LAB 5: *VPC ENDPOINT*

AIM: To create a VPC endpoint for aws.

THEORY:

→ A VPC endpoint enables customers to privately connect to supported AWS services and VPC endpoint services powered by AWS PrivateLink.

→ Amazon VPC instances do not require public IP addresses to communicate with resources of the service.

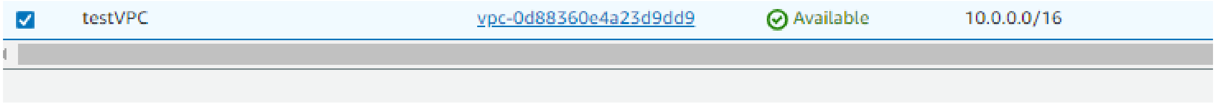
→ Traffic between an Amazon VPC and a service does not leave the Amazon network.

→ VPC endpoints are virtual devices.

→ They are horizontally scaled, redundant, and highly available Amazon VPC components that allow communication between instances in an Amazon VPC and services without imposing availability risks or bandwidth constraints on network traffic.

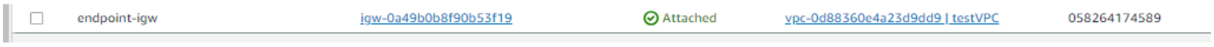
PROCEDURE:

1. Create a VPC.



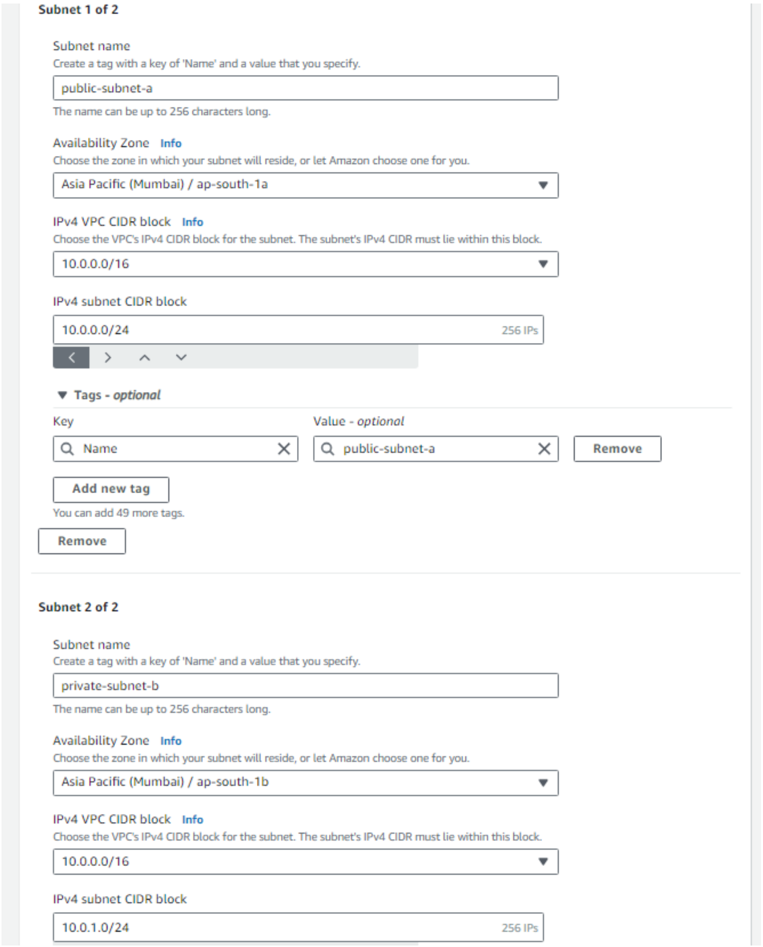
☑	testVPC	vpc-0d88360e4a23d9dd9	✓ Available	10.0.0.0/16

2. Create an internet gateway.



□	endpoint-igw	igw-0a49b0b8f90b53f19	✓ Attached	vpc-0d88360e4a23d9dd9 | testVPC	058264174589

3. Create PUBLIC and PRIVATE SUBNETS.



Subnet 1 of 2

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public-subnet-a
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1a

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.0.0/24 256 IPs

Tags - *optional*

Key	Value - *optional*
Name	public-subnet-a

You can add 49 more tags.

Subnet 2 of 2

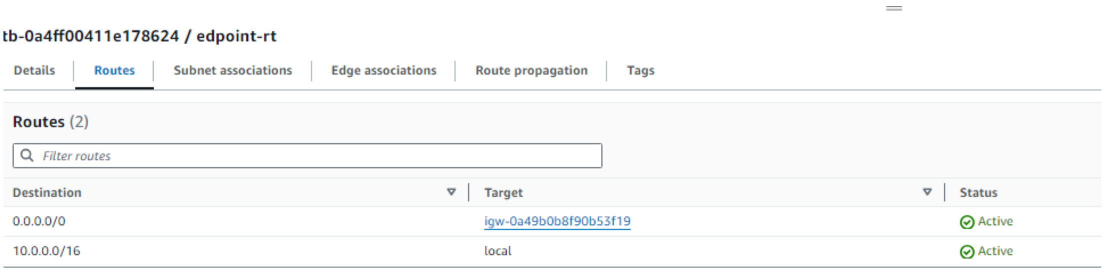
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
private-subnet-b
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Mumbai) / ap-south-1b

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

4. Create a route table and routing for all traffic through the INTERNET GATEWAY.

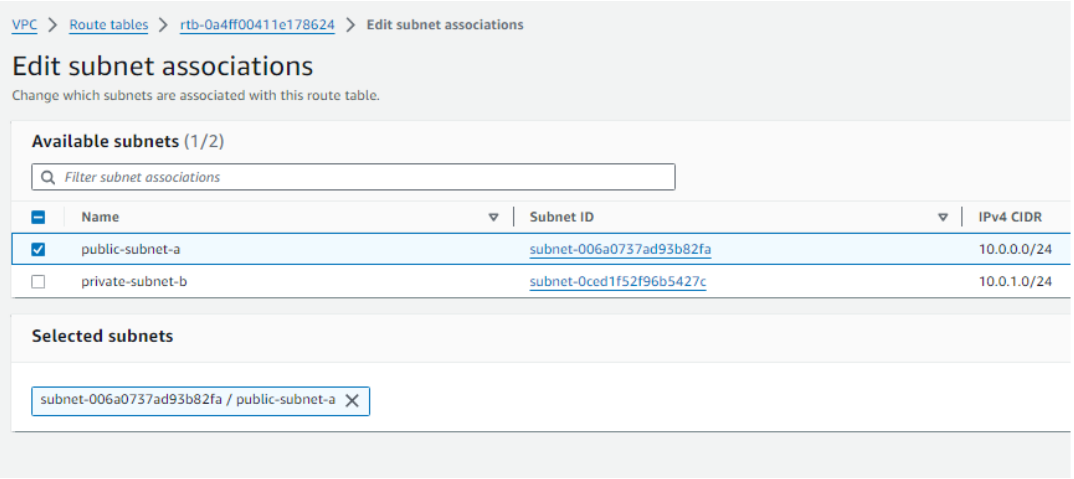


rtb-0a4ff00411e178624 / edpoint-rt

Routes (2)

Destination	Target	Status
0.0.0.0/0	igw-0a49b0b8f90b53f19	Active
10.0.0.0/16	local	Active

5. Edit subnet associations.



VPC > Route tables > rtb-0a4ff00411e178624 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

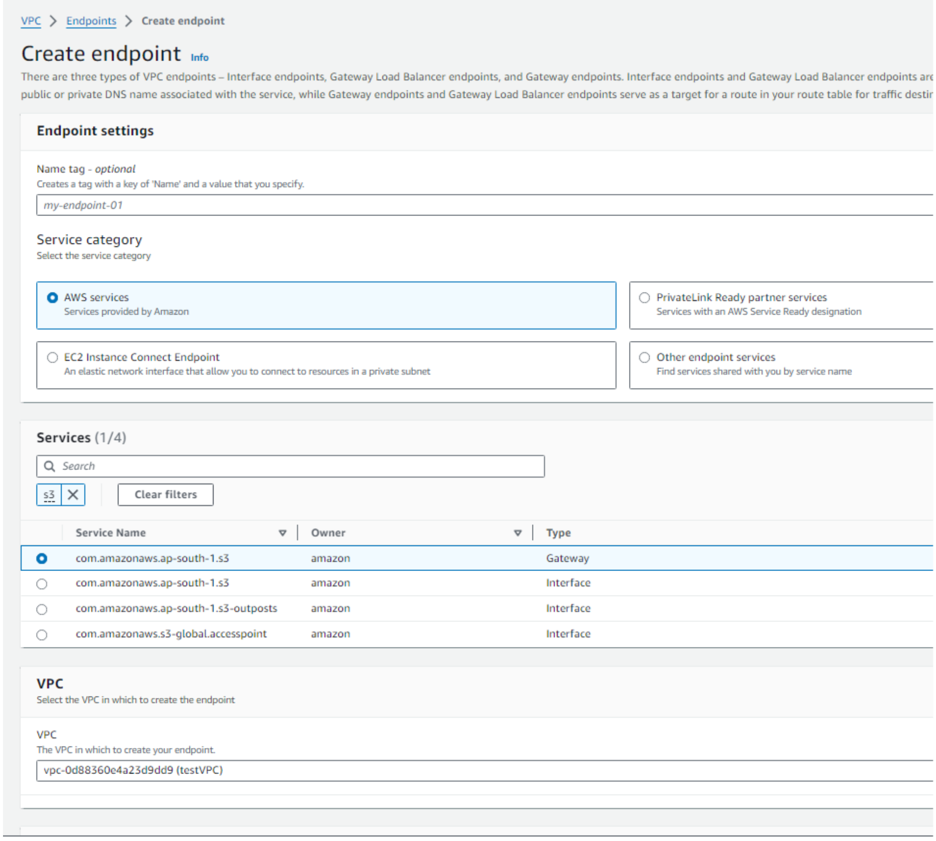
Filter subnet associations

☐	Name	Subnet ID	IPv4 CIDR
☑	public-subnet-a	subnet-006a0737ad93b82fa	10.0.0.0/24
☐	private-subnet-b	subnet-0ced1f52f96b5427c	10.0.1.0/24

Selected subnets

subnet-006a0737ad93b82fa / public-subnet-a ✕

6. Create endpoint and make it compatable with other services.



VPC > Endpoints > Create endpoint

Create endpoint Info

There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and Gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints ar
public or private DNS name associated with the service, while Gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic desti

Endpoint settings

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
my-endpoint-01

Service category
Select the service category

● AWS services
Services provided by Amazon

○ PrivateLink Ready partner services
Services with an AWS Service Ready designation

○ EC2 Instance Connect Endpoint
An elastic network interface that allow you to connect to resources in a private subnet

○ Other endpoint services
Find services shared with you by service name

Services (1/4)

Search

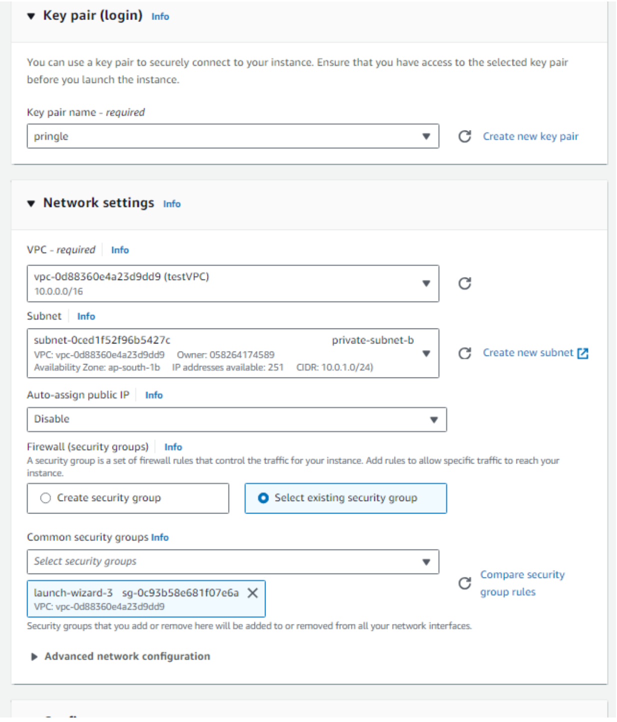
s3 ✕ Clear filters

	Service Name	Owner	Type
●	com.amazonaws.ap-south-1.s3	amazon	Gateway
○	com.amazonaws.ap-south-1.s3	amazon	Interface
○	com.amazonaws.ap-south-1.s3-outposts	amazon	Interface
○	com.amazonaws.s3-global.accesspoint	amazon	Interface

VPC
Select the VPC in which to create the endpoint

VPC
The VPC in which to create your endpoint.
vpc-0d88360e4a23d9dd9 (testVPC)

7. Launching public and private EC2 instances.



Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: pringle

Network settings Info

VPC - *required*: vpc-0d88360e4a23d9dd9 (testVPC) 10.0.0.0/16

Subnet: subnet-0ced1f52f96b5427c private-subnet-b
VPC: vpc-0d88360e4a23d9dd9 Owner: 058264174589
Availability Zone: ap-south-1b IP addresses available: 251 CIDR: 10.0.1.0/24)

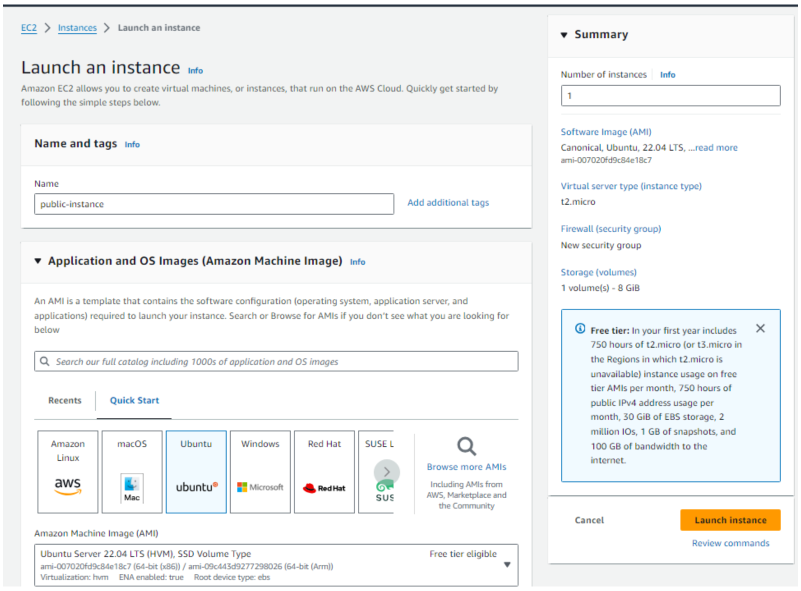
Auto-assign public IP: Disable

Firewall (security groups)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups: *Select security groups*
launch-wizard-3 sg-0c93b58e681f07e6a
VPC: vpc-0d88360e4a23d9dd9

Security groups that you add or remove here will be added to or removed from all your network interfaces.



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: public-instance

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI): Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-007020fd9c84e18c7 (64-bit (x86)) / ami-09c443d9277298026 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Summary

Number of instances: 1

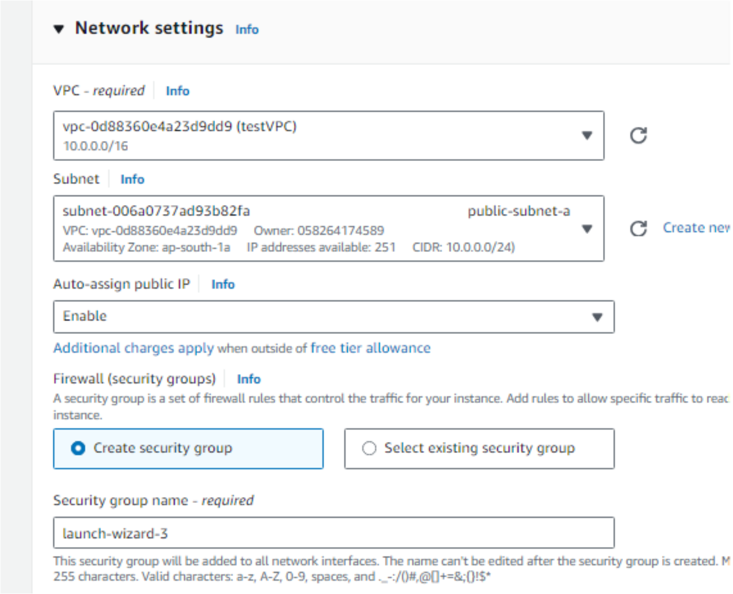
Software Image (AMI): Canonical, Ubuntu, 22.04 LTS, ...read more
ami-007020fd9c84e18c7

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.



▼ Network settings Info

VPC - *required* | Info

vpc-0d88360e4a23d9dd9 (testVPC)
10.0.0.0/16

Subnet | Info

subnet-006a0737ad93b82fa public-subnet-a
VPC: vpc-0d88360e4a23d9dd9 Owner: 058264174589
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.0.0/24)

Auto-assign public IP | Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) | Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reac
instance.

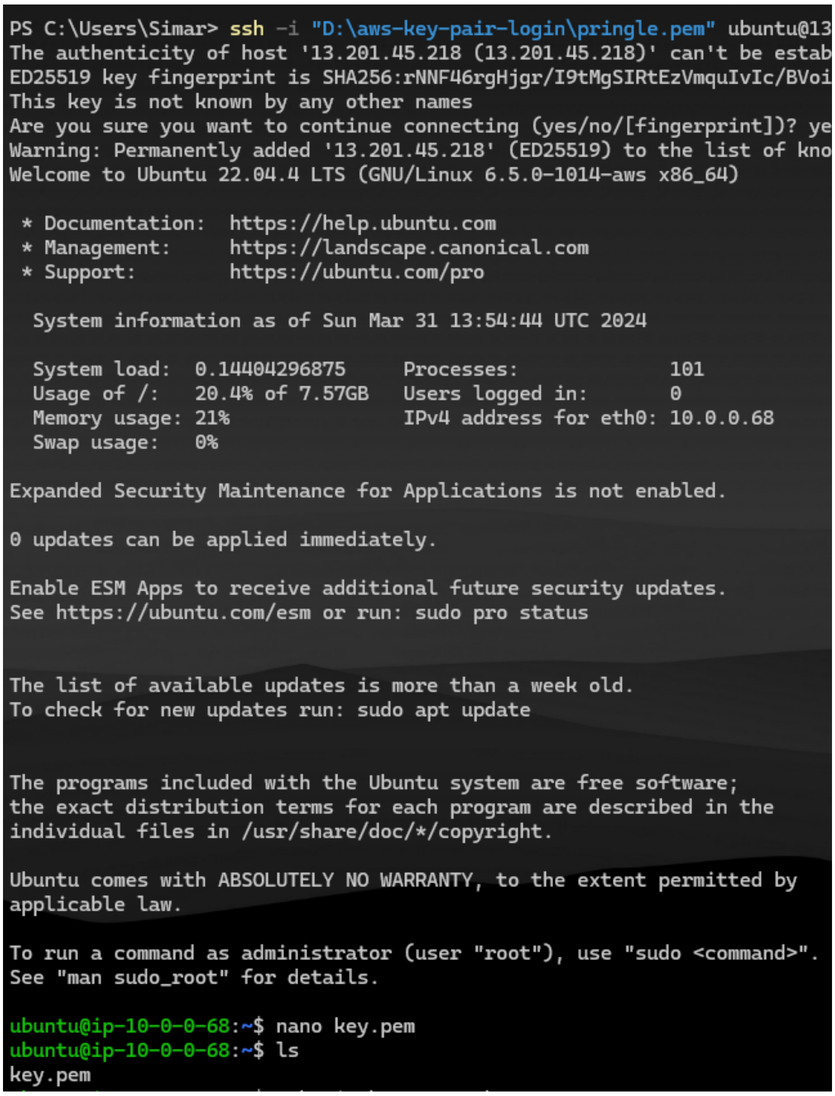
● Create security group ○ Select existing security group

Security group name - *required*

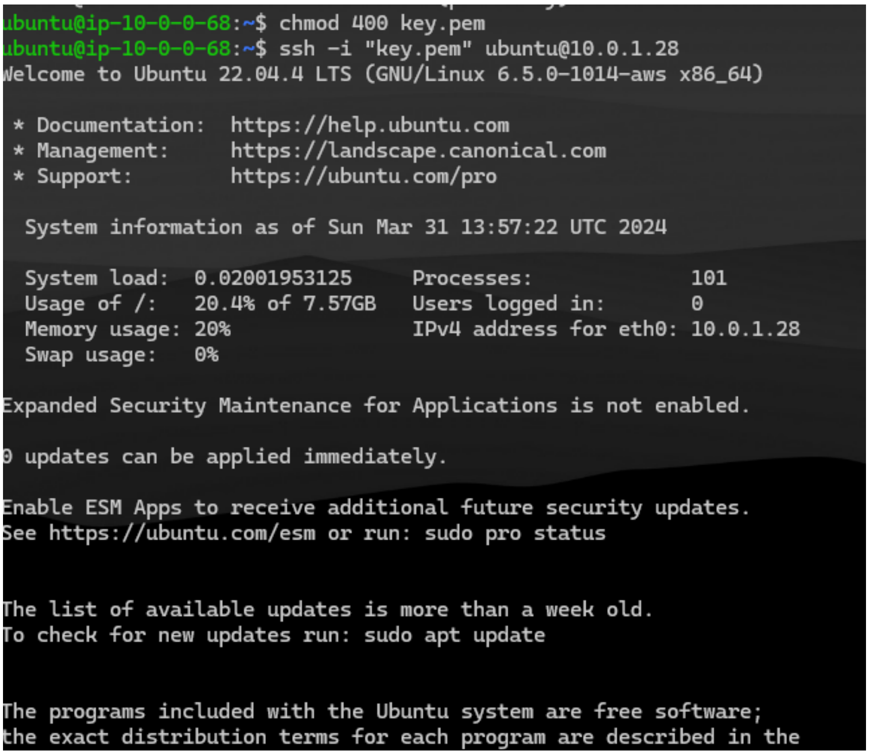
launch-wizard-3

This security group will be added to all network interfaces. The name can't be edited after the security group is created. M
255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

8. Setup the endpoints.



```
PS C:\Users\Simar> ssh -i "D:\aws-key-pair-login\pringle.pem" ubuntu@13
The authenticity of host '13.201.45.218 (13.201.45.218)' can't be estab
ED25519 key fingerprint is SHA256:rNNF46rgHjgr/I9tMgSIRtEzVmquIvIc/BVoi
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? ye
Warning: Permanently added '13.201.45.218' (ED25519) to the list of kno
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

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

  System information as of Sun Mar 31 13:54:44 UTC 2024

  System load:  0.144042968750     Processes:             101
  Usage of /:   20.4% of 7.57GB    Users logged in:       0
  Memory usage: 21%                IPv4 address for eth0: 10.0.0.68
  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-10-0-0-68:~$ nano key.pem
ubuntu@ip-10-0-0-68:~$ ls
key.pem
```



```
ubuntu@ip-10-0-0-68:~$ chmod 400 key.pem
ubuntu@ip-10-0-0-68:~$ ssh -i "key.pem" ubuntu@10.0.1.28
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1014-aws x86_64)

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

  System information as of Sun Mar 31 13:57:22 UTC 2024

  System load:  0.02001953125     Processes:             101
  Usage of /:   20.4% of 7.57GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for eth0: 10.0.1.28
  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
```