

NetReach on Amazon ECS Installation Guide

This quick guide provides the steps to host NetReach containerized application on Amazon ECS using Amazon EFS (Elastic File System) for persistent storage and a hostname for HTTPS.

NOTE: This guide assumes you're using AWS Fargate with Amazon ECS (Elastic Container Service).

Prerequisites

- An **AWS account**
- An **AWS Secrets Manager** to store WTI Azure Container Registry (ACR) credentials (provided by WTI)
- An **ACM (AWS Certificate Manager)** – For managing SSL/TLS certificates.
- Basic knowledge of VPCs, subnets and security groups
- An existing or planned **Application Load Balancer (ALB)** (this is key for HTTPS)
- IAM permissions to create/modify/execute ECS, EFS, ALB, and target groups

Step 1: Create AWS Secret Manager

1. Go to **Secrets Manager > Secrets**. Click store a new secret. WTI Tech Support will provide username/password for your Azure ACR.

Choose secret type: **Other type of secret**

Under key/value pair section

Add:

- Key: **username**, Value: <your-acr-username>
- Key: **password**, Value: <your-acr-password>



Key/value pairs <small>Info</small>	
Key/value	Plaintext
username	[Redacted]06 Remove
password	[Redacted]bc Remove
+ Add row	

2. Name the secret, e.g., acrDockerCredentials

Step 2: Create ECS task role and task execution role

1. Go to **IAM > Roles**

1. Create task role and task execution role with the following policies:

For ECS Task role

- Trusted entity type: **AWS service**
- Service or user case: **Elastic Container Service** (dropdown)
- Use case: **Elastic Container Service Task**

Add permission

- **AmazonElasticFileSystemClientFullAccess**


NetReachECSTask Info Delete

Allows ECS tasks to call AWS services on your behalf.

Summary Edit

Creation date
September 30, 2025, 09:32 (UTC-07:00)

Last activity
-

ARN
 arn:aws:iam::654654326454:role/NetReachECSTask

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Last Accessed | Revoke sessions

Permissions policies (1) Info Simulate Remove Add permissions

You can attach up to 10 managed policies.

Filter by Type
All types

< 1 > 

<input type="checkbox"/>	Policy name 	Type	Attached entities
<input type="checkbox"/>	  AmazonElasticFileSystemClientFullAccess	AWS managed	1

For ECS Task Execution role

- Trusted entity type: **AWS service**
- Service or user case: **Elastic Container Service** (dropdown)
- Use case: **Task Execution Role for Elastic Container Service**

Add permission

- **AmazonECSTaskExecutionRolePolicy**
- **SecretsManagerReadWrite** (or read-only access to your secret)

NetReachESCTaskExecution Info
Delete

Allows access to other AWS service resources that are required to run Amazon ECS tasks.

Summary Edit

Creation date
September 30, 2025, 09:50 (UTC-07:00)

Last activity
-

ARN
arn:aws:iam::654654326454:role/NetReachESCTaskExecution

Maximum session duration
1 hour

Permissions
Trust relationships
Tags
Last Accessed
Revoke sessions

Permissions policies (2) Info
Simulate
Remove
Add permissions

You can attach up to 10 managed policies.

Filter by Type

All types

< 1 >

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonECSTaskExecutionRolePolicy	AWS managed	1
<input type="checkbox"/>	SecretsManagerReadWrite	AWS managed	1

Step 3: Create Security Group

In this section we'll create 3 main security groups:

- EFS Security Group (**netreach-efs-sg**)
- ECS Security Group (**netreach-ecs-sg**)
- ALB Security Group (**netreach-alb-sg**)

- Go to **VPC > Security group**
- For EFS security group (netreach-efs-sg) Inbound rule:**
 - Type: **NFS**
 - Port: **2049**
 - Source: **The security group of your ECS (netreach-ecs-sg)**

Inbound rules Info

Security group rule ID
sgr-0c1ccd97e5fc30179

Type Info

Protocol Info

Port range Info

Source Info

Description - optional Info

NFS

TCP

2049

Custom

Cancel
Preview changes
Save rules

For EFS security group (netreach-efs-sg) Outbound rule:

- Allow all traffic (default)

Outbound rules Info

Security group rule ID
sgr-0cb0012b5ce5e7c53

Type Info

Protocol Info

Port range Info

Destination Info

Description - optional Info

All traffic

All

All

Custom

3. For ECS security group (netreach-ecs-sg) Inbound rule:

- Type: **custom TCP**
- Port: **3000**
- Source: **The security group of your ALB (netreach-alb-sg)**

Inbound rules [Info](#)

Security group rule ID
sgr-02c9d5a21d3056f08

Type [Info](#) Protocol [Info](#) Port range [Info](#) Source [Info](#) Description - optional [Info](#)

Custom TCP TCP 3000 Custom

For ECS security group (netreach-ecs-sg) Outbound rule:

- Type: **NFS**
- Destinations: **The security group of your EFS (netreach-efs-sg)**
- Type: **All Traffic**
- Destination: **0.0.0.0/0**

Outbound rules [Info](#)

Security group rule ID
sgr-08eb1fe02d0b12e88

Type [Info](#) Protocol [Info](#) Port range [Info](#) Destination [Info](#) Description - optional [Info](#)

All traffic All All Custom

sgr-028ea4bf206b5a096

NFS TCP 2049 Custom

4. For ALB security group (netreach-alb-sg) Inbound rule:

- Type: **HTTP and HTTPS**
- Port: **80, 443**
- Source: **custom 0.0.0.0/0**

Inbound rules [Info](#)

Security group rule ID
sgr-0905c5a366c930e96

Type [Info](#) Protocol [Info](#) Port range [Info](#) Source [Info](#) Description - optional [Info](#)

HTTPS TCP 443 Custom

sgr-027af7aea3a528a93

HTTP TCP 80 Custom

For ALB security group (netreach-alb-sg) Outbound rule:

- Type: **All Traffic**
- Destination: **0.0.0.0/0**

Outbound rules [Info](#)

Security group rule ID
sgr-0bfa01b859b1b916e

Type [Info](#) Protocol [Info](#) Port range [Info](#) Destination [Info](#) Description - optional [Info](#)

All traffic All All Custom

Step 4: Create an Amazon EFS File System

1. Go to **Amazon EFS > File Systems**
2. Create file system
3. Under **Network** section click **Manage** and change default security group to your **EFS security group (netreach-efs-sg)**.

Network

Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system.

vpc-0c3e592040884cf1e
default

You must delete all existing mount targets in order to change the VPC of your file system.

Mount targets
A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone	Subnet ID	IP address type	IPv4 address	IPv6 address	Security groups	
us-west-1a	subnet-0d6ea39fc3ffb8	IPv4 only	172.31.2.189	-	Choose security g... sg- be netreach-efs-sg	Remove
us-west-1b	subnet-0533639fc68bb	IPv4 only	172.31.17.166	-	Choose security g... sg- be netreach-efs-sg	Remove

Add mount target

You can only create one mount target per Availability Zone.

Cancel Save

Step 5: Create an ECS Cluster

1. Go to **Amazon ECS > Clusters**
2. Click Create Cluster
3. Name your Cluster
4. Under **Infrastructure** section check **AWS Fargate (serverless)**
- 5 Click Create button

Clusters (1)

Info

Search clusters

Last updated
September 30, 2025, 10:47 (UTC-7:00)

Create cluster

< 1 >

Cluster	Services	Tasks	Container instances	CloudWatch monitoring	Capacity provider strategy
NetReachCluster	0	No tasks running	0 EC2	Default	No default found

Step 6: Create a Task Definition with EFS Volume

1. Go to **Amazon ECS > Tasks definitions**
2. Create new task definition
3. Name your Task definition family
4. Under **Infrastructure** requirements section
 - Launch Type – select **AWS Fargate**
 - Task roles – conditional
 - Task role: select **YourECSTaskRole**
 - Task execution role: select **YourECSTaskExecutionRole**

▼ Infrastructure requirements
Specify the infrastructure requirements for the task definition.

Launch type | [Info](#)
Selection of the launch type will change task definition parameters.

☒ **AWS Fargate**
Serverless compute for containers.

☐ Amazon EC2 instances
Self-managed infrastructure using Amazon EC2 instances.

OS, Architecture, Network mode
Network mode is used for tasks and is dependent on the compute type selected.

Operating system/Architecture | [Info](#)
Linux/X86_64

Network mode | [Info](#)
awsipc

Task size | [Info](#)
Specify the amount of CPU and memory to reserve for your task.

CPU
1 vCPU

Memory
3 GB

▼ Task roles - conditional

Task role | [Info](#)
A task IAM role allows containers in the task to make API requests to AWS services. You can create a task IAM role from the [IAM console](#).

NetReachECSTask

Task execution role | [Info](#)
A task execution IAM role is used by the container agent to make AWS API requests on your behalf. If you don't already have a task execution IAM role created, we can create one for you.

NetReachECSTaskExecution

► **Task placement - optional**

► **Fault injection - optional**

5. Under **Container** – Name your container e.g., *NetReachContainer*
6. **Image URI**, enter your full Azure registry (ACR) images:
 - **netreachacr.azurecr.io/netreach-image:<tag>**
 - **<tag>**: the specific version or tag of the image (e.g., latest, v1.00)
7. For Private registry:
 - Toggle “Private registry” ON
 - Paste the full ARN of the secret you created from step 1, on **AWS Secret Manager** to access Azure registry (ACR)

8. Port mappings:

- Container port: **3000** (the port NetReach app listens on)
- App Protocol: **HTTP**

▼ Container - 1 [Info](#)

Container details

Specify a name, container image, and whether the container should be marked as essential. Each task definition must have at least one essential container.

Name

NetReachContainer

Up to 255 letters (uppercase and lowercase), numbers, hyphens, and underscores are allowed.

Essential container

Yes

Image URI

netreachacr.azurecr.io/netreach-image:v1.00

Up to 255 letters (uppercase and lowercase), numbers, hyphens, underscores, colons, periods, forward slashes, and number signs are allowed.

[Browse ECR images](#)

Private registry [Info](#)

Store credentials in Secrets Manager, and then use the credentials to reference images in private registries.

☒ Private registry authentication

Secrets Manager ARN or name

~~arn:aws:secretsmanager:us-east-1:654654326454:secret:NetReach-DevOps-Credentials-LWTI-FILq63~~

Port mappings [Info](#)

Add port mappings to allow the container to access ports on the host to send or receive traffic. For port name, a default will be assigned if left blank.

Container port	Protocol	Port name	App protocol	
3000	TCP	NetReachapp port	HTTP	Remove

[Add port mapping](#)

9. Under **Storage** - Click Add volume:

- Name: e.g. **NetReach-EFS-Volume**
- Volume type: **EFS**
- File system ID: **Select your EFS FS ID**
- Root directory: / (default)
- Specify **Access point** if using one (optional)
- Transit encryption: **Enable** (recommended)
- IAM role: if needed for access points
- Specify mount point, click Add mount point:
 - Source volume: e.g. **NetReach-EFS-Volume**
 - Container path: **/home/NetReachCloud/**

▼ Volume - 1

Volume name [Info](#)

netreach-efs-volume

Up to 255 letters (uppercase and lowercase), numbers, hyphens, and underscores are allowed.

Configuration type [Info](#)

Choose to configure a volume in the task definition or later at deployment.

☒ Configure at task definition creation
 You can configure bind mount, Docker, Amazon EFS, and Amazon FSx for Windows File Server volumes when creating a task definition.

☐ Configure at deployment
 You can configure 1 Amazon EBS volume when creating or updating a service, or when running a standalone task.

Volume type [Info](#)

EFS

Storage configurations

File system ID [Info](#)

fs-01a50efd1b13819f5

Create new in Amazon EFS console [?](#)

Access point ID [Info](#)

None

Create new in Amazon EFS console [?](#)

Advanced configurations

Root directory [Info](#)

/

Directory within EFS.

Add volume

Container mount points [Info](#)

For each data volume associated with the task, add a container mount point to determine where the data volume is mounted.

Container	Source volume	Container path	Read only
NetReachContainer	netreach-efs-volume	/home/NetReachCloud/	<input type="checkbox"/> Read only

Remove

Add mount point

10. Click Create button.

Step 7: Create a Load Balancer

- Go to the **Load Balance > EC2 features**
- Click Create load balance
- Choose “**Application Load Balancer**”
- Under Basic configuration section:
 - Name: e.g. **netreach-lbc**
 - Scheme: **Internet-facing** (for public access)
 - Load balancer IP Address type: **IPv4**

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

netreach-lbc

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme [Info](#)

Scheme can't be changed after the load balancer is created.

☒ Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

☐ Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type [Info](#)

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ IPv4

Includes only IPv4 addresses.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

☐ Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

5. Under Network mapping section:

- VPC: Choose the **VPC** where your ECS service will run.
- Availability zones and subnets: Select public subnets in difference AZ.

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#).

vpc-0c3e592040884cf1e
172.31.0.0/16

(default)



[Create VPC](#)

IP pools [Info](#)

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view Pools in the [Amazon VPC IP Address Manager console](#).

☐ Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

Availability Zones and subnets [Info](#)

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☒ us-west-1a (usw1-az3)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0d6ea39fc3ffb8b8a
IPv4 subnet CIDR: 172.31.0.0/20

☒ us-west-1b (usw1-az1)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0533639fc68bb80ad
IPv4 subnet CIDR: 172.31.16.0/20

6. Under Security group section:

- Choose **ALB security group (netreach-alb-sg)**.

Security groups

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups



netreach-alb-sg

sg-021706c627fbb714 VPC: vpc-0c3e592040884cf1e

[Cancel](#)

[Save changes](#)

7. Under Listeners and routing section:

Overview Listeners and rule for HTTP and HTTPS

Listeners and rules (2) Info	Network mapping	Resource map	Security	Monitoring	Integrations	Attributes	Capacity	Tags
A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.								
<input type="text" value="Filter listeners"/>								
<input type="checkbox"/>	Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS	Trust store
<input type="checkbox"/>	HTTPS:443	<ul style="list-style-type: none">Forward to target group netreach-ecs-tg: 1 (100%) Target group stickiness: Off	1 rule	ARN	ELBSecurityPolicy-TLS13-1-2-...	test-aws.wti.com (Certificate I...	Off	Not applic
<input type="checkbox"/>	HTTP:80	<ul style="list-style-type: none">Redirect to HTTPS://#{host}:443/#{path}?# (query) Status code: HTTP_301	1 rule	ARN	Not applicable	Not applicable	Not applicable	Not applic

For Listeners: Add port 80 (HTTP)

- Protocol: **HTTP**
- Port: **80**
- Routing Action: **Redirect to URL**
- Protocol: **HTTPS**
- Port: **443**

Listener details
A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Listener ARN
 arn:aws:elasticloadbalancing:us-west-1:654654326454:listener/app/netreach-lbc/648a87de97a4f390/9927d9b265b1f2a2

Protocol
Used for connections from clients to the load balancer.

Port
The port on which the load balancer is listening for connections.

HTTP

80

1-65535

Default action [Info](#)
The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Routing action

☐ Forward to target groups

☒ Redirect to URL

☐ Return fixed response

Redirect to URL [Info](#)
Redirect client requests from one URL to another. You cannot redirect HTTPS to HTTP. To avoid a redirect loop, you must modify at least one of the following components: protocol, port, hostname or path. Components that you do not modify retain their original values.

[URI parts](#)

[Full URL](#)

Protocol
Used for connections from clients to the load balancer.

Port
The port on which the load balancer is listening for connections.

HTTPS

443

1-65535 or to retain the original port enter #{port}

☐ Custom host, path, query
Select to modify host, path and query. If no changes are made, settings from the request URL are retained.

Status code

301 - Permanently moved


For Listeners: Add port 443 (HTTPS).

- Protocol: **HTTPS**
- Port: **443**
- Routing Action: **Forward to target groups**

Listener details

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Listener ARN

 arn:aws:elasticloadbalancing:us-west-1:654654326454:listener/app/netreach-lbc/648a87de97a4f390/522947d965795d05

Protocol

Used for connections from clients to the load balancer.

HTTPS

Port

The port on which the load balancer is listening for connections.

443

1-65535

Default action

[Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Authentication action - optional

[Info](#)

Authentication requires IPv4 connectivity to authentication endpoints. [Learn more](#)

☐ Authenticate users

Configure user authentication through either OpenID Connect (OIDC) or Amazon Cognito.

Routing action

☒ Forward to target groups

☐ Redirect to URL

☐ Return fixed response

Create a target group.

- Click create target group link.

Forward to target group | [Info](#)
Choose a target group and specify routing weight of [create target group](#)

Target group
netreach-ecs-tg
Target type: IP, IPv4 | Target stickiness: Off

Weight
1
0-999

Percent
100%

[+ Add target group](#)
You can add up to 4 more target groups.

Target group stickiness | [Info](#)
Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.

☐ Turn on target group stickiness

- Target type: **IP mode (for ECS Fargate)**
- Target Group Name: e.g. **netreach-ecs-tg**
- Protocol: **HTTP**
- Port: **3000** (this should match your ECS container port; NetReach uses port 3000)
- Health check path: **/login**

netreach-ecs-tg

Actions

Details

 arn:aws:elasticloadbalancing:us-west-1:654654326454:targetgroup/netreach-ecs-tg/88621ba0356f7579

Target type

IP

Protocol : Port

HTTP: 3000

Protocol version

HTTP1

VPC

[vpc-0c3e592040884cf1e](#)

IP address type

IPv4

Load balancer

[netreach-lbc](#)

1

Total targets

1

Healthy

0

Unhealthy

0

Unused

0

Initial

0

Draining

0 Anomalous

Distribution of targets by Availability Zone (AZ)

Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (1)

[Info](#)

[Anomaly mitigation: Not applicable](#)

[Deregister](#)

[Register targets](#)

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Filter targets

< 1 > 

<input type="checkbox"/>	IP address	Port	Zone	Health status	Health status details	Administrative override	Override details	Anomaly detection...
<input type="checkbox"/>	172.31.8.150	3000	us-west-1a ...	Healthy	-	No override	No override is currently active on target	Normal

Targets	Monitoring	Health checks	Attributes	Tags
Health check settings Edit				
Protocol HTTP	Path /login	Port Traffic port	Healthy threshold 5 consecutive health check successes	
Unhealthy threshold 2 consecutive health check failures	Timeout 5 seconds	Interval 30 seconds	Success codes 200	

8. Under Default SSL/TLS Server Certificate:

- Choose an existing certificate from **AWS Certificate Manager (ACM)**
- If none exists, go to **ACM**, or request a new ACM certificate, and validate your domain.

Secure listener settings [info](#)

Security policy [info](#)
 Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compare security policies](#)

Security category All security policies
Policy name ELBSecurityPolicy-TLS13-1-2-Res-2021-06 (recommended)

Default SSL/TLS server certificate
 The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source

☒ From ACM
 ☐ From IAM
 ☐ Import certificate

Certificate (from ACM)
 The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

test-aws.wti.com
 463297b7-25cd-4365-b502-2f2921b5bbd5

[Request new ACM certificate](#)

Client certificate handling [info](#)
 Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

☐ **Mutual authentication (mTLS)**
 Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.

Step 8: Create a Service

1. Go to **ECS > Clusters > Your Cluster > Create Service**

2. Service details

- Task definition family: **Select your task definition family**
- Service name: e.g., **netreachapp-service**

Create service [Info](#)

Service details

Task definition family
 Select an existing task definition family. To create a new task definition, go to [Task definitions](#).

netreachapp-task-definition

Task definition revision Latest
 Select the task definition revision from the 100 most recent entries, or enter a revision. Leave the field blank to use the latest revision.

2

Service name
 Assign a service name that is unique for this cluster.

netreachapp-service

Up to 255 letters (uppercase and lowercase), numbers, underscores, and hyphens are allowed. Service names must be unique within a cluster.

3. Environment > Compute configuration

- Compute option: **Capacity provider strategy**
- Capacity provider: **FARGATE**

Environment

Existing cluster

NetReachCluster

▼ **Compute configuration - advanced**

Compute options | [Info](#)

To ensure task distribution across your compute types, use appropriate compute options.

☒ **Capacity provider strategy**
Specify a launch strategy to distribute your tasks across one or more capacity providers.

☐ **Launch type**
Launch tasks directly without the use of a capacity provider strategy.

Capacity provider strategy | [Info](#)

Select either your cluster default capacity provider strategy or select the custom option to configure a different strategy.

☐ Use cluster default
No default capacity provider strategy configured for this cluster.

☒ Use custom (Advanced)

Capacity provider

FARGATE ▼

Base | [Info](#)

0

Weight | [Info](#)

1

[Add capacity provider](#)

You can add up to 1 more capacity provider strategy item.

Platform version | [Info](#)

Specify the platform version on which to run your service.

LATEST ▼

► **Troubleshooting configuration - recommended, new**

4. Networking > Choose **subnets** and **security group(s)** for your service:

- Choose Security group from existing security group: **ECS security group (netreach-ecs-sg)**

▼ **Networking**

VPC | [Info](#)

Select a VPC to use for your Amazon ECS resources.

vpc-0c3e592040884cf1e
default ▼

[Create a new VPC](#)

Subnets

Choose the subnets within the VPC that the task scheduler should consider for placement.

Choose subnets ▼

[Clear current selection](#)

subnet-0533639fc68bb80ad
us-west-1b 172.31.16.0/20

subnet-0d6ea39fc3ffb8b8a
us-west-1a 172.31.0.0/20

Security group | [Info](#)

Choose an existing security group or create a new security group.

☒ Use an existing security group

☐ Create a new security group

Security group name

Choose an existing security group.

Choose security groups ▼

sg-085f8a2c0abeab392
netreach-ecs-sg

Public IP | [Info](#)

Choose whether to auto-assign a public IP to the task's elastic network interface (ENI).

☒ Turned on

5. Load balancing > select Use load balancing checkbox

- Application Load Balancer: *use an existing load balancer or create a new one if not exist*

▼ Load balancing - optional

Configure load balancing using Amazon Elastic Load Balancing to distribute traffic evenly across the healthy tasks in your service.

☒ Use load balancing

VPC
The VPC for your load balancing resources must be the same as the VPC for your service with awsvpc.

vpc-0c3e592040884cf1e

Load balancer type | [Info](#)
Specify the load balancer type to distribute incoming traffic across the tasks running in your service.

☒ **Application Load Balancer**
An Application Load Balancer makes routing decisions at the application layer (HTTP/HTTPS), supports path-based routing, and can route requests to one or more ports.

☐ **Network Load Balancer**
A Network Load Balancer makes routing decisions at the transport layer (TCP/UDP).

Container
The container and port to load balance the incoming traffic to

NetReachContainer 3000:3000

Host port:Container port

Application Load Balancer
Specify whether to create a new load balancer or choose an existing one.

☐ Create a new load balancer
☒ Use an existing load balancer

Load balancer
Choose an existing load balancer to distribute traffic. View existing load balancers and create new one in [EC2 Console](#).

netreach-lbc
netreach-lbc-212816422.us-west-1.elb.amazonaws.com

internet-facing

- Listener: *use an existing listener or create a new one if not exist*

Listener | [Info](#)
Specify the port and protocol that the load balancer will listen for connection requests on.

☐ Create new listener
☒ Use an existing listener

Listener

HTTPS:443

Listener rules for 443:HTTPS (1)
Traffic received by the listener is routed according to its rules. Rules are evaluated in priority order, from the lowest value to the highest value. The default rule is evaluated last.

< 1 >

Priority	Rule path	Target group
default	/	netreach-ecs-tg

- Target group: *use an existing target group or create a new one if not exist*

Target group [Info](#)

Specify whether to create a new target group or choose an existing one that the load balancer will use to route requests to the tasks in your service.

- ☐ Create new target group
- ☒ Use an existing target group

Target group name

netreach-ecs-tg

Health check path

/login

Health check protocol [Info](#)

HTTP

5. Click create button to create a service.

If NetReach successfully deploy, you will see the status is active, task is running and target health is healthy.


netreachapp-service [Info](#)


Last updated
October 1, 2025, 13:40 (UTC-7:00)

[Delete service](#)


[Update service](#)

Service overview [Info](#)

Status  Active

Tasks (1 Desired)  0 Pending | 1 Running

Task definition: revision [netreachapp-task-definition:2](#)

Deployment status  Rollback failed

Health and metrics

Tasks

Logs

Deployments


Events


Configuration and networking


Service auto scaling

Tags

Status [Info](#)

Service name  netreachapp-service

Service ARN  arn:aws:ecs:us-west-1:654654326454:service/NetReachCluster/netreachapp-service

Deployments current state  1 Completed task

Created at
October 1, 2025, 11:30 (UTC-7:00)

Health check grace period
0 seconds

▼ Load balancer health

Load balancer 	Load balancer type	Container name:port	Listeners 	Target group 	Target health
netreach-lbc	Application Load Balancer	NetReachContainer:3000	HTTPS:443	netreach-ecs-tg Details	 1 Healthy  0 Unhealthy

Step 9: Test

1. visit <https://netreachapp.yourdomain.com>
 - SSL cert should show valid
 - HTTP should redirect to HTTPS
2. ALB distributes load across ECS tasks.
3. Default NetReach Username/Password: ***netreach/netreach***

