

Integrasi User Account dengan LDAP

Bagian 1 dari 3 Artikel

Salah satu kemudahan di jaringan MS Windows, Anda dapat mengakses semua server hanya dengan satu *username* dan satu *password*. Jangan khawatir, di Linux ada fasilitas setara yaitu menggunakan LDAP, solusi integrasi username untuk memperingan tugas system administrator dan mempermudah *user*.

InfoLINUX edisi Januari (01/2005) dan Maret (03/2005) telah mengenalkan LDAP (*Lightweight Directory Access Protocol*) dan contoh konfigurasinya di distro SUSE. Mulai edisi ini penulis akan membahas penggunaan LDAP sebagai solusi integrasi *user account* berbagai server, dengan distro Fedora Core. Bagian pertama ini membahas teknologi dan aplikasi sejenis LDAP, serta contoh konfigurasi dan penggunaan LDAP.

Pengantar teknologi single sign-on

Fasilitas integrasi semua server dengan satu *username* dan satu *password* dinamakan *single sign-on*. Keuntungan yang didapat dari penggunaan *single sign-on* ialah:

- **User tidak perlu menghafal lebih dari satu username dan password.**

Hal ini akan memudahkan system administrator karena user akan jarang meminta system administrator untuk *reset password*-nya karena lupa.

- **System administrator akan bekerja lebih efisien.**

Untuk membuat username seorang karyawan baru, mengubah konfigurasi username, dan menonaktifkan username tersebut pada saat ada seorang karyawan keluar, cukup dengan menambah, mengubah, atau menghapus satu username sekali saja.

- **Meminimalkan kesalahan administrasi.** Setelah system administrator mengubah atau menonaktifkan satu username de-

ngan sekali perintah saja, semua server secara otomatis mengikuti perubahan tersebut tanpa ada yang terlewatkan.

Secara logika, kepraktisan *single sign-on* adalah seperti gedung dengan beberapa ruangan akan lebih praktis jika ada satu kunci master yang dapat membuka semua ruangan itu. Namun kepraktisan ini jika tidak dijaga dengan benar akan menjadi kelemahan. Jika kunci master tersebut jatuh ke tangan orang yang tidak berhak, akan menimbulkan dampak ke seluruh ruangan dalam gedung tersebut. Jadi, system administrator harus bisa menjaga keamanan *password*-nya.

Beberapa aplikasi single sign-on yang populer

1. Winbind

Windbind merupakan servis pada Microsoft Windows NT server, yang berfungsi memberikan data informasi user dan group serta melakukan autentikasi.

Untuk mengintegrasikan autentikasi mesin Linux/Unix ke MS Windows NT Server dapat menggunakan samba. Cara ini tidak dianjurkan mengingat rentanya keamanan pada Windows NT Server jika digunakan sebagai master autentikasi server. Jika master autentikasi server keamanannya lemah, maka seluruh client server akan sangat dirugikan keamanannya.

2. Microsoft Active Directory

Microsoft Active Directory adalah service

directori yang terdistribusi yang terdapat kali pertama pada MS Windows 2000 Server yang kemudian dikembangkan lebih lanjut pada MS Windows Server 2003. Active Directory mempunyai fungsi sebagai direktori yang terpusat yang dapat mengatur seluruh sumber daya yang ada pada network secara aman. Ini memungkinkan untuk memperluas penggunaannya ke seluruh gedung, kota, atau beberapa lokasi di dunia.

Kerberos V5 merupakan protokol autentifikasi standar di Active Directory. Sedangkan LDAP adalah protokol akses direktori yang mendasari Active Directory ini. Active Directory mendukung LDAP versi 2 dan LDAP versi 3 yang menggunakan *Secure Sockets Layer* (SSL).

Mekanisme autentikasi digunakan untuk mengecek identitas user atau komputer. Setelah proses autentikasi identitas user selesai, domain controller akan membuat sebuah *access token* untuk menyatakan akses level dari user tersebut dalam mengakses segala sumber daya dalam network. Dengan *access token*, user tidak perlu melakukan login berulang-ulang pada saat mengakses servis lain pada server lain yang ada dalam satu domain, pada saat proses autentikasi dilakukan.

Autentikasi di antara domain berdasarkan kepercayaan (*trust*). Hubungan kepercayaan di adakan di antara satu atau dua domain untuk mengizinkan user dalam satu domain diautentikasi oleh *domain controller* dalam domain lainnya.

3. NIS

Network Information Service (NIS) merupakan sebuah servis pada Unix dan Linux yang menyediakan informasi ke semua mesin-mesin di network. Informasi yang didistribusikan oleh NIS contohnya adalah username, password, home directory (/etc/passwd), dan informasi group (/etc/group). NIS sebelumnya dikenal sebagai Sun Yellow Pages (YP). Nama Yellow Pages merupakan merk terdaftar dari British Telecom di Inggris dan tidak boleh digunakan tanpa seizin perusahaan tersebut, sehingga Sun akhirnya mengubah namanya menjadi NIS.

4. NIS+

NIS+ merupakan penyempurnaan NIS lebih lanjut oleh Sun Microsystems. Kelebihanannya ialah peningkatan keamanan protokol NIS, seperti setiap paket data terenkripsi, serta item-item data yang disimpan lebih banyak dan lebih detail sehingga dapat menangani sistem pada organisasi yang besar. Kelemahan utamanya, NIS+ merupakan standar tertutup yang dimiliki oleh Sun. Meskipun perusahaan lainnya dapat membuat client berdasarkan teknologi NIS+, tetapi untuk memperoleh NIS+ server harus membeli dari Sun. NIS+ server jalan pada sistem operasi Sun Solaris. Model penamaan dari NIS+ ialah berdasarkan struktur pohon (tree). Tiap titik dalam pohon berhubungan ke sebuah NIS+ object, yang terdiri atas enam tipe: direktori, entri, group, link, tabel, dan privat.

5. Novell eDirectory

eDirectory adalah direktori servis yang merupakan pengembangan lebih lanjut dari NDS (*Novell Directory Service*) yang dulu populer pada sistem operasi jaringan Novell NetWare. eDirectory menggunakan LDAP sebagai standar protokol pengaksesan. Kelebihan eDirectory ini kompatibel dengan berbagai protokol standar seperti LDAP versi 3, XML, DSML, SOAP, dan lain-lain. eDirectory dapat dijalankan pada berbagai operating sistem: Linux, Windows, Solaris, AIX, NetWare, dan HP-UX. eDirectory menjadi dasar yang menghubungkan user dengan hak akses mereka, dengan sumber daya yang dimiliki perusahaan.

Di luar kelima teknologi single sign-on di atas masih ada beberapa yang lainnya. Ke-

lima teknologi single sign-on ini sering ditemui oleh para user pada saat sekarang ini di lingkungan sistem operasi Windows, Novell dan Linux/Unix. Dari kelima teknologi tersebut, dua teknologi yang terbaru adalah MS Active Directory dan Novell eDirectory, yang menggunakan LDAP sebagai protokol pengaksesan. Bahkan Sun sendiri pada saat ini memutuskan untuk tidak meneruskan pengembangan NIS+ tetapi menggunakan Sun One Directory Server yang juga menggunakan LDAP. Produk tersebut dibeli dari Netscape yang sebelumnya bernama Netscape Directory Server. Jelaslah bahwa LDAP telah menjadi standar protokol untuk pengakses servis direktori saat ini.

Servis direktori

Servis direktori adalah suatu database khusus yang dioptimasi untuk membaca dan mencari informasi direktori. Direktori berisi deskripsi dan atribut yang mempunyai kemampuan untuk menyaring (filter) dengan baik. Servis direktori umumnya tidak mendukung proses transaksi rumit seperti *roll-back* yang lazimnya ditemukan di sistem manajemen database (DBMS) yang didesain untuk menangani volume data dalam jumlah sangat besar dengan proses update yang kompleks.

Proses update direktori merupakan proses sederhana. Direktori didesain untuk memberikan respon dengan cepat untuk pencarian data dengan volume besar. Direktori mempunyai kemampuan untuk mereplikasi/mengandakan informasi secara luas agar dapat diakses setiap saat, informasi di dalamnya dapat dipercaya, dan waktu respon yang pendek. Ketika informasi dalam direktori direplikasi, ketidakkonsistenan sementara antara replika adalah wajar, selama beberapa saat kemudian mereka disinkronkan.

Metode yang berbeda mengizinkan berbagai informasi untuk disimpan dalam direktori dan diletakkan sesuai dengan ketentuan (rule) yang berbeda. Misalnya, bagaimana informasi kemudian direferensikan, diambil, dan di-update/diperbarui, bagaimana diproteksi dari akses yang tidak diizinkan, dan sebagainya.

Servis direktori lokal menyediakan servis ke konteks yang terbatas untuk lingkungan tertentu saja (contoh, servis whois di satu

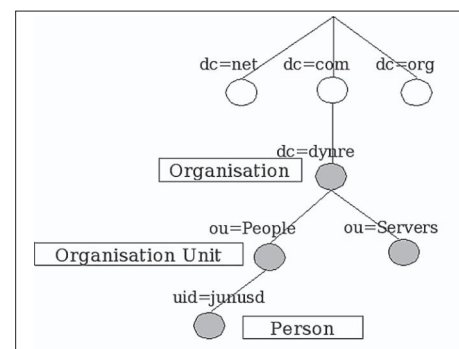
mesin). Sedangkan servis global menyediakan servis ke konteks yang lebih luas (contoh, ke seluruh Internet). Servis global biasanya terdistribusi, artinya data mereka tersebar luas pada banyak mesin, yang semuanya bersama-sama saling membantu beroperasi untuk menyediakan servis direktori. Internet Domain Name System (DNS) adalah contoh dari servis direktori terdistribusi secara global.

LDAP

LDAP merupakan singkatan dari *Lightweight Directory Access Protocol* (Protokol Akses Direktori Ringan). Artinya, ini adalah protokol kelas ringan untuk mengakses servis direktori, yang berdasarkan pada protokol servis direktori X.500. LDAP berjalan melalui protokol TCP/IP. Pendefinisian secara detail LDAP ada dalam RFC 2251 "The Lightweight Directory Access Protocol (v3)" dan dokumen lainnya menyatakan spesifikasi teknik ada pada RFC 3377.

Model informasi LDAP adalah berdasarkan entri. Sebuah entri adalah koleksi atribut yang mempunyai nama yang terbedakan (Distinguished Name/DN) secara global. DN ini digunakan sebagai referensi ke entri yang secara unik berbeda dengan nilai DN yang lainnya. Setiap atribut entri mempunyai sebuah tipe dengan satu nilai atau lebih. Tipe biasanya string singkatan khusus, seperti "cn" untuk *common name*, atau "mail" untuk alamat e-mail.

Sintaks dari nilai bergantung kepada tipe atribut. Contoh, atribut cn mungkin berisi kata-kata "Junus Djunawidjaja". Atribut mail mungkin berisi alamat email "junus@dynre.com". Atribut jpegPhoto mungkin terdiri sebuah foto dalam format binari JPEG.



Gambar 1. Pohon direktori LDAP.

Dalam LDAP, entri direktori disusun dalam sebuah hirarki struktur seperti pohon (tree). Struktur pohon LDAP pada umumnya saat sekarang ini berdasarkan nama domain internet. Pendekatan penamaan servis direktori mirip dengan penamaan pada DNS ini yang paling populer. Gambar 1 menunjukkan sebuah contoh pohon direktori LDAP menggunakan penamaan berdasarkan domain.

Selain secara struktur pohon dengan penamaan internet, juga dapat berupa struktur pohon dengan cara penamaan tradisional. Struktur ini merefleksikan geografis atau lingkup organisasi. Entri-entri mewakili negara-negara, terlihat di atas dari pohon (tree). Di bawah mereka adalah entri yang menyatakan provinsi dan organisasi nasional. Di bawah nya lagi mungkin entri yang menyatakan unit organisasi, orang, printer, dokumen, dan lain-lain.

LDAP dapat mengontrol atribut-atribut yang diperlukan dan diizinkan dalam sebuah entri, melalui penggunaan atribut spesial yang dinamakan *objectClass*. Angka-angka dari atribut *objectClass* menyatakan aturan (rule) schema yang ditaati oleh entri.

Sebuah entri direferensi oleh nama yang berbeda dari yang lain, yang dibentuk dari nama entri itu sendiri. Ini dinamakan nama relatif yang membedakan (Relative Distinguished Name/RDN) dan menggabungkan nama-nama dari entri-entri di atasnya atau sebelumnya. Sebagai contoh, entri untuk "Junus Djunawidjaja" pada penamaan berdasarkan Internet contoh di atas mempunyai RDN: uid=junusd dan DN dari uid=junusd, ou=People,dc=dynre,dc=com.

Operasi update yang ada, seperti untuk menambah dan menghapus sebuah entri dari direktori, adalah mengubah entri yang ada dan mengubah nama dari sebuah entri. Sebagian besar waktu LDAP digunakan untuk operasi mencari informasi dalam direktori (query). Operasi pencarian LDAP memungkinkan beberapa bagian dari direktori untuk mencari entri-entri yang sama dengan beberapa kriteria yang dispesifikasikan oleh filter search.

Sebagai contoh operasi pencarian (*query*):

- Mencari cabang dari direktori di bawah dc=dynre, dc=com untuk orang-orang dengan nama "Junus", lalu memanggil

alamat kantor dari setiap entri yang ditemukan.

- Atau juga dimungkinkan untuk mencari entri secara keseluruhan di bawah entri ou=Group untuk organisasi yang mempunyai kelompok Group="admin", lalu menampilkan semua anggota group di dalamnya.

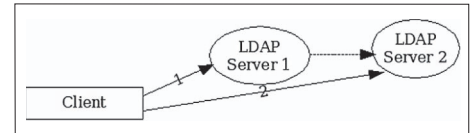
Cara kerja LDAP

Secara teknis, LDAP adalah sebuah protokol untuk mengakses ke servis direktori X.500, yang merupakan direktori servis yang diatur oleh OSI. Awalnya, client LDAP mengakses gateway ke servis direktori X.500. Gateway ini menjalankan LDAP di antara client dan gateway, dan menjalankan Protokol Akses Direktori (Directory Access Protocol/DAP) X.500 antara gateway dan X.500 server. DAP adalah sebuah protokol kelas berat yang beroperasi melalui tumpukan protokol OSI secara penuh dan memerlukan pemrosesan yang sangat signifikan dari sumber daya komputasi. LDAP didesain untuk beroperasi melalui TCP/IP dan menyediakan sebagian besar dari fungsi DAP dengan biaya yang sangat lebih rendah.

Service direktori LDAP berdasarkan model client-server. Satu atau lebih server LDAP membentuk pohon (tree) direktori informasi. Client terkoneksi ke server dan mengajukan pertanyaan. Server merespon dengan jawaban dan/atau dengan pointer, ke arah mana client dapat mendapat tambahan informasi (khususnya ke server LDAP yang lain). Gambar 2 menunjukkan proses koneksi dari client ke server LDAP pertama dan server LDAP kedua yang ditunjuk oleh server LDAP pertama.

Tidak masalah pada server LDAP yang mana seorang client akan terkoneksi. Client tersebut akan mendapat informasi yang sama dari server direktori berupa sebuah nama yang direpresentasikan ke satu LDAP server sebagai entri referensi yang akan menunjuk ke server LDAP lainnya. Ini ciri khas penting bagi servis direktori global seperti LDAP.

Servis direktori LDAP menyediakan proteksi keamanan, yang dapat diset pada saat orang akan melihat informasi diharuskan untuk melewati proses autentifikasi atau login terlebih dahulu. Sehingga orang yang



Gambar 2. Proses koneksi dari client ke server LDAP pertama dan kedua.

tidak terautentifikasi identitasnya, tidak berhak untuk melihatnya.

LDAP Server pada lingkungan Unix dan Linux

Pada lingkungan sistem operasi Unix dan Linux terdapat berbagai macam LDAP server misalnya:

- IBM Directory Server dan Sun One Directory Server sebagai contoh produk *proprietary* atau tidak free.
- University of Michigan LDAP server dan OpenLDAP server sebagai contoh produk yang free.

Kita akan membahas penggunaan OpenLDAP server, karena software ini telah menjadi LDAP server standar pada berbagai distribusi Linux besar seperti Red Hat, SUSE, Mandrake, maupun Debian. OpenLDAP server dibuat berdasarkan pada versi terakhir dari University of Michigan LDAP Server.

OpenLDAP mempunyai daemon *slapd* dan *slurpd*. Daemon *slapd* yang berdiri sendiri dapat dilihat sebagai sebuah servis direktori X.500 kelas ringan. Ini tidak mengimplementasi Protokol Akses Direktori kelas berat X.500. Sebagai direktori server kelas ringan, *slapd* hanya mengimplementasi sebagian kecil dari model X.500. Sedangkan daemon *slurpd* digunakan mereplikasi informasi direktori dari daemon *slapd*. Client tidak dapat meng-update informasi direktori yang ada pada *slurpd* secara langsung. *slurpd* akan mereferensi ke *slapd* jika ada permintaan untuk update informasi. Guna dari replikasi direktori menggunakan *slurpd* untuk memperingan beban pada daemon utama *slapd*, serta untuk redundansi pada saat *slapd* tidak berjalan. Jadi, mesin-mesin client akan tetap dapat mengakses informasi direktori melalui *slurpd*.

Pembahasan di atas merupakan penjelasan prinsip dasar LDAP secara garis besar sehingga diharapkan pembaca awam akan mudah untuk memahaminya. Jika pembaca

ingin mendapat informasi lebih detail dapat membaca OpenLDAP User Guide di (www.openldap.org).

Contoh penggunaan OpenLDAP

File dengan format LDIF berisi struktur data LDAP. Ini merupakan file input standar pada utility-utility ldap client seperti slapadd dan ldapadd. File format LDIF ini dapat dibuat menggunakan sembarang text editor (misalnya: vi, pico, dan emacs). Sangat jarang pengguna membuatnya dengan mengetikkan langsung secara interaktif ke utility ldap client, karena banyaknya teks yang harus diketikkan.

Berikut ini contoh file format LDIF yang berisi data sebuah account user dari server direktori dengan base dn: dc=dynre,dc=com. Ranting-ranting utamanya berisi data kelompok People dan Group. Dalam ranting kelompok People dan Group berisi data username dan group dari user "junusd". Di sini untuk mempersingkat contoh file LDIF, hanya diberikan contoh dua data kelompok People dan Group saja. Server direktori sebenarnya dapat berisi data kelompok: Aliases, Hosts, Mounts, Netgroup, Networks, Protocols, RPC, Services, dan sebagainya.

```
dn: dc=dynre,dc=com
dc: dynre
objectClass: top
objectClass: domain
objectClass: domainRelatedObject
associatedDomain: dynre.com
dn: ou=People,dc=dynre,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: dynre.com
structuralObjectClass: organizationalUnit
entryUUID: d0ba50c-0340-1029-8601-8d42d871530d
creatorsName: uid=root,ou=people,dc=dynre,dc=com
modifiersName: uid=root,ou=people,dc=dynre,dc=com
createTimestamp: 20050125171803Z
modifyTimestamp: 20050125171803Z
entryCSN: 2005012517:18:03Z#0x0001#0#0000
dn: ou=Group,dc=dynre,dc=com
ou: Group
objectClass: top
```

```
ou: People
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: dynre.com
```

```
dn: ou=Group,dc=dynre,dc=com
ou: Group
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: dynre.com
```

```
dn: cn=junusd,ou=Group,dc=dynre,dc=com
objectClass: posixGroup
objectClass: top
cn: junusd
userPassword: {crypt}x
gidNumber: 500
```

```
dn: uid=junusd,ou=People,dc=dynre,dc=com
uid: junusd
cn: junusd
sn: junusd
mail: junusd@dynre.com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$1$.Irzjld0
$junusdpAqo1DU12efs3074b0
shadowLastChange: 12803
```

```
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/junusd
```

Simpan file di atas dengan nama dynre.ldif. Lalu tambahkan file ini ke dalam LDAP database dengan perintah:

```
# slapadd -l dynre.ldif
```

Kemudian untuk mengecek apakah data LDAP telah dimasukkan dengan benar, ketik perintah:

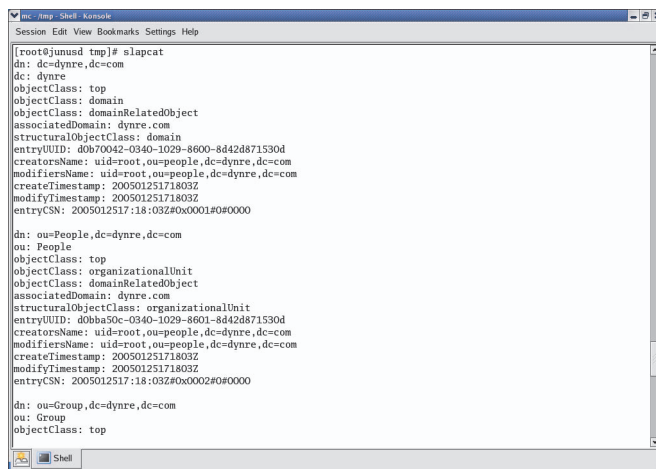
```
# slapcat
```

Cara menampilkan data LDAP ini dapat menggunakan utility LDAP client yang berbasis grafis, sehingga lebih mudah untuk dilihat dan dimengerti. Gambar 4 menunjukkan data LDAP dapat dilihat menggunakan contoh utility LDAP client, JXplorer.

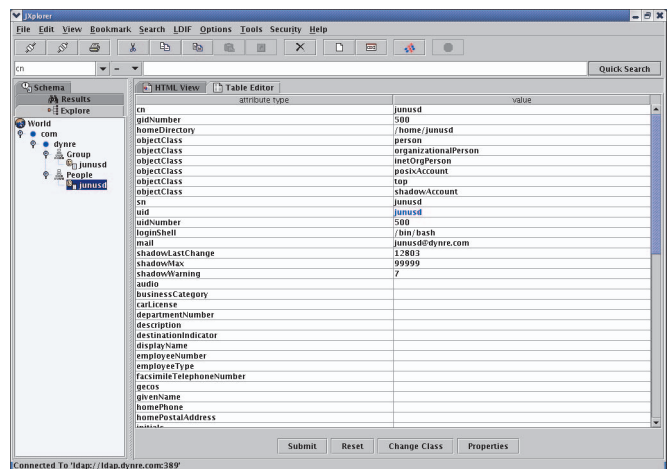
Artikel berikutnya akan menjelaskan cara men-setting OpenLDAP server dan menghubungkannya sebagai servis autentifikasi pada mesin client, cara menghubungkannya dengan mail server, web server, serta servis-servis umum lainnya. Ditambah dengan cara administrasi data username yang ada pada LDAP server.

Artikel bagian ketiga akan menjelaskan cara men-setting Samba versi 3 dengan menggunakan LDAP sebagai servis informasi direktori, serta cara-cara administrasinya yang lebih mendalam.

Junus Djunawidjaja (junusd@dynre.com)



Gambar 3. Hasil keluaran perintah slapcat.



Gambar 4. Tampilan JXplorer.

Integrasi User Account dengan LDAP

Bagian 2 dari 3 Artikel

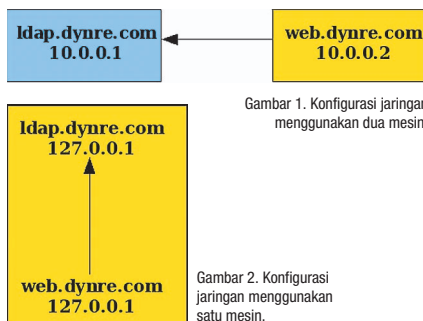
Pada bagian pertama kita telah mempelajari pengertian *single sign-on* dan penjelasan tentang apa itu protokol LDAP. Bagian kedua ini membahas cara-cara penggunaan *single sign-on* pada client dan server.

Untuk menghindari konfigurasi yang kompleks, artikel kedua ini belum membahas penerapan fungsi *secondary/slave* LDAP server menggunakan daemon *slurpd* maupun penggunaan protokol enkripsi *ssl*. Fokus kita hanya menginstalasi dan mengonfigurasi OpenLDAP client dan server. Sebagai langkah awal, pembaca hanya perlu mengetahui teknik dasar *men-setup network* berbasis TCP/IP pada Linux dan teknik dasar administrasi user di Linux.

Konfigurasi jaringan

Sebagai contoh di sini menggunakan penamaan *domain* *dynre.com*. Nama domain ini dapat diganti sesuai dengan nama domain pada sistem komputer pembaca. Jika tidak memungkinkan untuk memiliki dua mesin seperti gambar 1, proses ini juga dapat dilakukan dalam satu mesin saja dengan menggunakan alamat IP *localhost* (127.0.0.1). Jadi proses client dan server bisa berjalan dalam satu mesin seperti pada gambar 2.

Pada konfigurasi satu mesin, untuk



Gambar 1. Konfigurasi jaringan menggunakan dua mesin.

Gambar 2. Konfigurasi jaringan menggunakan satu mesin.

menghindari kebingungan konfigurasi mana yang untuk server *ldap.dynre.com* dan mana untuk *web.dynre.com*, kedua domain itu dimasukkan ke file */etc/hosts* (mapping ip address ke nama mesin):

```
127.0.0.1 localhost ldap.dynre.com web.dynre.com
```

Paket software

Distribusi Linux yang digunakan untuk uji coba adalah Fedora Core 2, yang merupakan versi non-komersial dari Red Hat. Fedora Core 2 tersebut disarankan untuk diinstal dengan pilihan installation type: "server". Kemudian IP address diberikan pada mesin ini sesuai dengan penjelasan di atas. Semua paket RPM untuk OpenLDAP server dan client telah tersedia pada Fedora Core 2 CD.

Semua proses administrasi di bawah ini dilakukan dengan login sebagai root. Jika pilihan tipe instalasi server, dua paket RPM di bawah ini terinstall secara otomatis pada saat instalasi awal distribusi (terdapat dalam Fedora Core 2 CD nomor 1):

- *openldap-2.1.29-1.i386.rpm*
- *nss_ldap-217-1.i386.rpm*

Paket RPM *openldap* di atas hanya berisi kumpulan library *openldap* yang dibutuhkan oleh paket-paket RPM aplikasi lainnya. Di dalam paket ini tidak termasuk file executable untuk server dan client dari *openldap*.

Paket RPM *nss_ldap* berisi dua program client LDAP *nss_ldap* dan *pam_ldap* yang berguna sebagai library client *ldap* untuk

servis penamaan (NSS) dan autentikasi password (PAM).

Sedangkan paket RPM *openldap* server dan client tidak terinstall secara otomatis kalau tidak dipilih pada saat instalasi awal distribusi (kedua file ini terdapat dalam Fedora Core 2 CD nomor 3).

- *openldap-clients-2.1.29-1.i386.rpm*
- *openldap-servers-2.1.29-1.i386.rpm*

Selain keempat paket RPM di atas, paket di luar Fedora Core 2 CD yang perlu di-download dari Internet adalah:

- Paket untuk administrasi user, Directory Administrator 1.6.0, yang bisa di-download dari website: <http://diradmin.openit.org>.
- Modul autentikasi PAM bagi Apache server, untuk mendapatkannya dapat diambil dari alamat website: http://pam.sourceforge.net/mod_auth_pam/dist/mod_auth_pam-2.0-1.1.1.tar.gz.

Konfigurasi server

1. Menginstal paket RPM *openldap-server* dan *openldap-client*

```
# rpm -ivh openldap-servers-2.1.29-1.i386.rpm
# rpm -ivh openldap-clients-2.1.29-1.i386.rpm
```

Sebenarnya di sini hanya membutuhkan paket RPM *openldap-server* saja, tetapi paket RPM *openldap-client* yang berisi seperti *ldappd* dan *ldapsearch* akan sangat membantu untuk menelusuri (*trace*) jika terjadi masalah.

2. Edit file `/etc/openldap/slapd.conf`
 - a. Tambahkan `misc.schema` di antara `nis.schema` dan `autofs.schema`:

```
include /etc/openldap/
schema/nis.schema
include /etc/openldap/
schema/misc.schema
include /etc/openldap/
schema/redhat/autofs.schema
```

- b. Tambahkan Access Control: Untuk mengizinkan `uid=root` mengubah semua atribut termasuk `userPassword`. Sedangkan user biasa hanya diijinkan untuk membaca dan mengubah atribut `userPassword`-nya sendiri, dan bisa membaca atribut lain. Akses tanpa user dan password (*anonymous access*) dipaksa untuk diautentifikasi.

```
access to attr=userPassword
    by dn="uid=root,ou=
People,dc=dynre,dc=com" write
    by self write
    by anonymous auth
access to *
    by dn="uid=root,ou=
People,dc=dynre,dc=com" write
    by self write
    by anonymous read
```

- c. Edit suffix dan rootdn, sesuaikan dengan nama domain:

```
suffix "dc=dynre,dc=com"
rootdn "uid=root,ou=
people,dc=dynre,dc=com"
```

3. Persiapan sebelum menjalankan utility migrasi:

- a. Periksa file `/etc/passwd`:

Sebagai konfigurasi awal dimulai dengan ada 2 user aktif, yaitu `root` dan misalnya `junusd`. Anda dapat melihat file `passwd`-nya:

```
root:x:0:0:root:/root:/bin/
bash
bin:x:1:1:bin:/bin:/sbin/
nologin
daemon:x:2:2:daemon:/sbin:/
sbin/nologin
...
gdm:x:42:42::/var/gdm:/sbin/
nologin
junusd:x:500:500::/home/
junusd:/bin/bash
```

- b. Untuk menghindari kesalahan saat migrasi, edit file `/etc/services`. Pada baris ke-472 perlu diberi tanda comment (#), karena protokol `echo` sudah keluar pada bagian TCP/IP sebelumnya. Di sini tidak terlalu diperlukan, karena `echo` ini untuk protokol `AppleTalk`.

```
nbp 2/ddp # Name
Binding Protocol
#echo 4/ddp # AppleTalk
Echo Protocol
zip 6/ddp # Zone
Information Protocol
```

4. Menjalankan utility migrasi

- a. Edit file `/usr/share/openldap/migration/migrate_common.ph`. Edit default domain dan default base.

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN =
"dynre.com";
# Default base
$DEFAULT_BASE =
"dc=dynre,dc=com";
```

Kira-kira 15 baris di bawahnya, edit `extended_schema`.

```
# turn this on to support
more general object classes
# such as person.
$EXTENDED_SCHEMA = 1
```

- b. Buat file kosong `/etc/netgroup`. Ini untuk menghindari adanya pesan error saat migrasi, karena Fedora Core tidak mempunyai `/etc/netgroups`.

```
# touch /etc/netgroup
```

- c. Jalankan file `/usr/share/openldap/migration/migrate_all_offline.sh`. Tampilan yang akan keluar di layar adalah:

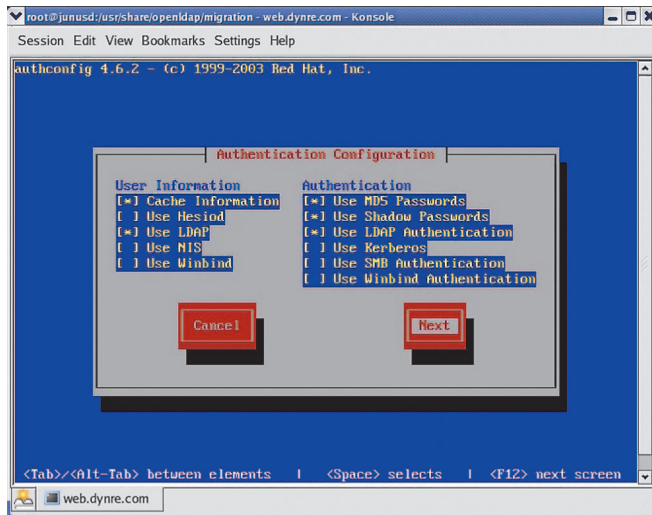
```
Creating naming context
entries...
Migrating aliases...
Migrating groups...
Migrating hosts...
Migrating networks...
Migrating users...
Migrating protocols...
Migrating rpcs...
Migrating services...
Migrating netgroups...
```

Pesaing Anda kini mengenal Linux*

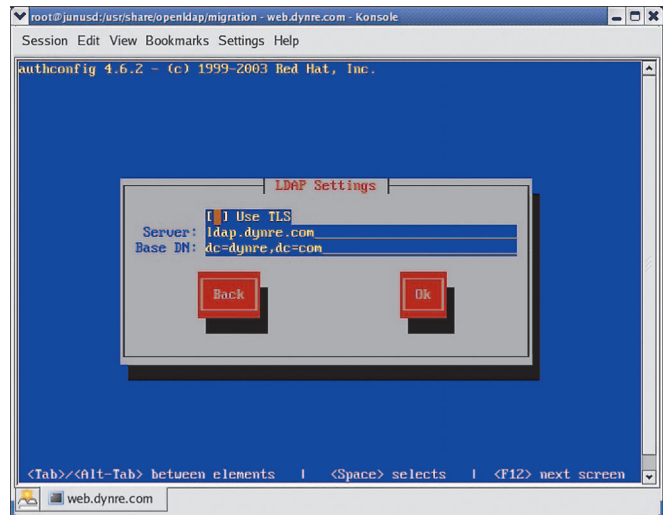


Saatnya menutup semua jendela

* Got The Software Freedom from:
GudangLinux
Migration - Center
www.gudanglinux.net



Gambar 3. Tampilan dialog Authentication Configuration.



Gambar 4. Tampilan dialog LDAP Settings.

```
Importing into LDAP...
Migrating netgroups (by
user)...
Migrating netgroups (by
host)...
Preparing LDAP database...
```

Catatan:

Jika tidak terjadi kesalahan, lanjutkan ke langkah berikutnya. Tetapi jika terjadi kesalahan (keluar *error message*), perbaiki file yang berhubungan dengan kesalahan tersebut. Sebelum menjalankan ulang langkah c di atas, hapus database ldap lebih dahulu:

```
# rm /var/lib/ldap/*
```

Cara kerja utility migrasi ini sebenarnya adalah hanya membuat file dengan format LDIF. Kalau pada sistem database SQL, mirip file dengan format yang berisi perintah-perintah SQL untuk menambah data. Hanya, format LDIF ini bukan perintah, tetapi hanya berisi struktur datanya saja. Kemudian utility migrasi itu akan menjalankan perintah `slapadd` untuk membuat file-file ldap database di dalam direktori: `/var/lib/ldap`.

d. Langkah terakhir untuk instalasi server ialah mengubah *owner* file-file dalam `/var/lib/ldap` agar menjadi milik user ldap. Kemudian *restart* daemon `slapd`.

```
# chown ldap:ldap /var/lib/
```

```
ldap/*
# service ldap restart
```

Konfigurasi client

Konfigurasi untuk mesin client tidak sesulit mesin server. Anda cukup menjalankan utility setup. Perlu diperhatikan, jika tidak terjadi koneksi antara mesin client dan server biasanya karena adanya servis *firewall*. Maka sebelum menjalankan konfigurasi client, proses firewall harus dimatikan terlebih dahulu pada mesin client dan server. Firewall pada Fedora Core 2 biasanya dinyalakan secara otomatis secara default pada instalasi awal. Berikut ini perintah untuk mematikan service firewall:

```
# service iptables stop
```

Menjalankan utility setup

- Jalankan setup
- Pilih “Authentication configuration”
- Pada bagian “User Information”:
 - * enable “Cache Information”
 - * enable “Use LDAP”
- Pada bagian “Authentication”:
 - * enable “MD5 Passwords”
 - * enable “Shadow Passwords”
 - * enable “Use LDAP Authentication”
- Tekan tombol “Next”
- Karena di sini tidak digunakan protokol enkripsi, maka kosongkan pilihan “Use TLS”
 - * Server: ldap.dynre.com
 - * Base DN: dc=dynre,dc=com
- Kemudian tekan tombol “OK” untuk keluar.

- Di layar akan tampak daemon `nscd` di-restart:

```
Stopping nscd:      [ OK ]
Starting nscd:      [ OK ]
```

Daemon `nscd` ini berguna sebagai cache untuk proses resolving servis nama termasuk user name dan password yang di-*request* ke server. Jika daemon `nscd` tidak dijalankan maka trafik paket antara mesin client dan server akan sangat banyak. Setiap kali proses *resolving* akan dimintakan ke server langsung, meskipun nama yang sama sudah pernah diminta sebelumnya.

Utility setup di atas akan mengubah file konfigurasi pada mesin client yang terdapat pada file `/etc/ldap.conf`. Untuk meminimumkan terjadinya kesalahan, sebaiknya file tersebut tidak perlu diedit secara manual. Setiap ingin melakukan perubahan sebaiknya melalui utility setup.

Sekarang bisa dicoba untuk melakukan tes login.

- Pertama-tama hapus satu baris user `account` (dalam contoh ini adalah user `account junusd`) dari file `/etc/passwd`. Lalu Anda dapat mencoba login sebagai user tersebut. Jika anda bisa masuk login, berarti mesin tersebut mendapat data login anda dari server ldap. Jika tidak bisa, periksa ulang apakah langkah-langkah instalasi di atas ada yang terlewatkan.
- Sebagai standar praktik administrasi yang baik, setelah mengubah konfigurasi yang

berhubungan dengan servis autentifikasi login, jangan langsung keluar dari konsol Anda. Gunakan konsol yang lainnya. Jika terjadi kesalahan, anda tetap mempunyai *login root* yang masih terbuka. Sehingga walaupun terjadi kesalahan, anda tidak perlu me-*reboot* mesin dan masuk menggunakan mode linux single.

- Untuk melakukan tes login melalui konsol yang lainnya pada saat Anda bekerja dalam mode grafik, tekan: Ctrl+Alt+F2 untuk menuju ke konsol kedua. Untuk kembali lagi ke mode grafik, tekan: Alt+F7.

Administrasi user

Untuk administrasi user, tersedia utility yang memudahkan tugas administrator yaitu Directory Administrator.

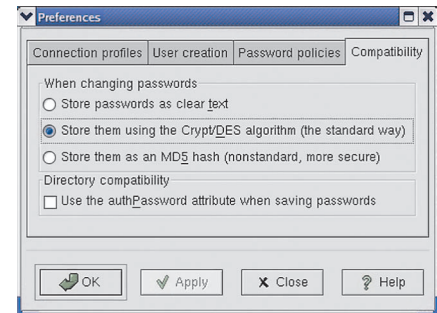
Kelebihan utility ini ialah kemudahannya, karena menggunakan mode grafis dan terintegrasi secara baik dengan aplikasi lain yang menggunakan LDAP, seperti email dan samba.

Sedangkan kelemahan utility ini ialah struktur data atribut hanya untuk samba versi 2, padahal Fedora Core 2 ini telah menggunakan samba versi 3.

Catatan:

Pada bagian ketiga mendatang, kita tidak akan menggunakan Directory Administrator ini untuk me-*manage user*, tetapi akan menggunakan utility *command line* *smbldap* yang sudah terdapat dalam paket RPM samba, ditambah utility external *jxplorer* yang merupakan editor LDAP berbasis Java.

Directory Administrator merupakan salah satu aplikasi administrasi LDAP yang populer untuk solusi single *sign-on*. Paket ini telah di-download lebih dari 20 ribu kopi dan telah dipaketkan bersama dengan berbagai distribusi Linux seperti Mandrake/Connectiva (Mandriva) Linux dan Debian Linux, serta berbagai distribusi Unix lainnya. Sayangnya, distribusi Fedora Core 2 ini tidak menyertakannya.



Gambar 5. Dialog Preferences dari Directory Administrator.

1. Install Directory Administrator:

```
# rpm -ivh directory_
administrator-1.6.0-1.i386.
rpm
```

2. Menjalankan Directory Administrator:

```
# directory_administrator
```

Dapat juga dijalankan melalui menu: *System Settings*|*Directory Administrator*.

- Akan muncul dialog "Welcome", tekan tombol "Next".

Professional 100% Linux Training & Solution

Ingin Menguasai Linux Secara LENGKAP ?!

Paket A-Z Linux

-Linux Concept & Fundamental
-Linux System Administration
-Linux Internet + Intranet Server
-Linux Security

56 hours (14 day @ 4 hours)

Only : Rp.4.850.000,-

Special Offer Crash Programme !

PATIN (Paket Intensif)

-Linux Concept and Fundamental
-Linux System Administration
-Linux Internet + Intranet Server
42 hours (6 days@ 7 hour)

Only : Rp.3.750.000,-

PAKIS (Paket Ekonomis)

-Linux Concept and Fundamental
-Linux System Administration
-Linux Internet + Intranet Server.
44 hours (11 days@ 4 hour)

Only : Rp.3.650.000,-

Ketik: Info PATIN atau Info PAKIS kirim SMS ke 0856 7771030 SMS Server powered by eSMSis (www.eSMSis.com)

SMS Server & Gateway



Linuxindo

PUSAT : Wisma Bisnis Indonesia Suite #415 - JAKARTA
BANDUNG: (022) 7234192 - CIREBON: (0231) 200418 - SOLO: (0271) 662318

PERINGATAN ! Linux bisa membuat Anda kecanduan, menambah PD dan belum ada obatnya. Tidak Setiap Paket Promosi tersedia di Cabang.

MySMSPass

Start Making Money from your Website!

- SMS Autentication System for Web Content
- Short Number by Telco Operators

Demo Website : www.InfoLINUX.web.id/sections

(021) 5362390
www.Linuxindo.com

- Profil name dapat diisi nama domain (misalnya dynre). Tekan tombol "Next".
- Server address diisi alamat ip server LDAP (ldap.dynre.com).
- Search base diisi attribut base dari domain LDAP (dc=dynre,dc=com).
- Kosongkan opsi "Enable TLS", karena server LDAP tidak menggunakan enkripsi.
- Tekan tombol "Next".
- Connection DN (user name) diisi DN user untuk koneksi (uid=root,ou=people,dc=dynre,dc=com).
- Password for the DN diisi password dari DN (diisi password root).
- Tekan tombol "Next".
- Tekan tombol "Test Connection". Jika semua konfigurasi benar akan keluar dialog "The connection was successful".
- Tekan tombol "Next".
- Tekan tombol "Finish" untuk mengakhiri proses setup awal penggunaan Directory Administrator ini.

Konfigurasi opsi preferensi:

- Pilih menu "Settings" -> "Preferences..."
- Pilih tab "Compatibility"
- Pilih "Store them as an MD5 hash (non standard, more secure)"
- Disable "Use the authPassword attribute when saving passwords"

Untuk melakukan administrasi user, tekan tombol "Connect", maka seluruh icon

user dan group akan keluar. User-user dan group-group tersebut berasal dari file `/etc/passwd` dan `/etc/group` yang telah di-convert ke dalam database LDAP.

Administrator dengan mudah dapat menambah, mengubah, dan menghapus user dan group yang ada tersebut.

Perhatikan pada saat menambah user baru:

- Kosongkan opsi "Grant access to all computers in the network", karena objectClass account tidak dibuat pada saat migrasi awal. Kemudian dalam dialog "Access Control information" tersebut akan muncul kotak isian hostname. Tetap kosongkan kotak isian tersebut.
- Kosongkan pula opsi "This user logs in from Windows workstation", karena struktur schema samba belum dimasukkan dalam file `/etc/openldap/slapd.conf`.

Sebagai evaluasi pencocokan konfigurasi, pilih Menu "Directory" | "Manage Profiles..." kemudian ditekan tombol "Modify profile". Akan tampil seperti gambar 6.

Autentifikasi servis-servis lainnya

Sistem autentifikasi di Linux menggunakan prinsip modular, dalam hal ini contohnya PAM (*Password Authentication Module*). PAM ini menyediakan library interface umum sebagai perantara antara modul-modul autentifikasi dan aplikasi yang menggunakannya. Modul PAM yang ber-

fungsi sebagai modul autentifikasi LDAP (file bernama `pam_ldap`) telah diinstall secara otomatis dalam paket RPM `nss_ldap-217-1.i386.rpm` pada saat instalasi awal distribusi Fedora Core 2.

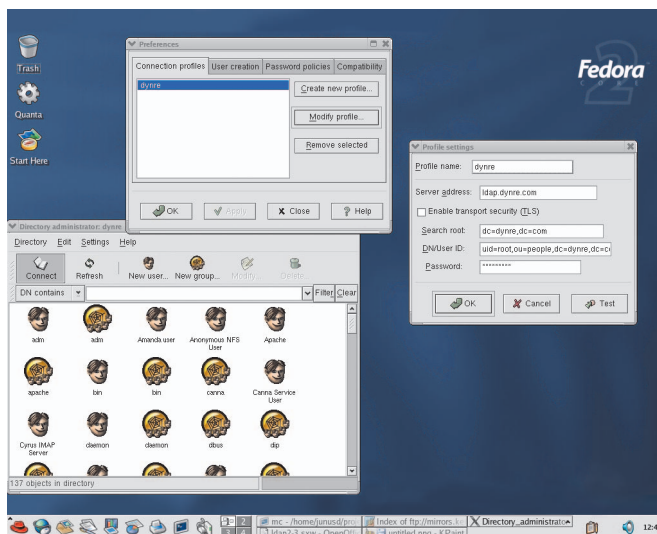
Jadi, semua mesin client telah terkonfigurasi melalui utility "setup" di atas, maka servis-servis di dalamnya seperti ftp, email dan servis-servis lainnya secara otomatis mendapatkan data username dan password dari server LDAP, tanpa perlu melakukan perubahan konfigurasi tambahan.

Perlu diingat, karena utility seperti Directory Administrator hanya menambahkan data user ke LDAP database saja tanpa membuat direktori `/home/user` bagi user tersebut secara lokal, maka perlu membuat direktori bagi user tersebut secara manual pada tiap-tiap mesin client. Atau cukup sekali saja dibuat direktori `/home/user` tersebut kemudian di-sharing-kan dengan menggunakan protokol NFS.

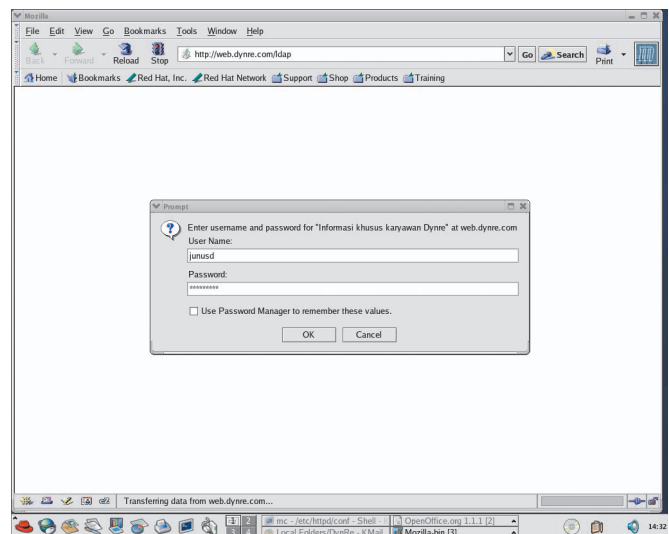
Masalah direktori `/home/user` ini penting bagi servis ftp yang mengijinkan tiap user untuk mengakses direktori home-nya. Juga penting bagi email server yang di dalam direktori `/home/user` terdapat file-file konfigurasi misalnya seperti `.forward` bagi tiap user-nya.

Contoh autentifikasi server web

Secara default, konfigurasi server web Apache pada Fedora Core 2 tidak seperti servis-servis ftp, email ataupun yang lainnya yang menggunakan modul autentifi-



Gambar 6. Contoh konfigurasi pada Directory Administrator.



Gambar 7. Hasil tes web browser ke alamat `http://web.dynre.com/ldap`.

kasi PAM. Oleh karena itu, di bawah ini dijelaskan cara mengonfigurasinya agar Apache terkoneksi menggunakan modul autentikasi LDAP.

- Ekstrak file paket source code:

```
# tar xvfz mod_auth_pam-2.0-1.1.1.tar.gz
```

- Kemudian masuk ke dalam direktori mod_auth_pam, lalu lakukan kompilasi dan install:

```
# make
# make install
```

- Hasil perintah di atas, mod_auth_pam, so akan terinstall di dalam direktori /usr/lib/httpd/modules.

- Edit file /etc/pam.d/httpd, ubah dua baris di bawah ini. Setelah itu mod_auth_pam.so siap untuk digunakan.

```
auth required pam_stack.so service=system-auth
account required pam_stack.so service=system-auth
```

Contoh, misalnya alamat website http://web.dynre.com/ldap ini tidak dapat dibuka oleh semua orang umum. Hanya karyawan kantor saja yang boleh membukanya. Maka setiap kali user akan melihat alamat website tersebut, user diharuskan memasukkan password terlebih dahulu. Konfigurasinya sebagai berikut:

- Edit file /etc/httpd/conf/httpd.conf:

Pada bagian LoadModule tambahkan satu baris berikut ini:

```
LoadModule auth_pam_module
modules/mod_auth_pam.so
```

Bagian akhir file httpd.conf ini, tambahkan beberapa baris di bawah. Di sini dimisalkan direktori yang akan diproteksi secara fisik adalah /var/www/ldap.

```
Alias /ldap/ /var/www/ldap/
<Location "/ldap">
    AuthName "Informasi
    khusus karyawan Dynre"
    AuthType Basic
    Require valid-user
</Location>
```

Untuk mengatur hanya user tertentu atau group tertentu yang boleh masuk, dapat menggunakan parameter "Require user username" dan "Require group groupname". Keterangan lebih lanjut parameter Require dapat dilihat pada alamat website: http://httpd.apache.org/docs/mod/core.html#require

- Restart httpd (daemon server web):

```
# service httpd restart
```

- Tes dengan menggunakan web browser ke alamat http://web.dynre.com/ldap. Hasilnya terlihat pada gambar 7, tiap user yang akan melihat alamat tersebut akan diminta memasukkan username dan password.

Pada InfoLinux edisi selanjutnya (bagian ketiga) akan menjelaskan tentang cara setup Samba versi 3 dengan LDAP sebagai servis informasi direktori serta cara-cara administrasinya. 🐧

Junus Djunawidjaja (junusd@dynre.com)

Pelopor Training LINUX Indonesia Mewujudkan Kepercayaan Anda dengan:

Program Intensif LINUX Profesional

Linux Server Development ⌚ 200 jam

MATERI :

- **Hardware & Jaringan**
Komponen & Konfigurasi Komputer, Setup & Membuat LAN
- **Linux Fundamental**
Basic User, X-Window, System Administration & Networking
- **Internet & Aplikasi WEB**
Browser, Search Engine, Email, FTP, HTML, CSS & JavaScript
- **Shell Programming**
- **Advanced System Administration**
- **Advanced Networking Administration**
- **PHP & MySQL**

KARIER KELULUSAN:

- IT Division pada perusahaan yang menggunakan komputer dlm menyelesaikan pekerjaan sehari-hari
- Support System Administration & Networking
- ISP (Internet Service Provider) ● WEB Hosting
- Warnet Development ● System Integration

FASILITAS

- ☺ Ruang kuliah full AC
- ☺ Tiap peserta 1 PC, Min PIII, Ram 128, Network & Multimedia
- ☺ Internet
- ☺ Modul Pelatihan
- ☺ Cotton Bag
- ☺ T-Shirt Exclusive
- ☺ CD Linux
- ☺ Block Notes
- ☺ Disket
- ☺ Sertifikat

JADUAL

- ☞ Senin s.d. Kamis (3 bulan)
- ☞ Sabtu & Minggu (6 bulan)
- ⌚ Jam: 08.00 s.d 12.00 WIB.
- ⌚ Jam: 13.30 s.d. 18.00 WIB.

Migrasi Ke Linux

- Server
- Network & System Support
- Web & Desktop Application



LEMBAGA PENDIDIKAN KOMPUTER NURUL FIKRI

- Jl. Margonda Raya No. 522 - **Depok** ☎/Fax. (021) 7874223-24, 77206991
- Jl. Mampang Prapatan X/4 **Jakarta Selatan** ☎ (021) 7947115, 7975235, 7901205
- Jl. A. Yani - Sentra Niaga B.I/12, **Bekasi** ☎/Fax. (021) 88956879, 8853537
- Jl. Kopi No. 23A / Depan UNILA (Komp. Yys. Darul Hikmah)
Gedong Meneng - **Bandar Lampung** ☎ (0721) 7425345, 747403

BERKUALITAS

TERPILP
LPKNF

www.pilp.web.id
www.nurulfikri.com
info@nurulfikri.com

Integrasi User Account dengan LDAP

Bagian 3 dari 3 Artikel

Fungsi utama komputer server di kantor ukuran kecil dan menengah biasanya sebagai file dan printer server. Samba sangat penting keberadaannya sebagai pengganti Windows Server yang populer dengan kemampuannya sebagai file dan printer server.

Perkantoran menggunakan file server sebagai pusat tempat untuk menyimpan file yang gunanya untuk men-share file, memberikan keamanan/*security* kepada file-file tersebut karena letaknya tersentralisasi, dan membuat proses *back-up* data lebih efisien. Sedangkan sebagai printer server, ini akan menghemat printer yang dibeli karena tidak perlu semua komputer di kantor dibelikan printer satu-satu.

Bagian ketiga seri tulisan ini akan menjelaskan cara men-*setting* Samba versi 3 dengan menggunakan LDAP sebagai servis informasi direktori serta cara-cara administrasinya. Berikut adalah kebutuhan sebelum kita memulai setting LDAP untuk Samba:

- Artikel ini hanya menekankan penggunaan LDAP bagi Samba sebagai servis autentikasi user. Pembaca diharapkan telah menguasai kemampuan administrasi dasar Samba.
- Server LDAP di-*setting* sesuai artikel kedua.
- Samba domain yang digunakan ialah *dynre*. Nama domain ini dapat diganti disesuaikan dengan nama domain pada sistem komputer pembaca.
- Mesin bernama *samba.dynre.com* dikonfigurasi sebagai Primary Domain Controller (PDC). Servis Samba ini dapat diletakkan pada dua mesin yang terpisah seperti yang dijelaskan dalam

artikel kedua pada bagian “Konfigurasi Jaringan” ataupun di dalam satu mesin dengan LDAP server.

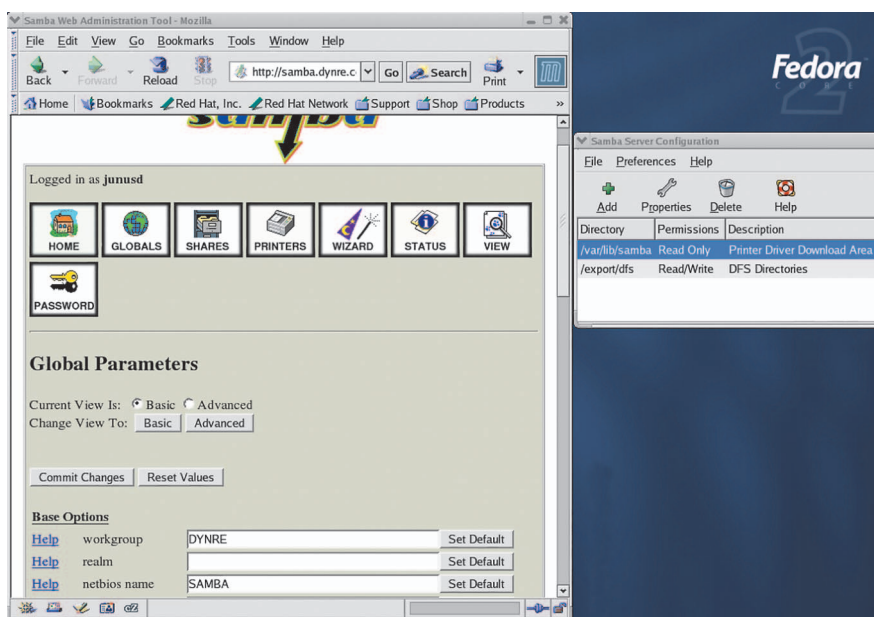
Kebutuhan software

Seluruh kebutuhan paket RPM Samba ini tersedia di dalam CD Fedora Core 2.

- *samba-common-3.0.3-5.i386.rpm* (tersedia dalam CD 1), berisi file-file Samba umum yang harus diinstal terlebih dahulu sebelum paket RPM Samba yang lainnya.
- *samba-client-3.0.3-5.i386.rpm* (tersedia dalam CD 1), berisi file-file Samba client saja. Untuk mesin yang akan digunakan sebagai mesin samba client saja, cukup menginstal paket RPM ini, tidak perlu menginstal paket RPM berikutnya yaitu paket RPM Samba server.
- *samba-3.0.3-5.i386.rpm* (tersedia dalam CD 1), berisi file-file Samba daemon server. Di dalam paket RPM ini terdapat utility *smblldap* yang akan digunakan untuk administrasi user-user Samba server yang terkoneksi dengan LDAP server.

Selain paket RPM Samba di atas, di dalam distribusi Fedora Core 2 ini terdapat utility yang akan mempermudah administrasi Samba:

- *system-config-samba-1.2.9-2.noarch.rpm* (tersedia dalam CD 1), berisi utility administrasi Samba berbasis grafis.
- *samba-swat-3.0.3-5.i386.rpm* (tersedia dalam CD 4), berisi utility administrasi berbasis web yang menggunakan protokol HTTP dengan port 901.



Gambar 1. Samba SWAT dan system-config-samba.

Kedua utility administrasi Samba ini berguna untuk mempersiapkan konfigurasi dasar Samba sebelum kita men-settingnya menggunakan LDAP sebagai autentikasi servis. Contoh kedua utility administrasi ini dapat dilihat pada gambar 1.

Sangat dianjurkan untuk selalu men-update Samba ini dengan versi yang terbaru karena versi yang terbaru memperbaiki bug-bug yang cukup penting bagi sistem komputer produksi. Untuk mempermudah proses konfigurasi, maka semua paket RPM diambil dari CD Fedora Core 2. Pada saat artikel ini dibuat Samba terbaru dapat di-download dari www.samba.org. Perlu diingat, jika meng-compile sendiri, harap memasukkan module LDAP ke dalam module binari samba. Untuk mengecek apakah samba telah terkompilasi dengan module LDAP di dalamnya ketikkan perintah berikut:

```
# smbld -b | grep -i ldap
```

Hasilnya akan demikian:

```
HAVE_LDAP_H
HAVE_LDAP
HAVE_LDAP_DOMAIN2HOSTLIST
HAVE_LDAP_INIT
HAVE_LDAP_INITIALIZE
HAVE_LDAP_SET_REBIND_PROC
HAVE_LIBLDAP
LDAP_SET_REBIND_PROC_ARGS
pdb_ldap pdb_smbpasswd pdb_
tdbsam pdb_guest rpc_lsa rpc_reg
rpc_lsa_ds rpc_wks rpc_net rpc_
dfs rpc_srv rpc_spoolss rpc_samr
idmap_ldap idmap_tdb auth_rhosts
auth_sam auth_unix auth_winbind
auth_server auth_domain auth_
builtin
```

Sedangkan utility smbldap dapat di-download dari www.idealx.org/prj/samba/index.en.html.

Proses konfigurasi

Diasumsikan servis Samba telah terinstal dan terkonfigurasi secara dasar sebagai file dan printer server. Dengan keadaan demikian, berarti servis Samba tersebut secara default menggunakan file tdb yang berada pada local server sebagai autentikasi data. Pada bagian ini, kita akan mulai untuk mengonfigurasi koneksi ke LDAP server sebagai autentikasi server.

1. Buka file `/etc/samba/smb.conf`, lalu tambahkan lima baris berikut ini:

```
passdb backend = ldapsam:
"ldap://ldap.dynre.com"
```

➔ Ini data autentikasi password yang digunakan untuk menyimpan dan mengubah password menggunakan LDAP dengan LDAP server: `ldap.dynre.com`.

```
ldap suffix = dc=erlangtech,
dc=com
```

➔ Ini data direktori LDAP kelompok bersuffiks `dc=erlangtech,dc=com` yang akan digunakan sebagai data direktori.

```
ldap admin dn = uid=root,ou=
people,dc=erlangtech,dc=com
```

➔ Account DN koneksi ke server LDAP untuk mengambil data password user.

```
ldap passwd sync = Yes
```

➔ Password LDAP akan disinkronisasikan dengan data password atribut NT dan LM, kemudian di-update atribut waktu `pwdLastSet`.

```
ldap delete dn = Yes
```

➔ Operasi delete dalam LDAP akan menghapus seluruh data untuk user account yang dipilih.

Berikut ini merupakan file konfigurasi `/etc/samba/smb.conf` dengan contoh konfigurasi dasar:

- Printer yang di-share menggunakan Cups daemon printer.
- Direktori yang di-share adalah direktori homes (`/home/junusd`) dan data (`/export/data`).

```
[global]
```

```
workgroup = DYNRE
netbios aliases = samba
server string = DynRe WinNT
Server
```

```
passdb backend = ldapsam:
"ldap://ldap.dynre.com"
```

```
ldap suffix = dc=dynre,
dc=com
```

```
ldap admin dn = uid=root,
ou=people,dc=dynre,dc=com
```

```
ldap passwd sync = Yes
```

```
ldap delete dn = Yes
```



```

domain admin group =
"@Domain Admins"

printcap name = cups
printing = cups

logon script = logon.bat
logon drive = H:
logon home =
logon path =

domain logons = Yes
os level = 33
preferred master = Yes
domain master = Yes
wins support = Yes
log file = /var/log/samba/
%m.log
[printers]
comment = All Printers
path = /var/spool/samba
browseable = No
guest ok = Yes
printable = Yes
use client driver = Yes
printer admin = root
[print$]
comment = Printer Driver
Download Area
path = /var/lib/samba
write list = root
guest ok = Yes
[homes]
comment = Home Directories
writeable = yes
browseable = No
[data]
comment = DFS Directories
path = /export/data
writeable = yes

```

2. Edit konfigurasi LDAP server.

Copy samba.schema ke direktori /etc/openldap/schema

```
# cp /usr/share/doc/samba-3.0.3/LDAP/samba.schema /etc/openldap/schema
```

Edit file /etc/openldap/slapd.conf

- Tambahkan samba.schema di bawah autofs.schema

```
include /etc/openldap/
schema/redhat/autofs.schema
```

```
include /etc/openldap/
schema/samba.schema
```

- Ubah ACL, setiap ada perintah untuk membaca dan menulis attribut sambaLMPassword dan sambaNTPassword, diharuskan untuk autentifikasi lebih dahulu, sama seperti mengakses atribut userPassword.

```

access to attr=userPassword,
sambaLMPassword,
sambaNTPassword
    by dn="uid=root,ou=people,
dc=dynre,dc=com" write
    by self write
    by anonymous auth
access to *
    by dn="uid=root,ou=people,
dc=dynre,dc=com" write
    by self write
    by users read
    by anonymous read

```

3. Masukkan password DN admin yang digunakan untuk mengambil data user account dari LDAP server.

```
# smbpasswd -w ldappassword
(uid=root,ou=people,dc=dynre,dc=com)
```

4. Restart daemon servis LDAP dan Samba.

```
# service ldap start
# service smb start
```

Administrasi user dengan smbldap

Bagian ini menjelaskan secara praktis cara penggunaan utility smbldap yang siap digunakan untuk keperluan administrasi user samba sehari-hari. Sebagai referensi smbldap lebih detail dapat dibaca dari www.idealx.org/prj/samba/samba-ldap-howto.pdf.

Konfigurasi awal

- Edit /usr/share/doc/samba-3.0.3/LDAP/smbldap-tools/smbldap_conf.pm, dengan mengubah variabel berikut:

```

$slaveLDAP = "ldap.dynre.com";
$slavePort = "389";
$masterLDAP = "ldap.dynre.com";
$masterPort = "389";
$ldapSSL = "0";
$suffix = "dc=DYNRE,dc=COM";
$usersou = q(People);
$computersou = q(Computers);

```

```

$groupsou = q(Group);
$bindpasswd = "ldappassword
(uid=root,ou=people,dc=dynre,
dc=com)";
$mk_ntpasswd = "/usr/sbin/
mkntpwd";

```

- Copy skrip smbldap ke direktori /usr/sbin:

```

cd /usr/share/doc/samba-
3.0.3/LDAP/smbldap-tools
cp smbldap*.p? /usr/sbin
chmod 753 /usr/sbin/smbldap_
conf.pm
chmod 750 /usr/sbin/smbldap*.
pl
chgrp 512 /usr/sbin/smbldap*.
p?

```

- Compile utility pembuat password yang compatible dengan WinNT password mkntpwd:

```

# cd /usr/share/doc/samba-
3.0.3/LDAP/smbldap-tools/
mkntpwd
# make
# cp mkntpwd /usr/sbin

```

- Jalankan smbldap-populate.pl, untuk inisialisasi LDAP database dengan user dan group account yang diperlukan untuk administrasi sesuai Windows NT:

```
# smbldap-populate.pl
```

Hasil *output*-nya akan terlihat seperti di bawah. Ada beberapa pesan kesalahan tetapi itu tidak menjadi masalah karena struktur data kelompok LDAP tersebut telah dibuat pada pembahasan artikel kedua:

```

Using builtin directory
structure
adding new entry:
dc=DYNRE,dc=COM
failed to add entry: Already
exists at ./smbldap-populate.
pl line 323, <GEN1> line 2.
adding new entry: ou=People,
dc=DYNRE,dc=COM
failed to add entry: Already
exists at ./smbldap-populate.
pl line 323, <GEN1> line 3.
adding new entry:
ou=Group,dc=DYNRE,dc=COM
failed to add entry: Already
exists at ./smbldap-populate.

```



```
pl line 323, <GEN1> line 4.
adding new entry:
ou=Computers,dc=DYNRE,dc=COM
adding new entry:
uid=Administrator,ou=People,
dc=DYNRE,dc=COM
adding new entry: uid=nobody,
ou=People,dc=DYNRE,dc=COM
failed to add entry: Already
exists at ./smbldap-populate.
pl line 323, <GEN1> line 7.
adding new entry: cn=Domain
Admins,ou=Group,dc=DYNRE,dc=COM
adding new entry: cn=Domain
Users,ou=Group,dc=DYNRE,dc=COM
adding new entry: cn=Domain
Guests,ou=Group,dc=DYNRE,dc=COM
adding new entry:
cn=Administrators,ou=Group,
dc=DYNRE,dc=COM
adding new entry: cn=Users,
ou=Group,dc=DYNRE,dc=COM
failed to add entry: Already
exists at ./smbldap-populate.
pl line 323, <GEN1> line 12.
```

```
adding new entry: cn=Guests,
ou=Group,dc=DYNRE,dc=COM
adding new entry: cn=Power
Users,ou=Group,dc=DYNRE,dc=COM
adding new entry: cn=Account
Operators,ou=Group,dc=DYNRE,
dc=COM
adding new entry: cn=Server
Operators,ou=Group,dc=DYNRE,
dc=COM
adding new entry: cn=Print
Operators,ou=Group,dc=DYNRE,
dc=COM
adding new entry: cn=Backup
Operators,ou=Group,dc=DYNRE,
dc=COM
adding new entry: cn=Replicat
or,ou=Group,dc=DYNRE,dc=COM
adding new entry: cn=Domain
Computers,ou=Group,dc=DYNRE,
dc=COM
```

Administrasi user

Perintah-perintah untuk administrasi user dan group ini sintaksnya sangat mirip de-

ngan perintah standar untuk administrasi user dalam Linux, seperti userdel, useradd, dan usermod. Hanya di sini ditambah beberapa parameter yang khusus untuk samba.

- **smbldap-usermod.pl**: memodifikasi user account yang ada.

User account Linux dalam LDAP server yang dibuat tanpa menggunakan utility smbldap ini tidak akan mempunyai objectclass sambaSamAccount. Dalam artikel kedua telah terdapat user account junusd, tetapi user account ini tidak dapat digunakan untuk login ke Samba server sebelum ditambahkan objectclass sambaSamAccount, lalu masukkan password:

```
# smbldap-usermod.pl -a junusd
# smbldap-passwd.pl junusd
```

- **smbldap-useradd.pl**: menambah user dan komputer account.

Pada Samba, jika di-setting konfigurasinya menyerupai Windows NT, nama workstation terlebih dahulu harus ditambahkan ke server melalui smbldap-useradd.pl -w ini. Jadi utility smbldap ini berguna untuk



LEMBAGA PENDIDIKAN KOMPUTER NURUL FIKRI

Membangun Internet Sharing, Proxy dan Billing Internet Berbasis Linux Untuk Warnet

WORKSHOP SEHARI



TARGET

Para Peserta Workshop akan mampu membangun internet sharing dan Proxy berbasis sistem operasi Linux serta mampu menginstal dan mengkonfigurasi billing warnet di Linux.

BIAYA

■ Rp. 250.000,-

WAKTU & TEMPAT

09.00 s.d. 16.00 WIB.

LPKNF - DEPOK

Jum'at, 9 September 2005

LPKNF - JAKARTA

Jum'at, 16 September 2005

LPKNF - BEKASI

Jum'at, 23 September 2005

FASILITAS

- ☺ 1 PC untuk 1 peserta
- ☺ CD Linux & Software
- ☺ NF Billing Warnet
- ☺ Modul + Block notes
- ☺ Coffee Break
- ☺ Makan Siang

Linux Server Development 200jam

FASILITAS

- ☺ Ruang kuliah full AC
- ☺ Tiap peserta 1 PC, Min PIII, RAM 128, Network & Multimedia
- ☺ Internet
- ☺ Cotton Bag
- ☺ T-Shirt Exclusive
- ☺ Modul Pelatihan
- ☺ CD Linux
- ☺ Block Notes
- ☺ Disket
- ☺ Sertifikat



Waktu Belajar

☺ Hari: Senin s.d. Kamis
☺ Jam: 08.00 s.d 12.00 WIB.

Discount 25%



PILP CERIA

Hardware & Jaringan
Linux Fundamental
Internet & Aplikasi WEB
Shell Programming
Advanced System Administration
Advanced Networking Administration
PHP & MySQL

- Jl. Margonda Raya No. 522 - **Depok** ☎/Fax. (021) 7874223-24, 77206991
- Jl. Mampang Prapatan X/4 **Jakarta Selatan** ☎ (021) 7947115, 7975235, 7901205
- Jl. A. Yani - Sentra Niaga B.I/12, **Bekasi** ☎/Fax. (021) 88956879, 8853537
- Jl. Kopi No. 23A / Depan UNILA (Komp. Yys. Darul Hikmah)
Gedong Meneng - **Bandar Lampung** ☎ (0721) 7425345, 747403

www.pilp.web.id
www.nurulfikri.com
info@nurulfikri.com

administrasi user account dan komputer account. Itu berlaku untuk setiap mesin workstation yang terkoneksi ke server.

- *smbldap-userdel.pl*: menghapus user dan komputer account.
- Selain bertujuan utama menghapus user account, komputer account dapat dihapus dengan menyebutkan nama komputer account tersebut.
- *smbldap-usershow.pl*: menampilkan user account tertentu.

Administrasi group

- *smbldap-groupmod.pl*: memodifikasi group yang ada.
 - Group Linux dalam LDAP server yang dibuat tanpa menggunakan utility *smbldap* ini tidak akan mempunyai objectclass *sambaGroupMapping*. Dalam artikel kedua, telah terdapat group users, tetapi group ini tidak dapat digunakan sebagai group Samba sebelum ditambahkan objectclass *sambaGroupMapping*:
- ```
smbldap-groupmod.pl -a users
```
- *smbldap-groupadd.pl*: menambah group.
  - *smbldap-groupdel.pl*: menghapus group.
  - *smbldap-usershow.pl*: menampilkan group tertentu.

### Migrasi dari Windows NT

Migrasi Windows NT server yang telah bertahun-tahun ada dalam kantor dapat dilakukan menjadi Samba server, dengan tetap

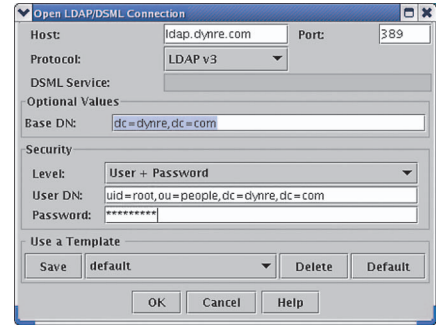
mempertahankan user, group, dan komputer account yang ada di Windows NT. Setelah proses migrasi selesai, tidak terjadi perubahan sama sekali di sisi mesin-mesin workstation client, atau transparan. Hal ini sangat penting untuk meminimalkan komplain dari user. Jika berhasil dengan baik, kemudian pemindahan file-file data yang ada, printer driver, dan ACL atribut sekuriti yang ada juga berlangsung dengan lancar, akan membuat user tanpa sadar telah menggunakan Samba sebagai pengganti Windows NT server.

Di sini tidak diberikan secara detail caranya, hanya diberikan garis besarnya untuk menghindari kompleksitas artikel ini.

- Pada Windows NT server, login sebagai Administrator, lalu jalankan utility *pwdump* yang bisa didownload dari <ftp://ftp.samba.org/pub/samba/pwdump/>.
- Kemudian file teks hasil *pwdump* ini di-copy ke mesin Samba, lalu jalankan *smbldap-migrate-accounts.pl* dan *smbldap-migrate-groups.pl*.
- Terakhir, dengan teliti dan hati-hati sesuaikan uid dan gid dari tiap-tiap user dan group account yang telah ada di Linux dengan user dan group account yang ada pada Windows NT.

### Administrasi user dengan JXplorer

JXplorer merupakan utility LDAP browser berbasis Java. Sebelum menjalankan utility ini, terlebih dahulu download JRE (Java Runtime Environment) dari [www.javasoft.com](http://www.javasoft.com).



Gambar 2. JXplorer dialog koneksi.

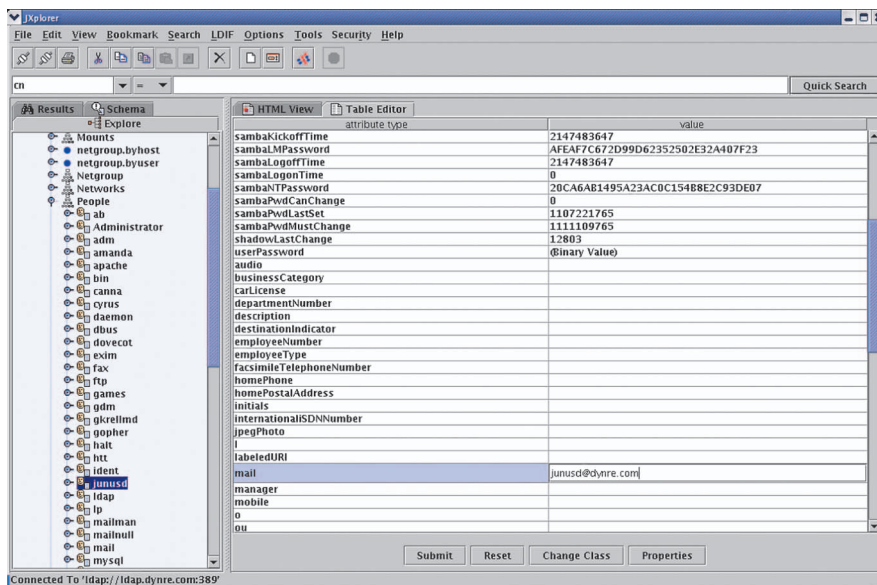
com. Sedangkan JXplorer dapat di-download dari [www.pegacat.com/jxplorer](http://www.pegacat.com/jxplorer). Melalui utility ini atribut tiap item dalam direktori dapat ditambah, dihapus, maupun dimodifikasi langsung secara manual.

Berikut ini contoh untuk mengedit alamat email dari user *junusd*. Melalui contoh ini, pembaca dapat mengubah atribut-atribut lainnya sesuai dengan yang dikehendaki.

- Jalankan *jxplorer.sh*, kemudian ke menu "File" -> "Connect"
- Ketikkan account untuk koneksi ke LDAP server seperti tampak dalam gambar 2.
  - Host: *ldap.dynre.com*
  - Base DN: *dc=dynre,dc=com*
  - Level: *User + Password*
  - User DN: *uid=root,ou=people,dc=dynre,dc=com*
  - Password: *"ldappassword(uid=root,ou=people,dc=dynre,dc=com)"*
- Tekan tombol "OK". Hasilnya seperti gambar 3.
- Pada pohon (tree), klik kelompok "People", lalu klik "*junusd*", lalu klik Tab "Table Editor" pada bagian kanan atas.
- Pada atribut "mail" ketik alamat e-mail.
- Tekan tombol "Submit".

Dalam ketiga artikel telah dijelaskan cara penggunaan servis direktori LDAP sebagai pusat autentifikasi user account, sehingga seluruh data user account pada sistem komputer pada perkantoran terintegrasi secara penuh. Namun, manfaat LDAP ini tidak hanya tertutup sebagai pusat autentifikasi user account saja. Masih ada manfaat lain dari LDAP yang pada pokoknya merupakan servis yang berfungsi memberikan informasi direktori. Misalnya, sebagai informasi direktori karyawan, *address book* dari aplikasi e-mail, dan sebagainya. 📧

**Junus Djunawidjaja** ([junusd@dynre.com](mailto:junusd@dynre.com))



Gambar 3. Modifikasi atribut alamat email dengan JXplorer.