AWS re:Start LAB

Troubleshooting a Network Issue

WEEK 3

aws re/start

Overview

Customer scenario

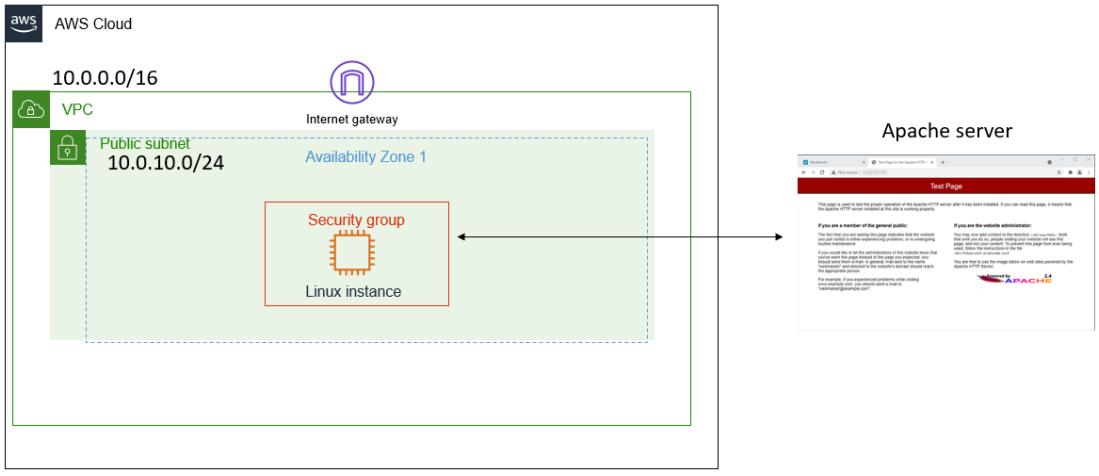
Your role is a cloud support engineer at Amazon Web Services (AWS). During your shift, a consulting company has a networking issue within their AWS infrastructure. The following is the email and an attachment of their architecture.

Ticket from your customer

Hello, Cloud Support!

When I create an Apache server through the command line, I cannot ping it. I also get an error when I enter the IP address in the browser. Can you please help figure out what is blocking my connection?

Thanks!
Ana
Contractor



Task 1

Use SSH to connect to an Amazon Linux EC2 instance

Initial preparations

In the AWS Management Console, select the EC2 instance and make note of the **Public IPv4 address**.

Download the private key file **labsuser.pem**. Change to the Downloads directory and modify the permissions on the key to be read-only (r--------).

Connect to the instance using SSH

Establish a connection to the EC2 instance using the ssh command, the key and the instance's public IPv4 address.

```
support@HP-Pavilion-Laptop:~/Downloads$ ssh -i labsuser.pem ec2-user@34.219.182.160
The authenticity of host '34.219.182.160 (34.219.182.160)' can't be established.
ED25519 key fingerprint is SHA256:b/s6K1VZ/wXn3w6/7zlODtoBNw6yMygsK3wymqxEJTw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.219.182.160' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-10-162 ~]$
```

aws re/start

Task 2

Install httpd

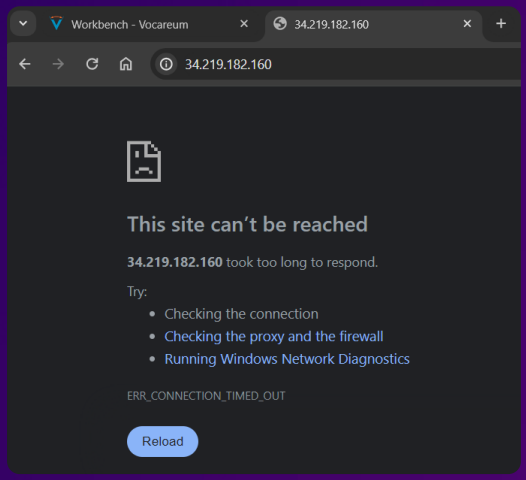
Step 1: Start the Apache HTTP server

Start the httpd service with the systemctl start command.

```
[ec2-user@ip-10-0-10-162 ~]$ sudo systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
[ec2-user@ip-10-0-10-162 ~]$ sudo systemctl start httpd.service
[ec2-user@ip-10-0-10-162 ~]$ sudo systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-04-15 19:44:56 UTC; 2s ago
     Docs: man:httpd.service(8)
 Main PID: 2513 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─2513 /usr/sbin/httpd -DFOREGROUND
           ├─2514 /usr/sbin/httpd -DFOREGROUND
           ├─2515 /usr/sbin/httpd -DFOREGROUND
           ├─2517 /usr/sbin/httpd -DFOREGROUND
           ├─2522 /usr/sbin/httpd -DFOREGROUND
           └─2539 /usr/sbin/httpd -DFOREGROUND

Apr 15 19:44:56 ip-10-0-10-162.us-west-2.compute.internal systemd[1]: Starting The Apache HTTP Server...
Apr 15 19:44:56 ip-10-0-10-162.us-west-2.compute.internal systemd[1]: Started The Apache HTTP Server.
[ec2-user@ip-10-0-10-162 ~]$
```

Step 2: Check the httpd service

The httpd service may be running, but if you attempt to visit http://34.219.182.160 in a browser, the page will not load.



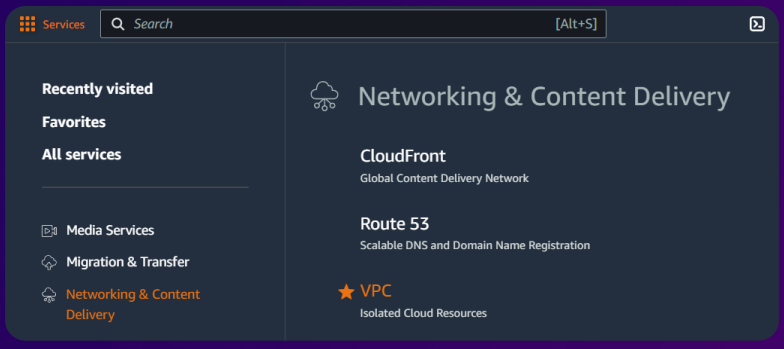
aws re/start

Task 3

Investigate the customer's VPC configuration

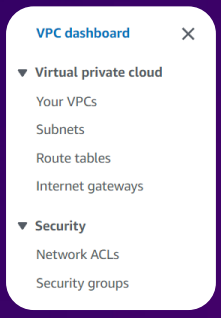
Step 1: Access the AWS Management Console

Open the AWS Management Console, and select VPC.



Step 2: Use the VPC left navigation pane

Use the left navigation pane and check each service within the VPC to confirm that each resource is configured correctly.



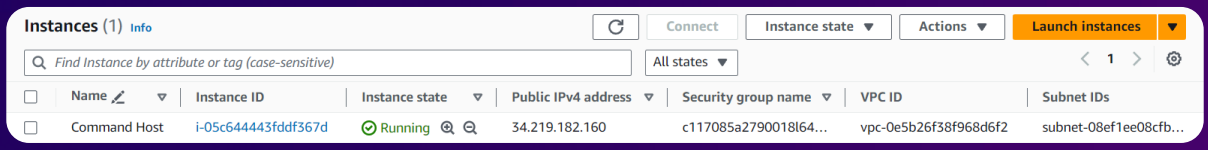
aws re/start

Task 3

Investigate the customer's VPC configuration

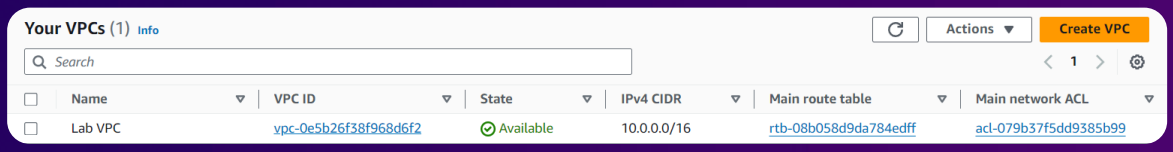
Step 3: Investigate the Instance

The Command Host instance is running in the Public Subnet 1 and is linked to the security group Linux instance SG.



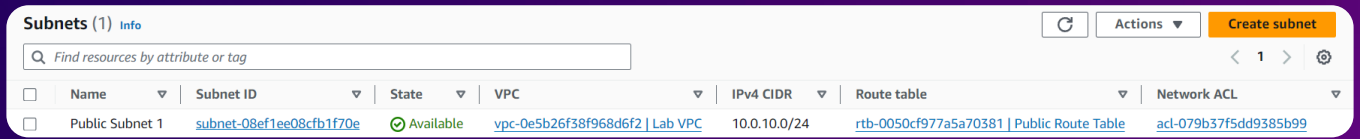
Step 4: Investigate the VPC

The Lab VPC is available and associated with a network ACL.



Step 5: Investigate the Subnet

Public Subnet 1 is available in the Lab VPC and is associated with a network ACL and with the Public Route Table.



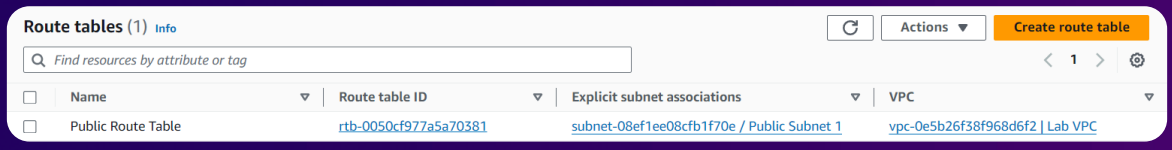
aws re/start

Task 3

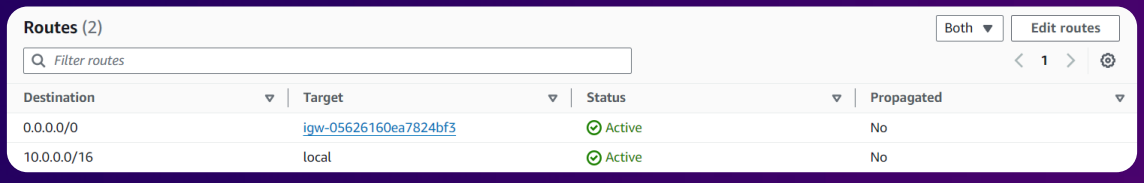
Investigate the customer's VPC configuration

Step 6: Investigate the Route Table

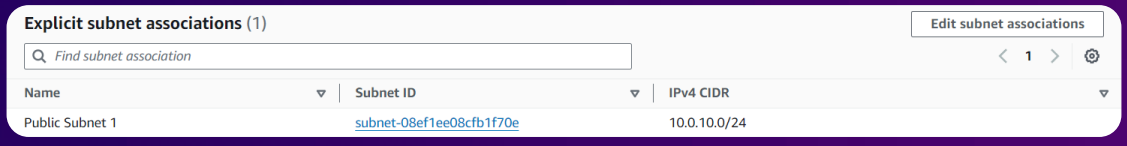
The Public Route Table is correctly linked to the Lab VPC.



There is a route directing all internet traffic to the internet gateway.



The route table is explicitly associated with Public Subnet 1.



aws re/start

Task 3

Investigate the customer's VPC configuration

Step 7: Investigate the Internet Gateway

The internet gateway is properly attached to the Lab VPC.

Internet gateways (1) Info

Actions ▼ | Create internet gateway

Search

1

Name	Internet gateway ID	State	VPC ID
–	igw-05626160ea7824bf3	Attached	vpc-0e5b26f38f968d6f2 | Lab VPC

Step 8: Investigate the Network ACL

The network ACL is correctly associated with Public Subnet 1.

Network ACLs (1) Info

Actions ▼ | Create network ACL

Find resources by attribute or tag

1

Name	Network ACL ID	Associated with	VPC ID
–	acl-079b37f5dd9385b99	subnet-08ef1ee08cfb1f70e / Public Subnet 1	vpc-0e5b26f38f968d6f2 / Lab VPC

The current rules allow all inbound and outbound traffic.

Inbound rules (2)

Edit inbound rules

Filter inbound rules

1

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

Outbound rules (2)

Edit outbound rules

Filter outbound rules

1

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

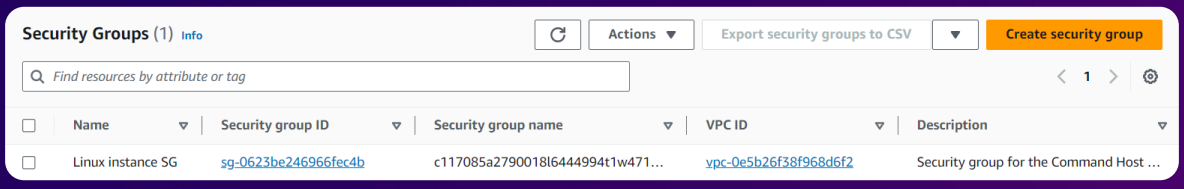
aws re/start

Task 3

Investigate the customer's VPC configuration

Step 9: Investigate the Security Group

The Linux instance SG security group is linked to the Command Host instance. The current inbound rules allow only SSH traffic. The outbound rules allow all traffic.

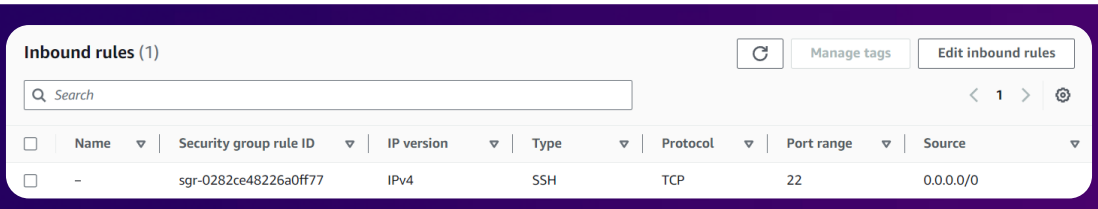


Security Groups (1) Info

Actions | Export security groups to CSV | Create security group

Find resources by attribute or tag

Name	Security group ID	Security group name	VPC ID	Description
Linux instance SG	sg-0623be246966fec4b	c117085a2790018l6444994t1w471...	vpc-0e5b26f38f968d6f2	Security group for the Command Host ...

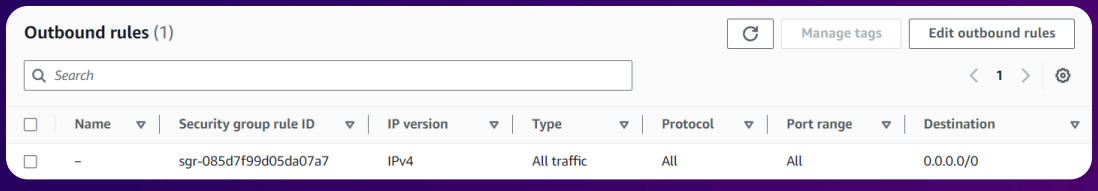


Inbound rules (1)

Manage tags | Edit inbound rules

Search

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-0282ce48226a0ff77	IPv4	SSH	TCP	22	0.0.0.0/0



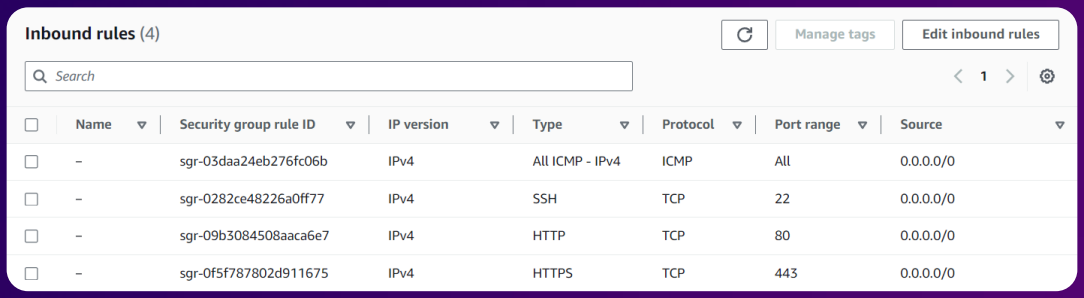
Outbound rules (1)

Manage tags | Edit outbound rules

Search

Name	Security group rule ID	IP version	Type	Protocol	Port range	Destination
-	sgr-085d7f99d05da07a7	IPv4	All traffic	All	All	0.0.0.0/0

Add new inbound rules to allow ICMP, HTTP and HTTPS traffic.



Inbound rules (4)

Manage tags | Edit inbound rules

Search

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-03daa24eb276fc06b	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0
-	sgr-0282ce48226a0ff77	IPv4	SSH	TCP	22	0.0.0.0/0
-	sgr-09b3084508aaca6e7	IPv4	HTTP	TCP	80	0.0.0.0/0
-	sgr-0f5f787802d911675	IPv4	HTTPS	TCP	443	0.0.0.0/0

Task 3

Investigate the customer's VPC configuration

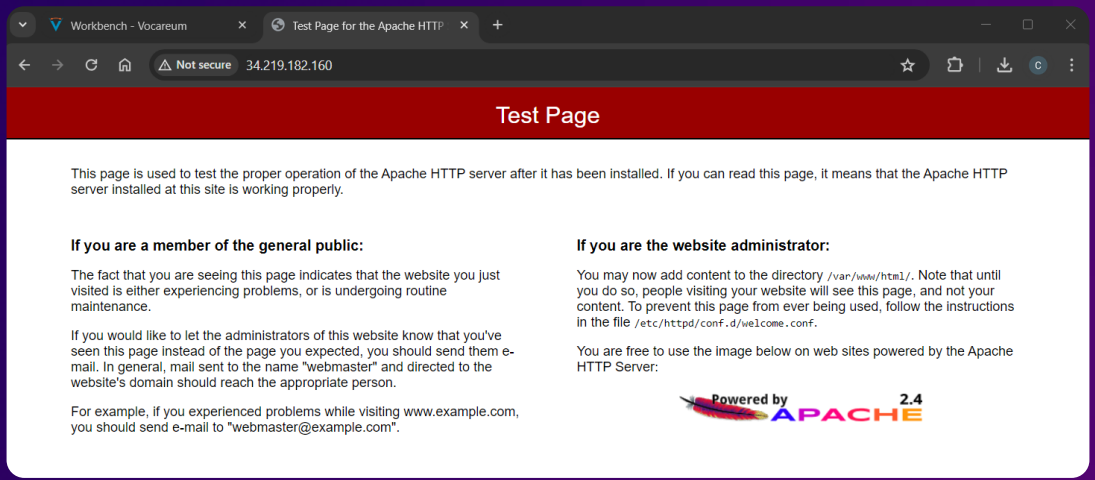
Step 10: Test ICMP traffic

Ping the Apache HTTP server to verify its reachability.

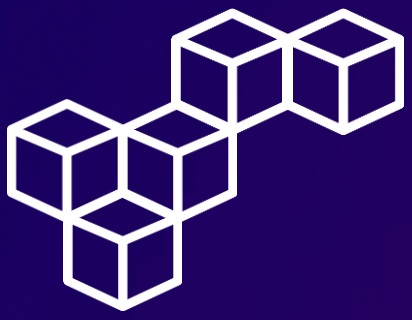
```
[ec2-user@ip-10-0-10-162 ~]$ ping -c 4 34.219.182.160
PING 34.219.182.160 (34.219.182.160) 56(84) bytes of data.
64 bytes from 34.219.182.160: icmp_seq=1 ttl=254 time=0.168 ms
64 bytes from 34.219.182.160: icmp_seq=2 ttl=254 time=0.142 ms
64 bytes from 34.219.182.160: icmp_seq=3 ttl=254 time=0.217 ms
64 bytes from 34.219.182.160: icmp_seq=4 ttl=254 time=0.169 ms

--- 34.219.182.160 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.142/0.174/0.217/0.027 ms
[ec2-user@ip-10-0-10-162 ~]$
```

Step 11: Test HTTP traffic

Open a new tab in a browser and visit http://34.219.182.160 to confirm that the Apache HTTP server is working.



aws re/start



Conclusions

Subnets
Subnets enable segmentation of resources within a virtual network, aiding in better resource management and security control.

Route Tables
Route tables dictate the traffic flow between subnets and external networks, ensuring efficient routing and connectivity.

Internet Gateways
Internet gateways serve as the entry and exit points for internet-bound traffic, facilitating communication between VPC resources and the internet.

Network ACLs
Network ACLs provide an additional layer of security by filtering inbound and outbound traffic at the subnet level based on specified rules.

Security Groups
Security groups act as virtual firewalls for instances, controlling inbound and outbound traffic based on defined rules to enhance network security and access control.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru