



Troy Ingram

Jun 1, 2022 · 4 min read · Member-only



Adding an SSL Certificate to an Application Load Balancer in AWS

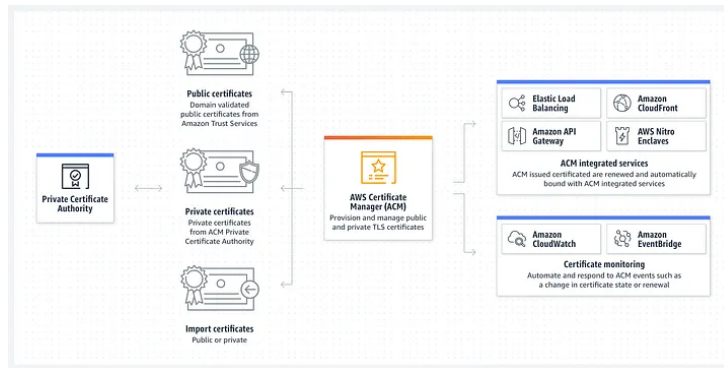


Image from <https://aws.amazon.com/certificate-manager/>

AWS Certificate Manager

AWS Certificate Manager (ACM) is a service that allows you to create, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services. ACM simplifies the certificate process by removing the manual process of purchasing, uploading, and renewing SSL/TLS certificates. Once created, the SSL/TLS certificate can be deployed on ACM-integrated AWS resources. Certificates provisioned through ACM for use with ACM-integrated services are free and certificates will auto-renew.

Why Use SSL/TLS Certificates

A SSL/TLS certificate is a digital certificate that authenticates your site identity and secures connections between browsers, applications and your site. SSL/TLS certificates are used to secure network traffic and establish the identity of websites over the Internet and private networks by creating an encrypted link between a web server and a web browser.

Prerequisites

1. AWS Account
2. Existing Application Load Balancer
3. EC2 instances in a Target Group

My Current Environment

I used Terraform to create a custom VPC, Subnets, One EC2 in each Subnet with an internet facing Application Load Balancer in us-east-1. If you want to use this code to spin up a quick environment to test this out you can here: <https://github.com/troy-ingram/terraform-alb>

Please note that as mentioned in the Prerequisites you will need to have a purchased Domain through Route53. For this project to make things easy I just used A Cloud Guru's AWS Sandbox environment that has their own DNS Records.



Troy Ingram

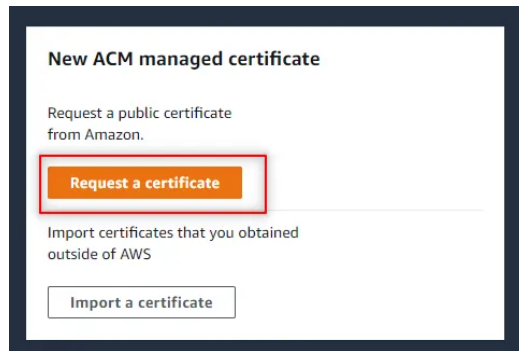
831 Followers

Cloud DevOps Engineer | 5x AWS Certified |
Terraform Associate | Python | Linux | DevOps

Follow

Certificate

1. Navigate to Certificate Manager.
2. Click Request a certificate.



3. Select Request a public certificate. Click Next.

4. On the Request public certificate page you will need to enter a Fully qualified domain name. To protect several sites in the same domain I will be using an asterisk (*) to request a wildcard certificate. Then select DNS validation. Click Request.

Request public certificate

Domain names [Info](#)

Fully qualified domain name [Info](#)

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Select validation method [Info](#)

Select a method for validating domain ownership

☒ **DNS validation - recommended**
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

☐ **Email validation**
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

Tags [Info](#)

To help you manage your certificates you can optionally assign your own metadata to each resource in the form of tags.

Tag key

Tag value - optional

[Remove tag](#)

[Add tag](#)

You can add 49 more tags.

[Cancel](#) [Previous](#) [Request](#)

DNS Validation

The status for the certificate request states the Status is *Pending validation*. We will need to create a CNAME record to validate.

AWS Certificate Manager > Certificates

Certificates (1)

[Delete](#) [Manage expiry events](#) [Import](#) [Request](#)

<input type="checkbox"/>	Certificate ID	Domain name	Type	Status	In use?	Renewal eligibility
<input type="checkbox"/>	8f137d56-c5d5-43bd-af17-1d5302a68953	*.cmcloudlab1606.info	Amazon issued	Pending validation	No	Ineligible

1. Click on the Certificate ID.

<input type="checkbox"/>	Certificate ID	Domain name
<input type="checkbox"/>	8f137d6a-c6d6-42bd-af17-1d57f2de8953	*.cmcloudlab1606.info

2. Under the Domain section click Create records in Route 53 button. We could mainly create the CNAME record using the CNAME name and CNAME value, but AWS has made the process easier for users.

3. Click Create records.

4. Now wait for DNS to validate the new CNAME record. This process could take several minutes. Refresh until the Status shows as *Issued*.

Update Security Group

1. Navigate to EC2 > Security Groups.
2. Make sure to modify the ALB Security Group to allow HTTPS inbound traffic from 0.0.0.0/0 or desired CIDR.

Assign the Certificate to the ALB

1. Navigate to EC2 > Load Balancers.
2. Select **Listeners** tab and click **Add listener** button

3. Input the following on the Add listener page:

- Protocol HTTPS
- Port 443
- Default actions: Forward to desired Target Group
- Default SSL/TLS certificate: Select your certificate from the drop down

Then click Add.

4. Modify the existing HTTP listener by removing the current Forward to and adding a new HTTP:80 Redirect action:

- Select Itemized URL
- HTTPS:443

Create DNS Record for ALB

1. Copy the DNS name of the ALB.
2. Navigate to Route53 > Hosted zones.
3. Click the Domain name to view the current records.
4. Create a new A record using the following inputs from the screenshot then click Create records. I prepended the site with “cert”, but you can name yours whatever you want. Click Save.

Testing

1. Copy and paste the record name into a browser using https.
2. Now attempt the same but use HTTP instead of HTTPS
3. The same page should still appear and this time it redirects the HTTP request to HTTPS.
4. If you click on the lock symbol in the browser you can see the certificate details.

More content at [PlainEnglish.io](https://plainenglish.io). Sign up for our [free weekly newsletter](#). Follow us on [Twitter](#) and [LinkedIn](#). Check out our [Community Discord](#) and join our [Talent Collective](#).

[AWS](#) [Aws Certificate Manager](#) [Application Load Balancer](#) [Cloud Computing](#)
[Cloud](#)

 --  3

More from AWS in Plain English

New AWS, Cloud, and DevOps content every day. Follow to join our 3.5M+ monthly readers.

Follow

Read more from AWS in Plain English

