ATTACK DEFENSE

by PentesterAcademy

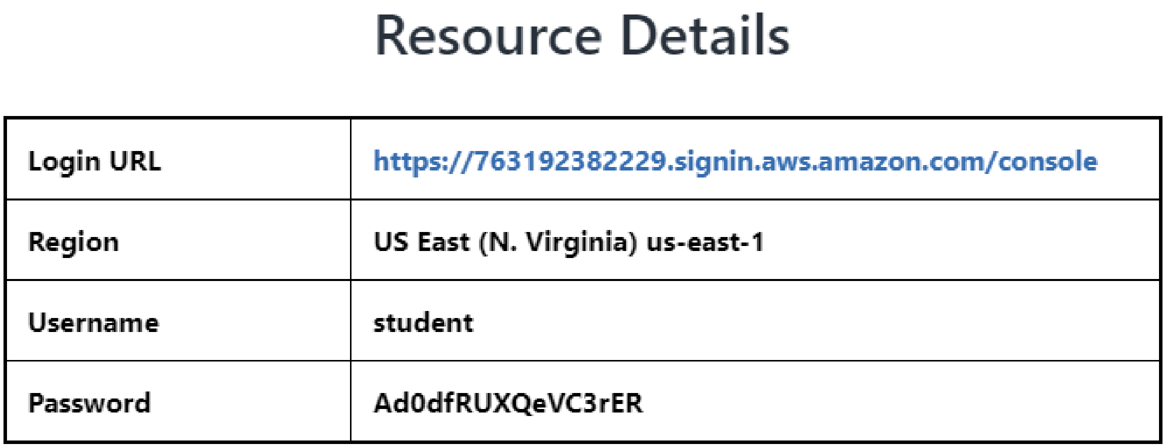
Name	ECS Enumeration
URL	https://attackdefense.com/challengedetails?cid=2444
Type	AWS Cloud Security : ECS and ECR

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

We will enumerate the ECS service provided by amazon. ECS stands for Elastic Container Service it is a container orchestration service that makes it easy to deploy, manage, and scale containerized applications.

Step 1: Click on the lab link button to get access to AWS lab credentials.

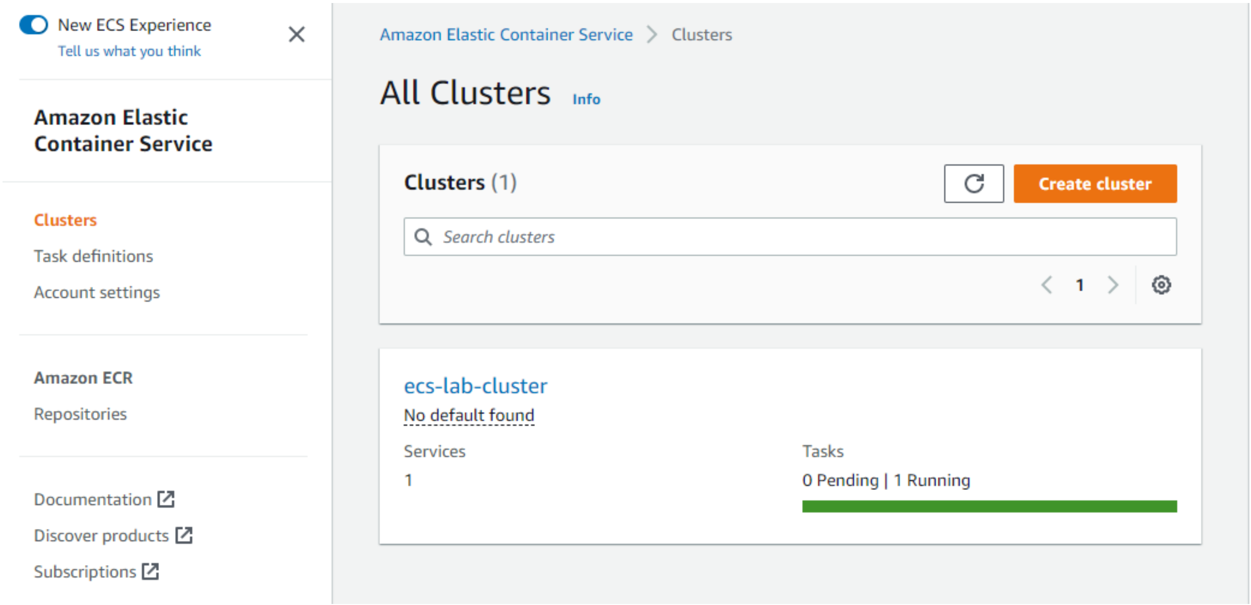


Resource Details

Login URL	https://763192382229.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad0dfRUXQeVC3rER

Step 2: Log in to the AWS account through the console search for Elastic Container Service and click on it.

Step 3: Switch to the new ECS experience by using the toggle. This page gives an overview of the clusters and the tasks running on these clusters. Click on the **ecs-lab-cluster.**

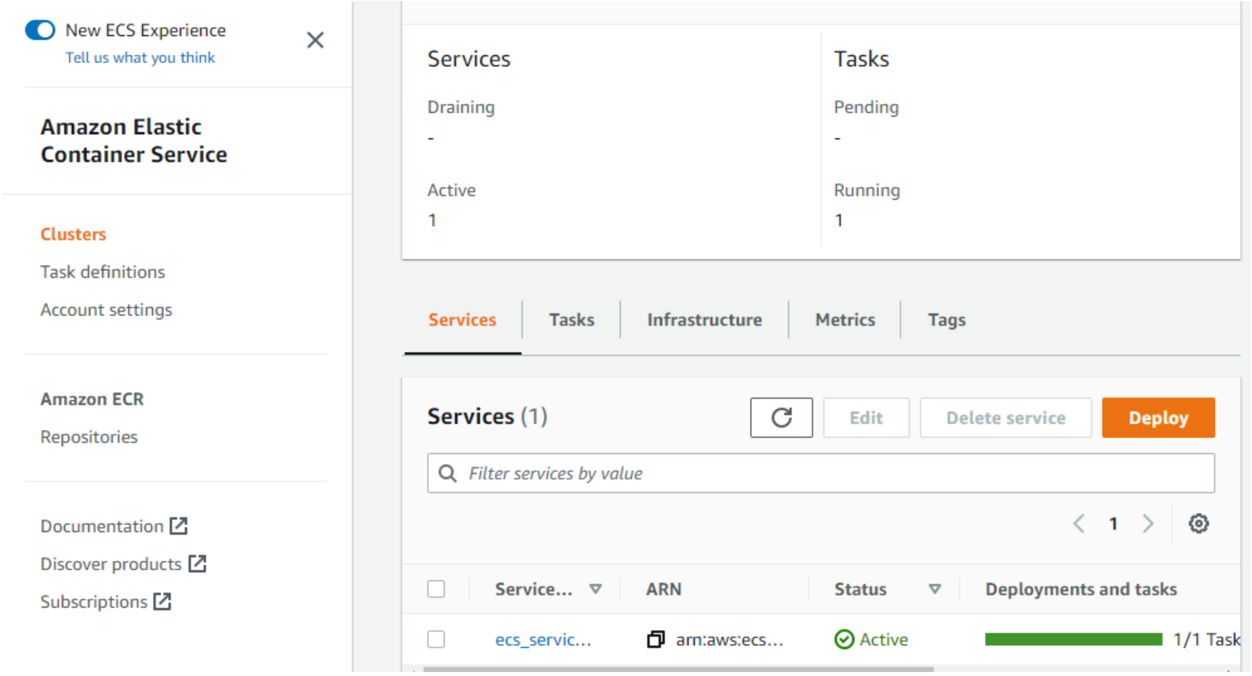


ecs-lab-cluster

No default found

Services: 1

Tasks: 0 Pending | 1 Running



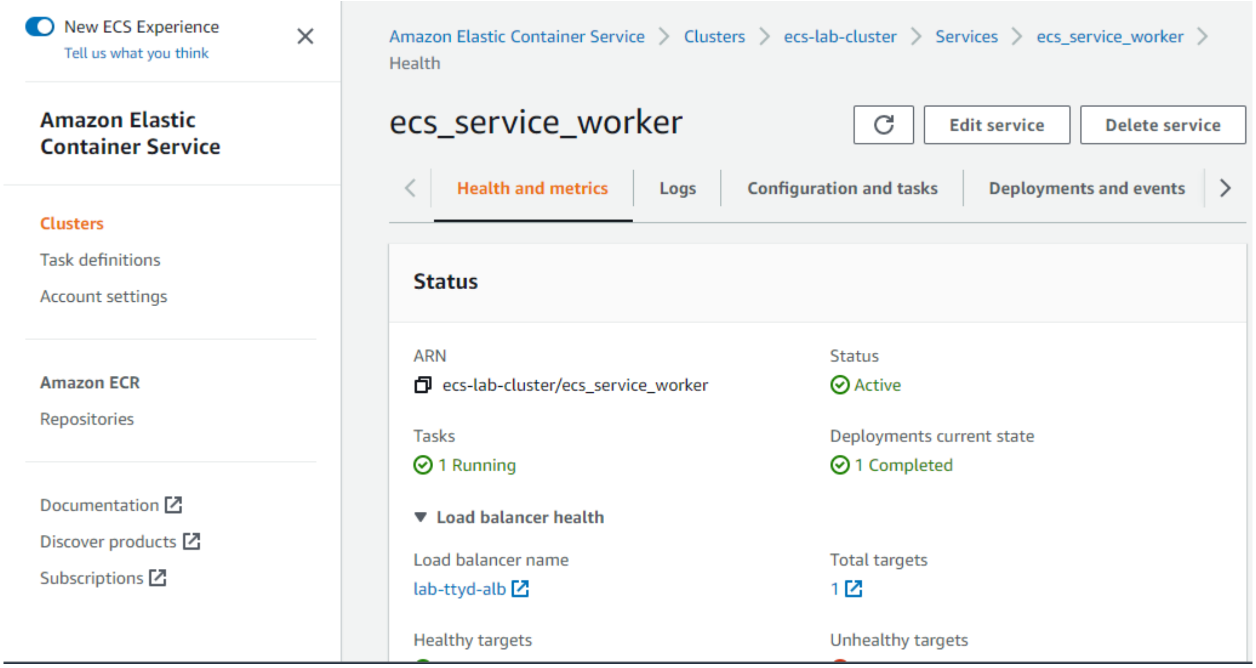
Services	Tasks
Draining	Pending
-	-
Active	Running
1	1

Services (1)

□	Service...	ARN	Status	Deployments and tasks
□	ecs_servic...	arn:aws:ecs...	✓ Active	🟩 1/1 Task

The Services overview tab displays the running services on the cluster. A service makes sure that a particular number of tasks are continuously running on the cluster. The tasks to be run can be configured by using the task definition.

Step 4: Click on the **ecs_service_worker** service.



ecs_service_worker

Status

ARN
ecs-lab-cluster/ecs_service_worker

Status
Active

Tasks
1 Running

Deployments current state
1 Completed

Load balancer health

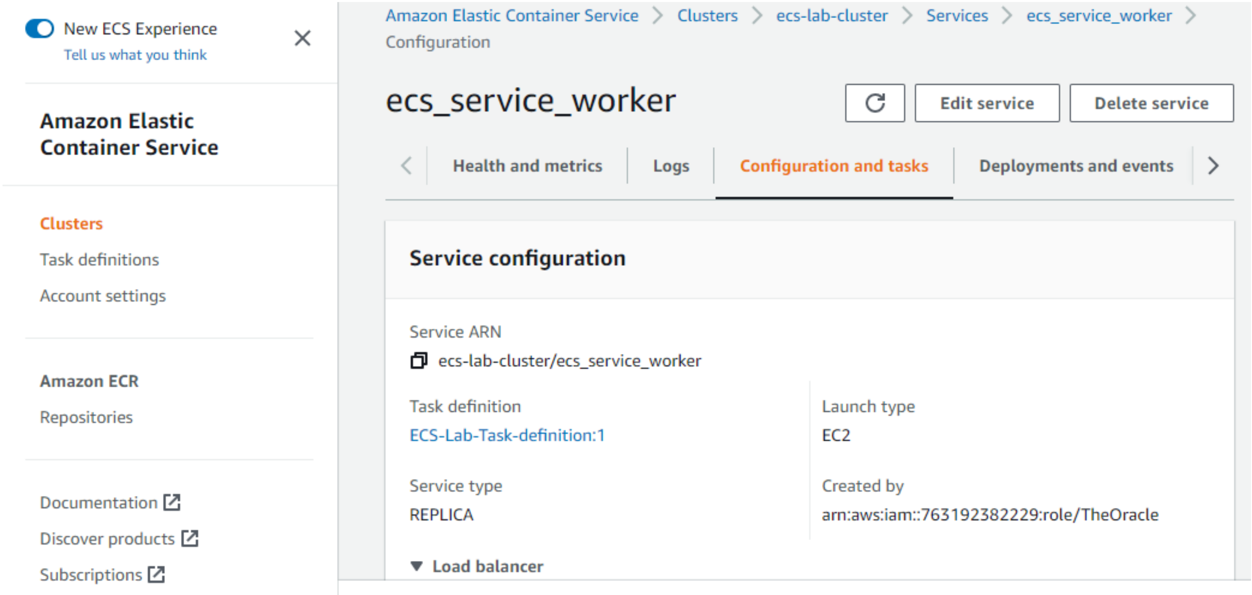
Load balancer name
lab-ttyd-alb

Total targets
1

Healthy targets

Unhealthy targets

This page displays the status of the service tasks, for an ideal situation the Desired tasks should be equal to the Running tasks. This page also shows the CPU and memory utilization of the task on the host EC2 instance. Next click on the Configuration and tasks tab.



ecs_service_worker

Service configuration

Service ARN
ecs-lab-cluster/ecs_service_worker

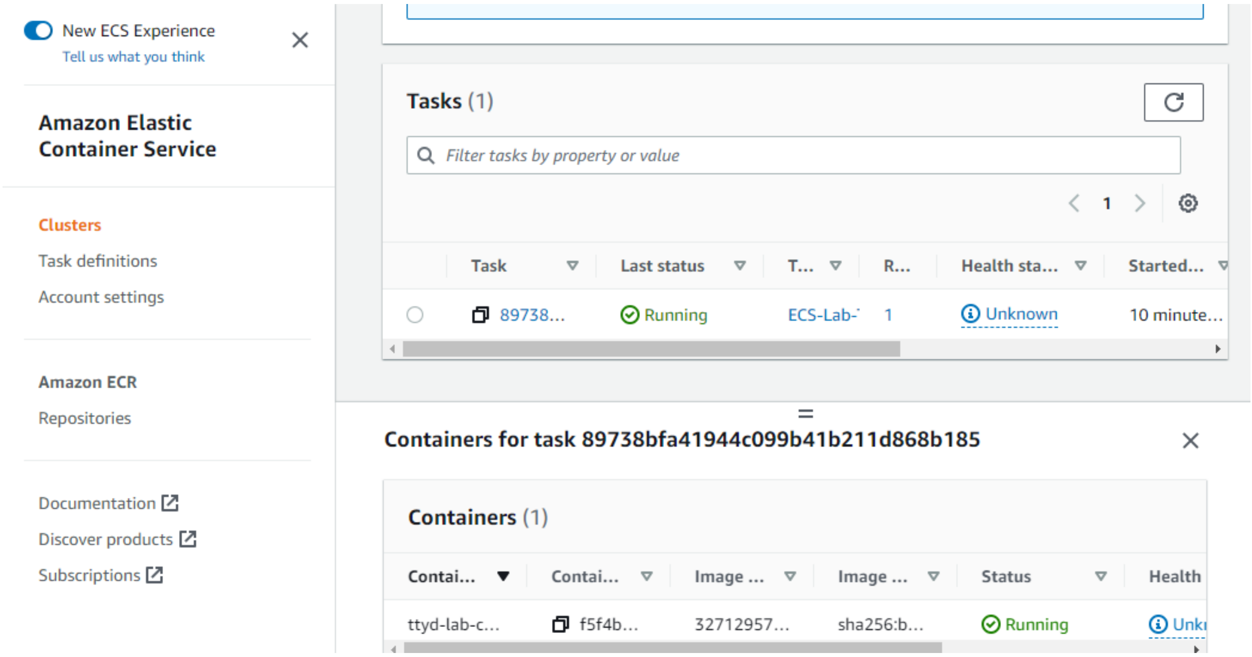
Task definition
ECS-Lab-Task-definition:1

Launch type
EC2

Service type
REPLICA

Created by
arn:aws:iam::763192382229:role/TheOracle

Load balancer



Tasks (1)

	Task	Last status	T...	R...	Health sta...	Started...
○	89738...	Running	ECS-Lab-`	1	Unknown	10 minute...

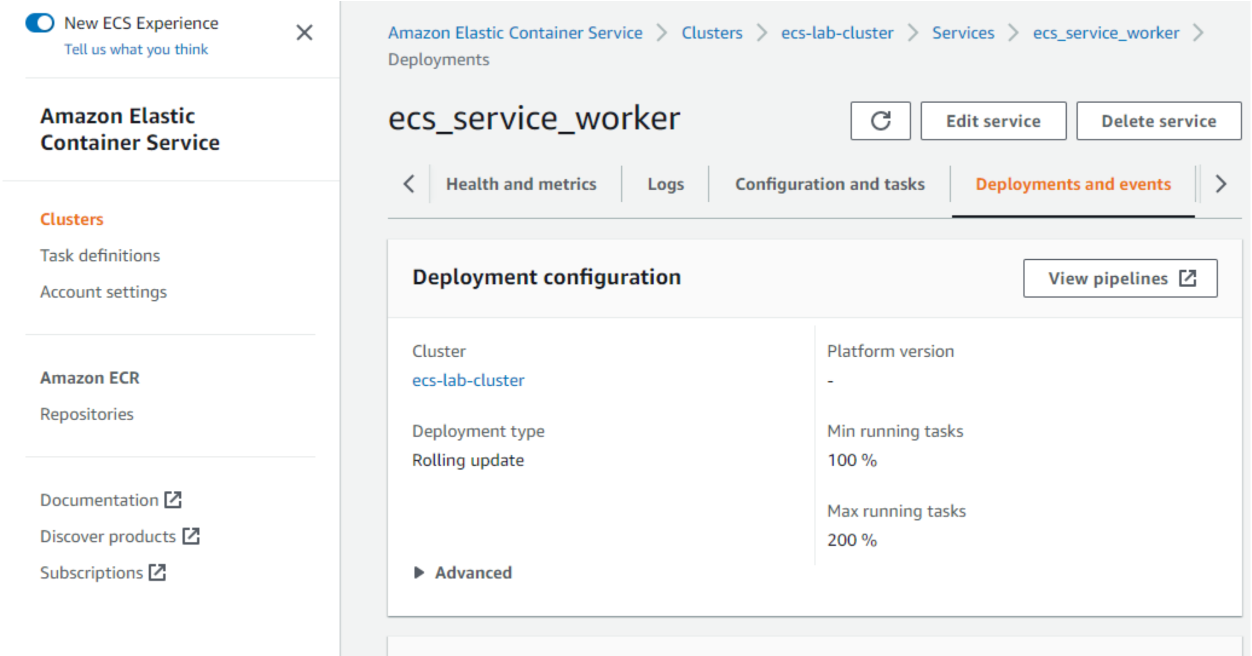
Containers for task 89738bfa41944c099b41b211d868b185

Containers (1)

Contai...	Contai...	Image ...	Image ...	Status	Health
ttyd-lab-c...	f5f4b...	32712957...	sha256:b...	Running	Unk

This page displays the configuration of the service. This includes the Task definition being used along with its revision, the status of the running task, the container instance identifier and the allocated CPU and Memory units. The containers bottom sheet displays the container name, status and other information regarding the running container.

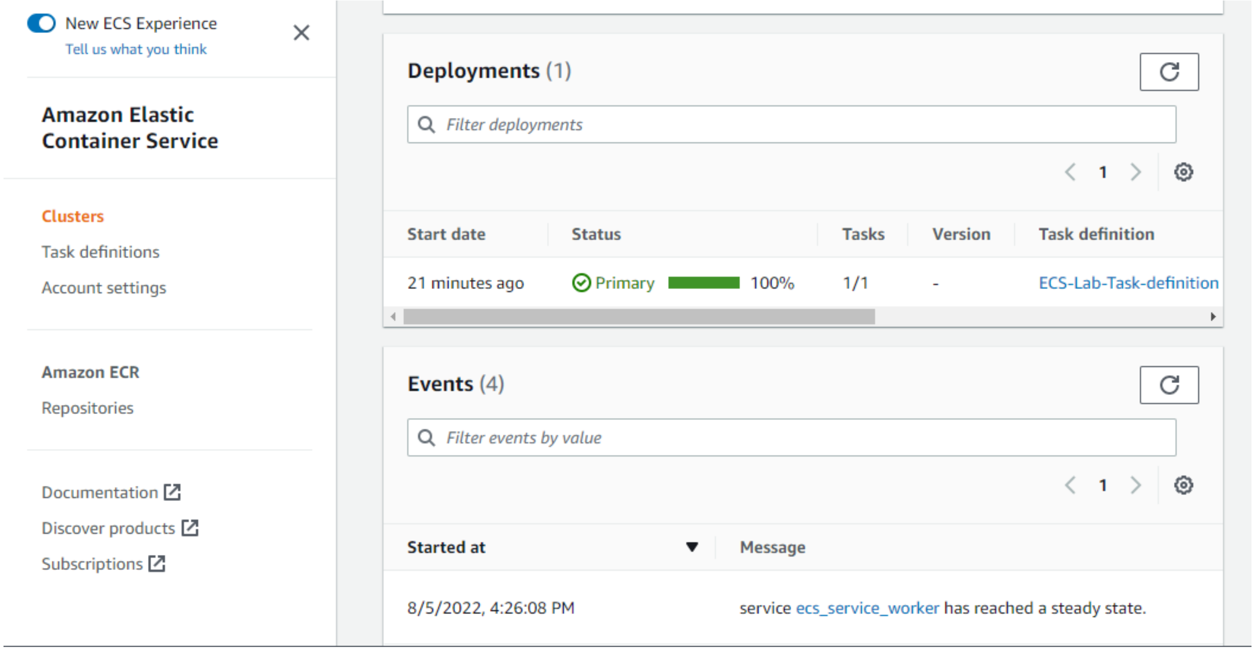
Step 5: Click on the Deployments and events tab. This tab displays the deployment configuration, the past deployments and their statuses. Along with the service event logs.



ecs_service_worker

Deployment configuration

Cluster ecs-lab-cluster	Platform version -
Deployment type Rolling update	Min running tasks 100 %
	Max running tasks 200 %



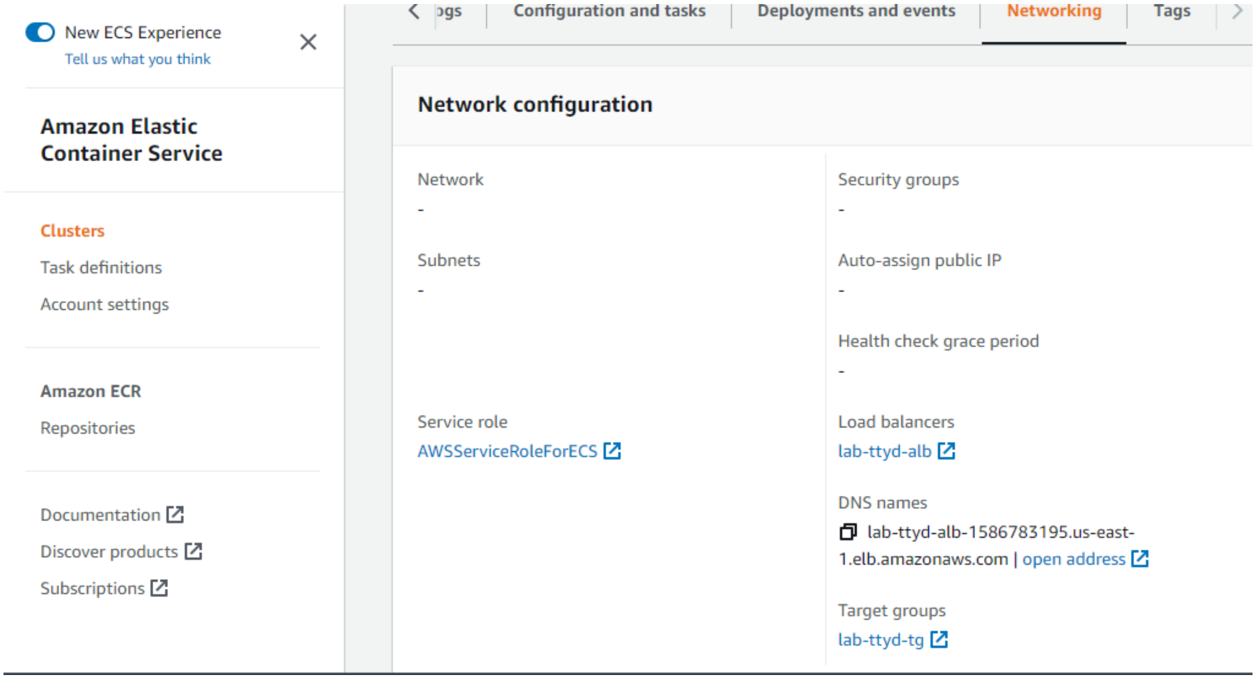
Deployments (1)

Start date	Status	Tasks	Version	Task definition
21 minutes ago	✓ Primary 100%	1/1	-	ECS-Lab-Task-definition

Events (4)

Started at	Message
8/5/2022, 4:26:08 PM	service ecs_service_worker has reached a steady state.

The next tab is **Networking**. It displays the network configuration along with the Load balancers associated with the cluster with its dns name, and the target groups for the load balancers.



Network configuration

Network
-

Subnets
-

Service role
AWSServiceRoleForECS

Security groups
-

Auto-assign public IP
-

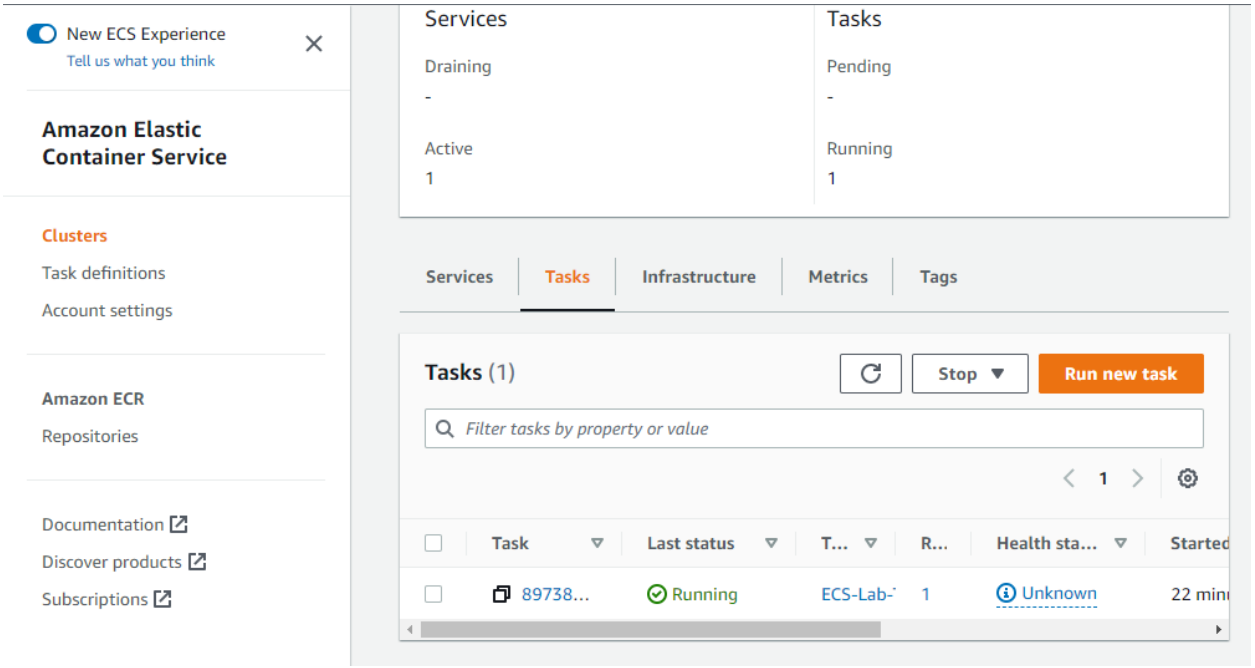
Health check grace period
-

Load balancers
lab-ttyd-alb

DNS names
lab-ttyd-alb-1586783195.us-east-1.elb.amazonaws.com | open address

Target groups
lab-ttyd-tg

Step 6: Go back to the **ecs-lab-cluster** page and navigate to the **Tasks tab.**



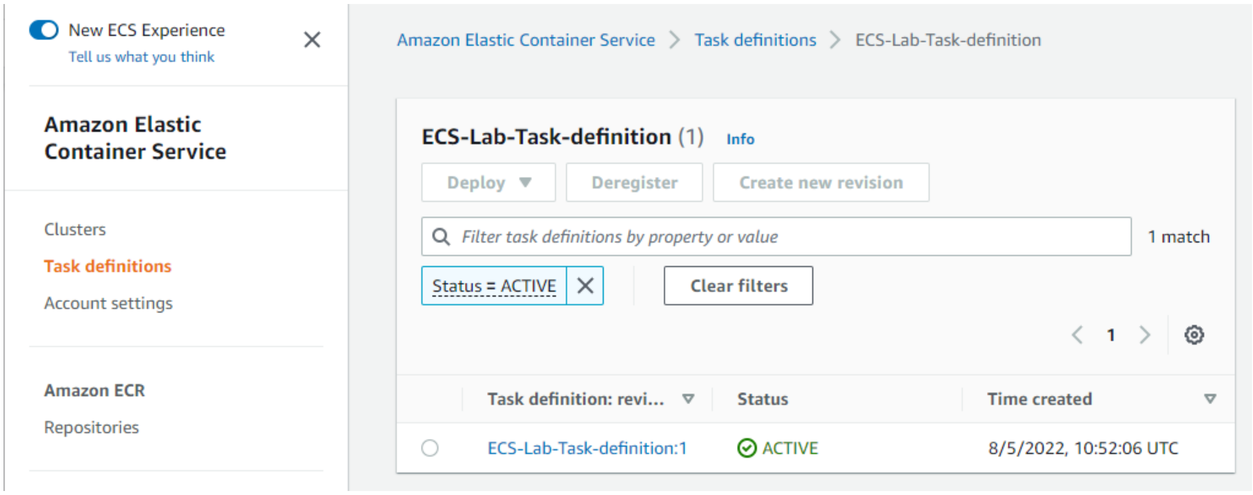
Services
Draining
-
Active
1

Tasks
Pending
-
Running
1

Tasks (1)

	Task	Last status	T...	R...	Health sta...	Started
□	89738...	Running	ECS-Lab-'	1	Unknown	22 min

This page also displays the tasks for this cluster. Click on the **ECS-Lab-Task-definition** option to view the task definition.



New ECS Experience
Tell us what you think

Amazon Elastic Container Service

Clusters
Task definitions
Account settings

Amazon ECR
Repositories

Amazon Elastic Container Service > Task definitions > ECS-Lab-Task-definition

ECS-Lab-Task-definition (1) Info

Deploy ▼ | Deregister | Create new revision

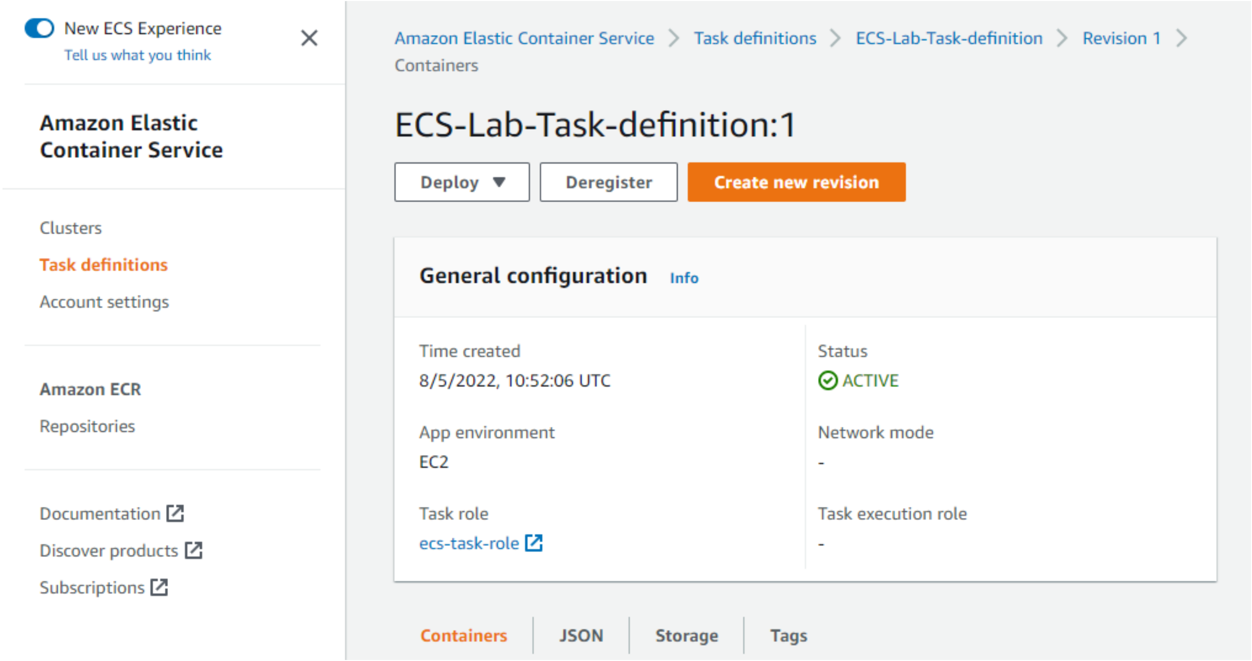
Filter task definitions by property or value — 1 match

Status = ACTIVE ✕ | Clear filters

< 1 >

	Task definition: revi...	Status	Time created
○	ECS-Lab-Task-definition:1	✓ ACTIVE	8/5/2022, 10:52:06 UTC

Next click on **ECS-Lab-Task-definition:1**



ECS-Lab-Task-definition:1

General configuration

Time created: 8/5/2022, 10:52:06 UTC

Status: ACTIVE

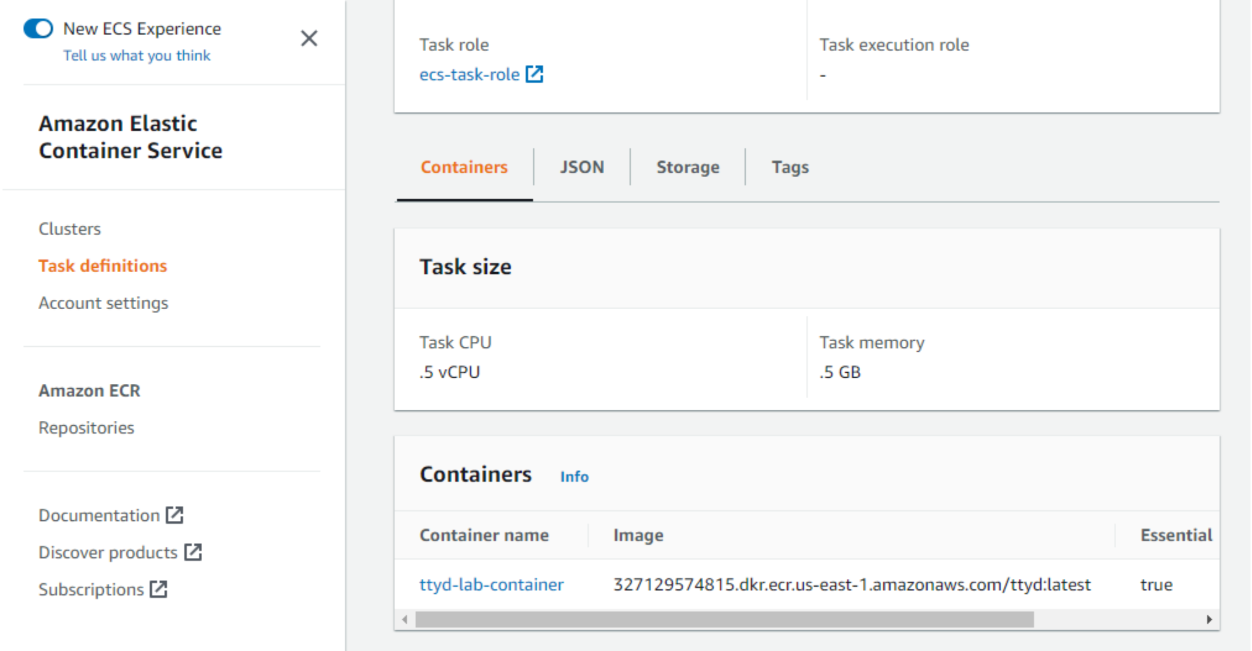
App environment: EC2

Network mode: -

Task role: ecs-task-role

Task execution role: -

The task definition is required to run docker containers in ECS. In the **Containers** tab you can see the container and the image that the container is running along with the CPU and Memory units being used.



Task role: ecs-task-role

Task execution role: -

Task size

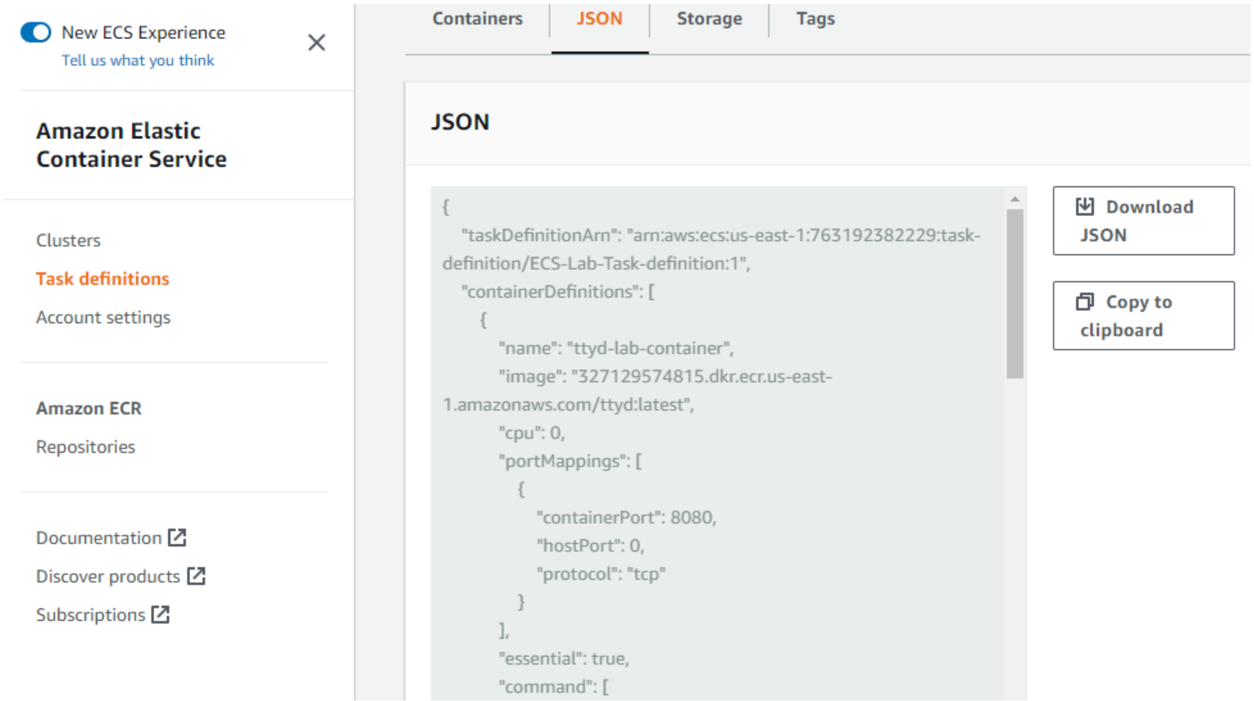
Task CPU: .5 vCPU

Task memory: .5 GB

Containers

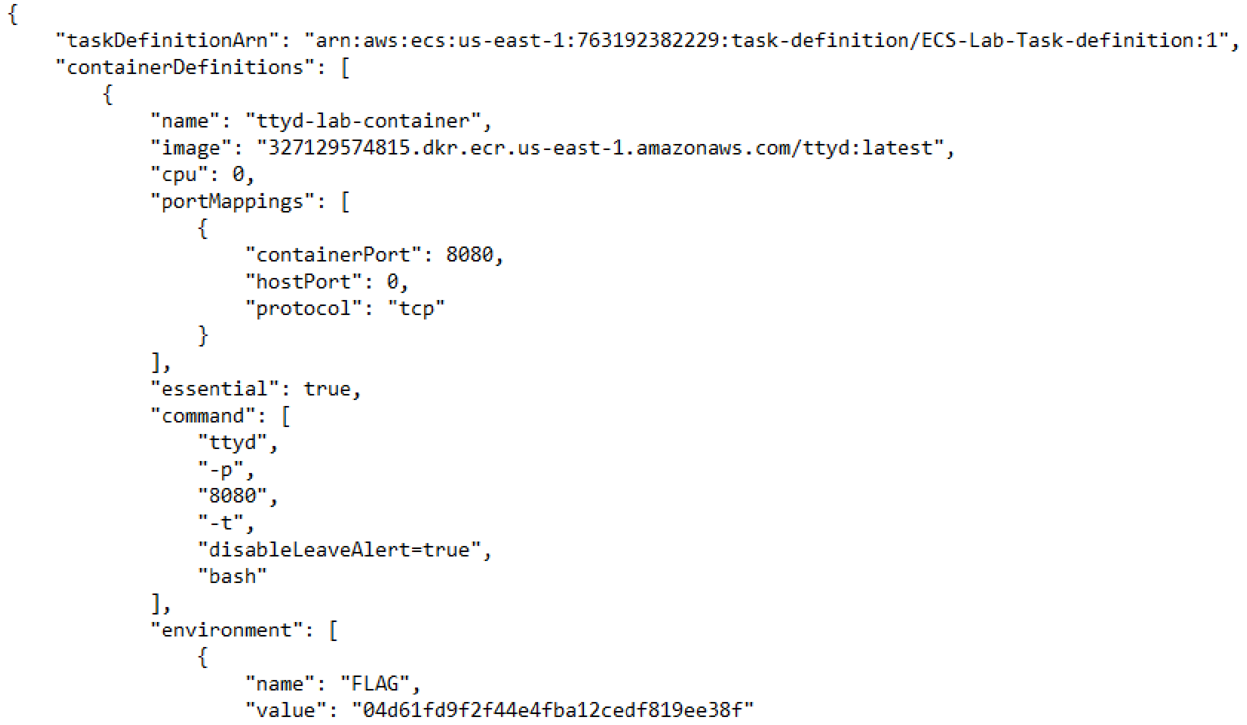
Container name	Image	Essential
ttyd-lab-container	327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest	true

The **JSON** tab contains the task definition json, this json has configuration information for the container that runs using this definition. It includes the container port mappings, linux capabilities, mount points, environment variables for the containers and lots of more information.



```
{
  "taskDefinitionArn": "arn:aws:ecs:us-east-1:763192382229:task-definition/ECS-Lab-Task-definition:1",
  "containerDefinitions": [
    {
      "name": "ttyd-lab-container",
      "image": "327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest",
      "cpu": 0,
      "portMappings": [
        {
          "containerPort": 8080,
          "hostPort": 0,
          "protocol": "tcp"
        }
      ],
      "essential": true,
      "command": [
```

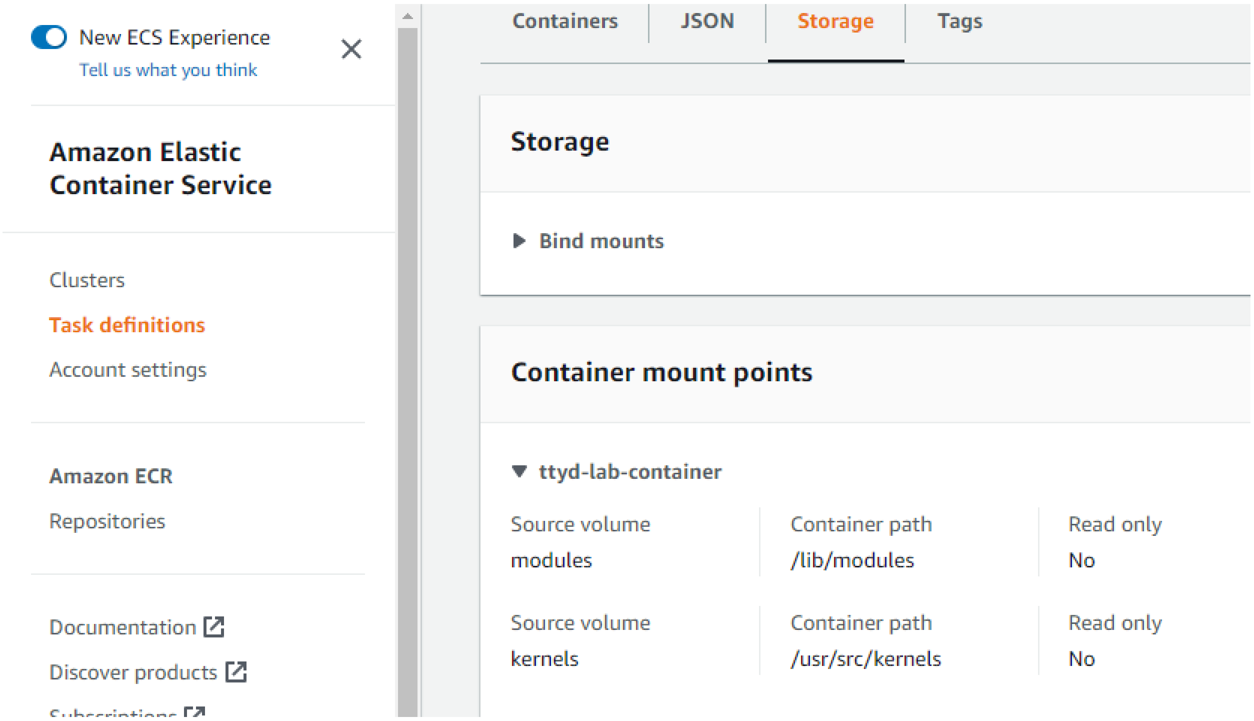
Click on the **Download JSON** button to download the json to view it.



```
{
    "taskDefinitionArn": "arn:aws:ecs:us-east-1:763192382229:task-definition/ECS-Lab-Task-definition:1",
    "containerDefinitions": [
        {
            "name": "ttyd-lab-container",
            "image": "327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest",
            "cpu": 0,
            "portMappings": [
                {
                    "containerPort": 8080,
                    "hostPort": 0,
                    "protocol": "tcp"
                }
            ],
            "essential": true,
            "command": [
                "ttyd",
                "-p",
                "8080",
                "-t",
                "disableLeaveAlert=true",
                "bash"
            ],
            "environment": [
                {
                    "name": "FLAG",
                    "value": "04d61fd9f2f44e4fba12cedf819ee38f"
```

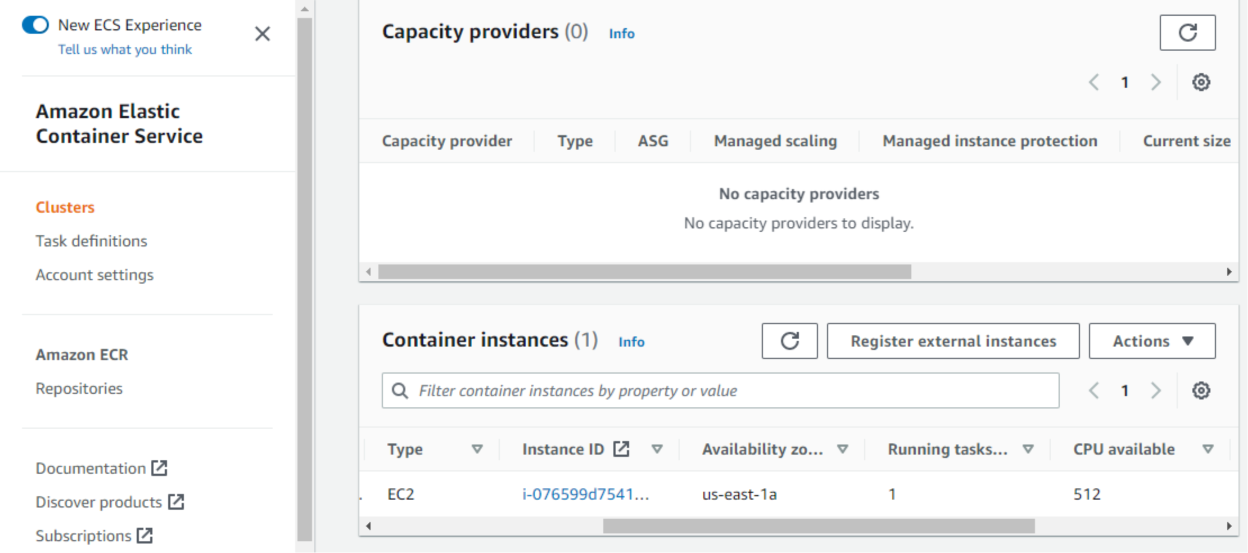
The task definition contains lots of configuration information it also has environment variables that may contain sensitive information being passed down to the container. Here we have found the flag.

The **Storage** tab lists the mounts on the container, this container has two bind mounts names modules and kernels.



Source volume	Container path	Read only
modules	/lib/modules	No
kernels	/usr/src/kernels	No

Step 8: Navigate back to **ecs-lab-cluster** and then the **Infrastructure** tab.



Capacity providers (0)

Capacity provider	Type	ASG	Managed scaling	Managed instance protection	Current size

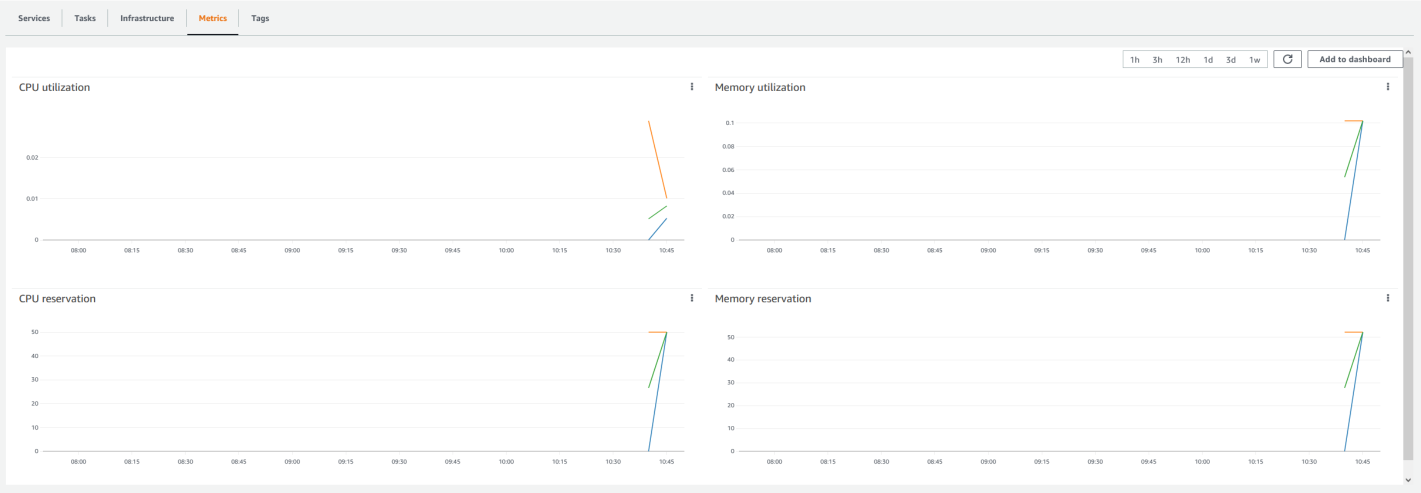
No capacity providers

No capacity providers to display.

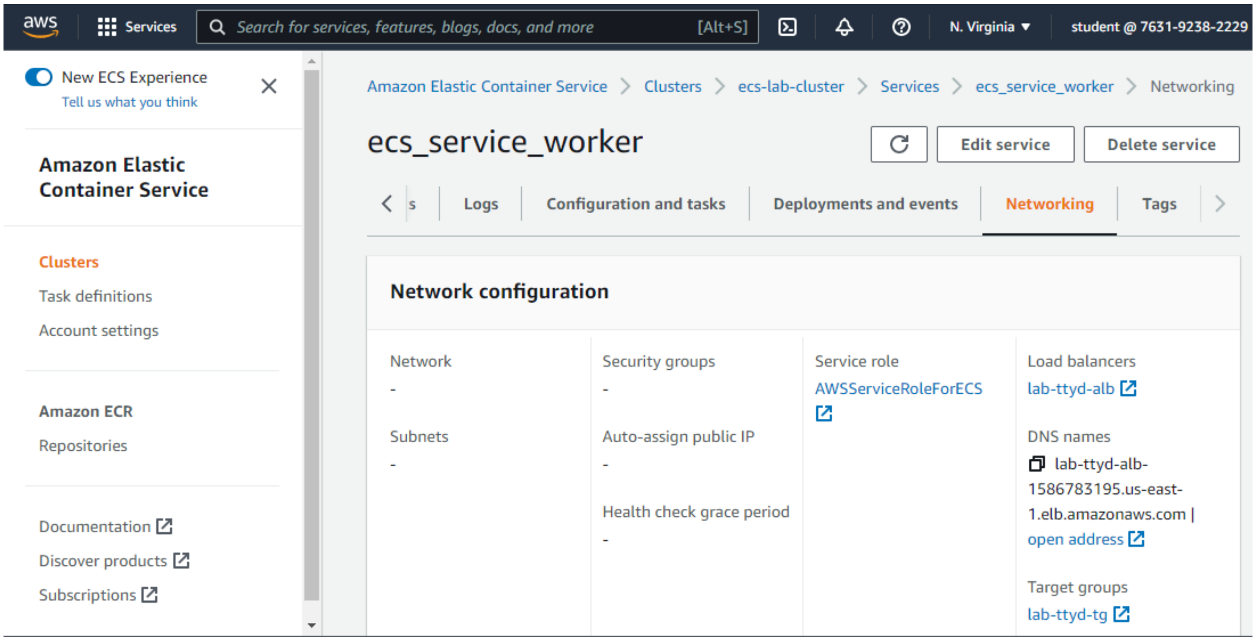
Container instances (1)

Type	Instance ID	Availability zo...	Running tasks...	CPU available
EC2	i-076599d7541...	us-east-1a	1	512

This lists the EC2 instances which are associated with the cluster and the Cpu and memory available on the instance. In the **Metrics** tab you can see the graphs depicting the cluster CPU and Memory utilization and reservations.



Step 9: From the **ecs-service-worker**'s **Networking** tab click on **lab-ttyd-alb** load balancer.



ecs_service_worker

Network configuration

Network
-

Subnets
-

Security groups
-

Auto-assign public IP
-

Health check grace period
-

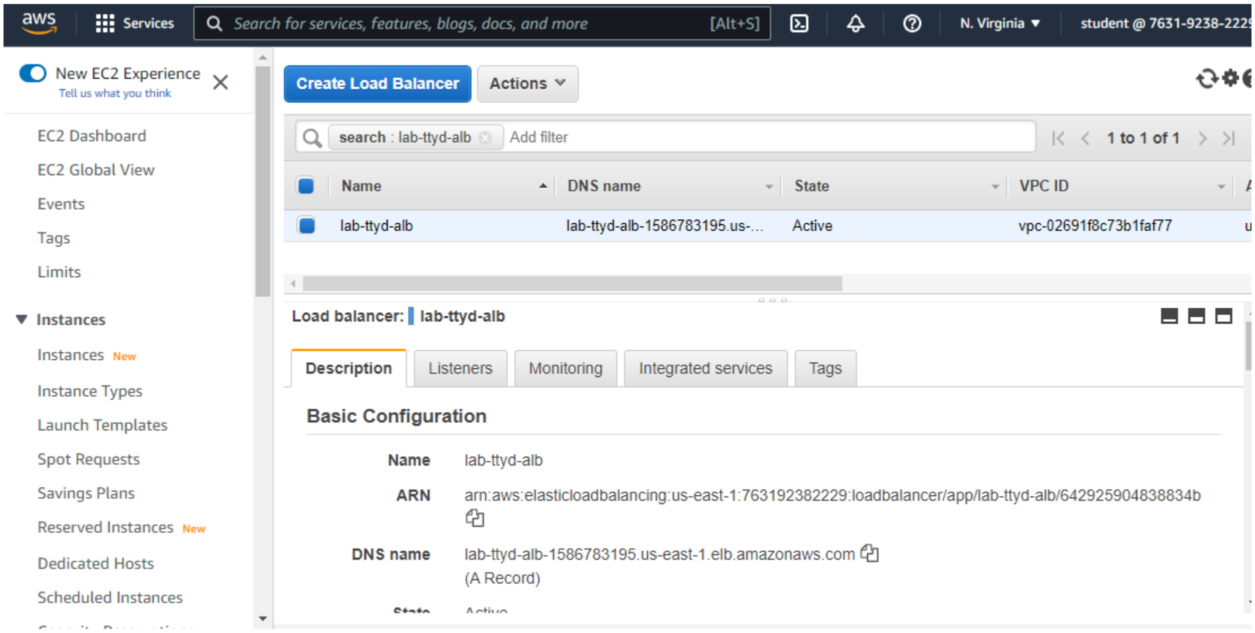
Service role
AWSServiceRoleForECS

Load balancers
lab-ttyd-alb

DNS names
lab-ttyd-alb-1586783195.us-east-1.elb.amazonaws.com | open address

Target groups
lab-ttyd-tg

This brings you to the load balancers page, the bottom sheet's **Description** tab shows the configuration for the load balancer. This here is an internet-facing application load balancer.



Name	DNS name	State	VPC ID
lab-ttyd-alb	lab-ttyd-alb-1586783195.us-...	Active	vpc-02691f8c73b1faf77

Load balancer: lab-ttyd-alb

Basic Configuration

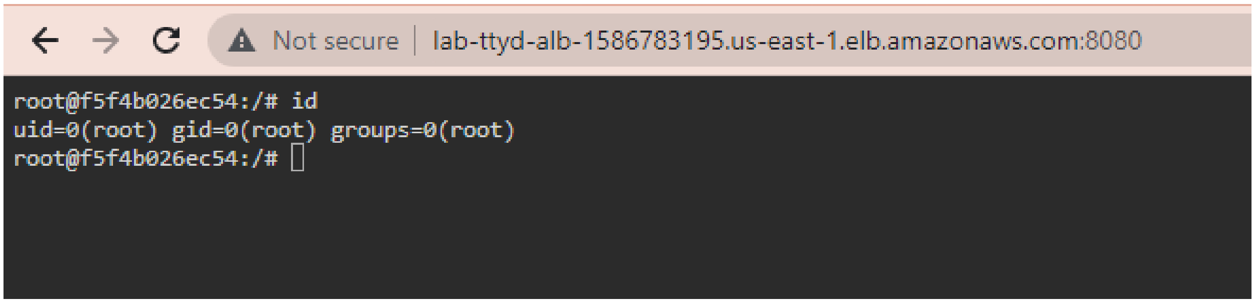
Name lab-ttyd-alb

ARN arn:aws:elasticloadbalancing:us-east-1:763192382229:loadbalancer/app/lab-ttyd-alb/642925904838834b

DNS name lab-ttyd-alb-1586783195.us-east-1.elb.amazonaws.com (A Record)

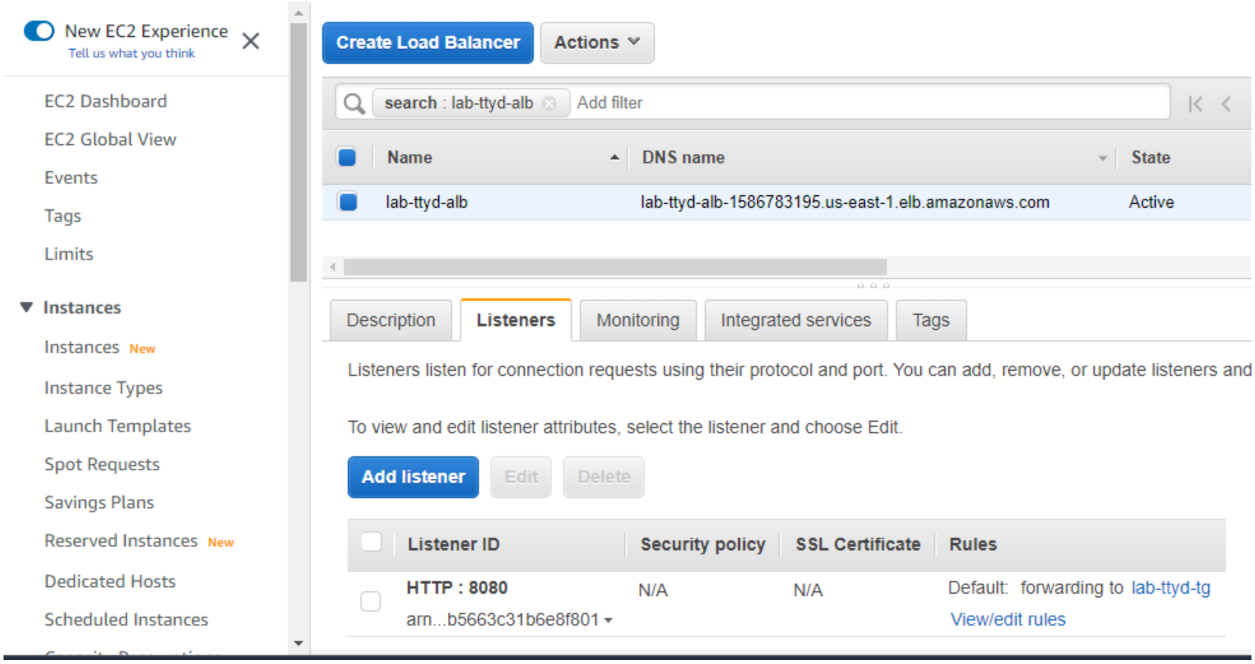
State Active

You can copy the DNS name, append "**:8080**" to it and paste in a new tab.



```
root@f5f4b026ec54:/# id
uid=0(root) gid=0(root) groups=0(root)
root@f5f4b026ec54:/# 
```

This brings you inside the container running on the EC2 instance, orchestrated by ECS. Next you can move to the **Listeners** tab, here you can see the listeners associated with the load balancers. The listener is listening for HTTP traffic on port 8080 and forwarding it to the **lab-ttyd-tg** target group.



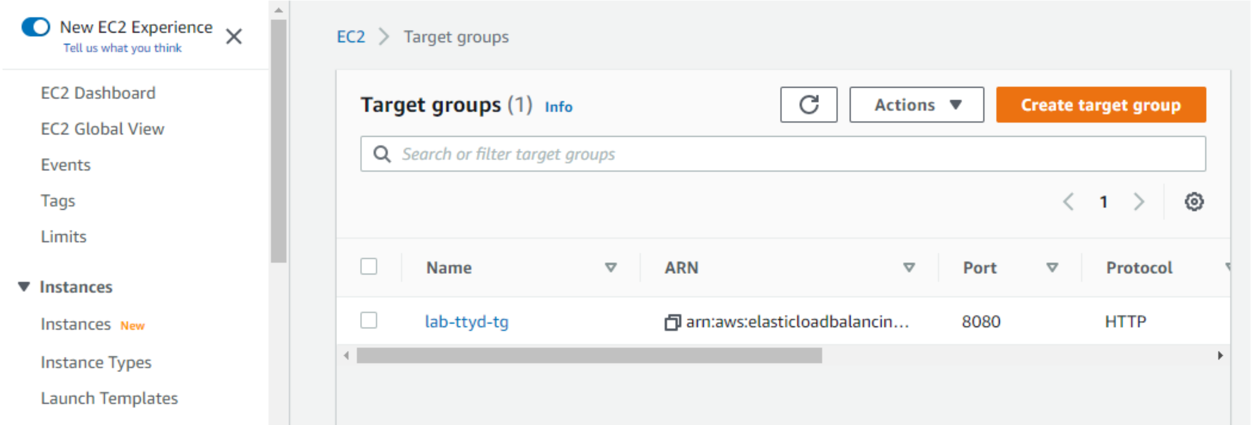
Name	DNS name	State
lab-ttyd-alb	lab-ttyd-alb-1586783195.us-east-1.elb.amazonaws.com	Active

Listeners listen for connection requests using their protocol and port. You can add, remove, or update listeners and

To view and edit listener attributes, select the listener and choose Edit.

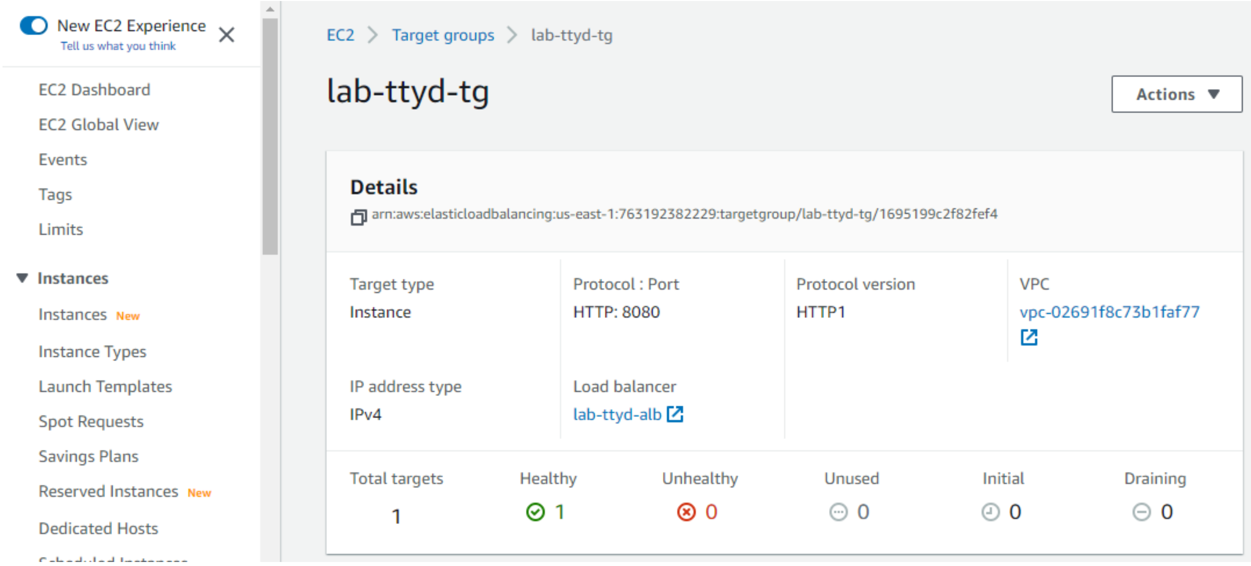
Listener ID	Security policy	SSL Certificate	Rules
HTTP : 8080 arn...b5663c31b6e8f801	N/A	N/A	Default: forwarding to lab-ttyd-tg View/edit rules

Step 10: Click on **lab-ttyd-tg.**



Target groups (1) Info

Name	ARN	Port	Protocol
lab-ttyd-tg	arn:aws:elasticloadbalancin...	8080	HTTP



lab-ttyd-tg

Details

arn:aws:elasticloadbalancing:us-east-1:763192382229:targetgroup/lab-ttyd-tg/1695199c2f82fef4

Target type: Instance

Protocol : Port: HTTP: 8080

Protocol version: HTTP1

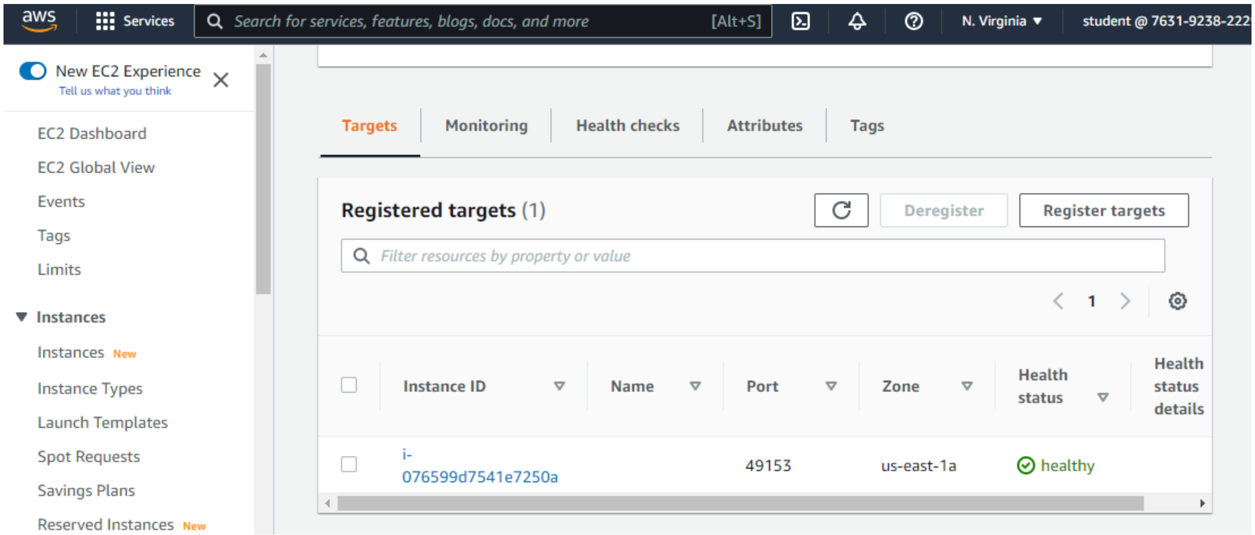
VPC: vpc-02691f8c73b1faf77

IP address type: IPv4

Load balancer: lab-ttyd-alb

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
1	1	0	0	0	0

This shows the target group which consists of the instances part of the ECS cluster. The **Details** tab on the bottom sheet has an overview of the Target group status. A Healthy status indicates instances that are properly configured and working with the target group.

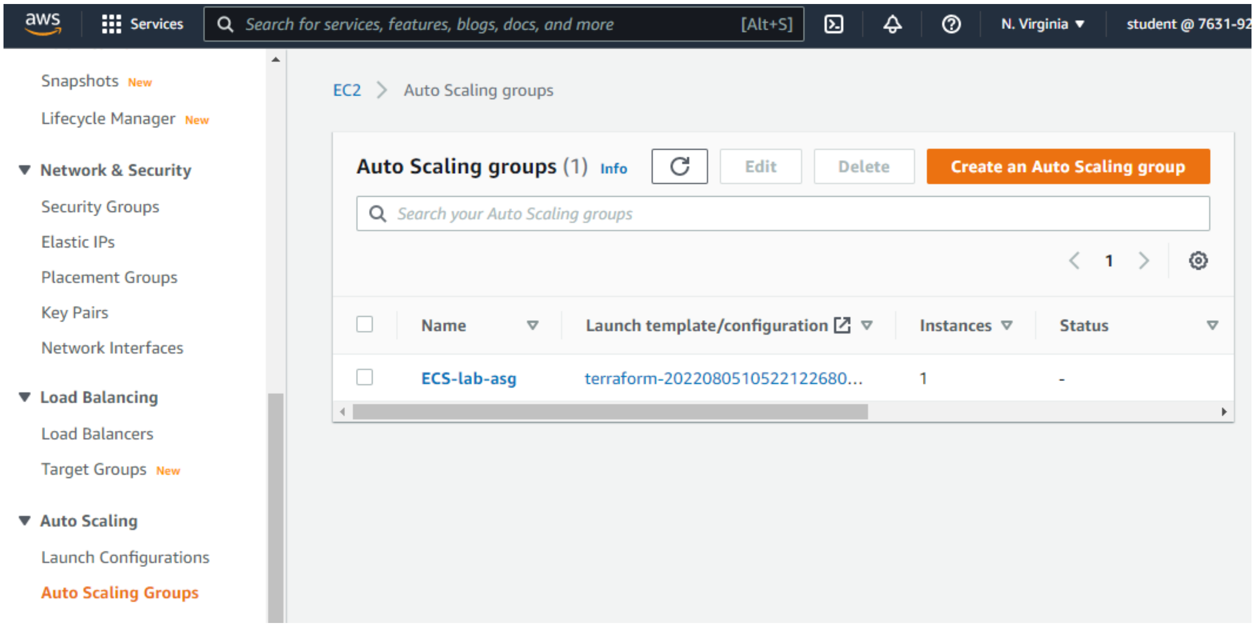


Registered targets (1)

□	Instance ID	Name	Port	Zone	Health status	Health status details
□	i-076599d7541e7250a		49153	us-east-1a	✓ healthy	

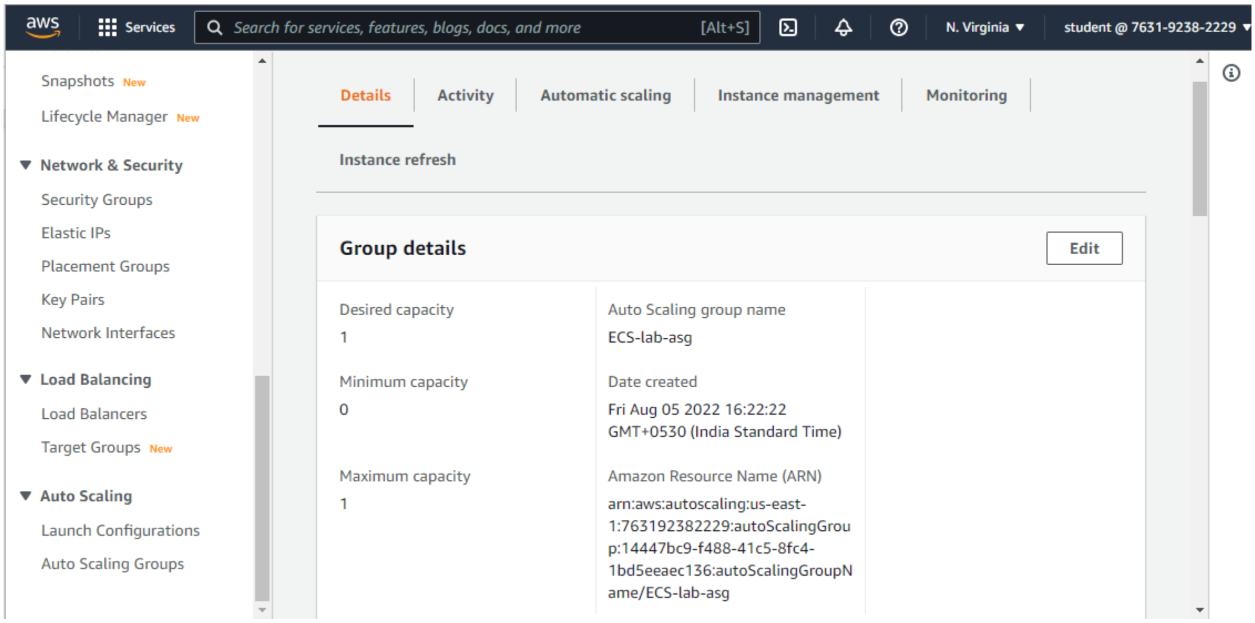
The **Targets** tab shows the registered instances which are working with the ECS cluster.

Step 11: ECS relies on Auto Scaling Groups to maintain the number of desired instances in the cluster. From the bottom of the side panel click on the **Auto Scaling Groups** option.



□	Name	Launch template/configuration	Instances	Status
□	ECS-lab-asg	terraform-2022080510522122680...	1	-

Click on **ECS-lab-asg.**



Group details

Desired capacity
1

Minimum capacity
0

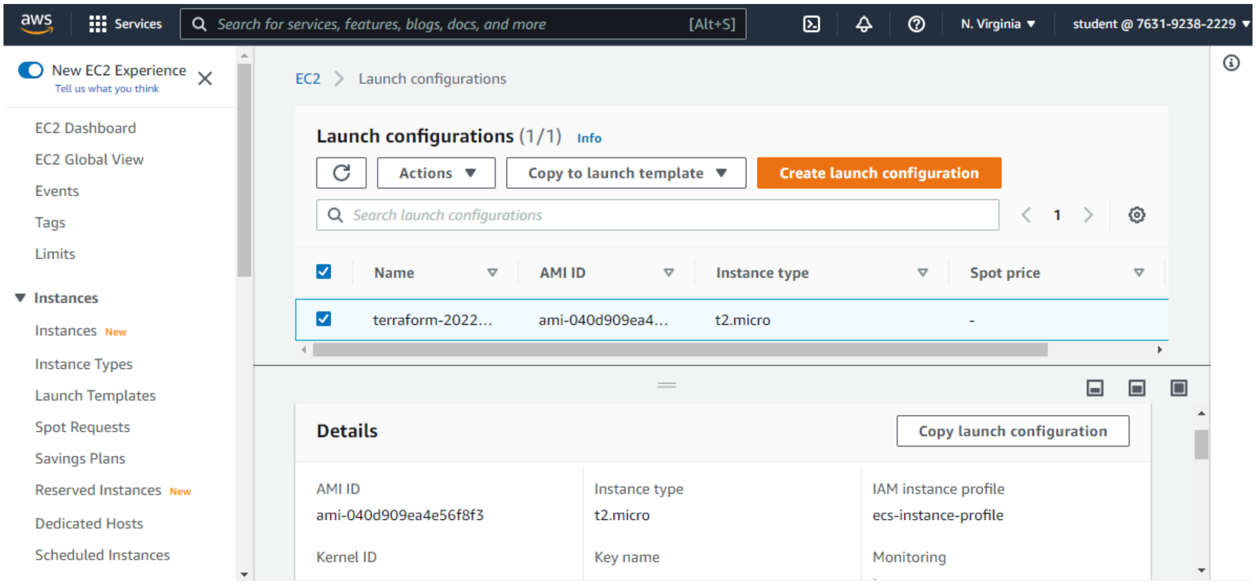
Maximum capacity
1

Auto Scaling group name
ECS-lab-asg

Date created
Fri Aug 05 2022 16:22:22 GMT+0530 (India Standard Time)

Amazon Resource Name (ARN)
arn:aws:autoscaling:us-east-1:763192382229:autoScalingGroup:14447bc9-f488-41c5-8fc4-1bd5eeaec136:autoScalingGroupName/ECS-lab-asg

The **Group details** section displays the desired, minimum and maximum capacity of instances to be running. The **Launch configuration** section contains the details about the launch configuration of the instances of the Auto scaling group. To view the launch configuration in detail, click on the **View details in the launch configuration console** link.

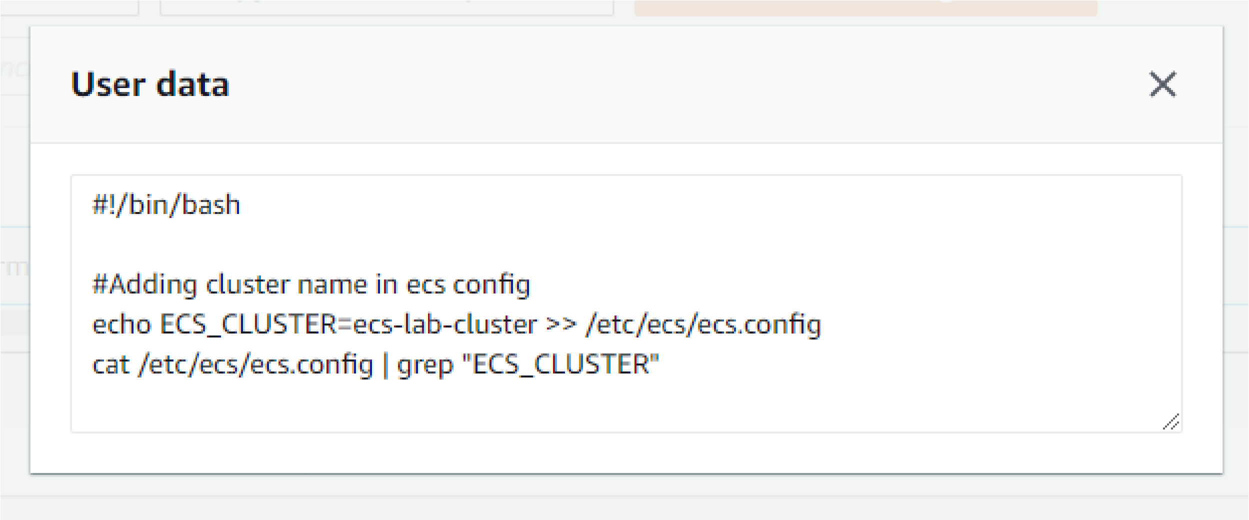


☑	Name	AMI ID	Instance type	Spot price
☑	terraform-2022...	ami-040d909ea4...	t2.micro	-

Details

AMI ID: ami-040d909ea4e56f8f3
Instance type: t2.micro
IAM instance profile: ecs-instance-profile
Kernel ID
Key name
Monitoring

This displays the instance type, instance profile, security group and other configurations that the new instances need. It also contains user data to be run on the instance, we can view it by clicking on the **View user data** link.


User data

```
#!/bin/bash

#Adding cluster name in ecs config
echo ECS_CLUSTER=ecs-lab-cluster >> /etc/ecs/ecs.config
cat /etc/ecs/ecs.config | grep "ECS_CLUSTER"
```

The user data file adds a line into the ecs.config file, this aids the ecs agent to attach the instance to the cluster.

References:

1. AWS ECS Documentation (https://aws.amazon.com/ecs/)