제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

LDAP 상호운용성 시험을 위한 시험도구 구현

김연수*, 이승희*
*인제대학교 전자정보통신공학과
e-mail : 2002b610@gurum.inje.ac.kr

The test tool implementation of LDAP interoperability test

Youn-Su Kim*, Soong-Hee Lee*
*Dept. of, Electronic and Telecommunication Engineering, INJE University

요 약

본 논문은 LDAP 클라이언트와 서버사이에서의 상호운용성 시험을 위한 시험도구 구현에 대한 것이다. 여러 벤더에 의해 구현된 LDAP 제품들을 업무에 적용하기 위해서는 상호간의 접속 운용이 가능한지를 시험하기 위한 것으로 표준적합성 시험과 함께 상호운용성 시험이 선행 되어야 한다. 이러한 시험을 위한 시험도구로 이미 구현된 것이 있으나, 이들은 OS 에 따른 설치 시 제약조건이 많으며, 시험 실행방법의 어려움과, 시험 시 시험항목 및 LDAP 서버에 저장된 데이터가 한정되어 불편한 점이 있다. 이를 보완하기위해 BLITS 를 기반으로 한 OS 의 제약이 적고, 사용자가 시험 항목을 수정 가능한 시험도구를 구현하였다. 구현한 시험도구의 타당성 검증을 위해 두 개의 LDAP 서버를 대상으로 하여 실제 상호운용성 시험을 수행 하였다. 시험 결과 203.241.249.185 의 주소를 가지는 서버는 선정된 시험항목과 사용자가 정의한 시험에 대해 모두 정상적인 시험결과를 출력하였으며, www.openldap.com 주소를 가지는 서버는 관리자 권한이 필요치 않은 항목에 대해서는 정상적인 시험결과를 출력하여 구현한 시험도구가 정상적으로 동작함을 확인하였다.

1. 서론

최근 정보사회의 도래는 행정환경에도 많은 변화를 초래하여, 온라인을 통한 비 대면 전자문서기반 환경으로 변화하고 있다. 네트웍을 통한 정부 주요 문서 및 개인 정보의 유통이 급격히 증가하게 된 것이다. 이러한 변화와 함께, 온라인 상에 노출되는 정보들에 대한 불법적인 도청, 위조, 변조 및 신분위장 등 각종 역기능에 의한 위협이 심각하게 대두되고 있다. 이러한 역기능에 대처하기 위해 정부 차원에서 공개키 암호기술을 이용하는 정부 전자서명 기반구조(GPKI : Government Public Key Infrastructure)의 조성을 꾀하고 있다. 그리고 정부 차원에서 작성한 문서인 "행정기관 전자서명 인증기반 상호 연동기술 기반" 에서는 디렉토리 서버에 접근하기 위한 프로토콜로 LDAP(Lightweight Directory Access Protocol) v3 를 제시하고 있다. 한편 국내의 여러 업체에서는 LDAP 기능을 탑재한 제품들이 출시되고 있으며 일부 업체에서는 LDAP 을 적용한 시스템 구축이 이루어지고 있다. 그 외에도 국내외적으로 디렉토리 서비스의 확산을 위해서 LDAP 기능의 경량화, 적정화, 보안대책을 강구하고 있는 LDAP v3 의 표준화 작업등이 활발히 이루어지고 있다. 그러나 여러 벤더에 의해 개발된 LDAP 기능을 탑재한 제품들을 위에서 언급한 용도로 사용하기 위해서는 표준에 적합하게 구현되었는지, 상호운용성에는 문제가 없는지 등에 대한 사전 검증이 필수적이다.

현재 국내에는 LDAP 상호운용성 및 표준 적합성시험을 위한 시스템이 구현 되어있지 않은 실정이며, 국외의 경우 Open Group, AT&T Lab, Mind Craft 등에서 시험 도구 및 시험 스위트를 제시하고 있다. 그러나 이들은 시험을 위한 비용부담이 많으며, 시험도구 설치를 위한 기반 OS(Operating System)에 따른 제약조건으로 인한 설치의 어려움이 많아 접근이 용이하지 않다[1][9][10].

그러므로 비용부담과 OS 에 따른 설치 문제를 해결하기 위해 BLITS(Basic LDAP Interoperability Test Suite)를 기반으로 하여 시험항목을 선정하고, 프로그램의

편의를 위해 Netscape Directory SDK4.0 for Java API 를 이용하여 시험도구를 구현하였다. 이렇게 구현한 시험도구의 검증을 위해 리눅스 환경에 자체적으로 구축한 LDAP 서버와 이미 구현되어 일부 데이터가 개방되어있는 LDAP 서버에 대해 상호운용성 시험을 수행하여 구현한 시험도구의 성능과 타당성을 확인하였다.

2. LDAP 상호운용성 시험

LDAP 은 RFC 2251 에 의해 정의된 표준으로 그림 1 에서 보는 바와 같이 TCP/IP 기반에서 클라이언트와 서버, 서버와 서버사이의 상호동작을 규정한 것이다.

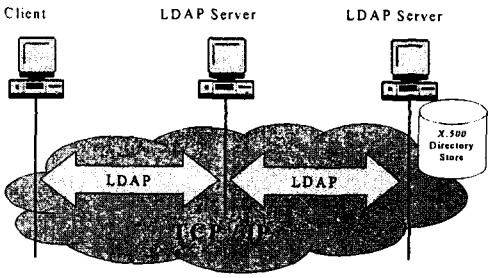

그림 1. LDAP 적용 범위

LDAP 표준은 디렉토리 서버에 간단히 읽기/쓰기 동작을 하는 관리 프로그램이나 클라이언트 어플리케이션 프로그램에 특히 적합하도록 되어있다.

LDAP 표준을 적용한 서버 및 어플리케이션 제품들이 많이 출시 되어 있지만 상호간의 접속운용 시 상이한 표준해석이나 개발접근방법의 차이 등에 의해 문제가 발생할 수 있는 소지를 안고 있다. 따라서 동일한 LDAP 표준에 의해 구현된 제품들이라도 상호간의 접속운용 시 상호운용성에 대한 시험이 우선되어야 한다.

LDAP 에 관한 시험으로는 LDAP 를 기반으로 구현한 제품의 세부적인 기능들이 RFC 문서(2251~2256)에서 기술한 표준규격의 내용과 일치하는가를 시험하기 위한 표준 적합성 시험과 여러 벤더에서 구현한 LDAP 서버의 기능을 확인하고 서버와 클라이언트 사이에서 클라이언트의 요구에 대한 서버의 응답이 올바른지를 시험하기위한 상호운용성 시험이 있다. 표준 적합성과 상호운용성 시험의 관계는 그림 2 에서 보여지듯 표준적합성 시험이 선행되어야 하며, 표준 적합성이 검증되지 않은 제품에 대한 상호운용성의 시험은 의미가 없다. 따라서 본 논문에서 구현한 시험도구의 시험대상인 두개의 LDAP 서버는 표준 적합성 시험을 완료한 것으로 가정하고 상호운용성 시험을 실시 하였다.

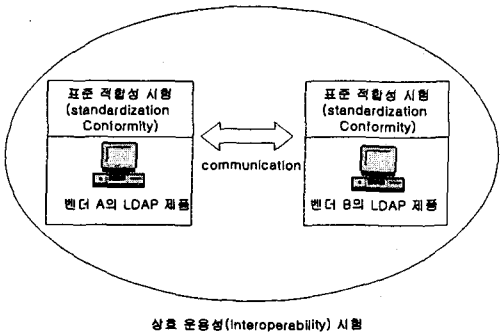

그림 2. 표준 적합성과 상호운용성의 관계

현재 구현된 표준 적합성과 상호운용성 시험을 위한 시험도구로는 OpenGroup 의 VSLDAP 과 "Security Testing of Protocol Implementation"의 프로젝트의 부산물로 나온 test suite 로 PROTOS Test Suit : c06-ldapv3 가 있다. PRPTOS Test Suit 의 경우는 총 6688 개의 Test case 가 있으며, 시험 항목은 확인을 할 수가 없다. 그리고 시험 항목으로는 AT&T Lab 에서 LDAP 클라이언트/서버 사이의 상호운용성 시험을 위해 고안한 BLITS 가 있다[9]. 현재 BLITS 는 OpenGROUP 에서 관리되며, 현재 BLITS 3.0 Test Cases 로 되어있다. 시험항목은 일반에게 개방되어 있어 누구라도 시험항목을 이용해 시험도구를 개발할 수 있다 [7].

다음은 BLITS 를 기반으로한 LDAP 상호운용성 시험도구 구현에 대해 기술 한다.

3. LDAP 시험 도구 구현

LDAP 시험도구를 구현하기 앞서 BLITS v3.0 의 시험항목 중 가장 기본이 되는 일부 시험항목을 선정하였다. 선정된 시험 항목은 표 1 에서와 같이 LDAP 클라이언트의 기본적인 동작인 Bind, Unbind, Search, Add, Modify, Delete, ModifyDN, Compare 요구에 따른 LDAP 서버의 응답에 관한 항목 중 기본이 되는 항목을 위주로 하였다.

표 1. 기본 시험 항목 선정

LDAP 동작	시험 항목
Bind/Unbind Tests	3.3.1.1 Anonymous Bind
	3.3.1.2.1 Bind With Simple Password
	3.3.1.2 Unbind
Search Tests	3.3.2.1.1 Simple Search Filters(Equality Matching)
Modify Tests	3.3.3.1.1 Modify-Add Tests (Add Value – Create Attribute)

	3.3.3.2.1 Modify-Delete Tests (Delete One Value of a Multi-valued Attribyte)
Add Tests	3.3.4.1 Add New Entry
Delete Tests	3.3.5.1 Delete Existing Object
ModifyDN Tests	3.3.6.1 Rename a Leaf Entry
	3.3.6.71 ModifyDN Errors (entry Already Exists)
Compare Tests	3.3.7.1 Comparison with FALSE Return Code
	3.3.7.2 Comparison with TRUE Return Code

BLITS 에 제시된 시험 수행 과정은 클라이언트에서 요구메시지를 생성하여 서버로 전송하고, 서버로부터의 응답을 받아 예상된 결과와 비교하여 처리하게 된다. 또한 상호운용성 시험 결과는 시험 대상인 LDAP 서버들로부터 같은 결과를 받았을 때 상호운용성이 가능한 것으로 평가할 수 있다[7].

다음으로 BLITS 에서 정의된 동작을 구현 하기 위한 프로그램 도구로 OS 의 제약이 적고, GUI 환경의 소프트웨어 구현이 쉬운 JAVA 를 이용하였다. 그리고 프로그래밍의 편의를 위해 Netscape 에서 배포한 Netscape Directory SDK4.0 을 사용하였다[8]. 이러한 개발도구를 이용하여 사용자 인터페이스 구현에 앞서 LDAP 메시지 생성과 동작 정의를 위해 LdapTest 객체를 생성하였다. 객체에 포함된 메소드는 선정한 시험 항목을 수행하기위해 메소드를 정의 하였으며, 각각의 메소드와 메소드에 정의된 인자들의 자료형은 그림 3 과 같다.

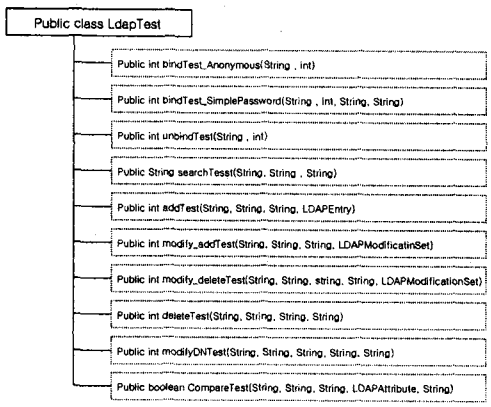

그림 3. LDAPTest 객체와 메소드

사용자 인터페이스는 그림 4 에서와 같이 각각의 시험 항목별로 나누어 탭폼으로 구성하고, 시험 결과를 출력하기 위해 결과출력 창을 두어 시험 결과를 쉽게 확인 할 수 있게 구성하였다. 그리고 메뉴바에는 시험결과를 저장하는 '저장', '새 이름으로 저장' 메뉴와 새로운 시험을 위한 '새 파일' 메뉴로 구현하였다. 그리고 시험 항목 하나하나 선택하여 시험 하지 않고 선정된 시험항목 모두를 일괄처리가 가능하게 하기위해 메뉴바에 시험 메뉴에 두었다. 마지막으로 시험도구의 전반적인 정보와 시험 방법 등의 정보를 제공하기 위해 도움말 메뉴를 구현하였다.

이렇게 구현한 시험도구를 사용하여 실제 LDAP 서버를 시험한 결과를 다음에 기술한다.

그림 4. 시험도구 사용자 인터페이스

4. 시험 결과 분석

현재 LDAP 표준을 적용한 LDAP 디렉토리 서버가 많이 출시 되어 있으나 이들 중 무료로 사용 가능한 제품은 openldap 서버가 있으며, 그 외 다른 제품은 비용을 부담해야 한다. 이런 이유로 구현한 시험도구의 시험대상을 많은 종류의 LDAP 서버를 대상으로 할 수 없었다. 따라서 본 논문에서 실시한 LDAP 상호운용성 시험은 무료로 사용 가능한 openldap 서버를 리눅스에 구현하고, BLITS 에서 정의 되어진 데이터를 저장한 서버와 이미 구현되어 일부 데이터가 공개되어 있는 www. openldap.com 의 주소를 가지는 LDAP 서버를 시험의 대상으로 선택 하였다. 시험 대상이 된 LDAP 서버 중 리눅스에 구현된 서버(203.241.249.185)는 관리자 권한을 가지고 있으며, 다른 하나는 관리자 권한을 가지고 있지 못하다. 관리자 권한의 소유 여부는 상호운용성 시험에 서 중요한 부분으로 BLITS 에서 제시된 시험항목을 수행하기 위해서는 관리자 권한을 가져야 시험이 가능하므로 Anonymous Bind, Unbind, Search, Compare 와 같이 관리자 권한이 없이 시험이 가능한 항목을 제외한 대부분의 시험 항목은 LDAP 서버의 관리자 권한을 필요로 하는 것이므로 구현한 시험 도구를 사용하여 서버를 시험하는 많은 제약이 있다. 그러나 관리자 권한을 가지고 있는 203.241.249.185 의 LDAP 서버는 구현한 도구를 통해 시험한 결과 만족할 만한 결과를 출력함을 알 수 있다.

표 2 에 나타난 결과를 보면 203.241.249.185 의 LDAP 서버는 모든 시험에서 정상완료를 하였으나,

www.openldap.com 의 주소를 가지는 LDAP 서버는 관리자 권한을 가지지 못하기 때문에 대부분의 시험에서 서버로부터 invalid Credentials 에 해당하는 LDAP resultcode 49 를 리턴함을 알 수 있다.

표 2 Ldap v3 Test 시험결과

시험 항목	203.241.249.185	www.openldap.com
Anonymous Bind	정상 완료	정상 완료
Bind With Simple Password	정상 완료	LDAP Resultcode(49)
Unbind	정상 완료	정상 완료
Simple Search Filters	정상 완료	실패
Modify-Add	정상 완료	LDAP Resultcode(49)
Modify-Delete	정상 완료	LDAP Resultcode(49)
Add	정상 완료	LDAP Resultcode(49)
Delete	정상 완료	LDAP Resultcode(49)
ModifyDN(rename a Leaf Entry)	정상 완료	LDAP Resultcode(49)
ModifyDN(entry Already Exists)	정상 완료(68)	LDAP Resultcode(49)
Compare (FALSE)	정상 완료	정상 완료
Compare (TRUE)	정상 완료	실패

Compare (FALSE) 시험의 경우 서버의 Entry 중 조건과 일치하는 Attribute 가 존재하지 않으면 LDAP 서버는 FALSE 를 리턴하게 된다.(LDAP Result code 는 32 번으로 "noSuchObject"에 해당 함) 그러나 시험도구에서 시험한 결과 www.openldap.com 서버에는 BLITS 에서 제공된 데이터가 없으므로 일치하는 Attribute 를 찾지 못하기 때문에 성공이라는 결과를 출력하게 되었다. 그러나 Compare(TRUE) 시험은 데이터가 저장되어 있지 않으므로 시험에서 실패하였다.

또한 구현한 시험도구는 사용자가 서버에 입력된 데이터를 정확히 알고 있다면 BLITS 라는 시험항목에 한정되지 않고 유연성 있는 시험이 가능하다. 예를 들어 Simple Search Filters 시험에서 BLITS 의 경우 www.openldap.com 서버에 저장된 데이터를 기반으로 Filter 를 구성하여 시험한 결과 시험결과는 정상적인 시험 결과를 출력함을 볼 수 있었다.

구현한 시험도구를 사용하여 얻은 정보를 바탕으로 하여 LDAP 서버에 대해 실제 운용 시 문제를 발생시킬 소지가 있는 부분을 미리 파악할 수 있어 제품사용 전 상호운용이 가능하게 수정 및 보완이 가능할 것이다.

5. 결론

현재 구현되어 있는 LDAP 시험도구는 시험항목의 수정이 어렵고, 시험을 위한 데이터의 제한이 있어 유연성 있는 시험이 어려우며, 많은 비용을 부담해야 한다. 이러한 단점을 보완하기 위해 시험항목의 일부를 저장되어 있는 데이터에 맞게 수정하여 시험이 가능하고, 한번의 동일한 설정으로 여러개의 서버를 동시에 시험가능한 시험도구를 구현하였다.

구현한 시험도구의 타당성은 상호운용성 시험을 수행하여 기본 시험항목 및 수정을 한 시험항목에서 모두 정상 동작함을 시험결과를 통해 확인 하였다. 그러나 구현된 시험도구는 시험항목수가 적고, 인증을 위한 정확한 기준이 제시되어 있지 않으므로 앞으로 보다 정확한 시험을 위해 많은 수의 시험항목을 수행할 수 있고, 사용하기 편리한 시험 도구의 구현이 필요하다. 또한, 상호운용성과 표준적합성 시험뿐 아니라 서버로부터의 응답시간을 이용하여 서버의 성능을 함께 시험할 수 있는 도구가 구현된다면 상호 접속 운영에 있어 많은 도움이 될 것으로 사료된다. 또한 시험도구 개발에 앞서 표준적합성 및 상호운용성 시험을 위한 시험항목의 개발과, 시험결과에 대해 인증 조건을 명확한 정의가 선행 되어야 할 것이다.

참고문헌

[1] M. Wahl, et. al. "Lightweight Directory Access Protocol(v3)", IETF RFC 2251, 1997

[2] M. Wahl, et. al. "Lightweight Directory Access Protocol(v3): attribute Syntax Definitions" IETF RFC 2252, 1997. 12

[3] M. Wahl, et. Al. "Lightweight Directory Access Protocol(v3): UTF-8 string Representation of Distinguished Naves" IETF RFC 2253, 1997. 12

[4] T. Howes, "The String Representation of LDAP Search Filters" IETF RFC 2254, 1997. 12

[5] T. Howes, M. Smith, " The LDAP URL Format" IETF RFC 2255, 1997. 12

[6] T. Howes, "The String Representation of LDAP search Filters" IETF RFC 1960, 1996. 7

[7] The Open GROUP, "BLITS 3.0 Test Cases" 2003. 4. 14 http://www.opengroup.org/dif/blitspub/blits3.0/cases.htm#1.

[8] Netscape Directory SDK 4.0 for Java Programmer's Guide

[9] 이승희, "LDAP 기술 및 동향 분석", 전자문서유통체계 개선방안 소과제, 2001.11.

[10] 이승희, "LDAP 시험 방법 및 시험도구 분석", 전자문서유통체계 개선 방안 소과제, 2002,03