목차

인증서 갱신 오류 Certificate Renew Internal Error 3
로그 확인 3
해결방법 6
참고사항 6

인증서 갱신 오류 Certificate Renew Internal Error

Nginx Proxy Manager(이하 NPM) 사용시 인증서를 새로 갱신하려 할때 아래와 같은 오류가 발생한다.

또는 원래 인증서 유효기간이 30일 미만으로 남았을때 자동 갱신되어야 하는데 동작하지 않는다.

이는 certbot의 인증서 파일 구조가 바뀌어서 그럴수 있다.

로그 확인

certbot이나 npm의 로그를 확인해보면 아래와 같은 로그가 찍힌다.

시스템 로그 메시지 messages또는 syslog 또는 journalctl -f 로 확인시 아래와 같은 로그

```
Oct 22 20:22:56 proxy npm[425719]: [10/22/2024] [11:22:56 AM] [SSL      ] ›
   info      Renewing Let'sEncrypt certificates via Cloudflare for Cert #10:
*.fatp.org, fatp.org
Oct 22 20:22:56 proxy npm[425719]: [10/22/2024] [11:22:56 AM] [SSL      ] ›
   info      Command: certbot renew --force-renewal --config
"/etc/letsencrypt.ini" --work-dir "/tmp/letsencrypt-lib" --logs-dir
"/tmp/letsencrypt-log" --cert-name 'npm-10' --disable-hook-validation --no-
random-sleep-on-renew
Oct 22 20:22:56 proxy npm[425719]: [10/22/2024] [11:22:56 AM] [Global   ] ›
   debug     CMD: certbot renew --force-renewal --config
"/etc/letsencrypt.ini" --work-dir "/tmp/letsencrypt-lib" --logs-dir
"/tmp/letsencrypt-log" --cert-name 'npm-10' --disable-hook-validation --no-
random-sleep-on-renew
Oct 22 20:22:56 proxy npm[425719]: [10/22/2024] [11:22:56 AM] [Express  ] ›
⚠  warning   Saving debug log to /tmp/letsencrypt-log/letsencrypt.log
Oct 22 20:22:56 proxy npm[425719]: Renewal configuration file
/etc/letsencrypt/renewal/npm-10.conf is broken.
Oct 22 20:22:56 proxy npm[425719]: The error was: expected
```

```
/etc/letsencrypt/live/npm-10/cert.pem to be a symlink
Oct 22 20:22:56 proxy npm[425719]: Skipping.
Oct 22 20:22:56 proxy npm[425719]: 0 renew failure(s), 1 parse failure(s)
Oct 22 20:22:56 proxy npm[425719]: Ask for help or search for solutions at
https://community.letsencrypt.org. See the logfile /tmp/letsencrypt-
log/letsencrypt.log or re-run Certbot with -v for more details.
```

위 메시지 내용을 보면 알겠지만

```
Oct 22 20:22:56 proxy npm[425719]: Renewal configuration file
/etc/letsencrypt/renewal/npm-10.conf is broken.
Oct 22 20:22:56 proxy npm[425719]: The error was: expected
/etc/letsencrypt/live/npm-10/cert.pem to be a symlink
```

이라는 부분을 확인할 수 있다.

현재 문제가 발생하는 시스템의 디렉토리 구조는 아래와 같다.

```
.
├── archive
│   ├── npm-10
│   │   ├── cert1.pem
│   │   ├── cert2.pem
│   │   ├── chain1.pem
│   │   ├── chain2.pem
│   │   ├── fullchain1.pem
│   │   ├── fullchain2.pem
│   │   ├── privkey1.pem
│   │   └── privkey2.pem
│   └── npm-9
│       ├── cert1.pem
│       ├── cert2.pem
│       ├── chain1.pem
│       ├── chain2.pem
│       ├── fullchain1.pem
│       ├── fullchain2.pem
│       ├── privkey1.pem
│       └── privkey2.pem
├── credentials
│   ├── credentials-10
│   └── credentials-9
├── live
│   ├── npm-10
│   │   ├── cert.pem
│   │   ├── chain.pem
│   │   ├── fullchain.pem
│   │   ├── privkey.pem
│   │   └── README
```

```
│   ├── npm-9
│   │   ├── cert.pem
│   │   ├── chain.pem
│   │   ├── fullchain.pem
│   │   ├── privkey.pem
│   │   └── README
│   └── README
├── renewal
│   ├── npm-10.conf
│   └── npm-9.conf
└── renewal-hooks
    ├── deploy
    ├── post
    └── pre
```

디렉토리 구조에서 보는바와 같이 실제 인증서 파일이 `live`디렉토리 아래에 존재하게 된다. 하지만 `certbot`은 실제 파일 자체를 `archive`디렉토리에 존재시키고 심볼릭 링크만 `live`디렉토리에 두는 형태로 되어있다.

```
.
├── archive
│   ├── npm-12
│   │   ├── cert1.pem
│   │   ├── cert2.pem
│   │   ├── chain1.pem
│   │   ├── chain2.pem
│   │   ├── fullchain1.pem
│   │   ├── fullchain2.pem
│   │   ├── privkey1.pem
│   │   └── privkey2.pem
│   └── npm-9
│       ├── cert1.pem
│       ├── cert2.pem
│       ├── chain1.pem
│       ├── chain2.pem
│       ├── fullchain1.pem
│       ├── fullchain2.pem
│       ├── privkey1.pem
│       └── privkey2.pem
├── credentials
│   ├── credentials-10
│   └── credentials-9
├── live
│   ├── npm-12
│   │   ├── cert.pem -> ../../archive/npm-12/cert2.pem
│   │   ├── chain.pem -> ../../archive/npm-12/chain2.pem
│   │   ├── fullchain.pem -> ../../archive/npm-12/fullchain2.pem
│   │   ├── privkey.pem -> ../../archive/npm-12/privkey2.pem
│   │   └── README
│   ├── npm-9
```

```
│   │   ├── cert.pem
│   │   ├── chain.pem
│   │   ├── fullchain.pem
│   │   ├── privkey.pem
│   │   └── README
│   └── README
├── renewal
│   ├── npm-12.conf
│   └── npm-9.conf
└── renewal-hooks
    ├── deploy
    ├── post
    └── pre
```

두번째 환경의 디렉토리를 구조에서 npm-12와 npm-9의 차이를 보면 확실히 알수 있게 된다. npm-12는 정상적인 디렉토리 구조인데 실제 인증서는 archive에 존재하고 그중 가장 최신 인증서만 심볼릭 링크로 live디렉토리에 존재하는 형태인 것을 알 수 있다. 물론 갱신할때마다 파일명은 맨 뒤의 숫자가 1씩 올라가는 구조이다.

해결방법

따라서 해결방법은 현재 존재하는 인증서를 archive디렉토리 하위로 옮기면서 가장 최근 인증서 번호+1 한 파일로 변경하고 live디렉토리에는 해당 인증서의 심볼릭 링크만 걸어주면 된다. 귀찮다면 그냥 기존 만료된 인증서중에 1번에 해당하는것을 그냥 링크로 걸어준다음 수동으로 인증서 갱신(renew) 작업을 한번 해주면 자동으로 처리된다.

주의할점은 반드시 인증서파일명 + 숫자 형태로 만들어야 한다. 뒤에 숫자가 없다면 인식하지 못한다.

참고사항

만약 컨테이너 환경이 아니라 네이티브 환경이라면 단순히

```
$ certbot update_symlinks
```

이 명령어로 자동으로 심볼릭 링크 환경으로 변경해준다.

왜인지는 모르겠지만 인증서 갱신 과정에서 이러한 오류가 종종 발생하는것으로 보인다.

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/%EC%9D%B8%EC%A6%9D%EC%84%9C_%EA%B0%B1%EC%8B%A0_%EC%98%A4%EB%A5%98_certificate_renew_internal_error

Last update: **2024/10/22 12:19**