

KODE MODUL

NTW.MNT.300.(3).A'



SEKOLAH MENENGAH KEJURUAN
BIDANG KEAHLIAN TEKNOLOGI INFORMASI DAN KOMUNIKASI
PROGRAM KEAHLIAN TEKNIK KOMPUTER DAN JARINGAN

Mengadministrasi Server dalam Jaringan



PENYUSUN
TIM PENULIS MODUL DIKMENJUR

BAGIAN PROYEK PENGEMBANGAN KURIKULUM
DIREKTORAT PENDIDIKAN MENENGAH KEJURUAN
DIREKTORAT JENDERAL PENDIDIKAN DASAR DAN MENENGAH
DEPARTEMEN PENDIDIKAN NASIONAL
2005

KODE MODUL

NTW.MNT.300.(3).A*



SEKOLAH MENENGAH KEJURUAN
BIDANG KEAHLIAN TEKNOLOGI INFORMASI DAN KOMUNIKASI
PROGRAM KEAHLIAN TEKNIK KOMPUTER DAN JARINGAN

Mengadministrasi Server dalam Jaringan

PENYUSUN

TIM PENULIS MODUL DIKMENJUR

1. Deni Warsa
2. Drs. Mahyunus, MT
3. Adi Purwanto, Iina ilai
4. Adnan Purwanto S
5. Drs. Bekti Afianto
6. Drs. T. Adi Wijaya, MT

BAGIAN PROYEK PENGEMBANGAN KURIKULUM
DIREKTORAT PENDIDIKAN MENENGAH KEJURUAN
DIREKTORAT JENDERAL PENDIDIKAN DASAR DAN MENENGAH
DEPARTEMEN PENDIDIKAN NASIONAL

2005

KATA PENGANTAR

Modul dengan judul “ **Mengadministrasi Server dalam Jaringan** ” merupakan bahan ajar yang digunakan sebagai panduan praktikum peserta diklat Sekolah Menengah Kejuruan (SMK) untuk membentuk salah satu bagian dari kompetensi bidang keahlian Teknologi Informasi dan Komunikasi pada Program Keahlian Teknik Komputer dan Pengelolaan Jaringan.

Modul ini menguraikan tentang langkah-langkah yang diperlukan untuk mengadministrasi server dalam jaringan dimulai dari persiapan yang diperlukan sampai dengan pelaporan hasil mengadministrasi server dalam jaringan. Modul ini terdiri dari 6 kegiatan belajar. Kegiatan Belajar 1 membahas tentang mengidentifikasi jenjang pengguna dan aplikasi pada jaringan , Kegiatan Belajar 2 membahas tentang mengatur service yang berjalan pada server , Kegiatan Belajar 3 membahas tentang mengecek kondisi server berdasarkan log file Kegiatan Belajar 4 membahas tentang mengisi log sheet / report sheet , kegiatan belajar 5 membahas tentang security dan kegiatan 6 melaporkan hasil mengadministrasi Server.

Modul ini terkait dengan modul-modul lain yang membahas tentang Melakukan Administrasi Server. Oleh karena itu, sebelum menggunakan modul ini peserta diklat diwajibkan telah mengambil modul tersebut.

Tangerang, Nopember 2005

Penyusun

DAFTAR ISI MODUL

	Halaman
HALAMAN DEPAN	i
HALAMAN DALAM	ii
KATA PENGANTAR	iii
DAFTAR ISI MODUL	iv
PETA KEDUDUKAN MODUL	vi
PERISTILAHAN / GLOSSARY	viii
I. PENDAHULUAN	1
A. DESKRIPSI JUDUL.....	1
B. PRASYARAT	1
C. PETUNJUK PENGGUNAAN MODUL	
1. Petunjuk Bagi Siswa	
2. Peran Guru	
D. TUJUAN AKHIR	
E. KOMPETENSI	
F. CEK KEMAMPUAN	
II. PEMELAJARAN	
A. RENCANA PEMELAJARAN SISWA	
B. KEGIATAN BELAJAR	
1. Kegiatan Belajar 1 : membahas tentang mengidentifikasi jenjang pengguna dan aplikasi pada jaringan	
a. Tujuan Kegiatan Pemelajaran	
b. Uraian Materi 1	
c. Rangkuman 1	
d. Tugas 1	
e. Tes Formatif 1	
f. Kunci Jawaban Formatif 1.....	
g. Lembar Kerja 1	
2. Kegiatan Belajar 2 : mengatur service yang berjalan pada server	
a. Tujuan Kegiatan Pemelajaran	
b. Uraian Materi 2.....	
c. Rangkuman 2	
d. Tugas 2	

- e. Tes Formatif 2
- f. Kunci Jawaban Formatif 2.....
- g. Lembar Kerja 2
- 3. Kegiatan Belajar 3 : mengecek kondisi server berdasarkan log file

 - a. Tujuan Kegiatan Pembelajaran
 - b. Uraian Materi 3.....
 - c. Rangkuman 3.....
 - d. Tugas 3
 - e. Tes Formatif 3.....
 - f. Kunci Jawaban Formatif 3.....
 - g. Lembar Kerja 3.....

- 4. Kegiatan Belajar 4 : tentang mengisi log sheet / report sheet.....

 - a. Tujuan Kegiatan Pembelajaran
 - b. Uraian Materi 4.....
 - c. Rangkuman 4.....
 - d. Tugas 4
 - e. Tes Formatif 4.....
 - f. Kunci Jawaban Formatif 4.....
 - g. Lembar Kerja 4.....

- 5. Kegiatan Belajar 5 : tentang Security

 - a. Tujuan Kegiatan Pembelajaran
 - b. Uraian Materi 5.....
 - c. Rangkuman 5.....
 - d. Tugas 5
 - e. Tes Formatif 5.....
 - f. Kunci Jawaban Formatif 5.....
 - g. Lembar Kerja 5.....

- 6. Kegiatan Belajar 6 : tentang Melaporkan hasil Administrasi Server.....

 - a. Tujuan Kegiatan Pembelajaran
 - b. Uraian Materi 6.....
 - c. Rangkuman 6.....
 - d. Tugas 6
 - e. Tes Formatif 6.....

- f. Kunci Jawaban Formatif 6.....
- g. Lembar Kerja 6.....

III. EVALUASI

A. PERTANYAAN

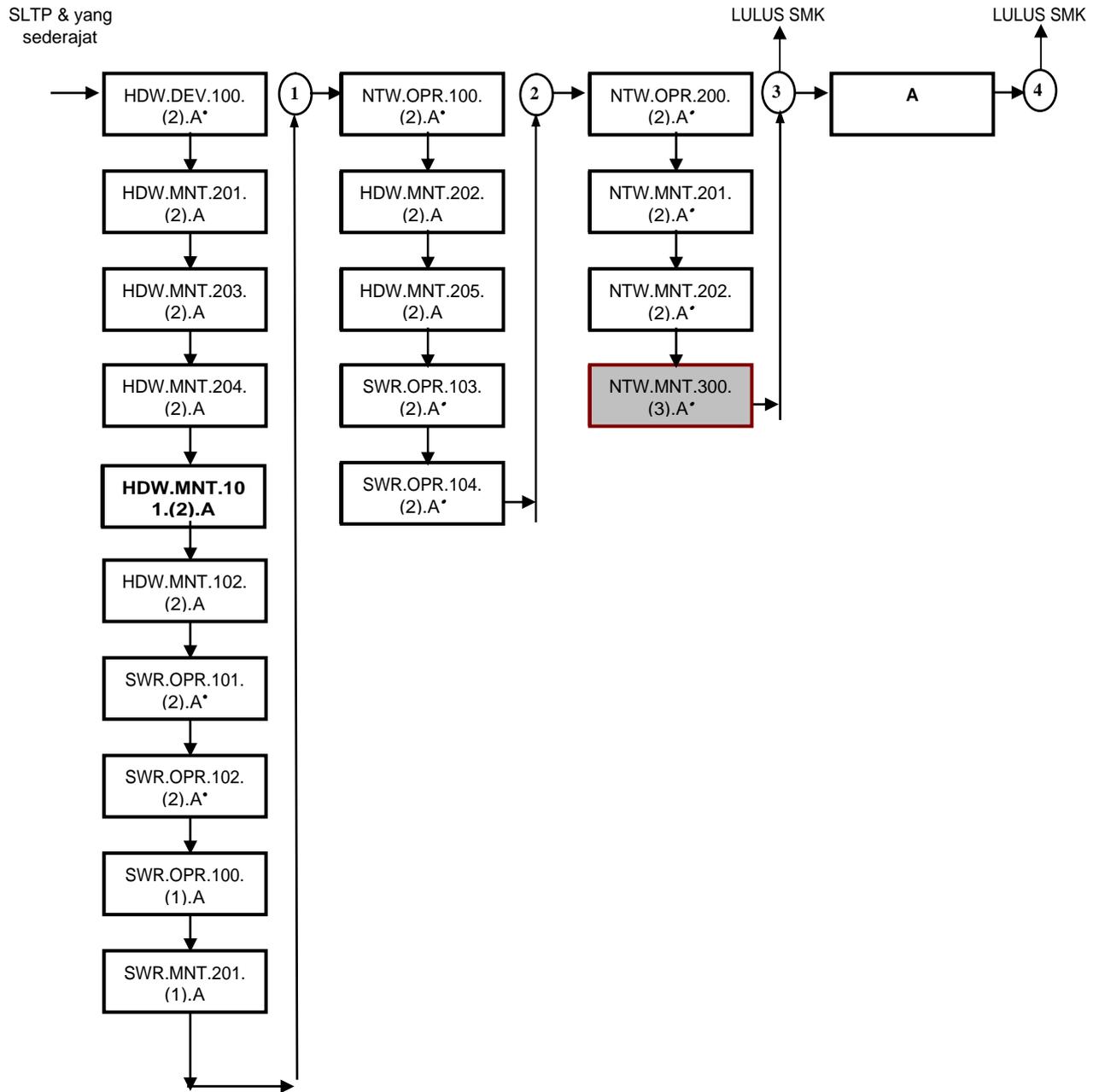
B. KUNCI JAWABAN EVALUASI

C. KRITERIA KELULUSAN

IV. PENUTUP

DAFTAR PUSTAKA

PETA KEDUDUKAN MODUL



PERISTILAHAN/GLOSSARY

LAN	:	Lokal Area Network
WAN	:	Wide Area Network
Scandisk	:	adalah tol yang digunakan untuk memeriksa struktur file system
Disk defiragmeter	:	tool yang digunakan untuk mengatur struktur atau tat letak file sehingga akan mengurangi fragmentasi sebuah space hardisk.
VGA card	:	komponen computer yang difungsikan untuk mengolah grafik untuk ditampilkan ke dalam layer monitor
CPU	:	komponen ini merupakan otak dari computer, kecepatan dan kecerdasan prosesor tergantung dari kecepatannya.
Montherboard	:	merupakan tempat dari semua komponen computer terpasang.
Heatsink	:	Pendingin

BAB I

PENDAHULUAN

A. DESKRIPSI JUDUL

Mengadministrasi Server dalam jaringan merupakan modul teori dan atau praktikum yang membahas dasar-dasar mengadministrasi server dalam mengelola suatu jaringan baik sebagai jaringan local atau jaringan berbasis luas (WAN). Di sebuah komputer yang digunakan oleh banyak user dan belum diterapkan pemberian Disk Quota, seringkali masing-masing user menyimpan datanya tanpa memperhatikan kapasitas harddisk komputer tersebut. Tentu saja hal ini akan menimbulkan masalah-masalah yang membuat pusing seorang administrator. Untuk mengatasi agar masing-masing user tidak dapat menyimpan data melebihi kapasitas yang diizinkan , maka seorang administrator perlu menerapkan pemberian disk quota pada masing-masing user tersebut. Akan tetapi mungkin saja ada beberapa user yang ingin diberikan disk quota yang lebih besar atau bahkan mungkin diberikan disk quota yang tidak terbatas. Karena itu dengan penerapan disk quota ini dapat diatur pembagian quota masing-masing user sesuai dengan yang dikehendaki.

Banyak pilihan yang dapat digunakan dalam menentukan cara untuk memberikan batas quota yang mungkin dialokasikan untuk seorang user atau group yaitu apakah dengan menentukan ruang disk atau dengan menentukan banyak file yang boleh mereka buat. Anda boleh saja membatasi alokasi ruang disk (block quota) atau berdasarkan jumlah file (inode quota) atau mungkin kombinasi keduanya. Masing-masing pembatasan ini kemudian akan dibagi atas dua kategori, yaitu kategori hard limit dan soft limits.

Hard limit tidak boleh dilewati. Setelah seorang user mencapai hard limitnya, dia tidak akan mendapatkan tambahan alokasi baru pada file sistem tersebut. Sebagai contoh jika user tersebut mempunyai hard limit 500 blok dalam sebuah file sistem saat dia telah menggunakan 490 blok, maka user tersebut hanya tinggal memiliki

alokasi 10 blok. Jika dia mencoba untuk mengalokasikan tambahan 11 blok, maka usaha ini akan gagal karena sudah melewati hard limitnya.

Sebaliknya soft limit dapat dilewati tapi hanya selama waktu yang telah ditetapkan. Periode ini dikenal dengan sebutan grace period, yang harga defaultnya adalah seminggu atau tujuh hari. Jika seorang user tetap mempertahankan kelebihan quota di batas soft limit lebih lama dari grace period yang dimilikinya, maka soft limit ini akan berubah menjadi hard limit. Kemudian karena sifat hard limit, dia tidak akan memperoleh tambahan alokasi lagi. Saat user tersebut mengembalikan lagi pemakaian ruang disk di bawah batas quota yang dimilikinya, grace period akan diset ulang.

B. PRASYARAT

Kemampuan awal yang dipersyaratkan untuk mempelajari modul ini adalah :

1. Peserta diklat telah lulus modul / materi diklat Menginstalasi perangkat jaringan LAN (Local Area Network)
2. Peserta diklat menguasai pengetahuan pengoperasian computer`
3. Peserta diklat mampu mengoperasikan komputer sesuai dengan intruksi manual book.

C. PETUNJUK PENGGUNAAN MODUL

1. Petunjuk Bagi Siswa

Siswa diharapkan mampu berperan aktif dan berinteraksi dengan sumber belajar yang mendukungnya, karena itu harus diperhatikan beberapa hal sebagai berikut :

A. Langkah – langkah Belajar

Modul ini berisi materi mengenai kompetensi Mengadministrasi Server dalam jaringan yang tersambung jaringan Luas, oleh sebab itu perlu diperhatikan beberapa hal agar peserta diklat lebih berkompeten dan professional, yaitu :

- 1) Apa yang harus dikerjakan pertama kali dalam Mengadministrasi Server dalam jaringan yang tersambung jaringan lokal?
- 2) Bagaimana cara Mengadministrasi Server dalam jaringan yang tersambung jaringan Luas (WAN)?
- 3) Apakah diagnosis permasalahan Mengadministrasi Server dalam jaringan dan instalasi perangkat server yang tersambung jaringan lokal atau luas sudah sesuai dengan aturan dan apakah sistem dapat bekerja dengan baik dan benar ?

B. Perlengkapan yang Harus Dipersiapkan

Untuk menunjang kelancaran tugas yang akan Anda lakukan, maka persiapkanlah seluruh perlengkapan yang diperlukan sesuai dengan jenis tugas pada masing-masing kegiatan pembelajaran.

C. Hasil Pelatihan

Anda akan mampu melakukan tugas/pekerjaan permasalahan Mengadministrasi Server dalam jaringan yang tersambung jaringan.

2. Peran Guru

Guru yang akan mengajarkan modul ini hendaknya mempersiapkan diri sebaik-baiknya yaitu mencakup aspek strategi pembelajaran, penguasaan materi, pemilihan metode, alat bantu media pembelajaran dan perangkat evaluasinya.

D. TUJUAN AKHIR

Setelah mempelajari modul ini, peserta diklat diharapkan kompeten dan professional melakukan tugas/pekerjaan Mengadministrasi Server dalam jaringan sesuai kebutuhan yang dihadapi.

E . Kompetensi

KOMPETENSI : Mengadministrasi sever di dalam jaringan

KODE : NTW.MNT.201.(2).A

DURASI PEMELAJARAN : 120 Jam @ 45 menit

LEVEL KOMPETENSI KUNCI	A	B	C	D	E	F	G
	2	1	2	2	1	2	2

F. CEK KEMAMPUAN

Untuk mengetahui kemampuan awal yang telah Anda miliki, maka isilah cek lis (√) seperti pada table di bawah ini dengan sikap jujur dan dapat dipertanggungjawabkan.

Sub Kompetensi	Pernyataan	Saya dapat Melakukan Pekerjaan ini dengan Kompeten		Bila Jawaban "Ya" Kerjakan
		Ya	Tidak	
Mengadministrasi server dalam jaringan	1. membahas tentang mengidentifikasi jenjang pengguna dan aplikasi pada jaringan			Tes Formatif 1
	2. mengatur service yang berjalan pada server			Tes Formatif 2
	3. Mampu mengisolasi permasalahan dan instalasi yang tersambung jaringan			Tes Formatif 3
	4. Membahas tentang mengisi log sheet / report sheet			Tes Formatif 4
	5. Security			Tes Formatif 5
	6. Melaporkan hasil Adminisrtasi server			Tes Formatif 6

Apabila anda menjawab **TIDAK** pada salah satu pernyataan diatas, maka pelajarilah modul ini.

BAB II

PEMELAJARAN

A. RENCANA PEMELAJARAN SISWA

Kompetensi : Jaringan Komputer

Sub Kompetensi : Mengadministrasi server dalam jaringan

Jenis Kegiatan	Tanggal	Waktu	Tempat Belajar	Alasan Perubahan	Tanda Tangan Guru
Membahas tentang Mengidentifikasi jenjang pengguna dan aplikasi pada jaringan					
mengatur service yang berjalan pada server					
Mampu mengisolasi permasalahan dan instalasi yang tersambung jaringan					
Membahas tentang mengisi log sheet / report sheet					
Security					
Melaporkan hasil Adminisrtasi server					

B. KEGIATAN BELAJAR

7. Kegiatan Belajar 1 : membahas tentang mengidentifikasi jenjang pengguna dan aplikasi pada jaringan

a. Tujuan Kegiatan Pemelajaran

1. Peserta diklat mampu mengetahui posisi user dan admin serta aplikasi yang dapat digunakan atau difungsikan.
2. Peserta diklat mampu mengetahui Performance dan kondisi administrasi server dalam jaringan

b. Uraian Materi 1

Mengadministrasi server dalam jaringan merupakan pekerjaan yang harus dilakukan oleh administrator jaringan. Pekerjaan ini memerlukan ketelitian dan kesabaran yang tinggi agar di dapat hasil yang baik.

Komputer yang terhubung jaringan local atau luas harus diatur dengan baik oleh seorang admin, baik dari sisi akses data , pembagian kegunaan atau pembagian pakai , kemanan dan kenyamanan data untuk di akses , dan masih banyak lagi yang harus di tata rapi oleh seorang administrator jaringan. Pada Materi ini kita akan membahas tentang mengidentifikasi jenjang pengguna dan aplikasi pada jaringan. Sistem operasi yang akan kita gunakan sebagai user adalah Linux Red hat 9.0 dan dari sisi client menggunakan linux atau windows.

Seringkali masing-masing user menyimpan datanya tanpa memperhatikan kapasitas harddisk komputer tersebut. Tentu saja hal in akan menimbulkan masalah-masalah yang membuat pusing seorang administrator

Untuk mengatasi agar masing-masing user tidak dapat menyimpan data melebihi kapasitas yang diizinkan , maka seorang administrator perlu menerapkan pemberian disk quota pada masing-masing user tersebut. Akan tetapi mungkin saja ada beberapa user yang ingin diberikan disk quota yang lebih besar atau bahkan mungkin diberikan disk quota yang tidak terbatas. Karena itu dengan penerapan disk quota ini dapat diatur pembagian quota masing-masing user sesuai dengan yang dikehendaki.

Kernel merupakan inti dari sistem operasi Linux. Program-program lainnya seperti kompiler, editor, window manager dsb adalah paket distribusi yang disertakan melengkapi sistem Linux. Kernel berisi program yang dimuat saat boot dan berfungsi sebagai interface antara software dan hardware. Kernel juga bertugas menangani permintaan membaca atau menulis peralatan disk, melakukan tugas-tugas network, proses input/output, manajemen memori, dsb. Kita harus mengkonfigurasi kernel dan mengkompilernya agar benar-benar efisien dan sesuai dengan sistem Linux kita. Pada dasarnya linux adalah kernel. Program-program lainnya seperti kompiler, editor, window manager dsb yang disertakan adalah paket distribusi yang melengkapi kernel menjadi sebuah sistem yang operasi yang lengkap. Informasi mengenai perkembangan kernel khususnya yang terbaru bisa dilihat di homepage <http://www.kernel.org> atau <http://www.linuxtoday.org>.

Konfigurasi Quota

Sebelum mencoba untuk menggunakan disk quota perlu diingat bahwa quota harus sudah dikonfigurasi di kernel anda dan sistem anda sudah terinstall paket quota. Pada Linux Redhat versi 6.2, paket quota bisa diinstall dengan rpm jika saat instalasi sistem, paket quota tidak dipilih. Setelah itu konfigurasi ulang kernel anda dan pada bagian quota support ketikkan y :

```
Quota support (CONFIG_QUOTA) [n] y
```

Pada Linux redhat 6.2, jika quota sudah diinstall, maka secara otomatis saat booting sistem akan mengaktifkan quota. Untuk mengecek apakah quota sudah aktif lakukan perintah berikut :

```
# /usr/sbin/quotacheck -avug
```

Kemudian hidupkan quota :

```
# /usr/sbin/quotaoon -avug
```

Setelah itu anda harus menyunting file /etc/fstab untuk mengaktifkan disk quota per baris file sistem, dimana anda dapat mengaktifkan quota untuk masing-masing user atau group atau keduanya untuk semua file sistem yang ada di Linux. Sebelum quota diaktifkan tampilan file /etc/fstab adalah sbb:

```
/dev/hda1 / ext2 defaults 1 1
/dev/hda2 /home ext2 defaults 1 1
```

Untuk mengaktifkan quota user, tambahkan "usrquota" pada kolom keempat setelah "defaults" menjadi :

```
/dev/hda1 / ext2 defaults 1 1
/dev/hda2 /home ext2 defaults,usrquota 1 1
```

Cara untuk mengaktifkan quota group hampir sama, yaitu hanya dengan mengganti options usrquota menjadi grpquota. Sedangkan untuk mengaktifkan keduanya, dapat dilakukan dengan mengubah options seperti berikut :

```
/dev/hda1 / ext2 defaults 1 1
/dev/hda2 /home ext2 defaults,usrquota,grpquota 1 1
```

Kemudian perlu dibuat juga file yang berfungsi menyimpan record quota yaitu quota.user dan quota.group. Keduanya harus diset owner sebagai root, dan hanya boleh di read-write oleh root saja. File ini biasa diletakkan di partisi /home.

```
# cd /home
# touch quota.user
# touch quota.group
# chmod 600 quota.user
# chmod 600 quota.group
```

Untuk keterangan lebih lanjut tentang fstab, baca manualnya :
man fstab

Selanjutnya reboot sistem agar quota dapat berjalan. Jika operasi sudah berjalan normal anda tidak perlu lagi menjalankan perintah quotacheck dan quotaon. Anda hanya perlu memastikan bahwa quota benar-benar sudah diaktifkan. Cara yang mudah untuk melakukan ini ialah dengan menjalankan perintah quota -v. Dari keluaran perintah ini dapat anda lihat satu baris informasi tentang pemakaian disk dan batas quota saat itu untuk masing-masing file sistem yang telah diaktifkan quotanya.

Untuk mengalokasikan batas quota digunakan perintah edquota. Perintah dapat digunakan baik untuk mengatur quota seorang user maupun quota

sebuah group. Apabila perintah edquota digunakan untuk mengatur quota seorang user maka setelah perintah edquota bisa diikuti dengan flag `-u` atau bisa juga tidak, baru kemudian diikuti namauser yang akan diatur quotanya. Jika perintah edquota tidak diikuti flag, maka secara default perintah edquota tersebut dianggap akan mengatur quota seorang user alias menggunakan flag `-u`. Karena itu, jika perintah edquota ini akan digunakan untuk mengatur quota sebuah group, maka setelah perintah ini harus diikuti flag `-g` baru kemudian diikuti nama group yang akan diatur quotanya. Selain itu perintah edquota ini juga dapat digunakan untuk mengatur quota dua atau lebih user atau group sekaligus. Sintaksnya :

```
# edquota <user1> <user2> <user3> ...dst  
dan untuk mengatur dua atau lebih group digunakan :  
# edquota -g <group1> <group2> <group3> ...dst
```

Ketika perintah edquota diminta, secara otomatis sistem akan menggunakan fasilitas teks editor vi untuk menyunting batas-batas quota yang dikehendaki. Penggunaan perintah edquota dapat dilihat pada contoh berikut :

Untuk edit quota user

```
# edquota -u bagus  
Quotas for user bagus:  
/dev/hda2: blocks in use: 2594, limits (soft = 5000, hard = 6500)  
          inodes in use: 356, limits (soft = 1000, hard = 1500)
```

"blocks in use" adalah jumlah total blok (dalam kilobyte) yang telah dipakai oleh user. "inodes in use" adalah jumlah total file yang dimiliki user dalam partisi tersebut.

Untuk edit quota group

```
# edquota -g asisten  
Quotas for group asisten:  
/dev/hda4: blocks in use: 5799, limits (soft = 8000, hard = 10000)  
          inodes in use: 1454, limits (soft = 3000, hard = 4000)
```

Seringkali seorang administrator ingin supaya ia dapat mengatur batas quota pada suatu rentang uid atau user ID, sehingga dia tidak perlu memberikan batas quota masing-masing user satu demi satu yang tentu saja akan

memakan waktu dan tenaga. Hal ini dapat dilakukan dengan menggunakan flag `-p` pada perintah `edquota`. Hal pertama yang harus dilakukan dalam penduplikasian batas quota untuk sejumlah user ini adalah menentukan batas quota yang akan dijadikan contoh atau prototype pada seorang user saja. Setelah itu proses duplikasi dapat dilakukan. Jika diasumsikan shell anda adalah `csh` dan user ID dimulai pada nomor 500 maka digunakan perintah :

```
# edquota -p bob `awk -F: '$3 > 499 {print $1}' /etc/passwd`
```

Jika anda ingin mengeset sendiri grace periode, dapat dilakukan perintah `edquota -t`. Maka akan ditampilkan :

```
# edquota -t
Time units may be: days, hours, minutes, or seconds
Grace period before enforcing soft limits for users:
/dev/hda2: block grace period: 0 days, file grace period: 0 days
```

Jika anda ingin mengeset grace periode menjadi 5 hari maka anda cukup mengubah angka 0 days menjadi 5 days, disesuaikan dengan block dan filenya.

Keterangan selengkapnya baca di manual :

```
# man edquota
```

Setelah disk quota aktif pada system, tentu saja administrator ingin memeriksa batas quota dan kapasitas disk quota yang telah digunakan. Untuk melakukan hal itu, selain dapat menggunakan perintah `quota`, juga dapat digunakan perintah `repquota`. Perintah `quota` hanya dapat digunakan oleh seorang user untuk memeriksa quota user dan group, dan pemakaian kapasitas disk yang dimilikinya. Perintah ini tidak bisa digunakan untuk melihat informasi quota yang dimiliki user lain atau group lain, jika hanya menggunakan account user biasa. Hanya superuser atau yang memiliki account root yang dapat melihat informasi quota yang dimiliki user lain beserta pemakaiannya. Perintah `repquota` dapat digunakan untuk mendapatkan ringkasan dari semua informasi quota dan pemakaian disk untuk file system yang telah diaktifkan quotanya.

Berbeda dengan perintah edquota, pada perintah repquota ini jika anda tidak menambahkan flag apapun, secara otomatis yang akan ditampilkan adalah quota untuk masing-masing user dan quota untuk masing-masing group (jika keduanya ada). Jadi misalkan ingin melihat alokasi quota tiap user di file system /home digunakan perintah :

```
# repquota -u /home
```

misalnya tipe user di file sistem /home ini telah diatur, akan muncul tampilan :

Block limits					File limits			
User	used	soft	hard	grace	used	soft	hard	grace
root	-- 175419	0	0		14679	0	0	
bin	-- 18000	0	0		735	0	0	
uucp	-- 729	0	0		23	0	0	
man	-- 57	0	0		10	0	0	
bagus	-- 13046	15360	19200		806	1500	2250	
andri	-- 2838	5120	6400		377	1000	1500	

Penggunaan perintah quota -v oleh seorang user dapat dilakukan untuk melihat batas quota yang dimilikinya di file system tertentu. Sebagai contoh di bawah ini user adjie akan melihat batas quota yang dimilikinya :

```
# quota -v
```

Disk quotas for user adjie (uid 501) :

Filesystem	blocks	quota	limit	grace	files	quota	limit	grace
/home	525*	500	550	5days	17	0	0	
/usr	0	500	550		0	0	0	

Pada file system /home dari contoh di atas dapat dilihat bahwa user tersebut telah lewat 25 blok dari batas quota yang diizinkan dan mempunyai sisa perpanjangan waktu 5 hari lagi. Tanda asterisk (*) menunjukkan bahwa user tersebut saat ini telah melewati batas quota yang dimilikinya. File system yang tidak digunakan sama sekali oleh user biasanya tidak akan ditampilkan dalam keluaran perintah quota, meskipun user tersebut mempunyai jatah quota pada file system tersebut. Jadi pada contoh di atas (user adjie selain punya quota di /home juga ada di /usr). Jika perintah quota digunakan tanpa flag apapun, maka quota user adjie di /usr tidak akan ditampilkan karena dia sama sekali

belum menggunakan jatah quotanya di file system tersebut. Tapi karena perintah `edquota` menggunakan flag `-v` maka semua informasi tentang quota yang dimilikinya akan ditampilkan.

c. Rangkuman 1

Membahas tentang mengidentifikasi jenjang pengguna dan aplikasi, membuat seorang admin jaringan harus bisa mengatur quota untuk client-clientnya agar tidak saling tubrukan dan acak-acakan. Data yang ada wadah jaringan tersebut harus diberi wewenang sesuai dengan kebutuhan setiap client atau server. Akan tetapi server selalu dapat menjalankan disfungsi atau aplikasi yang akan diinginkannya.

d. Tugas 1

1. konfigurasi quota

e. Tes Formatif 1

1) Jelaskan fungsi dari quota

2) Jelaskan yang dimaksud dengan hard limit dan soft limit

f. Kunci Jawaban Formatif 1

1. Fungsi dari Quota adalah Untuk mengatasi agar masing-masing user tidak dapat menyimpan data melebihi kapasitas yang diizinkan,

II. Hard limit tidak boleh dilewati. Setelah seorang user mencapai hard limitnya, dia tidak akan mendapatkan tambahan alokasi baru pada file sistem tersebut. Sebagai contoh jika user tersebut mempunyai hard limit 500 blok dalam sebuah file sistem saat dia telah menggunakan 490 blok, karena usaha ini akan gagal karena sudah melewati hard limitnya

Sebaliknya soft limit dapat dilewati tapi hanya selama waktu yang telah ditetapkan. Periode ini dikenal dengan sebutan *grace period*, yang harga defaultnya adalah seminggu atau tujuh hari. Jika seorang user tetap mempertahankan kelebihan quota di batas soft limit lebih lama dari *grace period* yang dimilikinya, maka soft limit ini akan berubah menjadi hard limit.

Kemudian karena sifat hard limit, dia tidak akan memperoleh tambahan alokasi lagi. Saat user tersebut mengembalikan lagi pemakaian ruang disk di bawah batas quota yang dimilikinya, grace period akan diset ulang.

a. Lembar Kerja 1

Alat dan bahan

- 1) Komputer dengan sistem operasi Linux Red hat 9.0
- 2) Komputer terhubung jaringan LAN
- 3) Sebelum mencoba untuk menggunakan disk quota perlu diingat bahwa quota harus sudah dikonfigurasi di kernel anda dan sistem anda sudah terinstall paket quota

Kesehatan dan Keselamatan Kerja

- 1) Berdo'alah sebelum memulai kegiatan belajar.
- 2) Gunakan alas kaki yang terbuat dari karet untuk menghindari aliran listrik ketubuh (tersengat listrik)
- 3) Bacalah dan pahami petunjuk praktikum pada setiap lembar kegiatan belajar.
- 4) Letakkan Komputer pada tempat yang aman.
- 5) Pastikan komputer dalam keadaan baik, semua kabel penghubung terkoneksi dengan baik.
- 6) Jangan meletakkan benda yang dapat mengeluarkan medan elektromagnetik di komputer (magnet, handphone, dan sebagainya).
- 7) Jangan meletakkan makanan dan minuman diatas komputer
- 8) Gunakanlah komputer sesuai fungsinya dengan hati-hati.

Langkah Kerja

1. Untuk edit quota user

```
# edquota -u bagus
Quotas for user bagus:
/dev/hda2: blocks in use: 2594, limits (soft = 5000, hard = 6500)
          inodes in use: 356, limits (soft = 1000, hard = 1500)
```

2. Untuk edit quota group

```
# edquota -g asisten
```

Quotas for group asisten:
/dev/hda4: blocks in use: 5799, limits (soft = 8000, hard = 10000)
inodes in use: 1454, limits (soft = 3000, hard = 4000)

2. Kegiatan Belajar 2: Mengatur service yang berjalan pada server

a. Tujuan Kegiatan Pemelajaran

- 1) Peserta diklat mampu mengatur service yang berjalan pada server
- 2) Peserta diklat mengetahui pengertian, konfigurasi, instalasi dan menjalankan samba server

b. Uraian Materi 2

Mengatur service yang berjalan pada server

1. Samba

Samba adalah server yang sangat powerful yang dapat membuat sistem berbasis Unix (seperti Linux) untuk melakukan sharing resource dengan sistem berbasis Windows. Hal ini tentu sangat berguna pada sebuah LAN yang terdiri atas beberapa workstation dengan platform sistem operasi Linux dan Windows sehingga dapat lebih efisien dengan adanya pembagian resource, seperti file dan printer, untuk dapat digunakan secara bersama-sama. Samba merupakan sebuah software aplikasi buatan Andrew Tridgel dari ANU (Australian National University) dengan mengimplementasikan protokol SMB (Server Message Block) pada sistem operasi Unix. Protokol ini kadang-kadang dapat berlaku sebagai protokol CIFS (Common Internet File System), LanManager, NetBIOS. Protokol SMB ini dapat membuat sebuah komputer dengan sistem operasi Unix menjadi file atau print server menjadi file atau print server atau seperti klien ftp untuk mengakses share SMB baik di Samba server atau di sever lain yang kompatibel seperti Windows NT, mendukung nameserving dan browsing NetBIOS, dan lain-lain.

2. Mekanisme SMB

2.1. Username dan Password

Untuk memahami hubungan antara Linux/Samba/Windows, kita harus mempelajari sistem file, printer, dan user pada kedua operating sistem. Beberapa manajemen pengaturan username dan password :

- **Linux Password Authentication Module (PAM)**, akan membuat autentikasi user dengan PDC sehingga kita tetap mempunyai dua user, satu di lokal dan satu lagi di PDC , tapi user hanya perlu menyimpan password hanya dalam sistem window.
- **Samba sebagai PDC**, akan menyimpan login dan password pada sistem Linux.
- **Membuat solusi sendiri dengan Perl**, kita dapat membuat sendiri. Hal ini dilakukan dengan menggunakan Winperl dan modul-modul Perl yang memungkinkan pengubahan paa Security Access Manager (SAM), untuk meng-update daftar password PDC. Script Perl pada sisi Linux dapat berkomunikasi dengan script WinPerl untuk menjaga sinkronisasi account.

2.2. Encrypted Password

Sejak Windows NT 4, Windows 98, dan Windows 95 OSR2, Windows menggunakan password terenkripsi saat berkomunikasi menggunakan PDC dan setiap server yang memerlukan autentikasi (termasuk Linux dan Samba). Algoritma enkripsi Windows berbeda dengan UNIX, sehingga tidak kompatibel. Untuk menangani hal itu, kita dapat melakukan pilihan-pilihan sebagai berikut :

- Mengedit Registry pada klien Windows untuk mendisable penggunaan password terenkripsi. Bagian registry yang harus diubah terdapat pada direktori docs paket Samba.
- Mengkonfigurasi Samba agar menggunakan password terenkripsi Windows.

Pilihan pertama mempunyai kelebihan dengan tidak adanya pola password yang lebih kompleks. Pada sisi lain, kita harus membuat registry yang tetap pada semua klien. Untuk pilihan kedua sebaliknya, yakni sedikit lebih kompleks pada sisi server, tapi kita tidak usah mengubah bagian klien.

2.3. Perbedaan smbd dengan nmbd

Sebenarnya Samba disusun atas dua daemon, yaitu smbd dan nmbd. Smbd adalah daemon yang secara nyata menangani servis sharing file sistem dan printer untuk klien. Pada saat sebuah klien melakukan autentikasi, smbd akan membuat duplikat dirinya, bagian asli akan kembali ke port 139 untuk mendengarkan permintaan baru dan bagian duplikat menangani koneksi terhadap klien. Duplikat ini juga mengubah ID user efektifnya dari root ke user yang terautentikasi. Misalnya, kalau user "smkti" melakukan autentikasi dengan smbd, duplikat baru akan berjalan dengan permissi "smkti", dan bukannya permissi "root"). Duplikat ini akan berada di memory selama masih terkoneksi dengan klien.

Daemon nmbd bertanggung-jawab untuk menangani permintaan server name NetBIOS. Ia akan mendengarkan port 137, tidak seperti smbd, nmbd tidak membuat contoh dirinya untuk menangani setiap pertanyaan. Kedua daemon itu harus dijalankan agar Samba bekerja dengan baik.

3. Instalasi Paket Samba Server

Paket Samba release terbaru bisa dilihat di homepage Samba : <http://us1.samba.org/samba/samba.html> atau melalui FTP site: 63.238.153.11. Bila tersedia, paket juga bisa diambil melalui ftp site-ftp site terdekat. Pada modul ini, kita akan coba untuk menginstall paket : samba-2.0.7.tar.gz. Pastikan file source ini sudah didownload dan diletakkan di direktori /usr/local/src (atau direktori lainnya).

3.1. Instalasi Dalam Bentuk Tarball

Instalasi dalam bentuk tarball adalah instalasi dengan source dalam bentuk file berekstensi tar.gz. Instalasi ini hanya bisa dilakukan dengan account root. Berikut adalah langkah-langkah instalasinya :

Masukkan ke direktori tempat diletakkannya source Samba :

```
# cd /usr/local/src
```

Kemudian ekstrak file tersebut dengan perintah :

```
# tar -zxvf samba-2.0.7.tar.gz
```

Setelah diekstart akan terbentuk direktori samba-2.0.7, masuklah ke direktori tersebut, dan di sana akan terdapat direktori source, docs , dan sebagainya :

```
# cd samba-2.0.7
```

Lalu masuklah ke direktori source dan jalankan script configure yang ada di sana. Dalam konfigurasi ini, kita dapat menambahkan beberapa option, misalnya kita akan menambahkan option sebagai berikut :

Option	Deskripsi
--with-pam	Agar Samba dapat menggunakan Password Authentication Module (PAM).
--with-mmap	Agar mendukung MMAP untuk meningkatkan performansi Samba.

```
# ./configure --with-smbmount --with-pam --with-mmap
```

Kemudian install Samba dengan mengetikkan perintah make lalu make install:

```
# make all  
# make install
```

Samba akan terinstall di direktori /usr/local/samba. Setelah perintah instalasi di atas dieksekusi, akan terbentuk direktori bin yang berisi sejumlah file binary yang berfungsi seperti untuk mengontrol Samba server seperti smbd, nmbd, dan smbclient, dan lain-lain.

Samba akan terinstall di direktori /usr/local/samba.

```
# install -m 755 script /mksmbpasswd.sh /usr/bin/
```

Perintah ini akan menginstall script "mksmbpasswd.sh" pada direktori "/usr/bin/". Script ini diperlukan untuk mensetup user Samba diijinkan terkoneksi ke server via file "smbpasswd".

Untuk mempelajari Samba secara lebih mendalam, kita dapat membaca manualnya yang disertakana dalam paket. Manual Samba secara default terletak di direktori /usr/local/samba/man. Agar manual Samba bisa dibaca (diakses) dengan perintah man pada shell Linux, lakukan sebagai berikut :

```
# cp /usr/local/samba/man/man1/* /usr/man/man1
# cp /usr/local/samba/man/man5/* /usr/man/man5
# cp /usr/local/samba/man/man7/* /usr/man/man7
# cp /usr/local/samba/man/man8/* /usr/man/man8
```

4. Konfigurasi Samba Server

Dalam membuat konfigurasi Samba server ini sangat bergantung pada kebutuhan dan arsitektur dari jaringan komputer kita. Misalkan Samba server ini bisa dikonfigurasi hanya terkoneksi satu klien atau bahkan terkoneksi dengan 1000 klien. File dokumentasi konfigurasi lengkap Samba server ini dapat didownload di internet dengan alamat: <http://www.openna.com/books/floppy.tgz>. Untuk menjalankan Samba server, dibutuhkan file-file berikut ini dan harus dibuat atau dikopi pada direktori-direktori yang cocok pada server kita.

4.1. Konfigurasi file "smb.conf"

File konfigurasi utama untuk Samba server ini adalah "/usr/local/samba/lib/smb.conf", dimana kita dapat menentukan direktori yang ingin kita akses dari komputer Windows, IP address mana yang diijinkan, dsb. Pada file ini juga terdapat banyak sekali option (pilihan). Untuk informasi lebih lanjut tentang berbagai setting dan parameter dapat dilihat di dokumentasi Samba.

Konfigurasi yang akan kita bahas di bawah adalah file konfigurasi minimal Samba yang mendukung password terenkripsi. Kita harus terlebih dahulu mengkopikan file konfigurasi default lalu mengeditnya sesuai dengan yang kita inginkan :

```
# cd /usr/local/samba/examples
# cp smb.conf.default /usr/local/samba/lib
# cd /usr/local/samba/lib
# mv smb.conf.default smb.conf
# pico smb.conf
```

```
workgroup= SMKTI
```

Isilah dengan workgroup server kita, yang akan tampak saat diminta oleh klien. Klien dan server harus mempunyai workgroup yang sama.

server string= Samba Server

Option ini akan menampilkan string yang akan ditampilkan pada user dalam comment box print manager, atau pada koneksi IPC pada bagian "net view" pada komputer Windows.

encrypted password= True

Jika option ini diset "True", Samba akan menggunakan password terenkripsi bukan menggunakan password berbentuk teks sederhana saat berhubungan dengan klien. Password terenkripsi ini tidak akan bisa dideteksi dengan sniffer. Untuk keamanan sebaiknya option ini diset "True".

security= user

Bila option security ini diisi dengan "user", klien harus masuk (log-on) dengan username dan password yang benar, jika tidak, koneksi akan diputus (connection refused). Hal ini berarti bahwa username dan password yang benar harus terdapat pada file "/etc/passwd" sistem Linux dan file "/etc/smbpasswd" pada Samba server, jika tidak koneksi dari klien akan gagal.

smb passwd file= /etc/smbpasswd

Option ini menentukan letak file "smbpasswd" terenkripsi. File "smbpasswd" ini merupakan kopi dari file "/etc/passwd" sistem Linux yang berisi username dan password yang valid agar bisa terkoneksi dengan Samba server. Samba server akan membaca file ini (smbpasswd) saat ada permintaan koneksi.

log file= /var/log/samba/log.%m

Option ini menyatakan letak file log yang dicatat Samba. Dengan ekstensi %m kita dapat membuat file log yang terpisah untuk masing-masing user atau mesin yang log-on pada Samba server.

socket options= IPTOS_LOWDELAY TCP_NODELAY

Dengan option ini kita dapat menentukan parameter-parameter konfigurasi Samba untuk meningkatkan performansi Samba. Secara default, koneksi untuk jaringan lokal dibuat maksimal, dan meningkatkan performansi Samba server dalam transfer file.

domain master= Yes

Option ini untuk mengeset Samba server daemon "nmbd" sebagai domain master browser untuk group yang telah ditentukan. Option ini biasanya harus diset "Yes" hanya dalam satu Samba server untuk keseluruhan Samba server yang lain pada workgroup dan jaringan yang sama.

local master= Yes

Dengan option di atas, Samba server daemon, nmbd, akan mencoba untuk menjadi domain master browser pada workgroup yang telah ditentukan.

preferred master= Yes

Option "preferred master" akan menentukan dan mengontrol jika "nmbd" dibuat sebagai master browser untuk workgroup yang bersangkutan.

os level= 65

Dengan mengatur nilai os level, nmbd dapat menjadi master browser lokal untuk workgroup pada daerah broadcast lokal. Jika terdapat NT server pada jaringan kita, dan kita ingin agar Samba server Linux menjadi browser lokal untuk workgroup pada broadcast lokal maka option di atas harus diisi 65. Ingat option ini hanya untuk satu Linux Samba server.

dns proxy= No

Bila diset "yes" , Samba server daemon "nmbd" ketika menjadi sebuah WINS server dan nama Net BIOS belum teregistrasi, maka ia harus memperlakukan nama Net BIOS kata demi kata sebagai nama DNS. Jika kita belum pernah mengkonfigurasi Samba sebagai WINS Server, kita tidak usah membuat option ini "Yes". Dengan memilih "Yes" juga akan dapat mengurangi performansi Samba.

`name resolve order= lmhosts host bcast`

Option ini menyatakan nama servis yang dipakai untuk mengubah hostname ke IP address. Pilihan di atas akan menyebabkan file "lmhosts" lokal Samba akan dituju terlebih dahulu.

`bind interfaces only= True`

Jika option ini diset "True", kita dapat membatasi interface-interface yang melayani permintaan "smb". Sebaiknya option ini diset demikian untuk keamanan.

`interfaces= eth0 192.168.1.1`

Option di atas berguna untuk menentukan jenis interface yang digunakan Samba server saat digunakan browsing dan registrasi nama, pada contoh di atas yakni eth0 dengan IP address 192.168.1.1. Defaultnya, Samba akan mengecek semua device pada kernel.

`hosts deny= ALL`

Kita dapat menentukan host-host yang tidak boleh mengakses Samba. Secara default kita melarang akses dari seluruh host, dan mengijinkan akses untuk host-host tertentu yang didefinisikan pada "hosts allow" di bawah ini.

`hosts allow= 192.168.1.4 127.0.0.1`

Host-host yang diijinkan untuk mengakses Samba server didefinisikan pada bagian ini, pada contoh di atas kita mengijinkan host dengan IP 192.168.1.4 dan localhost 127.0.0.1.

`debug level= 1`

Di sini kita dapat menentukan level log pada file "smb.conf". Sebaiknya "debug level" ini tidak lebih dari 2, karena server akan log file yang tidak perlu setelah melakukan operasi sehingga akan menurunkan performansi.

`create mask= 0644`

Option "create mask" akan menset permisi-permisi yang penting yakni bila terjadi mapping dari DOS ke permisi UNIX. Jika dibuat 0644, semua file yang dibuat atau dikopi dari WINDOWS ke sistem UNIX akan mempunyai permisi 0644 secara default (untuk lebih jelasnya dibahas pada bagian sistem operasi Linux).

`directory mask= 0755`

Mirip seperti di atas, hanya ini berlaku untuk semua direktori yang dikopi atau dibuat dari Windows ke sistem UNIX akan mempunyai permisi default 0755.

`level2 oplocks= True`

Jika option ini dibuat "True", akan meningkatkan keandalan file-file akses yang tidak umum ditulis seperti file-file aplikasi .EXE.

`read raw= no`

Ini berguna untuk menentukan apakah Samba server akan mendukung permintaan raw read SMB saat mentransfer data pada klien. Agar mapping memory lebih efektif, sebaiknya option ini dibuat "no".

`write cache size= 262144`

Option ini akan membuat Samba meningkatkan keandalan sistem jika terjadi kemacetan disk subsystem. Nilai option ini dinyatakan dalam byte (262144=256k)

`comment= Temporary File Space`

Option ini untuk menyatakan komentar yang akan terlihat saat ada permintaan klien ke server.

`path= /tmp`

Kita dapat menentukan direktori mana user service ini diberikan akses.

`read only= No`

Maksud option di atas adalah kita dapat menentukan apakah user hanya dapat membaca file atau tidak. Jika diisi "No" user tidak hanya dapat membaca file saja.

valid user= admin

Option ini berisi daftar user yang diijinkan login. Pada contoh di atas user "admin" diijinkan untuk akses.

invalid users= root bin daemon nobody named sys tty disk mem kmem users

Option "invalid users" berisi daftar yang tidak diijinkan login yang biasanya user "paranoid". Sebenarnya hal ini hanya untuk memastikan setting yang tidak benar dan dapat membahayakan dari segi keamanan

4.2. Konfigurasi file /etc/lmhosts

File "/etc/lmhosts" adalah file untuk memetakan nama Net BIOS Samba ke IP address. Format file ini mirip "/etc/hosts", tapi komponen dari hostname harus sesuai dengan format penamaan Net BIOS. Pertama-tama kita harus membuat file "/etc/lmhosts" ini.

```
# touch /etc/lmhosts
```

Pada file ini, tambahkan host-host klien sbb:

```
# pico /etc/lmhosts
```

```
127.0.0.1          Localhost
192.168.1.1       smkti1
192.168.1.2       smkti2
192.168.1.3       smkti3
```

Teruskan pengisian file di atas untuk semua hosts yang ada dalam network kita.

4.3. Konfigurasi file /etc/pam.d/samba

File ini berguna untuk menjalankan autentikasi pam (untuk lebih jelasnya dapat dilihat pada bagian security). Lakukan perintah berikut ini :

```
# touch /etc/pam.d/samba
```

```
# pico /etc/pam.d/samba
```

Tambahkan baris-baris berikut ini:

```
Auth      required    /lib/security/pam_pwdb.so nullok shadow
Account   required    /lib/security/pam_pwdb.so
```

4.4. Konfigurasi file `/etc/logrotate.d/samba`

File konfigurasi ini akan menampilkan file-file log tiap minggu secara otomatis.

```
# touch /etc/logrotate.d/samba
```

Tambahkan baris-baris berikut ini :

```
/var/log/samba/log.nmb {
    notifempty
    missingok
    prostrorate
    /usr/bin/killall -HUP nmbd
    endrotate
}
/var/log/samba/log.smb {
    notifempty
    missingok
    postrotate
    /usr/bin/killall -HUP smbd
    endotrate
}
```

4.5. Membuat password Clie Samba terenkripsi

File `/etc/smbpasswd` adalah file password Samba yang terenkripsi. File ini berisi username, UID, password terenkripsi masing-masing user yang dapat mengakses Samba. Jika seorang user tidak terdaftar dalam file ini, maka ia tidak dapat melakukan koneksi ke server. Untuk membuat account Samba, user-user samba harus sudah ada dalam file `/etc/passwd` Linux. Jika kita ingin menambahkan user yang dapat mengakses Samba, kita harus menambahkan nama user tersebut

pada file `"/etc/passwd"` sistem Linux kita sbb: (Misal kita ingin menambahkan user `"smbclient"`).

```
# adduser smbclient
```

```
# passwd smbclient
```

```
Changing password for user smbclient
```

```
New UNIX password:
```

```
Retype new UNIX password:
```

```
passwd:all authentication tokens updated successfully
```

Setelah kita menambahkan semua client Samba pada file `"/etc/passwd"`, Kita dapat membuat file `"/etc/smbpasswd"` dari file `"/etc/passwd"` dari Linux server (Ingat agar semua user yang akan mengakses samba sudah ada dalam file `"/etc/passwd"`) dengan perintah sbb:

```
# cat /etc/passwd | mksmbpasswd.sh > /etc/smbpasswd
```

Kemudian kita harus membuat account user Samba pada file `"/etc/smbpasswd"` sebelum kita dapat menggunakannya.

```
# smbpasswd -a smbclient
```

```
New SMB password:
```

```
Retype new SMB password:
```

```
Added user smbclient
```

```
Password changed for user smbclient.
```

Kemudian ubahlah setting permisi file `"smbpasswd"` ini agar hanya bisa dibaca dan ditulisi oleh account `"root"` :

```
# chmod 600 /etc/smbpasswd
```

Untuk memeriksa kesalahan dalam penulisan file `"smb.conf"`, lakukan perintah ini :

```
# testparm
```

Untuk menjalankan dan menghentikan daemon Samba, `nmbd` dan `smbd` secara otomatis kita dapat menjalankan script file `"/etc/rc.d/init.d/smb"`. Pastikan bahwa

file ini mempunyai permisi yang hanya bisa dibaca, ditulis, dan dieksekusi oleh user "root".

```
# chmod 700 /etc/rc.d/init.d/smb
```

Lalu buat simbolik link rc.d pada Samba dengan perintah :

```
# chkconfig --add smb
```

Agar sript Samba secara otomatis menjalankan daemon nmbd dan smbd saat sistem dihidupkan (atau direboot) lakukan perintah berikut ini :

```
# chkconfig --level 345 smb on
```

5. Menjalankan Samba

Sebelum menjalankan Samba kita harus membuat direktori seperti yang sudah didefinisikan pada file Makefile. Hal ini karena direktori ini tidk secara otomatis dibuat saat mengeksekusi perintah make install.

```
# mkdir /usr/local/samba/var
```

Samba dapat dijalankan dengan dua macam cara. Pertama dijalankan sebagai daemon dan kedua menjalankannya dari inetd. Samba yang dijalankan sebagai daemon akan sedikit lebih cepat dalam melayani permintaan client jika dibandingkan dengan Samba yang dijalankan dari inetd. Biasanya berbagai distribusi Linux sudah mempunyai script untuk menstart dan menstop servis Samba. Untuk menjalankan Samba kita harus menjalankan daemon smbd dan nmbd. Lakukan perintah berikut ini :

```
# /usr/local/samba/bin/smbd -D
```

```
# /usr/local/samba/bin/nmbd -D
```

Agar Samba selalu dijalankan setiap kali Linux melakukan booting, kita dapat menambahkan baris-baris di atas pada file /etc/rc.d/rc.local :

```
# pico /etc/rc.d/rc.local
```

```
/usr/local/samba/bin/smbd -D
```

```
/usr/local/samba/bin/nmbd -D
```

Apabila dalam sistem kita tidak mempunyai script untuk menjalankan Samba secara otomatis, maka kita harus menuliskannya secara manual. Misalkan dengan cara membuat file `"/usr/local/bin/start smb/"` untuk menjalankan dan menghentikan secara otomatis daemon Samba server.

```
# pico /usr/local/samba/bin/start smb
```

Tambahkan baris-baris berikut ini :

```
#!/bin/sh
```

```
/usr/local/samba/bin/smbd -D
```

```
/usr/local/samba/bin/nmbd -D
```

Untuk menjalankan Samba kita tinggal mengeksekusi file `start smb` tersebut.

```
# /usr/local/samba/bin/start smb
```

Untuk mematikan Samba, kill proses `smbd` dengan cara sbb :

```
# ps ax|grep smbd
```

Dengan perintah di atas akan tampak proses `smbd` beserta nomor PID-nya.

```
# kill -9 [nomor PID smbd]
```

c. Rangkuman 2

Samba adalah server yang sangat powerful yang dapat membuat sistem berbasis Unix (seperti Linux) untuk melakukan sharing resource dengan sistem berbasis Windows. Hal ini tentu sangat berguna pada sebuah LAN yang terdiri atas beberapa workstation dengan platform sistem operasi Linux dan Windows sehingga dapat lebih efisien dengan adanya pembagian resource, seperti file dan printer, untuk dapat digunakan secara bersama-sama. Samba merupakan sebuah software aplikasi buatan Andrew Tridgel dari ANU (Australian National

University) dengan mengimplementasikan protokol SMB (Server Message Block) pada sistem operasi Unix. Protokol ini kadang-kadang dapat berlaku sebagai protokol CIFS (Common Internet File System), LanManager, NetBIOS. Protokol SMB ini dapat membuat sebuah komputer dengan sistem operasi Unix menjadi file atau print server menjadi file atau print server atau seperti klien ftp untuk mengakses share SMB baik di Samba server atau di sever lain yang kompatibel seperti Windows NT, mendukung nameserving dan browsing NetBIOS, dan lain-lain.

- d. Tugas 2
- e. Tes Formatif 2
- f. Kunci Jawaban Formatif 2
- g. Lembar Kerja 2
- 3. Kegiatan Belajar 3 : mengecek kondisi server berdasarkan log file .
 - a. Tujuan Kegiatan Pemelajaran
 - 1. Memahami arti dan fungsi dari sebuah proxy server.
 - 2. Memahami konsep parent-siblings
 - 3. Memahami perbedaan proxy server yang dijalankan yang dijalankan pada mode httpd-accelerator dan proxy-caching mode
 - 4. Mengetahui file-file konfigurasi proxy server.
 - 5. Membuat konfigurasi file squid.conf
 - 6. Mengetahui file-file log squid

b. Uraian Materi 3

mengecek kondisi server berdasarkan log file

1. Proxy Server

Proxy server sudah menjadi hal yang populer di kalangan para pengguna internet saat ini, berkaitan dengan kemampuannya untuk menghemat bandwidth, meningkatkan keamanan, dan menambah kecepatan web-surfing. Dalam jaringan yang menerapkan sistem proxy, hubungan komunikasi ke internet dilakukan melalui sistem pendelegasian. Komputer-komputer yang dapat dikenali oleh internet bertindak sebagai wakil.

2. Proxy Server Squid

Proxy server yang cukup populer saat ini adalah squid, karena selain gratis juga mendukung ICP. ICP digunakan untuk pertukaran data tentang suatu URL dengan cache-cache lainnya. Secara sederhana, squid dapat dikatakan sebagai software yang diaplikasikan untuk membuat http atau ftp cache. Cara kerja squid dapat dianalogikan seperti browser (IE/Opera/Netscape) yang menyimpan data suatu site di hardisk sehingga untuk menampilkan site yang sama tinggal mengambil data di cachanya.

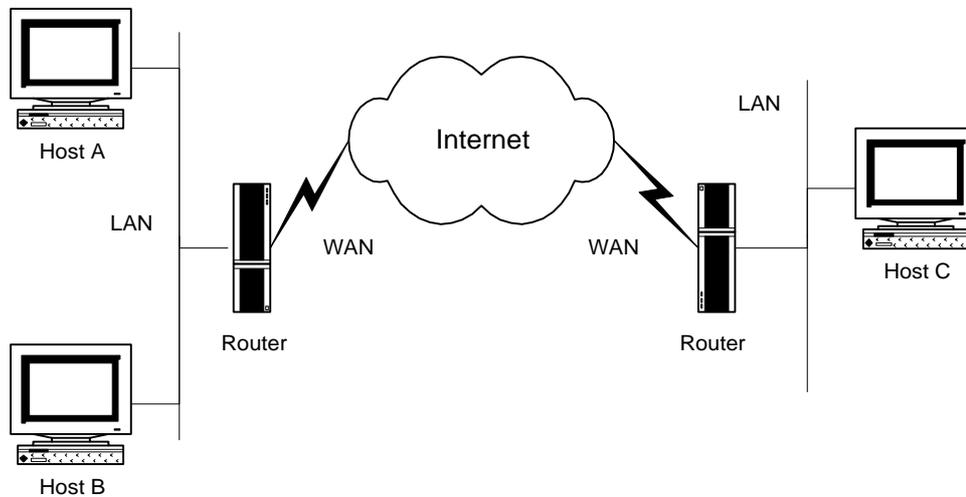
Squid dapat dikonfigurasi sebagai :

- Mode httpd-accelerator untuk meningkatkan performansi web server kita.
- Proxy caching-server agar seluruh user dalam jaringan kita dapat menggunakan squid untuk mengakses internet.

Pada konfigurasi pertama, squid server berlaku seperti reverse proxy-cache, squid akan menerima permintaan client, memberikan data di cachanya, jika tidak ada akan mengambil langsung dari server aslinya (reverse proxy).

Sebagai proxy cache server, kita dapat mengontrol secara keseluruhan kinerja jaringan kita dan memberlakukan beberapa aturan dalam memberkian data yang dapat dilihat, diakses atau didownload. Kita juga dapat mengontrol penggunaan bandwidth, waktu koneksi dan sebagainya. Sebuah proxy cache dapat dikonfigurasi sebagai Squid dapat menghemat bandwidth dapat diterangkan sebagai berikut :

Misal suatu host meminta www.detik.com, maka squid akan mengambil dan meletakkannya di hardisk server untuk selanjutnya diambil oleh host yang bersangkutan. Bila ada host lain yang meminta data yang sama, server tidak perlu lagi mendownloadnya dari www.detik.com, tapi cukup memberikan data yang ada di cachanya sehingga akan lebih cepat dan menghemat bandwidth. Untuk lebih jelasnya perhatikan gambar berikut ini:



Gambar Posisi host di internet

Selain itu, squid dapat melakukan filtering, yaitu squid dapat memblokir permintaan client terhadap URL-URL tertentu, sehingga pengelola jaringan dapat lebih santai tanpa khawatir adanya penyalahgunaan yang tidak dikehendaki. Dalam squid dikenal istilah parent dan sibling. Parent akan mengambil langsung ke web site yang diminta, sedangkan sibling akan mencarinya dulu ke parent. Bila tidak ada, maka sibling mencarinya langsung ke web site yang bersangkutan.

Sebuah proxy cache dapat dikonfigurasi untuk berjalan standalone server atau sebagai hierarki cache dengan dengan proxy-proxy lainnya, yang akan kita bahas lebih lanjut berikut ini.

- Standalone server, tanpa parent dan sibling

Ini merupakan konfigurasi yang paling sederhana yang biasa dipakai oleh ISP (Internet Service Provider) dan warung internet dimana squid server local akan langsung mencari ke web server www.detik.com untuk memenuhi permintaan client bila data tidak terdapat di cache.

- Sibling tanpa parent

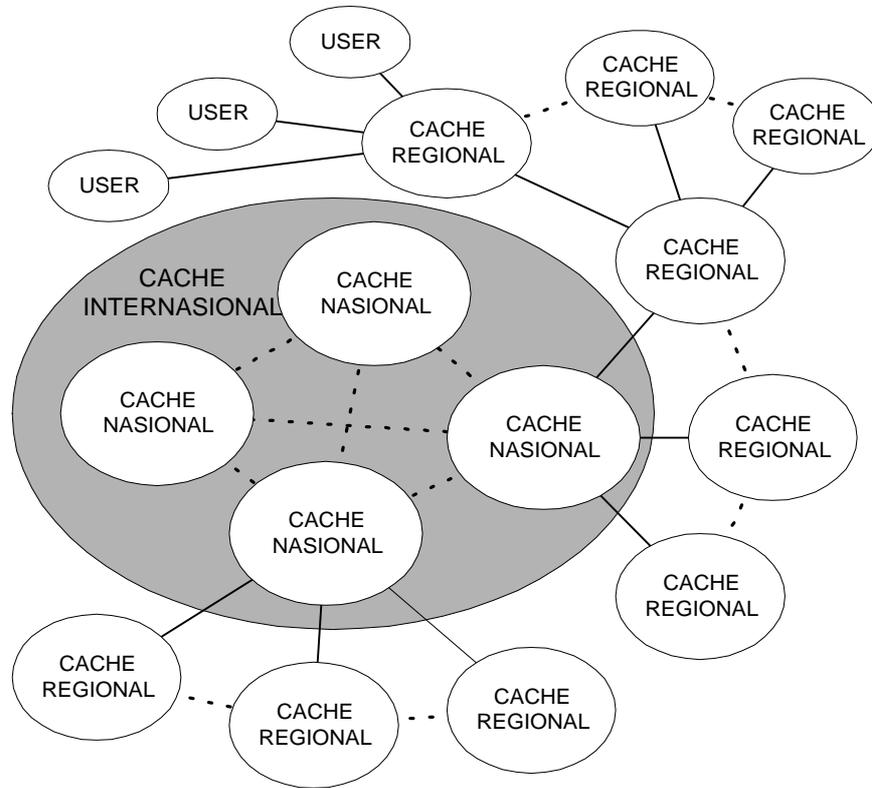
Biasanya konfigurasi ini dipakai untuk jaringan yang tidak terlalu besar. Permintaan oleh klien pada suatu URL akan diterima lokal yang akan mencarinya ke sibling, bila tidak ada, lokal akan langsung mencarinya langsung ke webserver yang bersangkutan.

- Parent dan sibling

Biasanya konfigurasi ini diterapkan untuk jaringan yang besar. Efisiensi jaringan ini cukup baik, karena yang bekerja untuk mendapatkan halaman web keluar jaringan hanyalah parent sisanya sibling dan para client tidak dapat memperolehnya secara langsung (dengan firewall). Klien yang meminta halaman web www.detik.com akan diterima squid server lokal yang kemudian akan memeriksa cachanya, bila tidak ada dia akan mencari ke sibling, bila ada sibling akan memberikannya ke lokal, namun bila tidak ada lokal akan meminta ke parent. Sebagai parent ia harus melayani permintaan ini. Walaupun ia tidak memiliki halaman yang diminta, ia harus memenuhinya dengan mengambil langsung ke www.detik.com. Setelah itu permintaan dikembalikan ke lokal dan akhirnya ke klien.

3. Hierarki Squid

Server proxy dapat dihubungkan dengan server-server proxy lain dan membentuk hierarki seperti pada sebuah organisasi. Jika server proxy bergabung dalam sebuah hierarki, sebuah server proxy bisa memilih untuk mengambil dokumen yang diinginkan dari server proxy lain dalam hierarki atau mengambil dari server asal. Hierarki ini terdiri dari cache pada tingkat nasional, regional, dan organisasi. Dalam prototipe ini cache pada tingkat nasional melayani permintaan akses untuk domain negara tersebut. Misalnya terdapat permintaan dokumen dari URL <http://www.republika.co.id> yang berada di bawah domain id (Indonesia), maka dokumen tersebut diminta dari cache tingkat nasional di Indonesia.



Gambar 4. Prototipe hierarki cache

4. Instalasi Squid

Untuk mendapatkan source squid terbaru dapat download di <ftp://squid.nalr.fr/squid/> atau homepage squid <http://www.squid-cache.org/>. Dalam modul ini kita akan melakukan instalasi secara manual yaitu squid-2.3.STABLE2-src.tar.gz. Sebelum instalasi pastikan source ini sudah ada (misal di direktori /usr/local).

1. Masuklah ke direktori /usr/local/ dan ekstark source dengan perintah:

```
# cd /usr/local
# tar zxvf squid-2.3.STABLE2-src.tar.gz
```

2. Squid proxy-server tidak dapat berjalan sebagai sebagai super user root, oleh karena itu kita harus membuat account khusus tanpa shell untuk menjalankan Squid Proxy Server :

```
# useradd -d /cache/ -r -s /dev/null 2>&1
# mkdir /cache/
# chown -R squid.squid /cache/
```

Perintah pertama akan menambahkan user "squid" ke file /etc/passwd, lalu membuat direktori "/cache" (jika belum ada) kemudian mengubah kepemilikan direktori "/cache" ke user "squid".

3. Setelah proses ekstarksi akan terbentuk direktori squid-2.3.STABLE2-src, masuk ke direktori tersebut dan lakukan configure otomatis yang akan memberikan output berupa file Makefile.

```
# ./configure --prefix=/usr/local/squid
```

4. Selanjutnya lakukan kompilasi dan install sbb:

```
# make  
# make install
```

Hasil instalasi bisa dilihat di direktori /usr/local/squid. Di dalamnya terdapat direktori /bin, /logs dan /etc.

5. Konfigurasi Squid

Setelah proses instalasi selesai, langkah selanjutnya adalah mengkonfigurasi squid. File konfigurasi ini biasanya terletak pada direktori /usr/local/squid/etc. Squid biasanya sudah menyediakan file konfigurasi default yaitu squid.conf.default, yang berisi parameter-parameter squid secara lengkap, berikut deskripsi serta contoh penggunaannya.

5.1. Konfigurasi file Squid.conf

Dalam direktori /usr/local/squid/bin akan terdapat file-file sbb:

squid	program utama
dnsserver	server untuk melayani request pemetaan ip <-> nama tiap child proses squid
cachemgr	program tambahan untuk memantau server secara otomatis
runchace	script untuk memulai squid

Sedangkan dalam direktori /usr/local/squid/etc akan terdapat file-file konfigurasi sbb :

squid.conf.default	file konfigurasi squid default
mime.conf.default	file konfigurasi mime default

Sedangkan file-file log akan terdapat pada direktori /usr/local/squid/logs, yaitu :

access.log	mencatat log aktivitas-aktivitas yang dilakukan oleh klien.
------------	---

cache.log mencatat log yang dicatat oleh cache server.
store.log mencatat setiap log yang berhubungan dengan database.

5.2. Konfigurasi Mode Httpd-Accelerator

Berikut kita akan membahas bagian-bagian yang perlu diedit pada file squid.conf :

`http_port 80`

Option ini menyatakan nomor port yang akan digunakan Squid untuk permintaan HTTP client. Jika diset 80, client akan seolah-olah terkoneksi dengan Webserver Apache.

`icp_port 0`

Option ini menentukan nomor port tempat Squid mengirim dan menerima permintaan ICP dari cache lainnya. Untuk mendisable kita set 0, karena kita mengkonfigurasi Squid sebagai mode accelerator Web Server. ICP diperlukan hanya pada multilevel cache dengan multilevel siblings dan parent.

`acl QUERY urlpath_regex cgi-bin \? and no_cache deny QUERY`

Option ini menyatakan objek yang tidak pernah dicached.

`cache_mem 16 MB`

Option ini menyatakan jumlah memori (RAM) yang digunakan untuk caching. Squid menggunakan memori lebih besar dari nilai yang tertera. Sebaiknya jumlah ini sepertiga dari memori total.

`cache_dir ufs /cache 200 16 256`

Option "cache_dir" menyatakan jenis sistem storage yang digunakan (ufs). Space disk sebesar 200 MB, jumlah subdirektori tingkat pertama dalam direktori cache adalah 16 dan jumlah subdirektori tingkat kedua yang dibuat dalam direktori cache tingkat pertama adalah 256. Dalam mode accelerator hal ini berkaitan dengan besar dan jumlah file yang ingin di tampilkan pada webserver Apache.

`emulate_httpd_log on`

Jika option ini dibuat "ON", Squid akan membuat format file log yang sama dengan Webserver Apache. Hal ini berguna terutama jika kita ingin menggunakan program seperti Webalizer.

```
redirect_rewrites_host_header off
```

Jika diset "OFF", Squid tidak akan menulis ulang suatu host.

```
replacement_policy GDSF
```

Option "replacement_policy" menyatakan objek dalam cache yang akan dihapus Squid saat proxy membutuhkan ruang disk yang lebih banyak.

```
acl all src 0.0.0.0/0.0.0.0 and http_access allow all
```

Options "acl" and "http_access" mengatur batasan akses terhadap Proxy server Squid. Pada contoh di atas, kita berarti mengizinkan setiap orang terkoneksi lewat proxy.

```
cache_mgr admin
```

Option "cache_mgr" menyatakan alamat e-mail administrator yang bertanggung-jawab pada server.

```
cache_effective_user squid and cache_effective_group squid
```

Options ini menyatakan UID/GID dimana cache berjalan.

```
httpd_accel_host 167.205.206.100 and httpd_accel_port 80
```

Dari option ini, Squid akan mengetahui nomor port HTTP server yang sebenarnya dan IP address yang digunakan. Pada contoh di atas IP address webserver adalah 167.205.206.100 pada port 80.

```
log_icp_queries off
```

Jika kita tidak menggunakan ICP sebaiknya option ini diset "OFF".

```
cachemgr_passwd my-secret-pass all
```

Option "cachemgr_passwd" menyatakan password yang diperlukan untuk mengakses utilitas program "cachemgr.cgi". Isilah <my-secret-pass> dengan password yang diinginkan. Keyword <all> akan membuat password yang sama untuk semua

buffered_logs on

Option "buffered_logs" yang diset "ON" dapat menambah kecepatan penulisan beberapa file log.

5.3. Konfigurasi Mode Proxy-Caching Mode

Pada proxy-caching server, semua user dalam network kita menggunakan Squid untuk mengakses Internet. Tentu saja kita dapat menerapkan beberapa aturan dan menghemat bandwidth. Konfigurasi Squid sebagai proxy-caching mode tidak jauh berbeda dengan mode sebelumnya, hanya mungkin ada beberapa option yang diubah atau ditambahkan. Perbedaan utama dengan mode sebelumnya adalah adanya access control list (ACL). ACL berguna untuk merestriksi akses berdasarkan IP address asal (src), IP address tujuan (dst), domain asal, domain tujuan, berdasarkan waktu akses, dsb. Konfigurasi ACL yang umum digunakan adalah sebagai berikut :

- Akses berdasarkan IP address asal
acl [alamat] src a.b.c.d/e.f.g.h
- Akses berdasarkan IP address tujuan
acl [alamat] dst a.b.c.d/e.f.g.h
- Akses berdasarkan domain asal
acl [alamat] srcdomain [nama.domain]
- Akses berdasarkan domain tujuan
acl [alamat] dstdomain [nama.domain]

Untuk lebih jelasnya perhatikan contoh isi file konfigurasi proxy-cache server berikut ini :

```
# pico squid.conf
```

```
icp_port 0
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_mem 16 MB
cache_dir ufs /cache 200 16 256
redirect_rewrites_host_header off
replacement_policy GDSF
```

Misalkan kita ingin agar proxy server Squid hanya membolehkan akses untuk client dalam jaringan kita dan proxy server itu sendiri dengan menggunakan port-port tertentu yaitu 80 (http), 21 (ftp), 23 (telnet) 25 (smtp), dan 443 (https). Selain itu, proxy Squid akan meolak setiap IP address asal dan semua port yang mencoba terkoneksi. Bila jaringan kita menggunakan IP Private kelas C 192.168.1.0 kita dapat membuat konfigurasi sbb :

```
acl localnet src 192.168.1.0/255.255.255.0
acl localhost src 127.0.0.1/255.255.255.255
acl Safe_ports port 80 443 210 119 70 21 1025-65535
acl CONNECT method CONNECT
acl all src 0.0.0.0/0.0.0.0
http_access allow localnet
http_access allow localhost
http_access deny !Safe_ports
http_access deny CONNECT
http_access deny all
cache_mgr admin@nama.domain
cache_effective_user squid
cache_effective_group squid
log_icp_queries off
cachemgr_passwd my-secret-pass all
buffered_logs on
```

Sedangkan option-option yang lain sama seperti yang sudah dijelaskan untuk mode sebelumnya.

6. Menjalankan Squid

Setelah membuat konfigurasi Squid lewat file squid.conf, selanjutnya kita harus menstart squid agar server itu dapat berjalan dengan baik. Proses squid sebaiknya dijalankan oleh user squid dan bukan oleh root demi keamanan.

- To run Squid server in httpd-accelerator mode, the following files are required and must

be created or copied to the appropriate directories on your server.

Copy the **squid.conf** file in the `"/etc/squid/"` directory.

Copy the **squid** script file in the `"/etc/rc.d/init.d/"` directory.

Copy the **squid** file in the `"/etc/logrotate.d/"` directory.

- To run Squid server in proxy-caching mode, the following files are required and must be

created or copied to the appropriate directories on your server.

Copy the **squid.conf** file in the `"/etc/squid/"` directory.

Copy the **squid** script file in the `"/etc/rc.d/init.d/"` directory.

Copy the **squid** file in the `"/etc/logrotate.d/"` directory.

Create the **squid** script file (`touch /etc/rc.d/init.d/squid`) and add:

```
#!/bin/bash
# squid This shell script takes care of starting and stopping
# Squid Internet Object Cache
#
# chkconfig: - 90 25
# description: Squid - Internet Object Cache. Internet object caching is \
# a way to store requested Internet objects (i.e., data available \
# via the HTTP, FTP, and gopher protocols) on a system closer to the \
# requesting site than to the source. Web browsers can then use the \
# local Squid cache as a proxy HTTP server, reducing access time as \
```

```
# well as bandwidth consumption.  
# pidfile: /var/run/squid.pid  
# config: /etc/squid/squid.conf
```

Untuk menjalankan squid Pertama-tama kita harus membuat user squid yang akan menjalankan proses Squid proxy server. Loginlah sebagai user squid dan lakukan perintah berikut ini :

```
# squid -z
```

Perintah ini akan membuat direktori cache sebanyak dan sedalam yang telah dideklarasikan pada file squid.conf. Lalu jalankan program squid :

```
# /usr/local/squid/bin/squid -sY &
```

Perhatikan pesan yang muncul pada console, dan perhatikan juga file /usr/local/squid/log/cache.log barangkali terjadi suatu kegagalan atau error. Agar saat sistem direboot program Squid akan langsung berjalan secara otomatis, tambahkan baris berikut ini pada file /etc/rc.d/rc.local/ :

```
# pico /etc/rc.d/rc.local
```

Tambahlah baris-baris berikut ini :

```
/usr/local/squid/bin/squid -sY &
```

- c. Rangkuman 3
- d. Tugas 3
 - a. Instalasi Squid
 - b. Konfigurasi Squid.conf
 - c. Konfigurasi Mode Proxy-Caching Mod
 - d. Menjalankan Squid
- e. Tes Formatif 3
- f. Kunci Jawaban Formatif 3
- g. Lembar Kerja 3

1. Instalasi Squid:

```
# cp squid-2.3.STABLE2-src.tar.gz /usr/local
```

```
# cd /usr/local
# tar zxvf squid-2.3.STABLE2-src.tar.gz
# useradd -d /cache/ -r -s /dev/null 2>&1
# mkdir /cache/
# chown -R squid.squid /cache/
# ./configure --prefix=/usr/local/squid
# make
# make install
```

2. Konfigurasi squid.conf

```
Httpd-Accelerator
http_port 80
icp_port 0
acl QUERY urlpath_regex cgi-bin \? and no_cache deny QUERY
cache_mem 16 MB
cache_dir ufs /cache 200 16 256
emulate_httpd_log on
redirect_rewrites_host_header off
replacement_policy GDSF
acl all src 0.0.0.0/0.0.0.0 and http_access allow all
cache_mgr admin
cache_effective_user squid and cache_effective_group squid
httpd_accel_host 167.205.206.100 and httpd_accel_port 80
log_icp_queries off
cachemgr_passwd my-secret-pass all
buffered_logs on
```

3. Konfigurasi Mode Proxy-Caching Mod

```
icp_port 0
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_mem 16 MB
```

```

cache_dir ufs /cache 200 16 256
redirect_rewrites_host_header off
replacement_policy GDSF
acl localnet src 192.168.1.0/255.255.255.0
acl localhost src 127.0.0.1/255.255.255.255
acl Safe_ports port 80 443 210 119 70 21 1025-65535
acl CONNECT method CONNECT
acl all src 0.0.0.0/0.0.0.0
http_access allow localnet
http_access allow localhost
http_access deny !Safe_ports
http_access deny CONNECT
http_access deny all
cache_mgr admin@nama.domain
cache_effective_user squid
cache_effective_group squid
log_icp_queries off
cachemgr_passwd my-secret-pass all
buffered_logs on

```

4. Menjalankan Squid

Loginlah sebagai squid

```
login : squid
```

```
# squid -z
```

```
# /usr/local/squid/bin/squid -sY &
```

```
# pico /etc/rc.d/rc.local
```

Tambahkan baris berikut ini :

```
/usr/local/squid/bin/squid -sY &
```

4. Kegiatan Belajar 4 : tentang mengisi log sheet / report sheet

a. Tujuan Kegiatan Pemelajaran

b. Uraian Materi 4

Membahas tentang mengisi log sheet / report sheet

Disini hanya akan diberikan pengenalan tentang sintaks SQL dalam MySQL yang sederhana dan paling sering digunakan baik untuk penggunaan biasa ataupun untuk administratif.

Berikut adalah beberapa sintaks dasar SQL dalam MySQL

a. Level Database

- Membuat database

Untuk membuat database baru, sehingga tidak berlaku jika database sudah ada atau anda tidak memiliki privilege.

Sintaksnya :

```
CREATE DATABASE nama_db
```

- Menghapus database

Untuk menghapus database beserta seluruh table di dalamnya. Perintah ini tidak berlaku jika database tidak ada atau anda tidak memiliki privilege.

Sintaksnya :

```
DROP DATABASE nama_db
```

- Menggunakan database

Untuk menjadikan database menjadi default dan referensi dari table yang nantinya anda gunakan. Perintah ini tidak berlaku jika database tidak ada atau anda tidak memiliki privilege. Sintaksnya :

```
USE nama_db
```

- Menampilkan database

Untuk menampilkan daftar yang ada dalam system saat itu. Sintaksnya :

```
SHOW DATABASES
```

Tampilannya adalah :

```

+-----+
| Database |
+-----+
| contoh_db |
| mysql   |
| test    |
| ujian   |
+-----+
4 rows in set (0.00 sec)

```

b. Level Tabel

- Membuat table

Untuk membuat table minimal anda harus menentukan namanya dan tipe kolom yang anda inginkan. Sintaks yang paling sederhana (tanpa ada definisi lain) adalah :

```

CREATE TABLE nama_tbl
      (kolom1 tipekolom1(),kolom2 tipekolom2(), ...)

```

Contoh : Anda ingin membuat table dengan nama profil yang memiliki kolom nama (bertipe char, lebar 20), kolom umur (bertipe integer), kolom jenis_kelamin (bertipe enum, berisi M dan F). Sintaksnya :

```

CREATE TABLE profil (
      nama CHAR(20), umur INT NOT NULL,
      jenis_kelamin ENUM('F','M') )

```

Sedangkan perintah yang agak lengkap dalam membuat sebuah table adalah dengan menyertakan definisi tertentu. Misalnya perintah seperti ini :

```

CREATE TABLE peserta (
      No SMALLINT UNSIGNED NOT NULL AUTO_INCREMENT,
      Nama CHAR(30) NOT NULL,
      BidangStudi ENUM('TS','WD') NOT NULL,
      PRIMARY KEY (No),
      INDEX (Nama, BidangStudi) )

```

Perintah di atas berarti membuat table peserta dengan kolom No sebagai PRIMARY KEY yaitu indeks table yang unik yang tidak bisa diduplikat dengan atribut AUTO_INCREMENT yaitu kolom yang otomatis dapat

mengurutkan angka yang diisikan padanya. Sedangkan kolom Nama dan BidangStudi dijadikan indeks biasa.

- Membuat indeks pada table

Menambahkan indeks pada table yang sudah ada baik yang unik ataupun yang biasa.

Sintaksnya :

```
CREATE INDEX nama_index ON nama_tbl (nama_kolom)
CREATE UNIQUE INDEX nama_index ON nama_tbl (nama_kolom)
```

- Menghapus table

Untuk menghapus table dalam database tertentu. Jika dilakukan maka semua isi, indeks dan atribut lain akan terhapus. Sintaksnya :

```
DROP TABLE nama_tbl
```

- Menghapus indeks

Untuk menghapus indeks pada suatu table. Sintaksnya :

```
DROP INDEX nama-index ON nama_tbl
```

- Melihat informasi table

Untuk melihat table apa saja yang ada di database tertentu. Sintaksnya :

```
SHOW TABLES FROM nama_db
```

Sedangkan untuk melihat deskripsi table atau informasi tentang kolom gunakan sintaks :

```
DESC nama_tbl nama_kolom
atau SHOW COLUMNS FROM nama_tbl FROM nama_db
```

Misal untuk contoh di atas akan ditampilkan :

```
+-----+
| Tables_in_contoh_db |
+-----+
| peserta          |
| profil          |
+-----+
2 rows in set (0.00 sec)
```

```

+-----+-----+-----+-----+-----+-----+
| Field      | Type      | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| nama       | char(20)  | YES  |     | NULL    |      |
| umur       | int(11)   |      |     | 0       |      |
| jenis_kelamin | enum('F','M') | YES  |     | NULL    |      |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.02 sec)

```

- Mendapatkan atau menampilkan informasi dari table

Untuk menampilkan isi table dengan option-option tertentu. Misalnya untuk menampilkan seluruh isi table digunakan :

```
SELECT * FROM nama_tbl
```

Untuk menampilkan kolom-kolom tertentu saja :

```
SELECT kolom1,kolom2,... FROM nama_tbl
```

Untuk menampilkan isi suatu kolom dengan kondisi tertentu

```
SELECT kolom1 FROM nama_tbl WHERE kolom2=isikolom
```

- Modifikasi struktur table

Dapat digunakan untuk mengganti nama table atau mengubah strukturnya seperti manambah kolom atau indeks, menghapus kolom atau indeks, mengubah tipe kolom dsb. Sintaks umum :

```
ALTER TABLE nama_tbl action
```

Untuk menambah kolom baru di tempat tertentu dapat menggunakan :

```
ALTER TABLE nama_tbl
ADD kolom_baru type() definisi
```

Untuk menambah kolom_baru bertipe integer setelah kolom1 digunakan :

```
ALTER TABLE nama_tbl
ADD kolom_baru INT NOT NULL AFTER kolom1
```

Untuk menambah indeks baru pada table tertentu baik yang unik ataupun yang biasa:

```
ALTER TABLE nama_tbl ADD INDEX nama_index (nama_kolom)
ALTER TABLE nama_tbl ADD UNIQUE nama_indeks (nama_kolom)
ALTER TABLE nama_tbl ADD PRIMARY KEY nama_indeks
(nama_kolom)
```

Untuk mengubah nama kolom dan definisinya, misalnya mengubah nama kolom_baru dengan tipe integer menjadi new_kolom dengan tipe char dengan lebar 30 digunakan:

```
ALTER TABLE nama_tbl  
CHANGE kolom_baru new_kolom CHAR(30) NOT NULL
```

Untuk menghapus suatu kolom dan seluruh atributnya, misal menghapus kolom1 :

```
ALTER TABLE nama_tbl DROP kolom1
```

Untuk menghapus indeks baik yang unik ataupun yang biasa digunakan :

```
ALTER TABLE nama_tbl DROP nama_index  
ALTER TABLE nama_tbl DROP PRIMARY KEY
```

- Modifikasi informasi dalam table.

Untuk menambah record atau baris baru dalam table, sintaksnya :

```
INSERT INTO nama_tbl (nama_kolom) VALUES (isi_kolom)  
atau INSERT INTO nama_tbl SET nama_kolom=isi_kolom
```

Misalnya untuk menambah dua baris pada table profil dengan isi nama = deden & ujang dan isi umur = 17 & 18 adalah :

```
INSERT INTO profil (nama,umur) VALUES (deden,17), (ujang,18)  
atau INSERT INTO profil SET nama=deden, umur=17  
INSERT INTO profil SET nama=ujang, umur=18
```

Untuk memodifikasi record atau baris yang sudah ada yang bersesuaian dengan suatu kolom. Misalnya untuk mengubah umur deden menjadi 18 pada contoh di atas dapat digunakan sintaks :

```
UPDATE profil SET umur=18 WHERE nama=deden
```

Untuk menghapus record atau baris tertentu dalam suatu table. Misalnya untuk menghapus baris yang ada nama ujang digunakan sintaks :

```
DELETE FROM profil WHERE nama=ujang
```

Jika WHERE tidak disertakan maka semua isi dalam table profil akan terhapus.

2. Tipe-tipe data MySQL

MySQL dapat mengetahui beberapa tipe data antara lain :

- Data Numerik

MySQL dapat menerima masukan berupa angka-angka yang dibagi atas integer (angka tanpa pecahan) dan floating-point (angka dengan pecahan).

MySQL juga mengerti notasi scientific yaitu integer atau floating-point yang diikuti tanda 'e' atau 'E', tanda '+' atau '-'. Misalnya angka 1.34E+ 12 atau 3.23e-5.

- **Data Karakter/String**

Merupakan deretan huruf yang membentuk kata yang diapit oleh tanda petik (') atau tanda petik ganda ("").

- **Data Waktu**

Merupakan data yang berisi tanggal (date) dan jam (time) misalnya "2001-10-15" untuk tanggal dengan format YYYY-MM-DD dan "12:45:15" untuk jam dengan format hh:mm:ss.

- **Data kosong (NULL)**

NULL berarti kosong atau tidak diisi data atau bisa juga berarti data yang tidak jelas, data yang hilang ataupun yang lainnya.

2.1 Tipe-tipe kolom MySQL

Setiap table yang dibuat dalam database selalu terdiri atas kolom-kolom. Ketika anda membuatnya dengan perintah CREATE TABLE, anda harus menentukan tipe masing-masing kolom. Tiap tipe kolom memiliki karakteristik berikut :

- Jenis harga apa yang dapat diisikan
- Berapa banyak ruang yang dapat menampung harga tersebut
- Bagaimana harga dari tipe tersebut dibandingkan dan disaring
- Apakah tipe tersebut boleh mengisi dengan NULL atau tidak
- Apakah tipe tersebut boleh diindeks atau tidak

Secara garis besar kolom MySQL terbagi menjadi tiga tipe yaitu :

- Tipe kolom Numerik
- Tipe kolom Karakter/String
- Tipe kolom Waktu

Selanjutnya akan dijelaskan dengan singkat anggota-anggotanya.

2.2 Tipe Numerik

Tipe ini untuk harga integer dan floating-point. Untuk integer kolom haruslah PRIMARY KEY atau indeks yang unik jika ia diberi atribut AUTO_INCREMENT

(dapat otomatis mengurutkan angka). Jika diberikan atribut UNSIGNED berarti angka tidak boleh negatif. Sedangkan atribut ZEROFILL menandakan bahwa angka diawali dengan angka nol.

- TINYINT

Berarti integer dengan range yang sangat kecil yaitu -2^7 sampai 2^7-1 atau 0 sampai 2^8-1 jika UNSIGNED. Atribut yang dibolehkan adalah AUTO_INCREMENT, UNSIGNED, dan ZEROFILL. Harga default adalah NULL jika bisa atau 0 jika NOT NULL dengan penyimpanan 1 byte.

- SMALLINT

Berarti integer dengan range yang kecil yaitu -2^{15} sampai $2^{15}-1$ atau 0 sampai $2^{16}-1$ jika UNSIGNED. Atribut yang dibolehkan adalah AUTO_INCREMENT, UNSIGNED, dan ZEROFILL. Harga default adalah NULL jika bisa atau 0 jika NOT NULL dengan penyimpanan 2 byte.

- MEDIUMINT

Berarti integer dengan range yang sangat kecil yaitu -2^{23} sampai $2^{23}-1$ atau 0 sampai $2^{24}-1$ jika UNSIGNED. Atribut yang dibolehkan adalah AUTO_INCREMENT, UNSIGNED, dan ZEROFILL. Harga default adalah NULL jika bisa atau 0 jika NOT NULL dengan penyimpanan 3 byte.

- INT

Berarti integer dengan range yang normal yaitu -2^{31} sampai $2^{31}-1$ atau 0 sampai $2^{32}-1$ jika UNSIGNED. Atribut yang dibolehkan adalah AUTO_INCREMENT, UNSIGNED, dan ZEROFILL. Harga default adalah NULL jika bisa atau 0 jika NOT NULL dengan penyimpanan 4 byte.

- BIGINT

Berarti integer dengan range yang sangat kecil yaitu -2^{63} sampai $2^{63}-1$ atau 0 sampai $2^{64}-1$ jika UNSIGNED. Atribut yang dibolehkan adalah AUTO_INCREMENT, UNSIGNED, dan ZEROFILL. Harga default adalah NULL jika bisa atau 0 jika NOT NULL dengan penyimpanan 8 byte.

- FLOAT

Berarti floating-point dengan range kecil yaitu antara $\pm 1.175494351E-38$ sampai $\pm 3.402823466E+38$ serta dengan single presisi. Atribut yang

dibolehkan adalah ZEROFILL. Harga default NULL jika bisa atau 0 jika NOT NULL. Tempat penyimpanan 4 byte.

- **DOUBLE**

Berarti floating-point dengan range besar yaitu antara $\pm 2.22507385072014E-308$ sampai $\pm 1.7976931348623157E308$ serta dengan double presisi. Atribut yang dibolehkan adalah ZEROFILL. Harga default NULL jika bisa atau 0 jika NOT NULL. Tempat penyimpanan 8 byte.

- **DECIMAL(M,D) atau NUMERIC(M,D)**

Berarti floating-point yang tersimpan sebagai string (1 byte untuk setiap digit, tanda desimal, atau tanda '-'). Range harga sama seperti DOUBLE. Atribut yang dibolehkan adalah ZEROFILL. Tempat penyimpanan sebesar M byte. Jika D diisi 0 berarti tidak punya nilai desimal.

2.3 Tipe String

- **CHAR(M)**

Karakter dengan panjang 0 sampai M byte. Atribut yang dibolehkan adalah BINARY. Harga default adalah NULL jika bisa atau "" jika NOT NULL. Tempat penyimpanan M byte.

- **VARCHAR**

Variabel karakter dengan panjang 0 sampai M byte. Atribut yang dibolehkan adalah BINARY. Harga default adalah NULL jika bisa atau "" jika NOT NULL. Tempat penyimpanan M+1 byte.

- **TINYTEXT**

Teks berukuran kecil dengan panjang 0 sampai 2^8-1 byte. Harga default adalah NULL jika bisa atau "" jika NOT NULL. Tempat penyimpanan sebanyak panjang harga plus 1 byte.

- **TEXT**

Teks yang normal dengan panjang 0 sampai $2^{16}-1$ byte. Harga default adalah NULL jika bisa atau "" jika NOT NULL. Tempat penyimpanan sebanyak panjang harga plus 2 byte.

- **MEDIUMTEXT**
Teks berukuran sedang dengan panjang 0 sampai $2^{24}-1$ byte. Harga default adalah NULL jika bisa atau "" jika NOT NULL. Tempat penyimpanan sebanyak panjang harga plus 3 byte.
- **LONGTEXT**
Teks berukuran besar dengan panjang 0 sampai $2^{32}-1$ byte. Harga default adalah NULL jika bisa atau "" jika NOT NULL. Tempat penyimpanan sebanyak panjang harga plus 4 byte.
- **ENUM("harga1","harga2",...)**
Berarti kolom hanya boleh diisi dengan salah satu dari harga yang ada. Harga default adalah NULL jika bisa atau harga1 jika NOT NULL. Tempat penyimpanan adalah 1 byte untuk enumerasi dengan anggota 1 sampai 255 dan 2 byte untuk enumerasi dengan anggota 256 sampai 65535.
- **SET("harga1","harga2",...)**
Berarti kolom boleh dikosongi atau diisi dengan beberapa harga dari daftar harga yang ada. Harga default adalah NULL jika bisa atau "" jika NOT NULL. Tempat penyimpanan adalah 1 byte untuk set dengan anggota 1 sampai 8, 2 byte untuk set dengan anggota 9 sampai 16, 3 byte untuk set dengan anggota 17 sampai 24, 4 byte untuk set dengan anggota 25 sampai 32, atau 8 byte untuk set dengan anggota 33 sampai 64.

2.4 Tipe Waktu

- **DATE**
Untuk kolom tanggal dengan format YYYY-MM-DD dan range antara "1000-01-01" sampai "9999-12-31". Harga default adalah NULL jika bisa atau "0000-00-00" jika NOT NULL. Tempat penyimpanan 3 byte.
- **TIME**
Untuk kolom jam dengan format hh:mm:ss atau -hh:mm:ss untuk harga negatif. Range harga antara "-838:59:59" sampai "838:59:59". Harga default adalah NULL jika bisa atau "00:00:00" jika NOT NULL. Tempat penyimpanan 3 byte.

- **DATETIME**
Gabungan antar hari dan jam dengan format YYYY-MM-DD hh:mm:ss dan range antar "1000-01-01 00:00:00" sampai "9999-12-31 23:59:59". Harga default adalah NULL jika bisa atau "0000-00-00 00:00:00" jika NOT NULL. Tempat penyimpanan 8 byte.
- **TIMESTAMP**
Hampir sama dengan DATETIME tapi dengan format YYYYMMDDhhmmss dan range antara 19700101000000 sampai suatu saat di tahun 2037. Harga default adalah hari dan jam saat itu. Tempat penyimpanan 4 byte.
- **YEAR**
Untuk kolom tahun dengan format YYYY dan range antara 1900 sampai 2155. Harga default adalah NULL jika bisa atau 0000 jika NOT NULL. Tempat penyimpanan 3 byte.

- c. Rangkuman 4
- d. Tugas 4
- e. Tes Formatif 4
- f. Kunci Jawaban Formatif 4
- g. Lembar Kerja 4

5. Kegiatan Belajar 5 : tentang Security

a. Tujuan Kegiatan Pemelajaran

- 1) Peserta diklat bisa mengamankan server
- 2) Peserta diklat mampu melakukan update system

b. Uraian Materi 5

Apakah Linux Aman?

Sering pengguna linux beranggapan bahwa system operasi system yang digunakannya sudah cukup aman, apalagi jika dibandingkan dengan system operasi lain, hal ini membuat pengguna menjadi lengah, padahal semua buatan manusia tidak ada yang sempurna.

Pada system operasi yang didistribusikan dengan lisensi open Source, begitu sebuah bak atau kelemahan program ditemukan, maka dalam waktu yang relative singkat akan muncul update atau versi perbaikan dari program tersebut.

Supaya kelemahan pada system tidak bisa diserang oleh pihak yang sudah mengetahui kelemahan tersebut, selalu melakukan update jika ada versi yang baru dari sebuah program atau layanan yang berjalan pada system linux tersebut.

Tergantung pada jenis linux yang digunakan, biasanya update tersedia diinternet pada masing-masing situsnya. Selain melakukan update system, untuk lebih memperkuat keamanan system linux, ada beberapa praktik yang dapat dilakukan. Bab ini akan menjelaskan beberapa caranya.

Memilih Password yang Baik

Hak akses seorang user pada system dilindungi sebuah password. Dengan adanya password, seorang user dapat mengakses system. Keamanan sebuah system tergantung pada password tersebut karena orang tidak memiliki hak akses dapat saja masuk ke system menggunakan password tersebut, oleh karena password harus dibuat agar tidak mudah diketahui orang lain. Berikut ini beberapa hal yang sebaiknya diperhatikan dalam membuat password:

1. Jangan menggunakan passwaord yang sama dengan nama login.
2. Jangan menggunakan kata yang berhubungan dengan anda, seperti misalnya nama anda, nama pacar atau isteri, no.telepon, dan lain-lain yang sudah diketahui oleh orang lain.
3. Jangan menggunakan password yang terlalu pendek, gunakan minimal 6 sampai 10 karakter.
4. Gunakan kombinasi antara huruf besar, huruf kecil, dan angka.
5. Gunakan password yang mudah diingat tetapi susah ditebak oleh oarang lain dan jangan menuliskan password dimana pun.
6. Jika diperlukan password dapat diganti setiap beberapa bulan sekali.

Contoh password yang aman tetapi mudah diingat adalah password yang disusun dari singkatan sebuah kalimat, misalnya kalimat: "berakit-rakit ke hulu, berenang-renang ketepian", dari kalimat tersebut, diambil huruf depan dari setiap kata sehingga menjadi "b-rkhhb-rkt" kemudian kombinasikan antara huruf besar dan huruf kecil sehingga menjadi "B-rkhB-rkt".

Hindari Menggunakan User root

User root adalah user yang memiliki hak akses penuh terhadap system. Jika tidak diperlukan sebaiknya user root ini sebaiknya tidak digunakan. Biasakan untuk selalu bekerja menggunakan user biasa, dan ketika hak akses root diperlukan, gunakan perintah su.

Perintah su digunakan untuk berpindah dari suatu user ke user lainnya termasuk untuk berpindah menjadi root. Untuk berpindah menjadi user lain perintahnya:

```
# su - namauser
```

Dimana nama user adalah user yang akan dituju, sedangkan untuk berpindah menjadi user root, perintahnya:

```
# su -
```

Untuk lebih meningkatkan keamanan, perintah ini dapat dibatasi sehingga hanya user-user tertentu saja yang dapat menggunakannya. Caranya adalah dengan mengedit file /etc/suauth, tambahkan baris berikut pada file tersebut:

```
Root:ALL EXCEPT GROUP wheel: DENY
```

Baris tersebut akan membatasi perintah su hanya dapat digunakan oleh user dalam group wheel.

Mematikan Service yang tidak Diperlukan

Dalam instalasi default, biasanya distribusi-distribusi Linux menyediakan banyak service seperti web server, e-mail, FTP dan lain-lain. Padahal kadang tidak semua service tersebut diperlukan. Semakin sedikit service yang berjalan, server tersebut akan semakin aman.

Untuk mengetahui proses apa saja yang berjalan pada server, gunakan perintah:

```
# ps -aux
```

Atau:

```
# pstree
```

Sedangkan untuk melihat port yang digunakan oleh masing-masing service, gunakan perintah:

```
# netstat -atu
```

Beberapa distribusi seperti Red Hat menggunakan perintah chkconfig untuk melihat service apa saja yang akan dijalankan ketika server dihidupkan. Perintahnya adalah berikut:

```
# chkconfig --del service
```

Di mana service adalah nama service yang akan dimatikan, contohnya:

```
# chkconfig --del sendmail
```

Setelah selesai mengurangi service yang tidak diperlukan, lakukan tes dengan cara restart server. Jika server tersebut masih belum digunakan, hal ini untuk memastikan bahwa memang service yang tidak diperlukan tidak akan berjalan lagi jika suatu hari server direstart. Perintahnya:

```
# shutdown -r now
```

Setelah itu periksa kembali dengan menggunakan perintah ps atau pstree dan netstat.

SUID dan SGID

SUID dan SGID adalah file yang sewaktu dijalankan oleh user biasa, akan memiliki hak akses yang sesuai dengan pemilik file tersebut. Jadi, jika pemilik file tersebut adalah root, maka ketika user biasa menjalankan file tersebut, file akan memiliki hak akses yang sama dengan root (mengenai hak akses, dapat dibaca pada bab sebelumnya). Berikut adalah contoh sebuah file SUID:

```
-r-sr-xr-x 1 root root 36453 Jun 10 11:32  
/usr/sbin/filesuid
```

Tanda s pada hak akses user (yang biasanya x) menandakan bahwa itu adalah file tersebut akan berjalan oleh user biasa, maka file tersebut akan berjalan dengan hak akses pemilik file tersebut, dalam hal ini adalah root.

Berikut adalah sebuah contoh file SGID:

```
-r-xr-sr-x 1 root root 36453 Jun 10 11:32  
/usr/sbin/filesiud
```

Perhatikan tanda s pada hak akses grup pada file tersebut yang menandakan bahwa ini adalah file SGID. File ini, jika dijalankan, akan berjalan dengan hak akses grup sesuai dengan hak akses pemilik file, dalam hal ini adalah root.

File SGID dan SUID ini sering digunakan oleh cracker untuk mendapatkan hak akses ke sistem. File jenis ini harus diawasi keberadaannya. Untuk mencari file jenis ini diseluruh sistem kita, gunakan perintah find (tentang perintah find sudah dibahas pada bab sebelumnya), caranya:

```
# find / -perm -4000 -0 -perm -2000 -exec ls -ldb {} \;  
>> hasil. Txt
```

Perintah di atas akan mencari sebuah file SUID dan SGID mulai dari direktori root dan menyimpan hasilnya dalam file hasil.txt.

Hak akses SUID dan SGID dapat dihilangkan dengan menggunakan perintah chmod (perintah ini sudah dibahas pada bab sebelumnya), perintahnya:

```
# chmod -s namafile
```

Di mana namafile adalah nama file yang akan dihilangkan hak akses SUID atau SGID-nya.

Periksa File yang Tidak Ada Pemiliknya

File yang tidak ada pemiliknya dapat mengindikasikan adanya seseorang yang berhasil memasuki sistem tanpa ijin. Carilah file semacam ini secara periodik dan jika ditemukan, file tersebut dapat dihapus atau dimasukkan ke dalam salah satu user dengan perintah chown. Cara mencari tipe file seperti ini adalah dengan perintah:

```
# find / -nouser -o -nogroup
```

Untuk mengganti pemilik file perintahnya:

```
# chown user.grup namafile
```

Dimana user adalah user yang akan dijalankan pemilik file dan grup adalah grup dari user tersebut, sedangkan namafile adalah namafile yang akan diganti pemiliknya.

Menggunakan umask

Perintah umask digunakan untuk mendefinisikan hak akses yang akan diterapkan ketika sebuah file dibuat. Perintah umask 022 akan membuat hak akses setiap file yang baru dibuat menjadi 644 atau read write untuk pemilik file dan read untuk group dan other.

Tambahkan perintah umask 022 tersebut pada file `/etc/profile` sehingga setiap kali komputer dihidupkan, perintah tersebut akan dijalankan.

Menggunakan chattr

Perintah chattr digunakan atribut sebuah file menjadi read-only atau hanya bisa dibaca dan append-only atau hanya bisa ditambah.

Sebuah file dibuat read-only untuk melindungi supaya tidak dapat diubah oleh semua user termasuk user root. Jika file tersebut perlu diubah, user root dapat menghapus atribut read-only tersebut terlebih dahulu, kemudian mengubah file.

Atribut append-only digunakan supaya file tersebut tidak dapat diubah, tetapi hanya dapat ditambah. File log seperti `/var/log/messages` lebih baik dibuat append-only supaya orang lain tidak dapat menghapus isinya, caranya:

```
# chattr +a /var/log/messages
```

Untuk mengilangkan atribut di atas, gunakan:

```
# chattr -a /var/log/messages
```

Untuk membuat sebuah file memiliki atribut read-only, gunakan perintah:

```
# chattr +i /etc/services
```

Untuk melihat atribut yang sudah di-set, gunakan perintah `lsattr`.

SSH

Jika diperlukan akses komputer lain dalam jaringan, jangan gunakan telnet karena telnet mengirimkan semua informasi termasuk data penting seperti password dalam bentuk teks biasa.

Untuk itu SSH dapat digunakan karena ia memiliki fungsi yang sama dengan telnet. Bedanya, pada SSH setiap data yang akan dikirim diacak terdahulu sehingga lebih aman.

Sewaktu instalasi Linux, biasanya SSH sudah terinstal, ada beberapa setting yang dapat diubah untuk membuat SSH lebih aman, letak file setting SSH ada di `/etc/ssh_config` dan `/etc/ssh/sshd_config`

Yang pertama adalah jangan menggunakan user root untuk login; untuk menghalangi user menggunakan user root, set parameter `permitRootLogin` menjadi `no`. Untuk mengakses user root pada komputer lain, login terlebih dahulu dengan user biasa, kemudian gunakan perintah `su` untuk mengubah user menjadi root.

Yang berikutnya, set parameter `StrictMode` menjadi `yes`. Parameter ini akan membuat user tidak mengakses direktori home dari user yang lainnya.

User yang diperbolehkan untuk mengakses sistem dengan menggunakan SSH juga dapat dibatasi, caranya adalah dengan menuliskannya pada parameter `AllowUsers`, contohnya:

```
AllowUser user1 user2 user3
```

Pembatasan tersebut juga dapat dilakukan berdasarkan nomor IP dari komputer yang mengakses, untuk itu gunakan parameter `AllowHosts`, contohnya:

```
AllowHosts 192.168.1.1 192.168.1.2
```

- c. Rangkuman 5
- d. Tugas 5
- e. Tes Formatif 5
- f. Kunci Jawaban Formatif 5
- g. Lembar Kerja 5

6. Kegiatan Belajar 6: tentang Melaporkan hasil Administrasi Server

- a. Tujuan Kegiatan Pemelajaran
- b. Uraian Materi 6
- c. Rangkuman 6
- d. Tugas 6
- e. Tes Formatif 6
- f. Kunci Jawaban Formatif 6
- g. Lembar Kerja 6

BAB IV

PENUTUP

Demikian modul pembelajaran **Mengadministrasi Server dalam jaringan**. Materi yang telah dibahas dalam modul ini masih sangat sedikit. Hanya sebagai dasar saja bagi peserta diklat diharapkan untuk belajar lebih lanjut. Diharapkan peserta didik memanfaatkan modul ini sebagai motivasi untuk menguasai teknik menadministasri server dalam jaringan yang lebih jauh sehingga peserta diklat dapat melakukan tindakan pengisolasian permasalahan yang terjadi pada jaringan lokal atau berbasis luas yang tersambung dengan jaringan.

Setelah menyelesaikan modul ini dan mengerjakan semua tugas serta evaluasi maka berdasarkan kriteria penilaian, peserta diklat dapat dinyatakan lulus/tidak lulus. Apabila dinyatakan lulus maka dapat melanjutkan ke modul berikutnya sesuai dengan alur peta kedudukan modul, sedangkan apabila dinyatakan tidak lulus maka peserta diklat harus mengulang modul ini dan tidak diperkenankan mengambil modul selanjutnya.

DAFTAR PUSTAKA

Onno W. Purbo: Red Hat 9.0 , Desain, dan Implementasi, Elek Media
Komputindo, Jakarta, 1998

Onno W. Purbo: Info Linux,

www.linux.com

<http://www.ilmukomputer.com> diambil pada tanggal 26 Oktober 2004

PERISTILAHAN/GLOSSARY

Disk cleaner	:	cairan yang digunakan untuk membersihkan head pada diskdrive
Floopy drive / diskdrive	:	merupakan komponen komputer yang digunakan untuk penggerak floopy atau disket sebagai media penyimpan data
Scandisk	:	adalah tool yang digunakan untuk memeriksa struktur file sistem
Disk defragmenter	:	tool yang digunakan untuk mengatur struktur atau tata letak file sehingga akan mengurangi fragmentasi sebuah space hardisk.
VGA card	:	komponen komputer yang difungsikan untuk mengolah grafik untuk ditampilkan ke dalam layar monitor
CPU	:	Komponen ini merupakan otak dari komputer, kecepatan dan kecerdasan prosesor tergantung dari kecepatannya
Motherboard	:	merupakan tempat dari semua komponen komputer terpasang
Expansion card	:	merupakan komponen tambahan yang terpasang pada komputer
Heatsink	:	Pendingin

This document was created with Win2PDF available at <http://www.daneprairie.com>.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.