Activity 7: Troubleshoot a VPC

Spurthy Mutturaj

Information Technology, Arizona State University

IFT 562: Cloud Security & Operations for IT

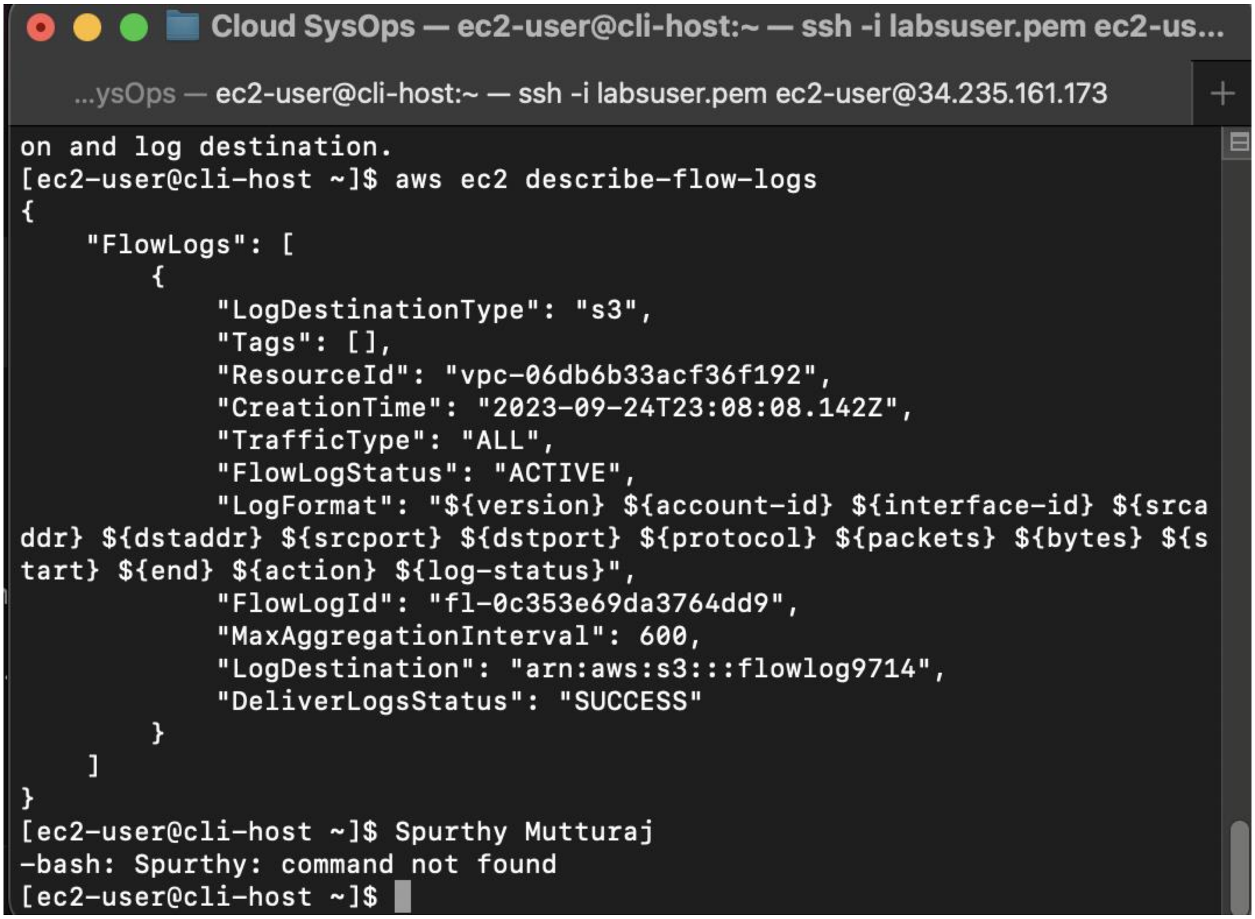
Daniel Wells

Sep 24, 2023

Activity 7: Troubleshoot a VPC

Figure 1

A screenshot to confirm the flow logs were created.

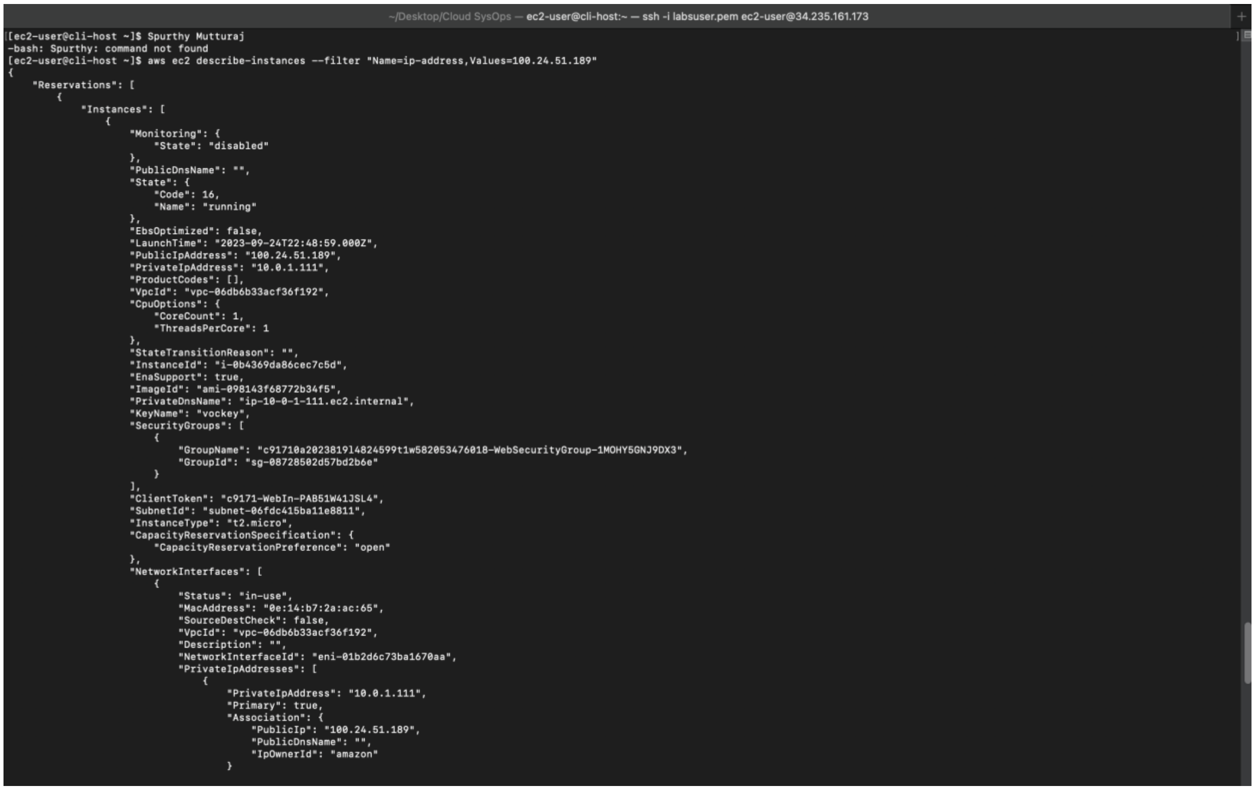


Cloud SysOps — ec2-user@cli-host:~ — ssh -i labsuser.pem ec2-us...
...ysOps — ec2-user@cli-host:~ — ssh -i labsuser.pem ec2-user@34.235.161.173

```
on and log destination.
[ec2-user@cli-host ~]$ aws ec2 describe-flow-logs
{
    "FlowLogs": [
        {
            "LogDestinationType": "s3",
            "Tags": [],
            "ResourceId": "vpc-06db6b33acf36f192",
            "CreationTime": "2023-09-24T23:08:08.142Z",
            "TrafficType": "ALL",
            "FlowLogStatus": "ACTIVE",
            "LogFormat": "${version} ${account-id} ${interface-id} ${srca
ddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${s
tart} ${end} ${action} ${log-status}",
            "FlowLogId": "fl-0c353e69da3764dd9",
            "MaxAggregationInterval": 600,
            "LogDestination": "arn:aws:s3:::flowlog9714",
            "DeliverLogsStatus": "SUCCESS"
        }
    ]
}
[ec2-user@cli-host ~]$ Spurthy Mutturaj
-bash: Spurthy: command not found
[ec2-user@cli-host ~]$
```

Figure 2

Screenshot of command to show the EC2 instance - Web Server.

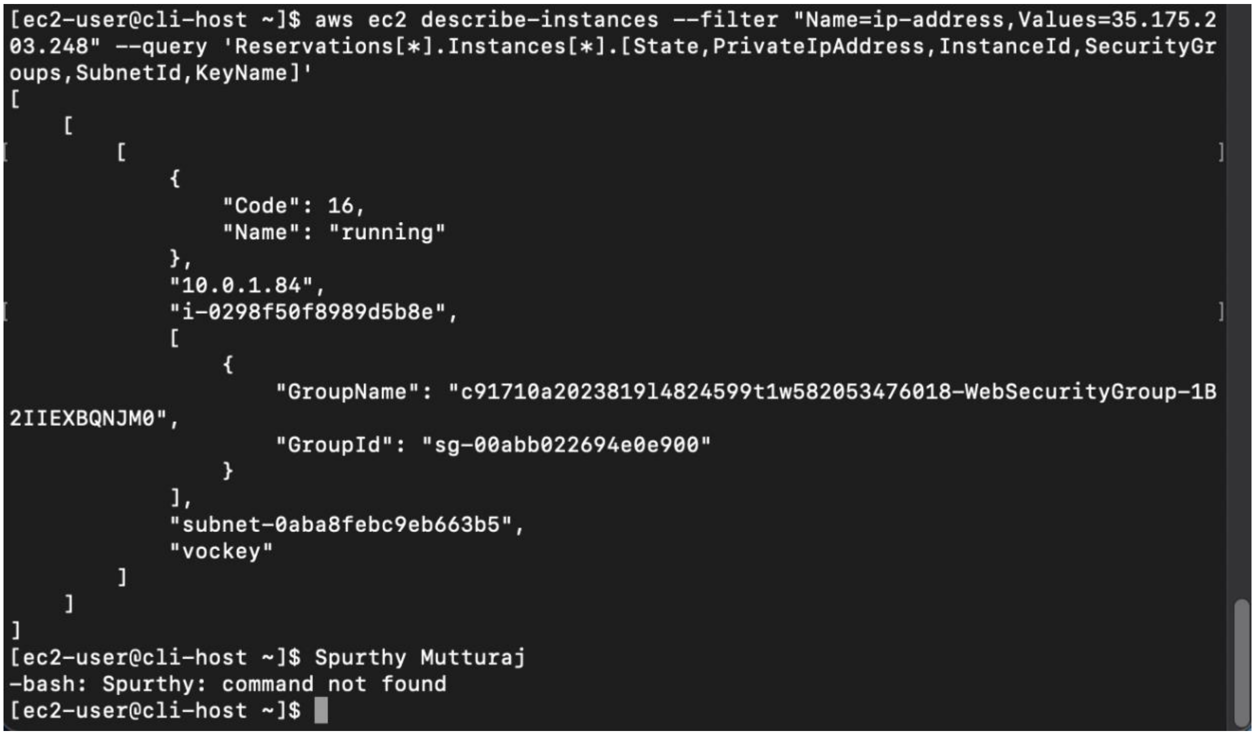

~/Desktop/Cloud SysOps — ec2-user@cli-host:~ — ssh -i labsuser.pem ec2-user@34.235.161.173

```
[[ec2-user@cli-host ~]$ Spurthy Mutturaj
-bash: Spurthy: command not found
[ec2-user@cli-host ~]$ aws ec2 describe-instances --filter "Name=ip-address,Values=100.24.51.189"
{
    "Reservations": [
        {
            "Instances": [
                {
                    "Monitoring": {
                        "State": "disabled"
                    },
                    "PublicDnsName": "",
                    "State": {
                        "Code": 16,
                        "Name": "running"
                    },
                    "EbsOptimized": false,
                    "LaunchTime": "2023-09-24T22:48:59.000Z",
                    "PublicIpAddress": "100.24.51.189",
                    "PrivateIpAddress": "10.0.1.111",
                    "ProductCodes": [],
                    "VpcId": "vpc-06db6b33acf36f192",
                    "CpuOptions": {
                        "CoreCount": 1,
                        "ThreadsPerCore": 1
                    },
                    "StateTransitionReason": "",
                    "InstanceId": "i-0b4369da86cec7c5d",
                    "EnaSupport": true,
                    "ImageId": "ami-098143f68772b34f5",
                    "PrivateDnsName": "ip-10-0-1-111.ec2.internal",
                    "KeyName": "vockey",
                    "SecurityGroups": [
                        {
                            "GroupName": "c91710a2023819l4824599t1w582053476018-WebSecurityGroup-1MOHY5GNJ9DX3",
                            "GroupId": "sg-08728502d57bd2b6e"
                        }
                    ],
                    "ClientToken": "c9171-WebIn-PAB51W41JSL4",
                    "SubnetId": "subnet-06fdc415ba11e8811",
                    "InstanceType": "t2.micro",
                    "CapacityReservationSpecification": {
                        "CapacityReservationPreference": "open"
                    },
                    "NetworkInterfaces": [
                        {
                            "Status": "in-use",
                            "MacAddress": "0e:14:b7:2a:ac:65",
                            "SourceDestCheck": false,
                            "VpcId": "vpc-06db6b33acf36f192",
                            "Description": "",
                            "NetworkInterfaceId": "eni-01b2d6c73ba1670aa",
                            "PrivateIpAddresses": [
                                {
                                    "PrivateIpAddress": "10.0.1.111",
                                    "Primary": true,
                                    "Association": {
                                        "PublicIp": "100.24.51.189",
                                        "PublicDnsName": "",
                                        "IpOwnerId": "amazon"
                                    }
```

Note. My name is typed in the first line (step 32).

Figure 3

Screenshot of command to show the EC2 instance filtered results - Web Server.

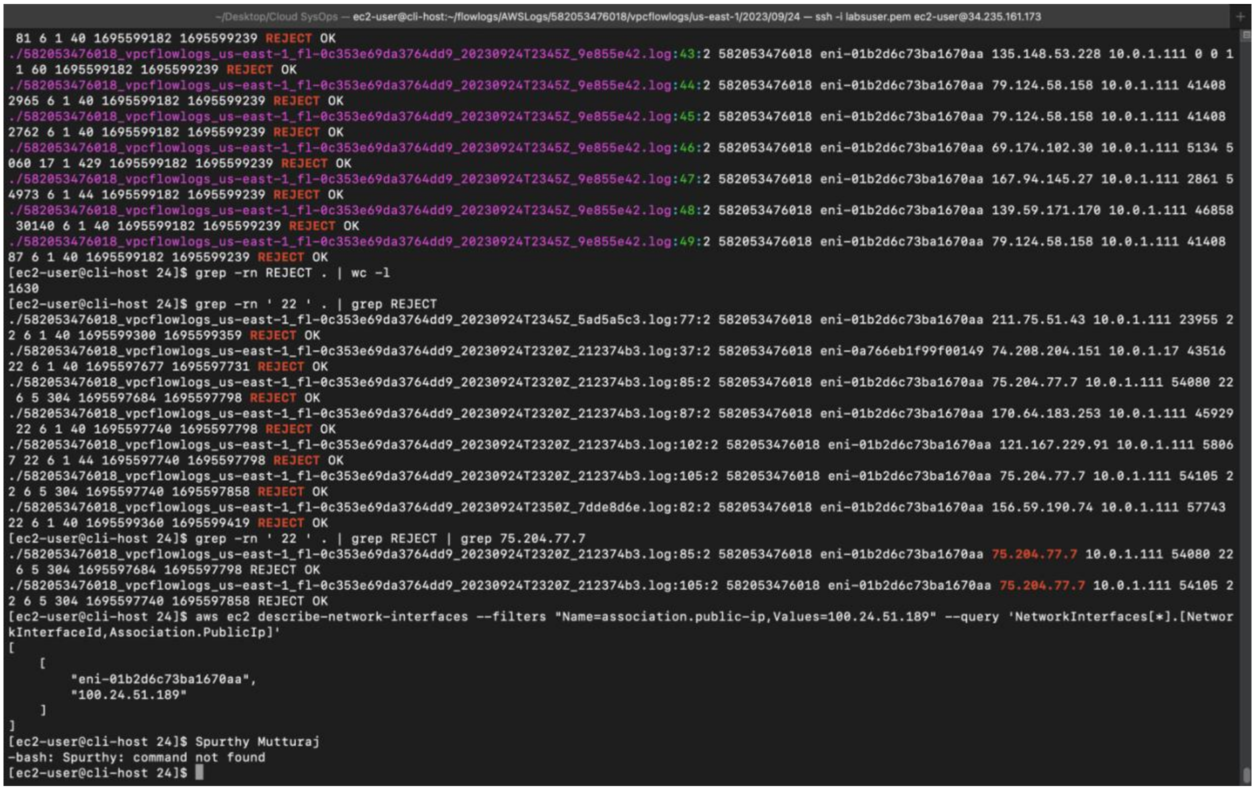


```
[ec2-user@cli-host ~]$ aws ec2 describe-instances --filter "Name=ip-address,Values=35.175.2
03.248" --query 'Reservations[*].Instances[*].[State,PrivateIpAddress,InstanceId,SecurityGr
oups,SubnetId,KeyName]'
[
    [
        [
            {
                "Code": 16,
                "Name": "running"
            },
            "10.0.1.84",
            "i-0298f50f8989d5b8e",
            [
                {
                    "GroupName": "c91710a2023819l4824599t1w582053476018-WebSecurityGroup-1B
2IIEXBQNJM0",
                    "GroupId": "sg-00abb022694e0e900"
                }
            ],
            "subnet-0aba8febc9eb663b5",
            "vockey"
        ]
    ]
]
[ec2-user@cli-host ~]$ Spurthy Mutturaj
-bash: Spurthy: command not found
[ec2-user@cli-host ~]$ 
```

Note. Step 33.

Figure 4

Screenshot of describe-network-interfaces command.


~/Desktop/Cloud SysOps — ec2-user@cli-host:~/flowlogs/AWSLogs/582053476018/vpcflowlogs/us-east-1/2023/09/24 — ssh -i labsuser.pem ec2-user@34.235.161.173

```
 81 6 1 40 1695599182 1695599239 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_9e855e42.log:43:2 582053476018 eni-01b2d6c73ba1670aa 135.148.53.228 10.0.1.111 0 0 1
 1 60 1695599182 1695599239 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_9e855e42.log:44:2 582053476018 eni-01b2d6c73ba1670aa 79.124.58.158 10.0.1.111 41408
2965 6 1 40 1695599182 1695599239 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_9e855e42.log:45:2 582053476018 eni-01b2d6c73ba1670aa 79.124.58.158 10.0.1.111 41408
2762 6 1 40 1695599182 1695599239 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_9e855e42.log:46:2 582053476018 eni-01b2d6c73ba1670aa 69.174.102.30 10.0.1.111 5134 5
060 17 1 429 1695599182 1695599239 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_9e855e42.log:47:2 582053476018 eni-01b2d6c73ba1670aa 167.94.145.27 10.0.1.111 2861 5
4973 6 1 44 1695599182 1695599239 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_9e855e42.log:48:2 582053476018 eni-01b2d6c73ba1670aa 139.59.171.170 10.0.1.111 46858
 30140 6 1 40 1695599182 1695599239 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_9e855e42.log:49:2 582053476018 eni-01b2d6c73ba1670aa 79.124.58.158 10.0.1.111 41408
87 6 1 40 1695599182 1695599239 REJECT OK
[ec2-user@cli-host 24]$ grep -rn REJECT . | wc -l
1630
[ec2-user@cli-host 24]$ grep -rn ' 22 ' . | grep REJECT
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2345Z_5ad5a5c3.log:77:2 582053476018 eni-01b2d6c73ba1670aa 211.75.51.43 10.0.1.111 23955 2
2 6 1 40 1695599300 1695599359 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2320Z_212374b3.log:37:2 582053476018 eni-0a766eb1f99f00149 74.208.204.151 10.0.1.17 43516
22 6 1 40 1695597677 1695597731 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2320Z_212374b3.log:85:2 582053476018 eni-01b2d6c73ba1670aa 75.204.77.7 10.0.1.111 54080 22
 6 5 304 1695597684 1695597798 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2320Z_212374b3.log:87:2 582053476018 eni-01b2d6c73ba1670aa 170.64.183.253 10.0.1.111 45929
 22 6 1 40 1695597740 1695597798 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2320Z_212374b3.log:102:2 582053476018 eni-01b2d6c73ba1670aa 121.167.229.91 10.0.1.111 5806
7 22 6 1 44 1695597740 1695597798 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2320Z_212374b3.log:105:2 582053476018 eni-01b2d6c73ba1670aa 75.204.77.7 10.0.1.111 54105 2
2 6 5 304 1695597740 1695597858 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2350Z_7dde8d6e.log:82:2 582053476018 eni-01b2d6c73ba1670aa 156.59.190.74 10.0.1.111 57743
22 6 1 40 1695599360 1695599419 REJECT OK
[ec2-user@cli-host 24]$ grep -rn ' 22 ' . | grep REJECT | grep 75.204.77.7
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2320Z_212374b3.log:85:2 582053476018 eni-01b2d6c73ba1670aa 75.204.77.7 10.0.1.111 54080 22
 6 5 304 1695597684 1695597798 REJECT OK
./582053476018_vpcflowlogs_us-east-1_fl-0c353e69da3764dd9_20230924T2320Z_212374b3.log:105:2 582053476018 eni-01b2d6c73ba1670aa 75.204.77.7 10.0.1.111 54105 2
2 6 5 304 1695597740 1695597858 REJECT OK
[ec2-user@cli-host 24]$ aws ec2 describe-network-interfaces --filters "Name=association.public-ip,Values=100.24.51.189" --query 'NetworkInterfaces[*].[Networ
kInterfaceId,Association.PublicIp]'
[
    [
        "eni-01b2d6c73ba1670aa",
        "100.24.51.189"
    ]
]
[ec2-user@cli-host 24]$ Spurthy Mutturaj
-bash: Spurthy: command not found
[ec2-user@cli-host 24]$ 
```