

Workshop I – EC2, ELB, and Autoscaling

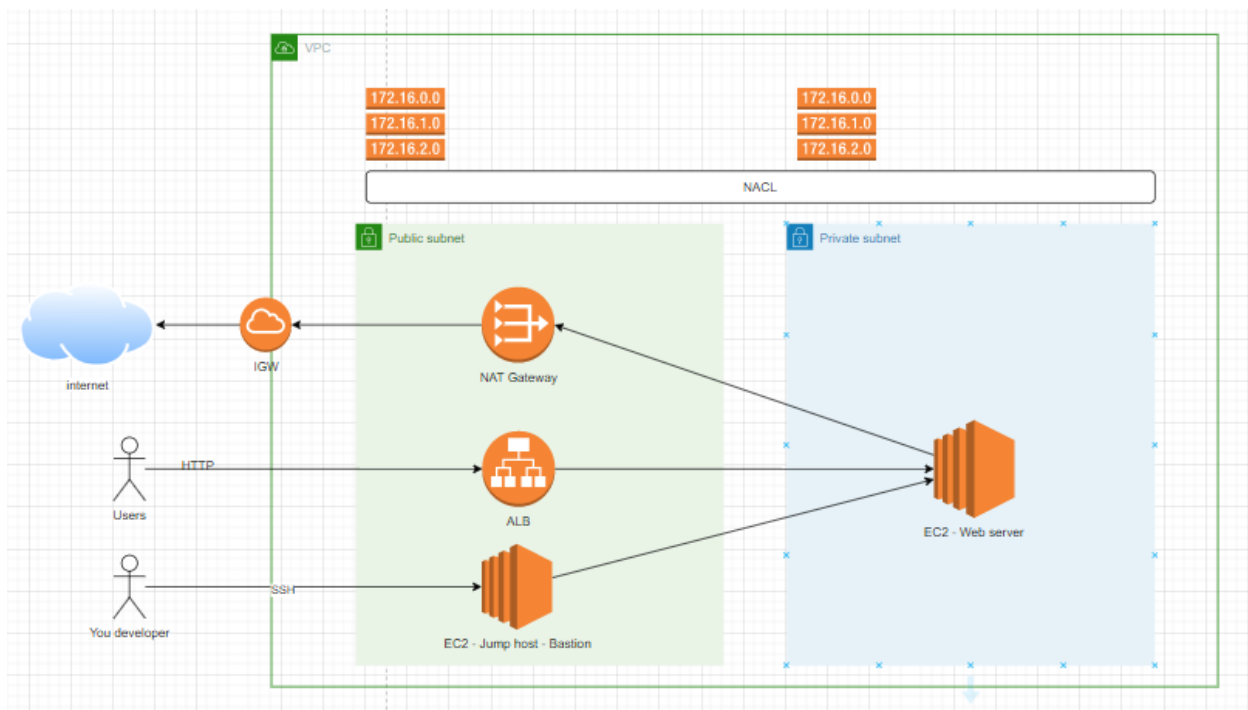
Today's task:

1. Create a web server inside private subnet. Create ALB in public.
 - a. You need to create a NAT gateway first to have internet access in private subnet so it can download required packages from the internet.
 - i. NAT will be created in public subnet.
 - ii. Create a RouteTable for private subnets. Associate private subnets with it.
 - iii. Add a route to the RouteTable for private subnets that points to your NAT gateway.
 - iv. **NAT is an expensive VPC component. Make sure that you delete after you have done the task and taken screenshots.**
 - v. **When create NAT, you assign an Elastic IP to it. Elastic IP costs when it is NOT used. But free if you are using it. After NAT gateway deletion, you must release the elastic IP otherwise you will get charged.**
2. Create a web app in EC2 inside ASG behind an ALB

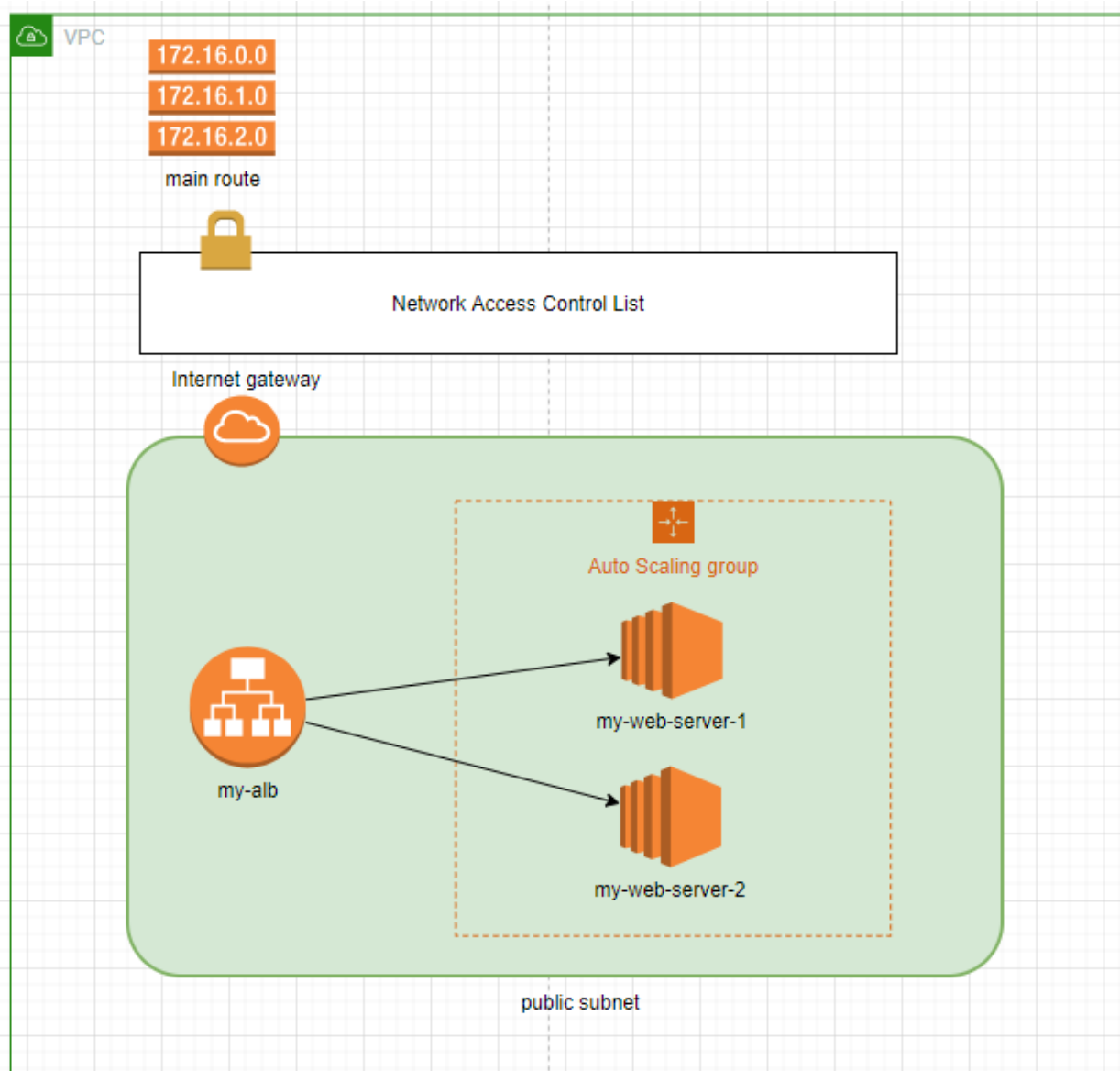
Submit items below in one pdf file:

1. Screenshot of ASG after it successfully creates EC2 instances
2. Screenshot of TG
3. Screenshot of the app with your name using ALB DNS.

Architecture of the task with NAT gateway.



Architecture of the task with ASG.



Instruction 1. Create Security Groups

- Create a SG for the ALB which is open to the world.
- Create a SG for web servers that allows ALB's SG.

Create Application Load Balancer Security Group (Outbound Rule is Default - All Traffic)

Security group name my-lab-alb-sg	Security group ID sg-03e5e025e377518eb	Description Lab Application Load Balancer Security Group	VPC ID vpc-0b978358e22761686
Owner 409673912482	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Tags

Inbound rules (1/1)						Manage tags	Edit inbound rules
Filter security group rules						< 1 >	
Type	Protocol	Port range	Source	Description			
HTTP	TCP	80	0.0.0.0/0	-			

Create EC2 Web Server Security Group (Outbound Rule is Default - All Traffic)

Security group name my-lab-EC2-Server-sg	Security group ID sg-0a370c15c5b405b61	Description Web Server Security Group	VPC ID vpc-0b978358e22761686
Owner 409673912482	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Tags

Inbound rules (1/1)						Manage tags	Edit inbound rules
Filter security group rules						< 1 >	
Type	Protocol	Port range	Source	Description			
HTTP	TCP	80	sg-03e5e025e377518eb	-			

my-lab-alb-sg
Security Group

Instruction 2. Create an ALB

- Create the default http:80 listener.
- Select VPC and public subnets.
- Select the ALB's SG that you created in Task 1.
- Create a target group, type as Instance. Don't register targets for now.

Go to the Load Balancers Display from the EC2 Dashboard

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	4	Load balancers	0
Placement groups	0	Security groups	7
Snapshots	0	Volumes	0

1) Click on Load Balancers

2) Click on Create Load Balancer

Select load balancer type

Elastic Load Balancing supports four types of load balancers: Application Load Balancers, Network Load Balancers, Gateway Load Balancers, and Classic Load Balancers. Choose the load balancer type that meets your needs.

[Learn more about which load balancer is right for you](#)

Application Load Balancer

HTTP
HTTPS

Create

Choose an Application Load Balancer when you need a flexible feature set for your web 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.

Network Load Balancer

TCP
TLS
UDP

Create

Choose a Network Load Balancer when you need ultra-high performance, low latency, and the ability to handle millions of requests per second securely.

Gateway Load Balancer

IP

Create

Choose a Gateway Load Balancer when you need to manage a fleet of third-party virtual appliances that support GENEVE. These appliances improve security, compliance, and policy controls.

3) Click on Create Application Load Balancer

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name ⓘ **4) Name Load Balancer**

Scheme ⓘ ☒ internet-facing
☐ internal

IP address type ⓘ

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
<input type="text" value="HTTP"/>	<input type="text" value="80"/>

[Cancel](#) [Next: Configure Security Settings](#)

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

VPC ⓘ **5) Select VPC**

Availability Zones

☒ **us-east-1a** **6) Select At Least 2 AZ Zones and Subnets**

IPv4 address ⓘ Assigned by AWS

☒ **us-east-1b**

IPv4 address ⓘ Assigned by AWS

☐ **us-east-1c**

Additional AWS services can be integrated with this load balancer at launch when you enable them below. You can also add these and other services after your load balancer is created by reviewing the "Integrated Services" tab for the selected load balancer.

AWS Global Accelerator ☐ Create an accelerator to get static IP addresses and improve the performance and availability of your application. [Learn more](#)
[Additional charges apply](#)

Your Accelerator will be created with the following name that you can customize. Once your Accelerator is created you can manage it from the Global Accelerator console.

Accelerator name

Maximum 64 characters. Letters and numbers only.

► Tags

7) Click Next

[Cancel](#) [Next: Configure Security Settings](#)

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 2: Configure Security Settings



Improve your load balancer's security. Your load balancer is not using any secure listener.

If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under [Basic Configuration](#) section. You can also continue with current settings.

8) Click Next

Cancel Previous Next: Configure Security Groups

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

Assign a security group ☐ Create a new security group
☒ Select an existing security group

Filter VPC security groups

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-002d4b487ca1292d2	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-0d09b0bf676ce516f	launch-wizard-2	launch-wizard-2 created 2021-07-08T19:37:07.572-05:00	Copy to new
<input type="checkbox"/> sg-0fc356187933ae278	launch-wizard-3	launch-wizard-3 created 2021-07-08T20:58:44.588-05:00	Copy to new
<input checked="" type="checkbox"/> sg-03e5e025e377518eb	my-lab-alb-sg	Lab Application Load Balancer Security Group	Copy to new
<input type="checkbox"/> sg-0a370c15c5b405b61	my-lab-EC2-Server-sg	Web Server Security Group	Copy to new

7) Select the ALB Security Group you Created

9) Click Next

Cancel Previous Next: Configure Routing

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify here. It also performs health checks on the targets using these settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer. You can edit or add listeners after the load balancer is created.

Target group

Target group ⓘ New target group

Name ⓘ my-lab-target

Target type
☒ Instance
☐ IP
☐ Lambda function

Protocol ⓘ HTTP

Port ⓘ 80

Protocol version ⓘ ☒ HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

10) Name Target Group

11) Select Instance

Health checks

Protocol ⓘ HTTP

Path ⓘ /

▶ Advanced health check settings

Cancel Previous Next: Register Targets

12) Click Next

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
No instances available.						

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 80

Cancel Previous Next: Review

13) Click Next

Step 6: Review

Please review the load balancer details before continuing

▼ Load balancer Edit

Name my-lab-alb

Scheme internet-facing

Listeners Port:80 - Protocol:HTTP

IP address type ipv4

VPC vpc-0b978358e22761686 (my-lab-vpc)

Subnets subnet-0ef43ef1cfcb561a0 (lab-sn-public-1A), subnet-03b7f8298553c4646 (lab-sn-public-1B)

Tags

▼ Security groups Edit

Security groups sg-03e5e025e377518eb

▼ Routing Edit

Target group New target group

Target group name my-lab-target

Cancel Previous Create

14) Click Create


Instruction 3. Create a launch template

- Select the web server's SG created in Task 1.
- Expand advanced and enter the user data below.

Go to Launch Templates Display from EC2 Display

New EC2 Experience [Learn more](#) ✕


EC2 Dashboard

- Events
- Tags
- Limits
- ▼ **Instances**
 - Instances New
 - Instance Types
 - Launch Templates 
 - Spot Requests
 - Savings Plans
 - Reserved Instances New
 - Dedicated Hosts
 - Scheduled Instances
 - Capacity Reservations

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	4	Load balancers	0
Placement groups	0	Security groups	9
Snapshots	0	Volumes	0


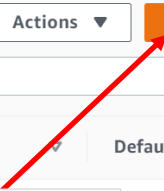
 1) Click Launch Templates



by Microsoft SQL Server Always On availability groups ✕
Wizard for SQL Server. [Learn more](#)


Create Launch Template

EC2 > Launch templates

Launch templates (1) [Info](#)

 **Actions** ▼ **Create launch template** 

 *Filter by tags or properties or search by keyword* < 1 > 

Launch template ID	Launch template name	Default version
 lt-0add0ae0ee0d310d3		

1) Click Create Launch Template

...

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Launch template name - *required*

my-lab-server

Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

☒ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

2) Name Template

Selecting Guidance will
show more Details

► Template tags

► Source template

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

▼ Amazon machine image (AMI) - required [Info](#)

AMI - *required*

Amazon Linux 2 AMI (HVM), SSD Volume Type

ami-0dc2d3e4c0f9ebd18

Catalog: Quick Start virtualization: hvm architecture: 64-bit (x86)

3) Select AMI

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible

4) Select Instance Type

[Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name

Don't include in launch template ▼



[Create new key pair](#)

▼ Network settings

Networking platform [Info](#)



Virtual Private Cloud (VPC)

Launch into a virtual network in your own logically isolated area within the AWS Cloud



EC2-Classic

Launch into a single flat network that you share with other customers.

Security groups

Select security groups ▼



my-lab-EC2-Server-sg sg-0a370c15c5b405b61 X
VPC: vpc-0b978358e22761686

5) Select Server security
Group you Created

▼ Storage (volumes) [Info](#)



Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp2))

AMI Volumes are not included in the template unless modified

Add new volume

▼ Resource tags [Info](#)

No resource tags are currently included in this template. Add a resource tag to include it in the launch template.

Add tag

50 remaining (Up to 50 tags maximum)

▼ Network interfaces [Info](#)

No network interfaces are currently included in this template. Add a network interface to include it in the launch template.

Add network interface

▼ Advanced details [Info](#)

... User Data at Bottom of Advanced Details

User data [Info](#)

```
#!/bin/bash
yum install httpd -y
cd /var/www/html
echo '<p>Hello from my EC2 Instance in Autoscaling Group Behind an ALB</p>' >
index.html
sudo service httpd start
```

☐ User data has already been base64 encoded

6) Insert Startup Commands
for EC2 Instance

7) Click Create Launch Template

Cancel

Create launch template

EC2 Instance Startup Commands

```
#!/bin/bash
yum install httpd -y
cd /var/www/html
echo '<p>Hello from the instance in autoscaling group behind an ALB</p>' >
index.html
sudo service httpd start
```

#!/bin/bash --> tells the OS to invoke the specified shell to execute the script commands

Instruction 4. Create Auto Scaling Group

- Select the launch template.
- Select the custom VPC and public subnets.
- Click on attach to an existing load balancer and select the default TG (Target Group) of the ALB.
- Desired capacity 2, min is 1, max is 3. Set target tracking scaling policy on the CPU utilization with any value from 10 to 90. AWS AutoScaling tries to maintain the CPU utilization at that level. If it exceeds, scales out.

Go to Auto Scaling Display from EC2 Display

Snapshots

Lifecycle Manager

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

▼ Load Balancing

Load Balancers

Target Groups **New**

▼ Auto Scaling

Launch Configurations

Auto Scaling Groups

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	4	Load balancers	1
Placement groups	0	Security groups	9
Snapshots	0	Volumes	0

1) Click on Auto Scaling Groups

Create Auto Scaling Group

Amazon EC2 Auto Scaling
helps maintain the availability
of your applications

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management of your applications.

Create Auto Scaling group

Get started with EC2 Auto Scaling by creating an Auto Scaling group.

Create Auto Scaling group

1) Click on Create Auto Scaling Group

...

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Choose launch template or configuration [Info](#)

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name

Enter a name to identify the group.

my-lab-as-group

2) Name Group

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

[Switch to launch configuration](#)

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

my-lab-server

3) Select Your Launch Template

[Create a launch template](#)

Version

Default (1)

[Create a launch template version](#)

Description

-

AMI ID

ami-0dc2d3e4c0f9ebd18

Key pair name

-

Launch template

[my-lab-server](#)
lt-0ca69b78349a3fb83

Security groups

-

Security group IDs

[sg-0a370c15c5b405b61](#)

Instance type

t2.micro

Request Spot Instances

No

Additional details

Storage (volumes)

-

Date created

Sun Jul 11 2021 11:24:24 GMT-0500
(Central Daylight Time)

4) Click Next

Cancel

Next

Step 1

[Choose launch template or configuration](#)

Step 2

Configure settings

Step 3 (optional)

[Configure advanced options](#)

Step 4 (optional)

[Configure group size and scaling policies](#)

Step 5 (optional)

[Add notifications](#)

Step 6 (optional)

[Add tags](#)

Step 7

[Review](#)

Configure settings [Info](#)

Configure the settings below. Depending on whether you chose a launch template, these settings may include options to help you make optimal use of EC2 resources.

Instance purchase options [Info](#)

Use the launch template to create a uniform configuration among all of the instances in the group. Or define options to accommodate a wide variety of requirements, such as launching Spot and On-Demand Instances.

☒ **Adhere to launch template**

The launch template determines the purchase option (On-Demand or Spot) and instance type.

☐ **Combine purchase options and instance types**

Specify how much On-Demand and Spot capacity to launch and multiple instance types (optional). This choice is most helpful for optimizing the scale and cost for a fleet of instances.

Network [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

vpc-0b978358e22761686 (my-lab-vpc)
10.0.0.0/16

[Create a VPC](#)

Subnets

Select subnets

us-east-1a | subnet-0ef43ef1cfc561a0 (lab-sn-public-1A)
10.0.0.0/24

us-east-1b | subnet-03b7f8298553c4646 (lab-sn-public-1B)
10.0.2.0/24

[Create a subnet](#)

5) Select VPC

6) Select Some Subnets

7) Click Next

[Cancel](#)[Previous](#)[Skip to review](#)[Next](#)

...

Step 1
Choose launch template or
configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and
scaling policies

Step 5 (optional)
Add notifications

Configure advanced options [Info](#)

Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.

Load balancing - optional [Info](#)

8) Select Attach to Existing Load Balancer

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

☐ No load balancer

Traffic to your Auto Scaling group will not be fronted by a load balancer.

☒ Attach to an existing load balancer

Choose from your existing load balancers.

☐ Attach to a new load balancer

Quickly create a basic load balancer to attach to your Auto Scaling group.

Step 6 (optional)
Add tags

Step 7
Review

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

☒ Choose from your load balancer target groups

This option allows you to attach Application, Network, or Gateway Load Balancers.

☐ Choose from Classic Load Balancers

Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

my-lab-target | HTTP
Application Load Balancer: my-lab-alb

9) Select Your Load Balancer Target Group

Health checks - optional

Health check type [Info](#)

EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

☒ EC2 ☐ ELB

Health check grace period

The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are put into service.

300 seconds

Additional settings - optional

Monitoring [Info](#)

☐ Enable group metrics collection within CloudWatch

10) Click Next

Cancel

Previous

Skip to review

Next

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Configure group size and scaling policies [Info](#)

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - optional [Info](#)

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity

Minimum capacity

Maximum capacity

11) Set Desired, Min, and Max Capacity

Step 7
Review

Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

☒ **Target tracking scaling policy**
Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

☐ None

Scaling policy name

Metric type

Target value

12) Set Target Tracking for CPU Utilization

Instances need

seconds warm up before including in metric

☐ Disable scale in to create only a scale-out policy

Instance scale-in protection - optional

Instance scale-in protection

If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

☐ Enable instance scale-in protection

13) Click Next

Cancel

Previous

Skip to review

Next

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Add notifications Info

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.

14) Click Next

...

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Configure settings

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Add tags Info

Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

ⓘ You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group. ×

Tags (0)

50 remaining

15) Click Next

...

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Review Info

16) Click Next

... Review What you have just Selected

Instruction 5. Verify and Test the ALB

View the Health Check on your the Target Group Details. Both Instances Should be Healthy

my-lab-target

Delete

arn:aws:elasticloadbalancing:us-east-1:409673912482:targetgroup/my-lab-target/785ca90756d47acd

Details

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-0b978358e22761686
Load balancer	my-lab-alb		

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	✔ 2	✘ 0	⌵ 0	⌵ 0	⌵ 0

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (2)

Refresh

Deregister

Register targets

Filter resources by property or value

< 1 > ⚙

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details
<input type="checkbox"/>	i-0179bc9cdca16967e		80	us-east-1b	✔ healthy	
<input type="checkbox"/>	i-0f05d00a3423df3ad		80	us-east-1a	✔ healthy	

DNS on Load Balancer Display. Each EC2 will have a public address but you cannot access due to security group settings.

Create Load Balancer

Actions

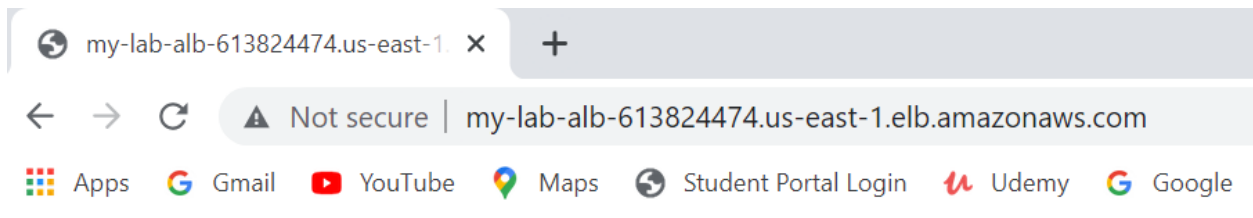
Filter by tags and attributes or search by keyword

DNS

1 to 1 of 1

<input type="checkbox"/>	Name	DNS name	State	VPC ID
<input type="checkbox"/>	my-lab-alb	my-lab-alb-613824474.us-east-1.elb.amazonaws.com	Active	vpc-0b978358e22761686

Test DNS with Web Browser



Hello from my EC2 Instance in Autoscaling Group Behind an ALB