Creating an ACM certificate in your Substrate account

Downloaded from Epic Games Confluence
Date: 2025-07-12 04:08:11
Original URL: https://confluence-epicgames.atlassian.net/wiki/spaces/CDE/pages/81068340

Document Level Classification

100

Introduction

If the service you're deploying to Substrate has an HTTP endpoint, you probably need a certificate in order to support TLS/SSL on the ALB. The instructions here will help get you started.

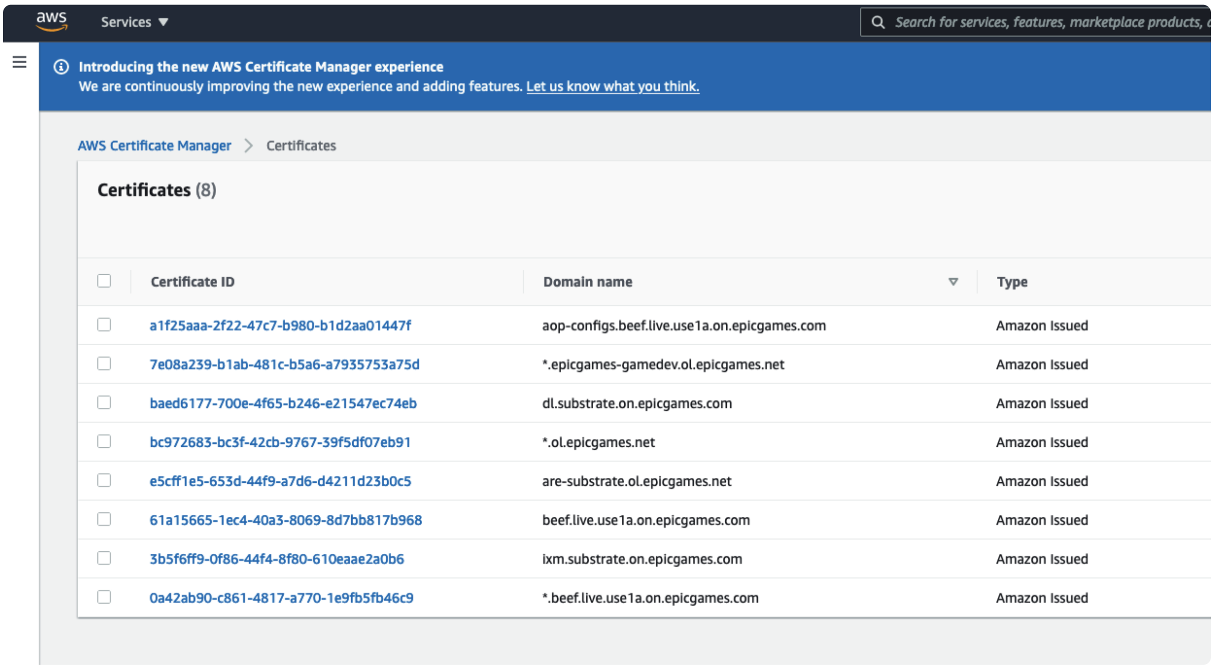
Each account in Substrate needs its own set of certificates. Certificates cannot be shared across AWS accounts.

Check if a certificate already exists for your account

Login to the console using the Okta tile or `aop login`

Once you're logged into your Substrate account, open the ACM console.

Look through the list of certificates to see if a certificate that you can use already exists.



Introducing the new AWS Certificate Manager experience
We are continuously improving the new experience and adding features. Let us know what you think.

AWS Certificate Manager > Certificates

Certificates (8)

□	Certificate ID	Domain name	Type
□	a1f25aaa-2f22-47c7-b980-b1d2aa01447f	aop-configs.beef.live.use1a.on.epicgames.com	Amazon Issued
□	7e08a239-b1ab-481c-b5a6-a7935753a75d	*.epicgames-gamedev.ol.epicgames.net	Amazon Issued
□	baed6177-700e-4f65-b246-e21547ec74eb	dl.substrate.on.epicgames.com	Amazon Issued
□	bc972683-bc3f-42cb-9767-39f5df07eb91	*.ol.epicgames.net	Amazon Issued
□	e5cff1e5-653d-44f9-a7d6-d4211d23b0c5	are-substrate.ol.epicgames.net	Amazon Issued
□	61a15665-1ec4-40a3-8069-8d7bb817b968	beef.live.use1a.on.epicgames.com	Amazon Issued
□	3b5f6ff9-0f86-44f4-8f80-610eaae2a0b6	ixm.substrate.on.epicgames.com	Amazon Issued
□	0a42ab90-c861-4817-a770-1e9fb5fb46c9	*.beef.live.use1a.on.epicgames.com	Amazon Issued

For example, in my beef-live account, I want to deploy my service with the hostname foo.beef.live.use1a.on.epicgames.com.

There's already a certificate at the bottom of the list that will work because it's a wildcard certificate for *.beef.live.use1a.on.epicgames.com.

I will select the certificate ID and copy the ARN into my ingress configuration annotations in EKS.

If a usable certificate doesn't exist, read on for how to create one.

Creating a New Certificate with Terraform (Preferred)

ACM certificates should work automatically with any public DNS records (`on.epicgames.com.` and subdomains). You can create and manage these records using Terraform. For a complete working example, refer to the custom DNS record we use with Substrate Vault. A snippet is included below:

```
resource "aws_acm_certificate" "substrate-vault" {
  domain_name       = local.vault_dns_name
  validation_method = "DNS"
}

resource "aws_route53_record" "substrate-cert-validation" {
  for_each = {
    for dvo in aws_acm_certificate.substrate-vault.domain_validation_op
      name = dvo.resource_record_name
      record = dvo.resource_record_value
      type = dvo.resource_record_type
    }
  }

  name = each.value.name
  records = [each.value.record]
  type = each.value.type
  ttl        = 60
  zone_id    = aws_route53_zone.vault.zone_id
  depends_on = [aws_acm_certificate.substrate-vault]
}

resource "aws_acm_certificate_validation" "substrate-vault" {
  certificate_arn         = aws_acm_certificate.substrate-vault.arn
  validation_record_fqdns = [for record in aws_route53_record.substrate
}
```

Refer to the `aws_acm_certificate_validation` documentation for further details.

Tip: Use a recent version of Terraform (>= 0.14.0) and a recent version of the Terraform AWS provider (>= 3.30.0) for the best results with DNS validation.

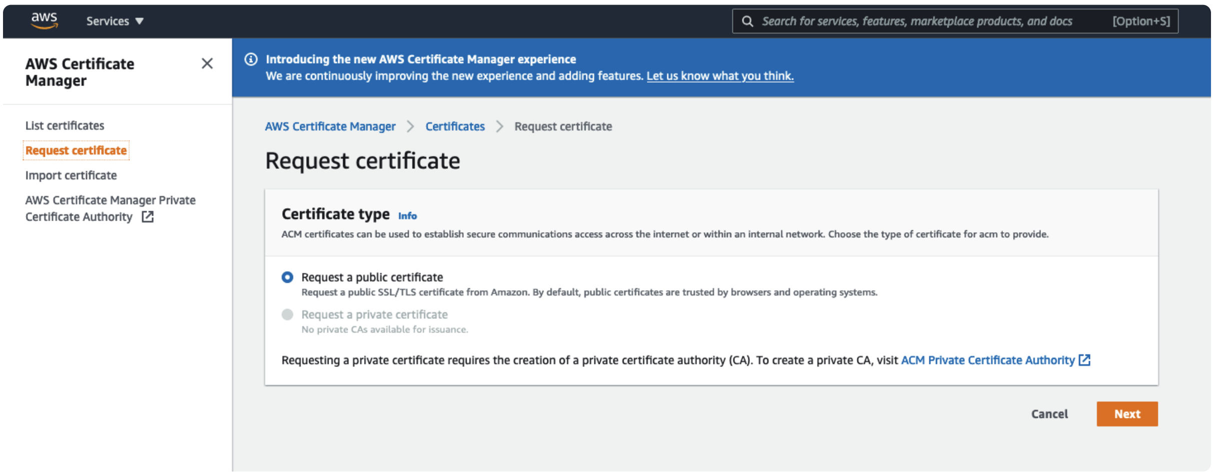
The internal.epicgames.net. private zone has automation to add the validation records without the need for access to the public zone, this means the terraform required is just the "aws_acm_certificate" resource.

```
resource "aws_acm_certificate" "substrate-vault" {
  domain_name       = local.vault_dns_name
  validation_method = "DNS"
}
```

Private zones, such as `on.epicgames.net.`, cannot be validated using DNS records and will instead need to be validated using email. Reach out us in #cloud-ops-support-ext with your certificate / DNS name to have it approved.

Creating a New Certificate From AWS Console

From the menu on the left, select Request Certificate, and choose the public option:



aws
Services ▼
Search for services, features, marketplace products, and docs
[Option+S]
AWS Certificate Manager
List certificates
Request certificate
Import certificate
AWS Certificate Manager Private Certificate Authority
AWS Certificate Manager > Certificates > Request certificate
Info
Cancel
Next

Introducing the new AWS Certificate Manager experience

We are continuously improving the new experience and adding features. Let us know what you think.

Request certificate

Certificate type

ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for acm to provide.

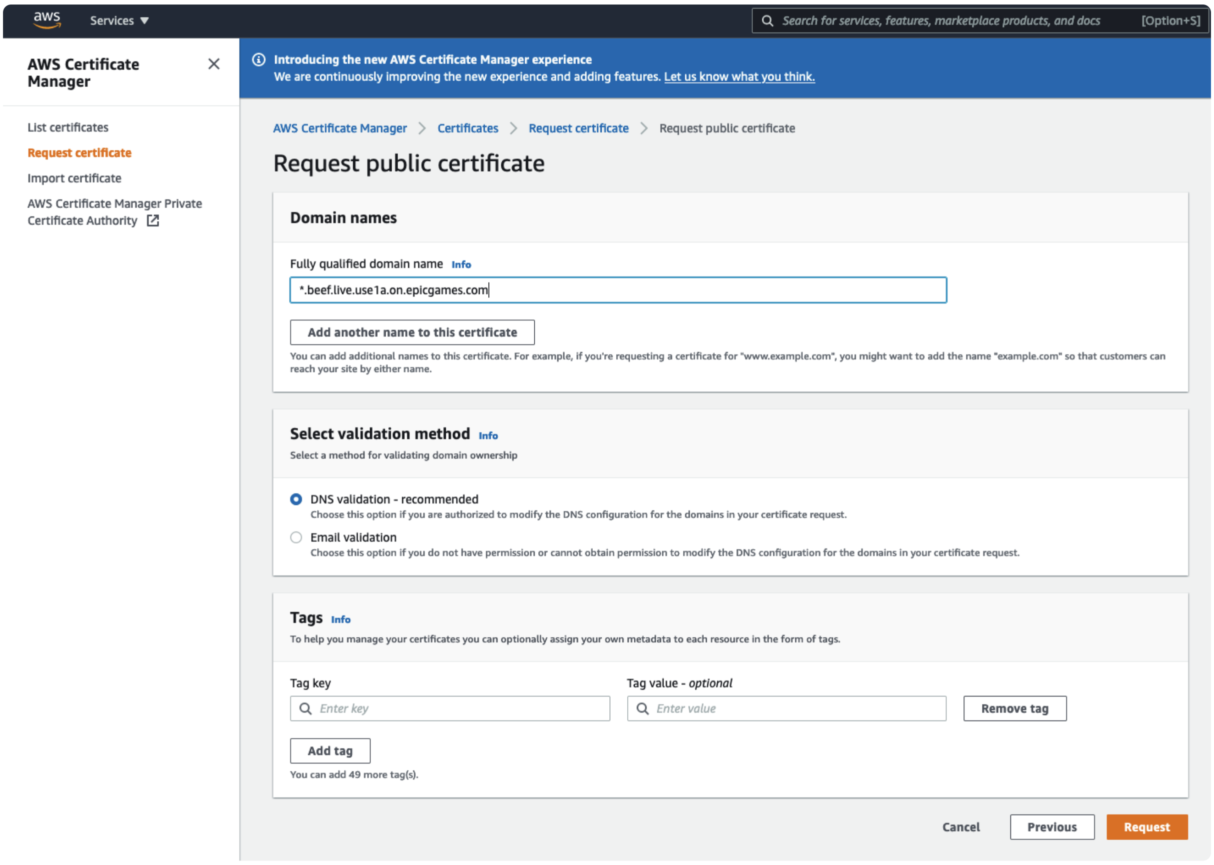
● Request a public certificate
Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.

○ Request a private certificate
No private CAs available for issuance.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit ACM Private Certificate Authority

Enter the name for your certificate (use either a wildcard, or the exact name of your service) using the DNS name of your account's route53 zone. In this case, I'm creating a new wildcard certificate.

Make sure to select DNS validation because this will make it so your certificate is automatically renewed in the following years!



aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
AWS Certificate Manager
List certificates
Request certificate
Import certificate
AWS Certificate Manager Private Certificate Authority

Introducing the new AWS Certificate Manager experience
We are continuously improving the new experience and adding features. Let us know what you think.

AWS Certificate Manager > Certificates > Request certificate > Request public certificate

Request public certificate

Domain names

Fully qualified domain name Info: *.beef.live.use1a.on.epicgames.com

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

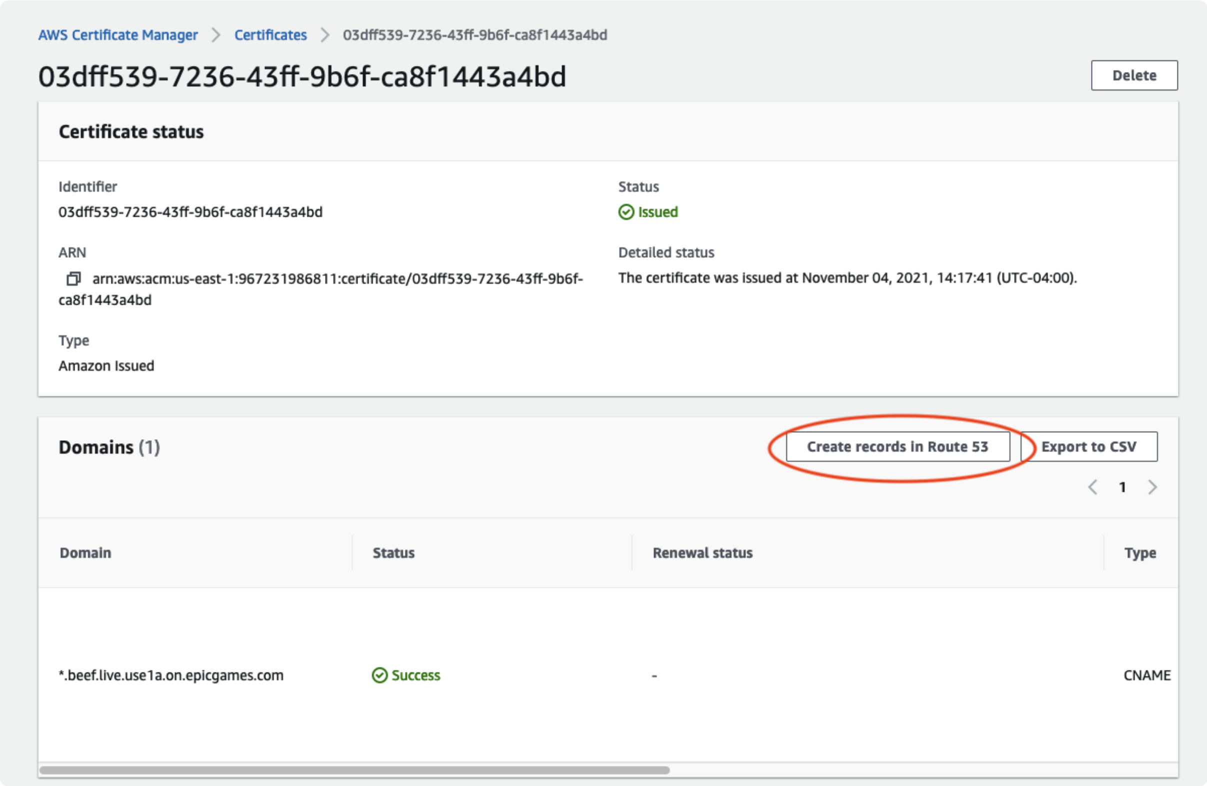
To help you manage your certificates you can optionally assign your own metadata to each resource in the form of tags.

Tag key: Enter key
Tag value - *optional*: Enter value

You can add 49 more tag(s).

After the cert is created, select it from the list and perform the final step to setup the DNS validation:

Creating records in Route 53 is not required for internal.epicgames.net domains.


AWS Certificate Manager > Certificates > 03dff539-7236-43ff-9b6f-ca8f1443a4bd
Delete
Create records in Route 53
Export to CSV
< 1 >

03dff539-7236-43ff-9b6f-ca8f1443a4bd

Certificate status

Identifier
03dff539-7236-43ff-9b6f-ca8f1443a4bd

Status
✓ Issued

ARN
arn:aws:acm:us-east-1:967231986811:certificate/03dff539-7236-43ff-9b6f-ca8f1443a4bd

Detailed status
The certificate was issued at November 04, 2021, 14:17:41 (UTC-04:00).

Type
Amazon Issued

Domains (1)

Domain	Status	Renewal status	Type
*.beef.live.use1a.on.epicgames.com	✓ Success	-	CNAME

Creating a new certificate from EKS

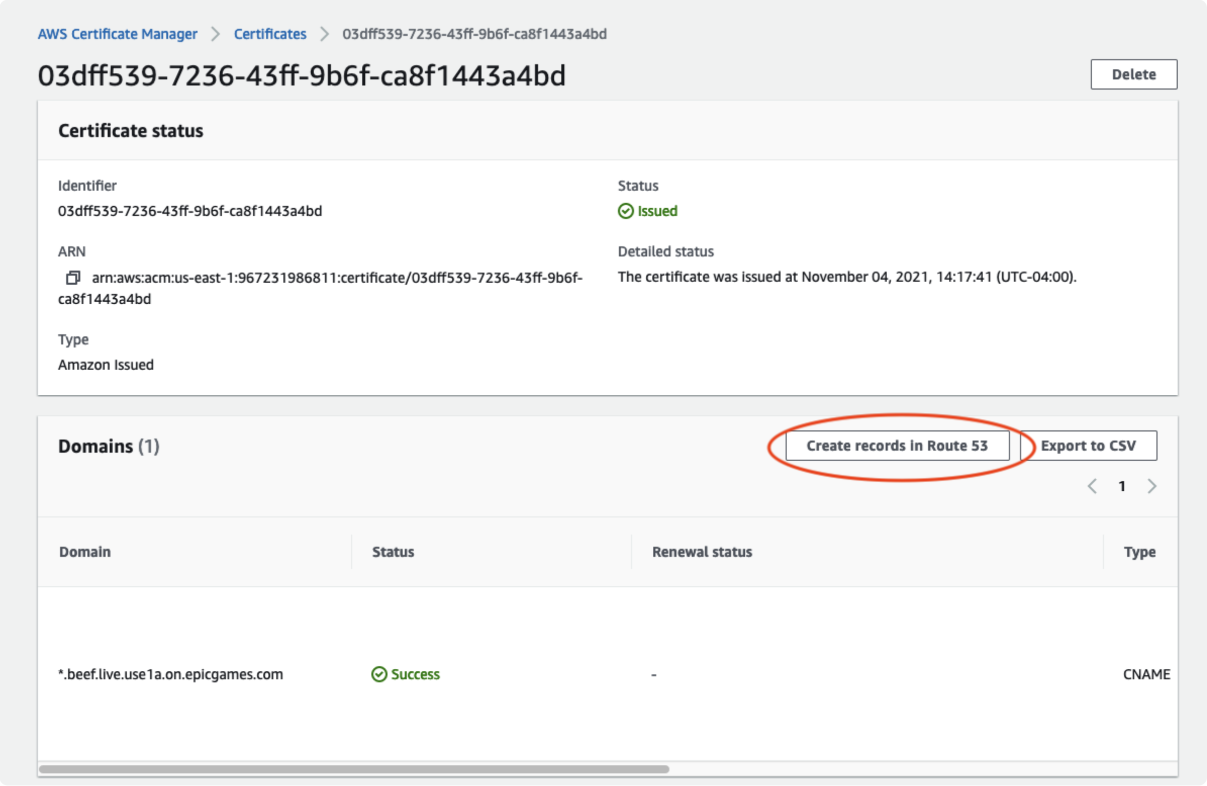
Automation exists within our EKS clusters to provision a certificate within ACM and update Kubernetes Ingress/Service resources to use the provisioned certificate.

First create a Certificate object, a documented example can be found below:

```
apiVersion: acm.epicgames.com/v1alpha1
kind: Certificate
metadata:
  # As with all Kubernetes resources, then name should be something uni
  # your application deployment.
  name: example
spec:
  # The request block contains all config relating to requesting a cert
  # from ACM. Any changes to fields in this block will result in a new
  # certificate request as the fields are immutable within AWS, this is
  # automatically and gracefully.
  request:
    # The domain name is used as the Common Name (CN) within the certif
    # request
    domainName: example.bbdc-dev.internal.epicgames.net

    # Extra Subject Alternative Names (SANs) can be specified for addit
    # domains the certificate should be valid for
    subjectAlternativeNames:
    - example2.bbdc-dev.internal.epicgames.net

    # Tags contains extra tags to add to the certificate within AWS ACM
    tags:
    - key: foo
      value: bar

  # Any Ingress objects referenced here will be updated with the
  # alb.ingress.kubernetes.io/certificate-arn annotation once the certi
  # has been created.
  #
  # This will attach the certificate to the ALB load balancer without e
  # steps.
  ingressRef:
    - name: name-of-ingress-to-add-annotation-to

  # Any Service objects referenced here will be updated with the
  # service.beta.kubernetes.io/aws-load-balancer-ssl-cert annotation on
  # certificate has been created.
  #
  # This will attach the certificate to the NLB load balancer without e
  # steps.
  serviceRef:
    - name: name-of-service-to-add-annotation-to
```

This will request a certificate from ACM, however before this certificate is issued by Amazon the domain must be validated. If the certificate is for a subdomain of `internal.epicgames.net` this validation happens automatically after a period of 2-5 minutes, for all other domains the DNS validation records currently must be created manually in the console.

To create the validation records for a non `internal.epicgames.net` domain you can navigate to the newly created certificate in the ACM UI and click "Create records in Route 53".


AWS Certificate Manager > Certificates > 03dff539-7236-43ff-9b6f-ca8f1443a4bd
Delete
Create records in Route 53
Export to CSV
< 1 >

03dff539-7236-43ff-9b6f-ca8f1443a4bd

Certificate status

Identifier
03dff539-7236-43ff-9b6f-ca8f1443a4bd

Status
✓ Issued

ARN
arn:aws:acm:us-east-1:967231986811:certificate/03dff539-7236-43ff-9b6f-ca8f1443a4bd

Detailed status
The certificate was issued at November 04, 2021, 14:17:41 (UTC-04:00).

Type
Amazon Issued

Domains (1)

Domain	Status	Renewal status	Type
*.beef.live.use1a.on.epicgames.com	✓ Success	-	CNAME

Page Information:
Page ID: 81068340
Space: Cloud Developer Platform
Downloaded: 2025-07-12 04:08:11