

## ◆ Certificate Manager

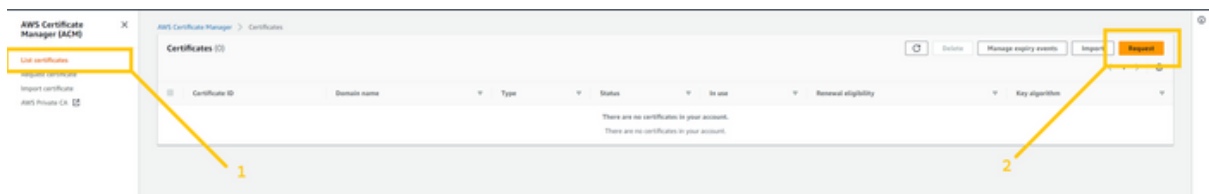
As you saw in previous screenshots, I have the domain name `abhis.cloud` in Route 53. Now I am going to use this domain name to create subdomains such as `api.abhis.cloud` and that will resolve **ALB-backend DNS**. Furthermore, we need an SSL certificate so that we can make the connection secure.

*Note: we are going to create certificates in both regions us-east-1 and us-west-2.*

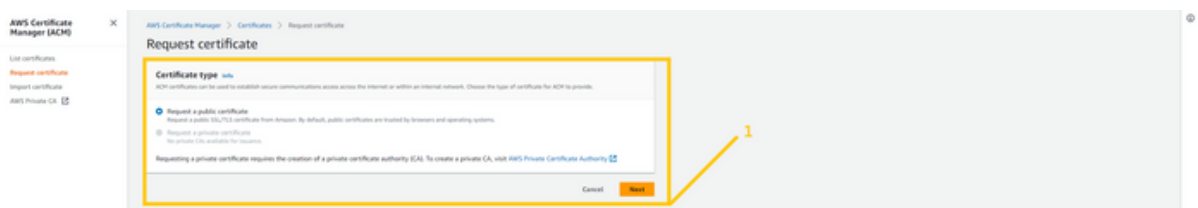
So let's head over to ACM (AWS certificate manager). Type certificate manager in the AWS console search bar. And click on the service.



Now click on the `list certificates` button on the left panel and then click on the `request certificate` on the top right corner.



Select the option Request the public certificate and click on the `next` button.



In the domain name field please type **\*.Your\_Domain\_Name.xyz** in my case it is **\*.abhis.cloud** DON'T DO ANY TYPO. In the validation method select DNS validation and click on the request certificate.

**Request public certificate**

**Domain names** Provide one or more domain names for your certificate.

Fully qualified domain name info

\*.abhis.cloud

Add another name to this certificate

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

**Validation method** info

Select a method for validating domain ownership.

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

☐ Email validation info  
Choose this option if you do not have permission to control domain-ownership or modify the DNS configuration for the domains in your certificate request.

**Key algorithm** info

Select an encryption algorithm. Some algorithms may not be supported by all AWS services.

☒ **RSA 2048** info  
RSA is the most widely used algorithm.

☐ ECDSA P-256 info  
Recommended for cryptographic strength to RSA 2048.

☐ ECDSA P-384 info  
Recommended for cryptographic strength to RSA 3072.

**Tags** info

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

Use tags associated with this resource.

Add tag

You can add 50 more tags.

Cancel Previous **Request**

Here you can see the status pending validation. Now we need to add a **CNAME record** in our domain. If you are not using route 53 then you need to add this CNAME record manually by going to your **DOMAIN REREGISTER**. And if you are using route 53 then click on the button create record in route 53 and click on the create record button. That's it.

**Security requested certificate with ID a1ddea4-1c89-4c47-8f0a-95cc5374a3cf**

**Certificate status**

Identifier a1ddea4-1c89-4c47-8f0a-95cc5374a3cf

Info arn:aws:acm:us-east-1:13029378792:certificate/a1ddea4-1c89-4c47-8f0a-95cc5374a3cf

Type Amazon issued

Status **Pending validation** info

**Domains (1)**

Domain	Status	Reason status	Type	CNAME name	CNAME value
*.abhis.cloud	Pending validation	-	CNAME	_csm5711336746027407230ad33049c7c.abhis.cloud	_csm5711336746027407230ad33049c7c408406a73758d-gpvmgpmg.acm-validation.com

**Details**

Info	Serial number	Requested on	Renewal eligibility
Key	NR	June 11, 2023, 02:46:33 GMT+05:30	Indefinite
Domain name	Public key info	Issued at	
*.abhis.cloud	RSA 2048	NR	
Number of additional names	Signature algorithm	Next before	
0	SHA-256 with RSA	NR	
	Can be used with:	Next after	
	CloudFront, Elastic Load Balancing, API Gateway and other integrated services.	NR	

**Tags (0)**

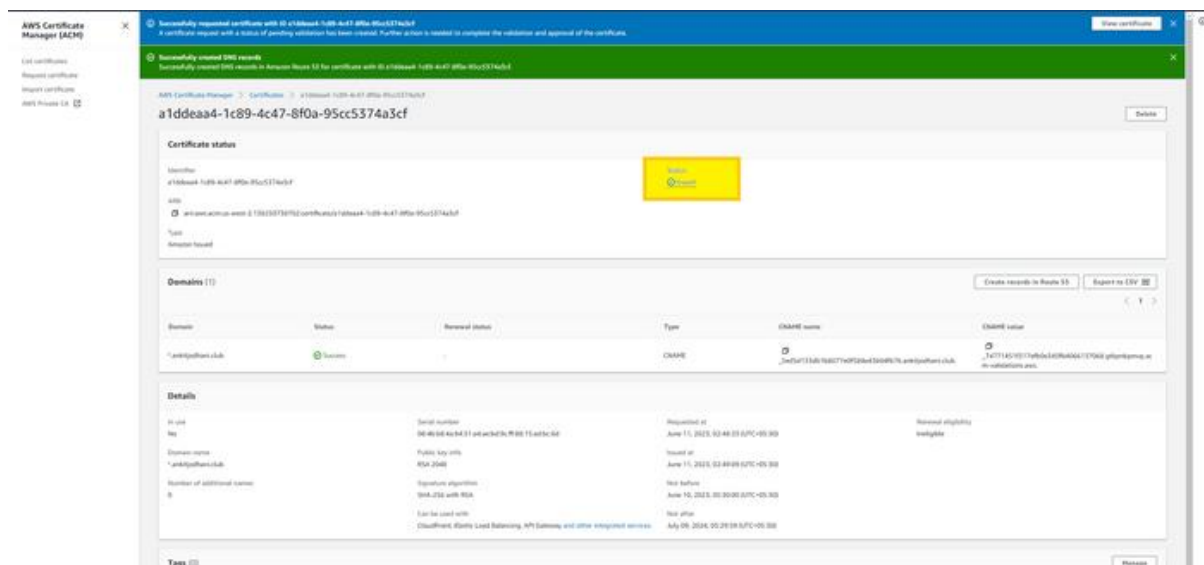
Key

Value

No tags

The tags associated with this resource.

And in just a few minutes you will see the status **issued**.



*Note: I created a certificate in N.virginia(us-east-1) but you need to do the same thing for the Oregon region( us-west-2 ).*