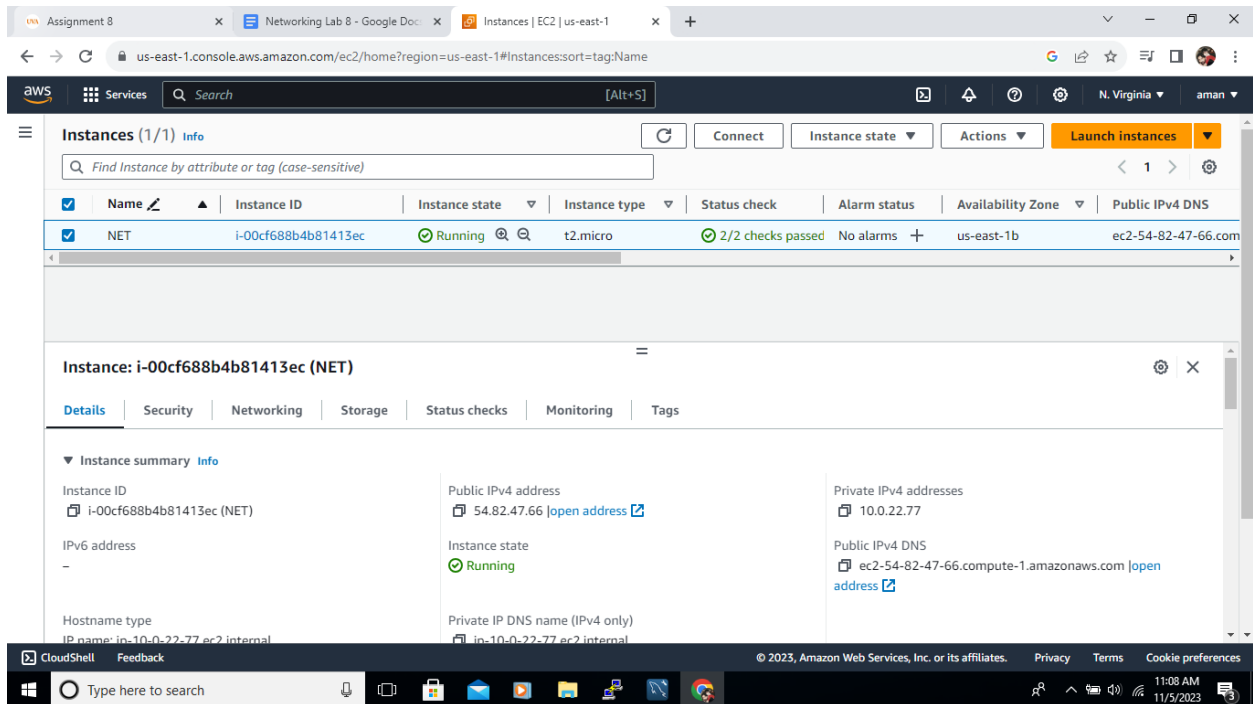


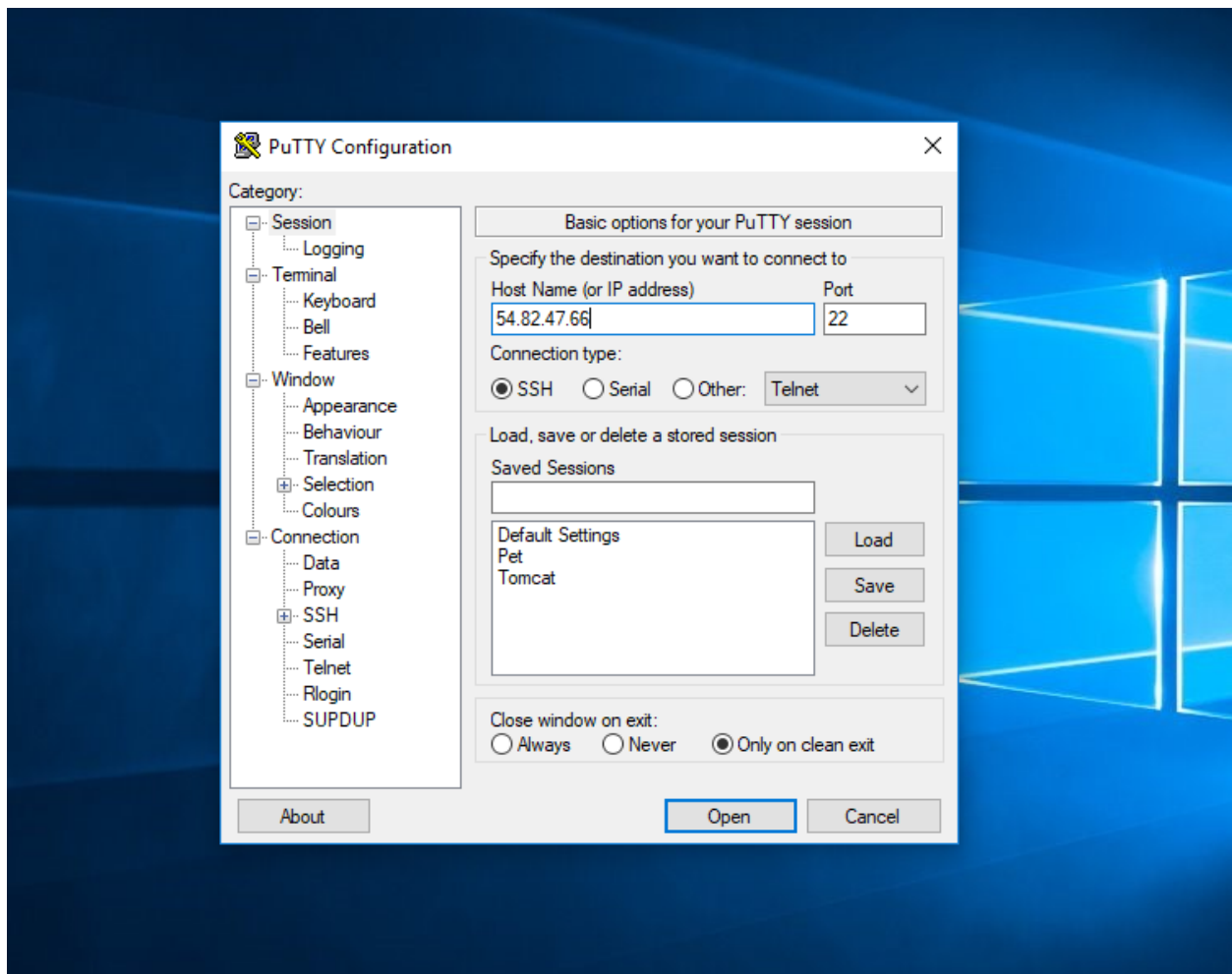
## Troubleshooting accessing an instance within a VPC

Follow the steps within Section 14, problem statement 1, to troubleshoot accessing an instance within a VPC:

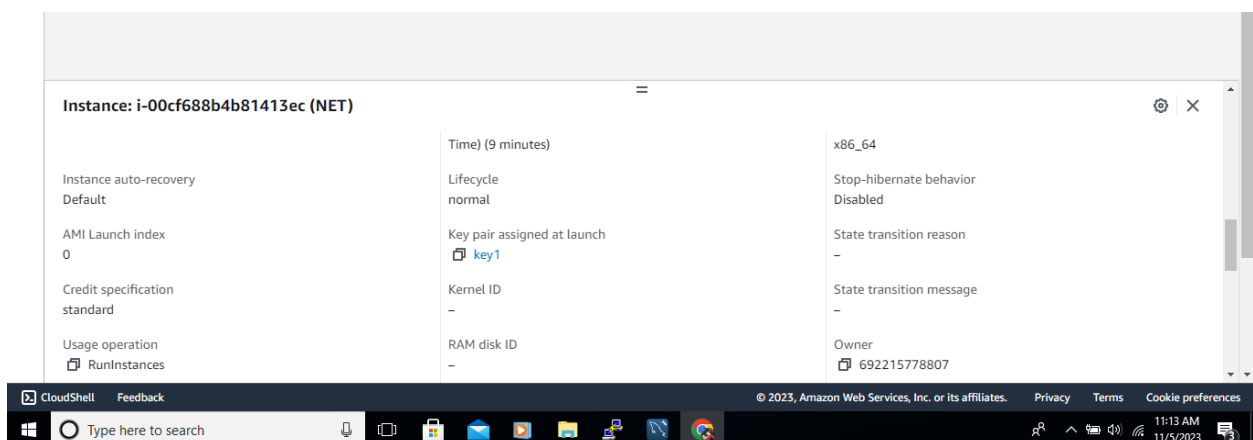
Submit a screenshot of step 1 in which the public IP v4 address and public DNS of the instance are visible.



Submit a screenshot of step 2 in which the IPV4 address and public DNS are visible in Putty.

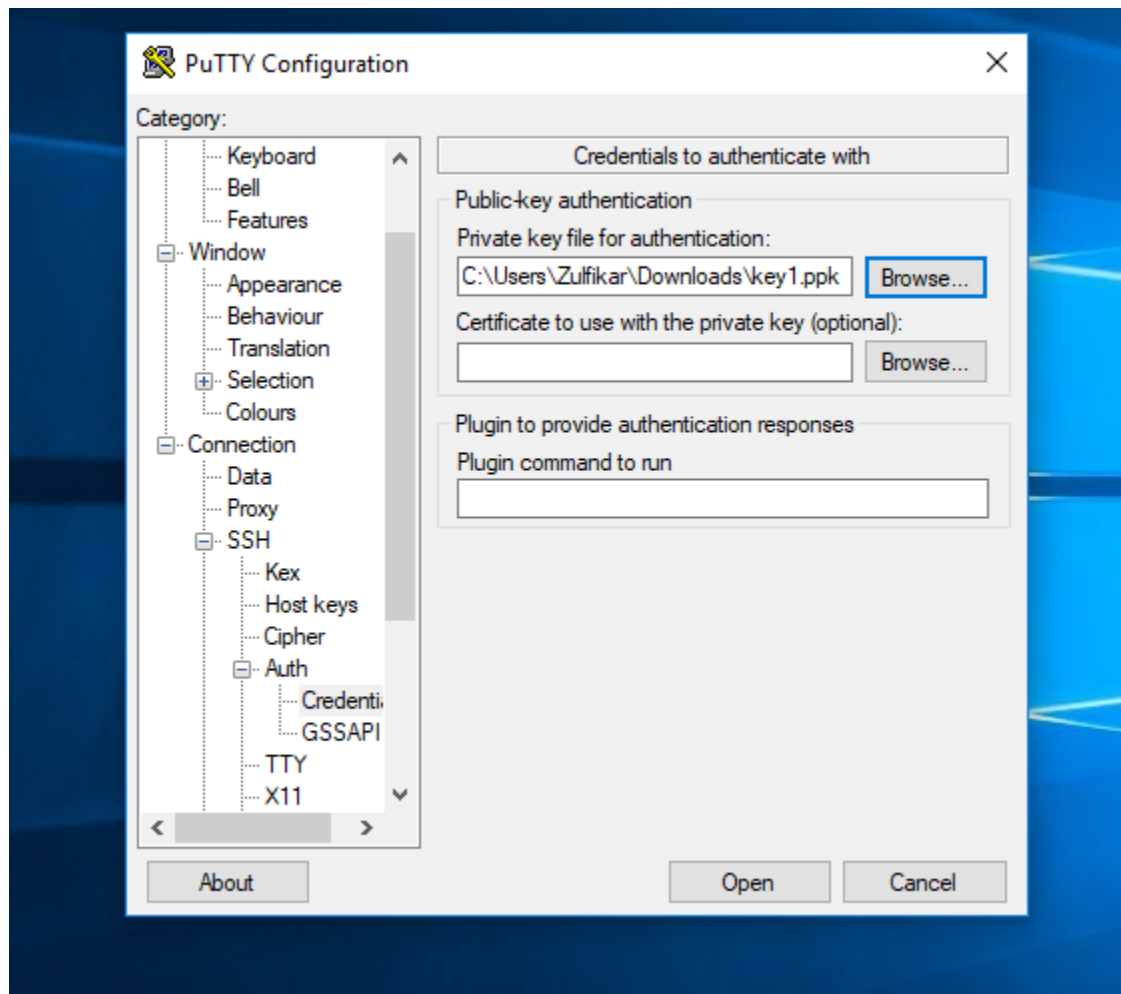


Submit a screenshot of step 3 in which the existing key pair for accessing the instance is visible.



Submit a screenshot of step 5 in which the private key file is loaded into Putty.

Follow the steps to verify that the security group associated with the instance has an inbound rule to accept the SSH connection with the proper port from the correct source.



Assignment 8 x Networking Lab 8 - Google Doc x Instances | EC2 | us-east-1 x +

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:sort=tag:Name

aws Services Search [Alt+S]

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Connect Instance state Actions Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
NET	i-00cf688b4b81413ec	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-54-82-47-66.com

Instance: i-00cf688b4b81413ec (NET)

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
-	sgr-0121e27582440424e	All	All	0.0.0.0/0	LAB-NET
-	sgr-05fc7348178b2122f	22	TCP	75.75.111.108/32	LAB-NET

Outbound rules

Filter rules

Name	Security group rule ID	Port range	Protocol	Destination	Security groups
-	sgr-0271d44cc90e35564	All	All	0.0.0.0/0	LAB-NET

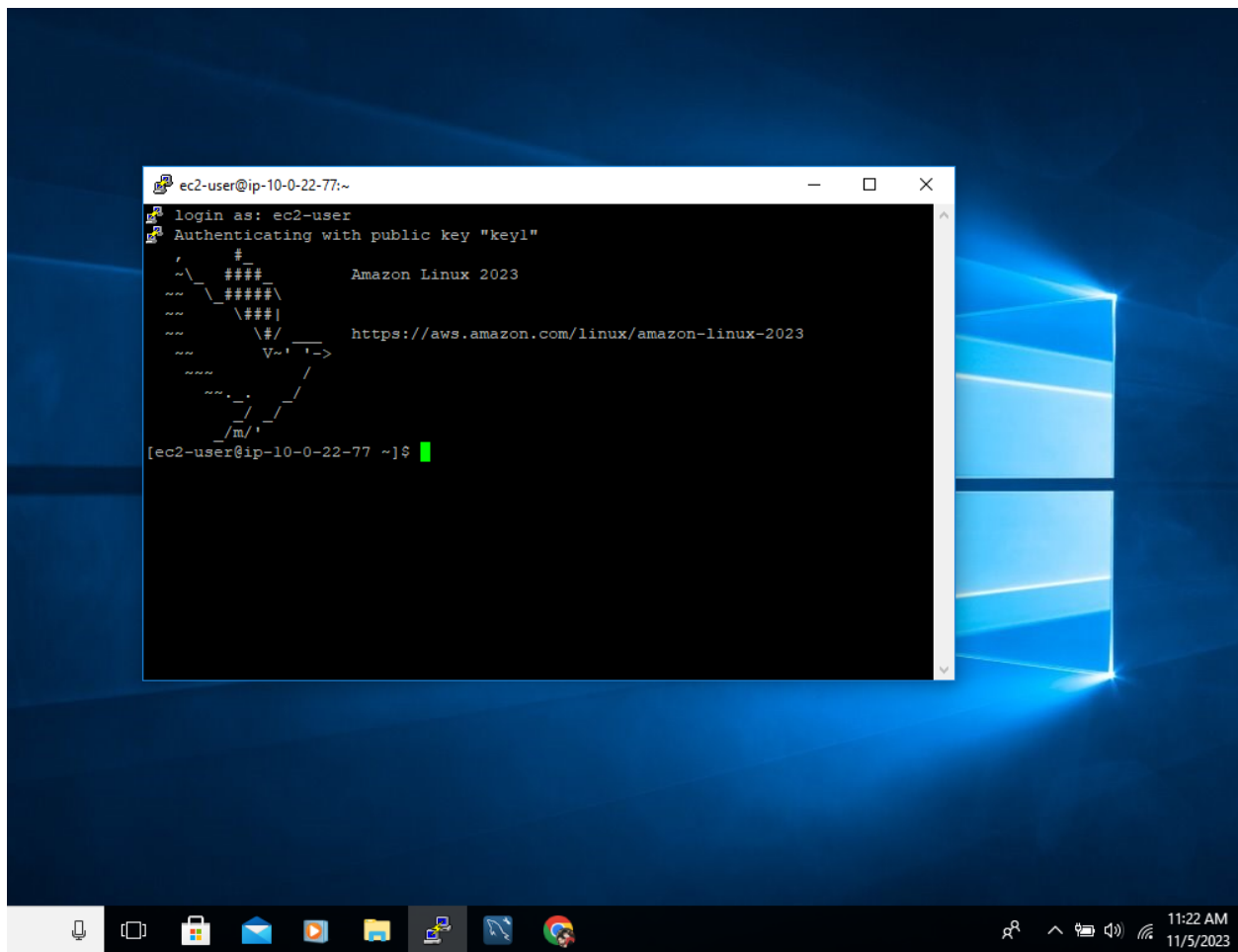
CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

11:21 AM 11/5/2023

Submit a screenshot of step 9 in which Putty successfully connects to the instance.



## Troubleshooting pinging an instance via IP address and DNS from the command line

Follow the steps to troubleshoot pinging an instance via IPv4 address and DNS from the command line:

Submit a screenshot of step 1 displaying the public DNS and IPv4 address of the instance.

Assignment 8 x Networking Lab 8 - Google Doc x Instances | EC2 | us-east-1 x +

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:sort=tag:Name

aws Services Search [Alt+S]

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
NET	i-00cf688b4b81413ec	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-54-82-47-66.com

Instance: i-00cf688b4b81413ec (NET)

Details Security Networking Storage Status checks Monitoring Tags

▼ Instance summary Info

Instance ID i-00cf688b4b81413ec (NET)	Public IPv4 address 54.82.47.66 <a href="#">open address</a>	Private IPv4 addresses 10.0.22.77
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-54-82-47-66.compute-1.amazonaws.com <a href="#">open address</a>
Hostname type IP name: in-10-0-22-77.ec2.internal	Private IP DNS name (IPv4 only) in-10-0-22-77.ec2.internal	

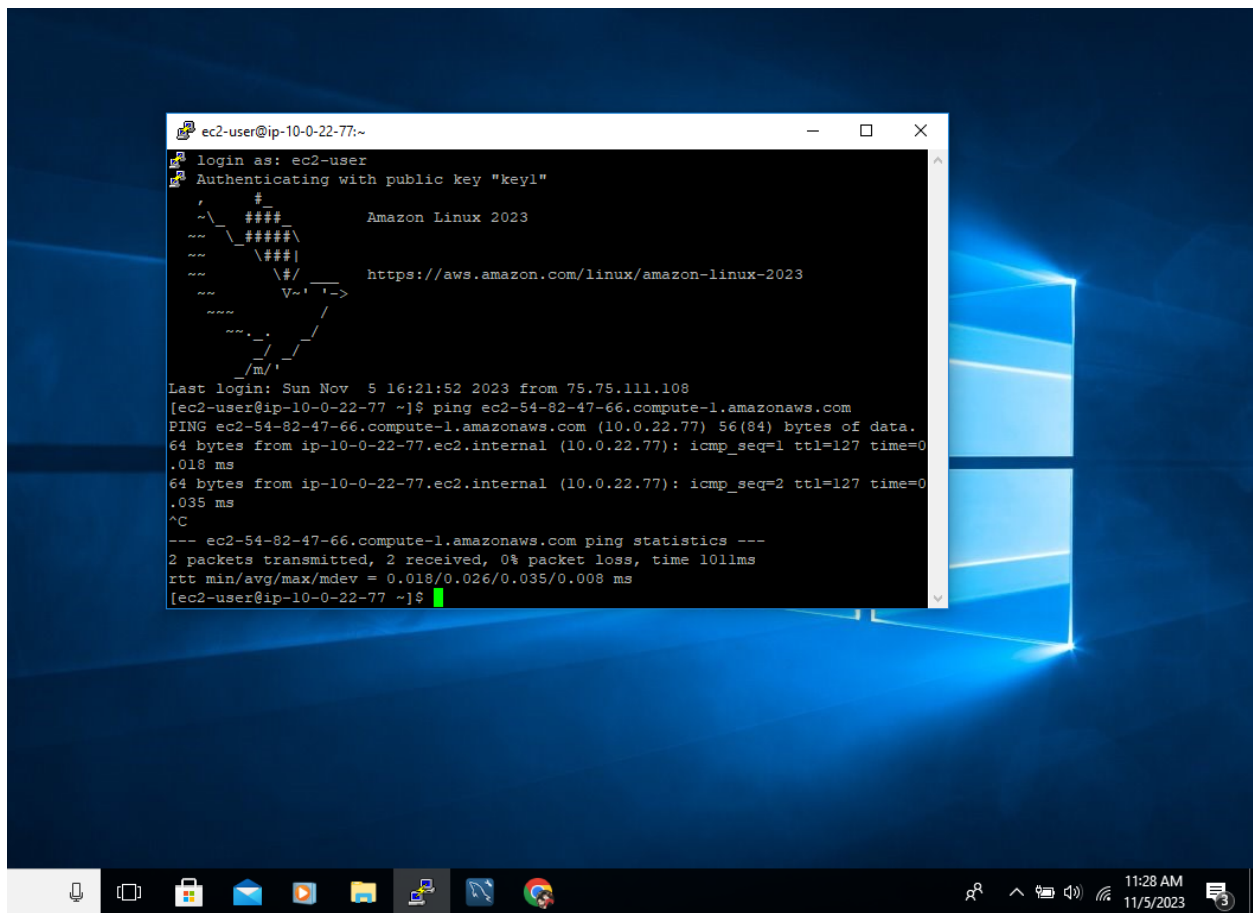
CloudShell Feedback

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

11:08 AM 11/5/2023

Submit a screenshot of step 2 pinging the instance using a public DNS from the command line.



Submit a screenshot of step 5 in which you verify that the security group has been modified with the All ICMP rule enabled.

Assignment 8 x Networking Lab 8 - Google x Instances | EC2 | us-east-1 x Security groups | EC2 | us-east-1 x ChatGPT x

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#instances:sort=tag:Name

aws Services Search [Alt+S] N. Virginia aman

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
NET	i-00cf688b4b81413ec	Running	t2.micro	2/2 checks passed	No alarms	us-east-1b	ec2-107-21-100-100

Instance: i-00cf688b4b81413ec (NET)

Inbound rules

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-0121e27582440424e	All	ICMP	75.75.111.108/32	LAB-NET

Outbound rules

CloudShell Feedback

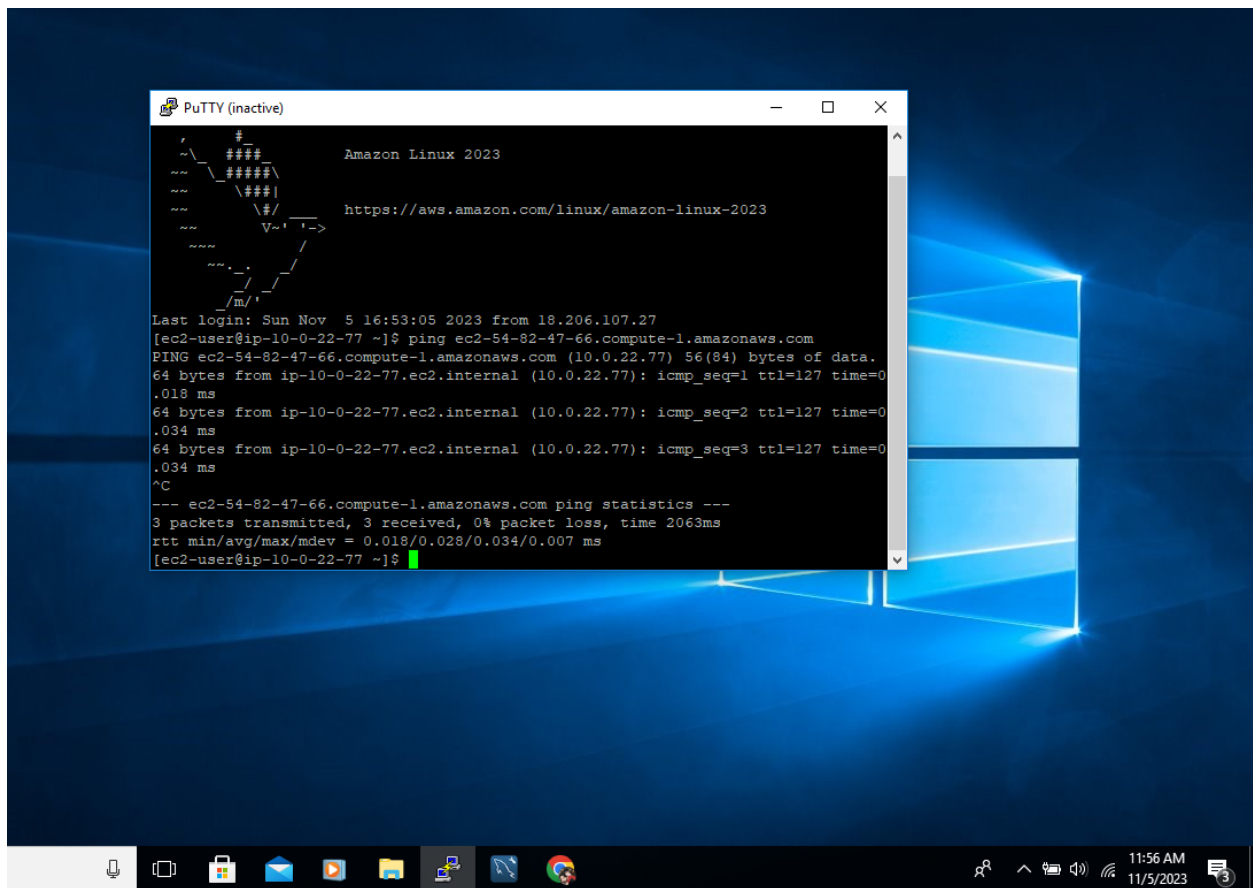
© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

11:31 AM 11/5/2023

Submit a screenshot of step 6 in which you successfully ping the instance in the VPC using a public DNS or IPv4 address.

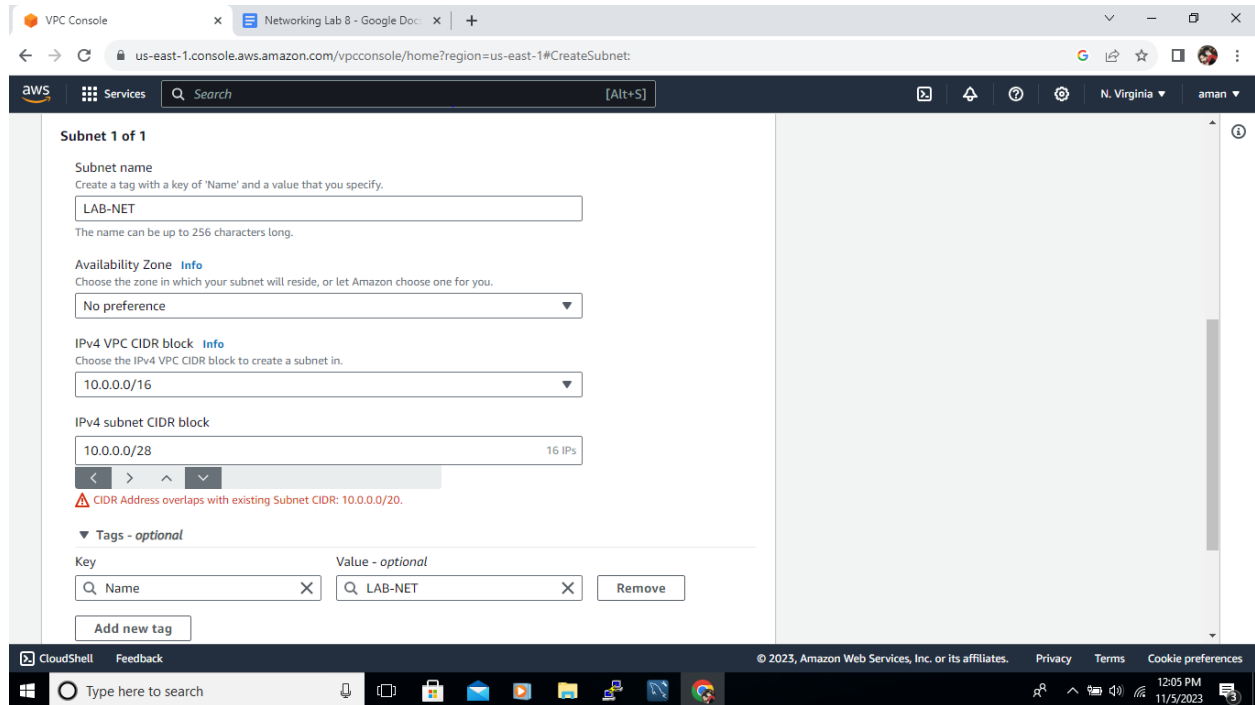




### Troubleshoot a VPC CIDR block overlap with a pre-existing CIDR block in a subnet

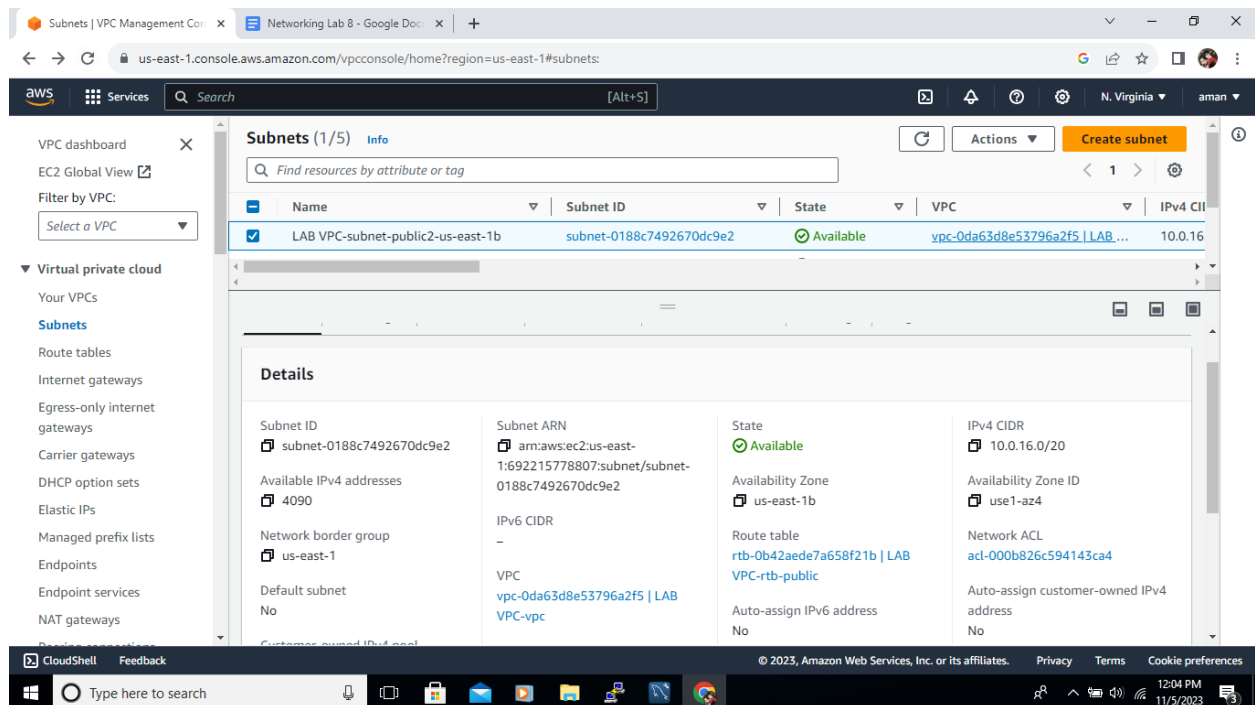
Follow the steps to troubleshoot a VPC CIDR block overlap with a pre-existing CIDR block in a subnet:

Submit a screenshot of step 4 in which you create the subnet.



Follow the steps to create a subnet that doesn't overlap.

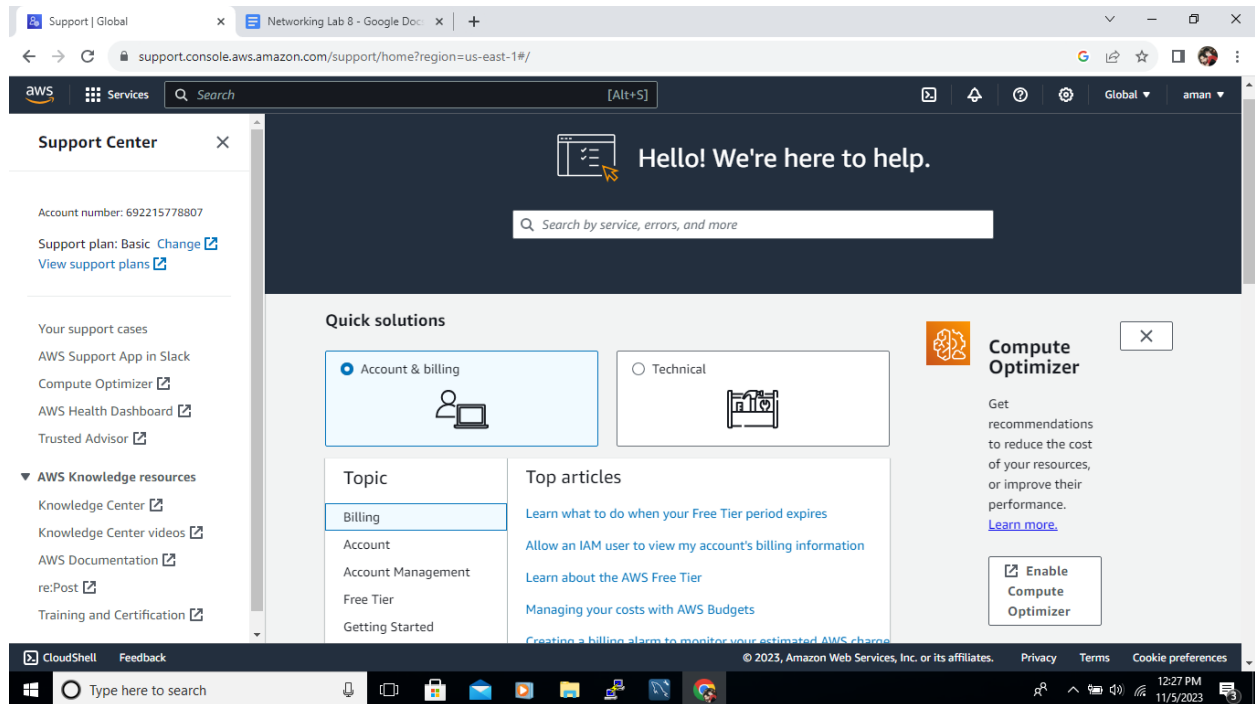
Submit a screenshot of step 2 in which you successfully create a subnet that does not overlap.



## Troubleshooting a suspended AWS Account

Follow the steps to view how to troubleshoot a suspended AWS Account.

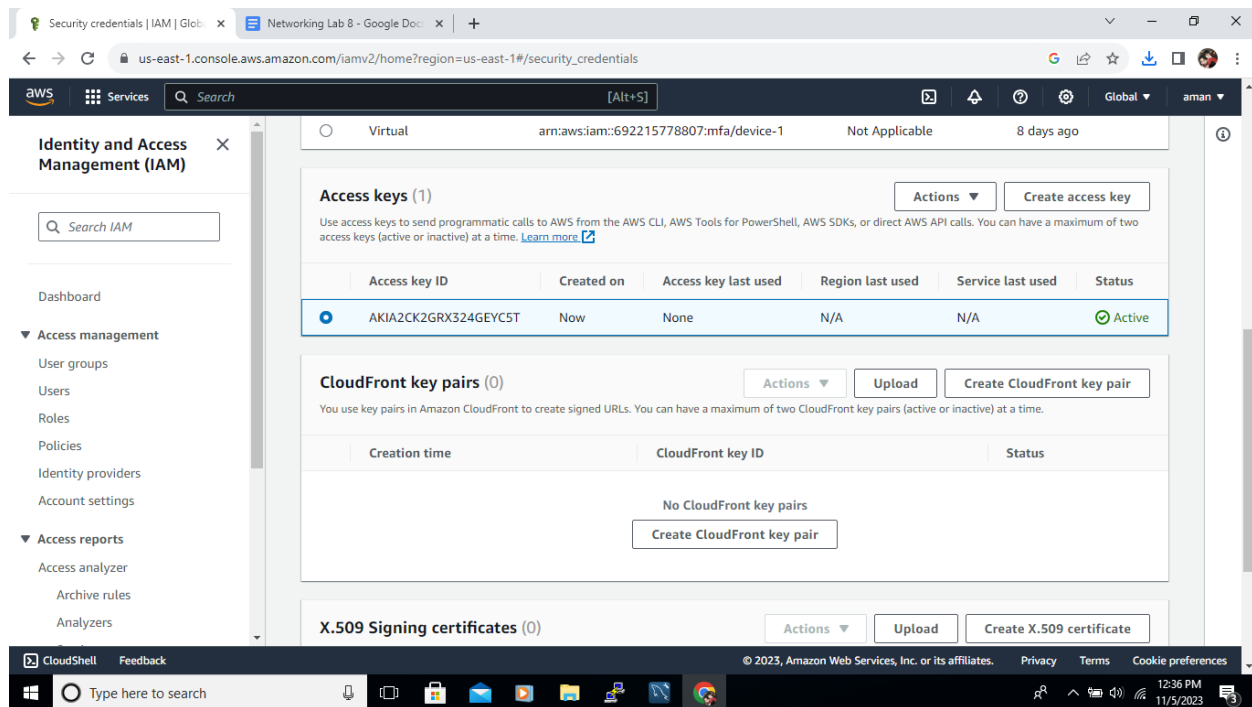
Submit a screenshot of AWS Support Center Console.



## Recovering access keys

Follow the steps to locate your access keys with AWS IAM console.

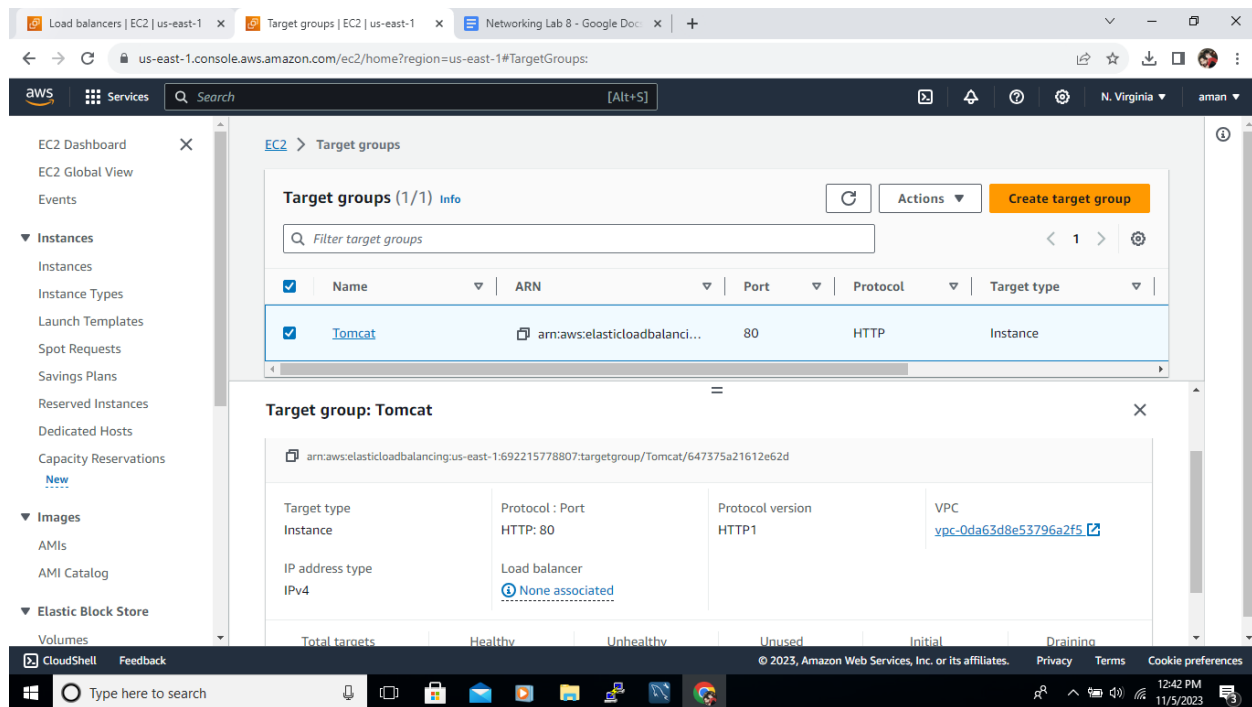
Submit a screenshot of the location of your access keys with Your Security Credentials.



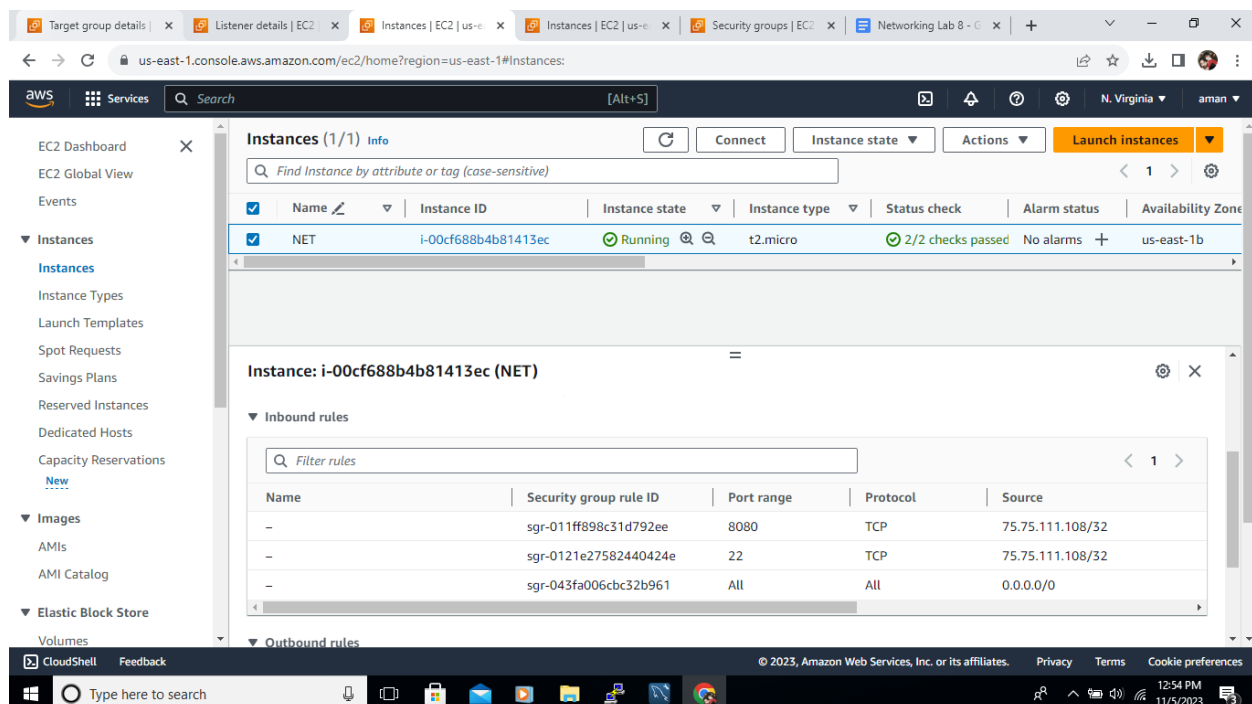
## Troubleshooting unhealthy targets for Elastic Load Balancing

Follow the steps to troubleshoot an unhealthy target assigned to Elastic Load Balancing:

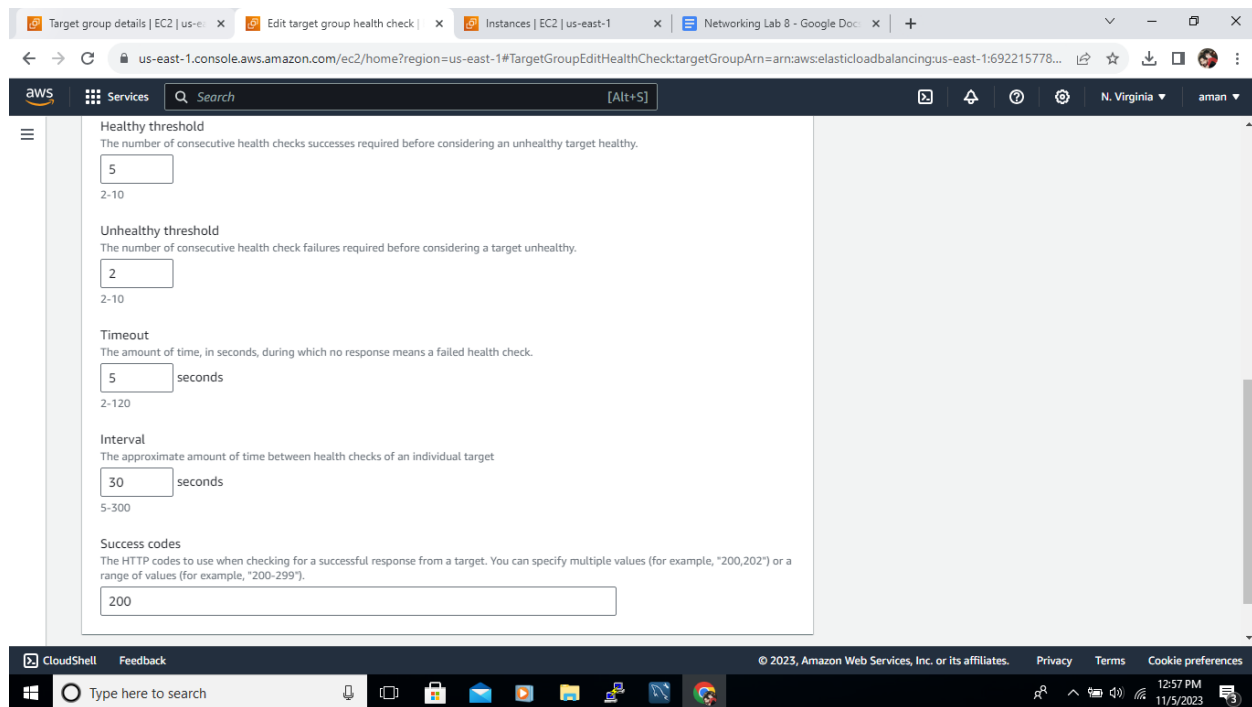
Submit a screenshot of step 1 in which you verify the listener is on port 80.



Submit a screenshot of step 3 in which you verify the registered targets, and verify have port 8080



Submit a screenshot of the Timeout, Interval, and Success codes set within the health checks of the Target Group.



## Troubleshooting connecting to a Tomcat server

Follow the steps to troubleshoot connecting to a Tomcat server. Follow the steps to edit the inbound rules in the security group associated with the instance and add a rule for port 8080.

Submit a screenshot of accessing Tomcat using the public DNS and port 8080.


← → ↻ ⚠ Not secure | 3.239.192.46:8080

🔖 ☆ 🏠 👤 ⋮


Home Documentation Configuration Examples Wiki Mailing Lists

Find Help

# Apache Tomcat/8.5.93



If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

[Security Considerations How-To](#)  
[Manager Application How-To](#)  
[Clustering/Session Replication How-To](#)

Server Status

Manager App

Host Manager

Developer Quick Start

[Tomcat Setup](#)  
[First Web Application](#)

[Realms & AAA](#)  
[JDBC DataSources](#)

[Examples](#)

[Servlet Specifications](#)  
[Tomcat Versions](#)

## Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 8.5 access to the manager application is split between different users.  
[Read more...](#)

[Release Notes](#)  
[Changelog](#)

## Documentation

[Tomcat 8.5 Documentation](#)  
[Tomcat 8.5 Configuration](#)  
[Tomcat Wiki](#)

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

[Tomcat 8.5 Bug Database](#)

## Getting Help

### FAQ and Mailing Lists

The following mailing lists are available:


[tomcat-announce](#)  
Important announcements, releases, security vulnerability notifications. (Low volume).

[tomcat-users](#)  
User support and discussion

[taglibs-user](#)  
User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)

Time here to search



6:45 PM