Win-ACME로 와일드카드 인증서 생성 과정 요약

기본 설정 및 실행

win-acme 실행 방법

```
# 관리자 권한으로 명령 프롬프트 실행
cd C:₩tools₩win-acme
wacs.exe
```

메뉴 선택

- M (Create certificate - full options) 선택
- 기본 설정으로는 와일드카드 인증서 발급이 어려우므로 **반드시 전체 옵션 선택**

도메인 입력 과정

와일드카드 인증서를 위한 도메인 입력

```
# 올바른 입력 방법 (쉼표로 구분)
example.com,*.example.com
```

중요 포인트:

- **띄어쓰기가 아닌 쉼표(,)로 구분**하여 입력
- 기본 도메인과 와일드카드 도메인을 함께 입력
- 이렇게 하면 기본 도메인(`example.com`)과 모든 1레벨 서브도메인을 포함하는 인증서 생성

도메인 입력 확인

정상적으로 입력되면 win-acme에서 다음과 같이 표시:

```
Certificate will be created for the following identifiers:
- example.com
- *.example.com
```

인증 방법 선택

DNS-01 챌린지 필수

와일드카드 인증서는 **반드시 DNS-01 챌린지 방식**을 사용해야 합니다:

- **옵션 6번**: Create verification records manually (수동으로 인증 레코드 생성)
- **옵션 7번**: Create verification records acme-dns
- **옵션 8번**: Create verification records with your own script

가장 일반적으로는 수동 방식(6번) 선택

DNS TXT 레코드 설정

TXT 레코드 생성 정보

win-acme에서 제공하는 정보:

```
Please deploy a DNS TXT record under the name:
_acme-challenge.example.com

with the following value:
asdvjkdsjagligjadsiiadgjiladgjagds
```

DNS 제공업체에서 설정

DNS 제공업체(가비아, 후이즈, Route53 등)에서 TXT 레코드 추가:

- **레코드 타입**: TXT
- **호스트명**: `_acme-challenge`
- **값**: win-acme에서 제공한 긴 문자열

설정 후 DNS 전파 시간(5-10분) 대기 후 Enter로 검증 진행

인증서 저장 위치

WACS 기본 저장 경로

```
# 인증서 파일
C:₩ProgramData₩win-acme₩httpsacme-v02.api.letsencrypt.org₩Certificates₩

# 설정 파일
C:₩ProgramData₩win-acme₩httpsacme-v02.api.letsencrypt.org₩
```

```
# 로그 파일
C:₩ProgramData₩win-acme₩Log₩
```

생성되는 인증서 파일들

```
example.com-chain.pem          # 인증서 체인
example.com-crt.pem            # 서버 인증서
example.com-key.pem            # 개인키
example.com-chain-only.pem     # 체인 인증서만
```

중요 고려사항

와일드카드 적용 범위

- `*.example.com`은 **한 레벨의 서브도메인**에만 적용
- `api.example.com`에 적용 ✓
- `sub.api.example.com`에 적용 ✗

자동 갱신 제한

- **수동 DNS 방식 사용 시 자동 갱신 불가능**
- 3개월마다 수동으로 갱신 과정 반복 필요

DNS 검증 반복 필요성

- 동일한 이름으로 인증서를 재생성할 때도 **매번 새로운 DNS 검증 과정** 필요
- 기존 TXT 레코드 재사용 불가 (새로운 챌린지 값 생성됨)

대안 방법

WSL2 활용 방법

win-acme에서 오류 발생 시 WSL2를 통한 acme.sh 스크립트 사용:

```
#!/bin/sh
# acme.sh 스크립트 사용
/root/acme.sh --issue --dns --force -d example.com -d *.example.com --yes-I-know-dns-manual-mode-enough-go-
```

```
ahead-please --server letsencrypt
```

자동화 권장사항

- **DNS API 지원 제공업체 사용**: Cloudflare, Azure DNS, Route53 등
- **acme-dns 서비스 활용**: CNAME 위임 방식으로 자동화

인증서 삭제 방법

WACS GUI를 통한 삭제

```
wacs.exe
# D (Delete certificate) 선택
# 삭제할 인증서 선택 후 확인
```

관련 설정 정리

1. IIS 바인딩 제거
2. 작업 스케줄러에서 갱신 작업 제거
3. 인증서 저장소 정리

이상이 win-acme를 사용한 와일드카드 인증서 생성의 전체 과정입니다. DNS-01 챌린지의 수동 설정이 핵심이며, 자동화를 위해서는 DNS API 지원이 필요합니다.