NetReach on Amazon ECS

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 an Amazon EFS File System

1. Go to **Amazon EFS** in the AWS Management Console.

2. Click **"Create file system"**.

3. Choose **VPC** that your ECS tasks will run in

4. Click **"Next"** until you reach **"Create"**.

Important:

- This creates an EFS, but it's not accessible yet, you need mount targets and security groups.

Step 2: Configure Security Group for EFS

1. Go to the **EFS → Network** section.

2. Confirm that **mount targets** exist in each AZ (Availability Zones) where your ECS tasks run.

3. Attach a **security group** to EFS that allows **NFS traffic (TCP 2049)**.

   o Choose/create security group (*e.g. netreach-efs-sg*)

      ▪ Inbound rule:

         • **Type:** NFS

         • **Port:** 2049

         • **Source:** The **security group of your ECS tasks** (not 0.0.0.0/0 for security).

      ▪ Outbound: Allow all traffic (default is fine).

4. In the ECS task's security group, allow **outbound traffic** on port 2049 to EFS's security group.

Step 3: Create an ECS Cluster

1. Go to Amazon ECS → Clusters

2. Click "Create Cluster"

3. Choose "Networking only (Fargate)"

4. Name your cluster and create it.

Step 4: Create a Task Definition with EFS Volume

1. Go to Task Definitions → Create new Task Definition.

   o Specify a unique task definition family name: e.g. *netreachapp-task-definition*

2. Under Infrastructure requirements

   o Select **AWS Fargate** launch type.

   o Fill out task details

      ▪ Task role with *AmazonElasticFileSystemClientFullAccess* permission

      ▪ Task execution role with *AmazonECSTaskExecutionRolePolicy* and *SecretsManagerReadWrite* permissions

3. Under Container details:

   - Name container

   - For **Image URI**, enter your full Azure registry (ACR) image:

     - e.g. **netreachacr.azurecr.io/netreach-image:<tag>**

       - **<tag>**: the specific version or tag of the image (e.g., latest, v1.00).

   - For Private registry:

     - Toggle "Private registry" ON

     - Paste the full ARN of the secret you created, on **AWS Secret Manager**, to access Azure registry (ACR)

   - Port mappings:

     - Container port: 3000 (the port NetReach app listens on).

     - App Protocol: HTTP

4. 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/

5. Click "**Create**"

Step 5: Create a Load Balancer

1. Go to the **Load Balancer Console**

2. Navigate to **EC2 > Load Balancers**

3. Click **"Create Load Balancer"**

4. Choose **"Application Load Balancer"**

5. Configure Load Balancer:

    o   Name: e.g. netreach-alb

    o   Scheme: Internet-facing *(for public access)*

    o   IP address type: IPv4

    o   Listeners: Start with **port 80** (HTTP). You can add **port 443** (HTTPS) later.

6. Select Availability Zones

    o   Choose the **VPC** where you ECS service will run

    o   Select public subnets in different AZ

7. Configure Security Group

    o   Choose/create a security group (*e.g. netreach-alb-sg*)

    o   Rules should allow:

        1. **Inbound HTTP (port 80)** and **HTTPS (port 443)** from anywhere (or restrict to your IP)

        2. **Outbound:** Allow all (default)

8. Configure routing

    o   You'll be prompted to **create a target group**

    o   Choose:

        1. Target type: IP mode (for ECS Fargate)

        2. Name: e.g. netreach-ecs-tg

        3. Protocol: HTTP

        4. Port: 3000 (this should match your ECS container port; Netreach uses port 3000)

        5. Health check path: /login

    Note: NetReach does not provide a healthy endpoint; use"/login" to get a healthy check.

9. Review and click "**Create Load Balancer**"

Step 6: Add HTTPS Listener (SSL/TLS)

After the ALB is created, add a **443 listener**:

To add HTTPS listener:

1. Go to **EC2 > Load Balancers**

2. Select your **ALB**

3. Under **Listeners** tab, click **"Add listener"**

4. Choose:

   o **Protocol:** HTTPS

   o **Port:** 443

   o **Default action:** Forward to your **target group**

5. Under **SSL certificate**:

   o Choose an existing cert from **AWS Certificate Manager (ACM)**

   o If none exists, go to **ACM**, request a certificate, and validate your domain

6. Redirect all HTTP traffic to HTTPS:

   o Edit rules:

      1. Add a rule to **redirect to port 443**

Step 7: Create a Service

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

   • **Launch type:** Fargate

   • **Task Definition:** The one you just created on **Step 4**

   • **Service name:** e.g. netreach-service

   • **Number of tasks:** e.g. 1

3. In **Networking** > Choose **subnets** and + ECS task **security group** *(e.g. netreach-ecs-sg)*
4. In **Load balancing:**

- Enable **Application Load Balancer**

- Select the ALB you've created on **Step 5**

- **Listener port:** Select 443 if you already created the HTTPS listener

- **Target group:** Create a new target group for your service (or reuse an existing one)

    o **Target type:** ip (for Fargate)

    o **Port:** 3000 (this should match your NetReach container port)

5. Click **Create Service**

Step 8: Test

1. Visit https://netreachapp.yourdomain.com

    o SSL cert should show valid

    o HTTP should redirect to HTTPS

2. ALB distributes load across ECS tasks.

Security Group Tips

Use 3 main security groups:

1. ALB Security Group **(netreach-alb-sg)**
   Attached to the ALB.

2. ECS Task Security Group **(netreach-ecs-sg)**
   Attached to ECS tasks.

3. EFS Security Group **(netreach-efs-sg)**
   Attached to EFS mount targets.

- ECS Task Security Group must allow **outbound** to EFS

- EFS Security Group must allow **inbound NFS (port 2049)** from ECS Task SG

- ALB's security group must allow **inbound to port 80 and 443**, and ECS Task SG must allow traffic from ALB SG