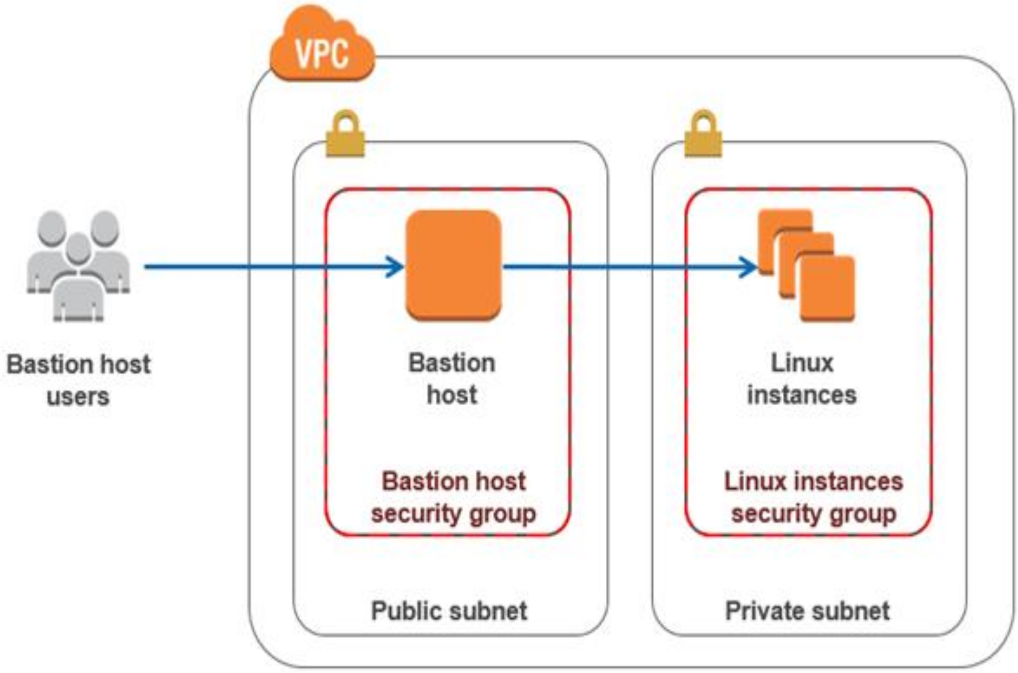
Use SSH to securely transfer files between two private Ips

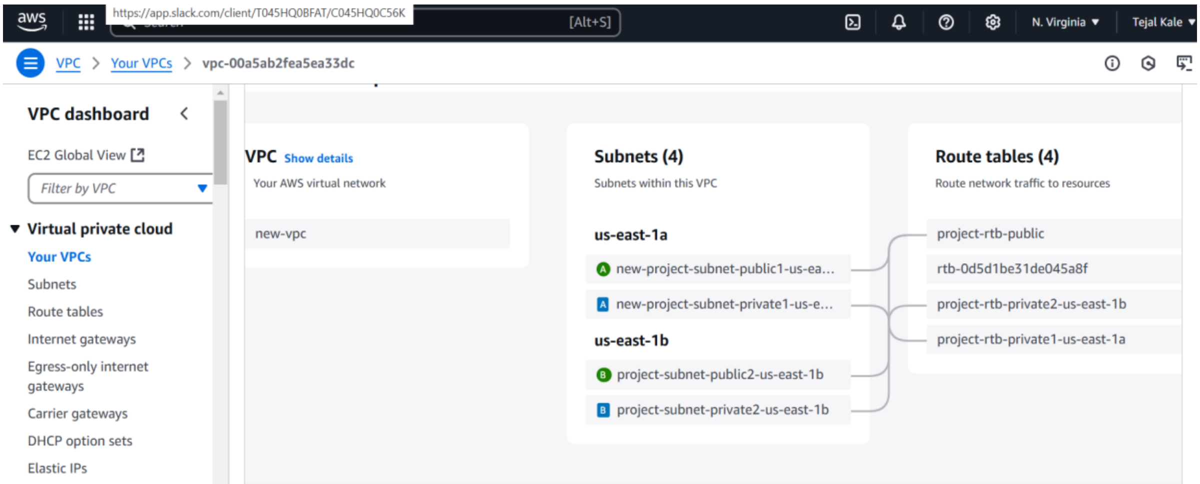
Objective

- Set up two private EC2 instances:
    - **Web Server**: Configured to serve as a web server.
    - **Client**: Configured to securely transfer files to/from the web server.
- Use a **Bastion Host** to access these private instances and facilitate secure file transfer using SSH.
- Architecture



Step 1: Launch EC2 Instances.

Launch three EC2 instances in the same VPC and different subnets:



VPC Show details
Your AWS virtual network
new-vpc

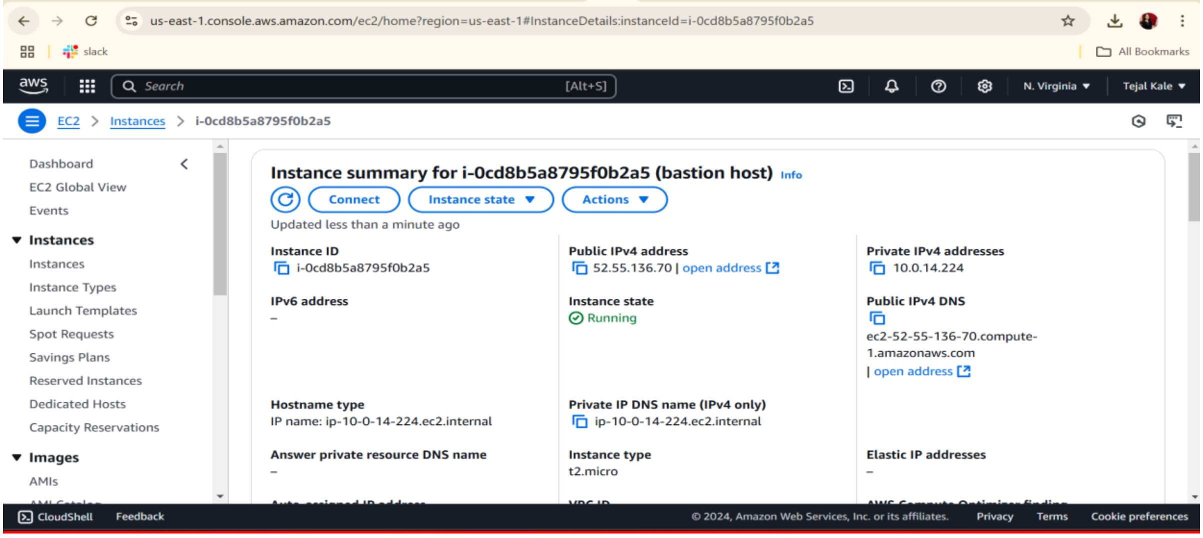
Subnets (4)
Subnets within this VPC

us-east-1a
- new-project-subnet-public1-us-ea...
- new-project-subnet-private1-us-e...

us-east-1b
- project-subnet-public2-us-east-1b
- project-subnet-private2-us-east-1b

Route tables (4)
Route network traffic to resources
- project-rtb-public
- rtb-0d5d1be31de045a8f
- project-rtb-private2-us-east-1b
- project-rtb-private1-us-east-1a

Step 2: Launch Bastion Host: Assign a public IP and public subnet.

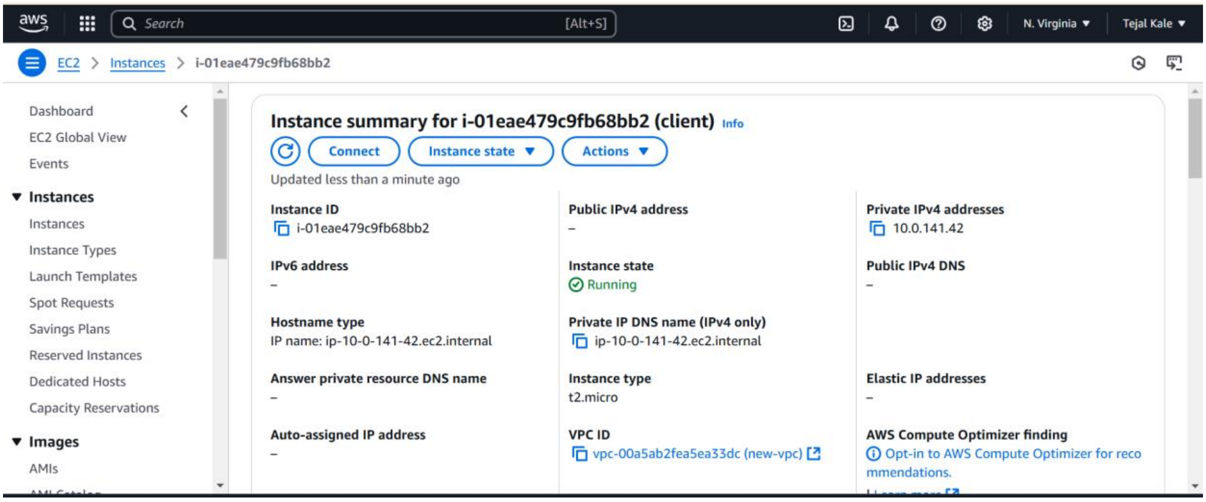


Instance summary for i-0cd8b5a8795f0b2a5 (bastion host) Info

Updated less than a minute ago

Instance ID i-0cd8b5a8795f0b2a5	**Public IPv4 address** 52.55.136.70 | open address	**Private IPv4 addresses** 10.0.14.224
IPv6 address –	**Instance state** Running	**Public IPv4 DNS** ec2-52-55-136-70.compute-1.amazonaws.com | open address
Hostname type IP name: ip-10-0-14-224.ec2.internal	**Private IP DNS name (IPv4 only)** ip-10-0-14-224.ec2.internal	
Answer private resource DNS name –	**Instance type** t2.micro	**Elastic IP addresses** –

Step 3: Launch Client: Private IP only and private subnet.

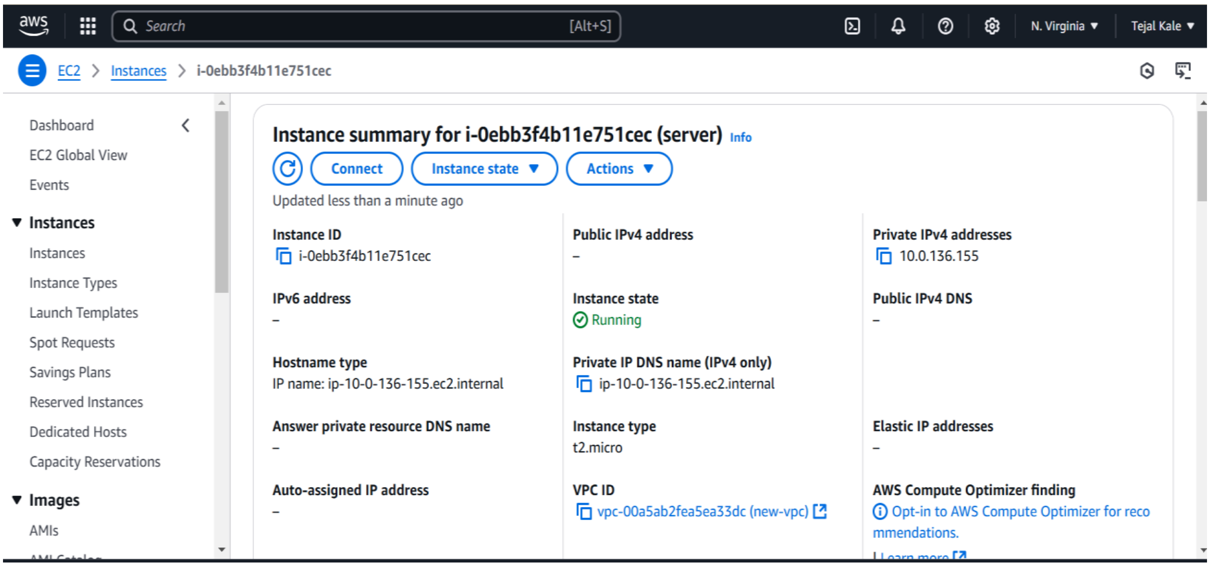


Instance summary for i-01eae479c9fb68bb2 (client) Info

Updated less than a minute ago

Instance ID i-01eae479c9fb68bb2	**Public IPv4 address** –	**Private IPv4 addresses** 10.0.141.42
IPv6 address –	**Instance state** Running	**Public IPv4 DNS** –
Hostname type IP name: ip-10-0-141-42.ec2.internal	**Private IP DNS name (IPv4 only)** ip-10-0-141-42.ec2.internal	
Answer private resource DNS name –	**Instance type** t2.micro	**Elastic IP addresses** –
Auto-assigned IP address –	**VPC ID** vpc-00a5ab2fea5ea33dc (new-vpc)	**AWS Compute Optimizer finding** Opt-in to AWS Compute Optimizer for recommendations.

Step 4: Launch Web Server: Private IP only and private subnet.



Instance summary for i-0ebb3f4b11e751cec (server)

Updated less than a minute ago

Instance ID: i-0ebb3f4b11e751cec

Public IPv4 address: –

Private IPv4 addresses: 10.0.136.155

IPv6 address: –

Instance state: Running

Public IPv4 DNS: –

Hostname type: IP name: ip-10-0-136-155.ec2.internal

Private IP DNS name (IPv4 only): ip-10-0-136-155.ec2.internal

Answer private resource DNS name: –

Instance type: t2.micro

Elastic IP addresses: –

Auto-assigned IP address: –

VPC ID: vpc-00a5ab2fea5ea33dc (new-vpc)

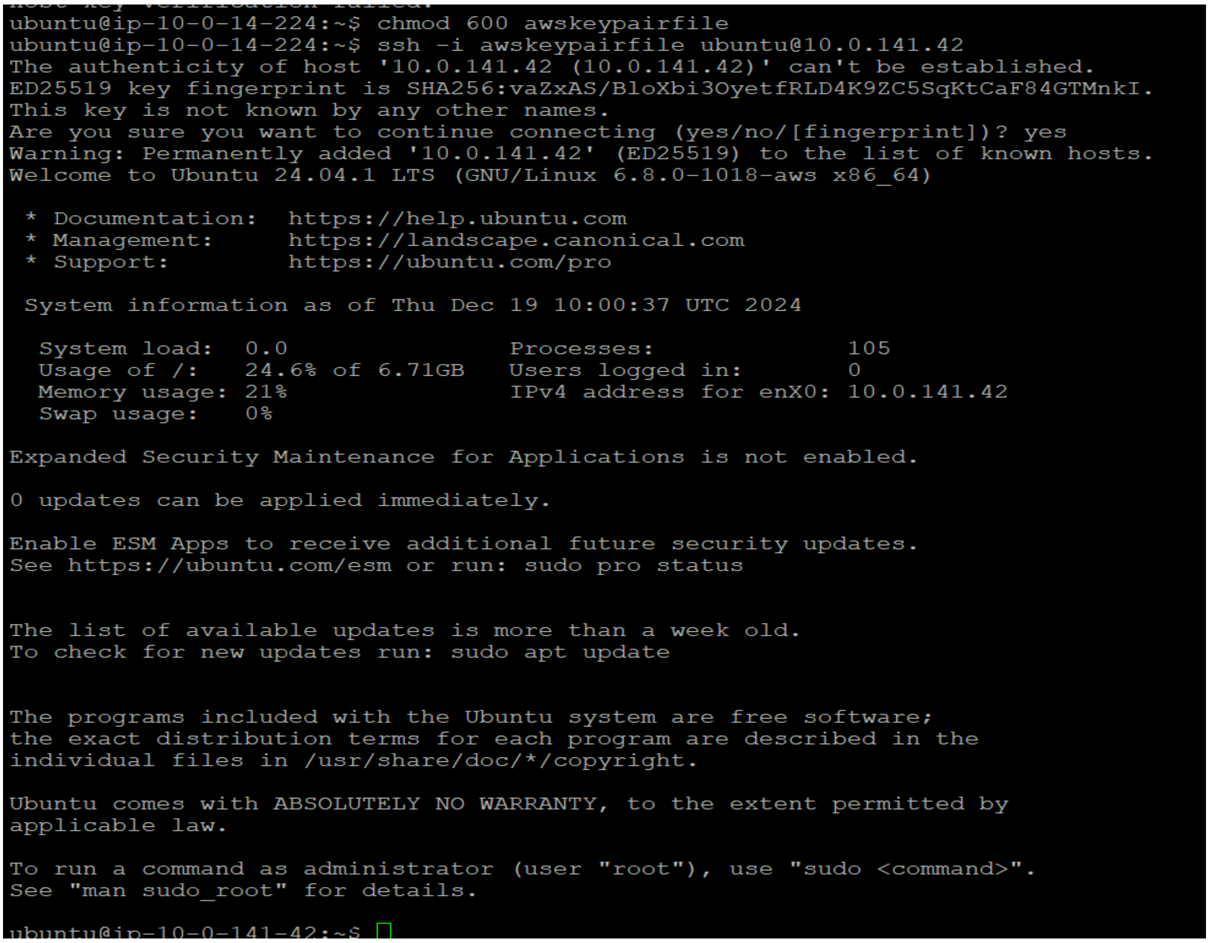
AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations.

Learn more

Step 5: Connect to the Bastion Host:

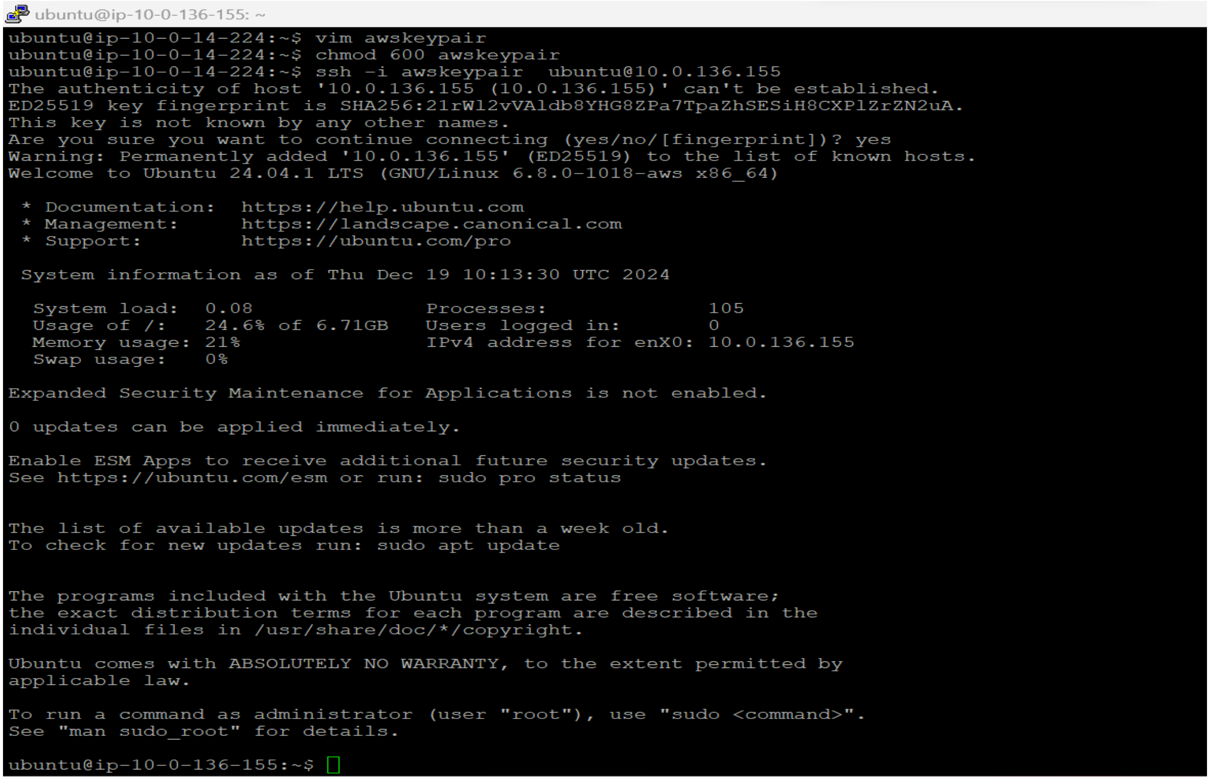
Use PuTTY to connect them with .ppk keypair.

Step 6: Access the Client via the Bastion Host



```
Host key verification failed.
ubuntu@ip-10-0-14-224:~$ chmod 600 awskeypairfile
ubuntu@ip-10-0-14-224:~$ ssh -i awskeypairfile ubuntu@10.0.141.42
The authenticity of host '10.0.141.42 (10.0.141.42)' can't be established.
ED25519 key fingerprint is SHA256:vaZxAS/BloXbi3OyetfRLD4K9ZC5SqKtCaF84GTMnkI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.141.42' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Dec 19 10:00:37 UTC 2024

  System load:  0.0               Processes:             105
  Usage of /:   24.6% of 6.71GB   Users logged in:       0
  Memory usage: 21%               IPv4 address for enX0: 10.0.141.42
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-141-42:~$ 
```

Step 7: Access the Web Server via the Bastion Host.



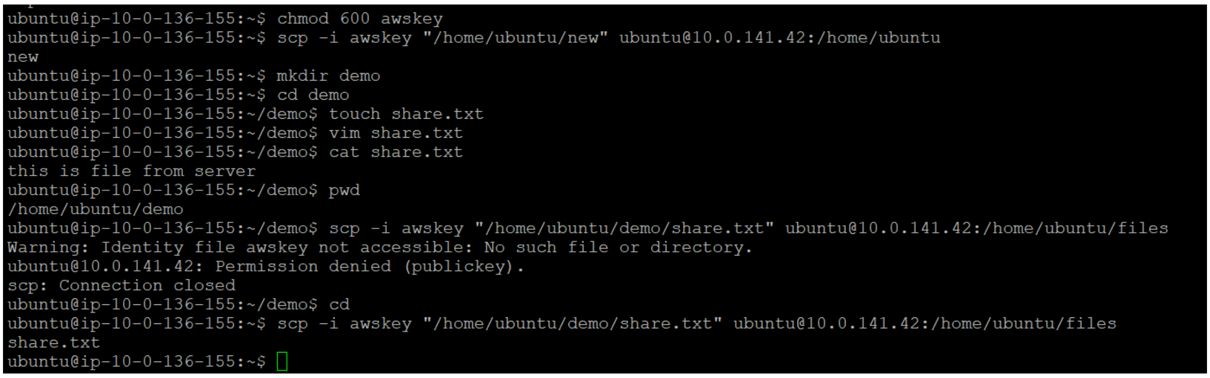
```
ubuntu@ip-10-0-14-224:~$ vim awskeypair
ubuntu@ip-10-0-14-224:~$ chmod 600 awskeypair
ubuntu@ip-10-0-14-224:~$ ssh -i awskeypair  ubuntu@10.0.136.155
The authenticity of host '10.0.136.155 (10.0.136.155)' can't be established.
ED25519 key fingerprint is SHA256:21rWl2vVAldb8YHG8ZPa7TpaZhSESiH8CXPlZrZN2uA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.136.155' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1018-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu Dec 19 10:13:30 UTC 2024

  System load:  0.08               Processes:             105
  Usage of /:   24.6% of 6.71GB    Users logged in:       0
  Memory usage: 21%                IPv4 address for enX0: 10.0.136.155
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-136-155:~$
```

Step 8: Secure File Transfer Between Private Instances

Create a file on the Web Server to transfer to the client .

Use the scp command to transfer the file.

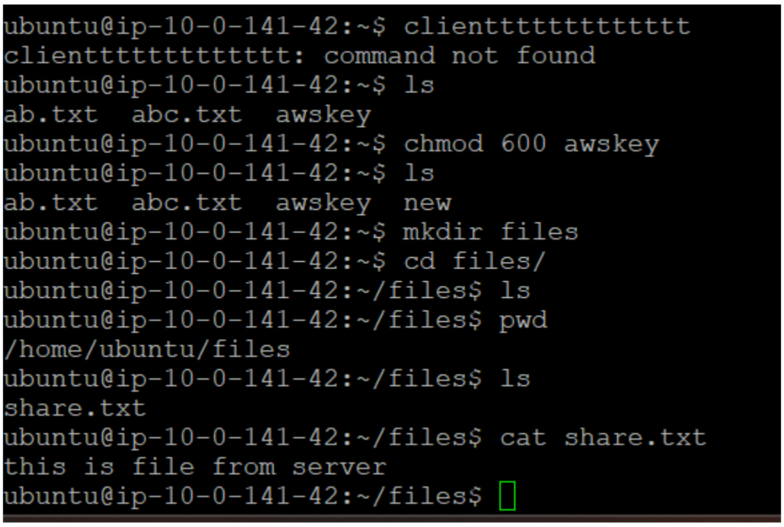
Syntax: scp -i keypair “path/of/file” hostname@private-ip:/destination/path



```
ubuntu@ip-10-0-136-155:~$ chmod 600 awskey
ubuntu@ip-10-0-136-155:~$ scp -i awskey "/home/ubuntu/new" ubuntu@10.0.141.42:/home/ubuntu
new
ubuntu@ip-10-0-136-155:~$ mkdir demo
ubuntu@ip-10-0-136-155:~$ cd demo
ubuntu@ip-10-0-136-155:~/demo$ touch share.txt
ubuntu@ip-10-0-136-155:~/demo$ vim share.txt
ubuntu@ip-10-0-136-155:~/demo$ cat share.txt
this is file from server
ubuntu@ip-10-0-136-155:~/demo$ pwd
/home/ubuntu/demo
ubuntu@ip-10-0-136-155:~/demo$ scp -i awskey "/home/ubuntu/demo/share.txt" ubuntu@10.0.141.42:/home/ubuntu/files
Warning: Identity file awskey not accessible: No such file or directory.
ubuntu@10.0.141.42: Permission denied (publickey).
scp: Connection closed
ubuntu@ip-10-0-136-155:~/demo$ cd
ubuntu@ip-10-0-136-155:~$ scp -i awskey "/home/ubuntu/demo/share.txt" ubuntu@10.0.141.42:/home/ubuntu/files
share.txt
ubuntu@ip-10-0-136-155:~$
```

Step 9: Verify File Transfer on the Client:

Using the Bastion Host, you securely accessed and transferred files between two private EC2 instances.



```
ubuntu@ip-10-0-141-42:~$ clienttttttttttttt
clienttttttttttttt: command not found
ubuntu@ip-10-0-141-42:~$ ls
ab.txt  abc.txt  awskey
ubuntu@ip-10-0-141-42:~$ chmod 600 awskey
ubuntu@ip-10-0-141-42:~$ ls
ab.txt  abc.txt  awskey  new
ubuntu@ip-10-0-141-42:~$ mkdir files
ubuntu@ip-10-0-141-42:~$ cd files/
ubuntu@ip-10-0-141-42:~/files$ ls
ubuntu@ip-10-0-141-42:~/files$ pwd
/home/ubuntu/files
ubuntu@ip-10-0-141-42:~/files$ ls
share.txt
ubuntu@ip-10-0-141-42:~/files$ cat share.txt
this is file from server
ubuntu@ip-10-0-141-42:~/files$ 
```

The Web Server securely transferred files to/from the Client using SCP