

Lab 4: Amazon EC2 and Load Balancing

Tutorial and Instructions

Type your answers and paste your screenshots directly in Lab4_Submission_File.docx in the indicated spots. Save the file with a filename in this format Lab4_*FirstName_LastName*.docx and upload it to D2L.

When asked to paste screenshots, please format screenshot so that your toolbar and system time are visible.

1. Setting up with Amazon EC2

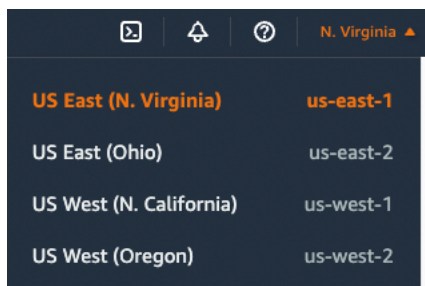
A. Create a Key Pair

AWS uses public-key cryptography to secure the login information for your instance. You specify the name of the key pair when you launch your instance, then provide the private key to obtain the administrator password for your Windows instance so you can log in using RDP (Remote Desktop Protocol).

If you haven't created a key pair already, you can create one using the Amazon EC2 console.

To Create a Key Pair

1. Sign in to AWS using your AWS Academy Account.
2. From the AWS dashboard, choose **EC2** to open the Amazon EC2 console.
3. From the navigation bar, select a region for the key pair. You can select any region that's available to you, regardless of your location (Our AWS Academy account may only allow US East N. Virginia us-east-1). The key pairs are specific to a region; for example, if you plan to launch an instance in the US East (N. Virginia) Region, you must create a key pair for the instance in the US East (N. Virginia) Region. Go to top right corner and you will see the below screenshot.



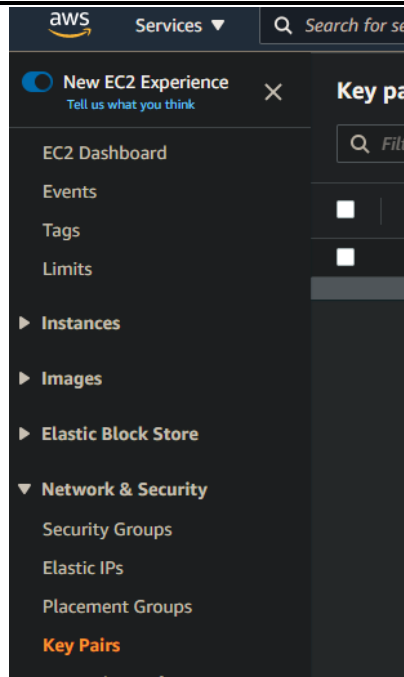
4. In the navigation pane, under **NETWORK & SECURITY**, click **Key Pairs**.

Tip

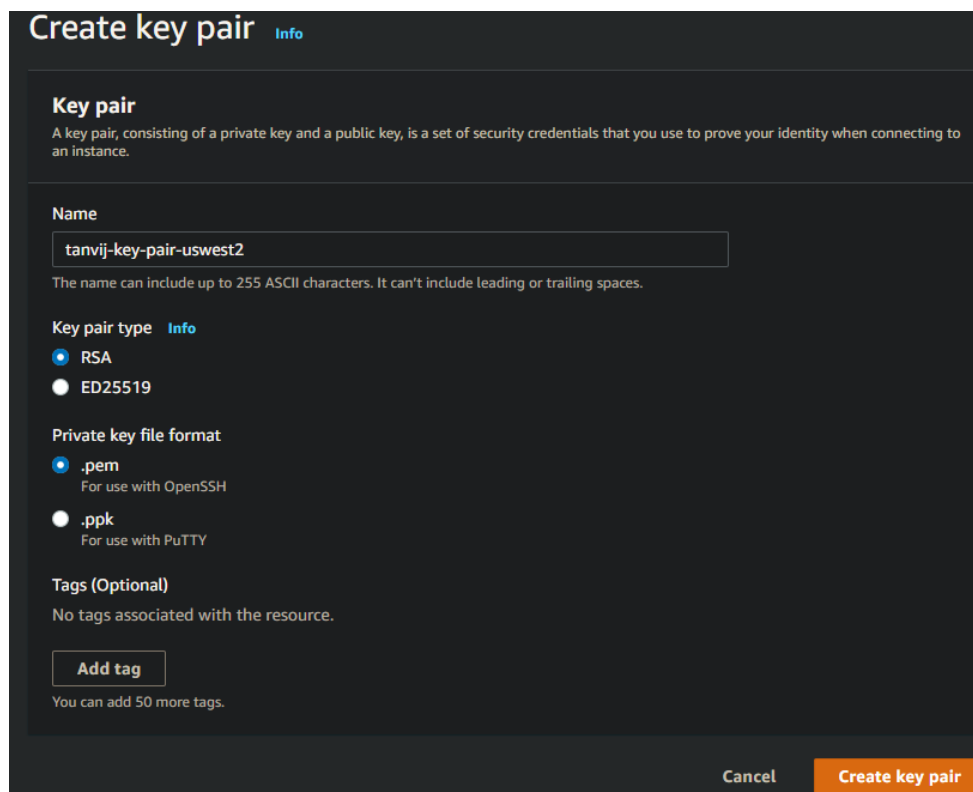
The navigation pane is on the left side of the console. If you do not see the pane, it might be minimized; click the arrow to expand the pane. You may have to scroll down to see the **Key Pairs** link.

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing



5. Click **Create Key Pair**.
6. Enter a name for the new key pair in the **Key pair name** field of the **Create Key Pair** dialog box, and then click **Create**. Choose a name that is easy for you to remember, such as your <NetID>, followed by -key-pair, plus the region name. For example, *netid-key-pair-useast1*.

A screenshot of the 'Create key pair' dialog box in the AWS Management Console. The title is 'Create key pair' with an 'Info' link. Below the title, there's a section 'Key pair' with a description: 'A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.' The 'Name' field contains 'tanvij-key-pair-uswest2'. Below the field, a note states: 'The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.' The 'Key pair type' section has two options: 'RSA' (selected with a blue radio button) and 'ED25519'. The 'Private key file format' section has two options: '.pem' (selected with a blue radio button, with the note 'For use with OpenSSH') and '.ppk' (with the note 'For use with PuTTY'). The 'Tags (Optional)' section states 'No tags associated with the resource.' and has an 'Add tag' button. At the bottom right, there are 'Cancel' and 'Create key pair' buttons.

Lab 4: Amazon EC2 and Elastic Load Balancing

- The private key file is automatically downloaded by your browser. The base file name is the name you specified as the name of your key pair, and the file name extension is”. **pem”** (**.cer on Mac**). Save the private key file in a safe place.

Important

This is the only chance for you to save the private key file. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

Key pairs (1) [Info](#)

Q Search

| <input type="checkbox"/> | Name | Type | Created | Fingerprint |
|--------------------------|---------------------------|------|------------------------|-------------------|
| <input type="checkbox"/> | weichen-keypair-us-east-1 | rsa | 2022/10/03 21:44 GMT-7 | 9b:5c:88:0c:65:46 |

Paste the Screenshot showing Key Pair Generated

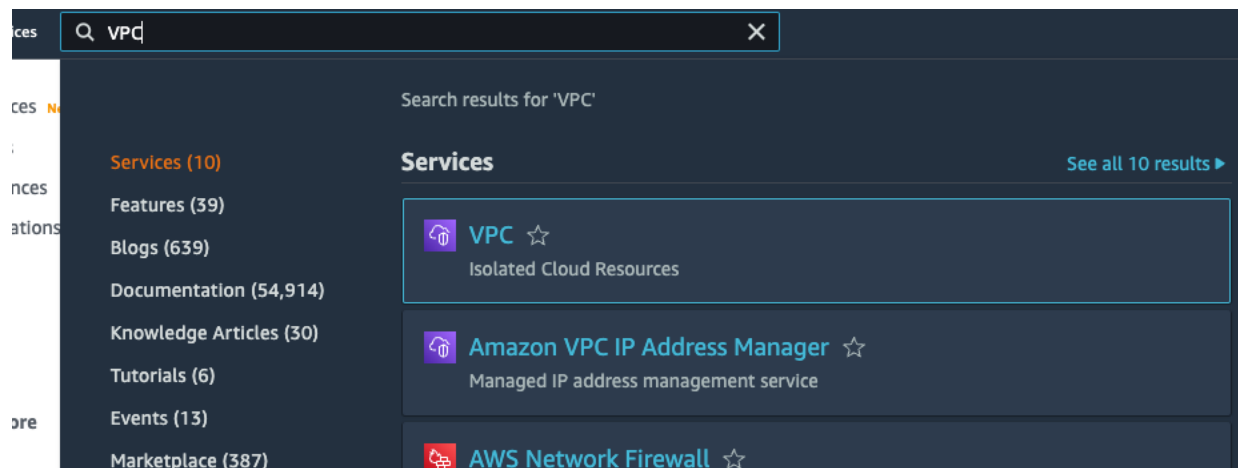
<<INSERT SCREENSHOT>>

B. Create a Virtual Private Cloud (VPC)

Amazon VPC enables you to launch AWS resources into a virtual network that you've defined. A Default VPC is already created, but we are creating a manual VPC.

To create a nondefault VPC

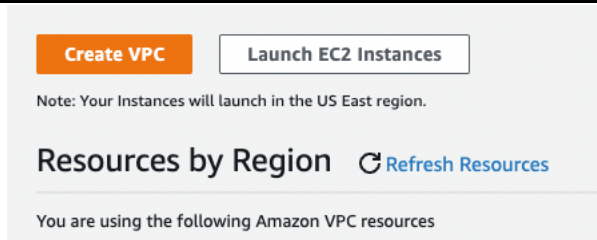
- Open the Amazon VPC console by searching for VPC in the search bar.



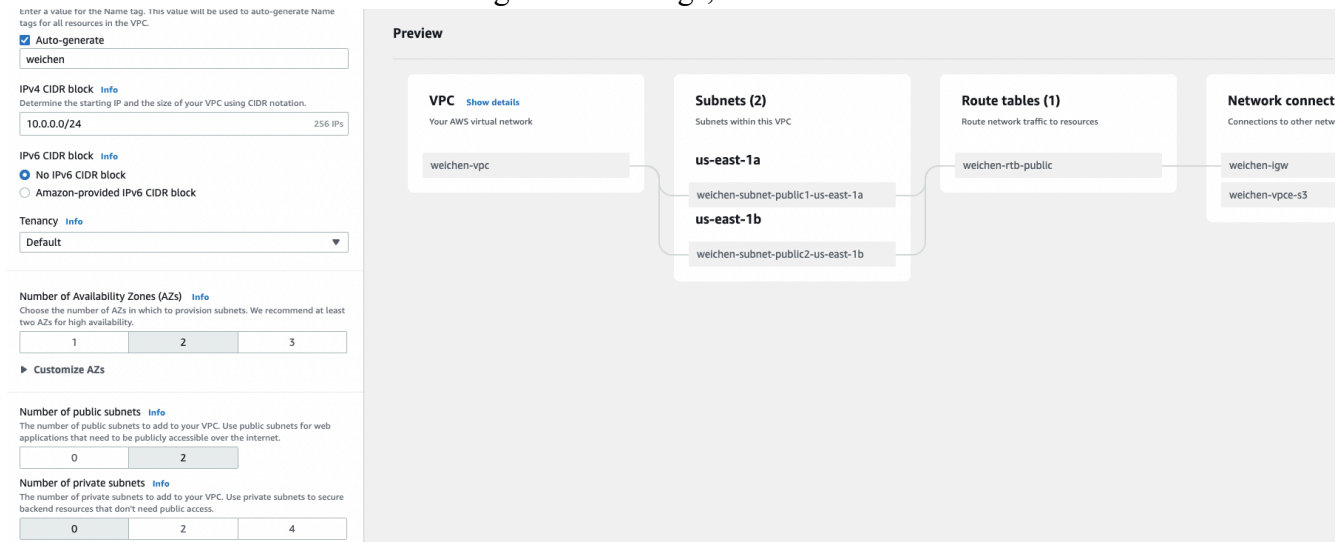
- From the navigation bar, select a region for the VPC. **VPCs are specific to a region, so you should select the same region in which you created your key pair.**
- On the VPC dashboard, click **Create VPC**.

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing



- On the **Create VPC** page, ensure that **VPC and more** is selected, and enter your netid for the **Auto-generate** name tag.
- Change your **IPv4 CIDR block** to 10.0.0.0/24, and ensure that we have 2 **public subnets**, and 0 **private subnets**. Leave the other default configuration settings, and click **Create VPC**.



Paste the Screenshot showing VPC

<<INSERT SCREENSHOT>>

Check subnets in different availability zones

- Select Subnets in VPC Dashboard. You will find the two subnets 10.0.0.0/28 and 10.0.0.16/28. Note that the first one was created in the Availability Zone us-east-1a, and the second one was created in the Availability Zone us-east-1b.

| Subnets (1/8) <small>Info</small> | | | | | | | | | |
|---|--------------------------|-----------|--------------------------------|----------------|---------|--------------------------|-------------------|--|--|
| <input type="text" value="Filter subnets"/> | | | | | | | | | |
| Name | Subnet ID | State | VPC | IPv4 CIDR | IPv6... | Available IPv4 addresses | Availability Zone | | |
| – | subnet-0d8bcbf5de089e558 | Available | vpc-00cdcd54eca03c94f | 172.31.0.0/20 | – | 4091 | us-east-1c | | |
| – | subnet-0a67cdf8fe2db21eb | Available | vpc-00cdcd54eca03c94f | 172.31.64.0/20 | – | 4091 | us-east-1f | | |
| – | subnet-06e9ae3a72d2d67d6 | Available | vpc-00cdcd54eca03c94f | 172.31.32.0/20 | – | 4091 | us-east-1b | | |
| – | subnet-0c5bccdf93aa7bf9f | Available | vpc-00cdcd54eca03c94f | 172.31.48.0/20 | – | 4091 | us-east-1e | | |
| weichen-subnet-public1-us-ea... | subnet-04461e01235d035a1 | Available | vpc-0e13244d663bbfe05 wel... | 10.0.0.0/28 | – | 11 | us-east-1a | | |
| weichen-subnet-public2-us-east-1b | subnet-05112d5f48f5b7240 | Available | vpc-0e13244d663bbfe05 wel... | 10.0.0.16/28 | – | 11 | us-east-1b | | |

Paste the Screenshot showing both your subnets in two different availability zones

<<INSERT SCREENSHOT>>

C. Create a Security Group

Security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level. You must add rules to a security group that enable you to connect to your instance from your IP address using RDP (Remote Desktop Protocol). You can also add rules that allow inbound and outbound HTTP and HTTPS access from anywhere.

Prerequisites

You'll need the public IPv4 address of your local computer. The security group editor in the Amazon EC2 console can automatically detect the public IPv4 address for you. Alternatively, you can use the search phrase "what is my IP address" in an Internet browser.

To create a security group with least privilege

1. From the navigation bar, select a region for the security group. Security groups are specific to a region, so you should select the same region in which you created your key pair (e.g., us-east-1).
2. Click **Security Groups** in the navigation pane.
3. Click **Create Security Group**.
4. Enter a name for the new security group and a description. Choose a name that is easy for you to remember, such as your <NetID> name, followed by _SG_, plus the region name. For example, *netid_SG_virginia*.
5. In the **VPC** list, select your VPC.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields:

Basic details

Security group name [Info](#)
weichen_SG_virginia
Name cannot be edited after creation.

Description [Info](#)
Security Group Virginia

VPC [Info](#)
vpc-0e13244d663bbfe05 (weichen-vpc)
10.0.0.0/24

6. Select the security group you created and on the **Inbound** tab, create the following rules (click **Add Rule** for each new rule), and then click **Create Security Group**:
 - Select **HTTP** from the **Type** list, and make sure that **Source** is set to **Anywhere-IPv4** (0.0.0.0/0).
 - Select **HTTPS** from the **Type** list, and make sure that **Source** is set to **Anywhere-IPv4** (0.0.0.0/0).

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

- Select **RDP** from the **Type** list. Choose **My IP** to specify your public IPv4 addresses in CIDR notation (You will need to update it just in case the next time your router obtains a different public IP).

Inbound rules [Info](#)

| Type Info | Protocol Info | Port range Info | Source Info |
|---------------------------|-------------------------------|---------------------------------|-----------------------------|
| HTTP | TCP | 80 | Anywhere... 0.0.0.0/0 |
| HTTPS | TCP | 443 | Anywhere... 0.0.0.0/0 |
| RDP | TCP | 3389 | My IP 24.11.144.58/32 |

Security Groups (3) [Info](#) [Refresh](#) [Actions](#) [Export security groups to CSV](#) [Create](#)

Filter security groups

| <input type="checkbox"/> | Name | Security group ID | Security group name | VPC ID | Description | Owner | Inbound rules count |
|--------------------------|------|----------------------|---------------------|-----------------------|-------------------------|--------------|----------------------|
| <input type="checkbox"/> | - | sg-03a4259f5eda97a09 | weichen_SG_virginia | vpc-0e13244d663bbfe05 | Security Group Virginia | 279035175453 | 3 Permission entries |

Paste the Screenshot showing security Group
<<INSERT SCREENSHOT>>

2. Launching an EC2 Instance

A. Launch an Instance

You can launch a Windows instance using the AWS Management Console as described in the following procedure.

1. Open the Amazon EC2 console through the Services menu or search bar.
2. From the console dashboard, choose **Launch Instance**.
3. Name it as <NetID>-server-1.
4. For the **Application and OS Images** (Amazon Machine Image), choose Windows, which will install Microsoft Windows Server 2022 Base. Notice that this AMI is marked "Free tier eligible."

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

Name and tags [Info](#)

Name


[Add additional tags](#)

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)


An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Quick Start


Amazon Linux




macOS




Ubuntu



Windows




Red Hat



S

>



Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

ami-0f1ee03d06c4c659c (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

- On the **Instance Type** dropdown menu, you can select the hardware configuration of your instance. Select the *t2.micro* type, which is selected by default.
- On the **Key pair (login)** item, choose the key pair that you have created.

▼ **Instance type** [Info](#)

Instance type

t2.micro

Free tier eligible

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

▼


[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 - required

▼



[Create new key pair](#)

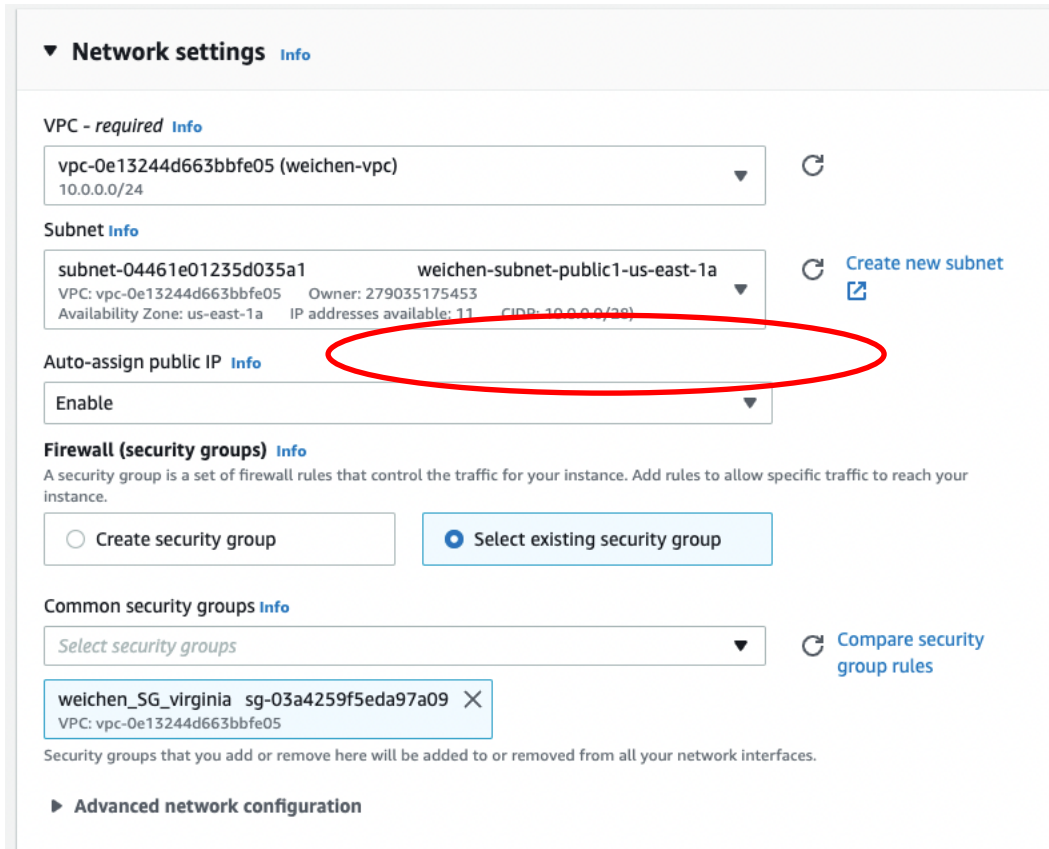
For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

Page 7 of 22

Caution

Don't select the **Proceed without a key pair** option. If you launch your instance without a key pair, then you can't connect to it.

- Click **Edit** for the **Network settings**. Change VPC to your non-default VPC, which you have created earlier. Change “Subnet” to **the first subnet** (weichen-subnet-public1-us-east-1a in my case. Second instance to the second subnet). Change “Auto-Assign Public IP” to **Enable**.
- Under **Firewall (security groups)**, choose **Select existing security group**, and select the security group that you have created earlier.



Network settings [Info](#)

VPC - required [Info](#)

vpc-0e13244d663bbfe05 (weichen-vpc)
10.0.0.0/24

Subnet [Info](#)

subnet-04461e01235d035a1 weichen-subnet-public1-us-east-1a
VPC: vpc-0e13244d663bbfe05 Owner: 279035175453
Availability Zone: us-east-1a IP addresses available: 11 (CIDR: 10.0.0.0/26)

Auto-assign public IP [Info](#)

Enable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group ☒ Select existing security group

Common security groups [Info](#)

Select security groups

weichen_SG_virginia sg-03a4259f5eda97a09 X
VPC: vpc-0e13244d663bbfe05

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

- On the **Summary** pane, choose **Launch instance**.
- A confirmation page lets you know that your instance is launching. Choose **View Instances** to close the confirmation page and return to the console.

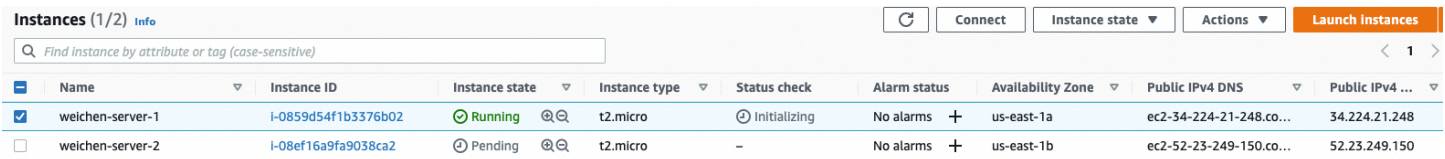
| Instances (1) Info | | | | | | | | | |
|--|------------------|---------------------|----------------|---------------|--------------|--------------|-------------------|-------------------------|-----------------|
| Find instance by attribute or tag (case-sensitive) | | | | | | | | | |
| <input type="checkbox"/> | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... |
| <input type="checkbox"/> | weichen-serve... | i-0859d54f1b3376b02 | Pending | t2.micro | - | No alarms | us-east-1a | ec2-34-224-21-248.co... | 34.224.21.248 |

- On the **Instances** screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is `pending`. After the instance starts, its state changes to `running` and it receives a public DNS name. (If the **Public DNS (IPv4)** column is hidden, choose the Show/Hide icon in the top right corner of the page and then select **Public DNS (IPv4)**.)

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

- It can take up to 5 minutes for the instance to be ready so that you can connect to it. Check that your instance has passed its status checks; you can view this information in the **Status Checks** column.
- Repeat the above steps to create a second instance. **Remember to create it in a different subnet.**



The screenshot shows the Amazon EC2 console 'Instances' page. At the top, there are buttons for 'Connect', 'Instance state', 'Actions', and a red 'Launch Instances' button. Below these is a search bar and a table of instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, and Public IPv4 ...

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... |
|------------------|---------------------|----------------|---------------|--------------|--------------|-------------------|-------------------------|-----------------|
| weichen-server-1 | i-0859d54f1b3376b02 | Running | t2.micro | Initializing | No alarms | us-east-1a | ec2-34-224-21-248.co... | 34.224.21.248 |
| weichen-server-2 | i-08ef16a9fa9038ca2 | Pending | t2.micro | - | No alarms | us-east-1b | ec2-52-23-249-150.co... | 52.23.249.150 |

Paste the Screenshot showing EC2 Instances

<<INSERT SCREENSHOT>>

B. Connect to Your Instance

To connect to a Windows instance, you must retrieve the initial administrator password and then specify this password when you connect to your instance using Remote Desktop.

The name of the administrator account depends on the language of the operating system. For example, for English, it's Administrator, for French it's Administrateur, and for Portuguese it's Administrador.

To connect to your Windows instance using an RDP client



- In the Amazon EC2 console, select the instance, and then choose **Connect**.
- In the **Connect to Instance** page, choose the **RDP client** tab. If you are on a Mac, you will need to download the Microsoft Remote Desktop app from the App Store (it is free).
- Click **Get password** at the bottom of the page (it will take a few minutes after the instance is launched before the password is available).
- Choose **Upload private key file** and navigate to the private key file you created when you launched the instance. Select the file and choose **Open** to copy the entire contents of the file into the **Contents** field.
- Choose **Decrypt Password**. The console displays the default administrator password for the instance in the **Connect to Your Instance** dialog box, replacing the link to **Get Password** shown previously with the actual password.
- Record the default administrator password, or copy it to the clipboard. You need this password to connect to the instance.


MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

Connect to instance [Info](#)
Connect to your instance i-0859d54f1b3376b02 (weichen-server-1) using any of these options


[Session Manager](#) | **RDP client** | [EC2 serial console](#)

 You may not be able to connect to this instance as ports 3389 may need to be open in order to be accessible. The current associated security groups don't have ports 3389 open. 


Instance ID
 **i-0859d54f1b3376b02** (weichen-server-1)

Connection Type


☒ **Connect using RDP client**
Download a file to use with your RDP client and retrieve your password.


☐ **Connect using Fleet Manager**
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#) 


You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

 **Download remote desktop file**

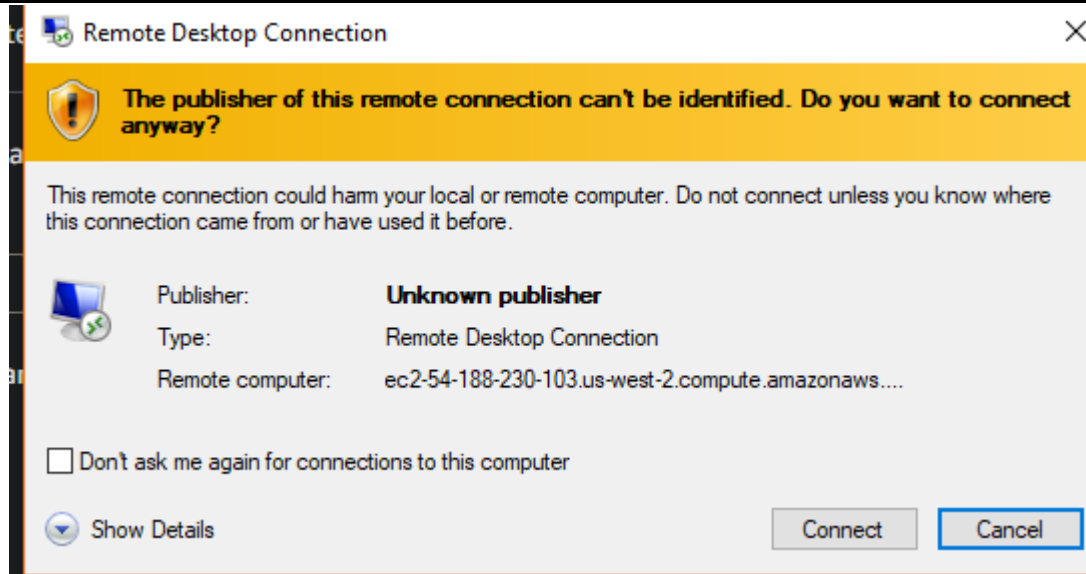
When prompted, connect to your instance using the following details:

Public DNS
 **ec2-34-224-21-248.compute-1.amazonaws.com**

User name
 **Administrator**

Password
 **pNW&LDYrXAHFqZO94uEEVvy7RHGDd\$y{**

7. Choose **Download Remote Desktop File**. Your browser prompts you to either open or save the .rdp file. Either option is fine. When you have finished, you can choose **Close** to dismiss the **Connect to Your Instance** dialog box.
 - If you opened the .rdp file, you'll see the **Remote Desktop Connection** dialog box.
 - If you saved the .rdp file, navigate to your downloads directory, and open the .rdp file to display the dialog box.
8. You may get a warning that the publisher of the remote connection is unknown. If you are using **Remote Desktop Connection** from a Windows PC, choose **Connect** to connect to your instance. If you are using **Microsoft Remote Desktop** on a Mac, skip the next step.

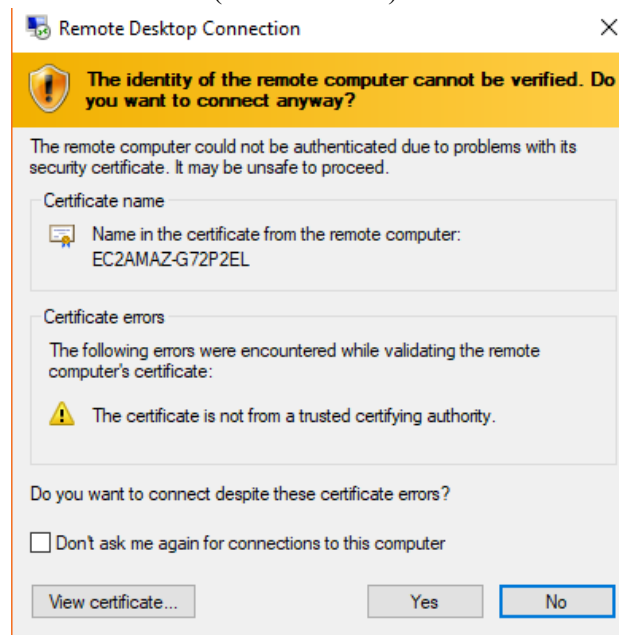


9. When prompted, log in to the instance, using the administrator account for the operating system and the password that you recorded or copied previously. If your **Remote Desktop Connection** already has an administrator account set up, you might have to choose the **Use another account** option and enter the user name and password manually.

Note

Sometimes copying and pasting content can corrupt data. If you encounter a "Password Failed" error when you log in, try typing in the password manually.


10. Due to the nature of self-signed certificates, you may get a warning that the security certificate could not be authenticated. Use the following steps to verify the identity of the remote computer, or simply choose **Yes** or **Continue** to continue if you trust the certificate (recommended).

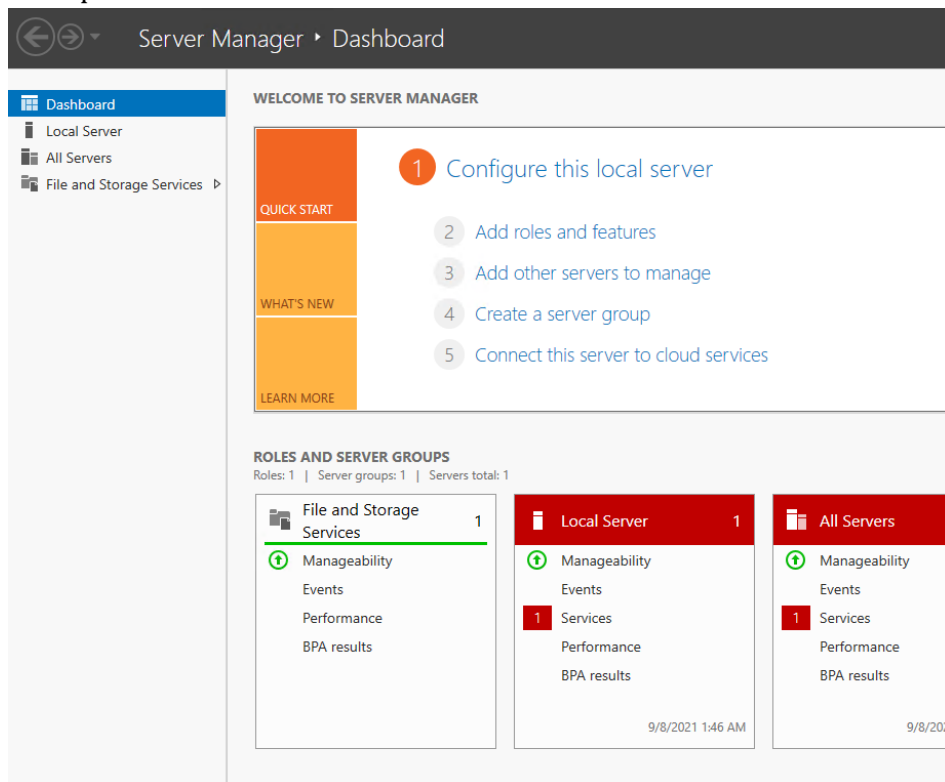


C. Setup the Internet Information Services (IIS)

You need to download Remote Desktop File for each instance. Here, I have explained the steps for 1st instance. You need to repeat the process for 2nd instance too.

These Steps would be repeated twice:

1. Click on the Remote Desktop File. You might need to wait for few minutes till the RDP Client load its profile.
2. Open the “Start” Menu or click on  and search for “Server Manager.” In the Top-Right, you will Click on “Manage,” and then “Add Roles and Features.”
 - You Might get a dialog box stating “Server Manager is collecting inventory data”(This happens because the Server Manager has not fully loaded). Click on OK. Wait for the Server Manager to load all its profile.

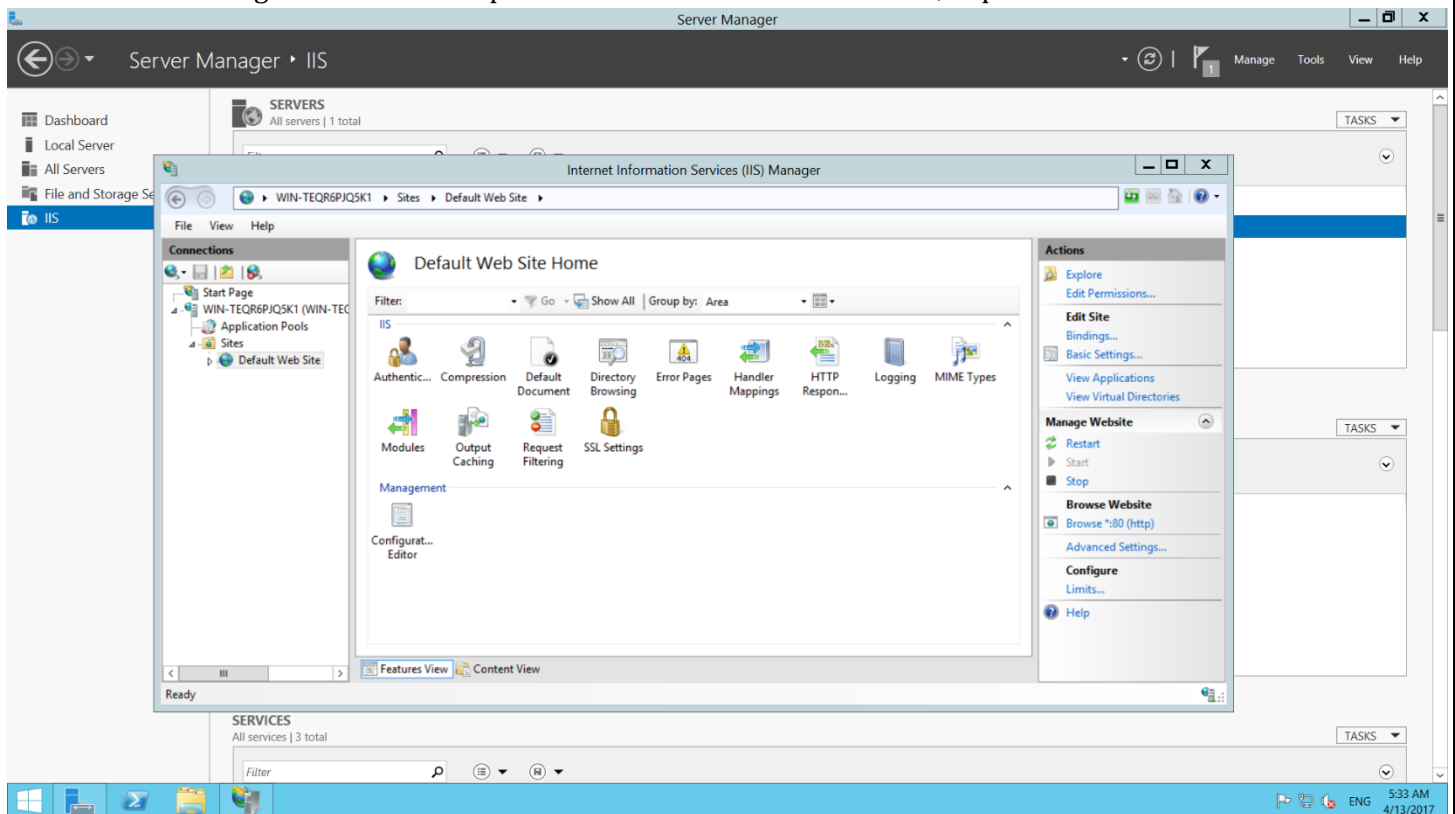


3. Click on Next in “Before you Begin.” In Installation type, “Role based or feature-based installation” is selected. In Server Selection, leave the default value and Click on Next.
4. In Server Role, scroll down and Select Web Server (IIS) and Click Add Features.
5. Leave the default values as it is and Click on Next till you reach “Confirmation”.
6. Click on Install to start the process.
7. After the installation is done, Click on IIS on the navigation pane.
8. Right Click on Server Name and Open Internet Information Services (IIS) Manager.

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

9. Go to the Navigation Pane and expand the content of IIS Server. Then, Expand the “Sites”



10. Right Click on **Default Web Site** and navigate to Explore. Delete the HTML Document “iisstart” and Copy paste the Index.html (Pay attention to the file extension. It may not be visible). Open the file in **Notepad**.
11. Replace the content with:

```
<html>
<body>
<p>Hello, <your_UA_Net_id>!</p>
<p>I am from MIS 543 AWS Lab 4</p>
<p>Machine 1 or 2</p>
</body>
</html>
```

Note: You will copy and paste “Index.html” for each Instance. Please specify for which instance this file belongs to. Is it for Machine 1(corresponds to first instance) or Machine 2(corresponds to second instance) (Highlighted in yellow). This step is necessary because load balancer routes the traffic to either 1st or 2nd instance (web page).

12. **Save** the changes.
13. Now, go back to your EC2 Instance Window, and copy the string from **Public DNS name** (for example, ec2-54-200-87-74.us-west-2.compute.amazonaws.com) and paste it into the address field of an Internet-connected web browser. If IIS is working, you see the default page of your server.

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

Instances (1/2) [Info](#)

| Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 ... |
|--|---------------------|----------------------|---------------|--------------------------------|--------------|-------------------|-------------------------|-----------------|
| <input checked="" type="checkbox"/> weichen-server-1 | i-0859d54f1b3376b02 | Running | t2.micro | 2/2 checks passed | No alarms | us-east-1a | ec2-34-224-21-248.co... | 34.224.21.248 |
| <input type="checkbox"/> weichen-server-2 | i-08ef16a9fa9038ca2 | Running | t2.micro | 2/2 checks passed | No alarms | us-east-1b | ec2-52-23-249-150.co... | 52.23.249.150 |

Instance: i-0859d54f1b3376b02 (weichen-server-1)

☐ i-0859d54f1b3376b02 (weichen-server-1)

IPv6 address
-

Hostname type
IP name: ip-10-0-0-12.ec2.internal

Answer private resource DNS name
IPv4 (A)

Auto-assigned IP address
☐ 34.224.21.248 [Public IP]

☐ 34.224.21.248 | [open address](#)

Instance state
Running

Private IP DNS name (IPv4 only)
☐ ip-10-0-0-12.ec2.internal

Instance type
t2.micro

VPC ID
☐ vpc-0e13244d663bbfe05 (weichen-vpc)

Public IPv4 DNS copied

☐ ec2-34-224-21-248.compute-1.amazonaws.com | [open address](#)

Elastic IP addresses
-

AWS Compute Optimizer finding
☐ [View findings](#)

← → ↻ ⚠ Not Secure | ec2-34-224-21-248.compute-1.amazonaws.com

Hello, weichen!

I am from MIS 543 AWS Lab 4

Machine 1

← → ↻ ⚠ Not Secure | ec2-52-23-249-150.compute-1.amazonaws.com

Hello, weichen!

I am from MIS 543 AWS Lab 4

Machine 2

Paste the Screenshot of the default page for **both** of the machines
<<INSERT SCREENSHOT>>

3. Application Load Balancer

A. Create Application Load Balancer

1. Open the Amazon EC2 console.
2. On the navigation bar, choose a region for your load balancer. Be sure to select the same region that you selected for your EC2 instances.
3. On the navigation pane, under **LOAD BALANCING**, choose **Load Balancers**.
4. Choose **Create Load Balancer**.
5. Choose **Application Load Balancer**, and then choose **Create**.

B. Define Your Load Balancer

You must provide a basic configuration for your load balancer, such as a name, a network, and a listener.

A listener is a process that checks for connection requests. It is configured with a protocol and a port for front-end (client to load balancer) connections and a protocol and a port for back-end (load balancer to instance) connections. In this, you configure a listener that accepts HTTP requests on port 80 and sends them to your instances on port 80 using HTTP.

To define your load balancer and listener

1. For **Load Balancer name**, use the name <NetID>-MIS543-LB for your load balancer.

The name of your Classic Load Balancer must be unique within your set of Classic Load Balancers for the region, can have a maximum of 32 characters, can contain only alphanumeric characters and hyphens, and must not begin or end with a hyphen.

2. Leave the default Scheme and IP address type configuration.

Basic configuration

Load balancer name
Name must be unique within your AWS account and cannot be changed after the load balancer is created.

weichen-MIS543-LB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | [Info](#)
Scheme cannot be changed after the load balancer is created.

☒ **Internet-facing**
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ **Internal**
An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type | [Info](#)
Select the type of IP addresses that your subnets use.

☒ **IPv4**
Recommended for internal load balancers.

☐ **Dualstack**
Includes IPv4 and IPv6 addresses.

- For Network Mapping, select both subnet in your manually created VPC.

Network mapping [Info](#)
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)
Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the confirm the VPC for your targets, view your [target groups](#).

weichen-vpc
vpc-0e13244d663bbfe05
IPv4: 10.0.0.0/24

↕

↺

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 balancer or the VPC are not available for selection.

☒ **us-east-1a**

Subnet
subnet-04461e01235d035a1 weichen-subnet-public1-us-east-1a ▼

IPv4 settings
Assigned by AWS

☒ **us-east-1b**

Subnet
subnet-05112d5f48f5b7240 weichen-subnet-public2-us-east-1b ▼

IPv4 settings
Assigned by AWS

- Next: **Security Groups**.

If you selected a VPC as your network, you must assign your load balancer a security group that allows inbound traffic to the ports that you specified for your load balancer and the health checks for your load balancer.

To assign security group to your load balancer

- On the **Assign Security Groups** page, select **Create a new security group**.
- Type a name and description for your security group. *For example*, Security group name: <NetID>-SG-loadbalancer. This new security group contains a rule that allows traffic to the port that you configured your load balancer to use. For the **Inbound rules**, change Type to **HTTP** and Source to **Anywhere**

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

weichen-SG-loadbalancer

Name cannot be edited after creation.

Description [Info](#)

security group for the load balancer

VPC [Info](#)

Q

vpc-0e13244d663bbfe05 (weichen-vpc)
10.0.0.0/24

vpc-00cdcd54eca03c94f
172.31.0.0/16

vpc-0e13244d663bbfe05 (weichen-vpc)
(default)

Type [Info](#)

HTTP

Protocol [Info](#)

TCP

Port range [Info](#)

80

Source [Info](#)

Anywhere-...

Q

0.0.0.0/0 X

Add rule

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

default

Select up to 5 security groups

[Create new security group](#)

default sg-05c69212cccc5d8bd X
VPC: vpc-0e13244d663bbfe05

C. Configure Routing for your EC2 Instances

Elastic Load Balancing automatically checks the health of the EC2 instances for your load balancer. If Elastic Load Balancing finds an unhealthy instance, it stops sending traffic to the instance and reroutes traffic to healthy instances. In this step, you customize the health checks for your load balancer.

To configure target group and health checks for your instances

1. On the **Listeners and routing** section, leave the default values for HTTP and 80.
2. For Default action, click **Create target group**. Select Instances for the target type.

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

☒ **Instances**

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

☐ **IP addresses**

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

☐ **Lambda function**

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

☐ **Application Load Balancer**

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

3. Change the target group name to <NetID>-lb-target, and ensure that your VPC is chosen.

Target group name

weichen-lb-target

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol

Port

HTTP

: 80

VPC

Select the VPC with the instances that you want to include in the target group.

weichen-vpc

vpc-Oe13244d663bbfe05
IPv4: 10.0.0.0/24

Protocol version

☒ **HTTP1**

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

☐ **HTTP2**

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

☐ **gRPC**

Send requests to targets using gRPC. Supported when the request protocol is gRPC.

4. For Health checks, leave the default value, and Choose **Next: Register Targets**.

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTP

Health check path

Use the default path of "/" to ping the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

► Advanced health check settings

► Tags - optional

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

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2)

Filter resources by property or value

< 1 > ⌂

| <input type="checkbox"/> | Instance ID | Name | State | Security groups | Zone | Subnet ID |
|--------------------------|---------------------|------------------|---------|---------------------|------------|--------------------------|
| <input type="checkbox"/> | i-0859d54f1b3376b02 | weichen-server-1 | running | weichen_SG_virginia | us-east-1a | subnet-04461e01235d035a1 |
| <input type="checkbox"/> | i-08ef16a9fa9038ca2 | weichen-server-2 | running | weichen_SG_virginia | us-east-1b | subnet-05112d5f48f5b7240 |

0 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

2 selections are now pending below. Include more or register targets when ready.

- On the **Register Targets** page, select the both the instances, and click **Include as pending below**.
- Choose **Create Target Group**
- Add target group to the Load Balancer. Choose **Protocol: Port = HTTP:80** and assign the newly created target group in the next field
- Click **Create load balancer**.

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

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

Port


HTTP ▼ : 80


1-65535

Default action [Info](#)

Forward to weichen-lb-target HTTP ▼

Target type: Instance, IPv4



[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

You can add up to 50 more tags.

D. Register EC2 Instances with Your Load Balancer

Your load balancer distributes traffic between the instances that are registered to it.

Note

When you register an instance with an elastic network interface (ENI) attached, the load balancer routes traffic to the primary IP address of the primary interface (eth0) of the instance.

To register EC2 instances with your load balancer

E. Verify and Test Your Load Balancer

After creating the load balancer, you can verify that it's sending traffic to your EC2 instances.

To create and test your load balancer

1. Select your new load balancer.
2. As shown in below screenshot, click on the **Listeners** tab. You should see that this load balancer is listening on Port 80, and will forward to weichen-lb-target target group.

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

To view and edit listener attributes, select the listener and choose Edit.

[Add listener](#) [Edit](#) [Delete](#)

| <input type="checkbox"/> | Listener ID | Security policy | SSL Certificate | Rules |
|--------------------------|--|-----------------|-----------------|---|
| <input type="checkbox"/> | HTTP : 80 arn...c801c9f3b0d7fa3b ▾ | N/A | N/A | Default: forwarding to weichen-lb-target View/edit rules |

3. Click Target Groups in your navigation pane. You can see the details of your weichen-lb-target target group here.

EC2 > Target groups > weichen-lb-target

weichen-lb-target

Actions ▾

Details

arn:aws:elasticloadbalancing:us-east-1:279035175453:targetgroup/weichen-lb-target/9ca324c39557905c

| | | | |
|-------------------------|--|---------------------------|--|
| Target type Instance | Protocol : Port HTTP: 80 | Protocol version HTTP1 | VPC vpc-0e13244d663bbfe05 |
| IP address type IPv4 | Load balancer None associated | | |

| | | | | | |
|---------------|---------|-----------|--------|---------|----------|
| 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](#)

| <input type="checkbox"/> | Instance ID | Name | Port | Zone | Health status | Health status details |
|--------------------------|-------------------------------------|------------------|------|------------|---------------|-----------------------|
| <input type="checkbox"/> | I-08ef16a9fa9038ca2 | weichen-server-2 | 80 | us-east-1b | healthy | |
| <input type="checkbox"/> | I-0859d54f1b3376b02 | weichen-server-1 | 80 | us-east-1a | healthy | |

4. If it indicates that some of your instances are not in service, it's probably because they are still in the registration process. If there is not registered then you can add them by Choosing Register Targets>> Select the machines from available instances>> Select Include as pending below>>Register the pending targets. Refer the below screenshot.
5. After at least one of your EC2 instances is in service, you can test your load balancer. Copy the string from **DNS name in Description Tab** (for example, weichen-mis543-lb-2103397369.us-east-1.elb.amazonaws.com) and paste it into the address field of an Internet-connected web browser. If your load balancer is working, you see the default page of your server. Refresh the page, you will see the content of both your Instances, that is, Machine 1 and Machine 2.

[Reload this page](#) [Not Secure](#) weichen-mis543-lb-2103397369.us-east-1.elb.amazonaws.com

Hello, weichen!

I am from MIS 543 AWS Lab 4

Machine 1

MIS 543 Online – Business Data Communications & Networking

Lab 4: Amazon EC2 and Elastic Load Balancing

Paste the Screenshot of the Listener tab for the load balancer

<<INSERT SCREENSHOT>>

Paste the Screenshot of the Targets tab for the target groups

<<INSERT SCREENSHOT>>

Paste two Screenshots of visiting the load balancer DNS name in browser, one showing machine 1, and another showing machine 2

<<INSERT SCREENSHOT>>