HTTPS ON WEBSERVER

SERVER WITH NGINX - OPTION 1

SPAWN SERVER

- Login at digitalocean.com (or any other cloud vps provider)
- Create a server (Ubuntu 18.04)
  - Including SSH keys for easy access

LOGIN TO SERVER

```
ssh root@<IP address received>
apt-get update # Pull latest packages
apt-get upgrade # Upgrade so we don't have security issues
```

INSTALL WEBSERVER - NGINX

```
apt-get install nginx
```

ADD DNS RECORD

Login to your DNS service

Add A record for the IP address of the server

Check with dig that the DNS is propagating

SERVER WITH NGINX - OPTION 2

Configure *terraform* to be able to spin up server, install Nginx and setup DNS.

Not covered is installation, initialization of terraform providers (Gere: DO, AWS)

TERRAFORM - SERVER ON/OFF

```
variable "letsencryptdemodroplet_count" {
  # 1=Spin up server for demo, 0=Kill server
  description = "The number of servers to spin up."
  default = 1
}
```

SERVER CONF (1)

```
resource "digitalocean_droplet" "letsencryptdemodroplet" {
  count = "${var.letsencryptdemodroplet_count}"
image  = "ubuntu-18-04-x64"
name = "letsencryptdemodroplet"
region = "fra1"
size   = "s-1vcpu-1gb"
private_networking = true
ssh_keys = [ "97:48:83:5d:41:b2:1b:8b:15:39:d4:80:bc:0e:40:e7"]
```

SERVER CONF (2)

```
connection {
  user = "root"
  type = "ssh"
  private_key = "${file("~/.ssh/id_rsa")}"
  timeout = "2m"
  }
  provisioner "remote-exec" {
    inline = [
      "sudo apt-get update",
      "sudo apt-get -y upgrade",
      "sudo apt-get -y install nginx"
    ]
  }
}
```

DNS

```
resource "aws_route53_record" "letsencryptdemodroplet" {
  count = "${var.letsencryptdemodroplet_count}"
  name = "dm557certificatedemo"
  zone_id = "${aws_route53_zone.gr8conf_domain.id}"
  type = "A"
  ttl      = "60"
  records = ["${ digitalocean_droplet.letsencryptdemodroplet.ipv4_address}"]
}
```

INSPECT DNS

```
dig dm557certificatedemo.grydeske.org
```

LOGIN TO SERVER

```
ssh root@dm557certificatedemo.grydeske.org
```

SETUP NGINX

Check Config

```
vim /etc/nginx/sites-enabled/default
```

Update `server_name` to the chosen DNS name

Check nginx Configuration

```
nginx -t
```

Restart

```
systemctl stop nginx
systemctl start nginx
```

MAKE SURE WE HAVE THE RIGTH SERVER

Visit the server on the IP in a browser

```
vim /var/www/html/index.nginx-debian.html
```

Update title

ADD CERTBOT/LETSENCRYPT

```
add-apt-repository ppa:certbot/certbot
apt install python-certbot-nginx
```

CREATE CERTIFICATE

```
certbot --nginx -d dm557certificatedemo.grydeske.org
```

Answer the few questions

Check files in `/etc/letsencrypt/live/<dns-name>`

UPGRADE TLS VERSIONS

```
vim /etc/letsencrypt/options-ssl-nginx.conf
```

```
#ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_protocols TLSv1.2 TLSv1.3;
```

CHECK TLS

- Check in Browser
- Check with nmap
  - `nmap --script ssl-enum-ciphers -p 443 <IP Address>`
- Run SSL Test: https://www.ssllabs.com/ssltest