Part 1: EC2 with ELB and ASG

Objective: Learn how to create a scalable and highly available web application environment using Amazon EC2 instances, ELB, and ASG.

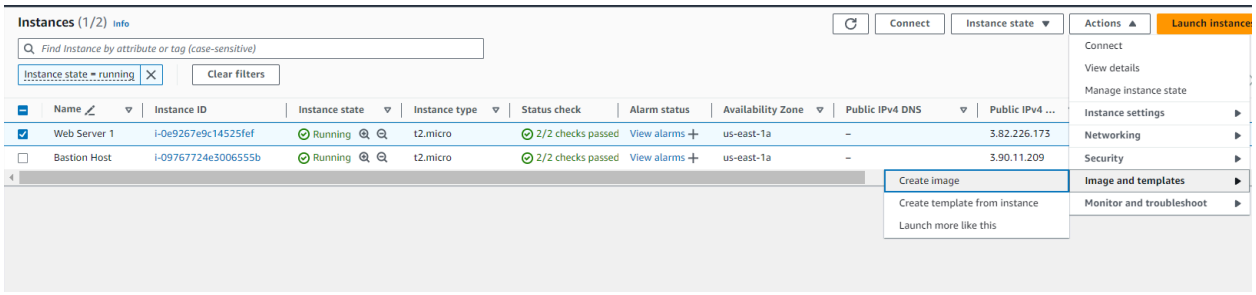
Approach:

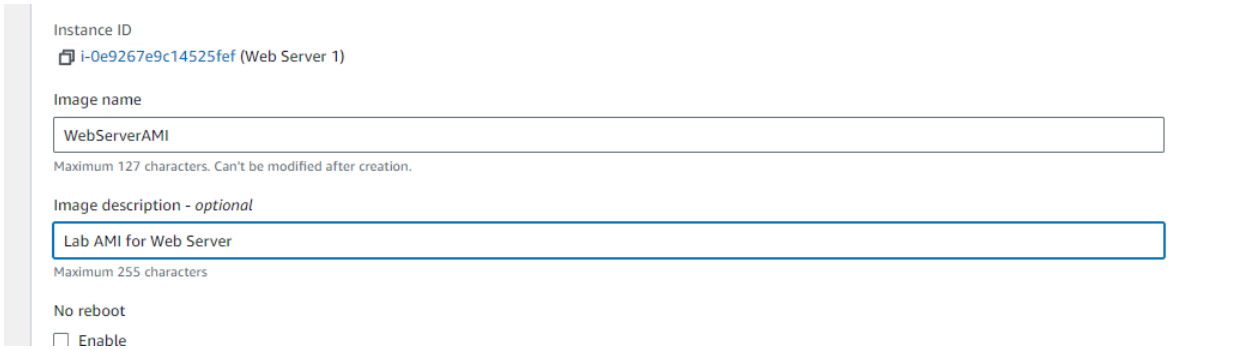
1. Launch EC2 Instances: Start by launching two or more EC2 instances. These instances will run a simple web application (e.g., a "Hello World" page or any basic web service).
2. Configure Load Balancer: Set up an Elastic Load Balancer (ELB) to distribute incoming web traffic across your EC2 instances. This step ensures high availability and fault tolerance.
3. Set Up Auto Scaling Group (ASG): Create an ASG that uses the launched EC2 instances. Configure ASG policies to automatically scale the number of instances up or down based on criteria like CPU usage or network traffic.
4. Test Your Setup: Simulate traffic to test the scaling policies and the load balancer. Observe how ASG adds or removes instances and how ELB distributes traffic.
5. Verify Website Functionality: Ensure that the website hosted on EC2 instances remains accessible and functional during scaling operations.

Goal: By the end of this lab, students will have a hands-on understanding of setting up a load-balanced and auto-scaled web application using AWS services.

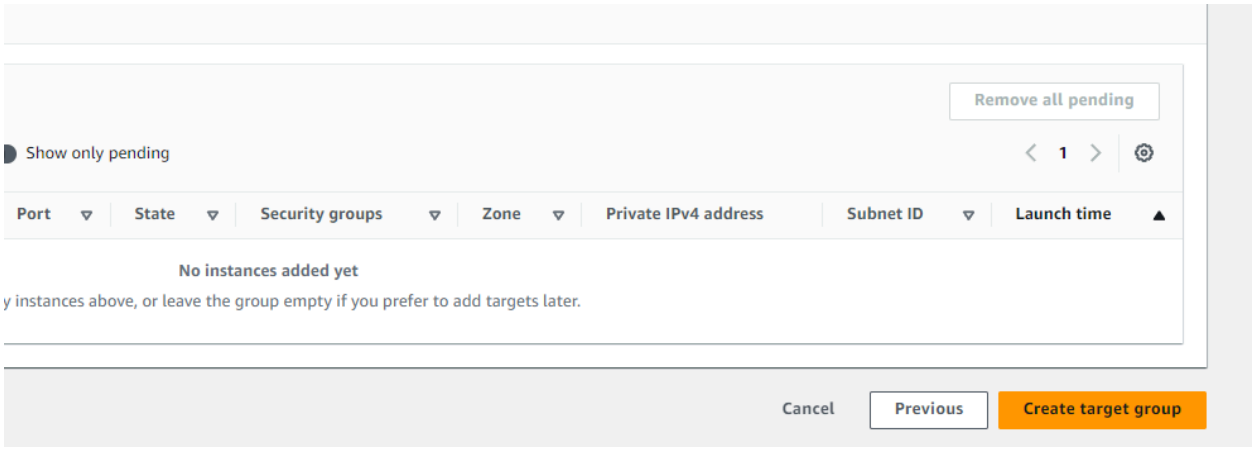
Auto scaling and ELB

Creating AMI for the given EC2 instance:

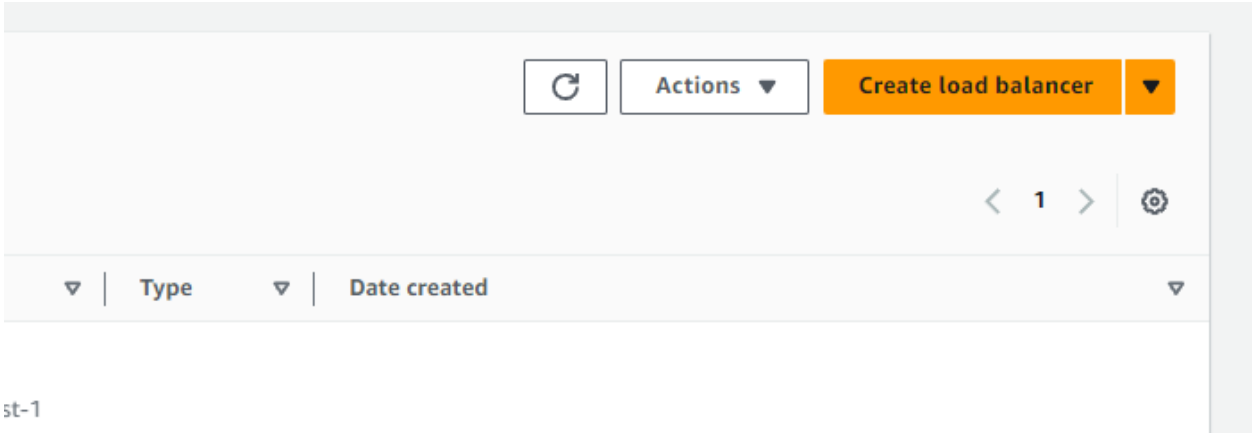




Creating Load balancer:
First create a target group.

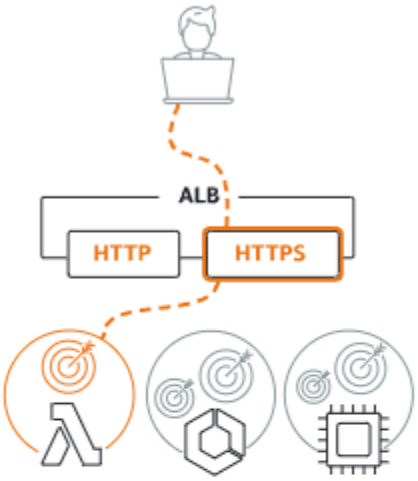


Now create load Balancer:



Create Application Load balancer:

Application Load Balancer Info



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create

Mappings | Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☑ **us-east-1a (use1-az2)**

Subnet

subnet-0595a05bc29148d7d — Public Subnet 1

IPv4 address

Assigned by AWS

☑ **us-east-1b (use1-az4)**

Subnet

subnet-08358b7cb592559e8 — Public Subnet 2

IPv4 address

Assigned by AWS

Security groups Info

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

Web Security Group
sg-0d157249119e0d417 VPC: vpc-07888501c4117a3da

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener **HTTP:80** Remove

Protocol: HTTP : Port: 80 (1-65535)

Default action | Info

Forward to: LabGroup — Target type: Instance, IPv4 — HTTP

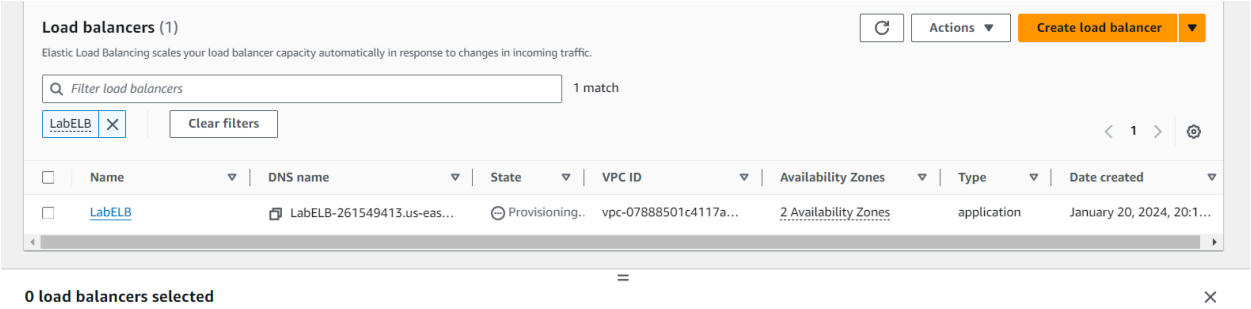
Create target group

Listener tags - *optional*

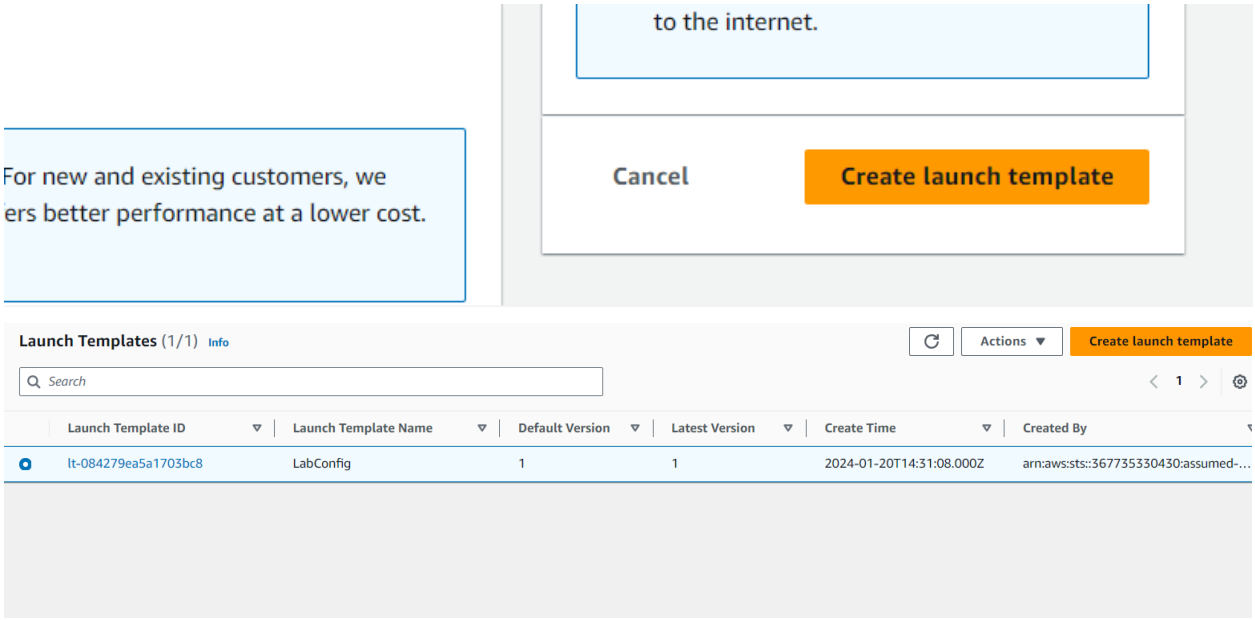
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tag

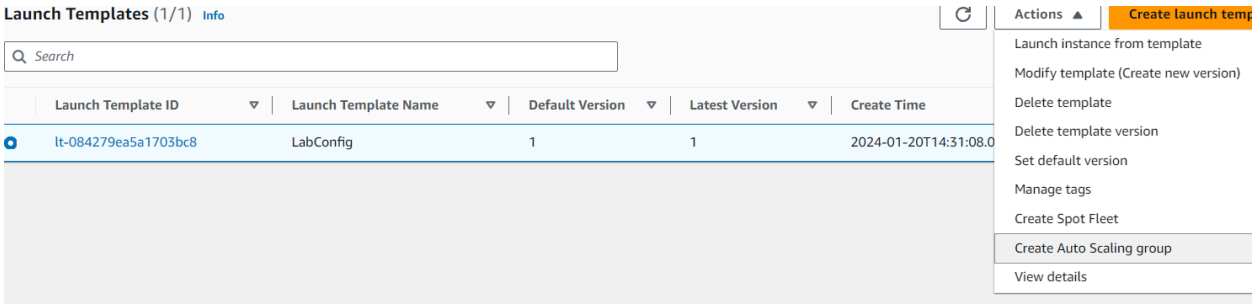
Load Balancer created:



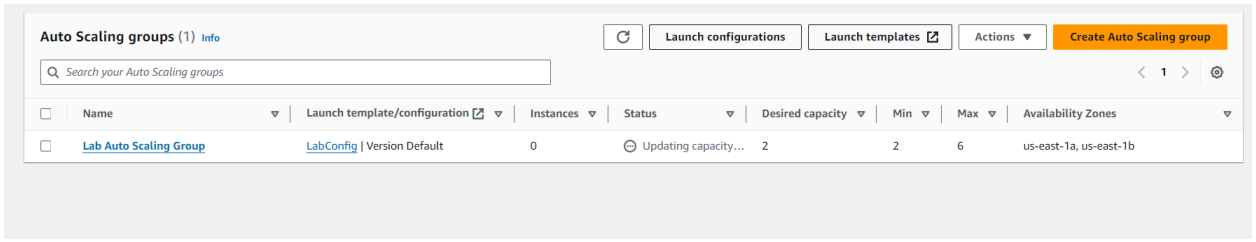
Create a Launch Template and an Auto Scaling Group



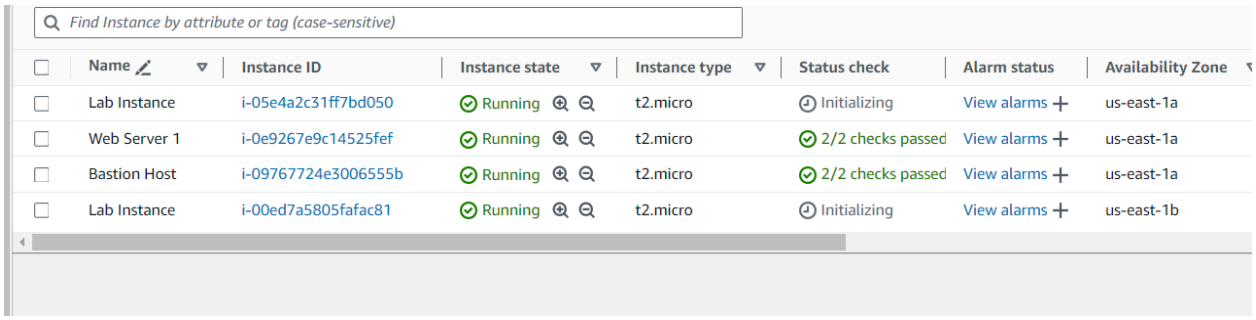
Create Auto Scaling Group



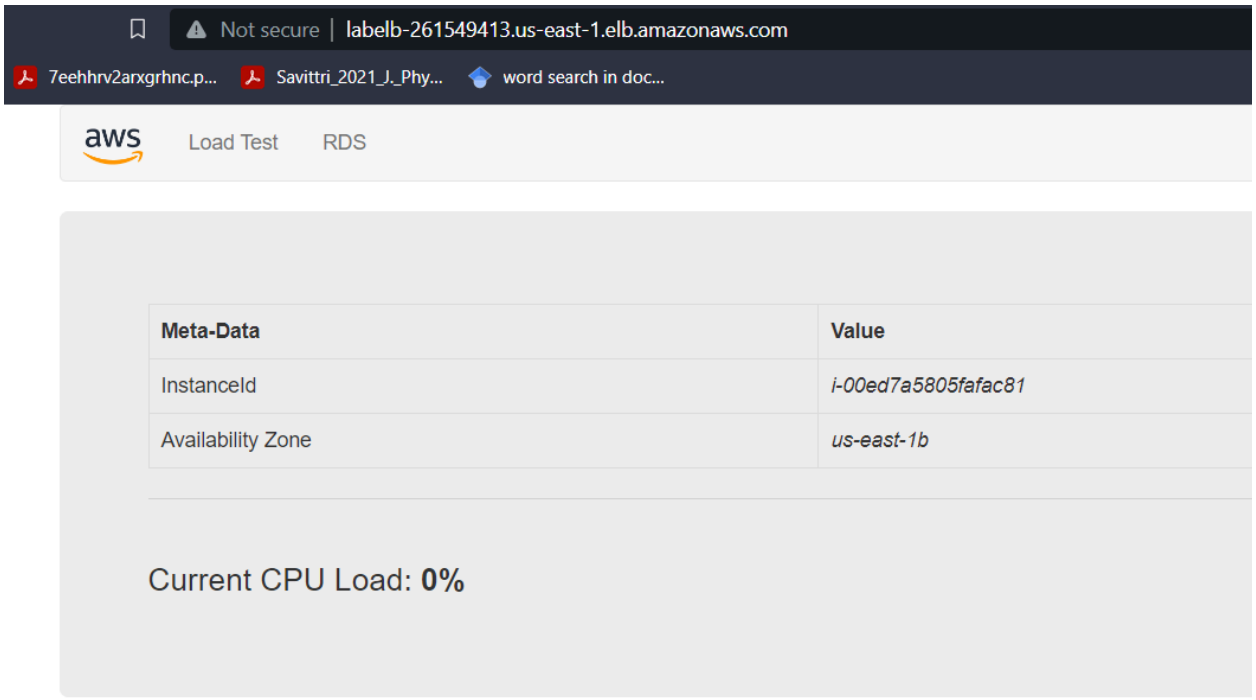
Create auto scaling group:

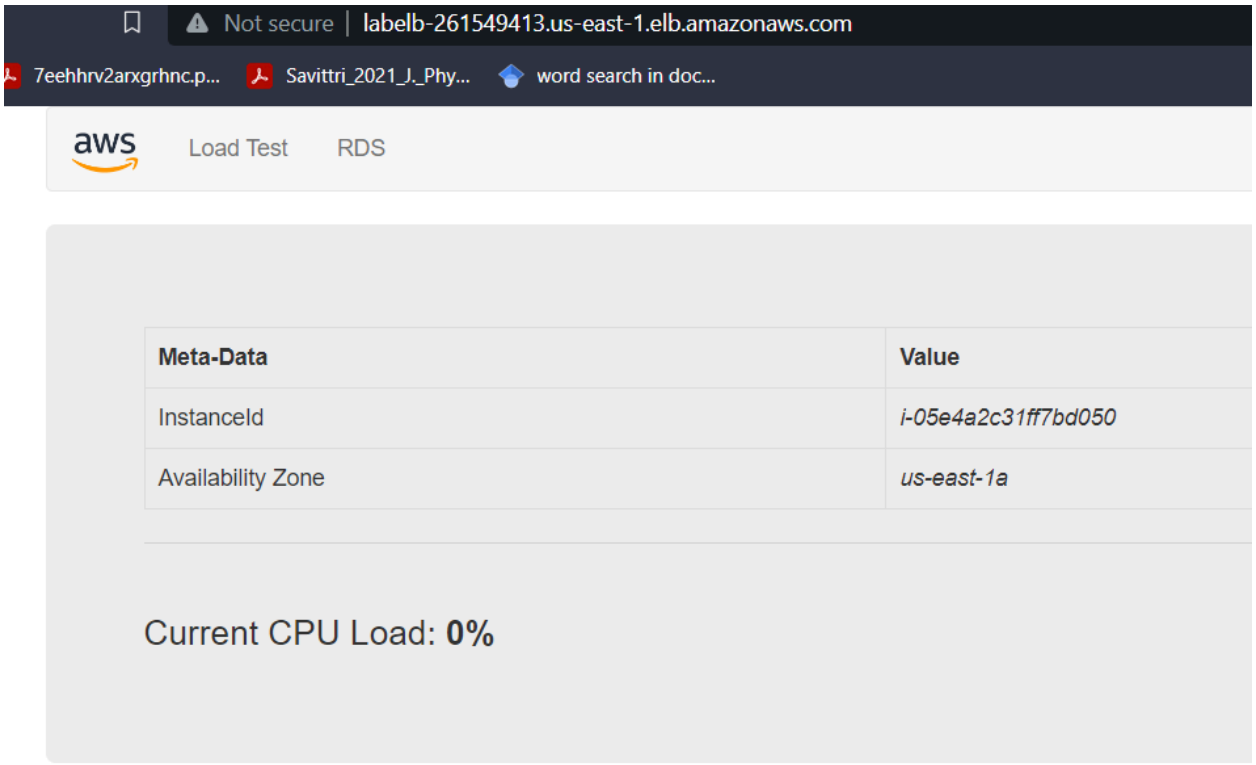


Auto scaling group create 2 desire instance:



Testing load balancer:





note : 2 different instance is returned