

EC2 Dashboard

Events

Tags

Reports

Limits

INSTANCES

Instances

Launch Templates

Spot Requests

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

Lifecycle Manager

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

LOAD BALANCING

Load Balancers

Target Groups

AUTO SCALING

Launch Configurations

Create Load Balancer

Actions

Filter by tags and attributes or search by keyword

1 to 1 of 1

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
acm-pca-usecase-6-alb	acm-pca-usecase-6-alb-112...	active	vpc-	us-east-1b, us-east-1a	application	August 2, 2019 at 10:27:19 ...

Step 1 :

- You should see the load balancer that is created in your account under EC2 -> Load Balancers
- Copy the DNS name of the load balancer and copy it into your notes application. We will need this information later

Load balancer: acm-pca-usecase-6-alb

Description

Listeners

Monitoring

Integrated services

Tags

Basic Configuration

Name	acm-pca-usecase-6-alb
ARN	arn:aws:elasticloadbalancing:us-east-1:...
DNS name	acm-pca-usecase-6-alb-... (A Record)
State	active
Type	application

Certificates

Certificate Manager

Private certificate authority

Private CAs

Step 2 :

- **Let's issue a private certificate**
- **Click Get Started**



AWS Certificate Manager

AWS Certificate Manager (ACM) makes it easy to provision, manage, deploy, and renew SSL/TLS certificates on the AWS platform.

[Get started](#)[User guide](#)

Provision certificates

Provide the name of your site, establish your identity, and let ACM do the rest. ACM manages renewal of SSL/TLS certificates issued by Amazon for you.

[Learn more.](#)

Deploy SSL/TLS-based sites and applications

Create an Elastic Load Balancer or Amazon CloudFront distribution and use ACM-provided or imported certificates with SSL/TLS to securely identify your site.

[Learn more.](#)

Manage certificates

See all of your ACM-provided and imported certificates in one place in the AWS Management Console. Automate management tasks by using the ACM API, SDK, or CLI.

[Learn more.](#)

Choose **Import a certificate** to import an existing certificate instead of requesting a new one. [Learn more.](#)

 **Import a certificate**

Request a certificate

Choose the type of certificate you want, and then choose **Request a certificate**

- ☐ **Request a public certificate** - Request a public certificate from Amazon. By default, public certificates are trusted by browsers and operating systems. [Learn more.](#)
- ☒ **Request a private certificate** - Request a private certificate from your organization's certificate authority. [Learn more.](#)

Step 3 : Request a private certificate

Cancel

Request a certificate



Request a private certificate

Step 1: Select CA

Step 2: Add domain names

Step 3: Review

Select certificate authority (CA) ?

You can create your certificate by specifying a CA.

CA

acmsubordinateca g1 : 

Type	Subordinate
Organization (O)	mycompany
Organization unit (OU)	payroll
Country name (C)	US
State or province	washington
Locality name	seattle
Common name (CN)	acmsubordinateca g1

Cancel

Previous

Next



Step 4 :

- **Select the subordinate CA with common name acmsubordinateca g1**
- **The issued private certificate will be signed by this subordinate issuing CA**

Request a private certificate

Step 1: Select CA

Step 2: Add domain names

Step 3: Review

You can use AWS Certificate Manager certificates with other [AWS Services](#).

Add domain names ?

Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, `www.example.com`). Use an asterisk (*) to request a wildcard certificate to protect several sites in the same domain. For example: `*.example.com` protects `www.example.com`, `site.example.com` and `images.example.com`.

Domain name*

Remove

acm-pca-usecase-6-alb- [redacted] us-east

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. [Learn more](#).

*At least one domain name is required

Cancel

Review and request

Step 5 :

- **Fill in the domain name for the certificate with the DNS name of the ALB that you copied in Step 1**



Services ▾

Resource Groups ▾



N. Virginia ▾

Support ▾

Request a private certificate

[Step 1: Select CA](#)

[Step 2: Add domain names](#)

Step 3: Add Tags

[Step 4: Review](#)

Add Tags

To help you manage your certificates you can optionally assign your own metadata to each resource in the form of tags. [Learn more.](#)

Tag Name

Value

Add Tag

[Cancel](#)

Previous

Review and request

Step 6 :

- **Don't put any tags here as we won't be using tags on private certificates**
- **FYI ACM Private Certificates now supports tag on create.**

Request a private certificate

[Step 1: Select CA](#)[Step 2: Add domain names](#)**Step 3: Review and request**

Review and request ?

Review your choices. [Learn more.](#)

Certificate Authority

[Edit](#)

CA acmsubordinateca g1 : [REDACTED]

Domain names

[Edit](#)

Domain name acm-pca-usecase-6-alb-[REDACTED]-us-east-1.elb.amazonaws.com

[Cancel](#)[Previous](#)[Confirm and request](#)

Step 7 : Verify that the domain name is accurate and click Confirm and request

Certificates

Certificate Manager

Private certificate authority

Private CAs

Certificates



AWS Certificate Manager logs domain names from your certificates into public certificate transparency (CT) logs when renewing certificates. You can opt out of CT logging. [Learn more](#)



Success

Your certificate was requested successfully.

[Request a certificate](#)[Import a certificate](#)

Actions ▾



« < Viewing certificates 1 to 1 > »

<input type="checkbox"/>	Name ▾	Domain name ▾	Additional names	Status ▾	Type ▾	In use? ▾	Renewal eligibility ▾
<input type="checkbox"/>		acm-pca-usecase-6-alb-  s-east-1.elb.amazonaws.com		Issued	Private	No	Ineligible

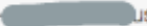
Status

Certificate created successfully**Status** Issued**Detailed status** The certificate was issued at 2019-08-03T23:06:01UTC

Details

Type Private

In use? No

Domain name acm-pca-usecase-6-alb-us-east-1.elb.amazonaws.com

Number of additional names 0

Identifier [187e0aaf-339e-43ea-ac4a-df2e8e141a36](#)

Serial number d7:c1:14:2f:6e:d9:1f:e3:4e:9d:3d:e6:63:56:63:4b

Requested at 2019-08-03T23:05:58UTC

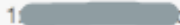
Issued at 2019-08-03T23:06:01UTC

Not before 2019-08-03T22:05:59UTC

Not after 2020-09-03T23:05:59UTC

Public key info RSA 2048-bit

Signature algorithm SHA256WITHRSA

ARN arn:aws:acm:us-east-1:certificate/187e0aaf-339e-43ea-ac4a-df2e8e141a36

CA [arn:aws:acm-pca:us-east-1:!\[\]\(93a800b136548d380c0cb54631afba93_img.jpg\)](#)

Quiz : (please open the quiz in a new browser tab)

***In the previous step you saw that private certificate was created successfully.
Please click on the link below to take the quiz***

<https://bit.ly/2KXE06k>