

AMAZON KUBERNETES SERVICES

Amazon has a ECS (Elastic Container Service) under its container services which is used to run Docker applications on a scalable cluster. You can deploy the Docker application with Load Balancing [optional], as it automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones.

Elastic Load Balancing supports the following types of load balancers: Application Load Balancers, Network Load Balancers, and Classic Load Balancers. Amazon ECS services can use either type of load balancer. Application Load Balancers are used to route HTTP/HTTPS (or Layer 7) traffic.

Prerequisites

- Account on AWS with Free Tier or Paid.
- <https://aws.amazon.com/>

STEPS

1. DVWA Docker Image deployment
 - a. Login to AWS Console.

AWS Management Console

AWS services

Find Services

You can enter names, keywords or acronyms.

🔍 Example: Relational Database Service, database, RDS

▼ Recently visited services



EC2



Elastic Kubernetes Service



Elastic Container Service



Elastic Container Registry



CloudWatch

▼ All services



Compute

EC2

Lightsail

Lambda

Batch

Elastic Beanstalk

Serverless Application

Repository

AWS Outposts

EC2 Image Builder



Containers

Elastic Container Registry

Elastic Container Service

Elastic Kubernetes Service



Blockchain

Amazon Managed
Blockchain



Satellite

Ground Station



Quantum Technologies

Amazon Braket



Management & Governance

AWS Organizations

CloudWatch

AWS Auto Scaling

CloudFormation



Security, Identity, & Compliance

IAM

Resource Access Manager

Cognito

Secrets Manager

GuardDuty

Inspector

Amazon Macie

AWS Single Sign-On

Certificate Manager

Key Management Service

CloudHSM

Directory Service

WAF & Shield

AWS Firewall Manager

Artifact



Storage

b.

c. In AWS Management Console, choose **Elastic Container Service** (All Services > Containers > Elastic Container Service).

d. On the Left Pane, Choose **Clusters** under Amazon ECS.

e. Click on **Get Started**.

f. In Step 1, **Custom image configure** (Container and Task -> Container definition)

g. Give any container name.

- h. Image: **vulnerables/web-dvwa**
- i. Memory Limits: **300**
- j. Port mappings: **80 tcp**.
- k. In Step 2, **Load Balancer type: None (default)**. But if you want to add then create a Load Balancer in ELB, then add it under **Application Load Balancer**.
- l. Give a **Cluster name**.
- m. Click **Next** and then **Create**.

n.

Getting Started with Amazon Elastic Container Service (Amazon ECS) using Fargate

Launch Status

We are creating resources for your service. This may take up to 10 minutes. When we're complete, you can view your service.

[Back](#)
[View service](#)

Additional features that you can add to your service after creation

Scale based on metrics
You can configure scaling rules based on CloudWatch metrics

Preparing service : 10 of 10 complete

ECS resource creation		complete
Cluster	docker-dvwa	complete
Task definition	first-run-task-definition:3	complete
Service	docker-dvwa-service	complete
Additional AWS service integrations		complete
Log group	The log group [/ecs/first-run-task-definition] already exists	complete
CloudFormation stack	ECSContainerService-docker-dvwa	complete
VPC	vpc-065fa7e4f95d4d24	complete
Subnet 1	subnet-046cd6576035cd9e7	complete
Subnet 2	subnet-000d09a512f8a2fcd	complete
Security group	sg-0c12e347194a1420	complete
Load balancer	arn:aws:elasticloadbalancing:us-east-2:156700625770:loadbalancer/app/EC2Co-EcsEl-NG9KXN8U0XN774B99974919d0d7	complete

2. Opening the DVWA Application

- a. **Click on your Cluster Name** that you just created. (Amazon ECS > Clusters > Cluster-Name)

Clusters > docker-dvwa

Cluster : docker-dvwa

Update Cluster Delete Cluster

Get a detailed view of the resources on your cluster.

Cluster ARN am:aws:ecs:us-east-2:156700625770:cluster/docker-dvwa

Status **ACTIVE**

Registered container instances 0

Pending tasks count 0 Fargate, 0 EC2

Running tasks count 1 Fargate, 0 EC2

Active service count 1 Fargate, 0 EC2

Draining service count 0 Fargate, 0 EC2

Services Tasks ECS Instances Metrics Scheduled Tasks Tags Capacity Providers

Create Update Delete Actions

Last updated on September 8, 2020 10:42:33 PM (0m ago)

Filter in this page Launch type ALL Service type ALL < 1-1 >

	Service Name	Status	Service...	Task D...	Desired...	Runnin...	Launch...	Platfor...
<input type="checkbox"/>	docker-dvwa-service	ACTIVE	REPLICA	first-run-...	1	1	FARGATE	LATES...

- b. **Go to Tasks** tab, and click on the task which should be in RUNNING STATE.

Cluster : docker-dvwa

[Update Cluster](#)[Delete Cluster](#)

Get a detailed view of the resources on your cluster.

Cluster ARN am:aws:ecs:us-east-2:156700625770:cluster/docker-dvwa

Status **ACTIVE**

Registered container instances 0

Pending tasks count 1 Fargate, 0 EC2

Running tasks count 0 Fargate, 0 EC2

Active service count 1 Fargate, 0 EC2

Draining service count 0 Fargate, 0 EC2

[Services](#) [Tasks](#) [ECS Instances](#) [Metrics](#) [Scheduled Tasks](#) [Tags](#) [Capacity Providers](#)

[Run new Task](#) [Stop](#) [Stop All](#) [Actions](#)

Last updated on September 8, 2020 10:48:49 PM (1m ago) [Refresh](#) [Help](#)

Desired task status: [Running](#) [Stopped](#)

Launch type [ALL](#)

< 1-1 > Page size 50

<input type="checkbox"/>	Task	Task def...	Contain...	Last sta...	Desired ...	Started at	Started ...	Group	Launch ...	Platform...
<input type="checkbox"/>	4e80553f...	first-run-t...	--	PROVISI...	RUNNING		ecs-svc/...	service:d...	FARGATE	1.3.0

c.

d. Find the **Public IP** mentioned for your application.

Task : 4e80553f6a214a9fb0428925022d8609

Run more like this

SI

Details

Tags

Logs

Cluster [docker-dvwa](#)
Launch type FARGATE
Platform version 1.3.0
Task definition [first-run-task-definition:3](#)
Group service:docker-dvwa-service
Task role None
Last status **RUNNING**
Desired status RUNNING
Created at 2020-09-08 22:48:42 +0530
Started at 2020-09-08 22:49:30 +0530

Network

Network mode awsvpc
ENI Id [eni-02fc62d1ae334e8ce](#)
Subnet Id subnet-046cf6576635cd5e7
Private IP 10.0.0.242
Public IP 3.15.195.170
Mac address 02:60:6c:28:70:4a

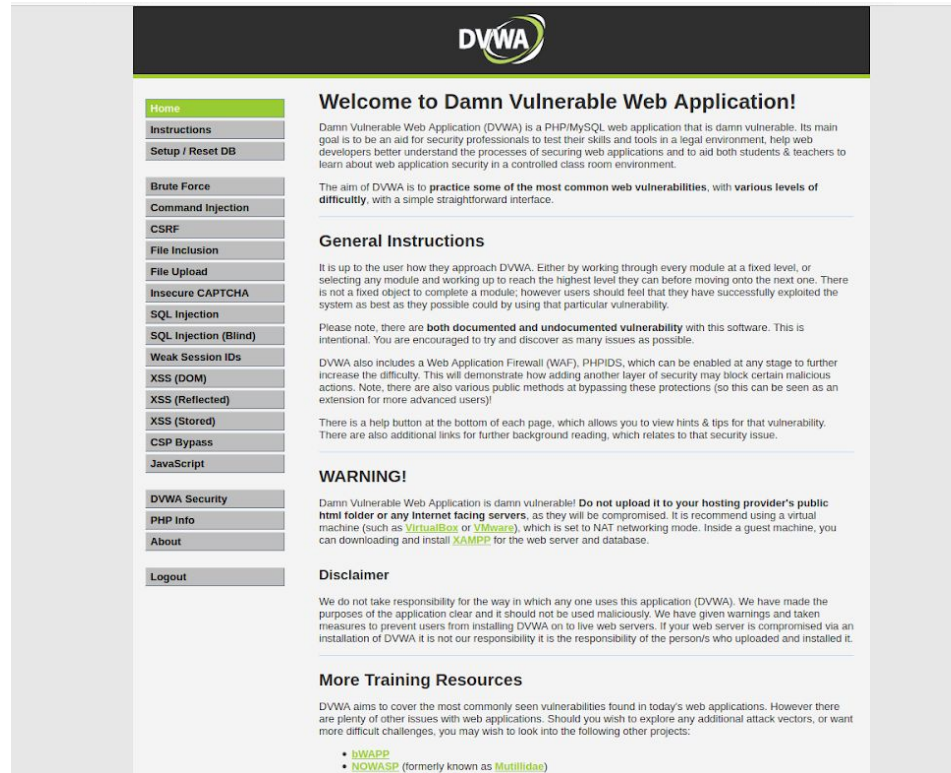
Containers

Last updated on September 8, 2020 10:50:59 PM (1m ago)



	Name	Container Runtime ID	Sta	Image	Image Digest
▼	docker-dvwa	8a27e58b5ef29f76bfe...	RU	vulnerables/web-dvwa	

- e.
- f. Just paste the Public IP, in your Browser url bar.
- g. You will see a DVWA application.



- h.
- i. Go to SQL Injection and do SQLi attacks.

3. Logs Generation

- a. **Click on your Cluster Name** that you just created. (Amazon ECS > Clusters > Cluster-Name)
- b. **Go to Tasks** tab.



- c.
- d. **Click the arrow** (before the Container Name) to get the details of the container.

Details

Network bindings - not configured

Environment Variables - not configured

Environment Files - not configured

Docker labels - not configured

Extra hosts - not configured

Mount Points - not configured

Volumes from - not configured

Ulimits - not configured

Elastic Inference - not configured

Log Configuration

Log driver: awslogs [View logs in CloudWatch](#)

Key	Value
awslogs-group	/ecs/first-run-task-definition
awslogs-region	us-east-2
awslogs-stream-prefix	ecs

- e.
- f. Click on the **View logs in CloudWatch**.
- g. There you will find all the logs of your application.


```
2020-09-08T20:22:40.225+05:3... 203.81.241.206 - - [08/Sep/2020:14:52:39 +0000] "GET /dwa/js/add_event_listeners.js HTTP/1.1" 200 626 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Li...
2020-09-08T20:22:40.225+05:3... 203.81.241.206 - - [08/Sep/2020:14:52:39 +0000] "GET /dwa/css/main.css HTTP/1.1" 200 1446 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; ...
2020-09-08T20:22:40.225+05:3... 203.81.241.206 - - [08/Sep/2020:14:52:40 +0000] "GET /dwa/images/logo.png HTTP/1.1" 200 5330 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_6...
2020-09-08T20:22:40.225+05:3... 203.81.241.206 - - [08/Sep/2020:14:52:40 +0000] "GET /dwa/images/spanner.png HTTP/1.1" 200 748 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86...
2020-09-08T20:22:43.225+05:3... 203.81.241.206 - - [08/Sep/2020:14:52:43 +0000] "POST /setup.php HTTP/1.1" 302 337 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:22:43.225+05:3... ==> /var/log/apache2/error.log <=
2020-09-08T20:22:43.225+05:3... [Tue Sep 08 14:52:43.075031 2020] [error] [pid 319] [client 203.81.241.206:55210] PHP Notice: Constant DVWA_WEB_PAGE_TO_ROOT already defined in /var/www/html/dvwa/...
2020-09-08T20:22:44.225+05:3... ==> /var/log/apache2/access.log <=
2020-09-08T20:22:44.225+05:3... 203.81.241.206 - - [08/Sep/2020:14:52:43 +0000] "GET /setup.php HTTP/1.1" 200 2184 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:22:50.226+05:3... 203.81.241.206 - - [08/Sep/2020:14:52:49 +0000] "GET /login.php HTTP/1.1" 200 1048 "http://3.137.140.87/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:23:01.228+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:00 +0000] "POST /login.php HTTP/1.1" 302 337 "http://3.137.140.87/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:23:01.228+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:01 +0000] "GET /index.php HTTP/1.1" 200 3037 "http://3.137.140.87/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:23:05.228+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:04 +0000] "GET /vulnerabilities/sqli/ HTTP/1.1" 200 1771 "http://3.137.140.87/index.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:23:05.228+05:3... 10.0.1.65 - - [08/Sep/2020:14:53:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:05.228+05:3... 10.0.0.53 - - [08/Sep/2020:14:53:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:16.230+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:16 +0000] "GET /vulnerabilities/sqli/?id=333d1&Submit=Submit HTTP/1.1" 200 503 "http://3.137.140.87/vulnerabilities/sqli..."
2020-09-08T20:23:23.231+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:22 +0000] "GET /vulnerabilities/sqli/ HTTP/1.1" 200 1772 "http://3.137.140.87/vulnerabilities/sqli/" "Mozilla/5.0 (X11; Ubuntu..."
2020-09-08T20:23:26.231+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:26 +0000] "GET /vulnerabilities/view_help.php?id=sqli&security=low HTTP/1.1" 200 1951 "http://3.137.140.87/vulnerabilities/sqli..."
2020-09-08T20:23:27.232+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:26 +0000] "GET /dwa/css/help.css HTTP/1.1" 200 522 "http://3.137.140.87/vulnerabilities/view_help.php?id=sqli&security=low" "..."
2020-09-08T20:23:35.233+05:3... 10.0.1.65 - - [08/Sep/2020:14:53:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:35.233+05:3... 10.0.0.53 - - [08/Sep/2020:14:53:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:23:45.234+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:44 +0000] "GET /vulnerabilities/sqli/?id=333d1&3da&27+UNION+SELECT+422text1&22&2c&22text2&22&3B---+426Submit&3DSubmit&Submit=5...
2020-09-08T20:23:57.236+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:57 +0000] "GET /security.php HTTP/1.1" 200 2456 "http://3.137.140.87/vulnerabilities/sqli/?id=333d1&3da&27+UNION+SELECT+422tex...
2020-09-08T20:23:58.236+05:3... 203.81.241.206 - - [08/Sep/2020:14:53:57 +0000] "GET /dwa/images/lock.png HTTP/1.1" 200 1045 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:24:01.237+05:3... 203.81.241.206 - - [08/Sep/2020:14:54:00 +0000] "POST /security.php HTTP/1.1" 302 427 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:24:01.237+05:3... 203.81.241.206 - - [08/Sep/2020:14:54:01 +0000] "GET /security.php HTTP/1.1" 200 2475 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:24:05.237+05:3... 203.81.241.206 - - [08/Sep/2020:14:54:04 +0000] "GET /vulnerabilities/sqli/ HTTP/1.1" 200 1812 "http://3.137.140.87/security.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)..."
2020-09-08T20:24:05.237+05:3... 10.0.1.65 - - [08/Sep/2020:14:54:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:24:05.237+05:3... 10.0.0.53 - - [08/Sep/2020:14:54:04 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:24:10.238+05:3... 203.81.241.206 - - [08/Sep/2020:14:54:09 +0000] "POST /vulnerabilities/sqli/ HTTP/1.1" 200 1845 "http://3.137.140.87/vulnerabilities/sqli/" "Mozilla/5.0 (X11; Ubuntu..."
2020-09-08T20:24:14.239+05:3... 203.81.241.206 - - [08/Sep/2020:14:54:13 +0000] "GET /vulnerabilities/view_help.php?id=sqli&security=medium HTTP/1.1" 200 1951 "http://3.137.140.87/vulnerabilities/sqli..."
2020-09-08T20:24:33.242+05:3... 203.81.241.206 - - [08/Sep/2020:14:54:32 +0000] "POST /vulnerabilities/sqli/ HTTP/1.1" 200 1845 "http://3.137.140.87/vulnerabilities/sqli/" "Mozilla/5.0 (X11; Ubuntu..."
2020-09-08T20:24:35.242+05:3... 10.0.1.65 - - [08/Sep/2020:14:54:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
2020-09-08T20:24:35.242+05:3... 10.0.0.53 - - [08/Sep/2020:14:54:34 +0000] "GET / HTTP/1.1" 302 442 "-" "ELB-HealthChecker/2.0"
```

No newer events at this moment. *Auto retry paused. Resume*

h.