HTTPS 웹 구축

구축 목적

: 기존 웹서비스에 인증서를 적용하여, 암호화를 통한 웹 접속으로 보안성을 향상시키기 위하여

참고

- 인증서는 무료 인증서 발급 기관인 Letsencrypt를 이용하여 인증서를 적용합니다.
- 무료인 대신 유효기간 90일 -> 자동 갱신 스크립트 필요
- Domain 주소가 필요하기 때문에 기존 사용 Domain이나, 없으면 Domain을 하나 구입하여 진행합니다.

  ex) xeno.fsdc.co.kr

서버 구축 진행

- 먼저 인증서를 적용하기 위하여 WEB서버 설치 와 DNS서버 설치를 먼저 진행합니다.

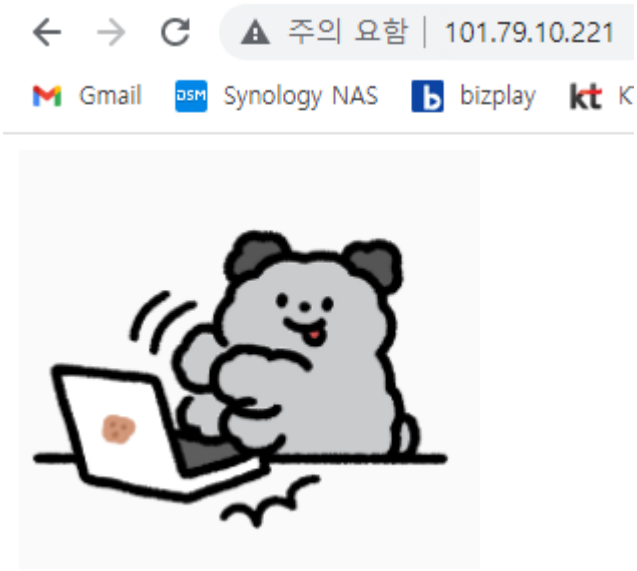
[WEB 서버 설치]

```
# yum -y install httpd-*


# vi /etc/httpd/conf/httpd.conf
----------------------------------
95 ServerName xeno.fsdc.co.kr:80
----------------------------------
( ServerName만 구매한 Domain으로 변경 )


# vi /var/www/html/index.html
( DocumentRoot 밑에 index.html 파일을 만들고 웹 생성 )
----------------------------------
HI, Xeno Web!!
----------------------------------
( 위와 같이 텍스트만 넣어서 테스트 가능 )

++추가
----------------------------------
<html>
<body>
<img src="mum.PNG">
</body>
</html>
----------------------------------
( 이미지 넣는 방법 예시 )
```

★ 웹 구축 완료 ★

WEB TEST

- 해당 웹 서버 IP로 접속하여 웹 페이지 정상적으로 나오는지 확인!



[DNS 서버 설치]

```
# yum -y install bind*


# vi /etc/named.conf
--------------------------------
13 listen-on port 53 { any; };
21 allow-query     { any; };
--------------------------------
( 53번 포트와 들어오는 쿼리에 대해서 any로 설정 )


# vi /etc/named.rfc1912.zones
--------------------------------
zone "fsdc.co.kr" IN {
        type master;
        file "fsdc.co.kr.zone";
        allow-update { none; };
};

zone "10.79.101.in-addr.arpa" IN {
        type master;
        file "fsdc.co.kr.rev";
        allow-update { none; };
};
--------------------------------
( 스크립트의 맨 아래부분에 도메인과 IP를 맞게 설정하여 zone파일과 rev파일 연결 설정 )
```

```
# cd /var/named

# cp /var/named/named.localhost /var/named/fsdc.co.kr.zone
# cp /var/named/named.localhost /var/named/fsdc.co.kr.rev
( 기존 설정파일을 복사하여 zone파일과 rev파일 생성 )

# chown .named ./fsdc.co.kr.zone
# chown .named ./fsdc.co.kr.rev
( 소유자 그룹을 named로 변경 )

# vi fsdc.co.kr.zone
-------------------------------------------------------------
$TTL 1D
@       IN SOA  fsdc.co.kr.             root(
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      xeno.fsdc.co.kr.
        IN      A       101.79.10.221
xeno    IN      A       101.79.10.221
dw      IN      CNAME   xeno.fsdc.co.kr.
-------------------------------------------------------------
( 정방향 - 네임서버 및 A 레코드 설정 적용 )


# vi fsdc.co.kr.rev
-------------------------------------------------------------
$TTL 1D
@       IN SOA  fsdc.co.kr.             root(
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      xeno.fsdc.co.kr.
221     IN      PTR     fsdc.co.kr.
221     IN      PTR     xeno.fsdc.co.kr.
-------------------------------------------------------------
( 역방향 - 네임서버 및 PTR 레코드 설정 적용 )


# vi /etc/resolv.conf
---------------------------
nameserver 127.0.0.1
---------------------------
( 윗줄에 네임서버 추가 - 동일서버에서 설정하여 루프백 주소 입력 ( 다른 DNS 서버를 사용했다면 해당 DNS 서버 주소 입력 ))
```

★ DNS 구축 완료 ★

[DNS TEST]

1. nslookup
    - Domain 주소
    - IP 주소
2. named-checkconf /etc/named.conf named-checkzone xeno.fsdc.co.kr /var/named/fsdc.co.kr.zone
   named-checkzone 10.79.101.in-addr.arpa /var/named/fsdc.co.kr.rev (설정 파일 정상여부 테스트)

[Letsencrypt 설치 및 적용]

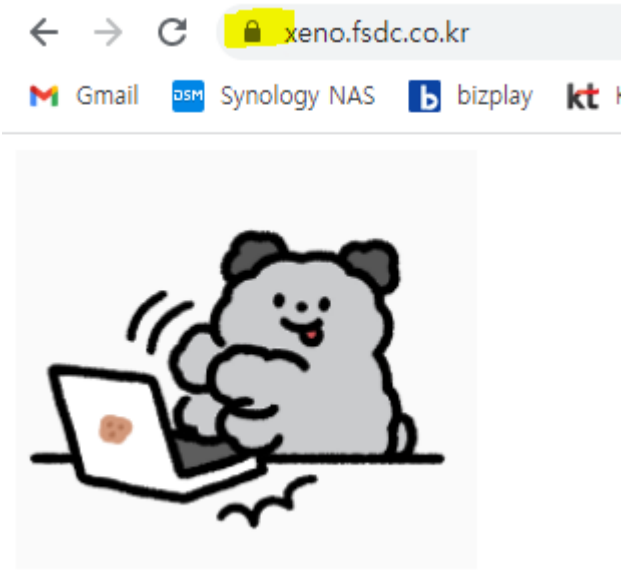
```
# yum -y install epel-release
# yum -y install certbot python2-certbot-apache


# certbot --apache certonly
------------------------------------------------------------------------------
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): chku153@xenosolution.co.kr
( 관리자용 이메일주소를 입력 )

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
(Y)es/(N)o: Y
( ACME 서버를 등록 )

We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
(Y)es/(N)o: N
( 뉴스, 캠페인 등 소식은 받지 않는다 )

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: xeno.fsdc.co.kr
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 1
( 설정한 도메인 주소 번호 입력 )
------------------------------------------------------------------------------
( 오류없이 Congratulations! 뜨면 성공 - 오류 내용 해결 아래에 기재)
-> 정상적으로 설치 완료되면 /etc/letsencrypt/live 디렉토리가 생성 됨!


# vi /etc/httpd/conf.d/ssl.conf
------------------------------------------------------------------------------
55 <VirtualHost *:443>  - 내용 변경
58 DocumentRoot "/var/www/html"
59 ServerName xeno.fsdc.co.kr
99 SSLCertificateFile /etc/letsencrypt/live/xeno.fsdc.co.kr/cert.pem
106 SSLCertificateKeyFile /etc/letsencrypt/live/xeno.fsdc.co.kr/privkey.pem
115 SSLCertificateChainFile /etc/letsencrypt/live/xeno.fsdc.co.kr/chain.pem
```

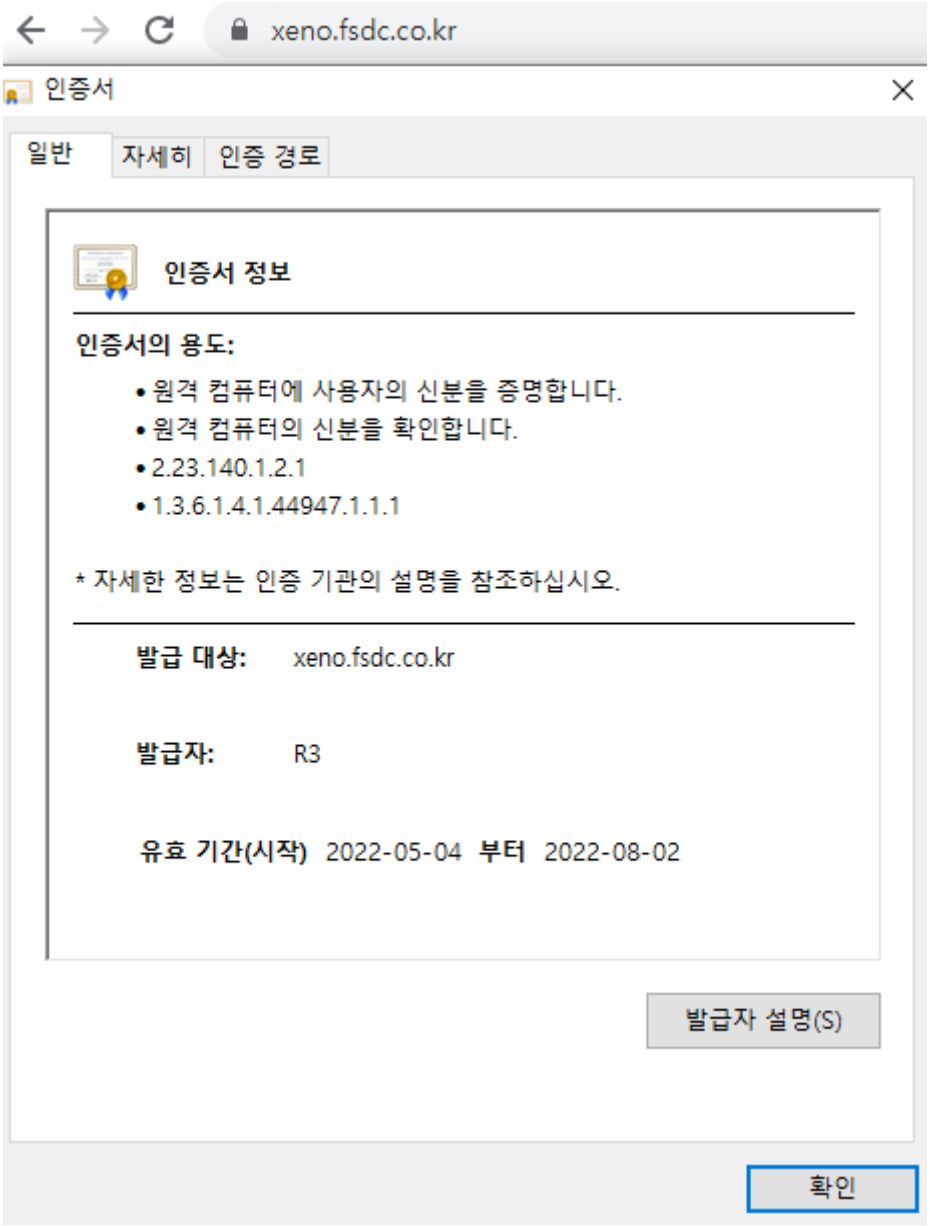
```
-------------------------------------------------------------------------------
( 해당 DocumentRoot와 ServerName 입력해주고, SSLCert 경로를 letsencrypt 경로의 인증서
들로 바꾸어 줌 )


# vi /etc/httpd/conf.d/virtual.conf
-----------------------------------------------
<VirtualHost *:80>
    ServerAdmin chku153@xenosolution.co.kr
    DocumentRoot "/var/www/html"
    ServerName xeno.fsdc.co.kr
    ErrorLog logs/ssl_error_log
    CustomLog logs/ssl_access_log combined

</VirtualHost>
-----------------------------------------------
( conf.d 밑에 해당 내용들에 맞게 Virtual Host 파일 생성 )


# systemctl restart httpd
( 위의 내용들 전부 완료한후에 아파치 재시작 후 인증서 적용 확인 )
```

★ Letsencrypt 구축 완료 ★

Letsencrypt TEST

- 웹 접속하여 인증서 정상적으로 적용되었는지 확인





++ 인증서 갱신 및 자동갱신

```
# certbot renew --dry-run
( 갱신 테스트 )

# certbot renew
( 실제로 갱신 )

# certbot certificates
( 인증서 만료일 확인 )

# crontab -e
0 9 1 * * /usr/bin/certbot renew --renew-hook="systemctl restart httpd"
( 매월 1일 9시에 인증서를 갱신하고 아파치를 재시작하는 Crontab )

# crontab -l
( crontab 리스트 확인 )
```

++ HTTP -> HTTPS 리다이렉트 설정

```
# vi /etc/httpd/conf/httpd.conf
-----------------------------------------------------
55 LoadModule rewrite_module modules/mod_rewrite.so
58 Include conf.d/virtual.conf
-----------------------------------------------------
55 : rewrite 모듈 사용
58 : vhost 설정을 하였을시에 vhost conf 파일 경로 입력 ( 현재경로 /etc/httpd 기준 )


# vi /etc/httpd/conf.d/virtual.conf
-------------------------------------------------------------
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R,L]
-------------------------------------------------------------
: 해당 vhost 설정 아래부분에 위 내용 추가
-> 1. Rewrite 모듈엔진 ON , 2. HTTPS가 off이면 , 3. https:// 로 리다이렉트
( 자세한 설정 내용은 맨 아래 참조사이트 참고 )


# systemctl restart httpd
( 아파치 리스타트 )
```

인증서 생성 오류 해결!

```
[Error 1]
Unable to find a virtual host listening on port 80 which is currently needed for
Certbot to prove to the CA that you control your domain. Please add a virtual host
for port 80.

-> httpd.conf 파일에 서버네임이 잘 등록되었는지 확인
-> Virtual host 파일 잘 등록되었는지 확인

[Error 2]
SSLError: ("bad handshake: Error([('SSL routines', 'ssl3_get_server_certificate',
'certificate verify failed')],)",)

-> --no-verify-ssl 옵션을 붙여서 실행

ex) # certbot --apache certonly --no-verify-ssl
```

★ 정상적으로 작동된다면 HTTPS 웹 구축 완료 ! ★

참조

- https://m.blog.naver.com/phongdaegi/221860968127
- https://funfunit.tistory.com/163
- https://puzji.tistory.com/entry/Certbot-SSL%EC%9D%B8%EC%A6%9D%EC%84%9C-%EC%A0%81%EC%9A%A9%ED%95%98%EA%B8%B0
- https://happist.com/548924/%EC%9B%8C%EB%93%9C%ED%94%84%EB%A0%88%EC%8A%A4-tips-lets-encrypt-%EB%AC%B4%EB%A3%8C-ssl%EC%9D%B8%EC%A6%9D%EC%84%9C-%EB%B0%9C%EA%B8%89-%EB%B0%8F-%EC%9E%90%EB%8F%99-%EA%B0%B1%EC%8B%A0
- https://devlog.jwgo.kr/2019/04/16/how-to-lets-encrypt-ssl-renew/

HTTPS 동작 방식

- https://jaeseongdev.github.io/development/2021/07/02/HTTPS,SSL,TLS/

HTTPS 리다이렉트

- https://cheershennah.tistory.com/157