Amazon Web Services ACM

Renewal

Legacy SSL Certificate

Renewal

Customer Owned SSL Certificate

Renewal

Amazon Web Services

Legacy Customer

IAMS SAFE Engineering

27 Jul 2022

IAMS SAFE Engineering

INTERNAL

RELEASE

Amazon Web Services ACM

A SAN ssl certificate containing 3 wildcard subdomains issued by AWS ACM is automatically renewed by AWS on May 21st annually.

*.prod.hidsafeservices.com

*.uat.hidsafeservices.com

*.dev.hidsafeservices.com

Renewal

No action is required but should review the renewal at this date annually.

Legacy SSL Certificate

Legacy customers use the following ssl certificate procured from https://www.cheapsslshop.com.

*.hidsafeservices.com

*.quantumsecureservices.com

01 Jun 2023

01 Jun 2023

01 Jun 2023

01 Jun 2023

n/a

01 Jun 2023

01 Jun 2023

01 Jun 2023

Renewal

Customer Owned SSL Certificate

Customer may use their own Domain and they must provide their own ssl certificate.

Must be wildcard or SAN certificate containing all required DNS aliases.

04 May 2022

27 May 2022

27 Oct 2021

16 Feb 2022

05 Jun 2023

Renewal

Amazon Web Services

convert the ssl certificate .pem format. split the private key from the certificate.

Legacy Customer

HID SAFE Wiki : Upload Docker Image to ECR via CLI (Copy)

Upload SAFE Nimbus build into docker image and then push to AWS ECR using Power shell.

Step 1: Open Powershell and go to the Web directory Under Nimbus\Src\

Example: "C:\Users\bthomas\source\repos\Nimbus\Src\Web"

Step 2: Run the ECR Login command as follows.

C:\Users\bthomas\source\repos\Nimbus\Src\Web>Invoke-Expression   -Command (Get-ECRLoginCommand -Region us-west-1).Command

Make sure the Region is specified correctly and you will see a "Login Succeed" message as shown below.

If you are getting an error from the above command, you probably missing the AWS Profile or no AWS default profile found, so go ahead and create profile using command "aws configure" and it will ask you to enter access key, secret key, region etc.

once you created this profile close the power-shell window and open again and then try run the ECRLogin command again.

Step 3: Run the command "docker build" as shown below :

C:\Users\bthomas\source\repos\Nimbus\Src\Web>docker   build   -f "C:\Users\bthomas\source\repos\Nimbus\Src\Web\Web.Safe\Dockerfile" -t nimbus:v1 .

Note: Make sure the docker file path is correct and also please do not ignore the dot at

the end of the command.

You will see the following screens which builds the docker image (This process can take up to 30 minutes)

Step 4: Run the docker tag and then run the docker push to ECR

C:\Users\bthomas\source\repos\Nimbus\Src\Web>docker tag nimbus:v1 202101588166.dkr.ecr.us-west-1.amazonaws.com/nimbus:v1

C:\Users\bthomas\source\repos\Nimbus\Src\Web>docker tag nimbus:v1 202101588166.dkr.ecr.us-west-1.amazonaws.com/nimbus:latest (Fargate can pickup the latest image always)

Step 6: Push the newly created docker image to AWS ECR

C:\Users\bthomas\source\repos\Nimbus\Src\Web>docker push 202101588166.dkr.ecr.us-west-1.amazonaws.com/nimbus:v1

C:\Users\bthomas\source\repos\Nimbus\Src\Web>docker push 202101588166.dkr.ecr.eu-west-1.amazonaws.com/nimbus:v1 (Upload to Ireland as a backup)

If you see "no basic auth credentials" error while pushing the image, then open your ~/.docker/config.json and remove the "credsStore": "wincred" entry and then try again.

Step 6: Verify the image & tag on ECR

:

PUBLISHED

IAMS Engineering and Product Teams

Product IT

RESTRICTED

Attachments:

HID SAFE Wiki : Maintain 10.40.25.x IP Assignment

Information for network configuration:

Subnet: 255.255.255.0

Gateway: 10.40.25.1

Preferred DNS: 10.40.2.37

Alternate DNS: 10.41.137.15

10.40.25.1 to 10.40.25.254 N/W IP Range Assignment sheet

S.No

IP Address

Hostname

Purpose

Own By

All Procured Licenses installed

Remark

USED

Attachments:

Document generated by Confluence on Jul 30, 2024 06:29

Login to SAFE App Server where our SAFE LDAP Agent is running

How to run the tool:

Open the DOS command prompt and the type the following command; Replace server and port number as appropriate.

openssl s_client -connect serverName:port > serverName.txt

Certificate information will be in the output file "serverName.txt". The name of the server in the certificate was found to be serverName

Open the Output file and copy the BEGIN CERTIFICATE to END CERTIFICATION on another notepad and save as crt extension

Open the crt file to review the certificate

Eg

Your browser does not support the HTML5 video element

Attachments:

HID SAFE Wiki : Background Check Web Service (BCWS)

What is BCWS?

BCWS is TSC's API for integrating with their Designated Aviation Channeling (DAC) platform. This API enables third-party integrators such as QS SAFE to integrate with their service on the airport's behalf utilizing specific automated workflows.

BCWS Agent Documentation

TSC-BCWS Integration Prerequisites (find URLs here).

Purpose of BCWS Companion Website.

Purpose of Staging Portal.

BCWS Test Cases

4.9.3 Baseline BCWS Test case

MPA BCWS Test cases (w/ badge application).

BCWS Sanity Test cases

Attachments: