AWS load balancer with auto scale quick setup

- Overview
- · Launching AWS Auto Scaling group with classic load balancer from custom AMI
 - 1. Create new AMI
 - 2. Create new Load Balancer
 - 3. Create new Launch Configuration4. Create new Auto Scaling group
- Launching Application Load Balancer using existing instances
 - 1. Instances launching
 - 2. Application Load Balancer creation
 - 3. Websocket listener target group creation
 - 4. Listener parameters configuration
- Launching AWS Auto Scaling group with load balancing from AWS Marketplace AMI
 - 1. Create launch template
 - 2. Create Auto scaling group
- Testing

Overview

WCS Amazon instances support AWS load balancer.

WebSocket connections will be distributed between active load balancer instances. In case a scaling policy is executed (when the policy target – e.g., CPU load on instance - is reached) and new instances are launched, they will be added to the load balancer.

The following components would be required

- · AMI on the basis of which new instances will be created for scaling out
- Load Balancer
- Launch Configuration
- Auto Scaling Group

Launching AWS Auto Scaling group with classic load balancer from custom AMI

Load balancer with autoscaling deployment from custom AMI can be useful for logn term projects (months and years). In this case, AWS Marketplace image will be more expensive due to hourly payment, therefore it is recommended to buy and activate WCS monthly subscription.

Note that classic load balancer will work till August 2022.

1. Create new AMI

1.1.Launch an instance from a FlashphonerWebCallServer AMI and configure the WCS

- activate license
- import certificates
- change configuration settings as required

1.2. In AWS console, select the instance and then "Actions" | "Image" | "Create Image" and create a new image:

aws	Serv	ices	• I	Resource G	iroups	5 ¥	\$						
Reports	^		Launc	h Instance	-	Conne	ect	Actions A					
Limits								A		-			
			Q, Fi	ter by tags an	d attrib	outes or se	earch	Connect Get Windows Password					
INSTANCES				Namo	- In	etanco II		Create Template From Instan	псе	ility Zony	- Ir	etanco Stato 🔺	Status Chocks
Instances				vanie	* III	Istance IL	' I	Launch More Like This			* II	Istance state -	Status Checks
Launch Templates					i-0)6ef5f5eb3	15264	Instance State	•	1d	•	running	2/2 checks
Spot Requests					i-0)3a717e99	dd40	Instance Settings	•	1b		stopped	
Reserved Instance	s				i-0)3b463eb0	89460	Image		Create	e Image		
Dedicated Hosts					i-0)550b9a66	i1f719	Networking	►	Bundl			re AMI)
Scheduled Instance	es				i-C)b6ca56b7	'32c4l	CloudWatch Monitoring	•	1d	(stopped	

2. Create new Load Balancer

2.1. In AWS console, go to "EC2" | "Load Balancers" and click "Create Load Balancer"

aws	Servi	ices	✓ Resource Group	ıs ~ \$	¢	
	^		Create Load Balancer	Actions 👻		
Load Balancers		•	Q Filter by tags and attr	ibutes or search by ke	eyword	К <
Target Groups			Name	▲ DNS n	ame - State	- VPC ID
-						
AUTO SCALING					You do not have any load balancers it	this region
Launch Configurations						r una region.
Auto Scaling Group	ps					

2.2 Select "Classic Load Balancer" type (This type allows specifying port for health check.)

aws Services ~ R	esource Groups 👻 🔦	4							
Select load balancer type									
Elastic Load Balancing supports three typ type that meets your needs. Learn more a	lastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers (new), and Classic Load Balancers. Choose the load balancer /pe that meets your needs. Learn more about which load balancer is right for you								
Application Load Balance	er N	etwork Load Balancer	Classic Load Balancer						
HTTP HTTPS		TCP TLS	PREVIOUS GENERATION for HTTP, HTTPS, and TCP						
Create Choose an Application Load Balancer need a flexible feature set for your we with HTTP and HTTPS traffic. Operati request level, Application Load Balance advanced routing and visibility feature application architectures, including mi and containers. Learn more >	r when you bb applications ng at the connections at cers provide st argeted at croservices	Create vork Load Balancer when you need ormance, the ability to terminate TLS scale, centralize certificate do static IP addresses for your berating at the connection level, Balancers are capable of handling tests per second securely while ra-low latencies.	Create Choose a Classic Load Balancer when you have an existing application running in the EC2-Classic network. Learn more >						

2.3. When defining load balancer, add required protocols. For exampleTCP, port 8080 for WebSocket connections (ws:<host>:8080).

aws Services v	Resource Groups 👻 🔦	4		
1. Define Load Balancer 2. Assign Se	acurity Groups 3. Configure Security Settin	gs 4. Configure Health Check	5. Add EC2 Instances	6. Add Tags 7. Review
Step 1: Define Load Ba	alancer			
Basic Configuration				
This wizard will walk you through settin balancers you might create. You will al balancer port to any port on your EC2 Load Balancer nam Create LB Insid Create an internal load balance Enable advanced VPC configuratio Listener Configuratio	g up a new load balancer. Begin by givin so need to configure ports and protocol instances. By default, we've configured e: TEST-LB le: My Default VPC (172.31.0.0/16) er: (what's this?) nn: (http://www.configured.com/in/com/in	ng your new load balancer a unic s for your load balancer. Traffic f your load balancer with a standa	que name so that you ca rom your clients can be ard web server on port 8	n identify it from other load routed from any load 0.
Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Por	t
HTTP ~	8081	HTTP ~	8081	8
TCP ~	8080	TCP ~	8080	8
Add				
			Cancel Next:	Assign Security Groups

2.4. Assign a security group.

2.5. Configure health check

The URL for health check is

- for HTTP: http://WCS_ADDRESS:8081/?action=stat

- for HTTPS:https://WCS_ADDRESS:8444/?action=stat

aWS Services	✓ Resource (Groups 👻 1	*	4			
1. Define Load Balancer 2. As:	sign Security Groups	3. Configure Sec	curity Settings	4. Configure Health Check	5. Add EC2 Instan	ces 6. Add Tags	7. Review
Step 4: Configure H Your load balancer will automatic health check, it is automatically i	Health Chec cally perform health removed from the lo	k checks on your E ad balancer. Cus	EC2 instances tomize the hea	and only route traffic to in ith check to meet your sp	stances that pass th ecific needs.	e health check. If a	an instance fails the
Ping Protoc	ol HTTP	\sim					
Ping Po	ort 8081						
Ping Pa	th /?action=sta	at					
Advanced Details							
Response Timeout (j) 5	seconds					
Interval (j) 30	seconds					
Unhealthy threshold (j) 2	\sim					
Healthy threshold (i) 10	\sim					
					Cancel	Previous	xt: Add EC2 Instances

2.6. Add existing EC2 instances as required

By default, cross-zone load balancing is enabled to distribute traffic between all available availability zones in your region.

2.7. Complete the wizard to create the load balancer

2.8. Enable stickiness for HTTP/HTTPS LB ports

Create Load Balancer	actions V				Ð	¢	0
Q Filter by tags and attribute	s or search by keyword			K < 1 to	1 of 1		
Name	DNS name	- State	✓ VPC ID	 Availability Zones 	- Тур	e	
LoadBalancerHLS	LoadBalancerHLS-1	555758	vpc-abb341d2	eu-west-1a, eu-west-1c.	. clas	sic	
Port Configuration	8080 (TCP) forwarding	Edit stickiness		×	¢		> 4
	8081 (HTTP) forwardin Stickiness: Disabled Edit stickiness 8082 (HTTP) forwardin Stickiness: Disabled	 Disable stickiness Enable load balance Enable application g Expiration Period: 300 Leave blank to disable 	r generated cookie stickiness enerated cookie stickiness				
Security	Edit stickiness			Cancel Save			

3. Create new Launch Configuration

3.1. In AWS console, go to "EC2" | "Launch Configurations" and click "Create launch configuration"

aws	Services	v Resource Groups v 🖈	
Key Pairs	^	Create launch configuration Create Auto Scaling group Copy to launch template Actions 💙	
		Filter: Q Filter launch configurations X	- K <
LOAD BALANCING		New ANUD Instance Test Data Contine Time	
Target Groups		Name AMI ID T Instance Type T Spot Price T Creation Time T	
AUTO SCALING		No launch configurations found	
Launch Configurations			
Auto Scaling Group	s		

3.2. When choosing AMI, select the AMI previously created from an instance with required WCS configuration

aws Services	 Resource 	Groups 🗸 🗙							
1. Choose AMI 2. Choose Insta	ance Type 3. Cor	nfigure details 4. Add	Storage 5. Configure Security G	oup 6. Review	w				
Create Launch Con An AMI is a template that contain Marketplace; or you can select o	Cancel and Exit Adv 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 darketplace; or you can select one of your own AMIs:								
Quick Start	Quick Start								
My AMIs	Q Search my A	AMIS	X						
AWS Marketplace	۵	FlashphonerWeb	CallServer-5.1.3777-x86_64 -	ami-00893635e	e5c0a2526				Select
Community AMIs		Root device type: ebs	Virtualization type: hvm Owner: 170	65852928					64-bit
 Ownership 	۵	Template ami-02	190a301e00baced						Select
Owned by me	_	Root device type: ebs	Virtualization type: hvm Owner: 170	65852928					64-bit

3.3. Complete the wizard to create the configuration

Detailed monitoring, where data is available in 1-minute periods, can be enabled when configuring details.

aws Servio	es v Re	esource	Groups 👻	*	4			
1. Choose AMI 2. Choose	Instance Type	3. Co	nfigure details	4. Add Storage	5. Configure Security Grou	ıp 6. Reviev	V	
Create Launch C	Configura	ation						
	Name	(j)	TEST-LG					
Purcha	sing option	()	Request S	Spot Instances				
	IAM role	()	None		~			
	Monitoring	(j)	Enable Cl	oudWatch detailed	I monitoring			
Advanced Details								
Later, if you want to cannot be edited.	use a different l	aunch co	onfiguration, you	can create a new o	ne and apply it to any Auto	Scaling group.	Existing launch con	figurations
					(
					Cancel	Previous	Skip to review	Next: Add Storage

4. Create new Auto Scaling group

4.1. In AWS console, go to "EC2" | "Auto Scaling Groups" and click "Create Auto Scaling group"

aws	Services	✓ Resource Groups ✓ ♦
Target Groups	^	Welcome to Auto Scaling
 AUTO SCALING Launch Configurations 	4	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
Auto Scaling Groups		Create Auto Scaling group
-		Note: To create your Auto Scaling groups in a different region, select your region from the navigation bar.

4.2. Select the required launch configuration or template, or select to create a new one

aws Services - Resource Groups - 🕻	Ą
Create Auto Scaling Group Complete this wizard to create your Auto Scaling group. First, choose either a law template to specify the parameters that your Auto Scaling group uses to launch in	Cancel and Exit inch configuration or a launch instances.
● Launch Configuration You can continue to use your launch configurations if they support the Amazon EC2 features you need. Learn more C	C Launch Template New Launch templates give you the option of launching one type of instance, or a combination of instance types and purchase options. Launch templates include the latest Amazon EC2 features and can be updated and versioned. Learn more C [↑] Create new launch template C [↑]
 Create a new launch configuration Use an existing launch configuration QFilter launch configurations X 	$ \langle \ \langle$ 1 to 1 of 1 Launch Configurations $ angle \ angle$
Name AMI ID - Ins	stance Type - Spot Price - Security Groups -
TEST-LG ami-0cf30f44be371890d t2.sr	mall sg-03b1bc951522cb94a
	Cancel Next Step

4.3. Configure Auto Scaling group details

- add required subnets add required load balancer

aws Services - Resource Group	s • • • Δ	
1. Configure Auto Scaling group details 2. Configure scaling	g policies 3. Configure Notifications 4. Configure Tags 5. Review	
Create Auto Scaling Group		Cancel and Exit
Group name (j	TEST-ASG	
Launch Configuration (j)	TEST-LG	
Group size (1)	Start with instances	
Network (j)	vpc-714e7e15 (172.31.0.0/16) (default)	
Subnet (i)	subnet-d3d17ff9(172.31.48.0/20) Default in us- ×	
	east-10 subnet-861169e3(172.31.64.0/20) Default in us- ×	
	east-1c	
	Each instance in this Auto Scaling group will be assigned a public IP address. (1)	
 Advanced Details 		
Load Balancing (j)	Receive traffic from one or more load balancers Learn about Elastic Load Balancing	
Classic Load Balancers (i) TEST-LB ×		
Target Groups (j)		
Health Check Type 🧃	●ELB OEC2	
Health Check Grace Period (j)	300 seconds	
Monitoring (j	Enable CloudWatch detailed monitoring	
Learn more		
Instance Protection ()		
Service-Linked Role 🧃	AWSServiceRoleForAutoScaling View Role in IAM	
	Cano	Next: Configure scaling policies

4.4. Configure scaling policies

a	WS	Services 🗸	Resource Groups 👻	۵ ک					-		
1. Confi	gure Auto Sca	aling group details	2. Configure scaling policies	3. Configure Noti	ifications	4. Configure	Tags 5	5. Review			
Crea You can instructio remove execute	Create Auto Scaling Group fou 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 nstructions 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.										
	ОКеер	this group at its	initial size								
	🖲 Use so	caling policies to	o adjust the capacity of this	group							
	Scale be	etween 1 and	3 instances. These will b	e the minimum and	1 maximum	size of your (group.				
	Scale	Group Size							⊗		
		Name:	CPU								
		Metric type:	Average CPU Utilization		\sim						
	т	arget value:	70								
	Inst	ances need:	300 seconds to warm up a	ifter scaling							
	Disa	ble scale-in:									
	Scale th	e Auto Scaling gr	oup using step or simple scali	ng policies (j)							
				Ca	ancel F	Previous	Review	Next: Cor	figure Notifications		

4.5. Complete the wizard to create the auto scaling group

Launching Application Load Balancer using existing instances

Sometimes, a certain set of instances is already launched and configured (Origin servers group in CDN, for example), and load balancing between those servers should be set up. Use Application Load Balancer to do this.

1. Instances launching

Launch and configure server instances as needed by this manual.

2. Application Load Balancer creation

2.1. In EC2 Console menu, go to "Load balancers - Load balancers" section and click "Create load balancer". Click Create for Application Load Balancer

Select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. Learn more 🗹

Load balancer types



2.2. Enter the balancer name, choose Internet-facing type (supposed by default)

reate Application Load Balancer Info	
e Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and splicable, it selects a target from the target group for the rule action.	i, based Lif
How Application Load Balancers work	
Basic configuration	
Load balancer name Name must be unique within your AWS account and cannot be changed after the load balancer is created.	
TEST-APP-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.	
O Dualstack Includes IPv4 and IPv6 addresses.	

2.3. In "Network mapping" section choose a subnets needed

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 I confirm the VPC for your targets, view your target groups ∠. - vpc-e305fc9a IPv4: 172.31.0.0/16	ce changed after the load balancer is created. To
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. Avail balancer or the VPC are not available for selection. Subnets cannot be removed after the load balancer is created, but additional subnets can be eu-west-1a	ability Zones that are not supported by the load e added.
Subnet-003b4c5a	
IPv4 settings Assigned by AWS	
eu-west-1b	
eu-west-1c	

2.4. Choose or create security groups as needed

ecurity groups	
Select security groups	▼ C

Note that a standard WCS ports set should be opened in load balancer security group

Create new based on seller settings A new security group will be generated by AWS Marketplace. It is based on recommended settings for Web Call Server 5 version 5.2.267. Name your security Group WCS 5.2 Description WCS server 5.2 **Connection Method** Protocol Port Range Source (IP or Group) SSH 0.0.0.0/0 tcp 22 Anywhe ~ 0.0.0.0/0 tcp 554 Anywhe 30000-33000 Anywhe 0.0.0.0/0 udp 8080-8084 Anywhe 0.0.0.0/0 V tcp 0.0.0.0/0 tcp 8443-8445 Anywhe Anywhe 8888 0.0.0.0/0 V tcp 9091 Anywhe 0.0.0.0/0 tcp 0.0.0.0/0 Anywhe tcp 1935 1935 Anywhe 0.0.0.0/0 udp Rules with source of 0.0.0.0/0 allows all IP addresses to access your instance. We recommend limiting access to only known IP addresses. Cancel Save

2.5. In "Listeners and routing" section add Websocket port listener (mandatory) and HTTP port listener (if needed)

Listener HT	FP:8080		Remove
Protocol	Port	Default action Info	
HTTP v	: 8080	Forward to test-ws-app-group Target type: Instance, IPv4	нттр 🖉 С
Listener HT	FP:8081		Remove
▼ Listener HT	Port	Default action Info	Remove
 Listener HT Protocol HTTP 	Port : 8081	Default action Info Forward to test-http-app-group Target type: Instance, IPv4	Remove

A target group must be created for every listener, see below.

2.6. Click Create load balancer

 Tags - optional Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Vexample, you can have Key = production-webserver, or Key = webserver, and Value = production. Summary Review and configurations. Estimate cost Basic configuration Edit TEST-APP-LB Internet-facing IPv4 Internet-facing IPv4 	Value' is optional. For
Summary Review and confirm your configurations. Estimate cost I Security groups Edit Network mapping Edit Listeners and Basic configuration Edit Security groups Edit Network mapping Edit Listeners and TEST-APP-LB • default VPC vpc-e305fc9a I • HTTP:8080 • Internet-facing • g-9c127cdf I • eu-west-1a • HTTP:8081 • IPv4 • ubmet-003b4c5a I • Http://west-1a • Http://west-1a	routing Edit
Basic configuration Edit Security groups Edit Network mapping Edit Listeners and TEST-APP-LB • default VPC vpc-e305fc9a 2 • HTTP:8080 • Internet-facing sg-9c127cdf 2 • eu-west-1a test-ws-app- • IPv4 subnet-003b4c5a 2 • HTTP:8081	routing Edit
(csentep op) defaults to group [2] defaults to p-group [2]
Add-on services Edit Tags Edit None None	
Attributes Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.	

Load balancer is created

Successfully created load balancer: <u>TEST-APP-LB</u> Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic. Targets will also take a few minutes to complete the registration proces	is and pass initial health checks.
EC2 > Load balancers	
 Suggested next steps Review, customize, or enable attributes for your load balancer and listeners using the Description and Listeners tabs within TEST-APP-LB. Discover other services that you can integrate with your load balancer. Visit the Integrated services tab within TEST-APP-LB. 	

3. Websocket listener target group creation

3.1. Choose target type Instances (supposed by default), set group name

Step 1 Specify group details	Specify group details Your load balancer routes requests to the targets in a target group and performs health checks on the targets.
Step 2 Register 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.
	 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.
	 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
	test-ws-app-group
	A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen. Protocol Port
	HTTP V : 8080

3.2. Set WCS instance Websocket port (8080), choose subnet and protocol version (HTTP1)

H	TTP 🔻 : 8080	
VPC	c	
Sele	ect the VPC with the instances that you want to include in the target group.	
- VF	pc-9305fc9a	
IP	v4: 172.31.0.0/16	
IP Pro	vterol version	
Pro	http://www.argets.using.	
Pro	http://www.analysia.com/analysi	
Pro	Pv4: 172.31.0.0/16 ptocol 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.	

3.3. In "Health check" configigure instance health check using HTTP port (8081) and statistics page query /?action=stat

Health check protocol TTP ▼ HTTP ▼ HTTP ▼ Health check path Use the default path of '/' to ping the root, or specify a custom path if preferred. ?/action=stat Up to 1024 characters allowed. Restore defaults Port The port the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer, but you can specify a different port. Traffic port Override 8081 1-65555 Healthy threshold The number of consecutive health check failures required before considering an unhealthy target healthy. S 2-10 Unhealthy threshold The number of consecutive health check failures required before considering an unhealthy. Ten ord of the consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures required before considering a target unhealthy. Ten ord of the number of consecutive health check failures require	Health checks The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their s	itatus.
Health check path Use the default path of "/" to ping the root, or specify a custom path if preferred. [?action=stat Up to 1024 characters allowed. Advanced health check settings Restore defaults Port The port the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer uses of the number of consecutive health checks successes required before considering an unhealthy target healthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 2 2-10 2 2-10 The amount of time, in seconds, during which no response means a failed health check.	Health check protocol	
J2action=stat	Health check path Use the default path of "/" to ping the root, or specify a custom path if preferred.	
 ★ Advanced health check settings Restore defaults Port The port the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer, but you can specify a different port. Traffic port Override 8081 1-65535 Healthy threshold The number of consecutive health checks successes required before considering an unhealthy target healthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 2 2.10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 2 2.10 Timeout The amount of time, in seconds, during which no response means a failed health check. 5 seconds	/?action=stat Up to 1024 characters allowed.	
Port The port the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer, but you can specify a different port. Traffic port Override 8081 1-65535 Healthy threshold The number of consecutive health checks successes required before considering an unhealthy target healthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 2 1-0 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 5 2-10	Advanced health check settings	Restore defaults
Healthy threshold The number of consecutive health checks successes required before considering an unhealthy target healthy. 5 2-10 Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 2 2-10 Timeout The amount of time, in seconds, during which no response means a failed health check. 5 seconds	Port The port the load balancer uses when performing health checks on targets. The default is the port on which each targer load balancer, but you can specify a different port. Traffic port Override 8081 1-65535	t receives traffic from the
Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 2 2-10 Timeout The amount of time, in seconds, during which no response means a failed health check. 5 seconds	Healthy threshold The number of consecutive health checks successes required before considering an unhealthy target healthy. 5 2-10	
Timeout The amount of time, in seconds, during which no response means a failed health check. 5 seconds	Unhealthy threshold The number of consecutive health check failures required before considering a target unhealthy. 2-10	
5 seconds	Timeout The amount of time, in seconds, during which no response means a failed health check.	
	5 seconds	

Then click Next

)2™) or a range
)2") or a range
)2") or a range
em.

3.4. At "Register targets" page select instances as needed and click "Include as pending below"

Regi	legister targets										
Select in	stances, specify ports, and add the in	stances to	o the list of pending targe	ets. Repea	t to add additional comb	bination	s of instances and ports to the list of pending target	ts. Once you are satisfied	with yo	ur selections, click Register pending targets.	
Avai	Available instances (2/2)										
Q	Filter resources by property or value										< 1 > 💿
	Instance ID	⊽	Name	▽	State	▽	Security groups	Zone	⊽	IPv4 address	Subnet ID
	i-0dec078d94e7520ef				⊘ running		Web Call Server 5-5-2-944-systemd246- AutogenByAWSMP-	eu-west-1b		3.249.98.141	subnet-41072d27
	i-0dbaf422e637b2d9a				⊘ running		Web Call Server 5-5-2-944-systemd246- AutogenByAWSMP-	eu-west-1b		34.240.11.186	subnet-41072d27
							2 selected				
							Ports for the selected instances Ports for routing traffic to the selected instances. 8080 1-65535 (separate multiple ports with commas)				
							Include as pending below				

Then click "Register pending targets"

Review	targets								
Targe All	ets (2) Q. Filter res 	sources by property or value							Remove all pending
Remov	ve Health status	Instance ID v	Name \triangledown	Port ⊽	State ⊽	Security groups	Zone 🗸	IPv4 address	Subnet ID
×	Pending	i-0dbaf422e637b2d9a		8080	⊘ running	Web Call Server 5-5-2-944-systemd246-AutogenByAWSMP-	eu-west-1b	34.240.11.186	subnet-41072d27
×	Pending	i-0dec078d94e7520ef		8080	⊘ running	Web Call Server 5-5-2-944-systemd246-AutogenByAWSMP-	eu-west-1b	3.249.98.141	subnet-41072d27
2 pending	g							Cancel	Register pending targets

Target group is created

O Successfully created target group: test-ws-app-group		3
EC2 > Target groups		
Target groups (3) Info	C Actions Create target group	*
Q Search or filter target groups	< 1 > ©	Ľ
Name ▼ ARN ▼ Port ▼ Protocol ▼ Target type ▼ Load balancer		l
test-ws-app-group arm:aws:elasticloadbalancin 8080 HTTP Instance -	vpc-e305fc9a	
		1
		*
Select a target group above.		

Application load balancer using this group will forward requests to it after at least one of the group instances passes health check.

4. Listener parameters configuration

If Application Load Balancer is created to use in Autoscaling group (see below), HTTPS listener cannot be configured on creation, only HTTP. In this case, listener parameters shoul be changed.

4.1. In EC2 Console section "Load balancers - Load balancers" choose "Listeners" tab for load balancer to configure. Choose Websocket listener and click Edit

ad ba	llancer: TestAppLb			U.	
)escri	ption Listeners Mo	nitoring Integrat	ted services Ta	gs	
isten	ers listen for connection requ	ests using their prot	tocol and port. You o	can add, remove, or update listeners and listener rules.	
īo viev	w and edit listener attributes,	select the listener a	ind choose Edit.		
Add	listener Edit Delet	e			
	Listener ID	Security policy	SSL Certificate	Rules	
	Listener ID HTTP : 8080	Security policy	SSL Certificate	Rules Default: forwarding to TestAppLbTargetGroup	
	Listener ID HTTP : 8080 arn6b57d519144f72fa -	Security policy	SSL Certificate	Rules Default: forwarding to TestAppLbTargetGroup View/edit rules	
	Listener ID HTTP : 8080 arn6b57d519144f72fa - HTTP : 8081	Security policy N/A N/A	SSL Certificate	Rules Default: forwarding to TestAppLbTargetGroup View/edit rules Default: forwarding to TestAppLbHttpTargetGroup	

4.2. Choose HTTPS protocol and set Secure Websocket port (8443 for example)

Listener details A listener is a process that checks for connect routed per your specification. You can specify	tion requests, using the p y multiple rules and mult	protocol and port you configure. Traffi iple certificates per listener after the l	received by the listener is then oad balancer is created.
Protocol Port HTTPS HTTPS HTTPS HTTPS			
 Specify the default actions for traffic on this istener. Rules can be configured after the list T. Forward to Info 	listener. Default actions a tener is created.	apply to traffic that does not meet the	conditions of rules on your
Target group	C	Weight (0-999)	
Tost Appl bTarget Croup	HTTP 🔻	1 X	
Target type: Instance, IPv4		100%	
Target type: Instance, IPv4	Traffic distribution:	10070	
Target type: Instance, IPv4 Select a target group	Traffic distribution:	0 ×	

4.3. In "Secure listener settings" section choose SSL certificate to use with domain asigned to load balancer entry point or create a new one. Then click "Save changes"

Security policy Your load balancer use to negotiate SSL conne	s a Secure Socket Layer (SSL) negotiation configuration, known as a security policy, actions with clients.	
ELBSecurityPolicy	-2016-08	
Compare security p	olicies 🗹	
Compare security p Default SSL certifica The certificate used if a more certificates after	olicies ate a client connects without SNI protocol, or if there are no matching certificates. You can add you create the load balancer.	
Compare security p Default SSL certifica The certificate used if a more certificates after From ACM	olicies ate a client connects without SNI protocol, or if there are no matching certificates. You can add you create the load balancer. ▼ .flashphoner.com d62e2c7d-23a5-4ef2-8244-6b7dc92d9246	

Load balancer listener parameters are changed and will be applied immediately

Suggested next steps	
Review or customize your listener. Edit listener	

Launching AWS Auto Scaling group with load balancing from AWS Marketplace AMI

Load balancer with autoscaling deployment from AWS Marketplace AMI can be useful for periodic servers group launching, for example, during the event (lasting for hours, days, weeks). In this case, WCS monthly subscription may be more expensive then AWS hourly payment, therefore it is recommeded to use AWS Marketplace AMI.

1. Create launch template

1.1. In EC2 Console go to "Instances - Launch Templates" section and click "Create launch template". Launch template creation wizard will open. Enter template name and description

reate launch templa	ate	
ating a launch template allows you to er time. Templates can have multiple ve	create a saved instance configuration that can be ersions.	reused, shared and launched at a
Launch template name and d	lescription	
Launch template name - required		
TestTemplate		
Must be unique to this account. Max 128 char	rs. No spaces or special characters like '&', '*', '@'.	
Template version description		
Test autoscaling launch template]
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		

1.2. Choose latest FlashphonerWebCallServer image

aunch temp becify the deta	te contents of your launch template below. Leaving a field blank will result in the field not being included in the launch
Amazon r	chino imago (AMI) un
Amazon r	
Flashphone ami-035ddfe	ebCallServer-5.2.629-x86_64-hourly-01e37234-6170-4b8d-98b



t2.micro Family: General purpose 1 vCPU 1 GiB Memory On-Demand Linux pricing: 0.0126 USD per Hour On-Demand Windows pricing: 0.0172 USD per Hour	Free tier eligible	Instance types 🔼
ey pair (login) Info		
ey pair name		
test_userdata	▼	Create new key pair
letwork settings		
etworking platform Info		
letwork settings etworking platform Info Virtual Private Cloud (VPC) Launch into a virtual network in your own logically isolated area within the AWS cloud	 EC2-Classic Launch into a single flat network other customers 	vork that you share with
letwork settings etworking platform Info Virtual Private Cloud (VPC) Launch into a virtual network in your own logically isolated area within the AWS cloud ecurity groups Info	 EC2-Classic Launch into a single flat network other customers 	vork that you share with

1.4. Set disk size and parameters for instances

Storage (volumes) Info		
 Volume 1 (AMI Root) AMI Volumes are not included in 	he template unless modified	
Volume type Info EBS	Device name - <i>required</i> Info /dev/sda1	Snapshot Info snap-Ofee0446fee3252a5
Size (GiB) Info	Volume type Info	IOPS Info
10	General purpose SSD (gp2)	▼ 2000
Delete on termination Info	Encrypted Info	Key Info
Yes	▼ No	▼ МуКеу
Add new volume		

1.5. Expand "Advanced details" section. Insert custom update and setup script to "User data" text box

#!/bin/bash	Â	
# Stop WCS before reconfiguring		
PID="\$(pgrep -f 'com.flashphoner.server.Server' grep -v bash)"		
if [-n "\$PID"]; then		
service webcallserver stop		
fi		
# Update WCS to the latest build (optionally, set to false if you don't)		
UPDATE=true		
if \$UPDATE; then	-	
cd /tmp		
User data has already been base64 encoded		
	Cancel	Create template version

The setup script example to update WCS to latest build and to configure CDN Edge server for WebRTC playback

Edge setup script

```
#!/bin/bash
# Stop WCS before reconfiguring
PID="$(pgrep -f 'com.flashphoner.server.Server' | grep -v bash)"
if [ -n "$PID" ]; then
    service webcallserver stop
fi
# Update WCS to the latest build (optionally, set to false if you don't)
UPDATE=true
if $UPDATE; then
   cd /tmp
   wget --timeout=10 --no-check-certificate https://flashphoner.com/download-wcs5.2-server.tar.gz -O wcs5-
server.tar.gz
   if [ $? -eq 0 ]; then
       mkdir -p FlashphonerWebCallServer-5.2-latest && tar xzf wcs5-server.tar.gz -C FlashphonerWebCallServer-
5.2-latest --strip-components 1
       cd FlashphonerWebCallServer-5.2-latest
       chmod +x install.sh
       ./install.sh -silent
       cd ..
       rm -rf FlashphonerWebCallServer-5.2-latest wcs5-server.tar.gz
    fi
fi
# Configuration setup
WCS_CONFIG=/usr/local/FlashphonerWebCallServer/conf/flashphoner.properties
JVM_CONFIG=/usr/local/FlashphonerWebCallServer/conf/wcs-core.properties
USERS_CONFIG=/usr/local/FlashphonerWebCallServer/conf/database.yml
#CDN settings
CDN_ROLE=edge
CDN IP=0.0.0.0
CDN_POINT_OF_ENTRY=172.31.43.82
echo -e "\ncdn_enabled=true" >> $WCS_CONFIG
echo -e "\ncdn_ip=$CDN_IP" >> $WCS_CONFIG
echo -e "\ncdn_role=$CDN_ROLE" >> $WCS_CONFIG
echo -e "\ncdn_point_of_entry=$CDN_POINT_OF_ENTRY" >> $WCS_CONFIG
echo -e "\ncdn_nodes_resolve_ip=false" >> $WCS_CONFIG
# Configure heap settings
HEAP_SIZE=512m
sed -i -e "s/^\(-Xmx\).*\$/\1$HEAP_SIZE/" $JVM_CONFIG
# Disable demo user (optionally, set to true if you want to disable)
DISABLE DEMO=false
if $DISABLE_DEMO; then
if grep "demo:" $USERS_CONFIG > /dev/null 2>&1; then
 sed -i -e "/demo:/s/active:\ true/active:\ false/" $USERS_CONFIG
fi
fi
# Start WCS after reconfiguring
PID="$(pgrep -f 'com.flashphoner.server.Server' | grep -v bash)"
if [ -n "$PID" ]; then
   service webcallserver restart
else
    service webcallserver start
fi
# Disable internal firewall, ports are allowed/blocked on security group level
iptables -F
```

Add tag	are currently included in this template. Add a resource tag to include it in the launch template.
0 remaining (Up to	50 tags maximum)
Network inte	
lo network inter	faces are currently included in this template. Add a network interface to include it in the launch
emplate.	
emplate. Add network	interface
emplate. Add network	interface details Info

aunch templates				C Actions V Create launch	template
Q Filter by tags or properties or search	by keyword			< 1	1 > @
Launch template ID		♥ Default version		▼ Create time	,
) lt-04d44d426947bae18	TestTemplate	1	1	2020-07-14T06:40:07.000Z	

2. Create Auto scaling group

2.1. In EC2 Console go to "Instances - Auto Scaling Groups" section and click "Create an Auto Scaling Group". Autoscaling group creation wizard will open. Enter group name

ep 1 Noose launch template or	Choose launch temp	late or configurati	ON Info
onfiguration	Specify a launch template that contains	ettings common to all EC2 instances	s that are launched by this Auto Scaling group. If
Step 2 Configure settings	you currently use launch configurations, t	you might consider migrating to laur	ich templates.
Step 3 (optional) Configure advanced options	Auto Scaling group name Enter a name to identify the group.		
Step 4 (optional) Configure group size and scaling policies	TestAutoscalingGroup Must be unique to this account in the curren	t Region and no more than 255 characters	
Step 5 <i>(optional)</i> Add notifications	Launch template Info		Switch to launch configuration
Step 6 (optional) Add tags	Launch template Choose a launch template that contains the security groups.	instance-level settings, such as the Amazo	n Machine Image (AMI), instance type, key pair, and
	TestTemplate		▼ C
Step 7 Review	Create a launch template 🖄 Version Default (1) V C Create a launch template version 🖄]	
	Description Test autoscaling launch template	Launch template TestTemplate 2 It-04d44d426947bae18	Instance type -
	AMI ID ami-035ddfe555ad2e6f8	Security groups	Security group IDs -
	Key pair name		

2.2 Choose launch template, set "Latest" version

Launch template Info		Switch to launch configuration
Launch template Choose a launch template that contains security groups.	the instance-level settings, such as the Amazon Ma	achine Image (AMI), instance type, key pair, and
TestTemplate		C
Create a launch template 🗹		
Version		
Latest (2)	2	
Create a Jaunch template version D	~	
create a taunch temptate version E	-	
Description	Launch template	Instance type
-	TestTemplate 🗹	t2.micro
	lt-04d44d426947bae18	
AMI ID	Security groups	Security group IDs
ami-035ddfe555ad2e6f8	-	sg-0ec50e70028ff86d7 🔀
Key pair name		
test userdata		
Additional details		
Storage (volumes)	Date created	
/dev/sda1	Tue Jul 14 2020 14:02:03 GMT+070	0
	(Novosibirsk Standard Time)	

2.3. Set instances distributon percentage (on demand/spot). By default 70 % on demand will be set, it is recommended to raise this value to 100 %

hoose launch template or	Configure settings Info
onfiguration	Configure the settings below. Depending on whether you chose a launch template, these settings may include options to help you make optimal use of EC2 resources.
tep 2 Configure settings	Purchase options and instance types Info
tep 3 (optional) Configure advanced options	Adhere to launch template Combine purchase options and instance types
tep 4 (optional) Configure group size and caling policies	The launch template determines the purchase option (On- Demand or Spot) and instance type. Specify how much On-Demand and Spot capacity to launch and multiple instance types (optional). This choice is most helpful for optimizing the scale and cost for a fleet of instances.
tep 5 <i>(optional)</i> dd notifications	Instances distribution Optional On-Demand base Specify how much On-Demand capacity the Auto Scaling group should have for its base portion. The maximum group size will be increased
tep 6 (<i>optional</i>) Idd tags	(but not decreased) to this value. 0 On-Demand Instances
tep 7 Ieview	On-Demand percentage above base Define the percentage split of On-Demand Instances and Spot Instances for your additional capacity beyond the base portion. 70 % On-Demand
	30 % Spot
	 Capacity optimized - Launch Spot Instances optimally based on the available Spot capacity (recommended)

2.4 Choose instance types

2	e the instance types that best suit the needs	s of your application.
Primar	ry instance type	Weight Info
1.	t 2.micro 1vCPU 1 Gib Memory	▼
Additio	Your launch template does not specify an i chosen. You can continue by adding an ins onal instance types	instance type. As a result, Adhere to launch template cannot be tance type above.
Additio Redo r	Your launch template does not specify an chosen. You can continue by adding an ins onal instance types ecommendations	instance type. As a result, Adhere to launch template cannot be tance type above.

2,5. Choose VPC and subnets for instances

Network Info	
For most applications, you can use multip zones. The default VPC and default subne	Ne Availability Zones and let EC2 Auto Scaling balance your instances across the ets are suitable for getting started quickly.
VPC	
vpc-e305fc9a 172.31.0.0/16 Default	▼ C
Create a VPC 🔀	
Subnets	
Select subnets	▼ C
Create a subnet 🔼	
	Cancel Previous Skip to review Next

2.6.Choose "Attach to a new load balancer"

Step 1 Choose launch template or	Configure advanced options Info
configuration	Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.
Step 2 Choose instance launch options	Load balancing - optional Info
Step 3 (optional) Configure advanced options	Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.
Step 4 (optional) Configure group size and scaling policies	 No load balancer Traffic to your Auto Scaling group will not be fronted by a load balancer. Attach to an existing load balancer Choose from your existing load balancer to attach to your Auto Scaling group.
Step 5 (optional) Add notifications	
Step 6 (optional)	Attach to a new load balancer
	Denne a new toat batancer to create for actacimient to this Auto scaling group.
Step 7 Review	Load balancer type Choose from the load balancer types offered below. Type selection cannot be changed after the load balancer is created. If you need a different type of load balancer than those offered here, visit the Load Balancing console.
	Application Load Balancer HTTP, HTTPS

2.7. Choose "Application Load balancer" type, set the name, choose Internet-facing, set availability zones and corresponding subnets

	o create for attachment to this Auto Sca	aling group.
Load balancer type Choose from the load baland different type of load baland	er types offered below. Type selection c er than those offered here, visit the Lo a	annot be changed after the load balancer is created. If you need a ad Balancing console.
• Application Load HTTP, HTTPS	Balancer	Network Load Balancer TCP, UDP, TLS
Load balancer name Name cannot be changed af	ter the load balancer is created.	
TestAppLb		
Internal	arter the load balancer is created.	
Network mapping	be created using the same VPC and Avai	ability Zone selections as your Auto Scaling group. You can select
Network mapping Your new load balancer will different subnets and add su	be created using the same VPC and Avai bnets from additional Availability Zones	lability Zone selections as your Auto Scaling group. You can select
Network mapping Your new load balancer will different subnets and add su VPC vpc-5e65c237	be created using the same VPC and Avai bnets from additional Availability Zones	lability Zone selections as your Auto Scaling group. You can select
Network mapping Your new load balancer will different subnets and add su VPC vpc-5e65c237 2 Availability Zones and su You must select a single sub	be created using the same VPC and Avai ibnets from additional Availability Zones ibnets net for each Availability Zone enabled. C	lability Zone selections as your Auto Scaling group. You can select s.
Network mapping Your new load balancer will different subnets and add su VPC vpc-5e65c237 2 Availability Zones and su You must select a single sub eu-north-1a	be created using the same VPC and Avai ibnets from additional Availability Zones ubnets net for each Availability Zone enabled. C subnet-d2cb6fbb	Internet-facing Internet-facin
Network mapping Your new load balancer will different subnets and add su VPC vpc-5e65c237 2 Availability Zones and su You must select a single sub eu-north-1a eu-north-1c	be created using the same VPC and Avai ibnets from additional Availability Zones ibnets net for each Availability Zone enabled. C subnet-d2cb6fbb Select a subnet	Internet-facing Iability Zone selections as your Auto Scaling group. You can select S. Only public subnets are available for selection to support DNS resolution.

2.8. In "Listeners and routing" section set Websocket port (8080), choose "Create a target group" and set the target group name to be created

Protocol	Port	Default routing (forward to)
HTTP	8080	Create a target group 🔻
		New target group name An instance target group with default settings will be created.
		TestAppLbTargetGroup
Tags - optional Consider adding Add tag	l tags to your load balancer. Tags	enable you to categorize your AWS resources so you can more easily manage them.

Then click Next

Additional settings - optional						
Monitoring Info Enable group metrics collection within CloudWatch						
	Cancel	Previ	ous	Skip to revi	ew	Next

2.9. Set the maximum group size

ep 1 hoose launch template or	Configure group size and scaling policies Info
onfiguration	Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.
tep 2 Configure settings	Group size - optional Info
itep 3 (optional) Configure advanced options	Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.
Step 4 (optional) Configure group size and scaling policies	Desired capacity
Step 5 (optional) Add notifications	Minimum capacity
Step 6 (optional) Add tags	Maximum capacity 3
Step 7 Review	Scaling policies - optional
	Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. Info
	• Target tracking scaling policy Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.
	Scaling policy name
	Target Tracking Policy

2.10. Select scaling policy by CPU utilization, set target value and instance warming time

	ether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. Info
• Targe Choos policy that o	et tracking scaling policy se a desired outcome and leave it to the scaling y to add and remove capacity as needed to achieve outcome.
caling pol	icy name
Target Tra	acking Policy
letric type	2
Average (CPU utilization
arget valu	le la
80	
80 Instances n	eed
80 1stances n 60	eed seconds warm up before including in metric
80 nstances n 60] Disable	eed seconds warm up before including in metric scale in to create only a scale-out policy
80 Instances n 60 Disable Instance	eed seconds warm up before including in metric scale in to create only a scale-out policy scale-in protection - optional

2.11. Review group parameters

EC2 > Auto Scaling groups >	Create Auto Scaling group						
Step 1 Choose launch template or configuration	Review Info						
Step 2	Step 1: Choose laun	ch template o	or configuration		Edit		
Configure settings	Group details	Group details					
Step 3 (optional) Configure advanced options	Auto Scaling group na TestAutoscalingGroup	me					
Step 4 (optional) Configure group size and scaling policies	Launch template		Version	Description			
Step 5 (optional) Add notifications	TestTemplate 🗹 lt-04d44d426947bae1	8	Latest				
Step 6 (optional) Add tags	Step 2: Configure se	ettings			Edit		
Step 7	Purchase options	and instance	e types				
Review	Instances distribu	tion					
	On-Demand base		On-Demand and Spot percentages	Spot allocation strategy			
	Designate the first 0 ir Demand	istances as On-	100 % On-Demand 0 % Spot	Capacity optimized			
	Instance types						
	Instance type	vCPUs	Memory	Network perform	ance		
	1. t2.micro	1 vCPU	1 GiB	Low to Moderate			

2.12. Click "Create Auto Scaling group"

Step 5: Add no	tifications		Edit
Notification	IS		
No notifications	5		
Step 6: Add tag Tags (0)	gs		Edit
Кеу	Value	Tag new instances	
		No tags	

Autoscaling group will be created, and one instnce will be launched

New EC2 experience Tell us what you think		TestAutoscalingGroup, 1 Scaling policy created successfully						
EC2 Dashboard New	EC2 > Auto Scaling groups							
Events New								
Tags	Auto Scaling groups (1)	C Edit Delete Create an Auto Scaling group						
Reports	Q. Search your Auto Scalina aroups	< 1 > @						
Limits								
INSTANCES	□ Name ▼ Launch template/configuration II ▼ Instances ▼	Status \triangledown Desired capacity \triangledown Min \triangledown Max \triangledown Availability Zones \triangledown						
Instances	TestAutoscalingGroup TestTemplate Version Latest 0	Updating capacity 1 1 3 eu-west-1a						
Instance Types								
Launch Templates								

2.13. Configure load balancer listener as described above

Testing

If load balancer has no running instances, then a new instance will be started when an auto scaling group receiving traffic from the load balancer is created. More instances will be started in case scaling is triggered. (For testing purposes, streaming with transcoding – e.g., streaming RTMP to auto created mixer – can be used to load server CPU.) All the started instances will be auto added to the corresponding load balancer.

When an instance (one or more of the added to the balancer) is in service, ws-connection can be done to, e.g., ws://<Load balancer DNS name>:8080.

A demo – e.g., Two-way Streaming - example (opened either by the balancer or an instance address) can be used to establish ws-connection:

😯 Flashp	honer Web Call Serv	er X	🦻 Flashphoner W	eb Call Server	×	+				
← → C	۵	(i)	test-lb-19794975	97.us-east-1.e	elb.am	azonaws.	.com:8081/	admin/de	emo.htr	nl#
🕑 Demo	🚡 Security 👻 🕻	2 License							v.0.5.28.2	2753-5.2.69-
Streaming Streamer			-	Two-way	Strea	aming				
Player	[Local		[Playe	r		
Two-Way Streaming										
Firewall Streaming										
WebRTC as RTMP										
Stream Recording										
Stream Snapshot		d9bb		Publish		d9bb	Play	Available		
Stream Diagnostic			-LB-1979497	597.us-east-1.elb.;	amazona	ws.com:8	Disconnect			
Screen Sharing				ESTAB	ISHED					

To verify that the connections are distributed between active load balancer instances, use the stats page: http://WCS_ADDRESS:8081/?action=stat

Open the page for each of the instances to see the connection_websocket number:

ec2-3-82-201-0.compute-1.	ama 🗙	ec2-54-224-92-107.compute-1. X	+			
$\overleftarrow{\leftarrow}$ \rightarrow \bigcirc \textcircled{a}	i ec2-3-82-201-0.compute-1.amazonaws.com:8081/?action=stat					
Connection Stats connections=2 connections rtmfp=0 connections_websocket=2 Port Stats ports_media_free=499 ports_media_busy=0 ports_media_guarantine=0 Stream Stats						