

Contents

Lab 4: Amazon Load Balancing.....	2
Task Breakdown	2
Task 1: Take an AMI of your Wordpress instance	2
Task 2: Launch another instance using the AMI.....	3
Task 3: Create a load balancer and add both the instances under it.	6
Task 4: Manage ELB using CLI.....	12

Lab 4: Amazon Load Balancing

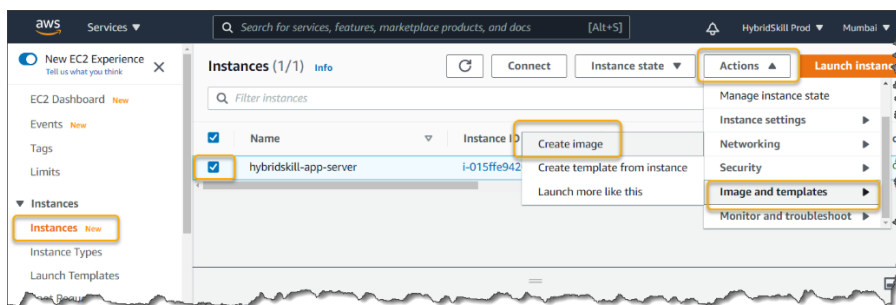
In this lab we will explore amazon elastic load balancing features

Task Breakdown

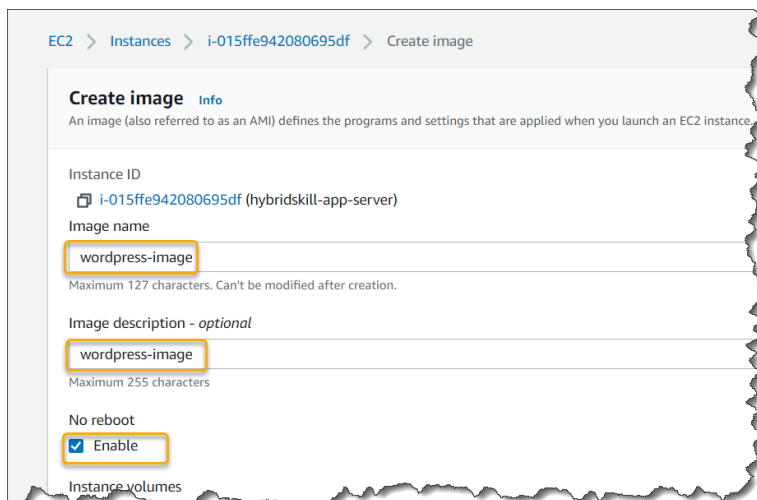
- Take an AMI of your wordpress instance
- Launch another instance using the AMI
- Create a load balancer and add both the instances under it.
- Test if load balancing is working successfully.

Task 1: Take an AMI of your Wordpress instance

1. On the Main **EC2 Dashboard**, on the left-hand side of the screen, select **Instances**, Select your wordpress instance. Next click **Actions** and then select **Image** and then click **Create Image**.



2. Enter a **wordpress-image** as the **Image name**, enter a short **Image description**, Select the **No reboot** option and finally click **Create Image**.

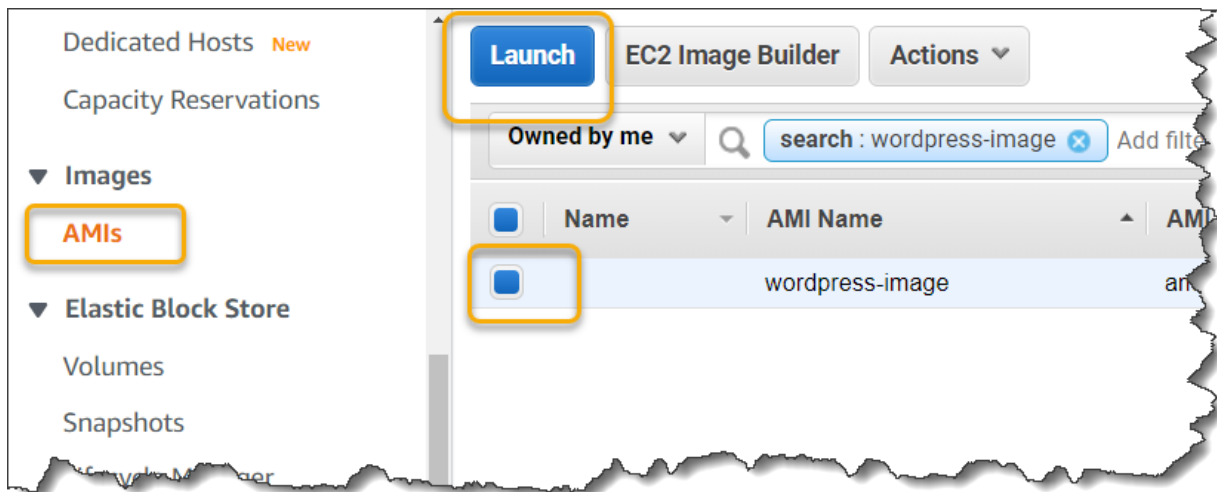


3. Your AMI should be successfully created.

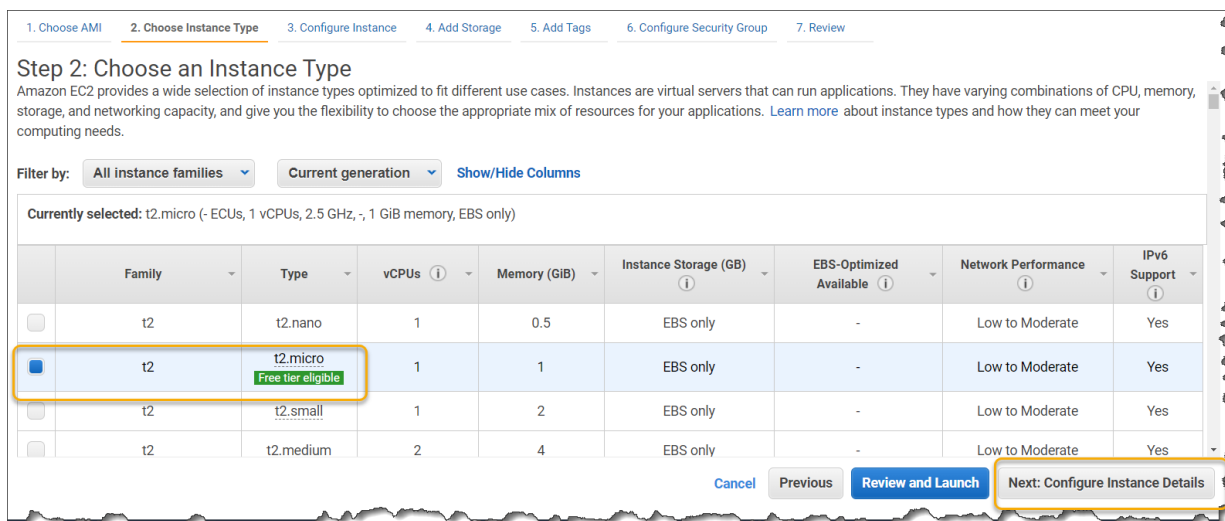
✔ Successfully created [ami-0598f743df0d6cd6c](#) from instance i-015ffe942080695df.

Task 2: Launch another instance using the AMI

1. Click **AMIs**, select your **wordpress-AMI** you created earlier and click **Launch**



2. As before select **t2.micro** as the **Instance Type** and Click **Next: Configure Instance Details**



- For the **Subnet**, select the other AZ this time (**subnet-xxxx ap-south-1b** in my case). Leave all options as default and 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
4090 IP Addresses available

Auto-assign Public IP

Placement group ☐ Add instance to placement group

Capacity Reservation

Domain join directory Create new directory

Cancel Previous Review and Launch Next: Add Storage

- Leave all options as default and click **Next: Add Tags**.

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

Step 4: Add Storage

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. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-052c89cb98546a101	10	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt

Add New Volume

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

Cancel Previous Review and Launch Next: Add Tags

- This time give **hybridskill-app-server-02** as the name of the instance and click **Next: Configure Security Group**

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

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.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances (1)	Volumes (1)
Name	hybridskill-app-server-02	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous **Review and Launch** Next: Configure Security Group

- Click **Select an existing security group**, select your **hybridskill-app-server-sg** as the name of your security group and click **Review and Launch**.

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

Step 6: Configure Security Group

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 ID	Name	Description	Actions
sg-83c20ce8	default	default VPC security group	Copy to new
sg-cde43ca6	hybridskill-app-server-sg	created 2018-02-18T22:49:12.538+05:30	Copy to new
sg-9ea004f5	rds-sg	rds-sg	Copy to new

Inbound rules for sg-cde43ca6 (Selected security groups: sg-cde43ca6)

Type (1)	Protocol (1)	Port Range (1)	Source (1)	Description (1)
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	:::0	

Cancel Previous **Review and Launch**

- Review your settings and click **Launch**.

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

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](#)

wordpress-ami - ami-3984d856
wordpress-ami
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

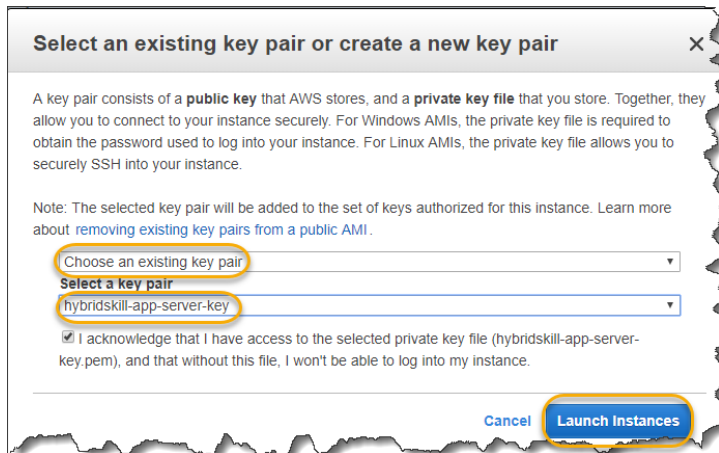
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security Group ID	Name	Description
sg-cde43ca6	hybridskill-app-server-sg	created 2018-02-18T22:49:12.538+05:30

Cancel Previous **Launch**

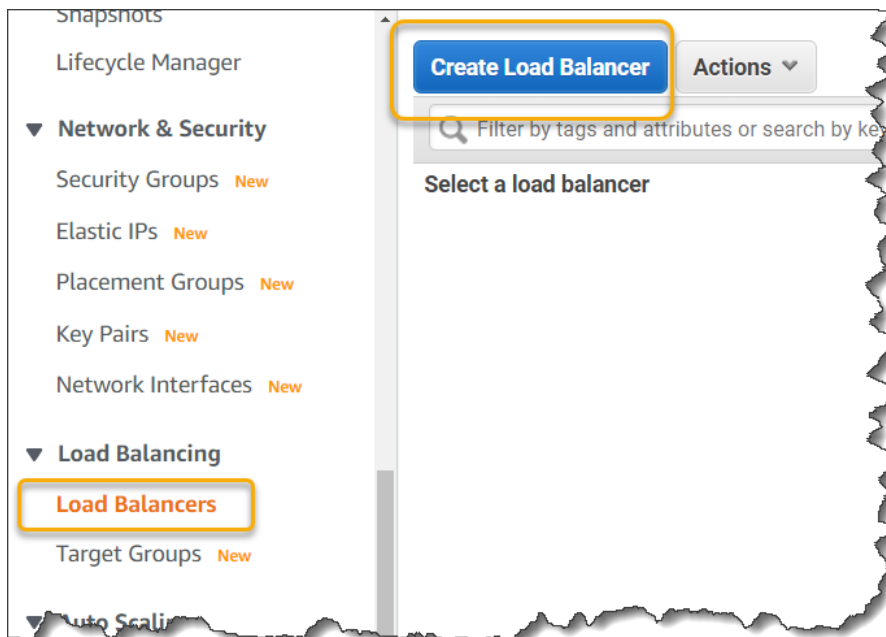
8. Select **Choose an existing key-pair** select the key you created earlier and Click **Launch Instances**



9. Your instance should be launching now.

Task 3: Create a load balancer and add both the instances under it.

1. On the main EC2 instance dashboard under the **LOAD BALANCING**, click **Load Balancers** and then click **Create Load Balancer**



2. Select **Application Load Balancer** as your load balancer type and click **Create**.

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	Network Load Balancer	Classic Load Balancer
<p>HTTP HTTPS</p> <p>Create</p> <p>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.</p>	<p>TCP TLS UDP</p> <p>Create</p> <p>Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while</p>	<p>PREVIOUS GENERATION for HTTP, HTTPS, and TCP</p> <p>Create</p> <p>Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network. Learn more ></p>

3. Enter **hybridskill-lb** as the **Load Balancer name**. Leave the **Load balancer protocol** as **HTTP**

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

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 port is 80.

Name ⓘ hybridskill-lb

Scheme ⓘ ☒ internet-facing
☐ internal

IP address type ⓘ ipv4

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
HTTP	80

Add listener

4. Select the **Default VPC** and **Availability zones a and b** leave all options as default and **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 ⓘ vpc-a23837ca (172.31.0.0/16) | Default (default) ⓘ

Availability Zones

☒ **ap-south-1a** subnet-332c185b ⓘ
IPv4 address ⓘ Assigned by AWS

☒ **ap-south-1b** subnet-54264318 ⓘ
IPv4 address ⓘ Assigned by AWS


☐ **ap-south-1c** subnet-7c2b8707 ⓘ

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

5. Click **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 2: Configure Security Settings

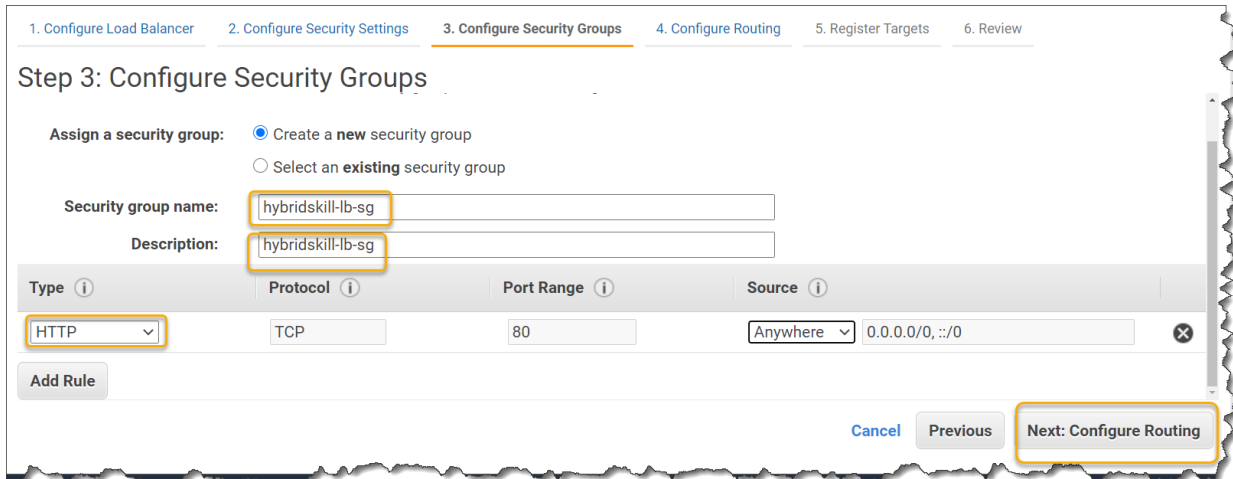


Improve your load balancer's security. Your load balancer is not using any secure listener.

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.

[Cancel](#) [Previous](#) [Next: Configure Security Groups](#)

6. Select **Create a new security group**. Enter **hybridskill-lb-sg** as the **Security group name**, enter a short **Description**. Select **HTTP** select the Source as **Anywhere**. And **Select Next: Configure Routing**



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

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

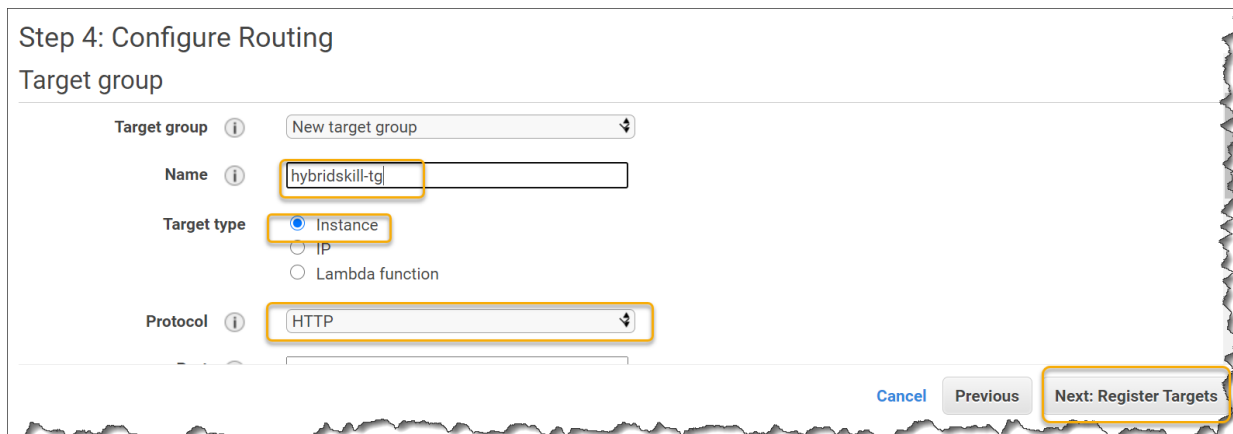
Security group name:
 Description:

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

Add Rule

Cancel Previous **Next: Configure Routing**

7. Select **New target group**, select the **Target type** as **Instance** and the **Protocol** as **HTTP**. Leave other options as default and click **Next: Register targets** .



Step 4: Configure Routing

Target group

Target group

Name

Target type ☒ Instance
☐ IP
☐ Lambda function

Protocol

Cancel Previous **Next: Register Targets**

8. Select both your EC2 instances you created earlier and click **Add to registered**. Click **Next:Review**

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
<input type="checkbox"/>	i-015ffe942080695df	hybridskill-app-server	80	running	hybridskill-app-server-sg	ap-south-1a
<input type="checkbox"/>	i-0e0ffbeb59c2a202d	hybridskill-app-server-02	80	running	hybridskill-app-server-sg	ap-south-1b

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

Search instances X

<input type="checkbox"/>	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-015ffe942080695df	hybridskill-app-server	running	hybridskill-app-server-sg	ap-south-1a	subnet-332c185b	172.31.32.0/20
<input checked="" type="checkbox"/>	i-0e0ffbeb59c2a202d	hybridskill-app-server-02	running	hybridskill-app-server-sg	ap-south-1b	subnet-54264318	172.31.0.0/20


Cancel Previous **Next: Review**

9. Review your settings and click **Create**.

Cancel Previous **Create**

10. Your load balancer has been created. Click **hybridskill-lb** to view more info about your load balancer

Load Balancer Creation Status


Successfully created load balancer

Load balancer **hybridskill-lb** was successfully created.
Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

- Discover other services that you can integrate with your load balancer. Visit the **Integrated services** tab within **hybridskill-lb**
- Consider using AWS Global Accelerator to further improve the availability and performance of your applications. [AWS Global Accelerator console](#)

Close

11. Under Description copy the DNS name and visit it on a browser

Create Load Balancer
Actions

search : arn:aws:elasticloadbalancing:ap-south-1... Add filter

Load balancer: **hybridskill-lb**

Description
Listeners
Monitoring
Integrated services
Tags

Basic Configuration

Name	hybridskill-lb
ARN	arn:aws:elasticloadbalancing:ap-south-1:069607445159:loadbalancer/lb/7a5e1eef8b4b2c9a
DNS name	hybridskill-lb-1868296412.ap-south-1.elb.amazonaws.com (A Record)
State	provisioning

Your wordpress application should be visible from the load balancer DNS

Task 4: Manage ELB using CLI

Now that we have explored ELB through the console, let's do the same through the CLI. Run the following commands on the command line interface that you had setup earlier.

1. Launch box from created AMI without using user-data and Note down the instance ID.

```
aws ec2 run-instances --image-id ami-0e356a61 --count 1 --instance-type t2.micro --key-name hybridskill-test --security-groups hybridskill-sg-test
```

2. Create a ELB.

- a. Create Subnet for ELB:

```
:~$ aws ec2 create-security-group --group-name wordpressapp-elb-test --description "created via awscli"
{
  "GroupId": "sg-3bcd6750"
}
```

3. Add ELB ingress rule:

```
:~$ aws ec2 authorize-security-group-ingress --group-name wordpressapp-elb-test --protocol tcp --port 80 --cidr 0.0.0.0/0
```

4. Run below command and get Subnet ID

```
:~$aws ec2 describe-subnets
{
  "Subnets": [
    {
      "AvailabilityZone": "ap-south-1b",
      ..
      "SubnetId": "subnet-3f312b72",
      "VpcId": "vpc-d6a00fbe",
      ..
    },
    {
      "AvailabilityZone": "ap-south-1a",
      ..
      "SubnetId": "subnet-7e248f16",
      "VpcId": "vpc-d6a00fbe",
      ..
    }
  ]
}
```

5. Use one of the subnet and create ELB

```
:~$ aws elb create-load-balancer --load-balancer-name wp-test-elb --listeners "Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80" --subnets subnet-3f312b72 --security-groups sg-3bcd6750
{
  "DNSName": "wp-test-elb-1143976224.ap-south-1.elb.amazonaws.com"
}
```

6. Now register instance using instance ID under ELB

```
:~$ aws elb register-instances-with-load-balancer --load-balancer-name wp-test-elb --instances i-04f8608c2e791aa76 i-0ea9e37dd06475610
```

```
{
  "Instances": [
    {
      "InstanceId": "i-0ea9e37dd06475610"
    },
    {
      "InstanceId": "i-04f8608c2e791aa76"
    }
  ]
}
```

7. Check Instance status:

```
:~$ aws elb describe-instance-health --load-balancer-name wp-test-elb --instances i-0ea9e37dd06475610
```

```
{
  "InstanceStates": [
    {
      "InstanceId": "i-0ea9e37dd06475610",
      "State": "InService",
      "ReasonCode": "N/A",
      "Description": "N/A"
    }
  ]
}
```