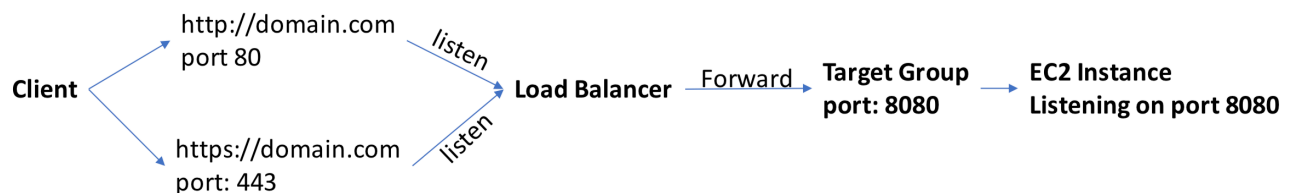


AWS DEPLOY WEB APP ON EC2 WITH SSL CERTIFICATE (HTTPS)

GENERAL IDEA AND MY PERSONAL UNDERSTANDING



PROCEDURE

1. Buy a domain name from **route 53**

Choose a domain name

.com - \$12.00

Availability for 'yourdomain.com'

Domain Name	Status	Price /1 Year	Action
yourdomain.com	✗ Unavailable		

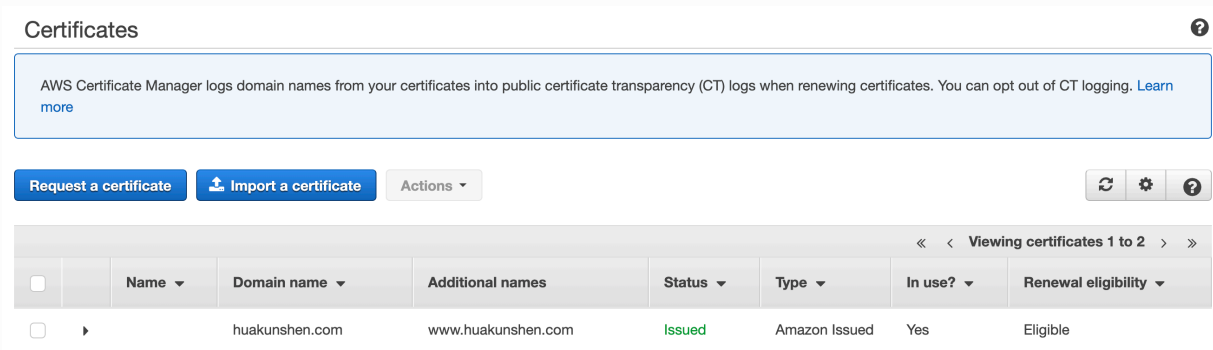
Related domain suggestions

Domain Name	Status	Price /1 Year	Action
fixyourdomain.com	✓ Available	\$12.00	<input type="button" value="Add to cart"/>
makeyourdomain.net	✓ Available	\$11.00	<input type="button" value="Add to cart"/>
sellyourdomain.net	✓ Available	\$11.00	<input type="button" value="Add to cart"/>
yourarticle.net	✓ Available	\$11.00	<input type="button" value="Add to cart"/>

Find and select an available one.

2. Request a SSL certificate from ACM (Certificate Manager)

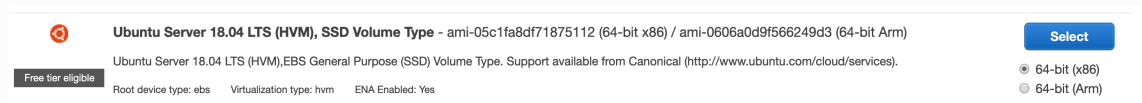
such as **domain.com** or **www.domain.com**



3. Server

- Go to EC2. Launch a new instance (server), select ubuntu for example.

◦



- When configuring **Security Group**, add **SSH**, **HTTP**, **HTTPS**, and **Custom TCP Rule**(Optional).
 - For the **Custom TCP Rule**, set Port Range to 8080 (or whatever your app will be listening on such as 3000)
 - Set **source** to **anywhere**, so that everyone from any ip address can access the port.
 - Download and keep the private key in a safe location, it will be used to connect to server remotely using ssh. It cannot be downloaded again, so keep it in a place you'll remember.
 - Remember to set a name for your security group. In the future you could find it easily.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group

☐ Select an existing security group

Security group name:

your security group name

Description:

launch-wizard-1 created 2019-09-23T02:57:59.616-04:00

Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>
SSH <small>⌵</small>	TCP	22	Anywhere <small>⌵</small> 0.0.0.0/0, ::/0
HTTP <small>⌵</small>	TCP	80	Anywhere <small>⌵</small> 0.0.0.0/0, ::/0
HTTPS <small>⌵</small>	TCP	443	Anywhere <small>⌵</small> 0.0.0.0/0, ::/0
Custom TCP <small>⌵</small>	TCP	8080	Anywhere <small>⌵</small> 0.0.0.0/0, ::/0

Add Rule

4. Load Balancer

Step 1: Configure Load Balancer

- o In EC2, go to **Load Balancer**-> Create Load Balancer -> Select Application Load Balancer (HTTP&HTTPS)
- o Give the load balancer a name
- o In Listeners, add a HTTPS listener with port=443

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name i

load-balancer-name

Scheme i

- ☒ internet-facing
☐ internal

IP address type i

ipv4 ⌵

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port	
HTTP <small>⌵</small>	80	<small>✕</small>
HTTPS (Secure HTTP) <small>⌵</small>	443	<small>✕</small>

Add listener

- o Select at least two availability zones.

Step 2: Configure Security Settings

- Choose the certificate that you just requested from Certificate manager, make sure the certificate has been issued (check Route 53, it takes some time)

Step 2: Configure Security Settings

Select default certificate

AWS Certificate Manager (ACM) is the preferred tool to provision and store server certificates. If you previously stored a server certificate using IAM, you can deploy it to your load balancer. [Learn more](#) about HTTPS listeners and certificate management.

Certificate type ⓘ

- ☒ Choose a certificate from ACM (recommended)
- ☐ Upload a certificate to ACM (recommended)
- ☐ Choose a certificate from IAM
- ☐ Upload a certificate to IAM

[Request a new certificate from ACM](#)

AWS Certificate Manager makes it easy to provision, manage, deploy, and renew SSL Certificates on the AWS platform. ACM manages certificate renewals for you. [Learn more](#)

Certificate name ⓘ

huakunshen.com (arn:aws:acm:us-east-2:814759424895:certificate/c27: ↕ 🔄)

Select Security Policy

Security policy ⓘ

ELBSecurityPolicy-2016-08 ↕

[Cancel](#)

[Previous](#)

[Next: Configure Security Groups](#)

Step 3: Configure Security Groups

- Select an existing security group:

select the one you just created while launching EC2 instance (find it by the name you set)

Step 4: Configure Routing

- Create a new target group, keep everything as default but the port
- Change the port to the port your app will be listening on, 8080 in my case

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.

Target group

Target group ⓘ

New target group

Name ⓘ

target-group-name

Target type

- ☒ Instance
- ☐ IP
- ☐ Lambda function

Protocol ⓘ

HTTP

Port ⓘ

8080

Health checks

Protocol ⓘ

HTTP

Path ⓘ

/

▶ Advanced health check settings

[Cancel](#)

[Previous](#)

[Next: Register Targets](#)

Step 5: Register Target

- Select the target group you just created, click **Add to registered**.

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove

<input type="checkbox"/>	Instance	Name	Port	State	Security groups	Zone
<input type="checkbox"/>	i-06e5f6e8ca...	MyWebsit...	8080	● running	MyWebsiteSecurityGroup	us-east-2c

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered

 on port

X

<input type="checkbox"/>	Instance	Name	State	Security	Zone	Subnet ID	Subnet CIDR
<input checked="" type="checkbox"/>	i-06e5f6...	MyWeb...	● run...	MyWeb...	us-east...	subnet-9f19c3d3	172.31.32.0/20

Cancel

Previous

Next: Review

Finally, review and create load balancer.

5. Go to **Route 53**, click on **Hosted zones**, find the domain you purchased, click on it.
 - o Click **Create Record Set**
 - o Name = nothing if you are not working on a subdomain, subdomain name otherwise
 - o Type = A
 - o Alias = Yes
 - o Alias Target = the load balancer you just created

Create Record Set

Name: huakunshen.com.

Type: A – IPv4 address

Alias: ☒ Yes ☐ No

Alias Target: dualstack.MyWebsiteLoadBalance-19{

Alias Hosted Zone ID: Z3AADJGX6KTTL2

You can also type the domain name for the resource. Examples:

- CloudFront distribution domain name: d111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-2.elb.amazonaws.com
- S3 website endpoint: s3-website.us-east-2.amazonaws.com
- Resource record set in this hosted zone: www.example.com
- VPC endpoint: example.us-east-2.vpce.amazonaws.com
- API Gateway custom regional API: d-abcde12345.execute-api.us-west-2.amazonaws.com

[Learn More](#)

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. [Learn More](#)

Evaluate Target Health: ☐ Yes ☒ No

- Optionally, create a **www.** Record Set that also goes to the same load balancer

Edit Record Set

Name: .huakunshen.com.

Type: A – IPv4 address

Alias: ☒ Yes ☐ No

Alias Target:

Alias Hosted Zone ID: Z3AADJGX6KTTL2

You can also type the domain name for the resource. Examples:

- CloudFront distribution domain name: d111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-2.elb.amazonaws.com
- S3 website endpoint: s3-website.us-east-2.amazonaws.com
- Resource record set in this hosted zone: www.example.com
- VPC endpoint: example.us-east-2.vpce.amazonaws.com
- API Gateway custom regional API: d-abcde12345.execute-api.us-west-2.amazonaws.com

[Learn More](#)

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. [Learn More](#)

Evaluate Target Health: ☐ Yes ☒ No

- o Of course you can use any subdomain name.
6. ssh to connect to your server with the private key you downloaded while launching EC2 instance.

Start an app whose server listens on port 8080 (or your application's port number).

7. Go to browser, go to <http://huakunshen.com> or <https://huakunshen.com> for example.

With https, you will see that the browser no longer identifies you as not secure, and has a little lock on the address bar.