

1) Create a VPC with IP of 172.18.0.0/16 then add tags “Env” and “Dev”. (In N.Virginia)

The screenshot displays the AWS Management Console interface for the 'us-east-1' region. The left-hand navigation pane shows the 'Virtual private cloud' section expanded, with 'Your VPCs' selected. The main content area, titled 'Your VPCs (1/1)', contains a table listing the VPCs. A single VPC, 'vpctest', is listed with the environment tag 'Dev' and the IP address '172.18.0.0/16'. Below the table, the 'Details' tab for the VPC 'vpc-0b7516caec034453b' is shown. The details are organized into a grid:

| Details | | | |
|---|---|---|---|
| VPC ID vpc-0b7516caec034453b | State Available | DNS hostnames Disabled | DNS resolution Enabled |
| Tenancy Default | DHCP option set dopt-0141f1574c9926180 | Main route table rtb-096980ad505d2a969 / Default | Main network ACL acl-0e928c62dc35f5b5a |
| Default VPC No | IPv4 CIDR 172.18.0.0/16 | IPv6 pool - | IPv6 CIDR (Network border group) - |
| Network Address Usage metrics Disabled | Route 53 Resolver DNS Firewall rule groups - | Owner ID 342634125439 | |

The bottom of the console shows the footer with '© 2023, Amazon Web Services India Private Limited or its affiliates.' and the date '17/01/2023'.

2) Create 4 subnets in same VPC(172.18.0.0/16) select different availability zone for each subnet. Add tags “Env” and “Dev”.

The screenshot shows the AWS Management Console interface for the 'Subnets (4)' page. The left sidebar contains a navigation menu with categories: Virtual private cloud, Security, and Network Analysis. The main content area displays a table of subnets. The table has columns: Name, Subnet ID, VPC, IPv4 CIDR, Available IPv4 addresses, and Availability Zone. There are 4 subnets listed: sub1, sub2, sub3, and sub4, each in a different availability zone (us-east-1a, us-east-1b, us-east-1c, us-east-1d). A 'Create subnet' button is located in the top right corner. The bottom of the screen shows the Windows taskbar with various application icons and the system clock.

| Name | Subnet ID | VPC | IPv4 CIDR | Available IPv4 a... | Availability Zone |
|------|--------------------------|--------------------------------|---------------|---------------------|-------------------|
| sub1 | subnet-0785a4eecb4c081eb | vpc-0b7516caec034453b vpc... | 172.18.0.0/24 | 250 | us-east-1a |
| sub2 | subnet-0756a31b485af80da | vpc-0b7516caec034453b vpc... | 172.18.1.0/24 | 251 | us-east-1b |
| sub3 | subnet-02e8e795898c17228 | vpc-0b7516caec034453b vpc... | 172.18.2.0/24 | 250 | us-east-1c |
| sub4 | subnet-0b65dfe956443e128 | vpc-0b7516caec034453b vpc... | 172.18.3.0/24 | 251 | us-east-1d |

- 3) Create route table and add subnets in both the route table.
First two subnets in default route table and other two subnets in another route table.

The screenshot shows the AWS Management Console for the us-east-1 region. The left sidebar contains navigation links for VPC dashboard, EC2 Global View, and various VPC services. The main content area displays the 'Route tables (1/2)' page. A table lists two route tables: 'Default' and 'route-table-1'. The 'Default' route table is selected, and its details are shown below. The 'Routes' tab is active, displaying a table of routes for the 'Default' route table.

| Name | Route table ID | Explicit subnet associations | Main | VPC | Owner ID |
|---|-----------------------|------------------------------|------|---------------------------------|--------------|
| <input checked="" type="checkbox"/> Default | rtb-096980ad505d2a969 | 2 subnets | Yes | vpc-0b7516caec034453b vpctest | 342634125439 |
| <input type="checkbox"/> route-table-1 | rtb-04ae60f6a9dd0b6df | 2 subnets | No | vpc-0b7516caec034453b vpctest | 342634125439 |

| Destination | Target | Status | Propagated |
|---------------|-----------------------|--------|------------|
| ::/0 | igw-05f00ce0e552ca789 | Active | No |
| 0.0.0.0/0 | igw-05f00ce0e552ca789 | Active | No |
| 172.18.0.0/16 | local | Active | No |

4) Adding subnets in the 2nd route table

The screenshot displays the AWS Management Console interface for the 'Route tables (1/2)' page. The left sidebar shows the navigation menu with categories like 'Virtual private cloud', 'Security', and 'Network Analysis'. The main content area shows a list of route tables. The 'route-table-1' is selected, and the 'Subnet associations' tab is active. The 'Explicit subnet associations (2)' section shows two subnets associated with the route table: 'subnet-02e8e795898c17228 / sub3' with IPv4 CIDR '172.18.2.0/24' and 'subnet-0b65dfe956443e128 / sub4' with IPv4 CIDR '172.18.3.0/24'. Below this, the 'Subnets without explicit associations (0)' section is shown, indicating that no subnets are currently associated with the route table without explicit associations.

| Name | Route table ID | Explicit subnet associations | Main | VPC | Owner ID |
|---------------|-----------------------|------------------------------|------|---------------------------------|--------------|
| Default | rtb-096980ad505d2a969 | 2 subnets | Yes | vpc-0b7516caec034453b vpctest | 342634125439 |
| route-table-1 | rtb-04ae60f6a9dd0b6df | 2 subnets | No | vpc-0b7516caec034453b vpctest | 342634125439 |

rtb-04ae60f6a9dd0b6df / route-table-1

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (2)

Find subnet association

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---------------------------------|---------------|-----------|
| subnet-02e8e795898c17228 / sub3 | 172.18.2.0/24 | - |
| subnet-0b65dfe956443e128 / sub4 | 172.18.3.0/24 | - |

Subnets without explicit associations (0)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Find subnet association

Subnet ID | IPv4 CIDR | IPv6 CIDR

5) Create internet gateway and add tags and attach to the VPC.

The screenshot shows the AWS Management Console for the us-east-1 region. The left sidebar contains navigation links for VPC dashboard, EC2 Global View, and various VPC services. The main content area is titled 'Internet gateways (1/1) Info'. It features a table with the following data:

| Name | Internet gateway ID | State | VPC ID | Owner |
|------|-----------------------|----------|---------------------------------|--------------|
| IG-1 | igw-05f00ce0e552ca789 | Attached | vpc-0b7516caec034453b vpctest | 342634125439 |

Below the table, the details for the selected gateway 'igw-05f00ce0e552ca789 / IG-1' are shown. The details section includes the following information:

- Internet gateway ID: igw-05f00ce0e552ca789
- State: Attached
- VPC ID: vpc-0b7516caec034453b | vpctest
- Owner: 342634125439

6) Add internet gateway in route table.

The screenshot displays the AWS Management Console interface for the 'Route tables' section. The left-hand navigation pane shows the 'Virtual private cloud' section expanded, with 'Route tables' selected. The main content area shows a list of route tables. The 'ROUTE1' route table is selected, and the 'Routes' tab is active, displaying two routes.

| Name | Route table ID | Explicit subnet associations | Main | VPC | Owner ID |
|---------|-----------------------|------------------------------|------|-----------------------------------|--------------|
| default | rtb-079cfac99678c82 | - | Yes | vpc-0079ce47a19aa2d48 VPCTEST | 342634125439 |
| ROUTE1 | rtb-07f57d42f331017ca | 2 subnets | No | vpc-0079ce47a19aa2d48 VPCTEST | 342634125439 |
| - | rtb-0a245f97b614dbc4b | - | Yes | vpc-0542512aec31e7036 VPC88-... | 342634125439 |

| Destination | Target | Status | Propagated |
|---------------|-----------------------|--------|------------|
| 0.0.0.0/0 | igw-0b2267300b40d69c3 | Active | No |
| 172.18.0.0/16 | local | Active | No |

7) Open EC2 and create instances (VM-Server) which don't have public IP.

The screenshot displays the AWS Management Console interface for EC2 instances. The left sidebar shows navigation options like EC2 Dashboard, Events, Tags, Limits, Instances, Images, Elastic Block Store, and Network & Security. The main content area shows a list of instances under the heading 'Instances (1/2)'. Two instances are listed: 'VM jump server' and 'VM-server'. The 'VM-server' instance is selected, and its details are shown in the 'Instance: i-0744b856c65946e75 (VM-server)' panel. The instance is in a 'Running' state, located in 'us-east-1c' availability zone, with a private IP address of '172.18.2.153' and subnet ID 'subnet-02e8e795898c17228'. The instance type is 't2.micro'.

| Name | Instance ID | Instance state | Availability Zone | Private IP address | Subnet IDs |
|----------------|---------------------|----------------|-------------------|--------------------|--------------------------|
| VM jump server | i-04569a66348ef6f7b | Running | us-east-1a | 172.18.0.39 | subnet-0785a4eeb4c081eb |
| VM-server | i-0744b856c65946e75 | Running | us-east-1c | 172.18.2.153 | subnet-02e8e795898c17228 |

Instance: i-0744b856c65946e75 (VM-server)

| Details | Security | Networking | Storage | Status checks | Monitoring | Tags |
|--|--|---|---|---|----------------------|------|
| Instance summary | | | | | | |
| Instance ID i-0744b856c65946e75 (VM-server) | Public IPv4 address - | Private IPv4 addresses 172.18.2.153 | Instance state Running | Private IP DNS name (IPv4 only) ip-172-18-2-153.ec2.internal | Public IPv4 DNS - | |
| IP name: ip-172-18-2-153.ec2.internal | Instance type t2.micro | Elastic IP addresses - | Private IP DNS name (IPv4 only) ip-172-18-2-153.ec2.internal | Instance type t2.micro | Public IPv4 DNS - | |
| Answer private resource DNS name IPv4 (A) | VPC ID vpc-0b7516cae034453b (vpctest) | AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more | Subnet ID subnet-02e8e795898c17228 (sub3) | Auto Scaling Group name - | | |
| Auto-assigned IP address - | | | | | | |
| IAM Role - | | | | | | |

8) Create instance 2nd (VM-JUMP-SERVER) which have public IP. In this select free Linux then add key file. Also add subnet-1 and enable auto assign public IP in network setting. Add security group and launch the instance.

The screenshot displays the AWS Management Console interface for the 'Instances' page. The left sidebar shows navigation options like 'EC2 Dashboard', 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main content area shows a list of instances, with 'VM jump server' selected. Below the list, the 'Security' tab for instance 'i-04569a66348ef6f7b' is open, showing details such as IAM Role, Owner ID, Launch time, Security groups, and Inbound/Outbound rules. The instance is running in the us-east-1a availability zone with a public IP address of 172.18.0.39. The security group is 'sg-0ea23f47ba6858b98 (launch-wizard-1)'. The inbound rules allow ICMP and TCP port 22 access from 0.0.0.0/0.

| Name | Instance ID | Instance state | Availability Zone | Private IP address | Subnet IDs |
|----------------|---------------------|----------------|-------------------|--------------------|--------------------------|
| VM jump server | i-04569a66348ef6f7b | Running | us-east-1a | 172.18.0.39 | subnet-0785a4eeb4c081eb |
| VM-server | i-0744b856c65946e75 | Running | us-east-1c | 172.18.2.153 | subnet-02e8e795898c17228 |

Instance: i-04569a66348ef6f7b (VM jump server)

Security details

IAM Role: --

Owner ID: 342634125439

Launch time: Tue Jan 17 2023 15:15:44 GMT+0530 (India Standard Time)

Security groups: sg-0ea23f47ba6858b98 (launch-wizard-1)

Inbound rules

| Name | Security group rule ID | Port range | Protocol | Source | Security groups | Description |
|------|------------------------|------------|----------|-----------|-----------------|-------------|
| -- | sgr-0f5788228b7ec2c7c | All | ICMP | 0.0.0.0/0 | launch-wizard-1 | -- |
| -- | sgr-0a2d06c90d62f682c | 22 | TCP | 0.0.0.0/0 | launch-wizard-1 | -- |

Outbound rules

| Name | Security group rule ID | Port range | Protocol | Destination | Security groups |
|------|------------------------|------------|----------|-------------|-----------------|
|------|------------------------|------------|----------|-------------|-----------------|

9) Create instance 2nd (VM-SERVER) which don't have public IP. In this select free Linux then add key file. Also add subnet-3 and disable auto assign public IP in network setting. Add security group and launch the instance.

The screenshot displays the AWS Management Console interface for the EC2 service. The main content area shows the 'Instances (1/2)' page. A table lists the instances, with 'VM-server' (Instance ID: i-0744b856c65946e75) selected. The instance is in the 'Running' state, located in the 'us-east-1c' availability zone, and has a private IP address of 172.18.2.153. The 'Security' tab is active, showing the instance's security details. The IAM Role is '-', the Owner ID is 342634125439, and the Launch time is Tue Jan 17 2023 15:18:27 GMT+0530 (India Standard Time). The Security groups section shows 'sg-0ea23f47ba6858b98 (launch-wizard-1)'. The Inbound rules section shows two rules: one for ICMP and one for TCP port 22, both from 0.0.0.0/0. The Outbound rules section is also visible.

| Name | Instance ID | Instance state | Availability Zone | Private IP address | Subnet IDs |
|----------------|---------------------|----------------|-------------------|--------------------|--------------------------|
| VM jump server | i-04569a66348ef6f7b | Running | us-east-1a | 172.18.0.39 | subnet-0785a4eeb4c081eb |
| VM-server | i-0744b856c65946e75 | Running | us-east-1c | 172.18.2.153 | subnet-02e8e795898c17228 |

Instance: i-0744b856c65946e75 (VM-server)

Security details

IAM Role: -

Owner ID: 342634125439

Launch time: Tue Jan 17 2023 15:18:27 GMT+0530 (India Standard Time)

Security groups

sg-0ea23f47ba6858b98 (launch-wizard-1)

Inbound rules

| Name | Security group rule ID | Port range | Protocol | Source | Security groups |
|------|------------------------|------------|----------|-----------|-----------------|
| - | sgr-0f5788228b7ec2c7c | All | ICMP | 0.0.0.0/0 | launch-wizard-1 |
| - | sgr-0a2d06c90d62f682c | 22 | TCP | 0.0.0.0/0 | launch-wizard-1 |

Outbound rules

| Name | Security group rule ID | Port range | Protocol | Destination | Security groups |
|------|------------------------|------------|----------|-------------|-----------------|
|------|------------------------|------------|----------|-------------|-----------------|

10) ping VM2 using jump server

- Logging in into VM2 with help of jump server and keys

```

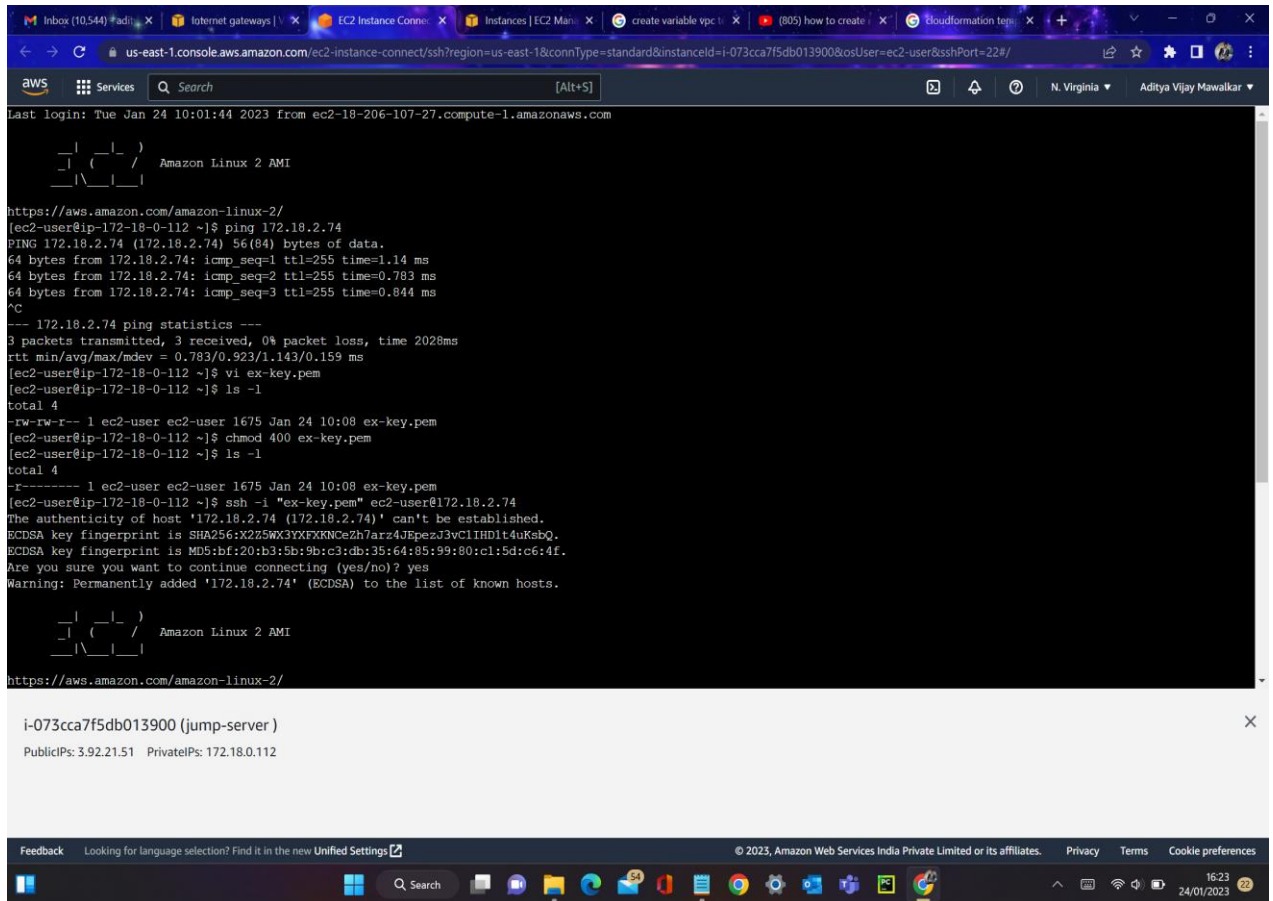
Select ec2-user@ip-172-18-2-153:~
┌─[ec2-user]─┐
└─[ec2-user]─┘ Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-18-0-217 ~]$ ping 172.18.2.153
PING 172.18.2.153 (172.18.2.153) 56(84) bytes of data.
64 bytes from 172.18.2.153: icmp_seq=1 ttl=255 time=1.52 ms
64 bytes from 172.18.2.153: icmp_seq=2 ttl=255 time=1.05 ms
64 bytes from 172.18.2.153: icmp_seq=3 ttl=255 time=1.03 ms
64 bytes from 172.18.2.153: icmp_seq=4 ttl=255 time=1.07 ms
64 bytes from 172.18.2.153: icmp_seq=5 ttl=255 time=0.967 ms
64 bytes from 172.18.2.153: icmp_seq=6 ttl=255 time=0.992 ms
^Z
[1]+  Stopped                  ping 172.18.2.153
[ec2-user@ip-172-18-0-217 ~]$ vi my_key.pem
[ec2-user@ip-172-18-0-217 ~]$ ls
my_key.pem
[ec2-user@ip-172-18-0-217 ~]$ chmod 400 my_key.pem
[ec2-user@ip-172-18-0-217 ~]$ ls -l
total 4
-r----- 1 ec2-user ec2-user 1680 Jan 17 10:53 my_key.pem
[ec2-user@ip-172-18-0-217 ~]$ ssh -i "my_key.pem" ec2-user@172.18.2.153
The authenticity of host '172.18.2.153 (172.18.2.153)' can't be established.
ECDSA key fingerprint is SHA256:0+JpGFnORP3q6qI3yH9jG7J1t3jIjQlg344MF4VJ+Q.
ECDSA key fingerprint is MD5:61:2f:04:ef:f4:27:53:10:a4:01:6c:d7:28:e1:83:c9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.18.2.153' (ECDSA) to the list of known hosts.
Last login: Tue Jan 17 09:58:15 2023 from 172.18.0.39

┌─[ec2-user]─┐
└─[ec2-user]─┘ Amazon Linux 2 AMI

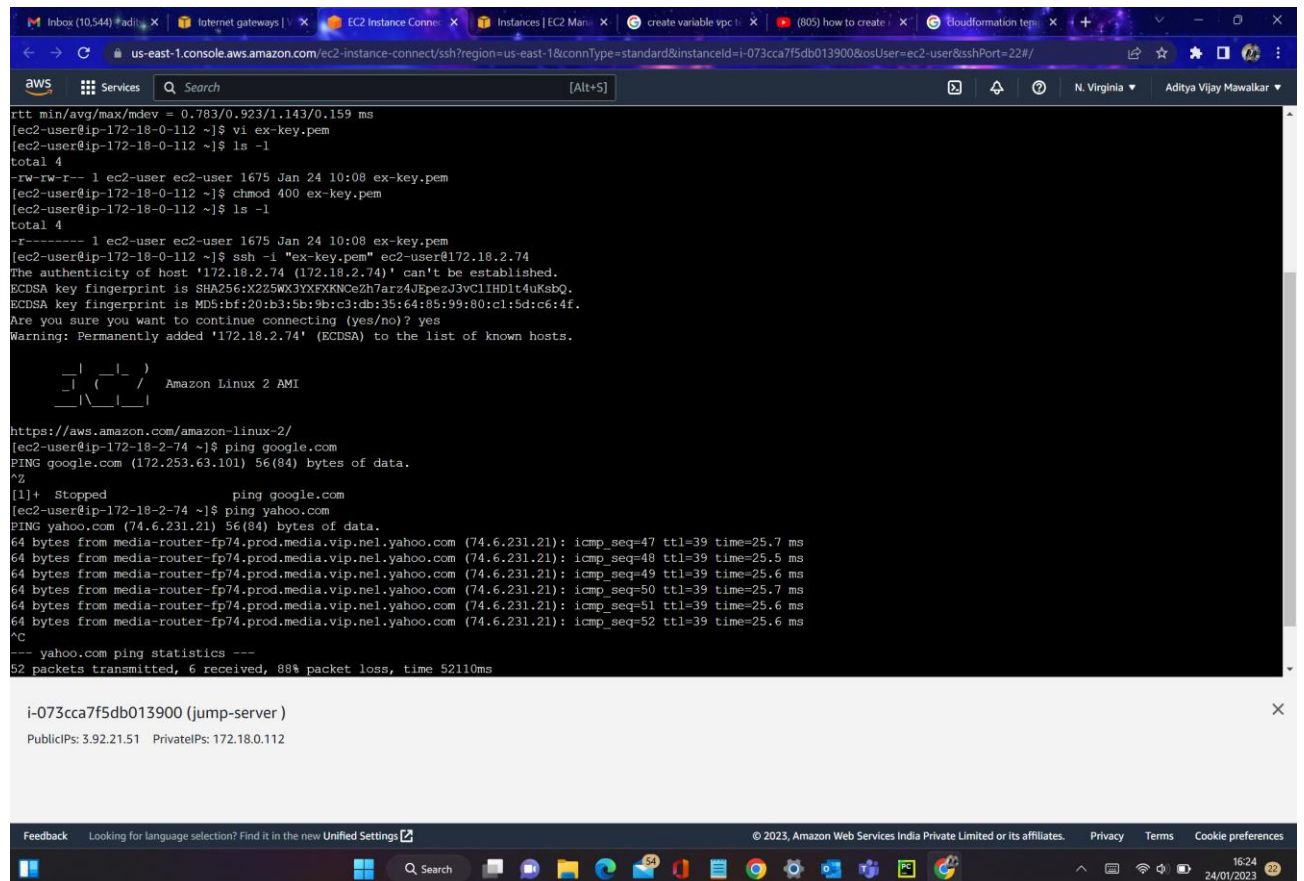
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-18-2-153 ~]$
```

11) Successfully logged in to the VM 2 using Jump server.



```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-073cca7f5db013900&osUser=ec2-user&sshPort=22#/  
Last login: Tue Jan 24 10:01:44 2023 from ec2-18-206-107-27.compute-1.amazonaws.com  
  
  _  _  _  _  
 _/  _/  _/  _/  Amazon Linux 2 AMI  
 _/  _/  _/  _/  
  
https://aws.amazon.com/amazon-linux-2/  
(ec2-user@ip-172-18-0-112 ~)$ ping 172.18.2.74  
PING 172.18.2.74 (172.18.2.74) 56(84) bytes of data:  
64 bytes from 172.18.2.74: icmp_seq=1 ttl=255 time=1.14 ms  
64 bytes from 172.18.2.74: icmp_seq=2 ttl=255 time=0.783 ms  
64 bytes from 172.18.2.74: icmp_seq=3 ttl=255 time=0.844 ms  
^C  
--- 172.18.2.74 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2028ms  
rtt min/avg/max/mdev = 0.783/0.923/1.143/0.159 ms  
(ec2-user@ip-172-18-0-112 ~)$ vi ex-key.pem  
(ec2-user@ip-172-18-0-112 ~)$ ls -l  
total 4  
-rw-rw-r-- 1 ec2-user ec2-user 1675 Jan 24 10:08 ex-key.pem  
(ec2-user@ip-172-18-0-112 ~)$ chmod 400 ex-key.pem  
(ec2-user@ip-172-18-0-112 ~)$ ls -l  
total 4  
-r----- 1 ec2-user ec2-user 1675 Jan 24 10:08 ex-key.pem  
(ec2-user@ip-172-18-0-112 ~)$ ssh -i "ex-key.pem" ec2-user@172.18.2.74  
The authenticity of host '172.18.2.74 (172.18.2.74)' can't be established.  
ECDSA key fingerprint is SHA256:X225W3YXFXKNCe2h7ars4JFpezu3vCIHHD1t4uKsBQ.  
ECDSA key fingerprint is MD5:b1:20:b3:5b:9b:c3:db:35:64:85:99:80:c1:5d:c6:4f.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '172.18.2.74' (ECDSA) to the list of known hosts.  
  
  _  _  _  _  
 _/  _/  _/  _/  Amazon Linux 2 AMI  
 _/  _/  _/  _/  
  
https://aws.amazon.com/amazon-linux-2/  
  
i-073cca7f5db013900 (jump-server)  
PublicIPs: 3.92.21.51 PrivateIPs: 172.18.0.112
```

12) Pinged the VM2 using jump server



The screenshot shows the AWS Management Console interface with a terminal window open. The terminal displays the following commands and output:

```
rtt min/avg/max/mdev = 0.783/0.923/1.143/0.159 ms
[ec2-user@ip-172-18-0-112 ~]$ vi ex-key.pem
[ec2-user@ip-172-18-0-112 ~]$ ls -l
total 4
-rw-rw-r-- 1 ec2-user ec2-user 1675 Jan 24 10:08 ex-key.pem
[ec2-user@ip-172-18-0-112 ~]$ chmod 400 ex-key.pem
[ec2-user@ip-172-18-0-112 ~]$ ls -l
total 4
-r----- 1 ec2-user ec2-user 1675 Jan 24 10:08 ex-key.pem
[ec2-user@ip-172-18-0-112 ~]$ ssh -i "ex-key.pem" ec2-user@172.18.2.74
The authenticity of host '172.18.2.74 (172.18.2.74)' can't be established.
ECDSA key fingerprint is SHA256:X2Z5WX3YXFKNCEzh7ar24JEpzJ3vC1IHD1t4uKsbQ.
ECDSA key fingerprint is MD5:bf:20:b3:5b:9b:c3:db:35:64:85:99:80:c1:5d:c6:4f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.18.2.74' (ECDSA) to the list of known hosts.

 _ _ _ _ _
| | | | |
|_|_|_|_|_|
Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-18-2-74 ~]$ ping google.com
PING google.com (172.253.63.101) 56(84) bytes of data.
64
^C
[1] + Stopped ping google.com
[ec2-user@ip-172-18-2-74 ~]$ ping yahoo.com
PING yahoo.com (74.6.231.21) 56(84) bytes of data.
64 bytes from media-router-fp74.prod.media.vip.net.yahoo.com (74.6.231.21): icmp_seq=47 ttl=39 time=25.7 ms
64 bytes from media-router-fp74.prod.media.vip.net.yahoo.com (74.6.231.21): icmp_seq=48 ttl=39 time=25.5 ms
64 bytes from media-router-fp74.prod.media.vip.net.yahoo.com (74.6.231.21): icmp_seq=49 ttl=39 time=25.6 ms
64 bytes from media-router-fp74.prod.media.vip.net.yahoo.com (74.6.231.21): icmp_seq=50 ttl=39 time=25.7 ms
64 bytes from media-router-fp74.prod.media.vip.net.yahoo.com (74.6.231.21): icmp_seq=51 ttl=39 time=25.6 ms
64 bytes from media-router-fp74.prod.media.vip.net.yahoo.com (74.6.231.21): icmp_seq=52 ttl=39 time=25.6 ms
^C
--- yahoo.com ping statistics ---
52 packets transmitted, 6 received, 88% packet loss, time 52110ms
```

Below the terminal output, the instance details for **i-073cca7f5db013900 (jump-server)** are shown, including PublicIPs: 3.92.21.51 and PrivateIPs: 172.18.0.112.