SSO(Single Sign-On)체제 구축을 위한 웹 사이트 회원정보와 LDAP(Lightweight Directory Access Protocol)정보 동기화

천인혁° 이태석 이상환 김남근 신기정
한국과학기술정보연구원
{sorisera°, tsyi, sanglee, bio, kjshin}@kisti.re.kr

Synchronization of the LDAP(Lightweigth Directory Access Protocol) information with web site member information for a SSO(Single Sign-On) setup

Inhyeuk Cheon° T.S. Yi S.H. Lee N.G. Kim Kijeong Shin
Korea Institute Science and Technology Information

요 약

공공 부문이나 대기업에서 운영하는 웹 사이트의 규모가 커지면서 분야별로 사이트가 나누어지게 되는데, 사이트를 이동할 때 마다 로그인을 다시 해야 하는 불편이 있다. 따라서 최근 이용자들의 불편을 줄이기 위하여 SSO(Single Sing-On) 통합인증 체제를 도입하는 사례가 늘고 있다. 통합 인증 시스템을 구축하면서 다수 웹 사이트의 회원을 통합하고 이에 대한 회원 정보 DB를 구축하여야 하는데, 빠른 인증서비스를 위해서 LDAP(Lightweight Directory Access Protocol)를 사용하는 것이 일반적이다. 이때 회원정보 DB와 LDAP의 정보에 대한 동기화 문제와 웹 사이트를 통한 회원가입과 동시에 적용되어야 하는 요구사항을 만족시키기 위해 본 논문 에서는 회원 정보 DB와 LDAP의 정보 사이의 동기화 방법을 제안하고 구현하여 그 성능을 분석 하였다.

1. 서 론

웹 사이트의 회원제 서비스가 공공부문이나 민간부문에서 운영하는 웹 사이트의 규모가 커지면서 세부 분야별로 사이트가 나누어지게 되어 있어서 이용자들의 등록과 인증의 불편을 줄이기 위하여 SSO(Single Sign-On) 통합인증 체제를 도입하는 사례가 늘고 있다.

일반적인 인터넷 사용자는 웹 사이트마다 반복되는 등록 절차를 매우 번거롭게 생각하고 있다. 여러 군데 등록해 두었기 때문에 주소 변경 등도 여러 군데에서 수행해야 한다. 또한 각 사이트의 ID와 패스워드를 암기하는 것이 매우 어렵기 때문에 보통 동일 ID와 패스워드를 사용하거나 패스워드를 메모해 두게 되는 이는 보안상 큰 문제가 아닐 수 없다[1].

통합 인증 시스템을 구축하면서 다수 웹 사이트의 회원을 통합하고 구축하기 위해 빠른 인증서비스를 위해서 LDAP(Lightweight Directory Access Protocol)을 사용하는 것이 일반적이다. 그러나, 대용량 및 다수의 사이트인 경우 회원정보 DB와 LDAP의 정보에 대한 동기화 문제가 발생하는데, 이를 해결하기 위하여 기존에는 배치작업으로 동기화하였지만 웹 사이트를 통한 회원가입과 동시에 실시간으로 적용되어야 하는 요구사항을 만족 시킬 수는 없다.

따라서, 이러한 문제를 해결하기 위해 본 논문 에서는 회원 정보 DB와 LDAP의 정보 사이의 동기화 방법을 제안하고 구현하여 그 성능을 분석 하였다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구에 대해여 기술하고, 3장에서는 SSO 통합인증 회원 DB와 LDAP 정보간 동기화 방안에 대하여 제시하고, 4장에서는 제시한 방안에 대하여 성능 테스트 및 평가하였고, 5장에서 결론과 향후 연구방안에 대하여 기술한다.

2. 관련연구

2.1 SSO(Single Sign-On)

SSO(Single Sign-On)는 한번의 로그인을 통해 모든 서버에 접속할 수 있는 권한을 갖게 되는 개념이다. SSO 시스템의 일반적인 구성은 local authentication, credentials, service로 구성된다[2, 3].

특히, 디렉토리 시스템인 LDAP 서버를 중심으로 인증서를 CA에서 받는 방식으로 응용프로그램과 SSO 서버 사이의 API 메커니즘을 이용한 여러 가지 구현 시스템들이 나오고 있다. SESAME(A Secure European System for Applications in a Multi-vender Environment), Netscape, Suitspot, Novell 등에서 SSO 모델을 제시하고 있다[6, 7].

그림 1은 기존 시스템 환경과 SSO를 적용한 시스템을 비교한 SSO 개념도이다.

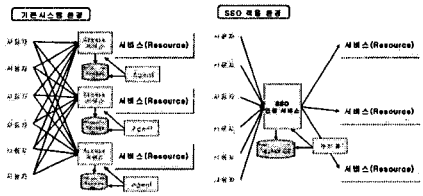

그림 1 SSO(Single Sign-On) 개념도

2.2 LDAP(Lightweight Directory Service Protocol)

LDAP은 모든 형태의 디렉토리형 자료를 표준화된 방식으로 저장하고 검색하기 위한 통신규약으로서 미국 미시간 대학에서 ITU-T의 X.500을 근거로 개발되었다[4, 9]. LDAP은 X.500을 기반으로 개발된 통신규약이며, X.500은 인터넷 사용이 가능한 곳이라면 전 세계 어디에서라도 이용이 가능하도록 나라, 기관, 사람, 기계 등과 같은 객체들을 관리하고 정보를 제공하는 디렉토리 서비스 표준이다[5, 8].

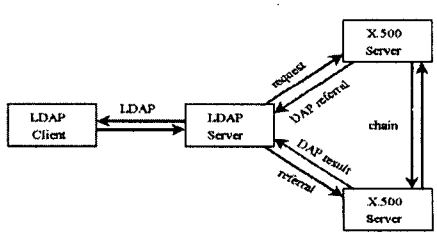

그림 2 LDAP 계층도

3. 회원정보 DB와 LDAP 동기화 방안

3.1 회원정보 DB와 LDAP 동기화 처리 개념도

회원정보 DB와 LDAP의 정보 간의 동기화가 필요한 상황은 단지 웹 사이트에서만 필요한 것이 아니라 클라이언트/서버 프로그램이나 관리자가 데이터베이스 관리 도구를 사용해서 회원정보를 변경하였을 경우에도 필요하다.

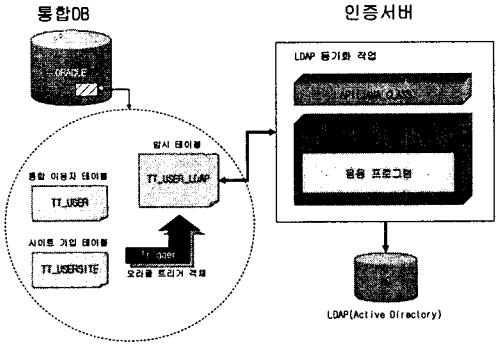

그림 3 LDAP 동기화 프로그램 처리 개념도

그림 3은 LDAP 동기화 프로그램의 처리 개념도를 나타낸 것이다. 우선 LDAP 동기화에 필요한 데이터는 통합 이용자 테이블(TT_USER)과 사이트 가입 테이블(TT_USERSITE)에서 인증과 사이트 접속권한에 필요한 컬럼들을 오라클 트리거를 이용해서 임시테이블(TT_USER_LDAP)에 저장하는 방식을 채택하였다.

임시테이블에는 이용자 또는 관리자가 통합회원 정보의 변경시(회원가입, 탈퇴, 수정 등) 데이터가 저장된다. 임시테이블에 저장된 데이터를 LDAP에 반영하는 역할은 인증서버 측의 웹 프로그램이나 응용 프로그램에서 하게 된다.

3.2 API를 이용한 회원정보 DB와 LDAP 동기화 해결

LDAP 동기화를 위해 본 연구에서는 웹 프로그램에서 API를 이용하는 응용프로그램으로 처리하고자 한다.

실시간(real time)으로 이용자 정보를 LDAP에 동기화하는 방식으로 하기 위해 인증서버 측의 서비스 플랫폼을 JAVA 기반의 네이밍 서비스(Naming Service)API를 이용하였다. 이용자가 통합 회원에 가입하는 상황을 예로 들어 처리 구조를 설명하면 다음과 같다.

이용자가 회원에 가입하면 TT_USER 테이블에 회원정보가 저장되고 오라클 트리거가 작동하여 TT_USER_LDAP에 인증에 필요한 회원 기본정보를 저장한다. 웹 프로그래밍에서는 이용자 가입 처리가 끝나면 LDAP 동기화 처리 API를 호출한다. LDAP 동기화 처리 API에서는 이용자 ID로 TT_USER_LDAP 테이블에서 관련 데이터를 검색하고, LDAP에 반영하고 난 후 임시테이블에 있는 데이터를 지우는 방식으로 처리하고 있다.

응용 프로그램 방식은 TT_USER_LDAP 테이블에 미처리 데이터가 남아 있는 경우 응용 프로그램 방식으로 운용하여 통합DB와 LDAP간의 데이터 보정작업을 할 때 이용한다.

표 1 API를 이용하는 응용프로그램 방식 프로퍼티

```
[ORACLE DATABASE]
#TT_USER_LDAP 테이블의 데이터 건수에1을 더한 수를 지정한다
ORA_MAXROWNUM = 21
[Timer Thread]
#한번 처리하고 응용 프로그램을 종료함
PROCESS_COUNT = 1
INITIALDELAY = 0
#5 * 1000(1 millisecond) = 5 sec
SUBSEQUENCERATE = 5000
SERVER_APPLICATION=FALSE
```

3.3 회원정보 DB와 LDAP 동기화 처리 클래스

회원정보 DB와 LDAP 정보간의 동기화를 처리하는 클래스는 5개의 클래스로 처리하며, 각 해당 클래스간의 관계를 클래스 다이어그램으로 설명하고자 한다.

- SyncUserData.java : 메인(main) 클래스
- LdapUtil.java LDAP : 연동 관련 클래스
- PropertyLoader.java : 프로퍼티 파일 관련 클래스
- SyncLDAP.java : 벌크로딩 관련 클래스
- SyncLdap.properties : 프로퍼티 파일

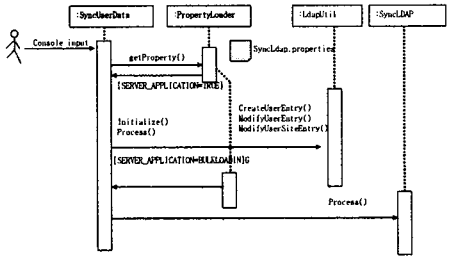

그림 4 동기화 클래스 다이어그램

그림 4는 동기화를 수행하는 클래스 다이어그램이며, 그 설명은 표 2와 같다.

표 2 동기화 처리 클래스 처리순서 및 메소드

구분	내 용(클래스명.메소드명)
클래스 처리 순서	1. 콘솔에서 프로그램을 실행한다(SyncUserData). 2. 프로그램은 프로퍼티 파일을 읽어 들이고 PropertyLoader.getProperty의 속성값을 확인한다. 3. 프로퍼티 파일이 데몬 프로그램으로 설정되어 있으면 데몬 프로그램으로 처리한다 4. 프로퍼티 파일이 벌크로딩 프로그램으로 설정되어 있으면 벌크로딩 프로그램으로 처리한다.
메소드	◦SyncUserData.Initialize : 오라클 데이터베이스 연결하고 쓰레드를 초기화하는 메소드 ◦SyncUserData.Process : LDAP에 동기화 작업을 하는 메소드 ◦SyncLDAP.Process : 벌크로딩을 작업을 하는 메소드 ◦LdapUtil.CreateUserEntry : 이용자 정보를 LDAP에 저장하는 메소드 ◦LdapUtil.ModifyUserEntry : LDAP에 있는 이용자 정보를 수정하는 메소드 ◦LdapUtil.ModifyUserSiteEntry : 이용자 사이트 가입 정보를 저장 및 수정하는 메소드

4. 평가 및 결과

4.1 실험환경 및 방법

SSO 회원 DB와 LDAP의 정보 사이의 동기화 Loading Test를 위한 시스템 실험환경은 WINDOWS 2003서버와 오라클 8i이고, 소프트웨어 환경은 LDAP동기화프로그램, JDK 1.4.x, ActiveX 에이전트로 구성하였으며, 그림 5와 같다.

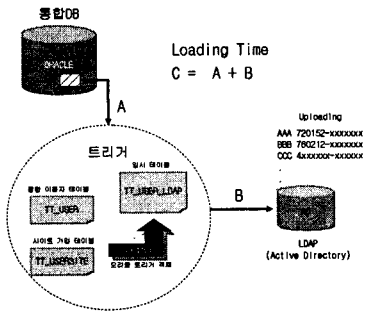

그림 5 동기화 실험 구성도

실험방법은 실시간으로 웹 페이지에서 동시 등록 및 수정을 통해 SSO 회원 DB와 LDAP의 정보 사이의 동기화 테스트와 Loading Test를 일반적인 벌크방식과 제안한 API방식에 대한 실험을 수행하였다.

4.2 평가 결과

SSO 회원 총 28만명 중 표본 샘플 총 10000명의 데이터를 가지고 BULK방식과 API방식으로 LOADING TEST를 실시한 결과 다음과 같은 결과를 얻었다.

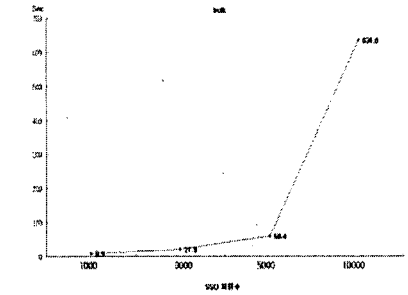

그림 6 벌크방식 로딩 테스트 결과

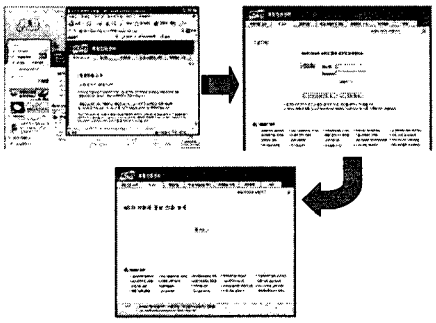

그림 7 벌크방식 회원 동기화 테스트

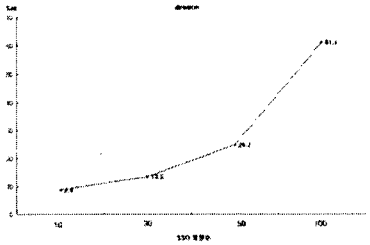

그림 8 API방식 로딩 테스트 결과

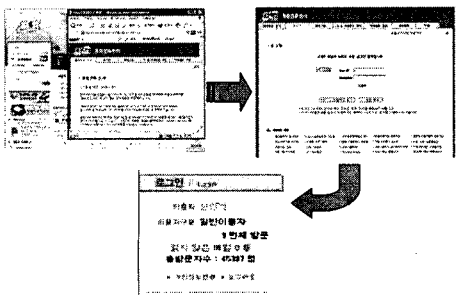

그림 9 API방식 동기화 테스트 결과

상기 결과로 Loading Time은 Bulk방식이 API방식보다 상대적으로 빨랐으나, 회원가입과 동시에 실시간(real time)으로 인증하는 부분에서 실패하였음을 보았다. 그러나, 본 논문에서 제안한 API방식에서는 Bulk에 비해 로딩시간이 느렸지만 실시간으로 인증 테스트에서 성공하였다.

따라서, 벌크방식이 회원통합 DB와 LDAP DB 간의 동기화 테스트 부분에 동기화 되지 않음을 확인 할 수 있었으며, API방식이 로딩시간과 편차가 크지만 동기화 테스트 결과 동기화됨을 알 수 있었다.

5. 결론

웹 사이트의 회원제 서비스가 공공부문이나 민간부문에서 운영하는 웹 사이트의 규모가 커지면서 세부 분야별로 사이트가 나누어지게 되어 있어서 이용자들의 등록과 인증의 불편한 문제점은 KISTI 패밀리 사이트에서도 마찬가지이다.

KISTI에서 운영하고 있는 20 여 개의 패밀리 사이트가 있지만 서로 같은 이용자에 대해 중복 정보를 보유하고 있으며, 이들 회원 정보들을 효율적인 관리와 운영에도 문제가 발생하였다. 이러한 문제들을 해결하기 위해 위하여 LDAP기법을 이용한 SSO(Single Sign-On) 통합인증 체제를 구현하였다.

그러나, KISTI와 같은 대용량, 다수사이트를 단일 인증체제로 통합하여 실시간으로 회원가입과 동시에 인증한 사례가 없었다. 따라서, 본 연구에서 회원 통합 DB와 LDAP DB간 실시간(real time)으로 동기화 문제를 해결하기 위해 API방식을 제안하였다.

API방식으로 가입과 동시에 실시간으로 이용자 정보를 인증되는 결과를 보였고, 대용량 일괄(batch) 회원 통합 작업이나 갱신작업시에는 Bulk 방식을 활용하고 회원인증시 동기화 부분에서는 API방식을 적용하여 효율적인 관리와 운영이 가능하였다.

향후 연구방안으로 제안한 API방식의 실시간으로 로딩시간을 개선하는 알고리즘과 방안이 필요하다.

[참고문헌]

[1] Daeseon Choi, Sangrae Cho, Seunghun Jin, Kyoil Chung, "An Information Security Model for the next Generation Application Service", IWA2002, Taiwan, October 2002.
[2] J. Hursi, "Unified Single Sign-On", Proceedings of the Helsinki University of Technology Seminar on Network Security Fall 1998.
<http://www.tml.hut.fi/Opinnot/Tik-110.501/1998/papers/3singlesignon/singlesign-on.htm>
[3] P. Carden, "The New Face of Single Sign-On", 1999.
<http://www.networkcomputing.com/1006/1006f1.html>
[4] W. Yeong, T. Howes, S. Kille, "Lightweight Directory Access protocol", RFC1777, 1995. 3.
[5] W. Yeong, T. Howes, S. Kille, "X.500 Light-weight Directory Access Protocol", RFC1487, 1993. 7.
[6] White Paper, "Windows 2000 Kerberos Interoperability", Microsoft.
[7] X/Open Single Sign-On Service(XSSO)-Pluggable Authentication Modules, The Open Group, 1997.
[8] 정진원, "디렉토리 서비스의 핵심 기술 'LDAP'", Network Times, 2001.
[9] 최진주, "LDAP 프로토콜에 대한 고찰", 한국통신정보보호학회 3, v9, 1999.