Troubleshooting AWS Network Connectivity: Security Groups and NACLs

00:53:50 Exit Lab Complete Lab

1 hour 30 minutes duration Practitioner Rate this lab

Videos Guide

Troubleshooting AWS Network Connectivity: Security Groups and NACLs

Introduction

Troubleshooting basic network connectivity issues is an important skill. This troubleshooting scenario is an opportunity to assess your skills in this area.

In this lab scenario, a junior administrator has deployed a VPC and instances, but there are a few things wrong. `Instance3` is not able to connect to the internet and the junior admin can't determine why. Being a senior administrator, it's your responsibility to troubleshoot the issue and ensure the instance has connectivity to the internet, so that you can ping and log in to the instance using SSH.

Solution

Log in to the AWS Management Console using the credentials provided on the lab instructions page. Make sure you're using the *us-east-1* region.

Determine Why the Instance Cannot Connect to the Internet

1. Navigate to the **EC2** dashboard.
2. Click **Instances (running)**.
3. Select **Instance3** from the list and review the instance details. *(NOTE: Notice `Instance3` does not have a public IP address.)*
4. At the top of the page, click **Actions**, to select **Networking**, and select **Manage IP addresses**.
5. In the tooltip box, click **allocate** to be redirected to the Elastic IP addresses list.
6. In the top-right corner, click **Allocate Elastic IP address**.
7. Leave the settings as default and click **Allocate**.
8. Select the IP address and click the **Actions** dropdown menu to select **Associate Elastic IP address**.
9. For *Instance*, select **Instance3** and click **Associate**.
10. In the left-hand menu, click **Instances**.
11. Select **Instance3** from the list and review the instance details. *(NOTE: Notice `Instance3` now has a public IP address.)*
12. Copy the public IP address of Instance 3 and attempt to ping the instance from either your own local terminal or ssh into Instance 1. to do the ping test:
    ```
    ping <Instance3_Public_IP_Address>
    ```

Identify the Issues Preventing the Instance from Connecting to the Internet

1. Navigate back to AWS Instances page.
2. Select **Instance3** from the list of instances.
3. Click **Security** tab to review the associated security group.
4. Review the security group details.
5. In the left-hand menu, click **Security Groups**.

6. Scroll to **Security group name** and expand the field to locate `EC2SecurityGroup3`.
7. Click **Inbound rules** tab to view the allow and deny inbound rules.
8. Click **Outbound rules** tab to view the allow and deny outbound rules.
9. In the left-hand menu, click **Instances**.
10. Select **Instance3** and click **Networking** tab to view the private subnet IP address.
11. In a new tab, navigate to **VPC**.
12. In the left-hand menu, click **Subnets** to find the private subnet IP address that matches `Instance3`.
13. Select **PublicSubnet4** and click **Network ACL** tab.
14. Click on the link next to *Network ACL*.
15. Click **Inbound rules** tab to view the allow and deny inbound rules.
16. Click **Outbound rules** tab to view the allow and deny outbound rules.
17. Click the "X" on the *Network ACL ID* or **Clear filters** to view all available Network ACLs.
18. Select **Public3-NACL**.
19. Click **Inbound rules** tab to view the allow and deny inbound rules.
20. Click **Outbound rules** tab to view the allow and deny outbound rules.
21. In the left-hand menu, click **Subnets** and select **PublicSubnet4**.
22. Click **Network ACL** tab and click **Edit network ACL association**.
23. For *Network ACL ID*, select **Public3-NACL** from the dropdown menu.
24. Click **Save**.
25. Navigate back to the terminal to verify ping results.
26. Navigate back to the AWS Subnets page and click **Route table** tab to view the associated route table, `Private3-RT`.
27. Click **Edit route table association**.
28. For *Route table ID*, select **Public3-RT** from the dropdown menu.
29. Click **Save**.
30. In the left-hand menu, click **Route Tables**.
31. Select **Public3-RT** and click **Routes** tab to view the routes attached.
32. Navigate back to the terminal to confirm successful ping results. *(NOTE: Feel free to try to SSH using the provided credentials.)*

Conclusion

Congratulations — you've completed this hands-on lab!

Tools

Lab Diagram Instant Terminal

Credentials

How do I connect?

AWS Account

Username

cloud_user

Password

RAq!q0PG6g6oe^7*Su$S

Open Link in Incognito Window

Cloud Server INSTANCE1

Username

cloud_user

Password

G4uEOg7]

PRIVATE IP address of INSTANCE1

10.1.0.238

PUBLIC IP address of INSTANCE1

3.80.212.161

Launch Instant Terminal

Additional Resources

Make sure you are in the `us-east-1 region`.

Based on our scenario, you will need to troubleshoot why `Instance3` is not internet accessible. There are issues preventing the instance from connecting to the internet. Your task is to identify and fix those issues, then verify SSH connectivity to the instance.

Need a hint? Review the Solution Hints video. You can verify your solution by watching the Solution video.

> *Note:* The assigning of the Elastic IP steps have slightly changed. See the lab guide on the assigning of the Elastic IP steps if needed.

Learning Objectives

0 of 2 completed

- [ ] Determine Why the Instance Cannot Connect to the Internet
- [ ] Identify the Issues Preventing the Instance from Connecting to the Internet