

---

# 공인인증기관 LDAP 서버 접근설정 방법

---

Date : 16 Sep 2011

Doc No : KICA-공인인증기관 LDAP 서버 접근설정 방법

## 공인인증기관 LDAP 서버 접근설정 방법

### ● 작업 대상 서버

- WEB/WAS 서버
- 당사의 제품을 설치한 서버

### ● 작업 내용

- 방화벽 설정: LDAP 서버 접근 허용
  - 인증서 유효성 검증을 수행하기 위하여 5개 공인인증기관 인증센터의 LDAP 서버에 도메인명 등록과 포트 개방
  - GPKI를 사용하실 경우는 행정전자서명 인증센터의 LDAP 서버에 도메인명 등록과 포트 개방

#### NPKI 인증서 사용할 경우

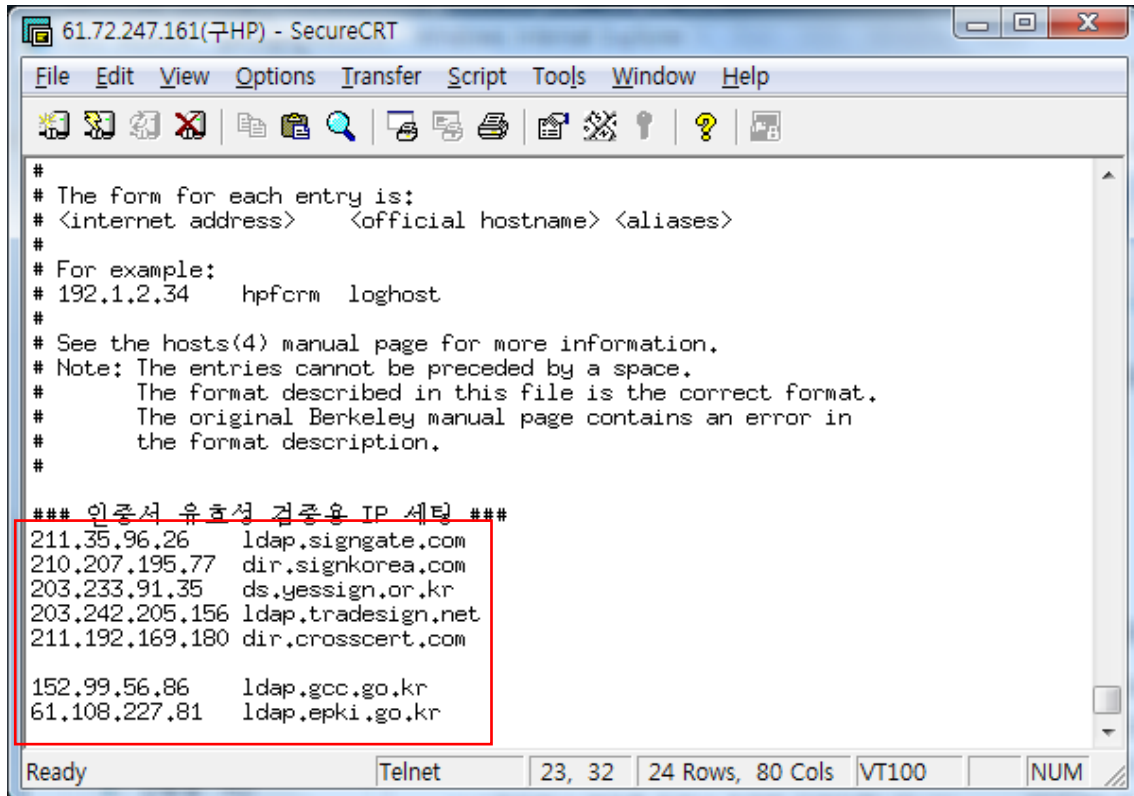
서비스	URL	IP	Port	비고
LDAP	ldap.signgate.com	211.35.96.26	389	outbound
	dir.signkorea.com	210.207.195.77		
	ds.yessign.or.kr	203.233.91.35		
	ldap.tradesign.net	203.242.205.156		
	dir.crosscert.com	211.192.169.180		

#### GPKI 인증서 사용할 경우

서비스	URL	IP	Port	비고
LDAP	ldap.gcc.go.kr	152.99.56.86	389	outbound
	ldap.epki.go.kr	61.108.227.81		

※ outbound port : 작업대상 서버에서 외부로 나가는 포트

- hosts 파일 내에 서버 환경 설정 수정
  - /etc/hosts 파일 내에 URL과 IP 정보 등록
  - (ex) /etc/hosts 파일에 정보 등록



name server에 연결되지 않는 서버의 경우 등록이 필요하다. Windows의 경우

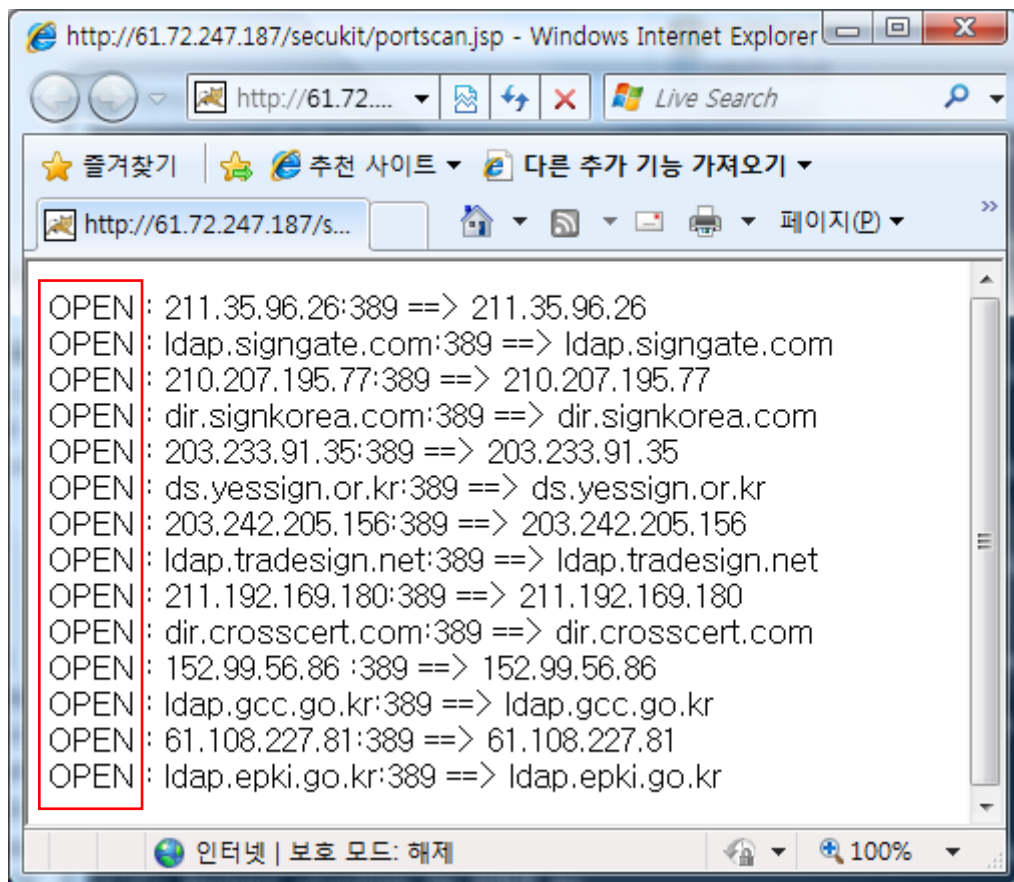
C:\Windows\system32\drivers\etc\hosts 파일에 아래와 같은 예로 등록한다.

예)

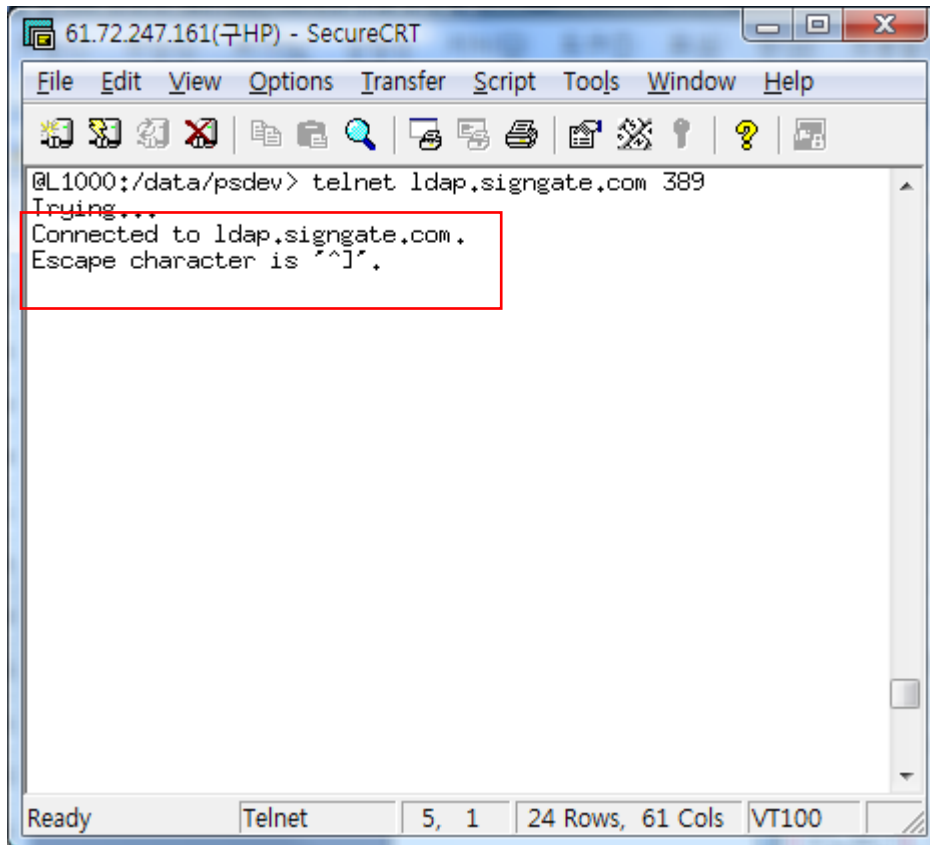
```

127.0.0.1      localhost
211.35.96.26   ldap.signgate.com
210.207.195.77 dir.signkorea.com
203.233.91.35 ds.yessign.or.kr
211.192.169.180 dir.crosscert.com
203.242.205.156 ldap.tradesign.net
    
```

- WAS서버에서 실행할 경우 등록된 LDAP 서버 연결 여부 확인 방법
  - 1) 해당 WAS서버에서 인증서 유효성 검증 서비스를 실행하는 경로에 제공하는 "portscan.jsp"를 복사한다.
  - 2) "portscan.jsp" 브라우저에서 실행하여 아래와 같이 OPEN으로 표시되는지 확인한다.
    - ※ CLOSE로 표시되는 경우 도메인명이 인식하는지 또는 389 포트를 네트워크 담당자에게 확인하시기 바랍니다.



- 서버에서 직접 Java를 실행할 경우 등록된 LDAP 서버 연결 여부 확인 방법
  - 1) 해당 서버에 telnet을 통한 설치 계정으로 로그인
  - 2) telnet 명령어로 해당 LDAP 서버 연결여부 확인
    - ex) telnet ldap.signgate.com 389



- 3) “Escape character is ‘\_`’.” 로 표시 된 경우 정상적으로 연결 성공  
 “Trying...”, “unkown host” 등의 다른 메시지 일 경우 연결 실패  
 ※ 연결 실패 시는 네트워크 관리자에게 문의하거나 **hosts**파일에 정상적으로 등록되었는지 확인함.