

AWS EC2 conclusion:

Load balancer -> Autoscaling group

Application Loadbalancer

Network Loadbalancer

Gateway Loadbalancer

Application LB -> operates at Layer 7, ex: http, https, microservices, advanced routing, path-based-routing.

Network Load balancer: at OSI Layer 4 --> Transport layer --> whenever you want to provide ultra high performance with lowest latency --> Gaming application, video streaming, IOT application -> wherever latency should be minimum

Gateway LB --> works at Layer 3 Network layer: whenever you want to go with Third-party communications like VPN. VPNs, Firewalls, where security concerns are high. Requires high security Firewall (VPN) ---> Gateway Loadbalancer

| |
S1 S2

The screenshot shows the AWS Management Console 'Network settings' page. Under the 'Firewall (security groups)' section, the 'Create security group' option is selected. Below this, a dropdown menu for 'Common security groups' shows 'DevOps-sg sg-031a081efd38c0e3a' selected. A button 'Compare security group rules' is visible on the right. The page also shows 'Network' and 'Subnet' settings.

```
#!/bin/bash
sudo su
yum install httpd -y
cd /var/www/html
echo "<html><h1>Banking Server 1</h1></html>" > index.html
systemctl start httpd
```

```
#!/bin/bash
sudo su
yum install httpd -y
cd /var/www/html
echo "<html><h1>Banking Server_2</h1></html>" > index.html
systemctl start httpd
```



Banking Service 1

It should be Banking Server 1 and 2 because these are Monolithic applications not Microservices



Banking Service_2

Network LoadBalancer: it is TCP, UDP

Application LoadBalancer: it is HTTP, HTTPS

Target group:

[Target groups](#) > Create target group

- Step 1
- ☒ Specify group details
- Step 2
- ☐ Register targets

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 can't 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.

Target group name

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

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you created. This choice cannot be changed after creation

TCP



80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

☒ IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

☐ IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

-
vpc-0a752647f0a021f2e
IPv4 VPC CIDR: 172.31.0.0/16



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 perform health checks on the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

► Advanced health check settings

Attributes

ⓘ Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

► Tags - optional

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

Cancel

Next

get group

<input type="checkbox"/>	Instance ID	Name	State	Security groups
<input type="checkbox"/>	i-08e7dc429a8898b47	LinuxVM2	Running	DevOps-sg
<input type="checkbox"/>	i-0cdd7b5cedf8c085f	LinuxVM1	Running	DevOps-sg

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.

Review targets

Targets (2)

Filter targets

Show only pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address
i-08e7dc429a8898b47	LinuxVM2	80	Running	DevOps-sg	ca-central-1b	172.31.4.152
i-0cdd7b5cedf8c085f	LinuxVM1	80	Running	DevOps-sg	ca-central-1b	172.31.9.133

Register targets

Targets

Monitoring

Health checks

Attributes

Tags

Registered targets (2/2)

Filter targets

Deregister

Register targets

<

1

>

<input checked="" type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status det...	Administrative ...	Override details	Launch time
<input checked="" type="checkbox"/>	i-08e7dc429a889...	LinuxVM2	80	ca-central-1b (cac...	<div></div> Unused	Target group is no...	-	-	March 15, 2025, ...
<input checked="" type="checkbox"/>	i-0cdd7b5cedf8c0...	LinuxVM1	80	ca-central-1b (cac...	<div></div> Unused	Target group is no...	-	-	March 15, 2025, ...

Now go to Load Balancer

Application Load Balancer [Info](#)

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

[Create](#)

Network Load Balancer [Info](#)

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 applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Create](#)

Gateway Load Balancer [Info](#)

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

[Create](#)

► **Classic Load Balancer - *previous generation***

Create Network Loadbalancer

[Load balancers](#) > Create Network Load Balancer

Create Network Load Balancer [Info](#)

The Network Load Balancer distributes incoming TCP and UDP traffic across multiple targets such as Amazon EC2 instances, microservices, and containers. When the load balancer is created, you specify the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types.

Network Load Balancer now supports UDP for Dualstack
Set your IP address type as dualstack and enable prefix for IPv6 source NAT. Then configure UDP-based listeners to route to IPv6 targets.

► How Network Load Balancers work

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

MyNetworkLB

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

Scheme

Scheme can't be changed after the load balancer is created.

☒ Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

☐ Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.

Load balancer IP address type [Info](#)

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types.

☒ IPv4

Includes only IPv4 addresses.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

Availability Zones and subnets

Select one or more Availability Zones and corresponding subnets. Enabling multiple Availability Zones increases the availability of the load balancer. If the load balancer or the VPC are not available for selection,

☒ **ca-central-1a (cac1-az1)****Subnet**

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses

subnet-02a70284a8b5c8bb9

IPv4 subnet CIDR: 172.31.16.0/20

IPv4 address

The front-end IPv4 address of the load balancer in the selected Availability Zone.

☒ Assigned by AWS

☒ **ca-central-1b (cac1-az2)****Subnet**

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses

subnet-038c457fd7226e0ec

IPv4 subnet CIDR: 172.31.0.0/20

IPv4 address

The front-end IPv4 address of the load balancer in the selected Availability Zone.

☒ Assigned by AWS

☒ **ca-central-1d (cac1-az4)****Subnet**

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses

subnet-05422c9c80857b14b

IPv4 subnet CIDR: 172.31.32.0/20

IPv4 address

The front-end IPv4 address of the load balancer in the selected Availability Zone.

☒ Assigned by AWS

Security group selected

And TCP selected

Security groups support on Network Load Balancers can only be enabled at creation by including at least one security group. You can change security groups after creation. The security groups for your load balancer listener port and the health check port. For PrivateLink Network Load Balancers, security group rules are enforced on PrivateLink traffic; however, you can turn off inbound rule evaluation after creation within the

Select up to 5 security groups

DevOps-sg
sg-031a081efd38c0e3a VPC: vpc-0a752647f0a021f2e

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.

▼ Listener TCP:80

Protocol

TCP

Port

80

1-65535

Default action

Info

Forward to

Select a target group

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.

Add listener

Select Target group

Security groups - recommended

Security groups support on Network Load Balancers can only be enabled at creation by including at least one security group. You can change security groups after creation. The security groups for your load balancer listener port and the health check port. For PrivateLink Network Load Balancers, security group rules are enforced on PrivateLink traffic; however, you can turn off inbound rule evaluation after creation within the

Select up to 5 security groups

DevOps-sg
sg-031a081efd38c0e3a VPC: vpc-0a752647f0a021f2e

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.

▼ Listener TCP:80

Protocol

TCP

Port

80

1-65535

Default action

Info

Forward to

TG1

Target type: Instance, IPv4

TCP

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.

Add listener

Create load balancer

Summary

Review and confirm your configurations. [Estimate cost](#)

Basic configuration

Edit

Name: MyNetworkLB

Scheme: Internet-facing

IP address type: IPv4

Security groups

Edit

DevOps-sg

sg-031a081efd38c0e3a

Network mapping

Edit

VPC: vpc-0a752647f0a021f2e

Availability Zones and subnets:

- ca-central-1a
subnet-02a70284a8b5c8bb9
- ca-central-1b
subnet-038c457fd7226e0ec
- ca-central-1d
subnet-05422c9c80857b14b

Listeners and routing

Edit

TCP:80 | Target group: TG1

Service integrations

Edit

AWS Global Accelerator: -

Tags

Edit

-

Attributes

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Creation workflow and status

► Server-side tasks and status

After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.

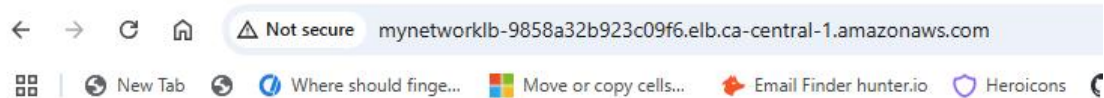
Cancel Create load balancer

Currently Provisioning

Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in i

Filter load balancers			
<input type="checkbox"/>	Name	DNS name	State
<input type="checkbox"/>	MyNetworkLB	MyNetworkLB-9858a32b92...	Provisioning..



Banking Service_2

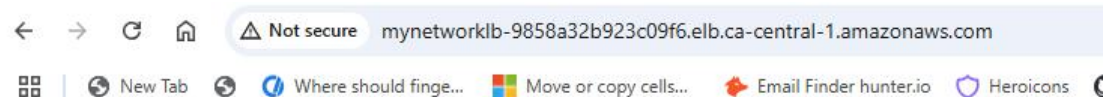
Security groups -> inbound rules

May be add All TCP -> 0.0.0.0/0

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info					
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	
sgr-01adffa81382cb320	RDP	TCP	3389	Custom	<input type="text" value="0.0.0.0/0"/>
sgr-059d9b42eb2895f8f	SSH	TCP	22	Custom	<input type="text" value="0.0.0.0/0"/>
sgr-085d44d7089c06b76	HTTPS	TCP	443	Custom	<input type="text" value="0.0.0.0/0"/>
sgr-0e5cef937ec2e0b52	All TCP	TCP	0 - 65535	Custom	<input type="text" value="0.0.0.0/0"/>
sgr-07d1078f0fa10518a	HTTP	TCP	80	Custom	<input type="text" value="0.0.0.0/0"/>
Add rule					



Banking Service 1

Why we have to go with Auto-scaling?

If you want to modify infrastructure based on the demand, auto-scaling comes into picture

Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling

helps maintain the availability of your applications

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management features. These features help you maintain the health and availability of your applications.

Create Auto Scaling group

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

Create Auto Scaling group

How it works



Pricing

Amazon EC2 Auto Scaling features have no additional fees beyond the service fees for Amazon EC2, CloudWatch (for scaling policies), and the other AWS resources that you use. Visit the pricing page of each service to learn more.

Create Auto Scaling Group

Launch template [Info](#)

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

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

Select a launch template

Create a launch template [?](#)

Cancel

Next

Click 'Create a launch template'

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused.

Launch template name and description

Launch template name - *required*

MyTemplate

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

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance [Info](#)

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

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

► **Template tags**

► **Source template**

Launch template name required

MyTemplate

Must be unique to this account. Max 128 chars. No spaces or special characters.

Template version description

my_template-v1.0

Max 255 chars

Auto Scaling guidance [Info](#)

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

☒ Provide guidance to help me set up a template that works with EC2 Auto Scaling.

► **Template tags**

► **Source template**

Launch template contents

Specify the details of your launch template below. Leaving a field blank will use the default value.

▼ **Application and OS Images (Amazon)**

An AMI is a template that contains the software configuration for an EC2 instance. If you don't see what you are looking for below, click the search icon to search for AMIs.

 Search our full catalog including 1000s of applications and operating systems.

Recents

Quick Start

☒ **Currently in use**

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

Debian
debian

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-0cc3a9edb87c91b53 (64-bit (x86), uefi-preferred) / ami-092dc7d756444f58e (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20250303.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date
64-bit (x86)	uefi-preferred	ami-0cc3a9edb87c91b53	2025-03-04

▼ Instance type [Info](#) | [Get advice](#)

Instance type

Don't include in launch template

Key pair name

devopsLinuxFeb22

▼ Network settings [Info](#)**Subnet** [Info](#)

Don't include in launch template

When you specify a subnet, a network interface is automatically added to your template.

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.

☒ Select existing security group☐ Create security group**Security groups** [Info](#)

Select security groups

DevOps-sg sg-031a081efd38c0e3a ✕
VPC: vpc-0a752647f0a021f2e**► Advanced network configuration****▼ Storage (volumes)** [Info](#)**EBS Volumes**

Configure Security groups, Keypair --> Create launch template

▼ Summary**Software Image (AMI)**Amazon Linux 2023 AMI 2023.6.2...[read more](#)
ami-0cc3a9edb87c91b53**Virtual server type (instance type)**

-

Firewall (security group)

DevOps-sg

Storage (volumes)

1 volume(s) - 8 GiB



Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#)[Create launch template](#)

Launch Templates (1) Info

Search

Launch Template ID

Launch Template Name

Default

lt-002e9ad73c7315050

MyTemplate

1

Go back to Create Auto Scaling Group

Create Auto Scaling group

Launch template

instance launch options

optional

te with other services

optional

are group size and scaling

optional

tifications

optional

js

Choose launch template Info

Specify a launch template that contains settings common to all EC2 inst

Name

Auto Scaling group name

Enter a name to identify the group.

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

Launch template Info

For accounts created after May 31, 2023, the EC2 console only not recommended but still available via the CLI and API until D

Launch template

Choose a launch template that contains the instance-level settings, such as the.

[Create a launch template](#)

Select 'MyTemplate'

MyAutoScalingGrp

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

Launch template Info

For accounts created after May 31, 2023, the EC2 console only supports creating Auto S

not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI)

MyTemplate

[Create a launch template](#)

Version

Default (1)

[Create a launch template version](#)

Description

my_template-v1.0

Launch template

MyTemplate

lt-002e9ad73c7315050

Click Next ---> Pick Availability Zones and Subnets

Network Info

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

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0a752647f0a021f2e

172.31.0.0/16 Default

[Create a VPC](#)

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

ca-central-1a | subnet-02a70284a8b5c8bb9

172.31.16.0/20 Default

ca-central-1b | subnet-038c457fd7226e0ec

172.31.0.0/20 Default

ca-central-1d | subnet-05422c9c80857b14b

172.31.32.0/20 Default

[Create a subnet](#)

Availability Zone distribution - new

Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

☒ **Balanced best effort**

If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

☐ **Balanced only**

If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

Cancel

Skip to review

Previous

Next

All others I want to keep it default ---> click Next

Review and create Auto Scaling Group

Additional settings

Instance scale-in protection
Disabled

Monitoring
Disabled

Default instance warmup
Disabled

Capacity Reservation preference

Preference
Default

Capacity Reservation IDs
-

Resource Groups
-

Step 5: Add notifications
Edit

Notifications

No notifications

Step 6: Add tags
Edit

Tags (0)

Key	Value	Tag new instances
No tags		

Preview code
Cancel
Previous
Create Auto Scaling group

Go to EC2 Instances

<input type="checkbox"/>	LinuxVM1	i-0cdd7b5cedf8c085f	Running	t2.micro	2/2 checks passed	VI
<input type="checkbox"/>	LinuxVM2	i-08e7dc429a8898b47	Stopped	t2.micro	-	VI
<input type="checkbox"/>		i-0e3cbeb50f4ad34d4	Running	c6a.large	Initializing	VI

We can see one more instance is being created automatically --> Auto scaling is creating this instance
We manually create LinuxVM1 and LinuxVM2, third is automatic

Now I go back to EC2 instances and I see that one more instance is automatically created. This is fault-tolerance of Auto scaling

<input type="checkbox"/>	LinuxVM1	i-0cdd7b5cedf8c085f	Terminated	t2.micro	-	
<input type="checkbox"/>	LinuxVM2	i-08e7dc429a8898b47	Terminated	t2.micro	-	
<input type="checkbox"/>		i-030d6afb0ef30dfba	Running	c6a.large	3/3 checks passed	
<input type="checkbox"/>		i-0e3cbeb50f4ad34d4	Terminated	c6a.large	-	

I terminate one more instance, which initializes another instance

<input type="checkbox"/>	LinuxVM1	i-0cdd7b5cedf8c085f	Terminated	t2.micro	-	
<input type="checkbox"/>	LinuxVM2	i-08e7dc429a8898b47	Terminated	t2.micro	-	
<input type="checkbox"/>		i-054cf2cc90eeaa599	Running	c6a.large	Initializing	
<input type="checkbox"/>		i-030d6afb0ef30dfba	Shutting-d...	c6a.large	-	
<input type="checkbox"/>		i-0e3cbeb50f4ad34d4	Terminated	c6a.large	-	

AutoScaling groups:

It is used to adjust the capacity required to handle the load

If number of requests are increasing, then servers must also be increased to give smooth experience for customers and similarly if requests are decreasing then number of servers should be decreased to manage cost. In that case, we can go with AutoScaling group.

1. Fault-tolerance
2. Cost management
3. High availability

---> To create AutoScaling group, we use Launch Template - it is used to specify configuration required to launch new VM whenever needed

=====

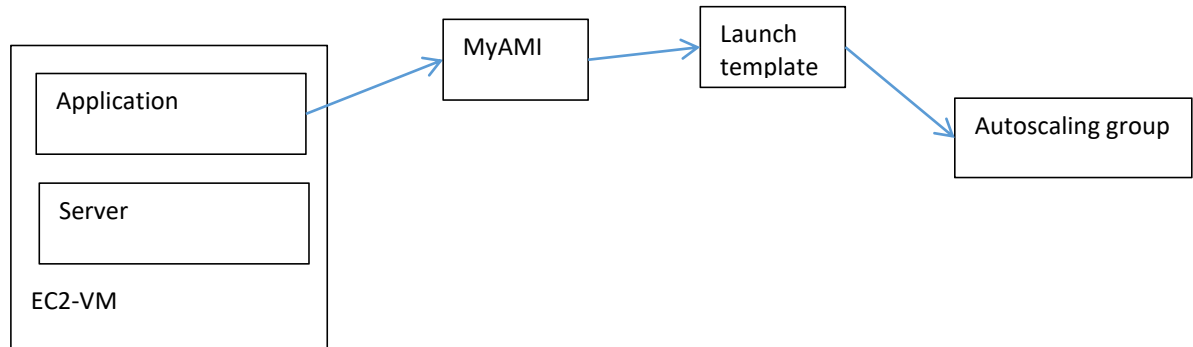
How an application will be deployed into a new VM created by AutoScaling group?

Kubernetes is the default option. However, lets look into custom AMI for now

Using custom AMI ---> what's AMI? Amazon Machine Image

User data script

Kubernetes cluster



Different types of AWS EC2 instances:

General purpose

Compute optimized

Storage optimized

Memory optimized

Accelerated computing

High performance computing

Select the instance ---> Actions --> Image and templates --> Create image

instances > i-Of1ab736776d0db76 > Create image

Instance ID
i-Of1ab736776d0db76 (MyVM1)

Image name

Maximum 127 characters. Can't be modified after creation.

Image description - optional

Maximum 255 characters

☒ **Reboot instance**
When selected, Amazon EC2 reboots the instance so that data is at rest when snapshots of the attached volumes are taken.

Instance volumes

Storage type	Device	Snapshot	Size	Volume type
EBS	/dev/x...	Create new snapshot from v...	8	

Add volume

i During the image creation process, Amazon EC2 creates a snapshot of each of the above volumes.

Click Create Image

Now click on Launch Instances

Now we see a new option : My AMIs earlier it was not there

Recents

My AMIs

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

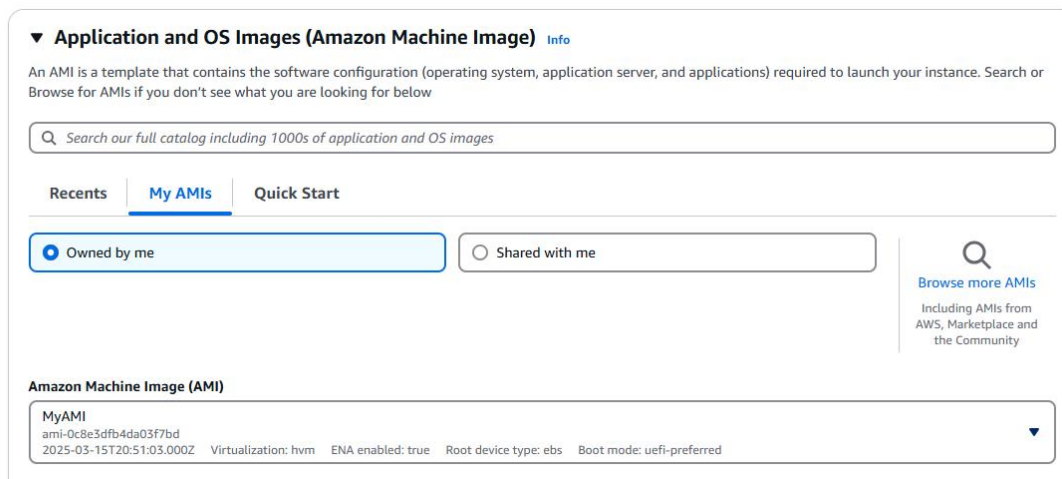
Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-0cc3a9edb87c91b53 (64-bit (x86), uefi-preferred) / ami-092dc7d756444f58e (64-bit (Arm), uefi)

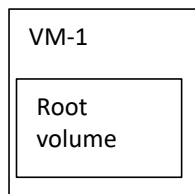
Virtualization: hvm ENA enabled: true Root device type: ebs

I can select MyAMI



Launch template looks like a new Launch instance only so it can go into AutoScaling groups if we want to deploy our application (from AMI) on all the automatically created EC2 instances

For every VM we create, by default root volume is there. We can add additional volumes.



I create a new VM2 with new Root volume. Yes, we can attach new volume to VMs. I can copy data from RV of VM2 into additional volume. Later, I will move Additional volume from VM2 into VM1. I think if VM1 and VM2 use different .pem files (keys), we got to do key replacement using a temporary VM. When I copy data from VM2 RV into Add volume on VM2, it will be according to private key of VM2. Whenever we try to access volumes, it will match public and private keys. In VM1, when we attach a volume it will compare with the private keys. Say if VM2 pem file is lost, create a new temporary VM ---> detach RV from VM1 attach in temp VM then copy from add vol into RV from VM1. The RV will now have IPs associated with the new pem file of temp VM. Now VM1 can use the temp VM pem file to access RV.