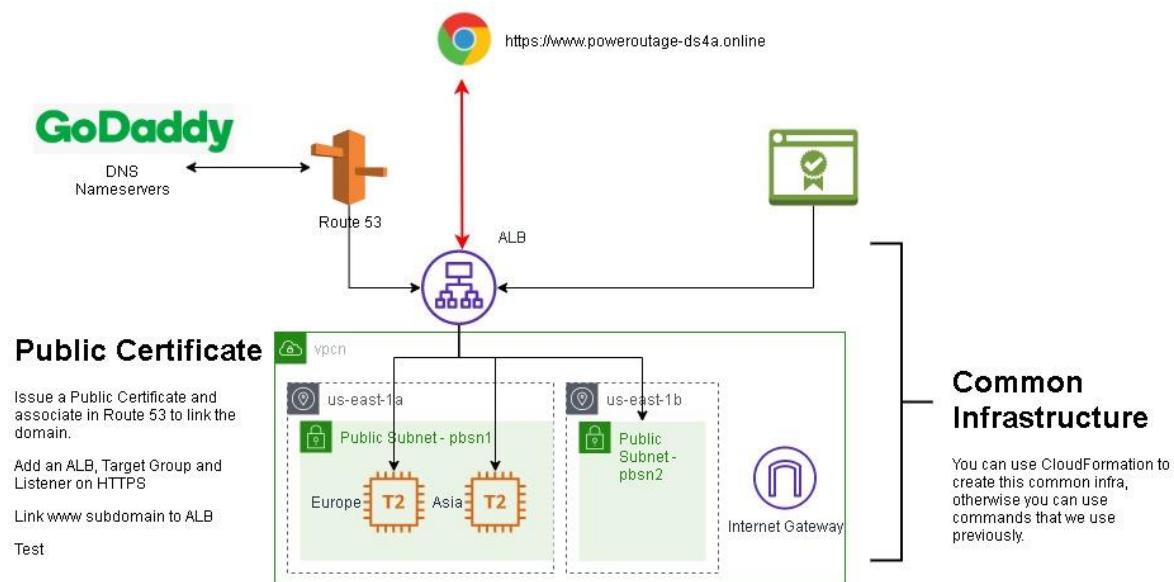


Contents

General Diagram	2
Prerequisites	2
Labs10: Lab Prerequisites (Option 1: Using Cloudformation)	2
Clean Resources	9

General Diagram



Reuse the Lab 10a to deploy the common infrastructure (VPC, Instances, ALB, Link Registrar to Route 53), then issue a TLS certificate to link to ALB and finally, create a CNAME record on Route 53 to ALB.

The common infrastructure is done using CloudFormation, and the remainder instructions are done using Web.

Prerequisites

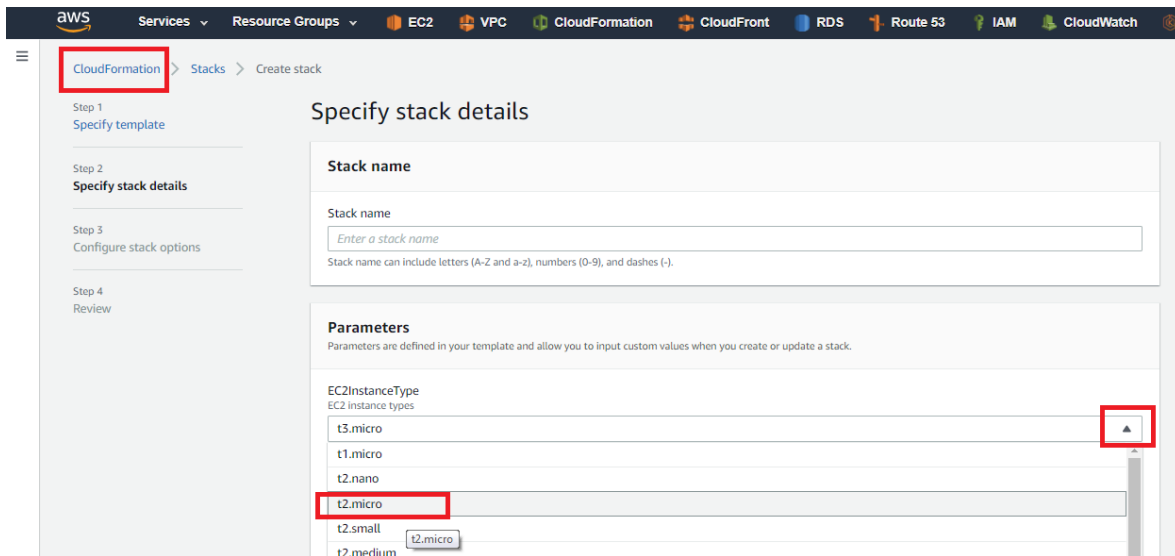
Labs1c1 have to be done and the context for Administrative user have to activated on Command Line Session.

To acquire knowledge about: DNS Concepts, Route 53 Hosted Zones, and Simple and Geolocation Routing Policies.

Labs10: Lab Prerequisites (Option 1: Using Cloudformation)

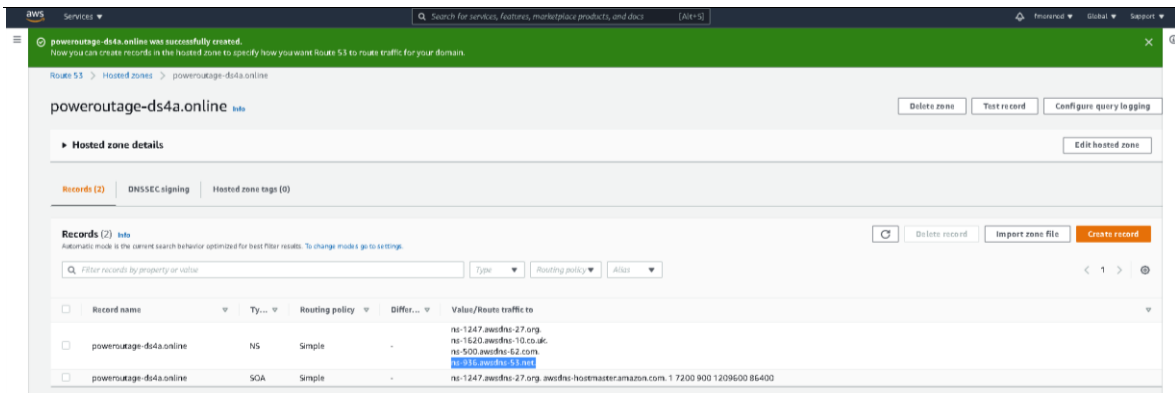
You can use the instructions of previous laboratory (Labs10c1) to create common infrastructure, with the recommendation to use t2.micro instances to use free tier for this lab.

There are subtle differences between the Cloudformation template from Labs10c1 and this lab (Labs10c2) such as: Empty subnet and ALB with public DNS.



In addition, you have to create the Registrar (GoDaddy) association to hosted zone (NS Record).

On Route 53, you create a Hosted Zone with the name of the domain (poweroutage-ds4a.online) and you every NS Record to put on the GoDaddy DNS Administration.



GoDaddy | Domain Manager

Domínios | Comprar y Vender | DNS | Configuración | Ayuda

Mis dominios

Administración de DNS

poweroutage-ds4a.online

Elige tus servidores de nombres.®

☐ Usaré los servidores de nombres GoDaddy (recomendado)

☒ Usaré mi propio servidor de nombres

ns-1247.awsdns-27.org

ns-1620.awsdns-10.co.uk

ns-500.awsdns-62.com

ns-936.awsdns-53.net

Agregar servidor de nombres

Guardar Cancel

Actualización del servidor de nombres

POWEROUTAGE-DS4A.ONLINE

⚠ Cambiar los servidores de nombres puede ser peligroso y los cambios podrían llevar a que tu sitio web desaparezca de la vista del público.

☒ Sí, doy mi consentimiento para actualizar los servidores de nombres para los dominios seleccionados.

Continuar Cerrar

Labs10c2: Issue a Public Certificate using ACM

Goes to AWS Certificate Manager and request a public certificate:

AWS Services

Search for services, features, marketplace products, and docs

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 for ACM to provide

☒ **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 - No Private CAs available for issuance. [Learn more](#)

Cancel [Request a certificate](#)

You must write the domain, you can use wildcard (*) of your domain, even you can create multiples domains on the same certificate.

Request a certificate

Step 1: Add domain names
Step 2: Select validation method
Step 3: Add tags
Step 4: Review
Step 5: Validation

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](#)

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*
*At least one domain name is required

[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](#)

[Cancel](#) [Next](#)

You have to show the ownership of that domain, therefore AWS create a CNAME or TXT record that you have to create on your DNS Administration.

Request a certificate

Step 1: Add domain names
Step 2: Select validation method
Step 3: Add tags
Step 4: Review
Step 5: Validation

Select validation method

Choose how AWS Certificate Manager (ACM) validates your certificate request. Before we issue your certificate, we need to validate that you own or control the domains for which you are requesting the certificate. ACM can validate ownership by using DNS or by sending email to the contact addresses of the domain owner.

☒ **DNS validation**
Choose this option if you have or can obtain permission to modify the DNS configuration for the domains in your certificate request. [Learn more](#)

☐ **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. [Learn more](#)

[Cancel](#) [Previous](#) [Next](#)

Request a certificate

Step 1: Add domain names
Step 2: Select validation method
Step 3: Add tags
Step 4: Review
Step 5: Validation

Review

Review your choices.

Domain name
The name you want to secure with an SSL/TLS certificate.

Domain name *.poweroutage-ds4a.online

Validation method
The method AWS uses to validate your certificate request.

Validation method DNS

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

Request a certificate

Step 1: Add domain names
Step 2: Select validation method
Step 3: Add tags
Step 4: Review
Step 5: Validation

Request in progress
A certificate request with a status of Pending validation has been created. Further action is needed to complete the validation and approval of the certificate.

Validation

Create a CNAME record in the DNS configuration for each of the domains listed below. You must complete this step before AWS Certificate Manager (ACM) can issue your certificate, but you can skip this step for now by clicking **Continue**. To return to this step later, open the certificate request in the ACM Console.

Domain	Validation status
*.poweroutage-ds4a.online	Pending validation

Add the following CNAME record to the DNS configuration for your domain. The procedure for adding CNAME records depends on your DNS service Provider. [Learn more](#).

Name	Type	Value
_c20b5dc5e12ba767c3ff2e919f7ab271.poweroutage-ds4a.online.	CNAME	_af64072526202f6d26a136602f64603.gwgc3lmt.acm-validations.aws.

Note: Changing the DNS configuration allows ACM to issue certificates for this domain name for as long as the DNS record exists. You can revoke permission at any time by removing the record. [Learn more](#)

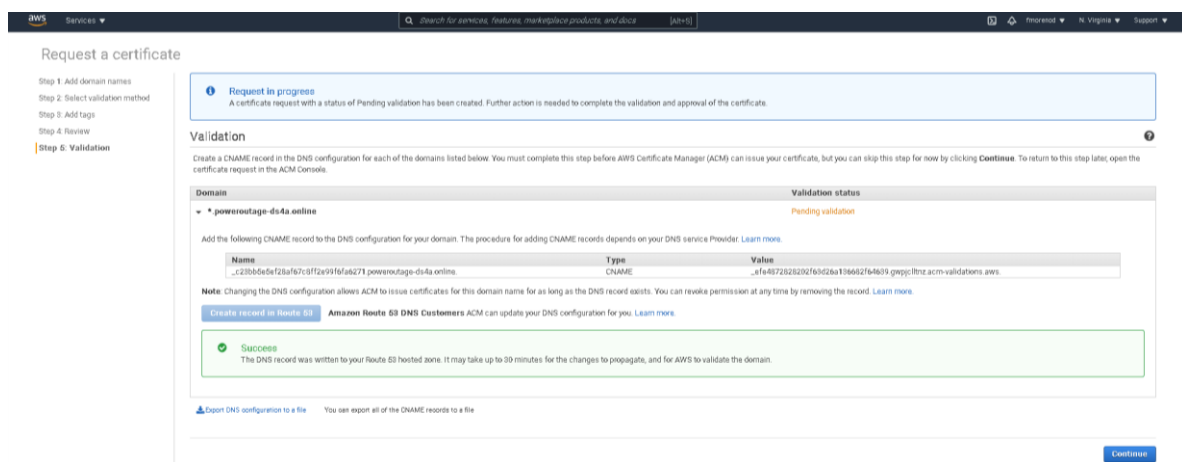
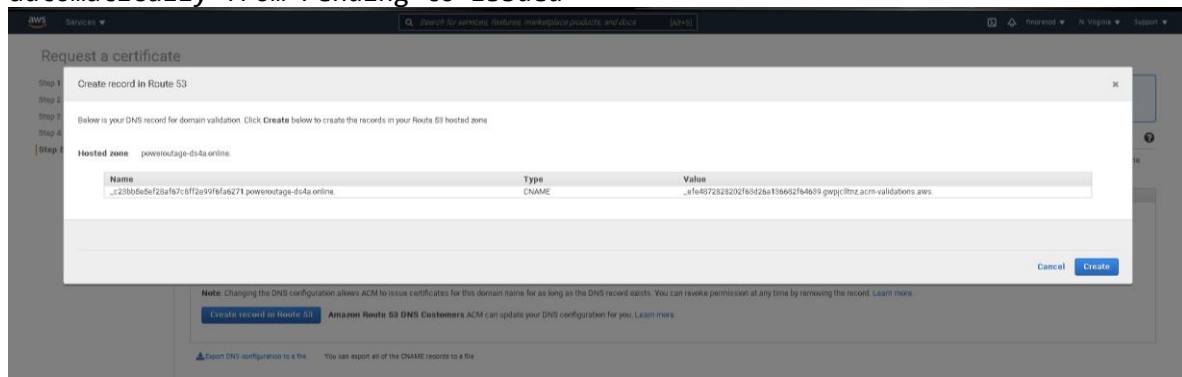
[Create record in Route 53](#) [Amazon Route 53 DNS Customers](#) ACM can update your DNS configuration for you. [Learn more](#)

[Export DNS configuration to a file](#) You can export all of the CNAME records to a file.

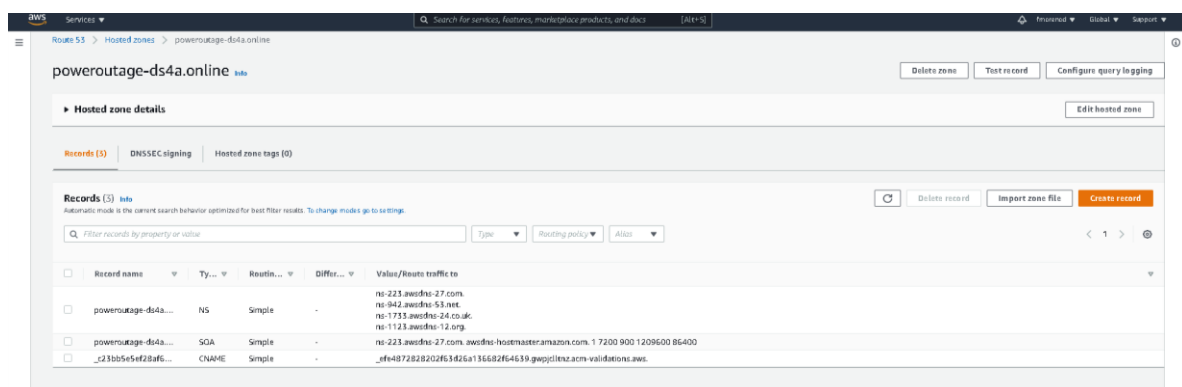
[Continue](#)

If you administer using Route 53 on the same account, you can use the “Create Record in Route 53” otherwise, you have to create the record manually and wait that AWS reckon that CNAME record. Aws change the status

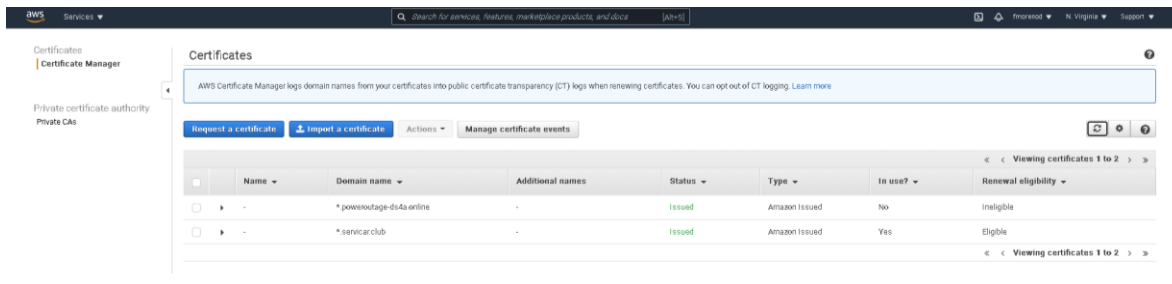
automatically from Pending to Issued



You can test on Route 53, if the record was created.

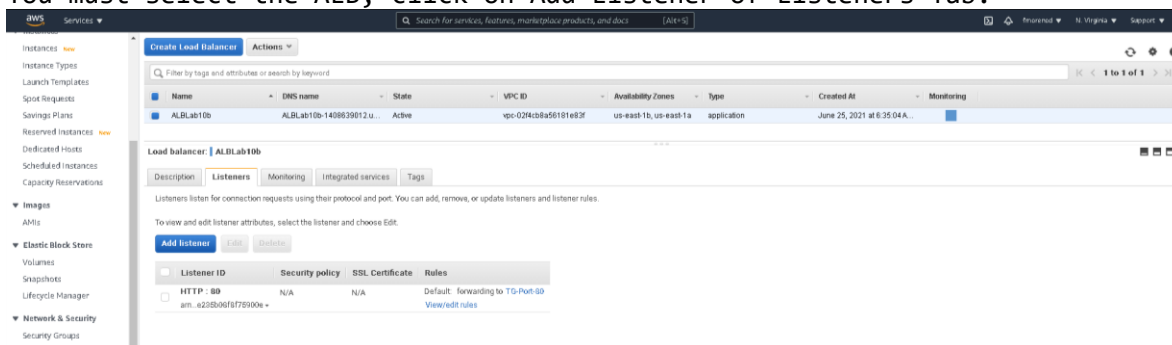


Again on ACM, you can check the Status changed to Issued.

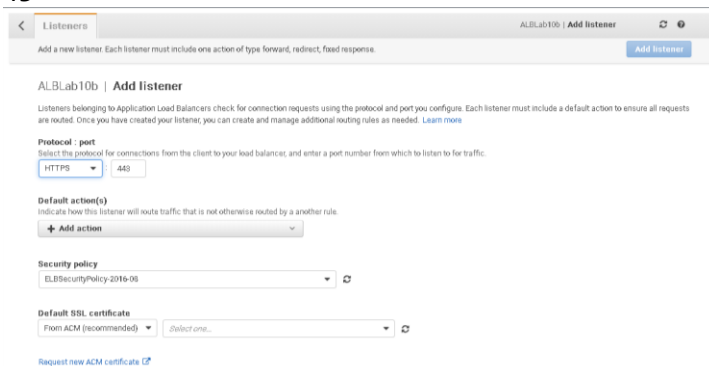


Labs10c2: Create a HTTPS Listener

On the ALB created by Cloudformation, you have to create a new listener on Port 443 (HTTPS) and associated with new certificate. You must select the ALB, click on Add Listener of Listeners Tab.



Then you choose as protocol HTTPS and AWS automatically modify the port to 443



On the action, you choose the Target Group created from Cloudformation and on Default SSL certificate, you choose the last created certification (poweroutage-ds4a.online).

ALB Lab10b | Add listener

Listeners belonging to Application Load Balancers check for connection requests using the protocol and port you configure. Each listener must include a default action to ensure all requests are routed. Once you have created your listener, you can create and manage additional routing rules as needed. [Learn more](#)

Protocol: **port**
 Select the protocol for connections from the client to your load balancer, and enter a port number from which to listen for traffic.
 HTTPS 443

Default action(s)
 Indicate how this listener will route traffic that is not otherwise routed by another rule.

1. Forward to...
 Target group: Weight (0-999) 1
 Traffic distribution: 100%
 Select a target group 0
 Group-level stickiness: ☒

Security policy
 ELBSecurityPolicy-2019-08

Default SSL certificate
 From ACM (recommended) [Select one...](#)
 *service-club-c9ad779-1132-4861-b169-c273ac776c4d
 *powerstage-ds4a-online-9b4b5833-ca3c-4cab-b2a8-abd40159a76
 *powerstage-ds4a-online-9b4b5833-ca3c-4cab-b2a8-abd40159a76

[Request new ACM certificate](#)

Finally, you have to check the configuration and follow Next options.

ALB Lab10b | HTTPS : 443

View/edit listener. Each listener must include one action of type forward, redirect, fixed response. Success: fully created listener on port 443 [Update](#)

ALB Lab10b | HTTPS : 443

Listeners belonging to Application Load Balancers check for connection requests using the protocol and port you configure. Each listener must include a default action to ensure all requests are routed. Once you have created your listener, you can create and manage additional routing rules as needed. [Learn more](#)

ARN
 arn:aws:elasticloadbalancing:us-east-1:768112764627:listener/app/ALB Lab10b:7a34b352b8b5bc/d594b5837e0692969

Protocol: **port**
 Select the protocol for connections from the client to your load balancer, and enter a port number from which to listen for traffic.
 HTTPS 443

Default action(s)
 Indicate how this listener will route traffic that is not otherwise routed by another rule.

1. Forward to
 Target group: 1 (100%)
 Group-level stickiness: Off

Security policy
 ELBSecurityPolicy-2019-08

Default SSL certificate
 From ACM (recommended) *powerstage-ds4a-online-9b4b5833-ca3c-4cab-b2a8-abd40159a76

[Request new ACM certificate](#)

aws Services [Search for services, features, marketplace products, and docs](#) [Alt+S]

Instances [Launch](#)

Instance Types
 Launch Templates
 Spot Requests
 Savings Plans
 Reserved Instances [new](#)
 Dedicated Hosts
 Scheduled Instances
 Capacity Reservations

▼ **Images**
 AMIs

▼ **Elastic Block Store**
 Volumes
 Snapshots
 Lifecycle Manager

▼ **Network & Security**
 Security Groups
 Elastic IPs

Create Load Balancer [Actions](#)

Filter by tags and attributes or search by keyword

Name	DNS name	State	VPC ID	Availability Zones	Type
ALB Lab10b	ALB Lab10b-1408639012 u...	Active	vpc-024c3b9a56181e33f	us-east-1b, us-east-1a	application

Load balancer: ALB Lab10b

[Description](#) [Listeners](#) [Monitoring](#) [Integrated services](#) [Tags](#)

Listeners listen for connection requests using their protocol and port. You can add, remove, or update listeners and listener rules.

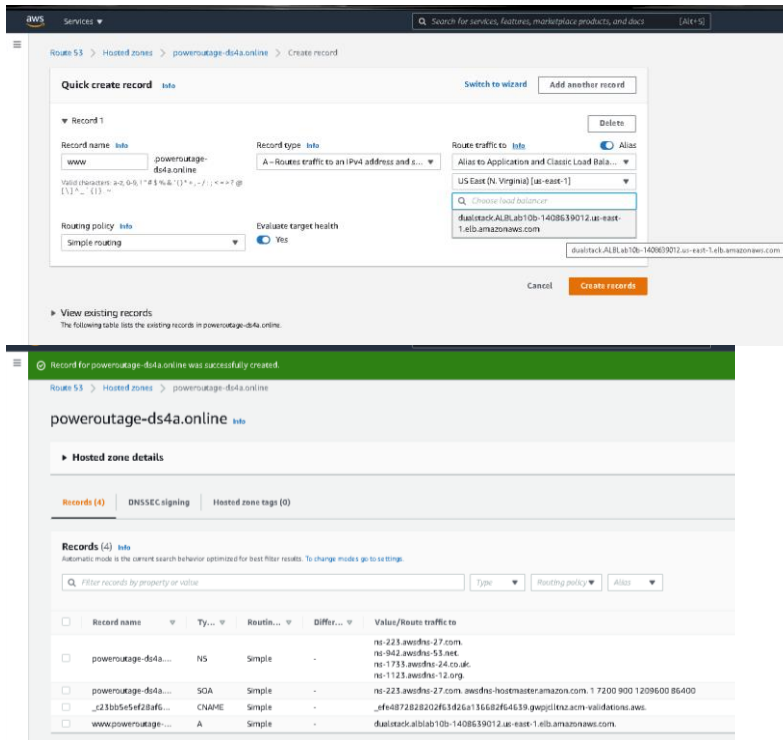
To view and edit listener attributes, select the listener and choose Edit.

[Add Listener](#) [Edit](#) [Delete](#)

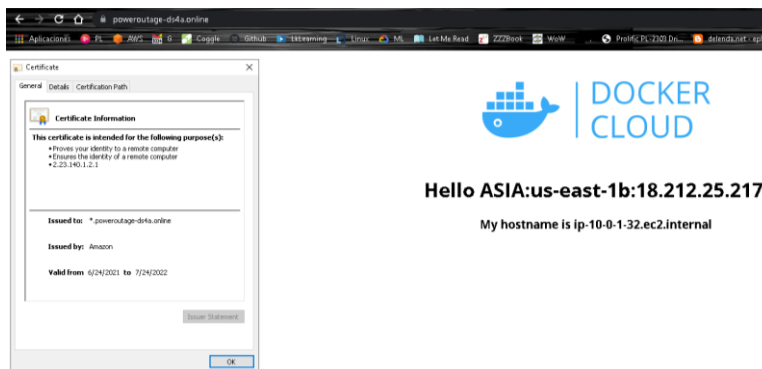
Listener ID	Security policy	SSL Certificate	Rules
<input type="checkbox"/> HTTP : 80 arn:aws:elasticloadbalancing:us-east-1:768112764627:listener/app/ALB Lab10b:7a34b352b8b5bc/d594b5837e0692969	N/A	N/A	Default: forwarding to TG-Port-80 View/edit rules
<input type="checkbox"/> HTTPS : 443 arn:aws:elasticloadbalancing:us-east-1:768112764627:listener/app/ALB Lab10b:7a34b352b8b5bc/d594b5837e0692969	ELBSecurityPolicy-2019-08	Default: powerstage-ds4a-online-9b4b5833-ca3c-4cab-b2a8-abd40159a76 (ACM) View/edit certificates	Default: forwarding to TG-Port-80 View/edit rules

Labs10c3: Create an alias with the name of the Domain on Route 53

Create the Route 53 Record Alias to your ALB



Tested using <https://www.poweroutage-ds4a.online> or the name of the record created previously.



Clean Resources

Delete using Cloudformation

Delete manually the certificates.