

[illegible]

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**.

The screenshot shows the AWS Management Console for Amazon Elastic Container Service (ECS). On the left, there is a sidebar with navigation links: 'New ECS Experience' (with a toggle and feedback link), 'Amazon Elastic Container Service' (with sub-links for 'Clusters', 'Task definitions', and 'Account settings'), 'Amazon ECR' (with 'Repositories'), and 'Documentation', 'Discover products', and 'Subscriptions' (each with an external link icon). The main content area is titled 'Amazon Elastic Container Service > Clusters' and 'All Clusters Info'. It features a 'Clusters (1)' section with a refresh button and a 'Create cluster' button. Below this is a search bar labeled 'Search clusters'. A pagination control shows '< 1 >' and a settings gear. The main cluster, 'ecs-lab-cluster', is listed with a link to 'No default found'. Below the cluster name, it shows 'Services' (1) and 'Tasks' (0 Pending | 1 Running). A green progress bar is visible at the bottom of the cluster details.

☒ New ECS Experience
[Tell us what you think](#)

Amazon Elastic Container Service

Clusters

[Task definitions](#)

[Account settings](#)

Amazon ECR

[Repositories](#)

[Documentation](#)

[Discover products](#)

[Subscriptions](#)

Services

Draining

-

Active

1

Tasks

Pending

-

Running

1

Services

Tasks

Infrastructure

Metrics

Tags

Services (1)



Edit

Delete service

Deploy

Filter services by value

< 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.

New ECS Experience Tell us what you think

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation

Discover products

Subscriptions

Amazon Elastic Container Service > Clusters > ecs-lab-cluster > Services > ecs_service_worker > Health

ecs_service_worker

Health and metrics | Logs | Configuration and tasks | Deployments and events

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.

New ECS Experience Tell us what you think

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation

Discover products

Subscriptions

Amazon Elastic Container Service > Clusters > ecs-lab-cluster > Services > ecs_service_worker > Configuration

ecs_service_worker

Health and metrics | Logs | Configuration and tasks | Deployments and events

Service configuration

Service ARN	ecs-lab-cluster/ecs_service_worker
Task definition	ECS-Lab-Task-definition:1
Service type	REPLICA
Launch type	EC2
Created by	arn:aws:iam::763192382229:role/TheOracle
▼ Load balancer	

The screenshot displays the Amazon ECS console interface. On the left, the navigation menu includes 'Amazon Elastic Container Service', 'Clusters', 'Task definitions', 'Account settings', 'Amazon ECR', 'Repositories', 'Documentation', 'Discover products', and 'Subscriptions'. The main content area shows the 'Tasks (1)' section with a search bar and a table of tasks. Below this, a modal window titled 'Containers for task 89738bfa41944c099b41b211d868b185' is open, displaying a table of containers for the selected task.

Tasks (1)

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

Containers for task 89738bfa41944c099b41b211d868b185

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.

The screenshot displays the Amazon ECS console interface. On the left is a navigation sidebar with sections for 'Amazon Elastic Container Service' (containing Clusters, Task definitions, and Account settings), 'Amazon ECR' (containing Repositories), and links for Documentation, Discover products, and Subscriptions. The main content area shows the breadcrumb path: Amazon Elastic Container Service > Clusters > ecs-lab-cluster > Services > ecs_service_worker > Deployments. The service name 'ecs_service_worker' is at the top with buttons for 'Edit service' and 'Delete service'. Below this are tabs for 'Health and metrics', 'Logs', 'Configuration and tasks', and 'Deployments and events' (which is selected). The 'Deployment configuration' section shows details for the 'ecs-lab-cluster', including 'Platform version' as '-', 'Min running tasks' as '100 %', and 'Max running tasks' as '200 %'. Below this is an 'Advanced' section. The 'Deployments (1)' section shows a single deployment with a search filter 'Filter deployments'. The deployment table has columns: Start date, Status, Tasks, Version, and Task definition. The first row shows a deployment from '21 minutes ago' with a 'Primary' status (green checkmark), '100%' completion, '1/1' tasks, version '-', and task definition 'ECS-Lab-Task-definition'. Below the deployments is the 'Events (4)' section with a search filter 'Filter events by value'. The events table has columns: Started at and Message. The first event shows the date '8/5/2022, 4:26:08 PM' and the message 'service ecs_service_worker has reached a steady state.'

Amazon Elastic Container Service > Clusters > ecs-lab-cluster > Services > ecs_service_worker > Deployments

ecs_service_worker

Health and metrics | Logs | Configuration and tasks | **Deployments and events**

Deployment configuration

View pipelines

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

► Advanced

Deployments (1)

Filter deployments

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

ECS-Lab-Task-definition

Events (4)

Filter events by value

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.

New ECS Experience
Tell us what you think

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation

Discover products

Subscriptions

pgs Configuration and tasks Deployments and events **Networking** Tags

Network configuration

Network	-	Security groups	-
Subnets	-	Auto-assign public IP	-
Service role	AWSServiceRoleForECS	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.

New ECS Experience
Tell us what you think

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation

Discover products

Subscriptions

Services **Tasks** Infrastructure Metrics Tags

Tasks (1)

Filter tasks by property or value

	Task	Last status	T...	R...	Health sta...	Started
<input type="checkbox"/>	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.

The screenshot shows the Amazon ECS console interface. On the left is a navigation sidebar with the following items: 'New ECS Experience' (with a feedback link), 'Amazon Elastic Container Service', 'Clusters', 'Task definitions' (highlighted in orange), 'Account settings', 'Amazon ECR', and 'Repositories'. The main content area shows the breadcrumb 'Amazon Elastic Container Service > Task definitions > ECS-Lab-Task-definition'. Below this, the title 'ECS-Lab-Task-definition (1)' is followed by an 'Info' link. There are three buttons: 'Deploy' (with a dropdown arrow), 'Deregister', and 'Create new revision'. A search bar contains the text 'Filter task definitions by property or value' and shows '1 match'. Below the search bar, a filter 'Status = ACTIVE' is applied, with a 'Clear filters' button. A table lists the task definitions with columns 'Task definition: revi...', 'Status', and 'Time created'. The table contains one entry: 'ECS-Lab-Task-definition:1' with status 'ACTIVE' and creation time '8/5/2022, 10:52:06 UTC'.

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**

☒ New ECS Experience
Tell us what you think

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation [↗](#)

Discover products [↗](#)

Subscriptions [↗](#)

Amazon Elastic Container Service > Task definitions > ECS-Lab-Task-definition > Revision 1 > Containers

ECS-Lab-Task-definition:1

Deploy ▼

Deregister

Create new revision

General configuration [Info](#)

Time created

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

Status

🟢 ACTIVE

App environment

EC2

Network mode

-

Task role

[ecs-task-role](#) [↗](#)

Task execution role

-

Containers

JSON

Storage

Tags

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.

☒ New ECS Experience
Tell us what you think

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation [↗](#)

Discover products [↗](#)

Subscriptions [↗](#)

Task role

[ecs-task-role](#) [↗](#)

Task execution role

-

Containers

JSON

Storage

Tags

Task size

Task CPU

.5 vCPU

Task memory

.5 GB

Containers [Info](#)

Container name

Image

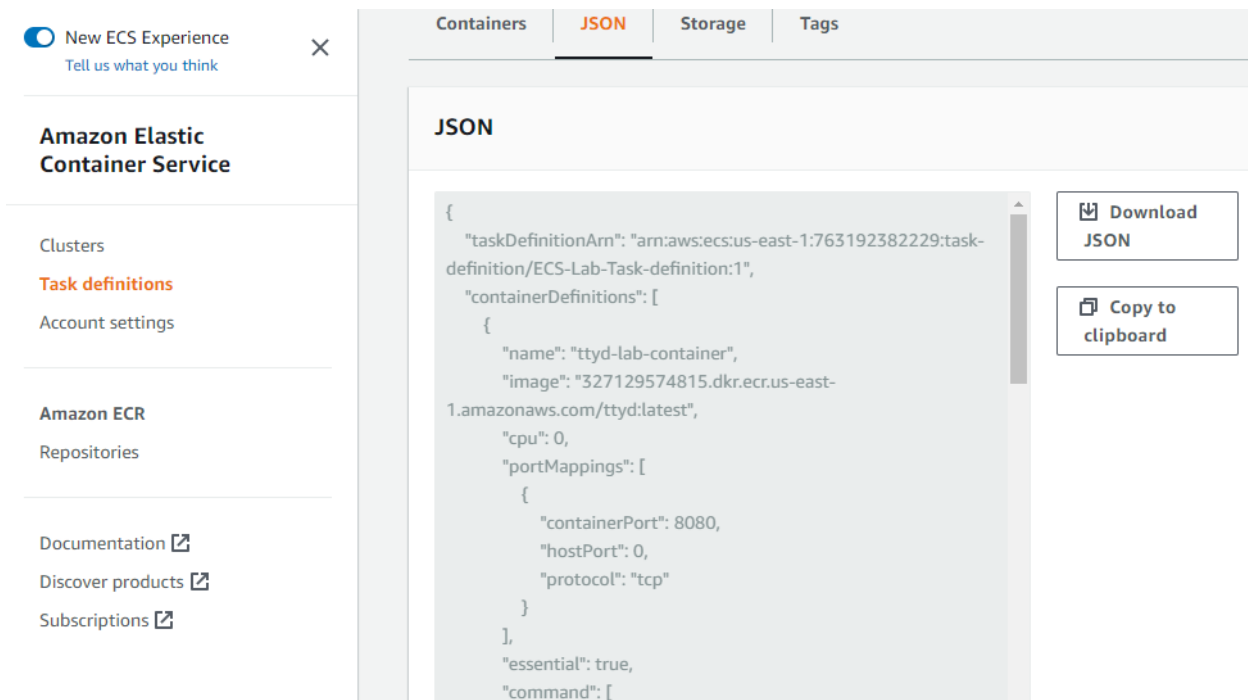
Essential

[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.



The screenshot shows the Amazon Elastic Container Service (ECS) console. On the left is a navigation sidebar with links for Clusters, Task definitions (highlighted), Account settings, Amazon ECR, Repositories, Documentation, Discover products, and Subscriptions. The main panel has tabs for Containers, JSON (selected), Storage, and Tags. The JSON tab displays a task definition in JSON format. To the right of the JSON editor are two buttons: 'Download JSON' and 'Copy to clipboard'.

```
{
  "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.

☒ New ECS Experience
Tell us what you think

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation [↗](#)

Discover products [↗](#)

Subscriptions [↗](#)

Containers

JSON

Storage

Tags

Storage

► Bind mounts

Container mount points

▼ ttyd-lab-container

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

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

New ECS Experience

Tell us what you think

×

Amazon Elastic Container Service

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Documentation

Discover products

Subscriptions

Capacity providers (0) Info

< 1 >

⚙️

Capacity provider	Type	ASG	Managed scaling	Managed instance protection	Current size
No capacity providers					
No capacity providers to display.					

Container instances (1) Info

↻

Register external instances

Actions ▾

🔍

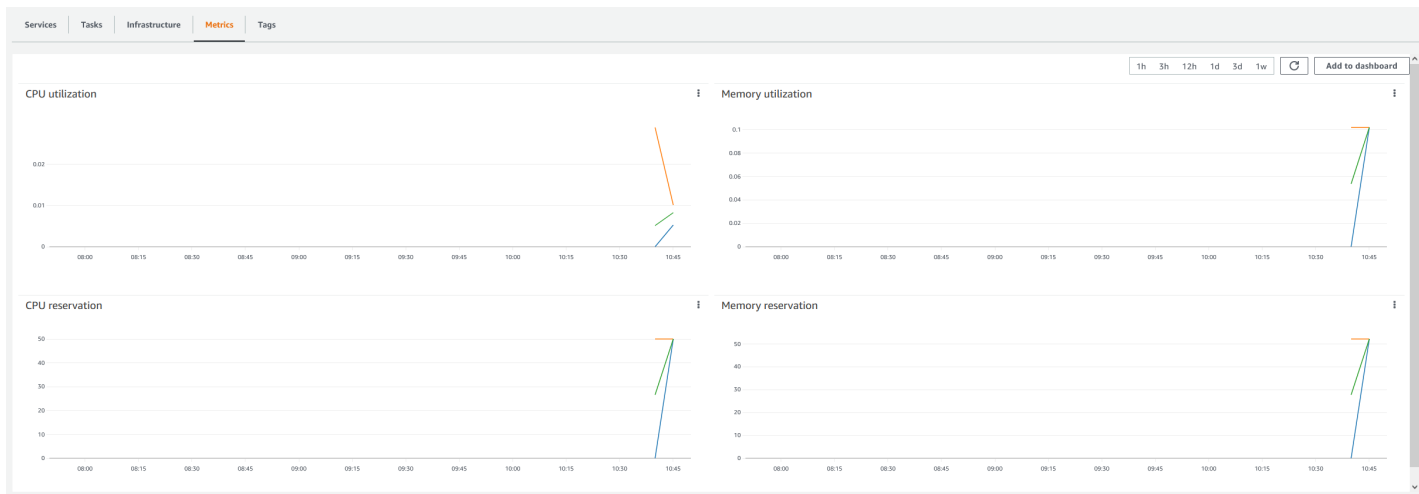
Filter container instances by property or value

< 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.

The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with options like 'New ECS Experience', 'Amazon Elastic Container Service', 'Clusters', 'Task definitions', 'Account settings', 'Amazon ECR', 'Repositories', 'Documentation', 'Discover products', and 'Subscriptions'. The main content area is titled 'Amazon Elastic Container Service > Clusters > ecs-lab-cluster > Services > ecs_service_worker > Networking'. Below this, there's a breadcrumb trail and buttons for 'Edit service' and 'Delete service'. The 'Networking' tab is selected, showing a 'Network configuration' section with a table of settings:

Network	Security groups	Service role	Load balancers
-	-	AWSServiceRoleForECS	lab-ttyd-alb
Subnets	Auto-assign public IP	Health check grace period	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.

The screenshot shows the AWS Management Console interface for the 'lab-ttyd-alb' load balancer. The left sidebar shows navigation options like 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', and 'Scheduled Instances'. The main content area is titled 'Create Load Balancer' and 'Actions'. Below this is a search bar and a table of load balancers:

Name	DNS name	State	VPC ID
lab-ttyd-alb	lab-ttyd-alb-1586783195.us-east-1.elb.amazonaws.com	Active	vpc-02691f8c73b1faf77

Below the table, the 'Load balancer: lab-ttyd-alb' section is shown with tabs for 'Description', 'Listeners', 'Monitoring', 'Integrated services', and 'Tags'. The 'Description' tab is selected, showing a 'Basic Configuration' section with the following details:

- 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.


```
← → ↻ ⚠ Not secure | lab-ttyd-alb-1586783195.us-east-1.elb.amazonaws.com:8080

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.

New EC2 Experience

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

▼ Instances

Instances New

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances New

Dedicated Hosts

Scheduled Instances

Create Load Balancer

Actions

search : lab-ttyd-alb

Add filter

K <

<input type="checkbox"/>	Name	DNS name	State
<input checked="" type="checkbox"/>	lab-ttyd-alb	lab-ttyd-alb-1586783195.us-east-1.elb.amazonaws.com	Active

Description

Listeners

Monitoring

Integrated services

Tags

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.

Add listener

Edit

Delete

<input type="checkbox"/>	Listener ID	Security policy	SSL Certificate	Rules
<input type="checkbox"/>	HTTP : 8080 arn...b5663c31b6e8f801	N/A	N/A	Default: forwarding to lab-ttyd-tg View/edit rules

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

©PentesterAcademy.com

www.attackdefense.com

The top screenshot shows the AWS Management Console 'Target groups (1)' overview page. It includes a search bar and a table with the following data:

	Name	ARN	Port	Protocol
<input type="checkbox"/>	lab-ttyd-tg	arn:aws:elasticloadbalancing...	8080	HTTP

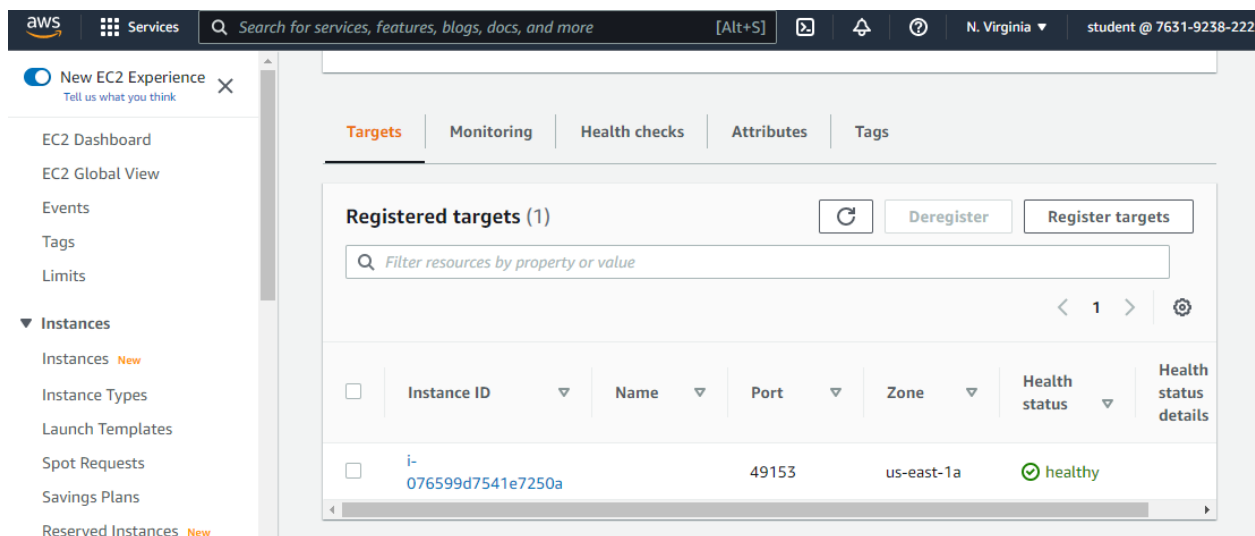
The bottom screenshot shows the 'lab-ttyd-tg' details page. It includes an ARN and a 'Details' section with the following information:

- Target type: Instance
- Protocol : Port: HTTP: 8080
- Protocol version: HTTP1
- VPC: vpc-02691f8c73b1faf77
- IP address type: IPv4
- Load balancer: lab-ttyd-alb

At the bottom of the details page is a status summary table:

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.



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.

Auto Scaling groups (1) Info Edit Delete Create an Auto Scaling group

Search your Auto Scaling groups

<input type="checkbox"/>	Name	Launch template/configuration	Instances	Status
<input checked="" type="checkbox"/>	ECS-lab-asg	terraform-2022080510522122680...	1	-

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

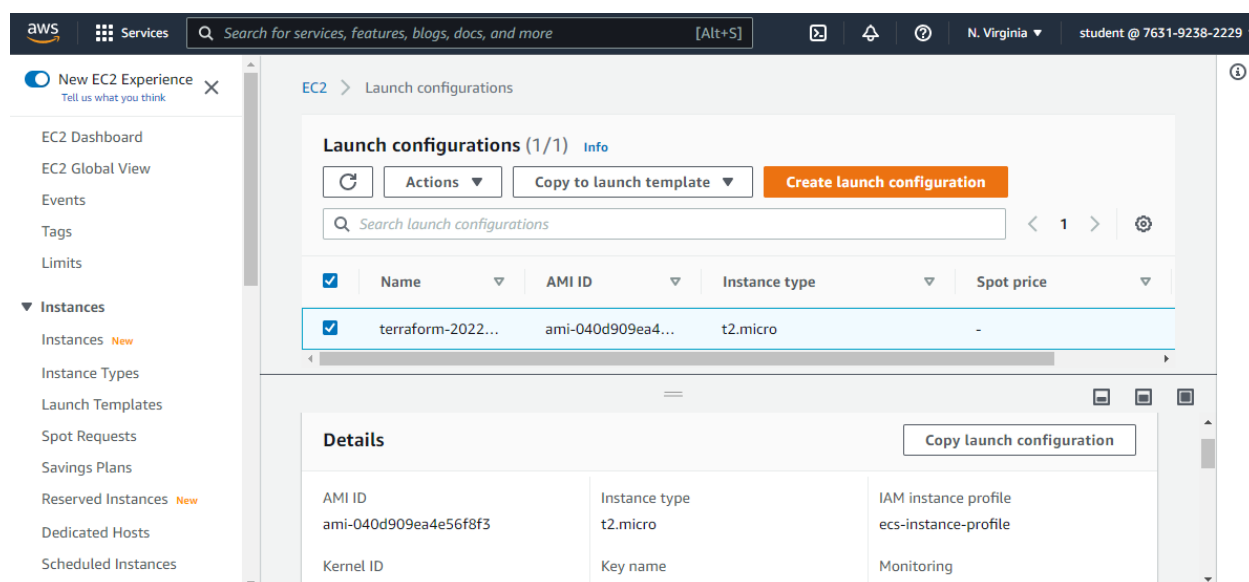
Details Activity Automatic scaling Instance management Monitoring

Instance refresh

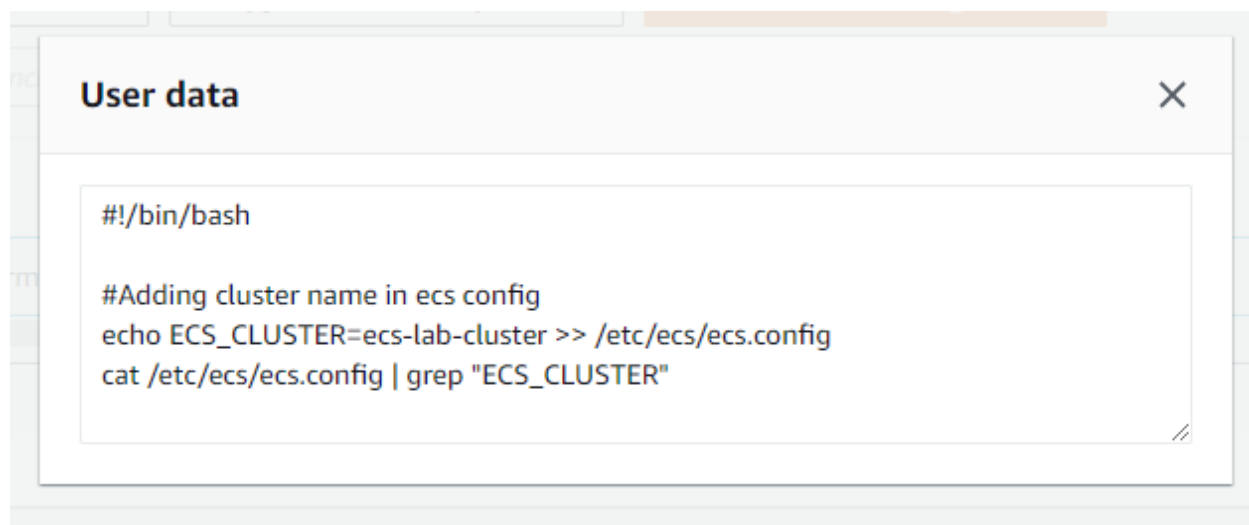
Group details Edit

Desired capacity 1	Auto Scaling group name ECS-lab-asg
Minimum capacity 0	Date created Fri Aug 05 2022 16:22:22 GMT+0530 (India Standard Time)
Maximum capacity 1	Amazon Resource Name (ARN) arn:aws:autoscaling:us-east-1:763192382229:autoScalingGroup:p: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.



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.



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/>)