ANALISIS DAN PERANCANGAN ARSITEKTUR SISTEM OTENTIKASI TERINTEGRASI ANTARA PLATFORM LINUX, WINDOWS 2000, DAN NOVELL NETWARE: STUDI KASUS JURUSAN TEKNIK INFORMATIKA FTIF ITS

Rully Soelaiman, I Wayan Widi Pradnyana, dan Wahyu Suadi
Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember
Kampus ITS, Jl. Raya ITS, Sukolilo – Surabaya 60111, Tel. + 62 31 5939214, Fax. + 62 31 5913804
Email: rully@its-sby.edu

ABSTRAK

Jurusan Teknik Infomatika merupakan suatu organisasi yang menggunakan jaringan komputer yang diakses dari beberapa domain dan menggunakan sistem operasi terpisah. Masing-masing sistem tersebut menggunakan pengelolaan autentikasi yang terpisah, dengan kenyataan bahwa seharusnya dapat diakses oleh setiap anggota organisasi ini. Kebutuhan pengguna dan pengelola jaringan akan efisiensi pemakaian informasi autentikasi menjadi permasalahan yang akan dibahasa dana makalah ini.

Pada makalah ini, dilakukan analisis kemungkinan dilakukannya otentikasi terintegrasi pada jaringan komputer Teknik Informatika yang menggunakan Windows 2000, Linux, dan Novell Netware. Analisis dilakukan dengan meninjau kemampuan integrasi direktori, metode otentikasi, dan kerjasama dengan sistem lain. Dari hasil pemetaan terhadap kebutuhan dan ketersediaan sumber daya teknologi pada jurusan, dipilih solusi otentikasi menggunakan Samba dan OpenLDAP untuk melayani permintaan otentikasi dari Windows 2000 dan Linux.

Uji coba telah dilakukan untuk otentikasi client Windows 2000 dan Linux , mencakup login dari masing-masing sistem operasi, domain yang berbeda, menggunakan satu username dan password. Uji coba juga dilakukan terhadap proses pemeliharaan sistem oleh administrator sistem.

Kata Kunci : *identity management, system integration, centralized authentication, Samba, OpenLDAP.*

1. PENDAHULUAN

Dalam jaringan komputer Jurusan Teknik Informatika FTIF ITS, terdapat pelbagai macam layanan jaringan dengan beberapa domain dan dengan beberapa sistem operasi, yaitu Windows 2000 Server, Unix/Linux, Novell Netware. Ketiga jenis sistem operasi tersebut memiliki karakterstik yang berbeda dalam hal melakukan pengaturan kemanan sumber daya.

Sistem yang sekarang sedang berjalan tidak menggunakan layanan otentikasi bersama, sehingga menimbulkan ketidakefisienan bagi administrator jaringan maupun pengguna umum.

Dari keterbatasan dan kurang efisiennya sistem di atas, maka diperlukan sebuah arsitektur sistem otentikasi terintegrasi bagi sistem jaringan yang menggunakan sistem berbasis Linux, Windows 2000, dan Novell Netware. Proses integrasi otentikasi ini mencakup: penentuan kebutuhan, perancangan arsitektur, pengimple-mentasian arsitektur.

2. SISTEM OTENTIKASI JURUSAN TEKNIK INFORMATIKA DAN MANAJEMEN IDENTITAS

Jaringan komputer di Jurusan Teknik Informatika FTIF ITS yang terdiri atas beberapa domain dan menggunakan beberapa sistem operasi, diantaranya yaitu: domain Ajk-Lab, domain Lab-Prog, domain Sisfo, domain Lab-RPL, domain Lab-Komputing, domain Lab-Ext, domain PascaSarjana, domain Dosen dan Karyawan.

Masing-masing domain tersebut meng-gunakan kombinasi antara komputer client berbasis Windows 2000 yang menggunakan Microsoft Windows 2000 Advanced Server dengan Active Directory sebagai domain controller dan server otentikasi, komputer Netware Client pada Windows 2000 yang memakai Novell NDS sebagai server otentikasi dan server direktori, dan client Linux yang menggunakan otentikasi lokal sendiri.

Pengguna dari sistem jaringan komputer yang ada pada Jurusan Teknik Informatika ini terbagi menjadi dua kelompok besar, yaitu: pengguna umum dan pengelola jaringan.

Pengguna umum yaitu anggota tidak secara aktif melakukan konfigurasi pada sistem, diantaranya :

1. Mahasiswa.
2. Dosen.
3. Karyawan.
4. Pengguna lain (*Miscelanous*).

Sedangkan pengelola jaringan berhak melakukan perubahan pada sistem ini yaitu:

1. Administrator utama, adalah administrator pusat mengelola keseluruhan sumber daya yang ada sistem jaringan komputer.
2. Administrator , yang berhak mengelola *user* yang melakukan akses *login* pada sistem.
3. Administrator domain, yang mengelola domain jaringan serta membuat hubungan kerjasama dengan domain lain .
4. Administrator komputer lokal, yang hanya berhak mengelola sistem komputer lokal atau *workstation*.

Berdasarkan terpisahnya pengelolaan *account user* untuk masing-masing domain dansistem operasi tersebut, maka dibutuhkan sebuah sistem khusus yang memungkinkan melakukan pengaturan proses login pada jaringan tersebut.

Untuk melakukan fungsinya masing-masing, masing-masing jenis pengguna memiliki proses-proses berbeda yang dilakukan dalam hubungannya dengan mengakses informasi yang ada pada jaringan.

Teknologi manajemen identitas bertujuan untuk mempermudah pengelolaan dari data yang tersebar, bertumpuk, dan kadang tidak sama menjelaskan informasi pemakai (*user*) dalam sebuah sistem. [4]

Manajemen identitas terdiri atas 6 komponen penyusun yaitu:

1. Arsitektur Informasi Organisasi (*Organization's System Architecture*), yaitu untuk memahami kebutuhan dan struktur bisnis dari sebuah organisasi
2. Manajemen hak dan ijin (*Permission and Policy Management*), yaitu untuk menentukan pihak-pihak yang berhak mengakses informasi
3. Layanan Direktori Organisasi (*Enterprise Directory Service*) mencakup proses analisis, perencanaan, dan integrasi direktori.
4. Otentikasi *User*, untuk memastikan identitas dari *user*, sehingga akses *user* terhadap sumber daya dapat dikelola.
5. Penyediaan *User* (*User Provisioning*), untuk mengimplementasikan hak akses anggota berdasarkan kebijakan organisai.
6. Alur proses (*Workflow*), yang akan memicu penambahan dan perubahan pada aplikasi dan informasi lain.

Sebuah sistem manajemen identitas memiliki kemampuan atau fungsi-fungsi dalam tujuannya untuk mempermudah pengelolaan identitas dalam suatu organisasi, [8] diantaranya yaitu:

1. Reset Password, untuk melakukan *reset password user* tanpa melibatkan banyak peran *help desk*.
2. Sinkronisasi Password, yaitu pemakaian satu pasword untuk melewati beberapa sistem yang berbeda
3. *Single Sign-On* (SSO), yaitu untuk dapat sekaligus mengakses aplikasi dan sistem menggunakan satu proses login.
4. Software Manajemen Akses, yaitu penggunaan aplikasi untuk melakukan pengelolaan identitas.

Otentikasi adalah proses pembuktian identitas pada informasi identitas yang dimiliki oleh layanan pembukti identitas.

Berdasarkan arah pembuatan otentikasi, terdapat dua jenis model otentikasi, yaitu *server-authentication* dan *client-authentication*.

Client-authentication hanya menggunakan peran aktif *client*, daripada *server-authentication* yang juga membutuhkan peran server yang mengotentikasikan dirinya ke client.

Terdapat dua jenis *client authentication*, yaitu *basic authentication*, dimana *user* harus menyediakan password baru untuk setiap server, serta administrator harus mengatur informasi dari nama dan *password* dari sertiap *user*, dan s*trong authentication* yang menggunakan *certificate* dan digunakan untuk mendukung Single Sign-On.

Layanan direktori merupakan penyusun utama timbulnya manajemen identitas karena memiliki struktur yang dapat mencerminkan keadaan struktur hirarki dalam dunia nyata.

Direktori adalah kumpulan dari sistem yang bekerja sama untuk menyimpan basis data lojik dan struktural dari sebuah informasi mengenai sekumpulan obyek dalam dunia nyata. [1]

Berikut ini merupakan fitur-fitur yang harus dimiliki oleh sebuah produk yang menggunakan direktori atau LDAP. [5]

1. *Information Model*, berisi informasi mengenai obyek dunia nyata. Informasi yang melambangkan sebuah obyek disimpan dalam sebuah *entry*
2. *Naming Model*, yaitu masing-masing *entry* dikenali dengan sebuah *Distinguished Name* (DN)
3. *Functional Model*, yaitu bagaimana informasi diakses dalam direktori, mencakup.: *interrogation, modification, authentication and control.*
4. *Distribution Model*, yaitu kemampuan direktori dapat melakukan replikasi.

Berikut ini adalah beberapa model arsitektur untuk replikasi direktori yang diatur dalam standar replikasi, yaitu.

1. *Single Master Model*, yaitu hanya satu sumber sebagai acuan untuk replikasi direktori oleh beberapa server lain sebagai *slave server*.
2. *Dual Master Model*, menggunakan dua master server pada slave server dan distribusi informasi hanya oleh satu master.
3. *Pseudo Multi Master Model*, menggunakan satu koordinator replikasi dari banyak master.
4. *Multi Master model*, yaitu untuk sebuah slave server yang memiliki lebih dari satu *master server* berbeda.

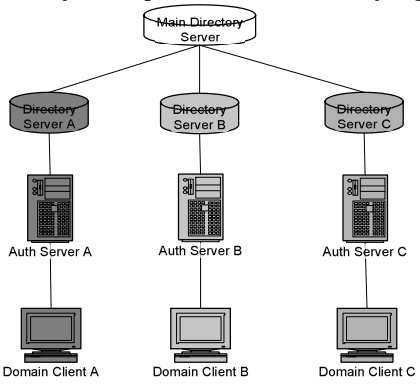
3. SISTEM OTENTIKASI TERINTEGRASI

Sebuah sistem otentikasi terintegrasi terbentuk dari beberapa permasalahan dan kebutuhan dari elemen-elemen dalam sebuah organisasi yang menggunakan jaringan komputer, yaitu:

1. Latar belakang yang menjadi faktor untuk dibuatnya otentikasi teritegrasi yaitu terdapatnya beberapa sub sistem dari sistem otentikasi pada jaringan komputer,yang memiliki proses atau metode otentikasi yang berbeda-beda dan sering terjadi kerjasama atau pertukaran informasi *sharing* antara sistem tersebut.
2. Kebutuhan pengguna, yang menganggap kondisi otentikasi terdistribusi yang ada adalah kurang efieisen dan efektif.
3. Syarat sistem yang harus dipenuhi yaitu dalam keterkaitannya dengan organisasi pengguna jaringan tersebut, antar komponen dan metode komunikasi dalam jaringan tersebut.

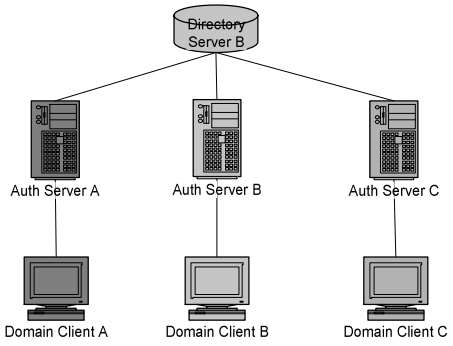
Beberapa macam solusi arsitektur untuk dapat merancang otentikasi terintegrasi antar platform yaitu:

1. Kerjasama direktori otentikasi, yaitu tersusun dari beberapa direktori yang melakukan kerjasama pertukaran informasi yang dimiliki.



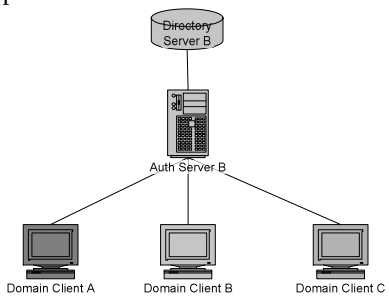
Gambar 1. Integrasi server direktori

2. Server direktori tunggal, yaitu satu buah server direktori akan melayani permintaan pembacaan informasi otentikasi dari beberapa server otentikasi.



Gambar 2. Server direktori tunggal

3. Server otentikasi tunggal, yaitu hanya terdapat satu server otentikasi yang menyediakan layanan otentikasi untuk beberapa jenis platform komputer client.



Gambar 3. Server otentikasi tunggal

Berikut tinjauan teknologi otentikasi yang digunakan pada jaringan komputer Jurusan Teknik Informatika FTIF ITS.

1. Otentikasi dan direktori pada linux
   Proses otentikasi pada jaringan Linux terdapat beberapa metode atau model otentikasi, yaitu : PAM, Kerberos, LDAP, Samba. OpenLDAP sebagai sebuah teknologi direktori pada Linux, memiliki beberapa fitur dalam implementasinya terhadap standar yang ditetapkan oleh RFC. Proses otentikasi pada Linux yang menggunakan Samba atau OpenLDAP menggunakan obyek-obyek user, samba, dan komputer untuk melakukan pencarian dan perbandingan pada direktori. [9] [10]
2. Otentikasi dan Direktori Pada Windows2000
   Dalam proses otentikasi, Windows 2000 mendukung *single sign-on*. Windows 2000 menggunakan 2 protokol dasar untuk melakukan otentikasi *user* melalui jaringan, yaitu dengan Kerberos dan NTLM. Windows 2000 menggunakan Microsoft Active Directory Server sebagai server direktori. Produk ini menggantikan domain model dalam Windows NT4.0 dan menggunakan data model dan konsep dari X.500. *Object User* pada Active Directory dibangun dari obyek-obyek*: Users, Mail Recipient, Person, Organizational Person, Security Principal.* [7]
3. Otentikasi dan Direktori Pada Novell Netware
   Proses otentikasi pada Novell Netware Client dan Novell Netware Server menggunakan Novell NDS, adalah menggunakan informasi tree, context, dan Novell Server, serta protokol NCP pada saat proses login. Pada tahun 1997 Novell menambahkan komponen *LDAP services for NDS*, pada paket instalasi server Novell Netware yang memungkinkan pengaksesan dari dan melalui server LDAP lain. [6]

Berikut ini pemetaan masing-masing solusi yang mungkin dilakukan untuk membuat sistem otentikasi terintegrasi dengan kondisi yang ada pada jaringan komputer Jurusan Teknik Informatika.

1. Belum dapat dilakukan integrasi direktori antara semua sistem, namun integrasi direktori tersebut dapat dilakukan secara parsial, antara Active Directory dengan OpenLDAP, atau Novell NDS dengan OpenLDAP.

Tabel 1. Pemetaan integrasi antar direktori

Integrasi antar produk	NDS 4	NDS 7.0	NDS 8.6	AD	Open LDAP
NDS 4	-	Tidak	Ya	Tidak	Tidak
NDS 7.0	-	-	Ya	Tidak	Tidak
eDirectory 8.6	-	-	-	Ya	Ya
Active Directory	-	-	-	-	Ya
Open LDAP	-	-	-	-	-

2. Untuk sentralisasi server direktori, dapat diambil beberapa kemungkinan yaitu:
   a. Novell NDS dapat menjadi server direktori tunggal untuk client Novell Windows dan Linux,
   b. Active Directory dapat menjadi server direktori tunggal yang melayani permintaan otentikasi dari client Linux dan Windows.
   c. OpenLDAP dapat menjadi server direktori tunggal yang melayani permintaan otentikasi dari Windows 2000 dan Linux

Tabel 2. Pemetaan server direktori dan sever otentikasi

DirSvr / AuthSvr	NDS 4	NDS 7.0	NDS 8.6	AD	Open LDAP
NW 4	Ya	Ya	Ya	Tidak	Tidak
NW 5	Tidak	Ya	Ya	Tidak	Tidak
NW 6	Ya	Ya	Ya	Tidak	Tidak
W2k Svr	Tidak	Tidak	Tidak	Ya	Tidak
Open LDAP	Tidak	Tidak	Ya	Ya	Ya
Samba	Tidak	Tidak	Ya	Ya	Ya

3. Sentralisasi server otentikasi, kemungkinan yang dapat dilakukan untuk melakukan integrasi otentikasi dengan menggunakan satu server direktori dan satu server otentikasi
   a. Novell Netware dapat menjadi server otentikasi bagi client Netware baik Windows 2000 dan Linux
   b. Windows 2000 Server dapat menjadi server otentikasi bagi client Windows 2000 dan Linux.
   c. OpenLDAP dapat menyediakan layanan otentikasi pada workstation Linux dan Windows 2000.
   d. Samba dapat menyediakan layanan otentikasi bagi komputer dengan Windows 2000 dan Linux

Tabel 3.
Pemetaan server otentikasi dan client otentikasi

AuthSrv / Client	NW 4	NW 5	NW 6	W2k Server	Open LDAP	Samba
W2k /XP	Ya	Ya	Ya	Ya	Ya	Ya
Linux	Ya	Ya	Ya	Ya	Ya	Ya

4. PERANCANGAN DAN IMPLEMENTASI SISTEM

Berdasarkan masing-masing solusi pada pembahasan sebelumnya dan terhadap ketersediaan teknologi yang dimiliki pada Jurusan Teknik Informatika Fakultas Teknologi Informasi, berikut dilakukan pemetaan untuk memilih solusi:

Tabel 4. Pemetaan teknologi yang dimiliki pada Jurusan Teknik Informatika

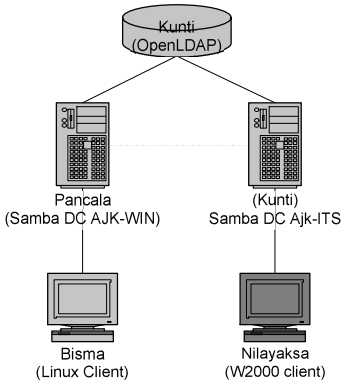
	Versi	Lisensi	Tersedia
Server Direktori			
Novell NDS	4	500 *User*	Ya
	7.0	3 *User*	Demo
	8.5	---	Tidak
Active Directory	2000	Tidak terbatas	Ya
OpenLDAP	2.1.22	Tidak terbatas, gratis	Ya
Server Otentikasi			
Novell Netware	5	3 *User*	Demo
	6	--	Tidak
Windows 2000 Server	2000	Tidak terbatas	Ya
Samba	3.0.0	Tidak terbatas, gratis	Ya

Beberapa kesimpulan untuk solusi sistem otentikasi terintegrasi pada Jurusan Teknik Informatika Fakultas Teknologi Informasi, yaitu:

1. Solusi yang menggunakan Client Novell Netware dan NDS yang didukung, belum dapat dicoba karena aplikasi tersebut dimiliki.
2. Selain solusi yang menggunakan Windows 2000 Server, solusi yang menggunakan Samba dengan OpenLDAP merupakan salah satu solusi yang menarik dan cukup layak untuk diimplementasikan karena bisa diperoleh untuk yang paling baru secara gratis.

Berikut ini perancangan terhadap satu solusi rancangan arsitektur sistem otentikasi terintegrasi pada Jurusan Teknik Informatika FTIF ITS.

1. Topologi sistem. Aplikasi yang digunakan adalah server OpenLDAP sebagai server direktori, Samba menjadi pengatur proses otentikasi, Linux client dan Windows 2000 menjadi client.



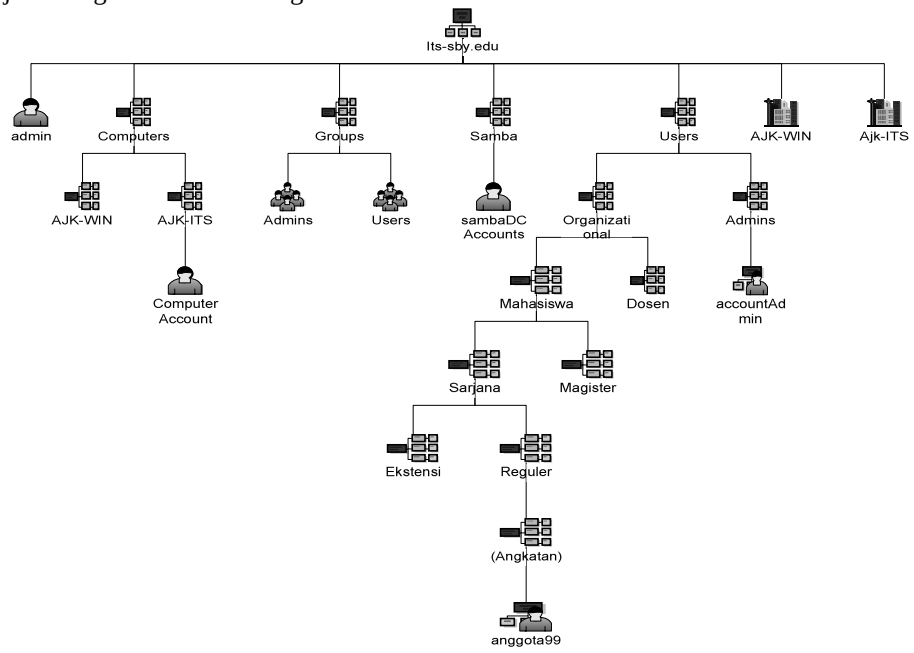
Gambar 4. Topologi sistem

1. Arsitektur proses. Beberapa langkah yang dilakukan untuk masing-masing proses dalam rancangan sistem ini yaitu : pada client Linux dan Windows 2000 terdapat beberapa proses yaitu proses login dari workstation, proses akses sumber daya, proses perubahan password.
2. Sedangkan pada domain controller terdapat proses pelayanan otentikasi, pendaftaran komputer.Pada server direktori terdapt pemeliharaan sistem direktori, termasuk pengaturan *account user*.
3. Arsitektur direktori. Arsitektur direktori yang akan dirancang mencakup struktur tree atau hirarki yang ada dalam direktori tersebut, tipe-tipe obyek yang akan dibuat, dan jenis-jenis *objectClass* yang digunakan.
4. Struktur Direktori. Pada direktori akan tersimpan object-object dengan susunan sebagai berikut : *entry root*, *role admininistrator utama*, *rntry workgroup name/ domain*, *container Groups*, container *User*s, container Computers, container Samba,
5. Struktur Object Tiap *Account*, yaitu *account* Samba, *account User*s, *account* Computers.
6. Struktur Akses Direktori

Daftar akses berikut dibuat berdasarkan entry-entry yang memiliki perlakuan khusus dan terbatas.

1. Entry keseluruhan, diakses oleh : admin utama berhak menulis dan secara *default* semua dapat melakukan pembacaan.
2. Entry *User*, diakses oleh: admin *account* dan *account* Samba untuk perubahan password.
3. Entry Computer *Account*, diakses oleh *account* Samba
4. Entry Groups, diakses oleh admin *account* dan *account* Samba, saat menambahkan nama pada groups.
5. Atribut perubahan password dan lainnya pada entry *user* diakses oleh *account* Samba, dan admin *account*

Implementasi dilakukan pada komputer Kunti, Pancala, komputer Bisma, komputer Nilayaksa sesuai topologi jaringan pada saat perancangan. [2] [3]

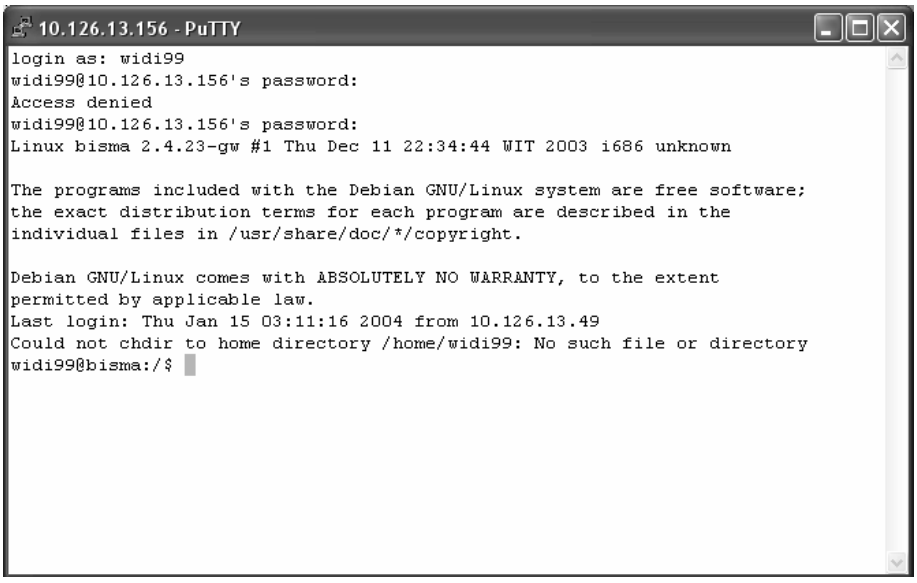


Gambar 5. Struktur Direktori

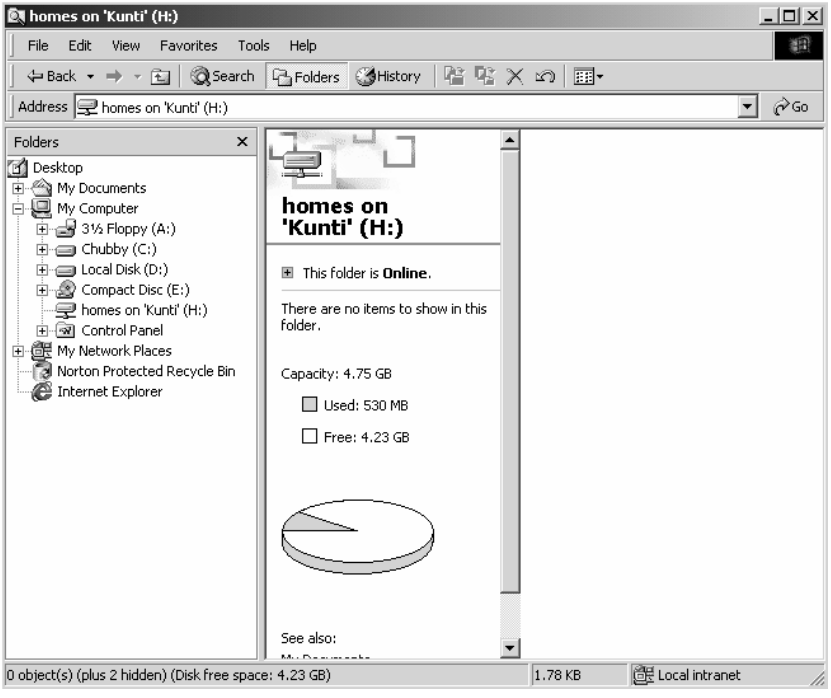
5. UJI COBA DAN EVALUASI

Skenario uji coba yang akan dilakukan pada masing-masing komputer berdasarkan fungsinya dalam sistem.

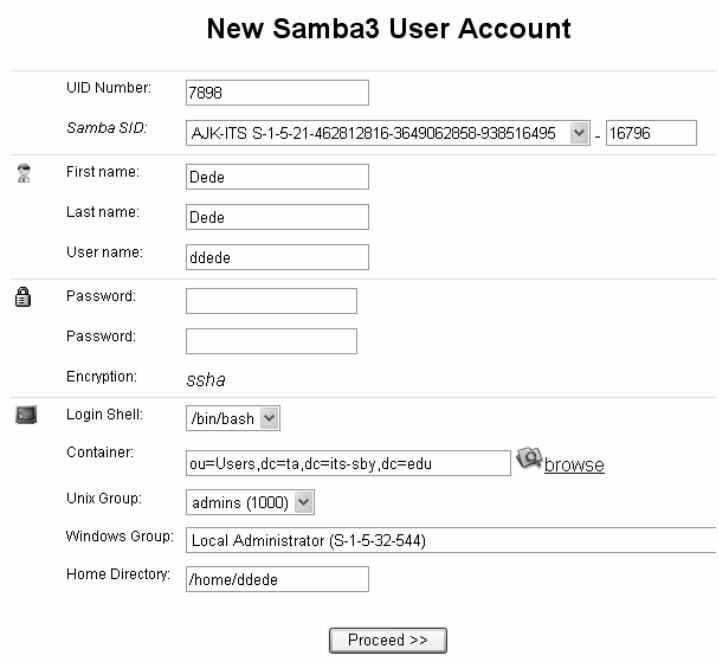
1. Uji coba proses otentikasi dan perubahan password. Beberapa uji coba tersebut, yaitu dengan cara: melakukan login pada sistem Linux menggunakan satu *account user* domain, melakukan perubahan password, melakukan pengaksesan file sharing yang ada pada komputer lain, dengan menggunakan password awal dan password baru, kemudian login pada client Windows 2000 dengan langkah-langkah yang mirip pada Linux sebelumnya.



Gambar 6. Login melalui komputer Bisma dengan sebuah *account*



Gambar 7. Setelah login sukses pada komputer Nilayaksa



Gambar 8. Pengisian nilai-nilai untuk atribut *accountUser*

2. Uji coba proses pemeliharaan sistem menggunakan beberapa aplikasi, menggunakan aplikasi SmbLDAP dan phpLDAPAdmin, yaitu pembuatan *account-account* oleh admin, mencakup pembuatan *account user*, dan pembuatan *account* komputer.

Berdasarkan beberapa uji coba yang telah dilakukan, maka evaluasi terhadap rancangan yang telah dibuat menunjukkan bahwa:

1. Pengguna umum jaringan. Dengan menggunakan rancangan ini pengguna dapat masuk atau login ke sistem operasi yang berbeda dan domain yang berbeda , baik Linux ataupun Windows, dan mengakses *file sharing* dengan menggunakan informasi otentikasi yang ada pada direktori (*username* dan *password* terbaru)
2. Pengelola jaringan. Dengan menggunakan rancangan ini pengelola jaringan dapat mengetahui struktur logis jaringan yang dimiliki, mengatur *account-account* anggota organisasi, dapat menggunakan aplikasi tunggal untuk mengelola informasi-informasi tersebut.

Dari evaluasi di atas dapat disimpulkan bahwa rancangan sistem otentikasi terintegrasi dengan menggunakan Samba dan OpenLDAP ini cukup layak untuk memenuhi kebutuhan sistem otentikasi jaringan komputer Jurusan Teknik Informatika.

6. KESIMPULAN DAN SARAN

Kesimpulan yang dapat diambil oleh penulis dalam penelitian ini ADALAH bahwa beragam solusi dapat digunakan untuk melakukan integrasi otentikasi pada jaringan komputer sesuai dengan kebutuhan organisasi tersebut, sedangkan layanan direktori (*directory service*) dapat menjadi sebuah solusi manajemen identitas dan jaringan sebuah organisasi, dan kombinasi antara OpenLDAP dan Samba dapat menjadi salah satu solusi otentikasi terintegrasi dalam jaringan sistem operasi Linux dan Windows.

Saran yang dapat diberikan oleh penulis untuk tindak lanjut penelitian ini yaitu bahwa Jurusan Teknik Informatika dapat menerapkan sistem manajemen identitas pada lingkungan sistem informasi jurusan, selain itu aplikasi-aplikasi lain dapat dikembangkan dengan menggunakan LDAP untuk integrasi dan kemudahan administrasi, dan selain menggunakan OpenLDAP, dapat juga dengan Active Directory ataupun Novell eDirectory 8.5.

7. DAFTAR PUSTAKA

1. IBM Corp. “Using LDAP for Directory Integration: A Look at IBM SecureWay Directory, Active Directory, and Domino” IBM Publishing, 2003
2. Jelmer R. Vernooij, John H. Terpstra, Gerald (Jerry) Carter. “Samba HOWTO Collection”. Samba Foundation, November 15, 2003. www.samba.org
3. Jim Collings “MandrakeSecure: Implementing a Samba LDAP Primary Domain” MandrakeSoft 22 Mei 2003

4. M-Tech Corp. “Defining Enterprise Identity Management” Available from http://www.psynch.com/docs/what_is_identity_ management.pdf, Accessed November 2003
5. M. Wahl, T. Howes, S. Kille, “RFC2251 Lightweight Directory Access Protocol (v3)”. IETF Desember 1997.
6. Novell Publishing, “Novell Documentation LDAP and NDS Integration - Novell LDAP Servers”, 2001.
7. Robert Williams, Mark Walla, “Understanding Active Directory Part I II III”, Addison Wesley., 1 Mei 2002.
8. Rutrell Yasin, “What is Identity Management?”, Info Security Magazine, April 2002. Available from http://infosecuritymag.techtarget.co m , Accessed November 2003.
9. The OpenLDAP Project , “OpenLDAP 2.1 Administrator’s Guide”, Open LDAP Foundation, 10 Januari 2003
10. Turbo Fredriksson, “OpenLDAP, OpenSSL, SASL and KerberosV HOWTO”, . www .bayour.com, 11 September 2003