Dodanie szyfrowania w ruchu

Do tego zadania będzie potrzebna własna domena. Koszt domeny wynosi od kilku-kilkunastu zł rocznie. Domenę można też wykupić za pośrednictwem AWS.

Domena i certyfikat

1. Zapisz nazwę domeny w parametrze SSM. Przykładowo:

```
/${Project}/${Stage}/network/domain/name
```

2. Utwórz certyfikat dla domeny w usłudze AWS Certificate Manager. Jeśli domena ma być także użyta w usłudze Amazon CloudFront, utwórz drugi certyfikat - koniecznie w regionie `us-east-1`. Użyj wildcard (przykładowo `*.mojadomena.pl`)

Ustawień tych parametrów można dokonać poza pipelinem wdrażającym resztę infrastruktury.

Ten krok najlepiej wykonać ręcznie.

Jeśli walidacja certyfikatu ma nastąpić poprzez DNS - należy dodać odpowiedni rekord CNAME (na serwerze DNS u dostawcy domeny lub w usłudze Route53 w hosted zone, w której AWS zarządza domeną)

3. Zapisz ARN certyfikatów w parametrze SSM:

```
/${Project}/${Stage}/network/domain/certificate-arn
```

Pliki do zapisania domeny i ARN certyfikatu w parametrach SSM (Uwaga - parametry trzeba utworzyć w 2 regionach; certyfikaty muszą być utworzone w 2 regionach i w plikach trzeba wpisać ARN certyfikatu z danego regionu):

```
memes-generator/network/templates/params.yaml
memes-generator/network/parameters/params-dev-us-east-1.json
memes-generator/network/parameters/params-dev.json
memes-generator/network/commands/deploy-params-us-east-1.sh
memes-generator/network/commands/deploy-params.sh
```

Ustawienia portów na Listenerze i w Security Groups

Aby ruch do load balancera był możliwy w ramach protokołu HTTPS, musimy zmienić port listenera z 80 na 443 oraz protokół z HTTP na HTTPS i odpowiednio zmodyfikować reguły w `security group`.

Pliki uwzględniające ustawienia SSL:

```
memes-generator/network/templates/security-groups.yaml
memes-generator/network/parameters/security-groups-dev.json
memes-generator/application/templates/application-auto-scaling.yaml
memes-generator/application/parameters/application-auto-scaling-dev.json
```

Dodanie certyfikatu do Listenera

W ustawieniach listenera należy ponadto zmienić nazwę protokołu (z HTTP na HTTPS) i podać ARN certyfikatu.

Ustawienia Amazon CloudFront

W ustawieniach CDN należy:

1. Dodać (sub)domenę jako alternatywną nazwę CNAME (W CloudFormation jest to property `Aliases`) - pod tą (sub)domeną będzie dostępna nasza aplikacja - np. `memes.mojadomena.pl`
2. W ustawieniach Origin dot. load balancera podać port HTTPS
3. Zmienić Origin Protocol Policy na `https-only`
4. Podać url load balancera, ale już w naszej domenie (np. `api-dev.mojadomena.pl`)
5. Podać ARN certyfikatu (tego, który został utworzony w regionie `us-east-1`)

Ustawienia DNS

W zależności od tego, czy domena jest zarejestrowana na AWS czy u innego providera, ten krok będzie wyglądał inaczej

Domena wykupiona u innego dostawcy

W panelu do zarządzania domeną trzeba dodać rekord CNAME: - rekord wskazujący na URL load balancera; nazwa rekordu to np. `api-dev.mojadomena.pl` - rekord wskazujący na URL dystrybucji CloudFront; nazwa rekordu to np. `memes.mojadomena.pl`

Domena wykupiona w AWS

W hosted zone, w której zarządzasz domeną, trzeba dodać rekord CNAME lub rekord A z włączoną opcją ALIAS:

- rekord wskazujący na URL load balancera; nazwa rekordu to np. `api-dev.mojadomena.pl`
- rekord wskazujący na URL dystrybucji CloudFront; nazwa rekordu to np. `memes.mojadomena.pl`

Ponadto u providera domeny należy podać nowe serwery nazw (są one widoczne w utworzonej hosted zone jako rekordy NS)

Ustawienia DNS można wykonać ręcznie