

## Project 1 Week 4: VPC Peering

### SS1: VPCs List

#### a. lab-vpc-01

Your VPCs (1/3) [Info](#)

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options
<input checked="" type="checkbox"/> lab-vpc-01	vpc-0c4d80743b459c685	<span>Available</span>	172.19.0.0/16	-	-	dopt-57bc3a3c
<input type="checkbox"/> -	vpc-ae3895c5	<span>Available</span>	172.31.0.0/16	-	-	dopt-57bc3a3c
<input type="checkbox"/> lab-vpc-02	vpc-08bc2b996409e1952	<span>Available</span>	172.16.0.0/16	-	-	dopt-57bc3a3c

vpc-0c4d80743b459c685 / lab-vpc-01

[Details](#) [CIDRs](#) [Flow logs](#) [Tags](#)

**Details**

VPC ID vpc-0c4d80743b459c685	State <span>Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-57bc3a3c	Route table rtb-02e3a32fc88080c9a / projectroute01	Network ACL acl-07b61f48b46b9f30f
Default VPC No	IPv4 CIDR 172.19.0.0/16	IPv6 pool -	IPv6 CIDR -
Owner ID 052604659223			

#### b. lab-vpc-02

Your VPCs (1/3) [Info](#)

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool	DHCP options
<input checked="" type="checkbox"/> lab-vpc-01	vpc-0c4d80743b459c685	<span>Available</span>	172.19.0.0/16	-	-	dopt-57bc3a3c
<input type="checkbox"/> -	vpc-ae3895c5	<span>Available</span>	172.31.0.0/16	-	-	dopt-57bc3a3c
<input type="checkbox"/> lab-vpc-02	vpc-08bc2b996409e1952	<span>Available</span>	172.16.0.0/16	-	-	dopt-57bc3a3c

vpc-0c4d80743b459c685 / lab-vpc-01

[Details](#) [CIDRs](#) [Flow logs](#) [Tags](#)

**Details**

VPC ID vpc-0c4d80743b459c685	State <span>Available</span>	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-57bc3a3c	Route table rtb-02e3a32fc88080c9a / projectroute01	Network ACL acl-07b61f48b46b9f30f
Default VPC No	IPv4 CIDR 172.19.0.0/16	IPv6 pool -	IPv6 CIDR -
Owner ID 052604659223			

## SS2: IGW List

### a. IGW01

Name	Internet gateway ID	State	VPC ID	Owner
projectIGW02	igw-07d205123e4189844	Attached	vpc-08bc2b996409e1952   lab-vpc-02	052604659223
projectIGW01	igw-0c90b1c3a09178cf3	Attached	vpc-0c4d80743b459c685   lab-vpc-01	052604659223
-	igw-e73b758f	Attached	vpc-ae3895c5	052604659223

igw-0c90b1c3a09178cf3 / projectIGW01

**Details** **Tags**

**Details**

Internet gateway ID igw-0c90b1c3a09178cf3	State Attached	VPC ID vpc-0c4d80743b459c685   lab-vpc-01	Owner 052604659223
--	-------------------	--	-----------------------

### b. IGW02

Name	Internet gateway ID	State	VPC ID	Owner
projectIGW02	igw-07d205123e4189844	Attached	vpc-08bc2b996409e1952   lab-vpc-02	052604659223
projectIGW01	igw-0c90b1c3a09178cf3	Attached	vpc-0c4d80743b459c685   lab-vpc-01	052604659223
-	igw-e73b758f	Attached	vpc-ae3895c5	052604659223

igw-07d205123e4189844 / projectIGW02

**Details** **Tags**

**Details**

Internet gateway ID igw-07d205123e4189844	State Attached	VPC ID vpc-08bc2b996409e1952   lab-vpc-02	Owner 052604659223
--	-------------------	--	-----------------------

## SS3: Edit Route List

### a. routetable01

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
<input type="checkbox"/> rtb-02c5933d79619342f	vpc-08bc2b996409e1952   lab-vpc-02	No	-	-	052604659223	
<input checked="" type="checkbox"/> projectroute01	rtb-02e3a32fc88080c9a	-	-	Yes	vpc-0c4d80743b459c685   lab-vpc-01	052604659223
<input type="checkbox"/> rtb-055c296e	vpc-ae3895c5	Yes	-	-	052604659223	
<input type="checkbox"/> rtb-081f3970b029f58bf	vpc-0c4d80743b459c685   lab-vpc-01	No	-	-	052604659223	
<input type="checkbox"/> projectroute02	rtb-09a6937ef8ca8cf80	-	-	Yes	vpc-08bc2b996409e1952   lab-vpc-02	052604659223

Route Table: rtb-02e3a32fc88080c9a

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-0c90b1c3a09178cf3	active	No

## b. Routetable02

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
<input type="checkbox"/> rtb-02c5933d79619342f	vpc-08bc2b996409e1952   lab-vpc-02	No	-	-	052604659223	
<input type="checkbox"/> projectroute01	rtb-02e3a32fc88080c9a	-	-	Yes	vpc-0c4d80743b459c685   lab-vpc-01	052604659223
<input type="checkbox"/> rtb-055c296e	vpc-ae3895c5	Yes	-	-	052604659223	
<input type="checkbox"/> rtb-081f3970b029f58bf	vpc-0c4d80743b459c685   lab-vpc-01	No	-	-	052604659223	
<input checked="" type="checkbox"/> projectroute02	rtb-09a6937ef8ca8cf80	-	-	Yes	vpc-08bc2b996409e1952   lab-vpc-02	052604659223

Route Table: rtb-09a6937ef8ca8cf80

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-07d205123e4189844	active	No

## SS4: Subnet List

### a. Subnet01

Subnet List											
	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table	
<input checked="" type="checkbox"/>	projectssubnet01	subnet-028fc463720524b5c	available	vpc-0c4d80743b459c685   lab-vpc-01	172.19.19.0/24	250	-	us-east-2a	use2-az1	rtb-02e3a32fc88080c9a   projectroute01	
<input type="checkbox"/>	projectssubnet02	subnet-0c9bc672da98d2003	available	vpc-08bc2b996409e1952   lab-vpc-02	172.16.16.0/24	250	-	us-east-2b	use2-az2	rtb-09a6937ef8ca8cf80   projectroute02	
<input type="checkbox"/>		subnet-3ab1db76	available	vpc-ae3895c5	172.31.32.0/20	4091	-	us-east-2c	use2-az3	rtb-055c296e	
<input type="checkbox"/>		subnet-48232132	available	vpc-ae3895c5	172.31.16.0/20	4091	-	us-east-2b	use2-az2	rtb-055c296e	
<input type="checkbox"/>		subnet-c5984cae	available	vpc-ae3895c5	172.31.0.0/20	4091	-	us-east-2a	use2-az1	rtb-055c296e	

Subnet: subnet-028fc463720524b5c											
<a href="#">Description</a> <a href="#">Flow Logs</a> <a href="#">Route Table</a> <a href="#">Network ACL</a> <a href="#">Tags</a> <a href="#">Sharing</a>											
Subnet ID	subnet-028fc463720524b5c	State	available	IPV4 CIDR	172.19.19.0/24	Available IPV4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table	
VPC	vpc-0c4d80743b459c685   lab-vpc-01	IPV4 CIDR	172.19.19.0/24	IPv6 CIDR	-	Auto-assign customer-owned	No	Route table	rtb-02e3a32fc88080c9a   projectroute01		
Available IPv4 Addresses	250	IPV6 CIDR	-	Route table	rtb-02e3a32fc88080c9a   projectroute01	Default subnet	No	Route table	rtb-02e3a32fc88080c9a   projectroute01		
Availability Zone	us-east-2a (use2-az1)	Route table	rtb-02e3a32fc88080c9a   projectroute01	Default subnet	No	Auto-assign customer-owned	No	Route table	rtb-02e3a32fc88080c9a   projectroute01		
Network ACL	aci-07b61148b46b9f30f	Default subnet	No	Auto-assign IPv4 address	No	Auto-assign IPv6 address	No	Route table	rtb-02e3a32fc88080c9a   projectroute01		
Auto-assign public IPv4 address	No	Auto-assign IPv4 address	No	Owner	052604659223	Route table	rtb-02e3a32fc88080c9a   projectroute01	Route table	rtb-02e3a32fc88080c9a   projectroute01		
Customer-owned IPv4 pool	-	Route table	rtb-02e3a32fc88080c9a   projectroute01	Route table	rtb-02e3a32fc88080c9a   projectroute01	Default subnet	No	Route table	rtb-02e3a32fc88080c9a   projectroute01		
Outpost ID	-	Route table	rtb-02e3a32fc88080c9a   projectroute01	Route table	rtb-02e3a32fc88080c9a   projectroute01	Auto-assign customer-owned	No	Route table	rtb-02e3a32fc88080c9a   projectroute01		

## b. Subnet02

Subnet List											
	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table	
<input type="checkbox"/>	projectssubnet01	subnet-028fc463720524b5c	available	vpc-0c4d80743b459c685   lab-vpc-01	172.19.19.0/24	250	-	us-east-2a	use2-az1	rtb-02e3a32fc88080c9a   projectroute01	
<input checked="" type="checkbox"/>	projectssubnet02	subnet-0c9bc672da98d2003	available	vpc-08bc2b996409e1952   lab-vpc-02	172.16.16.0/24	250	-	us-east-2b	use2-az2	rtb-09a6937ef8ca8cf80   projectroute02	
<input type="checkbox"/>		subnet-3ab1db76	available	vpc-ae3895c5	172.31.32.0/20	4091	-	us-east-2c	use2-az3	rtb-055c296e	
<input type="checkbox"/>		subnet-48232132	available	vpc-ae3895c5	172.31.16.0/20	4091	-	us-east-2b	use2-az2	rtb-055c296e	
<input type="checkbox"/>		subnet-c5984cae	available	vpc-ae3895c5	172.31.0.0/20	4091	-	us-east-2a	use2-az1	rtb-055c296e	

Subnet: subnet-0c9bc672da98d2003											
<a href="#">Description</a> <a href="#">Flow Logs</a> <a href="#">Route Table</a> <a href="#">Network ACL</a> <a href="#">Tags</a> <a href="#">Sharing</a>											
Subnet ID	subnet-0c9bc672da98d2003	State	available	IPV4 CIDR	172.16.16.0/24	Available IPV4	IPv6 CIDR	Availability Zone	Availability Zone ID	Route table	
VPC	vpc-08bc2b996409e1952   lab-vpc-02	IPV4 CIDR	172.16.16.0/24	IPv6 CIDR	-	Auto-assign customer-owned	No	Route table	rtb-09a6937ef8ca8cf80   projectroute02		
Available IPv4 Addresses	250	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Default subnet	No	Auto-assign IPv4 address	No	Route table	rtb-09a6937ef8ca8cf80   projectroute02		
Availability Zone	us-east-2b (use2-az2)	Default subnet	No	Auto-assign IPv6 address	No	Owner	052604659223	Route table	rtb-09a6937ef8ca8cf80   projectroute02		
Network ACL	aci-0d05831497d1080b7	Auto-assign customer-owned	No	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Route table	rtb-09a6937ef8ca8cf80   projectroute02		
Auto-assign public IPv4 address	No	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Default subnet	No	Route table	rtb-09a6937ef8ca8cf80   projectroute02		
Customer-owned IPv4 pool	-	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Auto-assign customer-owned	No	Route table	rtb-09a6937ef8ca8cf80   projectroute02		
Outpost ID	-	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Route table	rtb-09a6937ef8ca8cf80   projectroute02	Auto-assign IPv4 address	No	Route table	rtb-09a6937ef8ca8cf80   projectroute02		

## SS5: Instance Details

### a. EC2 instance01

**>Password Decryption Successful**  
The password for Instance i-053af5115780669e7 was successfully decrypted.

**Instances (1/2) [Info](#)**

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP
<input checked="" type="checkbox"/> winEC2_01	i-053af5115780669e7	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	No alarms	us-east-2a	–	18.191.4.149	–
<input type="checkbox"/> winEC2_02	i-0eb156892c200f986	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	No alarms	us-east-2b	–	3.133.100.221	–

**Instance: i-053af5115780669e7 (winEC2\_01)**

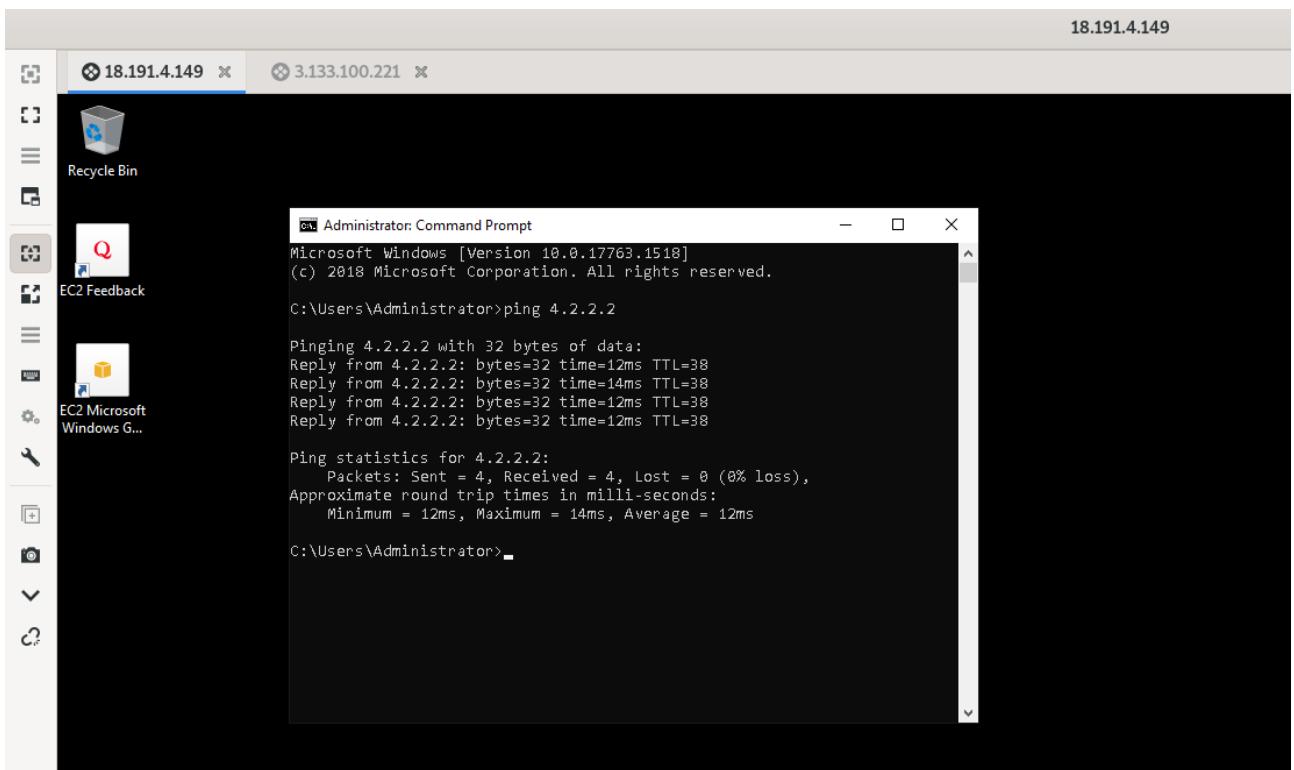
[Details](#) [Security](#) [Networking](#) [Storage](#) [Status Checks](#) [Monitoring](#) [Tags](#)

**Instance summary**

Instance ID i-053af5115780669e7 (winEC2_01)	Public IPv4 address 18.191.4.149   <a href="#">open address</a>	Private IPv4 addresses 172.19.19.99
Instance state <span>Running</span>	Public IPv4 DNS –	Private IPv4 DNS ip-172-19-19-99.us-east-2.compute.internal
Instance type t2.micro	Elastic IP addresses –	VPC ID vpc-0c4d80743b459c685 (lab-vpc-01)
IAM Role –	Subnet ID subnet-028fc463720524b5c (projectsubnet01)	

**Instance details**

Platform windows	AMI ID ami-0354df7841220296c	Monitoring disabled
---------------------	---------------------------------	------------------------



## b. EC2 instance02

>Password Decryption Successful  
The password for Instance i-053af5115780669e7 was successfully decrypted.

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv4 DNS	Public IPv4 ...	Elastic Ip
winEC2_01	i-053af5115780669e7	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	-	18.191.4.149	-
winEC2_02	i-0eb156892c200f986	Running	t2.micro	2/2 checks passed	No alarms	us-east-2b	-	3.133.100.221	-

Instance: i-0eb156892c200f986 (winEC2\_02)

Details Security Networking Storage Status Checks Monitoring Tags

Instance summary Info

Instance ID I-0eb156892c200f986 (winEC2_02)	Public IPv4 address 3.133.100.221 [open address]	Private IPv4 addresses 172.16.16.43
Instance state Running	Public IPv4 DNS -	Private IPv4 DNS ip-172-16-16-43.us-east-2.compute.internal
Instance type t2.micro	Elastic IP addresses -	VPC ID vpc-08bc2b996409e1952 (lab-vpc-02)
IAM Role -	Subnet ID subnet-0c9bc672da98d2003 (projectsubnet02)	

Instance details Info

Platform Windows	AMI ID ami-0354df7841220296c	Monitoring disabled
---------------------	---------------------------------	------------------------

3.133.100.221

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1518]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 4.2.2.2

Pinging 4.2.2.2 with 32 bytes of data:
Reply from 4.2.2.2: bytes=32 time=12ms TTL=38

Ping statistics for 4.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 12ms, Average = 12ms

C:\Users\Administrator>
```

## SS6: Success public, rto private IP

### a. Ping of EC2 instance01

#### a.1 ping of EC2 instance public IP from base machine

The screenshot shows the AWS CloudWatch Instances interface. It lists two instances: **winEC2\_01** (running, t2.micro, Public IPv4 DNS: 18.191.4.149, Private IP: 3.133.100.221) and **winEC2\_02** (running, t2.micro, Public IPv4 DNS: -, Private IP: 3.135.100.221). A terminal window titled "fish /home/milind" is open, showing the command "ping 18.191.4.149" and its output, which includes a packet loss of 100%.

#### a.2 Ping of EC2 instance02 from EC2 instance01

\*Public IP success

\*Private IP failed

The screenshot shows a Windows Command Prompt window with several ping commands issued:

- Ping to **18.191.4.149**: Success (64 bytes, 12ms TTL=38)
- Ping to **3.133.100.221**: Failure (Request timed out)
- Ping to **172.16.16.43**: Success (1ms, 14ms, 12ms)
- Ping to **172.16.16.43** again: Failure (100% loss)

## b. Ping of EC2 instance02

### b.1 Ping of EC2 instance public IP from base machine

The password for instance i-053af5115780669e7 was successfully decrypted.

Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
winEC2_01	i-053af5115780669e7	Running	t2.micro	2/2 checks passed	No alarms	us-east-2a	-	18.191.4.149	-
winEC2_02	i-0eb156892c200f986	Running	t2.micro	2/2 checks passed	No alarms	us-east-2b	-	3.133.100.221	-

Instance: i-0eb156892c200f986 (winEC2\_02)

Details Security Networking Storage Status Checks Monitoring Tags

Public IPv4 address copied

3.133.100.221 [open address]

Public IPv4 DNS -

Elastic IP addresses -

Subnet ID subnet-0c9bc672da98d2003 (projectsubnet02)

Platform windows AMI ID ami-0354df7841220296c Monitoring disabled

```
ping /home/milind
ping /home/milind 80x24
milind@milind-Latitude-3490 ~ ping 3.133.100.221
PING 3.133.100.221 (3.133.100.221) 56(84) bytes of data.
64 bytes from 3.133.100.221: icmp_seq=1 ttl=102 time=247 ms
64 bytes from 3.133.100.221: icmp_seq=2 ttl=102 time=263 ms
64 bytes from 3.133.100.221: icmp_seq=3 ttl=102 time=247 ms
64 bytes from 3.133.100.221: icmp_seq=4 ttl=102 time=250 ms
64 bytes from 3.133.100.221: icmp_seq=5 ttl=102 time=247 ms
64 bytes from 3.133.100.221: icmp_seq=6 ttl=102 time=247 ms
64 bytes from 3.133.100.221: icmp_seq=7 ttl=102 time=236 ms
64 bytes from 3.133.100.221: icmp_seq=8 ttl=102 time=256 ms
64 bytes from 3.133.100.221: icmp_seq=9 ttl=102 time=251 ms
64 bytes from 3.133.100.221: icmp_seq=10 ttl=102 time=247 ms
64 bytes from 3.133.100.221: icmp_seq=11 ttl=102 time=324 ms
64 bytes from 3.133.100.221: icmp_seq=12 ttl=102 time=247 ms
64 bytes from 3.133.100.221: icmp_seq=13 ttl=102 time=269 ms
```

### b.2 Ping of EC2instance01 from EC2instance02

\*Public IP success

\*Private IP failed

```
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.16.1

C:\Users\Administrator>ping 18.191.4.149

Pinging 18.191.4.149 with 32 bytes of data:
Reply from 18.191.4.149: bytes=32 time=1ms TTL=127

Ping statistics for 18.191.4.149:
    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>ping 172.19.19.99

Pinging 172.19.19.99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.19.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Administrator>
```

SS7: Peering with required and Acceptor

Peering connection name tag: projectpeer

Select a local VPC to peer with:

CIDR	Status	Status Reason
172.19.0.0/16	associated	

Select another VPC to peer with:

Account: My account

Region: This region (us-east-2)

CIDR	Status	Status Reason
172.16.0.0/16	associated	

Name	Peering Connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
projectpeer	pxc-0af37390186f19a95	Active	vpc-0c4d80743b4...	vpc-08bc2b996409e...	172.19.0.0/16	172.16.0.0/16	052604659223	052604659223

Peer Connection: pxc-0af37390186f19a95

Description	DNS	Route Tables	Tags
Requester VPC owner: 052604659223 Requester VPC ID: vpc-0c4d80743b459c685 Requester VPC Region: Ohio (us-east-2) Requester VPC CIDRs: 172.19.0.0/16 VPC Peering Connection: pxc-0af37390186f19a95 Expiration time: -	Acceptor VPC owner: 052604659223 Acceptor VPC ID: vpc-08bc2b996409e1952 Acceptor VPC Region: Ohio (us-east-2) Acceptor VPC CIDRs: 172.16.0.0/16 Peering connection status: Active		

## Routes added in both the route tables

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
projectroute01	rtb-02e3a32fc88080c9a	-	-	Yes	vpc-0c4d80743b459c685   lab-vpc-01	052604659223
	rtb-055c296e	-	-	Yes	vpc-ae3895c5	052604659223
	projectroute02	rtb-09a6937ef8ca8cf0	-	-	vpc-08bc2b996409e1952   lab-vpc-02	052604659223

Destination	Target	Status	Propagated
172.19.0.0/16	local	active	No
0.0.0.0/0	igw-0c90b1c3a09178cf3	active	No
172.16.0.0/16	pxc-0af37390186f19a95	active	No

The screenshot shows the AWS VPC console interface. At the top, there's a navigation bar with tabs like 'Create route table' and 'Actions'. Below it is a search bar and a table listing three route tables:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
projectroute01	rtb-02e3a32fc88080c9a	-	-	Yes	vpc-0c4d80743b459c685   lab-vpc-01	052604659223
projectroute02	rtb-055c296e	-	-	Yes	vpc-ae3895c5	052604659223
projectroute02	rtb-09a6937ef8ca8cf80	-	-	Yes	vpc-0bc2b996409e1952   lab-vpc-02	052604659223

Below the table, a specific route table (rtb-09a6937ef8ca8cf80) is selected. The 'Routes' tab is active, showing the following routes:

Destination	Target	Status	Propagated
172.16.0.0/16	local	active	No
0.0.0.0/0	igw-07d205123e4189844	active	No
172.19.0.0/16	pcx-0af37390186f19a95	active	No

## SS8: Success of private IP

The screenshot shows a Windows Command Prompt window titled 'Administrator: Command Prompt' with the IP address '18.191.4.149' at the top. The window displays the following ping results:

```

18.191.4.149

Administrator: Command Prompt
Ping statistics for 3.133.100.221:
    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>ping 172.16.16.43

Pinging 172.16.16.43 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 172.16.16.43:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\Administrator>ping 172.16.16.43

Pinging 172.16.16.43 with 32 bytes of data:
Reply from 172.16.16.43: bytes=32 time=1ms TTL=128

Ping statistics for 172.16.16.43:
    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>

```

3.133.100.221

18.191.4.149 3.133.100.221

Recycle Bin

EC2 Feedback

EC2 Microsoft Windows G...

Administrator: Command Prompt

```
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>tracert 172.19.19.99

Tracing route to 172.19.19.99 over a maximum of 30 hops
  1      1 ms      <1 ms      <1 ms  172.19.19.99

Trace complete.

C:\Users\Administrator>ping 172.19.19.99

Pinging 172.19.19.99 with 32 bytes of data:
Reply from 172.19.19.99: bytes=32 time=1ms TTL=128

Ping statistics for 172.19.19.99:
  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>
```

18.191.4.149

18.191.4.149 3.133.100.221

Recycle Bin

EC2 Feedback

EC2 Microsoft Windows G...

Administrator: Command Prompt

```
Connection-specific DNS Suffix . : us-east-2.compute.internal
Link-local IPv6 Address . . . . . : fe80::50fe:414a:bf86:bb6a%4
IPv4 Address . . . . . : 172.19.19.99
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.19.19.1

C:\Users\Administrator>ping 172.16.16.43

Pinging 172.16.16.43 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 172.16.16.43:
  Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
  Control-C
^C
C:\Users\Administrator>ping 3.133.100.221

Pinging 3.133.100.221 with 32 bytes of data:
Reply from 3.133.100.221: bytes=32 time=1ms TTL=127

Ping statistics for 3.133.100.221:
  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>
```

```

Administrator: Command Prompt
IPv4 Address . . . . . : 172.16.16.43
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.16.1

C:\Users\Administrator>
C:\Users\Administrator>ping 172.19.19.99

Pinging 172.19.19.99 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.19.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 18.191.4.149

Pinging 18.191.4.149 with 32 bytes of data:
Reply from 18.191.4.149: bytes=32 time=1ms TTL=127

Ping statistics for 18.191.4.149:
    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>

```

## Project 2 week 4: IAM

### Task1 Creating user without permissions – IAM password policy check

#### SS1: User summary with all tab information

Add user

**User details**

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name:  [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
 

Provides access by 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

**Require password reset:**

User must create a new password at next sign-in  
 Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

**Next: Permissions**

Add user

**Review**

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

**User details**

User name	Pratik
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

**Permissions summary**

The user shown above will be added to the following groups.

Type	Name
Managed policy	<a href="#">IAMUserChangePassword</a>

**Tags**

No tags were added.

**Create user**

You must change your password to continue

AWS account 052604659223

IAM user name Pratik

Old password  (Redacted)

New password  (Redacted)

Retype new password  (Redacted)

[Sign in using your user email](#)

English ▾

Terms of Use Privacy Policy © 1996-2020, Amazon Web Services, Inc. or its affiliates.

IAM Management Console

Pratik @ 0526-0465-9223 ▾ Global ▾ Support ▾

**IAM dashboard**

We encountered the following errors while processing your request:

- User: arn:aws:iam::052604659223:user:Pratik is not authorized to perform: iam:GetAccountSummary on resource: \*
- User: arn:aws:iam::052604659223:user:Pratik is not authorized to perform: iam>ListAccountMfa on resource: \*

We encountered the following errors while processing your request:

- User: arn:aws:iam::052604659223:user:Pratik is not authorized to perform: iam:GetAccountSummary on resource: \*
- User: arn:aws:iam::052604659223:user:Pratik is not authorized to perform: iam>ListAccountMfa on resource: \*

**Additional information**

IAM documentation  
Videos, IAM release history and additional resources  
Tools ▾  
Web identity federation playground  
Policy simulator  
**Quick links**  
My access key

**IAM resources**

**Best practices**

- Grant least privilege access [\(P\)](#). Establishing a principle of least privilege ensures that identities are only permitted to perform the most minimal set of functions necessary to fulfill a specific task, while balancing usability and efficiency.
- Disable unnecessary permissions. If you no longer need a permission for a user, group, or role, you can remove it. This applies to AWS services and applications, as well as AWS Organizations, where you can configure your identity source in AWS Single Sign-On.
- Enable MFA. For extra security, we recommend that you require multi-factor authentication (MFA) for all users.
- Rotate credentials regularly. Change your own passwords and access keys regularly, and make sure that all users in your account do as well.
- Enable IAM Access Analyzer. Enable IAM Access Analyzer to analyze public, cross-account, and cross-organization access.

[Learn more about all security best practices](#) [\(P\)](#)

**What's new**

Learn about the latest releases for AWS Identity & Access Management (IAM)

- Amazon Detective introduces IAM Role Session Analysis
- Now gain longer access to your AWS resources when switching roles in the AWS Management Console
- Manage your AWS Identity and Access Management quotas with AWS Service Quotas
- Tighten S3 permissions for your IAM users and roles using access history of S3 actions
- EC2 Instance Connect now supports Attribute Based Access Control (ABAC)
- Discover, review, and remediate unintended access to S3 buckets shared through S3 Access Points

Launch instance wizard

Pratik @ 0526-0465-9223 ▾ Onivo ▾ Support ▾

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 1: Choose an Amazon Machine Image (AMI)**

**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

	Search by Systems Manager parameter
Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-03657b65516ab7912 (64-bit x86) / ami-023b120e01f4779c1 (64-bit Arm)	1 to 18 AMIs
Amazon Linux 2018.03.0 (HVM), SSD Volume Type - ami-027cab9a7bf0155df	
Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0a54aef4ef365f881 (64-bit x86) / ami-0e05c6e81b5100c04 (64-bit Arm)	
SUSE Linux Enterprise Server 15 SP2 (HVM), SSD Volume Type - ami-03f4c416f489596a3 (64-bit x86) / ami-0d24f1c1b096d2b03 (64-bit Arm)	
Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-07efac79022b0107 (64-bit x86) / ami-00bcac5ae8c849ed7 (64-bit Arm)	

Select 64-bit (x86)  
Select 64-bit (Arm)  
Select 64-bit (x86)  
Select 64-bit (Arm)  
Select 64-bit (x86)  
Select 64-bit (Arm)

The screenshot shows the AWS S3 Management Console. In the top right corner, there is 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, the main interface shows the "S3 buckets" section. A red horizontal bar spans across the page with the text "Error" and "Access Denied". At the bottom, there is a table header for "Bucket name", "Access", "Region", and "Date created".

## Task2 Creating user without IAM password policy

### SS2: User summary with all tab information

The first screenshot shows the "Set user details" step of the "Add user" wizard. It includes fields for "User name" (set to "ketan"), "Access type" (checkboxes for "Programmatic access" and "AWS Management Console access" are checked), "Console password" (radio button selected for "Custom password"), and "Require password reset" (checkbox unchecked). The second screenshot shows the "Review" step, where 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." Both screenshots show the "Next: Permissions" button at the bottom.

It did not asked for password chang as we have unchecked the password policy

Task3 Create a user with S3 full access  
SS3: User summary

Screenshot of the AWS IAM User Summary page for user 'shreyansh'. The page shows the user's ARN, path, and creation time. It includes tabs for Permissions, Groups, Tags, Security credentials, and Access Advisor. Under Permissions, it lists 'Permissions policies (1 policy applied)' and shows the attached policy 'AmazonS3FullAccess' which is an AWS managed policy.

Screenshot of the AWS IAM Add User 'Review' step. The user details section shows 'User name': 'shreyansh', 'AWS access type': 'Programmatic access and AWS Management Console access', 'Console password type': 'Custom', 'Require password reset': 'No', and 'Permissions boundary': 'Permissions boundary is not set'. The 'Permissions summary' section shows the attached policy 'AmazonS3FullAccess'. The 'Tags' section indicates 'No tags were added'. At the bottom, there are 'Cancel', 'Previous', and 'Create user' buttons.

Screenshot of the AWS S3 Management Console. The left sidebar shows 'Amazon S3' with options like Buckets, Batch operations, Access analyzer for S3, and Block public access (account settings). The main area displays 'S3 buckets' with a search bar and a table showing four buckets: 'mil06061983', 'mil0versioning06061983', 'milowebhosting01', and 's3-letsupgradedemo'. The table includes columns for Bucket name, Access, Region, and Date created.

## Task4 Create a group with EC2 full access

### SS3: User summary

IAM Management Console

IAM > Groups > developers

**Summary**

Group ARN: am:aws:iam::052604659223:group/developers

Users (in this group): 2

Path: /

Creation Time: 2020-10-23 21:43 UTC+0530

**Users** **Permissions** **Access Advisor**

This view shows all users in this group: 2 Users

User	Actions
▲ Prash	Remove User from Group
▲ shreyansh	Remove User from Group

Remove Users from Group | Add Users to Group

IAM > Groups > developers

**Summary**

Group ARN: am:aws:iam::052604659223:group/developers

Users (in this group): 2

Path: /

Creation Time: 2020-10-23 21:43 UTC+0530

**Users** **Permissions** **Access Advisor**

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

**Attach Policy**

Policy Name	Actions
AmazonEC2FullAccess	Show Policy   Detach Policy   Simulate Policy

Inline Policies

Now user has access to EC2 full access also

Launch Instance wizard

https://us-east-2.console.aws.amazon.com/ec2/v2/home?region=us-east-2#LaunchInstanceWizard:

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

**Step 2: Choose an Instance Type**

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation ShowHide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, ~1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
	t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
	t3	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

## Task5: Add user to a group and check if user policy and group policy is reflecting on the user

### SS5: User summary with permissions

**Add user**

**Set user details**

User name: manish [Add another user](#)

Select AWS access type

Access type:  Programmatic access  AWS Management Console access

Console password:  Autogenerated password  Custom password   
  Show password

Require password reset:  User must create a new password at next sign-in Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

\* Required [Cancel](#) [Next: Permissions](#)

**Add user**

**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
ketan	None	None
Prash	developers	IAMUserChangePassword
<b>shreyansh</b>	developers	AmazonS3FullAccess

\* Set permissions boundary [Cancel](#) [Previous](#) [Next: Tags](#)

**Identity and Access Management (IAM)**

**Users > manish**

**Summary**

User ARN: arn:aws:iam::052604059223:user/manish [Edit](#)

Path: /

Creation time: 2020-10-23 22:02 UTC+0530

**Permissions** [Groups \(1\)](#) [Tags](#) [Security credentials](#) [Access Advisor](#)

**Permissions policies (2 policies applied)**

Policy name	Policy type
Attached directly	AWS managed policy
AmazonS3FullAccess	AWS managed policy
Attached from group	AWS managed policy from group developers
AmazonEC2FullAccess	AWS managed policy from group developers

**Permissions boundary (not set)**

IAM Management Console

<https://console.aws.amazon.com/iam/home?region=us-east-2#users>

Add user Delete user

Find users by username or access key

Showing 4 results

User name	Groups	Access key age	Password age	Last activity	MFA
ketan	None	Today	Today	Today	Not enabled
manish	developers	None	Today	None	Not enabled
Pratik	developers	Today	Today	Today	Not enabled
shreyansh	developers	Today	Today	Today	Not enabled

Launch instance wizard

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized for different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: i2.micro (1 ECUs, 1 vCPUs, 2.5 GHz, 1.0 GB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (ODB)	EBS-Optimized Available	Network Performance	IPv6 Support
i2	i2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
i2	<b>i2.micro</b> <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
i2	i2.small	1	2	EBS only	-	Low to Moderate	Yes
i2	i2.medium	2	4	EBS only	-	Low to Moderate	Yes
i2	i2.large	2	8	EBS only	-	Low to Moderate	Yes
i2	i2.xlarge	4	16	EBS only	-	Moderate	Yes
i2	i2.2xlarge	8	32	EBS only	-	Moderate	Yes
i3	i3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
i3	i3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
i3	i3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
i3	i3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
i3	i3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
i3	i3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
i3	i3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

S3 Management Console

Access S3-backed file shares on premises and reduce local storage costs using AWS Storage Gateway. 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.

Discover the console

All access types

Buckets

Create Bucket Edit public access settings Empty Delete

S3 buckets

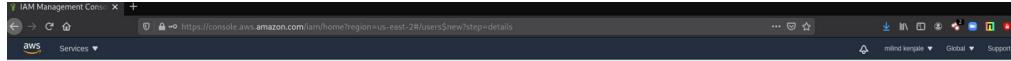
Search for buckets

4 Buckets 2 Regions

Bucket name	Access	Region	Date created
mliv0001983	US East (Ohio)	Oct 4, 2020 12:31:36 PM GMT+0530	
mlivversioning0001983	US East (Ohio)	Oct 4, 2020 1:38:34 PM GMT+0530	
mlivwebhosting01	Objects can be public	Oct 16, 2020 8:14:04 PM GMT+0530	
s3-lensupgradedemo	US East (Ohio)	Oct 10, 2020 1:02:49 PM GMT+0530	

## Task6: Copying policy from existing users

SS7: Attach user summary of the user from which you create a new user



Add user Step 1 of 5

### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name  [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

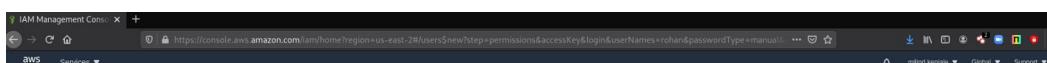
Enables a password that allows users to sign-in to the AWS Management Console.

#### Console password Autogenerated password Custom password

\*\*\*\*\*

Show password

[Require password reset](#)  User must create a new password at next sign-in



Add user Step 2 of 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
ankur	developers	None
ketan	None	None
manish	developers	AmazonS3FullAccess
Pratik	developers	IAMUserChangePassword
rakesh	None	None
shreyansh	developers	AmazonS3FullAccess



Permissions		Groups (1)	Tags	Security credentials	Access Advisor
<a href="#">Add permissions</a> <a href="#">Add inline policy</a>					
Policy name					Policy type
Attached directly	<a href="#">AmazonS3FullAccess</a>				AWS managed policy
Attached from group	<a href="#">AmazonEC2FullAccess</a>				AWS managed policy from group developers
Permissions boundary (not set)					

SS8: Login as this user show that this policy is in effect

S3 Management Console

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.](#)

**S3 buckets**

[Create bucket](#) [Edit public access settings](#) [Empty](#) [Delete](#)

Bucket name	Access	Region	Date created
milo06061983	Objects can be public	US East (Ohio)	Oct 4, 2020 12:31:36 PM GMT+0530
miloverseiong06061983	Bucket and objects not public	US East (Ohio)	Oct 4, 2020 1:38:34 PM GMT+0530
milowebhosting01	Objects can be public	US East (N. Virginia)	Oct 16, 2020 8:14:04 PM GMT+0530
s3-letsupgradedemo	Bucket and objects not public	US East (Ohio)	Oct 10, 2020 1:02:49 PM GMT+0530

**4 Buckets 2 Regions**

Launch instance wizard

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

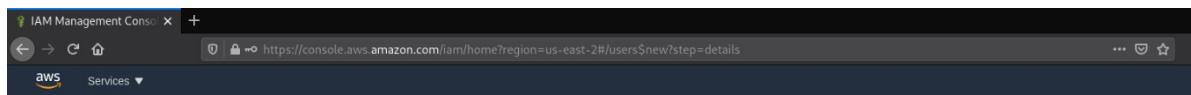
Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (~ ECUs, 1 vCPUs, 2.5 GHz, ~ 1 GiB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
t2	<b>t2.micro</b> <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.2xlarge	8	32	EBS only	Yes	Up to 5 Gigabit	Yes

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

## Task7: Add user to a group in the process of creating a user



### Add user

#### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[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.

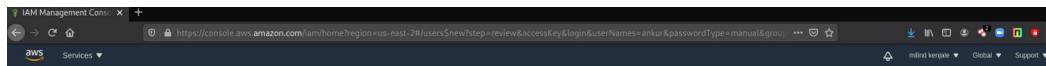
Console password\*  Autogenerated password

Custom password

Show password

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

Users automatically get the **IAMUserChangePassword** policy to allow them to change their own password.



### Add user

#### Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

#### User details

User name	ankur
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

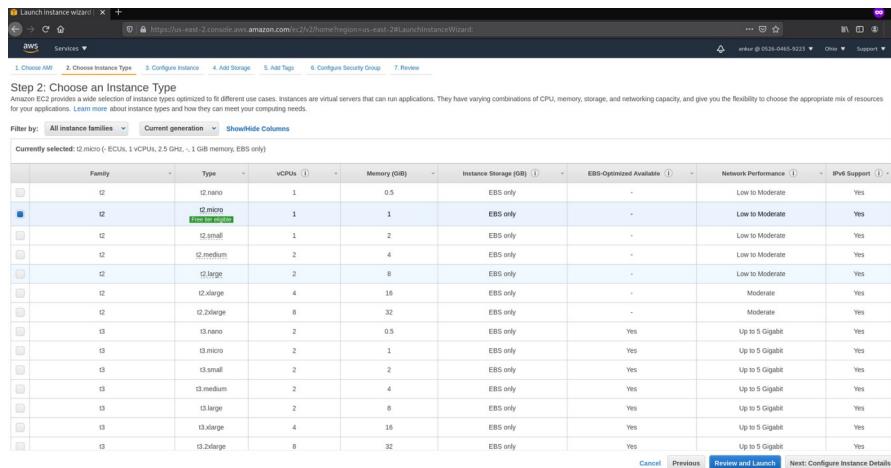
#### Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	developers

#### Tags

No tags were added.



## Task8: Setting Password policy

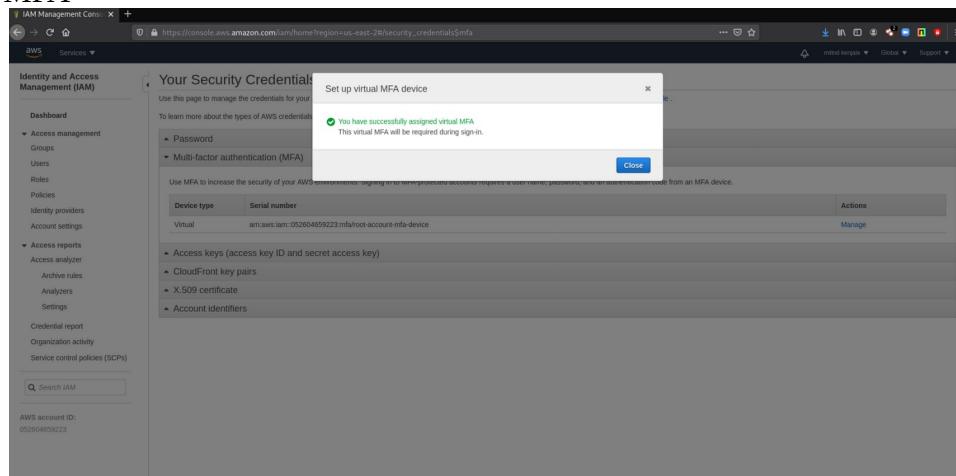
The screenshot shows the 'Set password policy' configuration page in the AWS IAM Management Console. It includes fields for minimum password length (10 characters), password complexity requirements (uppercase, lowercase, numbers, non-alphanumeric, and expiration), and user permissions (administrator reset, password change, and password reuse prevention). A note at the bottom indicates that users must remember up to 5 previous passwords.

The screenshot shows the 'Password policy updated' confirmation message in the AWS IAM Management Console. It lists the updated password policy rules: minimum length of 10 characters, requiring uppercase, lowercase, numbers, and non-alphanumeric characters, and a 90-day expiration. It also notes that users can change their own password and prevent password reuse. The message is displayed over the 'Identity and Access Management (IAM)' dashboard.

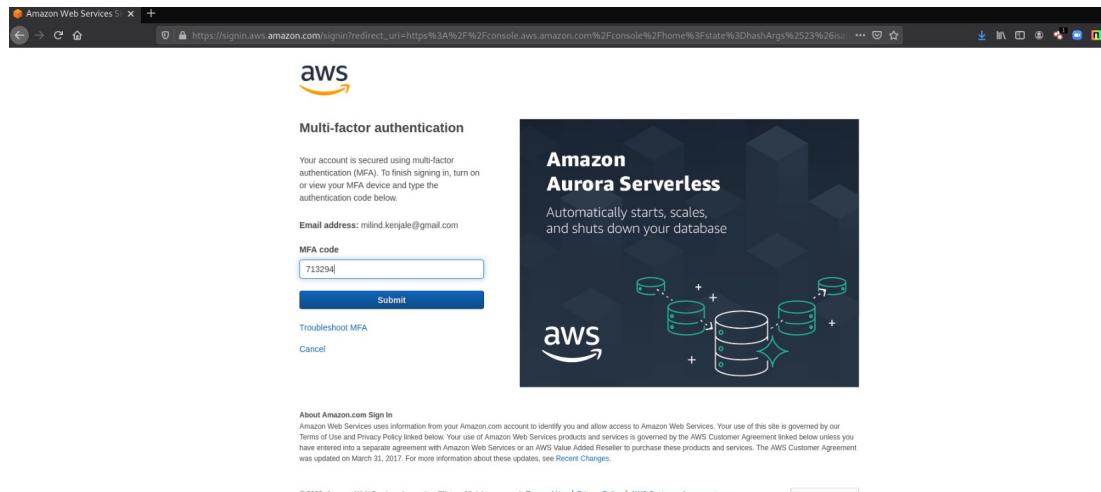
The screenshot shows the 'Add user' configuration page in the AWS IAM Management Console. It allows creating a new user with the name 'rakesh'. The 'Select AWS access type' section offers 'Programmatic access' (using access key ID and secret access key) and 'AWS Management Console access' (using a password). The 'Console password' field is filled with '\*\*\*\*\*'. The 'Require password reset' checkbox is checked, indicating users must change their password at sign-in.

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

### SS1: enable MFA



### SS2: login screen for MFA



=====  
=====