

Configuring SSL for CE Console

By default, the Cloud Edition Console served over HTTP through an Elastic Load Balancer. It is possible to configure the ELB to provide the access over SSL as well. This will cover the basic steps involved. For more detailed instructions see the AWS documentation for configuring a load balancer with an [HT TPS Listener](#).

Step 1

Create a domain for the ELB. You will need a domain name for your server certificate. To do this, you'll need to create (or request) a CNAME record pointing to the domain of the ELB created in the CE stack. The ELB domain can be found in the ELB console, in the Description tab:

The screenshot shows the AWS Management Console interface for configuring an Elastic Load Balancing (ELB) instance. The console displays the 'Basic Configuration' tab for the load balancer 'lustre-ba-ElasticL-1CDPZGHPIPKL2'. Key details include: Name: lustre-ba-ElasticL-1CDPZGHPIPKL2, Creation time: September 7, 2016 at 11:32:47 AM UTC-7, Hosted zone: Z35SXDOTRQ7X7K, Status: 1 of 1 instances in service, VPC: vpc-0bb2bc69, Scheme: internet-facing, and Availability Zones: subnet-ed216bab - us-east-1a. The 'Port Configuration' section shows port 80 (TCP) forwarding to 80 (TCP) with a note that stickiness options are not available for TCP protocols. The 'Security' section is also visible but empty.

Once the new domain is created, you can access the console using "http://<your domain>". It may take from several minutes to several hours for the new domain records to propagate, so it is a good idea to test this first before proceeding.

Step 2

Create the server certificate and key, using the domain created in Step 1 as the Common Name for the certificate.

For test purposes, this will create a self-signed (insecure) SSL certificate using OpenSSL:

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1001 -nodes -subj "/CN=console.example.com"
```

This method is only suggested of test purposes and this certificate should not be used for production.

Step 3

Finally, you can add an HTTPS listener to the Lustre ELB using the new certificate and key. Go to the ELB Console and select the Lustre ELB, and then select the Listeners tab.

The screenshot shows the AWS Management Console interface for an Elastic Load Balancing instance. The top navigation bar includes the AWS logo, 'Services', 'EC2', 'CloudFormation', 'S3', 'DynamoDB', and 'Edit'. The left sidebar contains a navigation menu with categories like INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and LOAD BALANCING. The main content area shows the 'Listeners' tab for the load balancer 'lustre-ba-ElasticL-1CDPZGHPIPKL2'. A table lists the current listener configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Cipher	SSL Certificate
TCP	80	TCP	80	N/A	N/A

An 'Edit' button is visible below the table. The footer contains 'Feedback', 'English', and copyright information for Amazon Web Services, Inc. (2008-2016).

Click on the Edit button in the Listeners tab. In the popup window, add a new Listener and choose HTTPS in the Load Balancer Protocol field.

The following listeners are currently configured for this load balancer:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port	Cipher	SSL Certificate
TCP	80	TCP	80	N/A	N/A
HTTPS (Secure HTTP)	443	HTTP	80	Change	Change

Buttons: Add, Cancel, Save

Click the "Change" link in the SSL Certificate column to open the edits window for adding a certificate. Choose "Upload a new SSL certificate..." option, and fill in the Certificate name field with your name for this new certificate. Then copy and past the PEM encoded private key and certificate into the appropriate fields. The Certificate Chain is optional and may be provide by a certificate signer when you have a secure certificate created.

Select Certificate

An SSL Certificate allows you to configure the HTTPS/SSL listeners of your load balancer. You may select an existing SSL certificate or create a new one below. [Learn more](#) about setting up HTTPS load balancers and certificate management.

Certificate type:

- Choose an **existing** certificate from AWS Certificate Manager (ACM)
- Choose an **existing** certificate from AWS Identity and Access Management (IAM)
- Upload a **new** SSL certificate to AWS Identity and Access Management (IAM)

Certificate name:* examplecert

Private Key:*

```
-----BEGIN RSA PRIVATE KEY-----
MIJJKQIBAAKCAgEArr8O9YQPO5ZiuTa8OQkiNrwyYw1E4B/hXnomrEBZY+LEv
M/S
(perm encoded)
```

Public Key Certificate:*

```
-----BEGIN CERTIFICATE-----
MIIFPjCCAyagAwIBAgIJAMit4KY2KX1IMA0GCSqGSIb3DQEBBQUAMB4xHDA
aBgNV
(perm encoded)
```

Certificate Chain: Optional

(pem encoded)

Cancel Save

Finally click save and then click save in the edit window. Once the HTTPS listener has been created successfully, you will be able to use "https://<your domain>" to access the CE console.