

Synology SSL : Synology DSM에 와 일드카드 SSL 인증서 설치

- 와일드카드 인증서 발행 목적
- Cloudflare API Token
- "acme.sh"를 통한 SSL 인증서 발급

와일드카드 인증서 발행 목적


만일 "aaa.synology.me" 같은 시놀로지 DDNS를 이용하신다면 이 과정은 필요가 없을 것 입니다.

하지만 별도 도메인을 구입하여 시놀로지에 적용하실 경우 와일드카드 인증서 발행이 지원되지 않습니다.

예를 들어 제 경우 "dhcloud.me"라는 도메인을 사용 중이고, 시놀로지 DSM 연결을 "aaa.dhcloud.me"와 같은 서브 도메인을 사용하고 싶을 경우가 생깁니다.

시놀로지 "보안"에서 인증서를 발행 할 경우 하나 하나 서브 도메인 인증서를 발행해야 합니다.

여기서 안내되는 과정을 진행 한다면 가지고 계신 도메인에 대한 와일드카드 인증서 (*.dhcloud.me)를 발행해 DSM에 사용할 수 있습니다.

**dhcloud.me** - 2023-09-07
(기본 인증서) (ECC)

발급자:

주제 대체 이름:

대해:

ZeroSSL ECC Domain Secure Site CA
dhcloud.me, *.dhcloud.me
로그 수신, Replication Service, VPN Server, WebDAV Server, Synology Drive Server, KMIP, FTPS, Synology Storage Console Server, 시스템 기본 설정, Virtualization - 14641, FileStation - 7001, NoteStation - 9351, SynologyPhotos - 5443, *:8181, SynologyDrive - 10003

Cloudflare API Token

제가 사용중인 Cloudflare DNS 기준으로 설명 드립니다.

SSL 인증서 발행에 앞서 먼저 Cloudflare의 API Token이 필요 합니다.

"<https://dash.cloudflare.com/profile/api-tokens>"에서 먼저 API Token을 생성 합니다.

"acme.sh"를 통한 SSL 인증서 발급

먼저 root 권한으로 변경 합니다.

```
sudo -i
```

root 디렉토리로 이동합니다.

```
cd ~
```

"acme.sh" 파일을 다운로드 합니다.

```
wget https://github.com/acmesh-official/acme.sh/archive/master.tar.gz
```

다운로드 받은 파일의 압축을 해제해 줍니다.

```
tar xvf master.tar.gz
```

압축해제된 디렉토리로 이동합니다.

```
cd acme.sh-master/
```

"acme.sh"를 실행하여 설치를 진행합니다.

```
./acme.sh --install --nocron --home /usr/local/share/acme.sh --accountemail "이메일주소"
```

아래 명령을 추가 실행해 줍니다.

```
source ~/.profile
```

사용하는 Cloudflare의 정보를 export 해줍니다. (아래 정보는 Cloudflare의 API에서 확인 가능 합니다.)

```
export CF_Email="Cloudflare 이메일"  
export CF_Token="Cloudflare API Token 값"  
export CF_Account_ID="계정ID"  
export CF_Zone_ID="영역ID"
```

인증서를 생성해 줍니다.

```
cd /usr/local/share/acme.sh  
export CERT_DNS="dns_cf"
```

아래의 도메인 입력은 "aaa.com"과 같은 A 레코드 주소와 "*.aaa.com" 같은 와일드카드를 같이 넣어주셔야 합니다.

```
./acme.sh --issue --home . -d '도메인' -d '*.도메인' --dns "$CERT_DNS"
```

아래와 같은 메시지가 출력되어야 정상입니다.

[Mon May 1 18:58:10 KST 2023] Cert success.

-----BEGIN CERTIFICATE-----



-----END CERTIFICATE-----

[Mon May 1 18:58:10 KST 2023] Your cert is in: ./도메인_ecc/도메인cer

[Mon May 1 18:58:10 KST 2023] Your cert key is in: ./도메인_ecc/도메인.key

[Mon May 1 18:58:10 KST 2023] The intermediate CA cert is in: ./도메인_ecc/ca.cer

[Mon May 1 18:58:10 KST 2023] And the full chain certs is there: ./도메인_ecc/fullchain.cer

만일 실패 시 아래와 같이 다시 진행 합니다.

```
./acme.sh --register-account -m 이메일주소 --issue --home . -d '도메인' -d '*.도메인' --dns "$CERT_DNS"
```

이제 시놀로지 인증서를 신규 발급받은 인증서로 교체 합니다. 주의점은 모든 2단계 인증을 꺼주셔야 합니다,

```
cd /usr/local/share/acme.sh
export SYNO_Username='시놀로지 로그인 ID'
export SYNO_Password='*시놀로지 로그인 비번'
export SYNO_Scheme="http"
export SYNO_Port="5000"
export SYNO_Certificate=""
./acme.sh --deploy --home . -d '도메인' -d '*.도메인' --deploy-hook synology_dsm
```

만일 2단계 인증을 사용중이시라면 Cookie를 통해 Device ID를 알아내어 아래 문구를 추가해 주셔야 합니다.

With OTP (2-Factor-Authentication)



Use your browser to sign in with the admin account you want to use. When entering the OTP code, check the "Save this device" checkbox and continue. Get the device ID from the cookie did (Left click on the lock to the left side of the URL -> Cookies and Copy the content of the did cookie). Set the environment variable to the cookie value:

```
export SYNO_DID="DID값"
```

주기적인 인증서의 자동 갱신은 시놀로지의 스케줄러를 통해 아래 스크립트를 명령해 주시면 됩니다.



```
/usr/local/share/acme.sh/acme.sh --cron --home /usr/local/share/acme.sh/
```

