

- Create Application Load balancer
  - Start a simple server in private EC2 8880
  - Target ALB to serve that server
  - ALB should be accessible through port 80 listener
  - Health Check
    - Register healthy on 3 success
    - Register unhealthy on 5 success
    - Timeout 5 Seconds
    - Interval 45 Seconds
  - Access the server via ALB publicly using ALB's DNS name.

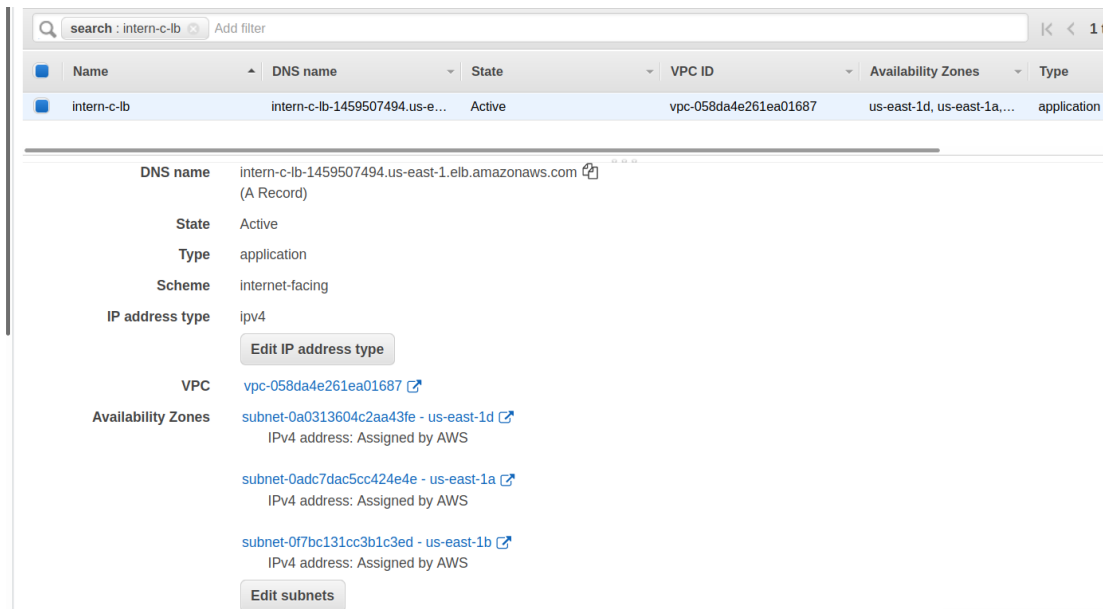
Application Load balancer was created by Selecting Load Balancer option on left side and Selecting 'Create Load Balancer' button.

Name of load balancer and listener is provided as http port 80 and subnets are assigned:

Then Target group is created with name intern-c-tgt with health check options:

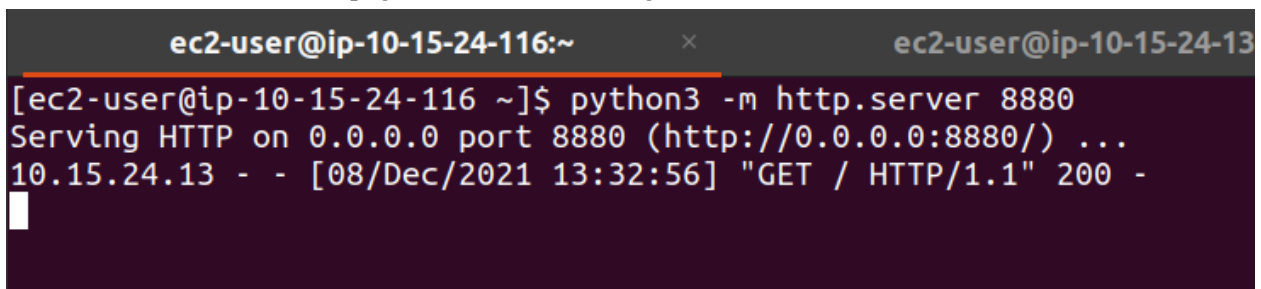
The screenshot shows the AWS Management Console interface for configuring a health check. The top navigation bar includes the AWS logo, 'Services' link, a search bar, and a language dropdown set to 'English (US)'. The main content area is titled 'The port the load balancer uses when performing health 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.' Below this, there are two radio buttons: 'Traffic port' (unselected) and 'Override' (selected). The 'Override' option has a text input field containing '8880' and a range indicator '1-65535'. The 'Healthy threshold' section is titled 'The number of consecutive health checks successes required before considering an unhealthy target healthy.' and has a spinner input set to '3' with a range of '2-10'. The 'Unhealthy threshold' section is titled 'The number of consecutive health check failures required before considering a target unhealthy.' and has a spinner input set to '5' with a range of '2-10'. The 'Timeout' section is titled 'The amount of time, in seconds, during which no response means a failed health check.' and has a spinner input set to '5' with a range of '2-120' and the unit 'seconds'. The 'Interval' section is titled 'The approximate amount of time between health checks of an individual target' and has a spinner input set to '45' with a range of '5-300' and the unit 'seconds'. The 'Success codes' section is titled 'The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").' and has a text input field containing '200-299'.

After this, we selected our instance and created the Load Balancer, which can be seen as:

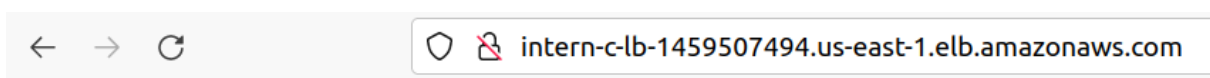


Then after selecting the target group, we have to register our target for a private subnet since our application is to be hosted on a private subnet.

Now, we serve an index.html page from inside the assigned subnet:



We then allow port 8880 from our security group and after this, when we enter the dns name in the browser, we can see our page being served.



the sever from private

- Create Route53 Hosted Zone
  - Either use your own Domain if you have as <team-name>.<your-domain> OR use mine ie intern.amitj.com.np to create new HZ for your use in pattern <team-name>.intern.amitj.com.np.
  - Show nslookup result for your domain.
  - Add R53 entry to map above created ALB at URL alb.<team-name>.<your-domain>

To create Route53 hosted zone, we can search Hosted Zones in search bar, which will take us to Route53 services page and we can select Hosted Zones and 'create hosted zone'

Route 53 > Hosted zones > Create hosted zone

### Create hosted zone [Info](#)

**Hosted zone configuration**  
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

**Domain name** [Info](#)  
This is the name of the domain that you want to route traffic for.  
  
 Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~

**Description - optional** [Info](#)  
This value lets you distinguish hosted zones that have the same name.  
  
 The description can have up to 256 characters. 21/256

**Type** [Info](#)  
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☒ **Public hosted zone**  
 A public hosted zone determines how traffic is routed on the internet.

☐ **Private hosted zone**  
 A private hosted zone determines how traffic is routed within an Amazon VPC.

And inside the hosted zone, we created a record by clicking Create Record button and routed the traffic to our private subnet by adding A Record:

Route 53 > Hosted zones > intern.amitj.com.np > Create record

### Quick create record [Info](#) [Switch to wizard](#)

▼ **Record 1** [Delete](#)

**Record name** [Info](#)  
 .intern.amitj.com.np  
 Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~

**Record type** [Info](#)

**Route traffic to** [Info](#)  
☒ **Alias**

**Routing policy** [Info](#)

**Evaluate target health**  
☒ **Yes**

[Add another record](#)

[Cancel](#) [Create records](#)

- Create ACM for above created R53 HZ with both top subdomain and its wild card ie <team-name>.<your-domain> and \*.<team-name>.<your-domain>
- Update ALB
  - Accept request only when **Host** = **alb.<team-name>.<your-domain>**, with default action response Code: 503, Message: “Unknown Request” on both HTTP and HTTPS requests.
  - Enable HTTPS support.
  - Redirect HTTP to HTTPS.

ALB was updated to accept the request only when host is alb.intern-c.intern.amitj.com.np

And rules were created for HTTP port 80 whenever accessed redirects the traffic via port 443 which is HTTPS.

The image displays two screenshots of the AWS Management Console, specifically the 'Rules' section for an Amazon Elastic Load Balancing (ALB) instance named 'intern-c-lb'.

**Top Screenshot: HTTP:80 Rules**

- Header:** intern-c-lb | HTTP:80
- Subheader:** intern-c-lb | HTTP:80 (2 rules)
- Rule Limits:** Rule limits for condition values, wildcards, and total rules.
- Rules Table:**

Order	ARN	IF	THEN
1	arn...7c0ed	Host is alb.intern-c.intern.amitj.com.np	Redirect to https://{host}:443/{path}?#{query} Status code: HTTP_302
last	HTTP 80: default action	Requests otherwise not routed	Return fixed response 503 (more...)

**Bottom Screenshot: HTTPS:443 Rules**

- Header:** intern-c-lb | HTTPS:443
- Subheader:** intern-c-lb | HTTPS:443 (2 rules)
- Rule Limits:** Rule limits for condition values, wildcards, and total rules.
- Rules Table:**

Order	ARN	IF	THEN
1	arn...9377c	Host is alb.intern-c.intern.amitj.com.np	Forward to intern-c-igt: 1 (100%) Group-level stickiness: Off
last	HTTPS 443: default action	Requests otherwise not routed	Return fixed response 503 (more...)

- (Optional) Create Private Route53 with domain **<team-name>.vpc-local** and attach it to your VPC with DNS resolve enabled.
  - Add A Record to map Private EC2's Private IP to **ec2.<team-name>.vpc-local**.
  - Run **telnet ec2.<team-name>.vpc-local 22**, from public EC2 and verify it gets connected.

Again, a hosted zone is created with type private:

**Domain name** [Info](#)  
This is the name of the domain that you want to route traffic for.

intern-c.vpc-local

Valid characters: a-z, 0-9, ! " # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~

**Description - optional** [Info](#)  
This value lets you distinguish hosted zones that have the same name.

intern c vpc local

The description can have up to 256 characters. 18/256

**Type** [Info](#)  
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☐ **Public hosted zone**  
A public hosted zone determines how traffic is routed on the internet.

☒ **Private hosted zone**  
A private hosted zone determines how traffic is routed within an Amazon VPC.

A record is created as:

Route 53 > Hosted zones > intern-c.vpc-local > Create record

**Quick create record** [Info](#) [Switch to wizard](#)

▼ Record 1 Delete

Record name [Info](#) Record type [Info](#) Value [Info](#) ☒ Alias

ec2 .intern-c.vpc-local A – Routes traffic to an IPv4 address and so... 10.15.24.116

Valid characters: a-z, 0-9, ! " # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~

Enter multiple values on separate lines.

TTL (seconds) [Info](#) Routing policy [Info](#)

300 Simple routing

1m 1h 1d

Recommended values: 60 to 172800 (two days)

Add another record

Cancel Create records

► View existing records

And running the Telnet command:

```
[ec2-user@ip-10-15-24-13 ~]$ telnet ec2.intern-c.vpc-local 22
Trying 10.15.24.116...
Connected to ec2.intern-c.vpc-local.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4
```