AWS re:Start

LAB

Networking Resources for a VPC

WEEK 3

aws re/start

Overview

Customer scenario

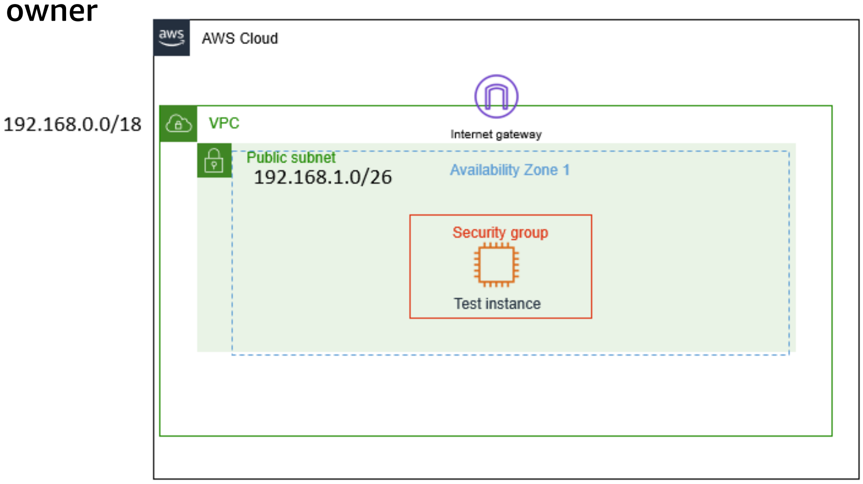
Your role is a Cloud Support Engineer at Amazon Web Services (AWS). During your shift, a customer from a startup company requests assistance regarding a networking issue within their AWS infrastructure. The email and an attachment of their architecture is below.

Email from the customer

Hello Cloud Support!

I previously reached out to you regarding help setting up my VPC. I thought I knew how to attach all the resources to make an internet connection, but I cannot even ping outside the VPC. All I need to do is ping! Can you please help me set up my VPC to where it has network connectivity and can ping? The architecture is below. Thanks!

Brock, startup owner

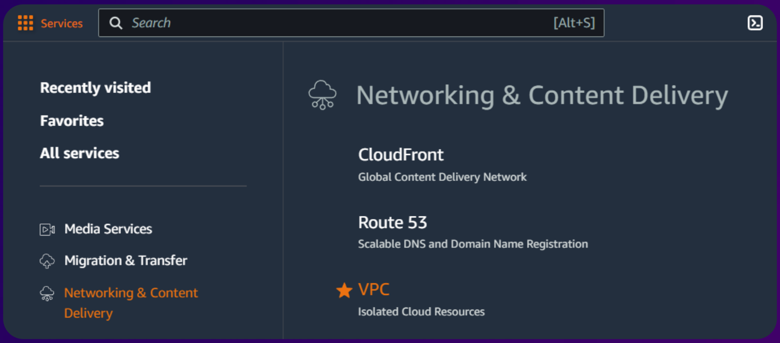


Task 1

Investigate the customer's environment

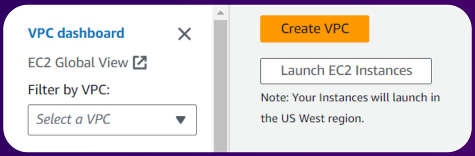
Step 1: Access the AWS Management Console

Open the AWS Management Console, and select VPC.



Step 2: Creating the VPC

In the **Amazon VPC** dashboard, choose the Create VPC button to launch the VPC wizard.



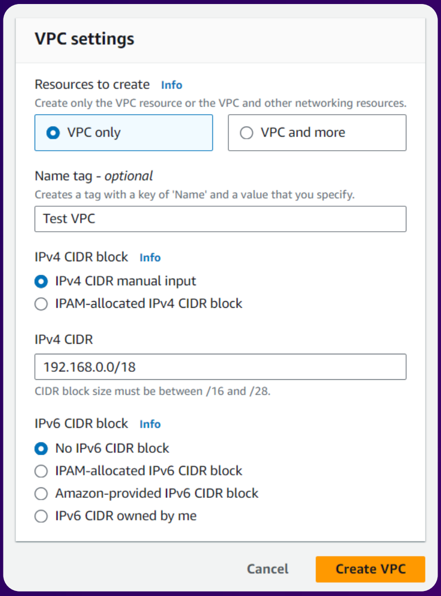
Note: Your Instances will launch in the US West region.

Task 1

Investigate the customer's environment

Step 3: Set up the VPC

Once in the VPC wizard, use the following parameters to configure the VPC settings.



VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

Test VPC

IPv4 CIDR block Info

● IPv4 CIDR manual input

○ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.168.0.0/18

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

● No IPv6 CIDR block

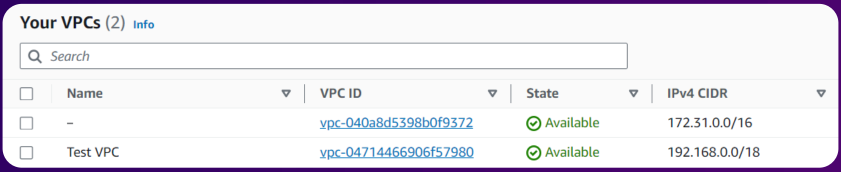
○ IPAM-allocated IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

○ IPv6 CIDR owned by me

Step 4: Review the VPC

Once you have created the VPC, navigate to the Amazon VPC dashboard and select **Your VPCs** to verify that your VPC is available.



Your VPCs (2) Info

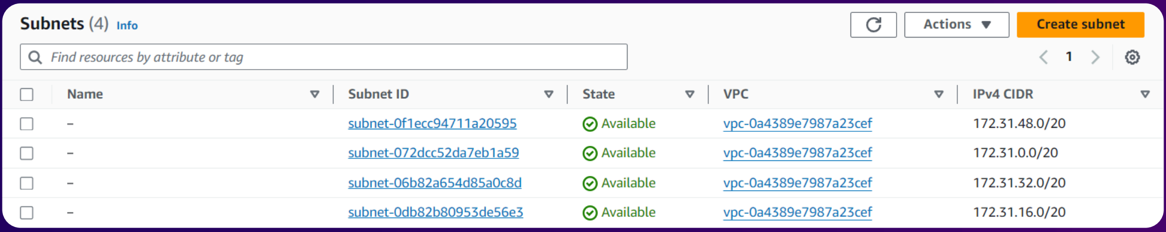
□	Name	VPC ID	State	IPv4 CIDR
□	–	vpc-040a8d5398b0f9372	✓ Available	172.31.0.0/16
□	Test VPC	vpc-04714466906f57980	✓ Available	192.168.0.0/18

Task 1

Investigate the customer's environment

Step 5: Creating subnets

Navigate to the **Subnets** section and select Create subnet.

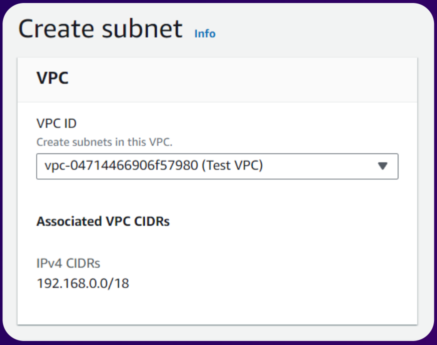


Subnets (4)

☐	Name	Subnet ID	State	VPC	IPv4 CIDR
☐	–	subnet-0f1ecc94711a20595	✓ Available	vpc-0a4389e7987a23cef	172.31.48.0/20
☐	–	subnet-072dcc52da7eb1a59	✓ Available	vpc-0a4389e7987a23cef	172.31.0.0/20
☐	–	subnet-06b82a654d85a0c8d	✓ Available	vpc-0a4389e7987a23cef	172.31.32.0/20
☐	–	subnet-0db82b80953de56e3	✓ Available	vpc-0a4389e7987a23cef	172.31.16.0/20

Step 6: Set up the public subnet

Use the following parameters to configure the subnet settings.



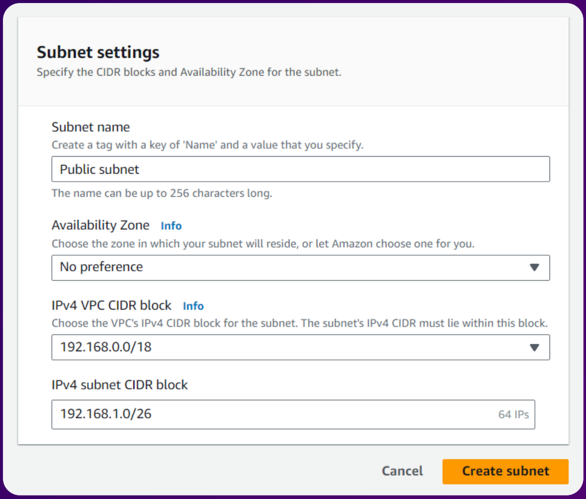
Create subnet

VPC

VPC ID
Create subnets in this VPC.
vpc-04714466906f57980 (Test VPC)

Associated VPC CIDRs

IPv4 CIDRs
192.168.0.0/18



Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

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

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

IPv4 VPC CIDR block
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
192.168.0.0/18

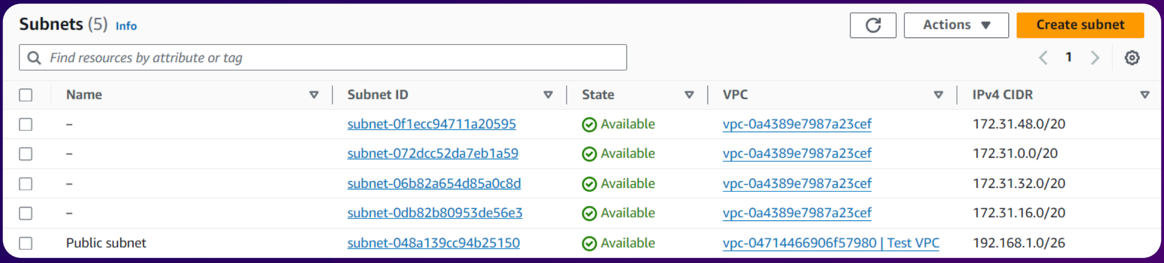
IPv4 subnet CIDR block
192.168.1.0/26 64 IPs

Task 1

Investigate the customer's environment

Step 7: Review the public subnet

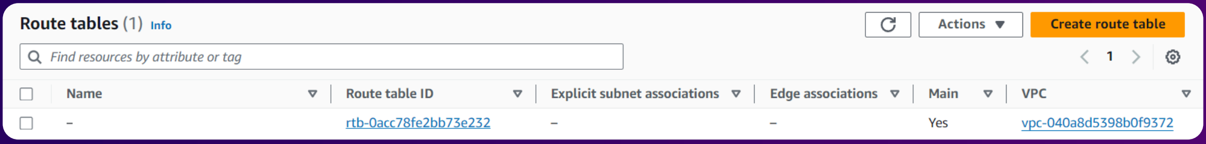
Once you have created the subnet, navigate to the **Subnets** section to verify that your public subnet is available.



□	Name	Subnet ID	State	VPC	IPv4 CIDR
□	–	subnet-0f1ecc94711a20595	✓ Available	vpc-0a4389e7987a23cef	172.31.48.0/20
□	–	subnet-072dcc52da7eb1a59	✓ Available	vpc-0a4389e7987a23cef	172.31.0.0/20
□	–	subnet-06b82a654d85a0c8d	✓ Available	vpc-0a4389e7987a23cef	172.31.32.0/20
□	–	subnet-0db82b80953de56e3	✓ Available	vpc-0a4389e7987a23cef	172.31.16.0/20
□	Public subnet	subnet-048a139cc94b25150	✓ Available	vpc-04714466906f57980 | Test VPC	192.168.1.0/26

Step 8: Create route table

Navigate to the **Route Tables** section and select Create route table.



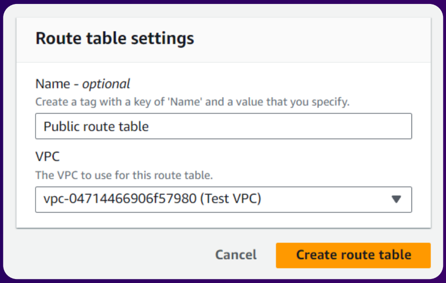
□	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
□	–	rtb-0acc78fe2bb73e232	–	–	Yes	vpc-040a8d5398b0f9372

Task 1

Investigate the customer's environment

Step 9: Set up the route table

Use the following parameters to configure the route table settings.



Route table settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

Public route table

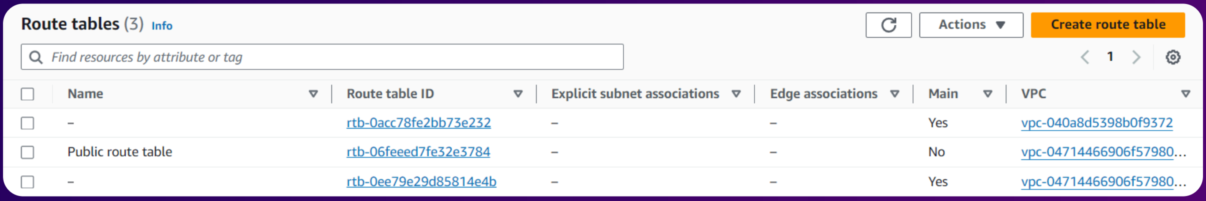
VPC

The VPC to use for this route table.

vpc-04714466906f57980 (Test VPC) ▼

Step 10: Review the route table

Once you have created the route table, navigate to the **Routes Tables** section to verify that your route table is now listed.



Route tables (3) Info

Find resources by attribute or tag

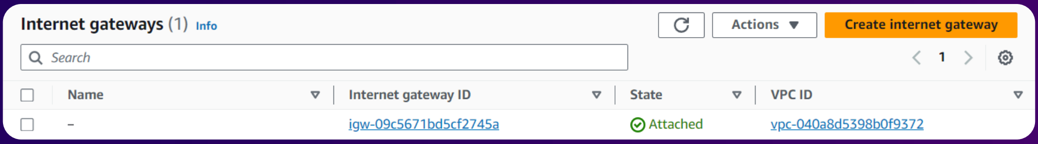
□	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
□	–	rtb-0acc78fe2bb73e232	–	–	Yes	vpc-040a8d5398b0f9372
□	Public route table	rtb-06feeed7fe32e3784	–	–	No	vpc-04714466906f57980…
□	–	rtb-0ee79e29d85814e4b	–	–	Yes	vpc-04714466906f57980…

Task 1

Investigate the customer's environment

Step 11: Create internet gateway

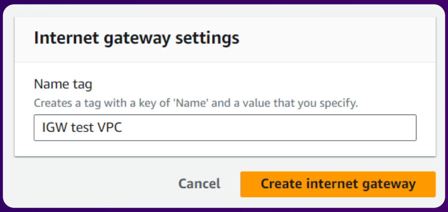
Navigate to the **Internet gateways** section and select Create internet gateway.



□	Name	Internet gateway ID	State	VPC ID
□	–	igw-09c5671bd5cf2745a	✓ Attached	vpc-040a8d5398b0f9372

Step 12: Set up the internet gateway

Use the following parameters to configure the internet gateway settings.


Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

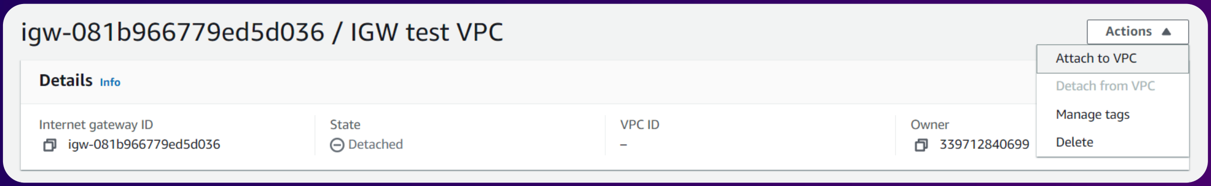
IGW test VPC

Task 1

Investigate the customer's environment

Step 13: Attach internet gateway

Once created, attach the internet gateway to the VPC by selecting the action Attach to VPC.



igw-081b966779ed5d036 / IGW test VPC

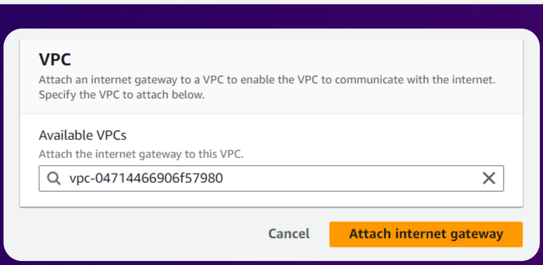
Details Info

Internet gateway ID: igw-081b966779ed5d036

State: ⊖ Detached

VPC ID: –

Owner: 339712840699



VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

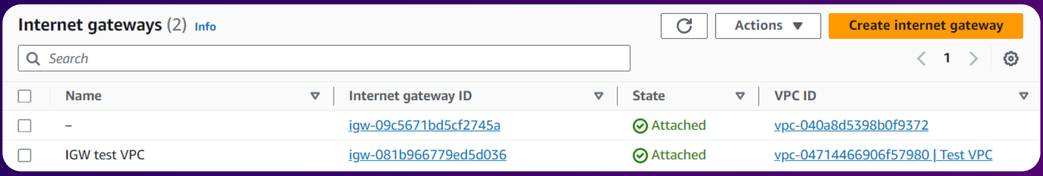
Available VPCs

Attach the internet gateway to this VPC.

vpc-04714466906f57980

Step 14: Review attachment

Once you have created and attached the internet gateway, navigate to the **Internet gateways** section to verify that your internet gateway is now attached.



Internet gateways (2) Info

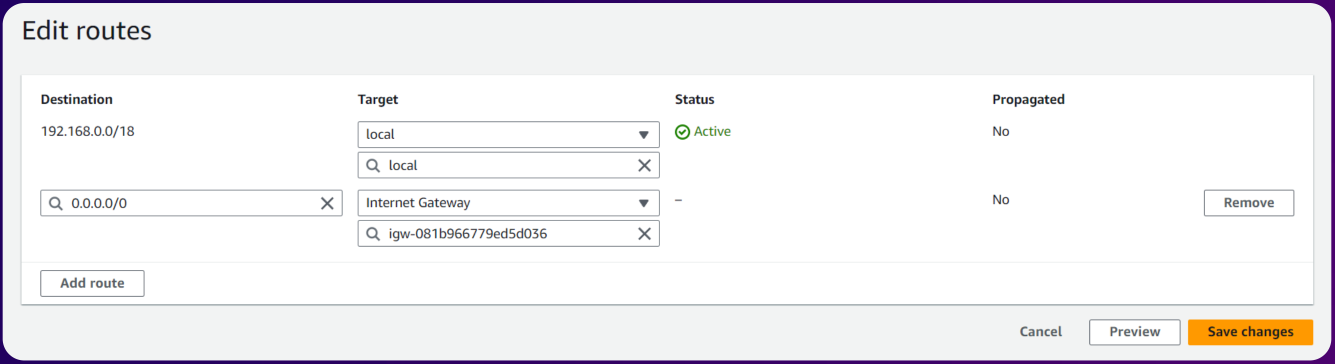
□	Name	Internet gateway ID	State	VPC ID
□	–	igw-09c5671bd5cf2745a	✓ Attached	vpc-040a8d5398b0f9372
□	IGW test VPC	igw-081b966779ed5d036	✓ Attached	vpc-04714466906f57980 | Test VPC

Task 1

Investigate the customer's environment

Step 15: Add route to route table

In the **Routes** tab, add a route to the route table so any traffic that needs internet connection will use 0.0.0.0/0 to reach the IGW.

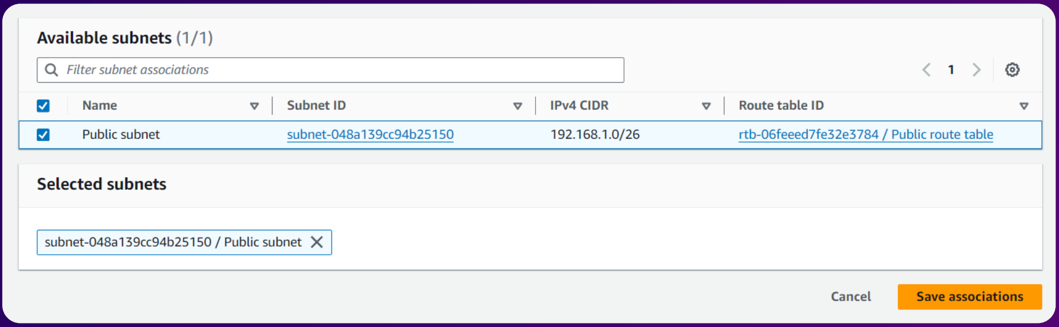


Edit routes

Destination	Target	Status	Propagated	
192.168.0.0/18	local local	✓ Active	No	
0.0.0.0/0	Internet Gateway igw-081b966779ed5d036	–	No	Remove

Step 16: Associate subnet to route table

In the **Subnet associations** tab, associate the Public subnet to the Public route table and click Save associations.



Available subnets (1/1)

☑	Name	Subnet ID	IPv4 CIDR	Route table ID
☑	Public subnet	subnet-048a139cc94b25150	192.168.1.0/26	rtb-06feeed7fe32e3784 / Public route table

Selected subnets

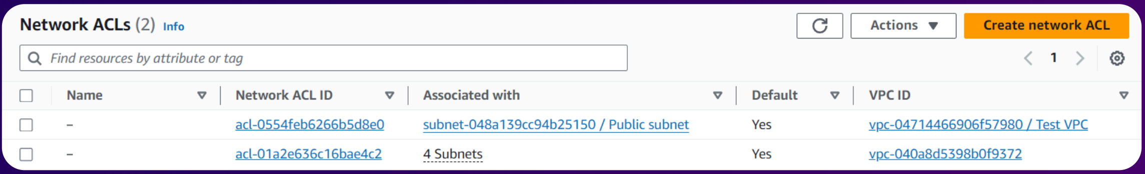
subnet-048a139cc94b25150 / Public subnet

Task 1

Investigate the customer's environment

Step 17: Creating a network ACL

Navigate to the **Network ACLs** section and select Create network ACL.

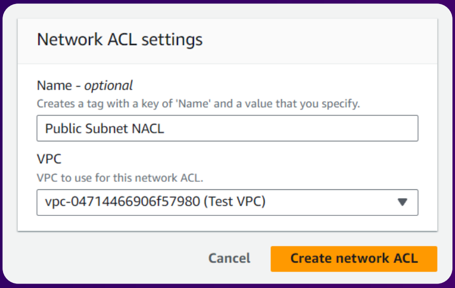


Network ACLs (2) Info

□	Name	Network ACL ID	Associated with	Default	VPC ID
□	–	acl-0554feb6266b5d8e0	subnet-048a139cc94b25150 / Public subnet	Yes	vpc-04714466906f57980 / Test VPC
□	–	acl-01a2e636c16bae4c2	4 Subnets	Yes	vpc-040a8d5398b0f9372

Step 18: Set up the network ACL

Use the following parameters to configure the network ACL settings.



Network ACL settings

Name - *optional*
Creates a tag with a key of 'Name' and a value that you specify.
Public Subnet NACL

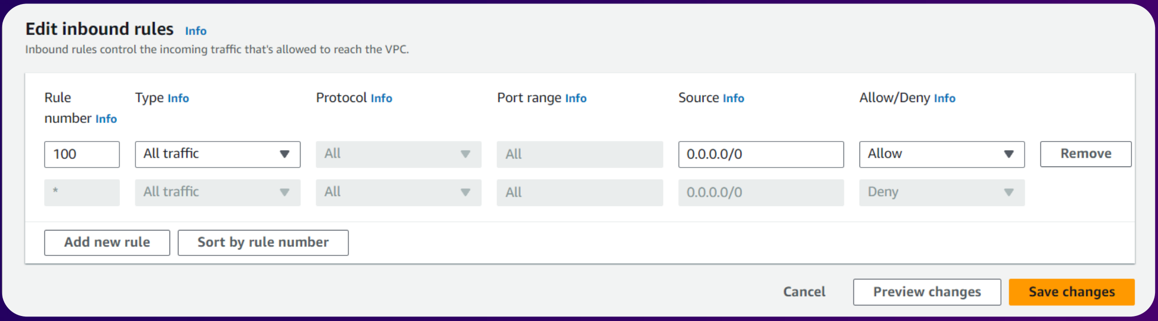
VPC
VPC to use for this network ACL.
vpc-04714466906f57980 (Test VPC) ▼

Task 1

Investigate the customer's environment

Step 19: Edit network ACL inbound rules

Add an inbound rule to the network ACL to allow all traffic.



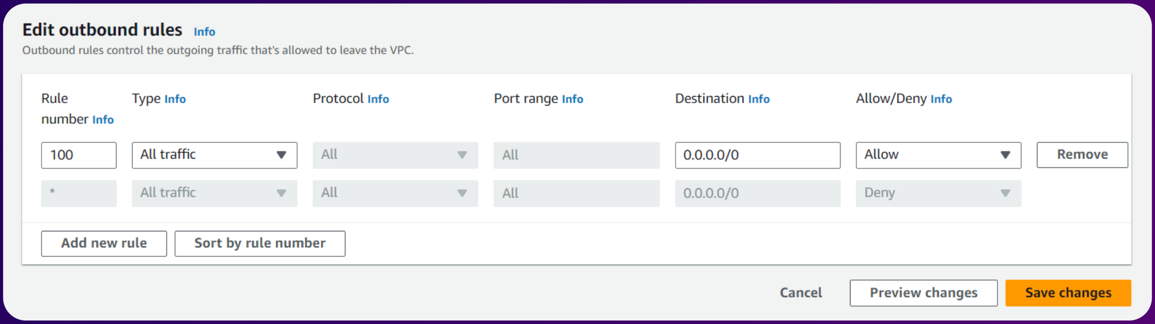
Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
100	All traffic	All	All	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

Step 20: Edit network ACL outbound rules

Add an outbound rule to the network ACL to allow all traffic.



Edit outbound rules Info

Outbound rules control the outgoing traffic that's allowed to leave the VPC.

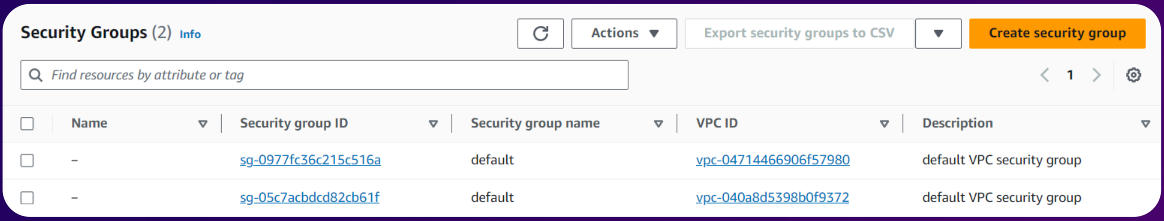
Rule number Info	Type Info	Protocol Info	Port range Info	Destination Info	Allow/Deny Info	
100	All traffic	All	All	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

Task 1

Investigate the customer's environment

Step 21: Creating a security group

Navigate to the **Security Groups** section and select Create security group.



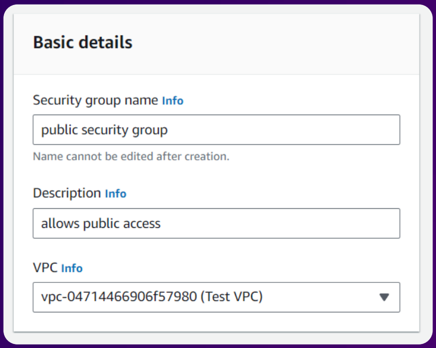
Security Groups (2) Info

Actions
Export security groups to CSV
Create security group
Find resources by attribute or tag
1

☐	Name	Security group ID	Security group name	VPC ID	Description
☐	–	sg-0977fc36c215c516a	default	vpc-04714466906f57980	default VPC security group
☐	–	sg-05c7acbdcd82cb61f	default	vpc-040a8d5398b0f9372	default VPC security group

Step 22: Set up the security group

Use the following parameters to configure the security group basic details.



Basic details

Security group name Info

public security group

Name cannot be edited after creation.

Description Info

allows public access

VPC Info

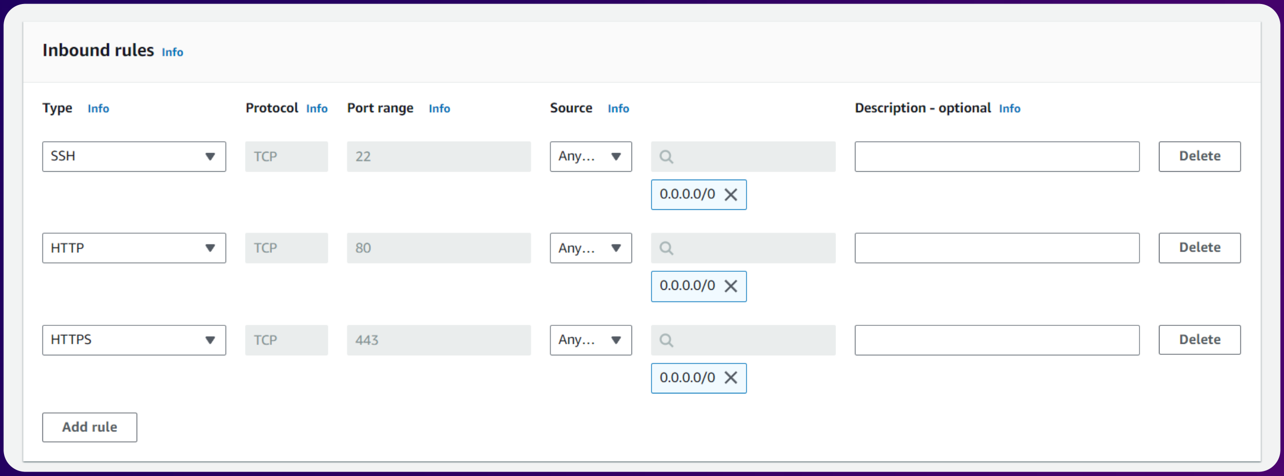
vpc-04714466906f57980 (Test VPC)

Task 1

Investigate the customer's environment

Step 23: Set up security group inbound rules

Configure the following inbound rules for the security group.



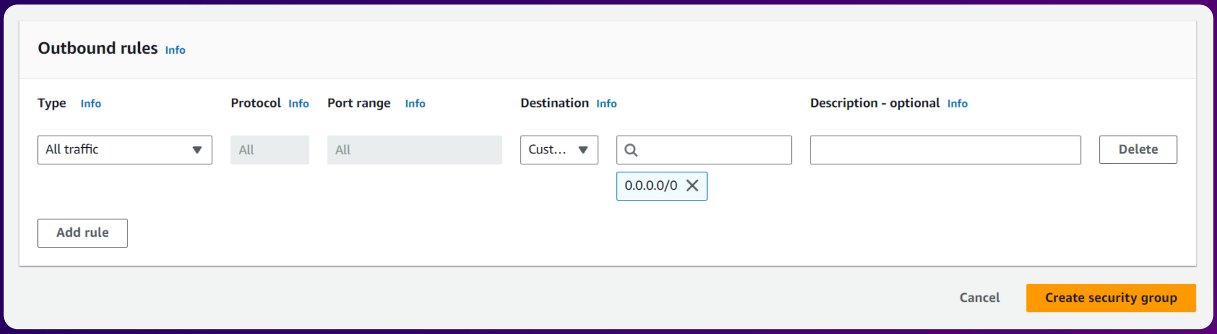
Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH	TCP	22	Any...	0.0.0.0/0		Delete
HTTP	TCP	80	Any...	0.0.0.0/0		Delete
HTTPS	TCP	443	Any...	0.0.0.0/0		Delete

Add rule

Step 24: Set up security group outbound rules

Configure the following outbound rules for the security group.



Outbound rules Info

Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
All traffic	All	All	Cust...	0.0.0.0/0		Delete

Add rule

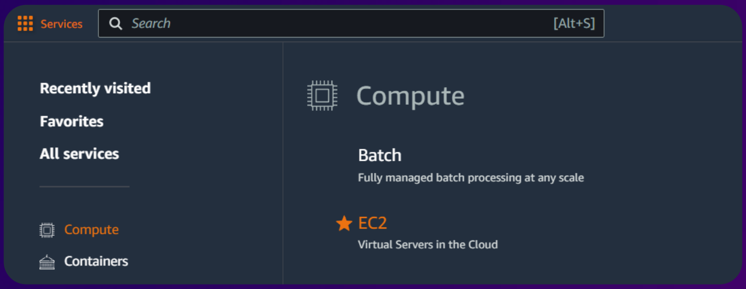
Cancel | Create security group

Task 2

Launch EC2 instance and SSH into instance

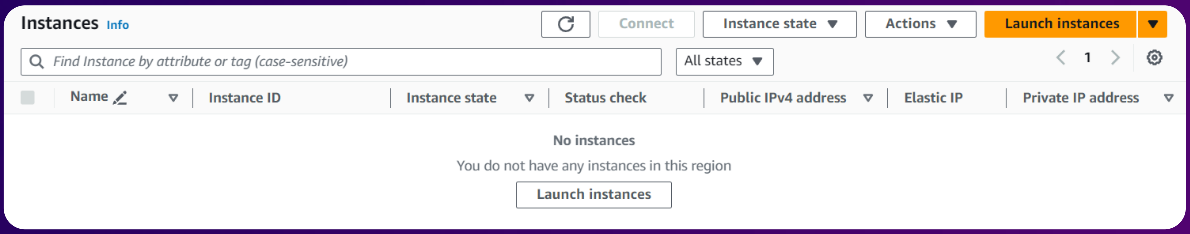
Step 1: Access the EC2 Management Console

Open the AWS Management Console, and select EC2.



Step 2: Launch instance

Navigate to the **Instances** section and select Launch instances.



No instances

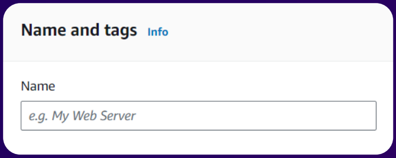
You do not have any instances in this region

Task 2

Launch EC2 instance and SSH into instance

Step 3: Set up the instance

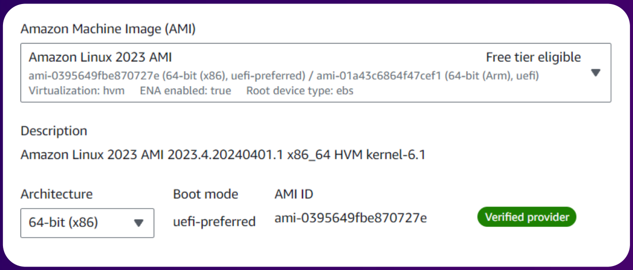
Use the following parameters to configure the instance settings.



Name and tags Info

Name

e.g. My Web Server



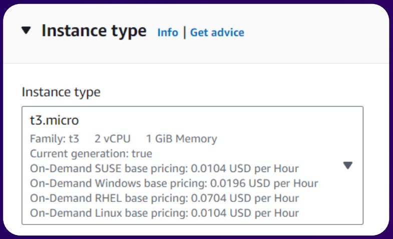
Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-0395649fbe870727e (64-bit (x86), uefi-preferred) / ami-01a43c6864f47cef1 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.4.20240401.1 x86_64 HVM kernel-6.1

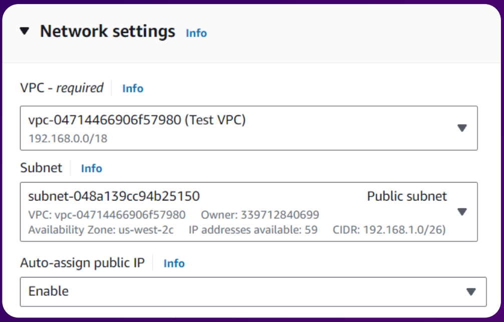
Architecture	Boot mode	AMI ID	
64-bit (x86)	uefi-preferred	ami-0395649fbe870727e	Verified provider



Instance type Info | Get advice

Instance type

t3.micro
Family: t3 2 vCPU 1 GiB Memory
Current generation: true
On-Demand SUSE base pricing: 0.0104 USD per Hour
On-Demand Windows base pricing: 0.0196 USD per Hour
On-Demand RHEL base pricing: 0.0704 USD per Hour
On-Demand Linux base pricing: 0.0104 USD per Hour



Network settings Info

VPC - *required* Info

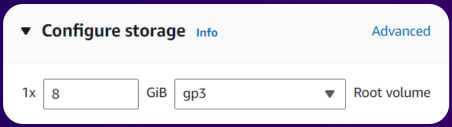
vpc-04714466906f57980 (Test VPC)
192.168.0.0/18

Subnet Info

subnet-048a139cc94b25150 — Public subnet
VPC: vpc-04714466906f57980 Owner: 339712840699
Availability Zone: us-west-2c IP addresses available: 59 CIDR: 192.168.1.0/26)

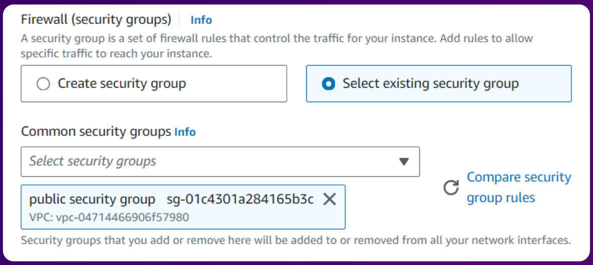
Auto-assign public IP Info

Enable



Configure storage Info — Advanced

1x 8 GiB gp3 Root volume



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 reach your instance.

○ Create security group ● Select existing security group

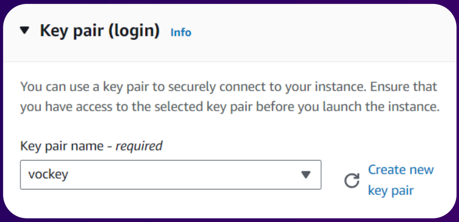
Common security groups Info

Select security groups

public security group sg-01c4301a284165b3c
VPC: vpc-04714466906f57980

Compare security group rules

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



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*

vockey

Create new key pair

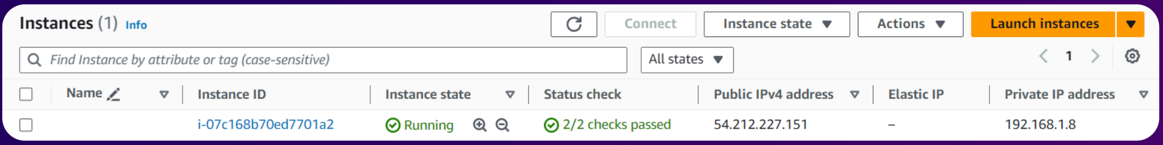
aws re/start

Task 2

Launch EC2 instance and SSH into instance

Step 4: Review the instance

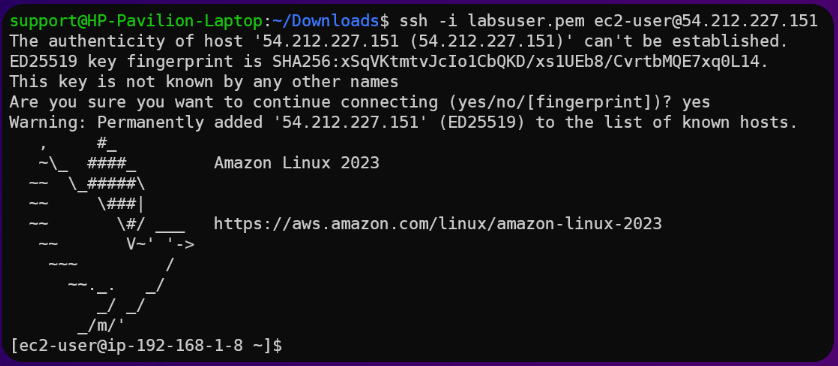
Once you have created the instance, navigate to the **Instances** section to verify that your instance is now running.



□	Name	Instance ID	Instance state	Status check	Public IPv4 address	Elastic IP	Private IP address
□		i-07c168b70ed7701a2	✓ Running	✓ 2/2 checks passed	54.212.227.151	–	192.168.1.8

Step 5: Use SSH to connect to an Amazon Linux EC2 instance

Establish an SSH connection to the instance using the private key and its public IPv4 address.



```
support@HP-Pavilion-Laptop:~/Downloads$ ssh -i labsuser.pem ec2-user@54.212.227.151
The authenticity of host '54.212.227.151 (54.212.227.151)' can't be established.
ED25519 key fingerprint is SHA256:xSqVKtmtvJcIo1CbQKD/xs1UEb8/CvrtbMQE7xq0L14.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.212.227.151' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-192-168-1-8 ~]$
```

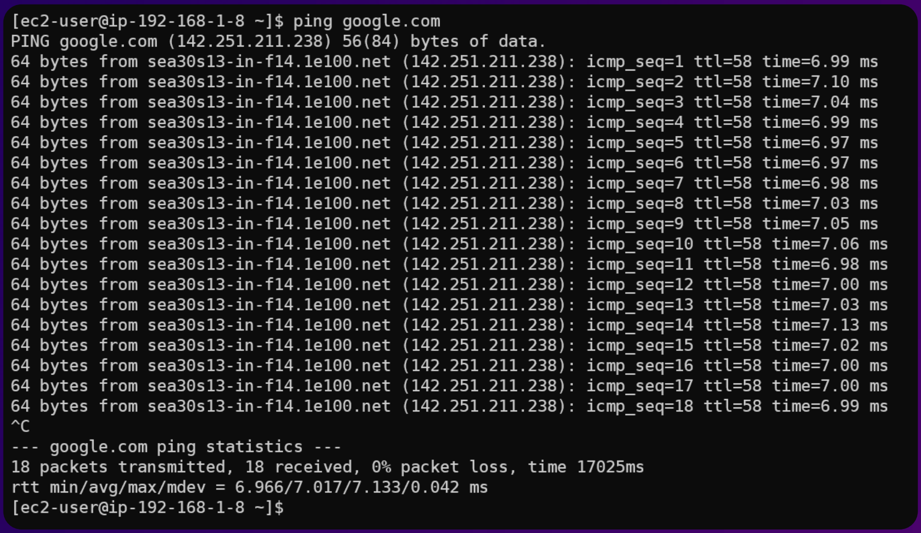
aws re/start

Task 3

Use ping to test internet connectivity

Run the ping command

Run the ping command to test internet connectivity. The results below are saying you have replies from google.com and have 0% packet loss. If you are getting replies back, that means that you have connectivity.



```
[ec2-user@ip-192-168-1-8 ~]$ ping google.com
PING google.com (142.251.211.238) 56(84) bytes of data.
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=1 ttl=58 time=6.99 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=2 ttl=58 time=7.10 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=3 ttl=58 time=7.04 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=4 ttl=58 time=6.99 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=5 ttl=58 time=6.97 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=6 ttl=58 time=6.97 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=7 ttl=58 time=6.98 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=8 ttl=58 time=7.03 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=9 ttl=58 time=7.05 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=10 ttl=58 time=7.06 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=11 ttl=58 time=6.98 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=12 ttl=58 time=7.00 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=13 ttl=58 time=7.03 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=14 ttl=58 time=7.13 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=15 ttl=58 time=7.02 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=16 ttl=58 time=7.00 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=17 ttl=58 time=7.00 ms
64 bytes from sea30s13-in-f14.1e100.net (142.251.211.238): icmp_seq=18 ttl=58 time=6.99 ms
^C
--- google.com ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17025ms
rtt min/avg/max/mdev = 6.966/7.017/7.133/0.042 ms
[ec2-user@ip-192-168-1-8 ~]$
```

Conclusions

Route tables

Route tables in networking define how packets are forwarded within a network or VPC, directing traffic based on destination IP addresses or specific routing rules.

Internet gateway

An internet gateway serves as a connection point between a VPC and the internet, enabling inbound and outbound traffic for resources with public IP addresses.

Network ACLs

Network Access Control Lists (ACLs) act as a virtual firewall at the subnet level, controlling traffic flow in and out of subnets based on rules defined for IP addresses, protocols, and ports.

Security groups

Security groups are virtual firewalls at the instance level, governing inbound and outbound traffic based on security rules defined by protocols, ports, and IP address ranges.

The ping command

The ping command is a network diagnostic tool used to test connectivity between devices by sending ICMP echo request packets and receiving ICMP echo reply packets, providing information about network reachability and response times.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru

aws re/start