AWS

–

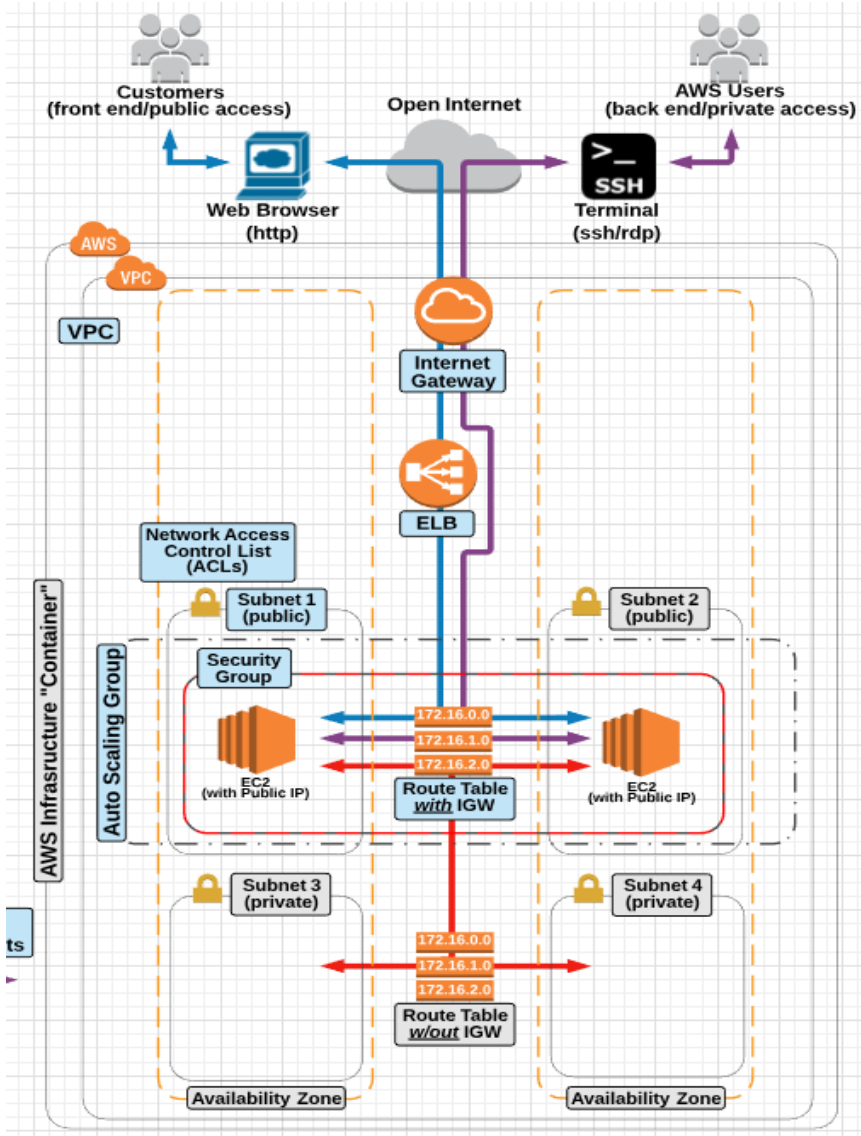
ELB & Auto Scaling Group

By

Keshav Kummari

Elastic Load Balancer

- A load balancer can **distribute incoming traffic** across your EC2 instances.
- This enables you to increase the **availability of your application**.
- The load balancer also **monitors the health of its registered instances** and ensures that it routes traffic only to healthy instances.
- You configure your load balancer to accept **incoming traffic** by specifying one or more **listeners**, which are configured with a **protocol** and **port number** for connections from clients to the load balancer and a protocol and port number for connections from the load balancer to the instances.
- Elastic Load Balancing supports **three types of load balancers**: ***Application Load Balancers, Network Load Balancers, and Classic Load Balancers***.
- All Elastic Load Balancing operations are *idempotent* , which means that they complete at most one time.
- If you repeat an operation, it succeeds with a **200** OK response code.


Customers
(front end/public access)
Open Internet
AWS Users
(back end/private access)
Web Browser
(http)
SSH
Terminal
(ssh/rdp)
AWS
VPC
VPC
Internet Gateway
ELB
Network Access Control List (ACLs)
Subnet 1 (public)
Subnet 2 (public)
Security Group
Auto Scaling Group
AWS Infrasructure "Container"
172.16.0.0
172.16.1.0
172.16.2.0
EC2
(with Public IP)
Route Table with IGW
EC2
(with Public IP)
Subnet 3 (private)
Subnet 4 (private)
172.16.0.0
172.16.1.0
172.16.2.0
Route Table w/out IGW
Availability Zone
Availability Zone

OSI (Open Systems Interconnection) 7 Layer Model

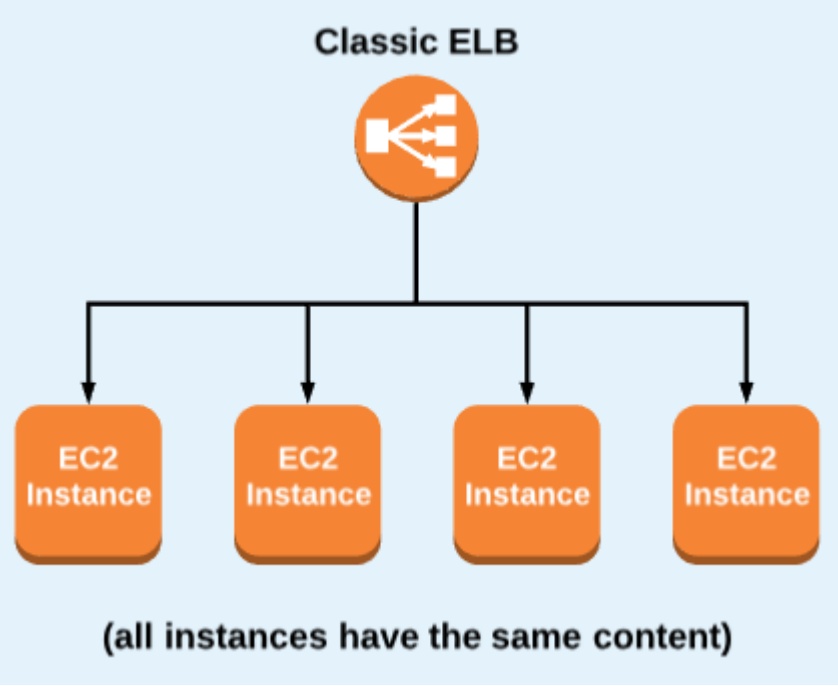
#	Layer	Application	Description	Example
7	Application	Data	Network process to application	DNS, FTP, HTTP, SMTP, Telnet, DHCP
6	Presentation	Data	Data representation and encryption	GIF, JPEG, SSL, MIME
5	Session	Data	Interhost communication	NetBIOS, Sockets, Named Pipes, RPC
4	Transport	Segments	End-to-end connections and reliability	TCP, UDP
3	Network	Packets	Path determination and logical addressing	IP, IPSec, ICMP, BGP
2	Datalinks	Frames	Physical addressing	Ethernet, Wifi, WLAN, MAC
1	Physical	Bits	Media, signal, and binary transmission	CAT5

Elastic Load Balancer(ELB)

- **Load Balancing** is a common method used for distributing incoming traffic among servers.
- An **Elastic Load Balancer** is an EC2 service that automates the process of distributing incoming traffic to all the instances that are associated with the ELB.
- Cross-Zone load balancing :
  - An elastic load balancer can load balance traffic to instances located across multiple availability zones.
  - This allows for highly availability and fault tolerant architecture.
- Elastic load balancing can be paired with **Auto Scaling** to enhance high availability and fault tolerance, and allow for automated scalability and elasticity.
- An ELB has it's own DNS record set that allows for direct access from the open internet access.
- **Important ELB Facts:**
  - An ELB can be **public-facing** or used as an **internal** load balancer and load balancer to internal EC2 instances on Private Subnets(As often done with Multi-Tier Applications).
  - ELB's will automatically stop serving traffic to an instance that becomes unhealthy(Via **healthy checks**)
  - An ELB or ALB can help reduce compute power or an EC2 instance by allowing for an SSL certificate to be applied directly to the elastic load balancer.

Classic Elastic Load Balancer – OSI Layer 4

- A "**Classic**" Elastic Load Balancer is designed for SIMPLE balancing of traffic to multiple EC2 instances.
- There are no granular routing "rules" – all instances get routed to evenly, and no special routing request can be made based on specific content request from the user.
- Protocols : TCP, SSL HTTP, HTTPS



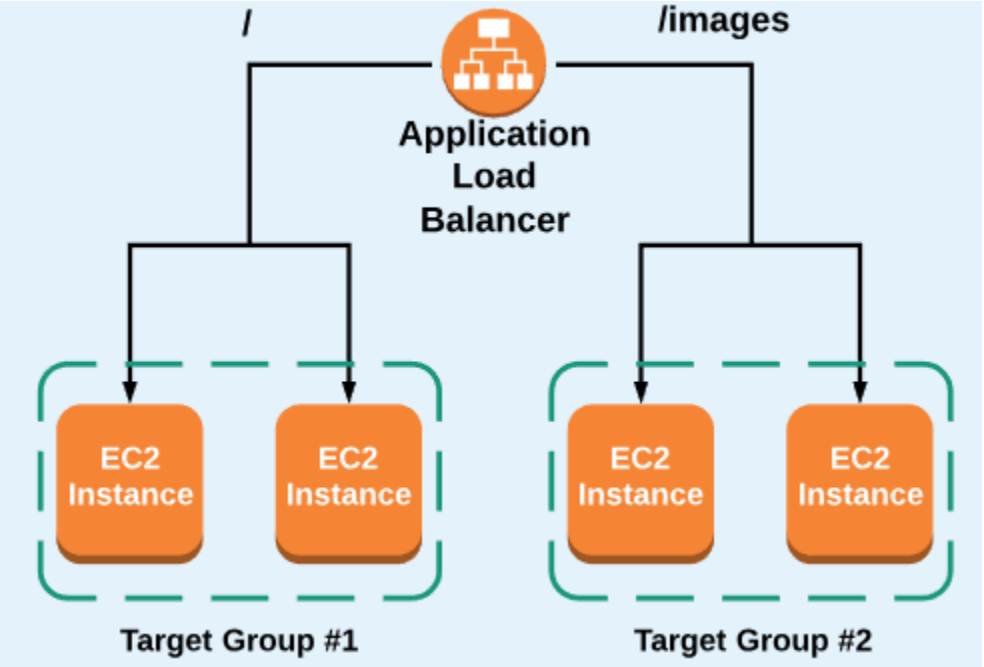
Application Elastic Load Balancer – OSI Layer 7

- An application load balancer is designed for balancing of traffic to one or more instance target grows using **Content-based "rules".**
- Content-based rules(setup on the listener) can be configured using:
  - **Host-based rules:** Route traffic based on the host field of the HTTP header
  - **Path-based rules:** Route traffic based on the URL path of the HTTP header
  - This allows you to structure your application as smaller services, and even monitor/auto-scale based on traffic to specific **"target groups".**
  - Can balance traffic to multiple ports
- An application Load balancer also supports :

ECS and EKS, HTTPS, HTTP/2,

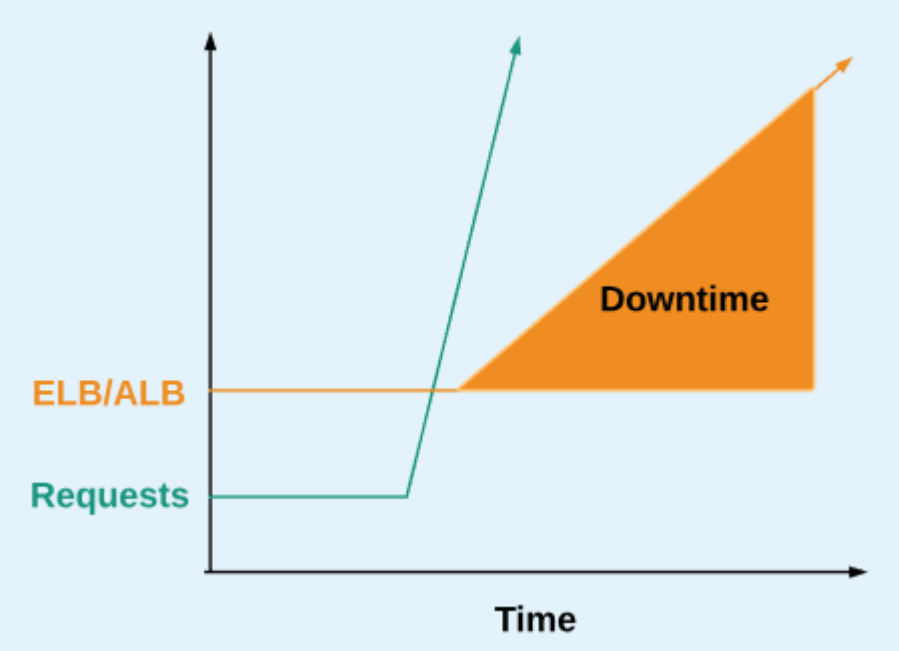
Web Sockets, Access Logs, Sticky Sessions,

and AWS WAF(Web Application Firewall).



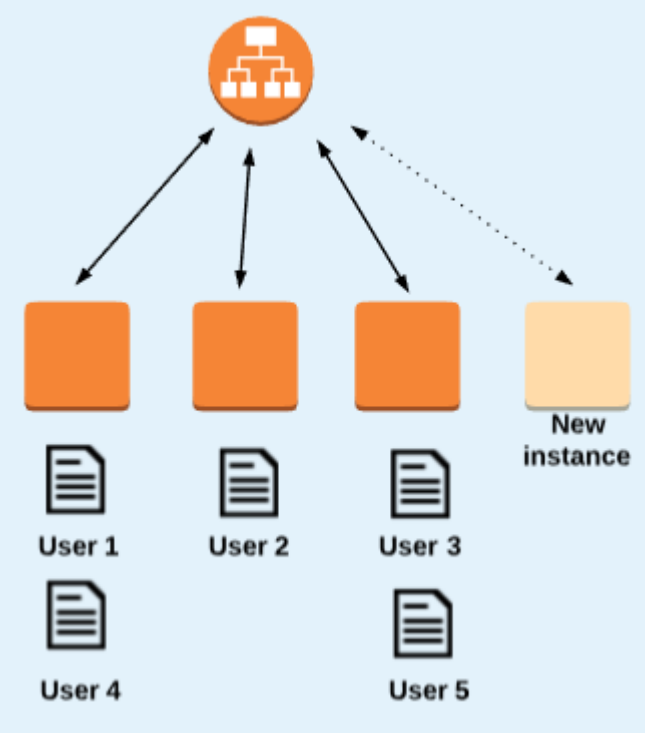
Network Elastic Load Balancer – OSI Layer 3

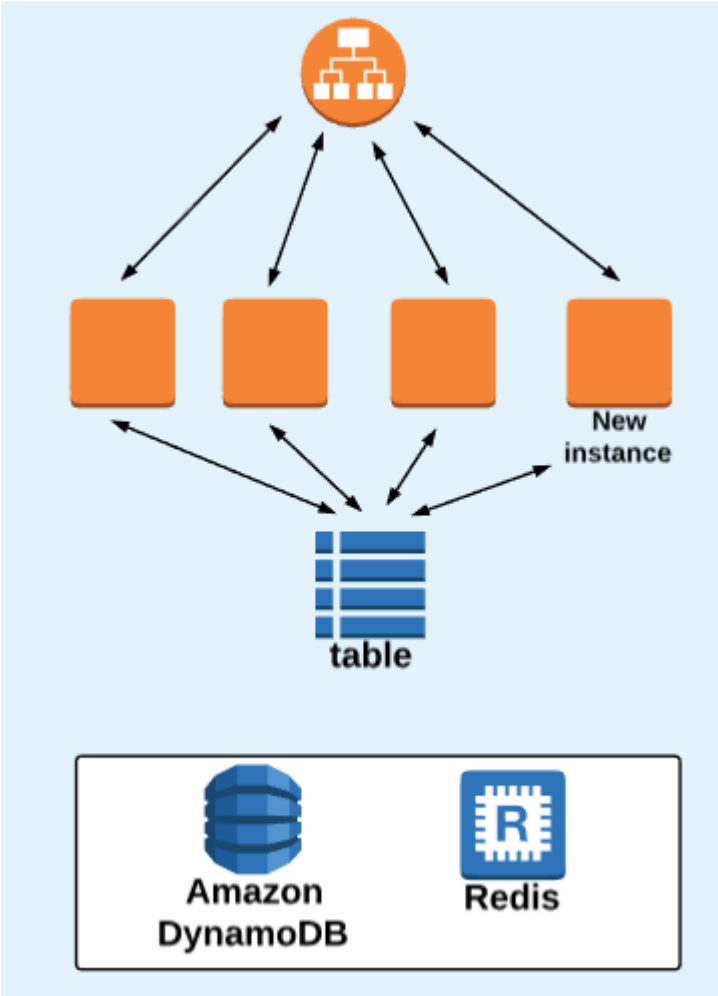
- The Network Load Balancer is designed for extreme performance.
- It does not need to scale to handle large traffic spikes.
- Layer 4 (TCP) load balancing
- Static / Elastic IP address per AZ
- IP Addresses as Targets
- No SSL Offloading



Stateless Architecture

- Store State information Off-Instance
- NoSQL Database
- Shared FileSystem



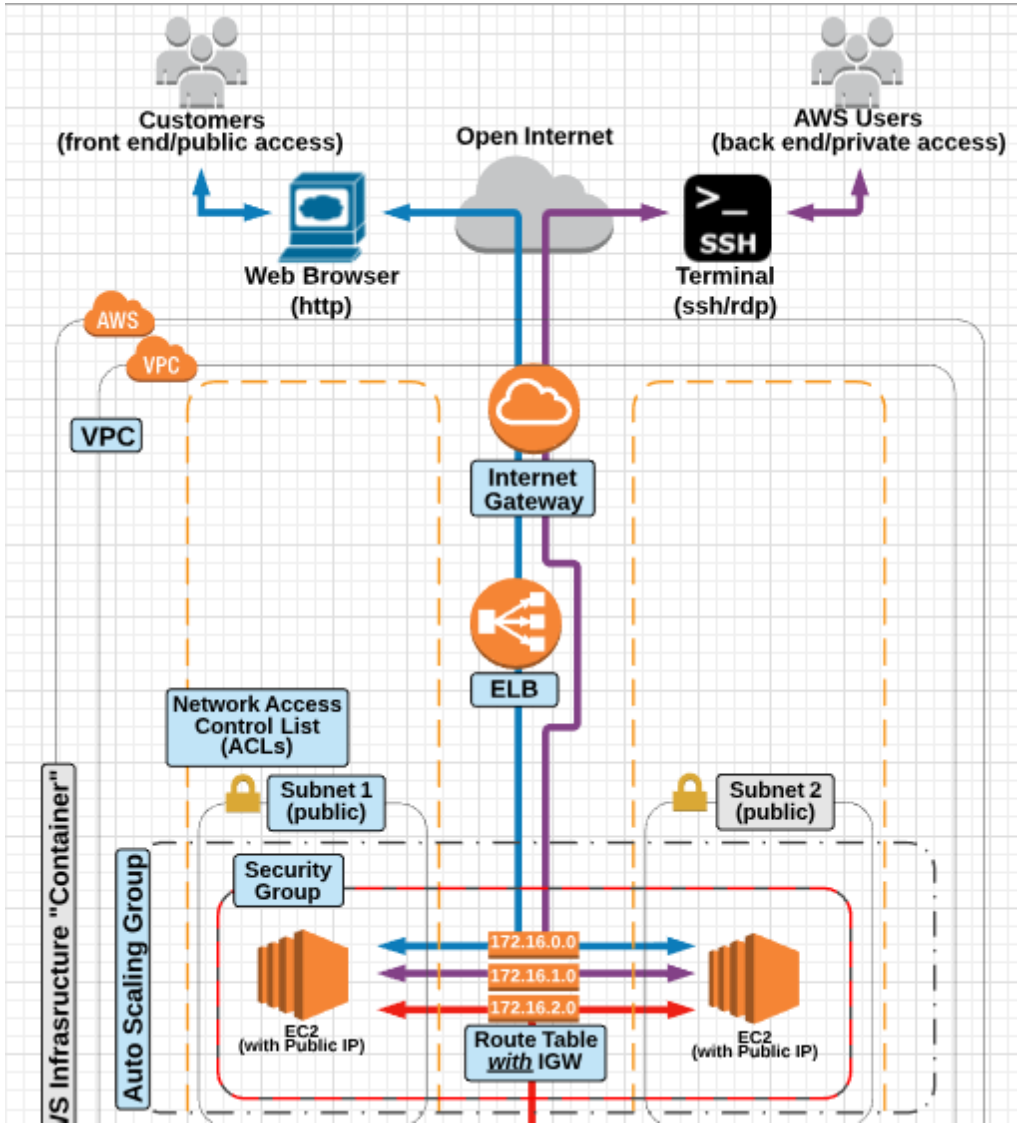


AWS ELB CLI Commands List

https://docs.aws.amazon.com/cli/latest/reference/elb/index.html

- add-tags
- apply-security-groups-to-load-balancer
- attach-load-balancer-to-subnets
- configure-health-check
- create-app-cookie-stickiness-policy
- create-lb-cookie-stickiness-policy
- create-load-balancer
- create-load-balancer-listeners
- create-load-balancer-policy
- delete-load-balancer
- delete-load-balancer-listeners
- delete-load-balancer-policy
- deregister-instances-from-load-balancer
- describe-account-limits
- describe-instance-health
- describe-load-balancer-attributes
- describe-load-balancer-policies
- describe-load-balancer-policy-types
- describe-load-balancers
- describe-tags
- detach-load-balancer-from-subnets
- disable-availability-zones-for-load-balancer
- enable-availability-zones-for-load-balancer
- modify-load-balancer-attributes
- register-instances-with-load-balancer
- remove-tags
- set-load-balancer-listener-ssl-certificate
- set-load-balancer-policies-for-backend-server
- set-load-balancer-policies-of-listener
- wait

Create Classic Elastic Load Balancer



Step-1 Create Classic ELB

Classic Load Balancer

PREVIOUS GENERATION

for HTTP, HTTPS, and TCP

Create

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

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you migh
ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your loa
port 80.

Load Balancer name: myClassicELB

Create LB Inside: My Default VPC (172.31.0.0/16)

Create an internal load balancer: ☐ (what's this?)

Enable advanced VPC configuration: ☑

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Step-2 : Select Subnets

Select Subnets

You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availat Zones to provide higher availability for your load balancer.

VPC vpc-8b5ba2f0 (172.31.0.0/16)

Available subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR
⊕	us-east-1b	subnet-7647072b	172.31.32.0/20
⊕	us-east-1d	subnet-e52c60ca	172.31.80.0/20
⊕	us-east-1e	subnet-88b6f9b7	172.31.48.0/20
⊕	us-east-1f	subnet-0325ea0c	172.31.64.0/20

Selected subnets

Actions	Availability Zone	Subnet ID	Subnet CIDR
⊖	us-east-1a	subnet-ea8194a1	172.31.16.0/20
⊖	us-east-1c	subnet-baab9bde	172.31.0.0/20

Step-3 : Create Security Groups on Port 80 and assign

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances | 6. Add Tags | 7. Review

Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assi
changed at any time.

Assign a security group: Create a **new** security group

Select an **existing** security group

Security group name: elb_sg_01

Description: Classic Elastic Load Balancer - Port-80

Type	Protocol	Port Range	Source
Custom TCP F	TCP	80	Custom 0.0.0.0/0

Step-4 : Configure Health Check

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | **4. Configure Health Check**

Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 instances and only route traffic to insta
balancer. Customize the health check to meet your specific needs.

Ping Protocol TCP

Ping Port 80

Advanced Details

Response Timeout 5 seconds

Interval 10 seconds

Unhealthy threshold 2

Healthy threshold 2

Step-5 : Add EC2 instances to Elastic Load Balancer using Manual or Auto Scaling

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances

Step 5: Add EC2 Instances

The table below lists all your running EC2 Instances. Check the boxes in the Select column to add those instances to this load balancer.

VPC vpc-8b5ba2f0 (172.31.0.0/16)

	Instance	Name	State	Security groups

Availability Zone Distribution

1 instance in us-east-1a

1 instance in us-east-1b

☑ Enable Cross-Zone Load Balancing

☑ Enable Connection Draining 300 seconds

Step-6 : Add Tags & Click on Create

1. Define Load Balancer | 2. Assign Security Groups | 3. Configure Security Settings | 4. Configure Health Check | 5. Add EC2 Instances | **6. Add Tags** | 7. Review

Step 6: Add Tags

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more about tagging your Ar

Key	Value
Name	DevOps_Java-Application

Create Tag

myClassicELB	myClassicELB-1256450764....	vpc-8b5ba2f0	us-east-1a, us-east-1b	classic

Load balancer: myClassicELB

Description | Instances | Health Check | Listeners | Monitoring | Tags | Migration

Basic Configuration

Name: myClassicELB

* **DNS name:** myClassicELB-1256450764.us-east-1.elb.amazonaws.com (A Record)

Type: Classic (Migrate Now)

Scheme: internet-facing

Availability Zones: subnet-7647072b - us-east-1b, subnet-ea8194a1 - us-east-1a

Creation time: August 27, 2018 at 4:58:54 PM UTC+5:30

Hosted zone: Z35SXDOTRQ7X7K

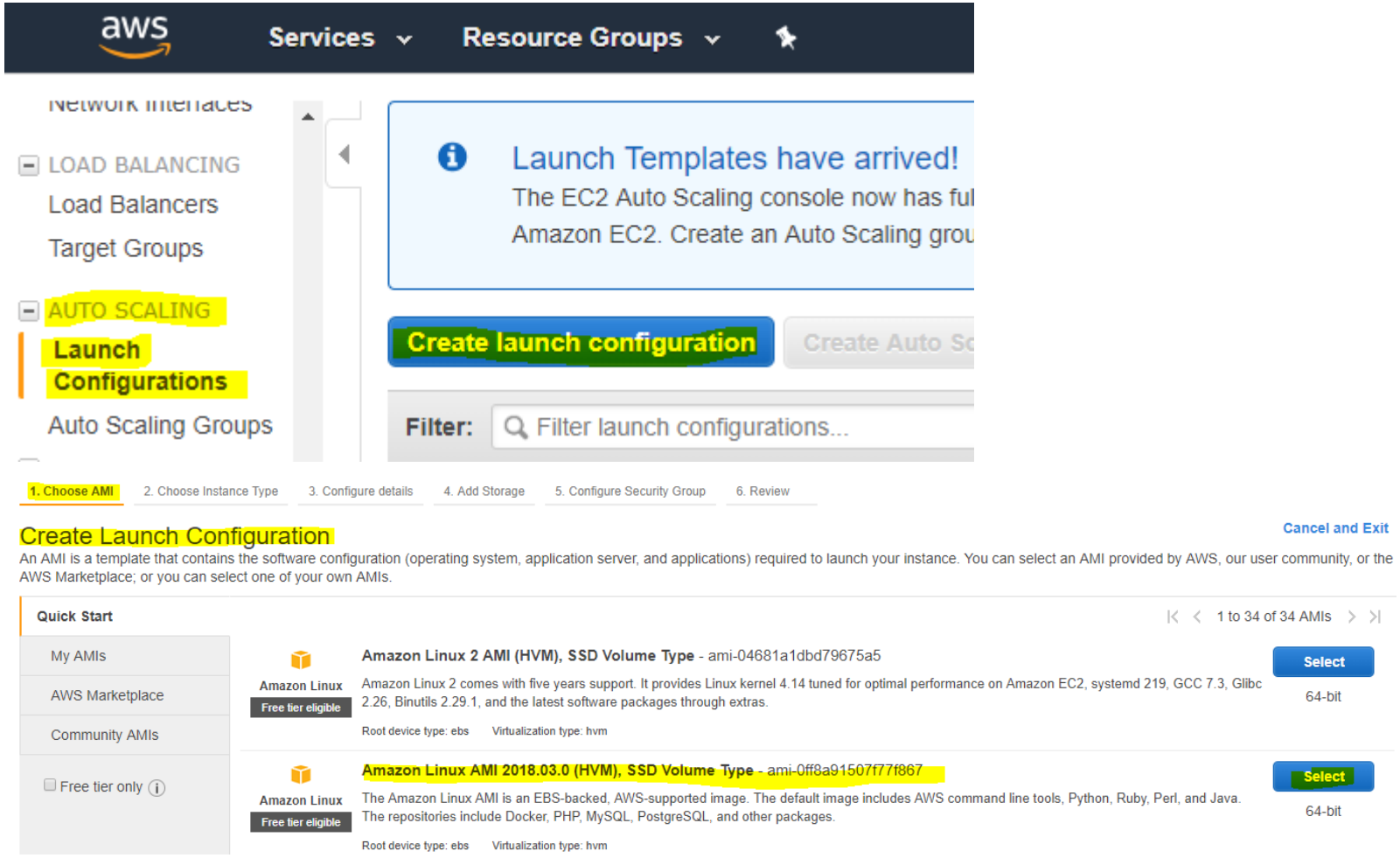
Status: 0 of 2 instances in service

VPC: vpc-8b5ba2f0

Cross check the ELB, EC2 instance configuration

- Go to Browser and verify the ELB DNS Name
- http://myclassicelb-1256450764.us-east-1.elb.amazonaws.com/

Auto Scaling Group & Launch Configuration



Select the Instance Type

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

Create Launch Configuration

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications
capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how th

Filter by: All instance types | Current generation | Show/Hide Columns

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

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)
☐	General purpose	t2.nano	1	0.5	EBS only
☑	General purpose	t2.micro Free tier eligible	1	1	EBS only

Configure the Bootstrap Script

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

Create Launch Configuration

Name test_AS_Config

Purchasing option Request Spot Instances

IAM role None

Monitoring Enable CloudWatch detailed monitoring
Learn more

Advanced Details

Kernel ID Use default

RAM Disk ID Use default

User data As text As file Input is already base64 encoded

```
#!/bin/bash
yum update -y
yum install http* --skip-broken -y
service httpd start
echo "Welcome to ELB&AS Group(Server-1)" > /var/www/html/index.html
```

IP Address Type Only assign a public IP address to instances launched in the default VPC and subnet. (default)
Assign a public IP address to every instance.
Do not assign a public IP address to any instances.
Note: this option only affects instances launched into an Amazon VPC

Add Storage & Create Security Group

1. Choose AMI | 2. Choose Instance Type | 3. Configure details | **4. Add Storage** | 5. Configure Security Group | 6. Review

Create Launch Configuration

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

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput
Root	/dev/xvda	snap-09ccbc8bc8ae7e4e9	8	General Purpose (SSD)	100 / 3000	N/A

1. Choose AMI | 2. Choose Instance Type | 3. Configure details | 4. Add Storage | **5. Configure Security Group** | 6. Review

Create Launch Configuration

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a 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 abou

Assign a security group: Create a **new** security group

Select an **existing** security group

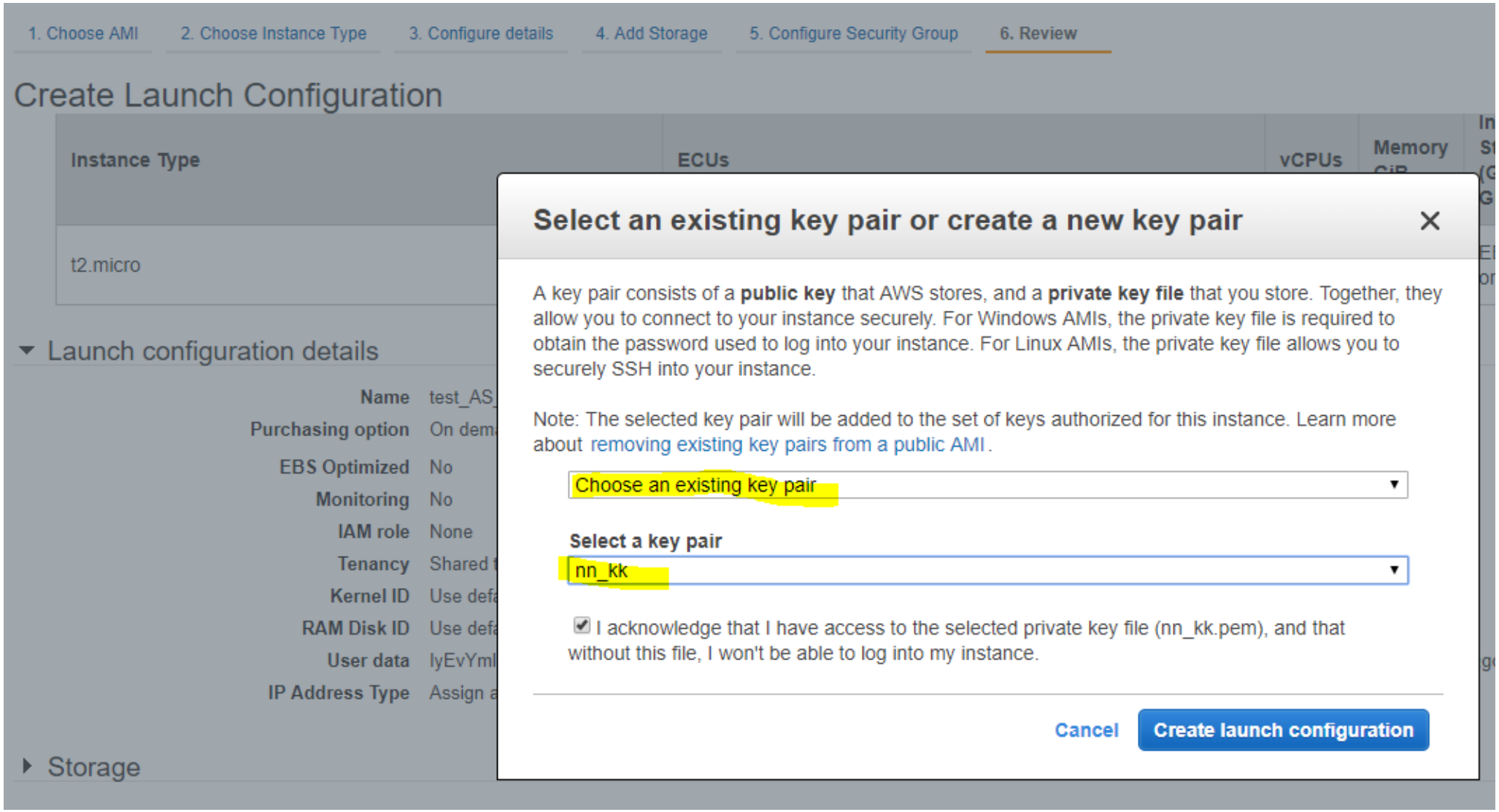
Security group name: sg_elb_as

Description: SSH-HTTP-HTTPS-ICMP

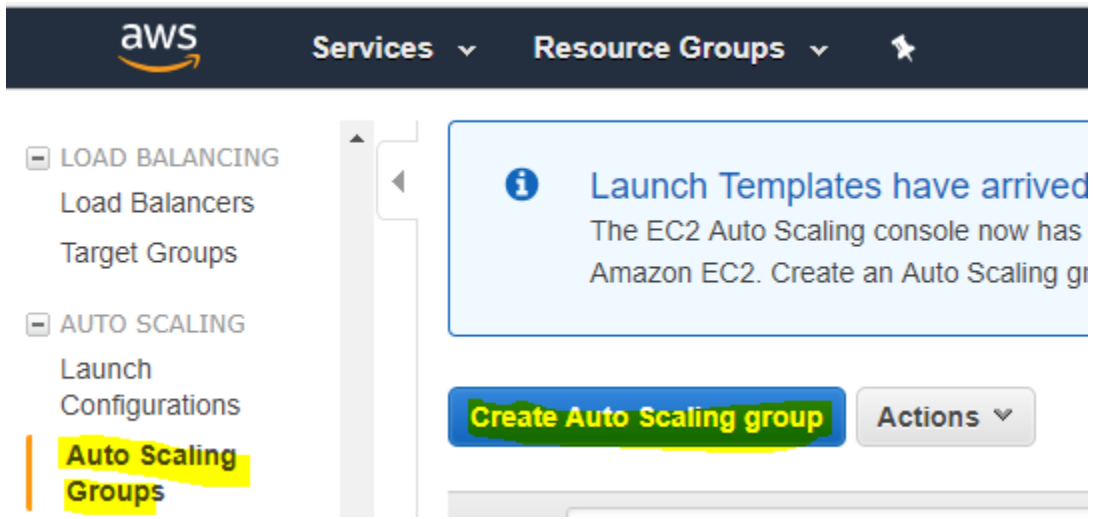
Type	Protocol	Port Range	Source	
SSH	TCP	22	Anywhere	0.0.0.0/0
HTTP	TCP	80	Anywhere	0.0.0.0/0
HTTPS	TCP	443	Anywhere	0.0.0.0/0
All ICMP	ICMP	0 - 65535	Anywhere	0.0.0.0/0

Add Rule

Select the Keypair and Click on Create



Now, Auto Scaling Group Creation Process



Create Auto Scaling Group

Cancel a

Complete this wizard to create your Auto Scaling group. First, choose either a launch configuration or a launch template to specify the parameters that your Auto Scaling group uses to launch instances.

Launch Configuration

You can continue to use your launch configurations if they support the Amazon EC2 features you need. Learn more

Launch Template New

Launch templates can be updated and versioned, and include support for the latest features of Amazon EC2.

Learn more

Create new launch template

Create a new launch configuration

Use an existing launch configuration

Filter launch configurations...

1 to 2 of 2 Launch Configu

Name	AMI ID	Instance Type	Spot Price	Security Groups
test_AS_Config	ami-0ff8a91507f77f867	t2.micro		sg-08c718e156d46ca85
wp_lc-20180820124151014000000004	ami-0e14421c1455b4c61	t2.micro		sg-08d2be38b2c0bf5a7

1. Configure Auto Scaling group details | 2. Configure scaling policies | 3. Configure Notifications | 4. Configure Tags | 5. Review

Create Auto Scaling Group

Launch Configuration test_AS_Config

Group name test-AS-Group

Group size Start with 2 instances

Network vpc-8b5ba2f0 (172.31.0.0/16) (default) Create new VPC

Subnet
- subnet-ea8194a1(172.31.16.0/20) | Default in us-east-1a
- subnet-7647072b(172.31.32.0/20) | Default in us-east-1b

Create new subnet

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

Advanced Details

Load Balancing ☑ Receive traffic from one or more load balancers Learn about Elastic Load Balancing

Classic Load Balancers myClassicELB ×

Target Groups

Health Check Type ○ ELB ◉ EC2

Health Check Grace Period 300 seconds

Monitoring Amazon EC2 Detailed Monitoring metrics, which are provided at 1 minute frequency, are not enabled for the launch configuration test_AS_Config. Instances launched from it will use Basic Monitoring metrics, provided at 5 minute frequency.
Learn more

Instance Protection

Service-Linked Role AWSServiceRoleForAutoScaling View Role in IAM

1. Configure Auto Scaling group details | **2. Configure scaling policies** | 3. Configure Notifications | 4. Configure Tags | 5. Review

Create Auto Scaling Group

You can optionally add scaling policies if you want to adjust the size (number of instances) of your group automatically. A scaling polic CloudWatch alarm that you assign to it. In each policy, you can choose to add or remove a specific number of instances or a percenta triggers, it will execute the policy and adjust the size of your group accordingly. Learn more about scaling policies.

- ○ **Keep this group at its initial size**
- ◉ **Use scaling policies to adjust the capacity of this group**

Scale between 2 and 5 instances. These will be the minimum and maximum size of your group.

Increase Group Size

Name: Increase Group Size

Execute policy when: No alarm selected ▾ Add new alarm

Take the action: Add ▾ 0 instances ▾

Add step

Instances need: 300 seconds to warm up after each step

Create a simple scaling policy

Decrease Group Size

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

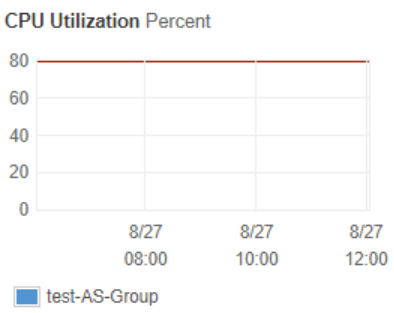
Send a notification to: No SNS topics found... create topic

Whenever: Average of CPU Utilization

Is: >= 80 Percent

For at least: 1 consecutive period(s) of 5 Minutes

Name of alarm: awsec2-test-AS-Group-High-CPU-Utilization



Cancel Create Alarm

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data rea

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: DevOpsEngineers cancel

With these recipients: keshav.kummari@gmail.com

Increase Group Size

Name: Increase Group Size

Execute policy when: awsec2-test-AS-Group-High-CPU-Utilization Edit Remove
breaches the alarm threshold: CPUUtilization >= 80 for 300 seconds
for the metric dimensions AutoScalingGroupName = test-AS-Group

Take the action: Add 0 instances when 80 <= CPUUtilization < +infinity

Add step

Instances need: 300 seconds to warm up after each step

Increase Group Size

Name: Increase Group Size

Execute policy when: awsec2-test-AS-Group-High-CPU-Utilization Edit Remove
breaches the alarm threshold: CPUUtilization >= 80 for 300 seconds
for the metric dimensions AutoScalingGroupName = test-AS-Group

Take the action: Add 1 instances when 80 <= CPUUtilization < +infinity

Add step

Instances need: 300 seconds to warm up after each step

Decrease Group Size

Name: Decrease Group Size

Execute policy when: No alarm selected ▾ Add new alarm

Take the action: Remove ▾ 0 instances ▾

Add step

Create a simple scaling policy

Scale the Auto Scaling group using a target tracking scaling policy

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: DevOpsEngineers (keshav.kummari@gm ▾ create topic

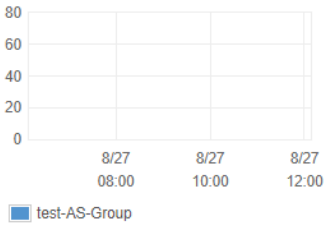
Whenever: Average ▾ of CPU Utilization ▾

Is: >= ▾ Percent

For at least: 1 consecutive period(s) of 5 Minutes ▾

Name of alarm: awsec2-test-AS-Group-High-CPU-Utilization

CPU Utilization Percent



Cancel Create Alarm

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

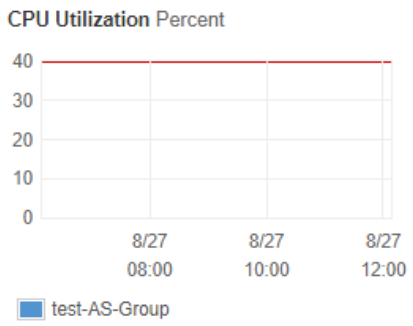
Send a notification to: DevOpsEngineers (keshav.kummari@gm ▾ create topic

Whenever: Average ▾ of CPU Utilization ▾

Is: <= ▾ 40 Percent

For at least: 1 consecutive period(s) of 5 Minutes ▾

Name of alarm: awsec2-test-AS-Group-High-CPU-Utilization



Cancel **Create Alarm**

Decrease Group Size

Name: Decrease Group Size

Execute policy when: awsec2-test-AS-Group-High-CPU-Utilization Edit Remove

breaches the alarm threshold: CPUUtilization <= 40 for 300 seconds

for the metric dimensions AutoScalingGroupName = test-AS-Group

Take the action: Remove ▾ 1 instances ▾ when 40 >= CPUUtilization > -infinity

Add step

Add Notification groups if any? Or else skip

1. Configure Auto Scaling group details | 2. Configure scaling policies | **3. Configure Notifications** | 4. Configure Tags | 5. Review

Create Auto Scaling Group

Configure your Auto Scaling group to send notifications to a specified endpoint, such as an email address, whenever a specified
termination, and failed instance termination.

If you created a new topic, check your email for a confirmation message and click the included link to confirm your subscription. N

Add notification

1. Configure Auto Scaling group details | 2. Configure scaling policies | 3. Configure Notifications | **4. Configure Tags** | 5. Review

Create Auto Scaling Group

A tag consists of a case sensitive key-value pair that you can use to identify your group. For example, you could define a tag with Key = Environment and Value = Producti
instances in the group when they launch. Learn more.

Key	Value	T
name	AutoScaling-ELB-Test	

Add tag 49 remaining

Verify the ELB & Auto Scaling

myClassicELB	myClassicELB-1256450764....	vpc-8b5ba2f0	us-east-1a, us-east-1b	classic

Load balancer: myClassicELB

Description | **Instances** | Health Check | Listeners | Monitoring | Tags | Migration

Connection Draining: Enabled, 300 seconds (Edit)

Edit Instances

Instance ID	Name	Availability Zone	Status	Actions
i-0838b9d95cb699459		us-east-1a	InService	Remove from Load Balancer
i-041188d49d2e1a22a		us-east-1b	InService	Remove from Load Balancer

Cross check the ELB, EC2 instance configuration

- Go to Browser and verify the ELB DNS Name
- http://myclassicelb-1256450764.us-east-1.elb.amazonaws.com/

- Go to Browser and verify the EC2_1 instance DNS Name/IP

http://ec2-54-85-38-140.compute-1.amazonaws.com

http://54.85.38.140

- Go to Browser and verify the EC2_2 instance DNS Name/IP
- http://ec2-54-198-154-106.compute-1.amazonaws.com
- http://54.198.154.106

Auto Scaling Group CLI Commands

- Auto scaling Plans:

https://docs.aws.amazon.com/cli/latest/reference/autoscaling-plans/index.html

1. create-scaling-plan
2. delete-scaling-plan
3. describe-scaling-plan-resources
4. describe-scaling-plans
5. update-scaling-plan

Application Auto Scaling

https://docs.aws.amazon.com/cli/latest/reference/application-autoscaling/index.html

1. delete-scaling-policy
2. delete-scheduled-action
3. deregister-scalable-target
4. describe-scalable-targets
5. describe-scaling-activities
6. describe-scaling-policies
7. describe-scheduled-actions
8. put-scaling-policy
9. put-scheduled-action
10. register-scalable-target

Auto Scaling

https://docs.aws.amazon.com/cli/latest/reference/autoscaling/index.html

1. attach-instances
2. attach-load-balancer-target-groups
3. attach-load-balancers
4. batch-delete-scheduled-action
5. batch-put-scheduled-update-group-action
6. complete-lifecycle-action
7. create-auto-scaling-group
8. create-launch-configuration
9. create-or-update-tags
10. delete-auto-scaling-group
11. delete-launch-configuration
12. delete-lifecycle-hook
13. delete-notification-configuration
14. delete-policy
15. delete-scheduled-action
16. delete-tags
17. describe-account-limits
18. describe-adjustment-types
19. describe-auto-scaling-groups
20. describe-auto-scaling-instances

11. delete-launch-configuration
12. delete-lifecycle-hook
13. delete-notification-configuration
14. delete-policy
15. delete-scheduled-action
16. delete-tags
17. describe-account-limits
18. describe-adjustment-types
19. describe-auto-scaling-groups
20. describe-auto-scaling-instances
21. describe-auto-scaling-notification-types
22. describe-launch-configurations
23. describe-lifecycle-hook-types
24. describe-lifecycle-hooks
25. describe-load-balancer-target-groups
25. describe-load-balancer-target-groups
26. describe-load-balancers
27. describe-metric-collection-types
28. describe-notification-configurations
29. describe-policies
30. describe-scaling-activities
31. describe-scaling-process-types
32. describe-scheduled-actions
33. describe-tags
34. describe-termination-policy-types
35. detach-instances
36. detach-load-balancer-target-groups
37. detach-load-balancers
38. disable-metrics-collection
39. enable-metrics-collection
40. enter-standby

41. execute-policy
42. exit-standby
43. put-lifecycle-hook
44. put-notification-configuration
45. put-scaling-policy
46. put-scheduled-update-group-action
47. record-lifecycle-action-heartbeat
48. resume-processes
49. set-desired-capacity
50. set-instance-health
51. set-instance-protection
52. suspend-processes
53. terminate-instance-in-auto-scaling-group
54. update-auto-scaling-group

Thank you!