



lab



lab title

**AWS Elastic Load Balancers**

**V1.01**



Course title

**BackSpace Academy**  
**AWS Certified Associate**



# Table of Contents

## Contents

Table of Contents.....	1
About the Lab .....	2
Implementing an Application Load Balancer .....	3
Creating a WordPress Server .....	3
Creating a Magento Server .....	6
Creating Target Groups.....	8
Create an Application Load Balancer.....	12
Create Routing Rules .....	15
Clean Up.....	18
Implementing a Network Load Balancer and Auto Scaling .....	20
Creating a Target Group .....	20
Creating an Auto Scaling Launch Configuration .....	21
Creating an Auto Scaling Group.....	24
Adding the Auto Scaling Group to an ELB Target Group .....	26
Creating a Network ELB .....	27
Clean Up.....	31

## About the Lab

**Please note that not all AWS services are supported in all regions. Please use the US-East-1 (North Virginia) region for this lab.**

These lab notes are to support the hands on instructional videos of the Elastic Load Balancing section of the AWS Certified Associate Course.

**Please note that AWS services change on a weekly basis and it is extremely important you check the version number on this document to ensure you have the latest version with any updates or corrections.**

# Implementing an Application Load Balancer

In this section we will create two EC2 servers running WordPress and Magento. We will then front these with an Application Load Balancer and implement path based routing.

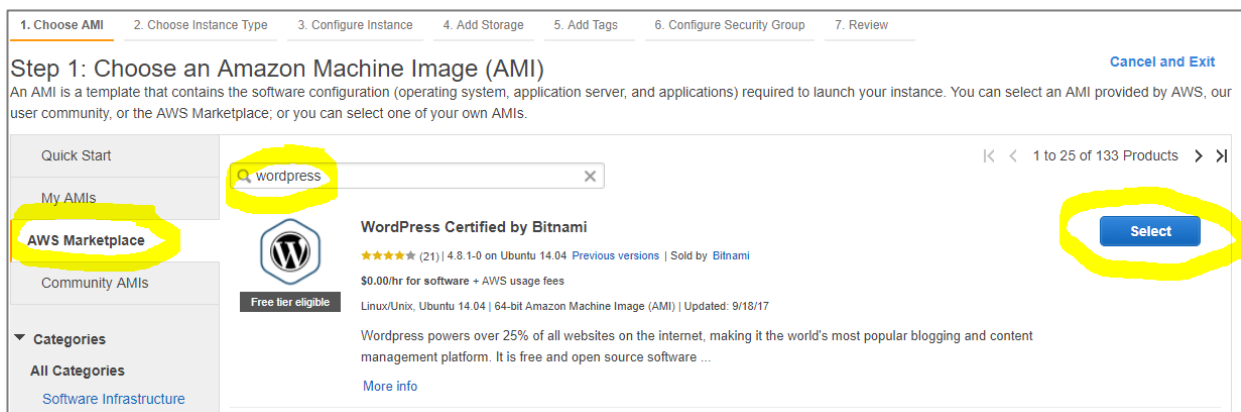
## Creating a WordPress Server

Click on the services menu and select EC2.

Click "Launch Instance"

Select "AWS Marketplace" and search for "Wordpress"

Select the Bitnami Wordpress AMI



Select t2 micro instance type

## Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation [Show/Hide Columns](#)

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

Note: The vendor recommends using a m3.medium instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Instance Details](#)

Click "Next Configure Instance Details"

Select "Auto Assign Public IP"

Click "Next Add Storage"

## Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances  [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)

Auto-assign Public IP

IAM role  [Create new IAM role](#)

Shutdown behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Add Storage](#)

Click "Next Add Tags"

Add key "name" and value "WordPress"

Click "Review and Launch"

**Step 5: Add Tags**

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	WordPress

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Security Group](#)

Click “Launch”

**Step 7: Review Instance Launch**

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**⚠ Improve your instances' security. Your security group, WordPress Certified by Bitnami-4-8-1-0 on Ubuntu 14-04-AutogenByAWSMP-1, is open to the world.**  
 Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ **AMI Details** [Edit AMI](#)



**WordPress Certified by Bitnami**

<https://bitnami.com>



Root Device Type: ebs Virtualization type: hvm

**Hourly Software Fees:** \$0.00 per hour on t2.micro instance (Additional taxes may apply.)  
 Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's

[Cancel](#)
[Previous](#)
[Launch](#)

Select a key pair and click “Launch Instances”

**Select an existing key pair or create a new key pair** ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Choose an existing key pair

Select a key pair

pcoady-us-east-1

☒ I acknowledge that I have access to the selected private key file (pcoady-us-east-1.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#)
[Launch Instances](#)

## Creating a Magento Server

Click on the services menu and select EC2.

Click "Launch Instance"

Select "AWS Marketplace" and search for "Magento"

Select the Bitnami Magento AMI

**Step 1: Choose an Amazon Machine Image (AMI)** Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

**AWS Marketplace**

Community AMIs

Categories

All Categories

Software Infrastructure (51)

Search:

1 to 25 of 62 Products

**Magento Certified by Bitnami**

★★★★★ (5) | 2.1.8-1 on Ubuntu 14.04 [Previous versions](#) | Sold by Bitnami

\$0.00/hr for software + AWS usage fees

Linux/Unix, Ubuntu 14.04 | 64-bit Amazon Machine Image (AMI) | Updated: 9/18/17

Free tier eligible

Magento is one of the most popular open source e-Commerce shopping cart systems in the world. It is extremely flexible and has a huge variety of plugins and add-ons to build just ...

[More info](#)

**Select**

Select t2 micro instance type

**Step 2: Choose an Instance Type**

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All instance types** **Current generation** [Show/Hide Columns](#)

**Currently selected:** t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

**Note:** The vendor recommends using a **m3.medium** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	<b>t2.micro</b> Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Instance Details](#)

Click "Next Configure Instance Details"

Select "Auto Assign Public IP"

Click "Next Add Storage"

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances  [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)

Auto-assign Public IP

IAM role  [Create new IAM role](#)

Shutdown behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring  
Additional charges apply

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

Click "Next Add Tags"

Add key "Name" and value "Magento"

Click "Review and Launch"

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	Magento

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Click "Launch"



**Step 7: Review Instance Launch**

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

▼ AMI Details [Edit AMI](#)**Magento Certified by Bitnami**<https://bitnami.com>

Free tier eligible

Root Device Type: ebs Virtualization type: hvm

**Hourly Software Fees: \$0.00 per hour** on t2.micro instance (Additional taxes may apply.)  
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#)

▼ Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance

[Cancel](#)[Previous](#)[Launch](#)

Select a key pair and click “Launch Instances”

**Select an existing key pair or create a new key pair** ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair ▼

**Select a key pair**

pcoady-us-east-1 ▼

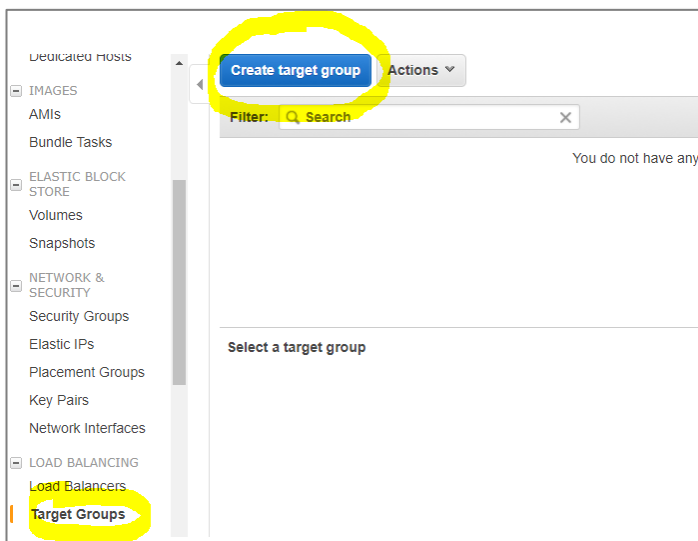
☒ I acknowledge that I have access to the selected private key file (pcoady-us-east-1.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#)[Launch Instances](#)

## Creating Target Groups

Scroll down and select “Load Balancers”

Click “Create Target Group”



Create a target Group called “WordPress”

The screenshot shows the 'Create target group' form in the AWS Management Console. The form is titled 'Create target group' and includes a close button (X) in the top right corner. Below the title is a descriptive text: 'Your load balancer routes requests to the targets in a target group using the protocol and port that you specify, and performs health checks on the targets using the health check settings that you specify.'

The form contains the following fields:

- Target group name:** A text input field with the value 'WordPress' highlighted in yellow.
- Protocol:** A dropdown menu with 'HTTP' selected.
- Port:** A text input field with the value '80'.
- Target type:** A dropdown menu with 'instance' selected.
- VPC:** A dropdown menu with 'vpc-72d25a0b (172.31.0.0/16) (My Default V' selected.

Below these fields is the 'Health check settings' section, which includes:

- Protocol:** A dropdown menu with 'HTTP' selected.
- Path:** A text input field with the value '/'.

At the bottom of the form is a section for 'Advanced health check settings' with a right-pointing arrow. In the bottom right corner, there are two buttons: 'Cancel' and 'Create', with the 'Create' button highlighted in yellow.

Create another Target Group called “Magento”

**Create target group**

Your load balancer routes requests to the targets in a target group using the protocol and port that you specify, and performs health checks on the targets using the health check settings that you specify.

Target group name *i*

Protocol *i*

Port *i*

Target type *i*

VPC *i*

**Health check settings**

Protocol *i*

Path *i*

► **Advanced health check settings**

[Cancel](#) [Create](#)

Select the WordPress Target Group

Select the "Targets" tab

Select "Edit"

**WordPress** 80 HTTP instance vpc-72d25a0b

Target group: **WordPress**

Description **Targets** Health checks Monitoring Tags

The load balancer starts routing requests to a newly registered target as soon as the registration process completes and the target passes the initial health checks. If demand on your targets increases, you can register additional targets. If demand on your targets decreases, you can deregister targets.

[Edit](#)

Registered targets

Select the WordPress EC2 instance

Click "Add to Registered"

Click "Save"

**Register and deregister targets** ✕

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

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-0980eb9e08edcb7da	WordPress	80	running	WordPress Certified by Bitnami-4-8-1-0 on Ub...	us-east-1c

**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.

on port

✕

<input type="checkbox"/>	Instance	Name	State	Security	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-0980eb9e08edcb7da	WordPress	running	WordPress Certif...	us-east-1c	subnet-227d386a	172.31.16.0/20
<input type="checkbox"/>	i-04dc7e0255352...	Magento	running	Magento Certifie...	us-east-1c	subnet-227d386a	172.31.16.0/20

Select the Magento Target Group

Select the "Targets" tab

Select "Edit"

<input checked="" type="checkbox"/>	Magento	80	HTTP	instance	vpc-72d25a0b
<input type="checkbox"/>	WordPress	80	HTTP	instance	vpc-72d25a0b

**Target group: Magento**

The load balancer starts routing requests to a newly registered target as soon as the registration process completes and the health checks pass. If demand on your targets increases, you can register additional targets. If demand on your targets decreases, you can deregister targets.

Select the Magento EC2 instance

Click "Add to Registered"

Click "Save"

**Register and deregister targets**

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

Remove

Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/> i-04dc7e0255352d73c	Magento	80	● running	Magento Certified by Bitnami-2-1-8-1 on Ubu...	us-east-1c

**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

Search Instances

Instance	Name	State	Security	Zone	Subnet ID	Subnet CIDR
<input type="checkbox"/> i-0980eb9e08edc...	WordPress	● running	WordPress Certif...	us-east-1c	subnet-227d386a	172.31.16.0/20
<input checked="" type="checkbox"/> i-04dc7e0255352...	Magento	● running	Magento Certifie...	us-east-1c	subnet-227d386a	172.31.16.0/20

Cancel Save

## Create an Application Load Balancer

Select "Load Balancers"

Click on "Create Load Balancer"

Snapshots

NETWORK & SECURITY

- Security Groups
- Elastic IPs
- Placement Groups
- Key Pairs
- Network Interfaces

LOAD BALANCING

- Load Balancers**
- Target Groups

AUTO SCALING

Create Load Balancer

Filter: Search

You do not have any load balancers.

Select a load balancer

Select "Application Load Balancer"

## Select load balancer type

Elastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers (new), 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, TLS termination and visibility features targeted at application architectures, including microservices and containers.

### Network Load Balancer

TCP

Create

Choose a Network Load Balancer when you need ultra-high performance and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second while maintaining ultra-low latencies.

### Classic Load Balancer

PREVIOUS GENERATION  
for HTTP, HTTPS, and TCP

Create

Choose a Classic Load Balancer when you have an existing application running in the EC2-Classical network.

[Learn more >](#)

## Give the ELB a name

### 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 with a listener that receives HTTP traffic on port 80.

Name ⓘ

Scheme ⓘ ☒ internet-facing ☐ internal

IP address type ⓘ

## Select all Availability Zones

## Click "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 ⓘ

<input checked="" type="checkbox"/> Availability Zone	Subnet ID	Subnet IPv4 CIDR	Name
<input checked="" type="checkbox"/> us-east-1a	subnet-d6455ab3	172.31.0.0/20	
<input checked="" type="checkbox"/> us-east-1b	subnet-a9e06d85	172.31.80.0/20	
<input checked="" type="checkbox"/> us-east-1c	subnet-227d386a	172.31.16.0/20	
<input checked="" type="checkbox"/> us-east-1d	subnet-c0a2279a	172.31.32.0/20	
<input checked="" type="checkbox"/> us-east-1e	subnet-a7b38b9b	172.31.64.0/20	
<input checked="" type="checkbox"/> us-east-1f	subnet-4770eb4b	172.31.48.0/20	

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

## Click "Next: Configure Security Groups"

## Select "Create a new security group"

## Click "Next: Configure Routing"

### 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

Security group name: load-balancer-wizard-2  
Description: load-balancer-wizard-2 created on 2017-10-18T17:40:42.325+11:00

Type	Protocol	Port Range	Source
Custom TCP	TCP	80	Custom 0.0.0.0/0, ::/0

Add Rule

Cancel Previous **Next: Configure Routing**

Select the WordPress Target Group as the default routing

Click "Register Targets"

### Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

#### Target group

Target group: Existing target group  
Name: WordPress  
Protocol: HTTP  
Port: 80  
Target type: instance

#### Health checks

Protocol: HTTP  
Path: /

Advanced health check settings

Cancel Previous **Next: Register Targets**

Click "Next Review"

Click "Create"

## Step 6: Review

Please review the load balancer details before continuing

## ▼ Load balancer

[Edit](#)

**Name** TestELB  
**Scheme** internet-facing  
**Listeners** Port:80 - Protocol:HTTP  
**IP address type** ipv4  
**VPC** vpc-72d25a0b  
**Subnets** subnet-d6455ab3, subnet-a9e06d85, subnet-227d386a, subnet-c0a2279a, subnet-a7b38b9b, subnet-4770eb4b  
**Tags**

## ▼ Security settings

[Edit](#)

**Certificate name**  
**Security policy name**

## ▼ Security groups

[Edit](#)

**Security groups** load-balancer-wizard-2

[Cancel](#)[Previous](#)[Create](#)

## Create Routing Rules

Select the "Listeners" Tab

Click "View/edit rules"

Load balancer: **TestELB**

Description | **Listeners** | Monitoring | Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route can add, remove, or update listeners and listener rules.

[Add listener](#) [Actions](#)

<input type="checkbox"/>	Listener ID	Security policy	SSL Certificate	Rules
<input type="checkbox"/>	HTTP : 80 arn...2281744604bfd85b	N/A	N/A	Default: forwarding to WordPress <a href="#">View/edit rules</a>

Click add rules icon

Click "Insert Rule"

Rules for: TestELB HTTP 80

Insert Rule: Click a location for your new rule.

[Insert Rule](#)

	IF	THEN
last HTTP 80: default action <i>This rule cannot be moved or deleted</i>	✓ Requests otherwise not routed	Forward to WordPress



Select "Path"

Enter "/store"

Select "Magento" Target Group

Click "Save"

Insert Rule: Click a location for your new rule.

Insert Rule

1	RULE ID	IF	THEN
	A rule ID (ARN) is generated when you save your rule.	<div>Host Path</div> <div>is /store</div> <div>&amp;</div>	<div>Forward to</div> <div>Magento</div>
			<div>Save Cancel</div>

last HTTP 80: default action  
This rule cannot be moved or deleted

IF  
✓ Requests otherwise not routed

THEN  
Forward to WordPress

Click add rules icon

Click "Insert Rule"

Select "Path"

Enter "/store/\*"

Select "Magento" Target Group

Insert Rule: Click a location for your new rule. ✓ New rule was created successfully.

Insert Rule

1	RULE ID	IF	THEN
	A rule ID (ARN) is generated when you save your rule.	<div>Host Path</div> <div>is /store/*</div> <div>&amp;</div>	<div>Forward to</div> <div>Magento</div>
			<div>Save Cancel</div>

2 ARN

IF  
✓ Path is /store

THEN  
Forward to Magento

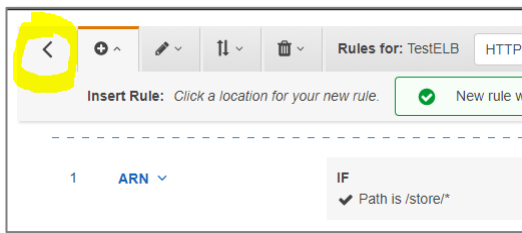
Insert Rule

last HTTP 80: default action  
This rule cannot be moved or deleted

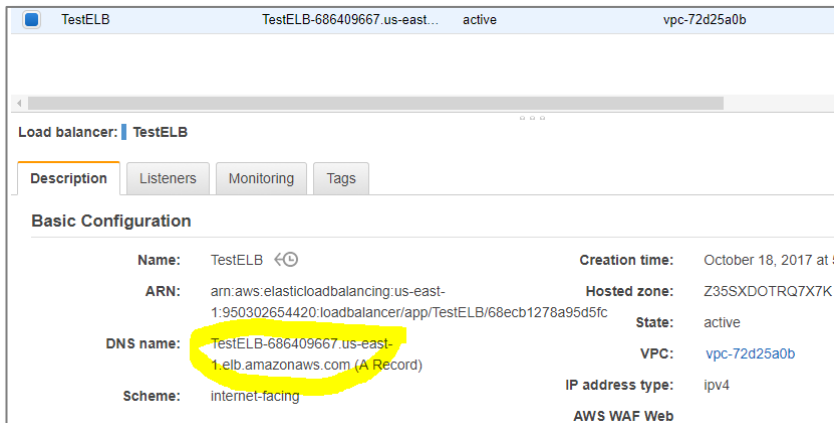
IF  
✓ Requests otherwise not routed

THEN  
Forward to WordPress

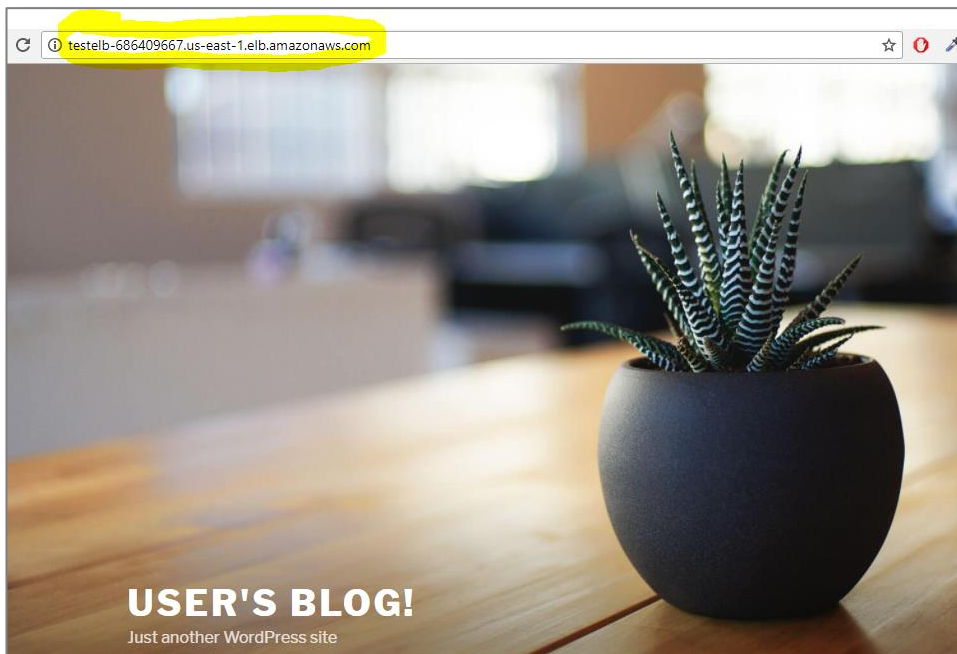
Go Back to Load Balancer



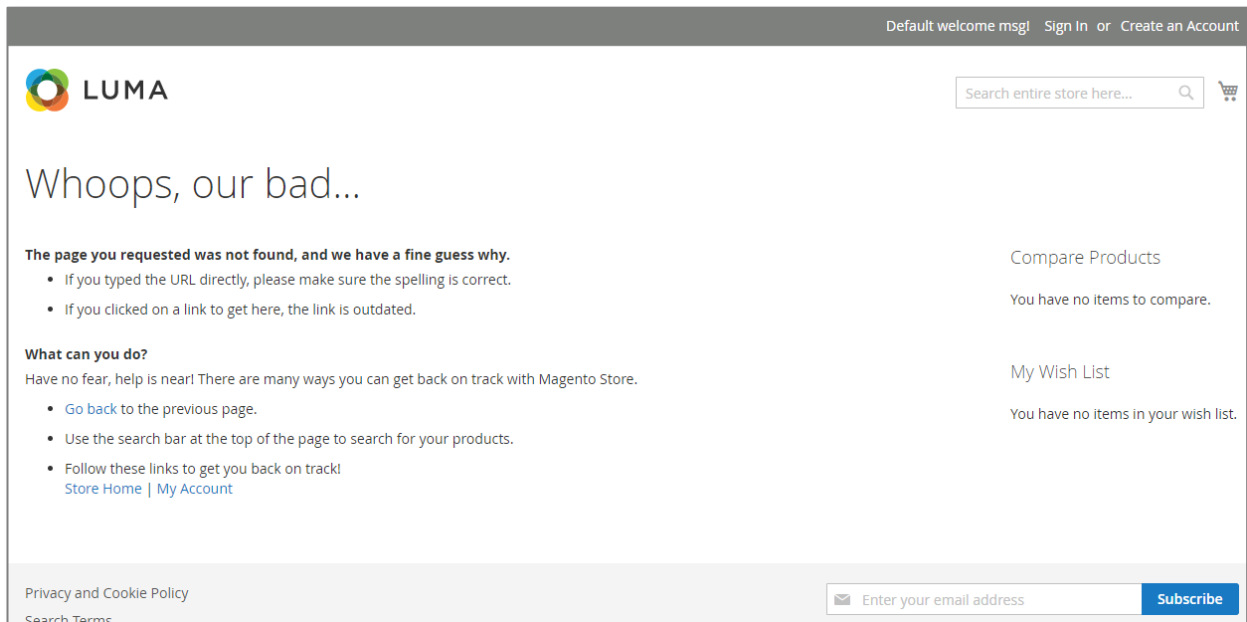
Copy the Load Balancer URL



Open URL in Browser to see the WordPress Blog



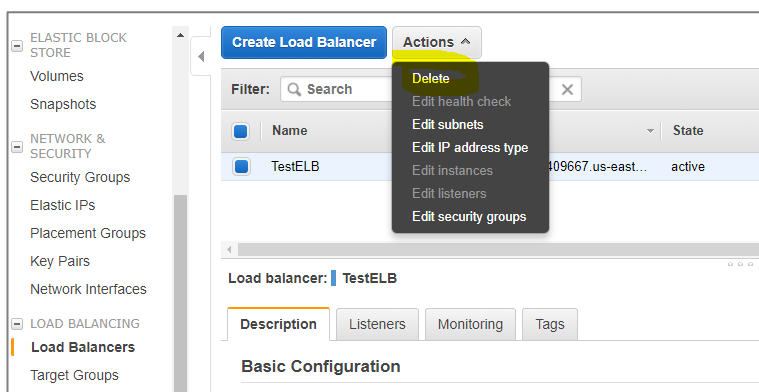
Now add "/store" to the end of the URL to see the Magento Store



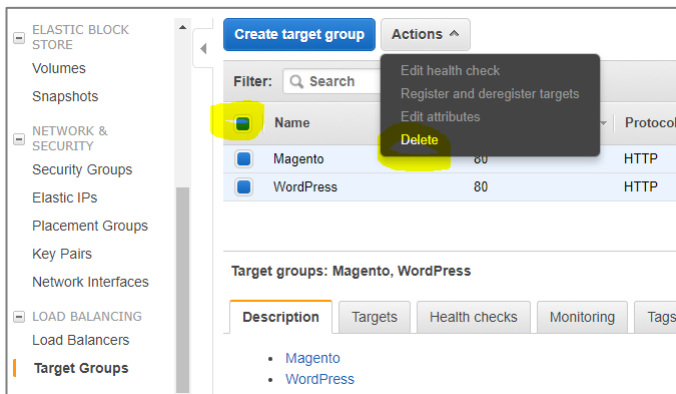
Although it has successfully routed to Magento, the Magento “not found” page will be show as the Magento home page settings will need to be changed to the “/store” path.

## Clean Up

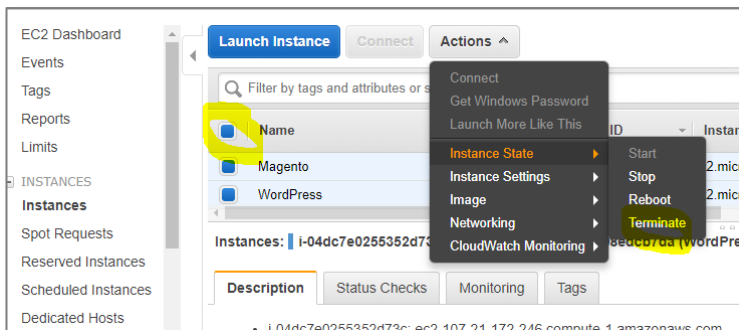
### Delete the Load Balancer



### Delete the Target Groups



## Terminate the instances



# 🎥 Implementing a Network Load Balancer and Auto Scaling

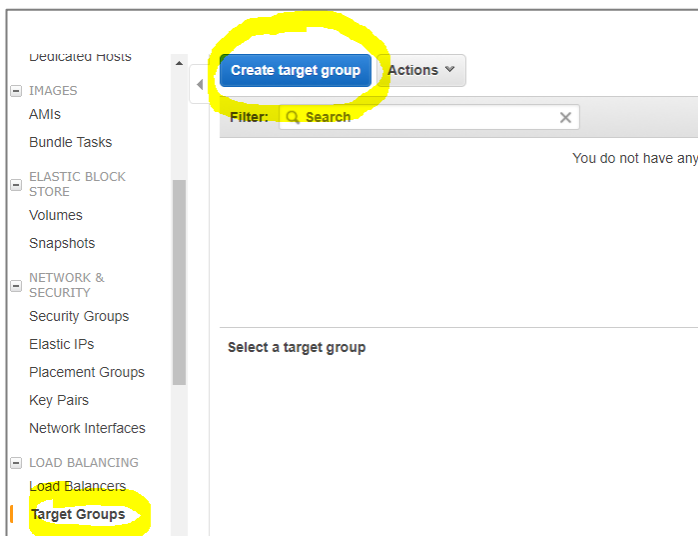
In this section we will create an Auto Scaling group. We will then add this to a target group and create a network load balancer to serve TCP traffic to the Auto Scaling group.

## Creating a Target Group

Click on the services menu and select EC2.

Scroll down and select “Load Balancers”

Click “Create Target Group”



Create a target Group called “NetworkELB”

Select “TCP” for Protocol

**Create target group** ✕

Your load balancer routes requests to the targets in a target group using the protocol and port that you specify, and performs health checks on the targets using the health check settings that you specify.

Target group name ?

Protocol ?

Port ?

Target type ?

VPC ?

**Health check settings**

Protocol ?

► **Advanced health check settings**

[Cancel](#) [Create](#)

Click "Create"

Filter:

<input type="checkbox"/>	Name	Port	Protocol	Target type	VPC ID
<input checked="" type="checkbox"/>	NetworkELB	80	TCP	instance	vpc-72d25a0b

## Creating an Auto Scaling Launch Configuration

Select "Launch Configurations"

Click "Create Auto Scaling group"

**ELASTIC BLOCK STORE**

- Volumes
- Snapshots

**NETWORK & SECURITY**

- Security Groups
- Elastic IPs
- Placement Groups
- Key Pairs
- Network Interfaces

**LOAD BALANCING**

- Load Balancers
- Target Groups

**AUTO SCALING**

- Launch Configurations**
- Auto Scaling Groups

**SYSTEMS MANAGER**

**Welcome to Auto Scaling**

You can use Auto Scaling to manage Amazon EC2 capacity automatically, maintain the right number of instances for your application, operate a healthy group of instances, and scale it according to your needs.

[Learn more](#)

[Create Auto Scaling group](#)

Note: To create your Auto Scaling groups in a different region, select your region from the navigation bar.

**Benefits of Auto Scaling**

**Reusable Instance Templates**

Provision instances based on a reusable template you define, called a launch configuration.

[Learn more](#)

**Automated Provisioning**

Keep your Auto Scaling group healthy and balanced, whether you need one instance or 1,000.

[Learn more](#)

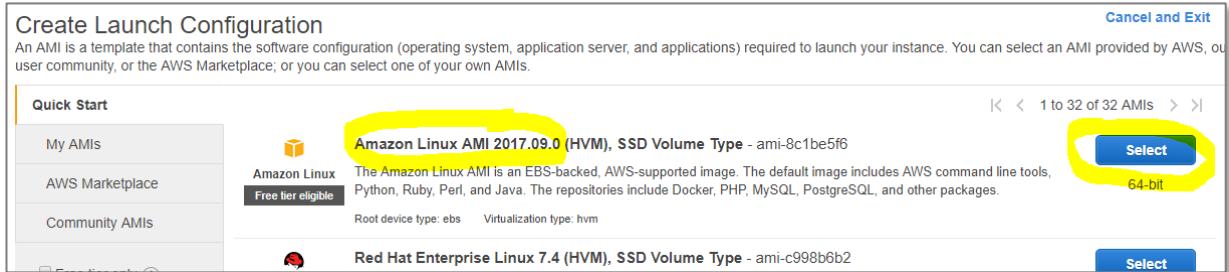
**Adjustable Capacity**

Maintain a fixed group size or adjust dynamically based on Amazon CloudWatch metrics.

[Learn more](#)

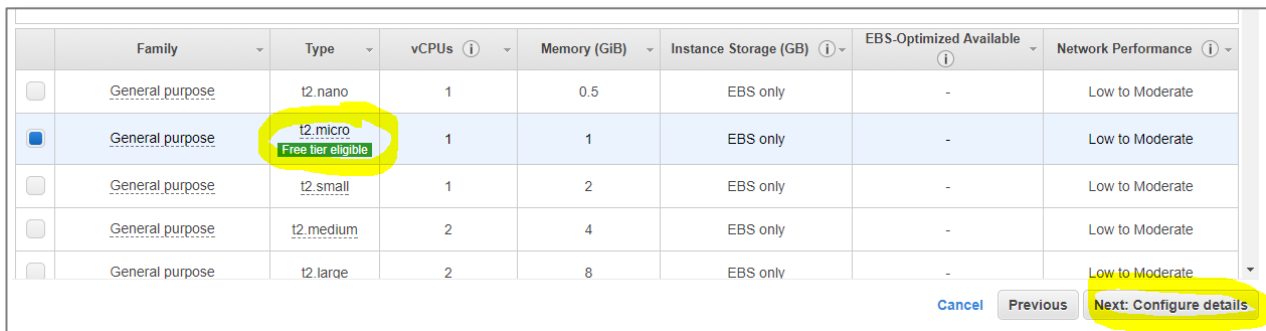
Click “Create launch configuration”

Select the Amazon Linux AMI



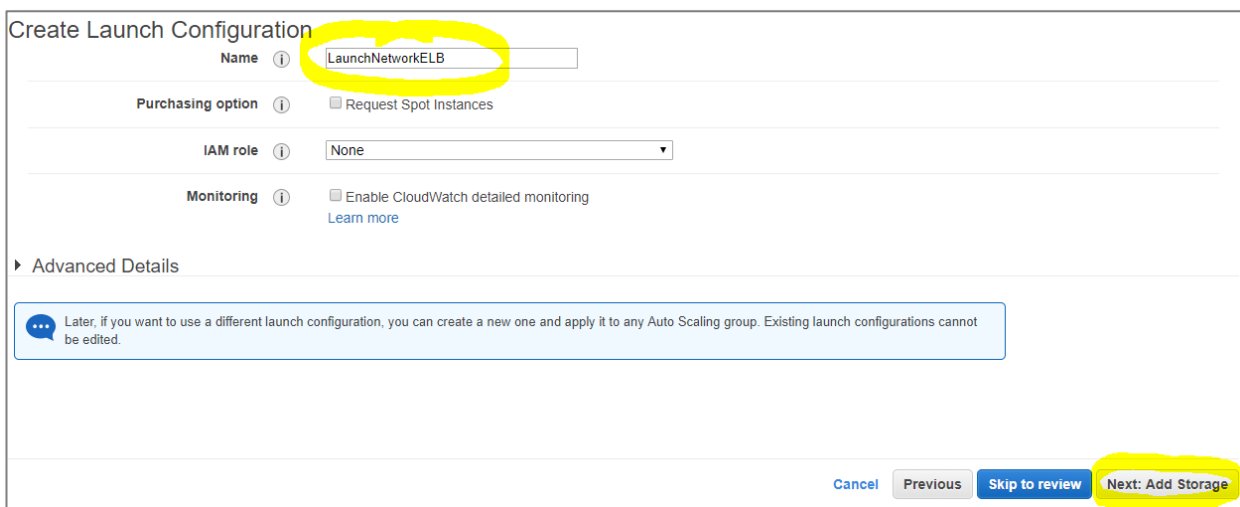
Select t2 micro instance type

Click “Next: Configure details”



Give the Launch Configuration a name

Click “Next: Add Storage”



Click “Next: Configure Security Group”

## Create Launch Configuration

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. <https://docs.aws.amazon.com/console/ec2/launchinstance/storage> about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput	Delete on Termination	Encrypted
Root	/dev/xvda	snap-080eb3cb2eda29974	8	General Purpose (SSD)	100 / 3000	N/A	<input checked="" type="checkbox"/>	No

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Skip to review](#) [Next: Configure Security Group](#)

Select "Create a new security group"

Add a rule for TCP on port 80, source anywhere.

Click "Review"

## Create Launch Configuration

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

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

Security group name: AutoScaling-Security-Group-2  
 Description: AutoScaling-Security-Group-2 (2017-10-19 18:49:49.542+11:00)

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0
Custom TCP Rule	TCP	80	Anywhere 0.0.0.0/0

[Add Rule](#)

### Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review](#)

Click "Create Launch Configuration"



### Create Launch Configuration

Review the details of your launch configuration. You can go back to edit the details of each section before you finish.

**⚠ Improve security of instances launched using your launch configuration, LaunchNetworkELB. Your security group, AutoScaling-Security-Group-2, is open to the world.**

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ **AMI Details** [Edit AMI](#)

**Amazon Linux AMI 2017.09.0 (HVM), SSD Volume Type - ami-8c1be5f6**

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs    Virtualization Type: hvm

▼ **Instance Type** [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory GiB	Instance Storage (GiB)	EBS-Optimized Available	Network Performance

[Cancel](#)   [Previous](#)   [Create launch configuration](#)

Then select a key pair to finish creating the launch configuration.

## Creating an Auto Scaling Group

You will now be presented with the Auto Scaling Group creation page

Give the Group a name

Select the subnets for each availability zone.

**Network**  ⓘ vpc-72d25a0b (172.31.0.0/16) (default) [Create new VPC](#)

**Subnet**  ⓘ

subnet-4770eb4b(172.31.48.0/20) | Default in us-east-1f ✕

subnet-227d386a(172.31.16.0/20) | Default in us-east-1c ✕

subnet-c0a2279a(172.31.32.0/20) | Default in us-east-1d ✕

subnet-a7b38b9b(172.31.64.0/20) | Default in us-east-1e ✕

subnet-d6455ab3(172.31.0.0/20) | Default in us-east-1a ✕

subnet-a9e06d85(172.31.80.0/20) | Default in us-east-1b ✕

[Create new subnet](#)

Each instance in this Auto Scaling group will be assigned a public IP address. ⓘ

Click to expand “Advanced Details”

Select the Target Group we created

Select “ELB” for Health Check Type

Click “Next: Configure scaling policies”

**Advanced Details**

**Load Balancing** *i* ☒ Receive traffic from one or more load balancers [Learn about Elastic Load Balancing](#)

**Classic Load Balancers** *i*

**Target Groups** *i*

**Health Check Type** *i* ☒ ELB ☐ EC2

**Health Check Grace Period** *i*  seconds

**Monitoring** *i* Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration LaunchNetworkELB. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency. [Learn more](#)

**Instance Protection** *i*

[Cancel](#) [Next: Configure scaling policies](#)

Select "Use scaling policies to adjust the capacity of this group"

Scale between 1 and 6 instances.

Target value: 50

Instances need: 300 seconds to warm up after scaling

Click "Review"

**Create Auto Scaling Group**

You can optionally add scaling policies if you want to adjust the size (number of instances) of your group automatically. A scaling policy is a set of instructions for making such adjustments in response to an Amazon CloudWatch alarm that you assign to it. In each policy, you can choose to add or remove a specific number of instances or a percentage of the existing group size, or you can set the group to an exact size. When the alarm triggers, it will execute the policy and adjust the size of your group accordingly. [Learn more](#) about scaling policies.

☐ Keep this group at its initial size

☒ Use scaling policies to adjust the capacity of this group

Scale between  and  instances. These will be the minimum and maximum size of your group.

**Scale Group Size** *x*

**Name:**

**Metric type:**

**Target value:**

**Instances need:**  seconds to warm up after scaling

**Disable scale-in:** ☐

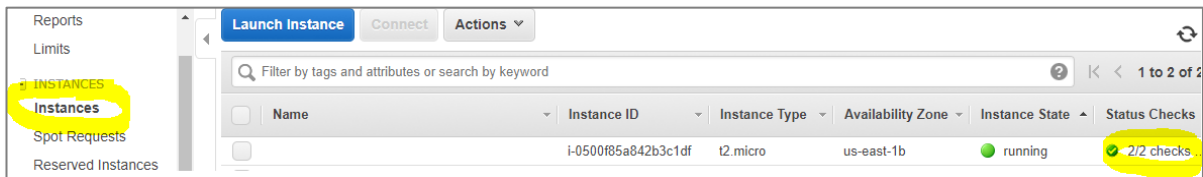
[Scale the Auto Scaling group using step or simple scaling policies](#) *i*

[Cancel](#) [Previous](#) [Review](#) [Next: Configure Notifications](#)

Click "Create Auto Scaling Group"

Select Instances and you will eventually see an EC2 instance being launched by the Auto Scaling Group.

Wait the until Status Checks have been completed.

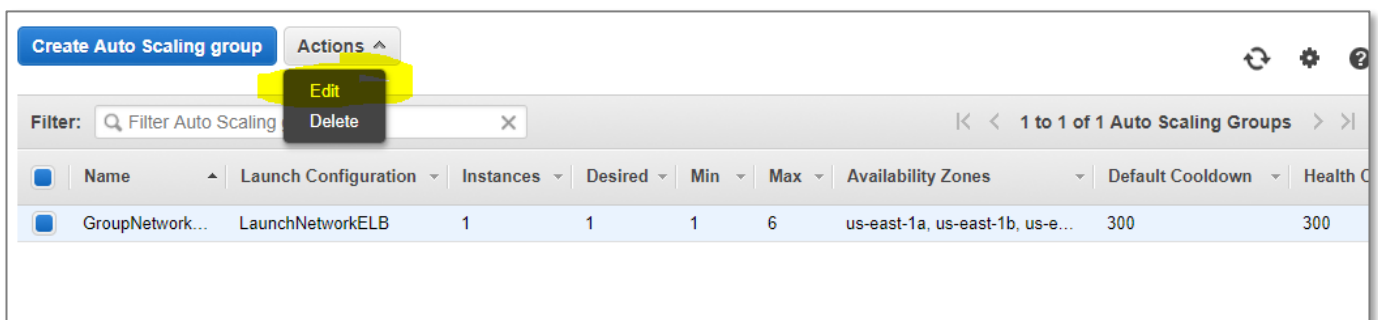


## Adding the Auto Scaling Group to an ELB Target Group

Go back to the Auto Scaling page

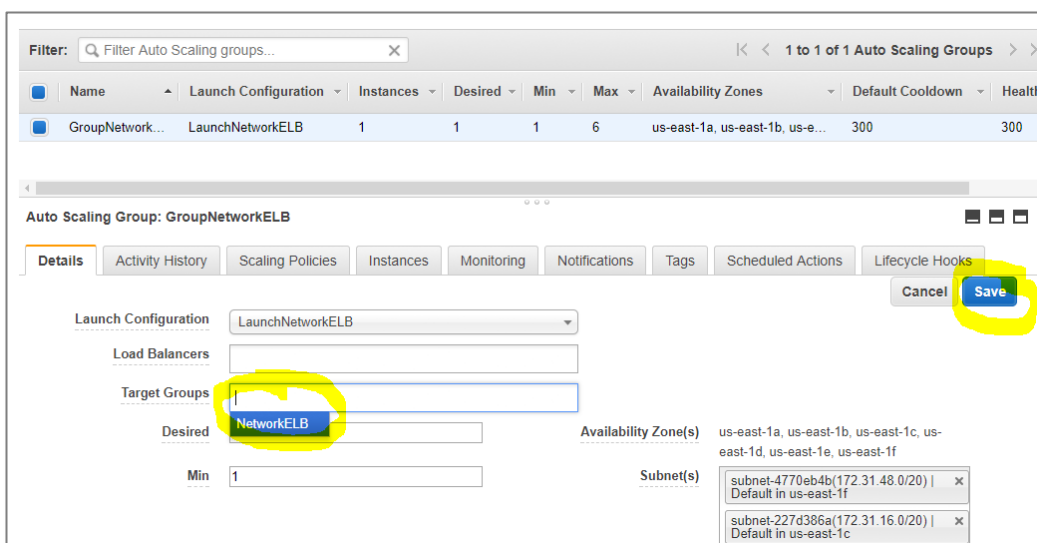
Select the Auto Scaling Group

Select "Actions" "Edit"

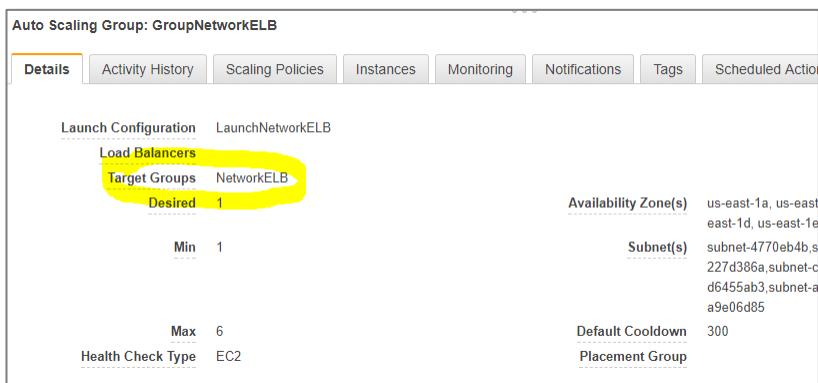


Select the Target Group we created in the "target Groups" field

Click "Save"



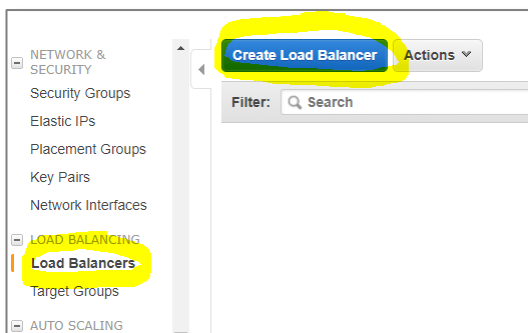
The Target Group will now be added to the Auto Scaling Group



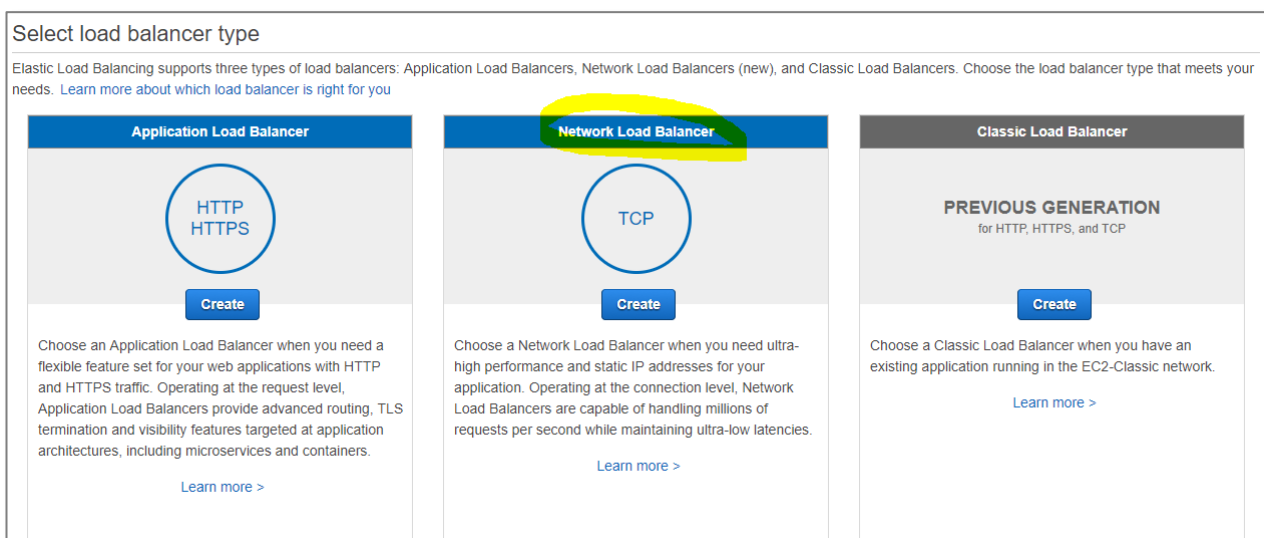
## Creating a Network ELB

Select “Load Balancers”

Click “Create Load Balancer”



Select “Network Load Balancer”



## Give the Load Balancer a name

1. Configure Load Balancer 2. Configure Routing 3. Register Targets 4. Review

### 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 network with a listener that receives TCP traffic on port 80.

**Name** ⓘ

**Scheme** ⓘ ☒ internet-facing ☐ internal

#### 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
TCP	80

[Add listener](#)

## Select all Availability Zones

## Click “Next: Configure Routing”

### 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 may also add one Elastic IP per Availability Zone if you wish to have specific addresses for your load balancer.

[Click here](#) to manage your Elastic IPs.

**VPC** ⓘ

<input type="checkbox"/>	Availability Zone	Subnet ID	Subnet IPv4 CIDR	Elastic IP	Name
<input checked="" type="checkbox"/>	us-east-1a	subnet-d6455ab3	172.31.0.0/20	<input type="text"/>	
<input checked="" type="checkbox"/>	us-east-1b	subnet-a9e06d85	172.31.80.0/20	<input type="text"/>	
<input checked="" type="checkbox"/>	us-east-1c	subnet-227d386a	172.31.16.0/20	<input type="text"/>	
<input checked="" type="checkbox"/>	us-east-1d	subnet-c0a2279a	172.31.32.0/20	<input type="text"/>	
<input checked="" type="checkbox"/>	us-east-1e	subnet-a7b38b9b	172.31.64.0/20	<input type="text"/>	
<input checked="" type="checkbox"/>	us-east-1f	subnet-4770eb4b	172.31.48.0/20	<input type="text"/>	

Tags

[Cancel](#) [Next: Configure Routing](#)

## Select the existing “NetworkELB” Target Group we created previously.

## Click “Next: Register Targets”

## Step 2: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

### Target group

Target group	Existing target group
Name	NetworkELB
Protocol	TCP
Port	80
Target type	Instance

### Health checks

Protocol	TCP
----------	-----

► Advanced health check settings

Cancel Previous **Next: Register Targets**

You will see the EC2 instance created by the Auto Scaling has been automatically added to the Target Group.

Click "Next: Review"

## Step 3: Register Targets

### Configure Security Groups

The security groups for your instances must allow traffic from the VPC CIDR on the health check port.

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

The following targets are registered with the target group that you selected. You can only modify this list after you create the load balancer.

Instance	Port
i-08566ff43927b9813	80

Cancel Previous **Next: Review**

Click "Create"

### Step 4: Review

Please review the load balancer details before continuing

▼ Load balancer

Name

TestNetworkELB

Scheme

internet-facing

Listeners

Port:80 - Protocol:TCP

VPC

vpc-72d25a0b

Subnets

subnet-d6455ab3, subnet-a9e06d85, subnet-227d386a, subnet-c0a2279a, subnet-a7b38b9b, subnet-4770eb4b

Tags

▼ Routing

Target group

Existing target group

Target group name

NetworkELB

Port

80

Target type

instance

Protocol

TCP

Health check protocol

TCP

Health check port

traffic port

Healthy threshold

3

Cancel

Previous

Create

You can now see your Network ELB listed.

Click on the ELB and select the "Listeners" tab.

You can now see the listener is forwarding requests to the Target Group.

Click on the target group.

Create Load Balancer

Actions ▼

Filter: Search

< > 1 to 1 of 1

<input type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type
<input checked="" type="checkbox"/>	TestNetworkELB	TestNetworkELB-5591d273f...	provisioning	vpc-72d25a0b	us-east-1d, us-east-1f, ...	net

Load balancer: TestNetworkELB

Description

Listeners

Monitoring

Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

Add listener

Actions ▼

<input type="checkbox"/>	Listener protocol	Listener port	Default action	Listener ARN
<input type="checkbox"/>	TCP	80	Forward to NetworkELB	arn...5b5ce086b473c265

Select the "Targets" tab

You will see an instance is registered with the ELB.

\* Please note the instance will be marked as unhealthy because no application is running on the instance to respond to the TCP requests.

Filter:

Name	Port	Protocol	Target type	VPC ID	Monitoring
NetworkELB	80	TCP	instance	vpc-72d25a0b	

Target group: NetworkELB

Description Targets Health checks Monitoring Tags

The load balancer starts routing requests to a newly registered target as soon as the registration process completes and the target passes the initial health checks. If demand on your targets increases, you can register additional targets. If demand on your targets decreases, you can deregister targets.

Edit

None of these Availability Zones contains a healthy target. Requests are being routed to all targets.

Registered targets

Instance ID	Name	Port	Availability Zone	Status
i-0a2125280962dade0		80	us-east-1f	unhealthy

## Clean Up

We will now delete the resources.

First delete the ELB

Placement Groups

Key Pairs

Network Interfaces

LOAD BALANCING

Load Balancers

Target Groups

AUTO SCALING

Launch

Configurations

Create Load Balancer

Filter:

Name

TestNetworkELB

State

active

VPC ID

vpc-72d25a0b

Actions

- Delete
- Edit health check
- Edit subnets
- Edit IP address type
- Edit instances
- Edit listeners
- Edit security groups

Now delete the Target group

Placement Groups

Key Pairs

Network Interfaces

LOAD BALANCING

Load Balancers

Target Groups

AUTO SCALING

Launch

Configurations

Create target group

Filter:

Name

NetworkELB

Protocol

TCP

Target type

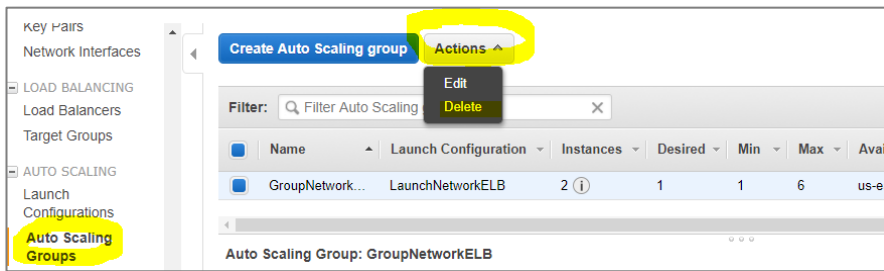
instance

Actions

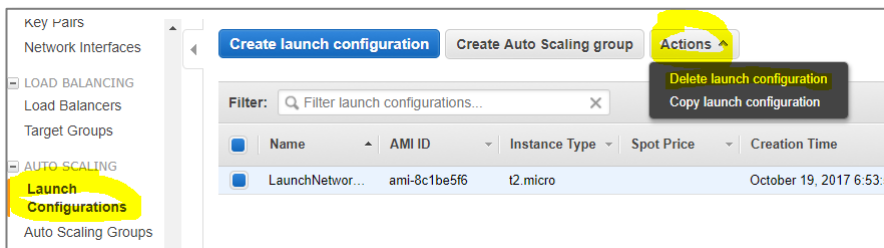
- Edit health check
- Register and deregister targets
- Edit attributes
- Delete

Now delete the Auto Scaling group





Now delete the Launch Configuration



Check that the instances are terminating.

