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>***

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

Step 2: Create ECS task role and task execution role

1. Go to ***IAM*** > ***Roles***

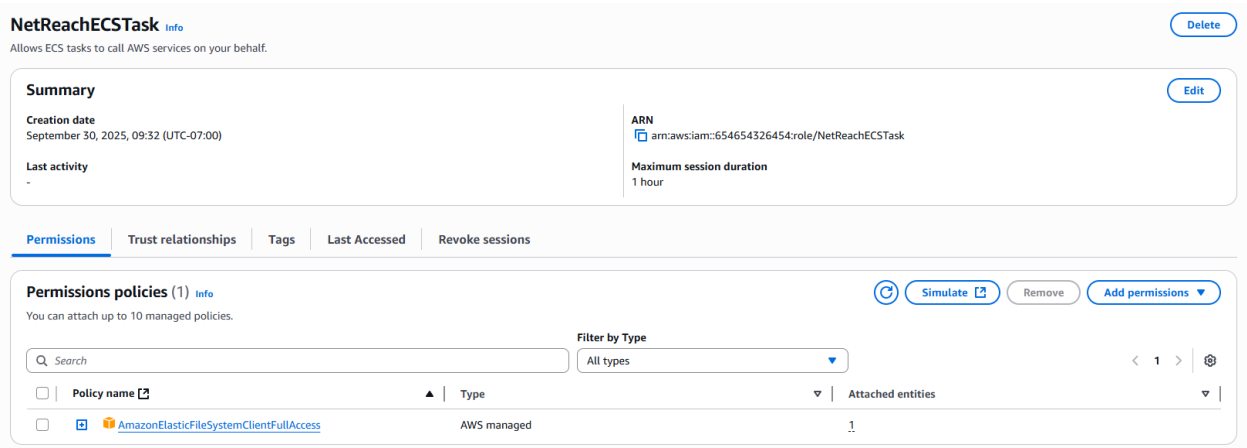
    1. Create task role and task execution role with the following policies:

        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***

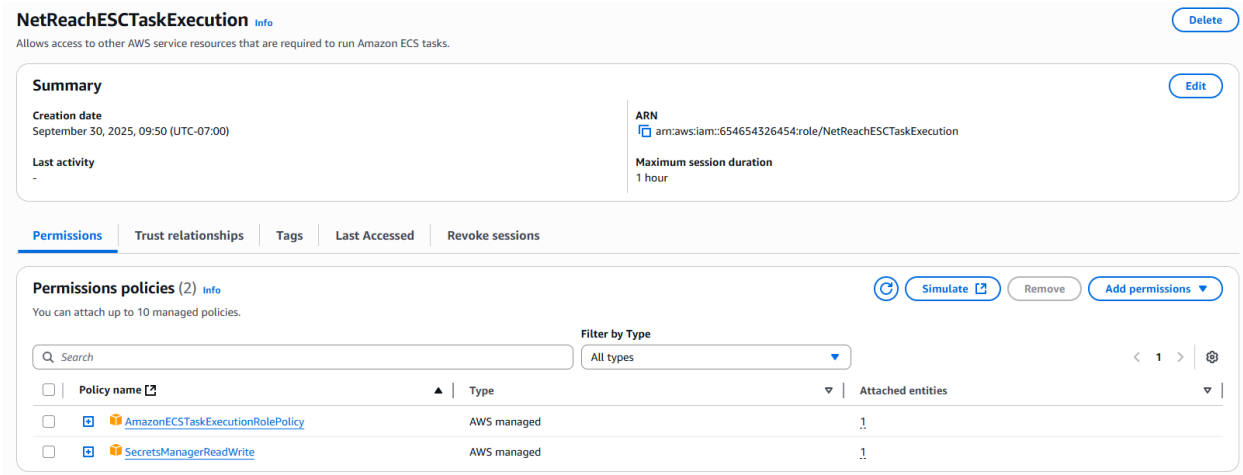


For ECS Task Execution role

- 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)



Step 3: Create Security Group

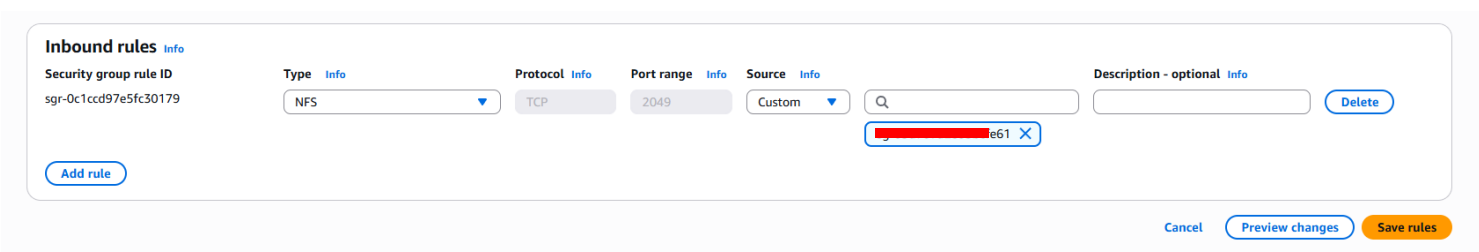
In this section we'll create 3 main security groups:

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

1. Go to ***VPC*** > ***Security group***

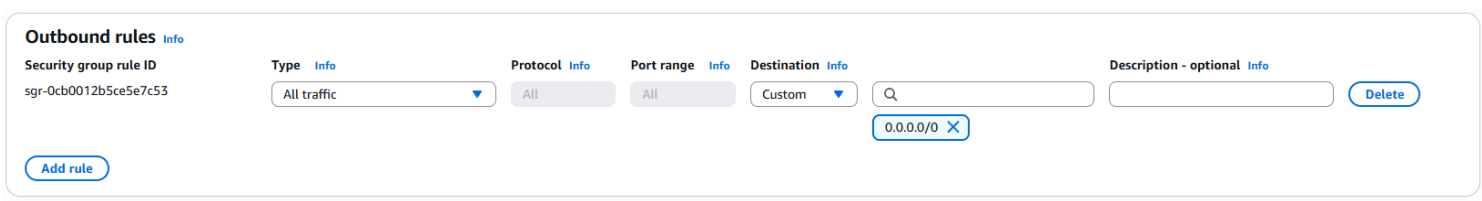
2. **For *EFS security group* (netreach-efs-sg) Inbound rule:**

   - Type: ***NFS***
   - Port: ***2049***
   - Source: ***The security group of your ECS (netreach-ecs-sg)***



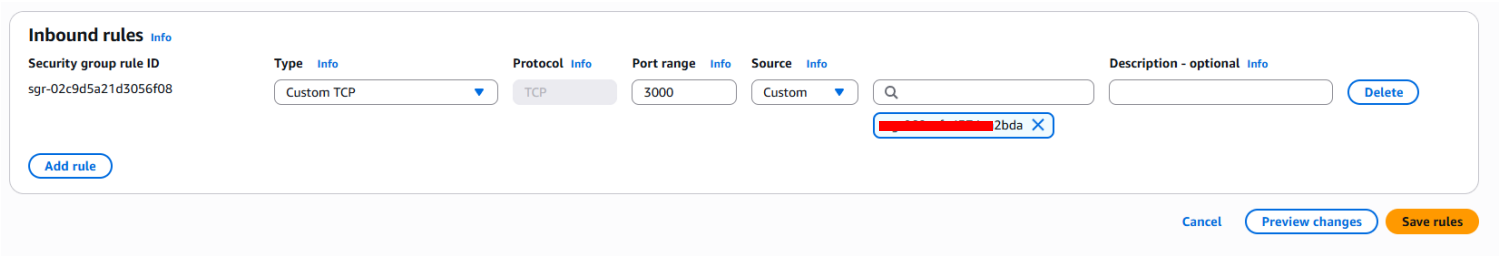
For *EFS security group* (netreach-efs-sg) Outbound rule:

- Allow all traffic (default)



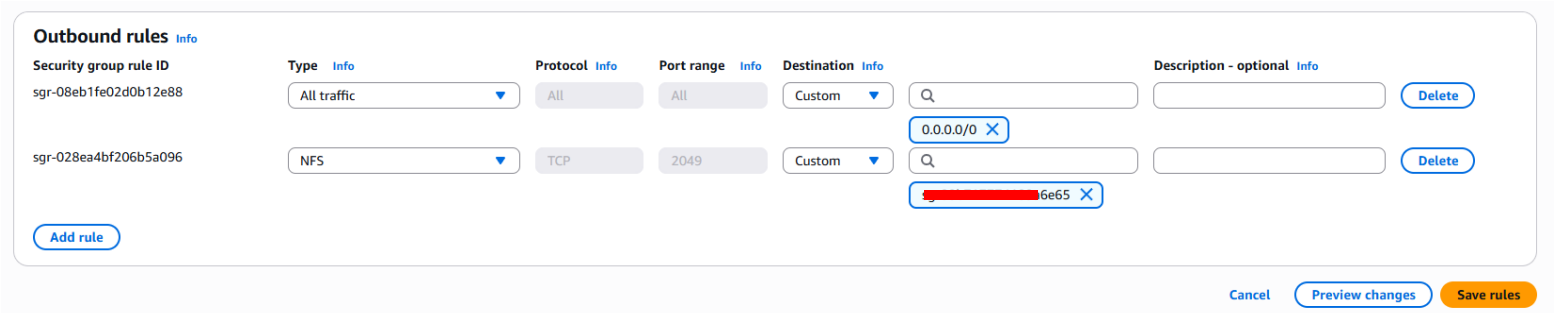
3. **For ECS security group (netreach-ecs-sg) Inbound rule:**

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



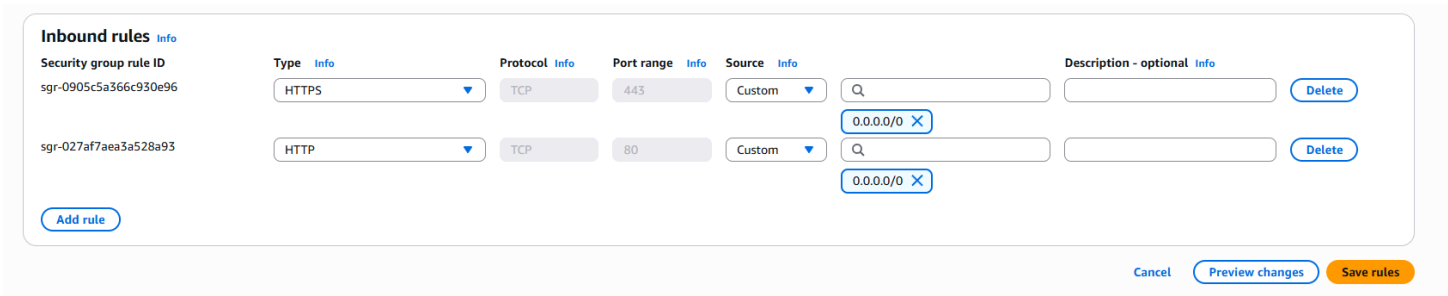
For ECS security group (netreach-ecs-sg) Outbound rule:

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



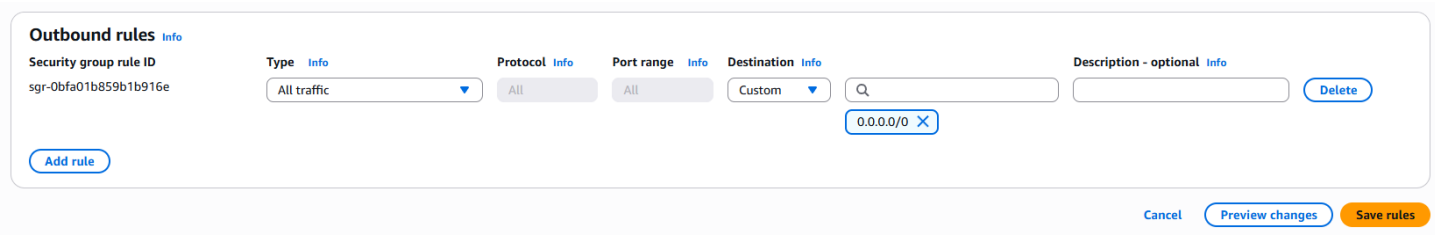
4. **For ALB security group (netreach-alb-sg) Inbound rule:**

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



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

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

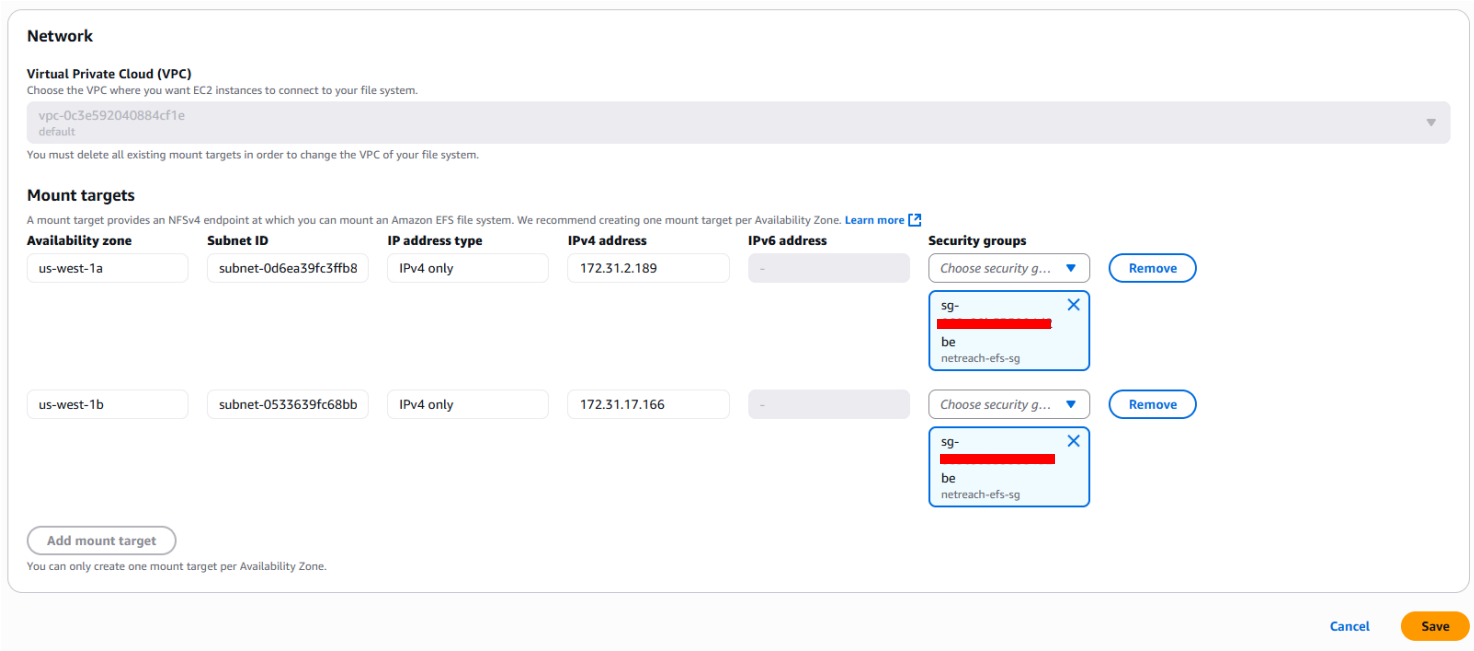


Step 4: Create an Amazon EFS File System

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)***.



Step 5: Create an ECS Cluster

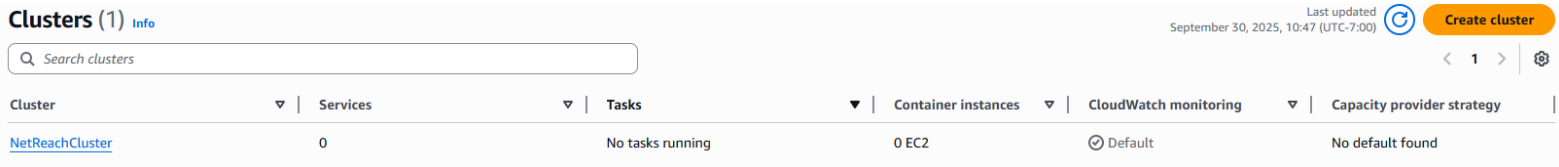
1. Go to ***Amazon ECS*** > ***Clusters***

2. Click Create Cluster

3. Name your Cluster

4. Under ***Infrastructure*** section check ***AWS Fargate (serverless)***

5 Click Create button



Step 6: Create a Task Definition with EFS Volume

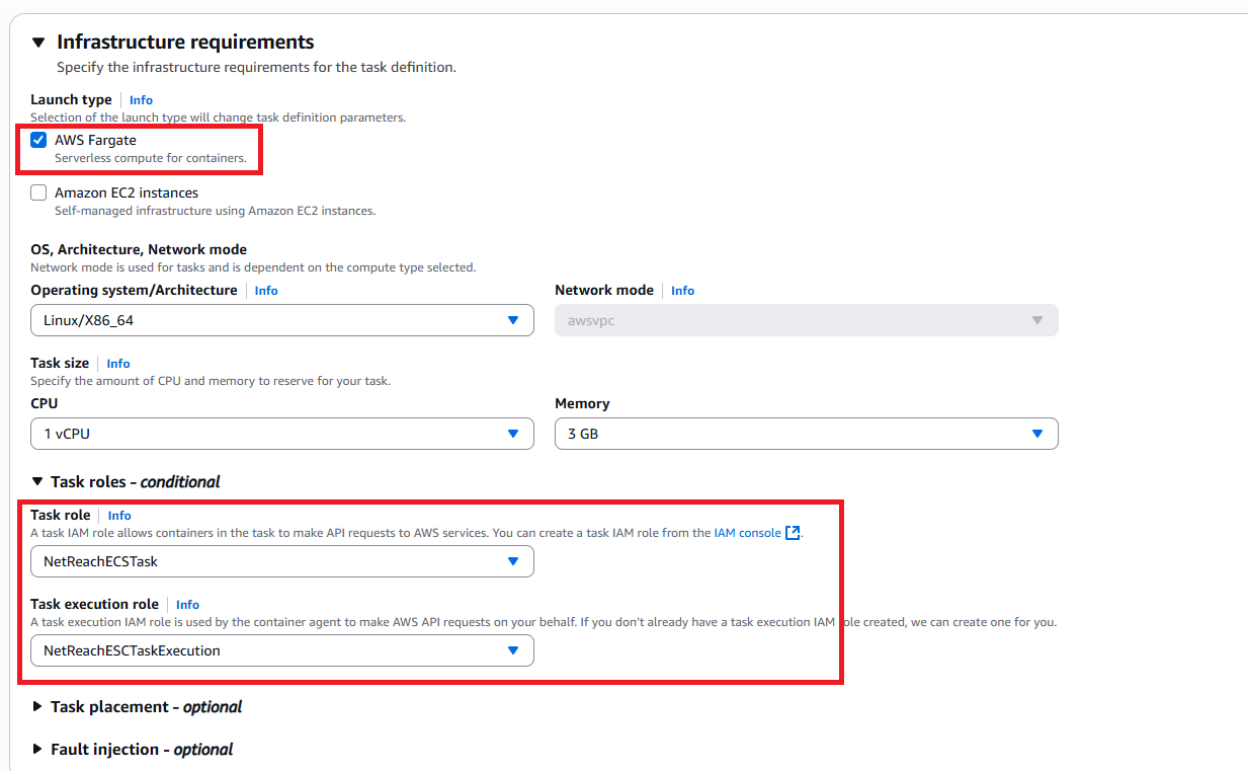
1. Go to ***Amazon ECS*** > ***Tasks definitions***

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***



5. Under ***Container*** – Name your container e.g., *NetReachContainer*

6. ***Image URI***, enter your full Azure registry (ACR) images:

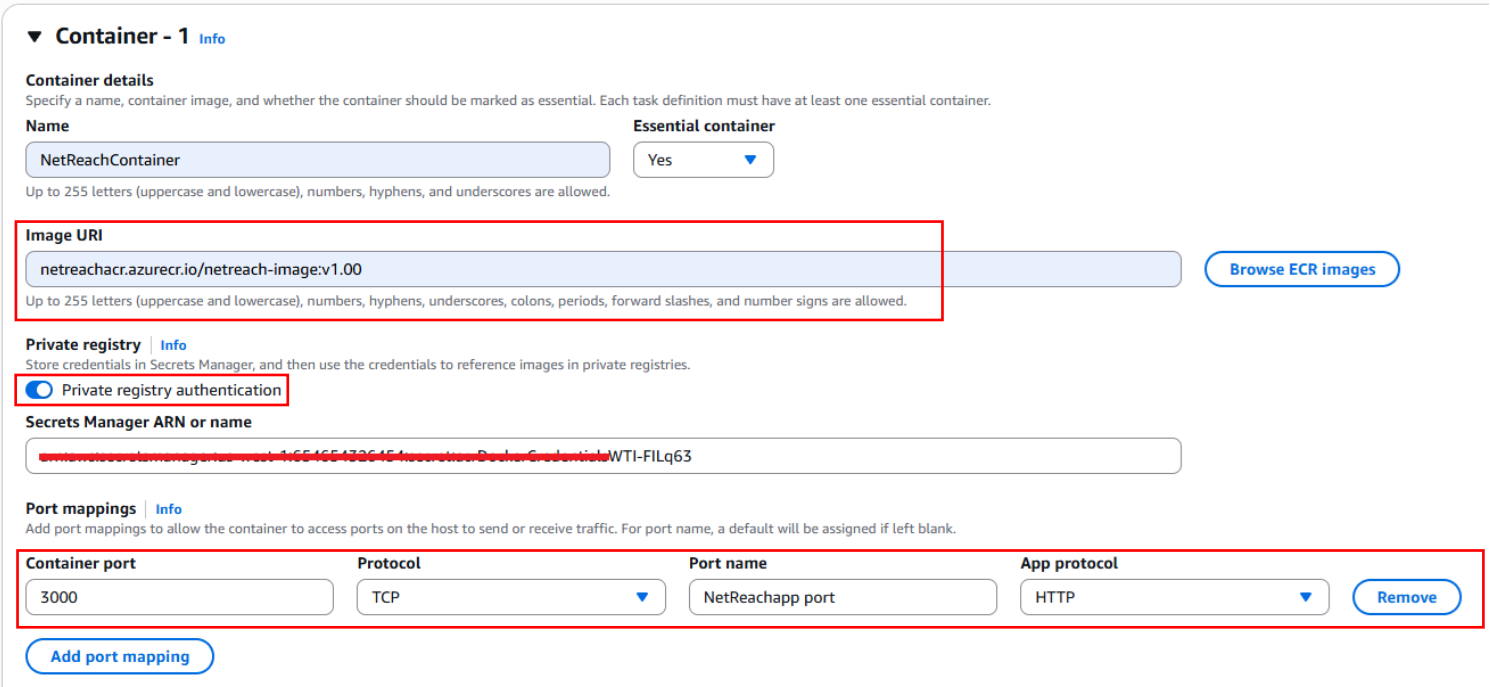
- ***netreachacr.azurecr.io/netreach-image*:<tag>**
- **<tag>**: the specific version or tag of the image (e.g., latest, v1.00)

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)

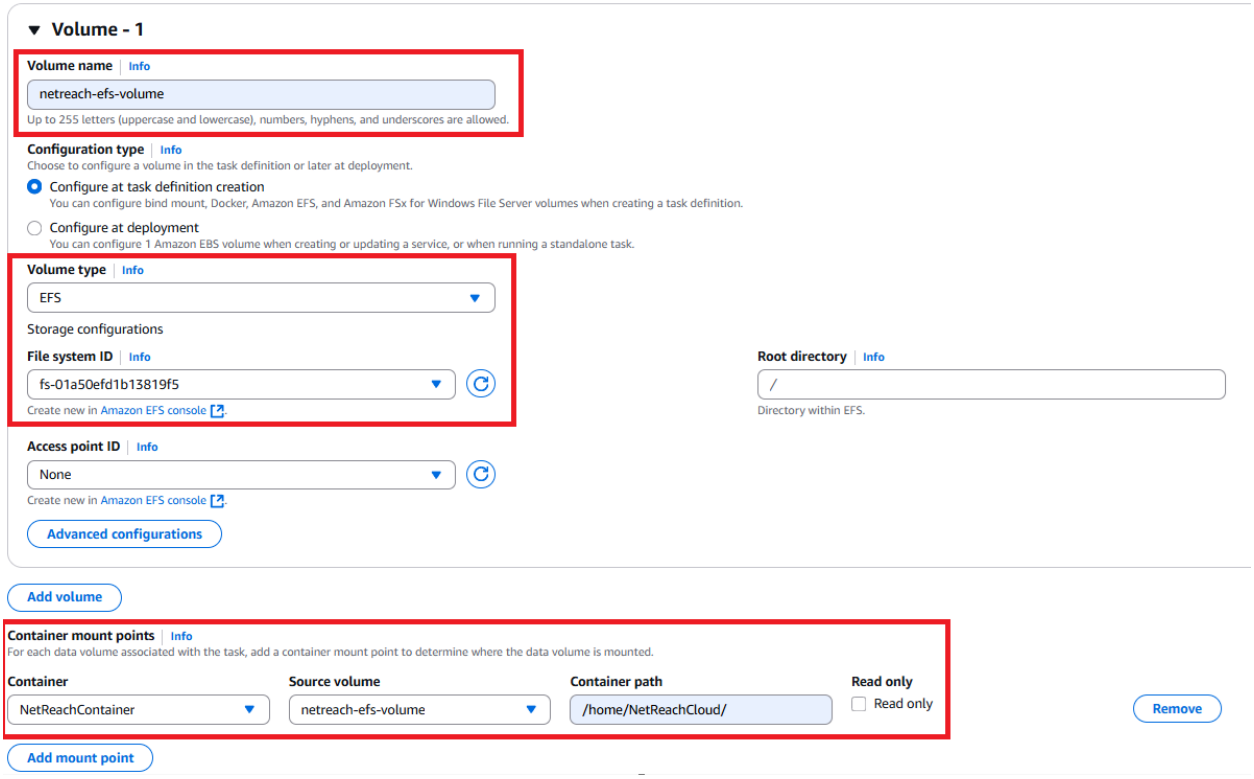
8. Port mappings:

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



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/***



10. Click Create button.

Step 7: Create a Load Balancer

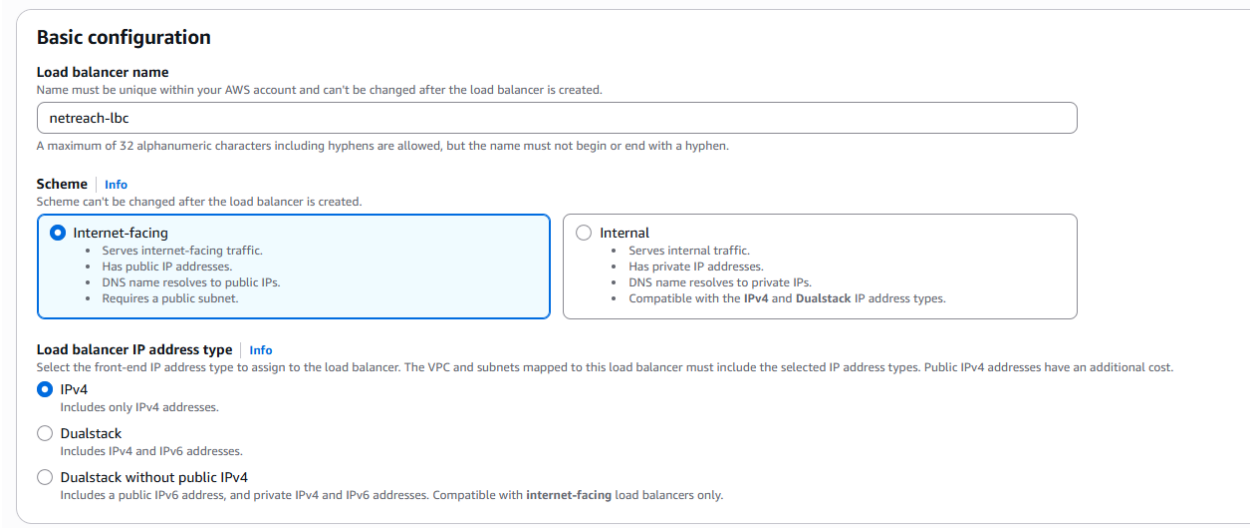
1. Go to the ***Load Balance*** > ***EC2 features***

2. Click Create load balance

3. Choose "***Application Load Balancer***"

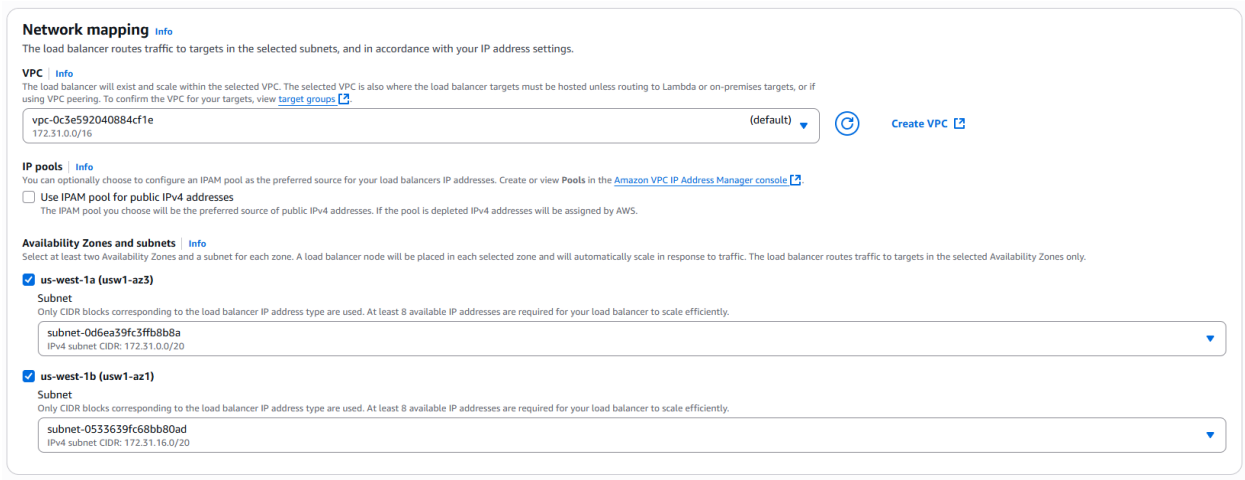
4. Under Basic configuration section:

- Name: e.g. ***netreach-lbc***
- Scheme: ***Internet-facing*** (for public access)
- Load balancer IP Address type: ***IPv4***



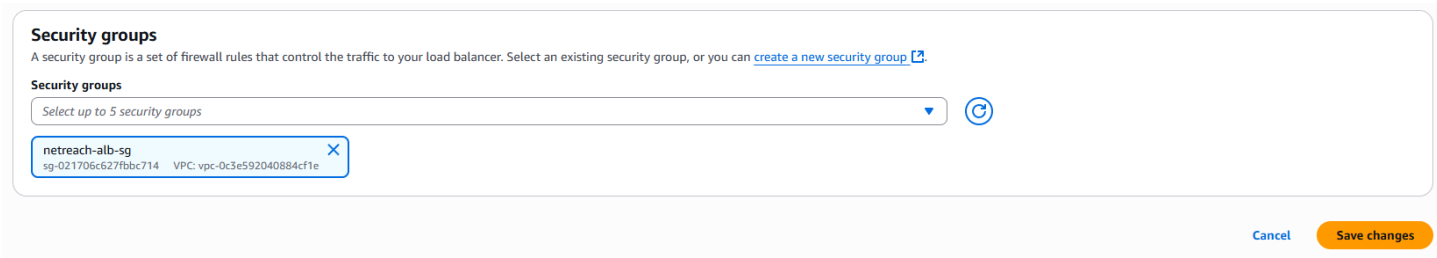
5. Under Network mapping section:

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



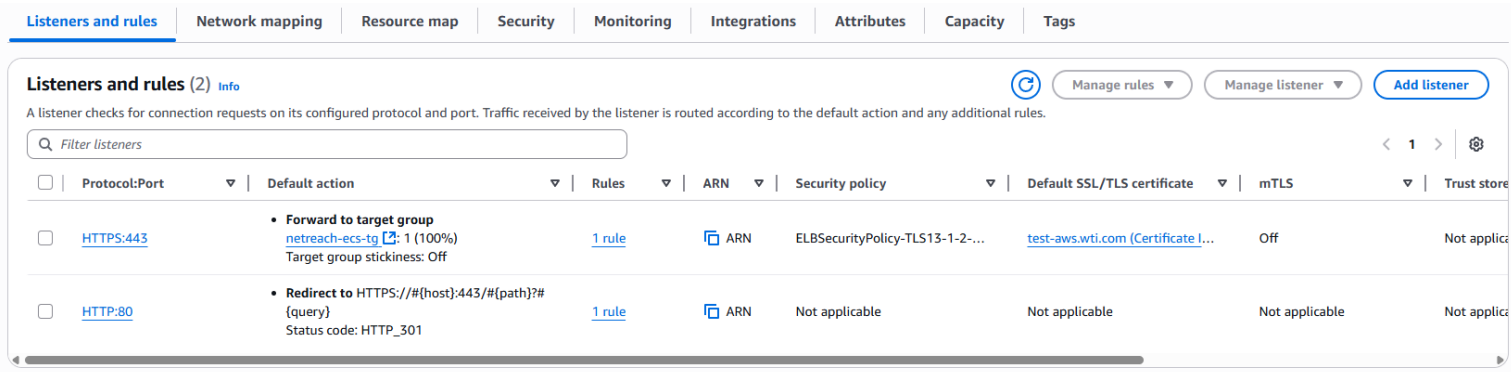
6. Under Security group section:

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



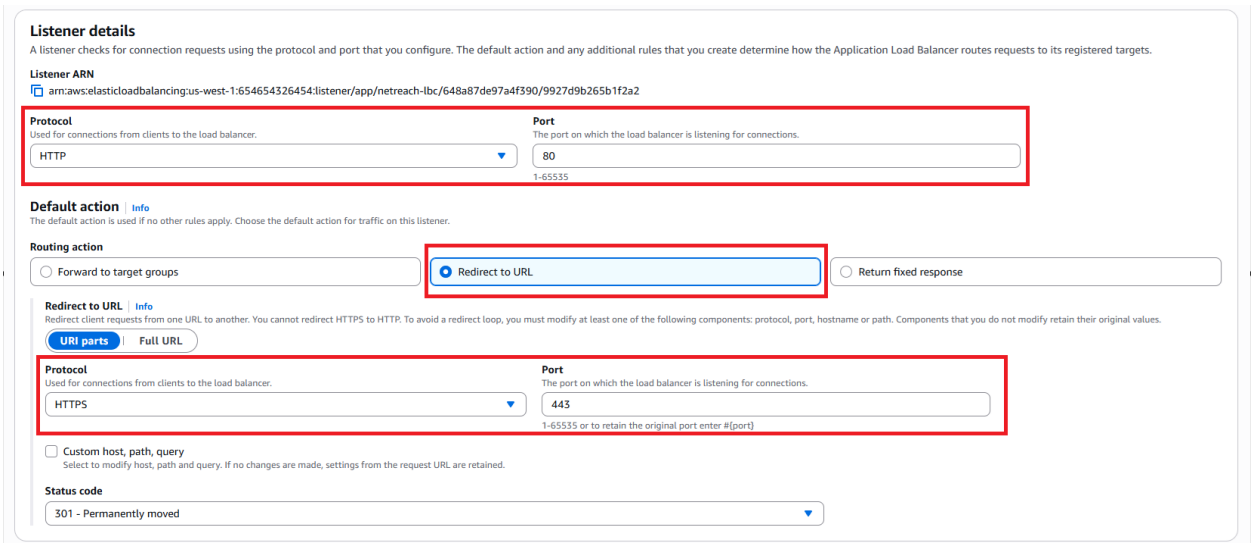
7. Under Listeners and routing section:

Overview Listeners and rule for HTTP and HTTPS



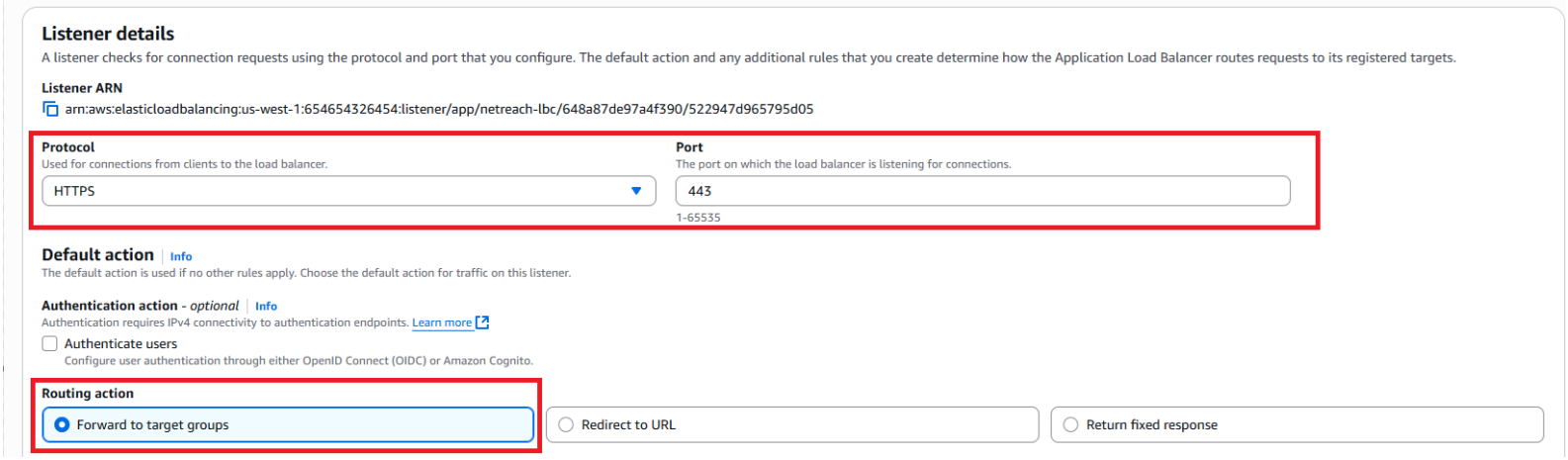
For Listeners: Add port 80 (HTTP)

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



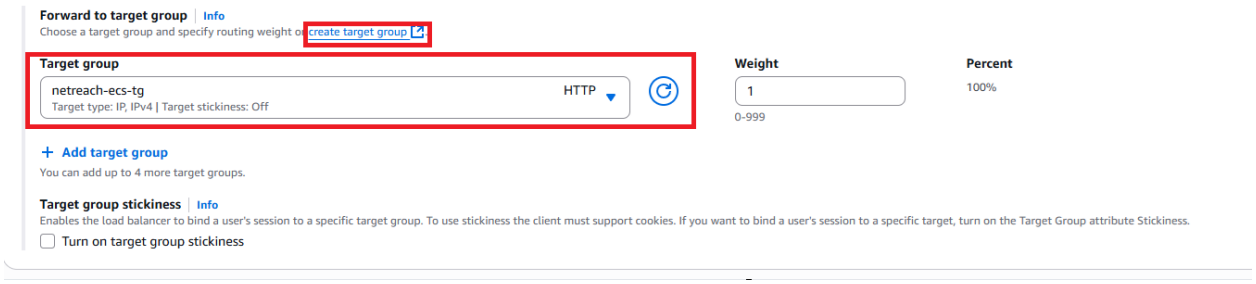
For Listeners: Add port 443 (HTTPS).

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

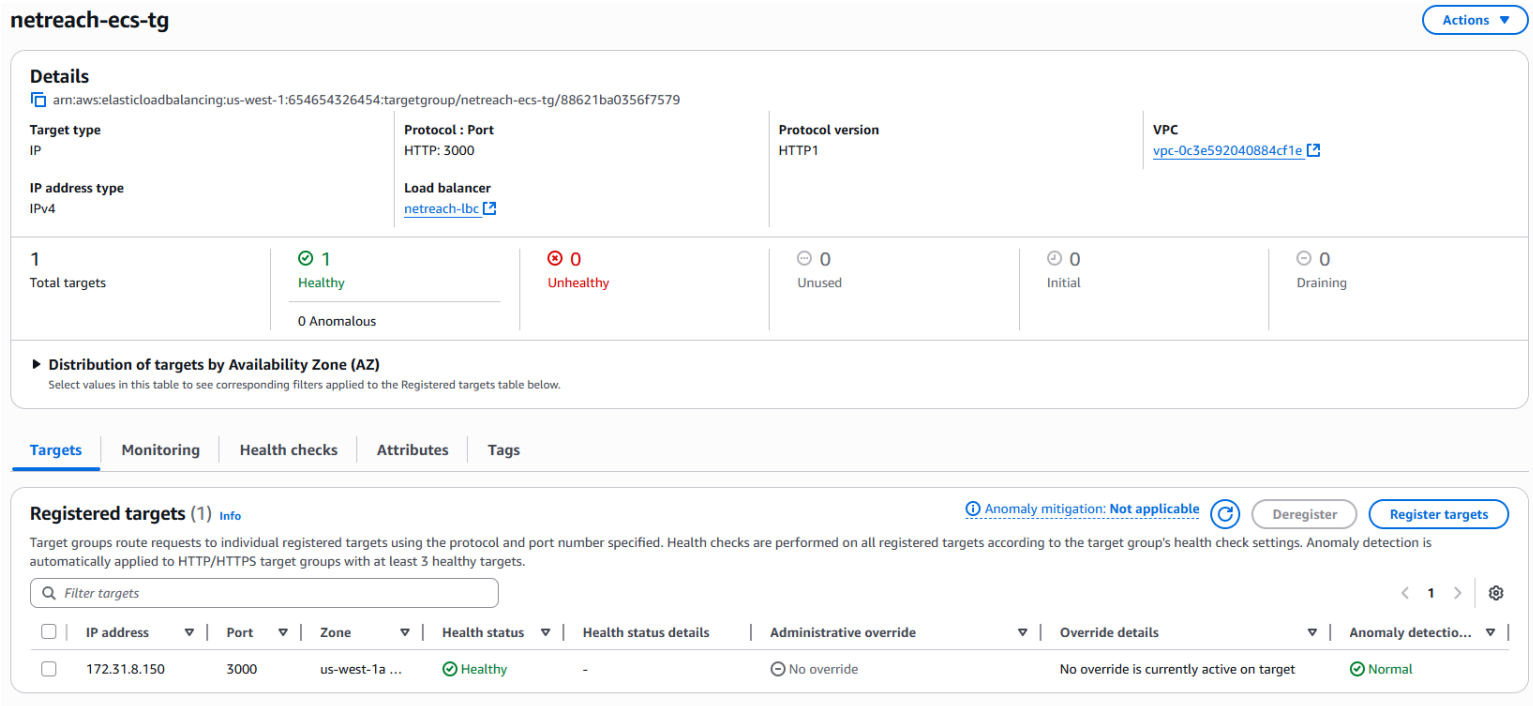


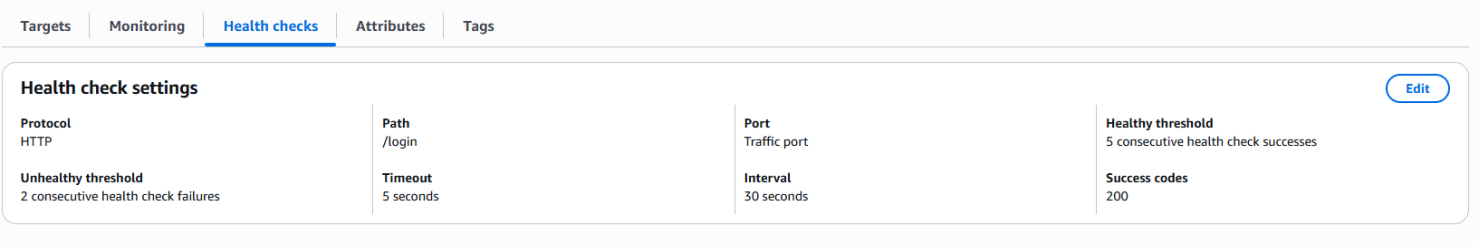
Create a target group.

- Click create target group link.



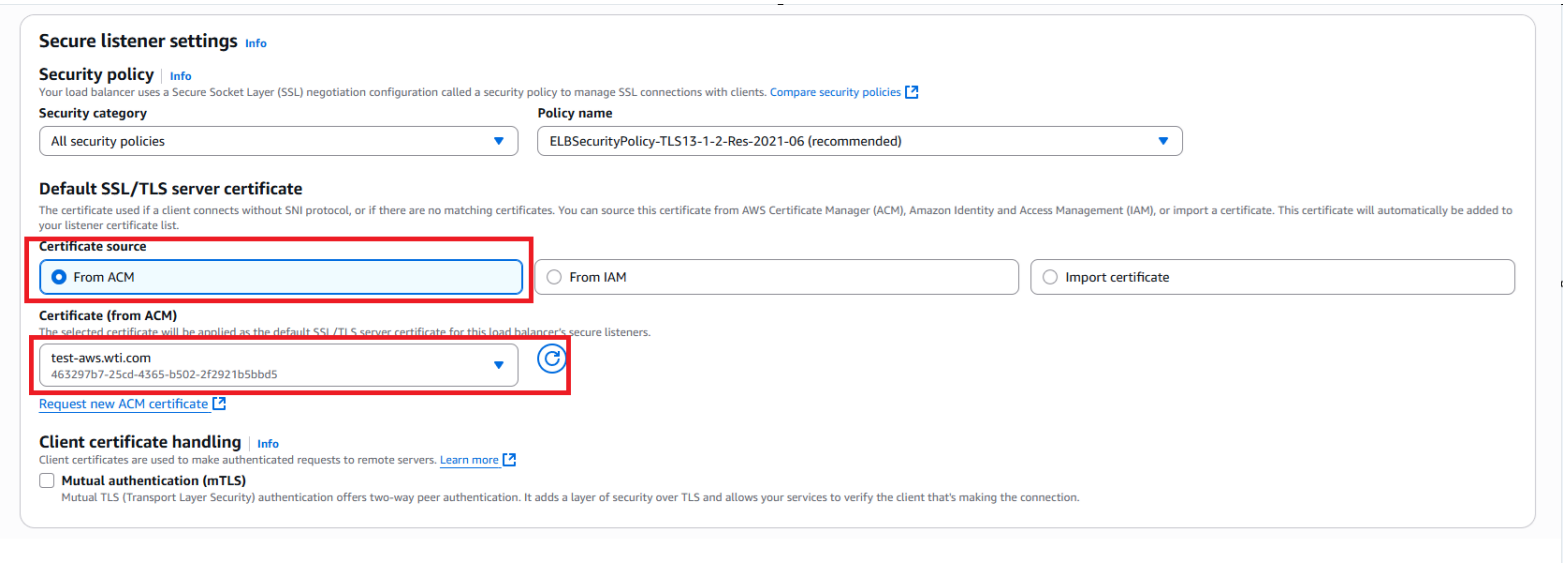
1. Target type: ***IP mode (for ECS Fargate)***
2. Target Group Name: e.g. ***netreach-ecs-tg***
3. Protocol: ***HTTP***
4. Port: ***3000*** (this should match your ECS container port; NetReach uses port 3000)
5. Health check path: ***/login***





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.

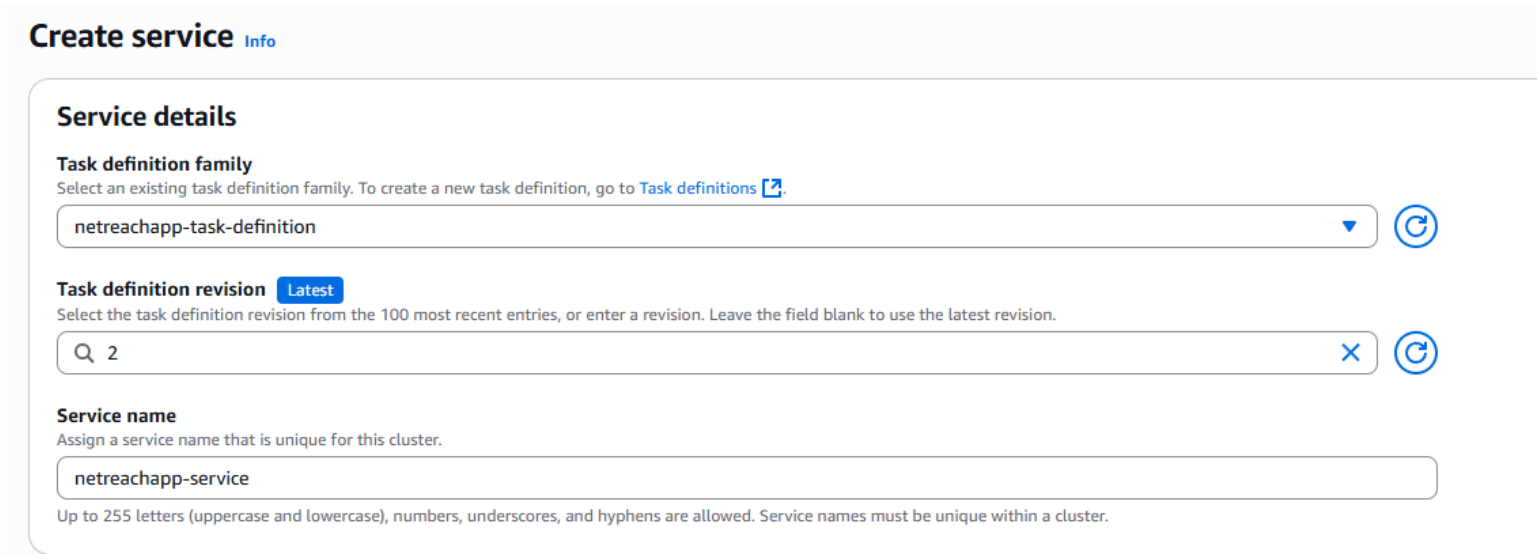


Step 8: Create a Service

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

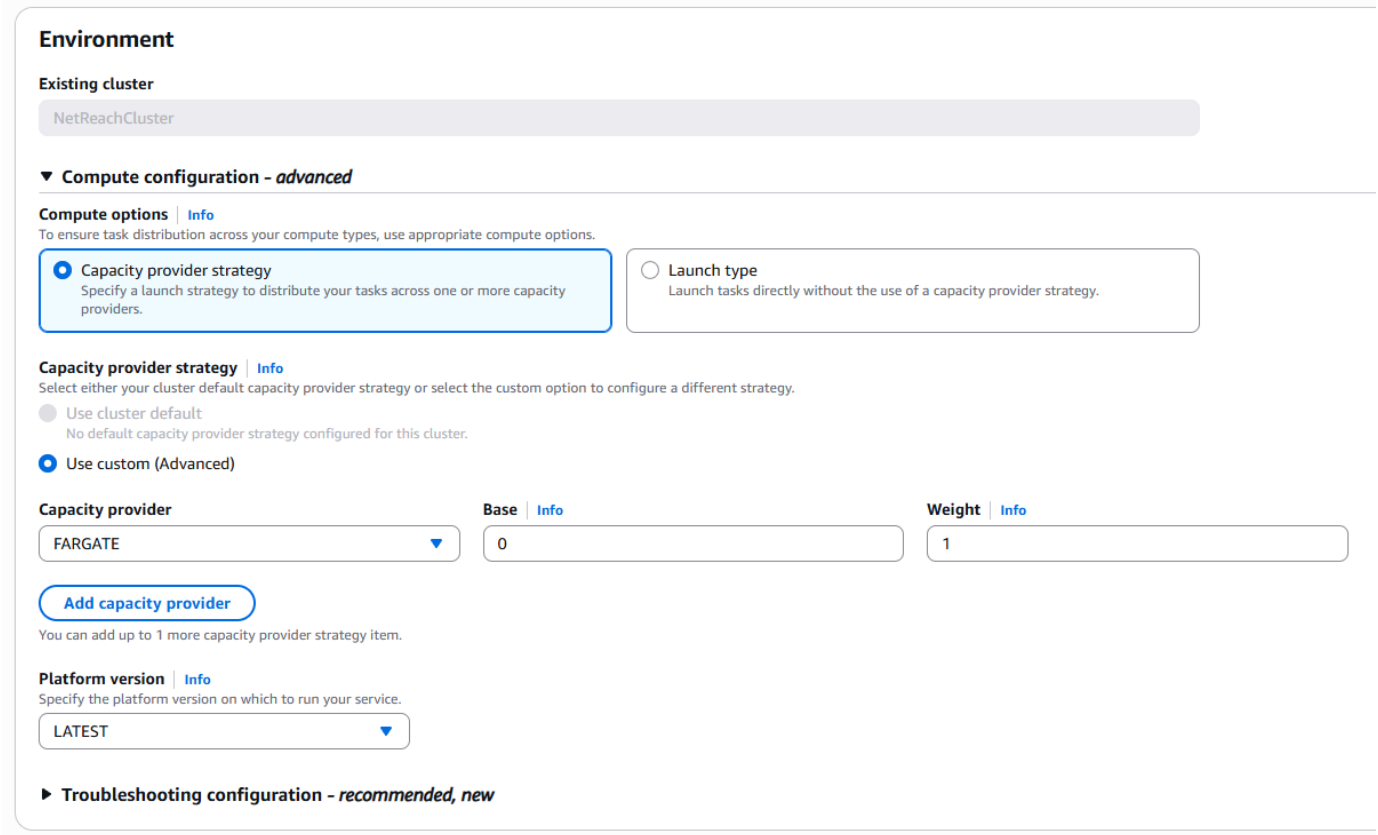
2. Service details

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



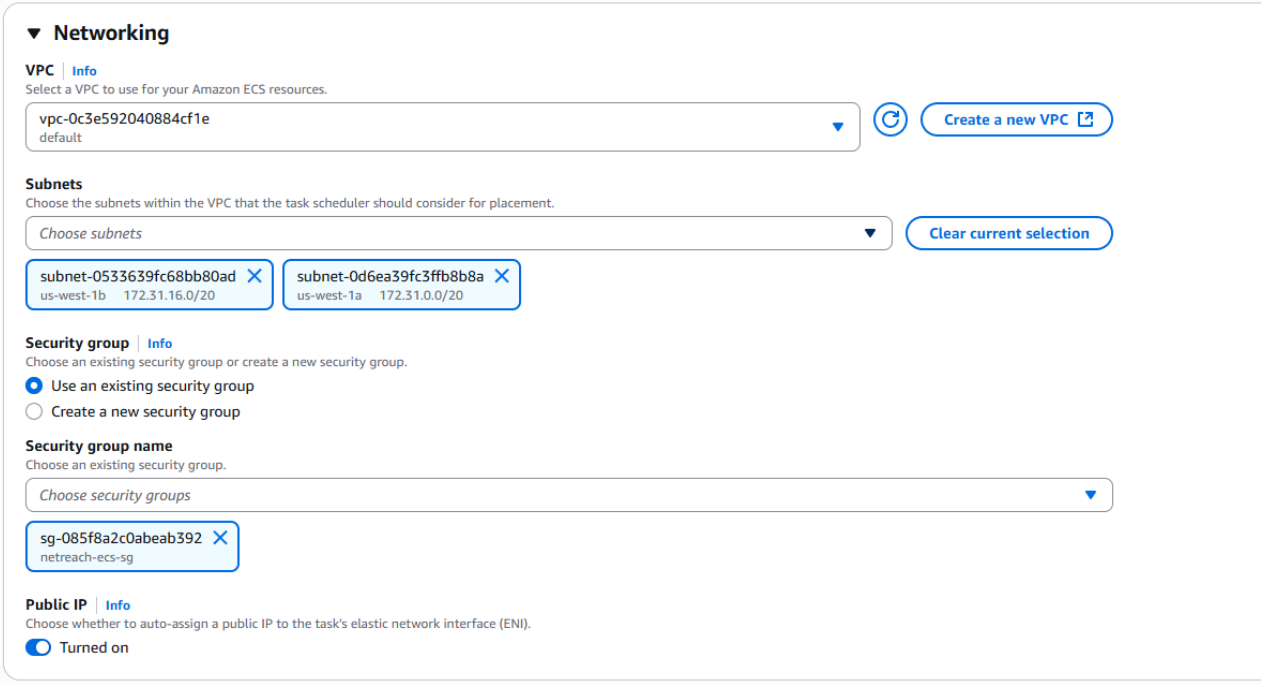
3. Environment > Compute configuration

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



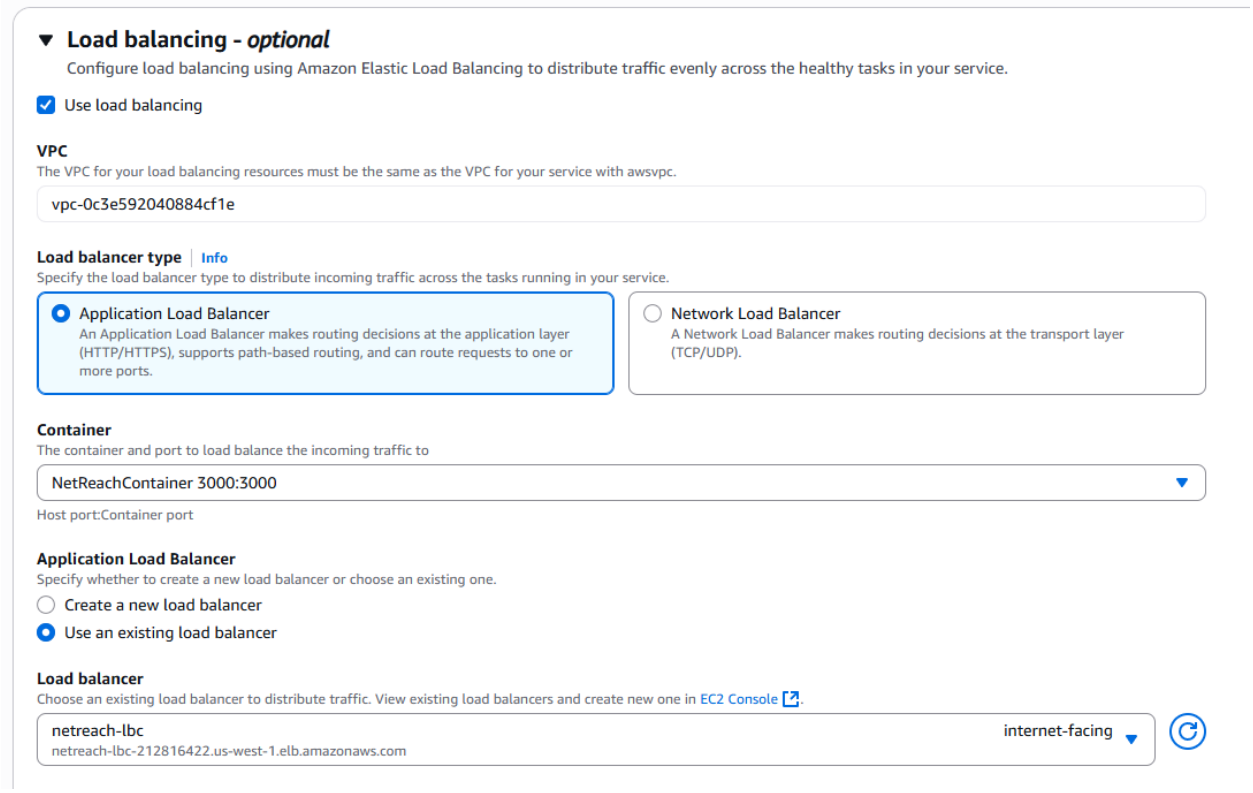
4. Networking > Choose ***subnets*** and ***security group(s)*** for your service:

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

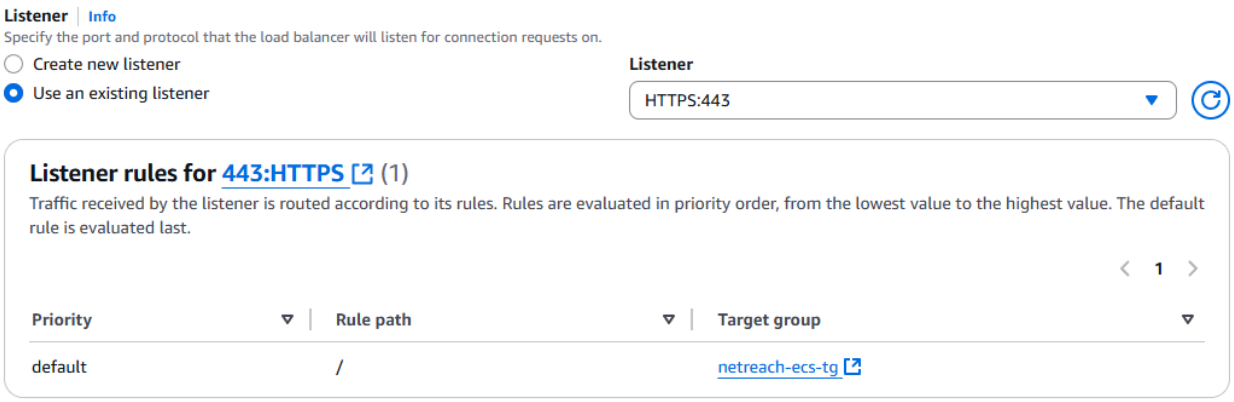


5. Load balancing > select Use load balancing checkbox

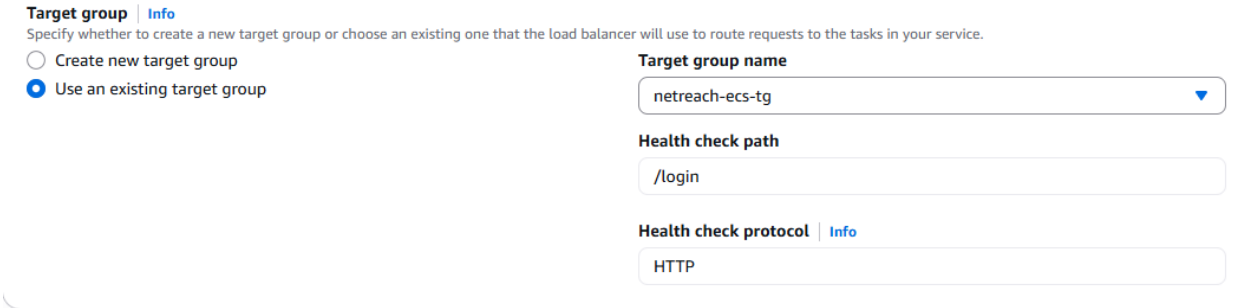
- Application Load Balancer: ***use an existing load balancer or create a new one if not exist***



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

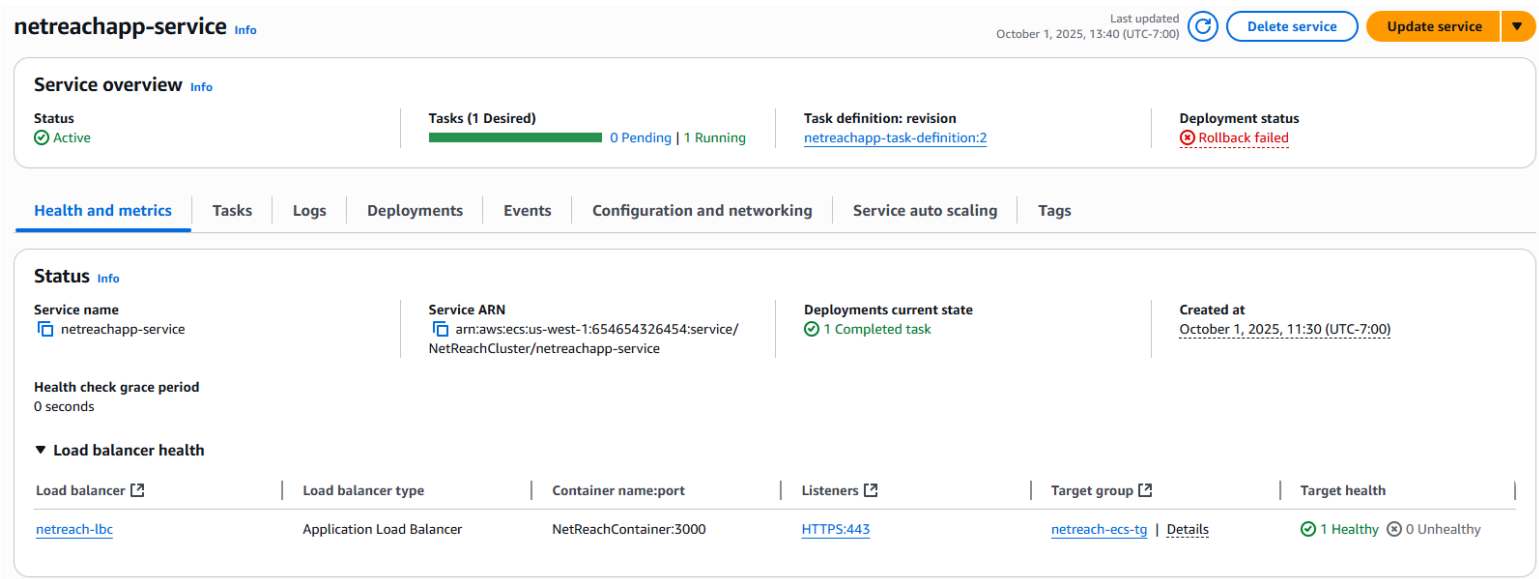


- Target group: ***use an existing target group or create a new one if not exist***



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.



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***