Nginx SSL 인증서(https) 설정

이 문서는 Nginx SSL 인증서 설정을 공유하기 위해 작성되었다. Nginx 는 일반적으로 .pem 확장자로 SSL 인증서 설정을 진행합니다.

PEM 암호를 제거하는 방법

`openssl rsa`명령을 사용하여 암호를 제거 할 수 있습니다 . 인수로 SSL을 전달 하고 파일을 출력으로 `.key`얻습니다 .

```
$ openssl rsa -in root_with_pass.key -out root.key
```

Nginx.conf에 해당 SSL 인증서 정보를 입력합니다.

- crt 파일

Nginx.conf 추가

```
    ssl_certificate     /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;
```

- pem 파일

Nginx.conf 추가

```
    ssl_certificate      root.pem;
    ssl_certificate_key  root.key;
```

예시 1) Confluence

```
server {
    listen www.example.com:80;
    server_name www.example.com;

    listen 443 default ssl;
    ssl_certificate     /etc/nginx/ssl/nginx.crt;
    ssl_certificate_key /etc/nginx/ssl/nginx.key;

    ssl_session_timeout  5m;

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers 'ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-
AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-
ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-
RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-
SHA:!DSS';
    ssl_prefer_server_ciphers   on;

location /synchrony {
        proxy_set_header X-Forwarded-Host $host;
        proxy_set_header X-Forwarded-Server $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_pass http://localhost:8091/synchrony;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "Upgrade";
    }
  location /confluence {
        client_max_body_size 100m;
        proxy_set_header X-Forwarded-Host $host;
        proxy_set_header X-Forwarded-Server $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_pass http://localhost:8090/confluence;
    }
}
```

예시 2) Bamboo

```
    server {
    listen       443 ssl;
    server_name  confluence.curvc.com;


    ssl_certificate      root.pem;
    ssl_certificate_key  root.key;

    ssl_session_timeout 5m;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:!RC4:HIGH:!MD5:!aNULL:!EDH;
    ssl_prefer_server_ciphers on;


    location / {
    proxy_pass_header Server;
    proxy_set_header X-Forwarded-Host $host;
    proxy_set_header X-Forwarded-Server $host;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_pass https://1.1.1.10:8080;  # IP
    }


    error_page   401 402 403 404 /error.html;
    location = /error.html {
    root   html;
    }

    error_page   500 502 503 504  /50x.html;
    location = /50x.html {
    root   html;
    }

}
```