

Langkah-langkah deploy CTD

Sediakan server yang akan digunakan, ara2021 menggunakan upcloud dengan server Ubuntu server. Pada server yang digunakan pastikan dahulu docker dan docker-compose sudah terinstall. Jika docker belum terinstall, bisa di install melalui link berikut <https://docs.docker.com/engine/install/>

Langkah-langkah dibawah ini bisa dilakukan untuk server yang menggunakan server Ubuntu. Pertama, silahkan login menggunakan SSH untuk mengakses server. Setelah berhasil login ke dalam server, masukkan perintah terminal dibawah ini

1. Menghapus versi docker lama

```
$ sudo apt-get remove docker docker-engine docker.io containerd runc
```

2. Setup the repository

```
$ sudo apt-get update

$ sudo apt-get install \
    apt-transport-https \
    ca-certificates \
    curl \
    gnupg-agent \
    software-properties-common
```

3. Tambahkan Docker's official GPG key

```
$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo
apt-key add -
```

4. Tambahkan repository

```
$ sudo add-apt-repository \
```

```
"deb [arch=amd64] https://download.docker.com/linux/ubuntu \
$(lsb_release -cs) \
stable"
```

5. Install Docker

```
$ sudo apt-get update
$ sudo apt-get install docker-ce docker-ce-cli containerd.io
```

Setelah melakukan instalasi docker, selanjutnya clone CTFd platform dari github pada server.

```
$ git clone https://github.com/csivitu/ctfd
$ cd CTFd
```

setelah clone platform CTFd, jalankan docker dengan perintah

```
$ docker-compose up -d
```

Proses ini akan memerlukan waktu, silahkan tunggu beberapa saat. Setelah itu CTFd akan berjalan pada port 8000 di server. Silahkan mencoba mengakses server pada port 8000 dan akan terlihat halaman CTFd

Setelah itu, silahkan membeli nama domain untuk dipasang pada server, setelah itu setting domain agar menuju ke server kita. Setelah domain terpasang, silahkan mencoba mengakses domain dan akan terlihat halaman CTFd

Setelah melakukan langkah-langkah diatas, selanjutnya kita akan melakukan settings firewall, nginx dan rate limiting. Pertama, lakukan instalasi ufw (firewall service) dan nginx pada server

```
$ sudo apt update
$ sudo apt install nginx ufw
```

Selanjutnya, setting firewall nya

```
$ sudo ufw allow 'Nginx Full'
$ sudo ufw allow 'OpenSSH'
```

Setelah itu jalankan firewall nya

```
$ sudo ufw enable
```

Selanjutnya batasi rate-limiting hanya dengan 10 request per detik dan max 10 simultaneous koneksi per IP address dalam satu waktu, dan settings nginx untuk menuju port 8000 saat domain kita dipanggil

Buat sebuah file pada /etc/nginx/sites-available/namadomain dan isi dengan kode berikut

```
limit_req_zone $binary_remote_addr zone=mylimit:10m rate=10r/s;
limit_conn_zone $binary_remote_addr zone=addr:10m;
server {
    server_name namadomain;
    limit_req zone=mylimit burst=15;
    limit_conn addr 10;
    limit_req_status 429;
    client_max_body_size 8M;
    location / {
        proxy_pass http://localhost:8000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

Jika menggunakan Cloudflare, ganti `$binary_remote_addr` menjadi `$http_cf_connecting_ip`. Setelah itu, buat symlink dengan perintah dibawah ini

```
$ sudo ln -s /etc/nginx/sites-available/namadomain /etc/nginx/sites-enabled/namadomain
$ sudo nginx -s reload
```

Setelah melakukan langkah diatas, coba kembali akses server apakah semua berjalan dengan baik. Jika berjalan dengan baik langkah selanjutnya adalah menambahkan SSL. SSL yang digunakan adalah Let's Encrypt service yang menyediakan sertifikat ssl gratis

Lakukan langkah-langkah dibawah ini

```
$ sudo apt-get update
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository universe
$ sudo apt-get update

$ sudo apt-get install certbot python3-certbot-nginx
```

Setelah itu jalankan certbot dengan perintah

```
$ sudo certbot --nginx
```

Pastikan memilih opsi always redirect to HTTPS. tetapi jika menggunakan cloudflare, silahkan memilih no redirect. Setelah itu, coba kembali akses domain nya, dan kita akan melihat bahwa koneksi sudah berada pada HTTPS.

Untuk menghubungkan dengan cloudflare, pertama silahkan buat akun pada cloudflare dan tambahkan nama domain yang akan digunakan. Kedua, pilih free plan kecuali jika budget biaya yang tersedia banyak silahkan pilih plan yang lain. Setelah itu ganti Nameserver pada penyedia domain menjadi nameserver yang disediakan oleh Cloudflare. Setelah berhasil, silahkan pergi ke halaman Page Rules dan setting rules

untuk domain kita menjadi always use HTTPS. Lalu pergi ke halaman SSL tab dan setting ke Full(Strict). Lalu coba akses kembali server apakah semua berjalan dengan baik.