

[illegible]

Name	ECS: Retrieving secrets from task definitions
URL	https://attackdefense.com/challengedetails?cid=2448
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.

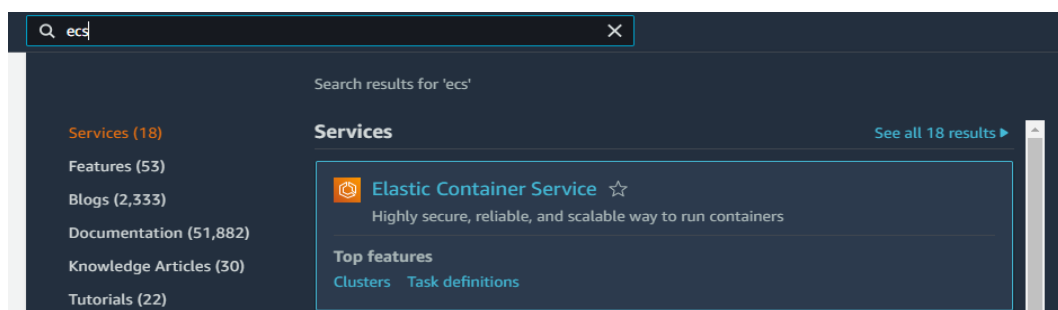
Solution:

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

Access Credentials to your AWS lab Account

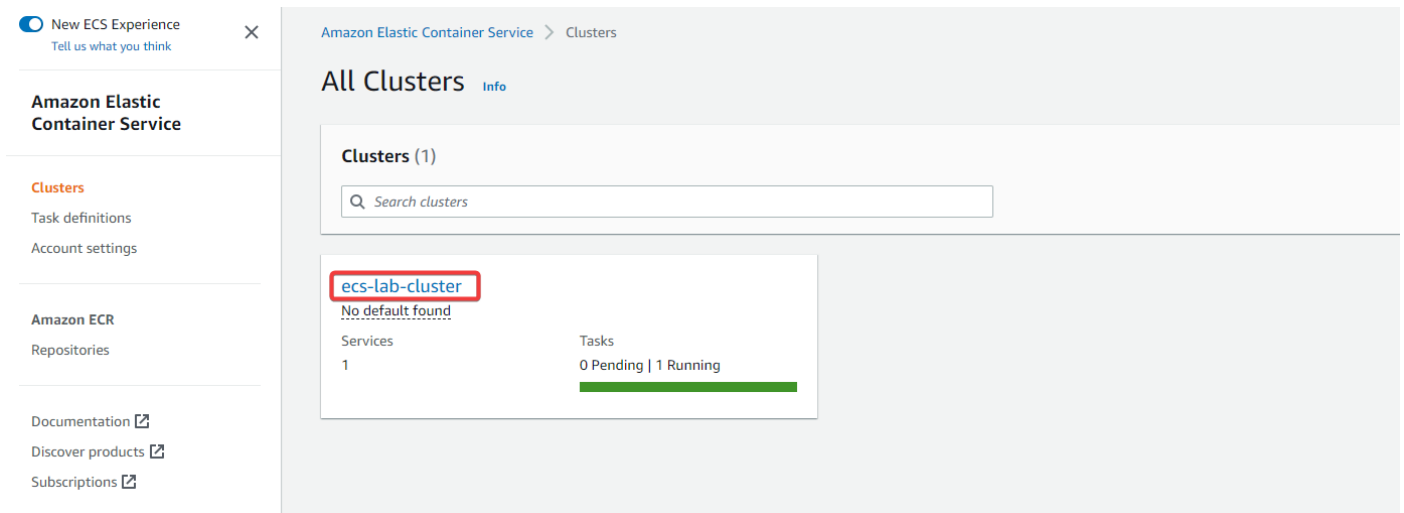
Login URL	https://656293157125.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	student
Password	Ad1b7jyhBWdQQXkp

Step 2: Search for ECS and navigate to ECS dashboard.



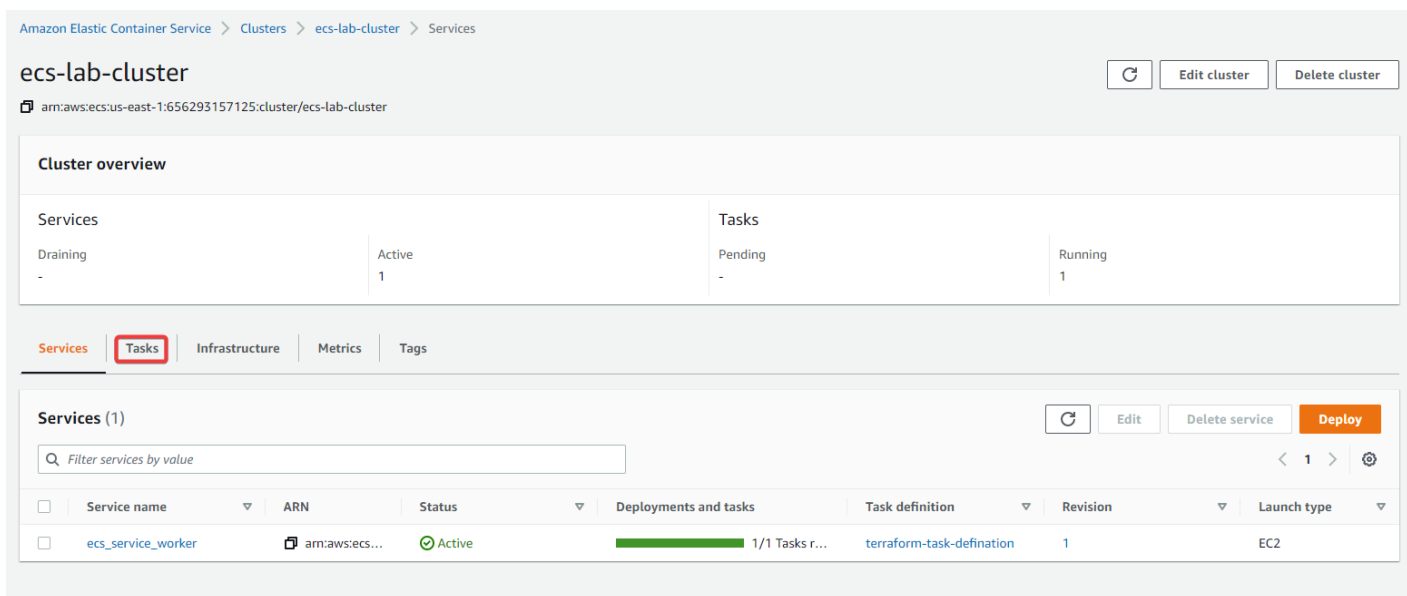
Step 3: Navigate to Clusters and click on “ecs-lab-cluster”.

It will list tasks and services in this cluster.



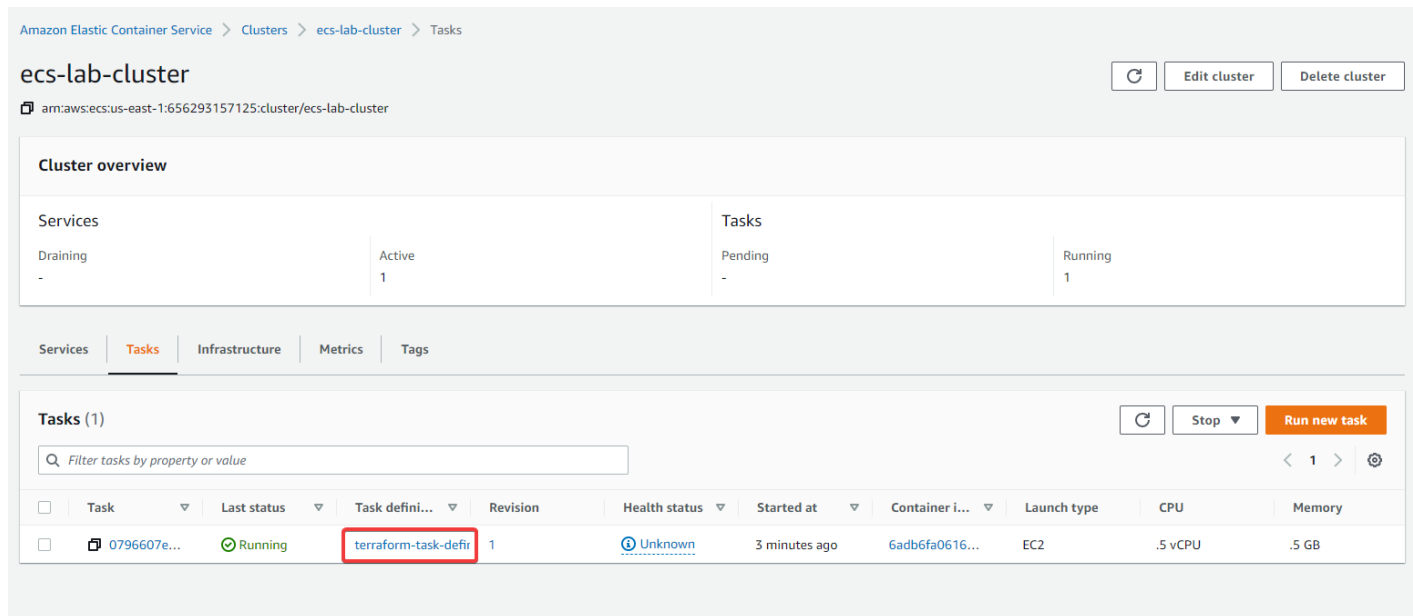
The screenshot shows the Amazon ECS console. On the left, the navigation menu includes 'New ECS Experience', 'Amazon Elastic Container Service', 'Clusters', 'Task definitions', 'Account settings', 'Amazon ECR', 'Repositories', 'Documentation', 'Discover products', and 'Subscriptions'. The main content area is titled 'All Clusters' and shows a search bar and a list of clusters. The cluster 'ecs-lab-cluster' is highlighted with a red box. Below the cluster name, it shows 'No default found', 'Services: 1', and 'Tasks: 0 Pending | 1 Running' with a green progress bar.

Step 4: Navigate to the Tasks.



The screenshot shows the 'ecs-lab-cluster' page in the Amazon ECS console. The breadcrumb trail is 'Amazon Elastic Container Service > Clusters > ecs-lab-cluster > Services'. The page title is 'ecs-lab-cluster' with a refresh button, 'Edit cluster', and 'Delete cluster' buttons. Below the title is the ARN: 'arn:aws:ecs:us-east-1:656293157125:cluster/ecs-lab-cluster'. The 'Cluster overview' section shows a table with 'Services' (Draining: -, Active: 1) and 'Tasks' (Pending: -, Running: 1). Below this is a tabbed interface with 'Services', 'Tasks' (selected and highlighted with a red box), 'Infrastructure', 'Metrics', and 'Tags'. The 'Tasks' tab shows a table with 'Services (1)' and a search bar. The table has columns: Service name, ARN, Status, Deployments and tasks, Task definition, Revision, and Launch type. The row for 'ecs_service_worker' shows it is 'Active' with a green progress bar, using 'terraform-task-definition' revision 1, and has a launch type of 'EC2'.

Step 5: Click on the task definition name.



Amazon Elastic Container Service > Clusters > ecs-lab-cluster > Tasks

ecs-lab-cluster

arn:aws:ecs:us-east-1:656293157125:cluster/ecs-lab-cluster

Cluster overview

Services	Tasks
Draining -	Pending -
Active 1	Running 1

Services | **Tasks** | Infrastructure | Metrics | Tags

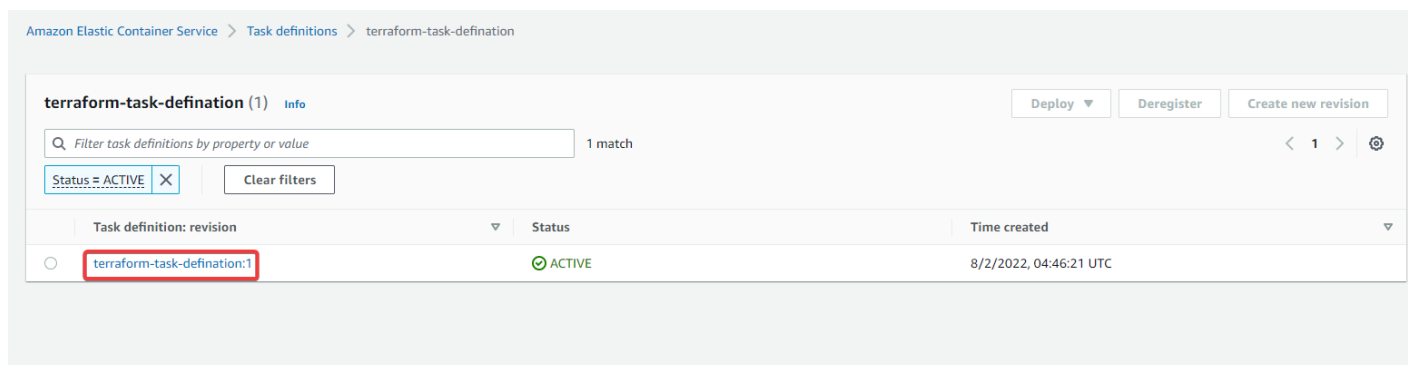
Tasks (1)

Filter tasks by property or value

<input type="checkbox"/>	Task	Last status	Task defini...	Revision	Health status	Started at	Container I...	Launch type	CPU	Memory
<input type="checkbox"/>	0796607e...	Running	terraform-task-defini	1	Unknown	3 minutes ago	6adb6fa0616...	EC2	.5 vCPU	.5 GB

Step 6: Click on the task-definition: revision name.

A task definition revision is a copy of the current task definition with the new parameter values replacing the existing ones. All parameters that you do not modify are in the new revision.



Amazon Elastic Container Service > Task definitions > terraform-task-definition

terraform-task-definition (1) Info

Deploy | Deregister | Create new revision

Filter task definitions by property or value 1 match

Status = ACTIVE Clear filters

<input type="radio"/>	Task definition: revision	Status	Time created
<input type="radio"/>	terraform-task-definition:1	ACTIVE	8/2/2022, 04:46:21 UTC

Step 7: Click on the container name.

It will trigger a pop up window containing the details about the container.

Amazon Elastic Container Service > Task definitions > terraform-task-definition > Revision 1 > Containers

terraform-task-definition:1

Deploy ▼ Deregister Create new revision

General configuration Info

Time created 8/2/2022, 04:46:21 UTC	Status ✔ ACTIVE	App environment EC2
Network mode -	Task role ecs-task-role	Task execution role ecs-task-role

Containers JSON Storage Tags

Task size

Task CPU .5 vCPU	Task memory .5 GB
---------------------	----------------------

Containers Info

Container name	Image	Essential	CPU	Memory
tttyd-lab-container	327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest	true	0	-

n-task-definition:1

configuration

6:46:21 UTC

ie

JSON

Sta

S Info

me

ainer

environment

execution role

ask-role

Essential

true

Dept

ttyd-lab-container

Environmental settings

CPU	Memory	GPU
0	-	-

Port mapping

Host port:container port/protocol

8080:8080/tcp

Environment

Environment variables

Key	Type	Value
Flag1	value	5bcbf1935e31b6fe875fd8d5ff4ca07d

Environment files (S3 ARN)

-

Done

Successfully got the first flag.

Flag: 5bcbf1935e31b6fe875fd8d5ff4ca07d

Step 8: Click on JSON from the tabs.

This will list the JSON configuration of the container.

terraform-task-defination:1

Deploy ▾

Deregister

Create new revision

General configuration [Info](#)

Time created
8/2/2022, 04:46:21 UTC

Network mode
-

Status
ACTIVE

Task role
[ecs-task-role](#)

App environment
EC2

Task execution role
[ecs-task-role](#)

Containers

JSON

Storage

Tags

Task size

Task CPU
.5 vCPU

Task memory
.5 GB

Containers [Info](#)

Container name	Image	Essential	CPU	Memory
ttyd-lab-container	327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest	true	0	-

Step 9: Copy or download the JSON file and check the configuration.

Containers

JSON

Storage

Tags

JSON

```
{
  "taskDefinitionArn": "arn:aws:ecs:us-east-1:656293157125:task-definition/terraform-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": 8080,
          "protocol": "tcp"
        }
      ],
      "essential": true,
      "command": [
        "ttyd",
        "-p",
        "8080",
        "-t",
        "disableLeaveAlert=true",
        "bash"
      ],
      "environment": [
        {

```

Download JSON

Copy to clipboard

Open the json file in a text editor to view the applied configurations.

```
{ data.json > ...
1  {
2    "taskDefinitionArn": "arn:aws:ecs:us-east-1:656293157125:task-definition/terraform-task-definition:1",
3    "containerDefinitions": [
4      {
5        "name": "ttyd-lab-container",
6        "image": "327129574815.dkr.ecr.us-east-1.amazonaws.com/ttyd:latest",
7        "cpu": 0,
8        "portMappings": [
9          {
10             "containerPort": 8080,
11             "hostPort": 8080,
12             "protocol": "tcp"
13           }
14         ],
15        "essential": true,
16        "command": [
17          "ttyd",
18          "-p",
19          "8080",
20          "-t",
21          "disableLeaveAlert=true",
22          "bash"
23        ],
24        "environment": [
25          {
26            "name": "Flag1",
27            "value": "5bcbf1935e31b6fe875fd8d5ff4ca07d"
28          }
29        ],
30        "mountPoints": [],
31        "volumesFrom": [],
32        "secrets": [
33          {
34            "name": "Flag2",
35            "valueFrom": "arn:aws:secretsmanager:us-east-1:656293157125:secret:Flagv7-ahthi6"
36          }
37        ]
38      }
39    ],
40    "family": "terraform-task-definition",
41    "taskRoleArn": "arn:aws:iam:656293157125:role/ecs-task-role",
42    "executionRoleArn": "arn:aws:iam:656293157125:role/ecs-task-role",
```

Container is open at port 8000 and also the flag is present inside the secrets manager.

The image used by the container is ttyd. Now obtain the public dns URL and append it with :8080. It will give access to the docker container using a ttyd terminal.

Step 10: Click on “Clusters” from the left navigation menu.

Clusters

Task definitions

Account settings

Amazon ECR

Repositories

Step 11: Click on the Cluster name.

ecs-lab-cluster

No default found

Services

1

Tasks

0 Pending | 1 Running

Step 12: Click on the Task id.

Services Tasks Infrastructure Metrics Tags										
Tasks (1)										
<input type="text" value="Filter tasks by property or value"/>										
<div>⌂ Stop Run new task</div>										
<div>< 1 > ⚙</div>										
<input type="checkbox"/>	Task	Last status	Task defini...	Revision	Health status	Started at	Container i...	Launch type	CPU	Memory
<input type="checkbox"/>	0796607e...	Running	terraform-task-defir	1	Unknown	11 minutes ago	6adb6fa0616...	EC2	.5 vCPU	.5 GB

Step 13: Click on Launch type.

Configuration

Operating system/Architecture Linux/X86_64	Capacity provider -	ENI ID -	Public IP -
CPU Memory .5 vCPU .5 GB	Launch type EC2 6adb6fa061684a86a6e968c51eeb124	Network mode -	Private IP -
Platform version -	Task definition terraform-task-definition:1	Subnet ID -	MAC address -

Containers (1)

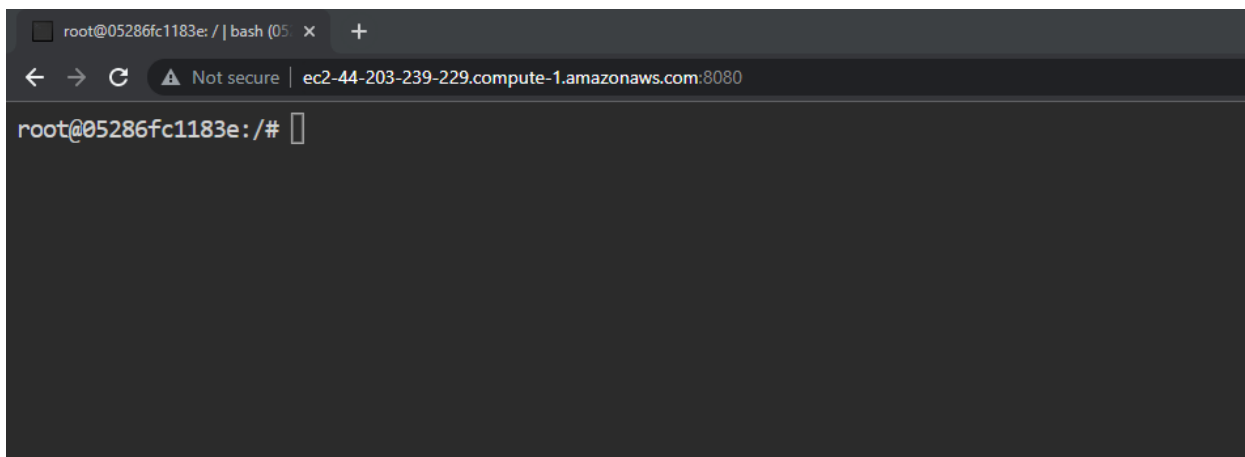
Container name	Container runtime	Image URI	Image Digest	Status	Health status	CPU	Memory hard/soft
ttyd-lab-container	05286fc1183ec7...	327129574815.dkr....	sha256:b02f3640b4...	Running	Unknown	0	- / -

Step 14: Copy the public DNS and paste it into the browser.

Resources & networking			
Resources			
CPU			
Registered 1024	Available 512		
Memory			
Registered 982	Available 470		
Ports			
Registered ports 6	Ports in use 22, 2376, 2375, 51678, 8080, 51679		

Networking			
Public DNS ec2-44-203-239-229.compute-1.amazonaws.com	Private DNS ip-10-0-1-95.ec2.internal	Public IP 44.203.239.229	Private IP 10.0.1.95

Step 15: Navigate to the URL by appending “:8080” into it.



Step 16: Retrieve the flag in the environment variables.

Command: printenv

```
root@05286fc1183e: /# printenv
AWS_EXECUTION_ENV=AWS_ECS_EC2
AWS_CONTAINER_CREDENTIALS_RELATIVE_URI=/v2/credentials/8e3f6913-872a-416e-9a83-cd39b93ee93a
HOSTNAME=05286fc1183e
PWD=/
ECS_CONTAINER_METADATA_URI_V4=http://169.254.170.2/v4/ee8babe3-1bc0-41cd-ae79-597aa28fc84e
TZ=Etc/UTC
Flag1=5bcbf1935e31b6fe875fd8d5ff4ca07d
Flag2= {
  "FLAG": "777e84ef2be3549a4949748e29366e4b"
}

HOME=/root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30
=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:
z=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.
sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31
35:*.mjpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.
pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=
1;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm
=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.wav=00;36:
:
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm-256color
LESSOPEN=| /usr/bin/lesspipe %s
ECS_CONTAINER_METADATA_URI=http://169.254.170.2/v3/ee8babe3-1bc0-41cd-ae79-597aa28fc84e
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
DEBIAN_FRONTEND=noninteractive
_=/usr/bin/printenv
root@05286fc1183e: /#
```

Flag: 777e84ef2be3549a4949748e29366e4b



References:

1. AWS ECS documentation
(<https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html>)