ca47714ab618cc / demovpc2**

**Details**   **CIDRs**   **Flow logs**   **Tags**

**Details**

VPC ID vpc-003ca47714ab618cc	State <span style="color: green;">Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-70a7231t	Route table rtb-07ffd0d2fd29368b	Network ACL acl-06f6c8ac844cd19b
Default VPC No	IPv4 CIDR 172.16.0.0/16	IPv6 pool -	IPv6 CIDR -
Owner ID 581731927073			

Feedback English (US) ▾ Type here to search © 2006 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use PRUTHVI RAJ M Ohio Support

Screenshot of the AWS VPC console showing the confirmation message for creating the 'demovpc2' VPC.

**You successfully created vpc-003ca47714ab618cc / demovpc2**

**vpc-003ca47714ab618cc / demovpc2**

**Details**   **Info**

VPC ID vpc-003ca47714ab618cc	State <span style="color: green;">Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-70a7231t	Route table rtb-07ffd0d2fd29368b	Network ACL acl-06f6c8ac844cd19b
Default VPC No	IPv4 CIDR 172.16.0.0/16	IPv6 pool -	IPv6 CIDR -
Owner ID 581731927073			

**CIDRs**   **Flow logs**   **Tags**

**IPv4 CIDRs**   **Info**

CIDR	Status
172.16.0.0/16	<span style="color: green;">Associated</span>

**IPv6 CIDRs**   **Info**

CIDR	Pool	Status

Feedback English (US) ▾ Type here to search © 2006 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use PRUTHVI RAJ M Ohio Support

## TASK 2: IGW LIST

The screenshot shows the AWS VPC Internet Gateways list page. The left sidebar navigation includes options like VPC Dashboard, Filter by VPC, and various network-related services. The main content area displays a table of Internet gateways:

Name	Internet gateway ID	State	VPC ID	Owner
demoigw1	igw-07af768241bff0947	Attached	vpc-0e9263143a66b81df   demovpc1	581731927073
-	igw-4d296525	Attached	vpc-7e4ae915	581731927073

Below the table, a specific gateway entry is expanded:

**igw-07af768241bff0947 / demoigw1**

**Details** **Tags**

Internet gateway ID igw-07af768241bff0947	State Attached	VPC ID vpc-0e9263143a66b81df   demovpc1	Owner 581731927073
--	-------------------	--	-----------------------

The screenshot shows the confirmation page for creating an Internet gateway. The message states: "The following internet gateway was created: igw-07af768241bff0947. You can now attach to a VPC to enable the VPC to communicate with the internet." Below this message, the gateway details are displayed:

**igw-07af768241bff0947 / demoigw1**

**Details** **Info**

Internet gateway ID igw-07af768241bff0947	State Detached	VPC ID -	Owner 581731927073
--	-------------------	-------------	-----------------------

**Tags**

Key Name	Value demoigw1
-------------	-------------------

Screenshot of the AWS VPC Internet Gateways page showing the successful attachment of an internet gateway to a VPC.

The screenshot shows the AWS VPC Internet Gateways page with the message: "Internet gateway igw-04272ee048f13da8f successfully attached to vpc-003ca47714ab618cc".

The table lists three internet gateways:

Name	Internet gateway ID	State	VPC ID	Owner
demoigw2	igw-04272ee048f13da8f	Attached	vpc-003ca47714ab618cc   demovpc2	581731927073
demoigw1	igw-07f768241bf0947	Attached	vpc-0e9263143a66b81df   demovpc1	581731927073
-	igw-4d296525	Attached	vpc-7e4a915	581731927073

The details for the selected internet gateway (igw-04272ee048f13da8f / demoigw2) show it is attached to a VPC with ID vpc-003ca47714ab618cc | demovpc2, owned by user 581731927073.

Screenshot of the AWS VPC Internet Gateways page showing the creation of a new internet gateway.

The screenshot shows the AWS VPC Internet Gateways page with the message: "The following internet gateway was created: igw-04272ee048f13da8f. You can now attach to a VPC to enable the VPC to communicate with the internet." and a "Attach to a VPC" button.

The details for the newly created internet gateway (igw-04272ee048f13da8f / demoigw2) show it has an Internet gateway ID of igw-04272ee048f13da8f, a State of Detached, and is owned by user 581731927073.

The Tags section shows a single tag named "demoigw2".

# TASK 3: ROUTE LIST

The screenshot shows the AWS VPC Route Table list page. The selected route table is "demoroute1" (rtb-0f924585b580031ff). The table details are as follows:

Route Table ID	Summary	Main	VPC
rtb-0f924585b580031ff	Explicitly Associated with Owner 581731927073	Yes	vpc-0e9263143a6bb81df   demovpc1

The screenshot shows the AWS VPC Route Table list page. The selected route table is "demoroute2" (rtb-0f7788c42c6d85b35). The table details are as follows:

Route Table ID	Summary	Main	VPC
rtb-0f7788c42c6d85b35	Explicitly Associated with Owner 581731927073	Yes	vpc-003ca47714ab618cc   demovpc2

## TASK 4: SUBNET LIST

The screenshot shows the AWS VPC Subnet list page. On the left, there's a navigation sidebar with options like New VPC Experience, VPC Dashboard, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Managed Prefix Lists, Endpoints Services, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, and Customer Gateways. The main area displays a table of subnets:

Name	Subnet ID	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table	Network ACL
demosubnet1	subnet-0f76efef7f5f3e86	vpc-0e9263143a66b81df	172.19.19.0/24	251	-	us-east-2c	use2-az3	rtb-0f924585b580031ff   demovpc1	aci-09
	subnet-20a7c6c	vpc-7e4ae915	172.31.32.0/20	4091	-	us-east-2c	use2-az3	rtb-3c7c1757	aci-7d
	subnet-8906063	vpc-7e4ae915	172.31.16.0/20	4091	-	us-east-2b	use2-az2	rtb-3c7c1757	aci-7d
	subnet-1467ac9f	vpc-7e4ae915	172.31.0.0/20	4091	-	us-east-2a	use2-az1	rtb-3c7c1757	aci-7d

Below the table, a detailed view of the subnet `subnet-0f76efef7f5f3e86` is shown. It includes fields for Subnet ID, VPC, Available IPv4 Addresses, Availability Zone, Network ACL, Auto-assign public IPv4 address, Customer-owned IPv4 pool, Outpost ID, State, IPv4 CIDR, IPv6 CIDR, Route Table, Default subnet, Auto-assign customer-owned IPv4 address, Auto-assign IPv6 address, and Owner.

The screenshot shows a confirmation dialog box titled "Create subnet". It contains a green message box with the text "The following Subnet was created:" followed by the Subnet ID "subnet-0f76efef7f5f3e86". At the bottom right of the dialog is a "Close" button.



Screenshot of the AWS VPC Subnets list page.

**Subnets List:**

Name	Subnet ID	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table	Network ACLs
demosubnet2	subnet-036efc53f94e1981	vpc-003ca47714ab610cc   demovpc2	172.16.16.0/24	251	-	us-east-2a	use2-az1	rb-05f78c42c6d6b35   demoroute2	aci-06
demosubnet1	subnet-07f6ef7f5f9e66	vpc-0e9263143a66b81df   demovpc1	172.19.19.0/24	250	-	us-east-2c	use2-az3	rb-092458b6500031ff   demoroute1	aci-09
	subnet-20a7cf6c	vpc-7e4ae915	172.31.32.0/20	4091	-	us-east-2c	use2-az3	rb-3c7c1757	aci-7d
	subnet-890606f3	vpc-7e4ae915	172.31.16.0/20	4091	-	us-east-2b	use2-az2	rb-3c7c1757	aci-7d
	subnet-4167acf	vpc-7e4ae915	172.31.0.0/20	4091	-	us-east-2a	use2-az1	rb-3c7c1757	aci-7d

**Subnet Details:** subnet-036efc53f94e1981

Description	Flow Logs	Route Table	Network ACL	Tags	Sharing
-------------	-----------	-------------	-------------	------	---------

Subnet ID: subnet-036efc53f94e1981  
VPC: vpc-003ca47714ab610cc | demovpc2  
Available IPv4 Addresses: 251  
Availability Zone: us-east-2a (use2-az1)  
Network ACL: ac-5096c9ac944cd919b  
Auto-assign public IPv4 address: Yes  
Customer-owned IPv4 pool: -  
Outpost ID: -  
State: available  
IPv4 CIDR: 172.16.16.0/24  
IPv6 CIDR: -  
Route Table: rb-05f78c42c6d6b35 | demoroute2  
Delete subnet: No  
Auto-assign customer-owned IPv4 address: No  
Auto-assign IPv6 address: No  
Owner: 581731927073

Screenshot of the AWS Create Subnet confirmation page.

**Create subnet**

The following Subnet was created:

Subnet ID: subnet-036efc53f94e1981
------------------------------------

**Close**

Screenshot of the AWS Create Subnet confirmation page (continued).

**Create subnet**

The following Subnet was created:

Subnet ID: subnet-036efc53f94e1981
------------------------------------

**Close**

## TASK 5: INSTANCE DETAILS

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with links like EC2 Dashboard, Events, Tags, Limits, Instances (selected), Images, Elastic Block Store, Network & Security, and more. The main content area displays a table of instances. One instance, 'demoserver-1', is selected and shown in detail. Its details include:

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv4 DNS	Public IPv4 ...	Elastic Ip
demoserver-1	i-09bca9bc4fa994c2c	Running	t2.micro	2/2 checks ...	No alarms	us-east-2c	-	18.219.115.183	-
-	i-008f3c1c17394249f	Terminating	t2.micro	-	No alarms	us-east-2b	-	-	-

The detailed view for 'demoserver-1' shows the following configuration:

Details	Security	Networking	Storage	Status Checks	Monitoring	Tags
<b>Instance summary</b>						
Instance ID i-09bca9bc4fa994c2c (demoserver-1)	Public IPv4 address 18.219.115.183   open address	Private IPv4 addresses 172.19.19.34				
Instance state Running	Public IPv4 DNS -	Private IPv4 DNS ip-172-19-19-34.us-east-2.compute.internal				
Instance type t2.micro	Elastic IP addresses -	VPC ID vpc-0e9263143a66b81df (demovpc1)				
IAM Role -	Subnet ID subnet-0f76efef7f5f39e86 (demosubnet1)	Termination protection				
<b>Instance details</b>						
Platform windows	AMI ID ami-0354df7841220296c	Monitoring disabled				
Platform details	AMI name					

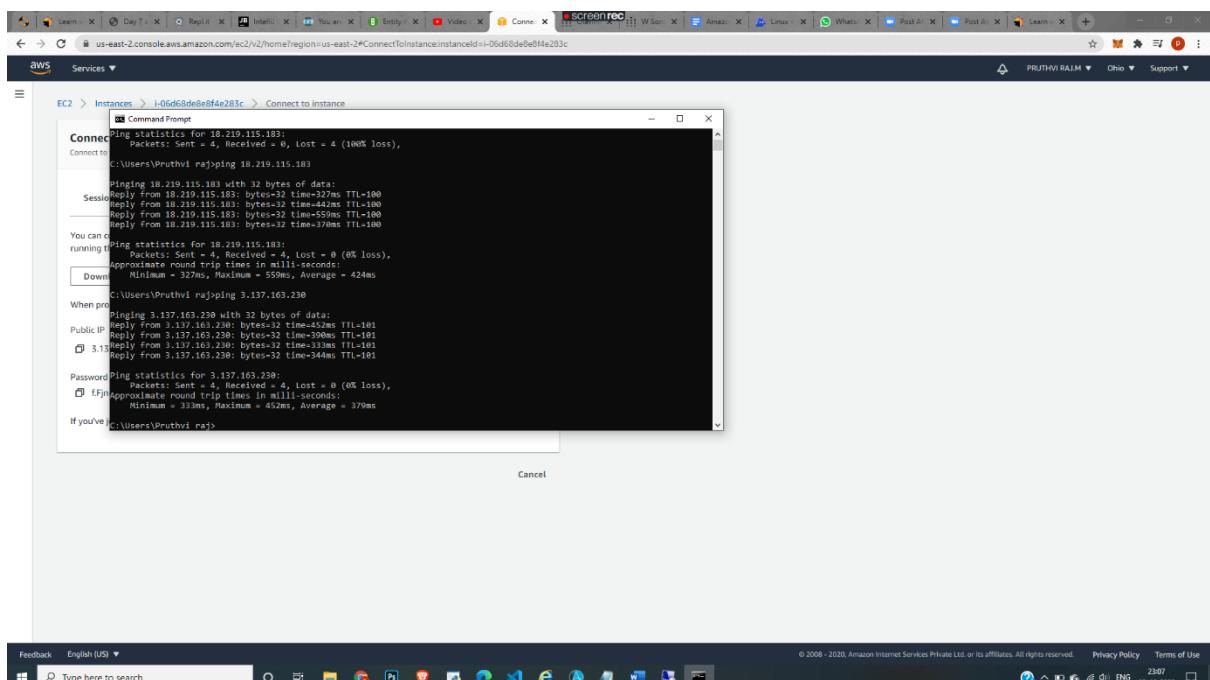
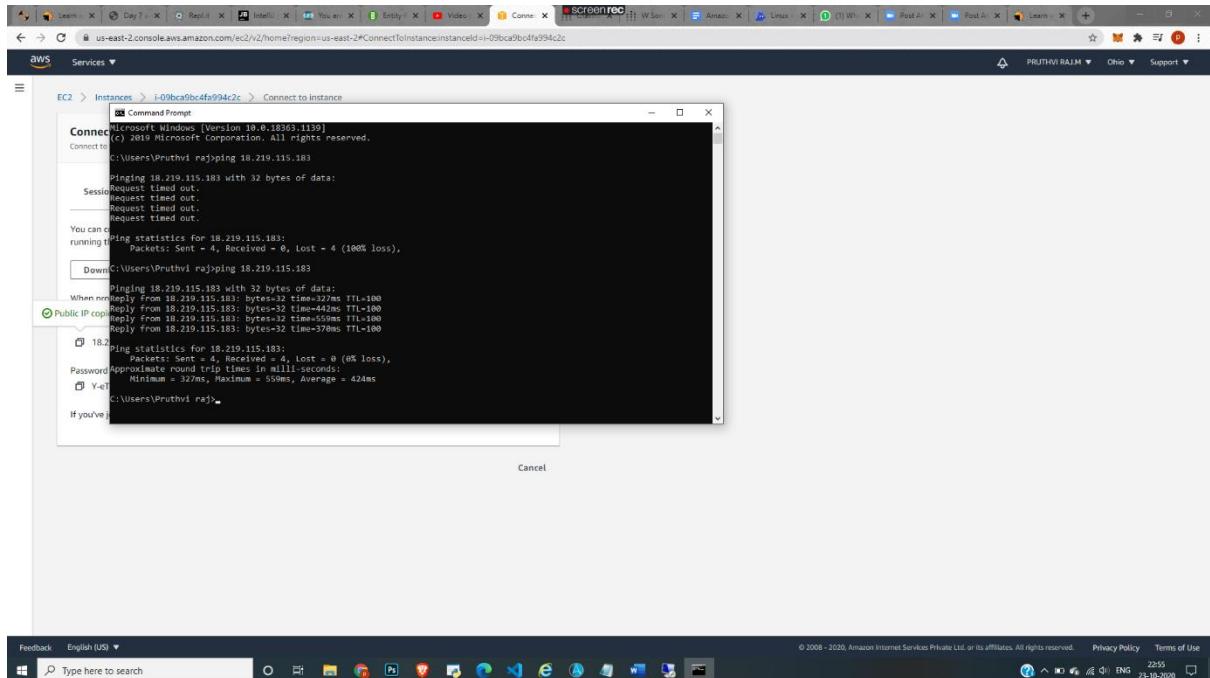
The screenshot shows the AWS EC2 Instances page. The left sidebar is identical to the previous screenshot. The main content area displays a table of instances. Two instances, 'demoserver-1' and 'demoserver-2', are selected and shown in detail. Their details include:

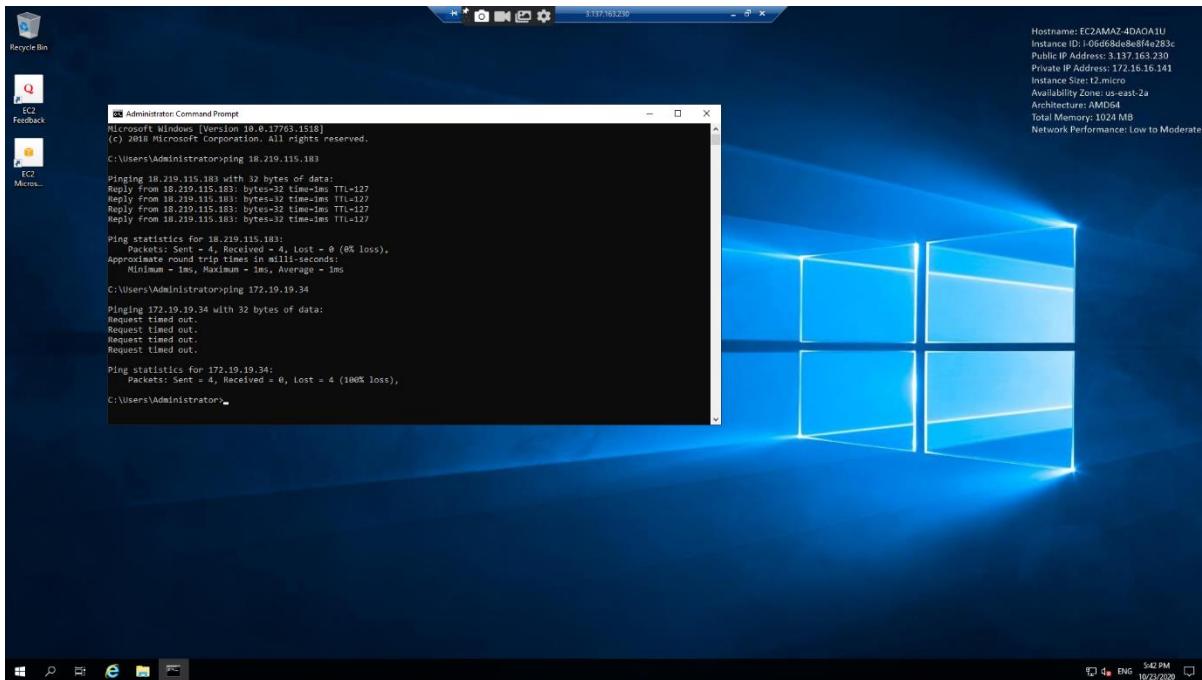
Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv4 DNS	Public IPv4 ...	Elastic Ip
demoserver-1	i-09bca9bc4fa994c2c	Running	t2.micro	2/2 checks ...	No alarms	us-east-2c	-	18.219.115.183	-
demoserver-2	i-06d68de8e8f4e283c	Running	t2.micro	2/2 checks ...	No alarms	us-east-2a	-	3.137.163.230	-
-	i-008f3c1c17394249f	Terminating	t2.micro	-	No alarms	us-east-2b	-	-	-

The detailed view for 'demoserver-2' shows the following configuration:

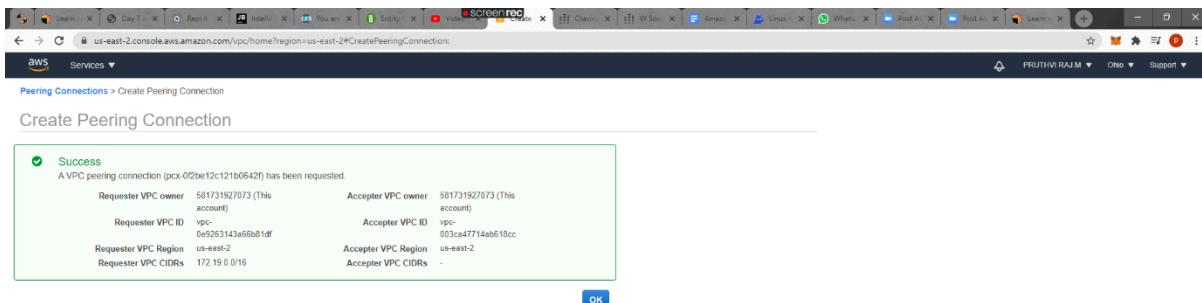
Details	Security	Networking	Storage	Status Checks	Monitoring	Tags
<b>Instance summary</b>						
Instance ID i-06d68de8e8f4e283c (demoserver-2)	Public IPv4 address 3.137.163.230   open address	Private IPv4 addresses 172.16.16.141				
Instance state Running	Public IPv4 DNS -	Private IPv4 DNS ip-172-16-16-141.us-east-2.compute.internal				
Instance type t2.micro	Elastic IP addresses -	VPC ID vpc-003ca47714ab618cc (demovpc2)				
IAM Role -	Subnet ID subnet-036ef3c5f94e1981 (demosubnet2)	Termination protection				
<b>Instance details</b>						
Platform windows	AMI ID ami-0354df7841220296c	Monitoring disabled				
Platform details	AMI name					

## TASK 6: SUCCESS PUBLIC , RTO PRIVATE IP





## TASK 7: PEERING WITH REQ AND ACCETOR



The screenshot shows the AWS Management Console interface for managing VPC peering connections. The left sidebar navigation includes 'New VPC Experience', 'Services', 'Virtual Private Cloud', 'Your VPCs', 'Subnets', 'Route Tables', 'Internet Gateways', 'Egress Only Internet Gateways', 'DHCP Options Sets', 'Elastic IPs', 'Managed Prefix Lists', 'Endpoints', 'Endpoint Services', 'NAT Gateways', 'Peering Connections', 'Security', 'Network ACLs', 'Security Groups', 'Virtual Private Network (VPN)', 'Customer Gateways', 'Site-to-Site VPN Connections', and 'Client VPN Endpoints'. The 'Peering Connections' section is currently selected.

The main content area displays a table of peering connections. One entry is visible:

Name	Peering Connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs	Requester Owner	Acceptor Owner
demopeer	pxc-0f2be12c121b0642f	Active	vpc-0e9263143a6	vpc-003ca47714...	172.19.0.0/16	172.16.0.0/16	581731927073	581731927073

Below the table, a detailed view of the peering connection 'pxc-0f2be12c121b0642f' is shown with tabs for 'Description', 'DNS', 'Route Tables', and 'Tags'. The 'Description' tab displays the following details:

- Requester VPC owner: 581731927073
- Requester VPC ID: vpc-0e9263143a66b81df
- Requester VPC Region: Ohio (us-east-2)
- Requester VPC CIDRs: 172.19.0.0/16
- VPC Peering Connection: pxc-0f2be12c121b0642f
- Expiration time: -
- Acceptor VPC owner: 581731927073
- Acceptor VPC ID: vpc-003ca47714ab618cc
- Acceptor VPC Region: Ohio (us-east-2)
- Acceptor VPC CIDRs: 172.16.0.0/16
- Peering connection status: Active

The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating battery level, signal strength, and date/time (23-09-2020).

## TASK 8: SUCCESS FOR PRIVATE

The screenshot shows a Windows desktop environment. On the left, there's a Start menu with options like 'Recycle Bin', 'File Explorer', 'This PC', 'Control Panel', 'Network', 'File History', 'Task View', 'Search', 'Help & Support', and 'Sign Out'. The desktop background is the standard Windows 10 blue logo.

In the center, a Command Prompt window is open with the title 'Administrator: Command Prompt'. It contains the following command and output:

```
C:\Users\Administrator>ping 172.19.19.34

Pinging 172.19.19.34 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.19.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Administrator>ping 172.19.19.34

Pinging 172.19.19.34 with 32 bytes of data:
Reply from 172.19.19.34: bytes=32 time=1ms TTL=128

Ping statistics for 172.19.19.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\Users\Administrator>
```

To the right of the Command Prompt, there's a vertical text block with instance details:

Hostname: EC2AMAZ-4DAOA1U  
 Instance ID: i-06d68de8e8f4fa283c  
 Public IP Address: 3.137.163.230  
 Private IP Address: 172.16.16.141  
 Instance Size: t2.micro  
 Availability Zone: us-east-2a  
 Architecture: AMD64  
 Total Memory: 1024 MB  
 Network Performance: Low to Moderate

The bottom of the screen shows the Windows taskbar with icons for File Explorer, Task View, Start, and other system functions, along with the system tray showing battery level, signal strength, and date/time (16:09 PM 10/23/2020).

# PROJECT 2 : IAM

## TASK 1: CREATING USERS WITHOUT PERMISSIONS-IAM PASSWORD POLICY CHECK

The screenshot shows the 'Add user' review step in the AWS IAM console. The user details section includes:

- User name: manoj
- AWS access type: Programmatic access and AWS Management Console access
- Console password type: Custom
- Require password reset: Yes
- Permissions boundary: Permissions boundary is not set

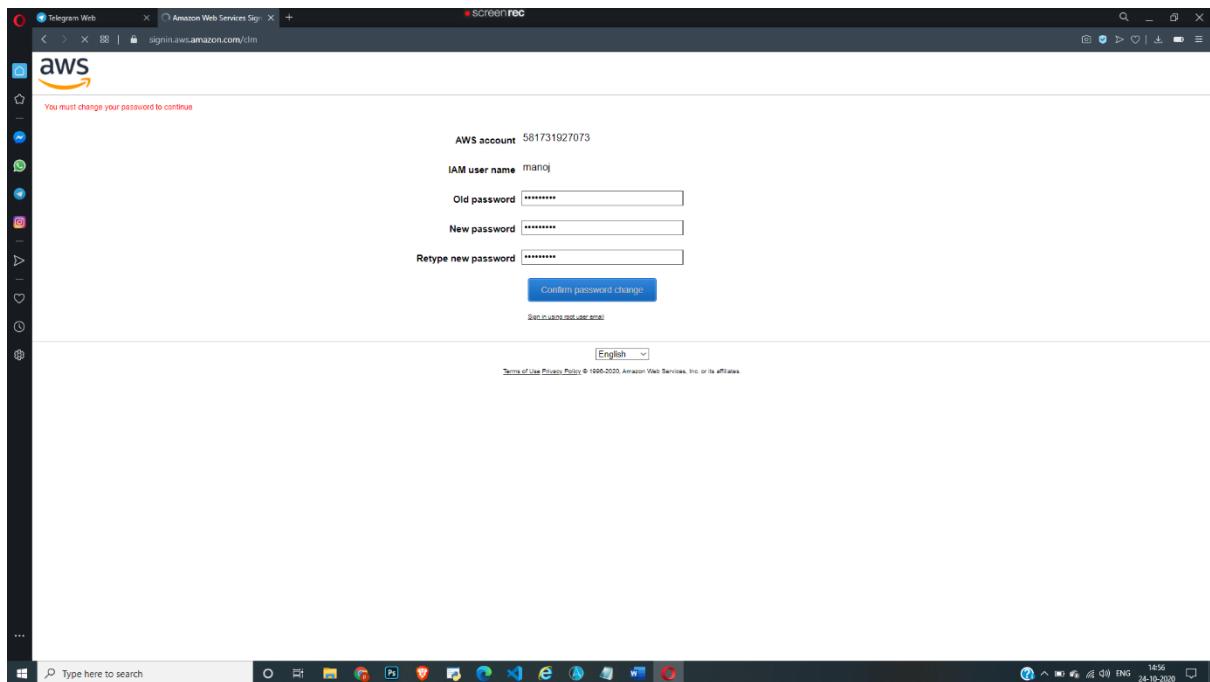
The 'Permissions summary' section shows the user will be added to the 'IAMUserChangePassword' group. There are no tags added.

At the bottom right, there are 'Cancel', 'Previous', and 'Create user' buttons.

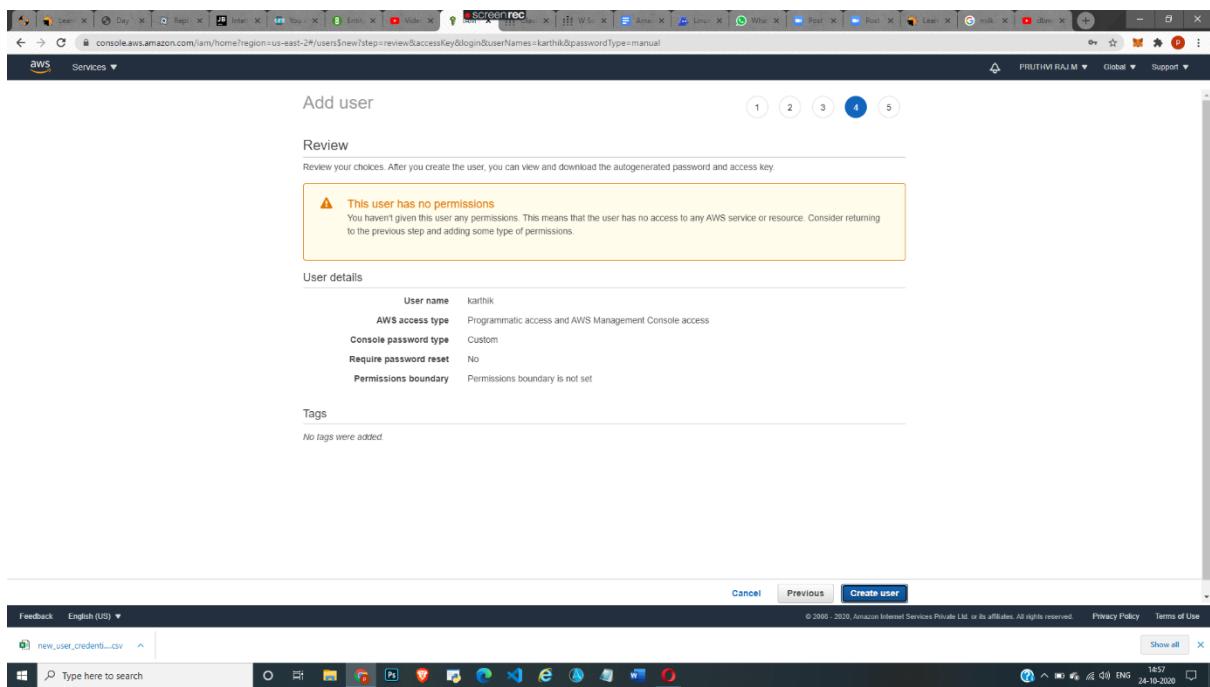
The screenshot shows the 'Summary' page for the user 'manoj'. The user ARN is arn:aws:iam::581731927073:user/manoj. The creation time was 2020-10-24 14:54 UTC+0530. The 'Permissions' tab is selected, showing one policy applied: 'IAMUserChangePassword' (AWS managed policy). The 'Attached directly' section lists this policy. The 'Permissions boundary (not set)' section is empty.

At the bottom right, there are 'Delete user' and 'Edit user' buttons.

At the very bottom, there is a link to 'new\_user\_credentials.csv'.



## TASK 2: CREATING USERS WITHOUT THE IAM PASSWORD POLICY



The screenshot shows the AWS Identity and Access Management (IAM) service. The URL is <https://console.aws.amazon.com/iam/home?region=us-east-2#users/karthik>. The page title is "Summary". The left sidebar includes links for Dashboard, Access management (Groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Archive rules, Analyzers, Settings), Credential report, Organization activity, and Service control policies (SCPs). A search bar for "Search IAM" and an AWS account ID (581731927073) are also present. The main content area displays the user's ARN (arn:aws:iam::581731927073:user/karthik), Path (/), and Creation time (2020-10-24 14:59 UTC+0530). It features tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor. Under the Permissions tab, there is a section titled "Get started with permissions" with a note: "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". A "Add permissions" button and a "Add inline policy" link are available. Below this is a section for "Permissions boundary (not set)".

The screenshot shows the AWS Management Console home page. The URL is <https://us-east-2.console.aws.amazon.com/console/home>. The page title is "AWS Management Console". The left sidebar has a vertical navigation menu with icons for various services like Lambda, S3, CloudWatch, etc. The main content area is divided into several sections: "AWS services" (Find Services, Recently visited services [EC2], All services), "Build a solution" (Launch a virtual machine, Connect an IoT device, Build a web app, Start migrating to AWS, Build using virtual servers, Start a development project, Register a domain, Deploy a serverless microservice), "Stay connected to your AWS resources on-the-go" (Download the AWS Console Mobile App), "Explore AWS" (Amazon Redshift, Run Serverless Containers with AWS Fargate, Scalable, Durable, Secure Backup & Restore with Amazon S3, AWS Marketplace), and "Recent activity" (karthik @ 5817-3192-7075, Ohio, Support). The bottom of the screen shows the Windows taskbar with the search bar containing "Type here to search".

# TASK 3: CREATE USER WITH S3 FULL ACCESS

The screenshot shows the 'Add user' review step in the AWS IAM console. The user 'pradeep' has been created with the following details:

- User name: pradeep
- AWS access type: Programmatic access and AWS Management Console access
- Console password type: Custom
- Require password reset: No
- Permissions boundary: Permissions boundary is not set

A warning message states: "This user has no permissions. You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions."

The browser taskbar at the bottom shows various open tabs and the system clock.

The screenshot shows the 'Summary' page for the user 'pradeep' in the AWS IAM console. The user ARN is am:aws:iam::581731927073:user/pradeep. The creation time is 2020-10-24 15:18 UTC+0530. The 'Permissions' tab is selected, showing the following information:

- 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.
- Add inline policy: A button to add a new inline policy.

The 'Permissions boundary (not set)' section is also visible.

The browser taskbar at the bottom shows various open tabs and the system clock.

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, a navigation pane lists various IAM management options like Dashboard, Access management, Groups, Users (selected), Roles, Policies, Identity providers, Account settings, Access reports, and Service control policies (SCPs). The main content area is titled 'Summary' for the user 'pradeep'. It displays the User ARN (arn:aws:iam::581731927073:user/pradeep), Path (/), and Creation time (2020-10-24 15:18 UTC+0530). Below this, tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor are shown, with 'Permissions' selected. Under 'Permissions', it shows 'Permissions policies (1 policy applied)' with an 'Add permissions' button and an 'Add inline policy' link. A table lists the attached policy 'AmazonS3FullAccess' as an 'AWS managed policy'. There is also a section for 'Permissions boundary (not set)'. At the bottom of the page, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

The screenshot shows the AWS S3 Management Console. The left sidebar includes links for Home, Buckets, Batch operations, Access analyzer for S3, Block public access (account settings), and Feature spotlight. The main content area is titled 'Manage tens to billions of objects in a few clicks with S3 Batch Operations. Learn more ». It displays a message: '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, it shows the 'S3 buckets' section with a search bar and a 'Discover the console' link. A table lists one bucket: 'pmp1218'. The table columns include 'Bucket name', 'Access', 'Region', and 'Date created'. The bucket details show 'Bucket name: pmp1218', 'Access: Objects can be public', 'Region: US East (Ohio)', and 'Date created: Oct 13, 2020 9:56:04 AM GMT+0530'. At the bottom of the page, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

## TASK 4: CREATE A GROUP WITH EC2 FULL ACCESS

The screenshot shows the AWS Identity and Access Management (IAM) service in the AWS Management Console. The user 'nithin' is selected. The 'Summary' tab is active, displaying the User ARN (arn:aws:iam::591731927073:user/nithin), Path (/), and Creation time (2020-10-24 15:49 UTC+0530). The 'Permissions' tab is selected, showing one policy applied: 'AmazonEC2FullAccess'. This policy is listed under 'Attached directly' and is identified as an 'AWS managed policy'. The 'Policy type' is listed as 'AWS managed policy'. The 'Permissions boundary (not set)' section is empty.

The screenshot shows the AWS EC2 Dashboard. The left sidebar includes sections for Instances, Images, Elastic Block Store, Network & Security, and more. The main area displays a welcome message about the new EC2 experience, resource counts (Running instances: 0, Snapshots: 0, Key pairs: 4), and service health information. It also shows scheduled events and zone status for the US East (Ohio) region. The right sidebar contains account attributes like supported platforms (VPC, Default VPC: vpc-7e4ae915) and explore options for custom AMIs and best price-performance.

## TASK 5 : ADD USER TO GROUP AND CHECK IF USER POLICY AND THE GROUP POLICY IS REFLECTING ON THE USER

The screenshot shows the AWS Identity and Access Management (IAM) Groups page. The left sidebar navigation includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'Groups' selected), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports', 'Access analyzer', 'Archive rules', 'Analyzers', 'Settings', 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. A search bar for 'Search IAM' and an 'AWS account ID' field (581731927073) are also present. The main content area displays the 'coders' group summary with details like Group ARN: arn:aws:iam:581731927073:group/coders, Users (in this group): 2, Path: /, and Creation Time: 2020-10-24 15:52 UTC+0530. Below this, a table lists the users in the group:

User	Actions
nithin	Remove User from Group
manoj	Remove User from Group

Buttons for 'Remove Users from Group' and 'Add Users to Group' are located at the top right of the user list.

The screenshot shows the AWS S3 Management Console. The left sidebar navigation includes 'Amazon S3' (with 'Buckets' selected), 'Batch operations', 'Access analyzer for S3', 'Block public access (account settings)', and 'Feature spotlight'. The main content area displays a message: 'Manage tens to billions of objects in a few clicks with S3 Batch Operations. Learn more »' and '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 table with one entry:

Bucket name	Access	Region	Date created
pmp1218	Public	US East (Ohio)	Oct 13, 2020 9:56:04 AM GMT+0530

Buttons for '+ Create bucket', 'Edit public access settings', 'Empty', and 'Delete' are available above the table. A 'Discover the console' link is also present.

Welcome to the new EC2 console  
We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know where we can make improvements. To switch between the old console and the new console, use the New EC2 Experience toggle.

**Resources**

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Running instances	0	Elastic IPs	0	Dedicated Hosts	0
Snapshots	0	Volumes	0	Load balancers	0
Key pairs	4	Security groups	25	Placement groups	0

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Service health**

Region: US East (Ohio) Status: This service is operating normally

**Zone status**

Zone	Status
us-east-2a (use2-az1)	Zone is operating normally
us-east-2b (use2-az2)	Zone is operating normally
us-east-2c (use2-az3)	Zone is operating normally

Enable additional Zones

**Explore AWS**

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

Launch Custom AMIs with Fast Snapshot Restore (FSR)

Reduce instance boot times and improve disaster recovery objectives with FSR. Learn more

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

## TASK 6 : COPY POLICIES FROM THE EXISTING USER

Add user

1 2 3 4 5

**Set permissions**

Add user to group Copy permissions from existing user Attach existing policies directly

Select an existing user from which to copy policies and group membership.

**Copy permissions from existing user**

User name	Groups	Attached policies
karthik	None	None
manoj	coders	IAMUserChangePassword
<b>nitin</b>	coders	AmazonEC2FullAccess
pradeep	None	AmazonS3FullAccess

Showing 4 results

**Set permissions boundary**

Cancel Previous Next: Tags

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, a sidebar menu includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'Groups' and 'Users' selected), 'Roles', 'Policies', 'Identity providers', and 'Account settings'. Under 'Access reports', there are 'Archive analyzer', 'Analyzer', and 'Settings'. At the bottom of the sidebar is a search bar labeled 'Search IAM' and an 'AWS account ID' field showing '581731927073'. The main content area is titled 'Summary' for user 'raj'. It displays the 'User ARN' as 'arn:aws:iam::581731927073:user/raj', 'Path' as '/', and 'Creation time' as '2020-10-24 15:56 UTC+0530'. Below this, tabs for 'Permissions', 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor' are visible. The 'Permissions' tab is active, showing 'Permissions policies (2 policies applied)'. Two policies are listed: 'AmazonEC2FullAccess' (Attached directly, AWS managed policy) and 'AmazonS3FullAccess' (Attached from group, AWS managed policy from group coders). A link to 'Add inline policy' is also present. The status bar at the bottom right shows 'PRUTHVI RAJ M Global Support'.

The screenshot shows the AWS S3 Management Console. On the left, a sidebar menu includes 'Amazon S3' (with 'Buckets', 'Batch operations', 'Access analyzer for S3', and 'Block public access (account settings)'), 'Feature spotlight', and 'Documentation'. The main content area has a banner stating 'S3 Replication lets you simply copy objects from one S3 bucket to another. Learn more ». 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, a search bar 'Search for buckets' and a button 'Discover the console' are shown. A table lists '1 Buckets' and '1 Regions'. One bucket named 'pmp1218' is listed with 'Access' set to 'Objects can be public', 'Region' as 'US East (Ohio)', and 'Date created' as 'Oct 13, 2020 9:56:04 AM GMT+0530'. The status bar at the bottom right shows 'raj @ 5817.3192.7073 Global Support'.

Welcome to the new EC2 console  
We're redesigning the EC2 console to make it easier to use and improve performance. We'll release new screens periodically. We encourage you to try them and let us know where we can make improvements. To switch between the old console and the new console, use the New EC2 Experience toggle.

**Resources**

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Running Instances	0	Elastic IPs	0	Dedicated Hosts	0
Snapshots	0	Volumes	0	Load balancers	0
Key pairs	4	Security groups	25	Placement groups	0

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Service health**

Region: US East (Ohio) Status: This service is operating normally

**Zone status**

Zone	Status
us-east-2a (use2-az1)	Zone is operating normally
us-east-2b (use2-az2)	Zone is operating normally
us-east-2c (use2-az3)	Zone is operating normally

Enable additional Zones

**Explore AWS**

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

Save up to 90% on EC2 with Spot Instances

Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

Launch Custom AMIs with Fast Snapshot Restore (FSR)

Reduce instance boot times and improve disaster recovery objectives with FSR. Learn more

## TASK 7: ADD USER TO A GROUP IN THE PROCESS OF CREATING A USER

Add user

Set permissions

Add user to group

Search: coders

Attached policies: AmazonS3FullAccess

Set permissions boundary

Cancel Previous Next: Tags

The screenshot shows the AWS Identity and Access Management (IAM) service interface. The left sidebar navigation includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (Groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Archive analyzer, Analyzers, Settings), 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. A search bar at the bottom left says 'Search IAM'. The top right shows the user 'PRUTHVI RAJ.M' and links for 'Global' and 'Support'. The main content area is titled 'Summary' for user 'pavan'. It displays the User ARN (arn:aws:iam::581731927073:user/pavan), Path (/), and Creation time (2020-10-24 15:58 UTC+0530). Below this, tabs for 'Permissions', 'Groups (1)', 'Tags', 'Security credentials', and 'Access Advisor' are shown. Under 'Permissions', it lists 'Permissions policies (1 policy applied)' with an 'Add permissions' button and an 'Add inline policy' link. It shows one policy attached from a group: 'AmazonS3FullAccess' (AWS managed policy from group coders). There is also a section for 'Permissions boundary (not set)'. At the bottom right of the summary page, there is a 'Delete user' button.

The screenshot shows the AWS S3 Management Console. The left sidebar navigation includes 'Amazon S3' (Buckets, Batch operations, Access analyzer for S3, Block public access (account settings)), 'Feature spotlight', and a 'Documentation' link. The main content area displays a message: '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, there is a search bar for 'Search for buckets' and a 'Discover the console' link. A table lists '1 Buckets' and '1 Regions'. One bucket is listed: 'Bucket name: pmp1218', 'Access: Objects can be public', 'Region: US East (Ohio)', and 'Date created: Oct 13, 2020 9:56:04 AM GMT+0530'. The top right shows the user 'pavan @ 5817-3192-7073' and links for 'Global' and 'Support'. The bottom right shows the system status: 15:58, EN5, 24-10-2020. The taskbar at the bottom shows various open applications like Screenrec, File Explorer, and Edge browser.

An error occurred describing your selected AMI.  
You are not authorized to perform this operation.

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace, or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

**Quick Start**

- My AMIs
- AWS Marketplace
- Community AMIs
- Free tier only (i)

AMI Name	Description	Root device type	Virtualization type	ENI Enabled	Select
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-03657b56516ab7912 (64-bit x86) / ami-023b120e01f4779c1 (64-bit Arm)	Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.	ebs	hvm	Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-027cab0a7bf0155d	The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.	ebs	hvm	ENI Enabled: Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a54ae4ef43b5fb81 (64-bit x86) / ami-0e05c6b1b5100c04 (64-bit Arm)	Red Hat Enterprise Linux version 8 (HVM); EBS General Purpose (SSD) Volume Type	ebs	hvm	ENI Enabled: Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-034c4194895956a3 (64-bit x86) / ami-05d41fc1ba96d2803 (64-bit Arm)	SUSE Linux Enterprise Server 15 Service Pack 2 (HVM); EBS General Purpose (SSD) Volume Type; Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	ebs	hvm	ENI Enabled: Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)
Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-07efac79022b86107 (64-bit x86) / ami-00bcac5ae8c849ed7 (64-bit Arm)	Ubuntu Server 20.04 LTS (HVM); EBS General Purpose (SSD) Volume Type. Support available from Canonical ( <a href="http://www.ubuntu.com/cloud/services">http://www.ubuntu.com/cloud/services</a> ).	ebs	hvm	ENI Enabled: Yes	<input checked="" type="radio"/> 64-bit (x86) <input type="radio"/> 64-bit (Arm)

Feedback English (US) ▾ Type here to search Privacy Policy Terms of Use 15:59 24-10-2020

## TASK 8 : SETTING A PASSWORD POLICY

Identity and Access Management (IAM)

Account settings

Change password policy Delete password policy

>Password policy updated.

A password policy is a set of rules that define the type of password an IAM user can set. Learn more

**Password policy**

This AWS account uses a password policy

- Minimum password length is 14 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 days
- Allow users to change their own password
- Remember last 2 password(s) and prevent reuse

Security Token Service (STS)

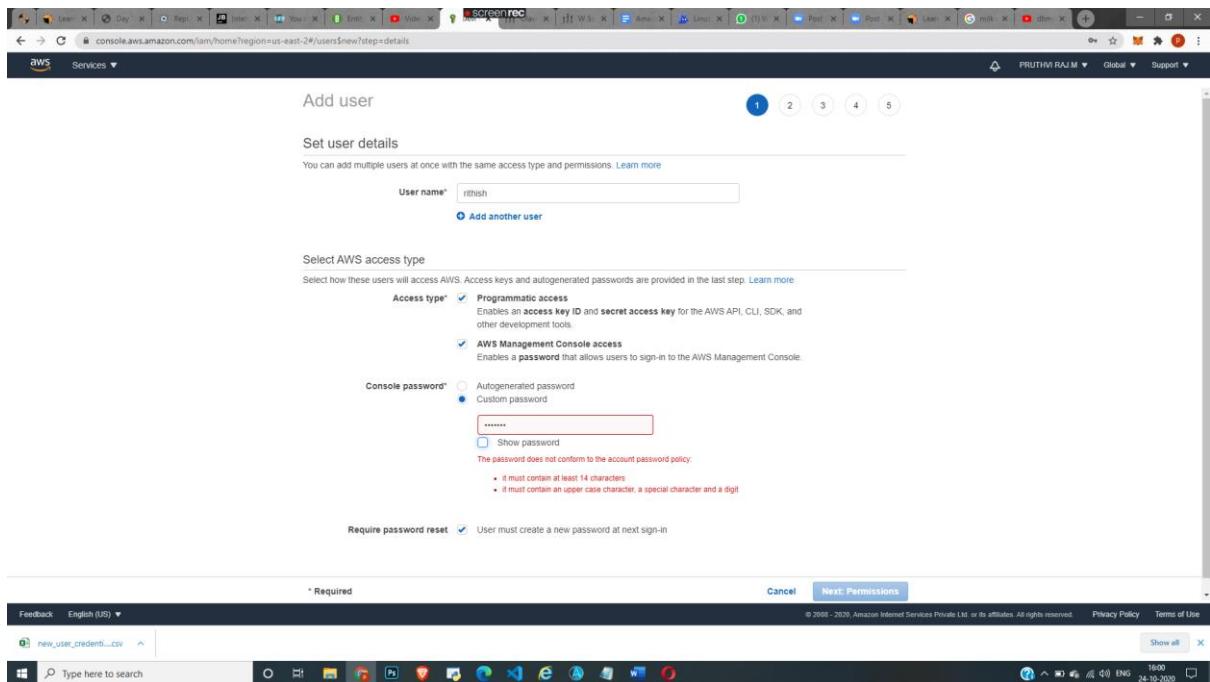
Session Tokens from the STS endpoint

Endpoints Region compatibility of session tokens Actions

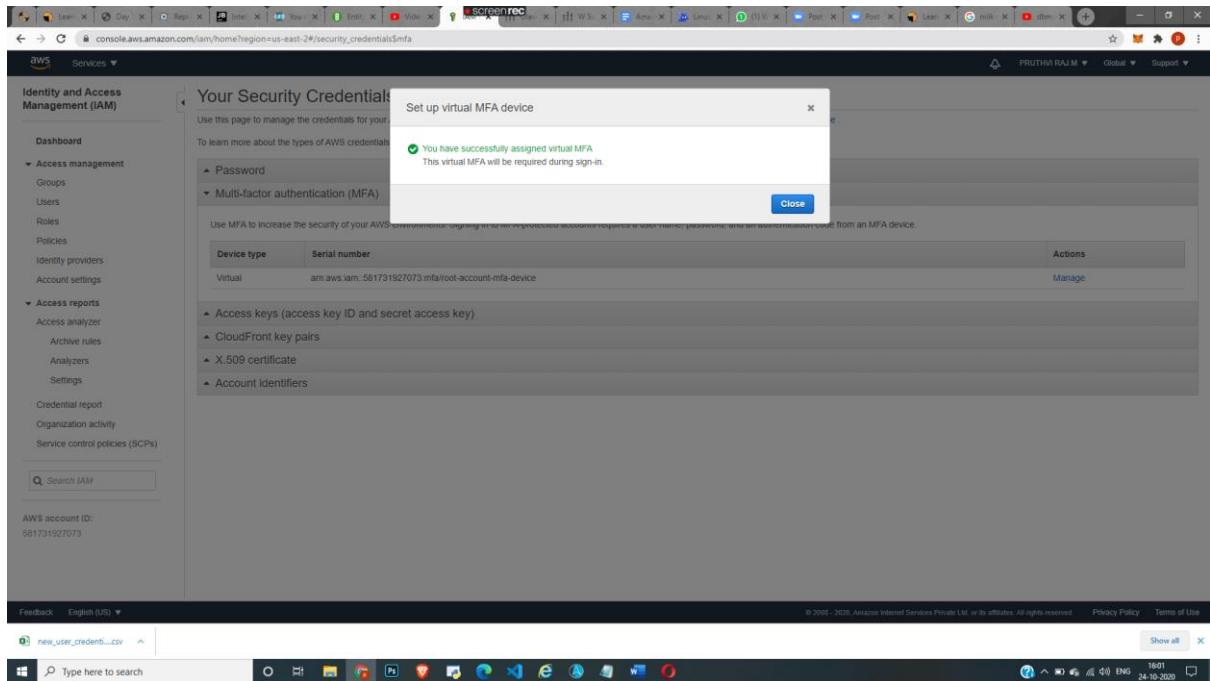
Endpoints	Region compatibility of session tokens	Actions
Global endpoint	Valid only in AWS Regions enabled by default	Edit
Regional endpoints	Valid in all AWS Regions	

Endpoints You can enable additional endpoints from which you can request temporary credentials. Activate only endpoints you intend to use. Learn more

Feedback English (US) ▾ new\_user\_credentials.csv Show all 15:59 24-10-2020



## TASK 9: ENABLING MFA AND USING AN MFA DEVICE



Screenshot of the AWS IAM Security Credentials page. The left sidebar shows navigation options like Dashboard, Access management, Access reports, and Credential activity. The main content area displays security credentials, including a table for MFA devices:

Device type	Serial number	Actions
Virtual	arn:aws:iam::581731927073:mfa/root-account-mfa-device	Manage

Below the table are sections for Access keys, CloudFront key pairs, X.509 certificate, and Account identifiers.

Screenshot of the AWS Multi-factor authentication sign-in page. It asks for an MFA code and includes links for troubleshooting and canceling the process. To the right, there is an advertisement for Amazon ElastiCache.

**Amazon ElastiCache**  
Get sub-millisecond performance at cloud scale when building real-time apps with ElastiCache for Redis



The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar has sections like 'Dashboard', 'Access management', 'Access reports', and 'Credential activity'. The main area is titled 'Your Security Credentials' and lists 'Multi-factor authentication (MFA)'. A modal window titled 'Manage MFA device' is open, asking 'Choose an action to perform on the MFA device for user:'. It has two options: 'Remove' (selected) and 'Resync'. Below this, it says 'This user will no longer be required to provide MFA during sign-in.' and 'This option is not available for U2F security keys.' At the bottom of the modal are 'Cancel' and 'Remove' buttons.

THE END