Task 3: L1 / L2 Troubleshooting Scenarios

VPC with Public & Private Subnets, NAT Gateway, and Bastion Host

This document lists **real-time L1 and L2 troubleshooting scenarios** based on the Task 3 architecture. Scenarios are written exactly how issues appear in **production / support environments**.

🔹 L1 TROUBLESHOOTING SCENARIOS

(L1 focuses on basic checks, connectivity, and escalation)

L1 Scenario 1: Unable to SSH into Bastion Host

Issue:
User cannot SSH into the Bastion EC2 instance.

L1 Checks: - Verify Bastion instance is in **running state** - Confirm correct **public IP** is used - Verify **key pair** permissions (`chmod 400 key.pem`) - Check security group allows **port 22 from user IP**

Resolution:
Correct SSH command or security group rule.

Escalation:
If still failing, escalate to L2 for route/NACL analysis.

L1 Scenario 2: Bastion Host Has No Internet Access

Issue:
Bastion cannot reach the internet.

L1 Checks: - Verify Bastion is in a **public subnet** - Check subnet route table has `0.0.0.0/0 → IGW` - Ensure **public IP** is assigned

Resolution:
Attach correct route table or enable public IP.

L1 Scenario 3: Private EC2 Not Reachable from Bastion

Issue:
SSH from Bastion to Private EC2 fails.

L1 Checks: - Confirm private EC2 is **running** - Verify correct **private IP** is used - Check private EC2 security group allows SSH from Bastion SG

Resolution:
Fix security group inbound rule.

L1 Scenario 4: CloudFormation Stack Failed

Issue:
Stack creation failed.

L1 Checks: - Review **Events tab** for error message - Check key pair exists - Validate template format

Resolution:
Fix parameter or retry deployment.

🔹 L2 TROUBLESHOOTING SCENARIOS

(L2 focuses on routing, NAT, NACLs, and deeper analysis)

L2 Scenario 1: Private EC2 Cannot Access Internet

Issue:
Private EC2 cannot run `yum update` or access external sites.

L2 Checks: - Verify private route table has `0.0.0.0/0 → NAT Gateway` - Confirm NAT Gateway is **Available** - Check NAT Gateway is in **public subnet** - Verify Elastic IP attached

Resolution:
Fix route table or recreate NAT Gateway.

L2 Scenario 2: NAT Gateway Exists but Traffic Fails

Issue:
NAT Gateway is present but private EC2 still has no outbound access.

L2 Checks: - Verify public subnet route table has IGW - Check NACL rules allow outbound traffic - Verify source/destination check

Resolution:
Correct NACL or routing configuration.

L2 Scenario 3: Intermittent SSH Issues to Private EC2

Issue:
SSH works sometimes but fails intermittently.

L2 Checks: - Check NACL rules for ephemeral ports - Verify Bastion CPU/memory usage - Review VPC Flow Logs

Resolution:
Fix NACL rules or scale Bastion instance.

L2 Scenario 4: Wrong Subnet Association

Issue:
Private EC2 accidentally launched in public subnet.

L2 Checks: - Verify subnet ID - Check auto-assign public IP setting

Resolution:
Terminate and relaunch EC2 in correct subnet.

L2 Scenario 5: Security Hardening Requirement

Issue:
Security team requests tighter SSH access.

L2 Actions: - Restrict Bastion SSH to corporate IP range - Enable Session Manager as alternative - Enable VPC Flow Logs

---

🔹 Common Commands Used in Troubleshooting

```
ssh -i key.pem ec2-user@<bastion-ip>
ssh -i key.pem ec2-user@<private-ip>
```

```
traceroute google.com
ping 8.8.8.8
```

🔹 Escalation Matrix

Issue Type	L1	L2
SSH Access	✔️	✔️
Routing	❌	✔️
NAT Issues	❌	✔️
NACL Issues	❌	✔️

🔹 Interview Tip

> Always explain **what you check first**, **why**, and **when you escalate**.

End of Document